Steps for Investigating Internet Crime

Investigators should perform forensic examinations on all equipment permitted in the search warrant.

**Interview the Victim**

Investigators need to interview the victim about the incident. While interviewing the victim, the investigator should ask the following questions:

- What incident occurred?
- How did the intruder get into the network?
- What was the purpose of the attack?
- What are the major losses from this incident?

**Prepare Bit-Stream Copies**

Investigators need to prepare bit-stream copies of all storage devices attached to the affected computer, using a tool such as SafeBack. Investigators should never directly work on original copies of evidence.

**Check the Logs**

Investigators need to remember to do the following when checking logs:

- Check the offsite or remote logs.
- Check the system, e-mail and Web server, and firewall log files.
- Check log files of chat sessions if the attacker monitored or had conversations with the victim through IRC services.

**Identify the Source of the Attack**

Investigators need to trace the source of the attack. The following are some of the possible initial sources:

- Web site
- E-mail address

**IP Addresses**

Each computer on the Internet has a unique IP address. Information is transmitted using the TCP/IP protocol suite. An IP address is a 32-bit integer value that is divided into four 8-bit integers separated by periods, as depicted in Figure 6-1. Each number is in the range from 0 to 255; these numbers can be used in different ways to identify the particular network and particular host on that network. An example of an IP address is 255.21.168.5.

The Internet Assigned Numbers Authority (IANA) allocates blocks of addresses to Regional Internet Registries (RIRs). The following are the five RIRs in the world:

- ARIN (American Registry for Internet Numbers)
- APNIC (Asia Pacific Network Information Centre)
- RIPE NCC (Réseaux IP Européens Network Coordination Centre)
- LACNIC (Latin American and Caribbean Internet Addresses Registry)
- AfriNIC (African Region Internet Registry)

Each of these RIRs doles out subblocks of IP addresses to the national registries and Internet service providers (ISP). They assign smaller blocks of addresses to smaller ISPs and single IP addresses to personal computers. The following are the four different classes of IP addresses:

1. **Class A**: This class is for large networks with many devices. It supports 16 million computers on each of 126 networks. The class A address range is from 10.0.0.0 to 10.255.255.255.