Certified Hacking Forensics Investigator

Module #02 : Computer Forensics Investigation Process

Eng. Mohammad Khreesha
Twitter: @banyrock
Facebook : http://www.fb.com/khreesha

Module Objectives

➔ **After Successfully completing this module, you will be able to :**

1. Understand the importance of computer forensics process.
2. Describe the various phases of the computer forensic investigation process.
3. Identify the requirements for building a computer forensics lab and an investigation team.
4. Understand the roles of a First Responder.
5. Perform search and seizure, evidence collection, management and preservation.
6. Understand chain of custody and its importance.
7. Discuss about data duplication, deleted data recovery and evidence examination.
8. Write an investigation report and testify in a court form.

Computer Forensics Process Phases

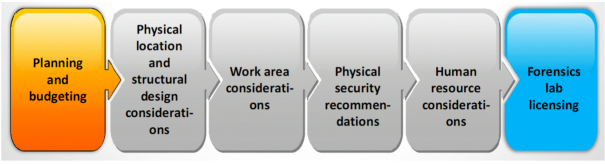
➔ Pre-investigation Phase:
- Setting up a computer forensics lab(CFL), toolkit, and workstation
- The investigation team and getting approval from the relevant authority
- Planning the process, defining mission goals, and securing the case perimeter and devices involved.

➔ Investigation Phase:
- Acquisition, preservation, and analysis of the data to identify the source of crime and the culprit.
- Implementing the technical knowledge to find evidence, examine, document, and preserve the findings.

➔ Post-investigation Phase:
- Ensure that the target audience can easily understand the report
- Ensure report provides adequate and acceptable evidence.
- Report should comply with all local laws and standards
- It should be legally sound and acceptable in the court of law.

Setting up a Computer Forensics Lab

- A Computer Forensics Lab (CFL) is a location designated for conducting computer-based investigation with regard to the collected evidence.
- The lab houses instruments, software and hardware tools, suspect media, and forensics workstations required to conduct the investigation.



Building Forensics Workstation

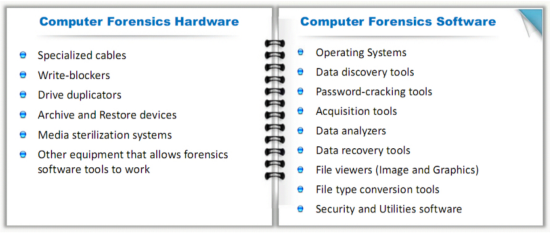
- **The Computer Forensics approach should be clearly defined before building the forensics workstation.**

- **The computer forensics workstation should have facilities and tools to :**

1. Support hardware-based local and remote network drive duplication.
2. Validate the image and file's integrity
3. Identify the date and time when the files have been modified, accessed, or created.
4. Identify the deleted files.
5. Support the removable media.
6. Isolate and analyze free drive space.

Build Computer Forensics Toolkit

- **Computer forensics tools can be divided into two types :**



Build Investigation Team

People Involved in an Investigation Team	
Photographer	Photographs the crime scene and the evidence gathered
Incident Responder	Responsible for the measures to be taken when an incident occurs
Decision Maker	Responsible for authorization of a policy or procedure for the investigation process
Incident Analyzer	Analyzes the incidents based on their occurrence
Evidence Examiner/Investigator	Examines the evidence acquired and sorts the useful evidence
Evidence Documenter	Documents all the evidence and the phases present in the investigation process
Evidence Manager	Manages the evidence in such a way that it is admissible in the court of law
Evidence Witness	Offers a formal opinion in the form of a testimony in the court of law
Attorney	Gives legal advice

Computer Forensics Investigation Process Methodology

- Get authorization to conduct the investigation, from an authorized decision maker.
- Document all the events and decisions at the time of the incident and incident response.
- Depending on the scope of the incident and presence of any national security issues or life safety issues, the first priority is to protect the organization from further harm.

Continue..

- Follow the Computer Forensics Investigation Methodology:

1. First Response
2. Search and Seizure
3. Collect the Evidence
4. Secure the Evidence
5. Data Acquisition
6. Data Analysis
7. Evidence Assessment
8. Documentation and Reporting
9. Testify as an Expert Witness

Documentation

- Documentation of the electronic crime scene is a continuous process during the investigation, making a permanent record of the scene. It includes photographing and sketching of the scene.
- If the evidence gathered by the CFP suggests that the suspect has committed a crime, he or she will produce that evidence in court. If the evidence suggests that the suspect has breached company policy, the CFP will hand over the evidence at the corporate enquiry.
- If the suspect is present at the time of the search and seizure, the incident manager or the laboratory manager may consider asking some questions. However, they must comply with the relevant human resources or legislative guidelines with regard to their jurisdiction

Scenario #1 :Dealing with Powered off Computers

- At this point of the investigation, do not change the state of any electronic devices or equipment:
  - If it is switched OFF, leave it OFF
  - If a monitor is switched OFF and the display is blank:
  - Turn the monitor ON, move the mouse slightly, observe the changes from a blank screen to another screen, and note the changes and photograph the screen.
  - If a monitor is switched ON and the display is blank
  - Move the mouse slightly. If the screen does not change, do not perform any other keystroke.
  - Photograph the screen.

Scenario #2 :Dealing with Networked Computers

- If the victim's computer has an Internet connection, the first responder must follow the following procedure in order to protect the evidence:
  - Unplug the network cable from the router and modem internet can make it vulnerable to further attack
  - Don't use the PC for evidence search because it may alter or change the integrity of the existing evidence
  - Unplug all the cords and devices connected to the computer and label them for later identification
  - Unplug the main power cord from the wall socket
  - Pack the collected electronic evidence properly and place it in a static-free bag
  - Keep the collected evidence away from magnets, high temperature, radio transmitters, and other elements that may damage the integrity of the evidence
  - Document the steps that involved in searching and seizing the victim's computer for later investigation

Follow us :

- https://www.fb.com/technawidotcom
- https://www.twitter.com/technawidotnet
- http://www.technawi.net

تكناوي technawi.net