UT Ethical hacking
chpr3

① Digital evidence

- Refers to any information that is stored or transmitted in a digital format & is relevant to a criminal investigation

- This can incude documents, emails, images, video etc

rules of digital evidence are

① Admissible

- Digital evidence must be relevant to the case & meet legal requirement to be admissible in court

② Authenticity

- It must be established that the digital evidence has not been tampered in any way.

③ Integrity

- Integrity should be maintained throughout the process.

④ Privacy

- Digital evidence may contain sensitive info, so it must be handled in a manner that protects the privacy rights.

③ Computer forensics

- It is a scientific method of investigation & analysis in order to gather evidence from digital devices which is suitable for presentation in a court of law

- It involves performing a structured investigatn while maintaining a documented chain of evidence to find out exactly what happened on a computer & who was responsible.

uses

- Recovering deleted files
- Recovering deleted emails
- analyzing internet browsing history
- identifying & analyzing malware.

challenges

- Rapid evolving technology, can make it difficult to keep up with new devices & storage formats
- The volume & complexity of digital data
- encryption can prevent access to digital evidence.

② evidence collection

- It involves the gathering & preservation of physical & digital evidence relevant to a legal investigation.

Type of evidence

- physical evidence (Real evidence)
- involves tangible evidence such as documents , flash drive etc

- Digital evidence
- such as emails , files etc

- Testimonial evidence
- statement made by witness or supects

- Hearsay
- evidence presented by a person who was not a direct witness.

④ Tools used in computer forensics .

* • hardware (advanced)

- Tools ranges from simple to comprehensive systems & servers.

- Basic & single purpose hardware tool
  - ACARD
  - AEC - 7720WP
  - ultra wide SCSi - to - IDE Bridge

- advanced
  - FRED system
  - DIBS system

* • Software
  - SafeBack
  - X-way forensincs
  - Encase
  - Access Data FTK

DE - digital Evidence

Page No.:

Date:

(5) evidence acquisition

- Evidence acquisition involves the process of collecting & preserving digital evidence for forensic analysis.

- Remote acquisition offers with Runtime software offers "HDHOST" programs.

- To use use these, it's best to have computer connected on the same local hub with minimal network traffic

steps in computer evidence processing includes

(1) identification

- identify potential sources of DE (computer)

(2) collectn

- collectiong the evidence using appropriate Tools

(3) preservation

- maintaing integrity

(4) analysis (determine the result's accuracy)

(5) presentation (summarize & present findings)

(6) documentatn (Document findings to use in court)

chP2

⑥ objective of Digital forensics

- Evidence to court (Presentation)
- Identifying the culprit
- Legal procedures
- Data redundary (recover the deleted files)
- analysis (draw conclusion)

Types of digital forensics

- Disk forensics

- deals with extracting raw data from the primary & or secondary storage of the device by searching active, modified or deleted files.

- Network forensics

- Involves monitoring & analyzing the computer network traffic.

- Database forensics

- deals with study & examinatn of databases.

- Malware forensicy

- identification of suspicious code, viruses, worm etc

- Email forensics

- Mobile phone f.

Chp2

Chain of custody

- The chain of custody is a process that documents the chronological history of evidence from the moment it is collected to it's presentation in court

- The purpose of COC is to establish the integrity & authenticity of the evidence & to prevent tampering.

Process of COC involves

① Documenting the collection of evidence (dat including time, data, location & individuals involved.

② packaging & labeling the evidence to prevent tampering or damage.

③ Maintaining a detailed record of who has had custody of the evidence & any action taken with it

④ Transporting the evidence securely

⑤ presenting the evidence in court along with documentation of the COC.

Anti - forensic - it is a term that contradicts cyber forensic

It aims to diminish the amount & reliability of evidence available at crime scene.

Anti - forensic techniques are strategies intended to complicate the investigation process

Their purpose is ~~the~~ to diminish both the quality & quantity of digital evidence

Here file hiding, stegnography etc technique are used to conceal digital evidence.

(8) • Incident response refers to the structured approach an organization takes to address & manage the aftermath of a cybersecurity incident.

• These incident can range from data breaches & malware infection to DOS & insider threats

• The primary goal is to minimize damage, reduce recovery time & cost & mitigate future risk

Roles of CSIRT - Computer Security incident response time

① Detection & monitoring (detecting incident

② Analysis (analyze nature & scope of incide

③ Eradicatn (removing malware)

④ forensic investigatn (to determine the root cause of incident)

⑤ documenting & reporting