TRAINING PROGRAMME
FOR
MYANMAR JUDGES
7TH DECEMBER 2022 AT NATIONAL JUDICIAL ACADEMY (NJA), BHOPAL

ELECTRONIC EVIDENCE:

NEW HORIZONS, COLLECTION, PRESERVATION & APPRECIATION

CYBER SECURITY CORPORATION

- DR. HAROLD D'COSTA

President - Cyber Security Corporation
Advisor - Law Enforcement Agencies
International Trainer - Judges & Public Prosecutors

WHO OWNS THE INTERNET?

No one actually owns the Internet, and no single person or organization controls the Internet in its entirety.

ELECTRONIC EVIDENCE

The term ‘Electronic Evidence’ signifies a piece of evidence generated by some mechanical or electronic processes which is often relevant in proving or disproving a fact or fact at issue, the information that constitutes evidence before the court. Electronic Evidence is commonly known as Digital evidence.

IT ACT 2000 – CHAPTER III
ELECTRONIC GOVERNANCE

Legal Recognition of Electronic Records.—Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is–

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference

IT ACT 2000 – CHAPTER XII-A
EXAMINER OF ELECTRONIC EVIDENCE

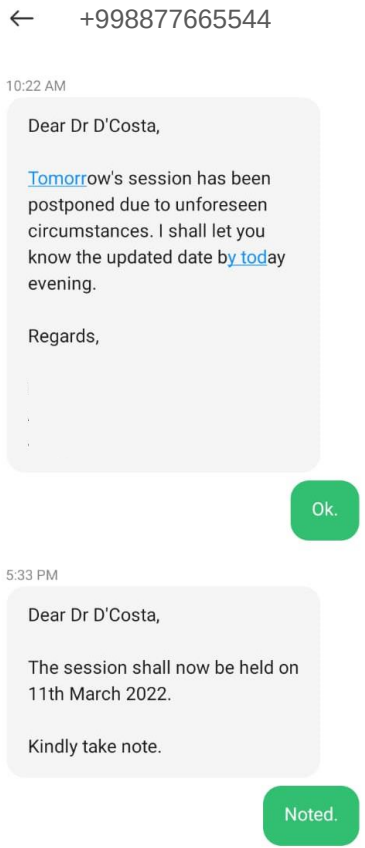
Central Government to notify Examiner of Electronic Evidence – The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the Official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

WHATSAPP CHAT MODIFICATION

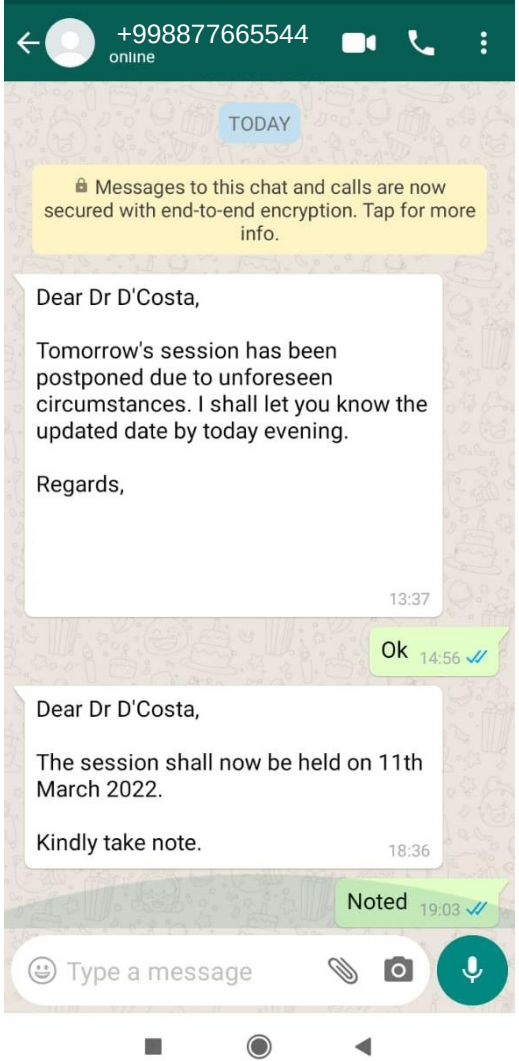
Even with end-to-end encryption WhatsApp messages can be modified

MESSAGE DATE AND TIME MODIFICATION

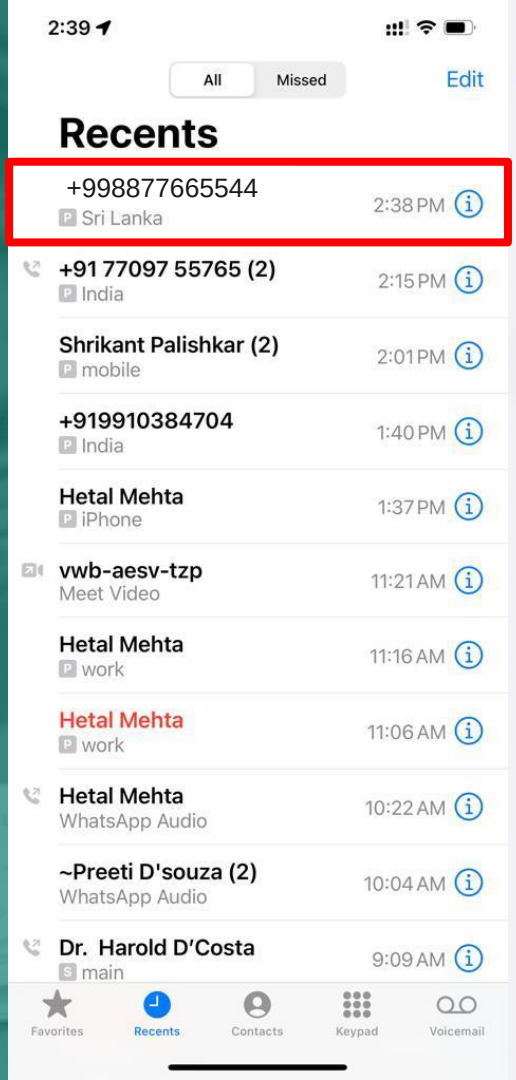
Message date and time can also be fabricated to show that message has been received before/after the original date and time.

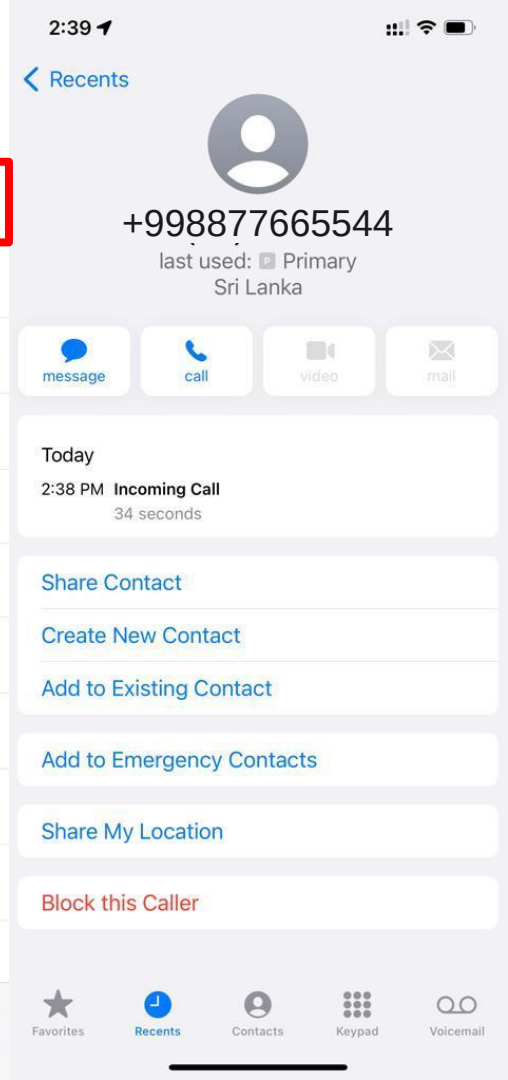


WHATSAPP MESSAGE SPOOFING



CALLER ID SPOOFING





EMAIL SPOOFING

Kayomarz Anklesvaria <support@cybersolution.in>

Session Postponed

ABC DEF - <office@gmail.com Fri, Feb 25, 2022 at 2:30 PM

To: support@cybersolution.in

Dear Dr. D'Costa,

The session scheduled on 26th February 2022 has been postponed to 11th March 2022 due to unforeseen circumstances.

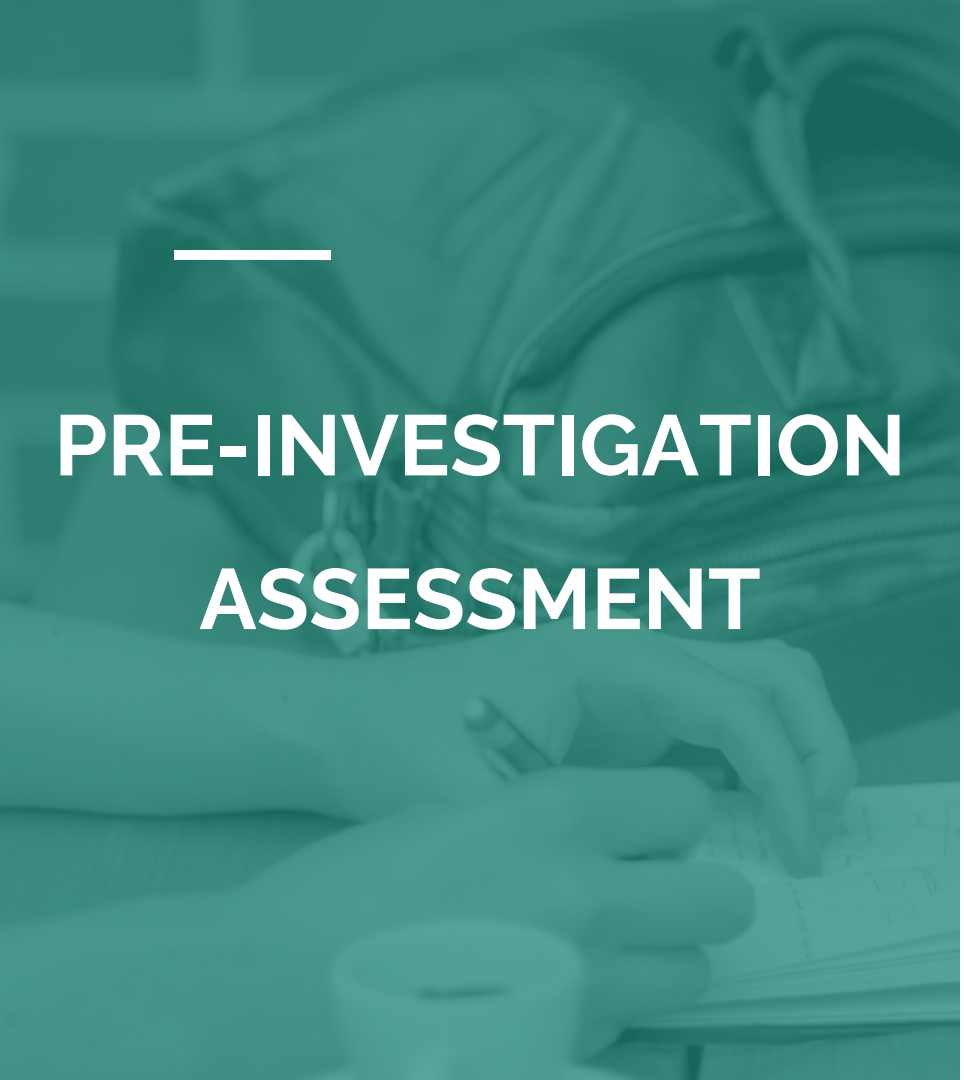
Kindly take note of the same.

Thanks & Regards,

PROCEDURE FOR COLLECTION OF CYBER EVIDENCE

Steps for Cyber Investigation:-

I. Pre-investigation Assessment
II. Evaluation of Scene of Crime
III. Collection of Physical Evidences
IV. Precaution for collecting digital evidences
V. Collection of Digital Evidences
VI. Forensic duplication
VII. Seizure of digital Evidence
VIII. Packaging, Labelling and transportation
IX. Legal procedure after seizure
X. Gathering information from various agencies



PRE-INVESTIGATION ASSESSMENT

I. Collection of all necessary information like:
   i) profiles of the suspect,
   ii) location,
   iii) circumstances,
   iv) computer system

II. Collection should be done by In-charge/cyber cell (Investigating Officer)

III. Analyzing scope of the offence and its possible outcomes.

EVALUATION OF THE SCENE OF CRIME

- Crime scene should be evaluated properly before collection of evidences.
- Digital evidences are very volatile in nature and could be available in number of devices, locations and formats.
- Evidences like number of computer system, type of connection (Wi-Fi, Ethernet), personal appliances and computer peripherals should be noted and photographed.

Categories of Crime Scene:

I. House of an individual having one or more computer network.
II. Office or coffee shop of an individual or company.
III. Public place

COLLECTION OF PHYSICAL EVIDENCES

- Identification and collection of potential evidences from crime scene.
- Evidences include- receipts of cyber appliances, left behind diaries, notes/password on slip, e-mail IDs, contact numbers or bank account number.
- Noting and sketching position of various equipment's at crime scene. For e.g. a mouse at left hand side of keyboard may indicate the user being dexterous.

PRECAUTION TO BE TAKEN WHILE COLLECTING DIGITAL EVIDENCES

- Minor mishandling may corrupt or vanish the evidence.
- Without proper documentation evidence may not be admissible in court of law.
- Special skills are required for leveling and preserving of digital evidence.
- Chain of custody should be prepared to identify who handled the evidence.
- A proper documentation like the Digital evidence form should be done separately for every device.
- Serial number of devices should be properly documented.

COLLECTION OF DIGITAL EVIDENCE

Switched off system:

- Disconnect all network connections. Allow printers to finish printing (if any).
- Label and photograph all components.
- Ask users for passwords, Operating Systems, details of other users and off-site data storage.
- The suspected drive should be connected using wire block device only for investigation.

Switched on System:

- Disconnect all network connection.
- Label and photograph all components.
- Ask users for passwords, Operating Systems, details of other users and off-site data storage.
- Use live forensic tools to collect evidence present in the RAM.

Cellphone:

- If device is switched off, do not turn it on and if it is on put it on flight mode.
- Photograph, label the device and screen display.
- Use Faraday bags for storing of evidence.
- Keep the device charged, record every activity with photograph and time.

FORENSIC DUPLICATION

In forensics duplication, the data should be copied accurately without making any change to it.
It can be done by following ways:

Logical backup

In this method, deleted files and residual data present in the device is not captured, it only capture and copies the directory and files of a logical volume.

Bit stream imaging

It is also known as imaging or cloning
It is a bit-by-bit copy of an original media.

Write blocker

It is a hardware or software tool which forbids computer writing on a storage media.

PRECAUTIONS:

- **The copied data should be exact copy of the original data so that the integrity of the data is maintained.**
- **To ensure integrity, hash value of the copied data should be calculated.**

SEIZURE OF DIGITAL EVIDENCES

It involves the following:

- Calculating hash value of the suspect storage media.
- Creating a digital fingerprint (image / clone) of the same.
- Calculating hash value of forensic image.

PRECAUTIONS:

- Professional approach and guidelines should be followed by I.O to maintain reliability, integrity and legal relevance of the evidence.
- Write blockers should be used to avoid change in time stampings.
- Permanent sterile new physical media should be used.
- New media should be fire proof and tamper proof.
- If already used hard disk is used, existing data should be wiped off.
- After imaging data into media, it should be marked with unique exhibit number related to case which is computed through hash algorithm.
- This number should be, mentioned in panchnama.
- Hash valued of copied image and the original data should be exactly same.
- The seizure memo should be prepared .
- Digital evidences collected should be preserved in anti-static cover.

PACKAGING, LABELLING AND TRANSPORTATION

I. The collected evidences should be numbered and labelled properly for future use.
II. A tag should be attached to evidence which will display all the details about the evidence.
III. For packaging of evidence, proper material of suitable size should be used.
IV. Good quality evidence envelopes, faraday bags should be used instead of common plastic/gunny bags.
V. Each evidence should be packed separately to avoid damage to the evidence.
VI. During Transportation, the evidences should be kept away from the place of frequent mechanical shocks or with drastic temperature change.
VII. The evidence should be carried by only trained and authorized, messenger and not by courier/post.

LEGAL PROCEDURE AFTER SEIZURE

I. After seizure, documentation and transportation of digital evidence, permission from court should be obtained to keep evidence in custody.

II. Ensure that no original evidence related to case are returned to owner.

III. Even if court instructs to return the original evidence, try to impress upon that only an authentically imaged copy of evidence is provided to owner.

GATHERING INFORMATION FROM VARIOUS AGENCIES

Information preserved by internet service providers and other firms, can be obtained by legal request.

The officer can acquire such information as given below:

Telecom service provider(TSP)/ Internet service provider(ISP):

- Username
- Telephone number in case of DSL/CDMA/3G,4G and dial up
- Personal details like name, email ID, address etc. mentioned in CAF form.
- Day-wise activity i.e. when and how long used etc.
- Physical address of the IP address.

E-mail service provider:

- Username, user activity i.e. date and time of logged in and time it is active, etc.
- Details of all incoming and outgoing e-mails along with mails stored in draft folder.
- The IP address from where the email ID is accessed.
- Registered details (IP address, date and time, other services availed) etc.

GATHERING INFORMATION FROM VARIOUS AGENCIES

Mobile service provider

- Customer acquisition forms- personal details like name and address.
- Calling number, caller number, time, type of call (ISD/STD/Local/SMS etc.)
- Roaming to other cities, Tower Location and tower data.

Social networking sites

- Username.
- Personal details updated in the profile.
- The IP address from where the profile is accessed.
- User activity i.e. date and time of logged in and duration of the active sessions etc.
- Friends and group with which the user is associated.
- Email –IDs updated in the personal information.

GATHERING INFORMATION FROM VARIOUS AGENCIES

Financial Institutions/ Internet Banking Institutions

1. Personal details updated in the profile of the account holder
2. Transactional details
3. Supporting documents submitted by the customer along with the introducer details.
4. IP address in case of Internet Banking.

Website domain/ Hosting providers

1. Registration details, Access details, FTP logs
2. Payment details
3. Technical/administrative/owner of the domain
4. Details of website developer

VoIP service providers

1. Registration details, Access details,
2. IP addresses, Payment details,
3. Calling/Called numbers.

ADMISSIBILITY OF DIGITAL EVIDENCE

ADMISSIBILITY OF ELECTRONIC EVIDENCE

Evidence Act provides that evidence can be given regarding only facts in issue or of relevance. Whereas section 65A provides that the contents of electronic records may be proved in accordance with the provisions of Section 65B.

Section 65B provides that not withstanding that anything contained in the Evidence Act, any information contained in an electronic record, i.e. the contents of a document or communication printed on a paper that has been stored recorded and copied in optical or magnetic media produced by a computer output, is deemed to be a document admissible as evidence without further proof of the original's production, provided that the conditions in section 65B(2) to (5) are satisfied.

CONDITIONS FOR ADMISSIBILITY OF ELECTRONIC EVIDENCE

(a) The computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried over that period by person having lawful control over the use of the computer;

(b) During the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in ordinary course of the said activities;

(c) Throughout the material part of the said period the computer was operating properly, or if not, then in respect of any period, in which it was not operating properly or was out of operation during that part of time, was not such as to affect the electronic record or the accuracy of its contents; and

(d) The information contained in the electronic record reproduces or is derived from such information fed into the computer in ordinary course of the said activities.

EXPERT OPINION

A new section 79A of the IT Act 2000, which provides that the Central Government may, for the purpose of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the official Gazette, any department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Pramod Mahajan Murder Trial

The learned trial Court of Bombay, dismissed the submission that the SMS is inadmissible as valid evidence, as the practical demonstration was conducted by the defense witness who was “not a cyber expert” as per law.

APPRECIATION OF DIGITAL EVIDENCE

SECTION 65(B)(4)

Under the section 65(B)(4) the certificate which identifies the electronic record containing the statement and describes the manner in which it was produced giving the particulars of the device involved in the production of that records and deals with the conditions mentioned in Section 65(B)(2) and is signed by a person occupying a responsible official position in relation to the operation of the relevant device shall be evidence of any matter stated in the certificate.

CONTENTS OF THE CERTIFICATE

- Following points are the necessary to be covered in the certificate to prove the authenticity of the evidence.
- That the information contained in the hard disks of the mentioned electronic device was regularly recorded into them in the ordinary course of activity.
- That during the period in question the mentioned device were operating properly at all times and there have been no such operational problems so as to affect the accuracy of electronic record.
- That the computer hardware and software used in the computer system have built in security systems.

WHEN IS IT APPLICABLE?

- When signed by a person occupying a responsible official position in relation to operation of relevant device.

- Source, authenticity which are the two hallmarks pertaining to electronic record sought to be used as evidence.

- Only if the electronic record is duly produced in the terms of the Section 65-B of Indian Evidence Act, the question would arise as to the genuineness thereof and in that situation, resort can be made to Section 45A- opinion of examiner of electronic evidence.

TEMPLATE OF THE CERTIFICATE

Certificate u/s 65B of the Indian Evidence Act, 1872.

This is to certify that I, _____, residing at_____, state to the best of my knowledge and belief that I have extracted the images from a mobile device having following details:

DEVICE DETAILS	
MODEL NUMBER	
DEVICE NAME	
SIZE	
SERIAL NUMBER	
IMEI NUMBER	

I state that the device used for extracting the photos was functioning normally at all times.

I further state that the device utilized by me was used to store and process data and were operating properly and there is no distortion in the accuracy of the contents of the copies of the images.

The above is stated to the best of my knowledge and belief.

_____

CASES WHERE 65-B WAS NOT GIVEN,BUT THE EVIDENCE WAS CONSIDERED

24. Om Prakash v. State (decided on - 23.05.2014) Dr. S. Muralidhar, J.	High Court of	2014 SCC OnLine Del 3213 : (2014) 143 DRJ 349	True caller report is admissible. While it is correct that no certificate under Section 65B of the Indian Evidence Act has been produced by the defence, an important fact that has been overlooked is that DWs 2 and 4, when shown the Truecaller Details, admitted that they were correct as regards their own mobile numbers. Therefore, to that extent the TDs could not be rejected as being inadmissible.

TIME OF 65-B(4) CERTIFICATE

31. Avadut Waman Kushe v. State of Maharashtra (decided on - 03.03.2016) R. P. Sondurbaldota J.	High Court of Bombay	2016 SCC OnLineBom 3236	The certificate need not be filed at the time of production of the electronic record. It can be filed at the time when the evidence is tendered in evidence and that subsequent filing cannot reduce its effectiveness. Section 65B is about the admissibility of the electronic record and the not the production of it.

PRODUCTION OF A FRESH CERTIFICATE

33. Nyati Builders v Rajat Dinesh Chauhan (decided on - 18.12.2015) R. G. Ketkar, J.	High Court of Bombay	2015 SCC OnLineBom 7578	At the time of filing of electronic records (emails), certificate u/s 65B was not filed. The learned trial Judge via order, allowed application of plaintiffs to produce a fresh certificate. The issue of admissibility was kept open at the stage of final hearing and thus, emails were neither discarded nor admitted in evidence. The emails thereof, were treated as

PERSON COMPETENT TO PRODUCE THE CERTIFICATE

35. Shradha Shipping Co. v. Adhithri Trading Co. (decided on - 25.11.2014) U.V. Bakre, J.	High Court of Bombay	2014 SCC OnLine Bom 2273 : 2015 Cri LJ (NOC 483) 158	Certificate under Section 65B of the Evidence Act must be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) so that the electronic record produced can be taken as admissible evidence. Held, private consultant with no responsible official position and no free access to computer cannot issue a 65B certificate.

ELECTRONIC EVIDENCE AS PRIMARY EVIDENCE (NO CERTIFICATE REQUIRED)

12. Sunil Panchal v State of Rajasthan decided on - 03.06.2016) Mohammad Rafiq and Vijay Kumar Vyas, JJ.	High Court of Rajasthan	2016 SCC OnLine Raj 5140 : (2017) 1 RLW 566 : 2016 Cri LJ 4238 : (2016) 4 WLC 437	A tape-recorded cassette is a primary and direct evidence of what has been said and recorded. Difference between primary and secondary evidence is of utmost importance. Therefore, tape recorder attached to land line telephone to be considered, without a 65B certificate. Voice of accused recorded at the time when ransom call was made by him has matched with his voice recorded in another cassette.

MOBILE PHONE FALLS UNDER THE DEFINITION OF COMPUTER

64. Syed Asifuddin v. State of Andra Pradesh (decided on - 29.07.2005) V.V.S. Rao, J.	High Court of Andhra Pradesh	2005 SCC OnLine AP 1100 : 2005 Cri LJ 4314 : (2006) 1 AIR Kant R (NOC 4) 2 : (2006) 1 AIR Jhar R (NOC 4) 1	The judgment examines how a cell phone works and compares it to the definition of 'Computer' and 'Computer Network' under the IT Act, to hold that, "a cell phone is a computer which is programmed to do among others the function of receiving digital audio signals, convert it into analogue audio signal and also send analogue audio signals in a digital form externally by wireless technology."

DIRECTIONS ON ADMISSIBILITY OF EMAILS

67. Nidhi Kakkar **v.** MunishKakkar (decided on - 10.02.2011) K. Kannan, J.	High Court of Punjab and Haryana	2011 SCC OnLine P&H 2599 : (2011) 1 HLR 533	If the party denies having sent the email, a 65B certificate from the operator of the server of what the text contained will be required to authenticate the text of the transmission.

DR. HAROLD D'COSTA

+91-7709619249

hld@rediffmail.com

CYBER SECURITY CORPORATION