Information Technology Forensic

Week 1

The Aim of Learning

- Students could explain IT Forensics concepts and its boundaries and implementations in Informatics Technology.
- Students could explain the various methods used for IT Forensics on computer hardware, mobile devices, and networking.
- Students could show his ability to use severals tools for IT forensics.

Background

- IT technology is developed in many areas, including in Law and Security.
- Some cases containing digital evidence need to be interpreted by IT Forensics to disclose the cases

Case 1

- There are several cases of customer account balances being mysteriously reduced in a Bank.
- What are the causes:
  - The database of account balances and PIN number are leaked
  - ATM cards are copied illegally
- There are numerous transactions using illegal methods
- How to disclose the case??

Case 2

- Defamation of an official by twitter account from a Social Organizational Chief.
- The officials reported the Social Organizational Chief to police and demanded in law.
- How to prove that the twitter account is really owned by the Social Organizational Chief?
- How to prove that the Social Organizational Chief updated the status by himself nor hacked by intruder?

Case 3

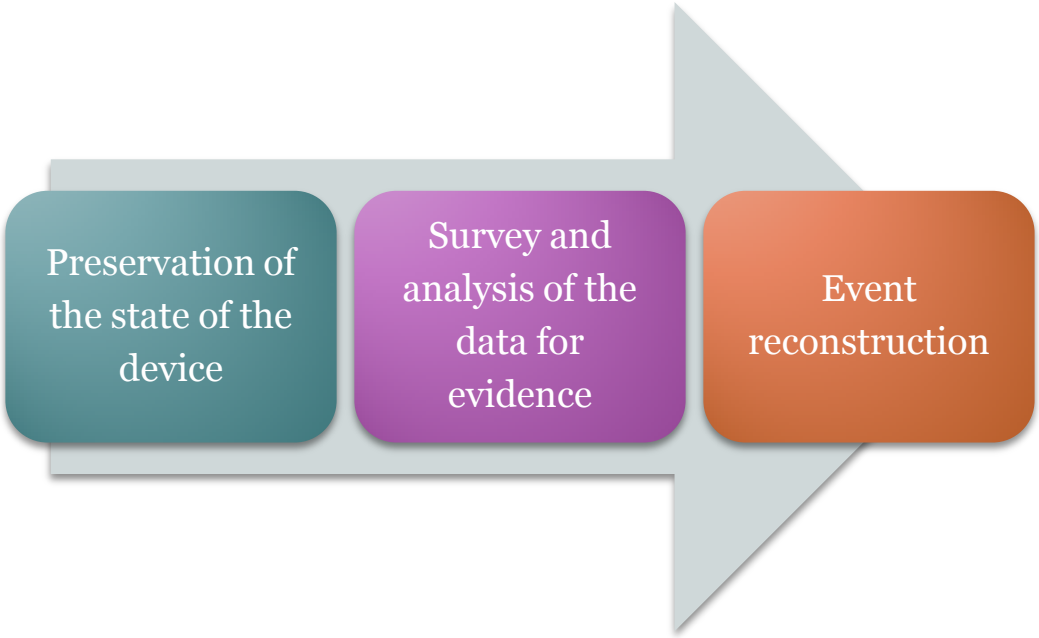
- A free video player software suspected as a malware which steal data from the computer.
- How to disclose the case?

Definition of IT Forensics

"The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations."

Digital Forensics

- General Process in IT Forensics



The Boundaries of IT Forensics

- Networks (Network Forensics)
- Small Scale Digital Devices
- Storage Media (Computer forensics)
- Code Analysis

The Aim of IT Forensics

- Classic Forensics
- Computer forensics uses technology to search for digital evidence of a crime
- Attempts to retrieve information even if it has been altered or erased so it can be used in the pursuit of an attacker or a criminal
- Incident Response
  - Live System Analysis
- Computer Forensics
  - Post-Mortem Analysis
- Mobile Forensics

Paths to Careers in CF

- Paths to Careers in CF
- Certifications
- Associate Degree
- Bachelor Degree
- Post Grad Certificate
- Masters
- Doctorate

Job Functions

- Functions
- CF Technician
- CF Investigator
- CF Analyst/Examiner (lab)
- CF Lab Director
- CF Scientist

Discussion

- Free Talk Discussion.
  - Example:
    - What should be concerned to investigate a case with digital evidence?
    - etc