Guide to Computer Forensics and Investigations Third Edition

Chapter 11
Network Forensics

Objectives

- Describe the importance of network forensics
- Explain standard procedures for performing a live acquisition
- Explain standard procedures for network forensics
- Describe the use of network tools

Network Forensics Overview

- **Network forensics**
  - Systematic tracking of incoming and outgoing traffic
    - To ascertain how an attack was carried out or how an event occurred on a network
- Intruders leave trail behind
- Determine the cause of the abnormal traffic
  - Internal bug
  - Attackers

Securing a Network

- **Layered network defense strategy**
  - Sets up layers of protection to hide the most valuable data at the innermost part of the network
- **Defense in depth (DiD)**
  - Similar approach developed by the NSA
  - Modes of protection
    - People
    - Technology
    - Operations

Securing a Network (continued)

- Testing networks is as important as testing servers
- You need to be up to date on the latest methods intruders use to infiltrate networks
  - As well as methods internal employees use to sabotage networks

Performing Live Acquisitions

- Live acquisitions are especially useful when you’re dealing with active network intrusions or attacks
- Live acquisitions done before taking a system offline are also becoming a necessity
  - Because attacks might leave footprints only in running processes or RAM
- Live acquisitions don’t follow typical forensics procedures
- **Order of volatility (OOV)**
  - How long a piece of information lasts on a system

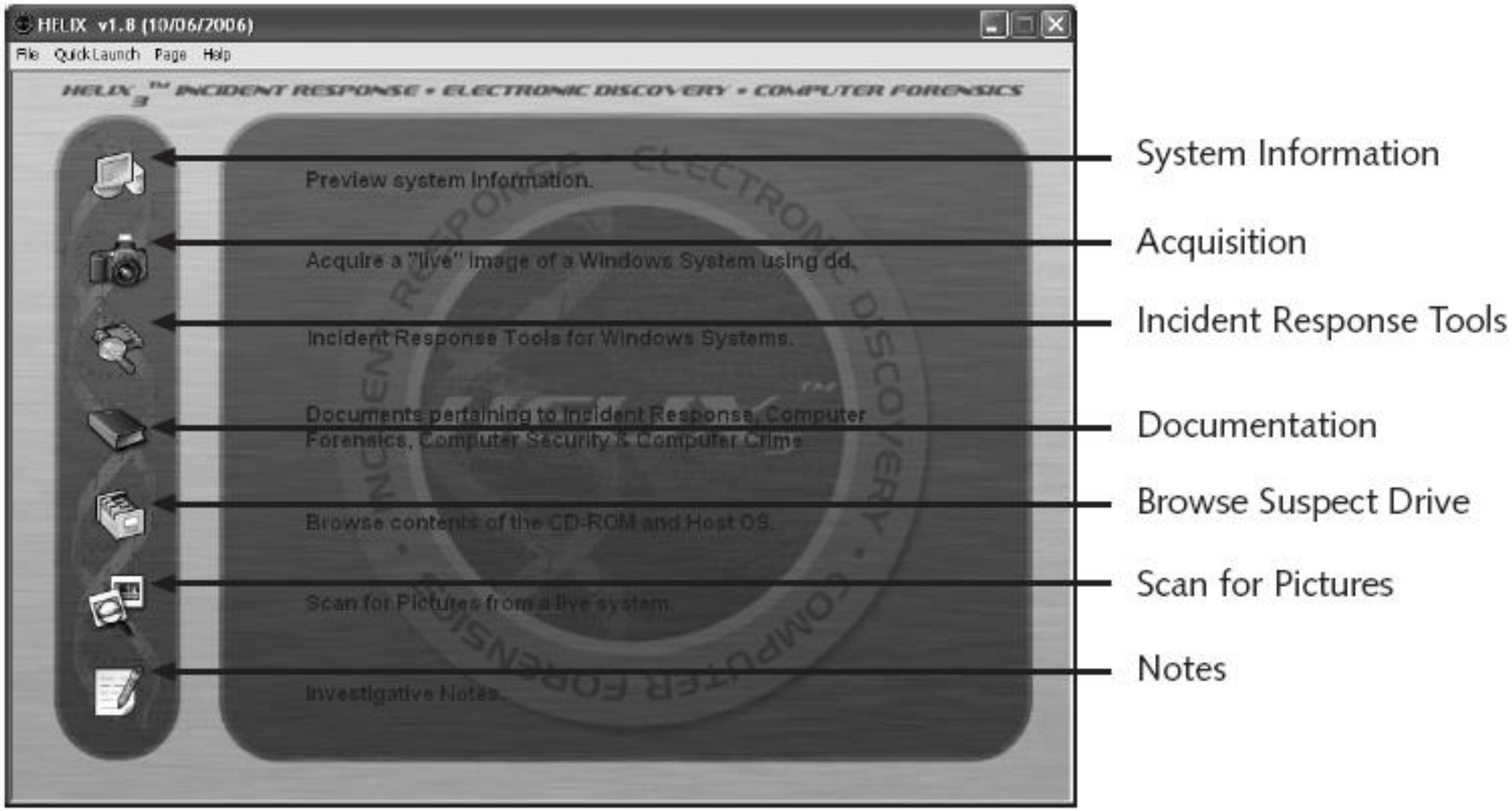
Performing Live Acquisitions (continued)

- Steps
  - Create or download a bootable forensic CD
  - Make sure you keep a log of all your actions
  - A network drive is ideal as a place to send the information you collect
  - Copy the physical memory (RAM)
  - The next step varies, depending on the incident you’re investigating
  - Be sure to get a forensic hash value of all files you recover during the live acquisition

Performing a Live Acquisition in Windows

- Several bootable forensic CDs are available
  - Such as Helix (now commercial) and DEFT
- Helix operates in two modes:
  - Windows Live (GUI or command line) and bootable Linux
- The Windows Live GUI version includes a runtime prompt for accessing the command line
- GUI tools are easy to use, but resource intensive

Performing a Live Acquisition in Windows (continued)



Preview system Information.

Acquire a "live" image of a Windows System using dd.

Incident Response Tools for Windows Systems.

Documents pertaining to Incident Response, Computer Forensics, Computer Security & Computer Crime

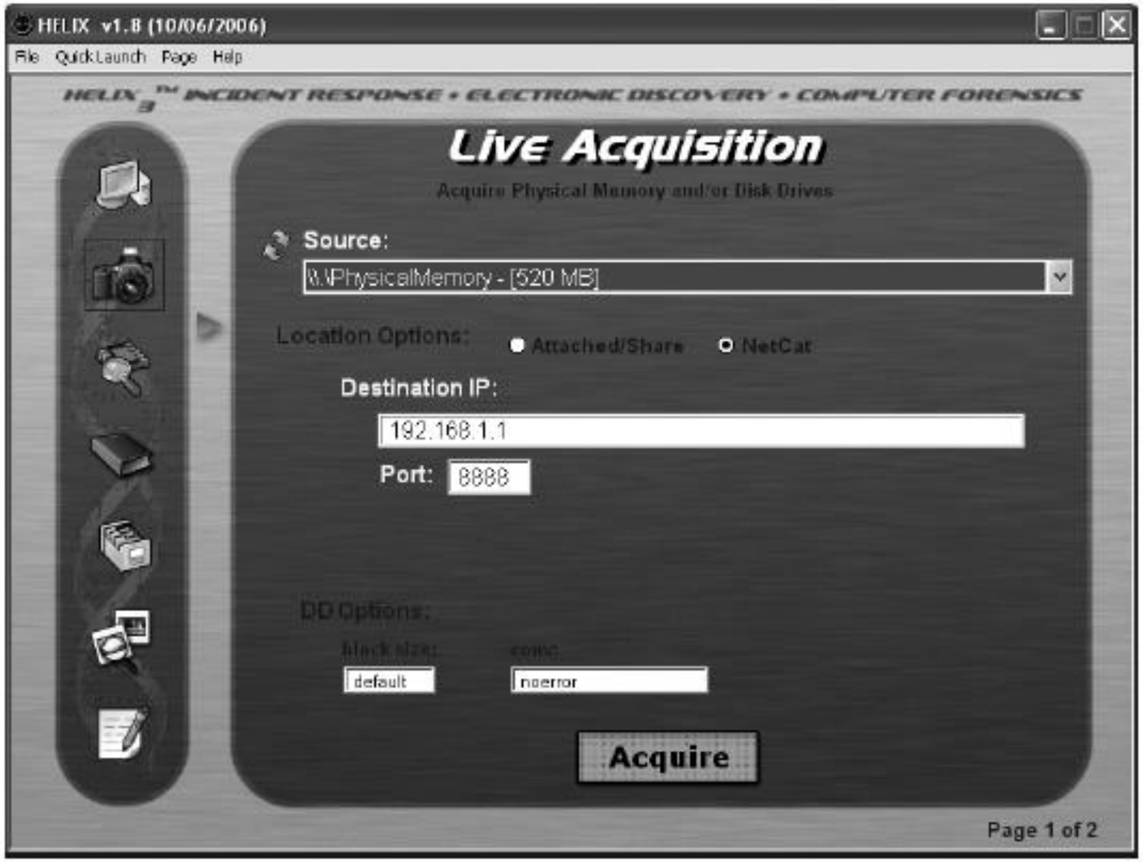
Browse contents of the CD-ROM and Host OS.

Scan for Pictures from a live system.

Investigative Notes.

Figure 11-1 The opening window in Helix

Performing a Live Acquisition in Windows (continued)


HELIX v1.8 (10/06/2006)
File QuickLaunch Page Help
HELIX 3 TM INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Live Acquisition
Acquire Physical Memory and/or Disk Drives

Source: \\.\PhysicalMemory - [520 MB]

Location Options: ○ Attached/Share ● NetCat

Destination IP: 192.168.1.1

Port: 8888

DD Options:

block size: default

conv: noerror

Figure 11-2 Live acquisition of physical memory in Helix

Developing Standard Procedures for Network Forensics

- Long, tedious process
- Standard procedure
  - Always use a standard installation image for systems on a network
  - Close any way in after an attack
  - Attempt to retrieve all volatile data
  - Acquire all compromised drives
  - Compare files on the forensic image to the original installation image

Developing Standard Procedures for Network Forensics (continued)

- Computer forensics
  - Work from the image to find what has changed
- Network forensics
  - Restore drives to understand attack
  - Often can boot image to VM and scan for intrusion
- Work on an isolated system
  - Prevents **malware** from affecting other systems

Reviewing Network Logs

- Record ingoing and outgoing traffic
  - Network servers
  - Routers
  - Firewalls
- Tcpdump tool for examining network traffic
  - Can generate top 10 lists
  - Can identify patterns
- Attacks might include other companies
  - Do not reveal information discovered about other companies

Using Network Tools

http://technet.microsoft.com/en-us/sysinternals/default.aspx

- Sysinternals
  - A collection of free tools for examining Windows products
- Examples of the Sysinternals tools:
  - RegMon shows Registry data in real time
  - Process Explorer shows what is loaded
  - Handle shows open files and processes using them
  - Filemon shows file system activity
  - Disk2vhd creates VHD from running machine

Using Network Tools (continued)

- Tools from PsTools suite created by Sysinternals
  - PsExec runs processes remotely
  - PsGetSid displays security identifier (SID)
  - PsKill kills process by name or ID
  - PsList lists details about a process
  - PsLoggedOn shows who’s logged locally
  - PsPasswd changes account passwords
  - PsService controls and views services
  - PsShutdown shuts down and restarts PCs
  - PsSuspend suspends processes

Using UNIX/Linux Tools

- http://s-t-d.org/
- Knoppix Security Tools Distribution (STD)
  - Bootable Linux CD intended for computer and network forensics
- Knoppix-STD tools
  - Dcfldd, the U.S. DoD dd version
  - memfetch forces a memory dump
  - photorec grabs files from a digital camera
  - snort, an intrusion detection system
  - oinkmaster helps manage your snort rules

Using UNIX/Linux Tools (continued)

- Knoppix-STD tools (continued)
  - john
  - chntpw resets passwords on a Windows PC
  - tcpdump and ethereal are packet sniffers
- With the Knoppix STD tools on a portable CD
  - You can examine almost any network system

Using UNIX/Linux Tools (continued)

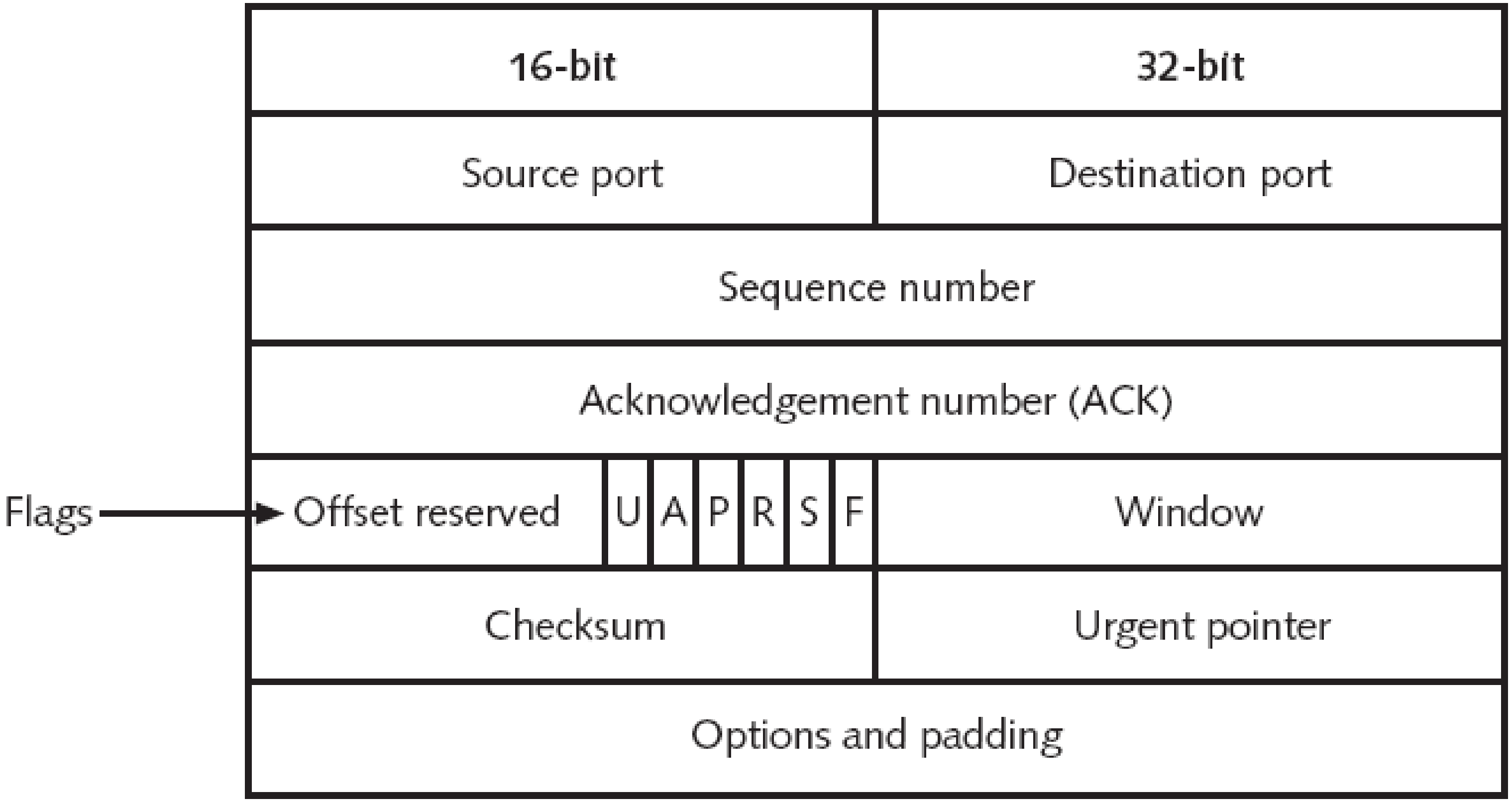
- http://remote-exploit.org/
- BackTrack
  - Top rated Linux live distribution focused on penetration testing
  - Based on Whax and Auditor and contains more than 300 tools for network scanning, brute-force attacks, Bluetooth and wireless networks, and more
  - Includes 24 tools specifically for forensics, such as Autopsy and Sleuth
  - Easy to use and frequently updated

Using Packet Sniffers

- Packet sniffers
  - Devices or software that monitor network traffic
  - Most work at layer 2 or 3 of the OSI model
- Most tools follow the PCAP format
- Some packets can be identified by examining the flags in their TCP headers
- Tools
  - Tcpdump, Ethereal / Wireshark

http://www.lenholgate.com/archives/000638.html

Using Packet Sniffers (continued)



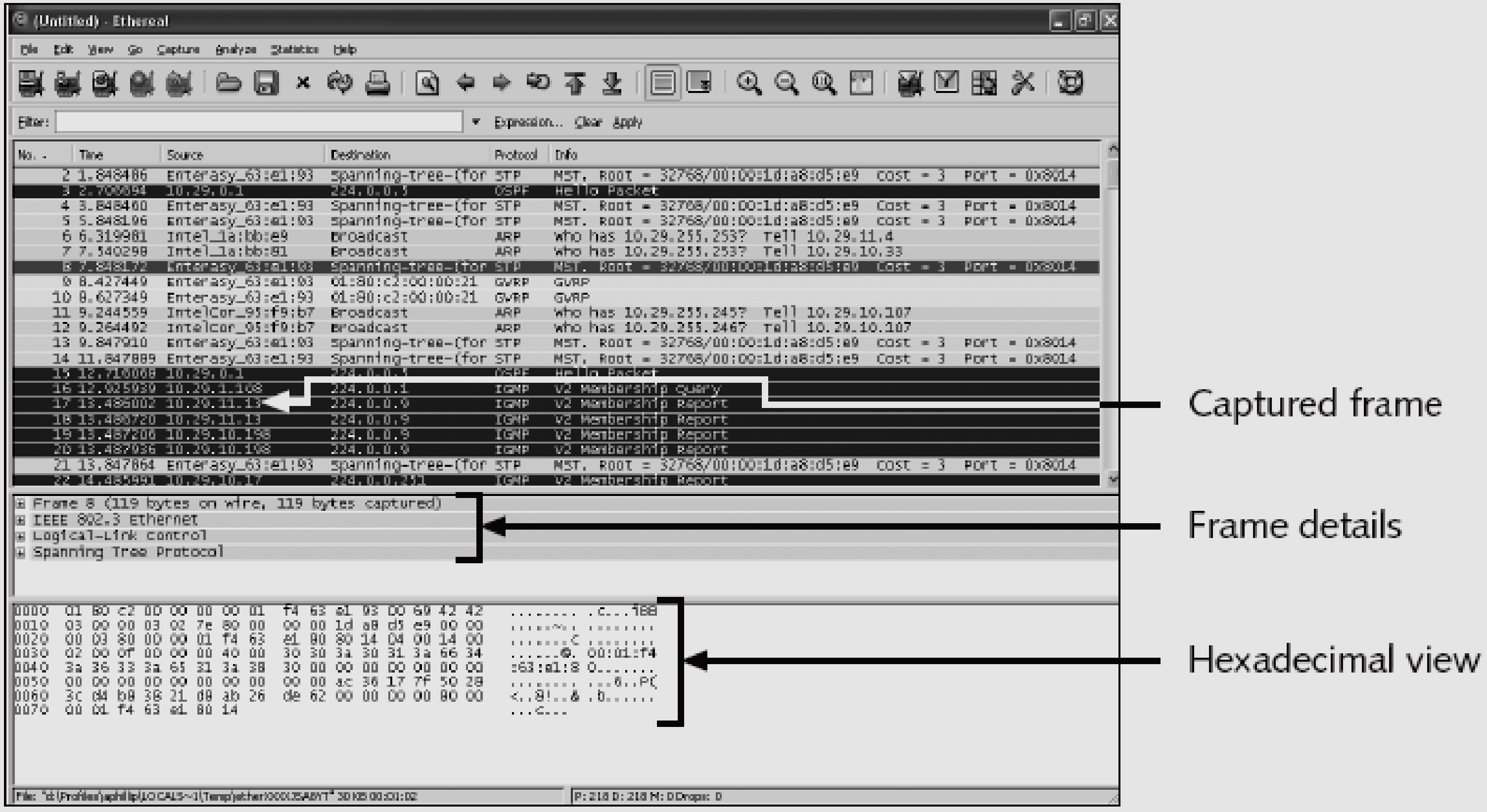
<table>
<tr><th colspan="7">16-bit</th><th>32-bit</th></tr>
<tr><td colspan="7">Source port</td><td>Destination port</td></tr>
<tr><td colspan="8">Sequence number</td></tr>
<tr><td colspan="8">Acknowledgement number (ACK)</td></tr>
<tr><td>Offset reserved</td><td>U</td><td>A</td><td>P</td><td>R</td><td>S</td><td>F</td><td>Window</td></tr>
<tr><td colspan="7">Checksum</td><td>Urgent pointer</td></tr>
<tr><td colspan="8">Options and padding</td></tr>
</table>

Figure 11-7 A TCP header

Using Packet Sniffers (continued)

- http://www.cacetech.com/products/network_toolkit_tools.html
- Snort
- Tcpslice
- Tcpreplay
- Tcpdstat
- Ngrep
- Etherape
- Netdude
- Argus
- Ethereal / Wireshark

Using Packet Sniffers (continued)


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
Captured frame
Frame details
Hexadecimal view

```
No. -  Time       Source              Destination          Protocol Info
     2 1.848486   Enterasy_63:e1:93   Spanning-tree-(for   STP      MST. Root = 32768/00:00:1d:a8:d5:e9  Cost = 3  Port = 0x8014
     3 2.709694   10.29.0.1           224.0.0.5            OSPF     Hello Packet
     4 3.848460   Enterasy_63:e1:93   Spanning-tree-(for   STP      MST. Root = 32768/00:00:1d:a8:d5:e9  Cost = 3  Port = 0x8014
     5 5.848196   Enterasy_63:e1:93   Spanning-tree-(for   STP      MST. Root = 32768/00:00:1d:a8:d5:e9  Cost = 3  Port = 0x8014
     6 6.319981   Intel_1a:bb:e9      Broadcast            ARP      Who has 10.29.255.253?  Tell 10.29.11.4
     7 7.340298   Intel_1a:bb:81      Broadcast            ARP      Who has 10.29.255.253?  Tell 10.29.10.33
     8 7.848172   Enterasy_63:e1:93   Spanning-tree-(for   STP      MST. Root = 32768/00:00:1d:a8:d5:e9  Cost = 3  Port = 0x8014
     9 8.427449   Enterasy_63:e1:93   01:80:c2:00:00:21    GVRP     GVRP
    10 8.627349   Enterasy_63:e1:93   01:80:c2:00:00:21    GVRP     GVRP
    11 9.244559   IntelCor_95:f9:b7   Broadcast            ARP      Who has 10.29.255.245?  Tell 10.29.10.107
    12 9.264492   IntelCor_95:f9:b7   Broadcast            ARP      Who has 10.29.255.246?  Tell 10.29.10.107
    13 9.847910   Enterasy_63:e1:93   Spanning-tree-(for   STP      MST. Root = 32768/00:00:1d:a8:d5:e9  Cost = 3  Port = 0x8014
    14 11.847889  Enterasy_63:e1:93   Spanning-tree-(for   STP      MST. Root = 32768/00:00:1d:a8:d5:e9  Cost = 3  Port = 0x8014
    15 12.710068  10.29.0.1           224.0.0.5            OSPF     Hello Packet
    16 12.925939  10.29.1.108         224.0.0.1            IGMP     V2 Membership Query
    17 13.486002  10.29.11.13         224.0.0.9            IGMP     V2 Membership Report
    18 13.486720  10.29.11.13         224.0.0.9            IGMP     V2 Membership Report
    19 13.487206  10.29.10.198        224.0.0.9            IGMP     V2 Membership Report
    20 13.487936  10.29.10.198        224.0.0.9            IGMP     V2 Membership Report
    21 13.847864  Enterasy_63:e1:93   Spanning-tree-(for   STP      MST. Root = 32768/00:00:1d:a8:d5:e9  Cost = 3  Port = 0x8014
    22 14.485991  10.29.10.17         224.0.0.251          IGMP     V2 Membership Report
```

```
⊞ Frame 8 (119 bytes on wire, 119 bytes captured)
⊞ IEEE 802.3 Ethernet
⊞ Logical-Link Control
⊞ Spanning Tree Protocol
```

```
0000  01 80 c2 00 00 00 00 01  f4 63 e1 93 00 69 42 42   ........ .c...iBB
0010  03 00 00 03 02 7e 80 00  00 00 1d a8 d5 e9 00 00   .....~.. ........
0020  00 03 80 00 00 01 f4 63  e1 80 80 14 04 00 14 00   .......c ........
0030  02 00 0f 00 00 00 40 00  30 30 3a 30 31 3a 66 34   ......@. 00:01:f4
0040  3a 36 33 3a 65 31 3a 38  30 00 00 00 00 00 00 00   :63:e1:8 0.......
0050  00 00 00 00 00 00 00 00  00 00 ac 36 17 7f 50 28   ........ ...6..P(
0060  3c d4 b8 38 21 d8 ab 26  de 62 00 00 00 00 80 00   <..8!..& .b......
0070  00 01 f4 63 e1 80 14                               ...c...
```

```
File: "C:\Profiles\aphilip\LOCALS~1\Temp\etherXXXXJSABYT" 30 KB 00:01:02    P: 218 D: 218 M: 0 Drops: 0
```

Figure 11-8 Ethereal in a Windows environment

Summary

- Network forensics tracks down internal and external network intrusions
- Networks must be hardened by applying layered defense strategies to the network architecture
- Live acquisitions are necessary to retrieve volatile items
- Standard procedures need to be established for how to proceed after a network security event has occurred

Summary (continued)

- By tracking network logs, you can become familiar with the normal traffic pattern on your network
- Network tools can monitor traffic on your network, but they can also be used by intruders
- Bootable Linux CDs, such as Knoppix STD, BackTrack and Helix, can be used to examine Linux and Windows systems