

# Cyber Security Technologies

## **Session 14 – Computer Forensics**

**Shawn Davis**  
ITMS 448 – Spring 2016

Slides contain original content from Davis, S.

# File Copy

- Logon to your RADISH Win8.1 VM
- We will also use your Kali VM
- In your RADISH Win 8.1 VM, copy the Forensic Tools folder to your desktop from M:\Tools
- Pull up the Week 14 In-Class Labs pdf from Blackboard

# Homework9 & 11 Review

- I will go over these assignments and answer any questions

# Homework9 Seth E.C. Script

```
#!/bin/bash
#get variables from command line
key=$1
file=$2

#store array of cipher
typesciphers=("aes-128-cbc" "aes-128-ecb" "aes-192-cbc" "aes-192-ecb" "aes-256-
cbc" "aes-256-ecb" "camellia-128-cbc" "camellia-128-ecb" "camellia-192-cbc"
"camellia-192-ecb" "camellia-256-cbc" "camellia-256-ecb" "des3" "rc2-40-cbc"
"rc2-64-cbc" "rc2-cbc" "seed-cbc" "seed-ecb")

for i in "${typesciphers[@]}";
do
    openssl $i -base64 -d -k $key -in $file -out decrypted.txt 2> output.txt
    if egrep "bad decrypt|error" output.txt
    then
        echo "WRONG!"
    else
        echo "FOUND IT! Decrypted text is now in decrypted.txt"
        break
    fi
done
```

# Homework9 Seth E.C. Script

```
root@448K-01:~# ./seth wheaton plans
bad decrypt
140666978821776:error:06065064:digital envelope routines:EVP_Decrypt
Final_ex:bad decrypt:evp_enc.c:544:
WRONG!
bad decrypt
139757415622288:error:06065064:digital envelope routines:EVP_Decrypt
Final_ex:bad decrypt:evp_enc.c:544:
WRONG!
FOUND IT! Decrypted text is now in decrypted.txt
```

```
root@448K-01:~# cat decrypted.txt
The DDOS on ExelCorp will occur on 050516
```

# Today

- This lecture will focus on Windows Forensics as it is the most common Operating System
- We will not cover Mobile Forensics in this lecture
- We will also not cover Network Forensics as we covered that in the IDS/IPS and Exploit Kit lectures

# Overview

Part I – Forensics Overview & Laws

Part II – Forensic Acquisition/Imaging

Part III – Forensic Analysis

# Part I

---

# Forensics Overview & Laws



# Forensics: Three Main Parts

- Evidence Acquisition
  - Determining systems involved
  - Collecting volatile and non-volatile evidence through forensic imaging
- Evidence Analysis
  - Investigation to determine what happened
  - File and artifact extraction
  - Forming of timeline of events
- Reporting
  - Creation of report detailing findings

# Types of Legal Cases

- Criminal
  - Local, State, or Federal government prosecutes a case in which a person (defendant) is charged with a crime
- Civil
  - Person, company, or government agency acts as a plaintiff and files a lawsuit against an individual, company, or government agency (defendant).

# Evidence Acquisition

- Forensic acquisition generally involved acquiring evidence in support of one of the following entities:
  - Prosecution:
    - Legal enforcement body that filed a criminal complaint
  - Plaintiff:
    - Individual filing a civil suit
  - Defendant:
    - Individual being sued in a civil suit or charged in a criminal case

# Common Criminal Case Types Involving Forensics

- Child Exploitation
- Data Breaches / Attacks
- Intellectual Property Theft
- Fraud
- Murder
- Espionage
- Terrorism
- Violation of Various Other State/Federal Laws

# Common Civil Case Types Involving Forensics

- Intellectual Property Theft
- Employment Discrimination
- Evidence Spoliation
- Violation of Various Other State/Federal Laws

# Some Federal Laws Involving Computer Forensics

- Computer Fraud and Abuse Act (CFAA)
- Electronic Communications Privacy Act (ECPA)
- Digital Millennium Copyright Act (DMCA)

# Computer Fraud and Abuse Act (CFAA)

- Gain unauthorized access to a “protected” computer:
  - To harm U.S. or benefit foreign nation
  - To obtain protected financial or credit information
  - With intent to defraud
  - To damage it (malware, etc.)
  - To engage in trafficking of computer passwords
  - To threaten it with intent of extorting money

# “Protected Computer”

- Computer in use by U.S. Govt. or financial institution
- Computer involved in interstate or foreign commerce or communication\*
  - \*This applies to most every computer



# Electronic Communications Privacy Act (ECPA)

- Illegal to intercept stored or transmitted electronic communication without authorization
- Includes any transfer of signs, signals, writing, images, sounds, data, or intelligence transmitted in whole or in part by wire, radio, electromagnetic, photo electronic, or photo optical system that affects interstate or foreign commerce.

# Digital Millennium Copyright Act (DMCA)

- Prohibits circumventing a technological measure designed to protect a copyright
- Examples:
  - Keygens
  - Circumventing DVD anti-piracy measures
  - Accessing online videos without permission
  - Reverse engineering of software
  - Etc.

# Famous Cases Involving Computer Forensics

- Dennis Rader
  - Police used EnCase to retrieve metadata identifying BTK serial killer from deleted Word document on floppy disk
- Dr. Conrad Murry
  - Investigators found documentation on his computer that he authorized lethal amounts of propofol which resulted in Michael Jackson's death

# Famous Cases Involving Computer Forensics

- Krenar Lusha
  - Forensic experts discovered instructions on his laptop for building suicide belts and explosives
- Casey Anthony
  - Sheriff's department processed forensic evidence of her computer but only looked at Internet Explorer artifacts
  - They failed to extract browser history from Firefox which showed searches for "how to make chloroform," "neck breaking," and "foolproof suffocation."
  - Casey was found not guilty in death of her daughter

# Jobs in Forensics

- Federal Government
  - FBI RCFL
  - Secret Service
  - State Department
  - NCIS, Army CID
  - NSA, CIA
  - Postal Service OIG
  - Veteran's Administration
  - Defense Cyber Crime Center (DC3)
- State Government
  - State Police
  - Attorney General
  - Office of Inspector General
  - Sheriff and City Police Depts.

# Jobs in Forensics (Cont.)

- Consulting Companies
  - KPMG
  - Deloitte
  - Trustwave
  - Stroz Friedberg
  - Forensicon
  - 4Discovery
  - Navigant
  - DTI
  - Dell Secureworks
  - Ernst & Young
  - PwC
  - Verizon
- In-House for Companies
  - Motorola
  - Allstate
  - United
  - Most Fortune 100 companies

# Jobs in Forensics (Cont.)

- Government Contractors
  - Booz Allen Hamilton
  - Lockheed Martin
  - Raytheon
  - Northrop Grumman

# Chicago RCFL

- Partnership of computer forensics professionals from following organizations:
- CPD, Cook County Sheriff, Cook Country State Attorney, Joliet PD, Lombard PD, Oak Park PD, Palatine PD, Berwyn PD, Aurora PD
- FBI
- US Customs and Border Protection



# E-Discovery

- Electronic Discovery is the process of identifying, preserving, collecting, preparing, reviewing, and producing of Electronically Stored Information (ESI) in the context of the legal process
- Can happen in criminal or civil cases
- Litigation holds often issued to ensure ESI in connection with pending or reasonably anticipated litigation is not destroyed or deleted

# Forensics vs. E-Discovery

- Forensics is the technical and investigative aspect of acquiring and analyzing electronic information
- E-Discovery identifies and organizes information collected from computer forensics as well as other ESI such as:
  - Electronic Images
  - PDFs, Word Docs
  - Databases, Spreadsheets
  - Etc.

# Selecting a Forensic Workstation

- Isolated from Internet and fully patched
- Write Blockers
- Various Interfaces (SAS, SATA, IDE, USB, Firewire, Etc.)
- Imaging Software
- Analysis Software
- Reporting Software

# Part II

---

# Forensic Acquisition/Imaging

# Rule 401 – Definition of “Relevant Evidence”

- Evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.

# Evidence Examples

- Files / Deleted Files
  - Images, Documents, Videos, Etc.
- Browser Artifacts
  - History, Cache, Cookies, Etc.
- Email
  - Local or Cloud Based
- Location Data
- Evidence of Malware or Attack

# Evidence Preservation

- Admissibility
  - Evidence must be relevant and authentic
- Integrity
  - Evidence must not be altered and hashing must be used to prove that
- Chain of Custody
  - Guarantee identity and integrity of evidence item as case progresses from collection to court testimony

# Write Blocker

- Simply turning on a computer will cause changes to occur to the disk which could change timestamps, remove deleted file artifacts, etc.
- A write blocker allows a read only connection to a drive so no changes to the drive can occur



# Hardware Write Blocker

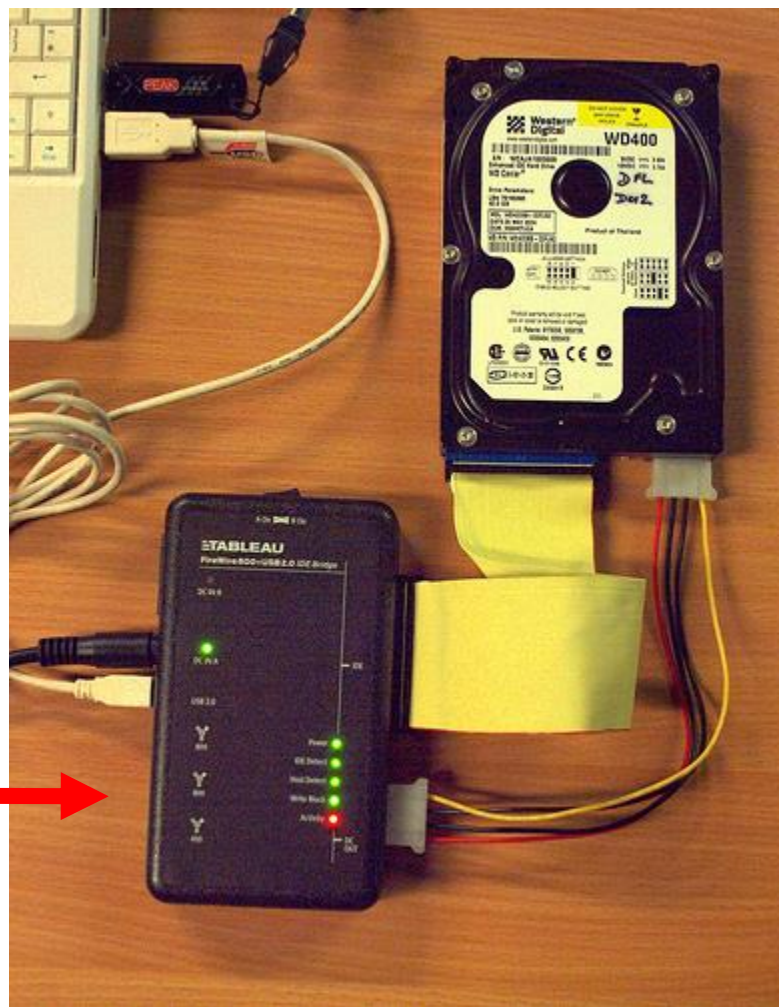
- Uses a device between the evidence drive and the acquisition drive in order to block writing to the evidence drive
- Interface can be USB, Firewire, IDE/PATA, SAS, SATA, eSATA, Card Reader, etc.
- Some examples:
  - <http://www.digitalintelligence.com/forensicwriteblockers.php>
- \$349 - \$459

# Tableau Hardware Write Blocker

Acquisition Computer  
(which can use its  
internal drive to store  
the image or an  
external drive)

Evidence Drive

Write Blocker



# Software Write Blocker

- Uses software to block writing to a particular interface

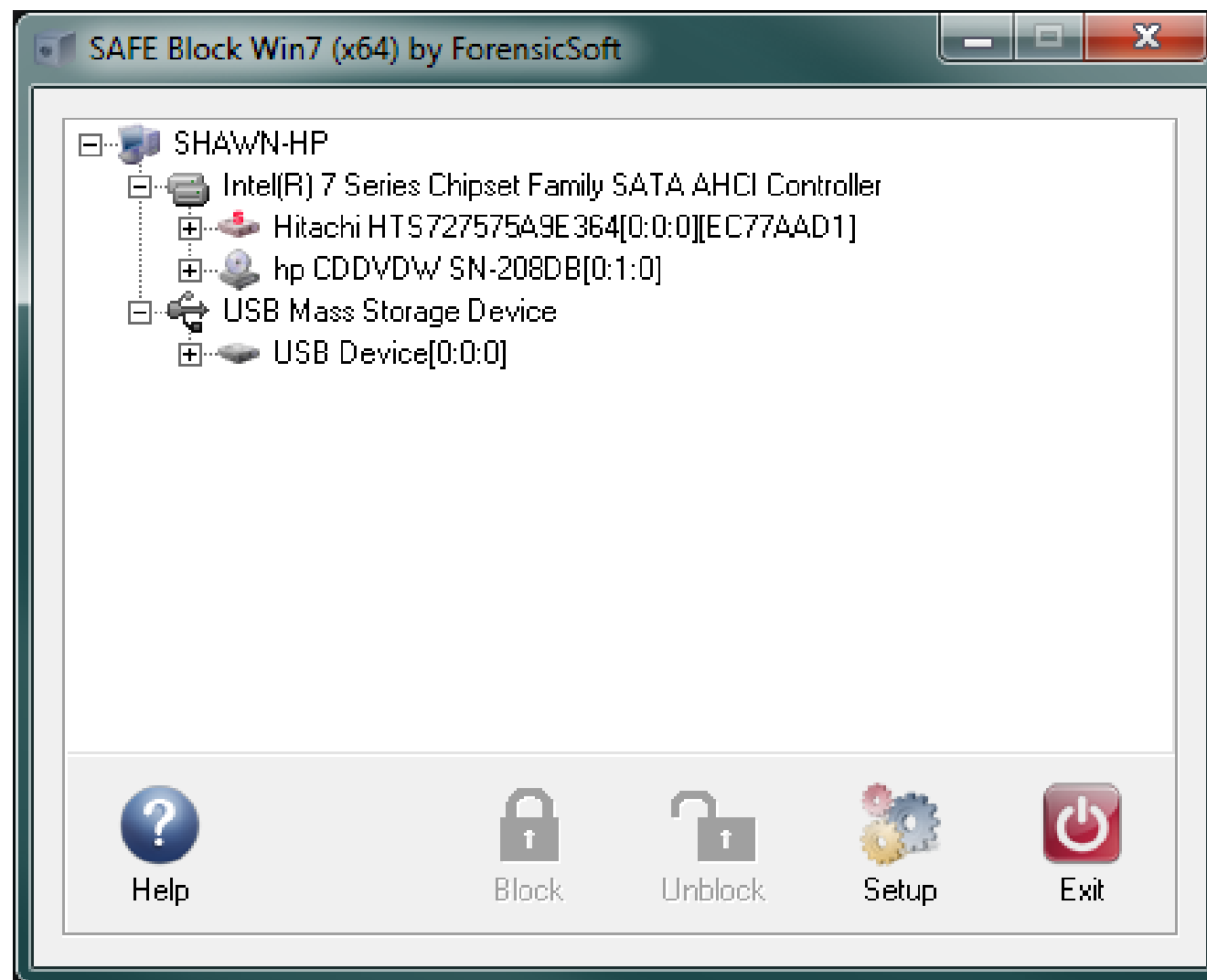
## Windows Registry Method – Software Write Blocker

- Windows has a registry shortcut that can be created to block writing to all USB ports
- Can work nicely if you are imaging an external USB drive or drive in a USB enclosure and will store the image directly on your computer
- An issue occurs when you need to also connect an external USB drive to hold the resulting image as well as writing to that drive would also be blocked
- Example instructions here:
  - <https://samsclass.info/121/proj/p5-USB-writeblock-registry.pdf>
- May not be a fool proof method!

# ForensicSoft SAFE Block Software Write Blocker

- Can be used to selectively block interfaces
- Block writing on one for evidence drive
- Allow writing on another for acquisition storage drive
- Tested to ensure no writes occur
- \$219 - \$549

# ForensicSoft SAFE Block Software Write Blocker



# Allocated vs. Unallocated Space

- Allocated
  - Active files on the filesystem that may be in use
  - Doesn't include deleted files
  - Most evidence found here
- Unallocated
  - Free Space
  - Non-active files
  - Deleted files or fragments of former files found here
  - Some evidence occasionally found here

# Partitioned vs. Un-partitioned Space

- Partitioned Space
  - Holds a filesystem
  - Can be used as a volume to store files or can hold an Operating System
  - Identified by logical drive letters C:, D:, etc.
- Un-partitioned Space
  - Space on disk not in use and not occupied by a partition



# Clusters & Slack Space

- Cluster:
  - Disk Sectors grouped into blocks called clusters
  - Every file needs its own cluster
  - There is often free space that is wasted if a file doesn't fill up an entire cluster
- Slack Space:
  - Free space between the logical end of a file and the end of the cluster
  - Evidence can occasionally reside in this space

# Evidence Acquisition\*

- Physical Drive Images
- Logical Drive Images
- Contents of a Folder
- Memory Acquisition

\*Above are four options in FTK Imager

# Physical Drive Images

- Bit by Bit copy of entire physical hard drive
- Contains allocated and unallocated space
- Contains partitioned and un-partitioned space
- Contains deleted files, fragments of files, etc. from entire disk
- Contains file system metadata

# “Logical Drive Images”\*

- Bit by Bit copy of drive partition only such as C:
- Contains only contents from partitioned space
- Contains allocated and unallocated space only from selected partition
- Contains deleted files, fragments of files, etc. only from selected partition
- Contains file system metadata

\*FTK Imager option. Some software's logical images may not contain unallocated space or deleted files

# Contents of a Folder

- Only contains active files in a folder
- Also, sometimes referred to as a “Logical Image” which can lead to confusion
  - Not the same thing as a “Logical Drive Image”
- Not a bit by bit copy
- Does not contain unallocated space, deleted files, file fragments, filesystem metadata, etc.

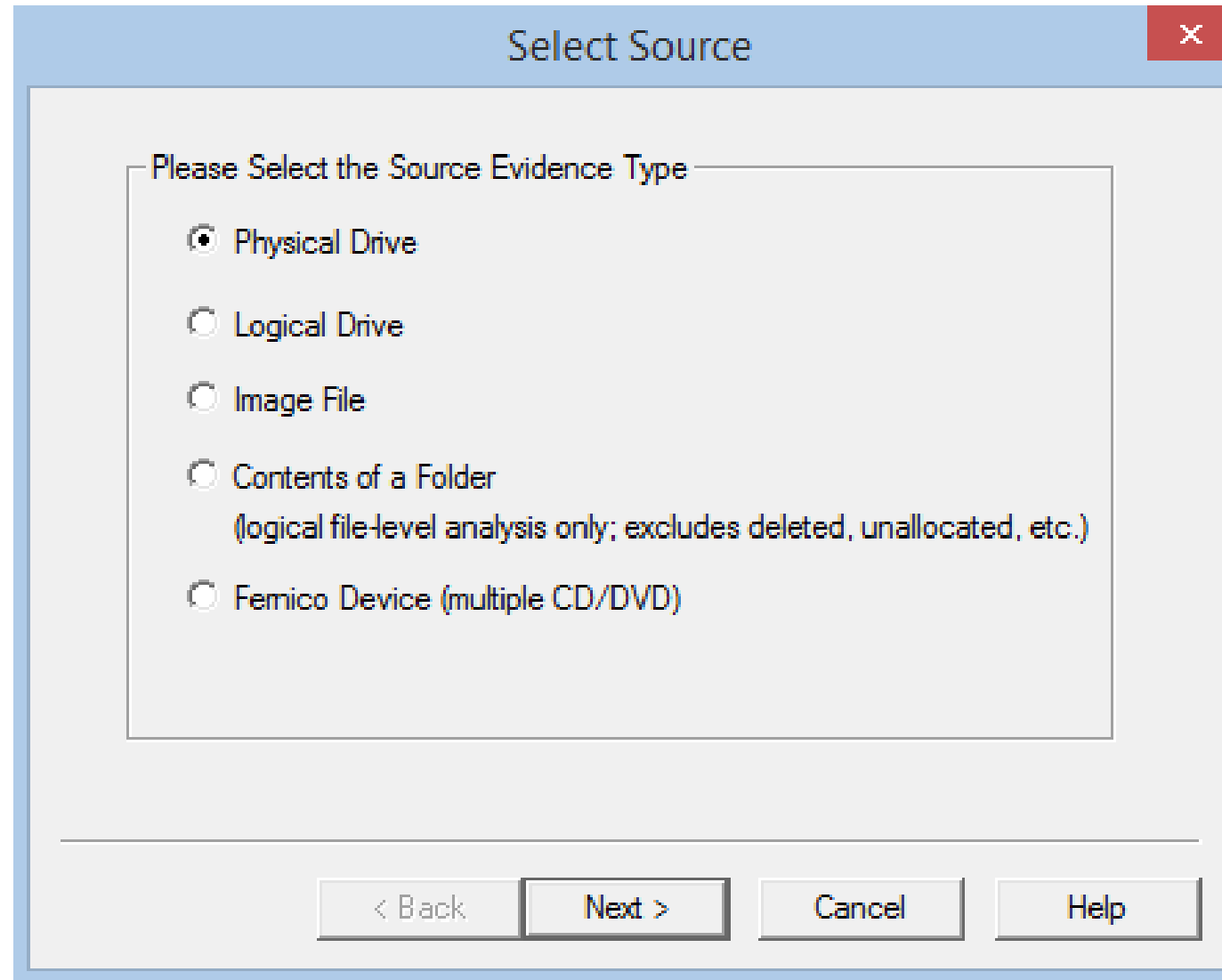
# Memory Acquisition

- Collection of volatile memory (RAM) from running system
- May contain information on:
  - Encryption Keys
  - Malware / Root Kits
  - Open Files
  - Network Connections
  - Running Processes
  - Etc.

# FTK Imager

- FTK Imager is a free acquisition tool that can acquire all four of the previous types of images
- It can also:
  - Capture memory and registry files
  - Be used to preview evidence on a live system
  - Be used to mount previously taken images as drives to review
- FTK does **not** write block evidence

# FTK Imager





# Dead vs. Live Acquisitions

- Dead Acquisition:
  - Computer is off when you arrive
  - Don't turn it on
  - Drive is removed and physical image is taken
- Live Acquisition:
  - Computer is running
  - What you do next is dependent on a few things...

# Dead vs. Live Acquisitions

- The old standard was to pull the plug on a running computer, take out the drive, and perform a physical image on it
- Why wouldn't we want to do that now???
  - We would lose all of the artifacts in memory that are volatile and would disappear!
  - Computer might also have full disk encryption and examiner wouldn't be able to logon when restarting it but could have grabbed the decryption key from RAM while the system was running

# Steps For Live Acquisition

- Always check to see if a system has full disk encryption before shutting it down
- One free tool is the Encrypted Disk Detector:
  - <https://www.magnetforensics.com/free-tool-encrypted-disk-detector/>
- If you are certain it is not encrypted:
  - Capture the RAM anyways for other artifacts
  - Shut down the computer, pull the drive, and take a physical image of it

# Dead vs. Live Acquisitions (Cont.)

- If system's drive is encrypted:
  - Capture the RAM and the Protected Registry Files
  - Perform a "Logical Drive" image or "Export to Logical Image" (for files/folders) with FTK and you will capture the unencrypted data

# Steps For Live Acquisition

- There might be also be times where you encounter a non-encrypted computer or server that cannot be shut down
- Then, you would:
  - Capture the RAM and Registry Files with FTK
    - Registry files cannot be copied from a live running system through the Windows OS
  - Use FTK to perform a physical drive, logical drive, or logical folder image.

# Dead vs. Live Acquisitions (Cont.)

- Note, that FTK does allow you to use their “Physical Drive” image function on a live system
- However, if encrypted, you will simple have an image of the encrypted data

**Go to:**  
**In-Class Lab 1 Slides**

# Imaging Hand's On

- In your RADISH VM 8.1 VM:
  - Create a folder on the Desktop called Sales Docs
  - Create a text file called sales1 and sales2 in the Sales Docs folder
  - Put a random sentence in each one and save the files
  - Delete the sales2 file
  - Close the Sales Docs folder

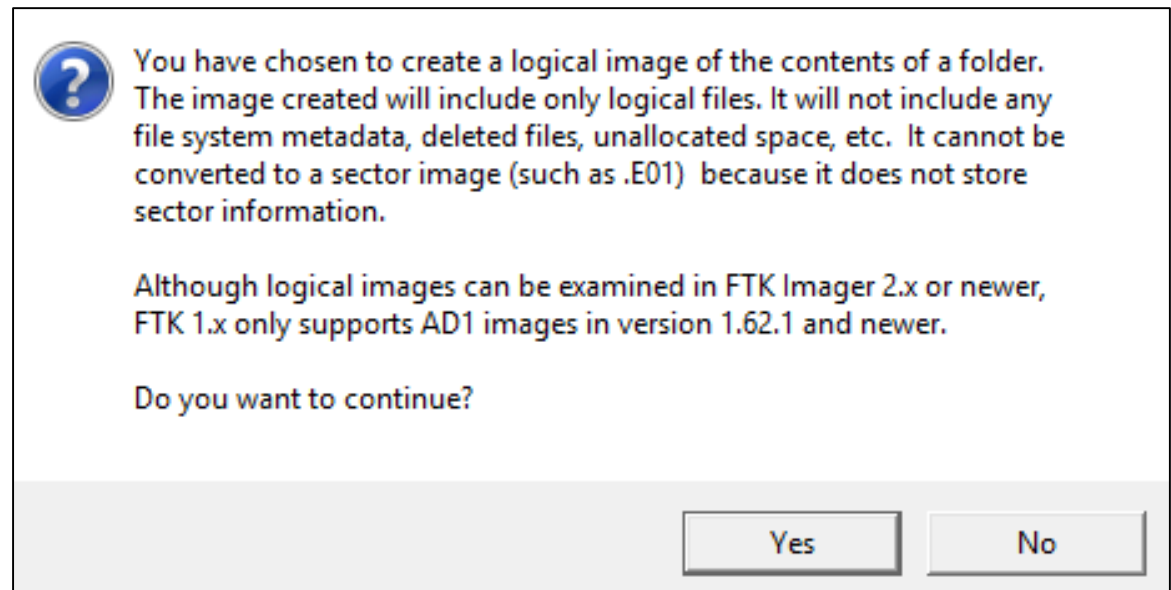
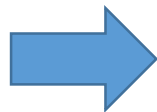


# Imaging Hand's On

- In your RADISH Win 8.1 VM, if you haven't already done so, copy the Forensic Tools folder to your desktop from M:\Tools
- Open the FTK Imager Lite folder and launch FTK Imager
- For UAC:  
**.\student  
student**

# Imaging Hand's On

- We will practice taking an image of a folder on a live system
- In FTK Imager:
  - File / Create Disk Image / Contents of a Folder
  - Hit Next
  - Yes to warning



# Imaging Hand's On

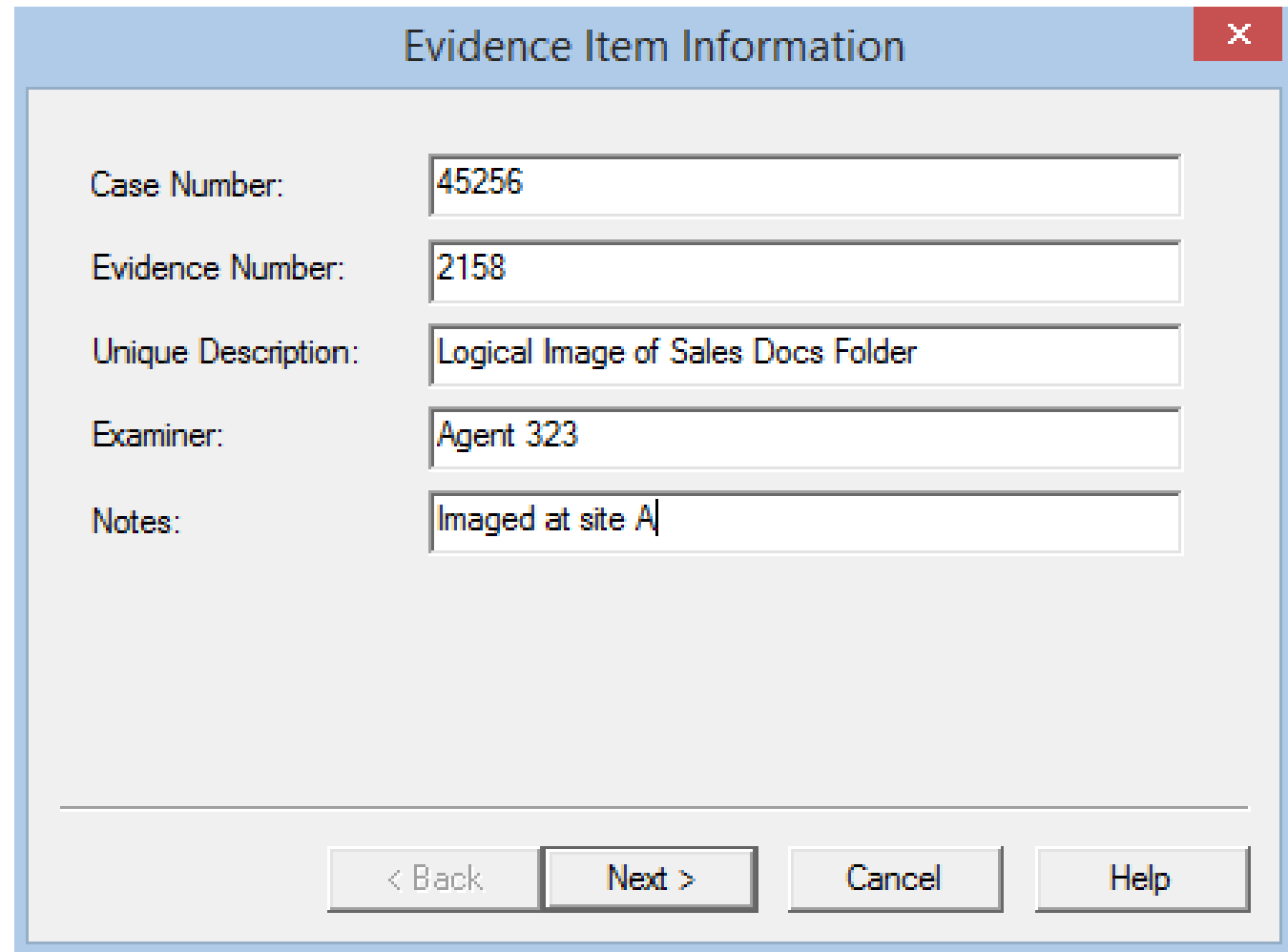
- Select “Browse”
- Choose “This PC” / PersistentDataDisk (D:) / Users / *yourname* / Desktop / Sales Docs
- Hit “OK”
- Selected Finish

# Imaging Hand's On

- We have now added our image source
- Now we need to select the destination for the image file
- Normally, we would set this to be an external drive but for today, will just select our Desktop in a second
- Make sure “Verify images after they are created” and “Create directory listings...” are both checked

# Imaging Hand's On

- Hit “Add...”
- Enter the following info:
- Hit “Next”



A screenshot of a software dialog box titled "Evidence Item Information". The dialog box has a light blue header bar with a red close button (X) in the top right corner. The main area is white and contains five labeled text input fields. The labels are "Case Number:", "Evidence Number:", "Unique Description:", "Examiner:", and "Notes:". The corresponding input values are "45256", "2158", "Logical Image of Sales Docs Folder", "Agent 323", and "Imaged at site A". At the bottom of the dialog box, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

Field Label	Value
Case Number:	45256
Evidence Number:	2158
Unique Description:	Logical Image of Sales Docs Folder
Examiner:	Agent 323
Notes:	Imaged at site A

Buttons: < Back, Next >, Cancel, Help

# Imaging Hand's On

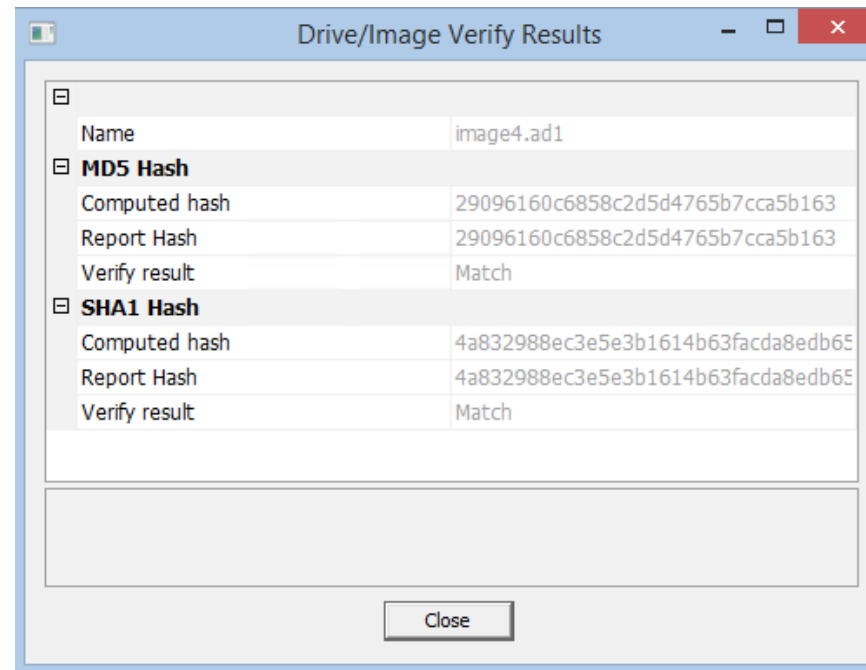
- Hit “Browse”
- Choose “This PC” / PersistentDataDisk (D:) / Users / *yourname* / Desktop
- Hit OK

# Imaging Hand's On

- Enter image4 as the “Image Filename”
- Keep “Image Fragment Size” as 1500
  - You would only use this if you needed to break a large image apart into several chunks to fit on small separate media such as CDs or DVDs
- Leave the compression setting as is
- Don't select “Use AD Encryption”
  - Why might you want to encrypt a forensic image?
- Don't select “Filter by File Owner”

# Imaging Hand's On

- Hit “Finish”
- Hit “Start” and it will finish quickly
- Notice the hash calculation before and after the image match:





# Imaging Hand's On

- Hit “Close”
- Hit “Close” again
- Look at the “Image Summary”
- Hit “OK”
- Hit “Close”
- Your desktop should now contain three new files

# Imaging Hand's On

- image4.ad1 is the actual image that can now be used in analysis programs or opened in FTK
- image4.ad1.txt contains the image summary
- image4.ad1.csv contains the directory listing of all of the files recovered
  - Right click on image4.ad1.csv and hit “Edit with Notepad++”

# Imaging Hand's On

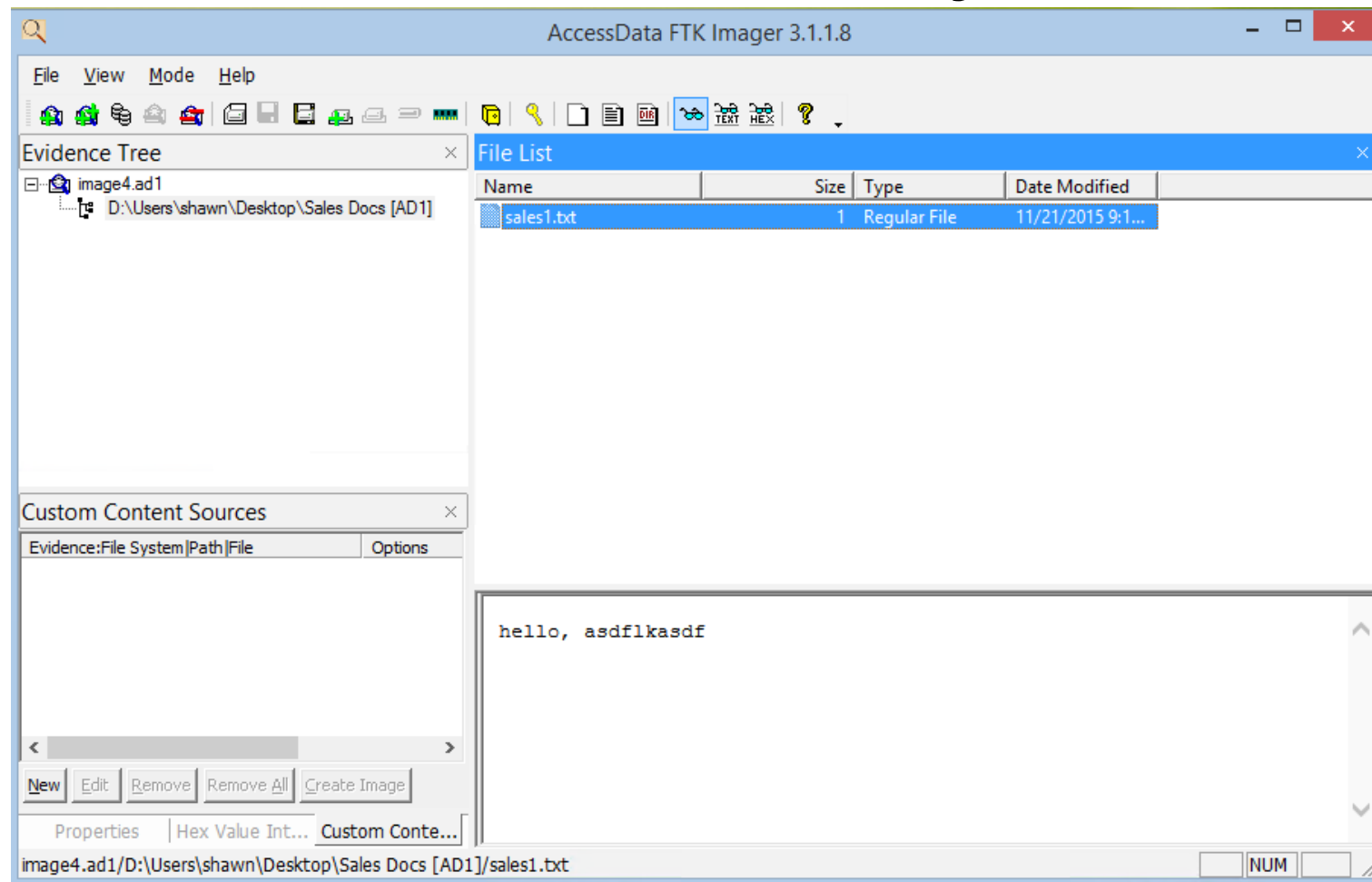
- You should see sales1.txt in there. Why is sales2.txt not listed???
- The logical folder image option does not capture unallocated space and therefore does not contain deleted files

# Imaging Hand's On

- Close Notepad++
- We can also use FTK to view our image
- File / Add Evidence Item / Image File / Next
- Browse to the image4.ad1 file on your Desktop
- Hit "Finish"

# Imaging Hand's On

- Expand the tree on the left side and you will see the file



# Imaging Hand's On

- File / Remove All Evidence Items
- Leave FTK Imager Lite open

# Imaging Hand's On

- FTK can also be used to capture the registry from a live system
  - File / Obtain Protected Files
  - Select Destination Path as your user's Desktop
    - Choose "This PC" / PersistentDataDisk (D:) / Users / *yourname* / Desktop / Sales Docs
  - There are two options:
    - Minimum files for logon password recovery (Copies SAM)
    - Password Recovery and all registry files (SAM and all hives)
  - Choose the "Password Recovery and all registry files"
  - "OK"

# Imaging Hand's On

- You should see that the system, software, default, and SECURITY hives as well as the SAM were captured.
- We'll talk about those in the next section
- You can close FTK Imager



# **In-Class Lab 1 - Complete**

# Memory Acquisition

- FTK can also be used to capture the volatile memory from a live system
- We will **not** demo this but the steps would be:
  - File / Capture Memory
  - Select Destination Path
  - Include pagefile (Swap file for Windows)
  - Create AD1 file
  - Hit “Capture Memory”

# Example of Acquisition Engagement

- You work for a 3<sup>rd</sup> party forensics firm and were hired on behalf of a plaintiff that is suing a former employee for trade secret theft in a civil suit
- A court has ordered that evidence can be collected
- You arrive at the defendant's home need to image their personal desktop which is turned on when you arrive
- You check and determine there is no full disk encryption software

## Example of Acquisition Engagement (Cont.)

- You capture the memory anyways as it could become useful later
- You shut down the computer and remove the hard drive and write down the serial number on a chain of custody form
- The evidence drive is 80GB and is connected to a write blocker with SATA and the write blocker is connected to the technician's laptop via USB 3.0

## Example of Acquisition Engagement (Cont.)

- The technician's laptop has an external 160GB USB 3.0 drive connected to it to store the resultant image
- The technician uses FTK and creates a physical image by selecting the 80GB evidence drive as the source and the 160GB external USB 3.0 drive as the image destination

## Example of Acquisition Engagement (Cont.)

- After completion, the technician arrives at the plaintiff's building and images all of the computers that the employee used while working there as well as their PST file containing their email

# Part III

---

# Forensic Analysis

# Forensic Analysis

- Once all evidence is collected and imaged, analysis can start
- Analysis is not simply recovering artifacts
- It is about finding evidence to answer specific questions relevant to the case!
- Also, creating an accurate timeline of when things happened is very important as well.



# Forensic Analysis Potential Questions

- Was a computer used to:
  - Transmit malware?
  - Open a specific file?
  - Send a specific email or emails?
  - Steal information onto a USB key?
  - Used in a hacking attack and connected to a specific access point?
  - Search the internet for specific terms?
  - Download restricted information or images?

# Forensic Analysis Categories

- String Searching / Data Carving / Artifacts / Log Files
- Registry Forensics
- Browser Forensics
- Email Forensics
- Memory Forensics

# Part III - I

---

**String Searching / Data Carving /  
Artifacts / Log Files**

# Mainly involves:

- Searching for strings in active and deleted files
- Carving or recovering deleted files from unallocated space
- Analyzing various artifacts
- Viewing images
- Etc.

# Forensic Analysis Suites

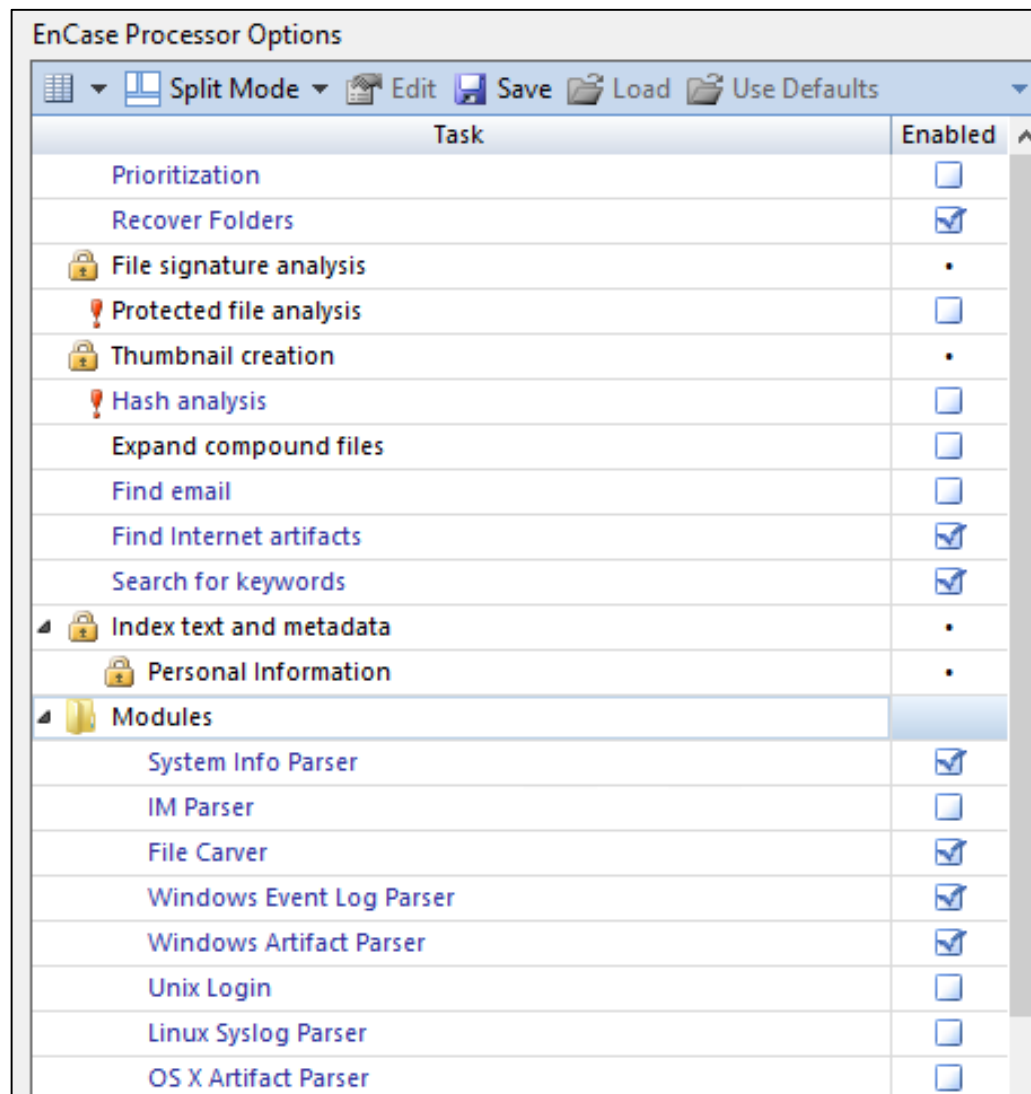
- Paid:
  - EnCase
  - FTK
  - X-Ways
- Free:
  - Autopsy/TSK
  - ProDiscover

**Go to:**  
**In-Class Lab 2 Slides**

# EnCase Hand's On

- I previously used an XP VM to perform various tasks and then took a live image of it
- I then previously performed the following in EnCase:
  - Created a new case
  - Added the evidence file
  - Selected the processing options

# EnCase Hand's On





# EnCase Hand's On

- Guidance Software offers good free videos if you want to know how to create a new case, add evidence files, select processing options, and perform other tasks
- <https://www2.guidancesoftware.com/training/Pages/encase-essentials.aspx>
- We are now going to analyze an existing case file where everything was already processed

# EnCase Hand's On

- In your Win 8.1 VM, open Forensic Tools\Evidence from your Desktop
- Open a second File Explorer and go to Local Disk C:
- Drag the EnCase Case folder to an empty spot on the Local Disk C: folder in the second window
- Go back to the Evidence folder on the first Window and open the “Image” folder
- Drag the case39344 file to an empty spot on the Local Disk C: folder in the second window
- Hit “Continue” if prompted (.\\student and student)

# EnCase Hand's On

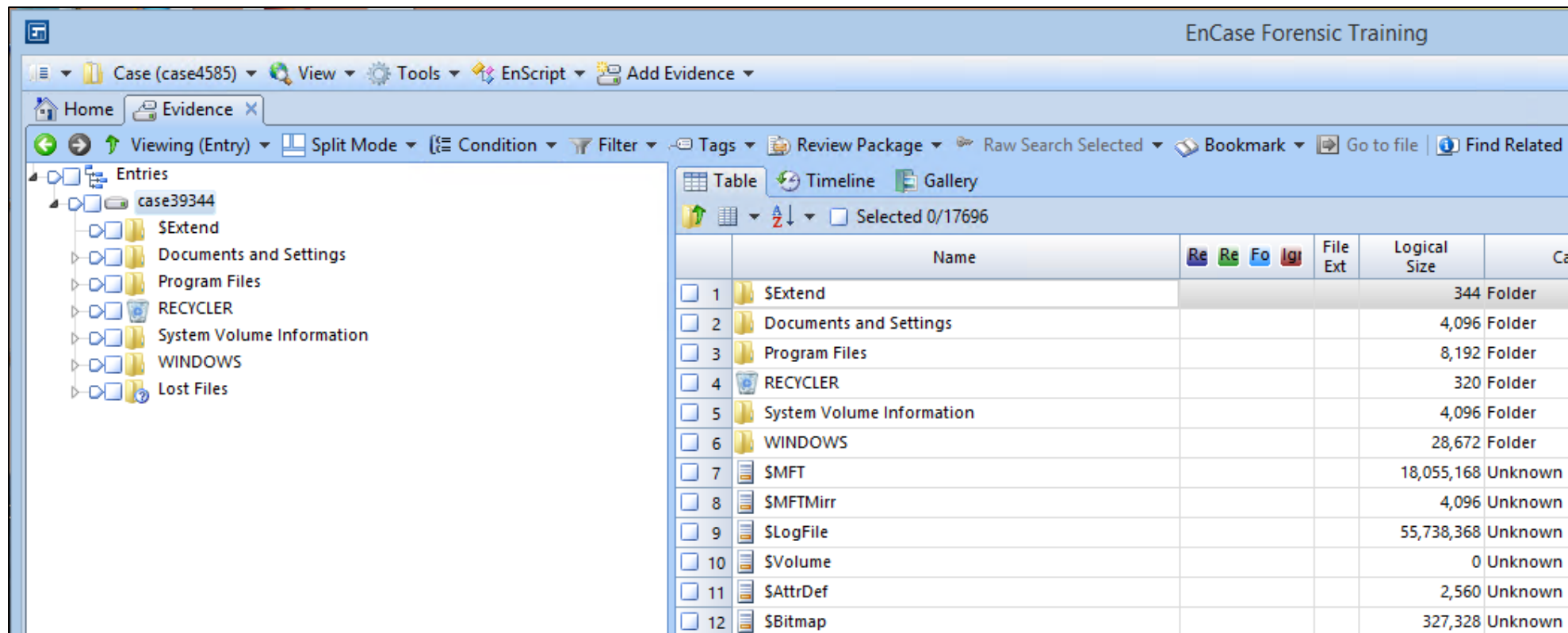
- Close both folders
- Open EnCase from the shortcut on your Desktop
- Enter .\student and student for the UAC and select “Yes”
- Select “Open”
- Expand “This PC”
- Local Disk C:\EnCase Case\case4585
- Select the case4585 file inside the case4585 folder
- Select “Open”

# EnCase Hand's On

- Make sure the title bar of EnCase states “EnCase Forensic Training”
- If it said “EnCase Acquisition” that would mean the license file didn't load properly

# EnCase Hand's On

- Select “Evidence” under the “BROWSE” section
- Select the “Open” icon



# EnCase Hand's On

- You can manually browse to different folders on the image
- Go to case39344\Documents and Settings\Forsec1\Desktop
- What is on the suspect's desktop?

# EnCase Hand's On – String Searching

- We can also search the entire image for certain strings.
- You have been told that the suspect may have committed identify theft against Ringo Johnson whose SSN is 239-23-5324
- Select the “View” icon and select “Search” which opens a new tab

# EnCase Hand's On – String Searching

- The “Index” window allows you to type in strings to search over the entire image
  - This only works if the image has been processed which I performed previously
- Enter 239-23-5324 in the “Index” window
- You should see two hits were found.
- Click once on the stolen doc 1.txt file so it turns blue



# EnCase Hand's On – String Searching

- Drag the bottom panel's window up a bit
- When was the file last written to?
- On the bottom panel, select the "Text" tab
- What information is shown about Ringo?
- Now we have some evidence that the suspect may have been involved in the identity theft

# EnCase Hand's On – String Searching

- Let's bookmark it since it is important
- Right click on the stolen doc1.txt and select Bookmark and Single Item and enter ID theft and hit "OK"

# EnCase Hand's On – Internet Records

- Now let's view some of the processing items that were found
- Select “View” and “Records”
- Select the “Internet” folder and click on “Internet” in blue on the right side window

# EnCase Hand's On – Internet Records

- You should see folders for IE and Chrome
- On the left side, go to IE \ History \ Typed URL
- Select the top NTUSER.DAT file and change the bottom window to the “Transcript” tab
- Look through the different NTUSER.DAT files on the right window and determine what URLs were typed?
- Look through the “Visited Link” folder now and what suspicious item was searched for on Google?

# EnCase Hand's On – Internet Records

- Now, lets look at the cached images from IE
- Select IE \ Cache \ Image on the left
- On the right, choose the “Gallery” tab
- Take a look through the pictures that were cached be the suspect's browser
- Bookmark the SecTools.Org picture and add a descriptive comment
- Take some time to check out the other IE artifacts

# EnCase Hand's On – Other Artifacts

- Hit the Green back button on the upper left
- Check out the Thumbnails in the Gallery view
- See anything suspicious?
- Hit the Green back button and go to the Evidence Processor Module Results
- Go to Windows Artifact Parser \ Recycle Bin \ INFO2 and click on INFO2 to view the contents
- When was the secret loot folder deleted?

# EnCase Hand's On – Other Artifacts

- Bookmark that folder
- Find the System Info Parser – Records
- Drill down
- When was the OS was installed and what is the time zone of the machine?
  - Time zone is especially important when creating a timeline

# EnCase Hand's On – Other Artifacts

- Also, in System Info Parser, do you see any suspicious user accounts?
- Bookmark the account
- Now, let's look at our bookmarks
- Go to “View” & “Bookmarks” which opens a new tab and you should see your findings
- EnCase can also be used to create a report of your findings but we won't cover that today



# **In-Class Lab 2 - Complete**

## Part III - II

---

# Registry Forensics

# Windows Registry Structure

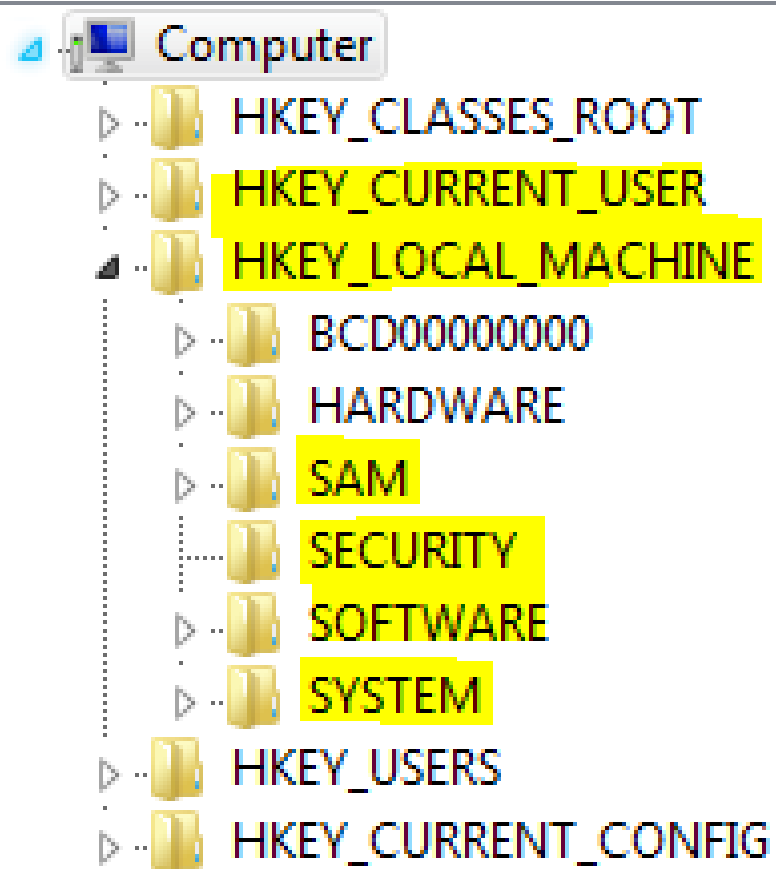
- Hierarchical database structured in a tree format
- Contains root keys, hives, keys, and values

# Windows Registry – Root Keys

- HKEY\_CLASSES\_ROOT
- HKEY\_CURRENT\_USER
- HKEY\_LOCAL\_MACHINE
- HKEY\_USERS

# Windows Registry – Hives

- Logical group of keys, subkeys and values



# Windows Registry – Hives

- Hives can be extracted from an image or from a live system
- Hives can only be extracted from a live system with special tools (such as FTK Imager)

# Windows Registry – Hive File Locations

- HKEY\_LOCAL\_MACHINE\SAM
  - C:\Windows\system32\config\SAM
- HKEY\_LOCAL\_MACHINE\Security
  - C:\Windows\system32\config\SECURITY
- HKEY\_LOCAL\_MACHINE\System
  - C:\Windows\system32\config\system
- HKEY\_LOCAL\_MACHINE\Software
  - C:\Windows\system32\config\software
- HKEY\_CURRENT\_USER\NTUSER.DAT
  - WinXP: C:\Documents and Settings\<username>\NTUSER.dat
  - Vista+: C:\Users\<username>\NTUSER.dat

**Go to:**  
**In-Class Lab 3 Slides**



# Registry Analysis Hand's On

- We are going to use EnCase to export registry files from the image into our case file
- Go to the “Evidence” Tab and select the “Table” view
- case39344 \ Documents and Settings \ Forsec1
- Right click on NTUSER.DAT and use Entries \ Copy Files
- Hit Next, Next, Finish
- Minimize EnCase

# Registry Analysis Hand's On

- On your Desktop, open Forensic Tools \ Evidence \ Registry Artifacts
- Open another Windows Explorer Window and go to:
- C:\EnCase Case\case4585\Export
- Copy and paste the NTUSER.DAT file from there to the Registry Artifacts folder on your Desktop
- I have already copied the other hives for you

# AccessData Registry Viewer

- This viewer allows you to import various hives and browser through the suspect's registry
- This is useful when you are experienced and know what you are looking for
- In the Forensic Tools \ Evidence \ Registry Artifacts folder on your Desktop
  - **.\student & student**
- Execute AccessData Registry Viewer and install it with all of the default options

# AccessData Registry Viewer

- Execute the shortcut on the Desktop for Registry Viewer
- Select “No” and “OK”
- Open the SAM file
  - Desktop \ Forensic Tools \ Evidence \ Registry Artifacts
- This is the file that can be used with pwdump to extract the password hashes

# AccessData Registry Viewer

- Browse to SAM \ SAM \ Domains \ Account \ Users
- Select the different users and look at the “Key Properties”
  - You aren’t shown the actual hashes as a “Syskey” is used to make the hashes harder to decrypt and is stored in the System hive
- Close the SAM hive and open the software hive
- Browse around a bit to see the various keys and values

# Registry Forensics

- Close Registry Viewer
- As mentioned, it can be difficult to determine what is useful if you don't have much experience with the registry
- A tool that helps and organizes everything for you is RegRipper, created by Harlan Carvey
- You can also write your own plugins in Perl to detect other keys/values in the registry

# RegRipper Hand's On

- In the Forensic Tools / Evidence / Registry Artifacts Folder, open the regripper folder
- Execute the rr application
- Set the path of Hive File by browsing to:
  - D:\Users\youruser\Desktop\Forensic Tools\Evidence\Registry Artifacts\NTUSER
- Set the path of the report file as
  - D:\Users\youruser\Desktop\Forensic Tools\Evidence\Registry Artifacts\regripper reports
  - Set file name as ntuserreport and hit Save

# RegRipper Hand's On

- Change Plugin File to “ntuser”
- Hit “Rip It”
- Keep RegRipper open but open the regripper reports file in Windows Explorer
  - Desktop \ Forensic Tools \ Evidence \ Registry Artifacts \ regripper reports
- In the regripper reports folder are two files
  - The smaller file is a log file from the tool
  - The larger file is the report
- Open the report



# RegRipper Hand's On

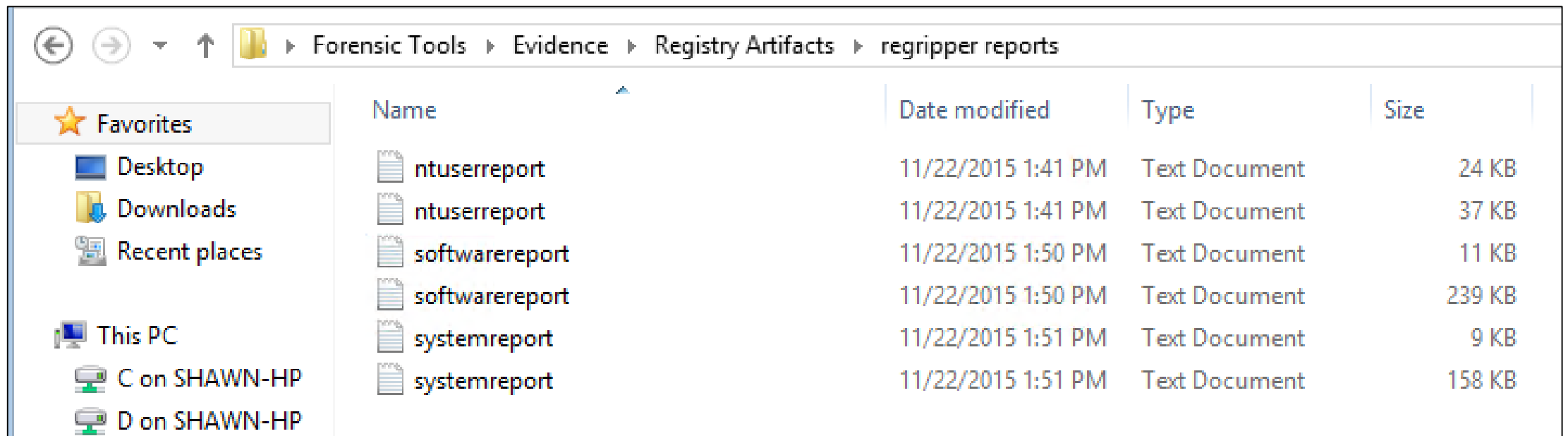
- Use the report to answer the following questions:
  1. What remote drives were mounted to the suspect's computer?
  2. Was the suspect using a proxy?
  3. What documents were recently viewed by the suspect?

# RegRipper Hand's On

- Go ahead and run regripper on the software and system hives
  - Choose the correct path for each hive file
  - Create a report file with the same name as the hive like before and store in the regripper reports folder
  - Choose the correct plugin for each
- \*The software one might take a bit to finish

# RegRipper Hand's On

- Your regripper reports folder should look like this when finished:



Name	Date modified	Type	Size
ntuserreport	11/22/2015 1:41 PM	Text Document	24 KB
ntuserreport	11/22/2015 1:41 PM	Text Document	37 KB
softwarereport	11/22/2015 1:50 PM	Text Document	11 KB
softwarereport	11/22/2015 1:50 PM	Text Document	239 KB
systemreport	11/22/2015 1:51 PM	Text Document	9 KB
systemreport	11/22/2015 1:51 PM	Text Document	158 KB

# Answer the Following Questions

- Software Hive Report

1. Is system restore on or off on the suspect's computer?
2. What uses the Run key to autostart at boot?
3. What Windows version and service pack is the suspect running?

# Answer the Following Questions

- System Hive Report
  1. What applications are authorized to get past the Firewall for the StandardProfile?
  2. What was the computer's private IP address?
  3. What is the computer's time zone?
  4. Were any USB devices attached to the system?

# Time Zone

- One of the most important things to determine in the beginning of an investigation is the time zone from the System hive:

```
-----|
timezone v.20080324
(System) Get TimeZoneInformation key contents
```

```
TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time Sat Nov 21 23:55:45 2015 (UTC)
  DaylightName    -> Central Standard Time
  StandardName    -> Central Standard Time
  Bias            -> 360 (6 hours)
  ActiveTimeBias  -> 360 (6 hours)
-----
```

## Time Zone (Cont.)

- You also need to know if your tools and Windows artifacts are displaying time in local time or UTC time
- When preprocessing the evidence, I already selected the correct time zone of CST
- However, if you determine the correct time zone later, you can set that up in Encase at that point
- Bring up Encase

## Time Zone (Cont.)

- Select the “Evidence tab”
- Right click on case39344
- Device / Modify time zone settings
- You can see it is already set up CST
- Leave it as is, but we could change it here if we had determined the suspect’s local time zone was different after viewing the time zone information in the System registry hive



# RegRipper Hand's On

- Close the Time Properties window
- Keep Encase open
- Close registry ripper and the reports

# **In-Class Lab 3 - Complete**

# Part III - III

---

## **Browser Forensics**

# Browser Forensics Interesting Items

- **History**
- Cookies
- Cache
- Session Restore
- Flash/Super Cookies
- Download History
- Auto-Complete/Form History
- Installed Extensions

# Browser Forensics

- We used EnCase to see some of the Browser details
- There are additional tools developed by NirSoft that can further organize the different browser data files
- One such tool is called Browsing History View which can interpret the history files of most major browsers
- The first step is to find the files

# Browser History File Locations

## • IE History

XP: %userprofile%\Local Settings\History\History.IE5\index.dat

Vista+: %userprofile%\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat

## • Firefox History

XP: %userprofile%\Application Data\Mozilla\Firefox\Profiles\<random text>.default\places.sqlite

Vista+: %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\places.sqlite

## • Chrome History

XP: %userprofile%\LocalSettings\Application Data\Google\Chrome\User Data\Default\History

Vista+: %userprofile%\AppData\Local\Google\Chrome\User Data\Default\History

**Go to:**  
**In-Class Lab 4 Slides**

# Browser Forensics Hand's On

- We are going to use EnCase to export the browser history file for Chrome
- Go to the “Evidence” Tab
- case39344 \ Documents and Settings \ Forsec1 \ Local Settings \ Application Data \ Google \ Chrome \ User Data \ Default
- Right click on History and use Entries \ Copy Files
- Hit Next, Next, Finish



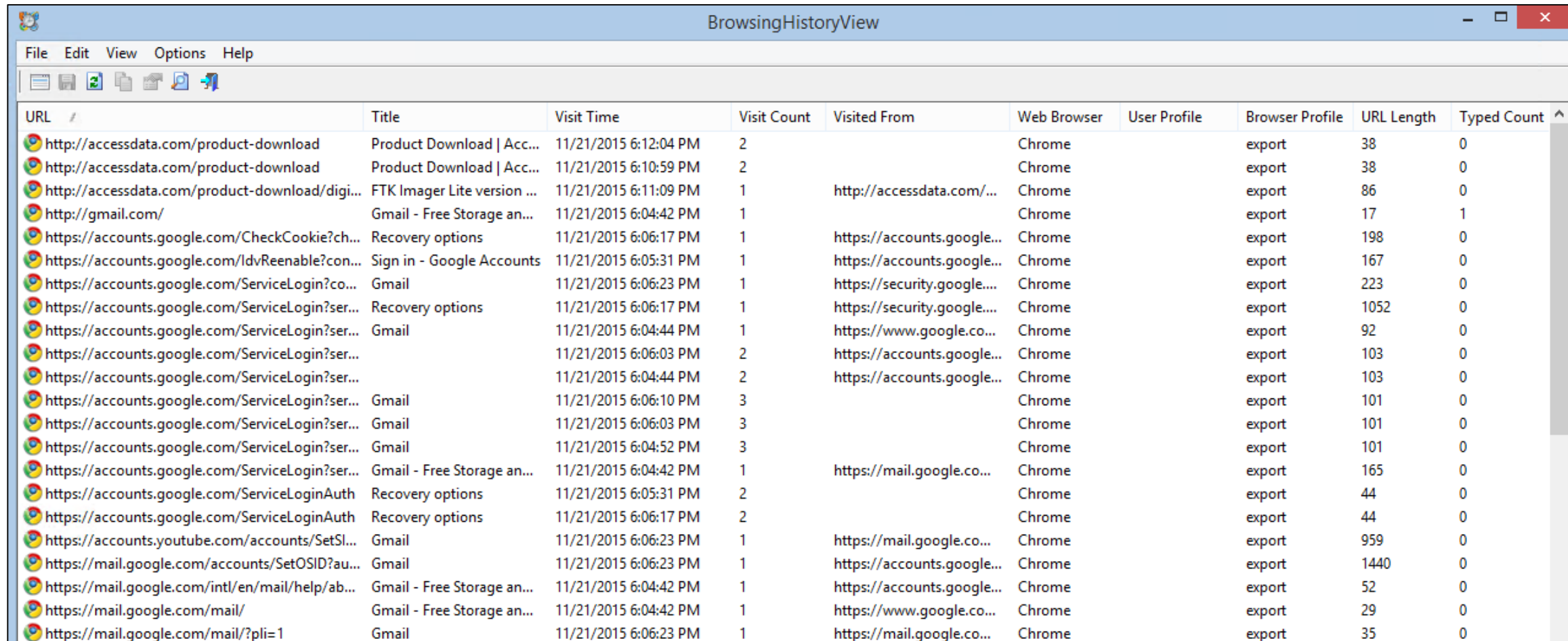
# Browser Forensics Hand's On

- Notice in EnCase, Chrome's Default folder contains a wealth of information aside from the history
- Minimize EnCase
- In your Forensic Tools folder on your Desktop, go to
- Evidence \ Browser Tools and open Browsing History View
- Change top dropdown to "Load history items from any time"

# Browser Forensics Hand's On

- Change middle dropdown to “Load history from the specified history files”
- Add the following path under “Chrome history files:”
  - C:\encase case\case4585\export\history
- Hit “OK” two times
- Maximize Browsing History View

# Browser Forensics Hand's On



URL	Title	Visit Time	Visit Count	Visited From	Web Browser	User Profile	Browser Profile	URL Length	Typed Count
http://accessdata.com/product-download	Product Download   Acc...	11/21/2015 6:12:04 PM	2		Chrome		export	38	0
http://accessdata.com/product-download	Product Download   Acc...	11/21/2015 6:10:59 PM	2		Chrome		export	38	0
http://accessdata.com/product-download/digi...	FTK Imager Lite version ...	11/21/2015 6:11:09 PM	1	http://accessdata.com/...	Chrome		export	86	0
http://gmail.com/	Gmail - Free Storage an...	11/21/2015 6:04:42 PM	1		Chrome		export	17	1
https://accounts.google.com/CheckCookie?ch...	Recovery options	11/21/2015 6:06:17 PM	1	https://accounts.google...	Chrome		export	198	0
https://accounts.google.com/IdvReenable?con...	Sign in - Google Accounts	11/21/2015 6:05:31 PM	1	https://accounts.google...	Chrome		export	167	0
https://accounts.google.com/ServiceLogin?co...	Gmail	11/21/2015 6:06:23 PM	1	https://security.google....	Chrome		export	223	0
https://accounts.google.com/ServiceLogin?ser...	Recovery options	11/21/2015 6:06:17 PM	1	https://security.google....	Chrome		export	1052	0
https://accounts.google.com/ServiceLogin?ser...	Gmail	11/21/2015 6:04:44 PM	1	https://www.google.co...	Chrome		export	92	0
https://accounts.google.com/ServiceLogin?ser...		11/21/2015 6:06:03 PM	2	https://accounts.google...	Chrome		export	103	0
https://accounts.google.com/ServiceLogin?ser...		11/21/2015 6:04:44 PM	2	https://accounts.google...	Chrome		export	103	0
https://accounts.google.com/ServiceLogin?ser...	Gmail	11/21/2015 6:06:10 PM	3		Chrome		export	101	0
https://accounts.google.com/ServiceLogin?ser...	Gmail	11/21/2015 6:06:03 PM	3		Chrome		export	101	0
https://accounts.google.com/ServiceLogin?ser...	Gmail	11/21/2015 6:04:52 PM	3		Chrome		export	101	0
https://accounts.google.com/ServiceLogin?ser...	Gmail - Free Storage an...	11/21/2015 6:04:42 PM	1	https://mail.google.co...	Chrome		export	165	0
https://accounts.google.com/ServiceLoginAuth	Recovery options	11/21/2015 6:05:31 PM	2		Chrome		export	44	0
https://accounts.google.com/ServiceLoginAuth	Recovery options	11/21/2015 6:06:17 PM	2		Chrome		export	44	0
https://accounts.youtube.com/accounts/SetSl...	Gmail	11/21/2015 6:06:23 PM	1	https://mail.google.co...	Chrome		export	959	0
https://mail.google.com/accounts/SetOSID?au...	Gmail	11/21/2015 6:06:23 PM	1	https://accounts.google...	Chrome		export	1440	0
https://mail.google.com/intl/en/mail/help/ab...	Gmail - Free Storage an...	11/21/2015 6:04:42 PM	1	https://accounts.google...	Chrome		export	52	0
https://mail.google.com/mail/	Gmail - Free Storage an...	11/21/2015 6:04:42 PM	1	https://www.google.co...	Chrome		export	29	0
https://mail.google.com/mail/?pli=1	Gmail	11/21/2015 6:06:23 PM	1	https://mail.google.co...	Chrome		export	35	0

# Browser Forensics Hand's On

- Answer the following questions:
  1. What date and time did the suspect use Google to search for “netcat for windows?”
  2. What date and time did the suspect compose a new email?
- You can close BrowsingHistoryView

# **In-Class Lab 4 - Complete**

# Part III - IV

---

# Email Forensics

# Email Forensics

- Email can contain a great amount of relevant evidence in an investigation
- The first step is to determine where the email evidence is located
  - In a host based email client such as Outlook
  - In a web based email client such as Gmail, Yahoo, Etc.
  - On a server
  - On a phone

# Email Forensics: Items To Focus On

- Headers to determine the sender and recipient addresses and where it was sent from/to
- Timestamps
- Content of the message
  - Body
  - Attachments



# Email Forensics: Outlook

- Locate the PST file which is the main local repository for email
- XP:
  - %userprofile%\Local Settings\Application Data\Microsoft\Outlook
  - &userprofile%\AppData\Local\Microsoft\Outlook
- Deleted messages may also be contained in the PST file

# Email Forensics: Tool

- EnCase can view data in PST files but it is often more useful to be able to open the entire file
- Kernel Outlook PST Viewer can view content of PST file

# Part III - VI

---

# Memory Forensics

# Memory Forensics

- Cutting edge area of Forensics/Incident Response/Malware Analysis that involves analyzing the memory (RAM) of a system
- As previously mentioned, FTK Imager can be used to capture memory from a live system
- Allows analyst to look at artifacts such as:
  - Which processes were running
  - Open network connections
  - Executed commands

# Volatility Framework

- Open Source implemented in Python
- Only for analysis (does not acquire memory)
- Command line application
  - Does not come with a front end GUI
- Contains different profiles for various OS as well as analysis plugins
- Example syntax:  

```
python vol.py -f <filename> --profile=<profile>  
<plugin> [args]
```

**Go to:**  
**In-Class Lab 5 Slides**

# Volatility Framework – Hand's On

- I previously took a memory capture of our suspect's system which had 512MB of ram
- Open Kali and your itms448 share which should be mounted from last class as a folder on your desktop
  - If not, go ahead and mount it or just watch your neighbor
- Go to Tools/Forensic Tools/Evidence/Memory Image
- Drag memdump.mem to your desktop
- Open a terminal

# Volatility Framework – Hand's On

- Change directories to /root/Desktop
- First, we need to figure out what the OS is of the system so that we can choose the correct profile
- **volatility -f memdump.mem imageinfo**
- What OS profile was suggested?



# Volatility Framework – Hand's On

```
root@KLY-IR105:~/Desktop# volatility -f memdump.mem imageinfo
Volatility Foundation Volatility Framework 2.4
Determining profile based on KDBG search...

Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with Win
XPSP2x86)
AS Layer1 : IA32PagedMemoryPae (Kernel AS)
AS Layer2 : FileAddressSpace (/root/Desktop/memdump.mem)
PAE type : PAE
DTB : 0x315000L
KDBG : 0x8054d2e0
Number of Processors : 2
Image Type (Service Pack) : 3
KPCR for CPU 0 : 0xffdff000
KPCR for CPU 1 : 0xf892a000
KUSER_SHARED_DATA : 0xffdf0000
Image date and time : 2015-11-23 00:05:22 UTC+0000
Image local date and time : 2015-11-22 18:05:22 -0600
```

- WinXPSP3x86

# Volatility Framework – Hand's On

- First let's see what processes were running
- **volatility -f memdump.mem --profile=WinXPSP3x86 pslist**
- What suspicious processes were running?

# Volatility Framework – Hand's On

- Let's look at our plugin options
- **volatility -h**
- Let's see if the suspect was using the command line
- **volatility -f memdump.mem --profile=WinXPSP3x86 consoles**
- Start at the top
- See anything interesting???

# Volatility Framework – Hand's On

- What connections did the suspect have open?
- **volatility -f memdump.mem --profile=WinXPSP3x86 connections**
- What is suspicious in their internet history?
  - IE history also shows local files that were opened
- **volatility -f memdump.mem --profile=WinXPSP3x86 iehistory**

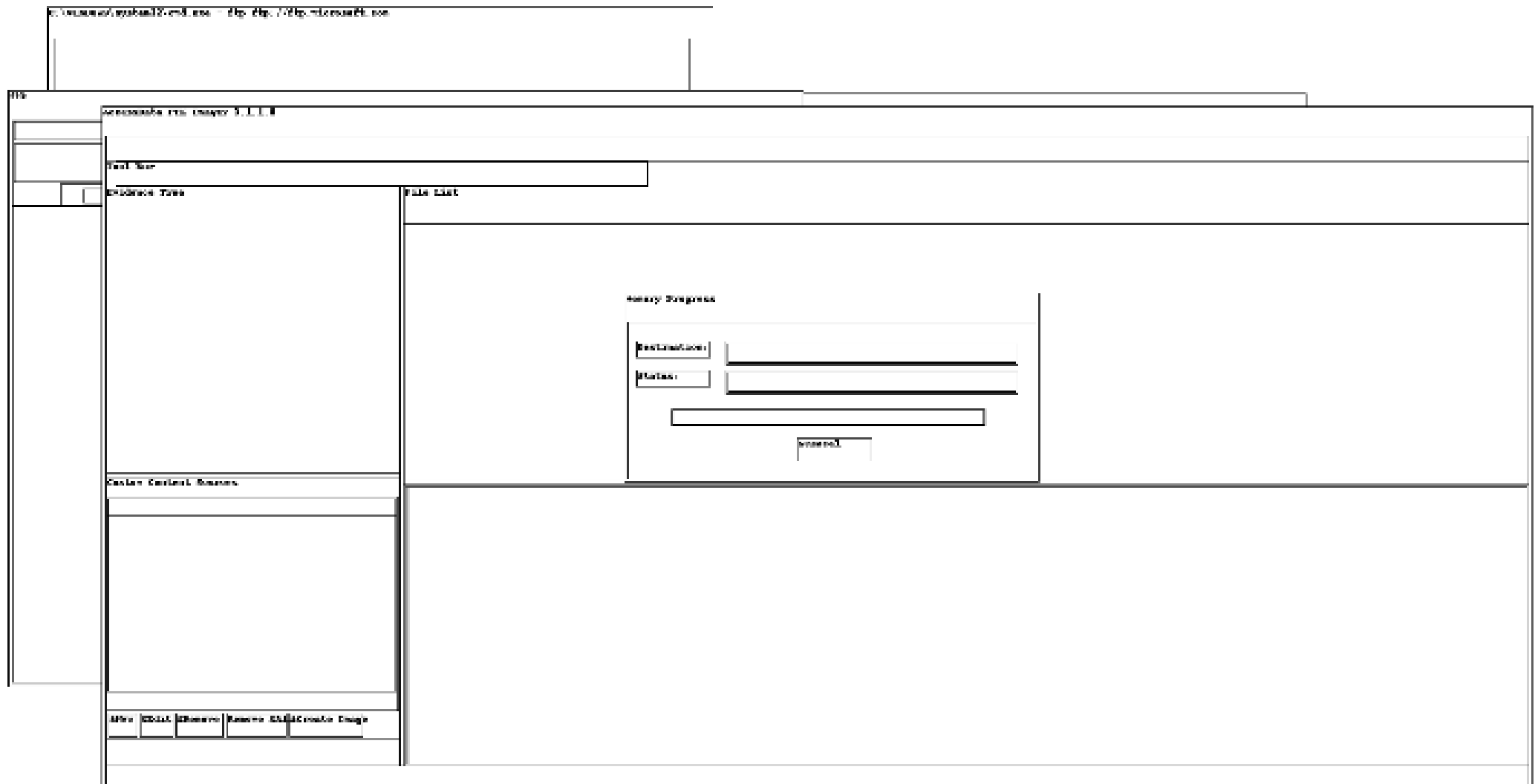
# Volatility Framework – Hand's On

- Another item stored in RAM are logon credentials to websites
- You know the attacker has a hotmail account but don't know the email address or password
- See if you can figure it out with a string search
- **volatility -f memdump.mem --profile=WinXPSP3x86  
yarascan --yara-rules="hotmail"**

# Volatility Framework – Hand's On

- You can also sometimes recreate a frame of a screenshot of the GUI from memory
- Create a directory called shots on your Desktop
- **mkdir shots**
- **volatility -f memdump.mem --profile=WinXPSP3x86 screenshot -D shots**
- Open the shots folder and view the images
- At least one should show a frame

# Volatility Framework – Hand's On



# Volatility Framework – Hand's On

- If time, feel free to run **volatility -h** and play around with the other plugins
- The developers of volatility wrote a great book called “The Art of Memory Forensics” for anyone who is interested in learning more about this growing field



# **In-Class Lab 5 - Complete**

# Follow On Classes

- I provided you a high level overview but very hand's on crash course on several of the areas in Forensics
- IIT offers ITMS538 Cyber Forensics in the Spring semesters
- Here are a few sites with sample images for practice:
- <http://www.forensicfocus.com/images-and-challenges>
- Also, an EnCase practice image:
- [http://media.johnwiley.com.au/product\\_ancillary/63/04709010/DOWNLOAD/tdurdenex01.html](http://media.johnwiley.com.au/product_ancillary/63/04709010/DOWNLOAD/tdurdenex01.html)

# Homework

- No New Homework for the rest of the semester
  - Homework 13 still due before Midnight on Sunday, 4/17
- We will have a short lecture on Wireless Network Security & Attacks next week as well as a Final Exam Review
- April 25<sup>th</sup> is a mandatory class where you will present your Individual Project slides and videos
- May 2<sup>nd</sup> is the Final Exam