24/05/2021 Data Mining Digital Forensics

PRABHAT
PAGE NO. : 1
DATE 24/05/2024

Forensics: The use of science and technology to investigate and establish facts in court of law.

Elements of good forensic process

1) Cross Validation
2) Proper handling of evidence
   Observer effect
   chain of custody
3) Completeness of investigation
4) Management of Archives
5) Technical competency
6) Clear definition and justification
7) Legal compliance
8) Flexibility

27/05/2021

Stages (process of forensics)

1) Identification
2) Collection and preservation
3) Analysis
4) Production and presentation.

→ Identification

- Scop Determine the scope and identify quantity of data.
- Identify repositories (Different tools for different repositories)

- Strategy for presenation : The presenation must occur quickly
- Establish the chain of custody
  - Who can access the evidence
- Preview the data

→ Collection and Preservation :
- Collect data in forensically correct manner
- Identify the soure media.
- Select acquisition parameters
- Create the image
- Authenticate : You create the hash of the evidence
  - Cryptographic hash function : MD5, SHA

→ Analysis :

It has forensic techniques which needs to be carried out to analyze the presented data

PRABHAT
PAGE NO.: 3
DATE: / /

→ Production and Presentation:
You should be able to make it simple to understand.

After Investigation.
—x— Archieve the Data in the end —x—

After Investigation:

→ How much data should be archieved? (which images, which dataset would you require)

→ How long the data should be archieved?

→ How likely the case would be escalated? (For example: the appeal)

—x— —x— —x—

→ Computer forensic lab
- Equipments.
- Suspect media.

- Security of lab:
  - People having access to lab

- Airgap (physical isolation) } Preventing spoilage through air network.
  Firewall }

29/05/2021 ~~Design and Analysis~~ of Algo

Digital Forensics :

→ Spoilage of evidence through physical access :

- Social Engineering

→ Proper environmental Safeguards

→ i) Network Access
Encase Tool

keep these separate and away :-

- Laptops for Internet access
- Administrative purposes
- Processing evidence, testing, training.

ii) Physical Access
- Structural Design
- Locks, doors and windows
(pincodes mechanism) (hinges for the door)
(Evidence lockers)
- Policies and Procedures.
(Access Control List)
- Who are allowed
- Who is allowed to escorting them
- Reason and Time and Day of visit

→ Environmental damage:

- Fire:
  (Automatic sprinklers)
  (Splash proof vents)
  (fireproof enclosure)

- Flooding
- Temperature control
- Power protection

→ Types of Cyber Crimes:

Conventional crime:
Act prohibited with penal consequences.

Cyber Crime: Any criminal activity that use a computer either as a tool or a target. or both

Tools
- Financial crimes
- illegal sale
- gambling
- IPR violation (Intellectual property rights)
- Forgery
- email spoofing
- stalking
- defamation.

TARGET
- Theft of info
- Masquerading
- Salami Attack.
- Trojans
- logic bomb
- Ransomware.

31/05/2021

PRABHAT
PAGE NO. 6
DATE 31/05/21

→ What are the reasons for cybercrime ? (Vulnerability)
- Capacity to store data in a comparatively small space.
- Ease of access
- Complexity of System Softwar (os)
- Negligence
- Loss of evidence of crime

→ Motive behind a cybercrime
- Money
- Blackmailing
- Political agenda
- Defamation
- Testing technical stress

→ Types of CyberCrimes

1) Hacking (unethical) cracking:
IT ACT 2000 sec 66 define hacking as whoever with the intent to cause or knowing that he is likely to cause [wrongful loss] or [damage] to the public or any person who [destroys] or [deletes] or [alters] any information residing in a computer resource or [diminishes] its value or utility or [affects] it injuriously by any means commits [hacking]

3 years imprisonment upto 2lakhs of fine or both

PAGE NO. : 7
DATE : / /

2) Security related crime :
- stored data
- intransit data

3) Network packet sniffers
~~- promiscuo mode : Network~~

IP spoofing / masquerade

3) Password Attacks.
Brute force / dictionary
Trojan
Phishing

4) Frauds on Internet
- online investment
- Forums / bulletin boards.
- Email Scams
- Credit card Frauds
- Multilevel Marketing and pyramid schemes.
- ~~Falsi~~ Publishing of false digital signatures

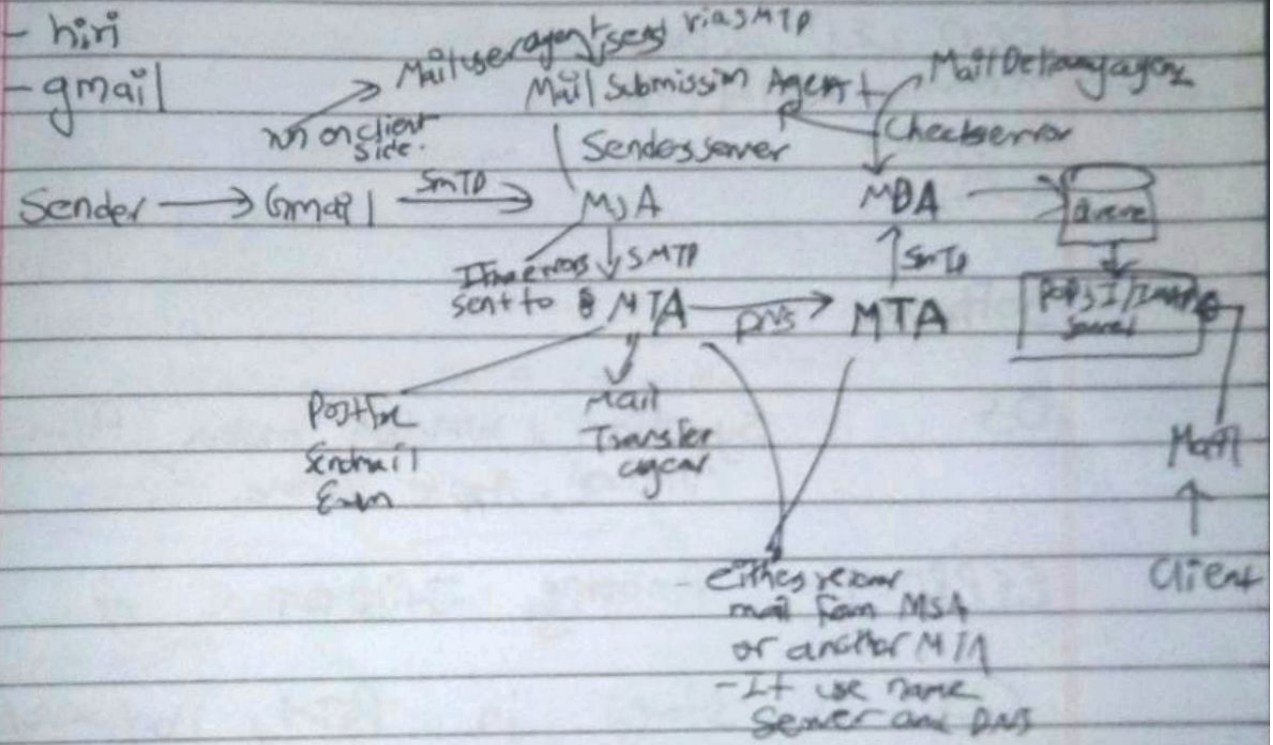
Section 73 of IT Act 2000
Jail upto 2 years & or both
1 lakh rupees

Email Forensics

- Client - Server architecture

Email servers
- Microsoft exchange server
- Postfix
- Sendmail
- Exim

Mail clients
- Outlook
- Mozilla Thunderbird
- Yimi
- gmail



→ Investigating crimes
1) Spam, Unsolicited emails

PAGE NO.
DATE: / /

Mobile forensics.

- Hardware
  RAM
  DSP (digital signal processing)
  Radio
  Microphone
  Speaker
  Keypads
  GPS and other sensors
  LCD, LED display
  removable memory cards
  Bluetooth
  WiFi

- Software

  OS — Symbian, Windows mobile, Palm OS, Android, Apple Iphone

  EEPROM — Rooting, JailBreak

  OS is stored in ROM, Non-volatile.

  SIM (Subscriber Identity Module)

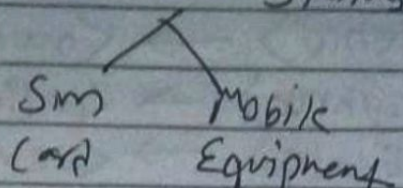
  ↳ SIM consist of microprocessor

  4MB EEPROM
  high capacity high density SIM cards

PAGE NO.
DATE: / /

1GB EEPROM

Mobile phones as mobile Stations.



Sim card function.

1) Identify to subscriber
2) Stores personal info
3) Address books and mages
4) Series related information.

Inside PDA, pages.

SD card
MMC
Synchronize with a computer
hard wired
wireless

Info that you can gather.

- Call history
- Contacts.
- Sms text, MMs, whatsapp, Telegram.
- Calling data.
- Browser data