Appreciation of Electronic Evidence

By Neeraj Aarora
Advocate, Supreme Court
CISSP, CISA, FCMA, CEH, CFCE

Learning Objectives

- Introduction – Electronic Evidence
- Electronic Records & their Admissibility
- Relevant Provisions of Sri Lanka Laws
- Hard Disk, SMS, Computer Printouts, Banking Records, Email etc.

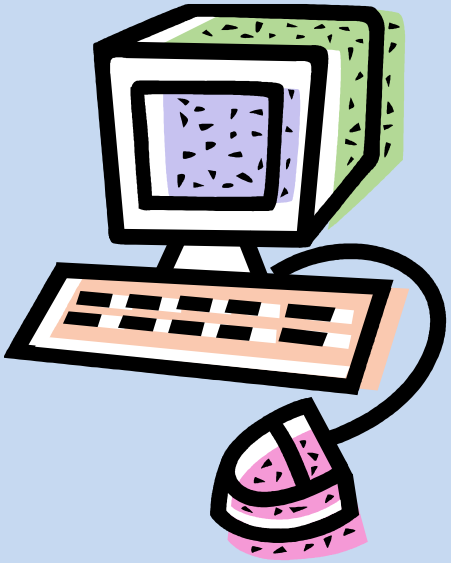
Challenges of Digital Evidence

- Identifying the Electronic Evidence;
- Seizure and Preservation of Electronic Evidence;
- Forensic Examination Process
- Presenting the Evidence in Court;

Electronic Evidence- Important Consideration

Computer Output or Computer as a Tool

- *Use of computer as a tool*
- *Record generated by Software*
- *Record partly fed & partly generated*

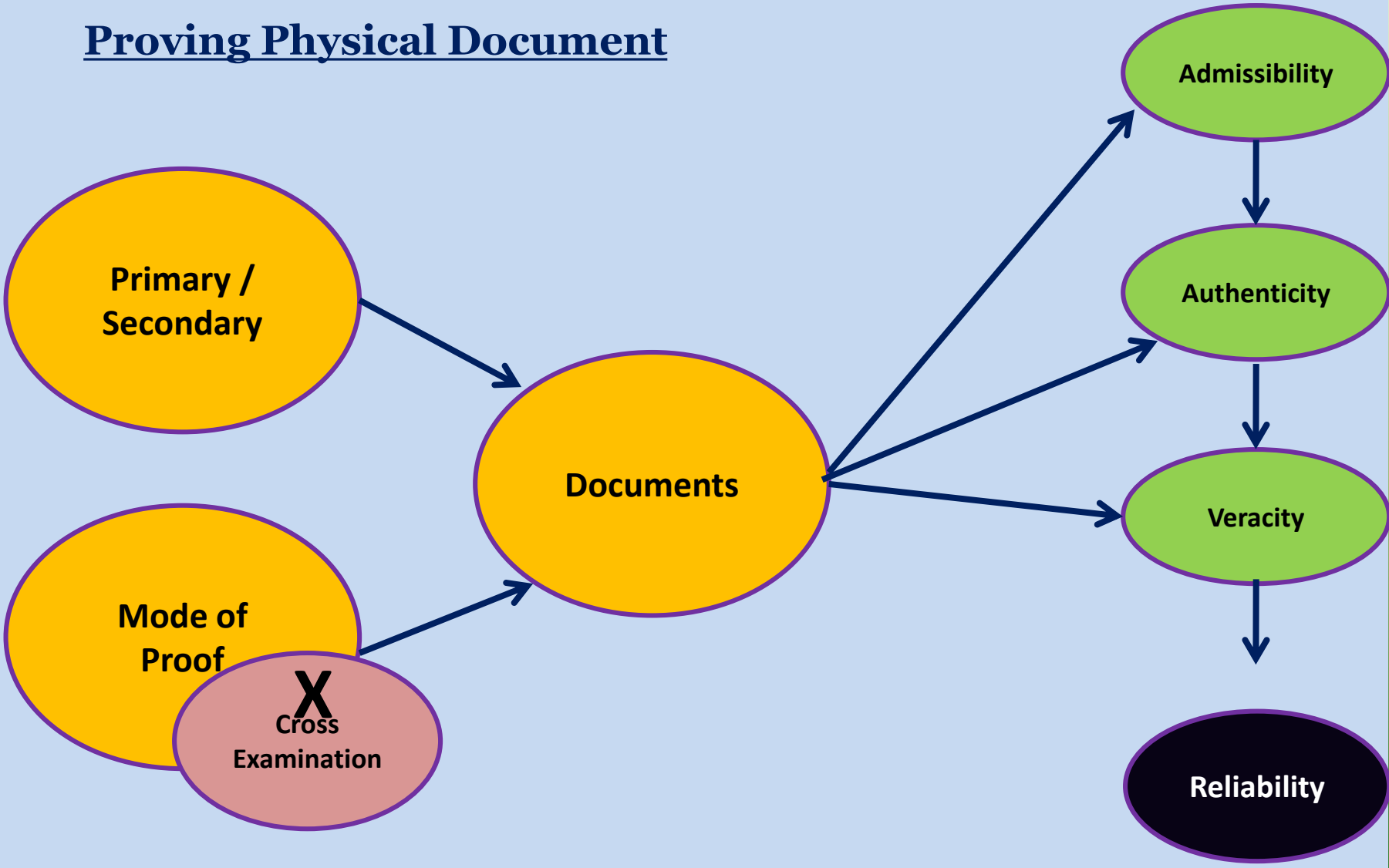


Other Characteristics of ESI:

- *Volatile and easily alterable*
- *Easily Manipulated/Forged*
- *Encryption & Cloud Computing*

Proving Electronic Documents – New Admissibility Issues

Proving Physical Document



Electronic Records Are Documents

- **Section 3 of EA**

  "Evidence" – 'Evidence' means and includes—

  (1) all statements which the Court permits or requires to be made before it by witnesses, in relation to matters 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.

Electronic Record under IEA

- **2(r) "Electronic Form"** with reference to information means any Information Generated, Sent, Received or stored in Media, Magnetic, Optical, Computer Memory, Micro Film, Computer Generated Micro Fiche or similar device;

- **2(t) "Electronic Record"** means Data, Record or Data Generated, Image or Sound Stored, Received or Sent in an Electronic Form or Micro Film or Computer Generated Micro fiche;

Electronic under ETA (Sri Lanka)

- **(26)"Electronic Record"** means a written documents, or other record created, stored, generated, received or communicated by electronic means;

- **(26) Electronic** means information generated, sent, received or stored by electronic, magnetic, optical or similar capacities regardless of the medium;

Requirement of Metadata – Sec 4 & 7, IT Act

- **Legal Recognition of Electronic Record** – Information is in electronic form and accessible for subsequent reference

- **Retention of Electronic Record-** The record are retained in electronic form if

  (a) Information remains accessible for a subsequent reference

  (b) the electronic record is retained in the format in which it was originally generated, sent or received.

  (c)Maintains details facilitating the identification of origin, destination, date & time of dispatch and receipt of electronic record

Recognition of Electronic Data – Sec 4 & 6 ETA Sri Lanka

- **Legal Recognition of Electronic Record** – Information is in electronic form and accessible for subsequent reference

- **Retention of Electronic Record-** Notwithstanding the fact that such information was not originally generated in electronic form, if the record are retained in electronic form and

  (a) Information remains accessible for a subsequent reference

  (b) the electronic record is retained in the format in which it was originally generated, sent or received.

  (c)Maintains details facilitating the identification of origin, destination, date & time of dispatch and receipt of electronic record

Section 65B - Admissibility of Electronic Records

Sec. 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 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.*

Section 65B – Admissibility of Electronic Records

Sec. 65B(2):

1. The **computer** from which the record is generated was **regularly used to store or process information in respect of activity regularly carried on** by a person having **lawful control over the period**, and relates to the period over which the computer was regularly used;

3. The **computer** was operating properly, and if not, was not such as to affect the electronic record or its accuracy;

Regularly Used to Store or Process the Information Activity Regularly Carried Out

Lawful Control Operating Properly

Section 65B – Admissibility of Electronic Records

Sec. 65B(2):

Contd...

2. **Information** was fed in computer in the ordinary course of the activities of the person having lawful control over the computer;

4. **Information** reproduced is such as is fed into computer in the ordinary course of activity.

Ordinary Course of Activities Information Fed & Derived

Information Derived from Information Fed

Section 65B – Computer/Groups of Computers

Sec.65B(3): The following computers shall constitute as single computer-

- *by a combination of computers operating over that period; or*
- *by different computers operating in succession over that period; or*
- *by different combinations of computers operating in succession over that period; or*
- *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,*

- **Printout from LAN/WAN**
- **Change of technology**

Section 65B – Contents of certificate

Sec. 65B(4): Contents of certificate may contain any of the following -

- *identifying the electronic record containing the statement and describing the manner in which it was produced;*
- *giving the particulars of any device involved in the production of that electronic record*
- *dealing with any of the matters to which the conditions mentioned in sub-section (2) relate,*

Section 65B – Competent Person to be Issue

Contd...

- *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.

ANVAR P.V. VS. P.K. BASHEER AND OTHERS [MANU/SC/0834/2014]

The Supreme Court held:-

- The original electronic record is admissible as a primary evidence u/s 62 EA.
- Electronic Record can be produced in terms of Section 65B Evidence Act which has overriding effect.
- If no certificate under Section 65B, no expert opinion u/s 45EA can be resorted to prove the electronic record.
- If no certificate u/s 65B, no oral evidence can be resorted
- Section 65B would prevail over Section 63/Section 65 of Evidence Act.

SRI LANKA- Admissibility of Electronic Evidence

- Evidence (Special Provisions) Act (No. 14 of 1995)
  - Sec. 5 – Computer Evidence
  - Section 7 - Notice to have access to inspect
- Electronic Transactions Act 19 OF 2006
  - Requirement of Original Form – Sec 5
  - Rules Governing Evidence – Sec 21 & 22

Requirement of Original Form – Sec 5 (ETA)

- **To prove the original form of an electronic record**
  - If there exist a reliable assurance as to the integrity of the information from the time when it was made available in electronic form and
  - The information contained in data message, electronic documents, electronic record or other communication is available and can be used for subsequent reference.
  - **2(a) –** whether such information as remained complete & unaltered apart from the addition of any endorsement or any change which arise in the normal course of communication, storage or display
  - **2(b) –** standard of reliability of assurance shall be assessed having regard to the purpose for which the information was generated and all other relevant circumstances

Admissibility of Electronic Evidence – ETA Sri Lanka

- **(2) Any information contained in a Electronic Record/Communication**

  (a) touching any fact in issue or relevant fact ; and

  (b) compiled, received or obtained during the course of any business, trade or profession or other regularly conducted activity, shall be admissible in any proceedings:

  Provided that,

  direct oral evidence of such fact in issue or relevant fact if available, shall be admissible ; and

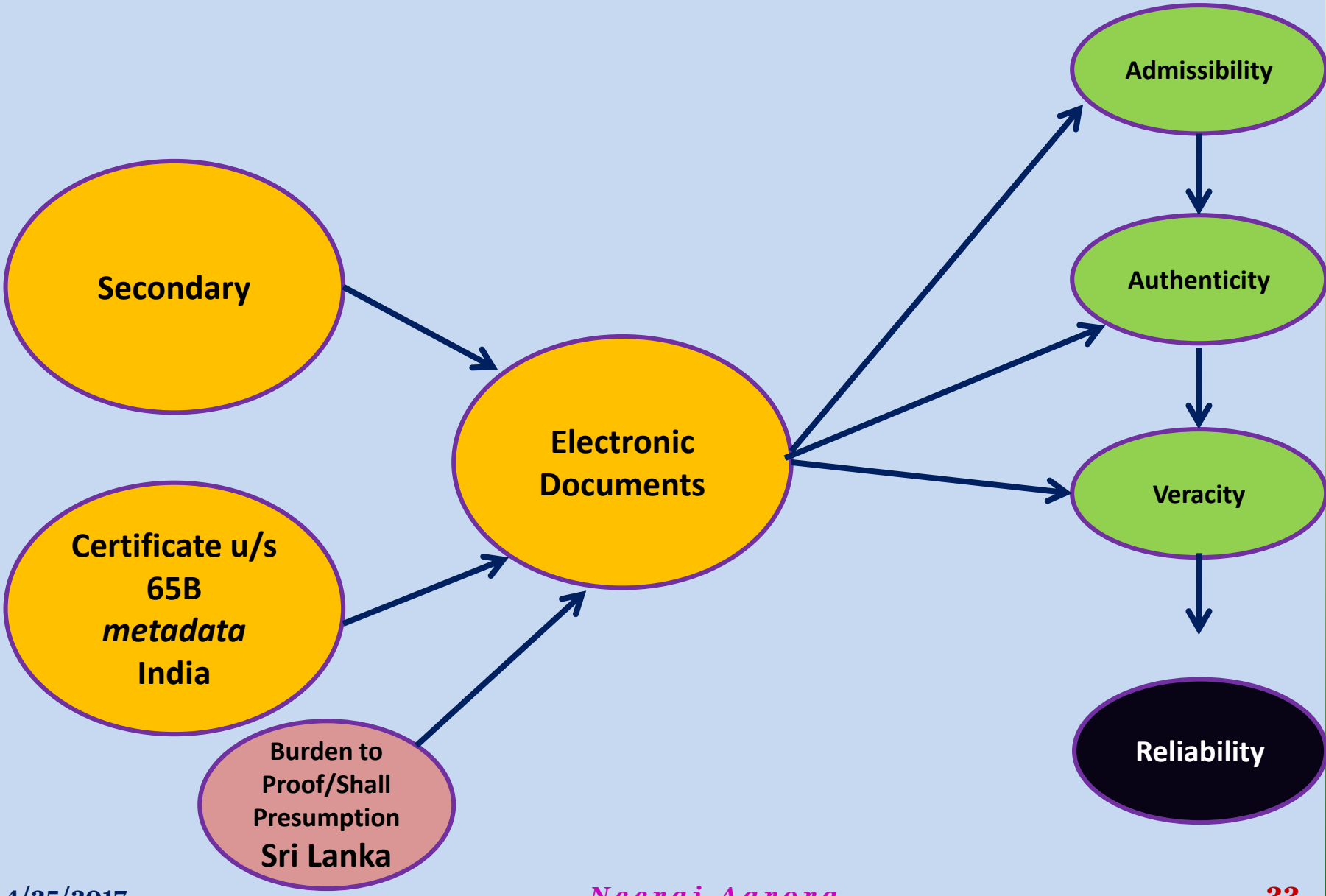
  there is no reason to believe that the information contained in a data message, or any electronic document, electronic record or other communication is unreliable or inaccurate

Admissibility of Electronic Evidence – ETA Sri Lanka

(3) The Courts shall, unless the contrary is proved,

- presume the truth of information contained in a data message, or in any electronic document or electronic record or other communication and
- in the case of any data message, electronic document, electronic record or other communication made by a person, that the data message, electronic document or electronic record or other communication was made by the person who is purported to have made it and
- similarly, shall presume the genuineness of any electronic signature or distinctive identification mark therein.

Proving Electronic Documents- Secondary



Proving Electronic Evidence– Other Considerations

- Section 58 – facts admitted need not be proved
- Section 22A – Oral admission as to content of electronic documents
- Section 65(b) – Secondary copy is filed by the party in possession of original
- Section 106 – Burdon of proving fact the especially with knowledge
- Section 114 – Court may presume existence of certain facts

Section 65B – Proving Electronic Evidence

- **Proving the Electronic Evidence**
  - *Relevancy and admissibility*
  - *Genuineness, veracity & reliability*

- **Kundan Singh Vs. The State [MANU/DE/3674/2015]**

- **ANVAR P.V. VS. P.K. BASHEER AND OTHERS [MANU/SC/0834/2014]**

Challenges as to Integrity

- **Integrity test (*Kishan Tripathi Vs. The State*)**
  - System Integrity
  - Record Integrity
- **Unauthorized Access to Media**
  - Lapse on the Part of Prosecution
- **Mobarik Ali Ahmed Vs. State of Bombay, AIR1957 SC857**
  - Metadata or Internal Evidence

Holistic Approach to proving of Electronic Evidence

Genuineness

- **System Integrity**
  - Identity of the Computer
  - Original or Secondary
- **Record Integrity**
  - Creation to Computer Output
  - Computer output to Production in Court

Veracity

- Truthfulness or quality

Reliability

- Free from material error, bias, not false

Holistic Approach to proving of Electronic Evidence

- **Challenge**
  - Preservation & Sanctity of record after its creation
  - Process, procedures for use of equipment
  - Access policies
- **Unauthorized Access**
  - Metadata or Internal Evidence
- **Probative Value**
  - Genuineness, Veracity & Reliability
  - Corroborative Material
  - Contradictory Material

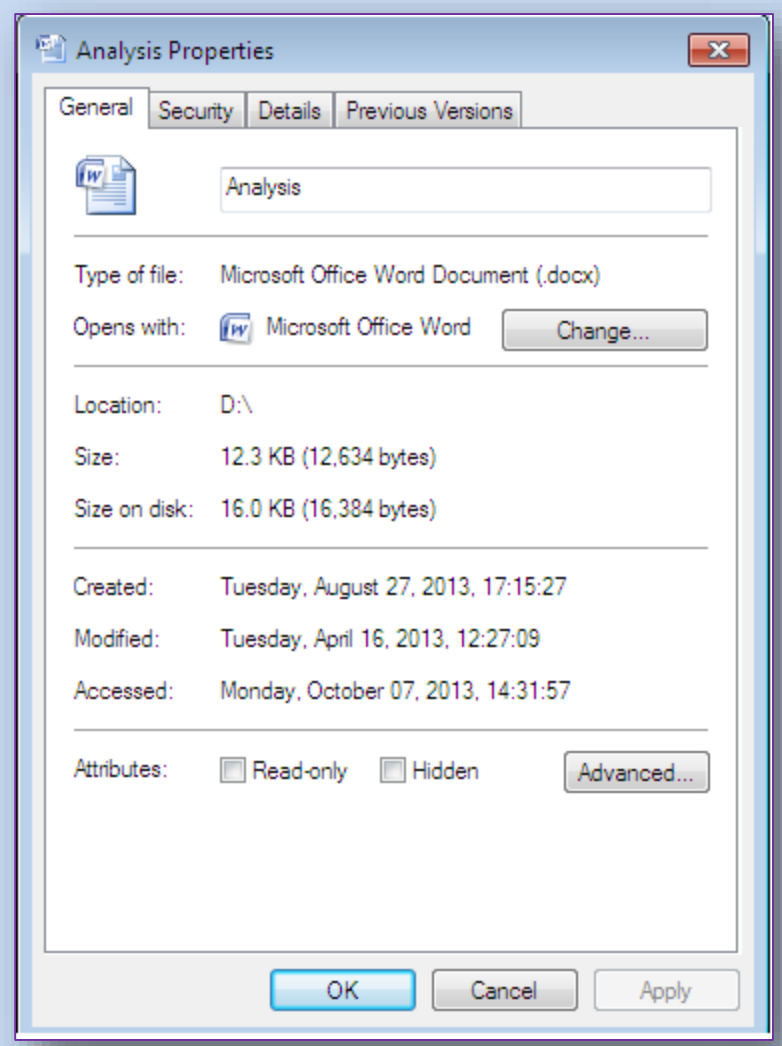
Metadata

- **BTK Killer Dennis Rader**
  - *BTK – Bind, torture and kill*
  - *Committed 10 murders between 1974-1991*
  - *Send boasting letter to police & newspaper*
  - *Send email/letter in one of floppy*
  - *Name of the author, as Dannis and name of his organization – Christ Lutheran Church*

- **Williams v. Sprint/United *Mgmt Co*., 2005 WL 2401626 (D. Kan. Sept. 29, 2005),**

  the Federal court ruled that "when a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order."

Word Metadata



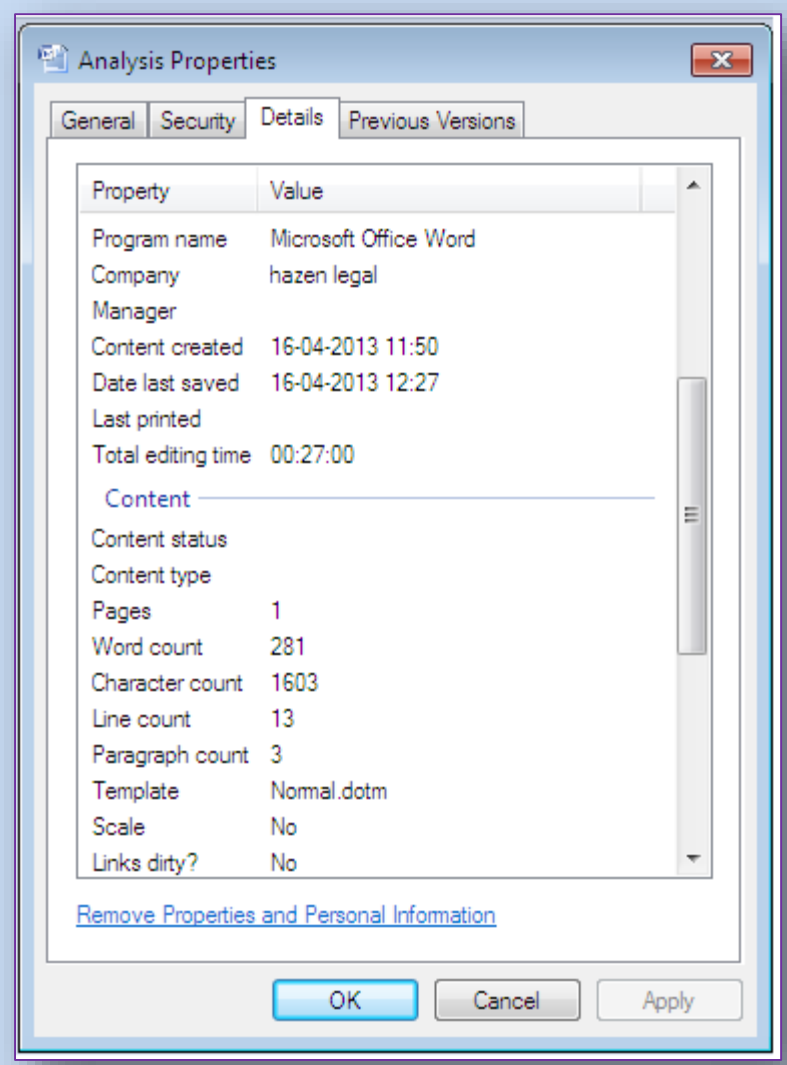
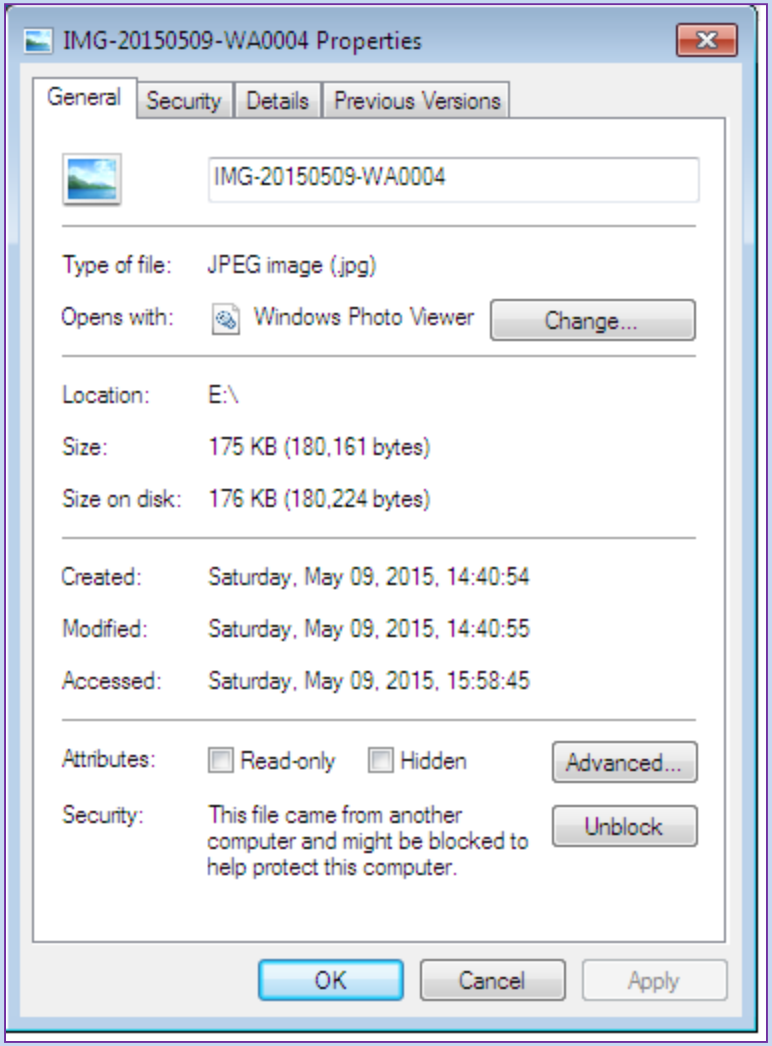
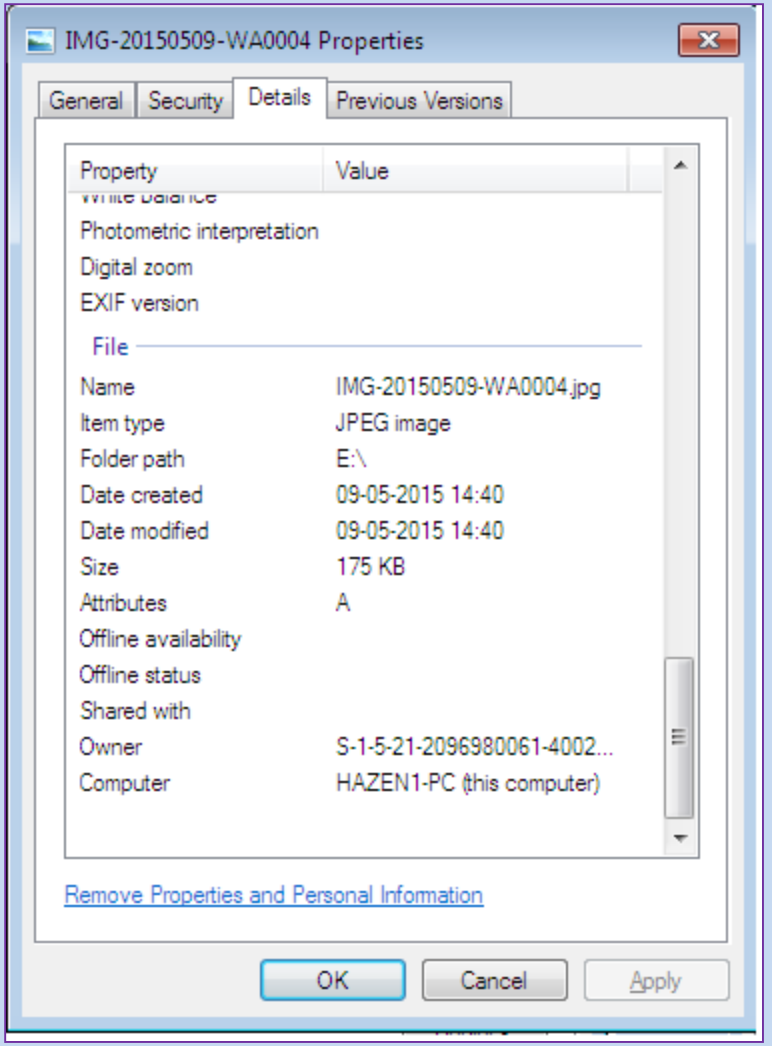


Image Metadata





Electronic Evidence- Challenges

- **Data from**
  - *Witnesses*
    - *Interested Witness- Complainant*
    - *Independent Witnesses*
  - *Accused*
    - *Recovery consequent to disclosure*
    - *Recovered during seizure in CDs/DVDs*

- **Retention of Data**

Hashing – Emerging Challenge

Solid State Drive

- **Garbage Collection**
- **Wear Levelling**
- **TRIM**
- **Challenge**
  - *Hash value may not match*
  - *Deleted data may not be recover*

Computer Printouts

- Admissible as per **Sec 65B EA**
- Banker Books :- Require three certificate as per Sec 2A of **BBEA**
  - *A certificate regarding authenticity of entry/printout by the principal accountant or branch manager.*
  - *Authenticity certificate from person in-charge of computer system regarding:-*
    - Details of Computer System
    - Process of Data Storage
    - Safeguard to protect Computer System and Data
  - *such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question.*

Dharmabir Vs. CBI - Admissibility of Hard Disk

- New Hard Disk is a storage device.
- Hard Disk once written becomes a electronic record.
- Hard Disk resorted to original position shall remain a electronic record as deleted data can be recovered to scientific methods.
- Two Levels of Electronic Record:-
  - *Active memory;*
  - *Subcutaneous memory;*
- U/s 207 Cr.P.C. – The accused is entitled to active and subcutaneous memory – Mirror Image.

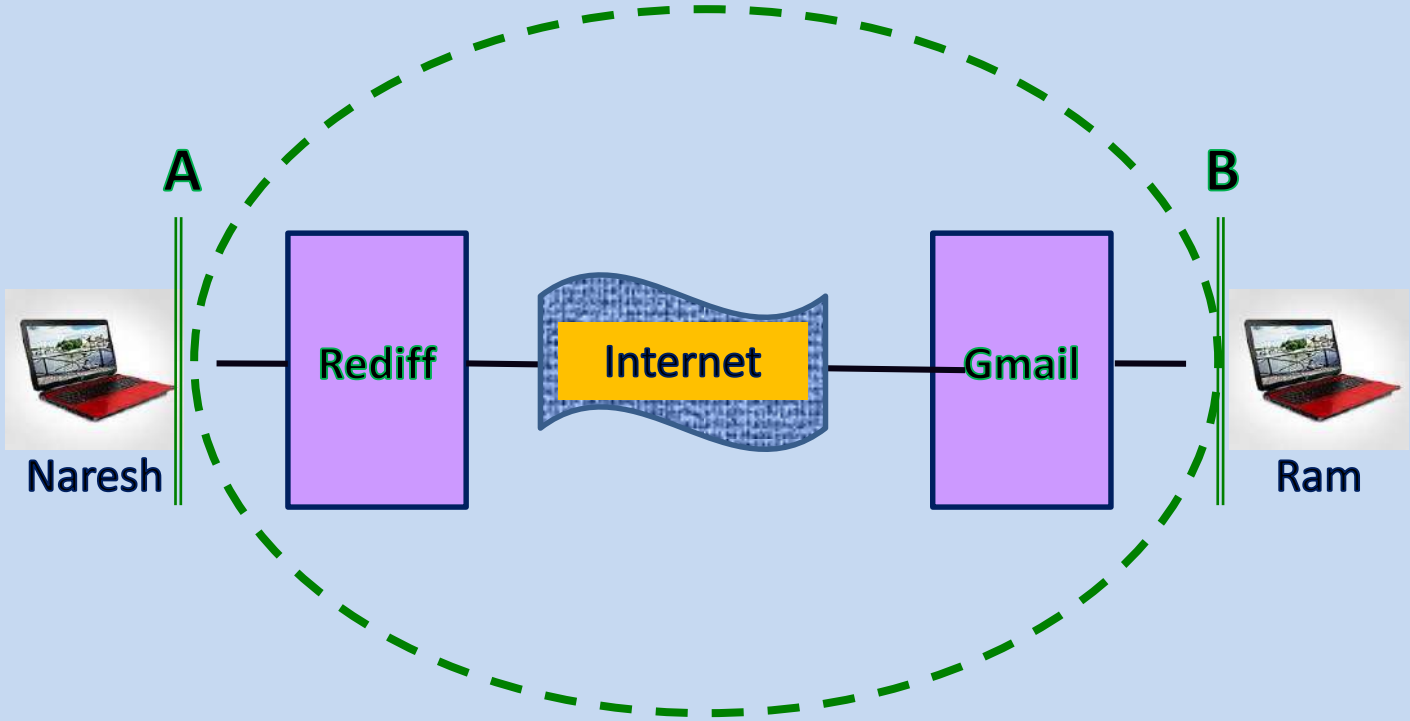
Admissibility of Documents

- **SMS** can be proved by –
  - *Original mobile phone containing the SMS*
  - *Extracted copies of SMS along with Certificate* ***U/s 65B Evidence Act.***
- **Spoofed SMS is a challenge**

Email Admissibility

- **E-mail on web with intermediaries**
  - *Gmail, Hotmail, etc*
  - *Certificate U/s 65B EA*
- **Section 88A – Presumption as to Electronic Messages**
- **E-mail on server of the company**
  - *Server owned by the company*
  - *Certificate u/s 65B by incharge of a computer*
- **E-mail Header Required - Section 7**
- **Forged e-mail - a challenge – https://emkei.cz/**

Presumption U/s 88 A



Legal Challenges of Computer Forensic

- **Open Source Tools vs Close Source Tool**
- **Daubert Principle**
  - *Testing*
  - *Error Rates*
  - *Publication*
  - *Acceptance*
- **Smt. Selvi and Ors. Vs. State of Karnataka**

State of Florida v. Casey Marey Anthony

- *Casey Marie Anthony daughter was murdered. Tests were conducted on air and carpet samples of the vehicle. The reports stated high level of chloroform in trunk of the car.*
- *Investigators searched Anthony's family computer and found searches for 'chloroform'.*
- *The computer forensics unit copied the hard drive using Encase and extracted the internet history data which was fed into two programs: NetAnalysis and CacheBack.*
- *That site was visited once, according to NetAnalysis used by the Police officials, and visited 84 times, according to the forensic expert who used CacheBack analysis .*


Q&A

THANKYOU !

Neeraj Aarora
Advocate-on-Record
Supreme Court
E-mails: neeraj@hazenlegal.com
Website: www.neerajaarora.com
D-10/4, Sector-8, Rohini, Delhi-110085
Ph.011-27940129; +91-9871435035