Unit-5
Forensics and Incident Analysis

- Forensic Technologies
- Digital Evidence Collection
- Evidentiary Reporting
- Incident Preparation
- Incident Detection and Analysis
- Containment, Eradication, and Recovery
- Proactive and Post Incident Cyber Services

Forensics

- Forensics is related to scientific methods of solving crimes, involving examining the objects or substances are involved in the crime.
- Cyber forensics/ Digital Forensics/ Computer Forensics is the process by which experts collect, examine, and analyze all of the data from compromised computer systems and storage devices.
- This is done in a manner consistent with best-practices so that the evidence could be admissible in a court of law if necessary.
- Evidence collection includes identifying and securing infected devices and all data, including latent data, from the systems.

Forensic Technologies

- Digital forensics is a relatively new branch of forensic science.
- This involves the identification, validation, investigation, recovery, and presentation of facts during criminal cases regarding digital evidence found on computers and other digital devices.
- With help from advanced technology, information moves very fast.
- Additionally, the information could be stored or in this case hidden in different apps or software.
- Traditional criminal justice workers may not have the skills or capability to recover this information and use it to prosecute criminals.
- This creates the need for skilled personnel such as digital forensics technologists and forensics technologies.
- Such technologies are explained below.

The Sleuth Kit and Autopsy:

- This is a kit of commands lines for system analysis.
- This valuable forensic software helps us to navigate through the files from the suspect computer without altering anything on the computer.
- In addition, this forensic tool like many others is able to show us a detailed list of deleted files and hidden files.
- However, a disadvantage of this forensic tool is that you must to memorize all commands, and it is tedious but is here in this part when Autopsy can help.

- Autopsy is a forensic tool with a graphical user interface and browser to analysis evidence.
- Autopsy can analysis different types of data format such as FAT, Ext2 / Ext3, NTFS, etc.
- Autopsy is based on HTML, So, this feature permits the connection with the server of Autopsy employing a web browser.
- Also, deleted files and data are shown by an interface of Autopsy called "File Manager".

ProDiscover Basic:

- ProDiscover Basic is a free digital forensic tool that like Autopsy has a graphical user interface.
- This forensic tool is designed to make copies of the hard disk without altering any data on this.
- ProDiscover Basic also permits to create images of USB flash memory, RAM memory images, BIOS image and hard drives images. Once the image is ready, we can analyze in detail the evidence found for this wonderful software. Some features of this digital forensic tool are:
    - View Deleted files
    - Search for contents of a disk
    - Retrieve a file that was accidentally deleted
    - Registry view
    - Event log view
    - Internet history view

EnCase Enterprise:

- EnCase is an instinctive tool that has a useful user interface and amazing performance.
- EnCase forensic digital analysis in deep investigations with accuracy and safety.
- It is a software that ensures the full integrity of the information, even deleted data.
- Some features of this forensic tool are:
    - Support for multiple images systems such as Linux, Windows, MAC OS etc.
    - Full Support for Unicode
    - The ability of multiple systems analysis

- Search tools
- Gets data from disk or RAM, documents, pictures, email, web mail, Internet appliances, cache and web history, reconstruction of HTML websites, chat sessions, archives, backup files, and encrypted files.

DEFT:

- DEFT (Digital Evidence and Forensic Toolkit) is a distribution of Linux based tool with a GUI for forensic applications.
- DEFT is designed to police, researchers, system administrators or forensic specialists.
- DEFT is a useful forensic tool because it is able to provide accurate and reliable analysis to forensic investigators, and this is because DEFT ensures the integrity of data structures and metadata in the system that is being analyzed without altering the data.
- When the system is booting, the partition in the system that must be analyzed is not touched by DFET to make any changes.

Internet Evidence Finder:

- Internet Evidence Finder is a software tool that enables the recovery of data that has been deleted or that are currently stored on the hard drive, as a result of communications right through the internet.
- This means that Internet Evidence Finder can recover all types of social networks data, such as popular web mail applications, browsing the history, chat histories, instant messaging, and other online communications.

Digital Evidence Collection

- Digital evidence can be defined as the information or valuable data stored on a computer or a mobile device that was seized by a law enforcement organization as part of a criminal investigation.
- The information stored or transmitted in binary form on a computer hard drive, a mobile phone, or any other electronic device can be used as digital evidence by the forensic responders in a court of law.
- This evidence can include files on emails or mobile phones of the suspects, which could be critical to track their intent and location at the time of the crime and the searches they made on search platforms like Google or YouTube.

Typical Digital Evidence sources

- Web browser cache (LOCAL)
- Browsing History
- Web page program features

- Mobile phone (LOCAL & REMOTE)
- Sent and received calls/SMS
- Network logs

Steps to Collection

- Seizing the available electronic media.
- Acquiring and creating a forensic image of the electronic media for examination.
  - Find the evidence where is it stored.
  - Find relevant data using recovery techniques.
- Analyzing the forensic image of the original media to ensure the data is not modified.
- Create a good documentation of all the actions.

Evidentiary Reporting

- An Evidence is a piece of information that supports a conclusion.
- Digital evidence is an any data that is recorded or preserved on any medium in or by a computer system or other similar digital device.
- The digital evidence can be read or understood by a person or a computer system or other similar device.
- It is important that information about the investigation be limited to as few people as possible.
- Information should be given on a need-to-know basis, which limits the possibility of the investigation being leaked.

Process of evidentiary writing

- List every piece of evidence analyzed, including serial numbers, hash values, photographs, etc. Write thorough descriptions for photographs, including information on the camera type, date, timestamps and locations.
- Clearly show the steps taken to collect and analyze artifacts, including listing any software or hardware used to extract and analyze data.
- Create a timeline. It’s helpful to create a visual that demonstrates the chronological sequence of events in a way that’s easy for readers to grasp.
- Remember to put yourself in the shoes of the reader.
- What questions might you have about the evidence if you were in their position? If you can adequately answer these questions in your report, you may be released from testifying.

Incident Preparation

- Preparation is the key to effective incident response.

- Even the best incident response team cannot effectively address an incident without predetermined guidelines.
- A strong plan must be in place to support team. In order to successfully address security events, these features should be included in an incident preparation plan:
    - **Develop and Document IR Policies:** Establish policies, procedures, and agreements for incident response management.
    - **Define Communication Guidelines**: Create communication standards and guidelines to enable seamless communication during and after an incident.
    - **Incorporate Threat Intelligence Feeds**: Perform ongoing collection, analysis, and synchronization of threat intelligence feeds.
    - **Conduct Cyber Hunting Exercises:** Conduct operational threat hunting exercises to find incidents occurring within environment. This allows for more proactive incident response.
    - **Assess Threat Detection Capability:** Assess current threat detection capability and update risk assessment and improvement programs.

Incident Detection and Analysis

- Incident detection is the process of identifying, investigating and recovering from a cyber-attack.
- Sometimes, even the best defenses are breached and sensitive data is compromised.
- Incident detection and analysis process focuses on these key areas:
    - Ensuring threat actors are no longer present in the network,
    - Developing and implementing the incident response plan,
    - Identifying the scope of the breach and the data impacted,
    - Closing the vulnerability that allowed the data breach occur.

Questions to address during incident detection and analysis

- When did the event happen?
- How was it discovered?
- Who discovered it?
- Have any other areas been impacted?
- What is the scope of the compromise?
- Does it affect operations?
- Has the source (point of entry) of the event been discovered?
- Have artifacts/malware from the attacker been securely removed?
- Has the system been hardened, patched, and updates applied?
- Can the system be re-imaged?

Containment, Eradication, and Recovery

Write the topic of these three terms

Containment

- Once a threat has been identified, the IR (incident response) team should work to contain the threat to prevent further damage to other systems and the organization at large.
- The responder quickly isolates any infected machine and works on backing up any critical data on an infected system, if possible.
- Next, a temporary fix should be implemented on an infected machine to prevent the threat from escalating. The goal is to minimize the threat.
- Damaged systems removed from production; devices are isolated, compromised accounts are locked down — the bleeding stops here.

4. Eradication

- Eradication is removing and remediating any damage discovered in the identification phase.
- This is normally done by restoring systems from backup and re-imaging workstation systems.
- It's important to note that proper eradication of a cyber infection should be done by trained professionals and should only be done after comprehensive investigation into the incident is completed.
- During the eradication phase, the IR team should also be documenting all actions required to eradicate the threat.
- In addition, any defenses in the network should be improved so that the same incident doesn’t occur again.

Recovery

- Recovery is the testing of the fixes in the eradication phase and the transition back to normal operations.
- Vulnerabilities are remediated, compromised accounts have passwords changed or are removed altogether and replaced with other more secure methods of access.
- At the recovery stage, any production systems affected by a threat will be brought back online.
- This includes any data recovery or restoration efforts that need to take place as well.
- To ensure that they are back to normal operation, test, check, and track the affected systems.

Proactive and Post Incident Cyber Services

- This step provides the opportunity to learn from our experience so we can better respond to future security events.
- Take a look at the incident with a humble but critical eye to identify areas for improvement.
- Then add those improvements to documentation.
- A central part of the incident response methodology is learning from previous incidents to improve the process.
- This helps analyze and document everything about the breach. Determine what worked well in response plan, and where there were some holes.
- Lessons learned from both mock and real events will help strengthen systems against the future attacks.