

Step 6: Evidence Gathering and Forensic Analysis

Objectives:

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

Understand what evidence gathering and forensic analysis is.

Explain what Step 6, Evidence Gathering and Forensic Analysis, of the IH&R process is.

Identify what the process flow for Evidence Gathering and Forensics Analysis should be for the IH&R team.

Define the role that evidence handling plays in evidence gathering and forensics analysis of evidence for the IH&R team.

External Resources:

Step 6 Evidence Gathering and Forensic Analysis

What is the process flow for Evidence Gathering and Forensics Analysis? -

1. The IH&R team will collect evidence about the incident and simultaneously create a chain of custody document.
2. The investigators analyze the evidence to identify the cause and nature of the incident.
3. They document the results of the forensic analysis and submit their report to management.
4. If analysis can identify a perpetrator, management decides whether to prosecute, or whether to allow the organizational disciplinary team to handle it.
5. If there is need for law enforcement, management or a designated authority contacts a third-party law enforcement agency.
6. If the investigation fails to identify the perpetrator, then management decides whether to close the investigation or to pass it to an external investigation agency for further action.
7. If third-party investigators can identify a perpetrator, then they report their findings to management.
8. If third-party investigators also fail to identify a perpetrator, the IH&R team or management can recommend an update to the IH&R processes that may enable them to carry out successful investigations in the future.

To gather evidence effectively, the organization must perform the following:

- o Train employees to become incident handlers/responders
- o Create and implement forensic readiness policies and procedures
- o Enable logging on all systems

The process of collecting evidence includes:

- o Identification of target resources, networks, and connected resources
- o Securing and documenting the crime scene
- o Extracting the fragile and volatile evidence
- o Securely handling, packing, and transportation of all evidence/devices
- o Extraction of static evidence stored as media and other resources

What about Evidence Handling? -

Evidence handling or preservation is an integral part of the evidence gathering process.

Preservation involves completely backing up all the affected systems for further investigation and recovery into/onto appropriate media devices.

The IH&R team must store the backups in a physically secure location.

Protect the collected evidence from physical or logical damage and maintain a well-documented chain of custody.

Only the individuals authorized for legal or data recovery purposes should have access to the backup.