

# Workbook

## 1-3



SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | [sans.org](https://sans.org)

**PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.**

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

**BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.**

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

**Governing Law:** This Agreement shall be governed by the laws of the State of Maryland, USA.

# © SANS Institute 2020

## Exercise 0a – SIFT and Windows VM Setup

### Objectives

- Install and prepare your lab workstation for Battlefield Forensics this week.

### Installing the FOR498 Windows and Linux VMs – WINDOWS HOST

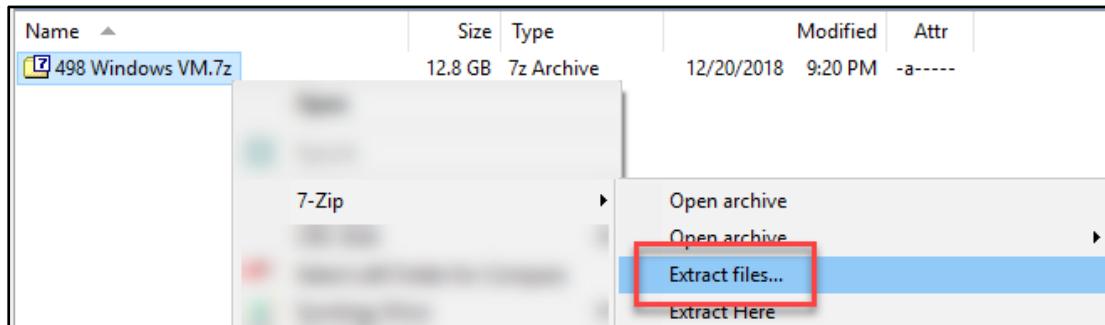
### Exercise Preparation

1. Install VMware Workstation or VMware Player.
  - <https://www.for498.com/workstation>
  - <https://www.for498.com/player>
2. Install 7zip program.
  - Located on your **FOR498 USB A**, under **\Installers\7z-x64.exe**

### Part 1—Unzipping the 498 Windows Virtual Machine

This section is for people using a Windows computer as their host. If you are using an Apple product as your host, please skip ahead to “Exercise 0b – SIFT and Windows VM Setup” that follows this exercise.

1. Insert the **FOR498 USB A** into your host system. You will receive the **FOR498 USB A** by the first day of the course, if you do not have it now. Please wait until you receive the USB keys before configuring your system.
2. On the USB, browse to the **root** directory.
3. Unzip the **FOR498 Windows VM.7z** file to a **Virtual Machines** folder you have created on your host, as shown below:
  - Right-click the file to get the **7-Zip** options and select **Extract files...**



- Select a Folder on your system to "Extract to:" Generally, we recommend a folder where you keep your virtual machines such as C:\Users\<Username>\Documents\Virtual Machines.
- Uncheck the check-box below the "Extract to:" path and click **OK**.

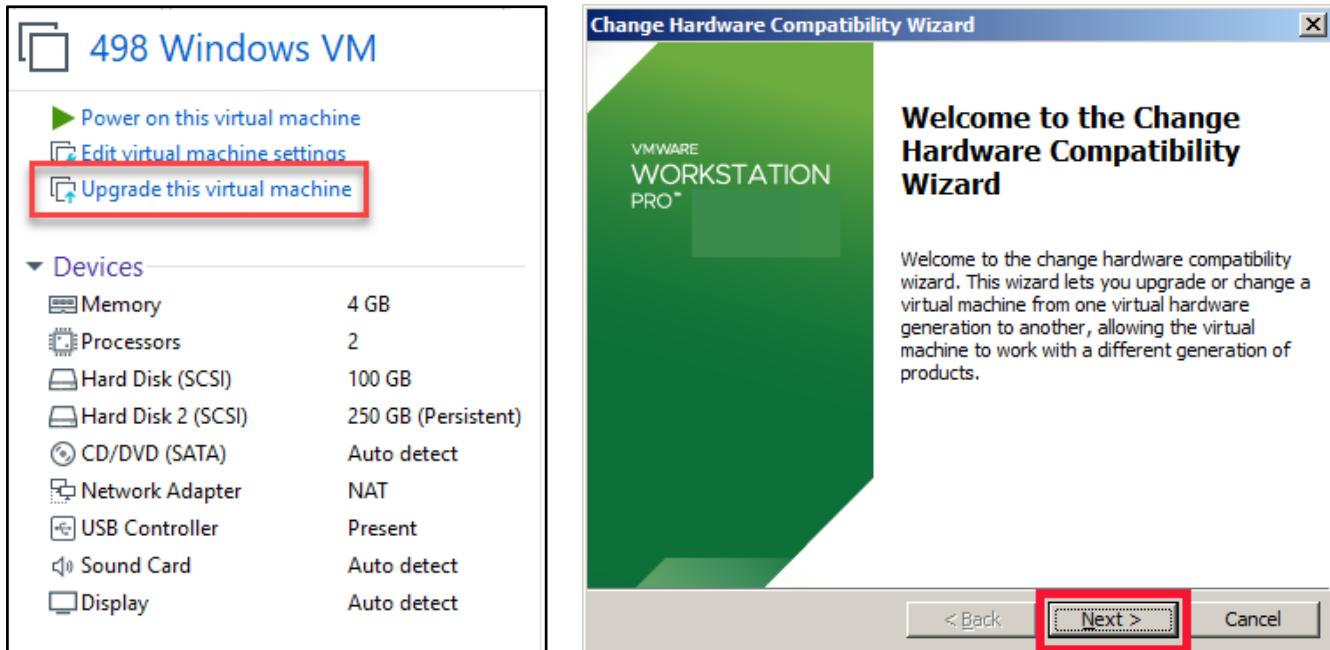


- After a long extraction process (maybe 20–45 min), you should see a new folder in your selected export folder called **FOR498 Windows VM**.

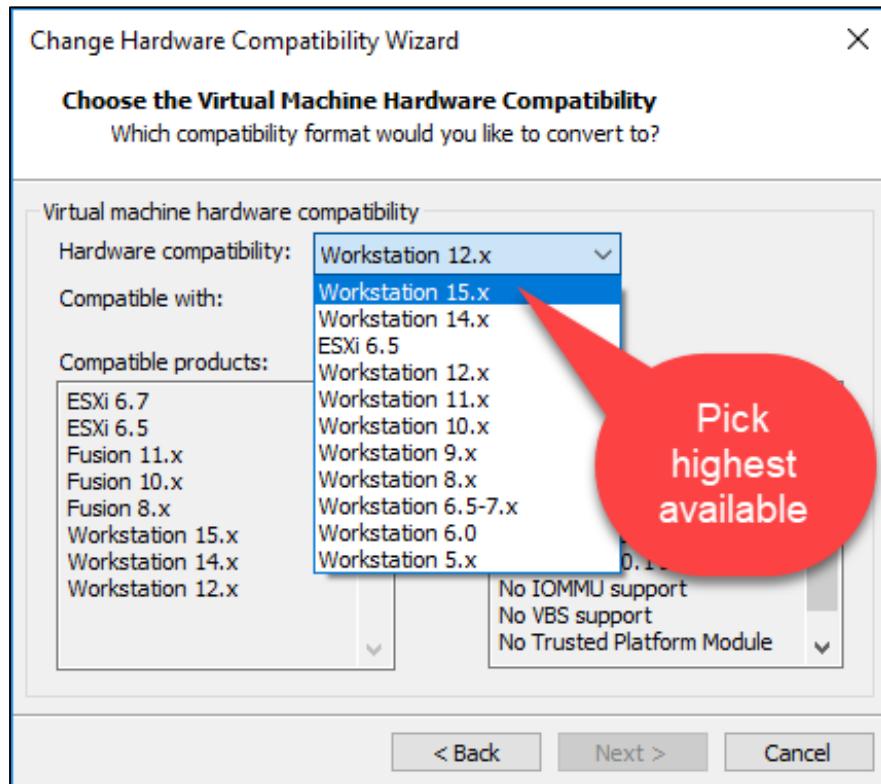
## Part 2—Configuring the 498 Windows Virtual Machine Hardware Settings

1. Start VMware Workstation or Player, and open (**File → Open**, or **Player → File → Open** on VMware Player) the virtual machine file located in the **root** directory called **FOR498 Windows VM.vmx**. This will load the **FOR498 Windows VM** in your VMware application.
2. If you receive an error regarding **Windows Credential Guard**, refer to the document at <http://dfir.to/cg> for instructions on how to disable it.

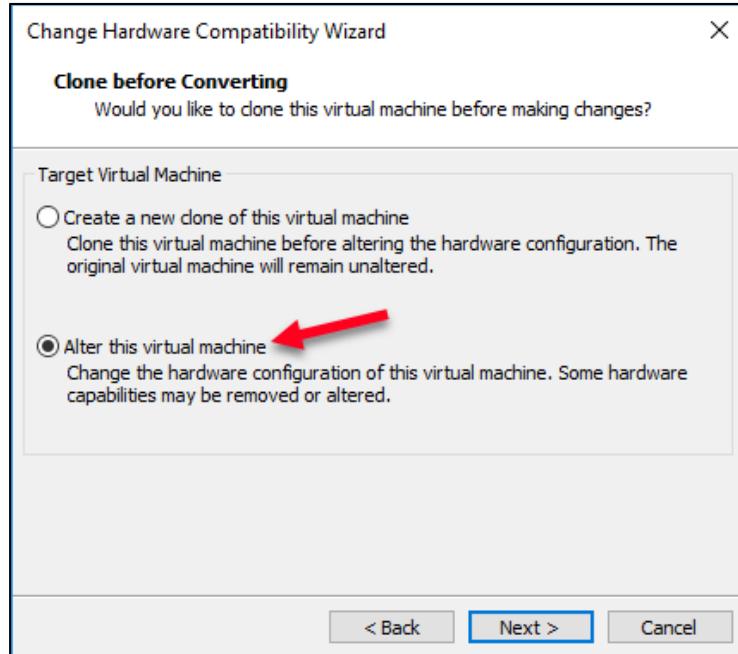
3. Upgrade your virtual machine if you can, by selecting **Upgrade this virtual machine**. VMware Player does not have this feature.



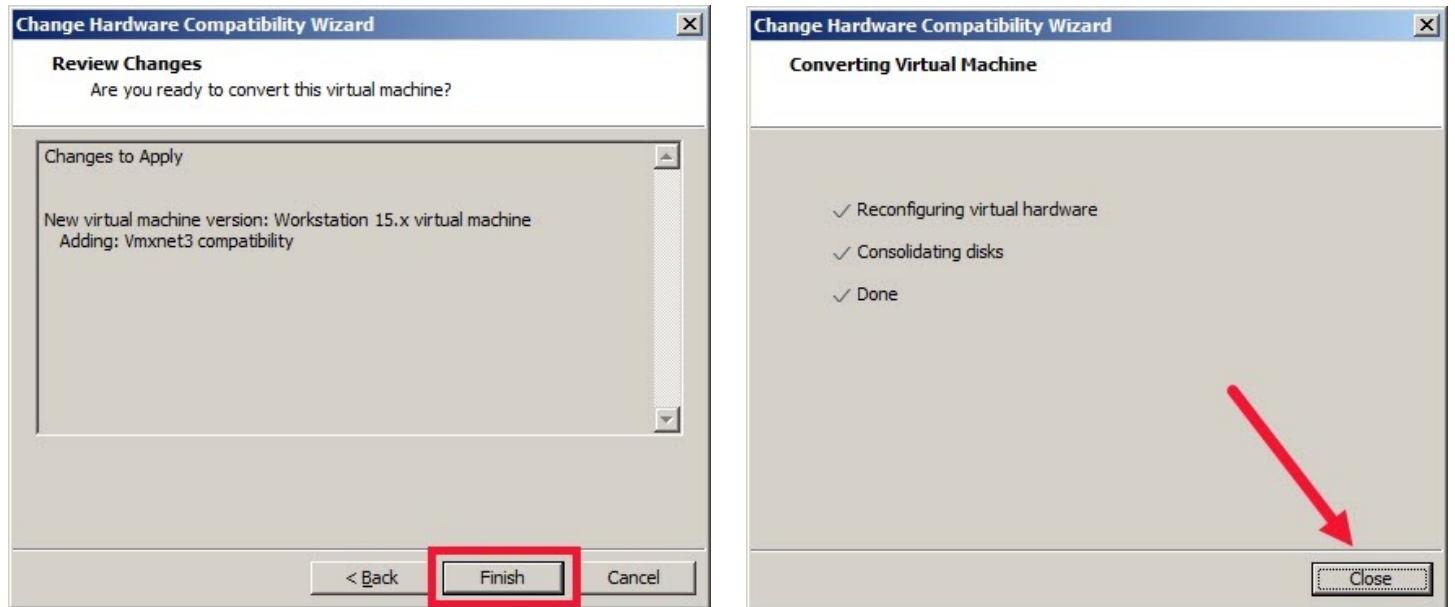
4. Complete the **Change Hardware Compatibility Wizard** that appears and choose the highest available version from the Hardware Compatibility pull-down list and click **Next**.



5. On the next screen, make sure you simply “Alter” the VM and do not create a new clone, which will take some time. Again, click **Next**.

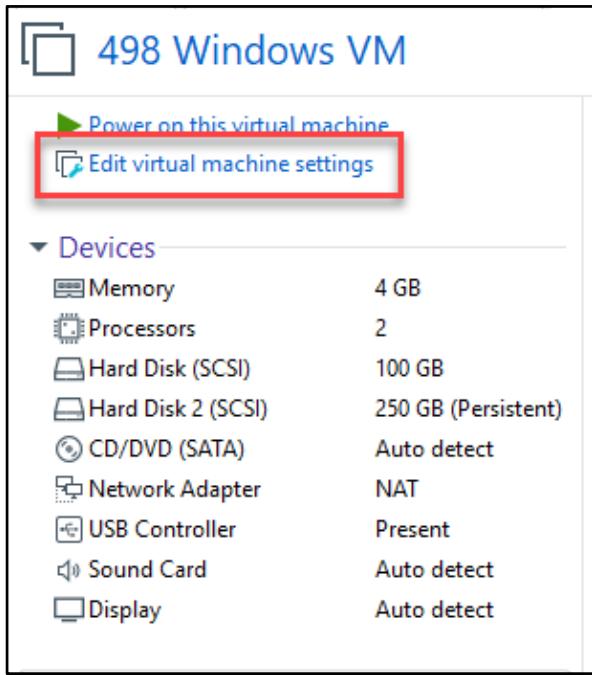


6. The next screen will review the changes you have made. Click **Finish**, and then on the screen that follows, click **Close**.

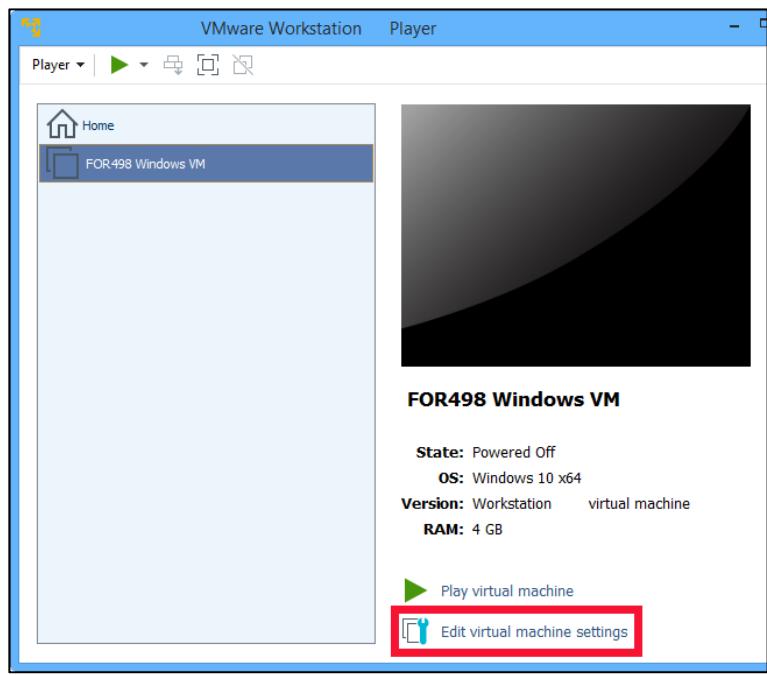


- The **FOR498 Windows VM** requires at least 4 GB of RAM. If your host system has 8 GB of RAM, do not adjust this setting. You should allocate no more than half of your host's RAM to this **VM**. If your host has more than 8 GB RAM, such as 16 or 32 GB, then the **FOR498 Windows VM** can perform better by assigning it more RAM. To do so, adjust the memory by selecting **Edit Virtual Machine Settings** and selecting **Memory**.

➤ Choose **Edit Virtual Machine Settings** as follows:



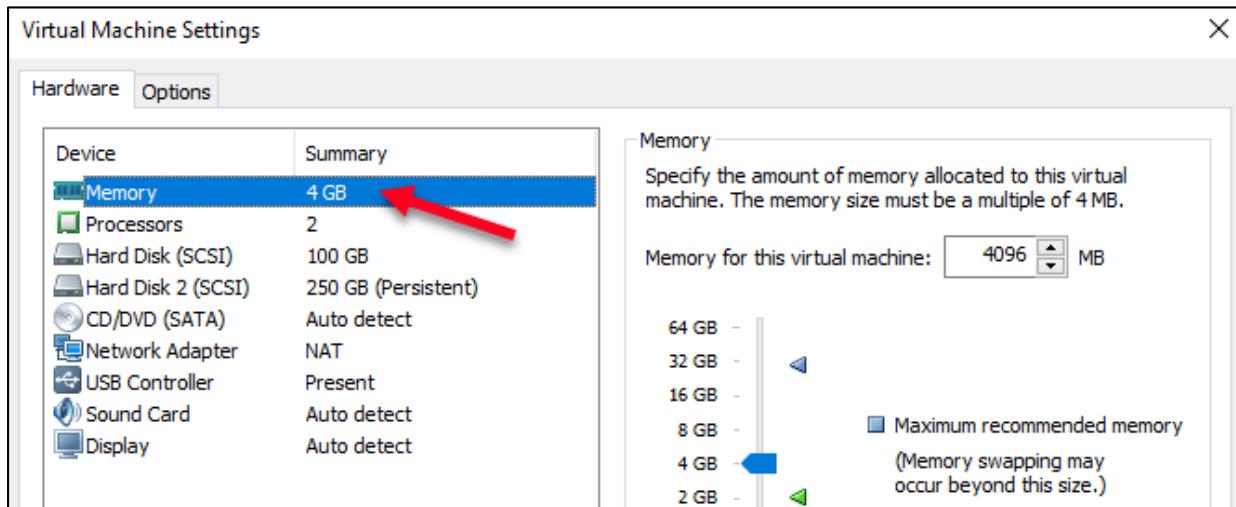
VMware Workstation – Edit VM Settings



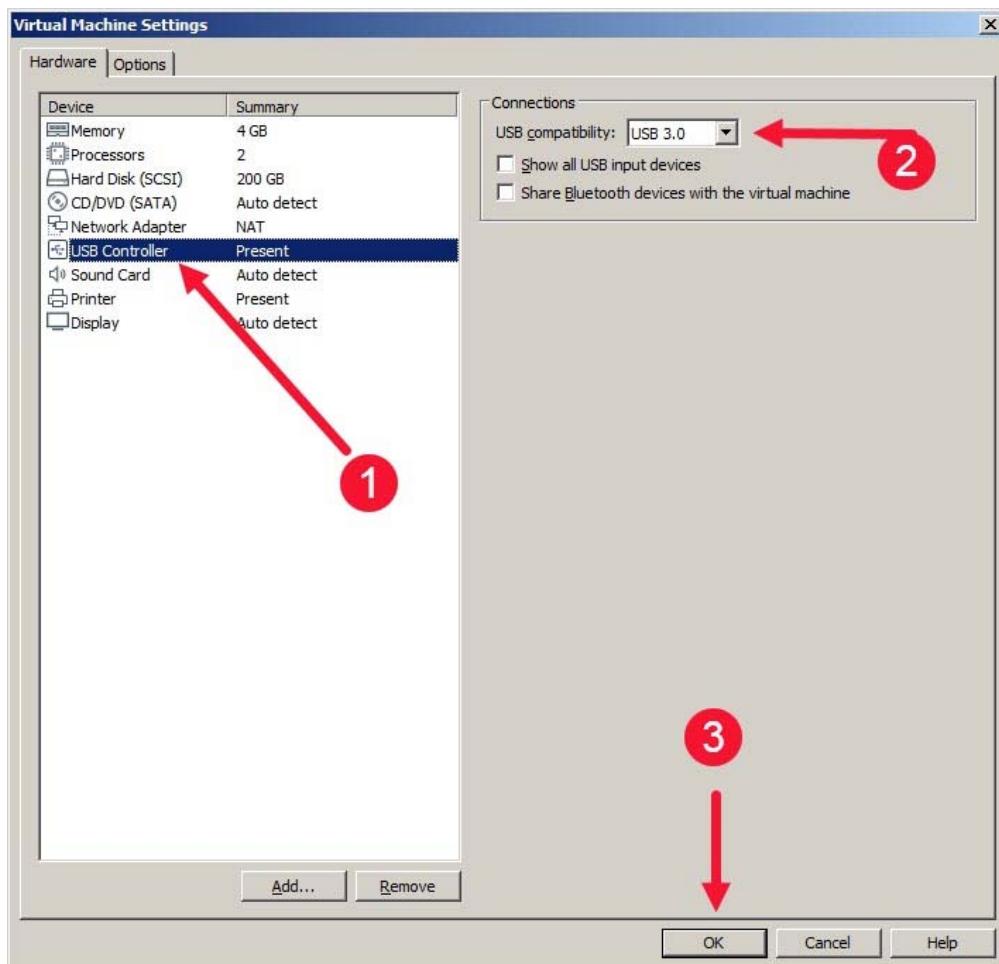
VMware Player – Edit VM Settings

➤ Then make the appropriate adjustments to **Memory**.

- Note: You can also adjust the number of **Processors**. Similar to RAM, it is not recommended to assign more than half the total number of CPU cores available on your host system.

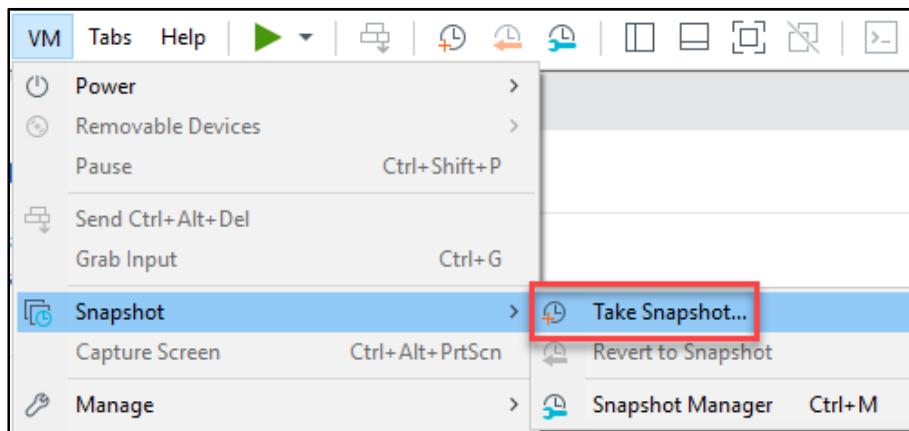


- Check your USB settings (select **USB Controller**). Make sure the USB Compatibility is set for **USB 3.0** (select this even if you don't have USB 3.0 on your system). The reason for this is that **VMware** will still attempt to copy files at a greater speed.

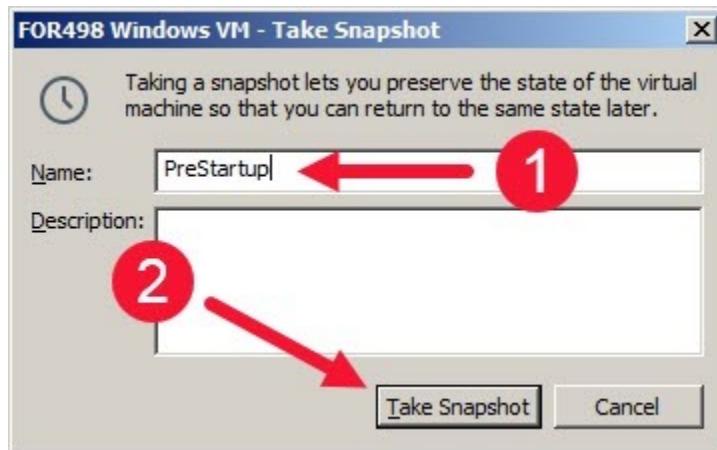


*VMware Workstation/Player – USB Compatibility to USB 3.0*

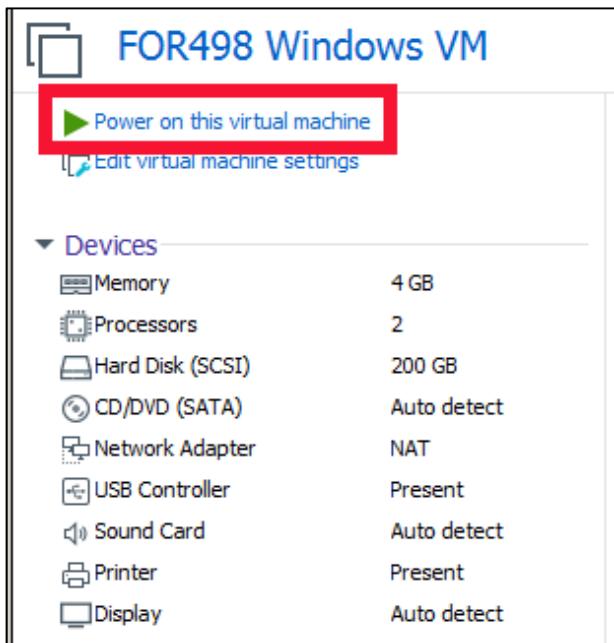
- Take a **Snapshot** of the current state of the virtual machine via the **VM → Snapshot → Take Snapshot** option. If you are using **VMware Player**, you cannot take a **Snapshot**.



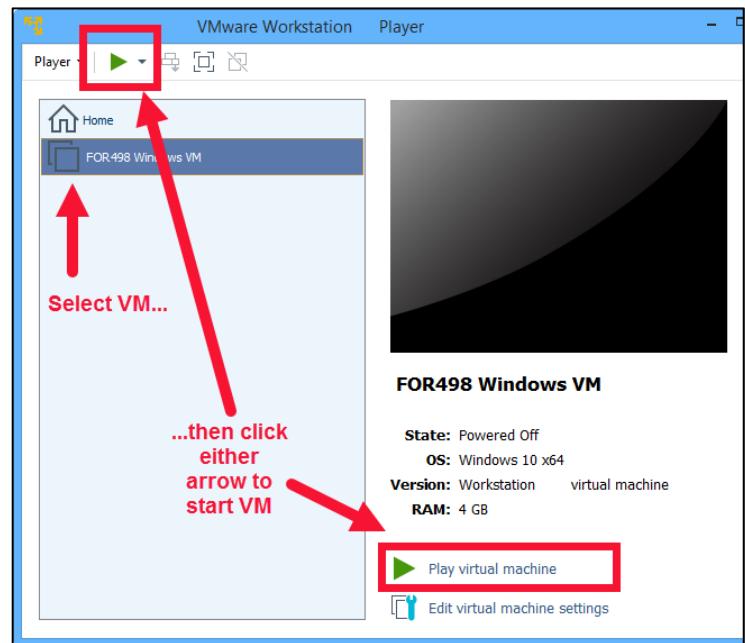
10. Name the Snapshot PreStartup.



11. Power on your virtual machine. If you see any update messages, do NOT accept them.

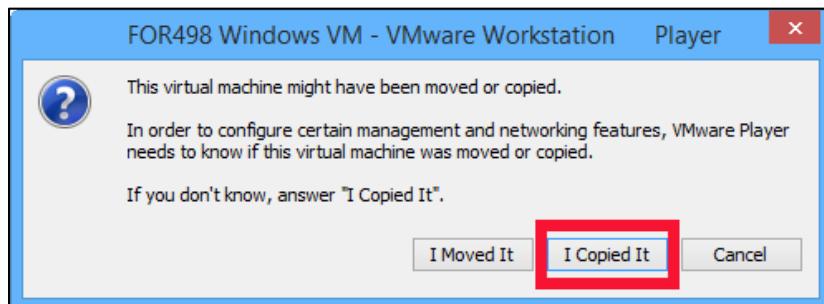


VMware Workstation – Start VM

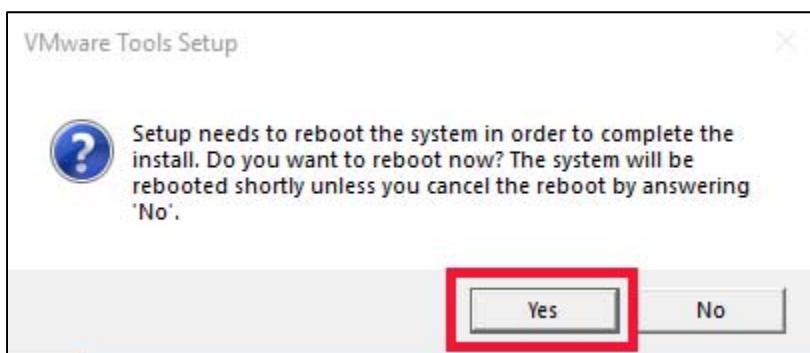


VMware Player – Start VM

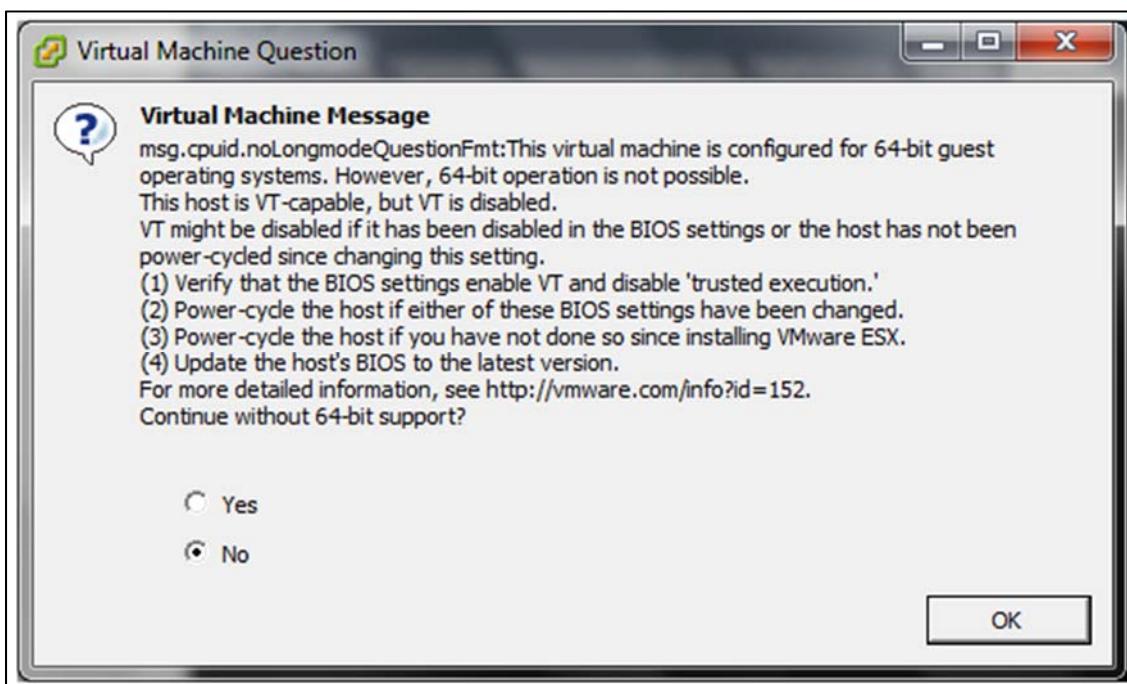
12. If prompted, select “I Copied It”.



13. You may receive a message regarding having to reboot your VM as seen below. If you get this message, reboot the VM.



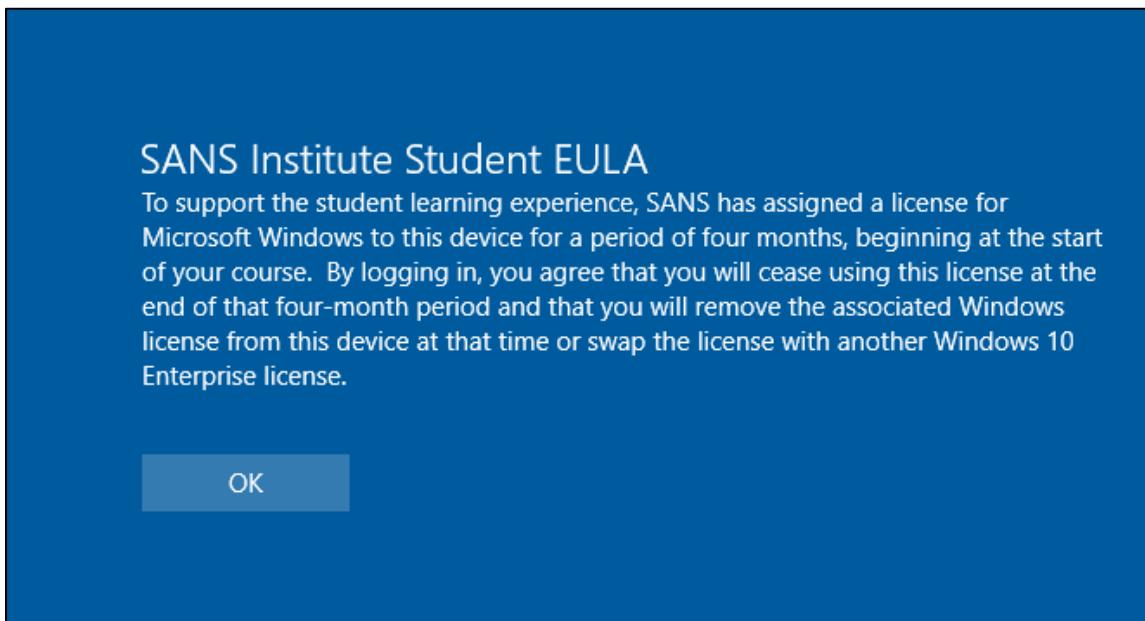
14. **NOTE:** If you DO NOT receive an error on boot, please skip to **Part 3**. Some might get this error: **This host is VT-capable, but VT is disabled.**



#### Possible VM Error if VT Threading Is Not Enabled

15. If you receive this error, you may not have virtual machines allowed in your BIOS/UEFI. If you need assistance changing the setting, speak to your instructor. If you are using OnDemand, contact the Subject Matter Expert.

- When presented with the **SANS EULA**, read it carefully, then press **OK**.

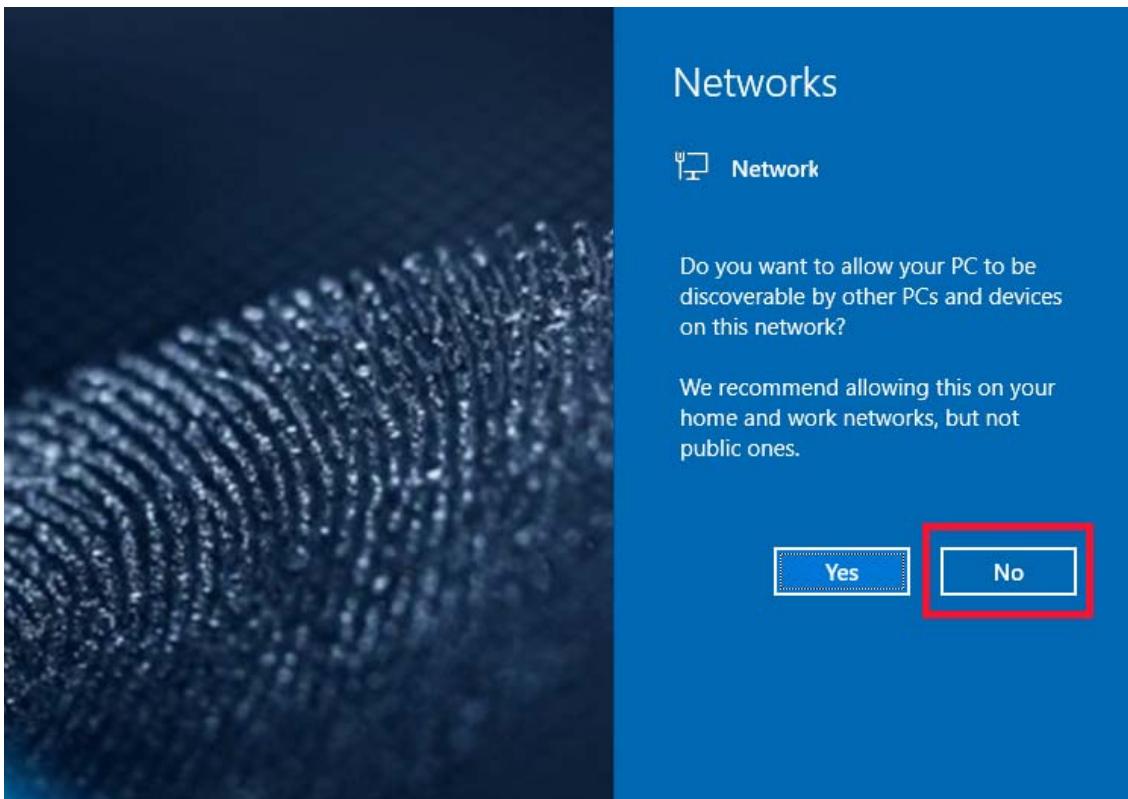


- Click anywhere on the screen to display the log in dialog. Login to the **FOR498 Windows VM** using the following credentials:
  - Username: **SANSDFIR**
  - Password: **forensics**

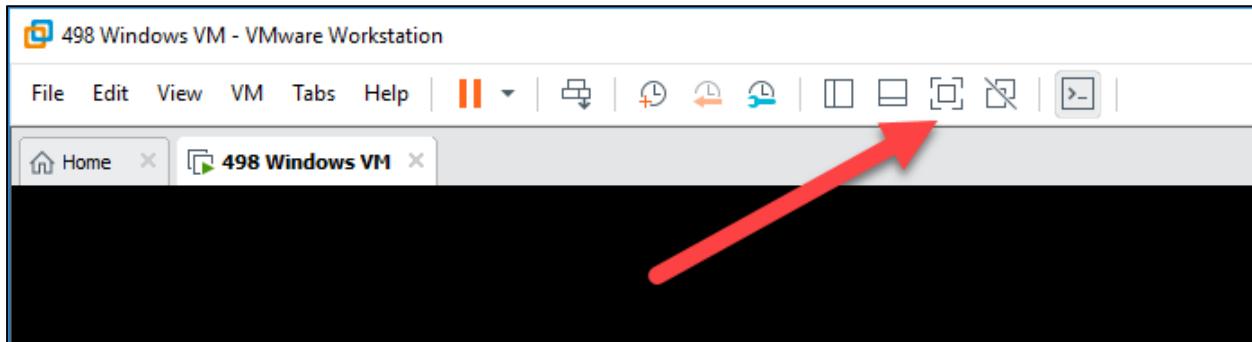


- Once logged in, you should see a standard Windows desktop with several sets of shortcuts on the **Desktop**. It is recommended to attempt to use the highest screen resolution as possible. We highly recommend that you set your display to one of the following: 1920x1080 or 1366x768. If you are comfortable with your settings as is, then don't change them.

4. You may see a **Networks** box appear on the right edge of your desktop, asking if you want to allow your PC to be discoverable by other PCs. Click **No** and the box will disappear.



5. You will typically have the best experience in full-screen mode in **VMware**. The icon to enter **Full Screen Mode** looks like the following (**VMware Player** bar looks slightly different, but icon is the same):

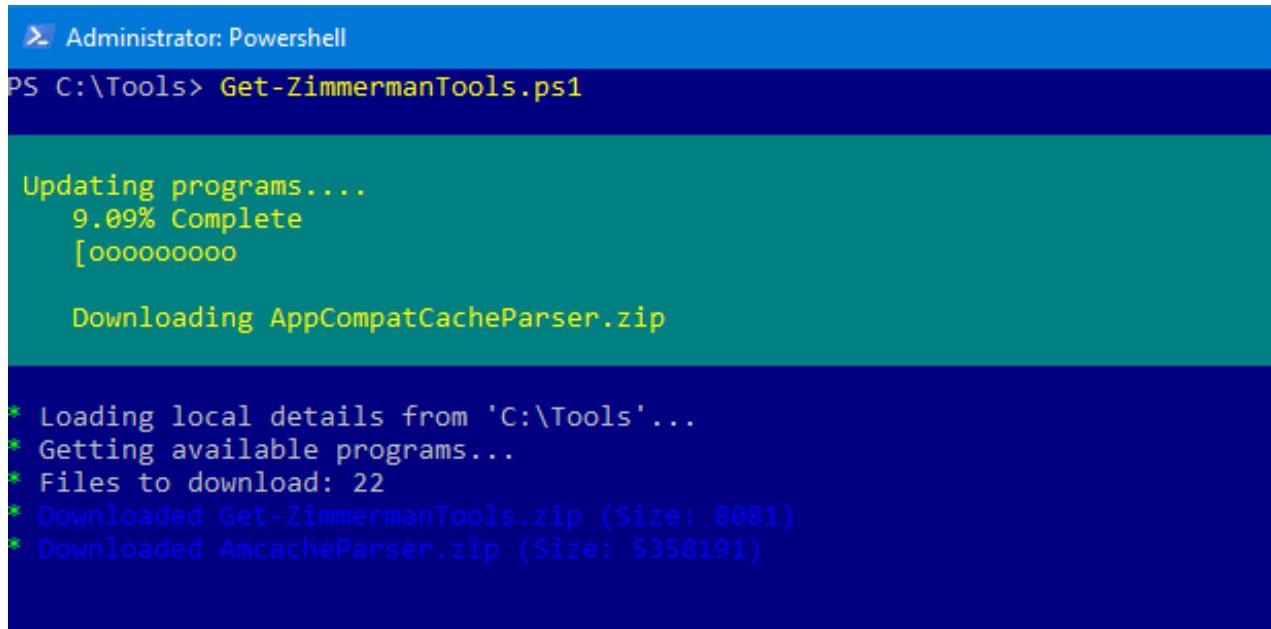


To exit full-screen mode, hover at the top of the screen to bring the **VMware** drop-down toolbar into view. You can then click the same icon to exit **Full Screen Mode**. You can also click on the pin icon at the far left of the toolbar to keep the toolbar visible.



6. **Update Zimmerman Tools:** Open a **PowerShell** window from the **Desktop** shortcut. Run the following command in the **PowerShell** window and press **ENTER** to update all available tools to their latest version.

```
Get-ZimmermanTools.ps1
```



```
Administrator: Powershell
PS C:\Tools> Get-ZimmermanTools.ps1

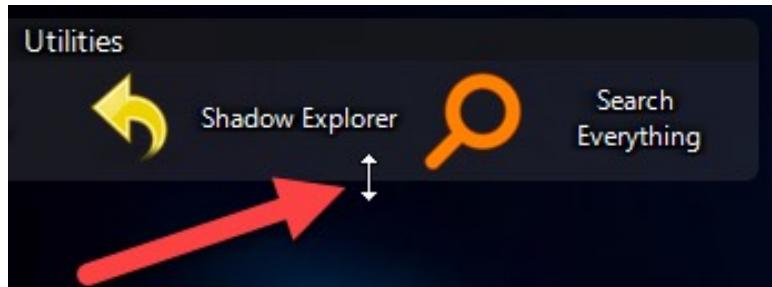
Updating programs....
 9.09% Complete
 [oooooooooo

Downloading AppCompatCacheParser.zip

* Loading local details from 'C:\Tools'...
* Getting available programs...
* Files to download: 22
* Downloaded Get-ZimmermanTools.zip (Size: 8081)
* Downloaded AmcacheParser.zip (Size: 5358191)
```

You can also simply right-click on the script on your **Desktop** entitled **Update Zimmerman Tools** and choose **Run with PowerShell** from the context menu.

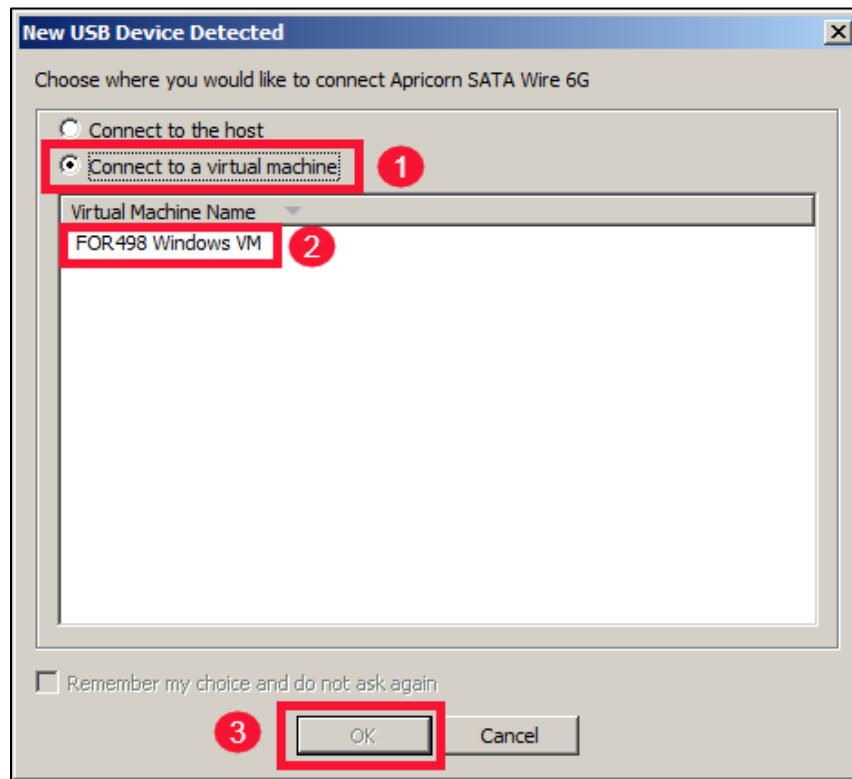
7. The **Desktop** contains several groups of icons, such as **Utilities** and **Network Tools**. Occasionally these groups are not big enough to show all of the icons in the group. For each of the groups on the **Desktop**, rearrange and resize the groups so all the shortcuts are visible. To resize a group, move the mouse to the bottom or side of the group until the cursor changes, as shown below. Then drag the group to make it bigger.



To move a group, click and drag on the group name, then move the group as needed.



8. Connect the SANS provided SATA to USB adapter to the student provided hard drive, then connect it to your host computer.
9. When you plug your device in, VMWare may offer to connect it to the VM. If it does, connect the external hard drive to the VM.

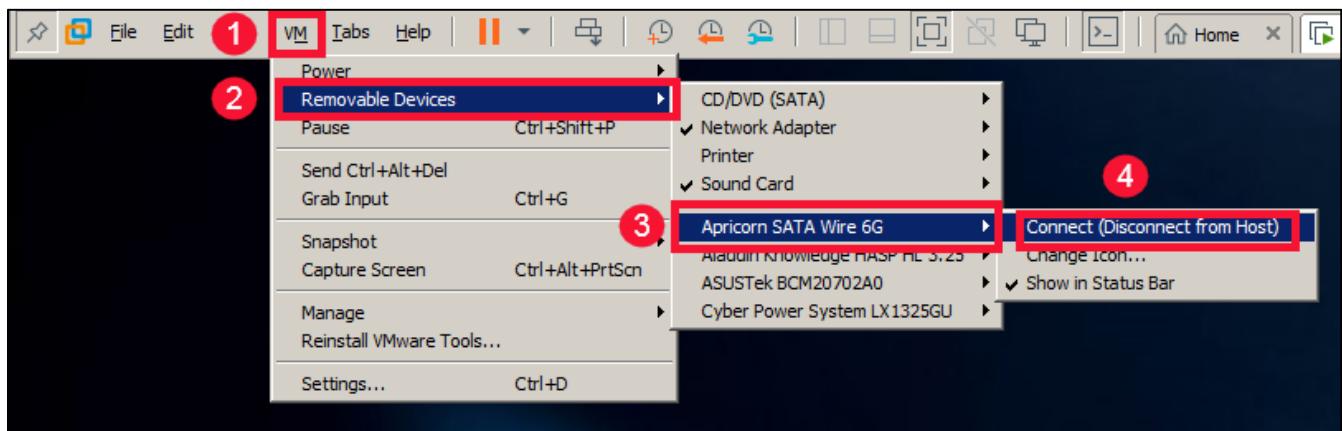


10. You may also see a box like the one below. It is merely listing all of the devices that are available to be connected to the VM. Your list will certainly differ from the one below. You can check the box that says, “Do not show this hint again” (if you don’t want to see it again), and then click OK.

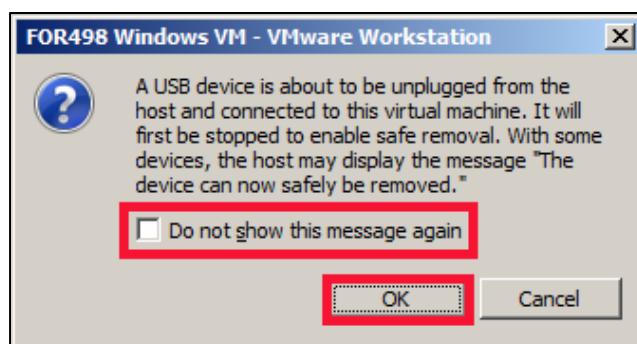


11. If you are not prompted, connect the drive to the VM manually via VM → Removable Devices → <Device name> → Connect (Disconnect from Host).

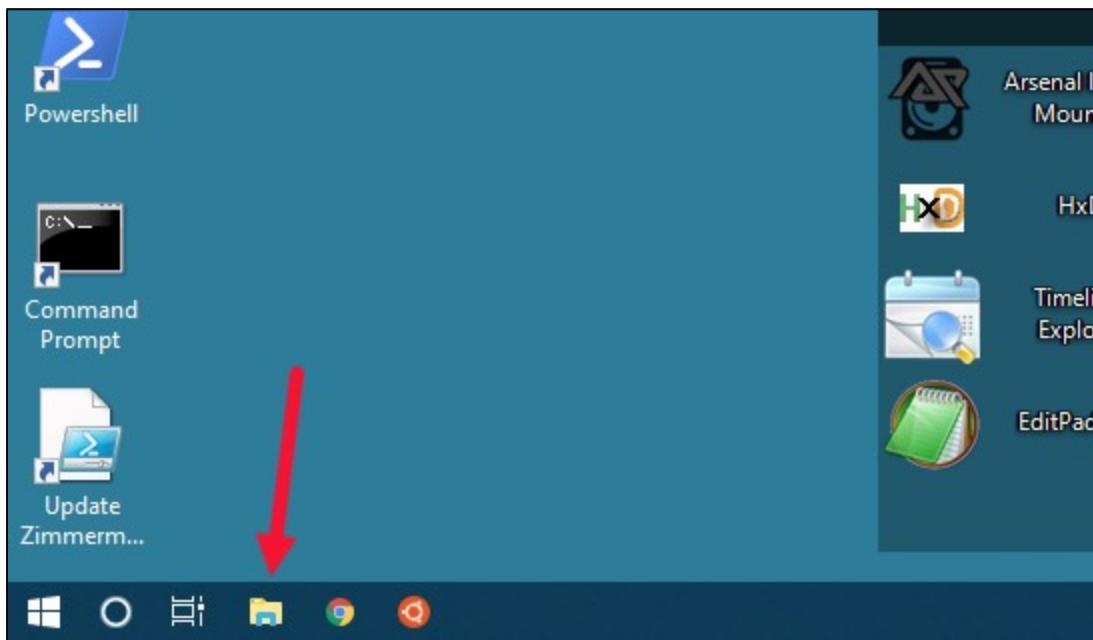
You will of course have to find the appropriate device to connect (an Apricorn SATA Wire 6G is shown in the example below).



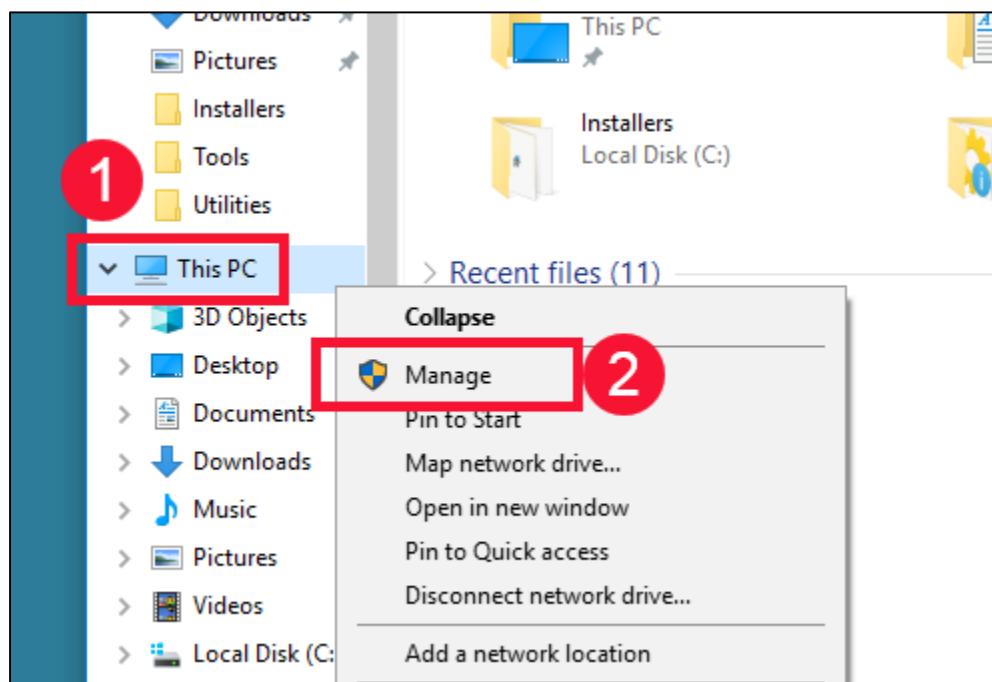
12. If you have had to connect your drive using the method in step 10 above, you may then see the message below. You can choose to check the box or not, and then click OK.



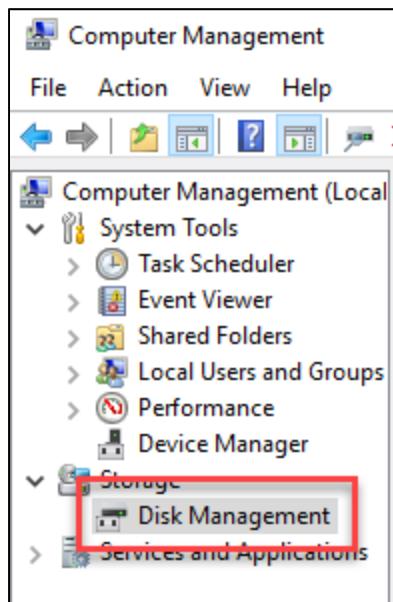
13. In the FOR498 Windows VM, start File Explorer...



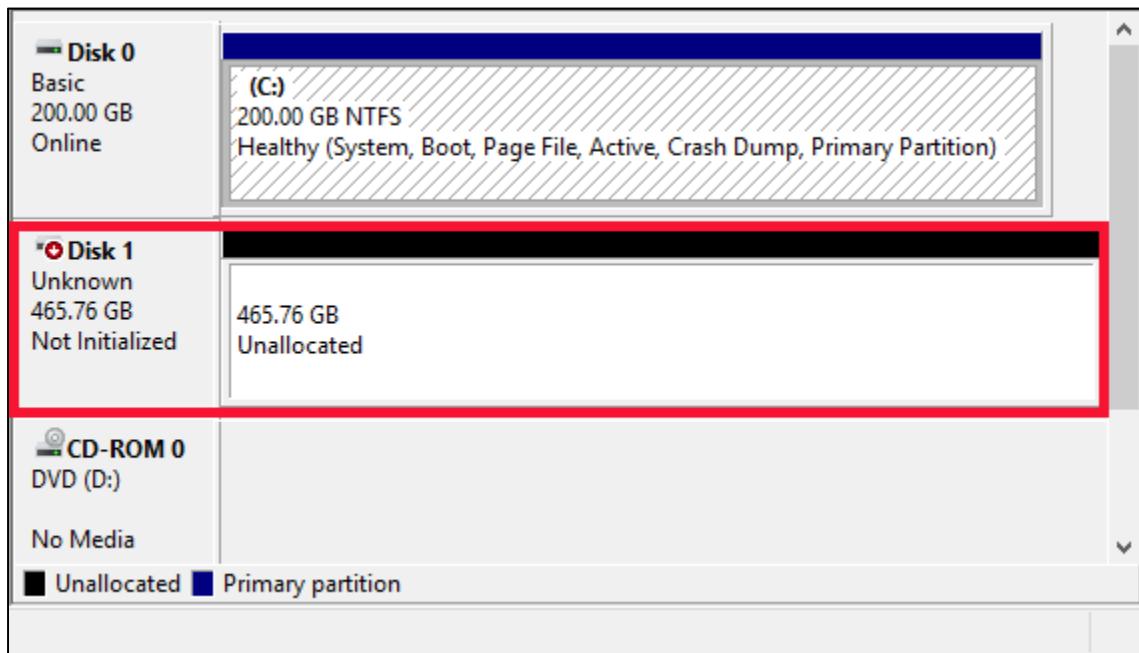
14. ...then right-click on This PC and chose Manage.



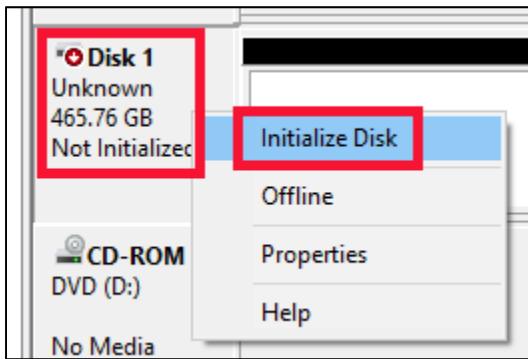
## 15. Click Disk Management.



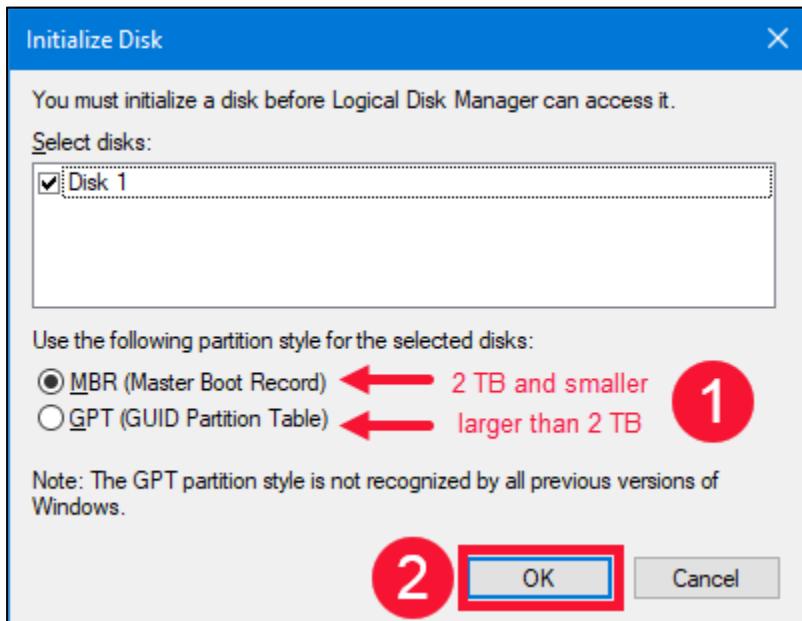
16. Find the device you just connected in the list of devices shown. You will see one of two things, depending on the format status of your hard drive. If your hard drive is brand new and/or is not formatted, you will see the highlighted item below. Depending on your hard drive, its size will not be the same as the size below. If your **Disk** does not say “**Unallocated**”, proceed to **step 20**.



17. Right click on **Disk 1** (your disk may be a different number) and select **Initialize Disk** from the drop-down menu.

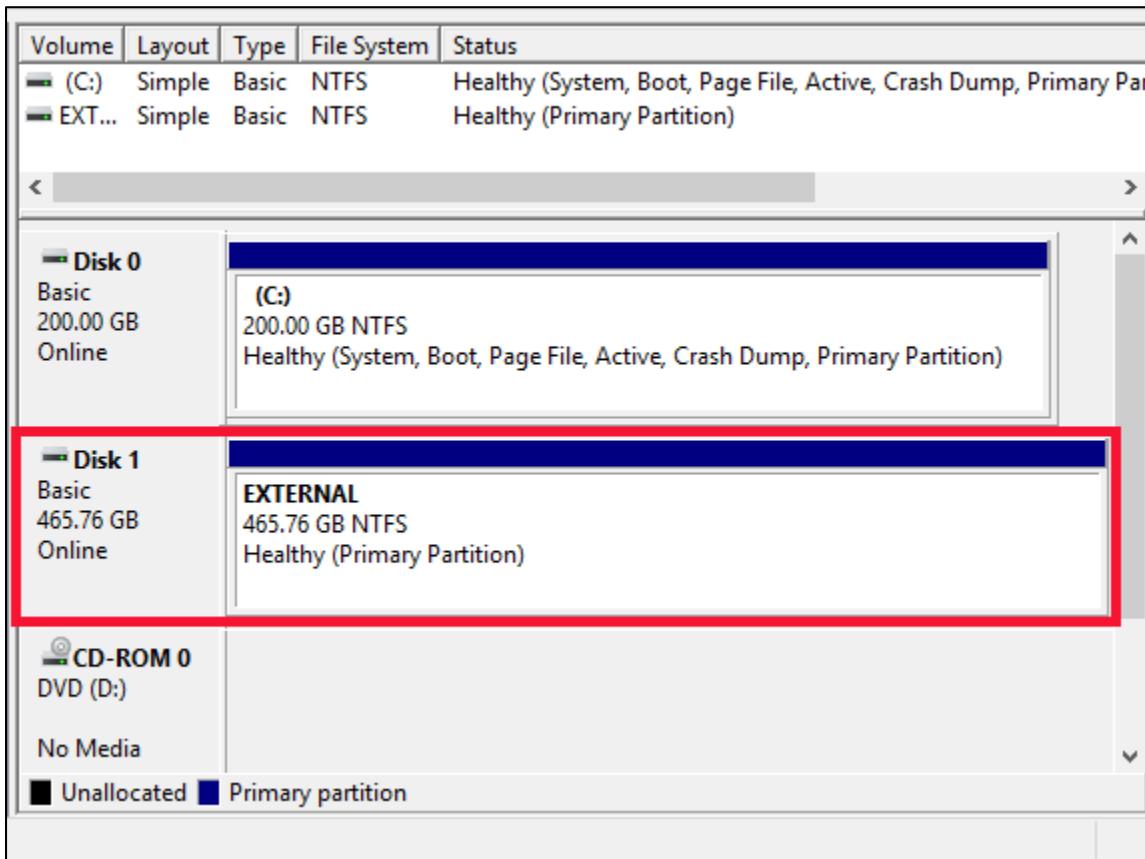


18. You will be presented with the **Initialize Disk** box. Your disk should be selected. If your disk is 2 TB or smaller in size, select **MBR**. If your disk is larger than 2 TB, select **GPT**. Then click **OK**. In fact, you may be presented with this box during **step 16**. Deal with it in the same way.

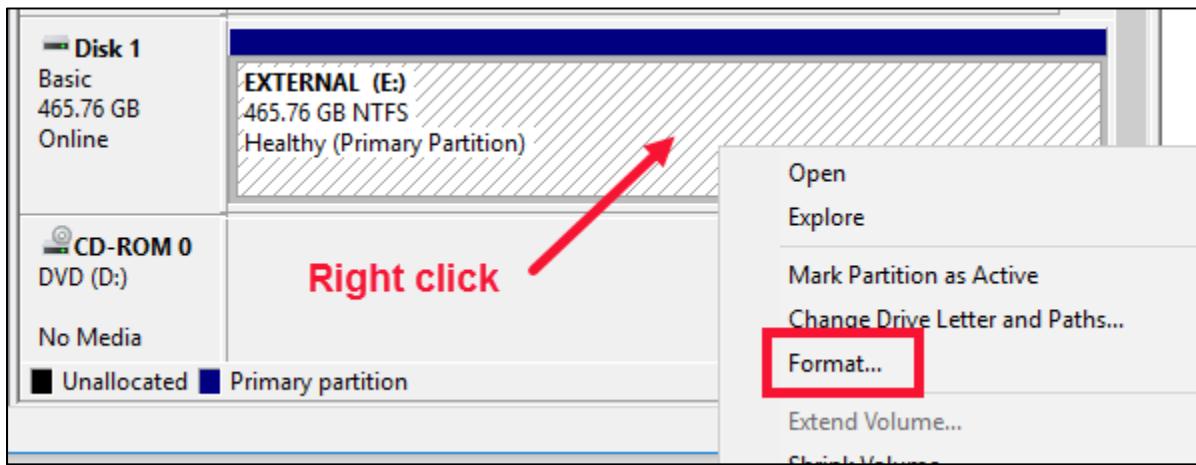


19. The **Disk 1** box will no longer have the red and white arrow originally seen. At this point, proceed to **step 21**. Although your drive is still indicated as **Unallocated**, follow the same steps as in **step 21**.

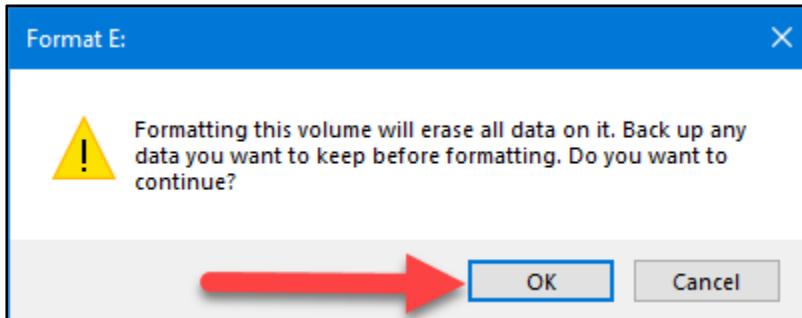
20. If your hard drive is currently formatted, you will see the highlighted item below (probably with a different name). Depending on your hard drive, its size will not be the same as the size below.



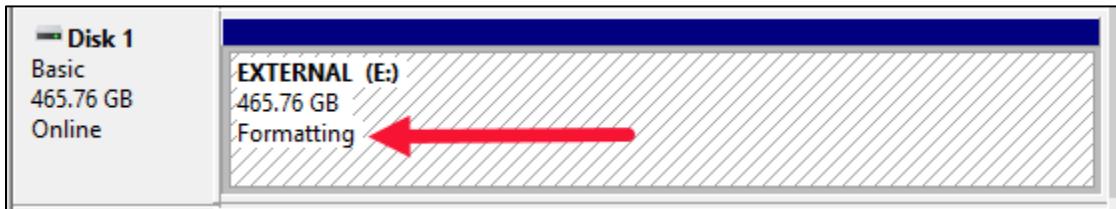
21. Right-click on the device, then choose **Format** from the context menu. If your drive is not formatted, you will not see the below. In that case, proceed to step 26.



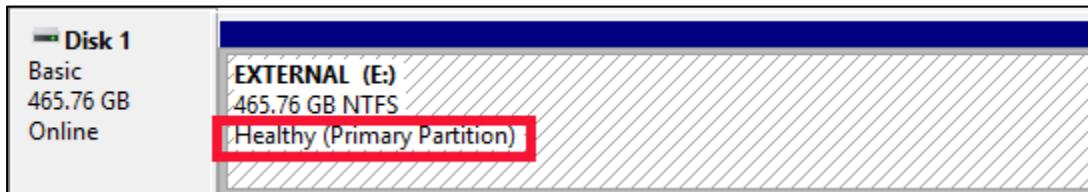
22. When prompted about erasing the data, click **OK**.



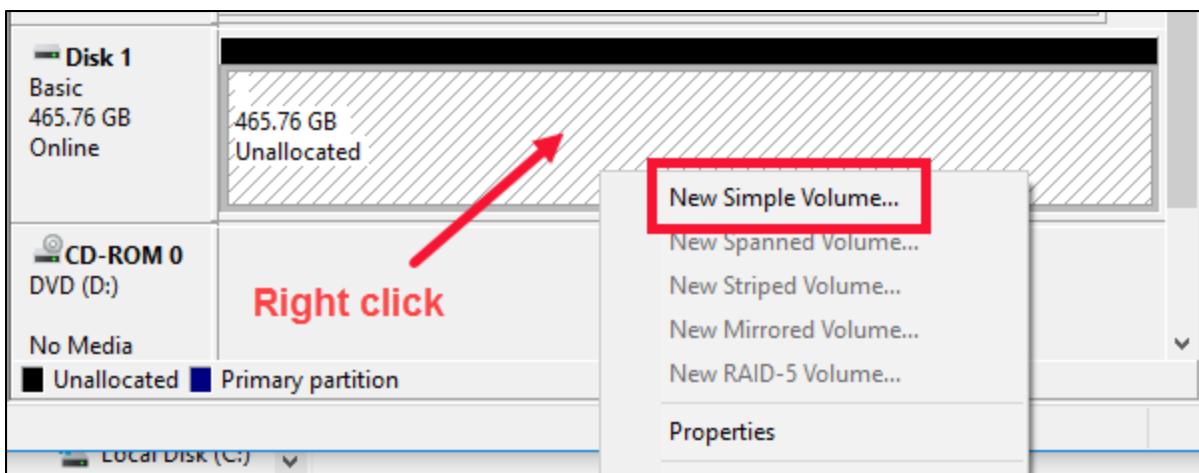
23. As the drive is being formatted, the device will show “**Formatting**” as seen below.



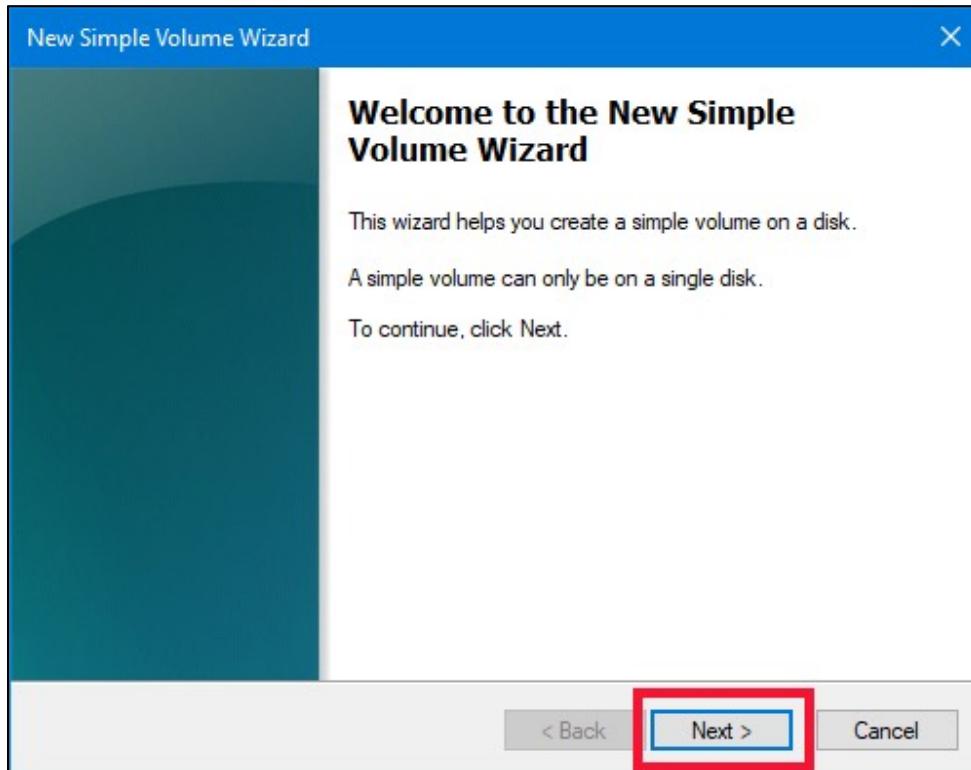
24. When the format is finished, the drive’s status will show the drive as **Healthy**.



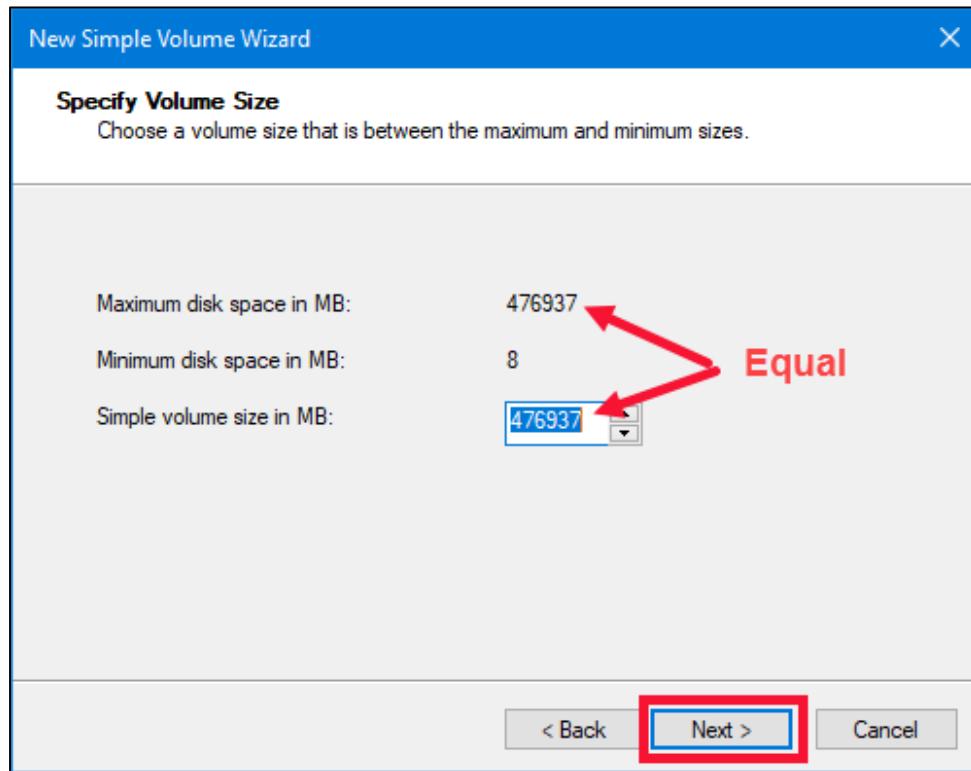
25. You can now properly eject your external hard drive, and power down your **FOR498 Windows VM**. If you don’t, the next exercise part (**Part 4**) may take longer. Proceed to **Part 4**.
26. If your drive is not formatted, you will see the below. In this case, right click on the device and choose **New Simple Volume** from the context menu.



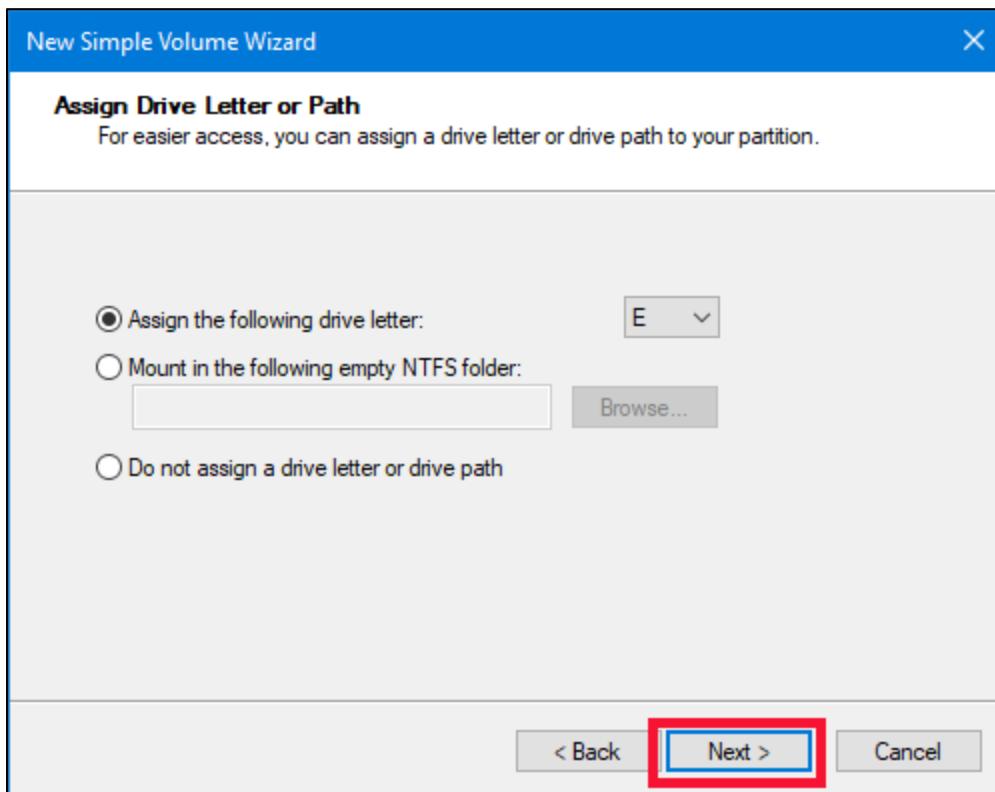
27. The New Simple Volume Wizard will start. Click Next.



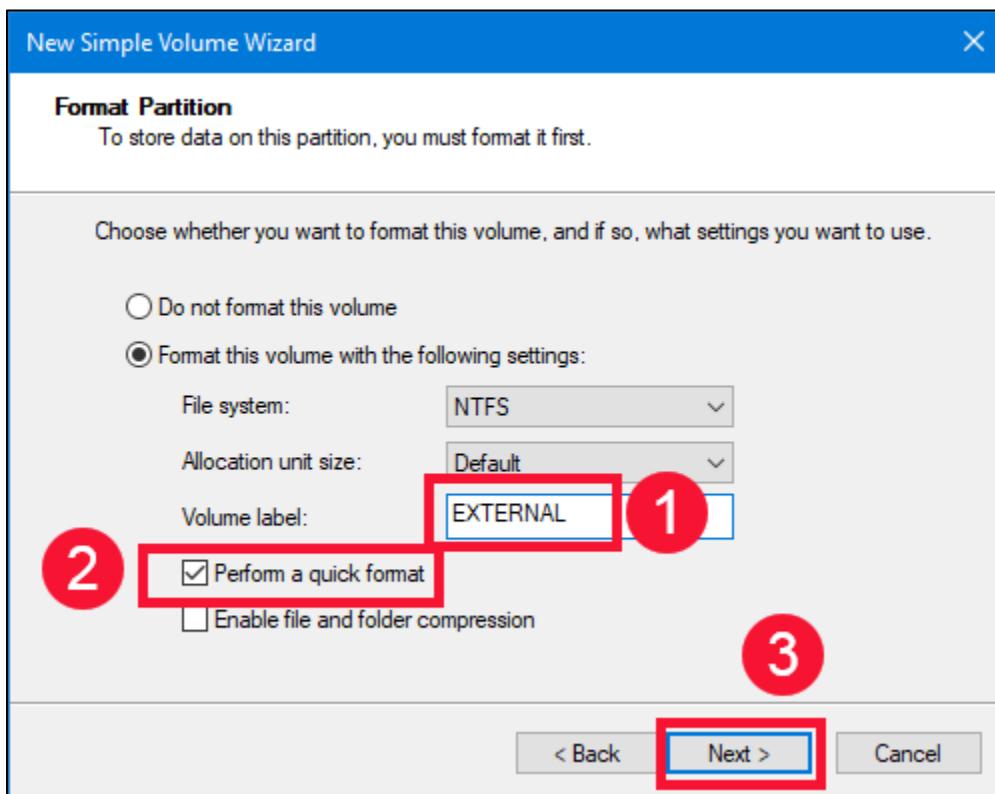
28. In the **Specify Volume Size** box, ensure that the **Maximum disk space** and the **Simple volume size** are equal, and then click **Next**.



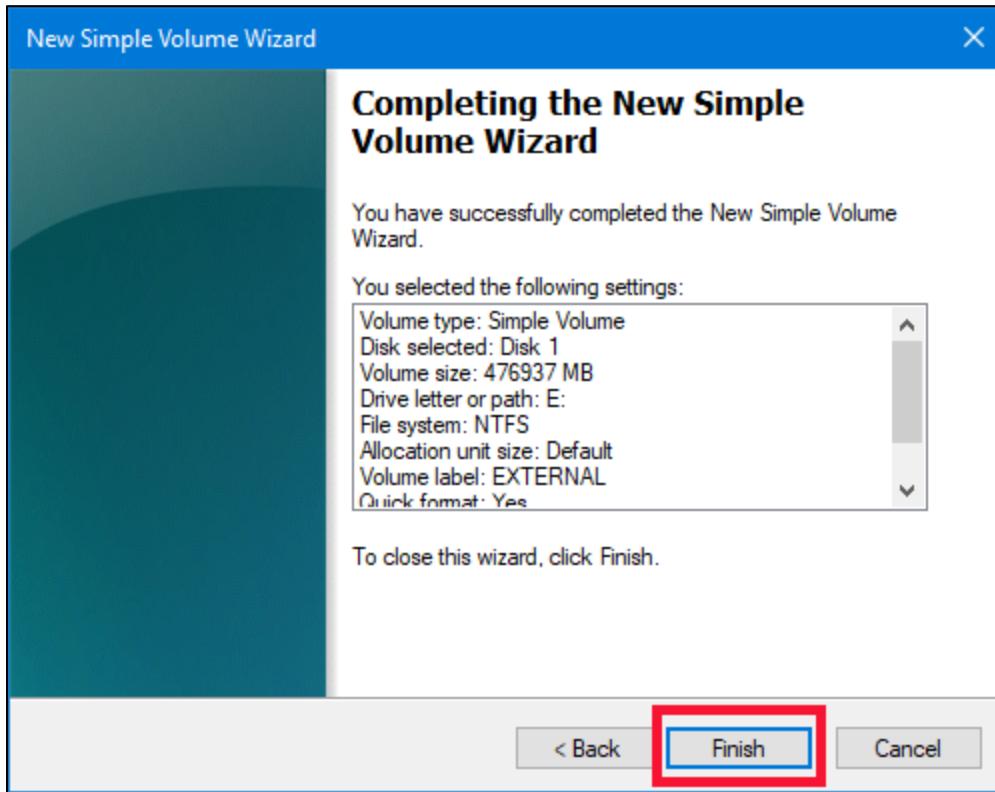
29. The **Assign Drive Letter or Path** box will appear. Accept all defaults and click **Next**.



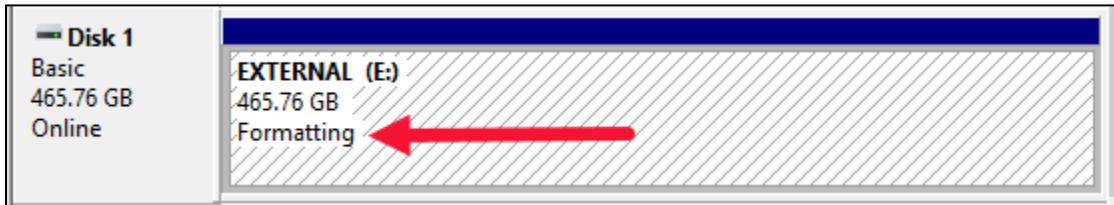
30. In the **Format Partition** box, change the **Volume label** to **EXTERNAL**. Ensure that the **Perform a quick format** box is checked. Click **Next**.



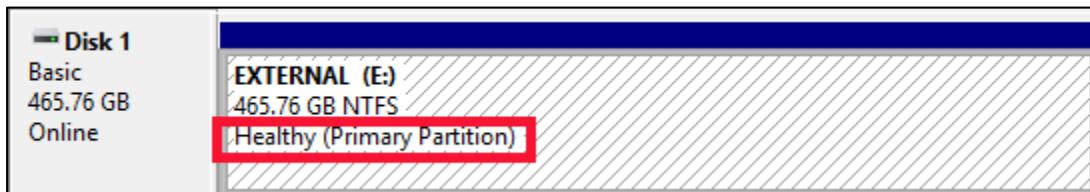
31. A box summarizing your chosen settings will be shown. Click **Finish**.



32. As the drive is being formatted, the device will show “**Formatting**” as seen below.



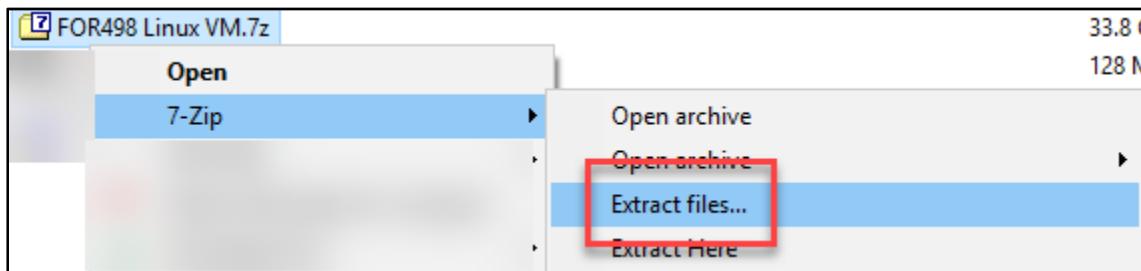
33. When the format is finished, the drive’s status will show the drive as **Healthy**.



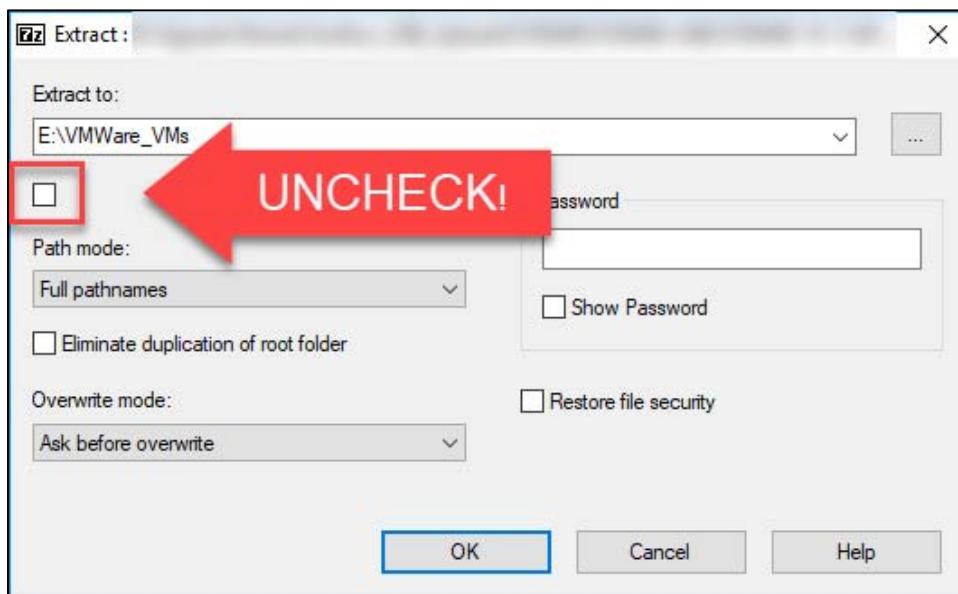
34. You can now properly eject your external hard drive, and power down your **FOR498 Windows VM**. If you don’t, the next exercise part (**Part 4**) may take longer.

**Part 4—Unzipping the 498 Linux Virtual Machine**

1. Insert the **FOR498** USB **B** into your host system. You will receive the **FOR498** USB **B** by the first day of the course, if you do not have it now. Please wait until you receive the USB keys before configuring your system.
2. On the USB, browse to the **root** directory.
3. Unzip the **FOR498 Linux VM.7z** file to your **Virtual Machines** folder on your host, as shown below:
  - Right-click the file to get the **7-Zip** options and select **Extract Files...**:



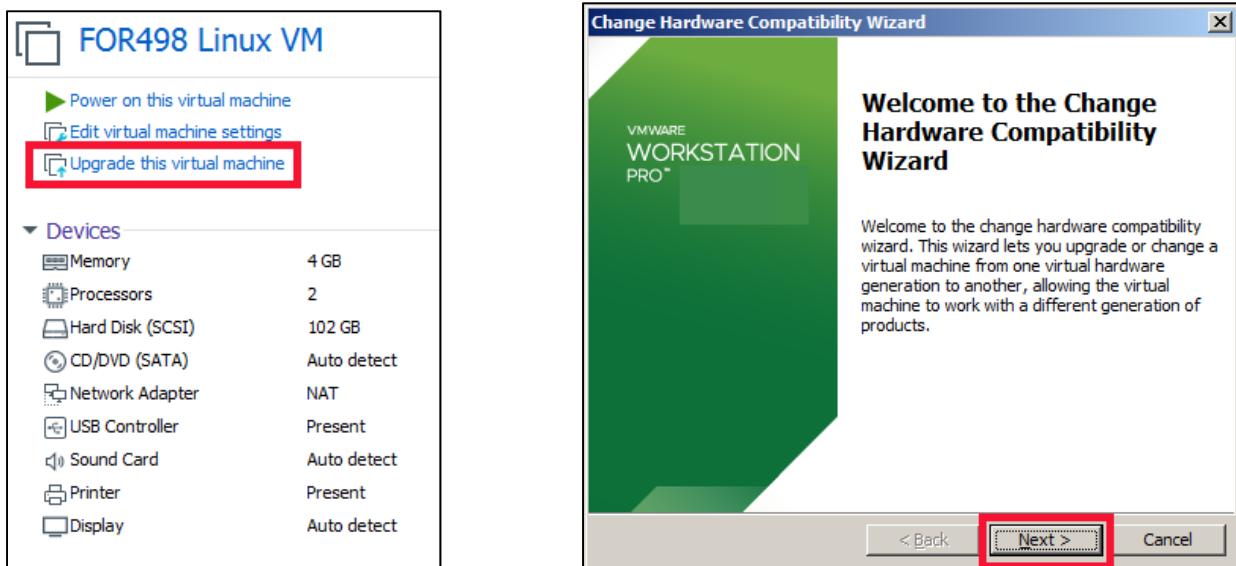
- Select a Folder on your system to “**EXTRACT TO:**” Generally, we recommend a folder where you keep your virtual machines such as **C:\Users\<Username>\Documents\Virtual Machines**
- Uncheck the check-box below the “**Extract to:**” path, and click **OK**.



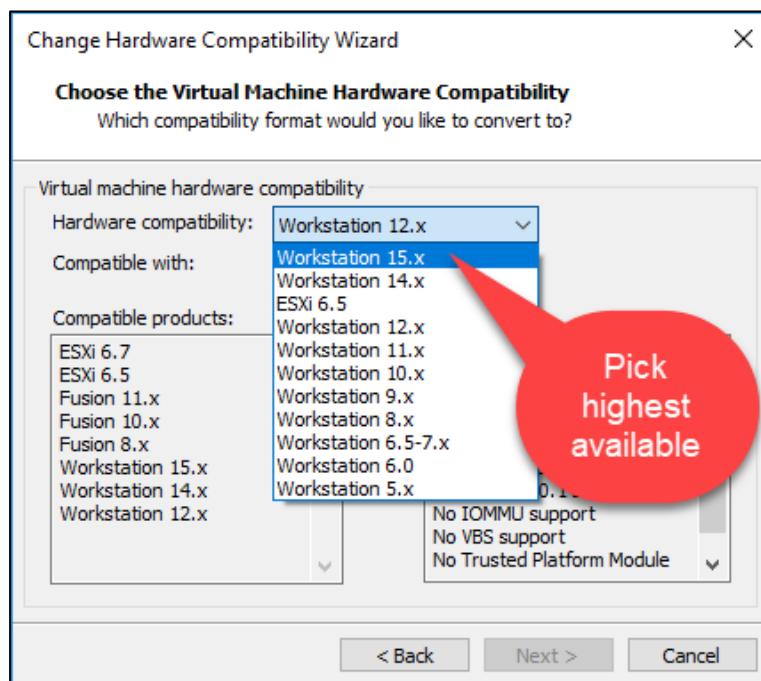
- After the extraction process is complete (maybe 10–20 min), you should see a new folder in your selected export folder called **FOR498 Linux VM**.

**Part 5—Configuring the 498 Linux Virtual Machine**

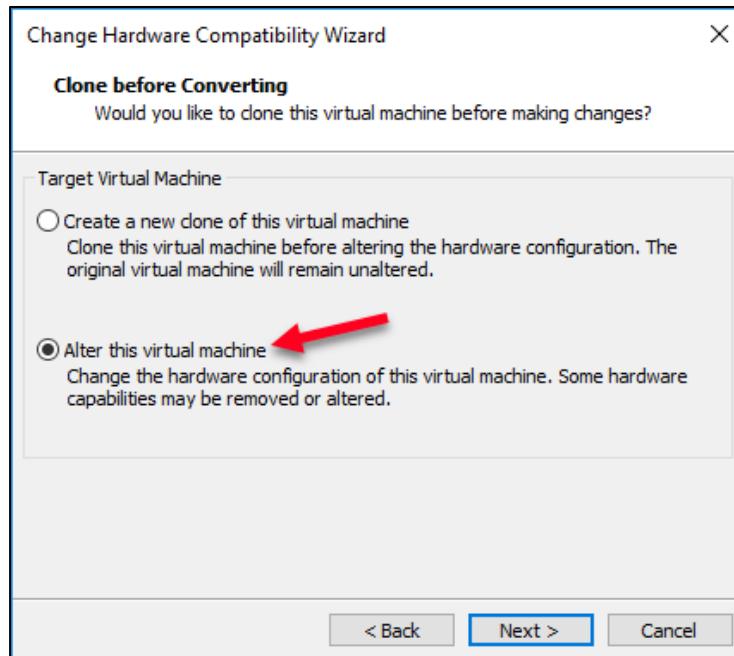
1. Start **VMware Workstation** or **Player** and open (**File → Open**, or **Player → File → Open** on VMware Player) the virtual machine file located in the **FOR498 Linux VM** directory called **FOR498 Linux VM.vmx**. This will load the **FOR498 Linux VM** in your **VMware** application.
2. Upgrade your virtual machine if you can, by selecting **Upgrade this virtual machine**. VMware Player does not have this feature.



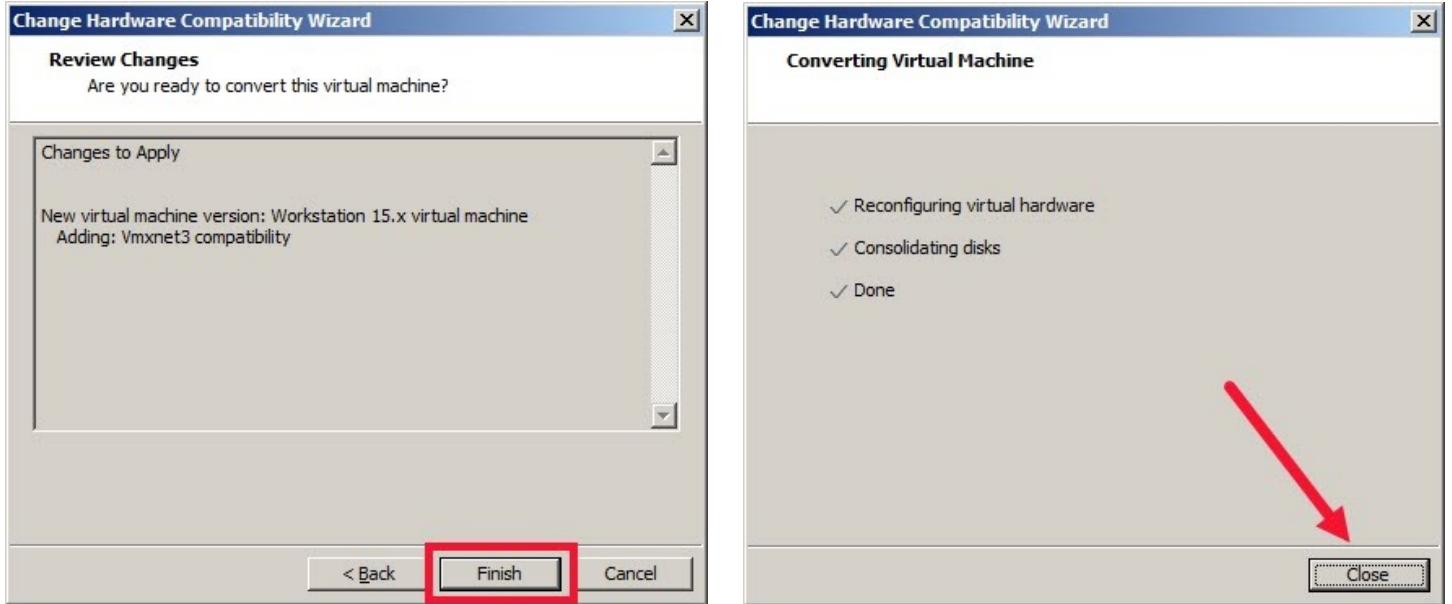
3. Complete the **Change Hardware Compatibility Wizard** that appears and choose the highest available version from the **Hardware Compatibility** pull-down list and click **Next**.



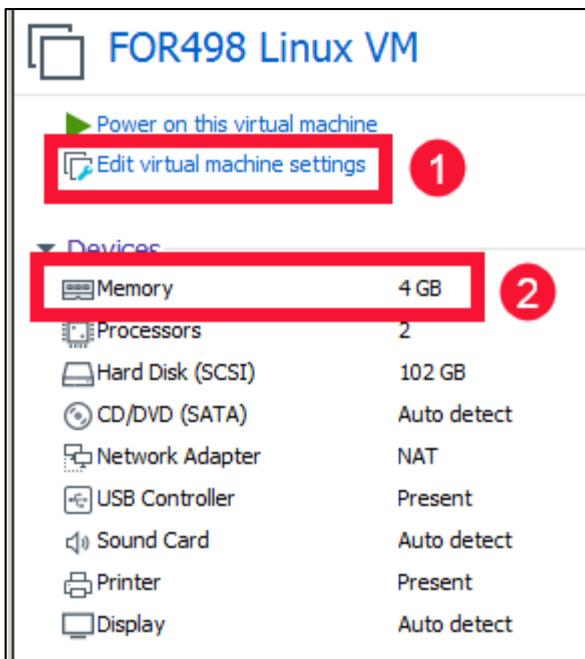
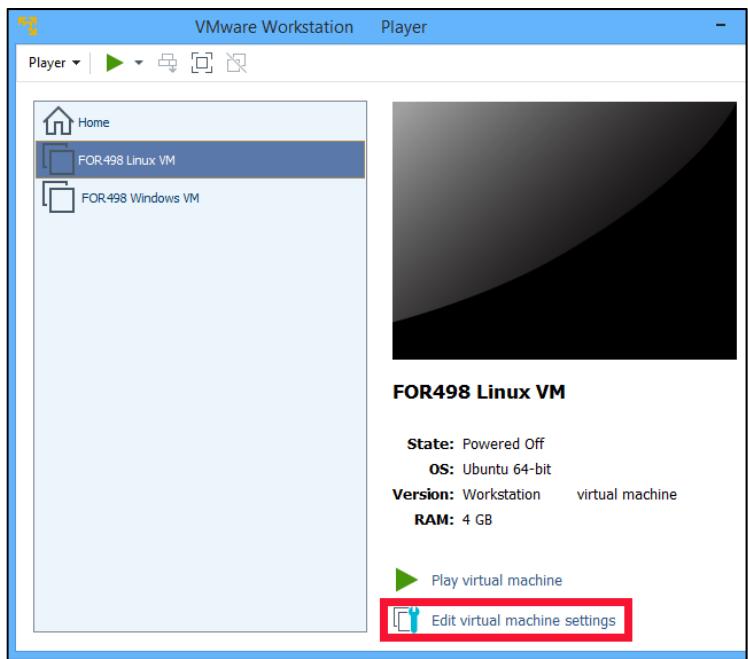
- On the next screen, make sure you simply “Alter” the VM and do not create a new clone, which will take some time. Again, click **Next**.



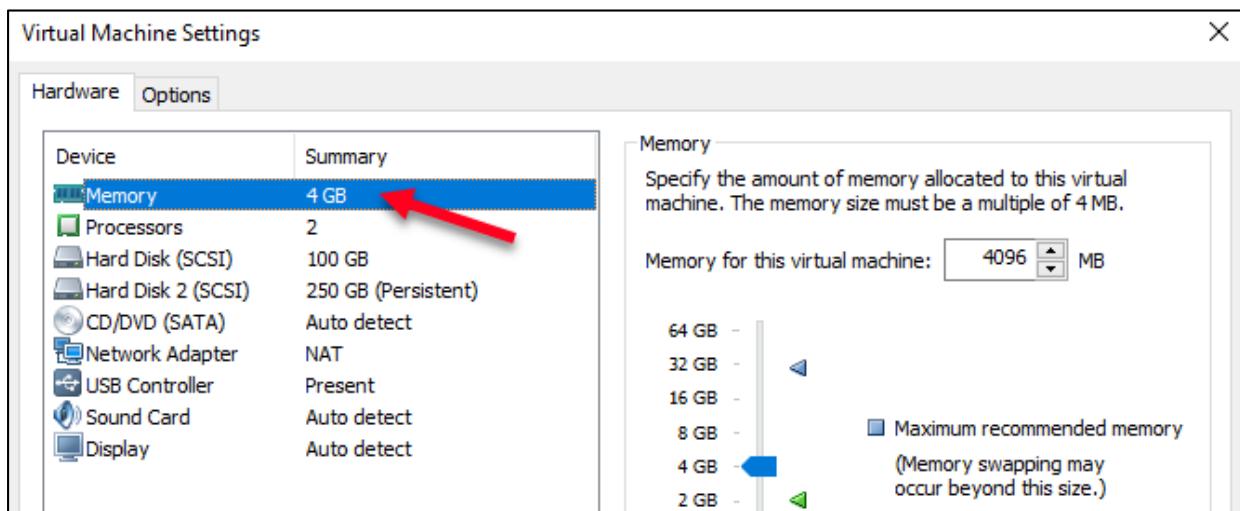
- The next screen will review the changes you have made. Click **Finish**, and then on the screen that follows, click **Close**.



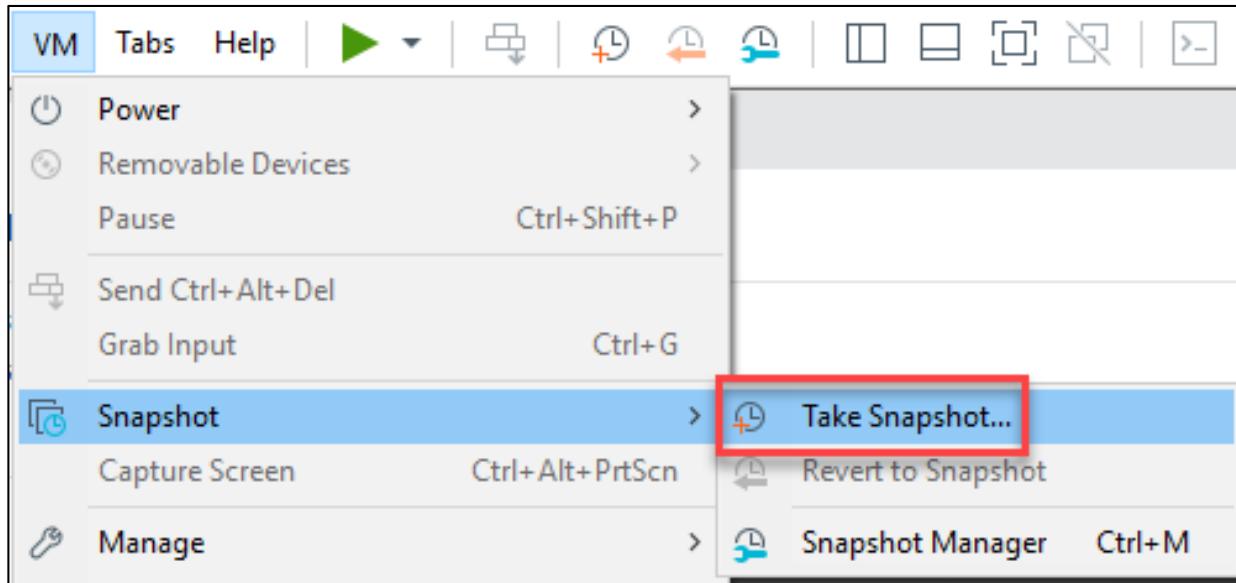
6. The **FOR498 Linux VM** requires at least 4 GB of RAM. If your host system has 8 GB of RAM, do not adjust this setting. You should allocate no more than half of your host's RAM to this **VM**. If your host has more than 8 GB RAM, such as 16 or 32 GB, then the **FOR498 Linux VM** can perform better by assigning it more RAM. To do so, adjust the memory by selecting **Edit virtual machine settings** and then selecting **Memory**.

VMware Workstation – Edit VM SettingsVMware Player – Edit VM Settings

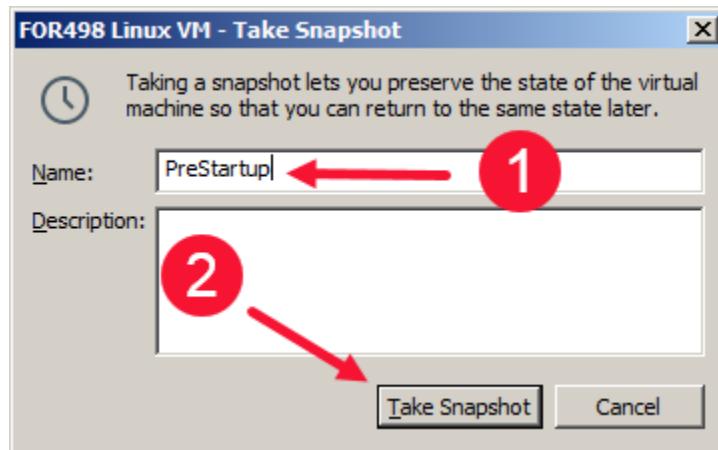
- Then make the appropriate adjustments to **Memory**.
  - Note: You can also adjust the number of **Processors**. Similar to RAM, it is not recommended to assign more than half the total number of CPU cores available on your host system.



7. Take a **Snapshot** of the current state of the virtual machine via the **VM** → **Snapshot** → **Take Snapshot** option. If you are using **VMware Player**, you do not have this option.

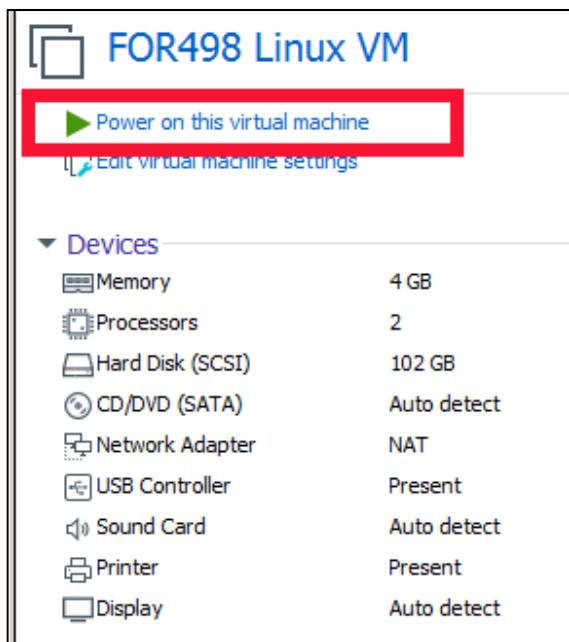
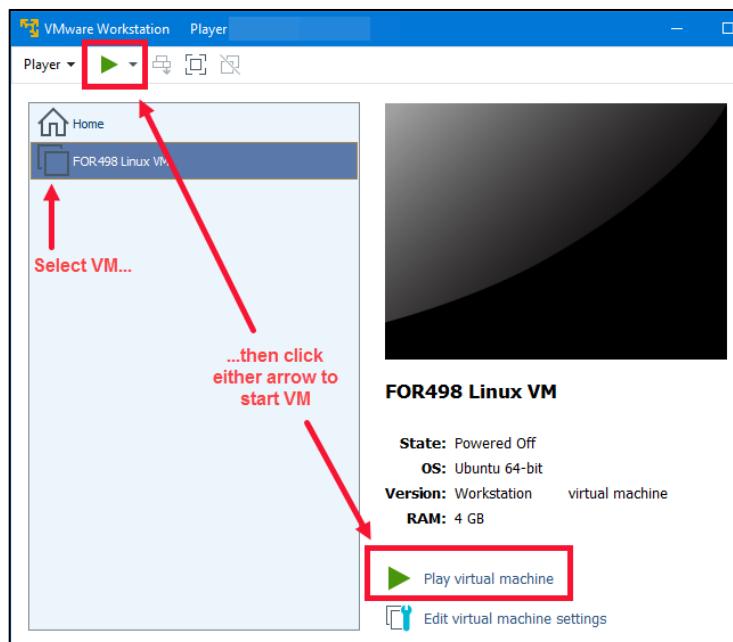


8. Name the **Snapshot PreStartup**.

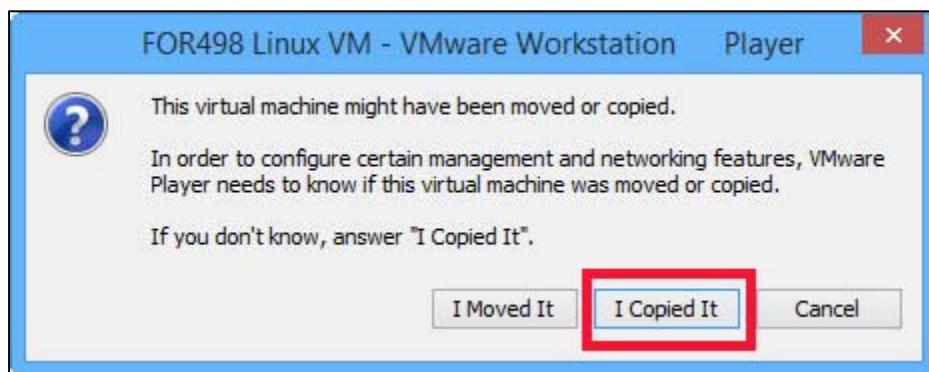


**Part 6—Running the 498 Linux Virtual Machine**

- Power on your virtual machine. If you see any update messages, do NOT accept them.

VMware Workstation – Start VMVMware Player – Start VM

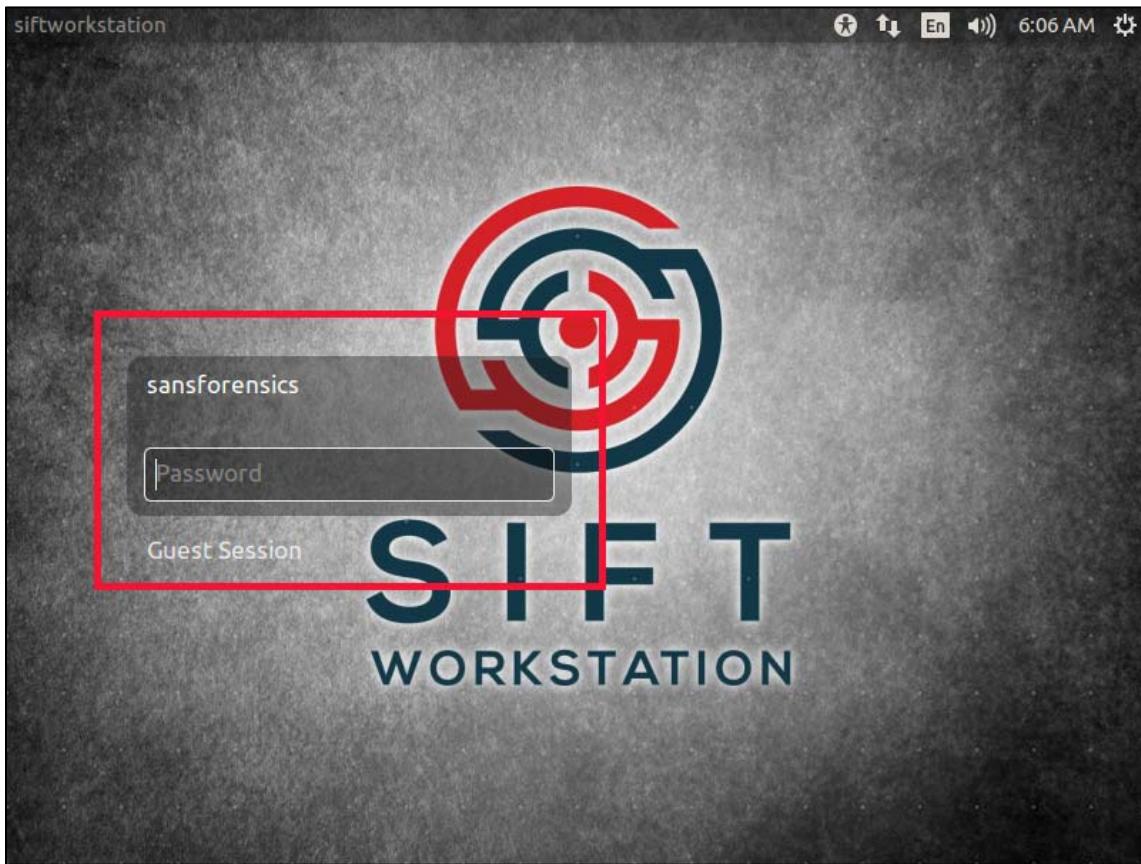
- If prompted, select “I Copied It”.



- After initiating the startup of the VM, you will see the login screen appear, prompting for credentials.

4. Login to the FOR498 Linux VM using the following credentials:

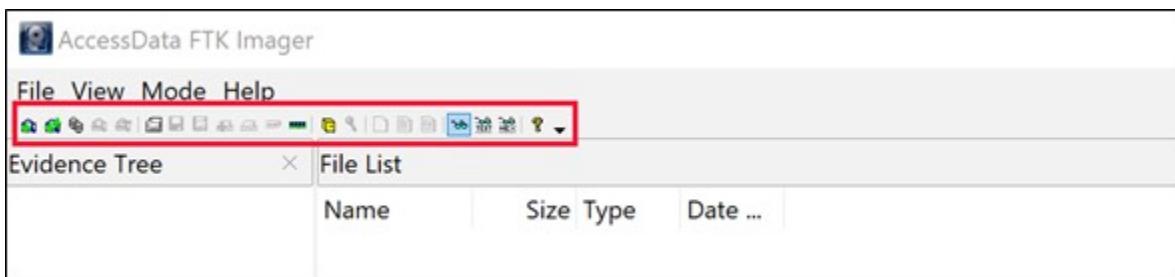
- Username: **sansforensics**
- Password: **forensics**



#### **Part 7—DPI Scaling Issues**

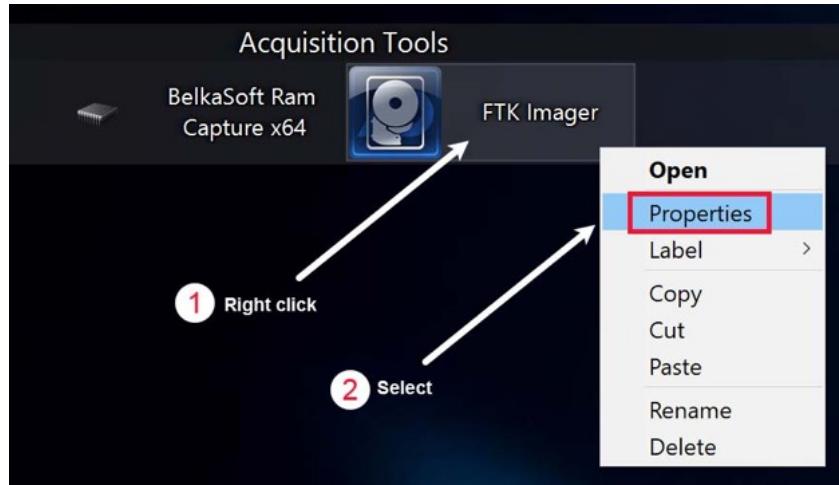
**This part of the exercise will not apply to every student.**

Notwithstanding the resolution size issues of a given Desktop on a given system, there is an extra issue that presents itself frequently with laptops containing Hi-res, or 4K screens. The issue leads to programs opening in VMs with less than optimal resolution. For example, in the FOR498 Windows VM, the icons in the tool bar may be so small as to be unusable or unreadable, as seen in the example below.

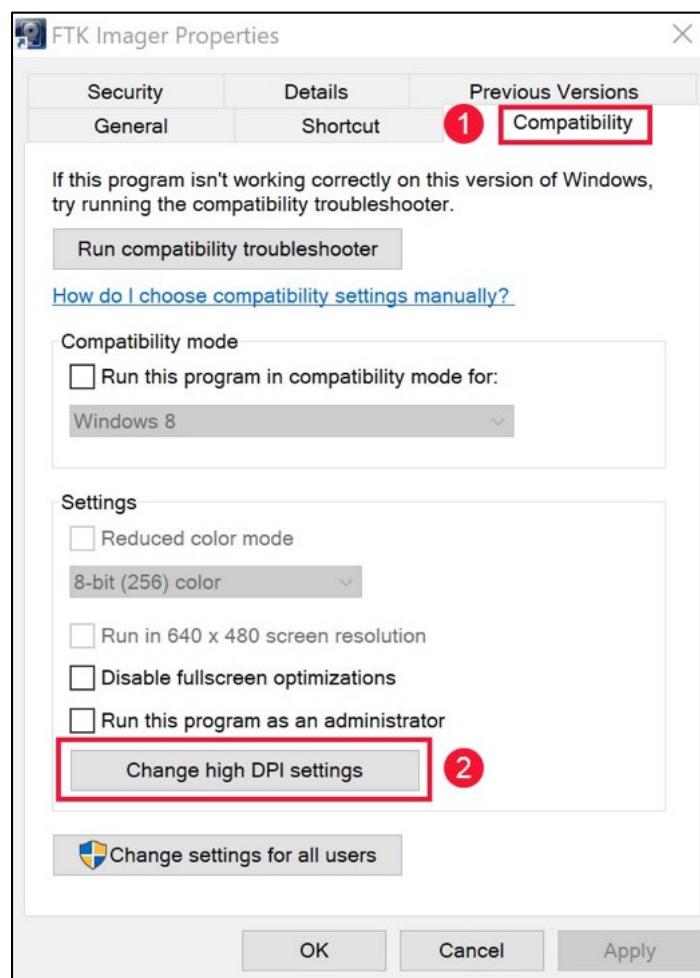


If this is the case, follow these steps:

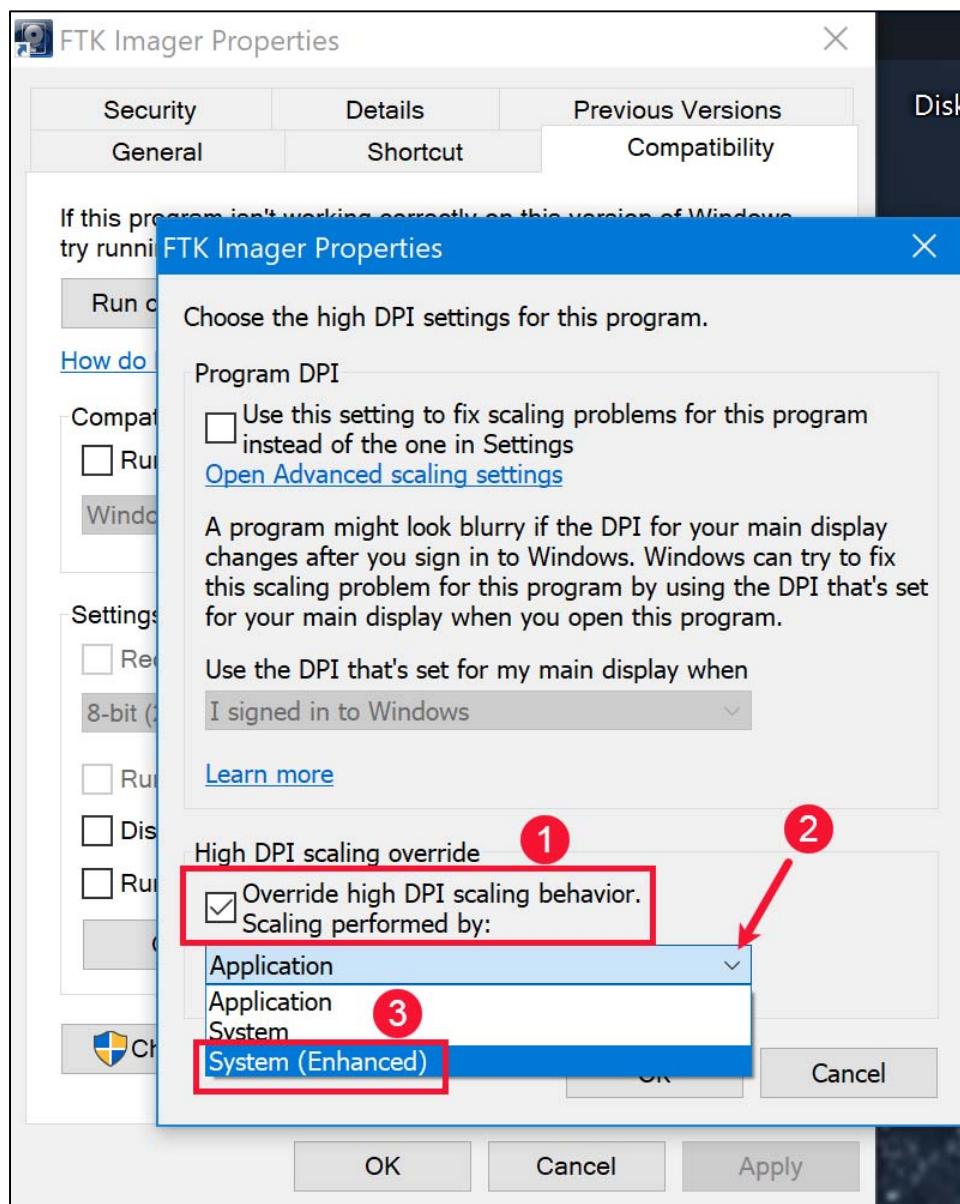
1. Close the program that is open, and then right click on the icon and select **Properties** from the drop-down menu.



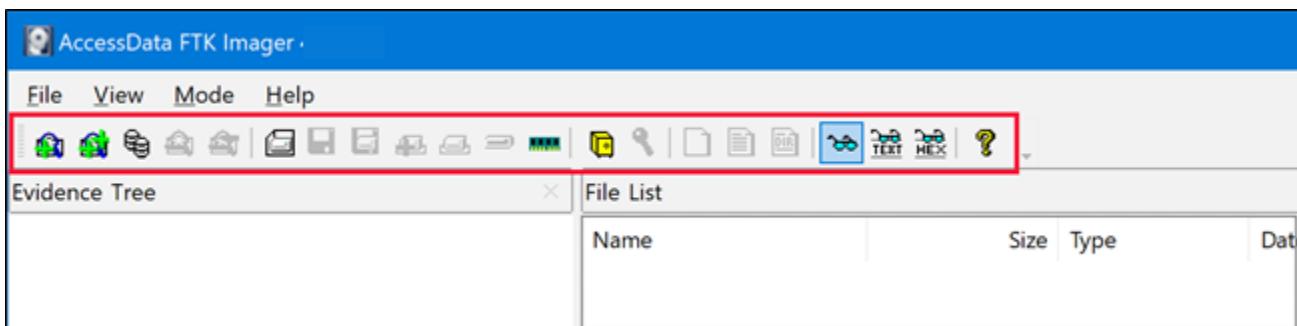
2. In the program **Properties**, a number of tabs will be visible. Click on the **Compatibility** tab, and then click on the **Change high DPI settings** button.



3. Another box will open. Place a checkmark in the box titled **Override high DPI scaling behavior**. Scaling performed by.. Click the arrow for the drop-down menu and select **System (Enhanced)**. Click **OK**, and then click **OK** again to be taken back to the **Desktop**.



4. Open the program again and the toolbar and other resolution issues should be solved.



# © SANS Institute 2020

## Exercise 0b – SIFT and Windows VM Setup

### Objectives

- Install and prepare your lab workstation for Battlefield Forensics this week.

### Installing the FOR498 Windows and Linux VMs – MAC HOST

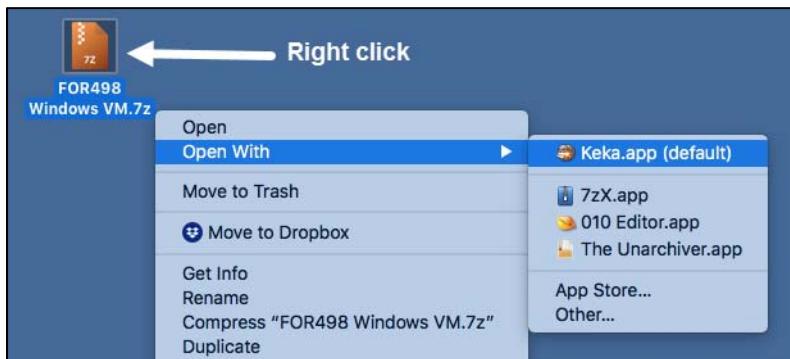
### Exercise Preparation

1. Install VMware Fusion.
  - <http://www.for498.com/fusion>
2. Install Keka program.
  - Located on your **FOR498 USB A** under **\Installers\Keka.dmg**

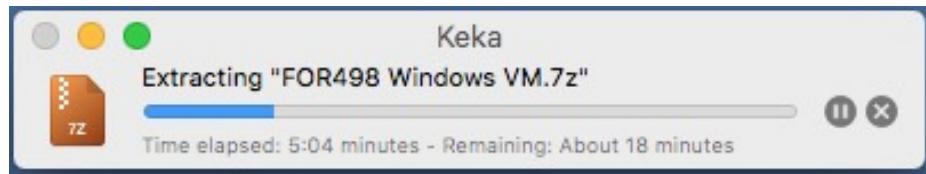
### Part 1—Unzipping the 498 Windows Virtual Machine

This section is for people using a Mac computer as their host. If you are using a Windows product as your host, please turn back to “**Exercise 0a – SIFT and Windows VM Setup**” that precedes this exercise.

1. Insert the **FOR498 USB A** into your host system. You will receive the **FOR498 USB A** by the first day of the course, if you do not have it now. Please wait until you receive the USB keys before configuring your system.
2. On the USB, browse to the **root** directory.
3. Copy/Paste the **FOR498 Windows VM.7z** file to a **Virtual Machines** folder you have created on your host. Once the **.7z** is copied over, right click on it, and select **Open With →Keka.app**. You may be prompted to specify a location on your host to save the extracted files. If so, unzip to the **Virtual Machines** folder. In most cases, double-clicking will automatically start the unzipping to the directory where the **.7z** file is. Do NOT do this from your USB, otherwise your machine may start unzipping the **.7z** back to the USB drive.



4. The extraction process will start.

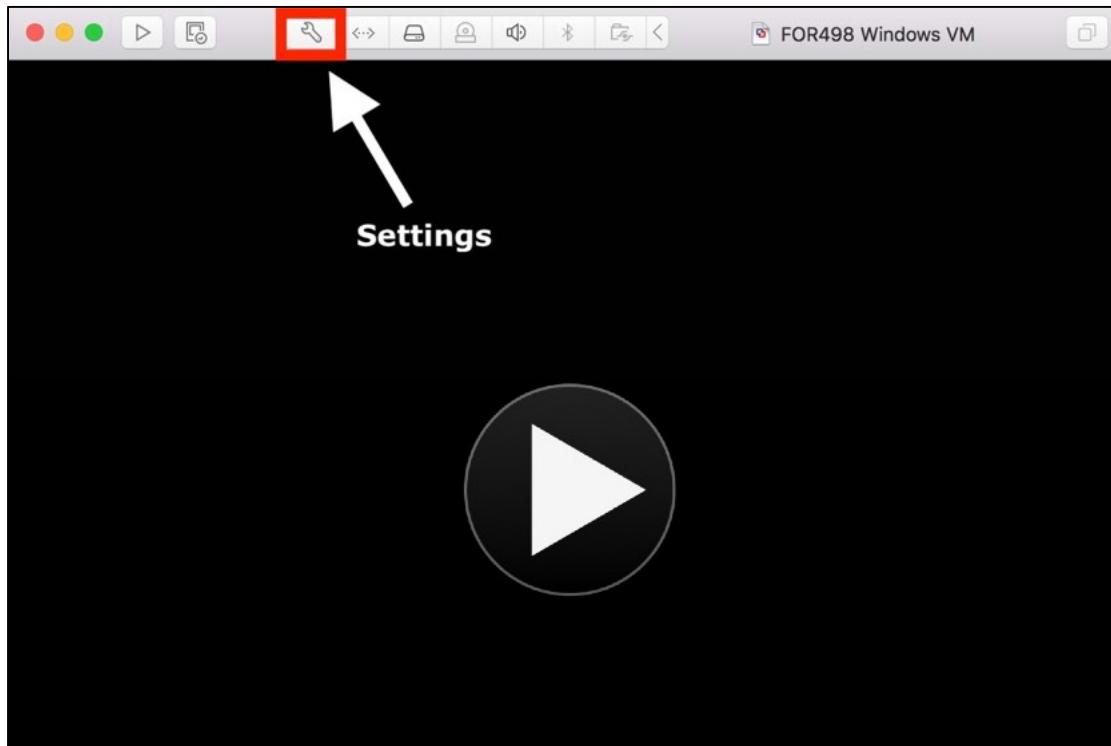


- After a long extraction process (maybe 20–45 min), you should see a new folder in your selected export folder called **FOR498 Windows VM**.
- In order to save space, you can delete the **.7z** file once the extraction process is complete.

## Part 2—Configuring the 498 Windows Virtual Machine Hardware Settings

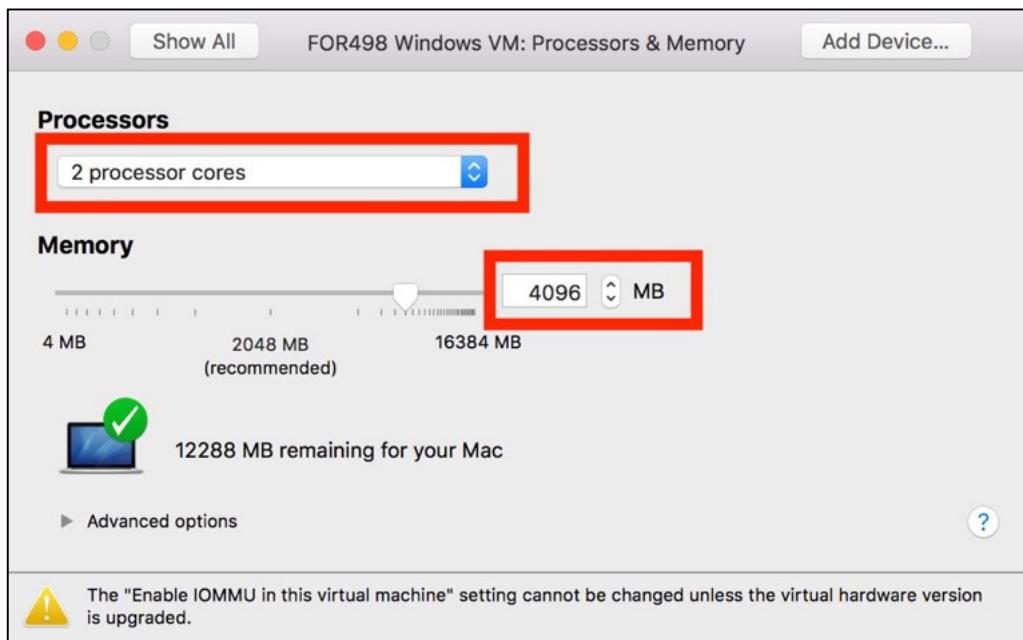
1. Start **VMware Fusion** and open (**File → Open**) the virtual machine file located in the **FOR498 Windows VM** directory called **FOR498 Windows VM.vmx**. This will load the **FOR498 Windows VM** in your **VMware** application.
2. The **FOR498 Windows VM** requires at least 4 GB of RAM. If your host system has 8 GB of RAM, do not adjust this setting. You should allocate no more than half of your host's RAM to this **VM**. If your host has more than 8 GB RAM, such as 16 or 32 GB, then the **FOR498 Windows VM** can perform better by assigning it more RAM. To do so, follow the next step.

- Choose **Settings** from the **Virtual Machine Library** for the **FOR498 Windows VM**:



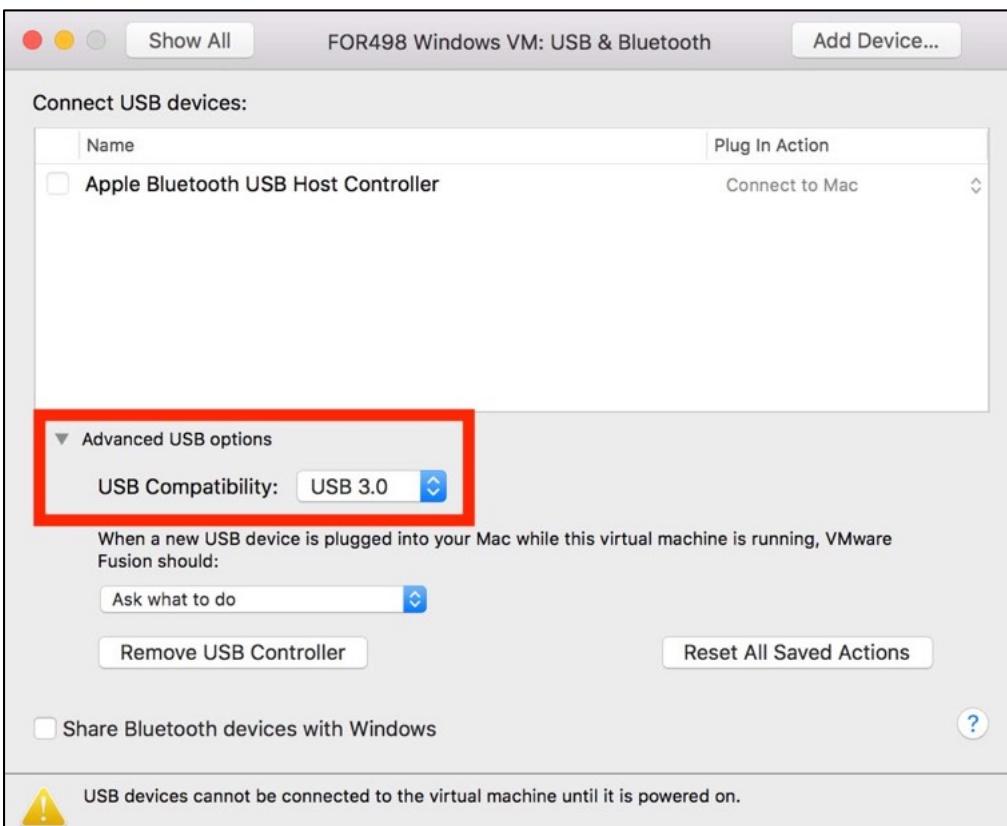
➤ Choose **Processors & Memory**. Then make the appropriate adjustments to **Memory**.

- Note: You can also adjust the number of Processors. Similar to RAM, it is not recommended to assign more than half the total number of CPU cores available on your host system.



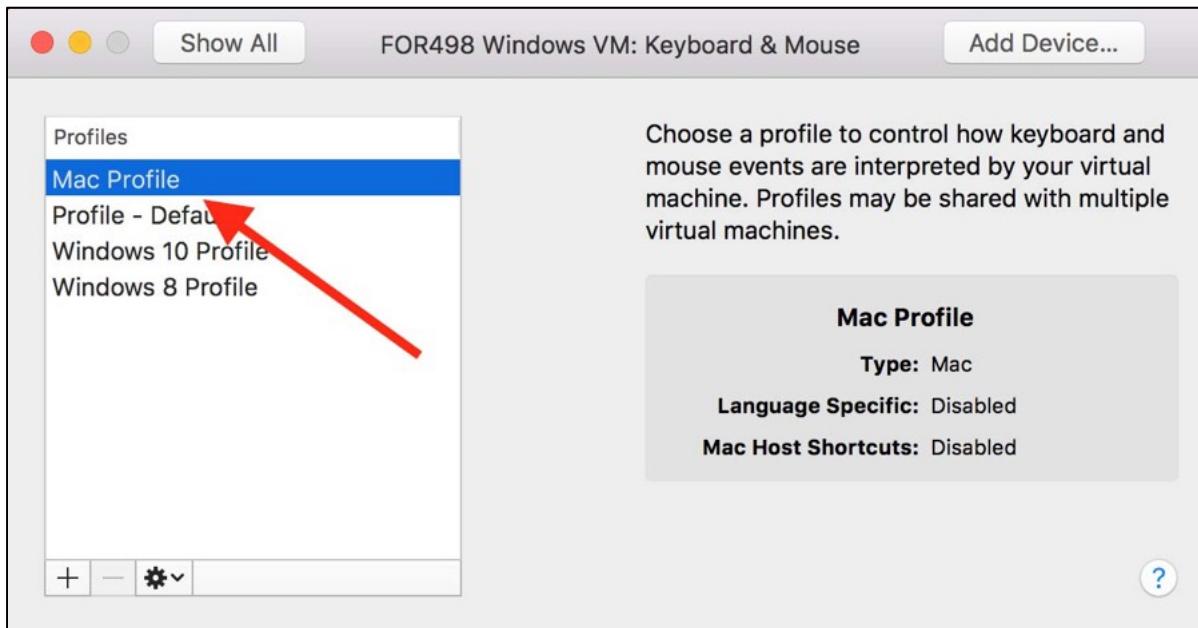
➤ Select **Show All** button at the top of the window to return to the main menu.

- Check your USB settings (select **USB & Bluetooth**). Make sure the **USB Compatibility** is set for **USB 3.0** (select this even if you don't have USB 3.0 on your system). The reason for this is that **VMware** will still attempt to copy files at a greater speed.



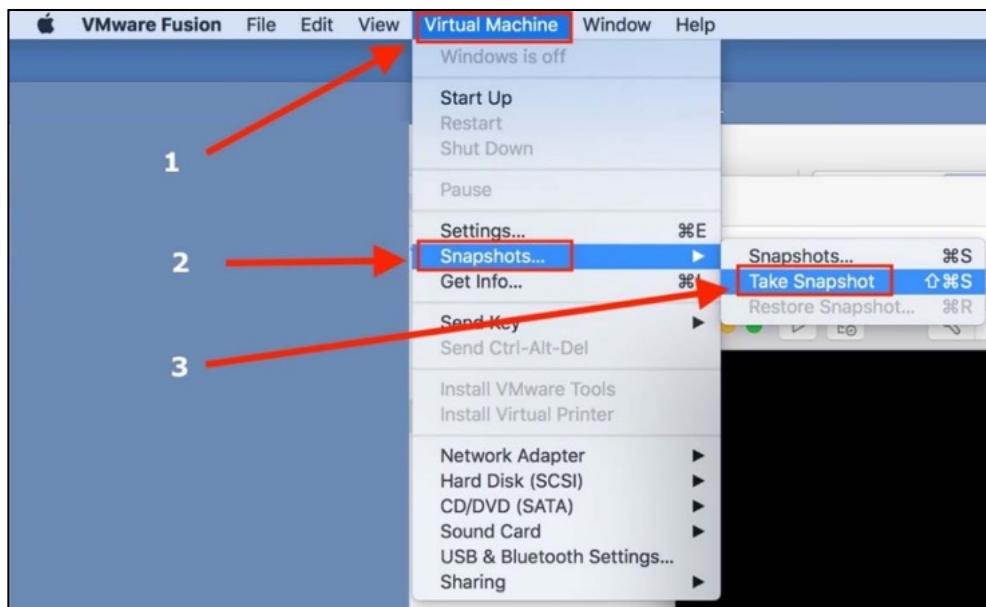
➤ Select **Show All** button at the top of the window to return to the main menu.

4. Finally, change the **Keyboard & Mouse** settings.



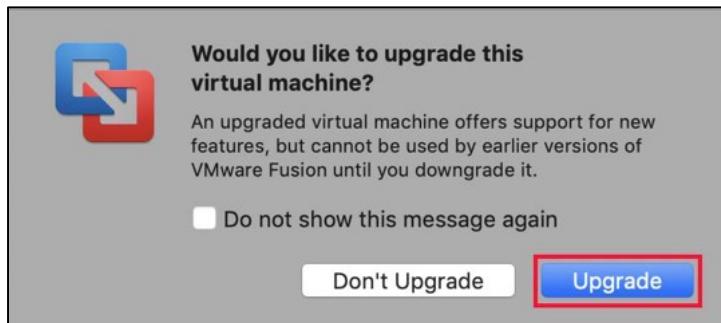
- You can now close the window.

5. Take a **Snapshot** of the current state of the virtual machine via the **Virtual Machine** → **Snapshots...** → **Take Snapshot** option. It will appear as though nothing has happened, but your snapshot has been created.

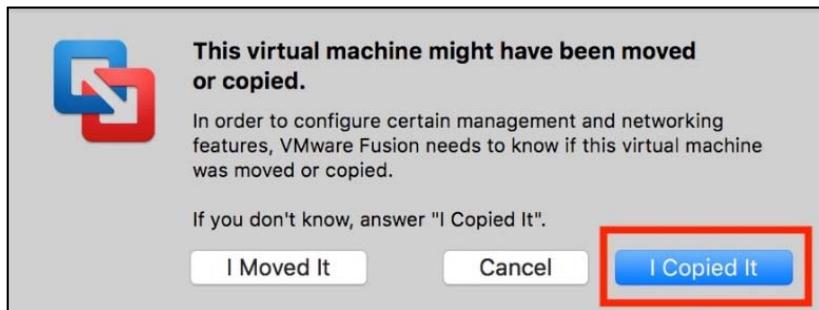


### Part 3—Running the 498 Windows Virtual Machine

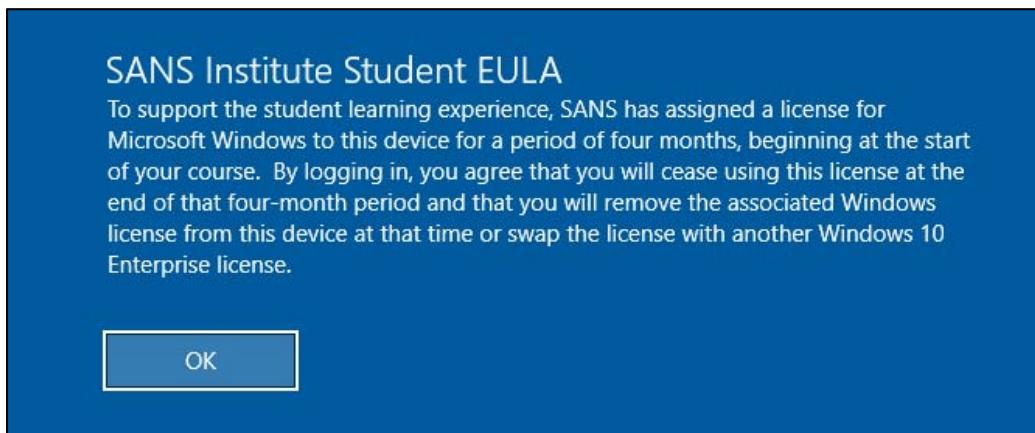
1. Power on your virtual machine. If you see any update messages, do **NOT** accept them. If prompted to “...upgrade the virtual machine”, click **Upgrade**.



2. If prompted, select “I Copied It”.



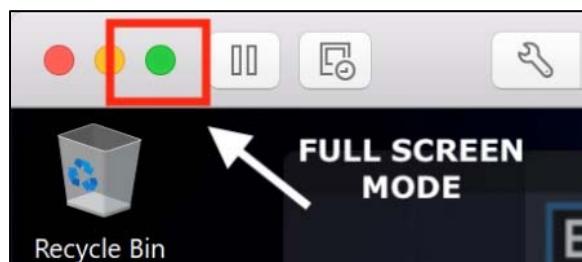
- When presented with the **SANS EULA**, read it carefully, then press **OK**



- Click anywhere on the screen to display the log in dialog. Login to the **FOR498 Windows VM** using the following credentials:
  - Username: **SANSDFIR**
  - Password: **forensics**



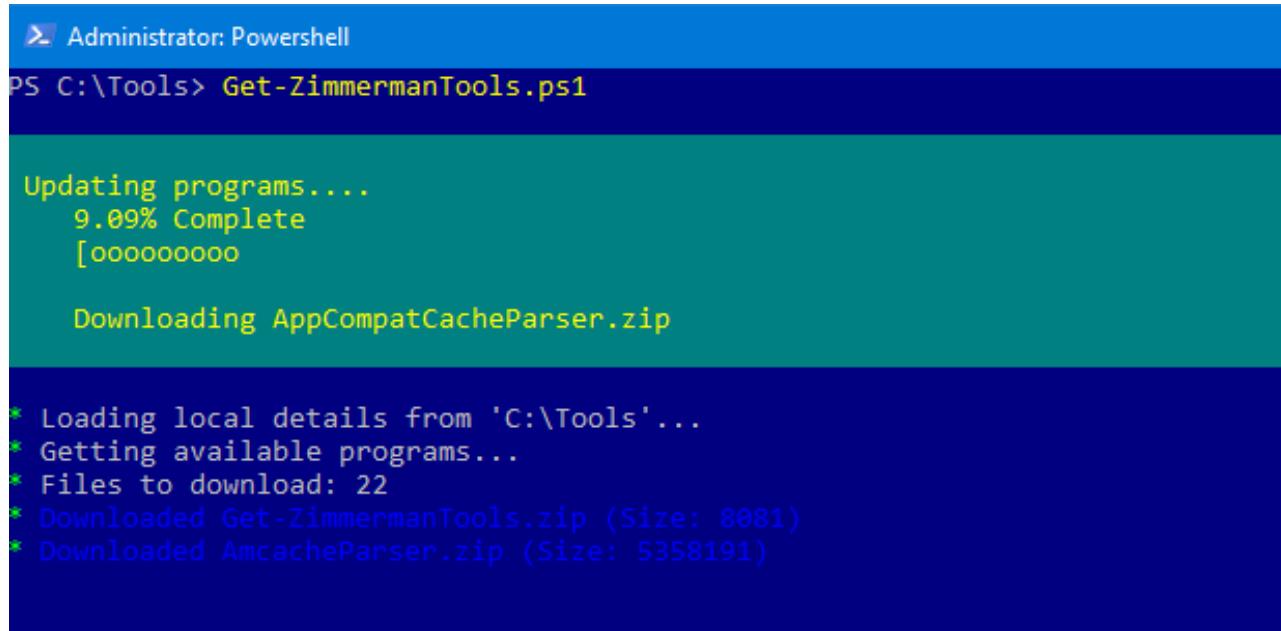
- Once logged in, you should see a standard Windows desktop with several sets of shortcuts on the **Desktop**. It is recommended to attempt to use the highest screen resolution as possible. We highly recommend that you set your display to one of the following: 1920x1080 or 1366x768. If you are comfortable with your settings as is, then don't change them.
- You will typically have the best experience in full-screen mode in **VMware**. To enter **Full Screen Mode**, simply click on the green circle on the top left corner of the window.



To exit full-screen mode, hover at the top of the screen and click to bring the **VMware** drop-down toolbar into view. You can then click the same green circle to exit **Full Screen Mode**.

7. **Update Zimmerman Tools:** Open a **PowerShell** window from the **Desktop** shortcut. Run the following command in the **PowerShell** window and **ENTER** to update all available tools to their latest versions.

```
Get-ZimmermanTools.ps1
```



```
Administrator: Powershell
PS C:\Tools> Get-ZimmermanTools.ps1

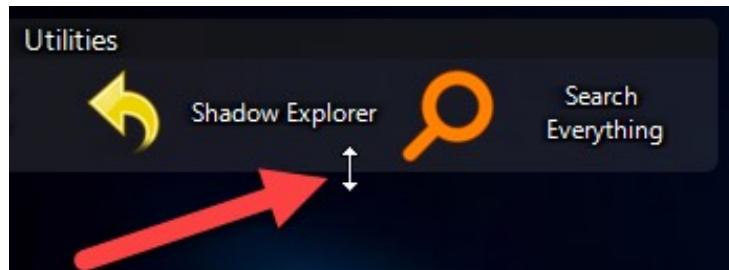
Updating programs....
 9.09% Complete
 [oooooooooo

Downloading AppCompatCacheParser.zip

* Loading local details from 'C:\Tools'...
* Getting available programs...
* Files to download: 22
* Downloaded Get-ZimmermanTools.zip (Size: 8081)
* Downloaded AmcacheParser.zip (Size: 5358191)
```

You can also simply right-click on the script on your **Desktop** entitled **Update Zimmerman Tools** and choose **Run with PowerShell** from the context menu.

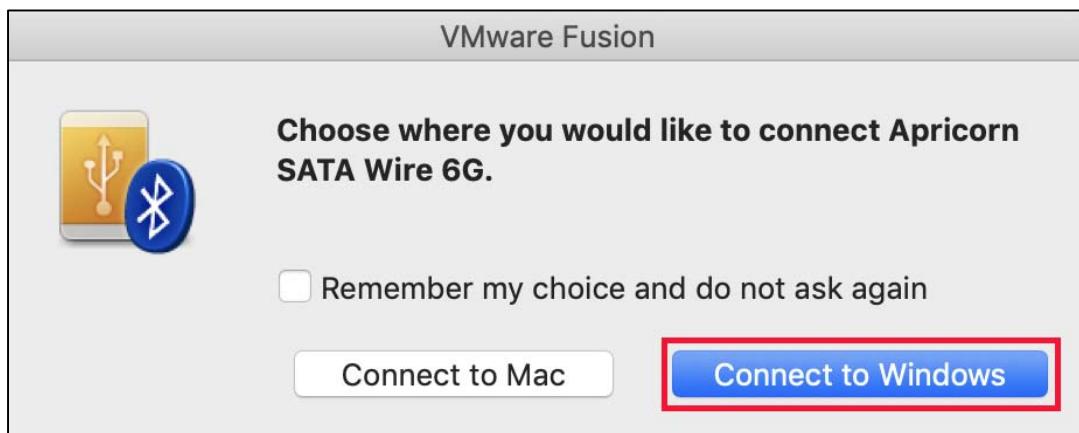
8. The **Desktop** contains several groups of icons, such as **Utilities** and **Network Tools**. Occasionally these groups are not big enough to show all of the icons in the group. For each of the groups on the **Desktop**, rearrange and resize the groups so all the shortcuts are visible. To resize a group, move the mouse to the bottom or side of the group until the cursor changes, as shown below. Then drag the group to make it bigger.



To move a group, click and drag on the group name, then move the group as needed.

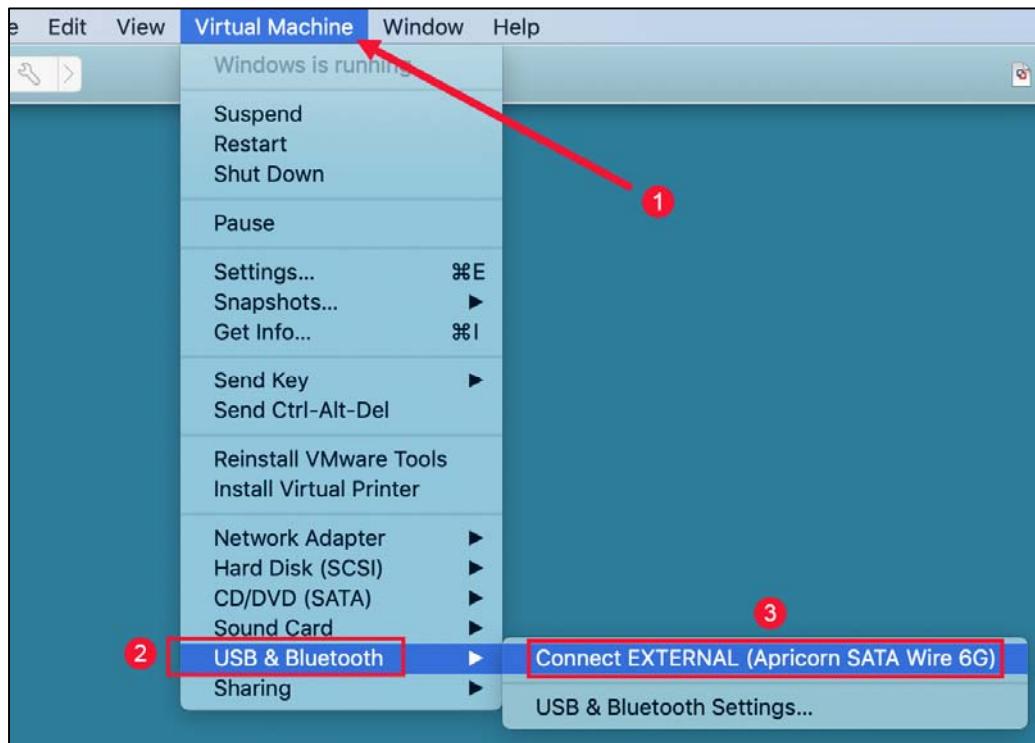


9. Connect the SANS provided SATA to USB adapter to the student provided hard drive, then connect it to your host computer.
10. When you plug your device in, VMWare may offer to connect it to the VM. If it does, connect the external hard drive to the VM (**Connect to Windows**).

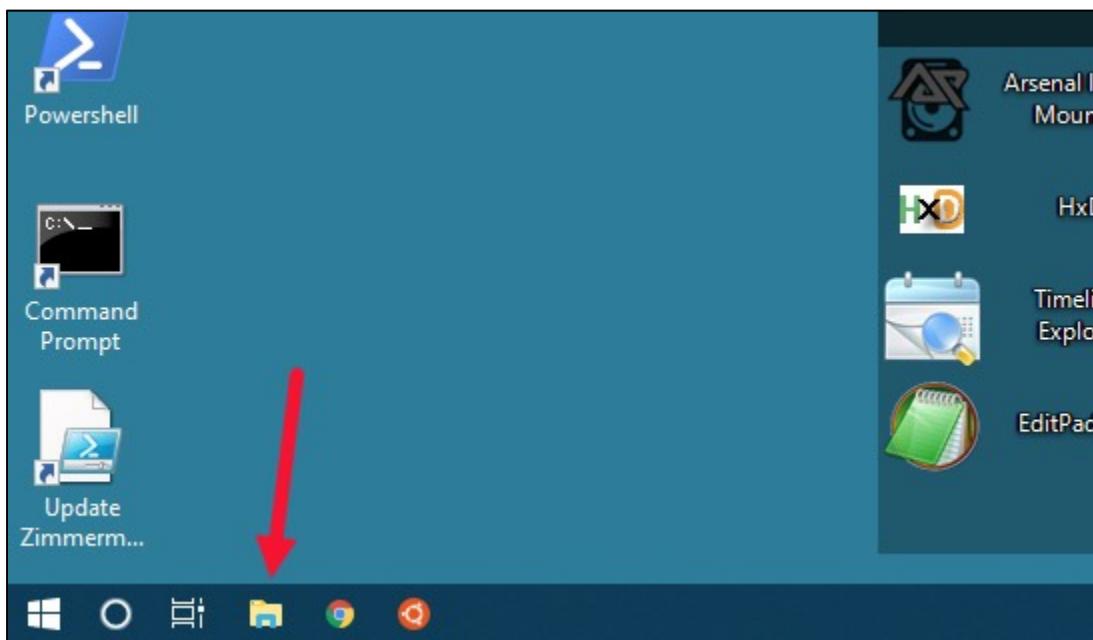


11. If you are not prompted as above, connect the drive to the VM manually via **Virtual Machine → USB & Bluetooth → Connect <Device name>**.

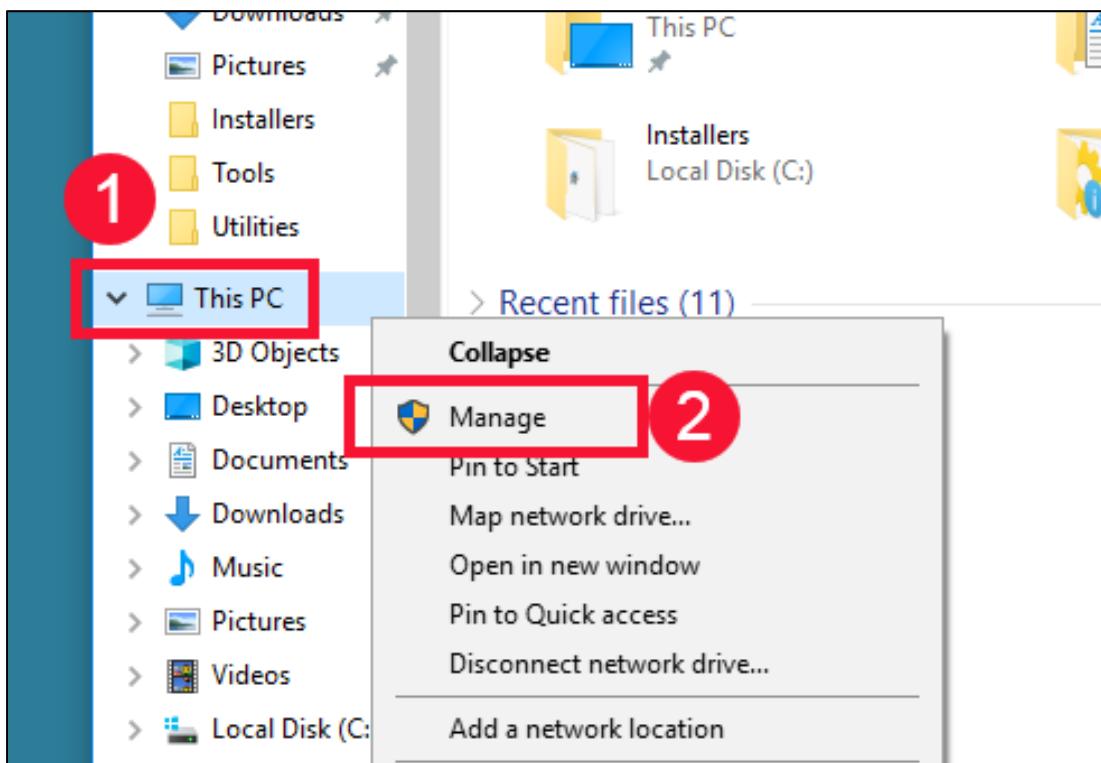
- You will of course have to find the appropriate device to connect (an Apricorn SATA Wire 6G named EXTERNAL is shown in the example below).



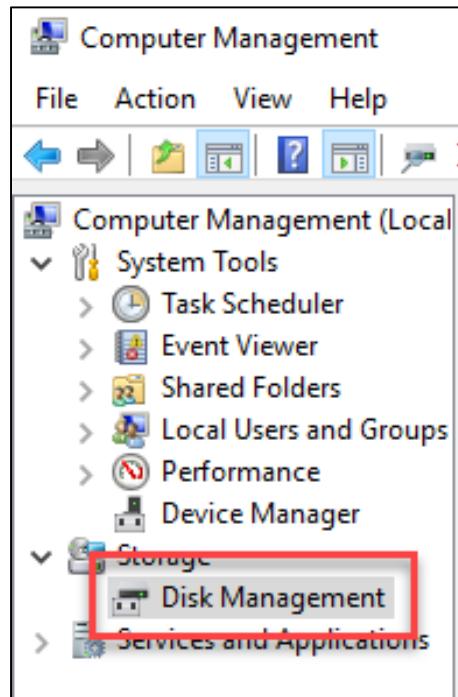
12. In the **FOR498 Windows VM**, start **File Explorer**...



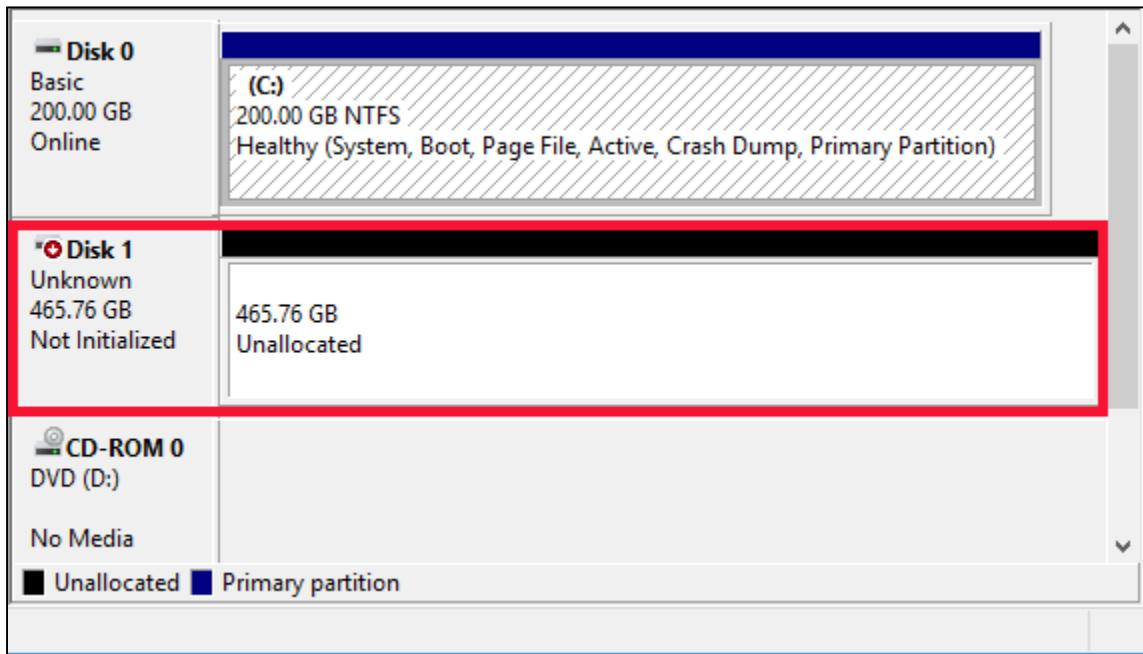
13. ...then right-click on This PC and chose Manage.



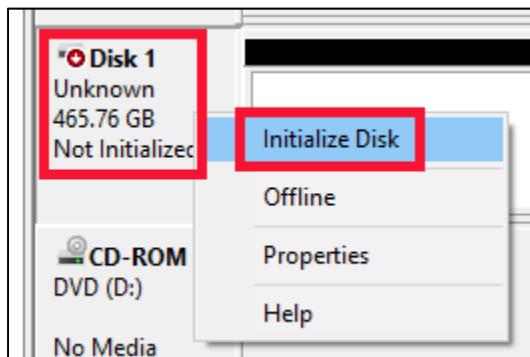
14. Click Disk Management.



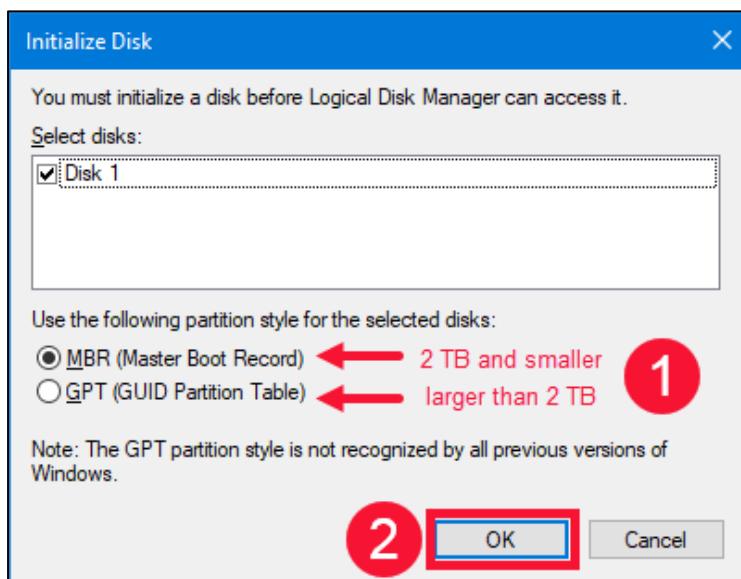
15. Find the device you just connected in the list of devices shown. You will see one of two things, depending on the format status of your hard drive. If your hard drive is brand new and/or is not formatted, you will see the highlighted item below. Depending on your hard drive, its size will not be the same as the size below. If your **Disk** does not say “**Unallocated**”, proceed to **step 19**.



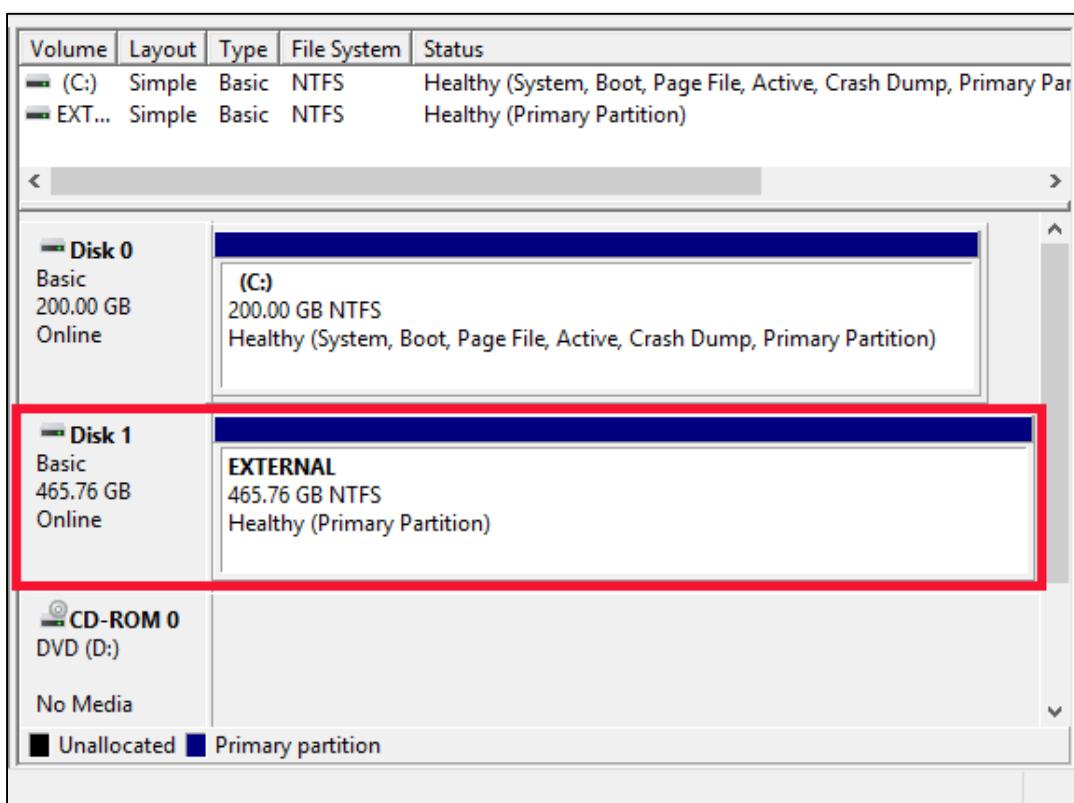
16. Right click on **Disk 1** (your disk may be a different number) and select **Initialize Disk** from the drop-down menu.



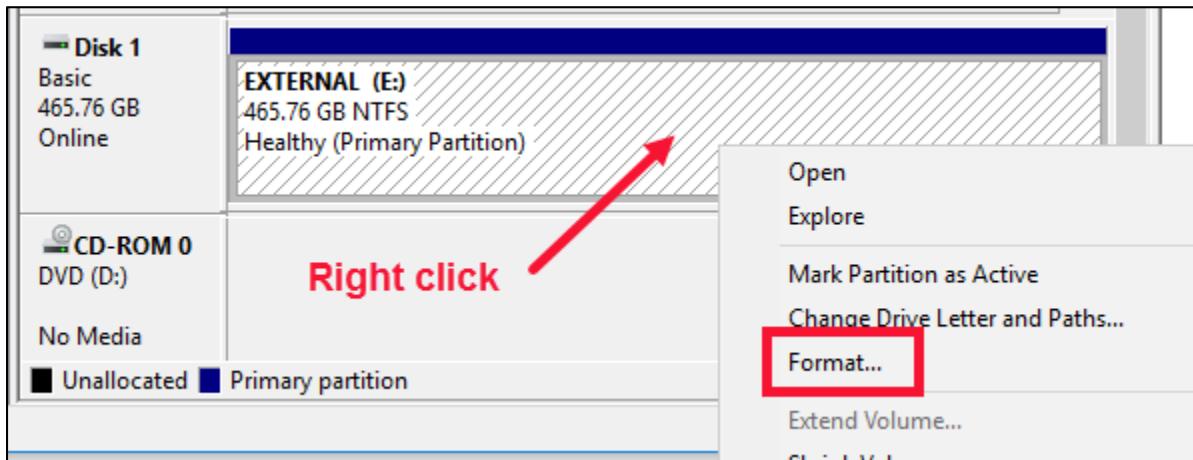
17. You will be presented with the **Initialize Disk** box. Your disk should be selected. If your disk is 2 TB or smaller in size, select **MBR**. If your disk is larger than 2 TB, select **GPT**. Then click **OK**. In fact, you may be presented with this box during **step 16**. Deal with it in the same way.



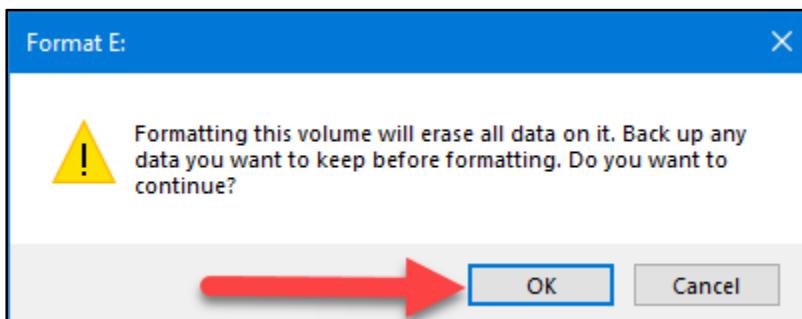
18. The **Disk 1** box will no longer have the red and white arrow originally seen. At this point, proceed to **step 20**. Although your drive is still indicated as **Unallocated**, follow the same steps as in **step 20**.
19. If your hard drive is currently formatted, you will see the highlighted item below (probably with a different name). Depending on your hard drive, its size will not be the same as the size below.



20. Right-click on the device, then choose **Format** from the context menu. If your drive is not formatted, you will not see the below. In that case, proceed to step 25.



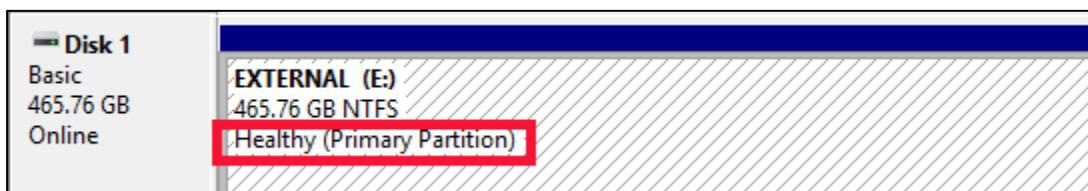
21. When prompted about erasing the data, click **OK**.



22. As the drive is being formatted, the device will show “**Formatting**” as seen below.

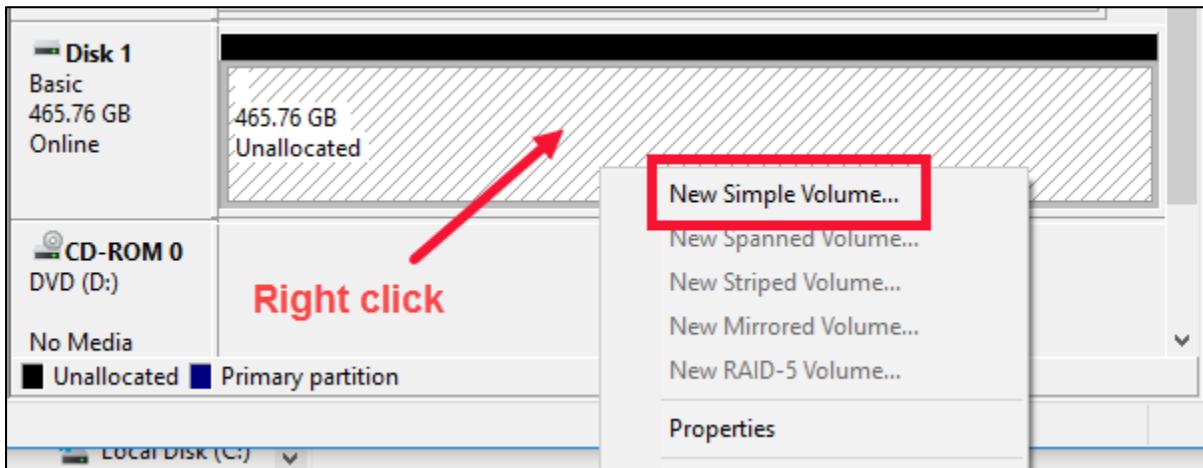


23. When the format is finished, the drive’s status will show the drive as **Healthy**.

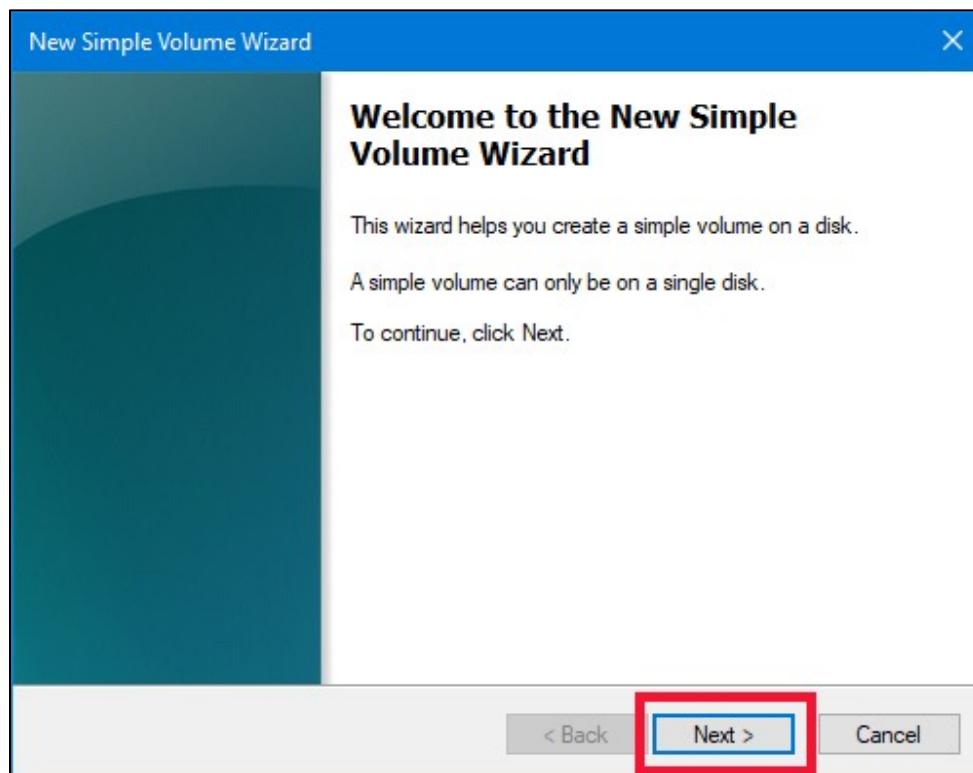


24. You can now properly eject your external hard drive, and power down your **FOR498 Windows VM**. If you don’t, the next exercise part (**Part 4**) may take longer. Proceed to **Part 4**.

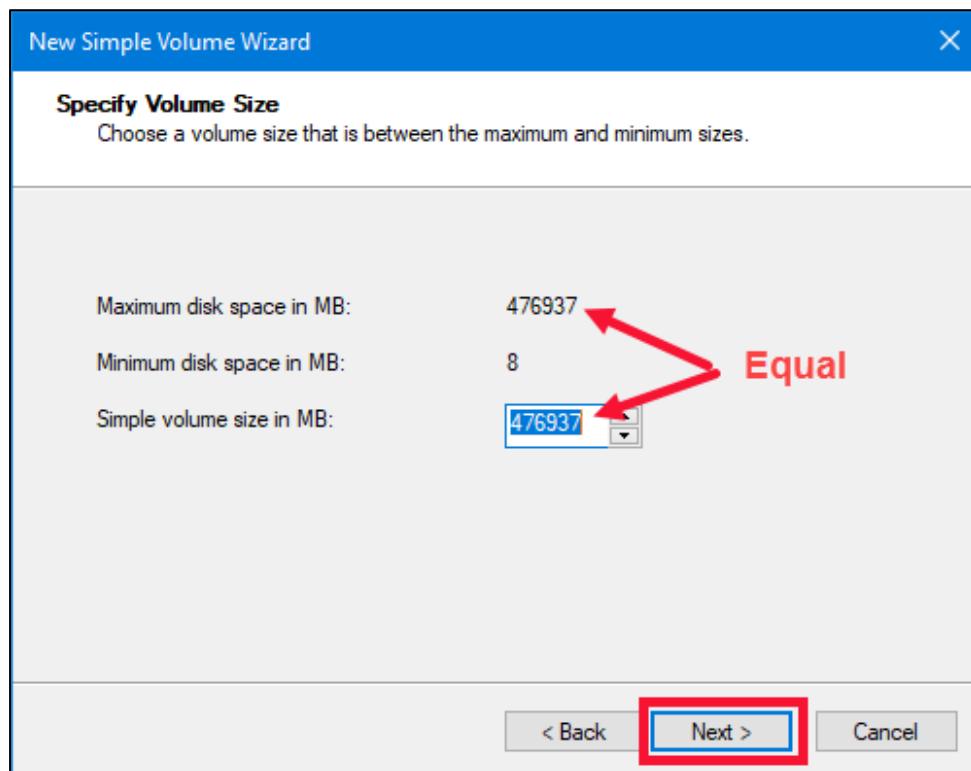
25. If your drive is not formatted, you will see the below. In this case, right click on the device and choose New Simple Volume from the context menu.



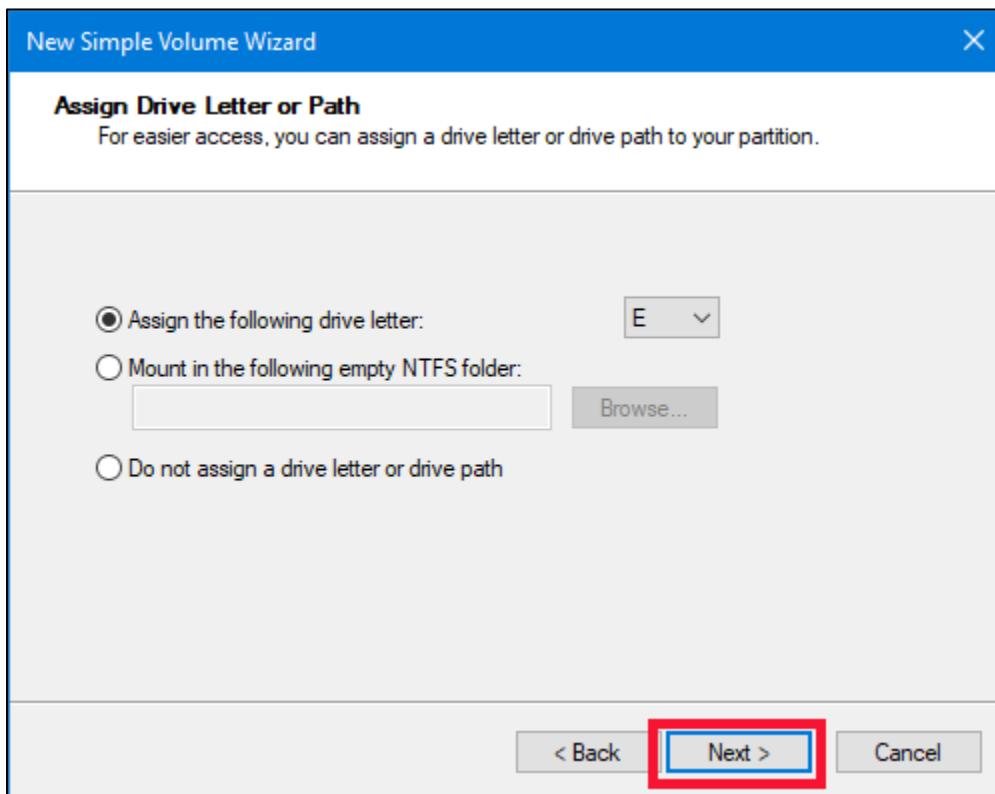
26. The **New Simple Volume Wizard** will start. Click **Next**.



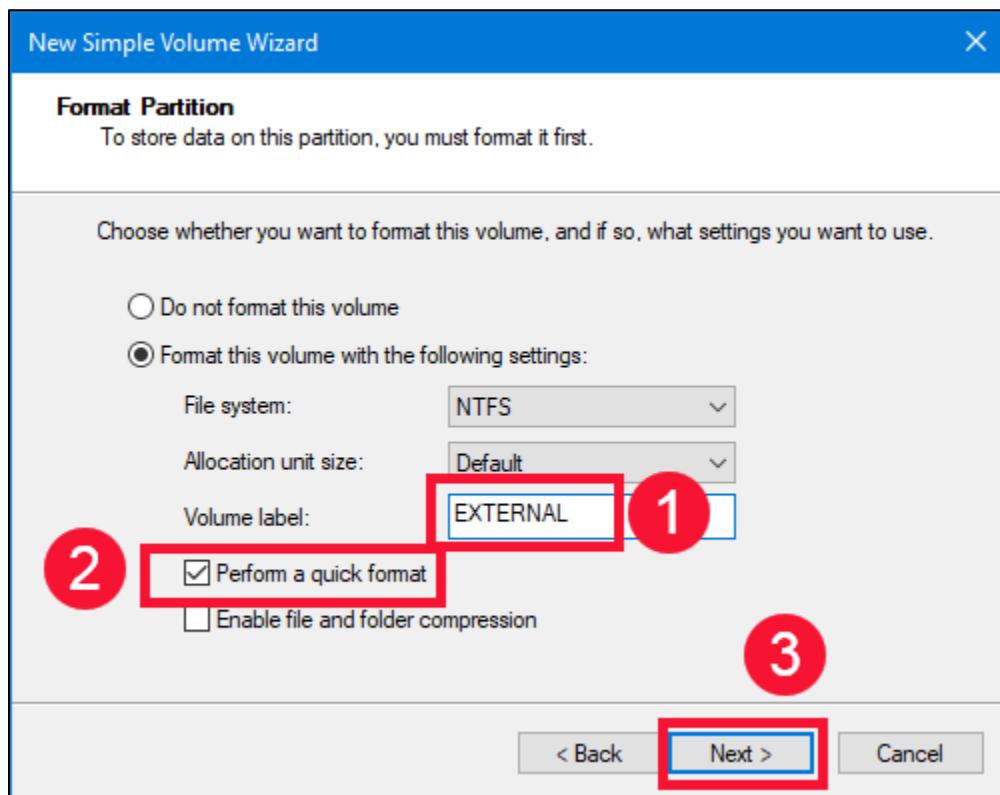
27. In the **Specify Volume Size** box, ensure that the **Maximum disk space** and the **Simple volume size** are equal, and then click **Next**.



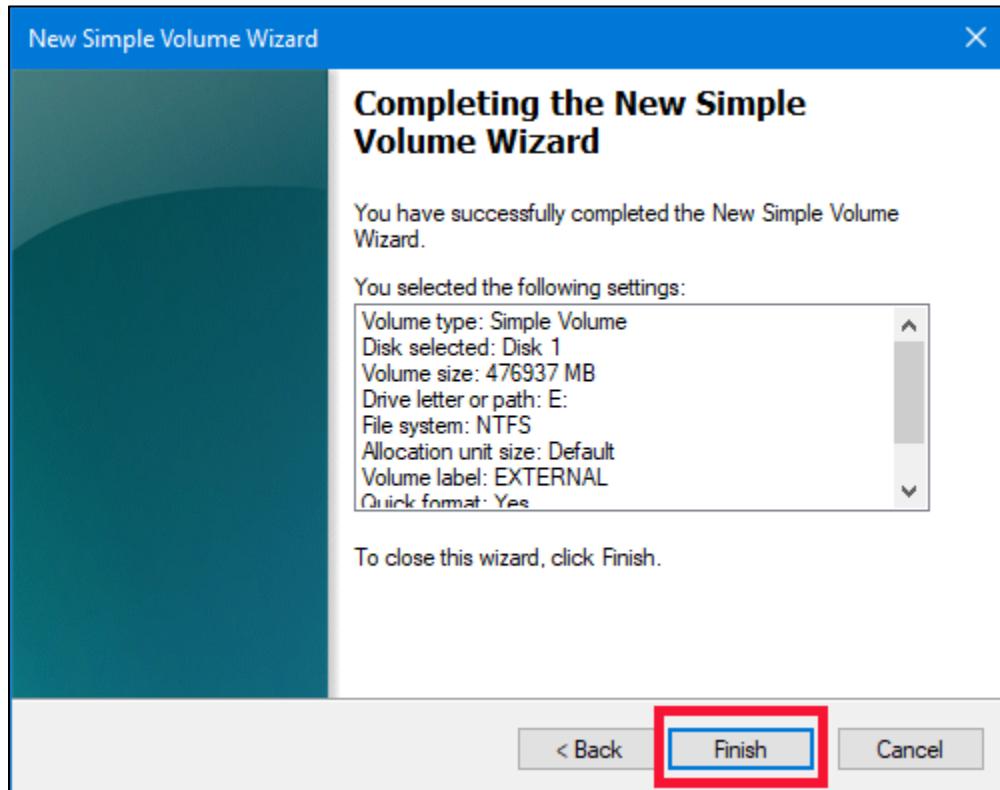
28. The **Assign Drive Letter or Path** box will appear. Accept all defaults and click **Next**.



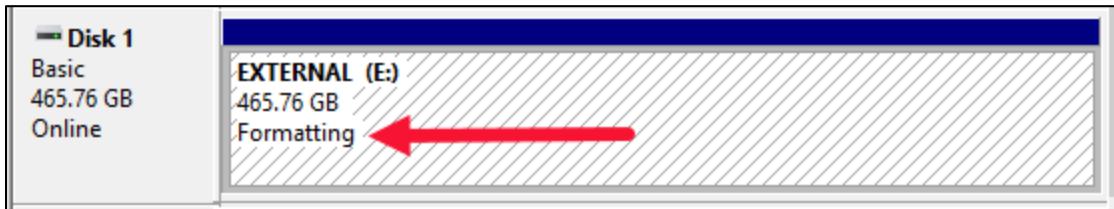
29. In the **Format Partition** box, change the **Volume label** to **EXTERNAL**. Ensure that the **Perform a quick format** box is checked. Click **Next**.



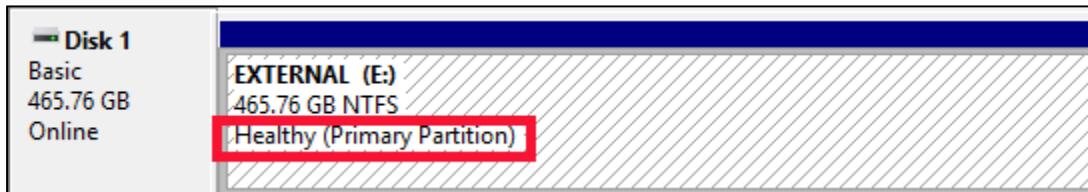
30. A box summarizing your chosen settings will be shown. Click **Finish**.



31. As the drive is being formatted, the device will show “Formatting” as seen below.



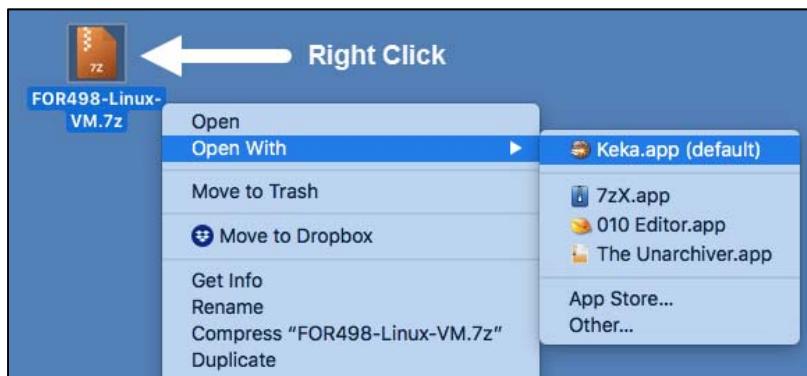
32. When the format is finished, the drive's status will show the drive as **Healthy**.



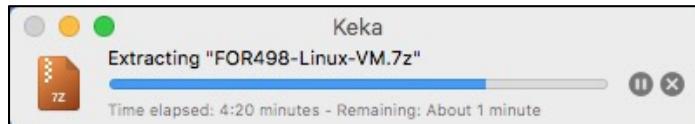
33. You can now properly eject your external hard drive, and power down your **FOR498 Windows VM**. If you don't, the next exercise part (**Part 4**) may take longer.

#### **Part 4—Unzipping the 498 Linux Virtual Machine**

1. Insert the **FOR498 USB B** into your host system. You will receive the **FOR498 USB B** by the first day of the course, if you do not have it now. Please wait until you receive the USB keys before configuring your system.
2. On the USB, browse to the **root** directory.
5. Copy/Paste the **FOR498 Linux VM.7z** file to a **Virtual Machines** folder you have created on your host. Once the **.7z** is copied over, right click on it, and select **Open With →Keka.app**. You may be prompted to specify a location on your host to save the extracted files. If so, unzip to the **Virtual Machines** folder. In most cases, double-clicking will automatically start the unzipping to the directory where the **.7z** file is. Do NOT do this from your USB, otherwise your machine may start unzipping the **.7z** back to the USB drive.



3. The extraction process will start.

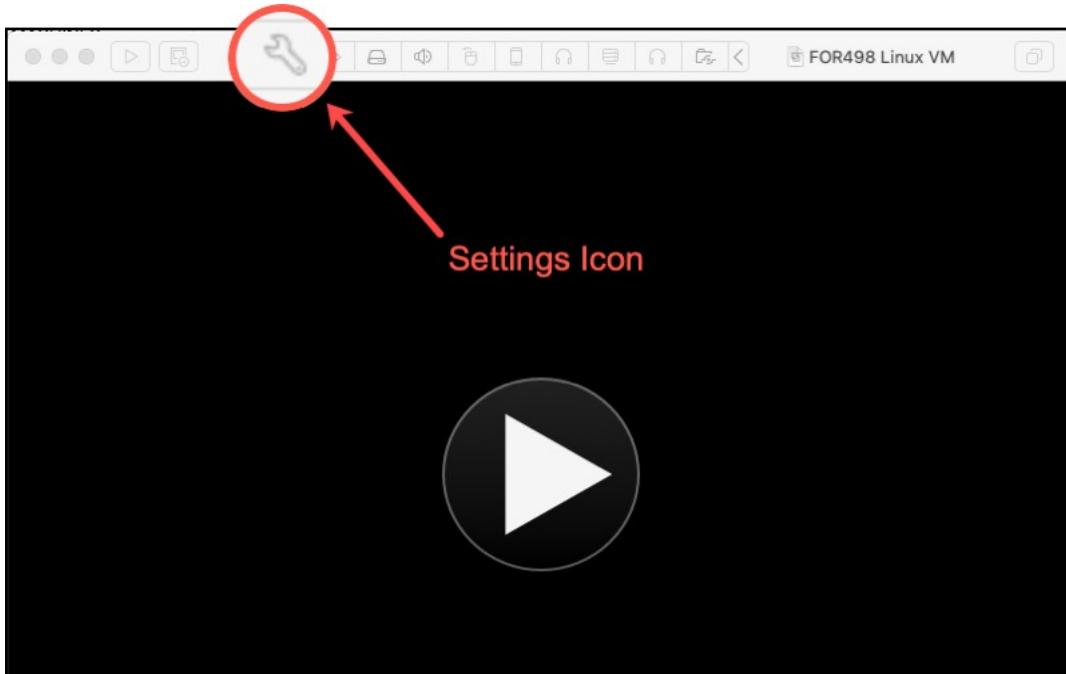


- After the extraction process (maybe 5–10 min), you should see a new folder in your selected export folder called **FOR498 Linux VM**.
- In order to save space, you can delete the **.7z** file once the extraction process is complete.

## Part 5—Configuring the 498 Linux Virtual Machine

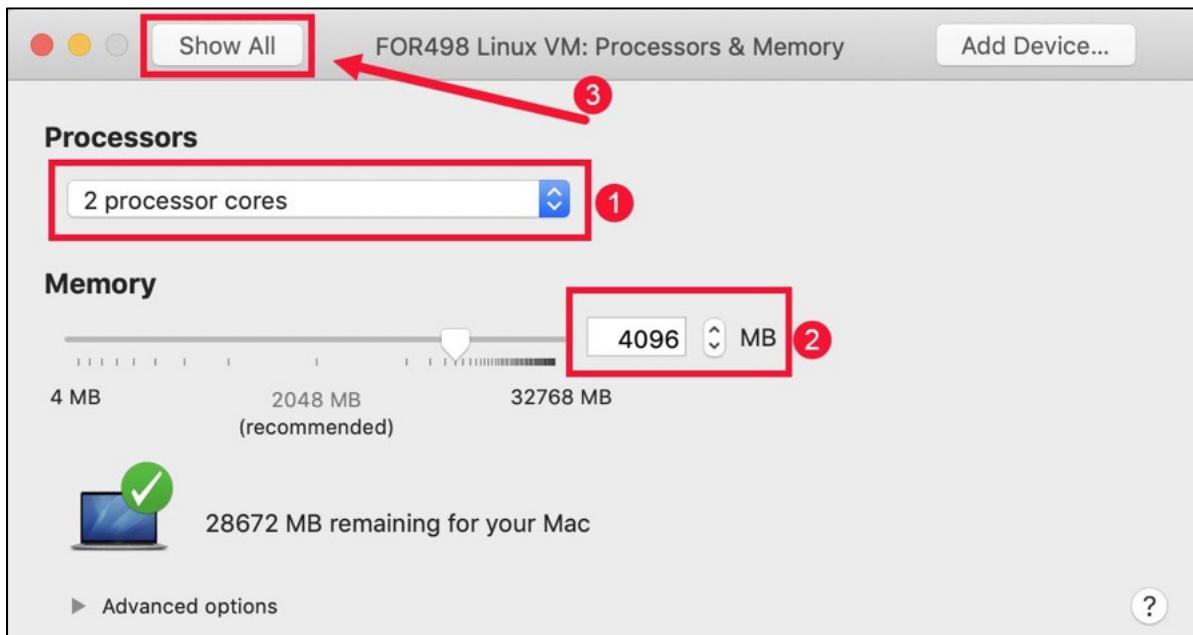
1. Start VMware Fusion and open (**File → Open**) the virtual machine file located in the **FOR498 Linux VM** directory called **FOR498 Linux VM.vmx**. This will load the **FOR498 Linux VM** in your **VMware** application.
2. The **FOR498 Linux VM** requires at least 4 GB of RAM. If your host system has 8 GB of RAM, do not adjust this setting. You should allocate no more than half of your host's RAM to this **VM**. If your host has more than 8 GB RAM, such as 16 or 32 GB, then the **FOR498 Linux VM** can perform better by assigning it more RAM. To do so, follow the next step.

- Choose **Settings** from the Virtual Machine Library for the **FOR498 Linux VM**:

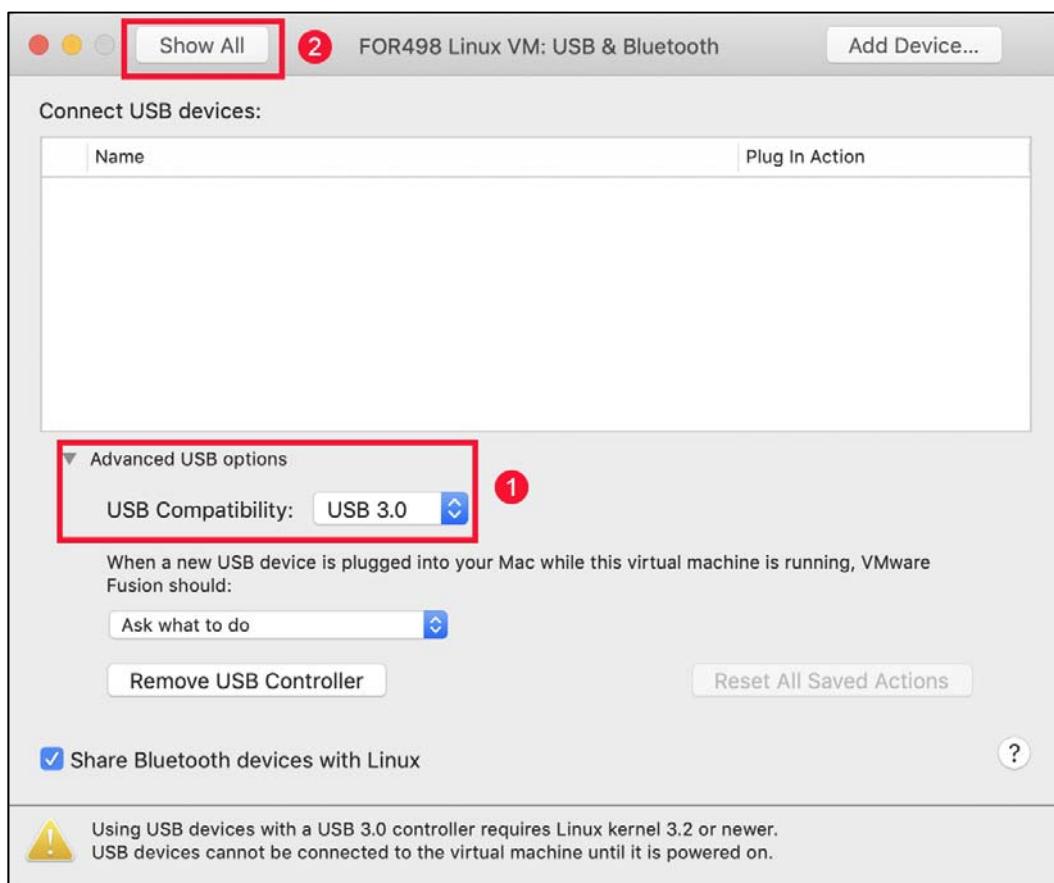


➤ Choose **Processors & Memory**. Then make the appropriate adjustments to **Memory**.

- Note: You can also adjust the number of **Processors**. Similar to RAM, it is not recommended to assign more than half the total number of CPU cores available on your host system.

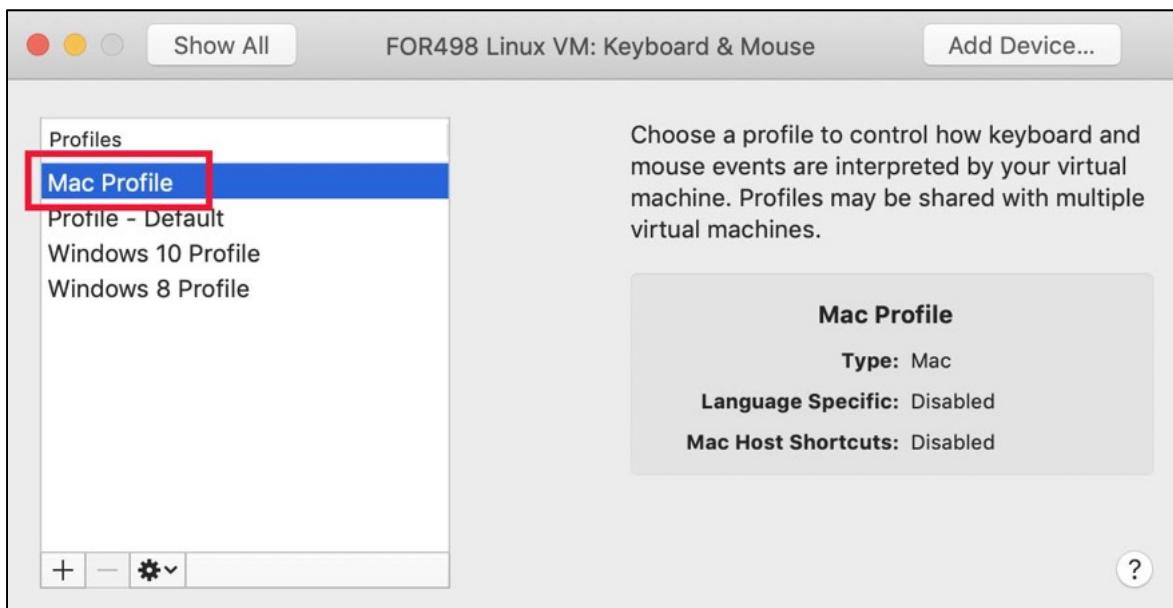


- Check your USB settings (select **USB & Bluetooth**). Make sure the **USB Compatibility** is set for **USB 3.0** (select this even if you don't have USB 3.0 on your system). The reason for this is that **VMware** will still attempt to copy files at a greater speed.



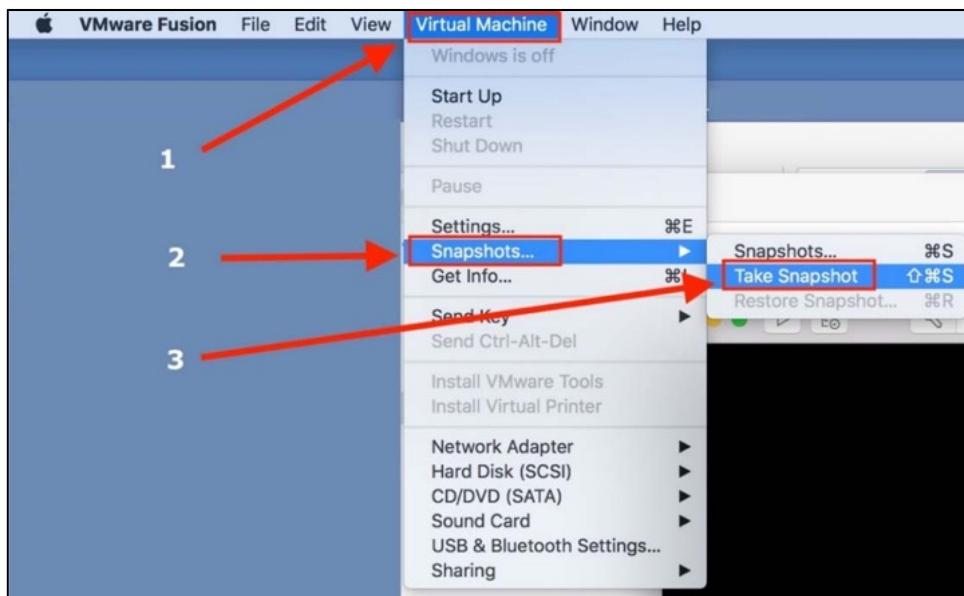
### **VMware Fusion – USB Compatibility to USB 3.0**

4. Finally, change the **Keyboard & Mouse** settings.



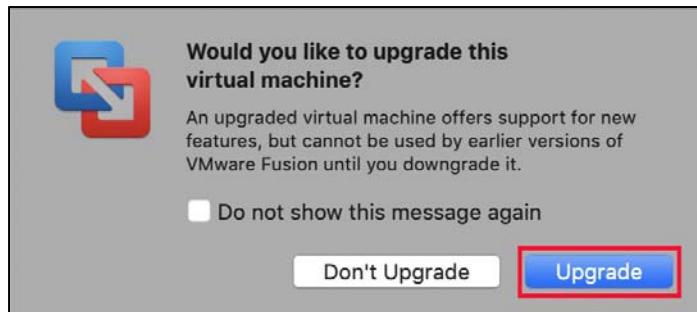
- You can now close the window.

- Take a **Snapshot** of the current state of the virtual machine via the **Virtual Machine** → **Snapshots...** → **Take Snapshot** option. It will appear as though nothing has happened, but your snapshot has been created.

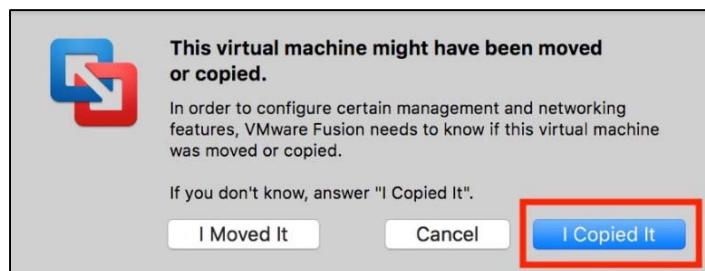


#### Part 6—Running the 498 Linux Virtual Machine

- Power on your virtual machine. If you see any update messages, do NOT accept them. If prompted to "...upgrade the virtual machine", click **Upgrade**.



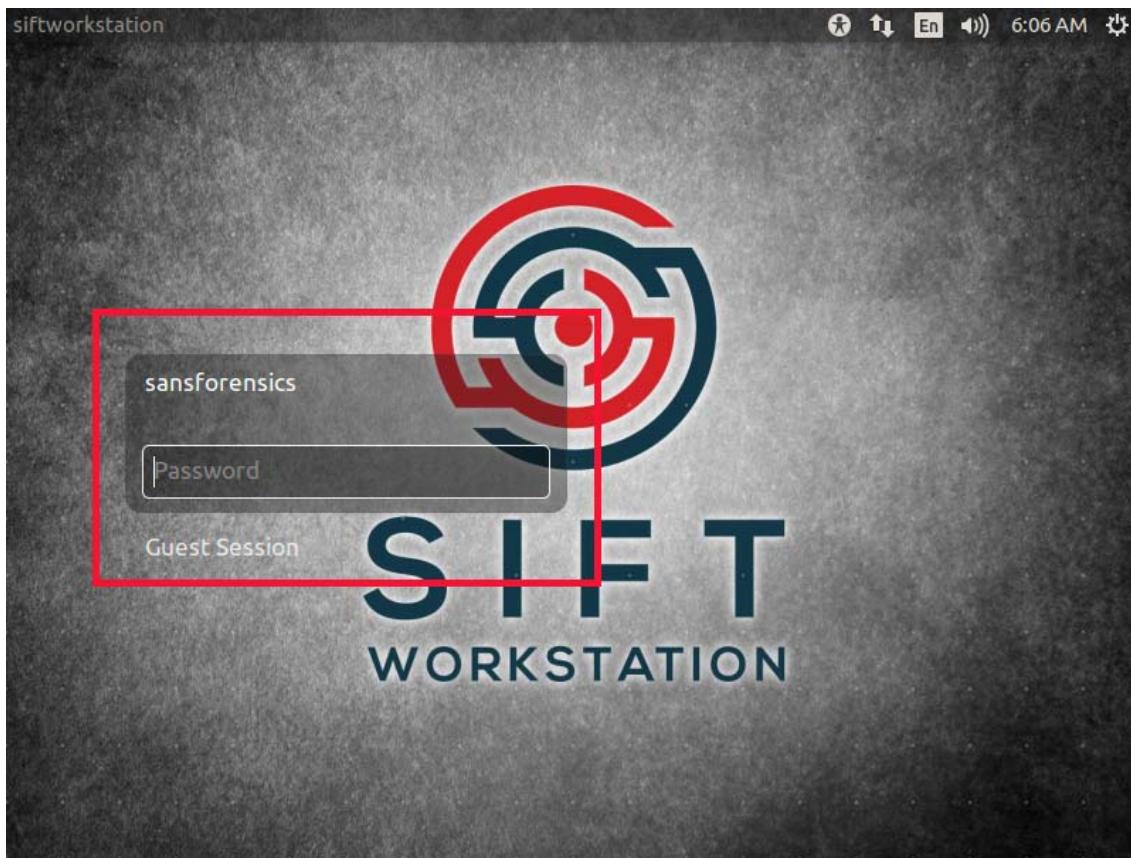
- If prompted, select "**I Copied It**".



- After initiating the startup of the **VM**, you will see the login screen appear, prompting for credentials.

4. Login to the **FOR498 Linux VM** using the following credentials:

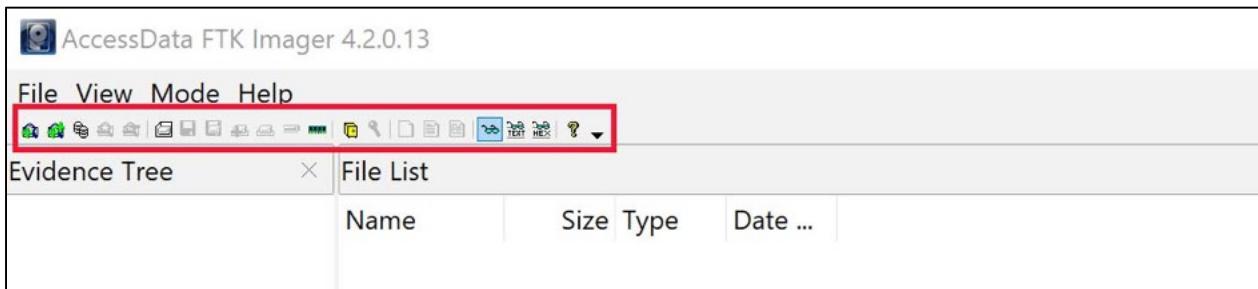
- a. Username: sansforensics
- b. Password: forensics



#### **Part 7—DPI Scaling Issues**

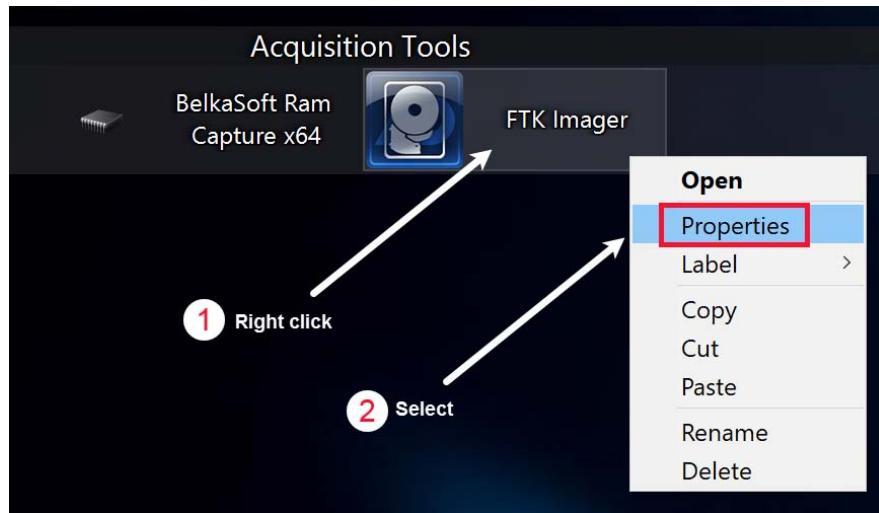
**This Part of the exercise will not apply to every student.**

Notwithstanding the resolution size issues of a given **Desktop** on a given system, there is an extra issue that presents itself frequently with laptops containing Hi-res, or 4K screens. The issue leads to programs opening in **VMs** with less than optimal resolution. For example, in the **FOR498 Windows VM**, the icons in the tool bar may be so small as to be unusable or unreadable, as seen in the example below.

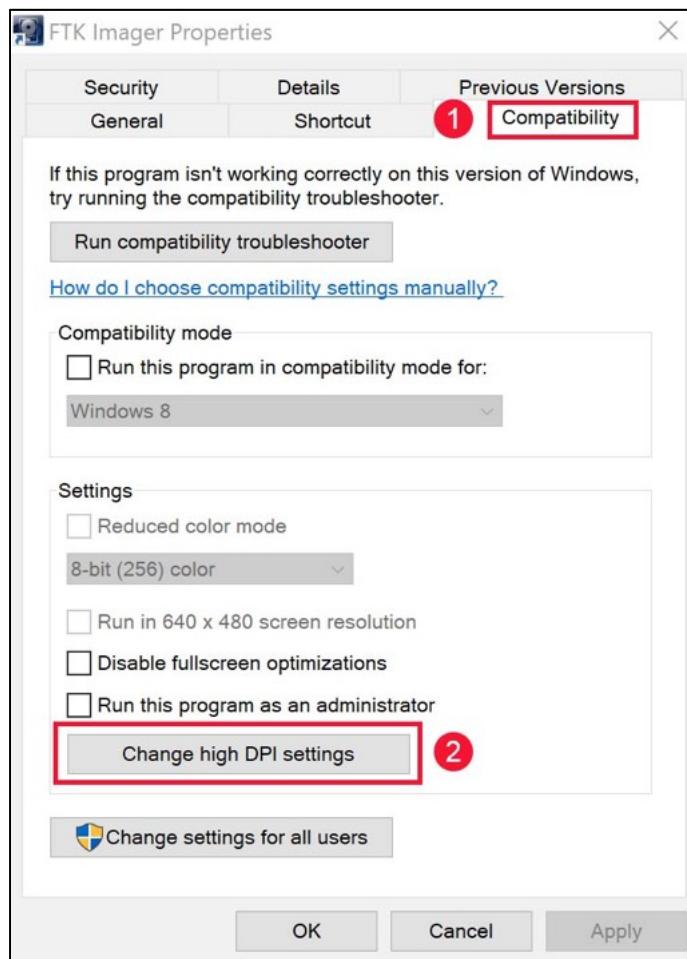


If this is the case, follow these steps:

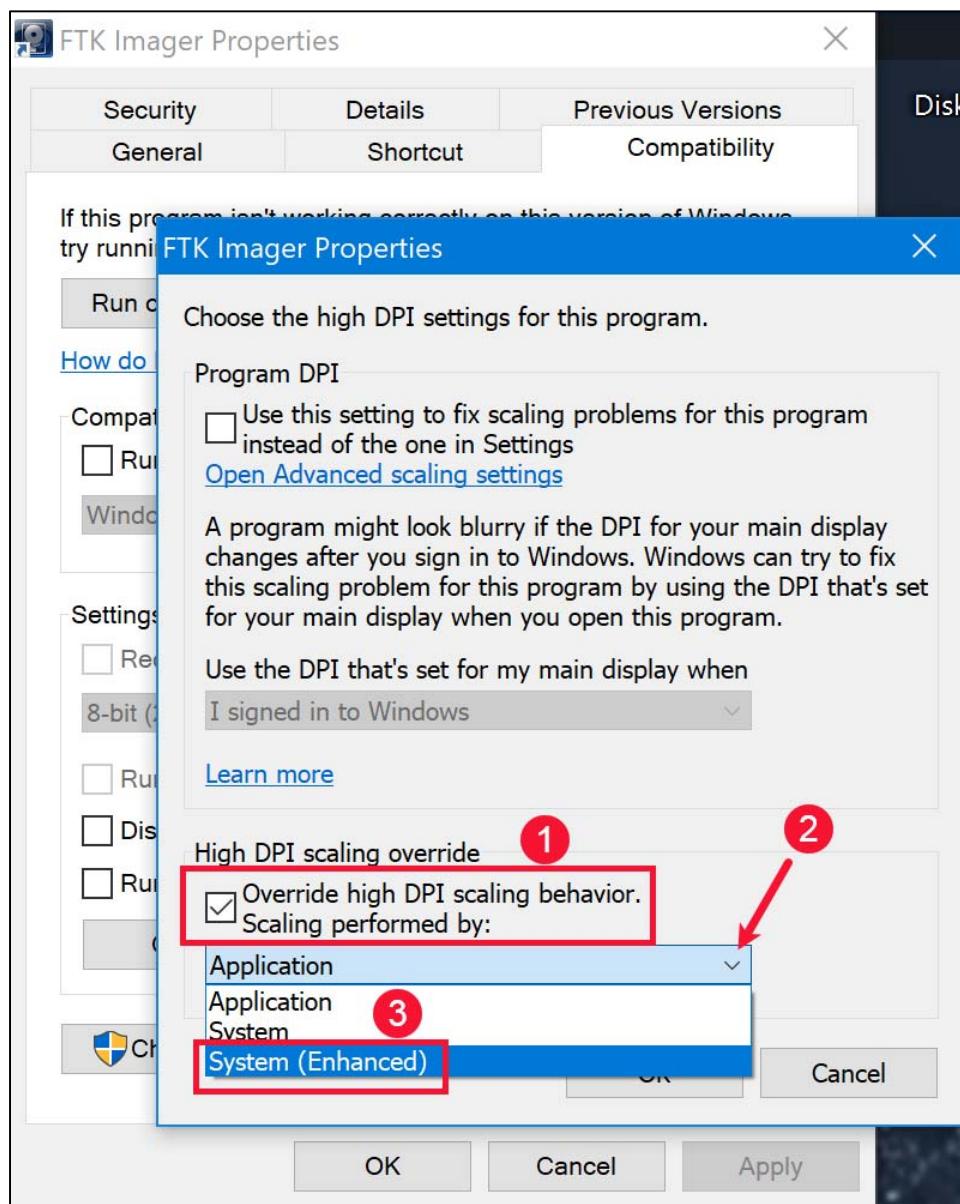
1. Close the program that is open, and then right click on the icon and select **Properties** from the drop-down menu.



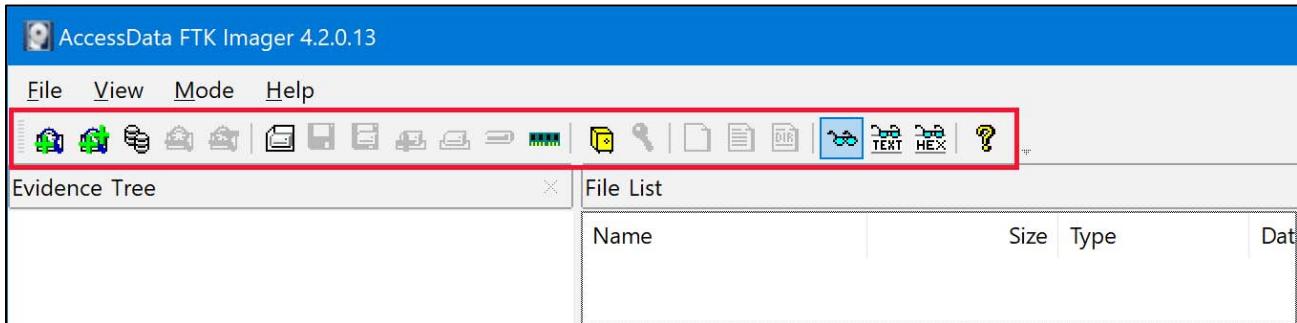
2. In the program **Properties**, a number of tabs will be visible. Click on the **Compatibility** tab, and then click on the **Change high DPI settings** button.



- Another box will open. Place a checkmark in the box titled **Override high DPI scaling behavior**. Scaling performed by.. Click the arrow for the drop-down menu and select **System (Enhanced)**. Click **OK**, and then click **OK** again to be taken back to the **Desktop**.



- Open the program again and the toolbar and other resolution issues should be solved.



# © SANS Institute 2020

## Exercise 1.1—Booting an Evidence File

### Background

Although the focus of this course is built around the notion of “...from seizure to actionable intelligence in 90 minutes or less...”, this does not mean that we will never again be dealing with evidence files. In many cases, you will be handed an E01 file and be told to extract this or that type of data quickly.

It is certainly easy to ask for data, but a great deal of data cannot be extracted from a “dead box” forensic image, such as file-less malware. Unless the system is running, nothing is detectable (or is certainly much more difficult to detect). Chat messages, contact lists, social media artifacts, and desktop notes are significantly quicker to extract from a running machine, than from a forensic image. In fact, something like a Quickbooks Audit Log cannot even be created, much less extracted, from an image.

To extract the data from within a forensic image (and hopefully have the proper tools to render it to an understandable and usable state) is one thing. To see it as it was meant to operate, without the abstraction of separate software meant to interpret it, is priceless.

Instead of spending significant time trying to coax the right data out of the evidence file, let’s just quickly create an environment where we can introduce the evidence file to virtualization software, and boot the image as though we were sitting at the user’s computer!

**xmount** is an open source tool that can be used to mount a forensic image, in this case an E01 evidence file, as a VMware virtual disk (VMDK). There is no conversion of the E01 image required. **xmount** can render an E01 into a fully functional VMDK in seconds.

In this exercise, we will use a Linux VM, **xmount** and VMware player to boot the evidence file as though it were a functioning computer, which enables us to see its contents and how they behave in the same manner that the user would have.

### Objectives

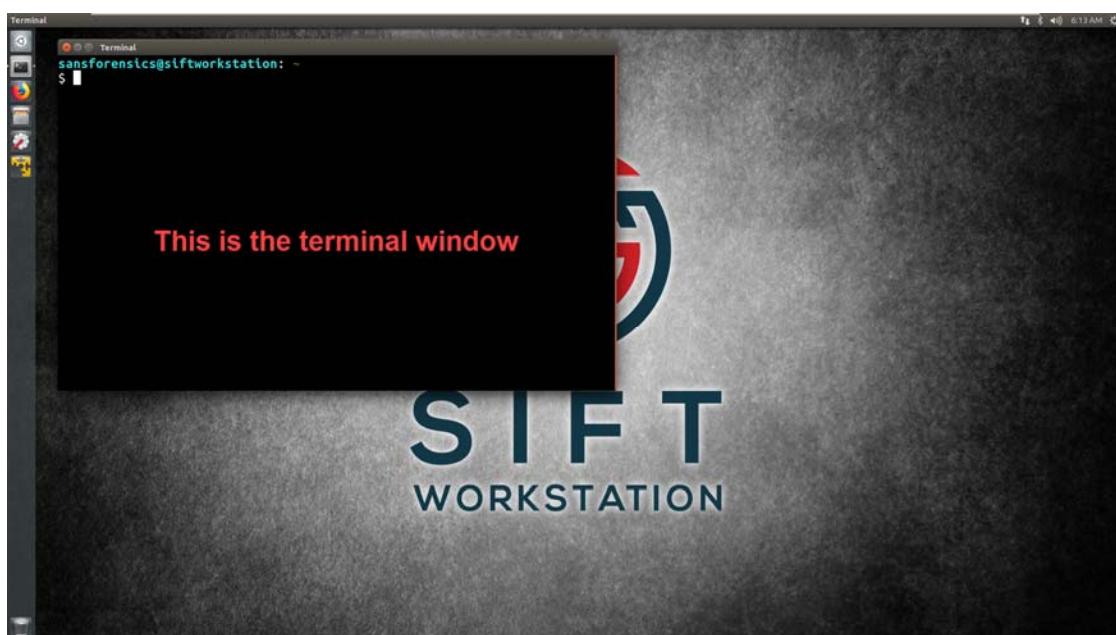
- Use **Linux** and **xmount** to mount an E01 file as a VMDK file.
- Use **VMware Player** to create a virtual machine of the newly mounted VMDK file.
- Boot the subject evidence file as if you were sitting at the subject’s computer.
- Navigate around inside this virtual machine, noting certain data and functions that are unavailable in a “dead box” analysis.

**Exercise Preparation**

1. Boot your **FOR498 Linux VM**
2. After about 20-40 seconds of a black screen with text on it, the login screen will appear, prompting for credentials.
3. Login to the **FOR498 Linux VM** using the following credentials:
  - a. Username: **sansforensics**
  - b. Password: **forensics**



4. Once logged in, a **terminal window** will be open at startup. The next command will be run from the command line in that terminal window.



5. This step will use the **xmount** utility. **xmount** is a tool to cross mount between multiple input and output hard disk image files. In this case, we are going to mount an E01 image as a VMDK. This occurs with no live conversion of files and therefore takes only seconds.

Mount the E01 image with **xmount** to virtually create the vmdk. The **xmount** command is shown below. Type CAREFULLY! The options used are:

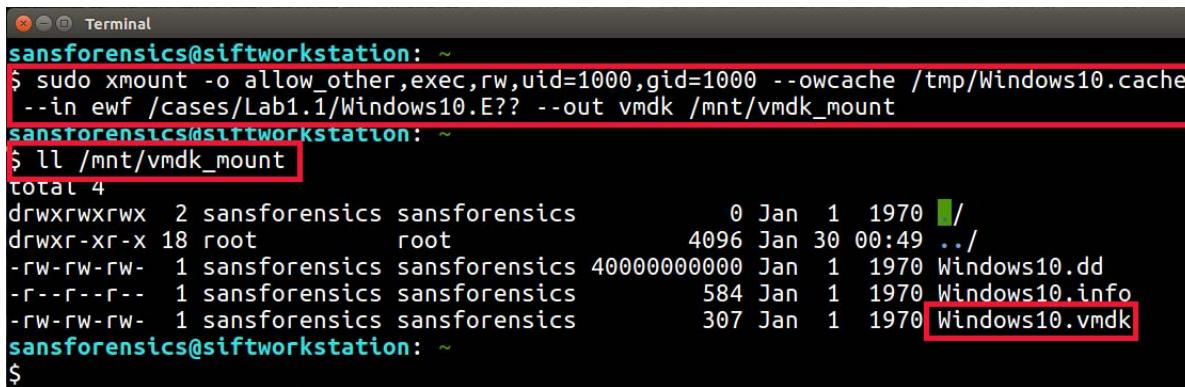
```
-o = options - The options used here are to set the permissions on the E01
      file to allow the operation we need to perform
--owcache - enables virtual write support and defines the file to write to.
--in   The format of the input file. The file name after that is the input
      file.
--out The format of the file to be mounted. The file name after that is the
      output file.
```

Note there are spaces at the end of the lines in the example below, or refer to the lines typed in the Terminal screenshot below. Also note that in a Linux terminal, all characters are case sensitive.

```
$ sudo xmount -o allow_other,exec,rw,uid=1000,gid=1000 --owcache
/tmp/Windows10.cache --in ewf /cases/Lab1.1/Windows10.E?? --out vmdk
/mnt/vmdk_mount
```

6. If everything was typed correctly, you will be presented with another command prompt.  
 7. Verify that the image file was mounted as a vmdk. (**the first two characters are ellipses, and not ones**)

```
$ ll /mnt/vmdk_mount
```



The screenshot shows a terminal window titled "Terminal". The user has run the command \$ sudo xmount -o allow\_other,exec,rw,uid=1000,gid=1000 --owcache /tmp/Windows10.cache --in ewf /cases/Lab1.1/Windows10.E?? --out vmdk /mnt/vmdk\_mount. After pressing Enter, the user runs \$ ll /mnt/vmdk\_mount to list the contents of the mounted directory. The output shows four files: a directory named "/", a file named "Windows10.dd" (size 4096), a file named "Windows10.info" (size 584), and a file named "Windows10.vmdk" (size 307).

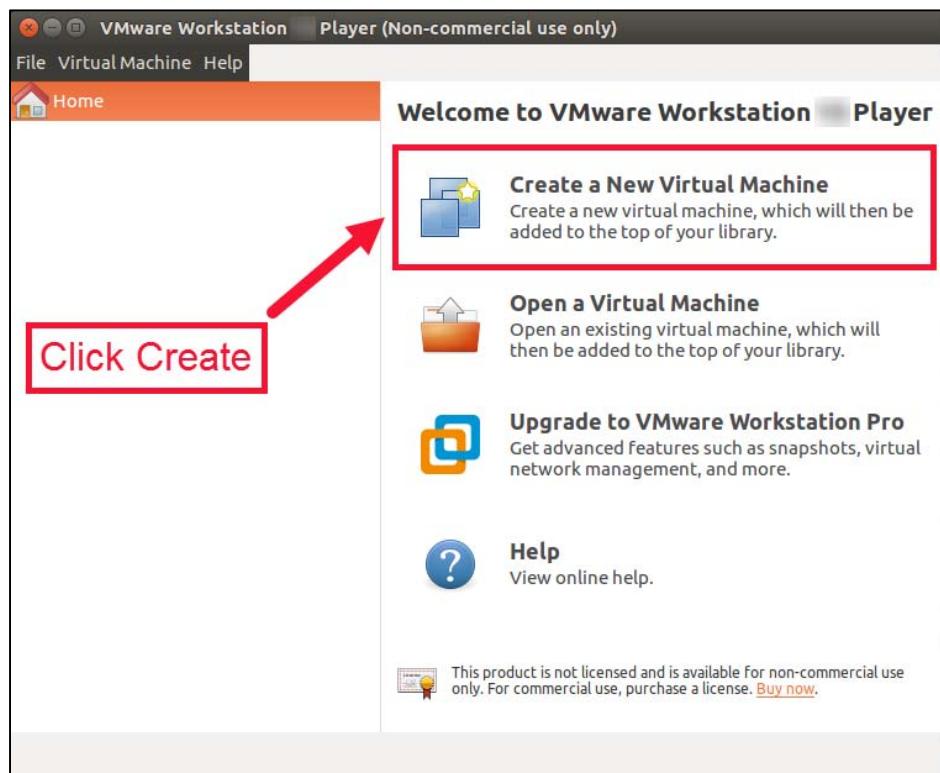
```
sansforensics@siftworkstation: ~
$ sudo xmount -o allow_other,exec,rw,uid=1000,gid=1000 --owcache /tmp/Windows10.cache
--in ewf /cases/Lab1.1/Windows10.E?? --out vmdk /mnt/vmdk_mount
sansforensics@siftworkstation: ~
$ ll /mnt/vmdk_mount
total 4
drwxrwxrwx  2 sansforensics sansforensics          0 Jan  1 1970 /
drwxr-xr-x 18 root          root              4096 Jan 30 00:49 ..
-rw-rw-rw-  1 sansforensics sansforensics 400000000000 Jan  1 1970 Windows10.dd
-r--r--r--  1 sansforensics sansforensics      584 Jan  1 1970 Windows10.info
-rw-rw-rw-  1 sansforensics sansforensics      307 Jan  1 1970 Windows10.vmdk
sansforensics@siftworkstation: ~
$
```

8. You can minimize the terminal window now, by clicking on the circled dash in the top left-hand corner of the window.

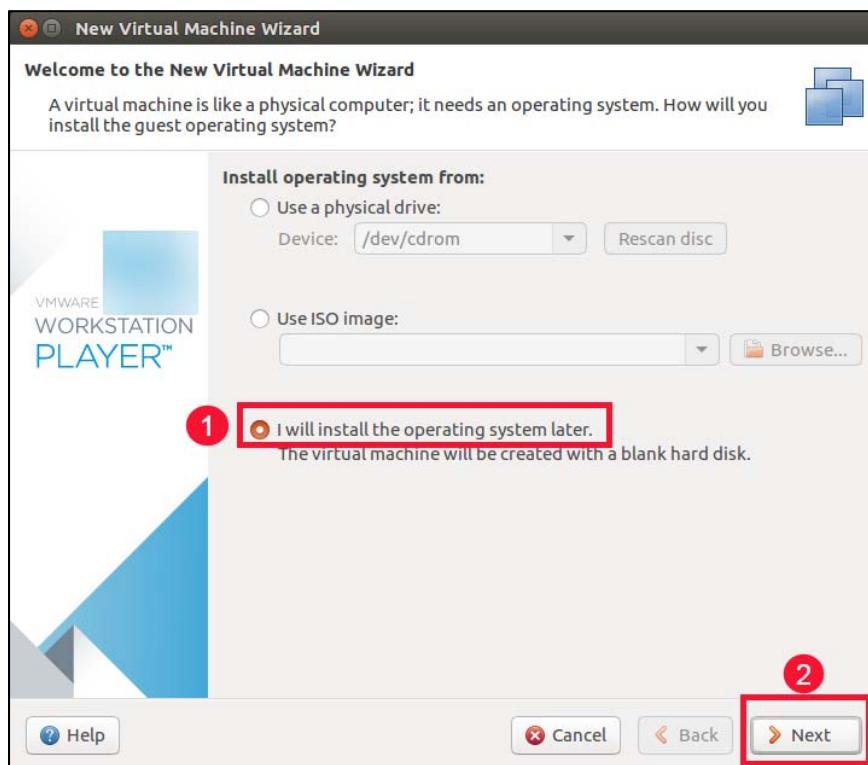
9. Open VMware Player by clicking on the icon in the left-hand toolbar.



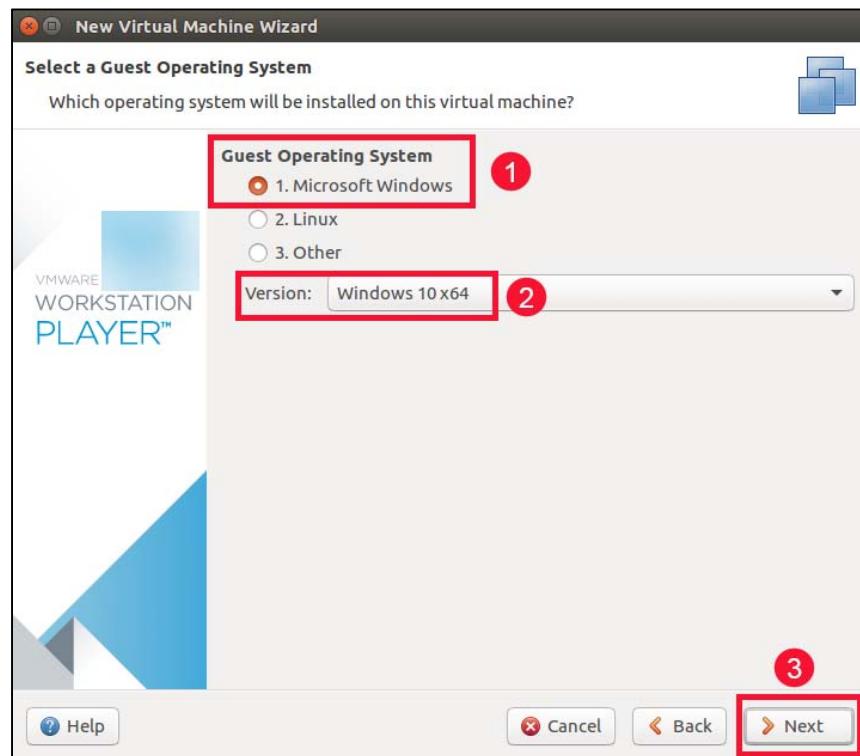
10. Once **VMware Player** launches, click **Create New Virtual Machine**. If prompted to perform a software update, do NOT do this.



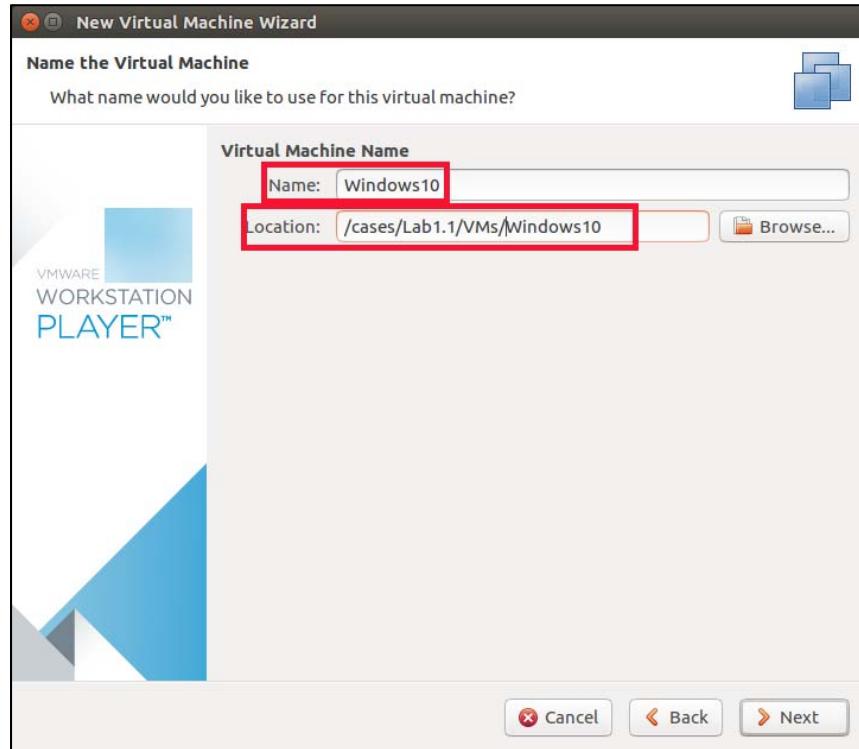
11. Select **I will install the operating system later** and click the **Next** button.



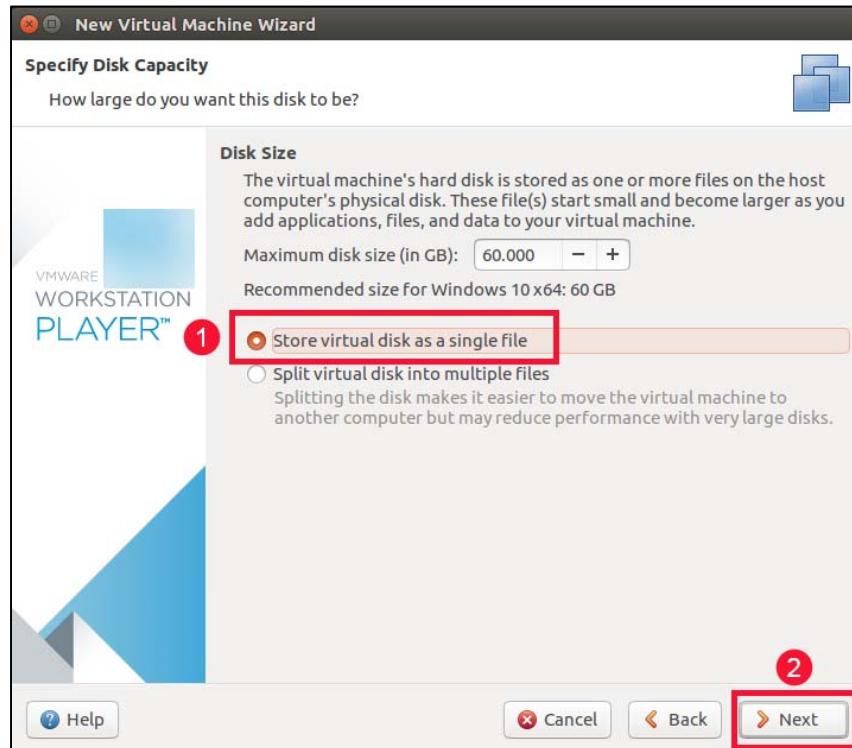
12. Under **Guest Operating System**, select **Microsoft Windows**. Beside **Version:** select **Windows 10 x64**. These are the operating system and version of the image you will be booting. In other cases, change these values accordingly. Click the **Next** button.



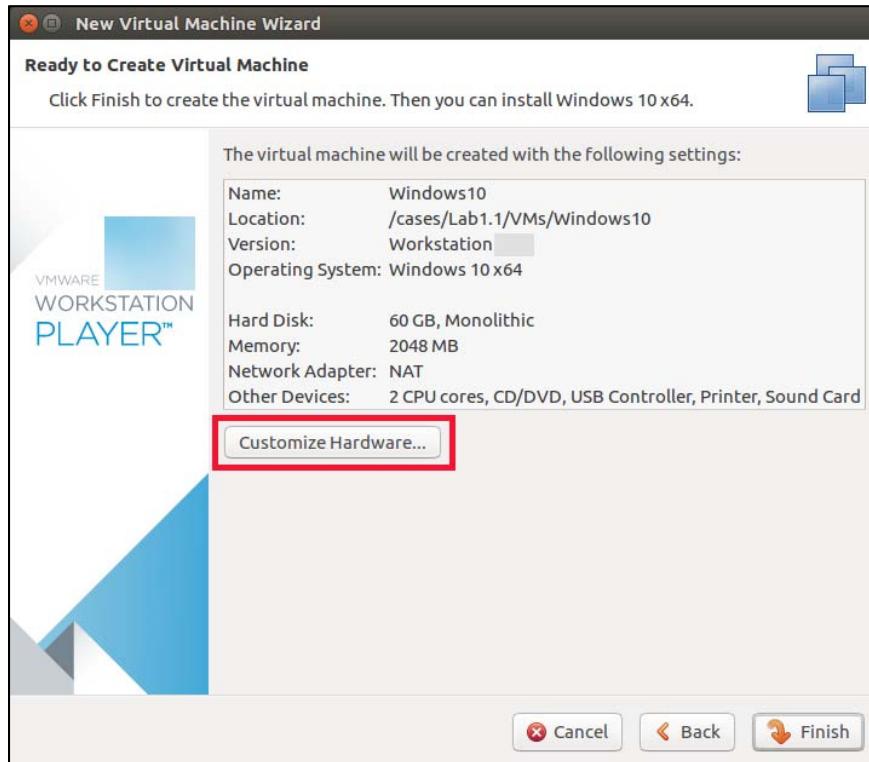
13. Name the Virtual Machine **Windows10** (Note there is no space). The location for the VM is **/cases/Lab1.1/VMs/Windows10** Click **Next** to move to the next screen.



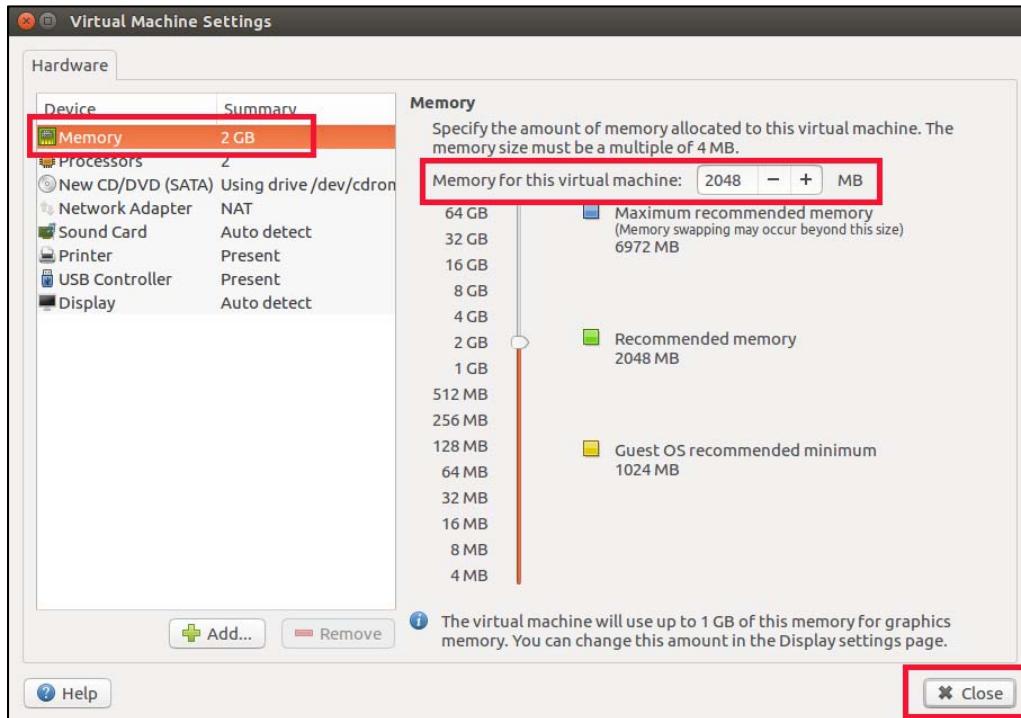
14. Accept the default **Disk Size of 60 GB**. Select **Store virtual disk as a single file**. This disk is just to allow you to get through the setup. You will replace this disk with the mounted vmdk in a step to follow. Click **Next** to move to the next screen.



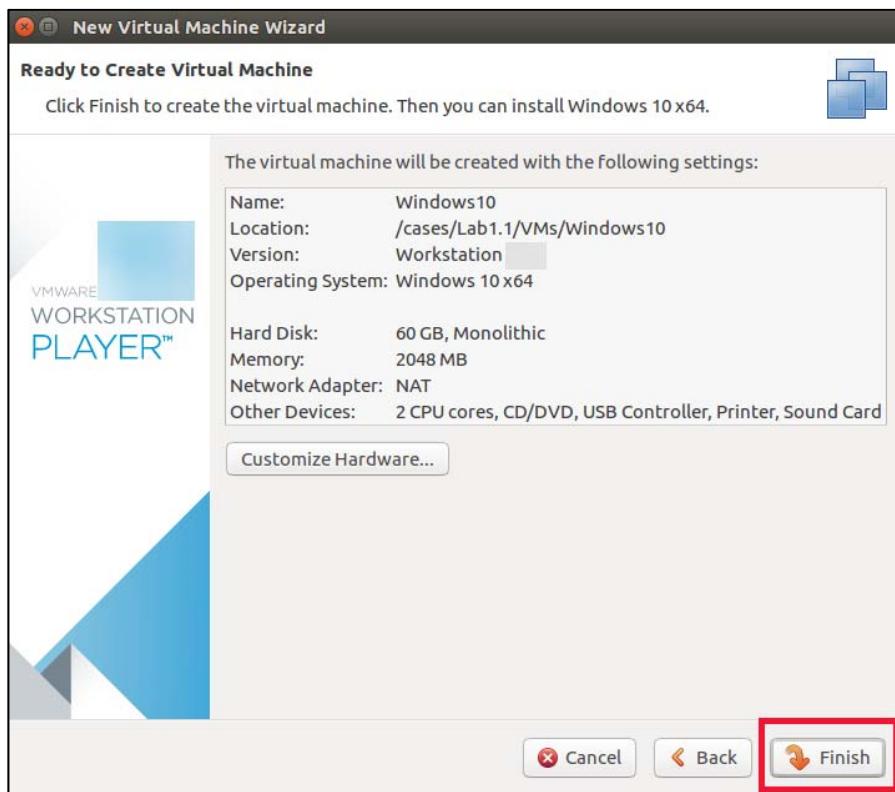
15. Click the **customize hardware** button.



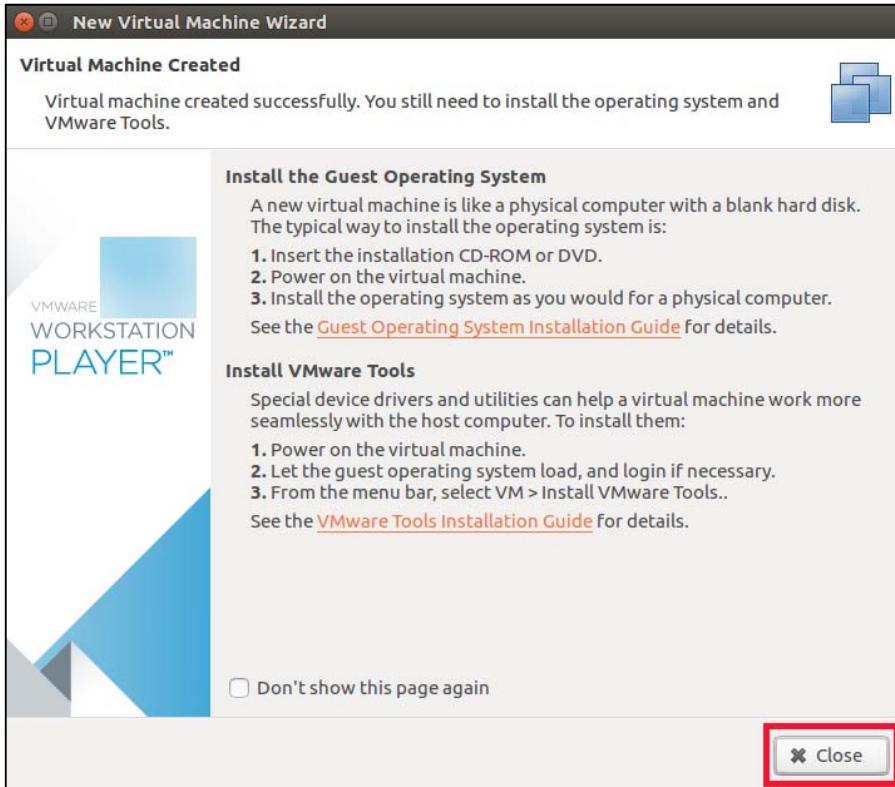
16. Make sure that the VM's memory is set for **2 GB**. Click **Close** to move to the next screen.



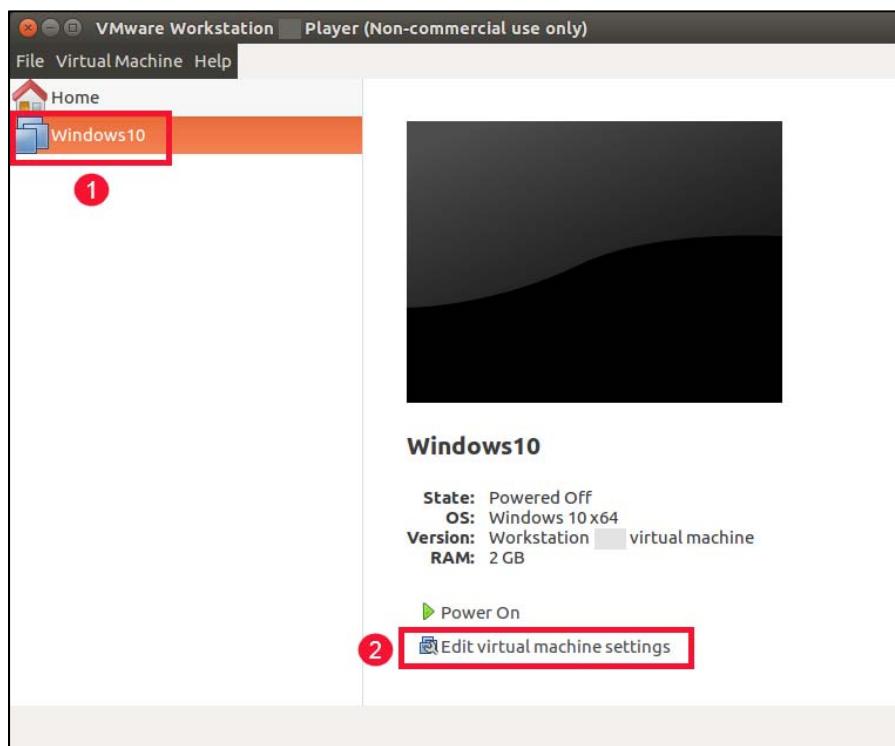
17. On the next screen click the **Finish** button.



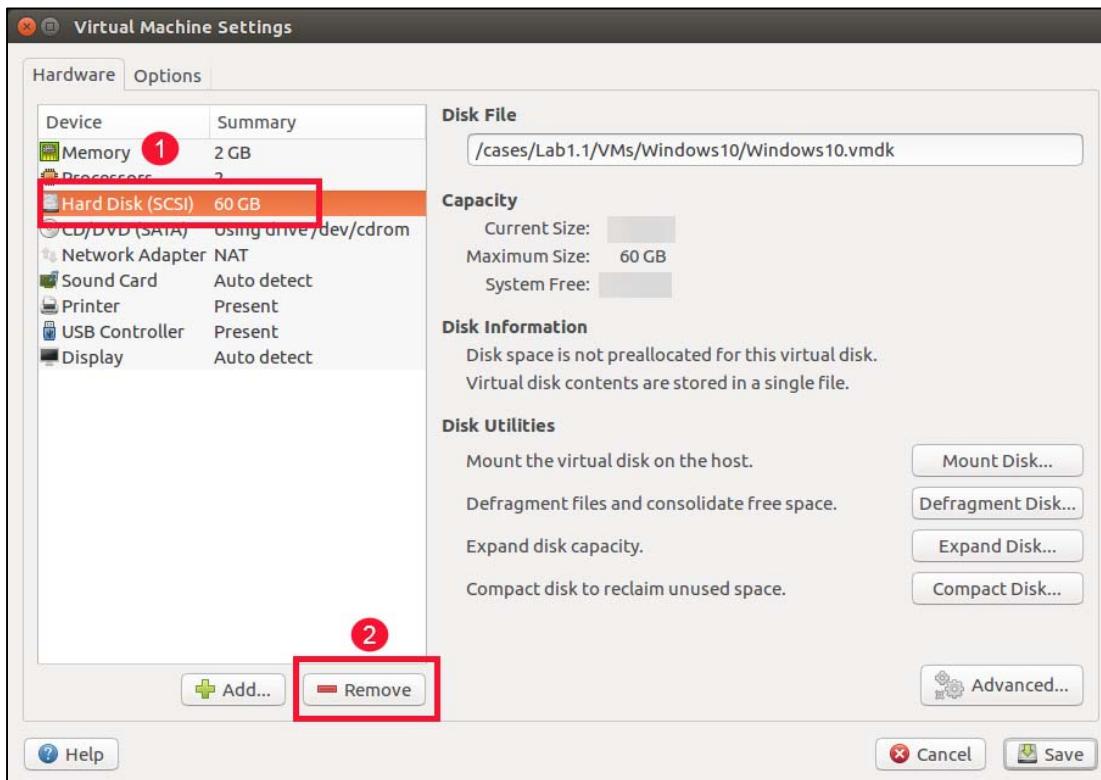
18. On the **Virtual Machine Created** screen, click **Close**.



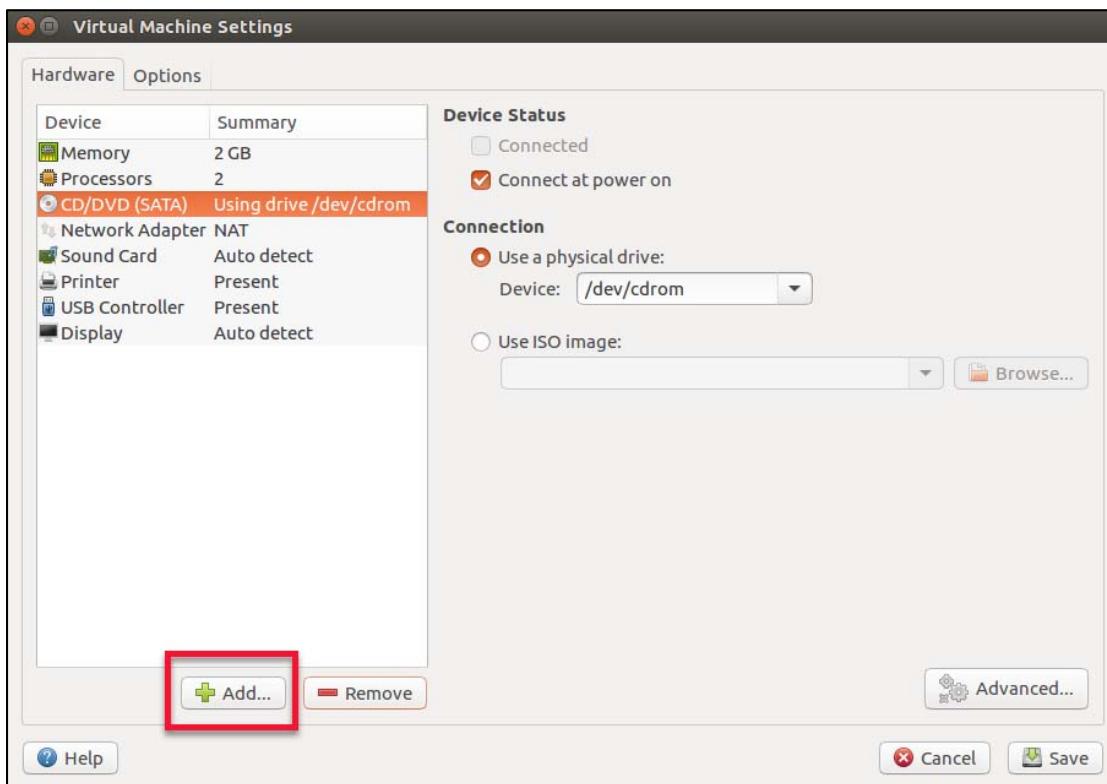
19. The Virtual Machine is now created, but we need to remove the default hard drive and attach the virtual drive (vmdk) that we created when we mounted the E01 image. Highlight the **Windows10 VM** and then click the **Edit virtual machine settings** link at the bottom of the window.



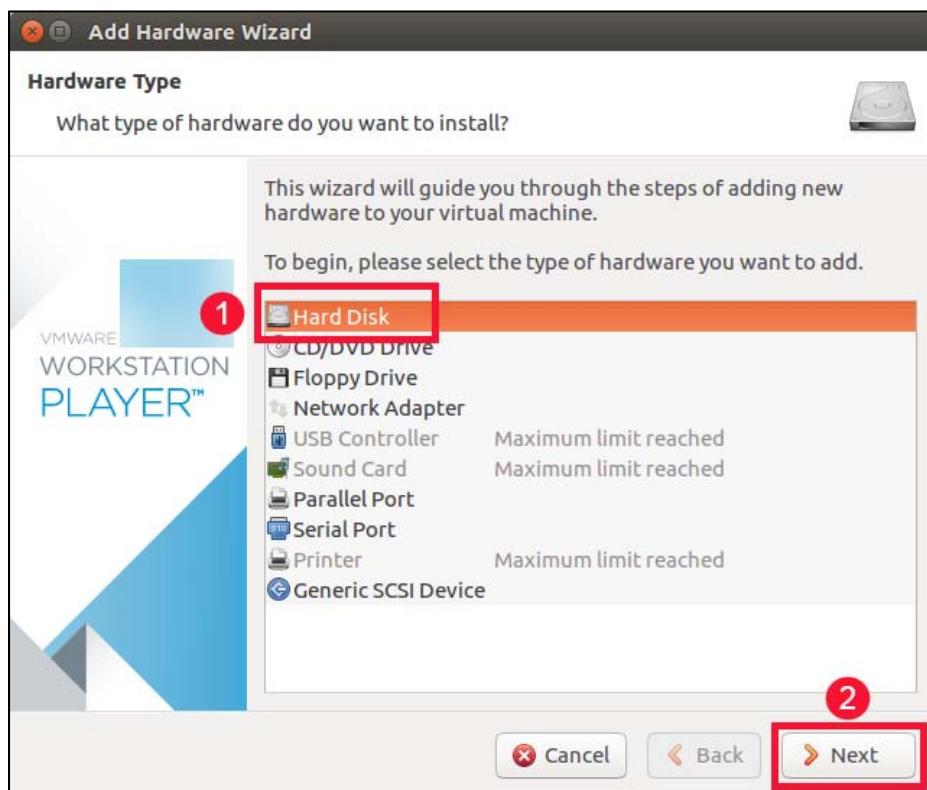
20. Select the **Hard Disk (SCSI) 60 GB** and click the **Remove** button.



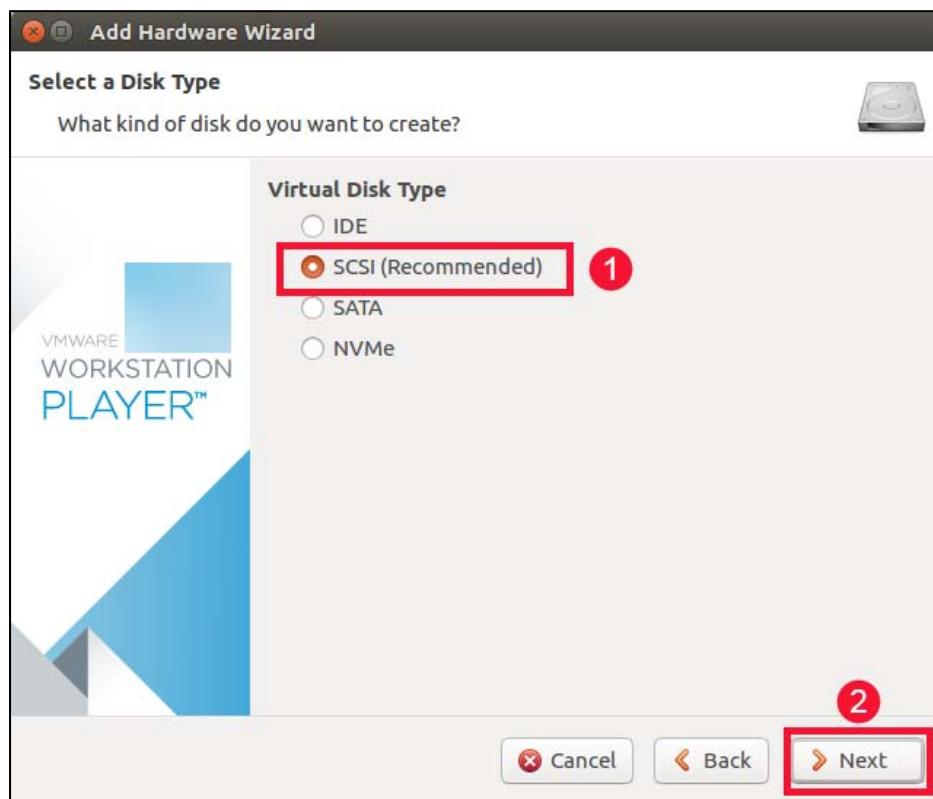
21. Click the **Add** button to create a new hard drive. This will be the one that you mounted from the E01 image.



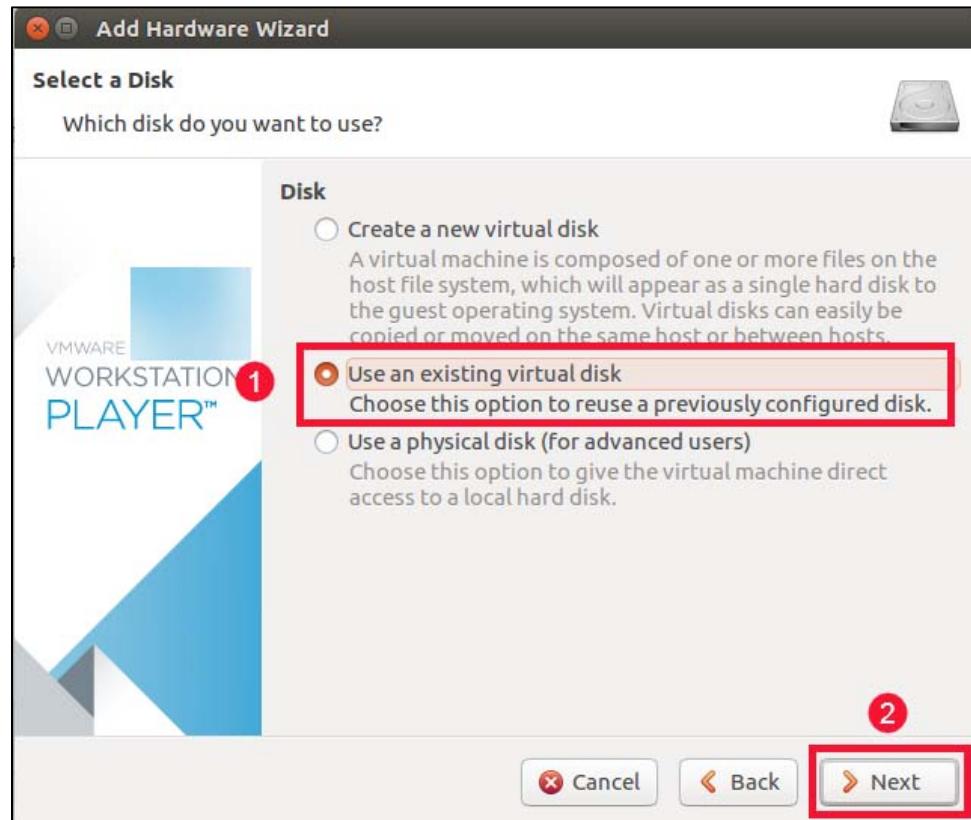
22. Select **Hard Disk**, and then click the **Next** button.



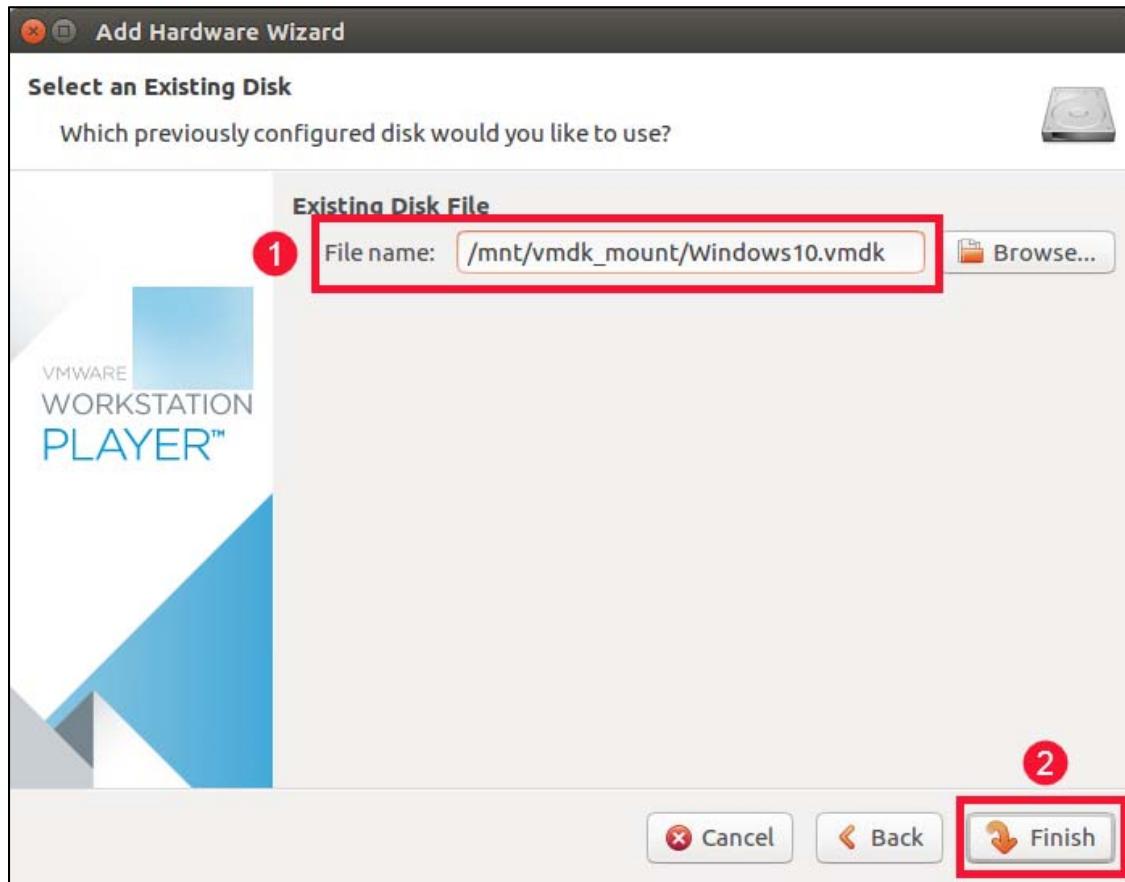
23. Select **SCSI (Recommended)** as the **Virtual Disk Type** and click the **Next** button.



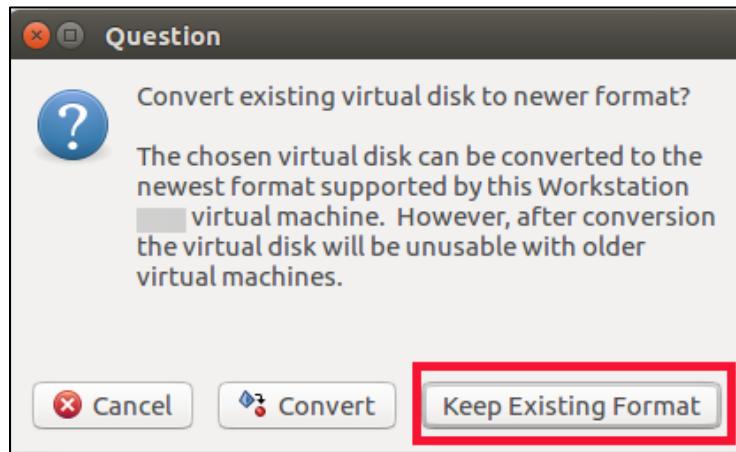
24. On the **Select a Disk** screen, select **Use an existing virtual disk** and click the **Next** button.



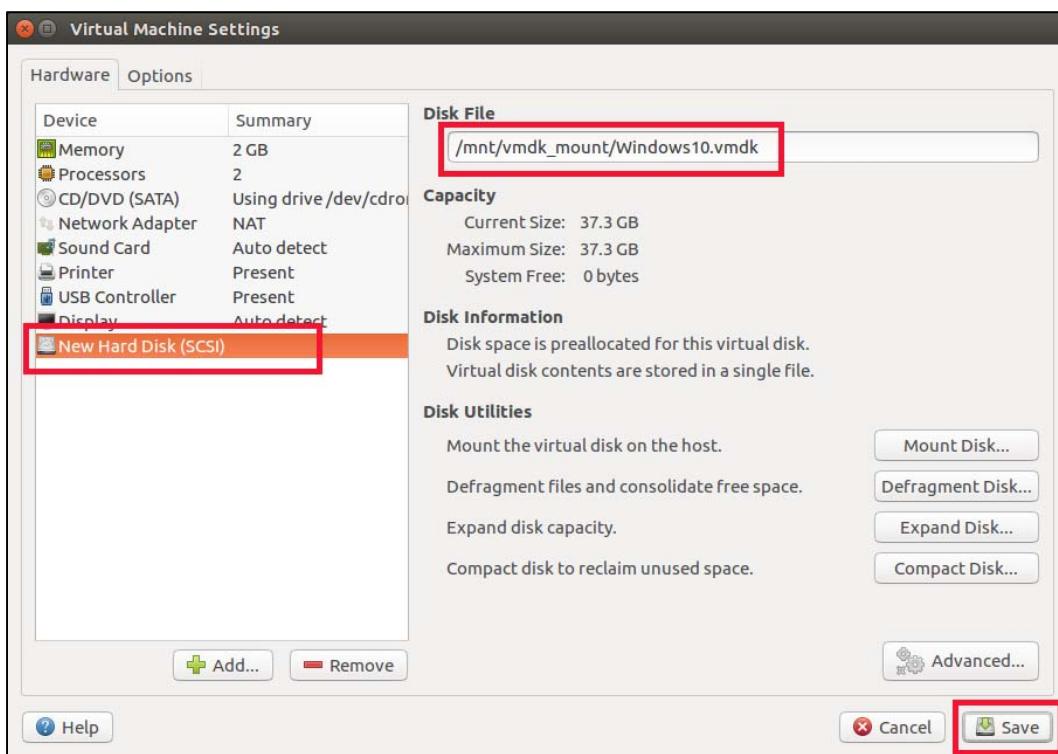
25. Type the path and filename `/mnt/vmdk_mount/Windows10.vmdk`, or use the **Browse** button to locate the path and file. Click the **Finish** button.



26. Do NOT convert the disk to the newer format. Select **Keep Existing Format**.



27. The new hard drive will be shown in the **Virtual Machine Settings**. Ignore information listed under **Capacity**. Click **Save**. Keep **VMware Player** open.



28. We will need to make one final update to the VM's settings. Open a terminal window and change directory to the Windows10 VM directory `/cases/Lab1.1/VMs/Windows10`

```
$ cd /cases/Lab1.1/VMs/Windows10/
```

```
sansforensics@siftworkstation: ~
$ cd /cases/Lab1.1/VMs/Windows10/
sansforensics@siftworkstation: /cases/Lab1.1/VMs/Windows10
$
```

29. Using the **gedit** program, you will **Edit** the **Windows10.vmx** file to change the firmware setting.

```
$ gedit Windows10.vmx
```

You need to replace the line that reads **firmware = "efi"** with **firmware = "bios"** to match the firmware utilized by the machine whose image we are using for this exercise. You can do this with the editor of your choice but "**gedit**" is the easiest to use if you are not familiar with Linux editors. The file is small, so you can just look for the correct line.

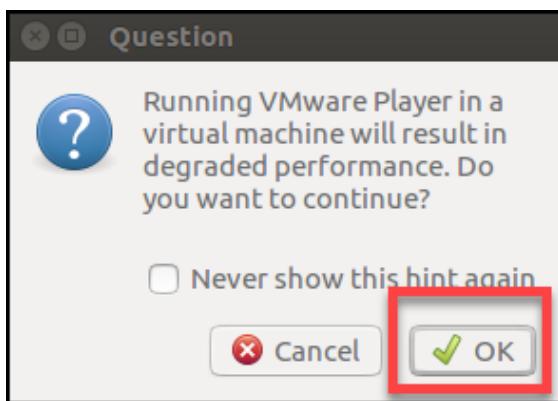
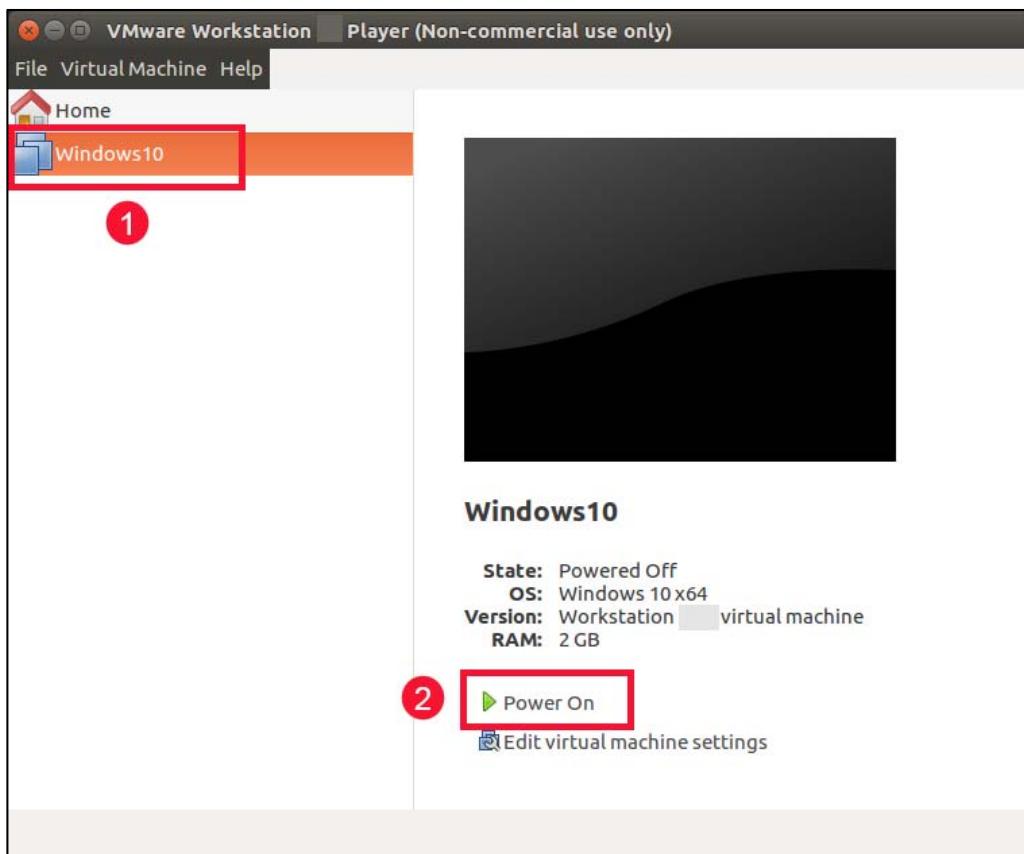
```
.encoding = "UTF-8"
config.version = "8"
virtualHW.version = "16"
mks.enable3d = "TRUE"
pciBridge0.present = "TRUE"
pciBridge4.present = "TRUE"
pciBridge4.virtualDev = "pcieRootPort"
pciBridge4.functions = "8"
pciBridge5.present = "TRUE"
pciBridge5.virtualDev = "pcieRootPort"
pciBridge5.functions = "8"
pciBridge6.present = "TRUE"
pciBridge6.virtualDev = "pcieRootPort"
pciBridge6.functions = "8"
pciBridge7.present = "TRUE"
pciBridge7.virtualDev = "pcieRootPort"
pciBridge7.functions = "8"
vmci0.present = "TRUE"
hpet0.present = "TRUE"
usb.vbluetooth.startConnected = "TRUE"
firmware = "efi" ← 1
sensor.accelerometer = "pass-through"
sensor.ambientLight = "pass-through"
sensor.compass = "pass-through"
sensor.gyrometer = "pass-through"
sensor.inclinometer = "pass-through"
sensor.location = "pass-through"
sensor.orientation = "pass-through"
displayName = "Windows10"

```

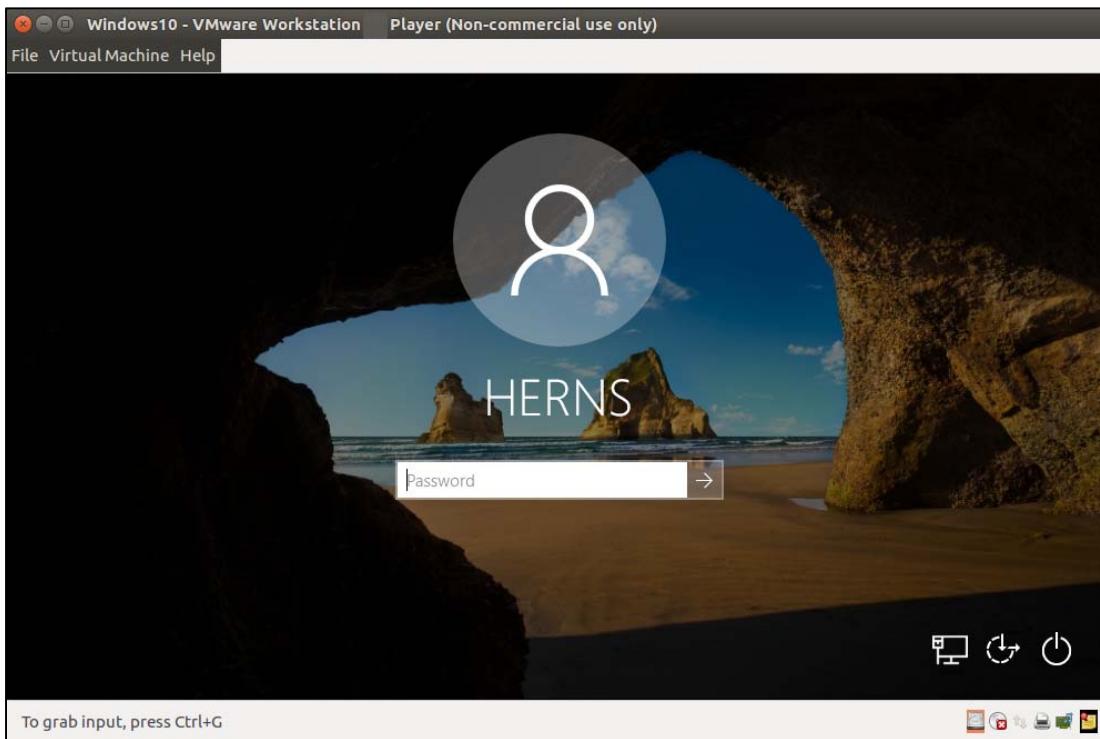
Plain Text ▾ Tab Width: 8 ▾ Ln 21, Col 17 ▾ INS

30. Once the edit is done, click **Save**, and then close the **gedit** window.

31. Switch back to the **VMware Player** window, make sure the **Windows10** VM is selected and click the **Power On** link. There may be several pop-ups displayed as the machine boots. Answer the pop-ups as shown in screenshots below show.



32. The **VM** will now begin to boot. There may be several configuration warnings displayed as the **VM** boots. They are not an issue, and you can ignore them. If all went well, you will see a Windows login screen. Depending on your hardware, this could take 2-3 minutes.

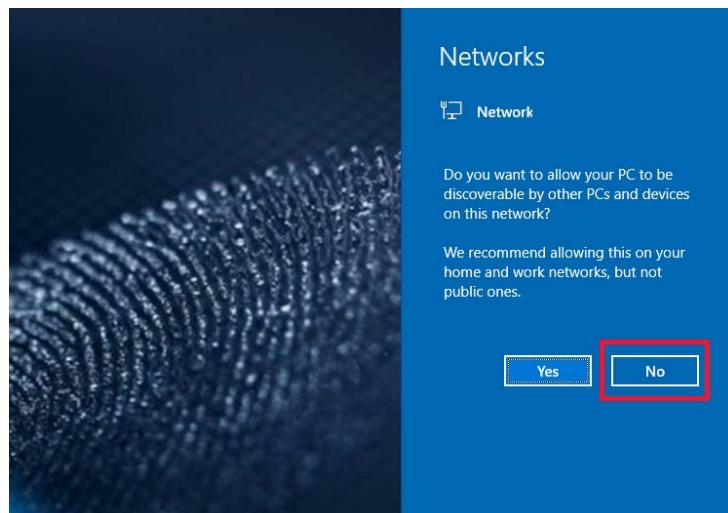


### Exercise Questions

1. What is the password for the user **HERNS**? Once determined, use it to log in.

---

2. You may see a **Networks** box appear on the right edge of your desktop, asking if you want to allow your PC to be discoverable by other PCs. Click **No** and the box will disappear.



3. What does the desktop screen say about the computer user?

---

4. Read the sticky note on the desktop. Who is Pratt?

---

5. Try to move the note on the **Desktop**. Are you able to do so?

---

### **Bonus Questions**

6. Who is 'Portnoy'?

---

7. Who is 'Hawkins'?

---

8. Based on the evidence you have discovered, who is the owner (or at least daily user) of this computer?

---

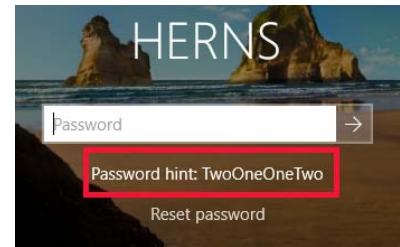
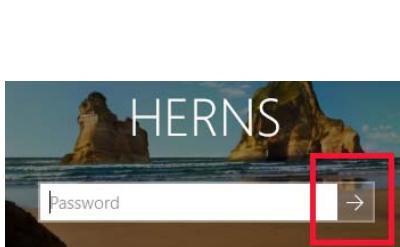
Although it may seem that only fans of this form of music, or this band would be able to determine the answers, and although these questions seem to require a bit of online intelligence gathering, this is what you face daily as a forensicator. You don't always know whose computer you have seized. You don't always know what is important or why. But with a little skill, ingenuity, and thinking outside the box, you will be successful!

## Exercise—Questions with Step-by-Step

1. What is the password for the user **HERNS**? Once determined, use it to log in.

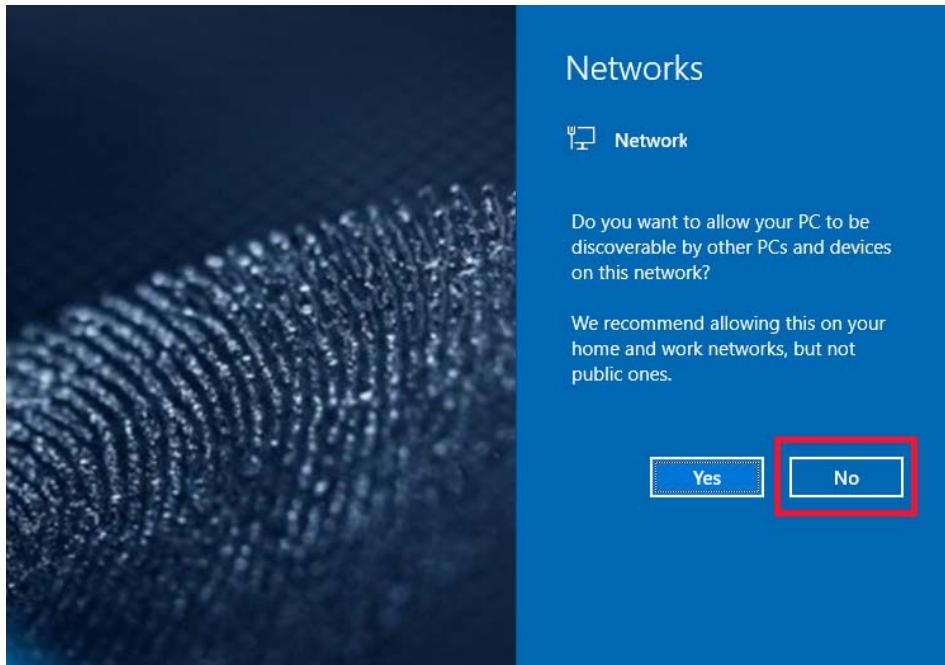
**2112**

**Click on the arrow beside the password field. You will get the error below. Click OK. Look at the password hint.**



This does not mean that you will be successful every time, but the takeaway is that just because you see something that leads you to believe you can't go any further, keep trying. You never know...

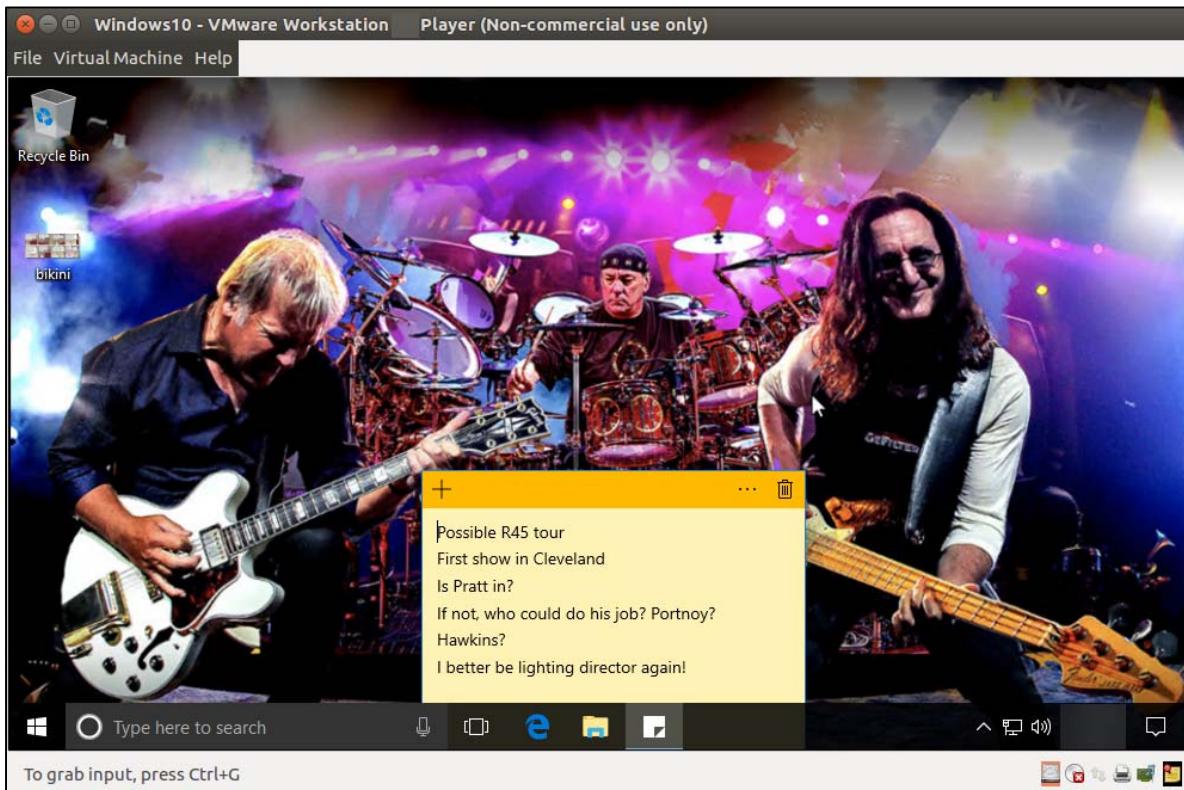
2. You may see a **Networks** box appear on the right edge of your desktop, asking if you want to allow your PC to be discoverable by other PCs. Click **No** and the box will disappear.



3. What does the desktop screen say about the computer user?

**They are a Rush fan**

**Google search on ‘GeFilter’ from the band member’s T-shirt, or search on ‘R45 tour’ will show you that this is the band Rush. People usually put pictures of their favorite things on their desktop.**



4. Read the sticky note on the desktop. Who is Pratt? **Google search on the term ‘Pratt Rush’**

**The drummer of the band Neil Peart**

5. Try to move the note on the **Desktop**. Are you able to do so?

**Yes**

Very clearly you have access and control over this computer!

### **Bonus Questions**

6. Who is ‘Portnoy’? **Google search on the term ‘Portnoy’**

**Mike Portnoy, drummer for Dream Theater**

7. Who is ‘Hawkins’? **Google search on the term ‘drummer Hawkins’**

**Taylor Hawkins, drummer for Foo Fighters**

8. Based on the evidence you have discovered, who is the owner (or at least daily user) of this computer?

**Howard Ungerleider**

**You know from the note that the user says “I” better be lighting director again. You know the band is Rush. Google ‘lighting director Rush’. You will also see a reference in the search hits for the name HERNS, which is Howard’s nickname.**

Although it may seem that only fans of this form of music, or this band would be able to determine the answers, and although these questions seem to require a bit of online intelligence gathering, this is what you face daily as a forensicator. You don’t always know whose computer you have seized. You don’t always know what is important or why. But with a little skill, ingenuity, and thinking outside the box, you will be successful!

### **Exercise—Key Takeaways**

- There is nothing quite like being able to see the user’s environment as the user did.
- In an investigation where a forensic image already exists, but time is of the essence, data can be interpreted and extracted much more quickly from a “working” computer.
- Extracting data from a working computer removes the need for a myriad of tools typically used by the examiner to make sense of databases and other repositories when parsing data from a “dead box” image.
- Artifacts in the form of desktop notes can be extremely quick wins. Most examiners never consider the notion of a user having notes on their desktop, nor do most forensicators even know where to find or parse them on a dead box image.

## *Exercise 1.2—Interface ID & BIOS/UEFI*

### **Background**

The acquisition process is arguably the most important part of the forensic investigation process. As long as the acquisition process is done correctly, all other phases except intake can be redone. Even for as important as the evidence intake process is, depending on the circumstances the acquisition can still stand on its own. But we cannot assume this in every case.

All of this is predicated on the proper steps of preparation for acquisition. You cannot show up at a seizure or acquisition unprepared. You must have the proper equipment, software, and collection methods if you are to do the task properly, and indeed be taken seriously.

Especially in the case of on-site acquisition, you do not have the luxury (in most cases) to go back to the lab for more tools. You must have a proper approach determined prior to collection. This does not happen a few minutes before you head out the door. This is a process that is honed from experience and common sense.

Proper adapters, tools, storage, process, and most importantly, knowledge are integral to a smooth collection process. What if you are told the acquisition involves a single hard drive in a home style computer, so you fly 1500 miles to collect it, only to find out it is a server with a 4 disk nested RAID 10? You must be able to adapt.

When you are working within a corporate environment where your acquisitions only ever happen in your lab, you can just walk back and get the appropriate adapter, or more storage. But this environment is well within the minority of collections. In legal matters, cases can be won and lost due to the acquisition process. Ensure your acquisition setup is not one of the opposing counsel's attack vectors.

### **Exercise Objectives**

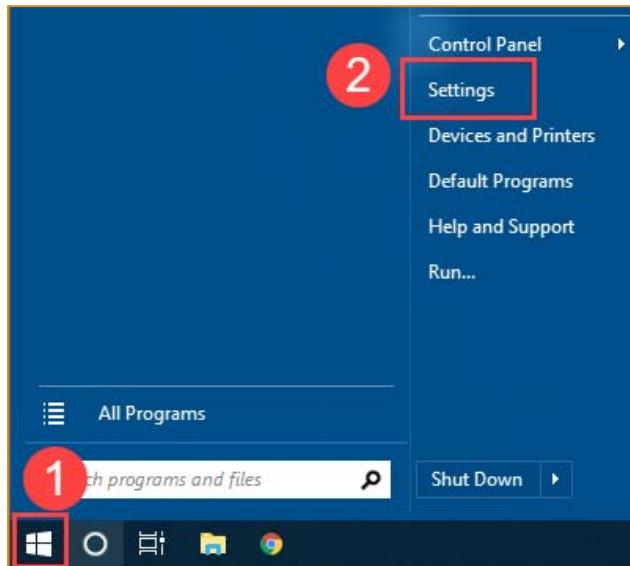
- Identify hard drive interfaces
- Learn process to access BIOS/UEFI and collect information

### **Exercise Preparation**

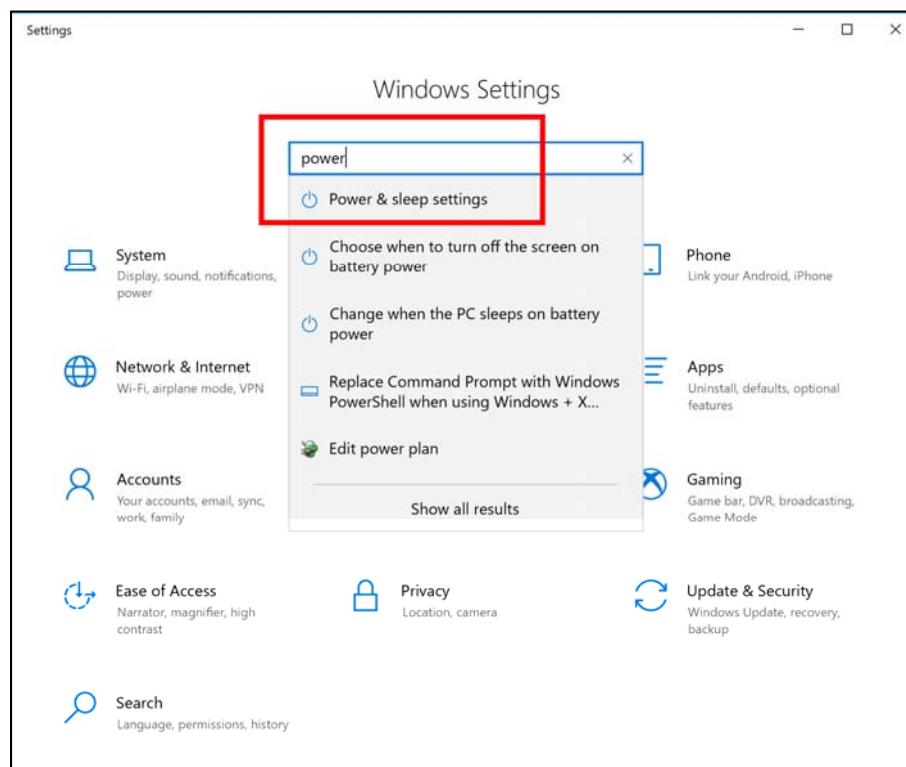
**There will be no step-by-step walk through of this section at the end, due to this section of the exercise being performed on the student's host machine. Each student's answers will be different.**

1. This section will be performed on your host machine. If your host machine is an Apple product, you can attempt it on your **FOR498 Windows VM**. In this case, treat your **VM** as your host. If you are using an Apple product, you do NOT need to follow the power setting changes outlined below. You can proceed directly to **step 17**.

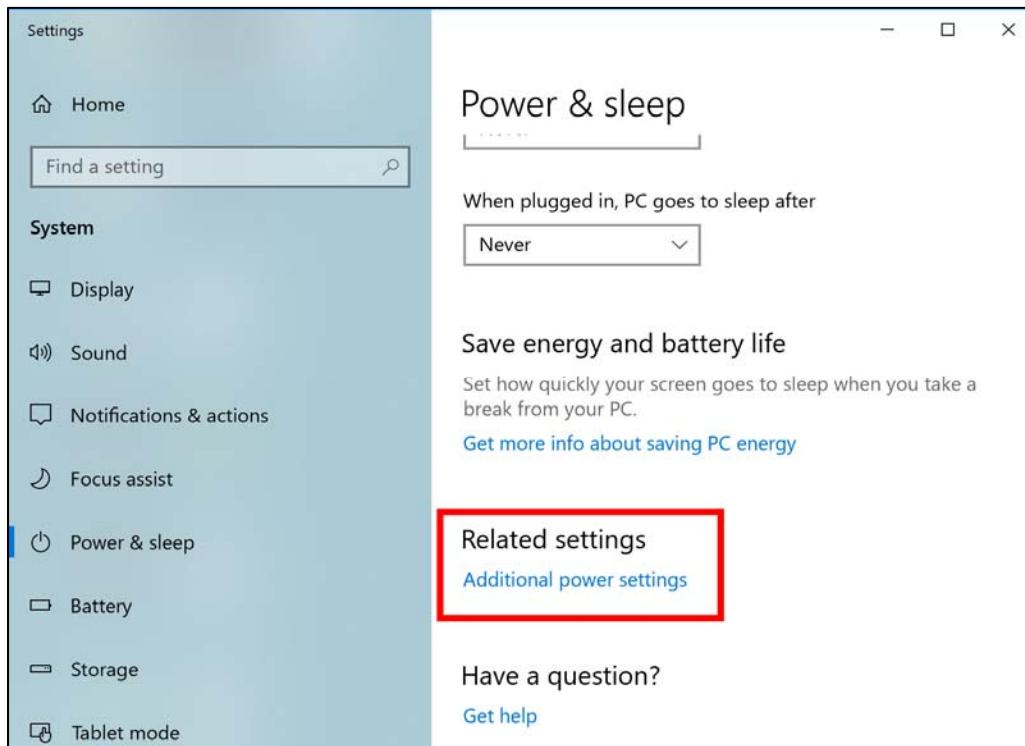
2. Ensure your **VM** is properly shut down, and then close all running programs on your host.
3. Power down your host machine fully. **Many newer Windows 10 machines do not power down completely, but we need the system powered down completely. Ensure your system is set to power down completely by performing the following steps.**
4. Click on **Start**, and then **Settings**.



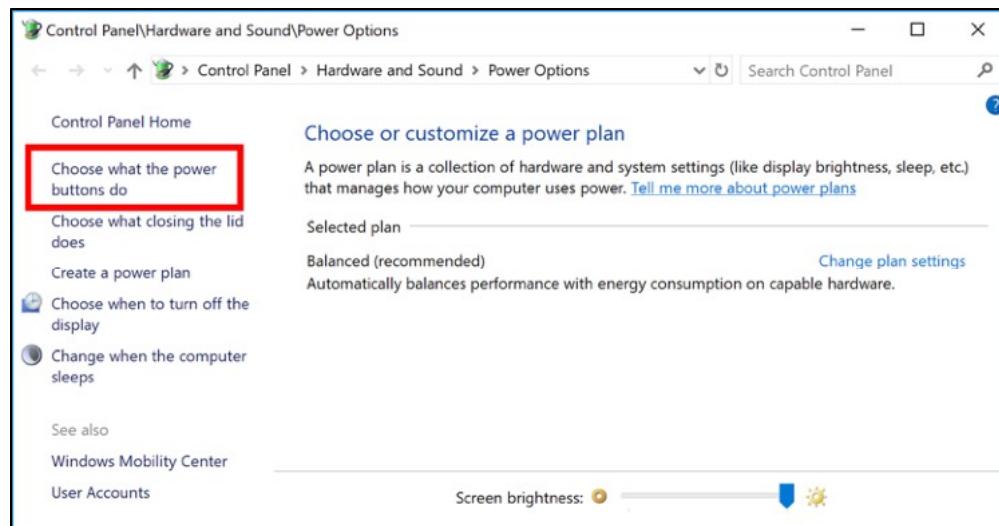
5. When the **Settings** window opens, locate the **Find a setting** field, and type **power**. A drop-down menu will appear. Click on **Power & sleep settings**.



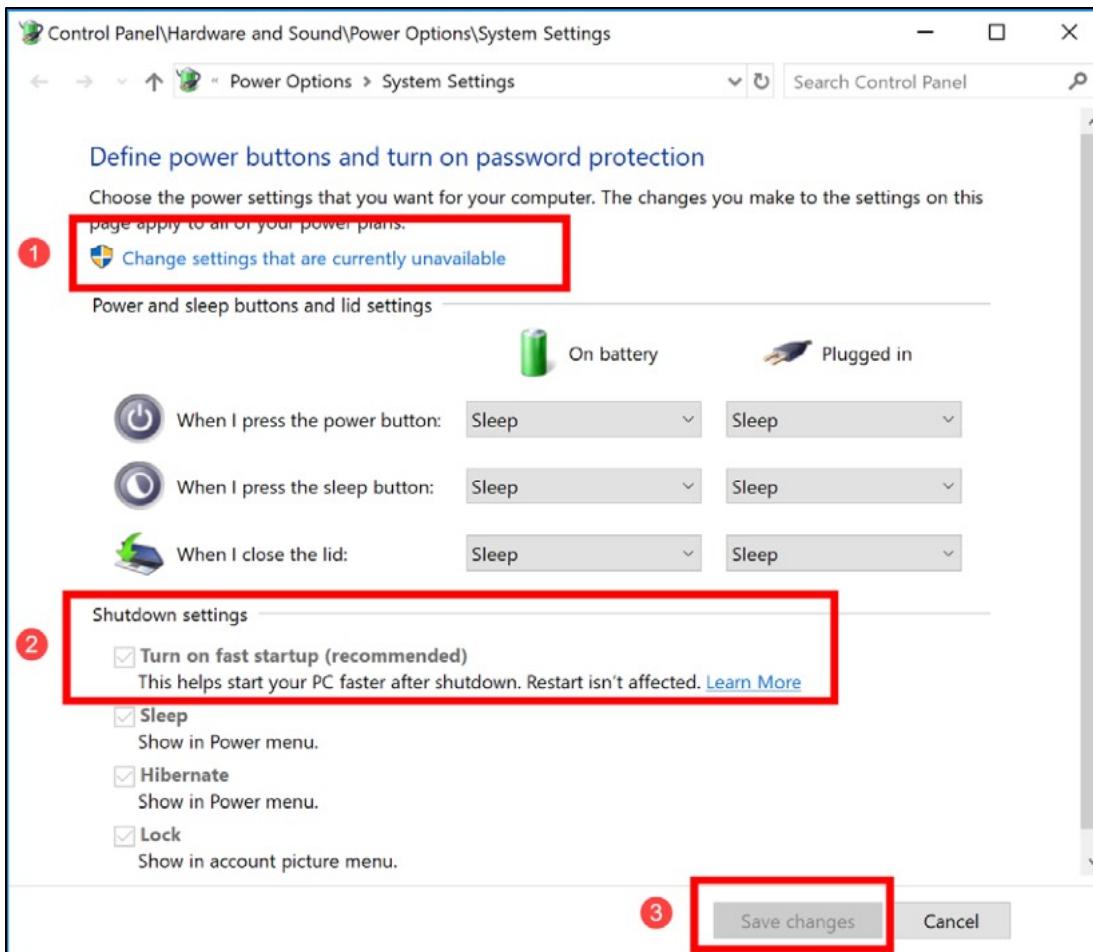
6. The **Power & sleep** window will open. Scroll down until you see the **Related settings** section and click on **Additional power settings**.



7. The **Power Options** window will open. On the left side, click on **Choose what the power button does**.



8. On the next window, look towards the bottom of the page (you may need to scroll) and find the **Shutdown settings**. Note that you cannot make changes, as these options are greyed out. At the top of the page, you will see a link that says **Change settings that are currently unavailable**. Once you click on it, the greyed options under **Shutdown settings** will be available. Uncheck the box that says **Turn on fast startup (recommended)** and then click **Save changes**. (Don't forget to change this back, when you are done!)

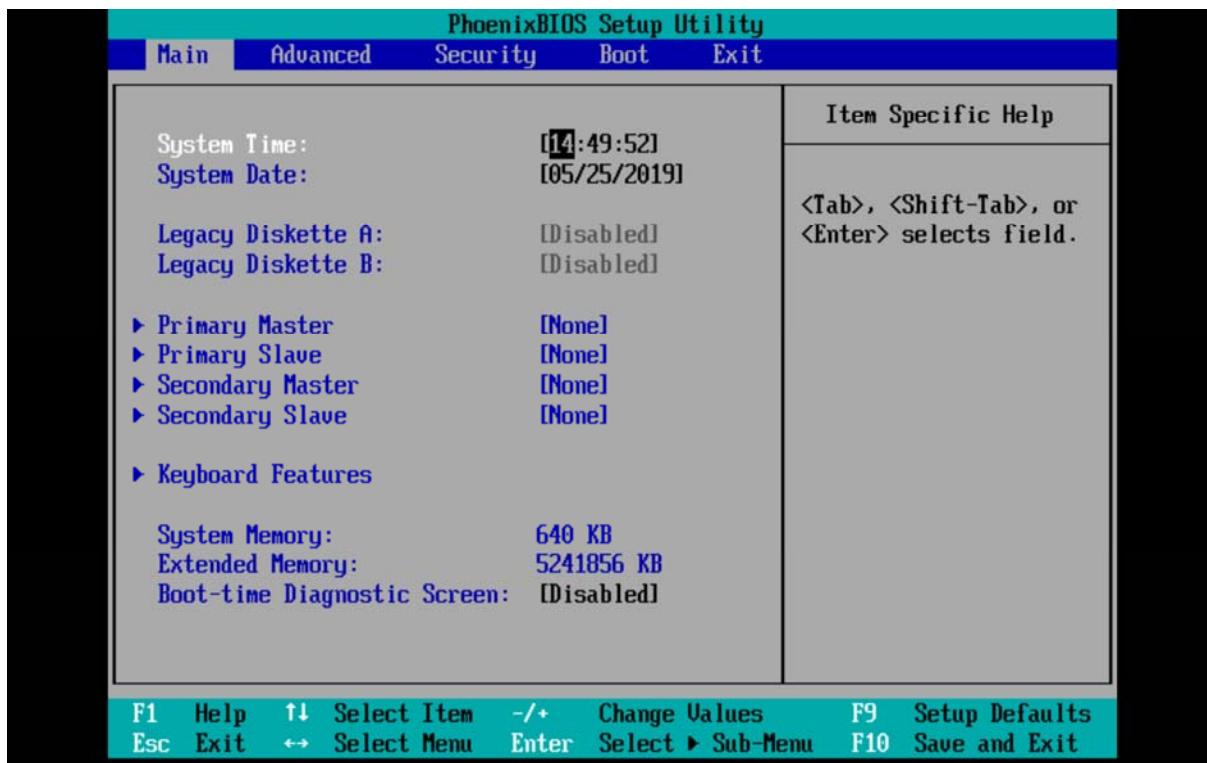


9. You can close all windows now, and power your computer down. Keep this in mind with any systems that you may be acquiring, for which you cannot remove the hard drive. If you forget this step, you will never be able to access the BIOS/UEFI.
10. Another important piece of data to have is any credentials needed to access the BIOS/UEFI. It is very possible (especially in enterprise environments), that there is a password needed to enter. This should be on your checklist of questions during the intake phase. In some cases, there are ways to get around an unknown BIOS password on older systems. You can refer to <http://for498.com/u3-62> or <http://for498.com/vih4u> for information on possible bypasses.
11. Now we must figure out how to get into the BIOS/UEFI. Most systems that you will come into contact with will almost certainly be branded. This is a virtual certainty with laptops.

12. Again, you will be doing this when the hard drive is out of the computer. If you have not or cannot remove the hard drive, or it is a live acquisition, you will not collect this data until after the acquisition is complete.
13. Turn on your computer and watch the screen closely. During boot up, did you see any splash screen show up briefly with an instruction such as **F2 = Enter setup?** If you did, you will power down the computer again, and when you power it up, immediately start tapping the **F2** key (or whatever instruction you saw) approximately 3-4 times per second until you see the computer entering the BIOS/UEFI.
14. If you did not see an instruction, you can start your computer back up and Google it (**Enter BIOS make/model**). The alternative is to guess. **F2, F1, F10, F12** are fairly common keys to use.
15. In a worst-case scenario, you can rapidly sweep your fingers back and forth across the top row of **F** keys from **F1** to **F12** and see if that works. There will certainly be a way. You just have to find it.
16. If you have discovered the proper key, you will see the BIOS/UEFI screen appear. Specifically, with most Dell computers, **F2** is the key for entering the BIOS, and **F12** is the key to enter the boot order.
17. The next few steps are for students using an Apple product as their host. The previous steps will not work on an Apple product, as there is no BIOS per se. As a result, we will perform essentially the same function from within the **FOR498 Windows VM**.
18. Power down the **VM**.
19. Start the **VM** and watch the boot up process for any indication of a key stroke to press in order to enter the BIOS. It should be **F2**. In the case of computers without the touch bar, the student will have to hold down the **Fn** key when tapping **F2**.



20. You will now see the VM BIOS.



## Exercise Questions

1. Navigate through the BIOS/UEFI using the instructions that will be present on the first screen. Enter the information as requested below.
  - a. Machine Date \_\_\_\_\_
  - b. Machine Time \_\_\_\_\_
  - c. Real Date \_\_\_\_\_
  - d. Real Time \_\_\_\_\_
  - e. Time Zone \_\_\_\_\_
  - f. CPU Make/Model \_\_\_\_\_
  - g. RAM amount \_\_\_\_\_

2. Look at the hard drive interfaces below and identify the type of interface.



A.

Slot number 1: \_\_\_\_\_

Slot number 2: \_\_\_\_\_



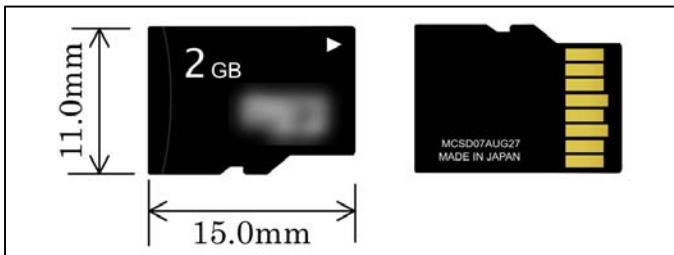
B. \_\_\_\_\_



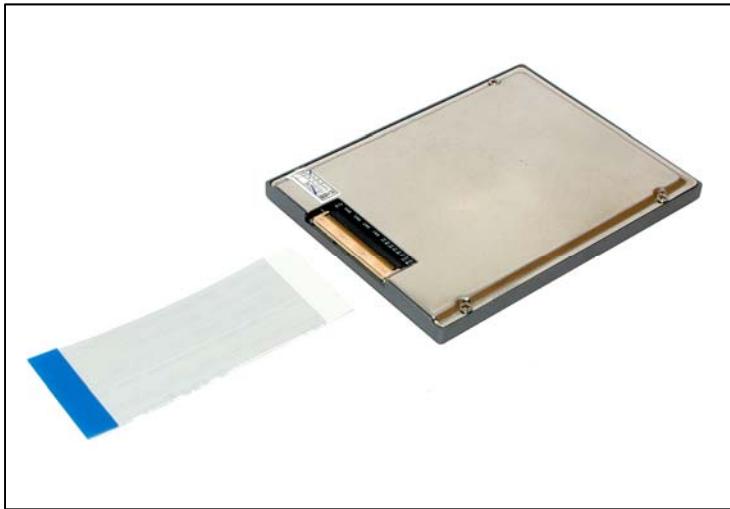
C. \_\_\_\_\_



D. \_\_\_\_\_



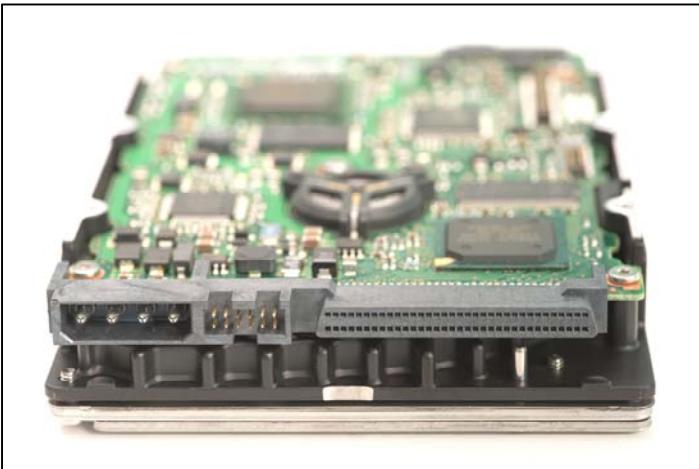
E. \_\_\_\_\_



F. \_\_\_\_\_



G. \_\_\_\_\_

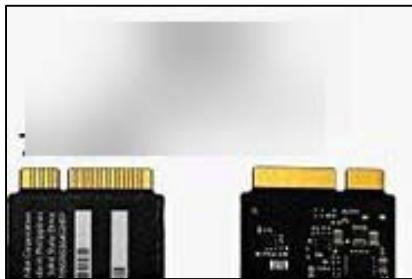


H. \_\_\_\_\_

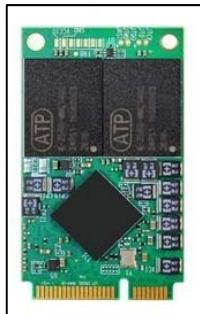


I. \_\_\_\_\_

## Bonus Questions



A. \_\_\_\_\_



B. \_\_\_\_\_

### **Exercise - Questions with Step-by-Step**

1. Look at the hard drive interfaces below and identify the type of interface.



A.

Slot number 1: **USB 3**

Slot number 2: **Thunderbolt**



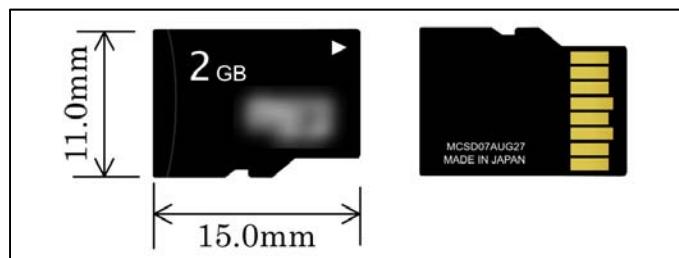
B. USB-C



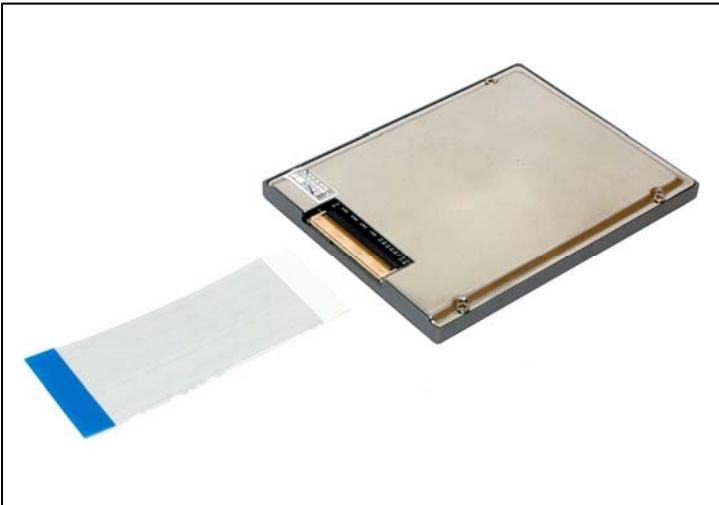
C. Fibre Channel



D. Micro SATA



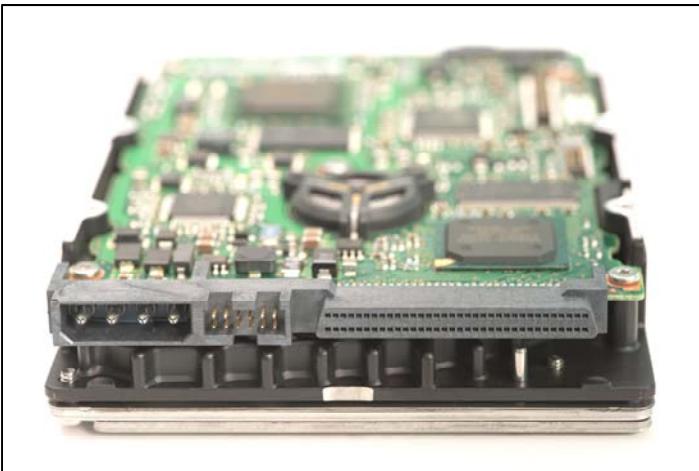
E. Micro Secure Digital



F. ZIF - Zero Insertion Force



G. SAS - Serial Attached SCSI

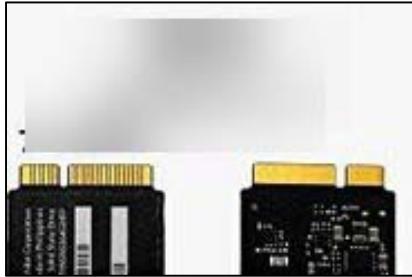


H. SCSI - Small Computer System Interface

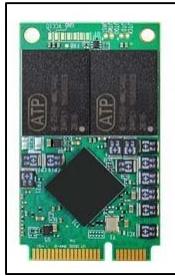


I. M.2 or NGFF - Next Generation Form Factor

**Bonus Questions**



A. MacBook Pro 2012 7+17 pin



B. mSATA SSD

***Exercise—Key Takeaways***

- BIOS is being deprecated for UEFI
- An examiner must know how to access BIOS/UEFI
- Without BIOS/UEFI information you may not be able to correlate data
- You can't image what you don't recognize
- You must have the correct adapters for a variety of storage media

This page intentionally left blank.

# *Optional - Out of Class*

## *Exercise 2.1A-Portable Device Acquisition - APPLE*

### **Background**

The most ubiquitous personal electronic device today (by far) is the smartphone. In criminal investigations, law enforcement is seizing these devices in unprecedented numbers. In fact, some law enforcement agencies have acquisition devices embedded in response units, so they can be on scene rapidly, not unlike K-9 and other units. Various units of the military are seizing devices from locations in combat theaters, and acquisition and analysis need to be done rapidly. On the civilian side of things, acquisition devices are seen to a lesser degree, but occurring more frequently, as employees are expected to be continually connected.

There are many acquisition tools on the market today that will allow personnel to perform a sound collection of evidence in a rapid manner. In some cases, this takes only minutes.

It is true that intelligence from these devices must be extracted as quickly as possible, but it is also extremely important that evidence be handled properly or its use in any future proceedings can potentially be placed into question.

In this exercise, the student will be performing a smartphone acquisition process on their own devices, using their own smartphone cable, along with a tool called UFED Physical Analyzer from Cellebrite. It is expected that the student possess a relatively standard Apple device, as well as the device charging/data cable.

### **Exercise Objectives**

- Connect student personal smartphone to the provided virtual machine
- Devices with MDM will not work completely
- Use **Cellebrite UFED Physical Analyzer** to create an evidence acquisition of student smartphone
- Open student acquisition with **Cellebrite UFED Physical Analyzer** software
- Note messages, pictures, and call logs; both active and deleted

### **Exercise Preparation**

1. Boot your **FOR498 Windows VM**.
2. Login to the **FOR498 Windows VM** using the following credentials:
  - a. Username: **SANSDFIR**
  - b. Password: **forensics**

3. Have student smartphone and charging/data cable ready. Cables are a strange thing and can cause issues. If you are having issues, unplugging and re-plugging may help.
4. Exercise assumes smartphone is powered on.

**NOTE:** In cases where your VM will not allow for external device connection, insert your supplied USB 2.0 hub, and connect through this.

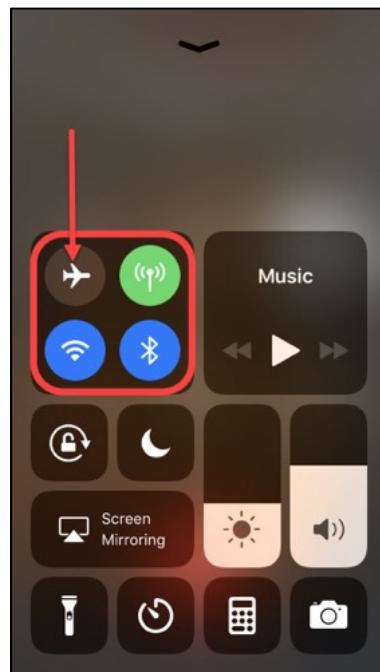
Acquisition of any smartphone or portable device is fraught with peril and can be quite frustrating. Although we have done our best to create these instructions based on the screens that presented themselves, it would not be surprising for a student to see something slightly different, as it is virtually impossible to account for every possible error message, permission message, or screen that a student may see. Any forensicator must be prepared to make informed, logical decisions. If you do not see your screen within the workbook, are you able to figure out what is expected? If not, call over your instructor, as you are working with a live device. For OnDemand students, please reach out to a SANS Online SME.

**Note: There is a risk that the latest version of iOS or your phone is not yet supported in the version of Cellebrite used in the class. If this is the case, you may not be able to complete the exercise as described. This is as close to a real-world situation as you'll encounter in this class. There will inevitably be instances where the tools have not yet caught up to the software and hardware. In those cases, you either need to wait for the tool to be updated to support the device or find an alternate method of collecting the data. This is all part of being a forensicator.**

**WARNING!** You are performing this exercise on a live device – YOURS. Proceed with caution, and at your own risk. SANS is not responsible for any data loss, or lack of a student having backups of their data. There is absolutely no way for portable device acquisition exercises to have perfectly matching screenshots against what a student might see. There are simply too many variables, options, devices, versions, etc., to cover every eventuality. If you do not wish to practice with your personal device, simply read through the exercise. Devices that contain Mobile Device Management may not work for this exercise.

## Exercise - Section 1

1. Place device into Airplane Mode by swiping up from the bottom of the screen to expose the Control Center and tapping the Airplane button. (Some iPhone versions swipe down from top)
  - \* If the Control Center does not appear, the device may be configured to not show it unless the device is unlocked. If this is the case, unlock the device, and try again. If any other of the four round icons in the box are still on, tap on them to disable them. Bluetooth is a good example.



- a. Record the date & time device placed in Airplane Mode:
- 

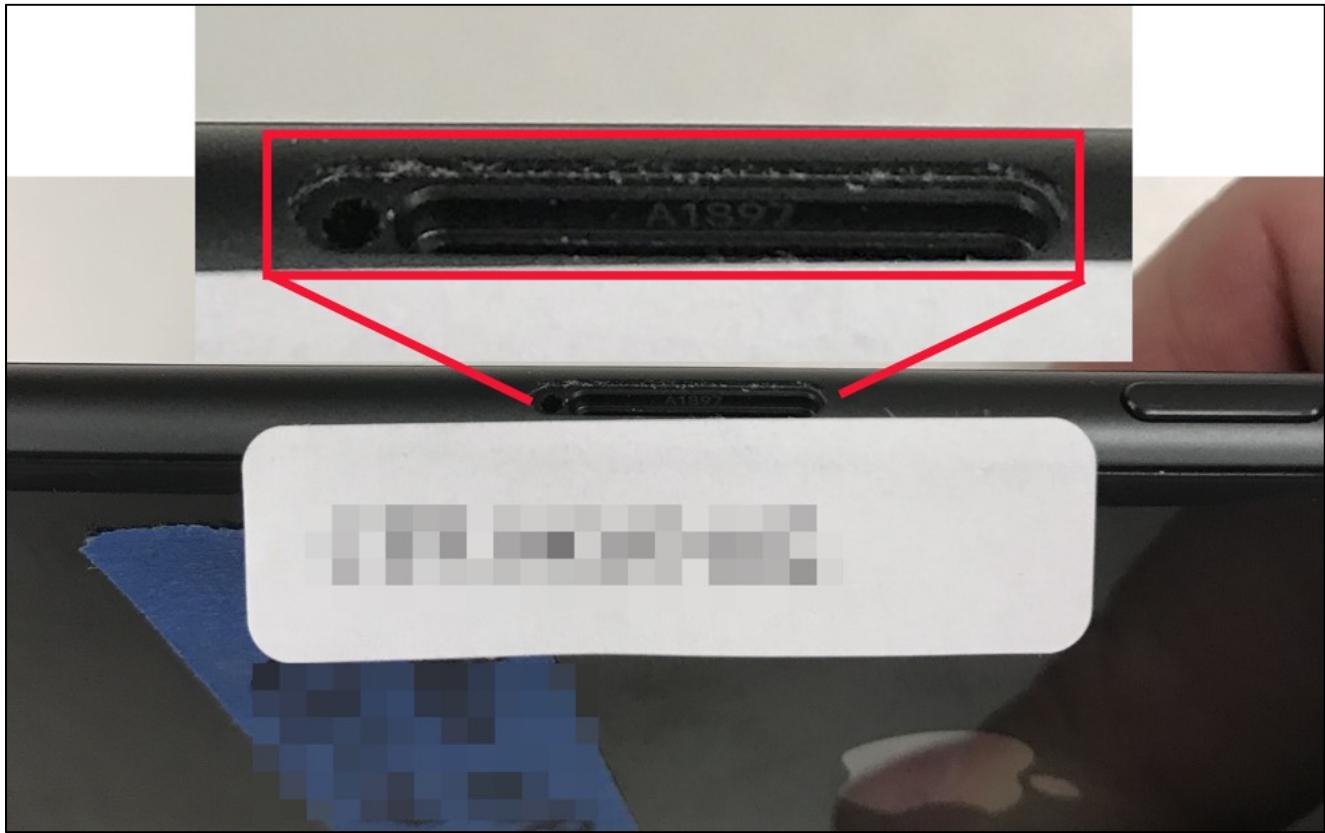
2. The first step to perform is evidence intake and identification. Turn the iPhone over and note details on the back side. In a real-world scenario, you would take a photo of the Model number. (in the case below, A1778). If your device is iPhone 8 or newer, this step will not work, as the information is not on the back. If that is the case, continue to step 3.



a. Record the device Model number:

- 
- On devices that are iPhone 8 and newer, there is no information on the back of the phone. The model number of the device is now printed inside the SIM card tray slot in the edge of the

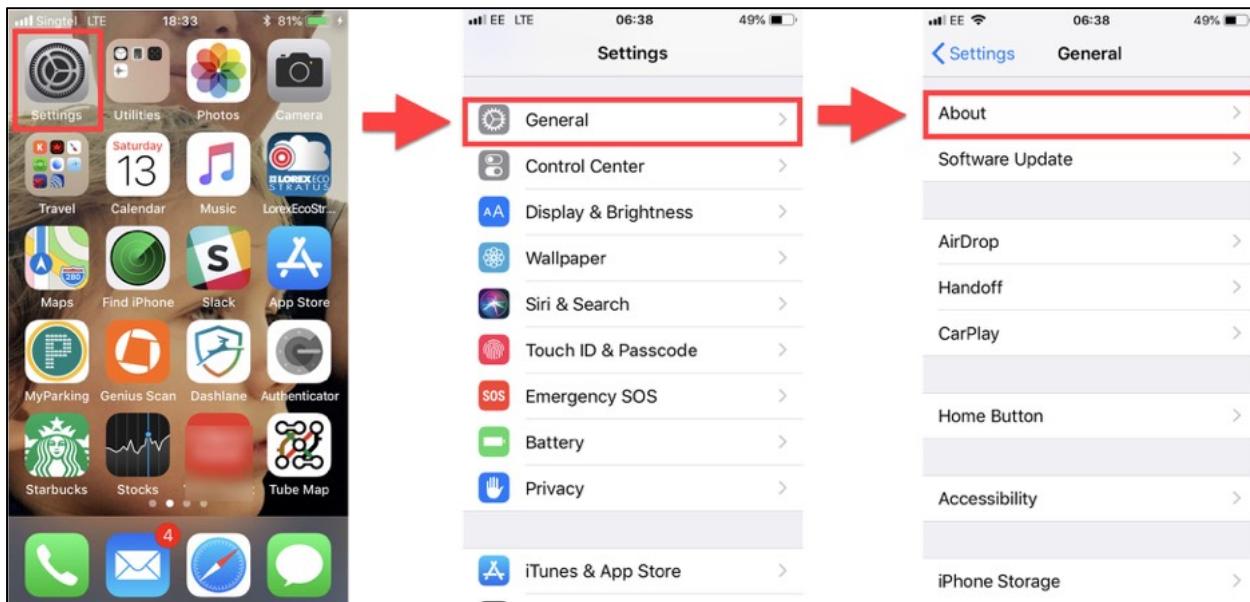
device. It is quite difficult to see with the naked eye. Typically, an examiner can take a photo with a flash, and then magnify the photo to read the model number.



- As for the IMEI, this is now etched directly on to the SIM card tray.



3. We may need to go one step further. This information does exist elsewhere. Although we must interact with the device to get the information, it is very necessary, because the acquisition equipment often will not specifically recognize the device, so we must have the information prior to performing the acquisition. We could follow these steps for most any model of iPhone, but we want to minimize our interaction with the device as much as possible.
4. In the case of iPhone 8 and newer, unlock the device, and then open the device settings by locating the “Settings” icon and tapping it. Select the “General” option, and then the “About” option.



5. Once within the “About” menu, you will collect the information as indicated, scrolling where necessary. You will note that the “Model Number” field has two values. The “Model Number” field in the left image shows a value of “MKQT2VC/A”, and the “Model Number” field in the middle image shows a value of “A1688”. Tapping the “Model Number” field will toggle between the two values, with the “A” value being the pertinent one for acquisitions.

11:20 AM 86% Name Kevin's iPhone > Software Version 13.3 Model Name iPhone 6s Model Number MKQT2VC/A Serial Number FK1 3RYG	11:21 AM 86% Name Kevin's iPhone > Software Version 13.3 Model Name iPhone 6s Model Number A1688 Serial Number FK1 3RYG	11:20 AM 86% Capacity 128 GB Available 116.04 GB Carrier TELUS 40.0 Wi-Fi Address B4:9 7:96:AC Bluetooth B4:9C:D 4:AD IMEI 35 54 4 2 ICCID 8912345678901234019 MEID 3554 584 Modem Firmware 7.30.02 SEID >
---	---	---

a. What is your device Name?

---

b. What is your device Version?

---

c. Who is your device Carrier?

---

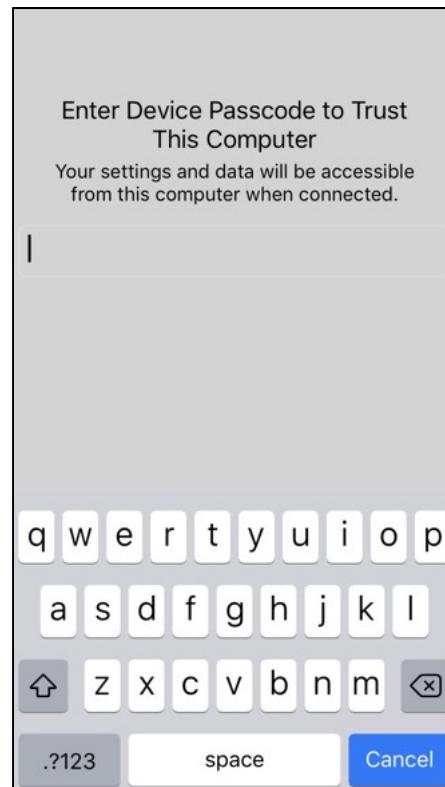
6. Ensure your **FOR498 Windows VM** is in full screen mode. If it is not, you may have connection issues when plugging a device in for analysis with the **VM**. The following screenshots refer to the use of **VMware Workstation** and **VMware Player**. For **VMware Fusion** users, jump to **step 11**.



7. Using your charging/data cable, plug your device into your computer. Your device may need permission to connect, via a message on the device screen asking you to unlock it. Below are just a couple of the

permission messages you may see. Follow the instructions on your device screen to cause the device to trust the computer.

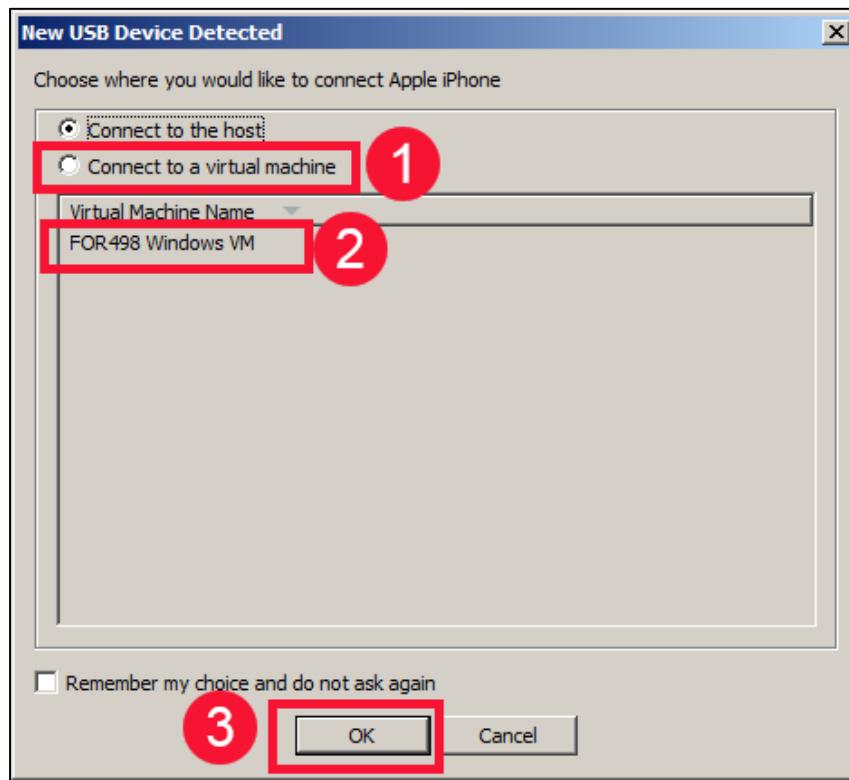
- It can not be overstated that you must watch the device screen. Often if the Cellebrite software does not seem to be working, it is attributable to the examiner not responding to a prompt on the device screen.



8. When you plug your device in, you will see either the window in **OPTION 1** below, or one of the two windows in **OPTION 2** below. Follow the instructions for your **OPTION** accordingly.

## OPTION 1

Once completed, go to **Section 2** of this exercise.

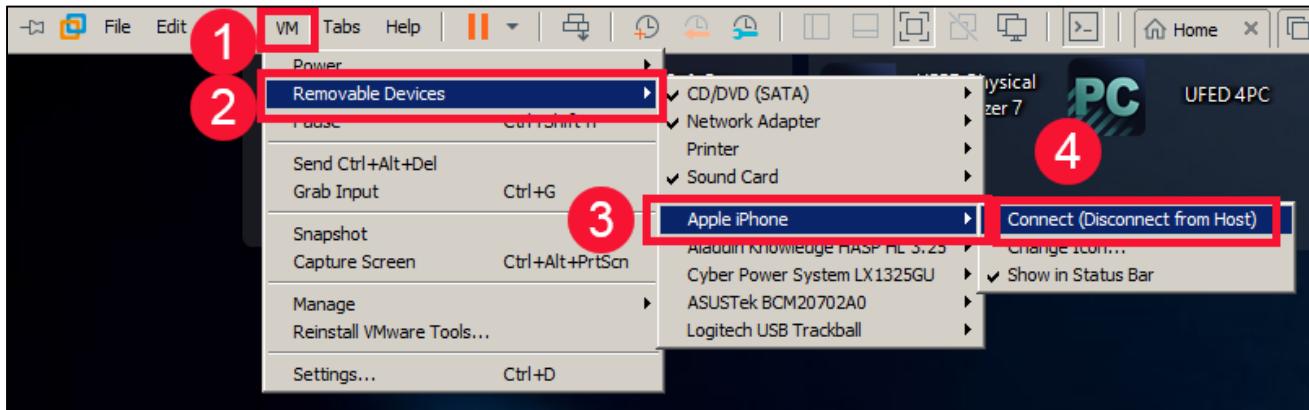


## OPTION TWO

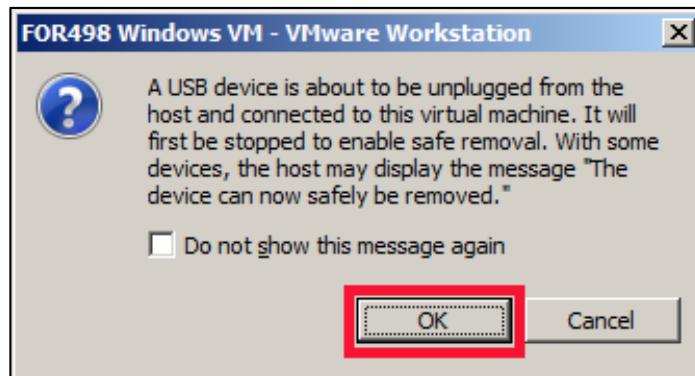
If you see **screen 1**, proceed to **Section 2** of this exercise. If you see **screen 2**, proceed to the next step.

SCREEN 1	SCREEN 2
<p>Removable Devices</p> <p>The following devices can be connected to this virtual machine using the status bar or choosing VM &gt; Removable Devices:</p> <p> Apple iPhone (connected to Windows)</p> <p>Each device can be connected either to the host or to one virtual machine at a time.</p> <p><input type="checkbox"/> Do not show this hint again</p> <p style="text-align: center;"><input type="button" value="OK"/></p>	<p>Removable Devices</p> <p>The following devices can be connected to this virtual machine using the status bar or choosing VM &gt; Removable Devices:</p> <p> Apple iPhone</p> <p>Each device can be connected either to the host or to one virtual machine at a time.</p> <p><input type="checkbox"/> Do not show this hint again</p> <p style="text-align: right;"><input type="button" value="OK"/></p>

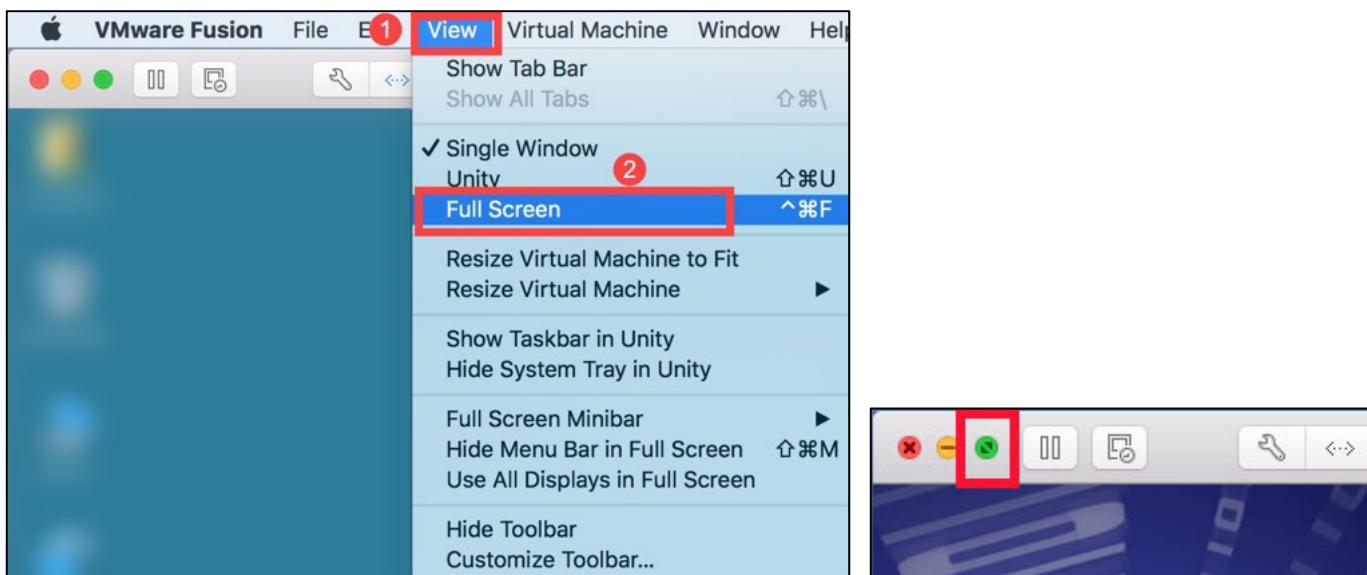
9. In the case of **screen 2**, the device has been ‘captured’ by the host computer rather than the **VM**, so you must tell the **VM** to take control of the device. Within the **VM**, click on **VM -> Removable Devices -> Apple iPhone -> Connect (Disconnect from Host)**.



10. You may receive a pop-up confirmation. Click **OK**. Proceed to **Section 2** of this exercise.



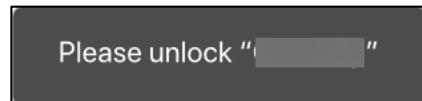
11. For **VMWare Fusion** users, ensure your **FOR498 Windows VM** is in full screen mode. If it is not, you may have connection issues when plugging a device in for analysis with the **VM**. You can place your **VM** into full screen mode by either one of the two methods below.



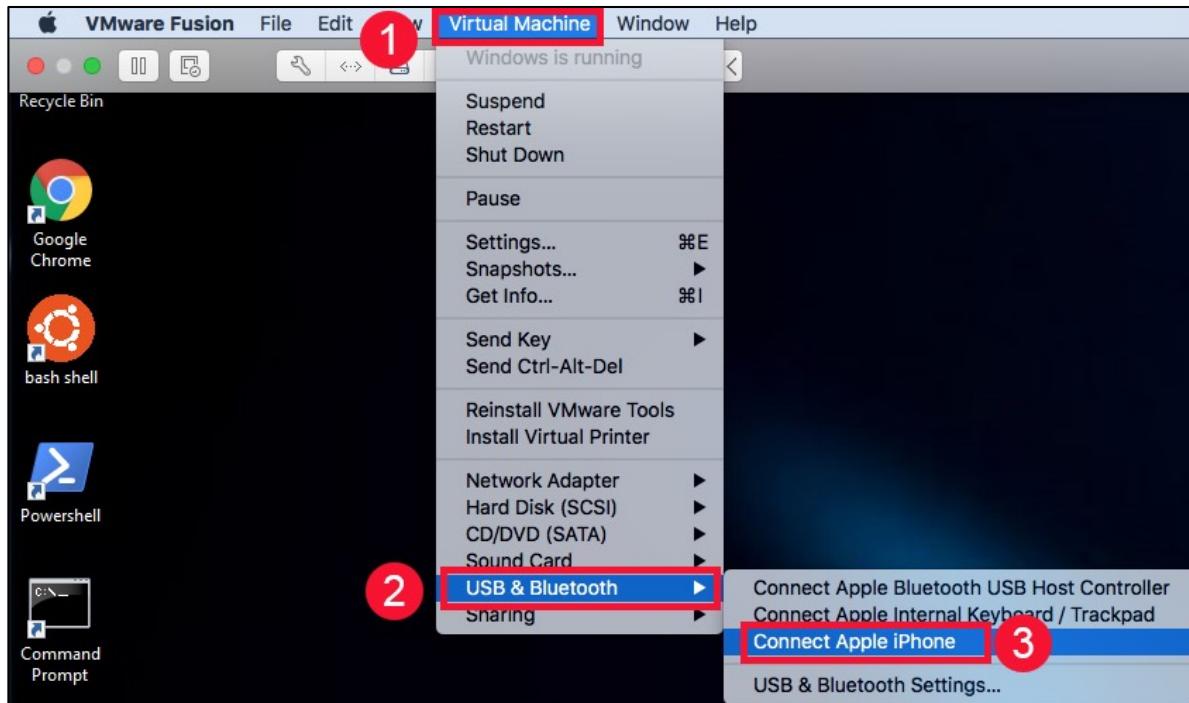
12. Using your charging/data cable, plug your device into your computer. Your device may need permission to connect, via a message on the device screen. Follow the instructions on your device screen to cause the device to trust the computer.
13. When you plug your device in, a box will appear asking where you want your device to connect. Select “**Connect to Windows**”, to connect the device to your **FOR498 Windows VM**. If there is an issue getting your device to connect, go to **HOST** System Preferences -> Security and Privacy -> General, and allow VMWare.



14. You may see another pop up triggered by your device asking you to unlock it.



15. If you do not see the previous pop-ups when attaching the iPhone to the VM, you need to attach it manually. Within the VM, click on **Virtual Machine** -> **USB & Bluetooth** -> **Connect Apple iPhone**.



16. If you receive any confirmation prompts, read them carefully before accepting them, and understand what they are asking for.

## Exercise - Section 2

1. Start the **UFED Physical Analyzer (PA)** application by double clicking the icon in the **Forensic Suites** box on your **Desktop**. This program takes a few seconds to open, so be patient. Note that you do NOT want two instances opening!

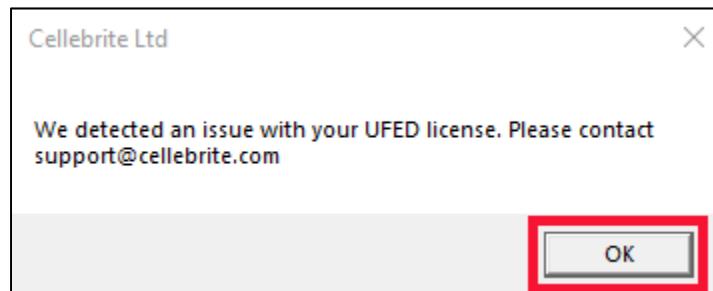


2. After a few seconds where it will appear that nothing is happening (BE PATIENT), a splash screen will appear.

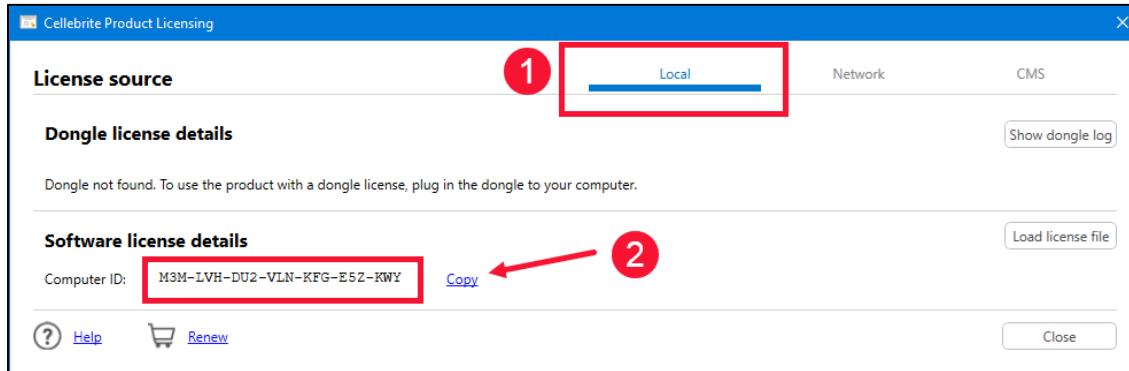


**NOTE:** You may be prompted to update **Physical Analyzer**. If the currently installed version of Cellebrite does not support the collection of your particular device, we recommend updating the software OUTSIDE CLASS. If the currently installed version is able to collect your phone, please avoid updating until after you have completed the class. Updating is optional and may “break” the functionality of the tool in regards to the other Cellebrite-based exercises in this class. Updating is at your own risk. The currently-installed version has been tested and confirmed to work with the remaining exercises! You will license the other tools right before they are needed in each lab. **Do not change any VM settings after licensing Cellebrite or your license may no longer work!**

3. If you get a pop up message during startup of the program, as indicated below, simply click **OK**, and the program will continue to load.



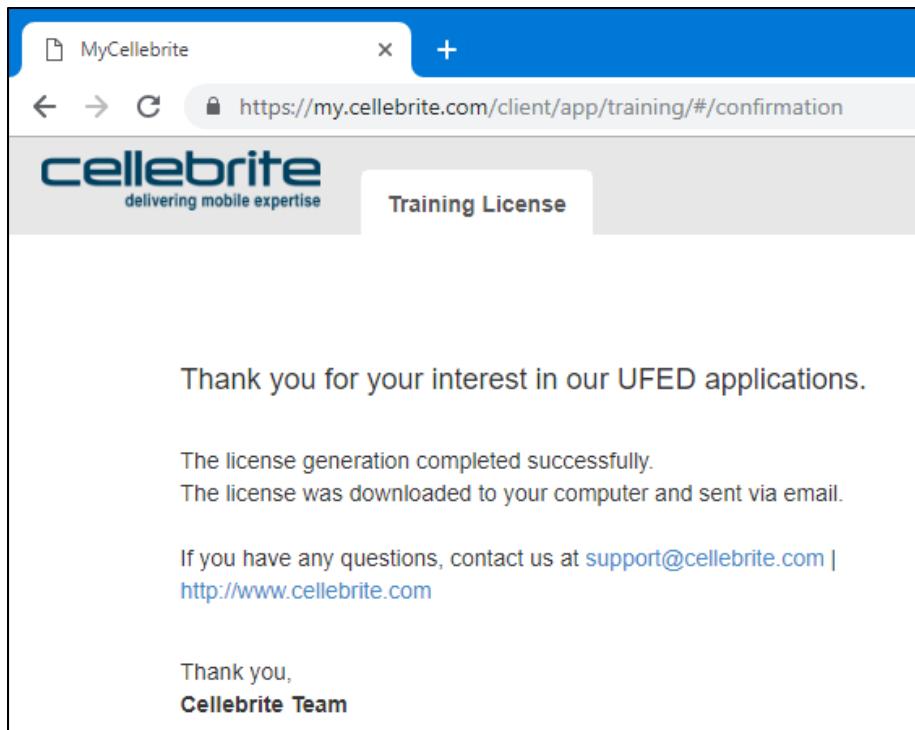
4. The prompt below pops up in **Physical Analyzer** when the tool launches. Copy your **Computer ID** from **Physical Analyzer**. Ensure the Local button is selected. If the prompt does not appear, select **Help > Show License Details**.



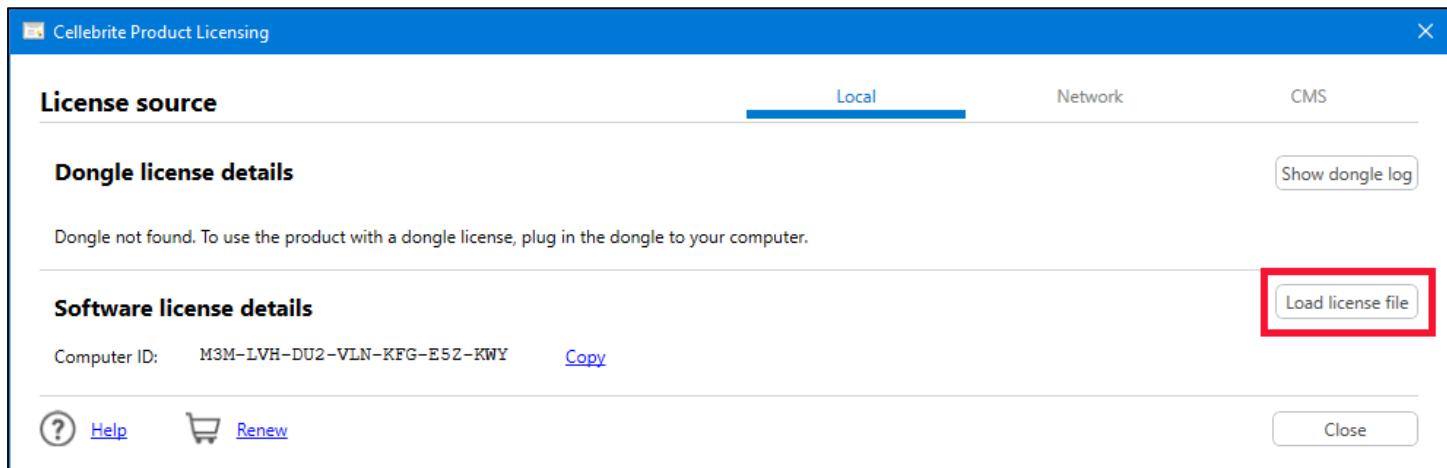
5. Open a browser window, go to <https://my.cellebrite.com/training> and fill out the required fields to receive your license file for this course. **NOTE: Do not provide your real information unless you want to be contacted by the Vendor. A fake email account is enough to get you a license. Feel free to use your own information if you already have an account with Cellebrite or plan to use any support.** (NOTE: The Activation Code is provided by SANS or the instructor. If you are an OnDemand student, please request the code by emailing online-sme@sans.org. The Computer ID is copied from UFED Physical Analyzer, as shown above.) Make sure you select something from each drop-down option, or you cannot proceed. Once everything is filled in, click **Generate License**.

The screenshot shows the 'Training License' page. It has fields for Primary Email (eaf@joes.com), First Name (Bilbao), Last Name (Baggins), Company (Acme), Phone (8085551212), Country (United States), State (California), City (Beverly Hills), Address (123 Anywhere Street), and Zip Code (90210). At the bottom, there are two input fields: 'Activation Code\*' (with placeholder 'Enter what SANS or instructor has provided') and 'Computer ID\*' (with placeholder 'Copy from the screen in UFED Physical Analyzer'). A red box highlights both these fields, and a red number 1 is circled around the 'Activation Code' field. A red arrow points from the 'Computer ID' field to a 'Copy' button (labeled with a red number 2) located at the bottom right of the page.

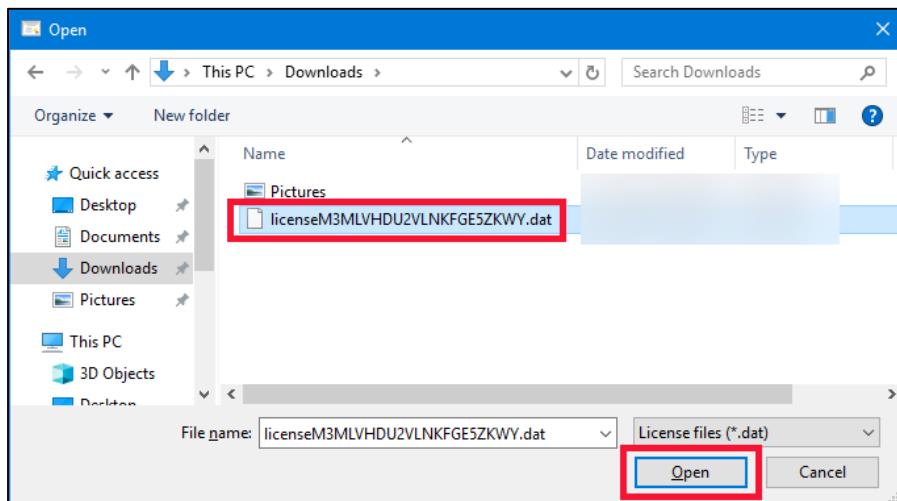
6. Your license should appear at the bottom of your screen after a minute. Select **Save** and the license file will be saved to your **Downloads** folder. In some cases, this has happened automatically.
7. When this is done, it will be indicated by a thank you message from Cellebrite. Close the browser window.



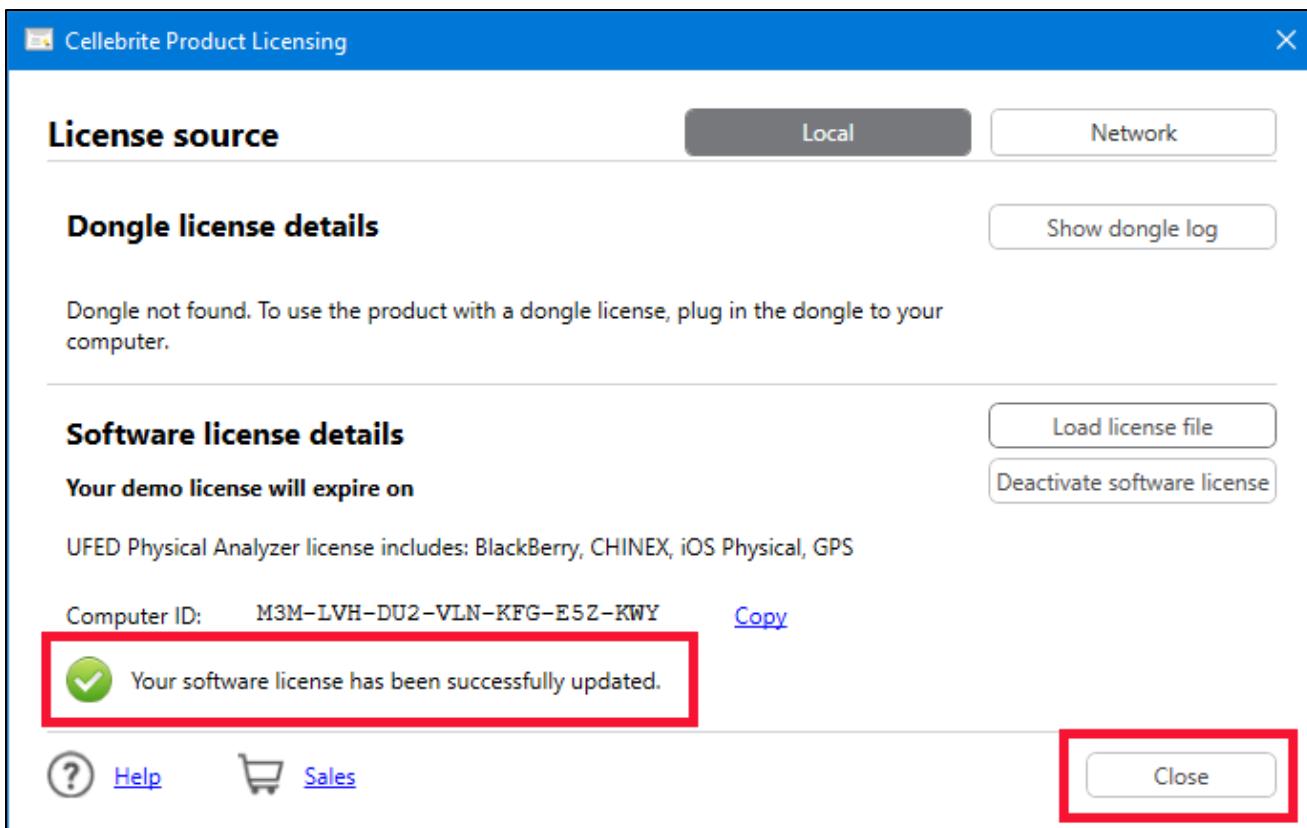
8. Go back into **Physical Analyzer** and select **Load license file**.



- A directory window will open. Navigate to your **Downloads** directory and select your **licenseXXX.dat** file and then click on **Open**.

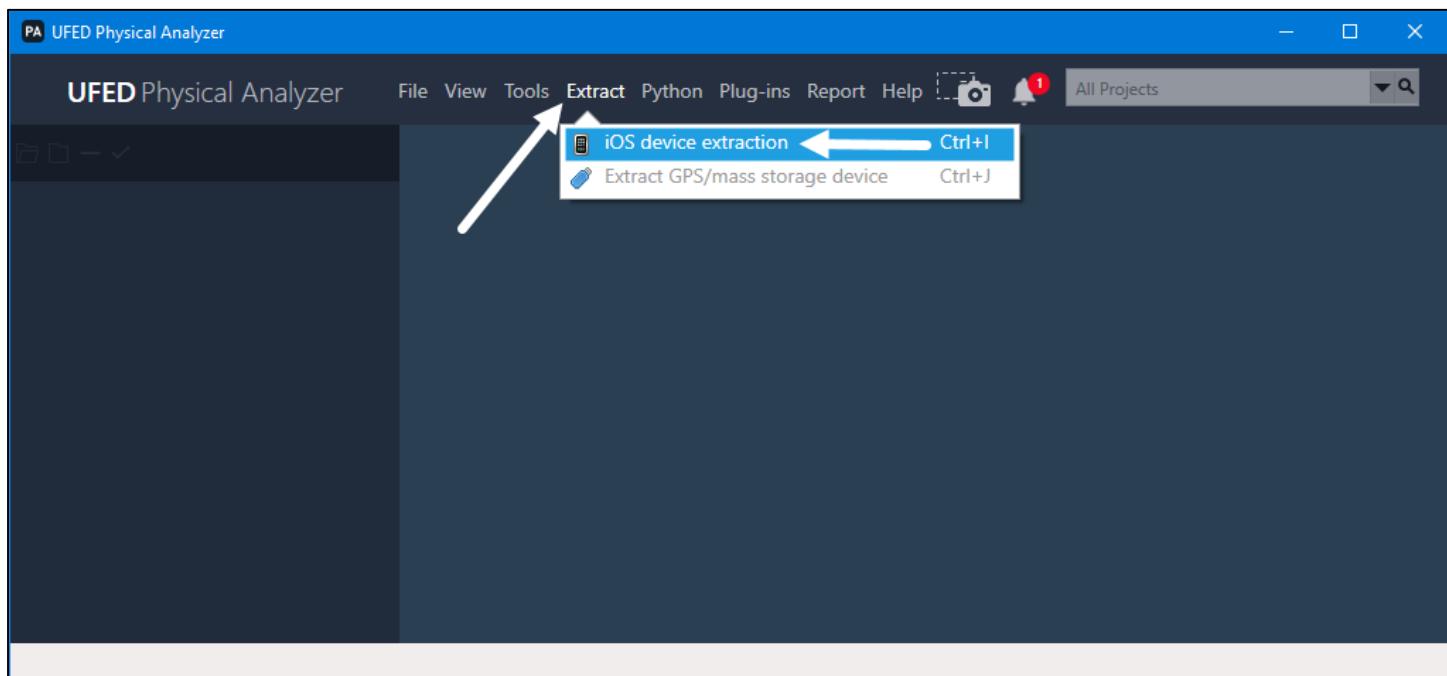


- Once done, you will see the **Product Licensing** window again. Note that the software license is now active. Click the **Close** button.

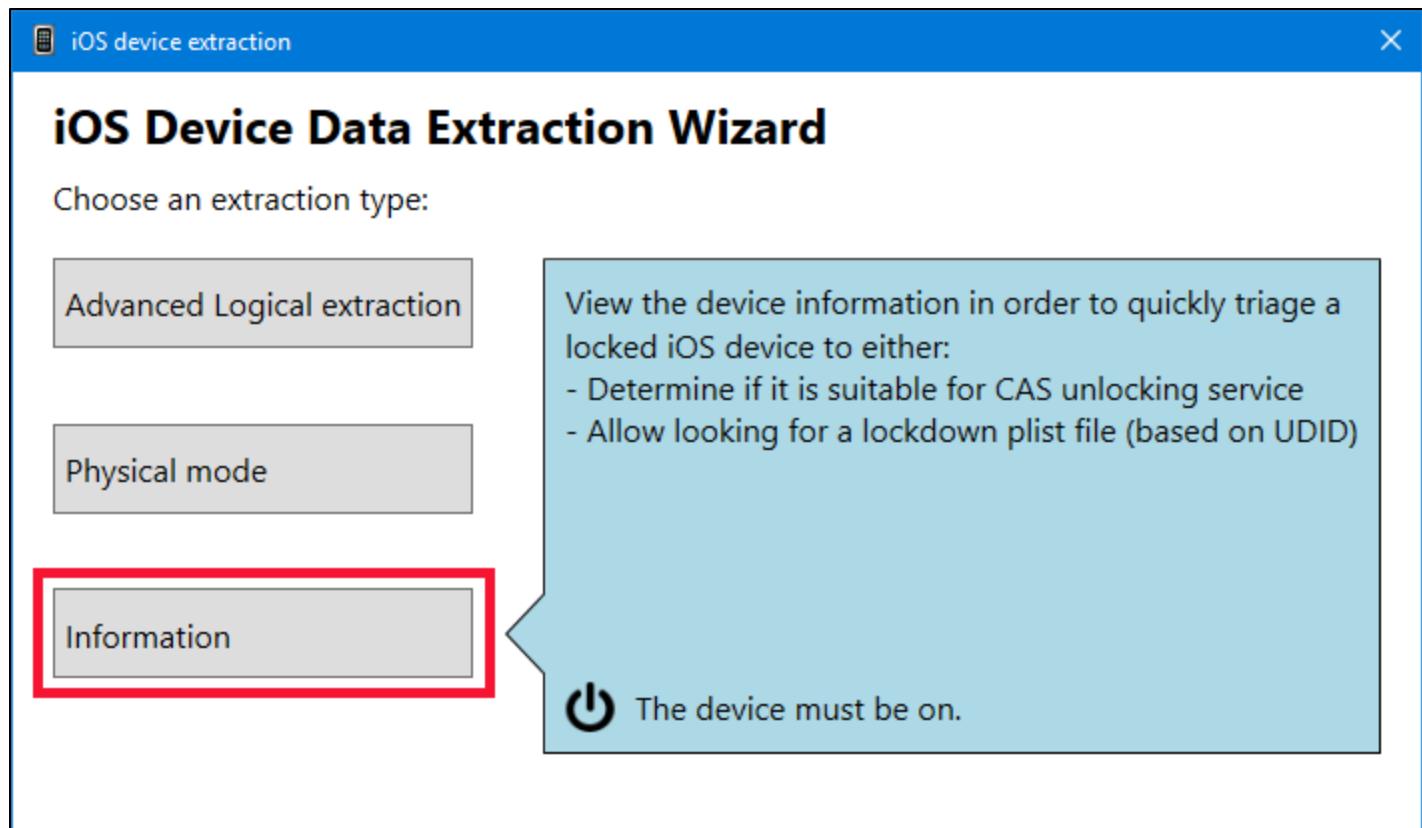


- You will now see the **Physical Analyzer** program open.

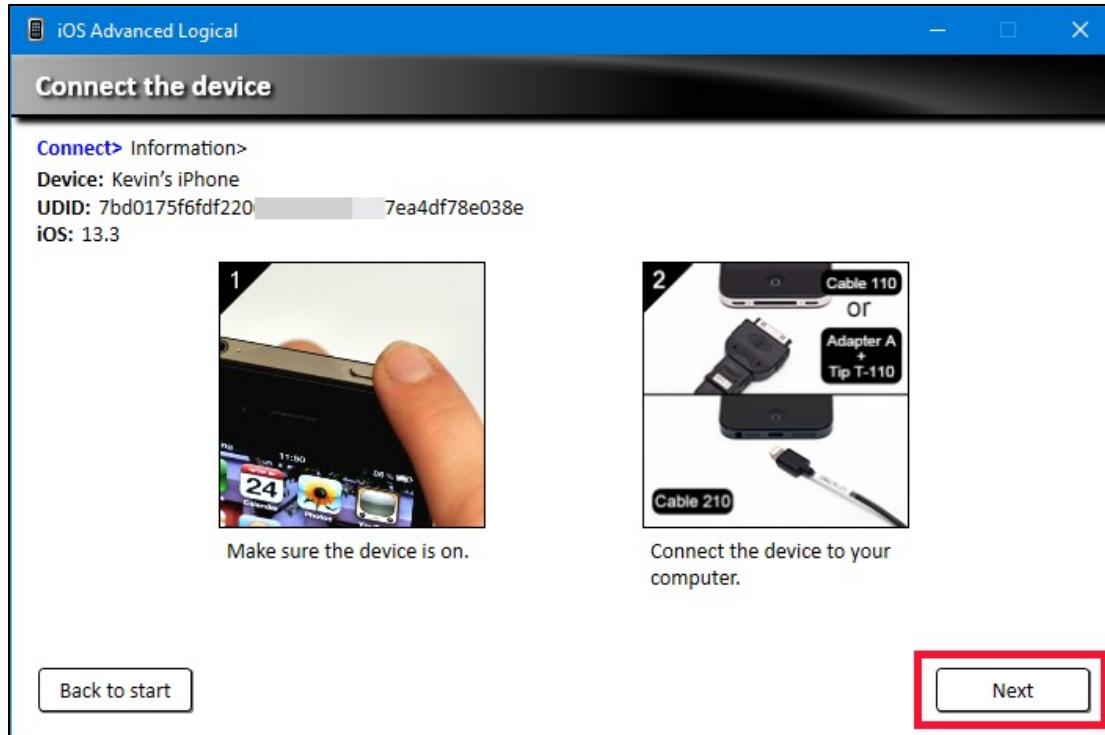
12. We are ready to initiate the collection process. You will now be at the **Physical Analyzer** main screen. Below, the **Extract** menu is shown. Click on this, and then select **iOS device extraction** from the drop-down menu.



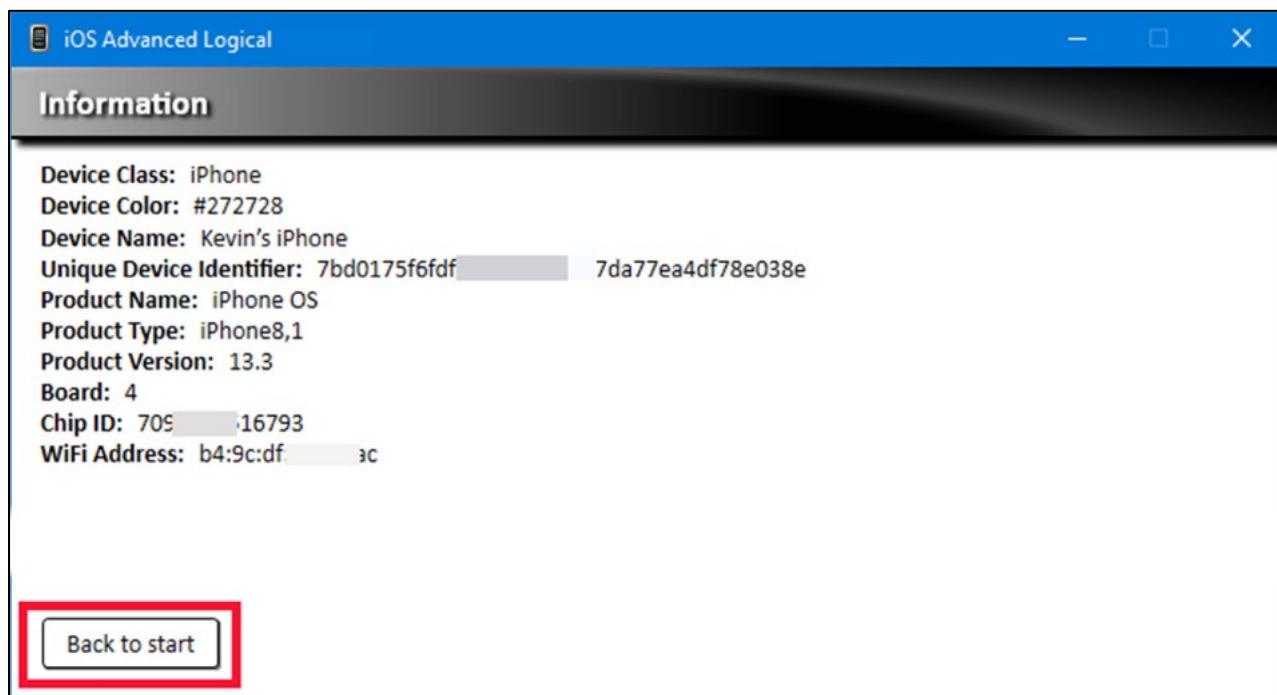
13. The **iOS Device Data Extraction Wizard** appears and shows three options. Select the **Information** tab.



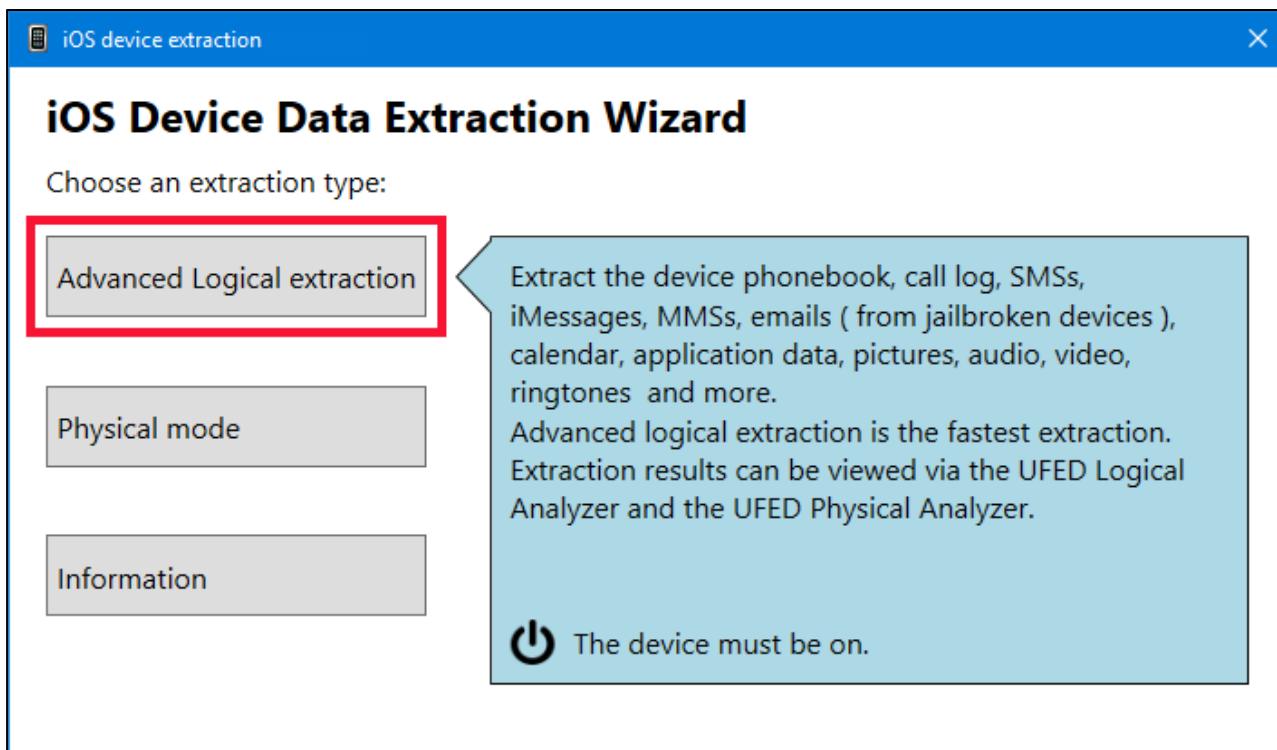
14. The screen will display the device that is connected, along with the **UDID** and **iOS**. It is a great idea to photograph this, during the collection process. Often the Device name is not included in the more detailed information screen that follows. We collect this data in an abundance of caution. As well, if the device has been factory reset, this is the only data available without interacting with the device. Once done, click **Next**.



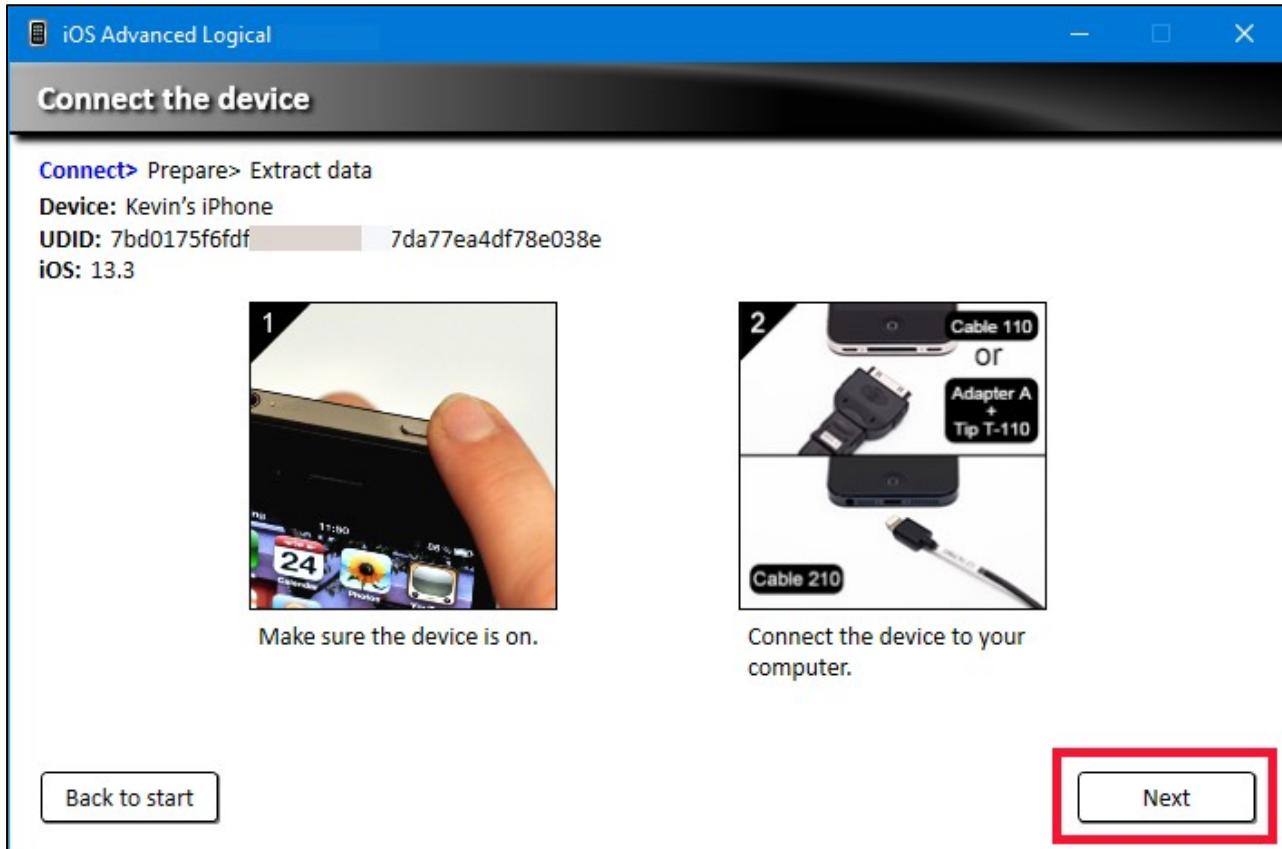
15. The **Information** screen appears and contains more in-depth information about the device. Again, it is a great idea to take a picture of this screen. Then click **Back to start**, and then **Back to start** again.



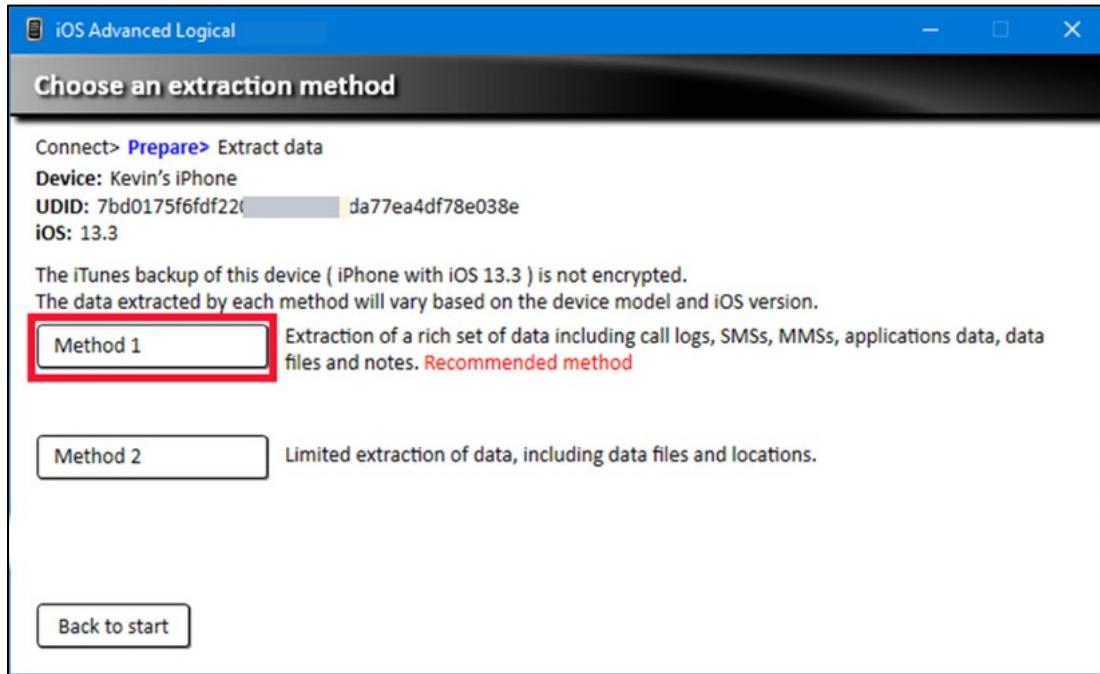
16. You should now have arrived back at the initial **Wizard** screen. This time, click on the **Advanced Logical extraction** option.



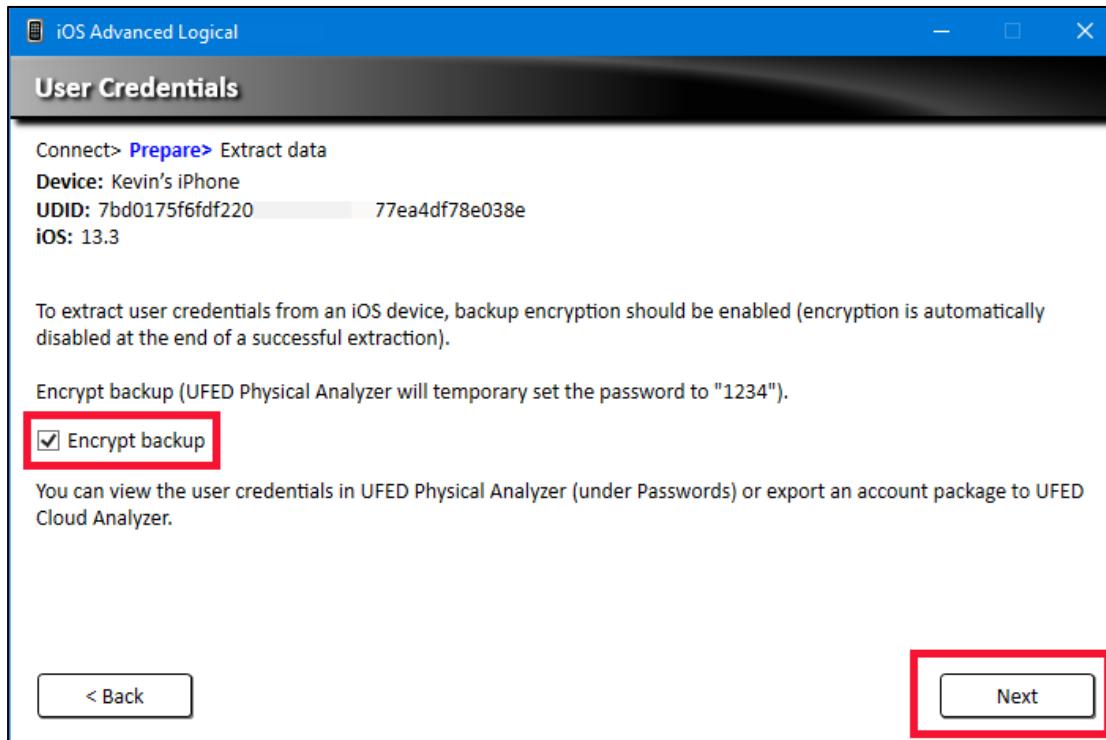
17. Once again, the **Connect the device** screen will appear. Click **Next**.



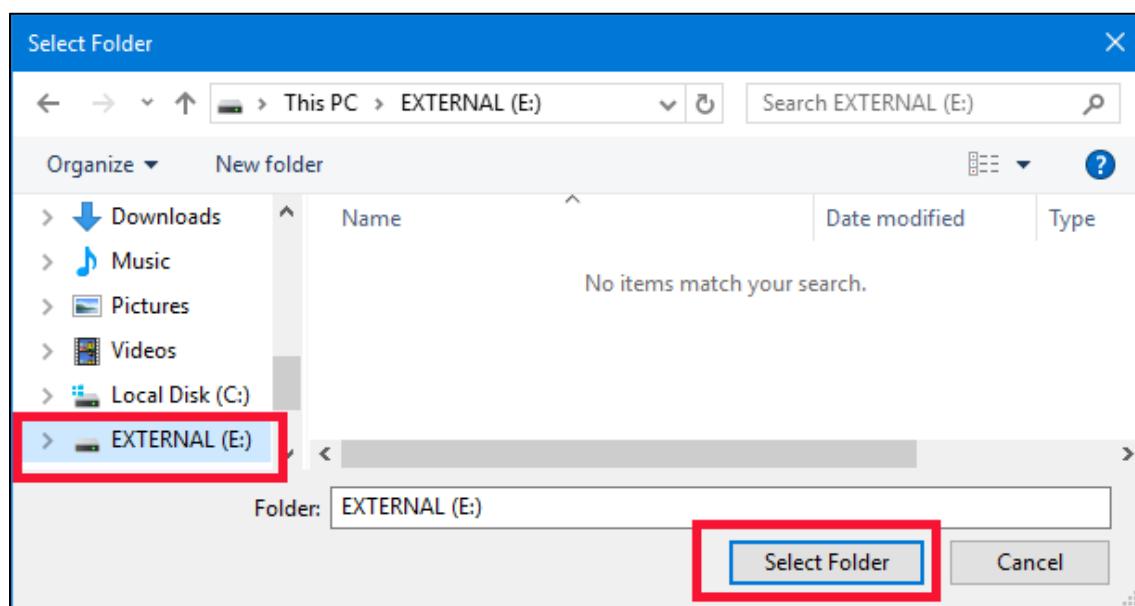
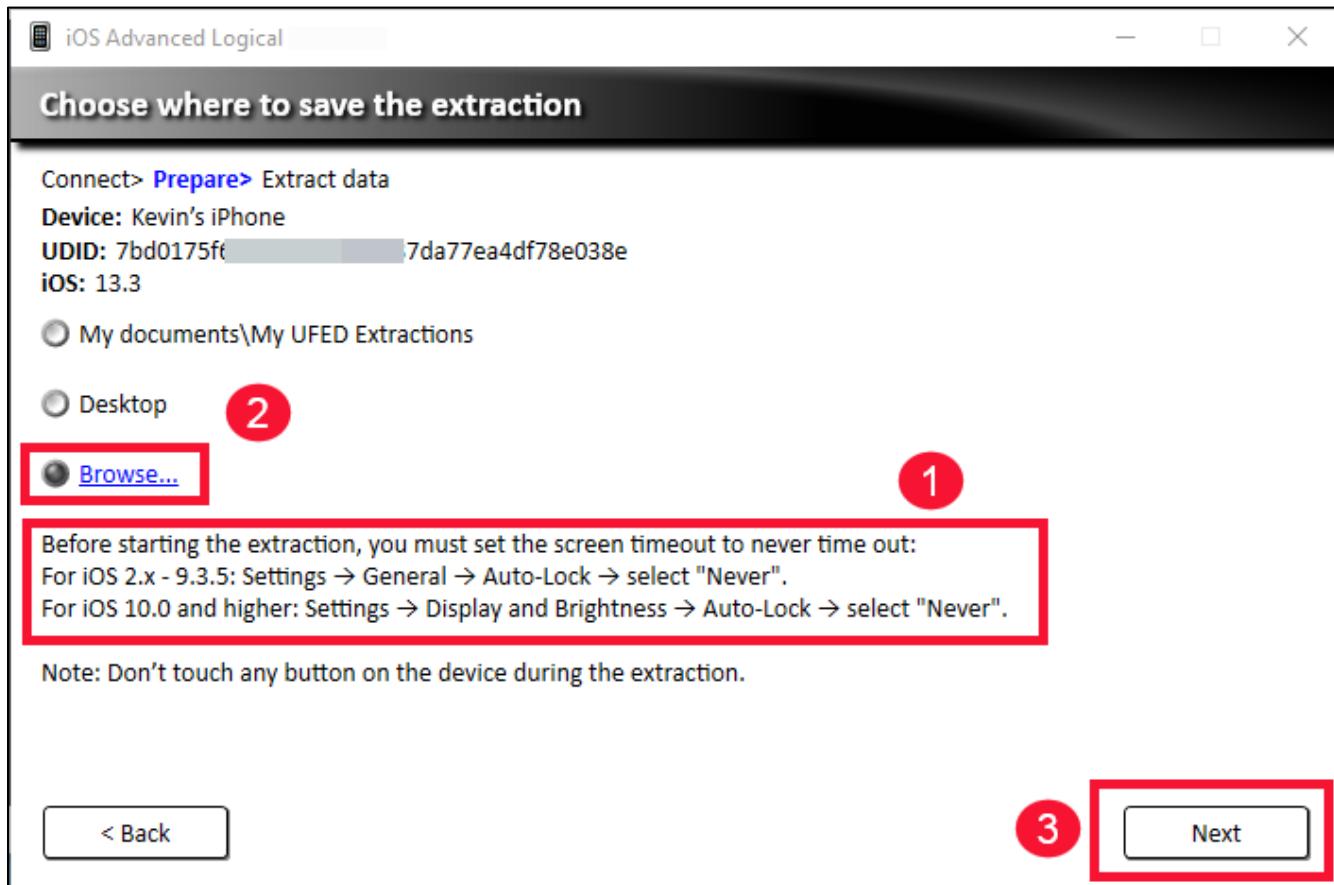
18. Choose the extraction method to use. Typically, you will select **Method 1**, as it gets a more complete extraction, including some deleted data. Having said that, if the device has ever been backed up to a computer or the cloud, and a backup encryption password was set at the time, you will need it after the acquisition, or you will not be able to mount the complete collection. This is NOT necessarily the same password as the password that accesses the device.



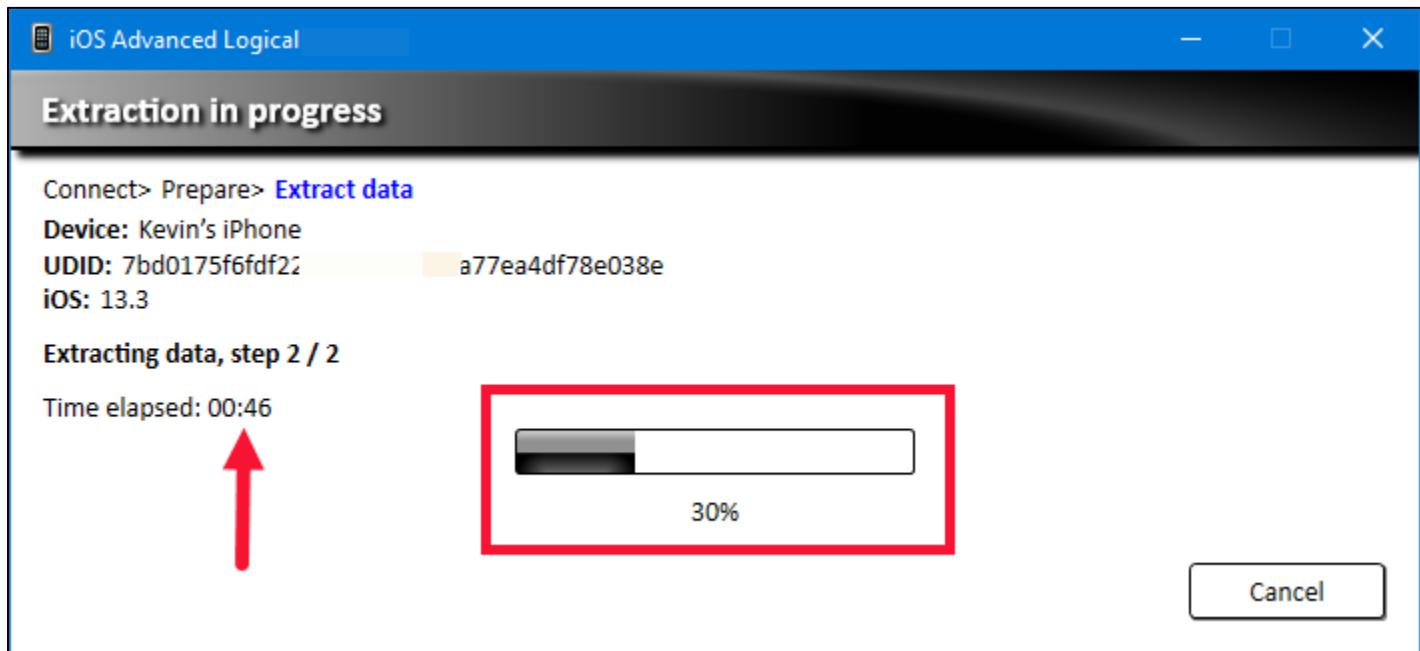
- If a backup has never been created, or was never encrypted at the time of encryption, you will be notified that **Physical Analyzer** will set a temporary password of **1234**. Check the **Encrypt backup** box, and then click **Next**. If an encrypted backup password has been previously set, you will not see this screen.



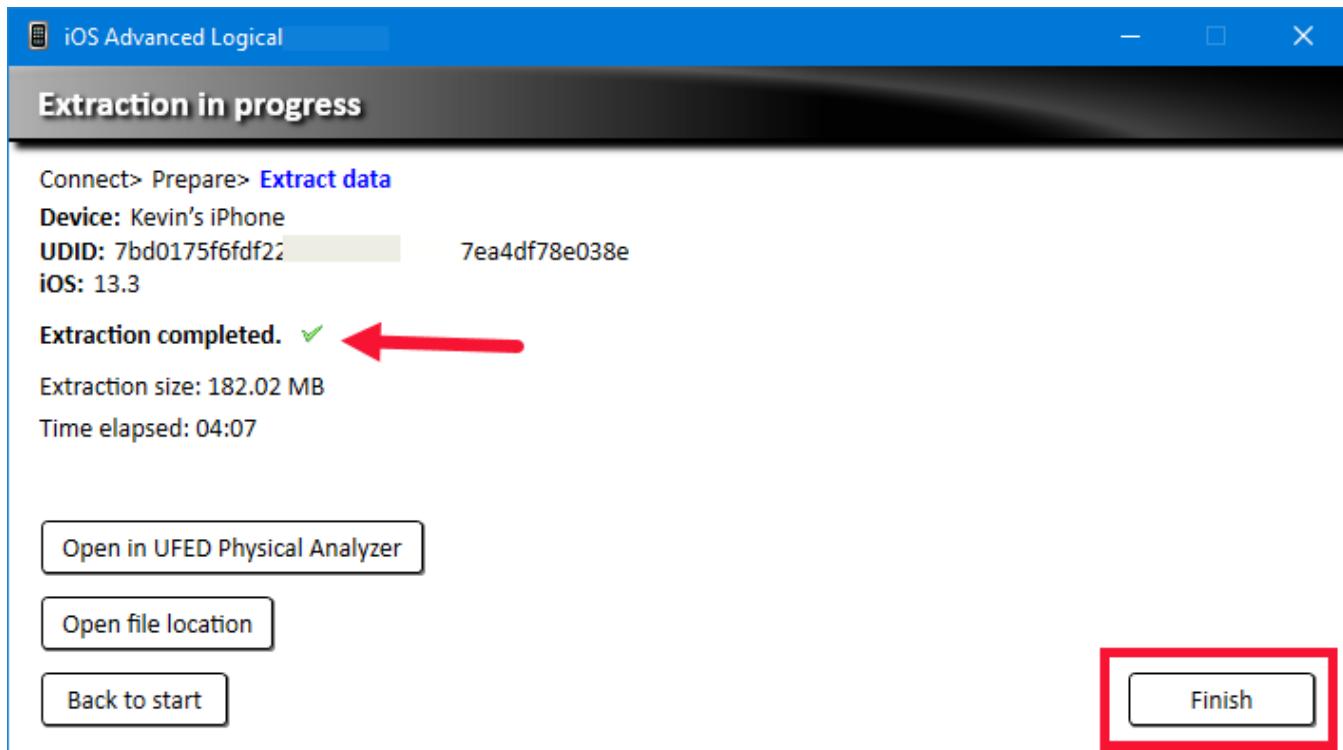
- In the next box, you will follow the instructions to perform on your device, as shown in **step 1** below. You will be asked where to save the extraction. Connect your student supplied external hard drive to your **FOR498 Windows VM**, then click **Browse...** and save the extraction to the root of your external hard drive as shown below. Click **Next**.



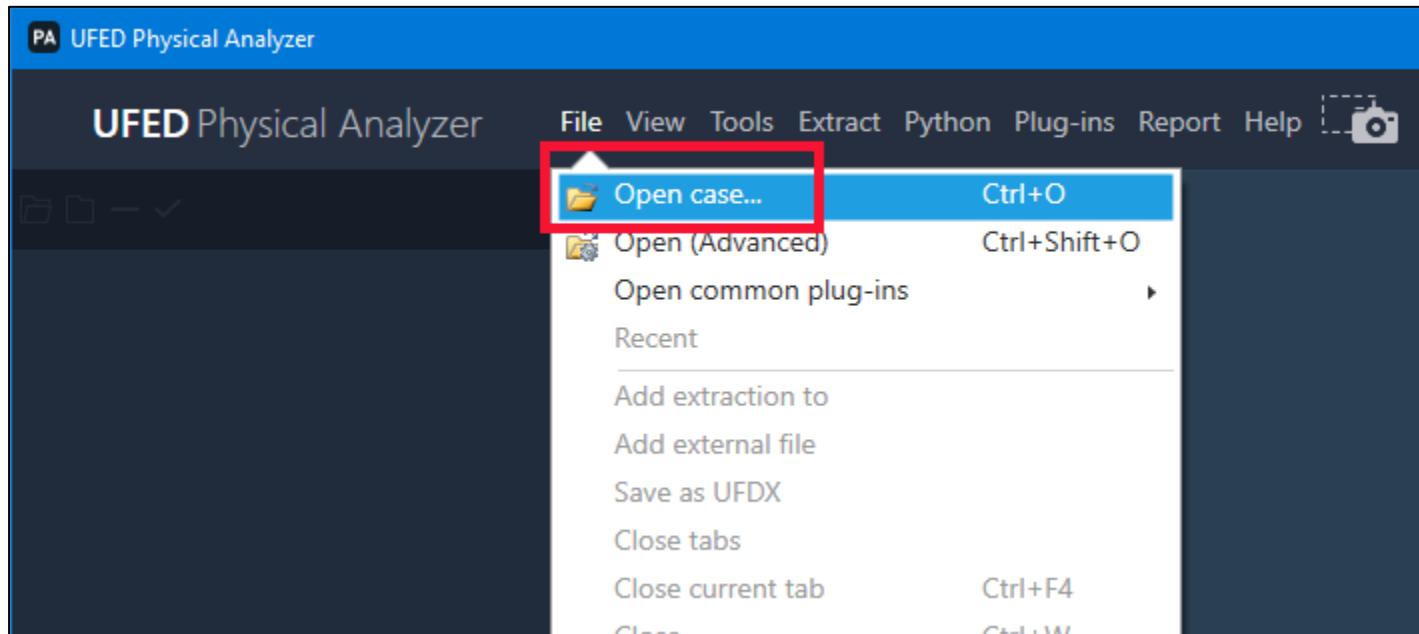
21. The extraction process will begin, and you will be able to see the **Time elapsed**, as well as a progress bar. Double check your device, as you may need to enter the passcode again. The storage size of the device, and the amount and density of the data will dictate how long the process will take.



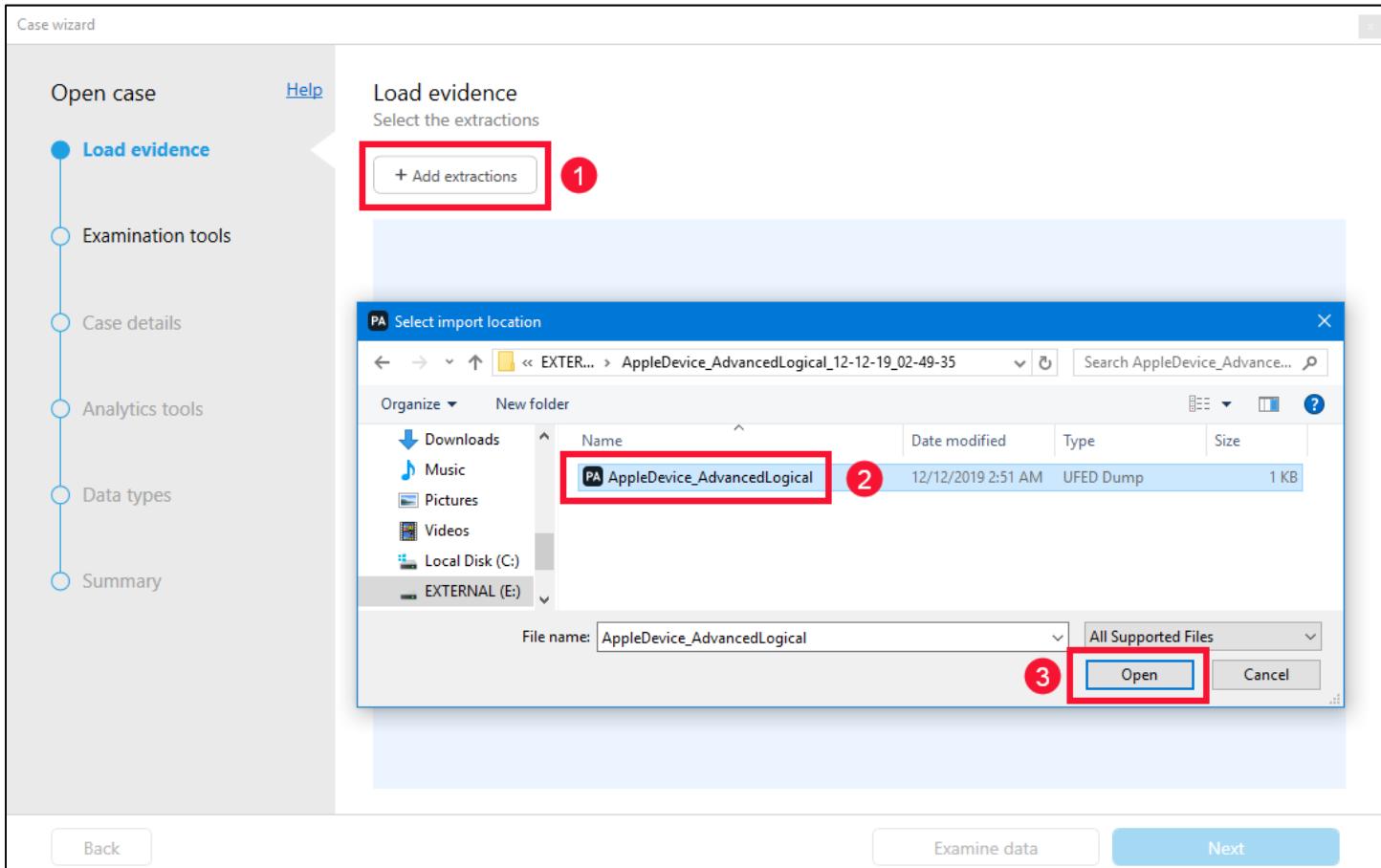
22. In certain unexplained circumstances, the progress bar will reach 100% and the time will still be running, but with no discernable activity. Double check that it is not waiting for the passcode again. After 3-4 minutes with the progress bar at 100%, but with no activity, press the **Cancel** button. The collection will have completed, but the **Extraction completed** screen will not appear. After pressing **Cancel**, proceed to **step 23**. Otherwise, the **Extraction completed** screen will appear. Click on **Finish**.



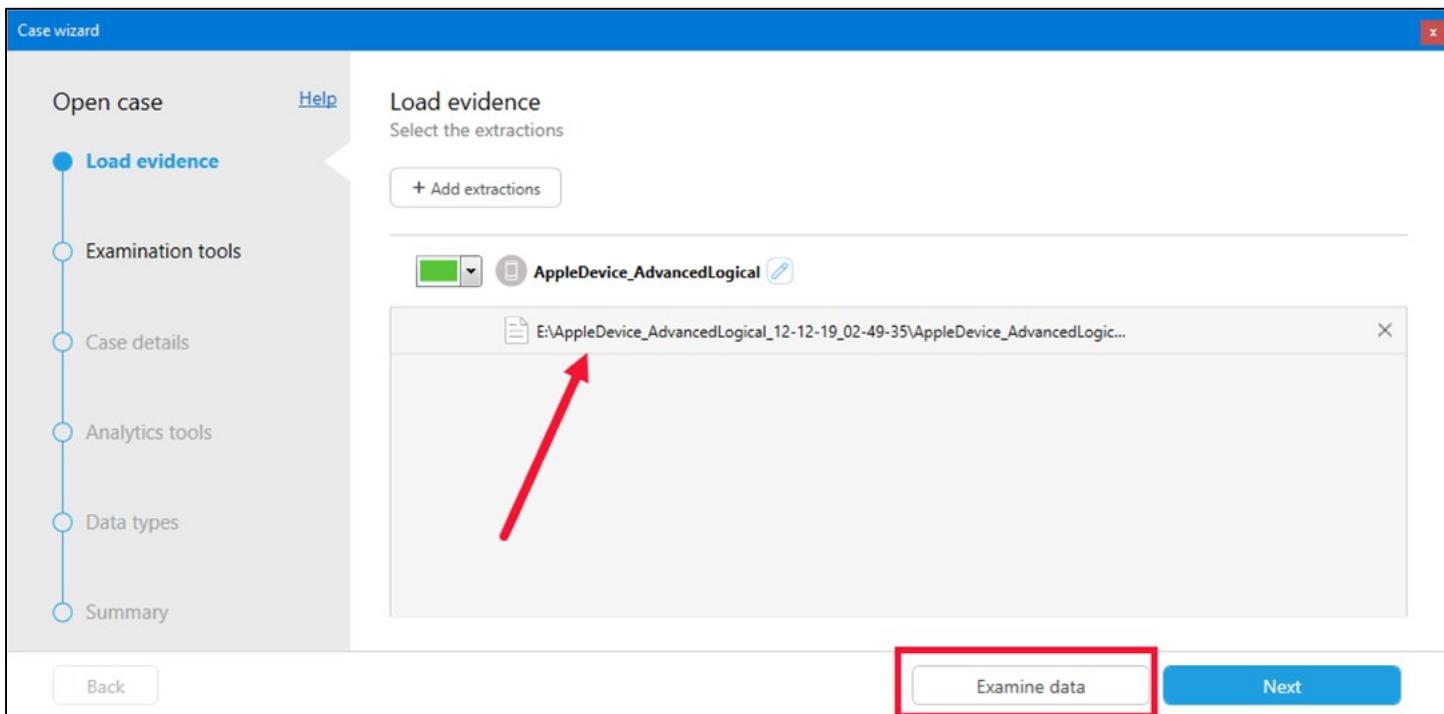
23. You should now be back at the **UFED Physical Analyzer** start screen. Click on **File → Open case...**



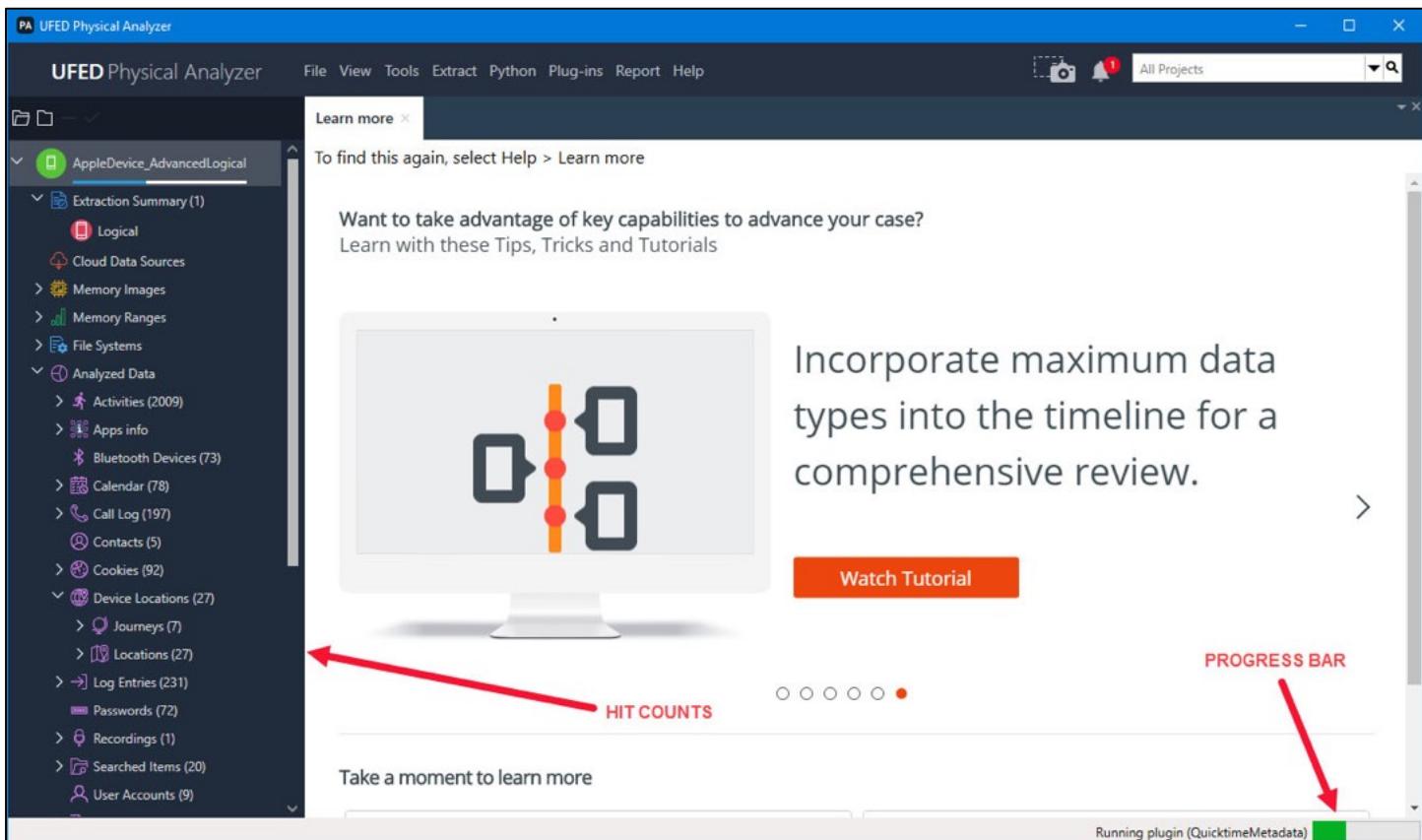
24. The **Case wizard** window will open. Click on the **+ Add extractions** button, navigate to your external hard drive, and locate the files you created, probably inside a folder entitled **AppleDevice\_AdvancedLogical\_<date>**. Locate the file entitled **AppleDevice\_AdvancedLogical.udf**. Select it and click **Open**.



25. The path to the collected data will now be visible in the **Case wizard** window. Click on **Examine data**.



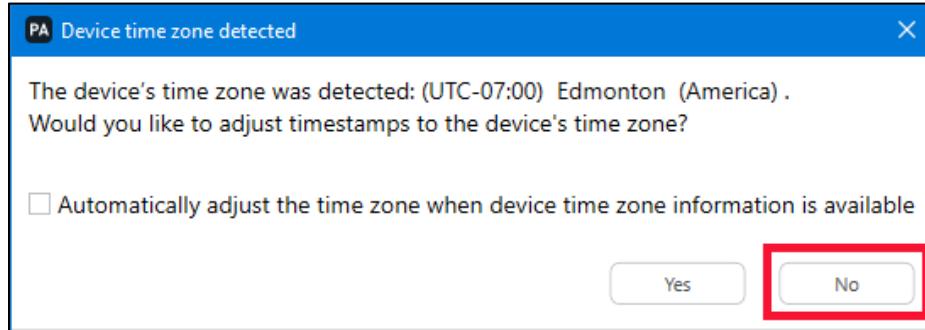
26. **UFED Physical Analyzer** will now start parsing the collected data, and you should see hit counts appearing in the left-hand column, as well as a progress report in the bottom right corner of the window.



- If the device previously had an encrypted backup created, you will receive a prompt at the beginning of the parsing process, asking for the password. If you do not have it, you cannot proceed further with this type of analysis.



- A box asking about the device time zone will appear. For the purpose of our exercise, select **No**.



29. Once the parsing process is complete, various pop-up boxes regarding enrichment of location data and others may appear. Simply click **Skip** or **No**.

30. Once the parsing is complete, you will see the **Extraction Summary**. The left column will show all artifacts collected. There will be a number in gray and sometimes a number in red. The number in red is the number of artifacts that were deleted but have been recovered. The recovered artifacts may be of little to no value, but they could also be critical. Double clicking on any given list item will show its artifacts in the main window under a new tab.

The screenshot shows the UFED Physical Analyzer software interface. The top navigation bar includes File, View, Tools, Extract, Python, Plug-ins, Report, Help, and a notification icon with a red '2'. The main window title is 'UFED Physical Analyzer'.

The left sidebar displays a tree view of the project structure:

- AppleDevice\_AdvancedLogical**
  - Extraction Summary (1)
    - Logical
    - Cloud Data Sources (0)
  - Memory Images
  - Memory Ranges
  - File Systems
  - Analyzed Data
    - Activities (2099)
    - Apps info
    - Bluetooth Devices (73)
    - Calendar (78)
    - Call Log (197)
    - Contacts (5)
    - Cookies (92)
  - Device Locations (27)
    - Journeys (7)
    - Locations (27)
  - Log Entries (231)
    - Passwords (72)
  - Recordings (1)
  - Searched Items (20)
  - User Accounts (9)
  - Web Bookmarks (7)
  - Wireless Networks (14)
- Data Files
  - Audio (1)
  - Configurations (736) (3)
  - Databases (74)
  - Images (281)
  - Text (2)
  - Videos (29)
  - Uncategorized (178)
- Carving
  - Images
  - Timeline (5754)
- Watch Lists
- Malware scanner
- Hex Tags (0)
- Tags (0)
- Reports

The central area is titled 'Extraction Summary (1)' and contains tabs for 'All Content' (selected) and 'Logical'. Below this is a summary section with a heading 'Extractions: 1' and a preview of a logical extraction for an Apple iPhone 6s. The preview shows the device image, extraction method (Logical [Method1]), start and end times, and the path E:\AppleDevice\_AdvancedLogical\_12-12-...

The 'Device Info' section lists various device details such as AirDrop ID, Apple ID, iCloud account present, Phone date/time, ICCID, IMEI, IMSI, Last user ICCID, Last used MSISDN, MSISDN, and Kevin's Phone information like Activation State, Baseband version, Bluetooth device address, Detected Phone Model, and Unique ID.

The 'Device Content' section lists categories with their counts: Activities (2009), Bluetooth Devices (73), Calendar (78), Call Log (197), Contacts (5), Cookies (92), Device Locations (27), Installed Applications (452), Log Entries (231), Passwords (72), and Recordings (1).

a. How many of all types of **Chats** do you have?

---

b. How many of all types of deleted **Chats** do you have?

---

c. How many resident entries do you have in your **Call Log**?

---

31. Spend some time clicking through a few of the entries in the left column to see the visible data from your device. Pay particular attention to some of the deleted activity. You may be surprised at what you see!

## **Exercise—Key Takeaways**

- There are many “quick wins” in the easily available data from a portable device.
- In an investigation where time is of the essence, much of the most important data can be quickly and easily obtained, provided you know the credentials of the device.
- With these easily obtained gains, you can further your investigation to the next stage, while lab analysis is carried out, rather than afterwards.

## Exercise 2.1B-Portable Device Acquisition-ANDROID

### Background

The most ubiquitous personal electronic device today (by far) is the smartphone. In criminal investigations, law enforcement is seizing these devices in unprecedented numbers. In fact, some law enforcement agencies have acquisition devices embedded in response units, so they can be on scene rapidly, not unlike K-9 and other units. Various units of the military are seizing devices from locations in combat theaters, and acquisition and analysis need to be done rapidly. On the civilian side of things, acquisition devices are seen to a lesser degree, but occurring more frequently, as employees are expected to be continually connected.

There are many acquisition tools on the market today that will allow personnel to perform a sound collection of evidence in a rapid manner. In some cases, this takes only minutes.

It is true that intelligence from these devices must be extracted as quickly as possible, but it is also extremely important that evidence be handled properly or its use in any future proceedings can potentially be placed into question.

In this exercise, the student will be performing a smartphone acquisition process on their own devices, using their own smartphone cable, along with a tool called UFED Physical Analyzer from Cellebrite. It is expected that the student possess a relatively standard Apple device, as well as the device charging/data cable.

### Exercise Objectives

- Connect student personal smartphone to the provided virtual machine
- Devices with MDM will not work completely
- Use **Cellebrite UFED4PC & UFED Physical Analyzer** to create and analyze an acquisition of student smartphone
- Note messages, pictures, and call logs; both active and deleted

### Exercise Preparation

1. Boot your **FOR498 Windows VM**
2. Login to the **FOR498 Windows VM** using the following credentials:
  - a. Username: **SANSDFIR**
  - b. Password: **forensics**

3. Have student smartphone and charging/data cable ready. Cables are a strange thing and can cause issues. If you are having issues, unplugging and re-plugging may help.
4. Exercise assumes smartphone is powered on.

**NOTE:** In cases where your VM will not allow for external device connection, insert your supplied USB 2.0 hub, and connect through this.

Acquisition of any smartphone or portable device is fraught with peril and can be quite frustrating. Although we have done our best to create these instructions based on the screens that presented themselves, it would not be surprising for a student to see something slightly different, as it is virtually impossible to account for every possible error message, permission message, or screen that a student may see. Any forensicator must be prepared to make informed, logical decisions. If you do not see your screen within the workbook, are you able to figure out what is expected? If not, call over your instructor, as you are working with a live device. For OnDemand students, please reach out to a SANS Online SME.

**Note: There is a risk that the latest version of iOS or your phone is not yet supported in the version of Cellebrite used in the class. If this is the case, you may not be able to complete the exercise as described. This is as close to a real-world situation as you'll encounter in this class. There will inevitably be instances where the tools have not yet caught up to the software and hardware. In those cases, you either need to wait for the tool to be updated to support the device or find an alternate method of collecting the data. This is all part of being a forensicator.**

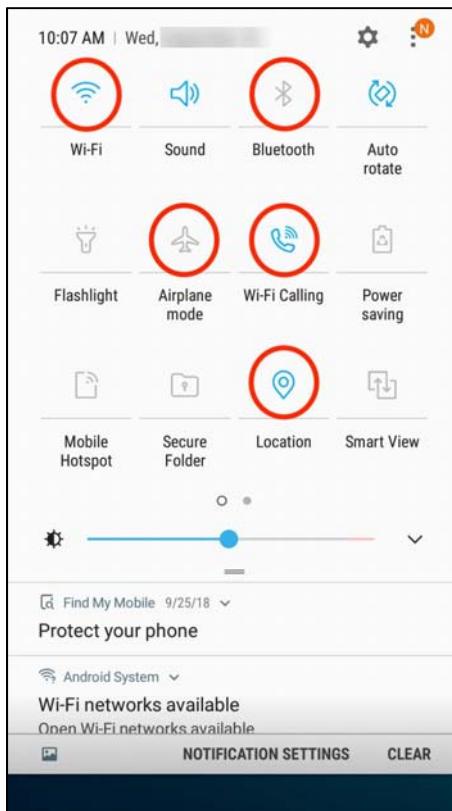
**WARNING!** You are performing this exercise on a live device – YOURS. Proceed with caution, and at your own risk. SANS is not responsible for any data loss, or lack of a student having backups of their data. There is absolutely no way for portable device acquisition exercises to have perfectly matching screenshots against what a student might see. There are simply too many variables, options, devices, versions, etc., to cover every eventuality. If you do not wish to practice with your personal device, simply read through the exercise. Devices that contain Mobile Device Management may not work for this exercise.

**Exercise - Section 1**

Android devices create an entirely different set of circumstances and problems for the examiner. Different models, as well as different versions, can have slight variances on how to prepare the device for acquisition.

**NOTE:** You MUST read the instructions below carefully, as there are several “and/or” steps and screenshots.

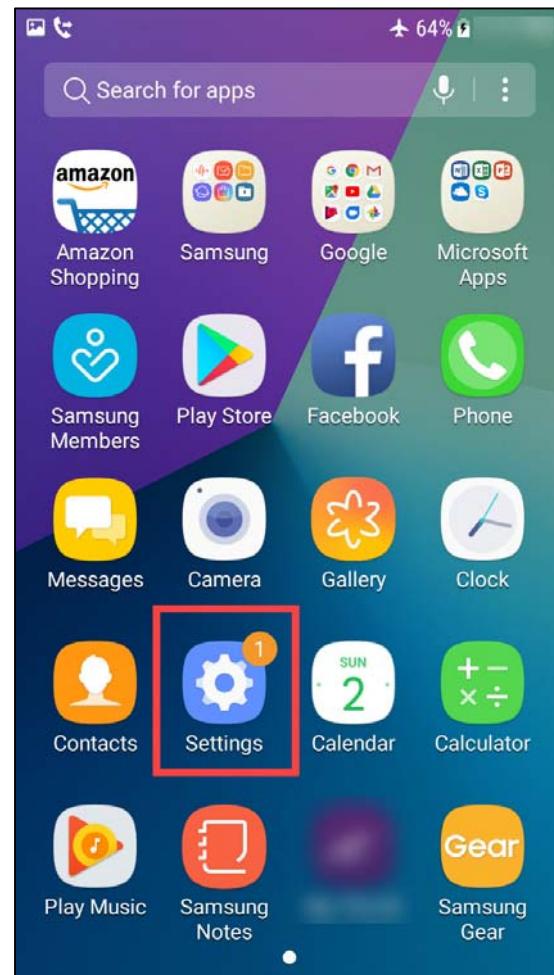
1. Place device into **Airplane Mode** by swiping down from the top of the screen to expose the **Notification Shade** and tapping the **Airplane** button. If the **Notification Shade** only comes down to cover half the screen, swipe down again.



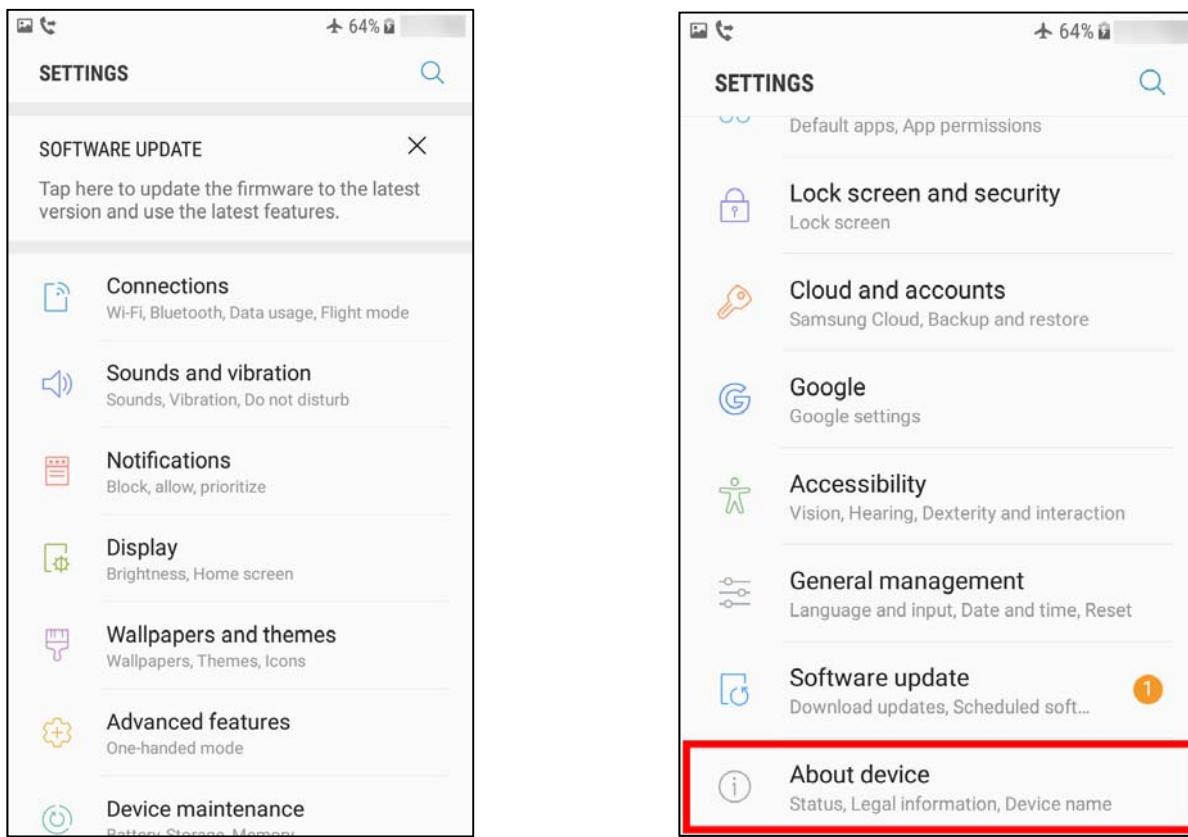
Date & time device placed in **Airplane Mode**: \_\_\_\_\_

If the **Notification Shade** does not appear, the device may be configured to not show it unless the device is unlocked. If this is the case, unlock the device, and try again. It is important to note that even minor version updates can cause changes to the **Notification Shade**, which can cause the location of the indicated icons to change. Depending on the version (and indeed the provider), there may even be different icons, or different names for icons. For example, the **Flashlight** icon may be called **Torch**. You may not see **Wi-Fi Calling** or **Smart View**. There are so many variables when it comes to Android devices, that common sense and “educated guesses” must be applied. This means looking through the icons in the **Notification Shade** and considering whether it would be prudent to deactivate them. If they seem like something that might allow for communication with the device from any type of remote connection, (Wi-Fi, cellular, Bluetooth, sync, etc.) then disable them. If you see an **Auto-Sync** icon, ensure that it is disabled as well. You may need to swipe from right to left to see it. When enabled, the icon is blue. When disabled, it is grey. You can return to the main screen by clicking on the device Home button.

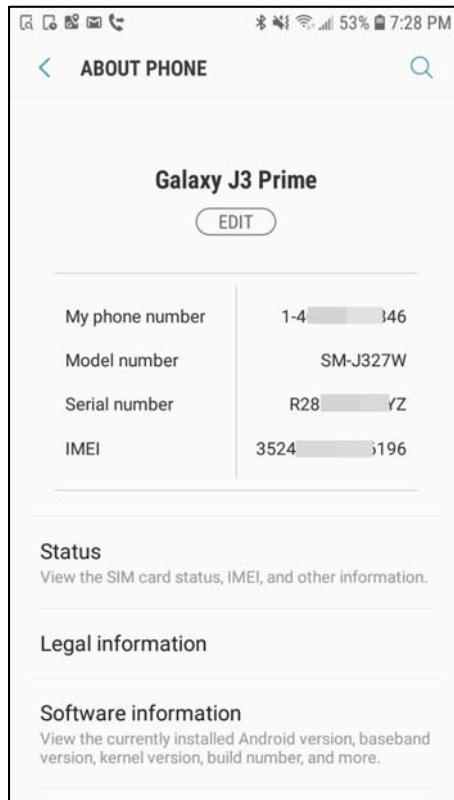
- At this point, you will perform evidence intake and identification. On Android devices, the model and serial number will almost always be underneath the battery. At some point, you will remove the battery and document this, however, this is NOT that time! We can get this data from other locations, for the time being. From the home screen, tap on the **Apps** icon, and then locate and tap on the **Settings** icon. This icon looks like a gear. You may have to swipe the screen left or right to find it.



3. Under the long list of **SETTINGS** options, locate the **About device** or **About phone** and tap on it.



4. Scroll down (if necessary) and locate the **Device name** and **Model number** and record them.



a. What is your device name?

---

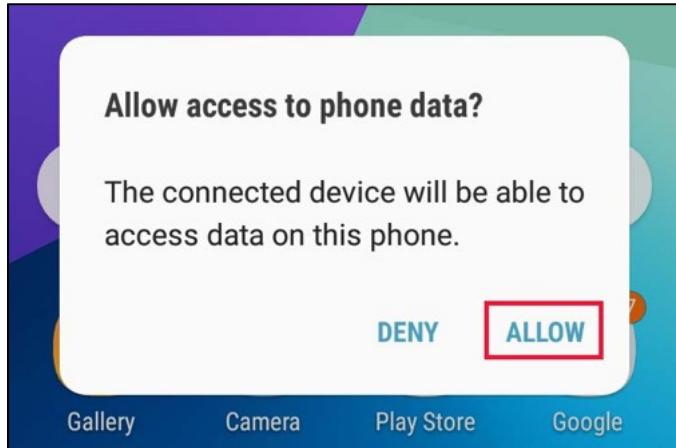
b. What is your device model number?

---

5. Press the home button on your device to return to the main page. Ensure your **FOR498 Windows VM** is in full screen mode. If it is not, you may have connection issues when plugging a device in for analysis with the **VM**. The following screenshots refer to the use of **VMware Workstation** and **VMware Player**. For **VMware Fusion** users, jump to **step 10**.



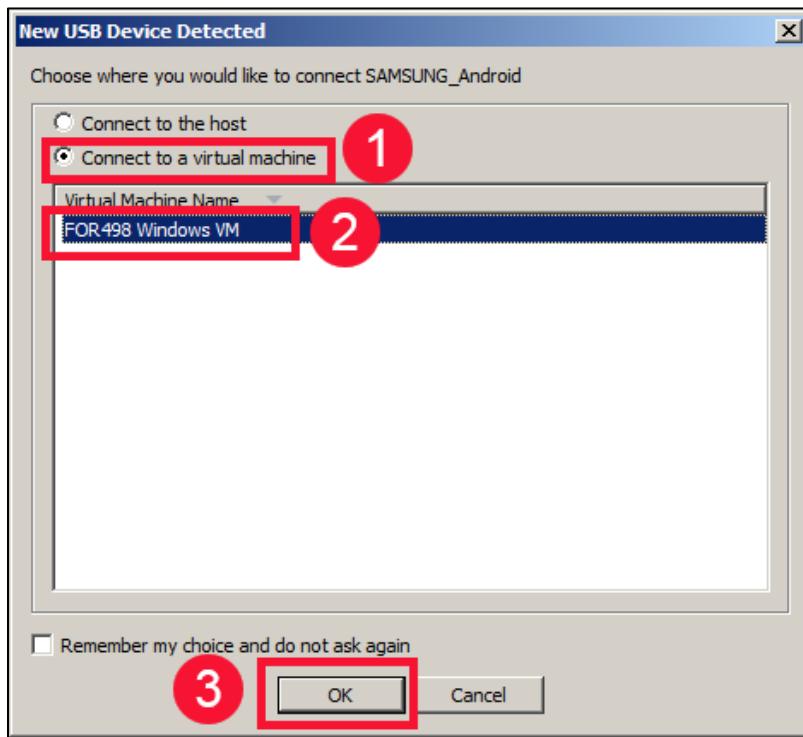
6. Using your charging/data cable, plug your device into your computer. Your device may need permission to connect, via a message on the device screen. Allow it. If you get any **AutoPlay** questions about what you want the computer to do with your device, select **Do nothing**, or just close them.



7. When you plug your device in, you will see either the window in **OPTION 1** below, or one of the two windows in **OPTION 2** below. Follow the instructions for your **OPTION** accordingly.

### OPTION 1

Once completed, go to Section 2 of this exercise.

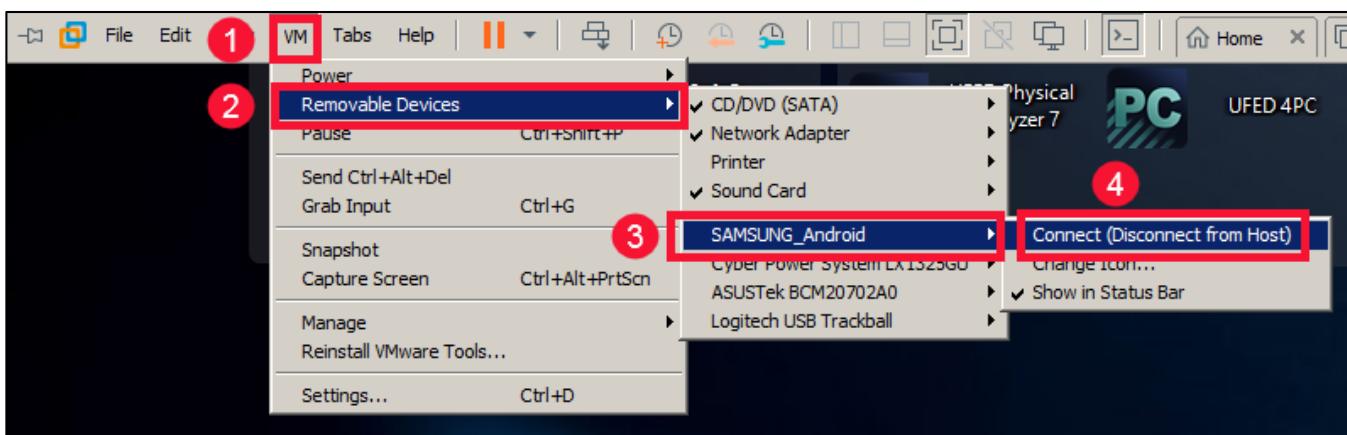


### OPTION TWO

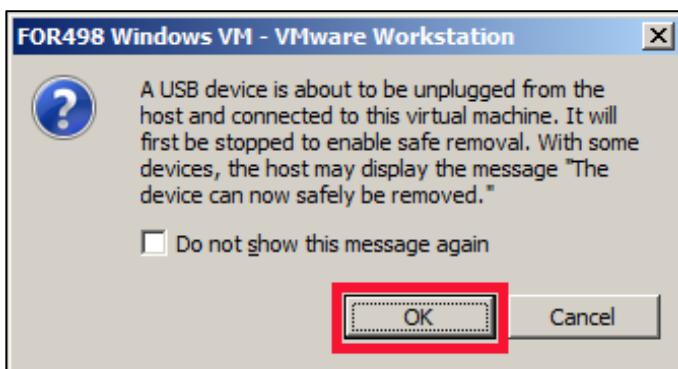
If you see **screen 1**, proceed to **Section 2** of this exercise. If you see **screen 2**, proceed to the next step.

SCREEN 1	SCREEN 2
<p><b>Removable Devices</b></p> <p>The following devices can be connected to this virtual machine using the status bar or choosing VM &gt; Removable Devices:</p> <p> SAMSUNG_Android (connected to Windows [redacted])</p> <p>Each device can be connected either to the host or to one virtual machine at a time.</p> <p><input type="checkbox"/> Do not show this hint again</p> <p style="text-align: center;"><b>OK</b></p>	<p><b>Removable Devices</b></p> <p>The following devices can be connected to this virtual machine using the status bar or choosing VM &gt; Removable Devices:</p> <p> SAMSUNG_Android</p> <p>Each device can be connected either to the host or to one virtual machine at a time.</p> <p><input type="checkbox"/> Do not show this hint again</p> <p style="text-align: center;"><b>OK</b></p>

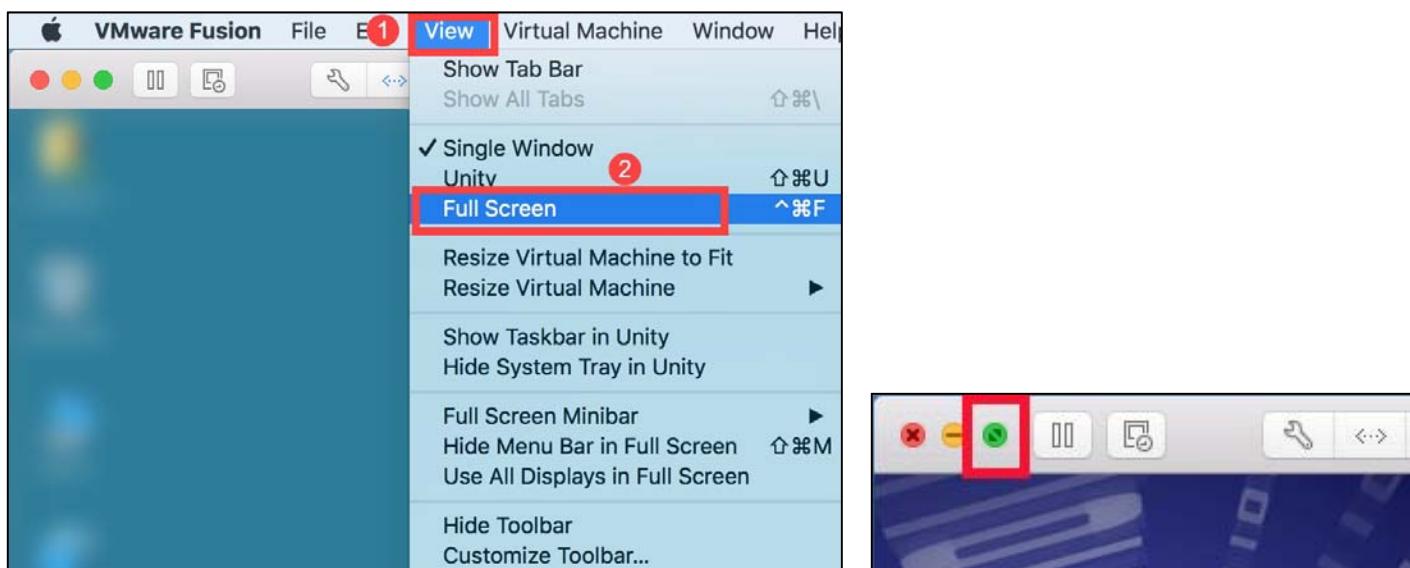
8. In the case of **screen 2**, the device has been ‘captured’ by the host computer rather than the VM, so you must tell the VM to take control of the device. Within the VM, click on **VM -> Removable Devices -> [your device name] -> Connect (Disconnect from the Host)**.



9. You may receive a pop-up confirmation. Click **OK**. Proceed to **Section 2** of this exercise.



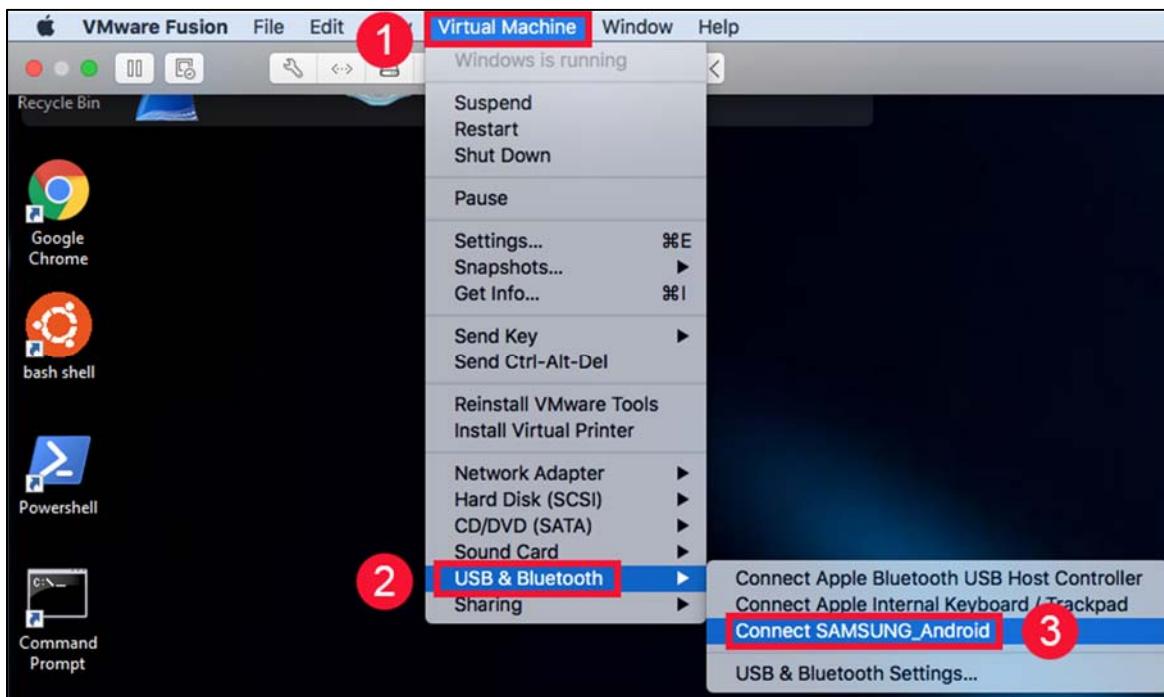
10. For **VMWare Fusion** users, ensure your **FOR498 Windows VM** is in full screen mode. If it is not, you may have connection issues when plugging a device in for analysis with the **VM**.



11. Using your charging/data cable, plug your device into your computer. Your device may need permission to connect, via a message on the device screen. Follow the instructions on your device screen to cause the device to trust the computer.
12. When you plug your device in, a box will appear asking where you want your device to connect. Select “Connect to Windows”, to connect the device to your **FOR498 Windows VM**. If there is an issue getting your device to connect, go to **HOST** System Preferences -> Security and Privacy -> General, and allow VMware.



13. If you do not see the previous pop up when attaching the device to the VM, you need to attach it manually. Within the VM, click on **Virtual Machine** -> **USB & Bluetooth** -> **Connect [your device name]**.



14. If you receive any confirmation prompts, read them carefully before accepting them (or not), and understand what they are asking for.

## Exercise - Section 2

1. Start the **UFED Physical Analyzer (PA)** application by double clicking the icon in the **Forensic Suites** fence on your **Desktop**. This program takes a few seconds to open, so be patient. Note that you do NOT want two instances opening!

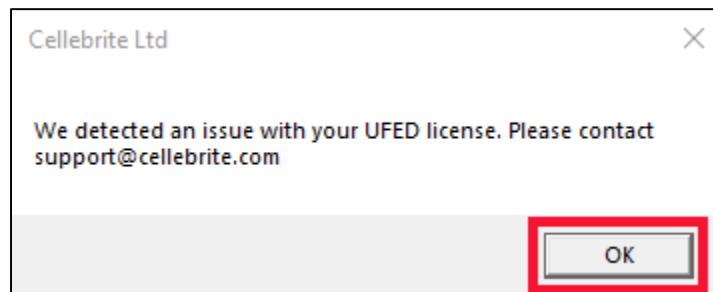


2. After a few seconds where it will appear that nothing is happening (BE PATIENT), a splash screen will appear.

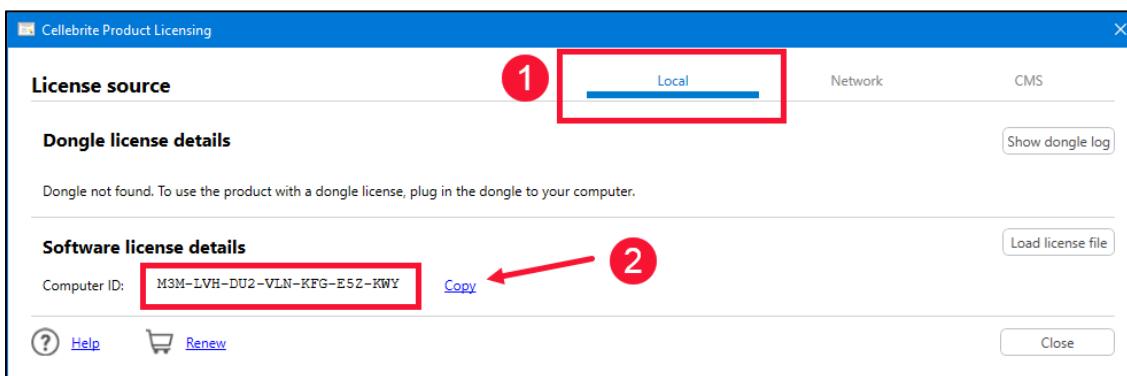


**NOTE:** You may be prompted to update **Physical Analyzer**. If the currently installed version of Cellebrite does not support the collection of your particular device, we recommend updating the software OUTSIDE CLASS. If the currently installed version is able to collect your phone, please avoid updating until after you have completed the class. Updating is optional and may “break” the functionality of the tool in regards to the other Cellebrite-based exercises in this class. Updating is at your own risk. The currently-installed version has been tested and confirmed to work with the remaining exercises! You will license the other tools right before they are needed in each lab. **Do not change any VM settings after licensing Cellebrite or your license may no longer work!**

3. If you get a pop-up message during startup of the program, as indicated below, simply click **OK**, and the program will continue to load.



4. The prompt below pops up in **Physical Analyzer** when the tool launches. Copy your **Computer ID** from **Physical Analyzer**. Ensure the **Local** button is selected. If the prompt does not appear, select **Help > Show License Details**.



5. Open a browser window, go to <https://my.cellebrite.com/training> and fill out the required fields to receive your license file for this course. **NOTE: Do not provide your real information unless you want to be contacted by the Vendor. A fake email account is enough to get you a license. Feel free to use your own information if you already have an account with Cellebrite or plan to use any support.** (NOTE: The **Activation Code** is provided by SANS or the instructor. If you are an OnDemand student, please request the code by emailing online-sme@sans.org. The **Computer ID** is copied from **UFED Physical Analyzer**, as shown above.) Make sure you select something from each drop-down option, or you cannot proceed. Once everything is filled in, click **Generate License**.

**Training License**

**UFED applications free trial**

Primary Email\*: eat@joes.com  
License will be sent to this address in addition to the download

First Name\*: Bilbao

Last Name\*: Baggins

Company\*: Acme

Phone\*: 8085551212

Country\*: United States

State\*: California

City\*: Beverly Hills

Address\*: 123 Anywhere Street

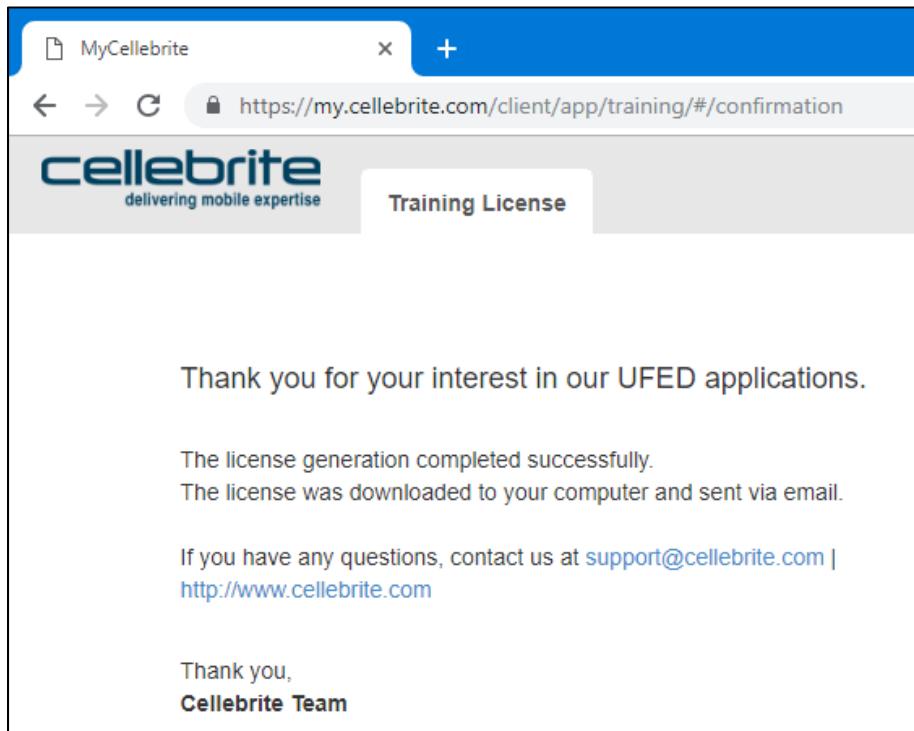
Zip/Code\*: 90210

Activation Code\*: Enter what SANS or instructor has provided

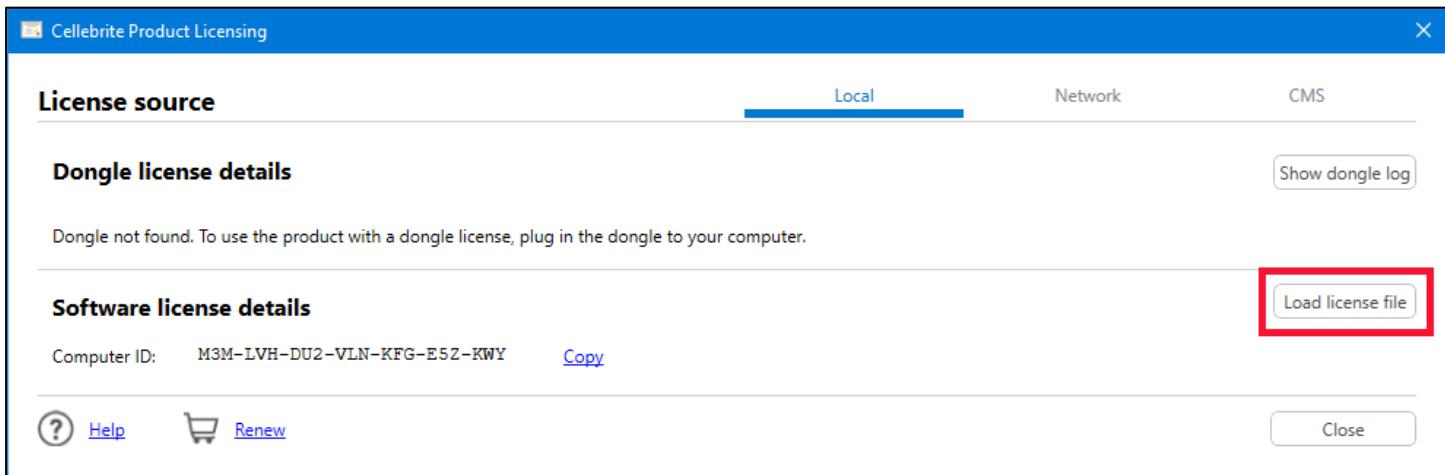
Computer ID\*: Copy from the screen in UFED Physical Analyzer

**Generate License**

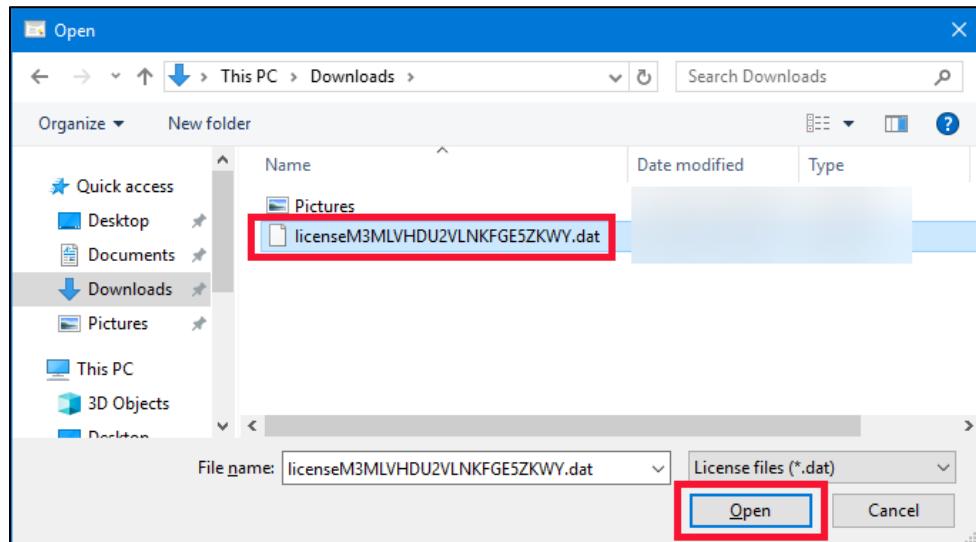
6. Your license should appear at the bottom of your screen after a minute. Select **Save** and the license file will be saved to your **Downloads** folder. In some cases, this has happened automatically.
7. When this is done, it will be indicated by a thank you message from Cellebrite. Close the browser window.



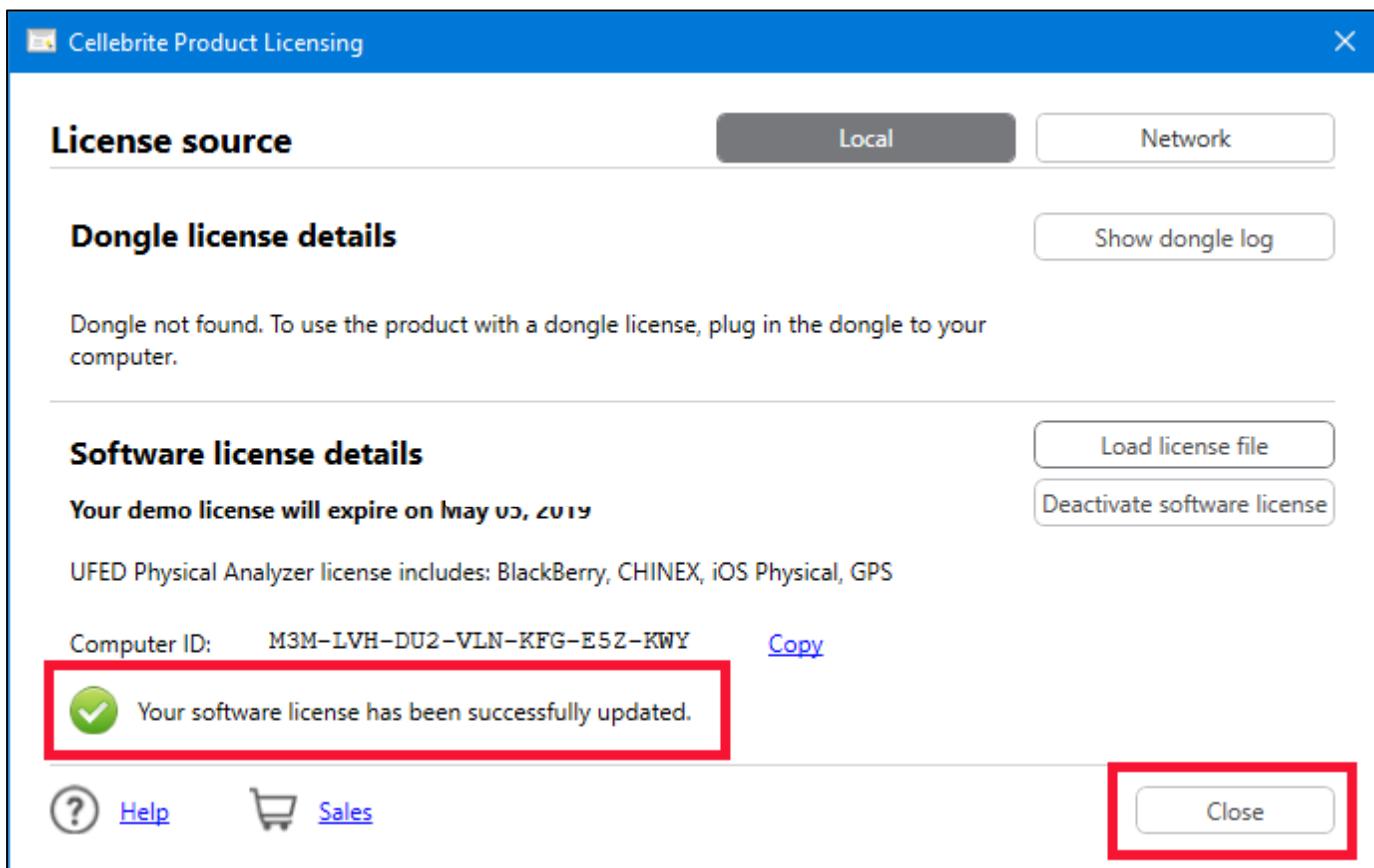
8. Go back into **Physical Analyzer** and select **Load license file**.



- A directory window will open. Navigate to your **Downloads** directory and select your **licenseXXX.dat** file and then click on **Open**.



- Once done, you will see the **Product Licensing** window again. Note that the software license is now active. Click the **Close** button.

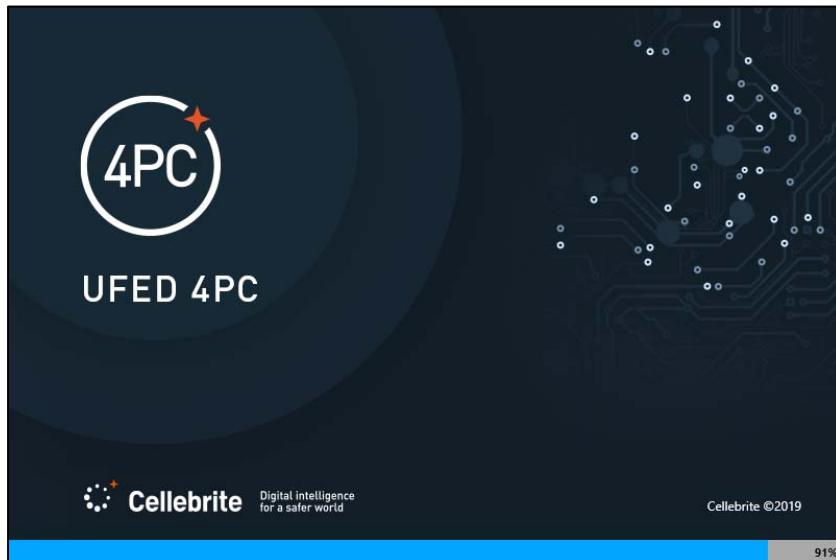


- You will now see the Physical Analyzer program open. You can simply close it once this happens.

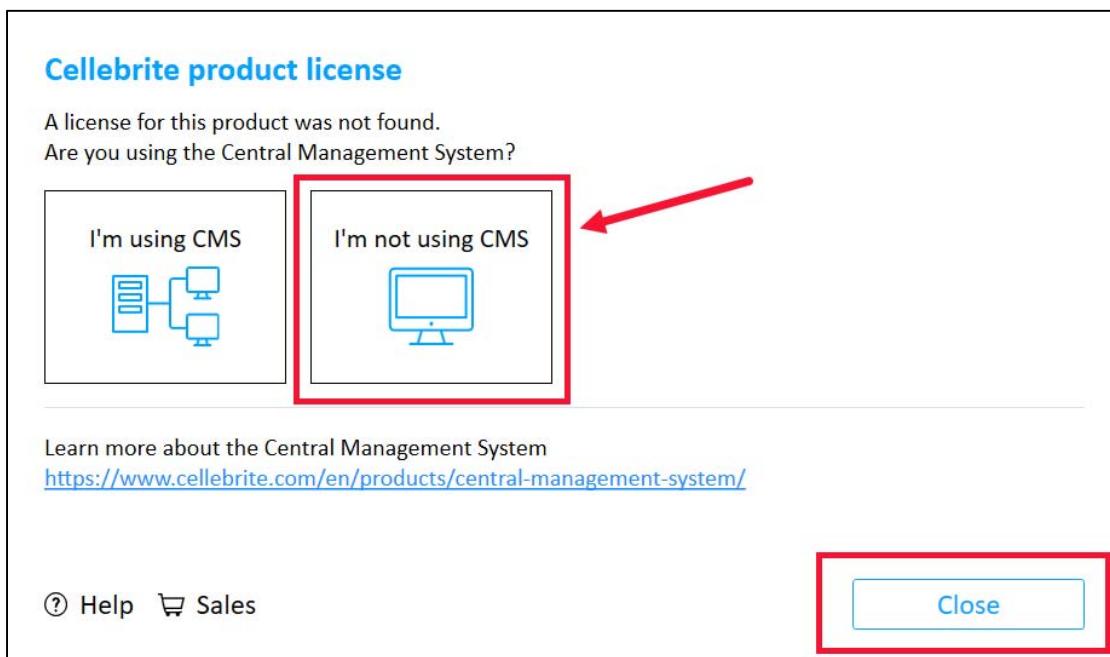
- We are ready to initiate the collection process. Start the **UFED 4PC** application by double clicking the icon in the **Forensic Suites** fence on your **Desktop**. Again, this program takes a few seconds to open, so be patient. Note that you do NOT want two instances opening!



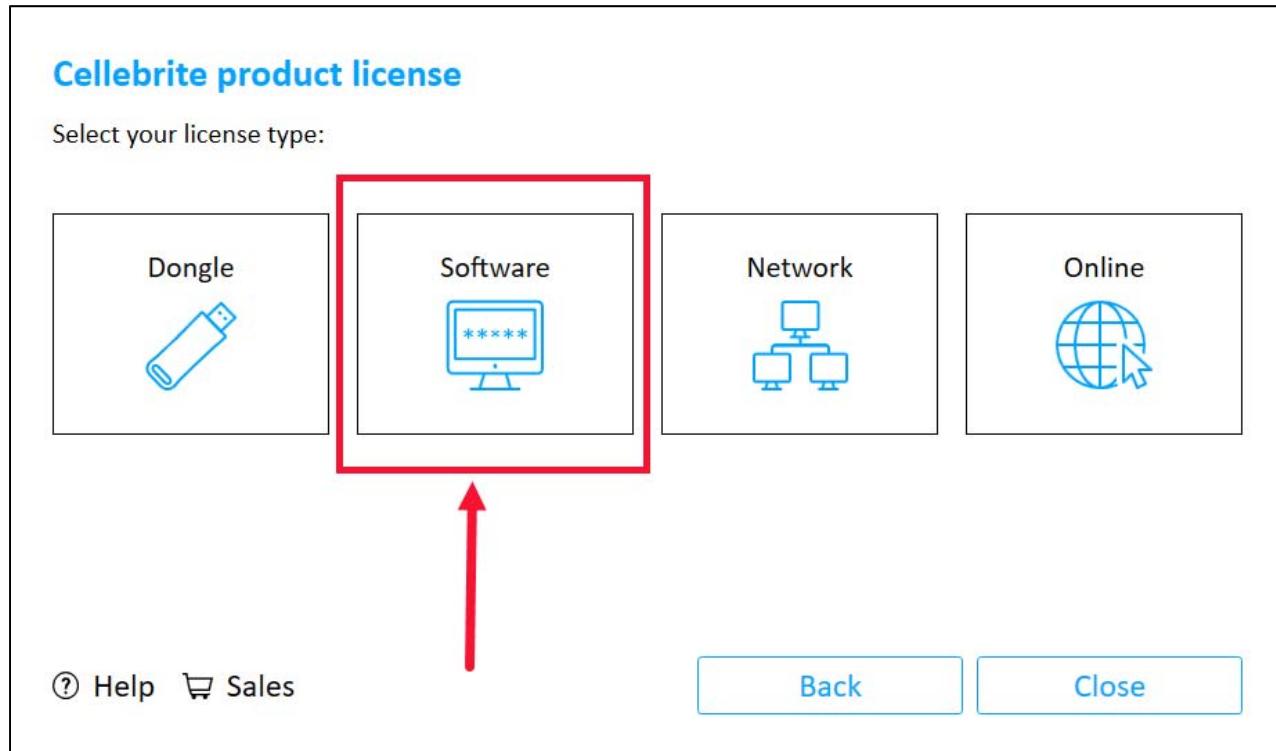
- After a few seconds where it will appear that nothing is happening (BE PATIENT), a splash screen will appear.



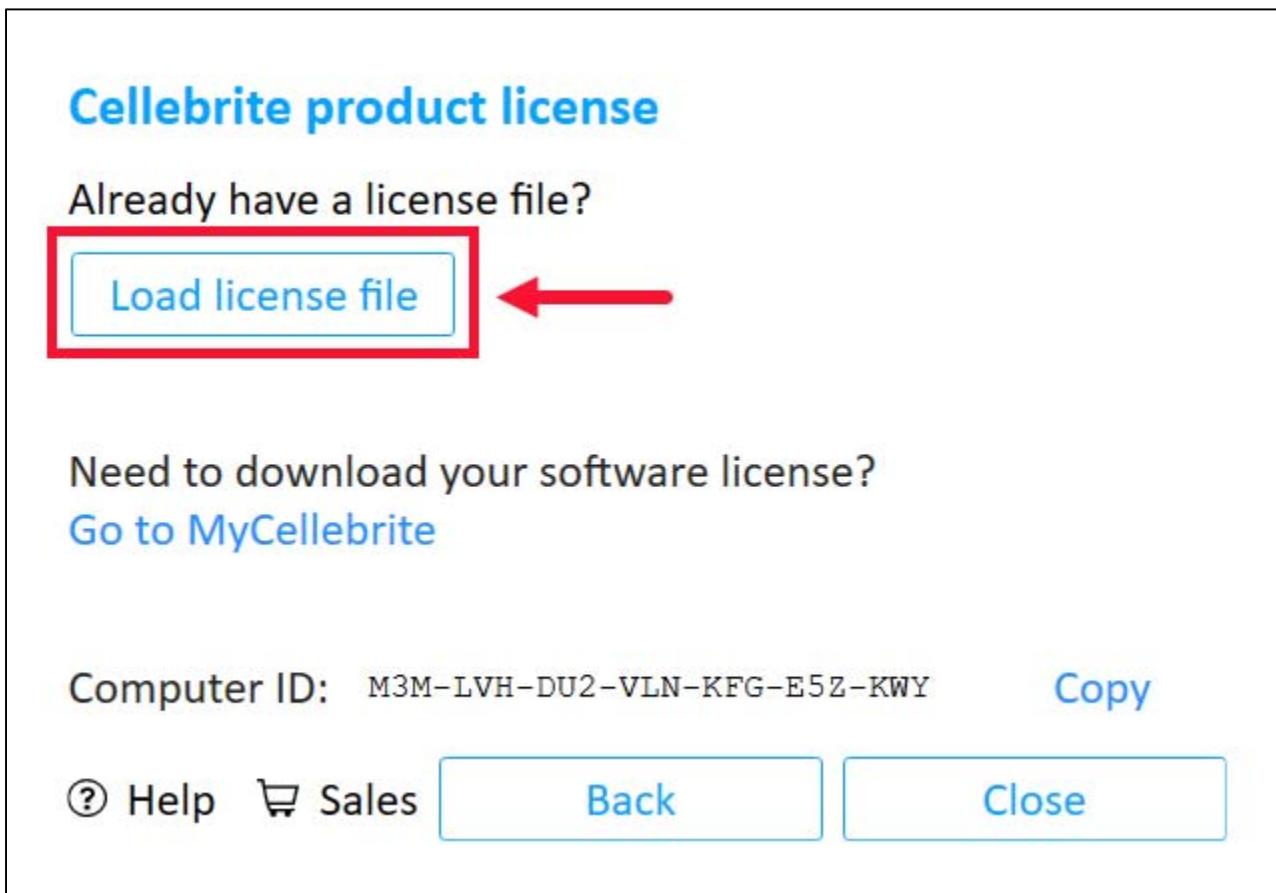
- When the program opens, you may get one of two licensing messages. The first may look like the screenshot below. If you get this box, just click **No**, (and then **Close**, if the box persists).



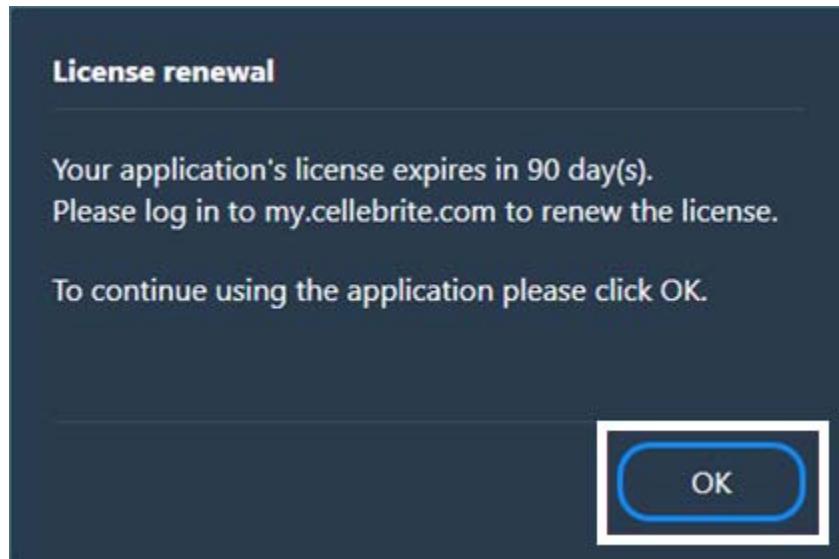
15. The second of two possible licensing prompts is below. Select the **Software** option.



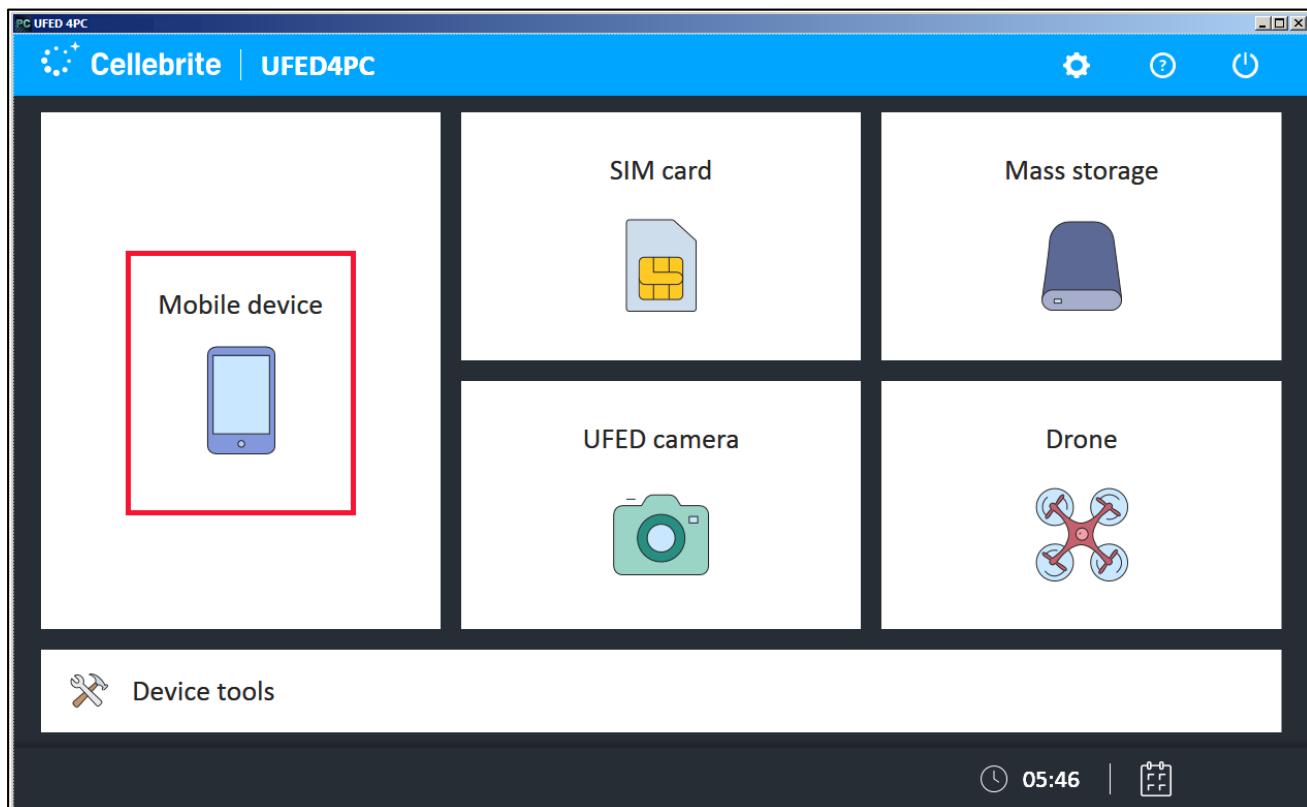
16. You don't have to go through the licensing process all over again. Click on the **Load license file** button.



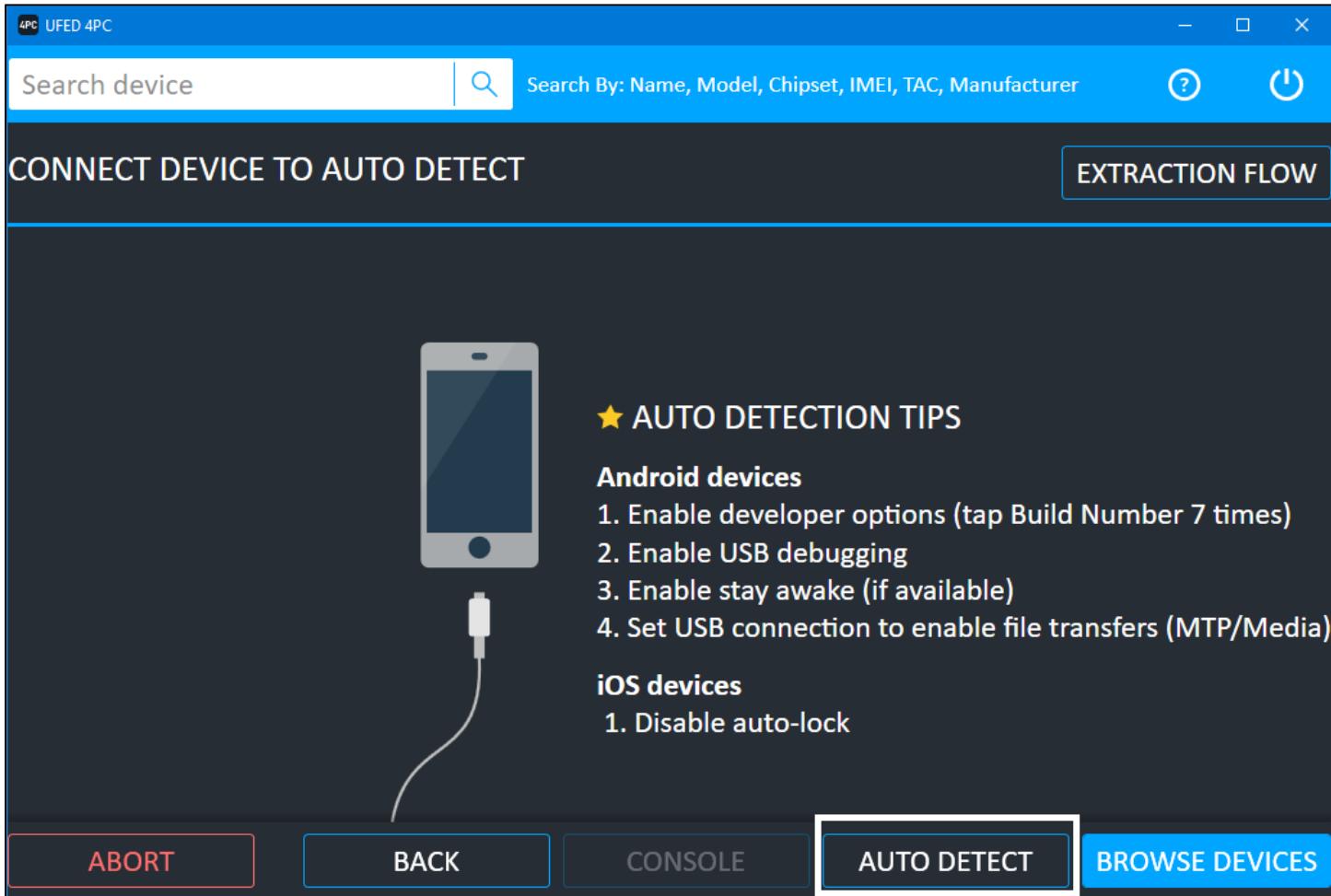
- When the **File Explorer** window opens, navigate to your **Downloads** folder again and select the license file and click the **Open** button, as you did with **UFED Physical Analyzer**. Once the license has been accepted, one last window may appear indicating your 90-day license. Click the **OK** button to close this prompt.



- You will now be at the **UFED 4PC** opening screen. Select **Mobile device** from the options presented.



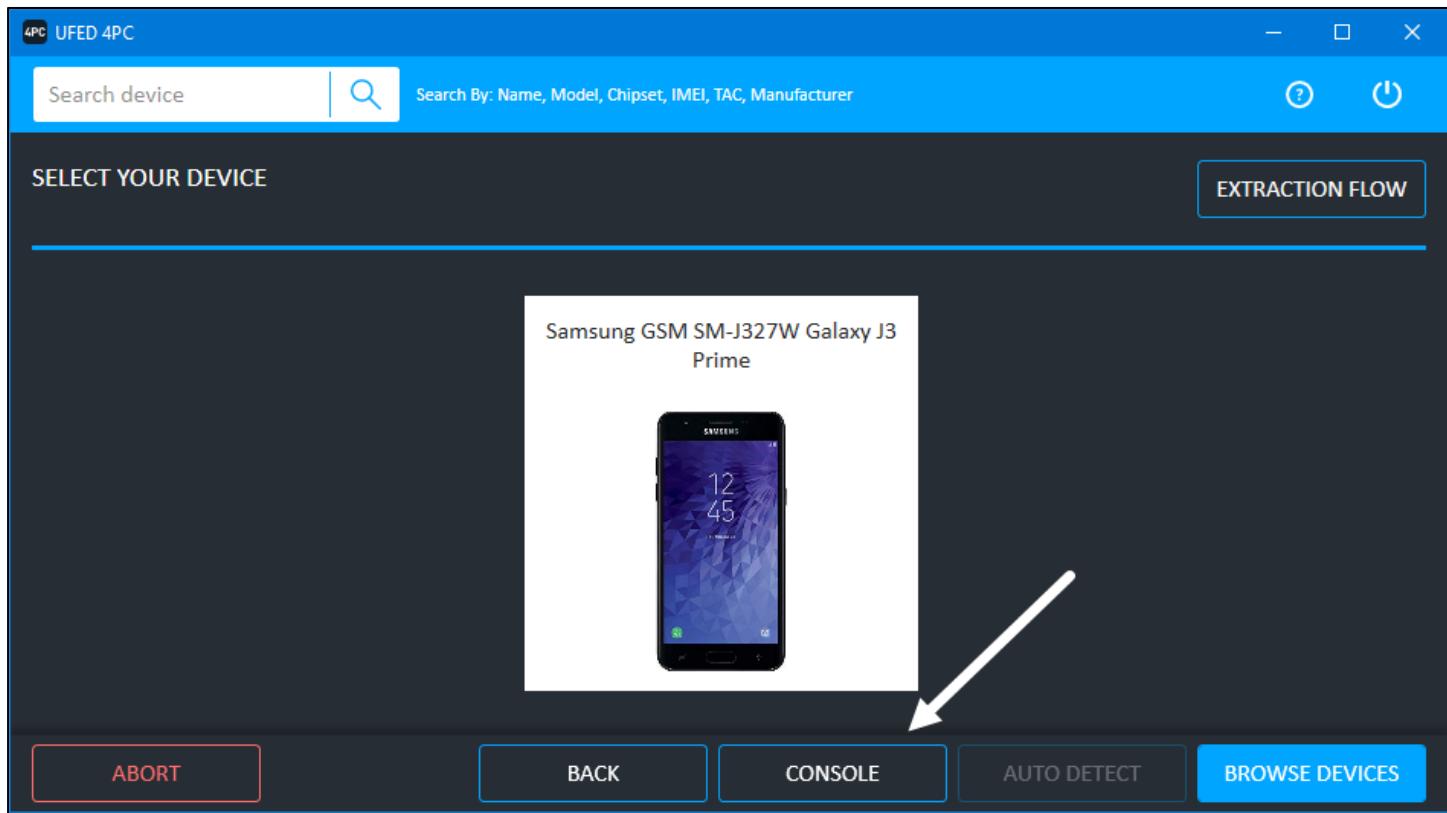
19. The **DETECT DEVICE** screen will appear. The instruction steps shown to set up your Android device will also be shown. You don't need to do these now, as there are steps in the next section for this. Click on **AUTO DETECT**. If nothing happens, unplug and replug your device, noting that you may have to authorize on your device again.



20. Depending on the model of device, you may be presented with more than one option, or you may be presented with no option at all. If you see your model shown on the screen, that is great; your device was detected. You may have to click **Allow** on your device again. The actual acquisition process starts in **Section 5** below.
21. If the device is not automatically detected, the set of steps are different. Immediately below, are instructions for an auto-detected device. Immediately following this section are instructions for a device that was not auto-detected, in "**Exercise - Section 4 – STEPS IF DEVICE NOT DETECTED**".

## Exercise - Section 3 - STEPS IF DEVICE DETECTED

1. Click on **CONSOLE**.



2. Note the instructions on the **Device Tools** screen that appears.

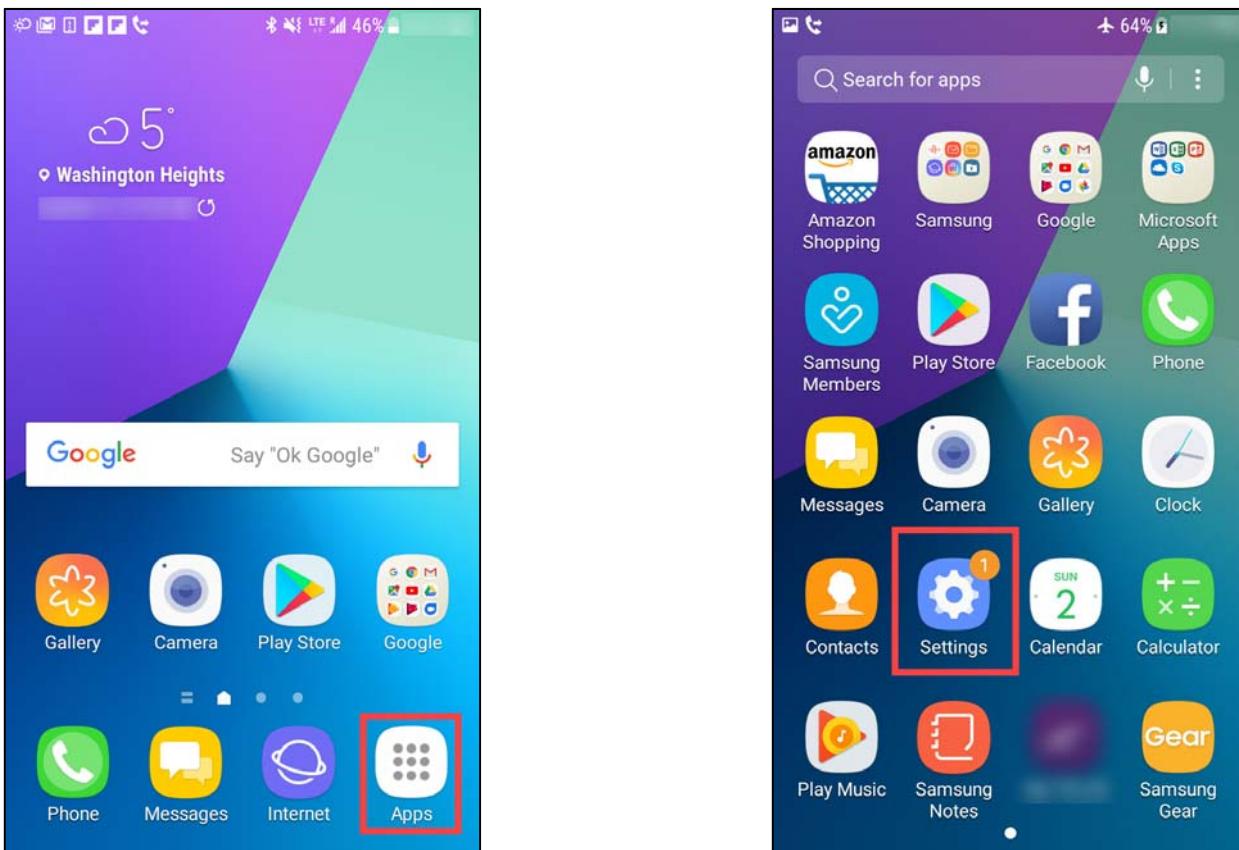
### Device Tools

**Android Debug Console:**  
This tool uses Android Debug Bridge (ADB) and requires that the “USB Debugging” mode is enabled.  
To use this tool:  
1. Go to the device settings > About/Information > tap the "Build number" 7 times. A message is displayed that you're now a developer.  
2. Go back to the Developer options menu, select “USB debugging” and “Stay awake” (if available).  
3. Approve the “Allow USB debugging” connection to the computer by selecting “Always allow”.  
4. Connect the device and press "OK".

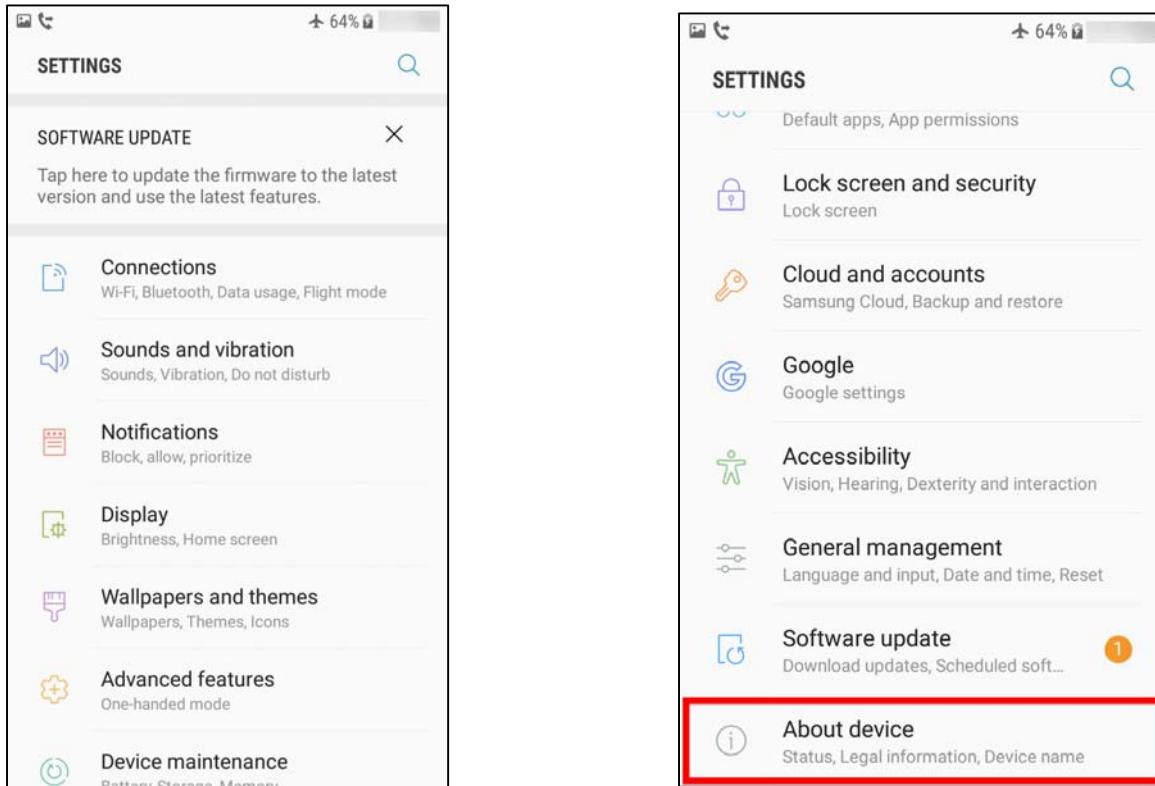
**OK**

3. You can perform them now using the following instructions, or you may be prompted to do them again later in the acquisition process.

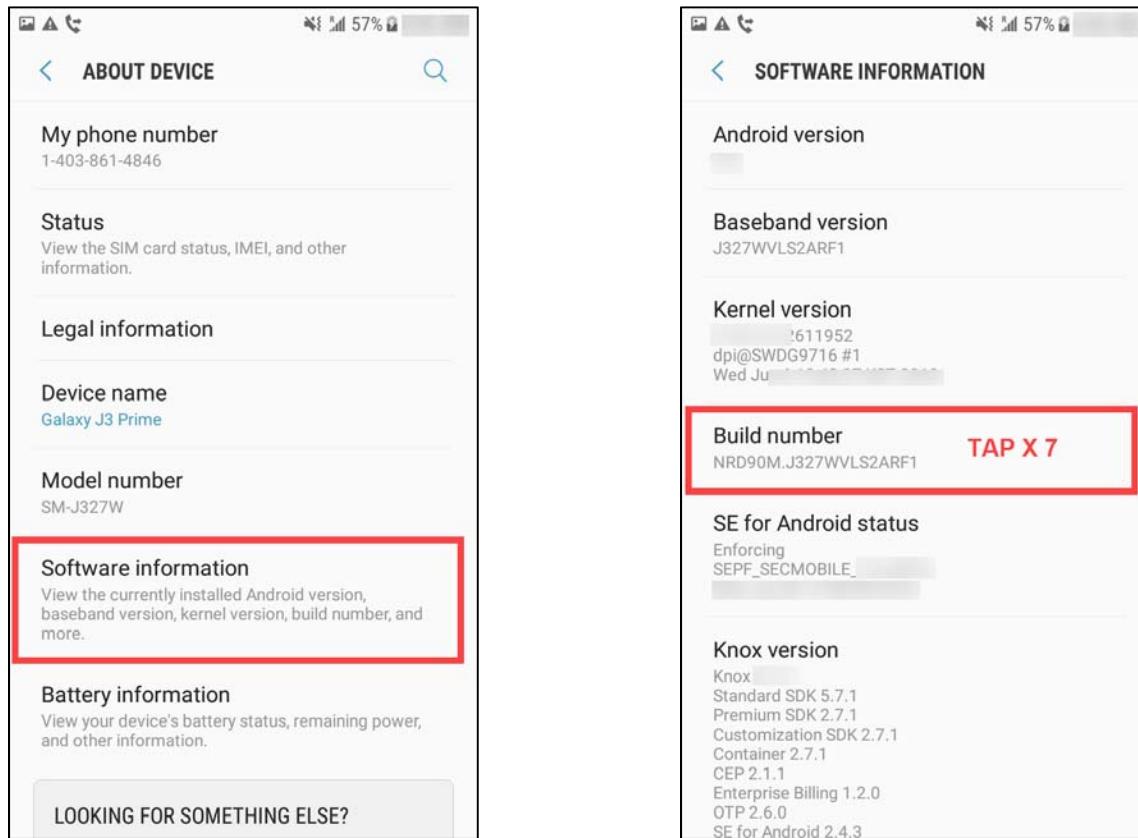
4. Open the **Apps** menu on the device and select **Settings**.



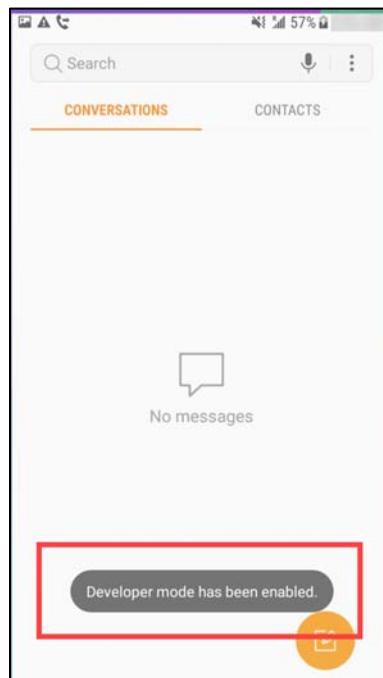
5. Scroll down the list of available settings and locate **About device** or **About phone**. Tap to open it.



6. In the next screen you see, locate an option entitled **Build number**. If you do not see a **Build number** option, locate the **Software information** option as seen below, and tap on it to see the **Build number** option. Once you locate it, tap on it 7 times...



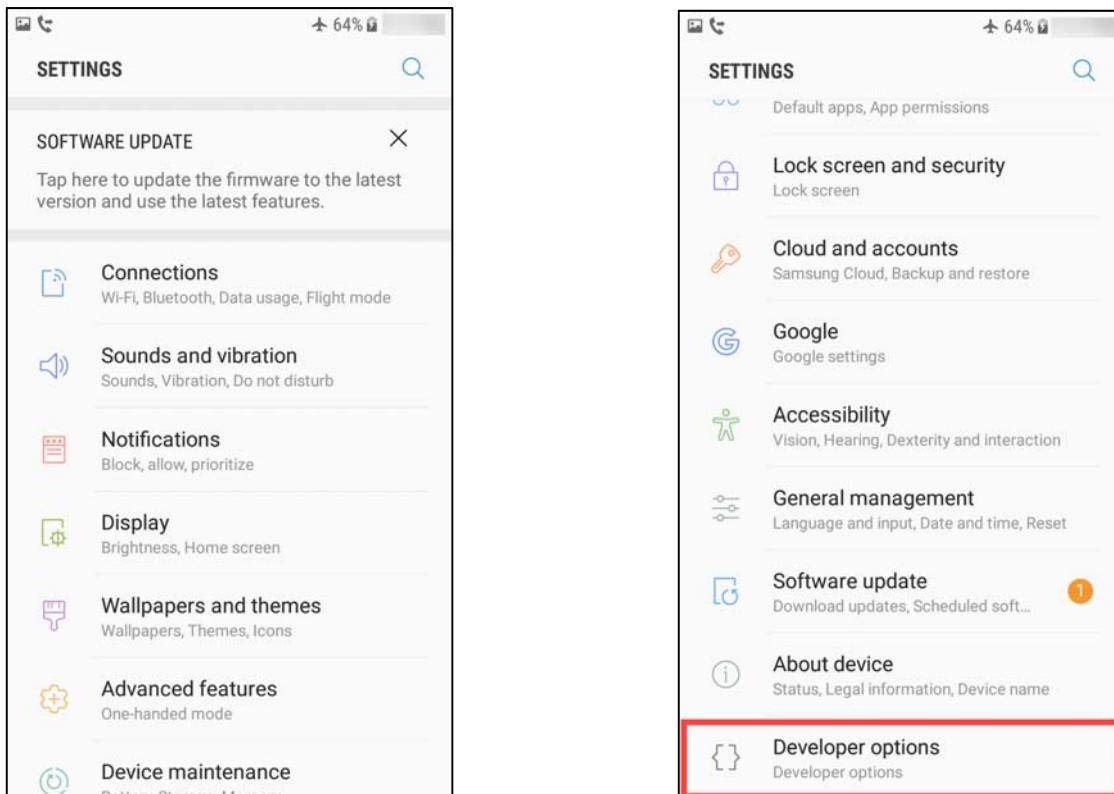
7. ...and you will see a note on the screen indicating that **Developer mode has been enabled**.



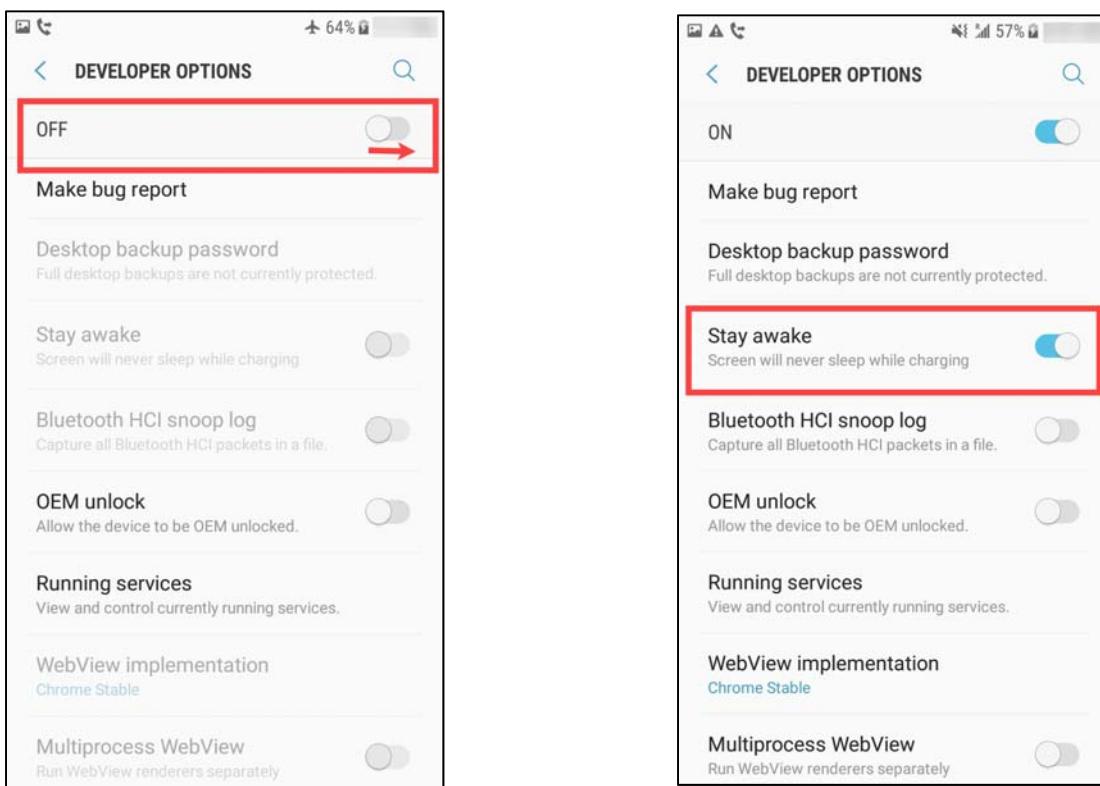
8. Navigate back to the home screen. Open the Apps menu on the device and select **Settings**.



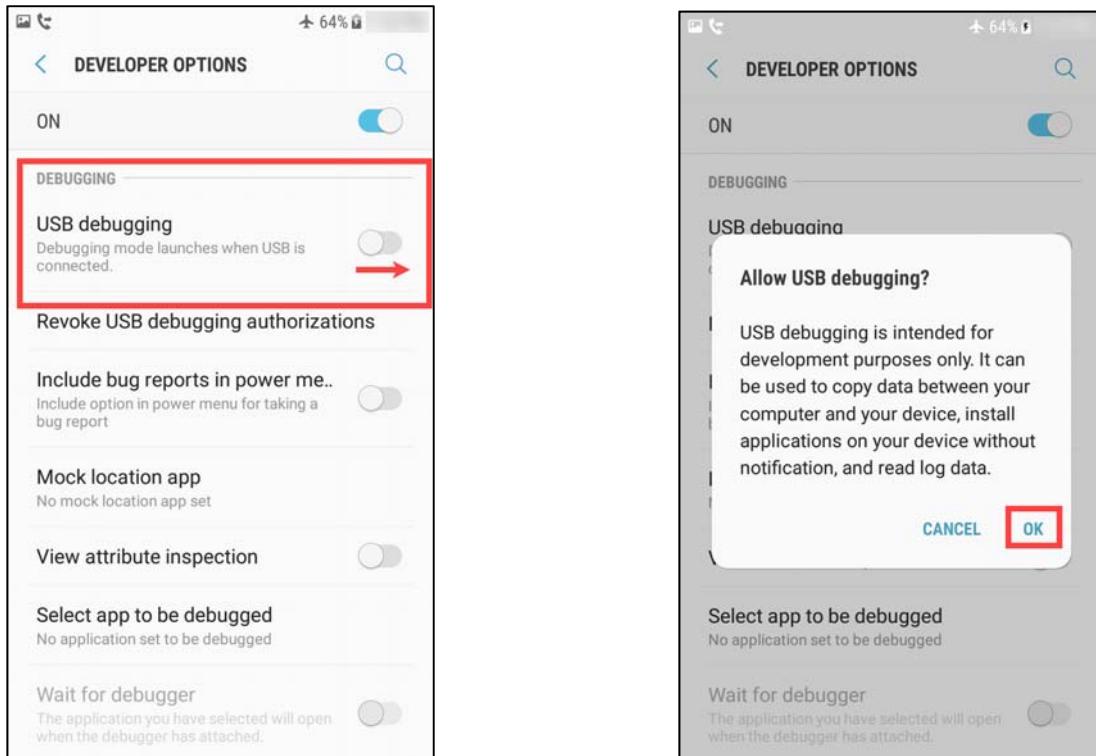
9. Scroll down the list of available settings and you should now see a new option below **About device** or **About phone**, called **Developer options**. Tap to open it.



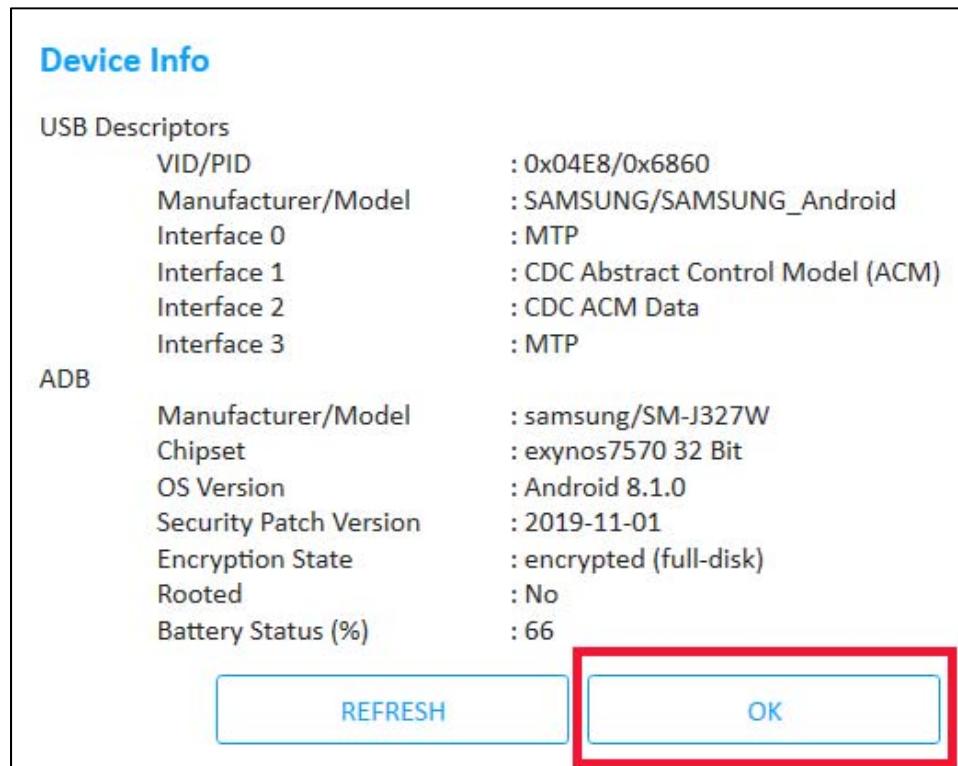
10. In the **DEVELOPER OPTIONS** menu, ensure the options are **ON**. If they are not, swipe the slider to the **ON** position. Further down the list of options is the **Stay awake** option. Ensure this is on, and if it is not, swipe it to the **ON** position. If you see any confirmation prompts at any time, accept them.



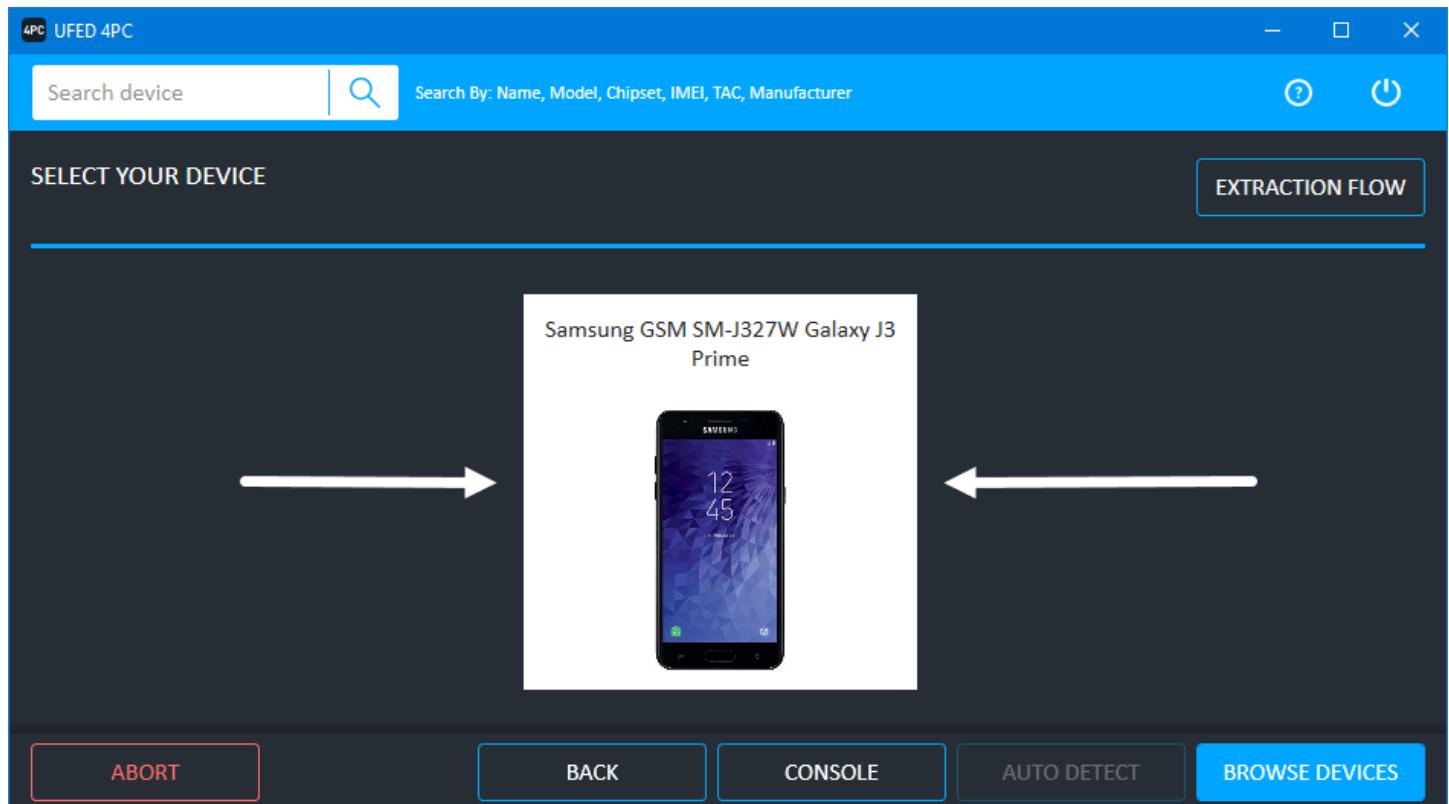
11. Scroll down the list of **DEVELOPER OPTIONS** until you see an option entitled **USB debugging**. Again, if it is off (greyed button), then swipe it to the **ON** position, and accept any confirmation requests.



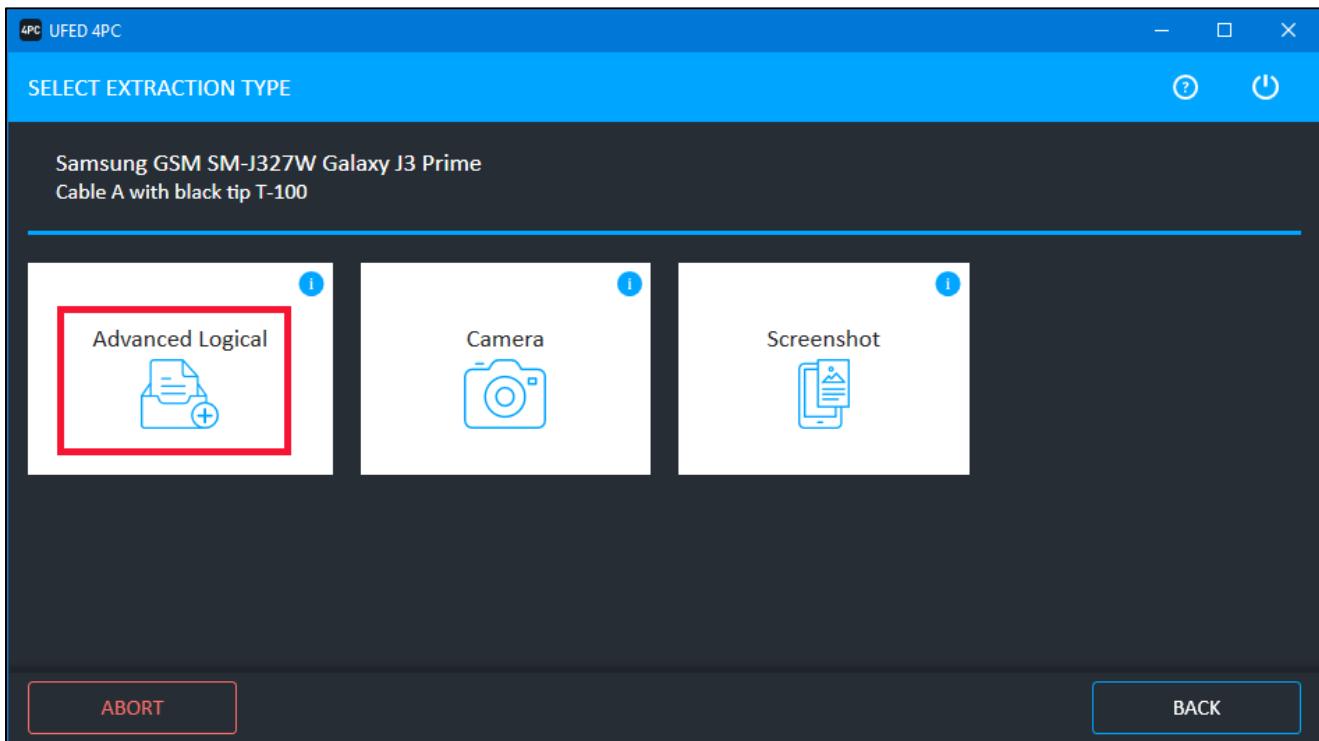
12. Once the above steps are done, (or if you chose to skip them for now) click **OK** on the **Device Tools** pop-up in **UFED 4PC**. **Device Info** is now shown. It is a great idea to photograph this or screenshot it. Then select **OK**.



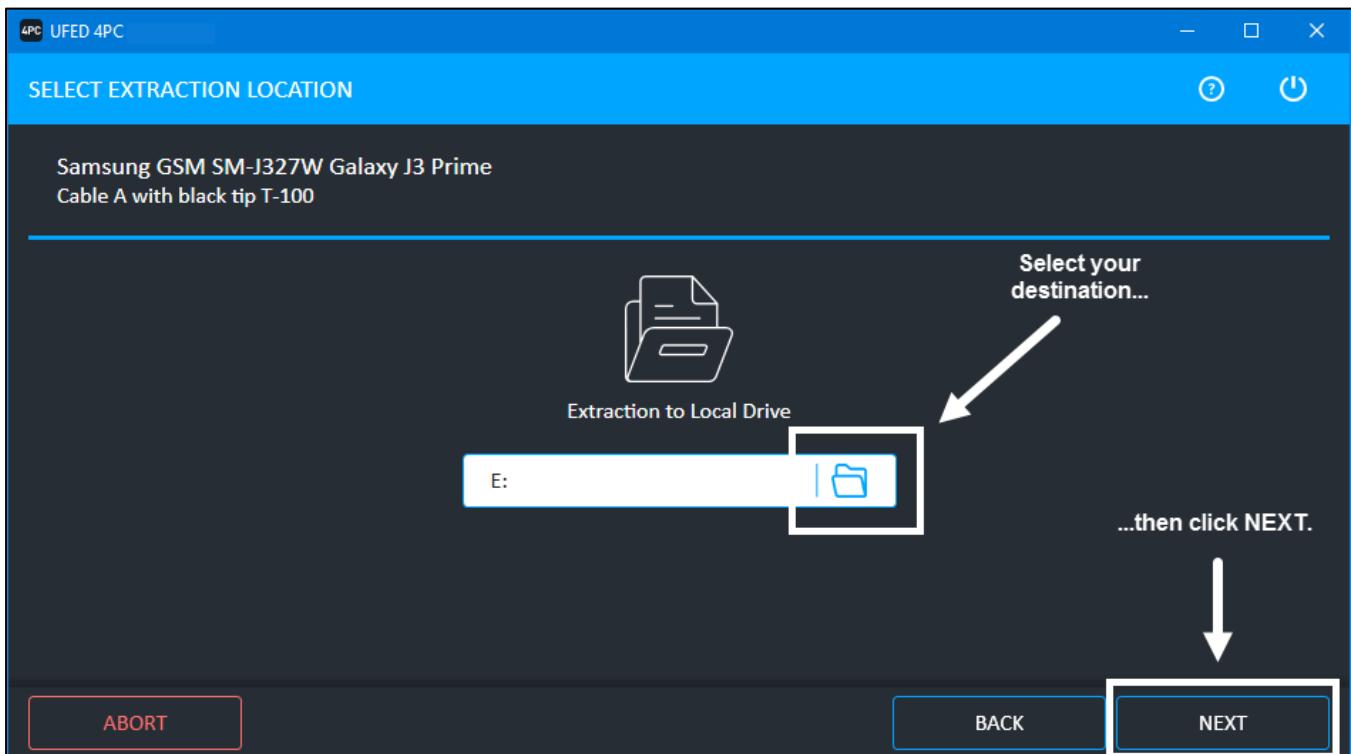
13. This should return you to the screen displaying your detected model. Click on the device picture itself.



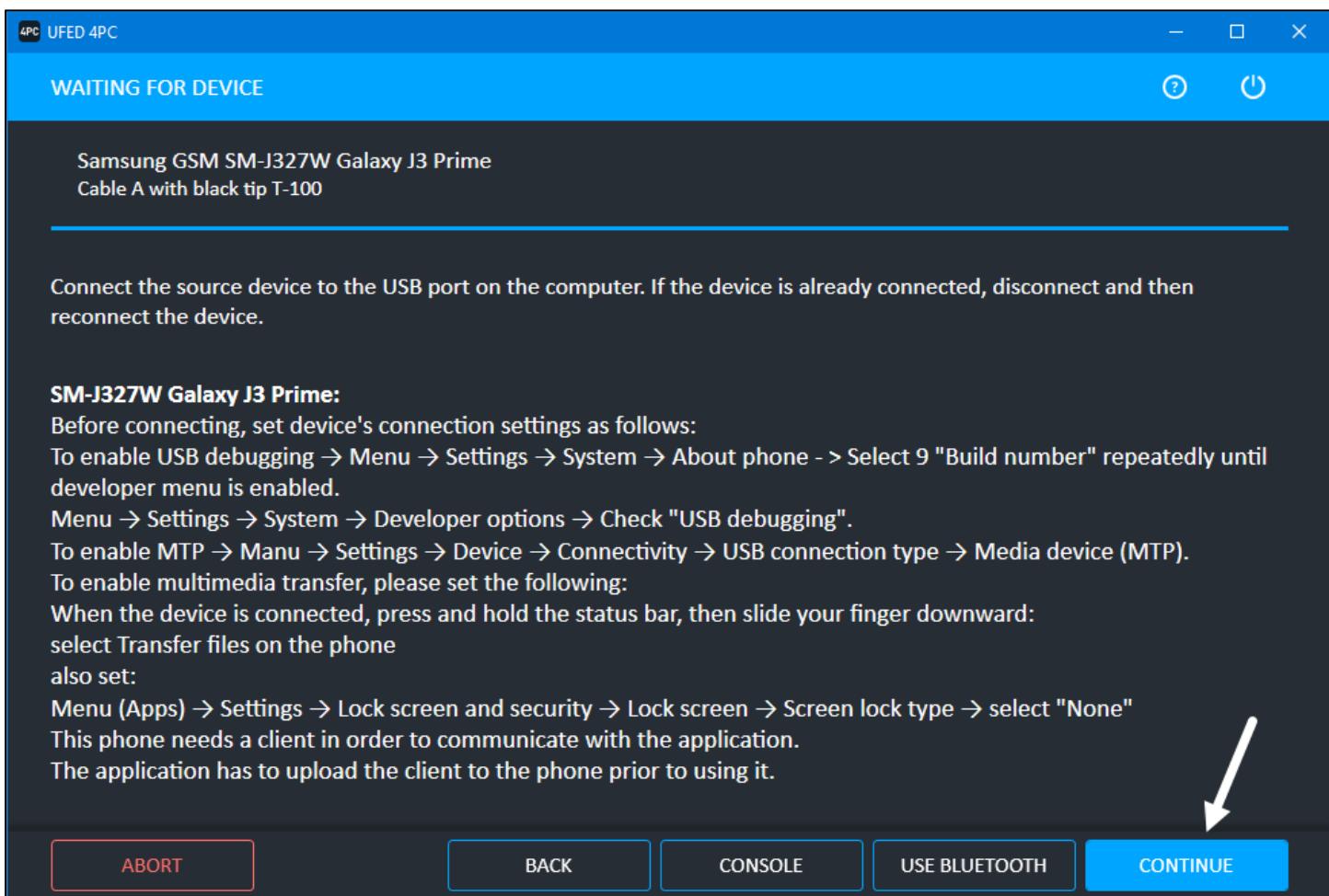
14. You will be prompted to **SELECT EXTRACTION TYPE**. There are potentially a number of options, and each model can be slightly different in its available options, both due to model, and due to OS version. For the purpose of this exercise, select the **Advanced Logical** option.



15. Choose where to save the extraction. Connect your student supplied external hard drive to your **FOR498 Windows VM**, then click the **Browse** icon to the right of the destination path and save the extraction to the root of your external hard drive. Click **Next**.



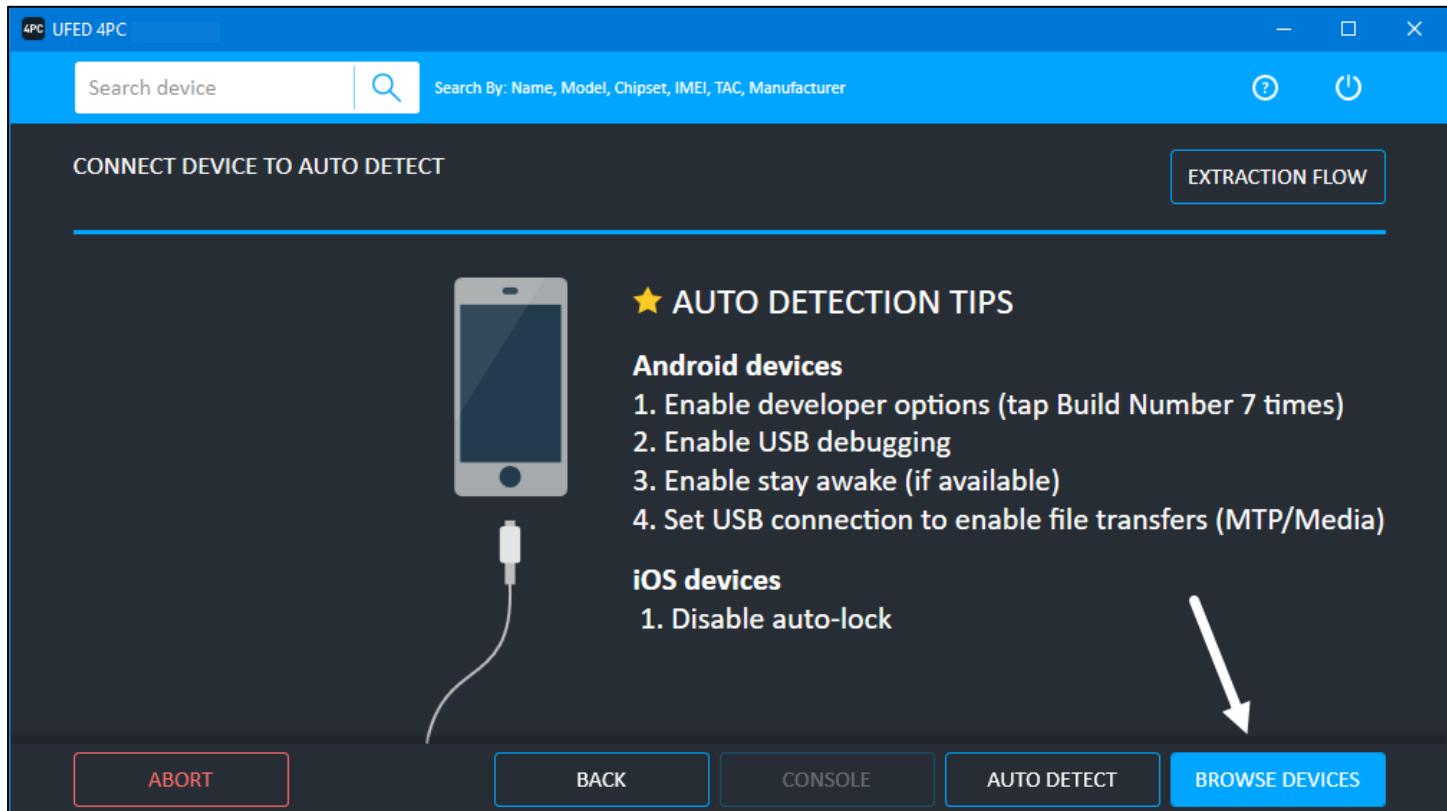
16. Instructions to prepare the device appear again, in more depth. If the **CONTINUE** button is not highlighted, unplug and re-plug the device. If you did not perform the instructions previously, perform them now. Once done and re-plugged, the **CONTINUE** button will be highlighted. Click on it.



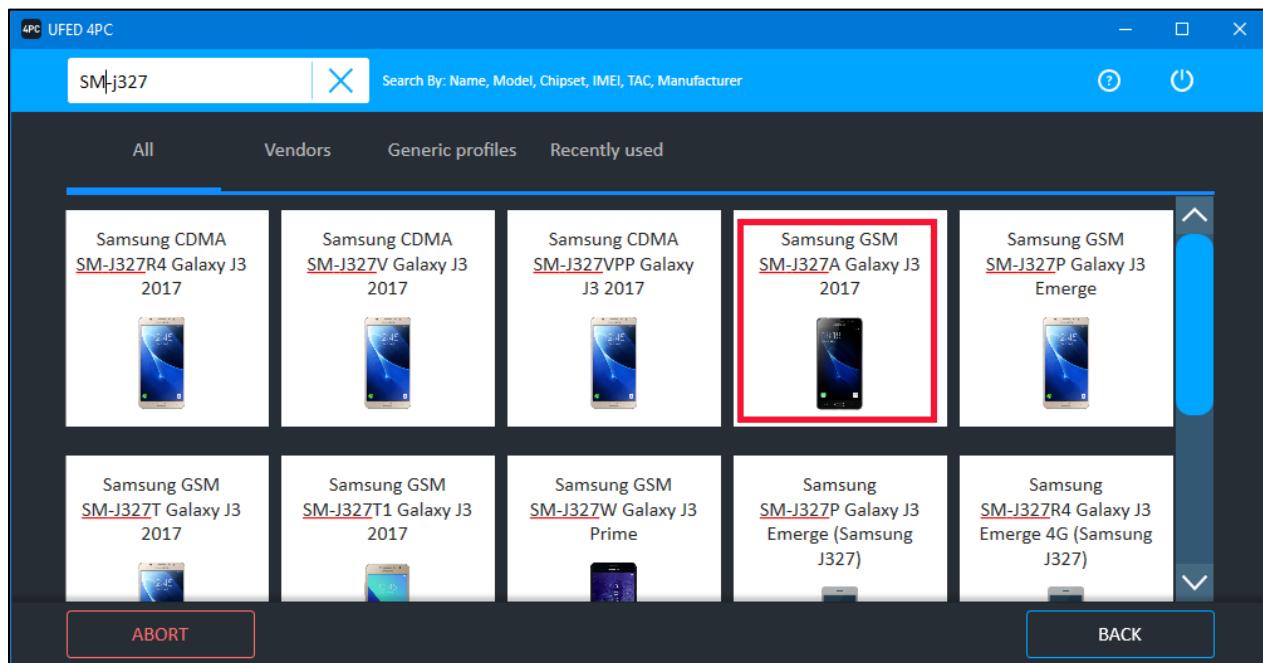
17. You may receive some prompts regarding allowing your device to connect. You will now be taken to the actual acquisition portion of the exercise. Proceed to **Section 5** of this exercise to continue.

## Exercise - Section 4 – STEPS IF DEVICE NOT DETECTED

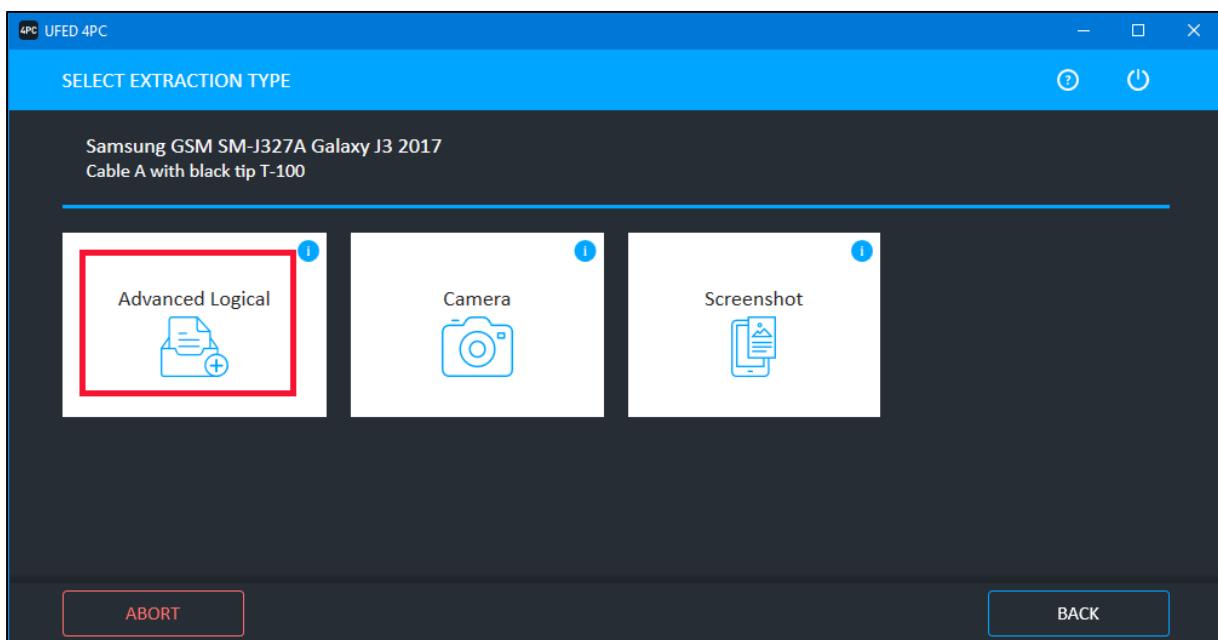
1. Click on the **BROWSE DEVICES** button.



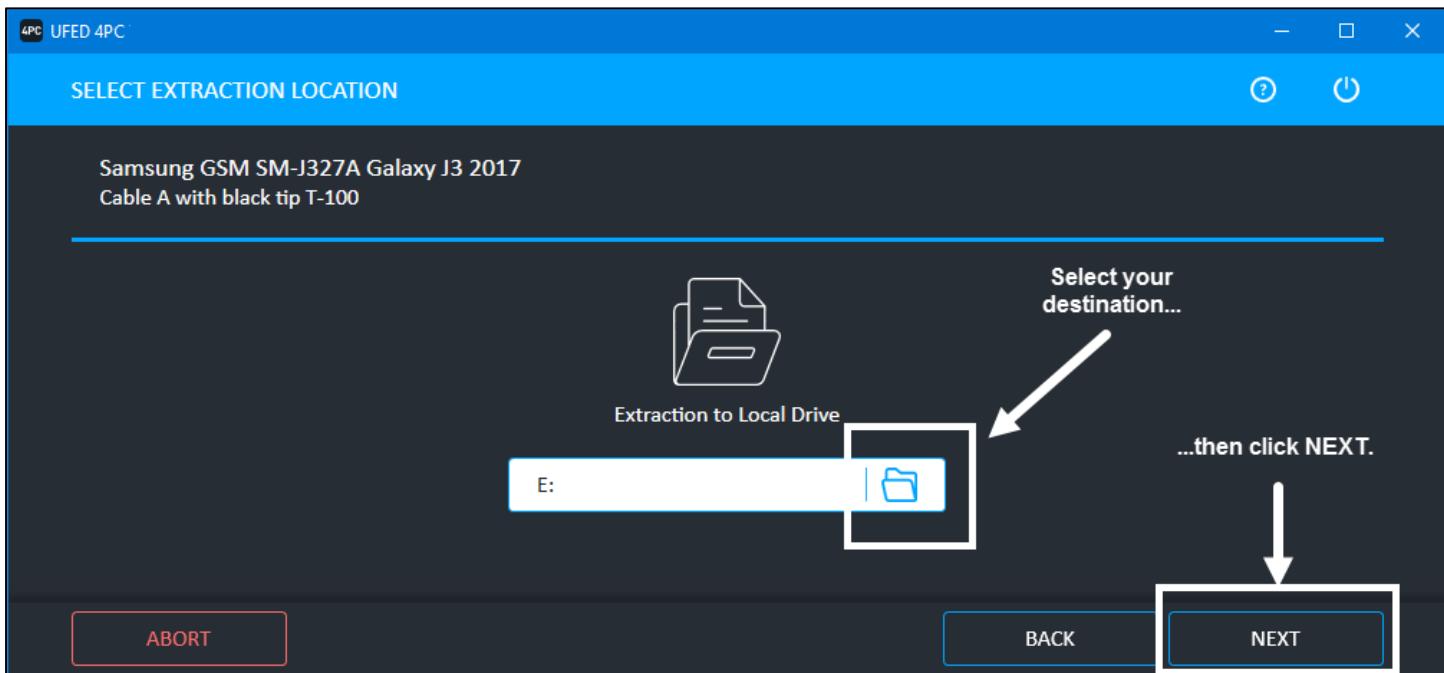
2. You will see a number of options available to locate your device. You can detect by model, vendor, profile, and others. Type your model number in the **Search device** box. As you type, you will see the list of possible devices get shorter. If you type the full model number in and find zero options, remove the last character from the model number, and select the closest match from what is left. This may not always be obvious, as is the case below. The model of the device in the example is a **SM-J327W**, however typing the entire model number shows no matches. Removing the **W** shows a few. With no other guidance, you may have to do more than one collection and compare the results. In the case below, **SM-J327A** would be my choice.



3. Once the model has been selected, you will see the **SELECT EXTRACTION TYPE** screen. For the purpose of this exercise, and in most cases in the field for the purpose of rapid extraction, you will select the **Advanced Logical** option.

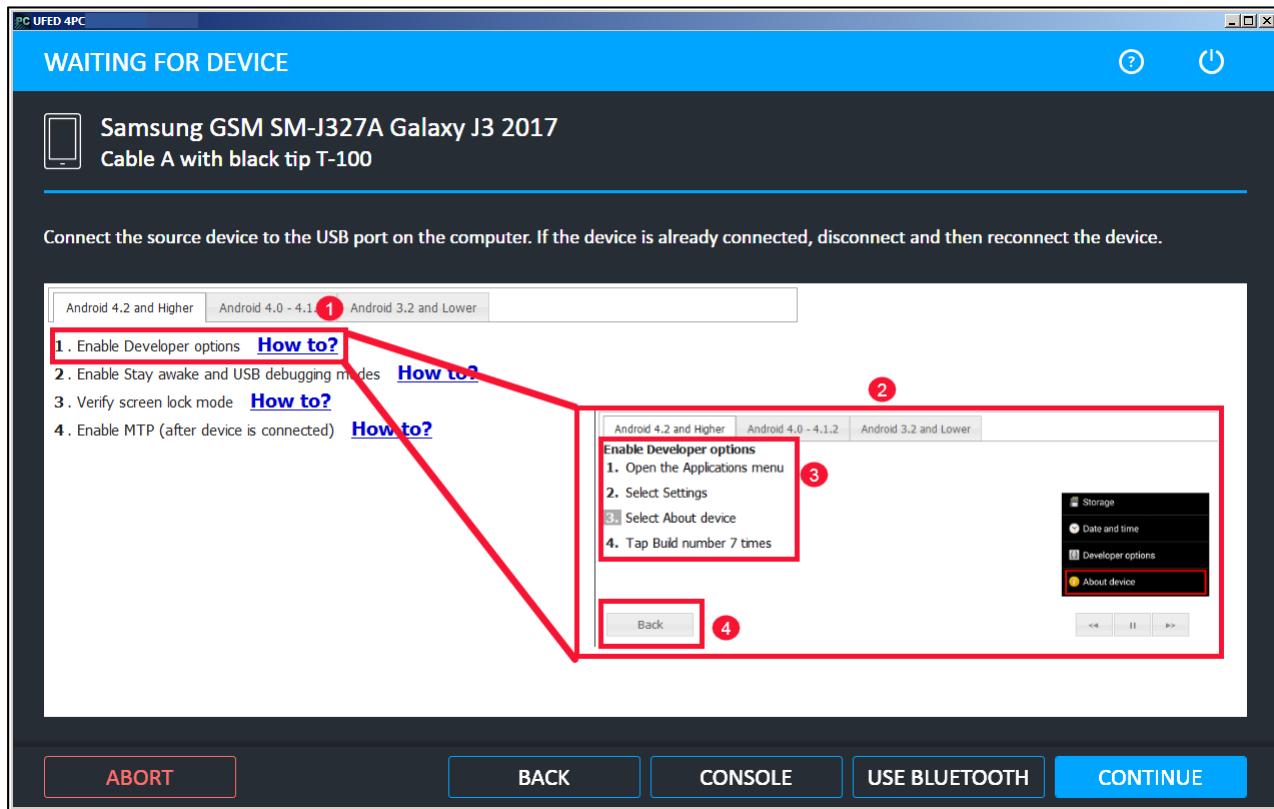


4. Choose where to save the extraction. Connect your student supplied external hard drive to your **FOR498 Windows VM**, then click the **Browse** icon to the right of the destination path and save the extraction to the root of your external hard drive. Click **Next**.



5. The next screen will advise you to perform several tasks on your device to prepare it for acquisition, as well as provide instructions on how to do so. It is important to perform these tasks. **As indicated by the instructions in the on-screen prompts, you should unplug and re-plug your device at this time.** Although the next number of steps should be fairly standard across all Android devices, there are specific instances where the Cellebrite software instructions (as helpful as they try to be) simply are not exactly like what an examiner may face. We will attempt to show variables on certain instructions, but again common sense may be the only dictator of the next step.

6. On your computer, you should see instructions as below, outlining the above-mentioned tasks. The first option is to **Enable Developer options**. You also see a clickable link immediately following that option entitled **How to?**. Clicking on this will bring up (usually) step by step instructions on how to perform the given task, if you need them.



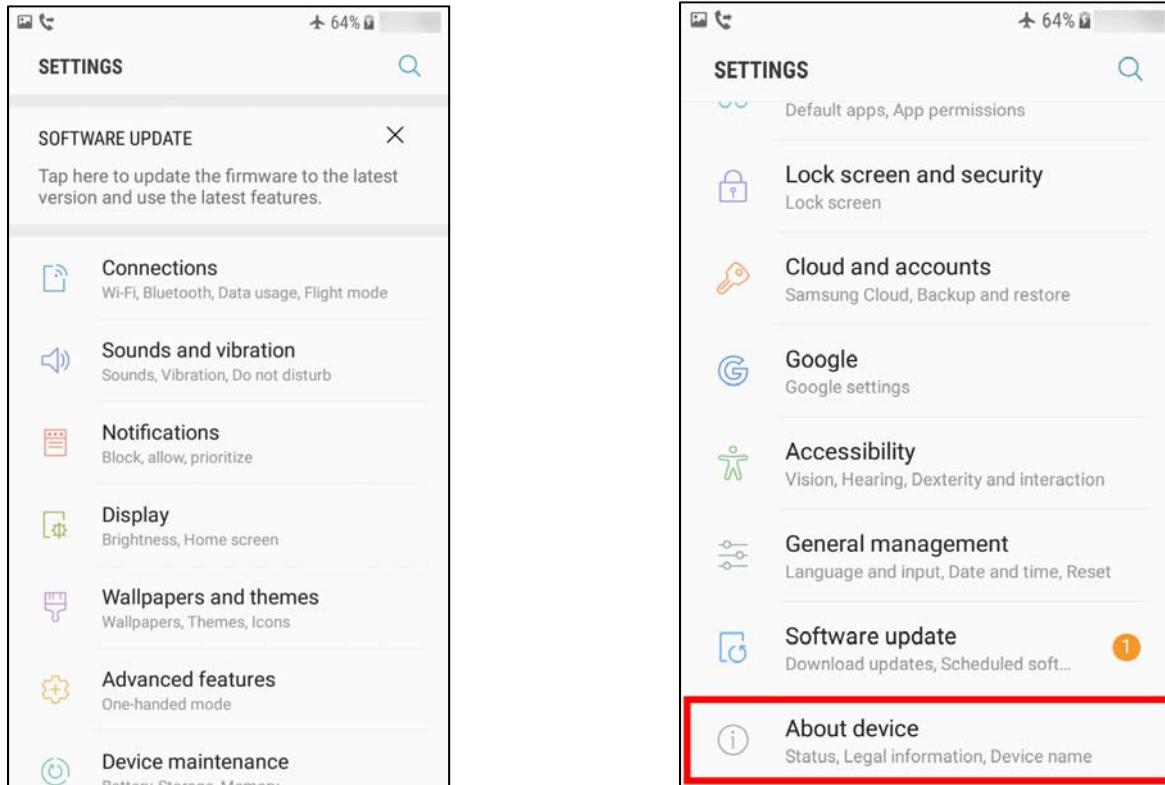
If you are comfortable following the instructions presented by the Cellebrite software, perform them and then move on to **Step 11** below.

If the options on the particular device you are acquiring differ from what you are told by the Cellebrite software, or if you want more in-depth instructions, they follow here.

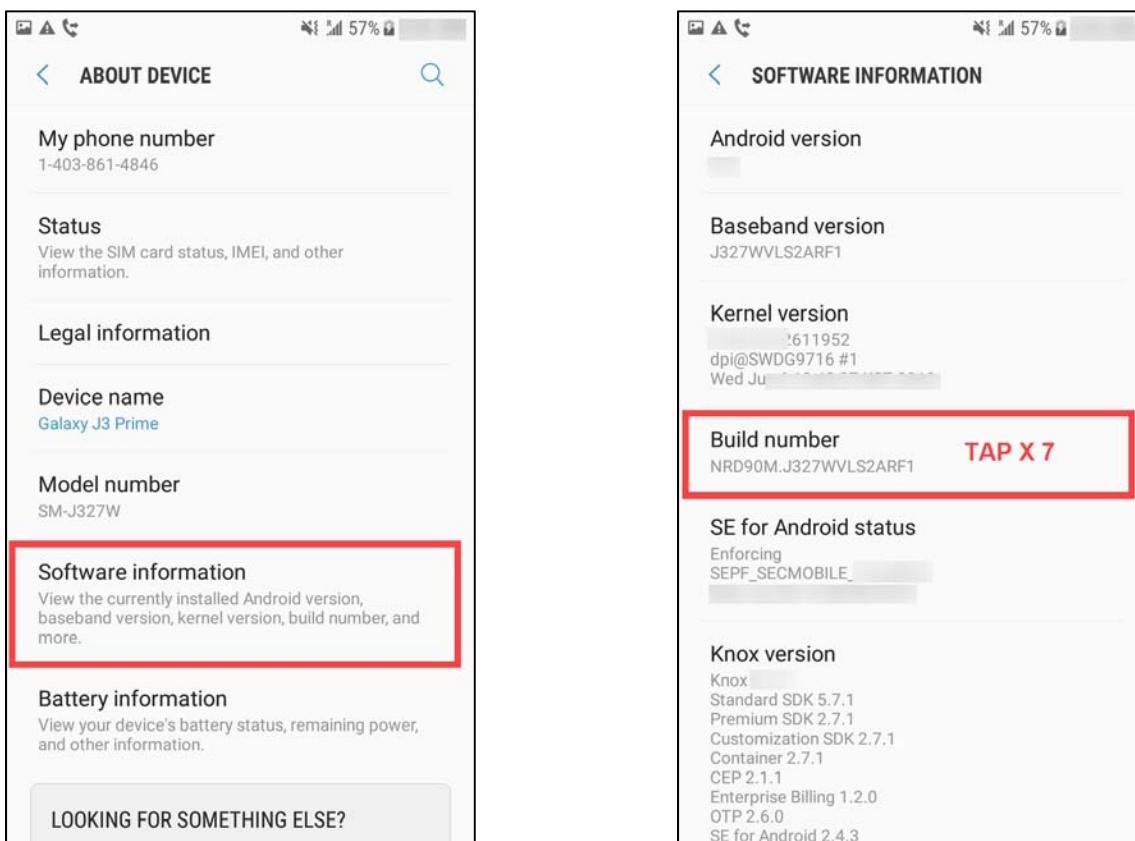
7. Open the **Apps** menu on the device and select **Settings**.



8. Scroll down the list of available settings and locate **About device** or **About phone**. Tap to open it.



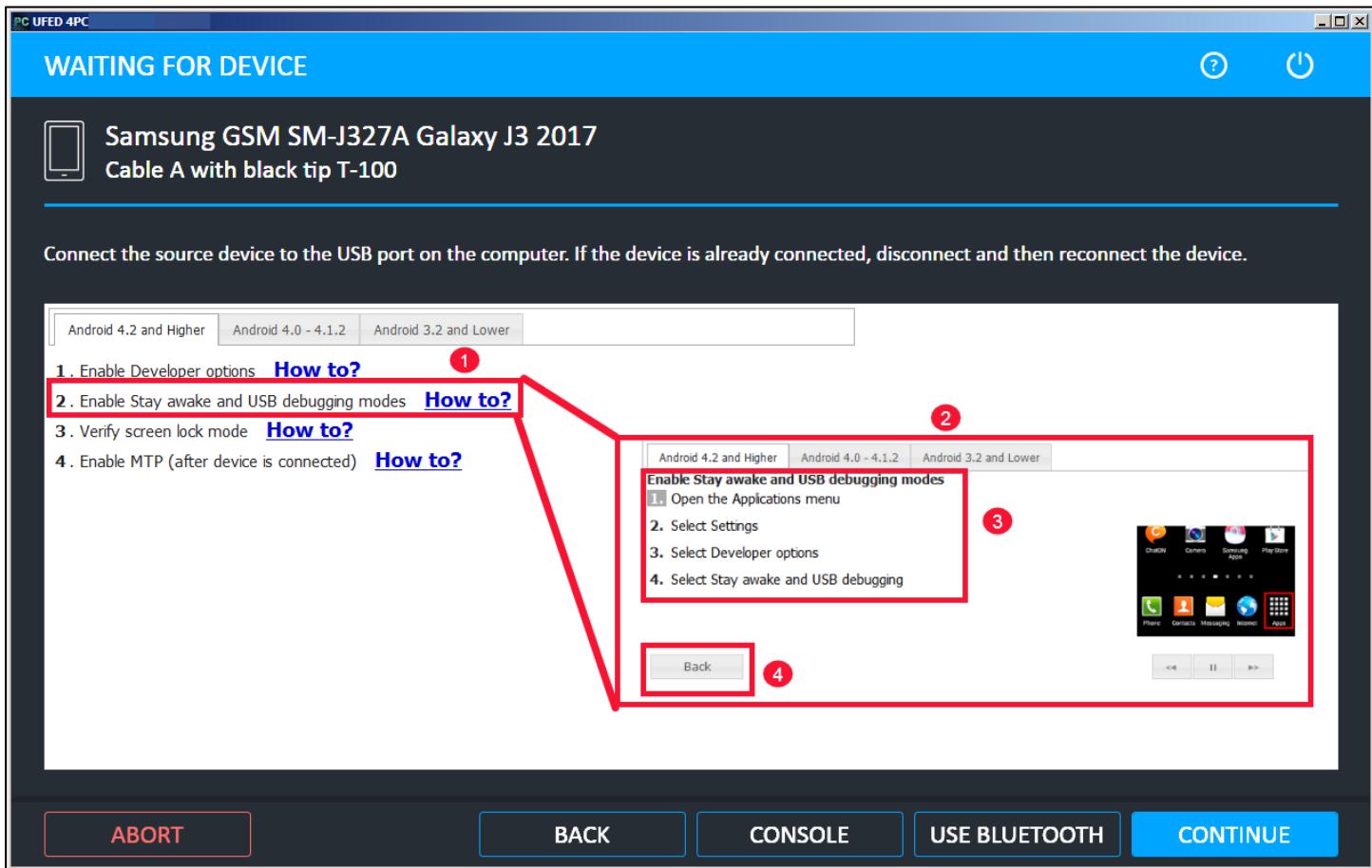
9. In the next screen you see, locate an option entitled **Build number**. If you do not see a **Build number** option, locate the **Software information** option as seen below, and tap on it to see the **Build number** option. Once you locate it, tap on it 7 times...



10. ...and you will see a note on the screen indicating that **Developer mode has been enabled**.



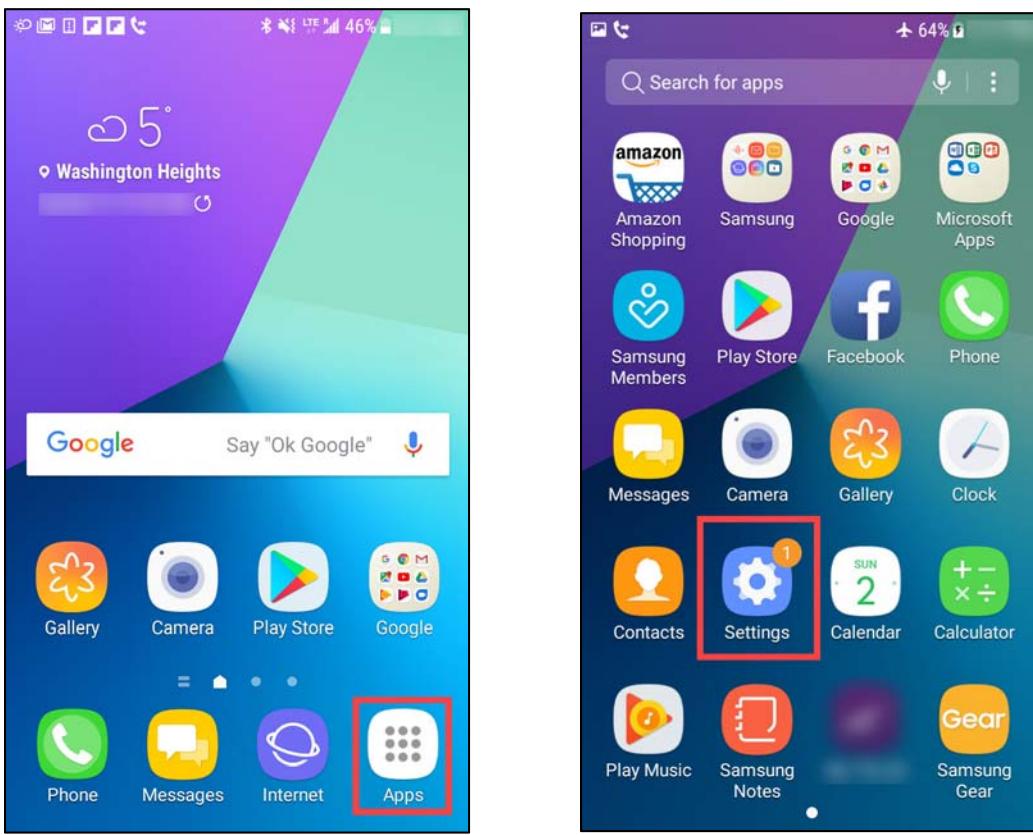
11. Now refer back to your computer and the Cellebrite software and click the **Back** button to be taken back to your preparation steps list. **Number 2** on the list is **Enable Stay awake and USB debugging modes**, and once again, you will see to the right of this, the **How to?** link. Click on the link for instructions on how to perform these tasks.



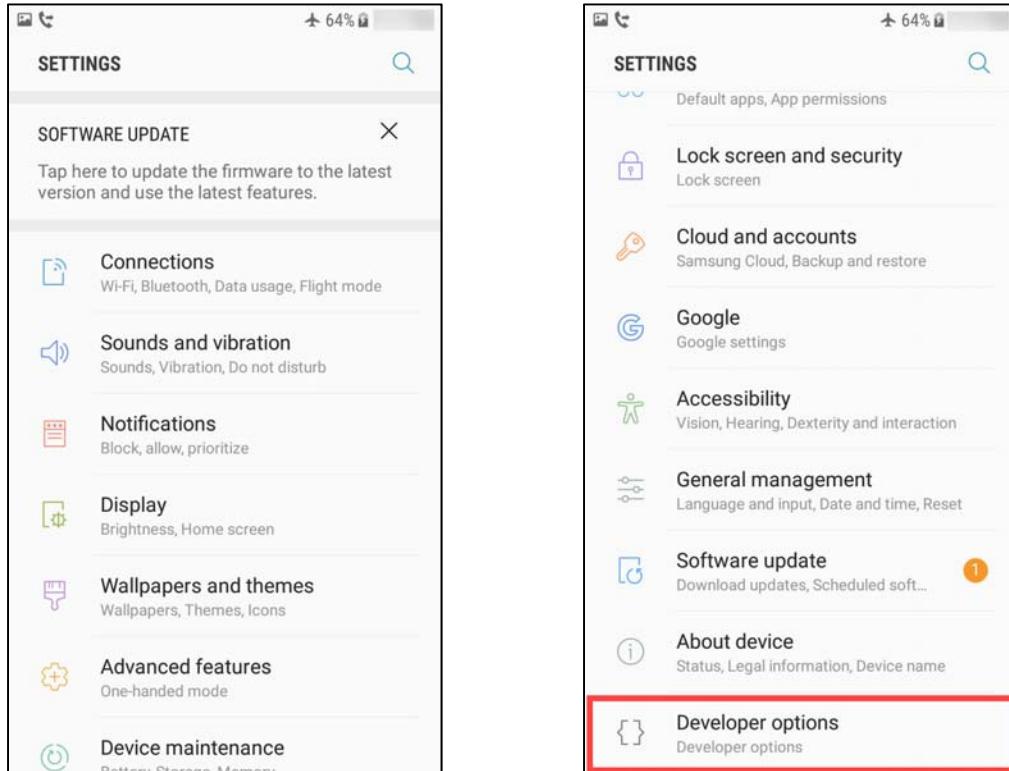
12. Once again if you are comfortable following the instructions presented by the Cellebrite software, perform them and then move on to **Step 17** below.

If the options on the particular device you are acquiring differ from what you are told by the Cellebrite software, or if you want more in-depth instructions, they follow here.

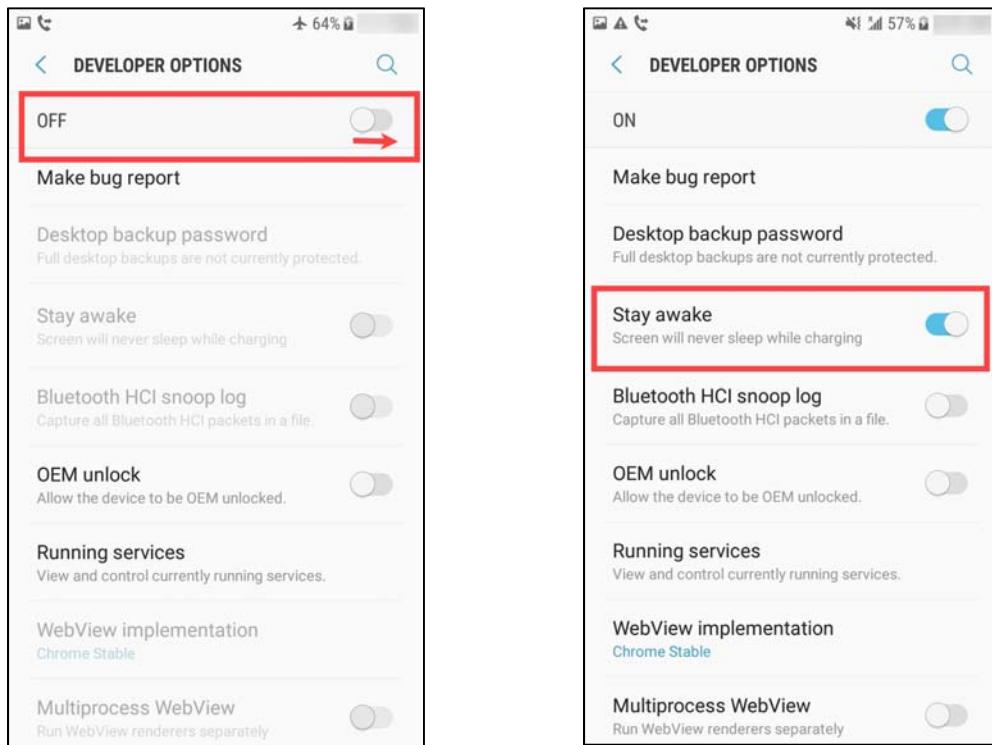
13. Open the **Apps** menu on the device and select **Settings**.



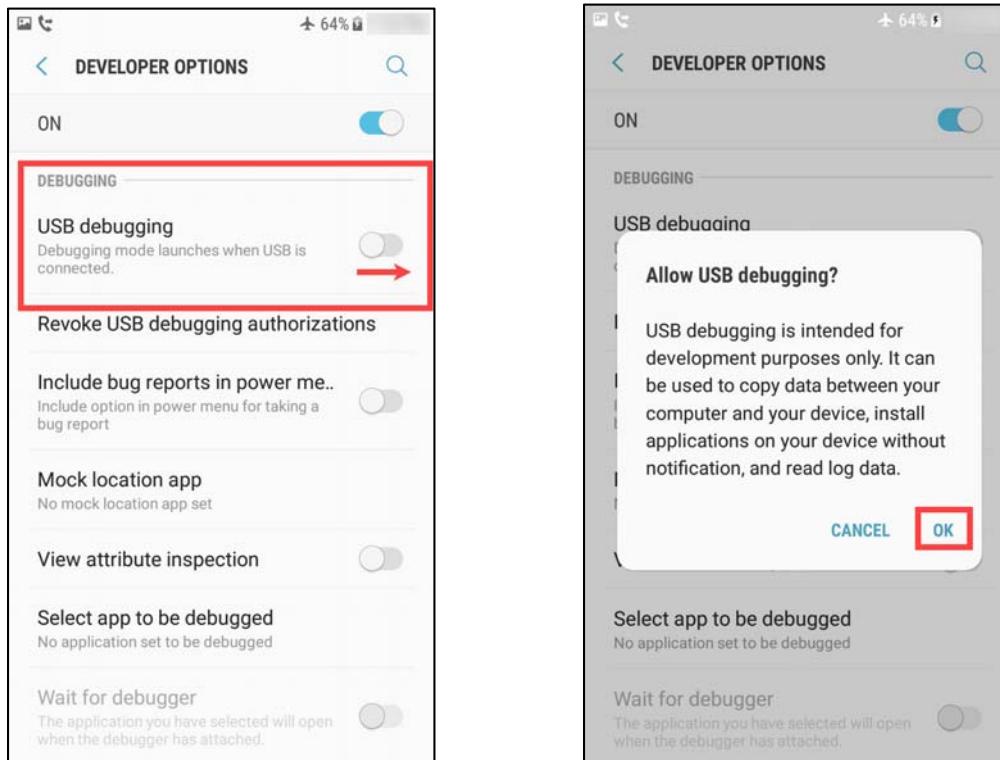
14. Scroll down the list of available settings and you should now see a new option below **About device** or **About phone**, called **Developer options**. Tap to open it.



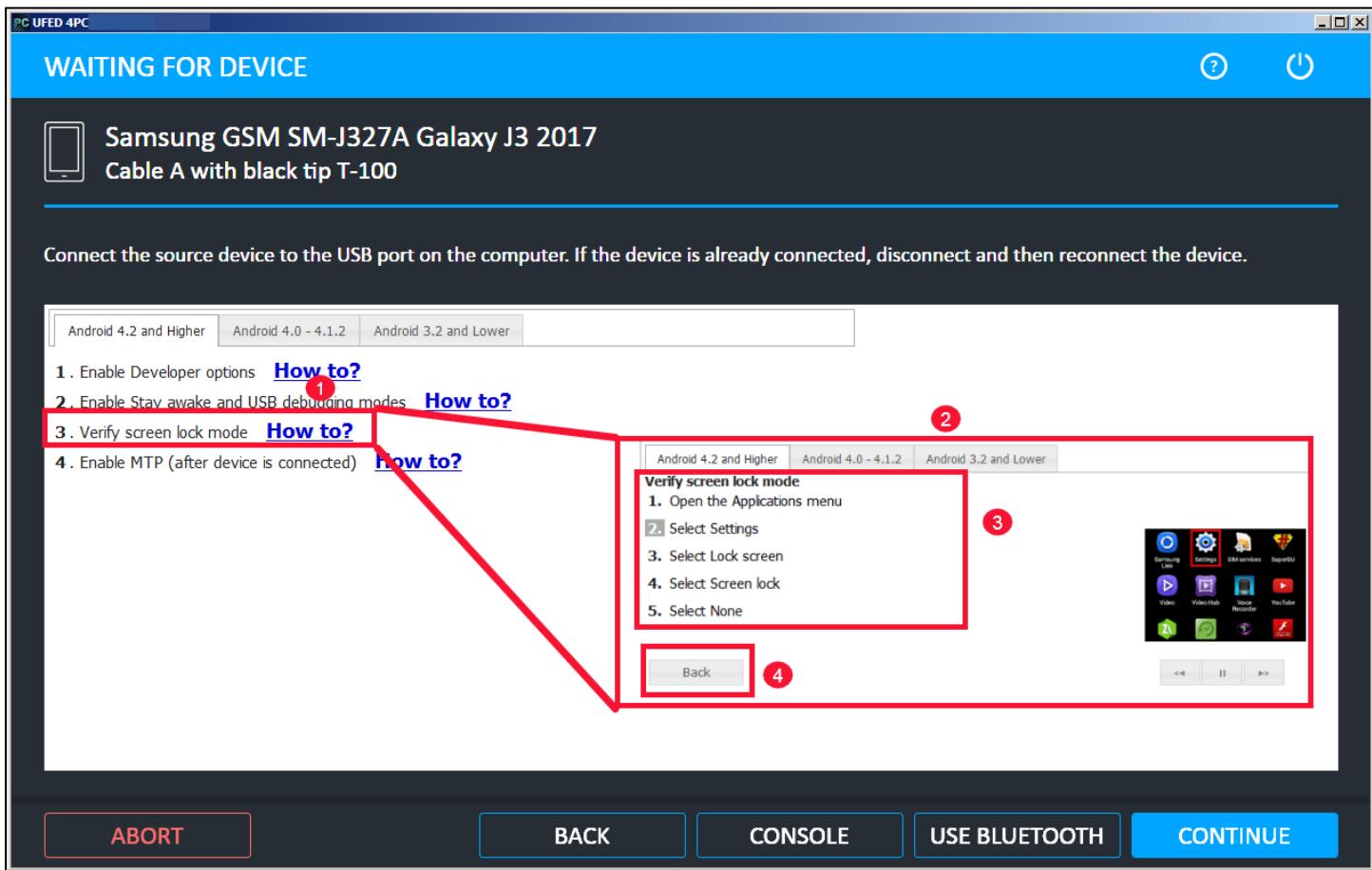
15. In the **DEVELOPER OPTIONS** menu, ensure the options are **ON**. If they are not, swipe the slider to the **ON** position. Further down the list of options is the **Stay awake** option. Ensure this is on, and if it is not, swipe it to the **ON** position. If you see any confirmation prompts at any time, accept them.



16. Scroll down the list of **DEVELOPER OPTIONS** until you see an option entitled **USB debugging**. Again, if it is off (greyed button), then swipe it to the **ON** position, and accept any confirmation requests.



17. Refer back to your computer and the Cellebrite software and click the **Back** button to be taken back to your preparation steps list. **Number 3** on the list is **Verify screen lock mode**, and once again, you will see to the right of this, the **How to?** link. Click on the link for instructions on how to perform this task.



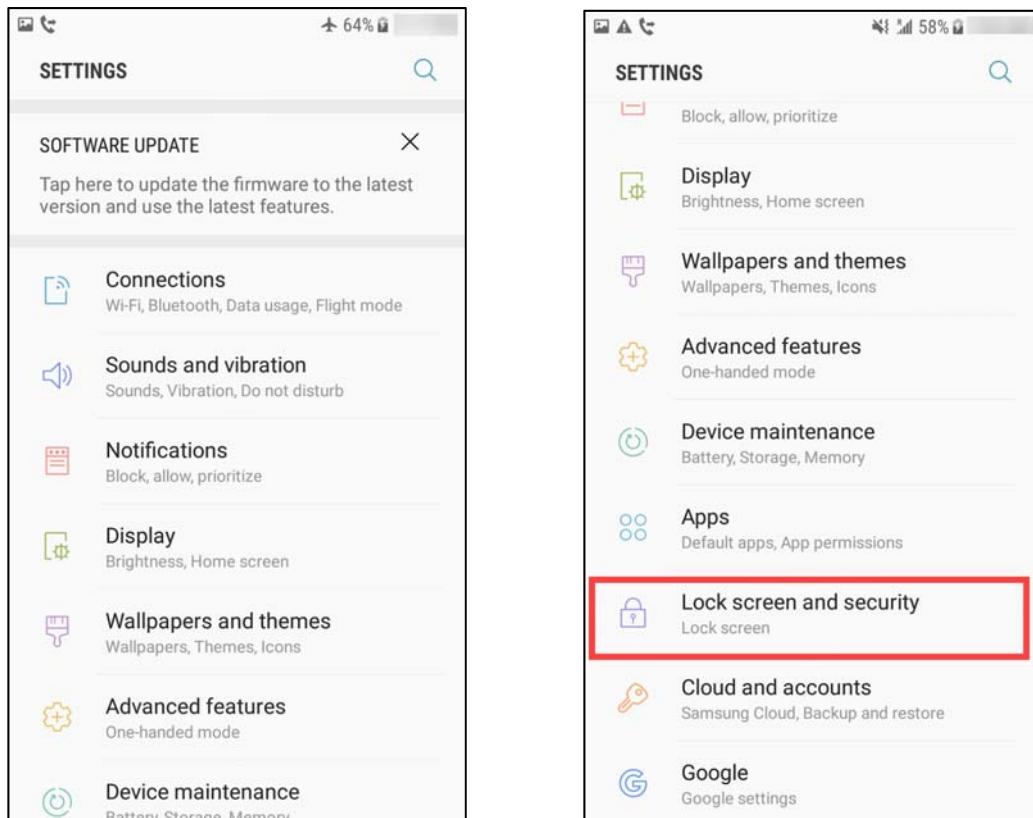
18. Once again if you are comfortable following the instructions presented by the Cellebrite software, perform them and then move on to **Step 23** below.

If the options on the particular device you are acquiring differ from what you are told by the Cellebrite software, or if you want more in-depth instructions, they follow here.

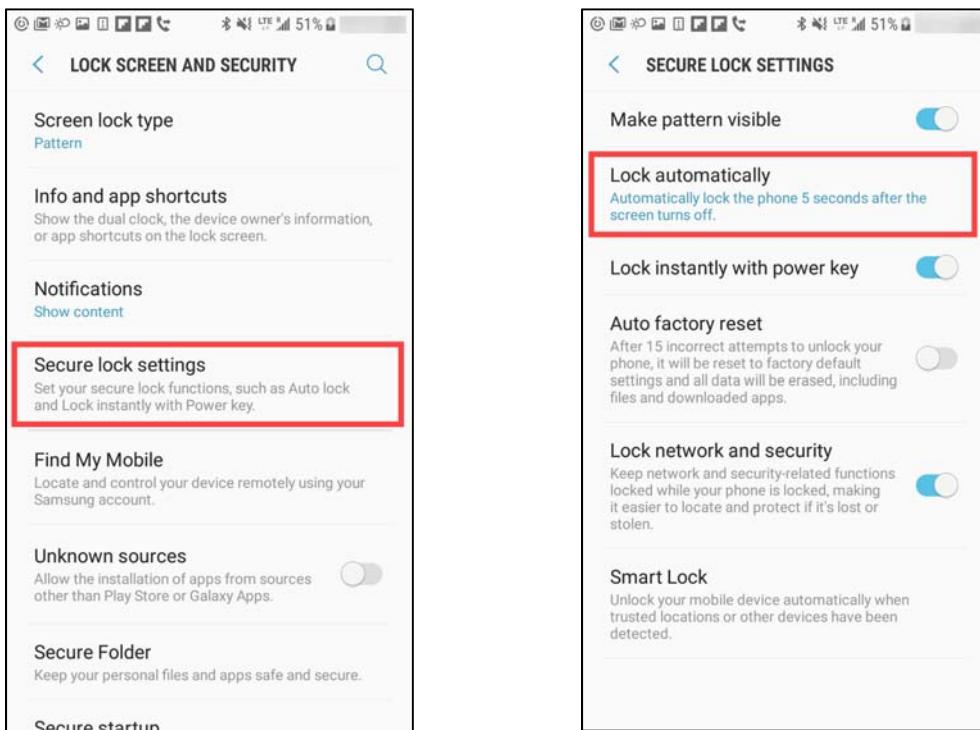
19. Open the **Apps** menu on the device and select **Settings**.



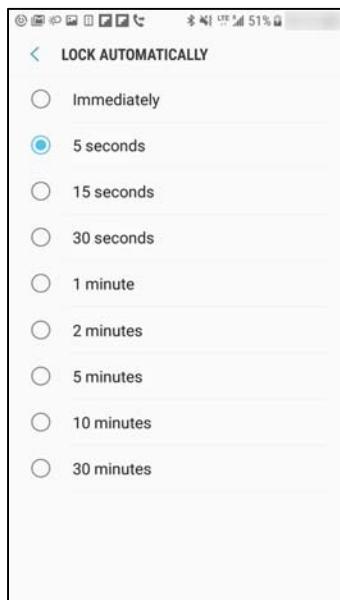
20. Scroll down the list of available settings and you should see an option called **Lock screen and security**. Tap to open it.



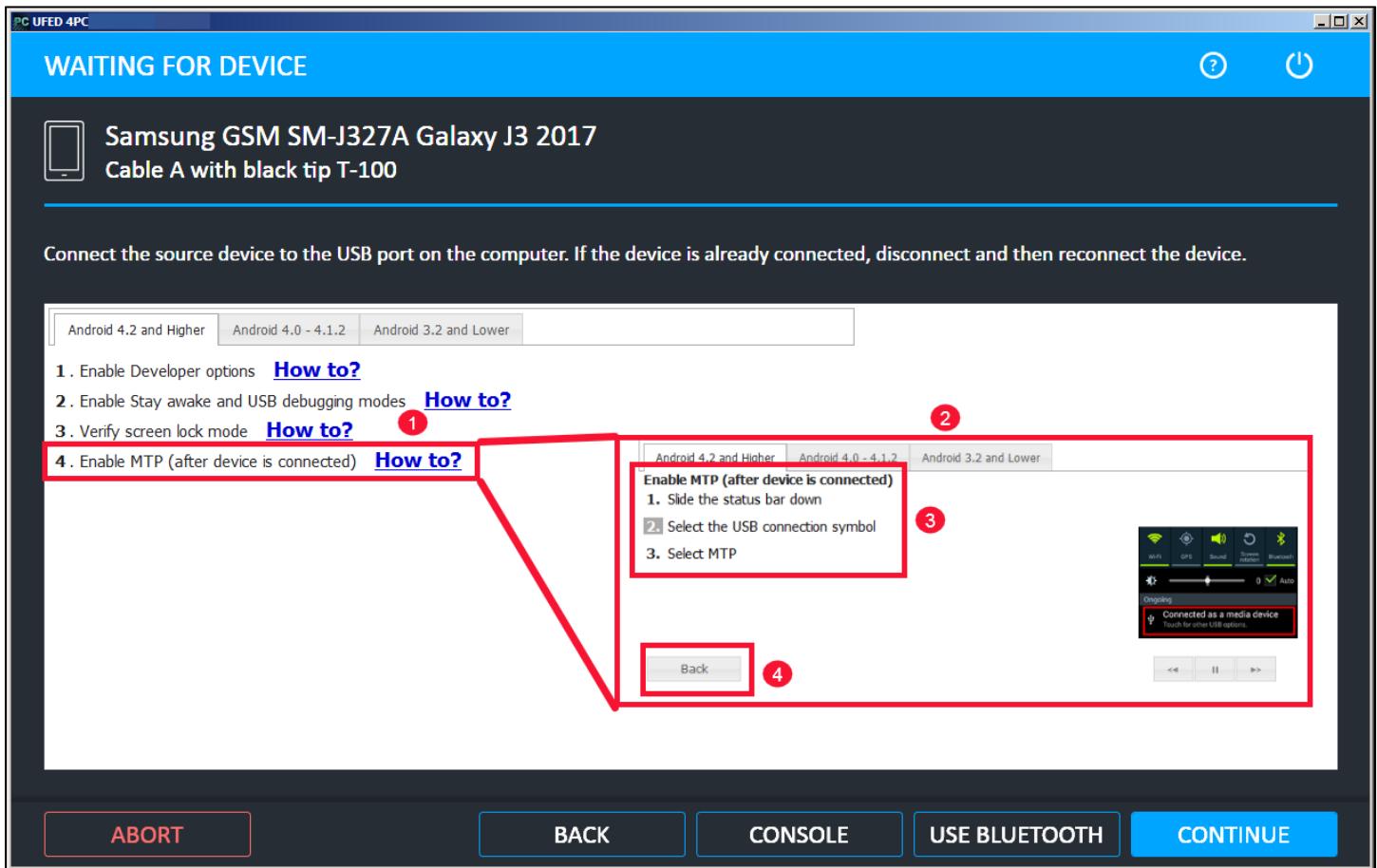
21. You will see an option called **Secure lock settings**. Tap on it to open. You will see an option called **Lock automatically**. You may see what appears to be clickable text below the title that states **Automatically lock the phone in X seconds after the screen turns off**. If you see this, and if you had previously enabled **Stay awake**, you will not need to make any changes.



22. Depending on the model of device and version of OS, the option you see may be subtly different in verbiage from "**Lock automatically**". It may be something like "**Lock screen time out**". In that case, when you tap on the option, you will be presented with a screen of time out options, as seen below. If there is an option for **Never**, that would be the one to select. If that option is not available, select the option with the most time, such as **30 minutes** or more. If the device lock screen enabled automatically during an acquisition, it could negatively affect, or even cancel the acquisition.



23. Refer back to your computer and the Cellebrite software and click the **Back** button to be taken back to your preparation steps list. **Number 4** on the list is **Enable MTP (after device is connected)**, and once again, you will see to the right of this, the **How to?** link. Click on the link for instructions on how to perform this task.

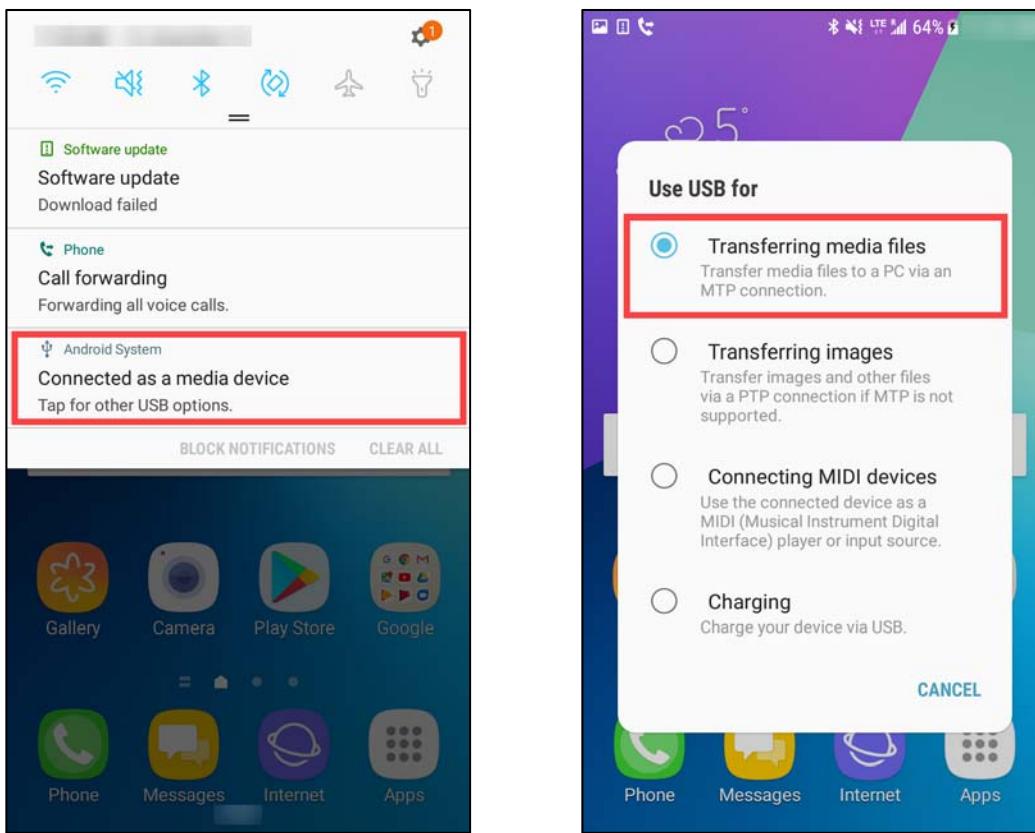


24. If you are comfortable following the instructions presented by the Cellebrite software, perform them and then move on to **Step 30** below.

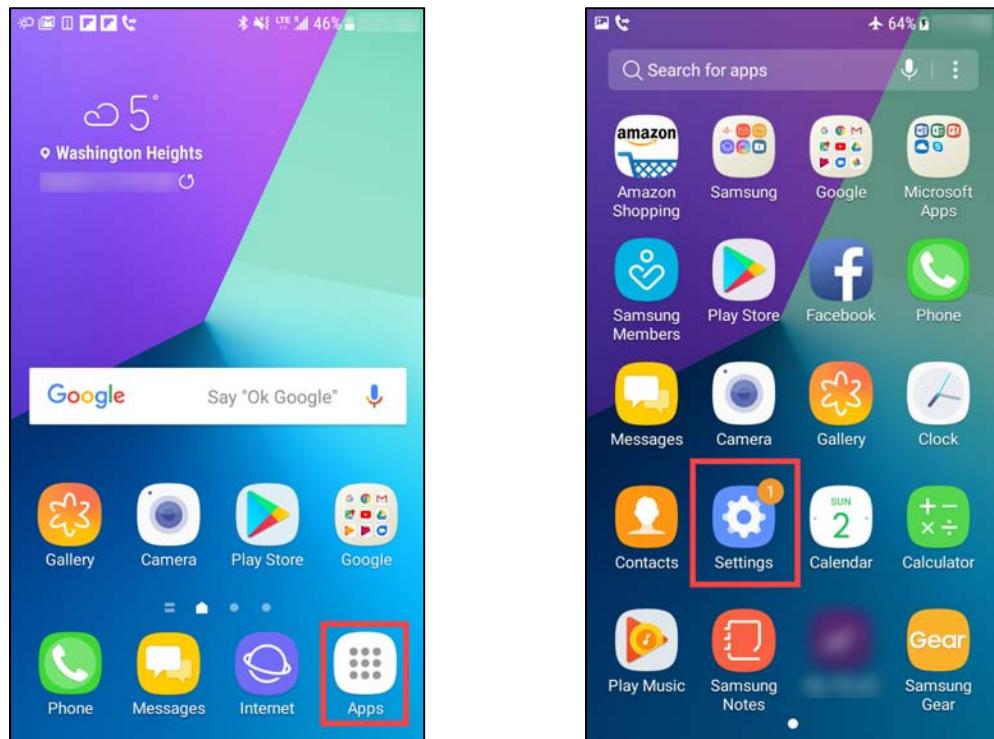
If the options on the particular device you are acquiring differ from what you are told by the Cellebrite software, or if you want more in-depth instructions, they follow here.

25. There are generally two ways to perform this function. They will be listed here in order of ease of performance.

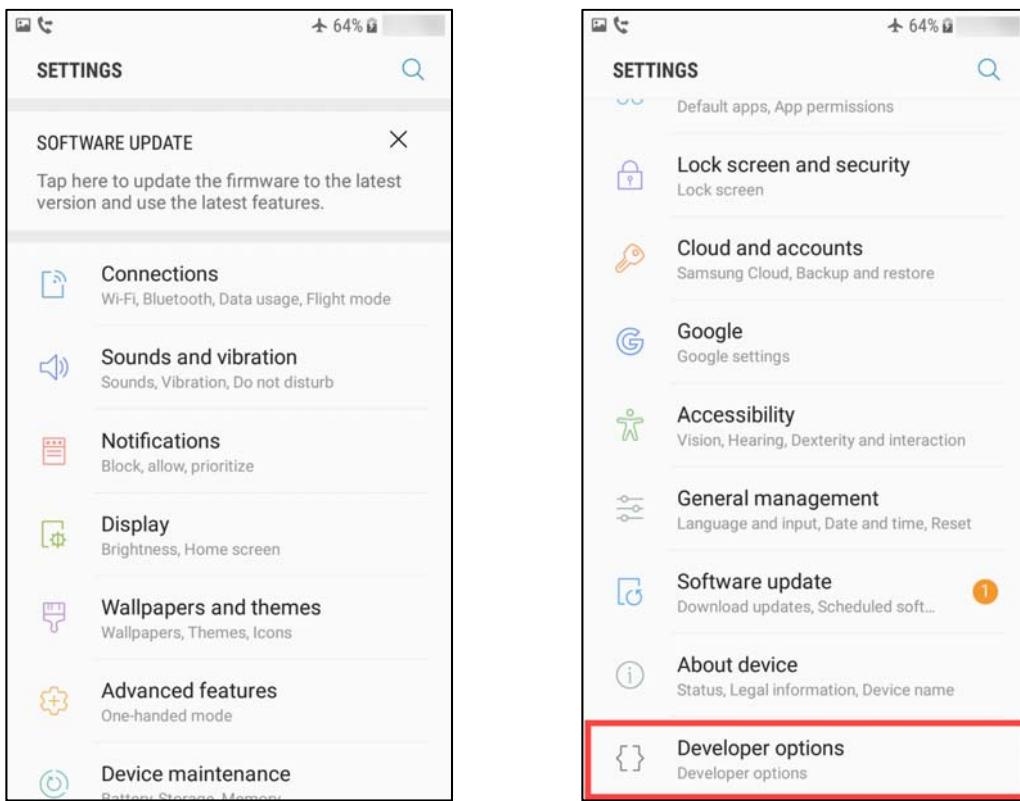
26. Method 1 starts with swiping down from the top of the device screen. Then locate the item in the list that says, **Connected as a media device**. Tap on this item, and you will see a new window open with a few options. Select **Transferring media files**, and you have achieved the goal. Proceed to **Section 5**.



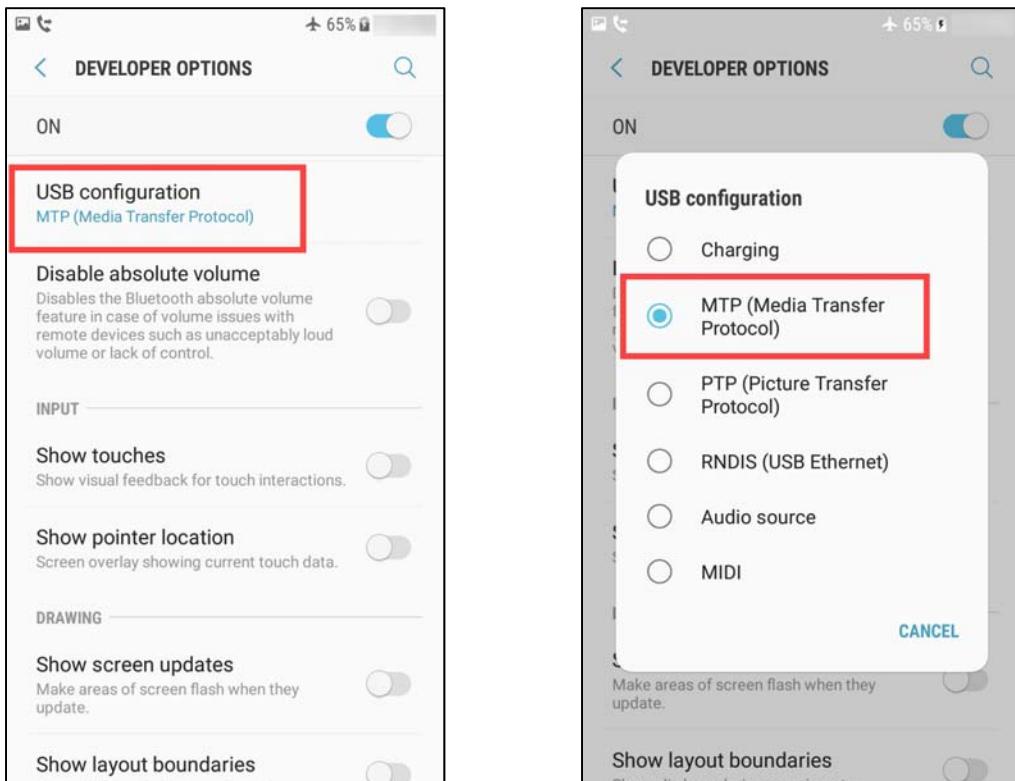
27. In method 2, open the **Apps** menu on the device and select **Settings**.



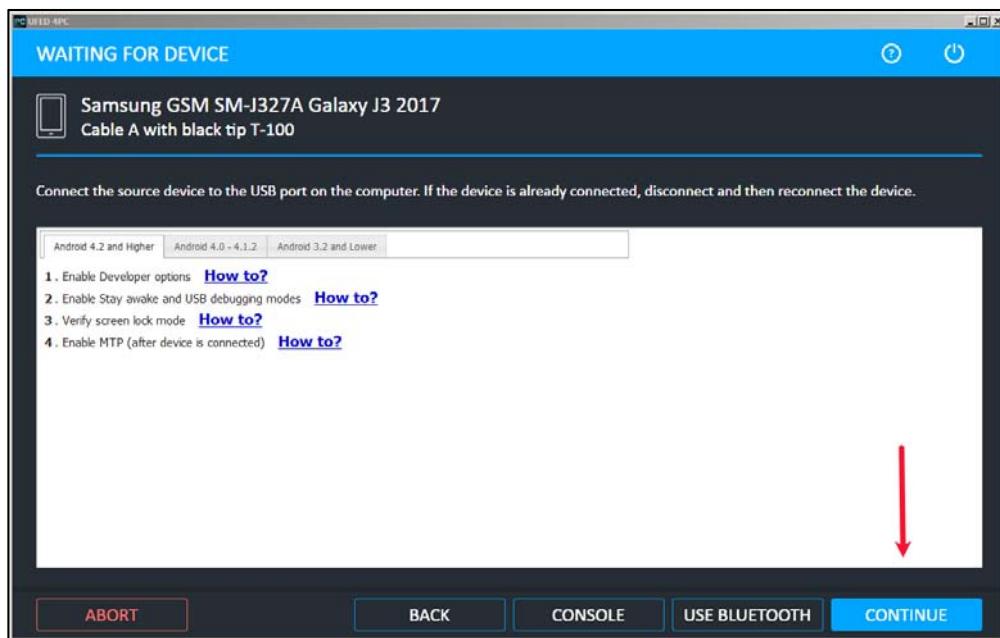
28. Scroll down the list of available settings and tap on **Developer options** to open it.



29. Scroll down the long list of **DEVELOPER OPTIONS** until you see an option entitled **USB configuration**. Tap on this option. A box will pop up with several options. Select the **MTP (Media Transfer Protocol)** option. If you get any confirmation prompts, accept them.

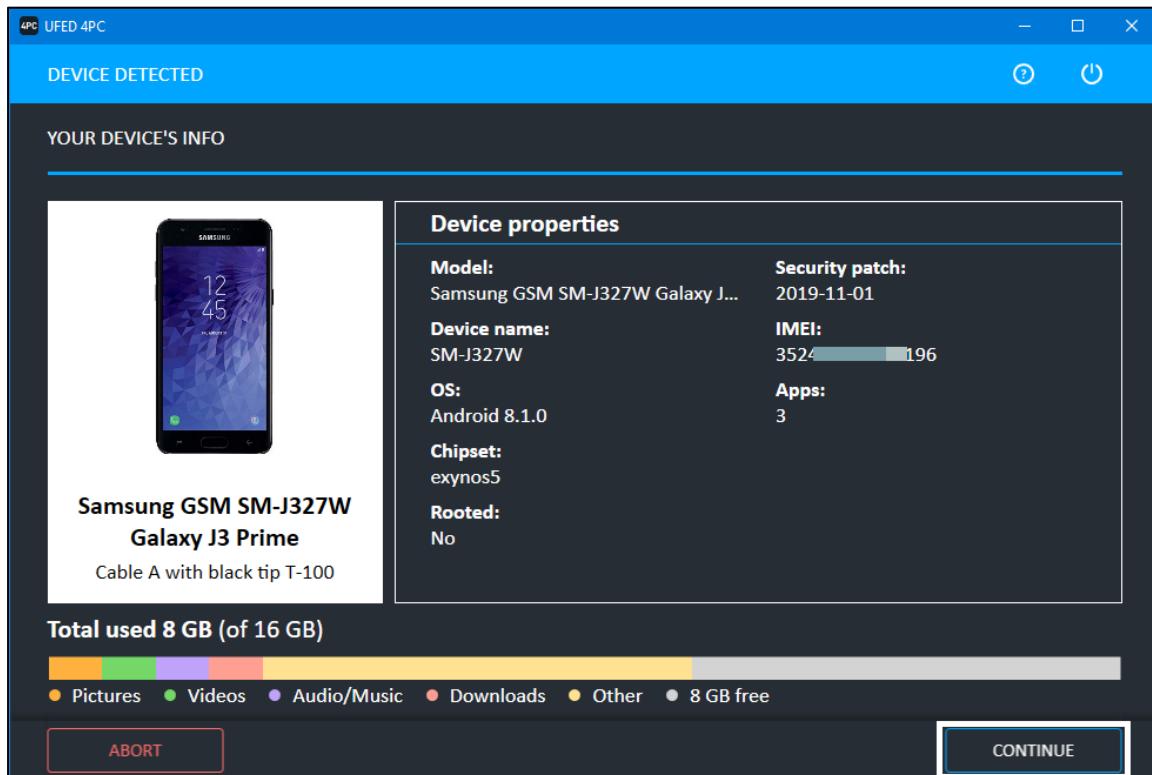


30. Refer back to your computer and the Cellebrite software and click the **Back** button to be taken back to your preparation steps list. At this point, click on **Continue**. If it is not highlighted, disconnect and reconnect the device.

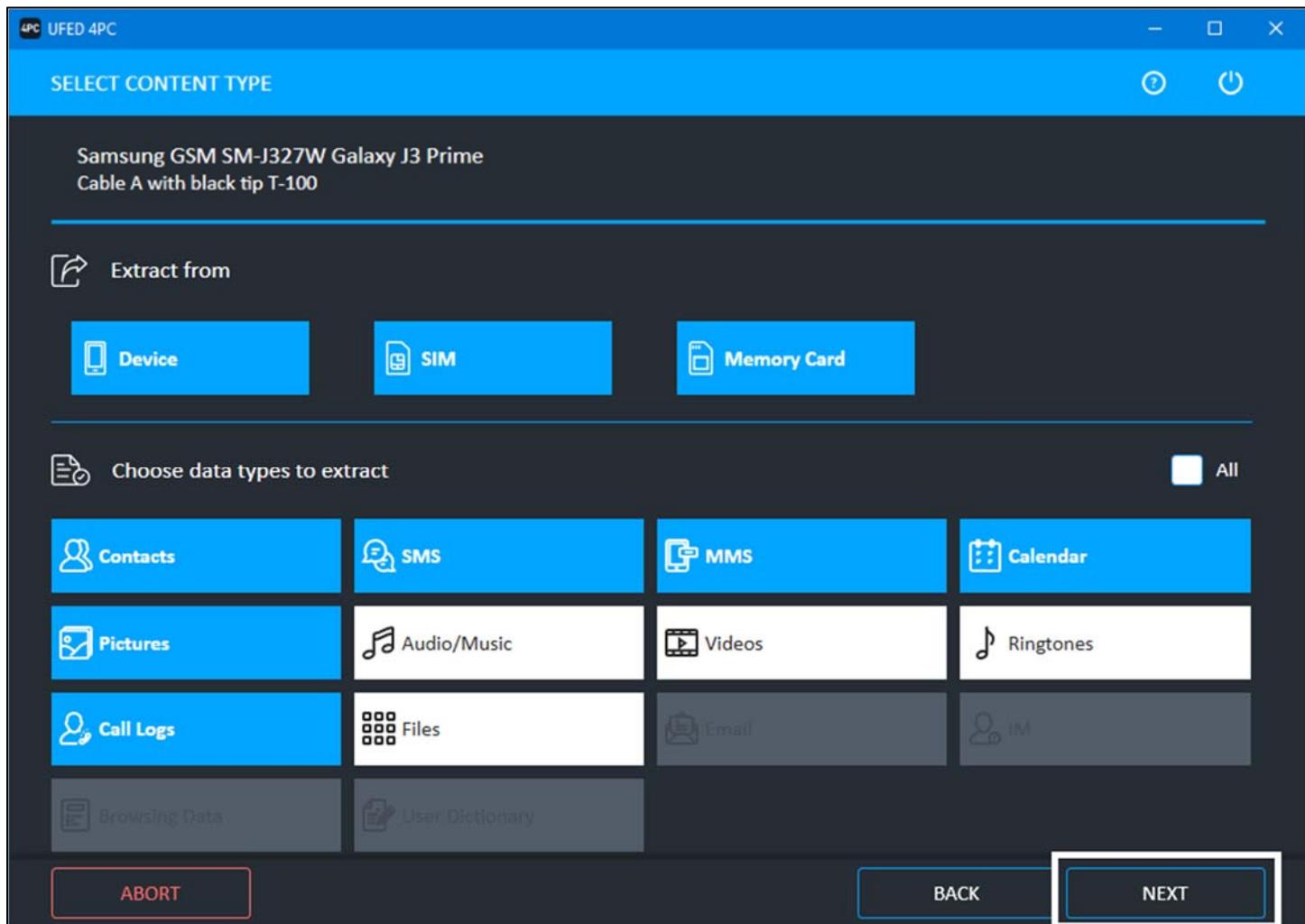


### Exercise - Section 5 – DEVICE ACQUISITION

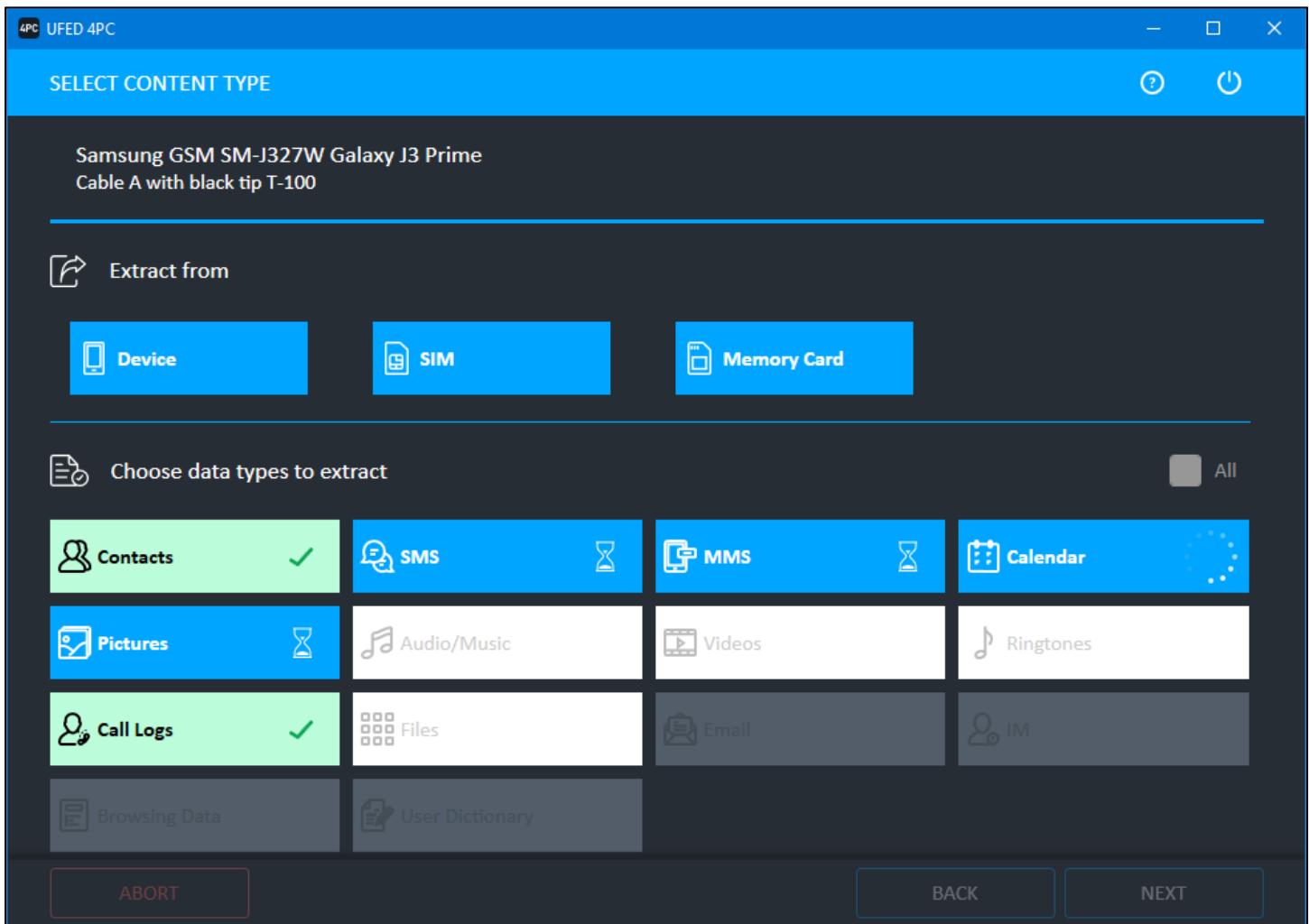
1. You will see a screen showing your device info. Review, or even take a photo or screenshot, and then click **CONTINUE**.



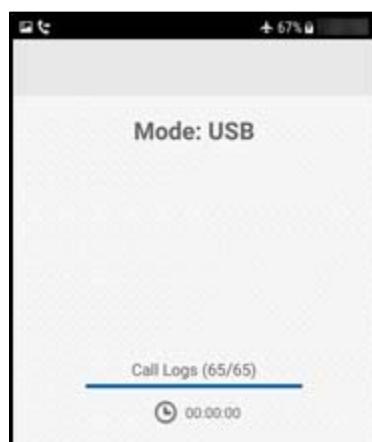
2. You will be presented with a screen showing various options available for extraction. Almost certainly, your computer screen will show different options than the ones below. These vary from device to device. Everything that **UFED 4PC** CAN access will be highlighted in blue, but for the purpose of this exercise, we have limited the selection. Choose only the artifacts highlighted in the screen below, if it is available at all. (Highlighted below means the more shaded boxes). Then click **NEXT**.



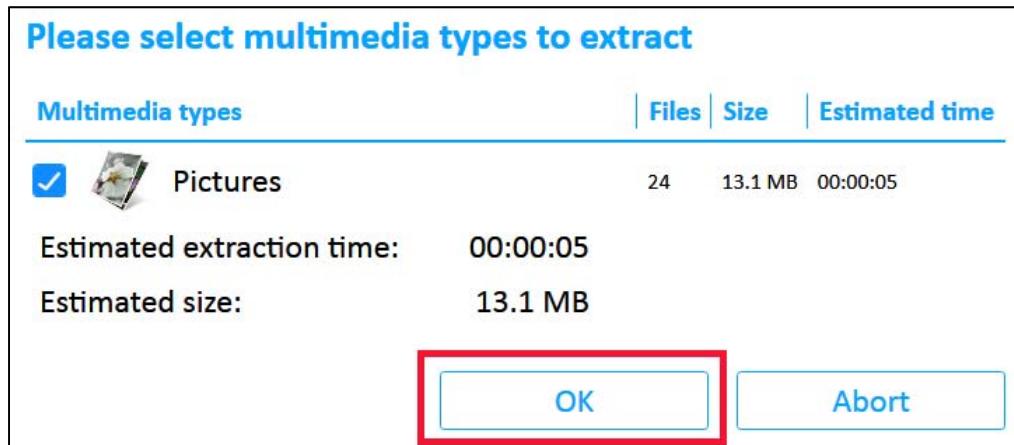
- The acquisition process will start, and you will see progress in the form of hourglasses, and spinning wheels, as well as artifact boxes turning green. You may be prompted to tap **ALLOW** on the screen of your device.



- You may see screens come and go on the device you are acquiring, such as the one below. If this happens, do NOT respond on the device unless requested to by the **UFED 4PC** program. You must keep a sharp eye on your device and your computer screen. If a prompt appears and you do not respond within a certain amount of time, the acquisition may stop/fail.



5. If any pop-ups appear asking for input, read and act upon them, based on what your needs are. In the example below, we are being prompted for which types of multimedia we want to extract.



6. The storage size of the device, as well as density of data, will dictate how long the process will take. It could be anywhere from 5 minutes to 35 minutes, or longer. You will be informed once the acquisition is complete. At that time, a screen from UFED 4PC will inform you to go back into the device and return the settings back to the way they were. This is typically not done on suspect devices, unless they are being returned after acquisition. Either perform the functions or click **Continue**.

### Source Instructions

**SM-J327W Galaxy J3 Prime:**  
Please restore the connection settings:  
Menu (Apps) → Settings (More) → Developer options/Advanced Settings → clear check boxes "USB debugging" and "Stay awake" (when present).

CONTINUE

#### RESTORE SCREEN FOR AUTO-DETECTED DEVICE

### Source Instructions

Android 4.2 and Higher    Android 4.0 - 4.1.2    Android 3.2 and Lower

1. Disable Stay awake and USB debugging modes [How to?](#)
2. Verify screen lock mode [How to?](#)
3. Disconnect the device from the cable

CONTINUE

#### RESTORE SCREEN FOR NON AUTO-DETECTED DEVICE

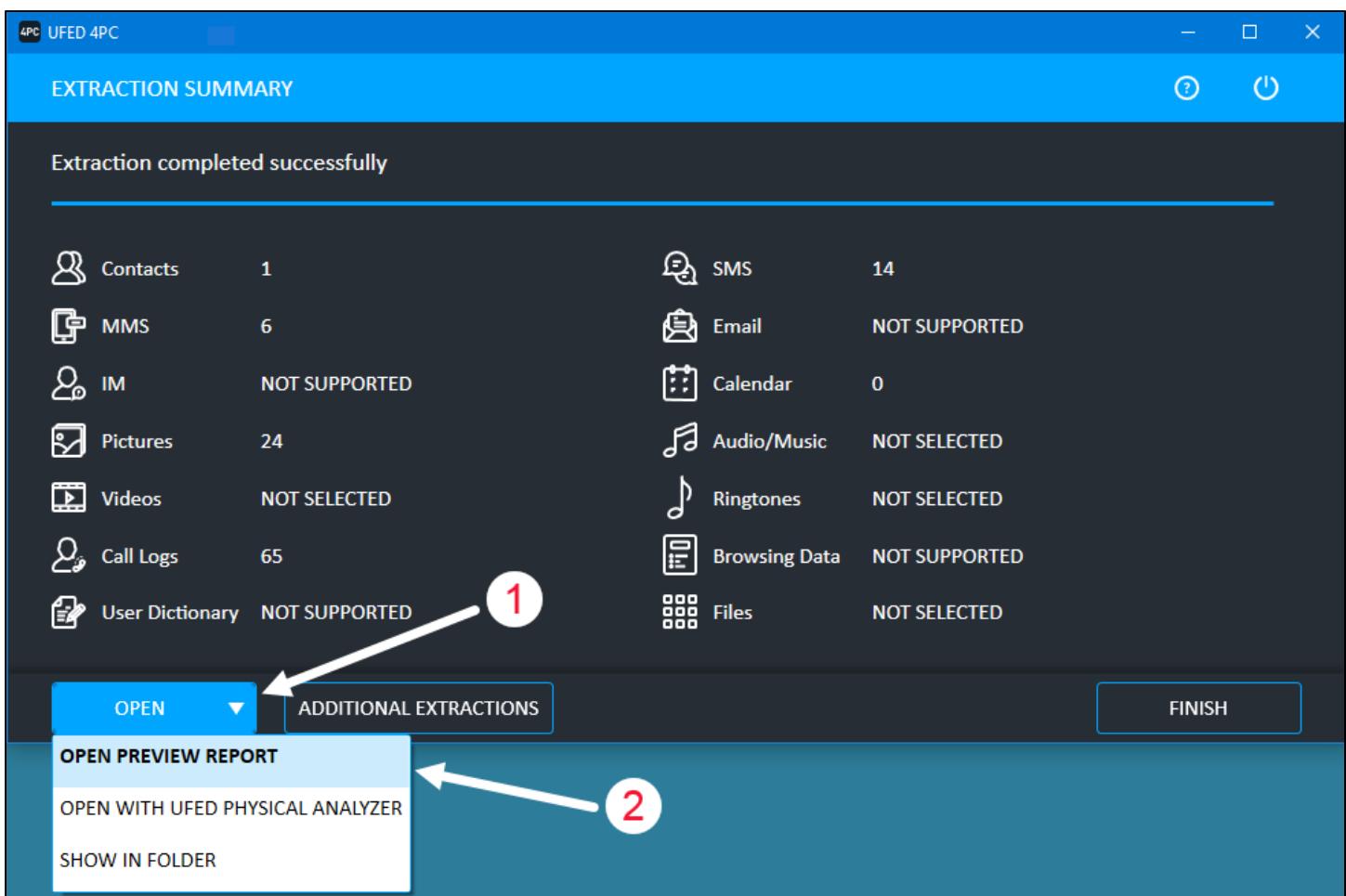
7. Were you able to successfully collect the image/data? If not, what troubleshooting steps would you take next in order to overcome the issues you experienced?

---

---

---

8. If successful, an **EXTRACTION SUMMARY** will be shown, outlining the results of the process. Click on **OPEN** and select **OPEN PREVIEW REPORT**. You could also open with **UFED Physical Analyzer**, but for the purpose of this exercise, we will not. Your data will differ from the data in the screenshot.



**Exercise - Questions**

1. A summary of the device itself will appear with numerous details regarding the device and the acquisition. Your information will differ from the screenshot. This will be the case for the remainder of this exercise and its screenshots.

The screenshot shows the UFED 4PC software interface. At the top, there's a search bar with placeholder text "Type to search..." and a magnifying glass icon. Below the search bar, the title "Phone Examination Preview Report Properties" is displayed. The main area contains a table with the following data:

Selected Manufacturer:	Samsung GSM
Selected Model:	SM-J327W Galaxy J3 Prime
Detected Manufacturer:	samsung
Detected Model:	SM-J327W
Revision:	8.1.0 M1AJQ J327WVLS4BSK1
IMEI:	35 [REDACTED] 196
MSISDN:	+1 [REDACTED] 46
ICCID:	89 [REDACTED] 3834019
IMSI:	302 [REDACTED] 34901
Extraction start date/time:	13/12/2019 0:37:44 (GMT)
Extraction end date/time:	13/12/2019 0:46:32 (GMT)
Phone Date/Time:	12/12/2019 7:38:10 (GMT-7)
Connection Type:	USB Cable
UFED Version:	Product Version: 7.24.0.1 , Internal Build: 7.24.0.1 UFED
UFED S/N:	1 [REDACTED] 4015

Note: This device is using client in order to communicate with UFED

For complete analysis and advanced reporting, open in UFED Physical/Logical Analyzer.

[Back](#) [Close](#)

2. Scroll down the page and note clickable links to the various data sets that were acquired.
  - a. How many text messages do you have?  
\_\_\_\_\_
  - b. How many **Images** do you have?  
\_\_\_\_\_
  - c. How many active entries in your **Call Log**?  
\_\_\_\_\_

## 3. Click on Call Logs.

UFED 4PC

Type to search...

**Generic Extraction Notes:**  
+ZZ – Extracted phone time stamp time zone is expressed in quarters of an hour  
Last IMEI digit might be incorrect. Please check manually on the device.

### Phone Examination Report Index

Contacts (1)	Selected
SMS - Text Messages (14)	Selected
Calendar/Notes/Tasks	Selected
Call Logs (65)	Selected
MMS - Multimedia Messages (6)	Selected
Email Messages	Not Supported
Instant Messages	Not Supported
Browser Bookmarks	Not Supported
Browser History	Not Supported
Web Searches	Not Supported
User Dictionary	Not Supported
Images (24)	Selected
Ringtones	Not Selected
Audio	Not Selected
Video	Not Selected

Back Close

4. You will be presented with the call log entries from the device.

4PC UFED 4PC

Type to search...

### Phone Incoming Calls List

Back to index

CLOG SHA256 Hash: 5C1FD4C5 893F2C6 F8C0991 005B3F5 860A38A E09C182 44067F2 F084174 332AF19

#	Type	Number	Name	Date & Time	Duration
1	Incoming	+156 47	null	0: (C) 1:34:32	N/A
2	Incoming	No N	null	0: (C) 1:06:53	0:02:04
3	Incoming	No N	null	0: (C) 1:06:05	N/A
4	Incoming	1915 1	null	2: (C) 1:27:41	N/A
5	Incoming	1403 7	null	2: (C) 1:39:51	N/A
6	Incoming	1915 1	null	2: (C) 1:51:31 (GMT-6)	0:00:07

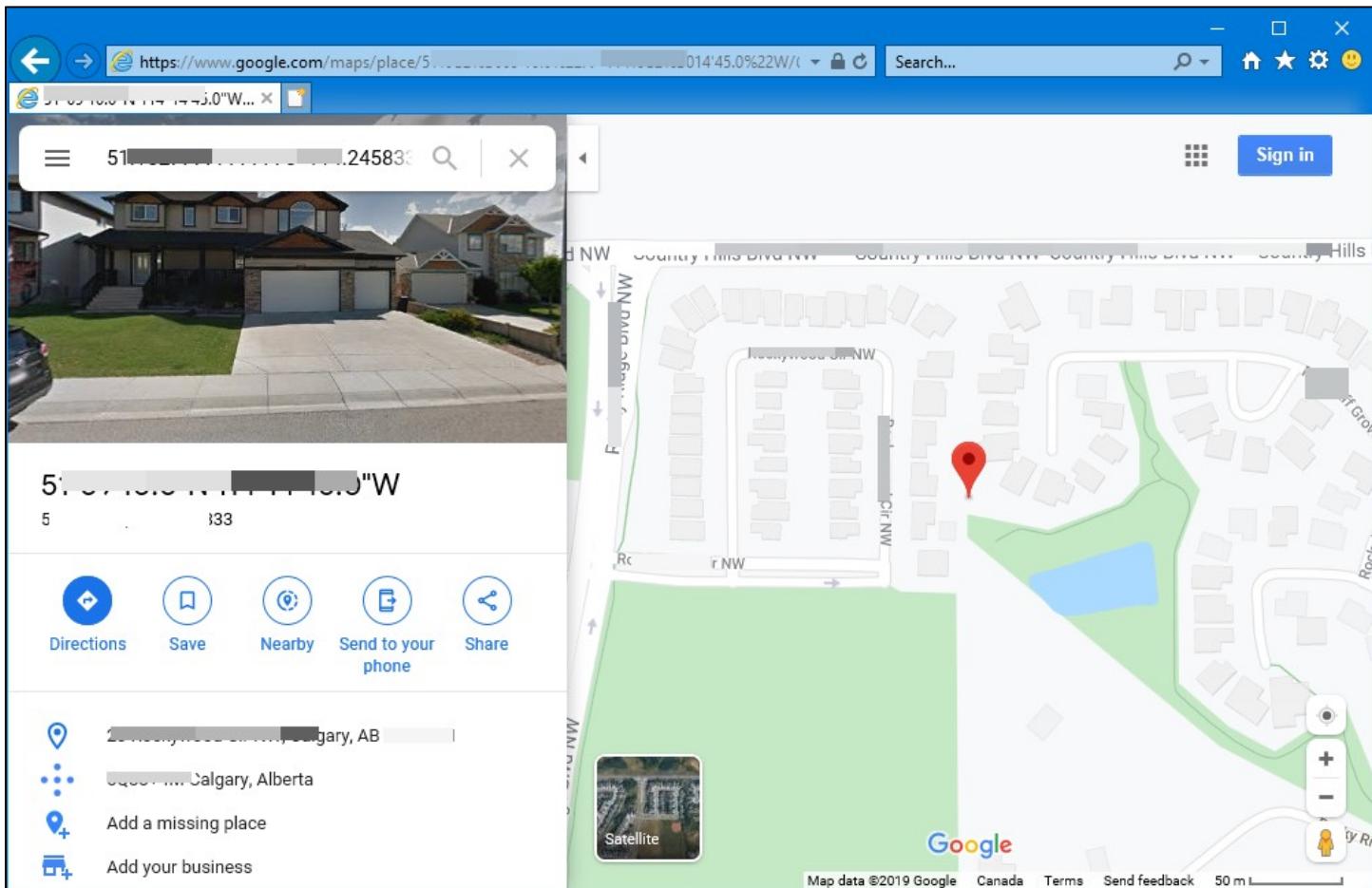
5. Click the **Back** button to revert back to the acquired data sets and click on **Images**.

4PC UFED 4PC

Type to search...

		<a href="#">Google maps link</a>	
3	<p>File Name: <a href="#">20181006_214418.jpg</a>          File Path: Phone/DCIM/Camera/          File Source: Phone          File Size: 1806590 Bytes          File Date/Time: 06/10/2018 22:44:18          SHA256: CE3857D1 0A65EDF 0F0CB6A 8E53D5A 5999C4C 2FDF83D 4CC857F 12BD0C8 66582D9</p>	<p>Resolution: 72x72 (unit: inch)          Pixel Resolution: 2576x1932          Camera Make: samsung          Camera Model: SM-J327W          Date/Time: 2018:10:06 21:44:18          Lat/Lon: 5 66666667 / -122.75081          GPS Time: 04:44:9  <a href="#">Google maps link</a></p>	
4	<p>File Name: <a href="#">20181010_133013.jpg</a>          File Path: Phone/DCIM/Camera/          File Source: Phone          File Size: 1463785 Bytes          File Date/Time: 10/10/2018 13:30:14          SHA256: F27A9370 D5BEC44 D972DAC DAA99E1 D866357 CD230CE 61F8B46 DAA2D70 04EEADE</p>	<p>Resolution: 72x72 (unit: inch)          Pixel Resolution: 2576x1932          Camera Make: samsung          Camera Model: SM-J327W          Date/Time: 2018:10:10 13:30:13          Lat/Lon: 5 7777778 / -114.24583          GPS Time: 19:30:8  <a href="#">Google maps link</a></p>	
5	<p>File Name: <a href="#">20181021_085252.jpg</a>          File Path: Phone/DCIM/Camera/          File Source: Phone          File Size: 3049465 Bytes          File Date/Time: 20/10/2018 17:52:52          SHA256: 9FA834A8 359D970 869970B 0A7F121 F03F632 B53D0CB CC2E0A0 3599A55 2365AA1</p>	<p>Resolution: 72x72 (unit: inch)          Pixel Resolution: 2576x1932          Camera Make: samsung          Camera Model: SM-J327W          Date/Time: 2018:10:21 08:52:52</p>	

6. Take some time to note the data that has been collected about the images that were taken with the device, and then right click on the **Google maps link** of any one of them, and select **Open in new window**. If location services are enabled on the device, and if you have Internet connectivity, you will be shown on a map where the photo was taken, to a relatively high degree of accuracy.



7. When done looking around, click **Close**, and then close the **UFED4PC** application.

### **Exercise—Key Takeaways**

- There are many “quick wins” in the easily available data from a portable device.
- In an investigation where time is of the essence, much of the most important data can be quickly and easily obtained, provided you know the credentials of the device.
- With these easily obtained gains, you can further your investigation to the next stage, while lab analysis is carried out, rather than afterwards.

This page intentionally left blank.

# © SANS Institute 2020

## Exercise 2.2A—Portable Device Analysis-Cellebrite

### Background

As you are conducting an investigation, whether it be roadside, or in a lab, you must have some idea of what is available on a smartphone. In addition, you must be able to access it quickly, but in the least intrusive manner possible. Although data may be very time sensitive, there also may be other data on the device in a deleted space that could be very important but will be destroyed by your actions. This creates a dilemma that can only be dealt with through intelligent “risk vs reward” determination.

Examiners may have tools at their disposal to create a data image of the device (notice we don’t say forensic image) that are quite varied. Some are quite expensive, but some can be quite cheap. The difference tends to be blurry, other than the ability to create hash values and verifications.

The more effective tools will allow for interaction with the found files, and the ability to cross reference them against other data on the device. For example, a photo from which an examiner can extract the exact location where it was taken, and/or date and time of when the photo was taken.

While these tools designed for “forensic” acquisition are incredibly effective, just how accurate are they? And how responsive are they to the updating processes from device manufacturers? Sometimes it is necessary to use less than optimal tools, and sometimes it is necessary to let more than one tool review a data dump to get the clearest picture of the data. We may even have to inspect a data dump from nothing more than a file/folder level.

### Exercise Objectives

- Use **Cellebrite UFED Physical Analyzer** to examine an Apple iPhone image

### Exercise Preparation

1. Boot your **FOR498 Windows SIFT VM**
2. Login to the **FOR498 Windows SIFT VM** using the following credentials:
  - a. Username: **SANSDFIR**
  - b. Password: **forensics**

3. Start the **UFED Physical Analyzer (PA)** application by double clicking the icon in the **Forensic Suites** fence on your **Desktop**. This program takes a few seconds to open, so be patient. Note that you do NOT want two instances opening!

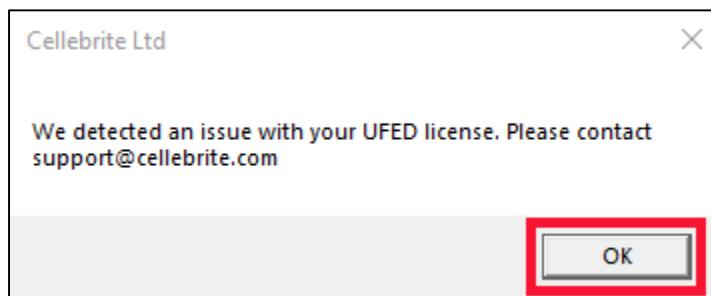


4. After a few seconds where it will appear that nothing is happening (BE PATIENT), a splash screen will appear.

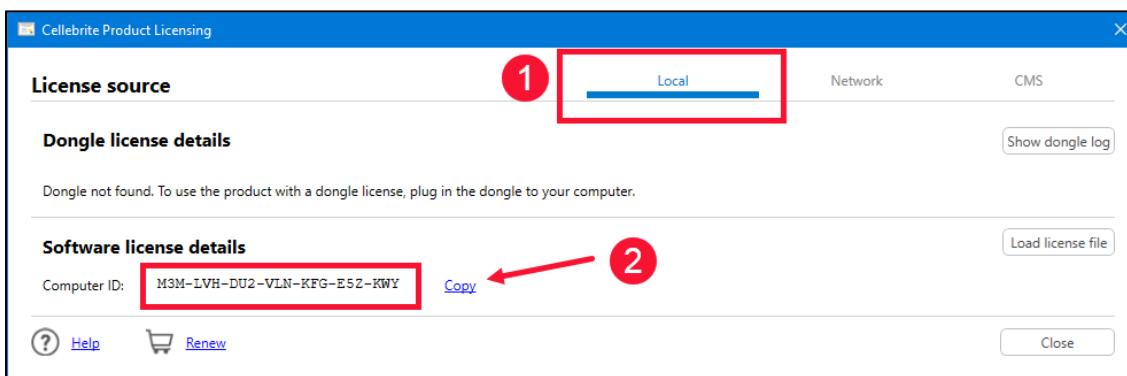


**NOTE:** You may be prompted to update **Physical Analyzer**. If the currently installed version of Cellebrite does not support the collection of your particular device, we recommend updating the software OUTSIDE CLASS. If the currently installed version is able to collect your phone, please avoid updating until after you have completed the class. Updating is optional and may "break" the functionality of the tool in regards to the other Cellebrite-based exercises in this class. Updating is at your own risk. The currently-installed version has been tested and confirmed to work with the remaining exercises! You will license the other tools right before they are needed in each lab. **Do not change any VM settings after licensing Cellebrite or your license may no longer work!**

5. If you get a pop up message during startup of the program, as indicated below, simply click **OK**, and the program will continue to load.



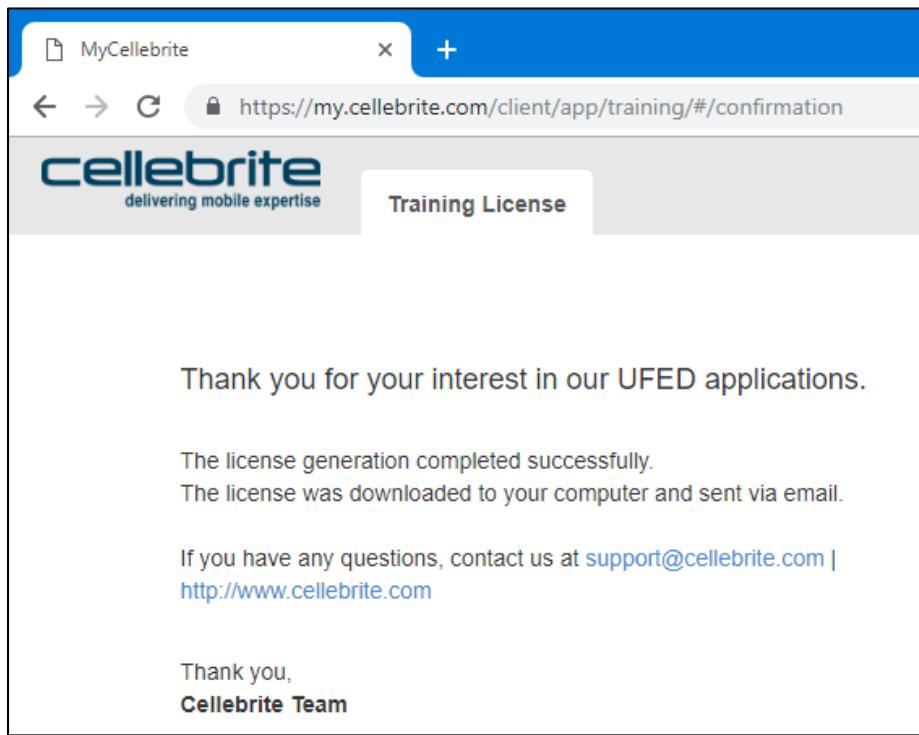
6. The prompt below pops up in **Physical Analyzer** when the tool launches. Copy your **Computer ID** from **Physical Analyzer**. Ensure the Local button is selected. If the prompt does not appear, select **Help > Show License Details**.



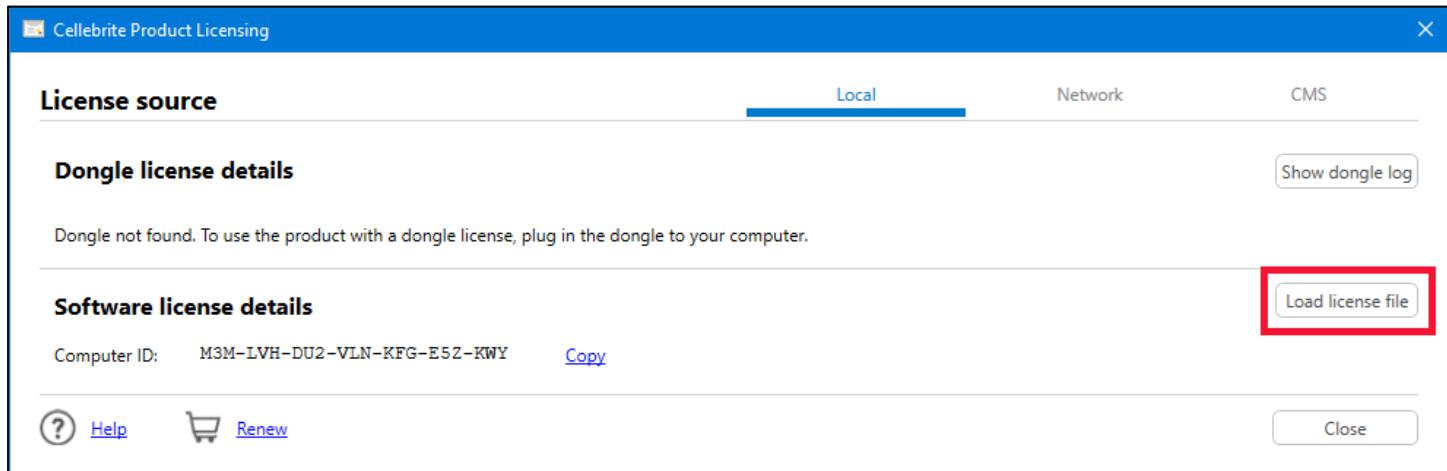
7. Open a browser window, go to <https://my.cellebrite.com/training> and fill out the required fields to receive your license file for this course. **NOTE: Do not provide your real information unless you want to be contacted by the Vendor. A fake email account is enough to get you a license. Feel free to use your own information if you already have an account with Cellebrite or plan to use any support.** (NOTE: The Activation Code is provided by SANS or the instructor. If you are an OnDemand student, please request the code by emailing online-sme@sans.org. The Computer ID is copied from UFED Physical Analyzer, as shown above). Make sure you select something from each drop-down option, or you cannot proceed. Once everything is filled in, click **Generate License**.

The screenshot shows the 'Training License' section of the Cellebrite website. It has a header 'cellebrite delivering mobile expertise' and a sub-header 'UFED applications free trial'. The form includes fields for Primary Email\*, First Name\*, Last Name\*, Company\*, Phone\*, Country\*, State\*, City\*, Address\*, Zip Code\*, Activation Code\*, and Computer ID\*. The 'Activation Code\*' and 'Computer ID\*' fields are highlighted with a red border and circled in red (step 1 and step 2). A red arrow points from the 'Computer ID\*' field to the 'Copy from the screen in UFED Physical Analyzer' link. A blue 'Generate License' button is at the bottom right.

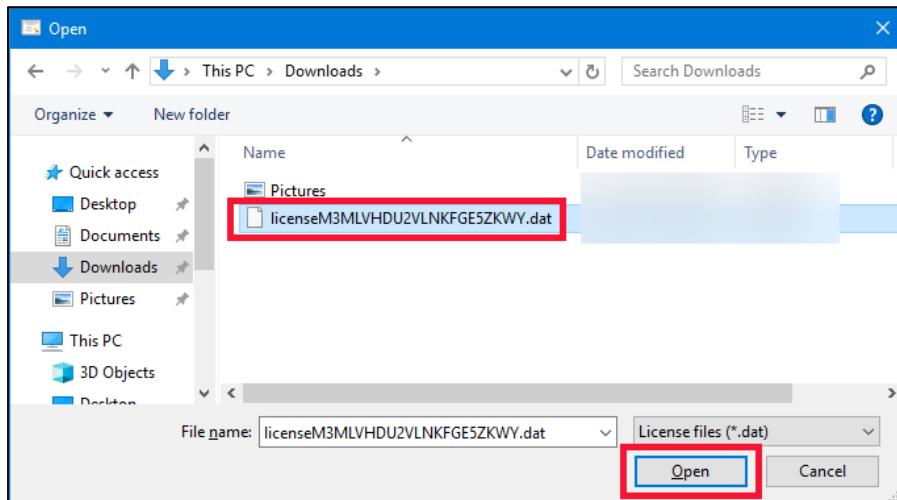
8. Your license should appear at the bottom of your screen after a minute. Select **Save** and the license file will be saved to your **Downloads** folder. In some cases, this has happened automatically.
9. When this is done, it will be indicated by a thank you message from Cellebrite. Close the browser window.



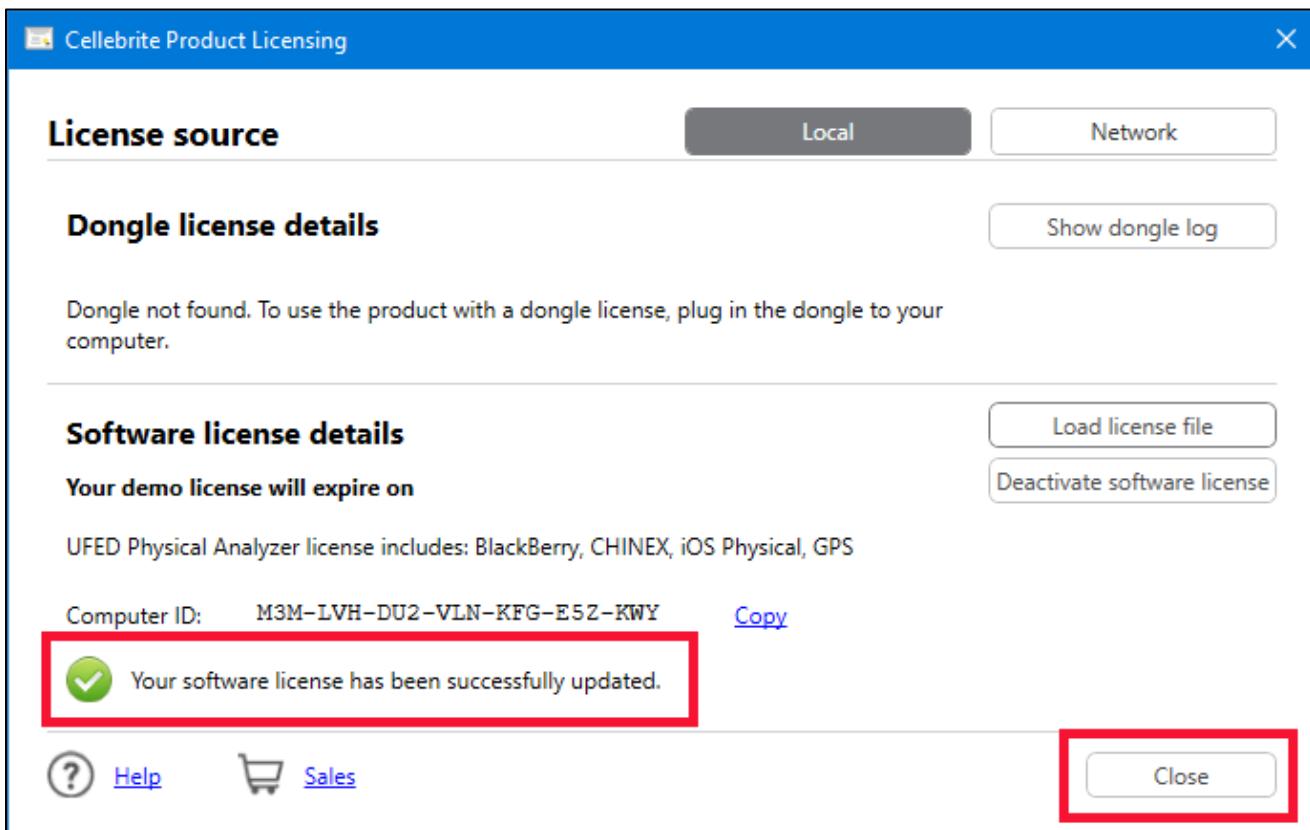
10. Go back into **Physical Analyzer** and select **Load license file**.



11. A directory window will open. Navigate to your **Downloads** directory and select your **licenseXXX.dat** file and then click on **Open**.

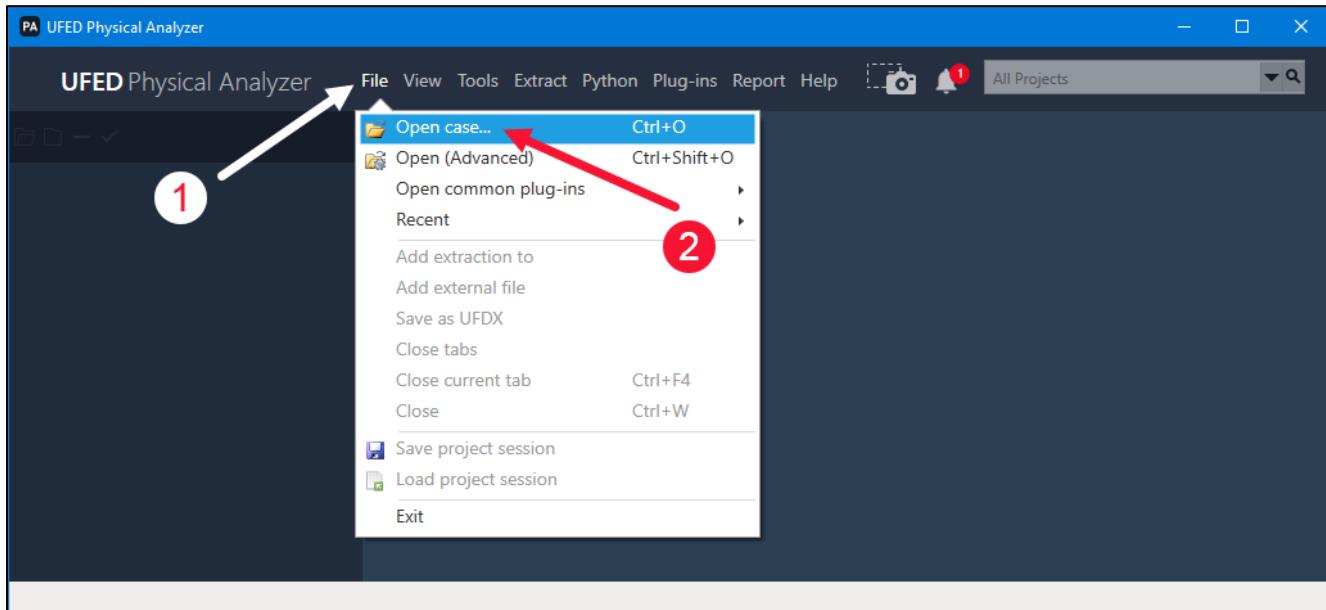


12. Once done, you will see the **Product Licensing** window again. Note that the software license is now active. Click the **Close** button.



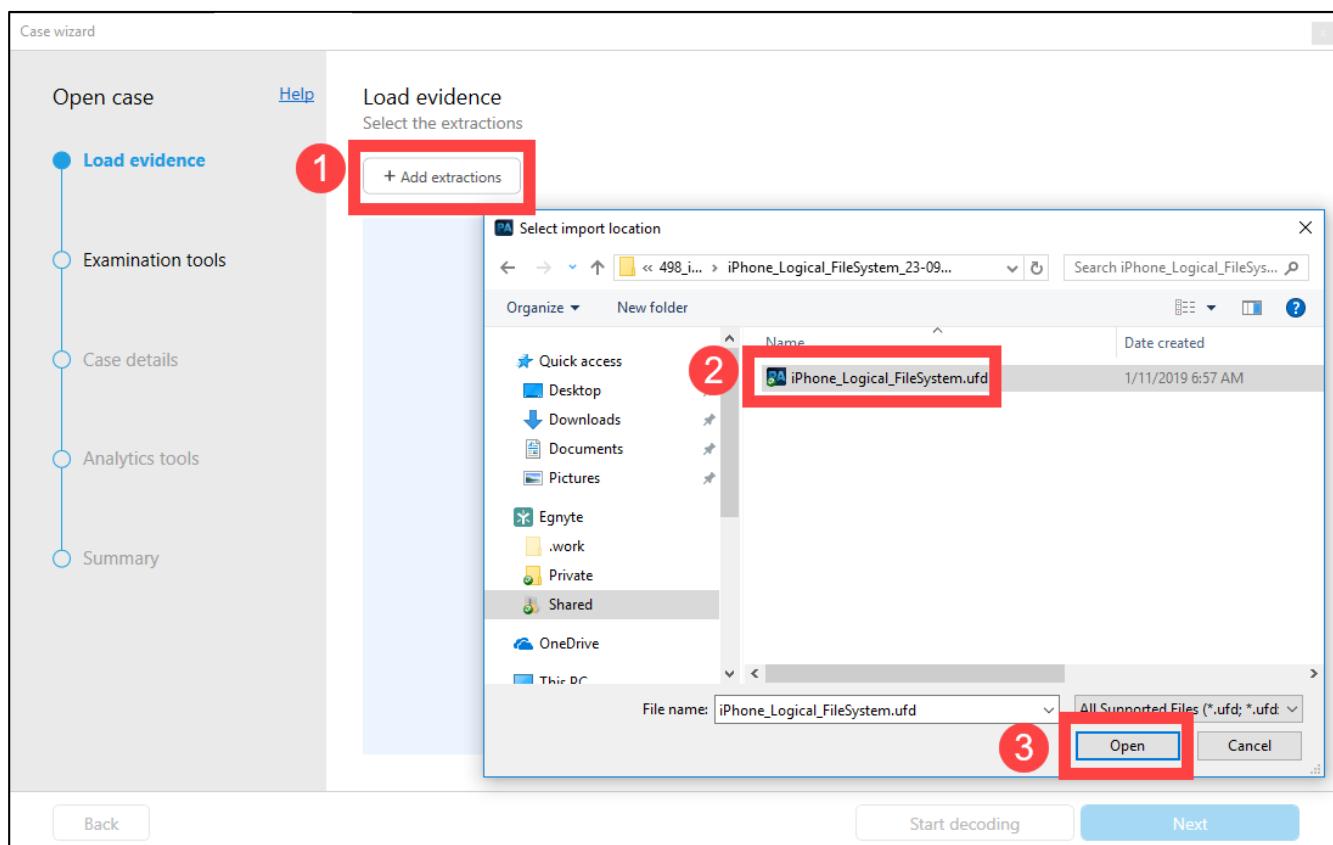
13. You will now see the **Physical Analyzer** program open.

14. Once Physical Analyzer has started, open the collected evidence file by clicking on File → Open case...



15. The Case wizard window will open. Click on +Add extractions, and navigate to the iPhone\_Logical\_FileSystem.udf file located at C:\Cases\498\_iPhone5\iPhone\_Logical\_FileSystem\_23-09-13\_09-02-01\iPhone\_Logical\_FileSystem.udf

You may not see .ufd at the end of the title. This is because you do not have viewing of file extensions enabled. We will address this in a later exercise.



16. Note the image you are requesting to open, and then click on the **Examine data** button. You will see data starting to load, and you will see plugins and parsers running to extract the data we seek to analyze.

The screenshot shows the UFED Physical Analyzer application window. On the left is a file tree with the following structure:

- iPhone\_Logical\_FileSystem (selected, highlighted in blue)
- Extraction Summary (1)
- Logical
- Cloud Data Sources
- Memory Images
- Memory Ranges
- File Systems
- Analyzed Data
  - Apps info
  - Calendar (12)
  - Call Log (62)
  - Carved Strings (14) (14)
  - Chats (16) (1)
  - Contacts (63)
  - Cookies (351) (12)
- Device Locations (51) (20)
  - Journeys (4)
  - Locations (43) (20)
- Device Notifications (2)
  - Emails (7)
  - MMS Messages (3)
  - Notes (2)
  - Passwords (4)
- Searched Items (38)
- SMS Messages (107) (8)
  - User Accounts (13)
  - User Dictionary (691)
  - Voicemails (4)

A red arrow points from the text "To find this again, select Help > Learn more" to the "Learn more" button in the top right corner of the application window.

In the center-right area, there is a "Learn more" pop-up window with the following content:

To find this again, select Help > Learn more

Want to take advantage of key capabilities to advance your case?  
Learn with these Tips, Tricks and Tutorials



Review tricks for seeing all the chats in a conversation view, including filtering and changing views.

[Watch Tutorial](#)

Take a moment to learn more

 Overcome Language Barriers with Smart Translator  
Do you need to examine textual content that is not in your native language? Evaluate our on-demand translator now!

 What do you really know about iOS 13?  
Follow Up Answers to the "Fact or Fiction – iOS 13 webinar by Heather Mahalik.

Running plugin (ContactsCrossReference)

A red arrow points from the bottom right of the "What do you really know about iOS 13?" section towards the bottom right corner of the application window.

17. When the parsing has completed, you will be presented with a screen showing a summary of the extraction. You may also be presented with an option asking if "...enrichment of the cell and BSSID data is desired." If you get this message, select to skip it.

**UFED Physical Analyzer**

File View Tools Extract Python Plug-ins Report Help

All Projects

Learn more Extraction Summary (1)

**Extraction Summary (1)**

All Content Logical

Extr... + Add extraction Add external file Project settings Generate report

Extractions: 1

**Logical**

Logical Extraction start date/time Extraction end date/time C:\Cases\498\_iPhone5\iPhone\_Logical\_Fil...

**Device Info**

Advertising Id (IDFA)	AF7ECDED-0825-461D-A476...	com.apple.lsidentifiers.plist...
Apple ID	livingstonhank11@gmail.com	Accounts3.sqlite : 0x5DAC
iCloud account present	False	
ICCID	89148000000276575306	com.apple.commcenter.plist...
Last user ICCID	89148000000276575306	csidata : 0x327
MSISDN	3392226970	com.apple.commcenter.plist ...
<b>Hank's iPhone</b>		
Detected Phone Model	iPhone 5 (A1429)	Info.plist : 0x21D
Detected Phone Model Identifier	iPhone5,2	Info.plist : 0x21D
Is encrypted	False	Manifest.plist : 0x995
OS Version	6.1.4	Info.plist : 0x255
Owner Name	Hank's iPhone	Info.plist : 0x138
Serial	C39JH1NPF8H2	Info.plist : 0x287
ICCID	89148000000276575306	Info.plist : 0x16A
IMEI	990002240212843	Info.plist : 0x1A2
<b>Network Interfaces</b>		
Internet network IP	108.18.120.217:53709 at 201...	ef942d048cf582a5.dat : 0x5
Internet network IP	74.96.90.129:53709 at 2013-0...	9234e0e7a4ab166c.dat : 0x5
Local network IP	192.168.1.7:53709 at 2013-09...	ef942d048cf582a5.dat : 0x5
Local network IP	192.168.1.9:53709 at 2013-09...	9234e0e7a4ab166c.dat : 0x5
<b>Phone Settings</b>		
Location Services Enabled	True	com.apple.locationd.plist : 0...

**Hash set info**

**Malware scanner**

Malware scan performed No

**Device Content**

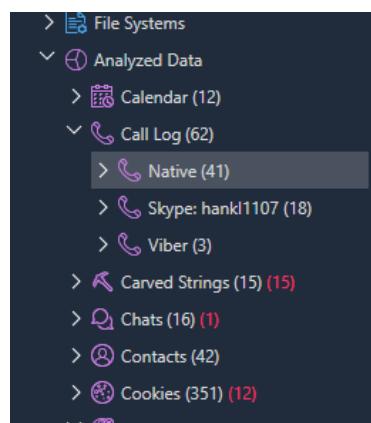
- 4 data sources can be extracted u:
- Phone Data**
  - Calendar 12
  - Call Log 62
  - Carved Strings 14 (14)
  - Chats 16 (1)
- Contacts 63
- Cookies 351 (12)
- Device Locations 111 (20)
- Device Notifications 2
- Emails 7
- Installed Applications 14

## Exercise - Questions

- At the top of the **Extraction Summary** window, there are two tabs. One is titled **All Content**, and it is supplying the information seen in the previous step. Clicking on the **Logical** tab beside it will show data about the logical acquisition and the device itself.

The screenshot shows the UFED Physical Analyzer interface. On the left, a sidebar lists various analysis categories like File Systems, Analyzed Data, and Call Log. The main area displays the 'Extraction Summary (1)' tab, which includes sections for Extraction (showing a smartphone icon and 'Logical' status) and Device Info. The Device Info panel on the right provides a detailed list of device properties for 'Hank's iPhone', such as OS Version (6.1.4), Serial (C39JH1NPF8H2), and various identifiers and connection details.

- Locate **Call Log** in the left column of the screen. You will see that there is an expansion arrow beside it. Click on this to see the different types of calls that exist on this device.



- a. How many call making/taking programs exist? \_\_\_\_\_
- b. Which one is used most frequently? \_\_\_\_\_
3. Double click on the **Native** call log to see a list of calls made to and from this device. By default, it is sorted by **Timestamps**, from newest call to oldest call. By hovering the mouse near the top of a column, you will see 5 dots appear. Clicking on these dots will reverse the sort order on that column. Clicking in the same area in any other column will cause sorting to be applied to that column instead. Note that you cannot sort on every column.

**Call Log**

Timestamp	Duration	Type	Country code	Network code	Network Name	Source
9/19/2013 1:30:52 AM(UTC+0)	0:01:43	Outgoing	311	480	Verizon Wireless (United States)	Logical Hank's iPhone/ var/wireless/ Library/ CallHistory/ call_history.db : 0x3A27 (Table: call, Size: 28672 bytes)

**Parties**

To: 6085159158 Dirty
----------------------

- a. What is the date and time of the last 2 **Outgoing** calls? \_\_\_\_\_

- b. What number were they to? \_\_\_\_\_

### Bonus Questions

- c. Who (most likely) is “**Dirty**”? \_\_\_\_\_
- d. Where did you get this information? \_\_\_\_\_

4. At the top of the **UFED PA** window, you will see tabs starting to accumulate for each artifact that you have explored (if you have explored any). This can quickly become unmanageable. You can click the **x** on each tab to close it. You will now explore chat-style communications. In the left column of artifacts, we see three different formats of chat. **Chats**, **MMS Messages**, and **SMS Messages**. If we expand the arrow beside each one, we can see all the programs and/or folders where we have chat content.

**Double click on SMS Messages.** You will see the messages populate in the program, sorted by **Date/Time**. The red **x** to the left of the telephone numbers indicates deleted messages. The slider at the bottom of the screen allows the examiner to see further data. The numbers in red beside the artifacts in the left column indicate how many deleted items were recovered for that artifact.

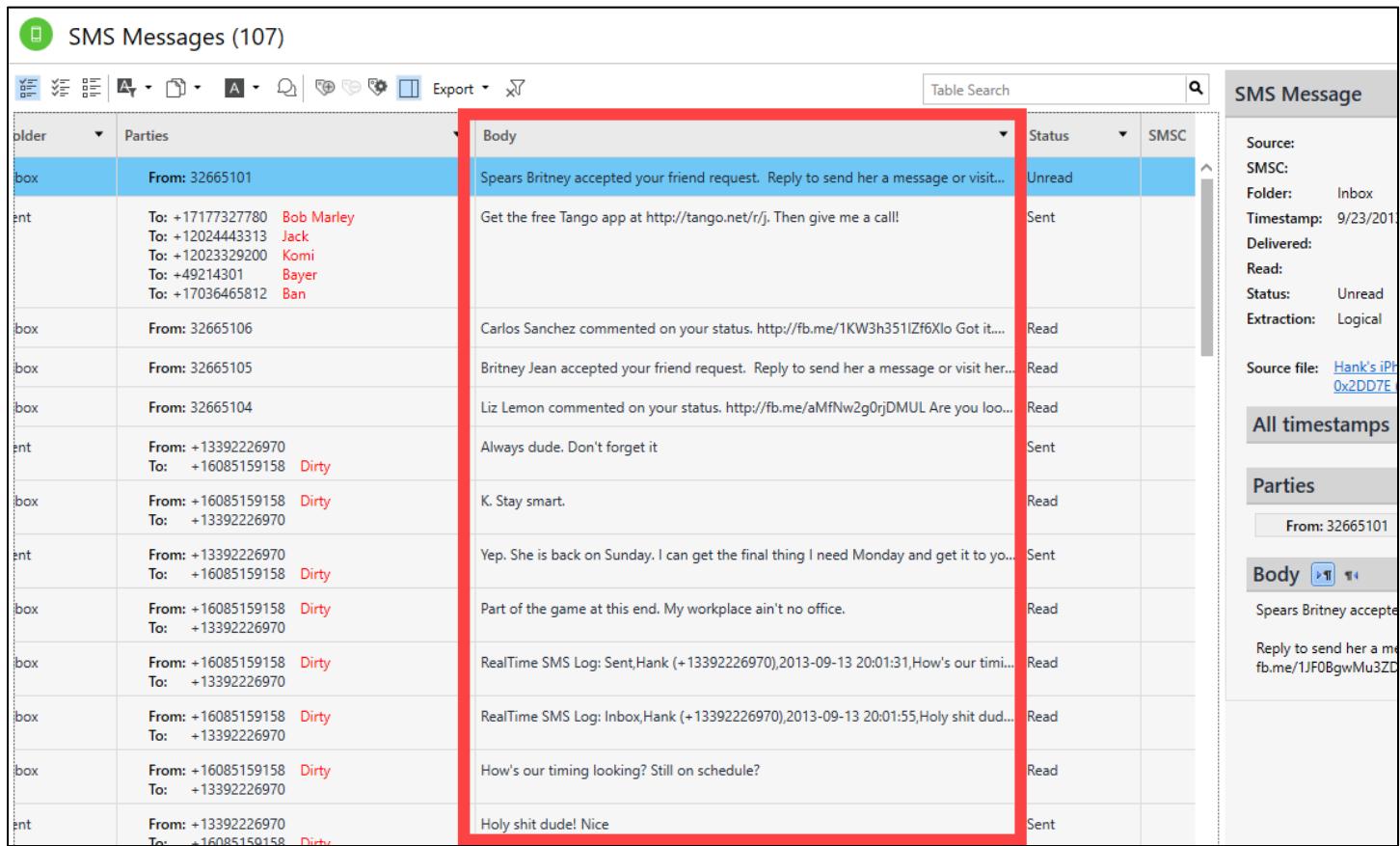
The screenshot shows the UFED Physical Analyzer interface. The left sidebar contains a tree view of analyzed data, including Memory Ranges, File Systems, Analyzed Data (with Chat (16), MMS Messages (8), and SMS Messages (107) expanded), Call Log (62), Contacts (42), Cookies (351), Device Locations (111), Device Notifications (2), Emails (7), Installed Applications (14), and Timeline (470). The main pane shows an 'SMS Messages (107)' extraction summary. A table lists 107 messages, with columns for Timestamp, Delivered, Read, Folder, and Parties. The table includes rows for various dates and times, such as 9/23/2013, 9/19/2013, 9/18/2013, etc., with details like 'Inbox' or 'Sent' status and recipient information. To the right of the table is a detailed view of a specific message, showing its source file path, parties involved, and the message body content. A red box highlights the 'MESSAGE' section of the detail view, and another red box highlights the 'MESSAGE DETAIL' section. A third red box highlights the 'DELETED CHATS' section, which is part of the sidebar's expanded 'Chats' category. A fourth red box highlights the 'CHAT PROGRAMS' section, which is part of the sidebar's expanded 'SMS Messages' category. A fifth red box highlights the 'SLIDER' at the bottom of the main pane.

- What was the date/time of most recent incoming **SMS** message? \_\_\_\_\_
- What was the date/time of most recent outgoing **SMS** message? \_\_\_\_\_
- Who was the most recent outgoing **SMS** message to? \_\_\_\_\_
- How many different “**Chats**” programs are in use? \_\_\_\_\_
- How many total **Messages** of all types are there? \_\_\_\_\_

## Bonus Questions

- f. What does “MMS” stand for, and what is unique about this type of message?

- 
5. If you use the slider as indicated in the previous step, and slide it to the right, you will see a column titled **Body**. This is the actual text of the message. Beside it is a **Status column**, indicating whether a message has been read or not.

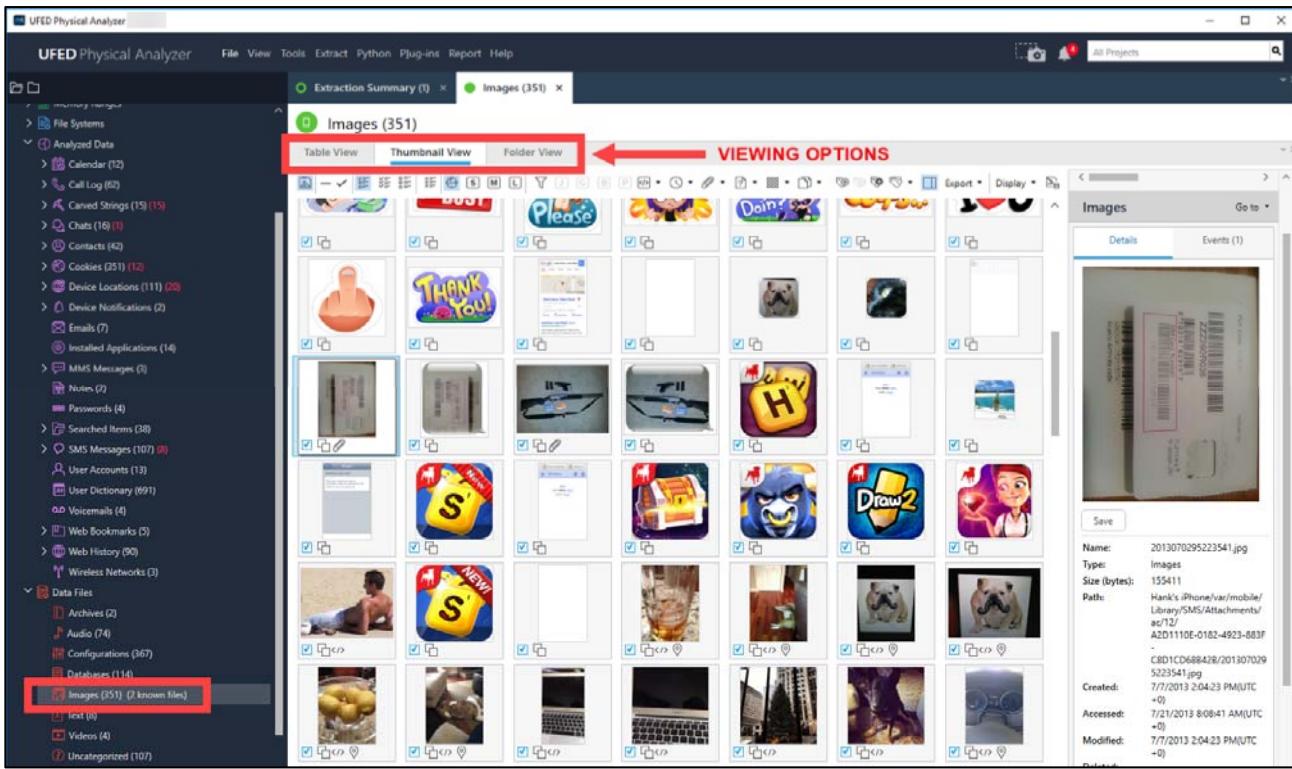


SMS Messages (107)			
Folder	Parties	Body	Status
box	From: 32665101	Spears Britney accepted your friend request. Reply to send her a message or visit...	Unread
ent	To: +17177327780 Bob Marley To: +12024443313 Jack To: +12023329200 Komi To: +49214301 Bayer To: +17036465812 Ban	Get the free Tango app at http://tango.net/r/j. Then give me a call!	Sent
box	From: 32665106	Carlos Sanchez commented on your status. http://fb.me/1KW3h351lZf6Xlo Got it...	Read
box	From: 32665105	Britney Jean accepted your friend request. Reply to send her a message or visit her...	Read
box	From: 32665104	Liz Lemon commented on your status. http://fb.me/aMfNw2g0rjDMUL Are you loo...	Read
ent	From: +13392226970 To: +16085159158 Dirty	Always dude. Don't forget it	Sent
box	From: +16085159158 Dirty To: +13392226970	K. Stay smart.	Read
ent	From: +13392226970 To: +16085159158 Dirty	Yep. She is back on Sunday. I can get the final thing I need Monday and get it to yo...	Sent
box	From: +16085159158 Dirty To: +13392226970	Part of the game at this end. My workplace ain't no office.	Read
box	From: +16085159158 Dirty To: +13392226970	RealTime SMS Log: Sent,Hank (+13392226970),2013-09-13 20:01:31,How's our timi...	Read
box	From: +16085159158 Dirty To: +13392226970	RealTime SMS Log: Inbox,Hank (+13392226970),2013-09-13 20:01:55,Holy shit dud...	Read
box	From: +16085159158 Dirty To: +13392226970	How's our timing looking? Still on schedule?	Read
ent	From: +13392226970 To: +16085159158 Dirty	Holy shit dude! Nice	Sent

The screenshot shows a software interface for analyzing mobile device data. On the left, there's a navigation bar with various icons. In the center, a large table lists 107 SMS messages. The columns are labeled 'Folder', 'Parties', 'Body', and 'Status'. The 'Body' column contains the text of each message, which is highlighted with a red box. To the right of the table is a sidebar with sections for 'SMS Message', 'All timestamps', 'Parties', and 'Body'. The 'SMS Message' section displays detailed information like Source, SMSC, Folder, Timestamp, and Delivered status. The 'Body' section shows the raw text of the messages.

- a. Have all the received **SMS** messages been read? \_\_\_\_\_
- b. When was the first **SMS Message** read on this device? \_\_\_\_\_
- c. What is the owner name of this device? \_\_\_\_\_
- d. What is their full name? \_\_\_\_\_
- e. What is their **AppleID**? \_\_\_\_\_

6. In the left column, we will explore some **Data Files** now; namely **Images**. Expand the **Data Files** section and double click on **Images**. You can see at the top of the **Images** pane, three viewing options. With **Thumbnail View** selected, you can see all of the pictures on the device. If you select a photo, you can see it, and its details, in the pane on the right of the screen.



7. Click on **Table View**, and scroll through the list looking for a picture with the name of **2013070295223541.jpg**. Once you find it, answer the questions associated with it.

		Image		Name	Path
⊕	(4*)	56		15FA97B1-D4CC-4486-B...	Hank's iPhone/var/mobile/Library/Caches/
⊕	(2*)	57	1	2013070295223541.jpg	Hank's iPhone/var/mobile/Library/SMS/At...
⊕	(2*)	58		2013070295223541-prev...	Hank's iPhone/var/mobile/Library/SMS/At...
⊕	(2*)	59	1	2013091395195722.jpg	Hank's iPhone/var/mobile/Library/SMS/At...
⊕	(2*)	60		2013091395195722_prev...	Hank's iPhone/var/mobile/Library/SMS/At...
⊕	(2*)	61		2350368359b92e052384...	TarArchive/2350368359b92e0523841c284...

The screenshot shows the same UFED interface but in Table View mode. The table lists image files by name and path. The file '2013070295223541.jpg' is highlighted in the table and also shown in a larger preview window on the right. The right pane also displays detailed information for this file, including its name, type, size, path, and timestamps.

- a. Where did the photo come from? (i.e. how did it get on the phone)

---

- b. What is the picture of? \_\_\_\_\_

---

- c. How many total Images are on the device? \_\_\_\_\_

---

## Bonus Question

- d. We believe there is a list of drugs on the device. What are the drugs on the list, and where (medium) was the list created? (**Hint:** start with images)

---

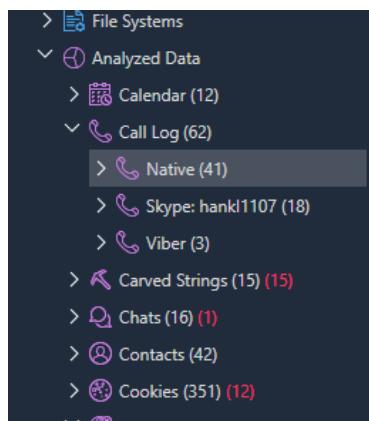
## Exercise - Questions with Step-by-Step

1. At the top of the **Extraction Summary** window, there are two tabs. One titled **All Content**, which is supplying the information seen in the previous step. Clicking on the **Logical** tab will show data about the logical acquisition and the device itself.

The screenshot shows the UFED Physical Analyzer interface. On the left, a sidebar lists various analysis categories like 'iPhone\_Logical\_FileSystem', 'Cloud Data Sources', 'Memory Images', etc. The main area displays the 'Extraction Summary (1)' tab, which includes sections for 'Extraction' (showing a smartphone icon and 'Logical' extraction type) and 'Device Info'. The 'Device Info' panel on the right contains a table of device details, such as OS Version (6.1.4), Serial (C39JH1NPF8H2), and various identifiers and connection details. A red box highlights the 'Logical' tab in the top navigation bar.

<input checked="" type="checkbox"/> Hank's iPhone	OS Version	6.1.4
<input checked="" type="checkbox"/> Serial	Serial	C39JH1NPF8H2
<input checked="" type="checkbox"/> Detected Phone Model	Detected Phone Model	iPhone 5 (A1429)
<input checked="" type="checkbox"/> Detected Phone Model Identifier	Detected Phone Model Identifier	iPhone5,2
<input checked="" type="checkbox"/> Is encrypted	Is encrypted	False
<input checked="" type="checkbox"/> IMEI	IMEI	990002240212843
<input checked="" type="checkbox"/> Owner Name	Owner Name	Hank's iPhone
<input checked="" type="checkbox"/> ICCID	ICCID	8914800000027657...
<input checked="" type="checkbox"/> General	Apple ID	livingstonhank11@g...
<input checked="" type="checkbox"/> iCloud account present	iCloud account present	False
<input checked="" type="checkbox"/> Advertising Id (IDFA)	Advertising Id (IDFA)	AF7ECDDE-0825-46...
<input checked="" type="checkbox"/> Last user ICCID	Last user ICCID	8914800000027657...
<input checked="" type="checkbox"/> ICCID	ICCID	8914800000027657...
<input checked="" type="checkbox"/> MSISDN	MSISDN	3392226970
<input checked="" type="checkbox"/> Network Interfaces	Local network IP	192.168.1.7:53709 at...
	1	ef942d048cf582a5.d...
	2	192.168.1.9:53709 at...
	Internet network IP	108.18.120.217:5370...
	1	ef942d048cf582a5.d...
	2	74.96.90.129:53709...
<input checked="" type="checkbox"/> Phone Settings	Location Services Enabled	True
		com.apple.locationond...

2. Locate **Call Log** in the left column of the screen. You will see that there is an expansion arrow beside it. Click on this to see the different types of calls that exist on this device.



- a. How many call making/taking programs exist? **3**
- b. Which one is used most frequently? **The native device**
3. Double click on the **Native** call log to see a list of calls made to and from this device. By default, it is sorted by **Timestamps**, from newest call to oldest call. By hovering the mouse near the top of a column, you will see 5 dots appear. Clicking on these dots will reverse the sort order on that column. Clicking in the same area in any other column will cause sorting to be applied to that column instead. Note that you cannot sort on every column.

**Native (41)**

**Call Log**

#	Parties	Timestamp	Duration	Type	Country code	Network code	Network Name	Source
2	To: 6085159158 Dirty	9/19/2013 1:30:52 AM(UTC+0)	00:14:43	Outgoing	311	480	Verizon Wireless (United...	
3	From: 6085159158 Dirty	9/18/2013 11:33:24 PM(UTC+0)	00:00:00	Missed	311	480	Verizon Wireless (United...	
4	From: 2054068371	9/18/2013 10:48:29 PM(UTC+0)	00:00:00	Missed	311	480	Verizon Wireless (United...	
5	From: 6085159158 Dirty	9/18/2013 9:50:14 PM(UTC+0)	00:00:00	Missed	311	480	Verizon Wireless (United...	
6	To: 7032758332	9/18/2013 11:54:14 AM(UTC+0)	00:00:24	Outgoing	311	480	Verizon Wireless (United...	
7	To: +15713954869	9/15/2013 7:49:35 PM(UTC+0)	00:00:31	Outgoing	311	480	Verizon Wireless (United...	
8	To: 7035568715	9/12/2013 7:35:44 PM(UTC+0)	00:06:10	Outgoing	311	480	Verizon Wireless (United...	
9	To: 7032411851	9/12/2013 3:03:53 PM(UTC+0)	00:01:34	Outgoing	311	480	Verizon Wireless (United...	
10	To: 7032411851	9/12/2013 3:03:23 PM(UTC+0)	00:00:14	Outgoing	311	480	Verizon Wireless (United...	
11	To: 7032411851	9/12/2013 2:55:37 PM(UTC+0)	00:00:26	Outgoing	311	480	Verizon Wireless (United...	
12	From: 3477752743	9/11/2013 7:27:47 PM(UTC+0)	00:00:00	Missed	310		Unknown network (Unite...	
13	To: 7032411851	9/11/2013 1:49:43 PM(UTC+0)	00:00:12	Outgoing	311	480	Verizon Wireless (United...	
14	To: 7032411851	9/11/2013 1:48:59 PM(UTC+0)	00:00:00	Outgoing	311	480	Verizon Wireless (United...	
15	To: 7032411851	9/11/2013 1:43:06 PM(UTC+0)	00:00:00	Outgoing	311	480	Verizon Wireless (United...	
16	To: +17033193689	9/5/2013 8:19:51 PM(UTC+0)	00:00:00	Outgoing	310		Unknown network (Unite...	
17	To: +18002221888	9/4/2013 12:33:44 AM(UTC+0)	00:00:00	Outgoing	310		Unknown network (Unite...	
18	To: 4127772000	8/31/2013 1:15:48 AM(UTC+0)	00:00:03	Outgoing	310		Unknown network (Unite...	
19	To: 7034241981	8/24/2013 4:57:39 PM(UTC+0)	00:00:36	Outgoing	311	480	Verizon Wireless (United...	
20	From: 6085159158 Dirty	8/24/2013 12:01:54 AM(UTC+0)	00:00:00	Missed	311	480	Verizon Wireless (United...	
21	From: 6085159158 Dirty	8/23/2013 11:47:39 PM(UTC+0)	00:00:00	Missed	311	480	Verizon Wireless (United...	
22	To: 7032979797	8/19/2013 9:05:36 PM(UTC+0)	00:00:34	Outgoing	311	480	Verizon Wireless (United...	

Total: 41 Deduplication: 0 Items: 41/41 Selected: 41

- a. What is the date and time of the last 2 **Outgoing** calls? Sorting the Type column might help with the answers.

**9/18/2013 11:54:14 AM UTC**

**9/19/2013 1:30:52 AM UTC**

- b. What number were they to?

**9/18/2013 11:54:14 AM UTC – 703 275 8332**

**9/19/2013 1:30:52 AM UTC – 608 515 9158**

### Bonus Questions

- c. Who (most likely) is “**Dirty**”? **Carlos Sanchez**
- d. Where did you get this information? **Contacts section**

4. At the top of the **UFED PA** window, you will see tabs starting to accumulate for each artifact that you have explored (if you have explored any). This can quickly become unmanageable. You can click the **x** on each tab to close it. You will now explore chat-style communications. In the left column of artifacts, we see three different formats of chat. **Chats**, **MMS Messages**, and **SMS Messages**. If we expand the arrow beside each one, we can see all the programs and/or folders where we have chat content.

Double click on **SMS Messages**. You will see the messages populate in the program, sorted by **Date/Time**. The red **x** to the left of the telephone numbers indicates deleted messages. The slider at the bottom of the screen allows the examiner to see further data. The numbers in red beside the artifacts in the left column indicate how many deleted items were recovered for that artifact.

The screenshot shows the UFED Physical Analyzer interface. The sidebar on the left lists various artifact types with their counts: Chats (16), MMS Messages (3), and SMS Messages (107). The main pane displays a table of SMS messages with columns for Timestamp, Delivered, Read, Folder, and Parties. A specific message is selected in the table, and its details are shown in a large preview pane on the right. The preview pane includes fields for Source, Destination, Date, Status, and Body. A red box highlights the 'Body' field, which contains a comment from 'Liz Lemon'. Below the preview pane, a red box highlights the 'Slider' at the bottom of the main pane, which is used to scroll through more messages.

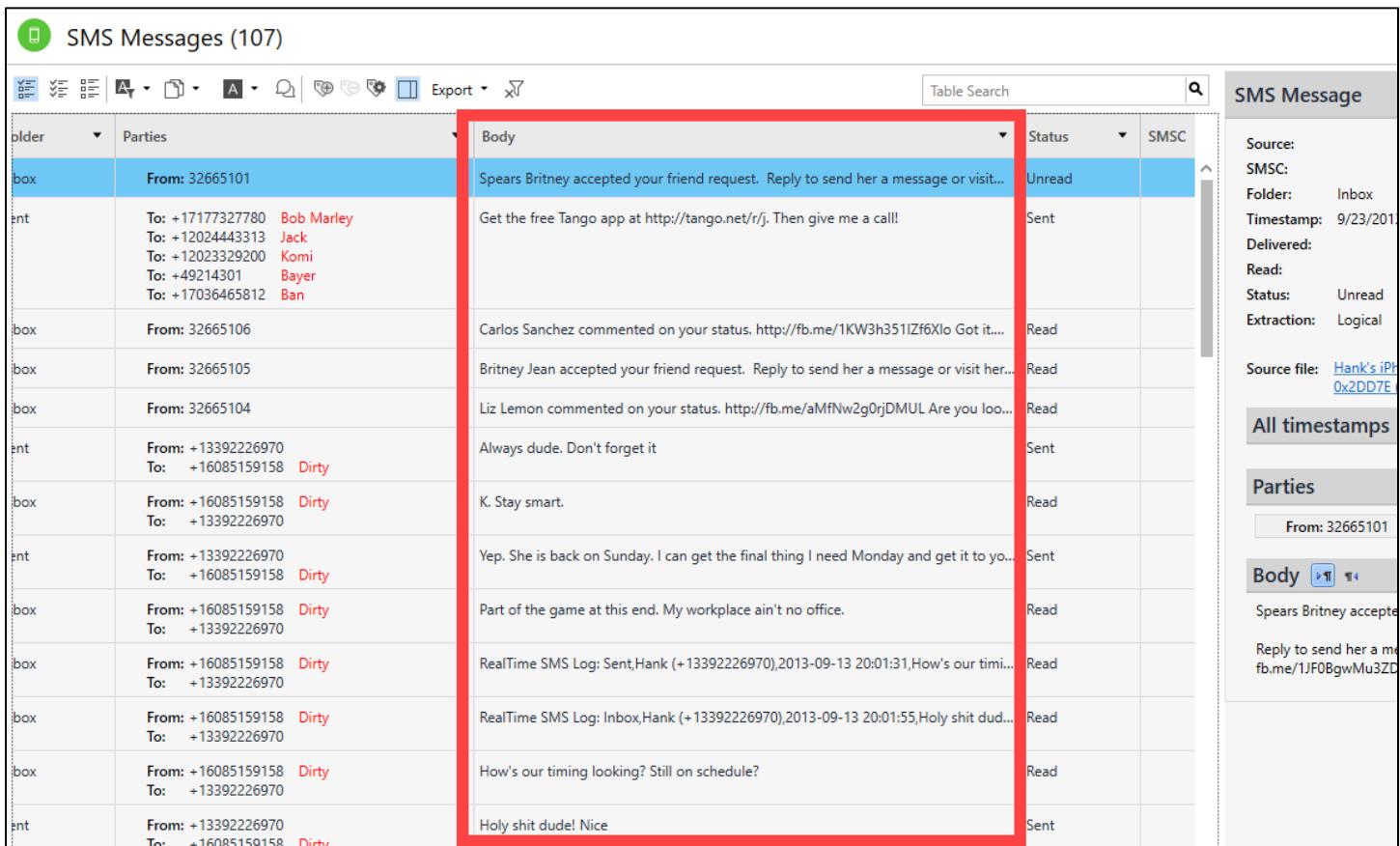
- What was the date/time of last incoming **SMS** message? **9/23/2013 12:40:46 PM UTC**
- What was the date/time of last outgoing **SMS** message? **9/19/2013 1:51:24 AM UTC**
- Who was the last outgoing **SMS** message to? **Bob Marley, Jack, Komi, Bayer, & Ban**
- How many different “**Chats**” programs are in use? **6**
- How many total **Messages** of all types are there? **126**

### Bonus Question

- What does “**MMS**” stand for, and what is unique about this type?

**Multimedia Messaging Service – This is an SMS that is carrying media, such as a picture**

5. If you use the slider as indicated in the previous step, and slide it to the right, you will see a column titled **Body**. This is the actual text of the message. Beside it is a **Status column**, indicating whether a message has been read or not.



The screenshot shows the Cellebrite UFED Pro interface with the following details:

- SMS Messages (107)**
- Table Headers:** Older, Parties, Body, Status, SMSC
- Table Data:** A list of 107 messages. The first few rows are:
  - From: 32665101 (Status: Unread)
  - To: +17177327780 (Bob Marley) (Status: Sent)
  - To: +12024443313 (Jack) (Status: Read)
  - To: +12023329200 (Komi) (Status: Read)
  - To: +49214301 (Bayer) (Status: Read)
  - To: +17036465812 (Ban) (Status: Read)
- Right Panel:**
  - SMS Message:** Source: SMSC: Folder: Inbox Timestamp: 9/23/2013 Delivered: Read: Status: Unread Extraction: Logical Source file: Hank's iPhone 0x2DD7E...
  - All timestamps**
  - Parties:** From: 32665101
  - Body:** Spears Britney accepted your friend request. Reply to send her a message or visit...
  - Message Preview:** Get the free Tango app at http://tango.net/r/j. Then give me a call!

- a. Have all the received **SMS** messages been read? Scroll to the right and note the Status column.

**No.**

- b. When was the first **SMS Message** read on this device? **6/20/2013 8:49:11 PM UTC**
- c. What is the owner name of this device? Found in Extraction Summary

**Hanks iPhone**

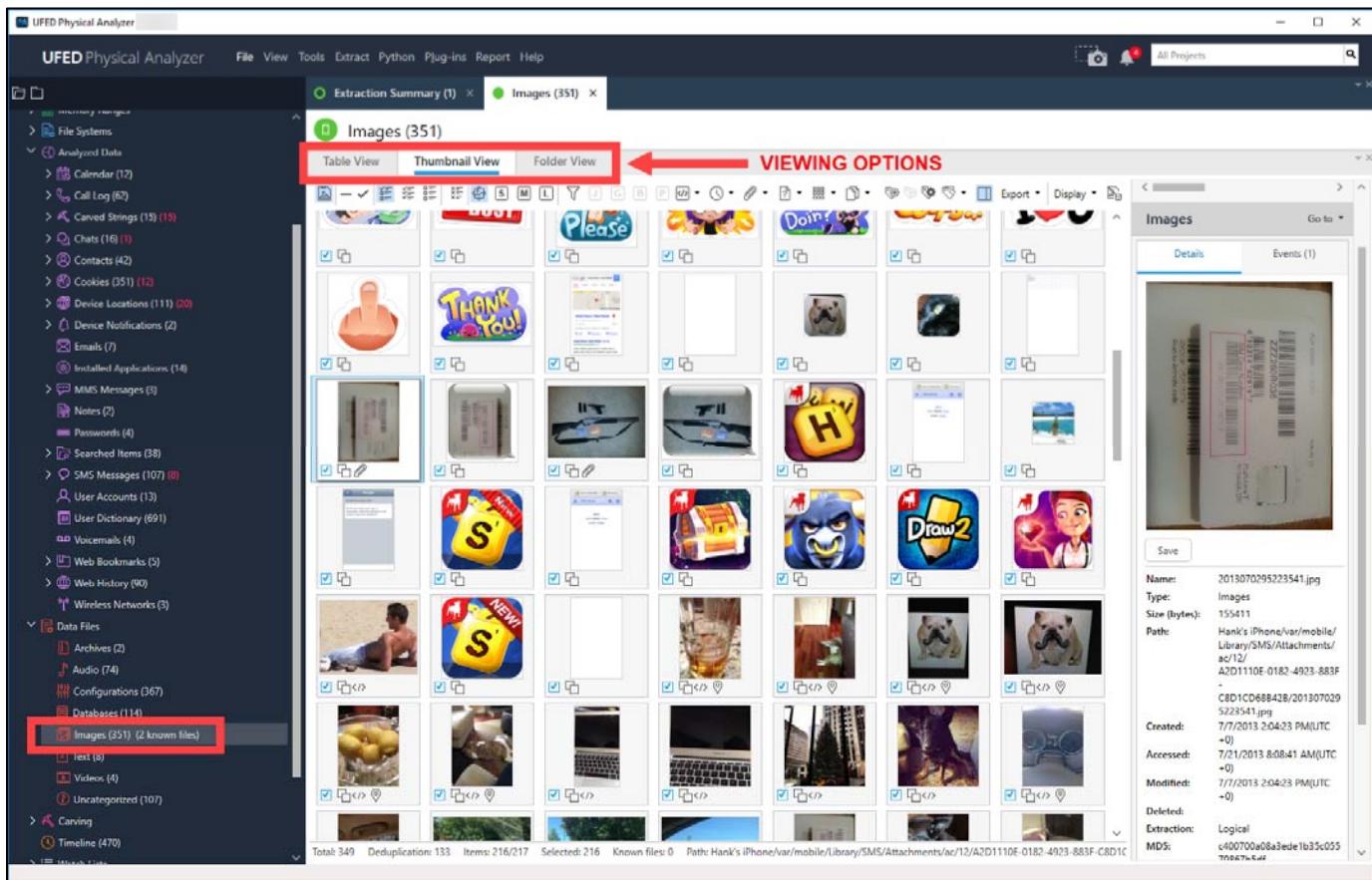
- d. What is their full name? Found in User Accounts - Skype

**Hank Livingston**

- e. What is their **AppleID?** Found in Extraction Summary

**livingstonhank11@gmail.com**

6. In the left column, we will explore some **Data Files** now; namely **Images**. Expand the **Data Files** section and double click on **Images**. You can see at the top of the **Images** pane, three viewing options. With **Thumbnail View** selected, you can see all of the pictures on the device. If you select a photo, you can see it, and its details, in the pane on the right of the screen.



7. Click on **Table View**, and scroll through the list looking for a picture with the name of **2013070295223541.jpg**. Once you find it, answer the questions associated with it.

Image ID	Name	Path
56	15FA97B1-D4CC-4486-8...	Hank's iPhone/var/mobile/Library/Caches/
57	2013070295223541.jpg	Hank's iPhone/var/mobile/Library/SMS/At...
58	2013070295223541-prev...	Hank's iPhone/var/mobile/Library/SMS/At...
59	2013091395195722.jpg	Hank's iPhone/var/mobile/Library/SMS/At...
60	2013091395195722-prev...	Hank's iPhone/var/mobile/Library/SMS/At...
61	2350368359b92e052384...	TarArchive/2350368359b92e0523841c28f4

- a. Where did the photo come from (i.e. how did it get on the phone)?

**Received in MMS from contact "Dirty"**

**Note through the data provided that this came from an SMS. You know that if an SMS carries media, it automatically becomes MMS. Check the MMS messages and find the photo. This will show where it came from.**

- b. What is the picture of?

**The packaging of a SIM card**

**You can double click on the photo to see a larger copy. Sometimes this merely shows a very blurry, unintelligible picture. You are probably seeing the thumbnail. Go through the Images and locate another copy.**

- c. How many total **Images** are on the device?

**351**

Bonus Question

- d. We believe there is a list of drugs on the device. What are the drugs on the list, and where was the list created? (**Hint:** start with images)

Roxicodone

Oxycodone

Hydrocodone

Fentanyl

Onsolis

List was created on the phone itself and found in a screen capture of the device.

Looking through the images, you can see a few images that look like lists. Highlighting one and opening it shows that the resolution is so low that we can't read the list.

	PreviewWellIm...	Hank's iPhone/var/mobile/Media/PhotoData/MISC/PreviewWell...	25562		9/18/2013 11:52:23 AM(UTC+...
--	------------------	--	-------	--	-------------------------------

Look for other versions of the list. Maybe you simply found the thumbnail and not the original. Further looking in the list shows another version where it appears the list is superimposed on top of a photo.

	thumb_33.bmp	Hank's iPhone/var/mobile/Media/PhotoData/Thumbnails/120x12...	28866
--	--------------	---	-------

This might lead you to believe that this is from a screenshot of the device, further leading you to believe that the list was created on the device. Continue looking through the images until you find a .PNG file that looks like it might be the list. Phones typically capture screenshots in a .PNG format.

	IMG_0047.PNG	Hank's iPhone/var/mobile/Media/DCIM/100APPLE/IMG_0047.PNG	53409
--	--------------	---	-------

When you find it, you will see that indeed (via the file path) it was taken with this device. Double click on the picture in the right column under Details, and you will see the list.

The screenshot shows the Cellebrite software interface with the following details:

- File Name:** IMG\_0047.PNG
- View Options:** Hex View, Image view (selected), File Info.
- Control Buttons:** Navigation arrows, refresh, zoom, and search.
- Table Data:** A table listing prescription items with columns: Item, Dosage, Quantity, SV, and total.

		#	SV	total
	Roxicodone	30 mg	500	20
	Oxycodone	80 mg	1000	30
	Hydrocodone	11.25 mL	500	5
	Fentanyl	25 ug patch	750	50
	Onsolis	200 mcg patch	100	50

### Exercise—Key Takeaways

- There are many “quick wins” in the easily available data from a portable device.
- You must be able to explain what you see and give reasons why.
- Vendors pack more and more features into their software every day. Software that looks easy and intuitive could have many intricate surprises, and you must become familiar with them.

## Exercise 2.2B—Portable Device Analysis-Axiom

### Background

As you are conducting an investigation, whether it be roadside, or in a lab, you must have some idea of what is available on a smartphone. In addition, you must be able to access it quickly, but in the least intrusive manner possible. Although data may be very time sensitive, there also may be other data on the device in a deleted space that could be very important but will be destroyed by your actions. This creates a dilemma that can only be dealt with through intelligent “risk vs reward” determination.

Examiners may have tools at their disposal to create a data image of the device (notice we don’t say forensic image) that are quite varied. Some are quite expensive, but some can be quite cheap. The difference tends to be blurry, other than the ability to create hash values and verifications.

The more effective tools will allow for interaction with the found files, and the ability to cross reference them against other data on the device. For example, a photo from which an examiner can extract the exact location where it was taken, and/or date and time of when the photo was taken.

While these tools designed for “forensic” acquisition are very effective, just how accurate are they? And how responsive are they to the updating processes from device manufacturers? Sometimes it is necessary to use less than optimal tools, and sometimes it is necessary to let more than one tool review a data dump to get the clearest picture of the data. Our only option may be to inspect data from nothing more than a file/folder level.

### Exercise Objectives

- Use **Axiom** to examine an Apple iPhone image

### Exercise Preparation

1. Boot your **FOR498 Windows SIFT VM**
2. Login to the **FOR498 Windows SIFT VM** using the following credentials:
  - a. Username: **SANSDFIR**
  - b. Password: **forensics**

Different software can produce different results when examining media. A very capable tool for analyzing many different types of data is a program called **AXIOM**, from Magnet Forensics.

3. Minimize the **UFED PA** program that you used in the previous steps. It is nice to have it available for comparison throughout this exercise.

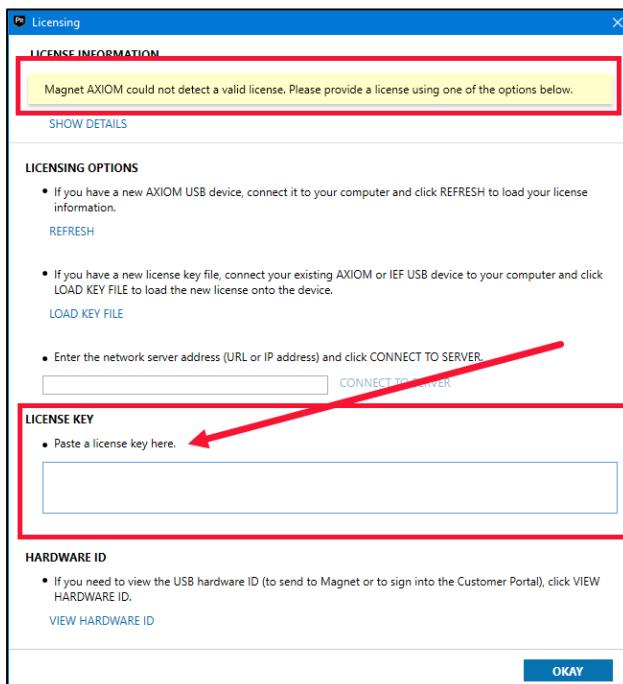
- Start the **AXIOM Process** application by double clicking the icon in the **Forensic Suites** fence on your **Desktop**. This program takes a few seconds to open, so be patient. Note that you do NOT want two instances opening!



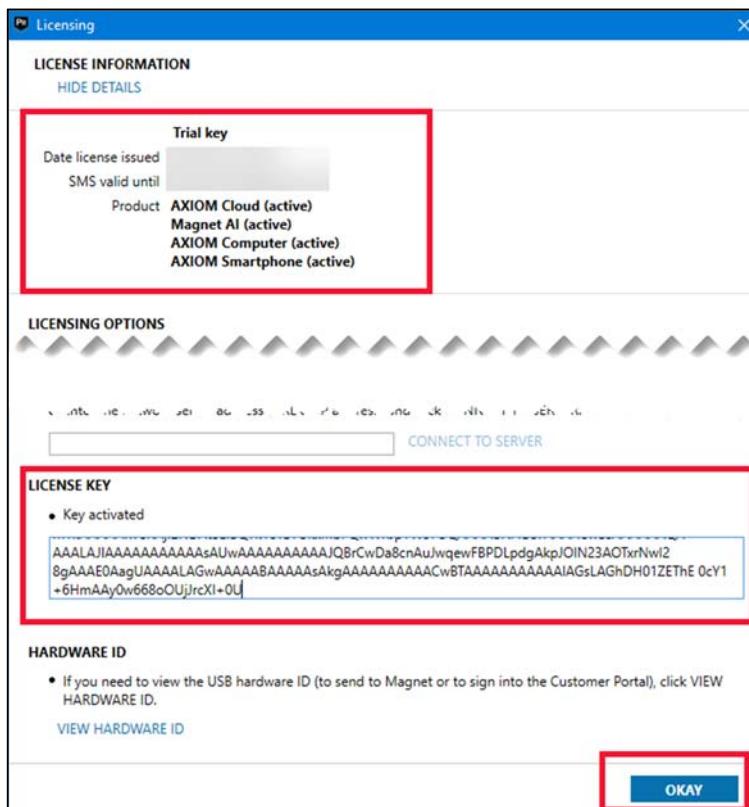
- After a few seconds where it will appear that nothing is happening (BE PATIENT), a splash screen will appear.



- NOTE:** If prompted to update your tool, please wait until you leave the classroom this evening or are on your home or hotel Internet to update (unless otherwise directed by your instructor). Updating is optional and may “break” the functionality of the tool. Updating is at your own risk as we know the versions installed in this **VM** work!
- Since this is the first time you are opening **AXIOM**, you will be asked for licensing information. This information has been provided by SANS or your instructor. You will see the Licensing window below. Take the **LICENSE KEY** that was provided to you and paste it into the box as indicated.

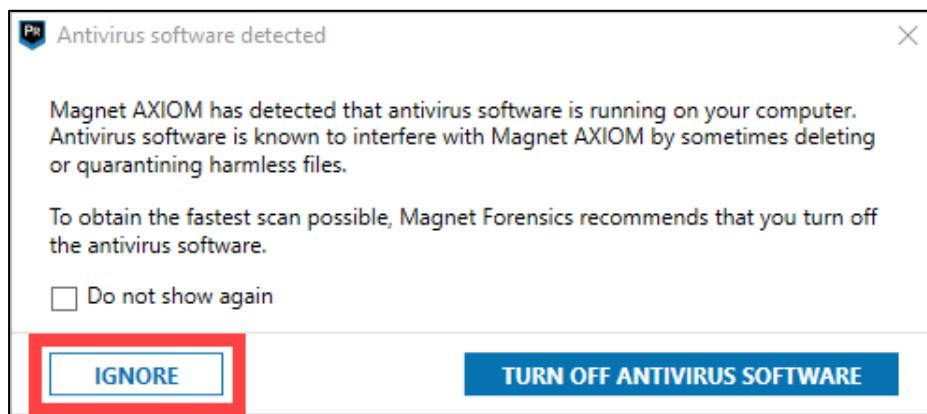


8. Once pasted in, the program will automatically detect the license and show the products it is for. If it does not, click the **OKAY** button. Once it is recognized, you will see the information in the screen. Click **OKAY**.

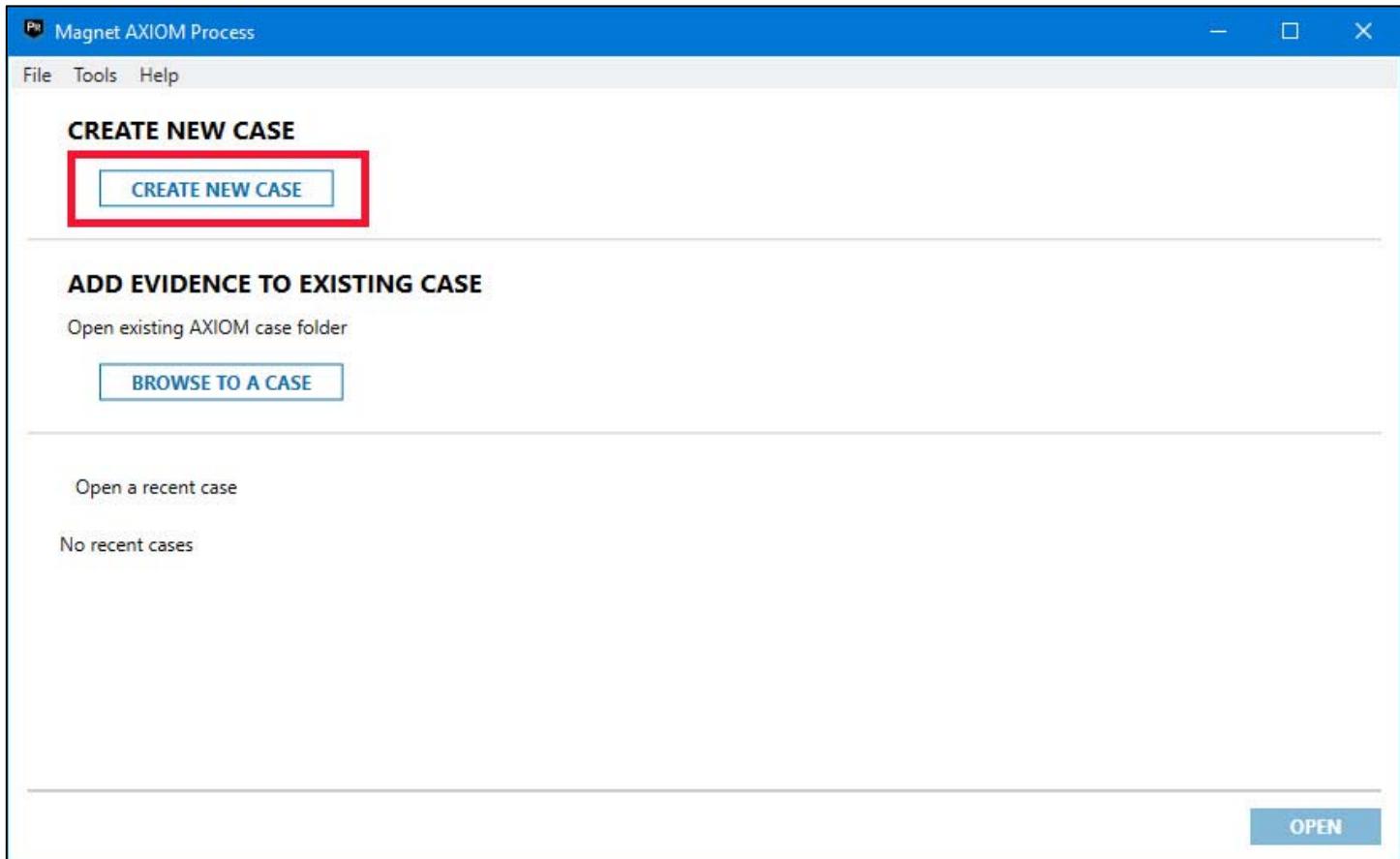


9. Once again, if prompted to update, **DON'T**.

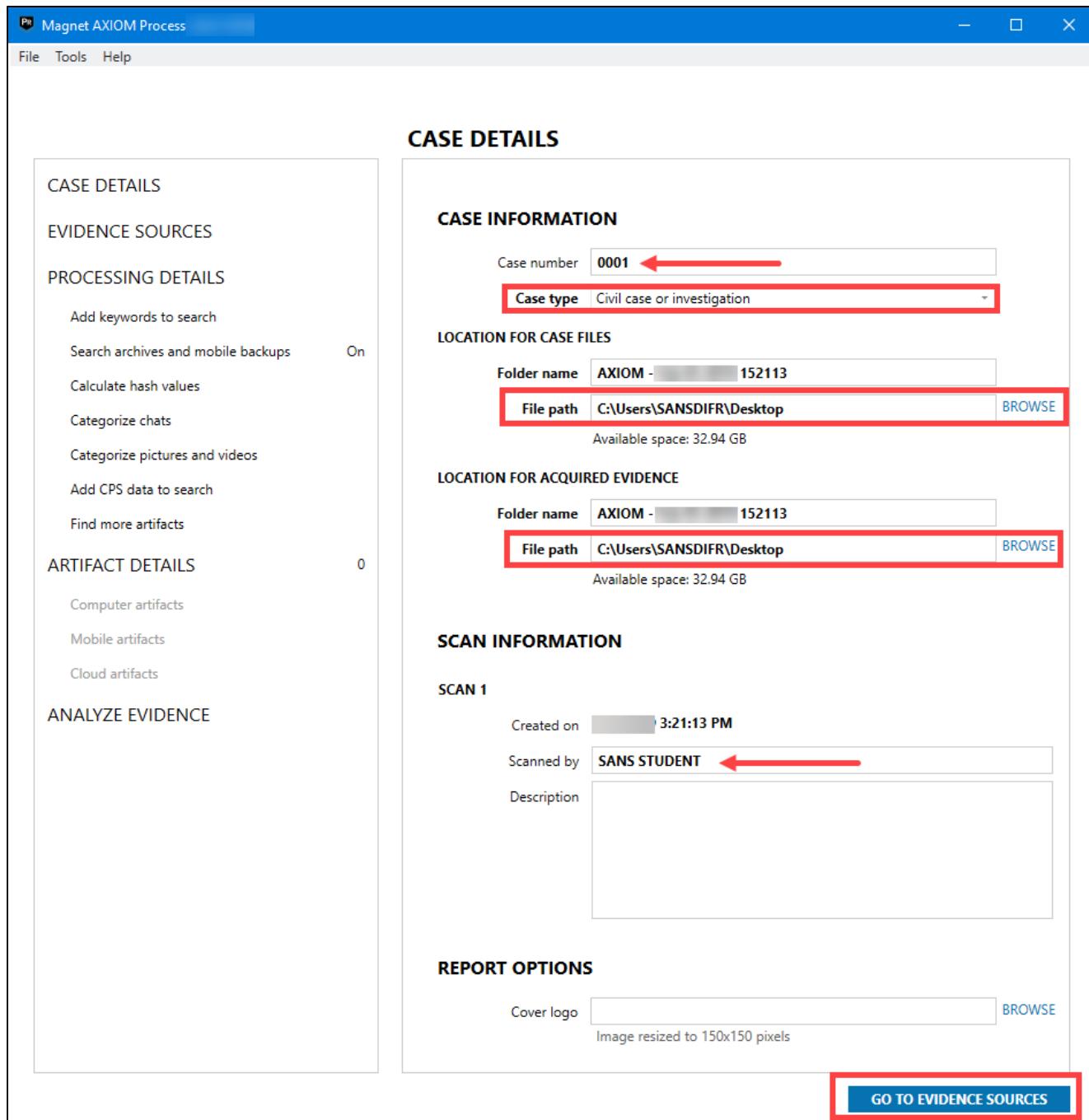
10. You may get a prompt regarding turning off your anti-virus. For the purpose of this lab, we will click **IGNORE**. This would not be a default setting! Your environment and protocols will vary.



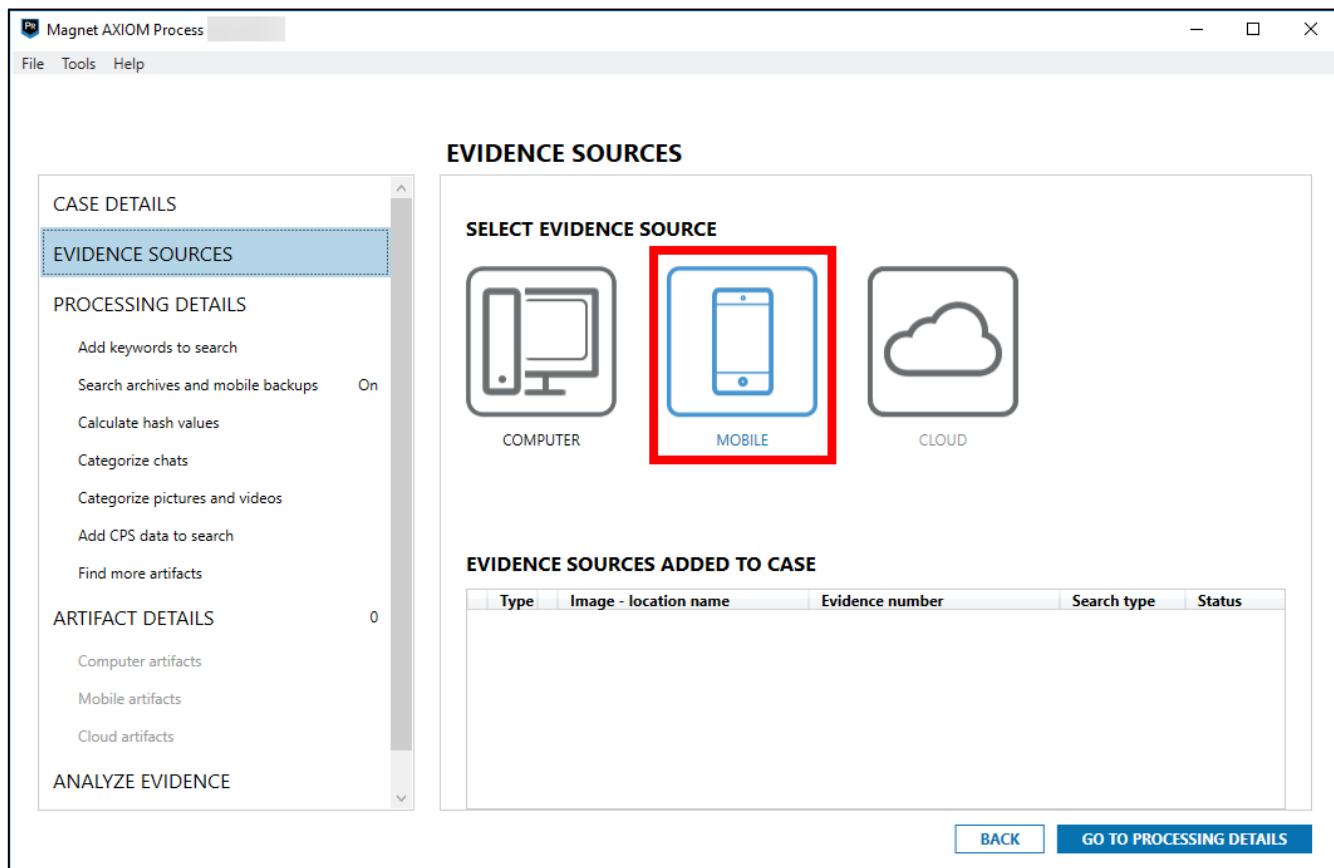
11. Once the application opens, click on **CREATE NEW CASE**.



12. The **CASE DETAILS** window will open. Every box needs data except the **Description** box and **REPORT OPTIONS**. Add a **Case number** under the **CASE INFORMATION** section, then click the arrow on the **Case type** field, and select **Civil case or investigation**. For both **LOCATION** fields, you can change the **Folder name** to something more memorable than the default if you wish, and then **BROWSE** to the **Desktop** and use it for the **File path**. Add a name to the **Scanned by** field under the **SCAN INFORMATION** section. Then click **GO TO EVIDENCE SOURCES**.



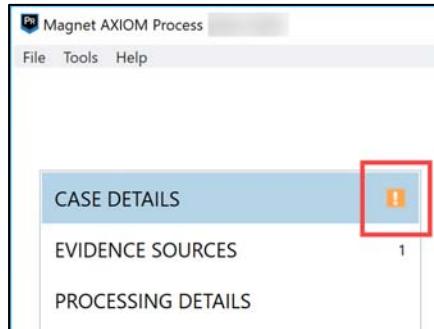
13. When the **EVIDENCE SOURCES** window opens, select **MOBILE** under the **SELECT EVIDENCE SOURCE** options.



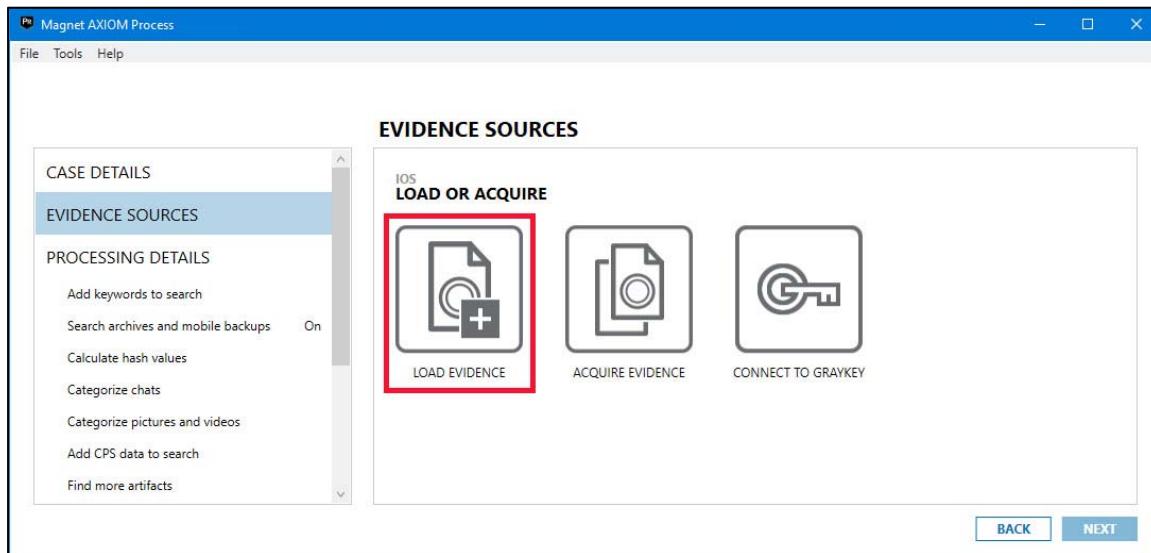
14. In the next window, select your image type. In the case of this exercise, select **IOS**.



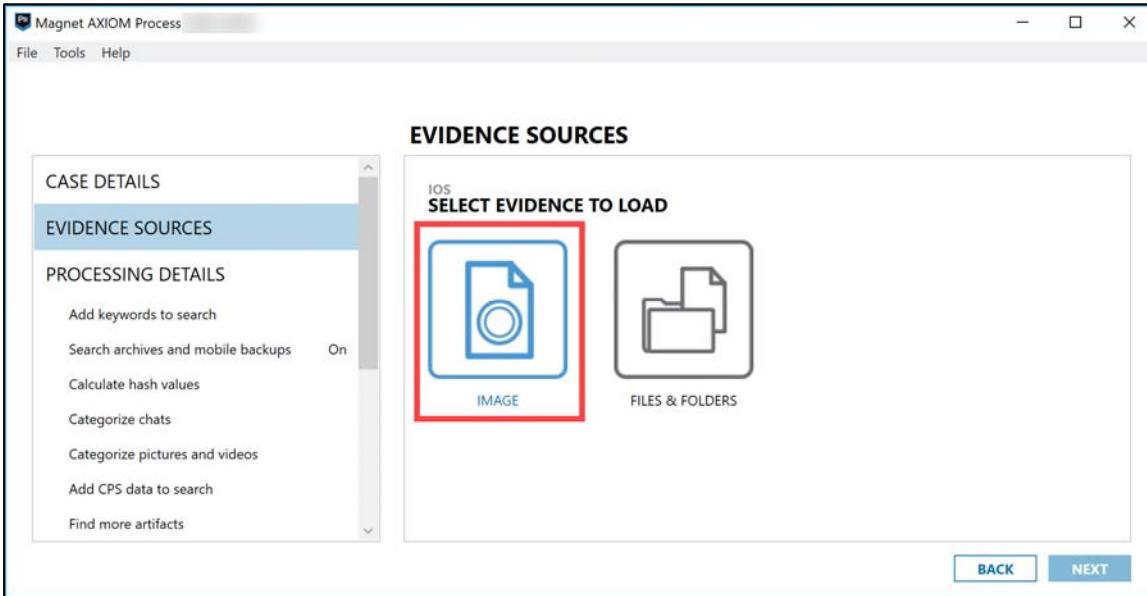
15. If you see the indicated white exclamation mark inside the orange box in the left column at any point, you have missed some required information. Press the **BACK** button and complete the entry, or the case will not analyze.



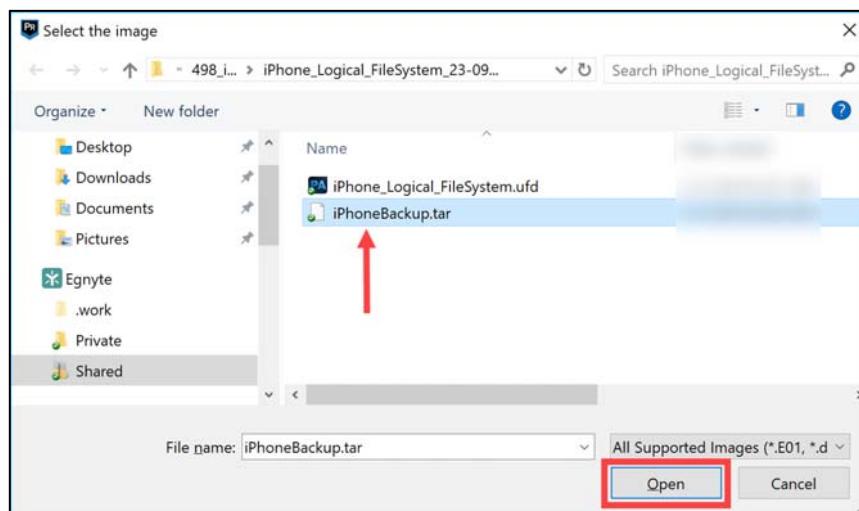
16. Select **LOAD EVIDENCE**.



17. Select the **IMAGE** option.



18. An explorer window will open. Navigate to **C:\Cases\498\_iPhone5\iPhone\_Logical\_FileSystem\_23-09-13\_09-02-01\**, click on the **iPhoneBackup.tar** file, and then click **Open**.



19. You will see a long list of the data that will be included for ingestion. All boxes should be checked, but if not, check them, then click **NEXT**.

**EVIDENCE SOURCES**

**CASE DETAILS**

**EVIDENCE SOURCES** (Selected)

**PROCESSING DETAILS**

- Add keywords to search
- Search archives and mobile backups On
- Calculate hash values
- Categorize chats
- Categorize pictures and videos
- Add CPS data to search
- Find more artifacts

**ARTIFACT DETAILS** 0

- Computer artifacts
- Mobile artifacts
- Cloud artifacts

**ANALYZE EVIDENCE**

**IOS ADD FILES AND FOLDERS**

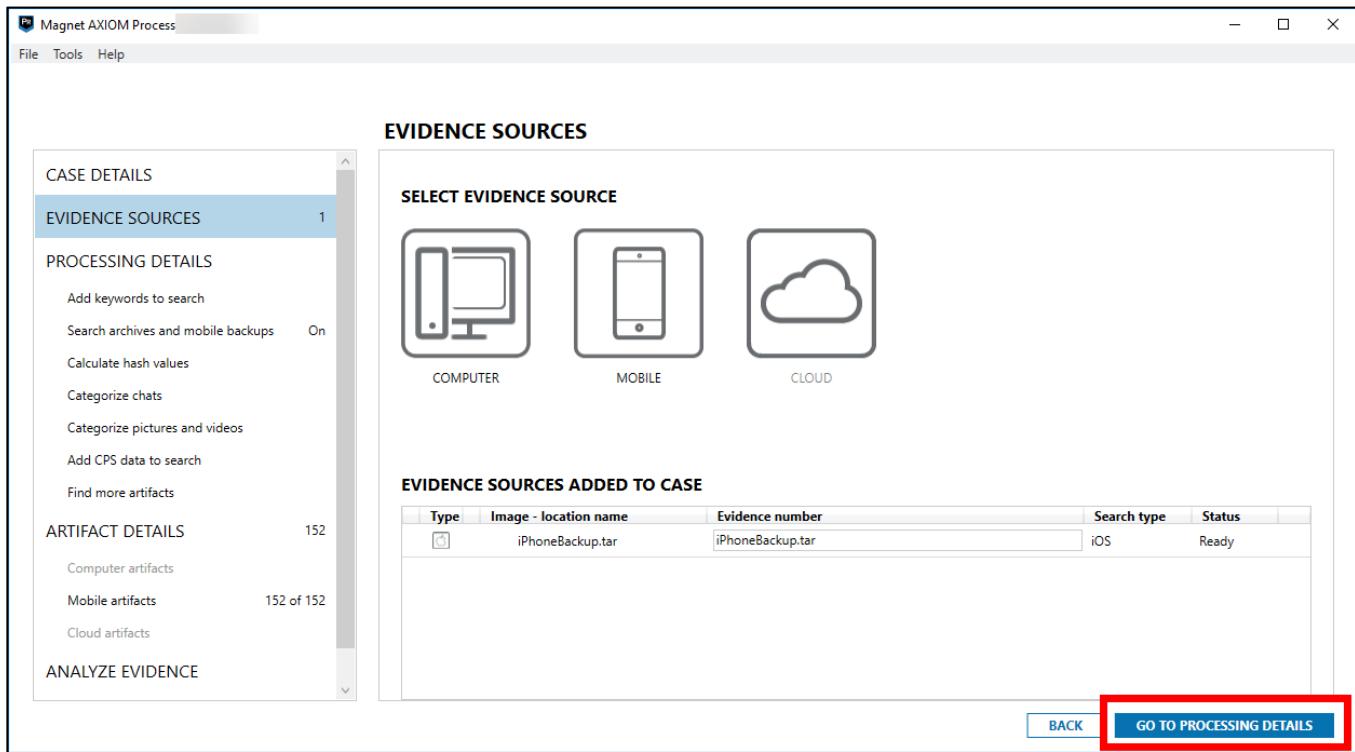
**CLEAR ALL**

iPhoneBackup.tar

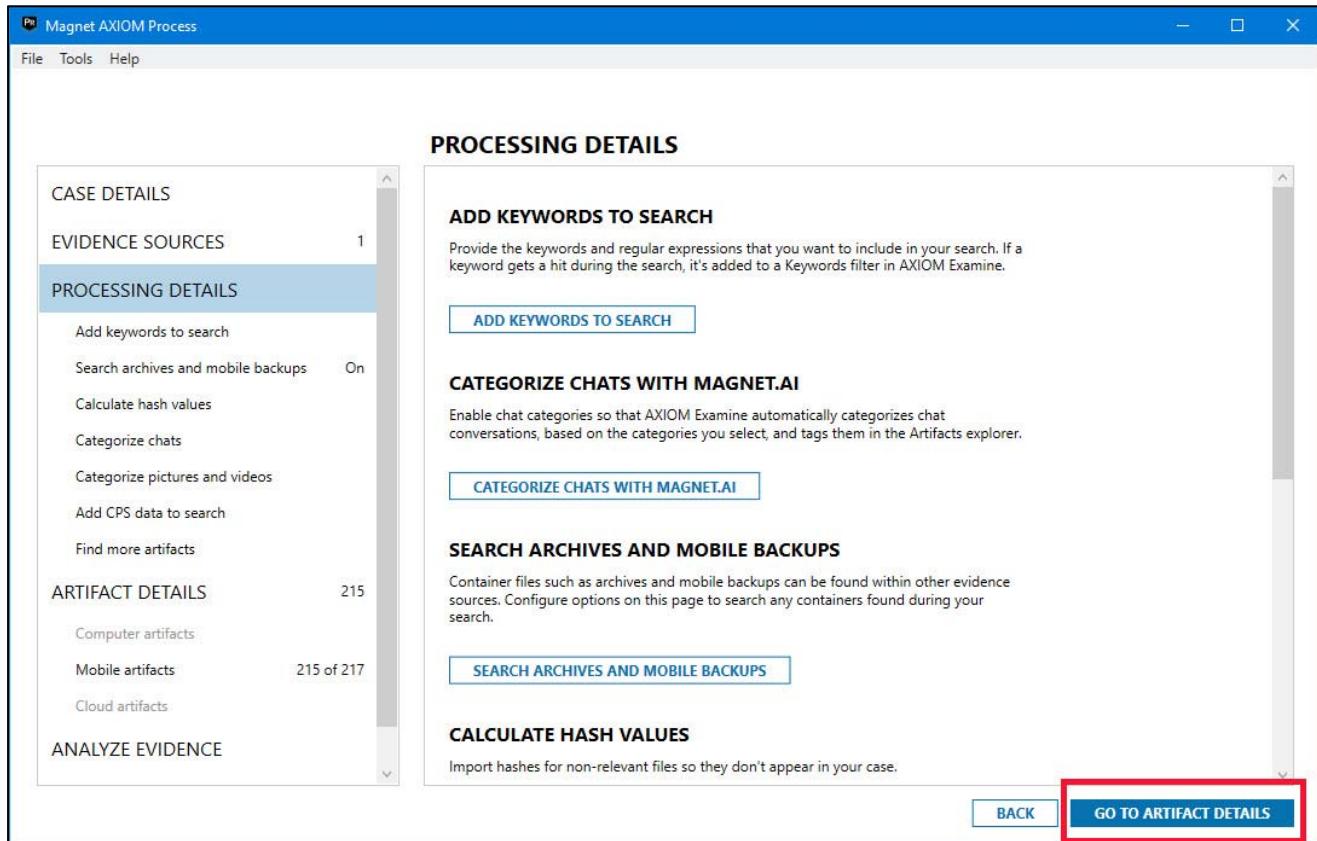
- 01585f17b1d76b180da8b3acf148bbf60d832453
- 018a1bc37d674452d9550bfb2b4cc4dda271da8
- 01d0699856a52d490042ab7a5c13395704a32c6c
- 027b84cbdea76458437524c15d2801fe1f48c3f2
- 03b4b9397c520e194f75ac7a32b436f9aab583e
- 05011952a6e84cedccc2c227e3b7288575e39a05
- 059a3fed6d5ccc69ca5d214766d91eb2964787ef
- 0692d95dc311a27738d74a54416d4bcea6f19b5a
- 06af93e6265bf32205de534582c3e8b8b3b5ee9e
- 06c643094e1111ec02fdb76f6303dff57836f475
- 06c7de38dab54923936ff72365d7477d3ee35895
- 06d624a45988c5177d0cca2902868f24e2d459ad
- 07a08b20964348b30b7023fe8275e746dffaf797
- 07baa2b107753ad039b2928a9a3ea5fff70bc8bc
- 07e5ca59da6b9bf3a04301094ab2a3b5d5cd5e36
- 0843cc4169950d27b19102adeef7ecd42eea7320
- 08f11d0ebeab557bd6deece0eb68f890fbfabed4
- 091760b3b35bada34a872fdd4b6b52b0c82c22bf
- 096afb1afab2fde5297409749174c642db9bdd4b
- 0987feb9d93d6d2933df2d3d633a75cf4c28f34c
- 0adb4e8277470cf8cbe5a8ea30aca04af1ceddea
- 0aa0081a637a5617a44fra794e7f76a52h66aaah

**BACK** **NEXT**

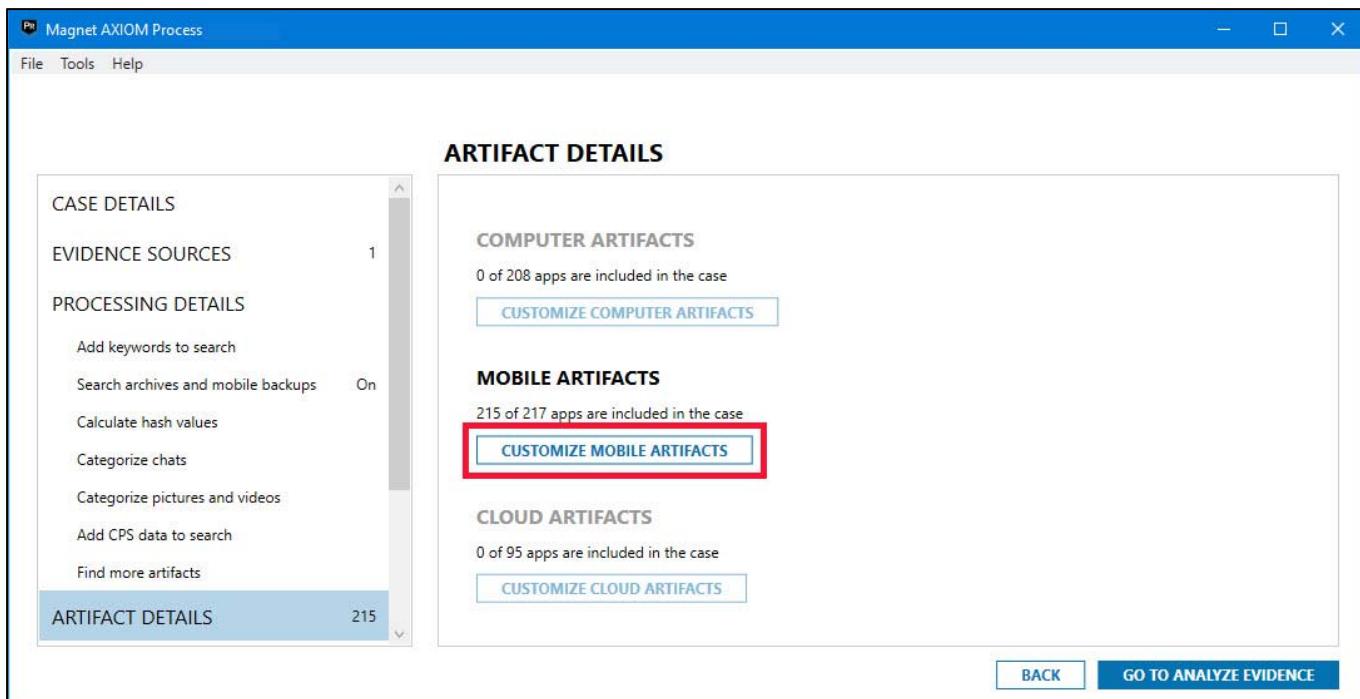
20. You will arrive back at the original **EVIDENCE SOURCES** window where you had chosen **MOBILE**. You can see the evidence that was just added to the case. Select **GO TO PROCESSING DETAILS**.



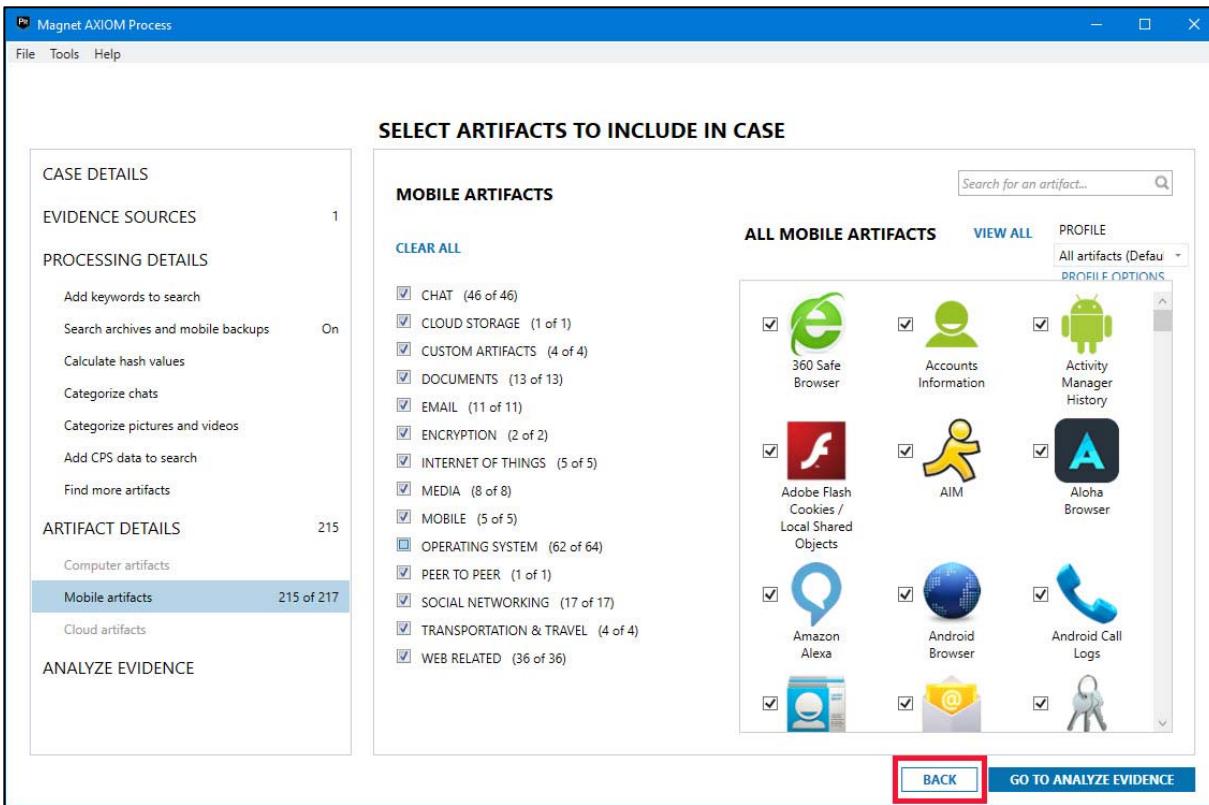
21. A number of different options are available at this point. Take a moment to scroll through the list and see what is possible. We will not be changing anything here. Click on **GO TO ARTIFACT DETAILS**.



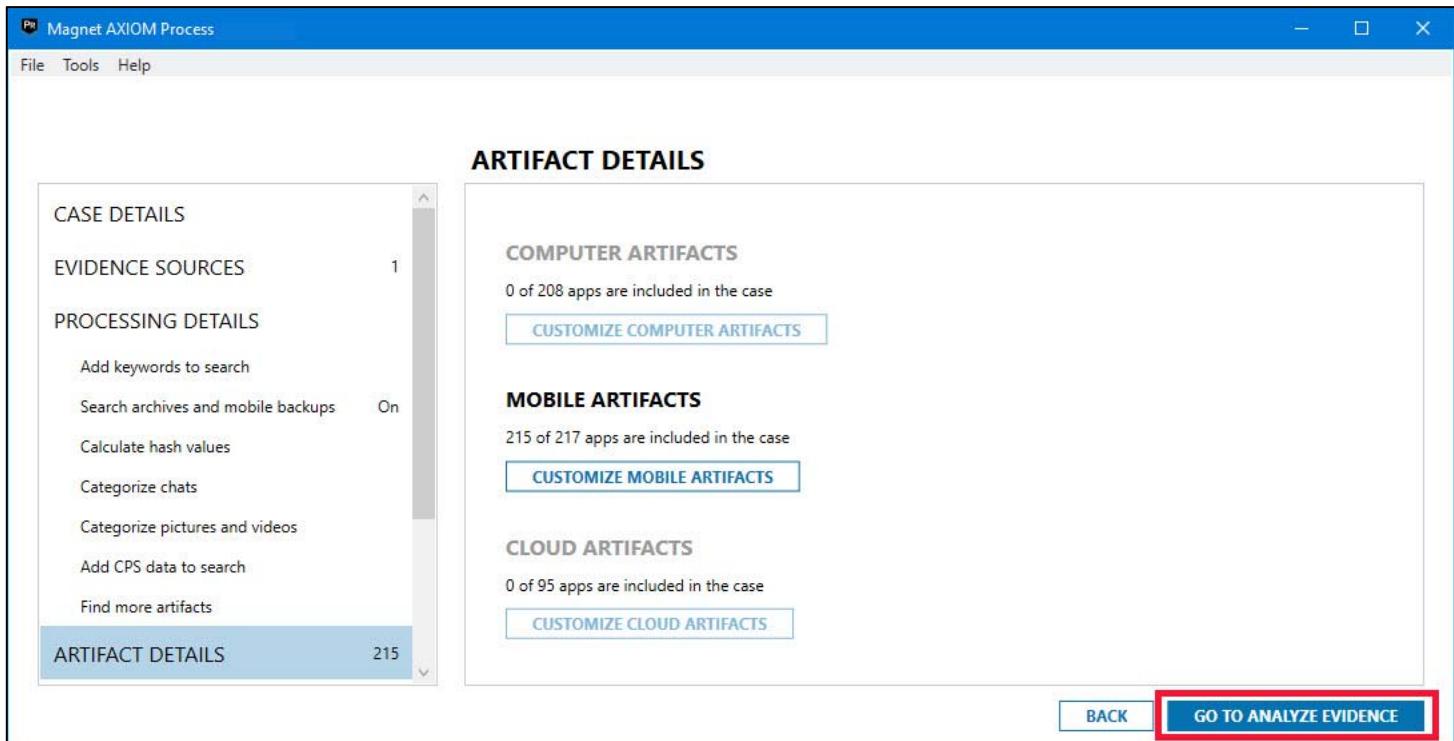
22. In the next window, you are able to select any customization as necessary. Although we will not be changing any settings, click on **CUSTOMIZE MOBILE ARTIFACTS** to see what is available.



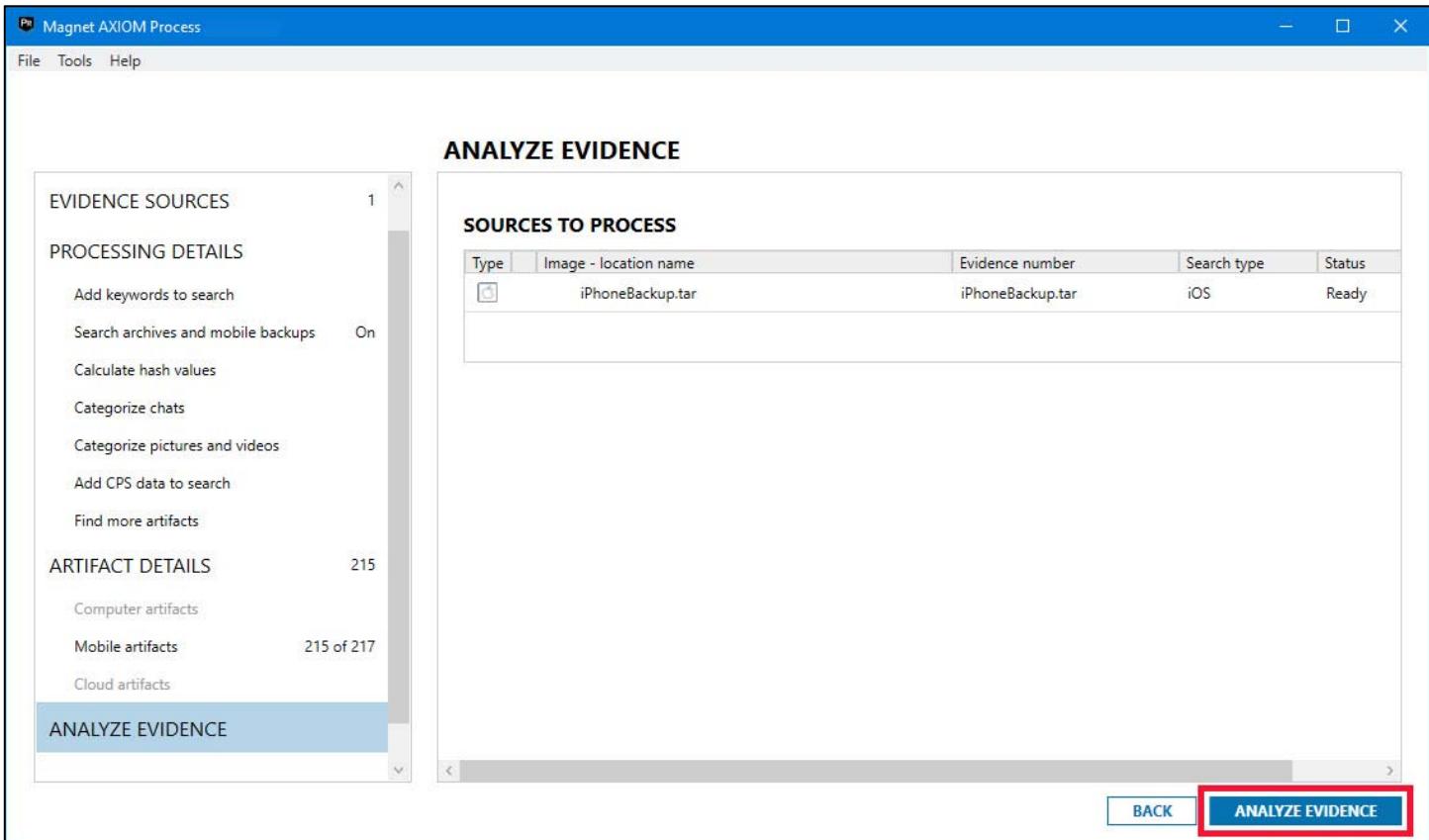
23. You will now see and be able to select whatever artifacts may be important for your investigation. Very seldom would we select all the options simply because, for example, Android artifacts are not necessary to be searched on an iPhone. Having all options selected also causes the processing to take longer. After scrolling to see the various options, simply click the **BACK** button without making any changes.



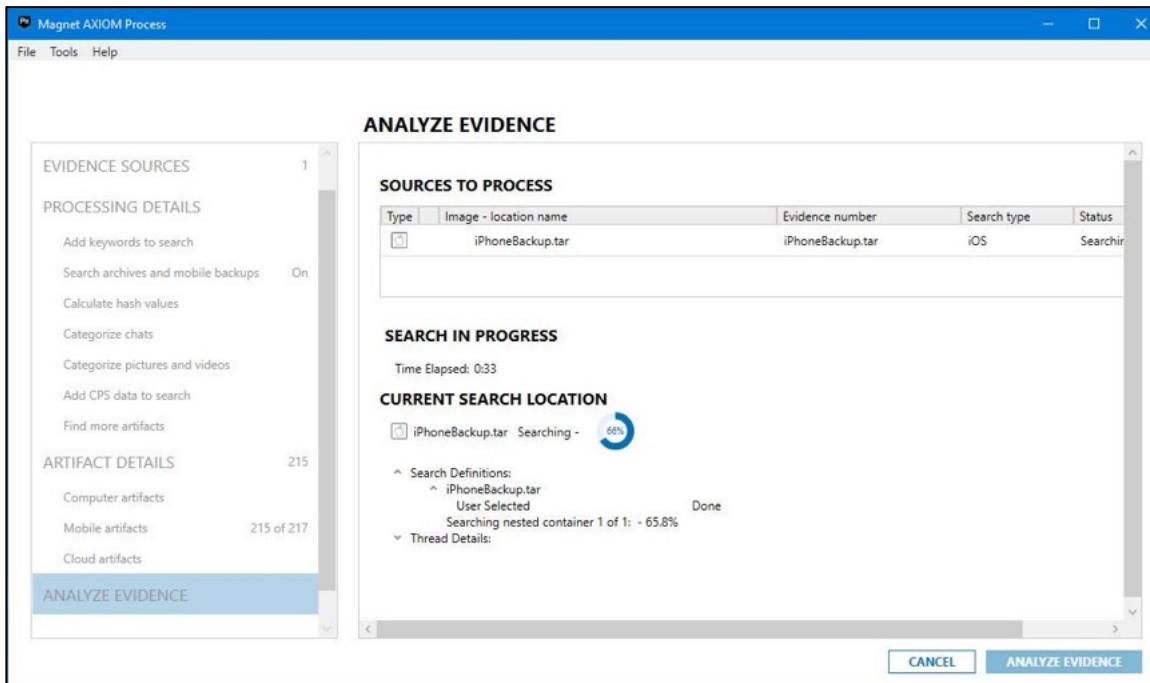
24. You will return to the previous screen. Simply click on the **GO TO ANALYZE EVIDENCE** button.



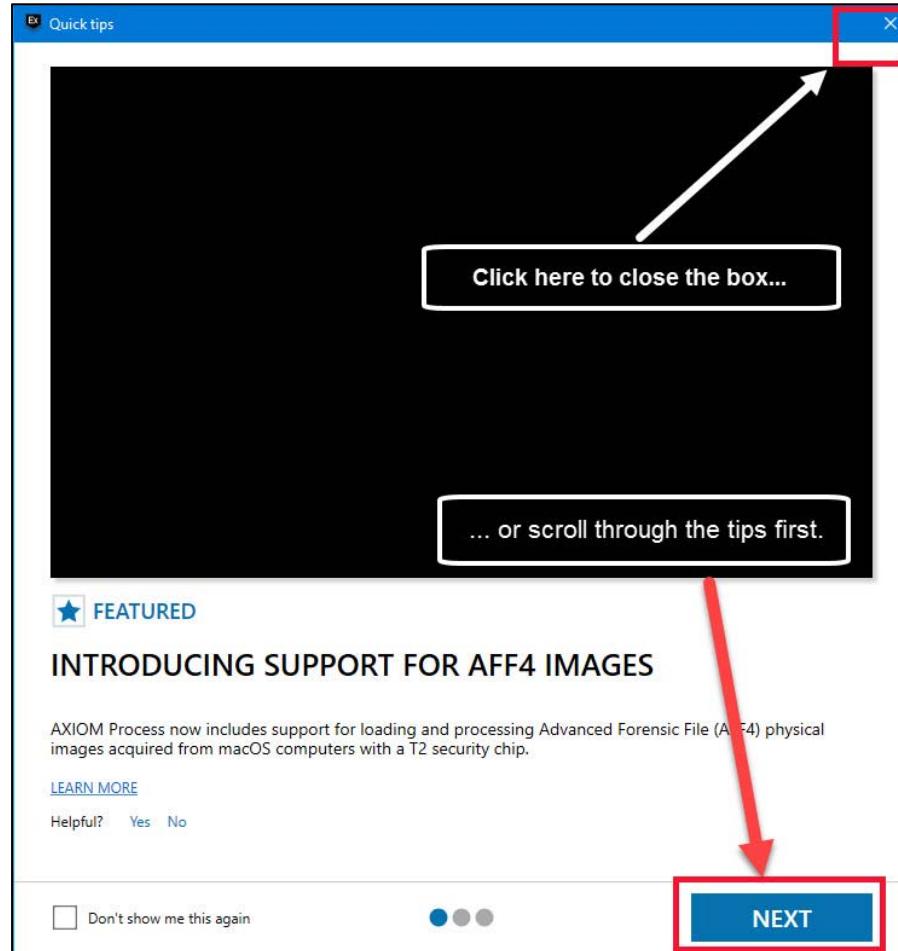
25. One final confirmation page, and you will click on **ANALYZE EVIDENCE**.



26. The processing function will now start, and the **Magnet Examine** application will open.



27. You may also see a box open offering **Quick tips**. You can simply close it, or click **NEXT** to scroll through the tips and **EXIT** when done.



28. Once processing is complete, it will be shown by the **Processing complete** indicator in the bottom left corner of the **Magnet Examine** window. Click on **OKAY** to force a refresh of the artifact numbers. Review the **CASE OVERVIEW** page and familiarize yourself with some of its features. At the top right corner under the **PLACES TO START** section, and inside **ARTIFACT CATEGORIES**, click on **VIEW ALL ARTIFACT CATEGORIES**.

[Case dashboard](#)

## CASE OVERVIEW

**CASE SUMMARY NOTES**

Record your case summary notes here. These notes will appear in the case report when the setting is enabled.

Examiner name:

Case summary:

**CASE PROCESSING DETAILS**

CASE NUMBER: 0001

SCAN 1

Scanned by: SANS STUDENT

Scan date: 12/10/2020 10:50 PM

Scan description:

**CASE INFORMATION**

The Case Information.txt file contains information about how the case was processed. For example, the file includes the settings that were applied to the search, search type, number of artifacts discovered, and more.

[OPEN CASE INFORMATION FILE](#)

Processing complete   OKAY

## EVIDENCE OVERVIEW

[ADD NEW EVIDENCE](#)

**iPhoneBackup.tar (3,469)**

[VIEW EVIDENCE FOR THIS SOURCE ONLY](#)

Evidence number	iPhoneBackup.tar
Description	<input type="text"/>
Location	iPhoneBackup.tar
Platform	Mobile

No picture added [CHANGE PICTURE](#)

## PLACES TO START

### ARTIFACT CATEGORIES

[VIEW ALL ARTIFACT CATEGORIES](#)

Evidence source: All

Number of artifacts: 3,465

Web Related	2,172
Mobile	475
Media	289
Refined Results	265
Chat	244
Operating System	20

### TAGS AND COMMENTS

### MAGNET.AI CATEGORIZATION

### CPS DATA MATCHES

### KEYWORD MATCHES

### PASSWORDS AND TOKENS

### MEDIA CATEGORIZATION

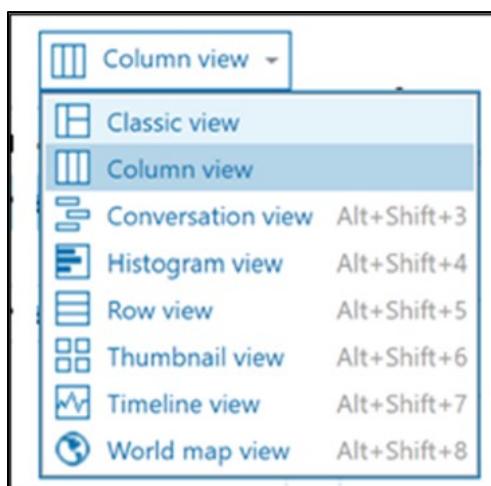
### PROFILES

Time zone: UTC+0:00

29. You will see an overview of all categories processed by AXIOM. Spend some time clicking around the evidence artifacts in the left column to familiarize yourself.

EVIDENCE (3,535)			
	Item	Type	Artifact c...
	TAR	File System Information	Operating System
	com.apple.weather	Installed Applications	Mobile
	com.apple.WebViewService	Installed Applications	Mobile
	com.facebook.Facebook	Installed Applications	Mobile
	com.pandora	Installed Applications	Mobile
	com.skype.skype	Installed Applications	Mobile
	com.sgiggle.Tango	Installed Applications	Mobile
	com.googleMaps	Installed Applications	Mobile
	com.kik.chat	Installed Applications	Mobile
	com.atebits.Tweetie2	Installed Applications	Mobile
	com.newtoysinc.WordsWithFriendsFree	Installed Applications	Mobile
	com.vinaixa.PrivateMSG	Installed Applications	Mobile
	com.viber	Installed Applications	Mobile
	com.facebook.Messenger	Installed Applications	Mobile
	com.midasplayer.apps.candycrushsaga	Installed Applications	Mobile
	1	iOS Kik Messenger Users	Chat
	2	iOS Kik Messenger Users	Chat
	3	iOS Kik Messenger Users	Chat

30. Note that at the top right of the **EVIDENCE** section, you see an icon titled **Column view**. If you click on it, a drop down will show you the various viewing options. Depending on the artifact you are investigating, you may want to change the view. For example, when viewing pictures, you may want the **Thumbnail view**. For chats, you may want the **Conversation view**. Remember that the only two views that show the **ALL EVIDENCE** column on the left are the **Classic view** and the **Column view**. To get back to seeing this column, just change your view back to **Column view**.



**Exercise Questions**

- Click on the **MOBILE** section to expand it, and then click on **iOS Call Logs**.

The screenshot shows the Magnet AXIOM Examine interface. On the left, there's a sidebar with filters like 'Evidence', 'Artifacts', 'Content types', etc., and a search bar. Below that is a tree view of evidence categories: WEB RELATED (2,172), CHAT (244), MEDIA (359), MOBILE (475), and OPERATING SYSTEM (20). The 'MOBILE' category is highlighted with a red circle labeled '1'. Under 'MOBILE', 'iOS Call Logs' is also highlighted with a red circle labeled '2'. The main pane shows a table titled 'EVIDENCE (41)' with columns for Local User, Partners, Part..., Dire..., Call T..., and Call... (with a 'Column view' button). The table lists various call entries. To the right, a detailed view for a 'Local User <iPhoneBackup.tar>' is shown, including sections for 'DETAILS', 'ARTIFACT INFORMATION', and 'EVIDENCE INFORMATION'. The 'ARTIFACT INFORMATION' section includes fields like Local User, Partners, Direction, Call Type, Call Status, Call Date/Time, Call Duration (Seconds), Service Provider Country Code, and Source. The 'EVIDENCE INFORMATION' section shows the source as 'iPhoneBackup.tar \2b2b0084a1bc3a5ac8c27afdf14a'. At the bottom right, it says 'Time zone UTC+0:00'.

- How many calls are in the call log?
- 
- Is this the same amount that we saw from Cellebrite?
- 
- If not, why do you think there is a difference?
-

2. Click on the **CHAT** evidence section to expand it. Explore the various types of chat, their views, and the messages in them. Then click on **Skype Chat Messages**.

The screenshot shows the Magnet AXIOM Examine interface. The left pane, labeled 'EVIDENCE (6)', lists various types of artifacts found in the evidence. A red box highlights the 'CHAT' category, which contains 244 items. A red circle with the number '1' is placed over the 'CHAT' category. Another red circle with the number '2' is placed over the 'Skype Chat Messages' item under the 'CHAT' category. The right pane, labeled '#hankl1107/\$hn... iPhoneBackup.tar', displays a preview of a Skype conversation between 'hankl1107' and 'hn...'. The conversation shows messages like 'Hey, How are you?', 'Hank Livingston requested to add hn... as a contact', and 'Howdy'. The bottom right corner of the interface shows the time zone as 'UTC+0:00'.

	Chat ID	Profile	Auth...	Reci...	From Di...
#hankl1107/\$hn...	hankl1107	hankl1107	hn...	Hank Livingston	
#hankl1107/\$hn...	hankl1107	hankl1107	hn...	Hank Livingston	
#hn...	hankl1107	hankl1107	hankl1107	hn...	
#hankl1107/\$hn...	hankl1107	hankl1107	hn...	Hank Livingston	
#hankl1107/\$hn...	hankl1107	hankl1107	hn...	Hank Livingston	
#hankl1107/\$d...	hankl1107	hankl1107	dirtyc...	Hank Livingston	

- a. How many different people has **hankl1107** been chatting with?
- 

- b. How many total chat messages are there of all types?
- 

- c. Is this the same amount of chats that Cellebrite found?
- 

- d. On 9/6/2013 4:04:38 AM, **hankl1107** was in a Skype chat. What was the public IP address, and where does it trace to?
-

3. Ensure your view is showing **Column view**, so you can see the **EVIDENCE** list on the left of the **AXIOM Examine** window. Expand the **MEDIA** section and click on **Pictures**.

The screenshot shows the Magnet AXIOM Examine interface. On the left, there's a sidebar with filters like 'Artifacts' (selected), 'Evidence', 'Artifacts', 'Content types', etc. Below this is a tree view of evidence categories: WEB RELATED (2,172), CHAT (244), MEDIA (359) (which is expanded, showing Pictures (221) circled with red number 1), MOBILE (475), and OPERATING SYSTEM (20). The main area is titled 'EVIDENCE (221)' and shows a table with columns: Image, File Name, File..., Created D... (with a dropdown menu open at row 2661, circled with red number 2, showing 'Column view' selected), and Last modified. A preview of a Kik logo image is shown on the right, with 'ZOOM 100%' below it. At the bottom right, there's 'ARTIFACT INFORMATION' with details: Size (Bytes) 2661, Skin Tone Percentage 0.0, Original Width 160, and Time zone UTC+0:00.

- a. Are there the same number of pictures as from Cellebrite?
- 

- b. What is in **IMG\_0020.jpg**?
- 

- c. When was the photo taken?
- 

#### Bonus Question

- d. What radio station was being listened to at 6/22/2013 2:46:19 PM? At what address? (This will take more than just this picture and its metadata to determine.)
-

**Exercise Questions Step-by-Step**

- Click on the **MOBILE** section to expand it, and then click on **iOS Call Logs**.

The screenshot shows the Magnet AXIOM Examine interface. On the left, there's a sidebar with filters like Evidence, Artifacts, Content types, Date and time, Tags and comments, Profiles, and Partial results. Below that is a list of categories: WEB RELATED (2,172), CHAT (244), MEDIA (359), MOBILE (475), and OPERATING SYSTEM (20). The 'MOBILE' category is highlighted with a red box and a red number '1'. Under 'MOBILE', 'iOS Call Logs' is also highlighted with a red box and a red number '2'. The main pane shows a table titled 'EVIDENCE (41)' with columns for Local User, Partners, Part..., Dire..., Call T..., and Call... . The right pane is titled 'Local User <iPhoneBackup.t...' and shows detailed information for a specific entry, including Local User, Partners, Direction, Call Type, Call Status, Call Date/Time, Call Duration (Seconds), Service Provider Country Code, and Source. The source is listed as 'iPhoneBackup.tar \2b2b0084a1bc3a5ac8c27afdf14a'. At the bottom right of the right pane, it says 'Time zone UTC+0:00'.

- How many calls are in the call log?

41

- Is this the same amount that we saw from Cellebrite?

NO

- If not, why do you think there is a difference?

**Different tools will extract data differently. As well, Cellebrite nests all call logs together, no matter the app that generated them. AXIOM puts them in separate places.**

2. Click on the **CHAT** evidence section to expand it. Explore the various types of chat, their views, and the messages in them. Then click on **Skype Chat Messages**.

The screenshot shows the Magnet AXIOM Examine interface. On the left, there's a sidebar with filters like 'Artifacts' and 'WEB RELATED' (2,172). A red box labeled '1' highlights the 'CHAT' section, which contains 244 items. Another red box labeled '2' highlights the 'Skype Chat Messages' item under CHAT, which has a value of 6. The main pane shows a table titled 'EVIDENCE (6)' with columns for Chat ID, Profile, Authentication, Recipient, and From Disk. To the right, a preview panel shows a conversation between 'hankl1107' and 'hnmc-dc'. The conversation includes messages like 'Hey, How are you?', 'Hank Livingston requested to add hnmc-dc as a contact', and 'Howdy'. The preview panel also shows the time zone as UTC+0:00.

- a. How many different people has **hankl1107** been chatting with?

**Two.**

**Dirtycsez and hnmc-dc**

- b. How many total chat messages are there of all types?

**244**

- c. Is this the same amount as Cellebrite found?

**No**

- d. On 9/6/2013 4:04:38 AM, **hankl1107** was in a Skype chat. What was the public IP address, and where does it trace to?

**Use Skype IP Addresses section under CHAT to find IP address 74.96.90.129 - Verizon account in Washington, DC area.**

**One way to find additional information on an IP address is to use Maxmind.**

<https://www.maxmind.com/en/geoip-demo>

The screenshot shows the MaxMind GeoIP2 City Database Demo page. On the left, there's a sidebar with 'GeoIP2 Precision Services' (Country, City, Insights, Free Trial Account) and 'GeoIP2 Databases' (Country, City, City Database by Continent). The main area has a heading 'GeoIP2 City Database Demo'. It features a large input field labeled 'IP Addresses' containing '74.96.90.129'. A red circle with the number '1' is over the input field, and a red box surrounds it with the text 'Enter IP address(s) you want to locate.' Below the input field is a smaller text box with the placeholder 'Enter up to 25 IP addresses separated by spaces or commas. You can also test your own IP address.' At the bottom of the input field is a blue 'Submit' button with a red circle containing the number '2' next to it, followed by the text 'Click "Submit"'.

You should get these results from Maxmind or similar tool.

The screenshot shows a table titled 'GeoIP2 City Results' with one row of data. The columns are: IP Address, Country Code, Location, Postal Code, Approximate Coordinates\*, Accuracy Radius, ISP, Organization, and Domain. The 'Location' and 'ISP/Organization' columns are highlighted with red boxes. The data in the table is:

IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius	ISP	Organization	Domain
74.96.90.129	US	Annandale, Virginia, United States, North America	22003	38.8307, -77.2142	5	Verizon Fios	Verizon Fios	verizo

3. Ensure your view is showing **Column view**, so you can see the **EVIDENCE** list on the left of the **AXIOM Examine** window. Expand the **MEDIA** section and click on **Pictures**.

The screenshot shows the Magnet AXIOM Examine interface. On the left, there's a sidebar with filters for Artifacts, Evidence, Artifacts, Content types, Date and time, Tags and comments, Profiles, and Partial results. A search bar at the top right has 'GO' and 'ADVANCED' buttons. The main area is titled 'EVIDENCE (221)'.

**Step 1:** The 'MEDIA' section is expanded, showing categories like Pictures (221), Videos (2), and others. The 'Pictures' item is highlighted with a red circle and a red box.

**Step 2:** A context menu is open over the evidence list, with 'Column view' highlighted with a red box and a red circle.

**Step 3:** The 'Column view' option is selected from the menu, indicated by a red circle.

The evidence list shows several items, including 'LockBackgroundThumbnail.jpg' (File Name), '9/23/2013 12:39:46 PM' (Created Date), and '2661' (Size). To the right, there's a preview of a Kik logo image and details about the artifact.

- a. Note: You may find it easier to view the photo thumbnails by switching to the “Row View”.

Are there the same number of pictures as from Cellebrite?

NO

- b. What is in **IMG\_0020.jpg**?

A Dog

- c. When was the photo taken?

**7/8/2013 11:21:24 AM UTC**

### Bonus Question

- d. What radio station was being listened to at 6/22/2013 2:46:19 PM? At what address? (This will take more than just this picture and its metadata to determine.)

**94.7 FM**

**306 Branch Road SE, Vienna, Virginia**

First let's find the radio station...

Find a photo with the above date and time (6/22/2013 2:46:19 PM) and click to highlight it.

The screenshot shows the Magnet AXIOM Examine interface. On the left, there is a sidebar with filters and a list of evidence categories. The main area displays a list of evidence items. A yellow callout box highlights the entry for 'IMG\_0012.JPG' with the instructions: 'Find and highlight picture... ...then double click on it.' A red arrow points from this callout to the thumbnail of the highlighted item. To the right, a preview window shows a close-up of a car's instrument cluster. The details panel on the right provides artifact information for the selected item, including file name, extension, creation date, and time.

ALL EVIDENCE 3,535	
<b>REFINED RESULTS 265</b>	
Classified URLs	12
Cloud Services URLs	8
Facebook URLs	8
Google Searches	84
Identifiers	145
Parsed Search Queries	2
Shipping Site URLs	4
Social Media URLs	2
<b>WEB RELATED 2,172</b>	
<b>CHAT 244</b>	
<b>MEDIA 359</b>	
AMR Files	4
Audio	132
<b>Pictures</b>	<b>221</b>
Videos	2
<b>MOBILE 475</b>	

**EVIDENCE (221)**

**IMG\_0012.JPG**

PICTURES — Media  
File Extension : JPG  
Created Date/Time : 6/22/2013 2:46:19 PM

**IMG\_0013.JPG**

PICTURES — Media  
File Extension : JPG  
Created Date/Time : 6/22/2013 2:46:25 PM

**IMG\_0014.JPG**

PICTURES — Media  
File Extension : JPG  
Created Date/Time : 6/22/2013 2:46:38 PM

**IMG\_0015.JPG**

PICTURES — Media  
File Extension : JPG  
Created Date/Time : 6/22/2013 2:47:12 PM

**IMG\_0017.JPG**

PICTURES — Media  
File Extension : JPG  
Created Date/Time : 7/8/2013 11:18:31 AM

**PREVIEW**

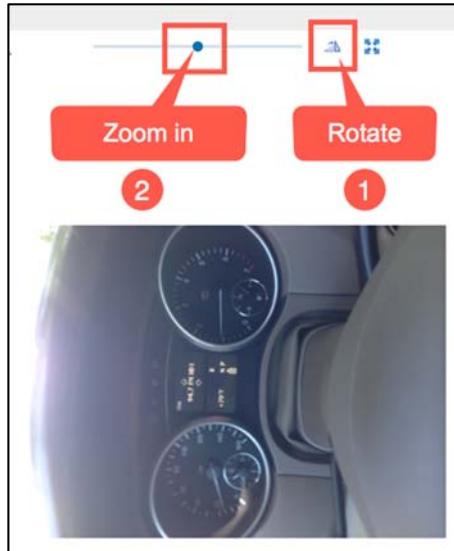
ZOOM 7%

**DETAILS**

**ARTIFACT INFORMATION**

File Name: **IMG\_0012.JPG**  
File Extension: **JPG**  
Created Date/Time: **6/22/2013 2:46:19 PM**  
Last Accessed Date/Time: **6/22/2013 2:46:19 PM**  
Time zone: **UTC+0:00**

Once the thumbnail is highlighted, you will see a larger version of the photo in the Preview section on the right side of the screen. Double click to open it in a new window.



**Rotate the image so it is upright, and then zoom in enough to read the radio station from the dashboard screen.**



**Now for the address...**

**Remember that the photo of the car dashboard was IMG\_0012.JPG. If you look at IMG\_0013.JPG, you will see that it was taken 6 seconds after the dashboard photo. In other words, the radio station was probably being listened to when this second photo was taken. Highlight that photo.**

**For this part of the exercise, switch to World map view.**

This screenshot shows the Magnet AXIOM Examine interface. On the left, there's a sidebar with filters and a list of evidence types. The main area displays a list of evidence items. A red arrow labeled '1' points to the 'Row view' button in a context menu that appears over the list. Another red arrow labeled '2' points to the 'World map view' button in the same context menu. To the right, there's a preview pane showing a photo of a guitar and a details panel.

If the map is taking up the whole screen, click on the DETAILS tab on the right edge of the screen.

This screenshot shows the Magnet AXIOM Examine interface with a world map view. A red arrow points to the 'DETAILS' tab on the right side of the screen. The map shows various locations with markers, and a specific location in the United States is highlighted with a yellow marker. The sidebar on the left shows matching results for media, with 'Pictures' selected.

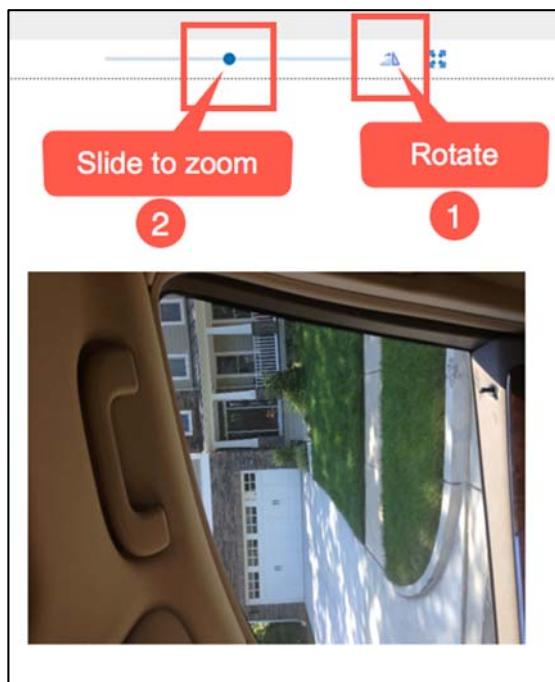
You should end up seeing something like the screenshot below. Double click on the larger photo in the preview pane. It will open in its own window.

The screenshot shows the Magnet AXIOM Examine interface. On the left, a sidebar displays 'MATCHING RESULTS' (31) and 'MEDIA' (31), with 'Pictures' selected. The main area shows 'MATCHING RESULTS (29 of 221)' with a map of North America and a highlighted location in the United States. Below the map is a list of three images:

- IMG\_0008.JPG**: PICTURES — Media, File Extension: JPG, Created Date/Time: 6/20/2013 8:20:53 PM
- IMG\_0012.JPG**: PICTURES — Media, File Extension: JPG, Created Date/Time: 6/22/2013 2:46:19 PM
- IMG\_0013.JPG**: PICTURES — Media, File Extension: JPG, Created Date/Time: 6/22/2013 2:46:25 PM

At the bottom of the list are options: CREATE REPORT / EXPORT, SAVE ARTIFACT TO..., and OPEN SOURCE FILE WITH... A yellow callout box points to the image preview area on the right, which shows a photo of a house through a window. The callout text says: "Double click to expand photo for zoom and rotation." The preview area also includes a 'PREVIEW' section with a thumbnail, a 'ZOOM 7%' button, and a 'DETAILS' section with file information.

Using the icons at the top of the window, rotate the photo so it is right side up.



Using the zoom function, zoom in and you can see the house number of 306.



**Close the window, go back to the listings, and double click on the thumbnail in the list.**

Screenshot of Magnet AXIOM Examine software interface showing matching results for media files.

**MATCHING RESULTS (29 of 221)**

**Double click** on the thumbnail of **IMG\_0013.JPG**.

File Name	Type	Created Date/Time
IMG_0008.JPG	PICTURES — Media	6/20/2013 8:20:53 PM
IMG_0012.JPG	PICTURES — Media	6/22/2013 2:46:19 PM
<b>IMG_0013.JPG</b>	<b>PICTURES — Media</b>	<b>6/22/2013 2:46:25 PM</b>

**PREVIEW** shows a thumbnail of the image file.

**DETAILS** and **ARTIFACT INFORMATION** panels are visible on the right.

**A Google map view will appear with a pin dot and a street. You can see that it is Branch Road SE, but you don't really know where in the world that street is.**

**MATCHING RESULTS (29 of 221)**

**Pin showing location photo was taken**

**Street name**

**IMG\_0013.JPG**  
iPhoneBackup.tar

**PREVIEW**

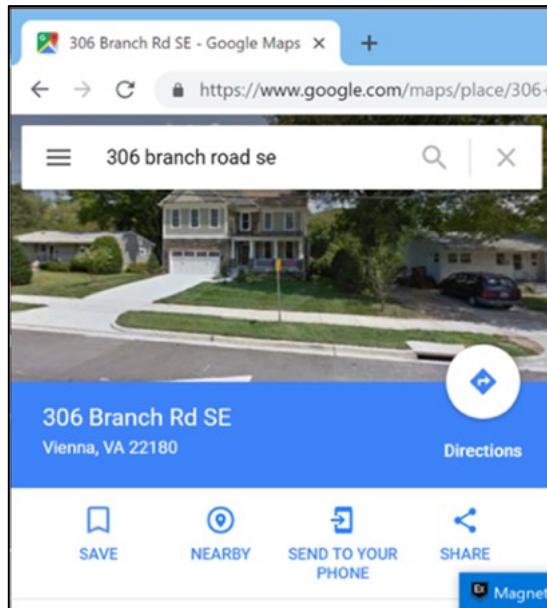
**DETAILS**

**ARTIFACT INFORMATION**

File Name: **IMG\_0013.JP**

Time zone: UTC+0:00

Open up a browser and go to [googlemaps.com](http://googlemaps.com). In the search bar, enter 306 Branch Road SE. It will show you anywhere that has an address like this. In this case, there is only one. It is in Vienna Virginia. Clicking on that Vienna, Virginia choice show you a picture of the house, which matches the one from your investigation.



### Exercise—Key Takeaways

- There are many “quick wins” in the easily available data from a portable device.

- You cannot take the results from one tool for granted. Different tools present data in different ways, and often show different results.
- You must be able to explain what you see and give reasons why.
- Vendors pack more and more features into their software every day. Software that looks easy and intuitive could have many intricate surprises, and you must become familiar with them.

# © SANS Institute 2020

## Exercise 2.3—Hard Drive Wiping & Formatting

### Exercise Objectives

- Learn process for wiping a hard drive using Windows tools
- Learn process for formatting a hard drive using Windows tools

### Exercise – Part 1

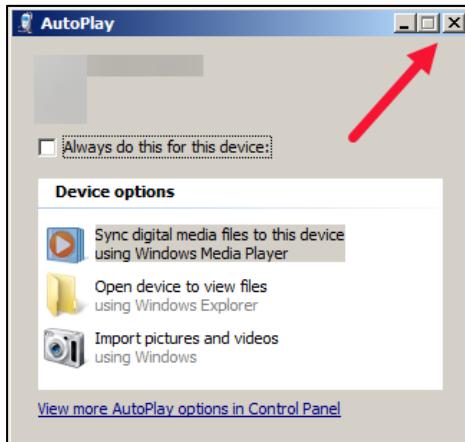
1. Boot your **FOR498 Windows VM**
2. Login to the **FOR498 Windows VM** using the following credentials:
  - a. Username: **SANSDFIR**
  - b. Password: **forensics**
3. Ensure your **FOR498 Windows VM** is in full screen mode. If it is not, you may have connection issues when plugging a device in for analysis with the VM. The following screenshots refer to the use of **VMware Workstation** and **VMware Player**. For **VMware Fusion** users, jump to **step 10**.



4. Using the student provided hard drive you brought to class with you and the SANS provided SATA to USB adapter, make the necessary connections and plug it into an available USB port of your computer.

**NOTE:** In cases where your VM will not allow for external device connection, insert your supplied USB 2.0 hub, and connect through this.

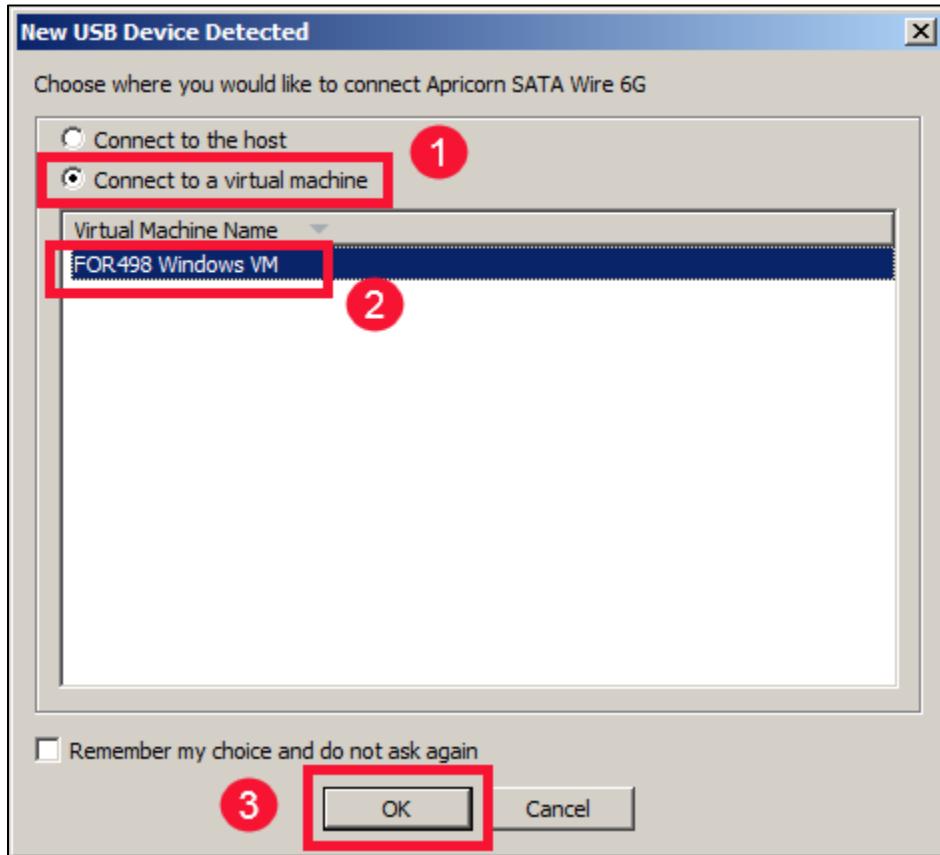
5. If **AutoPlay** presents a screen, simply close it.



6. Ignore any reference to device names in the screenshots to follow, as they may not match yours. When you plug your device in, you will see either the window in **OPTION 1** below, or one of the two windows in **OPTION 2** below. Follow the instructions for your **OPTION** accordingly.

### OPTION 1

Once completed, go to **step 14** of this exercise.

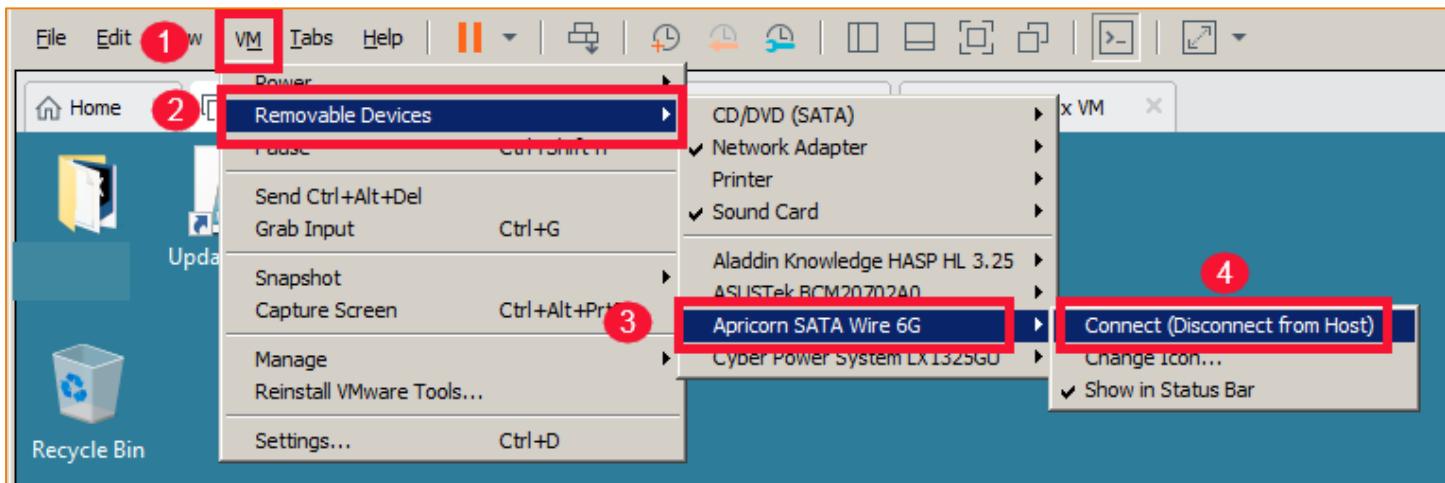


### OPTION TWO

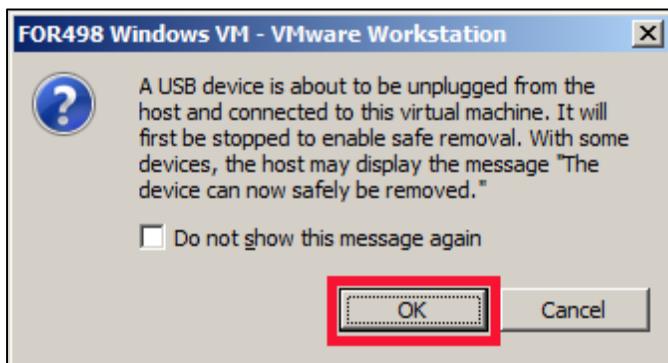
(You should only see the screens below if you took too long to respond to the screen above. If you see **screen 1**, proceed to **Step 14** of this exercise. If you see **screen 2**, proceed to the next step.)

SCREEN 1	SCREEN 2
<p><b>Removable Devices</b></p> <p>The following devices can be connected to this virtual machine using the status bar or choosing VM &gt; Removable Devices:</p> <p><input checked="" type="checkbox"/> Apricorn SATA Wire 6G (connected to Windows )</p> <p>Each device can be connected either to the host or to one virtual machine at a time.</p> <p><input type="checkbox"/> Do not show this hint again</p> <p style="text-align: center;"><b>OK</b></p>	<p><b>Removable Devices</b></p> <p>The following devices can be connected to this virtual machine using the status bar or choosing VM &gt; Removable Devices:</p> <p><input checked="" type="checkbox"/> Apricorn SATA Wire 6G</p> <p>Each device can be connected either to the host or to one virtual machine at a time.</p> <p><input type="checkbox"/> Do not show this hint again</p> <p style="text-align: right;"><b>OK</b></p>

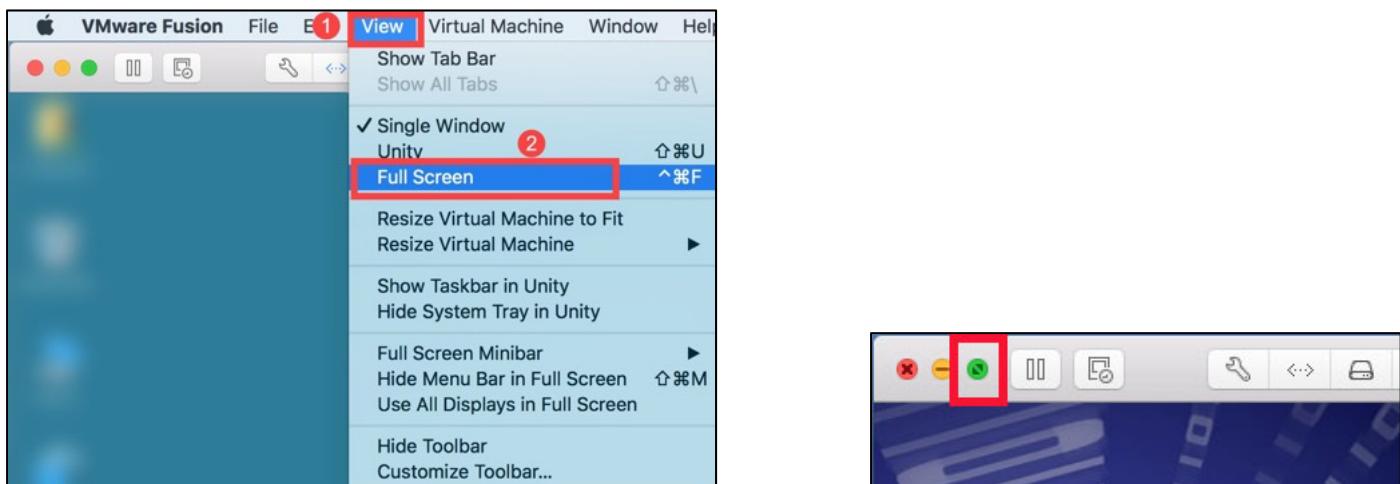
7. In the case of **screen 2**, the device has been ‘captured’ by the host computer rather than the VM, so you must tell the VM to take control of the device. Within the VM, click on **VM -> Removable Devices -> [your device name] -> Connect (Disconnect from the Host)**.



8. You may receive a pop-up confirmation. Click **OK**. Proceed to **Section 2** of this exercise.



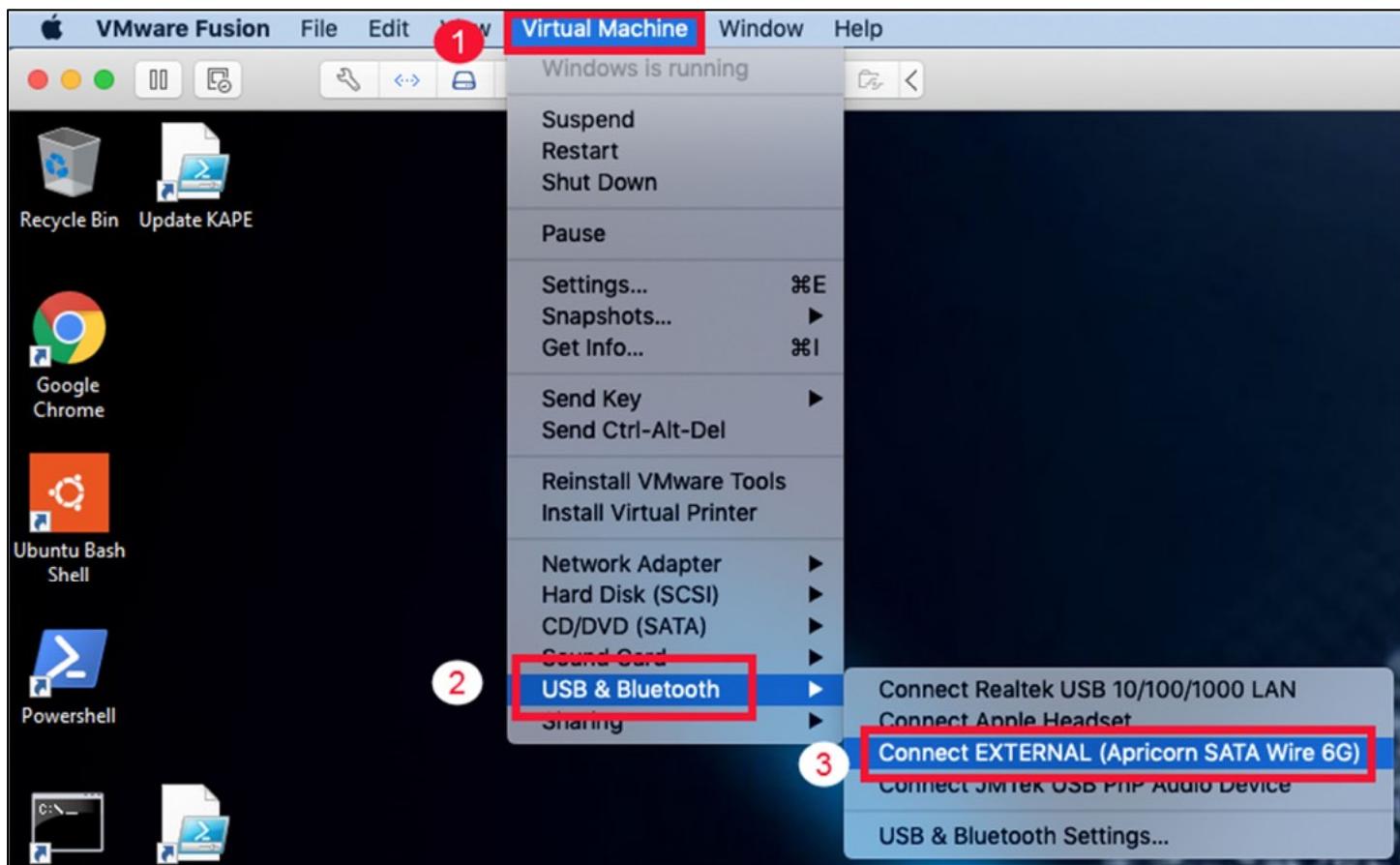
9. For **VMWare Fusion** users, ensure your **FOR498 Windows VM** is in full screen mode. If it is not, you may have connection issues when plugging a device in for analysis with the **VM**. You can choose either of the two methods below.



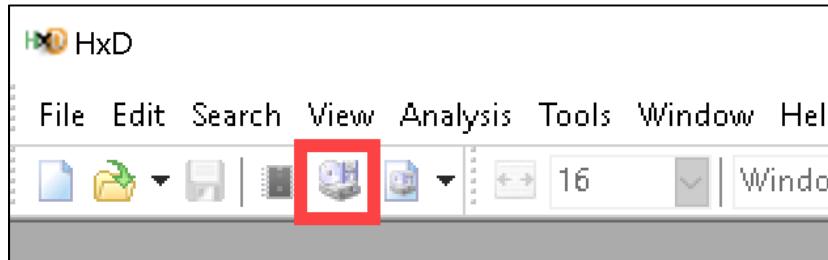
10. Using the student provided hard drive you brought to class with you and the SANS provided SATA to USB adapter, make the necessary connections and plug it into an available USB port of your computer.
11. When you plug your device in, a box will appear asking where you want your device to connect. Select **Connect to Windows**, to connect the device to your **FOR498 Windows VM**.



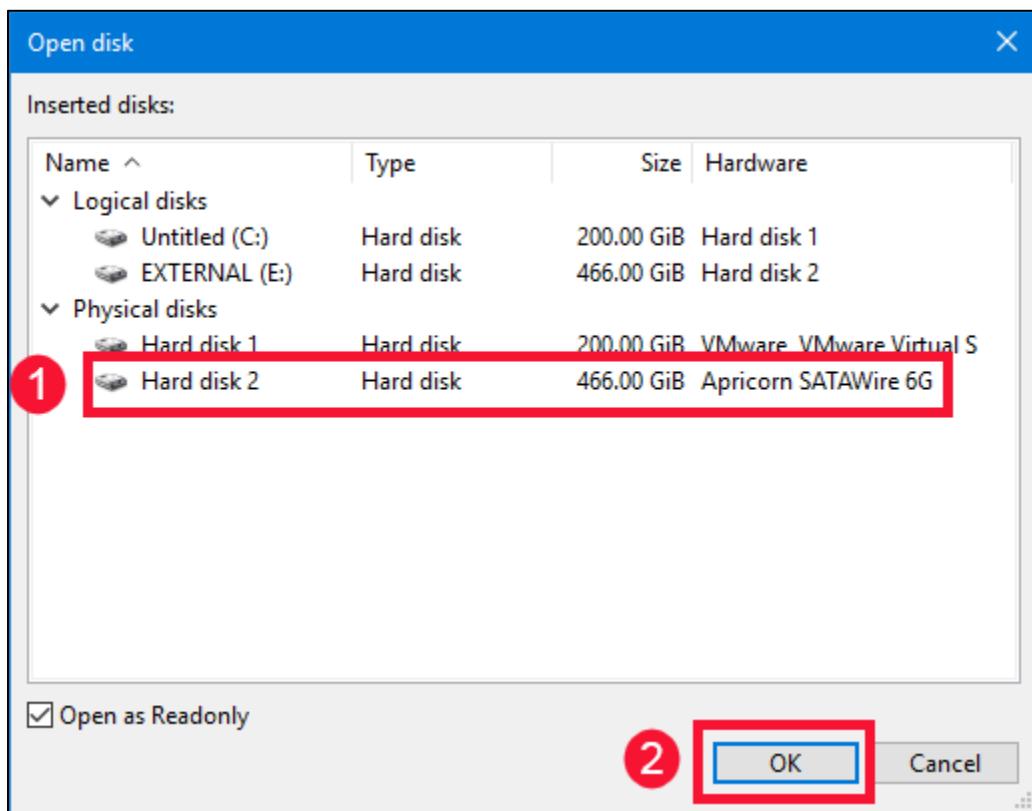
12. If you do not see the previous pop up when attaching the device to the VM, you need to attach it manually. Within the VM, click on **Virtual Machine** -> **USB & Bluetooth** -> **Connect [your device name]**.



13. If you receive any confirmation prompts, read them carefully before accepting them (or not), and understand what they are asking for.
14. Locate and start the **HxD** program by double clicking the icon in the **Utilities** fence on the Desktop.
15. Once the program is open, locate the **Open disk** icon and click on it.



16. A window will open showing you the available drives that **HxD** can see. Select the USB drive you plugged in. In my case it was **Hard disk 2**. Yours may be different. Then click **OK**.



17. Once the **HxD** hexadecimal window opens, it will show you the contents of your hard drive. If you brought a wiped drive, you will see nothing but zeros. Otherwise, you should at least see some partition information showing that the drive was not completely wiped. In the case that you can see data, when we perform this function again, you will see that your wiping was effective.

```

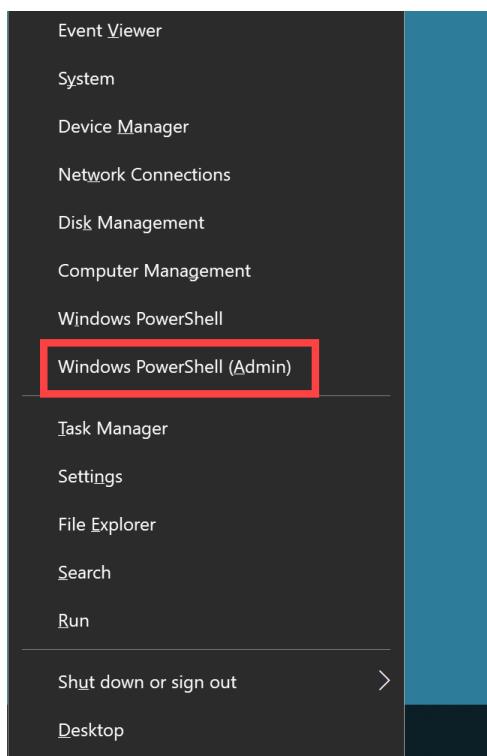
00000000120 61 68 00 00 07 CD 1A 5A 32 F6 EA 00 7C 00 00 CD ah...í.z2ðè.|..í
00000000130 18 A0 B7 07 EB 08 A0 B6 07 EB 03 A0 B5 07 32 E4 . ..ë. ¶.ë. µ.2ë
00000000140 05 00 07 8B F0 AC 3C 00 74 09 BB 07 00 B4 0E CD ...<.t.»..'.í
00000000150 10 EB F2 F4 EB FD 2B C9 E4 64 EB 00 24 02 EO F8 .ëððëý+Éädë.$.àø
00000000160 24 02 C3 49 6E 76 61 6C 69 64 20 70 61 72 74 69 $.ÃInvalid parti
00000000170 74 69 6F 6E 20 74 61 62 6C 65 00 45 72 72 6F 72 tion table.Error
00000000180 20 6C 6F 61 64 69 6E 67 20 6F 70 65 72 61 74 69 loading operati
00000000190 6E 67 20 73 79 73 74 65 6D 00 4D 69 73 73 69 6E ng system.Missin
000000001A0 67 20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74 g operating syst
000000001B0 65 6D 00 00 00 63 7B 9A 51 11 D6 D2 00 00 00 20 em...c{šQ.Öò...
000000001C0 21 00 07 FE FF FF 00 08 00 00 00 48 38 3A 00 00 !..þý.....H8:..
000000001D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
000000001E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
000000001F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA .....U*
00000000200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00000000210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00000000220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00000000230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00000000240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .

```

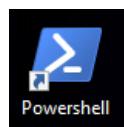
Sector 1

18. Close out of the **HxD** program. We will now proceed to wiping the external hard drive.

19. Right click on the **Start** menu and select **Windows PowerShell (Admin)**.



Alternatively, you can double click the **Powershell** icon on the **desktop**.



20. Ensure you are an administrator via the **PowerShell** window's title bar (it should start with **Administrator**). Type **diskpart** and press **Enter**. The program will open.

```
PS C:\WINDOWS\system32> diskpart
Microsoft DiskPart version 10.0.17763.1
Copyright (C) Microsoft Corporation.
On computer: SANS-FOR498-SIF

DISKPART>
```

21. At the **DISKPART** prompt, type **list disk** and press **Enter**. Make note of the Disk # for the USB disk you just connected.

```
DISKPART> list disk

Disk ###  Status     Size      Free      Dyn  Gpt
-----  -----  -----
Disk 0    Online    160 GB    0 B      *    
Disk 1    Online    58 GB     0 B
```

22. Type **select Disk {#}** and press **Enter**. Ensure that the **{#}** reflects the correct Disk number, or you will be having a long evening rebuilding a drive!

```
DISKPART> select Disk 1

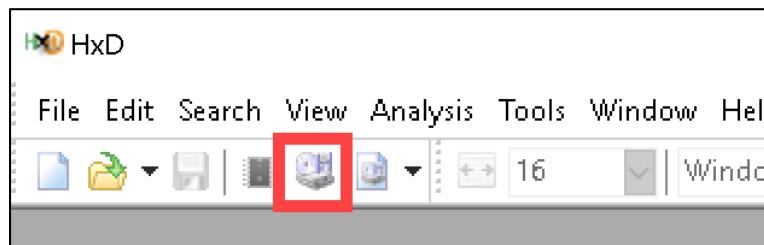
Disk 1 is now the selected disk.
```

23. Type **clean all** and press **Enter**. If you were planning on wiping the whole disk, this function could take hours. At this time, you do not see a command prompt. You simply see your cursor blinking on the line below.

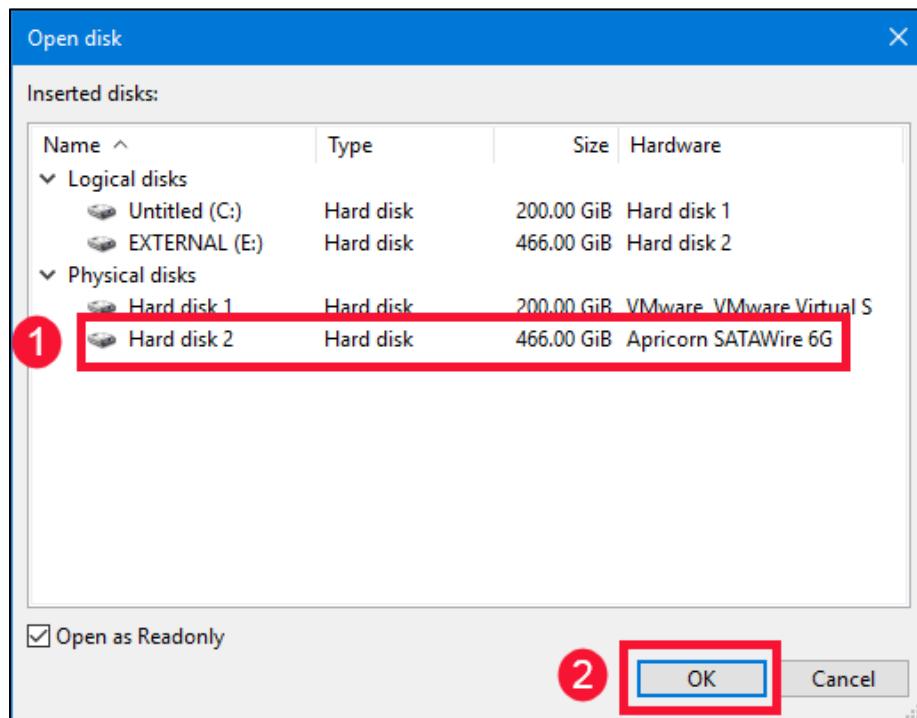
```
DISKPART> clean all
```

24. For the purpose of this exercise, allow about 2-3 minutes to go by and then close the **PowerShell** window. You cannot stop the **clean all** process. It will continue to run on the drive, because the instruction has been passed to the hard drive itself. Even though the **clean all** process is still running, you can continue with the next steps. We will address the continued wiping in the next section of this exercise. Most importantly, **DO NOT DISCONNECT YOUR EXTERNAL DRIVE RIGHT NOW!**
25. Let's now verify that wiping has occurred. Open **HxD** program by double clicking the icon in the **Utilities** fence on the **Desktop**.

26. Once the program is open, locate the **Open disk** icon and click on it.



27. Select your **Physical disk** again and click **OK**.



28. Once the **HxD** hexadecimal window opens, if everything worked as planned, everything should be zeros, and you should not see any of the data that you saw previously.

00000000170	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000000180	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000000190	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
000000001A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
000000001B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
000000001C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
000000001D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
000000001E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
000000001F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000000200	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000000210	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000000220	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000000230	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000000240	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000000250	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000000260	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000000270	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000000280	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000000290	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

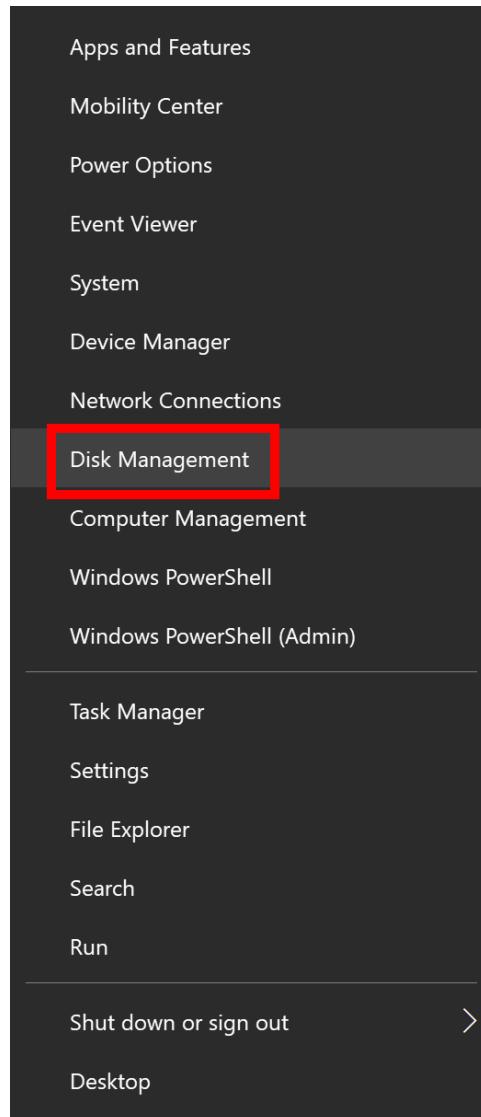
Sector 1

29. You can close any open windows and programs, but do not disconnect your external hard drive. You will need it for the next part of this exercise.

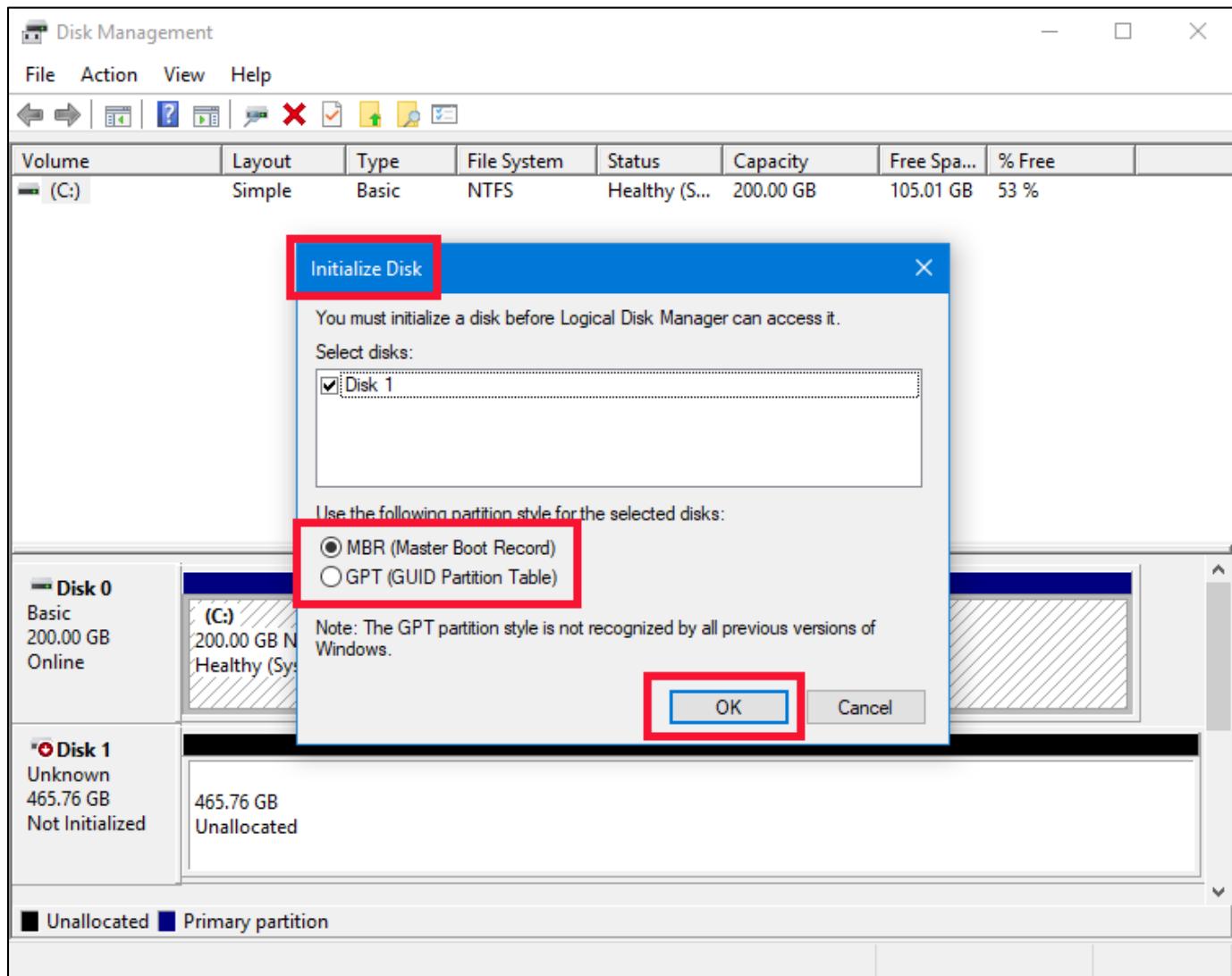
**Exercise – Part 2**

This part of the exercise deals with formatting a hard drive to prepare it for use. It is assumed that your external hard drive is still plugged in to your **VM** from the previous section.

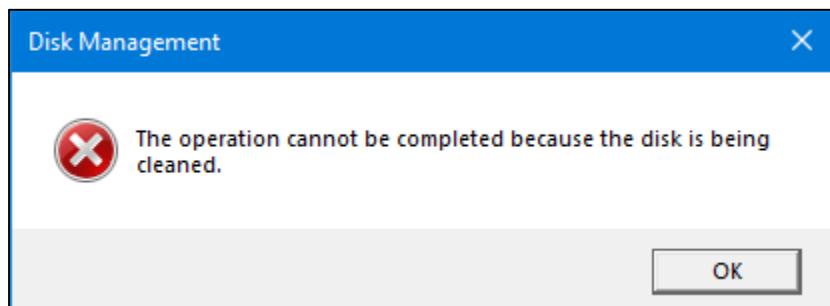
1. Right click on the **Start** button and select **Disk Management** from the menu.



2. The **Disk Management** utility will open. As well, an **Initialize Disk** window will open over top of it. Note that the message on the **Initialize Disk** window says that, “**You must initialize a disk before Logical Disk Manager can access it.**” Back to that in a moment. You will also be asked to select a partition style, and your choices are **MBR (Master Boot Record)**, or **GPT (GUID Partition Table)**. In most cases, and especially if your drive is 2 TB or less in size, you will select **MBR (Master Boot Record)**. If the drive you are working with is larger than 2 TB and you want it to have a single partition for the entire drive, you **MUST** use **GPT (GUID Partition Table)**. Once done, click **OK**.

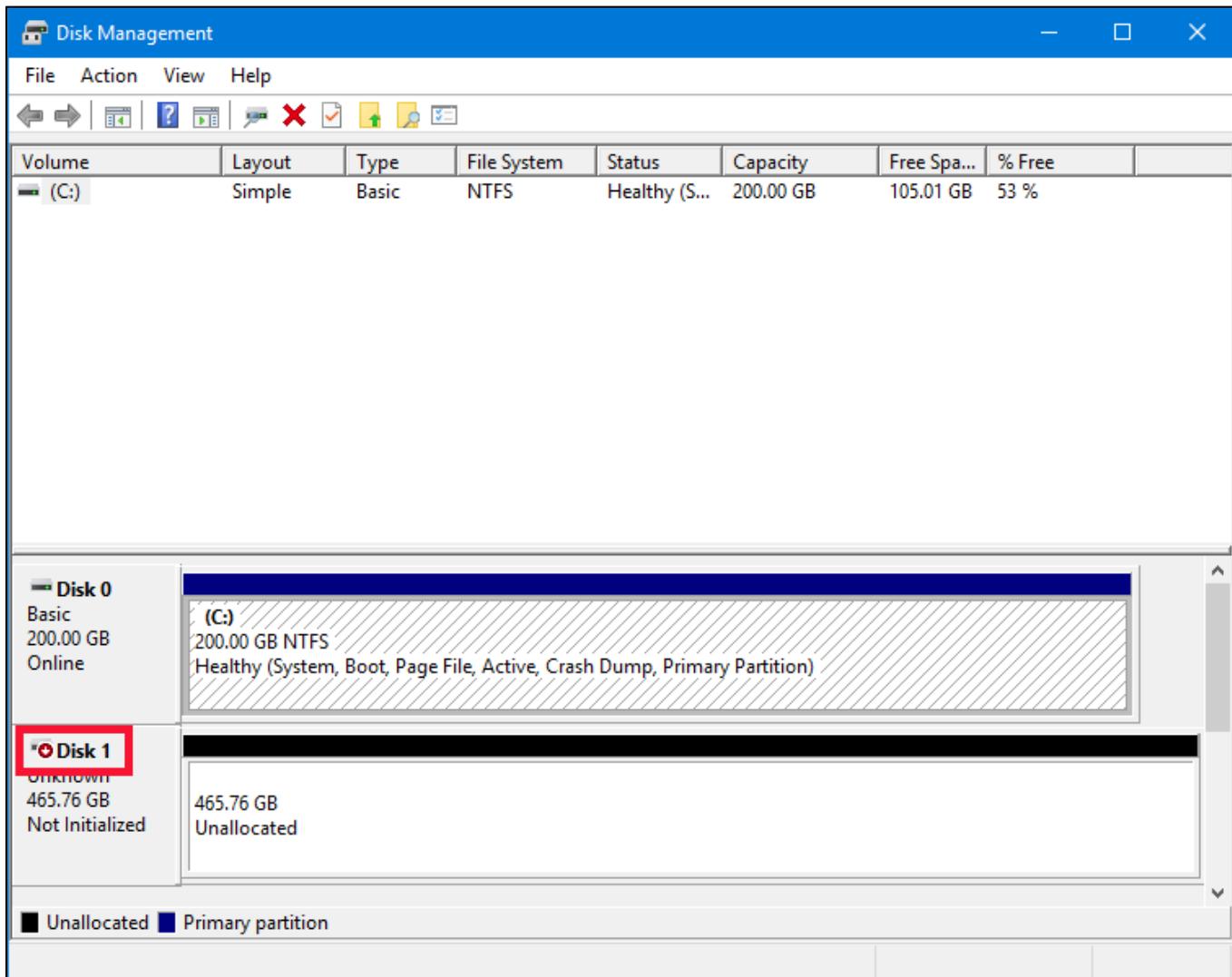


3. Once you click **OK** in the previous step, you may get an error message as seen below.

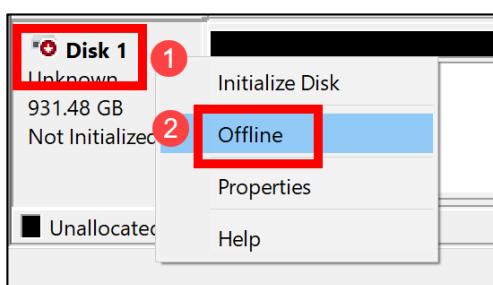


This is because, as mentioned previously, the **clean all** function is still running. We must stop this function before we can proceed. Remember we are only doing this for the exercise. Normally if you are wiping a drive, you are waiting for it to finish properly before trying to format it again. Simply click **OK**, and the error message (as well as the **Initialize Disk** window) will disappear.

4. Looking at the disk listings of the **Disk Management** window, you see the physical disks listed, and in this case, **Disk 1** (yours may have a different number) has a down arrow inside a red circle. This is because the disk is not initialized.



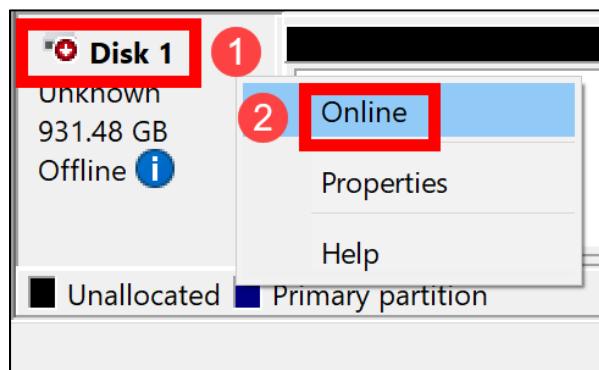
5. Right click on **Disk 1** and select **Offline**.



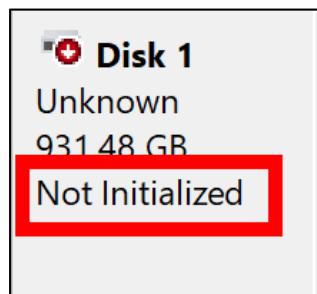
6. Note now that the **Disk 1** box shows the drive as being **Offline**.



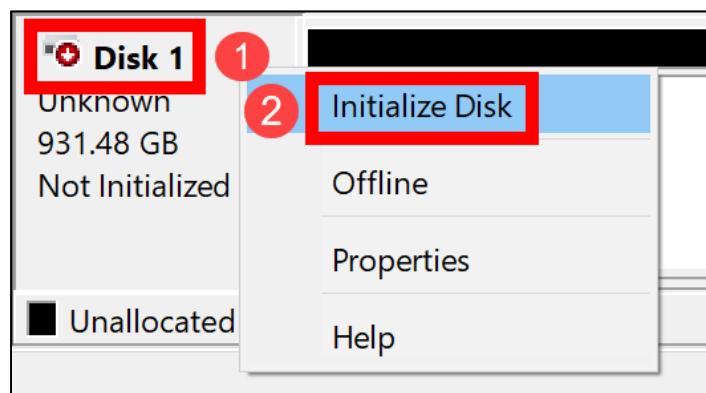
7. Right click on **Disk 1** again, and this time, select **Online**.



8. The status of **Disk 1** should now change to **Not Initialized** again.



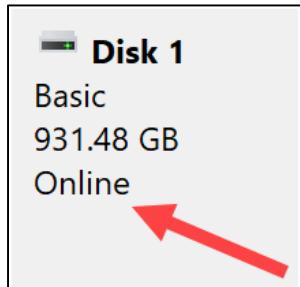
9. Right click on **Disk 1** yet again, but this time select **Initialize Disk**.



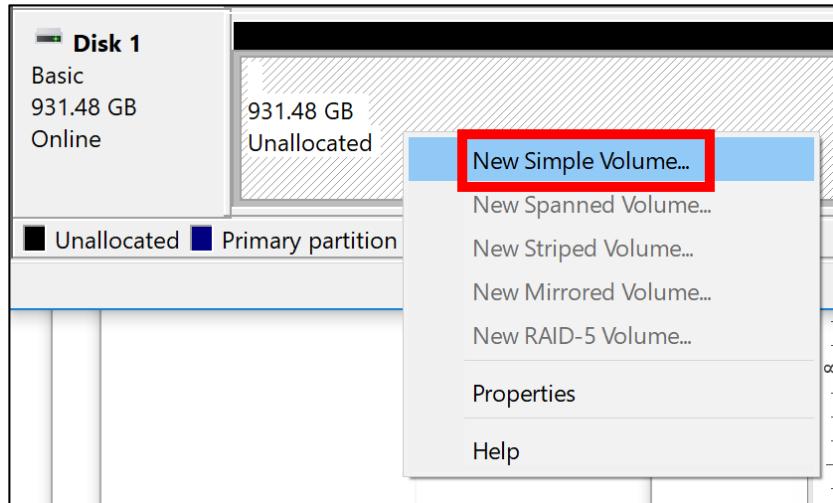
10. Upon clicking, the **Initialize Disk** window will open again. Select **MBR (Master Boot Record)** if your external drive is 2 TB or smaller, otherwise select **GPT (GUID Partition Table)**. Then click **OK**.



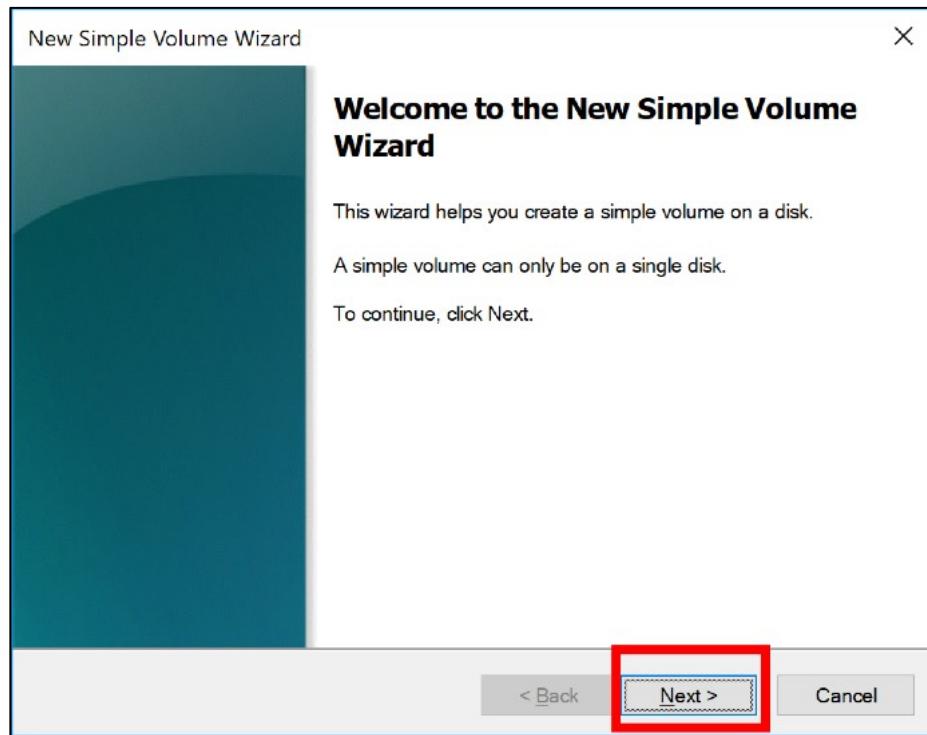
11. You should see the status of **Disk 1** as **Online**.



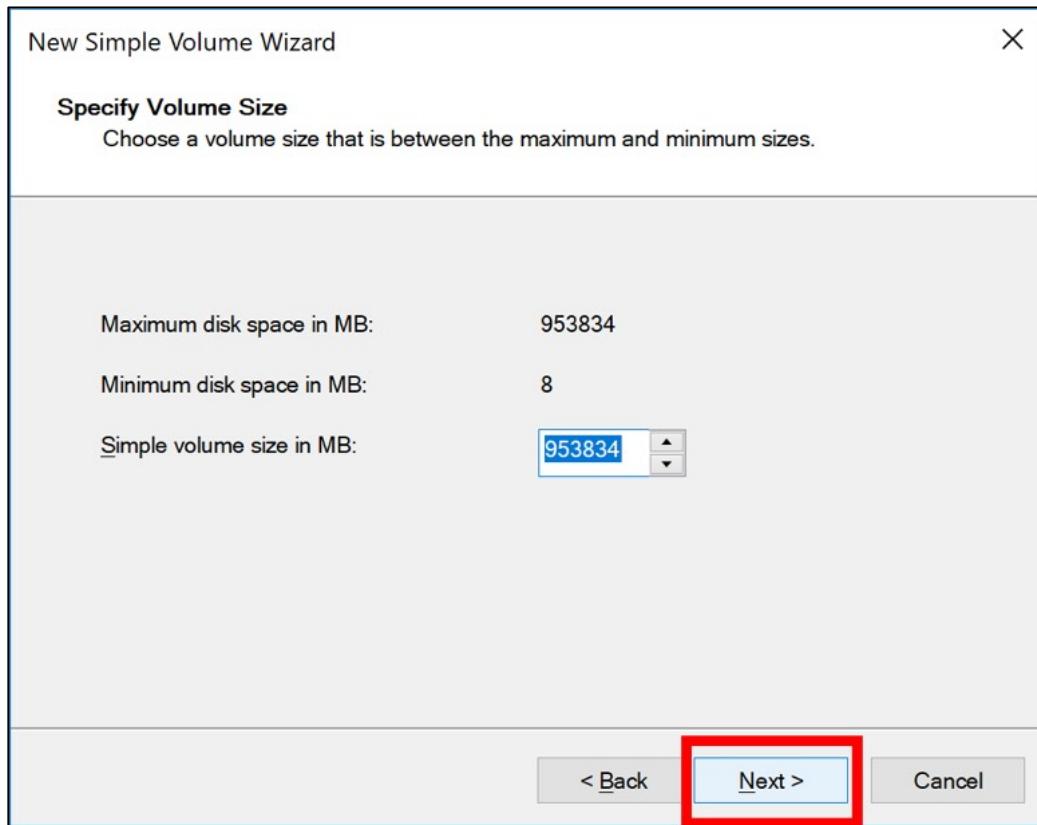
12. It is now time to format the disk. Right click anywhere in the **Unallocated** space of **Disk 1** and select **New Simple Volume**.



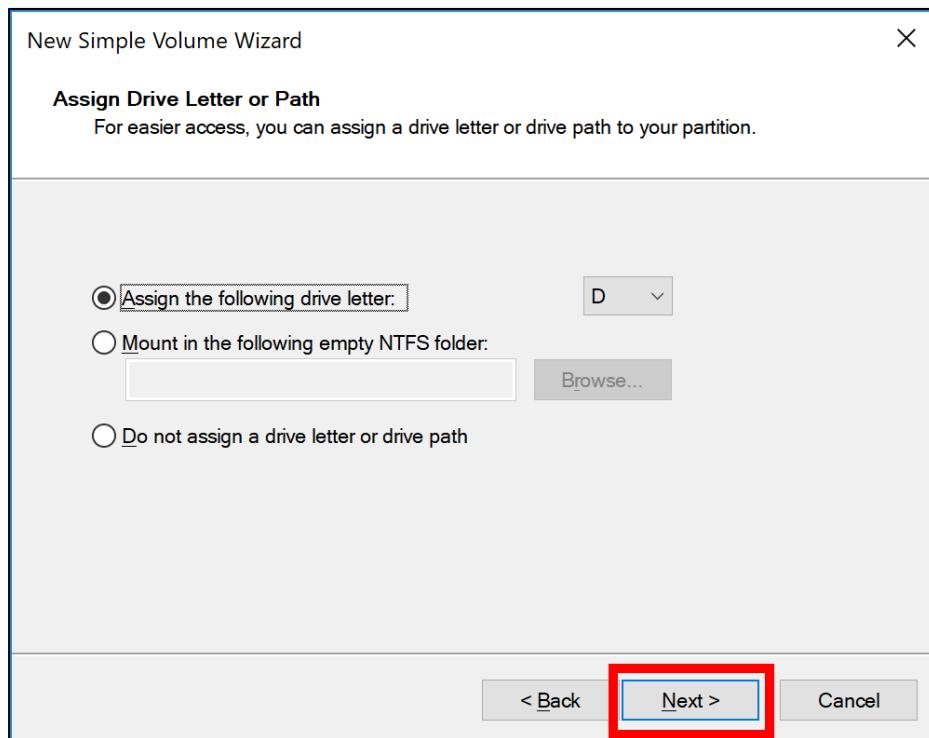
13. The New Simple Volume Wizard will open. Click **Next**.



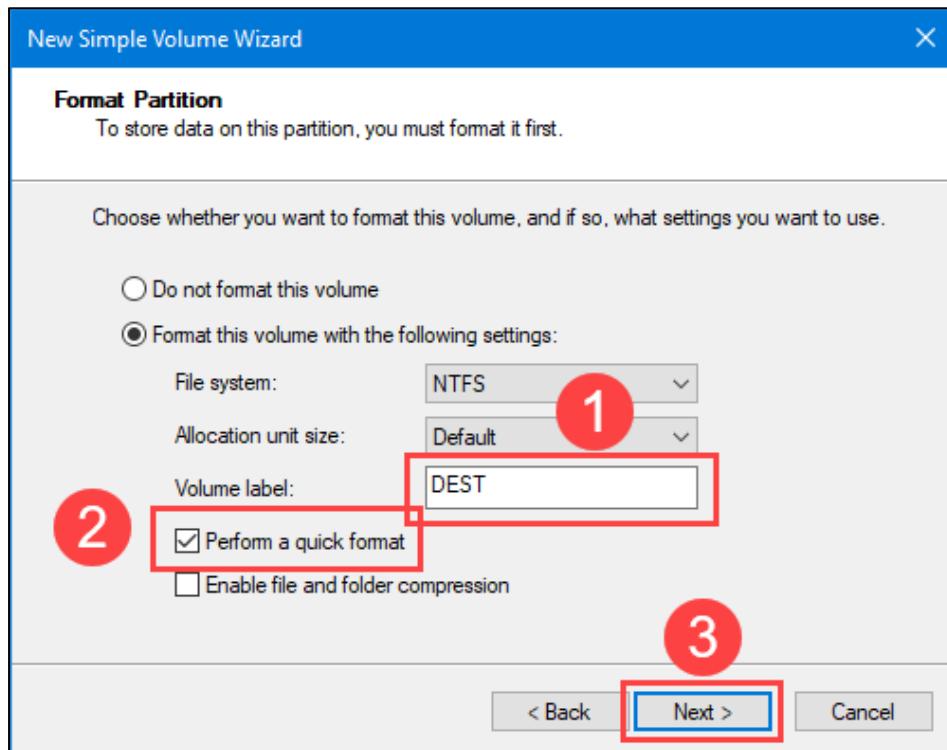
14. Specify the volume size. By default, the full size of the drive is selected. We will leave it that way and click **Next**.



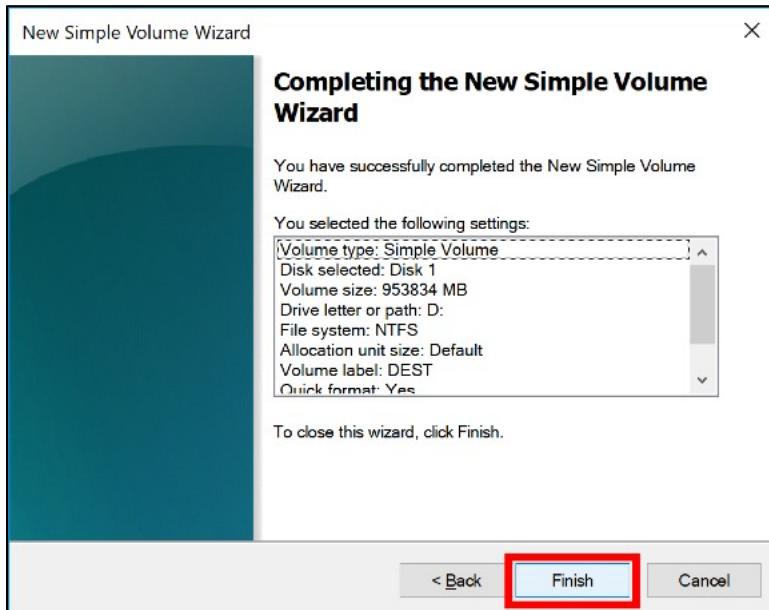
15. The next window allows us to select a drive letter. We will allow the wizard to assign one for us. Accept the default and click **Next**.



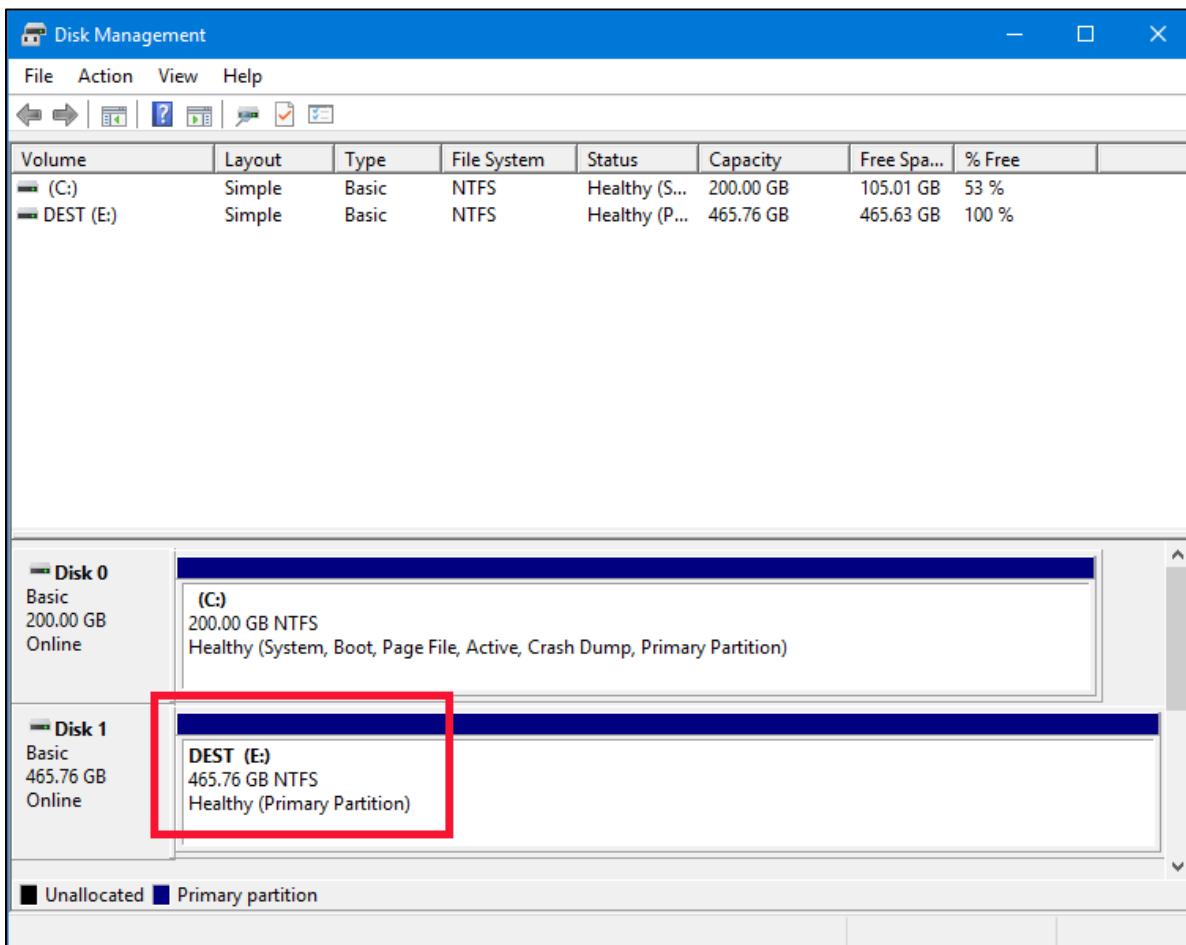
16. It is now time to select the final settings, as well as the volume label. We will leave the **File system** as the default **NTFS**, and we will not change the **Allocation unit size**. We will change the **Volume label** to **DEST**. Ensure that the **Perform a quick format** box is checked, and then click **Next**.



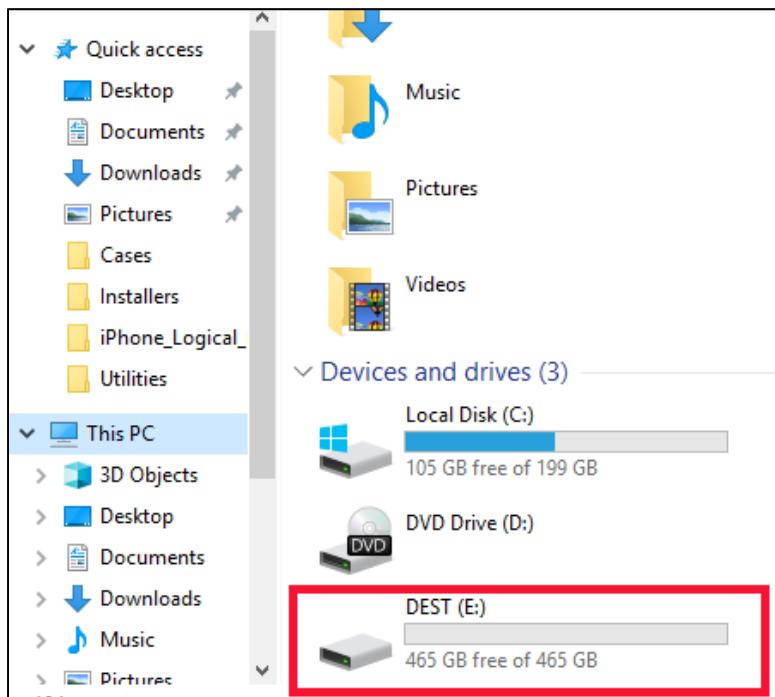
17. A window will show you a summary of your choices. Click **Finish**.



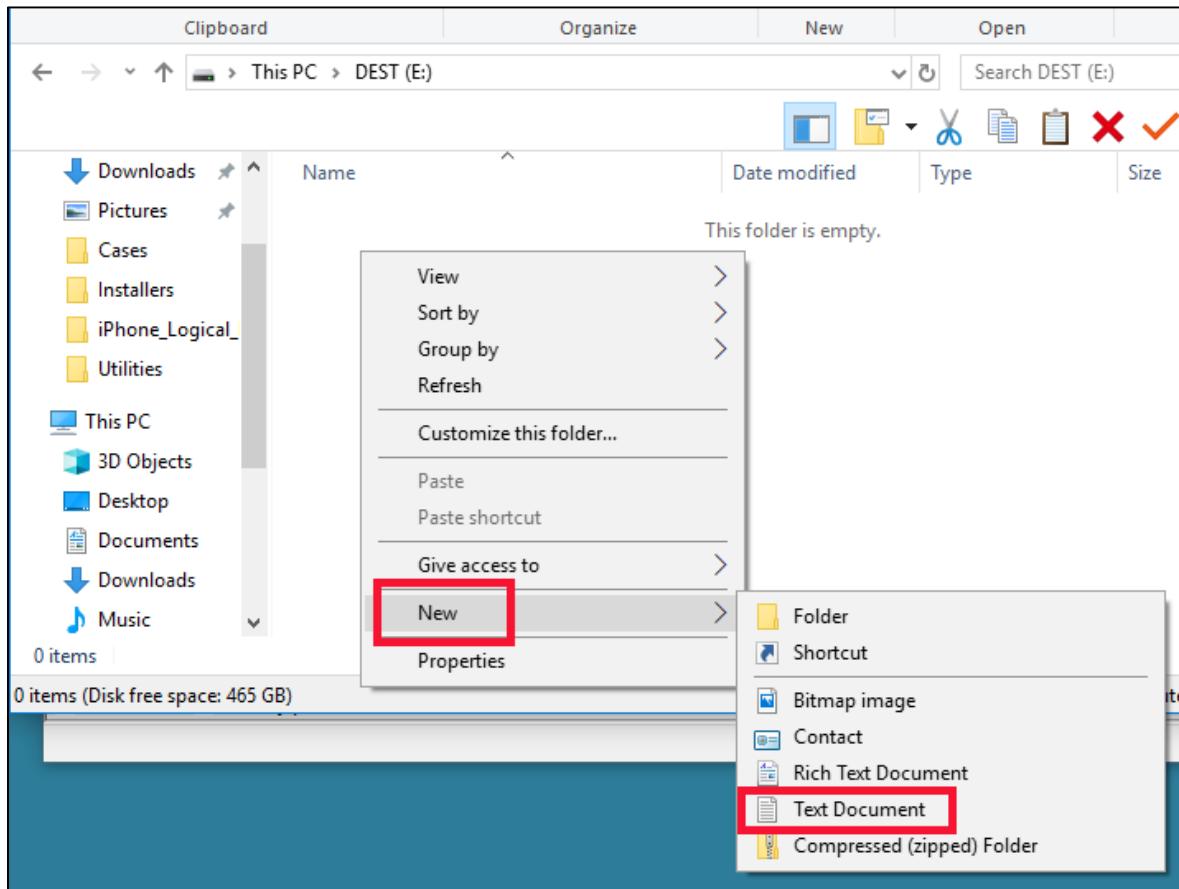
18. Back at the **Disk Management** window, after a few seconds we should see our new partition listed with its drive letter, file system, and status of the partition. In this case, **Healthy (Primary Partition)**. You can now close the **Disk Management** window.



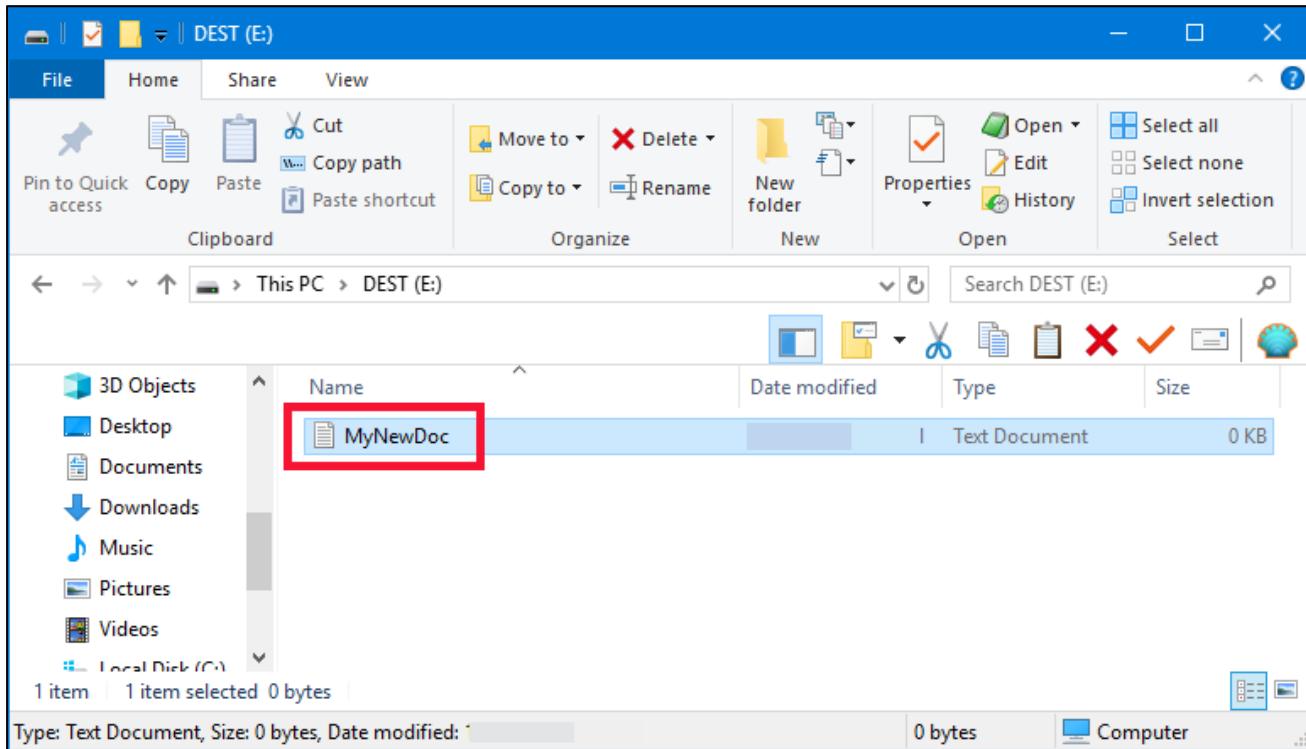
19. You can open a **File Explorer** window and note that the new volume is there, and ready to be used.



20. Let's create our first file on the newly formatted hard drive. Open the drive up and right click anywhere inside the drive. Select **New**, then **Text Document**.



21. Give the file a name of **MyNewDoc** and press **Enter**.



22. Close all open windows, eject your external device, and disconnect it.

#### Exercise—Key Takeaways

- There is no need for third party tools to forensically wipe a hard drive. The diskpart utility is built into every Windows operating system.
- There is a significant difference between formatting a hard drive and wiping it.
- Don't automatically trust that your software is performing a wipe. Verify, verify, verify.

## Exercise 2.4—Write Blocking Methodologies

### Exercise Objectives

- Set up write blocking using a hardware device
- Use SAFE Block software to write block a hard drive

### Exercise – Part 1

1. Unpack the UltraDock device from the pouch provided and remove all components and unwrap. We will be using only the components in the photo below for the lab today.



2. Take the components and orient them as per the photo below.



3. Plug the power cable in to the UltraDock (and a receptacle), then plug in the USB3 cable and the SATA connector.





4. Plug your hard drive into the SATA connector.



5. Once all is plugged in, turn on the UltraDock. Using the **Up/Down/Back/Enter** buttons, take some time to familiarize yourself with the various options.
6. Boot your **FOR498 Windows VM**
7. Login to the **FOR498 Windows VM** using the following credentials:
  - a. Username: **SANSDFIR**
  - b. Password: **forensics**

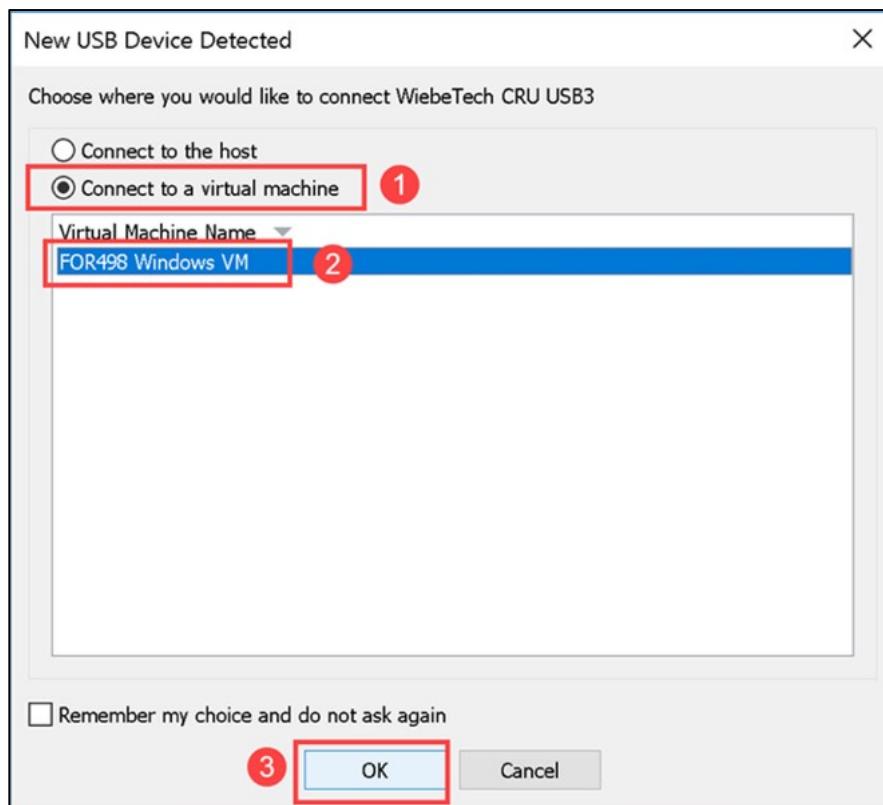
8. Ensure your **FOR498 Windows VM** is in full screen mode. If it is not, you may have connection issues when you turn UltraDock on. The following screenshots refer to the use of **VMware Workstation** and **VMware Player**. For **VMware Fusion** users, jump to **step 14**.



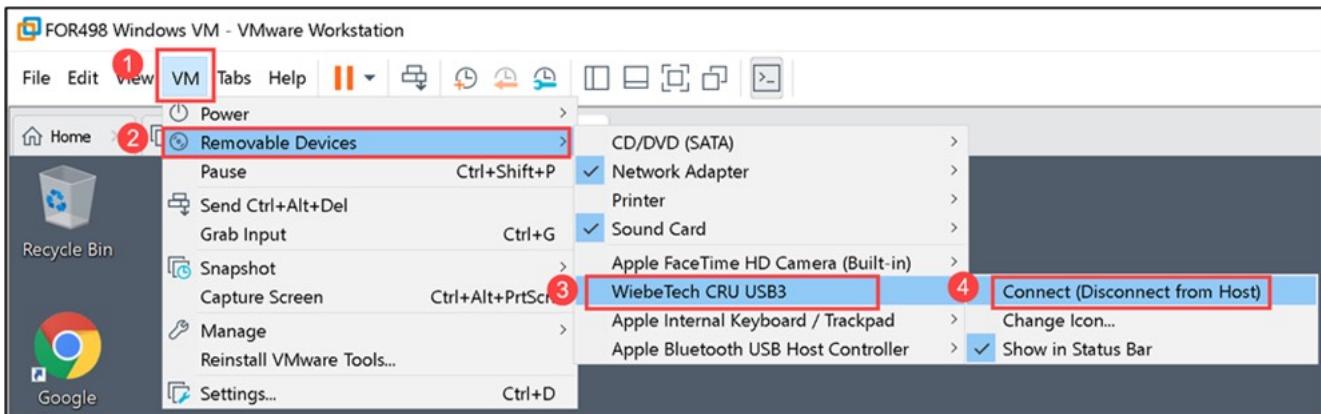
9. Turn the UltraDock on.
10. If **AutoPlay** presents a screen, simply close it.



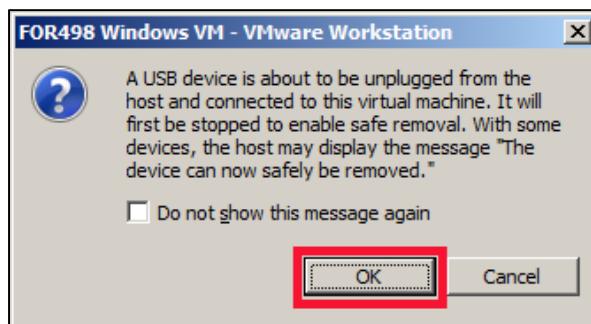
11. When you turn the UltraDock on, you will see the window below. If you do not, proceed to the next step.



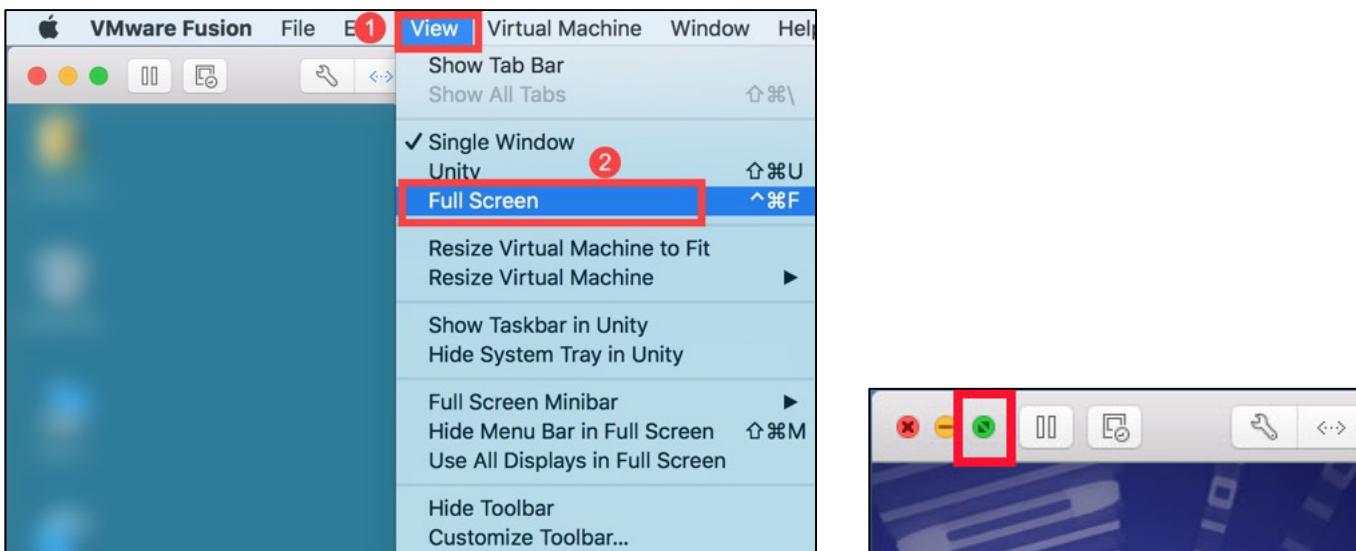
12. In the case of the screen below, the device has been ‘captured’ by the host computer rather than the VM, so you must tell the VM to take control of the device. Within the VM, click on VM -> Removable Devices -> [your device name] -> Connect (Disconnect from the Host).



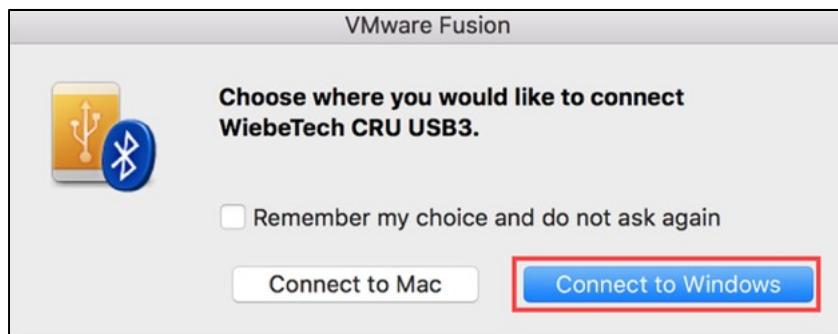
13. You may receive a pop-up confirmation. Click **OK**. Proceed to the **Exercise Questions** following this section.



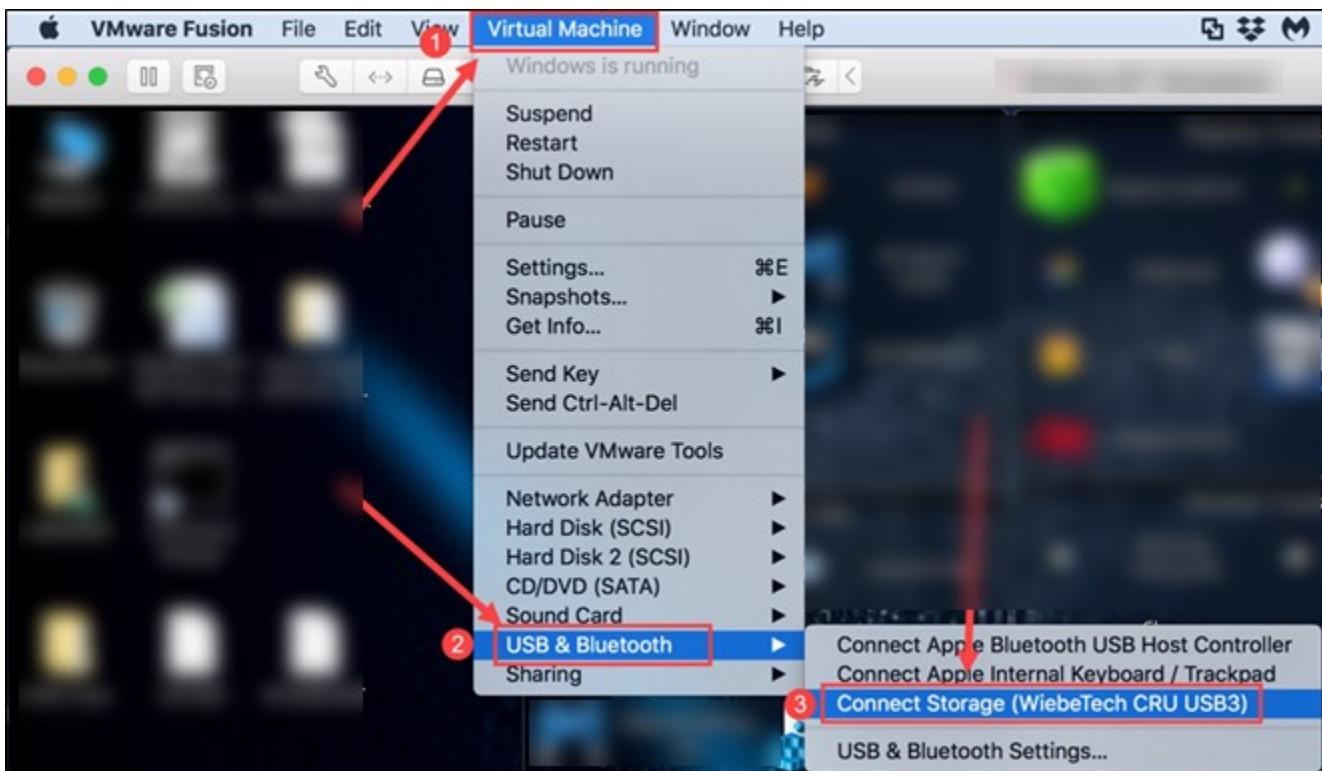
14. For **VMWare Fusion** users, ensure your **FOR498 Windows VM** is in full screen mode. If it is not, you may have connection issues when plugging a device in for analysis with the **VM**. You can choose either of the two methods below.



15. Turn the UltraDock on.
16. When you turn the UltraDock on, a box will appear asking where you want your device to connect. Select **Connect to Windows**, to connect the device to your **FOR498 Windows VM**. If it does not appear, proceed to the next step.



17. If you do not see the previous pop up when attaching the device to the VM, you need to attach it manually. Within the VM, click on **Virtual Machine** → **USB & Bluetooth** → **Connect [your device name]**.



18. If you receive any confirmation prompts, read them carefully before accepting them (or not), and understand what they are asking for.

**NOTE:** In cases where your VM will not allow for external device connection, insert your supplied USB 2.0 hub, and connect through this.

## Exercise Questions

1. Using the **Up/Down/Back/Enter** buttons on the UltraDock, answer the following questions.

- a. What is your drive temperature?

---

- b. How many power cycles have occurred on your drive?

---

- c. What is the serial number of your hard drive?

---

2. Access the hard drive from your computer and attempt to drag and drop the text file you created from the external hard drive over to your computer desktop.

- a. Were you able to move the file?

---

3. Access the hard drive from your computer and attempt to add a line of text to the file you created in the previous section.

- a. Were you able to edit the file?

---

4. Turn off the UltraDock, then turn it back on and access the hard drive from your computer again. Check the drive for the changes you made in the previous steps.

- a. What do you see?

---

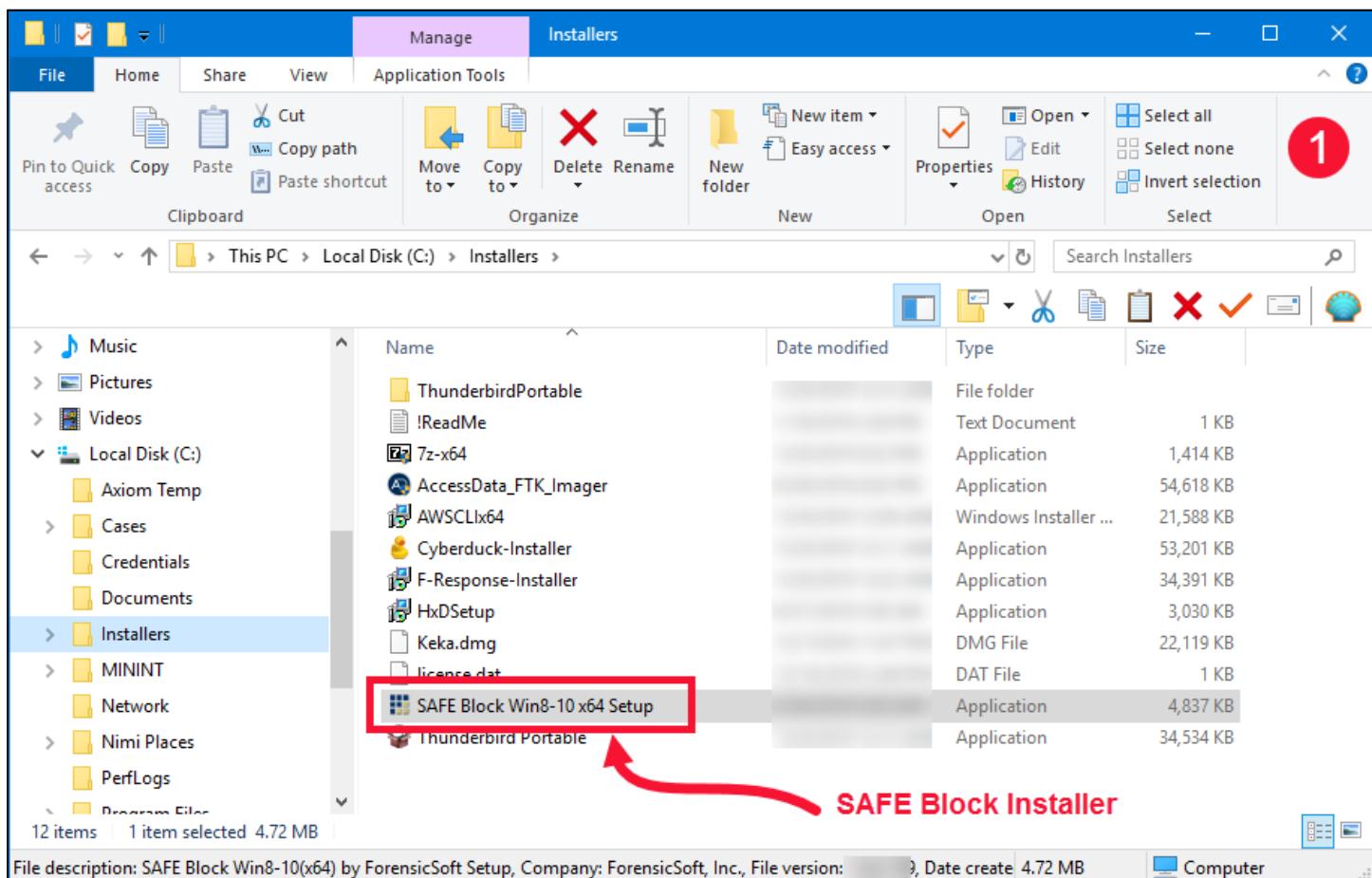
- b. Do you have an explanation?

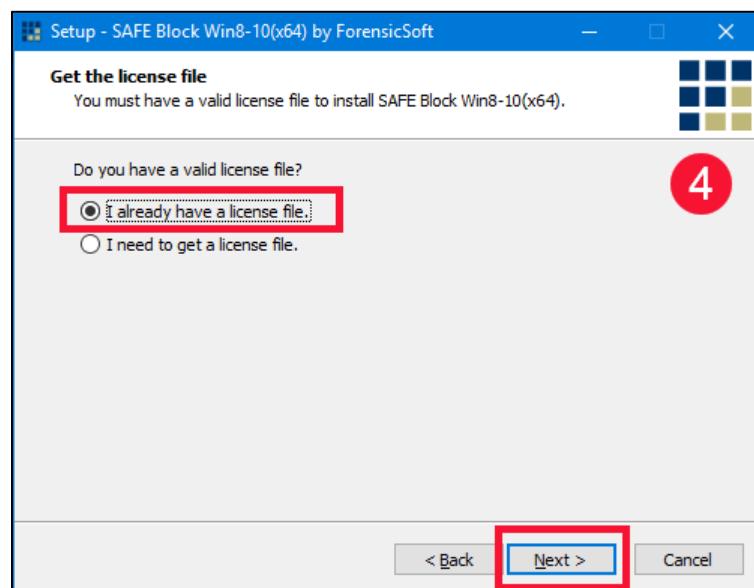
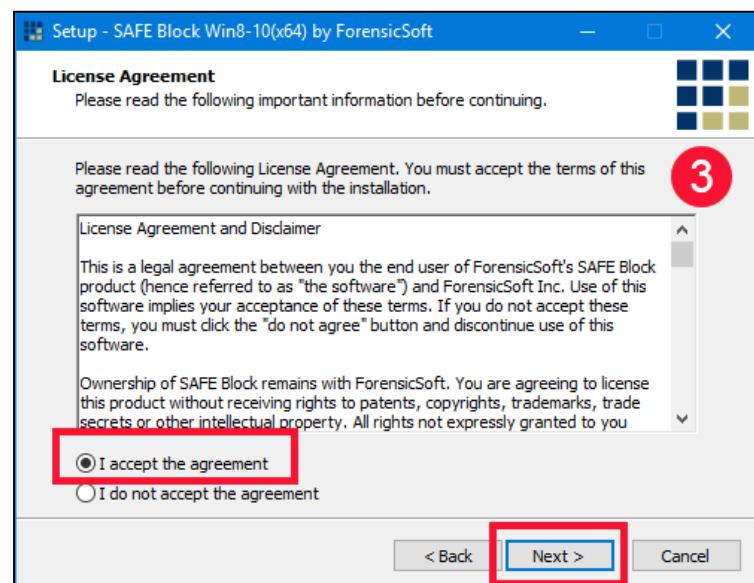
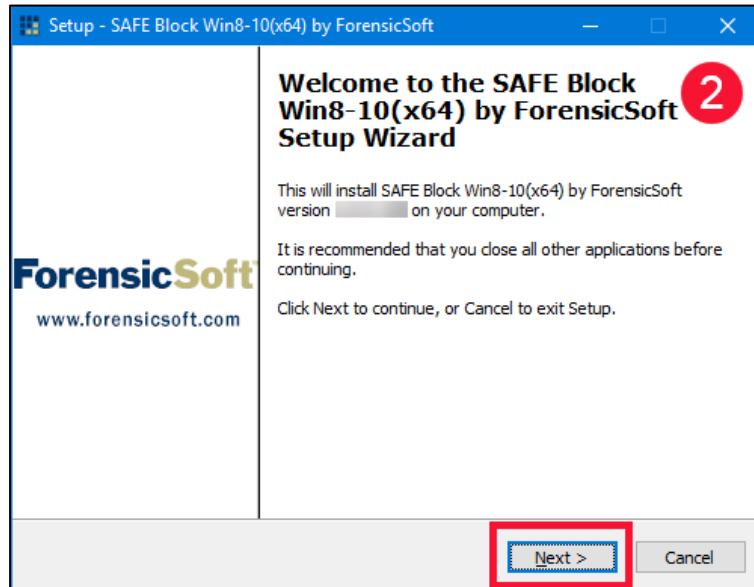
---

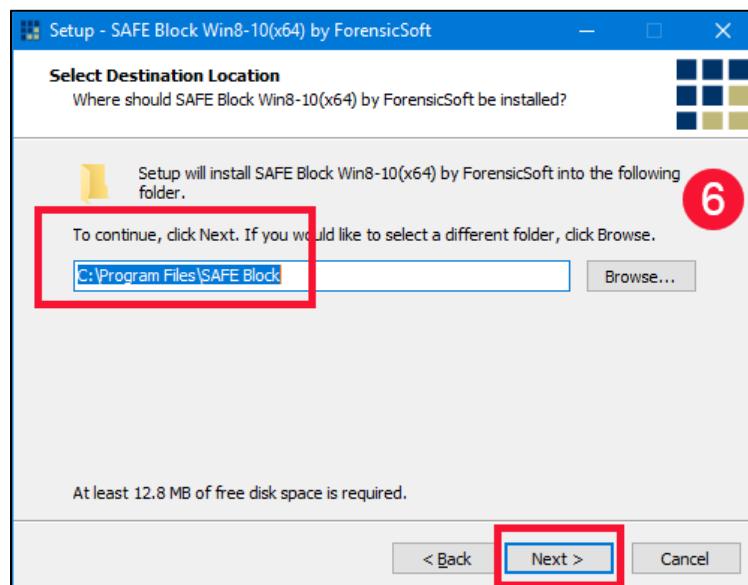
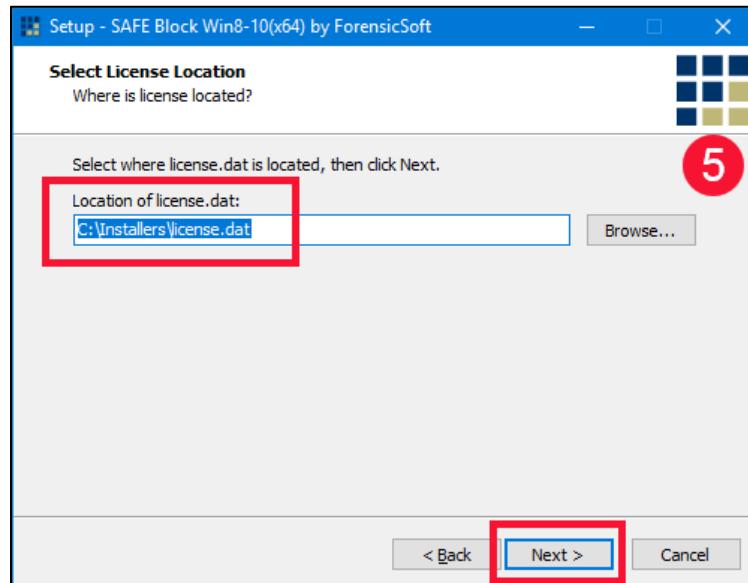
5. Turn off the UltraDock, properly eject it, and remove it from your computer. Disconnect your external hard drive from it.

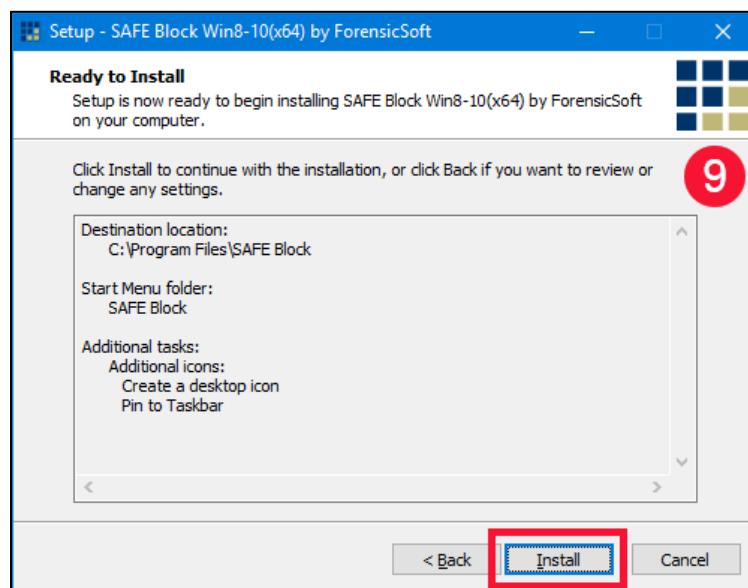
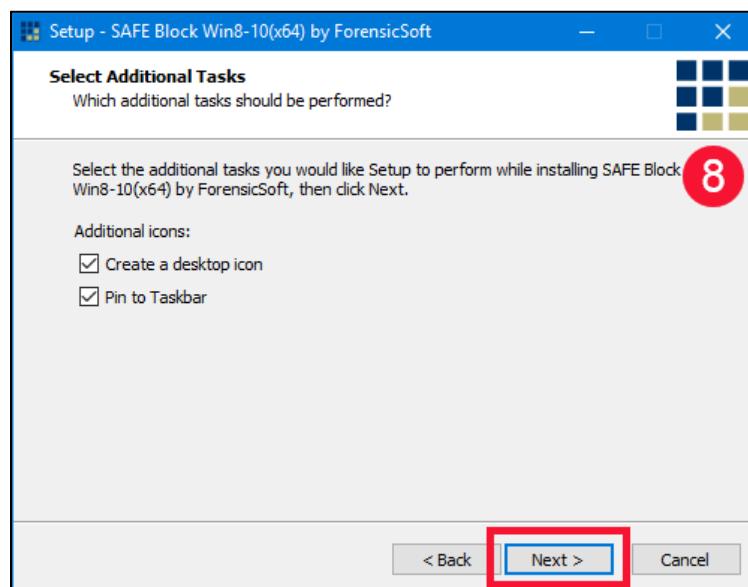
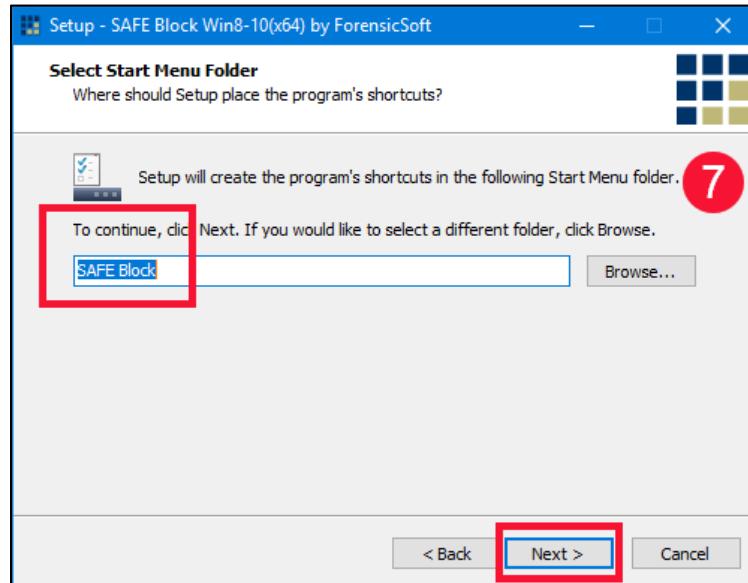
## Exercise – Part 2

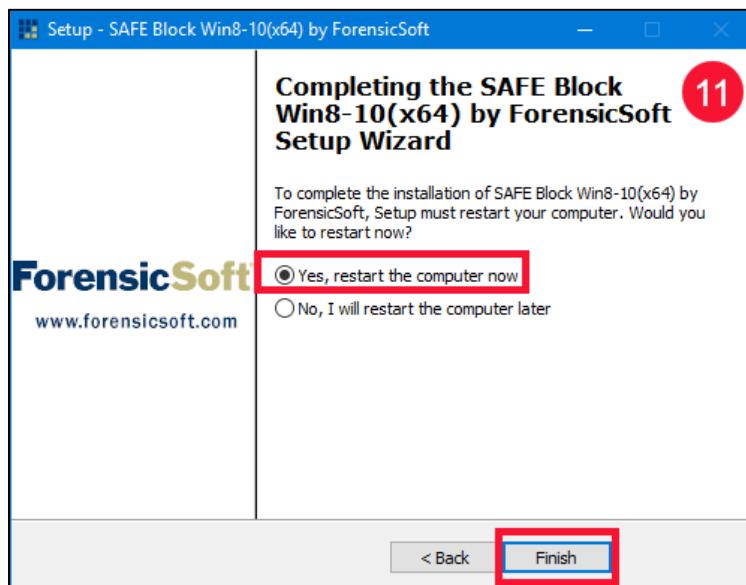
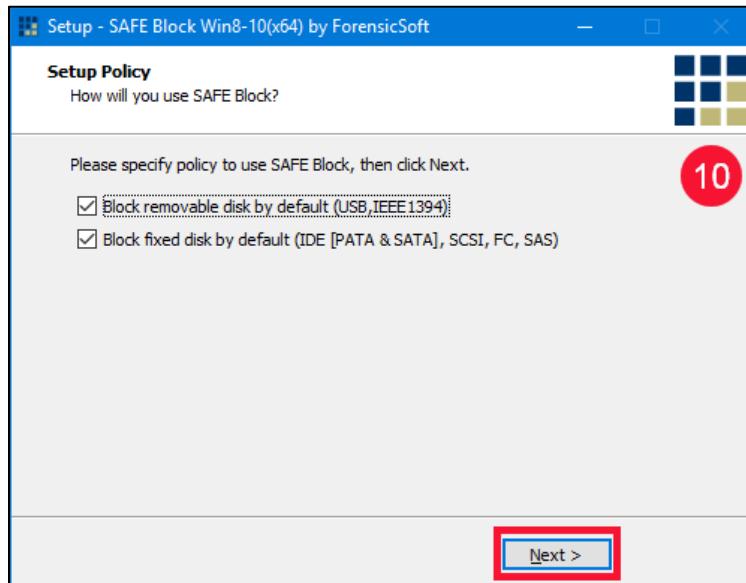
1. For the next part of this exercise we will use the software write-blocking utility **SAFE Block**. Your instructor will provide you with a download link for the **SAFE Block** license file that will be used during the **SAFE Block** installation process.
  - a. Using the link provided by your instructor, download and place the **SAFE Block license.dat** in the **C:\Installers** folder in your VM. The **SAFE Block** installer is also found in **C:\Installers** and is named **SAFE Block Win8-10 x64 Setup.exe**. The following screen shots show you the responses you should complete for each of the steps in the setup program. **You should accept all the default responses**. Double click the installer to begin the installation. **You must choose to restart your computer (VM) at the end of this installation process.**





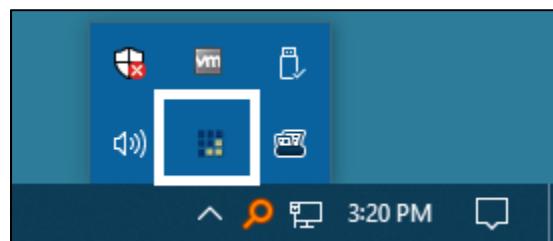






**Did you allow the setup program to restart your VM? If, not restart your VM before proceeding.**

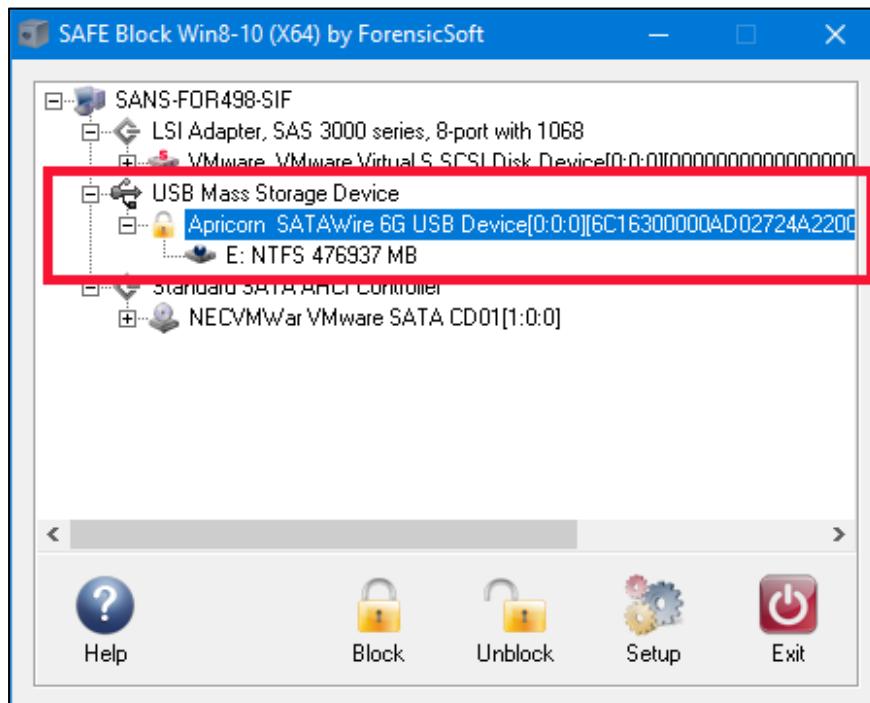
- From your taskbar tray, double click on the **SAFE Block** icon. You may have to expand your taskbar try to see it.



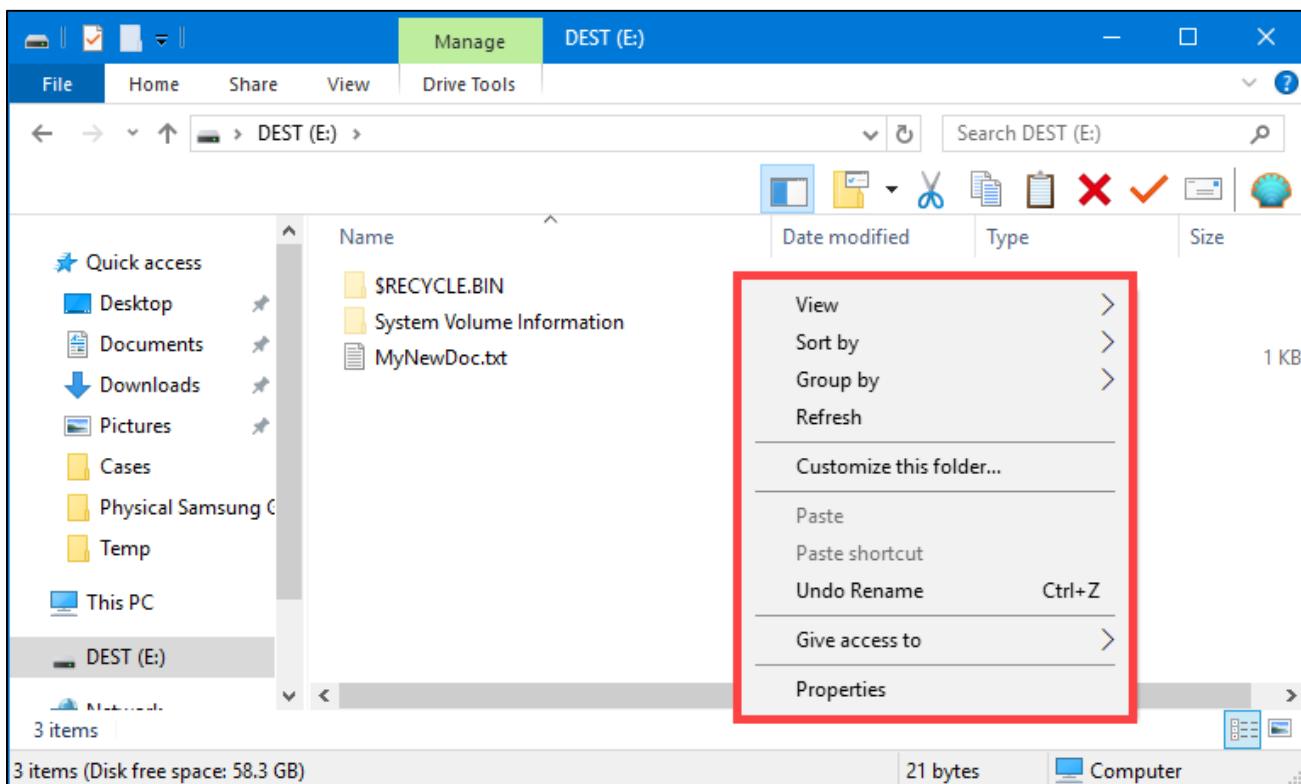
3. The first time that you launch **SAFE Block**, you will be prompted to setup a new password. Enter "forensics" as the password and click **OK**. You will need to confirm the new password by entering it again. You will be prompted for this password each time you launch **SAFE Block**.



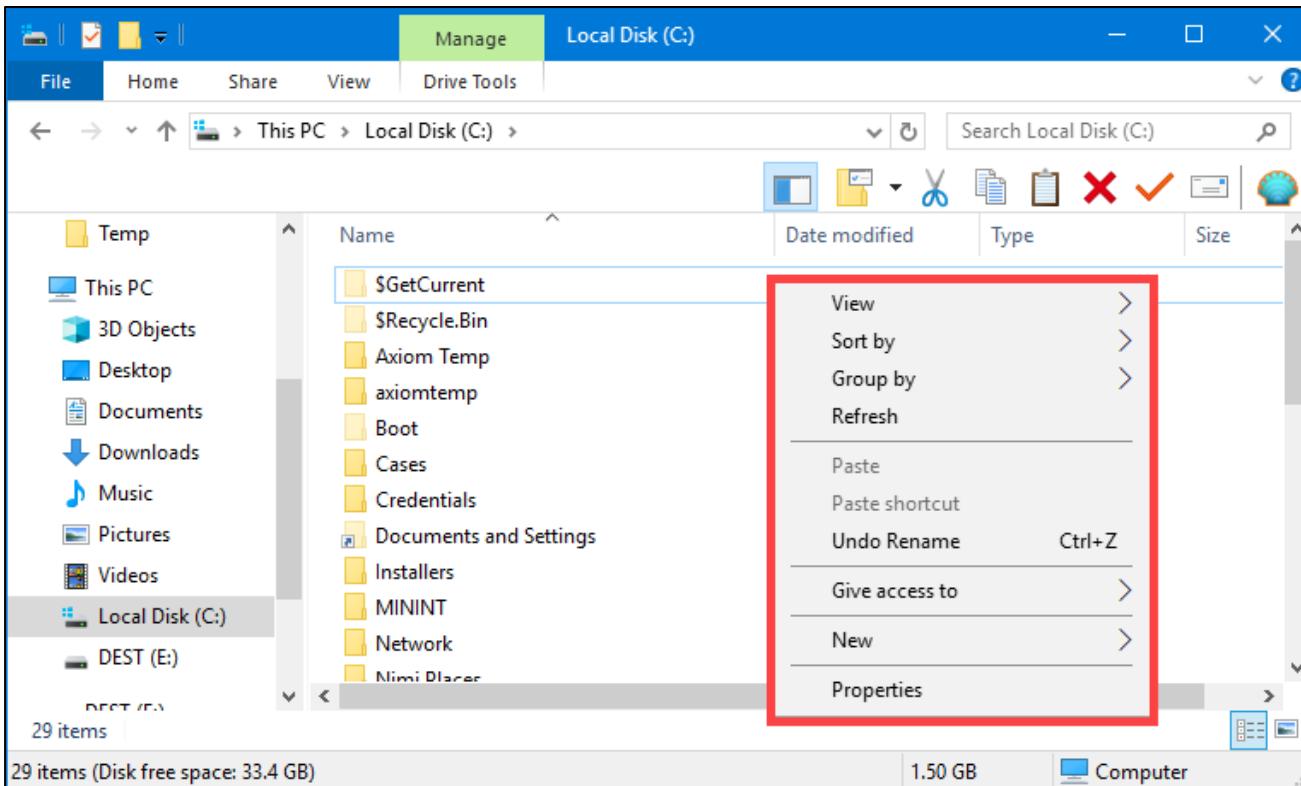
4. Attach the SATA adapter to your external hard drive and plug it into your computer. Ensure it attaches to the VM. After several seconds (as many as 10-20), you will see the external hard drive be detected by **SAFE Block**. You will also see that there is a padlock beside your physical drive.



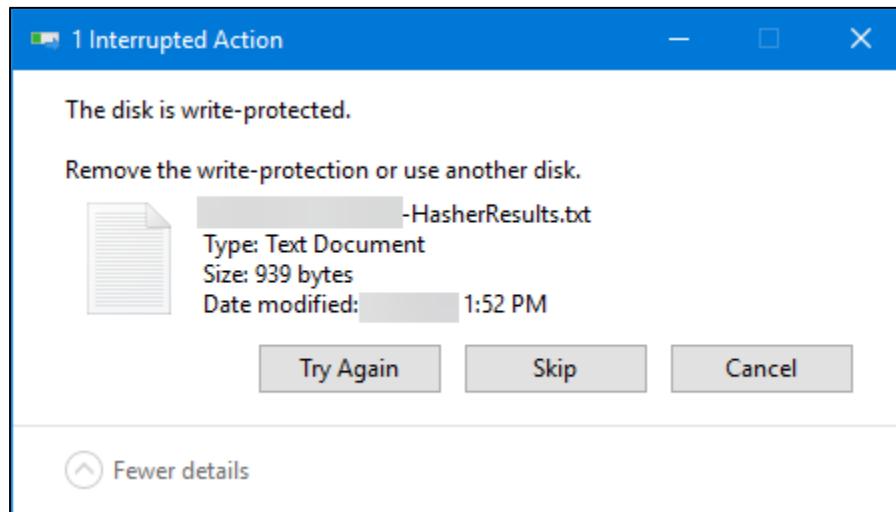
5. Open **File Explorer** and navigate to and open your external hard drive. Right click in the window and try to create a new file. You will note that you have no option of **New**, as you would normally.



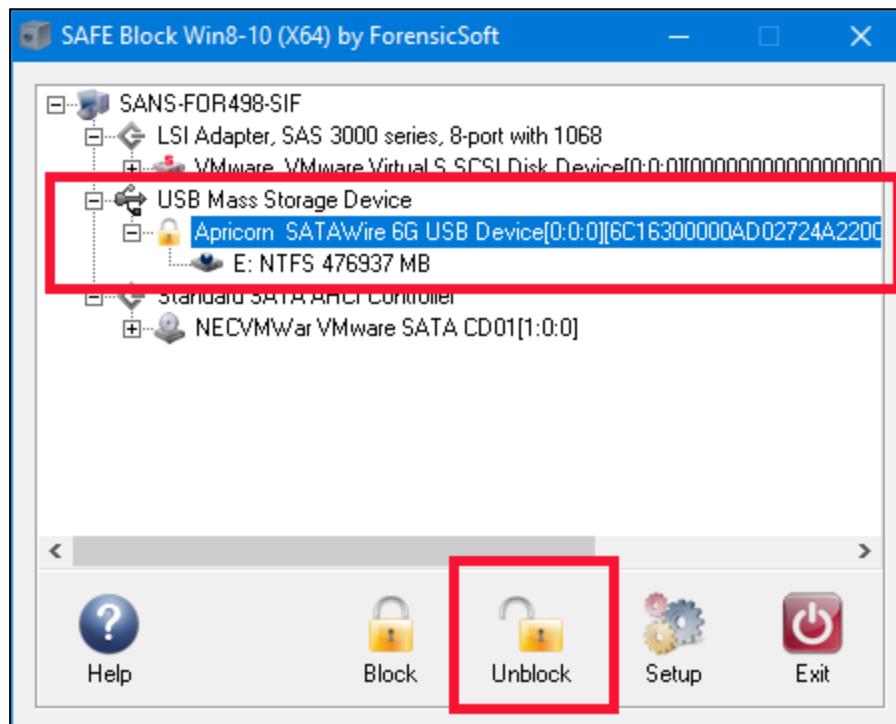
6. As a comparison, navigate to your **VM** hard drive and try to do the same thing. You see that a **New** option is present in the context menu.



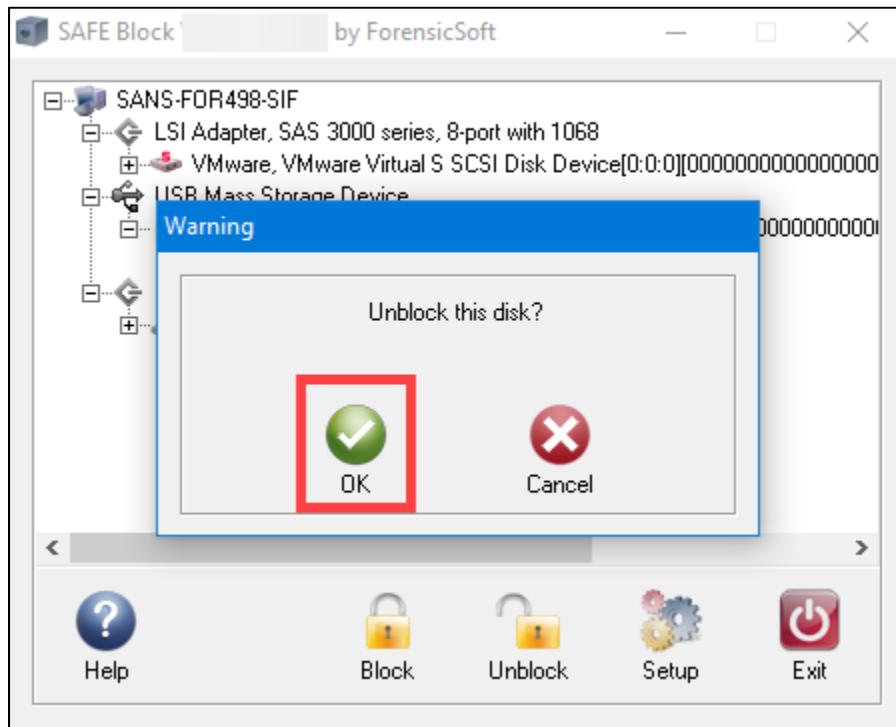
7. Select any file from your **VM** desktop and attempt to drag and drop it to your external hard drive. You will receive an error message. Click **Cancel**.



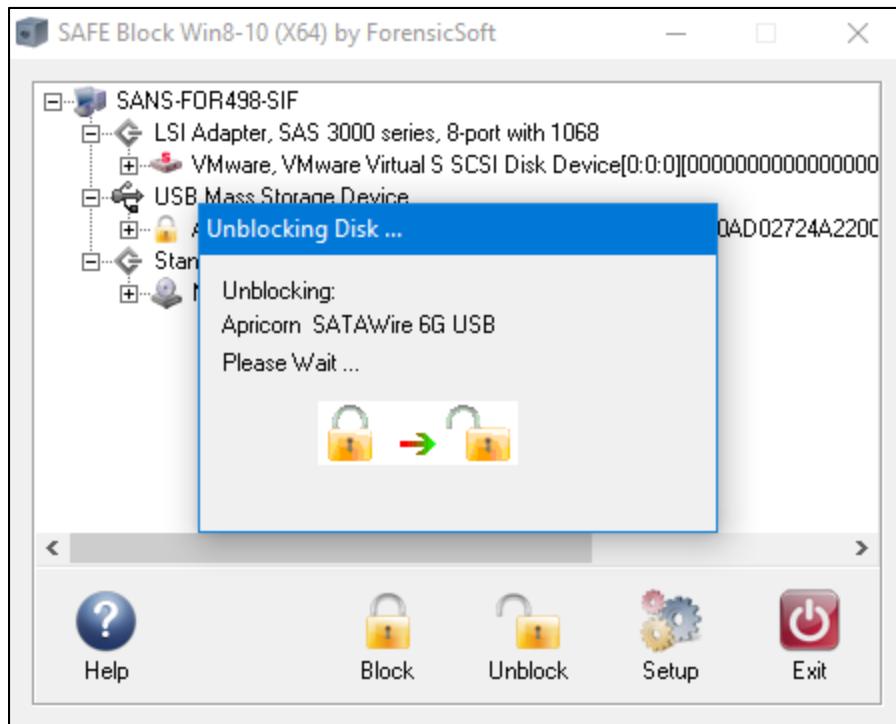
- We will now remove the write blocking on this hard drive. If the **SAFE Block** window is not still open on your desktop, go back to your taskbar and open it again. Highlight your physical drive and click on **Unblock**.



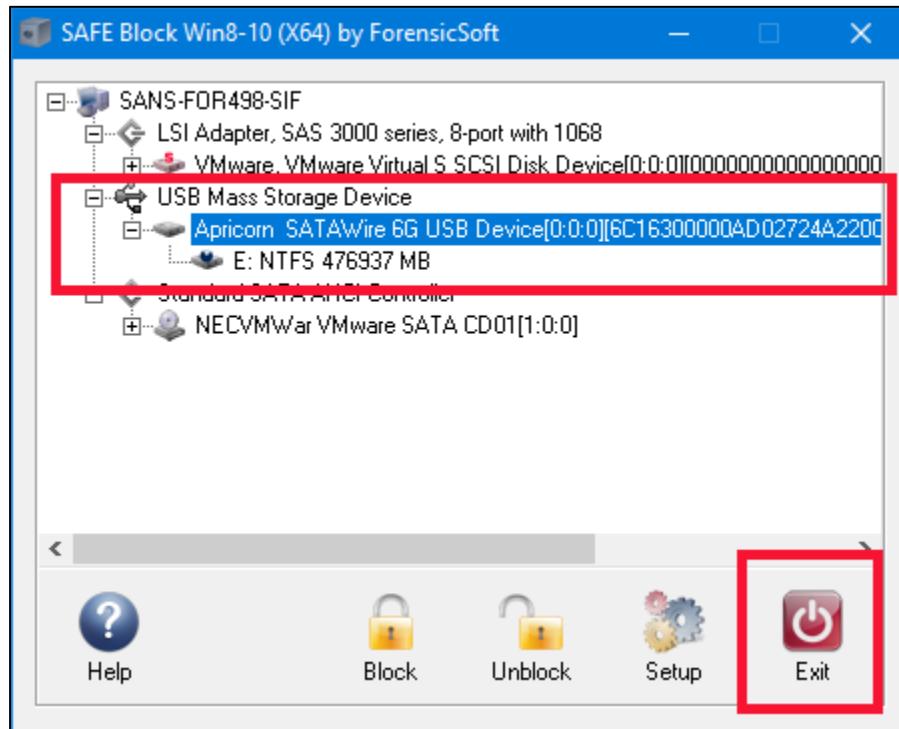
9. In the **Warning** box that appears, click **OK**.



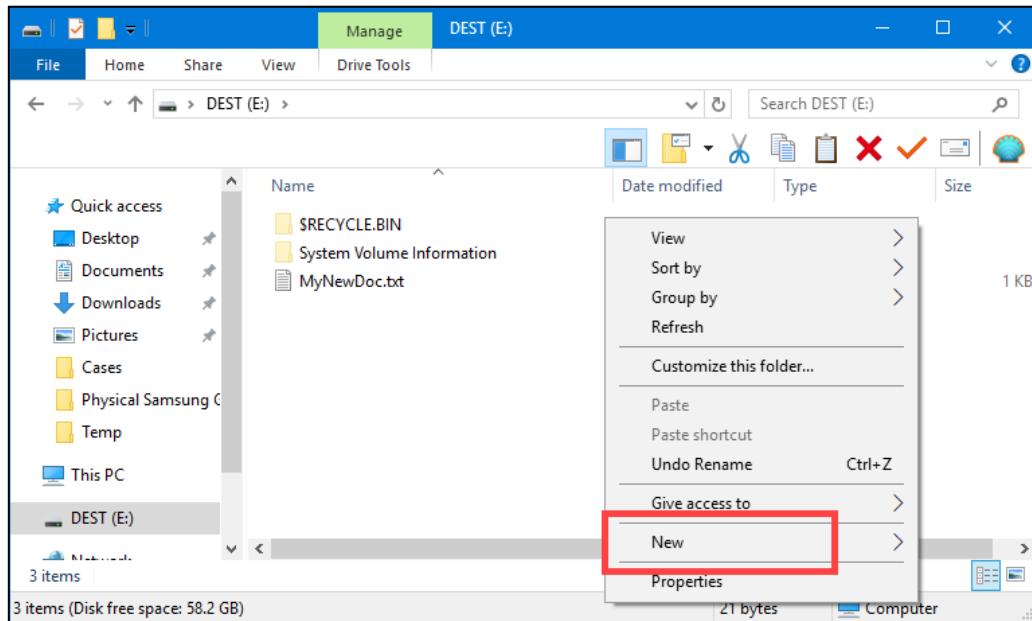
10. You will see the unblock process occurring.



- Once completed, you will see the **SAFE Block** window again, but now the padlock is missing from beside your external hard drive. Click **Exit**.



- Once again, open **File Explorer** and navigate to your external hard drive. Attempt to create a new file here by right clicking. You will note that the **New** option is available once again.



- Once you have done this, close all windows and properly eject your external hard drive. You should now go back to **SAFE Block** using the previous steps, enter **SETUP**, and disable the automatic blocking for both removable and fixed disks. Click **Exit** when done.

## BONUS EXERCISE (Optional)

1. Open **PowerShell** as admin and start the **diskpart** utility.
2. Using the steps in a previous exercise, clean the drive.
3. **These steps WILL cause irreversible data loss! Do not perform any functions until you are SURE of the drive you are wiping.**
4. With **diskpart** running, use the **help** command function to determine how to format your external hard drive with an **NTFS** file system and a name of **DEST**.
5. Test afterwards to ensure success.

## Exercise—Key Takeaways

- Any time you are acquiring media that has been removed from a machine, it must be write blocked.
- Until recently, hardware write blocking was the accepted standard.
- There is no tool on the market like SAFE Block for managing write blocking of non-standard devices.
- SAFE Block can write block virtually anything that can be connected to a computer via any interface.

## Exercise 2.5—Preparing the Analyst Machine

### Background

Out of the box, Windows is not configured in an ideal fashion for forensic investigators. For the casual user, it is a good thing for system files to remain hidden as it reduces the chances a critical file could be deleted.

From a forensic practitioner's perspective however, we often want to look at these system files as they contain a wealth of forensic information we can make use of.

Forensics programs generally come in two forms; those based on a graphical user interface (GUI), and those based on a command line interface (CLI). Because many powerful techniques and forensics tools are command line based, it is important for an analyst to be comfortable navigating from the command line in both Windows and Linux.

In this exercise, we will configure our Windows systems to show hidden files and file extensions, get familiar with Windows PowerShell based command line interfaces, and be introduced to Timeline Explorer which can be used to analyze Excel and CSV data.

### Objectives

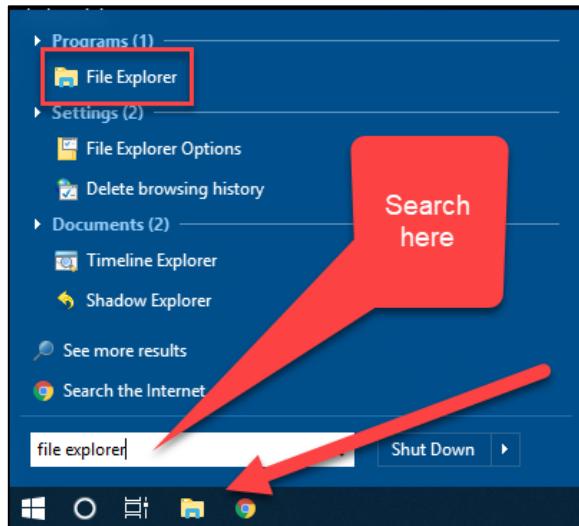
- Configure the FOR498 Windows virtual machine to show hidden folders and files, show hidden system folders and files, show file extensions, and configure folder consistency throughout the machine.
- Introduction to, and use of, PowerShell to get familiarized with how it works.
- Learn fundamental techniques for Timeline Explorer, to use it more effectively when sorting, managing, and reviewing artifacts.

### Exercise Preparation

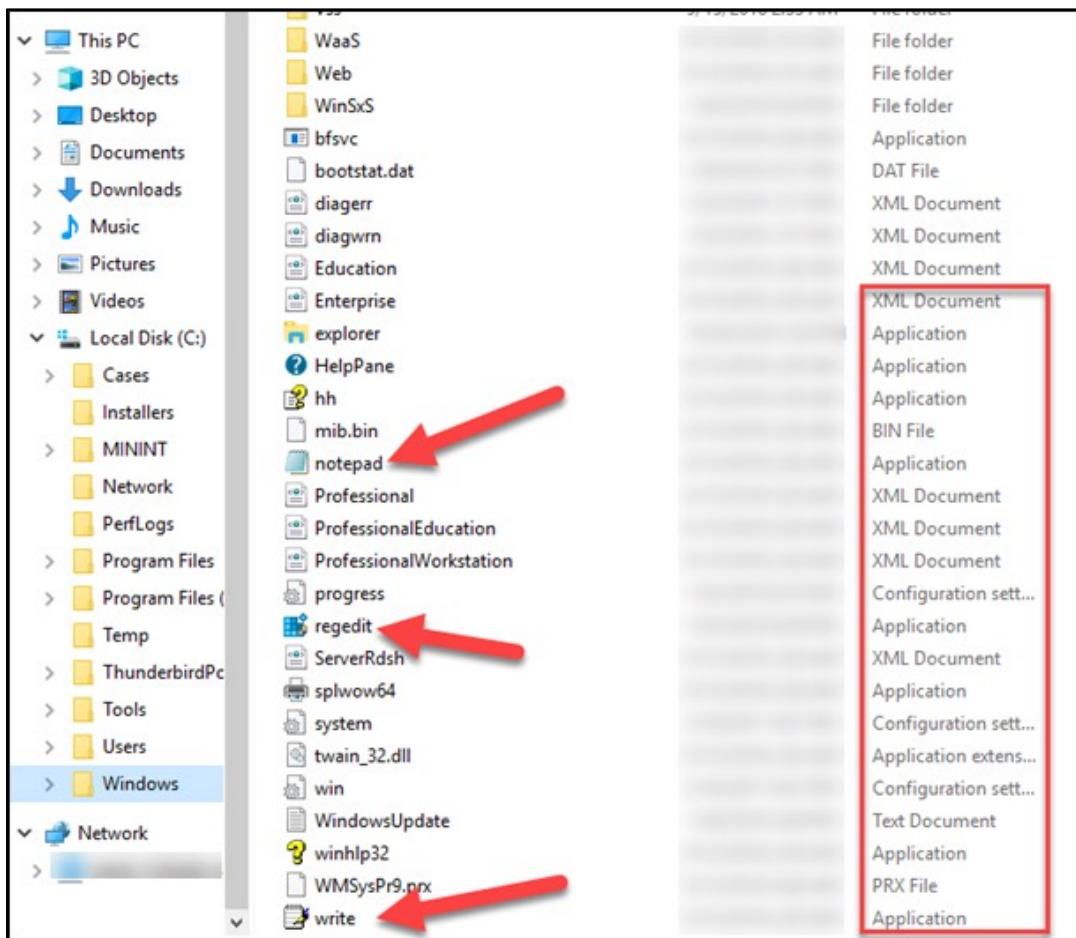
1. Boot your **FOR498 Windows VM**
2. Login to the **FOR498 Windows VM** using the following credentials:
  - a. Username: **SANSDFIR**
  - b. Password: **forensics**

NOTE: For this exercise, we will be performing all tasks inside the SIFT Workstation virtual machine. Ideally, all machines you use for forensics should be configured as outlined below.

3. Open File Explorer via the Start menu icon, or by searching for **File Explorer**.



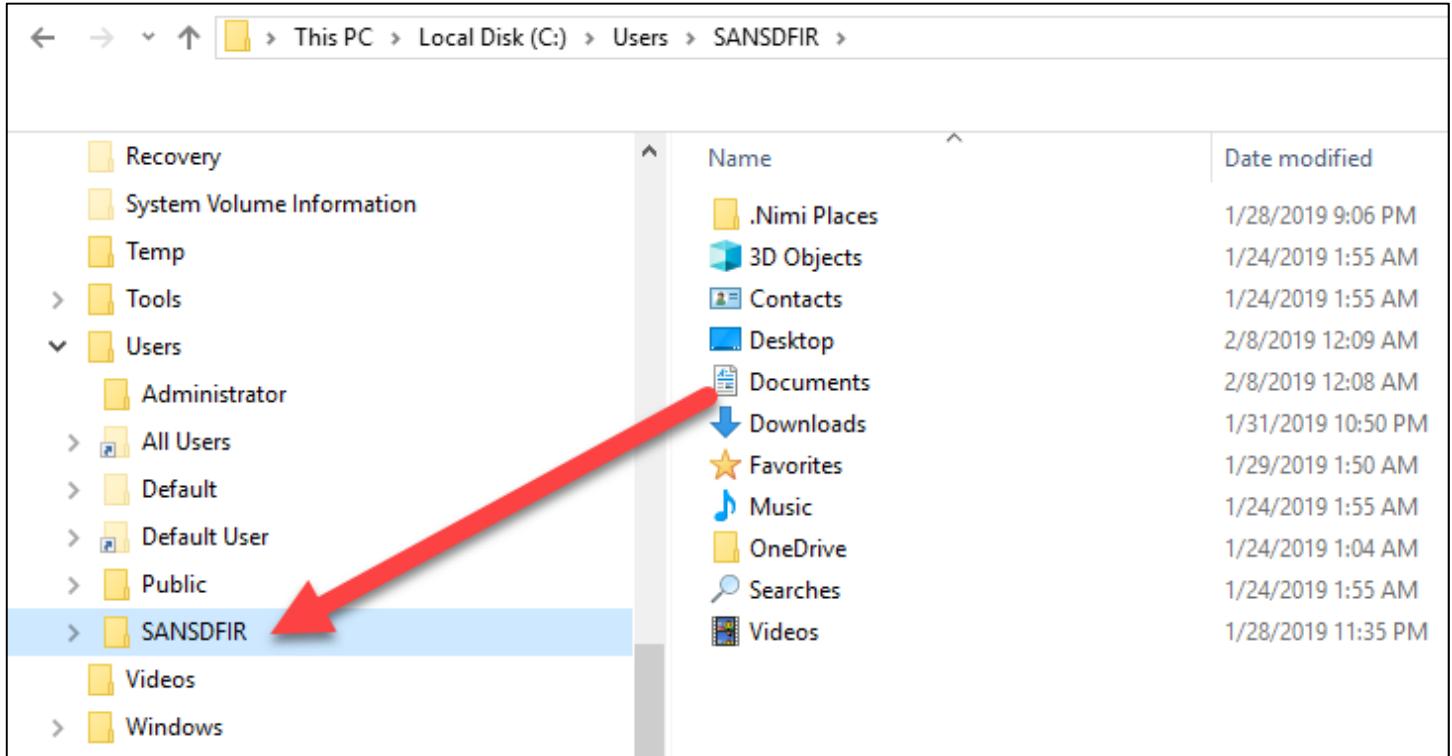
4. Expand **This PC**, expand **Local Disk (C:)**, then click on the **Windows** directory. Once this is selected, scroll down until you see files listed (toward the bottom).



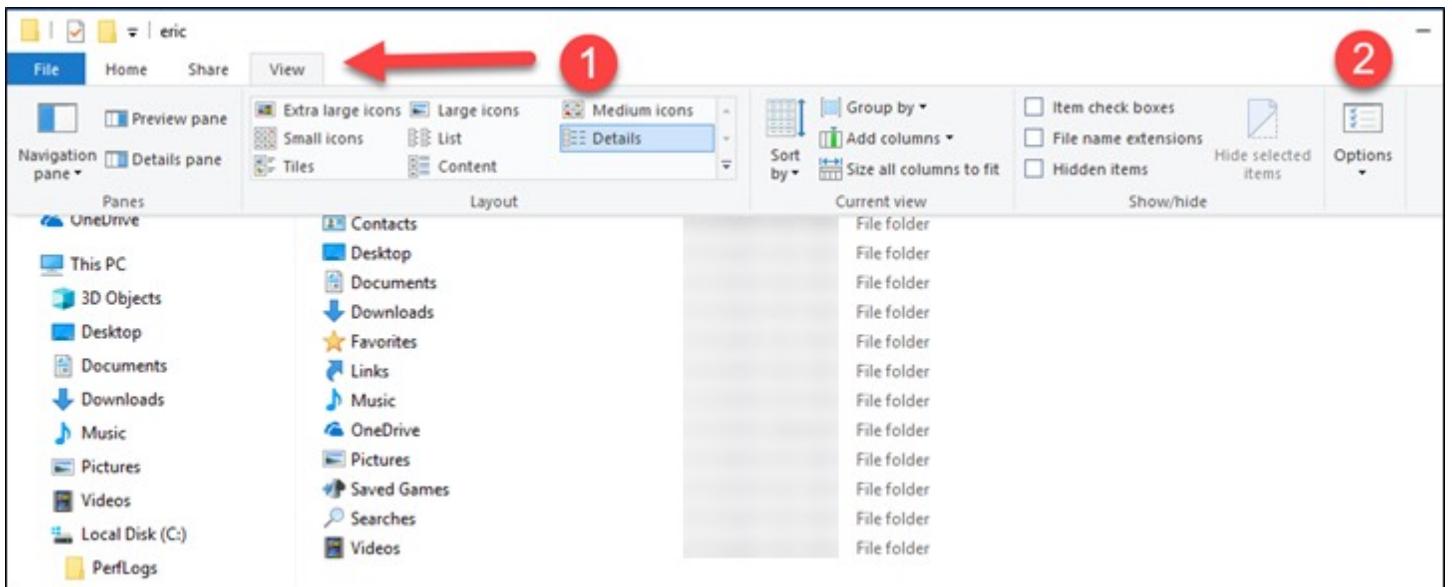
NOTE: Your version of the SIFT workstation may already be configured to show extensions. In this case, you will see the extensions, but continue along to see where this happens so you can configure other machines in the same way.

Notice that most files do not show an extension, but you can see the type of file to the right.

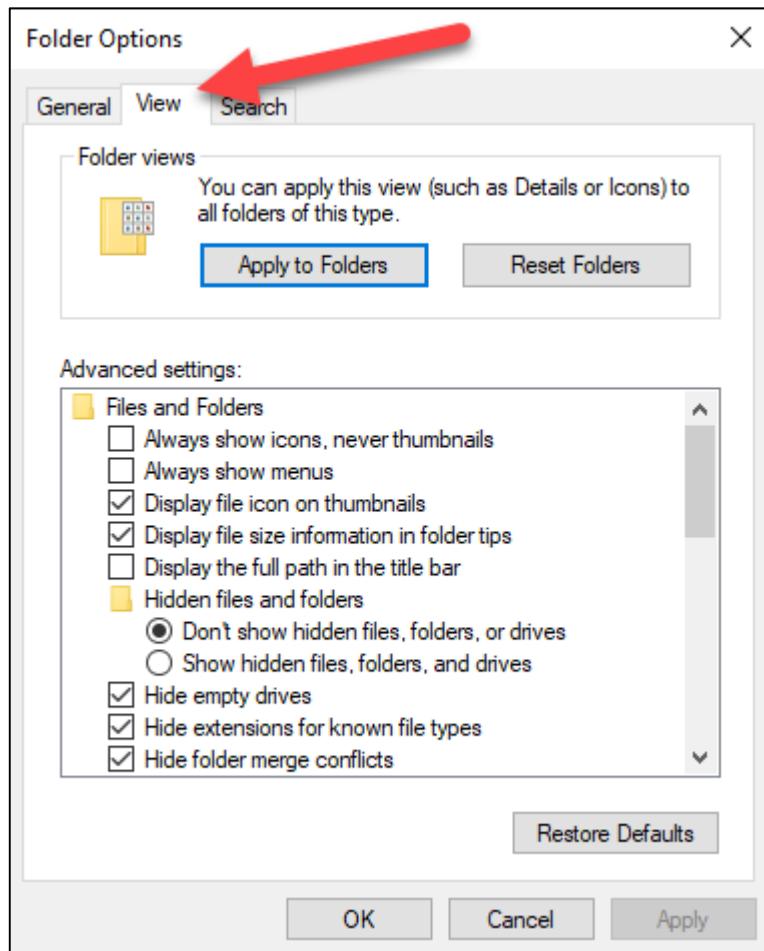
5. Under **Local Disk (C:)**, expand the **Users** folder, then select your profile directory. In the example below, the **SANSDFIR** user profile directory is selected. Notice we cannot see any files in the directory because system files are currently hidden from view.



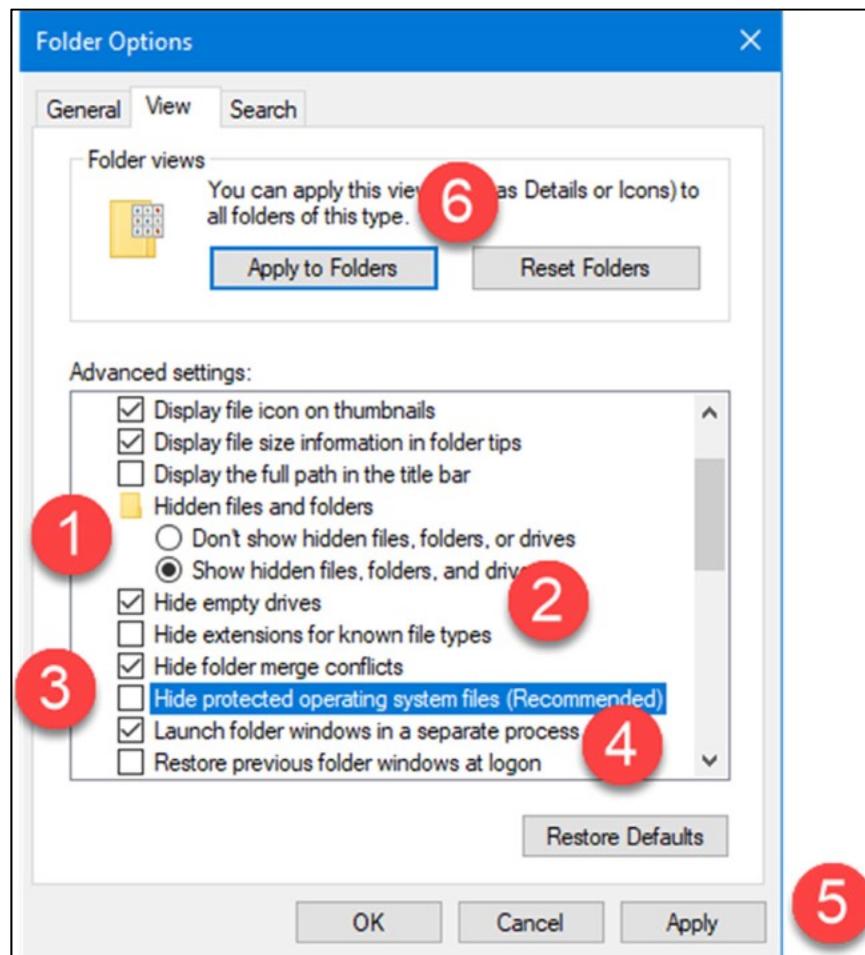
6. In the top menu, click on the **View** tab, then click **Options**.



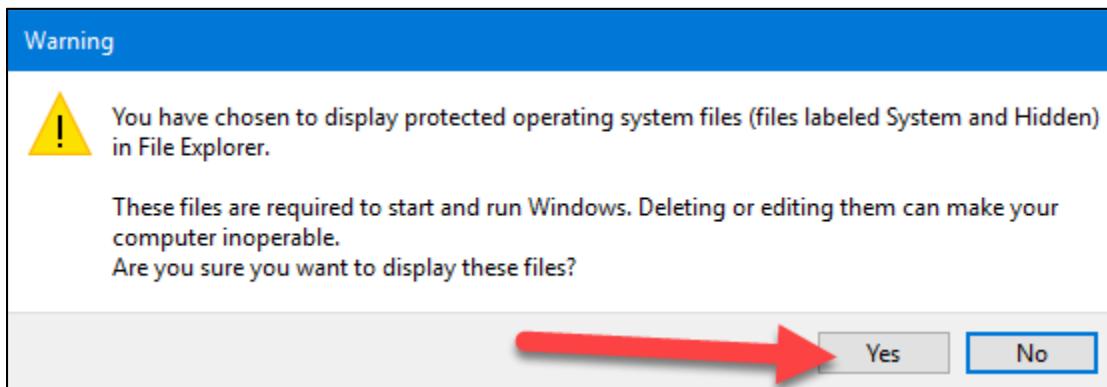
7. On the **Folder Options** dialog, click the **View** tab.



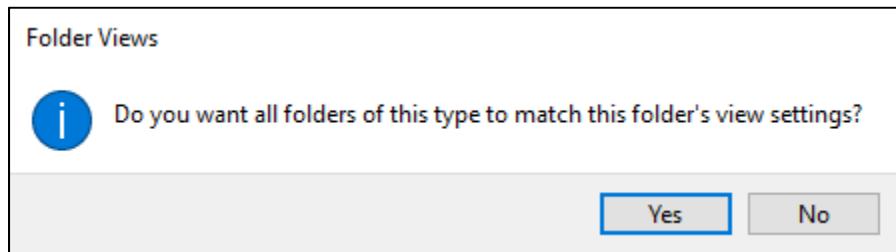
8. Select the radio button for **Show hidden files, folders, and drives** and uncheck **Hide extensions for known file types**, uncheck **Hide protected operating system files (Recommended)**, then scroll down and check **Launch folder windows in a separate process**. When done, click the **Apply** button, then the **Apply to Folders** button at the top.



**Note:** If you see this warning below when unchecking the **Hide protected operating system files** option, click **YES**.



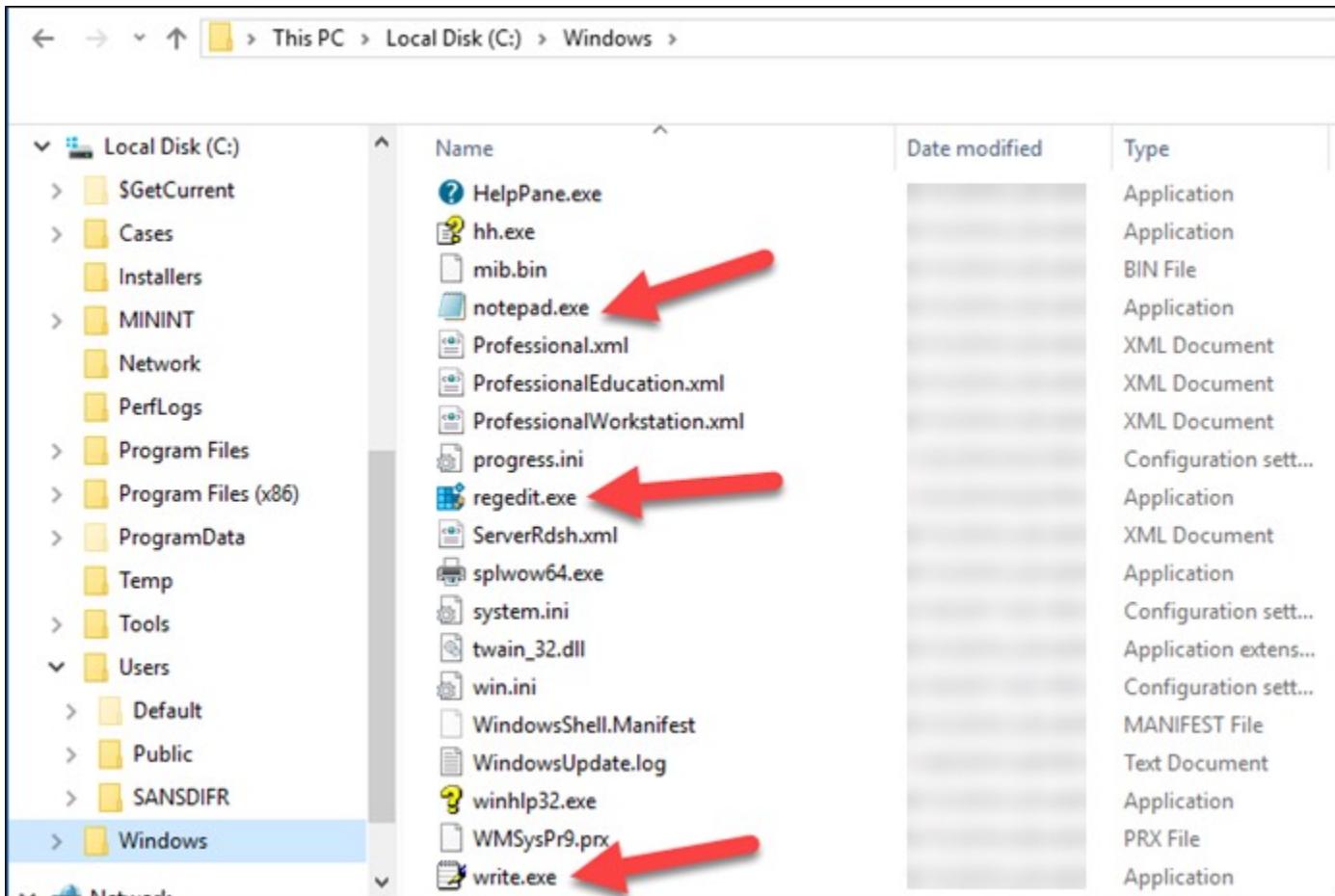
- Click **Yes** when prompted about matching this folder's display setting.



- Click the **OK** button on the **Folder Options** dialog to close it.
- In File Explorer, expand **Local Disk (C:)**, then the **Users** directory. Finally, select the **SANSDFIR** profile directory again. You should now see a number of new files and folders such as **NTUSER.DAT**, that we did not see before.

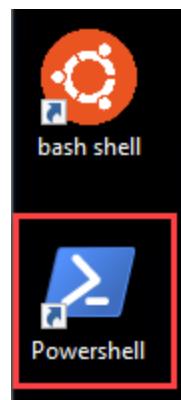
Name	Date modified	Type
.Nimi Places		File folder
3D Objects		File folder
AppData		File folder
Application Data		File folder
Contacts		File folder
Cookies		File folder
Desktop		File folder
Documents		File folder
Downloads	1	File folder
Favorites		File folder
Local Settings		File folder
MicrosoftEdgeBackups		File folder
Music		File folder
My Documents		File folder
NetHood		File folder
OneDrive		File folder
PrintHood		File folder
Recent		File folder
Searches		File folder
SendTo		File folder
Start Menu		File folder
Templates		File folder
Videos	1	File folder
NTUSER.DAT	1	DAT File
ntuser.dat.LOG1		LOG1 File
ntuser.dat.LOG2		LOG2 File
NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-...		BLF File
NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-...		REGTRANS-MS File
NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-...		REGTRANS-MS File
ntuser.ini		Configuration sett...
ntuser.pol		POL File

12. Select the **Windows** directory and scroll down to the bottom. Notice how all files have their file extensions showing now.

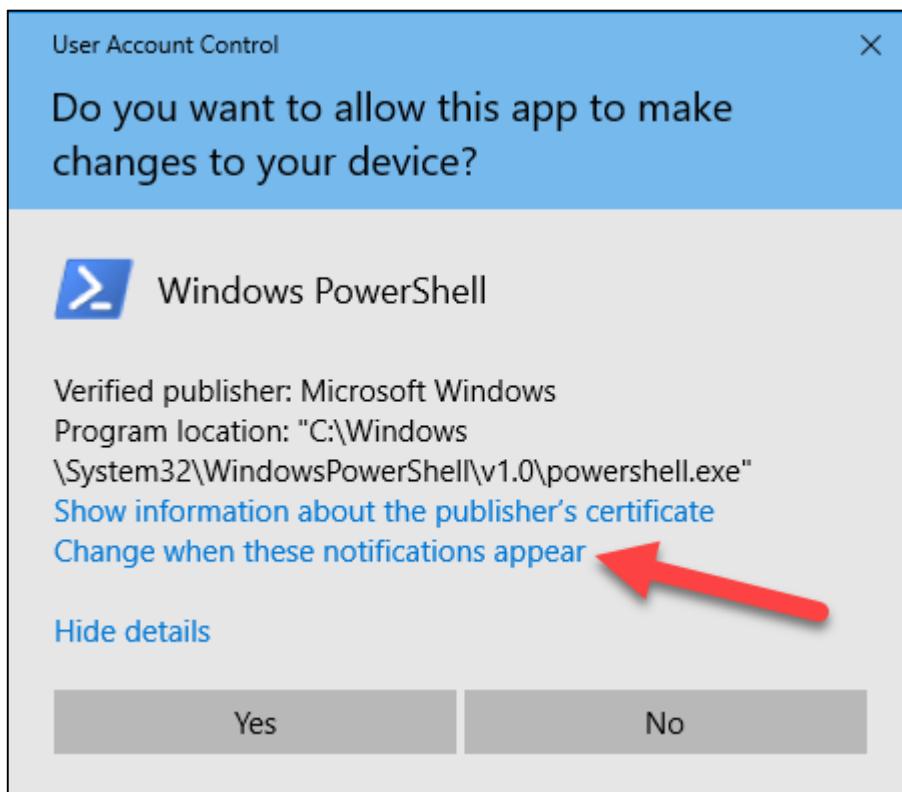
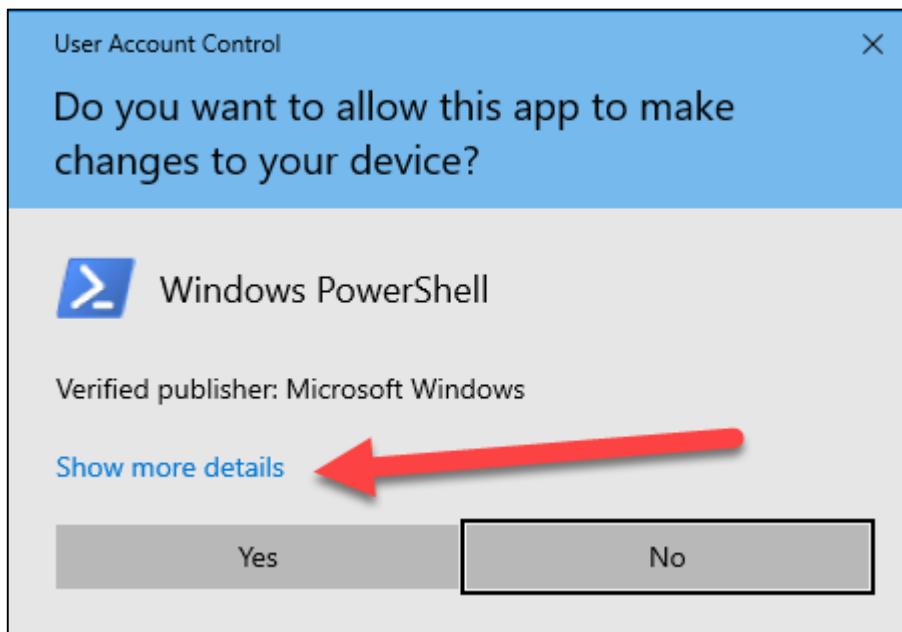


NOTE: Some versions of the SIFT VM may already have **User Account Control (UAC)** disabled. If you do not see the prompts as outlined in this exercise, **UAC** is disabled, but these steps let you disable it on any other machine.

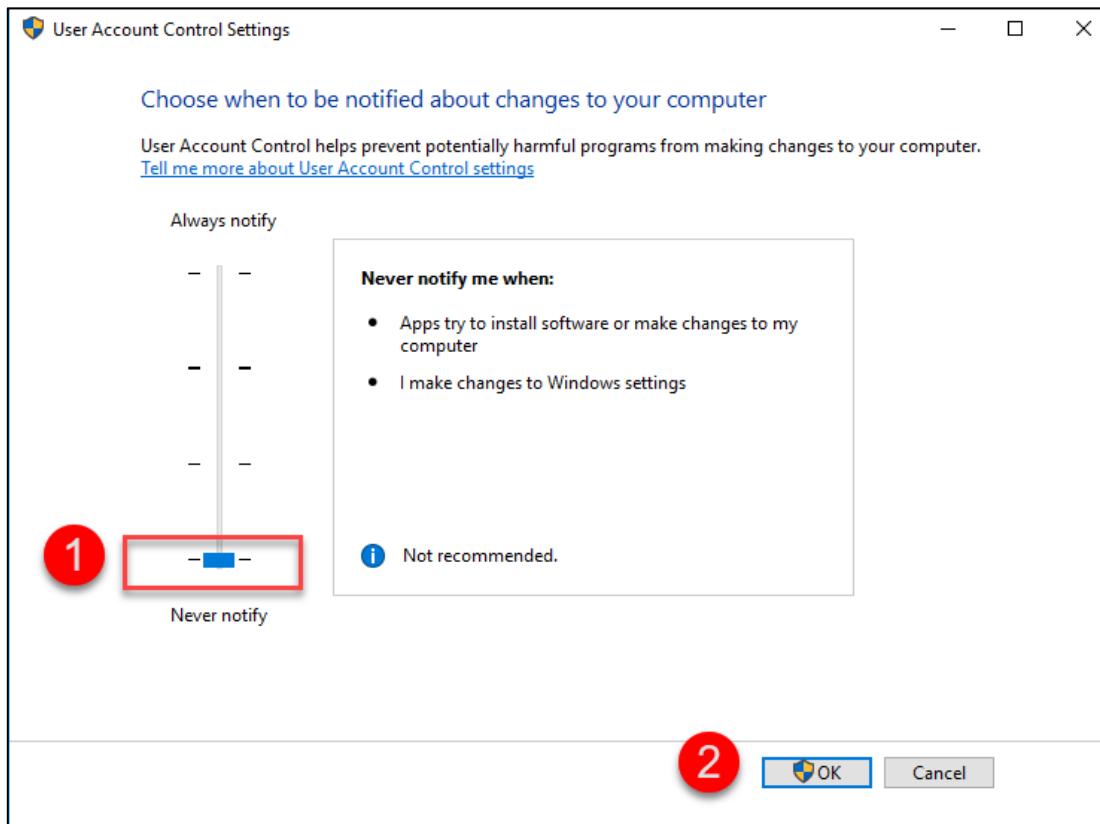
13. Next, we need to disable **UAC**. To do this, double click on the **Powershell** icon on the **Desktop**.



14. You will be prompted by **UAC** as to whether you want to allow **PowerShell** to run. Because so many of the programs we use for forensics require administrator rights, dealing with **UAC** all the time can be annoying. To disable **UAC**, first, click **Show more details**, then click **Change when these notifications appear**.



15. Move the slider all the way to the bottom, by **Never notify**, then click **OK**.



16. You will be prompted by **UAC** again, but this will be the last time. Click **Yes** when prompted.

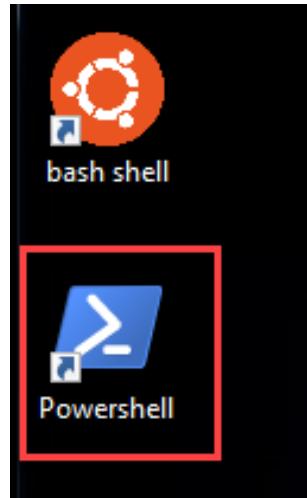


UAC is now disabled, and we will not be prompted again when running things as an Administrator.

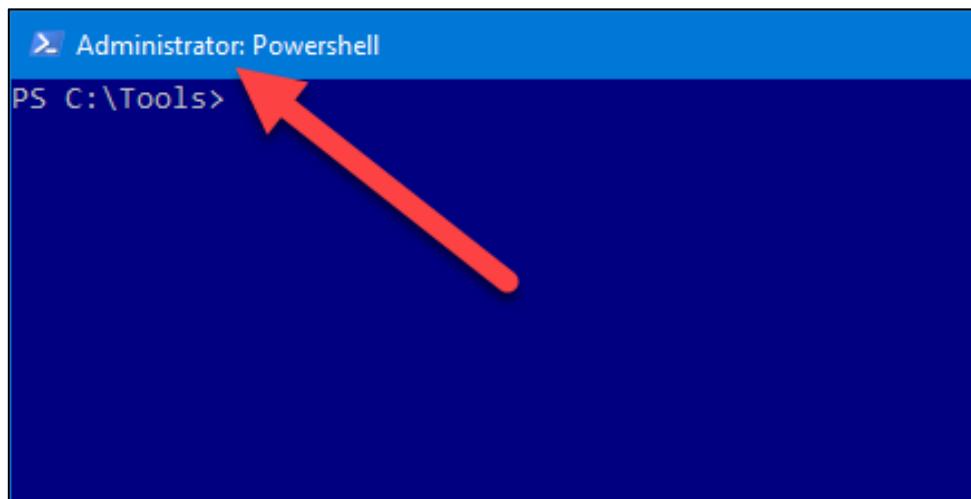
PowerShell is Microsoft's preferred way to interact with the operating system. If you have used the traditional command (cmd) interface in the past, using PowerShell will be very straightforward. For people familiar with command line interfaces on Linux, PowerShell will also seem familiar in some ways.

While PowerShell can do a wide range of things as it relates to interacting with a Windows system, we will focus on how to navigate directories and execute programs.

17. To start **PowerShell**, use the shortcut on the **Desktop** to automatically launch **PowerShell** as an Administrator.



18. **PowerShell** will start. Notice how the title bar shows that we are running **PowerShell** as an Administrator. This will be important for many of the programs we will be executing, as they require administrative rights to work properly.



19. The following chart shows some common commands we will be using:

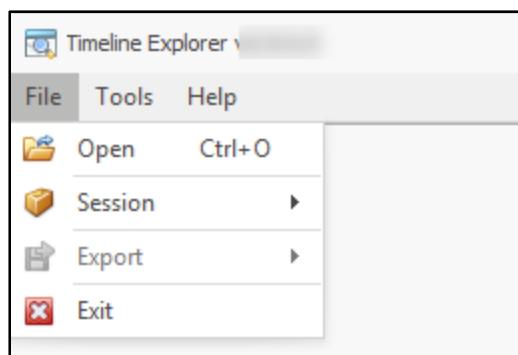
Command	Purpose	Example/notes
<drive letter>:	Change which drive letter is currently active	D: <enter> or C: <enter>
cd <directory>	Changes active directory. Note that this can also be used to switch drive letters as well	cd c:\temp <enter> or d:\temp\output <enter>
dir or ls	List the contents of the active directory	
<tab>	Completes or shows available matches	<p>Also known as command line completion, using the TAB key tells PowerShell to cycle through all available matches for a given path, program name, options, etc.</p> <p>For example, if c:\temp and c:\tools existed in c:\, typing cd c:\t&lt;tab&gt; would auto-complete the path, first to c:\temp and then to c:\tools with another press of &lt;tab&gt;. This is useful because it prevents typing mistakes and is much faster than typing out full file paths, etc.</p>
Get-Command	Lists all available cmdlets	A cmdlet is a lightweight command that is used in the Windows PowerShell environment.
alias	Shows all available aliases for commands	PowerShell includes many default aliases, like dir and ls, that map to the corresponding PowerShell cmdlet. dir and ls are aliased to the PowerShell cmdlet Get-ChildItem
Get-Help <cmdlet>	Brings up detailed help on <cmdlet>	Get-Help Write-Warning
	Used to pipe one cmdlet to another.	Get-Process   Format-Table
>	Redirect the output of a cmdlet to a file	Get-Process > C:\temp\processes.txt

20. **PowerShell** is different from traditional command line interfaces in that **PowerShell** commands are not text-based. In other words, while what we typically see when running a cmdlet is text on the screen, this is because it is displayed that way by default. The true output of **PowerShell** are objects, which have structured information that can be filtered, passed on to other cmdlets, or displayed as text (i.e., viewed in the console, written to a file, etc.).

For a more in-depth treatment of **PowerShell**, check out *Learn Windows PowerShell in a Month of Lunches*, by Don Jones.

**Timeline Explorer (TLE)** is a tool that helps analyze CSV and Excel files. It contains powerful features such as sorting, filtering, column grouping, and searching. Timeline Explorer will greatly simplify the task of reviewing the output from a wide variety of forensic tools.

21. Using **File Explorer**, navigate to **C:\Tools\TimelineExplorer** and double click **TimelineExplorer.exe**. You can also use the shortcut in the **Utilities** fence of the **Desktop** to launch **Timeline Explorer**.
22. **Timeline Explorer** can have multiple files loaded at the same time. Each file is loaded into a separate tab. Files are loaded into **TLE** via the **File | Open** menu option, or via drag and drop. Having said that, drag and drop will NOT work if **TLE** is running as Administrator.



Depending on how many files were opened or dropped, it may take a moment for them all to load. Once they are all loaded, each file is available in its own tab.

The next few steps will explain some of the basic features of **Timeline Explorer**. Once we see a few of these, we will load some CSV files and practice.

**NOTE:** The screen shots below are for illustration of features only. After reviewing some of the features of **Timeline Explorer**, the **Questions** section will cover using **Timeline Explorer** against a CSV file.

Line	Tag	Note	Source	Filename	Volume	Serial	Source	Created	Source	Modified	Source	Access	Executable Name
1			E:\[root]\Windows\Prefetch\MSIEXEC...		E8D4A909		2013-09-23	19:49:58	2013-10-18	0...	2013-09-23	19...	MSIEXEC.EXE
2			E:\[root]\Windows\Prefetch\WWAHO...				2013-09-23	19:48:18	2013-10-05	1...	2013-09-23	19...	WWAHOST.EXE
3			E:\[root]\Windows\Prefetch\RTFTR...				2013-09-23	19:48:10	2013-10-20	2...	2013-09-23	19...	RTFTRACK.EXE
4			E:\[root]\Windows\Prefetch\DSMUS...				2013-09-23	19:51:26	2013-10-23	0...	2013-09-23	19...	DSMUSERTASK.EXE
5			E:\[root]\Windows\Prefetch\LOGON...				2013-09-23	19:47:29	2013-10-23	0...	2013-09-23	19...	LOGONUI.EXE
6			E:\[root]\Windows\Prefetch\WWAHO...				2013-09-23	19:49:14	2013-10-06	1...	2013-09-23	19...	WWAHOST.EXE
7			E:\[root]\Windows\Prefetch\NGENT...				2013-09-23	19:50:24	2013-10-23	1...	2013-09-23	19...	NGENTASK.EXE
8			E:\[root]\Windows\Prefetch\NGENT...				2013-09-23	19:50:24	2013-10-23	0...	2013-09-23	19...	NGENTASK.EXE
9			E:\[root]\Windows\Prefetch\ITUNE...				2013-09-26	17:53:53	2013-10-18	0...	2013-09-26	17...	ITUNES.EXE
10			E:\[root]\Windows\Prefetch\EXPLO...		E8D4A909		2013-09-23	21:02:36	2013-10-21	1...	2013-09-23	21...	EXPLORER.EXE
11			E:\[root]\Windows\Prefetch\IEXPLO...				2013-09-23	20:54:18	2013-10-19	1...	2013-09-23	20...	IEXPLORE.EXE
12			E:\[root]\Windows\Prefetch\IEXPLO...				2013-09-23	20:54:18	2013-10-19	1...	2013-09-23	20...	IEXPLORE.EXE
13			E:\[root]\Windows\Prefetch\OPENW...				2013-09-23	20:54:08	2013-10-20	1...	2013-09-23	20...	OPENWITH.EXE
14			E:\[root]\Windows\Prefetch\ICLOU...				2013-09-23	20:51:49	2013-10-18	1...	2013-09-23	20...	ICLOUD.EXE
15			E:\[root]\Windows\Prefetch\WINWO...				2013-09-23	20:41:02	2013-10-22	1...	2013-09-23	20...	WORD.EXE

Notice the full path to the file is in the lower left and both the total and the visible number of lines is in the lower right.

23. Filtering allows you to quickly hone in on relevant data via one or more column headers, or by using the **Search** box in the upper right.

Source Filename	Volume1Seri...	Source Created	Source Modifi...	Source Access...	Executable Name
E:\[root]\Windows\Prefetch\EXPLO...	E8D4A909	2013-09-23 21:02:36	2013-10-21 1...	2013-09-23 21...	EXPLORER.EXE
E:\[root]\Windows\Prefetch\Op-EX...		2013-09-23 19:52:04	2013-10-22 1...	2013-09-23 19...	Op-EXPLORER.EXE-319FC3CE

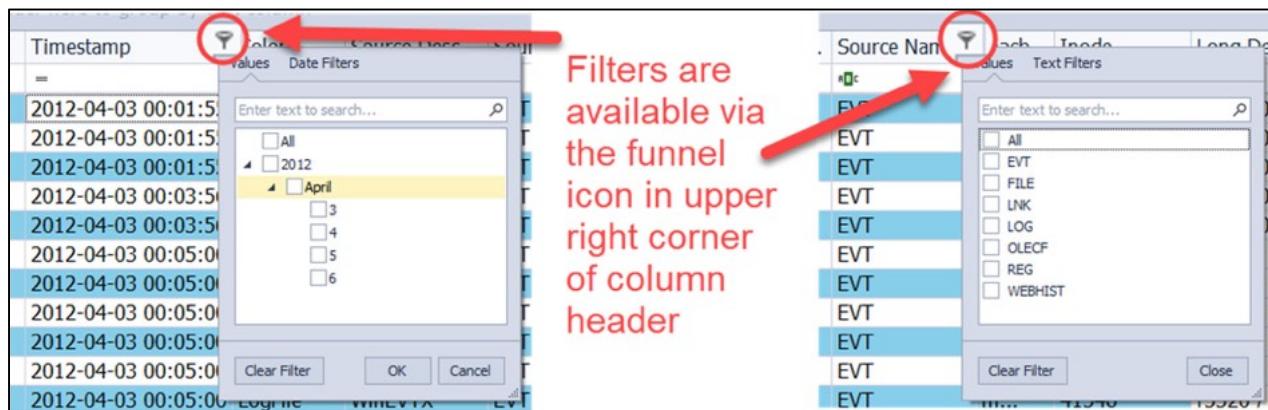
In the example above, the **Source Filename** column was filtered for any string containing '**explorer**' and two results were found.

Notice that you can also edit the current filter via the **Edit filter** button to the right, as well as remove the current filter entirely by clicking the '**X**' to the far left. To temporarily disable the filter, uncheck the box to the right of the '**X**'. Check the box again to re-enable the filter.

Source Filename	Volume1Seri...	Source Created	Source Modifi...	Source Access...	Executable Name
E:\[root]\Windows\Prefetch\EXPLO...	E8D4A909	2013-09-23 21:02:36	2013-10-21 1...	2013-09-23 21...	EXPLORER.EXE
E:\[root]\Windows\Prefetch\Op-EX...		2013-09-23 19:52:04	2013-10-22 1...	2013-09-23 19...	Op-EXPLORER.EXE-319FC3CE

To filter on additional columns, enter the filter criteria into the relevant column header.

In addition to entering in a value to search for, small funnel icons in the column header bring up a list of all unique values in the column.



You can browse the values or use the search box to quickly find what you want to filter by.

The **Search** option allows for filtering on various columns as well. To use **Search**, enter the filter criteria into the box and the data will be filtered across *all rows and columns*.

As an example, using **.exe +CON** results in what is shown below. This filter says "find all that contain .exe AND CON"

	Volume1Seri...	Source Created	Source Modifi...	Source Access...	Executable Name	Run Co
T	h\ICLOUD.EXE-E308F227...	2013-09-23 20:51:49	2013-10-18 1...	2013-09-23 20...	ICLOUD.EXE	=
	ch\WINWORD.EXE-AC543A3...	2013-09-23 20:41:02	2013-10-22 1...	2013-09-23 20...	WINWORD.EXE	
	ch\DWWIN.EXE-BB57490C...	2013-09-23 20:40:45	2013-10-21 2...	2013-09-23 20...	DWWIN.EXE	
	ch\CONSENT.EXE-1A8D066...	2013-09-23 19:47:39	2013-10-23 1...	2013-09-23 19...	CONSENT.EXE	
	ch\OUTLOOK.EXE-FB7CB58...	2013-09-23 19:47:37	2013-10-23 0...	2013-09-23 19...	OUTLOOK.EXE	
	ch\UNINST.EXE-4F2DA603...	2013-10-22 16:52:33	2013-10-22 1...	2013-10-22 16...	UNINST.EXE	
	ch\DLLHOST.EXE-B0C1E77...	2013-10-21 20:40:50	2013-10-21 2...	2013-10-21 20...	DLLHOST.EXE	
	ch\MSTSC.EXE-92424A71...	2013-10-21 20:21:33	2013-10-21 2...	2013-10-21 20...	MSTSC.EXE	
	ch\MAKECAB.EXE-D688311...	2013-10-21 20:10:14	2013-10-21 2...	2013-10-21 20...	MAKECAB.EXE	
	ch\IPCONFIG.EXE-1D6605...	2013-10-21 20:10:14	2013-10-21 2...	2013-10-21 20...	IPCONFIG.EXE	
	ch\RUNDLL32.EXE-40AC00...	2013-10-21 19:36:24	2013-10-21 2...	2013-10-21 19...	RUNDLL32.EXE	
	ch\PLUGIN-CONTAINER.EX...	2013-10-21 20:22:09	2013-10-22 1...	2013-10-21 20...	PLUGIN-CONTAINER.EXE	
	ch\DW20.EXE-5601E6AF.pf	2013-10-21 20:00:33	2013-10-21 2...	2013-10-21 20...	DW20.EXE	
	ch\F-RESPONSE-TACSUB.E...	2013-10-23 02:59:02	2013-10-23 0...	2013-10-23 02...	F-RESPONSE-TACSUB.EXE	
	ch\FVENOTIFY.EXE-CD975...	2013-10-21 20:11:58	2013-10-21 2...	2013-10-21 20...	FVENOTIFY.EXE	

24. **Timeline Explorer** has several search related options, such as filtering vs searching, matching conditions, etc. To access these options, click the **Search options** button and the various options are shown. In the upper right of the **Search** options is a ? icon that, when clicked, provides additional help about searching, such as more examples of how to use search and advanced syntax such as inclusion and exclusion of terms.

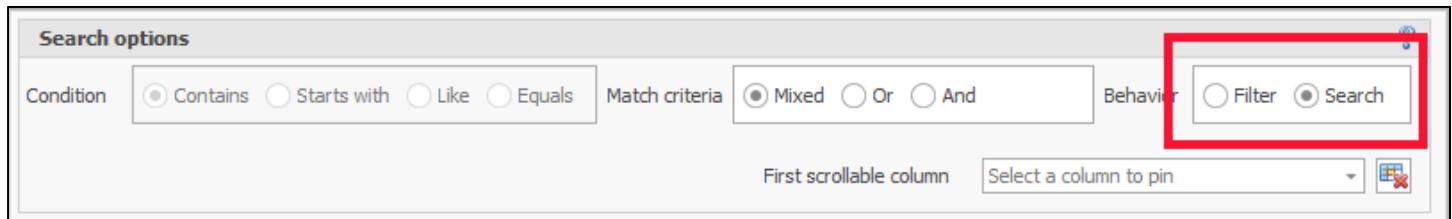
The screenshot shows a CSV file named '\_PECmd\_Output.csv' in the Timeline Explorer interface. A red box highlights the 'Search options' dialog at the top right of the window. This dialog contains fields for 'Condition' (set to 'Contains'), 'Match criteria' (set to 'Mixed'), and 'Behavior' (set to 'Filter'). There is also a 'Search options' button with a question mark icon. Below the dialog, the main pane displays a table with columns: Volume1Serial, File, Date, Time, Duration, and Process. Two rows are visible: one for 'ch\ICLOUD.EXE-E308F227...' and another for 'ch\WINWORD.EXE-AC543A3...'. The bottom status bar shows 'Total lines 242' and 'Visible lines 166'.

25. Grouping is useful to see all the unique values in one or more columns in a file. To group by a column, click and hold the left mouse button on a column header and drag it to the indicated area as shown below.

The screenshot shows the same '\_PECmd\_Output.csv' file in Timeline Explorer. A red arrow points to the 'Executable Name' column header, indicating it is being grouped. The main pane now displays a hierarchical list of executable names. The 'CLEANMGR.EXE' entry is expanded, showing its file path 'E:\[root]\Windows\Prefetch\CLEANMGR.EXE-6FFCB0...' and creation date '2013-09-23 20:25:35'. Other entries like 'CONHOST.EXE', 'CONSENT.EXE', and 'DISPLAYSWITCH.EXE' are also listed. The bottom status bar shows 'Total lines 242' and 'Visible lines 166'.

In the example above, the **Executable Name** column was grouped, and an entry was expanded. Notice how the details for each file are shown after expanding a row. You can also filter as we saw previously, to further drill down into the details.

26. The last piece of functionality to explore is understanding the difference between **Filter** and **Search**. To change between these options, use the **Search options** button. **Search** is different from **Filter** in that when you use **Search**, it will highlight the matches while keeping all rows visible and allow you to jump to each match in the file by pressing the **up** or **down arrow** buttons. Note also the scrollbar shows where in the file hits reside as well.



The screenshot shows the Timeline Explorer interface with a CSV file named '\_PECmd\_Output.csv' loaded. The search bar at the top contains 'host.exe'. The main table lists various executable names found in the prefetch folder. A red box highlights the search bar and the status bar at the bottom right which says 'Total lines 242 | Visible lines 242 | Search options ...'. A red arrow points to the row for 'BULKOPERATIONHOST.EXE'.

Line	Tag	Note	Source	Filename	Executable Name	Volume1Seri...	Source
230				E:\[root]\Windows\Prefetch\AUTHHOST.EXE-7385F8...	AUTHHOST.EXE		2013
26				E:\[root]\Windows\Prefetch\BACKGROUNDTRANSFER...	BACKGROUNDTRANSFERHOST.EXE		2013
55				E:\[root]\Windows\Prefetch\BDEUISRV.EXE-D93D11...	BDEUISRV.EXE		2013
54				E:\[root]\Windows\Prefetch\BDEUNLOCK.EXE-871B5...	BDEUNLOCK.EXE		2013
222				E:\[root]\Windows\Prefetch\BITLOCKERWIZARD.EXE...	BITLOCKERWIZARD.EXE		2013
197				E:\[root]\Windows\Prefetch\BTSERVER.EXE-7279C6...	BTSERVER.EXE		2013
28				E:\[root]\Windows\Prefetch\BULKOPERATIONHOST.E...	BULKOPERATIONHOST.EXE		2013
178				E:\[root]\Windows\Prefetch\CALC.EXE-DBDE74BE.pf	CALC.EXE		2013
113				E:\[root]\Windows\Prefetch\CCLEANER64.EXE-DE05...	CCLEANER64.EXE		2013
153				E:\[root]\Windows\Prefetch\CCSETUP406.EXE-3A4D...	CCSETUP406.EXE		2013
187				E:\[root]\Windows\Prefetch\CHROME.EXE-46AA1511...	CHROME.EXE		2013
185				E:\[root]\Windows\Prefetch\CLEANMGR.EXE-6FFCB0...	CLEANMGR.EXE		2013
184				E:\[root]\Windows\Prefetch\CMD.EXE-8E75B5BB.pf	CMD.EXE		2013
150				E:\[root]\Windows\Prefetch\CNMSEA7.EXE-DBE64A3...	CNMSEA7.EXE		2013
236				E:\[root]\Windows\Prefetch\CONHOST.EXE-E6AFC9F...	CONHOST.EXE		2013

In the above example, 65 instances of **HOST.EXE** were found. The currently selected hit has a border around the cell. If a column filter or **Search options** was in **Filter** mode, all rows that do not contain **HOST.EXE** would be hidden from view.

## Exercise Questions

1. Close any open **PowerShell** windows, then open a new **PowerShell** prompt via the shortcut on the desktop. You should be in the **C:\Tools** directory. Execute the following commands and describe what they do:

- a. Type the following command and press **Enter**. What is shown?

```
dir
```

- 
- b. Type the following command and press **Enter**. What is shown? Does it look the same as what we saw above? Why?

```
Get-ChildItem
```

- 
- 
- c. Type the following command and press **Enter**. Look for **dir** and **ls** in the list. What cmdlet is actually run when these commands are used?

```
alias
```

- 
- 
- d. Note the directory you are currently in. Write it down below, then type the following command and press **Enter**. What directory are you in now?

```
cd ..
```

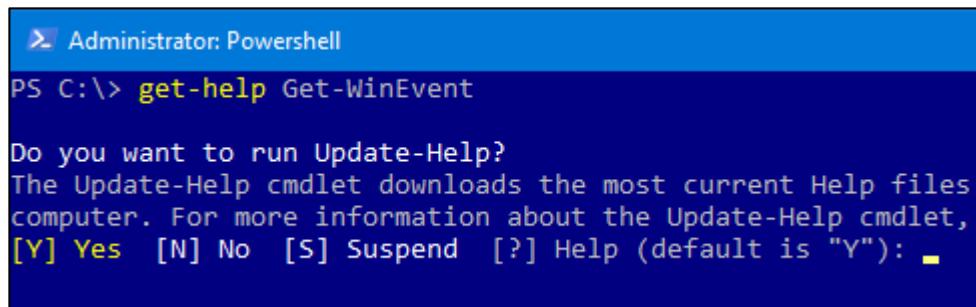
- e. Type the following command and press **Enter**. What cmdlets get returned? Write down a few of them.

```
Get-Command get-w*
```

- 
- 
- f. For any of the commands above, look at the help for the cmdlet by typing **Get-Help <cmdlet>** (An actual example is shown in the box below). Spend a minute reading through the available options.

```
Get-Help Get-ChildItem
```

**NOTE:** If you are prompted to run **Update-Help**, you can do so if you want to update the local **Powershell** help commands. This is generally a good idea to do, however it takes approximately 5 minutes, so should be done out of class.



```
Administrator: Powershell
PS C:\> get-help Get-WinEvent

Do you want to run Update-Help?
The Update-Help cmdlet downloads the most current Help files
from the internet. For more information about the Update-Help cmdlet,
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): ■
```

2. Start **Timeline Explorer** using the shortcut in the **Utilities** fence on the **Desktop**, if it is not already running. Using **Timeline Explorer**, open the CSV files located at **C:\Cases\CSVs** via the **File → Open** menu. Once the file selection dialog is shown, select both files to open them at the same time. Once both files are loaded, answer the following questions:

**NOTE:** We are not so much concerned with understanding all there is to know about the files we are looking at, but rather, we want to use **Timeline Explorer** to interact with data. With that said, the following background will be helpful:

**AppCompatCache** is an evidence of execution artifact that records the full path to an executable as well as the last modified date of the executable. In many cases there is also a flag that tells us if a program was run.

The MFT is the heart of NTFS and contains details like file names, parent path, timestamps, and more. We will dig into NTFS later, but for now, this is enough to look at the data.

Finally, notice you have **TWO** tabs open in **Timeline Explorer**. Click on each tab as necessary in the steps below.

- a. Looking at the **Windows81\_Windows2012R2\_SYSTEM\_AppCompatCache.csv** file, how many **Total lines** are there in the file? How many **Visible lines**?

---

- b. Looking at the **Windows81\_Windows2012R2\_SYSTEM\_AppCompatCache.csv** file, is there any indication that **ffmpeg.exe** was executed? If so, what is the last modified time of the executable?

---

- c. Looking at the **Windows81\_Windows2012R2\_SYSTEM\_AppCompatCache.csv** file, how many entries contain both the words **temp** and **installer**?

---

- d. Looking at the **Windows81\_Windows2012R2\_SYSTEM\_AppCompatCache.csv** file, how many were found on the **J:\** drive?

---

- e. Looking at the **MFTECmd\_\$MFT\_Output.csv** file, how many files and directories exist where the **Parent Path** contains **EdgarAllanPoe**?

---

- f. For the files and directories found in the last question, how many of the files found end in **.doc**?

---

- g. Looking at the **MFTECmd\_\$MFT\_Output.csv** file, how many *files* have a **\$** in their name? How many *directories*?

---

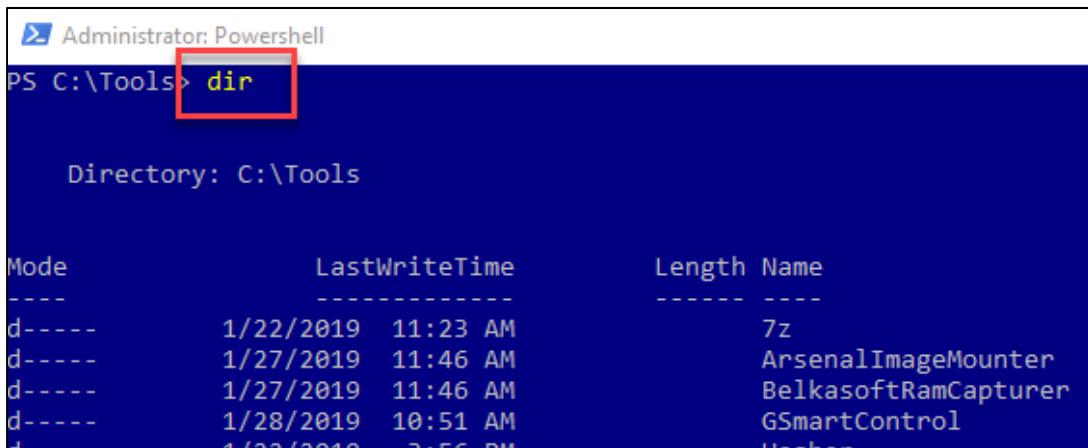
## Exercise Questions with Step-by-Step

1. Close any open **PowerShell** windows, then open a new **PowerShell** prompt via the shortcut on the desktop. You should be in the **C:\Tools** directory. Execute the following commands and describe what they do:

- a. Type the following command and press **Enter**. What is shown?

```
dir
```

Lists the contents of the C:\tools folder.



A screenshot of a Windows PowerShell window titled "Administrator: Powershell". The window shows the command "PS C:\Tools> dir" with a red box highlighting it. Below the command, the output is displayed in a table format:

Mode	LastWriteTime	Length	Name
d----	1/22/2019 11:23 AM	7z	
d----	1/27/2019 11:46 AM		ArsenalImageMounter
d----	1/27/2019 11:46 AM		BelkasoftRamCapturer
d----	1/28/2019 10:51 AM		GSmartControl
	1/28/2019 2:56 PM		WPS...

- b. Type the following command and press **Enter**. What is shown? Does it look the same as what we saw above? Why?

```
Get-ChildItem
```

The same thing as when we ran the previous command. It looks the same because “dir” is simply a pointer to the “Get-ChildItem” cmdlet.

```
PS C:\Tools> Get-ChildItem

Directory: C:\Tools

Mode                LastWriteTime     Length Name
----                -----          ---- 
d-----        1/22/2019 11:23 AM      7z
d-----        1/27/2019 11:46 AM  ArsenalImageMounter
d-----        1/27/2019 11:46 AM  BelkasoftRamCapturer
d-----        1/28/2019 10:51 AM  GSmartControl
d-----        1/22/2019 3:56 PM   Hasher
```

- c. Type the following command and press **Enter**. Look for **dir** and **ls** in the list. What cmdlet is actually run when these commands are used?

```
alias
```

The Get-ChildItem cmdlet is executed.

Note: The output below has been condensed in order to show both aliases at once.

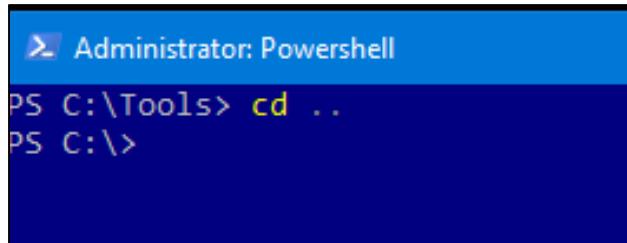
```
PS C:\Tools> alias

 CommandType      Name
 -----          --
 Alias           % -> ForEach-Object
 Alias           del -> Remove-Item
 Alias           diff -> Compare-Object
 Alias           dir -> Get-ChildItem
 Alias           dsn -> Disconnect-PSSession
 Alias           kill -> Stop-Process
 Alias           lp -> Out-Printer
 Alias           ls -> Get-ChildItem
```

- d. Note the directory you are currently in. Write it down below, then type the following command and press **Enter**. What directory are you in now?

```
cd ..
```

Currently we are in the C:\Tools directory. Typing cd .. takes us to the C:\ directory, or one level up from where we were.

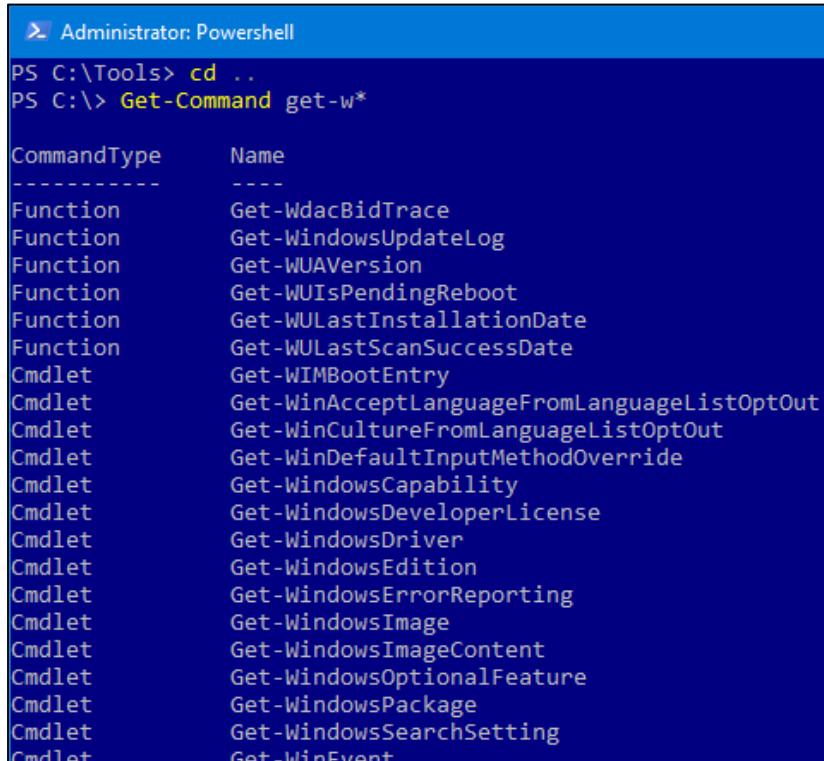


```
Administrator: Powershell
PS C:\Tools> cd ..
PS C:\>
```

- e. Type the following command and press **Enter**. What cmdlets get returned? Write down a few of them.

```
Get-Command get-w*
```

This command brings up a listing of all cmdlets that match the pattern provided. Any of the commands below could be written down for this one.



```
Administrator: Powershell
PS C:\Tools> cd ..
PS C:\> Get-Command get-w*

 CommandType      Name
 ----
 Function          Get-WdacBidTrace
 Function          Get-WindowsUpdateLog
 Function          Get-WUAVersion
 Function          Get-WUIsPendingReboot
 Function          Get-WULastInstallationDate
 Function          Get-WULastScanSuccessDate
 Cmdlet            Get-WIMBootEntry
 Cmdlet            Get-WinAcceptLanguageFromLanguageListOptOut
 Cmdlet            Get-WinCultureFromLanguageListOptOut
 Cmdlet            Get-WinDefaultInputMethodOverride
 Cmdlet            Get-WindowsCapability
 Cmdlet            Get-WindowsDeveloperLicense
 Cmdlet            Get-WindowsDriver
 Cmdlet            Get-WindowsEdition
 Cmdlet            Get-WindowsErrorReporting
 Cmdlet            Get-WindowsImage
 Cmdlet            Get-WindowsImageContent
 Cmdlet            Get-WindowsOptionalFeature
 Cmdlet            Get-WindowsPackage
 Cmdlet            Get-WindowsSearchSetting
 Cmdlet            Get-WinEvent
```

- f. For any of the commands above, look at the help for the cmdlet by typing **Get-Help <cmdlet>** (An actual example is shown in the box below). Spend a minute reading through the available options.

```
Get-Help Get-ChildItem
```

**NOTE:** If you are prompted to run **Update-Help**, you can do so if you want to update the local **Powershell** help commands. This is generally a good idea to do.

```
Administrator: Powershell
PS C:\> get-help Get-ChildItem

Do you want to run Update-Help?
The Update-Help cmdlet downloads the most current Help files
computer. For more information about the Update-Help cmdlet,
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): -
```

2. Start **Timeline Explorer** using the shortcut in the **Utilities** fence on the **Desktop**, if it is not already running. Using **Timeline Explorer**, open the CSV files located at **C:\Cases\CSVs** via the **File → Open** menu. Once the file selection dialog is shown, select both files to open them at the same time. Once both files are loaded, answer the following questions:

**NOTE:** We are not so much concerned with understanding all there is to know about the files we are looking at, but rather, we want to use **Timeline Explorer** to interact with data. With that said, the following background will be helpful:

**AppCompatCache** is an evidence of execution artifact that records the full path to an executable as well as the last modified date of the executable. In many cases there is also a flag that tells us if a program was run.

The MFT is the heart of NTFS and contains details like file names, parent path, timestamps, and more. We will dig into NTFS later, but for now, this is enough to look at the data.

Finally, notice you have **TWO** tabs open in **Timeline Explorer**. Click on each tab as necessary in the steps below.

- Looking at the **Windows81\_Windows2012R2\_SYSTEM\_AppCompatCache.csv** file, how many **Total lines** are there in the file? How many **Visible lines**?

**1024 total lines and 1024 visible lines.**

The screenshot shows the Timeline Explorer interface with two tabs open. The first tab is 'MFTECmd\_\$MFT\_Output.csv' and the second tab is 'Windows81\_Windows2012R2\_SYSTEM\_AppCompatCache.csv', which is currently selected and highlighted with a red box. The main pane displays a table with columns: Control Set, Cache Entr..., Executed, Last Modified Time ..., and Path. The table lists 12 rows of data. At the bottom of the window, the status bar shows 'C:\Cases\CSVs\Windows81\_Windows2012R2\_SYSTEM\_AppCompatCache.csv'. To the right of the status bar, a red box highlights the text 'Total lines 1,024 | Visible lines 1,024'. A red arrow points from this highlighted text towards the bottom center of the table area.

- b. Looking at the **Windows81\_Windows2012R2\_SYSTEM\_AppCompatCache.csv** file, is there any indication that **ffmpeg.exe** was executed? If so, what is the last modified time of the executable?

Yes, and the last modified time of the file is 2015-01-15 19:45:06.

This is found by filtering on the Path column for ffmpeg and verifying that the Executed flag is "Yes". Once filtered, the Last Modified Time is also displayed.

Executed	Last Modified Time ...	Path
Yes	2015-01-15 19:45:06	D:\Dropbox (Personal)\osTriage2\Plugins\__tmp\ffmpeg.exe

- c. Looking at the **Windows81\_Windows2012R2\_SYSTEM\_AppCompatCache.csv** file, how many entries contain both the words **temp** and **installer**?

First, clear any active filters at the bottom of the window by clicking the X in the lower left.

10 entries contain both the word temp and installer. There are several ways to get to this answer, but the Power filter is the easiest. Entering a criteria of temp +installer tells Timeline Explorer to find all entries that contain temp and installer. To find the number of rows, look in the lower right corner again.

Executed	Last Modified Time ...	Path
Yes	2015-02-23 19:33:35	SYSVOL\Users\eric\AppData\Local\Temp\JetPackages\d42b6806-aa:
Yes	2015-02-18 19:39:09	SYSVOL\Users\eric\AppData\Local\Temp\CitrixUpdates\GoToMeetin:
Yes	2015-02-12 23:22:16	SYSVOL\Users\eric\AppData\Local\Temp\CitrixUpdates\GoToMeetin:
Yes	2015-02-12 23:22:09	SYSVOL\Users\eric\AppData\Local\Temp\CitrixUpdates\GoToMeetin:
Yes	2015-02-09 23:02:32	SYSVOL\Users\eric\AppData\Local\Temp\is-KJ7RA.tmp\010EditorW:
Yes	2015-02-09 23:02:32	SYSVOL\Users\eric\AppData\Local\Temp\is-KJ7R9.tmp\010EditorW:
Yes	2015-02-09 23:02:32	SYSVOL\Users\eric\AppData\Local\Temp\is-4D875.tmp\010EditorW:
Yes	2015-02-09 23:02:32	SYSVOL\Users\eric\AppData\Local\Temp\is-VCITT.tmp\010EditorW:
Yes	2015-01-27 04:47:08	SYSVOL\Users\eric\AppData\Local\Temp\CitrixUpdates\GoToMeetin:
Yes	2015-01-14 18:37:11	SYSVOL\Users\eric\AppData\Local\Temp\CitrixUpdates\GoToMeetin:

- d. Looking at the **Windows81\_Windows2012R2\_SYSTEM\_AppCompatCache.csv** file, how many were found on the J:\ drive?

First, clear any active filters at the bottom of the window by clicking the X in the lower left.

16 entries. Filtering on the Path column for J:\ gets you to this answer. The total is in the lower right corner.

Timeline Explorer

File Tools Help

MFTECmd\_\$MFT\_Output.csv Windows81\_Windows2012R2\_SYSTEM\_AppCompatCache.csv

Drag a column header here to group by that column

Enter text to search...

Path

J:\

2014-08-10 16:48:04 J:\ShellBagsExplorer.exe  
 2013-06-07 15:06:04 J:\SetupRegexBuddy3EricPeterson.exe  
 2013-06-10 13:31:14 J:\SetupEditPadLite.exe  
 2014-05-22 14:38:19 J:\PortableRoboForm.exe  
 2014-03-06 19:11:54 J:\osTriage2\_RELEASE.exe  
 2014-12-11 17:40:07 J:\setup.exe  
 2015-01-23 10:00:00 J:\xwfpportable\zip.exe  
 2015-01-23 10:00:00 J:\xwfpportable\WinHex64.exe  
 2015-01-23 10:00:00 J:\xwfpportable\WinHex.exe  
 2015-01-23 10:00:00 J:\xwfpportable\xwforensics.exe  
 2015-01-23 10:00:00 J:\xwfpportable\xwforensics64.exe  
 2015-01-23 10:00:00 J:\xwfpportable\setup.exe  
 2015-01-23 10:00:00 J:\xwfpportable\Indexer.exe  
 2015-01-23 10:00:00 J:\xwfpportable\Indexer64.exe  
 2015-01-23 22:17:26 J:\Windows7-USB-DVD-Download-Tool-Installer-en-US.exe  
 2014-10-30 22:34:32 J:\SanDiskSecureAccessV2\_win.exe

Path Contains J:\ Edit Filter

C:\Cases\CSVs\Windows81\_Windows2012R2\_SYSTEM\_AppCompatCache.csv Total lines 1,024 Visible lines 16 Search options

- e. Looking at the **MFTECmd\_\$MFT\_Output.csv** file, how many files and directories exist where the **Parent Path** contains **EdgarAllanPoe**?

**126 files and directories exist. To get to this answer, filter on the Parent Path column, then check the lower right corner.**

The screenshot shows the Timeline Explorer application window with the following details:

- Title Bar:** Timeline Explorer
- Menu Bar:** File, Tools, Help
- Tab Bar:** MFTECmd\_\$MFT\_Output.csv (highlighted with a red box) and Windows81\_Windows2012R2\_SYSTEM\_AppCompatCache.csv
- Search Bar:** Enter text to search...
- Table Header:** Drag a column header here to group by that column
- Table Columns:** Number, In Use, Parent Path, File Name
- Table Data:** A list of entries where the Parent Path contains "EdgarAllanPoe". Some examples include:
  - 2 .\Documents and Settings\EdgarAllanPoe Outlook.pst
  - 2 .\Documents and Settings\EdgarAllanPoe My Documents
  - 2 .\Documents and Settings\EdgarAllanPoe dxtasy\_x.doc
  - 2 .\Documents and Settings\EdgarAllanPoe dxtasy\_y.doc
  - 2 .\Documents and Settings\EdgarAllanPoe\My Docume... Messages.dbx
  - 2 .\Documents and Settings\EdgarAllanPoe\My Docume... My Pictures
  - 2 .\Documents and Settings\EdgarAllanPoe Local Settings
  - 2 .\Documents and Settings\EdgarAllanPoe\Local Set... Temp
  - 2 .\Documents and Settings\EdgarAllanPoe\Local Set... Temporary Internet Files
  - 2 .\Documents and Settings\EdgarAllanPoe\Local Set... Content.IE5
  - 2 .\Documents and Settings\EdgarAllanPoe\Local Set... desktop.ini
  - 2 .\Documents and Settings\EdgarAllanPoe\Local Set... index.dat
  - 2 .\Documents and Settings\EdgarAllanPoe\Local Set... 0P2NGHQ3
  - 2 .\Documents and Settings\EdgarAllanPoe\Local Set... Messages.txt
  - 2 .\Documents and Settings\EdgarAllanPoe\Local Set... abostern[1].gif
  - 2 .\Documents and Settings\EdgarAllanPoe\Local Set... arrow\_blue\_5x9[1].gif
- Filter Bar:** Contains EdgarAllanPoe (highlighted with a red box)
- Status Bar:** Total lines 638, Visible lines 126, Search options

- f. For the files and directories found in the last question, how many of the files found end in **.doc**?

**2 files.** We can get to this answer by filtering on the Extension column in addition to the Parent Path as in the previous question.

ber	In Use	Parent Path	File Name	Extension	Is D
	<input type="checkbox"/>	EdgarAllanPoe			
2	<input checked="" type="checkbox"/>	.\Documents and Settings\EdgarAllanPoe	dxtasy_x.doc	.doc	
2	<input checked="" type="checkbox"/>	.\Documents and Settings\EdgarAllanPoe	dxtasy_y.doc	.doc	

Drag a column header here to group by that column

Enter text to search...

Parent Path Contains EdgarAllanPoe And Extension Contains .doc

Edit Filter

C:\Cases\CSVs\MFTCmd\_\$MFT\_Output.csv

Total lines 638 | Visible lines 2 | Search options ...

- g. Looking at the **MFTCmd\_\$MFT\_Output.csv** file, how many *files* have a \$ in their name? How many *directories*?

**1 directory and 20 files.** First, filter on File Name for \$. Next, you can either use the Is Directory column to filter for where this is true (directory count) and false (file count) and look in the bottom corner.

The other option is to group by Is Directory. To do this, left-click, hold, and drag the Is Directory column to the Drag a column header here to group by that column area.

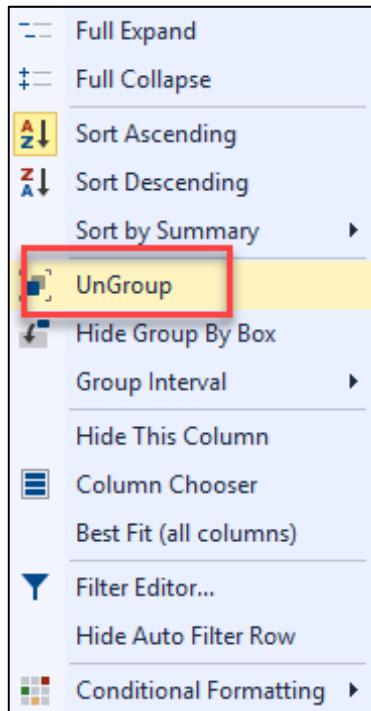
h	File Name	Extension	Is Directory	Ha
	\$		<input type="checkbox"/>	

There will now be two groups shown, one where Is Directory is true and one where it is false. The count at the end is the number of items in each group.

The screenshot shows a Timeline Explorer interface with two tabs: 'MFTECmd\_\$MFT\_Output.csv' and 'Windows81\_Windows2012R2\_SYSTEM\_AppCompatCache.csv'. The 'Is Directory' column is highlighted with a red box. The first row under this column has its 'Is Directory' entry checked (unchecked). The second row has its 'Is Directory' entry checked (checked). A red box highlights these two rows. The 'File Name' column shows entries like '\$' and 'AppCompatCache.dll'.

Line	Tag	Entry Number	Sequence Number	Parent Entry Number	File Name
Y	=	□	=	=	\$
	> Is Directory:	Unchecked (Count=20)			
	> Is Directory:	Checked (Count=1)			AppCompatCache.dll

To undo the grouping, drag the Is Directory column back down into the main group. You can also right-click on the Is Directory entry and choose UnGroup.



## Exercise—Key Takeaways

- Having a properly configured environment allows for consistency and being able to see all available files, especially those that are of forensic interest (and are hidden by default).
- Many forensic tools are command line driven, so being comfortable with both Windows and Linux command line interfaces is necessary.
- Many computer forensic tools output data into CSV format. By leveraging the capabilities of Timeline Explorer, interacting with this data becomes much easier to do.

This page intentionally left blank.

# © SANS Institute 2020

## Exercise 3.1—RAM Acquisition & Encrypted Media

### Background

In most incident response (IR) scenarios, you will need to quickly determine which data to collect, or at least which data to prioritize. This will often be a combination of both memory and files from one or more volumes. During this process, it is critical to always collect data in a way that considers the volatility of the data being collected. In other words, memory changes more often than files on a hard drive. Because of this, one of the first things typically done in IR is to collect Random Access Memory (RAM) from a running system, and then collect files from the hard drive.

Another thing to consider is whether the hard drive content is encrypted or not. This fact will decide whether you must do a full disk image or a triage collection, because if a hard drive is encrypted and is powered off, the contents of the drive will not be available again unless the password is made known somehow. Because of this, it is critical to check for signs of encryption and, if any encryption is found, take the appropriate steps to ensure the data stored on the hard drive is properly collected.

### Objectives

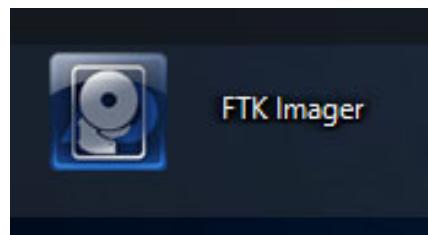
- Image Random Access Memory (RAM) on both a live and virtual system
  - Using FTK Imager
  - Using Comae Dumpl
- Use EDD to check for evidence of encryption on a live system and in a VM

### Exercise Preparation

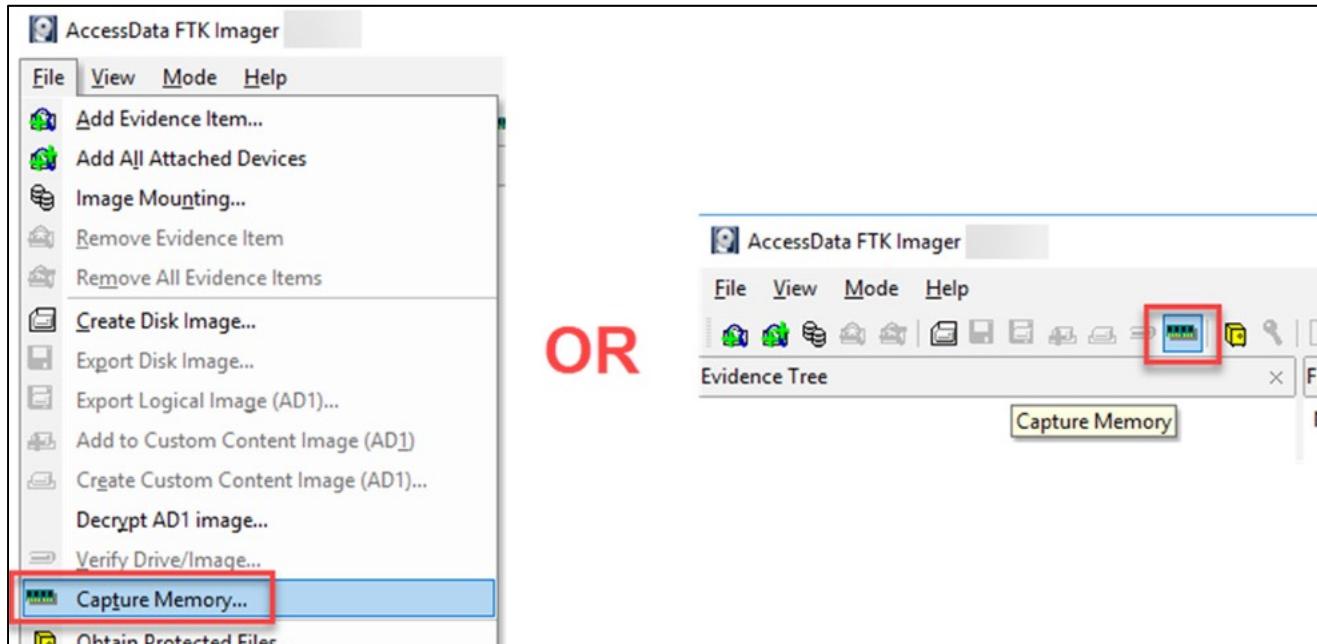
1. Boot your **FOR498 Windows VM**
2. Login to the **FOR498 Windows VM** using the following credentials:
  - a. Username: **SANSDFIR**
  - b. Password: **forensics**

**NOTE:** Normally you would run your collection tools from external media. You would also save the results of your collection to external media. For class purposes, we will launch our collection tools from either your host system or the **VM**.

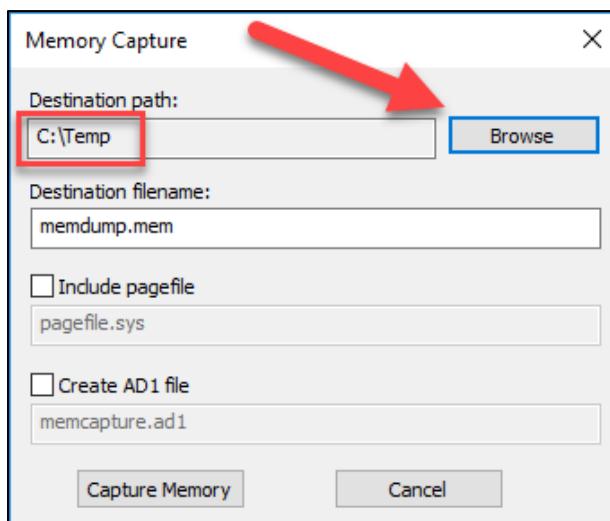
3. Start **FTK Imager** by double clicking the icon in the **Acquisition Tools** fence on the **Desktop**.



4. To start the memory imaging process, use either **File | Capture Memory** or click the **Capture Memory** button on the toolbar. Both options are shown below.

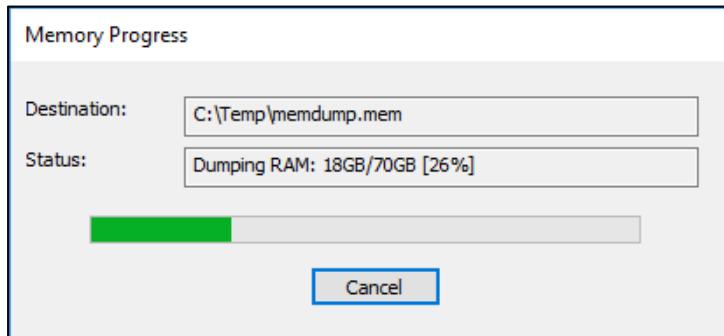


5. In the **Memory Capture** dialog, click the **Browse** button and select **C :\Temp** as the **Destination path** (If you do not have a **C:\Temp** directory, create one). You can optionally create a new directory under **C:\Temp**, such as **C:\Temp\MemoryCapture**, if you like.



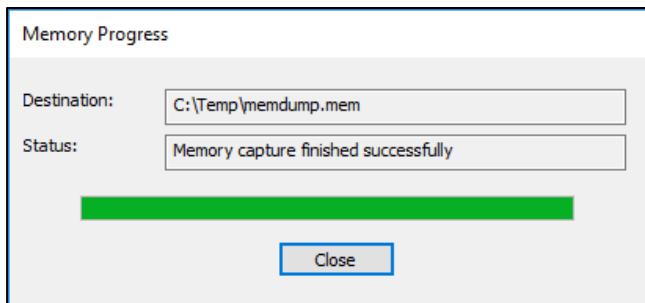
**NOTE:** You would never save a memory capture to the computer you are collecting RAM from, but for classroom purposes, this will suffice. You normally would set the Destination path to an external device such as an external hard drive, network location, or USB drive.

6. Leaving **Include pagefile unchecked**, click the **Capture Memory** button to begin the collection process.
7. A progress bar will be displayed indicating the status of the capture.



The speed of the memory capture depends on several factors, including the amount of memory in the machine being collected and the speed of the device the data is being written to. The time can range from several minutes to hours depending on the configuration being used.

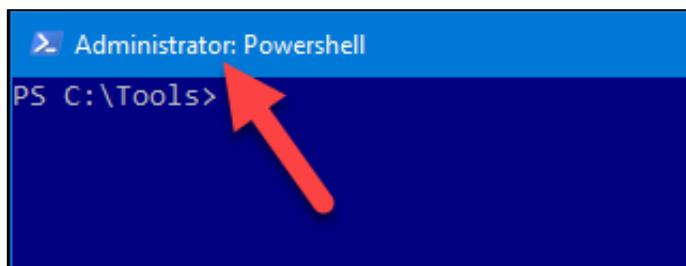
8. When the collection is finished, a summary dialog is displayed.



9. Click the **Close** button to return to the main **FTK Imager** interface.

### RAM Acquisition with DumpIt

10. On your **VM**, open a new **PowerShell** window using the shortcut on the **Desktop**. Verify you are running as an Administrator, as we need admin rights to capture memory.



11. Navigate to the C:\Tools directory (if you are not already there) and type .\DumpIt.exe /?

```
.\DumpIt.exe /?
```

```
PS C:\Tools> .\DumpIt.exe /?
```

```
DumpIt [REDACTED]
Copyright (C) 2007 - 2017, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2012 - 2014, MoonSols Limited <http://www.moonsols.com>
Copyright (C) 2015 - 2017, Comae Technologies FZE <http://www.comae.io>
Copyright (C) 2017 - 2018, Comae Technologies DMCC <http://www.comae.io>

Usage: DumpIt [Options] /OUTPUT <FILENAME>

Description:
    Enables users to create a snapshot of the physical memory as a local file.

Options:
    /TYPE, /T           Select type of memory dump (e.g. RAW or DMP) [default: DMP]
    /OUTPUT, /O          Output file to be created. (optional)
    /QUIET, /Q           Do not ask any questions. Proceed directly.
    /NOLYTICS, /N       Do not send any usage analytics information to Comae Technologies.
    This is used to improve our services.
    /NOJSON, /J          Do not save a .json file containing metadata. Metadata are the basic
    information you will need for the analysis.
    /LIVEKD, /L          Enables live kernel debugging session.
    /COMPRESS, /R         Compresses memory dump file.
    /APP, /A             Specifies filename or complete path of debugger image to execute.
    /CMDLINE, /C          Specifies debugger command-line options.
    /DRIVERNAME, /D        Specifies the name of the installed device driver image.
```

**DumpIt** provides many options to customize the collection. By default, running **DumpIt.exe** without any command line arguments will use the defaults and ask questions along the way.

12. In the **PowerShell** window, type the following command and press **Enter** to start a default collection.

```
.\DumpIt.exe
```

Notice how the **Destination path** reflects the computer name by default. The **/output** switch can be used to provide your own name for the dump file if needed.

**NOTE:** On computers with a large amount of memory, **DumpIt** will offer to enable compression. Enable this at your discretion. When using compression, you may need to convert the dump file to an uncompressed version for certain tools to work properly.

```
> Administrator: Powershell
PS C:\Tools> .\DumpIt.exe

DumpIt
Copyright (C) 2007 - 2017, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2012 - 2014, MoonSols Limited <http://www.moonsols.com>
Copyright (C) 2015 - 2017, Comae Technologies FZE <http://www.comae.io>
Copyright (C) 2017 - 2018, Comae Technologies DMCC <http://www.comae.io>

Destination path: \??\C:\Tools\SANS-FOR498-SIF-20190130-201709.dmp
Computer name: SANS-FOR498-SIF

--> Proceed with the acquisition ? [y/n] _
```

The output on your system will look different than what is shown above.

Press **y** to start the acquisition.

**y**

- At this point, the collection is underway. This step may take several minutes depending on several factors including the amount of memory being collected and the device the dump file is being written to.

```
[+] Information:
Dump Type: Microsoft Crash Dump

[+] Machine Information:
Windows version: [REDACTED]
MachineId: EF169E34-6528-3F0B-F5FE-B06EBFBA7380
TimeStamp: 131818426946786070
Cr3: 0x1ad002
KdCopyDataBlock: 0xfffffff801d585762c
KdDebuggerData: 0xfffffff801d59b0520
KdpDataBlockEncoded: 0xfffffff801d59e7f28

Current date/time: [REDACTED] (YYYY-MM-DD) [REDACTED] (UTC)]
+ Processing... _
```

You can interrupt the collection at any time by pressing **CTRL-C** in the command window. Rather than wait for the processing to finish, cancel the collection now and move on to the next stage of the exercise.

**NOTE:** Interrupting the process results in a partial memory capture, so delete the partial capture if you do interrupt it.

**OPTIONAL EXERCISE:** Repeat the collection process using **BelkaSoft Ram Capture** and compare the time it took between this tool and **FTK Imager**. There are shortcuts in the **Acquisition Tools** fence on the **Desktop** or you can manually start it via the **C:\Tools\BelkasoftRamCapturer** directory. Use the 64-bit version on the **VM**.

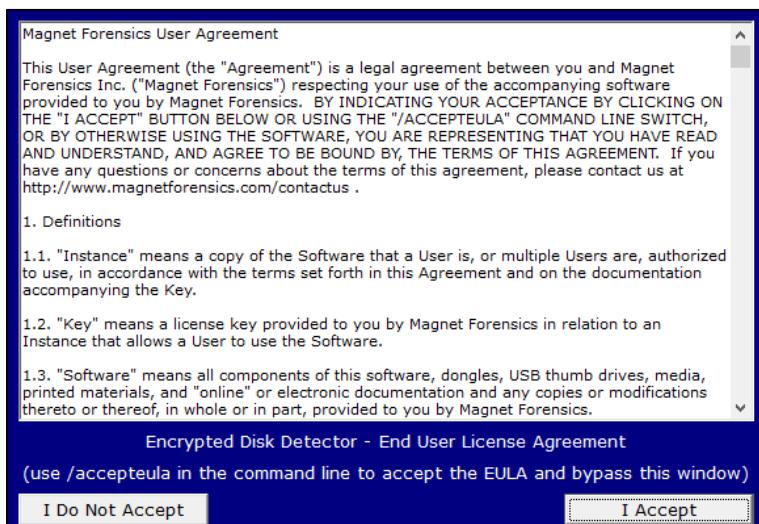
### Exercise Questions

- Referencing the **PowerShell** window where **Dumplit** was running, answer the following question:

- What is the computer name being collected?
- 

**NOTE:** If you are using a Mac host computer, the following program will not work. Skip to **step 10**.

- On the **host computer**, verify you have a **C:\Temp** directory. If not, create it.
- On the **VM**, use **File Explorer** and navigate to **C:\Tools**. Select **EDD.exe**, then press **CTRL-C** to copy it to the clipboard.
- On the **host computer**, use **File Explorer** to navigate to **C:\Temp**, then press **CTRL-V** to copy **EDD.exe** to the **host computer**.
- On your **host computer**, open a new **PowerShell** window **with administrative rights**.
- EDD** is a command line tool. If we run **EDD.exe** without any command line switches, we will be prompted to accept the EULA, as shown below. This also happens if you double-click **EDD.exe**.

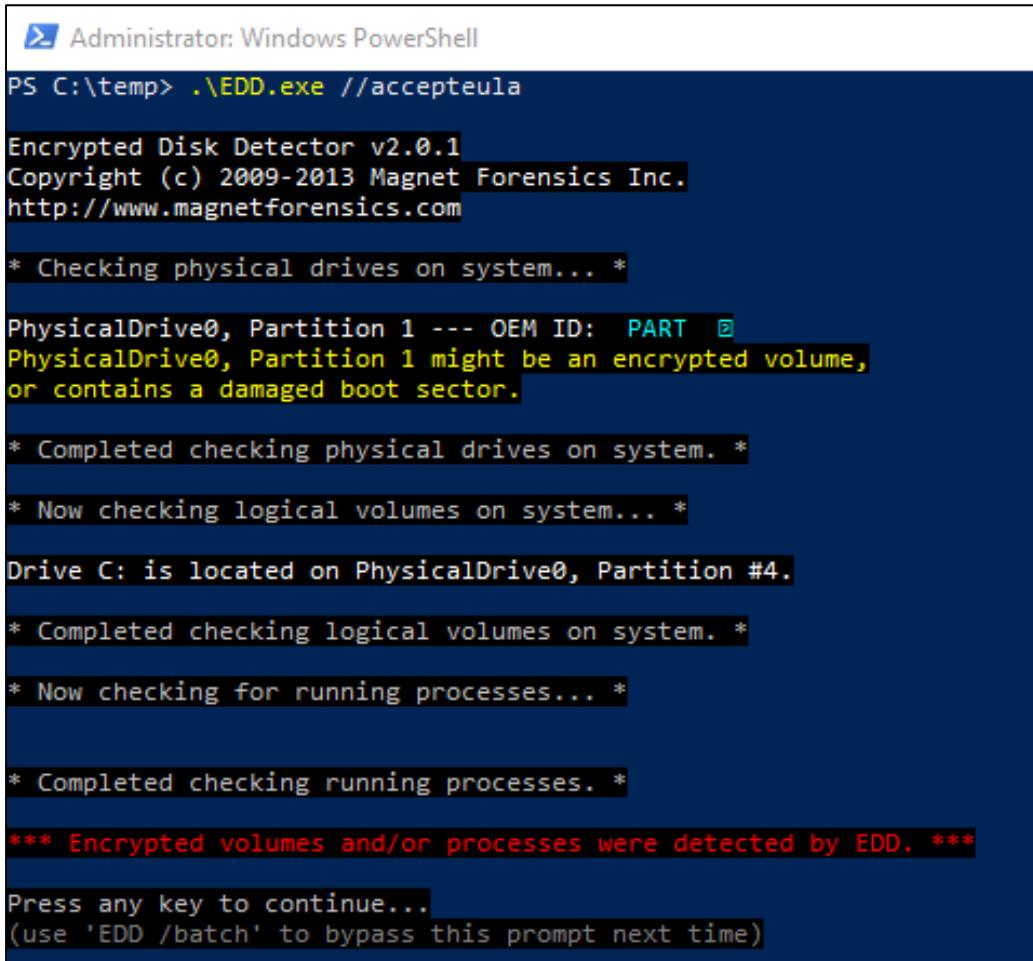


We do not want to have to deal with this every time we use **EDD**, however. We can avoid the dialog box by using the **//accepteula** switch when **EDD** is run.

7. Run the following command:

```
.\EDD.exe //accepteula
```

8. **EDD** will then check the system for signs of encryption (your output will vary from what is shown below).



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell" running on a Windows system. The command ".\EDD.exe //accepteula" is entered at the prompt. The output is as follows:

```
PS C:\temp> .\EDD.exe //accepteula

Encrypted Disk Detector v2.0.1
Copyright (c) 2009-2013 Magnet Forensics Inc.
http://www.magnetforensics.com

* Checking physical drives on system...

PhysicalDrive0, Partition 1 --- OEM ID: PART 0
PhysicalDrive0, Partition 1 might be an encrypted volume,
or contains a damaged boot sector.

* Completed checking physical drives on system. *

* Now checking logical volumes on system... *

Drive C: is located on PhysicalDrive0, Partition #4.

* Completed checking logical volumes on system. *

* Now checking for running processes... *

* Completed checking running processes. *

*** Encrypted volumes and/or processes were detected by EDD. ***

Press any key to continue...
(use 'EDD /batch' to bypass this prompt next time)
```

9. Review the output from **EDD** on your host system. Record any information related to any detected encryption in the space below.

---

---

---

---

10. Next, on your **Virtual Machine**, open a new **PowerShell** window using the shortcut on the **Desktop**.

11. Run **EDD.exe** on your VM in the same manner as you did on your host machine.

```
. \EDD.exe //accepteula
```

12. Review the output from **EDD** on your **VM** system. Record any information related to any detected encryption in the space below.

---

---

---

---

13. Compare the output from your host computer and the **VM** and answer the following questions:

a. Were there any differences in the types of encryption detected?

---

b. What would you have to do differently if you found encryption running on the host system?

---

c. What would you have to do differently if you found encryption running on the **VM** system?

---

**Exercise Questions with Step-by-Step**

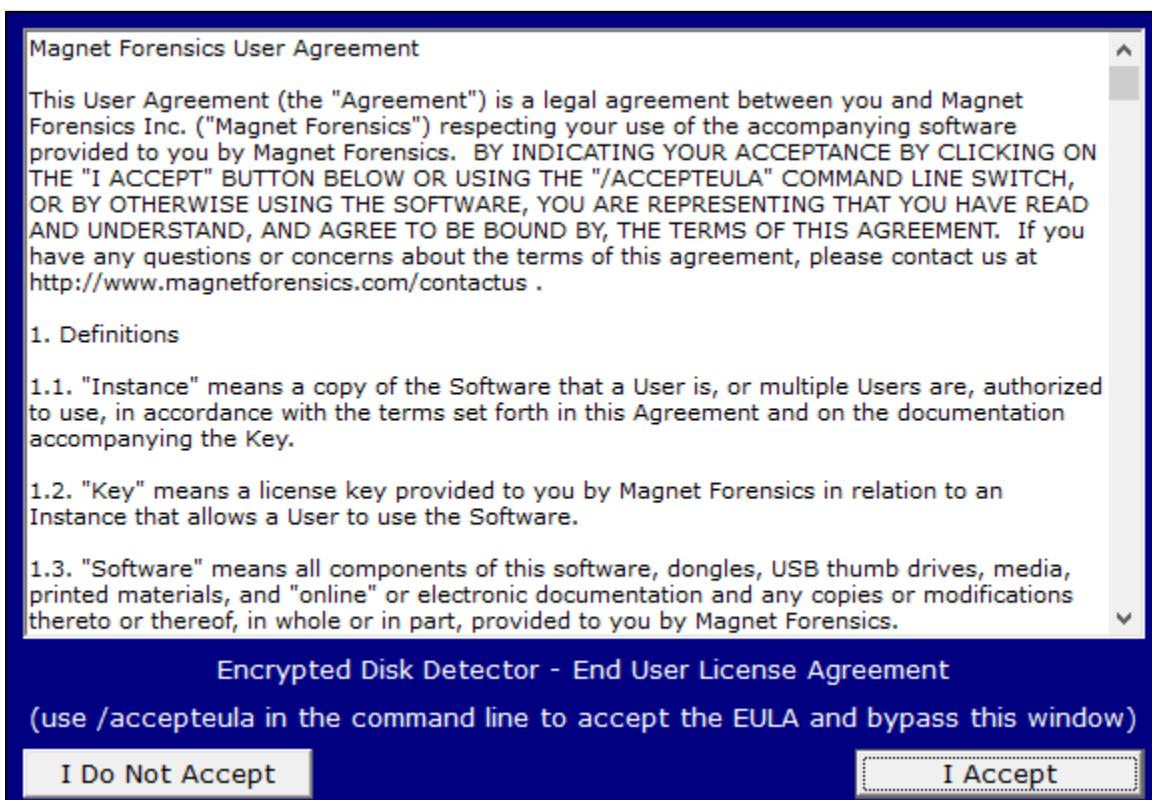
1. Referencing the **PowerShell** window where **DumpIt** was running, answer the following question:

- What is the computer name being collected?

**SANS-FOR498-SIF**

**NOTE:** If you are using a Mac host computer, the following program will not work. Skip to **step 10**.

- On the **host computer**, verify you have a **C:\Temp** directory. If not, create it.
- On the **VM**, use **File Explorer** and navigate to **C:\Tools**. Select **EDD.exe**, then press **CTRL-C** to copy it to the clipboard.
- On the **host computer**, use **File Explorer** to navigate to **C:\Temp**, then press **CTRL-V** to copy **EDD.exe** to the **host computer**.
- On your **host computer**, open a new **PowerShell** window **with administrative rights**.
- EDD** is a command line tool. If we run **EDD.exe** without any command line switches, we will be prompted to accept the EULA, as shown below. This also happens if you double-click **EDD.exe**.



We do not want to have to deal with this every time we use **EDD** however. We can avoid the dialog box by using the **//accepteula** switch when **EDD** is run.

7. Run the following command:

```
.\EDD.exe //accepteula
```

8. **EDD** will then check the system for signs of encryption (your output will vary from what is shown below).

The screenshot shows the output of the EDD.exe //accepteula command in an Administrator Powershell window. The output details the scanning process for physical drives and logical volumes, confirming NTFS file systems and identifying drives C, D, and E. It also states that no TrueCrypt, PGP, BitLocker, or other specified encrypted volumes were found. A final prompt asks the user to press any key to continue.

```
Administrator: Powershell
PS C:\Tools> .\EDD.exe //accepteula

Encrypted Disk Detector
Copyright (c) 2009-2013 Magnet Forensics Inc.
http://www.magnetforensics.com

* Checking physical drives on system... *

PhysicalDrive0, Partition 1 --- OEM ID: NTFS
PhysicalDrive0, Partition 2 --- OEM ID: NTFS

* Completed checking physical drives on system. *

* Now checking logical volumes on system... *

Drive C: is located on PhysicalDrive0, Partition #1.
Drive D: is a CD-ROM/DVD device (#0).
Drive E: is located on PhysicalDrive1, Partition #1.

* Completed checking logical volumes on system. *

* Now checking for running processes... *

* Completed checking running processes. *

*** No TrueCrypt, PGP, BitLocker, SafeBoot, BestCrypt, Checkpoint, Sophos, or
Symantec encrypted volumes detectable by EDD were found. ***

Press any key to continue...
(use 'EDD /batch' to bypass this prompt next time)
```

9. Review the output from **EDD** on your host system. Record any information related to any detected encryption in the space below.

**There is no encryption detected based on the information shown above.**

10. Next, on your **Virtual Machine**, open a new **Powershell** window using the shortcut on the **Desktop**.

11. Run **EDD.exe** on your **VM** in the same manner as you did on your host machine.

```
. \EDD.exe //accepteula
```

12. Review the output from **EDD** on your **VM** system. Record any information related to any detected encryption in the space below.

**On the SIFT VM, no encrypted volumes were found, as shown in the following screenshot.**

```
* Completed checking running processes. *

*** No TrueCrypt, PGP, BitLocker, SafeBoot, BestCrypt, Checkpoint, Sophos, or
Symantec encrypted volumes detectable by EDD were found. ***

Press any key to continue...
(use 'EDD /batch' to bypass this prompt next time)
```

13. Compare the output from your host computer and the **VM** and answer the following questions:

a. Were there any differences in the types of encryption detected?

**No**

b. What would you have to do differently if you found encryption running on the host system?

**Capturing memory would be ideal in case we can later extract any encryption keys in use.**

**Image the device in its running state to collect the data from any encrypted volumes in their unencrypted states. It would be important to image the logical partitions vs. the physical drive in this case as well.**

c. What would you have to do differently if you found encryption running on the **VM** system?

**The same as answer b. In addition, we could take a snapshot of the VM in order to preserve the system in its current state.**

## **Exercise—Key Takeaways**

- Memory capture is an event that an incident responder will typically only get one opportunity to perform. Having multiple tools like FTK Imager and Dumpit provides several avenues for memory collection.
- Once memory is collected, due diligence should be done to check for disk encryption.
- When encryption is located, appropriate steps need to be taken to preserve the data in its current, unencrypted state before shutting down the computer.

This page intentionally left blank.

# © SANS Institute 2020

## Exercise 3.2—Mounting Evidence & Manual Extraction

### Background

Once a forensic image of a hard drive is created, we need a way to access the data contained therein. While many forensic tools offer the ability to ingest image files, in some cases you will want to access an image file to copy out certain, specific files, and using a full forensic suite would be overkill.

Luckily, we have a tool that can mount image files in such a way as to emulate a true, physical disk. This is important because Windows will only expose things like Volume Shadow Copies when a physical disk is connected. In some cases, we will want to manipulate permissions for files in an image but want to do so while protecting the integrity of the image file.

In this lab, we will mount an E01 file and manually explore it to locate key artifacts and then copy them out to a different directory. Once the files are copied, we will extract information related to evidence of execution from one of these artifacts. This will give us a feel for what is possible while at the same time understanding how much is involved with manually triaging forensic images.

Finally, once the data is extracted from the forensic artifact, we will perform analysis using Timeline Explorer to rapidly zero in on key data.

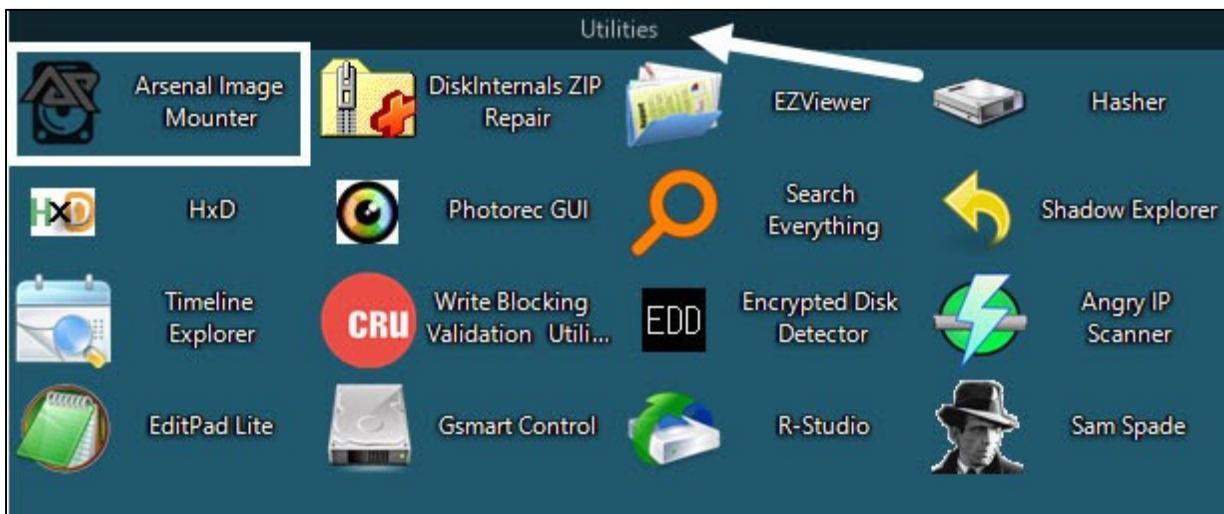
### Objectives

- Use Arsenal Image Mounter to mount and access an E01 image file
- Browse a mounted image and interact with different locations of the file system
- Manually locate and copy key artifacts from mounted device
- Use PECmd to process prefetch files and generate a CSV for analysis
- Use Timeline Explorer to review the CSV output from PECmd

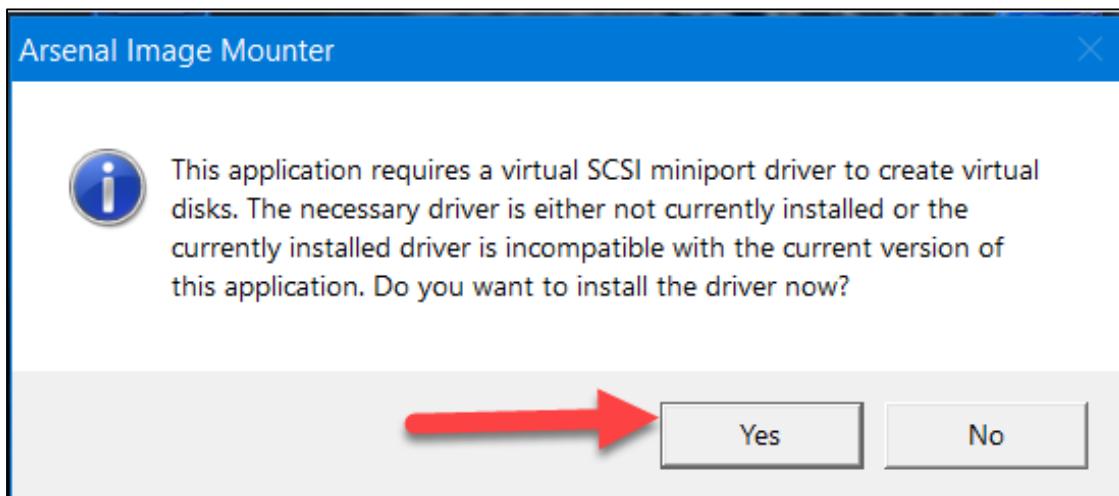
### Exercise Preparation

1. Boot your **FOR498 Windows VM**
2. Login to the **FOR498 Windows VM** using the following credentials:
  - a. Username: **SANSDFIR**
  - b. Password: **forensics**

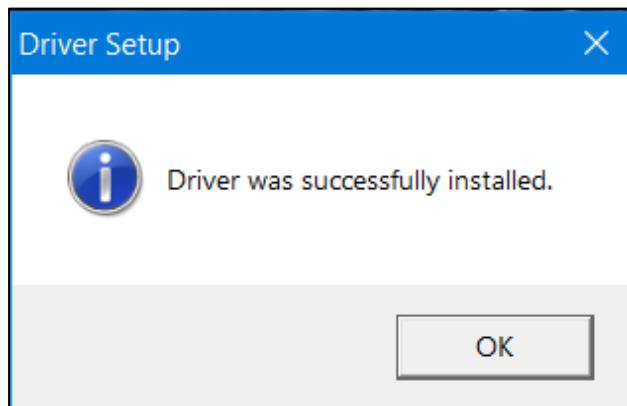
- Double click the AIM icon in the Utilities fence on the desktop to start **Arsenal Image Mounter**.



- If this is the first time you are starting **AIM**, it may prompt you to install the driver. If you update **AIM**, it may ask you to update the driver. In either case, let **AIM** update itself.



Which then shows this confirmation dialog.



- When the splash screen appears, click **OK** to go to the main menu.

**ARSENAL IMAGE MOUNTER** 

Brought to you by the developers of [Registry Recon](#)

**ARSENAL RECON**

Arsenal Image Mounter source code and APIs are available for royalty-free use by open source projects. Commercial projects must obtain alternative licensing. Contact [Arsenal Recon](#) for more information.

**No License Detected - Free Mode Enabled**

Arsenal Image Mounter is currently running in Free Mode which supports basic mounting of various disk image formats. For additional functionality, including mounting Volume Shadow Copies and launching virtual machines, please [upgrade to Professional Mode](#).

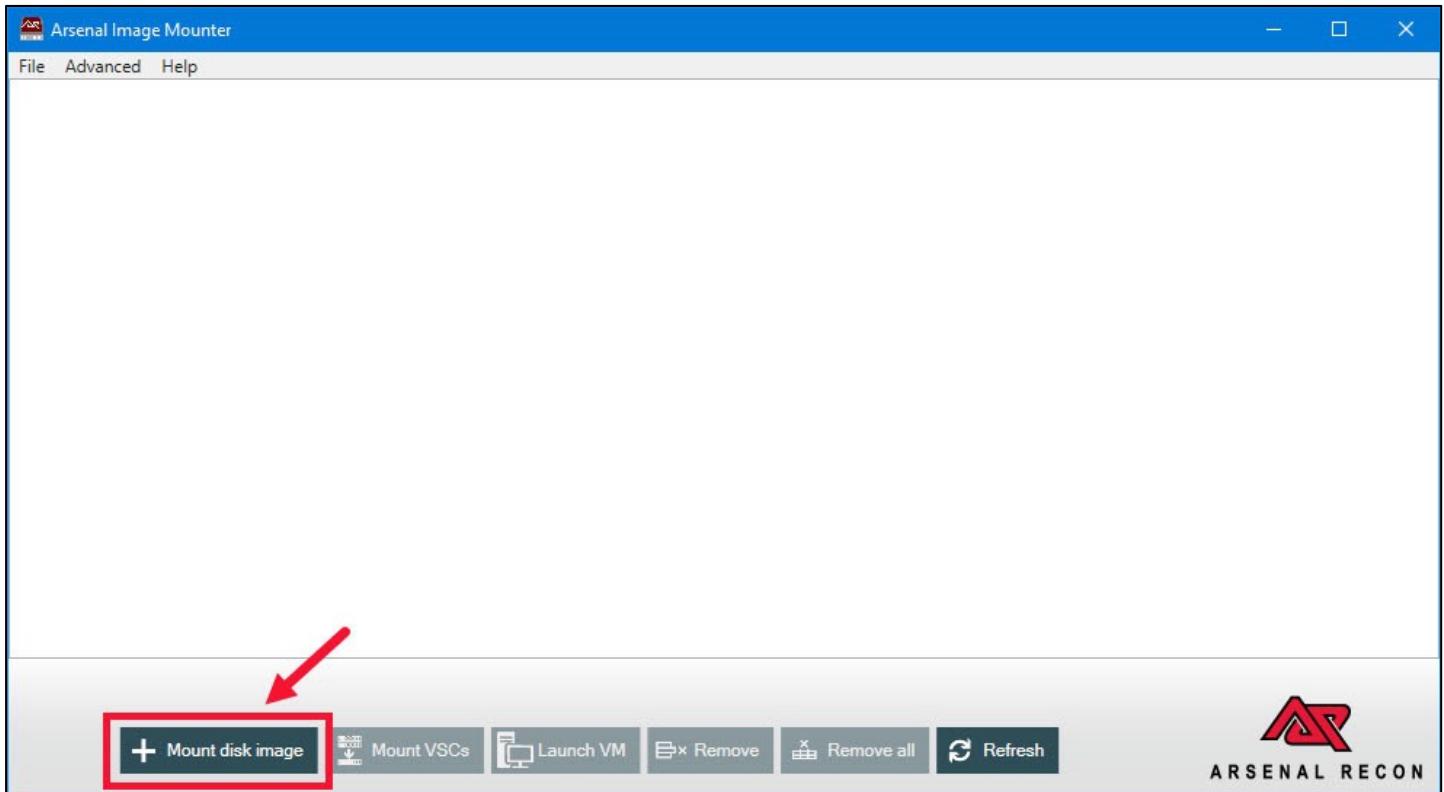
For digital forensics consulting services, contact [Arsenal Consulting](#).

**Disclaimer**

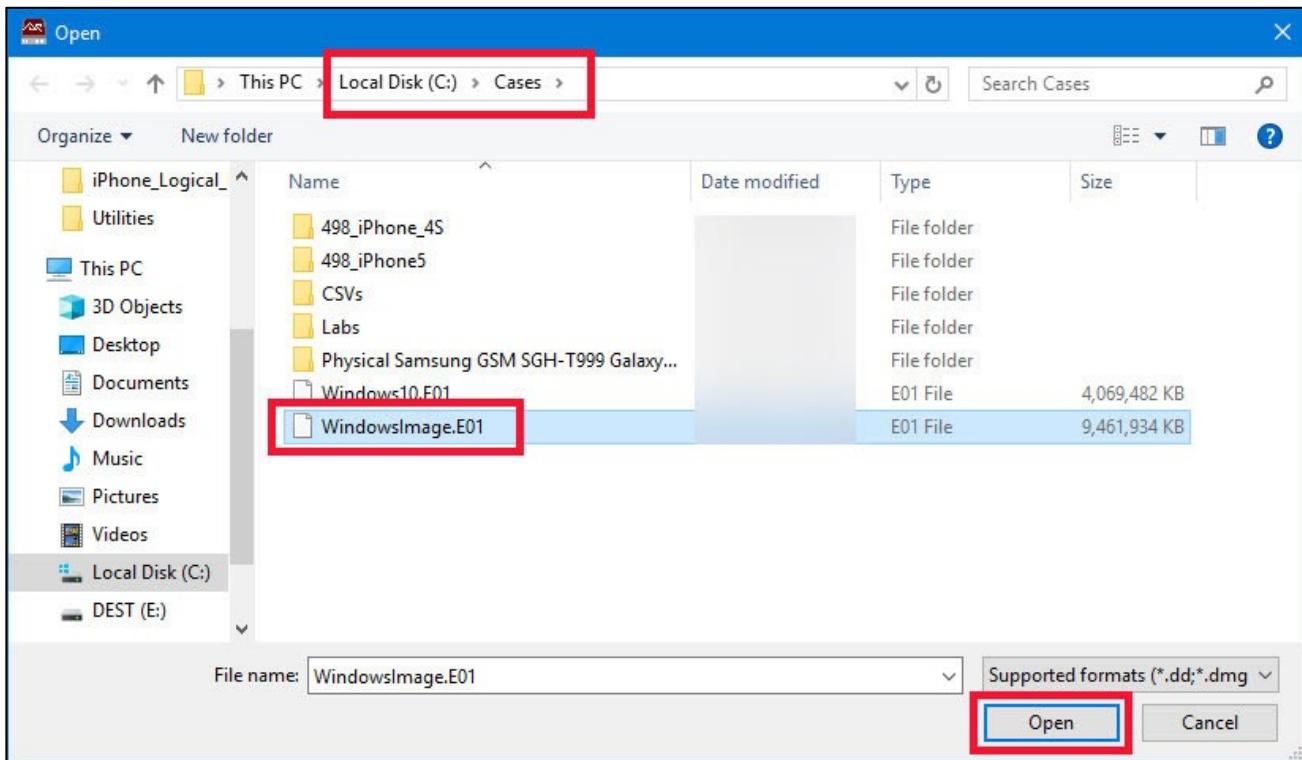
Arsenal Image Mounter ("the Software") is provided "AS IS" and "WITH ALL FAULTS," without warranty of any kind, including without limitation the warranties of merchantability, fitness for a particular purpose and non-infringement. Arsenal Consulting, Inc. (d/b/a "Arsenal Recon") makes no warranty that the Software is free of defects or is suitable for any particular purpose. In no event shall Arsenal Consulting, Inc. be responsible for loss or damages arising from the installation or use of the Software, including but not limited to any indirect, punitive, special, incidental or consequential damages of any character including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses. The entire risk as to the quality and performance of the Software is borne by you. Should the Software prove defective, you and not Arsenal Consulting, Inc. assume the entire cost of any service and repair.

**OK**   **Enter license**   **Acknowledgments**

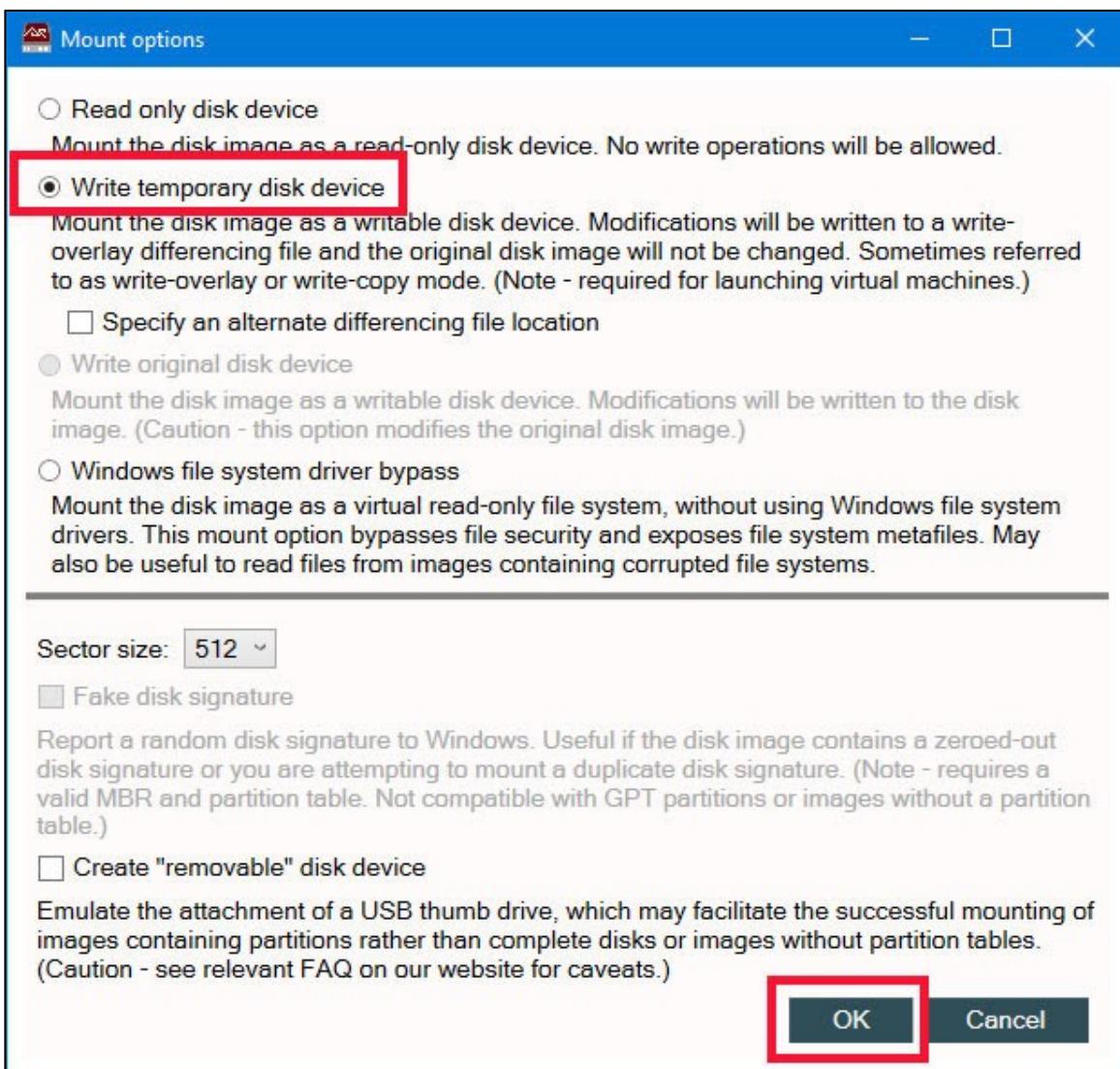
6. The main interface will now be displayed. To mount an image, click the **Mount Image** button on the lower left.



7. Navigate to C:\Cases and select the image named **WindowsImage.E01**. Click **Open**.



8. In the **Mount options** dialog, select the **Write temporary disk device** option via the radio button, then click **OK**.

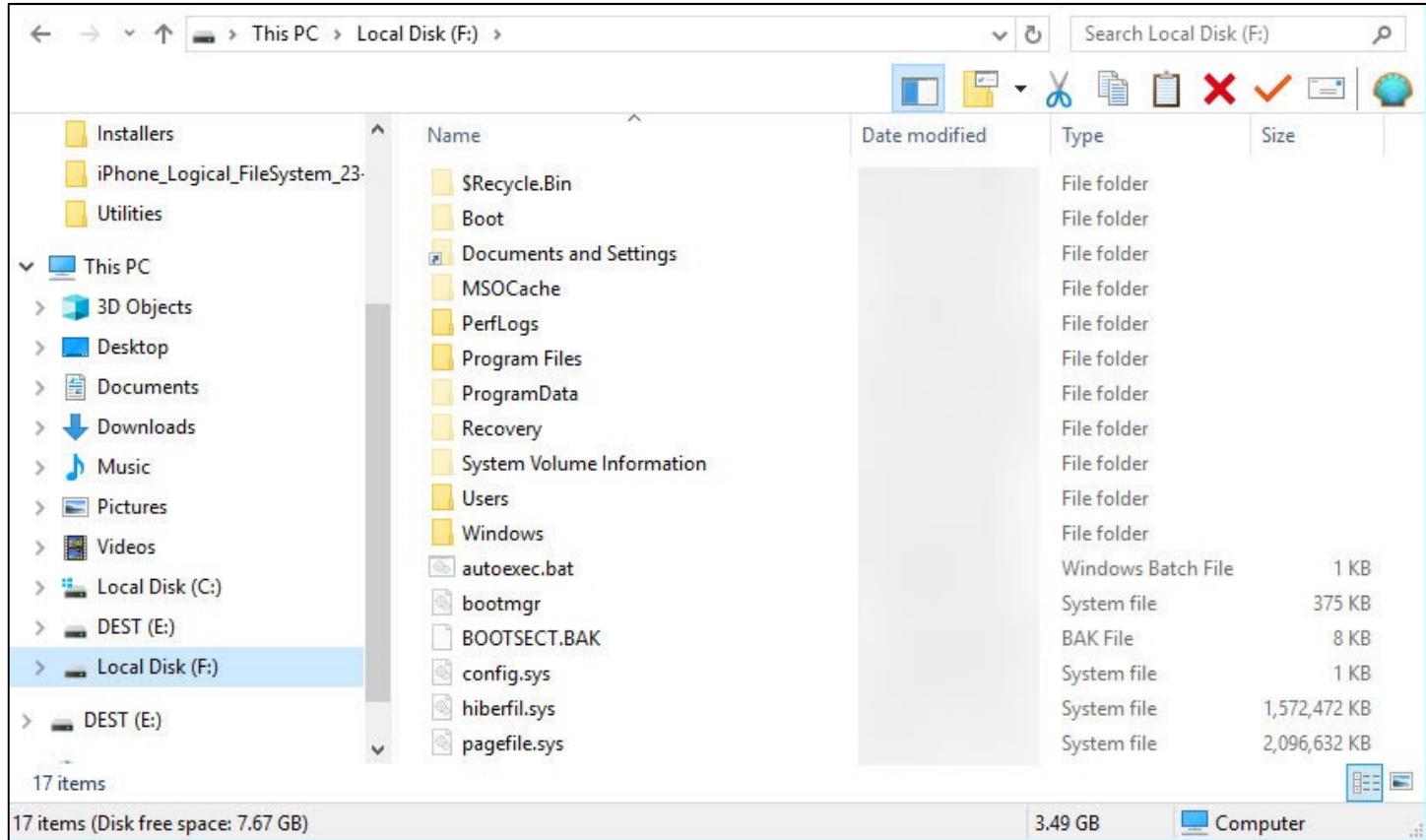


9. AIM will now mount the image and make it available to Windows. To see details, click on the + sign next to the mounted E01 in the main interface. In the example below, the image has been mounted as E:\, as seen in the lower left portion of the details.

C:\Cases\WindowsImage.E01							
Id:	000000	Disk device:	PhysicalDrive2	Signature:	EE80D3E5 (faked)	Read/write:	Write temporary
Online/Offline:	Online	Partition layout:	MBR	Disk size:	24.753 GB	Fixed/removable:	Fixed disk
Volumes:	W:\Volume{ee80d3e5-0000-0000-010000000000}\ (4 Volume Shadow Copies)						
Mount points:	F:\						

**Click + sign to expand mounted device details**

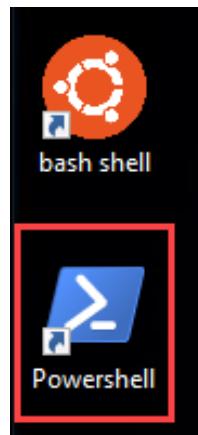
10. Open **File Explorer** and navigate to the drive letter where AIM mounted the image. It should look similar to what is shown below.



11. You now have full access to the Windows file system contained in the E01.

**NOTE:** Use **PowerShell**. **File Explorer** may not let you into every folder, even with administrative rights. It is just a nuance of using **File Explorer**. You CAN, however, navigate anywhere via **PowerShell**.

12. Open a **PowerShell** prompt using the shortcut on the **Desktop**.



## 13. Change directories to &lt;Drive letter&gt;:\Windows\System32\config

For example, if **AIM** mounted the E01 file to the E:\ drive, use the following command:

```
cd E:\Windows\System32\config
```

Verify the drive letter you need to use by looking at the **AIM** interface.

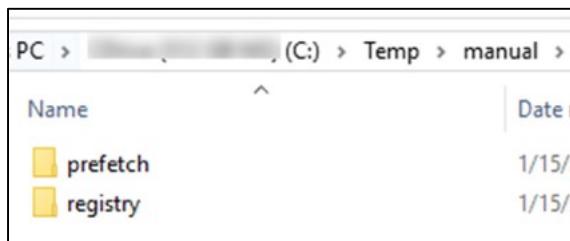
14. Type **dir** and press **Enter** to see the contents of the current folder. This folder contains Registry hives. There are several we are interested in, but first, we need to make a place to copy the files to.

```
dir
```

PS E:\Windows\System32\config> dir				
Directory: E:\Windows\System32\config				
Mode	LastWriteTime	Length	Name	
d----	7/14/2009 2:04 AM		Journal	
d----	3/30/2012 4:42 AM		RegBack	
d----	3/15/2012 10:24 PM		systemprofile	
d----	11/10/2010 6:22 PM		TxR	
-a---	11/10/2010 6:09 PM	28672	BCD-Template	
-a---	4/7/2012 9:48 AM	23592960	COMPONENTS	
-a---	4/7/2012 11:48 AM	262144	DEFAULT	
-a---	4/7/2012 4:14 PM	136	netlogon.ftl	
-a---	4/4/2012 8:02 PM	262144	SAM	
-a---	4/7/2012 2:49 PM	262144	SECURITY	
-a---	4/7/2012 4:17 PM	37748736	SOFTWARE	
-a---	4/7/2012 1:05 PM	15990784	SYSTEM	

15. Open another instance of **File Explorer** and create a new directory, C:\Temp\manual. Create the following subfolders underneath the manual folder:

```
registry
prefetch
```



These directories are where we will copy our manually extracted files into.

16. Back in the **PowerShell** window that is in **Windows\System32\config** directory, copy the following files using the commands shown below:

```
cp SAM C:\Temp\manual\registry\
cp SAM.LOG1 C:\Temp\manual\registry\
cp SAM.LOG2 C:\Temp\manual\registry\
cp SOFTWARE C:\Temp\manual\registry\
cp SOFTWARE.LOG1 C:\Temp\manual\registry\
cp SOFTWARE.LOG2 C:\Temp\manual\registry\
cp SYSTEM C:\Temp\manual\registry\
cp SYSTEM.LOG1 C:\Temp\manual\registry\
cp SYSTEM.LOG2 C:\Temp\manual\registry\
```

**PRO TIP 1** – When typing the file path (or most any instruction that allows), you can simply type the first few letters, and then press **Tab** to autocomplete the word.

**PRO TIP 2** – To save yourself a lot of typing, once you have typed the first instruction above and are back at the command line, simply press the **up** arrow on your keyboard. This will make the previously typed line reappear. Now just **back** arrow to change the parts that need changing. Press **Enter** from wherever you are to execute the command.

17. Using the **File Explorer** window that is in the **C:\Temp\manual** directory, double click on the **registry** directory and verify the files were copied.

Local Disk (C:) > Temp > manual > registry			
Name	Date modified	Type	Size
SAM	4/4/2012 3:02 PM	File	256 KB
SAM.LOG1	4/4/2012 3:02 PM	LOG1 File	25 KB
SAM.LOG2	7/13/2009 9:03 PM	LOG2 File	0 KB
SOFTWARE	4/7/2012 12:34 PM	File	36,864 KB
SOFTWARE.LOG1	4/7/2012 12:34 PM	LOG1 File	256 KB
SOFTWARE.LOG2	2/29/2012 12:23 AM	LOG2 File	256 KB
SYSTEM	4/7/2012 12:05 PM	File	15,616 KB
SYSTEM.LOG1	4/7/2012 12:05 PM	LOG1 File	256 KB
SYSTEM.LOG2	7/13/2009 9:03 PM	LOG2 File	0 KB

Notice that we selected not only the hives themselves, but also all the **.LOG\*** files with the same name. These **LOG** files are transaction logs and are critical to collect as well, so that we can be sure we have all the data from each of the Registry hives available.

18. Using the Administrative **PowerShell** window, change directories to <Drive letter>:\Windows\prefetch

For example, if **AIM** mounted the E01 file to the **E:\** drive, use the following command:

```
cd E:\Windows\Prefetch\
```

19. Copy all **Prefetch** files using the following command:

```
cp *.pf C:\Temp\manual\prefetch\
```

20. Using the **File Explorer** window that is in the **C:\Temp\manual** directory, double click on the **prefetch** directory and verify the files were copied.

Local Disk (C:) > Temp > manual > prefetch		
Name	Date modified	Type
A.EXE-8D56B1C4(pf)	4/3/2012 7:43 PM	PF File
A.EXE-F91CBA0E(pf)	4/7/2012 4:05 PM	PF File
ACRORD32.EXE-33939BD1(pf)	4/1/2012 9:17 AM	PF File
ADOBEARM.EXE-ACA00A4A(pf)	4/6/2012 2:43 PM	PF File
AT.EXE-E3131BD4(pf)	4/6/2012 8:41 AM	PF File
ATBROKER.EXE-FF58B71D(pf)	4/4/2012 7:21 AM	PF File
AUDIODG.EXE-D0D776AC(pf)	4/6/2012 2:42 PM	PF File
CMD.EXE-89305D47(pf)	4/6/2012 2:00 PM	PF File
CONHOST.EXE-3218E401(pf)	4/7/2012 2:00 AM	PF File
CONSENT.EXE-65F6206D(pf)	4/4/2012 3:05 PM	PF File

This process can, of course, be repeated for many more artifacts like user Registry hives, Ink files, jump lists, etc.

With the data we have collected though, let's see how we can go about processing it to extract out actionable intelligence. We will be focusing on the prefetch files next, but the Registry hives could be targeted with a tool like **RECmd** to extract out details from each of the Registry hives we collected just as easily.

21. Close any **PowerShell** windows that are open.

22. Using the shortcut on the **Desktop**, start a new **PowerShell** window.

23. Verify you are in the C:\Tools directory. If not, go there by typing cd c:\Tools

24. In the **PowerShell** window, type the following command:

```
.\PECmd.exe -d C:\Temp\manual\prefetch\ -q --csv C:\Temp\
```

```
PS C:\Tools> .\PECmd.exe -d C:\Temp\manual\prefetch\ -q --csv C:\Temp\  
PECmd version [REDACTED]  
  
Author: Eric Zimmerman (saericzimmerman@gmail.com)  
https://github.com/EricZimmerman/PECmd  
  
Command line: -d C:\Temp\manual\prefetch\ -q --csv C:\Temp\  
  
Keywords: temp, tmp  
  
Looking for prefetch files in 'C:\Temp\manual\prefetch\'  
  
Found 122 Prefetch files  
----- Processed 'C:\Temp\manual\prefetch\A.EXE-8D56B1C4(pf' in 0.00892920 seconds  
----- Processed 'C:\Temp\manual\prefetch\A.EXE-F91CBA0E(pf' in 0.00065590 seconds
```

**NOTE:** A few of the files fail parsing. This is fine and is not unusual. The failed files can be ignored.

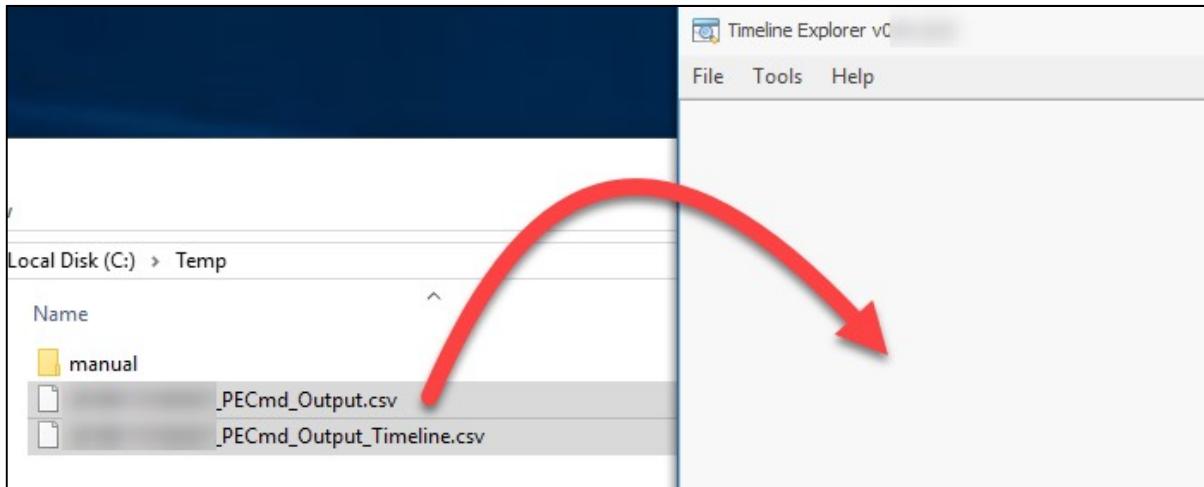
This command is processing all the **prefetch** files found in C:\Temp\manual\prefetch and generating a CSV which we can then analyze in **Timeline Explorer**.

25. Once **PECmd** generates the CSV file it can be loaded into **Timeline Explorer**.

### Exercise Questions

**NOTE:** In the following section we will be looking at data contained in Prefetch files. Prefetch is an evidence of execution artifact that tracks things like how many total times a program was executed, the last time it was executed, and more.

1. Open **Timeline Explorer** using the shortcut in the **Utilities** fence on your **Desktop**. Drag and drop the CSV files generated by **PECmd** into **Timeline Explorer**. The filenames should look something like this:



Notice that **PECmd** generated TWO files. The one ending with **\_Timeline** is a summary of all the timestamps and full paths to each executable that was found in all the prefetch files. The other one contains much more detail about each individual prefetch file. You will need to navigate between the two for the following questions.

2. Once the files are loaded in **Timeline Explorer**, answer the following questions.

- a. When was the last time **DLLHOT.EXE** was executed? How many total times was it executed?  
(Hint: Look in the **Executable Name** column)

---



---

- b. According to the prefetch files, was **PowerShell** executed on the machine where the prefetch files were found? If so, how many times?

---

- c. You are concerned that scheduled tasks may have been used for persistence in the investigation you are working on. Does prefetch show any evidence showing this to be true? If so, document how you came to this conclusion.

---



---



---

**NOTE:** There are two processes that deal with scheduled tasks on a Windows system:  
**schtasks.exe** and **at.exe**.

- d. How many unique directories was **DLLHOST.EXE** executed from? What are they?

---

---

---

**NOTE:** This question is easier to answer based on the contents of the **PECmd\_OutputTimeline.csv** file.

- e. Which seven executables were last run on April 5, 2012?

---

---

---

---

---

---

---

---

---

- f. **BONUS:** Why do all these prefetch files only contain one last run timestamp?

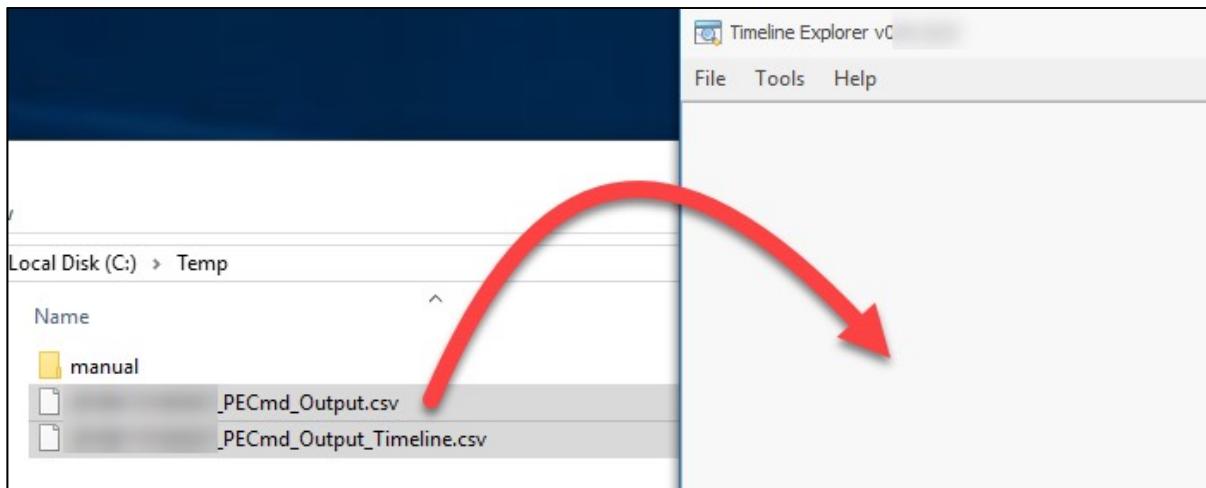
---

**OPTIONAL:** Use **RECcmd** in batch mode to extract out key details from the Registry hives you collected. The CSVs generated by **RECcmd** can be dropped into **Timeline Explorer** for analysis as well.

**Questions with step by step**

**NOTE:** In the following section we will be looking at data contained in Prefetch files. Prefetch is an evidence of execution artifact that tracks things like how many total times a program was executed, the last time it was executed, and more.

1. Open **Timeline Explorer** using the shortcut in the **Utilities** fence on your **Desktop**. Drag and drop the **CSV** files generated by **PECmd** into **Timeline Explorer**. The filenames should look something like this:



Notice that **PECmd** generated TWO files. The one ending with **\_Timeline** is a summary of all the timestamps and full paths to each executable that was found in all the prefetch files. The other one contains much more detail about each individual prefetch file. You will need to navigate between the two for the following questions.

2. Once the files are loaded in **Timeline Explorer**, answer the following questions.

- a. When was the last time **DLLHOT.EXE** was executed? How many total times was it executed?  
(Hint: Look in the **Executable Name** column)

Filtering for **dllhot** in the Executable Name column shows us one entry containing this string. The Run Count column contains how many times it was executed, which is 4.

For the last executed timestamp, look in the Last Run column, which shows **2012-04-03 22:12:42**.

The screenshot shows the contents of the "\_PECmd\_Output\_Timeline.csv" file in Timeline Explorer. The table has columns: File Created, Source Modified, Source Accessed, Executable Name, Run Count, and Hash. One row is highlighted with a red box around the "Executable Name" column, which contains "dllhot". A red arrow points to the "Run Count" column, where the value "4" is highlighted. The "Hash" column shows "9Bc".

File Created	Source Modified	Source Accessed	Executable Name	Run Count	Hash
-05-16 16:44:08	2012-04-03 22...	2019-05-16 16...	DLLHOT.EXE	=	9Bc
			dllhot	4	9Bc

- b. According to the prefetch files, was **PowerShell** executed on the machine where the prefetch files were found? If so, how many times?

No, PowerShell was not run, according to prefetch. This can be verified by filtering for PowerShell in the Executable Name column, then looking in the lower right for the number of visible rows, which is 0.

- c. You are concerned that scheduled tasks may have been used for persistence in the investigation you are working on. Does prefetch show any evidence showing this to be true? If so, document how you came to this conclusion.

Since we must look for two different processes here, first we can look for sctasks.exe in the Executable Name column, resulting in a visible row count of 0, so this program did not run.

Doing the same thing for at.exe however results in 3 visible rows, but only one that is for at.exe

Column header here to group by that column						
Executable Name	Run Count	Hash	Size	Version	Last Run	
at.exe	=	=	=	=	=	
AT.EXE	9	E3131BD4	13806	Windows V...	2012-04-06 13:41:09	
NETSTAT.EXE	3	6D34D712	12342	Windows V...	2012-04-03 23:10:02	
SHSTAT.EXE	3	3E759080	28986	Windows V...	2012-04-04 19:40:29	

**NOTE:** There are two processes that deal with scheduled tasks on a Windows system: **sctasks.exe** and **at.exe**.

- d. How many unique directories was **DLLHOST.EXE** executed from? What are they?

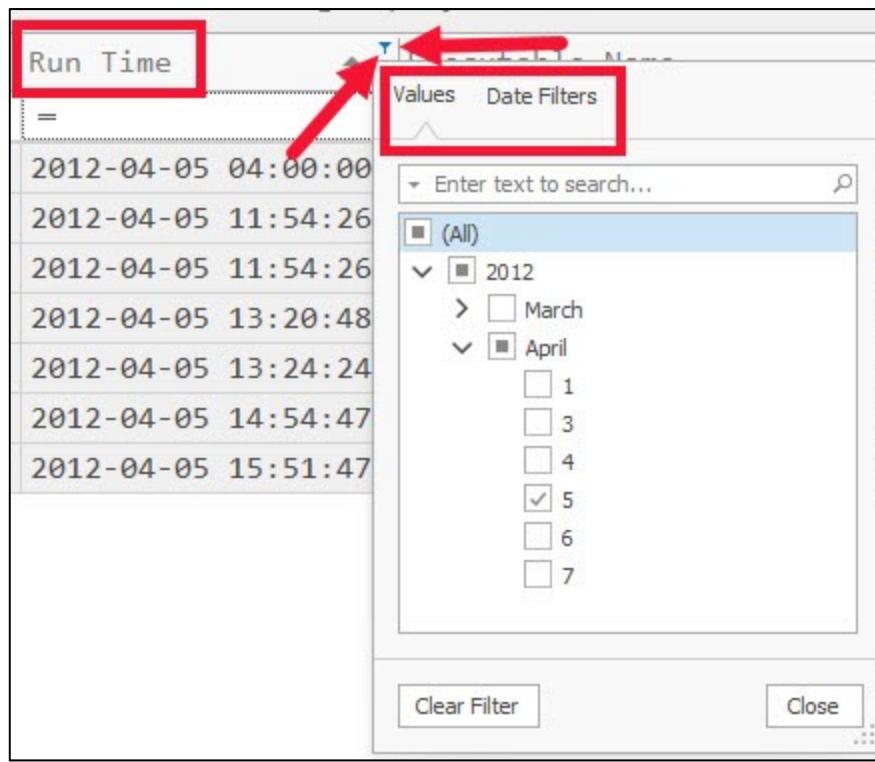
Looking at the Timeline CSV and filtering for dllhost.exe, we can see nine visible rows. Looking for unique directory names in the Executable Name column, we see two unique paths:

\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32  
\DEVICE\HARDDISKVOLUME1\

**NOTE:** This question is easier to answer based on the contents of the **PECmd\_OutputTimeline.csv** file.

- e. Which seven executables were last run on April 5, 2012?

In the PECmd\_OutputTimeline.csv file, use the Run Time column filter to find everything from April 5, 2012. Note that there are TWO possible filters here: Values and Date Filters, but we have Values active here so we can select the month and date.



This gets us to the list of executables:

DEFRAG.EXE  
DLLHOST.EXE  
HYDRAKATZ.EXE  
IPCONFIG.EXE  
OUTLOOK.EXE  
RUNDLL32.EXE  
SVCHOST.EXE

Executable Name
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\DEFRAG.EXE
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\DLLHOST.EXE
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\HYDRAKATZ.EXE
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\IPCONFIG.EXE
\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\MICROSOFT OFFICE\OFFICE14\OUTLOOK.EXE
RUNDLL32.EXE
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\SVCHOST.EXE

- f. **BONUS:** Why do all these prefetch files only contain one last run timestamp?

The prefetch files come from a version of Windows prior to Windows 8. Starting with Windows 8 and newer, prefetch files track the last eight execution times, but before Windows 8, only the last timestamp is recorded.

**OPTIONAL:** Use **RECmd** in batch mode to extract out key details from the Registry hives you collected. The CSVs generated by **RECmd** can be dropped into **Timeline Explorer** for analysis as well.

First, open a new PowerShell window and change directories:

```
cd C:\Tools\RegistryExplorer
```

RECmd can be used in batch mode to process each of the hives we copied, like this (all on a single line, with a space between -bn and .\BatchExamples):

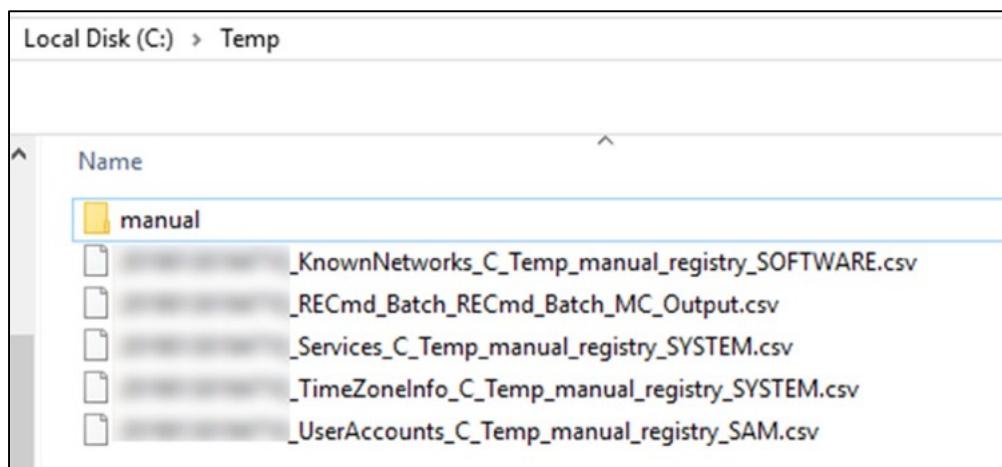
```
.\RECmd.exe -d C:\Temp\manual\registry\ --bn
.\BatchExamples\RECmd_Batch_MC.reb --csv C:\Temp\
```

```
Found key 'ControlSet001\Control\ComputerName\ComputerName' and value 'ComputerName'!
Found key 'ControlSet002\Control\ComputerName\ComputerName' and value 'ComputerName'!
Found key 'ControlSet001\Control\Session Manager\AppCompatCache'!
Found key 'ControlSet002\Control\Session Manager\AppCompatCache'!
Found key 'ControlSet001\Control\TimeZoneInformation'!
Found key 'ControlSet002\Control\TimeZoneInformation'!
Found key 'ControlSet001\Services'!
Found key 'ControlSet002\Services'!
Found key 'ControlSet001\Services\lanmanserver\Shares'!
Found key 'ControlSet002\Services\lanmanserver\Shares'!
Found key 'ControlSet001\Services\Tcpip\Parameters\Interfaces'!
Found key 'ControlSet002\Services\Tcpip\Parameters\Interfaces'!
Found key 'ControlSet001\Services\Tcpip\Parameters\Interfaces'!
Found key 'ControlSet002\Services\Tcpip\Parameters\Interfaces'!
Found key 'MountedDevices'!
Found key 'Setup'!
Found key 'Select' and value 'Current'!

Found 1,096 key/value pairs across 3 files
Total search time: 4.115 seconds

Saving batch mode CSV file to 'C:\Temp\RECmd_Batch_RECmd_Batch_MC_Output.csv'
```

This results in several files being created in C:\temp which can be opened in Timeline Explorer for review.



### Exercise—Key Takeaways

- Mounting evidence files in a forensically sound manner allows for copying out forensic artifacts for analysis.
- Manual collection of key forensic artifacts can be time consuming and, for more than a handful of files, can also be error prone.
- For specific artifacts, manually locating and copying files out of an image might be the fastest way to get to the data you need.
- Timeline Explorer can help make sense of a wide range of forensic data.

This page intentionally left blank.

# © SANS Institute 2020

## Exercise 3.3—Manual Triage Acquisition

### Background

As hard drive size keeps expanding, it becomes more and more impractical to take a full disk image of every device encountered. Given that 99% of the necessary evidence typically will exist in 1-2% of the data acquired, it is easy to see how a great deal of time is wasted following what may be considered outdated procedures in today's digital forensics world.

In this lab, we will explore how to access an already existing full disk image and perform a manual triage acquisition of data. This same technique could also be used against a live system. By performing the triage acquisition manually, we can see where the most commonly used forensic artifacts are located. This is the first step in a process we will continue to refine throughout the course.

Once we collect these artifacts, analysis on one of the file types collected will be performed and the results analyzed using Timeline Explorer.

### Objectives

- Use Arsenal Image Mounter to mount and access an E01 image file
- Locate and copy key artifact files for analysis including Registry hives, Ink files, jump lists, and prefetch
- Mount the triage acquisition using FTK imager
- Use LECmd to process the collected Ink files and review the results in Timeline Explorer

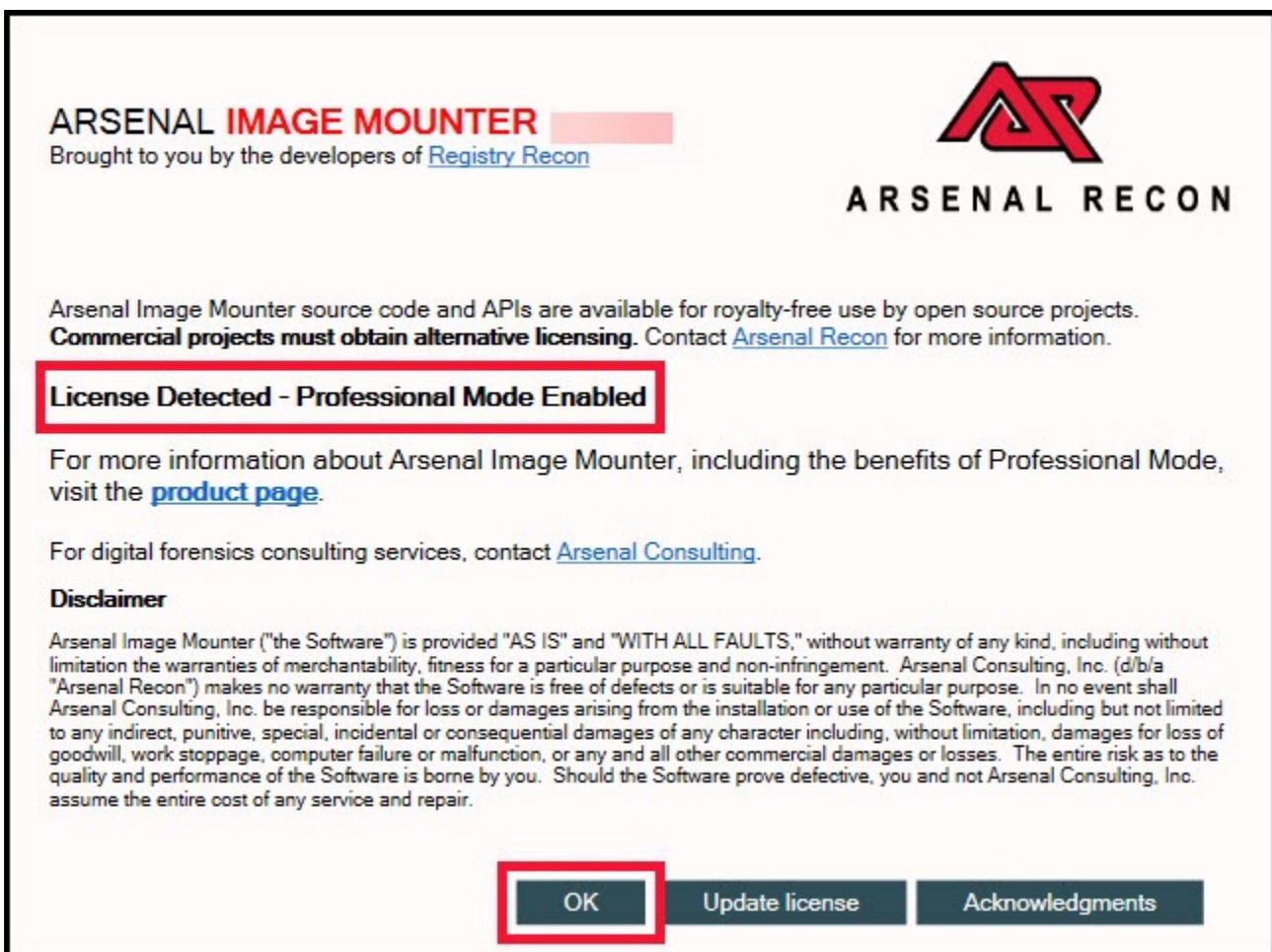
### Exercise Preparation

1. Boot your **FOR498 Windows VM**
2. Login to the **FOR498 Windows VM** using the following credentials:
  - a. Username: **SANSDFIR**
  - b. Password: **forensics**

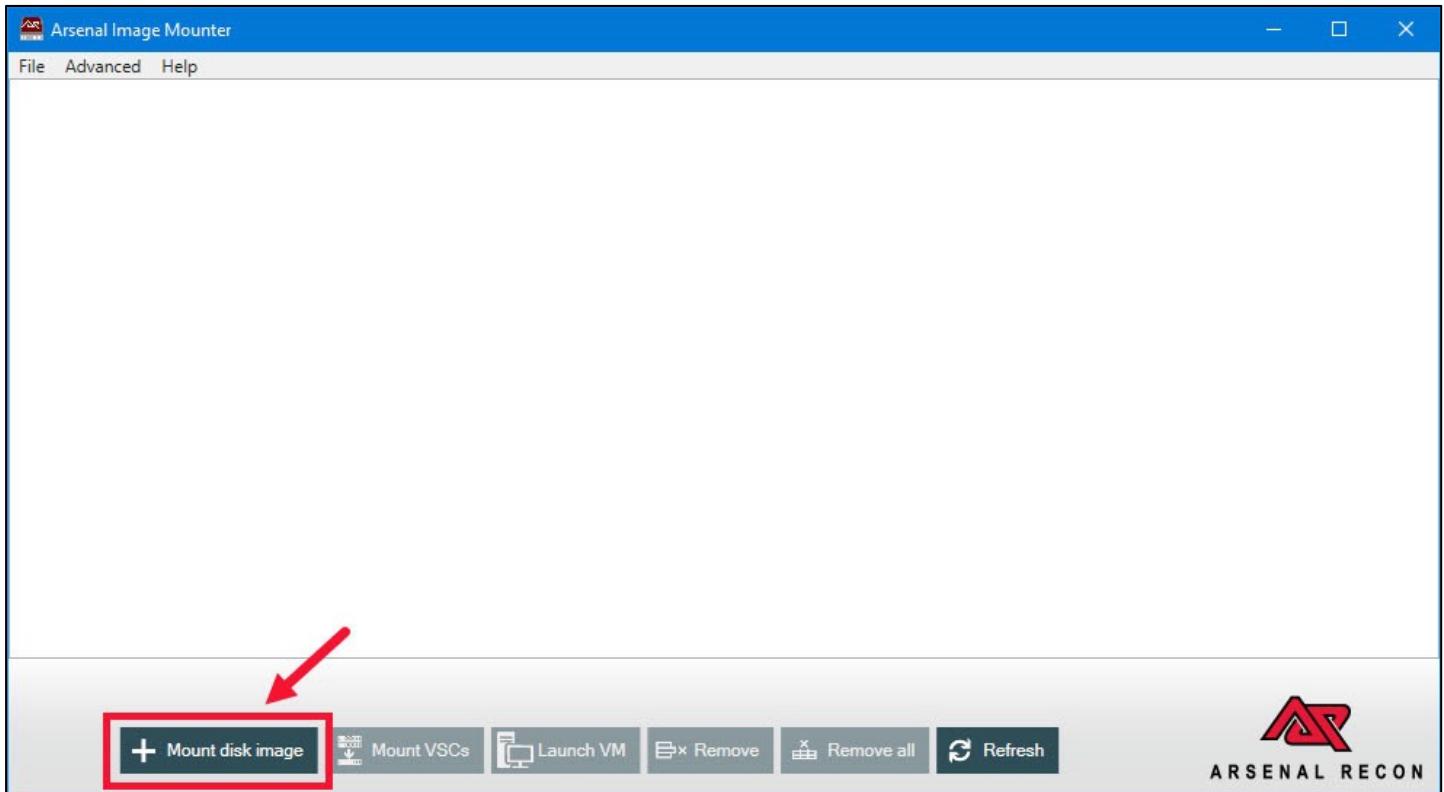
- Double click the AIM icon in the Utilities fence on the Desktop to start Arsenal Image.



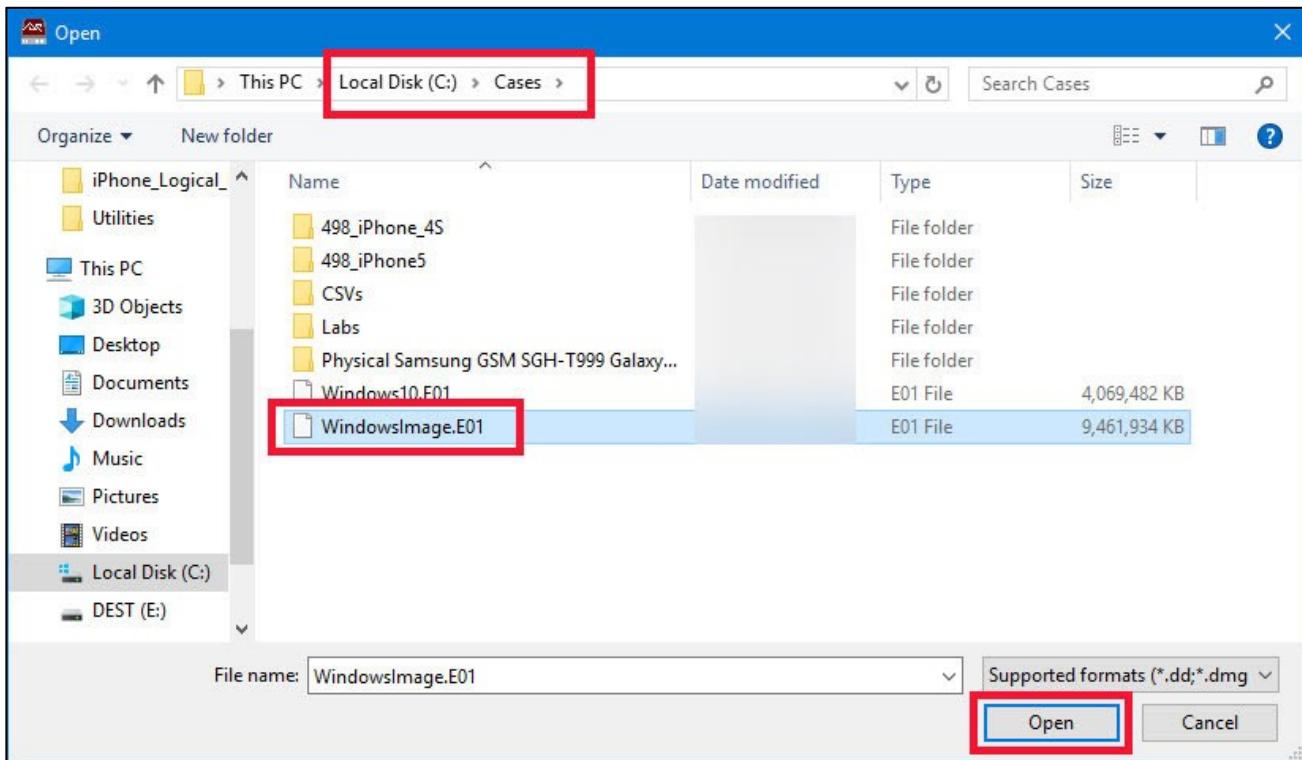
- When the splash screen appears, click **OK** to go to the main menu.



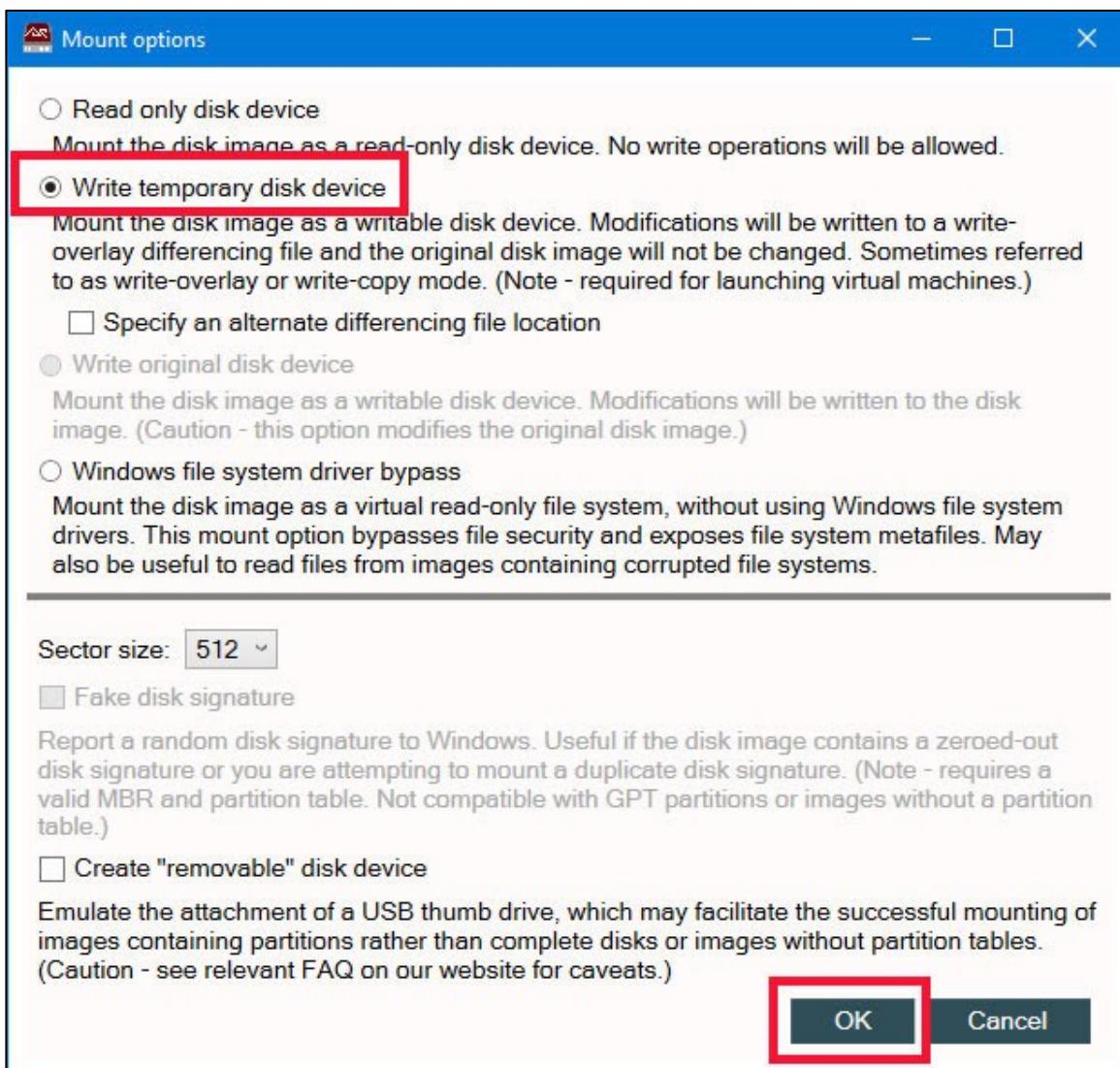
5. The main interface will now be displayed. To mount an image, click the **Mount Image** button on the lower left.



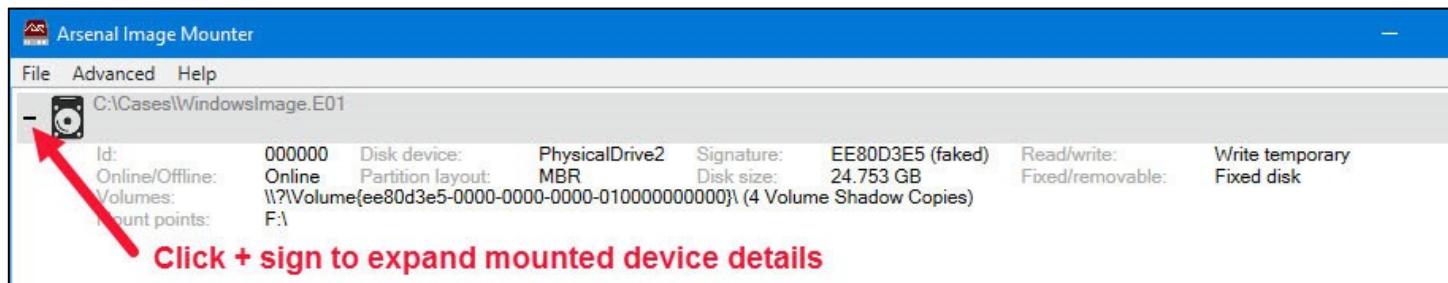
6. Navigate to **C:\Cases** and select the image named **WindowsImage.E01**. Click **Open**.



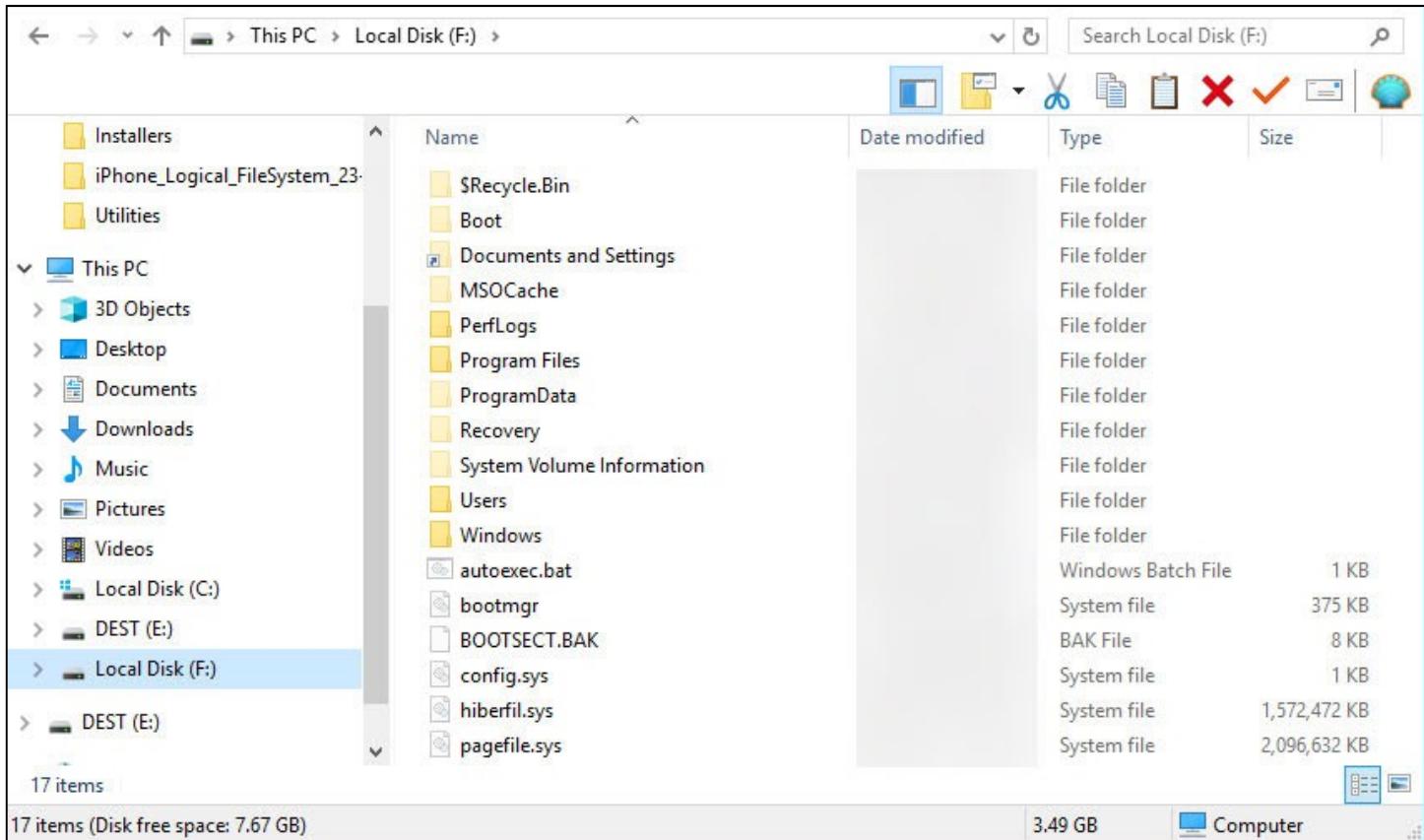
7. In the **Mount options** dialog, select the **Write temporary disk device** option via the radio button, then click **OK**.



8. AIM will now mount the image and make it available to Windows. To see details, click on the + sign next to the mounted E01 in the main interface. In the example below, the image has been mounted as E:\, as seen in the lower left portion of the details.

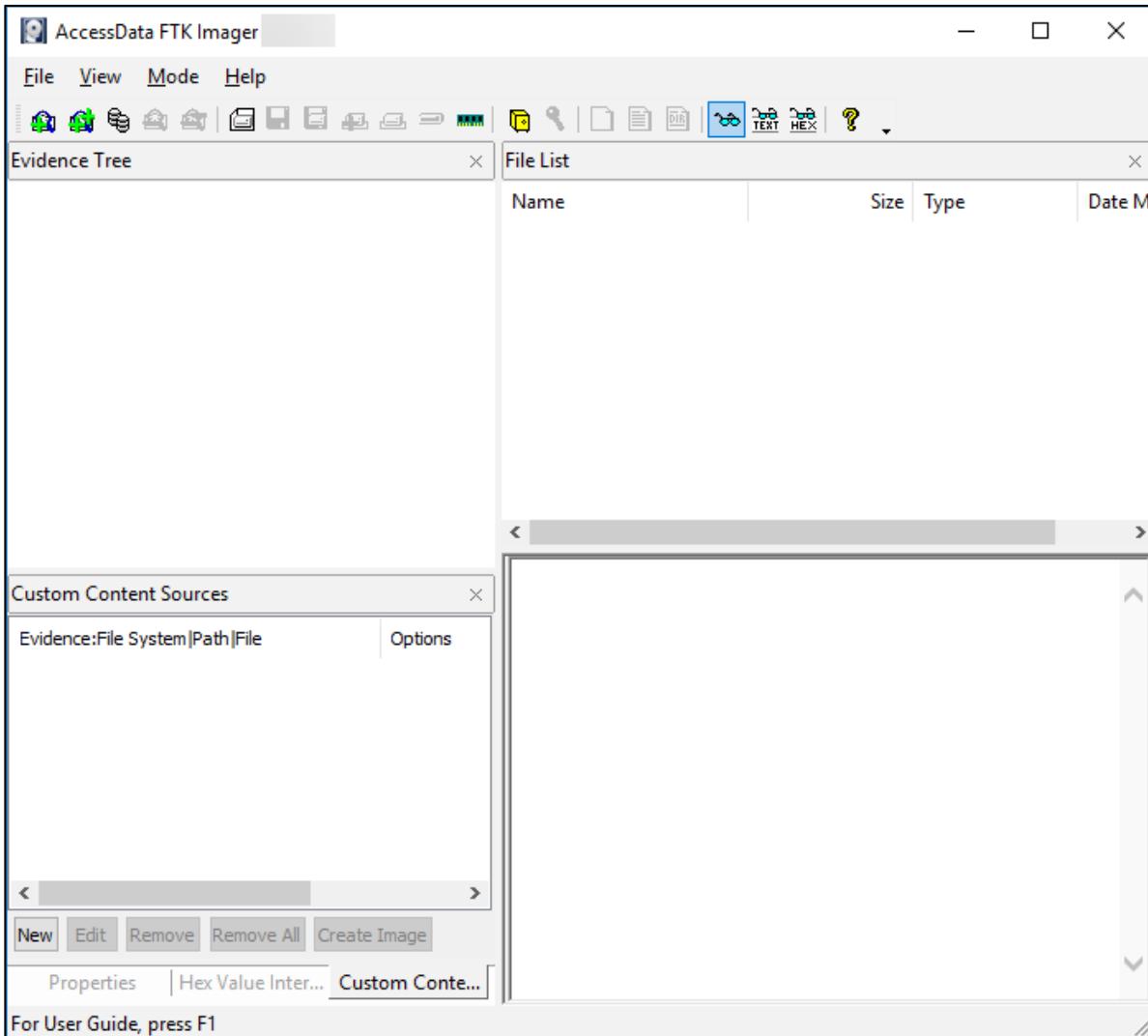


9. Open **File Explorer** and navigate to the drive letter where AIM mounted the image. It should look similar to what is shown below.

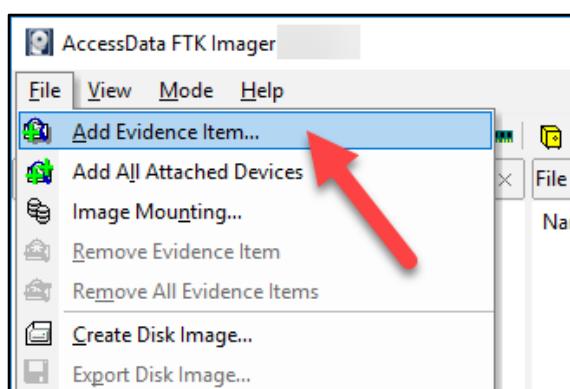


10. You now have full access to the Windows file system contained in the E01.

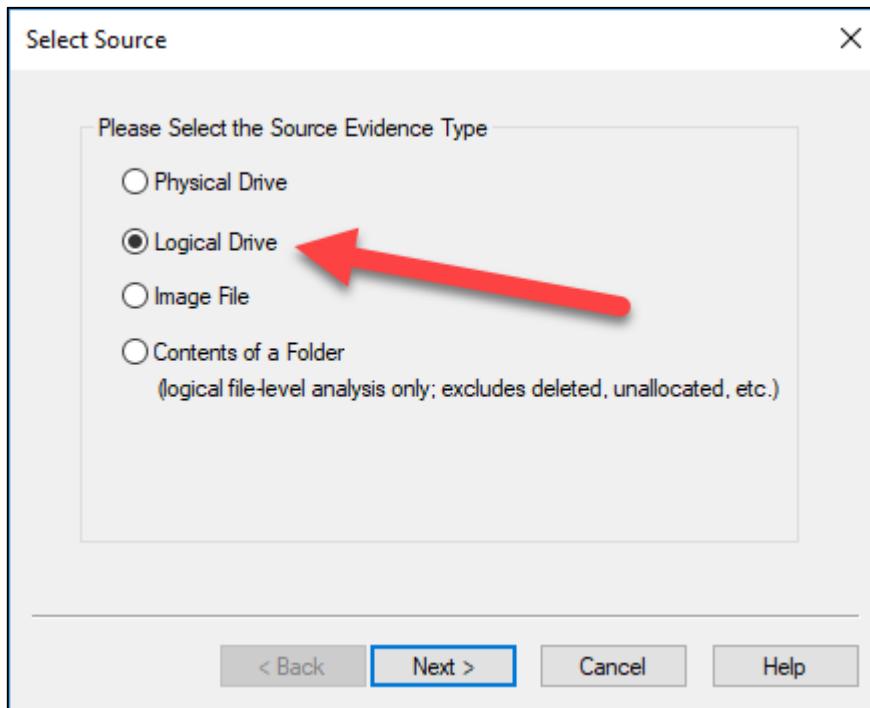
11. Start **FTK Imager** by double clicking the shortcut in the **Acquisition Tools** fence on the **Desktop**. This will show the main window.



12. While this technique is possible to perform on a running system, it can also be performed against an E01 opened in **FTK Imager**. Since we already have our **WindowsImage.E01** mounted from a previous step, we will use that as our source of data.
13. Click the **File** menu, then click **Add Evidence Item...**



14. In the **Select Source** dialog, click the radio button for **Logical Drive**, then click **Next**.

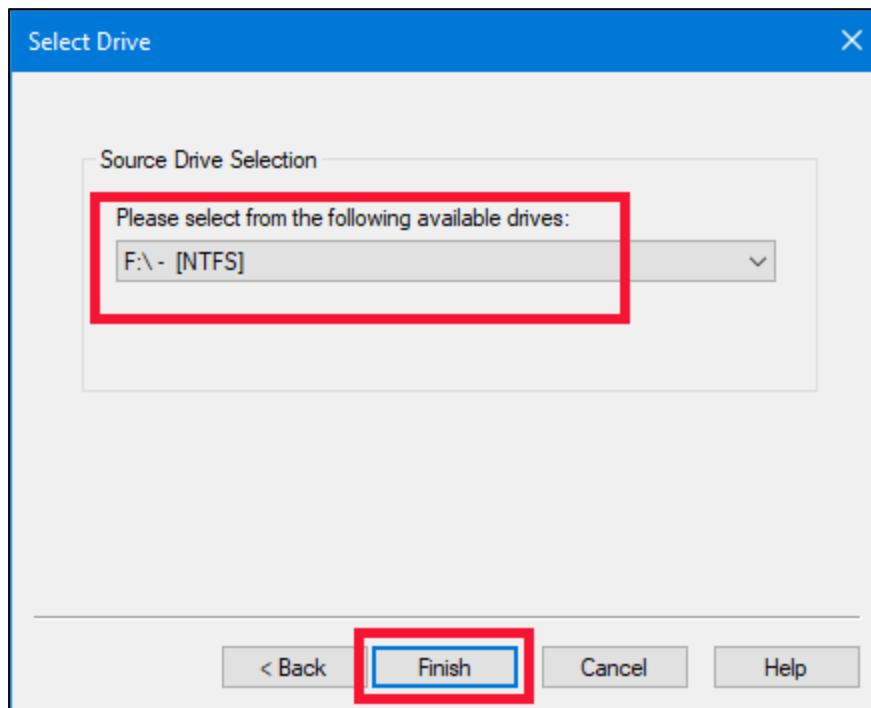


Note that it is also possible to directly open the E01 if it were not already mounted as well, but since we already have the image mounted, we are accessing it via the logical drive. This is to simulate a live triage acquisition.

15. From the dropdown list, select the logical drive that matches what is shown in the **Arsenal Image Mounter** window. In the example below, AIM mounted the E01 to the E:\ drive. Once the correct drive is selected, click **Finish**.

Id:	000000	Disk device:	PhysicalDrive2	Signature:	EE80D3E5 (faked)	Read/write:	Write temporary
Online/Offline:	Online	Partition layout:	MBR	Disk size:	24.753 GB	Fixed/removable:	Fixed disk
Mount points:	F:\						

In FTK Imager, select the same drive letter as shown in AIM.

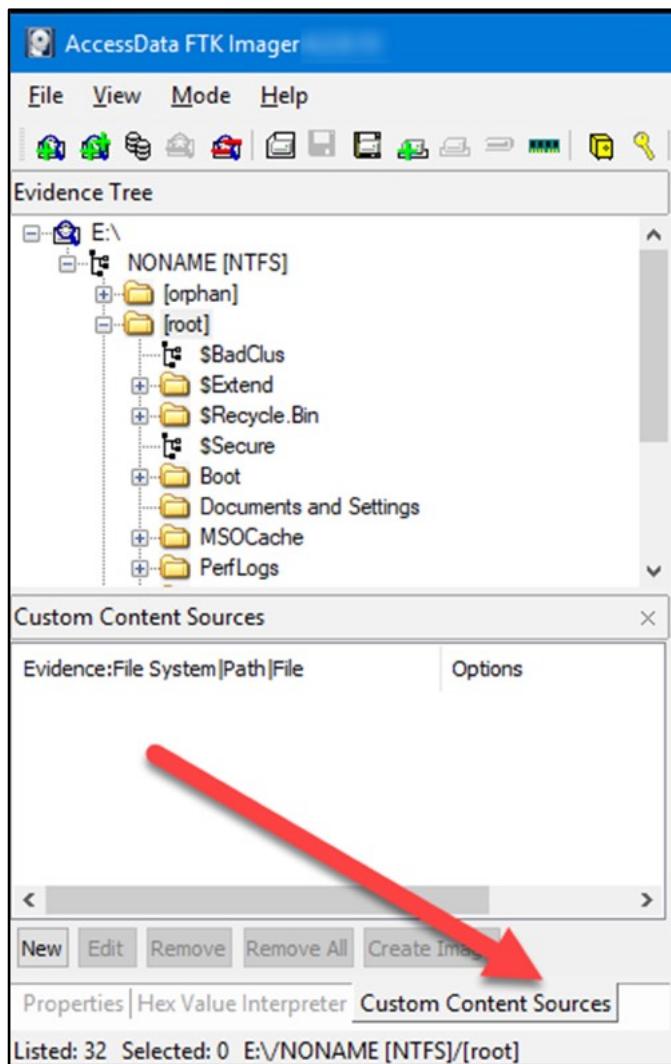


16. The selected source drive will now show up in **FTK Imager** in the tree to the left. In the image below, the tree has been expanded several levels and the contents of the file system are visible.

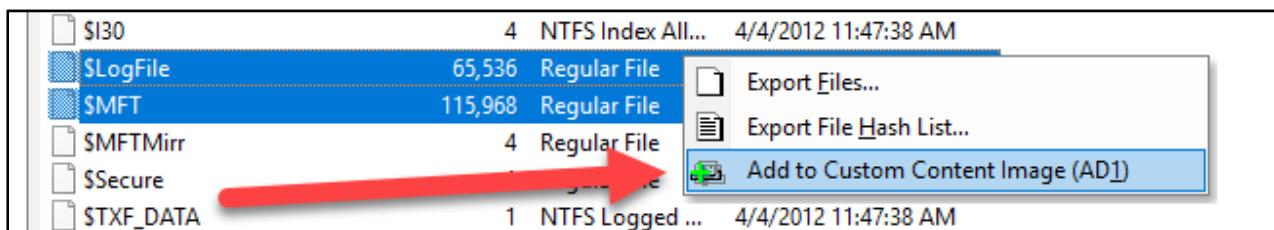
The screenshot shows the FTK Imager interface. The title bar says 'AccessData FTK Imager'. The menu bar includes 'File', 'View', 'Mode', and 'Help'. The toolbar has various icons for file operations. The main area is divided into two panes: 'Evidence Tree' on the left and 'File List' on the right. The 'Evidence Tree' pane shows a tree view of the selected drive, with an arrow pointing to the 'E:\ NONAME [NTFS]' node. The 'File List' pane shows a table of files with columns for Name, Size, and Type. The table lists numerous files and directories, including \$Extend, \$Recycle.Bin, Boot, Documents and Settings, MSOCache, PerfLogs, Program Files, ProgramData, Recovery, System Volume Information, Users, Windows, and many others.

Name	Size	Type
\$Extend	1	Directory
\$Recycle.Bin	1	Directory
Boot	1	Directory
Documents and Settin...	1	Reparse Point
MSOCache	1	Directory
PerfLogs	1	Directory
Program Files	1	Directory
ProgramData	1	Directory
Recovery	1	Directory
System Volume Infor...	1	Directory
Users	1	Directory
Windows	1	Directory
SAttrDef	3	Regular File
SBadClus	0	Regular File
SBitmap	793	Regular File
SBoot	8	Regular File
S130	4	NTFS Index All...
SLogFile	65,536	Regular File
SMFT	115,968	Regular File

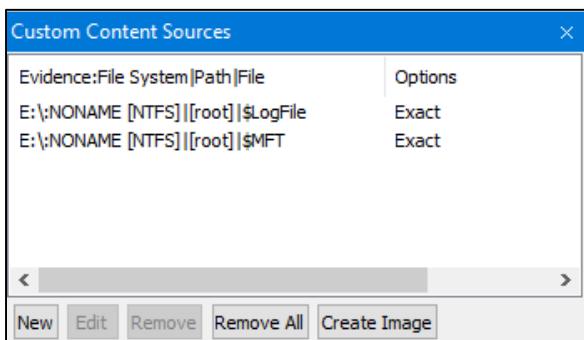
17. Take a few moments (5 minutes maximum) to browse around the available directories and files. Notice how the contents of files and directories are displayed as hex in the lower right.
18. To manually build a triage collection, we will now add files to the **Custom Content Sources** pane in **FTK Imager**. This pane is in the lower left corner of the interface. If the **Custom Content Sources** pane isn't active, click to select it.



19. There are two ways to add things as a source of data. The easiest is to find the files you are interested in, then use the context menu to add them to the collection. Select the **[root]** folder in the tree, then find and select both **\$LogFile** and **\$MFT** from the list on the right. Right-clicking on either of the selected files will bring up a context menu. Click on **Add to Custom Content Image (AD1)**.



20. Notice how we now have two files added to the **Custom Content Sources** pane.



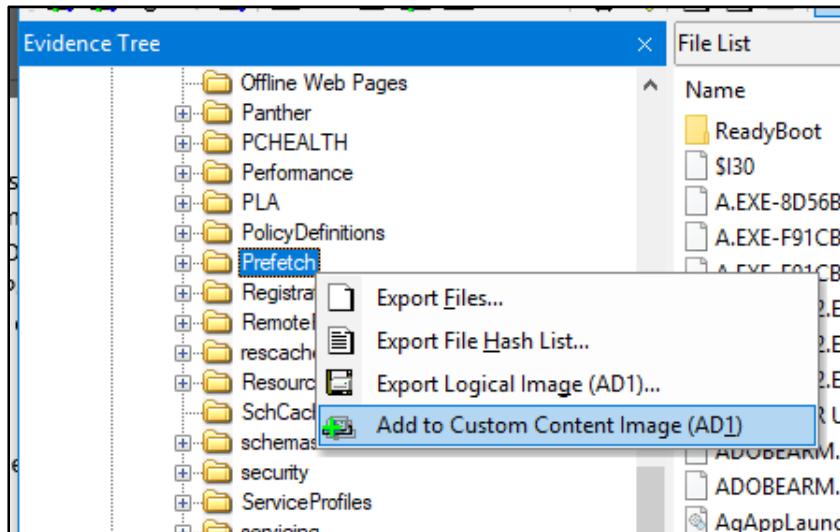
21. Expand the **[root]** folder and continue expanding child folders until you see the **Windows** folder.
22. Continue to expand child directories and navigate to **Windows\System32\config** and select **SAM**, **SOFTWARE**, and **SYSTEM** hives. These are part of the Windows Registry and are important to just about any investigation. Be sure to select the corresponding **LOG** files as well. Right click and add these to the **Custom Content Sources**.

**PROTIP:** Note in the screenshot below there is a file named **SAM.LOG1** and another one named **SAM.LOG1.FileSlack**. The **FileSlack** file contains the slack space of the **SAM.LOG1** hive. While this can be useful in some cases, for what we are doing here, we can ignore the **FileSlack** files. To make it easier to avoid the slack files, sort the files by "type" to group all the slack entries together.

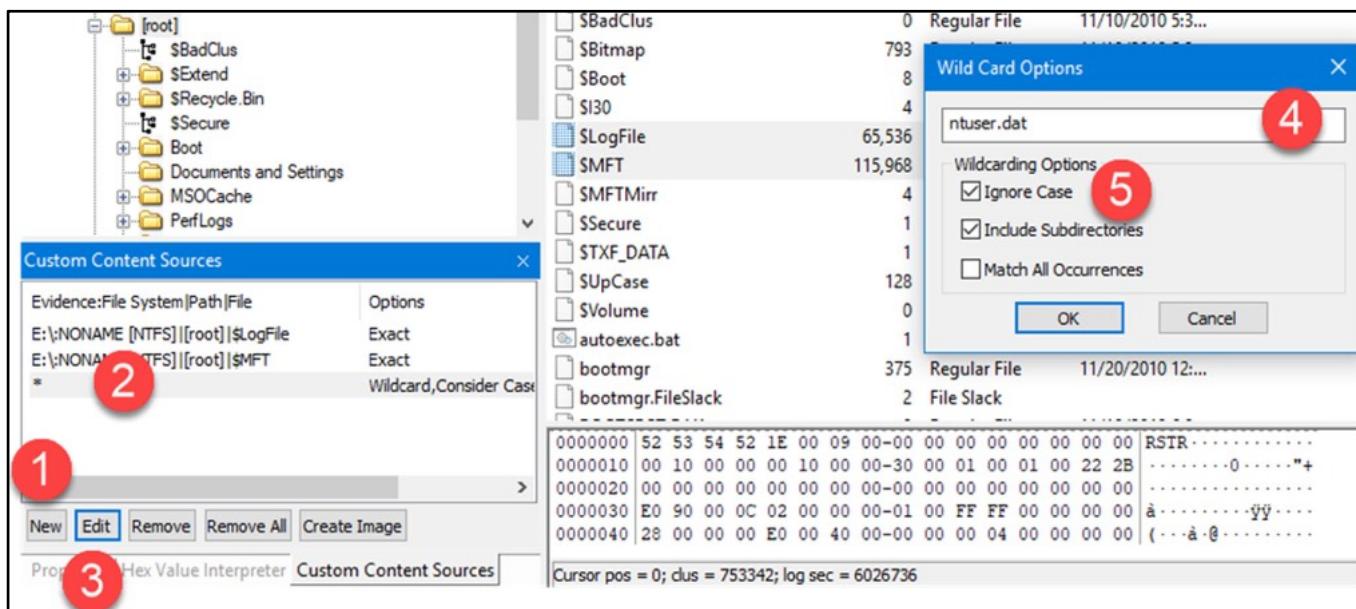
**NOTE:** To select more than one file at a time, hold the **CTRL** key on the keyboard while clicking each file. To select a range of files, click the first file, then hold the **SHIFT** key and click another file.

SAM	256	Regular File	4/4/2012 8:02:5...
SAM.LOG	1	Regular File	7/14/2009 7:56:...
SAM.LOG1	25	Regular File	4/4/2012 8:02:5...
SAM.LOG1.FileSlack	3	File Slack	
SAM.LOG2	0	Regular File	7/14/2009 2:03:...
SECURITY	256	Regular File	4/7/2012 4:38:0...
SECURITY.LOG	1	Regular File	7/14/2009 7:55:...
SECURITY.LOG1	25	Regular File	4/7/2012 4:38:0...
SECURITY.LOG1.FileSlack	3	File Slack	
SECURITY.LOG2	0	Regular File	7/14/2009 2:03:...
SOFTWARE	36,864	Regular File	4/7/2012 5:34:4...
SOFTWARE.FileSlack	148	File Slack	
SOFTWARE.LOG	1	Regular File	7/14/2009 7:56:...
SOFTWARE.LOG1	256	Regular File	4/7/2012 5:34:4...
SOFTWARE.LOG1.FileSlack	2,304	File Slack	
SOFTWARE.LOG2	256	Regular File	2/29/2012 6:23:...
SOFTWARE.LOG2.FileSlack	256	File Slack	
SOFTWARE{6cced2fd-...}	64	Regular File	6/15/2011 4:27:...
SOFTWARE{6cced2fd-...}	512	Regular File	6/15/2011 4:27:...
SOFTWARE{6cced2fd-...}	512	Regular File	6/15/2011 4:27:...
SYSTEM	15,616	Regular File	4/7/2012 5:05:1...
SYSTEM.FileSlack	240	File Slack	
SYSTEM.LOG	1	Regular File	7/14/2009 7:55:...
SYSTEM.LOG1	256	Regular File	4/7/2012 5:05:1...
SYSTEM.LOG1.FileSlack	4,352	File Slack	
SYSTEM.LOG2	0	Regular File	7/14/2009 2:03:...
SYSTEM.M...	64	Regular File	6/15/2011 4:27:...

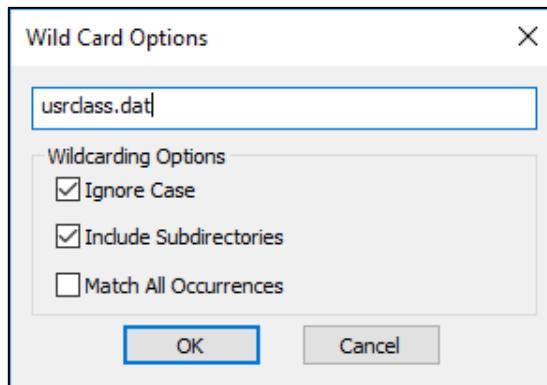
23. Finally, for our last manual step, navigate to **Windows\Prefetch**, but this time, right-click on the **Prefetch** folder and add the folder to the custom content image.



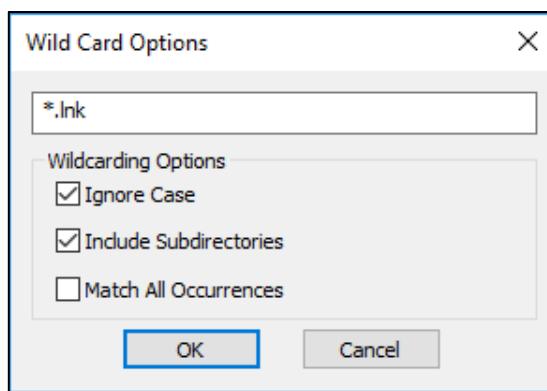
24. In the last few steps we have manually located and added files based on their path and name, but in many cases, this becomes tedious. In the next few steps, we will continue to add more files to our custom content image but will do so using a more flexible approach so we can locate files of interest regardless of the directory they are located in.
25. Click the **New** button under the Custom Content Sources pane, select the new entry (denoted by a \*) and click **Edit**. This new entry will be at the bottom of the list of items, so you may need to scroll to find it. In the dialog that appears, change the text box to reflect **ntuser.dat** and check the **Ignore Case** and option. Once you are finished, click **OK**.



26. Repeat this process, but this time, enter **usrclass.dat** in the text box.

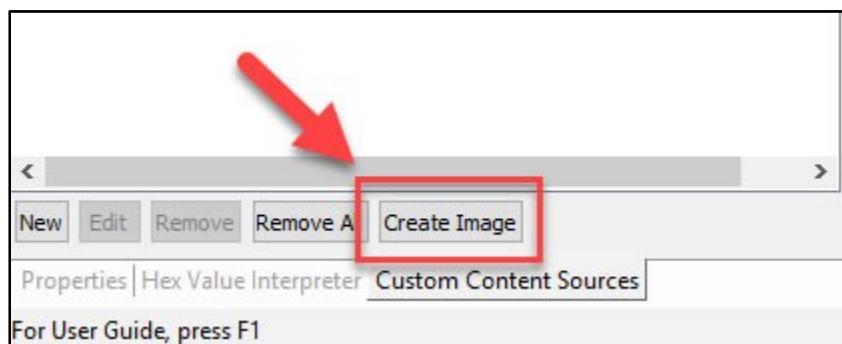


27. Do this one more time but enter **\*.lnk** in the text box.

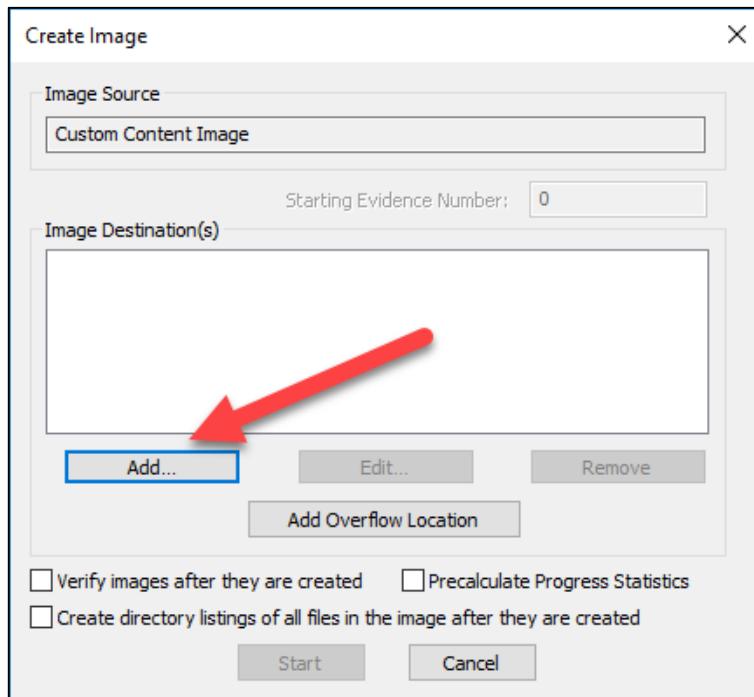


This process can be extended to any other type of file, from Word documents to pictures, etc. as required for your investigation.

28. With our specifications for our custom content complete, it is time to build the image file. Click the **Create Image** button in the **Custom Content Sources** pane to begin.



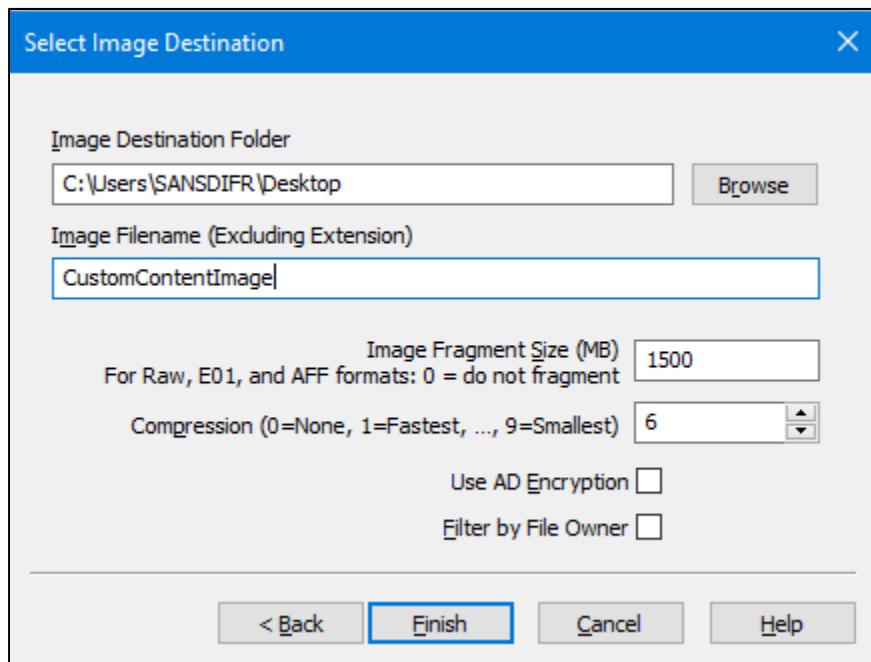
29. In the **Create Image** dialog, click the **Add** button.



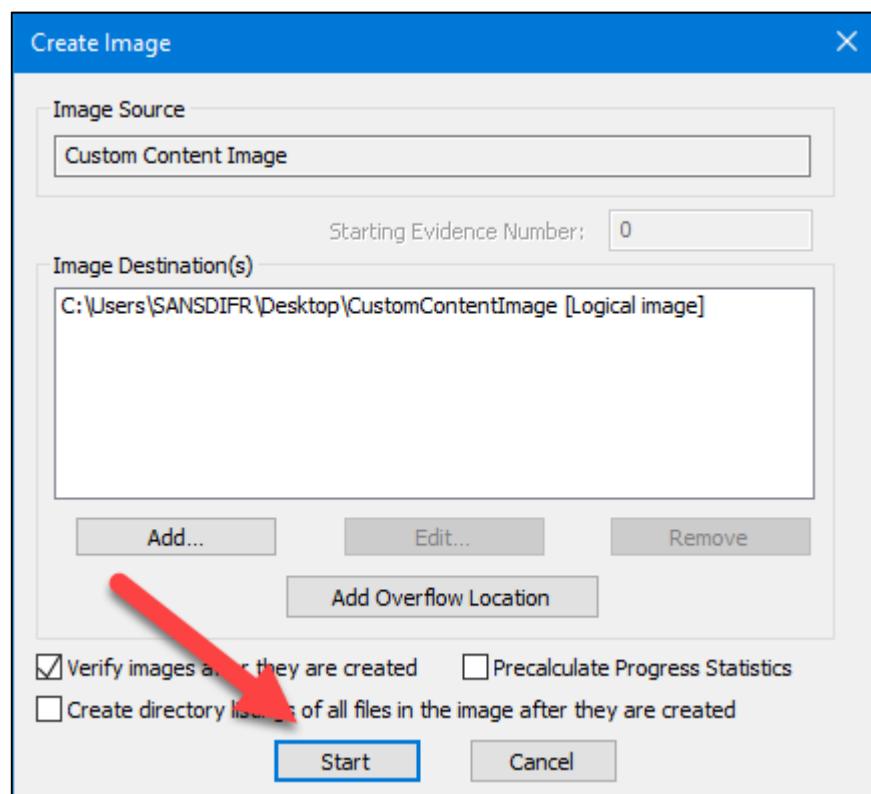
30. In the **Evidence Item Information** window, enter something like what is shown below, then click **Next**.

The screenshot shows the 'Evidence Item Information' window. It contains five input fields: 'Case Number' with the value 'SANS FOR-498', 'Evidence Number' with the value '12345', 'Unique Description' (an empty field), 'Examiner' with the value '<Your name here>', and 'Notes' (an empty field). At the bottom of the window are four buttons: '< Back', 'Next >' (which is highlighted with a blue border), 'Cancel', and 'Help'.

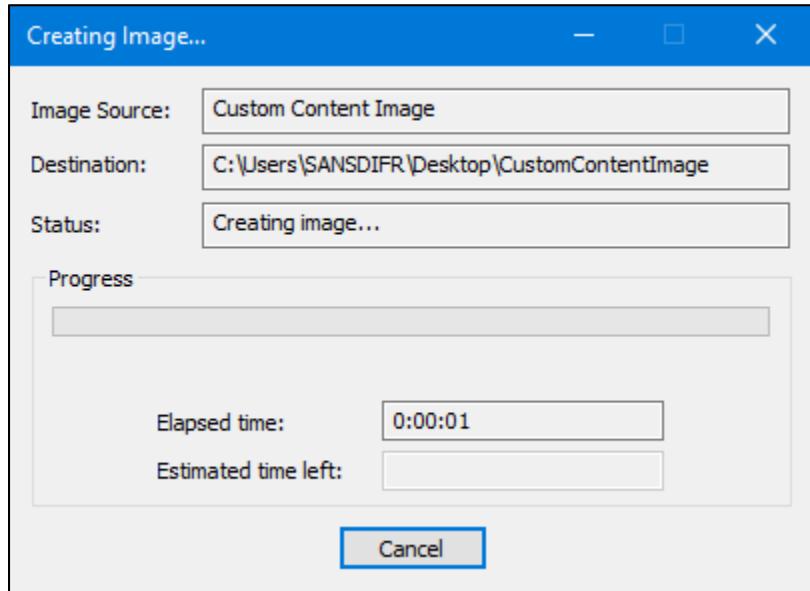
31. In the **Select Image Destination** window, use the **Browse** button to select the **Desktop** folder and enter a description for **Image Filename**, then click **Finish** to return to the **Create Image** dialog.



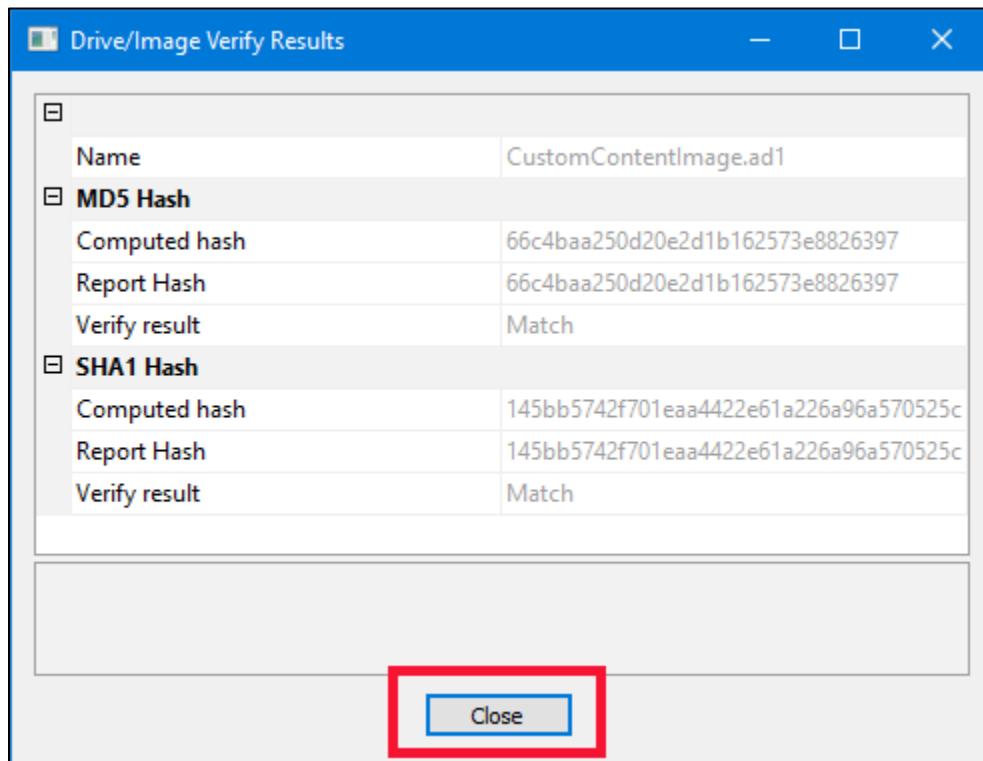
32. Ensure the **Verify images after they are created** option is checked since it will not add that much more time in this exercise and it's a good thing to do on a real case.
33. Once all options are set, click **Start** to begin the image creation process.



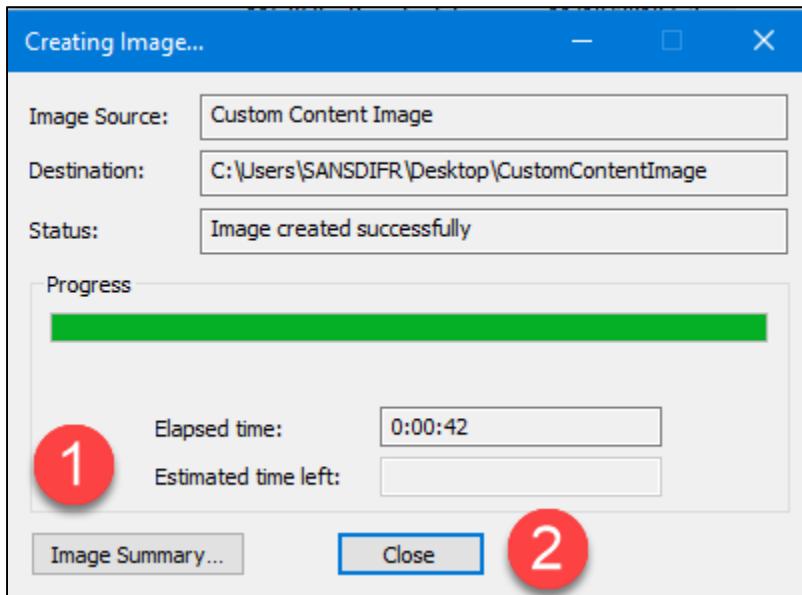
34. A dialog will be shown indicating the progress of the imaging. Depending on how big your source is, this may take anywhere from a few minutes to several hours.



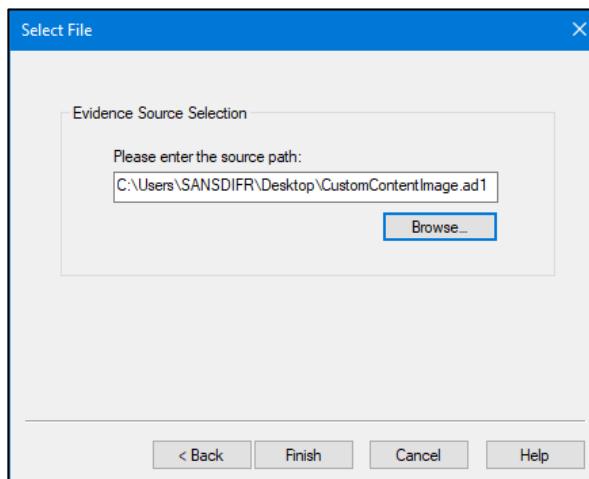
35. When imaging and verification are complete, a **Verify Results** window will open. Review, and then click **Close**.



36. You can click the **Image Summary** button to review key details about the imaging process. When done, close the **Image Summary** and click the **Close** button to return to the main interface.



37. With the custom content image complete, we can now load it into **FTK imager** to view the contents, as well as mount the custom content image as a drive letter. This is particularly helpful because it allows us to navigate the contents of the image to extract out files, point software tools at the mounted image, etc.
38. Click **File**, then **Add Evidence Item**. In the **Select Source** dialog, click the **Image File** option, click **Next**, and browse to the image created in the previous step. Clicking **Finish** will add the image to the tree on the left.



39. Click the + sign to expand out the contents of the custom content image. In the example below, the **vibranium** user's folder is selected. Notice how the **NTUSER.DAT** file is also present in this location.

**PROTIP:** Note in the screenshot below there is a file named **NTUSER.DAT** and another one named **NTUSER.DAT.FileSlack**. The **FileSlack** file contains the slack space of the **NTUSER.DAT** hive. While this can be useful in some cases, for what we are doing here, we can ignore the **FileSlack** files.

The screenshot shows the AccessData FTK Imager interface. The Evidence Tree pane on the left displays a hierarchical file structure. A red box highlights the 'CustomContentImage.ad1' entry under 'Custom Content Image([Multi]) [AD1]'. Below it, the 'vibranium' user folder is also highlighted with a blue box. The File List pane on the right shows a list of files with their sizes and types. A red arrow points from the 'vibranium' folder in the Evidence Tree to the 'NTUSER.DAT' file in the File List, which is listed as a 'Regular File' with a size of 768.

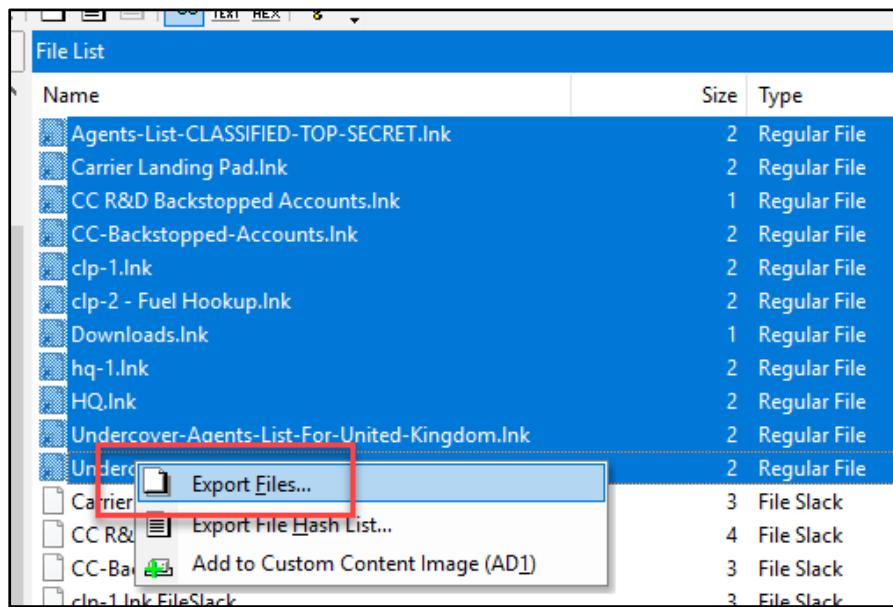
Name	Size	Type
AppData	1	Directory
Links	1	Directory
NTUSER.DAT	768	Regular File
NTUSER.DAT.FileSlack	48	File Slack

40. Navigate to the **[root]\Users\vibranium\AppData\Roaming\Microsoft\Windows\Recent** directory using the tree on the left. Click on the **Recent** folder, then click the **Type** column header to sort by that column.

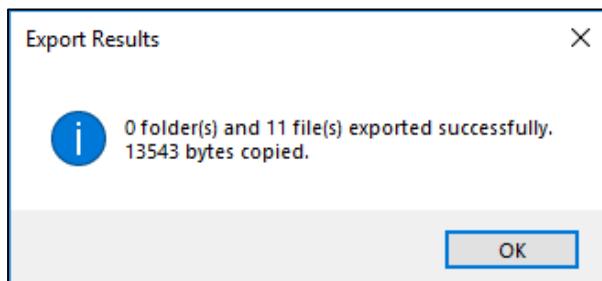
The screenshot shows the AccessData FTK Imager interface. The Evidence Tree pane on the left displays a hierarchical file structure. A red circle labeled '1' is over the 'Recent' folder under the 'vibranium\Roaming\Microsoft\Windows' path. The File List pane on the right shows a list of files with their sizes and types. A red circle labeled '2' is over the 'Type' column header. The list includes various files like 'Agents-List-CLASSIFIED-TOP-SECRET.Ink', 'Carrier Landing Pad.Ink', etc., with their corresponding sizes and file types (e.g., Regular File, File Slack).

Name	Size	Type
Agents-List-CLASSIFIED-TOP-SECRET.Ink	2	Regular File
Carrier Landing Pad.Ink	2	Regular File
CC R&D Backstopped Accounts.Ink	1	Regular File
CC-Backstopped-Accounts.Ink	2	Regular File
clp-1.Ink	2	Regular File
clp-2 - Fuel Hookup.Ink	2	Regular File
Downloads.Ink	1	Regular File
hq-1.Ink	2	Regular File
HQ.Ink	2	Regular File
Undercover-Agents-List-For-United-Kingdom.Ink	2	Regular File
Undercover-Agents-List-For-United-States.Ink	2	Regular File
Carrier Landing Pad.Ink.FileSlack	3	File Slack
CC R&D Backstopped Accounts.Ink.FileSlack	4	File Slack
CC-Backstopped-Accounts.Ink.FileSlack	3	File Slack
clp-1.Ink.FileSlack	3	File Slack
clp-2 - Fuel Hookup.Ink.FileSlack	3	File Slack
hq-1.Ink.FileSlack	3	File Slack
HQ.Ink.FileSlack	3	File Slack
Undercover-Agents-List-For-United-States.Ink.FileSlack	3	File Slack

41. Select the entries that end in .lnk (of Type Regular File), then right-click on a selected file to bring up a context menu. Select **Export files...** from the context menu.



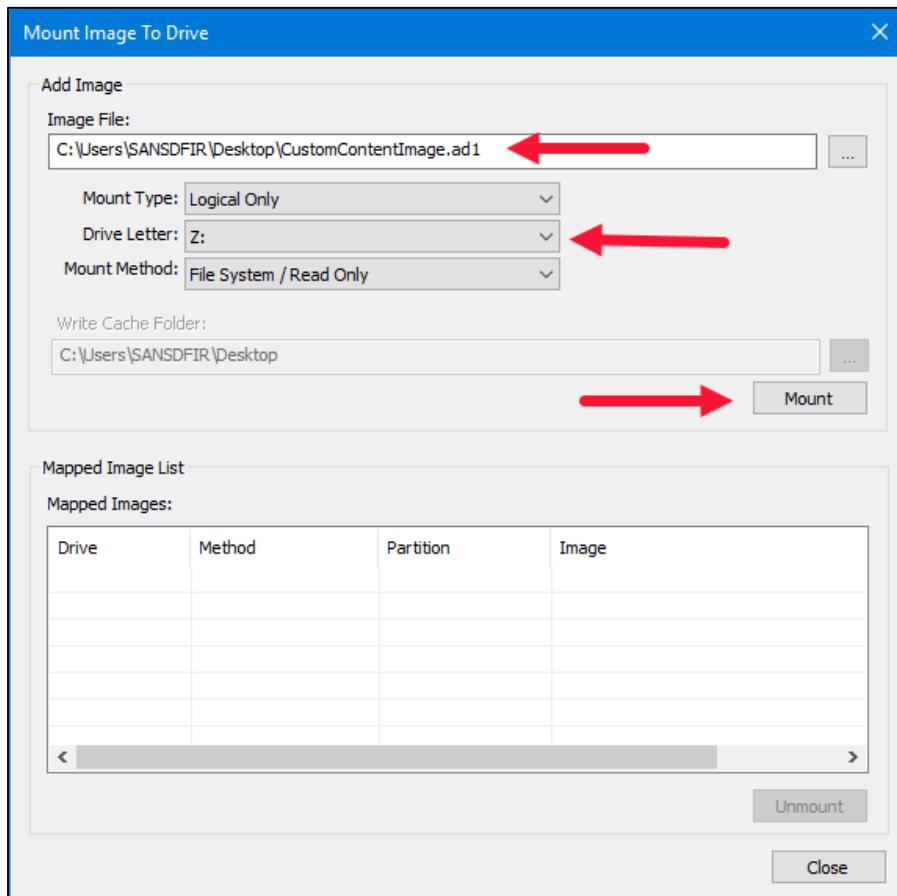
42. In the **Browse For Folder** dialog, make a new folder on the **Desktop** named **Exported lnk files**, then click **OK**. FTK imager will export the files from the image and display the results of the operation.



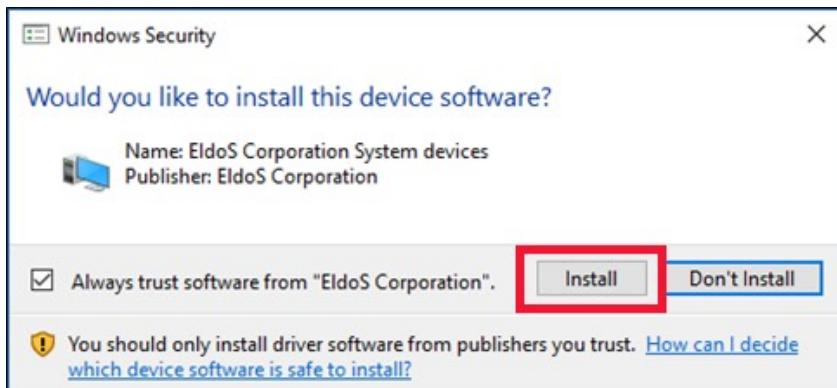
43. The new directory will contain the **lnk** files that were exported from the image. These files can now be processed using any tools or techniques required for your case.

Name	Date modified	Type	Size
Agents-List-CLASSIFIED-TOP-SECRET	4/4/2012 11:43 AM	Shortcut	2 KB
Carrier Landing Pad	4/4/2012 11:36 AM	Shortcut	2 KB
CC R&D Backstopped Accounts	4/4/2012 11:42 AM	Shortcut	1 KB
CC-Backstopped-Accounts	4/4/2012 11:42 AM	Shortcut	2 KB
clp-1	4/4/2012 11:36 AM	Shortcut	2 KB
clp-2 - Fuel Hookup	4/4/2012 11:36 AM	Shortcut	2 KB
Downloads	4/3/2012 6:40 PM	Shortcut	1 KB
HQ	4/4/2012 11:37 AM	Shortcut	2 KB
hq-1	4/4/2012 11:37 AM	Shortcut	2 KB
Undercover-Aagents-List-For-United-Kingdom	4/4/2012 11:43 AM	Shortcut	2 KB
Undercover-Aagents-List-For-United-States	4/4/2012 11:42 AM	Shortcut	2 KB

44. Finally, let's mount the entire custom content image as a drive letter. We will use this drive letter in the next stage of this lab to process some of the files contained in the image, but by mounting the image, we do not need to manually export out files to process them. First, click on the custom content image in the Evidence tree in **FTK imager**.
45. With the **Custom Content Image** selected, click **File → Image Mounting** and review the options shown.
46. Change the Drive Letter to **Z:\**, then click the **Mount** button to map the image to a drive letter. Notice how **FTK** automatically picks the next available letter. This is usually fine, but we want to use **Z:** for this exercise.



47. If you are prompted to install device software, click **Install**.



In some cases, the first time the driver is installed, the image may not mount properly. If this happens, close the dialog informing you of the error, restart **FTK imager**, and repeat the above process.

48. The **Mount Image To Drive** dialog now shows the container being accessible via a drive letter. In the example below, it is the **Z:** drive.

Mapped Image List			
Mapped Images:			
Drive	Method	Partition	Image
Z:	File System/Read Only	File System	C:\Users\SANSDFR\Desktop\CustomCor

49. With the image now mounted as a drive letter, we can process the files contained within the image.

**NOTE:** DO NOT CLOSE FTK IMAGER! If you do, the mounted directory will disappear and not be available anymore!

However, you can close the **Mount Image To Drive** dialog box and then minimize **FTK Imager**, if you like.

### Exercise Questions

1. Using the shortcut on the **Desktop**, start a new instance of **PowerShell**. You will be in the **C:\Tools** directory.
2. In the **PowerShell** window, type the following command:

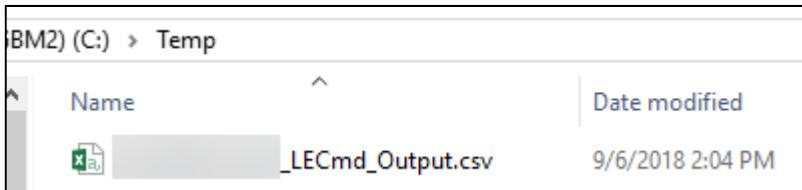
```
. \LECmd.exe -d z:\ --csv C:\Temp\ -q
```

This command assumes you mapped the **Custom Content Image** to drive letter **Z:** as described previously. If not, be sure to adjust the drive letter here to reflect where you mounted the **Custom Content Image**.

This command is processing all the **Ink** files found in the **Custom Content Image** and generating a CSV which we can then analyze in **Timeline Explorer**.

**NOTE:** Any errors in parsing can be ignored.

3. Once **LECmd** finishes, open **Timeline Explorer** and drag and drop the CSV file generated by **LECmd** into **Timeline Explorer**. The filename should look something like this:



4. Once the file is loaded in **Timeline Explorer**, answer the following questions.

a. How many **Ink** files have a **Drive Type** of '**Fixed storage media (Hard drive)**'? (Hint: Use the filter in the **Drive Type** column).

---

b. How many **Ink** files point to items located on the device with **Volume Serial Number** '**E06CC564**'?

---

c. How many **Ink** files have a **Local Path** that points to Excel documents (either .xls or .xlsx file extensions)?

---

d. How many **Ink** files were first opened in April of 2012? (Hint: A **Ink** file is created when a document is opened. The **Source Created** column contains the creation time of the **Ink** file).

---

e. How many **Ink** files have no **Arguments** at all?

---

f. What are the unique **Machine ID** values found across all the **Ink** files (ignore blank entries)?

---

**NOTE:** When done with this exercise, REBOOT your SIFT workstation to unmount everything. This can also be done by simply closing **FTK Imager** and **AIM**, but a quick reboot is the easiest way to reset things.

**Exercise Questions with Step-by-Step**

1. Using the shortcut on the **Desktop**, start a new instance of **PowerShell**. You will be in the **C:\Tools** directory.
2. In the **PowerShell** window, type the following command:

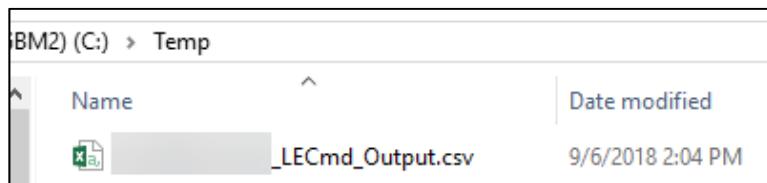
```
.\LECmd.exe -d z:\ --csv C:\Temp\ -q
```

This command assumes you mapped the **Custom Content Image** to drive letter Z: as described previously. If not, be sure to adjust the drive letter here to reflect where you mounted the **Custom Content Image**.

This command is processing all the **Ink** files found in the **Custom Content Image** and generating a CSV which we can then analyze in **Timeline Explorer**.

**NOTE:** Any errors in parsing can be ignored.

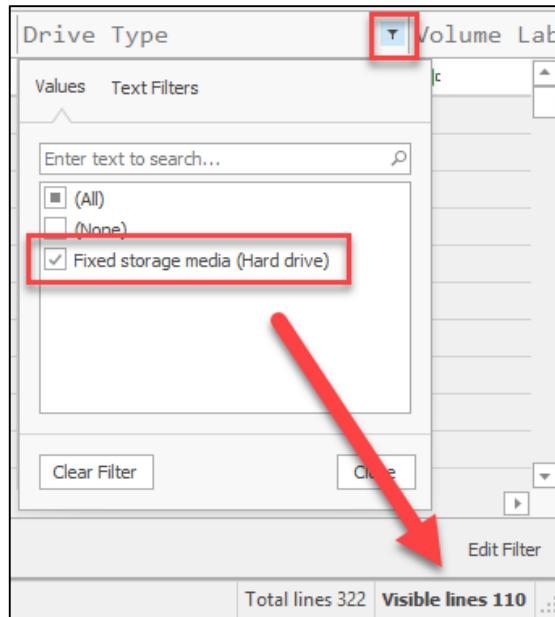
3. Once **LECmd** finishes, open **Timeline Explorer** and drag and drop the CSV file generated by **LECmd** into **Timeline Explorer**. The filename should look something like this:



4. Once the file is loaded in **Timeline Explorer**, answer the following questions.

- a. How many **Ink** files have a **Drive Type** of ‘**Fixed storage media (Hard drive)**’? (Hint: Use the filter in the **Drive Type** column).

**Using the Drive Type filter and selecting the appropriate value, we see there are 110 visible lines.**



- b. How many **Ink** files point to items located on the device with **Volume Serial Number** ‘**E06CC564**’?

**Entering a value of E06CC564 in the Volume Serial Number column shows there are two lines with that serial number.**

	Volume Serial Number	Drive Type
08...	E06CC564	Fixed storage med
08...	E06CC564	Fixed storage med

The status bar at the bottom right shows 'Total lines 307' and 'Visible lines 2'.

- c. How many **Ink** files have a **Local Path** that points to Excel documents (either .xls or .xlsx file extensions)?

Since we are interested in two extensions, and one is contained in the other, filtering on the Local Path column for .xls shows 16 lines visible. The file names of each unique file are shown below.

- Undercover-Agents-List-For-United-States.xlsx
  - Undercover-Agents-List-For-Australia.xls
  - Undercover-Agents-List-For-United-Kingdom.xls
  - CC-Backstopped-Accounts.xlsx
  - Credit-Card-Numbers-For-Research.xlsx
  - CC-Backstopped-Accounts.xlsx
  - Credit-Card-Numbers-For-Research.xlsx
  - Undercover-Agents-List-For-United-Kingdom.xls
  - Undercover-Agents-List-For-United-States.xlsx
- d. How many **Ink** files were first opened in April of 2012? (Hint: A **Ink** file is created when a document is opened. The **Source Created** column contains the creation time of the **Ink** file).

Filtering on the Source Created column for April, 2012 shows that 49 files were created in that month.

Source Cre...	Source Modifi...	Source Access...	Target
=	=		
2012-04-04 12...	2012		
2012-04-04 12...	2012		
2012-04-04 12...			
2012-04-03 22...	2012		
2012-04-03 22...	2012		
2012-04-03 22...			
2012-04-01 14...	2010		
2012-04-04 15...	2012		
2012-04-04 15...	2012		
2012-04-04 15...	2012		
2012-04-04 15...	2012		
2012-04-03 22...	2011		
2012-04-03 21...	2012		
2012-04-03 21...	2012		
2012-04-04 15...	2012		
2012-04-04 15...	2012		
2012-04-04 15...	2012		
0:00' And [Source Created] < '2012-05-01			
		Total lines 322	Visible lines 49

- e. How many **lnk** files have no **Arguments** at all?

Filtering on the Arguments column for (*Blanks*) shows that there are 270 lnk files that meet this criterion.

The screenshot shows a software interface for filtering data. At the top, there's a header with columns: Target, ID, Ab. Below it, a toolbar has 'Values' and 'Text Filters' tabs, with 'Text Filters' selected. An 'Enter text to search...' input field is present. A list of filters includes '(All)' and '(Blanks)', with '(Blanks)' checked. Buttons for 'Clear Filter' and 'Close' are at the bottom left. The main area shows a list of items, with a red arrow pointing from the '(Blanks)' checkbox down to the status bar which displays 'Visible lines 270'.

- f. What are the unique **Machine ID** values found across all the **lnk** files (ignore blank entries)?

While this can be answered by sorting by Machine ID and scrolling through the results, it is much easier to group by the Machine ID column (drag and drop this column to the Group by area).

When you are done reviewing things, drag the column header back into the header row to ungroup.

	Line	Tag	Source File	Source Cr
▼	=			=
▶	> Machine ID:		(Count: 96)	
▶	> Machine ID:	3714247d28-05	(Count: 6)	
▶	> Machine ID:	controller	(Count: 2)	
▶	> Machine ID:	nana-home	(Count: 6)	
▶	> Machine ID:	win-dc3j5p1qj61	(Count: 107)	
▶	> Machine ID:	win-v5t3csp8u4h	(Count: 14)	
▶	> Machine ID:	wks-win732bita	(Count: 91)	

The unique values are:

3714247d28-05

controller

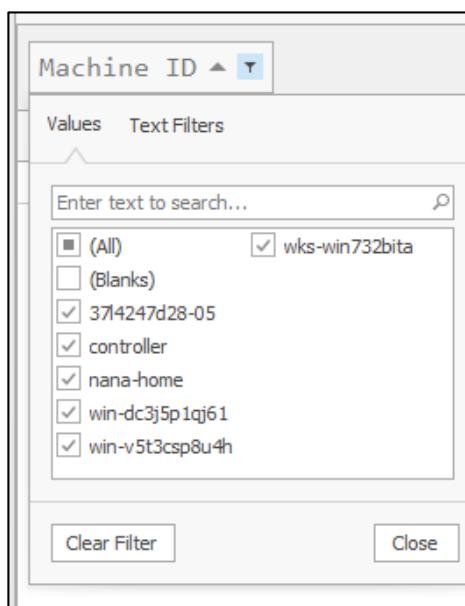
nana-home

win-dc3j5p1qj61

win-v5t3csp8u4h

wks-win732bita

These values can also be observed in the *Machine ID* column filter:



**NOTE:** When done with this exercise, REBOOT your SIFT workstation to unmount everything. This can also be done by simply closing **FTK Imager** and **AIM**, but a quick reboot is the easiest way to reset things.

### Exercise—Key Takeaways

- Being able to manually locate and select files on a live system or from a mounted image can save considerable time, since you can quickly get to the data you need.
- FTK Imager allows for specifically adding files to a custom image as well as being able to specify things using wildcards. Using wildcards can save time because FTK Imager will find and add matching files automatically.
- Once data is collected into a Custom Content Image, the image file can be mounted using FTK Imager to allow access to analytical tools.

# © SANS Institute 2020

## Exercise 3.4—Host Based Live Acquisition

### Background

In a previous lab, we discussed and saw how a targeted triage collection can be done against both a live system, as well as a forensic image such as an E01. There are, however, some cases where a triage collection will not suffice. The primary case in this regard would be when full disk encryption is detected. Because of the catastrophic results should a computer be shut down when encryption is present, it becomes necessary to image the computer while it is running. This effectively bypasses the encryption which allows us to get to all the files on the logical volume.

When encryption is present, it becomes necessary to image logical volumes vs physical ones. If the physical device is imaged, the encryption may still be in place and the imaging exercise would be moot as we would not have access to the data...without encryption keys.

### Objectives

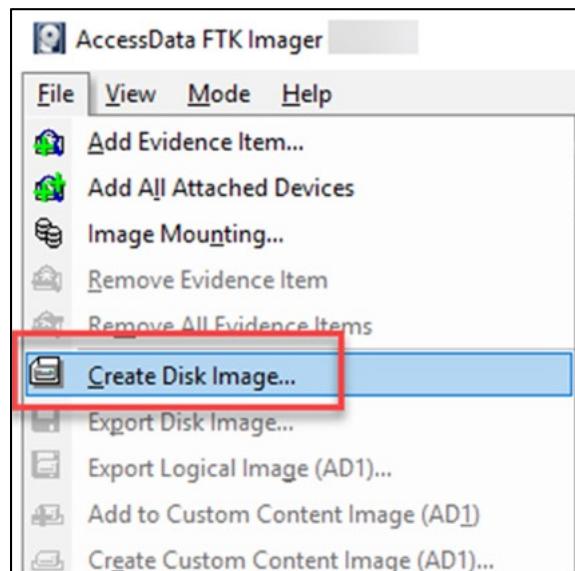
- Use FTK Imager to create a logical and physical disk image on a running computer
- Understand the differences between targeting a logical partition vs. physical device

### Exercise Preparation

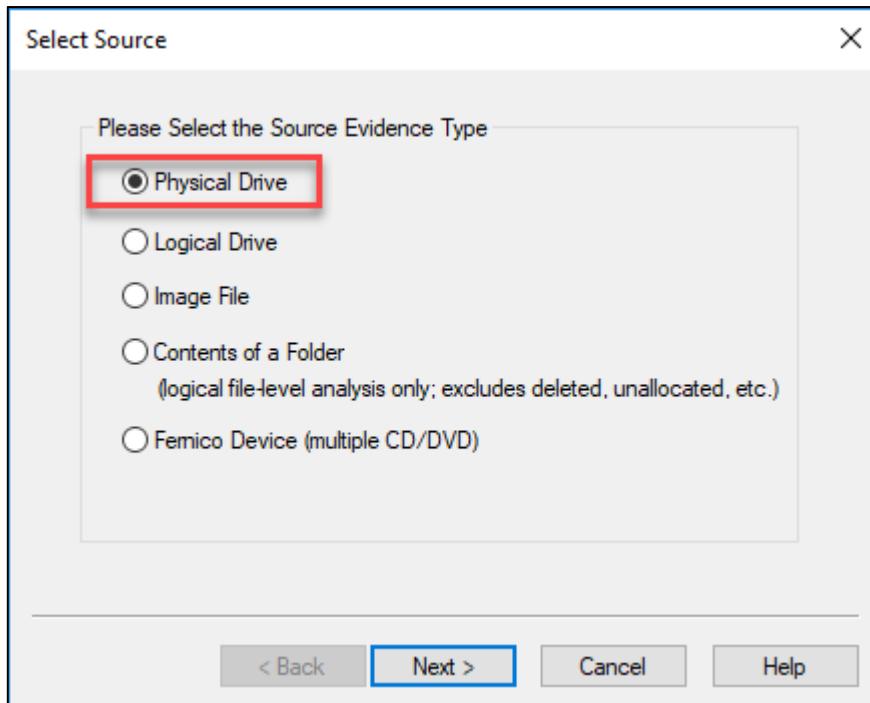
1. Boot your **FOR498 Windows VM**
2. Login to the **FOR498 Windows VM** using the following credentials:
  - a. Username: **SANSDFIR**
  - b. Password: **forensics**
3. On your **VM**, start **FTK Imager** by double clicking the **FTK Imager** shortcut in the **Acquisition Tools** fence on the **Desktop**.



4. To start the imaging process, click **File, Create Disk Image**.

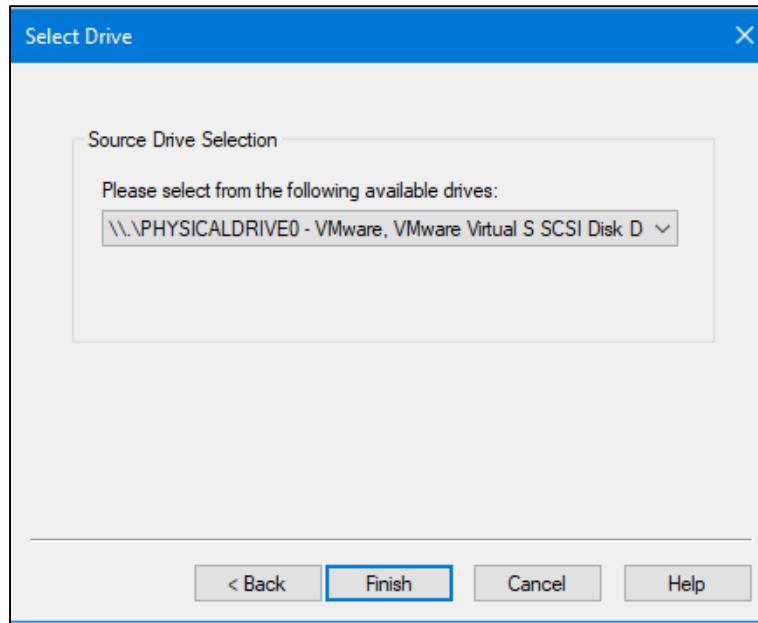


5. In the **Select Source** dialog, make sure **Physical Drive** is selected, then click **Next**.

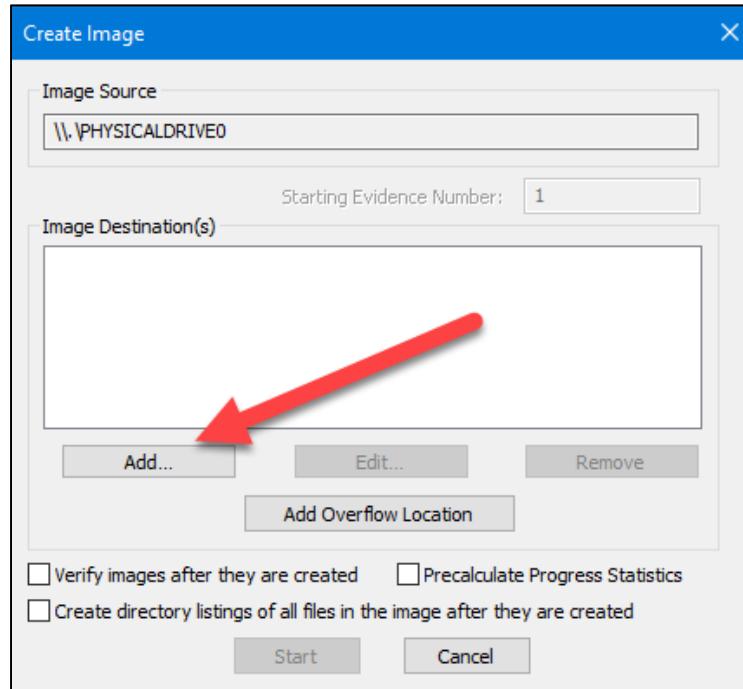


6. In the **Select Drive** dialog, select the physical device you want to image. Each device contains the manufacturer and size which can be used to ensure you select the proper device. Once the proper device is selected, click **Finish**.

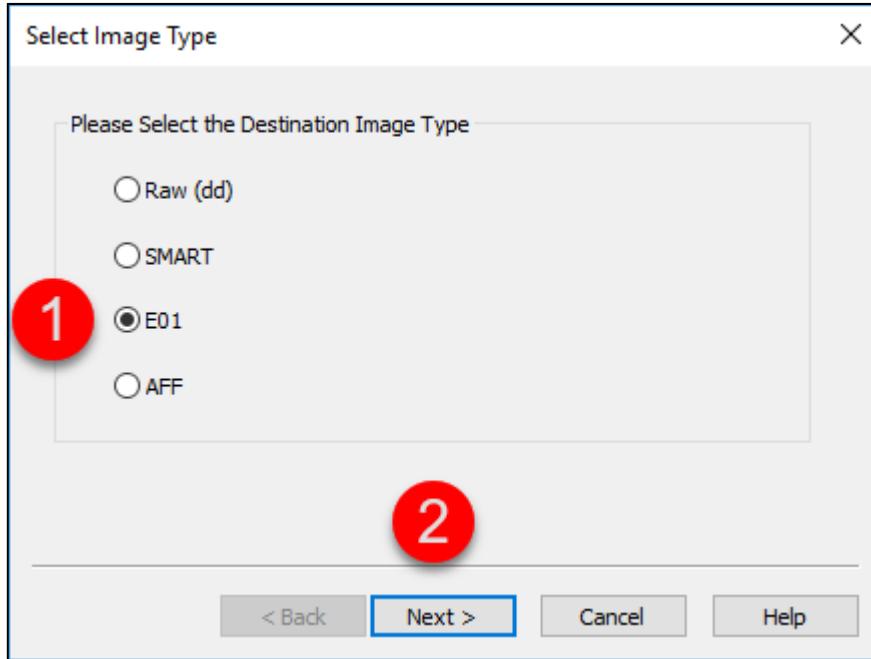
Since we are in the virtual machine, your drive should look very similar to what is shown below. When in doubt, select **PYHICALDRIVE0** from the dropdown list.



7. Next, click the **Add...** button, which brings up a wizard to choose the imaging format and location to save the image.



8. In the **Select Image Type** dialog, select **E01**, then click **Next**. Notice there are also other options available, but generally, E01 is the best choice, primarily because it compresses the data being imaged.



9. In the **Evidence Item Information** dialog, populate the fields with the appropriate data, then click **Next**.

Evidence Item Information

Case Number: FOR498 physical image

Evidence Number: 12345-p

Unique Description: Physical image of a drive

Examiner: <your name here>

Notes: Dell Dimension sn ABC123, Room 4

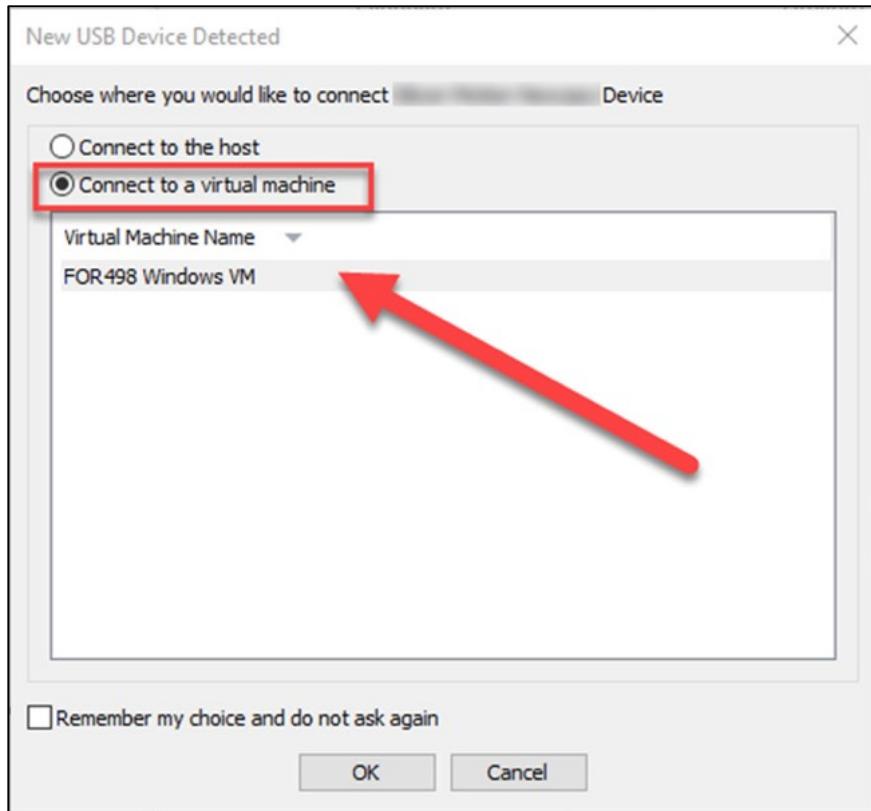
< Back **Next >** Cancel Help

Be as detailed as possible. It is often a good idea to include not only information about the device itself (storage device make, model, and serial #), but also information about the computer and from where the device came (make, model, and serial number, along with the room or location it was seized from).

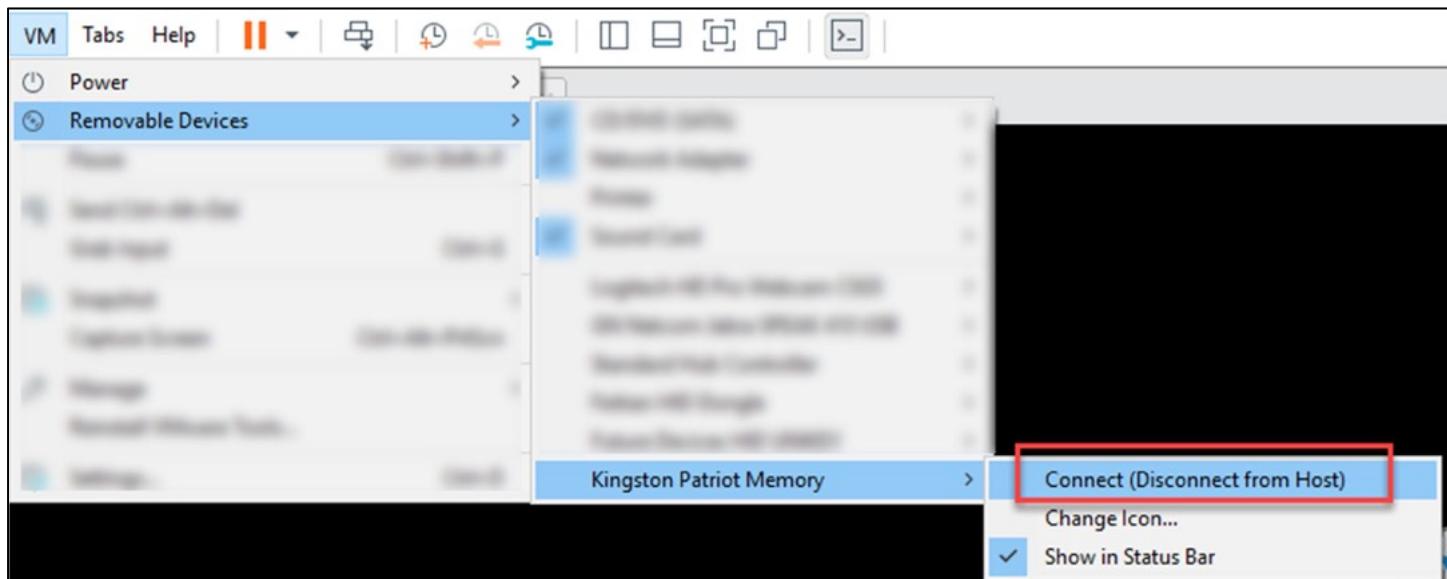
10. Connect the external drive you brought with you to class to your host computer, then connect the device to the virtual machine when prompted by VMWare.

**BEWARE:** If your device is not recognized, it is almost certainly because SAFE Block is blocking it from the SAFE Block Exercise you did yesterday. In this case, just go to SAFE Block and unblock the device.

**NOTE:** In cases where your VM will not allow for external device connection, insert your supplied USB 2.0 hub, and connect through this.



You can also do it manually via the menus at the top.

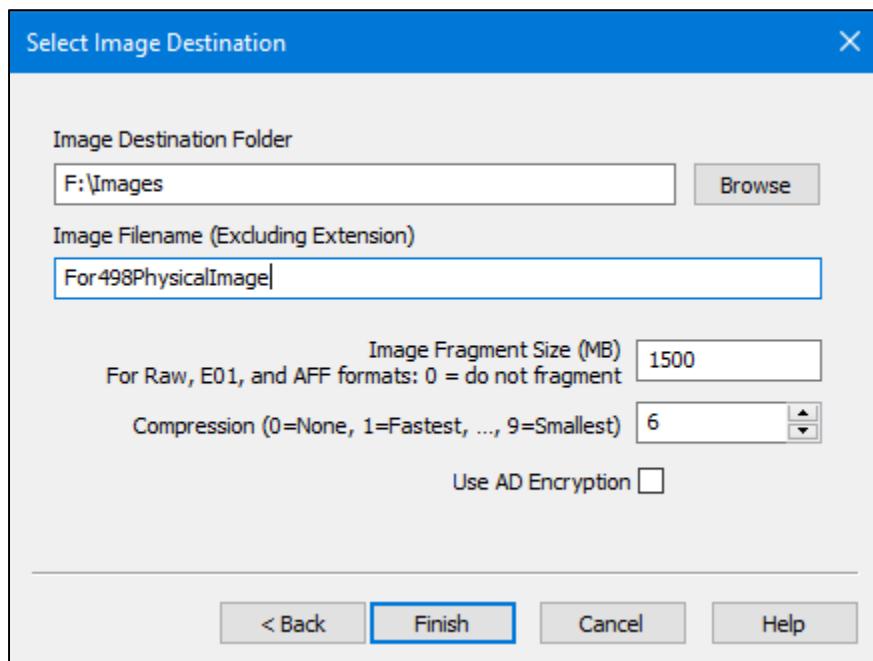


11. Using **File Explorer**, determine what drive letter your external device was assigned. In the example below, it has been assigned drive letter **F:**

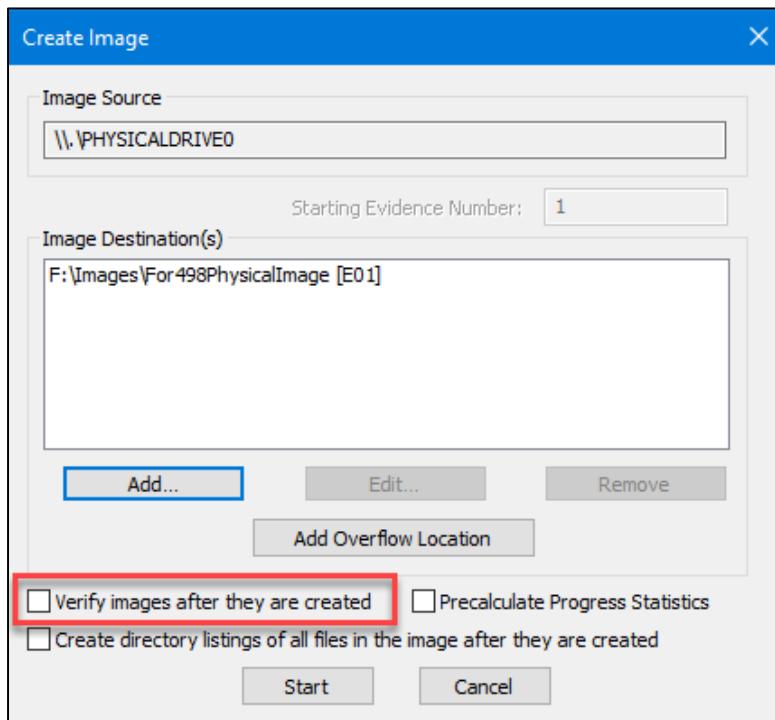


12. In the **Select Image Destination** dialog, click the **Browse** button and select the drive letter you identified above. If you do not have a directory named **Images** on the drive, create one, then select the **Images** folder and click **OK**. For the **Image Filename**, enter **FOR498PhysicalImage** without any extension. While **Image Fragment Size** can be adjusted, the defaults are usually fine. When the **Folder** and **Filename** are populated, click **Finish**.

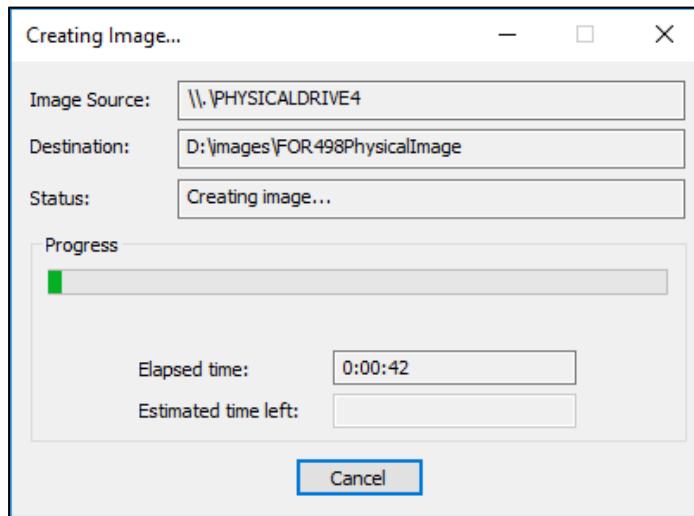
**NOTE:** You would never save a disk image to the computer you are imaging, but even if you tried, a warning would be displayed informing you that the destination must be different than the source.



13. After the **Finish** button is clicked, the **Image Destinations(s)** list is populated. Make sure the **Verify images after they are created** box is unchecked, then click **Start** to begin imaging. The verify option hashes the E01 and compares it to the source drive to ensure an exact copy was made. This adds time to the process, but it is important to ensure the integrity of the data. Since it adds extra time, we will skip it for now.



14. A progress window is displayed showing the status of the imaging process.



15. While imaging is taking place, files are being created in the F:\images directory. Here is an example of what they might look like (your images will be under the drive letter that was assigned by Windows):

(D:) > images			
Name	Date modified	Type	Size
FOR498PhysicalImage.E01	9/21/2018 9:39 AM	E01 File	1,535,865 KB
FOR498PhysicalImage.E02	9/21/2018 9:39 AM	E02 File	1,535,939 KB
FOR498PhysicalImage.E03	9/21/2018 9:39 AM	E03 File	0 KB

The size of the drive and the Image Fragment Size that was used determines how many segments will be created. Forensic tools know how to put the pieces back together though, so when processing the image in a forensic tool, simply choose the file with the E01 extension and the tool will take care of the rest.

16. Rather than wait for the image to finish, click **Cancel** in the **Creating Image** dialog. This will abort the imaging process. If the process could continue, we would, of course have many image segments, along with a text file that contains information about the imaging process. An example of what that might look like is below:

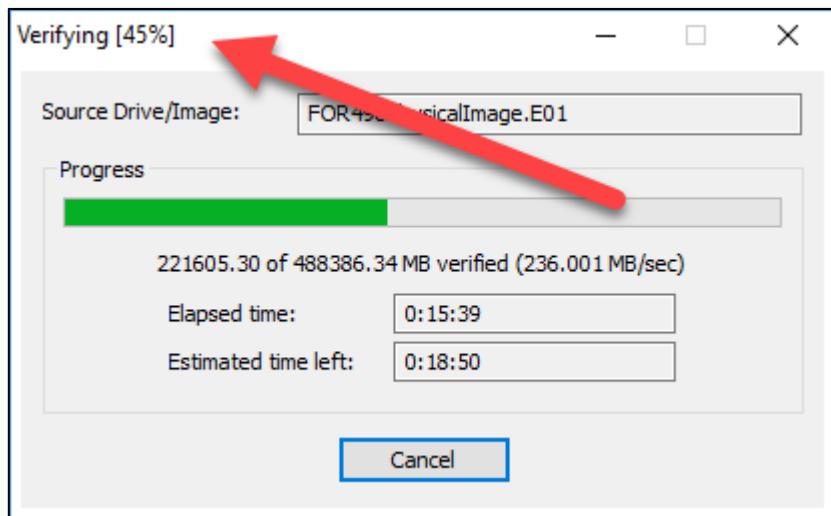
```
For498PhysicalImage.E01.txt
NOTICE: The imaging operation was cancelled! This image is incomplete!
Created By AccessData® FTK® Imager [REDACTED]

Case Information:
Acquired using: ADI [REDACTED]
Case Number: FOR498 physical image
Evidence Number: 12345-p
Unique description: Physical image of a drive
Examiner: <your name here>
Notes: Dell Dimension sn 12345, Room 4

-----
Information for F:\Images\For498PhysicalImage:
Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 13,054
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 209,715,200
[Physical Drive Information]
Drive Model: VMware, VMware Virtual S SCSI Disk Device
Drive Interface Type: SCSI
Removable drive: False
Source data size: 102400 MB
Sector count: 209715200
[Computed Hashes]
MD5 checksum: d86a57e2f11cd130963d9419fec17bf3
SHA1 checksum: 330bfce3c25cf055571f8df8a267ed4b50613256

Image Information:
Acquisition started: Wed Jan 30 11:18:54 2019
Acquisition finished: Wed Jan 30 11:19:21 2019
Segment list:
F:\Images\For498PhysicalImage.E01
```

Additionally, after imaging completes, and assuming the verify option was checked as would be the recommendation, a verification dialog is shown.



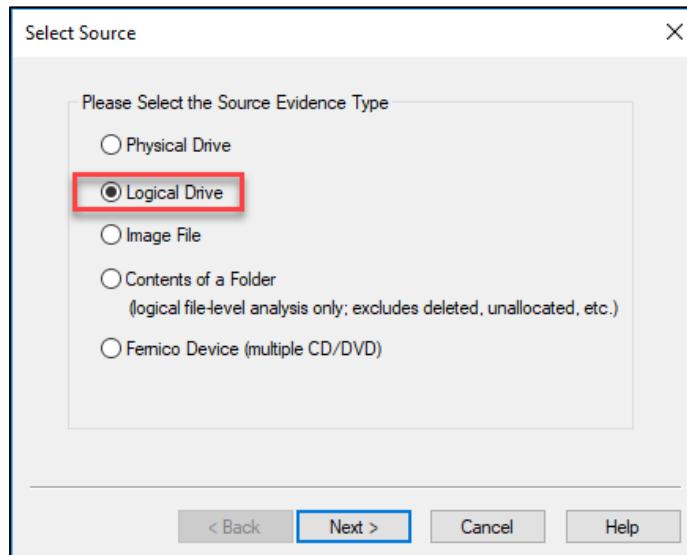
When verification finishes, the results are displayed:

Drive/Image Verify Results	
Name	FOR498PhysicalImage.E01
Sector count	1000215216
MD5 Hash	
Computed hash	7e589667ad764009f9b571e49d639a58
Stored verification hash	7e589667ad764009f9b571e49d639a58
Report Hash	7e589667ad764009f9b571e49d639a58
Verify result	Match
SHA1 Hash	
Computed hash	1f2251f333d34d2bbd02749b9c4d302064a1b:
Stored verification hash	1f2251f333d34d2bbd02749b9c4d302064a1b:
Report Hash	1f2251f333d34d2bbd02749b9c4d302064a1b:
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image
Close	

**Note:** Normally you would run your collection tools from external media. You would also save the results of your collection to external media. For class purposes, we will launch our collection tools from either your host system or the VM.

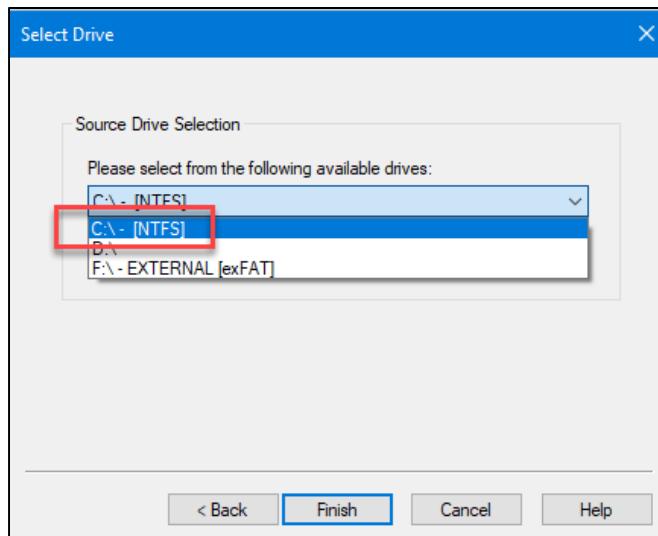
The following process will be like the previous one but pay attention to the source of the data being collected.

17. On your VM, start **FTK Imager** via the shortcut in the **Acquisition Tools** fence on the **Desktop** if it is not already running.
18. To start the imaging process, click **File, Create Disk Image**.
19. Select **Logical Drive** in the **Select Source** dialog, and then click **Next**.

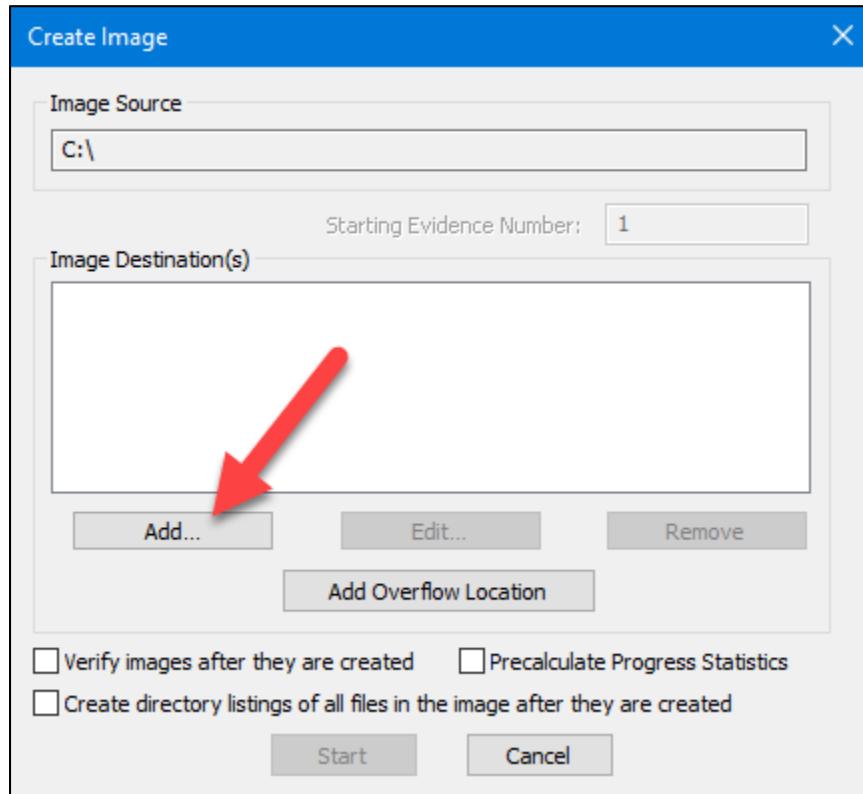


20. In the **Source Drive Selection**, select the C:\ drive from the list of available drives, and click **Finish**.

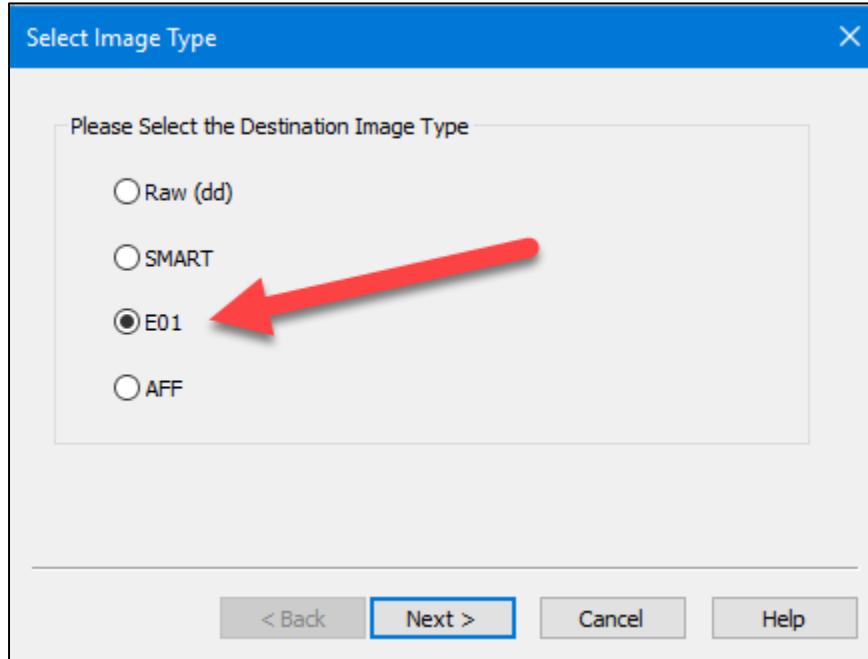
**Note:** Your drives may be different than what is shown below.



21. Click the **Add** button.



22. Select **E01** and click **Next**.



23. Fill out the details like we did in the previous stage, adjusting as necessary for things like **Evidence Item Information** and **Destination**:

**Evidence Item Information**

Case Number:	FOR498 logical image
Evidence Number:	12345-p
Unique Description:	Logical image of a drive
Examiner:	<your name here>
Notes:	Dell Dimension sn ABC123, Room 4

< Back    Next >    Cancel    Help

**Select Image Destination**

Image Destination Folder	F:\Images	Browse
Image Filename (Excluding Extension)	FOR498LogicalImage	
Image Fragment Size (MB)	1500	
For Raw, E01, and AFF formats: 0 = do not fragment		
Compression (0=None, 1=Fastest, ..., 9=Smallest)	6	
Use AD Encryption	<input type="checkbox"/>	

< Back    Finish    Cancel    Help

24. Once the imaging process is started, it functions as seen when imaging a physical device.
25. Once the logical image is underway, click **Cancel**.

**Exercise Questions**

- When imaging a drive, in what situations may the hashes not match?

---

---

---

---

- Can the type of drive being imaged affect whether the hashes match? Why, or why not?

---

---

---

- On a single device, can a logical partition be bigger than the physical device that contains it? Why or why not?

---

---

---

- On a single device, will a logical partition always be the same size as the physical device? Why or why not?

---

---

---

- On a single device, in what situations would you want to image the logical partition vs. the physical device?

---

---

---

- When imaging a drive, in what situations may the hashes not match?

The hashes should almost always match unless something went wrong when storing the image on the destination drive. The source hash is calculated during imaging, and when imaging is complete, this hash is then recomputed from the destination image. If the image was stored properly on the destination, the hashes should match. Keep in mind however, that this hash would most certainly not match any subsequent image of a live system since the data on the live system would most likely change between creating each image. Also, hard drives with damaged platter surface or damage to data areas may cause drive verification errors, as the contents have been changed by the imaging software. Imaging the hard drive via a write-blocker after the drive is removed from a device can prevent this in most cases (see the next question).

- Can the type of drive being imaged affect whether the hashes match? Why, or why not?

For any given image from start to finish, the hashes will most likely match, but if you start the process over (i.e. power down the SSD and power it up again), then take another image, the hash will almost certainly change because of wear leveling and TRIM.

- On a single device, can a logical partition be bigger than the physical device that contains it? Why or why not?

No, a logical partition could not exceed the size of the physical device, but a logical device can be smaller than the physical device if a logical partition was made that was smaller than the size of the physical device. The remaining space on the physical device can be assigned to a different partition or left as is. Of course, in a damaged or malfunctioning device, things may look differently than when a drive is performing normally.

- On a single device, will a logical partition always be the same size as the physical device? Why or why not?

No, if someone creates more than one partition on a drive, the logical partitions will be smaller than the physical drive.

- On a single device, in what situations would you want to image the logical partition vs. the physical device?

When full disk encryption is present, imaging the physical device would result in a copy of the encrypted data being collected, whereas imaging the logical partition will result in a decrypted image being created. Because of this, imaging the logical partition is the correct procedure when encryption is in use.

**Exercise—Key Takeaways**

- Imaging a device is generally a straightforward operation but can be time consuming.
- If encryption is found, it may be necessary to image the logical partition in its unencrypted state while the machine is running.

This page intentionally left blank.

# © SANS Institute 2020

## Exercise 3.5—Dead Box Acquisition

### Background

When we think about acquisition, it brings to mind opening the side of the computer, removing the hard drive, connecting to a write blocker or imaging equipment, and completing the task. While this is not an inaccurate assessment of the task, it does not address a great deal of the access and acquisition questions surrounding so much data today. If there is a requirement to collect a full disk image and you have many more drives to image than you have write blocking hardware, you may be better off imaging the drive inside the machine with a forensically sound Boot USB. This technique and its benefits hold true to dead box triage collections and collecting hard drives that are complicated or impossible to remove in the field.

This rather traditional method of acquisition, known as “dead box” acquisition, can be done both with the hard drive out of the machine, as well as with the hard drive in the machine, although again, outside the machine may make things quicker and safer.

Safer because any time you are attempting to boot a machine even just to collect BIOS/UEFI information, you run the risk of the machine booting to the internal hard drive instead. This would alter information.

It is quicker from the perspective that when you can remove a hard drive from a machine and collect the forensic image through a hardware imaging tool, it will almost always be faster than imaging the hard drive with its host machine.

Many so-called “Ultra Slim” laptops have hard drives soldered directly to the motherboard and cannot be removed. In the case of a computer that you cannot remove the hard drive from, you need other options.

### Exercise Objectives

- Create Paladin boot disk using SANS provided 16 GB USB drive
- Use Paladin boot disk to image hard drive of student computer, using student provided hard drive as destination media

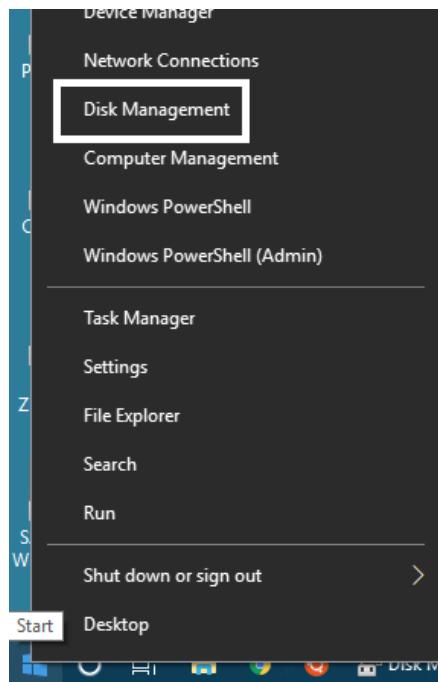
**WARNING:** On some Dell computers (and other brands), if you can't see the host drive once booted into Paladin, go into the BIOS on your host and change **RAID** to **AHCI**. Don't forget to change it back when you are done.

**Exercise – Part 1**

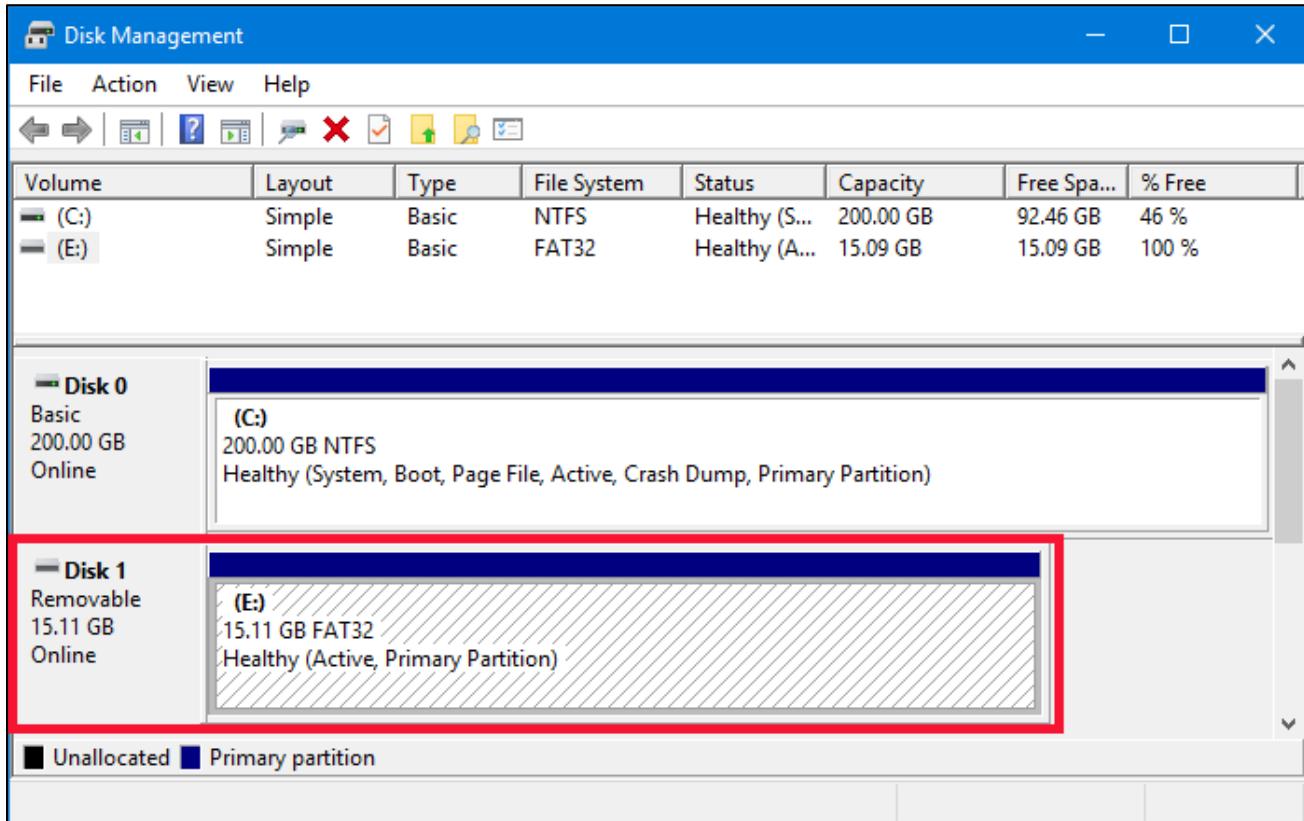
1. Boot your **FOR498 Windows SIFT VM**
2. Login to the **FOR498 Windows SIFT VM** using the following credentials:
  - a. Username: **SANSDFIR**
  - b. Password: **forensics**
3. Plug in your SANS provided 16 GB USB drive and ensure it connects to your **VM**.

**NOTE:** In cases where your VM will not allow for external device connection, insert your supplied USB 2.0 hub, and connect through this. For this lab, it will cause the file transfer to be unacceptably slow. If this occurs, come out of the VM, connect the SANS provided empty USB drive as well as the SANS provided USB-B drive, and you will find a copy of the Paladin files in a folder at the root of that drive. Copy them over from there.

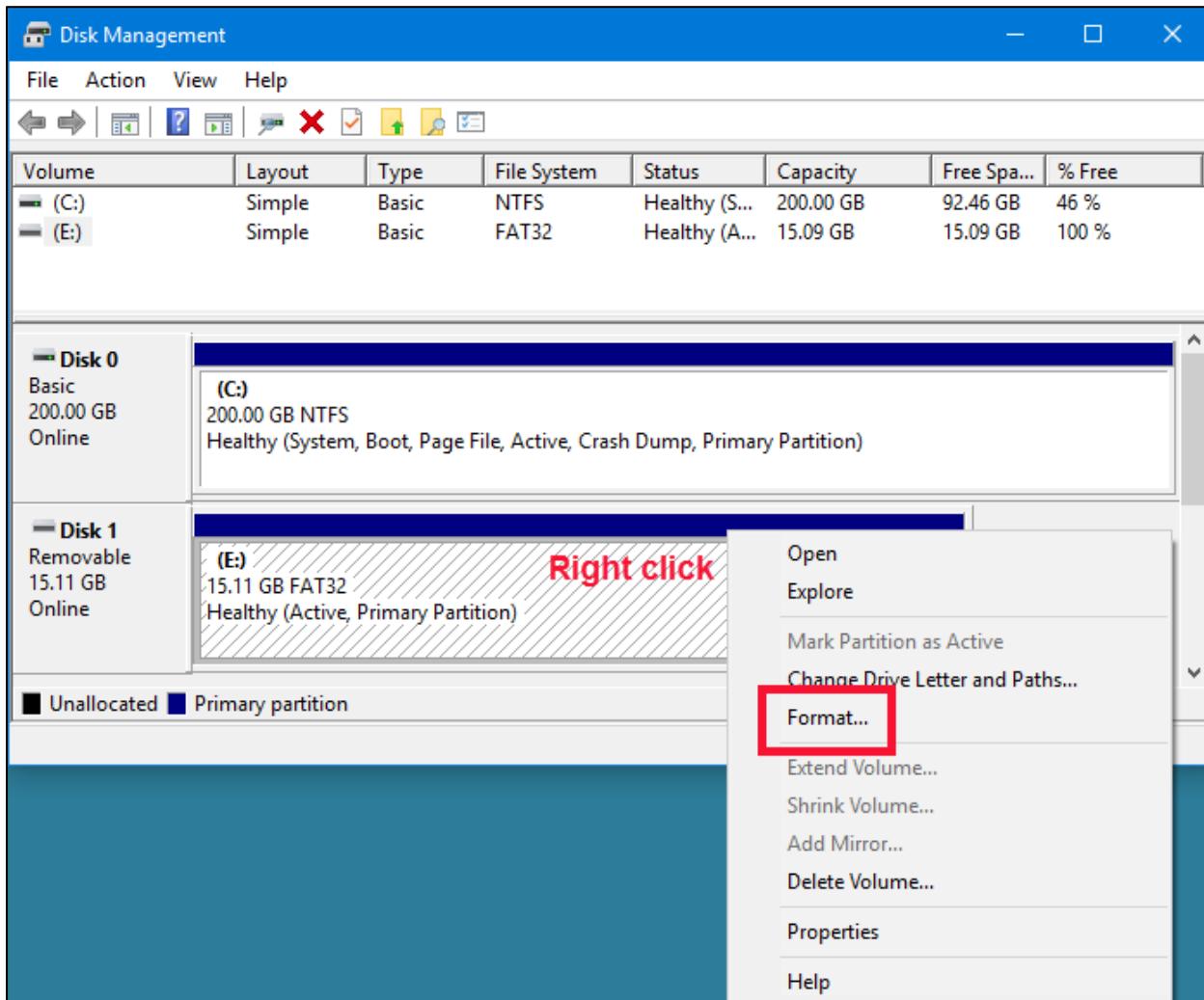
4. Right click on the **Start** button and select **Disk Management** from the menu.



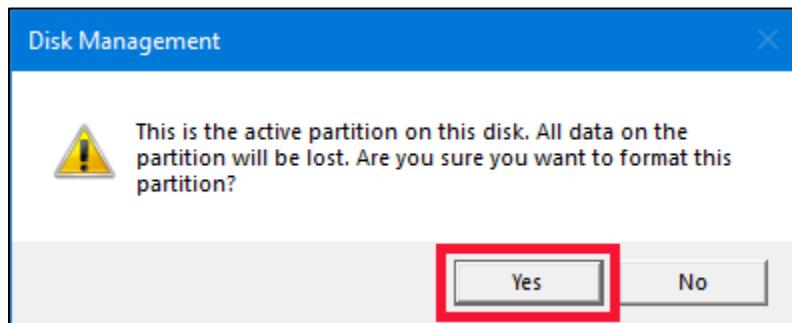
5. The **Disk Management** utility will open. Identify your SANS provided 16 GB USB drive and **Volume** in the list.



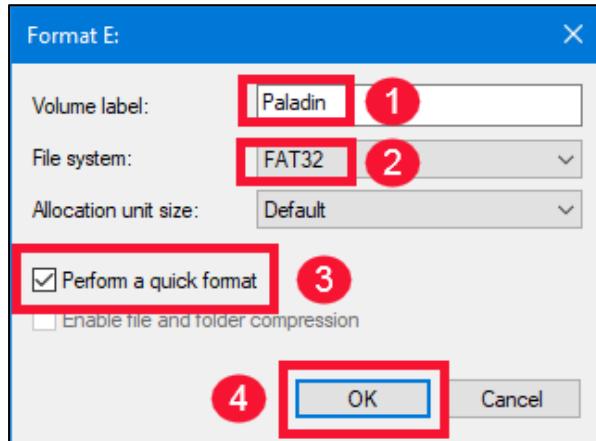
6. Right click on the volume itself and select **Format...**. Make sure you have selected the correct drive! Your volume name, drive letter, and file system type may differ from the screenshot.



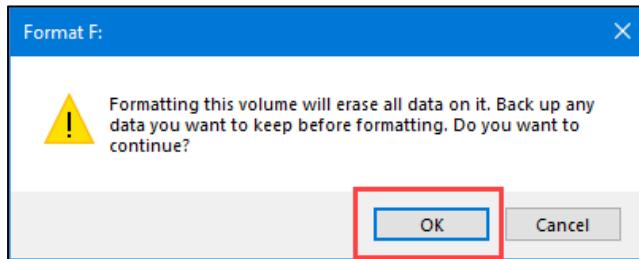
7. A **Disk Management** box may appear, with a warning regarding an active partition on the disk. As long as you are SURE that you are working with the correct drive, click **Yes**.



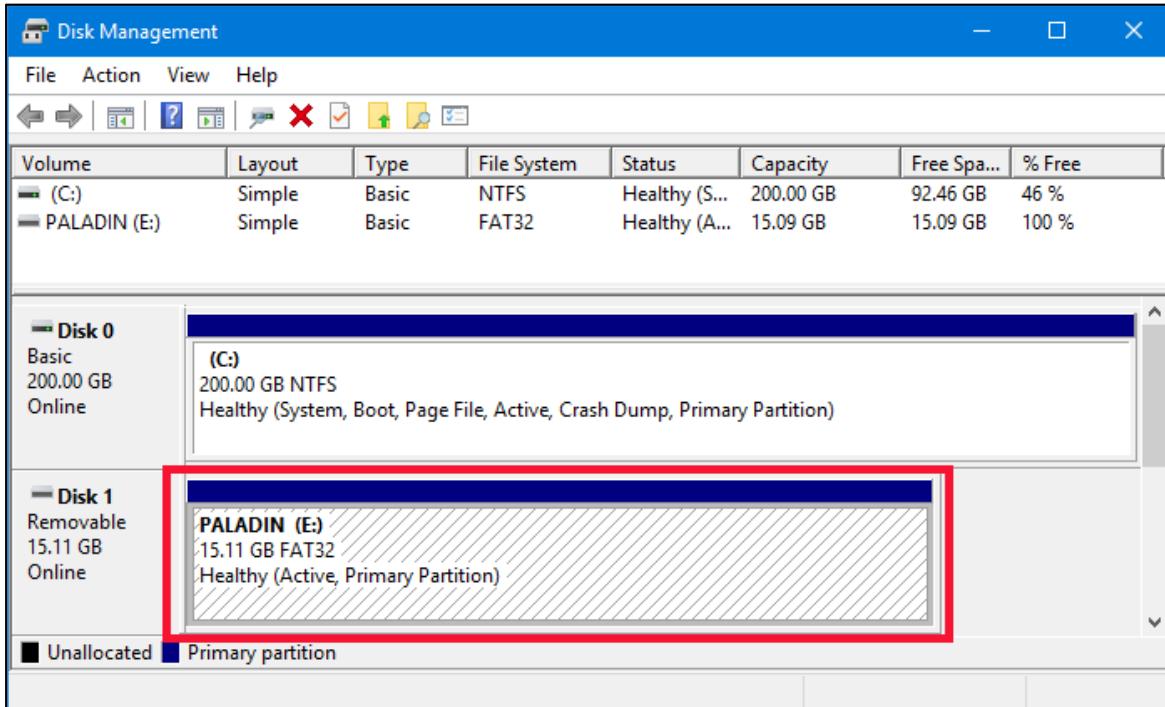
8. A box will appear with a number of options. Set the **Volume label** to **Paladin**. Set the **File system** to **FAT32**. Ensure the **Perform a quick format** is checked and leave everything else as is. Click on **OK**.



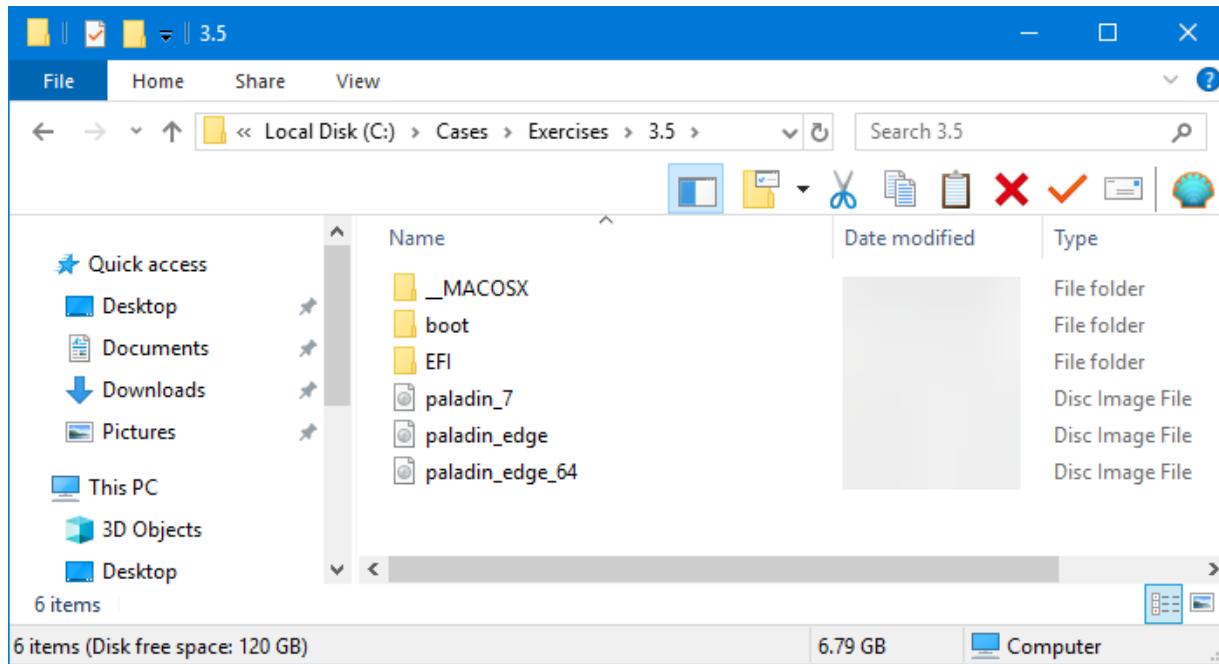
9. A warning message will appear. Click **OK** to accept it.



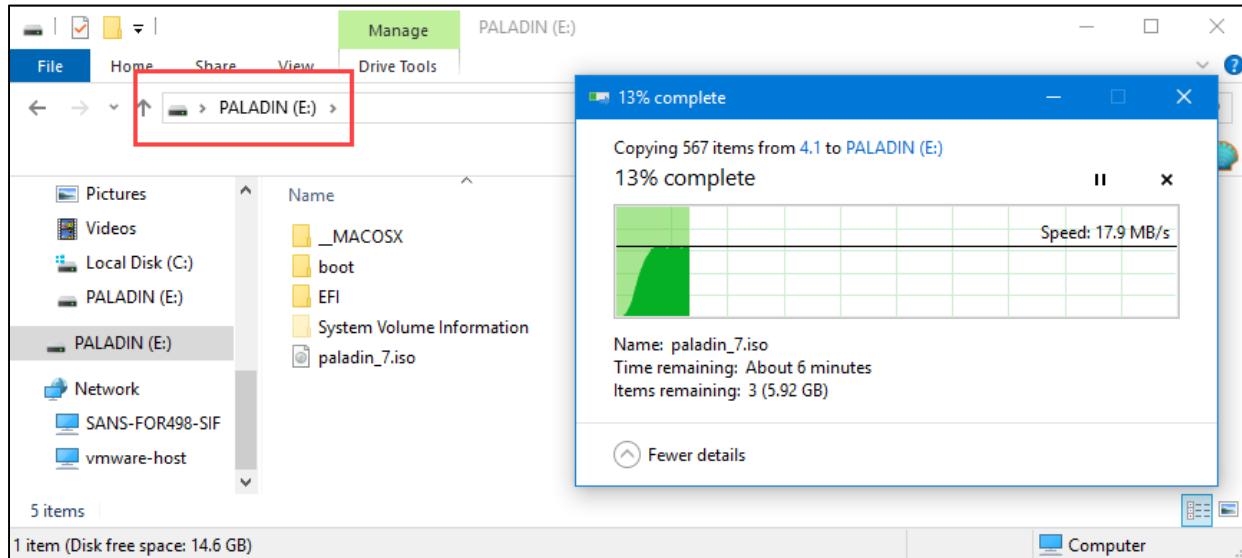
10. After a few seconds, the format will be complete. You will be back at the **Disk Management** window, and your new volume should be visible.



11. Close the Disk Management window. Open File Explorer and navigate to C:\Cases\Exercises\3.5



12. You should see 3 folders and 3 files in this directory. Select them all by clicking on **Ctrl+A**. You should see them all become highlighted. Now press **Ctrl+C** to copy them all. Navigate to your newly created **PALADIN** volume and click inside the window. Press **Ctrl+V**, and the contents you previously copied should start to appear. This will take between 5-10 minutes to complete.



13. Once done, close the window and power down your VM.

**Exercise – Part 2**

1. Have the student provided hard drive, and SANS provided USB drives ready.
2. For this part of the exercise, you will need 2 available USB ports on your host computer.
3. If you are using a Surface Pro, you **cannot** perform this exercise. The same applies if you are using an Apple product with a T2 Chip onboard. There are demos for these later in the course.
4. Power down your host machine fully. If you did not perform the steps to ensure this in the **Acquisition Practices** exercise, you may have problems.
5. Plug in the SANS provided 16 GB hard drive containing Paladin that you created, and also plug in the student provided external hard drive. It is assumed that the student provided hard drive is formatted with the NTFS file system. If not, stop and do this before proceeding, based on instructions provided in the **Acquisition Practices** exercise.
6. Because of the danger of accidental booting, extra measures must be taken. Collect the following information, and don't spend a great deal of time between steps of this process.
  - a. Record the current **Date/Time**:

---

- b. Record any relevant notes (outline what is being done):

---

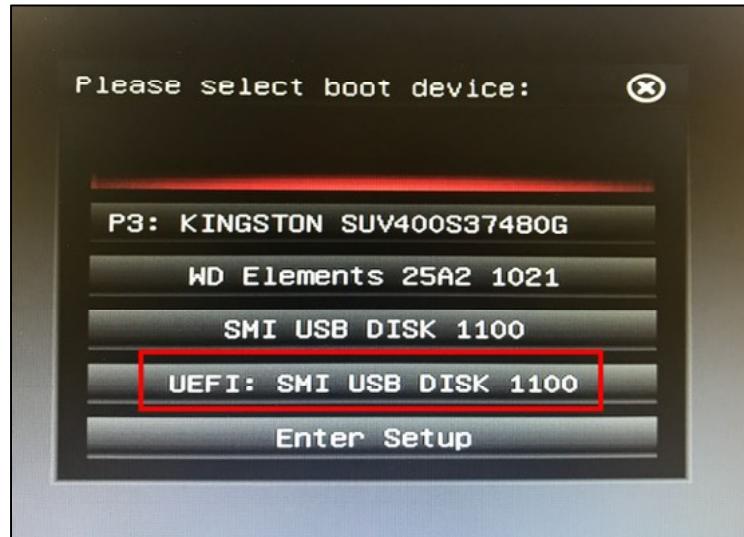
---

7. Back in the module and exercise regarding entering the computer's BIOS/UEFI, we discussed the methods of determining how to enter the BIOS/UEFI. You may recall from that exercise that your computer might have shown an entry mentioning a **Boot Menu**, along with a key to press to enter this **Boot Menu**. This would be the best of all worlds. Pressing the appropriate key to be given the **Boot Menu** will ensure that we can boot into the Paladin USB drive to perform the acquisition. It may very well be that you do not get an option for a **Boot Menu**. If you do not recall one, the best approach would be to enter the BIOS/UEFI and navigate through the menus looking for the boot order of the devices. In that menu, you will be able to choose what device order the computer starts in. Move your Paladin USB device to the top of the list and attempt a boot. There can be no question that this process is fraught with peril. It may take you a number of attempts to get it right, and each time, the computer will have booted. All you can do is clearly catalogue each happening in a detailed manner. This is why practice is so important, and is also why we remove the device hard drive first, if we can. It will not prepare you for every eventuality, but it will make you more comfortable with troubleshooting and expected possibilities.

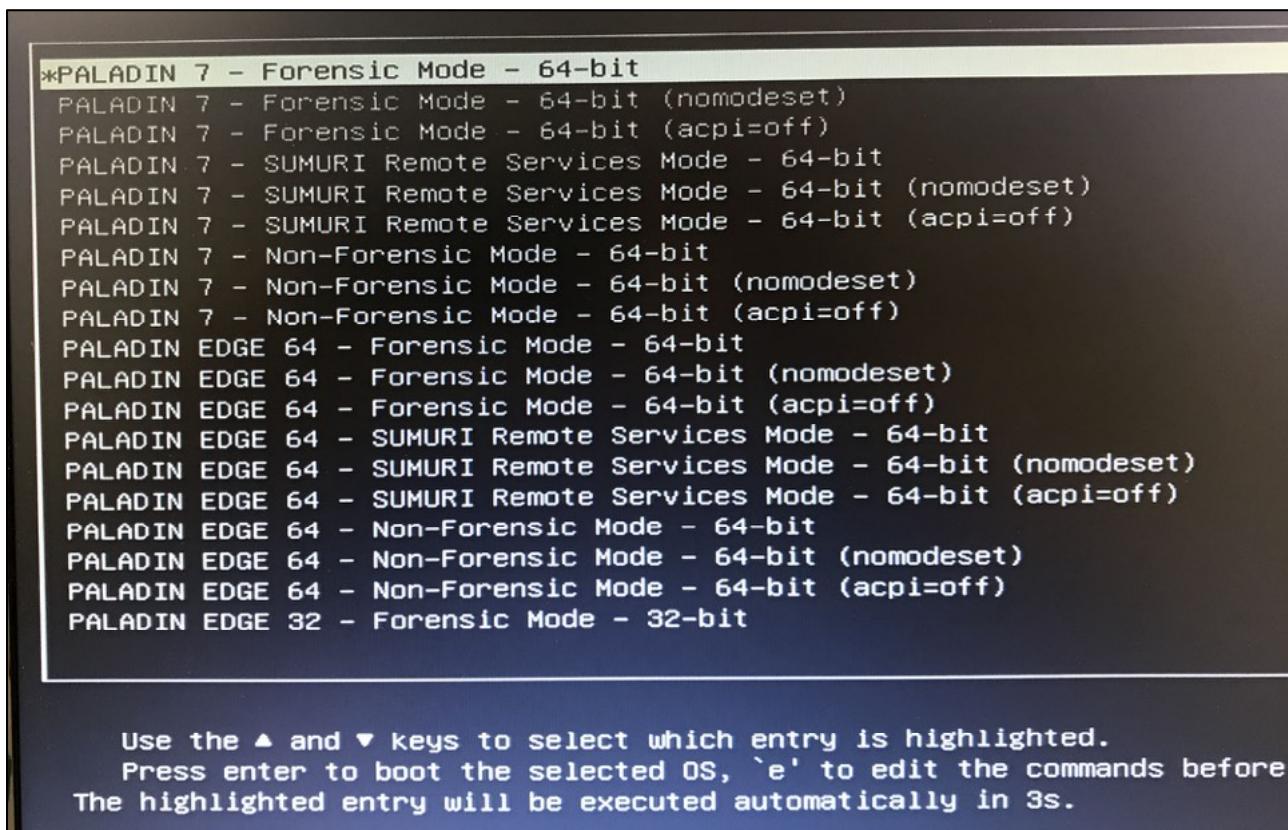
8. In the case of the example here, this computer showed the startup options.



9. It provided a **Boot Menu** after having pressed **F12**, and we selected the device that held the Paladin software. If you see an option for your drive, plus an option for your drive that is preceded by UEFI, select the one that is preceded by UEFI. If that doesn't work, then try the non UEFI version.



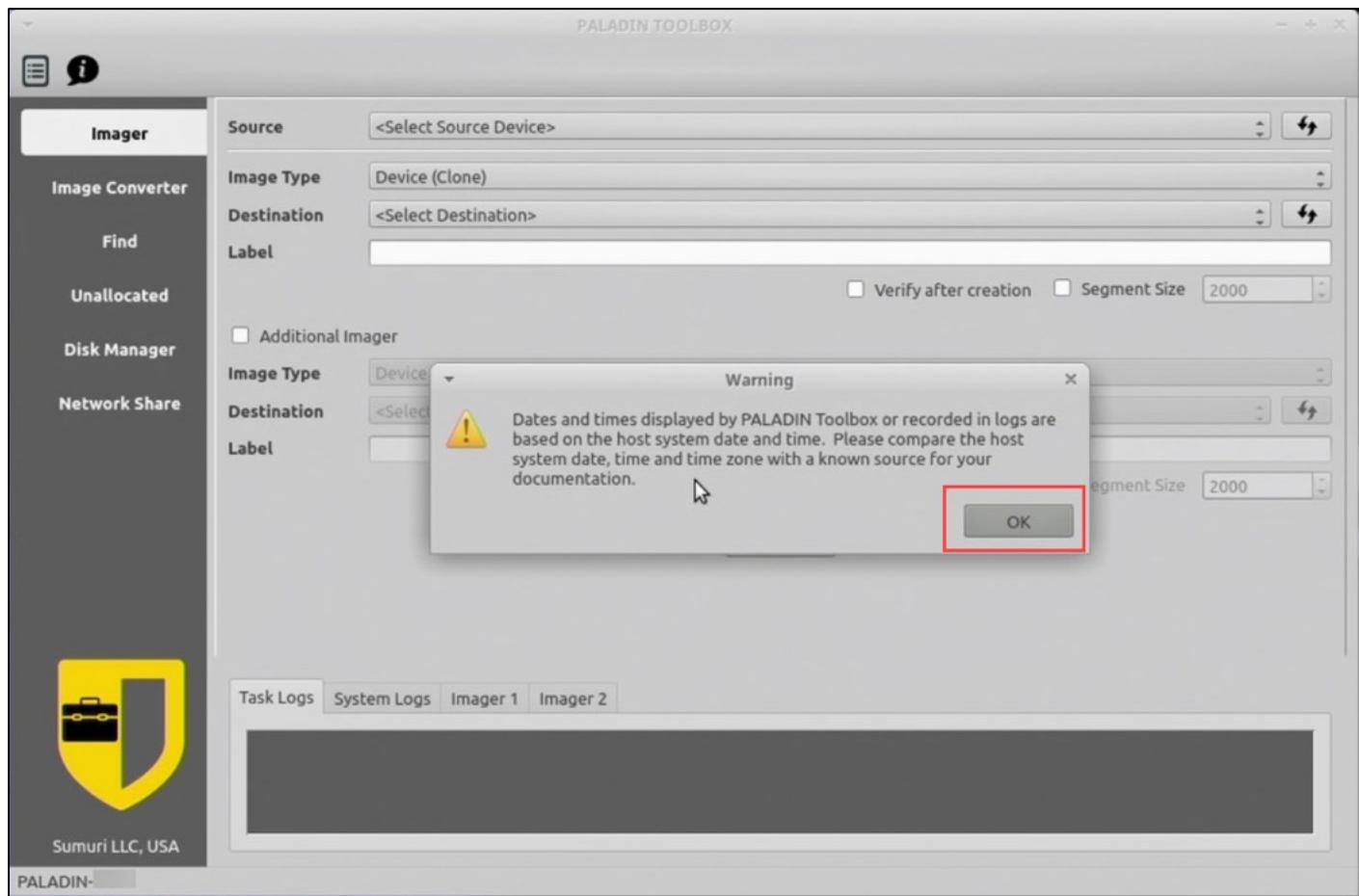
10. The **Paladin** boot menu screen shows. Allow the default setting to load. (If you get an error message regarding **Secure Boot**, you may need to enter your BIOS to disable it first).



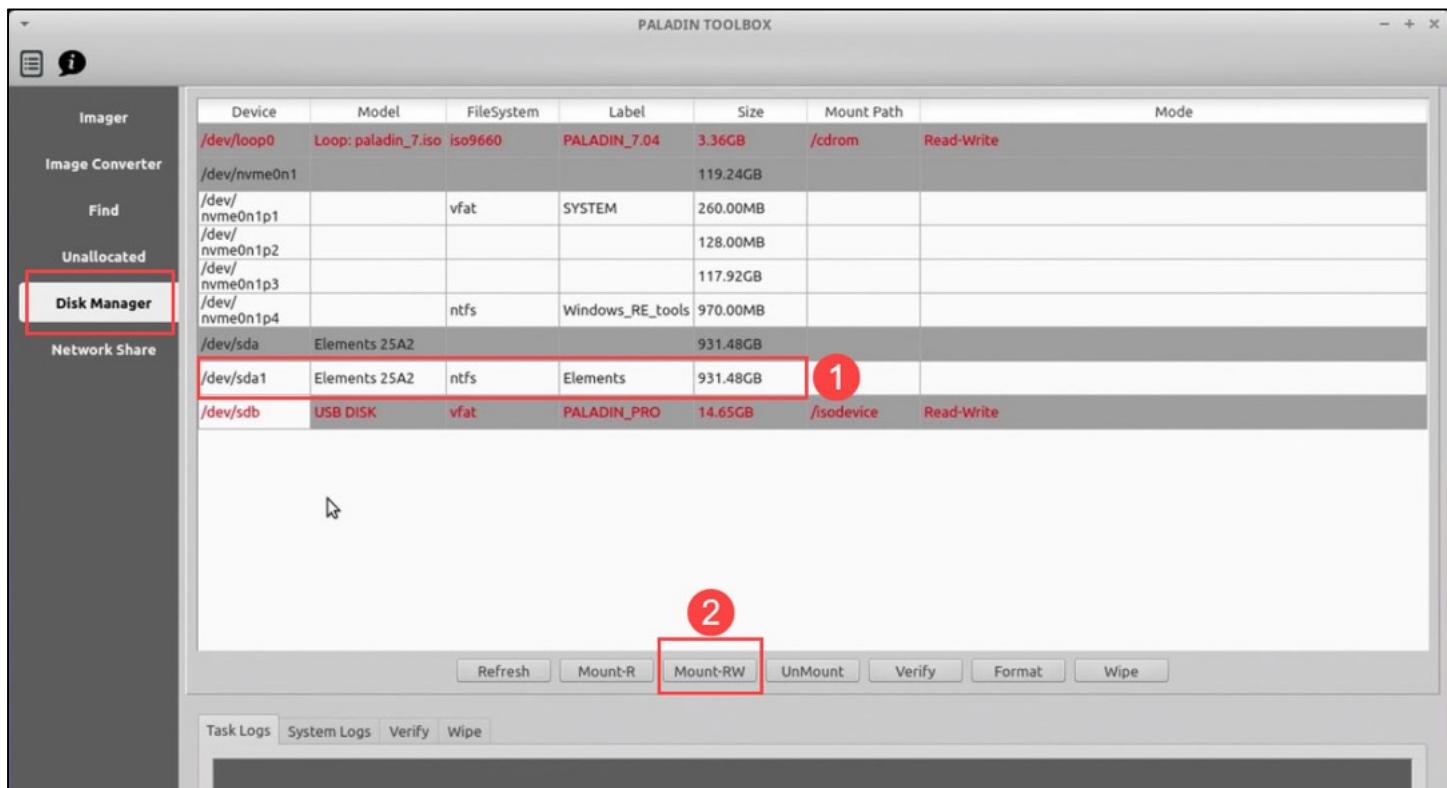
11. The computer now boots into the **Paladin** operating system and is ready for the acquisition process. Click on the **PALADIN TOOLBOX** at the bottom.



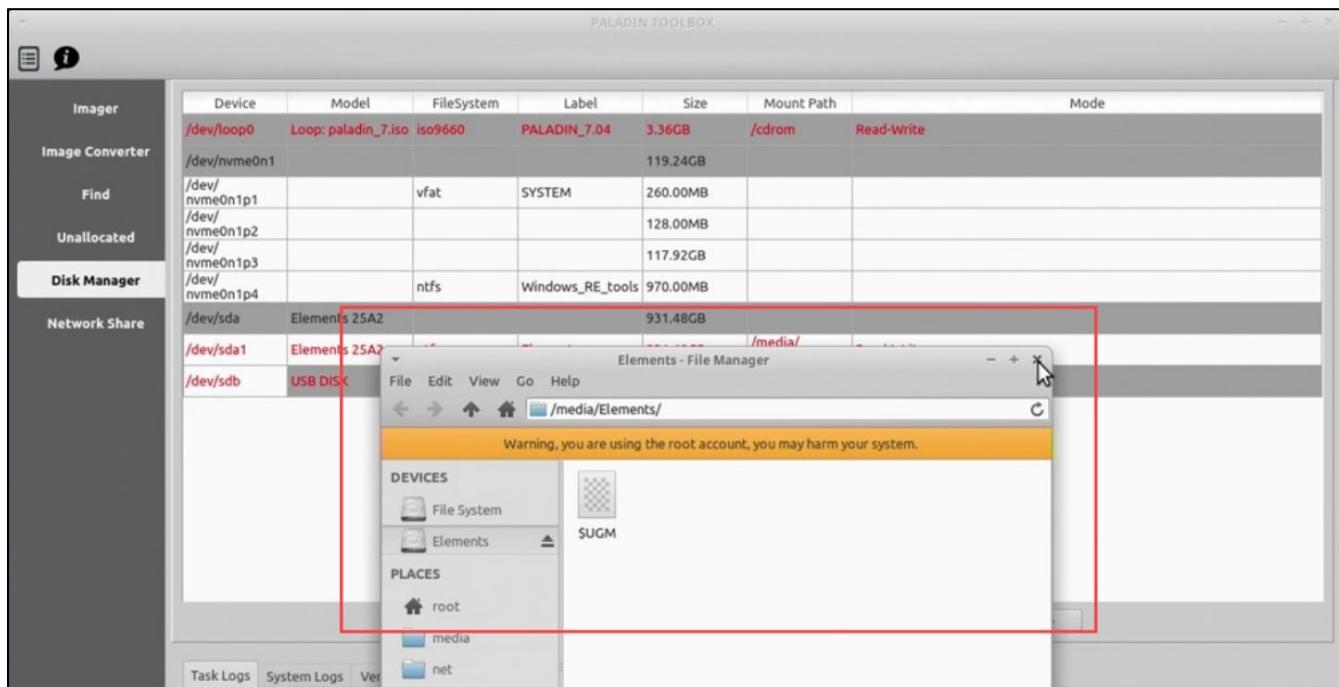
12. The PALADIN TOOLBOX will open. Read the warning and understand it and click OK.



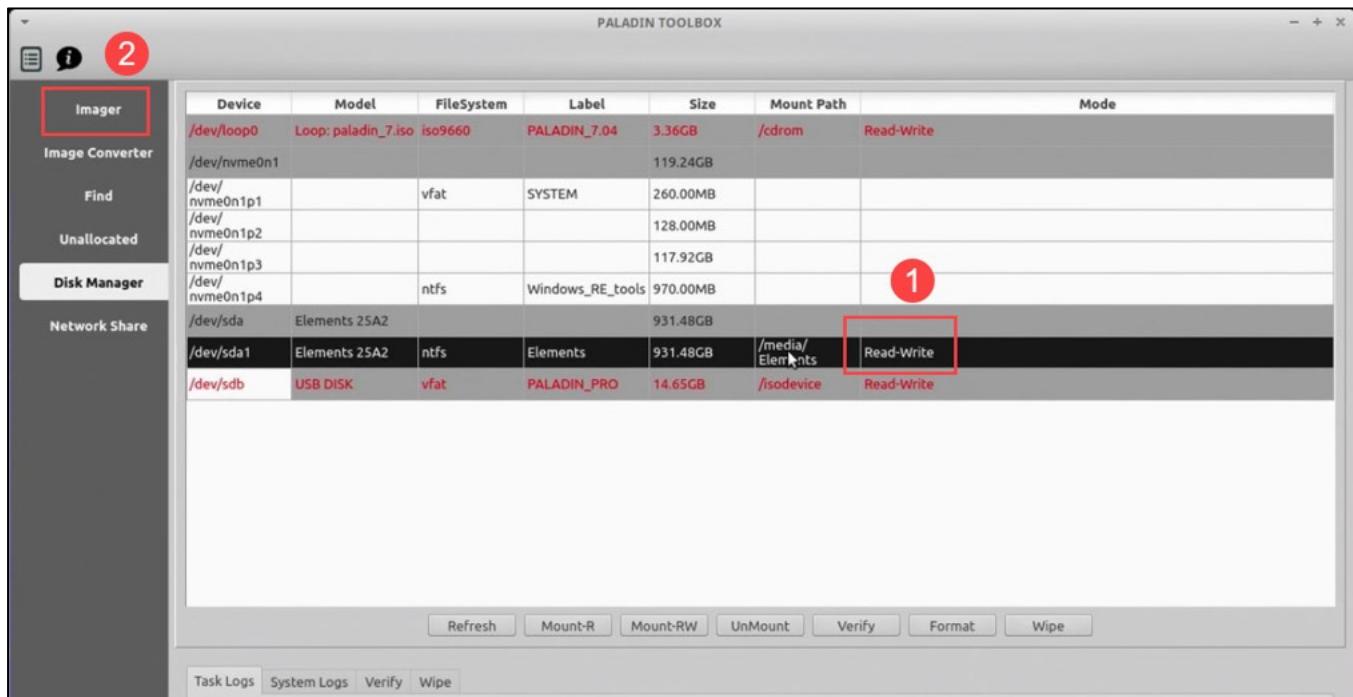
13. The different volumes and drives in the following slides almost certainly will not match the student computer. Before we can start setting up for the imaging process, we must prepare the destination hard drive. When **Paladin** boots, it does not access or mount any of the connected drives except itself. You must do this manually. Click on **Disk Manager**, highlight the **LOGICAL** partition and click **Mount-RW**. the logical partition will be represented by a device with a trailing number “**/dev/sda1**” and should have a filesystem represented in that column.



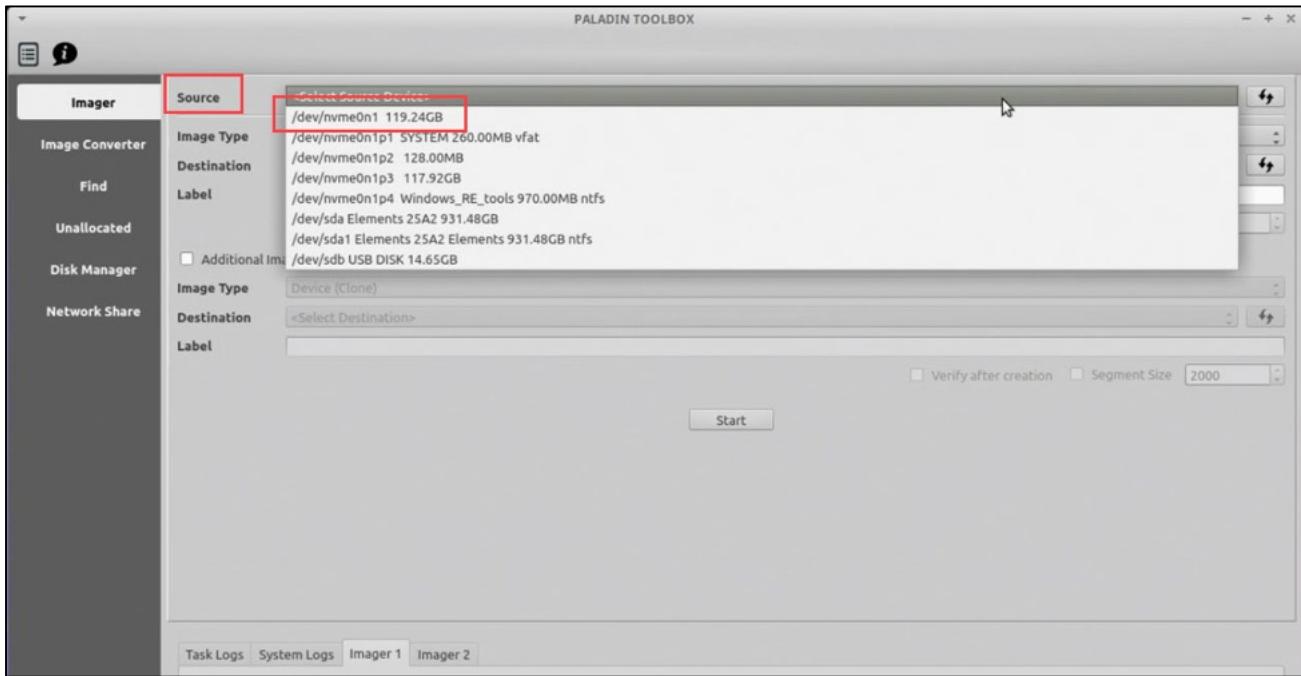
14. When the disk is mounted, it will open a window and show its contents. Simply close it.



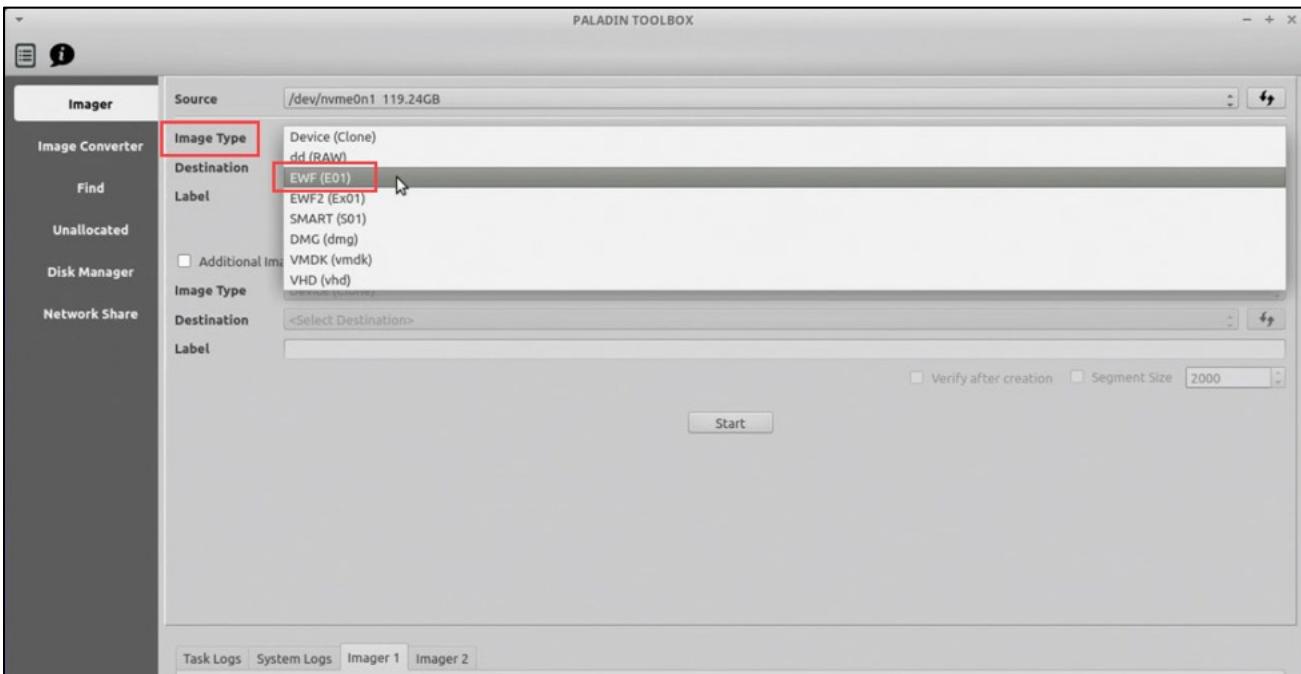
15. You will see that the logical partition of our destination drive is **Read-Write**. Click on the **Imager** tag on the left column.



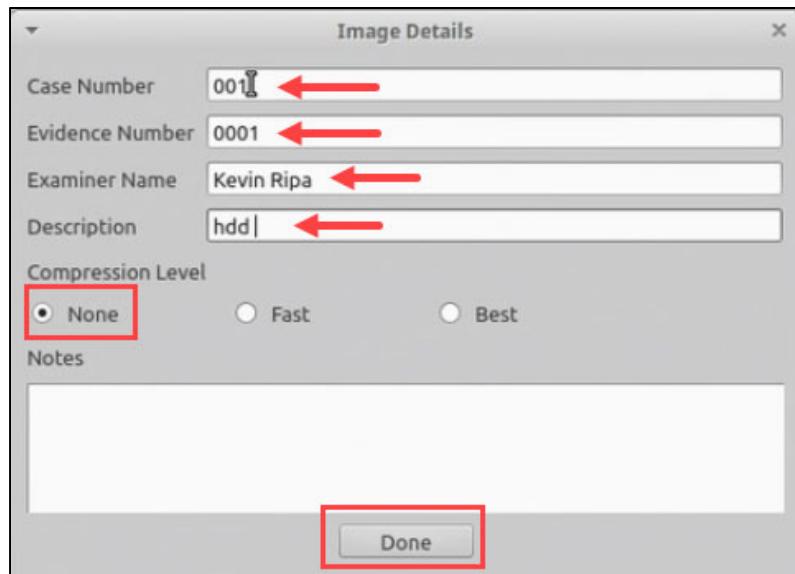
16. At the **Imager** screen, you will first select the **Source** device. In this case, you will be selecting the physical drive. This requires that you know the name or mount point of the drive you are imaging. In the screenshot, the drive that is being acquired does not have a drive name. It is an NVMe drive, and this is indicated. You then see 5 instances of it. Besides the first entry, you see p1 through p5. These are the logical partitions of the drive. Select the line without a partition designation. This is the physical drive.



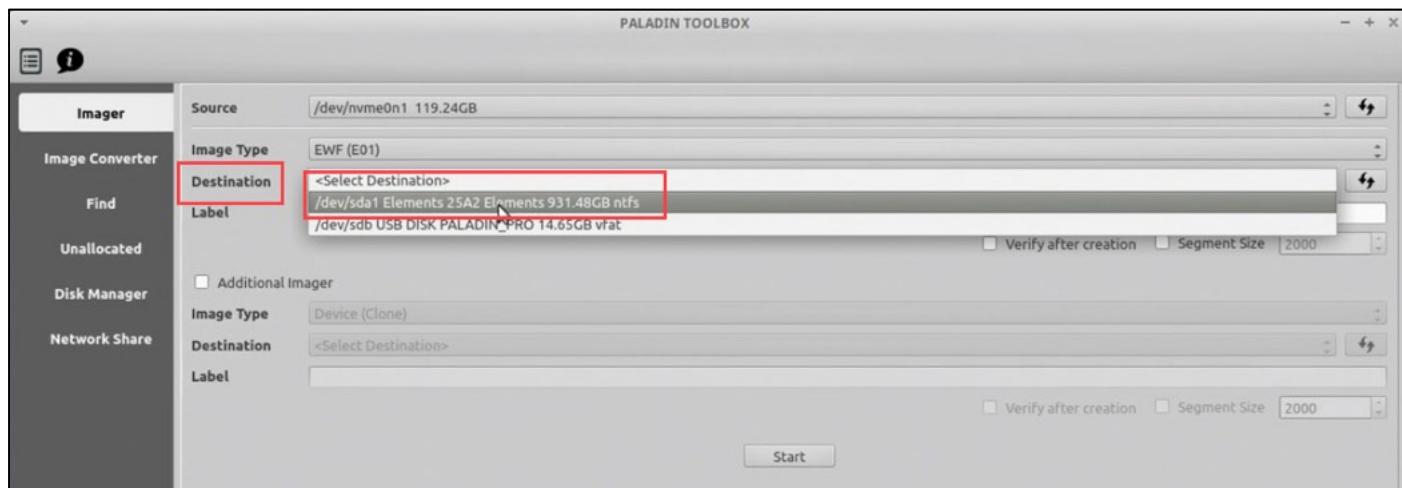
17. The next step is selecting the **Image Type**. Select the **EWF (E01)**.



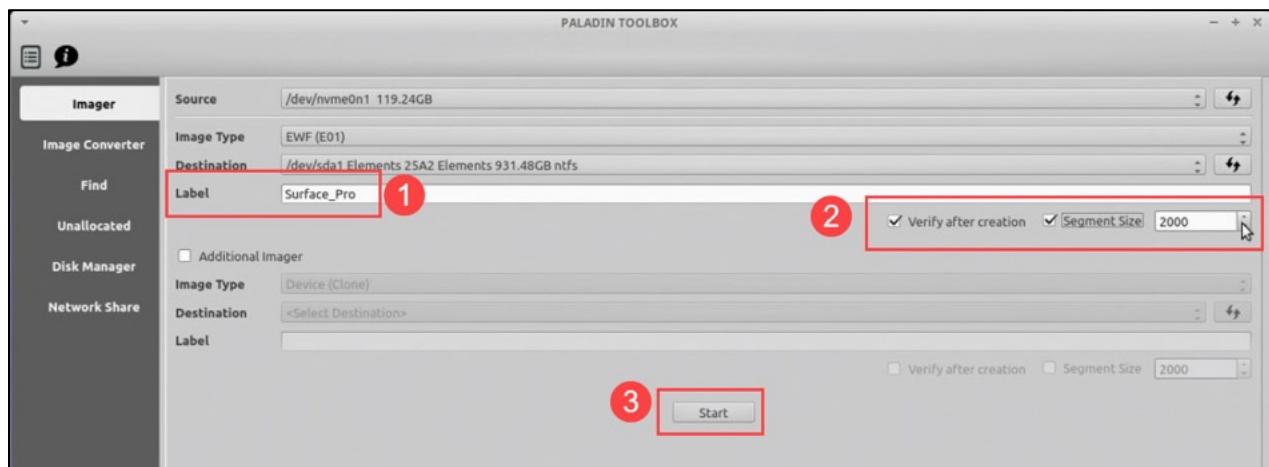
18. The moment you select the **Image Type**, an **Image Details** box will appear with several data fields. This **Image Details** box will be different based on the **Image Type** selected. (There can be times when Fast compression may be fine, and possibly faster). Fill in the fields based on the data below, and then click **Done**.



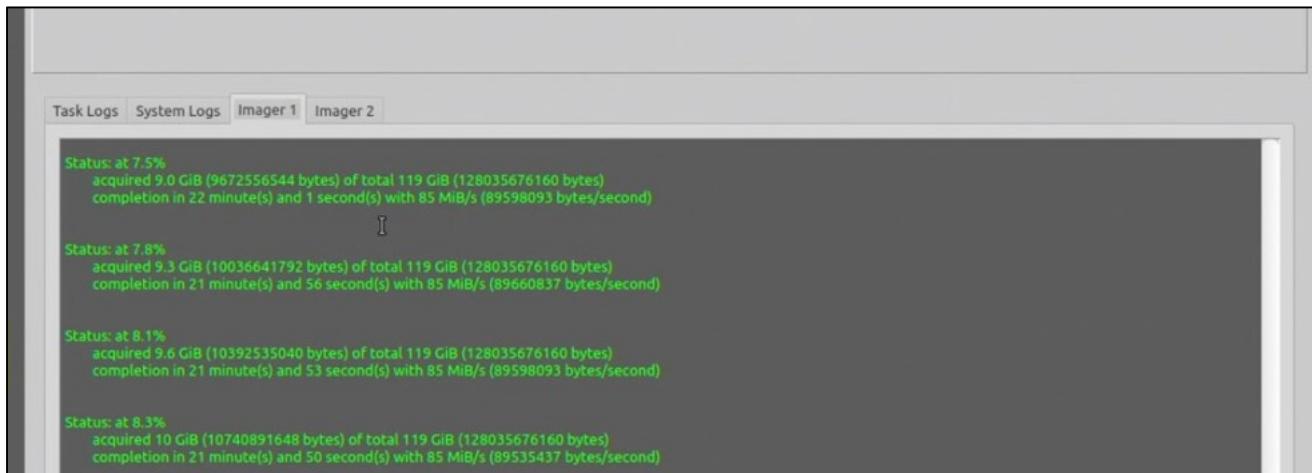
19. Designate the **Destination** drive by selecting it from the drop-down menu. Remember that the destination drive is the partition you just mounted as read/write.



20. Provide a name for the acquisition in the **Label** field. Check the box for **Verify after creation** and select **Segment Size of 2000**. Then click **Start**.

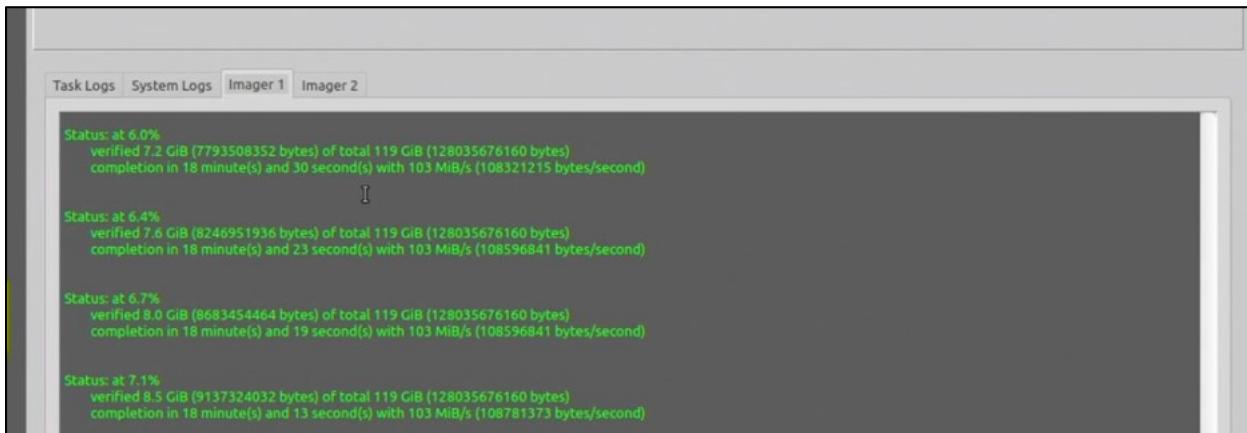


21. The acquisition will start, and you can monitor its progress.

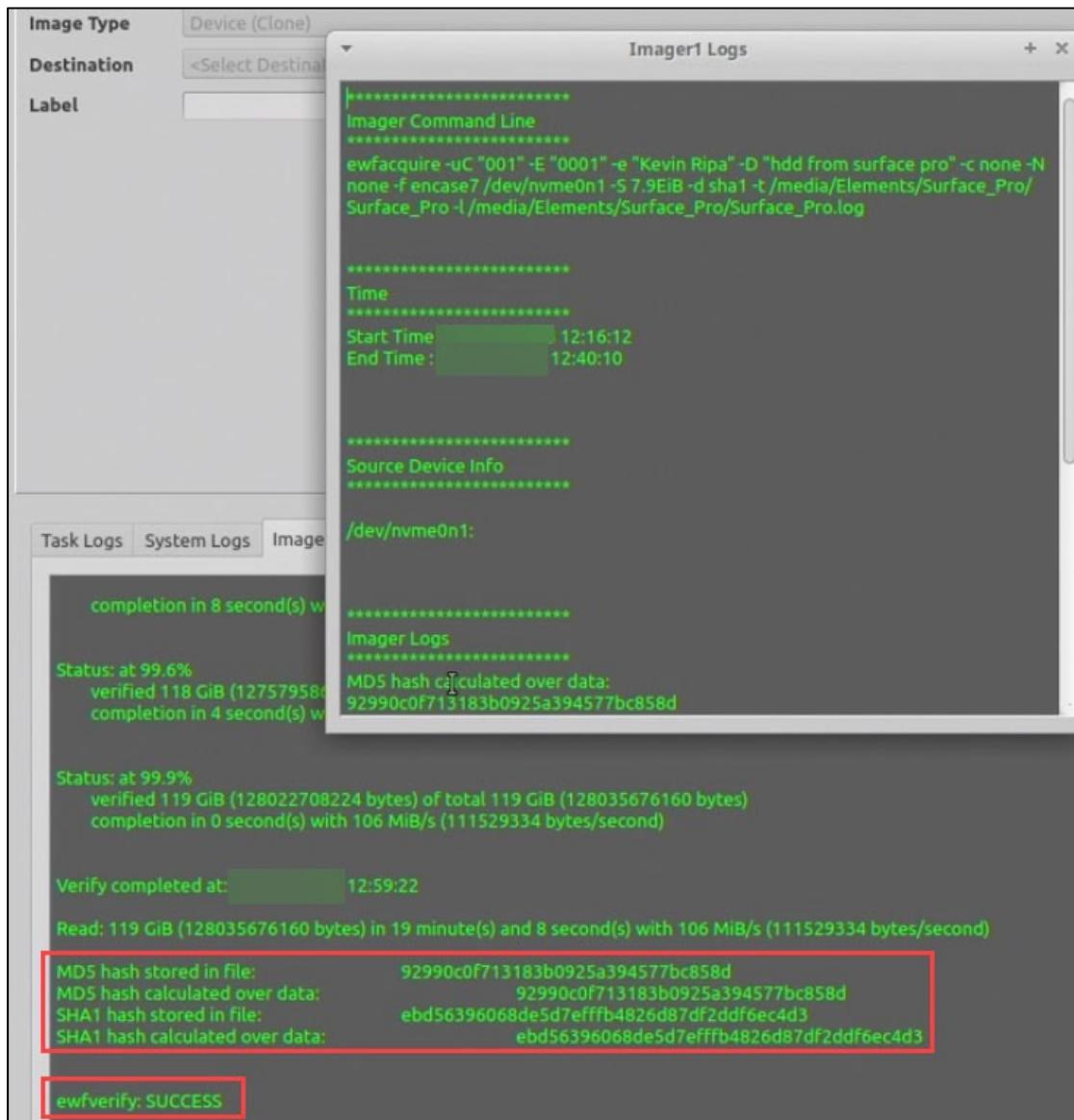


22. You can watch the process for a few minutes, but we will not be waiting for this process to finish, simply because of time. You can certainly re-run this exercise on your own time. Simply stop the process by clicking on the X on the right of the progress bar and accepting all the prompts. Log out of **PALADIN** and shut your computer off. You can remove all drives, and then restart your computer.

23. If you were to let the process run its course, you would see the acquisition end and the verification process start automatically.



24. Once complete, you will see a screen showing the full details of the acquisition and verification. This is also included in a file on the destination hard drive.



**Exercise—Key Takeaways**

- Using properly configured USB boot disks, an examiner can create a forensically sound acquisition of a device without any other manner of write blocker
- A Paladin boot disk is a great option for the purpose