

*Chapter .1.2*

# Investigation Procedure and Response



## Aim

To equip the students in order to understand the basics of a First Responders job, along with the policies, procedures, tools and techniques, and various standards developed by industry experts



# Instructional Objectives

After completing this chapter, you should be able to:

- Explain the entire First Investigation Process
- Describe the incident response in different situations
- Outline the computer investigation procedure

# First Investigation Process

---

# Computer Forensics Principles

The information stored in a computer or storage media must not be changed.

A person must be competent enough in handling the original data held on a computer or storage media.

An audit trail of all processes applied to computer-based electronic evidence, should be created and preserved.

A person who is responsible for the investigation must also be accountable for the adherence to the law and ACPO principles

# First Responder Procedures

The people who provide the first response during the forensic investigation are called as First Responders.


Employee of Law  
Enforcement agency

Local system  
administrators

Forensic Investigator

Examples for First Responders

## Role of a first responder

- 
- Identifying and verifying the crime scene
  - Protecting all the sources of evidence
  - Collecting all required information
  - Preserving temporary and fragile evidence
  - Documenting all actions and findings
  - Packaging and transporting the electronic evidence

## First responder Tool kit

The following procedures have to be followed to create a First Responder Toolkit:

Installation of a forensic computer

Documenting the details of the forensic computer

Documenting the summary of the collected tools

Testing the tools





## Quiz / Assessment

- 1) Who starts the first round of investigation when an incident is reported and confirmed?
- a) A first responder
  - b) A first investigator
  - c) A first interviewer
  - d) A best investigator



## Quiz / Assessment

2) Creating a First responder Toolkit includes \_\_\_\_\_.

- a) Data acquisition process details
- b) Data presentation process
- c) Documenting the forensic computer details
- d) Acquisition of the tool process



## Quiz / Assessment

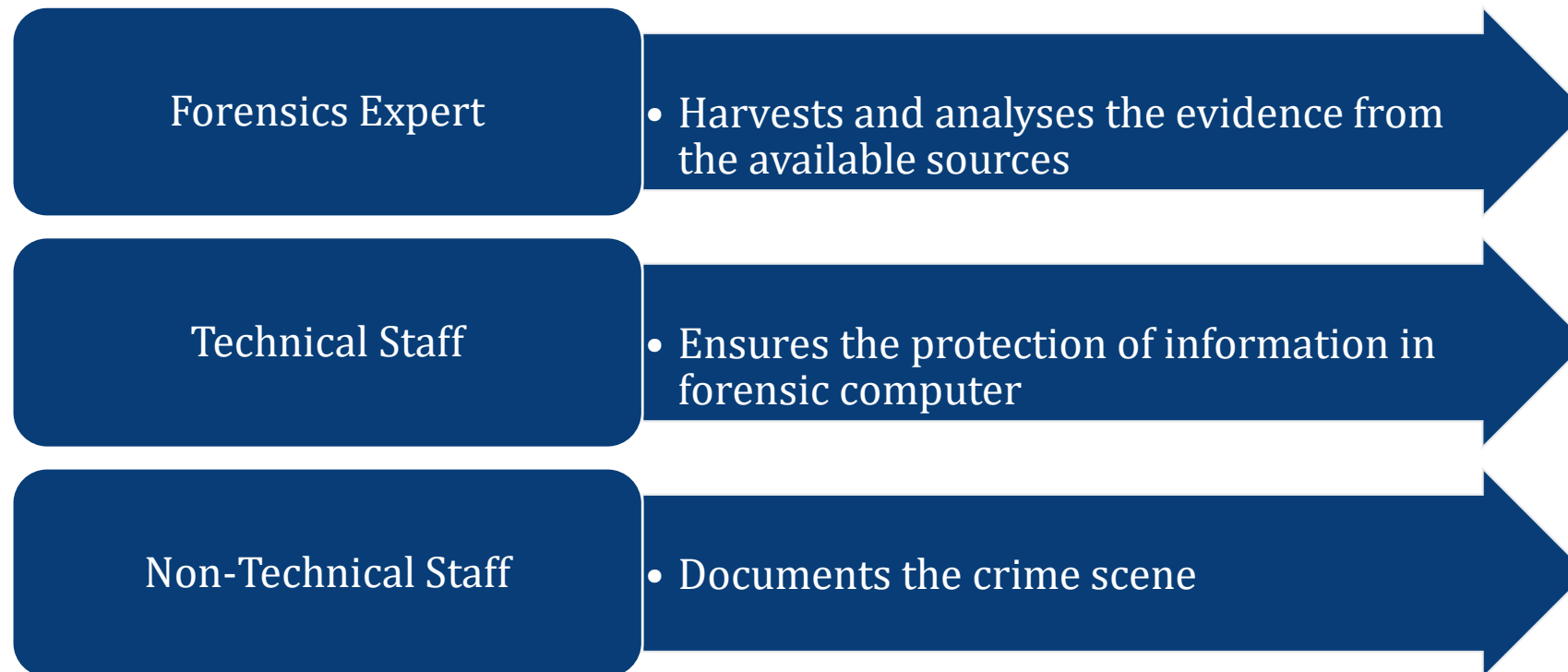
3) The role of a first responder is \_\_\_\_\_.

- a) The acquisition of crime scene
- b) Disturbing the crime scene
- c) Protecting the crime scene
- d) Protecting staff of crime

# Incident Response in Different Situations

# Incident Responses in Different Situations

An incident response can be done through following three groups:





## Quiz / Assessment

- 1) A \_\_\_\_\_ harvests and analyses the evidence from computers or any other form of data storage device.
- a) Forensics expert
  - b) Non-forensics expert
  - c) Technical person
  - d) System admin expert



## Quiz / Assessment

2) The system/network administrator plays an important role in ensuring \_\_\_\_\_.

- a) Local system/network protection
- b) Network access protection
- c) Local Responses protection
- d) Chain of data protection



## Quiz / Assessment

3) The responsibilities of a forensics expert include \_\_\_\_\_.

- a) Securing the crime scene
- b) Global access to crime scene
- c) Replica of crime scene
- d) Deviating the crime scene



# Computer Investigation Procedure

---

# Computer Forensics Investigation Procedure

Steps in Forensics Investigation:





## Quiz / Assessment

- 1) The first step of any forensic investigation is \_\_\_\_\_.
- a) Scoping
  - b) Detecting
  - c) Volatile data
  - d) Chain of custody



## Quiz / Assessment

2) There are two types of evidence that exist on any system in question that is \_\_\_\_\_ and non-volatile data.

- a) Volatile
- b) System description
- c) Data acquisition
- d) System advance



## Quiz / Assessment

3) \_\_\_\_\_ is the system activity records of all the files involved, with MAC times, i.e. Modified, Accessed and Created times for all the files.

- a) Function
- b) Timeline
- c) Media
- d) System



## Summary

- ✓ An incident is an event that threatens the security of a computer system or network in an organization. Today most businesses depend on computer networks and internet. Once the incident occurs the investigator search for the evidence.
- ✓ A forensics expert is one who collects and analyses the evidence from computers, laptops, networks, or any other form of data storage device.
- ✓ A successful forensics investigation depends upon the response provided by the first responder during the first interaction with the system
- ✓ SANS has developed one of the best forensics methodology which is utilized by the industry experts



## Activity

Online/Offline

**Online/Offline  
Activity  
(30 min)**

- Define FIR and discuss who can lodge a FIR
- List the basic phases of investigating crime scene



## e-References

- (2016). *Sans.org*. Retrieved 5 July 2016, from <https://www.sans.org/reading-room/whitepapers/incident/integrating-forensic-investigation-methodology-ediscovery-33448>
- *SANS Institute: Reading Room - Forensics*. (2016). *Sans.org*. Retrieved 5 July 2016, from <https://www.sans.org/reading-room/whitepapers/forensics>
- *First Responders*. (2016). *Transition.fcc.gov*. Retrieved 5 July 2016, from <https://transition.fcc.gov/pshs/emergency-information/guidelines/first-responders.html>
- *Computer Forensics and Investigation Methodology – 8 steps*. (2014). *Count Upon Security*. Retrieved 5 July 2016, from <https://countuponsecurity.com/2014/08/06/computer-forensics-and-investigation-methodology-8-steps>
- *Responding to IT Security Incidents*. (2016). *Technet.microsoft.com*. Retrieved 5 July 2016, from <https://technet.microsoft.com/en-us/library/cc700825.aspx>





## External Resources

1. Hayes, D. D. (2015). A Practical Guide to Computer Forensics Investigations. US: Pearson Education, Inc.
2. Nelson, B., Phillips, A., & Steuart, C. (2010). Guide to Computer Forensics and Investigations, Fourth Edition. USA: Cengage Learning.
3. Philipp, A., Cowen, D., & Davis, C. (2010). Hacking Exposed Computer Forensics, Second Edition. New York: McGraw-Hill.