Cyber Law and forensics

-- Missed Notes --

Situation 3: The monitor is off
→ Two things : ① Monitor is off
② CPU is off

↳ Turn on the monitor
→ check for outside connectivity
↳ If telephone number is present, attempt to identify the telephone number.
→ Avoid damage to potential evidence by removing any floppy disks
↳ package disk seperately and labeling the package

→ Photograph and diagram the connections of the computer and corresponding cables.
→ Label all connectors and cable ends
→ Collect non-volatile data
→ Remove cable and take hard drive if computer is off.

[Crime Scene flow chart]

Primary crime scene : Scene where crime occured
Secondary crime scene : Culprit threw evidence at another location. That location is 2° crime scene (discovered evidence)

Evidence packaging, transporting and storing

If multiple computer systems are collected, label each s/m so that it can be reassembled as found

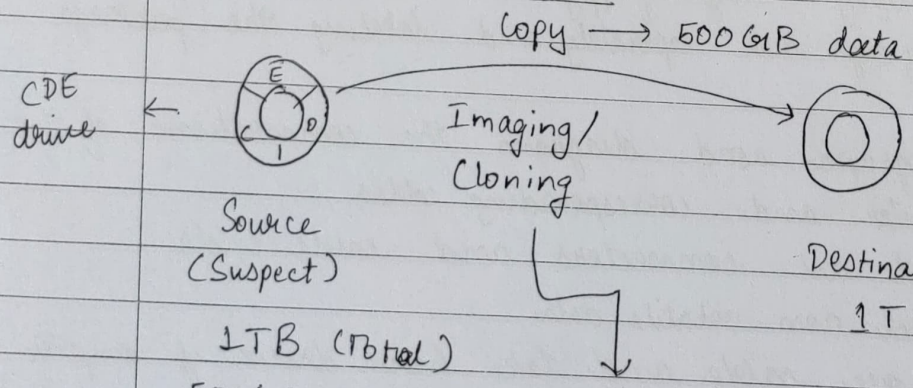
Transporting

→ Monitor placed on seat with screen down.
→ All package are secured to avoid shock.
→ Keep away from magnetic source

Storing

→ Store evidence in a secure area away from temperature and humidity extremes

Copy, image and clone



MBR - Master Boot Record

when Hard drive is cloned, MBR is also cloned

Clone → Boot Req.
Image → No Boot Req. → Compressed

⁂ Imaging always preferred over cloning.

→ For cloning, same size and same RPM required. (limitation)

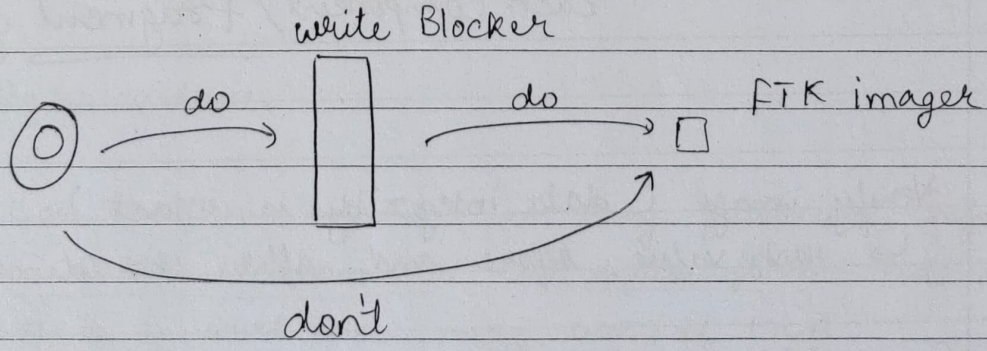
→ Booting required while analyzing evidence.

SAM file → Security Account Manager file
↳ System file → Cannot copy, delete, change.
↳ Cannot be analyzed in running system.

FTK Imager → Data imaging and previewing tool.

Tools to create image → FTK Imager
→ Guymager
→ DD, DCFLDD, DC3DD

→ Data Image
→ Data Preview



Destination Image type
- Raw (dd)
- SMART
- E01
- ~~AFF~~ Aff

Raw(dd) has no compression
Raw(dd) can be converted to any ~~time~~ type.

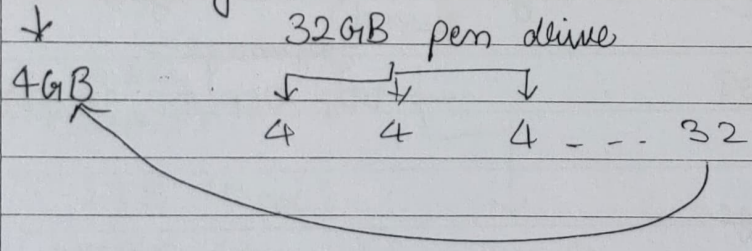
E01 → new format

→ E01 → Expert witness format.

EO1 → compressed (deflate algorithm)
→ contains metadata
→ Most tools support.

AFF4 (New version of AFF)
→ Advanced forensic file format.
→ Container - multiple data source in a single container.
→ Evimetry tool (AFF)
→ Selective imaging.
↳ Only selected file can be imaged
Eg. Only video and photo files.

FAT file System.



Each component / fragment given to FAT

Verify image (data integrity is intact)
↳ Hash value before and after should be same

Sec 3 IEA "Evidence" def.

Cyber crime def^n

Traditional laws & Acts

1306 laws in India

→ Constitution of India
→ Companies act
→ Consumer protection act
→ Indian penal code
→ Indian contract act
→ Indian stamp act
→ Sales of goods act
→ Right of Information act
→ Income Tax act
→ Limitation act (Statute of limitation)
→ Indian evidence act
→ Information technology act

Electronic evidence in smart crimes

At the time of investigation it is the first and foremost duty of forensic expert is to.. for collection to identify sources of digital evidence.

Digital evidence

DE or Electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial.

Sources

→ CPU
→ Monitor
→ Smart card
→ Dongle
→ Digital camera
→ gadget
→ Modem, Server
→ Printer
→ GPS
→ keyboard, mouse
→ Digital watch
→ Credit card skimmer..

Section 3 IEA "Evidence" def^n

- Four sources (of Digital evidence)
  - → Physical source : Phones, computer, laptop
  - → Electronic source : logs, emails
  - → External source : Clouds, Robot IOT device
  - → Social media : Social media application & logs

65B IEA → Copy of digital evidence when presented in court a certificate is needed.

CCTVs shall be best evidence - Supreme court

Onion layered security incidents
These incidents demand the most investigative time and resources to resolve multiple security controls.

Global cost of cyber crime

2019	2021
2T	6T

→ Cyber criminals took the data of Johannesburg city (SA) and Hacked the official website and demanded money (ransom) in Bitcoin.

→ Cyber attack on Macy's dropped down its stock price.

Cyber space

Cyber Space is just not restricted to interned - But it also includes computers, computer n/w, ... the internet, intranet, Software apps, data travelling in any form in digital world.

Surface web

Sites that search engine can index / list

Deep web.

Not discoverable by search engine but legal

Dark web

Illegal website, not discoverable by search engine.

Trading or even surfacing dark web is punishable by Indian laws.

Joseph - Marie Jacquard case - first recorded cyber crime case.

Cyber Space

Cyber space includes any data travelling in digital world. The scope of cyberspace is not restricted to internet but it also include comp, comp n/w, intranet, internet

Terms:-

① EH, ② cyber forensic, ③ cyber crime investigation, ④ cyber security and ⑤ cyber laws.

① EH is the process whereby a person is invited to hack particular s/m (comp, comp n/w etc.) in order to test its security. Here, the intention of EHer is not criminal. EHing is not a process which carried out by law enforcement agencies but infact it is the companies who invite EHer. EHing is sometimes called legal or white hat hacker.

② Forensic includes use of sci and tech. to investigate and prove the fact in court of law. Cyber/comp forensic is a practice to take out evidences from digital device and prosecute criminals in court of law.
This process of CF is a part carried out by law enforcement agencies at the time of confiscation of devices at the crime scene.

(3) CCI is a technical term which is infact a process that is follow by CC investigator in order to track the culprit in such a way that the procedure accepted by them could be used as evidence in court of law.

CCI is a process which is carried out by law enforcement agencies. In CCI, the main aim of investigator is to prove the investigation in court of law.

(4) CS is a method for protection and security of comp, comp resource, comp n/w from theft or damage. CS is a method to ensure safety of computer & comp. resources in a particular company. It is a practice which should be followed by everyone to ensure security of comp., comp n/w or comp. resources.

(5) CL is a law governing cyber space. It govern the legal infrastructure of cyber crimes in India. Indian Information Tech. Act (as ammended in 2008 is base of cyber laws in India.

Problems faced if India was not independent

Challenges to Indian laws (Traditional laws) and cyber crime scenario in India?

OR

Why do we need cyber laws in India?

OR

Challenges to traditional Indian laws with reference to cyber crime.

→ Jurisdiction issue is a big challenge in TL which limit scope of implementation toward CC.

→ TL are not effective for CC cases. such as online banking fraud, virus attack, credit card fraud etc.

→ Importance of digital data is not taken into consideration by TL.

→ Companies and bank's dependencies on digital media is not taken into consideration by TL.

→ Non-recognition of eContract under TL, which infact are fast, replacable and convinient form of buisness transaction

→ Online / digital shopping or trading are not taken into consideration by TL (inedequacy of eCommerce)

→ Electronic mode of communication is not considered in TL.

→ Inedequacy related to issue of source code theft.

→ TL are not succesful to resolve domain name issues.

948 - 649 099 ~~+99~~ = ~~+98~~ 1089
+990

→ Non-recognition of digital signature

→ eGovernance not taken into consideration, which is fast replacing traditional methods.

→ Non-recognition of e-Tender and e-Auction which has replaced the method of Tender and Auction

→ Digital evidence and cyber forensic is not given due credit under traditional laws.

→ TL are not successful in resolving mobile phone crime & ewallet issue

→ Not adequate to resolve issue regarding electronic payment.

→ TL are not adequate to resolve problem regarding Blockchain and Crypto currency.

→ Even in the case penalty & punishment are available in TL, they seem to be inappropriate to look into intensity of cyber crime.

→ Not successful for issues related to AI and IOT.

→ Not successful in implementation of issues related to privacy (online privacy)

→ TL are inadequate against cyber terrorism.

Windows Registry

HKCU (ntuser.dat) \ SOFTWARE \ Microsoft \ Windows \ Current Version \ Explorer.

↑ Path in Registry Editor

VID and PID can identify company & device used.
↑ From Registry.

VID => Vendor ID
PID => Product ID.

USBSTOR → USB device info.
NOTE: Friendly name → name given to pen drive.

System \ MountedDevices store information about mounted devices.

Software:
NirLauncher. Registry Explorer ← Last class.
NirSoft
USB Detective ← Not free but some features available.

Hives (PREFETCH)
- SYSTEM
- SOFTWARE
- NTUSER.DAT
- AMCACHE.hve
- Setupapi.dev.log

Prefetch

Each time that you run an application in your s/m, a prefetch file which contains information about the files loaded by the application is created by windows OS.

The information in prefetch file is used for optimizing the loading time of the application in the next time you run it.

Tool used for analysis is Winprefetchview by NirSoft.

Prefetch will store last & timestamp of running program.

C:\Windows\prefetch → .pf files are stored here.

- CC and types of CC in modern era
- Where can we find Elec. cevid.
- Onion layered scc. incident
- Cyber space & unseen web.
- Diff b/w EH and all that
- TL VS CL.
- Need Cyber law in India

CC and legal landscape around the world

✓check ✓works ✓works ✓works
✓works ✓works ✓works

Shellbags

Stores data related to path opened on compiler.

Shellbags analysis is done by many automated tool like Shellbags explorer. (Eric Zimmerman)
↳ GUI for browsing Shellbag data

It shows at some time a path existed. (Even for external drive).

Shellbags explorer can load both active and offline registry.

Volume Shadow copy

Released since windows XP.

Windows State backup
windows restore point (Similar to this)

Windows shadow copy is a service that either manually or automatically takes backup of drive

NirSoft → ShadowCopyView

LNK Files (Link files)

Windows shortcut files are of extension ~~.lnk~~
.lnk.

It is basically a meladata file, specific for Microsoft windows platform.
AppData (Hidden files) → Recent Items (have .lnk files)

Details found in LNK file

→ Original path to target file
→ Timestamp of target file and LNK file
→ Size of target file
→ Attributes associated with target file
→ S/m name, Volume name, volume serial number and sometimes MAC address of the S/m on which LNK file is present.

LECMD → Parse LNK file

Jump Lists

Taskbar feature
New in Windows 7

Files open recently in a particular system.
Eg: what tab open in chrome → Right click & see what is open. All of these things are stored in jump lists

open from command prompt → LinkFiles \ AutomaticDestinations

Eric Zimmerman → JumpListExplorer
and NirSoft
CustomDestinations also contain jump lists

Timestamp Analysis.

(Modified before created - How? Is it is tampered ?) [HW]
(How to tamper timestamp ?) [HW]

(International cyber law)

No, not tempered.
① File created
② file modified (T time) [T < T']
③ file copied to another ~~time~~ device (at T' time)
∴ modified before created.

($MFT record

MACB timestamp → Modified accessed chaged
MACb) Birth.

In $MFT, 2 places where time stored.
→ $STANDARD_INFO ($SI) → can be modified by user level software
→ $FILE_NAME ($FN) → only be modified by S/M kernel.

Anti-forensic technique ↳ timestomp.
↳ user level process like timestomp.

Search google Image
MFT Explorer - Eric Zimmerman

SANS cheat sheet
↳ Windows Times Rules $STDINFO

Look prefetch file to see that timestomp is used or not.

MFT2CSV → Tool.

Autopsy Tool

Orphan file :- files which have no source directory.

virustotal → Repo of Malware sample.
↳ Upload to Autopsy and it will compare files to see if its malicious. :-

- Recent activity
- Hash Lookup
- File Type Identification
- Extension Mismatch detector
- Embeded file Extractor
- Picture analyzer - (EXIF Metadata (GPS enabled - location))
- Keyword search (folder > file > content of file)
- Email parser (client are browser independent.
- Encryption detection
- Interesting files identifier (based on ~~set~~ certain given rule)
- Central Repo
- PhotoRec Carver
- Virtual Machine extractor
- Data source Integrity
- Android analyzer (aLEAPP)
- Drone analyzer
- Plaso (create timeline)
- YARA Analyzer
- IOS Analyzer (iLEAPP)
- GPX Parser (GPS data from GPX file)
- Android Analyzer (Third party app - data)

OCR can be enabled (Phone, CC, Email, IP address etc. can give false +ve)

check

.eml → Email file

Cyber laws

Cyber law which govern cyber space

Information Tech act Amended 2008.

enacted 9th June 2000

commenced 17th oct 200.

Major amendmant in 2008.

24 March 2015, SC of India Revoked Section 66(A) (offensive message) coz it invades Right to freedom of speech.

IT Amended section of diff. acts (major Acts)
- Indian Penal code, 1860
- Indian evidence
- Bankers Book
- RBI

OG act contained 94 section, divided 13 chapter and 4 schedules

- Act as legal base for e Governance.

- Given recognition to electronic records and digital signatures

- The laws apply to whole of India

- Person of other nationality can also be indicted under the Act if the crime involve a computer outside ...

Scope of CL

- Crypto
  ↳ Crypto currencies, BC assets, CBDC, DeFi, Smart contract, stable coin & tokens
- ECommerce
  ↳ Under IT Act & Consumer Protection (ECommerce) Rules, 2020
- Cyber crime Prosecution & Defence
- Presenting Digital Evidence in court
  ↳ Bitcoin, email, IOT device
- IP registrations & license drafting services.
  ↳ app, software, source code, website

Chronology of the Indian Cyber Law

2000

- ITA commenced from 17th Oct. 2000
- eCommerce and eRecord with gov.
- Penalizes various cyber crimes
- IPC changed include, forgery of eEvidence, cyber fraud
- I Evidence Act changed
- Banker's BOOK ↳ ↳ "
- Investigation and adjunction of cyber crime is done in accordance with the provisions of the Code of Criminal Procedure
- RBI act also ammended
- Cyber Regulations Apellate Tribunal Rules

2001

- IT (Certifying authority) Regulations

2002

- Digital signature certificate 12th Sep 2002
- Provision of act with regard to protected s/m
- Minor errors were rectified 19th Sep 2002

2003

- 17 March 2003, the IT Act Rule (Qualification & Experience of adjudicating officer)

2004

- Secure procedure
- Secure electronic record.
- Gujarat IT Rules were passed in order to regulate cyber cafes in state of gujarat

2006

- Certifying Authority

2007

- Rajasthan cyber cafe Rules

2009

- 2008 amendment, came into force 27 Oct 200

2010

- Kerala IT (E-delivery of Services)

2011

- Reasonable Security Practices and procedures and sensitive personal data or information)

2013

- Clarification on the IT (Intermediatary Guidelines)

- ICERT and manner of performing Func^n's and duties

2015

- Unique Identification Authority of India (UIDAI)

2016

- ICERT authorization
- E-Signature
- E-Authentication Technique
- Aadhar (26 March 2016)

2017

- Gov. Open data License National Data Sharing

2018

- Info. Security Practices & Procedures for Protected S/ms

↳ Intelligence Bureau
↳ Narcotics control "
↳ CBI
↳ RAW
↳ Commissioner of Police Delhi

2019

↳ FSI (Forensic Lab)