Digital forensic

The basic of digital forensics 2nd edition
the primer for getting start

- Digital forensic by Nilakshi Jain, DR Kalabangde

Ministry of Electronics and Information Technology (MeitY)
Govt of India Information:
coursera
computer Networks
Cyber Security | Cryptography

1. What is forensic science
Forensic Sc is an application of science to solve legal & crime related problem In
- In FS the law and science are integrated together

2. Digital Forensic Computer
The application of science and investigate procedure for an legal purpose involving the analysis of digital evidence. After proper search authority, chain of custody, validation with main use of validated tools, Repetability, reporting and possible expert presentation.

3. Digital Forensic process -> can be boiled down or segregated into series of stages. These phases are as follows
   - (a) Search authority
   - * (b) Chain of custody
   - * (c) Imaging and Hashing function
   - (d) Validated tools
   - (e) Repeatability
   - (f) Analyses

Analysis linking some activity with specific user account

Established in a timeline an event

(g) Reporting
(h) Possible expert presentation

- which are the devices & elements applied to the digital Forensic
  - (a) laptop
  - (b) desktop
  - (c) Hard disk
  - (d) pen drive (s)
  - (e) mobile devices
  - (f) Network
  - (g) Cloud
  - (h) image
  - (i) audio
  - (j) video
  - (k) text messages
  - (l) Word, excel, powerpoint documents.

- Usage of digital forensic

(a) Civil Investigation; Case Study [BTK Killer Dennis Radder]
(b) Civil litigation & discovery
e dis - electronic discovery. It refers to any process in which data is located, secured and searched with intent of using it as an evidence in a civil or criminal legal case.

(c) intelligence: Case Study [Maussauri K 7-11]
pilottz@123 hotmail com
matter(s)
(d) administrative ~~matter~~ : Case Study [SEC]

Security & Exchange commisson of America

A hash table of length 10

How we are filling this table

0	
1	
2	42
3	23
4	34
5	52
6	46
7	33
8	
9	

function $h(K) = K$

④ ~~Insert 42~~

(A) insert (46, 'A')

$h(K) = K \bmod 10$

$46 \bmod 10$ → 6

(B) insert (34, 'B')

$h(K) = K \bmod 10$

$34 \bmod 10$ → 4

(C) insert (46, 'C')

$h(K) = K \bmod 10$

$46 \bmod 10$ → 6

(D) insert (42, 'D')

DATE 25/07/2023
PAGE

1) Search Authority :-

(i) To initiate a digital forensic investigation we need a proper search authority releated document.

(ii) Search Autority releated document is required for collection the digital evidence.

(iii) Without a search Authority releated document. We are not allowed to investigate. If we investigate without a proper SA document then all the evidence which are collected are suppressed. and not being consider as a valid document.

(iv) For criminal investigation search Authority releated document is 'Woorant' or 'Sellpoena' etc - Issued by the court.

(v) For any civil investigation Search A releated documents are Issued by the public prosecution and from the side of to be accussed

2) Chain of Custody :-

(i) C of Custody is issued for every digital eveidence in order to maintain integrity.

(ii) C of custody is documented via from reports, notes and marking the actual evidence item

(iii) Each time during analysis if an item change it should be recorded.

3) Imaging & Hashing.

(i) After collecting a digital evidence experts avoided to work on the original evidence rather they prefer to make a clone of that evidence in order to prepare the clone of the original evidence an exact copy of every bit of that media is done. this copy is known as bit string copy and the whole procedure is known as imaging.

- Hashing technique - is mathematical process via an algorithm that produces a unique value that is essentially the digital fingerprint or DNA of a particular file piece of media etc.

(A) Validated Tools :-

(i) Forensic tools needs to be validated & tested before they are use so that we can ensure that this tools will give us correct result or accurate result.

(ii) Newly collected tools and updated tools both needs to be verified / validated.

(B) Repeatability :- / Quality assurance

(i) The result of forensic examitation should be able to be deplicated. So that the separate examiner should be able to repeate the process using same evidence same steps & same tools and come up with same result.

(c) Quality assurance is a procedure and practice in the digital forensic process which will help us

to give a guaranty of the accuracy based on my findings.

(iii) Q A address multiple issues such as skill and training of the examiner security of the evidence facility, reliability of the tools, case processing infrastructure and many more..

(6) Analysis :-

(i) Linking some activity with the specific user A/c
(ii) Establishing a time line of the events
(iii) Determining whether USB storage device is connected to your storage machine (Laptop/pc)
(iv) Breaking encryption.
(v) Identifying relationship or connection between individuals
(vi) Identifying that website that may have been visited
(vii) Determining whether certain files are open or downloaded. (ix) We recove the data

(7) Reporting :-

(i) In almost every center where digital F is used some type of reports needs to be generated.
(ii) Report may be of different forms or format
(iii) The name, length from (format & the report needs to be description specified by the reporting authority.
(iv) Many forensic tools are used to generate the report as we process a case. We are able to select specific artifact files to be included in the

report

(v) One major issue with report generation is they are often very technical. As report need to be presented before judge & jurors who may not be a technical person to understand the report, hence convincing a non technical person about a technical report is a challanging task.

(vi) A report should be precise, user friendly and should not be stand alone. It should include abstract, list of evidence, items examine, the methods, the tools (H/S) to perform the analysis, findings and conclusion.

(8) Possible expert presentation
The pinacle of the forensic process is the presentation of the findings to a judge or a jury.

~~Local~~ Locard's exchange principle.

Scientific Methods

(a) Scientific working on digital evidence.
(b) American academy of forensic Sciences.
(c) American society of prime Laboratory directors/Laboratory accreditation board
(d) National institute of standard and technology.
(e) American society for testing & material.
(f) Indian School of ethical hacking (ISOEH) - Mr. S. Sengupta

Components of a digital computer

- user
  - Naive
  - Normal user
  - application programmer
  - network & system Admin
  - database Manager (DBA)
- ~~system~~ software
  - System Software (OS, device driver etc)
  - Application software (Turbo C, Oracle 9i)
- Application Hardware
  - CPU
    - Register Array
    - ALU
      - AU
      - LU
      - shifter Unit
    - CU
      - Hardwired CU
      - Microprogramming
  - Memory
    - Register Array
      - Accumulator
      - General purpose
      - Special purpose register
    - Cache
      - L1
      - L2
      - L3
      - Many more
    - (Memory buffer, Memory Address)
    - RAM
      - Read-write Memory
      - DDR cache RAM, Static RAM, Dynamic RAM
    - ROM
      - ~~Electrically~~ programmable
        - EPROM
        - EEPROM
    - Secondary Memory
      - Magnetic
        - disk
        - tape
      - optically
        - CD
        - DVD

Analyze

1) Int
2) A
3) M
4)
5)
6)
of evid
7)

Introd

- Digita
  crimin
  proce
  dui proce
- Digita
  crime
  from
- Every
  prob
  comp
  by d
  nece
  mate
- Digit
  the
  devi
  com

Module - 3.

Analyze the evidence which are copied

1) Introduction to Cyber Crime Scene
2) Documenting scene and evident.
3) Maintaining the chain of custody
4) Forensic cloning of evidence.
5) Live and data system forensic.
6) Hashing concept to main the intrigity of evidence
7) Reprographing

Introduction to cyber crime

- Digital evidence has been identify to catch criminals to perform civil ~~administrative~~ processing & ~~to perform~~ administrative proceeding.
- Digital Forensic experts needs to visit the crime scene. After visit receving a warrant from court or higher administration
- Every crime scene and its evidence must be protected from accidental or internation compromise. Every crime scene must be protected by digital Forensic expert and police from nosey neighbour news media and other illegitamate trespasser
- Digital Forensic exper. must need to disconnect the cellphone, computer, laptop and digital devices from outside World so that host cannot connect with outside.

- The full crime area must be seized with protected boundaries by police or digital Forensic expert

- Computers and other wireless mobile must be made in accessible as soon as it is ensured that no volatile data would be lost

- Collecting digital Forensic evidence

1) CPU, CPU register, Cache Memory
2) Random Access Memory (RAM)
3) Magnetic Drives
4) Removable Flash Drives
5) Optical disc (DVD/CD) (R/W)
6) " " (DVD-R, DVD-W, CD-R, CD-W)

(1) Cell phone → Turn off the cellphone.
(2) If the phone is password protected.
(3) Try to open the cell phone in a digital protected environment and decrypt the password using a code in digital environment.

(3) Isolate the cell phone in a Faraday bag.
(4) Transport the evidence to the lab to be examined in a shield room.
(5) Capture the power cord or power bank of the cellphone as well.
(6) Place the phone in a special container which shield the phone from wireless signal.

- It is the net mess a

Order In o crim an o come after valat

It is essential to isolate like cellphones from the network. If not it can receive calls, text message or even command to delete the data

Order of valatility

In order to prioratize the evidnces from crime scence digital forensic expert follows an order. In this order most valatile evidences come first and less valatiles evidnces comes after that. This is order known as order of valatility

Digital Forensic

*) Computing environments: Collect

1) Stand-alone C.E.
A stand alone computer is one that is not connected to another computer. Stand-alone computers are easy to investigate.

2) Network computing env.
Computers might be connected via LAN, MAN or WAN. This type of environments introduce variety of variables into eqns. Hence, ~~this~~ the computers in this env. are difficult to investigate.

3) Mainframe C.E.
In this env, a centralized org. is observed from one location. Processor, storage and application can be controlled from a single location. But due to complexity of the system, it's very difficult to trace evidence in this env.

*) Cloud environment
Cloud offers software along with computing infrastructure and platforms on elastic pay-per-use model. [Gmail is cloud facility]

1) IAAS: Infrastructure As A Service.
With IAAS, organizations outsource their hardwares ~~that~~ needs to a service provide. Various hardwares can be used as an infrast. like mem. storage, processor, server, etc.

b) PaaS
PaaS
the abi
basis

c) SaaS
SaaS
custon
are h
provid

There
expe
a) Ac

a) Ac
or

b) A
part

c) An
you
Ent

1) Fi

3) H

b) PaaS: Platform as a Service:

PaaS keeps the developers (app. programmers) the ability to rent the env. on an as needed basis. Eg. Gmail, GCollab, overleaf, etc.

c) SaaS: Software as a Service:

Saas provides applications on demand to customers over the internet. These applications are hosted and maintained by the service providers. ~~As a digital forensic~~

: Data types :

There are 3 types of data a digital forensic expert must need to deal.

a) Active data b) latent data c) Archival data.

a) Active data are data that we use everyday on our devices/computers.

b) A latent data: data has been deleted or partially overwritten. Eg [ERT commander - recover data]

c) Archival data: On backups may take many forms.

External ~~hard~~ drives

: File System :

1) File Allocation table ~~system~~ (FAT) 2) NTFS (New technology File System)

3) HFST (Hierarchial File System) used by MacOs

Ghost Protected Area:

It refers to hidden areas on hard drive that are often difficult to detect. These areas are created by the manufactures. It can be accessed, modified and written by the end users, using specific open source and freely available tools.

Device configuration Overlays: are created by the manufacturers. They are protected area in hard disk or storage.

How magnetic hard drives store data?

[* data is stored in binary digits
*collection of sectors - cluster.]