2.6.6 Forensic Investigation Facts

Forensic investigation results can be used in a court of law if properly handled and documented. *Evidence* is the artifacts and objects collected to document a security breach. It is used to prove the truth or fallibility of declarations made in court. Not all evidence is admissible in a court of law. For evidence to be admissible, it must be:

- Directly related to the crime
- Collected fairly and lawfully
- Reliable
- Used for intended purposes only
- Recognized or acknowledged by either the witness, prosecutor, or defendant
- Marked correctly

When a security incident is identified, legal counsel will often anticipate a government audit and possible litigation as a result of the investigation. Internal counsel will generate a *legal hold*, which notifies the organization to preserve all relevant information. A legal hold will often require changes in the way system data is backed up, stored, and archived.

To ensure the use of evidence in a forensic investigation, certain protective measures must be taken at every stage in the life of evidence. The *evidence life cycle* describes the use of evidence in several stages, including collection, use in court, and eventual return to the owner. When managing evidence, you must make sure that it is properly handled to ensure its integrity. To ensure that evidence is admissible in court, you must be able to provide its *chain of custody*. The chain of custody:

- Documents the integrity of the evidence by providing a record of every person it has come in contact with and under what conditions the contact occurred. Without a chain of custody document, there is no way to prove who might have had access to the evidence, meaning that the evidence could have been altered after discovery. Failure to provide a valid chain of custody could make the evidence worthless in court.
- Should be started the moment evidence is discovered and should include what the evidence is, who found it, under what circumstances it was found, its location, the date and time of its original discovery, how it was handled, and all precautionary actions that have been taken to ensure its integrity.
- Should be maintained throughout the evidence life cycle to document the people and procedures used at each stage.

Be aware that many organizations will choose not to bring evidence to court to avoid the negative publicity that could be associated with a trial.

After you have analyzed the attack and gathered evidence, be aware that some states require you to notify individuals if their personal information might have been compromised. For example, if an incident involves the exposure of credit card numbers, identifying information (such as Social Security numbers), or medical information, you might be legally obligated to notify potential victims and take measures to help protect their information from additional attacks.

A forensic investigation may reveal the possibility of involvement by foreign actors. Evidence may point to economic espionage, which is the theft of trade secrets or proprietary information. Economic espionage could be used to benefit a foreign government. When this happens, you need to work closely with the FBI and other government agencies to gather intelligence and counterintelligence. Your company can implement policies and procedures to combat foreign threats and better protect company secrets. With active logging in place within your system, forensic evidence can be obtained from access logs that have been enabled for firewalls, databases, applications, and other systems.

The following table lists the main types of evidence:

Type	Description
Best	*Best* evidence includes original, authentic objects. As an exception to this rule, copies can be submitted for the following reasons: ▪ The original was lost in a fire, flood, or other natural disaster. ▪ The original was destroyed while following normal office procedure. This includes unintentional destruction by careless employees or cleaning staff. ▪ A third party outside of the court's subpoena power has the original. Oral evidence does not fall into this category.
Corroborative	*Corroborative* evidence is information that supports another fact or detail.
Hearsay	*Hearsay* evidence is obtained from a source other than personal, firsthand knowledge. Hearsay evidence is generally not admissible in court. Computer-generated records and other business records cannot be proven accurate and reliable and, therefore, are considered hearsay evidence. However, there are exceptions for records such as audit trails, audit trail reports, and incident reports that are: ▪ Made during the regular course of business and authenticated by witnesses familiar with their use. ▪ Relied upon in the regular course of business. ▪ Made by a person with knowledge of these records. ▪ Made by a person with information transmitted by a person with knowledge. ▪ Made at or near the time of occurrence of the act being investigated. ▪ Held in the custody of the witness on a regular basis.

The following table describes each stage of the evidence life cycle and the special precautions to take:

Stage	Description
Collection and Identification	All evidence must be properly marked as evidence at the time it is found. Any identifying characteristics of the evidence must also be recorded at this time. If at all possible, evidence should be placed in a plastic bag or clean storage container and properly marked. A chain of custody document should be started at this time. Evidence should not be collected if the method of collection violates private rights. Different methods for obtaining evidence are as follows: ▪ Tempting the attacker. This is known as *enticement* and is usually legal. ▪ Encouraging the attacker to attack. This is known as *entrapment* and is usually illegal. ▪ Obtaining an order authorizing search and seizure. This is usually in the form of a *search warrant* and is legal. ▪ Obtaining an order to summon a witness to appear in court. This is known as a *subpoena* and is legal.
Preservation and Analysis	Evidence analysis should be made by trained specialists only. Thorough examination and documentation of each piece of evidence is crucial. The International Organization on Computer Evidence (IOCE) sets the standards concerning preservation and analysis of computer evidence. According to the IOCE, preservation and analysis of all computer data must comply with the following rules: ▪ Evidence should never be altered by procedure. Instead, copies of digital evidence are made and procedures are performed on those copies. ▪ Procedures should be performed by a trained examiner. ▪ There should be a properly documented chain of custody. ▪ The examiner is responsible for all actions concerning the evidence.
Storage	The utmost care must be taken to store and preserve evidence. For example, a hard disk should be stored in an antistatic bag that is then sealed and placed in a cardboard box with foam lining.
Transportation and Processing	Evidence needs to be protected during all stages of transportation. Take all necessary measures to ensure that transported evidence is in the same condition when it arrives at the court room as it was when it left the lab or investigation site. Materials should be packaged to prevent damage, and the transportation method should ensure the appropriate environmental requirements for the evidence (such as heating, air conditioning, or humidity requirements). If the evidence is too large to transport, a detailed forensic examination may need to take place on site.
Presentation in Court	All evidence needs to have been submitted to the court and deemed admissible before it is presented during trial. Continue to maintain proper handling procedures and document the chain of custody during all stages of the trial.
Return to Owner	All evidence should be returned to the original owner after the case is completely settled, with the exception of some types of evidence, such as drugs or drug paraphernalia. It is important to note that some trials can take several years to be completely resolved, possibly resulting in the evidence not being returned during its usable lifetime.