Access the Router

A router needs to be accessed to acquire information and evidence related to the incident. An investigator must be careful while accessing the router because critical information can be lost if the router is not accessed properly. There are certain points that should be kept in mind while accessing the router.

The following guidelines should be followed:

- The router must be accessed through the console. It must not be accessed through the network.
- Record the entire console session.
- Record the actual time and the router time.
- Only show commands should be executed. Configuration commands must not be executed, as they may change the state of the router and complicate issues for the investigator.
- Volatile information must be given priority over persistent data, as volatile information is temporary in nature and can be destroyed easily.

Gather Volatile Evidence

Volatile evidence is evidence that can easily be lost during the course of a normal investigation. It must be given priority while accessing a router for investigative purposes. It is temporary in nature and can be lost at any time. Therefore, the investigator should take steps to gather it at the earliest opportunity.

The following items are considered volatile evidence:

- Current configuration
- Access list
- Time
- Log files

Volatile evidence can be collected in the following two ways:

- Direct access
- Indirect access

Direct Access

Direct access is carried out using show commands. The router is accessed directly through the router console. Some of the show commands (along with accompanying output for some) are as follows:

- show clock detail
  
  10:27:46.089 PST Wed Dec 25 2004

- show version

  Cisco Internetwork Operating System Software
  IOS (tm) 7000 Software (C7000-JS-M), Version 11.2(21), RELEASE SOFTWARE (fc1)
  Copyright (c) 1986-1999 by cisco Systems, Inc.
  Compiled Wed 15-Dec-99 23:44 by ccai
  Image text-base: 0x00001000, data-base: 0x008F86E8
  ROM: System Bootstrap, Version 11.2(3), SOFTWARE
  ROM: 7000 Software (C7000-AJSV-M), Version 11.2(3), RELEASE SOFTWARE (fc2)
  Router uptime is 1 hour, 38 minutes
  System restarted by power-on at 15:19:36 MEST Tue Apr 25 2000
  System image file is "c7000-js-mz_112-21.bin", booted via tftp from 172.17.240.250
  cisco RP1 (68040) processor (revision C0) with 65536K bytes of memory.
  Processor board ID 0025A50A
  G.703/E1 software, Version 1.0.
  SuperLAT software copyright 1990 by Meridian Technology Corp.