Seminar session 3: Principles of Digital Forensics and Cyber Law – Evidence collection

Things to do:

- You are required to participate in?
  →Discussion Forum
  →Start writing post
  →Include referencing (UoEO Harvard reference style)
  →Activities of weekly units
  →E-Portfolio activities
  →Weekly Reading

- Assignments
  ➔ Preparation
  ➔ Further Reading(if required)
  ➔ Data Collection
  ➔ Start working

Discussion Includes (Unit 3 E-Portfolio Activity 2)

- What is Digital Forensics?
- How strong is the Digital Forensics?
- Process of Digital Forensics
- Phases of Digital Forensics
  ➔ First response
  ➔ Search & Seizure
  ➔ Evidence Collection
  ➔ Securing Evidence
  ➔ Data Acquisition
  ➔ Data Analysis
  ➔ Evidence Assessment
  ➔ Documentation & Reporting
  ➔ Expert Witness Testimony

What is Digital Forensics:

- Branch of forensics science
- Focuses on digital devices & cybercrime
- Process of identifying, preserving, analyzing and documenting digital evidence

- Collection, assessment and presentation of the evidence obtain from digital media
- Evidence comes from mobile phones, computer and serves
- Helps in solving complicated cases
- Especially cases that depends upon evidence from electronic media

Power of Digital Forensics:

It is powerful because it is used for:

- Recovering data
- Recovering deleted data
- Discover evidence of misconduct
- Prove misuse of a company's property
- Mitigate damage cause by cyber misconduct
- Reverse system breakdown
- Restoring overwritten data

Digital Forensics Process:

- It a very intense process
- Steps includes:
  → Find evidence from the electronic devices
  ➔ Save the data and store it in a safe drive
  ➔ Analyze and document the information
  ➔ Once ready, evidence is handed over to police or
  ➔ Present it in a court to solve crime investigation and convict a criminal

9 Phases of Digital Forensics:

1 – First Response

- As soon as security incident occur or reported
- Digital forensic team start working
- Seize the crime scene/computer/devices
- Start collecting evidence

2 – Search & Seizure

- Start searching devices involve in crime
- Collect evidence and data from these devices
- Seize the device to stop perpetrators to change anything in the data or devices

3 – Evidence Collection

- Collecting of data from the seized devices
- Professionals collect data using forensic methods
- These methods are also used to handle the evidence

4 – Securing the Evidence

- Investigator stores evidence in a safe place/environment/device
- Seized data should be authenticated and proved
- Data should be accurate and accessible

5 – Data Acquisition

- Forensics team retrieves electronic stored information (ESI) from seized device
- Professional must used roper procedure
- Take care of data/evidence to avoid alteration in the data
- Make sure there is no danger to the integrity of the evidence

6 – Data Analysis

- Forensics professionals sort and examine data
- Check for the ESI authenticity
- Identify an cover data into useful information
- This information is used to present in a court

7 – Evidence Assessment

- Once ESI is identified as evidence, investigator start processing
- They assess the evidence in relation to the security incident
- They check the relation to the gathered data, whether it is directly related to the case or not

8 – Documentation & Reporting

- Once initially criminal investigation is performed, team members report and document all the evidence and data according to the court of law.

9 – Expert Witness Testimony

- Expert witness is a professional who work in the area/field related to the case
- Witness confirm that the data collect in this investigation is accurate and useful
- Also confirm that the data is useful as an evidence

- Expert witness present it in the court

➔ Process remains the same in nearly all digital forensic investigation, it does not depend on the case situation.