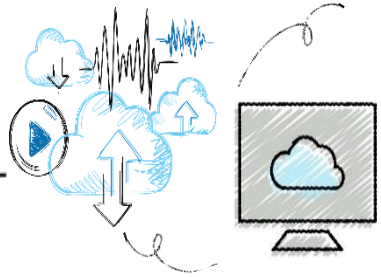
Guide to Computer Forensics and Investigations Sixth Edition

Chapter 10

Virtual Machine Forensics, Live Acquisitions, and Network Forensics



CENGAGE

Objectives

- Explain standard procedures for conducting forensic analysis of virtual machines
- Describe the process of a live acquisition
- Explain network intrusions and unauthorized access
- Describe standard procedures in network forensics and network-monitoring tools

An Overview of Virtual Machine Forensics (1 of 2)

- Virtual machines are common for both personal and business use
- Investigators need to know how to analyze them and use them to analyze other suspect drives
- The software that runs virtual machines is called a “hypervisor”
- Two types of **hypervisor**:
  - **Type 1** - loads on physical hardware and doesn’t require a separate OS
  - **Type 2** - rests on top of an existing OS

An Overview of Virtual Machine Forensics (2 of 2)

- Type 2 hypervisors are usually the ones you find loaded on a suspect machine
- Type 1 hypervisors are typically loaded on servers or workstations with a lot of RAM and storage

Type 2 Hypervisors (1 of 4)

- Before installing a type 2 hypervisor, enable virtualization in the BIOS before attempting to create a VM
- **Virtualization Technology (VT)** - Intel's CPU design for security and performance enhancements that enable the BIOS to support virtualization
- **Virtualization Machine Extensions (VMX)** - instruction sets created for Intel processors to handle virtualization

Type 2 Hypervisors (2 of 4)

- Most widely used type 2 hypervisors:
  - Parallels Desktop - created for Macintosh users who also use Windows applications
  - KVM (Kernel-based Virtual Machine) - for Linux OS
  - Microsoft Hyper-V - new hypervisor built into Windows 10
  - VMware Workstation and Player - can be installed on almost any device, including tablets
    - Can install Microsoft Hyper-V Server on it
    - Can create encrypted VMs
    - Can support up to 16 CPUs, 8 TB storage, and 20 VM

Type 2 Hypervisors (3 of 4)

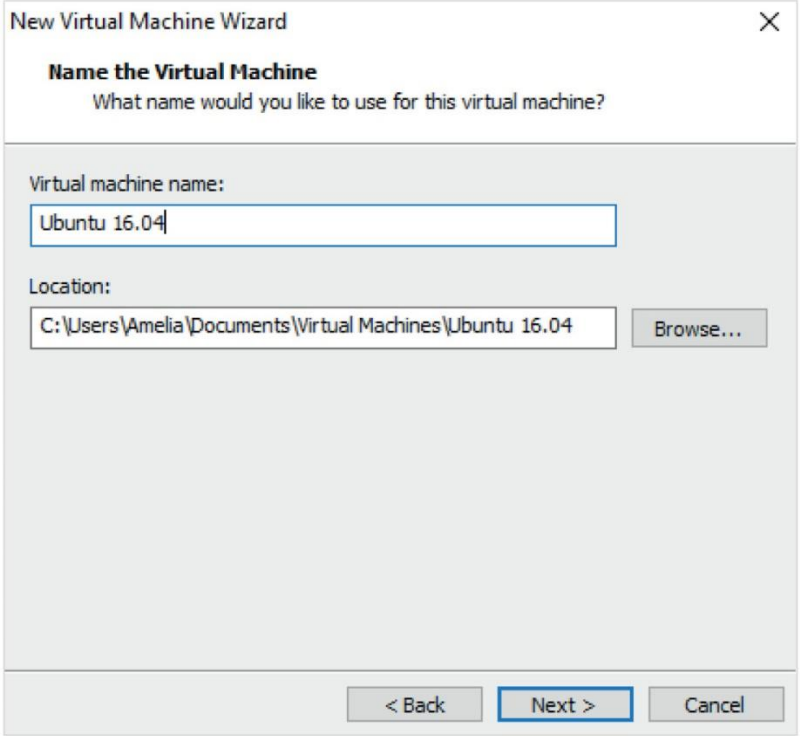


Figure 10-2 The default location of VMware Workstation Player files

Source: VMware, *www.vmware.com*

Type 2 Hypervisors (4 of 4)

- Most widely used type 2 hypervisors (cont'd):
  - VirtualBox - supports all Windows and Linux OSs as well as Macintosh and Solaris
    - Allows selecting types associated with other applications, such as VMware VMDK type or the Parallels HDD type
- Type 2 hypervisors come with templates for different OSs

Conducting an Investigation with Type 2 Hypervisors (1 of 9)

- Begin by acquiring a forensic image of the host computer as well as network logs
  - By linking the VM's IP address to log files, you may determine what Web sites the VM accessed
- To detect whether a VM is on a host computer:
  - Look in the Users or Documents folder (in Windows) or user directories (in Linux)
  - Check the host's Registry for clues that VMs have been installed or uninstalled
  - Existence of a virtual network adapter

Conducting an Investigation with Type 2 Hypervisors (2 of 9)

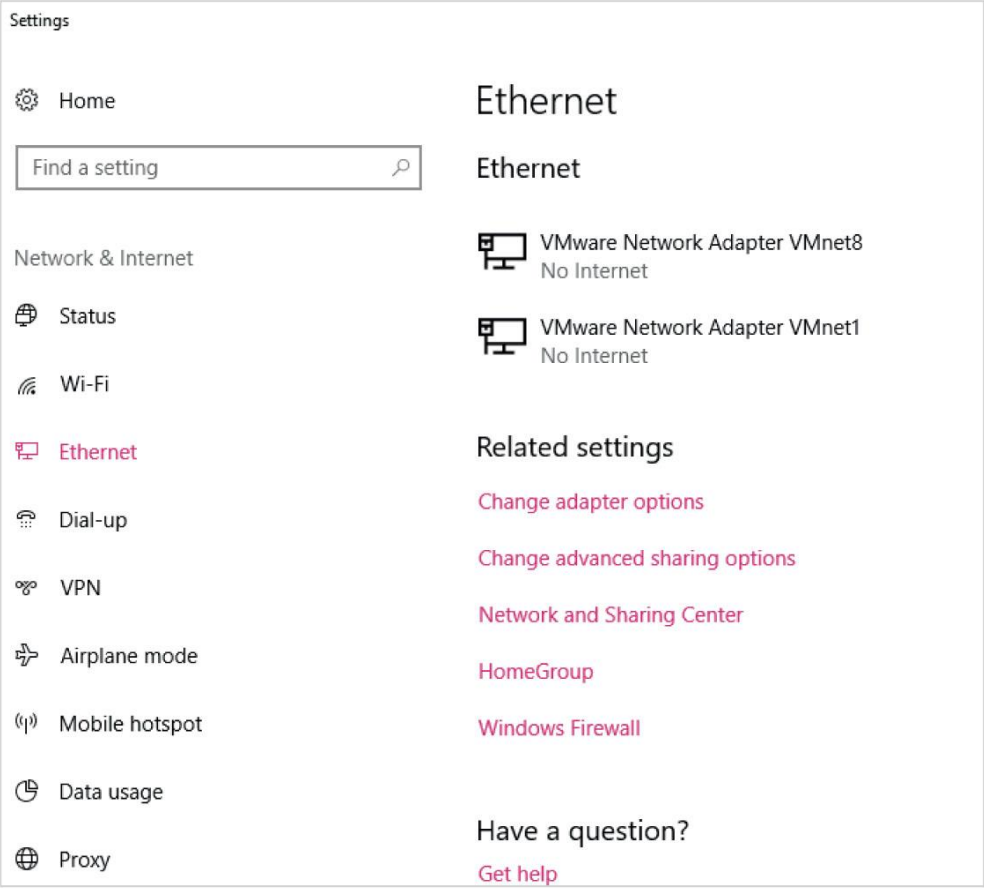


Figure 10-7 Ethernet Connections on a Windows 10 computer

Conducting an Investigation with Type 2 Hypervisors (3 of 9)

- In addition to searching for network adapters, you need to determine whether USB drives have been attached to the host
  - They could have live VMs running on them
- A VM can also be nested inside other VMs on the host machine or a USB drive
  - Some newer Windows systems log when USB drives are attached
  - Search the Windows Registry or the system log files

Conducting an Investigation with Type 2 Hypervisors (4 of 9)

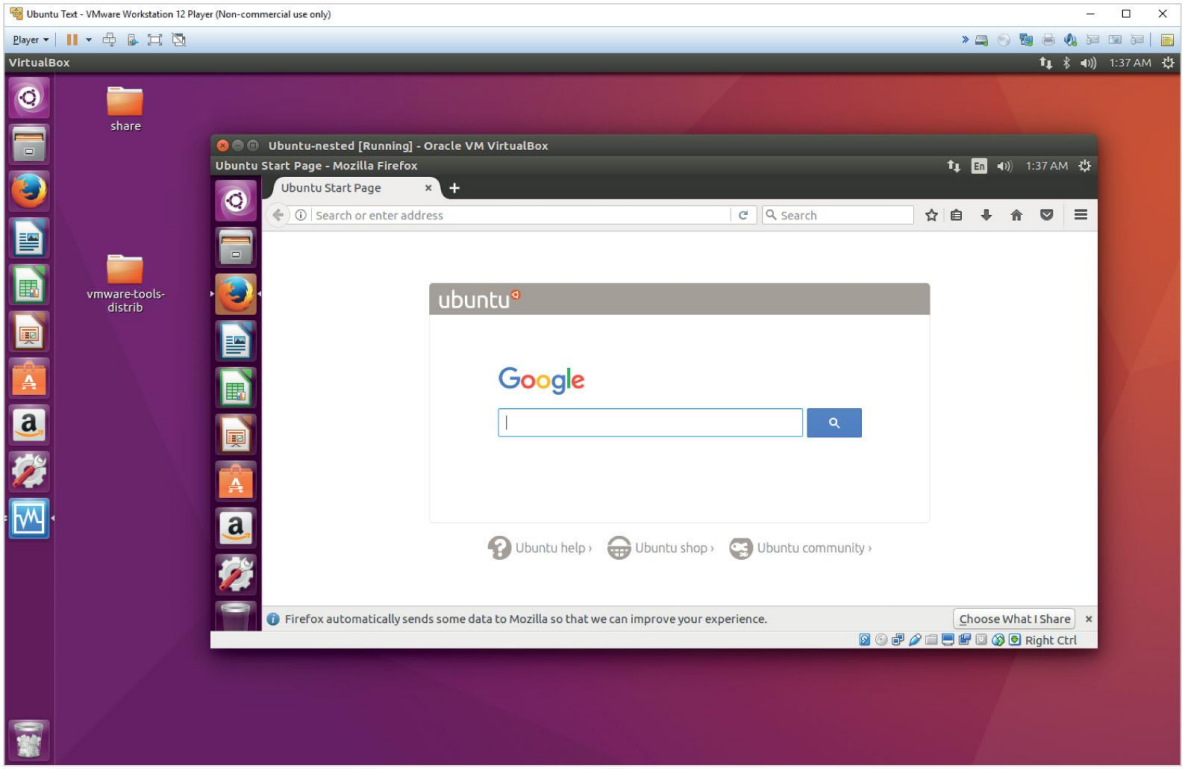


Figure 10-9 A VM nested inside another VM

Source: VMware, *www.vmware.com*

Conducting an Investigation with Type 2 Hypervisors (5 of 9)

- Follow a consistent procedure:
  - 1. Image the host machine
  - 2. Locate the virtualization software and VMs, using information learned about file extensions and network adapters
  - 3. Export from the host machine all files associated with VMs
  - 4. Record the hash values of associated files
  - 5. Open a VM as an image file in forensics software and create a forensic image or mount the VM as a drive

Conducting an Investigation with Type 2 Hypervisors (6 of 9)

- Live acquisitions of VMs are often necessary
  - They include all snapshots, which records the state of a VM at a particular moment (records only changes in state, not a complete backup)
- When acquiring an image of a VM file, snapshots might not be included
  - In this case, you have only the original VM
- Doing live acquisitions of VMs is important to make sure snapshots are incorporated

Conducting an Investigation with Type 2 Hypervisors (7 of 9)

- Follow the steps in the activity on page 426 to see how to examine your own system for evidence of a VM
- Follow the steps starting on page 427 to acquire an image of a VM

Conducting an Investigation with Type 2 Hypervisors (8 of 9)

- Other VM Examination Methods
  - FTK Imager, Magnet AXIOM and OSForensics can mount VMs as an external drive
    - By mounting a VM as a drive, you can make it behave more like a physical computer
    - Allows you to use the same standard examination procedures for a static hard drive
  - Make a copy of a VM's forensic image and open the copy while it's running
    - Start it as a live VM so that forensics software can be used to search for clues

Conducting an Investigation with Type 2 Hypervisors (9 of 9)

- Using VMs as Forensic Tools
  - Investigators can use VMs to run forensics tools stored on USB drives
- Follow steps starting on page 430 to see how to set up a VM on a USB drive

Working with Type 1 Hypervisors (1 of 2)

- This section is meant to help you understand the impact Type 1 hypervisors have on forensic investigations
  - Having a good working relationship with network administrators and lead technicians can be helpful
- Type 1 hypervisors are installed directly on hardware
  - Can be installed on a VM for testing purposes
  - Capability is limited only by the amount of available RAM, storage, and throughput

Working with Type 1 Hypervisors (2 of 2)

- Common type 1 hypervisors:
  - VMware vSphere
  - Microsoft Hyper-V 2016
  - XenProject XenServer
  - IBM PowerVM
  - Parallels Desktop for Mac
- Follow steps starting on page 433 to install XenServer as a VM in VirtualBox

Performing Live Acquisitions (1 of 2)

- 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
  - 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 (2 of 2)

- Steps
  - Create or download a bootable forensic CD or USB drive
  - 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 digital hash value of all files you recover during the live acquisition

Performing a Live Acquisition in Windows

- Several tools are available to capture the RAM.
  - Mandiant Memoryze
  - Belkasoft RamCapturer
  - Kali Linux (updated version of BackTrack)
- GUI tools are easy to use
  - But they often require a lot of system resources
  - Might get false readings in Windows OSs
- Command-line tools give you more control

Network Forensics Overview

- **Network forensics**
  - Process of collecting and analyzing raw network data and tracking network traffic
    - To ascertain how an attack was carried out or how an event occurred on a network
- Intruders leave a trail behind
  - Knowing your network's typical traffic patterns is important in spotting variations in network traffic
- Can also help you determine whether a network is truly under attack

The Need for Established Procedures

- Network forensics examiners must establish standard procedures for how to acquire data after an attack or intrusion
  - Essential to ensure that all compromised systems have been found
- Procedures must be based on an organization's needs and complement network infrastructure
- NIST created "Guide to Integrating Forensic Techniques into Incident Response" to address these needs

Securing a Network (1 of 2)

- **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 (2 of 2)

- 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
- Small companies of fewer than 10 employees often don't consider security precautions against internal threats necessary
  - Can be more susceptible to problems caused by employees revealing proprietary information

Developing Procedures for Network Forensics (1 of 2)

- Network forensics can be a long, tedious process
- Standard procedure that is often used:
  - Always use a standard installation image for systems on a network
  - Fix any vulnerability 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 Procedures for Network Forensics (2 of 2)

- In digital forensics
  - You can work from the image to find most of the deleted or hidden files and partitions
- In network forensics
  - You have to restore drives to understand attack

Reviewing Network Logs

- Network logs record ingoing and outgoing traffic
  - Network servers
  - Routers
  - Firewalls
- Tcpdump and Wireshark - tools for examining network traffic
  - Can generate top 10 lists
  - Can identify patterns

Using Network Tools

- Variety of tools
  - Splunk
  - Spiceworks
  - Nagios
  - Cacti

Using Packet Analyzers (1 of 5)

- **Packet analyzers**
  - Devices or software that monitor network traffic
  - Most work at layer 2 or 3 of the OSI model
- Most tools follow the Pcap (packet capture) format
- Some packets can be identified by examining the flags in their TCP headers
- Tools
  - `Tcpdump`
  - `Tethereal`

Using Packet Analyzers (2 of 5)

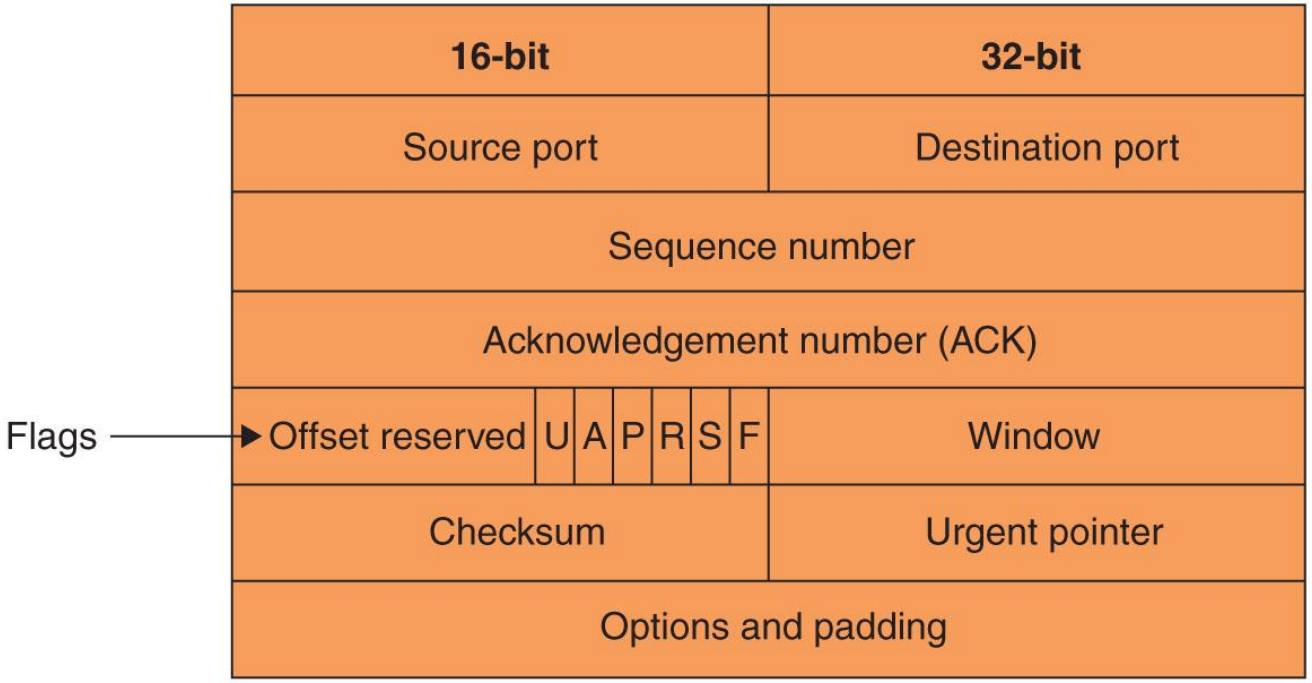


Figure 10-15 A TCP header

Using Packet Analyzers (3 of 5)

- Tools (cont'd)
  - Tcpslice
  - Tcpreplay
  - Etherape
  - Netdude
  - Argus
  - Wireshark
    - Follow the steps starting on page 442 to see how the Wireshark tool works

Using Packet Analyzers (4 of 5)

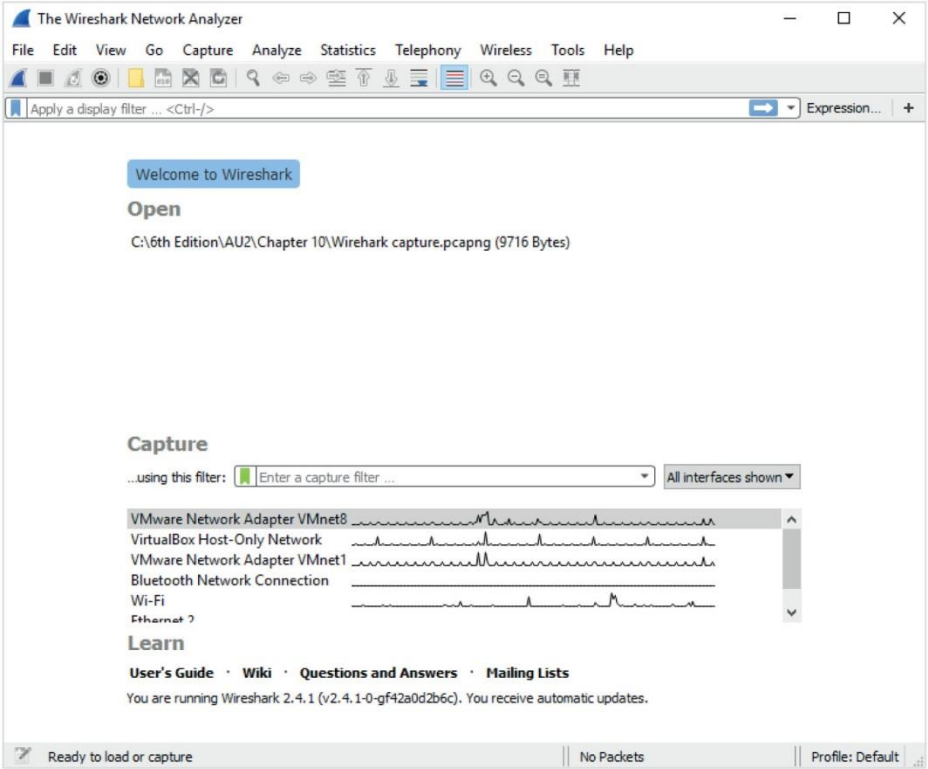
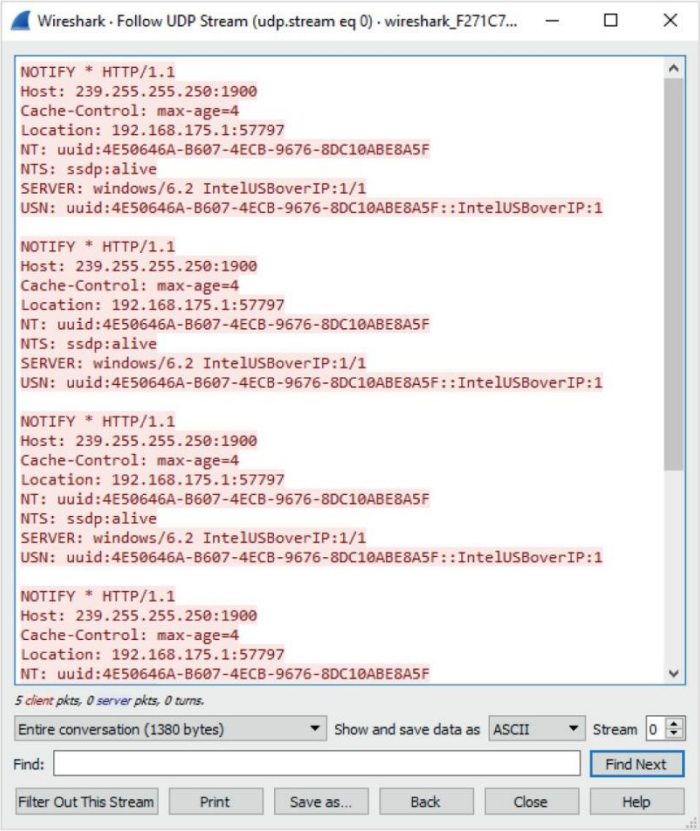


Figure 10-16 The opening window in Wireshark

Source: Wireshark Foundation, *www.wireshark.org*

Using Packet Analyzers (5 of 5)



Wireshark · Follow UDP Stream (udp.stream eq 0) · wireshark_F271C7...

```
NOTIFY * HTTP/1.1
Host: 239.255.255.250:1900
Cache-Control: max-age=4
Location: 192.168.175.1:57797
NT: uuid:4E50646A-B607-4ECB-9676-8DC10ABE8A5F
NTS: ssdp:alive
SERVER: windows/6.2 IntelUSBoverIP:1/1
USN: uuid:4E50646A-B607-4ECB-9676-8DC10ABE8A5F::IntelUSBoverIP:1

NOTIFY * HTTP/1.1
Host: 239.255.255.250:1900
Cache-Control: max-age=4
Location: 192.168.175.1:57797
NT: uuid:4E50646A-B607-4ECB-9676-8DC10ABE8A5F
NTS: ssdp:alive
SERVER: windows/6.2 IntelUSBoverIP:1/1
USN: uuid:4E50646A-B607-4ECB-9676-8DC10ABE8A5F::IntelUSBoverIP:1

NOTIFY * HTTP/1.1
Host: 239.255.255.250:1900
Cache-Control: max-age=4
Location: 192.168.175.1:57797
NT: uuid:4E50646A-B607-4ECB-9676-8DC10ABE8A5F
NTS: ssdp:alive
SERVER: windows/6.2 IntelUSBoverIP:1/1
USN: uuid:4E50646A-B607-4ECB-9676-8DC10ABE8A5F::IntelUSBoverIP:1

NOTIFY * HTTP/1.1
Host: 239.255.255.250:1900
Cache-Control: max-age=4
Location: 192.168.175.1:57797
NT: uuid:4E50646A-B607-4ECB-9676-8DC10ABE8A5F
```

5 client pkts, 0 server pkts, 0 turns.

Entire conversation (1380 bytes) Show and save data as ASCII Stream 0

Figure 10-17 Following a UDP stream

Source: Wireshark Foundation, *www.wireshark.org*

Investigating Virtual Networks

- Virtual switch is a little different from a physical switch
  - There's no spanning tree between virtual switches
- Additional complications
  - Hypervisors can assign MAC addresses to virtual devices
  - Devices can have the same MAC address on different virtual networks
  - Cloud service providers host networks for several to hundreds of companies
- Tools
  - Wireshark
  - Network Miner

Examining the Honeynet Project (1 of 2)

- The Honeynet Project was developed to make information widely available in an attempt to thwart Internet and network attackers
  - Provides information about attacks methods and how to protect against them
- Objectives are awareness, information, and tools
- **Distributed denial-of-service (DDoS) attacks**
  - A major threat that may go through other organizations' networks, not just yours
  - Hundreds or even thousands of machines (**zombies**) can be used

Examining the Honeynet Project (2 of 2)

- **Zero day attacks**
  - Another major threat
  - Attackers look for holes in networks and OSs and exploit these weaknesses before patches are available
- **Honeypot**
  - Normal looking computer that lures attackers to it
- **Honeywalls**
  - Monitor what's happening to honeypots on your network and record what attackers are doing

Summary (1 of 3)

- Virtual machines are used extensively in organizations and are a common part of forensic investigations
- There are two types of hypervisors for running virtual machines: Type 1 and Type 2
- Virtualization Technology is Intel's CPU design for security and performance enhancements that enable the BIOS to support virtualization
- Forensic procedures for VMs start by creating an image of the host machine, and then exporting files associated with a VM

Summary (2 of 3)

- Live acquisitions are necessary to retrieve volatile items, such as RAM and running processes
- Network forensics is the process of collecting and analyzing raw network data and systematically tracking network traffic to ascertain how an attack took place
- Steps must be taken to harden networks before a security breach happens
- Being able to spot variations in network traffic can help you track intrusions

Summary (3 of 3)

- Several tools are available for monitoring network traffic, such as packet analyzers and honeypots
- The Honeynet Project is designed to help people learn the latest intrusion techniques that attackers are using