Internet Forensics

Internet forensics is the application of scientific and legally sound methods for the investigation of Internet crimes, whose focus ranges from an individual system to the Internet at large. The computer forensics expert works on a different level than the person he or she is investigating. Internet forensics experts use different tools and engage in the same set of activities as the person he or she is investigating. Internet forensics experts use a combination of advanced computing techniques and human intuition to uncover clues about people and computers involved in Internet crime. In Internet forensics, it is usually the case that forensics experts go through the same level of education and training as the hacker, but the difference is one of morals, not skill. Computer forensics deals with physical things, while Internet forensics deals with ephemeral factors. Something that is ephemeral is transient or short lived in nature, as in network evidence, or ephemeral ports (ports above the well-known ports [0–1023] that are temporarily assigned for application communication).

Why Internet Forensics?

The large-scale and unregulated nature of the Internet provides a breeding ground for all kinds of scams and schemes. The purpose of Internet forensics is to uncover the origins of the spammers, con artists, and identity thieves that plague the Internet. Internet forensics techniques aid in unearthing the information that lies hidden in every e-mail message, Web page, and Web server on the Internet.

Internet forensics procedures are necessary because underlying Internet protocols were not designed to address the problems that complicate the process of identifying real sources of Internet crime. It is difficult to verify the source of a message or the operator of a Web site. Electronic evidence is fragile in nature and requires expert handling.

Goals of Investigation

The following are the goals of Internet forensic investigations:

- To ensure that all applicable logs and evidence are preserved
- To understand how the intruder is entering the system
- To discover why the intruder has chosen the target machine
- To gather as much evidence of the intrusion as possible
- To obtain information that may narrow the list of suspects
- To document the damage caused by the intruder
- To gather enough information to decide if law enforcement should be involved

Steps for Investigating Internet Crime

The following are the steps involved in investigating Internet crime:

1. Obtain a search warrant and seize the victim’s equipment.
2. Interview the victim.
3. Prepare bit-stream copies.
4. Identify the victim’s configuration.
5. Acquire the evidence.
6. Examine and analyze the evidence.
7. Generate a report.

Obtain a Search Warrant

The search warrant application should describe clearly that the investigators are to perform an on-site examination of the computer and network devices. The warrant needs to permit the seizure of all devices suspected to have been used in the crime, including the following:

- Victim’s equipment
- Router