MODULE - 4: COMPUTER FORENSIC INVESTIGATION PROCESS

INTRODUCTION TO COMPUTER CRIME INVESTIGATION

According to Warren G. Kruse II and Jay G. Heiser, authors of *Computer Forensics: Incident Response Essentials*, computer forensics is "the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis." The computer investigation model shown in figure 1 organizes the different computer forensics elements into a logical flow

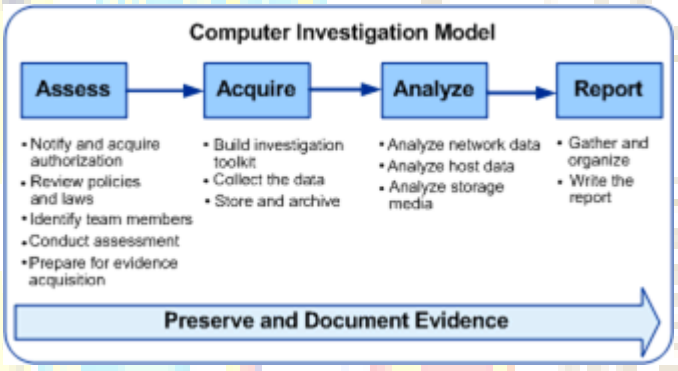

Figure 1: Computer investigation model

The four investigation phases and accompanying processes in the figure should be applied when working with digital evidence. The phases can be summarized as follows:

- **Assess the situation:** Analyze the scope of the investigation and the action to be taken.
- **Acquire the data:** Gather, protect, and preserve the original evidence.
- **Analyze the data:** Examine and correlate digital evidence with events of interest that will help you make a case.
- **Report the investigation:** Gather and organize collected information and write the final report.

Detailed information about each of the phases is provided in the proceeding sections of this unit.

2.2.1 Initial Decision-Making Process

Before you begin each of the general investigation phases you should apply the initial decision-making process shown in the *Figure 2*.

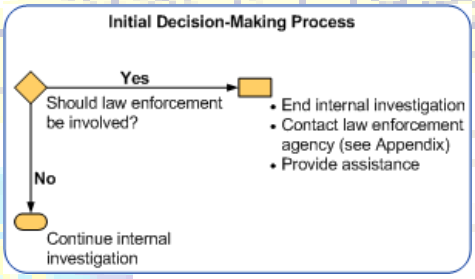

Figure 2: Initial decision making process

You should determine whether or not to involve law enforcement with the assistance of legal advisors. If you determine that law enforcement is needed, then you need to continue the internal investigation unless law enforcement officials advise you otherwise. Law enforcement might not be available to assist in the investigation of the incident, so you must continue to manage the incident and investigation for later submission to law enforcement.

Depending on the type of incident being investigated, the primary concern should be to prevent further damage to the organization by those person(s) who caused the incident. The investigation is important, but is secondary to protecting the organization unless there are national security issues.

2.6 ASSESS THE SITUATION

This section describes how to conduct a thorough assessment of the situation, how to establish scope, and the required resources for an internal investigation. Use the five-step process shown in the *Figure 3*.

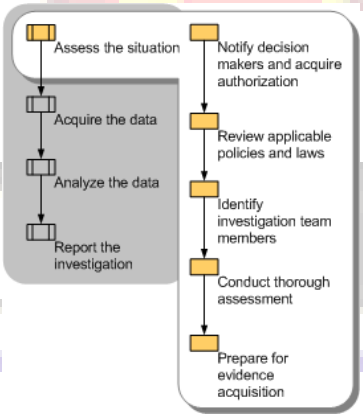

Figure 3: Assesment phase of the computer investigation model

2.3.6 Notify Decision Makers and Acquire Authorization