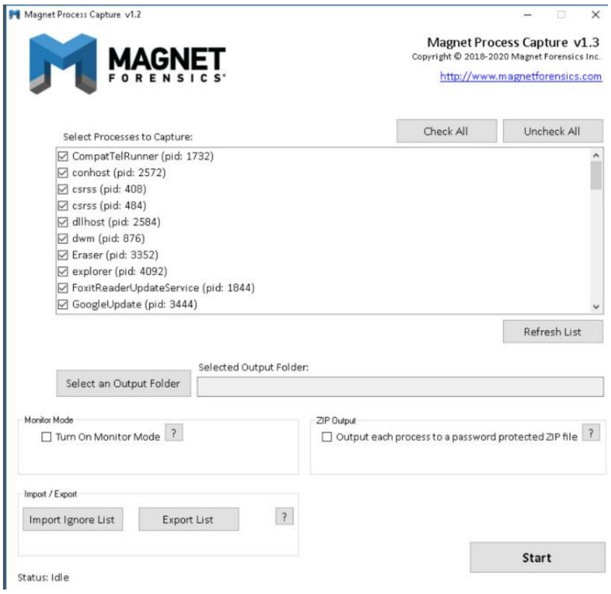
Digital Forensics

Lab 02: Live Acquisition

1. Getting Familiar with Magnet Process Capture

Let us get you familiar with some of the tools you will be using throughout this lab. The first one we will look at is Magnet Process Capture. This tool is ideal for incident response and forensic analysis because it allows an examiner to quickly view and extract processes running in volatile memory. It not only provides a list but carves out the part of the RAM that the process uses. This makes it a vital tool, especially when a quick review of the computer is needed.



Magnet Process Capture v1.3
Copyright © 2018-2020 Magnet Forensics Inc.
http://www.magnetforensics.com

Select Processes to Capture:
☑ CompatTelRunner (pid: 1732)
☑ conhost (pid: 2572)
☑ csrss (pid: 408)
☑ csrss (pid: 484)
☑ dllhost (pid: 2584)
☑ dwm (pid: 876)
☑ Eraser (pid: 3352)
☑ explorer (pid: 4092)
☑ FoxitReaderUpdateService (pid: 1844)
☑ GoogleUpdate (pid: 3444)

Selected Output Folder:

Monitor Mode
☐ Turn On Monitor Mode

ZIP Output
☐ Output each process to a password protected ZIP file

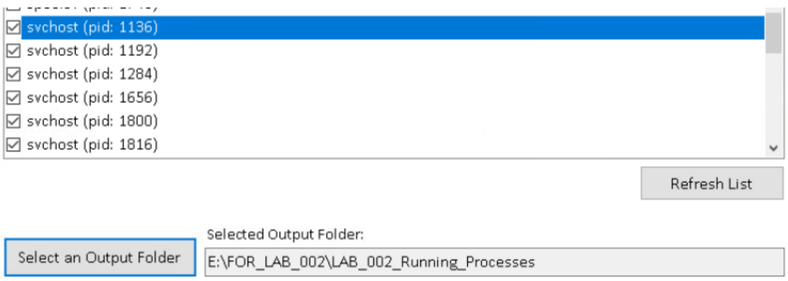
Import / Export

Status: Idle

2 Exporting Processes Using Magnet Process Capture

Live acquisition is a very delicate surgery-like process that, if done correctly, will provide tons of valuable data. However, if strict measures are not adhered to, you can destroy data and make your findings inadmissible in a court of law. The steps we teach in this lab will reveal the currently accepted processes. Follow these steps and take detailed notes of your actions to secure trustworthy evidence.

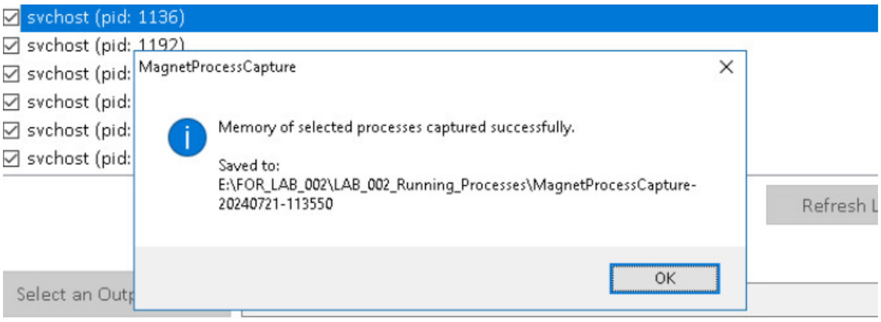
1. *Magnet Process Capture* should already be open. If it is not, reopen it and look at the **Select Processes to Capture** pane as highlighted below. Scroll through the list of processes to see if there are any that you recognize.



☑ svchost (pid: 1136)
☑ svchost (pid: 1192)
☑ svchost (pid: 1284)
☑ svchost (pid: 1656)
☑ svchost (pid: 1800)
☑ svchost (pid: 1816)

Selected Output Folder:
E:\FOR_LAB_002\LAB_002_Running_Processes

You have successfully captured specific processes and the contents of RAM associated with those processes. This ends the selective processes portion of the lab. Close the program by clicking the **X** at the top-right corner of the window.



☑ svchost (pid: 1136)
☑ svchost (pid: 1192)
☑ svchost (pid:
☑ svchost (pid:
☑ svchost (pid:
☑ svchost (pid:

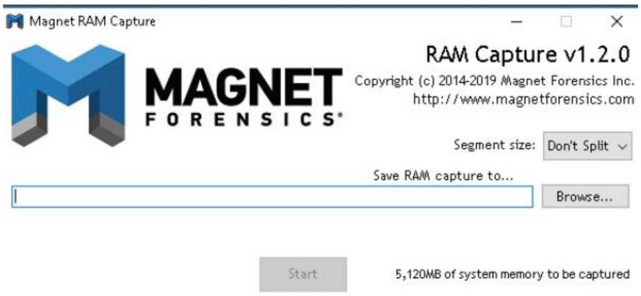
MagnetProcessCapture

Memory of selected processes captured successfully.

Saved to:
E:\FOR_LAB_002\LAB_002_Running_Processes\MagnetProcessCapture-20240721-113550

3 Getting Familiar with Magnet RAM Capture

The next tool we will look at is Magnet RAM Capture. This tool is designed for the lightweight acquisition of RAM. It also has a very simple interface and leaves very little evidence that it was running on the system.



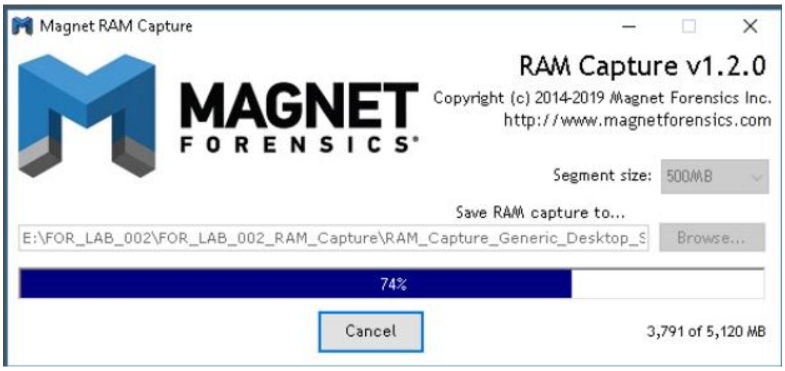
RAM Capture v1.2.0
Copyright (c) 2014-2019 Magnet Forensics Inc.
http://www.magnetforensics.com

Segment size: Don't Split

Save RAM capture to...

5,120MB of system memory to be captured

Save RAM capture to...	This is a textbox that will show the location at which you intend to store the RAM capture.
The Browse button	This button allows the user to browse to the drive/folder that the RAM capture will be stored in.
Segment Size	This dropdown menu allows you to choose the segment size of the image, which would split the file based on the selected size. You also have the option to leave the image whole, which is the option that is there by default.
Start	This button is located at the bottom of the window and allows you to start the RAM capture and store it in the selected location.



RAM Capture v1.2.0

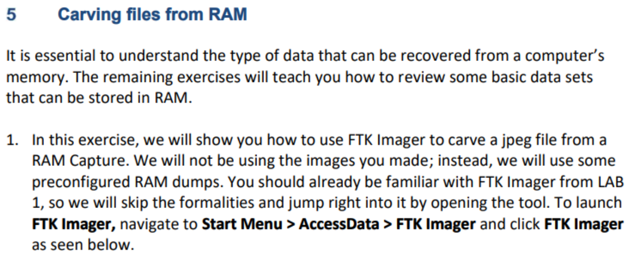
Copyright (c) 2014-2019 Magnet Forensics Inc.
http://www.magnetforensics.com

Segment size: 500MB

Save RAM capture to...

E:\FOR_LAB_002\FOR_LAB_002_RAM_Capture\RAM_Capture_Generic_Desktop_S

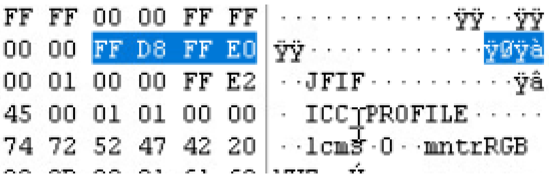
3,791 of 5,120 MB



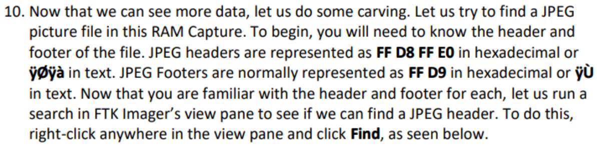
5 Carving files from RAM

It is essential to understand the type of data that can be recovered from a computer's memory. The remaining exercises will teach you how to review some basic data sets that can be stored in RAM.

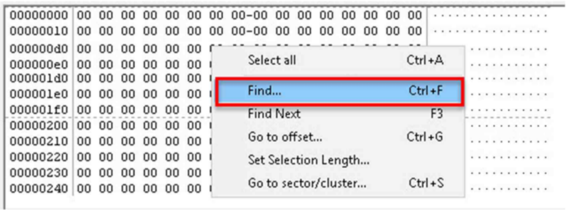
1. In this exercise, we will show you how to use FTK Imager to carve a jpeg file from a RAM Capture. We will not be using the images you made; instead, we will use some preconfigured RAM dumps. You should already be familiar with FTK Imager from LAB 1, so we will skip the formalities and jump right into it by opening the tool. To launch **FTK Imager,** navigate to **Start Menu > AccessData > FTK Imager** and click **FTK Imager** as seen below.



```
FF FF 00 00 FF FF   ············ÿÿ··ÿÿ
00 00 FF D8 FF E0   ÿÿ············ÿØÿà
00 01 00 00 FF E2   ··JFIF·········ÿâ
45 00 01 01 00 00   ·ICC_PROFILE·····
74 72 52 47 42 20   ··lcms·0··mntrRGB
```

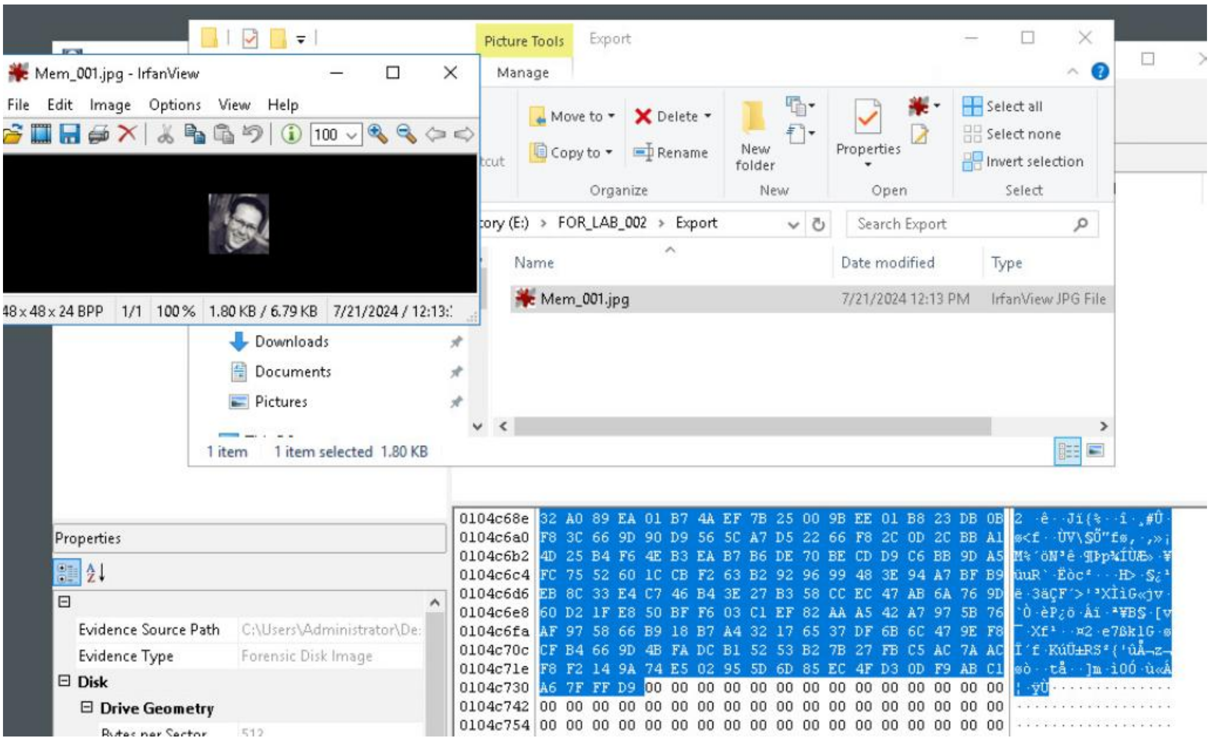


10. Now that we can see more data, let us do some carving. Let us try to find a JPEG picture file in this RAM Capture. To begin, you will need to know the header and footer of the file. JPEG headers are represented as **FF D8 FF E0** in hexadecimal or **ÿØÿà** in text. JPEG Footers are normally represented as **FF D9** in hexadecimal or **ÿÙ** in text. Now that you are familiar with the header and footer for each, let us run a search in FTK Imager's view pane to see if we can find a JPEG header. To do this, right-click anywhere in the view pane and click **Find**, as seen below.



```
00000000 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000010 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
000000d0 00 00 00 00 00 00
000000e0 00 00 00 00 00 00
000001d0 00 00 00 00 00 00
000001e0 00 00 00 00 00 00
000001f0 00 00 00 00 00 00
00000200 00 00 00 00 00 00
00000210 00 00 00 00 00 00
00000220 00 00 00 00 00 00
00000230 00 00 00 00 00 00
00000240 00 00 00 00 00 00
```

Just carved my first file from a windows memory dump (FTK Imager)



Mem_001.jpg - IrfanView
File Edit Image Options View Help
Picture Tools Export
Manage
Move to Delete Copy to Rename New folder Properties Select all Select none Invert selection
Organize New Open Select
Downloads
Documents
Pictures
Search Export
Properties

48 x 48 x 24 BPP 1/1 100 % 1.80 KB / 6.79 KB 7/21/2024 / 12:13:

ory (E:) > FOR_LAB_002 > Export

Name	Date modified	Type
Mem_001.jpg	7/21/2024 12:13 PM	IrfanView JPG File

1 item 1 item selected 1.80 KB

Evidence Source Path	C:\Users\Administrator\De:
Evidence Type	Forensic Disk Image
Disk	
Drive Geometry	
Bytes per Sector	512

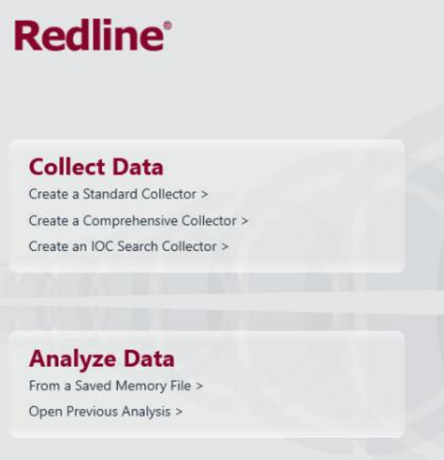
```
0104c68e 32 A0 89 EA 01 B7 4A EF 7B 25 00 9B EE 01 B8 23 DB 0B
0104c6a0 F8 3C 66 9D 90 D9 56 5C A7 D5 22 66 F8 2C 0D 2C BB A1
0104c6b2 4D 25 B4 F6 4E B3 EA B7 B6 DE 70 BE CD D9 C6 BB 9D A5
0104c6c4 FC 75 52 60 1C CB F2 63 B2 92 96 99 48 3E 94 A7 BF B9
0104c6d6 EB 8C 33 E4 C7 46 B4 3E 27 B3 58 CC EC 47 AB 6A 76 9D
0104c6e8 60 D2 1F E8 50 BF F6 03 C1 EF 82 AA A5 42 A7 97 5B 76
0104c6fa AF 97 58 66 B9 18 B7 A4 32 17 65 37 DF 6B 6C 47 9E F8
0104c70c CF B4 66 9D 4B FA DC B1 52 53 B2 7B 27 FB C5 AC 7A AC
0104c71e F8 F2 14 9A 74 E5 02 95 5D 6D 85 EC 4F D3 0D F9 AB C1
0104c730 A6 7F FF D9 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0104c742 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0104c754 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

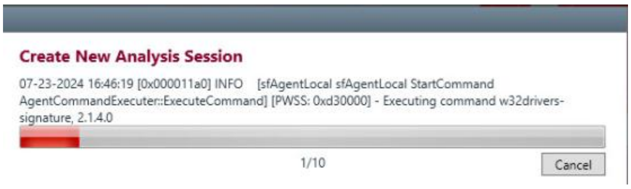
6 Getting Familiar with REDLINE

If you were successful in the previous lab, then you would have learned that a forensic image should be verified to ensure its integrity. Because the RAM is something that has processes running, it is not possible to get a hash verification. Instead, you can hash the file using a separate hashing tool and store the hash with this image file. This will ensure that it can be verified later if its integrity comes into question.

Even though we know you are excited to go over your own RAM captures, we will actually be using the same pre-prepared RAM dump from the previous task. We will do the analysis with a software called **REDLINE** created by FireEye. This is a handy Incident Response tool that has many features. We will only touch the tip of the iceberg in this lab, but it is definitely something you should research for a deeper understanding.

In this exercise, we will go over the features we will be using in Redline.

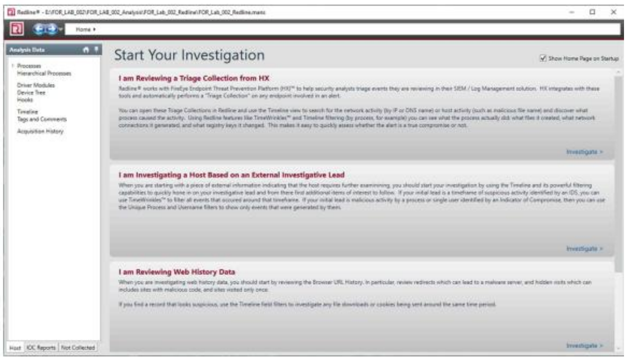

Redline®
Collect Data
Create a Standard Collector >
Create a Comprehensive Collector >
Create an IOC Search Collector >
Analyze Data
From a Saved Memory File >
Open Previous Analysis >


Create New Analysis Session

07-23-2024 16:46:19 [0x000011a0] INFO   [sfAgentLocal sfAgentLocal StartCommand AgentCommandExecuter::ExecuteCommand] [PWSS: 0xd30000] - Executing command w32drivers-signature, 2.1.4.0

1/10

12. If you see the window below, then this means all your work paid off. This is the home page, and it has several useful options that can help to automate your analysis process. In this lab, we will only be doing manual reviews of the images. However, in a more advanced session, we will cover some more interesting features of this powerful tool.


Redline® - E:\FOR_LAB_002\FOR_LAB_002_Analysis\FOR_Lab_002_Redline\FOR_Lab_002_Redline.mans

Start Your Investigation

☑ Show Home Page on Startup

I am Reviewing a Triage Collection from HX

Redline® works with FireEye Endpoint Threat Prevention Platform (HX)™ to help security analysts triage events they are reviewing in their SIEM / Log Management solution. HX integrates with these tools and automatically performs a "Triage Collection" on any endpoint involved in an alert.

You can open these Triage Collections in Redline and use the Timeline view to search for the network activity (by IP or DNS name) or host activity (such as malicious file name) and discover what process caused the activity. Using Redline features like TimeWrinkles™ and Timeline filtering (by process, for example) you can see what the process actually did: what files it created, what network connections it generated, and what registry keys it changed. This makes it easy to quickly assess whether the alert is a true compromise or not.

Investigate >

I am Investigating a Host Based on an External Investigative Lead

When you are starting with a piece of external information indicating that the host requires further examinining, you should start your investigation by using the Timeline and its powerful filtering capabilities to quickly hone in on your investigative lead and from there find additional items of interest to follow. If your initial lead is a timeframe of suspicious activity identified by an IDS, you can use TimeWrinkles™ to filter all events that occured around that timeframe. If your initial lead is malicious activity by a process or single user identified by an Indicator of Compromise, then you can use the Unique Process and Username filters to show only events that were generated by them.

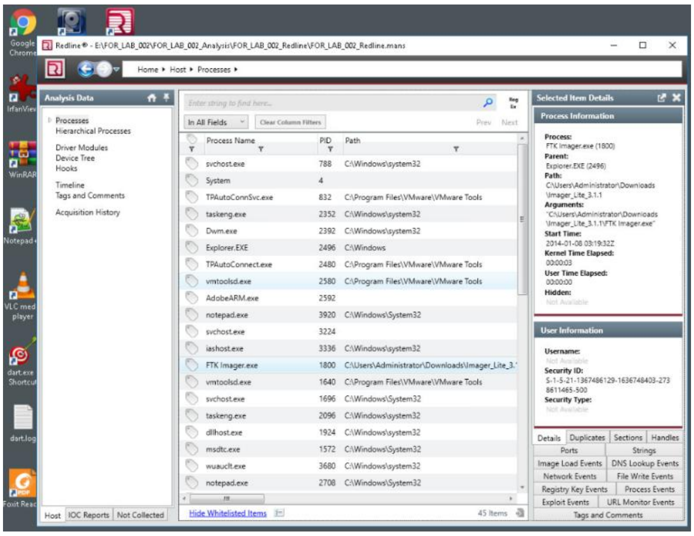
Investigate >

I am Reviewing Web History Data

When you are investigating web history data, you should start by reviewing the Browser URL History. In particular, review redirects which can lead to a malware server, and hidden visits which can includes sites with malicious code, and sites visited only once.

If you find a record that looks suspicious, use the Timeline field filters to investigate any file downloads or cookies being sent around the same time period.

Investigate >


Redline® - E:\FOR_LAB_002\FOR_LAB_002_Analysis\FOR_LAB_002_Redline\FOR_LAB_002_Redline.mans

Process Name	PID	Path
svchost.exe	788	C:\Windows\system32
System	4	
TPAutoConnSvc.exe	832	C:\Program Files\VMware\VMware Tools
taskeng.exe	2352	C:\Windows\system32
Dwm.exe	2392	C:\Windows\system32
Explorer.EXE	2496	C:\Windows
TPAutoConnect.exe	2480	C:\Program Files\VMware\VMware Tools
vmtoolsd.exe	2580	C:\Program Files\VMware\VMware Tools
AdobeARM.exe	2592	
notepad.exe	3920	C:\Windows\System32
svchost.exe	3224	
iashost.exe	3336	C:\Windows\system32
FTK Imager.exe	1800	C:\Users\Administrator\Downloads\Imager_Lite_3.'
vmtoolsd.exe	1640	C:\Program Files\VMware\VMware Tools
svchost.exe	1696	C:\Windows\System32
taskeng.exe	2096	C:\Windows\system32
dllhost.exe	1924	C:\Windows\system32
msdtc.exe	1572	C:\Windows\System32
wuauclt.exe	3680	C:\Windows\system32
notepad.exe	2708	C:\Windows\System32

Selected Item Details

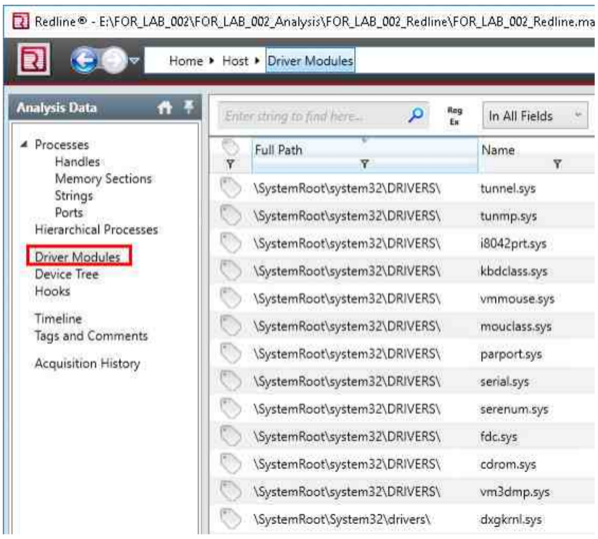
Process Information

Process: FTK Imager.exe (1800)
Parent: Explorer.EXE (2496)
Path: C:\Users\Administrator\Downloads\Imager_Lite_3.1.1
Arguments: "C:\Users\Administrator\Downloads\Imager_Lite_3.1.1\FTK Imager.exe"
Start Time: 2014-01-08 03:19:32Z
Kernel Time Elapsed: 00:00:03
User Time Elapsed: 00:00:00
Hidden: Not Available

User Information

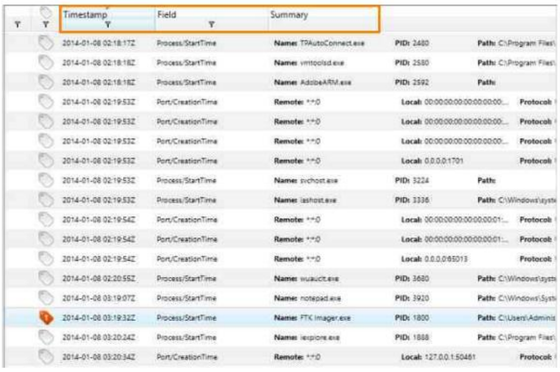
Username: Not Available
Security ID: S-1-5-21-1367486129-1636748403-2738611465-500
Security Type: Not Available

17. Another critical category is *Driver Modules*. This will reveal all the drivers that were loaded and running in RAM at the time of the capture. Select the **Driver Modules** option on the left navigation pane highlighted below. The window will show the names, full paths, and sizes of the loaded drivers, among other things. This is a great place to look for suspicious drivers that could be malicious.


Redline® - E:\FOR_LAB_002\FOR_LAB_002_Analysis\FOR_LAB_002_Redline\FOR_LAB_002_Redline.ma

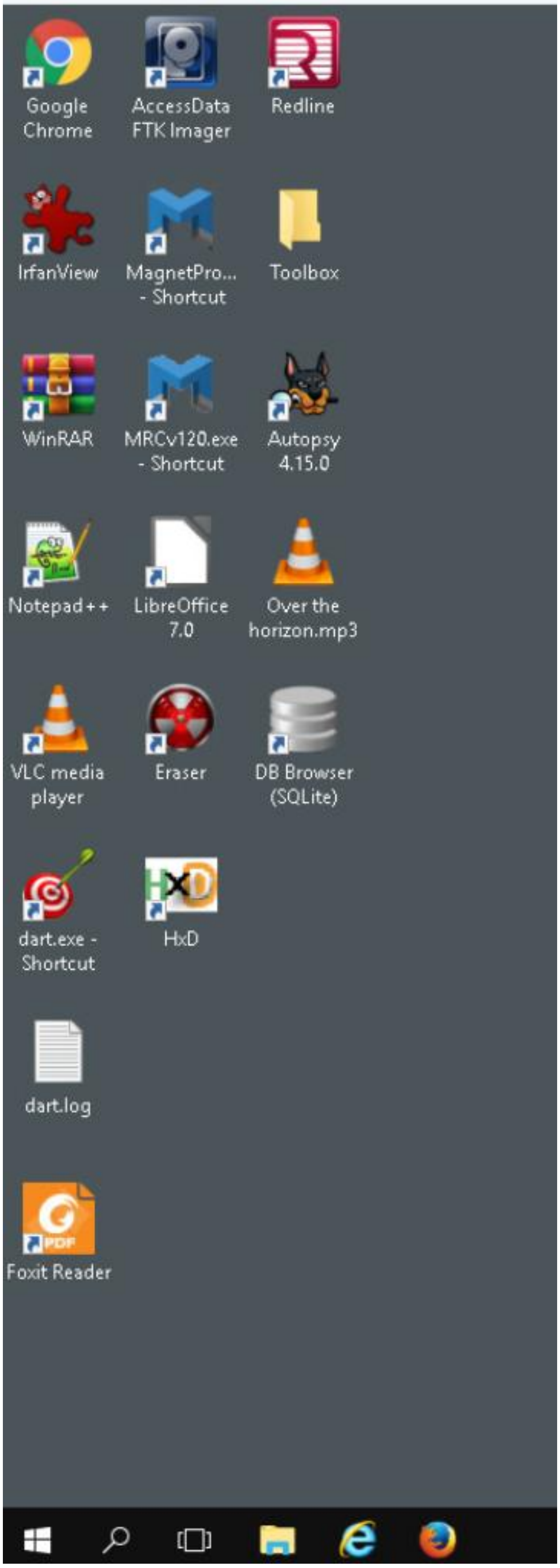
Full Path	Name
\SystemRoot\system32\DRIVERS\	tunnel.sys
\SystemRoot\system32\DRIVERS\	tunmp.sys
\SystemRoot\system32\DRIVERS\	i8042prt.sys
\SystemRoot\system32\DRIVERS\	kbdclass.sys
\SystemRoot\system32\DRIVERS\	vmmouse.sys
\SystemRoot\system32\DRIVERS\	mouclass.sys
\SystemRoot\system32\DRIVERS\	parport.sys
\SystemRoot\system32\DRIVERS\	serial.sys
\SystemRoot\system32\DRIVERS\	serenum.sys
\SystemRoot\system32\DRIVERS\	fdc.sys
\SystemRoot\system32\DRIVERS\	cdrom.sys
\SystemRoot\system32\DRIVERS\	vm3dmp.sys
\SystemRoot\System32\drivers\	dxgkrnl.sys

19. The timeline view has many options and choices for filtering out and narrowing the scope to a specific timeframe. For this exercise, leave the options in their default state and go over to the pane that contains the list of processes. The three column headings (**Timestamp, Field, and Summary**) highlighted below allow you to sort, filter, and review the processes and their details.



Timestamp	Field	Summary		
2014-01-08 02:18:17Z	Process/StartTime	Name: TPAutoConnect.exe	PID: 2480	Path: C:\Program Files\
2014-01-08 02:18:18Z	Process/StartTime	Name: vmtoolsd.exe	PID: 2580	Path: C:\Program Files\
2014-01-08 02:18:18Z	Process/StartTime	Name: AdobeARM.exe	PID: 2592	Path:
2014-01-08 02:19:53Z	Port/CreationTime	Remote: *:*:0	Local: 00:00:00:00:00:00:00:00:...	Protocol:
2014-01-08 02:19:53Z	Port/CreationTime	Remote: *:*:0	Local: 00:00:00:00:00:00:00:00:...	Protocol:
2014-01-08 02:19:53Z	Port/CreationTime	Remote: *:*:0	Local: 00:00:00:00:00:00:00:00:...	Protocol:
2014-01-08 02:19:53Z	Port/CreationTime	Remote: *:*:0	Local: 0.0.0.0:1701	Protocol:
2014-01-08 02:19:53Z	Process/StartTime	Name: svchost.exe	PID: 3224	Path:
2014-01-08 02:19:53Z	Process/StartTime	Name: iashost.exe	PID: 3336	Path: C:\Windows\syste
2014-01-08 02:19:54Z	Port/CreationTime	Remote: *:*:0	Local: 00:00:00:00:00:00:00:01:...	Protocol:
2014-01-08 02:19:54Z	Port/CreationTime	Remote: *:*:0	Local: 00:00:00:00:00:00:00:01:...	Protocol:
2014-01-08 02:19:54Z	Port/CreationTime	Remote: *:*:0	Local: 0.0.0.0:65013	Protocol:
2014-01-08 02:20:55Z	Process/StartTime	Name: wuauclt.exe	PID: 3680	Path: C:\Windows\syste
2014-01-08 03:19:07Z	Process/StartTime	Name: notepad.exe	PID: 3920	Path: C:\Windows\Syste
2014-01-08 03:19:32Z	Process/StartTime	Name: FTK Imager.exe	PID: 1800	Path: C:\Users\Adminis
2014-01-08 03:20:24Z	Process/StartTime	Name: iexplore.exe	PID: 1888	Path: C:\Program Files\
2014-01-08 03:20:34Z	Port/CreationTime	Remote: *:*:0	Local: 127.0.0.1:50461	Protocol:

20. Using the basic features we've introduced, you should be able to identify processes and programs that were running at the time of the RAM Capture.
21. If you got all the answers right, then that takes you one step closer to being a great digital forensic examiner and incident response specialist. There are many other tools available to perform RAM analysis. The tools and methods we revealed in this lab will whet your appetite and hopefully motivate you to explore more advanced methods of RAM analysis.
22. The lab is now complete; close *REDLINE* and any other open windows by clicking the **X** at the top-right corner of the window. You may end the reservation.


Google Chrome
AccessData FTK Imager
Redline
IrfanView
MagnetPro... - Shortcut
Toolbox
WinRAR
MRCv120.exe - Shortcut
Autopsy 4.15.0
Notepad++
LibreOffice 7.0
Over the horizon.mp3
VLC media player
Eraser
DB Browser (SQLite)
dart.exe - Shortcut
HxD
dart.log
Foxit Reader