Computer Investigations

Nelson et al, 6th edition

Chapter 1, pp 21-54 (top)

Additional material

Labs based upon Nelson but different

Agenda

Today's agenda:

- *Accessing RADISH desktop*
  - Windows 10
  - Kali Linux (via VMWare Workstation Pro)
- *Intro to Forensic Investigations*
  - Lecture
  - Lab:
    - *Based on Nelson text, Chapter 1*
    - *Montgomery_72018 Case*
- *Review and Upcoming Assignments*

RADISH Access

RADISH Access

You should have receivee an email that has the following information

Slides: *Remotely Accessing RADISH*

Instructions (including credentials)

Support Information

See next slide

RADISHng

Support

Preferred method: Google Form

Link: https://forms.gle/fjiN9WwqmQEdHXoX7

Email

Subject: Support for ITMS 538/438

Address to: forseclab@iit.edu

RADISHng

Assign01b_s

To complete Assign01b_s, you should

Navigate to https://radish.sat.iit.edu

Select and install VMWare Horizon Client

HTML5 (Web-based) or

Desktop client

Run VMWare Horizon Client

Connect to default server (https://radish.sat.iit.edu)

Enter your credentials

Launch your Windows 10 ITMS x38 Desktop

Forensics Investigations

An Introduction

Overview

This lecture is sort of a hands-on digital forensics technology overview

Nelson et al, 6th edition Chap 1 pp 21-54 is used as a base

We'll do a bit of digital forensics

Move through the steps of an investigation

Use a forensic software tool

We'll work with a flash drive image

Similar techniques can be used on much large disks

Investigation Procedure
Preliminaries

Prepare the Case

Is this a crime, civil, or administrative policy violation?

Begin the investigation

Take a systematic approach

- Assess the case
- Map out how you will proceed
- Plan the investigation
- Plan the gathering & securing information (potential evidence)

Understand the computer forensics workstations and software that you will use

Consider data recovery workstations, tools and software

Investigation Procedure
Lab Work: Discuss & Demonstrate

Often, labs will be demonstrated during class

Students will repeat or do similar labs as assignments.

DN0

Investigation Procedure
Lab Work: Discuss & Demonstrate

In this session we'll cover a simple forensic analysis of a case

- *Discuss some steps of the process*
- *Demonstrate others*

Follow closely the Nelson text

- *Collect and secure the sources from which we will develop evidence*
  - From a flash drive and other details
- *Create two forensic copies of the flash drive*
- *Investigate the flash drive*
- *Develop evidence*
- *Create a forensic report*

Slide 14

DN0 May want to remove the part where they collect and secure evidence and create forensic copies

Maybe I just need to mention that only the items in red will be demonstrated
Don Nelson, 2022-08-31T21:16:14.551

Investigation Procedure
Lab Work: Discuss & Demonstrate

Using tools, create an **exact** copy

*In our case tonight, we'll discuss creating an exact duplicate (i.e., **forensic image**) of the flash drive*

Be able to prove it is an exact copy

Secure the original material investigated

In our case tonight, we'll securing the original flash drive

Chain of custody

Using tools, gather information

Gather information from the forensic image

Not from the original

Investigation Procedure
Analysis, Report and Evaluation

Complete a case

Develop some hypotheses about how the crime or violation was committed

Develop evidence (based upon information gathered) that supports one hypothesis and refute the others

Write/generate a report

Prepare a Case

Prepare a Computer Investigation

Role of computer forensics professional

Gather information and from it develop evidence to prove a suspect committed a crime or violated a company policy

Collect information in a way that can be offered in court or at a corporate inquiry

Investigate the suspect's computer but preserve the evidence and perform the analysis on a different computer

Prepare a Computer Investigation

Follow an accepted procedure in preparing a case

This procedure may differ depending on whether the violation is administrative, civil or criminal

Chain of custody ← Important

Control and record the route the evidence takes from the time you find it until the case is closed or goes to court

A court will declare information inadmissible as evidence if there is a chance that the source of the data could be tainted

Examining a Computer Crime

Computers can contain information that helps law enforcement determine

Chain of events leading to a crime

Evidence that can lead to a conviction

Law enforcement officers should follow proper procedure when acquiring the evidence

Digital evidence can be easily altered by an overeager investigator

Examining a Computer Crime

Nelson's text describes a hypothetical crime scene

Suspected drug dealer

Police raided home

Hopefully with a warrant; if not, anything they found will be inadmissible in court

Seized several digital items that might yield evidence of a crime

The Computer Crime Scene

Figure 1-8 The crime scene

What do you see in the crime scene?

DN0

Examining a Computer Crime*

Now review ***An Overview of a Computer Crime*** on (p 23-top of p 24) of Nelson, 6th Ed

Then close your book

What steps did the acquiring officer follow in the seizure of the digital items?

You're told that the forensic examiner's office has a number of tools.

What tool might they have?

What tool might they not have?

Slide 23

DN0 Put in answers to what tools they might have.
Don Nelson, 2022-08-31T21:14:57.451

Examining a Company Policy Violation

Employees misusing resources can cost companies millions of dollars

Private enterprises are increasingly turning to forensic specialists to investigate policy violations

Vendors of forensic equipment and software report the following trends

- *Their sales to law enforcement and government entities are increasing*
- *Their sales to private organizations have grown and are still growing*
- *They have and are modifying their products and marketing to accommodate this trend*

Examining a Company Policy Violation

Examples of possible misuse

- *Surfing the Internet, especially on company time*
- *Sending personal e-mails*
- *Using company computers for personal tasks*
- *Using company computers in a private business*
- *Copying proprietary information*

A Company Policy Violation Scenario

We will use the following scenario for the rest of this session.

An employee named George Montgomery has been missing for a week without any notice

Another employee, Martha, is also missing without notice

No one seems to know anything about why they are gone

Steve Billings (George's supervisor) asks the IT Dept. to confiscate George's hard drive and any other storage media in his work area

Why can George's company do this?

What George's Company Can Do in Illinois, U.S.A.

The computer supplied by your employer and used by you both at work and home can be seized.

Your personally owned computer, when connected to your company's network is subject to searching

Your personally owned computer, when not network connected at all or connected to a public ISP is probably not legally subject to search or seizure

What if you're on your company network via wireless network?

Begin an Investigation

Taking a Systematic Approach
Really just common sense

1. Make an initial assessment about the type of case you are investigating
2. Determine an initial approach to investigating the case
3. Create a detailed design for the investigation
4. Determine the resources you need
5. Obtain & copy the evidence disk drive
6. Identify the risks
7. Mitigate or minimize the risks
8. Test the design
9. Analyze and recover the digital evidence
10. Investigate the data you recovered
11. Complete the case report
12. Critique the case

Assessing the Case

Systematically outline the case details:

- *General situation*
- *Specifics about the case*
- *OS involved*
- *Location of evidence*
- *Nature of the case*
- *Type of evidence*
- *Known disk formats*

Based on case details, you can determine the case requirements:

- *Type of evidence*
- *Computer forensics tools needed*
- *Special OSs that might be required*

Assessing the Case of Missing George Montgomery

Now review ***Assessing the Case*** (Nelson 6th ed, p 26 & 27)

Then close your book

Let's answers questions about the case

General situation..... Possible employee resource abuse

Nature of the case..... Side business on company computer

Specifics about the case.... Set up Web sites

Type of evidence..... USB drive

Known disk formats..... NTFS (on the flash drive)

Location of evidence..... A USB drive from George's computer
Custodian has it

Planning your Investigation

1. Acquire the evidence
2. Complete an ***evidence form*** & establish a ***chain of custody***
3. Transport evidence to a computer forensics lab
4. Secure evidence in an approved secure container
5. Prepare a forensics workstation
6. Obtain the evidence from the secure container
7. Make a forensic copy of the evidence
8. Return the evidence to the secure container
9. Process the copied evidence with computer forensics tools

Planning *Montgomery_72018* Investigation

1. Get flash drive from custodian
2. Start an *evidence form* and establish a *chain of custody*

   Where has the flash drive been since it was seized?

   Who has it.

   Keep track of where it is and who has it. Document!
3. Take the flash drive to the forensic lab
4. Secure it

   Lock it up in an approved secure way. Label it.

   Take precautions to keep it from being damaged

   Antistatic bags. Protective enclosure.

Planning *Montgomery_72015* Investigation

An evidence custody form helps you document what has been done with the original evidence and its forensics copies

It records the chain of custody

Nelson discusses two types of custody forms

Single-evidence form

Multi-evidence form

Multi-Evidence Form

Organization X
Security Investigations
This form is to be used for one to ten pieces of evidence

Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

	Description of evidence:	Vendor Name	Model No./Serial No.
Item #1			
Item #2			
Item #3			
Item #4			
Item #5			
Item #6			
Item #7			
Item #8			
Item #9			
Item #10			

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Item #	Evidence Processed by	Disposition of Evidence	Date/Time
			Page __ of ___

Figure 1-9 A sample multi-evidence form used in a private-sector environment

Single-Evidence Form

Metropolis Police Bureau
High-tech Investigations Unit
This form is to be used for only one piece of evidence.
Fill out a separate form for each piece of evidence.

Case No.:		Unit Number:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

Item # ID	Description of evidence:	Vendor Name	Model No./Serial No.

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Evidence Processed by	Disposition of Evidence	Date/Time
		Page __ of __

Single-Evidence Form *(filled out example)*

Metropolis Police Bureau
High-tech Investigations Unit
This form is to be used for only one piece of evidence.
Fill out a separate form for each piece of evidence.

Case No.:	Montgomery_72015	Unit Number:	----------
Investigator:	Vashiti Marin, Legal Dept.		
Nature of Case:	Possible use of company computer for non-Acme purposes		
Location where evidence was obtained:	Originally from desk of George Montgomery, Acme employee.		

Item # ID	Description of evidence:	Vendor Name	Model No./Serial No.
102-01	USB drive, red-orange "SAT@IIT ForSecLab" In red-orange letters on metallic background	None apparent	None apparent

Evidence Recovered by:	Vashiti Marin	Date & Time:	22 Jan 2020 10am
Evidence Placed in Locker:	Dawid Broda, evidence custodian	Date & Time:	22 Jan 2020 11am

Evidence Processed by	Disposition of Evidence	Date/Time
Vashiti Marin	Make forensic images of flash drive	22 Jan 2020,2pm
Dawid Broda	Replace flash drive in Locker	22 Jan 2020, 4pm

Securing your Evidence

Use computer safe products

Antistatic bags *Antistatic pads*

Use evidence bags to secure and catalog the evidence

Use padded containers if needed

Use evidence tape to seal bags and containers

Write your initials on tape to prove that evidence has not been tampered with

Consider computer-specific temperature and humidity ranges if needed

Forensic Workstations

A case may involve a wide variety of OSs, mass storage devices, etc.

So, a forensic lab needs to have

Many different OSs

Interfaces to attach to and read many different mass storage devices in a way guaranteed not to modify the content of the mass storage device

Being attached to a network is **not** desirable

Forensic workstations MUST NOT be network attached

But the lab needs other computers that are

OS Intrusiveness

All OSs are intrusive in that as they boot up, they will try to access mass storage devices and write to them

Also, if you are analyzing a flash drive, you can prevent it from being modified by setting the read-only switch

If it has one

OS Intrusiveness

But what if it doesn't have a read-only switch

Flash drives usually don't

Or what if we need to analyze a hard disk?

Both software and hardware "write-blockers" exist that can prevent writing to a hard disk

You can set up your personal Windows computer so that it can be a write blocker for USB devices

The following Lab shows you how to do this on your personal Windows computer if you wish to do it.

We will not do this because this is an online class and we would need physical computers

Lab 02a-1

Configure Win10 to write block USB devices

Do this on your **personal Windows computer**

Do **NOT** do this on your RADISHng VM

Overview

In Windows XP SP2, Microsoft added a feature that allows us to write block USB storage devices

It was first discussed on Microsoft TechNet

The details are also in a white paper by AccessData

This feature has been continued in Vista through Windows 11

Overview

There are also tools on the Internet

e.g., Thumbscrew

http://www.irongeek.com/i.php?page=security/thumbscrew-software-usb-write-blocker

Other similar tools are available

Always be careful what you download/installSo, we could download an app and use it

But you wouldn't learn much

Instead, lets learn something. Do it yourself!

Overview

The three basic steps

1. *Create a Windows 10 restore point on your personal computer*
2. *Modify the Registry*
3. *Create two **.reg** files that will allow you to easily move back and forth between blocking and not blocking*

Create a Win10 Restore Point
(so that if we mess up we can recover)

Go to

Change ***Control Panel*** view to ***Small Icons***

Click on ***System***

In the left pane, click ***System protection***

If you are prompted for confirmation, confirm to continue

Click on ***System Protection*** tab

Click on ***Create…***

Type a description of the restore point

e.g., USB Write protect registry hack

Click ***Create***

It will take between 10 and 30 seconds

Click ***OK***

Get out of all the pop-up windows and close the *Control Panel*

Modify the Registry

Run ***regedit*** *(as administrator)*

Go to

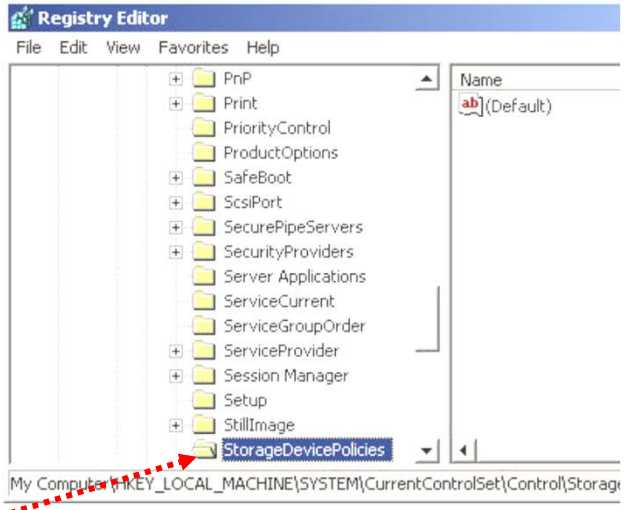
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet

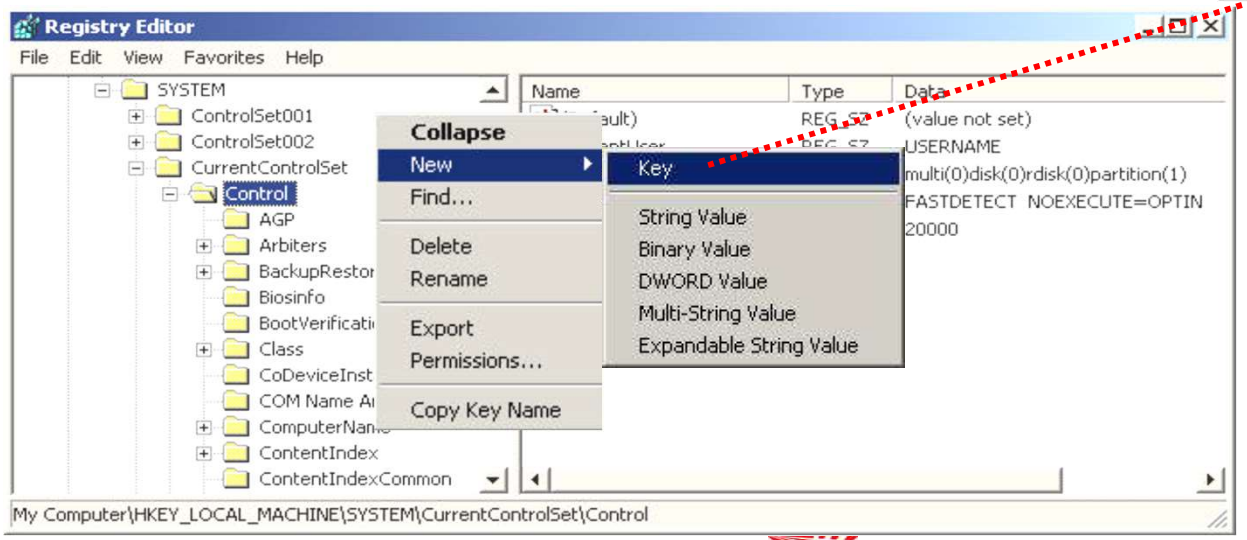
Highlight the *Control* key

Right click on *Control* and choose *New > Key*

You will get a highlighted *NewKey#1* item

Rename it ***StorageDevicePolicies*** *(no spaces)*



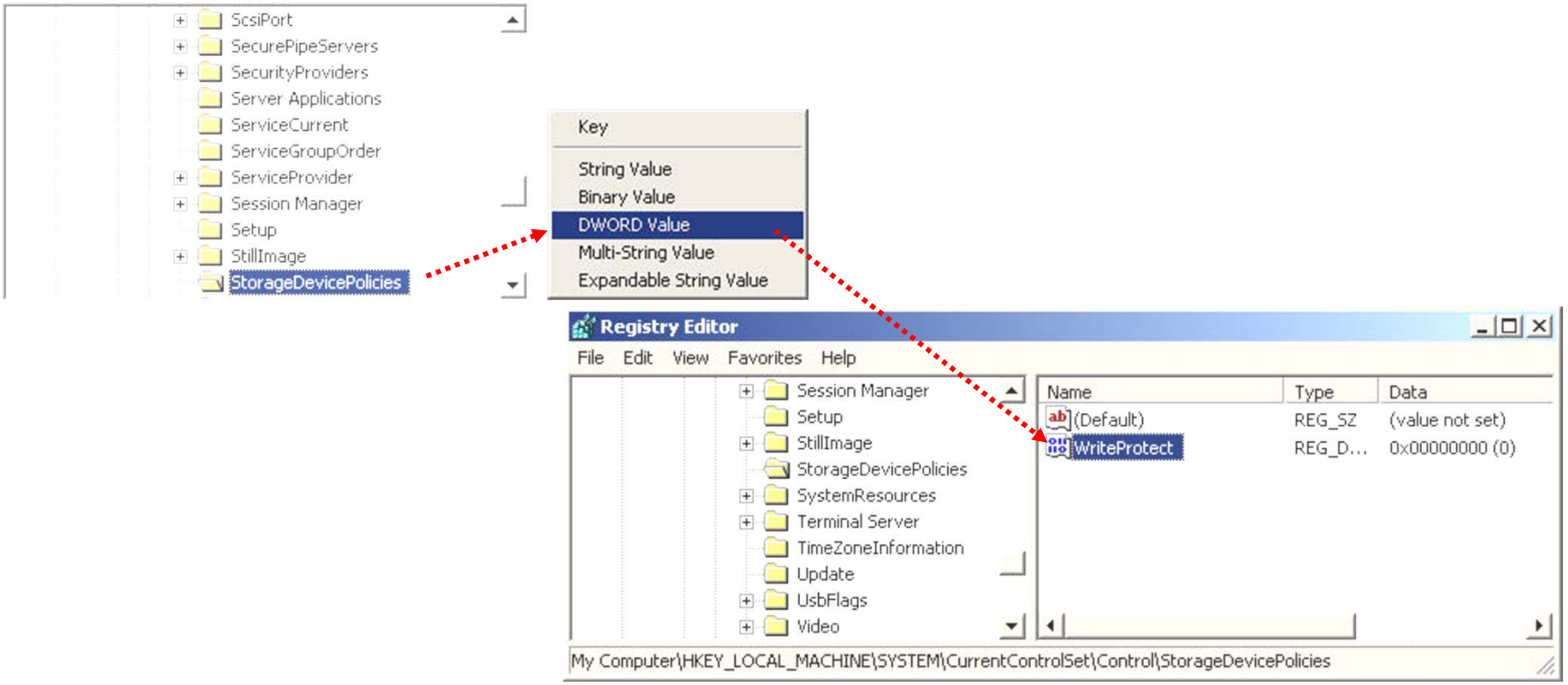


Modify the Registry

Right click on ***StorageDevicePolicies***

Select ***New → DWORD (32 bit) Value***

Rename it ***WriteProtect*** (no space)



Modify the Registry
To Make Win10 Prevent Writing to USB Devices

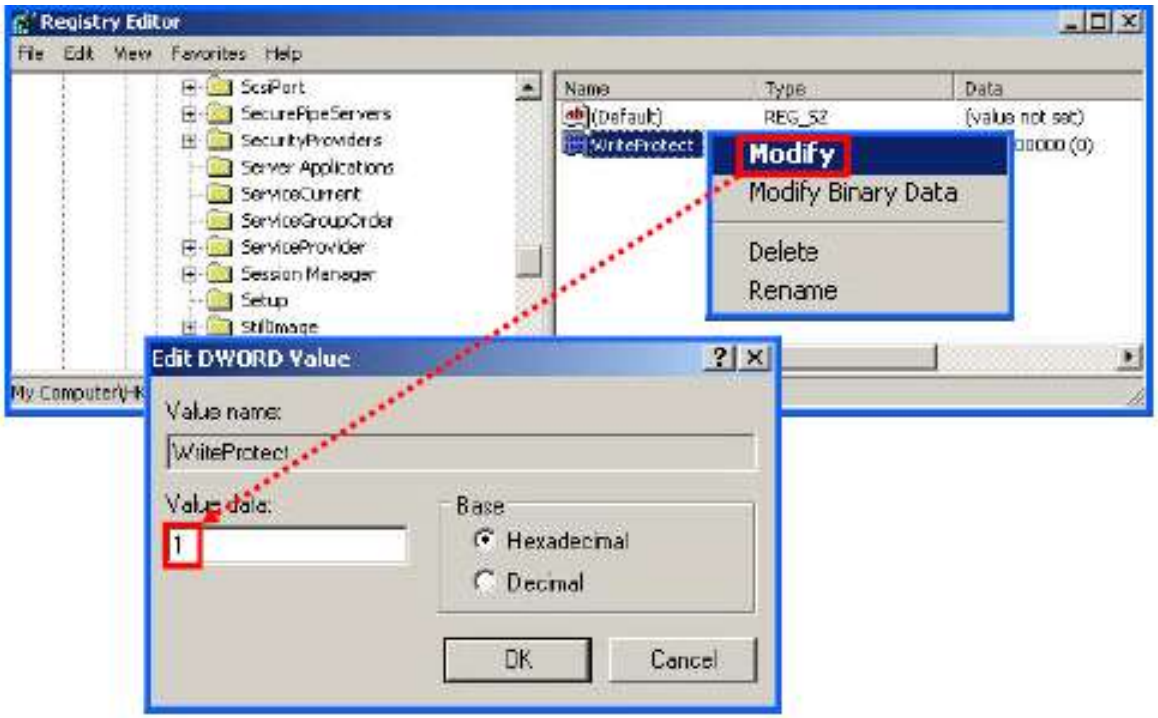
Right click on ***WriteProtect***

Select ***Modify***

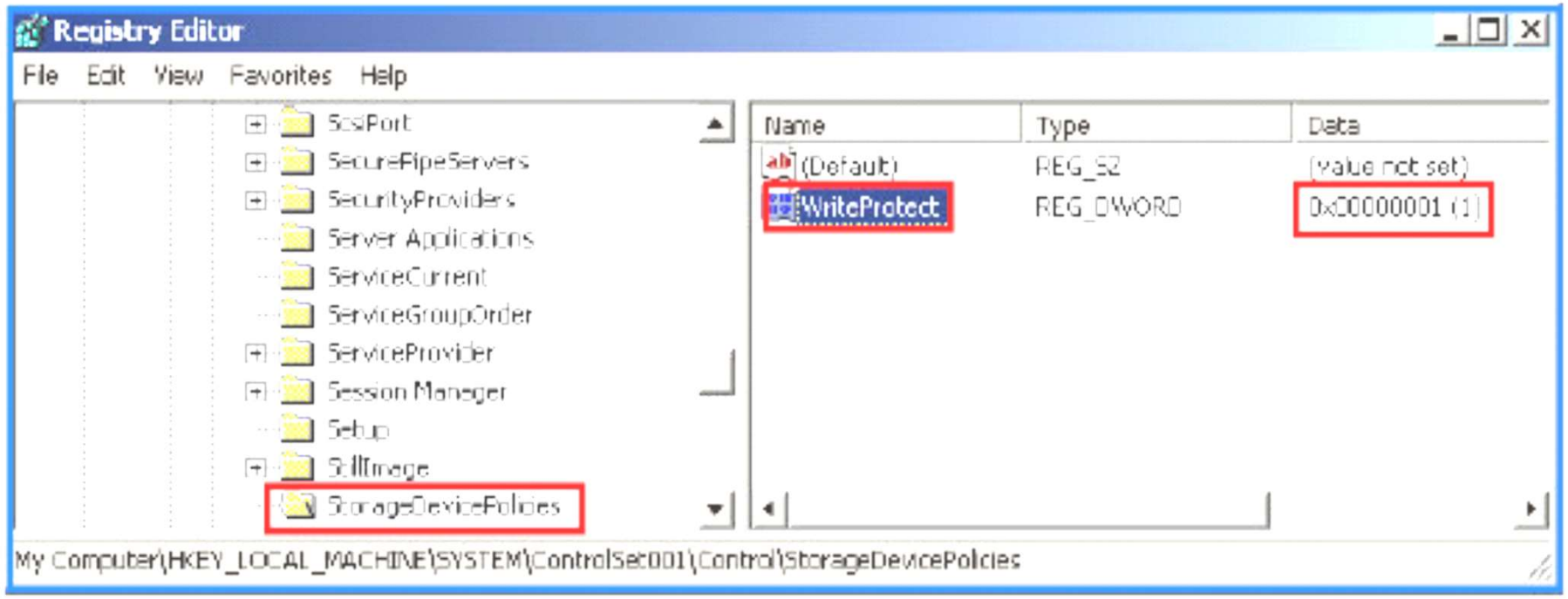
An “Edit DWORD Value” window will pop up

Change the value to “1”

Click “OK”



Result



Don’t close the registry yet!

Creating Desktop Links

You've created a new key and value that will write protect USB devices

But we need to easily move between write protect and no write protect

To do this we will create a desktop link

Creating Desktop Link
USB Write Protect ON

Right click on ***StorageDevicePolicies***

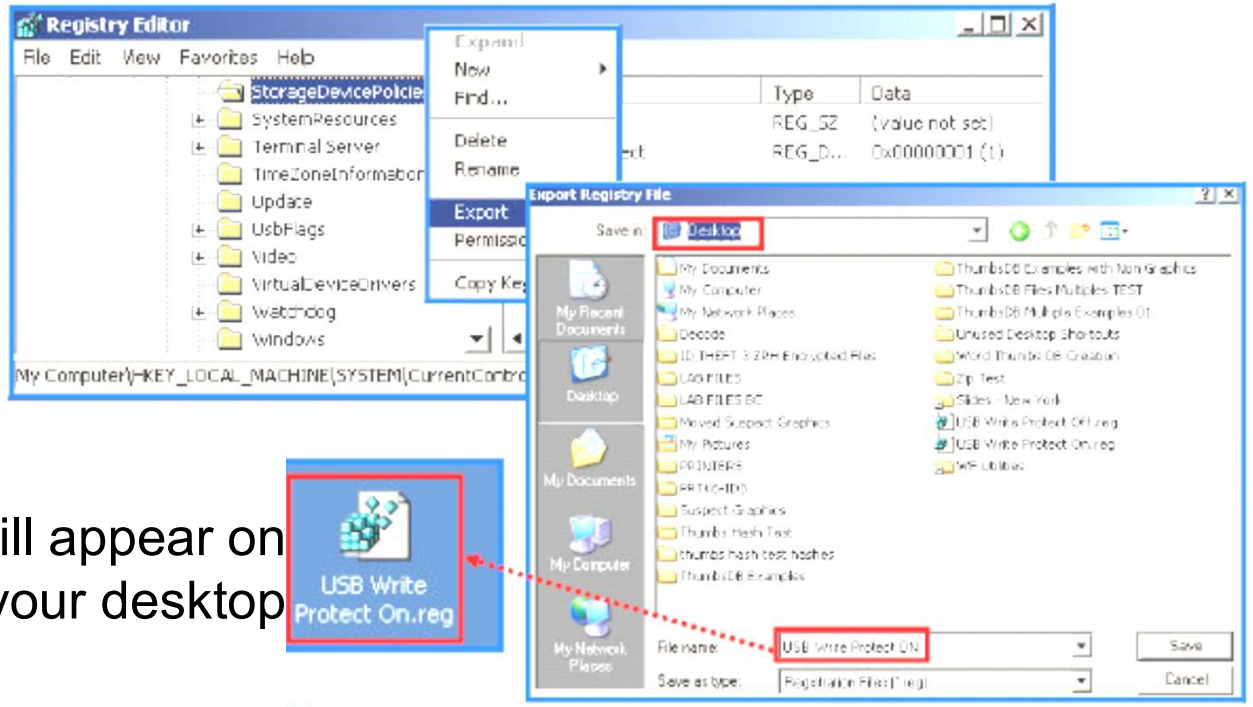
Select ***Export***

An “Export Registry File” window will pop up

Pick the Desktop at the top of the window

Name the file ***USB Write Protect ON***

Click ***Save***



A link will appear on your desktop

Modify the Registry
To Allow Win10 to Write to USB Devices

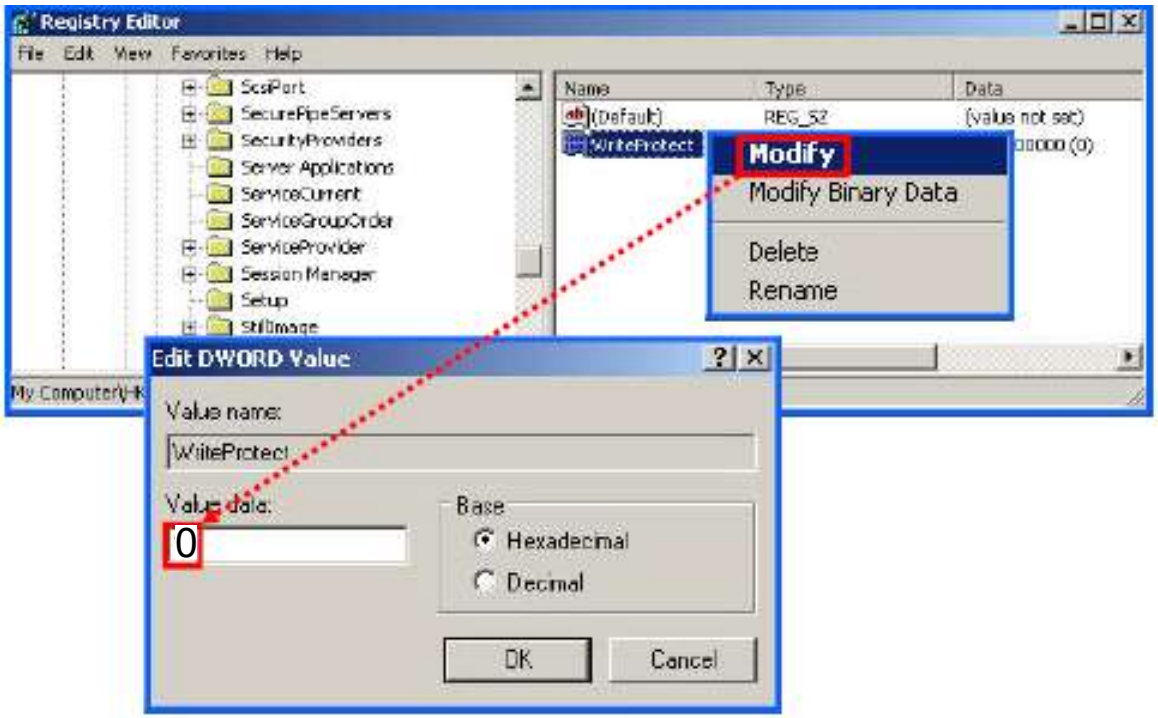
Right click on ***WriteProtect***

Select ***Modify***

The “Edit DWORD Value” window will pop up

Change the value to “0”

Click “OK”



Creating a 2nd Desktop Link
USB Write Protect OFF

Right click on ***StorageDevicePolicies***

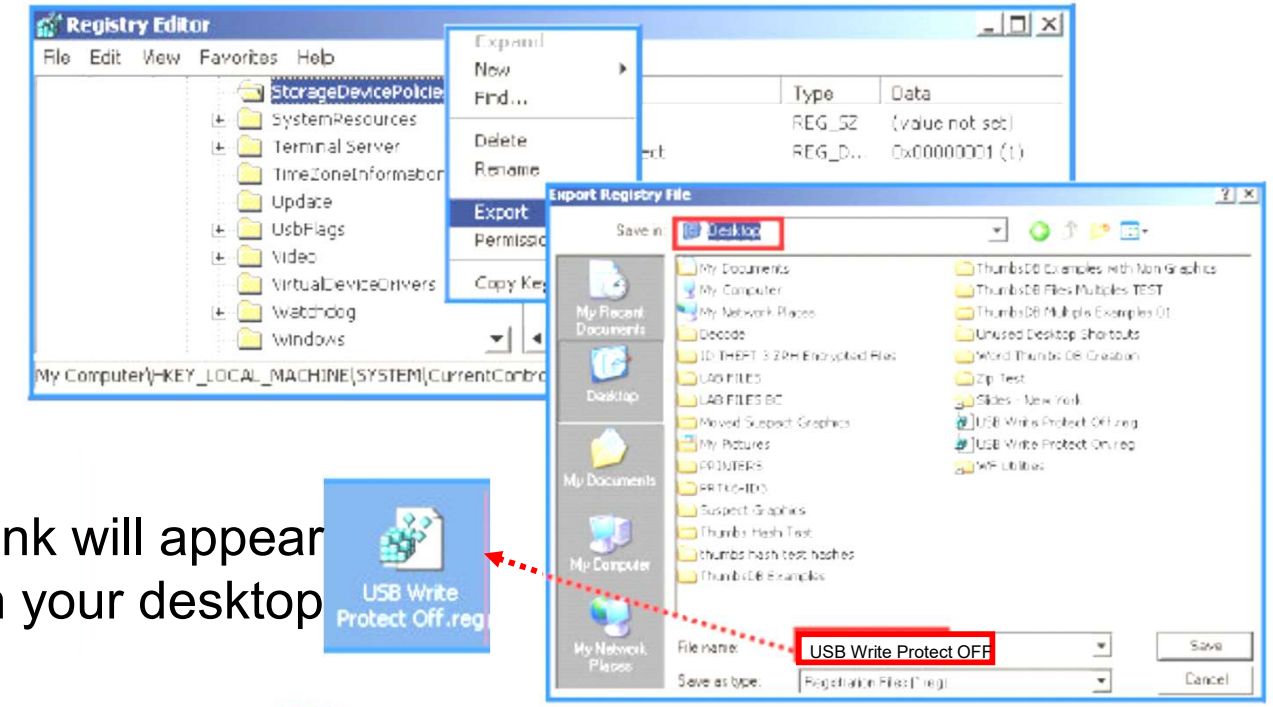
Select ***Export***

An “Export Registry File” window will pop up

Pick the Desktop at the top of the window

Name the file ***USB Write Protect OFF***

Click ***Save***



A 2nd link will appear on your desktop

Two New Links on Your Desktop

Close regedit

You should have two icon links on your desktop

With these you can change between

Blocking writing to USB devices and

Allowing writing to USB devices

These are not shortcuts; they are actual Registry code.

Comments on This USB Write Protect Policy

To write protect a USB device you must set the ***USB Write Protect Device Policy to ON*** **before** you plug in your USB device

When you plug in a USB device, Windows checks to see if it should allow writing

This capability is not good practice in real cyber forensic cases

Generally, not acceptable in court

Usually approved write blockers are used

We have some of these, but they are expensive

End of Lab 02a-1

Back to the *Montgomery_72018* Case

Conducting the Investigation

So far you

Have a plan for the investigation

Set up a workstation to be able to write protect USB devices

Installed some of the needed software

Actually, we installed it for you in order to save time

The other software was installed for you

Lab 02a-2

Gathering the Evidence

pp 41 of Nelson 6th ed

Steps 1-6

Lab 02a-2
Obtaining the Evidence; Preview

Review page 41 of Nelson 6th ed

Conducting an Investigation

Gathering the Evidence

Step 1-6 on p. 41 of Nelson:

Because this class is entirely online, we can't actually execute the procedures detailed in steps 1-6.

Instead, we will assume that steps 1-6 have already been done and the item is in the custodian's evidence locker

Lab 02a-2
Gathering the Evidence; Preview

We don't have an real evidence cabinet, locker or safe

- *In the past we used a red plastic box to simulate the evidence locker*
- *Each student would have a flash drive*
- *Each student would sign out the evidence, completing the chain of custody form*
- *After the student made forensic images of the flash drive, the would return the drive to the custodian and execute the transfer using the chain of custody form*

The custodian is in charge of the evidence locker

- *The* custodian *is not the same as the* forensic investigator
- Each student will be the forensic investigator and will image and investigate her or his own evidence

End of Lab 02a-2

Bit-by-Bit Copies

Aka:
Bit-image copy
Bit-stream copy
Forensic copy
Image copy

Bit-by-Bit Copies

This type of copying is a bit-by-bit copy of the original storage medium

Exact copy of the original storage medium

*Often referred to as a **"bit-image"**, **"bit-stream"** , **"image"** or **"forensic"** copy*

Different from a simple backup copy or the copying of files

Such simple copying copies only known files

Does not copy deleted files, file fragments, "empty" space on a disk, etc.

The "empty space" may not really be empty

Bit-by-Bit Copies

A bit-by-bit “image” file contains a bit-by-bit copy of

- *All data on a disk or partition*
- *All the empty space*
- *Positioned exactly as it is on the original device*

You usually need to copy the image file to a target disk that matches the original disk’s size, and model

- *Or at least to a disk that is larger than the original disk*
- *And maybe manufacturer*

This is a limitation of direct bit-by-bit copying

But you don't usually copy from the source disk to the destination disk directly

Bit-by-Bit Copies

Software exists that will make an "***image file"***

Image files *contains enough information so that software is able to recreate a bit-image copy of the source disk*

There exists approved "image file" software

Has been verified

Is accepted by legal courts

Image file software can adjust for a target disk that is not exactly the same as the source disk

For instance, if the target disk is larger than the source disk, you might still be able to achieve a bit-by-bit copy with the remainder of the target disk truly empty

Bit-by-Bit Copies

Here is a figure from Nelson

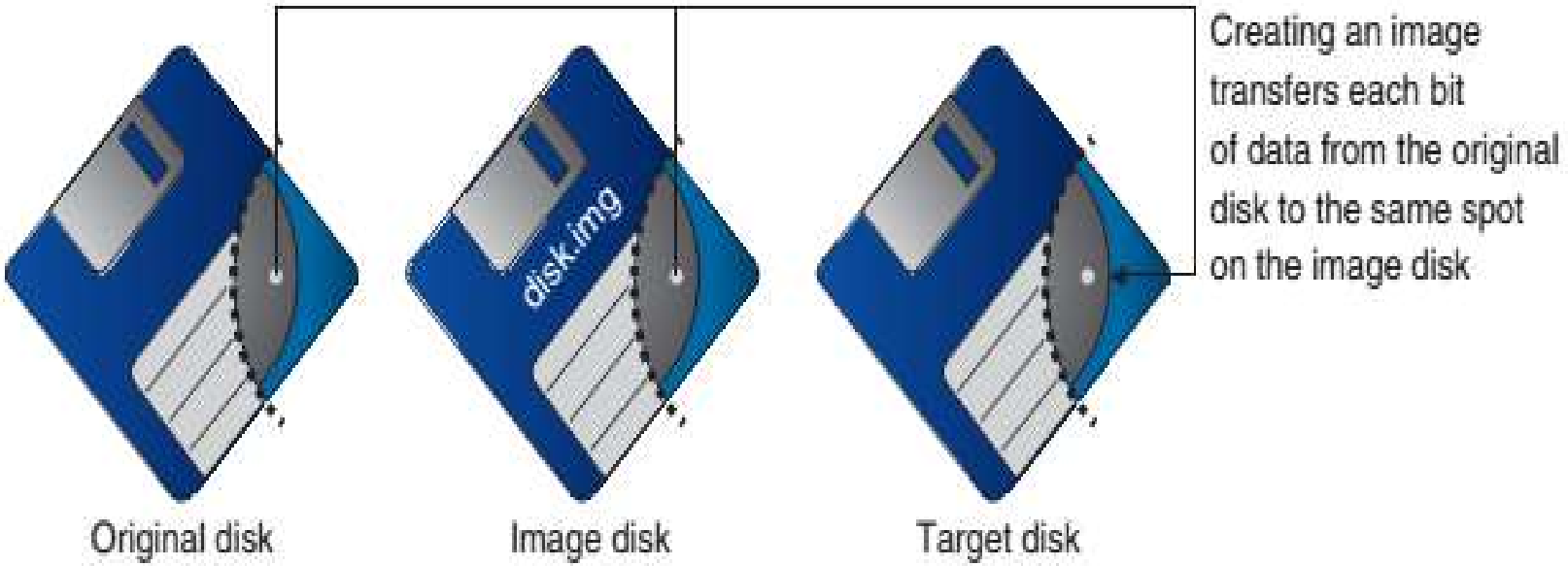
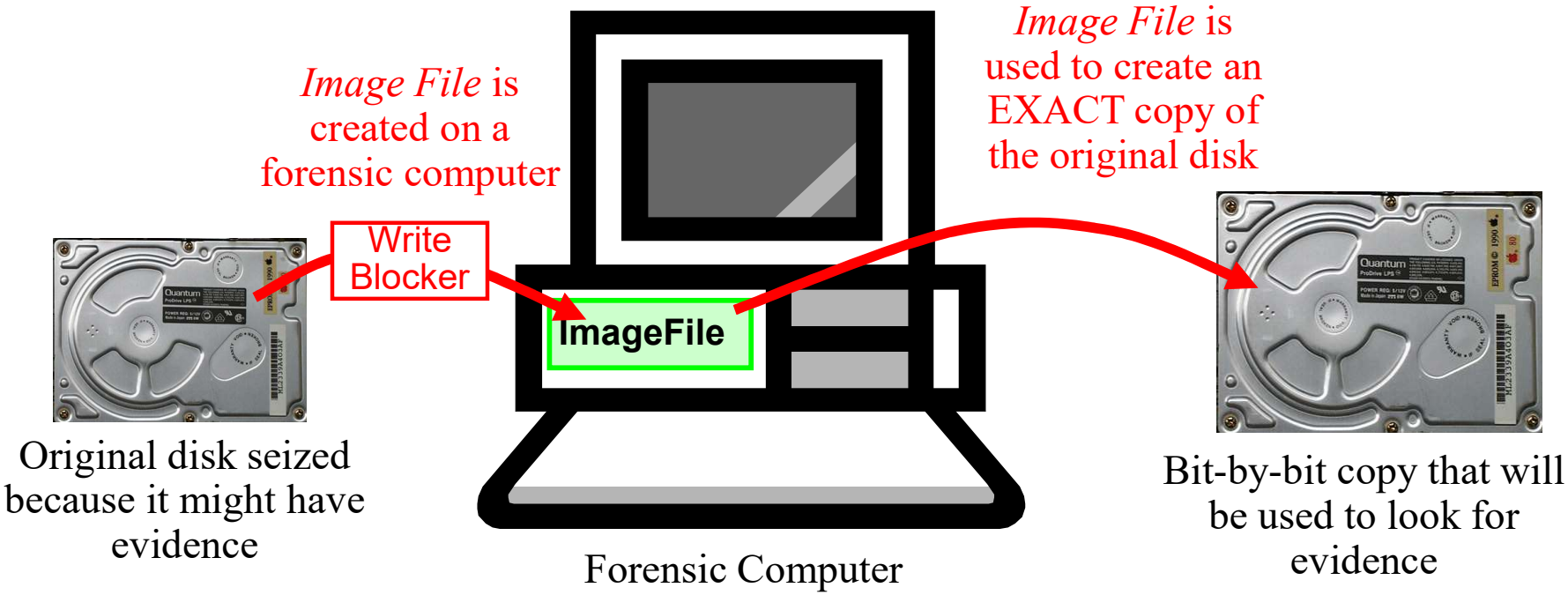


Figure 1-11 Transfer of data from original to image to target

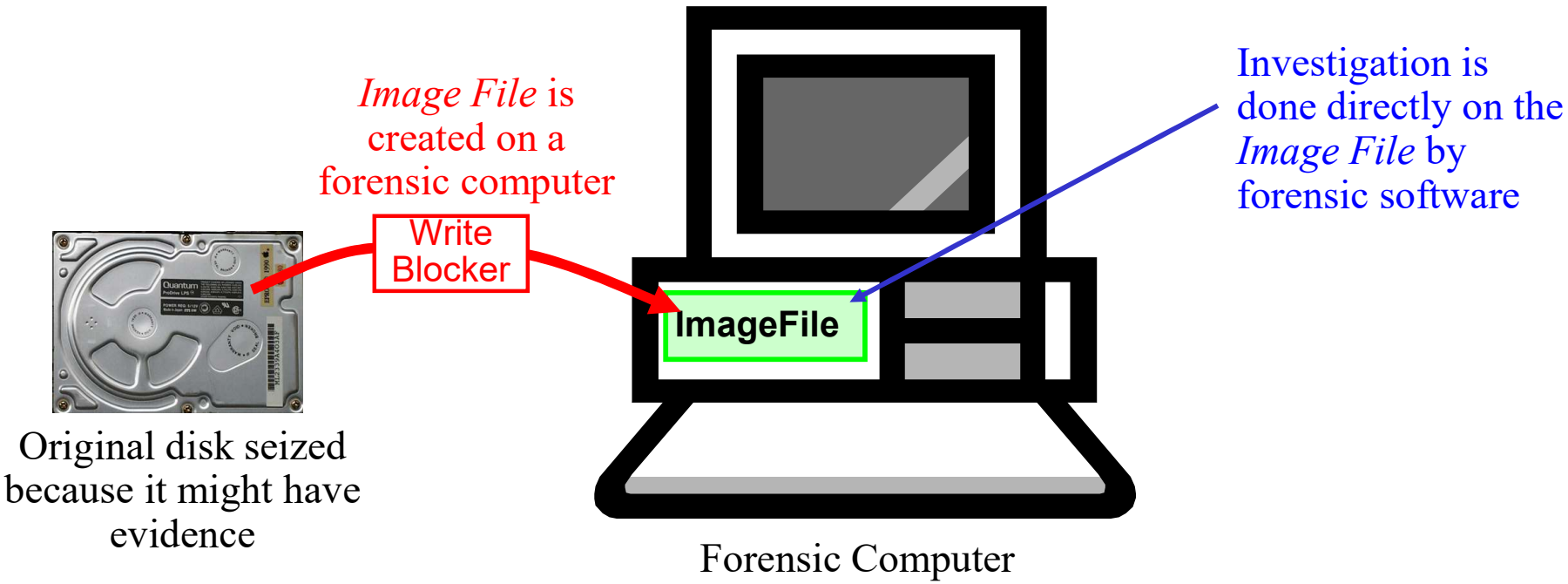
This is a misleading and obsolete figure. The middle image is usually a file on a hard disk.

Bit-by-Bit Copies



This is sometimes what goes on.

Bit-by-Bit Copies



But this is usually what typically happens

More on Bit-by-Bit (Image) Copies

More on Bit-by-Bit Copies

You can make a bit-by-bit (image) copies using many different tools

diskcopy	*(for diskettes only)*	*Comes with Windows OSs up to Win7*
Image		*Digital Intelligence*
FTK Imager		*AccessData*
ProDiscover		*Technology Pathways*
EnCase		*Guidance Software*
WinHex		*X-Ways Forensics*
dd		*All Unix/Linux distros*
Others		

Bit-by-Bit Copy Using *diskcopy*

Can be done from command line in any MS Windows OS up through Win7

diskcopy only works for diskettes

Creates neither a separate image file nor a hash

Not useable in legal court cases

1-step process

Original evidence disk → *Copy of evidence disk*

Diskette → *Diskette*

Bit-by-Bit Copy Using *image*

image creates an image file and a hash

Accepted by courts

Works with diskettes, flash drives or hard disks

2-step process:

Evidence Disk → *Image File* → *Copy of Evidence Disk*

Flash Drive → *File on Hard Drive* → *Flash Drive*

You can make more than one copy from the image file

Bit-by-Bit Copy Using
FTK Imager, dd, EnCase, ProDiscover *& WinHex*

FTK Imager, dd, EnCase, ProDiscover ***and WinHex*** create image files in several different formats

e.g., raw (dd), EnCase (e01), FTK (001), Ghost, ICS, Safeback and SMART formats

Several different hashes

Accepted by courts

Works with files, partitions, diskettes, optical format drives, flash drives or hard disks

Process:

original drive or file → *image file*

Can also clone the original disk or file

image file → *clone of original*

Imaging capability is free

Then What?

FTK, ***Autopsy,*** EnCase, ProDiscover, ***WinHex*** or other forensic software then can be used to analyze the image file directly, so you don't need to create a 2nd disk that is a cloned bit-by-bit copy of the evidence disk

All of the above run on any modern Windows OS

Autopsy also runs on Linux

Bit-by-Bit Copy Using *dd*

dd is the grandfather of all the cloning software

Free with all Unix and Linux distros

Versions for Windows exist

Has been around since 1960s

It is still the only "universal" cloning tool

Most imaging software includes ***dd*** as an option

dd makes a true bit-by-bit, sector-by-sector copy

Process

Source drive, partition or file → *Target*

Target can be a .dd image file or another disk

If a disk, it must be the same size or larger than the original disk

Lab 02a-3

Forensic Imaging

This is demonstration and discussion.

It use to be a lab.

First Steps in Process

Obtain the evidence from the custodian

Use chain of custody form

Next, make two (2) or more forensic copy sets, each set using different software

Each set should consist of:

A forensic physical image plus hashes

A forensic logical image plus hashes

Legally verify that all of the images are accurate

How?

Finally, return the evidence to the custodian

Use chain of custody form

What This Lab Used to Do

For actual evidence, students created:

MD5 of evidence

SHA1 of evidence

Using FTK Imager, students created

Physical and logical images of evidence

Then created

MD5 of physical image
SHA1 of physical image
MD5 of logical image
SHA1 of logical image

Using WinHex, students created:

Physical and logical images of evidence

Then created

MD5 of physical image
SHA1 of physical image
MD5 of logical image
SHA1 of logical image

Using ProDiscover, students created:

Physical and logical images of evidence

Then created

MD5 of physical image
SHA1 of physical image
MD5 of logical image
SHA1 of logical image

Results of What This Lab Used to Do

For actual USB drive, students used WinHex to take 2 hashes

USB drive size: 125, 952 KB

Then they took hashes of the USB drive.

MD5: 7213735569ef6a34e85840e67d05544a
SHA1: 2d1274be0c73067ca842aad90e03bdb4ae03aa37

Using FTK Imager, students created physical and logical **.001** images of the USB drive.

Physical image size: 125, 952 KB. Logical image size: 1,440 KB

Then they took hashes of the images.

MD5 of physical image: 7213735569ef6a34e85840e67d05544a
SHA1 of physical image: 2d1274be0c73067ca842aad90e03bdb4ae03aa37
MD5 of logical image: 2fcf64599b1d241cc4ba56aece1e8541
SHA1 of logical image: bcceaf6564da79741477f39fd97345ff25d88fa

Results of What This Lab Used to Do

Using WinHex, students created physical and logical **.dd** images of the USB drive.

Physical image size: 125, 952 KB. Logical image size: 1,440 KB

Then they took hashes of the images.

MD5 of physical image: 7213735569ef6a34e85840e67d05544a
SHA1 of physical image: 2d1274be0c73067ca842aad90e03bdb4ae03aa37
MD5 of logical image: 2fcf64599b1d241cc4ba56aece1e8541
SHA1 of logical image: cbcceaf6564da79741477f39fd97345ff25d88fa

Using Pro Discover Basic, students created physical and logical **.eve** or **.dd** images of the USB drive. Then they took hashes of the images.

MD5 of physical image: 7213735569ef6a34e85840e67d05544a
SHA1 of physical image: 2d1274be0c73067ca842aad90e03bdb4ae03aa37
MD5 of logical image: 2fcf64599b1d241cc4ba56aece1e8541
SHA1 of logical image: cbcceaf6564da79741477f39fd97345ff25d88fa

Imaging Results
Example from a past Lab

```
MD5
---
   PhyFtkMont   .001   7213733569ef6a34e85840e67d05544a   125,952 KB
   PhyProMont   .dd    7213733569ef6a34e85840e67d05544a   125,952 KB
   PhyWHxMont   .dd    7213733569EF6A34E85840E67D05544A   125,952 KB

   LogFtkMont   .001   7213733569ef6a34e85840e67d05544a   125,952 KB
   LogProMont   .dd    2fcd64599b1d241cc4ba56aece1e8541     1,440 KB
   LogWHxMont   .dd    2FCD64599B1D241CC4BA56AECE1E8541     1,440 KB

SHA1
----
   PhyFtkMont   .001   2d1274be0c73067ca842aad90e03bdb4ae03aa37   125,952 KB
   PhyProMont   .dd    2d1274be0c73067ca842aad90e03bdb4ae03aa37   125,952 KB
   PhyWHxMont   .dd    2D1274BE0C73067CA842AAD90E03BDB4AE03AA37   125,952 KB

   LogFtkMont   .001   2D1274BE0C73067CA842AAD90E03BDB4AE03AA37   125,952 KB
   LogProMont   .dd    cbcceaf6564da79741477f39fd97345ff25d88fa     1,440 KB
   LogWHxMont   .dd    CBCCEAF6564DA79741477F39FD97345FF25D88FA     1,440 KB
```

End of Lab 02a-3

Forensic Imaging

Lab 02a-4

Analyzing the Forensic Image

Analyzing the USB Drive Physical Image

Pages 43-52 (top) of Nelson

Use your RADISHng Win10 VM to do this.

We Can Do This Now

Although I said that I would demo or discuss most labs

But we can actually do this lab in class tonight

This is because Nelson, pp 43-52 are very detailed

It gives you step-by-step instructions about what to do

I've verified the pages

They all work as described with small exceptions.

Exceptions are due to changes in interface with newer versions of Autopsy

Analyzing Your Digital Evidence

Use your RADISHng Win10 VM to do all of this

Start at ***Analyzing Your Digital Evidence***, page 43 of Nelson

Do NOT do what is in the 1st Note near middle of p. 43

The latest version of Autopsy (v 4.19.3) is already installed for you.

There should be a shortcut on your Win10 Rng desktop

Prior to Opening Autopsy

The 2nd note near the bottom of p 43 tells you what to do

Create the folder C:\Work\Chap01\Chapter\ on your RADISHng VM

Instead of doing step 1 below the note, do the following:

Copy the file

R:\share\Labs\Chapter1\Ch01InChap01.dd → C:\Work\Chap01\Chapter\

Start Autopsy

Now do from

Step 2 on the bottom of p 43 to step 5 located below Figure 1-14 on p 45.

Modifications to text procedure:

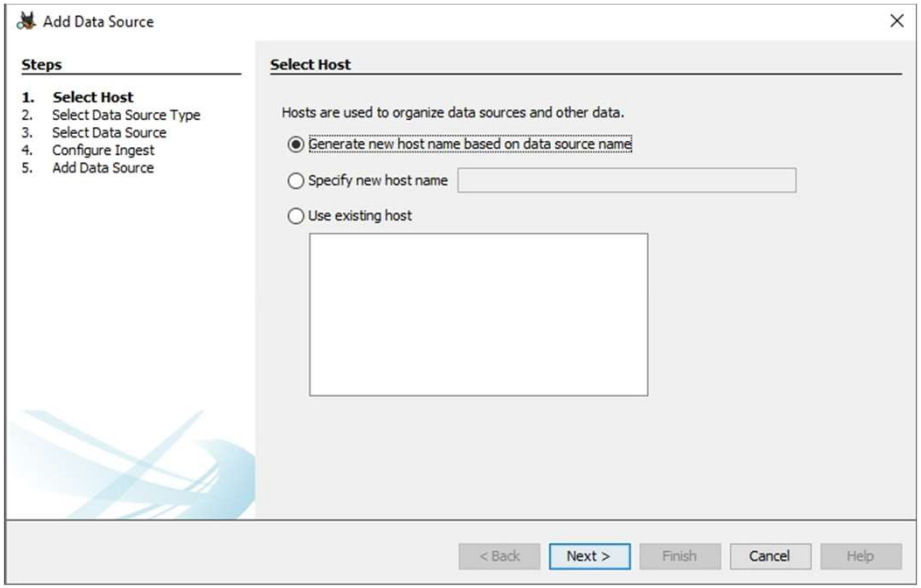
Step 2 is now a little different

Navigate to C:\Work\Chap01\Chapter

Click "Select"

Before **Step 4**, you will see a Add Data Source window (see right)

Use the default option (generate new host name). Click "Next".



Now **STOP!**

Let's make sure that we're all in sync.

Analyzing the Image

Start with step 1 near the bottom of p 45

Continue through step 7 on page 47.

There are a few differences between version's 4.3.0 and 4.19.3

Now **STOP after step 7**

Again, let's make sure that we're all in sync.

Finish Analysis

Finish up by going through from the bottom of p 47 to the top of p 52.

The Report Generator is sparse for this device, but there are items there

I've found that the law wants information that is more easily understood.

DN0

Conclusions
Domain Name Case

Is the information that you gathered accurate and without artifacts or missing info?

Was George Montgomery

Using his firm's computer in a private business?

What's your evidence?

Doing it on company time?

What's your evidence?

Was a goal of George's private business to make money?

What's your evidence?

Slide 94

DN0 Answer the questions in the notes

Don Nelson, 2022-08-31T23:07:03.815

Critique the Case
After You Complete It

After every case, ask yourself the following questions:

How could you improve your performance in the case?

Did you expect the results you found? Did the case develop in ways you did not expect?

Was the documentation as thorough as it could have been?

What feedback has been received from the requesting source?

Did you discover any new problems? If so, what are they?

Did you use new techniques during the case or during research?

Upcoming Assignments

Assignments

Reading/Discussion (Assign02a_rd)

Read Chapter 2 in Nelson text

Discussion boards

Respond to someone else's thread in Chapter 1 board

Create new thread in Chapter 2 board

Submit (Assign01b_s)

Log into your RADISH desktops and submit screenshots

Complete the Chapter1/Montgomery_72018 lab and submit artifacts/report