DIGITAL FORENSICS
COLLECTION, PRESERVATION
&
APPRECIATION OF ELECTRONIC EVIDENCE

Raja Vijayaraghavan
Judge
High Court of Kerala

What is digital/computer/electronic evidence?

- “Electronic form evidence” means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines-***explanation provided for the purpose of Section 79A of the IT Act, 2000***
- is “information and data of value to an investigation that is stored on, received, or transmitted by an electronic device” (National Institute of Justice [NIJ])
- Digital evidence is defined as information and data of value to an investigation that is stored on, received or transmitted by an electronic device- ***Electronic CSI, A Guide for First Responders, 2nd edition*****, National Institute of Justice, April 2008**

Simpler explanation

- Information that is stored/transmitted electronically is said to be “digital”-
- As it has been broken down into digits i.e-binary units of 0s & 1s
- That are saved and retrieved using a set of instructions by a software or code
- Which has probative value.

Digital evidence - Categories

- **Digital evidence**, also known as electronic evidence, is data or information that exists in digital format, that can be relied upon and used in a court of law. There are different types of digital evidence offering unique types of information.
- They are broadly categorized into two groups:

1. Evidence from data at rest (obtained from any device that stores digital information)
2. Data intercepted while being transmitted (interception of data transmission and communications) information that is stored/transmitted electronically is said to be “digital”-

- As it has been broken down into digits i.e-binary units of 0s & 1s
- That are saved and retrieved using a set of instructions by a software or code
- Which has probative value.

WHAT'S THE CHALLENGE ?

Digital evidence has a **wider scope**, can be **more personally sensitive**, **is mobile**, and **requires different training and tools** compared to physical evidence

- In today's "age of access" technology is present in every aspect of modern life.
- Almost every action contains a cyber element in it.
- Digital devices are used as a tool, target or both in the commission of crime.
- Digital/electronic evidence by its very nature, is fragile, easily alterable, damageable and easily destructible.
- It requires special tools to retrieve, requiring special precautions to properly collect, preserve, examine and worthy to be admissible in a Court of Law.

- Technology touches just about everything already and it is difficult to find a case today that does not have a nexus to computer technology.
- For example, evidence of crime can be tied to a cell phone or laptop, sent through email, posted on social media, or be something stored in the cloud or on a Dropbox account.

Now, Every Delhi District to Have a Cyber Crime Police Station Amid Rising Crime Rate

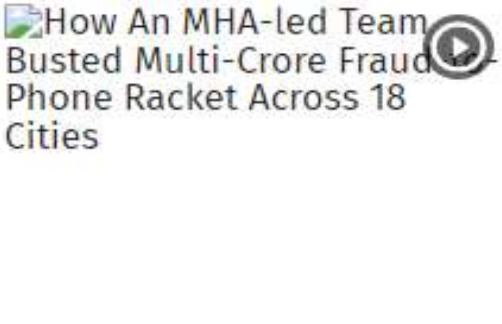
400% Increase in Cyber Crime Against Children in 2020 vs 2019, Most Cases of Sexual...

Eight Cybercriminals Arrested in Jharkhand's Deoghar District

15 Cybercriminals Arrested in Jharkhand's Deoghar

Govt Launches National Helpline to Report Cyber Fraud: Here's Everything You...

Imposter Asks Money via FB Account of Madhya Pradesh BJP Leader



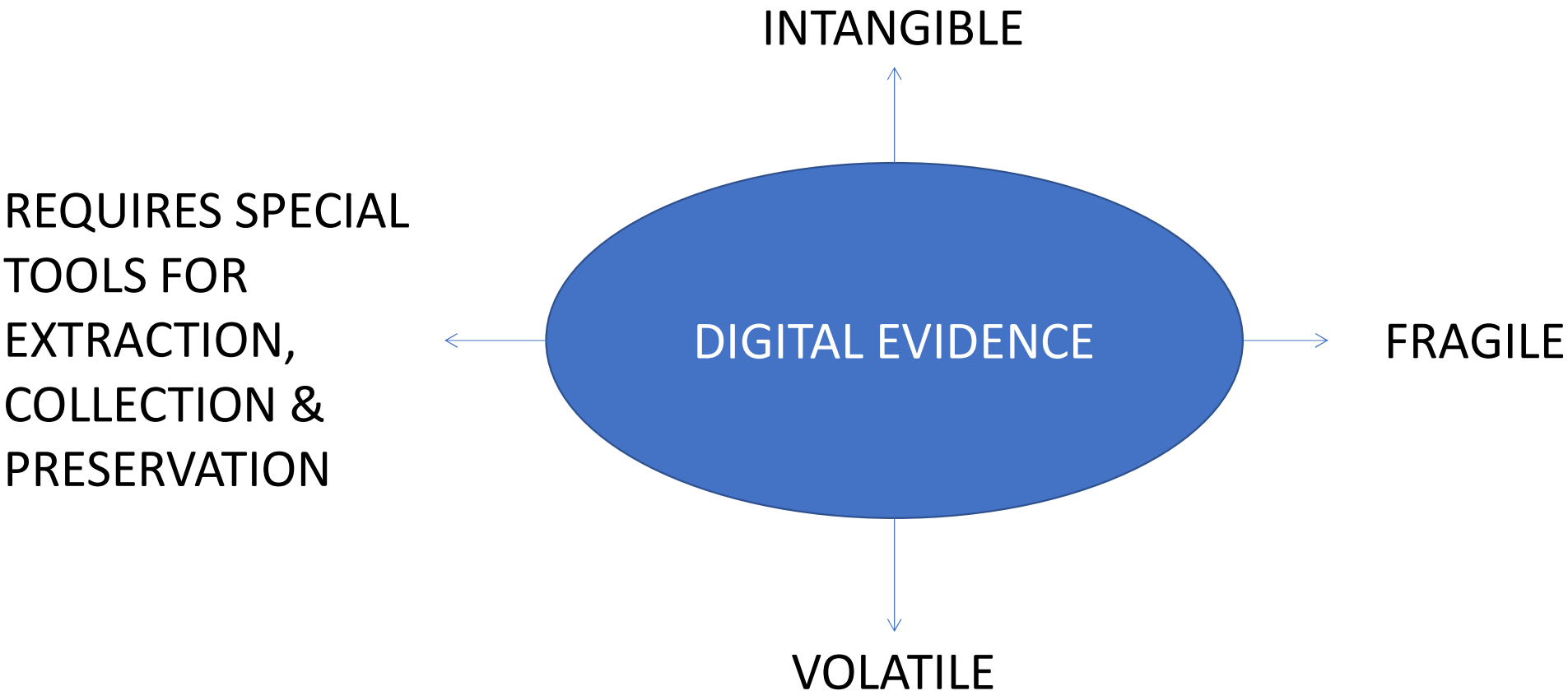
How An MHA-led Team Busted Multi-Crore Fraud-to-Phone Racket Across 18 Cities

Ransomware Attacks Increasing Due to Corporate Cyber Insurance, Call for...

Importance of digital evidence

- Activities in the digital realm leave digital traces – **think file fragments, activity logs, timestamps, metadata**, and so on – may be deemed to be of value, for any number of reasons.
- They may be **useful** as **evidence** in establishing the origins of a document or piece of software, for legal purposes in determining the activities of the parties involved in a criminal case, or even as a resource for cyber-criminals looking to reconstruct information or identifying credentials on their victims.
- The prolific usage of electronic devices such as smartphones and computers, **humongous amount of data generated** from these.
- As such, there can be an expectation within almost **any** investigation for the **need to identify digital evidence**.
- If identified, collected and analysed in a forensically sound manner, **electronic evidence can prove crucial to the outcome of criminal, civil and corporate investigations**.

Uniqueness of Electronic Evidence



Types of Digital Evidence

Digital Evidence Types

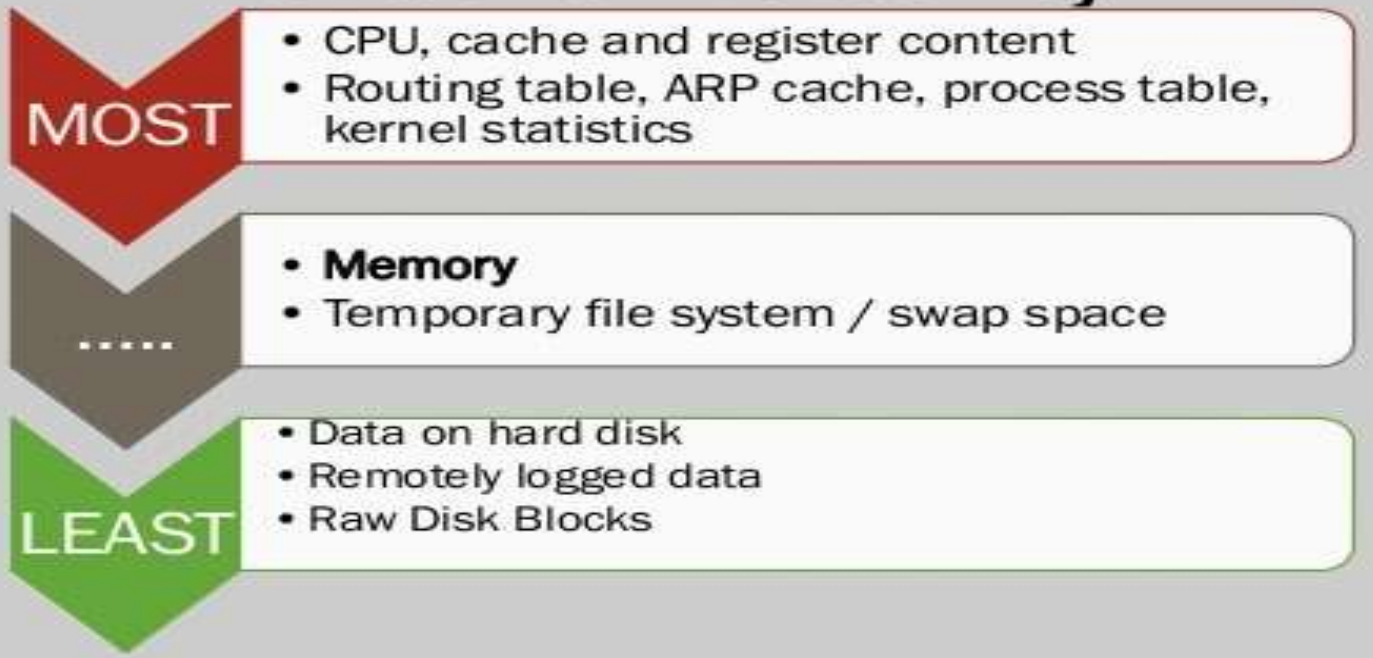
Volatile Evidence

- Memory
- Network Connections
- Running Process
- Open Files

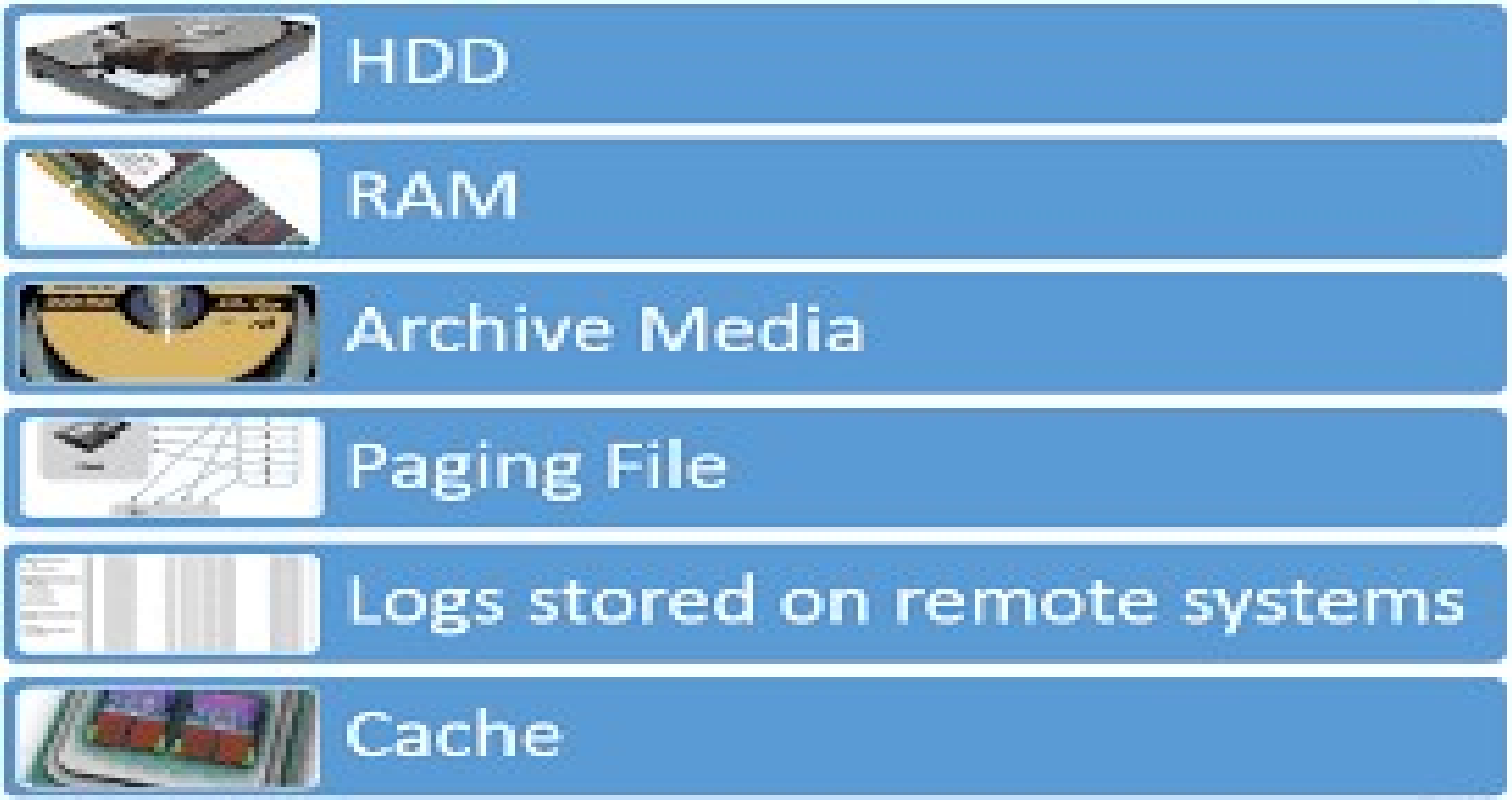
Non-Volatile Evidence

- Hard Drives
- USB Storage
- Floppy Disks
- CD/DVD

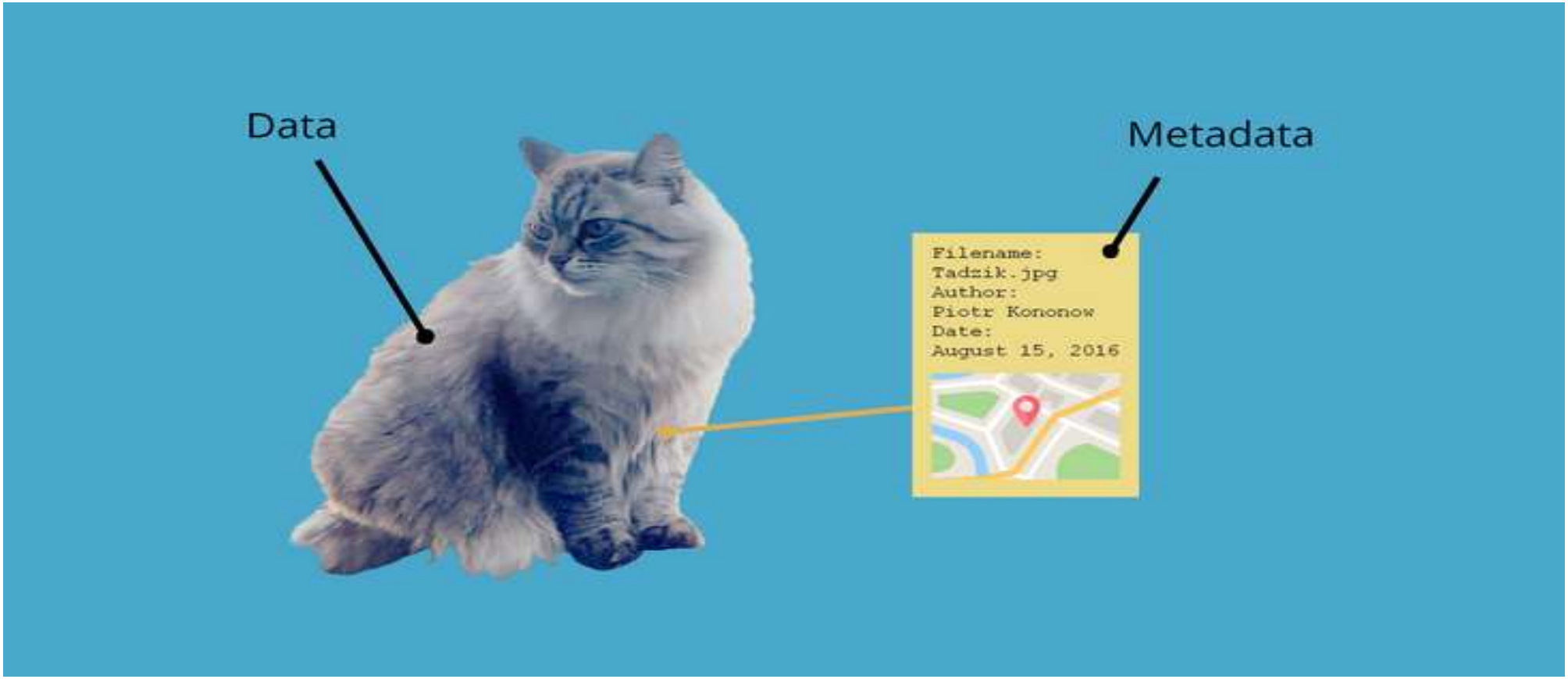
Order of Volatility



Non-Volatile Evidence



Meta Data


Data
Metadata
Filename:
Tadzik.jpg
Author:
Piotr Kononow
Date:
August 15, 2016

Types of evidence

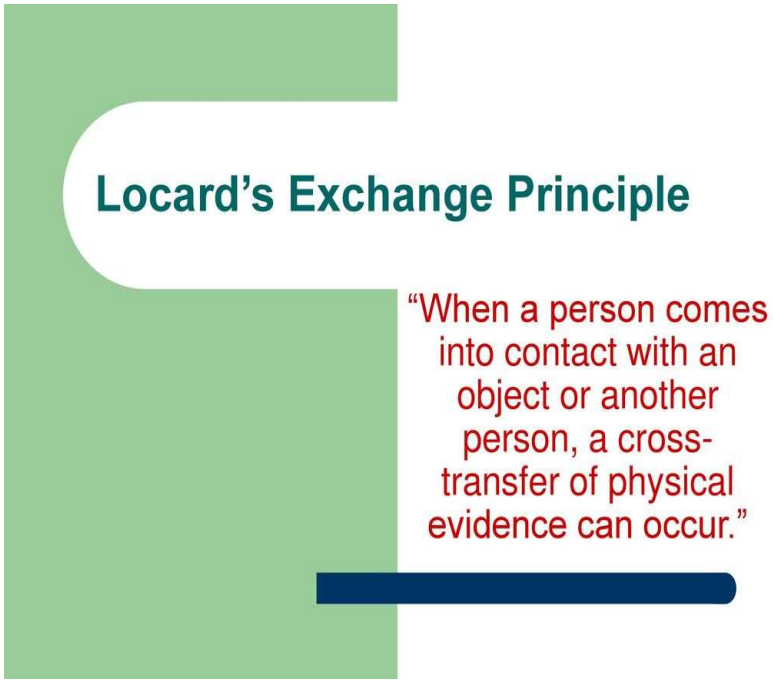
- Traditional Evidence may be divided into 2 parts; **Oral and Documentary**
- All electronic records produced for the inspection of the Court are called evidence
- Electronic evidence can be any information created or stored in digital form whenever a computer is used to accomplish the task and includes information databases, operating Systems, applications, programs, electronic and voicemail messages and records and other information or instruction residing in computer memory.
- In light of the recent spate of terrorism in the world, involving terrorists using highly sophisticated technology to carry out attacks, it is of great help to the prosecution to be able to produce electronic evidence as **substantial** evidence in court, as they prove the guilt of the accused much better than having to look for traditional forms of evidence.

Computer-Stored Declarations vs. Computer-Generated Output

- Accounting records, invoices, charts, graphs, and summaries - generally, any printouts reiterating data that has been entered into the computer are examples of computer stored declarations.
- Automated telephone call records, computer-enhanced photographic images, computerized test-scoring - generally, output not reiterating human declarations but simply performing programmed tasks on non-assertions are examples of computer generated output.

Computer Interactions

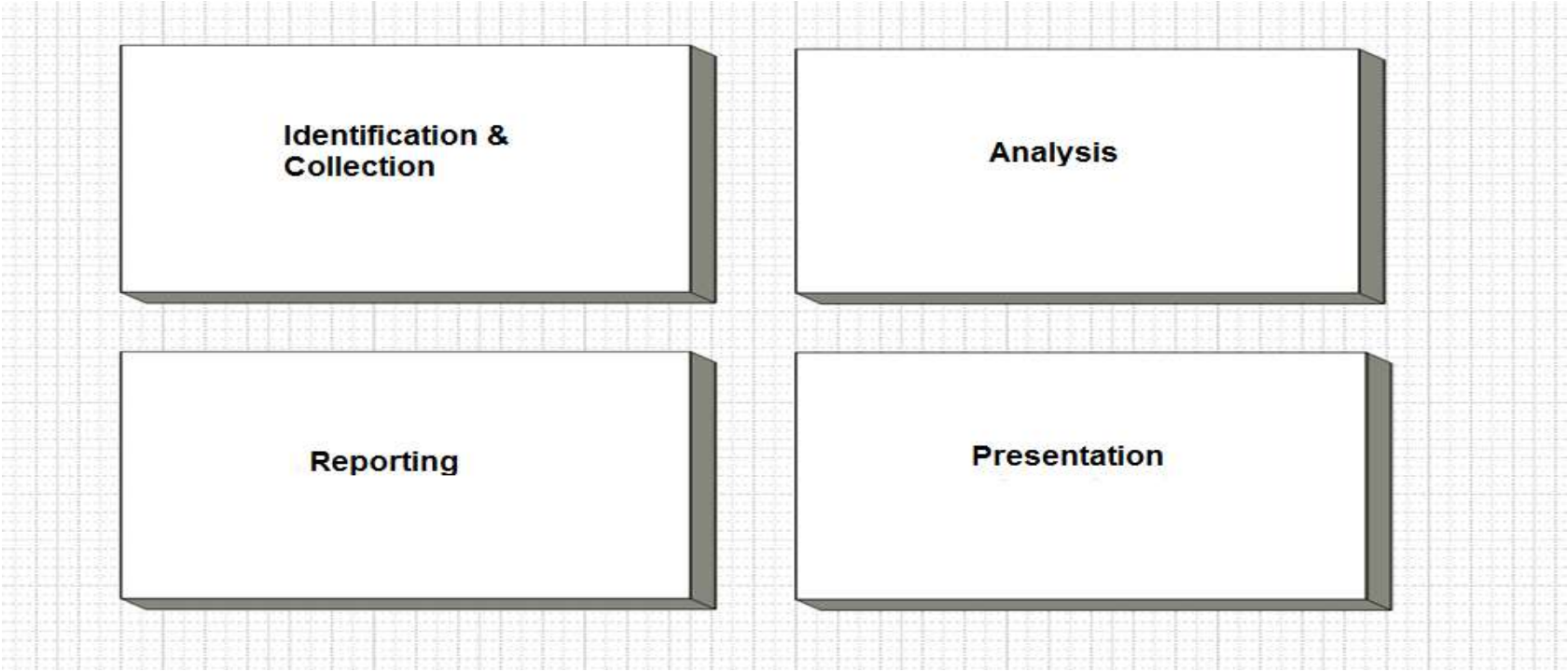
- **Locard's Exchange Principle -** when any two objects (i.e. person & computer) come into contact, there is always transference of material from each object onto the other.
- Each user's interaction with digital devices leaves both user and usage data and certain remnants of digital data that is contained in the device.



Forensics Linkages - More Useful Terms

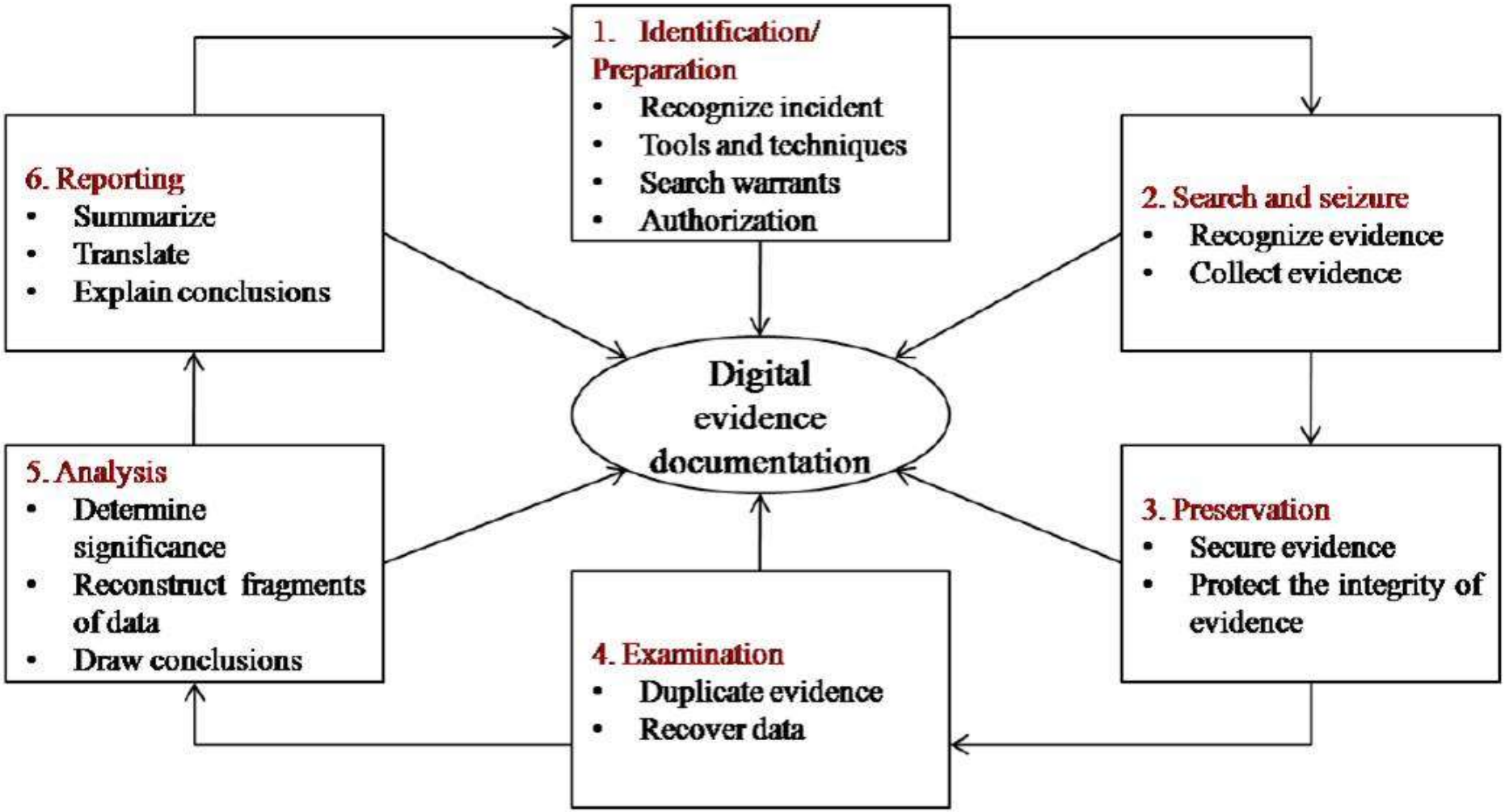
- Person
- Platform
- Application
- Data
- Time

The Four Forensic Processes



Incidents and Seizure (Collection)

1. An incident in the context of information technology is a presumptive or observed adverse event (s) that impact on expected and proper services, data integrity or confidentiality of use for a digital system.
2. The legal or administrative requirement to preserve, protect and produce extracts of digital data concerning users and users of a particular digital system


1. Identification/ Preparation
• Recognize incident
• Tools and techniques
• Search warrants
• Authorization
2. Search and seizure
• Recognize evidence
• Collect evidence
3. Preservation
• Secure evidence
• Protect the integrity of evidence
4. Examination
• Duplicate evidence
• Recover data
5. Analysis
• Determine significance
• Reconstruct fragments of data
• Draw conclusions
6. Reporting
• Summarize
• Translate
• Explain conclusions
Digital evidence documentation

Where Data is typically Found

- Email messages (deleted ones also)
- Office files
- Deleted files of all kinds
- Encrypted Files
- Compressed Files
- Temp files
- Recycle Bin
- Pictures,Videos

- Web history
- Cache files
- Cookies
- Registry
- Unallocated Space
- Slack Space
- Web/e-Mail Server access logs
- Domain access logs

What should be seized

- Floppy Disk(s)
- Hard Drive(s)
- CD, DVDs
- USB Mem. Devices
- Mag. Tapes
- RFID Tags
- PDAs
- Smart Cards
- Web pages
- Memory cards
- Voice mail
- e-Diary
- Scanner, Printer
- Fax, Photocopier
- Digital Phone Set
- iPods
- Cellphone
- DigiCam
- Config'n settings of digital devices
- External drives and other external devices
- Wireless network cards power supply units
- CPU

Measures for Seizure

- Enumerated list of data, devices and associated media
- Verified data extraction of logical and physical evidence – Hash and authoritative time/data
- Chain-of-Custody
- Transfer documentation
- Administrative records
- The collection team may or may not perform further forensics processes i.e. Examination – Analysis - Reporting

Collection & Chain Of Custody Of Digital Evidence

WHAT IS CHAIN OF CUSTODY & EVIDENCE HANDLING?

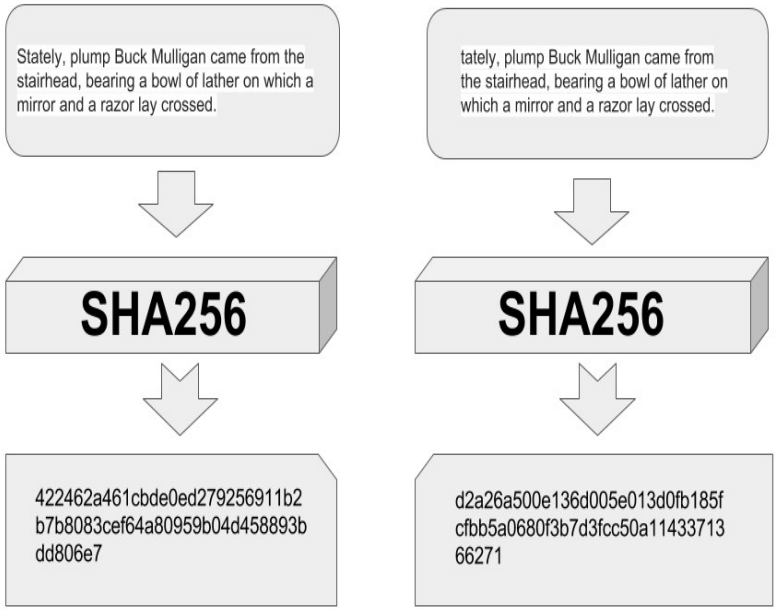
As electronic evidence is easy to tamper or to get damaged, it is necessary for the court to know exactly who, what, when, where, and why was the evidence transferred to the concerned person.
It will not be possible to prove the integrity of the evidence, if the chain of custody is not properly maintained.

- Chain of custody refers to the documentation that shows the people who have been entrusted with the evidence.
- These would be -

1. People who have seized the equipment
2. People who are in charge of transferring the evidence from the crime scene to the forensic labs.
3. People in charge of analysing the evidence, and so on.

Important Points to remember for Fool-proof Chain of Custody

- Always accompany evidence with their chain of custody forms
- Give evidence positive identification at all times that is illegible and written with permanent ink
- Establishing the integrity of the seized evidence through forensically proven procedure-”hashing”
- Hashing helps the Ayo to prove the integrity of the evidence.
- Similarly, the seized original data can be continued to be checked for its integrity by comparing its hash value, identify any changes to it.



Annexure 5-2: Chain of Custody Form

CHAIN OF CUSTODY

DETAILS OF THE DIGITAL EVIDENCE

Crime number..... Date of Seizure.....

Name of the I.O..... Time.....

P.F.Number.....

TECHINAL INFORMATION

MANUFACTURER	MODEL	SERIAL NUMBER	PF NUMBER

DESCRIPTION

CHAIN OF CUSTODY

REASON/ACTION	RECEIVED FROM	RECEIVED BY	DATE	TIME	REMARKS

Reason /action: IO shall ensure documentation of the reasons for transferring the seized evidence to other custodians in chronological order.

Some key elements that require documentation

- **How** the evidence was **collected**
- **When** was it **collected** (e.g. Date, Time)
- **How** was it **transported**
- **How** was it **tracked**
- **How** was it **stored** (for example, in secure storage at your facility)
- **Who has access to the evidence**

Annexure 5-3: Digital Evidence Collection Form

Digital Evidence Collection Form			
Crime Number:		Date:	
PS/Circle/SDPO:		Time:	
IO Name		Item Number:	
Location :		Custodian / Suspect Name:	

Computer Information			
☐ Laptop	☐ Desktop	Manufacturer	
☐ HDD Only	☐ External HDD	Model Number	
☐ Others		Serial Number	
Time Zone		Asset tag	
BIOS Date and Time		Actual Date and Time	

Evidence Drive			
Acquired By		Date of Acquisition	
Signature of I.O		Time of Acquisition	

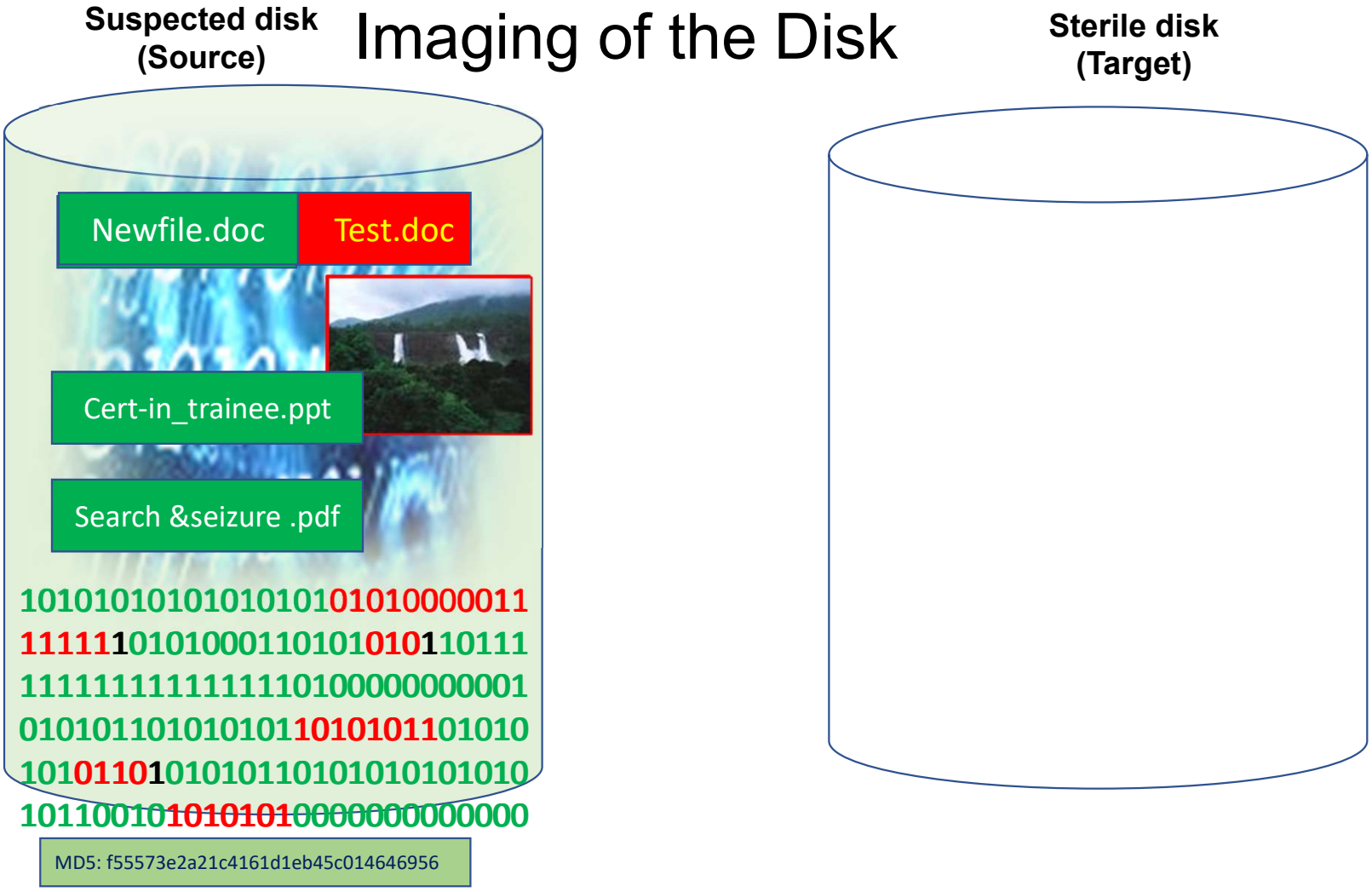
Acquisition Information			
☐ IDE	☐ SCSI	Manufacturer	
☐ SATA	☐ Other	Model Number	
		Serial Number	
		HDD Size	

Collection Details		Destination Drive Details	
Software used		Manufacturer	
Version		Model Number	
Write Protect Device Used		Serial Number	
Verified By		HDD Size	
Image File Name			
Notes			

Acquisitions

- Make an exact (bit-by-bit) verified copy of the media.
- This process is called making an ‘image’
- Process of retrieving data and making an image, is acquisition.
- Acquiring evidence is making sure nothing is added/written to the evidence in the process.

Imaging of the Disk



Why is it important to maintain Integrity of Digital Evidence?

- The ease with which digital evidence can be altered, destroyed or manufacture in a convincing way by even novice computer users is is alarming .
- Hence the requirement to preserve, archive and protect the integrity of the as well as the methods used for best have utmost prominence.
- Digital integrity can be defined as-the property whereby **digital data has not been altered in an unauthorized** manner since the time it was created, transmitted or **by an authorized source.**

Integrity of Digital Evidence?

- Digital data is vulnerable to intentional or unintentional alteration
- Integrity of digital evidence is required to be maintained, starting from seizure till analysis
- Forensic examiners have to ensure that digital evidence is not compromised during the computer forensic analysis process.
- Due to these reasons, to ensure the integrity of the digital evidence, a unique digitized tag is required
  - A fingerprint of the digital evidence could be its digest

Integrity of Evidence[+]

Method	Description	Common Types	Advantages	Disadvantages
Checksum	Method for checking for errors in digital data. Uses 16- or 32-bit polynomial to compute 16 or 32 bit integer result.	CRC-16 CRC-32	• Easy to compute • Fast • Small data storage • Useful for detecting random errors	• Low assurance against malicious attack • Simple to create data with matching checksum
One-Way Hash	Method for protecting data against unauthorized change. Produces fixed length large integer (80~240 bits) representing digital data. Implements one-way function.	SHA-1 MD5 MD4 MD2	• Easy to compute • Can detect both random errors and malicious alterations	• Must maintain secure storage of hash values • Does not bind identity with data • Does not bind time with data
Digital Signature	Secure method for binding identity of signer with digital data integrity methods such as one-way hash values. Uses public key crypto system.	RSA DSA PGP	• Binds identity to integrity operation • Prevents unauthorized regeneration of signature	• Slow • Must protect private key • Does not bind time with data

[+] Proving the Integrity of Digital Evidence with Time," International Journal of Digital Evidence, Spring 2002, V1.1, www.ijde.org (Oct 25, 2005)

Reliability is a pre-requisite for getting evidence admitted-

- The dictum laid down in Daubert V. Merrel-Dow-509 US 579 (1993) established that judges should be “gatekeepers of scientific evidence”
- Judges have a duty to ensure that scientific evidence is not only relevant but reliable.
- The four-part reliability test established in Daubert –

✓Has the scientific theory being tested empirically?

✓What is the known or potential error rate?

✓Has the scientific theory of technique being subjected to peer review and publication?

✓What are the expert’s qualifications and stature in the scientific community?

Daubert has been extensively discussed in Selvi V. State of Karnataka -(2010) 7 SCC 263

- Where the legal questions related to the involuntary administration of certain scientific techniques, namely narcoanalysis, polygraph examination and the Brain Electrical Activation Profile (BEAP) test for the purpose of improving investigation efforts in criminal cases.
- The Apex Court echoed the concerns expressed by the Supreme Court of Canada in R v. Beland, [1987] 36 C.C.C. (3d) 481, where it was observed that reliance on scientific techniques could cloud human judgment on account of an `aura of infallibility'.

All data, is information, which cannot exist without a physical medium or carrier.

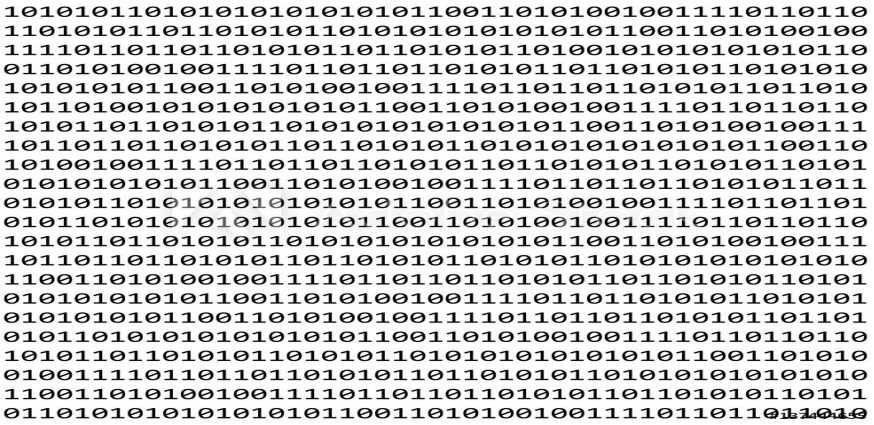
Digitized documents

- As **documents** came to be **digitised**, the **hearsay rule** faced several **new challenges**.
- While the law had mostly anticipated primary evidence (i.e. the original document itself) and had created special conditions for secondary evidence, increasing digitisation meant that more and more documents were electronically stored.
- As a result, the adduction of secondary evidence of documents increased. In the *Anvar* case, the Supreme Court noted that ***"there is a revolution in the way that evidence is produced before the court".***

MYTH OF PRIMARY & SECONDARY EVIDENCE

- Primary evidence means **the document itself.**

- PRIMARY format of what gets written as electronic record , **is computer-readable but is not human- readable**.

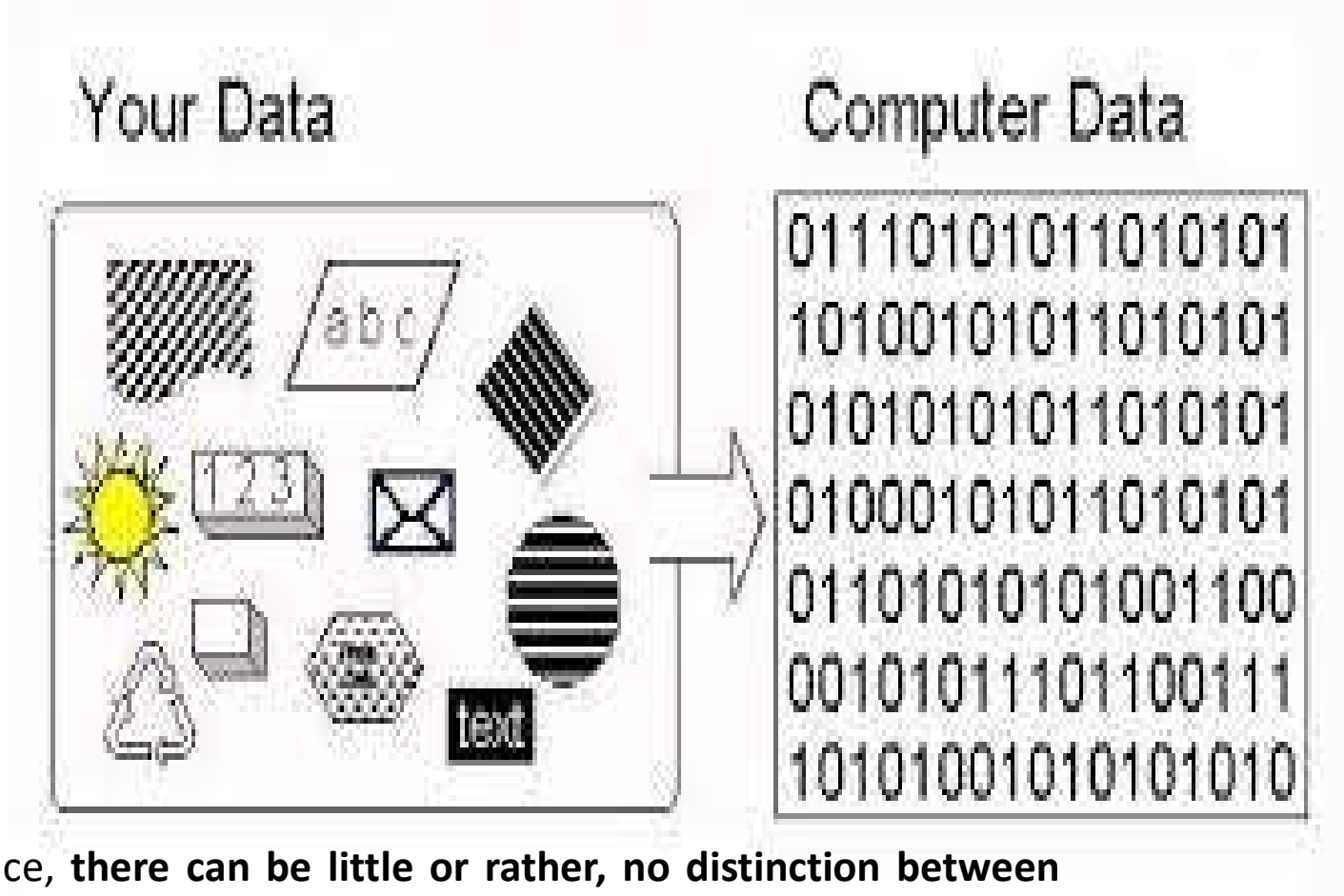


Hence, there can be little or rather, no distinction between primary evidence and secondary evidence in relation to digital/electronic records.

With this understanding, it could **ONLY** be secondary evidence that could be produced in the court with regard to electronic records.

ASCII TABLE

Decimal	Hexadecimal	Binary	Octal	Char
0	0	0	0	*[NULL]*
1	1	1	1	*[START OF HEADING]*
2	2	10	2	*[START OF TEXT]*
3	3	11	3	*[END OF TEXT]*
4	4	100	4	*[END OF TRANSMISSION]*
5	5	101	5	*[ENQUIRY]*
6	6	110	6	*[ACKNOWLEDGE]*
7	7	111	7	*[BELL]*
8	8	1000	10	*[BACKSPACE]*
9	9	1001	11	*[HORIZONTAL TAB]*
10	A	1010	12	*[LINE FEED]*
11	B	1011	13	*[VERTICAL TAB]*
12	C	1100	14	*[FORM FEED]*
13	D	1101	15	*[CARRIAGE RETURN]*
14	E	1110	16	*[SHIFT OUT]*
15	F	1111	17	*[SHIFT IN]*
16	10	10000	20	*[DATA LINK ESCAPE]*
17	11	10001	21	*[DEVICE CONTROL 1]*
18	12	10010	22	*[DEVICE CONTROL 2]*
19	13	10011	23	*[DEVICE CONTROL 3]*
20	14	10100	24	*[DEVICE CONTROL 4]*
21	15	10101	25	*[NEGATIVE ACKNOWLEDGE]*
22	16	10110	26	*[SYNCHRONOUS IDLE]*
23	17	10111	27	*[ENG OF TRANS. BLOCK]*
24	18	11000	30	*[CANCEL]*
25	19	11001	31	*[END OF MEDIUM]*
26	1A	11010	32	*[SUBSTITUTE]*
27	1B	11011	33	*[ESCAPE]*
28	1C	11100	34	*[FILE SEPARATOR]*
29	1D	11101	35	*[GROUP SEPARATOR]*
30	1E	11110	36	*[RECORD SEPARATOR]*
31	1F	11111	37	*[UNIT SEPARATOR]*
32	20	100000	40	*[SPACE]*
33	21	100001	41	!
34	22	100010	42	"
35	23	100011	43	#
36	24	100100	44	$
37	25	100101	45	%
38	26	100110	46	&
39	27	100111	47	'
40	28	101000	50	(
41	29	101001	51	)
42	2A	101010	52	*
43	2B	101011	53	+
44	2C	101100	54	,
45	2D	101101	55	-
46	2E	101110	56	.
47	2F	101111	57	/
48	30	110000	60	0
49	31	110001	61	1
50	32	110010	62	2
51	33	110011	63	3
52	34	110100	64	4
53	35	110101	65	5
54	36	110110	66	6
55	37	110111	67	7
56	38	111000	70	8
57	39	111001	71	9
58	3A	111010	72	:
59	3B	111011	73	;
60	3C	111100	74	<
61	3D	111101	75	=
62	3E	111110	76	>
63	3F	111111	77	?
64	40	1000000	100	@
65	41	1000001	101	A
66	42	1000010	102	B
67	43	1000011	103	C
68	44	1000100	104	D
69	45	1000101	105	E
70	46	1000110	106	F
71	47	1000111	107	G
72	48	1001000	110	H
73	49	1001001	111	I
74	4A	1001010	112	J
75	4B	1001011	113	K
76	4C	1001100	114	L
77	4D	1001101	115	M
78	4E	1001110	116	N
79	4F	1001111	117	O
80	50	1010000	120	P
81	51	1010001	121	Q
82	52	1010010	122	R
83	53	1010011	123	S
84	54	1010100	124	T
85	55	1010101	125	U
86	56	1010110	126	V
87	57	1010111	127	W
88	58	1011000	130	X
89	59	1011001	131	Y
90	5A	1011010	132	Z
91	5B	1011011	133	[
92	5C	1011100	134	\
93	5D	1011101	135	]
94	5E	1011110	136	^
95	5F	1011111	137	_
96	60	1100000	140	`
97	61	1100001	141	a
98	62	1100010	142	b
99	63	1100011	143	c
100	64	1100100	144	d
101	65	1100101	145	e
102	66	1100110	146	f
103	67	1100111	147	g
104	68	1101000	150	h
105	69	1101001	151	i
106	6A	1101010	152	j
107	6B	1101011	153	k
108	6C	1101100	154	l
109	6D	1101101	155	m
110	6E	1101110	156	n
111	6F	1101111	157	o
112	70	1110000	160	p
113	71	1110001	161	q
114	72	1110010	162	r
115	73	1110011	163	s
116	74	1110100	164	t
117	75	1110101	165	u
118	76	1110110	166	v
119	77	1110111	167	w
120	78	1111000	170	x
121	79	1111001	171	y
122	7A	1111010	172	z
123	7B	1111011	173	{
124	7C	1111100	174	|
125	7D	1111101	175	}
126	7E	1111110	176	~
127	7F	1111111	177	*[DEL]*



Hence, **there can be little or rather, no distinction between primary evidence and secondary evidence in relation to digital/electronic records**.

With this understanding, it could **ONLY** be secondary evidence, that could be produced in the court with regard to electronic records.

Changes Brought to IEA vis-a-vie ‘electronic records

- The definition of ‘**evidence**’ was amended to **include electronic records**
- Section **3(a),** Evidence Act-The definition of documentary evidence has been amended to **include electronic records produced for the inspection of the court**.
- The term ‘**electronic records**’ has been given the **same meaning as assigned to it in the Information Technology Act**, which provides, ‘data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche’.
- **Section 5** of the Evidence Act provides that evidence can be given only regarding facts that are in issue or where they are relevant, but no other facts, and section 136 **empowers a judge to decide as to the admissibility of the evidence.**
- **Section 17** Evidence Act is changed to include a statement, oral or documentary, or **contained in electronic form**, which suggests any inference as to any fact in issue or relevant fact.
- New **Section 22A** provides that oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic records produced is in question.
- Section 39 Evidence Act- When any statement of which evidence is contained **is part of electronic record evidence must be given of so much and no more of the electronic record as the court considers necessary in that particular case to the full understanding of the nature and effect of the statement and of the circumstances under which it was made**.

Electronic record

- Section 2(t) of the IT Act defines '**Electronic record**' to mean data, record or data generated, image or sound stored, received or send in an electronic form or micro film or computer generated micro fiche.

- 'electronic record', in its simplest term can be defined to mean data, kept in optical or magnetic media or digital form is an electronic record.

Electronic from

- Section 2(r) defines ‘Electronic form’, with reference to information, to mean an information generated, send, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.

- The relevant information, if kept in above mentioned media, then it is said to be kept in electronic from

Information

- Section 2 (v) - ‘Information’ includes data, message, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche.

- The definition of ‘Information’ can be clarified as ‘information’ in relation to information technology law means the information kept in computer generated source

Data

- Section 2 (o) - Data" means a representation of information, knowledge or facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form including computer printouts, magnetic, or optical storage media, punched cards, punched tapes or stored internally in the memory of the computer.

- 4 The definition of "data" also shows that the knowledge or facts, if kept in computer- resource, then it becomes 'data'

Computer resource

2 (k)- “Computer resource” means computer, computer system, computer network, data, computer data base or software.

- ‘Computer resource’ thus incorporates all kinds of computers and its data base.

Computer

- Section 2 (i)- “Computer” means any electronic, magnetic, optical or other high speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network.6 The definition of “Computer” shows that it includes all the input, output, processing and communication facilities which are done or performed in any magnetic or optical media

- “Computer” shows that it includes all the input, output, processing and communication facilities which are done or performed in any magnetic or optical media

Essence

- If the data, information, facts, knowledge, instructions or any other content generated, kept, stored, sent, received and communicated through electronic, magnetic, optical and digital media, then it would fall within the category of Electronic evidence.

- The information contained in the electronic record can be proved only as per the special procedure as provided in the Indian Evidence Act, 1872.

Section 3 of the Indian Evidence Act

- “Evidence” as defined in Sec.3 of the Indian Evidence Act, 1872 means and includes –
- (1) All statements which the court permits or requires to be made before it by witnesses, in relation to matter of fact under inquiry, such statements are called oral evidence.
- (2) All documents including electronic-records produced for the inspection of the court, such documents are called documentary evidence.

Admissibility of Electronic Records

- Any documentary evidence by way of an ‘electronic record’ under the Indian Evidence Act, in view of sec. 59 and 65A, can be proved only in accordance with the procedure prescribed under Sec. 65.
- Sec. 59 provides that all facts except the contents of document or ‘electronic records’, may be proved by oral evidence.
- Production of an ‘electronic record’ as an evidence in court, can only be under Sec. 65A and Sec. 65B of Evidence Act

Admissibility of Electronic Evidence

- Parliament in its wisdom Incorporated Ss. 65A & 65B in the Evidence Act.
- S. 65A is termed as-special provisions as to evidence relating to electronic record. Ss. 65A & 65B are a complete code in a code.
- ***S.65B. Admissibility of electronic record-*** requires special procedure for presenting electronic records as admissible in evidence, in a Court of law. It provides for technical and non-technical conditions and the method for presenting electronic records as admissible in evidence

S.65B(1)

- Notwithstanding anything contained in this Act, **any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media** produced by a computer (hereinafter referred to as the computer output) **shall be deemed to be also a document**, if the conditions mentioned in this section are satisfied in relation to the **information and computer** in question **and shall be admissible in any proceedings, without further proof or production of the original**, **as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible**.

Explanation-S.65B(1)

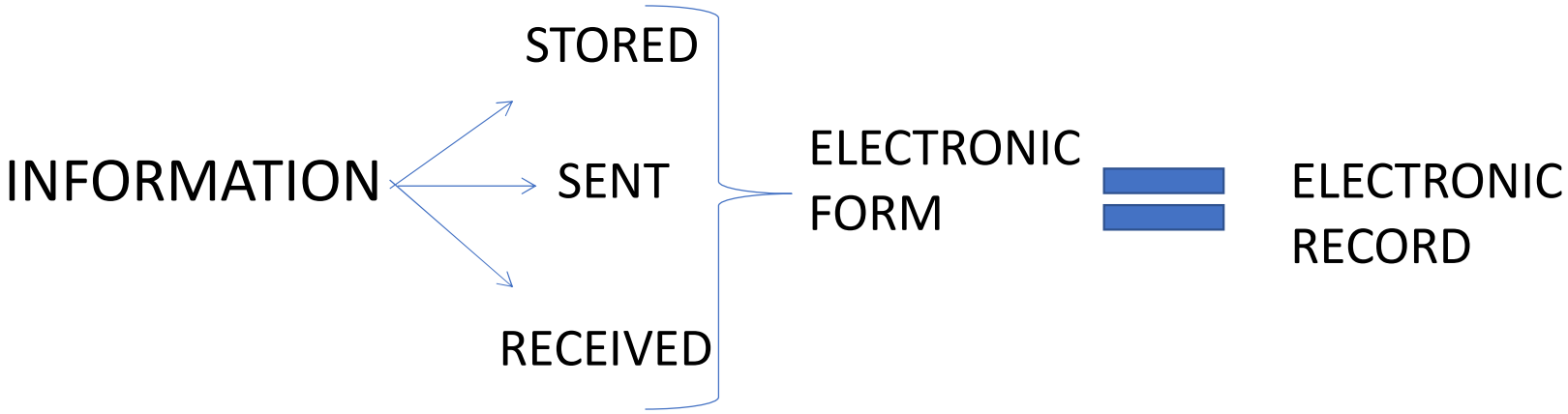
- Any information contained in an electronic record……
- S.2(1)(v)-‘information’-includes[data, message, text], images, sound, wise, courts, computer programs, software and databases or microfilm or computer-generated micro fiche
- S.2(1)(o)- ‘**data**’-means **a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed** in a computer system or computer network, and maybe in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer

contd..

- **S.2(1) (t)-‘electronic record’**-data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche
- printed on paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output)**shall be deemed to be also a document,** if the conditions mentioned in the section are satisfied in relation to the information and computer in question….

Contd....

- …and **shall be admissible in any proceedings**, **without further proof or production of the original**, as evidence of any content's of the original order of any fact stated therein of which direct evidence would be admissible.


INFORMATION
STORED
SENT
RECEIVED
ELECTRONIC FORM
ELECTRONIC RECORD

Technical Conditions Requirements under S. 65B(2)IEA

- (i) at the time of the creation of the electronic record, the computer that produced it must have been in regular use;
- (ii) the kind of information contained in the electronic record must have been regularly and ordinarily fed in to the computer;
- (iii) the computer was operating properly; and,
- (iv) the duplicate copy must be a reproduction of the original electronic record.

S.65B(3)

- Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether—
- (a) **by a combination of computers operating over that period**; or
- (b) **by different computers operating in succession over that period**; or
- (c) b**y different combinations of computers operating in succession over that period**; or
- (d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers, **all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer**; and references in this section to a computer shall be construed accordingly.

Non-technical Conditions To Establish Authenticity Of Electronic Evidence Under S. 65B (4) IEA

- In any proceedings where it is desired to give a statement in evidence by virtue of this section**, a certificate doing any of the following things**, that is to say,—
- (a) identifying the electronic record containing the statement and describing the manner in which it was produced;
- (b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
- (c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and
- purporting to 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) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

Annexure 5-10: Certificates under different Sections of the Indian Evidence Act

Certificate

(u/s 65B (4) (a) of the Evidence Act 1872)

Certified that this electronic record/computer output containing the statement of Shri ..... has been produced from (description of the system) using (description of the output device) and that its contents are true reproduction of the original to the best of my knowledge and belief.

Certificate

(u/s 65B (4) (b) of the Evidence Act 1872)

Certified that this electronic record/computer output has been produced from (description of the system) using (description of the output device) and that its contents are true reproduction of the original to the best of my knowledge and belief

Certificate

(u/s 65B (4) (c) of the Evidence Act 1872)

Certified that this computer output/electronic record has been produced from (description of the system) using (description of the output device) and its contents are true reproduction of the original to the best of my knowledge and belief

Further certified that conditions as laid down in section 65B(2) (a) to 65B(2) (d) of Evidence Ad, 1872 regarding the admissibility of computer output in relation to the information and the computer in question are fully satisfied in all aspects. These certificates are to be issued by a person occupying a responsible position in relation to the operation of the relevant system or the management of the relevant activities, whichever is appropriate.

The first of the three certificates pertains to an electronic record containing a statement This implies that a witness can now be examined through e-mail also, provided a certificate u/s 65B (4) (a) is obtained.

This becomes significant in cases where the witnesses are residing abroad or at faraway places in the country. Another significant amendment has been made in the Banker's Books Evidence Act 1891. Prior to this amendment, Section 2 of this act provided tint a copy of a bank statement would be admissible in the court only when it is certified to the effect.

However, since the banks have started maintaining their records on computers, they were finding it difficult to issue such a certificate. Keeping this in mind, the Banker's Books Evidence Act 1891 was amended vide Third Schedule of the Information Technology Act 2000. After this amendment, printouts of the data stored in a floppy, disk, tape, or any other electromagnetic media have also been made admissible provided the same are certified as per Section 2A of this act.

UNDERSTANDING THE IMPLICATIONS OF ARJUN PANDITRAO'S JUDGMENT- (2020) 7 SCC 1

- The Reference-
- Dealing with the interpretation of Section 65-B of the IEA by 2 judgements of the Apex Court-
- the first being a three-judge bench decision of the Apex Court in Anvar P.V. Vs. P.K. Basheer (2014) 10 SCC 473 and
- the 2nd being a division bench judgement of the Apex Court in Shafi Mohammad Vs. State of H.P. (2018) 2 SCC 801.

Arguments put forward by Appellant

- Referring to Tomaso Bruno's case (2015) 7 SCC 178 it was submitted/argued that the said judgement neither noticed the findings in Anvar's case nor did it notice S. 65-B IEA and hence it was per incuriam.

- that Shafi's case, being a 2 judge bench of the Apex Court could not have arrived at finding contrary to Anvar's case.

Continued...

- that the judgement of the Madras High Court in care. Ramajayam Vs. State 2016 SCConline Mad 451 laying down that evidence aliunde, that is outside S. 65-B IEA, can be taken in order to make electronic records admissible, being contrary to Anvar's case and hence unsustainable in law.

Arguments for Respondents

- that in the prevailing situation the High Court correctly recorded the oral testimony into writing, which witness statement signed by the RO, would itself amount to requisite Certificate being issued under S. 65-B (4) the facts of this case.

Continued....

- that S65-B is a procedural provision, and it cannot be the law that even where the Certificate is impossible to be procured, the absence of such Certificate should result in a denial of crucial evidence which would point at the truth or falsehood of a given set of facts, thus supporting Shafi's judgement

Argument for Intervener

- S. 65-B (4) IEA does not refer to the stage at which the Certificate under S. 65-B (4) ought to be furnished and that the requisite Certificate need not necessarily be given the time of tendering of evidence but could be at a subsequent stage of the proceedings, as in the cases where the requisite Certificate is not forthcoming due to no fault of the party would try to produce it, but who had to apply to a judge for its production.

Continued....

- that Ss. 65-A and 65-B being a complete code as to admissibility of electronic records, the “baggage” of primary and secondary evidence contained in Sections 62 and 65 of IEA should not be adverted to at all and that the drill of Ss. 65-A and 65-B alone should be followed regarding admissibility of information contained in electronic records.

While over ruling Shafi's judgment-

- the SC stated- **caveat** need be **entered in situations where as in the present case show that despite all efforts made by the Respondents, both by the High Court and otherwise to get the requisite Certificate under S. 65-B (4) of IEA from the authorities concerned, yet the authorities concerned wilfully refused, on some pretext or the other, to give such a Certificate.**
- **Remedies laid down by SC-** The party can apply to the Court for its production under provisions aforementioned of the IEA, CPC or Cr.P.C and one such application is made to the Court and the Court then orders or directs that the requisite Certificate be produced by person to whom it sends a summons to produce such Certificate, the party asking for the Certificate has done all that he can possibly do to obtain the requisite Certificate

Situation when a party has done all it can to obtain the requisite certificate and still unsuccessful

- The Court thereafter discusses 2 maxims-
- *lex non cogit ad impossibilia* i.e.-the law does not demand the impossible, and
- *impotentia excusat legem* meaning, where there is a disability that makes it impossible to obey the law, the alleged disobedience of law is excused.

Outcome

- Once party has done everything possible to obtain a Certificate, which was to be given by a third party over whom the party has no control, must be relieved of the mandatory obligation contained in the subsection.

The question regarding the stage at which S.65B(4) certificate need be produced

- to be furnished at the latest before trial begins.
- The Court stated that the only exception to the general is if the prosecution had “mistakenly” not filed document, the said document can be allowed to be placed on record as recognised in CBI Vs. R.S.Pai (2002) 5 SCC 82
- **the exercise of power by courts in criminal trials in permitting evidence to be filed at a later stage should not result in serious or irreversible prejudice to the accused**.

CONCLUSION

- **the Court finally held that the Certificate required under Section 65-B (4) is a condition precedent to the admissibility of evidence by way of electronic record and that oral evidence in the place of such Certificate cannot possibly suffice as Section 65-B (4) is a mandatory requirement of the law.**
- It also held that Section 65-B(4) of the IEA clearly states **that secondary evidence is admissible only if you lead in the manner stated and not otherwise and that to hold otherwise would render Section 65-B (4) otiose.**

Wrap up

- Anvar P.V. declared as the law regarding S.65B IEA. Tomaso Bruno,Shafi and K. Ramajayam, spoke otherwise.
- Clarified that certificate under S.65B(4) is unnecessary if the original document itself is produced.
- This can be done by the owner of a laptop computer, computer tablet or even a mobile phone , by stepping into the witness box and proving that the concerned device on which original information is first stored , is owned and/or operated by him.
- In cases where the 'computer' happens to be part of a 'computer system' or 'computer network' and it becomes impossible to physically bring such system or network to the court, then the only means of providing information contained in such electronic record can be in accordance with S.65B(1) and S.65B(4)
- Anvar PV is clarified to the extent-the last sentence in Para 24which reads as '..... If an electronic record as such is used as primary evidence under Section 62 of the Evidence Act...' is thus clarified; it is to be read without the words "under Section 62 of the Evidence Act...".

Presumptions Regarding Digital Evidence

- The Evidence Act has been amended to introduce various presumptions regarding digital evidence-
- Under the provisions of **section 81A**, the court **presumes the genuineness of electronic records purporting to be the Official Gazette or an electronic record directed by any law, providing the electronic record is kept substantially in the form required by law, and it is produced from proper custody**.
- **Section 84A** provides a **presumption that a contract is concluded where the digital signatures of the parties are affixed to an electronic record that purports to be an agreement**.

Secure Electronic Records And Digital Signatures

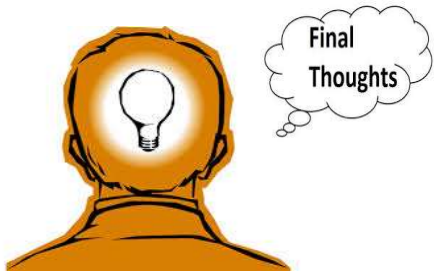
- **Section 85B** provides that where a security procedure has been applied to an electronic record at a specific point of time, then the record **is deemed to be a secure electronic record** from such point of time to the time of verification, unless the contrary is proved.
- Hence the Court **shall** presume that a secure electronic record has not been altered since the specific point of time to which the secure status relates, unless the contrary is proved.

Electronic Messages

- Under **S. 88A**, there is a **presumption that an electronic message forwarded by the sender through an electronic mail server to the addressee to whom the message purports to be addressed, corresponds with the message fed into his computer for transmission**.
- However, there is no presumption as to the person by whom such message was sent. **This provision only presumes the authenticity of the electronic message, and not the sender of the message**.

Electronic Records Five Years Old

- The provisions of **S.90A** provides that **where an electronic record is produced from any custody which the court in a particular case considers proper, and it purports to be or is proved to be five years old, it may be presumed that the digital signature affixed to the document was affixed by the person whose signature it was or any person authorized by them on their behalf**.



- **Judges play a gatekeeper role in determining what evidence is allowed in their courtroom and which experts are allowed to testify**.
- Due to the **relative newness of the field of computer crime, forensics and the Law relating to it, the issue could be a little exacerbated due to probably the limited contact that many judges have with technicalities of digital evidence**.
- **Judges need to make decisions** about admissibility of digital evidence **in terms of authenticity, reliability, veracity, and accuracy**.
- An **understanding of judges' knowledge and awareness of digital evidence is important** to both the **integrity of the entire judicial process as well as to ensure that judges are appropriately prepared for this function**.
- **Indian Judiciary** though has **come a long way** in **recognizing, accepting, appreciating and assimilating** these **aspects of digital evidence**, its importance and complexity, but there **still remains a lot of challenges** in the area **as technology keeps changing at a fast pace throwing up new challenges and the Law has a rather slower pace in keeping abreast** with.

Case Law

- **P.Gopalakrishnan @ Dileep v State of Kerala (2020) 9 SCC 161**

- Contents of the memory card/pen-drive being electronic record must be regarded as a document.
- The accused must be given a cloned copy thereof to enable him/her to present an effective defence during the trial.
- In cases involving issues such as of privacy of the complainant/witness or his/her identity, the Court may be justified in providing only inspection thereof to the accused and his/her lawyer or expert for presenting effective defence during the trial.
- The court may issue suitable directions to balance the interests of both sides.

State of Karnataka by Lokayukta, Police Station, Bangaluru Vs. Hiremath -(2019) 7 SCC 515

- Question that arose for consideration was whether the High Court had erred in coming to the conclusion that in the absence of a Certificate under Section 65B, when the chargesheet was submitted, the prosecution was liable to fail and the finding that the proceedings was required to be quashed and the stage?
- Held- The High Court has erred in coming to the conclusion that in the absence of a certificate under Section 65B when the charge sheet was submitted, the prosecution was liable to fail and that the proceeding was required to be quashed at that stage.
- The High Court ought to have been cognizant of the fact that the trial court was dealing with an application for discharge under the provisions of Section 239 of the CrPC.
- It is a settled principle of law that at the stage of considering an application for discharge the court must proceed on the assumption that the material which has been brought on the record by the prosecution is true and evaluate the material in order to determine whether the facts emerging from the material, taken on its face value, disclose the existence of the ingredients necessary to constitute the offence."

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1

- (a) Section 65-B(4) certificate is unnecessary if the device on which an electronic document is first stored is itself produced in court through a witness e.g., owner who operated a laptop, tablet, etc. stepping into the witness box to produce the laptop, mobile, etc. in evidence. If the document is on a computer that cannot be brought to court then the only means of producing the document is by way of a certificate under Section 65-B(4) . (
- (b) Section 65-B(4)'s requirements for issuing the certificate are to be read as cumulatively “all of them” (instead of text's “… any of them…” .
- (c) No proof of an electronic record by oral evidence is admissible if the requirements of Section 65-B are not complied with .
- (d) Anvar P. V. case stood clarified to make para 24 therein, “… if an electronic record as such in used a primary evidence under section of the Evidence Act…” to be read without the words “… under Section 62 of the Evidence Act…” .
- (e) A trial court may at any stage before the completion of a trial, order the production of the certificate under Section 65-B(4) subject to a criminal court in criminal trial safeguarding against any prejudice to the accused .
- (f) Authorities to examine the draft rules suggested by the Committee of five Judges (formed in consequence of the Chief Justices Conference held in April 2016) in its November 2018 report for statutory enactment in future. Data retention directions for call detail records issued to the cellular companies and internet service providers till rules and directions are enacted under Section 67-C of the Information Technology Act, 2000 .
- (g) The word “and” in Section 65-B(4)'s text “best of his knowledge and belief” has to be read as “or” because a person cannot testify to best of his or her knowledge and belief at the same time .

Contd..

- The difference between something in analogue form and the same thing in digital form and the reason why digital format throws more challenges.
- It is apparent that the images, if viewed together, are identical – will be identical, and the viewer will not be able to determine which is the original, and which image was manipulated. In this respect, the digital images are no different from the droplets of rain that fall, merge, then divide: there is no telling whether the droplets that split are identical to the droplets that came together to form the larger droplet.- **Justice V. Ramasubramanian in Arjun Pandit Rao's case**