Computer Forensics Tutorials

Instructor	Dr.Abdul Rehman Al-Ghamdi	Phone	+966-503770707
Office	CCIT	Version	one
Office Hours	0800 – 1400Hours	Email	

Forensics

fo·ren·sics (fə-rə˘n´sĭks, -zĭks) n. (used with a sing. verb) The use of science and technology to investigate and establish facts in criminal or civil courts of law.

Digital forensics/Computer forensics

The science of identifying, preserving, recovering, analyzing and presenting facts about digital evidence found on computers or digital storage media devices.

Figure1.

History of digital forensics

Computer forensics can be traced back to as early as 1984 when the FBI laboratory and other law enforcement agencies begun developing programs to examine computer evidence. Research groups like the Computer Analysis and Response Team (CART), the Scientific Working Group on Digital Evidence (SWGDE), Laboratory Accreditation Board (ASCLD-LAB), the Technical Working Group on Digital Evidence (TWGDE), and the National Institute of Justice (NIJ) have since been formed in order to discuss the computer forensic science as a discipline including the need for a standardized approach to examinations. International Data Corporation (IDC) reported that the market for intrusion-detection and vulnerability assessment software will reach 1.45 billion dollars in 2006.

Digital Evidence

One important element of digital forensics is the credibility of the digital evidence. Digital evidence includes computer evidence, digital audio, digital video, cell phones, digital fax machines etc.

Figure2.

Investigation process of digital forensics

Investigative process of digital forensics can be divided into several stages. There are four major stages: preservation, collection, examination, and analysis see figure 3.

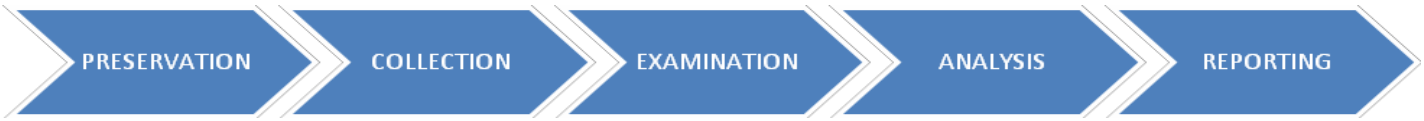

Figure3. Digital forensics Process

Preservation:

Preservation stage corresponds to \freezing the crime scene". It consists in stopping or preventing any activities that can damage digital information being collected. Preservation involves operations such as preventing people from using computers during collection, stopping ongoing deletion processes, and choosing the safest way to collect information.

Collection:

Collection stage consists in finding and collecting digital information that may be relevant to the investigation. Since digital information is stored in computers, collection of digital information means either collection of the equipment containing the information, or recording the information on some medium. Collection may involve removal of personal computers from the crime scene, copying or printing out contents of files from a server, recording of network traffic, and so on.

Examination:

Examination stage consists in a \in-depth systematic search of evidence" relating to the incident being investigated. The outputs of examination are data objects found in the collected information. They may include log files, data files containing specific phrases, times-stamps, and so on.

Analysis:

The aim of analysis is to "draw conclusions based on evidence found".

Reporting:

This entails writing a report outlining the examination process and pertinent data recovered from the overall investigation.

Answer the following questions

1. *What is forensic science?*

   ---
2. *Define digital forensics?*

   ---
3. *Write down the steps of digital investigation process?*

   ---
4. *What is a digital evidence?*

