



FORENSICS V2 LAB SERIES

Lab 02: Live Acquisition

Document Version: 2021-01-14

Copyright © 2021 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation in the United States and other countries. Google is a registered trademark of Google, LLC. Amazon is a registered trademark of Amazon in the United States and other countries.

Contents

Introduction	3
Objectives.....	3
Lab Topology	4
Lab Settings	5
1 Getting Familiar with Magnet Process Capture.....	6
2 Exporting Processes Using Magnet Process Capture	9
3 Getting Familiar with Magnet RAM Capture	15
4 Live RAM Capture	17
5 Carving files from RAM	22
6 Getting Familiar with REDLINE.....	32
7 Review the RAM Capture Using REDLINE	34

Introduction

RAM Analysis/Memory Forensics can reveal a lot of important information about its user(s) and a system. As the name suggests, the data in Random Access Memory is volatile, and oftentimes, the data never reaches the permanent storage (HDD). This lab aims to teach the student how to acquire RAM from a Windows OS and search the results to identify any data of evidentiary value. Let us get started!!

Objectives

- Create a Magnet Process capture '.dmp'
- Create a '.raw' image
- Import the Memory image '.mem' and conduct a raw keyword search

Lab Topology



Lab Settings

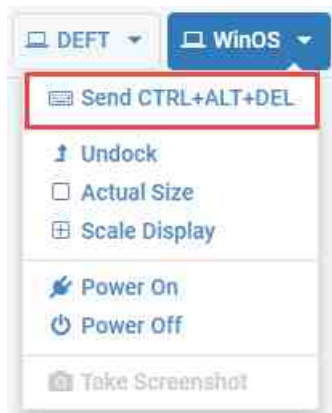
The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address / Subnet Mask	Account (if needed)	Password (if needed)
Caine	172.16.16.30	caine	Train1ng\$
CSI-Linux	172.16.16.40	csi	csi
DEFT	172.16.16.20	deft	Train1ng\$
WinOS	172.16.16.10	Administrator	Train1ng\$

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.

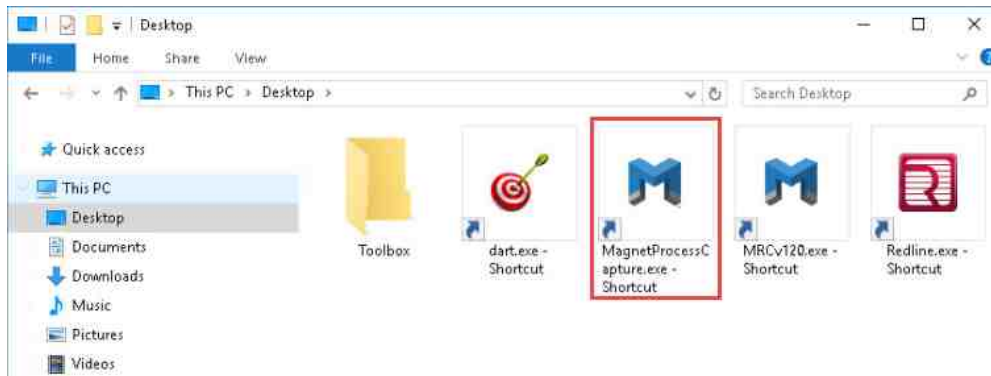
1. To begin, launch the WinOS virtual machine to access the graphical login screen.
 - a. Select Send CTRL+ALT+DEL from the dropdown menu to be prompted with the login screen.



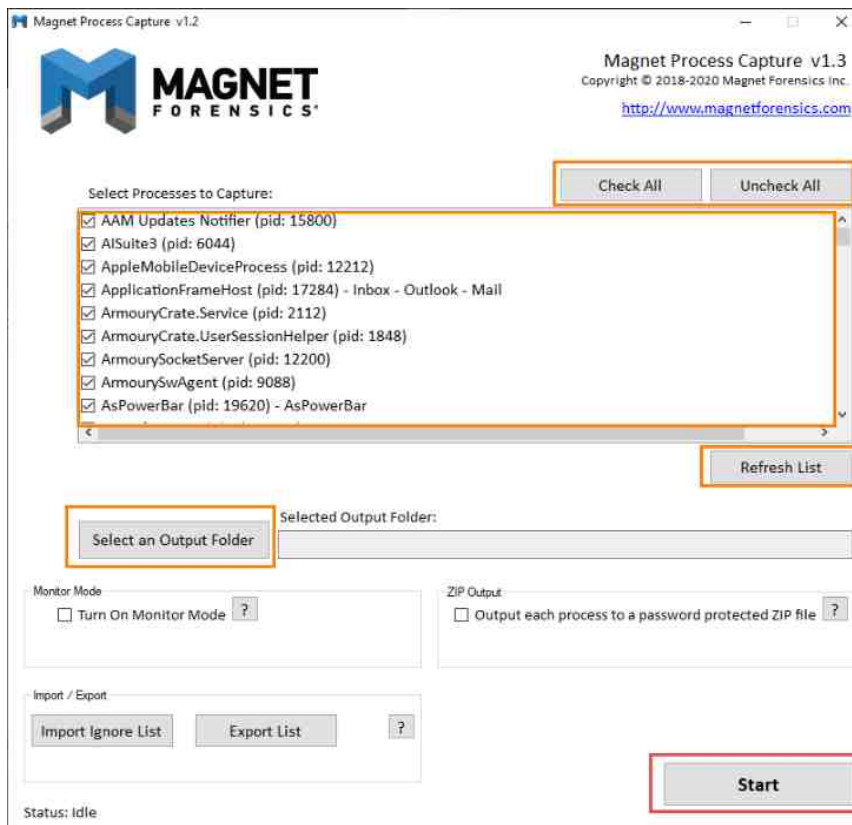
- b. Log in as Administrator using the password: Training\$
2. Once you are logged into the VM, open file explorer by clicking the icon on the taskbar as highlighted in red below.



3. Within file explorer, browse to Desktop and double-click the shortcut file named MagnetProcessCapture.exe-Shortcut highlighted below.



4. You should see the following window appear. The table below the screenshot outlines the purpose of the functions we will be using in our exercise. For information on the ones that were omitted, click the question mark? beside them.

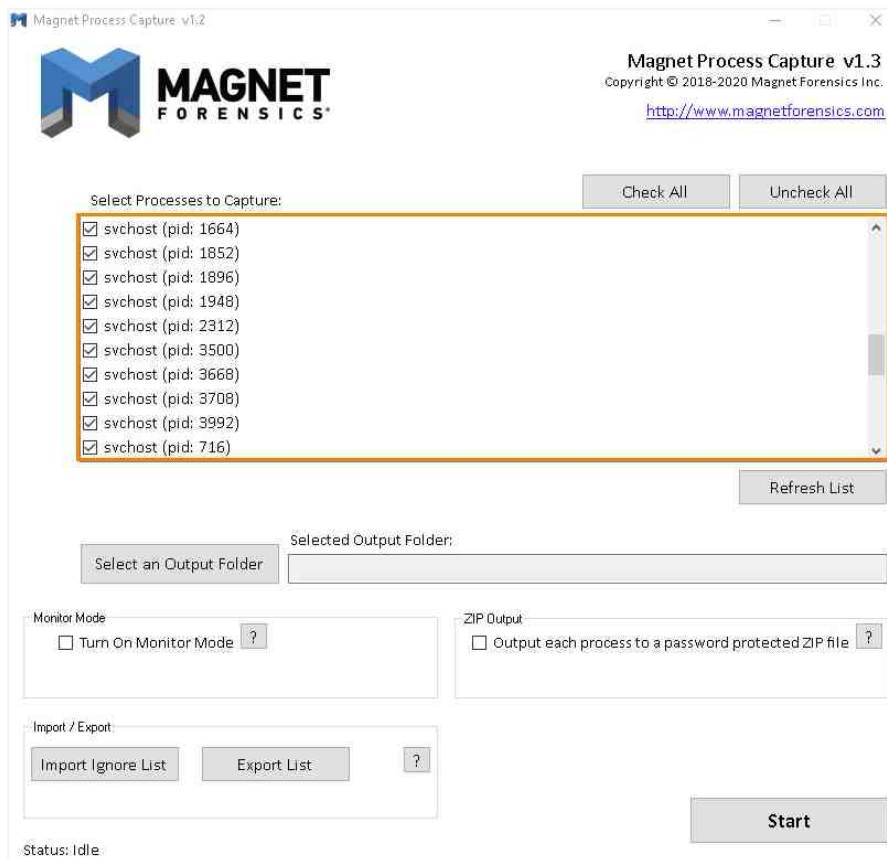


Check All & Uncheck All	These buttons provide the ability to select or unselect all the listed processes by placing checkmarks in the box beside the processes.
Select Processes to Capture pane	This is the primary window in the Magnet Acquire interface and reveals all the currently running processes on the host system. Each process is listed by process name and process ID, as well as a checkbox to choose between the processes that you intend to acquire.
Refresh List	This button is located at the bottom-right corner of the Select Processes to Capture window and allows you to refresh the list of running processes.
Select an Output Folder	The button is located on the left side of the window below the Refresh List button and allows you to browse for a location to store the captured processes.
Start	This button is located at the bottom-right corner of the window and allows you to start the capture of the selected processes.

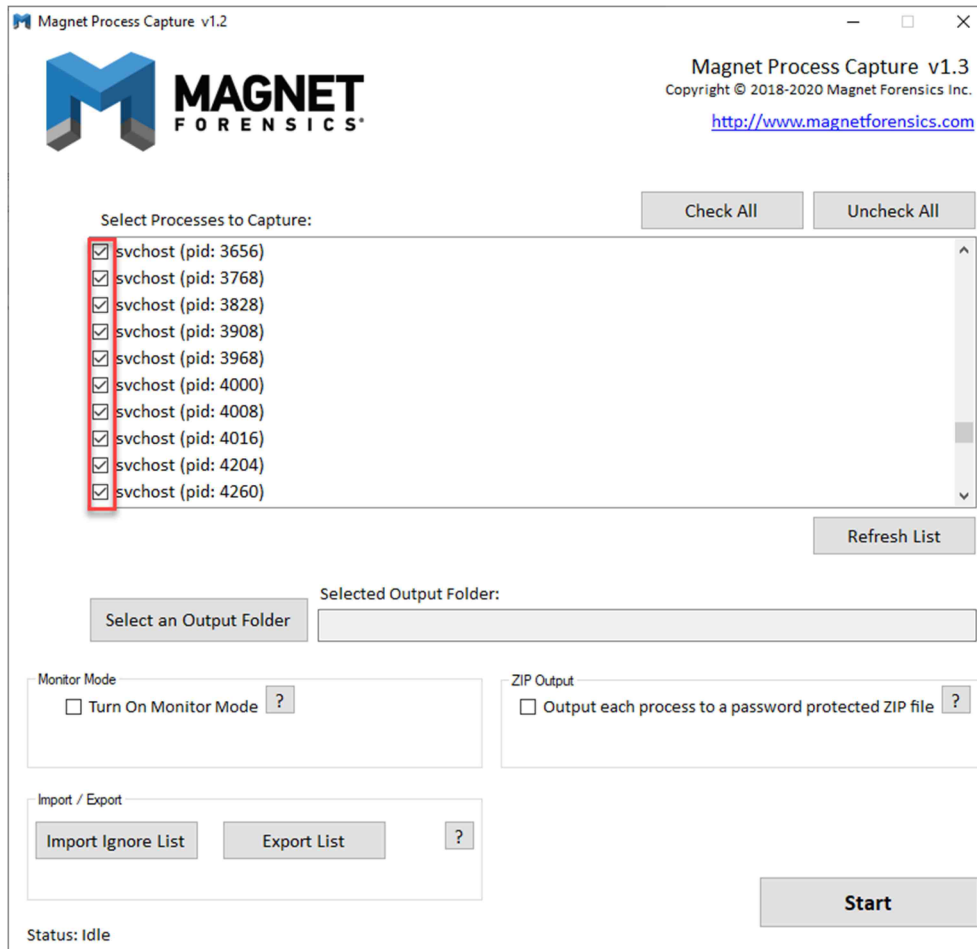
2 Exporting Processes Using Magnet Process Capture

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.

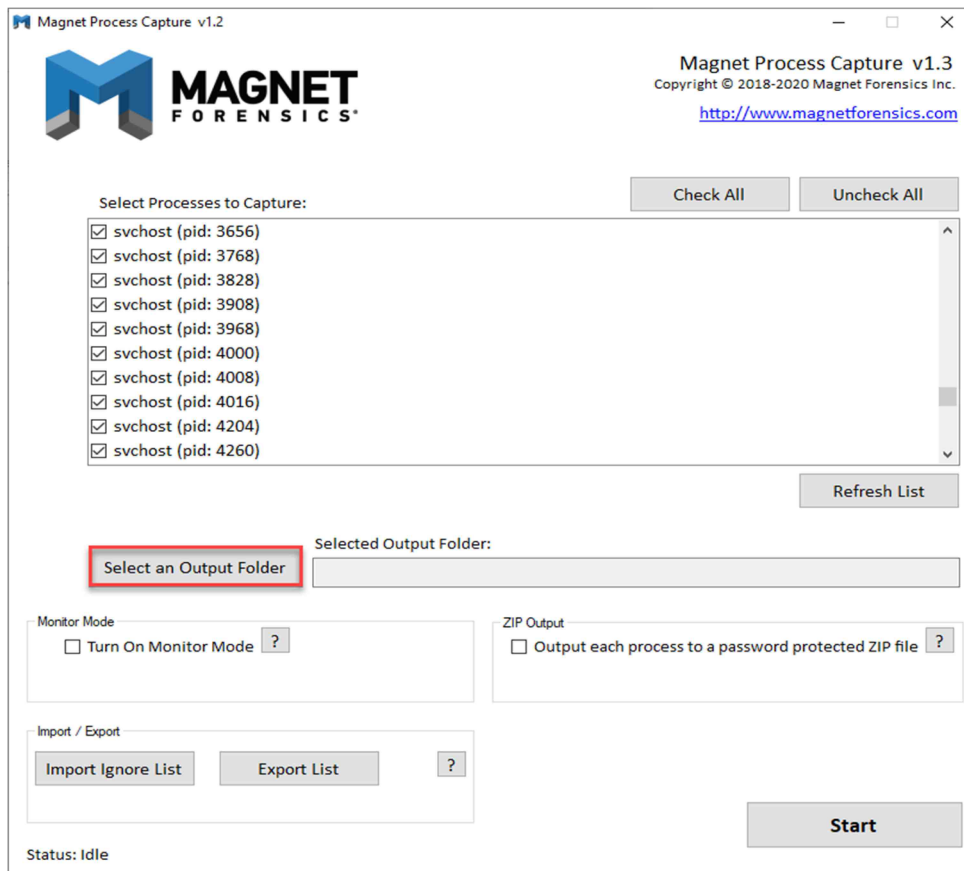
1. Magnet Process Capture should already be open. If it is not, reopen it and look at the Select Processes to Capture pane as highlighted below. Scroll through the list of processes to see if there are any that you recognize.



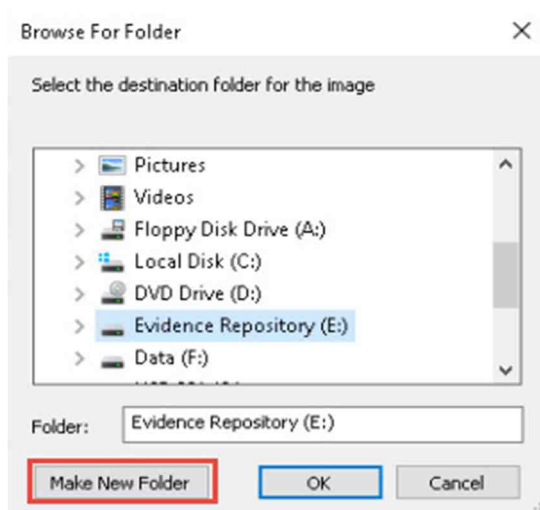
2. There may be cases where you do not need to capture all the listed processes; this tool allows you to choose the ones you want. If in doubt, it is always best to get everything and then eliminate the unnecessary ones. We will be exporting only the svchost processes for this exercise. Ensure that all the svchost processes are checkmarked by scrolling through the Select Processes to Capture pane and clicking each one. Ensure the checkboxes are all checked as seen below.



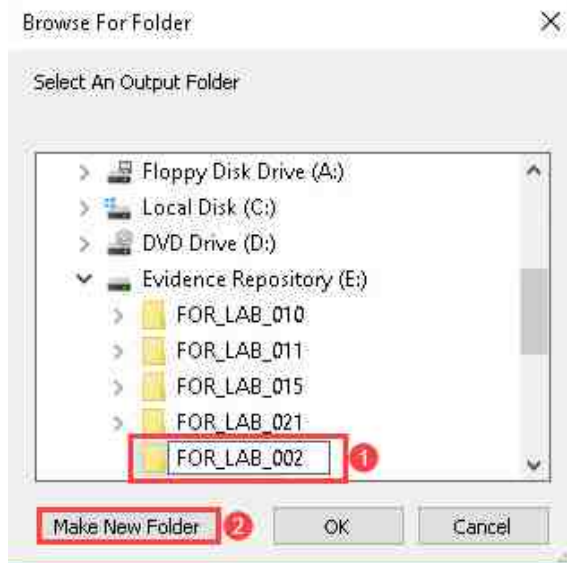
- Once you have verified that all the processes are selected, click the Select an Output Folder as highlighted below.



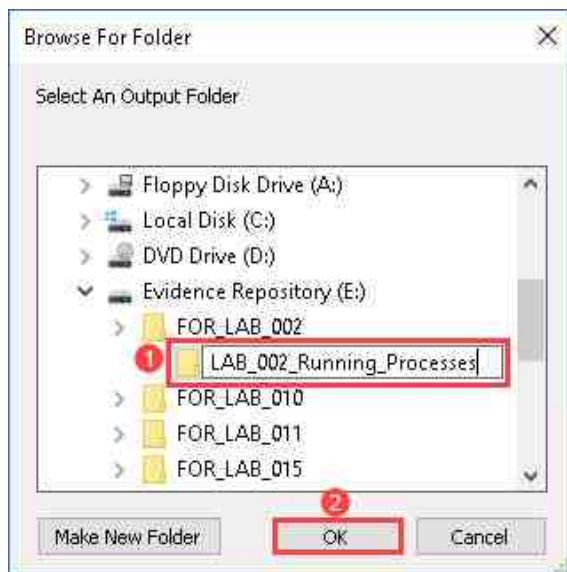
- This will reveal the Browse For Folder window, which will allow you to choose the destination for the captured processes. It is very important that all exports be stored on a separate disk drive to reduce the risk of overwriting data on the hard disk. In this exercise, we will simulate this by storing the output on the E:\ drive. Browse to the E:\ volume titled: Evidence Repository by navigating to This PC > Evidence Repository (E:) and clicking the Make New Folder button highlighted below.



5. Name the folder FOR_LAB_002 as seen in item 1 below. Next, click Make New Folder as seen in item 2 to create a subfolder inside FOR_LAB_002.

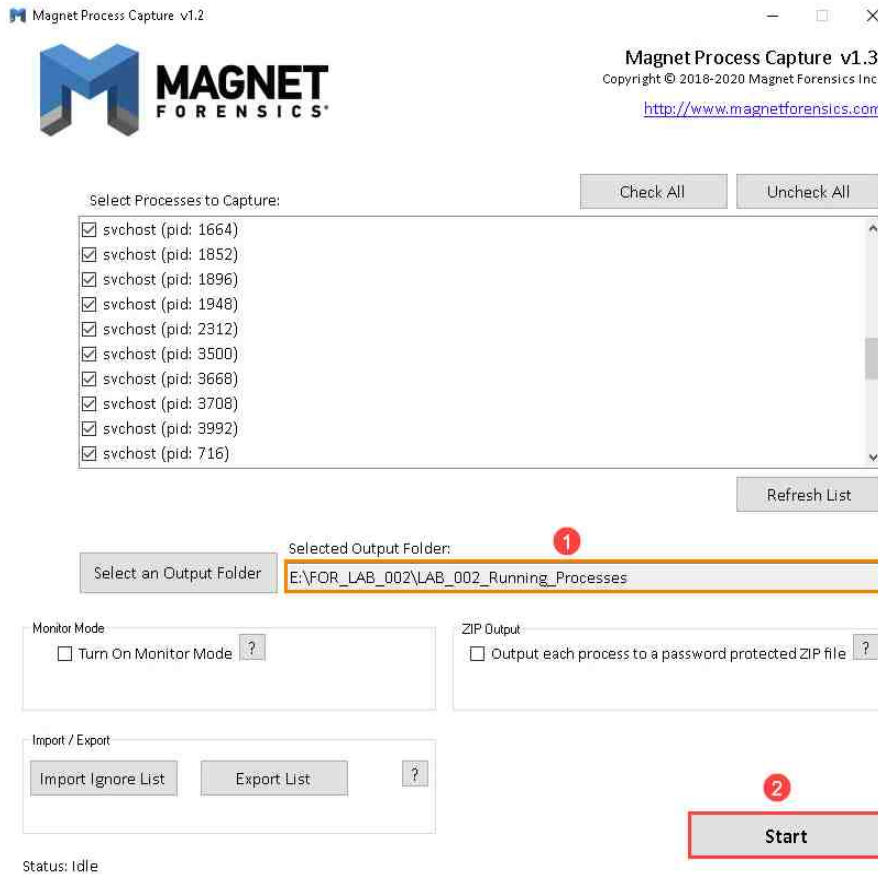


6. Name the new subfolder LAB_002_Running_Processes as seen in item 1 below. Once you have named the folders correctly, select the one titled LAB_002_Running_Processes and click the OK button highlighted in item 2 below.



Check that the process destination path (E:) is correct. It is common for the path to remain as New Folder, even after you rename it.

7. Great, you made it here, and you are now ready to complete the capture. Before beginning, verify that you have the correct path selected and if everything is correct, press the Start button seen in item 2 below. Remember to verify that the path is correct before proceeding.



The screenshot shows the Magnet Process Capture v1.3 application window. The title bar reads "Magnet Process Capture v1.2". The window contains the Magnet Forensics logo, version information, and a website link. A list of processes to capture is shown, all with "svchost" as the name and various PIDs. Below this list are buttons for "Check All", "Uncheck All", and "Refresh List". A "Selected Output Folder" field is highlighted with a red circle and the number 1, showing the path "E:\FOR_LAB_002\LAB_002_Running_Processes". Below this are sections for "Monitor Mode" (with a "Turn On Monitor Mode" checkbox), "ZIP Output" (with an "Output each process to a password protected ZIP file" checkbox), and "Import / Export" (with "Import Ignore List" and "Export List" buttons). A "Start" button is highlighted with a red circle and the number 2. The status at the bottom left is "Status: Idle".

Magnet Process Capture v1.2

MAGNET FORENSICS

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

Select Processes to Capture:

Check All Uncheck All

- ☒ svchost (pid: 1664)
- ☒ svchost (pid: 1852)
- ☒ svchost (pid: 1896)
- ☒ svchost (pid: 1948)
- ☒ svchost (pid: 2312)
- ☒ svchost (pid: 3500)
- ☒ svchost (pid: 3668)
- ☒ svchost (pid: 3708)
- ☒ svchost (pid: 3992)
- ☒ svchost (pid: 716)

Refresh List

Select an Output Folder

Selected Output Folder: **E:\FOR_LAB_002\LAB_002_Running_Processes**

Monitor Mode

☐ Turn On Monitor Mode ?

ZIP Output

☐ Output each process to a password protected ZIP file ?

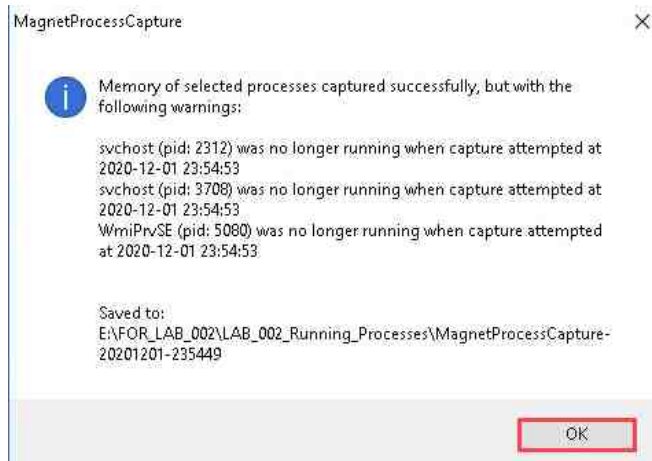
Import / Export

Import Ignore List Export List ?

Status: Idle

Start

8. When the capture is done, you will see the following window pop up. It is normal to get warnings that processes are no longer running as it depends on how long it takes you to get the capture started. Click OK to close the window.

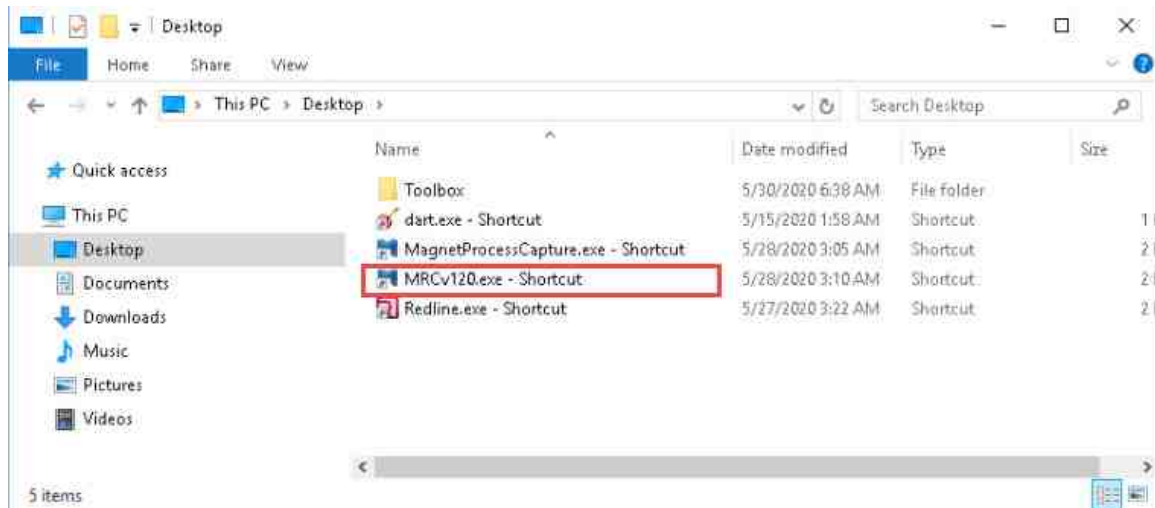


9. You have successfully captured specific processes and the contents of RAM associated with those processes. This ends the selective processes portion of the lab. Close the program by clicking the X at the top-right corner of the window.

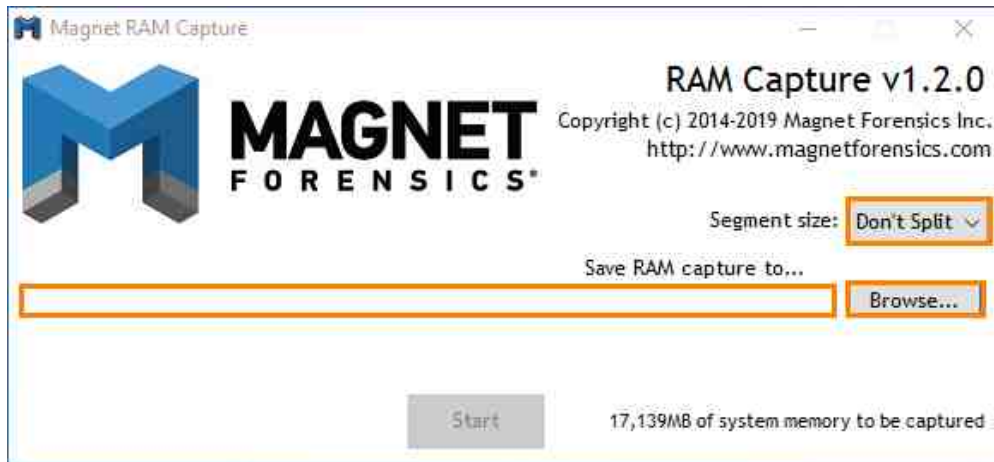
3 Getting Familiar with Magnet RAM Capture

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.

1. Within file explorer, browse to Desktop, double-click the file titled MRCv120.exe - Shortcut highlighted below.



- You should see the following window appear. The table below the screenshot outlines the purpose of the highlighted sections on the Magnet RAM Capture window.

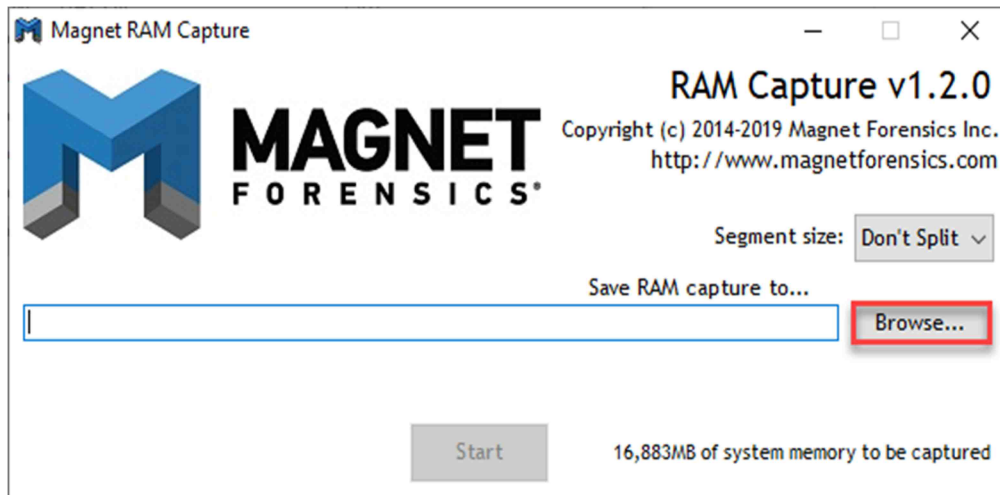


Save RAM capture to...	This is a textbox that will show the location at which you intend to store the RAM capture.
The Browse button	This button allows the user to browse to the drive/folder that the RAM capture will be stored in.
Segment Size	This dropdown menu allows you to choose the segment size 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.

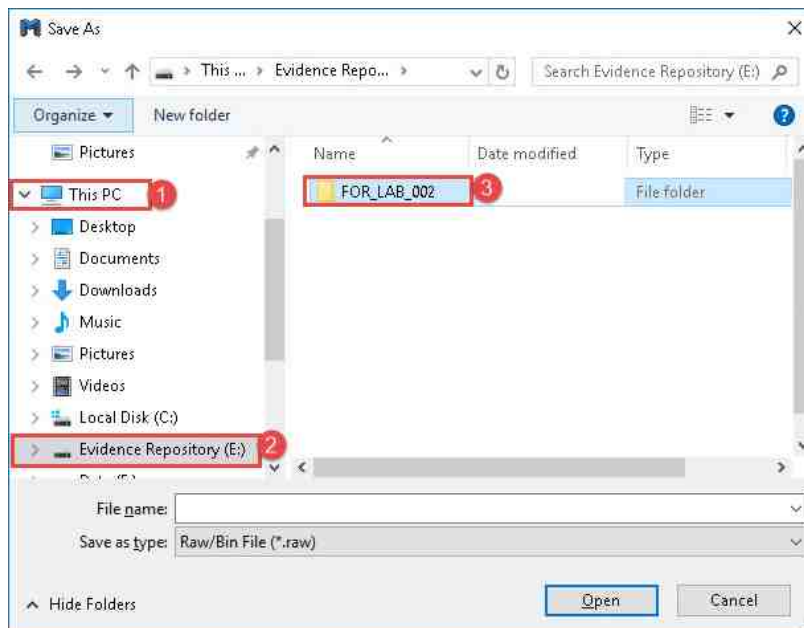
4 Live RAM Capture

Now that you are familiar with the RAM capture tool, we will teach you how to use it to make a copy of RAM that you can later analyze.

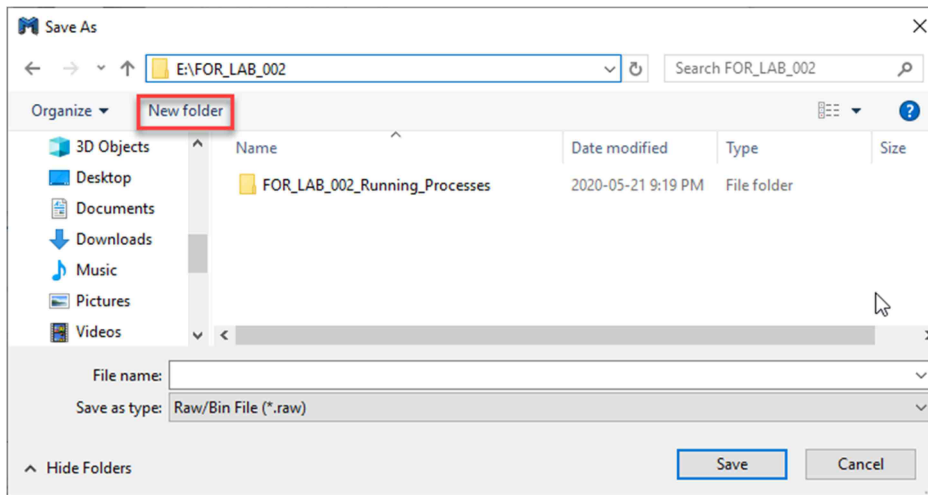
1. Magnet RAM Capture should already be open. If it is not, reopen it and select the Browse button highlighted in red below.



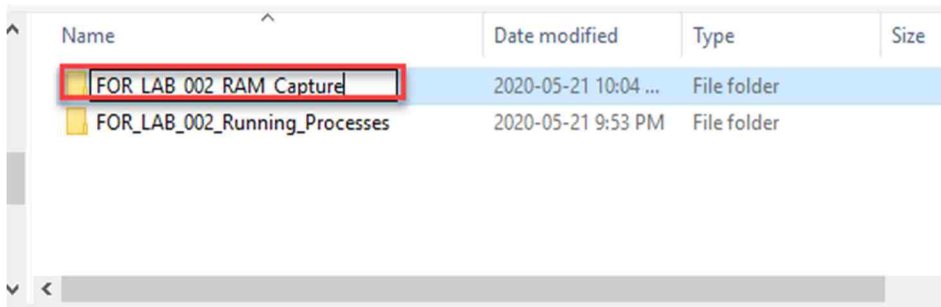
2. The Save as window will pop up. It allows you to choose the destination for the captured RAM data. It is very important that all exports be stored on a separate disk drive to reduce the risk of overwriting data on the host's hard disk. In this exercise, we will simulate this by storing the output on the volume titled Evidence Repository (E:). Browse to it by navigating to This PC > Evidence Repository (E:) and double-click the folder you created called FOR_LAB_002 to view its contents as seen below.



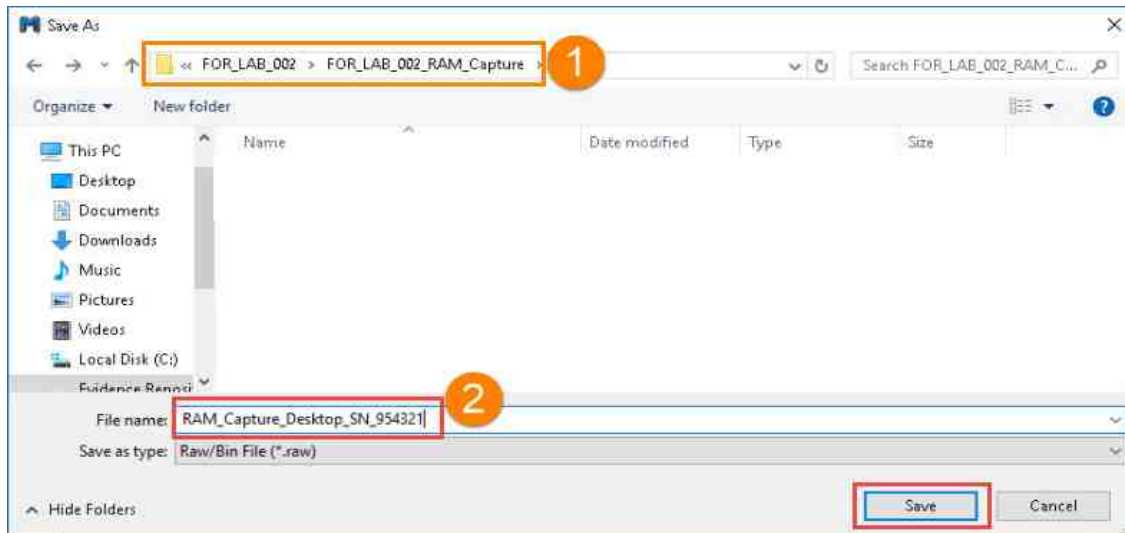
3. Create a new folder by clicking the New folder button highlighted below.



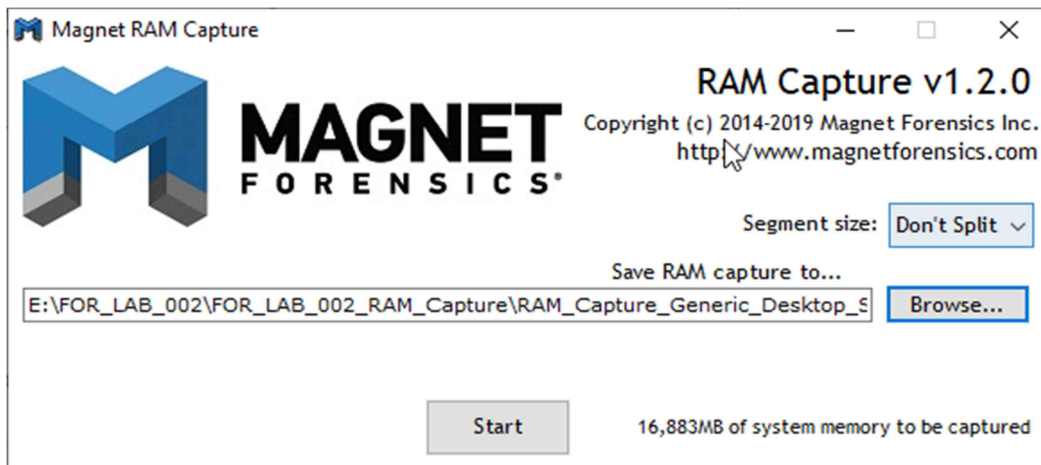
4. A new folder will appear; name it FOR_LAB_002_RAM_Capture as highlighted below.



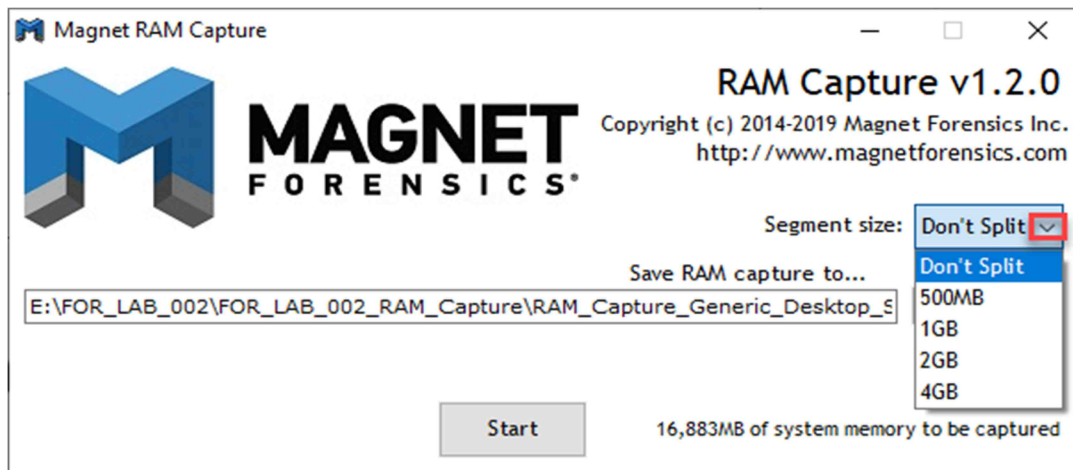
- Open the folder you named FOR_LAB_002_RAM_Capture by double-clicking on it. You now need to give the RAM Capture file a name before proceeding. Name the file RAM_Capture_Generic_Desktop_SN_954321. Once you are done typing the name, verify that everything is correct. Check the path and name, as seen in 1 and 2 below. If everything matches the path and filename seen below, then you are good to go. Click the Save button as seen below.



- You will return to the main window, which should look something like you see in the screenshot below.

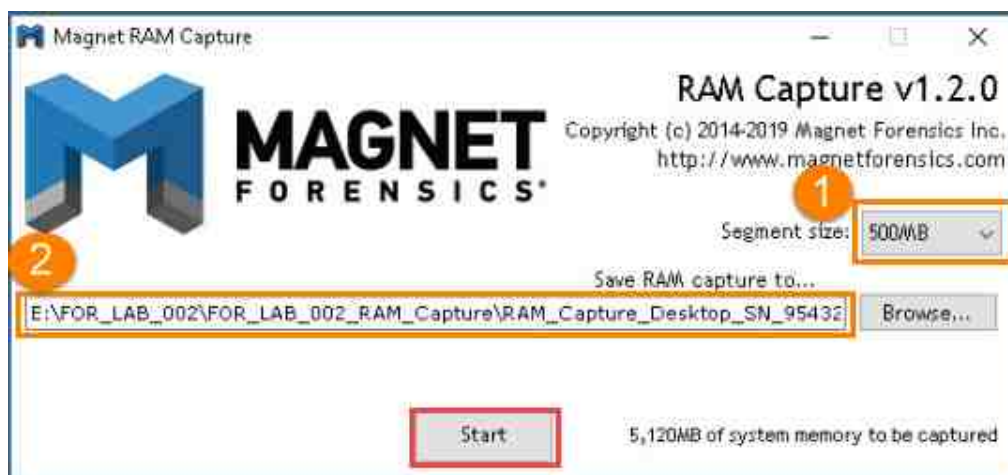


- Before proceeding, change the segment size option by clicking the arrow highlighted below.

**Please Note**

This option is important, especially if you are imaging to a USB drive that is formatted with a FAT32 file system which cannot store segments larger than 4GB.

- Let us use a 500MB segment size for this capture. Now that you are at this stage, do a verification by ensuring items 1 and 2, highlighted below, are correct. If you are comfortable with the settings, click the Start button highlighted above:

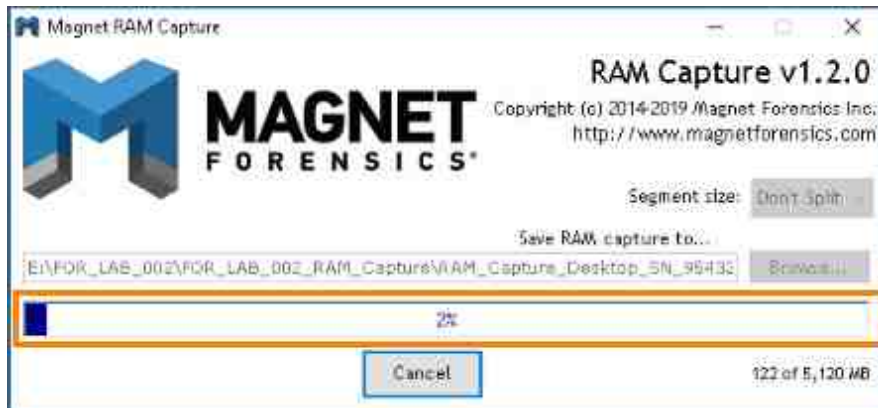


Changing the segment size to 500MB means that the individual files that make up the RAM capture will not grow larger than 500MB.

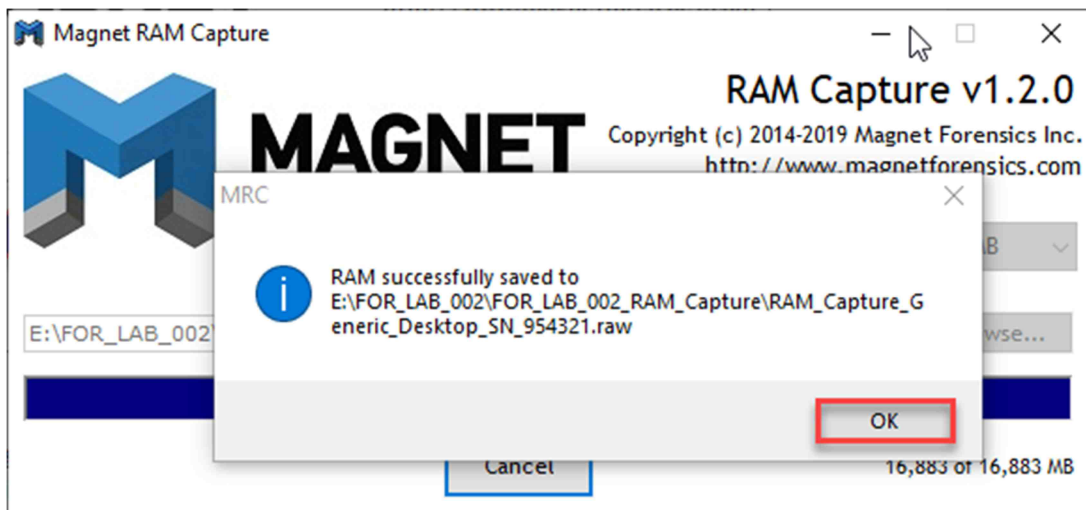


You may choose to cancel the RAM Capture at this point and skip steps 9, 10, and 11. The RAM captured from this process will not be a part of this lab, however, a preconfigured RAM acquisition was done and stored to be analyzed for section 5.

9. The process has started! You will see the progress bar moving, and a percentage will show the status as highlighted below.



10. When you are done imaging, you will see a pop-up window informing you that your capture was successful. Click OK as highlighted below.



11. If you are here, that means you did everything correctly, and you now have a full RAM capture. Your data is now ready to be analyzed.
12. You can move on to the next exercise, but before continuing, close Magnet RAM Capture and any other open windows by clicking the X at the top-right corner of the windows.

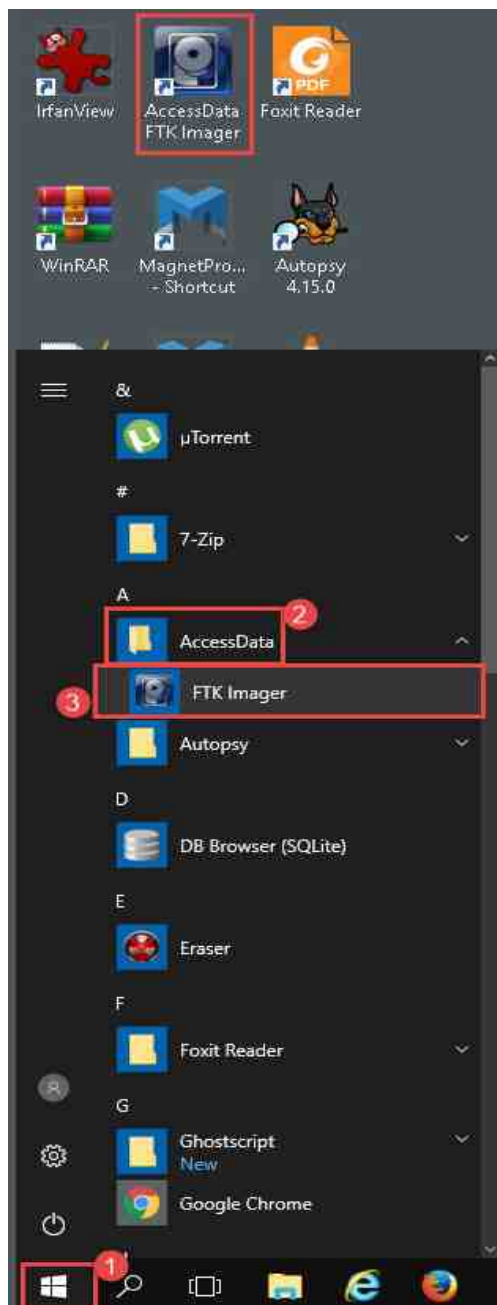


Due to the configuration of the lab, resources are limited and to ensure the other labs function as intended. If steps 9, 10 and 11 were completed, please delete the folder containing the Memory dump RAM_Capture_Generic_Desktop_SN_954321.raw located at This PC > Evidence Repository (E:) > LAB_002 > FOR_LAB_002_RAM_Capture

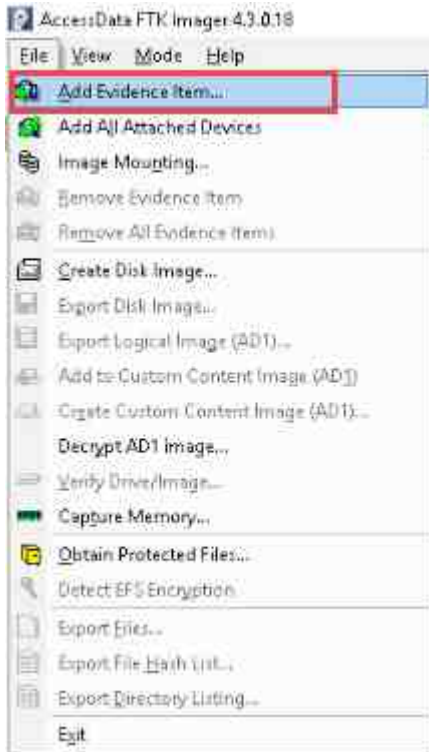
5 Carving files from RAM

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.

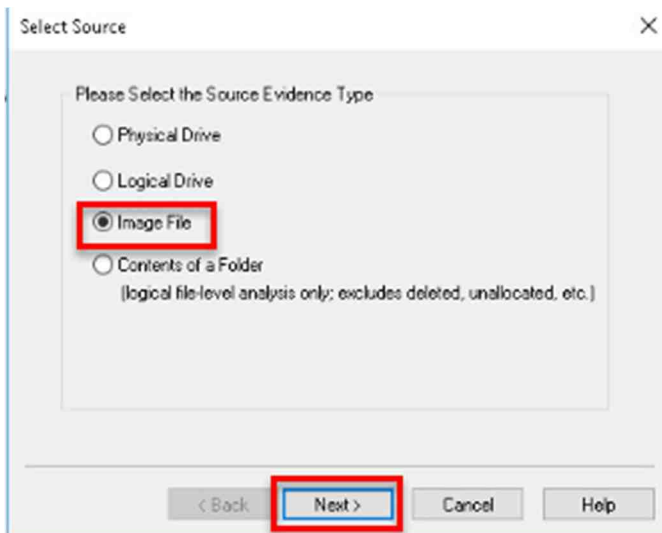
1. In this exercise, we will show you how to use FTK Imager to carve a jpeg file from a RAM Capture. We will not be using the images you made; instead, we will use some preconfigured RAM dumps. You should already be familiar with FTK Imager from LAB 1, so we will skip the formalities and jump right into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



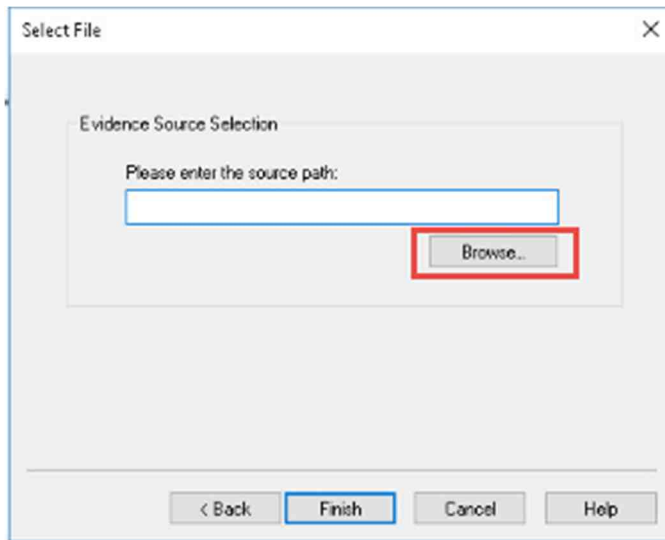
- Once you have FTK Imager open, let us load a RAM Capture. Do this by selecting the options File > Add Evidence Item, which will open the Select Source window.



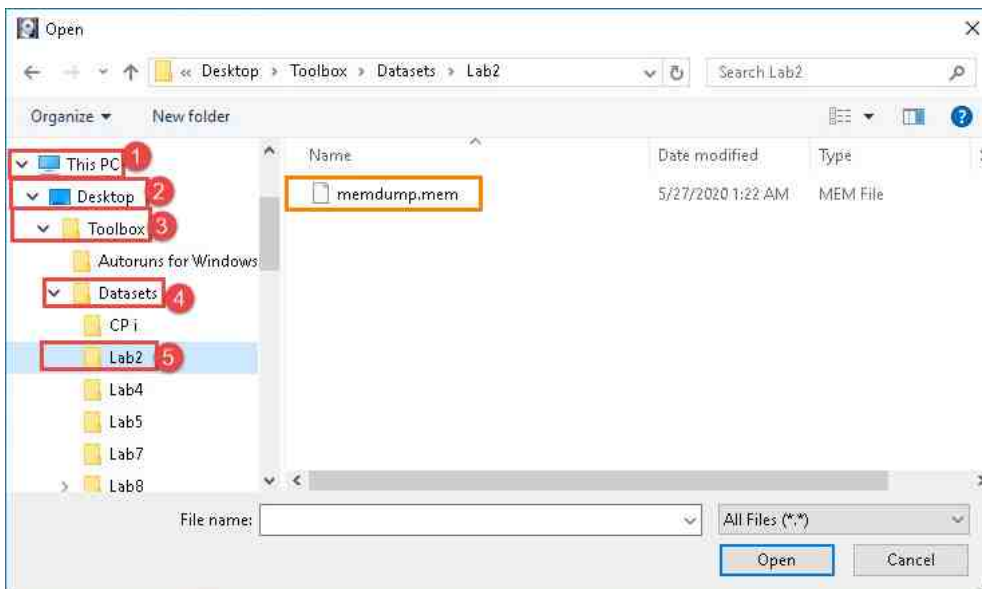
- In the Select Source window, select the Image File radio button and then select Next to proceed to the Select File window.



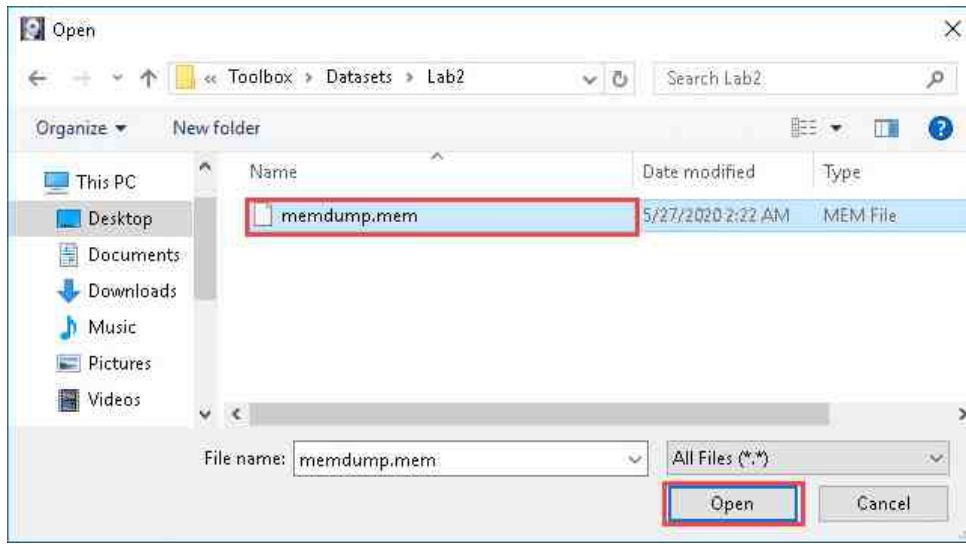
4. In the Select File window, click Browse highlighted in red in the screenshot below. This will open the File Selection window, which will allow you to browse to the appropriate image file.



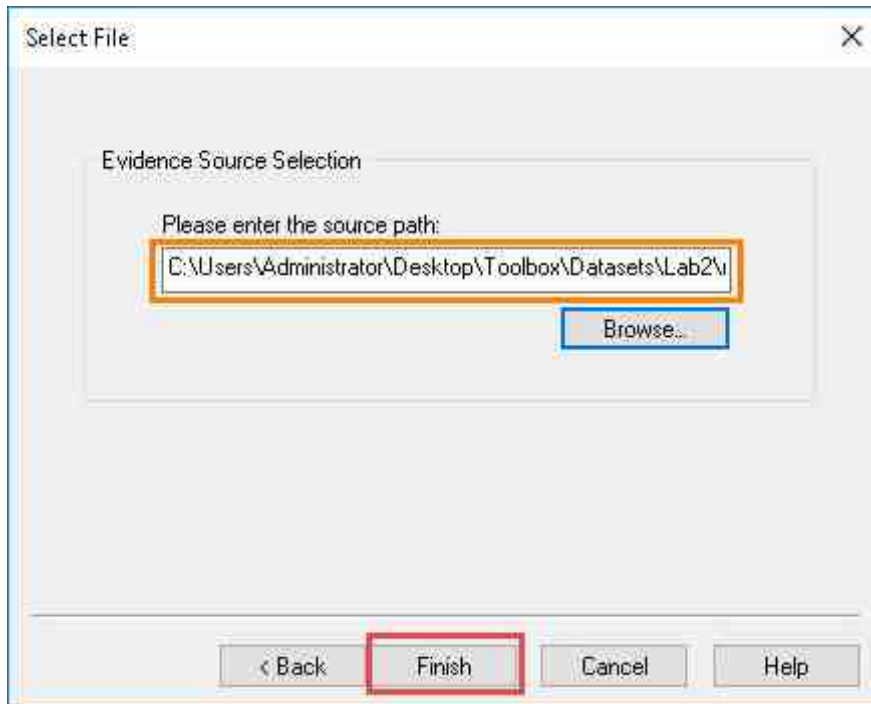
5. You are now at the Select File window. Browse to This PC > Desktop > Toolbox > Datasets > Lab2 as seen in items 1 - 5 below. This will open the folder revealing a RAM Capture called memdump.mem.



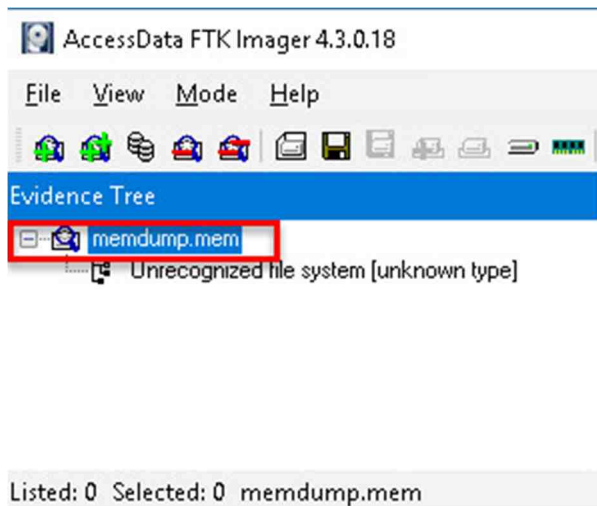
6. Select the file named memdump.mem and click the Open button as highlighted below. This will take you back to the Select file window.



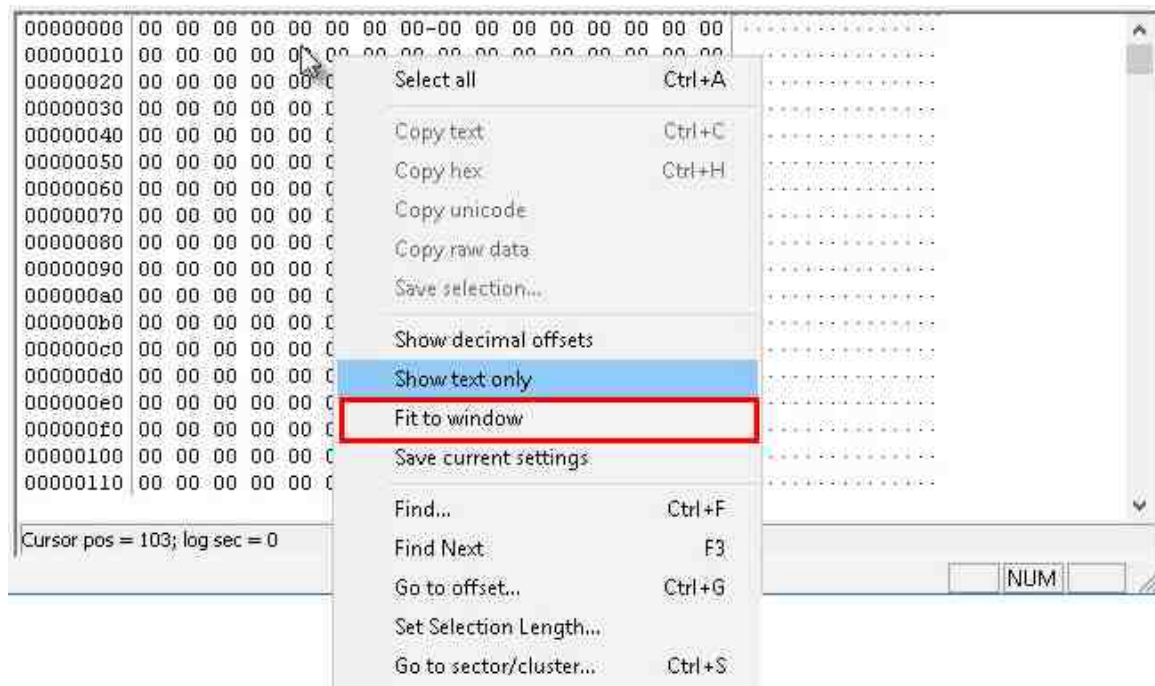
7. In the Select File window, verify that the path of the selected file matches the one highlighted in the screenshot below. Once you have verified, click the Finish button at the bottom of the window highlighted below. This will take you to the main GUI where the image will be loaded in the Evidence Tree pane.



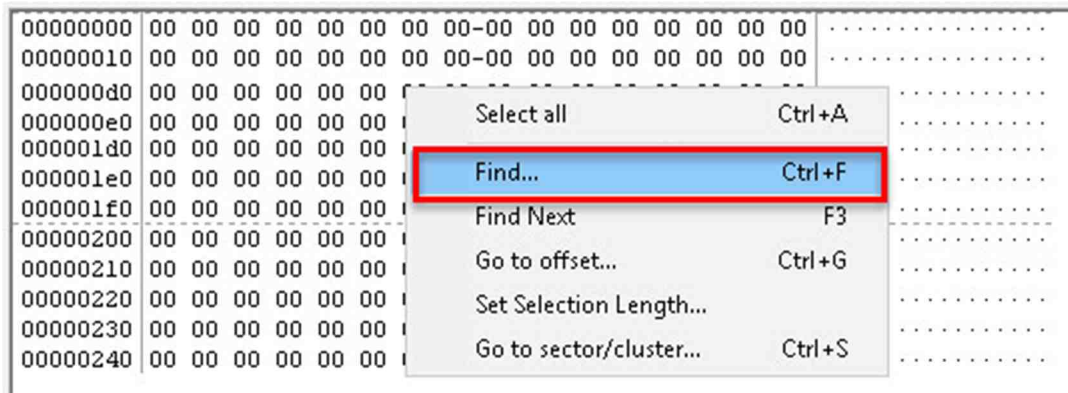
8. In the Evidence Tree pane, click the tree item memdump.mem highlighted below. This will select the image you are going to peruse.



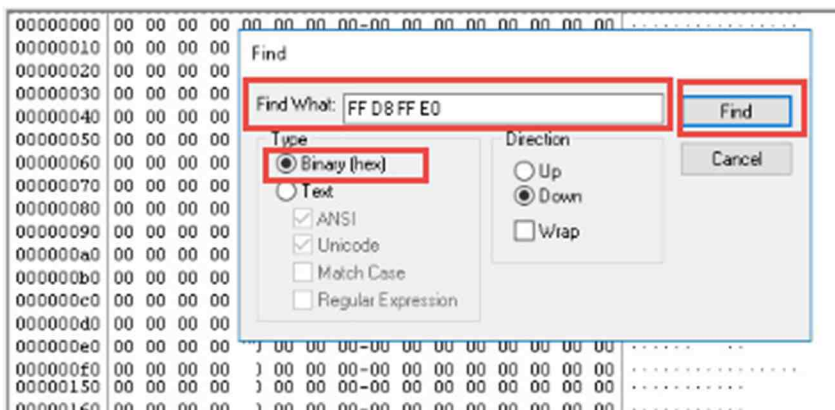
9. Now, turn your attention to the view pane at the bottom-right corner of the FTK Imager GUI window. This pane will show the RAW textual and hexadecimal interpretation of the RAM Capture. The first thing we will do is make the data more visible by expanding our view area. To do this, right-click anywhere in the view pane area and click Fit to window as seen below.



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 ÿÛ 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.



11. This will open the Find window that provides a search bar. Under the Type section, select the Binary (hex) radio button and then place the cursor in the Find What field and type the JPEG header FF D8 FF E0 as highlighted below. If you entered the header correctly, click Find:



12. If you got everything correctly, then your search will begin. Find will take you to the next occurrence of the string FF D8 FF E0 as seen below.

```

| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF 00
| 00 00 00 00 FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00
| 5F 50 52 4F 46 49 4C 45 00 01 01 00 00 02 90 6C 63 6D
| 63 70 72 74 00 00 01 40 00 00 00 4E 77 74 70 74 00 00
| A4 00 00 00 2C 72 58 59 5A 00 00 01 D0 00 00 00 14 62
| 59 38 94 2A 34 58 B1 4B 48 71 6A E7 BC 49 4F 60 94 FF
| 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58

```


13. Now that you found the string, verify that it is correct by looking at the matching text string on the right to see if it is `ÿØÿä . . JFIF` as highlighted below.

```

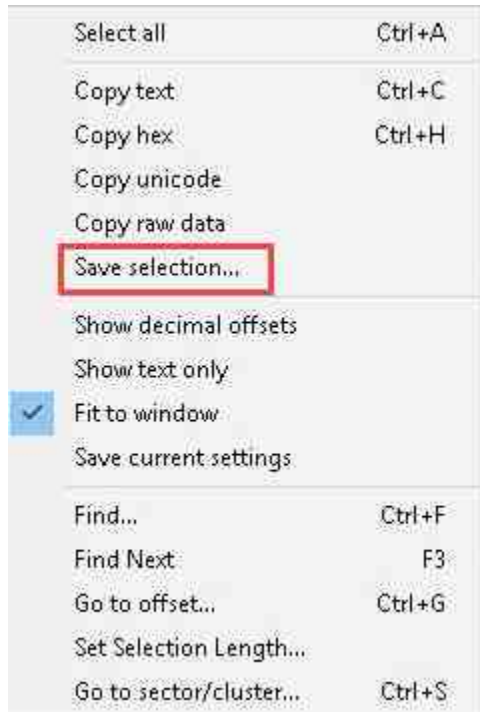
.....YY
.YYYY.....yøÿä..JFIF.....ÿä..ICC_PR
OFILE.....lcms-0..mntrRGB XYZ..ÿ.....;:acs
pAPPL.....öÖ.....ó-lcms.....d
esc.....8cprt..@..Nwtpt.....chad..*,
rXYZ..Ð.....bXYZ..ä.....gXYZ..ø.....rTRC
gTRC..,..bTRC..-L..chrn..-l..$mluc
.....enUS.....s-R-G-B..b-u-i-l-t..-i-n-m

```

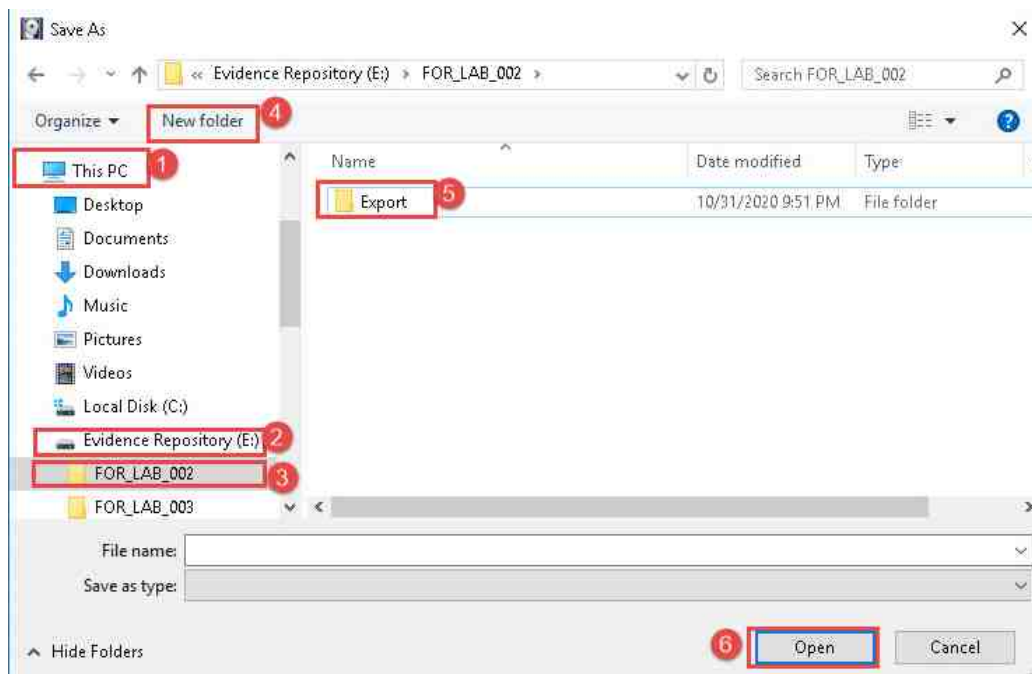
14. This is the tricky part; you must now highlight the data by clicking and holding the left mouse button down and sweeping from the beginning of FF D8 FF E0. You will need to continue sweeping and highlighting until you get to FF D9. An example can be seen highlighted below. Do not feel bad if you do not get it on your first try.

[illegible]

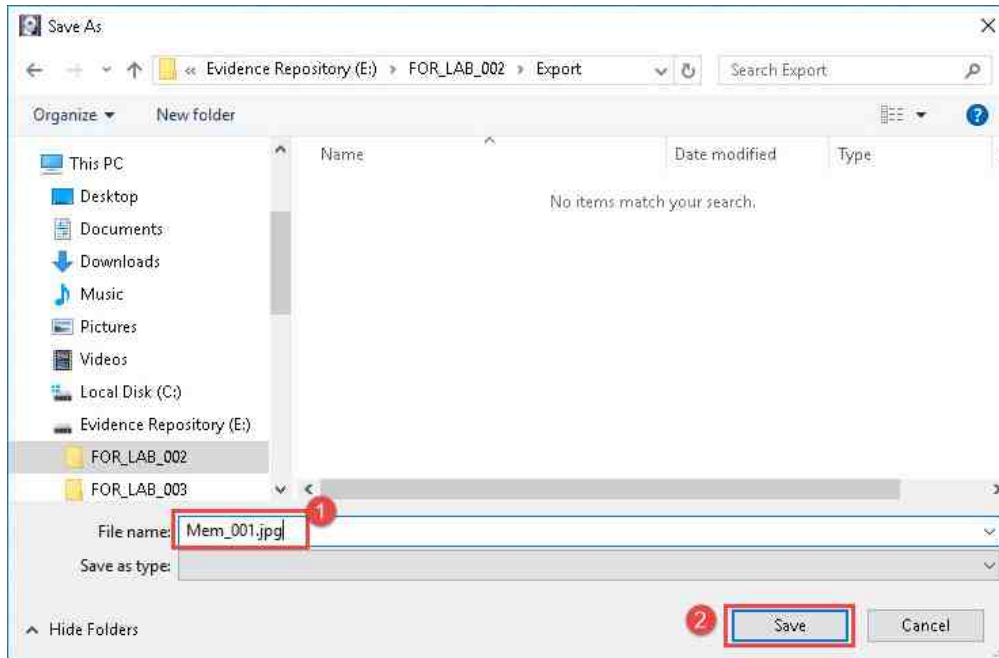
15. Now that your trial and error is complete and you finally got it selected correctly, let us export it and see what it is. To begin exporting/carving this file out, right-click in the view pane once again and click the option, Save selection as seen below.



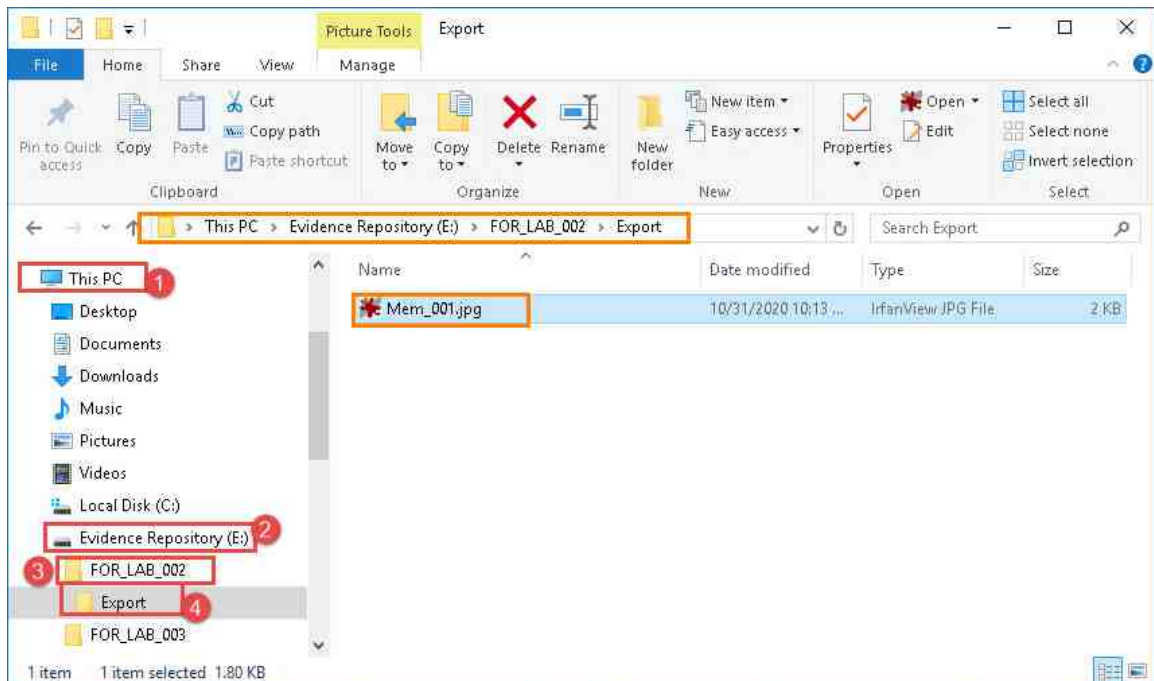
16. The Save As window will appear. Navigate to This PC > Evidence Repository (E:) > FOR_LAB_002 as seen in items 1 – 3. Create a new folder by clicking the New folder button highlighted at item 4 below. Name the folder Export and click Open as seen in items 5 and 6.



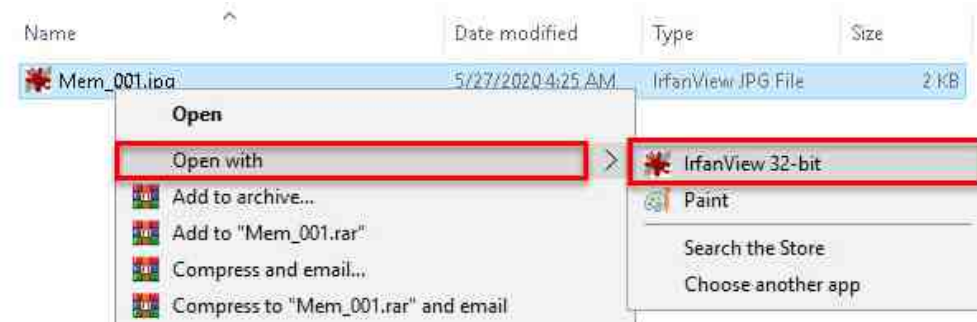
17. Now that you are in your newly created carved file folder, let us give the file a name. This can be done by typing in the File name field highlighted below. Name the file Mem_001.jpg and click Save.



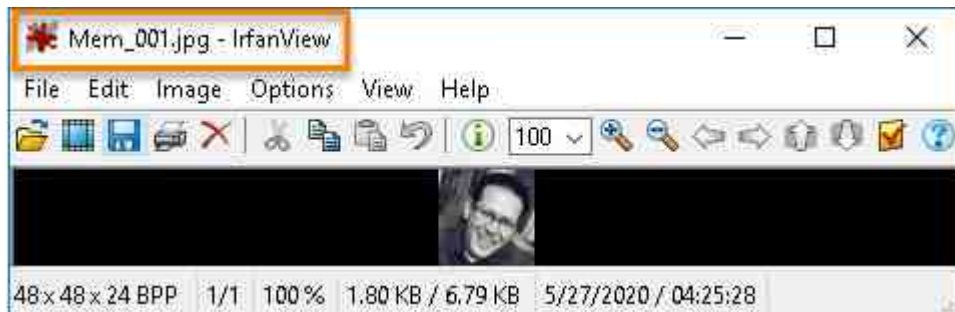
18. Your JPG file is now exported, and we can go see what it is. To do this, browse to the carved file folder by opening file explorer and navigating to This PC > Evidence Repository > FOR_LAB_002 > RAM_Capture_Review > Export as seen below.



19. You should see the file you carved and named Mem_001.jpg. Right-click on the file to bring up the context menu and navigate to the Open with option, which will reveal a submenu. From the sub-menu, select IrfanView 32-bit to open and view the Jpeg picture.



20. You should see the picture below. If you do not, then you may need to attempt the carve once again by repeating steps 8 - 17.



There are tools available that can search and automatically carve files from a RAM dump. These tools would be the ideal way to recover the files, but as a forensic examiner you should know how to manually carve files. This will be further explored in an upcoming lab.

21. We know it was not easy, but you just carved your first file from a windows memory dump. That is not a simple task.
22. You can move on to the next exercise, but before continuing, close FTK Imager and any other open windows by clicking the X at the top-right corner of the windows.

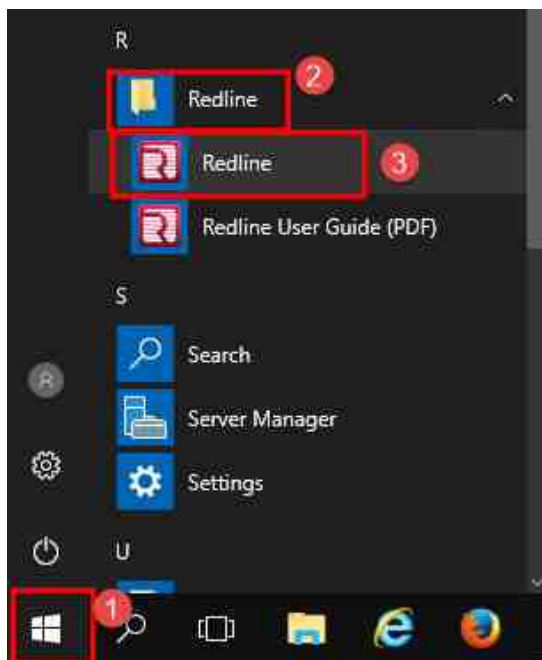
6 Getting Familiar with REDLINE

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.

1. Open REDLINE by Navigating to Start > REDLINE and click the program titled REDLINE highlighted below.



2. The Redline main window will appear, as seen below.

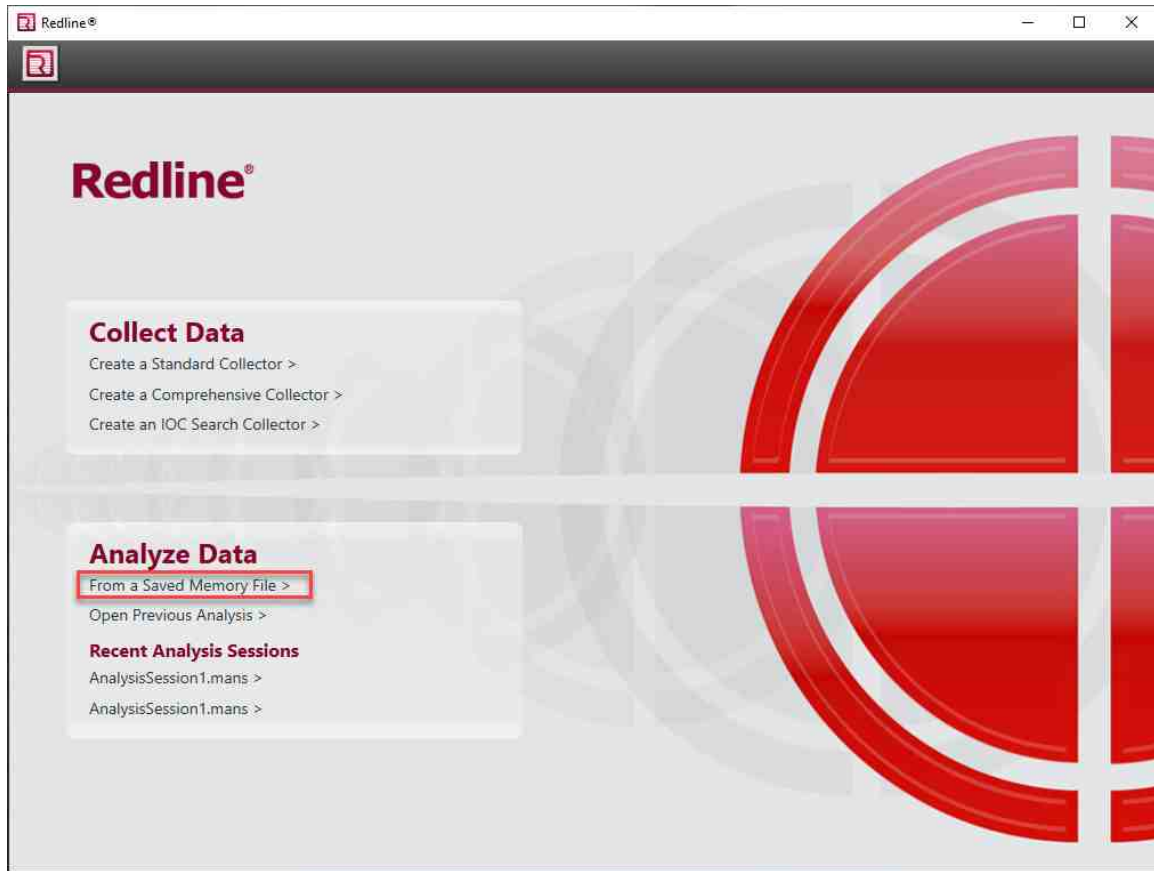


Collect Data	This option allows Redline to create a collection script that can be run on a target host to capture important volatile data that can aid in compromise investigations, as well as, many other types of analysis.
Analyze Data	This is the option we will be using and has 2 main options. Analyze data – From a Saved Memory File and Open Previous Analysis. We will be using the first option, which allows us to load captured RAM into Redline. The Recent Analysis Sessions option is for reopening a previously loaded case.

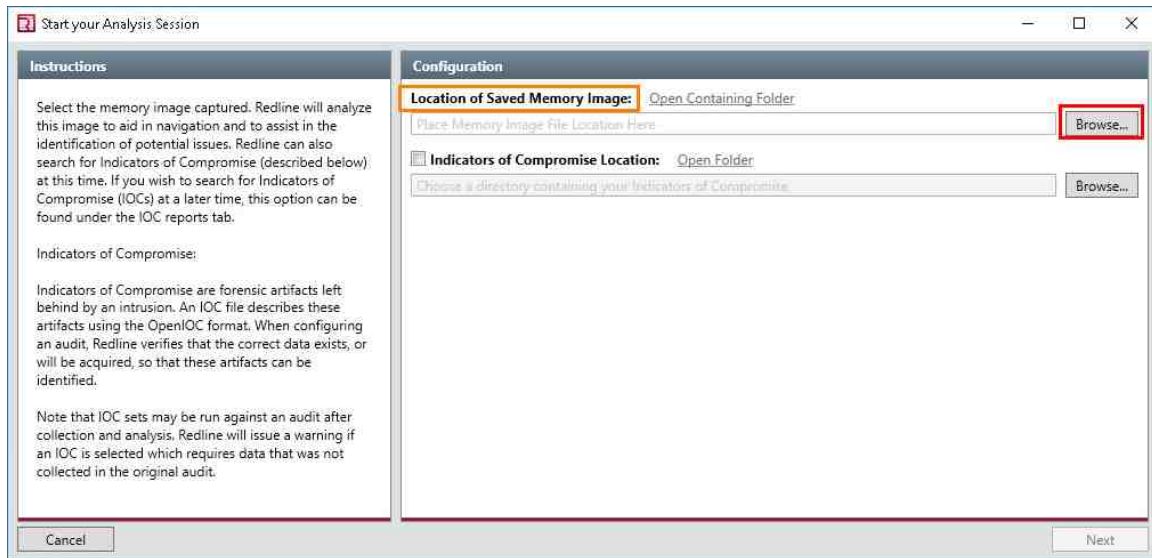
7 Review the RAM Capture Using REDLINE

Now that you are aware of the basics of Redline, let us load some data in it and look around.

1. You should already have Redline running, but if you do not, reopen it and click From a Saved Memory File under Analyze Data as seen below.

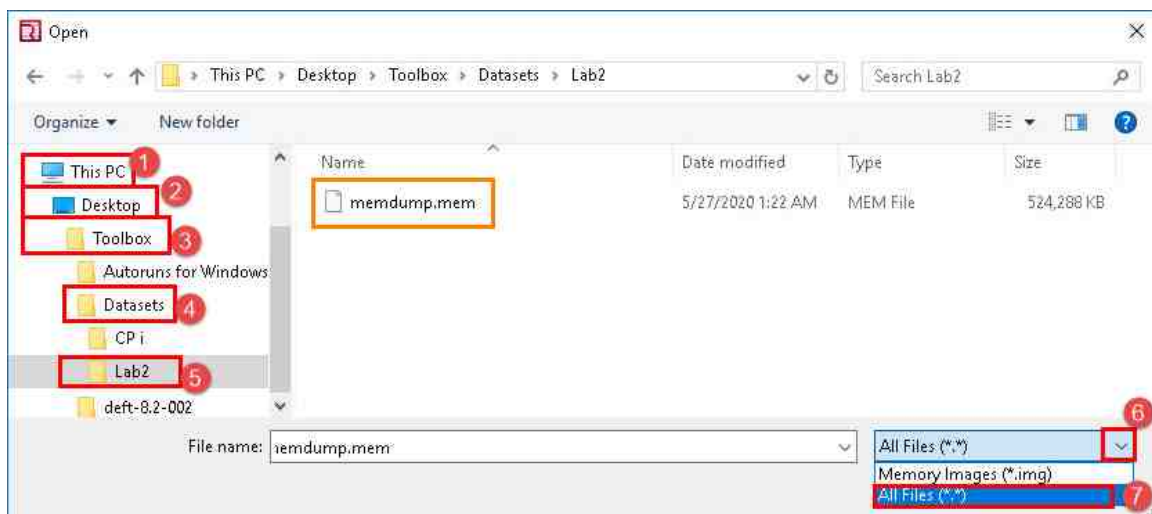


- You should now see the Start your Analysis Session window appear. Click the Browse button under Location of Saved Memory Image subheading as seen below.

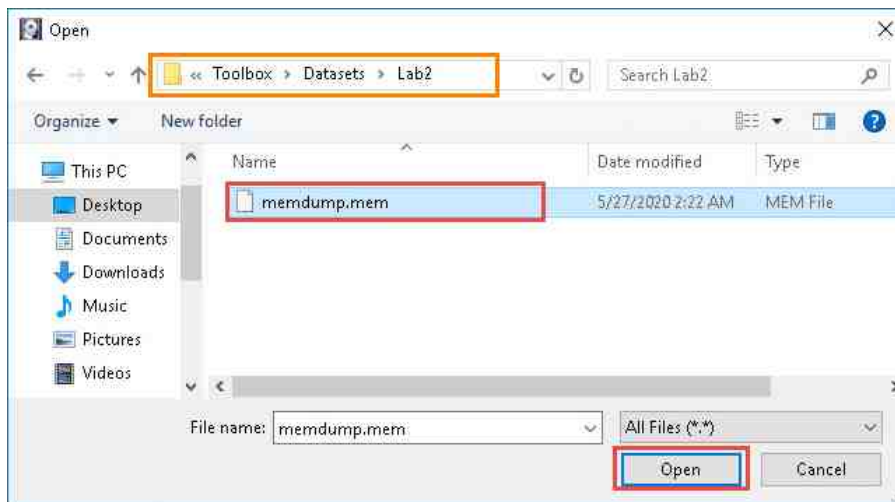


The Indicators of Compromise Location is a feature offered by Redline to automatically search for specific artifacts left behind by an intrusion.

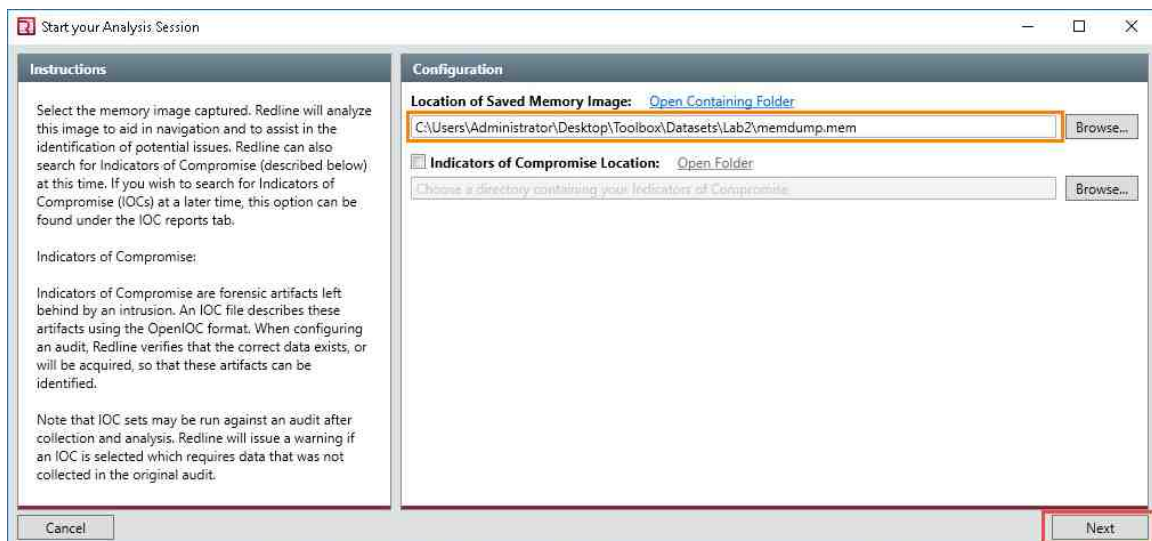
- When you see the Open window appear, navigate to the folders This PC > Desktop > Toolbox > Datasets > Lab2. Once you are in this folder, change the file type to All Files by clicking the dropdown menu in the bottom-right corner of the window. This will allow you to add file memdump.mem and not only ones that have an .img extension.



- You should now see the file called memdump.mem appear in the window. Select it and then click the Open button highlighted below.

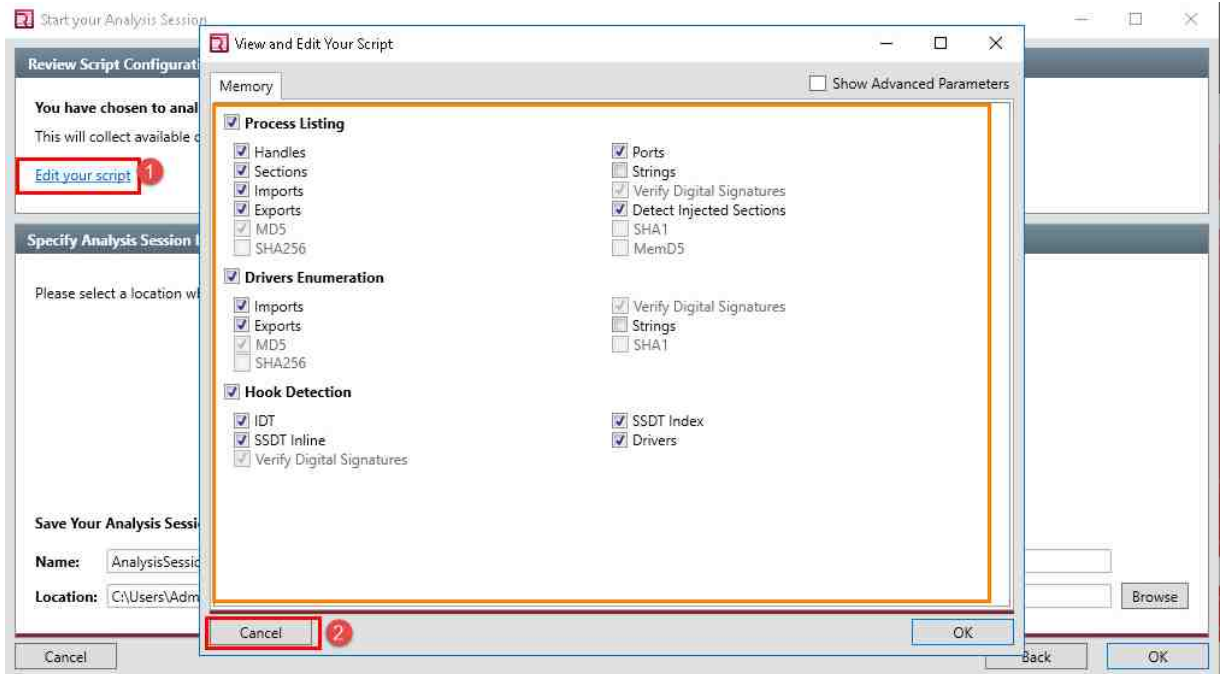


- You should now be back at the Start your analysis session window. Click Next as highlighted below. This will take you to another window, which will allow you to choose what type of artifacts you want to extract from the memory image.

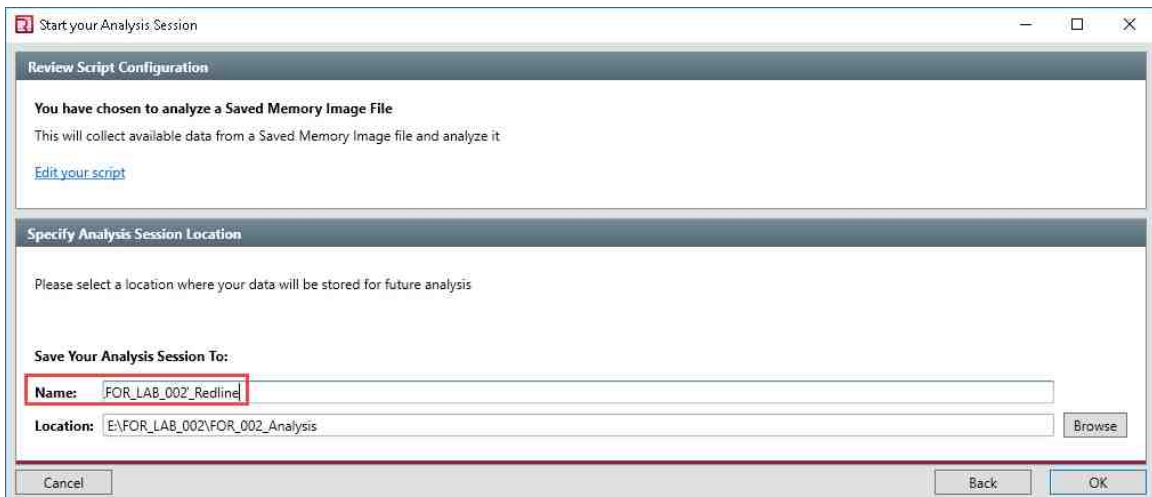


We will not be using an indicator of compromise in this exercise so leave that box unchecked.

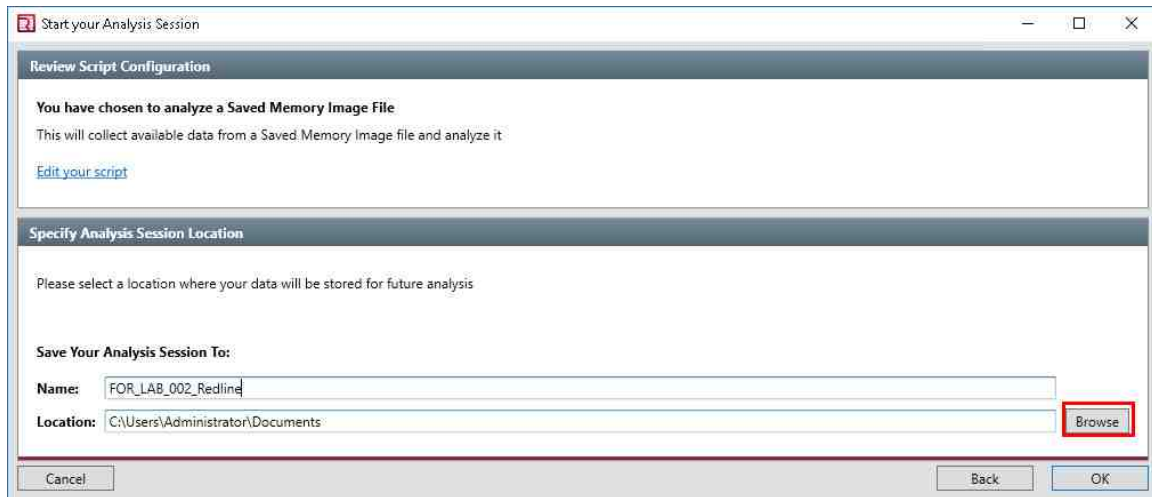
- At this window, you can click on the Edit your script option to see the different artifacts that will be parsed. We will be leaving all the options in their default state, but it is important to know where to find them in case you need to modify them when using it later.



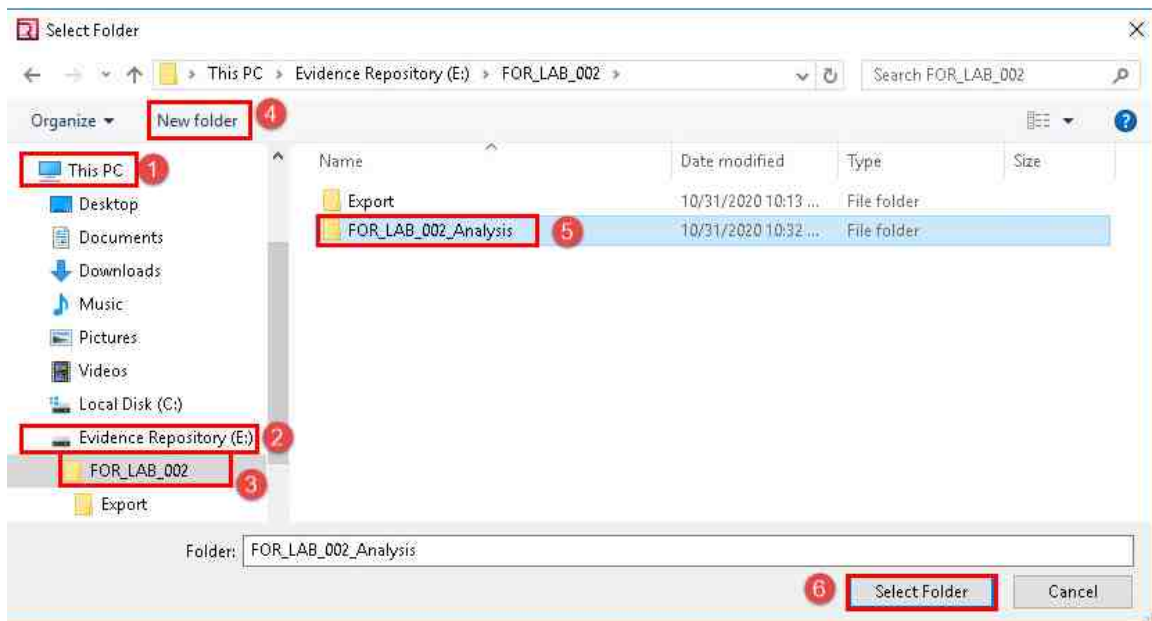
- Now that you are all set to begin the RAM parsing process, give your analysis the name FOR_Lab_002_Redline as highlighted below.



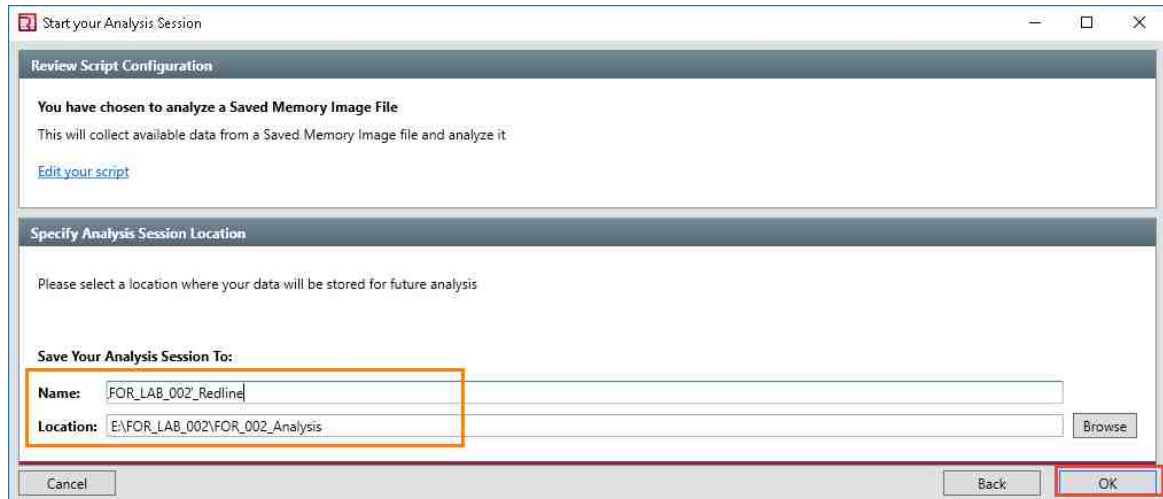
8. Next, let us select a storage location for the Redline case file. Click Browse as highlighted below to open the Select Folder window:



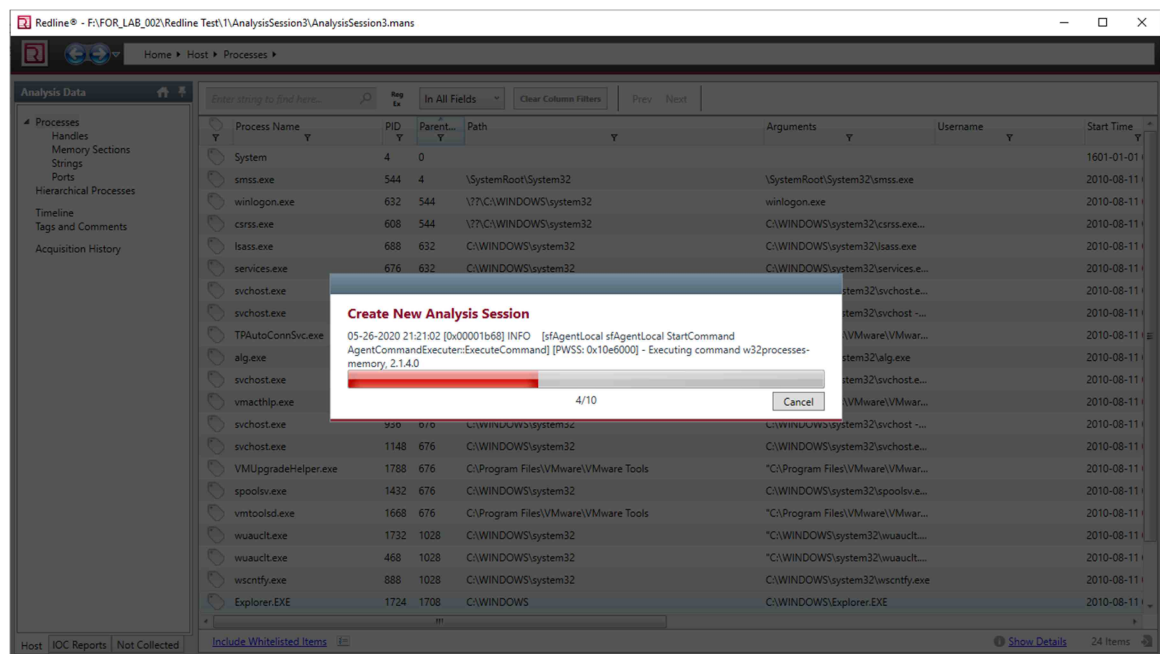
9. In the Select Folder window, browse to the folder This PC > Evidence Repository > FOR_LAB_002 and create a new folder by clicking the New Folder button highlighted below as items 1 - 4. Once the new folder is created, name the folder FOR_LAB_002_Analysis highlighted below as item 5. Once you have successfully created and named the folder, click the select folder button highlighted below as item 6.



10. Now you should be back at the Start your analysis session window with all the correct information entered. Before proceeding, ensure that the information in the Name and Location fields are the same as the ones highlighted below. If all is well, then click the OK button highlighted in the bottom-right corner below and grab a coffee; this might take a while.

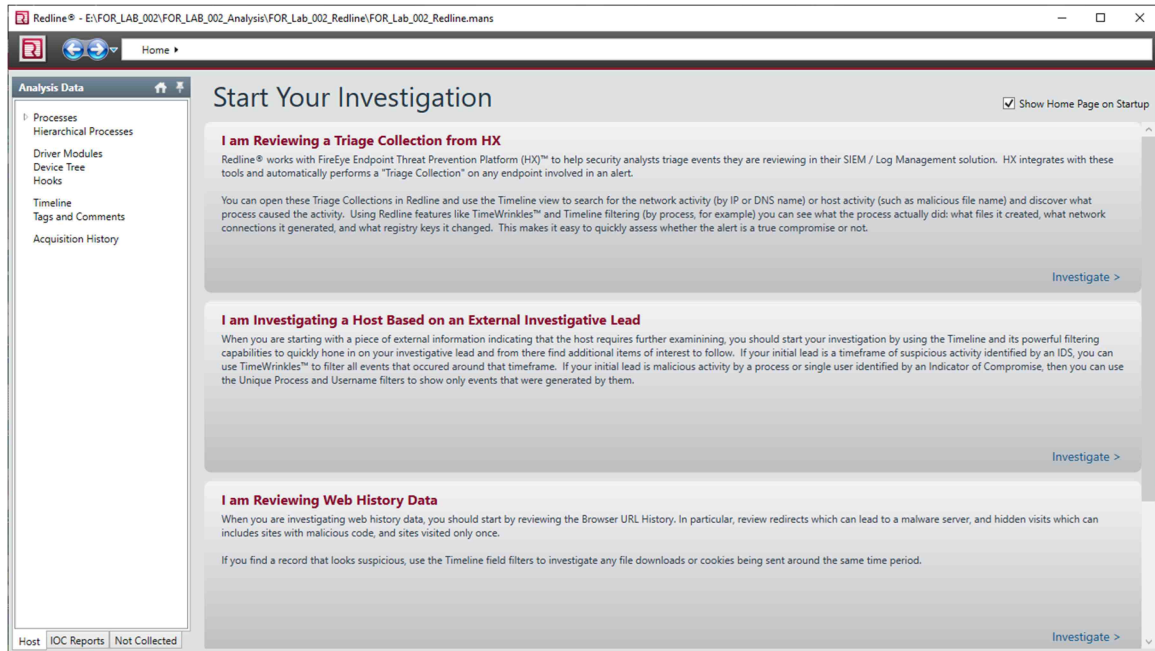


11. Yup, still going. The progress bar below should be filled before you can view any data.



Be sure to look out for the UAC pop-up from Windows asking for permission to run the Redline services. Click Yes if you see the pop-up.
















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.















13. On the left side of the window, you will see a navigation pane called Analysis Data. This pane contains the categories of parsed RAM artifacts. Let us start by looking at the carved processes by clicking the Processes option highlighted below.






14. You should now see the list of processes that were running on the Windows computer that this image was taken from. This list contains the process names, paths, Security Identifiers for users, process IDs, and Parent Process IDs, along with other useful information. Click on a random process to allow the show details button to appear.

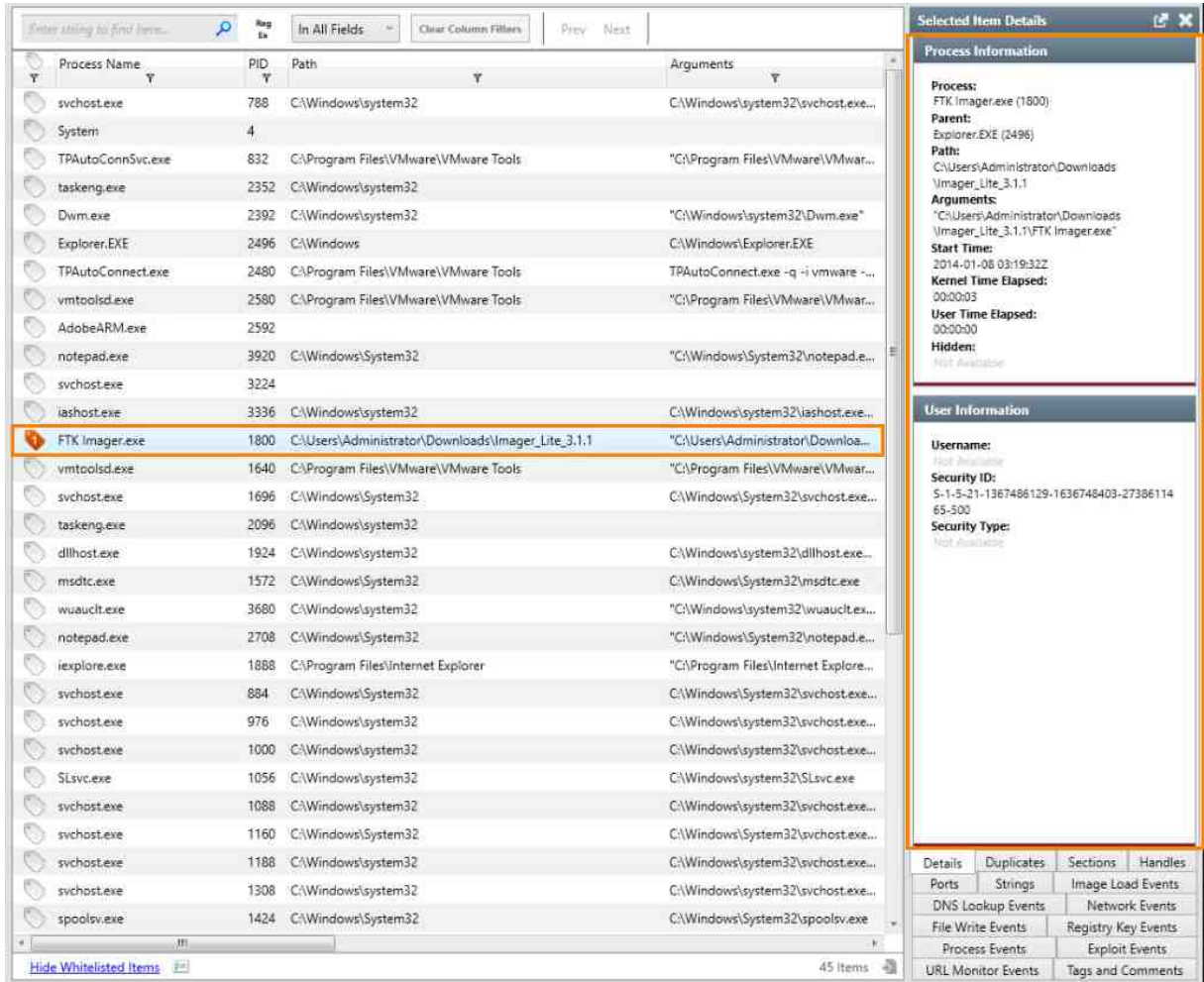
	Process Name	PID	Path	Arguments
	taskeng.exe	2096	C:\Windows\system32	
	dllhost.exe	1924	C:\Windows\system32	C:\Windows\system32\dllhost.exe...
	msdtc.exe	1572	C:\Windows\System32	C:\Windows\System32\msdtc.exe
	wuauclt.exe	3680	C:\Windows\system32	"C:\Windows\system32\wuauclt.ex...
	notepad.exe	2708	C:\Windows\System32	"C:\Windows\System32\notepad.e...
	ieexplore.exe	1888	C:\Program Files\Internet Explorer	"C:\Program Files\Internet Explore...
	svchost.exe	884	C:\Windows\System32	C:\Windows\System32\svchost.exe...
	svchost.exe	976	C:\Windows\system32	C:\Windows\system32\svchost.exe...
	svchost.exe	1000	C:\Windows\system32	C:\Windows\system32\svchost.exe...
	SLsvc.exe	1056	C:\Windows\system32	C:\Windows\system32\SLsvc.exe
	svchost.exe	1088	C:\Windows\system32	C:\Windows\system32\svchost.exe...
	svchost.exe	1160	C:\Windows\System32	C:\Windows\System32\svchost.exe...
	svchost.exe	1188	C:\Windows\system32	C:\Windows\system32\svchost.exe...
	svchost.exe	1308	C:\Windows\system32	C:\Windows\system32\svchost.exe...
	spoolsv.exe	1424	C:\Windows\System32	C:\Windows\System32\spoolsv.exe

15. To get more details of each process, click the Show Details option at the bottom-right corner of the window. This will open a pane on the right side of the window that provides details of any process that you select.

	TPAutoConnSvc.exe	1968	676	C:\Program Files\VMware\VMware Tools	"C:\Program Files\VMware\VMwar...	2010-08-11 06:0
	TPAutoConnect.exe	1084	1968	C:\Program Files\VMware\VMware Tools	TPAutoConnect.exe -q -i vmware ~...	2010-08-11 06:0
	Explorer.EXE	1724	1708	C:\WINDOWS	C:\WINDOWS\Explorer.EXE	2010-08-11 06:0
	VMwareUser.exe	452	1724	C:\Program Files\VMware\VMware Tools	"C:\Program Files\VMware\VMwar...	2010-08-11 06:0
	VMwareTray.exe	432	1724	C:\Program Files\VMware\VMware Tools	"C:\Program Files\VMware\VMwar...	2010-08-11 06:0
	wscntfy.exe	888	1028	C:\WINDOWS\system32	C:\WINDOWS\system32\wscntfy.exe	2010-08-11 06:0
	smss.exe	544	4	\SystemRoot\System32	\SystemRoot\System32\smss.exe	2010-08-11 06:0
	alg.exe	216	676	C:\WINDOWS\System32	C:\WINDOWS\System32\alg.exe	2010-08-11 06:0
	lsass.exe	688	632	C:\WINDOWS\system32	C:\WINDOWS\system32\lsass.exe	2010-08-11 06:0
	services.exe	676	632	C:\WINDOWS\system32	C:\WINDOWS\system32\services.e...	2010-08-11 06:0
	svchost.exe	1088	676	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.e...	2010-08-11 06:0
	vmacthlp.exe	844	676	C:\Program Files\VMware\VMware Tools	"C:\Program Files\VMware\VMwar...	2010-08-11 06:0
	svchost.exe	936	676	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost ~...	2010-08-11 06:0
	svchost.exe	1148	676	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.e...	2010-08-11 06:0
	VMUpgradeHelper.exe	1788	676	C:\Program Files\VMware\VMware Tools	"C:\Program Files\VMware\VMwar...	2010-08-11 06:0

Hide Whitelisted Items   Show Details 24 Items 

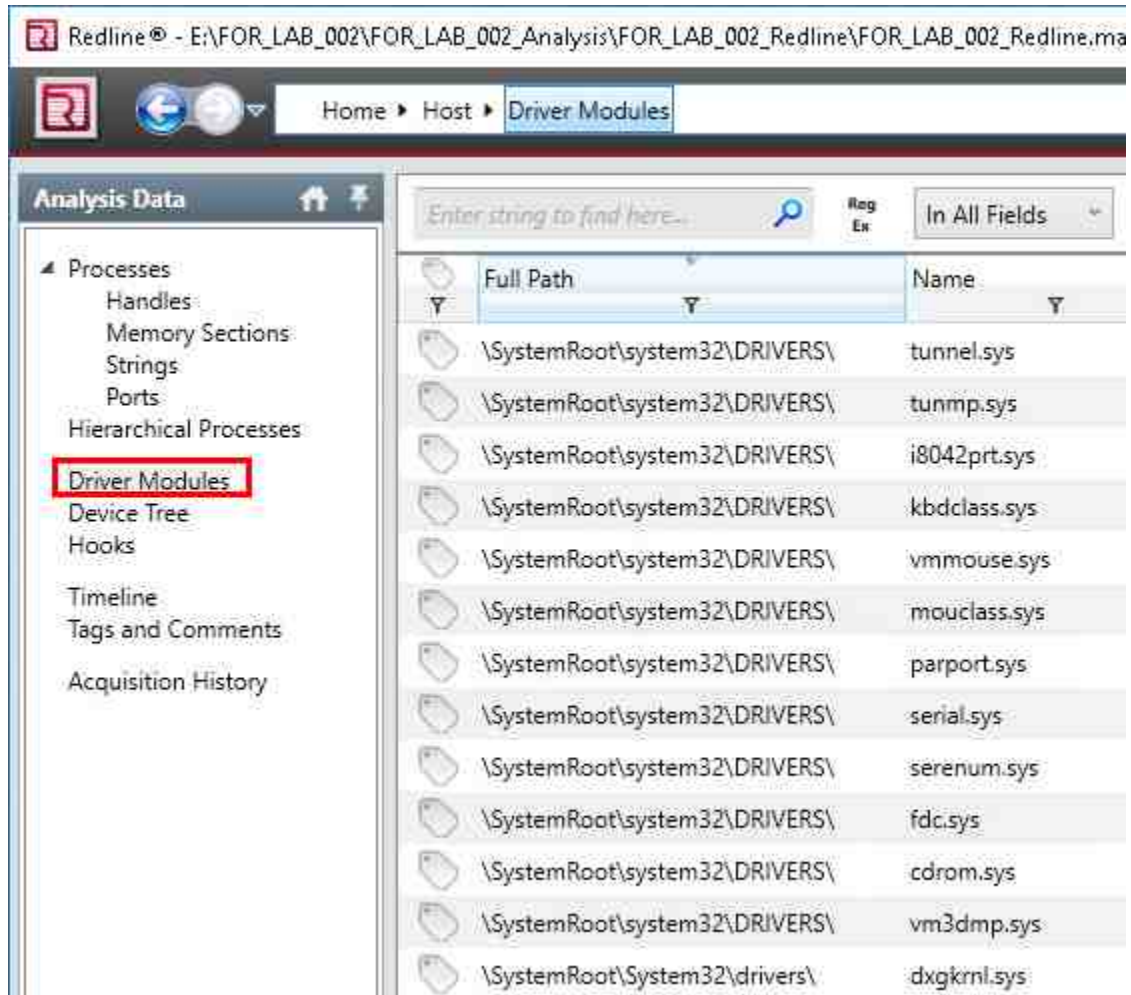
16. The Details pane can be seen on the right, as highlighted below.



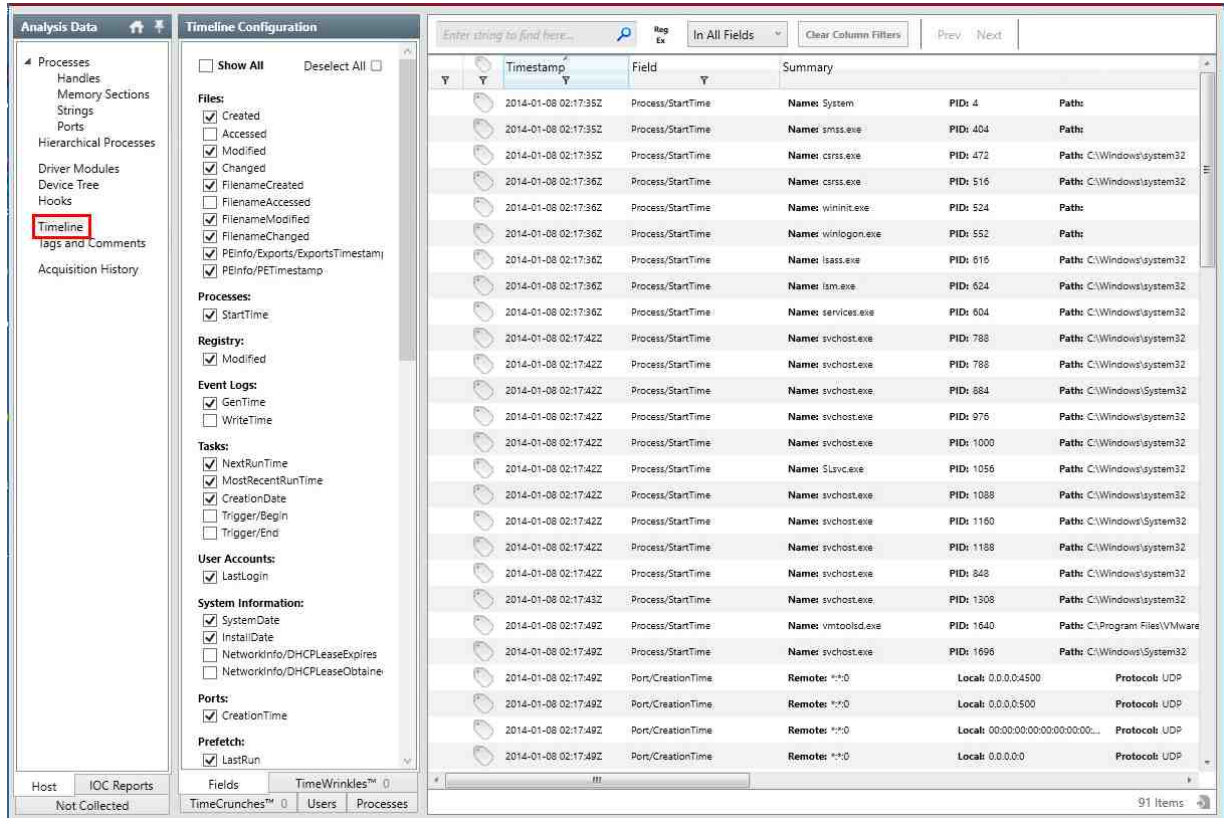
Process Name	PID	Path	Arguments
svchost.exe	788	C:\Windows\system32	C:\Windows\system32\svchost.exe...
System	4		
TPAutoConnSvc.exe	832	C:\Program Files\VMware\VMware Tools	"C:\Program Files\VMware\VMwar...
taskeng.exe	2352	C:\Windows\system32	
Dwm.exe	2392	C:\Windows\system32	"C:\Windows\system32\Dwm.exe"
Explorer.EXE	2496	C:\Windows	C:\Windows\Explorer.EXE
TPAutoConnect.exe	2480	C:\Program Files\VMware\VMware Tools	TPAutoConnect.exe -q -i vmware ~...
vmtoolsd.exe	2580	C:\Program Files\VMware\VMware Tools	"C:\Program Files\VMware\VMwar...
AdobeARM.exe	2592		
notepad.exe	3920	C:\Windows\System32	"C:\Windows\System32\notepad.e...
svchost.exe	3224		
lsass.exe	3336	C:\Windows\system32	C:\Windows\system32\lsass.exe...
FTK Imager.exe	1800	C:\Users\Administrator\Downloads\Imager_Lite_3.1.1	"C:\Users\Administrator\Downloa...
vmtoolsd.exe	1640	C:\Program Files\VMware\VMware Tools	"C:\Program Files\VMware\VMwar...
svchost.exe	1696	C:\Windows\System32	C:\Windows\System32\svchost.exe...
taskeng.exe	2096	C:\Windows\system32	
dllhost.exe	1924	C:\Windows\system32	C:\Windows\system32\dllhost.exe...
msdtc.exe	1572	C:\Windows\System32	C:\Windows\System32\msdtc.exe
wuauclt.exe	3680	C:\Windows\system32	"C:\Windows\system32\wuauclt.e...
notepad.exe	2708	C:\Windows\System32	"C:\Windows\System32\notepad.e...
iexplore.exe	1888	C:\Program Files\Internet Explorer	"C:\Program Files\Internet Explore...
svchost.exe	884	C:\Windows\System32	C:\Windows\System32\svchost.exe...
svchost.exe	976	C:\Windows\system32	C:\Windows\system32\svchost.exe...
svchost.exe	1000	C:\Windows\system32	C:\Windows\system32\svchost.exe...
SLsvc.exe	1056	C:\Windows\system32	C:\Windows\system32\SLsvc.exe
svchost.exe	1088	C:\Windows\system32	C:\Windows\system32\svchost.exe...
svchost.exe	1160	C:\Windows\System32	C:\Windows\System32\svchost.exe...
svchost.exe	1188	C:\Windows\system32	C:\Windows\system32\svchost.exe...
svchost.exe	1308	C:\Windows\system32	C:\Windows\system32\svchost.exe...
spoolsv.exe	1424	C:\Windows\System32	C:\Windows\System32\spoolsv.exe

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-1-5-21-1367486129-1636748403-27356114																											
Security Type: Not Available																											
<table border="1"> <thead> <tr> <th>Details</th> <th>Duplicates</th> <th>Sections</th> <th>Handles</th> </tr> </thead> <tbody> <tr> <td>Ports</td> <td>Strings</td> <td>Image Load Events</td> <td></td> </tr> <tr> <td>DNS Lookup Events</td> <td></td> <td>Network Events</td> <td></td> </tr> <tr> <td>File Write Events</td> <td></td> <td>Registry Key Events</td> <td></td> </tr> <tr> <td>Process Events</td> <td></td> <td>Exploit Events</td> <td></td> </tr> <tr> <td>URL Monitor Events</td> <td></td> <td>Tags and Comments</td> <td></td> </tr> </tbody> </table>				Details	Duplicates	Sections	Handles	Ports	Strings	Image Load Events		DNS Lookup Events		Network Events		File Write Events		Registry Key Events		Process Events		Exploit Events		URL Monitor Events		Tags and Comments	
Details	Duplicates	Sections	Handles																								
Ports	Strings	Image Load Events																									
DNS Lookup Events		Network Events																									
File Write Events		Registry Key Events																									
Process Events		Exploit Events																									
URL Monitor Events		Tags and Comments																									

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.



18. Another very useful feature of Redline is the Timeline feature. This option provides a chronologically sorted table of processes. To access the timeline, click the Timeline option in the Analysis Data pane as highlighted below.



The screenshot shows the Redline software interface. On the left, the 'Analysis Data' pane has a tree view with 'Timeline' highlighted. The 'Timeline Configuration' pane on the right shows various filters for Files, Processes, Registry, Event Logs, Tasks, User Accounts, System Information, Ports, and Prefetch. The main window displays a table of process events with columns for Timestamp, Field, and Summary.

Timestamp	Field	Summary
2014-01-08 02:17:35Z	Process/StartTime	Name: System PID: 4 Path:
2014-01-08 02:17:35Z	Process/StartTime	Name: smss.exe PID: 404 Path:
2014-01-08 02:17:35Z	Process/StartTime	Name: csrss.exe PID: 472 Path: C:\Windows\system32
2014-01-08 02:17:36Z	Process/StartTime	Name: csrss.exe PID: 516 Path: C:\Windows\system32
2014-01-08 02:17:36Z	Process/StartTime	Name: wininit.exe PID: 524 Path:
2014-01-08 02:17:36Z	Process/StartTime	Name: winlogon.exe PID: 552 Path:
2014-01-08 02:17:36Z	Process/StartTime	Name: lsass.exe PID: 616 Path: C:\Windows\system32
2014-01-08 02:17:36Z	Process/StartTime	Name: lsass.exe PID: 624 Path: C:\Windows\system32
2014-01-08 02:17:36Z	Process/StartTime	Name: services.exe PID: 604 Path: C:\Windows\system32
2014-01-08 02:17:42Z	Process/StartTime	Name: svchost.exe PID: 788 Path: C:\Windows\system32
2014-01-08 02:17:42Z	Process/StartTime	Name: svchost.exe PID: 788 Path: C:\Windows\system32
2014-01-08 02:17:42Z	Process/StartTime	Name: svchost.exe PID: 884 Path: C:\Windows\System32
2014-01-08 02:17:42Z	Process/StartTime	Name: svchost.exe PID: 976 Path: C:\Windows\system32
2014-01-08 02:17:42Z	Process/StartTime	Name: svchost.exe PID: 1000 Path: C:\Windows\system32
2014-01-08 02:17:42Z	Process/StartTime	Name: SLAV.exe PID: 1056 Path: C:\Windows\system32
2014-01-08 02:17:42Z	Process/StartTime	Name: svchost.exe PID: 1088 Path: C:\Windows\system32
2014-01-08 02:17:42Z	Process/StartTime	Name: svchost.exe PID: 1160 Path: C:\Windows\System32
2014-01-08 02:17:42Z	Process/StartTime	Name: svchost.exe PID: 1188 Path: C:\Windows\system32
2014-01-08 02:17:42Z	Process/StartTime	Name: svchost.exe PID: 848 Path: C:\Windows\system32
2014-01-08 02:17:42Z	Process/StartTime	Name: svchost.exe PID: 1308 Path: C:\Windows\system32
2014-01-08 02:17:49Z	Process/StartTime	Name: vmtoolsd.exe PID: 1640 Path: C:\Program Files\VMware
2014-01-08 02:17:49Z	Process/StartTime	Name: svchost.exe PID: 1696 Path: C:\Windows\System32
2014-01-08 02:17:49Z	Port/CreationTime	Remote: **0 Local: 0.0.0.0:4500 Protocol: UDP
2014-01-08 02:17:49Z	Port/CreationTime	Remote: **0 Local: 0.0.0.0:500 Protocol: UDP
2014-01-08 02:17:49Z	Port/CreationTime	Remote: **0 Local: 00:00:00:00:00:00:00:00 Protocol: UDP
2014-01-08 02:17:49Z	Port/CreationTime	Remote: **0 Local: 0.0.0.0 Protocol: UDP

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...	Protocol:
	2014-01-08 02:19:53Z	Port/CreationTime	Remote: **0	Local: 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...	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: pschost.exe	PID: 3224	Path:
	2014-01-08 02:19:53Z	Process/StartTime	Name: lashost.exe	PID: 3336	Path: C:\Windows\sysm
	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\sysm
	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.