Digital Forensics and Incident Response (DFIR)

This section is about Digital Forensics and Incident Response (DFIR), and we will cover:

- **Digital Forensics**
- **Incident Response**
- **Malware Analysis**

Digital Forensics

Forensics is the application of science to investigate crimes and establish facts. With the use and spread of digital systems, such as computers and smartphones, a new branch of forensics was born to investigate related crimes: computer forensics, which later evolved into, *digital forensics*.

In defensive security, the focus of digital forensics shifts to analyzing evidence of an attack and its perpetrators and other areas such as intellectual property theft, cyber espionage, and possession of unauthorized content. Consequently, digital forensics will focus on different areas such as:

- **File System: Analyzing a digital forensics image (low-level copy) of a system's storage reveals much information, such as installed programs, created files, partially overwritten files, and deleted files.**
- **System memory: If the attacker is running their malicious program in memory without saving it to the disk, taking a forensic image (low-level copy) of the system memory is the best way to analyze its contents and learn about the attack.**
- **System logs: Each client and server computer maintains different log files about what is happening. Log files provide plenty of information about what happened on a system. Some traces will be left even if the attacker tries to clear their traces.**
- **Network logs: Logs of the network packets that have traversed a network would help answer more questions about whether an attack is occurring and what it entails.**

Incident Response

An *incident* usually refers to a data breach or cyber attack; however, in some cases, it can be something less critical, such as a misconfiguration, an intrusion attempt, or a policy violation. Examples of a cyber attack include an attacker making our network or systems inaccessible, defacing (changing) the public website, and data breach (stealing company data). How would you *respond* to a

cyber attack? Incident response specifies the methodology that should be followed to handle such a case. The aim is to reduce damage and recover in the shortest time possible. Ideally, you would develop a plan ready for incident response.

The four major phases of the incident response process are:

- **Preparation: This requires a team trained and ready to handle incidents. Ideally, various measures are put in place to prevent incidents from happening in the first place.**
- **Detection and Analysis: The team has the necessary resources to detect any incident; moreover, it is essential to further analyze any detected incident to learn about its severity.**
- **Containment, Eradication, and Recovery: Once an incident is detected, it is crucial to stop it from affecting other systems, eliminate it, and recover the affected systems. For instance, when we notice that a system is infected with a computer virus, we would like to stop (contain) the virus from spreading to other systems, clean (eradicate) the virus, and ensure proper system recovery.**
- **Post-Incident Activity: After successful recovery, a report is produced, and the learned lesson is shared to prevent similar future incidents.**