Topic 1 Fundamentals of computer and network forensics

Lecture 1

Learning Outcome

- After successfully completing this lecture, you will be able to
  - Describe cyber-attacks and cybercrime threats to businesses and governments
  - Explain digital forensic processes to acquire, examine and present evidence in computers and networks

Road Map

- Cyberattack
- Cybercrimes
- What digital forensics is
- A digital forensics process

Cyber Attacks

- A cyberattack is any type of offensive maneuver employed by nation-states, individuals, groups, society or organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system

Cybercrimes

- Cybercrime is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.
- Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)"
- When will cyberattack become cybercrime?
- See reference : Computer Misuse Act, Personal Data Protection Act

Computer Misuse Act

Computer Misuse Act

Status: Current version as at 12 Apr 2020

9 Enhanced punishment for offences involvi...

Table of Contents

Part II OFFENCES

- 3 Unauthorised access to computer material
- 4 Access with intent to commit or facilitate commission of offence
- 5 Unauthorised modification of computer material
- 6 Unauthorised use or interception of computer service
- 7 Unauthorised obstruction of use of computer
- 8 Unauthorised disclosure of access code
- 8A Supplying, etc., personal information obtained in contravention of certain provisions
- 8B Obtaining, etc., items for use in certain offences
- 9 Enhanced punishment for offences involving protected computers

Timeline ▾ Subsidiary Legislation ☑ Amendment Annotation Actions ▾

Enhanced punishment for offences involving protected computers

9.—(1) Where access to any protected computer is obtained in the course of the commission of an offence under section 3, 5, 6 or 7, the person convicted of such an offence shall, in lieu of the punishment prescribed in those sections, be liable to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 20 years or to both.

[21/98]

(2) For the purposes of subsection (1), a computer shall be treated as a "protected computer" if the person committing the offence knew, or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for —

(*a*) the security, defence or international relations of Singapore;

(*b*) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

(*c*) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or

(*d*) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services.

Phases of a Cyberattack (Kill Chain)

Click Here to read detail descriptions

Types of Cybercrime are

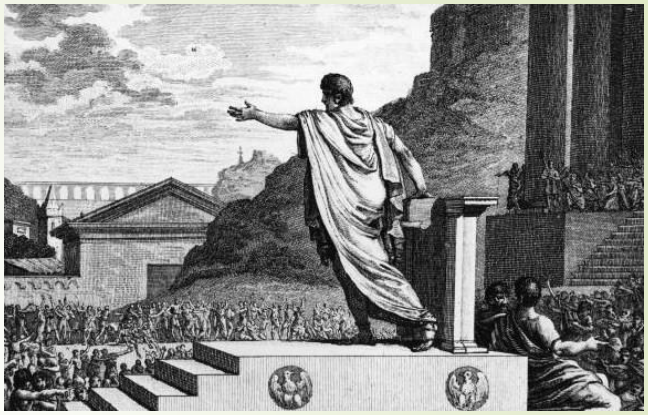
- Internal attacks
  - Espionage
  - Theft of Intellectual Property
  - Unauthorized manipulation of records
  - Trojans horse attack
  - Inappropriate use of IT resources
- External attacks
  - Identity theft
  - Personal data misuse
  - Denial of service attack
  - Cyber defamation (fake news)
  - Ransomwares

Counteracting Cybercrime

- Diffusion of Cybercrime
  - (more people committed cybercrime when cyberattack skills become widely available)
- Investigation (digital forensics)
- Legislations
- Penalties
- Awareness
- Intelligence

- Read more at Wikipedia : Combating Computer Crime

What is "Forensics"?



- The word **forensic** comes from the Latin adjective **forensis**, meaning "of or before the forum."
- In Roman times, a criminal charge meant presenting the case before a group of public individuals in the forum. Both the person accused of the crime and the accuser would give speeches based on their sides of the story. The individual with the best argument and delivery would determine the outcome of the case. This origin is the source of the two modern usages of the word forensic – as a form of legal evidence and as a category of public presentation

What is “Forensics”?

- Now "forensics" = "forensic science" can be considered correct as the term "forensic" is effectively a synonym for "legal" or "related to courts"

What do Digital Forensics Cover?

- Computer forensics
- Network forensics
- Mobile device forensics
- Forensic data analysis
- Database forensics
- Click here to read more details

Digital Forensics Vs Data Recovery

- Data recovery involves recovering information from a computer that was deleted by mistake or loss due to unforeseen circumstances
  - Typically you know what you are looking for
- Digital Forensics recovers data that are deleted or hidden, with the goal to ensure the recovered data is valid and can be used as evidence
  - Investigator often does not know if a computer contains evidence

When computer and network forensics are needed?

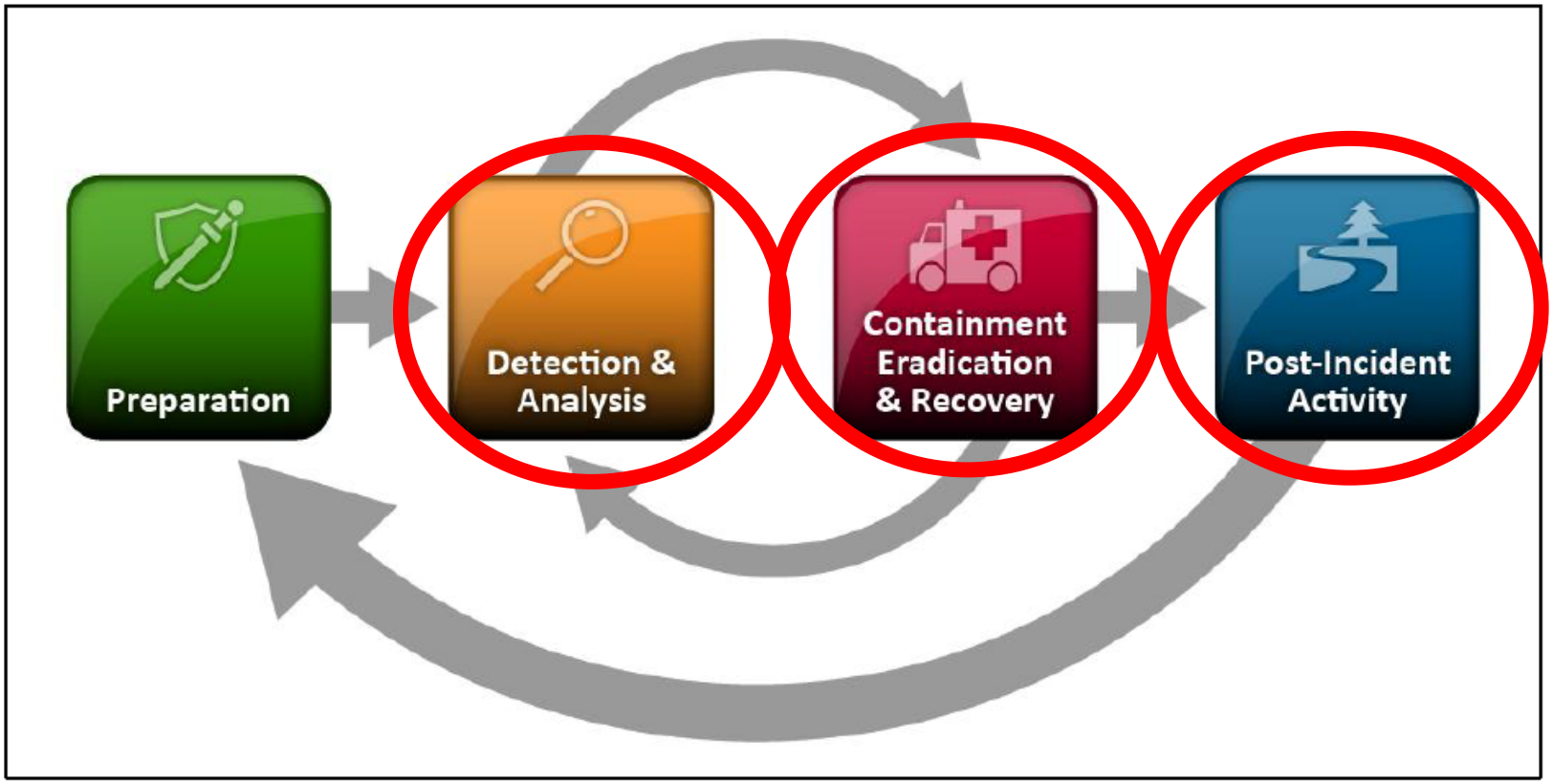


Figure 3-1. Incident Response Life Cycle

From Computer Security Incident Handling Guide SP 800-61 SP 800-86 Revision 2, NIST

What is a digital forensic process?

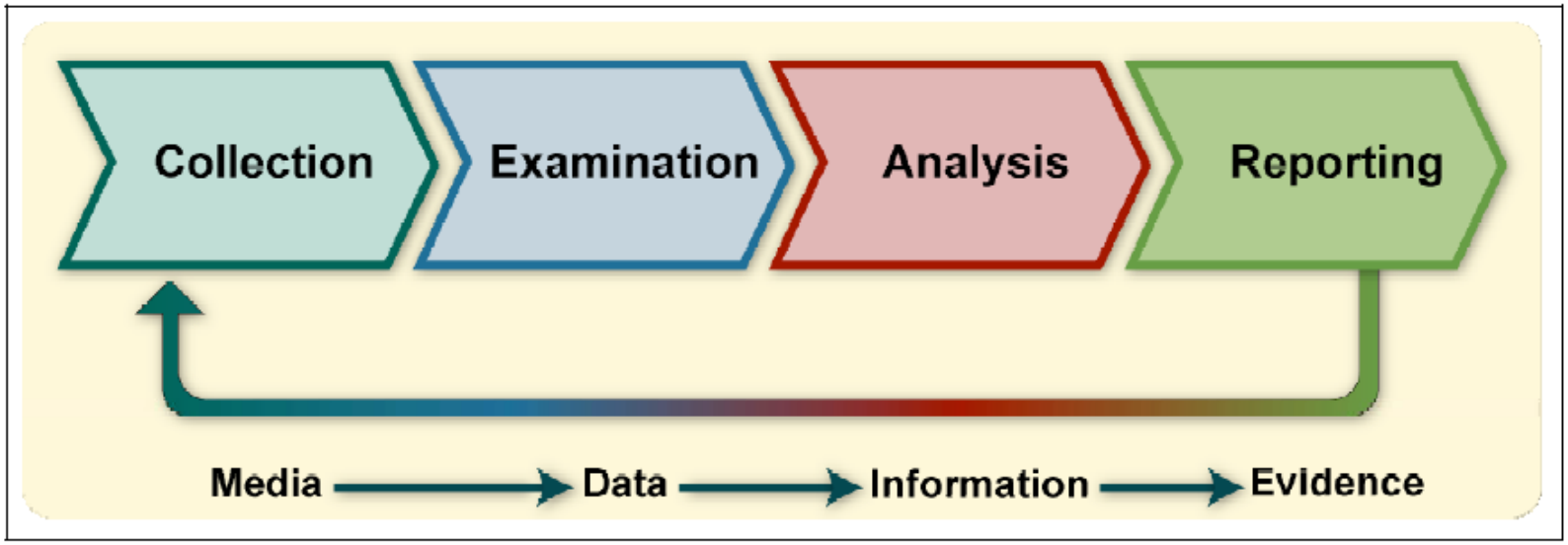


Figure 3-1. Forensic Process

From Guide to Integrating Forensic Techniques into Incident Response SP 800-86, NIST

Further Reading

- Read Section 3 "Performing the Forensic Process" in Guide to Integrating Forensic Techniques into Incident Response SP 800-86, NIST
- Read Kill Chain Wikipedia pages

Video on Cyberattacks/Cybercrimes Threats to Businesses and Governments

- Learning Outcomes
  - To explain Cyberattacks/Cybercrimes threat to businesses
    - Examples : 2013 South Korea MBC Broadcast company attack and Bank ATMs attacks
    - Cyber Pandemic : 2017 June Malware Notpetya attack
  - To explain Cyberattacks/Cybercrimes threat to governments
    - Economic and Psychological attacks
    - 11 Critical Information Infrastructure attacks

Video on Cyberattacks/Cybercrimes Threats to Government and Businesses (Click the image to view the video)

Summary

- Cyber-attacks and cybercrime are threats to businesses and governments
- Computer and network forensics are 2 branches in digital forensics
- A digital forensic process include acquiring, examining, analysing and reporting of evidence in computers and networks