Data Hiding / VMs / Network Forensics

Objectives

- Determine what data to analyze in a digital forensics investigation
- Explain common data-hiding techniques
- 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

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining What to Collect

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

What do we need?

- What portions of evidence to examine and analyze depends on the nature of the investigation
  - And the amount of data to process
- **Scope creep** - when an investigation expands beyond the original description
  - Because of unexpected evidence found
  - Attorneys may ask investigators to examine other areas to recover more evidence
  - Increases the time and resources needed to extract, analyze, and present evidence

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Approach

- Begin a case by creating an investigation plan that defines the:
  - Goal and scope of investigation
  - Materials needed
  - Tasks to perform
- The approach you take depends largely on the type of case you're investigating
  - Corporate, civil, or criminal

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Approach (Cont.)

- Follow these basic steps for all digital forensics investigations:
  - 1. For target drives, use recently wiped media that have been reformatted and inspected for viruses
  - 2. Inventory the hardware on the suspect’s computer, and note condition of seized computer
  - 3. For static acquisitions, remove original drive and check the date and time values in system’s CMOS
  - 4. Record how you acquired data from the suspect drive

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Approach (Cont.)

- Follow these basic steps for all digital forensics investigations (cont'd):
  - 5. Process drive's contents methodically and logically
  - 6. List all folders and files on the image or drive
  - 7. Examine contents of all data in all folders *
  - 8. Recover file contents for all password-protected files
  - 9. Identify function of every executable file that doesn't match hash values
  - 10. Maintain control of all evidence and findings

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Approach (Cont.)

- Refining and Modifying the Investigation Plan
  - Even if initial plan is sound, at times you may need to deviate from it and follow evidence
  - Knowing the types of data to look for helps you make the best use of your time
  - The key is to start with a plan but remain flexible in the face of new evidence

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Data Hiding

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Data-Hiding

- Data hiding - changing or manipulating a file to conceal information
- Techniques:
  - Hiding entire partitions
  - Changing file extensions
  - Setting file attributes to hidden
  - Bit-shifting
  - Using encryption
  - Setting up password protection

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

OS Data Hiding

- One of the first techniques to hide data was changing file extensions
- Advanced digital forensics tools check file headers
  - Compare the file extension to verify that it’s correct
  - If there’s a discrepancy, the tool flags the file as a possible altered file
- Another hiding technique
  - Selecting the Hidden attribute in a file’s Properties dialog box

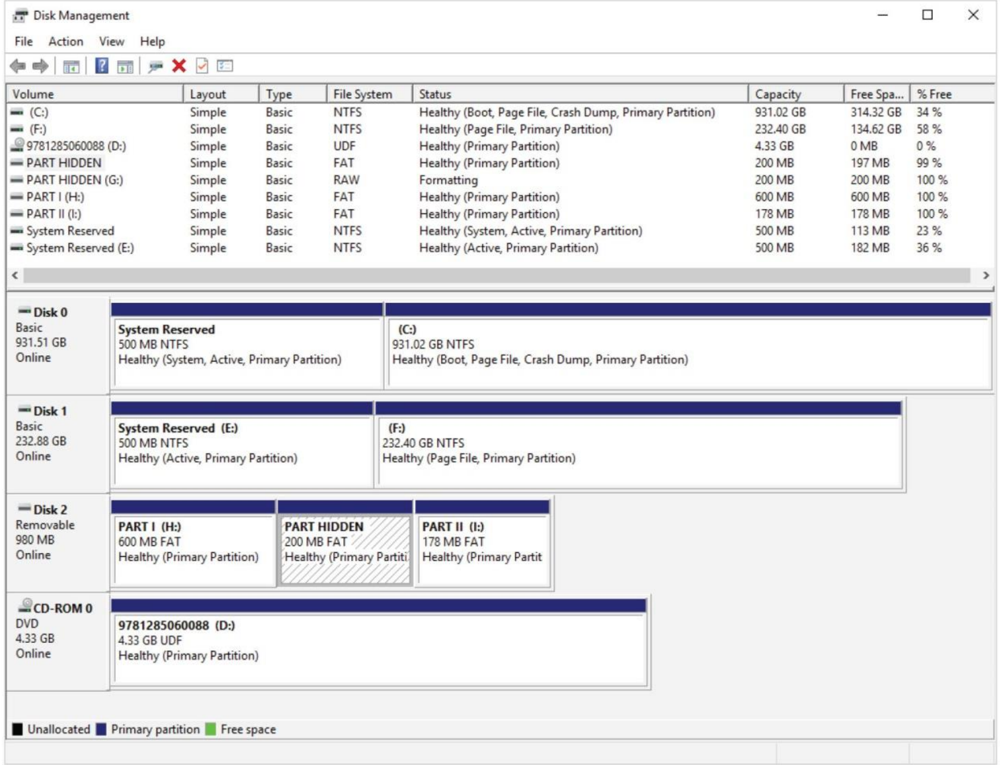
© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Hiding Partitions

- By using the Windows `diskpart remove letter` command
  - You can unassign the partition’s letter, which hides it from view in File Explorer
- To unhide, use the `diskpart assign letter` command
  - Other tools can do this too

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Example of Partition Without Assigned Drive Letter in Windows



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	931.02 GB	314.32 GB	34 %
(F:)	Simple	Basic	NTFS	Healthy (Page File, Primary Partition)	232.40 GB	134.62 GB	58 %
9781285060088 (D:)	Simple	Basic	UDF	Healthy (Primary Partition)	4.33 GB	0 MB	0 %
PART HIDDEN	Simple	Basic	FAT	Healthy (Primary Partition)	200 MB	197 MB	99 %
PART HIDDEN (G:)	Simple	Basic	RAW	Formatting	200 MB	200 MB	100 %
PART I (H:)	Simple	Basic	FAT	Healthy (Primary Partition)	600 MB	600 MB	100 %
PART II (I:)	Simple	Basic	FAT	Healthy (Primary Partition)	178 MB	178 MB	100 %
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	500 MB	113 MB	23 %
System Reserved (E:)	Simple	Basic	NTFS	Healthy (Active, Primary Partition)	500 MB	182 MB	36 %

Disk 0
Basic
931.51 GB
Online

System Reserved
500 MB NTFS
Healthy (System, Active, Primary Partition)

(C:)
931.02 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Basic
232.88 GB
Online

System Reserved (E:)
500 MB NTFS
Healthy (Active, Primary Partition)

(F:)
232.40 GB NTFS
Healthy (Page File, Primary Partition)

Disk 2
Removable
980 MB
Online

PART I (H:)
600 MB FAT
Healthy (Primary Partition)

PART HIDDEN
200 MB FAT
Healthy (Primary Partiti

PART II (I:)
178 MB FAT
Healthy (Primary Partit

CD-ROM 0
DVD
4.33 GB
Online

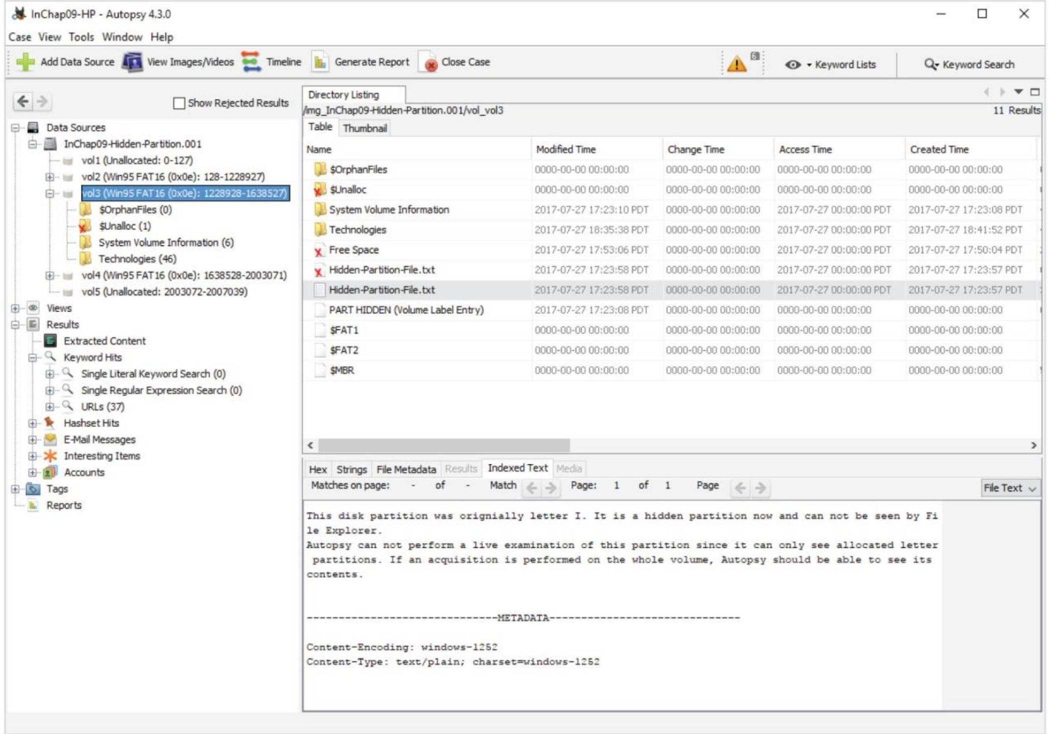
9781285060088 (D:)
4.33 GB UDF
Healthy (Primary Partition)

■ Unallocated 🟦 Primary partition 🟩 Free space

Figure 9-16 The Disk Management window

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Example of Hidden Partition in Autopsy


InChap09-HP - Autopsy 4.3.0
Case View Tools Window Help
Add Data Source
View Images/Videos
Timeline
Generate Report
Close Case
Keyword Lists
Keyword Search
□ Show Rejected Results
Data Sources
InChap09-Hidden-Partition.001
vol1 (Unallocated: 0-127)
vol2 (Win95 FAT16 (0x0e): 128-1228927)
vol3 (Win95 FAT16 (0x0e): 1228928-1638527)
$OrphanFiles (0)
$Unalloc (1)
System Volume Information (6)
Technologies (46)
vol4 (Win95 FAT16 (0x0e): 1638528-2003071)
vol5 (Unallocated: 2003072-2007039)
Views
Results
Extracted Content
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
URLs (37)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports
Directory Listing
Table
Thumbnail
Hex
Strings
File Metadata
Results
Indexed Text
Media
Matches on page: - of - Match
Page: 1 of 1 Page
File Text

/img_InChap09-Hidden-Partition.001/vol_vol3 11 Results

Name	Modified Time	Change Time	Access Time	Created Time
$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
$Unalloc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
System Volume Information	2017-07-27 17:23:10 PDT	0000-00-00 00:00:00	2017-07-27 00:00:00 PDT	2017-07-27 17:23:08 PDT
Technologies	2017-07-27 18:35:38 PDT	0000-00-00 00:00:00	2017-07-27 00:00:00 PDT	2017-07-27 18:41:52 PDT
Free Space	2017-07-27 17:53:06 PDT	0000-00-00 00:00:00	2017-07-27 00:00:00 PDT	2017-07-27 17:50:04 PDT
Hidden-Partition-File.txt	2017-07-27 17:23:58 PDT	0000-00-00 00:00:00	2017-07-27 00:00:00 PDT	2017-07-27 17:23:57 PDT
Hidden-Partition-File.txt	2017-07-27 17:23:58 PDT	0000-00-00 00:00:00	2017-07-27 00:00:00 PDT	2017-07-27 17:23:57 PDT
PART HIDDEN (Volume Label Entry)	2017-07-27 17:23:08 PDT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
$FAT1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
$FAT2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
$MBR	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

```
This disk partition was orignially letter I. It is a hidden partition now and can not be seen by Fi
le Explorer.
Autopsy can not perform a live examination of this partition since it can only see allocated letter
 partitions. If an acquisition is performed on the whole volume, Autopsy should be able to see its
contents.


-----------------------------METADATA------------------------------

Content-Encoding: windows-1252
Content-Type: text/plain; charset=windows-1252
```

Figure 9-18 Viewing a hidden partition in Autopsy

Source: *www.sleuthkit.org*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Marking Bad Clusters

- A data-hiding technique used in FAT file systems is placing sensitive or incriminating data in free or slack space on disk partition clusters
- Can mark good clusters as bad clusters in the FAT table so the OS considers them unusable
  - Only way they can be accessed from the OS is by changing them to good clusters with a disk editor

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Bit Shifting

- Some users use a program that changes the order of binary data
  - Makes altered data unreadable to secure a file, users run a program to scramble bits
  - Run another program to restore the scrambled bits to their original order
- **Bit shifting** changes data from its standard form to something that’s less distinguishable
- WinHex and Hex Workshop include a feature for shifting bits

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Basic Impact of a Bit Shift (Shift Left 1)

Binary	Decimal	Hex	ASCII
01000001	65	41	A

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Basic Impact of a Bit Shift (Shift Left 1)

Binary	Decimal	Hex	ASCII
01000001	65	41	A
10000010	130	82	□

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Basic Impact of a Bit Shift (Shift Left 1)

Binary	Decimal	Hex	ASCII
01000001	65	41	A
10000010	130	82	□
00000101	5	5	ENQ (enquiry)

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Steganalysis

- Steganalysis - term for detecting and analyzing steganography files

- Steganalysis methods
  - Stego-only attack – used when only the file suspected to contain steganography is available
  - Known cover attack – used when the original file without steganography applied is available
  - Known message attack – used when the message or data of a particular steganography instance is known
  - Chosen stego attack – used when tool used for steganography as well as potential pass phrases are known
  - Chosen message attack – used when the analyst applies their own message with stego and attempts to compare to the suspected file

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Encrypted Files

- To decode an encrypted file
  - Users supply a password or passphrase
- Many encryption programs use a technology called “**key escrow**”
  - Designed to recover encrypted data if users forget their passphrases or if the user key is corrupted after a system failure

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

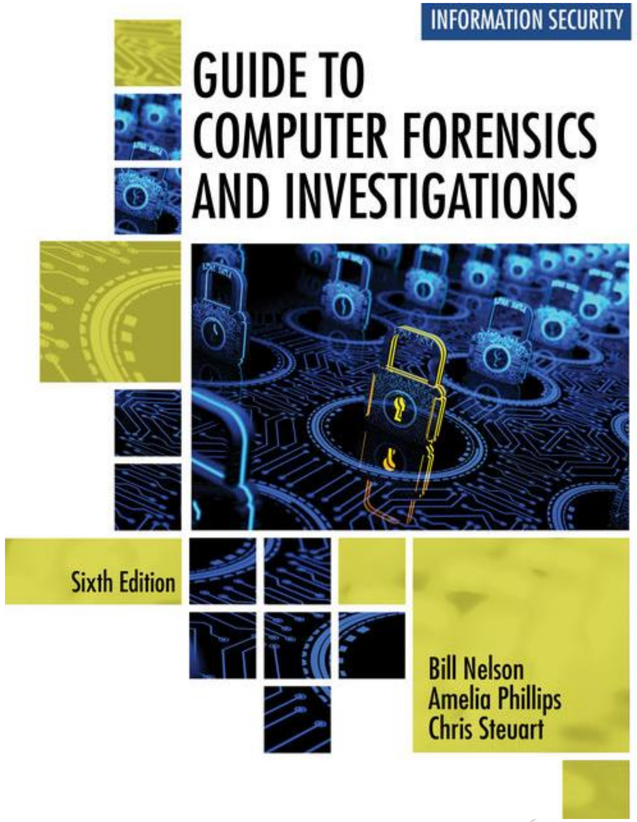
Recovering Passwords

- Password-cracking tools are available for handling password-protected data or systems
  - Some are integrated into digital forensics tools
- Stand-alone tools:
  - Last Bit
  - AccessData PRTK
  - ophcrack
  - John the Ripper
  - Passware

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

References

- *Guide to Computer Forensics and Investigations*
    - *ISBN: 9780357688595*



Bit Shifting w/ WinHex

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Virtual Machine Forensics Overview

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Background

- 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 hypervisors:
  - **Type 1** - loads on physical hardware and doesn’t require a separate OS
  - **Type 2** - rests on top of an existing OS (typical on a suspect machine)

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examples of Hypervisors

Type 2

- VMware Workstation, Workstation Player, Fusion
- VirtualBox
- Parallels Desktop

Type 1

- VMware vSphere (ESXi)
- Microsoft Hyper-V
- XenServer
- KVM

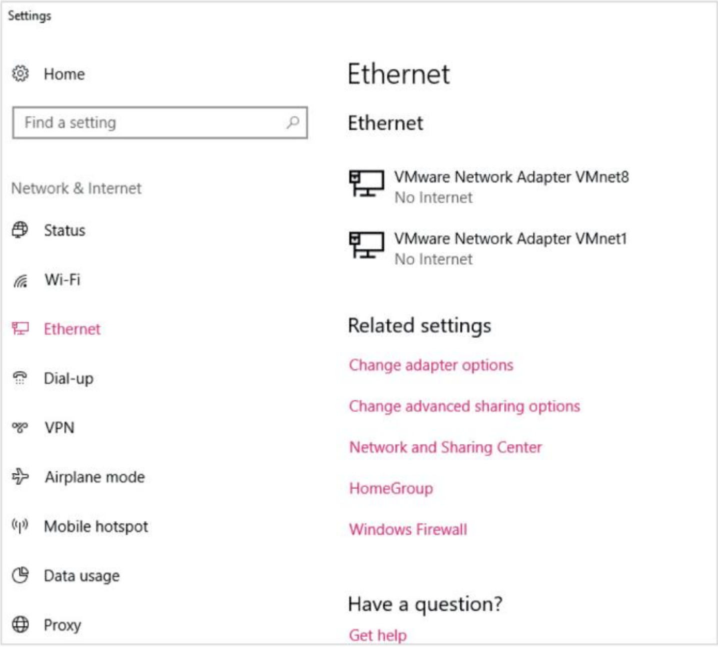
© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

VM Considerations

- VM Configuration is of interest (networking, storage, etc)
  - VMX for VMware; others will have different configuration locations
- VM detection with forensic suites
  - Look in the typical locations (Users/<Username>/Documents/Virtual Machines for VMware) for disk images (vmdk, qcow, vdi, vhd, raw, dd, etc.)
    - Autopsy searches the disk for vmdks
  - Check registry for evidence of VM interaction
  - Existence of virtual network adapter(s)

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Virtual Network Adapters on Host



Settings

Ethernet

Ethernet

VMware Network Adapter VMnet8
No Internet

VMware Network Adapter VMnet1
No Internet

Related settings

Have a question?

Figure 10-7 Ethernet Connections on a Windows 10 computer

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

VM Considerations (Cont.)

- Try and find any external devices that could have VMs stored on them
- Note: You can run virtual machines inside of other virtual machines

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Overall Steps (offline, captured system)

- Image host machine
- Extract VM disk images (format will vary, vmdk for VMware)
  - Hash these files and treat as additional system images
- Process the VM disk image as an evidence items
  - Most modern forensics software supports major VM disk formats. If yours is unsupported, you’ll have to extract to a format your forensics software understands

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Overall Steps (online, live system)

- 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 disk, 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

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

A Note on Virtual Networks

- Virtual switch is a little different from a physical switch
- 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

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

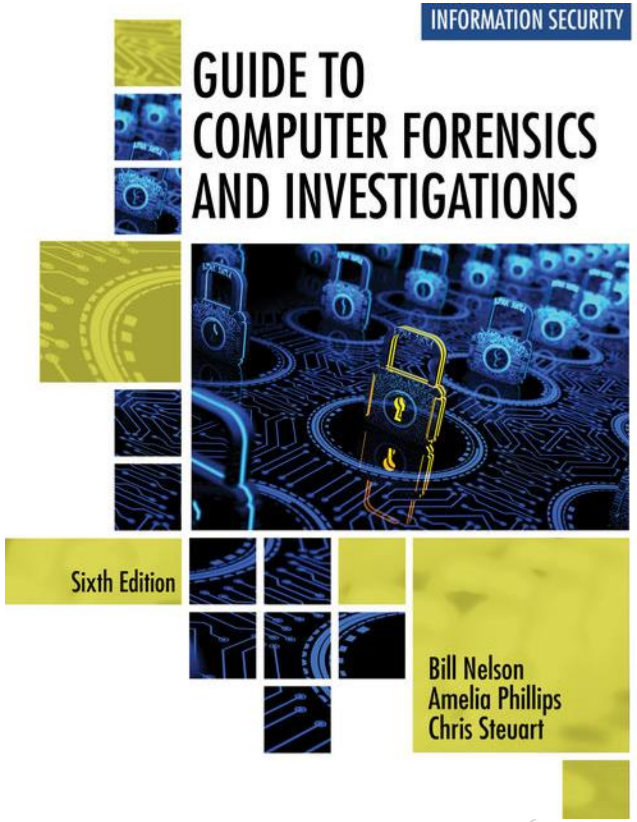
Example

- There are several projects in the text where you can setup a local VM if you wish to perform some basic analysis

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

References

- *Guide to Computer Forensics and Investigations*
  - *ISBN: 9780357688595*



Live Acquisition

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Extending Previous Acquisition Notes

- 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

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a
license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Steps for Live Acquisition

- Create or download a bootable forensic CD or USB drive
- Log your actions
- A network drive is ideal as a place to send the information you collect
  - External media will work too
- Copy the physical memory (RAM)
- The next step varies, depending on the incident you’re investigating
  - If you’re investigating an intrusion, you may want all system logs
  - If you’re investigating workplace misuse of time you may just want web history and email
- Be sure to get a hash of all files you recover during the live acquisition

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Example Live Acquisition Tools

- Memory
  - Mandiant Memoryze
  - FTK Imager
  - Magnet Axiom
- Filesystem Artifacts
  - Kroll KAPE
  - artifactcollector
  - FastIR Artifacts
  - FTK Imager

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Network Forensics

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

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

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Establish Procedures Ahead of Time

- 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

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Reviewing Network Logs / Captures

- Network logs record ingoing and outgoing traffic
  - Servers
  - Networking gear
  - Hypervisors

- Tcpdump and Wireshark - tools for capturing/examining network traffic
  - Helpful in interpreting data within packet captures

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Packet Analyzers

- **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

- Tools
  - `tcpdump`
  - `tethereal`
  - Wireshark
  - Network Miner

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Other Network Tools

- Splunk / ELK Stack / GrayLog – Log aggregation and interpretation
- Nagios – System Monitoring
- Cacti – Network graphing
- Arkime – Scalable packet capture index & search

- The list goes on, these are just examples
  - If network forensics sounds interesting, check out CSC 439 Threat Hunting & Incident Response w/ Dr. Cody Welu!

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

References

- *Guide to Computer Forensics and Investigations*
  - *ISBN: 9780357688595*