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

What is Virtualization?

- To understand virtualization, let us begin with a *virtual resource*

Virtual Resources

- Definition
  - Illusion of a resource, supported by an OS through use of a real resource
- Motivation
  - To have more number of resources available
  - To have more of a resource available, e.g., virtual memory
- Historical
  - The concept originated in 1960s!

Virtual Resources

- A virtual resource is an *abstraction*
- The OS implements the abstraction through use of real resources
- The implementation can be changed without affecting the application using the virtual resource
- An application can be migrated to any host offering the same abstraction—*portability*

Virtual Resources

- Use of virtual resources started with I/O devices
  - Motivation: Have more I/O devices available
  - Each user could have own I/O device
- Then came virtual memory
  - Motivation: Have larger memory
- And then .. *Virtual machines*
  - Motivation?

Virtual Machines

- Motivation: Provide a machine to each user so that a user could use an OS of own choice

Virtual Machines

- A virtual machine could be used in other contexts as well …
  - Motivation?
    - Since it is an abstraction, it can be made to have desirable properties, e.g., simplicity
      - Some programming languages have their own virtual machines, e.g., Pascal, Java
    - If implemented on several hosts, it provides portability

Virtualization

- Virtualization -- the abstraction of computer resources.

- *Virtualization* is the process of mapping the resources and interfaces of a virtual resource into the resources and interfaces of a host machine.

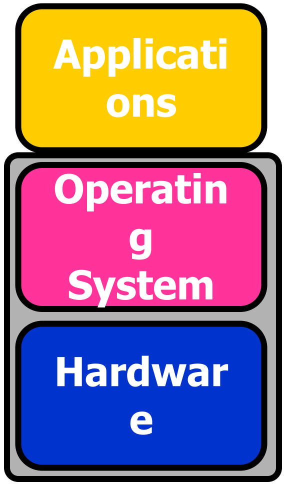
- Virtualization hides the physical characteristics of computing resources from their users, be they applications, or end users.

- This includes making a single physical resource (such as a server, an operating system, an application, or storage device) appear to function as multiple virtual resources; it can also include making multiple physical resources (such as storage devices or servers) appear as a single virtual resource.

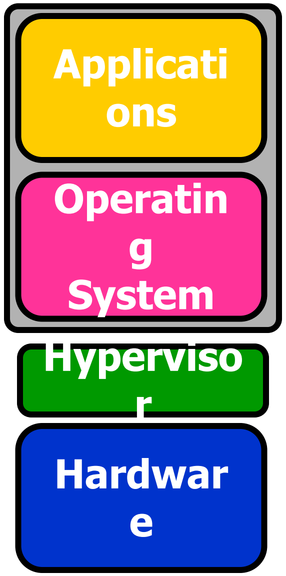
Issues in Virtualization?

- Complexity
- Correctness—includes reliability, security …
- Performance! (overhead of the mapping)

The Use of Computers



Virtualization



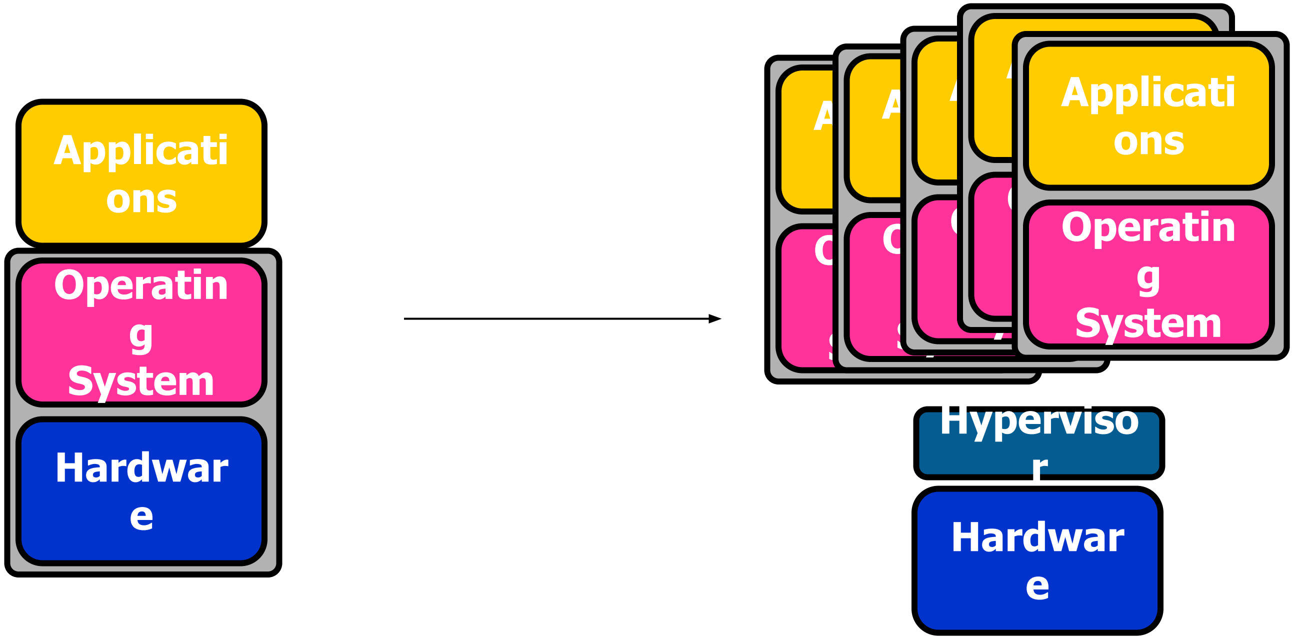
Applicati
ons

Operatin
g
System

Hyperviso
r

Hardwar
e

Virtualization -- a Server for Multiple Applications/OS

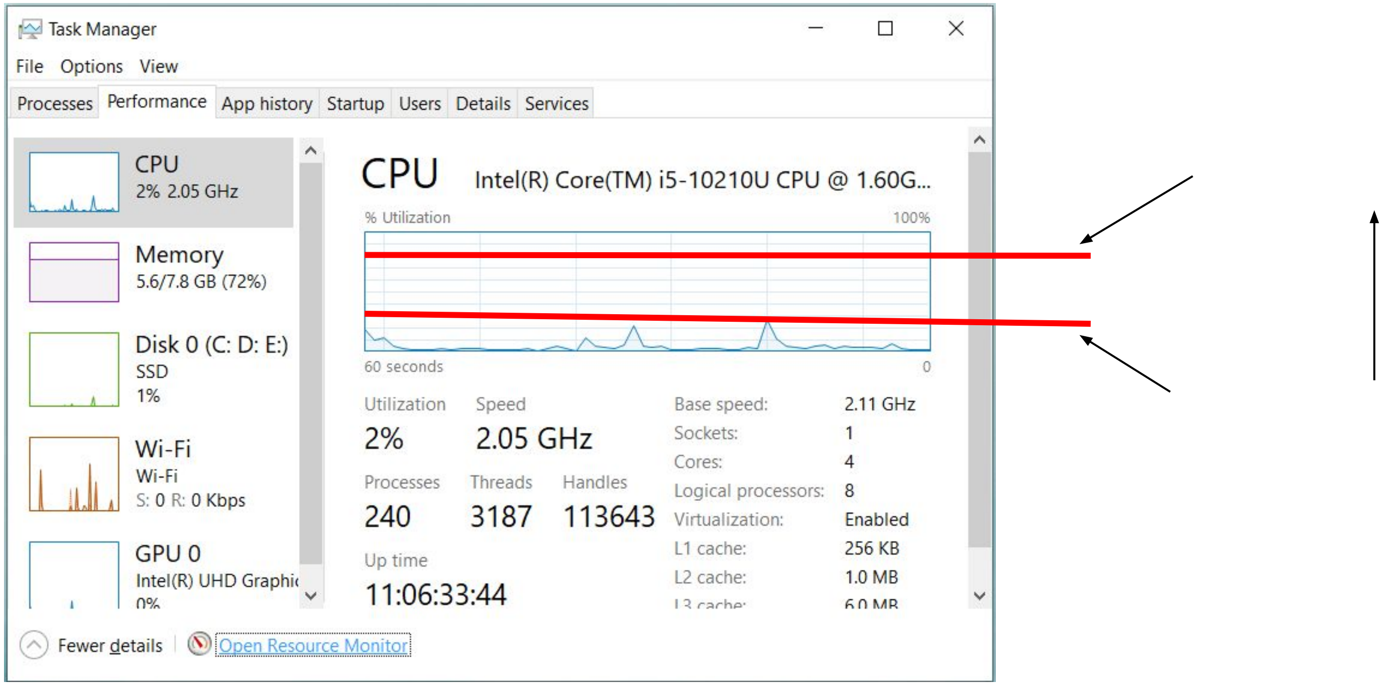


Hypervisor

virtualization

managers

Capacity Utilization



Task Manager

File Options View

Processes | Performance | App history | Startup | Users | Details | Services

CPU
2% 2.05 GHz

Memory
5.6/7.8 GB (72%)

Disk 0 (C: D: E:)
SSD
1%

Wi-Fi
Wi-Fi
S: 0 R: 0 Kbps

GPU 0
Intel(R) UHD Graphic
0%

CPU Intel(R) Core(TM) i5-10210U CPU @ 1.60G...

Utilization 2%
Speed 2.05 GHz
Processes 240
Threads 3187
Handles 113643
Up time 11:06:33:44

Base speed:	2.11 GHz
Sockets:	1
Cores:	4
Logical processors:	8
Virtualization:	Enabled
L1 cache:	256 KB
L2 cache:	1.0 MB
L3 cache:	6.0 MB

Full Virtualization

- A certain kind of virtual machine environment: one that provides a complete simulation of the underlying hardware.
- The result is a system in which all software (including all OS's) capable of execution on the raw hardware can be run in the virtual machine.
- Comprehensively simulate all computing elements as instruction set, main memory, interrupts, exceptions, and device access.
- Full virtualization is only possible given the right combination of hardware and software elements.

- Full virtualization has proven highly successful
  - Sharing a computer system among multiple users
  - Isolating users from each other (and from the control program) and
  - Emulating new hardware to achieve improved reliability, security and productivity.

Full Virtualization -- challenge

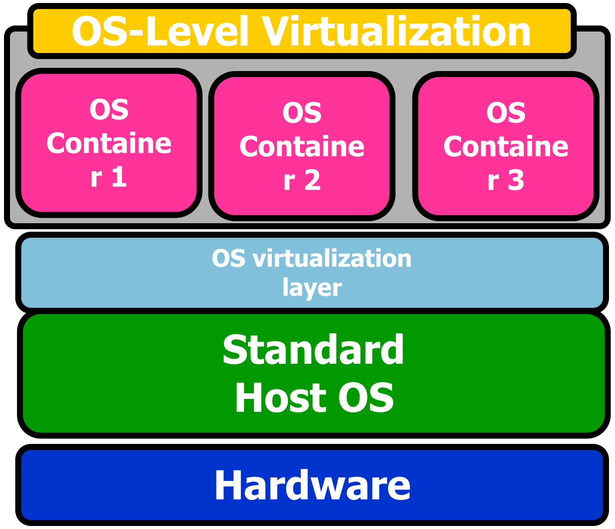
- Security issues -- Interception
- Simulation of privileged operations -- I/O instructions
- The effects of every operation performed within a given virtual machine must be kept within that virtual machine – virtual operations cannot be allowed to alter the state of any other virtual machine, the control program, or the hardware.
- Some machine instructions can be executed directly by the hardware,
  - E.g., memory locations and arithmetic registers.
- But other instructions that would "pierce the virtual machine" cannot be allowed to execute directly; they must instead be trapped and simulated. Such instructions either access or affect state information that is outside the virtual machine.
- Some hardware is not easy to be used for full virtualization, e.g., x86

OS assisted (Paravirtualization)

- Paravirtualization – via an modified OS kernel as guest OS
  - It is very difficult to build the more sophisticated binary translation support necessary for full virtualization.
  - Paravirtualization involves modifying the OS kernel to replace non-virtualizable instructions with hypercalls that communicate directly with the virtualization layer hypervisor.
  - The hypervisor also provides hypercall interfaces for other critical kernel operations such as memory management, interrupt handling and time keeping.
  - Paravirtualization is different from full virtualization, where the unmodified OS does not know it is virtualized and sensitive OS calls are trapped using binary translation.
  - Paravirtualization cannot support unmodified OS
- Example:
  - Xen -- modified Linux kernel and a version of Windows XP

OS-Level Virtualization

- OS-level virtualization
  - kernel of an OS allows for multiple isolated user-space instances, instead of just one.
  - Each OS instance looks and feels like a real server
- OS virtualization virtualizes servers on the operating system (kernel) layer. This creates isolated containers on a single physical server and OS instance to utilize hardware, software, data center and management efforts with maximum efficiency.
- OS-level virtualization implementations that are capable of live migration can be used for dynamic load balancing of containers between nodes in a cluster.



Containers

- Containers are packages of software that contain all of the necessary elements to run in any environment.
- In this way, containers virtualize the operating system and run anywhere, from a private data center to the public cloud or even on a developer’s personal laptop.
- From Gmail to YouTube to Search, everything at Google runs in containers.
- Containerization allows development teams to move fast, deploy software efficiently, and operate at an unprecedented scale.

Containers vs. Virtual Machines

- Containers are much more lightweight than VMs
- Containers virtualize at the OS level while VMs virtualize at the hardware level
- Containers share the OS kernel and use a fraction of the memory VMs require

Confusion…

- **OS-Level Virtualization.** A type of server virtualization technology which works at the OS layer. The physical server and single instance of the operating system is virtualized into multiple isolated partitions, where each partition replicates a real server. The OS kernel will run a single operating system and provide that operating system functionality to each of the partitions.
- Operating system virtualization refers to the use of software to allow system hardware to run multiple instances of different operating systems concurrently, allowing you to run different applications requiring different operating systems on one computer system. The operating systems do not interfere with each other or the various applications.

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)

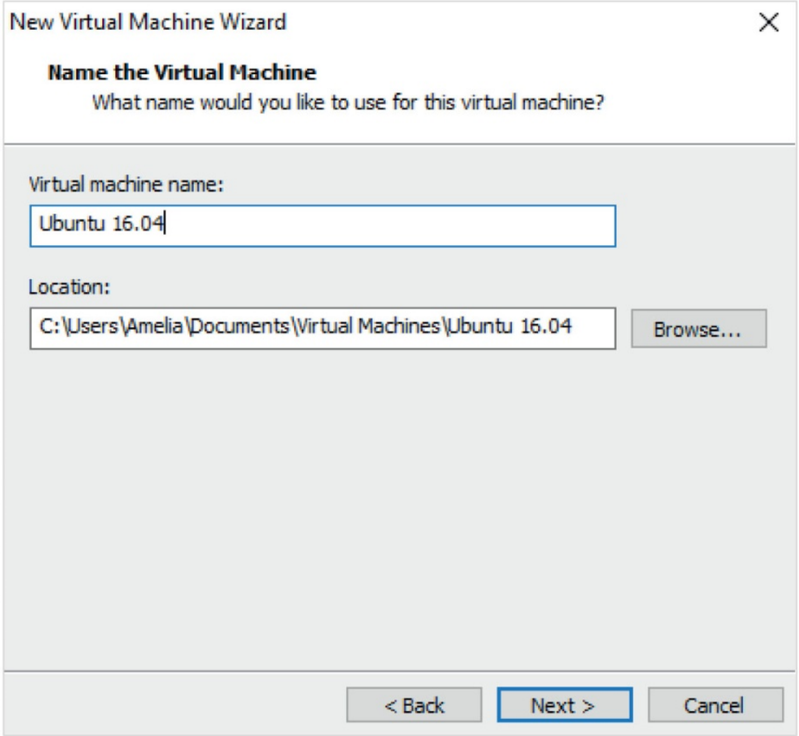
- Most widely used type 2 hypervisors:
  - Parallels Desktop - created for Macintosh users who also use Windows applications
  - KVM (Kernel-based Virtual Machine) - for Linux OS
  - Microsoft Hyper-V - new hypervisor built into Windows 10
  - VMware Workstation and Player - can be installed on almost 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)



New Virtual Machine Wizard

Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name: Ubuntu 16.04

Location: C:\Users\Amelia\Documents\Virtual Machines\Ubuntu 16.04

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

Source: VMware, *www.vmware.com*

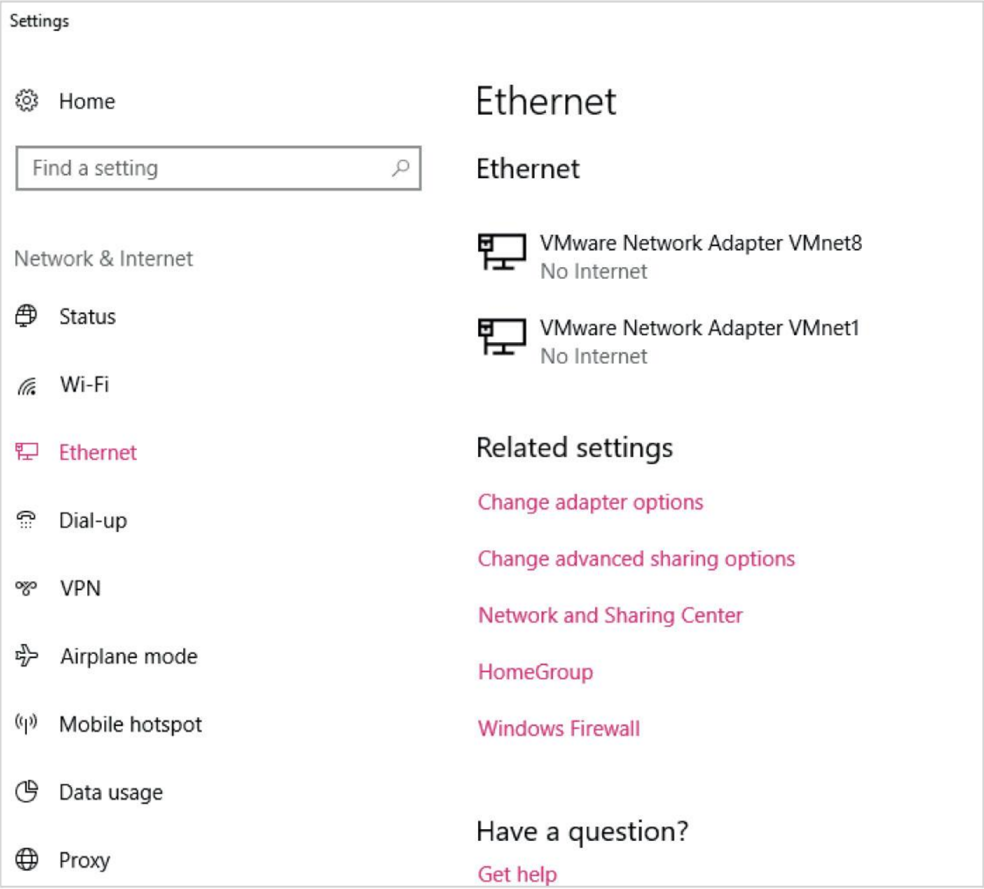
Type 2 Hypervisors (4 of 4)

- 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 8)

- 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 8)



Ethernet

Ethernet

VMware Network Adapter VMnet8
No Internet

VMware Network Adapter VMnet1
No Internet

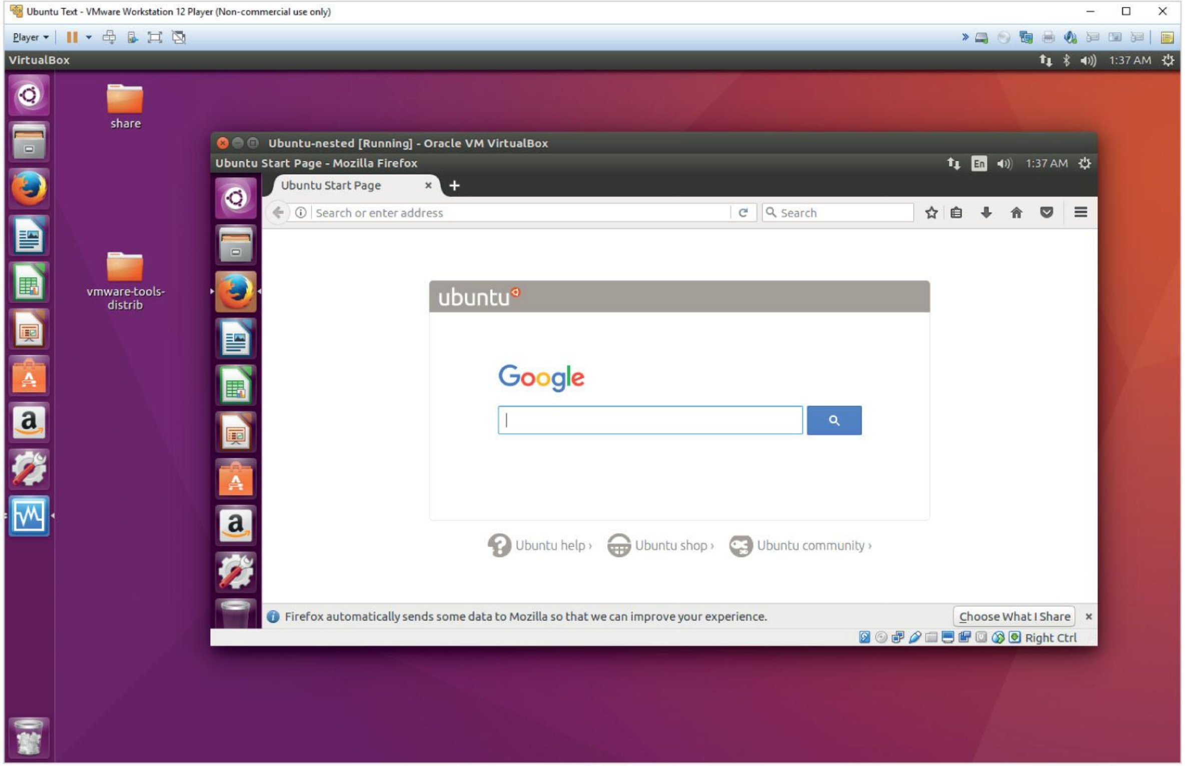
Related settings

Figure 10-7 Ethernet Connections on a Windows 10 computer

Conducting an Investigation with Type 2 Hypervisors (3 of 8)

- 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 8)



Firefox automatically sends some data to Mozilla so that we can improve your experience.

Figure 10-9 A VM nested inside another VM

Source: VMware, *www.vmware.com*

Conducting an Investigation with Type 2 Hypervisors (5 of 8)

- 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 8)

- 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 8)

- 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 (8 of 8)

- Using VMs as Forensic Tools
  - Investigators can use VMs to run forensics tools stored on USB drives

Working with Type 1 Hypervisors (1 of 2)

- To 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

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

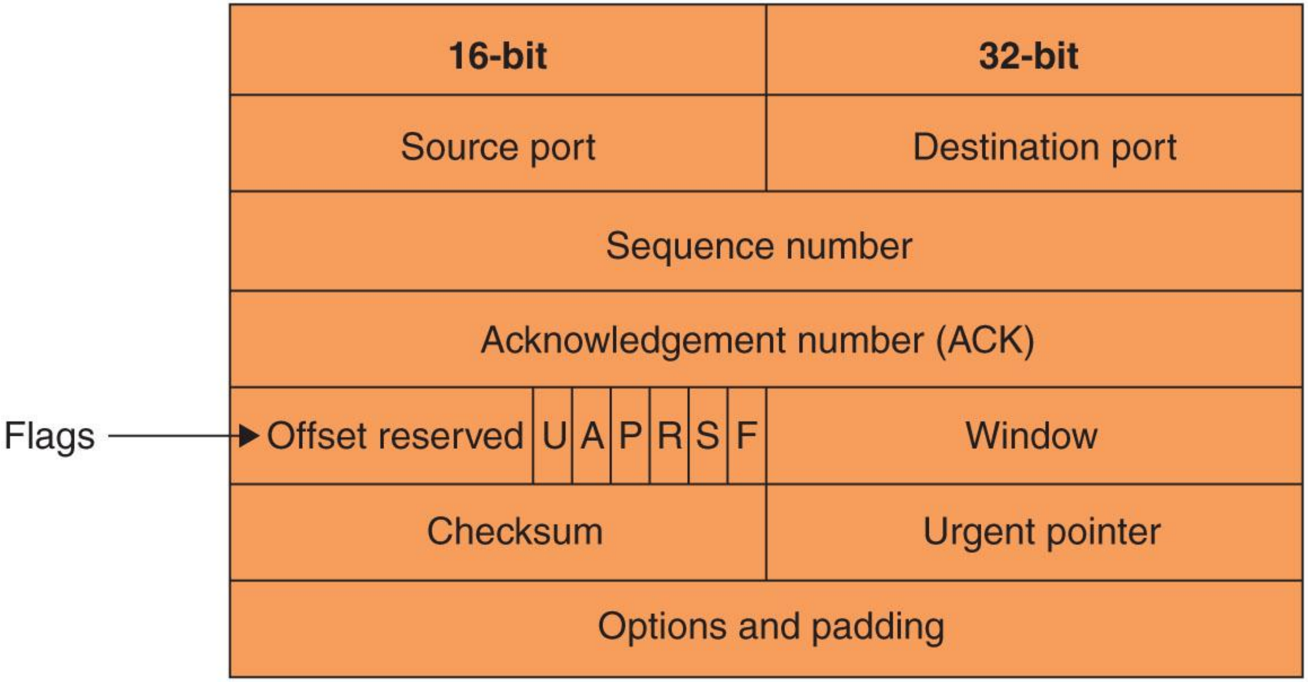
Using Network Tools

- 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)



16-bit

32-bit

Source port

Destination port

Sequence number

Acknowledgement number (ACK)

Flags

Offset reserved

U

A

P

R

S

F

Window

Checksum

Urgent pointer

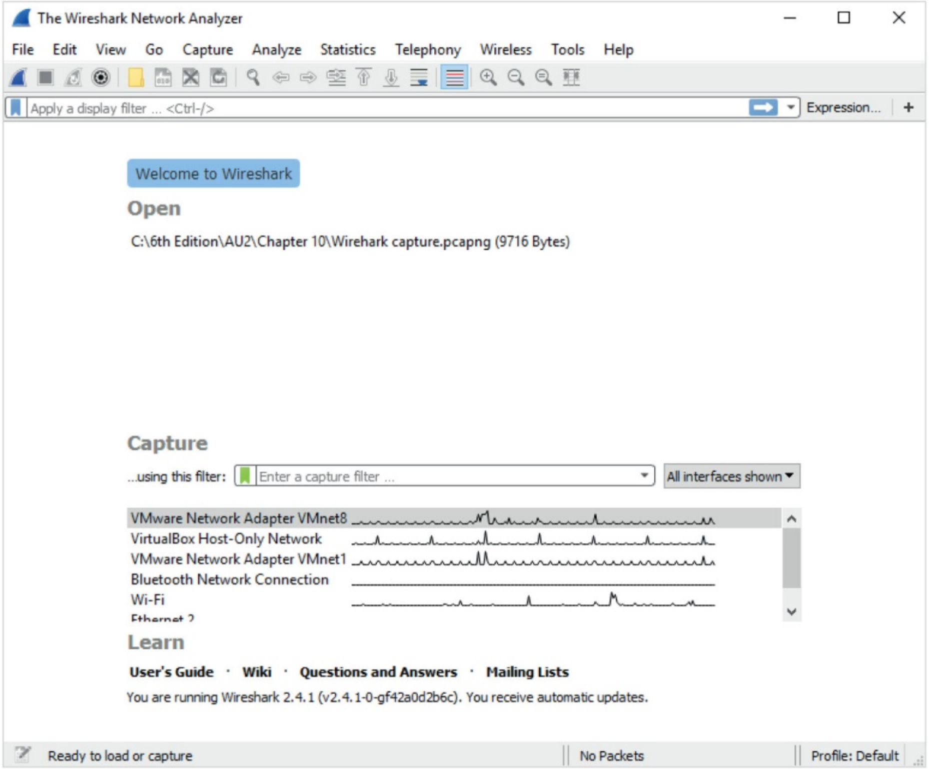
Options and padding

Figure 10-15 A TCP header

Using Packet Analyzers (3 of 5)

- Tools (cont'd)
  - Tcpslice
  - Tcpreplay
  - Etherape
  - Netdude
  - Argus
  - Wireshark

Using Packet Analyzers (4 of 5)


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Open

C:\6th Edition\AU2\Chapter 10\Wirehark capture.pcapng (9716 Bytes)

...using this filter: Enter a capture filter ...

All interfaces shown

VMware Network Adapter VMnet8
VirtualBox Host-Only Network
VMware Network Adapter VMnet1
Bluetooth Network Connection
Wi-Fi
Ethernet 2

Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

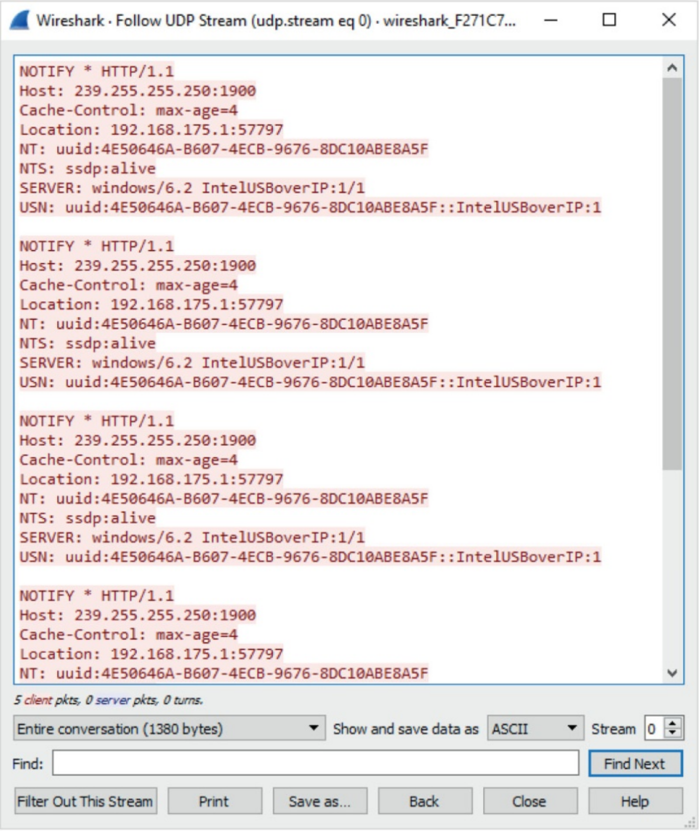
You are running Wireshark 2.4.1 (v2.4.1-0-gf42a0d2b6c). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

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