FORENSIC

Legal Informatics and Multimedia

Forensic Analysis for Computer Systems

Plan of the course:

1. Introduction
2. Evolution of Computer Forensics
3. Computer Forensics process
4. Types of Computer Forensics
5. Forensics Readiness

Course 2: Evolution of Computer Forensics

2.1 Introduction

2.2 The need of Computer Forensics

2.3 Rules of Computer Forensics

2.4 Computer Forensics team

2.1 Introduction

Most of the experts agree that the field of computer forensics began to develop more than 40 years ago:

- ✓ By the 1970s, electronic crimes were increasing, especially in the financial sector.

- ✓ Most computers in this era were mainframes, used by trained people with specialized skills who worked in **finance, engineering, and academia**.
- ✓ White-collar fraud* began when people in these fields known a way to make money by manipulating computer data.

*One of the most well-known crimes of the mainframe era is the one-half cent crime. Banks commonly tracked money in accounts to the third decimal place or more.

2.1 Introduction

- ✓ Some computer programmers corrupted this method by opening an account for themselves and writing programs that diverted all the fractional monies into their accounts.
- ✓ In large banks with many branch offices the amount reached hundreds of thousands of dollars.

The history of forensic science dates back thousands of years. Fingerprinting was one of its first applications. The ancient Chinese used fingerprints to identify business documents.

2.1 Introduction (Cont.)

- ✓ In 1984, FBI **Magnetic Media program**, which was later renamed to **Computer Analysis and Response Team (CART)**, was created and it is believed to be the beginning of computer forensic.

- ✓ By the early 1990s, specialized tools for computer forensics were available.
- ✓ In 1988, the **International Association of Computer Investigative Specialists (IACIS)**, an international non-profit corporation composed of volunteer computer forensic professionals introduced training on software for forensics investigations.

- ✓ However, no commercial GUI software for computer forensics was available until **ASR Data** created Expert Witness for Macintosh. This software could recover deleted files and fragments of deleted files.

2.1 Introduction (Cont.)

- ✓ One of the **ASR Data** partners later left and developed **EnCase**, which has become a popular computer forensics tool.

- ✓ It was followed by the formation of **International Organization on Computer Evidence (IOCE)** in 1995, which aims to brings together organizations actively engaged in the field of digital and multimedia evidence to foster communication and cooperation as well as to ensure quality and consistency within the forensic community.

2.1 Introduction (Cont.)

- ✓ With the rise in cybercrime, the G8 nations realized the importance of computer forensics,
- ✓ And in 1997 declared that Law enforcement personnel must be trained and equipped to address high-tech crimes.
- ✓ In 1998, G8 appointed **ICE (Immigration and Customs Enforcement)** to create:
  - international principles,
  - guidelines and
  - procedures relating to digital evidence.

- ✓ In the same year, INTERPOL Forensic Science Symposium was held.

2.1 Introduction (Cont.)

- ✓ As computer technology continued to evolve, more computer forensics software was developed:
  - **ILook**, is a Cyber forensic tool maintained by the IRS Criminal Investigation Division and limited to law enforcement, can analyze and read special files that are copies of a disk.
  - **Access Data Forensic Toolkit (FTK)** has become a popular commercial product that performs similar tasks in the law enforcement and civilian markets.

- ✓ Computers are getting more powerful day by day, so the field of computer forensics must rapidly evolve.

2.2 The need of Computer Forensics

The use of computer forensics is critical because of:

1. The world has become a global village since the beginning of computer, digital devices and the internet.

   - ✓ Life seems impossible without these technologies, as they are necessary for our workplace, home, street, and everywhere.
   - ✓ Information can be stored or transferred by desktop computers, laptop, routers, printers, CD/DVD, flash drives or thumb drives.
   - ✓ The variations and development of data storage and transfer capabilities have encouraged the development of forensic tools, techniques, procedures and investigators.

2.2 The need of Computer Forensics

The use of computer forensics is critical because of:

2. With the ever-increasing rate of cybercrimes, from:
   - Phishing* to hacking and
   - Stealing of personal information not only just limited to a particular country but globally at large:

→ So there is a need for forensic experts to be available in public and private organizations. To be able to handle this, it's vital for network administrator and security staff of networked organizations to have the knowledge to make sure that they have the laws relating to this on their fingertips.

* Phishing is a common type of cyber attack that targets individuals through email, text messages, phone calls and other forms of communication. A phishing attack aims to trick the recipient into falling for the attacker's desired actions, such as revealing financial information, system login credentials, or other sensitive information.

2.2 The need of Computer Forensics (Cont.)

3. The survival and integrity of any given network infrastructure of any company or organization strongly depends on the application of computer forensics.

   - ✓ They should be taken as the main element of computer and network security.
   - ✓ It would be a great benefit for a company if it has knowledge of all the technical and legal aspects of this field.
   - ✓ It will be of help in the provision of evidence and prosecution of the case in the court of law.

2.2 The need of Computer Forensics (Cont.)

3. New laws aimed at the protection of customer’s data are continuously being developed.
   - ✓ If they lose data the liability naturally goes to the company.
   - ✓ Such cases, if they occur will automatically result in the company or organization being brought to the court of law for failure to protect personal data, this can turn out to be very expensive.
   - ✓ But through the application of forensic science, huge chunks of money can be saved by the firms concerned.

2.3 Rules of Computer Forensic

There are several rules and boundaries that should be kept in mind while conducting an investigation. Which are:

1) Minimize or eliminate the chances of examining the original evidence

Make the accurate and exact copy of the collected information to minimize the option of examining the original:

- ✓ create duplicates and investigate the duplicates.
- ✓ we should make the exact copy in order to maintain the integrity of the data.

2.3 Rules of Computer Forensic

2) Don't Proceed if it is beyond our knowledge

If we see a roadblock while investigating, then stop at that moment and do not proceed if it is beyond our knowledge and skills:

- ✓ Consult or ask an experienced to guide you in a particular matter.
- ✓ This is to secure the data, otherwise, the data might be damaged which is unbearable.
- ✓ Do not take this situation as a challenge, go and get additional training because we are in the learning process and we love to learn.

2.3 Rules of Computer Forensic (Cont.)

3) Follow the rules of evidence

- ✓ The rule of evidence (the evidence should highlight the crime trace) must be followed during the investigation process to make sure that the evidence will be accepted in court.

4) Create Document

- ✓ Document the behavior, if any changes occur in evidence.
- ✓ An investigator should document the reason, result and the nature of change occurred with the evidence. Let say, restarting a machine may change its temporary files, note it down.

2.3 Rules of Computer Forensic (Cont.)

5) Get the written permission and follow the local security policy

Before starting an investigation process:

- ✓ We should make sure to have written permission with instruction related to the scope of your investigation.
- ✓ It is very important because during the investigation we need to get access or need to make copies of the sensitive data, if the written permission is not with we may find ourselves in trouble for breaching the IT* security policy.

*Information Technology security is a cybersecurity strategy that prevents unauthorized access to organizational assets including computers, networks and data.

2.3 Rules of Computer Forensic (Cont.)

6) Be ready to testify

- ✓ Since we are collecting the evidence then we should make ourselves ready to testify it in the court,
- ✓ Otherwise the collected evidence may become inadmissible.

7) Our action should be repeatable

- ✓ Do not work on **trial-and -error**, else no one is going to believe we and our investigation.
- ✓ Make sure to document every step taken.
- ✓ We should be confident enough to perform the same action again to prove the authenticity of the evidence.

2.3 Rules of Computer Forensic (Cont.)

8) Work fast to reduce data loss

Work fast to eliminate the chances of data loss:

- ✓ Volatile data may be lost if not collected in time.
- ✓ While automation can also be introduced to speed up the process, do not create a rush situation.
- ✓ Increase the human workforce where needed.
- ✓ Always start collecting data from volatile evidence.

2.3 Rules of Computer Forensic (Cont.)

9) Don't shut down before collecting evidence

This is a rule of thumb since the:

- ✓ **Collection of data or evidence** itself is important for an investigation.
- ✓ If the system is shut down, then we will lose the volatile data.
- ✓ Shutdown and rebooting should be avoided at all cost.

10) Don't run any program on the affected system

- ✓ Collect all the evidence, copy them, create many duplicates and work on them.
- ✓ Do not run any program, otherwise, we may trigger something that we don't want to trigger. Think of a Trojan horse*.

* A Trojan horse virus is a type of malware that disguises itself within legitimate applications and software.

2.4 Computer Forensics team

- ✓ Law enforcement and security agencies are responsible for investigating computer crime, however,
- ✓ every organization should have the capability to solve their basic issues and investigation by themselves.
- ✓ Even an organization can hire experts from small or mid-size computer investigation firms.
- ✓ Also, we can create our own firm that provides computer forensic services.

2.4 Computer Forensics team

- ✓ To do so, we need a
  - forensics lab,
  - permission from the government to establish a forensics business,
  - the right tools with the right people and rules/policies to run the business effectively and efficiently.

- ✓ Without this ability, it is very hard for an organization to determine :
  - the fraud,
  - illegal activities, policy,
  - or network breach or even they will find it hard to implement the cybersecurity rules in the organization.
- ✓ The need for such abilities may vary and it depends on the nature of business, security threats and the possible loss.

2.4 Computer Forensics team (Cont.)

Here are the key people that a computer investigation firm should have:

- ✓ **Investigators:** This is a group of people (number depends on the size of the firm) who handle and solve the case.
  - It is their job to use forensic tools and techniques in order to find evidence against the suspect.
  - They may call law enforcement agencies if required.
  - Investigators are supposed to act immediately after the occurrence of the event that is suspected of criminal activity.

- ✓ **Photographer:** To record the crime scene is as important as investigating it.
  - The photographer's job is to take photographs of the crime scene (IT devices and other equipment).

2.4 Computer Forensics team (Cont.)

✓ **Incident Handlers (first responder):** Every organization, regardless of type, should have incident handlers in their IT department.

- The responsibility of these people is to monitor and act if any computer security incidence happens,
- Such as breaching of network policy, code injection, server hijacking, RAT or any other malicious code installation.
- They generally use a variety of computer forensics tools to accomplish their job.

2.4 Computer Forensics team (Cont.)

- ✓ **IT Engineers & technicians** (other support staff): This is the group of people who run the daily operation of the firm.
  - They are IT engineers and technicians to maintain the forensics lab.
  - This team should consist of a network administrator, IT support, IT security engineers and desktop support.
  - The key role of this team is to make sure the smooth organizational functions, monitoring, troubleshooting, data recovery and to maintain the required backup.

- ✓ **Attorney:** Since computer forensics directly deal with investigation and to submit the case in the court, an attorney should be a part of this team.