iNURTURE
Education Solutions
TOMORROW'S HERE

*Chapter 1.1*

# Introduction to Computer Forensics

# Aim

To equip students the importance of cyber-crime, the various tools and techniques of  computer forensics

# Instructional Objectives

After completing this chapter, you should be able to:

- Explain Computer forensics in detail
- Describe computer forensics evidence
- Explain different forms of cyber crime
- Describe the rules to be followed before and after crime scenes
- Explain the use of different computer forensic tool
- Outline important skills needed by a forensic investigator

# Computer Forensics

# Computer Forensics

Computer forensics is a process to identify, collect, analyse, and report various forms of digital evidences in such a way that they are legally admissible in a court of law.

# Computer Forensics

## Myths About Computer Forensics

| Myth#1 | Myth#2 | Myth#3 |
| --- | --- | --- |
| • When a forensics practitioner conducts an investigation on a live system, it will inevitably alter that system in some manner, and thus, live forensics cannot be conducted as a valid forensic process. | • Actions taken by a digital forensics practitioner must not change the data held on a device's storage component, if such data is to be relied upon in a court of law. | • Actions taken by a Digital Forensics Practitioner must produce an evidence image that can be repeatedly collected whilst producing an identical hash value. Thus “live forensics” and “mobile phone forensics” cannot be considered “forensics.” |

# Computer Forensics

## Rules for Evidence Integrity

- Bit-by-bit copy
- Evidence is locked in safe and limited access cabinets called safes, or vaults
- The use of cryptographic hashes like md5, sha1, sha2, etc., to ensure the integrity of the original evidence media.
- The use of write blocker to protect the evidence from modification
- To create and maintain chain of custody documents

# Quiz / Assessment

1) Data recovery, data acquisition, and analysis and reporting are a part of computer forensics investigation. State true or false.

   a) True

   b) False

# Quiz / Assessment

2) Evidence is no longer acceptable in a court of law when a computer forensics practitioner conducts an investigation on a live system as it will alter that system. State true or false.

   a) True

   b) False

# Quiz / Assessment

3) Which of the following is used to validate the authenticity of evidence?

a) md5

b) sha7

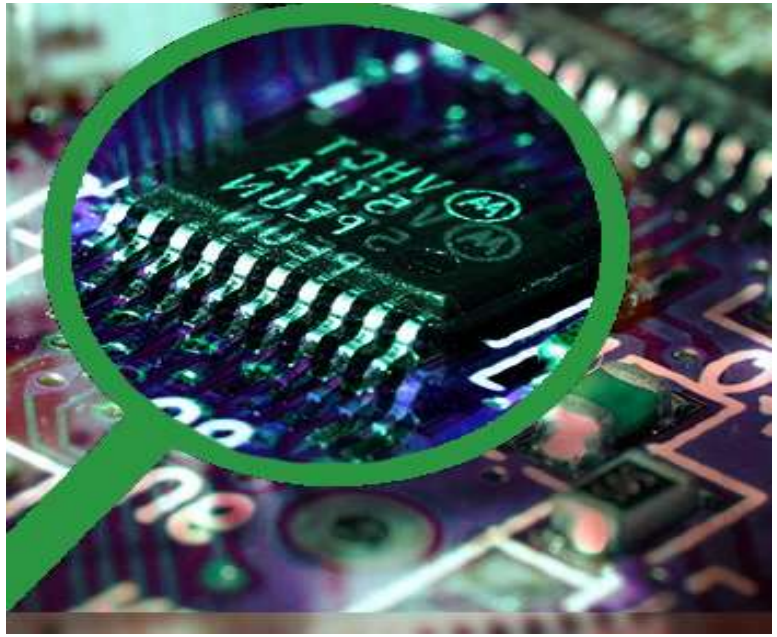
c) shap

d) sha3

# Computer Forensics Evidence

# Computer Forensics Evidence

Computers store a large amount of data and this information can be used as evidence.



*Computer Forensic Evidence stored in computers*

*"Any information with a probative value is evidence"* – CA: US born, 2003

Evidence must be relevant to a case in question and sufficient enough to prove a point.

Computers can store large data such as email addresses, contact details, pictures, financial details, videos, and Internet history and phone numbers.

All of this can give information about people's habits and interests, otherwise known as evidence.

# Computer Forensics Evidence

A computer forensics investigator needs to collect, preserve and analyze the information available in the computer.

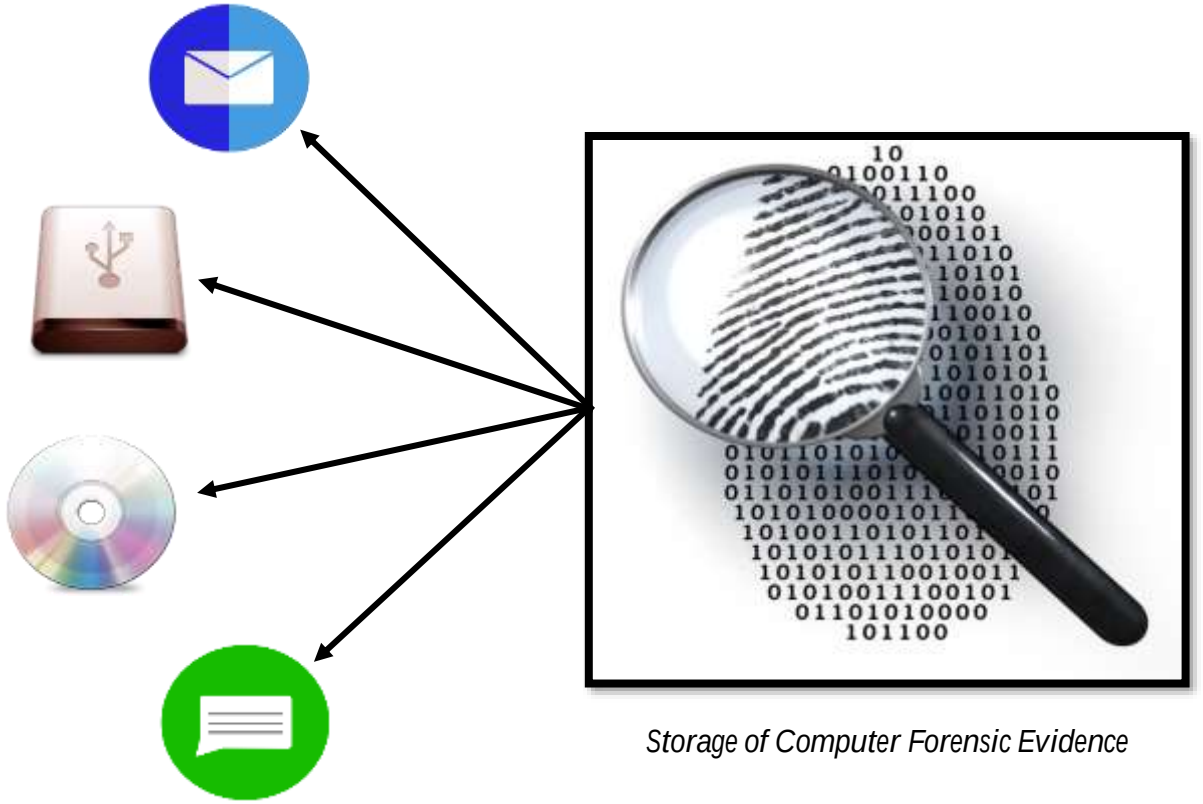
*Computer Forensic investigation*

# Computer Forensics Evidence

## Where can we find evidence?

Evidence may be stored in:

- CDs/DVDs
- USB devices
- Text messages
- E-mails
- Various application records and so on.



*Storage of Computer Forensic Evidence*

# Quiz / Assessment

1) Which of the following can be used to store evidence?

a) Hand-written notes
b) Memory cards
c) Hand-painted images
d) Empty boxes

# Quiz / Assessment

2) Mobile phones hold a lot of information that can be used as evidence in Computer forensics. State true or false.

a) True
b) False

# Quiz / Assessment

3) Evidence may be stored in _____.

a) Hard disc media

b) Disc media

c) Drive disc

d) CD drive

# Different Forms of Cyber Crime

# Different Forms of Cyber Crime

Cyber-crime happens in various forms. Some of them are listed below:

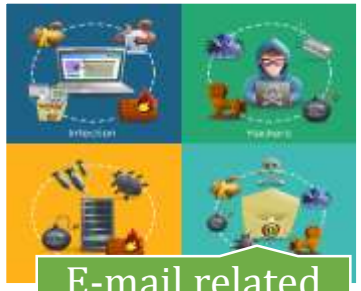
Intellectual Property theft


Industrial espionage

Employment disputes

Fraud and Forgeries

Bankruptcy



E-mail related crimes

Regulatory Compliance

Cyber Stalking

# Different Forms of Cyber Crime

Hacking has become an incredibly organised business, and has a lot of financial gain attached to it.

There are different types of hackers commonly referred to by geeks as black hat, white hat and gray hat hackers.

Types of Hacks

- Denial of Service Attack(DOS) or Distributed Denial of Service Attack(DOS)
- Sniffing
- Spoofing
- Malware/Back Door/Trojans/RAT
- Key Loggers
- Phishing & Social Engineering
- Website Hacking
- DNS Poisoning
- Phone Phreaking

# Different Forms of Cyber Crime

## Money Laundering

Money laundering is the process of making large amounts of money. It is usually acquired through committing serious crimes appears as though they have been legitimately acquired through valid sources.


*Money Laundering Scheme*

# Quiz / Assessment

1) What is the act of falsifying, or altering a document in order to benefit called?

a) Cheating
b) Phishing
c) Forgery
d) Hacking

# Quiz / Assessment

2) Which of the following is a form of hacking?

a) Hate-mail
b) Information
c) Malware
d) Stories

# Quiz / Assessment

3) The breaking down of larger amounts of money and depositing it into offshore accounts in countries where laundering laws and less stringent is called _____.

a) Burping
b) Smurfing
c) Merging
d) Curbing

# Computer Forensic Tools

# Computer Forensic Tools

Examiners use multiple tools during the acquisition/recovery of the evidence, validating, extracting, analysing and reporting the findings.

Computer forensics tools can be categorised under:

- Acquisition/recovery
- Validation and Discrimination
- Extraction and Analysis
- Reporting

# Computer Forensic Tools

Categories of Computer forensics tools:

## Acquisition

- Computer evidence is stored in various technological devices, and in various forms.
- To successfully analyse a case, one must be able to identify the relevant evidence, and able to acquire forensically sound evidence sets.

## Validation and Discrimination

- While creating a copy of the evidence, we create hashes of the evidence to verify the integrity of the evidence.

# Computer Forensic Tools (contd.)

Categories of Computer forensics tools:

## Extraction and Analysis

- After the evidence sets have been acquired, data extraction and analysis need to be performed for further identification and extraction of the evidence.
- In this category, two types of tools are employed: the first is the data recovery and key work searching tools, and the second is the analysis tools.

## Reporting

- Post analysis, the report has to be created, for client presentation, with proper evidence, in a chronological manner, to identify the sequence of events that leads to the incidents.
- Most of the commercial tools have an in-built reporting feature that allows us to select the components of the report while performing the analysis itself.

# Quiz / Assessment

1) Which of the following is a  tool used for forensics acquisition?

a) FTK
b) Encore
c) Mono Sodium
d) Access Denied

# Quiz / Assessment

2) Which of the following also does Data recovery?

a) Sleuthkit
b) FTT
c) MoonSol
d) Volity

# Quiz / Assessment

3) Sleuth Kit is an open source forensics tool. State true or false.

a) True
b) False

# Important Skills Needed by a Forensic Investigator

# Important Skills Needed by a Forensic Investigator

An investigator should have thorough knowledge about computers, along with:

- An excellent working knowledge of all the features of a computer, including hard drives, networking, and encryption.

Working knowledge

- Skills to recover and examine the data from the electronic storage devices to use it as evidence in criminal prosecutions.

Data recovery

- Skills to write technical reports, document the details of how computer evidence was discovered, and steps taken to retrieve data.

Technical reports

- Up to date knowledge about the latest methodologies and forensic technology.

New methodologies

# Quiz / Assessment

1) What An investigator should recover and examine during an investigation?

a) date from the electronic storage devices
b) data from the electronic storage devices
c) data from the ware house storage devices
d) devices from the electronic goods

# Quiz / Assessment

2) Reporting skills, communication skills, analysis skills, and data acquisition skills are all necessary to be a good forensics investigator. State true or false.

a) True
b) False

# Quiz / Assessment

3) Knowledge of cyber law is a must in order to be a forensics investigator. State true or false.

a) True
b) False

# Activity

## Offline Activity

**Offline Activity**
**(20 min)**

- List the qualities of a crime scene investigator, and explain the job description, duties and required skills.

# Summary

- ✓ Computer forensics is the process of gathering, analysing and reporting digital data in a way that is legally permissible.
- ✓ It can be used in the detection and prevention of crime, and in any dispute where evidence, or data, is stored digitally.
- ✓ Computer Forensics helps investigate cases that involve various forms of electronic storage media devices such as hard disks, USBs, SSDs (Solid State Devices), memory chips/cards, and the cloud.
- ✓ It requires a basic understanding of various operating systems, network devices, storage media and applications, etc.
- ✓ The aim of computer forensics is to perform an organised investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device, and who was responsible for it.

# Summary

- ✓ Over a period of time, the industry has developed various tools and techniques, and rules and standards, to be utilised during and after the investigation process.
- ✓ Cyber-crime laws have also been put into place to prosecute criminals.
- ✓ To become a good forensics investigator, one must have good knowledge of working with various operating systems, databases, networking fundamentals, investigative skills, report writing, interpersonal, and interview skills.
- ✓ You can start a career in the Computer Forensics field as a technician to help identify and acquire evidence, and perform basic processing jobs during and after the forensics investigation process.
- ✓ You can also gain experience by working on various cases and, later on, become a forensics investigator.

# e-References


- *What is IT forensics? | IT & Computer forensics beginner's guide | Forensic Control*. (2016). *Forensiccontrol.com*. Retrieved 7 June 2016, from https://forensiccontrol.com/resources/beginners-guide-computer-forensics/

- *Deleted Files - Computer Evidence – Computer Forensic Analyst - Computer Forensic Examination*. (2016). *Computerforensics.com*. Retrieved 7 June 2016, from http://www.computerforensics.com/faq.html

- *Cyber Crime – Types & Preventive Measures*. (2016). *Crossdomainsolutions.com*. Retrieved 7 June 2016, from http://www.crossdomainsolutions.com/cyber-crime/

- *Crime Scene Investigator Skills and Knowledge*. (2016). *Mymajors.com*. Retrieved 7 June 2016, from https://www.mymajors.com/career/crime-scene-investigator/skills/

# External Resources

1. Hayes, D. D. (2015). *A Practical Guide to Computer Forensics Investigations.* US: Pearson Education, Inc.
2. Nelson, B., Phillips, A., & Steuart, C. (2010). *Guide to Computer Forensics and Investigations, Fourth Edition*. Boston, MA: Course Technology Cengage Learning.
3. Philipp, A., Cowen, D., & Davis, C. (2010). *Hacking Exposed Computer Forensics, Second Edition*. New York: McGraw-Hill.