

# COLLECTION, PRESERVATION & APPRECIATION OF ELECTRONIC EVIDENCE



By – **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])



# 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.



# DIFFERENCE BETWEEN PHYSICAL AND ELECTRONIC EVIDENCE

- Hard in nature-Tangible
  - Cannot be easily destroyed
  - If tampered/forged can easily be made out
  - If destroyed, is lost forever
  - Is not fragile
  - Vast volume/enormity is visible
  - Is not volatile
- Intangible in nature
  - Can easily be destroyed
  - Cannot be easily made out if tampered unless by an expert
  - Can be retrieved(to an extent)
  - Is fragile
  - Vast volumes can't be seen and easily stored in small –sized devices
  - Is volatile



# 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



# WHAT IS DIGITAL FORENSICS?

- Digital forensics is legal and ethical science-based professional practices of:
  - Safeguarding,
  - Retrieving
  - Investigating and
  - Objective Reporting of digital data.
- The forensics process, data and reporting is of interest in administrative, civil or criminal matters



# COMPUTER INTERACTIONS

## Locard's Exchange Principle

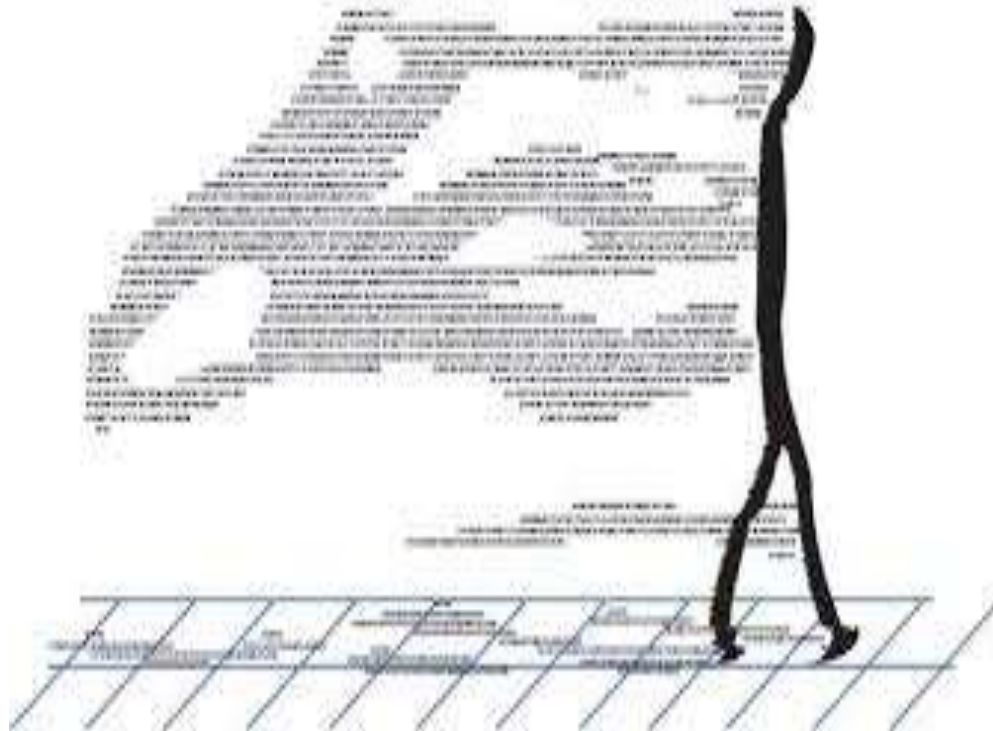
"When a person comes into contact with an object or another person, a cross-transfer of physical evidence can occur."

- 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.



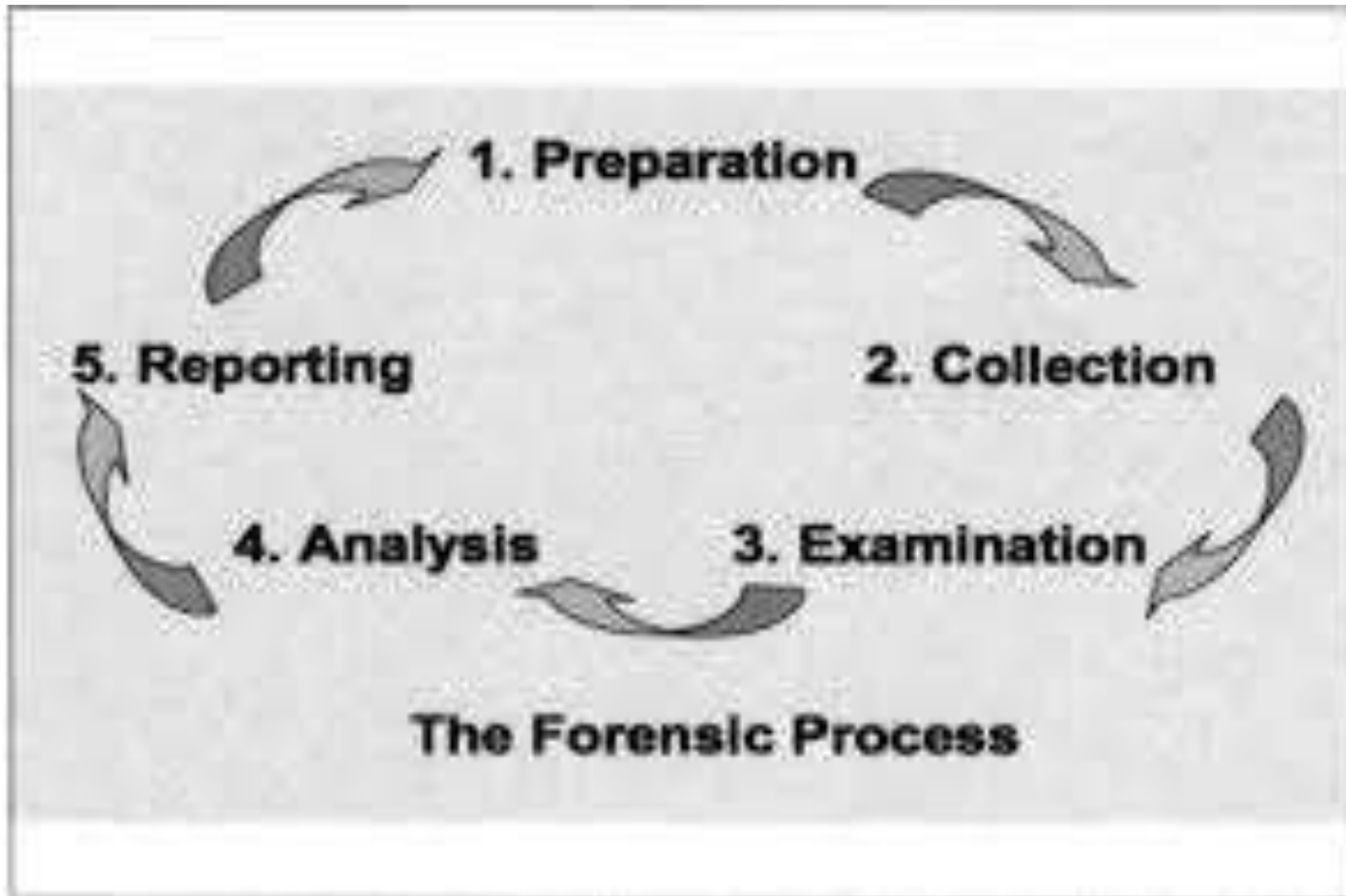
# FORENSICS LINKAGES - MORE USEFUL TERMS

- Person
- Platform
- Application
- Data
- Time





# THE FORENSIC PROCESSES



# GUIDELINES FOR HANDLING OF ELECTRONIC EVIDENCE AT A CRIME SCENE

- **Recognize, identify, seize** and **secure** all electronic evidence at the scene.
- **Document the entire scene** and the **specific location of the evidence found.**
- **Collect, label** and **preserve** the electronic evidence.
- **Package and transport** electronic evidence in a **secure manner.**



# Electronic Evidence Management timeline

1. Case preparation

- Case assessment
- Human resources
- Tools checklist
- Media destination

3. Evidence handling

- Personal computer
- Mobile device
- Digital media storage
- Other storage device
- Network device
- Network data
- Virtualized environment
- Internet/Cloud data

5. Evidence transportation

7. Evidence analysis

2. Evidence identification

4. Evidence classification

6. Evidence acquisition

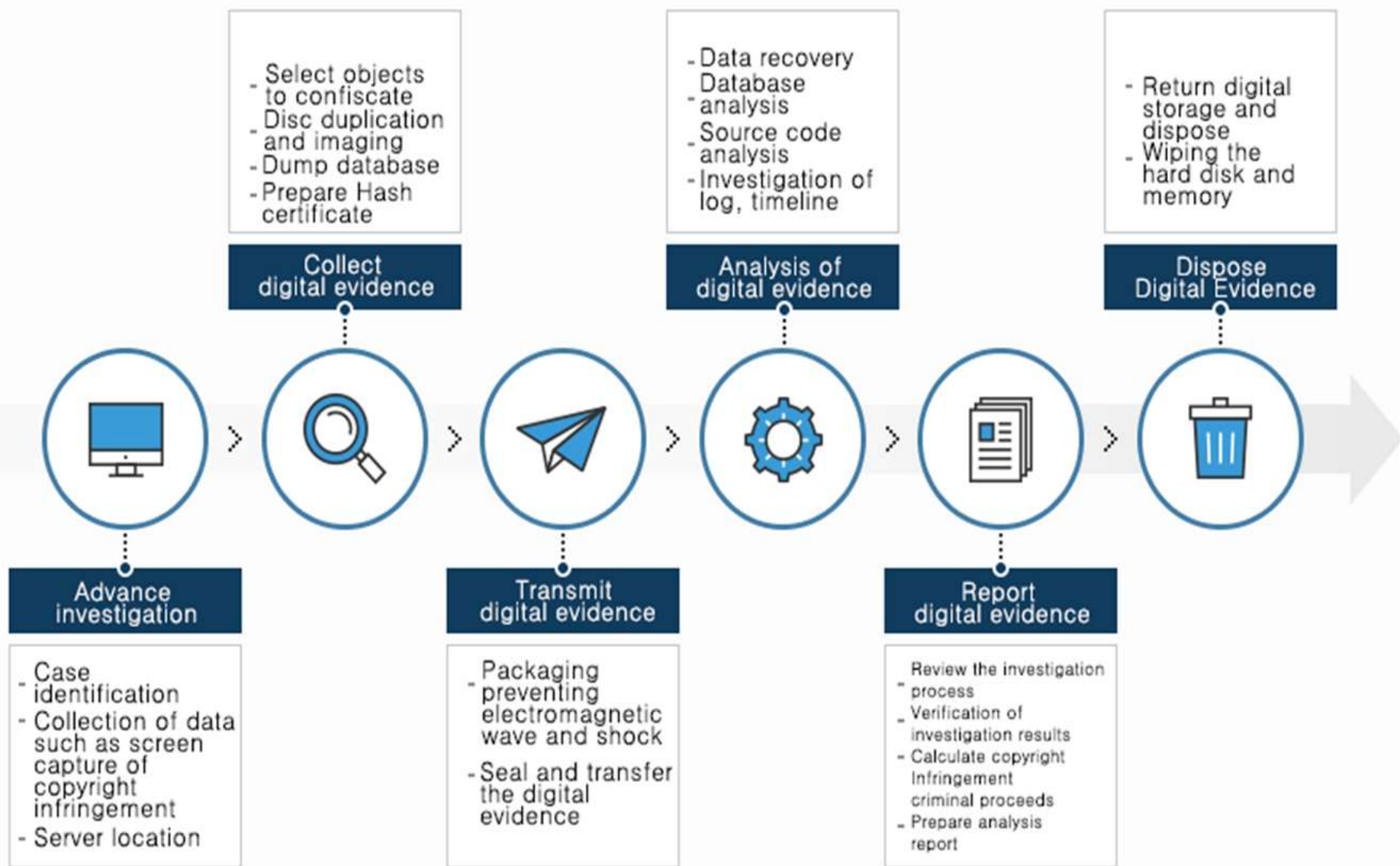
8. Evidence reporting



# 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





# REASONS TO BE CONSIDERED BEFORE SEIZING DEVICE & COLLECT RELATED EVIDENCE

- Whether the computer is **contraband or fruits** of a crime.
- Whether the computer system **contains evidence of a crime**.
- Whether the computer **is a tool of the offence**.
- Whether the computer is both the **instrument and storage device of a crime**.



# 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

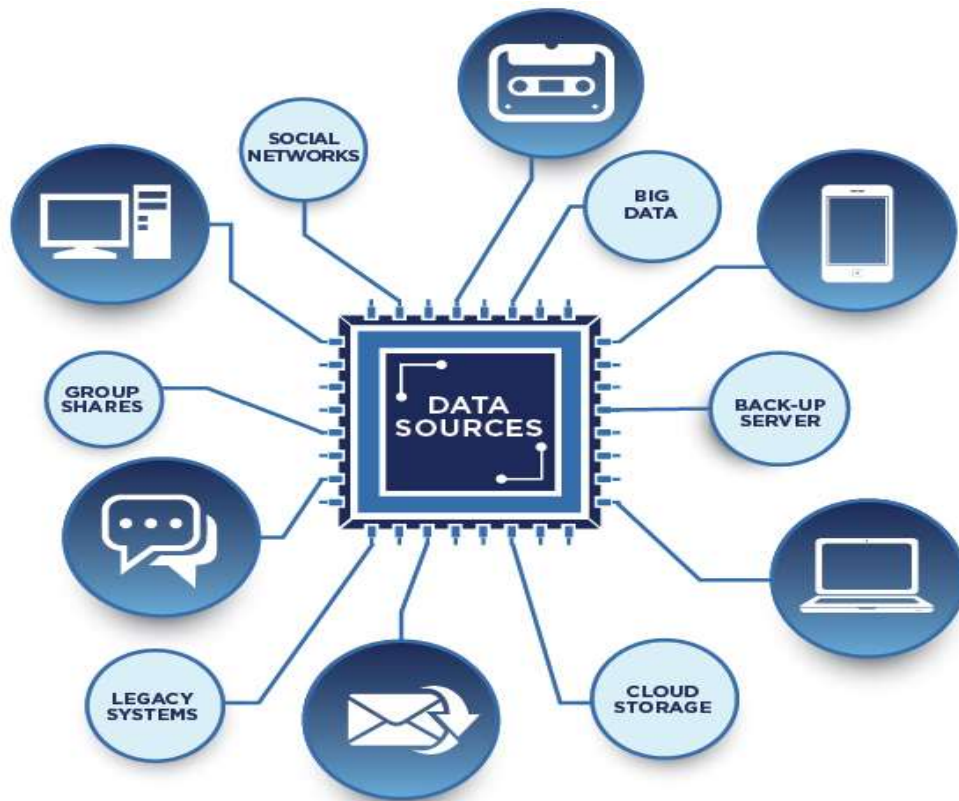


- Web history
- Cache files
- Cookies
- Registry
- Unallocated Space
- Slack Space
- Web/e-Mail Server access logs
- Domain access logs





# WHAT COULD BE SEIZED ?



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





# 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

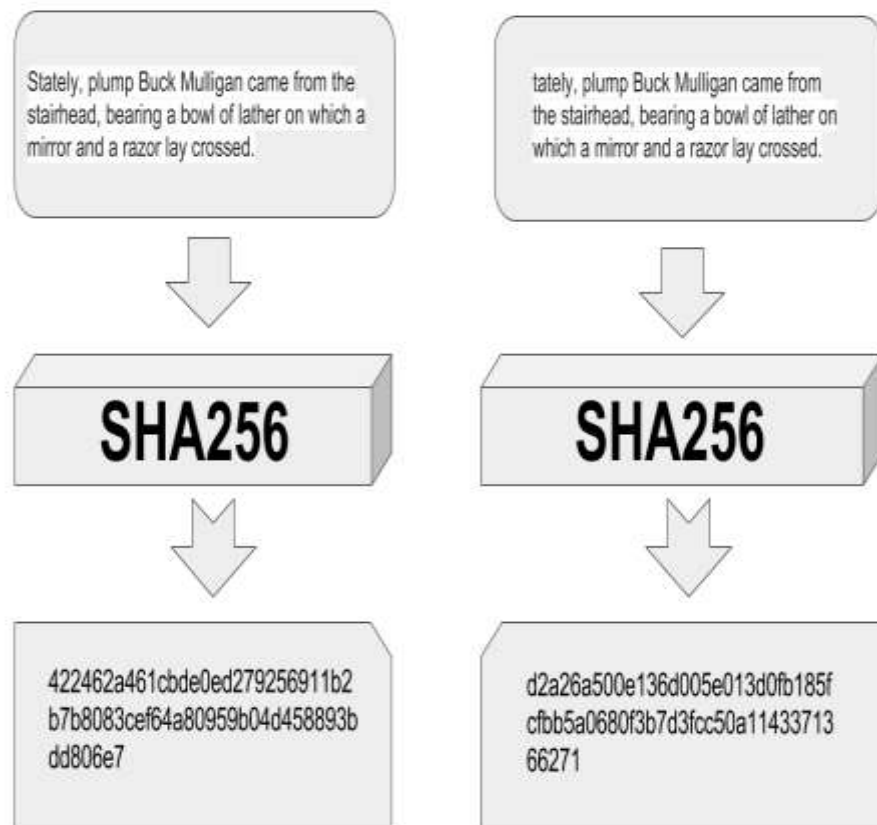




# POINTS FOR FOOL-PROOF CHAIN – OF- CUSTODY



- Always **accompany evidence with their chain of custody forms**
- Give evidence **positive identification** at all times that is **legible and written with permanent ink**
- **Establishing the integrity** of the seized evidence through forensically proven procedure-”**hashing**”
- **Hashing helps the IO 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.



# 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



# 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.

## Steps Volatile Evidence Acquisition

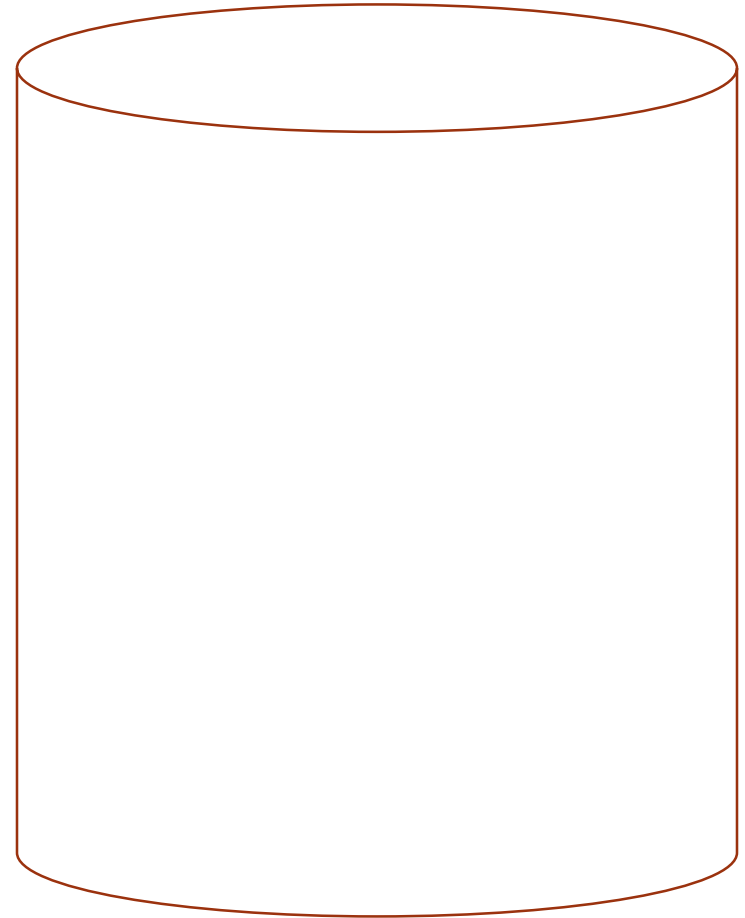
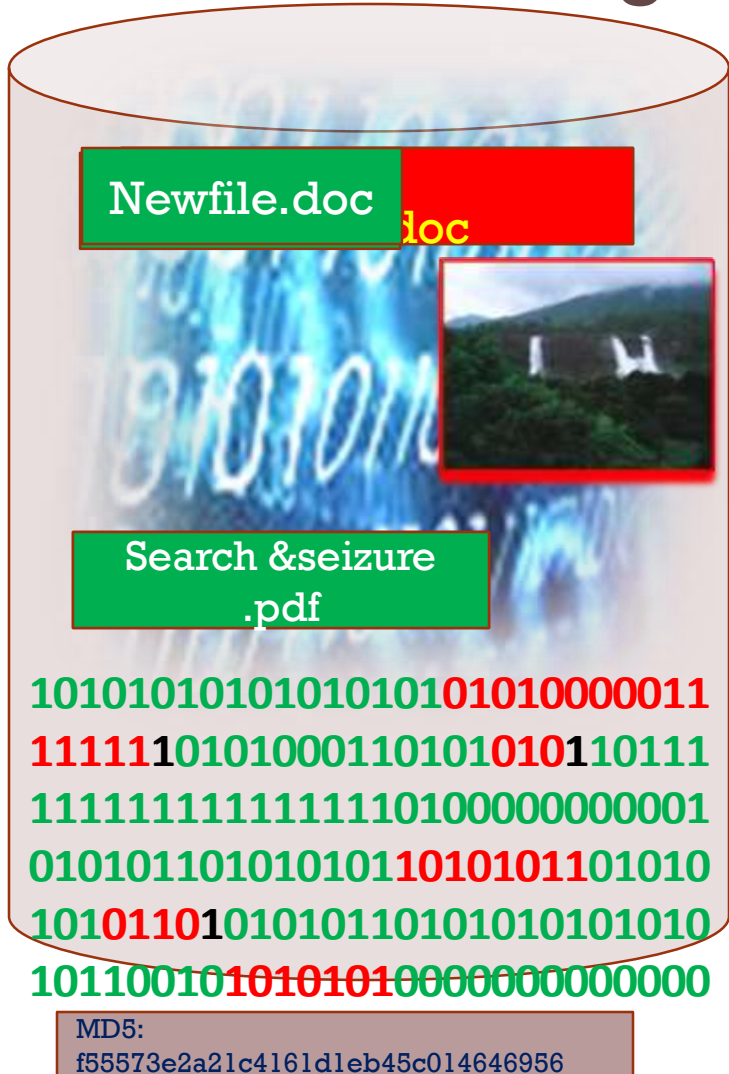
- 
- Risk Assessment
  - Install Volatile Data Capture Device
  - Run Volatile Data Collection Script
  - Stop The device
  - Remove the device
  - Verify the data output





Suspected disk  
(Source)

# Imaging of the Disk

Sterile disk  
(Target)



-  Active files
-  Deleted files





# 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









# 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..

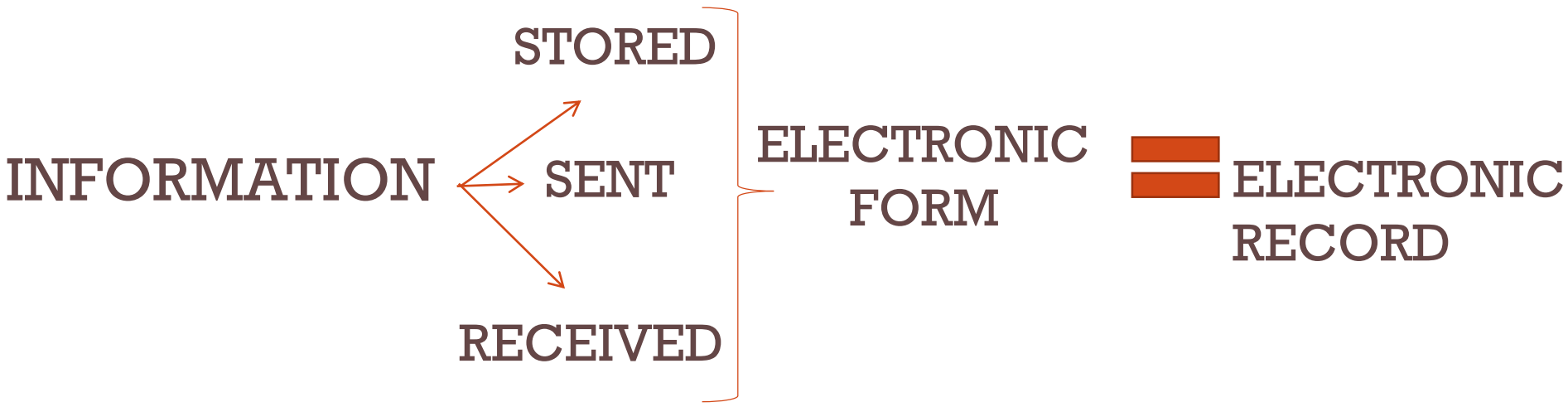
- **S.2(1) (t)-‘electronic record’**-data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.....
- 65B,,,,,,,,,,,,,,,,,,,,,printed on paper, stored, recorded or copied in optical or magnetic media produced by a computer (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.





# 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) by 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.



# THE MAIN CONDITIONS LAID DOWN IN THE SECTION ARE:-

- (i) the computer output, sought to be produced in evidence; must have been produced by a computer which was being used regularly for storing or process of the said information;
- (ii) such computer output, as sought to be produced before the Court, should have been entered into the computer for an activity which regularly carried out on that computer during the relevant period;
- (iii) such a regular activity on that computer must have been carried out by a person having lawful control over the use of that computer;
- (iv) the kind of information sought to be produced before the Court must be the information which was regularly fed in such a computer in ordinary course of the said activity;



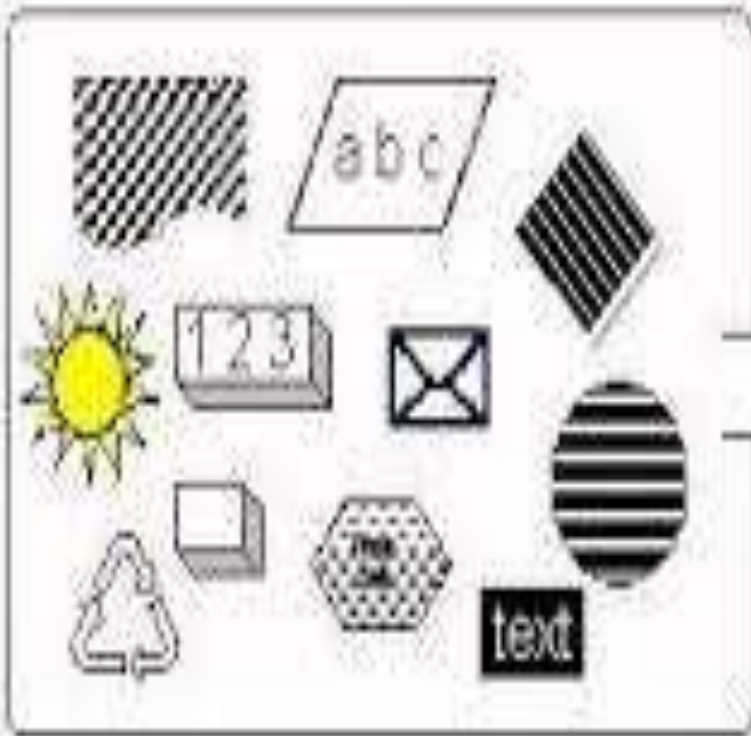
# CONTD....

- (v) such a computer, from which the information sought to be produced before the Court, was taken, should have been operated properly during the period when the information was processed by the computer, and if there was any defect in that computer, then the defect should not be of that nature which could have affected the electronic record or the accuracy of its contents;
- (vi) the information sought to be produced must be the exact copy of the information which was fed in the computer in ordinary course of such activities.





# Your Data



# Computer Data

```
01110101011010101
10100101011010101
01010101011010101
01000101011010101
01101010101001100
00101011101100111
10101001010101010
```

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.



# 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.



# RELEVANT CASE LAWS IN BRIEF

- **State of Maharashtra v. Dr. Praful B Desai (2003) 4 SCC 601**- no bar to the examination of a witness by video conferencing being essential part of the electronic method.
- **State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600**- cross-examination of the competent witness acquainted with the functioning of the computer during the relevant time and the manner in which the printouts of the call records were taken was sufficient to prove the call records
- **State of Punjab vs. Amritsar Beverages Ltd. (2006) 7 SCC 607**- proper course for the officers in such circumstances was to make out copies of the hard disk or to obtain a hard copy and affix their signatures or official seal in physical form upon the hard copy and furnish a copy to the dealer or the person concerned
- **Mohd Ajmal Mohammad Amir Kasab v. State of Maharashtra (2012) 9 SCC 1- Bombay Blast Case** - relevance of electronic evidence is also evident in the light of wherein production of transcripts of internet transactions helped the prosecution case a great deal in proving the guilt of the accused
- **Tukaram S. Dighole vs. Manikrao Shivaji Kokate, (2010) 4 SCC 329**-that new techniques and devices are order of the day and though such devices are susceptible to tampering, no exhaustive rule could be laid down by which the admission of such evidence may be judged.



# CASE LAWS CONT...

- **Tomaso Bruno V State of UP (2015) 7 SCC 178** - scientific temper in the individual and at the institutional level is to pervade the methods of investigation- computer generated electronic records in evidence are admissible at a trial if proved in the manner specified by Section 65B of the Evidence Act
- **Anvar vs Basheer (2014) 10 SCC 473** Supreme Court held that the admissibility of secondary evidence depends upon the satisfaction of the conditions as prescribed under Section 65 B. It was further held that if the primary evidence of the electronic record is adduced i.e. the original electronic records itself, then the same is admissible in evidence without compliance with section 65B

**State V M.R. Hiremath (2019) 7 SCC 515**  
Need for production of certificate under Section 65 (B) would arise only when the electronic record concerned is sought to be produced in evidence at the trial

## **P.Gopalakrishnan V State of Kerala-2019 SCC Online SC 1532**

Contents of a memory Card is an electronic Document- In cases involving privacy of an individual, the court may be justified in not handing over a cloned copy but can instead provide an opportunity to inspect the accused, his counsel and expert.

**Shafhi Mohammed vs State of Himachal Pradesh (2018) SCC 807** -Where electronic evidence is produced by a party who is not in possession of a device, applicability of S.63 and S.65 of the Evidence Act cannot be held to be excluded- It was further held that the applicability of requirement of certificate being procedural can be relaxed by court wherever interest of justice so justifies.

**Arjun Panditrao Khotkar vs Kailash and Ors** it was held by a the SC that the decision rendered in Shafhi requires reconsideration in view of Anvar which held the field earlier



# 4 CRIME SCENE MISTAKES THAT CAN SINK A CYBER FORENSIC INVESTIGATION

- **Mistake #1: Inadequate crime scene preservation**
- **Mistake #2: Missing the one chance for picture perfect**
- **Mistake #3: Lack of communication**
- **Mistake #4: Not having plans, policies and rules**





Final Thoughts

11001  
01100  
10011



- **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.**



