**Chapter 19: Investigations and Ethics**

Administrative investigations are internal investigations that examine either operational issues or a violation of the organization’s policies.

Criminal investigations, typically conducted by law enforcement personnel, investigate the alleged violation of criminal law. Criminal investigations must follow strict evidence collection and preservation processes.

Civil investigations typically do not involve law enforcement but rather involve internal employees and outside consultants working on behalf of a legal team. They prepare the evidence necessary to present a case in civil court resolving a dispute between two parties.

Regulatory investigations vary widely in scope and procedure and are often conducted by government agents. Some regulatory investigations may not involve government agencies. These are based on industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS).

To successfully prosecute a crime, the prosecuting attorneys must provide sufficient evidence to prove an individual’s guilt beyond a reasonable doubt.

The items of evidence that you maintain and may use in court are also known as artifacts.

There are three basic requirements for evidence to be introduced into a court of law. The evidence must be relevant, material (that is, related) to the case and competent, meaning it must have been obtained legally.

Types of Evidence

* **Real evidence** (also known as object evidence) consists of things that may actually be brought into a court of law. In common criminal proceedings, this may include items such as a murder weapon, clothing, or other physical objects.
* **Documentary evidence** includes any written items brought into court to prove a fact at hand.
* **Testimonial evidence** is, quite simply, evidence consisting of the testimony of a witness, either verbal testimony in court or written testimony in a recorded deposition. Witnesses must take an oath agreeing to tell the truth.
* **Demonstrative evidence** is evidence used to support testimonial evidence. It consists of items that may or may not be admitted into evidence themselves but are used to help a witness explain a concept or clarify an issue.

Media analysis, a branch of computer forensic analysis, involves the identification and extraction of information from storage media.

In-Memory Analysis - When gathering the contents of memory, analysts should use trusted tools to generate a memory dump file and place it on a forensically prepared device, such as a USB drive. This memory dump file contains all the contents collected from memory and may then be used for analysis.

Network forensic analysis, therefore, often depends on either prior knowledge that an incident is under way or the use of preexisting security controls that log network activity. These include IDS, IPS, Firewall, and other network devices logs. When collecting data directly from a network during a live analysis, forensic technicians should use a SPAN port on a switch (which mirrors data sent to one or more other ports for analysis).

Software Analysis - In some cases, when malicious insiders are suspected, the forensic analyst may be asked to conduct a review of software code, looking for backdoors, logic bombs, or other security vulnerabilities.

Hardware/Embedded Device Analysis - Forensic analysts often must review the contents of hardware and embedded devices.

Key Investigation Principles:

* Never conduct your investigation on an actual system that was compromised. Take the system offline, make a backup, and use the backup to investigate the incident.
* Never attempt to “hack back” and avenge a crime. You may inadvertently attack an innocent third party and find yourself liable for computer crime charges.
* If in doubt, call in expert assistance. If you don’t want to call in law enforcement, contact a private investigations firm with specific experience in the field of computer security investigations.

**Major Categories of Computer Crime**

Military and intelligence attacks are launched primarily to obtain secret and restricted information from law enforcement or military and technological research sources.

Business attacks focus on illegally jeopardizing the confidentiality, integrity, or availability of information and systems operated by a business.

Financial attacks are carried out to unlawfully obtain money or services. They are the type of computer crime you most commonly hear about in the news. The goal of a financial attack could be to steal credit card numbers, increase the balance in a bank account, or obtain fraudulent funds transfers.

Terrorist attacks are a reality in modern society. Terrorist attacks differ from military and intelligence attacks. The purpose of a terrorist attack is to disrupt normal life and instill fear, whereas a military or intelligence attack is designed to extract secret information.

Grudge attacks are attacks that are carried out to damage an organization or a person. The damage could be in the loss of information or information processing capabilities or harm to the organization or a person’s reputation. The motivation behind a grudge attack is usually a feeling of resentment.

Thrill attacks are the attacks launched only for the fun of it. Script kiddies often download programs and launch attacks against random targets.

Recently, the world has seen a rise in the field of “hacktivism.” Attackers, known as hacktivists (a combination of hacker and activist), often combine political motivations with the thrill of hacking.

**(ISC)2 Code of Ethics** is a simple code with a preamble and four canons. Ethics are simply rules of personal behavior. The (ISC)2 makes the acceptance of its Code of Ethics a requirement for certification.

* Preamble
  + Safety and welfare of society
* Canons
  + Protect society, the common good, necessary public trust and confidence, and the infrastructure.
  + Act honorably, honestly, justly, responsibly, and legally.
  + Provide diligent and competent service to principals.
  + Advance and protect the profession.