Forensics and first response

Objectives:

At the end of this episode, I will be able to:

Understand what the objectives of computer forensics are.

Explain what the phases involved in the Computer Forensics investigation process are.

Identify what the role of the First Responder is.

Define what the main responsibilities of first responders are.

External Resources:

Forensics and First Response

Computer forensics refers to a set of methodological procedures and techniques that help identify, gather, preserve, extract, interpret, document, and present evidence from computing equipment, whereby any evidence discovered is acceptable during a legal and/or administrative proceeding.

The objectives of computer forensics are to:

```
▪ Identify, gather, and preserve the evidence of a cyber crime
▪ Track and prosecute the perpetrators in the court of law
▪ Gather evidence of cyber crimes in a forensically sound manner
▪ Interpret, document, and present the evidence to be admissible during
prosecution
▪ Estimate the potential impact of a malicious activity on the victim, and
assess the intent of the perpetrator
▪ Find vulnerabilities and security loopholes that help attackers
▪ Understand the techniques and methods attackers use to avert prosecution
and overcome them
▪ Recover deleted files, hidden files, and temporary data that could be used
as evidence
```

What are the phases involved in the Computer Forensics investigation process? -

```
▪ Pre-investigation Phase - involves all the tasks performed prior to the
commencement of the actual investigation. It involves setting up a computer
forensics lab, building a forensics workstation, investigation toolkit, the
investigation team, getting approval from the relevant authority, and so on.
This phase also includes steps such as planning the process, defining mission
goals, and securing the case perimeter and devices involved.

▪ Investigation Phase - involves acquisition, preservation, and analysis of
the evidentiary data to identify the source of crime and the culprit. Trained
professionals perform all the tasks involved in this phase in order to ensure
quality and integrity of the findings.

▪ Post-investigation Phase - involves reporting and documentation of all the
actions undertaken and the findings during the course of an investigation.
Every jurisdiction has set standards for reporting the findings and evidence;
the report should comply with all such standards as well as be legally sound
and acceptable in a court of law.
```

What is Forensic readiness? -

Refers to an organization's ability to make optimal use of digital evidence in a limited period of time and with minimal investigation costs. It enables an organization to collect and preserve digital evidence quickly and efficiently with minimal investigation costs.

What is a Forensics policy? -

Sets guidelines for the employees, investigating personnel, and authorities to contribute to the forensics investigation process. The Chief Information Security Officer (CISO) should be responsible for setting proper guidelines in association with other security and audit personnel.

What are the Forensic readiness procedures we should be aware of? -

```
▪ Creating the Investigation Team
▪ Maintaining an Inventory
▪ Host Monitoring
▪ Network Monitoring
```

What is the role of the First Responder? -

A first responder plays an important role in the computer forensics process because he or she is the first person who arrives at the crime scene for initial investigation.

The main responsibilities of first responders are:

- Identify & protect the crime scene
- Preserve evidence
- Collect information about the incident
- Document ALL findings
- Package & Transport the evidence