Nuances of Search & Seizure of Electronic Evidence

Presented By: M K SIL

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 in issue; the information that constitutes the evidence before the court. It is commonly known as Digital Evidence.

Evidence

Regardless of whether the evidence is physical evidence, trace evidence, biological matter, or electronic evidence residing on a specialized device, all evidence must be treated the same.

Characteristics of Electronic Evidence

- Is invisible
- Is easily altered or destroyed
- Requires precautions to prevent alteration
- Requires special tools and equipment
- Requires specialized training
- Requires expert testimony

Where is Electronic Evidence

- Any kind of storage device
- Computers, CD's, DVD's, floppy disks, hard drives, USB drives,
- Digital cameras, memory sticks and memory / SIM cards, PDA's, cell phones
- Fax machines, answering machines, cord less phones, pagers, caller-ID, scanners, printers and copiers
- CCTV

Traditional data sources for electronic evidence


Desktop computers


Laptop computers


Servers including multiple disk storage


USB devices


CD/DVDs


Floppy disks


Backup devices including tapes

New sources of electronic evidence


Mobile phones including smart phones

GPS navigation devices – these devices can record location data


Multi-Function Printers (MFP's) – these devices can store print logs and potentially print jobs


Digital video recorders


Digital voice recorders


Digital still cameras including SD/CF cards and other types of memory cards


Internet and cloud storage (see callout box below)

Challenges with Electronic Evidence

Electronic Evidence plays larger role in Criminal Investigations.

Process of Acquisition, Authentication, and legal Admissibility of information stored on magnetic and or any other storage media is a challengeable task in Electronic evidence.

- Electronic evidence, by its very nature is invisible to the eye, must be developed using tools other than the human eye.
- Each step requires the use of specialised tools or / and knowledge, the process must be documented, reliable and repeatable.
- The process itself must be understandable to the court.
- Acquisition of evidence is both a legal and technical problem.
- The law specifies what can be seized, under what conditions, from whom, and from where it may be seized. The determination of what a particular piece of digital evidence is, requires its examination.

Chain of Custody & Evidence Handling?

- A process that tracks the movement of evidence through its collection, safe guarding, and analysis lifecycle by documenting each person who handled the evidence, the date / time it was collected or transferred, and the purpose for any transfers.

Admissibility: Before and In Court

Admissibility: Before Court

- Evidence collection
  - Correct legal processes
  - Accepted techniques and tools
  - Properly trained personnel
- Chain of custody
- Testimony of Experts
- Corroboration

Admissibility: In Court

- Presentation techniques
  - Graphics – “Showing and telling is better than just telling”
  - Ask them to explain the story if the technical issues are complex
- Made it as simple as by using appropriate techniques

Category Of Evidence

- Oral Evidence – Chapter IV of Indian Evidence Act
- Documentary Evidence – Chapter V of Indian Evidence Act

- General Rules of Evidence
  - Admissible
  - Authentic
  - Complete
  - Reliable & Believable

Common Electronic devices that Generate Electronic Evidence

- Sources of Digital Evidence
  - Internet based
  - Stand alone computer or devices
  - Mobile devices

Search & Seizure of Electronic Evidence – The relevant legal procedures - An Overview

- Chapter VII of CRPC 1973
  - Sec 91 – 100 relating to the summons to produce documents or other things with or without warrant.
  - A warrant is a legal document that issued by a Judge or Magistrate authorizing police officer to make arrest, search, seizure, seize properties and take action.

Search & Seizure of Electronic Evidence – The relevant legal procedures - An Overview cont…

- "EVIDENCE" TERM : STATUTORY PROVISIONS

- Section 3 of Indian Evidence Act, 1872 defines
- "Evidence" means and includes:
  - All documents including electronic records for the inspection of the court.
- Electronic Records
  - As per Sec 2(1)(t) of IT Act, 2000, it means:
    - Data record or data generated
    - Image or sound stored
    - Received or sent in electronic form or microfilm or computer generated microfiche
- Electronic Form
  - As per Sec 2(1)(r) of IT Act, 2000 with reference to information means
    - Any information generated, sent, received or stored
    - in media, magnetic, optical, computer memory, microfilm, computer generated microfiche or similar device.

Search & Seizure of Electronic Evidence – The relevant legal procedures - An Overview cont…

- "EVIDENCE" TERM : STATUTORY PROVISIONS – cont..
- Information
- – As per Sec 2(1)(v) of IT Act, 2000 it includes:
  - Data - Codes - Computer generated -Text
  - Computer programmes -Images - Software
  - Microfiches -Sound - database
  - Voice -Microfilm
- • Section 4 of IT Act, 2000 gives legal recognition to the Electronic records on two conditions
  - Rendered or made available in an electronic form.
  - Accessible so as to be usable for a subsequent reference.

Oral Evidence Vs Documentary Evidence

- Oral Evidence:
  - Section 22A declares Oral Evidence as to the contents of electronic records are not relevant unless the sanctity of electror record produced is in the question.
  - The foremost / primary requirement is to prove the sanctity of the document to make it admissible in the court of law.
- Documentary Evidence - Evidence can be of two types:

  Primary evidence: Sec 62 and Sec 64 Primary evidence means the document itself produced for the inspection of the Court.

  Secondary evidence: Sec 63 and Sec 65 Secondary evidence means Copies made from the original by mechanical processes which in themselves ensure the accuracy of the copy.

Admissibility of Electronic Evidence

- 65A and 65B are introduced to the Evidence Act under the Second Schedule to the IT Act.
- Section 5 of the Evidence Act provides that evidence can be given regarding only facts that are at issue or of relevance.
- Section136 empowers a judge to decide on the admissibility of the evidence.
- 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 anything contained in the Evidence Act, any information contained in an electronic record (i.e. the contents of a document or communication printed on paper that has been stored, recorded and copied in optical or magnetic media produced by a computer ('computer output')) , is deemed to be a document and is admissible in evidence without further proof of the original's production, provided that the conditions set out in Section 65B (2) to (5) are satisfied.

IT ACT 2000

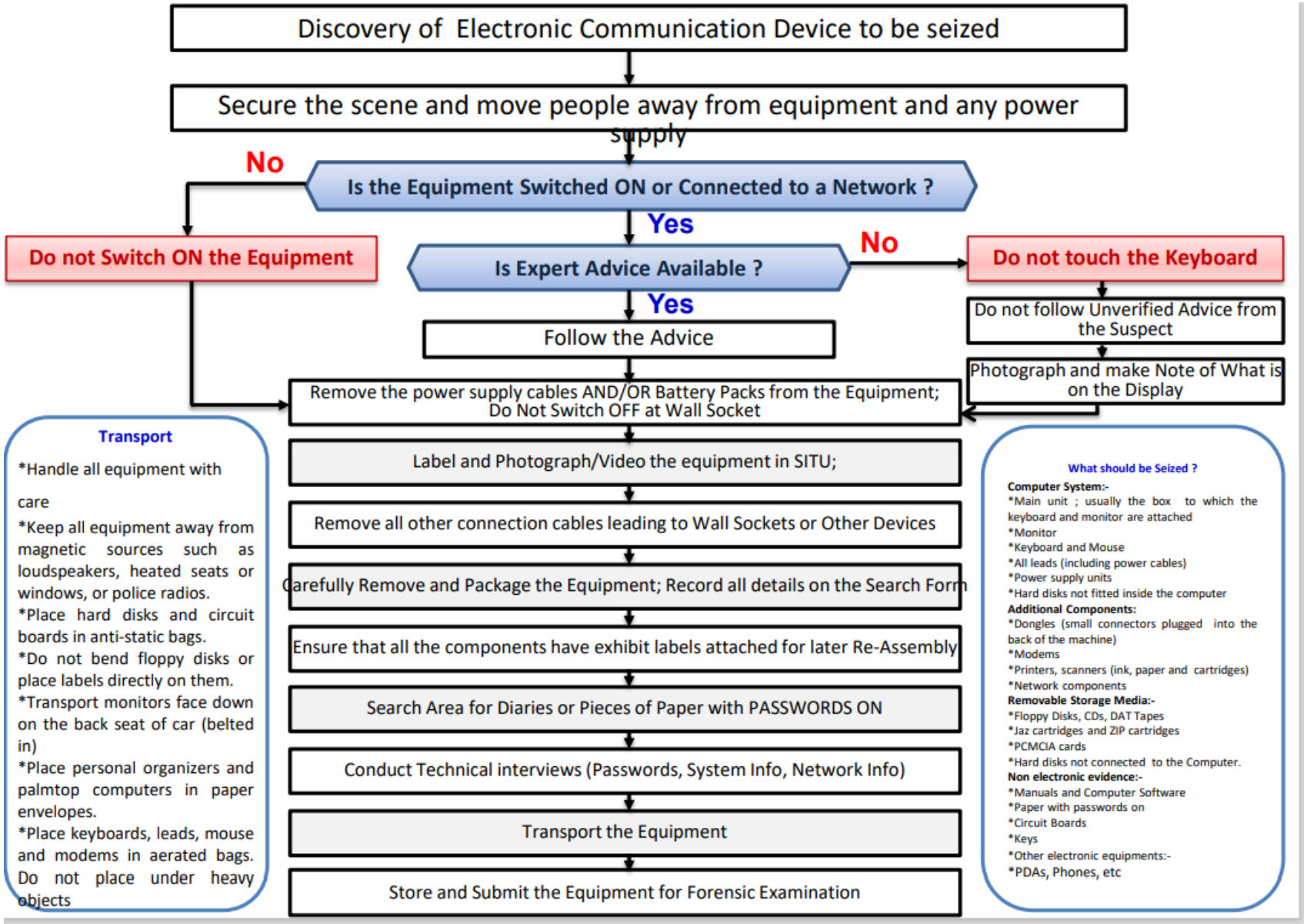
In India **Information Technology Act, 2000**

- On 17th October 2000, ITA 2000 was notified and along with it the Indian Evidence Act 1872 got amended with several new sections being added to address the issue of Electronic Evidence
- Investigation and adjudication of cyber crimes is done in accordance with the provisions of the Code of Criminal Procedure and the IT Act.
- The Indian Penal Code (as amended by the IT Act) penalizes several cyber crimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc.

Section 80

- Power of police officer and other officers to enter, search, etc.-(1) Not withstanding any thing contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Inspector of Police, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found there in who is reasonably suspected or having committed or of committing or of being about to commit any offence under this Act.

Seizure of Electronic Equipment



Electronic FORENSIC KIT

- A Electronic forensics field response kit may contain some of the following:
- 1. Electronic camera
- 2. Sterilized removable media
- 3. Forensic computer
- 4. Hardware write-blocking devices
- 5. Forensically sound boot disks
- 6. Mobile device acquisition tools
- 7. Tool kit (screw drivers, etc.)
- 8. Evidence packaging materials

Cyber Crime →Introduction

- Cyber crime in the present scenario assume greater responsibility to the Law enforcement agencies specially police officer being the nodal agency of the Country maintain law and order and crime detection. Police officers are duly empowered under the provisions of CRPC 73. The detection assumes greater importance while combatting the Cyber crime.

Indian Cyber Laws

Indian Cyber Laws were official born on 17th October 2000 with the Information Technology Act, 2000 coming into force.

- The Indian Penal Code (as amended by the IT Act) penalizes several cyber crimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc.
- Electronic Evidence is to be collected and proven in court as per the provisions of the Indian Evidence Act (as amended by the IT Act).
- In case of bank records, the provisions of the Bankers' Book Evidence Act (as amended by the IT Act) are relevant.
- Investigation and adjudication of cyber crimes is done in accordance with the provisions of the Code of Criminal Procedure and the IT Act.

Cyber Crime :- A few Cases

A few cyber crime cases so detected and offences involved in teams of IPC

- Sending threatening and defamatory message by e-mail – sec 503 & 499 IPC
- Forgery of electronic records like fake visa ,images etc. – sec 463 IPC
- Bogus website cyber fraud like hackers, OTP , false calls etc.- sec 420 IPC
- E-mail spoofing and abuse – sec 463 & 500 IPC
- Web jacking (Ransom on sport) – section 383 IPC

* Online Sale of Drugs / NDPS i.e medicine with false and forged prescription etc.- NDPS act 1985

* Online sales Arms without physical presence. – Arms Acts.

Conclusion

Reliability of Electronic Evidence depends on proper collection, preservation & production in the court proceedings.

A breach in the chain of custody or improper presentation of such evidence renders Electronic evidence vitiated, unreliable in Judicial proceedings.

Thank you