NATIONAL JUDICIAL ACADEMY

CAPACITY BUILDING SEMINAR TO HANDLE CYBER CRIMES

29th-31st January, 2016

VERBATIM REPORT

Prepared By:

Pragya Aishwarya
Law Associate, NJA

With Assistance From
Deeksha Garewal
Intern, NJA

Session 1

Dr. Geeta: Very Good Morning to all of you and happy New Year. So we meet in this new year for the first time, of course we have meet in other new year. I think first of all we will have introduction. I know all of you are shaking hands but I thought lets formally also introduce. So sir, maybe we came begin from right side so that we all know each other, it's a small group and surely at the end of this programme you will good friends, you will have your own network.

Participant: Good Morning to this august audience. I am Biswanath Somadder of Calcutta High Court.

Participant: I am

Participant: I am Pankaj Naqvi from Allahabad High Court

Participant: I am V.M. Velumani from Chennai High Court.

Participant: Raghvendra Singh Chauhan, Karnataka High Court

Participant: I am Dinesh Kumar, Karnataka High Court

Participant: I am P D. Rajan, Kerala High Court

Participant: I am Prashant Kumar Mishra, from Chhattisgarh High Court.

Participant: I am Sanjeev Sachdeva from Delhi High Court.

Participant: I am Ramalingeswara Rao from Andhra High Court.

Participant: I am Praveen Kumar from Andhra Pradesh High Court

Dr. Geeta: So Nappinai you would like to introduce yourself.

Nappinai: Good Morning, I am advocate from Mumbai, but originally from Chennai.

Mr. Deepak: good Morning Sir, I am Deepak, I work at Semantic, we are cyber Security Company and I am also the chair of BSA Policy, the software alliance. Thank you.

Participant: BSA stands for?

Mr. Deepak: BSA is basically a software company.

Participant: What is the full form of BSA?

Mr. Deepak: It used to be business software alliance, but now it is just called the software alliance.

Participant: Is it a private company?

Mr. Deepak: Yes it is private company.

Ms. Nappinai: It is the equivalent of Nasscom.

Dr. Geeta: I was just thinking I will give a background of this programme. It was demanded in the annual calendar meeting by all the Chief Justice and Judge In Charge of Judicial Education, reason being, all of you are aware I don't have to speak, like that, our world has drastically changed from communication to all our work now, we have shifted to another space all together and since we have ourselves transcended to another space, the crime has also grown to that another platform, and this seminar is actually about understanding, the kinds of crime and the new technologies that are developed, by industrial leaders, executives and government agencies, to curb that crime, to detect that crime, to investigate that crime and the difficulties that they face in producing evidences before courts, so that is why it is actually about cybercrimes, now with this we straightaway go to our technical session first which would be taken jointly by Ms. Nappinai and Mr. Deepak Maheshwari, what I will suggest the format of programme that both of you can take 25 minutes to each and then we have about 10-15 minutes to question answers, so that we get an idea as to what they actually want to convey to us and then we ask clarifications on what they are presenting.

Ms. Nappinai: Only one modification, since it was supposed to be two separate sessions for Deepak and me, the way we had structured it is I would make the presentations and during the presentations, we would do it kind of jugalbandi, so we will take totally 15 minutes, we will stick to your structure and the balance we will jeep for Q&A, in fact one other suggestions we put forth is, provided we do not put too much time in one topic, is that even while, we are discussing, we could make it an interactive session, so if you have queries or if you would like to share some of your experiences, we have a very rich table full of experience here, so if we could share.

Dr. Geeta: No but judges, excuse me, one second, no judges have complained to me that, then they do not get idea because what you are trying to convey, because many high court judges have said that if it goes too many question and answers, in the end of the day they do not know what is going on.

Nappinai: perfect, then we can have it.

Dr. Geeta: Later we can have tea over it, we can have full interactive session during tea break also.

Nappinai: Ok, done, then we will stick with that. Excellent. Thank you Geeta. Can you all hear me, is this working? Yes good morning everybody... So like I mentioned earlier I am originally from the Chennai bar and now with the Bombay bar in about 25 years and started off with the criminal law. So I am hoping to try and bring my inputs from criminal law perspective from hard core criminal law practise as supposed to cybercrime angle. I want to put this picture up to begin with itself because as you will all see the way law has been developing is at a nice, low meandering pace, however, technology does not have time for us, it is going at a superfast pace, so we are like square wheel, in the midst of all those round wheels, and we need to reinvent ourselves as to see how quickly we can become the round wheel at the earliest possible time. So going forward, I always like to be very beginning as the song goes, we are talking about cybercrime today, I am trying to give introduction of where it has all started over and where we are today but we should not forget the first principles that we have grown ups with While We're dealing with just a new field of law which has been dictated more by the medium rather than the development of law, as a standard alone process. As first principles go I would say that we have to keep in mind what the criminal justice system is therefore and what is the focus. We're here to ensure that the system delivers justice and in a manner which is fair and non-arbitrary. How do we do that given the fact that today we started, rather I would say, lets step back about 10-15 years to 20 years where did we start, we started with general laws being applied to a new domain .We started off with applying IPC provisions to new age technologies. We have come to stage where 66A was struck down, the court has to decide on whether it was a domain driven modification, or it was simpliciter by draftsman ship which led to the arbitrariness of the provisions. Given this background where do we stand today, today and again let me just move a few years forward to 2000, when the IT Act was enacted it did not come into place to deal with cybercrime. Today the focus is all about cybercrime, in the paper book that has been given to you it mentions how large this menace has become in India where you know the number of zeros have to be counted for you to know how many lakhs or crores it is likely to be. However, when in their wisdom the legislatures were focusing primarily on E-Commerce ,it was clearly an e-commerce driven enactment so much so that the problems which the world had already faced where several million dollars had been lost because of certain kinds of Cybercrimes were not even covered as a crime, it was left to the adjudicating officer to decide what is the damages to be paid on and those were officers like hacking , virus attacks, denial-of-service, which sound very normal but I will show you some of the cases that have come up in denial of service attacks which have brought whole Nation States to a standstill and this is how serious these offences were but they were all put under the provisions of section 43 which only listed them as civil penalties to be decided by the adjudicating officer. Those situations went through a little bit of change with the 2008 amendments which came into effect only on October 27 2009, two dates I wanted to bring before you all, one is this date the amendments came into effect nearly a later, the second aspect is there were certain compliances which were brought in by the 2008 amendments, whle some of the rules were brought into effect in 2009 which was by the delay of one year when it became affective, several other like under section 69, 69A and B brought into effect only in 2011, so the sequence becomes very important particular when you look at it from the perspective of criminal law because the effective date dictate when it becomes an offence, unfortunately if you see from December 2008 itself we have come across several instances cases registered and taken up. Sections are included though the sections had not come into effect as on that date. Therefore some of the basics I wanted to start with, what is cybercrime, what is it, why is it so different from crime as we perceived it, is it just the domain, is it the reach of the domain, is it the borderless nature of the domain, basically 1 most Nation have shied away from defining the term cybercrime. They have resorted to keep it open ended and leave it to either the provisions to dictate whether it is a crime or cybercrime or for enforcement authorities to decide where it would lie. The reason why I am mentioning this and I would like to touch upon this in the enforcement of session tomorrow is that most of the states have set up cybercrime cells, so there is always a disconnect in terms of where should it go. So when we look at cybercrime from the India perspective we start off with the first step of presumption that we do not have a definition for cybercrime. The second step is then how do we deal with this concept of cybercrime because it's an undefined terms, we have to look beyond the IT Act. One Today IT act provides substantial provisions to deal with crimes which are broadly classified as cybercrime but you also have other provisions under IPC itself and these provisions did not come into effect in 2008 they have been there from 2000, and even without those amendments, given the definition of document, it would have been even otherwise. Because forgery for instance was modified to include forgery of an electronic record. Forgery definition took into account making of a document with dishonest or fraudulent intention and the definition of document has not been changed even after the IT Act has come into effect. The reason being that it was so dynamic and so broad-based that it could encompass any medium. Expression in any medium and therefore it included electronic medium automatically. Nevertheless they introduced these amendments to 463-471 to include the electronic records as part of it. So we have to look beyond IT Act, we have to look beyond borders, we have to look most importantly beyond the traditional concepts of crime, the basic differences or the basic intent or purpose behind crime which used to be need has now become want . Because cybercriminal is an evolved character, he has moved from a person who would commit a crime because one he did not know that it was the crime or he did not have a choice to someone who consciously does something. Some of the cases that I come up with will tell you that they are so desperate for recognition, so it is such a dangerous field out there because you have a very young profile of offenders and the age level is going down day by day and secondly they do not understand the seriousness of their actions and third they are actually looking out for recognition in a field which otherwise is, can cause such Havoc and damage. So what do we do, t how do we deal with this situation what is the list that we started off with. This is a very basic list of offences which we would have to deal with and which have coming up on everyday basic. One of the instances, cyber stalking for instance, cyber bullying Cyber Bully apart from general offensive messages which were broadly classified a cyber defamation were all dealt under 66A, the difficulty that has happened with 66A's abuse is only the abuse was taken into account and it has been struck down but there were innumerable cases of Cyber Bully and you'll be surprised to see the some of the names there, it includes this CNIBN anchor, not Bharkha Dutta, other lady of equal stature, I'm running out name, Sagarika Ghose, thank you, so Sagarika Ghose is a persistent victim, not just a one-time victim of cyber bullying she says that every time she covers a controversial news article , people ask to add themselves as Twitter followers or LinkedIn and Facebook and all, as media people they don't have a choice they have to keep increase followers on social media. After they add themselves they started using her so that the abuse will be spread around her network also. So she has mentioned at least 3 instances, she filled a case under 66A, which has now died, one of the other very well known cases of the singer call Chinmay from Chennai but now she's been very famous on the Bollywood scene also. She was a victim of Cyber stalking and cyberbully. Her case has also died a death with 66A. What do we face today, now have a new provision under IPC for stalking which includes cyber stalking, that is effective of only from 2013 the criminal law amendment act 2013. But that is not going to protect offences committed prior to that but at least we now have a provision for it. Most of the jurisdictions and in US it is state, and state legislation, they have multiple legislations for state in United States for cyber bullying and most places have recognised to be a very serious offence, we do not have a provision today for cyber bullying, so these are all checks and balances we should quickly have a look at, which I am sure you will be covering at length also in the next the last session on cybercrime scheduled for today .Now just a little bit more on the generality before we move forward, 1 issue that concerns me immensely is that when we apply existing laws to new Age crime the one important role that law plays as deterrent is lost, so we do not, the person, I would say Kartar Singh is the best example or best quote in terms of, I am just going to go forward a bit and then come back to this. If you look at the ratio laid down in Kartar Singh, it is amazing, the way, the simplicity of it, is it just tell you that a person has to know before he commits a crime that what is doing is an offence. If he cannot know, if a reasonable man cannot know that what he's doing is wrong then why are we penalizing them, so when we are interpreting laws to apply to crimes, you know, harmonious or purposive interpretation maybe absolutely suitable or should I say should be adopted for civil proceeding or tortious liabilities but cannot be extended for criminal liability, have not already done this multiple times and are we not doing it going forward, it's not an alien concept for us, if I give very off the cuff example, price chits and money circulation schemes was extended to multi-level marketing. So we have done it but there is a direct connect over there, where is here we apply it through interpretation, this is one issue which I feels we really have address. So I am just going to go back to this now what is it that we have in terms of cybercrime, is it that we do not have definition of cybercrime at all. I would say that the simplest definition that has been given is a Kerala government circular to the police which very succinctly captures what a cybercrime is, it just says that it is a crime committed against computer, where the computer is the victim or by using a computer where the computer is the weapon, I think that literally cover the length and breadth of what cybercrime could be. If you look at this definition, South Africa's one of the rare and Saudi Arabia is planning to come out with definition also a but this is already in place, it is almost similar to what Kerala Government has put out in very simple terms, involve use of electronic communications and information systems including any device on the

Internet or any one or more of them. So this is a little complicated that's why I thought I will refer to the Kerala government one first because when cybercrime has evolved, effectively this is the definition which we have applied, computer as a victim, or computer as an offender, so if you look at the broad classifications it is the same as with IPC. So if you look at the structure of the IT Act it is very similar to IPC where you have substantially offences against the nation, in fact under the 2000 Act, there were only 10 provisions which were criminal in nature, and out of those 10 provisions only two pertained to individuals, everything else affected only the government, now with those sub clauses and additions, you have broadly about 20, lot of it now has moved to the individual domain and the economic offences. So I have tried to do a small segregation, so that it's kind of, but is not an exhaustive list, it's just given indicative list of where the section would fall under. There are 2 or 3 provisions which I would like to really focus on and rest of it I would like to approach it with Case Study kind of approach. SO these I am going to skip but I just thought it would be very easy if I could classify them and tell you what the new professions are. Just before we move to the section wise or offence wise discussions, one order background information that I want to share was on Section 66. Now we had an old section 66 also which was a recipe for disaster that was the profession which should have come to the limelight to begin with the before 66A took to the lime light. 66 read-like anything anybody who delete destroys alters any data residing in a computer, computer resources or computer network or diminishes its value or its utility, commits hacking and it was punishable with 3 years or 2 years imprisonment to begin with. Now this 66 was deleted the reason why I am mentioning this is this 66 was not deleted completely from the books , what they did was they took the essence of this which is deleting destroying or altering value or utility, moved it to section 43, two new sub clauses were added in 43, i and j . I was old 66, j is a convoluted addition of old 65, which still continues on the books, the idea. And they then made any act done under 43, with fraudulent or dishonest intention, because this intent part was missing in the old 66, so they added that, and said that anything done with fraudulent or dishonest intent is an offence and anything done under 43 with dishonest or fraudulent intent is an offence, so this is how they brought back 66, into the new Act, so it is not completely gone. Some of the others provisions which are relevant, these are all the offences which we will be going through, this in case we are unable to cover, we will cover in the last session tomorrow which is primarily the extra territorial jurisdiction aspect and the inconsistency or the harmonious interpretation required between section 75 IT Act which deals with extraterritorial jurisdiction and section 179 and 188 CrPc and how best they can be balanced out. That would be one very important aspect and we will also discuss the electronic evidence aspect . Intermediary liability was also before the Supreme Court, it has also been dealt with under the Shreya Singhal case but what the Supreme Court did was after very lengthy discussion on 66A, 69 an n 79 have been peremptorily disposed of. 79 however has been read down with most people seem to miss out because even today if you look at some of the cases that are being registered, it is being registered as if the victim has a right to ask for registration. So major difference Shreya Singhal brought about what it said that the intermediary would have to follow a notice, a takedown notice, only if it is an order of court or an order passed by the competent authority. Competent Authority is a person who is appointed under the rule, IT rules which were formulated in 2011 and they said that as long as that's done then you will have to comply with it. The reason that this reading down was necessary was that before this even if I am if I have a problem with what has been put up about me, if somebody says Nappinai is bad advocate or something and I don't like it, I write to the website which is hosting this information and say take it down and if they do not take it down it was considered a violation. The last few sections which I have put on encryption, strangely the person who is encrypting or not encrypting is not the offender. It is the intermediary who is an offender under those provisions, if they do not comply and therefore they said that this was restriction on free speech and should be removed. So let’s move on to the next thing which I thought was very relevant in terms of how we are going to interpret the IT Act which in Maneka Gandhi is what was followed in Shreya Singhal, in terms of what is the procedure, how do you say a law is a good law, the triple test which is that it must prescribe a procedure, so this is the triple test which the Supreme Court applied for holding 69A and 79. So it must have the procedure and procedure must withstand the test of fundamental right and equality Article 14. Very quickly the constitutional mandate we are looking at 14, 15 and 19, in terms of where we draw the line. The reason I put privacy in bracket is because of judgement what we are still awaiting, we have to keep our fingers crossed and hope that our right as a fundamental right is upheld and you will know why when we look at some of the cases pertaining to violation of privacy today. So now we will quickly move on to the cases, now 66, very quickly deals with multiple offences, when you look at 66, 43 read with 66 is what I mean, it does not deal with one broad classification of offences. So no case can really be registered with section 43 read with 66, it has to go as, 43A or b or c, because each sub clause deals with different offence. hacking as we know it, is purely unauthorised access, without the consent or owner or administrator, that is the first one which is there in 43, the second one is data theft, and third is virus attack and the fourth is denial of service attack. So these are the four primary offences, which are covered under 43 read with 66. And this I has already pointed out, how does it work. So these are the segregations which I have put over there, now let's go to some of the case studies, this is actually one of the most evocative images I have ever come across, this is now slightly older case of early 2015, I would still like to rely on it because this is how serious hacking can be. This case was where Sony's entire database was hacked, it was not just there proprietary content which was stolen, like the movies and television shows and whatnot music and all that. It was also the financials of all the employees of Sony, it was just about every possible information that they had .Why was the hack done because they were going to release this movie called the interview and that, the North Korea felt , it felt little discouraging of its premier and therefore they conducted the hack. So what Sony did was they released the movie in social media on you tube and all that, they said we are not going to be stopped and the threat was that if you do this, next we will be releasing, this next we will be releasing your financial and all that, but they refused to buckle down to that .Hacking can be one of the most serious offences which will impact us very largely, some of the cases which I have put out. Now September 2014 I have put this Hillary Clinton thing, the reason I have put up this is, I will mention the other case right away, in 2011, 12000 email id of government officials, who were dealing with DRTO, the reason for hack, china was suspected, because the emails that were accessed using that hack, pertained to Indo- Tibetan Army deployment of troops, we still don't know whether it was China or somebody else. But this is what is suspected. They had early warning but nobody paid attention to that. So this is how serious it can be, and as oppose to government hack we had Hillary Clinton's story out there because she used private server and the reports says despite repeated attacks they have been able to thwart it. You will see some of these cases are of very serious nature where, look at the, I have given some of the examples of government and economic offences. So if you look at the RPG group hack, or of this Global crime in which is the Middle Eastern Bank look at the timelines, now India and USA where the data was compromised. India was compromise in December. The data from USA say December 2012, USA data was compromised in March 2012, March 2013, so for 3 month do nothing and then the zero day attack happens in May from 27 countries. What is zero then why 1 days attack after 6 month is because the way a hacking ring functions, first they will collect every bodies credit and debit card's information, create fake cards and on one day, before banks wizen up to it and stops all these, they have already taken and run away, so prepare your keys first and enter the doors at the same time, that is the zero day attack. And this is how effective they were because, for 3 months plus nothing was done about it, they could have easily found which was the data compromised, replaced those cards, but not done. Norton, Deepak's competitors, of your company you have acquired now, always yours, that is his company. If you want any information about all the cybercrime attack and what is the status of each of them, the best source is go to the Symantec website, their reports will give you almost on a yearly basis what are the cybercrime attacks across the globe. So they have talked about this but this is also of 2012 I was not able to find the 2015 report details, I am sure Deepak will be able to share that with us. Deepak would you like to give some information on that. I wanted to give example of some of the cases that have happened in India of hacking, because, of its convoluted definition earlier, some of it is in the old 66, where a person A hires, for you to use a website this is how a process functions, first you have to get yourself a domain name, for instance I get myself nappinai.com. Then after that I have to host this on a web hosting server, so that web hosting server could be located anywhere in the world, thereafter I can have my own webpage and what not, I can host emails on nappinai.com, without having to rely on a webpage also. For instance google permits you to host external domain name also in it. Everything is therefore structured or layered, now what happens is A engages B for hosting his website, hosting agreement is entered into, for 6 months money is not paid, what does B do. He blocks the website. he issues notice for payment, not answered he blocked the website, case is filed against him saying you have deleted, destroyed, altered data on my computer resource or diminished its value. Now this is one aspect which I am going to focus on because you all are going to be at that stage where you are at level of interpreting the law, rather than at the first level of trying the case. The usage of or continues even today, if you look at 43 i, you will see, it still reads as deletes, destroys or alters any data in the computer, computer resource or computer network or diminishes its value. So the mens rea has been brought in because of the dishonest or fraudulent intent, but the actus reus being necessary as part of diminishing value has not been brought in. so what effectively happens when you read 43 and 66 together is , it says, if you dishonestly or fraudulently diminish the value of data also, you are liable how do you do diminish value not mentioned, so this is a huge a loophole still in the law which remains to be clarified and my interpretation of that is here we would necessarily have to apply the or equals and rule and say that it has to be actus reus plus the consequence to be read together, and that part despite the modification and it was not want of inputs from lawyers and industry when 66 was there originally , it already said that you have to combine the two because you have so many cases filed saying that I lost money because we used a b c d not because he deleted destroyed altered not because they committed data theft nothing, just that I lost money, so it is a very dangerous interpretation. The Other provisions which really has to be relooked is Section 66f. I am going to come to that after I complete this. I have just given some of the kinds of hacking that could take place, no these are all hacking of a computer resources.

So computer resource can be hacked either through a direct attack. Nowadays, hacking happens by first sending a Trojan into your computer. All of you must have got these messages I'm sure from the Income Tax Department. Have any of your got from the Income Tax Department, could I have a quick show of hands on this please. No? Saying that so and so amount has been deducted from your account because you have fallen short. No? Then what are the other kinds of mails that you would get. No I am not talking about the lottery kind .It would be these very misleading mail saying. I have got mails saying affidavit attached. I have got mail saying. What are the other kind you can come up with Deepak on this? One of the other things I've been getting are this apple mail ID where it will tell you that someone else's access your mail. We have a signing, the Apple Store and Play Store and all that. So it will send you a mail saying that someone else's access from some other computer please click on the link to confirm your Id and usage. The minute you click on the link you have already downloaded a Trojan into your computer. What is the Trojan do? It is like spy which has come into your computer which is going to keep collecting all this information that you are putting in there including what are called as keystroke. So if you are accessing your bank account, if you do net banking. If you look at the first page of your net banking page, it will give you the option of entering the password by using the virtual keyboard. The reason why they do that is because if you have a Trojan in your computer, the moment when you enter those keystrokes it can capture it and send it back to the person who has hacked into your account. So these are just the basic things they can do. They can take control of your computer, there have been instances of privacy violations where it is called RAT thing that is remote access, Trojan. So the RAT comes and take control of your computer camera and then uses it. There has been instances where most kids keep their computers in the bedroom so what happens is this Trojan activates the camera randomly, captures all this private detail and they are uploaded for no reason except that they can do it. There was this very interesting case of denial of service hack by this person who says I am slink, but instead of i he uses the work 1, sl1nk. Which when you look at visually it will look as slink. What he do, he starts, with smaller denial of service attacks on first the Oxford website. He tells them that I am going to do it again and I am going to do it on Cambridge also, so when ever, a denial of service attack is where you have lost control of your system. How do you lose control of your system, it is the best way to explain it is when someone say, you have s hop, a very small corner shop which can accommodate 5 people at a time, suddenly 100 people come in, there may be 2 people there to buy things, rest of them are there to block others from entering, so there are another 100 waiting outside, so effectively for the whole day you cannot do business because it has been blocked. So this is a denial of service, it is like a spam where you are flooded with mails , all of us know bandwidth, all of us have only that much band width, so a person spam you so that the real users cannot access you. There are two ways they do this. One is by just doing this attack of spamming you so that your server gets blocked out. There is other way that is there is reverse DOS which is happening now, which is on google ads, we have come across cases where you have to pay for each click, when you host a google ad. So you would have deposited like 5 lakhs, someone just decided to go there and keep clicking, they have no interest in your business they just know that you have paid and want you to lose money they just do it so that the real customer will not get to the add and they would have spammed you out. So this is a reverse that happens. So this person first does the universities so a denial of service will be done by using remote URL, once you block that URL your system will revive again. So what they will do is they keep skipping URLS and use some other ones and he doesn't just skip to again attack The Oxford, he says haven't you learn your lesson, don't you know I own you. Why are you even wasting your time you're making me angry? This was the attitude I was mentioning to you about earlier. He doesn't stop with this, he finishes his threat against Cambridge and all, and he is not satisfied because he has not got recognition. So then he attacked Kent police website and then he is upset because nobody knows that he is attracted because they don't release the story. Nobody wants to announce that the police website is hacked. So he then calls up the news room of the local newspaper and says I have done this, go there, and then I will do this attack while you are there. So this is the desperation which the hackers has to prove and it is more like a challenge for them. So you have things called as white hackers and black hackers, now the white hackers call themselves ethical hackers. Today it is one of the most profitable businesses around. One of the kids I knew become a CEO of his own company by the age of 25 and by the age of 30 he says I'm ready to retire, I made enough money and you know I am bored. What do they do, they are invited to hack your system and find the loophole so that can be plucked. The black hackers are the one who are like slink. This is one form. Hacking is where they make an entry into it, mostly virus attacks and hacking would go hand in hand and virus is the best, the reasons it is called Trojan is like the Trojan they come into your computer. Ya, we also started a bit late but Geeta said we would be having tea here and I can continue. So I am hoping we will be able to do that without biting too much into Deepak's time, so if I may just take 1 minute to show you all, how serious hacking can be. Because what we were talking about is all this while was hacking into a computer, your data being stolen, your privacy being lost, and probably money being stolen from your account. I can give one example of this person who took it upon himself to hack into just about any and every other person who made him angry. He got caught because he ordered pizza for $13 from one of the hacked debit card information. If he hadn't done that, he would have never been caught. He hacks into a person who makes him angry, it could be a professor, a neighbour etc. The Neighbour get this mail saying your account has been hacked, all of your information has been uploaded on so and so website, you may go there and have a look on it but I took pity on you so I changed your bank net banking password and I did not put the top of the website this is your new password. So this person does not believe this, he thought this must be one of those faking email. So he goes to his net banking account and tries old password, he cannot enter, so he tries the new password hacker has given to him and then he is able to access the his account. Then he go to the website to see every single detail there including all his email id and password for it. You know your life nowadays is online anything and everything to do about his life was there and he had to take the next 2 months to sort everything out, to change. He was a small business man who made this hacker angry, according to the hacker. So this is where we stand. We are talking about hacking of computer resources, this is next level, we cannot run away from software, every device in our life from cars to your washing machine is driven by software, that is how you are able to do a random access. Ok fine this is happening but this is the next level. Today we cannot run away from software every aspect every device in our life from Cars to your washing machine is driven by software, that is how you are able to do a random access to say when you see those adds you say I can switch on my AC from my office, if I forgot to switch on the washing machine when I have loaded the clothes in I can do it from my office or the market. So how are you able to do that, because everything is driven by software, I am not going to take too long on... ok...I will show this when we are stopping for tea. So I will move on. So but this is what it is about. So i9n May 2015, 2 hackers show a journalist how they can hack into his car while he is in it and the whole video will show how he loses control of the steering wheel and they just take control of the car, and this is a car which has a driver in it. Today we have moved to the world of automation, where we are, the Japanese premier sat in a driver less car when it was tested, in 2013 we are way behind all this. In 2013 they test drove this and there is a very interesting line he come up with, he says , will the car go for a driving licence test, Curiously enough, it does get a licence.

Session 2

Nappinai: I am quickly jumping into it, so that I do not take too much time in this. Since the first topic was I am just quickly jumping into that I don't know the first topic was primarily to identify what are the challenges that judges are likely to face in dealing with cybercrime. I way

I have structured it was to show what are the offences and how it would be dealt with. What are the issues and challenges that would come up while dealing with cybercrime? So one of the primary issue that comes up with hacking which is what we were talking about, is jurisdictional issues, because every incident may happen from your neighbour or from any part of the world. The recent trends have mostly been from Ukraine. Just to give a quick recap on what hacking is , it is by using a software, software is developed, I am not a technology person , so I may also, be given it in a lay person's term so Deepak pardon me for that or would you prefer to give the exact thing.

Deepak Maheshwari: One way in which hacking could occur apart from software is physical access. If someone's computer is open right now, unauthorized access may also happen. As she is saying, it often happens with remote tools, without knowledge of the person who is facing these challenge.

Participant: Someone sitting in Singapore, how can he access my computer in Bangalore?

Deepak Maheshwari: The way it happens is because of nature of internet, on internet, every computer is connected to other computer just like on your phone network, for example sitting here you can dial any phone number of Singapore, ok, if you have that in your subscription plan, same way every computer also has an address called the IP address, internet protocol address, now if you know that, or for that matter it is equivalent to domain name, like in our phone directory, for example like writing Nappinai and dialling her number, I don't have to remember her number I just look at Nappinai and dial that number, actually in my phone it takes Nappinai as the name which takes matching number which is there in the phone number and dial that numbers. Same way somebody sitting in Singapore or Ukrainian or India can access these computers from anywhere.

Nappinai: So putting it in lay man's term, the way they do it is, they get access to your computer from a long distance through th internet, when both computers are matching connected to net at the same time, they can from there from the IP address get your computer. Now they need that door to be opened from where they can come in. That door I was mentioning as the Trojan software, every single action that happens, where you call it virus or hacking etc. everything is done through a software programme, it is a code written to break in. for instance here all of us are connected to a Wi-Fi. I know that your Wi-Fi, because the minute I open my Wi-Fi link it shows there are 5 options available, I do not know what is your pass word, so there is a website, which will tell you how to get that password, there is a website which will tell you how to create fake sms, there is a website which tells you how to create anything and everything. There is an also an alternate dark side, you have what is called as dark net. In fact those are all things that I liked to cover, but I am sorry I was too slow.

Participant: We would like to know about dark net.

Nappinai: absolutely, what I will do it that in my next session I will try to combine little bit of those and then try to move forward. If I may just take the liberty of moving quickly on because I am sure these are all things which will be covered in subsequent sessions. So this was what I had put in terms of denial of service attacks but let me quickly move to dark net part. You have options where anything and everything is available online. In my enthusiasm I kept on adding more and more slides instead of reducing them, I am so sorry. So this is the dark net. You know this is all about, because this is where it is residing. All of you know this at the rate symbol, is what you put for your domain name and all, so where is the dark net. Dark net is just hiding there, it is just another internet connectivity only. It is also a similar to your http, but the dark net relies on what is called TOR, the onion router, so to answer your question also. Every connectivity is linked, through routers, so what we do, the denial of service attacks, it also refers to as DDos because the D stands for distributed denial of service attack. What is the distribution, I will decide, I have 15 computers here which are all probably connected to the same Wi-Fi as mine, so i have now the identity of the computers. It is like knowing 10 people's name, their addresses and which bank account they have, then all I have to find out is what the bank account password is. Once I find that I have entered into their bank accounts. Similarly I want to enter into your computers and then take over your life. So what I will do is, each computer also has an ID, I have your computer ids, I just have to enter into your computers, I will send out this mail or send out an attachment which will open the code. When you open it, it will contain some document or it will show some error but in the process it will have downloaded that software into your computer. That software is what would have given me access to your computer. From where ever I am , all I need to get that access is that you be on the internet, it does not mean that if you are all the internet you are safe. What will happen is software is also written sometime to garner all the information, store it and the minute you connect to internet, it will be sent to me, so net is the real link between two points.

Justice yatindra Singh: Working on standalone system is good. That is also advisable to your judiciary that you only work on a standalone system and don't work on a computer connected to internet, then probably some body will not be able to gain access.

Deepak Maheshwari: I will just add one caveat even there, even when you are using a standalone computer but suppose you put a pen drive there. Even that pen drive may have some document that may be malicious and may infect that stand alone computer. Despite the air gap this type of thing can happen. And one real example of that is strips net which happened in Iran's nuclear. So there is a particular refinery unit which was to be targeted through that software and the way it happened was not through the internet, it happened through a pen drive.

Nappinai: And what did it do, it affected the centrifuges of a nuclear power plant and reduced its life. There is a very interesting add on to the strips net story. Israel and US are supposed to have created that virus, now in 2015 when US was in talks with Iran, Israel used the same software, improved on it, hacked into every communication system uses for the talk so that they could listen in the talks because they wanted to know what is it that they are all talking about and how is going to affect me So these are some of the images which I am able to pull out in terms of dark net , so the dark net is equivalent dark side of white net. So if you have a Wikipedia, you have a dark Wikipedia which will tell you how to buy whatever you want. Now the dark net is used 80 percent for pornography. I wanted to complete the other part also. I wanted to complete on Zombie computers. You can connect to the dark net from your computers sitting here but the way it is done and how it functions. That is why I wanted to first explain the Zombie computers and then the TOR. Zombie computer is, as just I was mentioning, 10 of you are there I decide to take control of all 10 of your computers. When you leave from here, let me put it on the table I am not doing any of this, I am only saying this. So I decide whether I will take control of all your computer. I will not disclose that i have done it. I have better uses for it. So you go back thinking that your computers are safe but I am already in there. That’s called Zombie computer, computer which has already been taken control; of and can be put to use any time. Now the distributed denial of service attack what happens was this. Everything is just binary code for internet or cyber domain, we cannot remember in 0 and 1, we cannot remember our IP address. What the computer does it that it converts these object code into source code where or the reverse. There it shows you a human readable form. If you go to Nappinai. Com it will show you nappinai.com but it is not really, it is a string which connects to numerals, it is all numerals. It is just to make easy for the human beings to remember, to see and to identify, word equivalence have been given. Now the way the dark networks, it is called the onion router. Why because, like the onion it has many layers, if I want to access your computer I won't access from here to here. I will access it through his and 20 other countries and come there, why, because he is sitting over there trying to find out why I am accessing the net to do this. I don't want him to find out that this was the gun I used to kill him, so what I would do is, I would use this, it is called bouncing of multiple routers, so that tracking it backwards becomes difficult. At some point of time you will lose that tree. So I use these multiple routers. Everything has to do with the net and then reach the site and then buy that gun. I can also do this. So this is how extensive the dark net is, anything and everything you want under the sun you get it there. What is the reason for using the dark net, it is shocking that 90 percentage of supporters of dark net are free speech exponents. Not those who want to support criminal activities. Pornography also they justify under free expression, saying I am entitled to, but what really goes there is not general pornography but child pornography, unfortunately. Globally child pornography is one thing where retaining it, as well as disseminating is an offence, as we have in India also. So I will now, so these are just two instances that I wanted to mention. The first dark net is supposed to have already been registered in Lahore in 2016 for social media extortion market. Earlier cases are, when dark net came to focus was after the Paris attacks, what happened was, there is an organization called anonymous which hacked into 5550 twitter accounts and that was just the beginning, it went on to become 20,000. Why did they attack twitter account because that was how ISIS was recruiting. Just to close off in terms of what is the real challenge between, inform of enforcement authorities and the judiciary today, ISIS recruits through social media which is common knowledge. ISIS has now moved on to your gaming platform. So everything and anything using software is susceptible for intrusion. Suppose a person is playing a game and you have two kinds of game, one is standalone games or you are playing for somebody across the world. Same way you play with people from across the world and they get back to your computers. SO you are playing with someone across the world, you have your game chat rooms, so this person is playing a game and in the middle of it he gets a pop up message saying Do you want to ISIS and he reports it to the authorities. That is when they found out that play stations is also being used for ISIS recruitment, social media which was being used and that is why anonymous cut out that trail of recruitment by closing down the twitter accounts which were associated with ISIS. What did ISIS do, they went to dark net, so now they are more difficult to find than they were before. SO this is where technology is going. Any change that has been brought about by technology is called destruction. The anti-thesis of destruction is sustenance. I will not bite more into Deepak’s time. Thank you so much everybody.

Deepak Maheshwari: Thank you Nappinai, for laying down the background. I will just go through few slides and I just thought together we'll have some question answers and other than. So one I would say that there is changing landscape of cybercrime and I call it four S. One is speed, the speed is enormous, some of the things are happening extremely fast in terms of perpetration, so between somebody starts the chain and by the time it starts hitting, there may be multiple hoops but they can be crossed very fast. One of the reasons for that, as we discussed in the previous session was because of the ubiquitous and continuous connectivity. 20 years ago in India when we started internet access, it used to be mostly on dialup. So you would dial up and you would have the connection for certain amount of time and you would pay accordingly. Increasingly even at home we have BSNL connections, or cable connections and many of us who have smart phone, we are always connected. So that way even when you are not actively trying to do something the fact is your phone is always connected to the internet, for example you have got weather updates, stock updates, you got news update, or nothing but a push update. The moment email comes to your email account, email comes to your phone so this is possible because these things are connected. Second thing is scale, so originally started in an academic exercise in US, between few universities, that is how, internet started, but today we have got more than billion nodes, already in the world. In the coming days it is going to be much more than the population of the world. It has already happened. The reason is about 5 years back, total number of connections on the internet has crossed the human population. Not only computers, not just phones, but increasingly things are also getting connected on the internet. So for example, you have a thermostat connected to a geyser, which may be connected to internet. Today you could have engine of aircraft or railway engine or car connected to internet, even this mice or watch or many other things could be connected to internet. So lot of things are getting connected to the internet, if it is a jewellery which is called smart jewellery or fitness bands or many other things. Skills for cybercrimes is becoming readily available, not only on the dark net, even on the open net these things are available for hire so for example if you want to hack something, you don't know hacking. You don't have that expertise, but there are people who are offering their expertise by the hour, by the number of machines, by the type of attacks they can perpetrate. So there are on line market place for these kind of things. They are widely available and accessible. Spread is also there. There are globally organized chains so it is not just the stand alone script. Some of the young persons who actually know how to hack computers, some of them have actually become billionaires now. Some of the people who hack just for the fun, but today it has led to organized chains and networks on cybercrimes. What is the basic challenge in this whole thing is this. That internet technology and networks are global in jurisdictions but crimes are global and that is something which is creating problems for law enforcement `and the judiciary. This is one example I just wanted to give in terms of data points, this is based on, and there is something which is called phishing campaign. phishing campaign means that if you are getting particular mail that we discusses earlier, where it says please go to ICICI bank or SBI bank and can re verify these things where actually these are not SBI websites. There have been real cases where instead of pay pal. Com some body has registered a domain name paypa1. Instead on small l it was numeral 1, but on screen it would be look alike, so people would land up there on the website similar. Today banks are one of the example but there are many other organizations that have fake websites. Now what is happening is in 2014, this data is up to 2014, 2015 report will be out in April. One interesting thing here is there is a sharper focus. Phishing is when you do these types of things, where you send 100 or 1000 of mails. Sphere Phishing is where you are selecting your targets much more carefully, that is called sphere phishing. So there is a sharper focus. They also nowadays use what is called spray and paint technique. You put all the bait widely then keep on praying that at some point of time somebody will come and bite it, and the reason that they have such patience is that they are very well resourced in terms of people who are hiring them are paying them so much. In 2011 if we see, email per sphere phishing campaign was 78, it went up to 122 and it kept on going up. Sorry, it came down to 25, the email per campaign, so it was much lower. Now receipts per campaign also went down, the other thing was duration per campaign. Instead on 4 days 3 days, it became slightly longer. But the number of campaigns over all kept growing on. So this is something that shows, lot of people are using nowadays something sphere phishing, which is much more targeted but of course it requires much more sophistication also in doing these type of things.

Nappinai: One case I can just mention. just to give one example of what is sphere phishing, one person in Bombay went and brought a BMW, within two weeks he got a sms saying congratulations you were the 100th customer buying BMW so we are giving you one BMW free, so buy one get one free for a BMW also. In this case what was shocking is how they knew he bought a BMW and his mobile number, phishing attack did not come through email it came as sms, so it felt lot more real. Thankfully this person was carefully, he said this sounds too good to be true, and so he went to check because he parted with details. Then the case was registered, so sphere phishing is like this where an individual and single category of people are targeted as opposed to the wide net which you just throw out saying any fish that comes in. Absolutely it can happen through data leaks, and data leaks are not from one place they are from everywhere. Banks are the bigger data leaks in fact.

Deepak Maheshwari: Banks and Telecom companies and they are also the biggest repositories but increasingly if you see lot of government agencies are also having lot of data.

Nappinai: In one of the instances, a government agencies put out all the data they have collected in the name of transparency.

Deepak Maheshwari: For example in Chennai there was this voter list which was publicly accessible.

Participant: Adhar Cards is given to private agencies, it contains data of citizens of our country.

Deepak Maheshwari: If we look at some broad numbers in terms of information and communication system, in 70s India has few computers, most of them were with railways, some were with other government agencies, IITs and Indian Institute of Science they had some. Today if we see the number of installed PC base, it is not actually not moving very much in the country for past, that is also the case worldwide, the PC or fixed computers more are being sold every year but lot of them get retired every year so that number is app 70 million. The current installed capacity of fixed lines is actually 50 million plus but the number of lines we are losing every single day. Every single working day we are losing number of fixed lines connections in this country. Current number as per TRAI is, as of 30th November is 25.72 Million. And every month it is coming down. The mobile subscription, I am deliberately using the word subscription and not subscribers, because there is difference there. The subscriber is, for example, if I have got two different phones, I am still one subscriber but these are two different subscriptions. SO the number of mobile subscriptions is approximately 1 Billion. But the number of unique users is approximately 700 million. This is based on visitor location register maintained by telecom companies and other reports by telecom companies on number of people having multiple Sims or connections. Number of internet subscriptions, again I am using the term subscriptions, is 135 Million, as per TRAI. And about 120 million of them are using through mobile devices. The number of internet users, this is number of Indian users, now this is the number based on different surveys because there is no unique way of finding out. It is app 350 Million, some call it 300 Million, and some call it 400 Million. Depending on what is the criteria for that? If I have ever used internet it could be 400 million perhaps. If I use in past 1 month it could be much less. If I have used in past one week one day one hour, all these things may vary these number. Other thing about India is about 70 percentage of people are using internet only through mobile devices. People like us we are using internet through mobile devices, but also through desktops and laptops but lot of people are using it only through their mobile devices and that number is increasing every month. And number of smart phones which are being sold in the country is about 200 million. But this number will also change. That is why it is very important, a mobile is being used for internet access, and that becomes additional challenge when there is a fixed computer, for example there is a computer at my home and if that is being attacked or is being used for an attack, it is much easy to identify the location of that computer, whereas with mobile it is much more difficult. This is some other statistics, one is India is among the leading source as well as destinations of cyber-attacks in the world. However, in most cases the perpetrator are not based in India and that is what Nappinai has mentioned sometime back in terms of Trojans, that in lot of cases what is happening is in India we have computers which are , not secured well for different reasons, one could be that I am using lot of pirated software. Also if I am using genuine and licensed software, that does not by itself make my computer secure. They could be other practices that I may not be doing properly, in terms of behaviour and that may give access to other people to get into my computer and once they get here, they may install these small software that can be remotely activated. And then this computer can be used, so this has already become a victim in first place. Beyond this it has also now become a means of perpetrating attacks on other computers within and outside India. the second is critical infrastructure sectors are seeing increasing attacks, now this is something that has not come out in open because of two different reasons, because in India we have a provision right from 2000 October, when the Act came into force from 17th October, that section 70 which says, appropriate Government can notify any computer or computer system as a protected system and if there is hack into a protected system the penal provisions are much stronger, that is the concept. Broadly these protected systems, these infrastructure could be power energy systems, transport, railways, aviation, telecom, banking and financial services, critical manufacturing, in US even water base and dams are critical infrastructure. So any critical sector of economy could be considered as critical infrastructure but how many systems have actually being notified as protected system in this country so far. So far just one system has been notified so far as protected system and that was a tetra communication system supplied to Delhi police in 2010 by Motorola. That is the only system that has been notified by Union Government so far. so that means an Adhar data base, I am not talking of one Adhar doing something, the whole Adhar data base or income tax data base or voter id data base or for that matter critical legislation of defence, or space agencies, all of these, but more than outsourcing, the fact that none of these systems have actually been notified as protected systems. Although there are guidelines for their protection but which systems are protected systems have yet not been notified. On the other extreme we have example from one particular state government where they said each and every computer system belonging to the state government is critical infrastructure. For example every single computer of that state including computer in school is a critical infrastructure, which I think is also not a proper thing. So this is one thing which we still need to evolve and develop.

Justice Yatindra Singh: Critical Infrastructure is defined in the Act, if it falls in the parameter yes, if it doesn't it cannot be.

Deepak Maheshwari: But Sir, it has been notified under, but the other thing is the Act also says that the appropriate government shall also notify, and notifications have not yet happen. In US for lot of breaches, there is liability protection against notifications, so you can notify those breaches to specific authorities and you can enjoy certain protection from liability on that front. In Europe it is different way, it is much more liability but there is less mandate on the breach notifications. We don't have either of these things right now. More than piracy rate on computers and desktops I would say something else, what is happening is on mobile phones, whether it is an android phones, whether it is a windows phones, Blackberry or Mozilla anything, the fact is there is no piracy as such, because the OS is already original. But the challenge is something else. They are not protected by any other means, secondly, a mobile phone is much more susceptible to physical loss and also thirdly, a mobile phone is something which people are using more and more in public places, so there is something called visual privacy. That is if I am doing something on my computer and it is not being displayed here, it would be difficult for someone to find out what I am doing on that computer unless there are some cameras here. Whereas in a mobile phone if I am in a crowded place and doing something there could be four other people who could be just seeing over shoulder, that is called shoulder surfing and that is why lot of people they have got screen guards on the computers so that no one nearby can actually see. So this is one challenge for our country, on one hand yes we are using mobile phones which is difficult to track in terms of locations and other things but also most of these devices remain un patched. Un patched in the scene that initially people get a software that is installed in that port but after that as in when new updates are coming, many of them are not installed by people for two different reasons, one is lack of awareness and second, every time you do that there is data consumption that you will end up paying.

Nappinai: Only one point which I would like to add , the reason why he is emphasising on not notifying it as a protected system because once it is a protected system, the same offence of hacking or virus contamination etc. carries a higher punishment.

Deepak Maheshwari: Also it can go all the way up to life term because if it is construed as cyber terrorism under section 66F it can go all the way up to life term. SO in this whole data deluge, you have got five Vs, there is lot of Volume, it is like searching in a haystack, also variety, so the haystack is also not of one colour, needle is also not of one colour, there could be similar colour, size shape and may be material. Velocity, there is huge amount of data which keeps coming and which keeps getting accumulated. We need to have systems to channelize and make scene of it, otherwise if you have too much of data, it is also a problem. But we also have to bother about two other Vs, one is about veracity, so which is about authenticity of the data itself. The other is about Vapour, the term vapour I am using here is metaphor for cloud computing. So cloud computing basically means I am using some body's else computer for my work, so I have got computer, I have got mobile phone, or let's say I have got computer within my own organization and I am using that, for that matter I could be using services of third party, which could be in India or abroad, it could be a government organization, and it could be a private organization. For example digital locker is nothing but a cloud service, actually it is defined this way, a private space for citizens in a public cloud. The moment it comes to cloud computing there is lot of issues regarding cross border jurisdiction which was mentioned earlier also. Now MLATS have been around for long Lot of cybercrimes do have international trails, so you could have let's say IP address, used in India but actually assigned by a foreign registrar. It need not be that way. For example some of the government website, it could be that many of them were actually hosted abroad, all they did have .in domain name. but you could still host abroad or you could have a .com domain name, still host it in India, so all those things are technically possible, unlike telephone systems, if we have +91, it can be assigned only by a telecom licensee under section 4 of Indian Telegraph Act 1885. Whereas IP address can be assigned not only by an ISP licensee under section 4 of Indian Telegraph Act, but also by many other entitles within India or outside India. So could carry your IP address from one place to other place and you can use it. So effectively it is like using 19 century tool for 21st century, too slow and bureaucratic. By the way, the problem is not just in India, similar frustration is there on MLAT across the world, including some of the other countries with whom we have lot of interaction on these. So if you talk to officials of FBI or others, they also have challenges, they also say Indian process is too slow, we say their process is too slow and this is common frustration across worldwide. So one of the way people are trying to solve is through international cooperation. One example is council of Europe convention on cybercrime, also known as Budapest Convention, it came in 2001, and it was finalized. Now council of Europe is different from European Community or European Union EU as it is now known. EU has got 28 members now, Council of Europe has 50 members, and it is much older organization. This is the first or only global treaty having focus on cybercrime. It harmonizes laws, enhances investigation and enforcement efficiency. Effectively it gives us glossary of what are different time of cybercrimes. The penal provisions may differ in different countries. What will constitute as cybercrime in one country will also have some equivalence in other country. They will have some standard ways of investigation and enforcement. It has been ratified by 47 states and others have signed but they are yet to ratify. Non-European parties includes, there are about 8 countries which are non-European that does not mean all European countries have ratified. So Australia, Canada, Us, Mauritians, Sri Lanka these are some of the countries which are non-European which have signed, India has not signed, though post 2008 amendment provisions of IT act have been aligned with this convention and not fully aligned. One of the criticism of Budapest Convention in India and many other countries is there. One of the reasons is India was not involved probably because one we are not member of council of Europe and we won't be in which is fine. But many of these countries were also not involved in framing of this convention and obviously like any other convention, this can also undergo modification and changes. They have added additional protocol subsequently. For example Child Pornography protocol was added subsequently. But the fact is this is the only convention at this point of time in the world. We may or may not like it that is our prerogative as sovereign country. Currently government has decided not to sign it because India would like to see certain more commitments which is more binding in terms of because we are mostly seeking information from other country that is current state of affairs in our country in terms of law enforcement. Under this treaty you do have this harmonization and other things, it still does not have a binding impact on other countries to respond to each and every query which our law enforcement says. One way of doing it is, we join it and then we refine it and reform it but that is the choice that government has to take. So what is India latest statement on this whole affair, this was said about six weeks back by Mr. J.S Deepak, Secretary of Department of Information and Technology UN General Assembly had a high level submit, on WISIS+10, WISIS stands for World's Submit on Information Society which had taken place in 2003 and 2005 and this was after 10 years of that 2005, that when UN did review. Participant: It appears from the last line of the statement that the Secretary is not aware of the information.

Deepak Maheshwari: No Sir, he is very much aware of it, he says European Convention was something where not every country has a role to have control over its contours and structure, whereas what he is proposing from India is evolve a global convention, where all the member states, probably under the UN should be the part and parcel of that discussion. The best of the estimates according to people who are involved in this type of discussion is that we will take at least five year to frame this type of convention. That is an estimate which people have. But I think two things are necessary here. One is we are faced with difficulty regarding cyber security many of these are not well addressed and the second thing he is saying that in the context of security and alike public policy concerns, the government which bear ultimate responsible for essential services have a key role to play and be central to regarding security of the internet, so this is something which is till, this was just a proposal from India, other countries have also made different statements there. Some of the things we can do at this point of time is one is more effective international cooperation is needed , so cybercrime convention can be refined further but it needs participation. So there are different angles to it. Second this is government cannot address this challenge alone. Increasingly not only the private sector is the prime developer and deployed of technology but also in terms of critical infrastructure protection sector itself. Increasingly it is being run under the private sectors. Within India if you see, apart from Registrars and other things that you mentioned sir, look at the telecom services, the public sector has very limited proportion at this point of time. Look at energy, increasingly it is with the private sector, banking increasingly with the private sector, look at aviation. Many sector of economy it is the private sector that is playing a significant role and that is why governments cannot do it all alone. Capacity Building will be quiet effective, so enhancing the user awareness, liability protection for bona fide breach notifications. So if there is reasonable security practices and still something has happened, for example in banks there should be some way for them, some sort of safe guard for them, if they share those type of details with the victims or with the Reserve bank Of India or other such agencies. We also need legislative remedies for data protection and privacy. Justice Shah Committee has made recommendations in 2012, with 9 principles for privacy. There are two other things which I would just like to bring to your notice. One is let’s begin with synchronizing system, this is, and there was a real case. There was a person in Bangalore, who was arrested on a particular suspicion because service provider gave details to the law enforcement that for this particular IP address, this particular person was using at that point of time. Subsequently it was discovered that that person was not and some other person was using. So how did it happens, let us understand this. What happens is in internet we have got multiple systems, so different telecoms companies have got their own systems and they got their own date and time stamps. They have got logs that they maintain. In most case what is happening is, a particular IP address, which is being assigned to let us say to Nappinai, if she dials into BSNL right now, she might get that IP address. She disconnect it, after some time I dial in , I may get the same IP address now if something is happening at that point of time, 11am 6 minutes 22 seconds if there is a mall gap of synchronizes between these two systems, between my computer and telecom service provider or person who is running that website. Even if there is a once second difference, it can give in constituent or unmatchable result and that is something which the defence will take advantage of. This is one issue, although it has been known for more than a decade in the country, it has been flagged. I remember in 2003 or 2004 I had flagged it for the first time, there is no such mandate even today in the country about every service provider within the country having to synchronize their clock with the national clock that is one issue. It is a technical issue, but it is important that some where the regulators need to come. As per the earlier version IP version 4, number of IP address were extremely limited, it meant to the power 32, which number comes to 4 billion. Now this 4 billion number was a total number of IP address worldwide which could be uniquely assigned. That was the historical reason, in US certain universities had more number of IP addresses than the whole of India, one university had more IP address than the whole of India and that is why when more and more people has to use internet what started happening was that new technology was developing which was called network address translation, which is nothing but equivalence of EPABX. We have say 3 telephone line coming to our office but we have got 20 people sitting in the office, each of them have got an extension in sense as if they have a and if I have DID facility, it is actually equivalent to that. Only condition is that only 3 people could talk simultaneously. Now because of the internet technology not only 20 people, all those 20 people can talk simultaneously, all have got an internal IP address which has been assigned but externally it is one address. That is something which is causing the problem, so there is new protocol called internet protocol version 6 where number of IP addresses is theoretically enough to assign to each and every atom on this earth unique IP address. However the assignment of that is still not keeping pace because the technical infrastructure, the physical infrastructure has improved a lot, physical infrastructure I mean that telecom infrastructure and other things that is the router etc. Most of them are V6 compliant nowadays but most of the websites, most of the applications they are not yet V6 ready in the country. That is where we still have this challenge. The second thing I want to come to is regulatory consistency within country, so let me ask a question, suppose you are driving on a road and if you see two different signs, one says don't drive faster than 40 Km/Hr and the other says Don’t drive less than 130 Km/Hr, how do you comply with it. Can you comply with it? The fact is you can comply with it, don't drive. But even that choice is taken away. Let me come to that. So on 7th August 1999, Department of Telecommunication issued an amendment to internet, issued directions under the internet licence which were earlier issued on 6th November 1998, saying that users or organizations should not use encryption more than 40 bit, however if they want to do it, there were two conditions, they had to seek permission from the government and they also had to deposit key pair with the government, now this is something like this, if I want to use very strong 9 lever lock at my home, and the government has decided that you should not use more than 9 lever lock. If I use a 10 or 12 lever, I need to deposit a key pair with the local police station, it is almost like that and also seek their permission that whether I can do it and if they permit it I need to deposit there. What is the current situation, the government is yet to notify where to seek the permission from, in what form you need to deposit the key pair, not yet notified. That is one thing. Let us come to year 2000. SEBI permitted online trading in 2000. They said you will use minimum 64 0r 128 bit encryption. Around same time RBI also permitted net banking. They said minimum 128 bit encryption. Now if I am doing an online trading of a stock, what will happen is I am using internet so telecom regulation does apply, so I should not use more than 40 bits. If I am using online stock trading, SEBI says don't use less than 64 or 128 bit. Now if I am making or receiving online payment, RBI says not less than 128 bit, so this is a major case of regulatory inconsistency. I am not talking about global harmonization, I am talking about domestic harmonization. So effectively, anybody who is using it is violating the law and probably biggest violator is the government of India itself. It itself is rolling out lot of program, me like direct benefit transfer etc. where all these things are happening by default. This is one area where we need to consider in terms of what and how we should look at domestic regulations itself. Now under section 69 -A, we already have rules for interception, monitoring and decryption. So those rules are already there. Under Section 84 A, there is a provision that the Union Government may notify rules for encryption. So rules for decryption are already there which effectively says the person who has the decryption key shall have to assist the law enforcement in terms of decryption, of course the earlier section, in 69 prior to amendment was that only control of certifying authority had power to issue those decryption orders but now that is much widely available. So on the encryption side, *hamey ye to pata hai ki chabhi kaise khulwani hai but tala aap kaisa laga sakte hain*, what type of lock you can use, under what circumstances that is still in the grey zone. So on 18th September, 2015 the GOI did come out with a draft encryption policy, it was due for comments a few weeks later but on 22nd September, so on Friday it came out, on Tuesday the minister came on press conference and said that we are going to withdraw it and in the evening, they were withdrawn. So currently that is the situation that we have as far as encryption norms are concerned. Whatever encryption norms we have, they are not only outdated but also inconsistent with one another and we also have rules on decryption however. So the rules on decryption is like this if I am making a combination lock, if I make a number lock of 4 digits, usme bus 0 to 9 nhi haui, it could be also 0-9 and may be A B CD, may be aa, ee, or anything like that, so you can actually make it very complex. The way it is happening right now is, law enforcement when they come with these types of challenges, they are saying, Ok, they are going back to the OEM. Jis admi ne tala banaya hai, we are unable to open the lock, can you please help. Now the fact is even that person does not have the key. The combination is known by the person who has actually applied it. That is a big issue of challenge here, in terms of encryption. So this is all I wanted to cover right now. If there are any questions to me as well as Nappinai.

Participants: So far you have been talking about gaps that is there in law and in the previous session we were talking about vulnerabilities that is there. My question is how one can protect his computer.

Deepak Maheshwari: I would say that just like we look at health care, as an example. In health care what do we do, there are whole lot of viruses, bacteria and medicine under the tree. So what does WHO or ministry of family welfare prescribe. It says some basic level of inoculation. That is one thing, they also talk of some basic hygiene factor for example washing your hands and things like that and also about some basic level of nutrition. It does not mean that if we do all of this we will be 100 percent protected, but what will happen is that if we take some basic things properly, in most cases, we can either mitigate or recover from the particular situation much faster, now let me come to cyber equivalent of these. So online trust alliance, last year in January only they published a report that 9 out of ten cyber-attacks could be mitigated by some basic steps. One is using strong password. I would add one more thing, but suppose you have a very strong password but if you are using the same password with every other service also. One strong password is good but if you are using the same everywhere else that is a weakness. Second thing is there are multi factor authentication, for example I may have a password, to access my password, but there is something else. For Example, we call it multi factor authentication, authentication is often done on three things, who you are, what you know, and what you have. A cartoon in US magazine showed around 20 years back, they showed a dog saying that nobody on the internet shows that you are dog so same way who knows who I am on the internet.

Participant: Can biometrics also be used?

Deepak Maheshwari: yes it can absolutely be used, and that is the whole premise for that matter using biometric. Now one of the thing that happen is, for example I have a password but I also have this software which is on my phone, it is also available with lot of people. This number which you see, it will keep on changing every 30 seconds, on its own. Even if I am not connected to mobile, there is no mobile signal, no internet, there is a software which is running here which has been once synchronised with our office system. So everything I need to login in my system, in the office, even from here, I have to put my password and also this six digit. See this number has changed here. It will keep on changing. So this is combination of what I know, my password and also what I have. Or for that matter it could be biometric which you are saying sir. With biometrics, two issues are coming up in India. One is that in lot of cases, quality of biometric captured has not been very good because of the mutilation or deterioration of figure of many people because of manual labour and other thing. The second thing that has happened is biometric to be transmitted and online checked, you need much more bandwidth and much more computing power at the back end to do a match between the biometric which you are supplying. If I am saying I am Deepak, this is my Adhar card, they will pull up the file pertaining to my Adhar number. They are using different algorithms which I am not very sure but there are standards under the Bureau of Indian Standards that has been notified but there has been some people who are saying that these standards are not good enough in population like ours. So that is one big challenge.

Nappinai: And today you have, larger challenges also if you are relying on biometrics, 3d printers for instance. 3d printers have grown to a stage where they can capture a 2d image and convert it in a 3d image, so they do not even need a 3d to 3d to be read on. Augmented reality is how for instance.

Deepak Maheshwari: I just wanted to go back to one thing sir, today in computer technology, and terminology, we talk a lot about things like firewall and hackers etc., but who was Alibaba, he was a hacker, he stole somebody's password, khul Ja sim sim. What was lakshman Rekha, it was nothing but a firewall, all that it did was it offered a parametric protection, to Sita ki bhara se koi andar nahi aa sakega. But they moment she stepped out, she lost that protection. What was shikhandi, these were cases of impersonation. That is what keep happening even in today's world.

Participant: If anybody can hack into computer of an organization then how does the High court, which contains lot of information and how I as a judge protect the judgement that I have dictated because it is contained in a computer. Is there is a possibility of somebody changing the contents of my judgement before it is pronounced, because there might be a time lag between dictation and pronouncement of judgement in a court.

Deepak Maheshwari: possibility yes. Protection also yes. For example, if you are using digital signature under the same IT Act, then it can ensure certain things in terms of non-repudiation, integrity of message, confidentiality, and authenticity.

Nappinai: But the only problem is the digital signature are not affixed by the judges. It is being used by the secretary.

Deepak Maheshwari: In companies also it is same case. It is the Board of Director and the Company Secretary.

Nappinai: So if I could give a direct response to your question. There is a case already of this IELTS exam, exam being conducted by the British commission, so what they did was, this person who had taken the exam had, and payed of somebody who was in the back end of computer process to change the marking. So that was found out. I would put it this way, when we talk about electronic evidence. I call it the bread crumb trail, it is always there. Anyone who thinks that electronic evidence is so ephemeral, so it is not there is mistaken. It is just that we have to find out, how to find it. The trail can get complicated but the trail is always there. All that we need is to be able to find it.

Participant: It can be traced that why hackers can’t get caught?

Deepak Maheshwari: SO one is that the law enforcement is not very well equipped. Both in terms of technology and knowledge. Number two, lot of these hackers are operating from safe heavens. So from countries where they are enjoying protection.

Nappinai: I can give one example, that Estonia attack which I had mentioned. 2008, what happens is one set of hackers decide to take on Estonia, the reason is because they removed one Russian soldiers statute and they refused to recognize people who had settled in Estonia from Russia. So what they do is, first they stop all the government web sites, then the media, because they do not want the world to know that this is under attack, and then banks. It took three months for Estonia to come back. They initially suspected Russia, then they traced to a Russian government officials email but he syasmine was also a zombie computer which was used, finally it is tracked to a person in a place called Transnistra, I could not even pronounce it first. It is a secessionist country from Moldova. Look at the irony that law itself creates, the situation itself was that you have traced the criminal, it was difficult to implement the law why, because nobody was recognizing Transnistra as country. If you do not recognize the country itself then the extradition treaties or MLATs are not going to work.

Participant: larger problem is even the statelessness

Deepak Maheshwari: Also there is blurring between the state actors and the non-state actors. For example, in some of the countries, the state actors and the non-state actors, you do not exactly know.

Nappinai: So in this case they could not take action, though they found out who the person was. Because there was, one the nation itself was not recognized, two there was no international treaty binding them and I can give on more example of two big names also. Early days, I had mentioned that, even before 200, they were such huge instances of virus attacks, yet our laws did not recognize it as criminal offence at that time. One of the largest virus attack was in the US, if I am not mistaken it was, I love You Virus, where, messages were sent like this and they message people opened the virus was downloaded. Billions was lot. It was 2 instances of virus attack. One was traced to Philippines to a school boy and other was traced to Russia and that case is a reported case of Iven of, that was the name of the accused. The difficulties in both instances was that Philippines did not make virus attack and offence, similarly Russia also did not have a law which says that virus attack was an offence, so they refused to extradite the person,. In Philippines the boy got away probably because he was a young boy, but with Ivonof what happens was, after some time he gets an invite to come to US. He thought ok, I have got this invitation to talk about technology in this paradise on earth, and accepts, the minute he lands on US soil, and he is arrested. He pleaded guilty and was given a very nominal sentence. Nothing in comparison to what he costs. Some body took a leaf of the Ivonof case in India also, they were this one, and I rushed through that slide. A doctor was duped in a scam in Kerala, what the Kerala court did was, in Nigerian scam where got this mail and... Strangely enough I came across two lawyers who went all the way from Bombay to Delhi, because they were informed that they were going to get this huge bonsai. They have already paid of 80,000 rupees, this person asks for another sum. This kind of honey bait will always start with small amounts and then increase. You won't believe what lawyers have fallen for, this person says I will not, he thinks he is being very smart, he says I will not pay the money until I get the cheque of that X million pounds in my hands. So that person decided ok now I have to take you for a ride because, you are not going to pay me anymore. So he says you come to Delhi, because I do not want to cross the border, I will hand over the cheque from across the immigration and you can hand over 80,000 to me. They actually came all the way to Delhi for it in this case two Nigerian had done it and they could not extradite them, it is a long process. So what they did is he did the reverse in this case and told that you come here and I will pay you this amount, the minute they landed in Kerala they were arrested and the case is already over where they have been convicted also. So we have all this. In fact in picture I had put up it was an AK 47 to start with. So it is.

Justice Yatindra Singh: Email was circulated to everybody, almost to everyone, all judge that Justice Katju his money has been pickpocketed and he required some money.

Nappinai: So it is a dark world out there as far as cybercrime is concerned but it is not impossible. If I can give a closer to home example. It is of Phishing attack, one aspect is that they get your information etc., but at the end of the day, every crime has a Monet trail also. In the Isiis case now what the US government is doing is they are targeting the money trail that is also online. BIT coins, crypto currencies are the next generation of payment. Now I am coming to a very simple case of phishing. If I have told. Let’s take the Justice Katju case itself, now, he is asked for money but money has to be payed somewhere. If you look at where the loophole really is, it is in the KYC norms. No banks follow, KYC norms, so what happens is when KYC norms is not followed properly, your money trail has been opened out , so every phishing attack could have been avoided despite compromise of data, if the money trail had been stopped. But that even today after so many cases has not been done. IPC 417, 418 is also there but there they have just modified, the section is literally the same here the only variation is by using a computer resource. We could use forgery section and 418 even earlier, before the amendment came on.

Justice Yatindra Singh: One instance, where a very important person. His email was hacked, an email was sent that he required money, 64 lakhs was deposited in this account and within seconds 64 lakhs was taken away. The person said I did not do it. The matter was investigated, a very important person.

Nappinai: Like what I was discussing about the routers, the same way bank accounts also function, it is all multi-layered, it is never transferred from point A to point B alone and once it becomes, fundable cash, then you have lost it.

Deepak Maheshwari: KYC weakness is something that is creating problem throughout the system, for example, you mentioned in terms biometrics, it is the KYC norms that is weak for the telecom companies for example, if I am using the same id proof to open a bank account under the Pradhan mantra Jan dhan yojna, the same thing goes there, I can use the same ID proof for getting an Adhar number and then all of this get linked.

Nappinai: In fact if I may suggest very pleasant way of learning about cybercrimes, you must watch this movie called the net. It is an old movie, Syndra Bullocks, and very scary. In that they will show you how the Trojan gets installed in your computers. She loses her entire identity, she goes on a holiday and comes back and she has no identity. She is somebody else, it is all about how she recovers her identity.

Participant: Can you explain more on BIT coin

Nappinai: Bit coin is nothing but a string online. It is been created by unknown originator. They initially thought it was Japanese person, now I think they have traced it to an Australian person but it is very grey.

Deepak Maheshwari: It is an encrypted currency, it is virtual currency, it is like online wallet or something like that but which has been encrypted under multiple chains.

Nappinai: If I can put it in simpler terms, I am just going to explain it like a lay person. So the currency which we have the Indian rupee, will be printed by our mint, it is traced through those numbers which are there in the currency which is a unique number. So in a similar fashion Bit coin is traced to a ledger which says this is the, now if the ledger has issued 10 bit coins, it will have a code, same as the code which is in our rupees, and it is unique code which is only for one bit coin. It will then trace, ledger will record every transfer that it goes through. So it is actually virtual encrypted string.

Participant: What are the requirements of person to use bit coins.

Nappinai: yes there are two requirements of it, a very important question which you raised. I am writing about it also now. Every currency which you have in the world draws its legitimacy from a sovereign entity, whereas a bit coin is a privately issued currency, as on date contractual rights are what are dictating the legality of it. I give an example. Bit coin is something that has come into the picture today. Crypto currency is not new to us.

Nappinai: Nobody knows who has generated it, it is being valued, on the basis of the trading that is taking place. The sovereign nature of currency has not been addresses with respect to crypto currency. Today it is merely being regulated through contractual responsibility or liability. Now the other aspect of it is the opaqueness of crypto currency or BIT coins, now that opacity is being used for the benefit of criminals. I had mentioned how you can get control over any body's computer, so you will get a message saying, I have encrypted all the files on your computer the key will last only for 5 days, and within those 5 days I want you to pay me 8 bit coins. Now those bit coins on the market it carries a lot more value than 8. It is like shares of an undisclosed company, with an undisclosed owner. As long as, and these shares can be transferred with just one form by entry into that ledger, that is how it actually works. That transfer will get recorded into that ledger which is being maintained as a common ledger. This is how bit coins actually works and that is why since it is not traceable, and it is easy to move and it does not owe any allegiance to any sovereign, therefore it is international. Instead of contesting the legality of it what sovereign nations are doing and two nations have already come out with this proposal that US and China that they want to come out with an official virtual currency. SO US want to call it fed coin and last week china wants to come out with its own crypto currency which will replace bit coin, so instead of combating it they want yo join the race. It is actually an online hawala.

Deepak Maheshwari: Actually there are two things about it. One most of the time we do not realize the cost it causes to our economy. It costs banks on an average 36 rupees to process local cheque, now the fact is in India we do not charge either the payer or payee for the processing of that. It cost a bank about 15-20 rupees for an ATM transaction but much more for a branch transaction but we do not impose any amount. So what we have done is we have an incentive so we are imposing more cost if somebody is going more often to an ATM, there is a an additional cost but if I go every day to a bank branch and use a withdrawal slip or cheque, it cost the bank more but the bank cannot impose any cost on me. Second thing is it costs quiet a lot to the RBI itself, to print distribute and recollect and destroy the currency. They have got chimneys and other things where they destroy the soiled currency notes and old coins, so there is a lot of cost to that. So over all if you see the cost of amount of currency in circulation in the country, it is approximately 12 percentage of our GDP. That is actually currency which is outside the banking system in pockets and in wallets and in home of people which is significantly high proportion, compared to many other countries where it is just about 3-4 percentage, so there is huge cost and if you see RBI’s annual report, they are actually recording amount of money they spend on printing and distribution and these things on the currency. So the virtual currency on one hand gives them a way to manage that cost much better. Second thing is related to anonymity in the online space, today for example you can go to a market and buy things mostly anonymously certain things, without any body even the shop keeper to know who you are. So you go to a shop you buy a particular medicine, you go there, you pay for it and walk out, assuming that it is non-prescription medicine you can just do that. There could be other things also, buying milk, shopkeeper does not need to know who you are. It is becoming increasingly difficult today to do anonymous shopping. Crypto currencies are one of the ways by which in some places people are using that for anonymous purchases because of apprehension on surveillance and breach of privacy etc.

Participant: Will that not impact the GDP.

Deepak Maheshwari: It can affect. Even with the physical currency.

Nappinai: Earlier virtual currency has to be purchased using real coin. Bit coins changed that para dime by saying you don't need to buy it with real currency and how they did that was they started giving free bit coins every day. That way it was brought out in circulations.

Deepak Maheshwari: Currently bit coins are traded in dollars.

Participation: In Calcutta I remember when there was shortage of coins, token could be used.

Deepak Maheshwari: It was like an IOU note

Participant: In fact every currency issued by RBI is an IOU note.

Nappinai: It is IOU that is why signed by the Governor of RBI.

Participant: US currency does not say I promise to pay the bearer, it does not say that.

Nappinai: Thank you.

Session 3

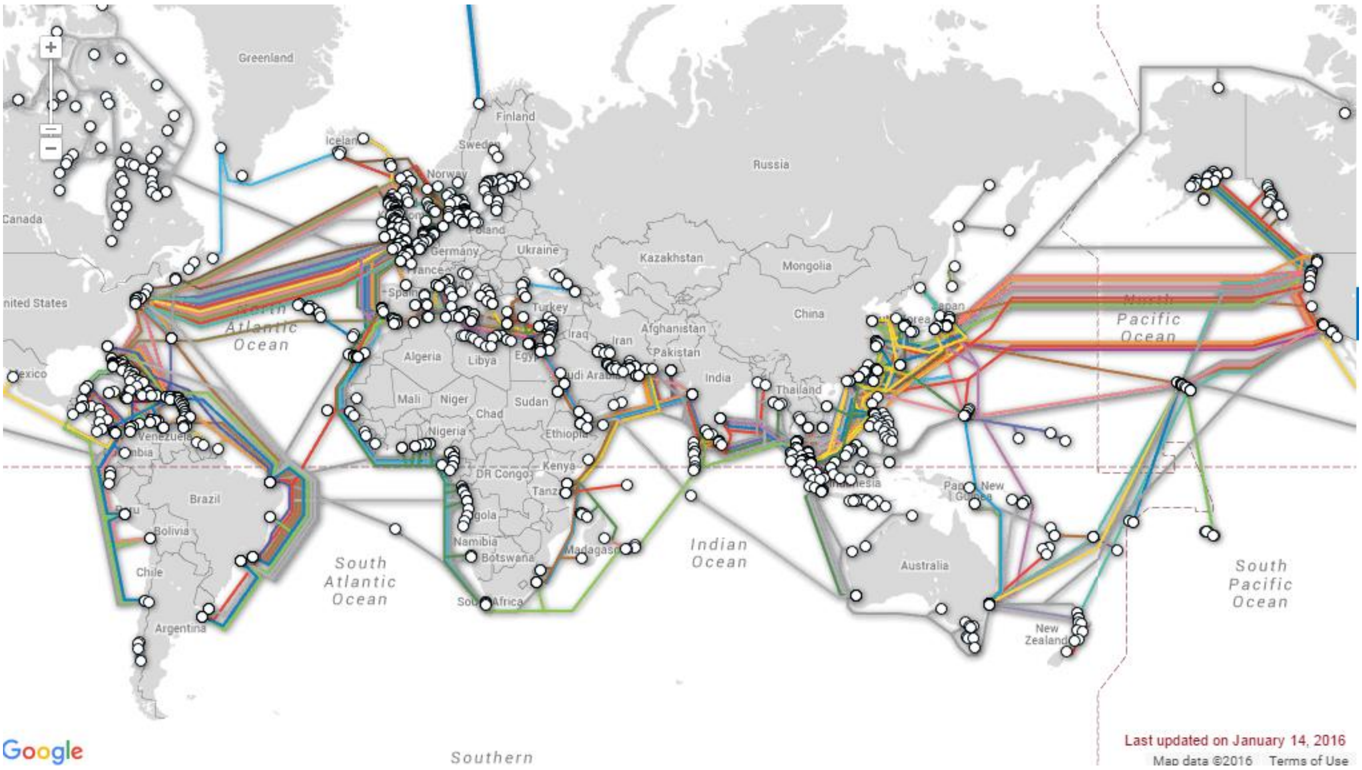
Mr. Murli: Good Morning Everybody, my name is Murli. I lead the cyber forensic practice for PwC in India and forensic practice for normal investigations for southern part of the country and many other things I do for living. But my passion always, for past 25 years has been technology in various forms and means and I am still hands on. I have never addressed such a gathering before, so If I do not use proper etiquettes, your lordships please, I pre emotively seek apology. My objective just being knowledge transfer. I don't really have to know the behavioural part in the courts. I have a team of people here, they will be here with you getting deep into the technology parts, actually showing you hard disk, mother board, showing the real things. We actually Pragya has planned hands on sessions, to actually get you feel doing something on the computer. We do it in a virtual network without getting connected to the network, we keep it inside the premises so that your packet does not go into the wild internet. Instead of giving you by power point I would like this session to be driven by you while after I finish some basics of Internet. I would have loved this session being first actually so the other two sessions would be more productive but still I think we are not so far in the day. So we will start on a lighter note, how storage has evolved. All the media are not looking at the cloud and everything is going to cloud as Deepak was saying, it is getting vaporised into the clouds now that is where the state of affairs is. Internet definition for all, means to connect to another device and all of them connective together, irrespective of the boundaries, is internet. This is very plain definition. Word protocol will come later. In the start of the day we talked about internet protocol, it exactly means what it means for you in a court of law, you have to follow protocol to file your grievances, in the same way if you want to talk on internet you have to follow a protocol, how do you send the data across the next guy in line, that is protocol. If you look at the evolution of Internet, it is just a research project, it started in 1968 and cold war or wars can have good side effects. Without Russia being on the other side we would never have internet. It started as research project so that communication could still work in time of nuclear war. That was the root cause of this development otherwise it might not have had happened. We have discussed domain name server, little bit in details and detailed protocols were published so that, it is called TCIP. We discuss that as we go forward. What those protocols do. First commercial internet and the world wide navigate, hyper link etc. First initially it was text based on Linux machines, there was no window machines. Browser was all text. So there was no graphics at all. This is very old video, it still survived I am surprised when I was looking to take this session. Very easy to understand.

Participant: Hope someone has not hacked your system.

Mr. Patil: Sir, these are encrypted computers. There are two ways of doing it. One is the encrypted hard drives that is one and second is access privileges so in order to hack into computer system one need administrative privilege. In android phone also people are doing well breaking because they need administrative privileges to install a virus. Installing an external virus is difficult, I won't say impossible.

Mr. Murli: Come to next part we will play the video later. Sometime you may wonder sitting here and accessing amazon. Com, or something else, how does this data goes all the way across the way, this is the network.

(Showed the following Slide)



This is the network. Submarines cables, fibre optic networks, every country, India is actually very gulf connected, there are multiple networks landing point near the ports. If I remember right Cochin has a landing point. Chennai, Vizag, Mumbai, also Rameshwaran.

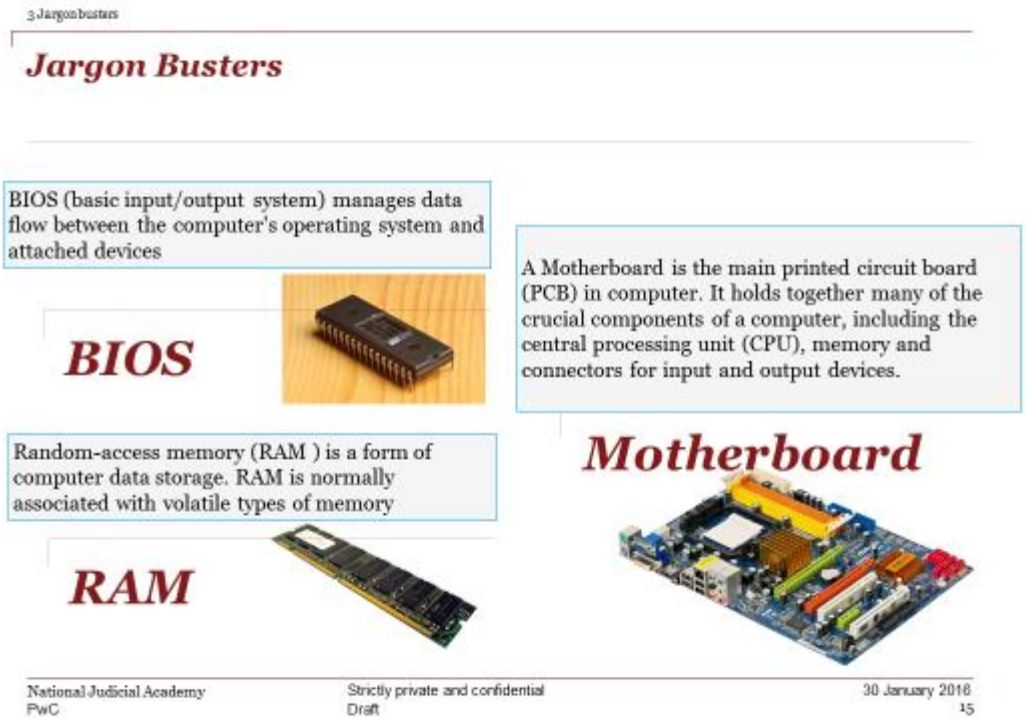
Participant: One in eastern India also. Tripura also.

Deepak Maheshwari: In addition of the cables which he is showing there is also satellite connectivity. But that is small capacity in comparison to that of submarine cables and for example if you see Nepal. They are significantly dependent on satellite because they are land locked countries.

Justice yatindra Singh: What about these cables, they are all Chinese?

Deepak Maheshwari: Actually let me tell you something about the cables. Most of these are owned actually by Indian Companies. So Bharati owns one of the highest capacity cables which is between Chennai and Singapore it is a worldwide cable. Tata companies owns some of the cables.

Mr. Murli: Satellite connectivity is not worth usage for internet because the lag is too much. The round trip time for packet to go all the way to satellite and come back is too much, so fibre will beat any day in terms of bandwidth. Do this is how the data travels around the world and each cable has multi terroid capacity to host a country, that’s how the large the pipes are. This is how the cross country traffic typically flows abd internet is a network of network so bsnl, has a network, Tata has a network but all the traffic has to cross each other at some place. That is called internet exchange. So the same way you have lot of roads in a city where you want to go to different parts of a city you have to come at cross road. Exact same way cross road is where the internet exchange happens. They have back to back files so that they do not take longer routs, so the junction is so big that they can easily cross over from one side of the road to other sides, those are called internet exchange. Now we get into jargon busters, before we get into that anything about technology, related or unrelated to internet which you want to ask, I am confident I can explain to you. Anything which is going on in your mind feel free to ask. Ok Motherboard is a large circle boards where you put smaller circle boards and smaller circle boards, as I consider, RAM is also circle board which has chips which store data but when to plug is off the data is gone. RAM looks like this, smaller or bigger in shape but looks like this. (Showed the following slide)



3 Jargon busters

Jargon Busters

BIOS (basic input/output system) manages data flow between the computer's operating system and attached devices

BIOS

A Motherboard is the main printed circuit board (PCB) in computer. It holds together many of the crucial components of a computer, including the central processing unit (CPU), memory and connectors for input and output devices.

Random-access memory (RAM) is a form of computer data storage. RAM is normally associated with volatile types of memory

RAM

Motherboard

National Judicial Academy
PwC

Strictly private and confidential
Draft

30 January 2016
15

Participant: where are the RAM slots?

Mr. Murli: You see all the slots here, this is where the RAM goes typically. Depending on number of slots and capacity you can increase the RAM. Now these are expansion slots, various names are there of the expansion slots based on capacity and speed. PCI, express so and so forth. But when you boot a computer BIOS takes care of the initial boot sequence on what exactly should happen once I get power. The initial sequences are all controlled by BIOS before it hands it over to operating system, that is what BIOS does, before the computer comes alive somebody else actually controls that is BIOS. So we are touching upon TCP and IP. These are protocols on which internet is built. If you do not conform to either one of them, you cannot talk. Like if you do not have a proper filling format, you cannot coming in a court to file, exact same way. It is defined, in those days it was opened by department of defence, IDEF is the standard body which owns runs standards which have to be on internet. Internet is a task force and they publish task force, there is a process whereby it goes for comments. Anybody can participate, whereby it publishes all kinds of standards including encryption, transcription, what not you name it. Everything is published by them. There is a little difference between TCP an IP. IP takes care of how a packet goes from one place to other place, it is the bottom most level. TCP tells you what the packets should have, and if the packet gets dropped in between what is the number that should make in to receive it back. So there is a separate function of IP and TCP.

Participant: Please explain, what is a packet?

Mr. Sachin: I was about to tell you that. So packet is a combination of information, like in digital world you have information going in o and 1, so if you have a message to send. So if you have to send packet that will get encapsulated in a packet and it will have a source address and destination address.

Participant: What is a packet?

Mr. Sachin: Packet is an encapsulation of information.

Mr. Deepak: Packet is in one way, suppose you want to send a novel from one place to another thing, so one way you send the whole novel in one packet and send it across. The other way could be that you take the novel take one page or one paragraph each, take it on a small post card and send it through different postcards, those postcards will go through different ways and will finally reach at one place and then each of them will get assembled in the same sequence as they were at the destination. So this is called packet data. Divining them into fragments, sending them and reassembling them at the other end.

Mr. Murli: Sir the usual example we use in internet world is if you want a train to small destination, it is not possible, eventually you have to break out and break into small carts, bicycles. If there is a large piece of video you want to send, you cannot send it because the pipe is so small so you have to break it into bite size pieces. So typically electronic packets means it has a header, IP header as you call it, IP header tell you where it has to go and then inside it there will be another layer, which tells what are these packets about and how do we make sure this packet has a number so that it can relate to another packet which is coming behind it or went ahead of it, how to join it with it. Inside it 101010...what is the information. It is virtually a postcard where you have all the details. In the same way post man and post office helps a post go from one place to their place. The same analogy applies here. All the three layers are there.

(Video Playing)

Mr. Murli: I will get into DNS first because that is very fundamental for understanding of internet. We have lot of weird numbers coming up 192.10. Bla. It is unique identification system of everything which has to communicate on internet. Without it you cannot communicate, because two people, cannot exist with same IP address on internet. It is traceable from which computer inside that firewall that packet has come. Otherwise they will not get a web page. There are various kinds of IP addresses then there is some reserves which cannot be sent on internet. If I remember right 192.168 172, 10.0...these are addresses, these people cannot exist on internet. Nobody with these IP will be allowed on internet. This is hard coded. Your packet will not go anywhere. This address everybody has. If you have any device, open up go to command prompt. You say ping 127.0.0.1 that means ping yourself. This means yourself, it is like writing a post card to yourself, so this address is reversed for everybody to test themselves that their network is working or not. I think these three are called RFC 1987 i think.

Participants: Who assigns these numbers, they are not assigned by us?

Mr. Murli: It was earlier done by US, it has only got democratised now, ICAN.

Participant: ICAN came later, first it was a defence thing.

Mr. Murli: Let’s go to LAN, typically on the outside face of a firewall you have public IP address. In internet world it is Internet routable IP address. We can take 108.10.0.8. If you are not a large company and you have not applied for addresses you are at the mercy of your telecom provider, they may give you a C class IP address. So if you have 2 people or 100 people behind your firewall but you have just one address to go out to the world.

This firewall builds a chat, justice 1 is going to www.ibm.com and his session number is xyz and I send him at this time. The web page you have asked it goes through only one IP address, when the packet comes back here, it says justice 1 has asked this packet and I see the sequence number matching and I throw it back to the person. So this thing is called network address translation. Officially you have only one IP address but behind you have multiple IP, but inside your network, this part is called LAN, this computer should still have unique addresses, behind the firewall, if there is no unique address they cannot talk. There will be one IP addresses. If there is no unique address they cannot talk, there will be IP address conflict no communication can happen. .

Participant: I have one thing to ask you, something of conflicting IP address. My storage which is a double storage house, and we have two broad band routers, now both have Wi-Fi , both have their now password, now when both are on they have a common password. Sometime it shows a yellow mark IP address in conflict.

Mr. Sachin: The scenario you are mentioning is static IP address. We have one IP address assigned to one computer. There is a scenario where we have dynamic IP address where DPCP, dynamic post control protocol. So what it does if keeps allocating on a daily basis, when a computer boots on. IP address is not static or not permanent, it keeps changing every day.

Mr. Murli: Let us not make it more complex. It is the IP pool owned by one of the telecom companies

Participant: bsnl. lets us bsnl example, so that will havwe ip network that gets connected to the wi-fi, so that wifi will be extending to 4 laptops here. that becomes an internal LAN and in that each computer has 192. All that computers have, it could be any series only the last number will vary. It is 192 generally. Supposing you have 4 laptops, only last digit will change.

Mr. Murli: It also has expiry time. That is protocol. It gives away IP address to you will expiry date and time. It could be one hour, it could be 365 days. It could be configured. That is how it is. The WIFI routers which is giving you IP address, it is using protocols called DNCP, it along with that it also gives a xy day to the IP address.

Participants: What happens when once you reach the expiry date?

Mr. Murli: If that number is already assigned to somebody else, because you are not online. Your computer will send a request hey I need an IP address, it is part of protocol communication. If the old IP address still exists, it gives otherwise it goes to the next one available. There is a range defined in the router from which number you have to start and which number you have to end.

Participant: So all this is being done automatically without our interference?

Mr. Murli: Absolutely, we have nothing to do. Let's go to the RAM definition. You know what LAN is, your home is home is your LAN, Local Area Network, a small reach, small number of computers, it is a LAN. WAN is outside your perimeter, outside your perimeter it could be as large as this campus or multiple campuses, and so on so forth. Multiple LANs together connected, is an internet that is how the term works.

Mr. Sachin: There is one more term called MAN, which is metropolitan area network, which connect two cities, it is called MAN.

Mr. Murli: These words they have gone in the books now, LAN MAN internet is good enough for you. There is a CAN Also, car area network. End of the day it is the network of the electronic device we are talking about.

Participant: I have a mobile, I can use internet on that. When I use my computer why do I need a modem? While travelling my mobile works but my computer does not. Why.

Mr. Murli: Because the computer does not any GSM, put in. Now the computers have slots, my computer has. There are laptops and computer available with sim card slots. From the phone you can use hotspots. Most of the phones are so good that, take a 4g pack, switch on hotspot, all the android and smart phones have it. That's all you need to do. If your phone has internet, I assume it takes 1 minute for me to put you on internet with your laptop also. Either blue tooth or serial port, which ever it is. Let us talk about fire wall for a moment because it is the most abused term. Lot of Indian customers think, mere pass firewall hai mere ko kuch nahi ho sakta. Almost like Amitabh Bacchan dialogue, mere pass ma hai kind. Firewall is a big locks all locks are time delay devices. Eventually the thief will get in. If you do not oil it and keep it un updated, it will break much faster because it gets rusted. Exact same logic goes for firewall, fire wall needs lot of monitoring, lot of maintenance and upkeep, and otherwise it will not protect the assets which it is supposed to protect. The firewall is typically a thing which has rules of who can walk through the doors, WHO CANNOT WALK AND WHO CAN WALK AT watch time, who can leave but cannot come. All those they are written down. How it is written down. It will write this IP address can only go to www.ibm.com. This IP address allowed through IBM. Com, it literally writes the rules. It is rule based inside a firewall. In the configuration of firewall rules are defined. SO you allow, disallow, block, all the features you have to define that.

Mr. Sachin: You can actually mention the range of IP which can visit google.com or certain set of IP which is not allowed to visit google.com. In organization if you see some hierarchy have access to Google or some sites, and people who are below certain level they will not have access to internet.

Participant: China had some problem with Google, it used that to stop access of its citizens to Google.

Mr. Murli: Google is not accessible in China. They have a great firewall of China. Big firewall, every packet is intercepted. That is where dark net is coming for freedom. They have plugged in firewalls at every submarine cable.

Participant: We had a similar problem in our High Court, where our bandwidth was being consumed substantially. We found out that the staff was accessing you tube, downloading movies. So we set up a firewall so that nobody can access Facebook, social media, things like that at least on that level.

Participant: We use lot of text file and if they start using you tube they suck up the bandwidth.

Mr. Murli: I think I wanted to explain DNS but I will make it simple. DNS is what gives you the names which you can remember. Human beings are not very good may be lawyers are good with section numbers but that is probably three digits predominately, if you want to remember, 192.168. Something, large number, it is very tough for us and the internet works on IP addresses which are always in this form. So if you want to type Google, DNS is 8.8.4.4. Something, but we cannot remember very well. That is they came up with a cross matching system which converts every number into a matching name. That hierarchical data base is called DNS, it is hierarchically organized. Let us say highcourts.in is owned by association of High Courts. If that is a route. If you want to give delhi.highcourt.in, it is actually 173.3. Numbers always works for internet. But human beings...

Participant: There is a question which was troubling me earlier also Mr. Murli: Google is not accessible in China. They have a great firewall of China. Big firewall, every packet is intercepted. That is where dark net is coming for freedom. They have plugged in firewalls at every submarine cable.

Participant: We had a similar problem in our High Court, where our bandwidth was being consumed substantially. We found out that the staff was accessing you tube, downloading movies. So we set up a firewall so that nobody can access Facebook, social media, things like that at least on that level.

Participant: We use lot of text file and if they start using you tube they suck up the bandwidth.

Mr. Murli: I think I wanted to explain DNS but I will make it simple. DNS is what gives you the names which you can remember. Human beings are not very good may be lawyers are good with section numbers but that is probably three digits predominately, if you want to remember, 192.168. Something, large number, it is very tough for us and the internet works on IP addresses which are always in this form. So if you want to type Google, DNS is 8.8.4.4. Something, but we cannot remember very well. That is why they came up with a cross matching system which converts every number into a matching name. That hierarchical data base is called DNS, it is hierarchically organized. Let us say highcourts.in is owned by association of High Courts. If that is a route. If you want to give delhi.highcourt.in, it is actually 173.3.3.3 Numbers always works for internet. But human beings...

Participant: There is a question which was troubling me earlier also. See this dot in came much later. The government approached and they got. In From whom they got this

Mr. Murli: ICAN

Mr. Murli: As I said it is hierarchical, .in ends with us, us ends with us. All the country names are given to country wise NIXI as you are saying sir. So every tree is given away to the country. You cannot go beyond the tree. Uske neeche branches sare hamare hain. I can access through all data under .in. DATA is probably not good, Meta data.

Participant: In India everything works under in. does ICAN know what data is under in suppose in RBI, in defence of India, if ICAN want can it know all the data. Mr. Murli: No, they are only giving the translation part. They are like telephone directory, number vs names. There is no another data there. There is other data like, high courts .in ka mail host kaun sa hai, which is Indian server related to .high courts, that data is there. Only that kind of data is there, no other data is there. It is very simple thing.

Justice Yatindra Singh: No computer is safe. Every computer can be hacked into.

Participant: the other thing is no data electronic or otherwise is safe.

Justice Yatindra Singh: Ya right, hard copies can always be eaten by the white ant.

Mr. Murli: As I was telling you, whether in physical life or virtual internet, everything protection mechanism is time delay demand. So data is just one entity inside that home or inside that server.

Participant: And remember every phone is a computer. All those who access their mails through phones have virtually opened everything. Your Gmail can be hacked, your computer can be like wise hacked. Even when your phone is switched off you can be tracked traced.

Mr. Sachin: Once I attended one marathon and after that i updated my face book profile. After that I started getting messages of using spa. How do they know, all of a sudden?

Participant: and the thing is their research mechanism every day that is improving. Lot of intelligence.

Mr. Murli: So browser is a tool lot of us use as internet explorer or chrome or your favourite Firefox, we all use. It is just a small application which understands html. HTML is a heretical web language

Participant: What is the full form?

Mr. Murli: Hypertext mark-up protocol. It is actually hypertext which Tim Berners-Lee designed. He is a British guy working in Switzerland, he designed it. So that information is hierarchical in nature. The present version is html 5 which has very rich features for media and graphics, you do not need flash any more. If you have flash installed in your computer remove it, flash is a much unsecured shitty product, remove it. HTML 5 is good enough to generate video and everything. Don't use flash.

Participant: Some of the programmes say you do not have flash installed

Participant: how do I know that my system is using html 5.

Mr. Murli: All the browsers have HTML 5. Even from past one, one and half year everybody is having HTML 5. I strongly recommend to remove flash if there is one. Industry opinion is not to go with flash.

Participant: One question, in our judiciary we are using what is called Ubuntu, they say that that is much better protected and whatever we are talking about, is that true or it is myth.

Mr. Murli: Ubuntu is just a Linux OS. A flour of Linux, out of the box it is little better but unless you secure it. If you believe operating system is like an office, you always needs doors for people to come in and get service. If you close everything that is the most secure computer in the world, it is disconnected computer. So you have to be connected and you have to be secure, that means you need, ad on protections like antivirus, firewalls, everything. Out of the box it is probably little better but not too far away, because windows have evolved quite a bit over the years, windows is very good nor per se. But what is it that they are doing in Ubuntu, what are the extra protection measures and maintenance measures, those do not go away irrespective or any OS you use. Deepak am I correct?

Mr. Deepak: yes, the fact is any software is susceptible to threats.

Participant: What about the IOS

Mr. Deepak: Even IOS sir. There is a reason for it. Apple operates in a highly closed environment. So all the apps they check, it is only on their hardware, it is only there OS. So that is why they have much better control, but still it is not that it does not get hacked and the fact is that in 2016, because of its increasing popularity, apple devices and because of higher costs. Apple devices are being increasingly targeted in 2016 and just 2 years back we had this big celebrity leak of photographs.

Mr. Patil: There is one more perspective regarding Apple devices. So what is happening is apple is there is one more opportunity for hackers to penetrate a data, because most of the apple devices are also associated with the ICloud accounts and the data is getting blacked up on iCloud. Now what is happening is that hackers are not targeting your phones, they are targeting the iClouds accounts. Now people are very careful when they have passwords of their email ids, but it comes to password of the iCloud accounts, these are the names of their spouses, children, and very normal predictable passwords. The hackers what they are doing know is rather than spending time on penetrating the Gmail id, because Gmail has come out with too much of preventive techniques, like two factor authentication. But for this there is no protection. Now not many people have actually stopped or disabled, simultaneous opening of iCloud on a computer system, but for most of the iCloud accounts what we observe is while iCloud can be accessed from mobile phones, it can be very well accessed parallel from any computer system across the globe. And people are targeting those without our knowledge and there is no kind of alert mechanism existing on that. That is one issue that we are observing.

Participant: Macintosh has an application, what is a basic difference, it is basically target is less susceptible.

Mr. Murli: Sir if you see IOS, in its present incarnation, not MAC OS. MAC OS is dead now. The present incarnation is VSG based, in our word it is UNIX. UNIX was traditionally layered security and out of the box it does not give right to anybody. Everything you have to expressly give right to somebody. To access file or access a network you need to define aright then only it lets you go there. So all the apps it has to be approved by Apple otherwise it cannot run on the apple system. And it weeks three weeks for a small apple app to be approved, if you are in priority list.

Justice Yatindra Singh: UNIX is supposed to be stable of the all operating system. Linux is also based on UNIX that is a reason they say Linux is also safer I am not a window fan I am a Linux fan and that is just one of the reason why the e-committee chose it as operating system.

Bombay High Court and Allahabad High Court put their foot down, they said they will not accept the window system at all.

Mr. Murli: URL, it is just an extension of a domain name we discussed. If a server name, in a technical word we call it FQGN, fully qualified domain name. Means it uniquely identifies its server. Let us say server1.ibm.com. It is a fully qualified name of the server. That server can have many websites, it can have thousands of websites. If you want to identify a website or web service, then you identify uniquely let us say example, putting www is not mandatory, we just got used to it so lot of websites have it. You can just have cleartrip.com also. There is no www. And DNS will automatically look back and clear trip is actually a web server and connect it. So lot of new websites don't have www.Initially it was accustomed not because of technology requirement but to tell people that this is website they used to do it and a mail server would typically have mail.facebook.com. Mail server have a prefix called mail. So this is all various kinds of servers which are publishing websites on the internet for various purposes.

Mr. Sachin: This video will actually explain how information actually flows on the internet. How packets are prepared, how it gets sort on internet.

(Video Playing)

Mr. Murli: router is like a police man in a cross road. It knows how many routs are there in the crossing and where the traffic is more and where the traffic is less and accordingly he manages it because not all routes are equally busy and not all routes are equally big so you have to prioritise and send them and given the name packetize, some packets, preceding packets can go ahead and succeeding packets can go back , there is no problem, because there is sequence number in TCP, they can come back together in a proper order when they reach the destination. And based on the traffic they can send same information through different routes but they will still reach the same destination, when they reach the destination all of them they became a single large chunk of data again, that is function of a router, to manage the traffic and send it to destination through best route possible based on traffic congestion and pricing. They use a protocol called VGP and you can actually configure saying that this route is one type expensive, this route is two time expensive. So if Onex is busy the packet goes through two x until it goes there.

(Video playing again)

Mr. Murli: Ok, Don't want to get into net neutrality at this point.

Participant: That was my next question. What is this the free basic issue?

Mr. Murli: I will give you free internet but you can only use Facebook. Facebook is the internet you cannot go to other websites Participant: So it is a quid pro quo.

Mr. Murli: For you to get on that platform I am giving you my platform but all other internet websites will be rationed or disconnected. So the very principle of internet is free propagation of information, is compromised upon by Facebook. SO TRAI and everybody said they. If Facebook chooses then you are allowed to go to flip kart

Participant: Is it that, for example, Dubai airport, they will give you a free Wi-Fi but you have to go and it opens their website. They do not allow you typo access google they are limited, you can open an email or other things .So they are also same.

Mr. Murli: Ya but they are at least giving something. They allow other website, they may block Google. The allow email to go from your account from your laptop and read it and all those things. It is not limited to specific website. It is limited by the time you are allowed to browse but not specific place or location. It is a very tough discussion, very complex discussion that is why I did not want to get into net neutrality debate in this session. We have lot of sessions where we can. Let’s jump to other slide. You have probably heard the buss word IOT, everybody is thinking what this IOT, and internet of things is. This is where the device connecting to internet directly, may be your phones do to some extent, but they are pretty large to be called IOT. And they have multiple functions. But most of the IOT devices like Deepak was talking about thermostat. Your thermostat is connected to internet and if you are in the home, on the road, no problem it can fix everything and it talks to the internet directly via Google. It does not need any body's intervention. It just needs battery and wireless connection but more often than not IOT devices should be miniature in size and should have low power consumption and should only need power once in few months not years. If all three are conforming then it can be called an IOT device. One of the thing is low powered networks penetration is not there, if you use a GSM or Wi-Fi your battery finished too fast. IOT devices don't need high battery. They constant blebs. Like I have this gadget which is on my hand. It monitors my heat meet, my work hour, walking, talking whatever. But the information it collects is very minimal if you compare to textual size, probably one kb or few kb a day for that you do not need Wi-Fi speed. Even the good old modem where we started our like 1024kbps modem is when we started our life will be already too much. It does not need it all day long. So we are developing low power networks which are pervasive. Whole city can be covered using low power network, for example it is called LORA. LORA is one kind of low power network. With 5 different Wi-Fi or 10 access point you can cover whole city. So any IOT device in that city can talk via LORA network and send its data. Typically IOT device would have, as a medical device you have various models, blood sugar, heart beat you have a stethoscope to monitor your motion, this way that way. You have optical cell to test the intensity of light, to switch on street lights, so on so forth. It is generally small decision making capacity and lot of sensors, put together with light weight internet technology is an IOT device.

Participant: many times the demand of the bar is that the campus of the court should be Wi-Fi covered, many times we have told that we cannot because of the security risk. Now why should we take security risk and if we take the risk what is the preventive measure because many times this demand is rejected only on the ground of that it is security risk.

Mr. Murli: No it is just incapable people covering their tracks.

Participant: I will answer this. Delhi yesterday when we were here launched a Wi-Fi for its lawyers. How we have done it is we have segregated the High Court network completely, it is a network now from airtel and there is partnership of airtel and Vodafone, where they are providing free access. So that is not connected to the High court network, so there is no question of security breach.

Justice Yatindra Singh: Allahabad bar association, it has a free Wi-Fi for the lawyers. Since 4 years ago it is absolutely free. But the NIC people they keep on saying that security problems are there and we will not be able to do it. They just do not know how to do it.

Mr. Murli: All our offices, across the world. We have 160 offices. I just have to open my laptop to get connected to them. I don't plugin cable, I do not do anything. I login with my user id and password. The only security measure is if you are uniquely able to identify the person and that person is allowed to access the resource there is no problem. But if you are not able to uniquely identify the user who is allowed to then there is a problem. Unique identification of user is all you need, then you can go on.

(Participants speaking all at once)

Mr. Murli: You need to pay to get good person.

Participant: they don't. When I was still in bar, I accessed the High Court's site and my computer showed that there is a spam in it. I went to NIC and said that look my system says that there is someone attacking your system. The reply that I got back was, your system might be outdated that is why it is so and our system is updated and we have not been able to detect.

Participant: NIC therefore gets hacked left, right and centre

Participant: The problem with NIC is, it repeatedly gets hacked and it slows down our network and we suffer.

Participant: That calls for a concern because all High courts are hosted on NIC, all government institutions.

Justice Yatindra Singh: All High Courts are not under the NIC. Allahabad High Court has its own server I think for last about 16 years, about 12 years we have our own server.

Participant: No, now we are all going for that Indian Judiciary. Gov.in. They are all hosted by NIC. Ultimately it all leads into NIC sever. NIC controls.

Justice Yatindra Singh: As far as for Allahabad it is the Allahabad High Court's server. It does not go into the NIC. Allahabad High Court address is not Allahabad high court.gov.nic.in. It is Allahabad high court.in. We have our own server. NIC is one source which is creating all sort of problems while we are pointing it out. Security problem bla bla.

Mr. Murli: I am done with my formal presentation. Anything out of the blue, any technology as I said, I repeat.

Participant: Please explain the concept of cloud. What exactly it is.

Mr. Murli: Sir we just spoke about server right. So I assume server is in the High court premises now I take that serve away from you and put it in a data centre. You do not know where the data centre is. But I am giving you full control of that server, still sitting in your High Court room. And I will run the hardware the hardware is my problem. You can run as much software as you want and let us say if your server is short in breath, it is not powered enough, and you can just click one button. I will add one server for you in one minute. It is, resources are backed at somebody else data centre, accessible for you through a file. Traditionally cloud, if you have seen in all architectural depiction internet is depicted by cloud, or clouds. So if anything hosted in internet and it is available to you at your whim and fancies it is cloud based services. It is an internet bases, it is the fancy term that we have coined, it is internet and we are able to access, that's it. But typical Microsoft or amazon cloud services will give you extremely powerful. So If I have to hack server I can use 100 servers for 10 minutes and hack it out.

Participant: The simplest example is your email account. Google is on cloud. You do not have your emails in your phones it is actually stored in a server somewhere.

Mr. Murli: Corporate perspective your capex will go very low but you will have to pay.

Participant: But judicial perspective we cannot have judicial data’s stored outside country

Mr. Murli: But Microsoft has already opened a data centre in India for cloud services and I am sure Amazon is reaching to do it.

Session 4

Justice Yatindra Singh: Namaste and a very good afternoon to all you. Session after lunch is very tricky especially after delicious and sumptuous lunch. On really feels like afternoon siesta. If you want that just go ahead, but beware, don't snore because you will wake up the person next to you. This session is two hour long, really very long session, it has four topics, for convenience I have divided into two parts. The first part contains the first three topics and the second part contains the fourth topic. The first three parts broadly relate to cybercrimes and the fourth part broadly relates to field of Information technology. So we proceed with the first part which broadly relates to cybercrimes. On the internet no one knows you are a dog. Has it got any relevance with the session cybercrimes? Is it a correct statement? Believe me that is the most fundamental thing in a session for cybercrimes, for some time bear with me I will connect it. This session is being divided into four sub parts. What is cyber claws, what are the violations of cyber laws, what is cybercrimes, its remedies and punishments? I used to do one more topic why cyber law is necessary. I have not added it because I thought there will be shortage of time but some of the questions here prompt me to speak something about it. Epimenidies was a 6th century philosopher, he came up with a very fundamental paradox, he used to live in Creek and he said all Christians are liars. It is like this, I am an Indian and I am saying, all Indians are liars. If you take it to be true it true it turns out to be false, if you take it to be false it turns out to be true. Button Russell’s he tried to sort it out and he gave another version of the story. He said there is a village and there is only one barber. He says I will save those who do not save themselves. The question is who saves the barber? Russel spend his life time in sorting it out. Russell and white head, they came out with principia Mathematica. There he thought he sorted out this problem. But in fact he had not. What he had doe was that barber was a female, he did not require a save. Something of this kind. His misconception continued till 1931, when came the greatest logician of all time. Kurt Godel, was biggest Godel ever born and he came out with a paper which in English, he translated the title. There exists a proposition which can neither be proved nor be disproved. This is known as theorem of incompleteness. Just given any system, you begin with whatever axiom to begin, there would be something, which you cannot prove right or wrong. The physical implication of this theorem is that any logical system is incomplete, there is not a fort which cannot be breached and there is no computer which cannot be hacked. Irrespective of whatever technological, Mr. Dinesh Maheshwari, is here, he is making anti-virus, and whatever anti-virus he may make there would be system which can be beaten. If you remember Independence Day, have you seen movie, if you see that, those are such advanced people ultimately the hero the film sends a small virus to their computer and removes the shield and that is how they destroy it. Do whatever you feel like and that is why cyber laws are necessary because technical people cannot save, ultimately they have to come back to us. Lawyers, judges and the legislatures, that is why having law is necessary. Let us go into the question of what is cybercrime. Invention, discoveries, new technologies, they widen the horizon of service. But so far as law is concerned, they create problems. Galileo he proved Copernicus right when he said that it is the earth which goes round the sun and not the other way round. In 1616, he was condemned and in 1623 he was put in house arrest till his death. Charles Darwin, he had evidence to show that life did not happen as stated in book of genesis, in Old Testament. It evolved through million and millions of years and he did not have courage to publish it, because he wanted to keep him safe and his wife was a devout Christian. It is only that when he received a letter from another scientist in Australia that published a joint letter in 1856. Muslims hated it, Jews hated it, and Christian hated it because they believed in Old Testament. The Americans hated it so much that it became an offence and the most famous trial in the history of science took place in 1923, known as the monkey’s trial. Scots was a biology teacher, he taught origin of species. He was prosecuted and fined 100 dollars. The

Supreme Court of Tennessee set aside the conviction, not on the ground that it is ultra vires but on the ground that judge instead of jury can fix the fine. Information Technology which is brought about by three things, which is brought about by three things, computer, I do not have to tell you what computers are, internet, just bear with me I will do it very quickly because I go in that sequence, in your court every court has got a computer, your court master or bench secretary they upload the information on server, in your chambers there are computers, your private secretaries they upload judgements on the servers and the computers are so connected, it is known as local area network or LAN. In the evening, all this information all this information is uploaded on the NIC server. If somebody has got telephone lines or satellite connections, he can see that. Internet is a network of network or a global network, which consists of the computers that are capable of communicating among themselves. Cyber space, if you have internet you can send a text file, video file or you can receive it. This happens in a virtual space which many people call, I mean I like to call cyber space. So these three things together have given birth to a technology called the Information Technology. This has created holes in all spheres of law, everyone was trying to find solutions. The legislatures are enacting laws. Government are making rules and regulations. Courts are fine tuning the guidelines or framing the laws where there is no such law. All this solutions put together, are known as information technology laws or computer laws or cyber laws. In the field of intellectual property rights, certain amendments have been made which we will deal in the second part of the session. For this part the most important Act is the IT Act. Section 91-94 of the IT Act, have also amended all other Acts, one in Indian Penal Code, Indian Evidence Act, RBI Act and Banker Book's Evidence Act. Second important amendment is 2008, now here is something very interesting, 2008 amended, has also amended Indian Evidence Act and Indian Penal Code, but it has omitted section 91-94 that had earlier amended the four Acts. Often the question is, what happens to those amendment, with this omission, they will go away or will they stand? I talk to some people, they gave a very divergent opinions about it, but if you look into section 6A of the General Clauses Act, according to that all these amendments which have already been made by IT act they will continue despite omission. Let us come to third part, what are the violations of the cyber laws. Violations of cyber laws can be divided into two parts, one in the field of IPR and second in fields other than IPR. This particular one we will do in the second part. For the other ones, they can also be divided into three parts. When I use word computer, I mean communication device as well. One when the computer is targeted or other when the computer is used as an object and three the IT Act prescribes lots of responsibilities duties and directions can be issued. Violations of these directions entrails responsibilities and duties is also punishable. But we will leave that. We will only consider the first two. As these first two are broadly known as cybercrimes. Let us see what are the broad sections, under the IT Act that deals with computer as object or target. Basically there are four sections, section 65, and tampering computer source document. Now what is particular source document is also explained in this section. I find it to be very very complicated one. I don't understand it. Let me explain to you what is a source document in a very lay man's language. Like in previous sessions, computers do not understand our language, they have their own language. They understand the language of yes and no. The switched, electric switches are either on or off, or language in one and zero, that is a binary. A computer chip, in fact it has got a billion of switched which are either on or off, that is how a computer chip is. Initially in 1970, I went to study at IIT Kanpur. They were computers at only two places in the entire country, one was IIT Kanpur. And this is how a computer is programme is being made. This is a punch card, now there used to be a type writer and when you type it punches wholes into it, if there is a whole, light can go in, if light can go in it is yes or one. IF light cannot go in it is zero it is no, and a computer programme consisted of 100 of these punch cards like rupee counting machine. Suppose there is problem with problem with some punching card there is problem with to understand where the mistake is. Slowly and slowly as technology developed you had advanced languages. Some of them you might have learned, or some of them you might have learned from your children like Basic etc. In all this high language there is something called compiler. It compiles into something which the computer can understand which is called object. Pigeon is one programme which assimilates or chat programmes, it is written in a language called C++. This is how a programme is written. I cannot make out anything probably Dinesh would be able to make out what is written there. But I can read it, I can read what is written there. When a programme is written it is called source code. Now source document is a document which contain this source. Now if you tamper with it then it is punishable under section 65. If you look into the material that has been supplied to you, Reliance they have come out with a particular scheme and they were serving new phone and Tata, some of the employees they said, you bring the phone to us and we will give you cheaper service. And what they did was they changed the source code so that, that particular phone can work with the Tata service as well. Reliance service filled an FIR under section 65 and also violation of copyright. The Andhra Pradesh quashed set aside all the section under IPC but they said that prima facie a case under section 65 of IT Act is made up. Let us see about other. I am sorry I forgot, you have I forgot to tell you, cybercrimes have two remedies, civil remedies and criminal remedies. Civil remedies are provided under chapter 9 and chapter 10. The most section in chapter 9 is chapter

43 and 43 A. 43 broadly talks about any illegal activity with the computer., sending of virus, they talked about dos attack, spyware, adware, I will tell you something more in detail. All this is covered under section 43, if any damage is caused then under section 43, penalty and compensation can be awarded. Up to 5 crore the matter is cognizable by adjudicating officer, all the IT secretaries have been nominated as adjudicating officer, and beyond 5 crore the matter has to go before the competent civil court. Appeal lies to appellate tribunal, cyber appellate tribunal and the second appeal lies to the High Court. But it is not like section 100 for appeal, only a question of law. It is a question of law and fact which I thought was very widely worded, it should be confined as same ground as section 100. There is another section 43 A that talks about failure to protect data and a compensation can be awarded. Now let us come back to section 66, now if you do any illegal activity with the computer which is mentioned under section 43, fraudulently or dishonestly then it is punishable as an offence under section 66. So difference between section 43 and 66 is mens rea, mens rea of dishonestly or fraudulently. That is the only difference, but whatever you do there, whatever illegality you do there, it is punishable here. It covers your computer receiving a virus, DOS attack, which I have not to explain again because it has already being explained, spyware and adware, probably these words were not used but something of this kind. Spyware and Adware, are programmes which gets installed into your computer wittingly or unwittingly and that actually send information when you surf, the said information on whose behalf they are installed. Then probably when you got to internet you see advertisement, what you want to buy, whatever you want to do, and this is spy ware and adware are not only against your privacy, but infact they take away lot of your resources, especially if you have a window based operating system. If you notice this or not, after some time, it gets slow. There are two reasons for that, one is you install more programmes, application on it, it takes away space, but basically it becomes slow because it has adware and spyware in your computer. If you format your hard disk or remove ad ware and spyware, for which you require help of an expert or the easiest way is sort of format and do it again, you will see that your computer will again become fast. Committing or conspiring to commit cyber terrorism, 66F. Now this is actually in two parts, part A and B. part A says if anyone with intention to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people, does any illegal activity with the computer, and the result of the illegal activity is that any damage is caused or likely to be caused or any life is lost or likely to be loosed then it is called cyber terrorism under part A. Part B is , there are certain computers were access to the computer is restricted because of the security reasons or friendly relationship in other state. if without authorization you access it or download

any data, in that event and with the intention to threaten the sovereignty or integrity of the country, friendly relation with other country, public defamation, contempt of courts Act , both are punishable under section 66A.

Participant: Will it include something like wiki leak?

Justice Yatindra Singh: Yes, provided, yes it will include wiki leaks provided, the information in that computer must be restricted in that computer for the reasons mentioned there in and if somebody access it does it, then yes. Section 70, securing or attempting to secure access of protected system. Government can of course protect a system, we talked about it in the morning. Computer having a critical infrastructure information can be declared as a protected computer and this critical information is also being defined as a computer, the destruction of which will hamper the security of the nation, economy, public health and safety, then that can be declared as a protected system. If you access or attempt to access it, then that would be punishable under section 70. Let us come to the second part, crime using computer or communication devices. If an Act is contrary to any law it is an illegal Act, if consequence of an illegal Act, is punishable also then it is an offence. Illegal act is a big sphere and offence is a part of that sphere. Every offence is an illegal act but every illegal act is not an offence. Adultery is one classic example. Some offences are punishable under the IT Act and some offences are punishable under the other ones. Let us see what the sections that are punishable under IT Act are. IPC and the Evidence Act, to my mind, they are the best drafted enactment ever, very well drafted. All our enactments are not so well drafted, that is why there are so little amendments in them. If you look into the IPC, it actually groups the similar offences at one place. It says offences affecting the body, of offences affecting property and like that. In It Act they are not at all grouped together, but I have tried to group them into three parts of offences affecting human persons, of offences affecting decency and Morals, of offences affecting property. There are two sections which were covering affecting human body and person, section 66 A and 66E. What Spam is to email, spin is to chatting device. This was punishable under section 66A, phising, it is a, like already explained in previous sessions. You receive an official looking kind of email requesting your confidential information that is phising. Cyber Bullying, it is something which we have gone through in our time, either we have bullied or have been bullied someone or at least we have seen some one being bullied. But you do it in cyber space is called cyber bullying. Cyber stalking.

Participant: Can I ask a question? Leave the world cyber. Take stalking, cyber use is a means to show that the crime that is committed is by means of electronic medium, medium which allows connectivity. There is an affected person, physically or otherwise and there is someone doing it. If you delete the word cyber for a moment then bullying.

Justice yatindra Singh: Bullying is an offence

Participant: Yes it is an offence, cyber or otherwise. What makes it so special?

Justice Yatindra Singh: No because you are doing. Let me explain it. I will just explain about cyber stalking then probably this point will be clear. Stalking is watching or following someone, or the girls, boys being lucky to get out of it. The girls have been victim of such stalking, which is very frightening and annoying. Now stalking by the way was not an offence at all under IPC. When you do in cyber space it is called cyber stalking. This was probably covered under section 66A. This has been declared by the Supreme Court to be ultra-Virus in Shreya Singhal case. I have lot of my reservation about this case because once nobody was, none of the petitioner was actually charged under section 66A. Under PIL it was done, affected person had not come forward. The minister who has drafted section 66A, under whose regime it was drafted, he said I am very happy, it is very wisely worded, I am very glad, the NDA minister who was part of committee which recommended as an amendment he also said I am very happy. If you read the judgement probably all this things are not covered and something else is covered. Perhaps if the affected person had come forward or they have filed a 486 or 226 petition, the court would have quashed section 66A, it would have said nothing doing, and at the most it may be defamation. If you think it is defamation you go for nuisance or as far as Calcutta case was concerned, Mamta Didi was there.

Participant: That was not stalking, that was when someone used face book or...

Justice Yatindra Singh: I am saying that, I am just trying to say that I have some reservations about this case because the question was not there but there after they say that it is too widely worded , it could have been saved by confining it, the result is perhaps phishing might be covered somewhere else which I will talk about, rest the three, spam and spam, cyber bullying and cyber stalking, were not covered, not punishable at all, after Nirbhaya incident, the Parliament has amended IPC and they have added section 354 D. 354 D talks about stalking as well as cyber stalking. Both the things have become punishable under 354D.

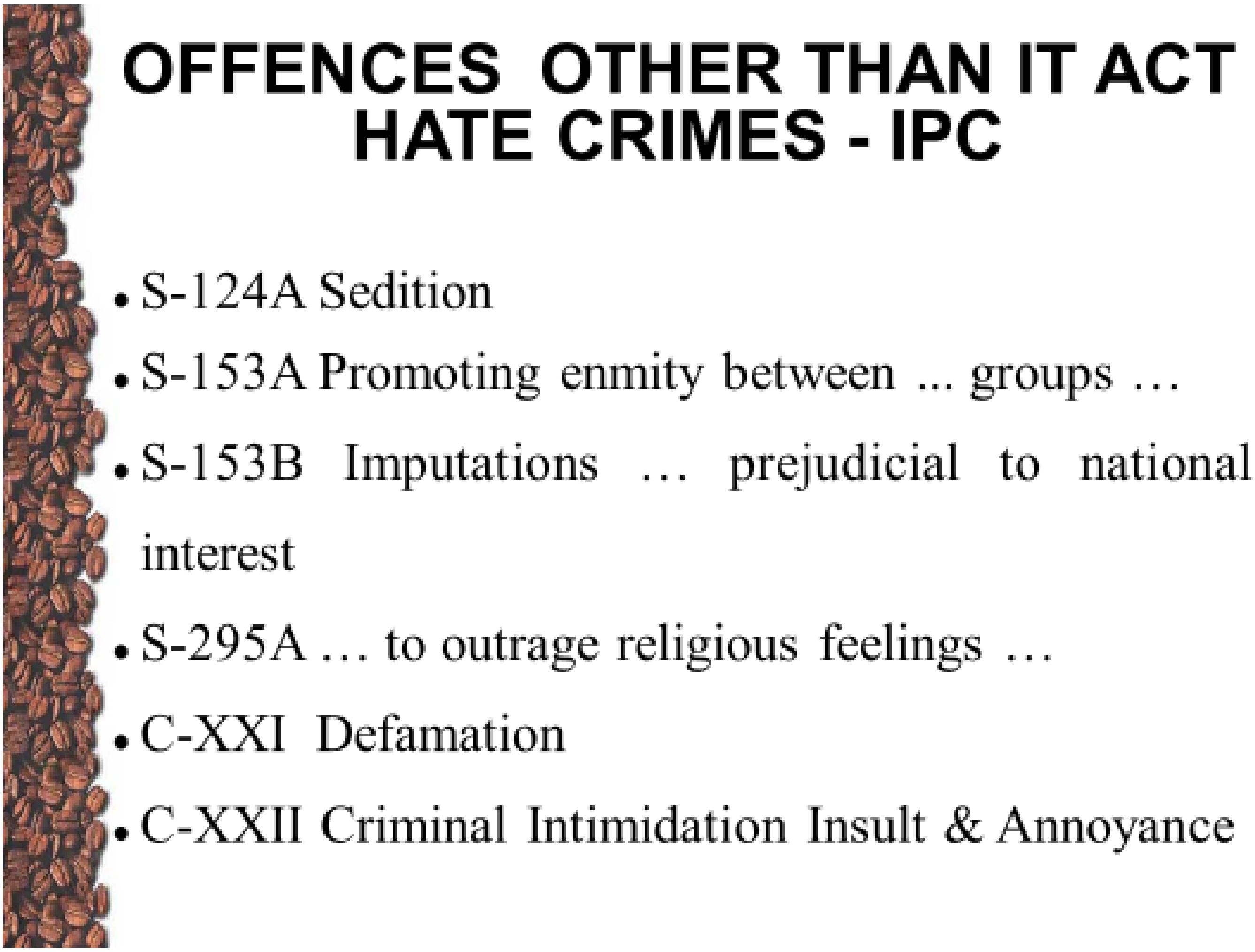
Participant: So it does not matter whether Shreya Singhal is there or not.

Justice Yatindra Singh: but spam and spam is there. Cyber bullying is there and Phishing may be covered or may not be covered. 66E is about punishment for violation of privacy, if you take electronic record, private parts of somebody or transmit pictures of private part of somebody, then without his or her consent, then that is punishable under section 66E. Affecting decency and morals. This is publishing or transmitting in electronic form any obscene material punishable under section 67, sexually explicit act or conduct 67A, child pornography is very widely worded, very widely worded and to my mind rightly very widely worded, if you try to entice a child. A child is defined as somebody who is under 18 years of age. If you entice somebody, cultivate on-line friendship, in order to do any sexual act or a conduct which is not approved by a reasonable adult, then that comes punishable under 67B. If you record, electronically record child abuse or child in sexually explicit act then that is also child pornography. But unfortunately the punishment is too little, it is just 5 years. It should be much more than 5 years. It also has some mandatory minimum punishment. Say 5 years 7 years, like in rape, you have to give special reason in order to give a punishment of less than 7 years. 67B also provides exception. It talks about, if it is in the interest of science, art, and culture then it is an exception carved out there. Affecting property, if a person dishonestly receives a stolen computer, which he has reasons to believe or knowing it to be stolen, then it is punishable under 66B. Identity theft, if you use passport of someone else, or unique identification number of someone else, that is called identity theft. Cheating by impersonation using a computer, computer device, that is punishable under section 66D. Now all financial crimes, credit card frauds, they are covered under 66C and 66D. Phishing to my mind would also be covered under 66D, because you receive an email, and somebody is impersonating to be RBI. There is much more cybercrime than it is reported, it is not only true for the individuals but for the corporations as well. The reasons is often that cybercrime is generally related to obscenity or pornography, that is something everyone tries to hide, so nobody reports, but basic reason is that people are often not confident enough that they can be resolved. A quick and a satisfactory resolution of cybercrime will definitely boost their confidence and perhaps more cybercrime would be reported. Before I end this session, I would like to use why I used the particular title, in the internet no one knows, you are a dog, infact the title is not mine, I have taken it from a cartoon on the internet, published by Peter Steiner in 1993, in a New York magazine and here is the cartoon.

(Showed the following Slide)

"On the Internet, nobody knows you're a dog."

I will do this then I will come back to it. This is what is says, on the internet nobody knows that you are a dog. Actually it is a paradox, it is a fallacy, and on the internet everyone knows you are a dog. There is nothing private on the internet, everything is public. You will always be caught, and the cybercrime is often there because people think they can get anonymous and then can get away with the crime. Like I talked about, illegal act is an offence if it is punishable, now third topic of our topic deals with, it talks about racism, xenophobia, and basically they are hate crimes. Now hate crimes are nowhere, mentioned in the IT Act, they are punishable only under the IPC, these are the sections where hate crimes are punishable.



OFFENCES OTHER THAN IT ACT
HATE CRIMES - IPC

- S-124A Sedition
- S-153A Promoting enmity between ... groups …
- S-153B Imputations … prejudicial to national interest
- S-295A … to outrage religious feelings …
- C-XXI Defamation
- C-XXII Criminal Intimidation Insult & Annoyance

They are committed by public speech, by distributing a pamphlet, writing an article. But if you do that in cyber space, by publishing a website or if you do that and spread the information by communication device. Then yes you would be punishable under these sections of IPC, though they are not covered under cybercrime. That comes to the end of one session. Ms. Nappinai would you like to say something about cybercrime, you may add if you wish to or if anyone has any question.

Participant: I feel that the punishments that are described are too little or too less.

Justice Yatindra Singh: Like for child pornography there is hardly any punishment, I say it should be minimum punishment, mandatory punishment of at least 5 years and in many countries it is death penalty for child pornography because it is something which you cannot tolerate. If something happens to your child it is very difficult to reverse it. It is very serious offence.

Ms. Nappinai: Sorry may I add one thing.

Justice Yatindra Singh: Ya please say

Ms. Nappinai: On the punishment part, if you look at 2000 act, it is even lesser, it is 2 year. But what they did was they increased the punishment but diluted its effect by making it bailable. It is much worse 90 percent of the offence under the IT Act has been made bailable and compoundable, only for compounding they have made a restriction saying offences against women and children and impacting integrity and sovereignty of India are not compoundable. The same idea should have been carried forward for bailable and non bailable offences, which is not done. Again if you remember, I mentioned that the Baji.com case was very instrumental in bringing about a lot of changes. This was one. There is one issue which I wanted to highlight, now I mentioned in my session that child pornography, even possession pornography is an offence under IPC. One of the most horrendous development of recent time is the videos which are being circulated. These are circulated through social media including WhatsApp. You may have a setting by which automatically the thing gets downloaded. You do not even know what the data is containing, that has been downloaded. The laws says how you came into possession that is not relevant, if you are in possession, you are an offender, and this is very dangerous. For simple reason that this is all technology based.

Justice Yatindra Singh: Child pornography is something, something, at least for me it has an irreversible effect.

Participant: What she said that sometime the things get automatically downloaded. Now the thing is if it gets downloaded you see it and delete it, actually it does not get deleted, it is still on your system and it can be retrieved. So what do you do?

Ms. Nappinai: There are two judgement from UK court which talks about Trojan horse defence. This Trojan is different from the Trojan I was mentioning in the morning. The morning one was Trojan software, this is Trojan horse defence which means that I did not do it, and somebody else did it. What happened in case 1 is, child pornography is found on the computer of one person, and he says that I did not put it there, but Trojan software came into my system and it got downloaded? But the forensic report came and it showed that the computer did had that Trojan. The second case was even stranger than fiction. Child pornography found on this computer. He say that the Trojan did it I did not do it. They verified that computer and found no such Trojan installed in it. He said yes you are right but this was a Trojan which had a self-destructive programme. So the Trojan came in, installed this pornographic material and then destructed itself and therefore you are not able to find it. When they verified that whether such Trojan software existed they found it and had to extend the benefit of doubt. So it works both way. These are the two extremes which happen. As I was telling discretion has to be applied case by case basis. Child pornography provisions substantially comply with the Budapest Convention. Though we are not signatories there we have adopted this. Even if POSCO if you see, the person who comes to know about the offence is also supposed to register, the only exception is only when you are a child or victim 90 percentage of the cases the perpetrators are themselves children. Cyber bullying also 90 percentage of cases are committed by children. At least 4 jurisdiction in US had introduced bullying laws because people committed suicide because of bullying. We also have a case already, Airforce Bal Bharati school, student was ragged by seniors, he goes to their Facebook page takes their photographs and of teachers, not just students, probably he finds that the teachers did not protect him. So if you see the cases offline victims may become online bullies or it could be both ways. He morphed it with nude pictures and circulated to all the students in the school and took it all over social media. In this case when issue of bail, before the juvenile court case, it said that it is just the work of a child because when child is angry as he goes and draws on the bathroom wall, he had done on social media. That is not the fact, whereas the bathroom wall remain within the four corners of the bathroom, this graffiti was all over the world. It is very difficult to have it removed. Once created is always there. So these balancing acts between children as perpetrators and children as victim is kind of missing.

Justice Yatindra Singh: Mr. Dinesh you wanted to say something.

Mr. Deepak: Deepak, sorry, I just wanted to say one thing...

Justice Yatindra Singh: Mr. Dinesh Maheshwari was a judge of Rajasthan High Court, and he knows that I am obsessed with that...hahaha Deepak. So…

Mr. Deepak: One other challenge that is coming, especially in respect to the Child Pornography being defined or discussed, if there is any graphics which is not actually picture of a particular person as such and how does the law deals with that situation. That is the other issue which is coming up.

Participant: An also sir, the illustration which she gave short while ago that this was a sort of reaction to the fact that this child faced certain situation which allowed him to go to that level and morph pictures of. How do us. Because this is a question which comes for adjudication, how one will decide. Please throw some light on that.

Justice Yatindra Singh: Let me confess that I am not the correct person to answer this. Maybe it is case to case, often you look at facts of a particular case, often you do not say that you just reprimand him and use say sold him, let him go away and many things. Like for example these problems keep on happening in real life as well. You look into it then explain to the person concerned. For example if you look into the bazi.com case. Let us take a reaction towards it. This boy from IIT Kharagpur what he did was he uploaded one mms on bazi.com. What happened to the MD of bazi.com is another question. He didn't have the bail, to my mind he should have got the bail immediately because there was no fault of his. He immediately removed it, he cooperated. Itis the matter has to come to Delhi High Court to get a bail, he should have got a bail immediately from the magistrates court itself. But see the boy who did that, who uploaded in bazi.com. He was restricted from IIT Kharagpur. If you were the judge and it would have come in writ petition before you, what you would have done. Or what any one of you would have done. If you take the opinion of all of us here. The opinion of all of us is going to be different from Participant: The answer is that how you present the matter. Even in a service law jurisprudence, dismissal from the service is the highest punishment.

Justice Yatindra Singh: No but it is very serious thing which he did. But what

Participant: But there is a doctrine of proportionality.

Justice Yatindra Singh: The doctrine of proportionality differs from judge to judge. It is not a very. Here, I don't keno what any one of you would have done, in this matter. I would have never restricted the boy. This is too harsh a punishment. I think the guy is brilliant, the guy came up with something. Something was wrong with upbringing. I would have never ever restricted the boy. I would have taken the boy in. The boy probably did not have his mental make-up correct. Otherwise he seems to be very business minded, may be in a wrong direction. Maybe he requires some correction.

Participant: may be counselling, it would have been an answer.

Justice Yatindra Singh: yes you are a police officer, what would you have done?

Mr. Patil: I have a different question, the question is about the age of the accused. During investigation what a police officer comes across is that either he is a college going student, one hand there is a social pressure to take action. Many times the issue grow up to such an extent, I have dealt with one case when I was there. A threat email was sent, an FIR was registered by an MLA, the accused turned out to be a juvenile. In such scenario do you feel that current law should be amended to bring the age of juvenile down?

Justice Yatindra Singh: they have passed a law, we have done it already. But to my mind, like my justices have said, probably the correct thing is counselling, it does not require anything more. Like you know bala sahab Thakre joke on Facebook for which those two case were tried. To my mind they did not even require counselling, they did nothing wrong. The cartoon about chief minister of Calcutta, it is ridiculous, there was nothing in it.

Participant: The question is, are we looking at it with mens rea of a hardened criminal or that of a person fooling around.

Justice Yatindra Singh: The question is once you are a public figure, you have to accept criticism. You cannot say I am beyond criticism. Some kind of joke, satire, and comment is always there.

Participant: You are subject to satire only because you are a public figure, otherwise, nobody will bother about you.

Justice Yatindra Singh: That thing you are right, and don't think it is only for the police officer, it is there for the judges also. Irrespective of what judges say. I am no longer a judge, I am a lawyer.

Participant: Once a judge is always a judge, you may not be talking office of a judge in the court room.

Justice Yatindra Singh: Judges are also in a way affected by media. To judge they are not affected, perhaps it is not true. They are affected. All of us are affected. Media is in fact today most powerful thing. If you look into two cases, why i say that example, both cases of two Supreme Court judges, where they had something to do with harassment. Now one judge had to resign because media became very offensive. For the second judge he was lucky enough to get a stay order from the High Court and he got away if it. If there was a no gag order then whether he is guilty or not guilty he had to buckle down under pressure. There is too much of pressure and one judge he buckled down under pressure whatever happened. There is so much of media attention.

Participant: The sad thing about it is that the media never took it that this lady on whose complaint all this happened simply evaporated after it.

Justice Yatindra Singh: No sometime you are passing very strong orders against somebody and you are a very clever chief minister or you are very clever person, a judge is very strong order, it is very easy to allege something and when media catches on it plays and plays and the same news is repeated for weeks and 24 hours.

Participant: That is because of the TRP rating, nothing else. The news will carry too much advertisement.

Nappinai: In light of last discussion, there is one more thing which I want to highlight is which was 66F. In fact I mentioned this in the morning that I want to point out grave problem in 66F. If you look at the provisions 66F is divided into two parts. I am talking about 66F (1). It is divided into two parts. The way it is divided with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people. This is not there in 66 F 1 B. So the mistake that the draft men has done is instead of putting it as part of 1, he has put it as 1 A. So when you read 66 1 b separately, what you will realize is that that they have transposed 19(2), directly into 66F 1 B

Participant: It is not a drafting mistake, it is almost like clerical mistake. Someone should have moved this to the top.

Ms. Nappinai: This is the time bomb that is waiting to burst. Contempt of court and defamation is a terrorist act? Unless somebody is waiting to clarify. If we were to read b as totality, this is how it reads. Whoever knowingly or intentionally,

Participant: because there is a disjunctive or,

Ms. Nappinai: therefore since there is A or, the way it would read is whoever knowingly or intentionally, so therefore there is no qualifier there and anything and everything there would become an offence.

Justice Yatindra Singh: but probably it is qualified by other, access of computer goes without authorization and bla bla bla and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations;

Ms. Nappinai: May I read it further sir. There is another conjunctive or there

Justice Yatindra Singh: Or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism. This is 19 (2)

Ms. Nappinai: yes it is 19(2) which has been transposed. Hopefully through interpretation.

Participant: This again drafting is an example of computer, copy paste technology...Copying it from there, did not know where to put Mr. Deepak: the other thing which happened was this, the amendment bill was introduced in 2006 in December .Prior to that expert committee was constituted in 2005. The final thing came up, it was very fast development after Mumbai attacks and all that, then we got 66F and some of the other provisions...

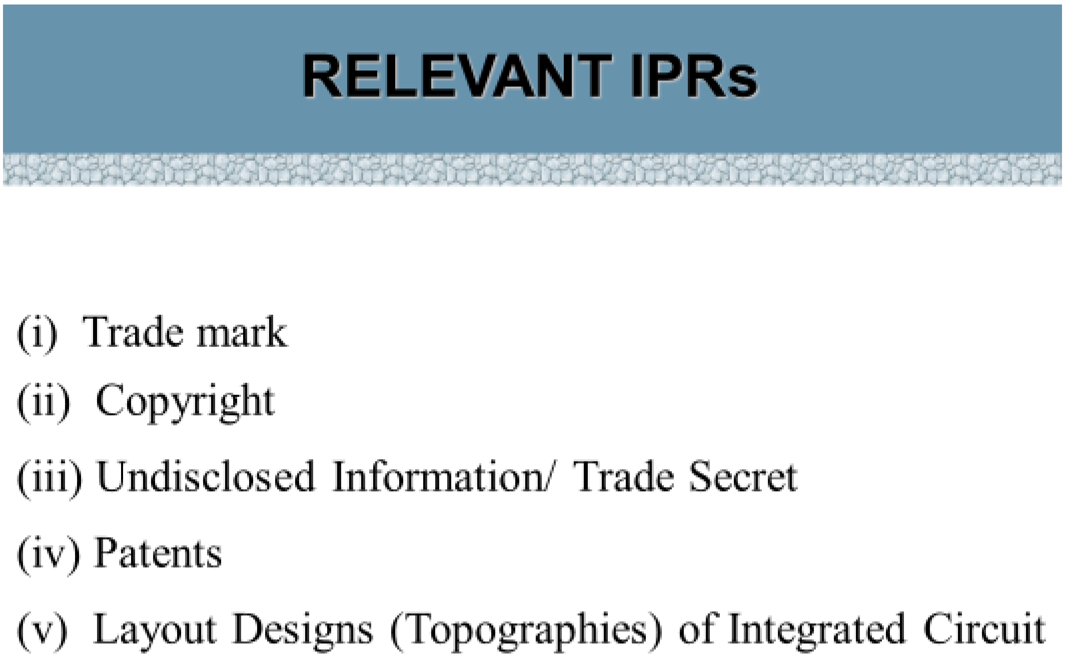
Justice Yatindra Singh: And they were quite different from the original bill.

Mr. Deepak: there was little discussion in the Parliament and birth the houses passes it.

Ms. Nappinai: In my presentation, I had put three cases, one of them is this Amitesh Singh which has been struck down by Gujrat High Court, but three are three cases which are very very scary. In two instances, in first instance the person was booked for 66F because he is in possession of Pakistani Sim card that is it. In the second instance, he is in possession of a

Pakistani Sim card but it has been used for making calls to Pakistan. The third is the most absurd of all. It is a case registered under 498A and 66F. So unless the husband terrorise the wife so much that they thought to proceed under 66F, it is impossible to how they manage o add 66F. Unfortunately the High court judgement is for compounding of case and for quashing. So I was unable to find anything further. But the sections show clear indication of how it has been misused.

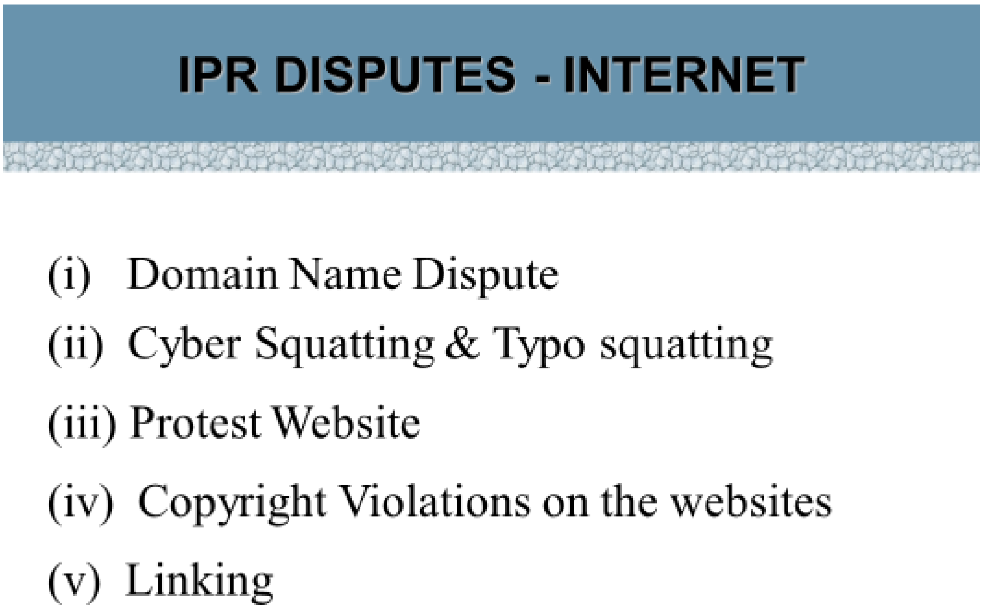
Justice Yatindra Singh: Let us come to the second part. The IR disputes in relation to information technology. About 100 years ago, exactly in 1916, petition j in London University vs University Tutorial Press case, he said, he observed one like, What is worth copying is worth protection. To my mind this most succulently captures the genesis of Intellectual property Rights. These rights are broadly creation of mind and they lie into two categories one copyright, two copyright which can be there in the literary work, it can be in artistic work, novel, story, painting, photograph and industrial rights, it could be patent, geographical indication, it could be trade mark. There are number of different kinds of IPRS. WTO conceives it as 7. There are much more than these 7. So far as IT is concerned five of them are relevant.



RELEVANT IPRs

(i) Trade mark
(ii) Copyright
(iii) Undisclosed Information/ Trade Secret
(iv) Patents
(v) Layout Designs (Topographies) of Integrated Circuit

Trademark and copyright, they are relevant as far as internet is concerned. Copyright and undisclosed information or trade secrets or patents they are important as far as protecting a computer software is concerned. Lay out design, topography and integrated circuits is concerned, many people think that Act is so successful that there is only one case. We will concentrate only in first four, so far as internet is concerned there are ten kinds of disputes. Pragya please read that slide



IPR DISPUTES - INTERNET

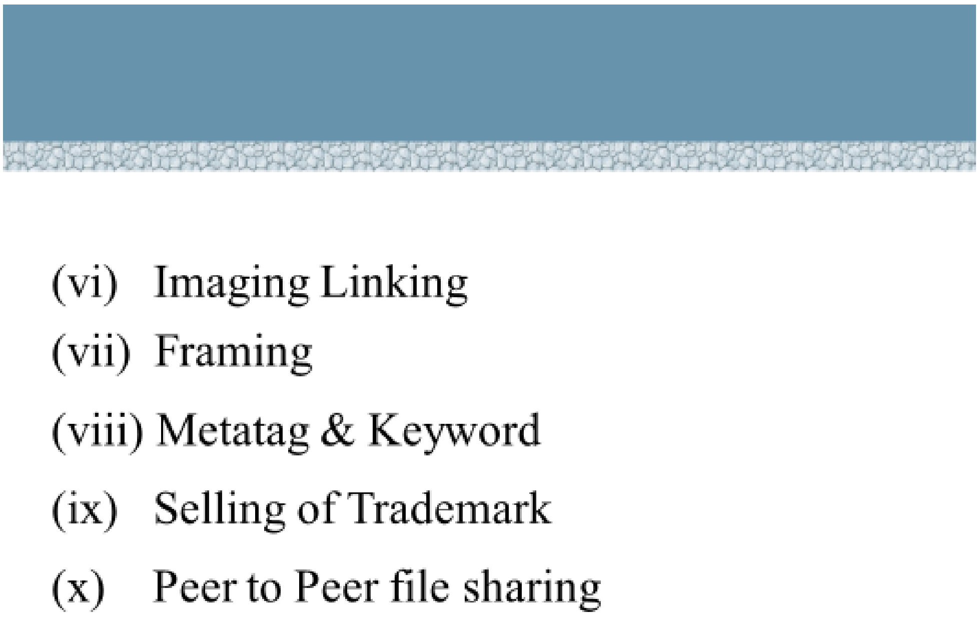
(i) Domain Name Dispute

(ii) Cyber Squatting & Typo squatting

(iii) Protest Website

(iv) Copyright Violations on the websites

(v) Linking



(vi) Imaging Linking

(vii) Framing

(viii) Metatag & Keyword

(ix) Selling of Trademark

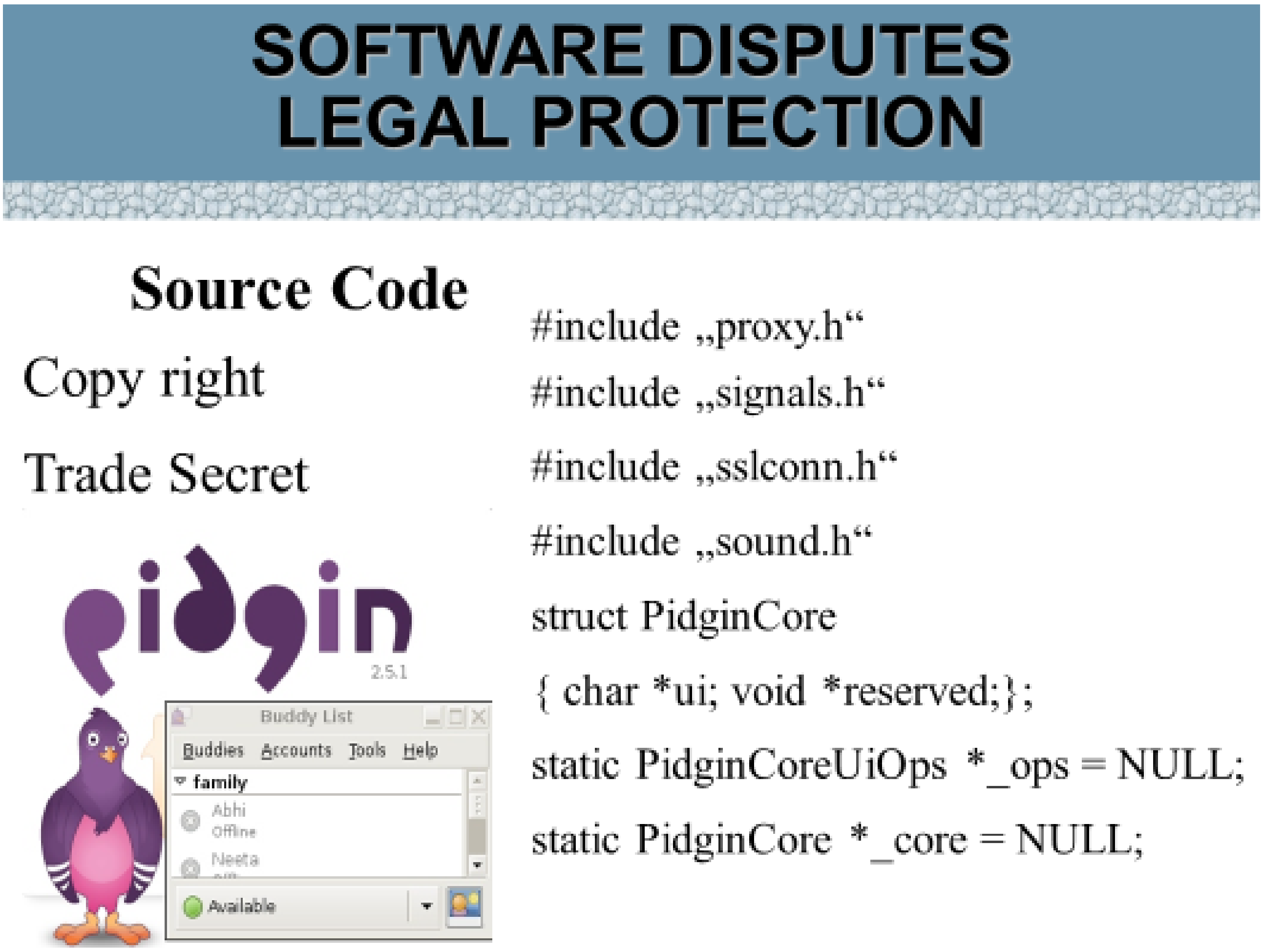
(x) Peer to Peer file sharing

The most important one is the domain name dispute. That is the one which is very prevalent, very common in our country. The rest of them, the cybersquatting, and typo squatting and protest website are kind of off shoot of domain name disputes. Rest of them are not so common at all, so we will concentrate on as far as domain name dispute is concerned. Rest of them we will leave it, after the session we discuss or if time is left we will talk about it. In order to understand domain name dispute, some kind of history would be necessary. Wind Cerf was a mathematician, he was a software engineer. Bob kahan was a computer engineer. I will do it very quickly. In 1970s they found out a way that information in a computer could be broken into small packets which Mr. Murli and Mr. Deepak were kind enough to explain what packets are in such a way that if they are sent to another computer, they're build the information again. This happens under a protocol which is called Transfer Control protocol TCP. This can happen not only if there are two computers but if there are number of computers or network of computers. This happens because of a protocol called Internet protocol. Every packet is like a post card or envelop. It has an address of computer sending and receiving it. This is knows as internet protocol and address of every computer on the internet is called internet protocol address or IP address. Internet, like told in earlier sessions also, is like a network of computers capable of communicating themselves, let us see what a web technology is. Tim Berners lee did his post-graduation in Physics from Oxford University where he was banned from using a computer because once he had hacked all the computers of Oxford University. After passing out he went and joined CERD. CERD is a nuclear physics laboratory of European nations. It is based in Switzerland. At that time they had different kind of scientists from all over European countries working there. They had different computers and their information was in different format. The basic job of Tim Berners lee was to ensure that information of one computer can be taken to the other computer and it can be read and modified there. While he was performing the particular job he started to think that is it a way, is it possible that information of all the computers be kept at one place may be kept in such a fashion that they appear at one particular place. While he was thinking about this particular solution, he invented Web technology, and in doing that he took the help of two things, one was hypertext mark-up language or HTML, the great advantage of writing of writing any information in this language is that you could link information which is written on HTML in this one and this is done by actually embedding the link in that information. This link appears on a special colour specially blue or special formatting generally underlined and if you click on it, it takes you to another information and this transfer takes place under protocol called hypertext transfer protocol or HTTP. The first web page was uploaded in CERN on 6th August 1991. This was intellectual property of CERN and they made it free on 30th April, 1993. So internet is a way of communication between network of computers, web is a particular way of doing it. But it is so convenient and it is free, does not cost you anything. Many times we understand that web and internet is same thing but it is one of the methods of communication whereas internet is much bigger sphere, web is the smaller part of the sphere. They call it web because if you look at spider web, two points are collected by a thread. here also two also information you could link it the way it is like a web pages anywhere around the world, that is why it is called world wide web www. Mr. Murli was very kind enough to explain in very detail IP address. A server generally all the information is on the server, you call a computer a server because that is connected to internet 24 hours. An IP address of a server is few digits separated by dots. If you look into IP address of yahoo, it is called 66.94.230.31. IP address of Allahabad high court is 221.134.71.211. Now it is very difficult to remember these digits, domain name is nothing but a very easy way of remembering these digits, this IP address. Domain name for Yahoo server is yahoo.com. For Allahabad high court it is allahabadhighcourt.in. Initially one domain name corresponded only one IP address and one IP address corresponded only to one domain name. This unique way of allotting domain name to IP address is called domain name system or DNS. Today a domain name may go to many IP address because traffic is increased so yahoo server could be many parts of the world, different parts of the world. So actually if you type yahoo.com it goes to the nearest server. So in that sense Ip address could be different but this is unique for yahoo. Suppose there is a particular information and you want to reach particular information. The Correct thing is first you reach particular server. Then you go to particular spot where that information is situate. For example like yahoo server, the website, website means the URL. Uniform resource locator. That is where the information is situate for yahoo it is http://www. HTTPT is nothing but hypertext transfer protocol. Www is World Wide Web. For Allahabad high court it is allahabadhighcourt.in. Now if you want to know information about judges of High Court, that in a server is located in a particular place, that is donated by service. It is donated by particular broadly if you type this address it will take you to the where the details of Allahabad judges is situate. Domain name system is managed by a corporation called ICAN. Internet Corporation of assigned names and addresses. If you see these last two words .com. Domain name is unique for that particular digits. Typo squatting, I will just briefly mention about it. Like if you see the last three words .com, they are called top level domain names or TLTs, there are many TLTs, .com stand for commercial, .gov stands for government, .net stands for network and different kind of these are there. Countries have also been given top level domain name. They are indicated by two words. India address is .in. Now ICAN does not manage these top level domain names. These different top level domain name is known as country code top level domain name. This is managed by different registries. They are managing it, they just manage it and in fact the domain name is issued by a registrar which is attached of these registries. Often a question arises. Can you take a domain name which is associated with someone else? Can I register a domain name in name of sharukh khan or Amitabh Bacchan, can I do that? Or if I have a very small business, can I have a domain name which has something to do with Tata. What will happen if this is done? When this kind of dispute arises this is called domain name dispute. In fact the leading case in our country on this is Satyam InfoTech vs sify this is a case Satyam Info way was doing a business in the name of sify. Sifynet started doing it in the name of sify. The question arose whether they can do it or not. Satyaminfonet filed a suit for injunction restraining it from doing it. I don't know what the trial court did but Karnataka High Court vacated the injunction order. The matter was taken to Supreme Court and there the Supreme Court said that a domain name have the characteristics of trade mark and they are protected under the law related to passing off. If they are similar they can be ground of complaint and defences are similar as in passing off action. So basically it is a trademark.

Mr. Deepak: I just wanted to mention two things. One thing i was working with sify at that time more than that another thing, today the company's name is sify technology limited. When the case happened, legal name of the entity was satyam info way limited however when this company got listed on 19th October 1999 and was the second company to get listed is NASTAG after Infosys.

The reason it is infy is that by NSATG the code that was given was to Infosys was infy. Same is with sifi, when sifi got listed in October 1999. They got the code as sifi and that is how sifi got trademark under sify.

Justice Yatindra Singh: There was another problem at that time because that was under the old trademarks act and trademark could not be associated with service. Trademark could only be associated with goods. The Supreme Court also said, no none the less it will be associated with service as well. All these registries, managing com, net, gov or .in, they have come out with policy to resolve the domain name dispute. But then jurisdiction, if I take a domain name in the name of TATA then TATTA can raise a particular dispute. The matter could be raised under dispute resolution policy, it will go to service provider and the service provider will decide a case. Generally it is very good decision, takes about three months to decide the entire matter and their decision is not final it is subject to decision of competent court. They can only cancel or give you domain name. But service provider cannot give you damages or compensation. So our courts have taken a view that apart from cancelling or getting back the domain name, if you are claiming for compensation, claiming for damages, then it is not necessary to first raise a dispute there. You can come to the court of law directly. cybersquatting is like, if I take a domain name in the name of Amitabh Bacchan or sharukh khan, a leading case on this point is that somebody has taken a domain name in the name of present finance minister Arun Jaithely .com and Arun jaithely filed a suit for getting back the domain name, he got the domain name back along with 5 lakhs of compensation. Typo squatting is something like Justice Sachdeva was mentioning. That 11 is written there instead of ll. The leading case about it is Air France case. A person had taken a domain name. Instead of Air, they mentioned Ari, and thinking by mistake if you come to this particular website they can sell something else. Generally for celebrity spotting, generally you take a domain name so that in future it can be sold for a profit, this is being done so that you can do survey or do something for them by misleading them. We will do the rest one after the time permits but let us go to back to second point protection of computer software. Computer Software has got two parts, one is source code once is called object code. In the last part of session I gave you this. This is also a kind of description.



SOFTWARE DISPUTES LEGAL PROTECTION

Source Code

Copy right

Trade Secret

```
#include „proxy.h“
#include „signals.h“
#include „sslconn.h“
#include „sound.h“
struct PidginCore
{ char *ui; void *reserved;};
static PidginCoreUiOps *_ops = NULL;
static PidginCore *_core = NULL;
```

This proxy heading or something of this kind, I can read it but I cannot make a sense out of it. Probably a computer programmer can make a scene out of this. It is also a kind of description. A description of a passage to a computer software. We know it very well, copyright lies in a description. So source code is protected by a copyright. There is one particular question, it is there, Sometime I feel in copyright Act, some mistake is there in Copyright Act or I would be under some kind of mistake. If this is published then this is protected as a copyright all propriety software is not published, that event it is protected as trade secret but if you look into the copyright act even if it is written not published, perhaps it is protected by copyright that is a reading of copyright act. Personally speaking for myself I feel there is some mistake in drafting, you cannot claim a copyright unless you publish it. because if someone else comes up with same kind of description he cannot be punished unless he has stolen that particular copyright , you cannot challenge him for violation of copyright unless it is published that is a fundamental thing. But this requires some shaking or some fault would be there. **Nappinai:** Once it is expressed in any medium it is published.

Justice Yatindra Singh: Unless it is published.

Nappinai: No publishing is difficult from expressing. What copyright talks about is expressing the work

Justice Yatindra Singh: I am not saying that. I may be wrong. There is a difference of opinion which may be there. I thought I thought that unless it is published, you cannot claim a copyright, the reason is someone else comes up with the same idea, same description, he cannot be prosecuted or punished.

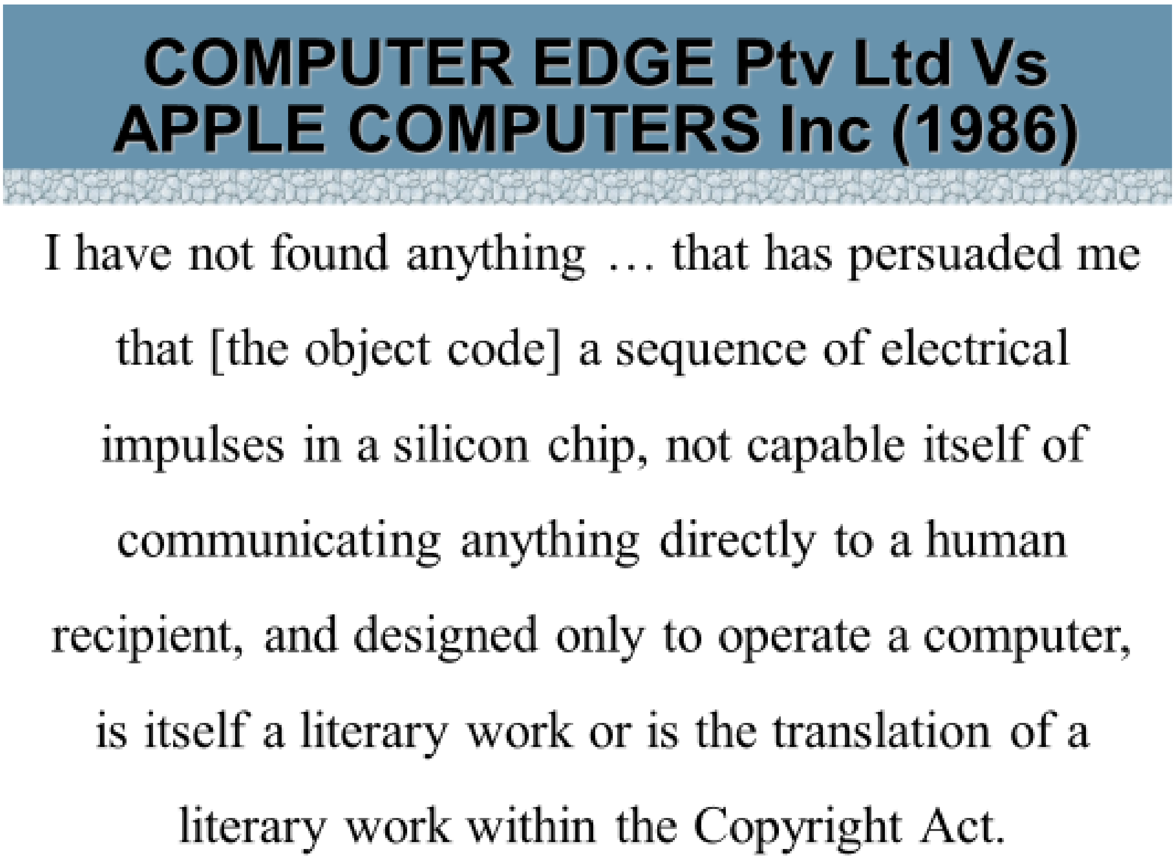
Participant: No there may be an attempt to prosecute, his defence would be...

Justice Yatindra Singh: May be you can put it that way, I will not go into it.

Nappinai: the only thing in IP that has a monopolistic right is patents.

Justice Yatindra Singh: We will come back. Just wait, we will come to it. That is why I called it is a dicey area. May be in some matter I never got this opportunity to decide many be one of your Lordships will get an opportunity to devise it, this question. But to my mind, all propriety software is not protected as a copyright, it is protected as a trade secret. Like windows, if you ask me, it is not protecting its source code as copyright, it is protecting as trade secret. That is one of the reason, if you look into the office. Liber office or open office.org is exactly the same. But windows cannot sue them for violation of copyright, they have what they have done it, they have reversed engineered it decompiled and they have used their format, doc format, doc is trade secret. But that is slightly a dicey area. But it is definitely protected as copyright. The question is how an object code is protected. There was difference of opinion, this matter went in Apple's Computers case to the Highest Court in Australia in 1986. This exactly, they allowed the appeal against the Apple Computers, and this is also what majority said. Pragya read it. This is what one of the judges, Justice Gibbs who was Chief Justice Gibbs of Australia High court this is what he says

(Ms. Pragya Aishwarya reading the following slide)



COMPUTER EDGE Ptv Ltd Vs APPLE COMPUTERS Inc (1986)

I have not found anything … that has persuaded me that [the object code] a sequence of electrical impulses in a silicon chip, not capable itself of communicating anything directly to a human recipient, and designed only to operate a computer, is itself a literary work or is the translation of a literary work within the Copyright Act.

Justice Yatindra Singh: *Mujhe to Bari muskil angrezi lag rhi thi ye to, main to iska matlab yehi samjha Nehru place Zindabad*...hahaha...that is the crux of this. I do not know what Indian Court would have decided or probably they would still be struggling with this problem. Still struggling at the framing of issues stage or something other.

Participant: Would the word literary substituted in the word propriety work

Justice Yatindra Singh: I have not found anything that would have persuaded me to object. Their argument was that this is protected as copyright.

Participant: There is not something that which cannot be protected under the copyright act cannot be protected.

Justice Yatindra Singh: May be the Australian High Court was only concerned, the argument was it is protected as a copyright. There is some history towards it, I will explain that why they use this particular words. Chief Justice Gibbs says that I am not saying that, I have just anything what the judgement says and this is one of the reason he gave, holding an object code, there is no copyright in the object code. What he wanted to say was is whatever the object code is in capable of being understood by capable of normal human being so it is not an expression of any idea, expression of anything, it is not also translation of any literary work so it is not protected as copyright. That is what exactly said. But thankfully in India this problem never arose, in the meantime the world Trade organization came into existence now WTO charter has about, 32 or 36 documents. These are part of WTO charter, if you want to become the member of WTO, you have to accept all these documents. One of the document is agreement on the trade related aspect of IPR in short TRIPS. Article 9 of TRIPS talks about Berne Convention. Article 10 talks about Computer Software. That is a source code as well as object code, should be protected as copyright. We also amended our copyright law, in 1995 and 1999 and now the computer object in our country be it object code or source code is projected as copyright. So if there is any illegal distribution of software, copying of software. Then of course there are, copyright act provides remedies. If there is a violation of a source code which is protected as trade secret, TRIPS also talks about that trade secret should also be protected under the law. But in our country unfortunately there is no law and we have not been taken to any court, that we should enact such law so we really does not have such law but if trade secret is violated, the only remedy is to file for breach of confidence. That is the only remedy available, there is no other remedy available. Patents is king of all IPRS, it is most powerful IPR. I must confess I am very open source supported and I don't have left leaning at all. People will think that open source is left leaning. Open Source got developed in America, capitalistic Country as a way of doing business and maybe I am slightly biased, you consider my talk in that angle. Patent , TRIPS also talk about patent, article 27 (1) says, patents should be patents, whether for process or for product, should be available in all field of technology, inventions, provided inventions are new, involve inventive steps and have industrial application. Sub Article 2 and 3 provides when it can be excluded. The reasons why patents are granted is that new inventions should come in public life. Under TRIPS it can be granted for 20 years, so you have to disclose everything how you are getting the patent. But for 20 years you cannot use it without getting licence from the person. People should spend more in research, experimentation and also for progress of science and technology. Nonetheless, if you look into the basic laws of the nation, mathematical formulas, algorithms, a discovery of new elements, discovery of new planet, new species. Now all these are tools to do science. If they are also patented then there would be counter products and that is the reason, patents are not granted for these kinds of things. They may be inventions, they may involve inventive steps, and they may, but nonetheless for these patents are never granted. Now these exceptions are provided for in the act itself. If they are not provided in the Act, courts have provided these information. Now patenting a software is a very debatable, very controversial issue and it will be a very good idea to have a global picture of it. Let us go and look into what is the way of United State of America. What the US does, whether we like it or not like it, the rest of the world follows. *Matlab super dada to hai hi, Jo change whai karemnge*. Nobody can say anything to them The Patent law of US, has no limitations at all, there are no statutory limitations, none the less, the American Supreme Court has created some exceptions. The first is Parker vs crook that is a case which involved a mathematical formula and the Supreme Court said that a mathematical formula cannot be patented there was a case where computer software was involved for converting decimal number into binary system, binary numbers. The Supreme Court said, computer system is a pure algorithm, it cannot be patented. Then came Mayo Vs Prometheus, this was case about, giving a medication to patient for a particular business. It is a process how much it is to be given, when it is to be given, it is a kind of process. Now Mayo Vs Prometheus was a case where they have summed up all this exceptions in one line. But they have also said, merely because an invention has a mathematical formula in it or algorithm, it does not become unpatentable. If there is a practical application of law of nature or mathematical formula or for that matter algorithm, then that can be patented and one of the exceptions they made was Diamond Vs Diehr case. This is a case rubber is vulcanized by heating it. You heat it to a particular temperature to a particular time. This relationship depends on an equation. In Diamond Vs Diehr case, what they have done was, there was a mould and they were heating. They were heating it and every second, the temperature was being monitored fed to a computer and at the right moment according to Arrhenius equation, the temperature was up, it would open a mould and rubber would come out and they filled an application to patent it. The American Supreme Court said that there, there is a computer programme. Here there is a fundamental law of nature. There is an equation Arrhenius equation but nonetheless there is a practical application, a computer software is along with an industrial process and is capable of patenting, then came a very debatable case. This is State Street Bank Vs Signature Financial Group There was a case where computer software was involved for converting decimal number into binary system, binary numbers. The Supreme Court said, computer system is a pure algorithm, it cannot be patented. Then came Mayo Vs Prometheus, this was case about, giving a medication to patient for a particular business. It is a process how much it is to be given, when it is to be given, it is a kind of process. Now Mayo Vs Prometheus was a case where they have summed up all this exceptions in one line. But they have also said, merely because an invention has a mathematical formula in it or algorithm, it does not become unpatentable. If there is a practical application of law of nature or mathematical formula or for that matter algorithm, then that can be patented and one of the exceptions they made was Diamond Vs Diehr case. This is a case rubber is vulcanized by heating it. You heat it to a particular temperature to a particular time. This relationship depends on an equation. In Diamond Vs Diehr case, what they have done was, there was a mould and they were heating. They were heating it and every second, the temperature was being monitored fed to a computer and at the right moment according to Arrhenius equation, the temperature was up, it would open a mould and rubber would come out and they filled an application to patent it. The American Supreme Court said that there, there is a computer programme. Here there is a fundamental law of nature. There is an equation Arrhenius equation but nonetheless there is a practical application, a computer software is along with an industrial process and is capable of patenting, then came a very debatable case. This is State Street Bank Vs Signature Financial Group, this is a case of federal court of appeal. Now here there was a computer implemented business method. Initially state had said that it should be licensed, it was refused they filled a petition for deceleration that patent is void. Trial court voided the patent, the appeal was filled, the appellate court said here computer software is producing concrete result in doing a particular business and it can be patented. Within observations it was remanded back to the trial court. After it was remanded the party compromised. So the matter was never tested before the US Supreme and for trial court also it got finished because the matter was compromised. Now this created a lot of problem. Amazon got patent for single click to get online transaction. Like if you go to amazon.com, purchase lot of things, and it asks, if you want to purchase it? You say yes, yes purchased. This patent was cancelled somewhere ago, by a Netherlands Blogger. He filled an objection, they had a patent and there was a case. They came out with, not a single click but double click. Gain it is Avery debatable question. Dukan me Gaye Dugan wale ne pooch Kya saman kahridna hai, Han Bhai kharidlo, isme how can a patent be granted for this, I fail to understand this. Well the patent was granted. You don't know what is true and what is not true.

Participant: In seconds lot of banks account can be hacked, money can be parked in some obscure bank.

Deepak Maheshwari: There was a case in Delhi where one gentlemen who looking at IT system in DESU, he actually, started rounding off the decimal and that money was going to his personal account. In those days quite a few lakhs.

Justice yatindra Singh: Slicing a very small amount of money.

Participant: I can share personal experience. I met to a restaurant, where the bill came to something. 63 paisa. Whereas the card was swiped, they rounded it off the nearest amount. I said look I am not paying you by cash, .63 paisa can easily be entered into the system and there will be an immediate electronic debit of 63 paisa from my account and it will be reflected, why you have made it to the next integer. i am just giving you an example. It is understandable that 63 paisa is not in your pocket so you collect the money.

Justice yatindra Singh: In fact all the restaurant owners are overcharging. If you look at it, bill in restaurant has a service element into it. They are charging service tax separately. 60 percent. Sale tax can only be charged on the 40 percentage of the price. Not on 100 percent. They are actually keeping the money in their pocket. Service charge they take 6o percentage. In restaurant when you eat they charge service tax as well. What happens is 60 percentage of the price or 40 percentage, I am not very sure, it is taken to be service tax. If you eat for 100 rupees, 60 rupees for the service and 40 for the goods. 60 rupees pe to service tax le rahen hai, 40 rupees per they should charge sale tax but they are charging sale tax on 100 rupees. This is wrong.

Participant: There was this argument made, that the fact that you are entering the restaurant is implicit that you want a service. Otherwise you can have the food in your house.0 rupees you are paying for aloo dum is actually the service you are paying for. So there is a double jeopardy.

Deepak Maheshwari: In telecommunication, in certain type of services both service tax and sale tax can be charged, independent of each other. Actually service tax is charged on a service component, and the sale tax is charged on the goods component and the Act itself sort of bifurcate between the two because the product itself has a service and goods component.

Participant: When GST comes, we will be in different regime.

Participant: Thank you so much Sir

Justice Yatindra Singh: Thank you

Ms. Pragya Aishwarya: Thank you Sir, now we have this demonstration session by PwC.

Mr. Sachin: You want to have bio break and come back?

Participant: rest room break. Bio Break

Session 5

Justice Murlidhar: Very Good Morning to all of you. It is going to be an exciting day for all of us. Hopefully we will have some useful interactions because we have got some very senior experienced persons who now their topics inside out and it is a privilege to have them here share their experiences with us and as I have always said in the Academy, we should be free to have discussions and forget all out individuals positions what we have. Be free to ask questions, also be critical, if you find if you have another point of view of a judgement, even if it be of Supreme Court, and in an Academy you should be able to freely discuss it. When you have resource persons who have vast experience, it will be useful for us to bounce our thoughts and ideas on them and see what we get as a result of that. My basic role will be just to chair the sessions, control the time limits and also the discussions that will follow the presentations. So the first session today is going to be on electronic evidence and this is a topic that is of immediate concern for entire judiciary because in last 10 years we have had huge volumes of electronic evidence flowing in our courts, not just the High Courts but also subordinate courts and barring the changes to the evidence act and some of the provisions brought by the Information Technology Act, we have not really device rules for electronic evidence for our courts and which is a serious gap and in the Delhi High Court we are trying to address it by actually sitting down to draft but this is actually the task of the legislature. For some reasons the legislature has not got into the act so each court has certain practice directions, like typically for video conferencing Trial have judicial orders determining how video conferencing to take place but it's not a uniform practice across the country and it can to a lot of problems because you to co-ordinate with many more Agencies just not just the court and also the level of equipment. Each Court may not have the same equipment to handle this so these are some of the issues how do you preserve electronic evidence. First of all how do you gather electronic evidence, how do you present electronic evidence, how do you prove electronic evidence. These are some of the real burning topics that we are all grappling with at various levels. So it's a pleasure to have two experts with us Mr Praveen Anand of course. And my Idea was that it's about 9:10 now you're supposed to end this action at 10, I think we can stretch it by about 10 more minutes so that we don't lose that hour that we have. Mr. Anand can go first for about 20 minutes followed by Mr Vakul Sharma for 20 minutes and then we could have interaction for the remaining 20 minutes so without much ado Mr Anand and I would request him to briefly introduce the kind of work that he has done.

Mr. Anand: I was under the impression that I have to speak for 1 hour in this session then yesterday I was told 30 minutes and today 20 minutes so, I will be rushing through the slides, so if you have any questions we can go through them at the end or as you feel comfortable but I will rush because I am squeezing a lot in less time. I have two presentations, I thought it was important to get into some fundamental principles about electronic evidence. I am not quite sure what background most of you have in terms of technology so I will dwell into few technical aspects and hope that those are well received, so first I would like to talk about evolution inn technology. I think it is very important to understand when electrical became electronic. We always had electricity passing through wires supplying currents to bulbs and other devices but those were analogue signals. It became electronic when concept of digitalization came. That is very important. First time technology was going digital and what digital meant was that you could for every switch, you could have an ON position or off position. So if you could have microscopic switches, you could put them as on or off and represent the on as 1 and of as 0. So if you could put ABCD in terms of 0s and 1s, you could have at the microscopic level on and offs at the chip level and so the A could be captured in memory. If you see the binary system, it takes a byte and a bit and essentially 8 zeros and ones constitute one bit and two hundred and fifty six combinations. So if you have A for example it is represented by 01010101 that may be A, B may be 010100. So the number of keys on key board are less than 256. You could have one combinations of 0 and 1 on each letter of key board, which effectively means if you are typing ABCD you are getting the answers in terms of 0s and 1s. Those 0 and 1 could at the microscopic chip level could be on and off switches and so the letters could, or anything can be captured at microscopic level. So the digitalization led to computers that is very important and with computers you needed instructions to tell them how to preform their task so you needed software. In computers, we went from printed circuit boards which was those green circuits which often come out of televisions and radios when they are being repaired. They went smaller and smaller to integrated circuits. You will not believe it but today on one printed circuit board you can have a billion integrated circuits. We are almost getting to such microscopic level. It is almost like getting molecular. That is why computers and devices are getting smaller and smaller. Software are the instructions given to computers. If it was man written computer that was called source code and then you had to convert it for a computer to understand. When you did it through a programme called compiler you called object code. That was a machine readable language. Early litigation, there was lot of misunderstanding regarding, only source code was protected or object code was also protected and there were various vies like the highest court in Australia took the view that since object code is not a humanely understood language, and therefore it cannot be literary work and therefore not capable for protection, and they had to get legislative reform in order to get tied over that difficulty. Then second major after digitalization came, networking. How you put various computers together and link them and if you link them in 1000 and 1000 you get an internet. So the internet was a creation of digitalization and networking and also compression technology because the digitalization meant you could put large amount of, for example the entire library of congress could be put into a box this big, that meant a lot of compression and that was only possible because of digitalization. So compression technology is developed. Then came a big change which was convergence, where your telephone, television at home and the computer would all become overlap in such an interesting way which I will just show you in a moment. So give your idea of this cyber landscape, first there are many pears involved and each one has got different interest. Cyber was the term used only when the internet came, so cyber essentially meant internet related. Cyber Crime meant today because of overlapping technology and how they merge into each other all devices multiple activities involving entering contracts, transferring money, buying selling, listening to music, seeing films, reading books, all this was covered under cybercrime. It was a civil wrong also a criminal offence and here I would like to show you second presentation, just to pause for a minute, just to give you a feel of. So you have at the regulatory level by the two ministries, department of telecommunications and information technology and then you have internet service providers like MTNL, airtel, idea. Do notice that there are roughly 249. Now internet service provider is different from telecom provider, we have only 11 of these. The first now requires, they put a cable in your office and home and then you can have a Wi-Fi. But that is easy that does not involve huge investment that is why there are so many of them. But there are few telecom service provider, here you need towers. You need broadband licenses and because of amount of investment involved and you have mobile phone producers like Motorola, Sony, and Samsung also. There are companies like Cisco that produce, routers and switches to enable the internet to happen. To pass information from one computer to another you need a device called router. Then there are chips producers, mostly now located in countries like Taiwan and China. Then you couple that with software, you have operating systems like Microsoft, Linux, apple, which are the basic software to run the computer. So when you switch on the button of the computer the software that enable the button of the computer to load the screen that is operating software, then you have applications. There are thousands and thousands of application producers. Anyone who can write any programme to enable any programme to be performed is an application software. There are many like Symantec, adobe and mobile phone apps. Now mobile phone became famous, everybody wanted equivalent on mobile phones, you have app stores from where you can buy these programmes. Then content generators like people who produce films like Walt Disney, universal stories, Books and publishers like penguin. Games, broadcasters like HBO, Star, CNN and colour. User generated is when you and me produce our own content and put it on internet or social media and here if you saw there are n numbers, which means no number and then you have websites like search engines, google and you have e-commerce websites, there you can have P to P, P to C and C to C and some of them will allow auction, some will only act as market place and will bring buyer and seller to meet each other. Then there are streaming sites, most of the piracy comes from direct download site and P to P sites which are pretty much dark. The torrent site are what you might call the dark net. So this is nutshell of what the landscape looks like so now let us look at the Information Technology Act.

Participant: Could be please talk about P to P, P to C

Mr. Anand: We would be all consumers so we are C and B would be business. suppose somebody is supplying raw material to a five star hotel, so it is one business selling to another business, end user is not involve that would be a B to B transaction, a business to Business transaction. If on the other hand I am selling my car, my second hand car on one of the side and you are a buyer then that is C to C. Customer to customer, similarly you have B to C. So The IT Act 2000, defines all these and I do not have time to go through this but just point out three places where I put content, so there is data, information and there is electronic record. These are content the other are all devices or machines so you have a communication device, visualize that as modem or telephone. You have computer. Then you have a computer network where many computers are linked together. Then you have a computer resource which is the whole system put together. the electronic record, the data plus this plus that everything put together is computer resource and the computer system is the input devices which you do not do ant arithmetic or logical functions themselves but only enable the inputting and outputting, the printers, the keyboard, the peripherals, those are the computer systems. The offences under the IT Act, I made an acronym that might help to remember all of this. AT MIT I SAT WITH THE CHIEF TECHNOLOGY OFFICER READING THE CPC. So A signifies access, anyone who has unauthorised access to a computer, then T for tampering, when you do anything like changing the figure, changing something, transferring something. Misrepresentation's, impersonation, and Identity Theft are the MIT where you are John but you call yourself peter, in the communication. Then information regarding contracts and cyber terrorism, privacy, breach of confidence, obscenity, theft. So this is kind of quick summary of various offences, there could be a lot. Every wrong is capable of now being done on internet so every wrong that you see, you always have an internet equivalent now. But this neatly puts it together into something which one can try and remember.

Apart from these offences there are privacy and other cybercrimes.

Participant: Just now you said obscenity, there is something same in the IPC. So we look in the general context or Classical definition context.

Mr. Anand: Classical definition but the act of communicating. The IT Act does not tell you what is obscene, it says if you are communicating, if you are doing any kind of sexual harassment, any obscenity or of that. It concentrates on the activity. Interestingly Internet is like water, it gets into every recipe. Literally it has a figure in every pie. Other issues are piracy and I don't have luxury of time to get into too much on that but to tell you little more on principles. On piracy internet has been called a giant copying machine and the interesting thing is the 100th photocopy is exactly the same as the first in digital world as compared to physical photocopy where you diminish in quality as you go along making copies. Now very interesting is the distinction. In classic IP law, you would have a distinction between the person who makes and the person who distributes. So making would be primary infringement and act of selling, distributing would be an act of secondary infringement and that distinction would also be practical because you would have lesser punishment to person who distributes and a greater punishment for the person who makes. But that distinction get burled on internet, you click a button, and automatically a copy is produced and it is disseminated. The second thing that happens is the transmission, used to be the source of wrong, the act of setting out from the creator. Whereas on the internet you found that if you have a server, people reach out to you, and it is the opposite. So they had to come up with a new right which they called making available right. When you are making your content available, rather distributing your content or transmitting it. The third principle was ephemeral reproduction. It Meant that unlike books, when you read them you do not photocopy a part of the book in your mind. But in the computer, you necessarily copy when you are running the programme, just by running it you are copying it in the RAM Chips of the computer, so you are making a copy into the computer and that is reproduction. But that is reproduction only till the time you are running the programme that is why it is called ephemeral reproduction. Finally cache memory, every time you go to a website there is a cache created which is a memory of what you did of your activity and unless you clear the cache, somebody tomorrow will be able to tell the entire history, or you went to car sites, you are very fond of Ferraris. So these are important, it is a buffer, the cache memory. Now the internet technologies, goods are now passing through wires and we will just see that in a moment. There are walls of anonymity. So the Delhi High Court in the yahoo, which was the first domain case, recognized that the potentiality of harm on the internet is far greater because A there is anonymity, you hide behind the walls of anonymity, people do not even know you are man or women or what and second you can cause so much more harm. Rather than distributing a letter to thousand people you press a button and it goes to millions. So the decentralized servers and architectural changes that have taken place. Then servers getting decentralized and change of architectural, this is very important. Because what that means is that when you are receiving an email from me that he is entitled to insert an advertisement in that email while it is being transmitted and then if he can insert an advertisement he can also tamper and change the contents. These are goods which pass through, films, music, software, books, they all pass through the wires. Now this was the yahoo case, a domain name case where they said, that for the internet, because earlier the American case laws have been saying that there is no distinction between standards between the internet vs that of the physical world. But the Delhi High Court took a view that because of the differences on the internet, the anonymity and the potentiality of the harm, we should have a stricter standards for the internet because half the time you cannot even discover who the person who has done the wrong is. Now Sony employed in order to encrypt the content on their CDs, they employed encryption technology which cost them millions of dollars. But it took a college students two dollars of open to discover to discover that the encryption was written on the edge of the dissect and if he put a black mark on the edge he broke the technology. That is why the concept arose of if you break a technology, it is like breaking a law, should there not be a punishment equivalent to stealing the content. WIPO came up with a treaty in 1996 where they called it circumvention of technical protection measures and anyone who tries to break a password or break an encryption or break a dongle, any locking device is equally punishable. How much time I have Sir? Around five minutes.

Participant: How do we implement the WIPO treaty?

Mr. Anand: I will just show that, it has been incorporated in the Indian domestic law by an amendment. So what is this, this is what I call a technology sandwich. So the first layer is a law which is let us say copyright law, which is do not copy somebody's book, the second layer is technology which is used by let us say, famous publishing house to protect that content from being copied from the internet, let us say an encryption or password scheme. If someone breaks that, then there is a second law which says that if you break that you are equally liable as you have violated copyright. So that is the second layer of law. And these are the kind of technologies which are being used. For text music, video, there are all different technologies which are being used in order to manage the software on the internet so if you break these technologies you are equally liable under the new law. What are the sources of electronic evidence? Phone calls, record obtained from tower logs, emails which are obtainable from server's hard disks, printer history, when a document was printed, so it may have been erased from the computer. Websites and web history and also do not ever forget web archives, there are archives where even when the whole website have been deleted you can still go to the archive and see that this website existed on such and such date. Then the HTML, the underlying code when a website is made can be looked it and you can find Meta tags which will give you the intention of the party. We had a case of Delhi High Court where somebody had copied on a website, Colgate's website, we could find html, in the html code the meta tags had the word Colgate so we could immediately know that the person, because the persons defence was I have done it independently but the smoking gun evidence was there in the HTML code. It is very easy for an IT person to open up html code for any website, you can be taught how to do it, it takes 10 minutes and then you will be able to check every website for html code. Two safeguard, one is confidential, and for that the Delhi High Court in the West guard Franscon case set up a confidentiality club so that the defendant cannot say that I will not disclose this information because it is confidential. The court said we will keep a confidentiality regime and you will then disclose. And then privilege, I have taken only a few privilege, section 126-129 of the Evidence Act. Deletion, when somebody deletes something it leads to an adverse inference that he is trying to hide something and hence companies these days have very strict procedure for when a deletion can take place. Intermediary under the IT Act and the Rules, are obliged to preserve all the information for up to 90 days, then there are two rules, I am rushing Sir, I will take two more minutes, Glow back rule and the quick peak rule. Essentially if you have taken too much in discovery then you are obliged to return that which was not relevant. These are the rules which US uses. We are trying to incorporate these through case laws. The evidence act there are relevant provisions, particularly section 65B that is how electronic evidence is proved, by having section 65 B affidavit. I will have more time in the second session of I will be able to cover some of it there. So let me conclude by saying that electronic evidence is a modern litigators tool and it can solve any crime where a person touch the internet and why because a lot which is not visible in a print or to the eye is visible electronically such as the meta data or time stamps of the creation which are visible when you print, or the deletion history, that is always there. Upto 8 layers you can go down. If a person deletes something and put something like that 8 times you can go down. Then finally once something is generated on internet it is very difficult to remove it and Tata green pea's case was a case where, we will talk about that in second session. But essentially Atta was called Tata demons by green peas and that there is a law suit which might be successful but that information will never go away from the internet. Once it gets there it remains somewhere there. Thank you very much.

Justice Murlidhar: Without much gap I request Mr. Vakul Sharma to continue.

Mr. Vakul Sharma: I think Mr. Anand has made my job much easier, just to put across certain facts. Till 1984 there was no word cyber space in the English Dictionary. It was a science frictional work by Neuro Menson. He in his work for the first time used the word cyber space. If you look at the root word, then this root word cyber has a Greek root work and it came from a word called cyber net ticks which again has an origin in quber net ticks which in Greek has to do with metaphysical and philosophical outlook. So the word cyber has origin from let is say the old school. Now looking from the point of view of appreciation of electronic evidence. Since I have one more detailed lecture so I will just try to introduce certain concepts here. The first and foremost thing is what electronic evidence is as such and when we are looking into an electronic evidence what kind of evidence we are looking into. If I just look into very simplistic definition of what is electronic evidence? The IT Act has a different word it says electronic form, so a digital form or electronic forms they are synonyms here. That a party to court may use it at trial. When I look at the electronic evidence which is presented before the court of law, first thing is collection, followed by analysis then its presentation before court of law. If I am going through all this processes from where I can get all this information. So in the centre i have user created digital evidence. It is in the form of my subscription to web email, my web chatting, the text messages which I have sent, the WhatsApp or any kind of chat platform in form of text, kind of messages, video, images and the kind of data base, which means kind of information which I am generating over a period of time. If I look my entire mail history is nothing but data base. I can classify them into different file, give them different names and yet it becomes a kind of data base. So data base is here a collection of information in form of a folder. So what kind of evidence am I looking into, when I say what kind of evidence i am looking into, I mean the kind of evidence the courts are looking into. Back up registry files, there are print outs of hundreds and thousands of pages presented before the courts, creating all sort of information, all sort of activity logs. If I am looking at point of view of call data record CDRs, it is nothing but could be offered as a backup by the registry files. So the point is this kind of voluminous information, which is being registered every second, every minute, this is registered where. It is being registered where calls are being registered. If I am making a call data, time, duration any such number are being routinely being recorded in a server. So the question arises what is a server, server is nothing but a advanced form of a computer, it means a computer that serves multiple computers in a simple manner, so a server is a huge computer which has huge capacity and that records each and every detail, every key if I am going to press and if I have net activity, then every key which I am going to press will be recorded somewhere. So what kind of collection I am looking into, emails, digital photographs, ATM transaction. What is in ATM transaction, the ATM cards which you have got has a magnetic film at the back and this film contains all necessary data. There are cards which come with very small chip, instead of magnetic tail it can have a smart chip also. That means every time I am going to use that card, my pin is being registered, my name, the activity is being registered somewhere, some server located. They instance messages, blackberry, WhatsApp, V chats, VOPI, skype, the issue is this is huge amount of details which are available in particular case which may be presented before a court by the prosecution or by defence council. The point is in order to appreciate their authenticity, relevancy and admissibility it is huge task. I will demonstrate in the second session, call data records which is being presented before the courts may be a fallacious thing. Court may not record the call data record which is being presented. The IP addresses which are being presented before the court, the court may have to look into the entire configuration of the IP addresses. In very simple term what is an IP address Ip Address represents internet protocol address. It is set of number. Every time I log on, my computer will terminate a particular set of number which will provide physical communication from where such reading was made. These set of numbers are being refereed as octaves. So the number could be. There is four set of numbers. This could be any number from 0 to 255. So every time I am logging there will be a specific number generated by me and that specific number will provide. I will just give an example. Suppose a cybercrime is being committed from NJA, Bhopal.

Participant: Who allocated these Ip address

Mr. Sharma: It is allocated by an international body, APNIC. Asia Pacific NIC. This provided a set of IP addresses to internet service provider. First number denotes whether it is from airtel, bsnl or any such provider. Second number provides the location. Third provides the state or the town and the last digit will provide pin point national Judicial Academy.

Participant: I use my laptop here with my data dongle. Will my IP Change?

Mr. Sharma: The moment you use the data dongle the carrier, kind of arrangement, suppose you are having an idea dongle and idea is not working here so idea has to latch on the airtel network here and the moment they do so, number will be placed and this is how it is done and this is considered to be a very good tool from the point of view of forensic evidence. Now the problem is we do not know when such kind of affidavits being presented by telecom or ISPs, saying that this is the number. First point is there has to be date and time. IP addresses keep on change they are not static. First question that is to be asked is do you have a static Ip address policy or do you have a dynamic Ip address policy. Number two what is the date and time. Without date and time, this IP address has no meaning.

Participant: Electronically is it possible is it possible for the creator of the IP address to manipulate the data

Mr. Sharma: The point is masking is possible that is why it is always possible that when such kind of evidence is being given by ISPS before the court they should file it on an affidavit. Spoofing techniques, when you are spoofing, you are altering the place, time, it is always possible because such application are available on the net. But the point is by forensic examination at the server level of ISPs they can find out that yes whether a masking has been done or not. Suppose I will just take one example here, national judicial Academy, I am not the only person using their Wi-Fi, there are 100 others using it. But my Wi-Fi has given to me in room number 6. So the moment I have committed a crime at room number 6, they will find out yes the Wi-Fi at NJA given to room number 6. If I am using a licensed service provider. There are proxy server also which are there. If I am a license service provider I am not supposed to use from cyber security point of view, I do not have to connect myself with the proxy servers because this is one much undertaking which most of them are following. It is known as ISO 27 thousand 1. There is a regular and inspection process to see whether the data is being compromised. The moment I am going to connect myself to your route server I am compromising the data of my users. The moment I enter into hotel room, the moment I put my card into that slot, someone is recording my coming and going , so I am leaving behind my digital foot prints every time. Suppose I am clicking a picture from my mobile phone, the moment I have clicked a picture from my smart mobile phone it will give away the latitude, longitude of this place. So the point is from the point of view of not only the collection of evidence but its presentation before the court and its appreciation that has to be taken from the point of view of this slide.

Participant: You said the IP address is never static, the money you log in the number would change.

Mr. Sharma: No the point is, I would just like to clarify here, once I have logged on I will get one IP address, I logged off. I again logged on I will have a different IP address, but it will depend whether that service provider is putting across to me a static, one address 24 hours or different addresses at different time period. SO the first question which is to be asked is do you have static or dynamic policy. Dynamic policy would be he would be giving new number every time I am logging on. These last may change the first would be same. There would not be variation in first 2. 1st is ISP, 2nd is reason, 3rd is which state and the town the exact location. If you are in same area first three would remain same. 2nd important thing is without data and time. I am seeing 100 of cases being filled where just on the basis of IP addresses without data and time it would have no value what so ever. There could be many reasons why IP address is showing not available. There could be some conflict with the device also. That is why you can some time get a message that someone else is sharing your IP address. This is some sort of configuration that has to be made with the device. Here the most important point with the point of view of court is the hard disk. Do I have 5 minutes? So in a very simple terms, what is a hard disk, it is nothing but a recording device. It records each and every key stroke. Even if I am deleting a device it can be recaptured from the hard disk. What could an inside of hard disk may look like? It could be a spoon like this. A magnetic spoon. If I flatten this magnetic spoon I will get a picture like this. The entire magnetic film is divided into sectors so when I save a file. I will save a file across like this. I have saved one more file. But if hard disk is not handled properly what is going to happen. Some of these sectors will become bad sector and I will have difficulty in reading the entire file. That means the integrity of the text or content will be lost. That is why the preservation of the hard disk is the most important aspect when we are looking into connection and subsequently retrieval and also from point of view of appreciation of such evidence by the court. Same thing is applicable when I am looking into memory card, we have memory cards, sim card all these have let us say a kind of spoon which records each and every thing and the difficulty is the kind of malkhana which we have got. The electronic evidence will be not saved for the entire trial period. At the first stage it when the application is moved by prosecution or any such party replica of a hard disk or clone is made. What is replica or clone? It is sector by sector copy in form of DVD. So even if the trial runs for many years. You are not going to touch the mother disk. You have the replica or clones which can be looked upon or presented before the court in form of authenticated thing. So I think in electronic evidence preservation this could be the first most important thing, considering the kind of situation which exist in our country so it is in form of replica or clone in a CD.

Participant: Will replica be an admissible evidence

Mr. Sharma: If it is being done with the permission of a court

Participant: Older High Courts like Calcutta from where I am, we had taken a policy decision to slowly digitalize all our archives and records. Now we started the process few years back. Unfortunately we had to give it to an outsourced agency and he wanted to make them into CDs. What happened is 2 of the Cds were corrupted and we had to, because we can always de materialize it, now some fortunately we knew some of those writ petitions or bail application which we had taken , luckily we were saved. We stopped that programme. There is a problem here at very practical level. We are thinking, not only our High Courts but other High Courts as well of slowly going into electronic storage now how to make it full proof, because even a replica or clone it can get corrupted.

Mr. Sharma: Sir the answer to your query is, once this replica or clone is made it is signed with the help of a digital signature.

Participant: What if the technology goes obsolete. We do not get DVDs any more.

Mr. Sharma: Yes, so point is the digital repositories, can be created and it should be created. Because the point is as your Lordship has rightly said, yes I mean even the .doc is moving to.dox so all this kind of lets us say format change are going to happen. the point is a digital repository is maintained and the point is replica and clones . What is the guarantee that they may not be tampered with? So as and when they are made, they should be signed with the help of digital signature, if there is any intercalation and any different date by someone then yes it will show that someone has changed the message. So this is how the text from that point of view can be preserved. One thing is we can always say, that how about digital signatures they can always be corrupted. If you ask me whether digital signatures are full proof, I will say that with the present computational strength available to me I can hack into digital signatures also but it will take me 10 to the power 9 years. This will happen when Sun and Mars will come and collide, yes I can hack into digital signature but it will take this much time period to hack.

Justice Murlidhar: I have a more practical question like, let us say that I have got a mobile phone which is used to make video clips and I want to tender that as evidence. Produce the mobile in the court and I say I cannot leave the phone with the court because it is an expensive phone. How will the phone then extract or make a clone of that.

Participants: very easy sir

Mr. Sharma: the point is whether a judicial officer can be asked to look into a mobile phone because a judicial officer has judicial wisdom but he is not having that technical wisdom available to him at that point of time, he may look into that particular thing. Now the possibility before him is forensic examination by FS l, so that person has to give application before the court for forensic examination, whether it is in one single flow or it is cut and paste, or for any other modification, so that can be done. So forensic examination that has to be done. If court has to look into some truth in the evidence.

Justice Murlidhar: Court cannot receive it till it is first presented to the FSL lab then a copy made and it is then presented to the court

Mr. Sharma: yes the court cannot receive it, the court cannot collect, and first an application has to be placed for getting the phone examined.

Mr. Anand: It is something we do all the time so I think I will give practical answer. Although your answer is the right answer, I will add to that. What we do it we take video on mobile phone, it is very easy to put that in the DVD then that DVD along with an affidavit of the person who own the phone with full details and the fact that this was the DVD done in his presence it is not tampered, all the information of 65 B is put in an affidavit and filled in the court. It is extremely rare, for a defendant to come and deny that.

Participant: the question was if you a phone, the phone would show it as a single video, the only way to check is whether there are gaps etc. is from the original. If you copy it on DVD the entire time stamp will change. From a DVD it is not possible to verify whether it is a continuous recording or there are breaks etc. That can only be done from original.

Mr. Anand: If all of that becomes relevant. It might be relevant in which case it is very important the exact thing but in civil action broadly, our experience is the defendants come and admit

Mr. Sharma: As a defence counsel I will ask that please give me details of the device from which this mobile phone has copied in the DVD so the point is and one thing more, by recording from mobile to a DVD there is a format change also, so all kinds of questions can be raised, from point of view what was there in the mobile and what is now being exhibited in DVD.

Participant: Even copying of the DVD, if, it is used for a device which is using pirated software.

Mr. Sharma: there are so many things when we are looking at from the point of view of capturing analysis and presenting before the court electronic evidence. This is a case of 2002.

Justice Murlidhar: Can I just suggest one thing, we will take a tea break then we will continue and we will then merge into next part. We will keep it from here.

Mr. Sharma: I will take 5 minutes on it and then I have one full session.

Justice Murlidhar: Let us now take a tea break and come back. 10:30

Session 6 and 7

Mr. Sharma: let me re assume. If I say electronic evidence in the light of 2002 judgement, then it is duty of the court to appreciate minutely carefully and analyse it, when it comes to electronic evidence per se things become extremely difficult. Why, because certain steps were not followed when the collection of electronic evidence was done, certain steps were not followed when they were analysed. So if there are gaps before the court need d not follow, it need not muster what the courts would say. So again in very simple terms, what is an electronic evidence in today's context? The evidence that existed in electronic form is being produced before the court in a tangible form, so the courts are presently examining, the print outs and yes we have section 65 certificate also. So the entire electronic evidence that is presented before the court is in tangible form in the first half we had talked about the hard disk part, and there is a judgement by the Lordship, Dharamveer vs CBI, where the Lordship has said that the hard disk is a document but one part of that judgement has been missed by us all. Lordship has also mentioned that the marked hardship should be kept in aseptic device, it is a case precedent so why not that hard disk of the important case be kept in a septic environment and I believe that judgment it is towards the end of it. So the point is that I am looking into it as electronic record so basically tangible form evidence that is electronic record data record or some document sent, received or stored in electronic for, microfilm or computer generated micro film. So we are basically looking into all sort of electronic evidences which is being generated by us. Whether it is in form or WhatsApp or ATM machine, in fact this presentation is nothing but presentation in electronic form so this is an electronic record. I think this is what the court is grappling with, can it be tampered with if such evidence is presented before the court. If this is true then these also are truth. They could get tampered. There could be tampering when such kind of Cds are there. So just maintain a DVD will not suffice unless and until it is signed with the help of a digital signature. So just merely a cd presented before the court because the point is section 3 of the IT act says, electronic records to be authenticated by means of digital signature so if dvd or cd is an electronic record or a document then yes under section 3 of the It Act, it has to be authenticated by means of a digital signature. So the example that we took before the court, are we expecting judicial officers that they are technocrats, the answer is no. Judicial officers cannot be seen in the light of technocrat but yes the court may lose an evidence not because of the technology but because of lack of appreciation of evidence. So I think that becomes the most important and I say buzz word, that of appreciation of technology as such, which is the most important thing with the point of view of appreciating the evidence that is being presented before the judiciary. The questions before the court when they are appropriating electronic evidence, did the investigating agency get the evidence or did they fake the evidence. Most of the time print outs. No one is challenging section 65 b. Millions of print outs being presented before the courts without section 65B. So the point is these print outs which I am receiving which is being deposited, which is part of court file it could be a fake print out also. So onus from that point of view is I should say very significant, this case that is Mohammed Azmal Kasab case, which has looked into the entire thing, the entire scenario of electronic evidence, whether it was in form of cctv footage, mobile devices, data cards, VOIP, everything has been dealt in detail. In fact Justice Taheleiani, this is the kind of work that he initially did. This is the kind of work which he did when he looked into the entire thing and infant the original judgement and the entire court judgement. Understanding the nuances of presentation and appreciation of electronic evidence before the court. I will stop here.

So we move on, there is a slight alteration in the schedule today, session 8 which was procedural law and investigation measures, we will have it right now because Mr. Pravin Anand has to leave early. So that is the session we will have now. We have two resource persons, Ms Nappinai and Mr. Pravin Anand, we will follow the same format, 20 minutes each. This is 2 hours so many be 40 minutes each.

Mr. Anand: You can take more time, I will cut short. I want to apologize to all of you, I am sorry to disturb the flow, it is only because I have to travel overseas tomorrow and that is why it is important to get back early. I am really sorry to disturb that. This topic was a very unusual topic, both of us were talking that there are 4-5 sub topics here and we have to make them flow and she has taken one interpretation of that and I have taken slightly different interpretation. I think between it I will be able to cover most of it in between. I would first like to mention a bit about procedure because procedure was important word in the topic and on procedure on the civil front we have had even before the commercial courts act was introduced, the Delhi high court particularly had fast track trials, local commission was appointed to introduce evidence we have a wonderful facility in the High Court where evidence is recorded. Sometimes on a day to day but mostly spelt out and it is done very quickly and those trials have concluded in a few months so you have witnesses coming in on Wednesday coming in on Wednesday or Thursday and back on Saturday. Sometime courts have even permitted recording of evidence in hotel. So it is business executive like environment facility, it is very quick and fast recoding of evidence. There were time where evidences were not able to come back because their evidence were not completed or in one case the witness got cancelled later detected. And so video conferencing was done to complete that evidence. Facilities ion the Delhi High Court are very efficient and they come with international formats. The evolution that has taken place on video conferencing has been first presence of High Commission from London was considered necessary and thereafter in subsequent cases and in the 3rd case, Justice end law passed an order that wide angle camera should be used to see that no assistance is being provided at the foreign end, it was considered good enough and it facilitated very quick recording of even a video conference, now with those fast track trials, there came a case in Supreme Court. Because of direction of Supreme Court, entire evidence was finished in 1 and 1/2 months and matter was concluded in 5 months from the time when Supreme Court passed that order. Now we have commercial courts act which introduced fairly new concepts which will speed up trials. In all this there is lot of use of, in civil litigation, computer downloads, website downloads, cell phone extracts, sms, etc. and so 65B an affidavit under section 65 B have been used and as Mr. Sharma very rightly pointed out these affidavits in most cases are not even challenged even when the person giving the affidavit was cross examined, they were not able to shake the testimony in any of the cases and as your Lordship rightly said in criminal case, the standard would be, you will have to go into far greater detail of how the technology works and to make sure there are no as your Lordship said, gaps. So you will have to be far more careful and far stricter standard would have to be adopted and for that the test is to understand how the technology works, that is most importantly and I think the Court has to understand that how technology works. Now section 78 under the IT Act, investigation of offences and search and arrest without warrant, those provisions are also part of procedure. I want to mention on preservative measures, investigation and production, I want to mention software piracy cases and these are very interesting. Originally when piracy cases started almost 25 years ago, they were channel cases and channel meant that in certain markets you find people selling, at that time on floppy disks, and thereafter on CDs, software worth millions and millions on one disk and it was all pirated and it was and you attack the retailer. Then it shifted to hard disk loading. Hard disk loading meant that the person selling his computer thought that if he will supply you with free software then it will be an incentive which will make you prefer his shop to another shop and so he asked you what you will use it for. You said you will use it for word processing, data based functions and he said I will give you such and such, Microsoft office I will give you, windows I will give you and free of cost that is an offence again and a civil wrong and is called hard disk loading. The third, very soon companies realized that they ought to attack the legitimate business, let us say a factory manufacturing shoes, but using illegal software or having one license or no license so under licensed under licensed by legitimate end users who are running their legitimate business but their activity of computing is illegal and those who are very useful for software companies because they will be able to very quickly get the companies to sign an agreement get an order 23, rule 3 application, settle the case , get the party to purchase legal software, and perhaps even get some damages and move on, those cases finish very quickly, you won't believe but last year there were 8 cases, a survey was done, the average time to dispose of a case was less than a month. Now from end user piracy we rare moving to internet piracy because we are getting to the cloud , the cloud is nothing but a very large computer maintained somewhere, housed somewhere in the United States or some other place and the company that holds that computer and gives out that service manages the cloud. Like Microsoft and you keep your documents on that computer rather than keeping them on your hard disk. So your memory is saved. So in all these piracy cases one of the usual order passed was the Anton pillar order, an order to search and seize hard disks, originally it was hard disks and in some cases the party said, they complained that the process of removing the hard disk, although it was removed with an expert, my data got corrupted. But because those complaint were made in some cases, full computer was sealed.

But the precautionary measure was the court quickly unsealed it after backup copies were taken, so as not to destroy, disturb in any way the business. The third phase came when there was some sort of resistance, and in two cases of the Delhi High Court, premises had to be seized. So it went from hard disks to computers to sealing of premises. Of course that is very strong order, very rare and would be passed only if there was real counter measures. The surprise element was extremely important because it is the nature of digital world that you destroy very quickly so, to give you one example, the first John Dow order passed by the Delhi Court was when the world cup was going on and ten sports got an order appointing the Registrar of Delhi High Court to go all over the country and to determine which were the parties using the stealing signal and broadcasting illegally and one of it happened to be a major cable operator is Mumbai. When they heard that somebody is coming, knocking on their door, they switched off the signal then got the registrar in their office. When the signal was switched off, everybody called up the office to complain because they lost the signal. lot of people were complaining, and the local commissioner sat their receiving those calls saying yes , when did you give your subscription, and noted down all the details all the subscriptions, details, everything, when was the signal switched off and filled that evidence in court. When that was done 3500 licenses were fined up in 20 days because the world cup was only a 1 month Intellectual property. After 1 month, there was no use and that was the effect of that order. The point here is surprise element is extremely important in these cases because of the ability to destroy. Now on production, section 76 of the IT Act talks of confiscation of and five things go together, the computers, the peripherals and the printers, the network, the computer resources, all the hard wares and the communication devices. All of them can be seized, can be confiscated, in violating any of the provisions of the IT Act. Jurisdiction is very tricky, you have section(2), of the IT Act which says it extends to offences, committed outside India by any person, irrespective of the nationality and then you have a support in section 75, which says offences outside India would be covered by the Act if the computer and all those things go together with the computer. If computer resources, those devices are located in India. Section 182 of the CrPc talks of a court where the receiver or sender resides would have jurisdiction and then in the civil context you have 2 decisions of the Delhi High Court in the banyan Tree and the WWE case and I could talk about that if time permits, but let me just give you a few practical example of what problems arise. For example we were talking in Mr. Sharma's talk earlier about tampering of evidence and destruction of signals. The first software case in India was a Microsoft case, a software piracy case and at that time software was put on a floppy disk. It was a criminal case and the police took the floppy disk and they took a sua and they put it through and they tied the floppy disk to the file. So of course complete evidence was destroyed. Now here is the Himalayas Drug Companies case where this was the website where they copied roughly 210 of the drugs of the Himalaya were copied and this site and other information except at and this site had no other information except at the bottom it said sumit@ something and sumit sounded like an Indian name but when it turned out, sumit was an Italian called Lusabianki and with an Italian address, now how do you get him. So most of the problem with these websites is that you stop at an injunction, you cannot go beyond that. Although in this case, the court exercised jurisdiction and that is the reason why I am using this case, to talk to jurisdiction. Although damages were granted of 15 lakhs of rupees, the suit was decreed, but nobody was there to pay the damages, so one of the biggest challenges in Internet cases is how you do, if a person has person at the time of registry of domain name has given a fake name. First registration is the domain name, no suppose I register the domain name alpha name and I register in fake name not my original name and fake register, they will register alpha.com they do not have a verification process. In fact the whole international debate has been, at the time of registering the domain name they should insist on the identity of the person because it is the biggest challenge. Now the opposite side of the debate was it hampers the freedom of speech, freedom of internet and there is lot of NGO support to it. So this is one case which ended in a degree but it is a paper decree. Then just to kind of talk little about, the isp was subsequently added as a party so that the order could be enforced. This challenge of not being able to stopping the wrong is the biggest challenge which we are facing.

Justice Murlidhar: The question is even io we are talking down from that IP adders it is possible to be loaded on another Ip address.

Justice Nappinai: The innocent of Muslim case is a classic example.

Participant: To travel from here to UK, we have to go through various processes, it does not mean that there is a restriction on the movement. But there is reasonable blocks in the ways. When you have to apply for a visa, have a valid passport and pay for ticket. If that can be accepted why not this.

Justice Murlidhar: There are millions of domain name which are fake which are already in use. So while talking of the future you have to deal with the present.

Mr. Anand: So just to give an example of what my lord is saying, suppose I stop somebody from using Tata1.com, the he registers tata2.com, then he registers tata3.com and he can go on like this . So it is like fighting bees with a hammer. It is like that. So this napster example is a perfect example where the peer to peer piracy it became tougher Nutella made the user a server so each person who used or uploaded his music in order to pass it on to another user became the server, so they changed the architecture and that made it tougher. Now came Kaza and Morpheus. This was a technology which enabled Nutella, most of the countries would ban it and in fact if you take the next one, Morpheus was sued in Holland and it took a view that we made the technology and released it on the net and now we have no control over it. So that was one of the biggest challenges. Then came bit torrent and there is lot of bit torrent still on the internet which is used for piracy. One of the biggest names in the piracy is bit torrent and then we have the Delhi High Court case, sorry I have covered some of those parts, it was an adult side which used data and the site was in the use and the Delhi High Court followed the phoolan Devi division bench case where the film bandit queen had been restrained by the Delhi high court but channel 4 television filled a suit saying that you can stop the commission of tort in India but not oversea and the Delhi high court said no we can, because they went into principles of private international law and said when there is such a direct nexus between actors and directors with India, then even if the tort is committed overseas we can extend our jurisdiction and the same logic was used in this Tata vs Hassan Yakub case of the Delhi high court by Justice, i forgot the name and an injunction was granted, recognizing that court had the power to stop the commission of a tort overseas.

Justice Murlidhar: Mr. Anand, have you had an experience of take down order not been complied with and what recourse can a party have, because the person who is supposed to comply is outside the jurisdiction

Mr. Anand: I think if for the same reason you cannot recover money if you have damages award. I think the maximum you can do is to approach the service provider and enforce through service provider but then you stop at just getting the website to come down and nothing more.

Justice Murlidhar: But is there way of blocking the URL. Can government do anything to block

Mr. Anand: The government has certainly been doing that in China. They have the technology to block and it gives rise to all sorts of protest.

Participant: In India also the service providers are blocking and now bit torrent you cannot access, you cannot access some of the sites on u tube, X video you cannot access.

Mr. Anand: There was a discussion that they would do that but are they doing it?

Participant: yes

Mr. Murali: Sir, Bit Torrent cannot be blocked per se because

Participant: No in India the access to bit torrent is blocked now.

Mr. Murali: Bit torrent is a small programme. The websites which hosts the streams can be blocked. As we explained it is peer to peer network so if we are the people in this room we can share with each other. It is impossible for the ISP to block this communication. But they can stop the seed which tells you that I am hosting a movie called Phoolan Devi that they can stop.

Mr. Anand: Phising which is another very interesting concept, there is a case from Delhi high court the Nasscom case where decree was granted damages were granted and essentially it is like this. You get a letter from city bank which says your details are out dated and you are requested to reconfirm them you fill up the form, write to them and that is a fake way of some party in Nigeria getting all your bank account detail and next thing you know, all your money is transferred out of your bank account. This tort is known as Phishing and the Nasscom case was case when someone using the name Nasscom to run seminar in India and they were stopped and that was another interesting tort. Then Framing, this was national geographic which brought a law suit against a party which was using their website, taking the entire content of their website. They formed a kind of frame, like putting some body's else's picture in your frame. Then hyper linking and deep hyper linking. There have been cases where people have been using their website but have been using links of other people's websites and have taken website of my diverting traffic and getting advantage of the iballs and increasing their own traffic in process. Meta tagging, if you went into the html code underlying the software, you would find catch word like Tata and this I have said in earlier presentation is a useful way to discover what the true intention of party who formed the infringing website. Then spamming, and today you have seen spam coming even in the telephone and we have had only one case in the Delhi High Court where an injunction have been granted but it is still in evidence, not concluded. We have travelled a long way, we have e courts. The UDRP is uniform dispute resolution system administered by WIPO. Here you file a complaint by email, the response is filled by email and the decision is given by email in about 45 days. All this is electronic and then of course the electronic evidence which we were speaking about and then the video conferencing and what was left was the money part and recently just about 10 days ago, there has been a decision where a website has been asked to pay 1 crore by the Delhi High Court because they were felling fake watches online and hopefully this money if not wholly but partly be recovered because this person is holding appearance and so is physically found. We have a physical address as well. So hopefully this one might yield in result otherwise it is very clear that you have to have forensic evidence probably tying up with international bodies is using information exchanges to follow because most of the websites that are selling the ecommerce accounts, they all have bank accounts. They all receive money and if that money could be followed it is good solution and if internationally in the US particularly FBI have been doing a lot of that and tying up with credit card companies, courier companies, shipping agencies, companies in order to get important information and that think that probably is the way to go.

Justice Murlidhar: Any questions from Mr. Anand, or we can take questions at the end of the session.

Ms. Nappinai: I am sorry I will just take one second to connect this. I was not sure whether we would be covering the topics separately or jointly so I have, as usual a lot of slides to cover. I have tried to combine both. On the question which you have raised that whether we have experience in take down orders not being complied with. I have had situations where take down orders have not been complied with. Now what happens when we reach enforcement stage? This is what I was going to focus in today's session. There are three aspects to how a case proceeds. First is just where we have a problem we approach a court. The procedural aspect which court has to follow is want to see what the reason is, what is the basis s for coming before the court. Second is an order is issued to protect the rights of the litigant but the third part which is where we have seen a lot of slips between the proverbial cups, is in implementing those orders. Particularly when it comes to the Internet and of course as Mr. Anand mentioned IPR, speed is of essence so in one case where and this was the situation which we had faced in many instances. This was just one of those. The company is involved in a very sensitive area of the Consulate, it is affiliated with consulate and it is working with them. Every assignment is given out on attender. At least just a week or maybe some times two days before tender. There will be post put up on social media maligning the company so this is just one instance where it was the company associated with the consulate, but this happens across the board, whether it is a manufacturing company or whatever invariably the person who is posting will use anonymous or something equivalent to that. The post goes up. You right to the service provider and they will choose service which are hosted outside India. So you right to the service provider they couldn't get caught. Pardon my language but that's the way, they don't care so they are not even going to respond to your notice to go to court you get your order and you send it to them. The process for sending it, so I am literally jumping to my last slide on this. The process for sending it if you are a private party is through the ministry of home department and they have to receive the order with 12 clear weeks. So even assuming we have received it with 12 weeks to transmit it. In the process if there is delay they will send it right back and say go back to court get your order again and come back with 12 clear weeks, so the letters rotatory and its service by its very nature is time consuming and by the time even services is completed. The reason for moving court is lost. So it is being a nightmare not just an ordinary impediment in terms of enforcing. So I am going to really rush because that's what I was doing I was cutting out a few slide and in trying to streamline it. Now I am going to try to focus on these 3 main aspects. The way I read the topic was to kind of that we were going to be at the end of two days session when we would have discussed specific issues and we were going to come down to a kind of summing up or consolidation of whatever would have been discussed over two days. So these were primary aspects which I wanted to focus on in the process. Now when we talked about electronics evidence I believe Mr Vakul Sharma has substantially covered the basics but I just wanted to put forth some of the concepts that I wanted you need to put before you all for discussion. When we talked about electronics evidence principles are the same. if you look at the whole cyber angle then we come down to first principles and if we look at electronic evidence, if we remove the possibility that technology brings in it all boils down to first principle authenticity, integrity and non-repudiation. These are the three main things we are going to be looking at. Some of the challenges that electronic medium has brought before us we could probably categorize as these principles are the same. if you look at the whole cyber angle then we come down to first principles and if we look at electronic evidence, if we remove the possibility that technology brings in it all boils down to first principles, authenticity, integrity and non-repudiation. These are the three main things we are going to be looking at. Some of the challenges that electronic medium has brought before us we could probably categorize as these. As i was discussing yesterday we have this print out before us. When we look at this paper we know that this has been printed probably yesterday or two days back or something like that. It is new, it is white. When I file this and 20 years back when I look at it I know it is 20 years old because it has gone yellow. If it goes through file may be there will be some left over what are we looking at when we are looking at an electronic evidence. What happened yesterday when I was trying to show a video, it just hung so it was there in one second and next it is gone so this is the split second we are looking at when we are looking at electronic evidence so to that extent yes there is a difference? The second aspect is the author and recipient aspect. We were discussing yesterday about electronic signatures and about how, whatever may be the authenticity that the electronic signature brings to a document it is still going to rely on human usage or human intervention to the extent of who is going to use it and practically we have noticed that the hands with science are no longer attached to the arm which is executing the signature. We have grown up with this and we have slept thinking about this but today when you look at the same sentence it no longer applies because earlier when we wrote this sentence because when we were in Delhi signing a document our arm is no going to go there without us, we are present physically and we say in witness whereof we the undersigned have put our hands to this document. Today when you put an electronic signature your hand does not have to be connected to the electronic signature, however the law says it is presumed to be connected to it. It is for the person who is calming the contrary the proved that the hand was not attached to the electronic signature. This is again one more issue which comes in terms of electronic vs paper document. What is the law on this? There were three aspects which I wanted to cover in terms of electronic signature. The first part is of course all pervasive section 65B and what it holds for us. the second aspect was with respect of the Dharambir case in fact in terms of giving , furnishing documents to the accused and where the pitfalls happened in practical scenario and the third aspect which according to me is the third time bomb waiting to burst which is with respect to electronic evidence. I would like to cover this very quickly I assume that Mr. Anand would be covering the civil aspect of the jurisdiction , so I wanted to touch upon only one aspect of criminal jurisdiction pertaining to the cybercrimes and with that I would be closing on today's session. Now we talked yesterday, there were some basics which I wanted to leave you all with. Because you have already covered some aspects about technology yesterday. We spoke at about the difficulty that the electronic trail leaves but as I mentioned yesterday, the bread crumbs are there everywhere. There is not one situation in the electronic domain where you cannot find the bread crumbs. All you have to do is to look for them and where you would look for it is what I have tried to give a very quick birds eyes view of it when a corporate entity or individual is looking for a trail they would preliminarily rely on the IT audits friends like Murali who come into picture. We are looking at an international intrusion again we have the bread crumb trails. I wanted to give you all a very quick example on this, so I have prepared one document. This is very simple document. Example I want to give of how an email virus email would look and where do you find the bread crumb trait in this kind of an email. I have given four scenario here. The first one is what you have on there I hope this one works today. So you have, ok this doesn't work. You have the original text which is how the email will look. So when you look at this this is about how you would read a header. When you look at this, I you remember I had mentioned you one of the times of email to get is like your Apple ID telling you that it has been access by somebody else somewhere.

So go to this link and verify that this is you who has access it but you can already tell from the email ID itself that it is a fake mail. You would be looking for the path. So when you look at the path, you have the mail id which is not an apple mail ID. It is a beneker.com kind of thing. The second place where you will get an indication of whether this is real or not will be the return mail ID and the headers. Now let's see where this mail has really come from. I go to the next stage of long headers and all of this when you open your computer and you open your mailbox and the actual email you will have what is called as the drop down menu which is right on top. When you go to that you will get all this and I have given you where you need to go also. Go to view then to messages and then the long headers. So when you put it as a long header, y you also get where the return comes. Now sometime they can mark just make it seem like this is a genuine mail but the written part will always show you whether this is a fake email or not and where it is coming from. The next thing you could not look for, this is the full details of the long header. It gives you the entire header of the mail, it will tell you, just to give an example because they made a test case for instance this long header will give you all the details that you need to know. Who has send the mail to whom where which is the recipient host. Recipient host is the server which is receiving the mail and what happened to the mail. Are there any attachments. So these are substantially anything lying with paper, anything can be forged or fabricated .You will have to exercise discretion at the end of the day to see whether this is fabricated or not and if so to what extent. Now there was one more respect I wanted to show. If you look at this time, what does hand indicates here, is that there is actually a hidden link in just a place which is otherwise claiming to be a copyright notice. So when you go there so the whole reason why the mail is formulated the way it is, in case you are the smart person who says oh this is a fake mail, I am not going to do anything with this, but accidentally you end up clicking this you've already given the door way in. You have opened it out because there is a link attach to it. Anywhere you have hand signals, you know that the link is there and link is showing over there, what the link is on top and the last one I have shown you is the rustics which will give you the entire details about the message. What I just mention to you return path delivered to the host, everything is mentioned there. So this example I wanted to rely on to show you where the breadcrumb trail is. Instead of saying it I thought an image.

Justice Murlidhar: I have a practical questions let’s say if this is a matrimonial dispute. We are talking of two individuals. Let us say one spouse says that he has been getting all the emails from the other spouse and let’s say two things. One is that you are able to preserve the mail on your inbox the other is you have deleted it because you're fed up with getting these kinds of mails, so initially you delete these mails. So in these two scenarios how do you take the whole thing to a court and how do you demonstrate to the court because I don't think it is good enough to simply print out this header. It will have to be shown on the screen to the court and how do you explain to the court all of this through that .That is scenario once you have it in your inbox Scenario two, if it gets deleted from your inbox, how do you do that. Then in scenario one can the other party still say no this is not authentic till the server gives the certificate.

Ms. Nappinai : So the last part I wanted to cover the 65 B thing of the proviso which is given to 65B which says that the certificate has to be given by person of authority in charge of the device or the activity , so if you So if you look at Anwar vs basher the court stops with the device. The second party of that, it has missed out which says, or the activity and given the practical implications of going to a Google server to prove every Gmail to my interpretation and I think that would be the only practical solution available. The Reason why they said or the activity has to be interpreter as the activity of printing out the document. Otherwise every time you necessarily have to carry the computer to court. I am going back to you first two queries. The first scenario is where the email is still there now the difficulty we are facing is that 65A and B where intended to be an enabler it was not meant to be a stumbling block it was not meant to say how dare you used electronic medium, we will make sure that you will regret it for the rest of your life. It said please use the electronic medium and we will make it easier for you that was the way it was intended but either due to some, you know, gap between implementation and draftsman ship or because of its interpretation and the way it has evolved 65b has become a stumbling block now and why is that because there are two sets of compliances which we are required to make if I can just quickly jump to the because I can show you where how I could probably explain this. So this is a literal reproduction of the provision but what would help us to go straight to Anwar vs Basheer and its interpretation. Now really speaking out of the five sub clauses which are there in 65B, 2 and 4 are the real relevant ones. Now the Supreme Court has integrated 65B 4. To me compliance of the three precondition set out there in and it says all three conditions have to be complied with. Where what 65B is actually says, if I were to go to the provision, if I can have a look at it. It says any of the three, the word any unfortunately seems to have been missed out. The word any. Now when you look at 65, I can just put it up, because that’s why I reproduce the provisions so that we can have it for reference. So if you look at it, it says any, a certificate doing any of the following, not all of the following. And what is the any that is set out in 65B 4. The first is you are just supposed to identify the record. The second is you have to give particular of the device which was involved in the production of the electronic record. And only the 3rd is to comply with 65b 4(2). But today what we have is, you have to comply with all three. Let's take each scenario. The first scenario which is a simple one is an email. The primary reason why the device was used is because it says, because if you look at 65A and B, it says that it should be the document prepare on a computer or it is a computer output to put it the very simply. Therefore for used to identify that it is in fact a computer output you are supposed to give that identification and the second part. Now when you are talking about her simplicity email or just the Word or Excel document you can prove easily that this is where it came from but what about the third .Now when you talk about the 65 B 2 . This is the complication it leaves you with. The wording used in 65 B 4 is any, what is done by Anwar vs Basheer is that you have to do all three and all three means all of this also. Which says that you must say it is not just computer output but that it was added in the ordinary course of business or activity, that it has not suffered any disruption, if it has suffered that it has not affected the content. The reason I am mentioning this is the second question you raised sir of having deleted it because a deletion is a disruption which affects the contents but where does it affect the content. It's not that because it is deleted it cannot be relied on. I will just explain how. Who gives the certificate that is the real issue? Let us complete this part and then move to the second part. So these are the preconditions which 2 imposes. Actually one good thing that Anwar vs Basheer has done., is it has simplified these two provision in by kind of like listing it so this is literally a verbatim reproduction Anwar vs Basheer. It says, this is what it says it says for 65 B 4 you have to give, the whatever is the relevant part is what I have highlighted there, which is that you must give certificate, describe the manner in which the electronic record was produced, must furnish the particulars of the device evolved in the production and it must comply with 65B 2 an must be signed by person occupying a responsible official position to the relevant device. But if you look at the provision, it goes on to say or relevant activity, that part is missing. Now if I can address your query. When you're talking about,

Participant: What is the citation of Anwar vs Basheer? It is 2014?

Ms Nappinai: Yes 2014, I can give it to you sir. I will just give it offline afterwards. In all fairness to Anwar vs Basheer, they have not discussed this aspect but it could be interpreted that this is the reason why they did it what is that reason, if you look at 65B A and 65B 1, it says, if you have any document, if you want to produce the computer output a printout or CD and all that, it says you have to comply with those conditions set out in 65 B 2. In 65 B , if you look at, to, the beginning, the first line of 65B, that could probably that is why the inconsistency is there between B 2 and B 4. If you look it 65 B 2, the first line, it says

Justice Murlidhar: It shall be the following, not any of the following.

Ms. Nappinai: It says the conditions stipulated by 65A, are set out here under. So that necessarily implies that 65 b 2 are the conditions looked out at 65 A. 65 B a. If you look at the first line in 65 B 2, the conditions referred in sub section 1, so subsection 1 is what I told you, for an electronic record to be to be accepted, it shall deem to be also a document, if the conditions mentioned in this sections are justified in relation to the information. That this condition in this section is qualified in 2, by saying the conditions refer to in sub section 2, in respect of computer output, shall be the following. So therefore Anwar vs Basheer is not wrong technically, it has just mentioned why 2 is necessary. So there is an inconsistency between 2 and 4 which Anwar vs Basheer has not taken into account to qualify or explain but today this is the law and we have to comply.

Justice Murlidhar: No, in cases of private emails. Person occupying important official position,

Ms. Nappinai: To the devise, yes that is the thing. So I had to take a long route to explain your query Sir. I will explain why I took the long route. I will tell you, much larger problem is there. The reason why I pointed out specifically, specifically why each and every condition that is needed is this. The emails are the easiest to prove because I am in charge of my computer, I have either input, and I am the author of the document also probably so I would be able to prove this.

Participant: no no no. I would disagree with you. How do you prove in Gmail?

Ms. Nappinai: No No that is what I am coming to. I'm just coming to that. I am taking it to larger issue and then bringing it back to emails. Let's take the situation of documents form online. I am I cannot for sure certified that this was produced by which device. I cannot say, I can only say is a computer output. I cannot say anything more than that. I cannot see who has created it and in what manner. I cannot say, for instance, he mention Google, so let's take Google or Gmail sir. How I am I going to give certificate saying Google has work without disruption forever. Or that the disruption has not impacted the contents. So if you look it 65B 2 and 4, even if you take it as or 4, the mistake of the draftsmen is they have taken a very myopic view of what is a computer document. If you look at it, there have actually thought about only this document which is like a word document which you prepare on your computer so you can actually talked to every aspect of it. That is why I said sir, I will come to it, at the aspect of email, afterwards because, better to start with the most difficult and then come back to the less difficult one. So let's come to the email part of it. If we are to interpret, 65 B 2, or 4 to say that the certificate is supposed to be from Gmail, nothing will get proven, because look at the quantum of information out there. How are they going to give certificate to each and every litigator across the world? One of the changes that even our neighbours have brought about, Sri Lanka pursuant to the Budapest cybercrime convention compliance, is to remove all impediments with respect to Electronic evidence. They have gone to the other extreme to say that the person who is claiming that something is forged has to prove.US was one of the earliest signatories, they have gone to the other extreme, UK has changed its pace to dilute the conditions, so that is the thing, we have drawn heavily from there. But we have not drawn completely from there and we have not taken into account, different kinds of electronic records.

Justice Murlidhar: We have borrowed 65b from the UK law. UK has repealed it.

Ms. Nappinai: They have changed and they have diluted it. If you kill you period they have revealed that and they have changed it and diluted substantially but we still live with this. So today no electronic record therefore can be accepted. You can change that. Now that's another thing 65B 4 does not say that you have proven the contents. Everything can be tampered with. I am looking for a slide, yes. So I just wanted to show where the presumptions are. Presumptions are for digital signatures or secured electronic signature. 65 B 4 does not say that you have proven the document. It only says that if you give the certificate you can admit the document as with any other document, even this document if IZ give evidence saying that, that is why I said we have to go back to the first principle. If we were to say that we have prepared this tabular column and you have to accept the content, it only means that we have admitted it for further evidence to be given on the authenticity of the evidence. It is more on the authenticity of the document that we are talking about here. So here if we go back to Justice Muralidhar's queries , as far as the email is concerned, yes you have to give with the certificate, but two it does not necessarily mean that it is authentic, the contents. The documents will be taken on record. The parties will still have to prove the contents of the document

Participant: There is a difference between the documents than the contents.

Ms. Nappinai: No No I am talking about, yes, you are right sir but my reading of it is also the authenticity of the document, I will tell you why, what I am taking about is, if you go to 63 and

65 which is what Navjot Sandhu relied on of secondary evidence, what is said is, because it is by a mechanical exercise, therefore there is a presumption of authenticity of a document. So here also if you look at it, if we talk about contents, I would absolutely disagree with you to say that the contents are proven because if I say that so and so killed so and so in my email and I am able to comply either every aspect of 65B 2 and 4 does it mean that it is proven that so and so killed so and so? It cannot be. It only proves that I sent the document. What they mean therefore.

Participant: It will be you making a statement that so and so, it will be a question of assessment of evidence.

Nappinai: I will tell you, the focus there is on the word you. So it only proves the authorship. There the issue which Justice Sachdeva pointed out that it can be tampered with so how are you going to establish that. That is the onus that has been moved on to the respondent, the rebuttal. Therefore the contents, what they are talking about is that this is the fact that this is a genuine document. The same as if a letter were to be accepted because it is an original, they say yes this is the things that it contents but not that the contents are proven. So that distinction which applies to a standard document, applies to an electronic document also. Because anything beyond that would lead to absurdity. The second aspect if I can just move on. I can see that you are not convinced but I would like to take that offline afterwards so that I complete at least today.

Participant: What my brother is asking is the contents of documents and the documents that means two things are to prove.

Nappinai: No, because I said it only leads to the authenticity of the document, and the contents have to be proven. His question was, the wordings used in A is contents, I am saying that what they mean by that is the document per se in terms of who sent it, where do you take it from and all that and not what is mentioned in the text of the document. For instance lets us go even beyond the text, let’s assume it contents an image. You cannot assume that the image is true.

Justice Murlidhar: When we do admission denial, even in regular trial, you always say document admitted not the contents.

Nappinai: Those first principles apply equally, that is why i am saying so when the wording used there is contents, it is about the authenticity of the document not the text images or whatever may be contained in the document, that still has to be proven. If we look at it that way it says the general principle says that a documentary proof will over rule the oral evidence. So to move on sir. One is yes, the email once it complies with it yes it can be accepted. Two it cannot be the only prof of it, you have to prove the contents. Second is a much more interesting twist to the tail of where the email has been deleted. Now there are three aspects which could happen. One is that I deleted from my inbox. In this case I can still access and retrieve it from my server. There are two different kinds of server. IMac will retain it on the server also. So if you have settings to that effect, you will be able to retrieve it from the server. And like he rightly pointed out, the real source where the document is residing is in the server. Technically what is there in your inbox is only a copy. But since it is a copy which has dropped into your machine without human intervention you could claim that to be an original also but otherwise the real document is on the server. So if you have to interpret it as a device then you might as well forget about allowing any electronic record on this medium to be admitted. Because Gmail also, Google server is not going to give you certificate. So we will have to necessarily rely on the second part and interpret the last part of the proviso which says all that you have to say is to the best of my knowledge it is there. So therefore the interpretation i draw even for online documents for instance is that I already know it is a computer output second is I know that from the time I have looked at it, from the time I have taken the print out the computer is working fine, so I only have to give a certificate to the best of my knowledge so i say that to the best of my knowledge this is the device which has produced it. I can identify it through website if not through personal knowledge so I say this is the device which has prepared it, from the time I have seen this document online to the time I have taken the print out it is working fine. To that extent and because of this small qualifier which gives you the leeway to say to the best of my knowledge you can take that liberty because without that you are gone. Because one of the most famous cases is of a wife who sued her husband for divorce and very big alimony because she found his car parked outside his mistress’s house through Google earth. Here we have to follow the technical way then you have lost all electronic document. So if it is on the server you can rely on it. The third level is there are two ways in which it can be deleted from the server, one is when I go there and delete it myself there is another option where you have stopped using your email id for a particular period of time, then the service provider will terminate your email id and all the data will be destroyed so if both have happened then you have lost out then the only other alternative is that you use the receipt of the mail and hope that they have produced it. The third aspect is you have deleted it but the server may have it in which case you will have to right to the service provider. The norm is that will retain it, it used to be 6 months earlier, I don't think that has changed much but very rarely they respond.

When it has been cases of grave violation then the service provider respond altlest to stop certain violations.

Justice Murlidhar: The other thing is timeliness. So suppose you don't realize in that point of time how important the email is and you realize it one year down the line. Suppose they chance upon the crime much later, by then all this has already happened and the server policy is not to retain more than 6 months so that evidence will be lost. That was the other thing.

Ms Nappinai: That was the reason why I put the first slide to show how ephemeral electronic evidence is. There is no alternative but for our legal systems to change its ways to ensure that evidence is collected at the earliest possible time. I had the privilege of being member of team which drafted the commercial courts Acts, I can still call it a privilege going down the line. But when we were looking at it, one of the things we took into account and one of the reason why we added this aspect of proving your document at the earliest point of time when you are filling your plaint or complaint. So that if something were to happen going forward at least at the time when you initiated your action you knew this was the document you had inland and any objections that the other side wanted to raise would happen at first point of time and this was the reason sir why did we put that. There is one more slide because it was looking too small when I clubbed everything together.

Justice Murlidhar: 88A may be relevant.

Ms. Nappinai: 88A is very relevant because of the presumption as to electronic evidence. If we can quickly look at 88A. In fact there are couple of Delhi High Court Judgement which have relied on 88A along with 65 B for certificate. The court may presume. I am going to behave I am in court right now, I will just read it out Sir.

88A. Presumption as to electronic messages:

The Court may presume that an electronic message, forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

Explanation:

For the purposes of this section, the expressions “addressee” and “originator” shall have the same meanings respectively assigned to them in clauses (6) and (za) of sub-section

(1) Of Section 2 of the Information Technology Act, 2000

If you look at it they have tried to look at certain aspects of electronic evidence. What was covered under 65 B if it could be termed as this document, 88A takes care of emails, electronic communications. I can give a fantastic example it in a situation

Where there is a presumption already which is much wider than 88A also. In Bombay we had very interesting case where certain people found a very certain way of taking over a company, what they did was, 3 people apply for digital signature in names of one of the directors of the company. They comply with the KYC norms. Using that electronic signature they filled fabricated minutes of meting as such the current board has been removed and replaced by new board. As simple as that, for electronic evidence where there is only a presumption of authenticity and I think in the technology session yesterday they were mentioning why it is authentic because it captures the day stamped and nothing can be changed there after once electronic signature is applied. There are, by the way, multiple kinds of electronic signatures, if I can just digress a bit here. How many of you use electronic signatures. I want you personally. All of us use electronic signatures. All of you have credit cards, right. There are multiple levels of electronic signatures. My just putting in that email earlier which I was as showing you. I add there regards MS Nappinai that is also an electronic signature. But it is of the lowest category. That is most insecure one. If digital signature of on encrypted signature is supposed to be the highest of those category. This case showed that at the end of the day vulnerabilities are going to be the same, irrespective of the domain. We have to finding the ways how we can address those vulnerabilities. I have skipped a lot of cases but I would like to go back to Dharambir to explain what the other issue that is happening is. I am in real honour to be in the presence of the person who gave us Dharambir. Now Mr. Sharma has already explained you about what Dharambir said. That documents in electronic forms is also an electronic document and therefore user are entitled to copies of it but let me tell you the practical issues what happens in the court. In every criminal case all these hard disks and various computer resources are seized, panchnamas are made. Copies are sent for forensic examination. Forensic report may be given but do you know what happens to the hard disks, how they come in the case? Despite all of this out here. The actual hard disk is submitted to the court, so what problem we have been facing practically is that the court says that that is an article not a document. Because it is the material. The print outs would be a document or if they have relied on it, if there is attachment of CD with report that they provide to you but the contents of the hard disk. Because the actual hard disk is given to the court not the contents of it. There is, for instance we talked about mirror imaging yesterday. So what happens is the mirror image hard drive is submitted as an article before the court. They do not realize that that article contains documents which have to be given to the accused. So this was very minute variation which we have been facing where we have to explain to the court that today it may be an article but tomorrow what happens three years or ten years down the line when prosecution relies on a document which forms part of that article and you say that I have not been furnished. The court says what you were doing for so long.

Justice Murlidhar: Actually we may come to stage, you just give accused the link. The counsel for the accused will be given a link with a password, that's it. You may not even hand over the disk. Because of the volume of the information. You can give in the read only format. Which you cannot download. It is all possible.

Mr. Murlidhar: It is already the case in US and Europe. They use it there All the hard disk you have collected sign out the relevant document and then the other side will read whatever they want. Eventually when the other side wants it, you have to give access. All the things if you want to produce it, it is called production in US terms. You take print outs in A0 size charts and take to court or you access it user and password protected to the court and to the other side also. We have been doing it for 7 years. Otherwise there is no other way.

Ms. Nappinai: But may I raise one question on that.

Justice Murlidhar: And also there is a practical problem. Let's say the electronic evidence is in form of a video clip. You cannot give a print out. The only possibility is that you give link where they can go and watch it, or hear a conversation.

Ms. Nappinai: May I ask one thing, if it is posted on a FTP site or on line or cloud and something and you give a link or something what is going to stop the respondent from saying that it has been tampered. Because that will only add to the complication of the issue then. That is one level of complication which may arise.

Justice Murlidhar: I am also looking at courts of tomorrow asking parties to develop drop boxes, where everybody can use the drop box for the documents including the court and it will be a secure encrypted drop box so that both parties known that this is tamper proof and this is far better way I think of instead of the courts getting into finding servers, store and all that.

Ms. Nappinai: Ujjwal just took Dharambir forward in terms of what is it that has to be given. In fact the situation which Murali was mentioning yesterday. Delhi has definitely being a fore runner in respect of all of this so the football analogy which Murali was mentioning yesterday came up in another case also of just dial which was a civil matter where they wanted to stop the competitor server because mirror imaging had to be done. They approached the Delhi High court saying that no it cannot be done because it takes 3 days for mirror imaging to be completed. There are other practical issues also. I wanted to quickly touch up on. Panchnama, by whatever name it is called in various states. Even today stock witnesses are being used for creating panchnamas, I will not use the word creating, for preparing panchnamas for seizure, even for electronic evidence. Now like he mentioned. Mirror imaging does not happen in 1 minute. You do not go and it does not happen like that. Some of these things take over night. Once the process has been started it just keeps going and two days down the line they would take copies and go. Sometimes the parties themselves submit the copies to the investigating agencies. 90% of seizure are likely to fail because none of the panchnamas are even familiar with what is being done. If you ask them what is the server. So when we talk about best evidence. This is a Madras high court Judgement which In this case a foreigner is murdered in a hotel and the CCTV footage is available in the lobby which is not seized by the police. So the court holds that that was best evidence that should d have been taken. Now when we talk about what happens in seizure and all that, look at how good is best evidence rule really in terms of electronic evidence. 90% of cases are being thrown out on technicalities rather than of reality. Just with Anwar vs Basheer which changed something 10 years down the line but did not put a saving provision. I was told that only in Maharashtra at least 10,000 cases were lost because certificates were not there. One other query that I have come up with is when does the certificate has to be given. Apparently the police are under the misconception that at the time when the document is being seized or submitted, it should be given. 65 B 4 does not say that, it says at the time of giving evidence. So there have been instances of cases being thrown out, the police themselves decide that this is not done so we are not perusing it. So these are all some of the Justice Murlidhar: If they wait till the time of trial or the certificate to be given the person who was in charge is no longer there, either retired , resigned or whatever.

Nappinai: Practically it may be a good idea sir but it cannot be a ground for throwing out the case.

Justice Murlidhar: Also the consciousness, because you will be talking of something that happened two years ago. Or four years ago. So that will lose its authenticity and cross examination will become extremely vulnerable.

Nappinai: Delay is another issue which is affecting corporates and litigants because even 2 years is a long time. Yes nobody wants to do it. And they are spending lot of time. They have to come for briefing advocates for making their affidavit. Then they have to go to court there is no certainty that it would be taken up. So after sometimes, after 2-3 hearings they drop out and compromise cases on this. Another important aspect that I wanted to touch upon is expert opinion. Now 45 was sufficient to cover export opinion for electronics medium because it covered Science as a sub medium, but what has happened with the addition of 45A is that it is only the opinion of the examiner of electronic evidence which is deemed to be an expert evidence with respect to the Electronic medium or electronic records to put it simply. One this examiner of electronic evidence is supposed to be appointed under 79 A of the IT Act and he is of the government appointing. The evidence Act is common to Civil and criminal cases, I mean as basic as that, which the examiners is going to come for a civil matter for that matter in arbitration etc. The reason why this is not come to focus because till date the examiner of electronic evidence is not appointed. There is now a writ petition filed asking for the appointment. Heaven alone knows what will happen to 45 a after his is appointed because there is clearly anon application of mind of the drafts men in adding this without realising that 99% of investigative processes are done till recently even by the government through private agency. So this is one other aspect. That is the equivalent of the government appointee but so there is let’s assume, but how is it going to be possible, Sir look at the volume of... let's assume each state has .I'll explain to you what is happen even with, I will explain to you why I'm telling you this is .Let's assume that the heads of every forensic lab is going to be appointed as the examiner of electronic record that would be the practical solution. The forensic report of pending from Maharashtra at least the logjam that is 3 years, I am telling you this is without the examination to go out to give evidence in civil cases

Participant: Let me tell you as far as Bengal is concerned we are also having backlog. It takes a long time.

Justice Murlidhar: for electronic evidence time is very important because it can detoriate.

Nappinai: and tomorrow we do not know that evidence is going to be there. For instance at the stage of FIR you get to know. Let's take a sample case for instance and say that when the computer was seized incriminating evidence was found on the computer but that evidence cannot be relied by court until the forensic report comes in. Now the forensic report does not come in and charge sheet is filled sometime by the investigating agencies to avoid 167 bail. So what happens with that is ones proceedings have started, the urgency is lost. 3 years down the line you do not know what the condition is going to be. If I were the cross examine that case, all I would have to ask is where was it kept, how was it kept, is it not correct to say that the situation is sufficient to affect the contents. You know all these and then you are done. It is over, that's why every instance with respect electronic evidence technicalities of what you are relying on to avoid

Participant: with judiciary there is a handicap, you have to depend on the agencies. This is the problem with all the legislation. It is not backed up with the support system by the government.

Nappinai: Sir, May I know how long I have or have I already overshot my time. 5 minutes if I may take.

Justice Murlidhar: yes yes you can

Nappinai. Thank you. I will just quickly finish that is why this is the last slide I was putting on evidence part, of what is it that we really have to look out for one is of course authenticity integrity etc., 2nd is preservation. I think yesterday that Technologies mentioned it more than even the lawyers did regarding the chain of custody, protection of the virtual train for an authentication, the paperwork and the eligibility of the persons who are giving evidence. This is something no 1 seems to be taking into account or sometimes they are handicapped from putting the best witness forward also. So the best evidence requires best witnesses to be put up. The reason I wanted to rush is that, there in one more point on jurisdiction which I wanted to touch upon these are of course the general principles which I love to rely on .So this is the essentials of Jurisdiction, created by law and authority used to it. Now what Mr. Anand mentioned very briefly on Banyan Tree. Pragya has done a fantastic job of adding that in the booklet that has been circulated. Very briefly what is it that has been decided on .Again we have Delhi to thank for this .India TV cases of the most amazing is that come across in terms of an analysis on jurisdiction .Now banyan tree just took India TV forward? What happened with Casio was you have now everything on website. Let's take a simple example of a defamation case. You can read and the things that is online at any part of the world. So if you're going to entertain a defamation case what are the grounds on which you will take it up? These are all cases particularly India TV was with respect to trademarks and Banyan Tree I don’t remember what it, it was also Trademark. So in this, yes of course you should know, you should know, yes or yes yes, I am sorry because sometimes we tend to forget you the author is. So what Banyan Tree did was that it clarified the inconsistency between Casio and India TV. I know it was yes yes so thankfully I have put up to say what was great about it.

Mr. Anand: When she kept saying Murali, I thought she is addressing you.

Nappinai: No No, I am so sorry his name is Murali. No no no I am I don't take touch Liberty .I known you for so long I still call you Mr Anand. Right. So in very brief time. Because I have 3 minutes to cover criminal also on this. What it says is a party must have purposefully availed of a particular jurisdiction and the minimum contacts talked about what is the interaction between the user and the webpage owner. And the third aspect which Banyan Tree gave us and I am saying it without thinking into account the author of it is here is that it showed that the interactive part, it is not sufficient merely because it is an interactive website. There has to be a further level of ailment for it to be confer r jurisdiction in a particular Court. Now this is something I'm going to skip through and leave it for offline discussion because this is something I wanted to focus on more. There is a major problem, if you remember Deepak session yesterday, he pointed out a very important aspect, which was inconsistencies within India between a legislations. We have the same problem with criminal jurisdiction. Why do we have a problem because we discussed yesterday that cybercrime is not limited to the information technology Act. It transcends that. The extra territorial jurisdiction given under section 75 given in IT Act is applicable only to the offences under the IT Act. You have other provisions for IPC and you have other provisions which will cover any kind of criminal prosecution. IPC Section 4 was amended to include offences committed outside India which would be available any personal any place without and beyond India committing an offence targeting of computer resource located in India. Now again if I could go back to yesterday's session, we talked about how a computer could either be at target, which is the victim or it could also be the perpetrator, which is the instrument used as a weapon now the wording I do not know whether they have used knowingly or inadvertently but the wording uses targeting a computer resource. So it is an inward flow. To that extent it is very similar to 179 which says where an Act is an offence because of the act and the effective word used there is consequences. You can take the case where either the act was committed or where the consequences ensured. So if the consequences as in the targeting of computer is inside India in case of inconsistency between the two, you can you can take it with 188. Because 188 says, it applies to citizens anywhere, it does not matter. It is technically for an NRI. Citizen who is on the high Seas or elsewhere so that means any NRI would be covered under that and non-citizens only on ships and air crafts registered in India. So what I wanted to give you was a kind of an example and show you how this is going to result in an inconsistency. I am really sorry for the number of slides, I just get carried away. So this is a case study I thought would help us in understanding how the sections are going, the interplay between the section. You have the scenario. This is an actual case which happened in Mumbai .Mumbai Police lost money. How did they lose money? The Debit card was used in zero day attack from Greece. How did the Greek criminals get their information? Skimmers were attached to an ATM machine in Colaba. So every person in Colaba who used it and that ATM was right next to the Colaba police station which is why police used the most and they lost the most. So they go and use it and there data is captured and taken outside, for you to user like I mentioned yesterday am doing a few assumptions you to show how the interplay. Credit card and debit cards are forged and use from all over the country where a target is in India. So right for targeting inside. India. It could also be targeting anywhere but affecting persons in India, so the consequences ensuing here. Now the Greek criminal would be covered under the IT Act and under Section 4 of IPC for forgery and for data theft. Banking fraud would come under general IPCC offences. Now if it is a foreigner you are lying on, then you can sue him in India, only problem is in bringing them here which was supposed to be my next slide of the letters rogatory and extraditions and all that but other than that, why is it that you can take it up here? 188 puts in the limitation saying that you need prior sanction of the government before you initiate action against an NRI. I am putting it very simply or a non-citizen who is on a ship or an aircraft. There is nothing about a person who is not on a ship or aircraft but look at the inconsistency there. The reason I mentioned about the skimmer in India is, there are Indians involved. So I have twisted it little bit to say the assumption I am taking into this is that NRIs are involved. The same offence, the same case just because he is an NRI, you need a sanction under 188 because IPC offences are also included as well as IT Act .Section 75 does not talk about a prior sanction. Now these are all inconsistencies which are likely to come up case by case and until it is resolved it is going to be there in the books. Somewhere some place somebody should have relooked at it. The overriding provision in the IT Act is not going to help us because 188 is not being brought into effect for IT Act offences, it is coming in for the IPC offence, so 81 is really not going to save us there. Letters rogatory I had already mentioned but this is something I want another point out that 166 A says that we will only deal with countries with MLATS, MoUs or agreements or on the basis of reciprocity. We talked about the Transista case yesterday, it doesn't even have to be as tough as that for us to not be able to enforce because we don't have reciprocity then you are out. The difficulties that we face in terms of the difference merely brought about by domain is that it has expanded itself out there. It is a borderless domain but our laws, our functionalities are restricted. We have to find newer methodology to deal with his new age problems. Thank You. I'm sorry it's the last slide where I wanted to say where there is a will there is a way kind of a quote. Which says where an act is conferred jurisdiction it also vests the court with the right to find the solutions so we have to find the solution for it. Thank you.

Justice Murlidhar: I am sure others will have other questions, I just have one practical question from point of the courts. Day in and day out we have people submitting to us, either sim cards or CDs, sometime chip. So how can the court receive it? In Delhi High court typically, on a full stamp paper, a CD will be simply posted with a cello tape and so how does one actually receive it. What is the court supposed to do which it is not doing? It could be happening even in subordinate courts. And these are courts without servers, without basic equipment to receive this evidence and it is highly likely that by the time it mistaken up, either for examination or trial more than 5 years may lapse. So what can the courts do for receiving electronic evidence? 2nd preserving electronic evidence and of course the more serious problem is retrieving it when it comes to trail. So what should be done?

Ms. Nappinai: I would do it from my practical experience. We do not do it the way you were mentioning, of pasting it on the paper. We put in in bubble wrap cover and into a fine.

Justice Murlidhar: So nobody would see it. Today this bubble wrap CD is given, even if it is a blank CD, we do not know.

Ms. Nappinai: What the court is required to do is to verify the contents to see, whether that is what and normally where possible, unless football kind of situation, where it is possible, we also give print out of the content. So all the court have to do is verify before and signs across the envelop to make sure that tomorrow if somebody is opening is there is still a chain of custody showing what was given, when was it verified , when was it reopened and check its contents were accessible or not.

Justice Murlidhar: The court must have a device, on which it can insert this electronic document submitted and which can read it.

Ms. Nappinai: failing which a party would have to provide that. So we also came across this query yesterday sir, what happens when file formats go out of.

Justice Murlidhar: Typically Sir, what happens is you are filling it at the counter, the court does not come in at that stage. It is not that we are taking it and presenting it to the judge so the person seeing it at the filling counter is as good as the court seeing it. So how do we insure that at the time of the filling counter till the time court sees it, it is gain.

Nappinai: It has to be a departmental process.

Mr. Murali: Mr. Anand I would like to jump into this. i propose let us have an electronic evidence receipt counter.

Participant: No we want at the court. He is only checking if the evidence is there.

Justice Murlidhar: Then let's be a nominated officer of the court.

Mr. Anand: Now we have that flexibility, we have an officer whose job is, if anything is filled in the electronic form, verify the contents. He is not going to check the contents but there are contents.

Justice Murlidhar: No Mr. Anand, we have to extend it to the lowest level of magistrates. I am looking at section 200 complaint. Let us say if police refuse to register an FIR. I as a private complainant have an electronic evidence to tender, usually you record my evidence at the stage of tender the complaint itself, so that court must have.

Nappinai: So sometime we have to provide the infrastructure until the infrastructure is available for the court. It is like video conferencing, if the parties is seeking that they want to utile technology they pay for it.

Justice Murlidhar: Will it tamper the document if you open it.

Mr. Murali: No Sir, it is in read only format, we discussed all that yesterday.

Justice Murali: When you tender it, you have to tender it with hash back signature

Nappinai: So whatever is tendered should be ion the encrypted form.

Justice Murlidhar: So first the court official will have to ask the person tendering, is it encrypted in a hash value, otherwise should not even receive it.

Mr. Murali: there must be an inward norms which mandate all this. He opens it checks it, signs it, yes all value.

Nappinai: Procedure in west and Singapore explains what should be done. We should probably have similar process.

(All speaking at once)

Justice Murlidhar: No the worry is, the electronic evidence which is already being tendered and received by the court without realizing what should have happened. So what are we going to do with all that is the big big question mark? We might end up losing lot of evidence because we have not followed this procedure.

Nappinai: In fact what we mean sir is actually practice directions. The Concept of Practice directions has been introduced first time by the commercial courts Act. What we mean is practice direction one for how do you receive electronic evidence, two how do you store it and the chain of custody that is why I put a thing about preservation. But there is another aspect also. Even 65 B certificate, everybody is unsure about whether it is supposed to be as an affidavit because section only says it. So is it sufficient if it is signed by the author or does it have to be in the form of the affidavit.

Mr. Anand: but these gaps are always filled up by good practices.

Nappinai: No those good practices are what we set out as practice.

Justice Murlidhar: I have another question here. So let us say you just preserve it after playing it in a device, you receive it in the court. You have to have certain temperature control. But let us day there is an earth quake and the entire building is destroyed.

Mr. Murlidhar: that is why I said sir, when case comes to court, the evidence should be loaded in the courts data centre whereby you distribute all evidence to all parties, whoever is mentioned in the petition. Then you can also give access to the files electronically to all the parties and have a backup technology. It is not at one place. It may look a very grand plan of things but it could be state wise effort or district wise effort.

Justice Murlidhar: We are looking at every court in the country. It is a massive kind of infrastructure.

Mr. Anand: there is an international body, opus magnum. Whatever electronic document you want to file, they will store it and they will give you deals and they will retain completely in their custody, confidential and completely protected.

Nappinai: We now have Digi locker also, which is India equivalent but the difficulty is everybody is not versed.

Justice Murlidhar: But how does it answer somebody saying that i want to test the device, which produced this electronic evidence. Somebody says this is a video clip taken on a mobile phone, I want to see the mobile phone. Taken on a digital camera, i want to see the camera. So how do you answer that query?

Mr. Anand: that camera or device should definitely be available at the time of the trial.

Justice Murlidhar: So that is the other requirement even when you receive the court cannot vouch for. The court is simply received the output, it has not got the device.

Nappinai: When it comes to electronic evidence, any process of verification has to happen at the earliest point of time, including by the defence in a criminal case. If they want to verify the original or put something at the desk, their application have to be at the earliest point of time.

Participant: Let us talk about civil procedure code. They have to follow the process given by the CPC.

Nappinai: Even then you have a process for admission and denial or even for inspection and discovery at the earliest point of time. With your plaint if you are relying on all of your electronic evidence and the other side can ask for discovery at that stage. they do not have to wait for completion of pleadings for completing discovery, if discovery has been completed at that point of time and recorded which is what is done in all criminal proceeding then the respondents cannot say, i forgot to take this at that point of time but now I want. So that is something that has to come into practice. Sorry sir, just to complete that, in the commercial courts act we have included that process which is the reason why we added this because in today's world literally every document is an electronic document. Sir Sorry. There is a presumption for electronic document which is 5 year which is similar for document 30 years old.

Justice Murlidhar: We can request Mr. Vakul Sharma to come in and talk to us about requirements of electronic evidence.

Mr. Sharma: I am thankful to Mam that she has finished my presentation also. Hahaha. I will just see what more do I have to say. Just to look from the point of view of preservation, most of the states have got their state data centres and they have got huge capacities. So if state data centres can be used for storing of such kind of electronic evidence which are in the process of being tendered before the court and most of the state data centres, Karnataka has got three such large data centres. They have not one but three. So these are the kinds of, let us say things, that can be used. Coming back to my presentation on electronic evidence.

Justice Murlidhar: There are one or two aspects which we have not covered, if you can touch a bit. How do you prove a CCTV footage? The other is how do you prove a tapped mobile conversation.

Mr. Sharma: I will first answer the CCTV. In most of the cases the CCTV footage is in a very granular manner it is a grainy picture, and once you are looking into a grainy picture, the persons face may not come out as a clear picture of an accused person. So the first thing that has to be seen is the record retention policy of the place where such CCTV has been installed. Because I have seen once it has been running for many many months, what is going to happen is one image is being imposed by another image? So one thing that has to be seen is what our record retention policy is. Are they maintaining any such blocks, CCTV blocks of previous months or any such kind of kinds? So maintenance of blocks of the secondary requirement. Third is, which is very important is, CCTV is link to direct electricity line or not. Whether there is a backup, electricity back up in that particular building or not. In case CCTV has been switched off then there will not be any recording and there have been cases where electricity has been switched off after office hours. So let us say these are certain parameters which have to be taken into consideration. Number two, regarding the grainy picture, there are certain software which are available which can clean a picture Upto certain extent. But there cannot be, let u say large scale thing but yes they can be cleaned. Number three, whether that CCTV is having, some sort of time or date stamping or not. Whether at time date stamping that comes on the screen is there or not, it is another crucial aspect to be looked on. Now from point of view of the. Sir, what was your second question.

Justice Murlidhar: How do you prove CCTV footage?

Mr. Sharma: CCTV footage, the point is, is it a computer output? The first thing is this? If it is a computer output the section 65B certificate. Most of the cases CCTV footage are being stored in a hard disk , whether that hard disk is apart of computer system or a computer resource, that thing has to be seen, only then section 65 B certificate will come into play. Basically we have to look from the point of view of that whatever the evidence that has been tendered before the court just relying on the CCTV may not do good, it is one part of the puzzle so that has to be seen but that should not be seen in complete isolation. One things which has to be seen is when I am looking into a CCTV footage you can go by frame by frame advance. You can also watch it with slight, let us say increased speed. There is a possibility that if there are gaps, you may be able to find when you slightly increased the speed. If I am going by a frame by frame you just look into the evidence part of it. There is a possibility that i might miss palace where some cut has been made, or some insertion has been incorporated. So it is better to see frame by frame advance. It is also good to see slightly increased speed which is beyond the normal speed just to have a different perspective. So I am saying it from the point of view of, to have a different perspective.

Mr. Deepak: There is another thing done in CCTV these days sir, they have multiple cameras so that people can use multiple images, so that people can see multiple images with the same time stamping and then try to recreates something which is like a three D model and that will also be one possibility. So they could be superimposed to create that. Second this is, what is done in terms of enhancing the picture quality, using different contrasts etc. but that is just a way of saying that you have manipulated the original image.

Mr. Sharma: No the point is, how the integrity is lost. You are seeing the same image, you are just putting a contrast or you are just putting certain filters. I mean you are not changing the content of it. The image will remain that image only. That person will not change. The person or his appearance will not change. The personal appearance will remain the same, you are just trying to polish the image. You are not altering the content.

Mr. Murali: It is the transient metadata which you are just altering. It is not tampering. It does not change the contents. To add one more things, all these computers of their own. All recording devices also use their own computers, just they are modified in different ways to record. At the side there is a mother board, which is a normal mother board, it is with a video accelerator. Mr. Patil: My experience when I was in system was that many times when times when we would seize CCTV, the time span for CCTV was different than the actual time. And we have observed that between same CCTV footage of the same incident, sometime the time difference would be of one hour but actually they are representing the same incident.

Participant: That is because we are getting carried away with this time stamp. First of all this word time stamp connotes someone entering the time. If data is entered one hour slow or one hour fast then the time stamp will show, not the actual time but the time as entered by the person who started the CCTV or the data.

Justice Murlidhar: Then the extra burden to show that an error was committed at the time of entering the time and date, that would be an extra burden.

Mr. Patil: I have two questions. One is about seizure of camera. When we are going to seize CCTV is it necessary to seize the camera because the question was specifically asked to be my commissioner at Hyderabad because these days we are acting as adviser to CCTV. The question was if we end up submitting the camera may be after 10 year they will not give me camera....hahaha. We are submitting in court of law, who will provide 65 B certificate.

Mr. Sharma: Ok so the point is, every The question was if we end up submitting the camera may be after 10 year they will not give me camera....hahhaha.We are submitting in court of law, who will provide 65 B certificate.

Mr. Sharma: Ok so the point is, every device has a product key number which is unique to itself, so there is no need to submit the entire computer system along with the CCTV like that. If you can note down the product key number and keep on mentioning it in whatever document you are going to prepare then yes that would suffice, number one. Number two, you can also create a digital photograph with in that product key, and you should have some sort of image identification that this was a CCTV that we have been using. This is one way of looking into the things because beneath that product key, you will have a bar code. That bar code will be a unique to that particular product. Third thing you have to note down is the make of that CCTV because these three things will identify your device from all other such devices.

Justice Murlidhar: No you have to preserve that device because anyone can ask for inspection of the device. That is the flip side of it, because of the slow process of court trial you have to end up preserving it. The whole point is that the device itself is a computer. Whenever you replace it, I am not saying that you have to take it off. You have to offer it for inspection. Someone will have to come and inspect it. You cannot produce it in court

Mr. Sharma: Having a product key with a bar code and a photograph of it will be let us say, one way of satisfying the court. Now the point is, I am looking into certain decided cases it will be beneficial from the point of view of evidentiary value before the courts. This was the case where the court has said that the CD contain the conservation is primarily a direct evidence admissible as what has been said and picked up by the record. It has to be proved that same has been prepared and preserved safely by authority.

Justice Murlidhar: Mr. Sharma I have a slight...In fact when I read this I had a doubt. If CD was part of the recorder itself then the CD would be primary evidence. If the CD was merely containing a copy of the contents of the recorder the CD cannot be the primary evidence. So I had this slight

Mr. Sharma: CD cannot be primary evidence but digital recorder can be primary evidence.

Justice Murlidhar: Yes correct, because that is a document.

Mr. Sharma: But Sir the point is in a digital recorder whether certain device was fit in to record it, because if that digital recorder because if I am looking in a digital camera. In a digital camera, the primary recording device will be a memory card, where all the digital photographs have been recorded. So if that recorder will have...

Justice Murlidhar: You see one is taking the memory card as it was there in the camera that can be called primary evidence. But if you want to make a copy of it and transfer it in another media then it cannot be any more a primary evidence.

Ms. Nappinai: you don't need 65B for primary evidence. That is the point.

Mr. Sharma: this is a case.

Ms Nappinai: you don't need 65B for primary evidence.

Justice Murlidhar: Yes yes, you drop the mobile phone itself. That mobile phone containing the original recording does not need 65 B. All you need to make sure is it works, whenever you want to activate it. Hahaha

Participant: Sir, if you are cloning it and preserving it...

Justice Murlidhar: Then you need 65 B.

Ms. Nappinai: Even the mirror image without any change in the hash value, it still need 65 B

Mr. Sharma: This is one case which I would like that because this case talks about, from the point of view of what is the standard of proof. This is related to hate speech during an election campaign. The court came out with a view that when it is from the point of view of electronic evidence then more accurate and stringent compared to other documentary evidence rule should be taken into consideration. So the court has laid down more accurate and stringent rule for electronic evidence appreciation. So this is one case.

Participant: What does it mean by the phrase accurate and stringent because all electronic evidence would be necessarily be accurate?

Mr. Sharma: No No no it is not so.

Justice Murlidhar: Since it is vulnerable to being tampered. Which is why they put higher degree of proof.

Mr. Sharma: So it is at the highest pedestal that the court has put. More accurate and stringent test.

Participant: Something captured on a CD, either it has to be accurate or it is no evidence. It is nothing. So what is the word more accurate?

Justice Murlidhar: It is like standard of proof. It is your satisfaction as a judicial officer what you ask to say that this is authentic. To be satisfied of the authenticity.

Mr. Sharma: In this case, there was an interview, there was certain incident which led to this particular case. So the court asked for the original recordings, original recordings were again supplied in CD form because the recording was being done by a let us say TV camera. So from TV camera that spool, in fact in this particular case that entire spool was taken and that entire spool was shown. Only then court came to conclusion that something wrong has been done. So the point is it was the original CD here means that spool from that camera, not the Cd. This is case I have still not able to grasp. This was a case about, which is known as BMW case also.

String Operation was there. By mistake NDTV formatted the original tapes. They subtitled before the court that we have formatted the original tapes but we are going to put before the court, the tapes which we have been showing to general public. Would it suffice? They admitted before the court that the originals have been formatted. But yes they have the footage and this is what they have broadcasted day in and day out. Now in this particular case, the court came with the view that, in the absence of original recording like negative of a photograph, reliance may be placed on positives. i think it is taking a leap of faith. I should say, judicial leap pf faith and in fact this particular view was challenged before the Supreme Court also. But I mean, this particular sentence prevailed. I mean I am still grappling with this that, this negative of photograph. So with a single sweep, I mean that is even the absence of negative was not considered.

Justice Murlidhar: I think just to conceptually understand it, Let us say, you are using actual film and you have raw footage which you edit to make the final output and then you say that I have somehow destroyed the raw footage, what I now have is just the edited footage and this edited footage should be treated as the original. So that is the difficulty here. We don't know how it has been edited, what has been left out. You don't know that and you are asking the court to consider it as the original.

Mr. Sharma: And from the defence point, it was pointed out that the narration has certain jerks and it was pointed out that this jerks means that the video footage has been sliced. But the court said nothing doing. I would request it is an amazing judgement to follow because these things was then followed in this case. Participant: But why was it suo moto.

Justice Murlidhar: Yes it did because court took it in its own motion in issuing contempt notices to Mr. R.K Anand. It was a programme telecast on the television and then the court took cognizance. The Delhi High Court Judgement is reported in DLT. Here it is not given yes.

Participant: Just you go back to the slide.

Mr. Sharma: I will send across to you, I must be having it. I will send across to you sir.

Participant: What do you want?

Participant: The DLT reference.

Participant: I will just see. You were asking for that Anwar vs Basheer that is 2014 10 SCC 473.

Nappinai: If you put the writ petition in Indian kanoon you can get the actual judgement.

Justice Murlidhar: technologically I just wanted to know, like you say 8 layers and whatever. When it comes to video recording, I don't think you can reconstruct. Can you, is it possible to reconstruct if you erase a video recording from a digital camera, and is it possible to reconstruct what you erased.

Mr. Murali: If you are saying digital camera then it is HD card or flash card, your video is just a data file. It is not a video file, a data file is a data file, and all the things which apply to text file will apply to a video file.

Justice Murlidhar: So you can reconstruct.

Mr. Murali: Ya, but beyond a point, video would be much hard to comprehend. Video bits and bits just can’t make sense.

Justice Murlidhar: Just on this NDTV example, let us say they said we don't have raw footage, we deleted or erased. You cannot reconstruct the raw footage? Can you?

Mr. Murali: My impression of the NDTV case was, these were the old video tapes, analogue tapes, they had not moved to hard disks and HD cards. Now they have. So they were old tapes with bigger width so it was totally different. There were analogue images not digital images.

Justice Murlidhar: So they could not have been reconstructed. So then all the more while it becomes problematic.

Mr. Sharma: These are the two cases where emails exchanged between the parties were accepted by the courts, why because both the parties in their pleadings relied on same set of mails. So here the court did not ask whether the mails were put with the help of a digital signature or not. Because in pleadings the parties have admitted that they have sent, they have received the same set of mails and infact Supreme Court had quoted verbatim from the mails, emails, exchanged between the parties. So this is one significance case, Trimax International. It is a 2010 3 SCC 1. There is Shakti Bhog foods limited vs kola shipping limited 200 2 SCC

134. In the first session we had talked about the role of IP address, this is a case where sanjay Kumar kedia was accused of having online pharmacy selling psychotropic drugs, he said no he was not involved but the IP address which was captured that IP address belonged to his office location. That was the only piece of evidence that all these sites have been hosted from that particular location which is the location of his office also. Now this is the case, it still; remains the first case in which Supreme Court in 2007 appreciated the value of IP address. This is a case about matrimonial dispute husband and wife they have Facebook posting, email exchanges, a divorce decree was granted based on the evidence tendered by both husband and wife which was available on their respective Facebook pages so the court took cognizance of all such materials and a divorce decree was granted. It is by Punjab and Haryana High court. This we have already discussed so I will skip. In fact IMEI number is a unique number it is 15 digit number, it is unique to every mobile phone, so these are the cases where, let us say, IMEI number was recognized and let us say the prosecution case was taken to its conclusion.

Participant: how to handle case where there is a fake IMEI number, the Chinese phones now come with.

Mr. Sharma: the point is, then it is impossible because 15 digits, depart of telecommunication in 2010 came out with a notification that numbers which are having a fake iMEI numbers or which are not given exhibiting IMEI number should not be registered. So what is happening is now the onus is on the service provider, since they are monitoring the traffic, if they come across any number which is fake, because IMEI number is given in kind of bunches so if they come out with number which they feel is fake, they have what is known as a white list, the onus is on to them to block that particular phone at that point of time. Because they are the only set of individuals who can safe guard these kind of things.

Ms. Nappinai: In fact in this Gajraj case there was an error in the IMEI number which was reported, the last two digits there was an error, and despite of that the court looked into the circumstances. Invariably in all decisions there will be a little online and offline evidences which is relied on to overcome these problems.

Mr. Sharma: I think this will answer your query.

Mr. Sachin: Sir I have a question. In cards have unique IMEI numbers, in fact sim card is cloned so how that evidence will be appreciable in court of law.

Mr. Sharma: If it is cloned means it can be used because if it is perfect clone and it becomes rather very difficult because if it is a perfect clone which it is then it becomes extremely difficult unless and until because if I am not mistaken all these fake sims are being produced in time . What is happening is that law enforcement agencies they can still look from point of view of that number. and from that number they can contact that manufacturing company, that is it or its authentication can be done by that manufacture for example every device let us say a computational device has its unique mac id which is also machine id likewise from that IMSI number that manufacturer can be located and that will provide the answer.

Participant: I just have a Philips where we go to manufacturers they gave us clear certificates that these are not ours, then the opposite parties has produced certificates of the same people saying that these are theirs...hahaha and the other difficulty of tomorrow would be nation states that regions and others that are not recognized, if manufacturer is based there, what one has to do?

Mr. Sharma: Sir, the thing is yes, it is a difficulty because what is being refereed is there is a wafer chip technology which is there and in fact to set up a plant of this nature it is a huge capital intensive and technology intensive. Cloning may not be technology intensive, cloning may not be but to set up a plant from scratch, it is technology and capital intensive. Sir the issue that you have asked, does it answer.

Justice Murlidhar: Ya, in this case that was not proved but how do you actually go about proving is a question because you have tape recording evidence, you have the Ram Singh case, very detailed set of instructions but can be ipso facto apply that to electronic recording of conversation.

Mr. Sharma: If I am not mistaken, there are voice recorders and a voice analysers. Those voice analysers, if the person permits or gives his voice sample then the voice can be analysed and whatever that sting tape that has been made there could be comparison. I can give you one example, a facial match if there is facial match of two photographs, there are 20,000 points in the face where toll mapping will be done and there will be software which is going to perform this task and say yes it is absolute match or it will say perfect say or they will also say if it is 90% match. But in a voice kind of thing, if a voice sample has been given and the voice that has been recorded , if there are means to know that whether it is parity in both the actual recording an the voice sample.

Justice Murlidhar: But let us say, either the person is not around or refuses to give his voice sample. Then how do you authenticate the voice.

Participant: or if he had feats and his face map changes

Justice Murlidhar: or he has got a sore throat

Mr. Sharma: Sore throat does not change it, there is not a problem and face contours, it is 20,000 points, it is not a single point, so the point is the problem will come when the person will say I will not give my voice sample, you may draw any adverse inference but if a voice sample is given then yes the voice spectrography can determine that the voice belongs to this person or not and with a great accuracy. Helium effect will taper off within 5 minutes.

Justice Murlidhar: In another context what happened was, we come to the accused at a much later stage, when you actually file a charge sheet or whatever but at the stage of investigation, you suspect that this is the voice of somebody else, of the person you are looking for, now under the Ram Singh test, the person listening to the conversation, should be aware of the voice of the person, whose voice he is comparing with. That is the difficult part. I don't know how many would know how Dawood Ibrahim sounds or something. You should be aware of this. Somebody should tell me this is the normal voice of Dawood Ibrahim, then when I am listing to a conversation, I can compare.

Mr. Sharma: Sir, there is one thing more, there are application which can change my voice. If my voice is tapped and I am aware of it, then applications are, I mean they will change my entire vocal cord, my intonation, every word, pronunciation part can be changed.

Justice Murlidhar: Even though, this brings back to the content thing. Even though he gives a 65 B certificate, saying I am the person who recorded this conversation, he cannot vouch for the fact that this voice belongs to the accused unless the accused gives his voice sample and the experts compares that.

Ms. Nappinai: So one thing I wanted to add on the earlier part about cloning, it is not about how you clone, you can clone on a machine. For instance you now have the Samsung phones where if I take this phone, insert the chip and it has clones it and I give back the chip to them and I can start making or receiving calls, so I would suggest that we should go back to 1st principles in terms of including that also. Take the other instances, like if call has come from

Kolkata and the person is sitting in Bhopal and he can prove through an alibi that I was in Bhopal. So it cannot be only electronic evidence.

Participant: One question I wanted to ask here, In case of signatures, we have section 74 but that kind of provision is not available is not available for courts to exercise jurisdiction, when it comes to electronic evidence. If the person concerned, if his voice sample is not available then what do you do with that piece of evidence. Secondly it has to be the certification of the IO in the first case and the IO is not an expert he does not have the idea what actually it is.

Mr. Sharma: And Sir, just to add one point here, most of the latest devices there are no forensic tools available to get that data that is stored inside that device. We are still grappling with let us say I phone 5, I phone 6 because and their manufacturer blame that yes we have made a device which is beyond the reach of any government or any forensic laboratories, so I mean these are the added difficulties which are being added with the passage of time.

Justice Murlidhar: What is this Faraday bag which they talk about?

Mr. Sharma: Faraday bag in fact it is a device, a cage blocking radiations.

Justice Murlidhar: see what they say, what I heard was there are devices where even if I give miss call to that phone, it can wipe out entire data in that phone. So what investigators in the US do is, particular with drug dealers. When they seize the mobile phone, they put into this Faraday Cage.

Mr. Murali: This is standard forensic procedure, when we receive a phone, we put in Faraday bag.

Justice Murlidhar: to protect the data in that.

Mr. Nair: Disconnected from the world.

Mr. Sachin: and if you don't have Faraday bag you can probably use aluminium foils also.

Mr. Patil: We are planning to discuss that today in our mobile forensic presentation, so we will deal with it then.

Mr. Sharma: Sir, this is the latest case, Shamsher Singh vs state of Haryana, just in 2015, where the courts have said that a compact disc is also a document form the point of view of 294(1) of CrPC. So that means that if I think this answers your question that if I appear before you and ask you that yes this should be taken into an evidence by this court, I move an application. I believe that the application may be accepted under 294(1) CrPC. So and the application should also say that this device should be examined by the forensic lab. Because I mean I have a right let us say, to exhibit as a accused or as a prosecutor to exhibit any such document. What i have done is, as mam has done, I have italicised some parts and underlined certain portions. Admissibility of electronic records produced by a computer shall be deemed also to be a document, information and computer in question shall be admissible in any proceedings without further proof of production of the evidence. This is 65 B 1 then it talks about certain conditions. Now what is a computer output, a printout could be a computer output, a Cd could be a computer output. So again there are lawful control, information received was regularly fed into the computer in the ordinary course of said activity.

Participant: Can I just, there was a question, very important question about cloned sim card but cloning is not possible without a computer. We will have to use the computer and the technology which drives that computer which has a software which allows to work.

Justice Murlidhar: Yes, it is also 65 B. Correct.

Mr. Sharma: The input equals to the output. If I am looking at very simplistic interpretation here, the input equals to the output, now if I am looking into this section 65 B, the lain reading of section 65 B is, it simply says that it is not meant for users like you and I . It is meant for the intermediaries, it is meant for the banks or any such large companies, but with the passage of time in the last 15 years, it has been mandatory who so ever is putting electronic records in form of print out before the courts. So if it is a LAN or WAN working or 165B it will suffice with all computers, all interconnected computers. Certificate signed by persons, now since mam has already talked about this, so what is the logic, what is the legal logic behind this section 65 B, step by step process to identify whether the computer in question, has properly proceed stored and reproduced whatever information it is receiving. So we have to see section 65 B from the point of view of this logical conclusion. Again just to highlight the conditions. Computer was used regularly, person having a lawful control, regularly fed in the ordinary course, must have been operating properly in the ordinary course of such activity. A person occupying a responsible official position in relation to the operation of the relevant device. So we are looking from the point of view of not a legal person, not a legal manager but a person in relation to the operation of the relevant device. And what he has to do, identifying the electronic record, giving such particulars of any device involved in the process. Point No B has never been followed, pick up section 65 B, there is no mention of which device, device having what kind of operating system. So and I do not know, they have been never challenged before the court of law. Why such technical details are not being mentioned in the law. In a cross, the first question would be, what the operating system was.

Justice Murlidhar: Where it takes most is the mobile service providers and giving certificates about call detail records, they are supposed to give details of the tower and this will never be satisfactory.

Mr. Sharma: For the first time this was mentioned in State vs Mohammad Afzal.

Mr. Sachin: I have one question. There is a case where we have to submit some email, so do I have to also produce the source where that email has been sourced.

Mr. Sharma: Section 65 B, that condition which i have just shown to you, you will have to mention A, B, C, D, E like that and that would be section 65 B along with the print outs.

Justice Murlidhar: No No but his point is, how he can talk of gmails server.

Ms. Nappinai: Not documentation, you have to make a statement.

Mr. Sharma: just a simple statement about that 1, 2, 3, 4

Mr. Sachin: Server has been migrated during the entire thing.

Ms. Nappinai: and that the migration has not affected the computer system.

Ms. Sharma: Interesting case, the bank admitted that there was a malfunctioning of ATM machines and yet it insisted giving section 65 B certificate, the court said once it is admitted by you that the computer was not working properly then no need of section 65. It is question whether it is a primary evidence or secondary evidence. In fact this question had troubled the Supreme Court the most and in fact in Navjot Sandhu's case, the issue before the court was that the conversation between the individuals they were not supported by a section 65 B certificate, so the defence argument was that under the circumstances these transcripts should not be seen of having any evidential value

Justice Murlidhar: Was it transcripts or CDRs.

Mr. Sharma: CDRs. in way that there were transcripts involved also there. So the court took a view that irrespective of the compliance with the requirement of section 65 B, there is no bar in adducing secondary evidence under the other provision of evidence Act, namely section 63 and 65. So in a way it nullified section 65B.

Participant: No No, not nullified. Section 65 B is not nullified by this.

Justice Murlidhar: There is no certificate under 65 b.

Ms. Nappinai: 65 B 4 is optional.

Justice Murlidhar: Actually what happened was, some other persons stepped into the box, responsible officials of the company stepped into the box and identified the signature of the person who had signed on these certificate. They were not strictly certificates they were only printouts of the CDRs, with the stamp of the company and signature. The person who signed himself did not get into the box, some other responsible officials came in and said I recognize the signature of this official, so this was secondary evidence because this was leading secondary evidence, in relation to a certificate issued by a person, so that subsequently in Anwar they said, could not have been done. The whole thing is because you are not able to bring the whole server to the court, 65 B is an exception to the rule of producing the document itself. So if it is an exception, you cannot have secondary evidence for that exception that is what Anwar is telling you.'

Ms. Nappinai: What he is trying to say is in Navjot Sandhu they said you can rely on secondary evidence, which was overruled.

Justice Murlidhar: this decision says you can but this is what is over ruled.

Mr. Sharma: Now Anwar vs Basheer, just pointing out, now one departure that Anwar vs Basheer has made from the point of view of, this judgement has included media storage devices also. If we look into section 65A, it is purely from the point of view of computers. If we see, they have said, most importantly, such certificates must accompany the electronic record like computer print outs, Compact disks, video compact disks, pen drive, etc. So I feel there is a departure from the well laid down principle of section 65 B. Now the court is also including the media storage devices, under the ambit of section 65 B, which was not the case before. SO they have enlarged the scope of section 65 B. The point is, why I am saying this is, Video compact disk, can be created minus computers also. It is a storage device.

Justice Murlidhar: No No, as long as it contains a document which is output of a computer.

Mr. Sharma: It may not be output of a computer.

Justice Murlidhar: No that is what it means, in this context it can only mean that.

Mr. Sharma: i will just give you the answer. Marriage ceremonies, video cameras, VCDs are been made, that VCD or a video camera cannot be called as a computer under section 2 (1) i of the IT Act. So the point is, the VCD is an output but is it a output of a computer.

Justice Murlidhar: yes

Ms. Nappinai: but it is also a copy made using a computer. If I just read out 65 b, it says what a computer output any information contained is in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer.

Mr. Sharma: It is being qualified by a word being produced by a computer.

Justice Murlidhar: that is an output.

Ms. Nappinai: The reason is VCD is an output of a computer. VCR would not be a computer but VCD is a computer. Pen Drive is also the same. It is created by a computer because you have to transcript through a computer.

Mr. Sharma: So just to summarise this, an electronic record by way of secondary evidence shall not be admitted in evidence unless the requirements under section 65 B are satisfied. Thus in the case of CD, VCD the moment I am talking about chip, chip is not defined, but the technical definition of a chip is there. So my view is that the storage media has been specifically covered by Anwar vs Basheer.

Justice Murlidhar: Yes so along as the media contains output of the computer. Mr. Sharma we have got a lunch call.

Participant: Unless you are giving us a cyber lunch....hahaha

Justice Murlidhar: Sent to your email accounts...hahaha.

Mr. Sharma: this is the last slide. three tests, the document in question is an electronic record, it is produced by a computer and accompanied by a certificate fulfilling the conditions as laid down in section 65 B so this could be a three prompt test from the point of view of admissibility of electronic record before the court of law.

Justice Muralidhar: And this is only admissibility, it is not proof.

Mr. Sharma: yes, it is not at all a proof. Thank you very much. Sir just one last slide...hahaha...section 79 A, till now only army forensic labs have been granted sanction under 79A...only this army labs, the point is that the FSL or CFSLs, they will be granted this kind of tag the entire lab not any individual person, once they have got this tag, section 79 will come into picture. That is it.

Mr. patil: there is one development regarding 79 A, that there is a mandate given by central government to computer emergency response team and CERT is preparing some guidelines and they are going to circulate to the states and they are going to certify state laboratories, police laboratories as certified laboratories.

Participant: Every state not only has CFL but there is also a forensic lab.

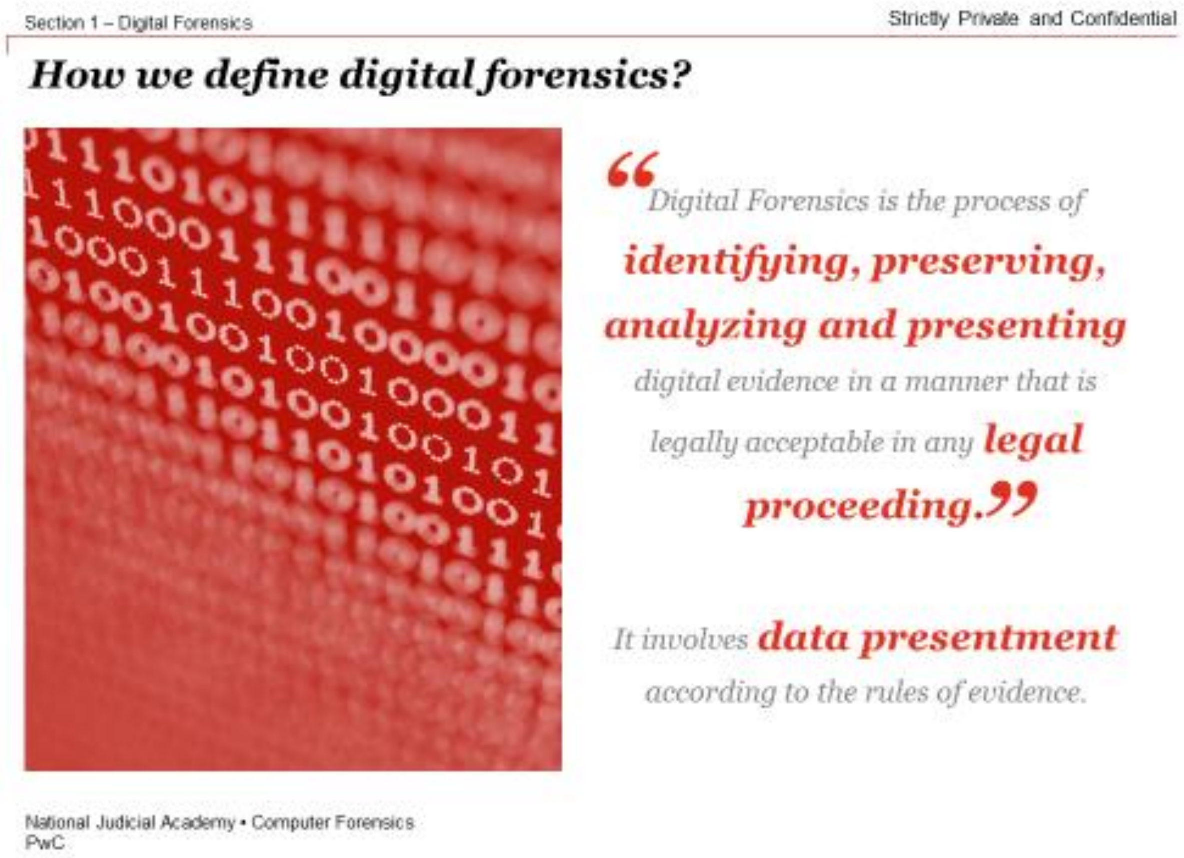
Thank you very much, so 2 o'clock, ok 2:30.

Session 8

Mr. Sachin: Should we start

Justice Muralidhar: Yes yes

Mr. Sachin: So those who were not here yesterday i would just like to introduce myself. My name is Sachin Yadav. I am part of Price water coopers, in their Mumbai office, primarily focussing on the forensic technology, forensic investigation. That is my brief introduction. Yesterday we saw some practical sessions, some demo as to how imaging was don, how hash value is calculated, and so and so. Today we are just going to talk about little bit in details what are analysis one can expect from a forensic experts. Rights. O this is the brief agenda I have just put up for this session. I am not sure whether we will cover all this because I am sure that discussion will go and go and finally we will not be able to cover all this but this is broad agenda. We are going to talk about DNA forensic, the source of information, chain of custody, how the forensic image will look like, authentication kaise hota hai etc. We will also dwell deep on analysis of data, so what kind of analysis we can do within the computers and within the mobile phones. Mobile phones we are going to show in the practical session, how mobile phone is images, what information it captured under mobile imaging. Then we will touch upon briefly upon electronic discovery. Just in previous session we talked about discovery of data, so we are going to tell you how that entire discovery framework works. So we will have very brief slides on those discovery process. So how do you define computer forensic. SO if you see the definition



Section 1 – Digital Forensics

Strictly Private and Confidential

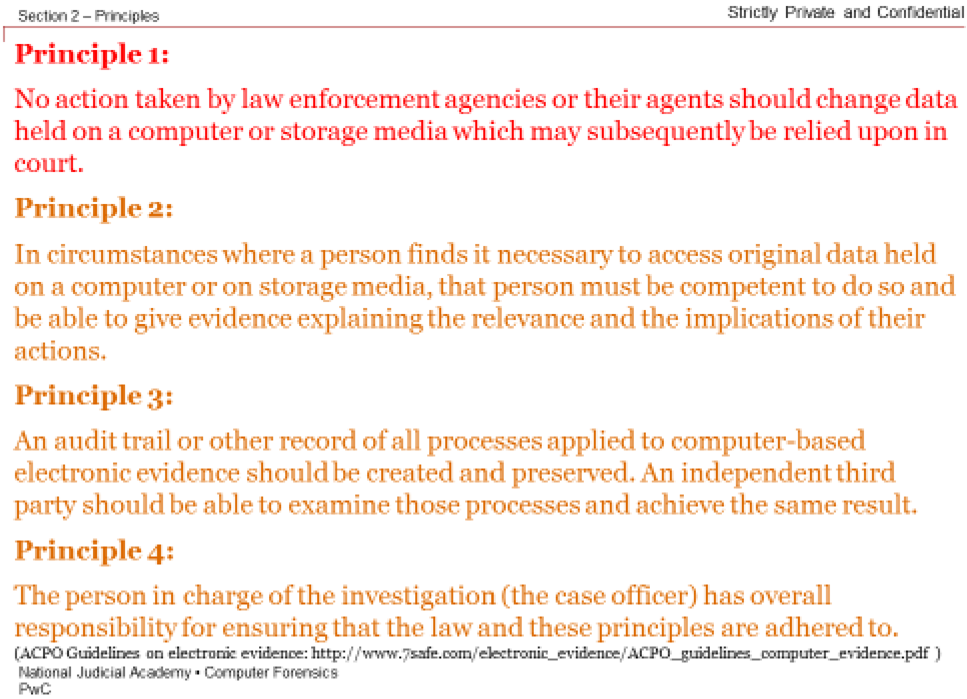
How we define digital forensics?

"Digital Forensics is the process of **identifying, preserving, analyzing and presenting** digital evidence in a manner that is legally acceptable in any **legal proceeding.**"

It involves **data presentment** according to the rules of evidence.

National Judicial Academy • Computer Forensics
PwC

I am just going to talk about the four principles of how digital forensic should work while doing investigation or while presenting before the court of law. So if you just go through this. (Pointed towards the following Slide)



Section 2 – Principles

Strictly Private and Confidential

Principle 1:

No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

Principle 2:

In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3:

An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

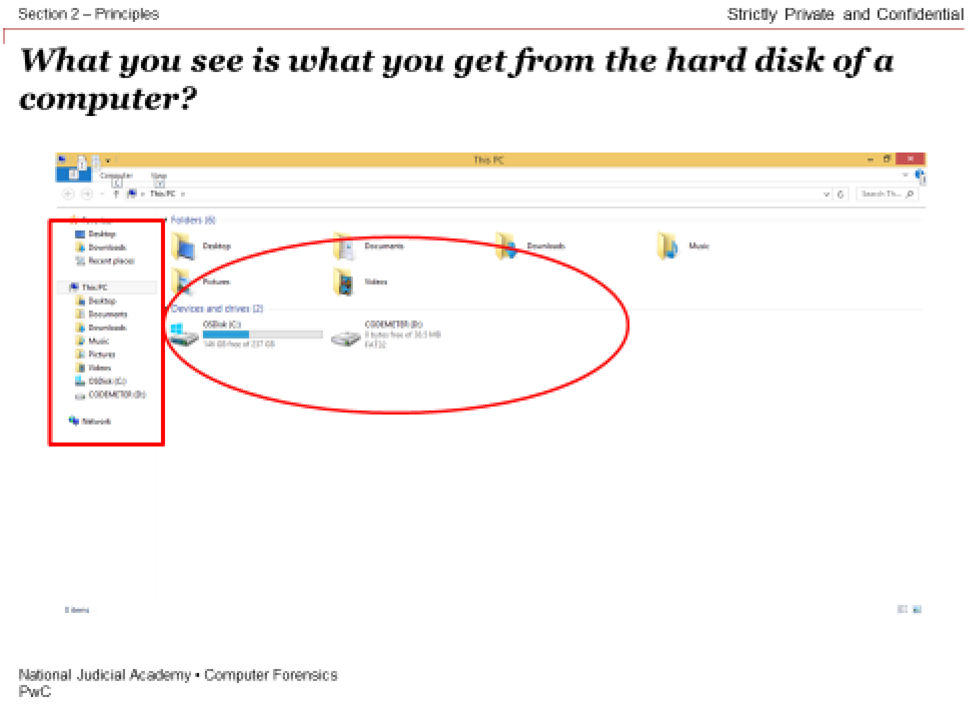
Principle 4:

The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

(ACPO Guidelines on electronic evidence: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf)

National Judicial Academy • Computer Forensics
PwC

Principle 1 says: "No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court." We talked about tampering of data yesterday, this is what this principle is covering. At any given point of time when the device is seized from the crime scene, that device should not be altered or tampered with nay form. All due care should be taken while collecting that data or preserving that piece of evince. What principle 2 says: "Principle 2:In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions." I He must know the outcomes, if he mishandles that particular device or information. Principle 3 which talks about chain of custody primarily. So every step he has taken should be captured in some fashion so it could be about chain of custody. I will show you how we maintain our chain of custody while marshalling from one person to another, second person to third person, I will just give you that piece of information. And fourth one is the person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to. So if you see the computer as a layman, how that computer will be seen to you. So once you open the windows explorer, I am just giving you an example of windows explorer, so once you see the windows explorer this is how you will see your windows explorer. There is a primarily partition called C then secondary partition called D and then there are these folders lying on the machine.



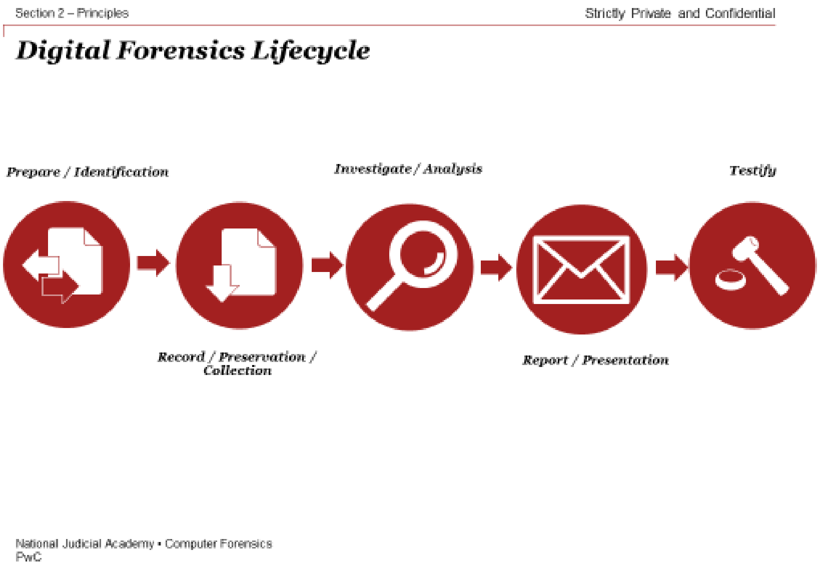
Section 2 – Principles

Strictly Private and Confidential

What you see is what you get from the hard disk of a computer?

National Judicial Academy • Computer Forensics
PwC

Any forensic expert if he wants to see any data how that data will be seen from his eyes. I am just going to next slide which talks about this. If you see it is like tip of the iceberg. Ok. So what you see as normal layman that is on the upper side, as a forensic expert you will see certain things which normal person cannot see. For example deleted data. Then we have operating system artefacts, which will have when then machine was booted, when that machine was shut down, who was the user of that machine, Ok. Then we have the file system, what kind of file system it has, whether it is a legacy file system called FAT, file allocation table or in case of UNIX, it is UNIX based file system, so I will explain to you , how that file system works Then we have another class. Yesterday I talked about a hard drive which has 500 GB as a label on the top however the space allocate could be 474 GB. However the remaining portion is for the hardware aspect of that hard drive. So 473 is the usable space, like carpet area ghar ka hota hai Na waise. So that is usable space, within that usable space we will have some partitions in that. So that is logical partition. So if I create two partitions of 100 GB each, I will have 4 partitions within 474 GB. So within that partition that is the logical storage we allocate within that physical hard drive. The space which is free which is called unallocated cluster. So when we buy any hard drive and when we do installation of any operating system it does the formatting initially then it starts writing operating system on the hard drive. It rights to certain extent, it uses certain space of the hard drive, and rest of the space is kept for storing the data. So now, when I am talking about file table. When file gets deleted what happens in the operating system. As we explained yesterday, it was like a book, If I tear I page of the book and remove index of that particular page just reference of that particular file is removed. When file is deleted. It could be hard deleted or normal soft deleted. But that file content will be there in the unallocated cluster which is the free space of the hard drive which is not allocated under any partition. So whenever we do recovery of any file what forensic expert does, every file has a header and footer to identify it as one file. So for example for doc file or word file, it will have a header as doc and it will have a footer as I don't remember. So how will Iu do the recovery of that file, I will look for the doc similar to doc character in the fee space, I will pick up that I will search for the footer of that particular file and then I will try and reconstruct that entire file. Or with the content of the file. This is how the recovery happens. Then next part comes with RAM> yesterday we had shown you the RAM circuit board which is Random Access Memory. It is used to enhance the speed of the machine. So instead of fetching data from the hard drive which is your bigger size it fetches data from The RAM which is recently accessed, then we talked about partitions. I showed how partitions looks in forensic applications. The clod and chat history and various internet artefacts. So various artifacts like your messaging, your web based emails, your chatting history, whatever web sites you have visited all that information we capture under the internet artifacts. So next is, this is the typical life cycle of any digital forensic analysis.



Section 2 – Principles

Strictly Private and Confidential

Digital Forensics Lifecycle

Prepare / Identification

Record / Preservation / Collection

Investigate / Analysis

Report / Presentation

Testify

National Judicial Academy • Computer Forensics
PwC

You need to identify source of data, a particular source of data. Then we carry out some kind of preservation mechanism, when we have original machine, seized on the crime scene, we do copy of the hard drive, the mirror image. One mirror image is preserved as it is to present in the court of law and second one which is working copy, the analysis is done on the working copy. Because then your primary copy will be intact. Then we have our report mechanism, then we do certain set of analysis based on the case and then we prepare report which can be given before the court of law, produced as an evidence. Then we have testify. As an expert witness, what test we carried out, so that we can stand as expert witness in the case. Any questions so far.

Participant: We have a C drive, D drive E drive?

Mr. Sachin: No necessary, it depends on how you have configured

Participant: there can be F drive?

Mr. Sachin: yes absolutely. If your computer has C and D drive and if you attach any pen drive, it is again a storage media right, that computer will assign that pen drive an s an F drive.

Justice Muralidhar: Whenever you browse the internet, is there any space used up in the computer because the cookies and all of that

Mr. Sachin: That entire things stored up in internet cache. So I will explain to you how that internet cache will look like

Justice Muralidhar: But that will be part of the analysis.

Mr. Sachin: yes that will be part of the analysis. Ya. It has a specific limit of that cache memory, if that over flows, it will definitely slow down your computer.

Justice Muralidhar: Will you also explain to us how the virus can come in through the net and what that does.

Participant: Sachin, one more question, does it, only a specialized person can, a forensic person can find out using a header and a footer or anybody can do that.

Mr. Sachin: For that we need to have, first deeper understanding of how operating system works second the right set of tools, which will actually give you access to the internal information.

Mr. Nair: When you do, every file has a propriety header and footer, not necessarily but it is that how the whole system is made. So you will get lot of false things in the whole process. So an expert will be a better person to tell which file is created exactly and which is not. A layman can do it with understanding of what is header and footer but to figure out which is right one, expert would be better.

Mr. Patil: So when we are talking about memory. When we are accessing internet or accessing any file there are three types of memory, one is cache memory, which is considered to be fastest memory. When we open mother board, we can see white spots, dots around the chip. So that is the cache memory. That is first memory. Second is RAM memory. The question is asked, can we access and retrieve cache memory. The answer is no. My friends can correct me. RAM can be forensically if not image, retrieved the data. Yes, we can do it but not in they read only format. It is not read only. SO we can capture the entire RAM as it is but we cannot take hash value because it is momentary, we are capturing at that moment. The RAM will continuously get refreshed. Still it is forensically secured. Third type of memory is where the data can reside like we are accessing any internet. What typically happens, if we are retrieving 20-30-50 web page so two of three web pages are very active. SO typically in active web pages the computer will automatically throw in virtual memory. So there is a possibility that we can retrieve from cache memory and it is part of hard disk on part of RAM.

Mr. Sachin: Just to give an example of how that cache memory works. So when you type google, you will get option. It will automatically suggest you options which you had used previously. So that previous options are part of your cache memory.

Mr. Nair: to do this particular activity, it would not store it on a cache or it would not store it on RAM, it would require itself only after 6 months when you have done it. So what is does it probably creates a file for that particular file. There is a small reference that is created in the drive which is not like an artifacts to say that OK so you have searched that particular thing on this particular device and it is not necessary when you go into your private browsing mode or whatever. Would you get that? The answer to that is yes or no. No being that I am on a private mode, I not necessarily should save that. But what happens is exactly like what Ravi said it ultimately stores it somewhere and there are chances that you get that file which is temporally created and you recreate it.

Mr. Sachin: And where you need this information while doing any kind of investigation for example if it is a suicide case, person may try and look for some Google, so places or some medicine or some poison. That piece of information will be retrievable form the cache memory. So that is very important. Next we are going to talk about what kind of information is available to the forensic analysis. It could be your computer, your mobile phone, it could be your email, sitting in Gmail or yahoo. It could be on your legacy devices like your own computers, your own computers, zip drives all that stuffs.

Mr. Patil: here I would like to draw you attention to discussion in morning. Madam had stated about two types of protocols, she mentioned that one is IMAC and second POP. What happens in IMac, suppose I have configured my company emails from Gmail on my mobile phone through IMAC typically I will get one copy and one copy remains with google server so this is replica. What happens with Pop that is post office protocol, the mails are physically transferred from server to computer system and it is a typical problem that we face when we are facing investigation of corporate frauds of any email that has been send from corporate. Taken an example, a threat email is sent from corporate employee to public servant. This mail is archived by that corporate employee. What is the meaning of archive, through post office protocol, this email will be physically removed from mail server of the company and will reside in his personal computer, so the only source of computer that I will be having with me to prove that this email is being send not from the server of his company but from his computer. This local storage comes into play. Any questions so far.

Participant: Suppose one person sends an email or threat email and the one which is retained in the computer is deleted by the sender. Is there any way by which one can forensically construct that.

Mr. Patil: the answer could be yes or no. because it depends on when it has happened. Whether it has been done just before the incident, whether he has got adequate time to over write something because there has been instances where the email has been instantly deleted. Typically people do it in panic state and all of them are technical experts to over rite. So in that scenario there is always a possibility to retrieve that email

Justice Muralidhar: No let us say, if there is a threat email, I not only delete it from sent items but also from bin. So what happens then?

Mr. Sachin: Email works little differently. Concept is that same. Email is typically stored in a container, we call it is a PSC. It is a personal storage file. So how it looks like. So this my one PSC o f I GB, it has 1000 emails, Ok. SO that PSC is divided in two parts, one is the free space and one is the actual PSC, so when one email is deleted it actually goes into the free space of the PSC contains, the same funda which we applied in computer memory. So when recovery happens from this portion. If some other email is deleted and it is over written on that particular space, that will not be, the earlier email will not be recoverable.

Mr. Patil: Sir to summarize what you said, even if it gets deleted from recycle. In there is a possibility that a copy is still residing in the container so long as it is not over written, there is a possibility of recovery.

Participant: Suppose it is over written.

Mr. Patil: Then we have to rely on trace evidence not the actual email.

Mr. Nair: There could be laws of email exchange. So like for a typical mail exchange it records certain things when it sends something from here to there. Probably you will not get body of the.

Participant: But then it makes no scene for the judge probably you will not get body of the.

Justice Muralidhar: It is like impression of seat rather than someone sitting on the seat

Mr. Patil: Sir in trace evidence typically what happens sometimes we get that there are bits of a particular email. Just to give an example, that in 2008 when we were following Indian Mujahedin and we were continuously getting data from google on every day basis stating so we used to follow the, we used to identify the location. So I identified a cyber cafe in Kathori in Muzzafernagar district. Now the cyber cafe didn't have a log so I had to depend, I had to do some quick searches to identify probably which of the computer was used by them, so what we did, I used a software and did some quick searches. Because we first retrieved the virtual RAM, did some quick searches and we found that one particular email id of another terrorist reflected in that page file? SO in all totality this is a very remote possibility that everybody would be knowing that email id. Then we seized that particular computer. So that kind of trace evidence could also be identified. I don't know what the evidential value is but it indicative of the fact that yes this particular email id was forensically retrieved from this particular device.

Justice Muralidhar: So One last question. Particular computer which ever it is as the IP address, how is that IP address detected for that machine. Through what system does that happen?

Mr. Sachin: Sir the entire IP address allocation happens through the ISP. Internet Service provider. So every area of every region has been given certain specific set of IPs. So when that allocation happens to the end machine, which could be your cyber cafe or home that happens on dynamic allocation. When as an examiner if I trace back the machine I will not be able to get back the end point of the entire network. I will get the IP address of that ISP. Then I will have to go to ISP, get those details at that point of time, that day, which IP was given to some other machine, to log, then to collaborate everything.

Justice Muralidhar: You have to go to that vendor who sold that machine, is it?

Mr. Sachin: No not that vendor ISP, the internet service provider.

Mr. Nair: So ultimately you might end up going to a router, for example. This is the Academy over here. You would have only one IP address, that is of the academy, or probably 2 or 3 to share the load basically. The academy could say that ok at that point of time, I had given this particular IP address and this is.

Justice Muralidhar: let me give example, I use a device which is not connected to the internet. I used that to generate a doc. Then I take it in a flash drive, go to Calcutta and then give it to someone who can send to someone through a computer in Calcutta. So it is difficult to trace it back obviously.

Mr. Nair: So in your case, we would not be looking at IP address. The file that got created.

Justice Muralidhar: No which ever device is used to send it across the net or whatever, you can get up to that device.

Mr. Sachin: With the help of ISP.

Mr. Sachin: This link, for example if you are in Bombay and travel to Calcutta. That link from Bombay to Calcutta has to be established.

Mr. Nair: Just to add on to your point. Now you have told us that you have ausb stick that was used. So we would corroborate it with the time at which the data was sent, along with the USB being plugged, an indicative evidence.

Justice Muralidhar: Would you know that it was sent through an USB.

Mr. Nair: No, we would only know that a particular file was attached and sent. At that particular point of time, like what Sachin was showing you, a lot of particular evidence, we look into. One of it is looking at what was accessed. One of it is USB that was plugged in at that time. That could be an indicative thing for us, to look for that particular device and look what was in it.

Mr. Sachin: So that would be one piece of evidence.

Participant: Every computer has its own IP address. So that will be recorded and the IP address of the service provider will be recorded.

Mr. Patil: Sirs question is that from that how we can trace that the person who has actually created that document. There is one more way of doing it. I can modify the Meta data if I am that expert, I can actually change the details and then send it across that is also possible. Only thing is that I cannot change the time and date, modification take. If I am taking photograph the camera mode will be there. Sir there are two situations. One is that that you are creating the file, and storing in the original folder. Absolutely it is possible.

Mr. Sachin: One of the pre-test for any forensic examiner is to first see what the time zone of that computer is. It is very much possible that possibly it is timed from UK to India

Participant: Not only that I am put a wrong date, wrong time.

Mr. Sachin: Ya that is also possible but that can be caught by seeing the system log that somebody has changed the time zone or time of the machine.

Mr. Nair: So basically in windows what happens is typically when you change your time or time zone there is something called, I am just being a bit technical over here, It is a particular service that runs, so we look at that particular service, when was it triggered. So this is an indicative evidence that there has been a change of the time.

Participant: If I remove it?

Mr. Nair: Even if you remove it.

Participant: Just to recall, you have already answered it but I am just reframing it. I have travelled from Bhopal to Bombay, go to a cyber cafe. Write a hate mail, send it from there and come back to Bhopal.

Mr. Patil: Sir what the agencies have started is, that if we know the time stamp, if we know the cyber cafe the location from which the hate mail has been sent, to be on safer side the agency would go and take tower log of that particular tower. With the hope that the person, even if he has taking precaution he has an alternate mobile number, he has called, contacted some one that kam hogaya hai. So within 10 minutes if there is some odd call then we can pick up and then we can trace back that if there is any number which was recently activated or which was never used after this particular thing. But yes.

Justice Muralidhar: Actually the crux of my question is it possible by staying out of internet use computers which are connected to computers at all, generate electronic evidence and then use other systems to just transfer it so that the last mind of tracing that from point of transmission to the point of creation, that makes it very difficult.

Participant: That is possible because once you put the pen drive in, you have also blocked the data

Justice Muralidhar: No No I hand it on to somebody else, the point is the person who created simply hand son the pen drive to someone else.

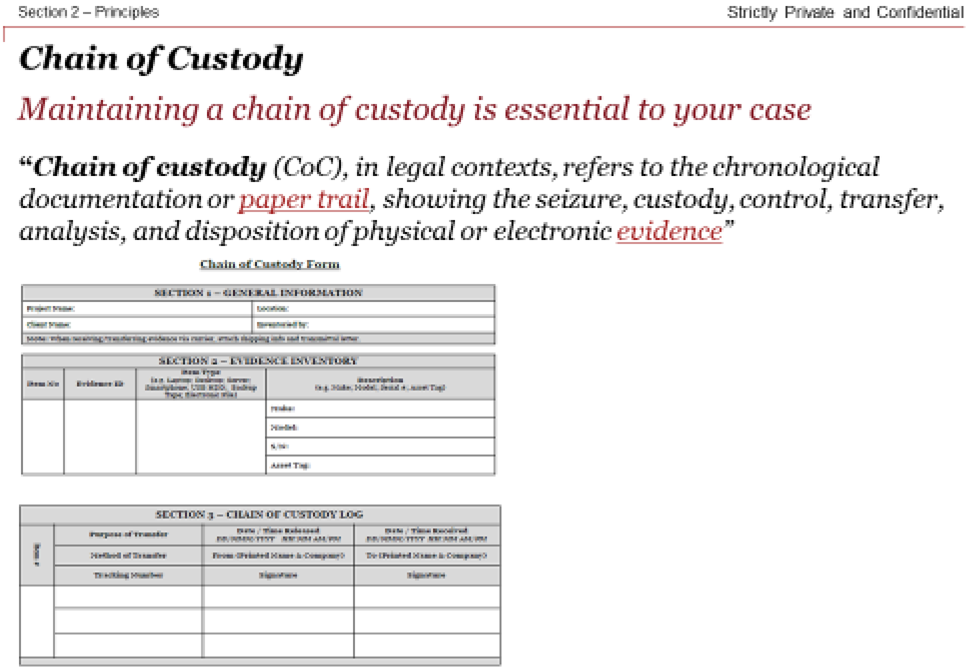
Participant: It is right but when the data was entered in the first instance. Justice Muralidhar: No No unless you get hold of that pen drive.

Mr. Sachin: Pen drive or that machine from where that file was created.

Justice Muralidhar: Ya, for example let us say, print out of that document and some =body just photographs it on a mobile phone. So you cannot get. There are many ways of staying outside the internet Mr. Sharma: Sir there is one point here. If we have a standalone computer system, but Wi-Fi is available, so there is a possibility that one of the Wi-Fi connections may recognize the machine ID of your system so you never connect to that.

Justice Muralidhar: O I see

Mr. Sachin: provided your Wi-Fi is enabled and all that conditions will apply...hahaha...right. Hahaha. So we talked about chain of custody how it should be maintained, how entire passage of the exhibit should be maintained and captured so we, our office, we use this type of form



Section 2 – Principles   Strictly Private and Confidential

Chain of Custody

Maintaining a chain of custody is essential to your case

*"**Chain of custody** (CoC), in legal contexts, refers to the chronological documentation or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence"*

Chain of Custody Form

SECTION 1 – GENERAL INFORMATION	
Project Name:	Location:
Client Name:	Received by:
Note: When receiving/transferring evidence via carrier, attach shipping info and transmittal letter.	

SECTION 2 – EVIDENCE INVENTORY			
Item No	Evidence ID	Item Type (e.g. Laptop, Desktop, Server, Smartphone, USB HDD, Backup Tape, Electronic File)	Description (e.g. Make, Model, Serial #, Asset Tag)
			Make:
			Model:
			S/N:
			Asset Tag:

SECTION 3 – CHAIN OF CUSTODY LOG			
Item #	Purpose of Transfer	Date / Time Released DD/MMM/YYYY HH:MM AM/PM	Date / Time Received DD/MMM/YYYY HH:MM AM/PM
	Method of Transfer	From (Printed Name & Company)	To (Printed Name & Company)
	Tracking Number	Signature	Signature

I would suggest that nay government agency which is seizing they should also follow similar set of information. i am sure they will be having it but probably Ravi can explain.

Mr. Patil: this chain of custody form, I think technology has created more problems and I think have no apprehensions that the case may take time if they do not fill in the chain of custody forms properly, for example in I phone, there is a Nano sim card, if we go to rural areas there is no key available, rather most of the constables they would fill the form and typically this chain of custody, we don't have this kind of chain of custody, we simply right the details on plain paper, so now they have started writing more physical description so that at least they can prove that this phone with this description, this angle, at least something can be proven that they have seized this phone only. That is one. Second challenge is that I I need an IMEI number because I have to keep that for tracing. Now how will I get an IMEI number, I have to switch it on. Now if I switch it one, the moment I switch it on there will be question defence lawyer that I have tapered. If I don't switch it on I have lost a critical piece of evidence. To give an example, I was assisting Maharashtra police, regarding the triple murder case, I was assisting CBI for Maharashtra police, they have seized 23 mobile phones from suspect's house, and few of these mobile phones belong to the main accused in this case. Now direct one, should we switch it on? The lawyers would give us suggestions that do not do it. Forensic science laboratory might come back to you after 2 years. By that time the mobile service providers will say that sorry, as per the DOT rules, we are supposed to maintain the records for 12 months. So that is kind of technical problem that we are facing right now as far as the chain of custody forms is concerned. This chain of custody forms works very well for computer forensics. I can remove the hard disks. But now look at the other side, switching on the mobile phone is not at all taboo, because even forensic science laboratory cannot proceed without switching it on. I cannot image a mobile in switched off stage that is a technological impediment. So either I will open it or they will Whenever I switch on an operating system on computer, windows records last shut down time, and that is what is always captured by forensic science laboratories to show the integrity. There is nothing called last shut down time for mobile phones. Because it is very small compact operating system. So the FSLs they want to do that that cannot identify. So typically my personal opinion is that based upon this technology limitation switching on a mobile phone per say is not tampering, unless the files are not tampered. So that is the

Justice Muralidhar: I read somewhere, that you can programme your phone in such a way that merely switching it on can wipe out the data.

Mr. Sachin: That is where the Faraday bag comes into picture. Whenever we seize any mobile device immediately we should put it in faraday bag. Which will protect the phone from getting a signal or if you don't have a faraday bag you can normally use aluminium foil which I mentioned. So if you see this chain of custody form you have very minute details captured in this chain of custody form. Right from the size of the hard drive, SAS, usb, make model serial number. We also capture what is the bios. Sir as we said if I remove the battery, I change the date but that date will get captured here. So while seizing I will first see the date of that bios and record it.

Mr. Nair: And just to add to the point about the date being wrong if I have a computer that is a having a wrong date and if I try to connect it to the internet I will not be able to do. So all the servers like for example, if you do a google .coma after that it will not authenticate your connection. It requires that you have a time sink. Partially that phase is going away from the computer forensic side of it.

Participant: Is it only google or any?

Mr. Nair: Any...most of the sites.99% of the sites, it will not. It will just tell that I am not able to authenticate you so basically there is security key that goes when you go into a website. That does not allow you permission. It just says we are not able to give you connection until you get your time right and also windows have got an option where it automatically aligns itself with the automatic clocks. SO that point is actually really fading away right now.

Mr. Sachin: We also have what is called accuration method. How do you collect information from the exhibit ok? There can be servers which cannot be shut down so in that case we have this live accuration we will have some tools attached to it and we will get that while the server is running. Sink of the RAM , which Ravi mentioned some time ago, from the RAM also you can get the entire meta data and we can actually do analysis on what was going on in that machine, just before taking that part. So if you access any website or if you put in any password username, probably if it is very weak password, we will be able to decode that. We can also capture the tool details like which tool has been used to image the hard drive.

Mr. Patil: And what I have observed that CBI has come up with a very good procedure. Typically what CBI is doing that they take FSL people around for imaging. The moment they take they ask the FSl people to come to scene of crime, image, and take two copy, provide one copy then and there to CBI. First of all because the imaging has been done by FSL, there is an evidentiary value and they will do the analysis in there lab which is better equipped than FSL to extract the data and even if somebody challenges they can also say that we have extracted and corroborated from FSl. that is also a good process and they will have similar chain of custody form

Mr. Sachin: So next we talk about how the actual accreditation will work. So yesterday we had shown you shown you some device, called light block device, this is how it is connected to the light blog so that no information taken on this primary evidence which is non- tampering of your information. As I discussed a while ago there are three types of imaging being done. One is your live imaging, one would be physical imaging. What happens in physical imaging once you have machine if you image it in full form that is your physical imaging of the hard drive. What do you mean by targeted or logic imaging. So when in case of server which cannot be shut down for imaging, in that case we do the logical imaging, which is partition based collection of data. So if there are C or D drives you would only connect C or D or may be some partitions present. Ok.What is the targeted imaging, in some cases we do not require to capture entire hard drive or could be entire partition, we are just interested in a file or folder, in that case also we can just image that particular file do the hashing total of that file and then present as an evidence. And we can then of course that has been supported from which machine, it has been taken, the time it has taken and all.

Mr. Patil: So as far as physical imaging is concerned now, the procedure is tried and tested, we know that hash value has to be taken, hash value has to be matched. It has to be done in switched off stage. The challenge arises pertaining to other two types of imaging. So when we are doing everything in switched on stage and the situation arises when we are imaging critical infrastructure related computer system. For example yesterday I was mentioning the Delhi International Airport virus attack case where we had to do imaging of their baggage reconciliation system. So this server has to always up and running, we cannot switch it off but the virus attack happened on the baggage reconciliation server, so we have to do imaging of that server but imaging has to be done in current stage. If I take hash value of this image and if I again try to take hash value of the original, original has changed by the time, because the data is continuously getting updated. Now I have, I am taking image of system what particular time a dpl case so after 5 minutes I cannot go back, yes I am taking hash value to ensure integrity of the file, I cannot show based on that hash value that this file system is exactly similar to the file system that exists in the original. Will just give an example. There are certain events logs that are continuously getting updated. What are event logs, as my colleagues have mentioned, if the time stamping change so there is an event ID generated, somebody has logged in, event id is generated, logged out, event ID is generated. So in live system event Ids will continuously get generated. I am taking that event log file for that moment and I am not sure such, because US courts live imaging and such imaging is always admissible as an evidence in the court of law. But we are increasingly coming across such cases wherein physical imaging is getting replaced with logical imaging and targeted imaging. Now this process is going very well in corporates because there is no need of doing something under the Indian Evidence Act. So this is where a kind of dilemma exists, even if it is technologically feasible, whether thus part would be legally admissible or not. But that, the practically it is the only solution available right now.

Mr. Sachin: So next part is how you authenticate what data you have captured is right and complete form. So this is how we can do that authentication. Like catch word in the hash value. Yesterday we showed you how to calculate the hash value and how it differs and then we have minute change in the content then the hash value will also get changed.

Participant: I think you used it in a case.

Mr. Nair: Ya we did the same thing yesterday, we did it for a file this is kind of for whole image. I am just going to tell what the difference from what we did yesterday is. We only did this yesterday. But if you look at something like this. This is like the actual date and the target date. This is actually telling you the time difference between the device that you have collected and the time difference that is sitting on your computer. So that is just an addition to the whole thing that we did yesterday.

Participant: just an idea which I would like to share with all of you in this august gathering, in the 1st session there was one situation which we were looking at is the CCTV taking` footage and the camera time may be different from the actual time. I think the investigator at very first stage can actually see the camera time as is logged in and can say that this one hour 30 minutes ahead or behind the actual time. That evidence can be resolve the problem of mismatch time.

Mr. Sachin: So next we will move to the types of analysis which can be done on any digital media, for example. I will just take the entire list of analysis. SO digital forensic which talks about your computer, your any storage media, it comes under digital forensics, also mobile is also digital but we categorize it just for the sake of understanding, we take it separately, ok. So what comes under computer forensics which should be...So there are couple of, set of analysis which we can carry out? One would be recovery of your files, recovery of partition, right. Apart from that what else we can do. This is to ask you question Sir, what analysis we can do in terms of computer analysis. So one is, malicious application, if you suspect, like in Delhi case, like you said there was a malware in the system

Mr. Patil: We had identified a malware in system 32 file, so we also identified a malware named kill.cmd. In system 32 file. We also identified code withheld of an expert to understand how it can actually affect the computer system, how it can cause damage.

Participant: Will you just explain to us a system 32

Mr. Patil: I will first explain the case and relate it to that. What happened on 29th June, 2011? A virus attack happened on Delhi Airport and we identified that this virus was inserted on 19th June 2013. Somebody had to insert that virus, he remotely accessed that system, bypass 4 firewall and took helped of user id and password of 2 different companies that are attached to Delhi International Airport authority and got an entry inserted a virus but virus did not execute. The person again came back on 26th June, inserted virus. It was very funny virus. The person had inserted the virus in win logger file. What is win logger that is windows logger? When anybody would log on the virus would get executed. It was actually fraud so that person who will log the virus will get executed and anybody want to catch, they will first catch hold of that person. The virus was inserted three days before in their domain control room. How this virus was supposed to be executed. There is a very important file of windows known as system 32. The executable file in system 32 have foot prints in the registry of the windows. So windows registry is nothing but heart and soul of windows it will decide when a programme will run, how the programme will run, whether the programme will run in backend, front end. What this person did, he inserted a file named kill.cmd. i can actually show you how it was done. Kill.cmd in system 32. Ans he created a foot print in win log on by adding a small command he did these activities. There was another employee, whose name was Jehnir Singh. He logged on after 3 days on 29th June for regular system back up. The virus got executed and the natural suspicion was upon him. But after two weeks we realized that there were certain IP addresses and yesterday we were discussing about firewalls. In firewalls, we identified that there was an outdrawn connection, to log me in. Log me in is a remote connectivity software. So there was one software where log me in was installed and for accessing, remotely accessing a particular computer and there was one computer which was weak link and on that laptop this log me in software was inserted, Installed and one person sitting in a cyber cafe in Bangalore, was accessing that software and through that software he could access entire system of Delhi airport. So what we can do at 4 when we start doing demo. i can actually show you how this virus was inserted and how this virus was executed, we can do that.

Mr. Sachin: next in line is the data carbing. One is deleted file, a copy happens in two fashion, one is recovery from the recycle bin or from any free space of hardware. That is one aspect, second aspect is data carbing. Carbing is taking up header and footer and try and reconstruct the file. That, it may not be sure that you will be able to reconstruct the entire file. It could be part of file which you can reconstruct but in terms of picture which is not over written or half over written probably you can get part of that picture. But that piece of evidence may be important for the case.

Mr. Patil: They are asking about deleted file, so there are different stages in which things can happen. First if file is deleted and it is inside recycle. In, you can recover. If file is deleted from recycle. In but there is also a container to keep file as this is one container. now imagine situation where a file has been deleted from both container and from as well as recycle so every file as it needs file header, so this file header is nothing but the file signature, so based upon this file header the forensic tool can identify that there exists a file lets us say a word file which is unallocated which is not having any reference in the muster file table but it shows that there is a word file. So if we start picking those files it is called file retrieved time. Typically what happens if it is word file, it is text file there will be chances that file will be recovered, even if it is practically recovered we can see something, if not directly then we can view on the forensic tools itself but when it is image or video file or an audio file, if the critical pixels are lost then you might recover 9.5 MB or 50 MB file so at most you can end up doing that once upon the time, file existed. So that is called deleted file recovery.

Mr. Sachin: So next is pass word cracking of any file. So most of the times important information is hidden in password form so a file is given password to open, so in that case we have this tool specialized tools top do the cracking of the password. So how this cracking works. So if it is alpha numeric password it is simple permutation combination, it runs in the back ground and then it pops up the password, if it is, so there is

Participant: Alpha numeric is special characters

Mr. Sachin: Ya that will process, it will take time, it will, you have to just give the possible range of the password and it will try different combination with the special character whatever asci characters is available information if you keep trying that password it may take from 5 minutes to 5 days, it could take 5 weeks also.

Mr. Nair: To be very frank, any alpha numeric, with symbols and numbers, if it goes beyond 7-8 characters, it takes lot of computers to run. So basically in US they have farms that do it like about 100-400 servers trying to crunch it out, that is what FBI uses to get it. Basically at PwC what we try to do is say for example, for example, I would give you an example of banking password, consider , we don't do it but that an example that I would use over here. You know that there are four alphabetical characters that are used there are 4 numbers that re used, this is a typical bank password. So we can use that in the software that we have, what these does it number of attempts goes down so the amount of time required is less, or alternatively what we try and do is we pull up a word list of all the orders that are sitting on the hard drive, those could be words that are coming from his word document so it is a natural tendency for people to go ahead and have a word that we usually use and run an attack based on those words and it is not a 100% sure shot solution but this is a way to run it out.

Mr. Sachin: and to create that repository of words that is called a dictionary attack, so that creates dictionary of all possible words that is on the machine.

Mr. Nair: But right now in India, dictionary attack or password cracking is bit tough to get through

Mr. Patil: It is bit of overdose, just after the lunch. Hahaha

Participant: technical overdose.

Justice Muralidhar: So should we have a ten minutes break.

Participant: Whatever information you are giving us do our law enforcement agencies have it.

Mr. Patil: they already have it.

Mr. Sachin: they are two steps ahead sir

Justice Muralidhar: Actually the difficulty is the age of the criminal, see what is happening is they are looking at ten years old, eleven years old who are expert hackers.

Mr. Patil: Sir, if you allow me I would give an example. I experienced just a month ago. I delete with a very interesting case in a, within this room I can share the details. This case is pertaining to Delhi Public School, Hyderabad Branch. DPS had started a process of empowering children by providing separated email ids, every school related activity, and they will send an email to the kids so even a 3rd standard kid will be having an email id. What happened, this case is of brother and sister. Sister is in 3rd standard and her brother is in 5th Standard, so sister used to always complain her brother that the class monitor troubles me a lot and she says that when I would go and complain, class teacher would always take side of class monitor and I would be scolded. Brother got furious. One day both of them in break went to school library, there is a computer access so that kids can access their emails. So what he did he said what your email id. Sister told, name. Surname is the standard email id format. So he could predict the email id of class monitor. Monitors email id is also name .surname. So he asked sister what is the password provided to you so the default password provided to you, school children cannot think of password, right. So the default password was name123 for all of them, so of course the monitors password would be name123 so what he did he opened monitors email account. Because nobody would change the password. Then he sent email abusive emails to class teachers, head mistress, all senior people in school. It is a real story. i had to actually sit with the father of kids because school had shot some help from us. So how did he pick up the abusive words, now this kid is in 5th standard? He has joined the school bus and goes with 10th standard kids who are known for giving abusive words and so he had picked few abusive words from his 10th standard senior friends. So he used those words sent the letter. So school appointed a cyber expert ok. Cyber expert is a funny word. I would not call myself a cyber expert. So these cyber experts came and first checked in the records what the IP address is? , IP address belonged to the school so this means that the email has been sent from our school. So we checked that a day before the girl had checked the email, a day after this girl had checked the email, the class monitor so he concluded that the class monitor had legitimate access to this mail and it was never hacked so he gave a report that there is no kind of odd activity identified in this particular email id. So based upon that the girl's parents were called and reprimanded, her father gave a apology letter. So you would ask how this was identified. What happened, another friend of this 5th standard boy told him that he is having issues with few other friends, he said I can give you a fantastic idea...hahaha...so this boy gave an idea do one think name. Surname, name 123. So this boy was so scared, he went and told his parents that this person was telling me all this. The boy father came and asked the school, is this the kind of training that you give to kids. 5th standard teacher went to 3rd standard teacher and told that I think similar incident happened in your class. This boy is suggesting to do something. Is there some relation between 5th standard and 3rd standard? And then they realized that his real sister is in 3rd standard and this is how the incident unfolded.

Participant: that is by accident. The 5th standard boy did this.

Mr. Patil: What is the offence by a 9 year old child under IPC? With this note we can break for tea. Practically they have failed because there is no way they can go back and check.

Participant: But yesterday we were told there is always a trail for this kind of activity.

Mr. Patil: Sir, the challenge with this kind of thing is there is a forensic, there is anti-forensics. So the reason why dark net is still very very difficult to crack. When wiki leaks was started it started educating people how to use torque and how to go undetected. When wiki leaks was blocked in US they started wikileaks.ch. And still continued with that, they kept on getting the data and US could not stop them. SO yes there are solutions but problems are manifold.

Mr. Sachin: Yesterday we discovered wiping, that is also anti forensic activity.

Participant: No this problem, first of all this is very juvenile not adult IPC crime the other thing is cctv monitoring in library could have been there.

Mr. Patil: But problem was that probably schools IP address could be access from many computers across the school so how can one predict that it has happened from only library. It could happen from any other location.

Justice Muralidhar: So we will come back in 10-15 minutes.

Session-9

Justice Murlidhar: friends we have this morning Mr. ashok dohre he is a 1985 batch ips officer and is presently he has held many positions such as additional SP, DIG, nigp, he is working as special director general police at jhangirabad, in Madhya Pradesh so it’s a pleasure to have Mr. dohre share his thoughts with us and his vast experience in the area of cybercrime and he will be followed by Mr. patil, so over to Mr. dohre.

Mr. Ashok Dohre: Very good morning to all of you I am grateful to the director of this academy who gives me an opportunity to interact with you I have been asked to introduce myself. I am associated with this field right from the year 2000 when the IT Act came out and have associated with all the amendments that have been coming through. I had the privilege to address the first ever colloquium of supreme court judges with respect to chief justice of India, Justice Lahoti who was a participant have been addressing the high court judges also in this academy. I will be giving presenting before you more of demonstrations of the soft wares that have been developed by government of India. at the outset I would admit we have very high level technologies to do all these interception seizure and analysis but then we are constrained by the law of the country and I am not an authority on speaking on law but I will specify what evidence would be admissible, so we have to use or Introducer thin the technologies that fit into the admissibility of prudence in the evidence act so it’s basically some sort of a compromise between very high technology we have and the imitation of the law interception is basically capturing electronic data or the electronic evidence when it is in transit so it is left on computer and it is reaching the other computer in between we type it now once a data has been created in a computer or it has been received by a computer then it is not called interception we have to seize that data and emu laces is off-course is how to how do we bake head and tail out of it now, most of the data that is moving in the cyber world moves through a technology called internet now internet is a software and unfortunately it was not designed for what we are using it today people confuse internet with the basic product that came out of a research by that path that is defence researcher agency of America but that is millet and a social version of that military network is called internet which was exhibited or given free of cost to the world to be used for academic interchange of information between professors so it has four major vulnerabilities and these vulnerabilities in fact help us to incept data on the internet they are called the PAPA vulnerability (privacy accuracy property and accessibility) having verification in various aspects of cybercrimes, this the exact wording of the professor who wrote about and he said that maths of twit will translate from millet should confirm to these four postulates the first is the technology is nonspecific to a particular technology so any computer so long as it follows a certain protocol will be able to connect to internet and that is what it says each distant network would have to stand on its own and no inter room changes would be required to any such network to connect to so socially social technology the second says communication would be on best efforts basis if a packet did not make it to the final destination it would shortly be retransmitted from the source so it simply says I am trying to send a message to someone if the message doesn't reach the receiver my computer without my knowledge will re transmit that message and it will keep on doing it till it ensures it reaches the destination now this is dangerous we will see why it’s dangerous, third one says black boxes would be used to connect the networks these would be later be called as gateways and routers there would be no information retained by the gateways about the individual flow of packets passing through them it simply says that if there is intervene in computer between the sender and the receiver the intervening computer will transmit that message but will not make a copy of that message and the third of course is and there will be no global control at the operational level so we don't have a head quarter of internet nobody controls the internet . Once it is on either you be part of it or you don't be part of it you cannot, no one can stop the internet. Now the second and third postulates are contradictory to each other and I will just bring out the difference this is how basically we connect on the internet the man composes a message it’s actually a packet so it has to specify the address of the computer it has to go and it carries his own address also the red path because otherwise the receiving computer will not know where the reply is to be sent so this packet moves into the internet it is received by the lady if she wants to reply she also composes a packet and this packet she knows the address where it has to go is received by the person and the connection is broken so it’s a state less connection it lasts only for a Nano second so we may claim that we are on the internet for two days but technically we may be on the internet only for a micro second now, this is what happens why I was mentioning packets and not messages so the green computer wants to send a message to the yellow computer this the message it is in that computer broken into small packets because if the whole message goes it will block the internet, now each packet has the address where it has to go the sender's address and part of a message they are pumped randomly into the internet and they start arriving from the least populated path to the receiver's computer. here when all the packets have received the message is reconstructed and then we get back the original message this raises the issue of accuracy and integrity how are we assured that the originating message is exactly same what has been reconstructed so that is why it is very difficult to implement internet over the e- commerce business where you deal with money or with wills and all so even today I think will cannot be written over the internet. now, this basically represents how the packets flow one of the packet may take a totally different path to cross the universe depending on the traffic: least traffic on that path, the second packet will flow through a different path altogether, the third packet through a different path but everything is travelling at speed of light so we don't feel we are not getting the packets. now, the third postulates says that these enter the computers will not store the message, so if Iam trying to send a very confidential document to America technically it doesn't matter if my packets are going through Pakistan or through Sri Lankan or through a friendly country but I said the second and the third postulates were not in parlance they were contradictory to each other this is what happens at the note so a packet has come to a note the man represents the computer the note examines this packet now, if this packet has got tampered somewhere something has gone wrong with packet the computer does not take note does not take any step to repair this packet it simply kills this packet because it knows the packet has not reached the destination so it will be retransmitted why should I waste my timing repairing this packet. now, if the packet has not been tampered it has to stop the previous computer from retransmitting that message, so it sends an acknowledgement packet, if it does not send an acknowledgement packet the previous computer will keep on resending it and ultimately one packet will junk the whole internet, so once it has sent an acknowledgement packet it decides on the next path of the packet has to take that is called routing and that is why these black boxes are now called routers. once it has decided the next path it has to transmit the packet, now the issue comes if this computer transmits the packet and the packet doesn't reach the destination so who will transmit it, it has stopped the previous computer from transmitting the message. So the note makes a copy of this packet and technically in digital world nothing ever is deleted so all these packets remain in all the notes through which our message has gone. this makes internet very unsafe, but at the same time it provides us an opportunity to intercepts all these packets so all I have to do is insert a new machine between the client and the server so when the client requests for an information the server will send the information, my machine is sitting in between so I just captured the packet and don’t send the acknowledgement, so now this server will retransmit the packet which I let it go to the client, this is called safing or interception over the internet, of course the law prescribes who can order this interception so its normally principal secretary home orders it. the technology is such it is very easy to capture everything but then there are some problems to it, and that is why it raises many issues, the first is where do we pro, insert that pro so in this slide all these the blue computers are called back bone computers so they actually in reality let the internet work we don't have direct access to the back bone, the back bone needs the taping which called an ISP- INTERNET SERVICE PROVIDERS and the internet service providers and then internet service providers in turn give it to sub internet service providers and we are connected through the internet service providers. so mapping the internet finding out the exact place where you have put the pro becomes a very big problem and most of the ISP follow the rule that they know the computers which are behind them, not the computers which are ahead them, so we have to find out the pyramid where both the computers are tire speed and put the pro there. This is documented not very difficult. the second issue in the interception is this is what a packet looks, so it has an IP address where it has to go, it has an IP address from where it has come and it get the message now, the pro I can give both the numbers i can put, give a command but you capture all the packets which are coming from this IP address of the criminal or so or you capture all the packets that are going to this IP address, now the problem with is both these numbers are provided by the suspect by my computer, so I can Program my computer to not reveal the exact address but give a fictitious address. if i don't want to record so Iam a top man of the criminal gang and just used to giving you instructions so I don't need a reply from them, so I can change this number.

Participant: got a question

Mr. Dohre: yes

Participant: person who is sending a message

Mr. Dohre: yes

Participant: masks his I I

Mr. Dohre: this is precisely masquerading thing, so he changes this number

Participant: that is what send is

Participant: but then

Mr. Dohre: if I don't the reply I masquerade

Participant: then this computer will not sending the packets because it has no response

Mr. Dohre: no its thing is that this packets should reach the destination,

Participant: so we need to keep sending the packets till it gets passes.

Mr. Dohre: yes

Participant: if we changes the IP address acknowledgement will never come

Mr. Dohre: I will send a message and shut down my computer that's all, you will get done and failure message on your e-mail box, that I am able to deliver message

Participant: packets we change

Mr. Dohre: yes

Mr. Dohre: it will go there, and he has not send, simply discarded so the problem here is your intelligence that which can only be successful if we know the destination, because he will not change his number, otherwise his messages will not reach that person. there is a bigger problem than this, this is masquerading or identity theft in IPR term, now, a let I want to say I am a good person I want to send a message to America I don't want it to be intercepted in Pakistan so what I do is could people can develop a technology that I will encrypt this message with a particular algorithm make it unreadable and then the person in America has the same algorithm he will decrypt it, now this technology has become so popular that most of the criminals are using it. this technology is available free of cost so even if I am able to intercept it I get the packet but I won't be able to read it so it becomes unless, so I have written this today strength of a nation depends on its crypt analytic capabilities. so America claims it can break to two fifty six bittle interceptions, I think India doesn't have the capability to break in sixty four bit inceptions and that is why America holds all the interceptions algorithms at par with arms fire arms so near, and you know in India we have a provision I will come to that if I don't decrypt this message if it has been intercepted by public key. The law provides I can be sentenced seven years of imprisonment. These are such technologies which cannot be broken. So now I come to seizure of embed dings there I repeat we have lot many technologies, the problem with digital forensics or the criminal aspects of it is we are bound by the law. all the soft wares developed by the government of India works like magic we don’t have to do anything the software does everything, now any evidence based on analysis of the software when produced in a court of law the court will ask how it has how the software has is doing and how the software is doing is means the company has to disclose the source code. No private organisation will ever disclose the source how its software works, so whatsoever software the government of India has developed I will show you it’s a very good software, I was part of it for last fifteen years developing it. We know the source code so we can explain it in front of court of law so whether it is good or bad we don't have an option. so this is how electronic record is defined in IT act so it can have texts, numbers, images, movies anything generation of electronic records what so ever we type, whatsoever we do with our mouse we scan, we record everything is converted into zero one zero one through a particular software which is called the operative software or the application software. So whatsoever is stored in the computer is in the form of. So I will show you how it is stored so it is all 0101. now when I read it the same operating system will reconvert it into something which I can perceive, so the very first thing is the electronic record has to be read with the same software or in the same environment in which it was created, so I created it this record like this using the green software but if I try to open it with some other software it will open because 0101 is there but it will not be the original thing. I have to use the same software to get back the things so, this is our biggest problem

Participant: can I ask you

Mr. Dohre: yes

Participant: your previous slide, the dark one the green and blue, see if you open it earlier with other software it also comes out something which is in readable state it comes which means this is not exactly the this is the

Mr. Dohre: yes

Participant: as empty, now in such a case when there is interception how a in a ultimately in a court of law one can understand that this was not the true data that was re transferred

Mr. Dohre: that I am giving demonstration of that also, whatsoever we create be a inadmissible evidence is not what we create is not only what we create, whenever we create something the computer also creates lot of data which is header to a file or footer to a file. I will give you a demonstration a file will have lot of data above it and lot of data below it so that is called meta data. by reading that meta data we get lot of information it's not only in which environment it was created it will have information when it was created and how many times it has been modified, in which computer it was created all that information is in that meta data. So when I give you a demonstration we have to ensure the Meta data also is not tampered with.

Participant: there is a possibility of Meta data tampering that's the

Mr. Dohre: if I open it in the rough manner I will show it you then I can change the Meta data but then the unique character we change. We will discuss that also.so I would like to bifurcate digital electronic evidence into two components one is the object on which the digital evidence is contests it could be memory stick it could be a CD-ROM that is the physical object and the other is the content of this so a collateral document these two normally not separable I can't scratch the pen drive and get the data because it is all magnetic particle. the good thing is now, the document I am dividing into three parts electronic evidence that are authenticated so they are digitally signed so those are admissible under section 67- A. the second is the generated by the computer admissible under 65-B. the third and the biggest problem is data which is not authenticated by which I mean all the files in my computer so there could be file created by any one of yourself or myself or my daughter so no origin nothing. the worst problem in IT act is this non- authenticated data we do not have any specific provision so the CrPc is not been amended we have to make seizure as a physical component, I will show you how we do it now, 67-A proof as a digital signature we have to just prove that the digital signature owned by this first and how it operates is the person creates an electronic record then he digitally signs it now this digital signature will ensure its authenticity its confidentiality its integrity and non-repetition and we have to prove that the digital signature certificate belongs to him because that digital signature will ensure all these four objects. 65-B is slightly complicated so it's a very big amendment and because this data is generated by the computer so now we have to satisfy two things the computer was working properly and no authorized person was permitted to access the data so this contains that 65-B certificate shall be issued after all these things have been complied with. so you can see no unauthorized can see what were the steps were taken to recover data in case of failure, possibly if everything is satisfied no evidence nothing will become evidence, but this what basically means this computer generates huge amount of data so the master switching center of a mobile station will record all the conversation of all the mobiles locks, this mobile locked down to this, this mobile rang up to this, there is millions of calls. Now the system administrator as for my demand will pull out some part of it now than he is supposed to digitally sign. So what is specified here is that with all the conditions laid down in 65-B my server was working properly i extracted this portion of data based on this query, this is the data. it’s a tough job but I will show you how it is done bringing out a very important suttle point which file would be evidence, so now my this small computer will play three roles, one is it will be my work station at the same time it act as server also I will explain when it will act as a server and it will act also a recipient computer so let us say this is a document which either I have created or I have extracted now I have to digitally sign. the software is already loaded on to this I right click over it and say encrypt and sign now this is my computer and now it is acting as a server so those are listed all the public keys of all the people in my group. All digital certificates are stored in server like this

Participant: we might use the expression like this, shall I take the view of the administrator,

Mr. Dohre : no no administrator is someone else he is the controller of the certifying authority so when I get a data digital certificate from him in his group he will add my public not my private key now, I have to tell the server where to whom I want to send it , prathibha is the person to whom I want to send it so I pull it down and I click OK now it is asking me so from the server it has come back to me now, it is asking me to enter your oblique key a private key so now I will enter a private key now this document has appeared this is digitally signed document this cannot be changed it contains the original file ashok now this will be received by prathibha through an email or through a normal transmission now. I will extract the file ashok from this again because she has to read this file that is not evidence because that file I can change so all what prathibha has to do is right click egp decrypt the very file immediately it is asking prathibha her private key now she will enter they private key OK so now it is asking where to store that file, so now there can't be two ashok on dextop so I will name it ashok 1 see this is the certificate of that file it was signed by ashok dohre on 31/ 01 at 9:30 p.m. so this is what the court will read and the file is of course is now here I can open and do it I can even change this file so what is evidence is the digitally signed file and not this file because I can change this file so this is of no purpose evidence each time I can use it for analysis purpose but when analysis is presented before court of law the honorable court will should ask for this file extract the file and compare with the file which has been used for analysis

Participant: how would the court extracts it?

Mr. Dohre: this file will come to me as an IO

Participant: court wants you to present it as an evidence and this is what an extract is

Mr. Dohre: yes sir!

Participant: prathibha is denying that I have received or what has received was different

Mr. Dohre: haa

Participant: if prathibha was producing it she produce a key and it will open in encrypted form

Mr. Dohre: right sir

Participant: if ashok wants to produce it then how will he produce it?

Mr. Dohre: then prathibha has to open it is mandatory under court of law

Participant: prathibha refuses to open

Mr. Dohre: she will be convicted under that 69 section not assisting the law or enforcement agencies seven days

Participant: for refusing to decrypt it

Mr. Dohre: decrypt it if the file has been encrypted with the public key of the person

Participant: public key is the private key

Mr. Dohre: no I can’t encrypt a file using your private key because I don't know your private key. What is on the net is on your public key.

Participant: but suppose you have stolen my pad

Mr. Dohre: then you are responsible for its security. That is the only identity you have in the digital world

Participant: . I require the clarification... This is my pad... You can see it... I go out to have my tea as you know that this is closed environment right and it is taken by someone. and someone has access to this corner .now I have kept in a closed environment .=so this basically there is password, now so if someone misuses it to commit an offence which is liable to be punished under law, I will be having defences

Mr. Dohre: yes, because the basic premise of public key infrastructure is that you will secure your private key and you will not tell it even to your spouse.

Participant: but that what we do for marrying purpose also... if someone access my bank locker so one key is with the branch manager and one is with the mature but, someone takes my key and masquerades it issued to someone goes to the bank and gives the branch manager to open and take out,

Mr. Dohre: the only good thing in PKI is nobody can even bake your private key by knowing your public key. it's a massive mathematical problem, it's an algorithm called RSA if we have time after the next speaker I will explain you how it is done, it cannot be unless you disclose your private key, to someone, you misplace it then immediately you have to report it that my key has been lost and it should be withdrawn from the server.

Participant: assuming the defendant is not there and plaintiff wants to produce this document as evidence, what will be happen

Mr. Dohre: it cannot it has to open with the

Participant: cannot it be open just to view it

Mr. Dohre: no... There algorithm is unbreakable RSA algorithm,

P**articipant**: algorithm is not, you are just one time view it then what is the purpose of this

Mr. Dohre: then the evidence is lost forever, the only evidence is that

Participant: algorithm is unbreakable as of today can I modify years later

Mr. Dohre no sir! It cannot be broken it's a massive factorization problem and there is a reward of millions.If you permit me I will show you a technique it is available free of cost you can totally change a file into a file and unless you have the original file you can never come to know that file has new file I will show it to you

Participant: private key is in the form of dongle or password.

Mr. Dohre: it is in the form of a dongle.

Participant: the key can be physically taken out

Mr. Dohre: the dongle can be stolen but then there many security things, like people will attack when dongle will only get activated, when you put your thumb impression.

Mr. Dohre: so basically all these technologies are for people

Mr. Dohre: it will work on your work station only, so it should have access to your computer also, so,

Participant: if it is specific that I want to work on this computer

Mr. dohre: they have registered your, like in our police headquarters, in our police head quarter we have implemented the security aspect, that as soon as I enter the police headquarter my mobile will get connected to the network but that connection is not through a password, the connection is physically IMI number of my mobile is feded to the server. so, even if I change my sim and carry a different mobile my mobile, the second mobile will not connect to the network, it has to be the original mobile only, and if Iam changing my mobile I have to specify to my system administrator that hence forth I am changing my mobile, this is my new IMI number so he will delete the previous IMI number and put the new IMI so that is the way even your computers work. The network are number of my computer is registered in the server so the dongle will only work when it is connected to that work station it will not work.

Participant: then what is the benefit of this encryption for the legal perspective?

Mr. Dohre: this is how you signed all your documents on the digital world

Participant: if we sign we need a digital pdf we cannot view what is there without opening the document, in the sense without rejudging the document

Mr. Dohre: no that’s not signing it, digital signatures means that is just like making it, you can't change it that’s all, but it doesn't carry a weightage of a signature

Participant: what we normally do on the high courts, is when we deliver the order or a judgement once it is uploaded into the server, we won't make our staff our assistant will star, we don't make the digital signature, no one can tamper with the, it is there for anyone to see, it’s in the pdf format, so we can also see, but you can't make any changes, the only way the change can take place when I may order then the file is opened and the modification is done

Mr. dohre: that is because digital signature the infrastructure says everyone will have two keys, now two keys means one is a private key and one is a public key, public key is in the open domain, now when I sign it using my, when I sign a document I use my private key, public key is known to everyone so your server is so configured that when you know the document it uses your private key when somebody opens it it automatically invokes your public key and opens the document but digital signatures will for a document or for a secure communication as defined in IT act it requires that both the persons should have their private and public key to ensure confidentiality,

Participant: in the previous situation of the judiciary, if X is my officer today, and this is the question that we X retires or goes to other department or has left the job whatever now that file is required to be opened, we don't have any access to any document,

Mr. Dohre: but his public key would be there na sir! So any document signed using his private key will be opened by his public key, public key will always be there

Participant: public key overrides the private key. You can never edit

Mr. Dohre: you can never edit the document, I will show you sir, and just a minute I will show you how it operates,

Participant: I don't understand... Sir limitations are there. If today if the assistant registrar's court recording in my court retires and then document cannot be modifies... the document cannot be modified because that document was created then. We are not interrupting.

Mr. Dohre: I think these three slides will satisfy most of us. The first thing under IT act is one addressing from what I brought, everything has to be done in a paperless environment so no digital. Photocopies, now any document has to satisfy these four things. what is the authenticity of the document meaning thereby the document comes from the high court of Madhya Pradesh so it would have something which tells me that it has come from some honorable justice of Madhya Pradesh high court, now once I establish that the second is what is the integrity of the document, meaning thereby I will establish that it is coming from this high court but then the contents are same what is written by the person. the third is what is the confidentiality of the document , so it should be readable only by the people who are authorized to read and the last is non repetition meaning thereby if the document has been created then the creator should not be able to say that I did not write this document. Now the act specifies this has to be done through these provisions that is digital signatures, cryptography and hash. So I just bring out what we mean by this cryptography. What the law says is we have to use a symmetric cryptography now in a symmetric cryptography the encrypting key is different from the decrypting key. Both the keys are owned by the same person. One of them is called the private key anyone of them which has to keep absolutely to himself will not tell to anyone. The second is distributed to everyone in the world so it is there on a server. Now the relation is electronic record coded by the private key cannot be decoded by the private key so once I have applied my private key the document will become encrypted now if I want to change the document I cannot decrypt it by the private key I have to apply my public key only. The other way also document coded using the public key cannot be decoded using the public key but vice versa is true. So from private key, public key private key. We use an algorithm called RSA all the three scientist are alive today it's a patented algorithm, so what I mean is if I encrypt this with the black key I cannot decrypt it with the black key. Some other document will come, but if I encrypt it with the black key I can decrypt it with the white key and vice versa. Now let us see the limitation of this technology. We don't have any other technology decides this. So electronic record I use my private key I get a coded electronic record, I transmit this. The person uses my public key and he decrypts it, now I will explain the implications. I have to buy these keys. So one day I will go and buy my two keys one I keep private and other I distribute to all of you sirs. Now I encrypt it and transmit it all of you can open it, this is what happens... Sir you server it on your server because the public key is in domain. I can't buy the keys everyday now, I have bought it for me it is not serving any purpose because my messages are not coded everyone can open it, but for you people sir it serves the purpose, it is been decoded by my public key means I have written the document, so for all of you if you are able to open the document using my public key you are assured that I have written the document. Now from your point of view any one of you can create a document encrypt it with my public key and send put it on the internet, the consequences that only I can open it none of you can open it, so from your point of view confenditiality is served. All of you are assured that if you have written a document only I can open it, it will be delivered to me only but from my point of view it is serving your purpose because I do not know who has sent it to me. so even A symmetric cryptography does not serve all the purposes, it doesn't answers all the questions that we have, so the solution is what is secured communication that everyone in the digital world has to have his own private and public key and then the system works like this an electronic record I encrypt it with my private key. the whole world can read it but I want this message CN 1 only to be read by Mr. patil, so I encrypt it using his public key, now CN 2 can only be read by Mr. patil no one can read it because private key of Mr. patil is only with Mr. patil and then everything becomes easy, Mr. patil will decrypt bring out CN 1 and then apply my public key and get back the electronic record, so most of us like.. The digital India will be a situation where everyone has his private and public key. I hope that answers questions, so any special yin evidence where we may not like the evidence to be known to everyone like case diary is a private, is a confidential document so if I have to submit a case diary to a court then it has to be signed with the private key of the IO and the public key of the honorable judge then it will remain confidential otherwise everyone will be able to read.

Participant: principle is same if the document is send by email and they send you a password by which you open the document, is the same

Mr. Dohre: that is actually symmetric cryptography. They use the same password to encrypt and the same password to decrypt it, but in a symmetric cryptography the password for encrypting and decrypting are different.

Participant: the example that you gave is very risky, both the IO if officer change which happens in the scenario... What you will do?

Mr. Dohre: no the signature has to be rank specific. Post specific, not the person specific.

Participant: it is handed over to the next person

Mr. Dohre: yes it is handed over to the next person.

Participant: every status of networks, that’s what happens, the next administrator takes oath form the earlier administrator all the high courts have network administrator.

Mr. Dohre: that dongle is handed over to me, and my thumb impression is changed in the server

Participant: why did not private per Se. when in cognition to.

Mr. Dohre: that post.

Participant: the person retires we have to change it every time.

Mr. Dohre: no sir! It is something very similar to a CE, the physical CE report. So it is something like that when I occupy a post the previous person gives me the dongle that this is the digital signature of your post and just like the bank the signature gets changed.

Participant: sir like SP. of so and so place he gets transferred someone else becomes the SP. the seal remains the same

Mr. Dohre: yes! The seal remains the same. So can we continue further sir?

Participants: yes! Please

Mr. Dohre: I have already mentioned sir the unauthenticated document, there is no specific provision in CrPc, has not been amended so even I suppose to make a physical seizure memo, specifying some details of the hard disk and the pen drive. now in physical evidence seizure and acquisition are inseparable but in digital evidence the problem is that I have to assign this pen drive has a physical object a specific number, the physical content then the digital content also I have to specify a particular number, otherwise if I simply seize the pen drive it has got no value. so physical component number and a digital component a number, I will skip this, so basically I have to ensure that nothing is contaminated at the scene of crime so when I am seizing this pen drive nothing is contaminated inside, because even if a bit changes it can make a lot of changes. Technically speaking I have to seize this without opening this file... Opening this pen drive. The moment I open it as I said computer generated data will change lot of data in this pen drive. How do I ensure the integrity of an electronic document? IT act says that we have to use hash algorithms, we have two families of hash algorithms one is called MD series and the latest is MD 5, that is available in free domain free of cost, so we can use it free of cost. The other is SHA SECURED HASH algorithm, it is patented algorithm, each time you use you have to pay for it to the RSA Company. Now these are brought for characters. The first is it says the evidence may be of any size, it may be one character it may be one terabyte of hard disk. When I run this algorithm it will return me a fixed length number, so irrespective of size of the evidence it will give me a fixed number that is called message digest. I will show you a demonstration of this. Now message digest is a random generated number meaning thereby without running the hash algorithm I cannot tell what would be the message digest of this pen drive. it is a totally random generated number, but there is uniqueness in the randomness that so long as the contents don't change you apply this algorithm anywhere in the world on any computer it will give me back the same random number. So if the evidence has not changed the random number will be the same. Even if a small change is made the random number will change, the message digest will change. What would be the quantum of change is also random, so it is not that each time I insert an A it will change by hundred steps. One it may change hundred step or one step may change thousand steps. the last is there is no particular way to know by looking at the message digest what the original content is, so reverse is not possible and the probability is so high, that two document.. Two evidence will not have the same hash functions. It is fixed, so if the hash function is same that means both the documents, both the evidences are exactly the same, I will show you it is very easy to run but very difficult to integrate into working. So I will use this document same document, now this is ashok... This is a hash calculator I lock this file. This is the message digest. This is a 256 message digest. Nothing happens to the evidence, this file remains the same. I can open it, I can analyses it, so I have opened it analyzed it, I have shut it back. I again apply, it will return me the same number. 9A039 this is totally random it will keep on returning me this number so long evidence is not changed. So we use this for seizing evidence. So basically what I do is I will hash this through an application software and digital seizure memo, now if something is changed I will just introduce a blank

Participant: if you send this to somebody, that person doesn't change it but tries to take off hash tag will it respond to your hash only.

Mr. Dohre: yes sir! If I send this file, if I give this file to you and you hash it in your computer it will give you the same hash. You take it to America you put it in an African computer it will give you the same value. If the Indians have not changed, if the file does not change. So I have introduced a blank, I save it now if I hash it the number would have changed. See A9550, so even this change is random now, this is how I use it for my forensics

Participant: how do you generate it for same drive itself?

Mr. dohre: I will give a practical demonstration.. Just five minutes...

Participant: yes 1 sure

Mr. dohre: so this is an electronic record sir, hash it generate a message digest nothing happens to the record, I make a bundle of it, so I hash it make a bundle of it sir and I present both these things to the court of law sir. Now when the arguments come let us the defiance council says this file was not there in the evidence all what the court has to do is it hashes the electronic record I have submitted generates a message digest, if the message digest I have given doesn't match he rejects the evidence and if it matches the defense council's plead fails. Now I come to the demonstration of this software how we implement this hash value and everything. It’s a software developed by ministry of information .It has got free components. One is to seize the word file evidence that is what on the RAM and the other what you called as the disk forensics, now this is how a computer works, we never work on a permanent memory. So we never work on a hard disk or pen drive. let me start a computer what we want to work on is pulled on to the run then we work on the RAM giving commands to the CPU receiving the changes so when I am typing a letter I am typing it on the RAM and not on the hard disk now I don't want to save it the RAM will simply discard it. it will not send it to the hard disk only on my command it will send it to the hard disk and it will be saved there so surprisingly for an IO what is on the RAM is more important then what is on the hard disk. People will normally ask me a question sir, it was a case of a pornography and we have seize the CD and the computer so we should be Challan. Can be Challan for the person seizes a computer and a CD... NO because like pornographic material in my custody is not crime but it becomes a crime only when I am showing it to someone... So I have

Mr. Dohre: so I have to just prove that the CD was running on this computer when the raid took place and it was running on the computer can only be proved when I see it being run. so before two years or so you did not have the software to seize the RAM fortunately now we have, so that you can seize the RAM also and I will show it I will demonstrate that lots and lots of information is contained in the RAM, so earlier we used to tell our IOs to take a photograph of the thing screen because at the bottom you have all what is running but now the software does it. I have prepared something, now this software comes on a small pen drive it is called ringlet as I said I should not change anything on the scene of crime, so I am not supposed to touch the criminal's computer, this is the criminal's computer the moment I insert it. it will start all the run, but since I was part of the team which made it we have disabled the particular component of this software, so it will not work automatically just for the demonstration purpose, I will demonstrate first it makes the seizure memo, then it gives an option what is to be seized then it seizes, so those components don't work in reality. I am inserting it here.

P**articipant**: this is a software developed in India itself

Mr. Dohre: yes! In India because at the starting I said we cannot use in the market, because we don't know the source code. This has been written by Indian people. We can depict in the courts of law. How it is working. so this is executable file of the software, now if you see this is just the seizure memo I will give it a name so national judicial academy RAM, police station number, seizure memo number, place of seizure, date, notes, suspect, address, witness I am just randomly typing something it hardly matters.. And see next see now the RAM contains all these things. the RAM will open all files network neighbourhood to all which this computer is connected its IP configuration, I will not seize all of them to save time I will just seize the let us say the PCs on- off time, screen capture and let us say.

Participant: open files

Mr. Dohre: next, now it is seizing everything, this is what it does and when it finishes it tells me so done, now let’s come to this, this is what it has stored so report it has made a report I can print it out. So see it is giving me all the hash values of required in formation, system information this is the hash value I can print it out get it signed by two witnesses and submit it in a court of law. Now we come to the acquired information so, this was the screen capture now, no need to photograph it, it has captured so it is giving me all. Open... I can have the PC on-off time also,

Participant: only thing I notice is the screen capture is not very clear...

Mr. Dohre: sir 1 that is only the enlarged one I can shorten it then I can give it you. Imaging. So PC on-off time. See it is maintaining a record ever since this computer was opened after 29Th July so on-of on-off, so it keeps a record by itself open files also, this is the systems information

Participant: do we need to require an internet to use this software?

Mr. Dohre: NO so it has all the information about this computer what is the PC... It is opening in the internet in the internet explorer because it has got lot of opening software, otherwise it is an external file. So it captures all the RAM which is relevant to us so processes. It will tell me Microsoft, power point is working and all these things. Lot of processes are running... Some where you will find power point also. Power point is running, I open one of the file in the MS word so it will tell me all the processes that are running so I can prove that this CD was also running. Now, coming to the last aspect that is seizure of the static data. so for seizing of static data I use five technologies, the software uses five technologies, and the whole process is divided into three components- first I will seize the evidence, then I am not supposed to work on evidence so I make an exact mirror copy of the evidence that is acquisition and then I will analyses. these three are distinct steps but to save time I will take first two steps together, and basically the technology I am using is first is right block whenever I am running this system the software the computer will not cannot write anything so I disable total computers writing capacity, so my evidence will not get changed at all, the second is a big stream look up or a backup, normally a computer reads one bite at a time, that was a primitive computer, then we had 16 bit computer, we had 32 bit computers, now we have 64 bit computers, now a days computer reads 8 bite at a time, but when I am doing the operation my computer will read only 1 bit at a time, so it will read each bit at a time it will store bit some where the numeric value 0101 and then it will use to hash it, similarly when I require it read this bit transfer it to my hard disk . It does it bit by bit and not bite. because when we read a bite we may read it wrongly,, or we may miss interpret also, the third is secured boot now once we start the computer there are certain instruction which are embedded on the microprocessor that cannot be changed so that is called bios, now, after this computer goes into two families one is the apple family the me cantos where the operating system is also embedded into the micro processing, so nobody can change the operating system so company is not the criminal the operating system is as pure as anything, you can run an apple computer without any fear and that is why they are costly, but with an IBM computer that is windows the operating system comes separately and it resides as software, so a criminal can change the function of the operating system, so in windows computers or IBM computers we cannot trust this operating system so I cannot run my seizure process on this particular operating system, so what I do is I before the criminal operating system load I will load the trusting operating system, this is essential because at time I may reach the scene of crime where I don't my computer so I have no other option but to use the criminal's operating system, this I will do, I will show you as I do it and this is the flow chart, during the seizure I have the evidence I read it bit by bit, all the bits I will collect somewhere I will generate a message digest this will write on a seizure memo, then in the lab or simultaneously I will read it bit by bit, transfer each bit to a destination , the file get the destination I hash it I compare it with the original hash, if it match that means this is the exact copy of the evidence, and lastly for analysis purpose I never open the original, but I open the copy I analyses it before analysis I hash it and then I analyses it, and if this gets spoiled I again make a copy . Now that is all I had to speak now I will make demonstration of all this. Just 10 minutes more. So let us say this is my suspected thin, I have to seize it I will show its contents. so it has got same pictures and the same file ashok, and another file called demo, now what the criminal had done is just before seizure he selects everything and he deletes it, now if I load this we see that the pen drive is empty so, and this empty.. So nothing is there on this pen drive. Now this is small pen drive which has second component of the cyber suit which is called true back, it is an imaging tool as well as seizure tool. True back component of cyber check suit. The whole set of software is called cyber check. the first one was will lift used to lift the RAM, the second is true back.it has an operating system now, when I shut this down the computer will load with this operating system and not with the windows, so I will shut it down. Now you see you do not load windows .so this is I am using criminal's computer to do my work because computer is defined by the operating system and not by the CPU, CPU is changed computer will not work, so for me it is as good as trusted system, now you see it has got options.. seize, acquire and seize and acquire I will do both the things together because I will save half of the time, so seize and acquire this is again the same, seizure memo thing so investigator's name tab address police station crime number, seizure number, date, suspects name, address, witness name, address, second witness name, address, notes if any.. so lab reference number because I am seizing it otherwise it is not there and the file name number NJA so next now it is telling me all the hard disks that are connected to the computer so first is the main hard disk second is through which I have booted and third is the suspect, it is 1 GB I will select it now it is asking me where to transfer the image so I transfer it to my hard disk and next. Now it is asking me various options some of them are technical so what hash I should use any compression for none, where the file would be and I say next. now it is re confirming the that I have submitted so if I want to change it I can go back otherwise I am confirming it as correct, next now it is reading bit by bit.. It is keeping in the pen drive to hash it is also transferring the image to my hard disk there also, it is keeping record of all the bits and will calculate message digest. When both of them match it will take it as a fixed... So it will take about two minutes or so. while handling digital evidence we have to be very patient we have to tell all the IOs to be patient it takes lot of time a tare bite hard disk, it may take roughly 8-9 hours top hash and repair a seizure memo, but when we do that we do not face all what we are facing today with respect to vyapam or something like that.

Participant: this technology that which we wants to settle down has it been implemented on police officers

Mr. Dohre: yes we are training all the police officers to do it and see that they are supporting the software that is centre for development for advanced computing and this given virtually free of cost to all the police organisation

Participant: is it available only for investigating purpose or as a court we can also ask for the same.

Mr. Dohre: yes! As a court also you can ask for the same. Total law enforcement can use it. So that includes judiciary.

Participant: discussing when any party or defiance present any electronic evidence to the court and then he want to receive it and keep it in the secure environment you will have to use.. Some methods of encryption.

Mr. Dohre: this is the scenario... but then there is a problem it is actually a very costly thing your normal hard disk that is magnetic in nature, if for a very long time it remains the earth magnetic field demagnetize it, because earth has a magnetic field so these things will get split lot, so for that there is a specific hard disk which.. Like magnetic particles are embedded in plastic thing so that they don't change over with the earth magnetic field so those hard disks are very costly. so if some evidence has to be kept for a long time let us say that case will go up to 7-8 years then we will have to use those hard disks or have a room which is non- magnetic- it does not permit magnetic radiant to come through.

Participant: all high courts, why it takes the administrative side all computers we prepare... We put pleadings, do we really encrypt that PC to keep files in hard copy. trial court is concerned just before I came... We have every emergency steps you need numbers. For all the e notes. There is one problem with the sub ordinate courts they keep typing the evidence by using computer. Nobody witnesses the line and the dash sign and two years later when the guy was gone... When the softcopy was asked it was not there. It was wiped up. So we lost completely the original evidence that was with the direction of the judicial sign so that he needs to preserve. And that has to be encrypted and also mailed that this evidence is of particular case and therefore the separate folder of the each case. Instructions even for the judicial work... so then when the document is generated on the computer we cannot afford to lose the soft copy and it should be in encrypted form.

Mr. Dohre: no sir! Encryption is ok but the simpler thing is that once a file has been completed it should be hashed. And the message digest should be kept somewhere so that whenever we re load it we first compare it with the hash

Participant: that is to be original, one system administers the thing for the entire thing

Mr. Dohre: no sir why I am insisting on the hash value is like you may not be able to dictate the whole judgement in one go so now what happens is you dictate 10 pages then you say come tomorrow but steno can change some relevant portion in the thing he has already typed

Participant: I am also looking at the administrative side

Mr. Dohre: now what happens is next day morning you start giving dictation from the 11th page and the judgement goes to the 34 pages after 3 days you may not recollect what all you had given on the first page so whenever a file is closed a hash of it should be kept somewhere. Then next day when it opened before typing it should be hashed and both the hash value should be compared

Participant: how do we do that?

Mr. Dohre: that is like having a small software like I am having

Participant: if is free or t has to buy for creating the hash tag

Mr. Dohre: MD 5 is available free of cost so that will save you the problem of going through all the 10-20 pages which you gave dictation 10 days back because encryption cause irritation. you encrypt a file and if he is really mischievous and changes 10 to 1 so all your things are gone because you cannot decrypt it now, so encryption is the best way sorry hash is the best way, write it down those 20 numbers next day again hash if they are saying then say now you start typing again.

Participant: this 01 is very important example because 0 added after a 1 without a decimal before has a value but 0 before a 1 without decimal point has no value.

Mr. Dohre: so we have done the seizure and acquisition is asking me to remove the pen drive. So I removed it I have kept it here. So technically I have not opened it. Ok. I do not want to seize any other drive because at times I may get 20- 30 CDs so I can continue I say no... Next. It is now creating a seizure report... so this is the seizure report. Now if we see this is the unique number of the physical media, this is unique to this pen drive physical aspect and at the end will see three hash values... so this is the hash value of the total media of the pen drive. It has split this media into the parts this is the hash value of all the blocks. it has even hashed the report so I cannot change the report also now I say next IO is supposed to write down these on the digital on the physical thing now it gives me a provision to print it out so if my computer is attached to a printer it will print out the seizure report or it will transfer it into a pen drive because we may

Participant: one simple mistake by the IO while writing down the hash value will

Mr. Dohre: so that is why it transfers it to a USB so. I transfer it to a USB I will insert this. I will say refresh and transfer it to other red pen drive I say ok. It is asking do you want to create more digital seizure memos. NO and my process is finished. And I exit. Now it is already in this hard disk you presume now this is in the run so I will run it in the normal windows environment and we will see the analysis part. Analysis part all the big scientists of this country. Have put it in. it does everything by itself. A person does not require any capabilities for running the analysis software. so let this computer starts I will show you the what is there in the digital seizure memo what was there in this file how we recovered back the deleted files what is in data,

Participant: what is the hard drive you were mentioning the special hard drive called. The plastic

Mr. Dohre: it is it was earlier used by the system called DIBS, they used to do the imaging on the DIBS, not much of progress has been done, but the vital evidence must be stored. Now a days we have those anti magnetic bags, so all the important things must be kept in that. Anti-static bags.

Participants: what is the price of these bags?

Mr. Dohre: it was very costly in 2001 I purchased one around 12,000 Rs. those disks are costly. now there are some other limitations also like for seizing one Tera bite hard disk there is a technical compulsion that the disk on which I am copying it has to be more than 1 Tera bite so.. do not have that hard disk in the market itself. How to strict into and store it. So

Participant: there could be forms of hard wares which are assistant to this kind of copying of a

Mr. Dohre: one of them is CD-ROM if it kept in what you say dust free environment. It does not get effected by magnetic field but then you don't have tera bite and two tera bites of hard disks CD-ROMs, so this is the only alternative way to be

Participant: I am talking of any let’s say the laptop has an inbuilt feature that makes it resistant to be copying using you’re... Like you want to make an image that I have a water melons can have a technology which will always there to take steps like that. So if in case i- phone 6 is very difficult to extract. Deleted stuff...

Mr. Dohre: from I-phone 6... It is possible

Participant: no no it is possible. What is in encrypted laptop?

Mr. Dohre: no encryption in itself is a problem, if you can break the encryption it is good. I-phone 6 total memory can be copied, the only thing is does not follow the normal data structure. The route directory and all that is not there. The bifurcation of the storage media is different. Celbride even does not extract data from many of the chines, it only does when the data structure is defined. Most of the Chinese cell phones does not follow the data structure. So cell bride even does not work for many 1000 rupees mobile phone manufactured in China. For computers how a hard disk will bifurcated is a normal standardized procedure. You have a boot sector, you have a route director, and you have all those things. So you can make generalize tools for computers. Mobile phone, the storage architecture has not been formalized over the world, so for specific thing you have to work with specific tools. It has the capability. We can recover it See operating system of an iPhone is a secret the output is not a secret.

Participant: data copying is not an issue. We are talking about the recovering deleted items from the iPhone let's not just stick to iPhone. I am talking about the IOS recovering deleted content is difficult

Mr. Dohre: see if the deleted content has been over written even in windows you cannot recover it

Participant: that is one aspect. Right, especially now a days use SSB hard wares which is much more difficult then recovering data from the normal hard ware.

Mr. Dohre: that is ok I agree with you. So it's specialized tools

Participant: India is in developing tool. And there is no tool as far as... Mobile forensic examination is concerned

Mr. Dohre: movie check is there in this computer I will show you developed by the

P**articipant**: that is only for the law enforcement agencies and not for the private parties.

Mr. Dohre: see governments serves only people..

Mr. Dohre: so what you are asking is... I will explain you what you and you are saying are data recovery tools and we are bothered about the data recovery tools we are bothered about the forensics, forensics has to be within the law. Give me a broken disk I will recover 010101 but law will not accept it. So why should I waste my energy in doing something which law does not accept... What you are saying is data recovery

Participant: no I am talking about the forensics

Participant: forensics... Laboratory across the country

Mr. Dohre: we discuss it afterwards. Even encase is not a forensic tool, forensic is the tool has to be within the legal framework. Then how can you say it is forensic tool. Encase does not prepare a seizure memo. Encase..pardon... Encase does not do it. I have worked on encase there is only one software in the world called I- LOOK which is used by the FDI which creates the seizure memo. That's all. Every other is a data recovery software. Encase is a data recovery software, for criminal case it is not accepted in the American courts. It is only accepted for civil litigation, and I am saying with an authority. So this is a seizure and an acquisition report which has been transferred into my pen drive and I take a printout get it signed by two witnesses sign myself. Submit it to a court all those things. Regarding the analysis portion it works with a dongle. Just two minutes and all magic is there. This is the analysis software,

Participant: this will help with the deleted files.

Mr. Dohre: it will give me proper picture of the hard disk. This is the interface so new investigator's name, password, reference number, file I think I have the name NJA, so now it is asking me where to export the things I extracted. See these are the files. So all the red files are deleted now, I have to just click on them this picture was there. This picture was there, this picture was there, this is what I was saying a Meta data, all this and it will continue for a very long time and this is what you were saying. Now this Meta data is very important. I will just give a small example. I create a file I password protect it, put it on a pen drive go to my office try to open that file, it ask me a password I give the password it opens. So where does the password lie? See when I am giving a password computer is checking it then only opening it so pen drive carries the password.. So password breaking is not a very problem for us, will actually analyses this Meta data, so it is there at the starting and at the end of the file. So all this is part of some other file. Then this is the Meta data. so this data contains all the information by what software it was written using which are, is it a MS office file ,it is a picture file, when it was created, which computer it was created, what is the password to open this file, so damaging the meta data is very bad and most of the things are lost.

Participant: this is not in binary form right?

Mr. Dohre: no this is not in binary form. This is in machine language. If you want to see the binary form, then this is 01 this is the exact the decimal display of that particular thing. It gives a very good thing of the whole disk. This file lying from this place to this place, so each of the square is called the sector or the page on the file, so I can, it is just the post-mortem of the whole disk. See I will lock this, this file is lying from this place to this place. At the starting you will find these, these are the characteristics of the file, how the characteristics how the disk is divided into sectors and all those things. So we use this particular component to give this physical media an identity the total content you have to give it to them. this software generates a report itself see I have not typed anything but it has already recorded what I loaded it, what is the version, I cannot write anything here, now suppose I am interested in this picture, so I have to just right click over it . Say append to report yes- both- ok I can add notes to it if I want. In the report I cannot add, here I can add it will get appended to the report. No-cancel-ok now if I see the report it has appended to me a report. With all the Meta data. And if I have done some analysis I can do the analysis also. Similarly I can do it for any other file. Append to report, and this append the report. So I need not write anything whatsoever interesting thing I get it will get appended and at the end of it I will save this report put it in a memory stick and give it to honourable court. So that’s what I had... Thank you very much.

Session 10

Mr. Patil: Good Morning everybody, today's topic for discussion is legal and procedural issues, more specific to interception of contained data. So what I would like to do, rather than talking too much of theory, I would share my thoughts based upon the life cases so that would help us better comprehend the reality. What I would do I would start again start with the same gyan. So on one slide I would not take more than 20 seconds for that because of paucity of time .So let us first understand what's the problem and then how are we trying to find the solution .Practically when we see that legal and procedural issues pertaining to the interception of data, we do not have a standard solution, we do not have one accepted standard set of procedure which is being applied by all agencies, different agencies are experimenting. There are two different types of procedures being adopted by different agencies both being correct, so that's why still people are experimenting with technology. So what is the problem statement, so problem statement is this, by Professor Harold A. Limestone? We are approaching the New Era with 21st century Technologies with 20th century governing processes and 19th century government structure. I don't know whether he made this statement as generic statement because I just tried to compare what's happening in India. The Indian penal code 1860 so it is 19 century so that's the governance structure if I call it and CrPc is 1974, so that is 20 century and it at the amended it in 2008 .So we are talking about reconciling the substantive codes, procedural codes and the reason why we're having discussion today is not just because this cybercrime investigation is restricted to only IT Act. Probably it is covering more questions related to Indian Penal Code, so if again for draw your attention to the first session day before yesterday when a definition of Cybercrimes that was adopted by South Africa. If we compare that, cybercrime is a crime in which computer is used either as a means or an end or both. So if we go by the that definitions then probably every crime is covered, every crime that we are facing with, it’s probably covered with some elements of IT Act and some elements of electronic evidence. I am going to discuss 2 case studies because I have time only of 45 minutes and I would not like to over shoot that and probably I will discuss lot of problems that we are facing every day, some of the day to day practical issues related to search and seizures, involving the interception of data. The first case is the investigation of 26/11 Mumbai terror attacks by Indian agencies and the second cases is intelligence operation which lead to arrest as well as conviction of David Coleman Headley. by here so what I have done I have attempted to visit FBI website, extracted only three or four critical lines from this and I'll try to understand whether as Indian agency if we start doing investigation what kind of challenges we will go through. Probably that would be an interesting discussion for of all of us, so that start with the investigation of 26/11. Now what is the issue of interception of data in this case? Now we would know that all this operation, while this operation was going on, Kasab and Abu Ismile, two in Oberoi, two in Nariman house and four in Taj were controlled by their handlers in Pakistan. They were talking to each other through a medium, unknown to Indian agencies. Of course it was being used on an individual basis but not for any organized crimes per se. That was Voice over Internet Protocol. Let us understand, this is very interesting discussion, this no need to write on anything. A graphical slide probably you would really appreciate this. So we talked about Lasker Commandants in Pakistan, so what we immediately think about is Hafiz Sayed, Sayed Salludin, so we have a typical image of a Lashkar Commandant in Pakistan. But what is happening right now, if anybody has read Frederick Forsyth books of God. In that book Taliban was advising all the Taleban supporters to adopt a new form, a new visible, it's the kind of attire, new expression, that is Takfirz. All Takfirz, they would be clean shaven, they would wear suit, they would wear tie but they would follow all the practices of Islam.

And I would keep on hating. They would be more hate full about westerners but this community would be known as Takfirz. This is what exactly ISI has done. It has issued a circular that please be clean shaven. Look wise like westerners so that you would not be identified by the investigating agency, so it to me the Lashkar commanders in Pakistan these days are like this. I am just comparing what happen on 26/11 so there was an Internet telephone known as voice over Internet protocol. It is a very technical name, common languages in Internet telephony. Ok so what happened some money transferred money by Western Union Money Transfer to a company known as Wlaksford that was in Germany that was in Belgium. Wlaksford had an office in New Jersey. All the transaction has happened to the office of New Jersey office. That company provided this number which number + 1201 253 182 400. This was VOIP number, which was hitting the international gateways for work for 3035 hours on the day. So what was happening technically all these calls with rooted to ILD gateway that is International long distance Gateway of India, can be intercepted that gateway, yes. Did we have capacity to intercept that gateway, yes? These calls with being made from an Internet telephony number to a regular mobile number so the call had to jump from ILD gateway to the mobile network and through the mobile switching station the call had to land on a mobile phone, that was a simple thing. That's why when the calls were being made to the hostages in Taj Oberoi, Nariman house we were able to intercept. Now what happens, intercepting is fine but when the agency started filing the charge sheet there were lots and lots of issues that I want to prove that this was a call made from Pakistan, what I am going to do. Now I am going to prove this is a challenge so what the agencies did, first was the testimony of Kasab .So I want to do the transaction end to end. What Kasab told that each of the 10 Terrorist will provided with one Nokia 1200 number with one sim card each .This is the information that was gather on the faithful night of 26/11 when the interrogation was parallel going on while the Agencies were fighting with the terrorists. So that would parable activity, what happened later, during investigation what was found only 5 out of the 10 mobile phones were identified. Where one or two mobile phones with identifying Oberoi, one belong to the lady victim. I am sure all of you would have read and would have seen that a couple was hiding in Oberoi. They accidentally left their mobile phones some of the relatives tried to call on that number and they realise that the phone was picked up by somebody. The lady called and through this we could actually identify the IMEI number and this was the first number intercepted at ATS headquarters. The second number was used with the Original Sim found in Oberoi. There were ten Nokia 1200 phones, with 10 sim card, so one of the 10 SIM cards that was originally provided to the terrorist got activated in Oberoi, so only one out of 10 SIM cards were used and duties that this was an Indian sim card. The Pakistan Handler, so that is a mystery, so there are conflicting stories, I may not be in a position to go into this. Some people say that this was failed Indian operation because they were knowing so intentionally these sim cards were planted but unfortunately before 26/11 none of the SIM card got activated. Indian Agencies were probably aware that there was something was happening with SIM cards were provided by upgrade IGP in Jammu Kashmir through one of the constables and through one of this sources in lashkar e Taiba but unfortunately this operation could not materialise because the phone sim card were never used before 26/11. Had they been used probably something positive would have come out. But it's Ok. 1 sim card was used in Taj one was used Nariman. You might have heard that there was one guy named Gabriel. He was brutally murdered .I'm sorry to say that I was at ATS head quarter listening to the conversation. At handler in Pakistan was actually giving instructions, Mar do isko. Early morning he receives a call and says Mar dun. And we can ear on telephone, that somebody screaming, somebody's being butchered. There is pin drop silence in the interception room that is happening, and his sim card that was probably inserted by the person. Probably, it was inserted before and before he was killed, then there was one unused mobile phone. On the day 1, mentioned that FBI had come to conduct an investigation so they identified one unused mobile with an unused sim card and they tried to do a data recovery from a partially burned sim card. So this is the actual seizure that we have done but can this seizure prove that these SIM cards and these mobiles belong to Pakistan. How do I prove it? I want to prove an international conspiracy, right. Five phones were recovered. Five out of the 10 mobile were recovered. Ok so what they have done, evidence submitted in the court of law. Look at this, first they have taken statement from Nokia India. So a senior officer form Nokia who hail from Gurgaon, he has given statement that none of the IMES had been even shipped to India and sold in India. Then ok officially, that's one. Could it suffice? NO. Then we have to go a step further. Then Global Nokia legal team was approached. They sit at this place in China named Doonga. People were approached, she sent an email to her Indian counterpart that 2 out of 5 IMEIs that we have recovered were sold in Pakistan. OK then there was a cross examination over video conferencing because we requested that lady to come to India. I didn't happen. So video conferencing was arranged when this lady was US and through video conferencing her testimony was recorded. Then of course the calls were being intercepted. The interception record of these calls, now there is a question of 65 B. Police, we are intercepting calls, who will provide. So these interceptions were provided along with the statement by the Inspector of ATS Mr N T Kadam. So this is what we did. The next question, the information that was provided by Kasab. The terrorist were asked to call on the VOIP number. I'm just going to split the first slide, the visual graphics representation into two parts. So Kasab told the terrorists were asked to call on the VOIP, this number as well as to long press the green button on Nokia 1200, so that it will be there will be an speed dial and the calls will be made to this number. This is what they were instructed .What happens next, what is the other findings during the investigation. The findings during   the investigation, gateway interception of calls from 4 IMEI numbers and multiple sim cards, already told. The VOIP servers, service provided was approached. Then KYC details were obtained. I am going to discuss in the next slide how is the KYC details were obtained and we have to also discuss whether it is possible in any other case to get details, in any normal case probably that is way impossible. What was evidence submitted. CDRs of 17 numbers, because agencies identified that all these 4 IMEI numbers because 5 were recovered, one was unused so there were 4. In all 17 sim cards were used. They try to use few SIM card but effective sim card used were only 4 or 5 but they attempted to use 17. Then from these CDRs, it only confirmed international calls. The problem is that when we take CDR of these numbers, it does not show me this number 120, it only shows that it is internet telephony because you only get an alpha numeric number in the CDR, so it can only prove to an extent that it is an internet telephony so this is a GPRS activity it is not a telephone activity, that’s all, nothing more than that. Then KYC record, it said that this number +120 had been, In the name of 1 subscribers Khadak Singh India. The way these people made my task difficult, sorry agencies’ task difficult, is that how to prove that this Khadak Singh is not the genuine Khadak Singh, then through FBI sources we obtained the passports that was submitted for getting this connection. The passport belonged to a Pakistani that was a big evidence. Then MoneyGram money transfer, so the fund transfer were not from Western Union sorry, I stand corrected, as far as 1st slide is concerned, it was through Money Gram. So we were really fortunate that they had sent money to the New Jersey branch because through API things became lot simpler and through that it could be identified through. Then the last and most critical which is the recent development, that Abu Jindal was arrested and after the arrest Abu Jindal that is Ansari, he said that he along with Washi and Tafa attended calls from Karachi. Abu Jindal is in Indian custody. So we have a voice sample of an Abu Jindal on 26/11.Now we have recent voice sample that case is going on currently. So this is still at investigation stage because Abu Jindal has recently been charge sheeted. The trial is still going on. Now there are certain issues that I would like to highlight, maybe that this discussion could be helpful. One it could not be proved basic technical evidence that the handle of a terrorist where receiving phone call from a Cell in Pakistan. See you have to prove that they were sitting under this tower and talking. Now this is technological infeasible because

Wok sworn informed that that did not maintaining any logs, without prior notice. Now this is typical BSNL activity. When we want CDRs from reliance, reliance provides. When you want CDRs of landline number of Tata Indicom, Tata Indicom provides. If you want CDRs of BSNL. BSNL says sorry please give us a prior notice then we'll start maintaining CDRs. Okay I don't know why the law is so different for BSNL. What is the advantage of not maintaining the logs but this is what is happening. So in this case also it said sorry doesn't happen. Now natural question merged for me, I am facing this problem in every case. Take the case of Ravi Pujari gang in Mumbai Ravi Pujari using Net network. It is a company in Malaysia. Now in case of Woks won, FB I could help in India agency. Now Qnet is a Malaysian company. It is routing its calls from somewhere in Indonesia. It is not maintaining any record. Ravi Pujari sits, somewhere in India or abroad and he keeps on threatening the businessmen. We do not have a clue as to where he is because the technology doesn't permit me to reach out to him. Next point , the KYC documents from the Woksvon as well as evidence from Money trail could not be obtained only because of the effective intervention of, could be obtains, sorry, only because of the , the effective intervention of API as the handlers admit them into the New Jersey. Next point, Mumbai police officer had to conduct visit to New Jersey. I know that there was a sanction for activity, May not happen for a normal case. May not happen for any other criminal organized crime. Then Nokia China legal representative, look at them. Now we are talking about 65 B certificate. Now this lady is sending an email to Nokia India office. This email is seized and submitted as an evidence in the Court of law. So we have to deal with this situation. Then the last point we are still awaiting the voice samples, so these are some of the practical issues. Now i would like to take you through another case of David Coleman Headley. It is a small case, might get over in 2-3 minutes. But that raises larger questions. What are these questions? Whether any evidence that is obtained through interception of emails would be or may be admissible in the court of law. Let us go through this. I would request one volunteer, if any of you Sir, if you can read out line by line, it would really help because that would keep all of us involved. Any one.

Participant: (reading from the slide) and at 5.12 pm (September 13, 2009), HEADLEY did a Google search for “Ilya’s Kashmiri “to read the latest reports. He repeated his search three days later on September 16 (2009) at 7.29 pm

Mr. Patil: In 2009 there was a rumour that Ilyas Kashmiri, who was no 3 of Al Quayeda, he was killed. So Ilyas Kashmiri was the handler of Hadley. Hadley got panicked. He called to his counterpart in Pakistan. Now he was worried whether, his call would get intercepted. Typically it happens with all of us, right, when we are talking on phone we are very careful. So he was talking and he said I heard that Doctor was married, he wanted to say I heard that Ilyas Kashmiri was buried. The other person on the other side said unfortunately yes then he said then what would happen to his family. So FBI was puzzled, if somebody is married then what would happen to your family. That was contradictory. Then next point, So 509 call ended 5:12 p.m. Headily did a Google search Ilyas Kashmiri, he did not do any search for doctor or Pir Sahab because you can use code words when you are talking to human beings, you can't use code word when you are talking with an idiot box .So computer would require a genuine word otherwise how would google help you. He did a genius Google search, only thing FBI concluded based upon this that these talks regarding doctor and Pir Sahab and Ilyas Kashmiri, they are part of same transaction because it just shut down phone and he typed on Google. So they are part of the same transaction. Next third point Sir.

Participant: On October 3 (2009), HEADLEY was off to Chicago O'Hare international airport on way to Pakistan, when FBI nabbed him.

Mr. Patil: Absolutely right Sir. So what happened actually, we are very good, in India in cell phone interception? Most of the agencies have a great team that can intercept telephone calls, analyse phone calls as well as integrate with google maps. I am going to show that as well today. If time permits of course. But what was additional thing that FBI was doing. They have integrated mechanism of interception. We do not have. We get GPRS data but as far as analysis of GPRS, I'll show you the screenshots as well, how GPRS is being analysed in our country. So they had an integrated analysed analysis based on which they could nab. Now the biggest question that is raised that as far as telephone interception is concerned, I am getting an approval under the Indian Telegraph Act. There is an competent authority named the home secretary or the union home secretary who authorises to intercept for one week without authorisation is possible, 2 months at a time which can be extended three times. So six month is the limit as per the Indian Telegraph act. Now the challenges is that we are in the process of creating an infrastructure for Internet monitoring, how this Infrastructures work .If we have a minute I can just explain to you. So what's happening I just give example of Mumbai? Suppose s Mumbai there are various Internet service provider MTNL, BSNL, VSNL then Airtel, Reliance. So these are the broadband operators. That would be many but I am just keeping myself to this list. How is happening MTNL doesn't have a gateway to MTNL uses BSNL Gateway. Ok. BSNL has its own gateway. Airtel has his own Gateway. Reliance has multiple gateways, the largest capacity is by my Reliance in this country. So typically the Agencies have started putting probes at these locations. What these probes are doing. They are replicating the data and they are allowing keyboard based searches so these probes are getting linked to an aggregation centre. This is all being done by the guidelines of one bodies known as TEC. Telecom Engineering Centre. From here law enforcement agencies can get a feeding. So this is a server. This is a client Take the case of any law enforcement agency. NIA or SID whatever it may be. They have got an interface so what they are doing in the morning we have checked about IP spoofing that in packet there is a source IP address, there is a destination IP address. This is a very very good software, it allows multiple types of searched, and it allows you to do searched based on an email id, user accounts, and Twitter accounts. So different types of searches are possible. So typically the Agencies are directly feeding the keywords and they are getting key words by key word based hits and they are storing as an evidence. Now I have a question over here. This is similar to what FBI has already done. This is at a nascent stage. May be after 5 years, once this pro installation is complete, we will start getting data. But unfortunately there is no regulator coming in picture. There is one regulator in framing the guideline. There is one regulator in designing, there is one agency like NTRO in providing technical support but this is all at agency level. Now what if the data gets intercepted and if that is produced as an evidence, who will provide the certificate to me. If I am intercepting Twitter data or Facebook data. Or data from trillion, who will provide me the certificate. Yes this is a very good thing, to get intelligence but will it be sufficient to prove an offence in the court of law, so that is a technical issue. OK I will take you through quickly maybe 5- 7 minutes because I have to finish by 11:45 maybe 11:50. Let us think about the types of interceptions in this country. One is lawful interception all of us are aware of. Then second is off the air interception. It was a fantastic method. It was solution to many many problems of law enforcement authority .Unfortunately Supreme Court has banned because of 1 mistake committed by NTRO that by mistake Amar Singh mobile call was captured and that created big big problems for the Agencies. I will tell you why because before this was happening many of the state agencies have started using this data, this machine for grabbing the entire Tower of say jails. Rather than preventing the criminals of using phone or mobile phone allowed them. Use telephones I will install this machine, start grabbing the entire tower, start intercepting all the calls, irrespective of whatever telephone you use. You may change your IMEI, you may change your iMEI number, I will keep on intercepting phone, that was a big big tool but unfortunately for the time being it is blocked. But Agencies have the capability, the machine are lying idle just waiting for some miracle to happen. Then monitoring of GPRS , 3G and interception Internet traffic is covered by the GR of agencies, if you have time permits, I would like to discuss but I don't think it will happen and of course intersection of landline phones . I will quickly take you through the mobile interception, what is happening and what is it heading towards .Most of the states starting interception with analogue voice logger and sometimes they have a Digital voice loggers but they have dial up connections , low bandwidth connection, problem is happening when you are intercepting a call. What is expected? Typically what happens very very rarely the Agencies have the suspect's phone number? Suspect is absconding. You intercept the e numbers of the family members of suspect, so if the suspect calls they can apprehend it that is the main reason. So analogue voice loggers are providing me the call immediately but what is more important that is known as IRI Intercept Related Information what is more important is CRI, that is call related information, what, who called from which tower he called, from which IMEI he called because other company is more important for some cases. Typical what is happening somebody's calling a girlfriend at 2 a.m. in the night, the constable would immediately wake SP and tell there is some call saying come meet? SP says, where this guy is, he says sorry sir will get to know tomorrow morning. Is this intelligence of any use? Many times we are filled but now what TEC has done. Let us go through that. Telecom engineering Centre has done, that there will be digital voice loggers with lease like connectivity, many of the agencies have started doing it. As per this GR, all telecom companies, it is mandatory to provide IRI and CRI together, means what, the moment call is intercepted I should be on the position to get who is calling, from which number, from which tower. So IMEI number, tower number and cell number, then additional data. Now the problem what is happening these days. What happens I am a criminal, my number is on interception, i suddenly decide that i should call somebody, I just click on something? I click and then I think no no it is dangerous to call, i cut it. This process is known as call initiation. As per the new GR, this is not even a missed call, this call is only latched up with the mobile tower and stopped, as per TEC Gr even call initiation has to be reported to the loggers. Then second is missed call of course I already told. Third is call on hold, this problem happens in old loggers. That I am calling somebody, I received a call, I put call on hold, I start talking to third person, then of course the people who are listening they fell three people are talking, either 1persons call is on hold or 3 calls are on conference, but this system should be in a position to provide me that one person is, Ravi Patil is talking to Sachin and Sachin has taken Vijay Nair on call and this three people are sitting at 3 location , so this information should be pushed together and it is being pushed together. Now what is the challenge, the challenge is that while at mobile service providers end procedure is compulsory, at Police officers level, procedure is optional so not many states have invested in logger. Then what is the second problem, you need a software, just pushing the data won't help. A kind of interface to analyse that data and produce the data in the format that is required by me and current reality is that every agency is doing its own business. Every agency is experimenting independently and that's why you may find out that one state has a different kind of setup so there would be multiple soft wares being incomplete that is a problem. Now let me take you through off the air interceptions, 1 minutes not more than that. What is off the air interception? Of the air interception is a process in which the apparatus is capable of all grabbing all the calls under a tower. These things can be done in 2 ways. One is known as passive GSM monitoring second is activity active monitoring. What is a passive GSM monitoring? I will give an example. Suppose in Arunachal Pradesh there is a very difficult terrain and agencies of chasing organised criminals. The towers are at longer distance, maybe few kilometres away from each other, so they need to continuously listen to the calls suppose, if they are chasing and they are 500 metres away and they should continuously monitor the calls. So this passive GSM does not, I would say does not grab entire tower , but even if the target is moving from one target to another, if they are able to identify the mobile number or IMEI they are in a position to grab the calls continuously when the target is moving, that is passive GSM. The problem with passive GSM is that there is one encryption, we have discussed a lot about encryption. In mobile phones also there is an Encryption. This encryption is known A 5.1 encryption. It is a very dangerous encryption. Vodafone Airtel have started using. I am sure by now many of the mobile service providers have implemented. Where passive GSM system is feeling every day, the second one is active GSM. This is particularly useful in the scenario like Taj and Oberoi, that target is idle, in 1 position. So the active GSM helps me to intercept call under one tower. It is when the target is not moving. What it does, it actually clones the BTS. BTS is nothing but Base Trans receiver Station. What it does suppose the original mobile tower is sending a signal at particular energy level. It will increase the wattage and take it to 40 WATS. Typical what happens if mobile phones identifies a stronger signal it will detach and it will latch to the nearest tower. So it is actually deceiving all the mobile phones in the area and forcing them to latch to your phone. What happens when the phones are latched automatically this encryption is overruled because my tower doesn't have, my BTS doesn't have encryption capabilities. So automatically all the calls of Vodafone and Airtel are decrypted and I can listen to the decrypted conversation. That is one. Secondly the beauty is that it can be integrated with location device so it is capable of telling me that this target is 300 metres distance in North-eastern direction and this information is very good. Imagine the case in Taj and Oberoi. If we would have got this information that probably they are between 14 to 16 floors, the things would have been a lot easier, lot faster. Ok next point. Sorry I am very fast, my sincere apologies. GPRS and 3 G interception. Only few slides. Ok at this, this is what the actual screenshot of GPRS interception is. What are we getting? We are getting, so this is a TCP protocol. Transmission Control protocol. Can you see this? This is TCP. Now I am only getting an IP address but agencies have to manually do a reverse look up and check. O he has configured a Gmail. Can I see the Gmail probably is the mobile service providers of pushing the actual email? But my software is not capable of reading that email. So it is big crisis as far as my software capabilities are concerned. No look at this. The second point... This is very interesting, this protocol, now nothing is lost there are few positive things. Look at this protocol. What is this? This is UDP. Ok. Union datagram Protocol. It is a broadcast protocol, anybody can grab it. And so long as you have a UDP, your software is capable of reading. What is mentioned? Mobile Maps. Content. Google.com. what is this? This is a Google Maps. The person is actually searching for some look location on Google map and you start getting real time interception and what your Agencies can do. Now this is one of the manual activity done by agency, still not integrated which GIS data but probably you will be happy to see. This is the cell site ID that I am getting. Ok. This is what is actually being done. So when you are intercepting GPRS data maybe that person is not calling but when he starts looking at some location, the moment the locational data is received it can be linked to this moment and we can probably predict that he is moving towards this direction. That's the benefit. This is more useful for intelligence activities other than the investigation and producing in the court of law. Another challenge that I want to highlight, is this software known as Nimbuzz. Nimbuzz Indian Mujahideen, now ISI has started another application but during Indian Mujahideen days Nimbuzz was continuously getting installed and they were sending Nimbuzz. These youth messages were UDP messages that means they are unencrypted messages .So there is a great opportunity to intercept s applications with the criminals me feel that ok they are out of reach of agencies but if there is good application with us probably such things can be intercepted. Okay Internet monitoring. There are three types of Internet monitoring. I have already discussed. I will just summarise. One of course is a real time Internet monitoring. That is a flagship project under NTRO. Dr Bhaskar is heading that project but technology at initial stage is still evolving. May be after 5 years after 10 years the situation would be different. Then of course obtaining back up data from service providers and ex-post facto analysis that is the standard process that we are doing. Unfortunately Gmail does not certified and I have not seen even a single case till now in which Google. Leave aside for civil, even for criminal case they don’t certified and they would only provide de facto information provided by Google is only the IP address and registration details. They do not provide either address book or mailbox data. What if you really want the address book or mail box data. They would request for MLAT which is not very easy. May be CBI can do it. NIA can do it. ATS can do it. Normal investigators district police out of reach. Monitoring incident response based upon threat assessment that is a somebody had asked question .What if somebody spoofed my website somebody create to look alike website that’s the mandate given to CERTEN Sachin and I have been to CERTEN and on multiple occasions and we have witnessed real time threat assessment. They keep on getting intelligence from other network resources also but internally also through IB or some other source they get an intelligence. They are capable of blocking that particular website. OK I will not deal with this. Probably I would like to spend 5 minutes on this because this is where that would be kind of most critical thing. Sir maximum 5 minutes Sir. One is legal challenges, transnational crimes. 2nd is privacy laws of foreign countries then of course I discussed about the technical capabilities of law enforcement Agencies. Now we want, we know that it's possible we don't have right software available or right capability with us. Then legal viability of investigating procedures. Now Dohre Sir had discussed about imaging. Now May times if imaging is done before seizure, it is question in the court of law because images from something very sacrosanct. It is supposed to be done only by the public servants who are not police officer so will that affect evidentiary value if the imaging is done before seizure. If there is a clarity of course the conviction rate will increase manifold if this particular point is clarified .Then like imagine, I have been discussing this point .Then of course Internet monitoring without any legal mandate given by, and unlike the way it is done under Indian Telegraph Act. They many a times we do not get, say for Facebook, Facebook is the movement somebody post office message after 15 minutes account is deleted. Facebook so sorry we are not maintaining because account is deleted so the only option left before is to take a screenshot before the account is delete. I will just give a recent example, Pathankot attack, this guy Maulana Masood Azhar posted a hate myself against India and he tagged to 12-13 people and the moment Indian government raised the issue Facebook suo moto deleted the account. Now we are left only with screenshots to prove the things. Facebook says sorry, we don't have data. This problem happens. Then regulatory challenges, maintenance of electronic records, now this is a very very big issue sir. I would really like to highlight Vodafone Airtel all service provider are maintaining 8 years CDRs because that is mandatory as per the audit procedures but when it comes to getting CDRs which are before 12 months they always give me the reason that as per the DoT regulation we are not supposed to provide after 12 months. Why are they not providing it because it will create a bad precedence? Then sometime CBI went to court and requested court, please issue orders under 92 CrPc then mobile service providers went offline and said please withdraw this petition we are going to provide you because they do not want to create kind of case law, precedence. But they have data for 8 years so why can't we force them to provide the data that is one. Then liability of private party in data preservation. It is a big issue, take the case of 2G spectrum, there would be multiple communication, take the case of competition commissioner, there are private parties. They can be forced to preserve their emails for 1 year at least. They can delete it .Lack of effective enforcement of TSCGR. As I mentioned, for mobile service providers it is compulsory, for police it is not compulsory. Nobody will allocate budget. I know that there are two districts in Maharashtra recently. One of them was Pegler. SP of that district was one batch junior to me. I used to ask, how you are functioning, he said. Sorry sir, I don't have digital loggers, i don't have loggers. By the time he was transferred no budget was allocated to him. That means he never intercepted even a single call during his tenure as a SP. Now network challenges. There are issues of network forensics. I will give an example. In Reebok fraud case. Email data was residing on server in Hong Kong. Now if you ask a sub inspector who was earlier a constable, now he has been promoted as a sub inspector, to seize a data from Hong Kong sitting in Delhi. What kind of procedure he should follow. It is big challenge. Then data stored on internet clouds, there is similar problem. Lack of adequate technology and image and analyse next gen mobile phone. I will again repeat the problems with I Phone. Now what has happened, the problem is not just with iPhone 5 or 6. Now on iPhone 5 also I can download the latest operating system of phone, latest version 9.1, 9.2. The moment I download 9.1, 9.2, technically it is like iPhone 6. Because ultimately it is not the hardware that is going to prevent me from imaging, it is the software that is going to prevent me from imaging. So with just one up gradation of my software, I have converted my IPhone 5 into 6 for practical purposes. So the plugin which was provided to me for IPhone 5 may not work on this phone now. So i had this. Any questions? Thank you so much. Sorry to be very very fast. Thank you so much.

Pavan Duggal: The last session should be very brief. So I will be very brief. But I think everything is already being covered. I thought I would just share some important cases that has happened which are very serious in terms of way forward as safeguards. First and foremost there are no magical formulas for safeguards. Primarily because the law is developing as we talk, the procedure, practices are all developing but let us take the latest case study that we have of Pathankot attack. Now if this kind of case would come to your Lordships and would be asked to look at it. We limit it to this kind of electronic evidence, where there would be phone calls which will be intercepted, recorded and produced by the prosecution. We don't exactly know how the prosecution will produce a 65B because there are challenges and of course depending on assuming somebody assuming them as xyz is arrested and is prosecuted. the defence is going to have an ammunition of materials to divert the prosecution including procedural aspects whether appropriate procedures were taken or not because national interest does not become a wiping kind of wand which can actually be used by just bypassing all procedures of law. That is the principle that Supreme Court has laid down, that what other judgements have primarily laid down but I thought a hypothetical case, if it was to come. It is too early, we do not even know what is coming up but if this was to come from judiciary stand point there will be large number of challenges. Number one ensuring that the electronic evidence was correctly picked up in accordance with law because the IT Act clearly says that the electronic evidence must be retained in the manner in which it was originally produced or in a manner which can be demonstrated to represent the information accurately originally generated. SO if the parameters of the IT Act are not complied with in terms of electronic evidence, then it will be the first thing the defence will come out with and the judge, the judiciary will have to deal with it. Second will be the issue pertaining to admissibility of electronic evidence. In this case, we do not know where they are originally intercepted. What is the exact location? How is relevant copies being made, the series being maintained and what kind of evidences have ultimately come into court of law? So these are hypothetical cases but challenges are going to be immense and of course unlike the actual world where we can bypass and short cut certain phases, in the electronic world it is going to be far more difficult, and far more complicated in terms of just the kind of issue the law is dealing. So the Indian Army website got hacked, so supposing this kind of case was to come before your Lordships, we are yet to see what kind of safeguards because everything is controlled within the army environment but still despite being on secured server the site gets hacked. So the relevant logs will have to be prepared. Again the relevant administrator will have to ensure compliance with 65 B but we do not know what kind of defence he is going to take but the challenges as I said are immense. No one principle is there, each case has its own particular facts. This company had a problem, the problem was that the salary accounts of employees were hacked and 50-60 lakhs of rupees were taken away. No unlike other company this company decided to reimburse the money and chose not to proceed forward. This man looks a noble man. He is doctor Prakash, former president of Indian orthopaedics association. One of the best orthopaedics in the country. He got arrested in Chennai in 2001 because he had a strange habit, he used to call people to his farm house in Chennai. Once people reached there they will be forced to strip, forced to engage in sexual acts. He will make blue films, he will take pictures and then uphold them on internet. He got picked up in December 2015. He got convicted for life imprisonment. Here there was electronic evidence, here there was physical evidence. He is the only document cybercriminal in India who has got a life imprisonment. Well because this is proper to the amendments coming in and he was convicted of other offences apart from the IT act 200. So these are some important cases and most of these cases present huge amount of challenges. I will take this second case. Here is a very page 3 personality. Let us call him Mr. John. Now he went to a party, somebody who is is own for a very string taste of wine and women. So Mr. X met Mr. John had a conversation and said can I have your number. So Mr. X got number of Mr. John but rather than saving the number as John actually went ahead and saved the number as Womaniser John. Few days later downloaded true caller as an app which goes into your address book, sends these data back then you have no control. This case the problem is whenever John is actually calling someone who has a true caller it would say womaniser John calling all the time. The matter was not registered, we have to work with the service provider. Work for 9 months to get the womaniser stuff out. But if these kind of matter was to be reported and was to come before the judiciary then there will be challenges because this was information which is transmitted through a mobile application. Then there will be additional layers of challenges Vis a Vis electronic evidence. Who will certify the output from the true caller mobile app was authentic, it was not tampered, altered. So there are going to be further challenges We Indians have a habit, we tend to forget. So we want to save the name with the exact adjective to make us recall who this person was. So there arose problems in this scenario. It got reported in the press but not reported to the police and much less would go towards the prosecution. But I think the fake recruitment scam is very very prominent these days. in top most companies, you will get people walking to your reception, they will carry your appointment letter, with your logo. They will say you have given appointment to us for Rs 35,000. Please allow us to join. But the company would then realise that it has become victim of cybercrime because these are online recruiters who tend to give an impression to the public that they are the company. In one case the recruiter actually represented that he is from Tata and called people for meeting. He actually rented out some space in a Tata building and called people actually for the interview. Got them interviewed so everybody thought I am going to Tata, this is Tata building, this is Tata letter and then subsequently he vanish. But in scenario like these challenges again will be how we will be able to get the evidence before the court and how we will be able to implement it. The last case is even more wonderful, this case was dealing with a 27 year old lawyer. There is a legal process out sourcing unit, in Gurgaon. They appointed this girl lawyer to be the manager. Now it was, there was open office on one side there was a chamber. So this girl being a manager was being given a chamber. In the night when she was on night duty she called one of the male colleagues and made love little did she realise that camera has recorded that entire exercise. So the next day she was picked she got called by the management and the management showed her what she has done last night and says you are the manager this is not what was expected. Either you resign or we remove you. So rather that doing that she shot 24 hours' time. She says I will come tomorrow. She does not go home. She goes to the local police station. Gets a case registered against the top management why because when you capture the images of private parts of somebody that is a specific offence under IT Act. In a scenario like this there will be further new challenges of the mind of evidence. first of all we will have to show that this spy camera by Mr. X then will be have to be show that this was working properly. Third it will have to be shown that there were no tampering, altering and fourth the issue will also be. If this kind of an evidence comes before court of law, we will have to potentially look at in camera proceeding because this kind of evidence will either be shown in the open court or cannot be allowed to be cross examined in the open court by the defence per se. Guruji was a very important music sergeant, this is few years back. If you wanted any Indian Song, you would go to guruju.com and you will get that song. T-Series told Guruji you have lot of my copyrighted songs. Please remove them. This is violation of my IPR. Guruji said do what you want. They filled criminal action against Guruji under the IT Act, under the copyright Act and the top management was arrested and the matter still continues. Prosecution is going to have challenges, how do you prove the relevant electronic evidence. Now this is a case that happened in civil domain but in this case somebody called nirmal baba, names that he is fraud or whatever so nirmal baba approached the Delhi high court saying that there is this defamation happening on internet, please stop it so the high court stops from defaming nirmal baba but the high court goes beyond. The High Court notices that nirmal baba is offering unscientific solutions to his solutions including having panipuri and getting God's kripa so high court actually restrains nirmal baba from offering unscientific solutions to his followers, but if this kind of matter was to come in criminal domain there will again be legal challenges of how the evidence because this evidence was on US server. This was foreign websites. The relevant outputs might still be taken in India and of course can be proved under 65B but the cross examination an open up Pandora's Box. It is not just normal people whose cases are likely to come before judiciary, there will be institutions. Here in this case the National Defence Academy, DRDO were hacked. The hackers actually hacked all emails accounts and put up on a website email accounts and passwords and openly claimed do what you can. No case was registered because getting that guy from Sweden, there would be new challenges but this is a very interesting case. 2014 December, this guy gets picked up from Bangalore. He is a normal guy working in a company. The Indian agency say that this guy is operating the Isis twitter handle and then he gets picked up. Case of cyber terrorism gets registered. Now the case is still under procedure but here there are new challenges. Though they have registered the case, there are challenges because the exact languages and parameters of 66F of IT Act would not be totally applicable and more so in the scenario like this, the prosecution is likely to put in lot of loopholes into the entire the entire problem. if you have a Gmail account accessed 10 years ago, try to access your first five emails, Gmail will take some time to locate it because it is looking somewhere to locate that and this big data is actually now providing them insight into your behaviour so if you are searching for terror, they will start showing you specific services which has got a connection with terror because that is where the big data analytic is happening. So over a period of time I expect that these issues would potentially come before the court but this is where the problem is. WhatsApp has become a national religion. Ask 10 smart phone users in India and out of them 10 will say that I have got WhatsApp but WhatsApp has created a huge problem. If you read the terms and conditions of WhatsApp they say all the data that you put on WhatsApp, all video, image, text is all public so there is no privacy. Number 2 getting WhatsApp data proved in the court of law is going to be challenged because ultimately it is through a mobile application that you download, but who is going to certify that there is no tampering in between. Practically speaking there are going to be challenges for judiciary and also for us. Because 65 B is not able to prove WhatsApp message. I think another one issue that judiciary should be concerned is the issue pertaining to dark net. It is not important in 2016 January but it will start getting more and more important. In one jurisdiction a judge was hearing a matter pertaining to cybercrime and he was into sentencing. The judge sentenced him to death and the judge got a death threat. The death threat originated from the dark net. Internet is an ice berg. The top 15-20 percentage of ice berg is what represents superficial internet. Beyond that there is a bigger portion where lot of stuff is indexed and you requires specific web search engines to do it but last 15-20 percentage represents the dark net where no search engine will go. You require specific specialized software known as the onion router. It will hide your identity behind various layers of anonymity so that you are unknown. Cybercrime is a way of service on dark net. Anything illegal that you can think off is available for sale on the dark net. Drugs, crime, guns, weapons, ammunitions, narcotics so much so that there are websites which says that we can kill anyone in the world barring the top ten most influential people, barring women and children. So till now law enforcement agencies have not been able to know that how we will deal with the dark net. Anonymity has created huge amount of practical challenges. I would expect more dark net related issues coming up before court. but the challenges of proving them is going to be anonymous because 65 B would be totally failing in the context of dark net because when your identity gets hidden being various layers there is going to be challenges on how you are going to prove the relevant nexus or the chain. 67 percentage of all Indians who are online today only access the internet through mobile devices so mobile web is big but mobile web brings new mobile crimes. I would expect more and more of these cases which are currently being unreported to start coming before courts of law. But again the challenges in those cases would be how you are able to pull out relevant mobile evidences. How will you be able to get them? Because service providers are not very very helpful. So cybercrimes is taking different ramifications. Silk route case that happened in US, has shown the practical difficulties like agencies etc., so challenges are immense and again there is no golden principle of this is what has to be followed. Each case has its own particular facts but I think some safeguards will have to be done. This is the guy Avnish Bajaj, he got picked up as a CEO of bazi for just a message that was put up on the website. He was tried for some time when the Supreme Court finally struck down his FIR on the ground that he was made party without a company or legal entity. But challenges are immense. This was a case where bank's network was used to send defamatory content against a former fiancé. She was identified, the bank was requested please do not do that, the bank took a moral stand saying that sorry this is a personal matter I will not interfere so a criminal case had to be registered against the bank and against the concerned employee who was sending defamatory content and the matter ultimately got settled down. Umashanker case is not a case from court of law, it is a case from an adjudicating officer which is a special authority under the IT Act. In this case ICICI bank was awarded damages, they were asked to pay 8 lacks rupees for their negligence in a phishing case because a NIRs account was phished. The NRI said return back the money the bank said nothing doing. Adjudicating officer found them by and large guilty. So one learning is very very apparent that the Indian Cyber law is becoming huge. When it was enacted in 2000, it was very small specific legislation aimed for promoting e-Commerce, but by the time we amended it in 2008, it has become an omnipotent legislation, anything digital in India, anything electronic in India is covered under the IT Act. On top of it is the section 81 of the IT Act, it says it is special law and the provisions of this law shall prevail over anything inconsistent there will contained in any other law for the time being in force, so according to me it has become one of the 3 most important piece of legislation in Indian history, the other two being the Constitution and the IPC. Anything digital is being covered under this law. This has become so huge. So all electronic evidence, all cybercrime matters will ultimately have to make sure that the compliances with the provisions and principles of IT Act are put in place. They wanted to create a framework for electronic governance, they did that. But like a Bollywood masala film, they added a chapter on cybercrime in the year 2000. They enhanced the chapter in 2008 so now various cybercrimes are covered under the law but the law enforcement agencies are still not comfortable with this law even after 15 years. They would be more comfortable registering cases under the IPC rather the it act but these four laws got amended but the amendment to this evidence act was what I thought most critical and crucial. The amendments was done in 2000. Today's 2016 realities are completely different. For example the electronic contracts are completely legal, so you are likely to get more cases where there is breach of electronic contract. I would like to conclude by some basic safeguards which could be useful as you go forward while dealing with cybercrimes matter. So first there is no choice. Compliance with 65 B is mandatory. This is despite the fact that 65 A says that electronic evidence may be proved in any other manner and 65 B only gives us one de facto method for proving the electronic evidence. So Supreme Court says after Anwar vs Basheer no choice 65 B compliance, then proceed, if you do not, if any one of the requirement not complied with entire electronic evidence thrown into the waste paper basket. It could not be appreciated at all. As time passes 65 B has to be relooked at, mobile evidence we are not able to prove 65 B even our best case scenarios because the conditions were written keeping in mind a computer networked world. The condition in 2000 were never made keeping in mind these mobiles Second safeguard I thought that these mobile devices related electronic evidences will have to be relooked. The government is working on a new law to revisit on this electronic evidence issue and may be they will be able to come up with new requirement on electronic mobile evidence. Currently 6 does not get fulfilled in mobile application based evidence format. Third, safeguards from the courts perspective is that courts should now adopt a very liberal approach of allowing detailed cross examination under 65 B because 65 B has opened up a new era in our lives. Earlier cross examination was very simple now as a guy gives a 65 B certificate he gets exposed to a very technical cross examination. I think it will be good idea to allow the defence to have a detailed cross examination because the Supreme Court has identified two phases for electrocute evidence. Phase 1 admissibility phase 2 genuineness. Detailed cross examination is very necessary and in various cases that i have done, I found out that the witness dies not come prepared. Majority of these nodal officers have no clue that who has taken what evidence from where, what certificates they are giving. What kinds of technical requirements are there so the problem is this? If we allow detailed cross examination we will have less convictions. But the problem is that if we do not allow cross examination we increase the level of litigation because the guy who was deprived of cross examination will utilize it as a n opportunity of going up and delaying the criminal trial per se. This genuineness issue that the Supreme Court has said, we have seen more clarity in Anwar vs Basheer. They have only touched up on the fact of genuineness but they have not detailed the parameters of what all is to be kept in mind while dealing with genuineness. Judiciary will have to come up with its own rules pertaining to dealing with genuineness of the electronic evidence. This is one safeguard which invariably isn't done which is need for appropriate preservation of electronic evidence in accordance with the IT Act, most of the time the electronic evidence gets picked up but is not either retained in the manner that the It Act provides under section 7 so that could be one challenge that any of the party could raise before the court and the court could be asked to adjudicate on the preservation of electronic evidence. Earlier you saw cases where floppy were collected and then a sua was put in the floppies to tie it along the case file, destroying the electronic evidence. We saw cases where scratches were deliberately put on the CD. We saw cases where hard disks were sealed with hot lax, thereby completely destroying the magnetic field. We have now seen new methodology coming. They give you some high quality magnets so the new technology that has come is, you get these magnets and supposing the electronic evidence is given, you do nothing you just ensure that your high density magnet is just swiped a couple of times around the evidence. That is enough to destroy the magnetic field. One that is destroyed the entire evidence becomes inadmissible or it does not even become capable of getting opened up. This is what clients keep on telling us. So there will be issues that will have to be appropriately addresses regarding these. Issue will be, intermediaries can be utilized for ensuring that they produce the evidence. Lot of time the prosecution will not be in a position to get all the evidence that the court needs for conviction and here I think more proactive role can be done by going into the routes of intermediaries. They are mandated to maintain data logs, electronic records. The IT act has substantially empowered the courts. Section 75 clearly says. Majority of these guys, the criminals are taking the servers located outside India for obvious reasons that is the reason we are not going to go any further. The matter dies off. China has started taking a different approach, China is saying you want to operate in china, comply with my law, otherwise don't so Google choose not to comply and Google was thrown out of China. I think India needs to take apolitical Act here. IT Act empowered but limited point. Most of these guys practical. Today when we give them notice under the It Act, sorry we give them court order, they say sorry this is not a normal court order, get me a US court order so they go around and round. By the time you get these orders they say the evidence is not evaporated. I will actually close by saying there is need for holistic interpretation and only in compliance with the existing law and principles the judiciary will go forward in effectively tacking cybercrimes, in ensuring cybercrime convictions. We have very poor rate, single digits or double digits but lots needs to be done. Justice Muralidhar: 90 percentage of these cybercrimes are not being registered and we lack the capacity to investigate cybercrimes. I think this is the harsh reality. Getting them registered as cybercrimes is a herculean task.

Mr. Duggal: Sir, I am the adviser to the Gurgaon police and the unofficial instructions we get is, we are not registering cases, tell us how not to register cases and we did a survey few years back. We found that for every 500 instances of cybercrimes only 50 were reported to the police and out of 50 only 1 gets registered as an FIR. So under reporting is by and large very much. I know of a case where with great difficultly the guy was able to get an FIR registered. The investigating officer did huge amount of work and after the challan the IO goes to the concerned client and says I have done lot of work what is my reward. So the guy says, I have been harassed, I have been the target of all the cybercrimes and you come back to me for reward? So practically there are huge challenges that are there. More citizen friendly approach has to be done as you go forward. We have very limited tied hands how do we proceed forward and that is a practical challenge but the law will have to develop with time. Thank You. It was my pleasure talking to you your Lordships. Thank you.