Cyber Security Technologies

Session 14 – Computer Forensics In-Class Labs

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 this slide deck from Blackboard to reference during the in-class labs

In-Class Lab 1

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

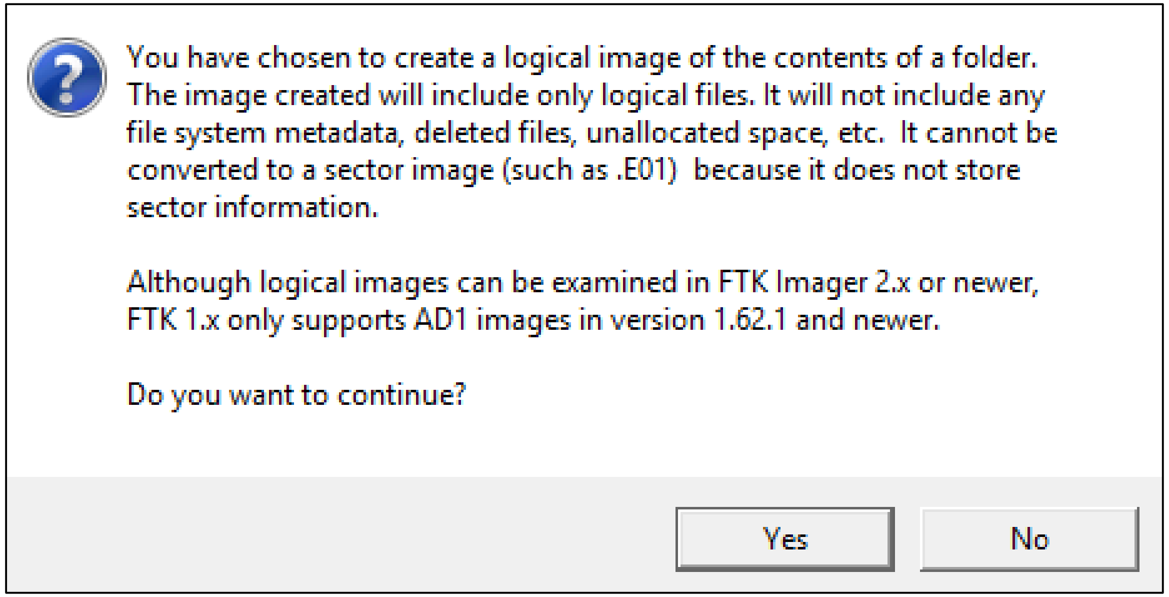
- In your RADISH Win 8.1 VM, if you haven't already done so, copy the Forensic Tools folder to your desktop from M:\Tools
- Open the FTK Imager Lite folder and launch FTK Imager
- For UAC:

.\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



You have chosen to create a logical image of the contents of a folder. The image created will include only logical files. It will not include any file system metadata, deleted files, unallocated space, etc. It cannot be converted to a sector image (such as .E01) because it does not store sector information.

Although logical images can be examined in FTK Imager 2.x or newer, FTK 1.x only supports AD1 images in version 1.62.1 and newer.

Do you want to continue?

Imaging Hand’s On

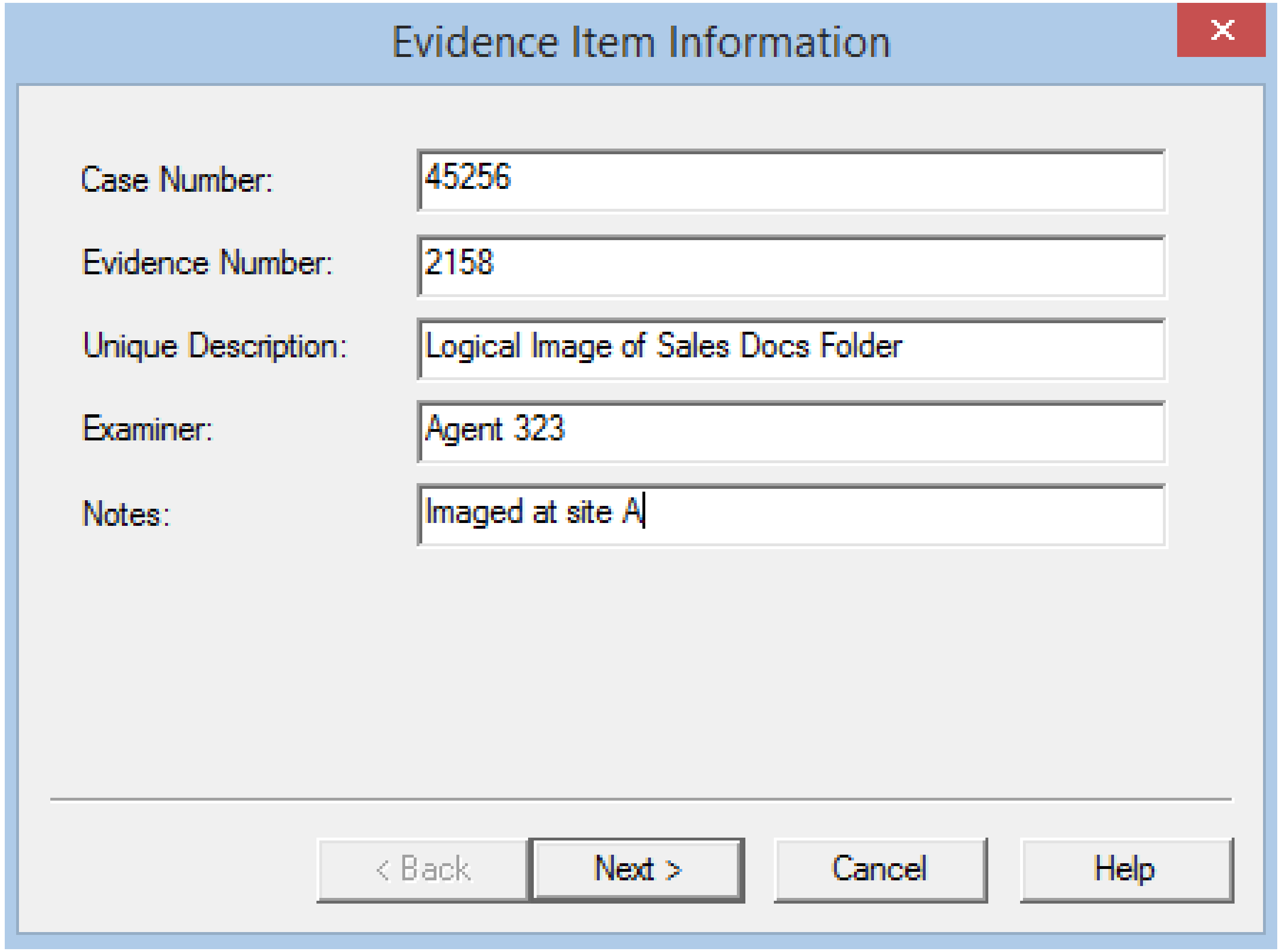
- Select “Browse”
- Choose “This PC” / PersistentDataDisk (D:) / Users / *yourname* / Desktop / Sales Docs
- Hit “OK”
- Selected Finish

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"



Evidence Item Information

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

Imaging Hand’s On

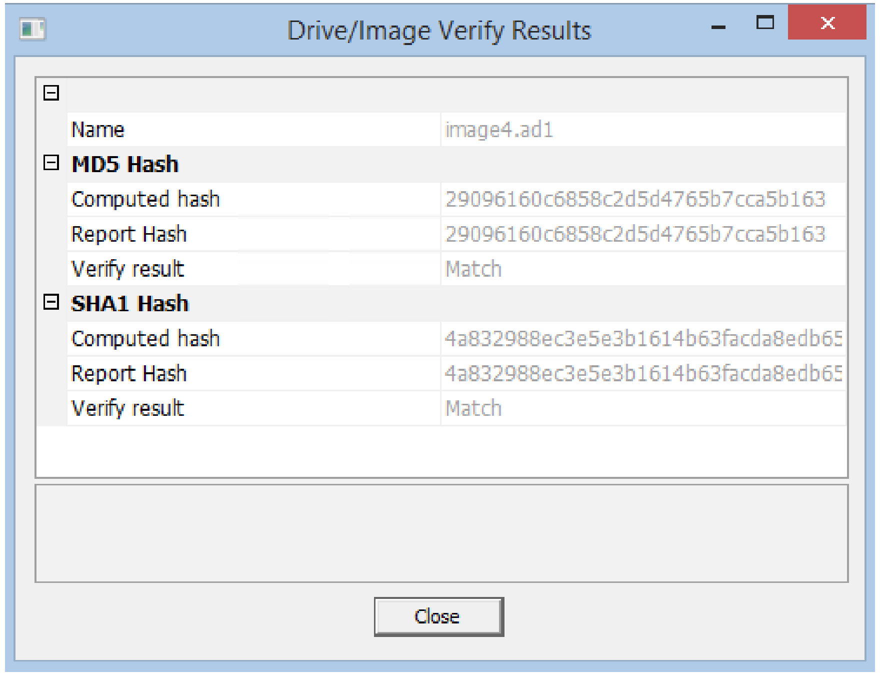
- Hit “Browse”
- Choose “This PC” / PersistentDataDisk (D:) / Users / *yourname* / Desktop
- Hit OK

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:



⊟	
Name	image4.ad1
⊟ **MD5 Hash**	
Computed hash	29096160c6858c2d5d4765b7cca5b163
Report Hash	29096160c6858c2d5d4765b7cca5b163
Verify result	Match
⊟ **SHA1 Hash**	
Computed hash	4a832988ec3e5e3b1614b63facda8edb65
Report Hash	4a832988ec3e5e3b1614b63facda8edb65
Verify result	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.as1.csv and hit “Edit with Notepad++”

Imaging Hand’s On

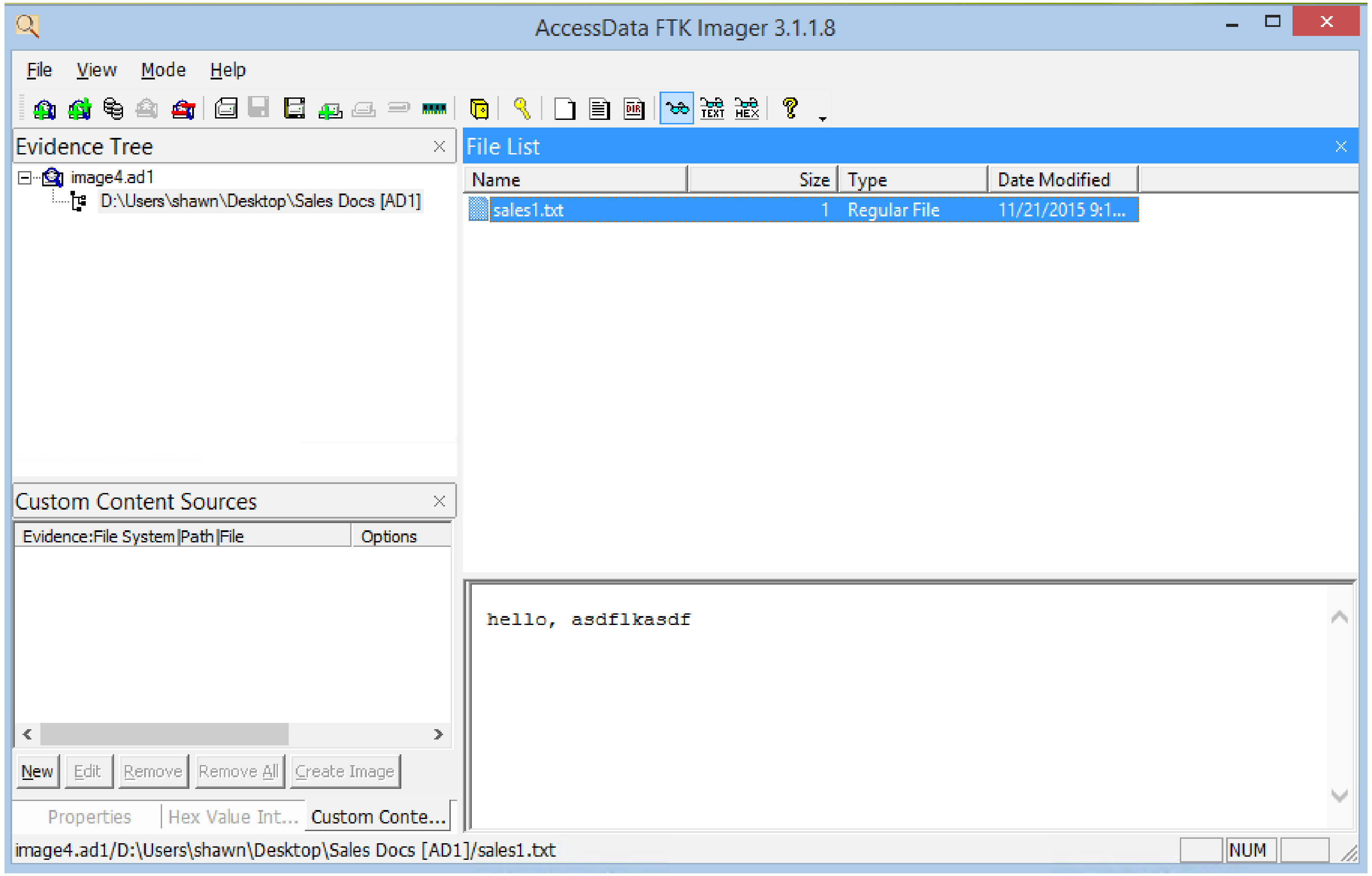
- You should see sales1.txt in there. Why is sales2.txt not listed???

Imaging Hand’s On

- Close Notepadd++
- 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


AccessData FTK Imager 3.1.1.8
File View Mode Help
Evidence Tree
image4.ad1
D:\Users\shawn\Desktop\Sales Docs [AD1]
File List
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Int... Custom Conte...
NUM

Name	Size	Type	Date Modified
sales1.txt	1	Regular File	11/21/2015 9:1...

```
hello, asdflkasdf
```

image4.ad1/D:\Users\shawn\Desktop\Sales Docs [AD1]/sales1.txt

Imaging Hand’s On

- Why didn’t you see the deleted file???
  - Folder images don’t contain unallocated space
- 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

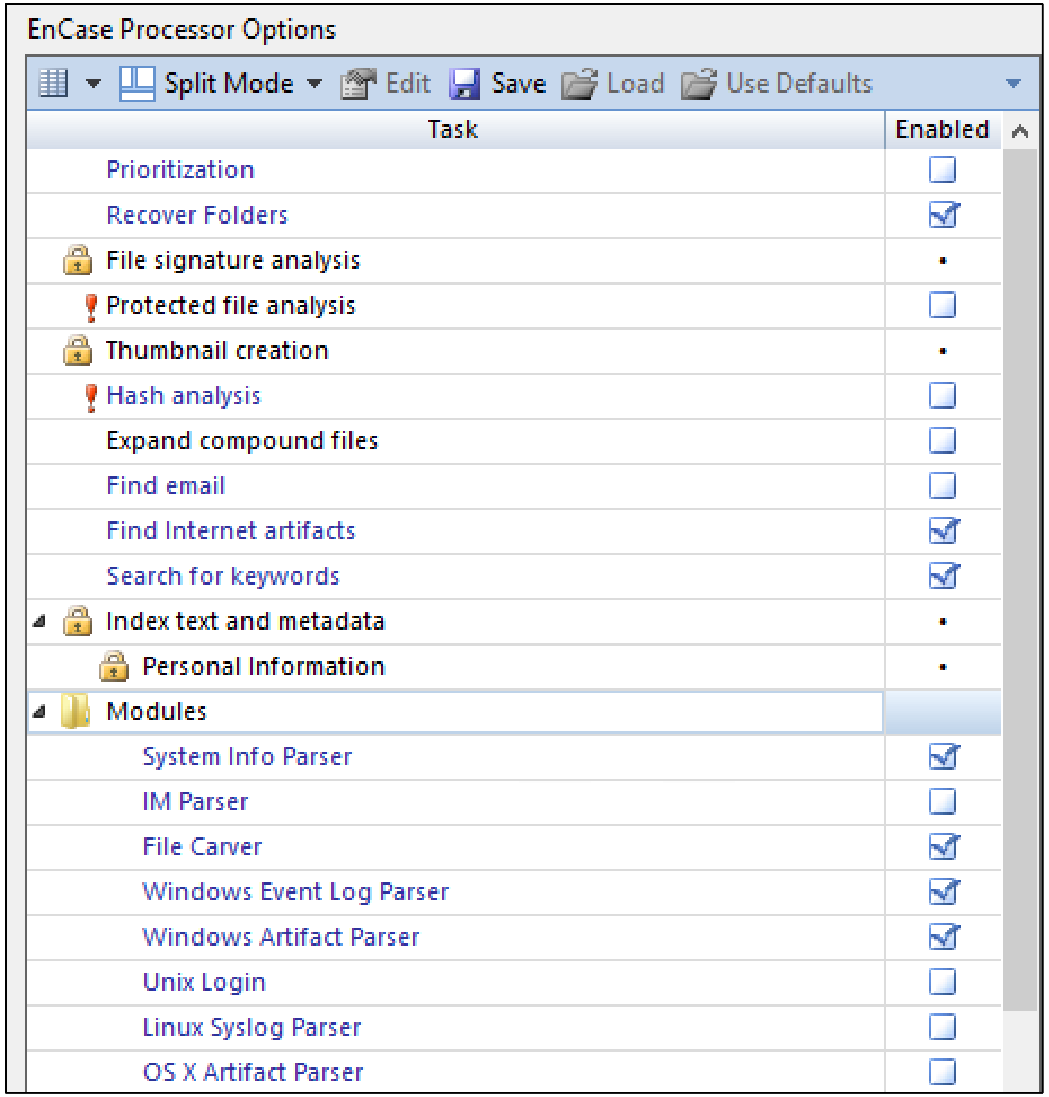
- You should see that the system, software, default, and SECURITY hives as well as the SAM were captured.
- We’ll talk about those in the next section
- You can close FTK Imager

In-Class Lab 2

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 Processor Options

Task	Enabled
Prioritization	☐
Recover Folders	☑
File signature analysis	•
Protected file analysis	☐
Thumbnail creation	•
Hash analysis	☐
Expand compound files	☐
Find email	☐
Find Internet artifacts	☑
Search for keywords	☑
Index text and metadata	•
Personal Information	•
Modules	
System Info Parser	☑
IM Parser	☐
File Carver	☑
Windows Event Log Parser	☑
Windows Artifact Parser	☑
Unix Login	☐
Linux Syslog Parser	☐
OS X Artifact Parser	☐

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

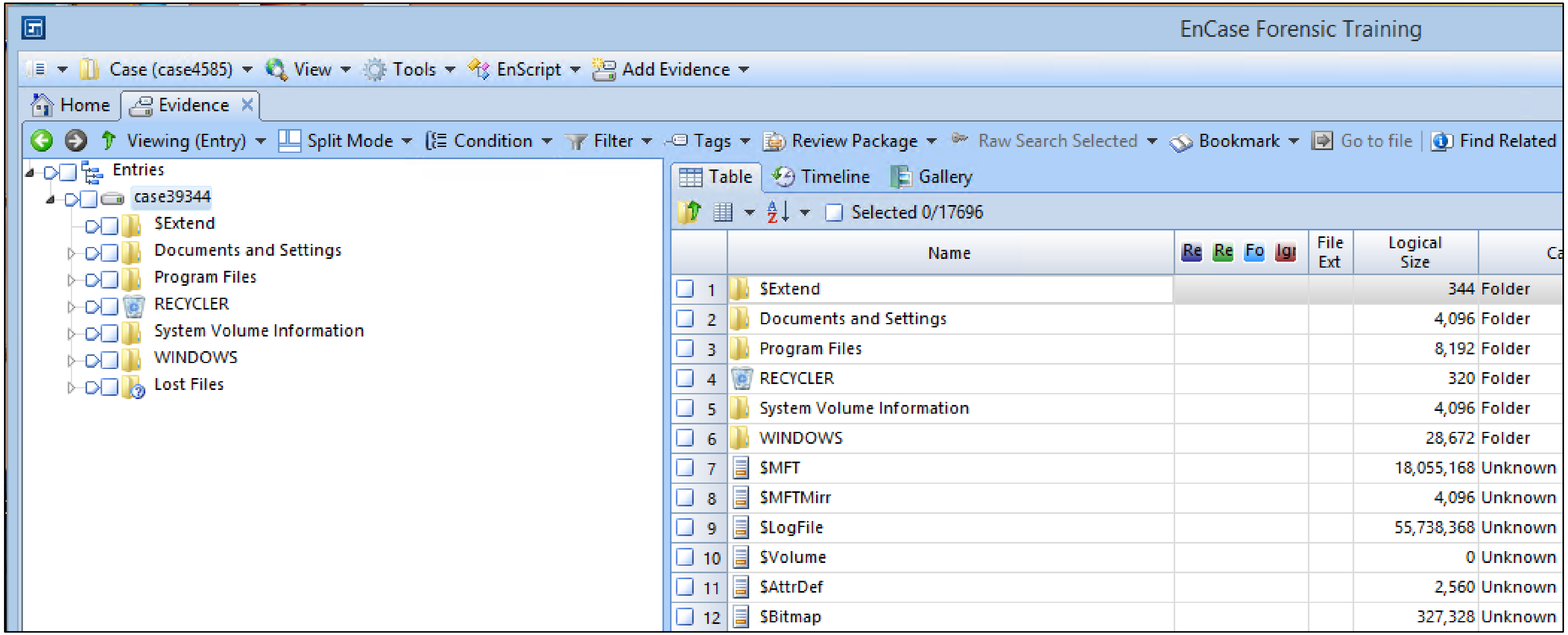
- Close both folders
- Open EnCase from the shortcut on your Desktop
- Enter .\student and student for the UAC and select "Yes"
- Select "Open"
- Expand "This PC"
- Local Disk C:\EnCase Case\case4585
- Select the case4585 file inside the case4585 folder
- Select "Open"

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



- Entries
  - case39344
    - $Extend
    - Documents and Settings
    - Program Files
    - RECYCLER
    - System Volume Information
    - WINDOWS
    - Lost Files

	Name	Re	Re	Fo	Igi	File Ext	Logical Size	Ca
1	$Extend						344	Folder
2	Documents and Settings						4,096	Folder
3	Program Files						8,192	Folder
4	RECYCLER						320	Folder
5	System Volume Information						4,096	Folder
6	WINDOWS						28,672	Folder
7	$MFT						18,055,168	Unknown
8	$MFTMirr						4,096	Unknown
9	$LogFile						55,738,368	Unknown
10	$Volume						0	Unknown
11	$AttrDef						2,560	Unknown
12	$Bitmap						327,328	Unknown

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 3

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 \ 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?

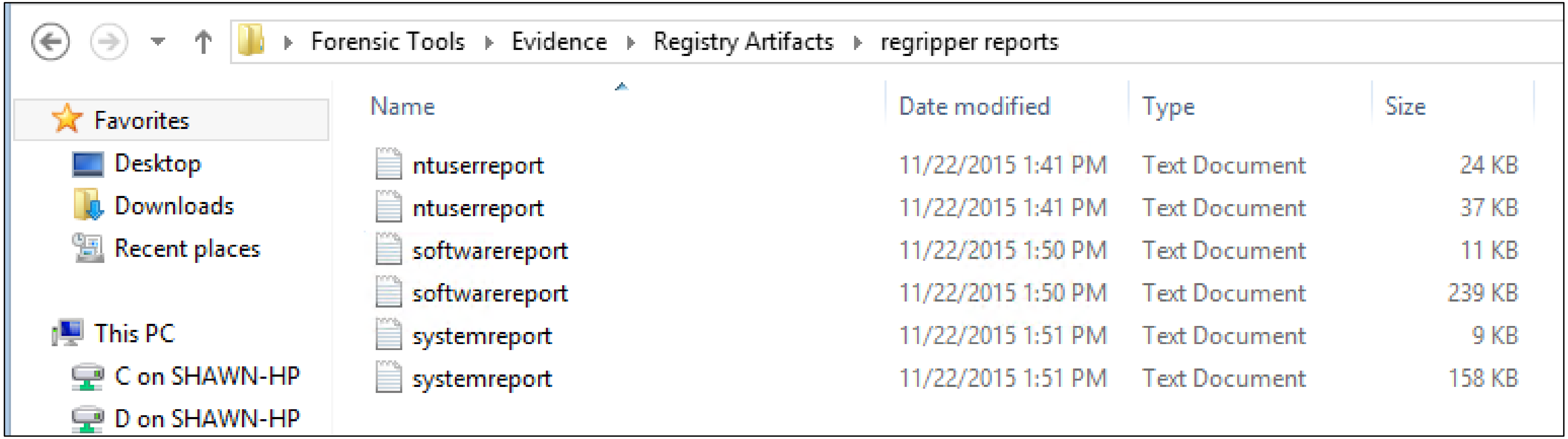
RegRipper Hand’s On

- 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?

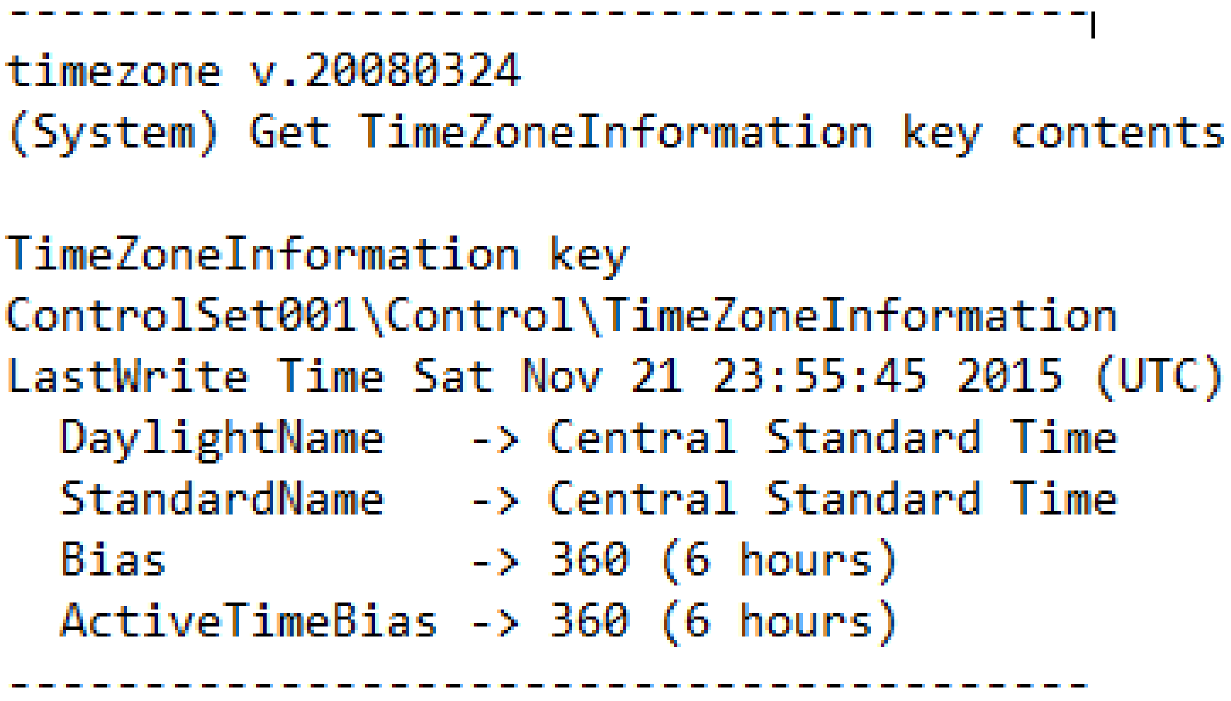
Answer the Following Questions

- 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 4

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

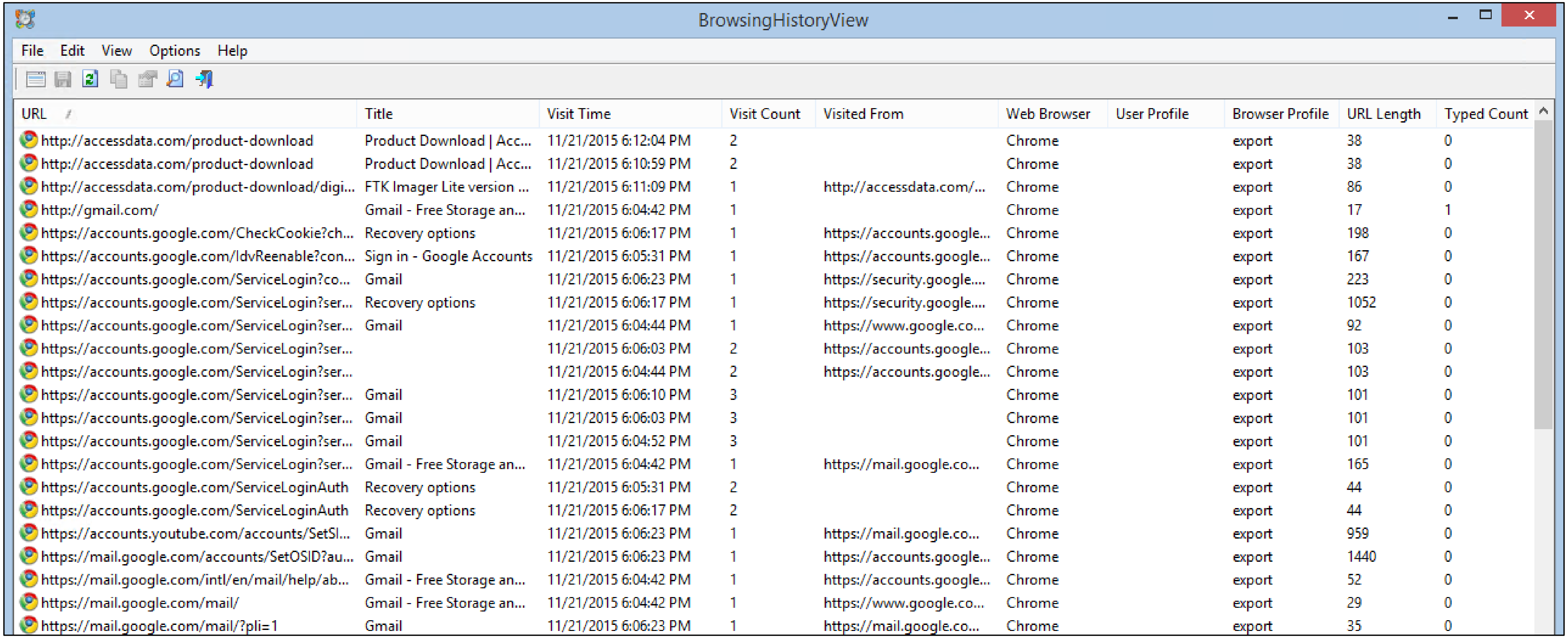
Browser Forensics Hand's On

- 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/SetSI...	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 5

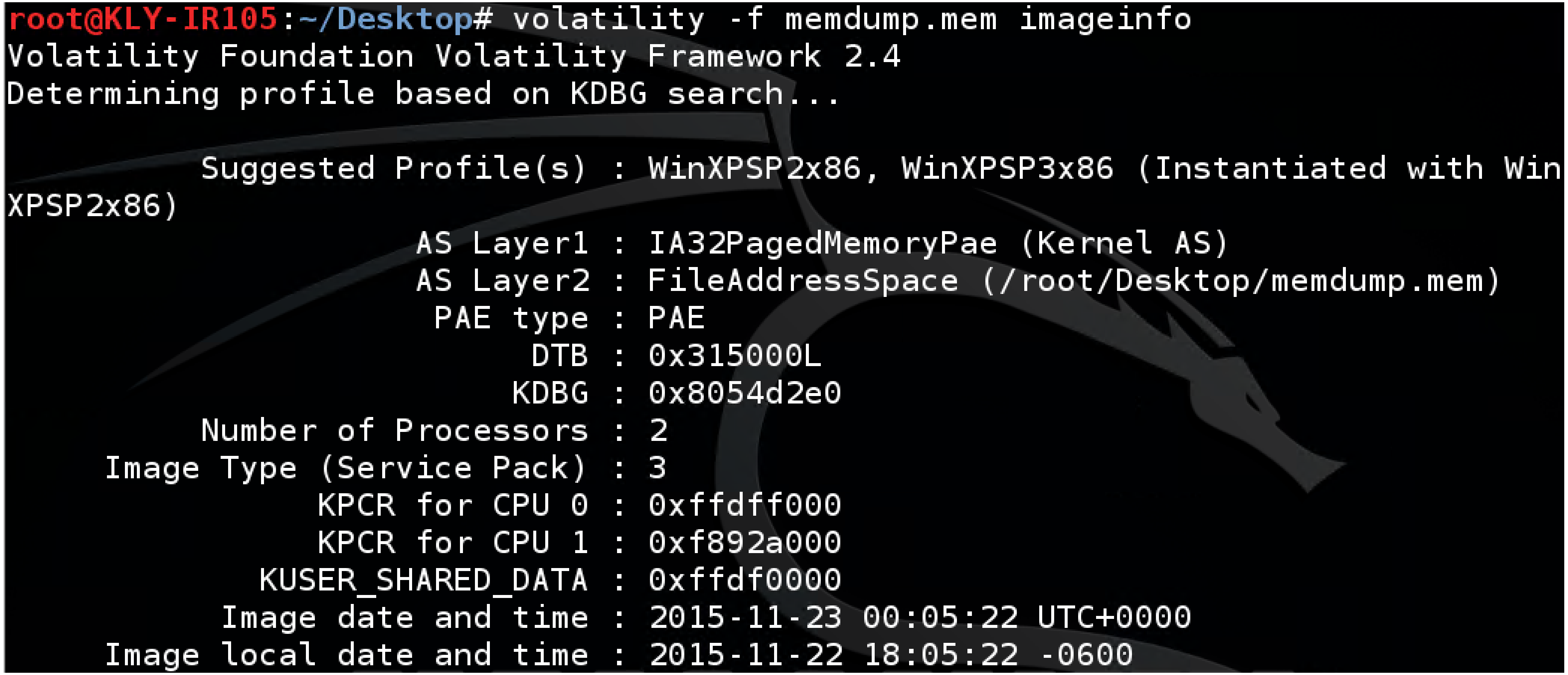
Volatility Framework – Hand's On

- 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**

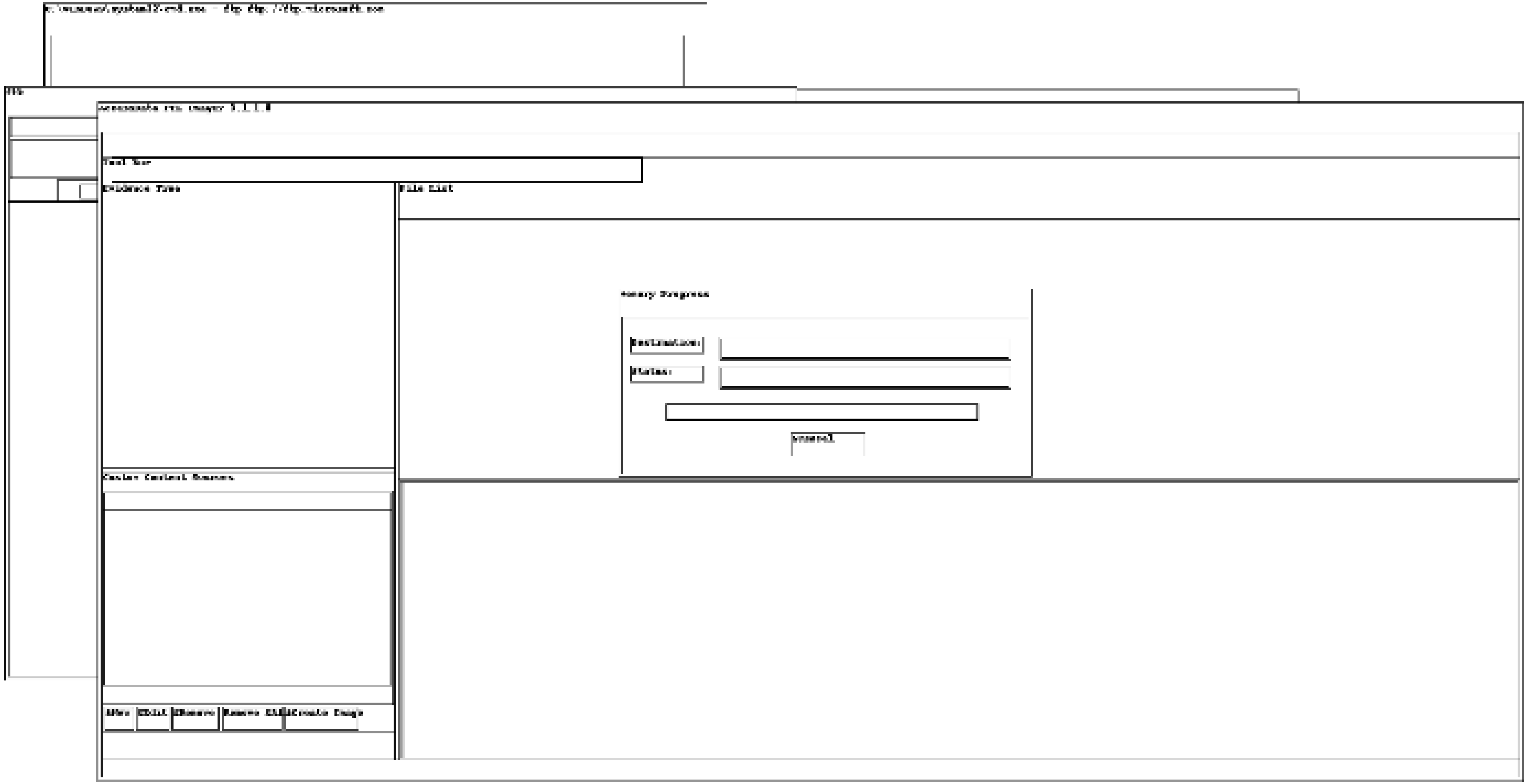
Volatility Framework – Hand's On

- 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