Lab Setup Instructions

These setup instructions contain everything you'll need to get ready for your upcoming SANS class. These can take some time to complete, and may involve downloading large files. So please allow ample time to complete them before you arrive at class - especially if you have limited Internet bandwidth.

If you require assistance with the instructions contained within this document, please contact support@sans.org. Be sure to include the name of your course, and if possible, your order number.

We're looking forward to having you in class!

Lab 0: Getting Started (Complete Prior to Class)

Objectives

- Locate and download FOR508 course materials from the SANS portal
- Install and prepare your course VMs for digital forensic analysis

Before Class Begins

Several steps must be accomplished before you start class. For those students attending a live class event, this means completing the setup process before you leave. In particular, downloading the course data should be accomplished before traveling, and well before class begins for those taking it online. FOR508 requires significant data downloading and hotel/venue Internet bandwidth will not be suitable for these downloads.

Preparation Steps

These steps are covered in the following sections of this document:

1. **Downloading Course Materials**
    - ISO "A" should be your first priority for downloading. It contains the two virtual machines critical for completion of the course labs.
    - ISO "B" and ISO "C" will be used later in the course. However, they are large files so it is highly recommended you start downloading them as soon as possible.
2. **Mounting Course ISOs**
3. **Decompressing and Booting Virtual Machines**
    - There are two virtual machines used in FOR508. The **508 Windows VM** will be used initially and most extensively throughout the class. Setting up this VM is the priority. The **508 SIFT Linux VM** will be used after the first day of class.
    - Ensure you can load and login to virtual machines prior to the beginning of class. The upcoming sub-sections *Specific Notes About the FOR508 Windows VM* and *Specific Notes About the 508 SIFT Linux VM* should be reviewed once you are able to log into each VM.
4. **Return here and continue through this Lab0 document.**

Important information about this setup guide

The first 3 sections listed above are purposely template content designed to be consistent across all SANS courses. As such, you will see screenshots that differ slightly from the FOR508 files. However, the file naming conventions and setup processes are the same by design.

The parts of this overall setup guide that are unique and specific to FOR508 are this initial section, titled ***Lab 0: Getting Started (Complete Prior to Class)***, and a short section titled ***Virtual Machine Credentials*** following the ***Decompressing and Booting Virtual Machines*** section. Please pay particular attention to these sections for guidance specific to FOR508.

Following the ***Virtual Machine Credentials*** section are a collection of resources to help troubleshoot the setup. They are primarily focused on VMware issues.

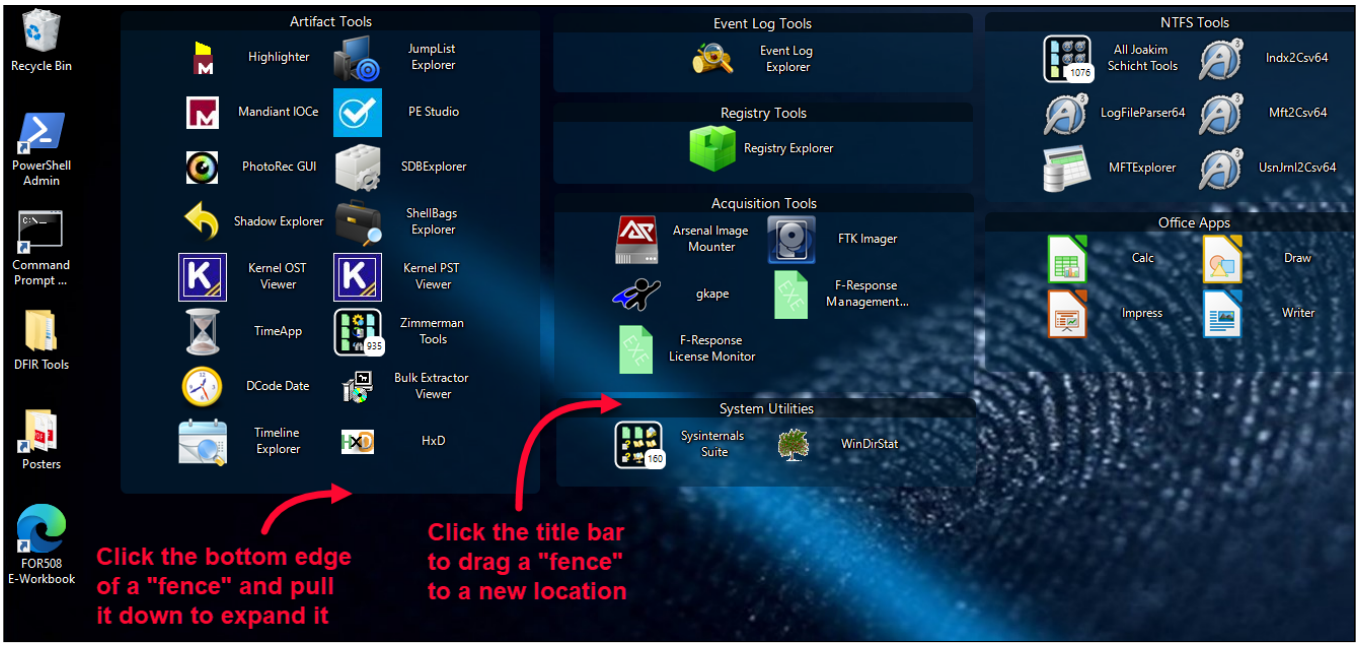
Time Zones and Operating System Upgrades

- It is critical that you **do not upgrade software** within the virtual machine unless specifically directed to do so in the lab instructions. Your virtual machine has been extensively tested in the configuration which it was distributed. SANS cannot ensure your labs will function properly if the software is updated.
- **Do not change your regional or time settings inside your VMs.** Your VMs' system time zones are set to UTC. The labs are written specifically for UTC time to avoid any confusion from region to region where we are teaching the course.
    - If you need a different keyboard language layout, we will show you how to change it in the FOR508 VM subsections below.

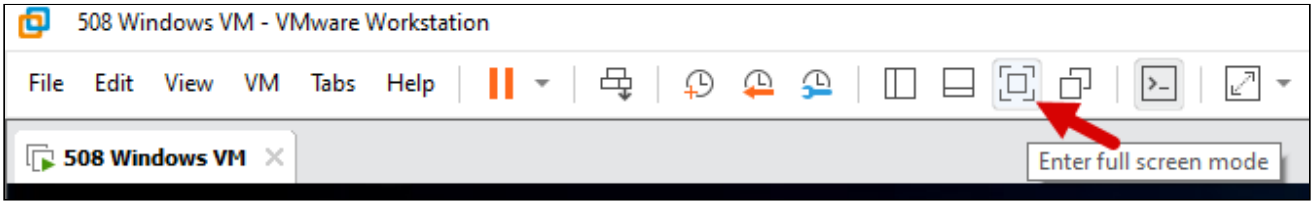
Specific Notes About the FOR508 Windows VM

Once you've completed the steps to install and login to the Windows VM (username `sansdfir`, password `forensics`), please come back to review these specific notes about the FOR508 Windows VM.

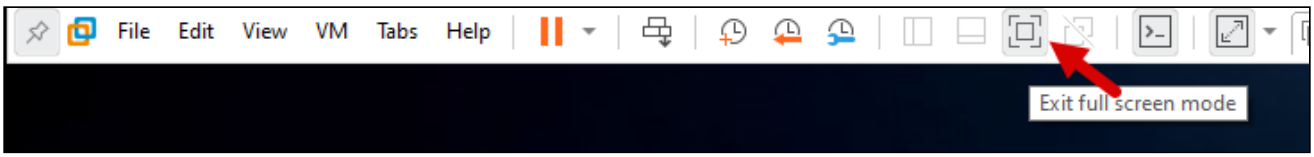
1. Upon first starting up the Windows VM, you may see a pop-up dialog box from VMware that says "Setup needs to reboot the system in order to complete the install. Do you want to reboot now?" Click "Yes" to reboot the VM (not the host) so that VMware Tools can finalize setup. This may be necessary to update the display drivers inside the VM.
2. Windows might pop up a Network dialog asking whether you want your VM to be discoverable by other devices on the network. Your choice does not matter for this class, although the suggested answer is Yes.
3. You should see the following on your desktop. If the "fences" do not look like this, you might need to adjust them. Your screen resolution determines how the fences initially arrange. Drag and expand the fences to best accommodate your VM's resolution.



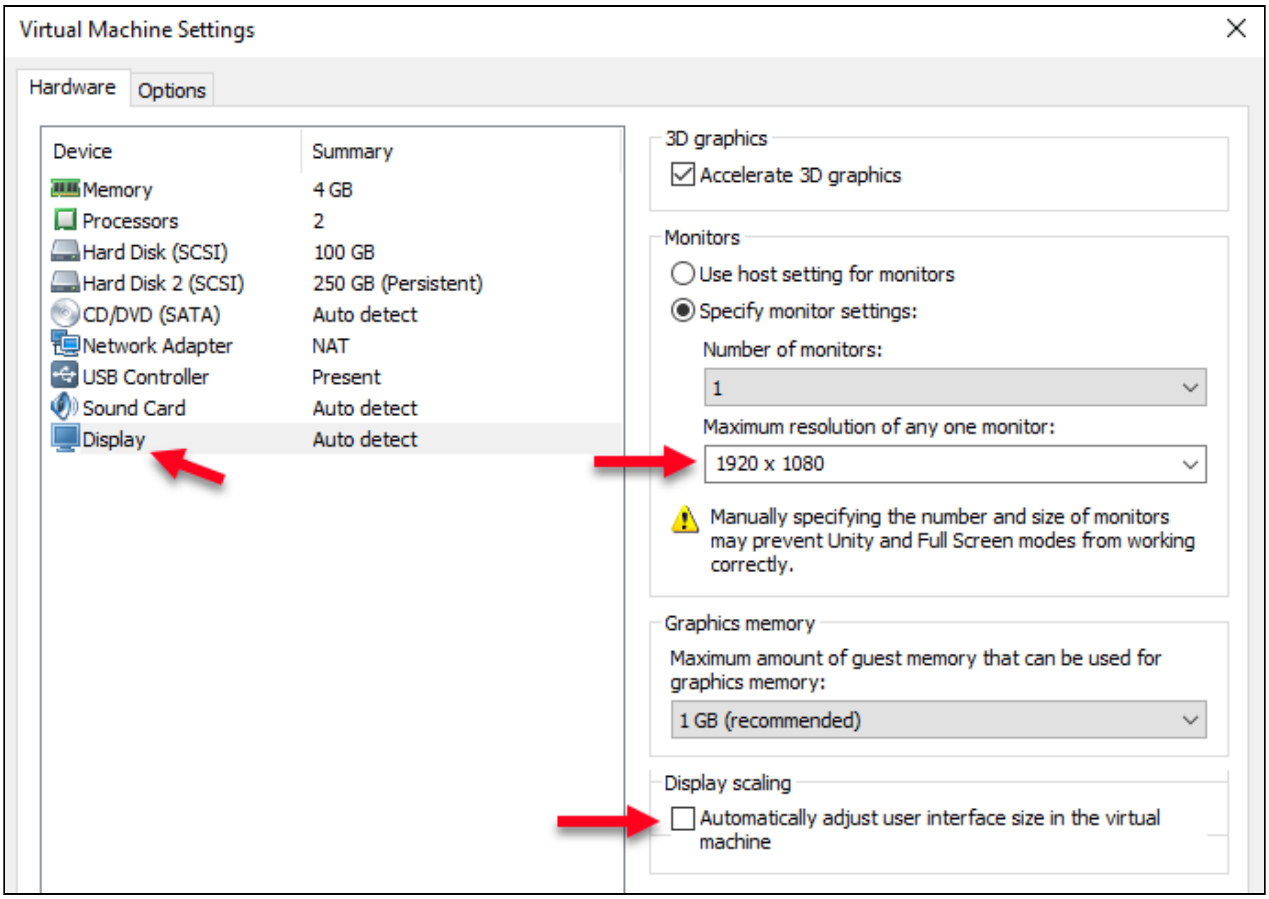
- You will typically have the best experience in full-screen mode in VMware. For VMware Workstation, the icon to **Enter Full Screen Mode** looks like the following:



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**:



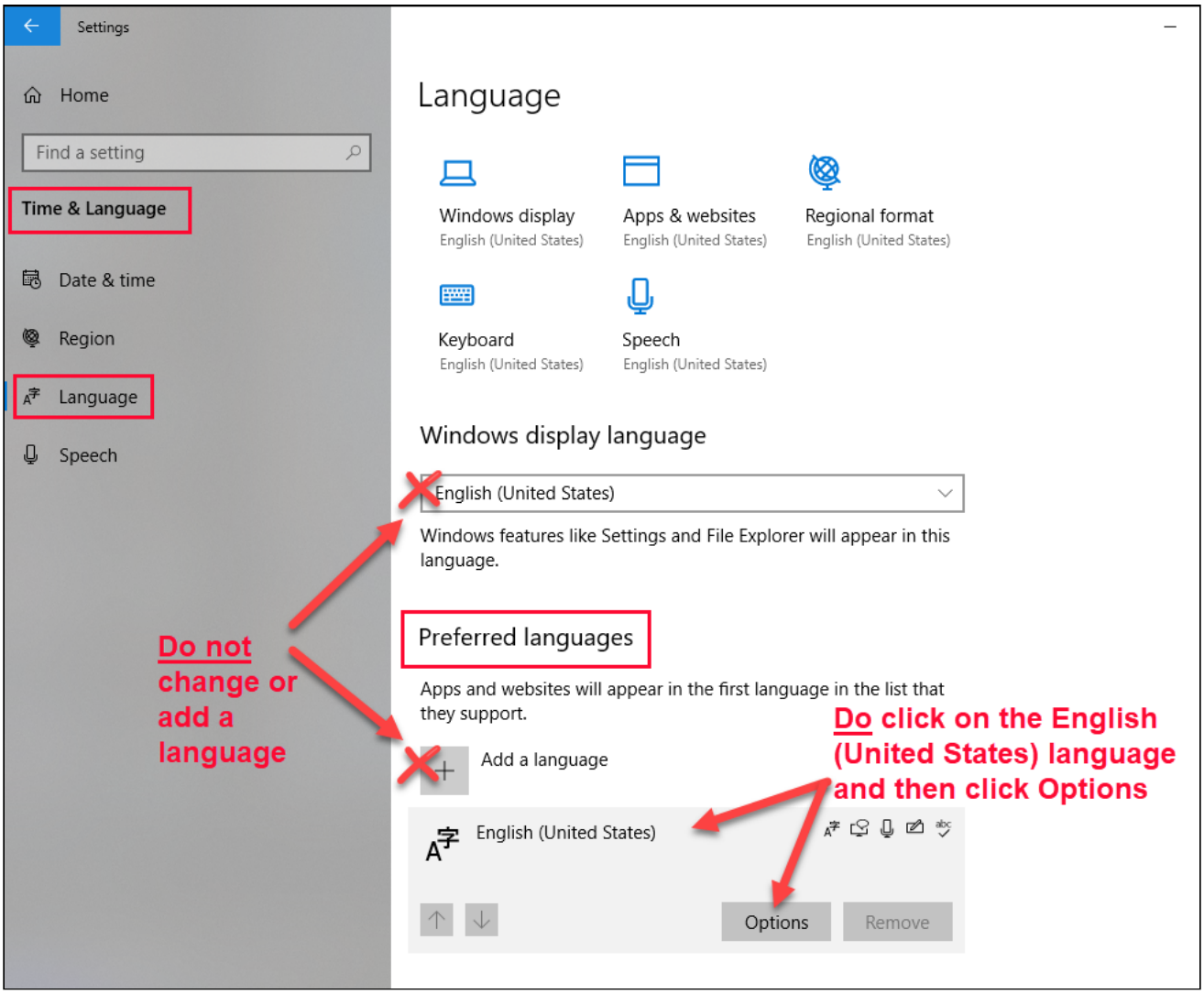
- If you are still experiencing scaling/display issues, try the following:
  - Shut down the VM (inside the VM, click the Windows **Start** menu > **Power** button > **Shut down**). Then go to **Settings** in VMware, click on **Display** and uncheck "Automatically adjust user interface size in the virtual machine". Please change the "Monitors" setting from "Use host setting for monitors" to "Specify monitor settings:" then manually set the "Maximum resolution of any one monitor" to 1920 x 1080, or test other values to find what works best.



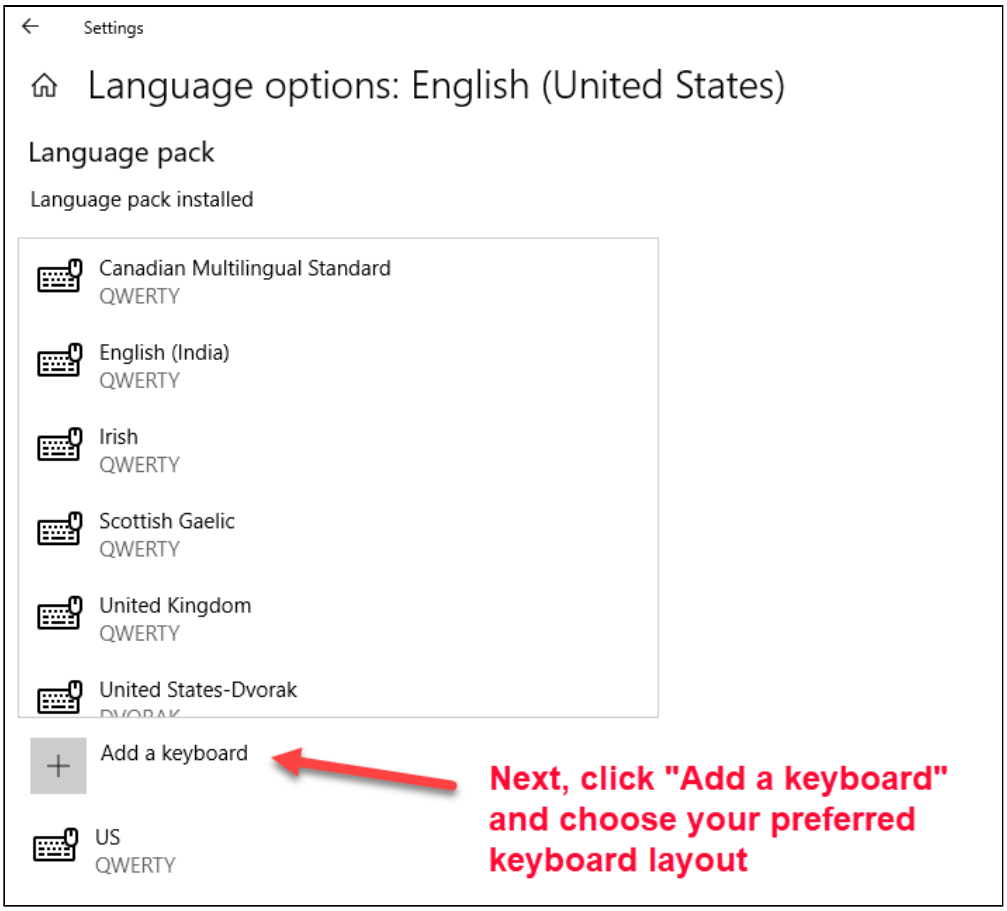
4. **Do not change regional or time settings.** The system is setup to output in ISO 8601 format (`YYYY-MM-DD HH:MM:SS`). Changing the regional and time settings will affect this and **likely break some tools we rely upon in class**.

   However, if you need to change your keyboard layout to a non-US keyboard, please adjust it as follows:

   - Select the **Start** menu > **Settings**. From the Settings dialog box, choose **Time & Language**. Then choose **Language**. Under "Preferred languages", click **Options**:



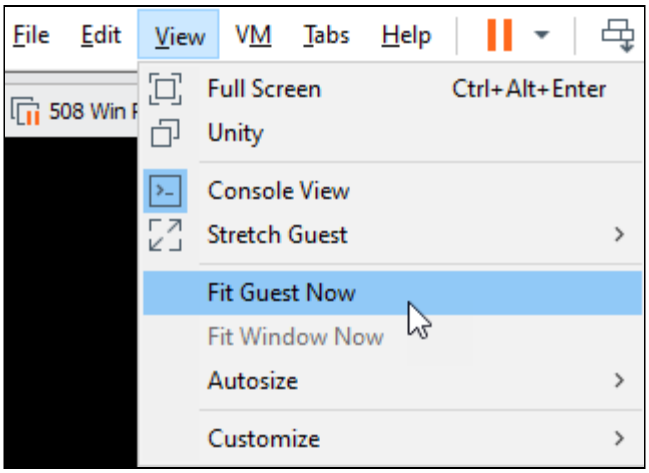
• From the "Language options: English (United States)" dialog box that appears, choose **Add a keyboard**:



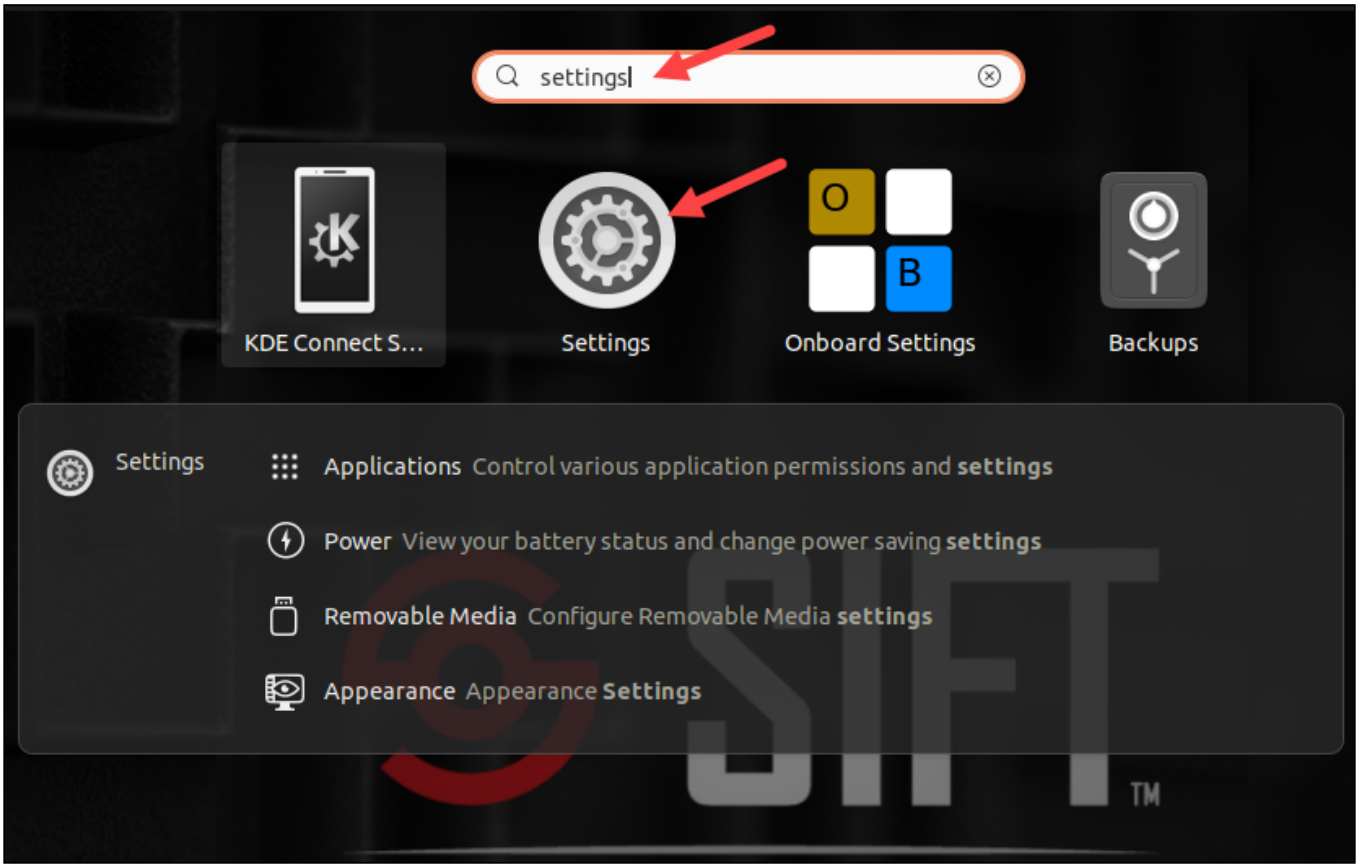
Specific Notes About the FOR508 SIFT Linux VM

Once you've completed the steps to install and login to the Linux SIFT VM (username `sansforensics`, password `forensics`), please come back to review these specific notes about the FOR508 SIFT Linux VM.

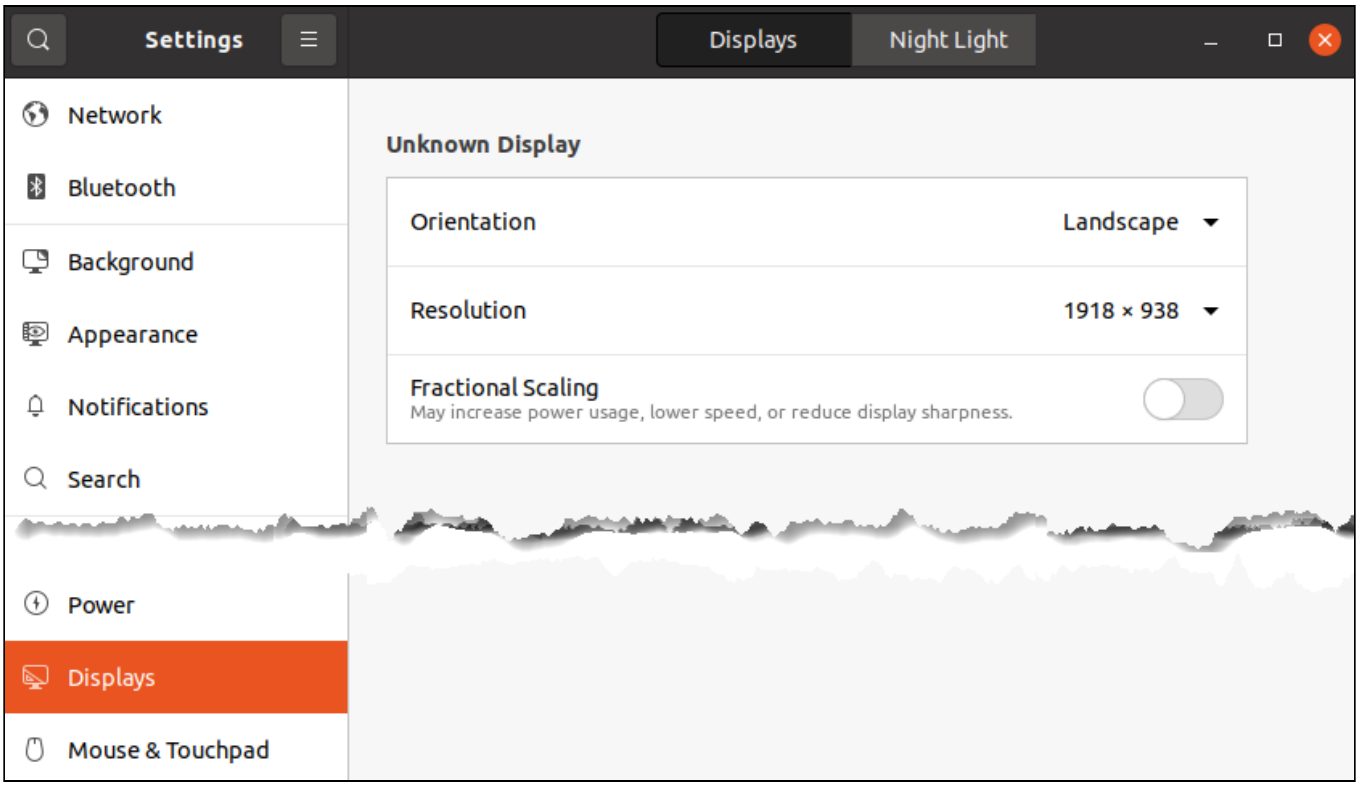
1. Your VM may need display adjustments. Here are a couple of options:
    - One of the first things to try is fitting the VM display to the VMware window. In VMware Workstation, go to View > Fit Guest Now.



• Another issue is high-resolution screens may need scaling adjustments. If so, click the bottom left grid button on the Activities bar (or press the Windows key / Mac Command key). Then type "settings" into the search field and choose the Settings app:



• Select Displays. Adjust size for best fit. The Fractional Scaling may also help with higher resolution displays.



2. If your host system has a non-US keyboard layout, you will probably want to adjust the SIFT VM's keys to match your system. Use the `setxkbmap` command to adjust it with the proper code. For example, to switch to a German layout, run the following in a Terminal window:

```
setxkbmap de
```

   - To get a *very* comprehensive list of language codes, run `man xkeyboard-config`.

Opening and Updating the Electronic Workbook

The FOR508 workbook content is stored locally in the FOR508 VMs so it's always available. Open a browser in the virtual machines and the homepage will default to the workbook.

Course authors occasionally update the source content with minor fixes, such as correcting typos or clarifying explanations. You should update the workbook in each VM at the start of class. You can pull down any available updates by running the following command in a Bash shell in the VMs:

Command lines

```
workbook-update
```

Expected results (when updates are available)

```
- Updating workbook files

Complete!
```

Expected results (when no updates are available)

```
- No workbook updates available

Complete!
```

Downloading Course Materials

Use these directions to download all of the digital file(s) that you will need for your SANS course. These downloads can be very large and must be completed before you start class. If you are attending a live course event, the site venue's Internet connection will likely be insufficient for you to download all of the necessary course materials.

Important notes

- **All downloads should be completed before the first day of class or beginning travel**. File sizes may be 1GB to 100GB or more. Downloading all course materials may require as much as an hour of keyboard time, plus a varying amount of download time based on your connection speed.
- Course books are protected with a password that must be entered each time a protected PDF file is opened. We suggest you keep this password in a password manager.
- By downloading these files and saving the SANS-provided course book password, you will have ongoing access to your course materials. The expiration date shown on the SANS site refers to the date when you can no longer download materials from your SANS account.
- Due to copyright protections, notations have been disabled from the course book PDFs. In lieu of highlighting we encourage taking notes on a separate document and including page numbers so you can reference at a later date.

Notice

Content and screenshots in this section are examples and do not reflect your specific course ID and name.

Preparation Before Class

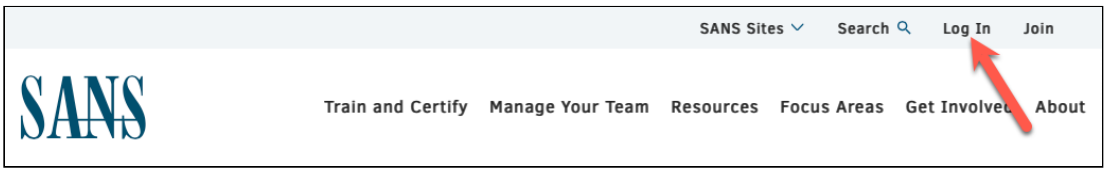
Before proceeding to the downloads themselves, please take a moment to review a few short videos that include important information and will help you to get the most out of the lab portions of your SANS course.

- What to complete prior to class
- Laptop system requirements

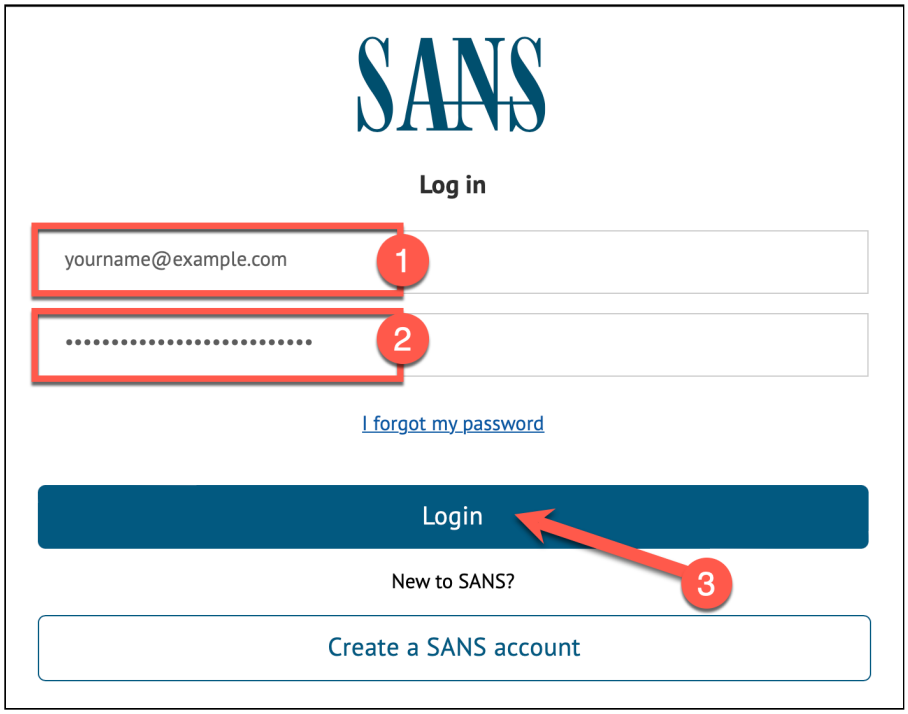
Download Instructions

We've also provided a video that demonstrates the process of downloading your class materials.

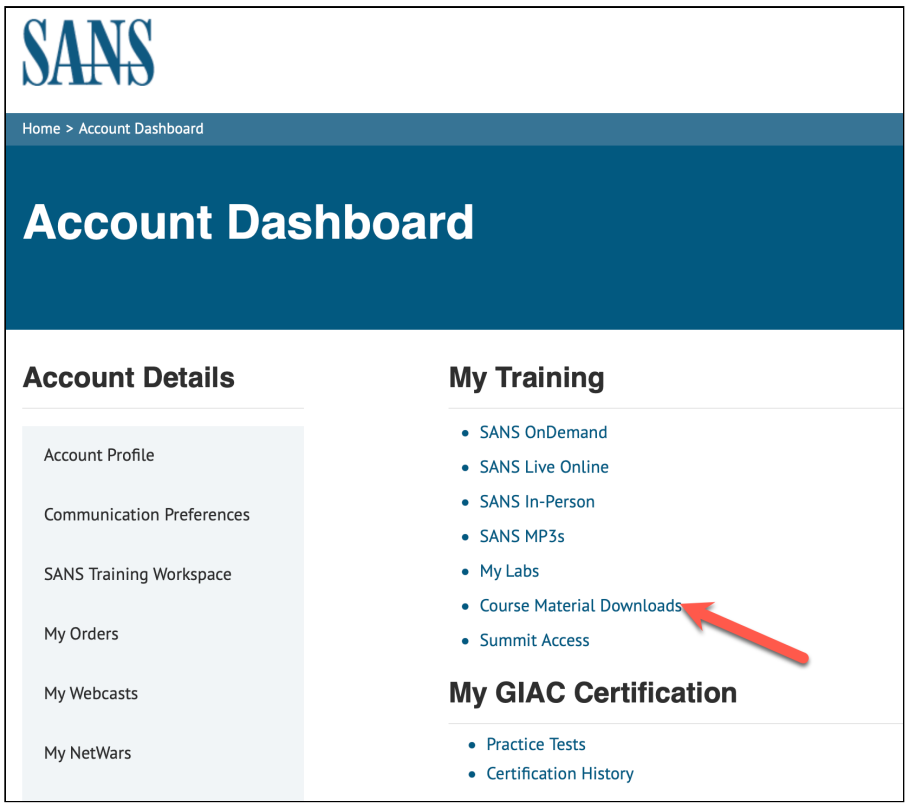
1. Visit sans.org and click "Log In" at the top of the page.



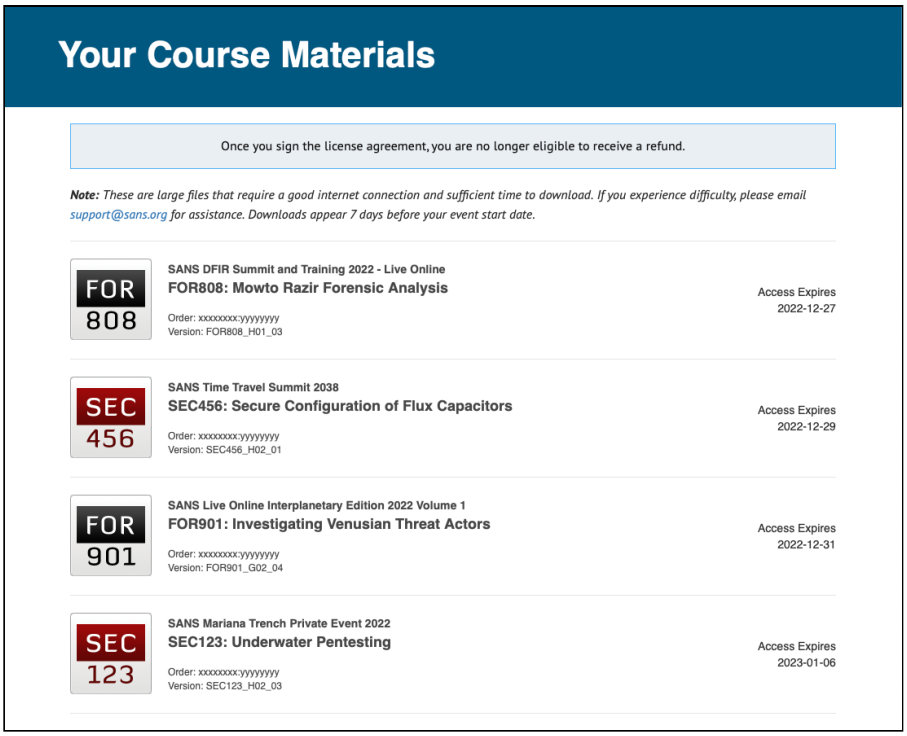
2. Enter the email address that you used to register for your course and your password, then click "Login".



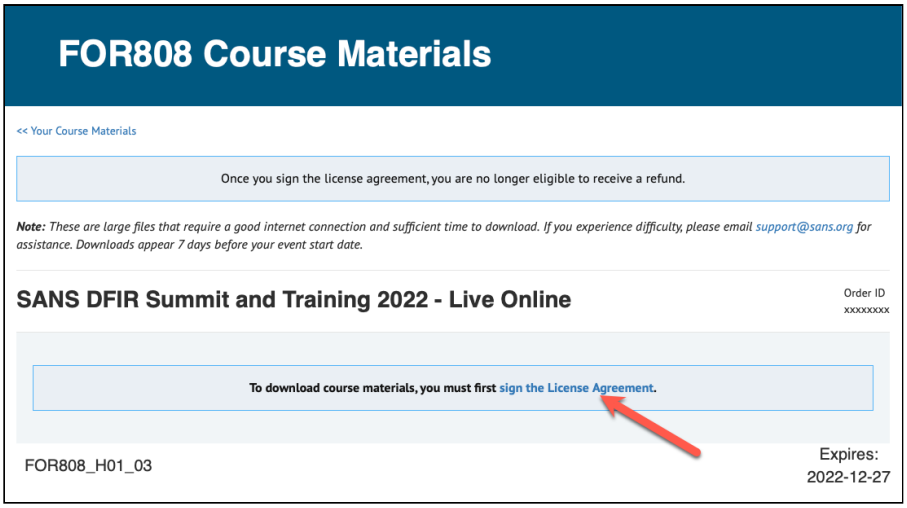
3. Click "Course Material Downloads"



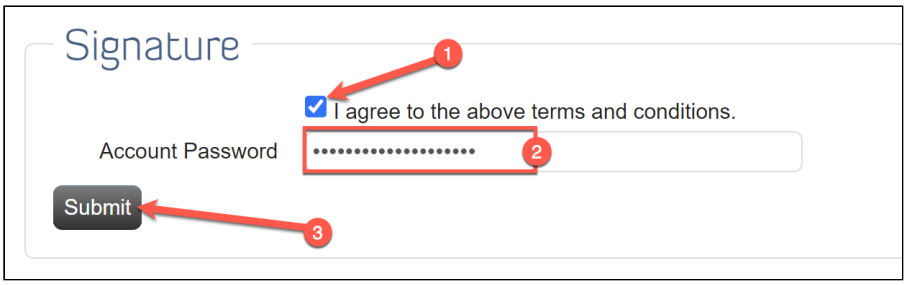
You may have a list of multiple courses. If so, select the course that you are downloading the materials for.



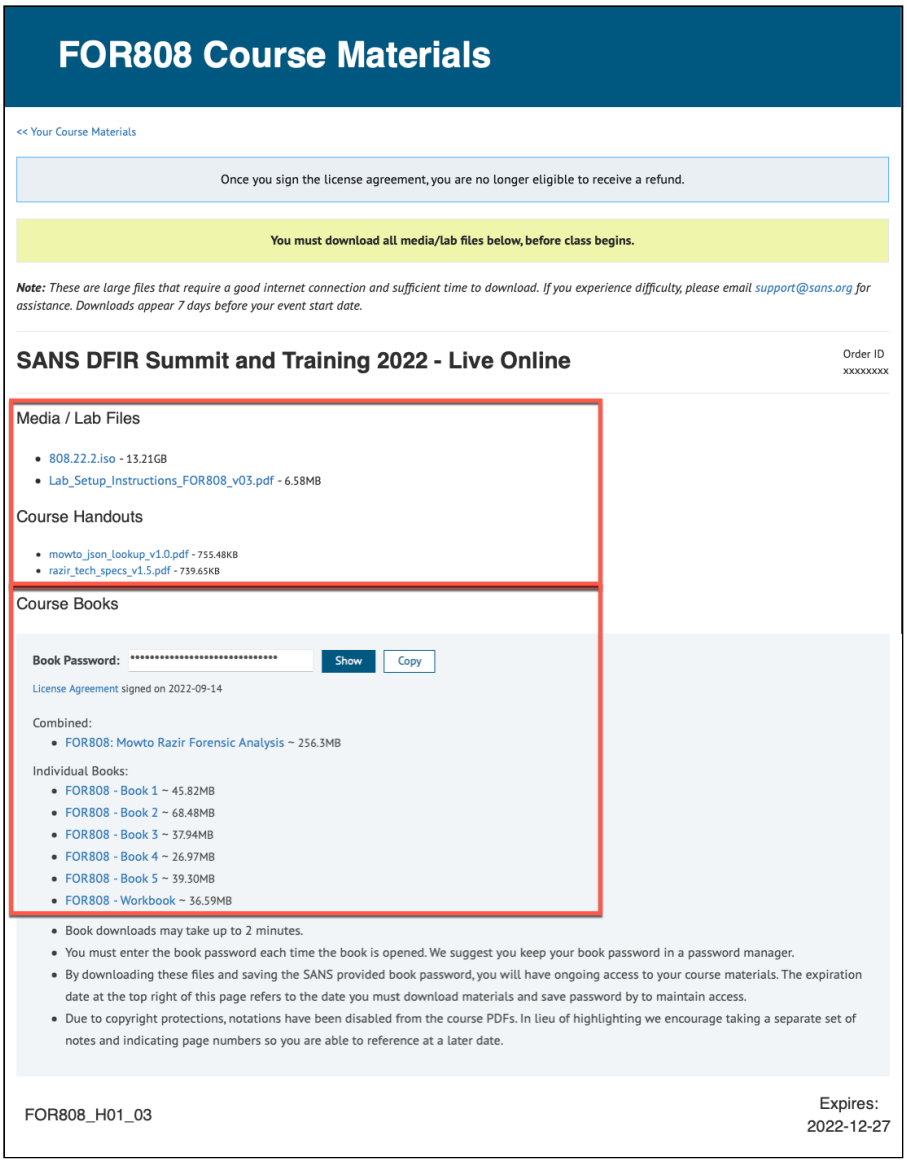
4. To access the course materials, you must sign the License Agreement. To do so, please click on the link.



5. Read the agreement, then scroll to the bottom and check the box to agree and re-enter your SANS Account password. Click on Submit when complete.



6. The following screen will differ, depending on the course you are taking. There may be several sections, potentially including the following. Not all courses have all sections.
    a. Media / Lab Files
        i. This section may have subsections labeled "Priority - Required for Day 1" and "Additional Required Files"
    b. Course Handouts
    c. Course Books



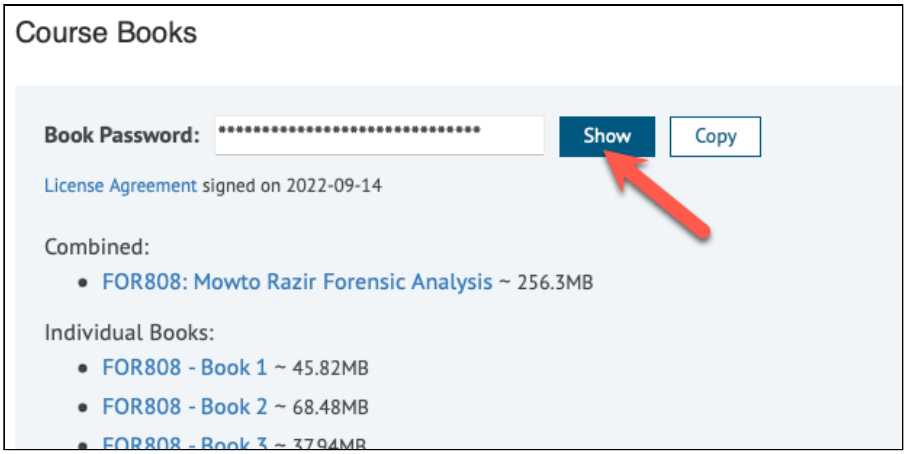
7. Download **all** files provided for your class! These may be between 1GB to over 100GB, so plan your time accordingly. We recommend placing these into a single subdirectory on your system, where all files related to your course can be held together. This also makes it easier for you to find them. Be sure these are backed up, so the files are safe from accidental deletion or corruption.

    If your course downloads include a "Priority - Required for Day 1" section, the files listed here should be downloaded first. Some or all of these files may be "ISO" files. ISO files are archives containing numerous files, similar to a zip or 7zip file.

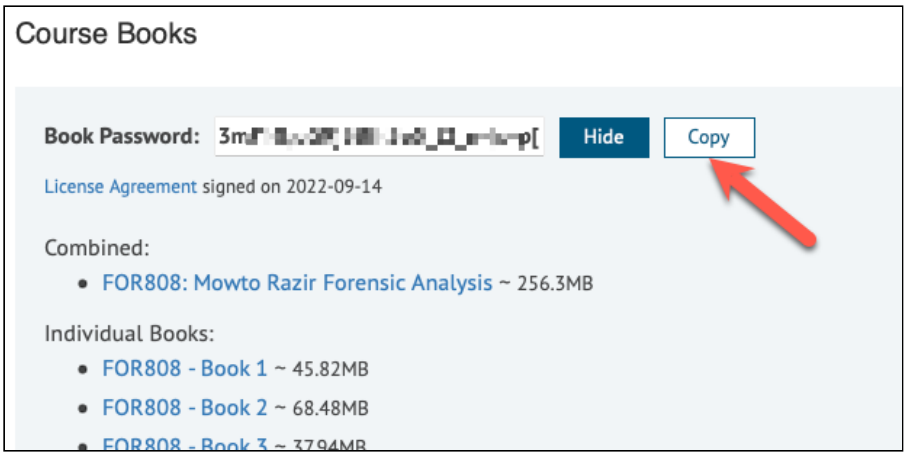
However, ISO files can be mounted to your host computer in the same way that a USB or network device can be mounted. See the following "Mounting Course ISOs" section for details on how to mount the ISO file(s) for your course.

Course books can be downloaded individually or as a combined PDF file.

8. Note that each course book is password protected. You will need the SANS-provided password to open each book. Click the "Show" button to see your personally-assigned password.

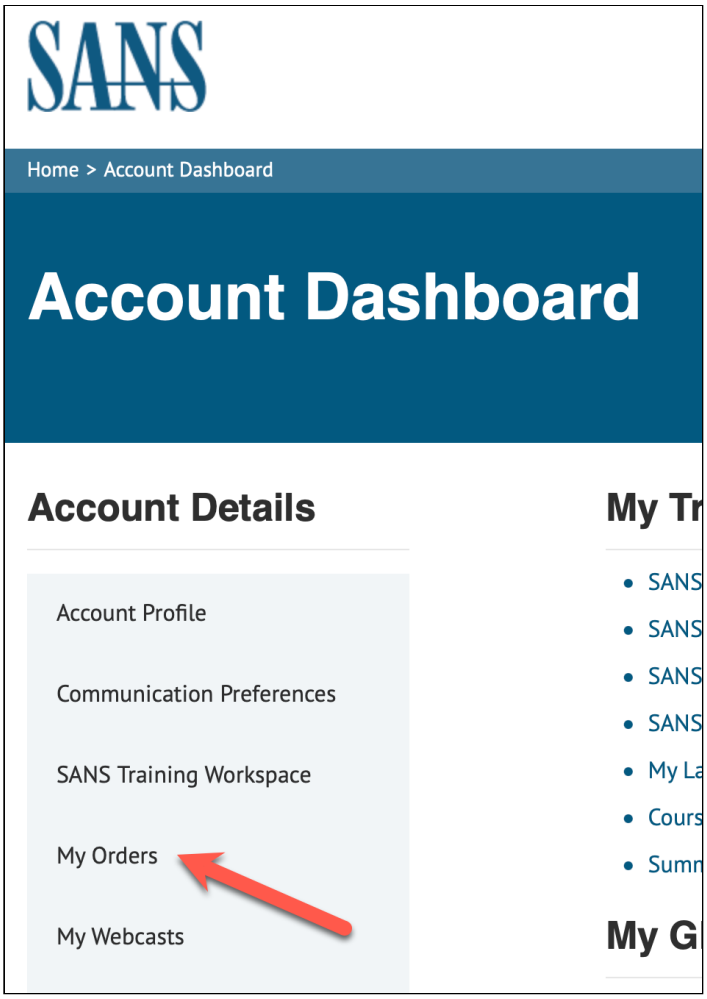


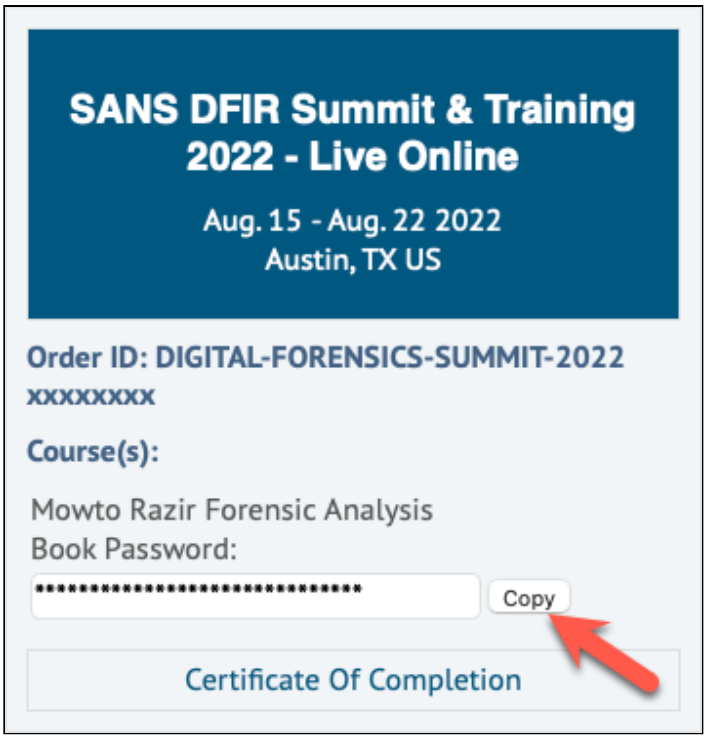
This is the password needed to open your course books. Click the "Copy" button to copy the password to your system's clipboard. We also recommend saving this in a password manager so you can continue to access your course books past the access expiration date shown in your account.



When opening the protected PDF files, you will need to provide the password provided in the dialog shown above. The process to enter the password will differ depending on your PDF reading software. Consult the documentation for your software if you need assistance with this step.

9. The "Course Material Downloads" link will show your course materials for four months after your class ends. After this time, your materials can no longer be downloaded. However, the password for the PDF copies of your courseware will remain in your SANS account after the download expires. Password for older courseware can be downloaded by selecting the "My Orders" link and then finding the order and copying the PDF password for use on files you've already downloaded.





10. If you are having difficulty downloading or accessing your course materials, contact support@sans.org for assistance.

Mounting Course ISOs

Some course content are contained within "ISO" files. ISO files are archives containing numerous files, similar to a zip or 7zip file. However, ISO files can be mounted to your host computer in the same way that a USB or network device can be mounted.

Note

Your course ISO files **do not** contain bootable operating systems. Do not attach the ISO directly to VMware unless specifically directed by the lab instructions.

These directions will cover how to mount and unmount ISO files on your host operating system. After your ISO file(s) are mounted, you may need to extract Virtual Machines for your course. Instructions for this are in the Decompressing Virtual Machines section.

Notice

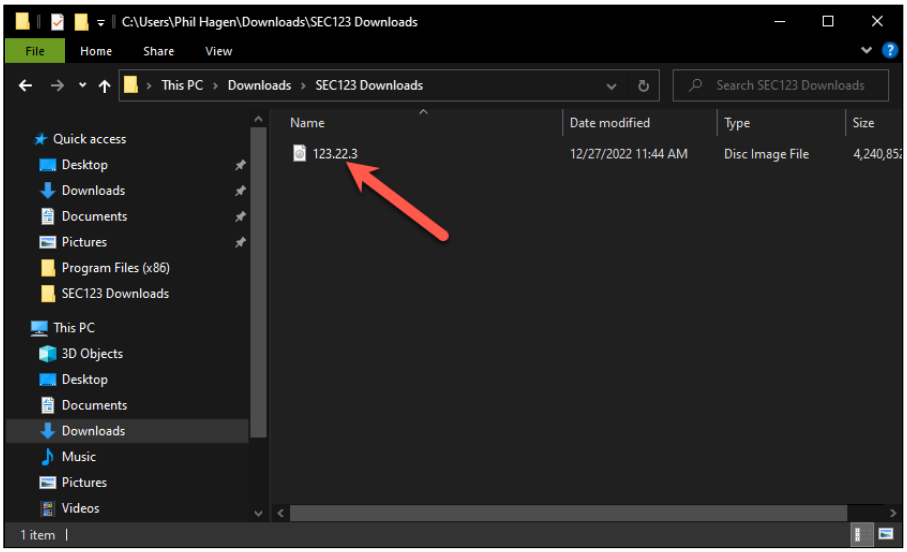
Content and screenshots in this section are examples and do not reflect your specific course ID and name.

Microsoft Windows Host (Graphical)

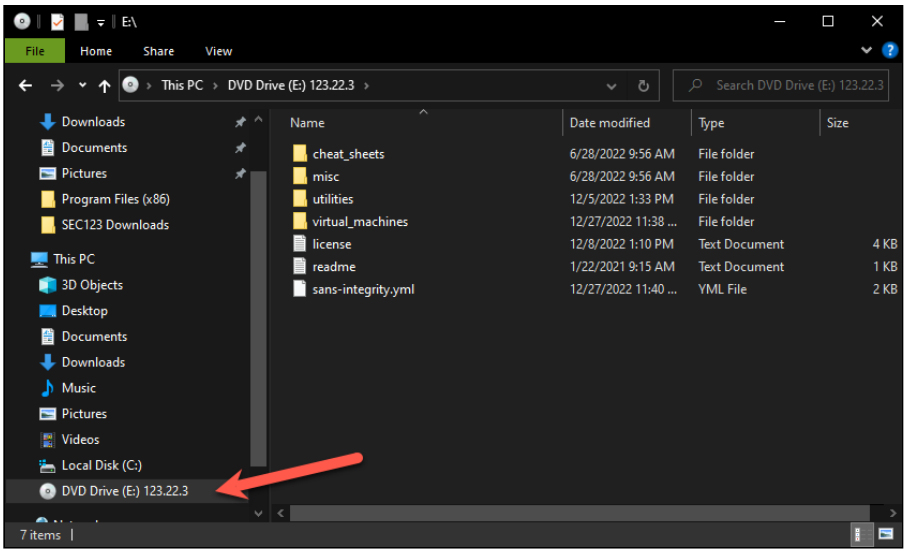
We've also provided a video demonstration that details the process of mounting an ISO in Microsoft Windows.

To mount ISO volumes:

1. Locate the downloaded ISO file(s) on your host system.
2. Double-click each ISO file to mount it.



3. In an Explorer window, the ISO content can be accessed from a drive letter assigned as a DVD drive.



4. In a command prompt, the ISO contents will be available from a drive letter assigned as a DVD drive.

Notional Results

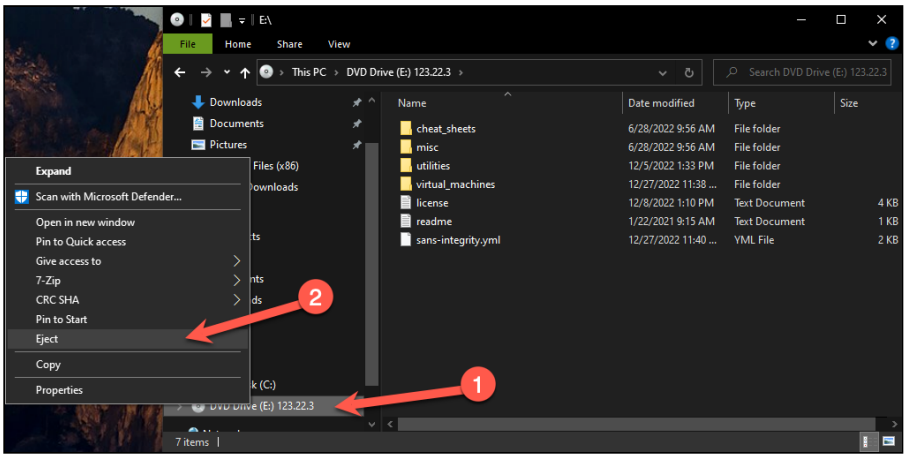
```
Microsoft Windows [Version 10.0.19044.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sansstudent>E:

E:\>dir
 Volume in drive E is 123.22.3
 Volume Serial Number is 1F00-A077

 Directory of E:\

06/28/2022  08:56 AM    <DIR>          cheat_sheets
12/08/2022  01:10 PM             3,403 license.txt
06/28/2022  08:56 AM    <DIR>          misc
01/22/2021  09:15 AM               291 readme.txt
12/27/2022  11:40 AM             1,609 sans-integrity.yml
12/05/2022  01:33 PM    <DIR>          utilities
12/27/2022  11:38 AM    <DIR>          virtual_machines
               3 File(s)          5,303 bytes
               4 Dir(s)               0 bytes free
```

Note

In some extremely rare cases, this method may not work as described. If the above steps are not successful, the Microsoft Windows Host (PowerShell Command Line) section of this section provides an alternate method to mount ISO images.

To unmount ISO volumes:

1. In an Explorer window, locate the mounted ISO volume under the "This PC" section.
2. Right-click the mounted volume and select "Eject".

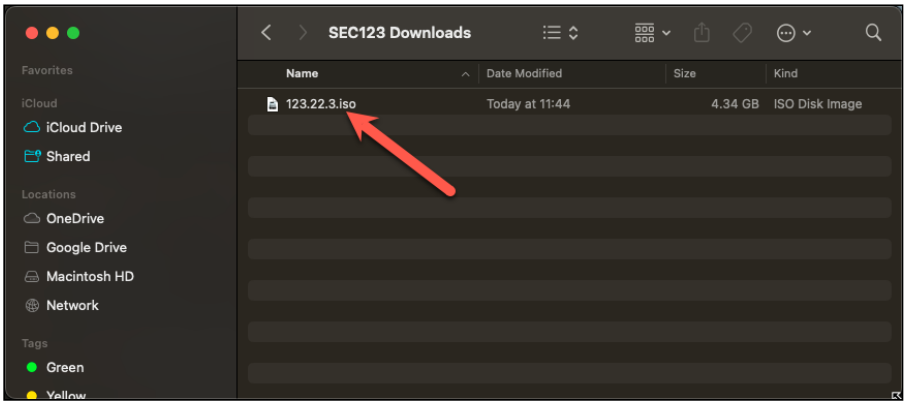


Apple macOS Host

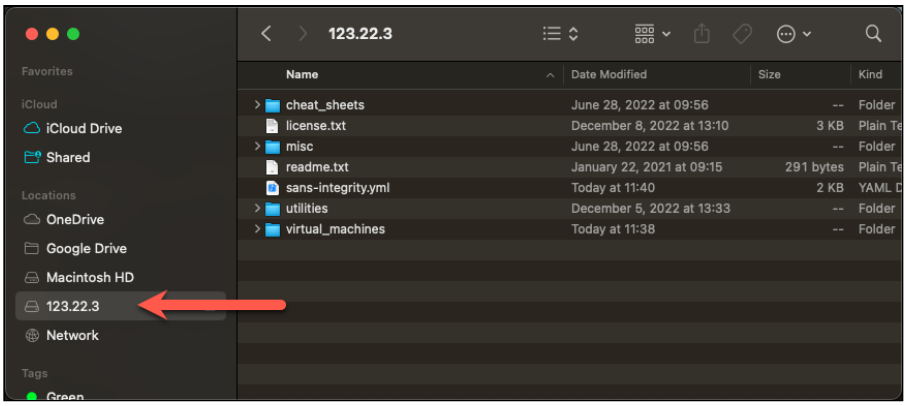
We've also provided a video demonstration that details the process of mounting an ISO in Apple macOS.

To mount ISO volumes:

1. Locate the downloaded ISO file(s) on your host system.
2. Double-click each ISO file to mount it.



3. In a Finder window, the ISO contents can be accessed from the volume name under the "Locations" section of the sidebar.



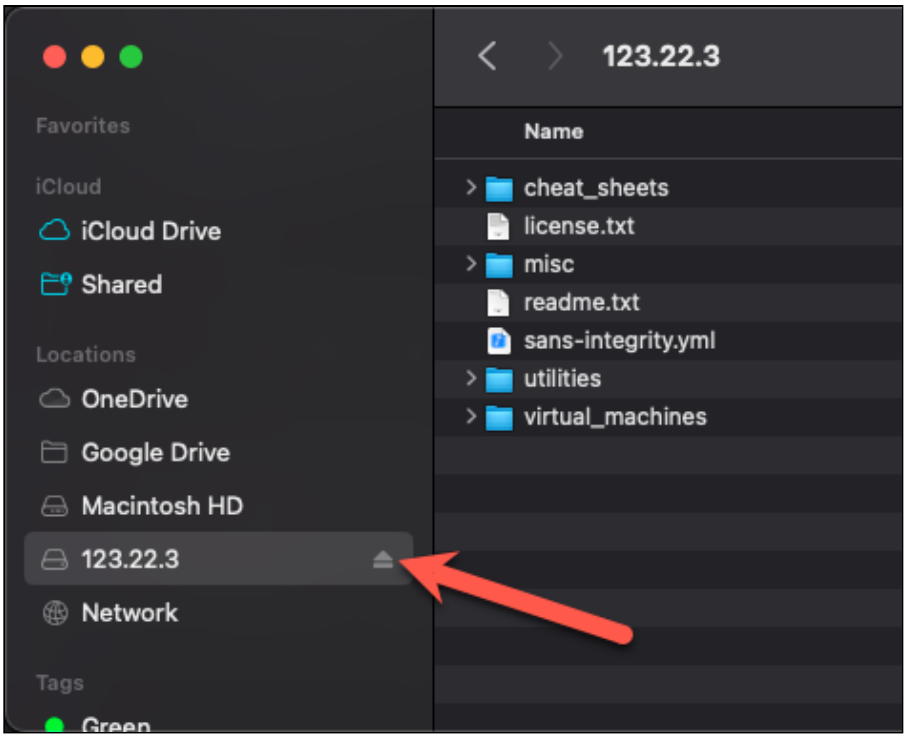
4. In a terminal window, the ISO contents will be available under the `/Volumes/` directory, with subdirectory names for each volume. For example, `/Volumes/123.22.1A/`.

Notional results

```
Last login: Tue Dec 27 11:51:18 on ttys008
sansstudent@SANS-MacBook-Pro ~ % cd /Volumes/123.22.3
sansstudent@SANS-MacBook-Pro 123.22.3 % ls -l
total 32
drwxr-xr-x  1 sansstudent  staff  2048 Jun 28  2022 cheat_sheets
-rwxr-xr-x  1 sansstudent  staff  3403 Dec  8 13:10 license.txt
drwxr-xr-x  1 sansstudent  staff  2048 Jun 28  2022 misc
-rwxr-xr-x  1 sansstudent  staff   291 Jan 22  2021 readme.txt
-rwxr-xr-x  1 sansstudent  staff  1609 Dec 27 11:40 sans-integrity.yml
drwxr-xr-x  1 sansstudent  staff  2048 Dec  5 13:33 utilities
drwxr-xr-x  1 sansstudent  staff  2048 Dec 27 11:38 virtual_machines
```

To unmount ISO volumes:

1. In a Finder window, locate the mounted ISO volume under the "Locations" section.
2. Click the "Eject" icon to the right of each volume you wish to unmount.

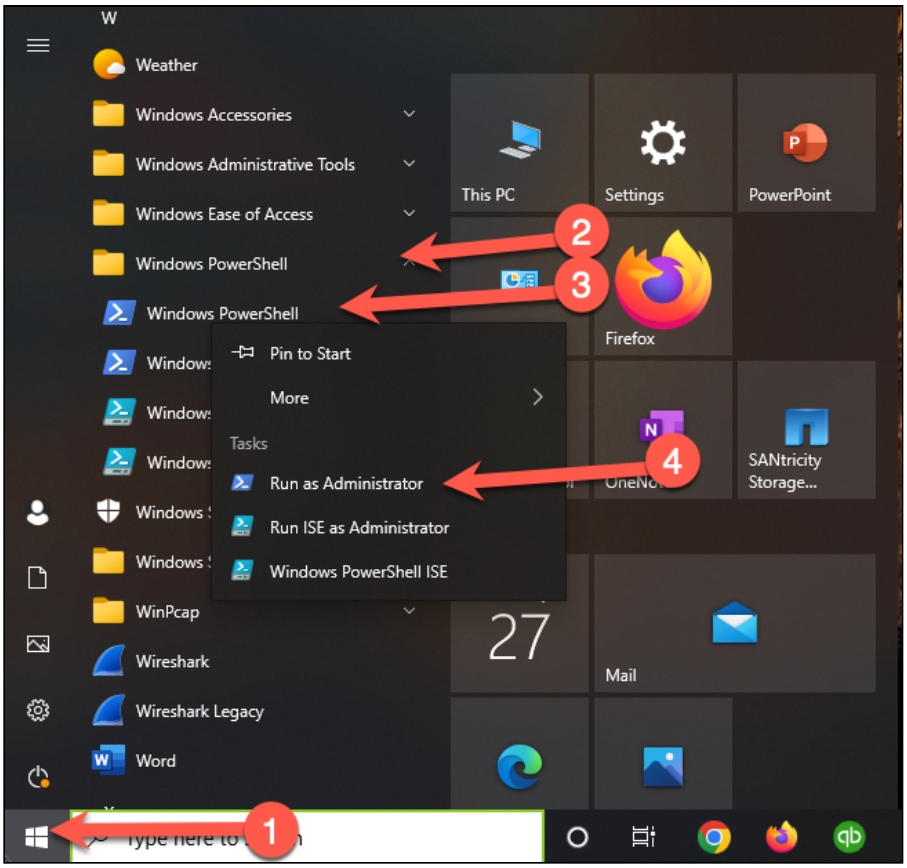


Microsoft Windows Host (PowerShell Command Line)

In some rare cases, the graphical methods explained above may not work. In this case, the following PowerShell commands can be used to mount the downloaded ISO(s).

To mount ISO volumes:

1. Run PowerShell as Administrator.



2. In the PowerShell window, run the following command, replacing the path and filename for the ISO file(s) you downloaded.

Command lines

```
Mount-DiskImage -ImagePath "C:\Users\sansstudent\Downloads\SEC123 Downloads\123.22.3.iso"
```

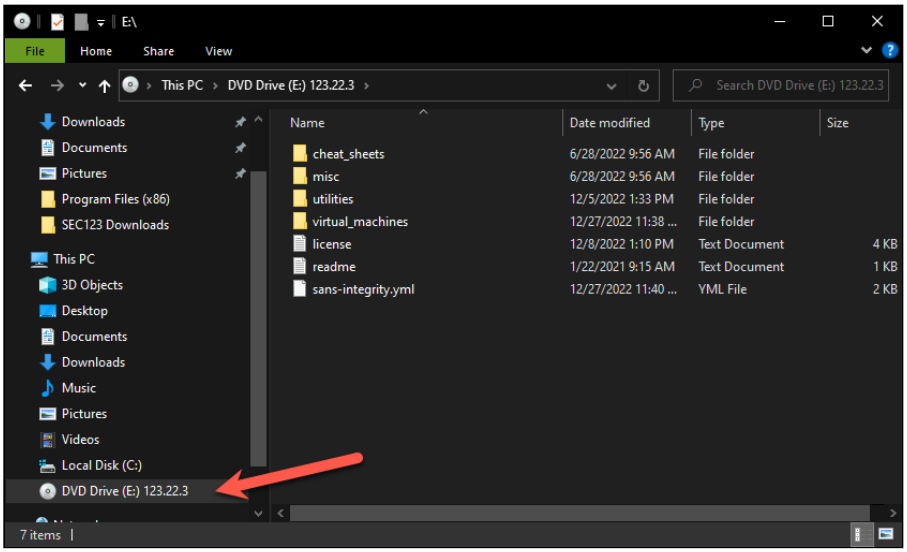
Note

This command *requires* the full path to the ISO image you wish to mount and does not support relative pathing!

Expected results

```
PS C:\Users\sansstudent> Mount-DiskImage -ImagePath "C:
\Users\sansstudent\Downloads\SEC123 Downloads\123.22.3.iso"

Attached          : True
BlockSize         : 0
DevicePath        : \\.\CDROM1
FileSize          : 19844464640
LogicalSectorSize : 2048
Number            : 1
Size              : 19844464640
PSComputerName    :
```

3. In an Explorer window, the ISO content can be accessed from a drive letter assigned as a DVD drive.



4. In a PowerShell prompt, the ISO contents will be available from a drive letter assigned as a DVD drive.

Notional Results

```
PS C:\Users\sansstudent> E:
PS E:\> dir


    Directory: E:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         6/28/2022   9:56 AM                cheat_sheets
d-----         6/28/2022   9:56 AM                misc
d-----         12/5/2022   1:33 PM                utilities
d-----        12/27/2022  11:38 AM                virtual_machines
--r---         12/8/2022   1:10 PM           3403 license.txt
--r---         1/22/2021   9:15 AM            291 readme.txt
--r---        12/27/2022  11:40 AM           1609 sans-integrity.yml
```

To unmount ISO volumes:

1. Follow the same unmounting instructions as detailed in the Microsoft Windows Host (Graphical) section of this section.

Decompressing and Booting Virtual Machines

Preparation

File Extraction Utilities

If you do not already have one of the following archive utilities installed on your host computer, install the appropriate software from the `/utilities/` directory of your ISO media file.

Microsoft Windows host: 7zip

- There is an installation binary for the 64-bit version of 7zip in your ISO media file. This installer must be run as an Administrator.

Apple macOS host: Keka

- There is a DMG file with the Keka archival utility in your ISO media file. This application should be installed to your host by double-clicking the DMG file and dragging the Keka icon to your "Applications" directory.

Virtualization Software

VMware Workstation Pro and VMware Fusion offer a 30-day evaluation license if necessary. VMware Workstation Player and VMware Fusion Player offer free licenses but a reduced set of features compared to Workstation or Fusion. Your course labs may not fully function with the Player versions. We strongly suggest the Workstation or Fusion products for this reason.

VMware Image File Extraction

After verifying that you have the proper archive utility installed, decompress the virtual machines from their respective archive files. If your course provided a virtual machine in the "Priority - Required for Day 1" section of the Course Downloads page, as described in the previous "Downloading Course Materials" section, the archive will be separate from the mounted ISO image. If the ISO media file for your course contains virtual machine archives, extract the `/virtual_machines/*.7z` files from the mounted ISO volume to a preferred location on your host system. Depending on your system and the size of the virtual machine, this may take several minutes to complete.

Warnings!

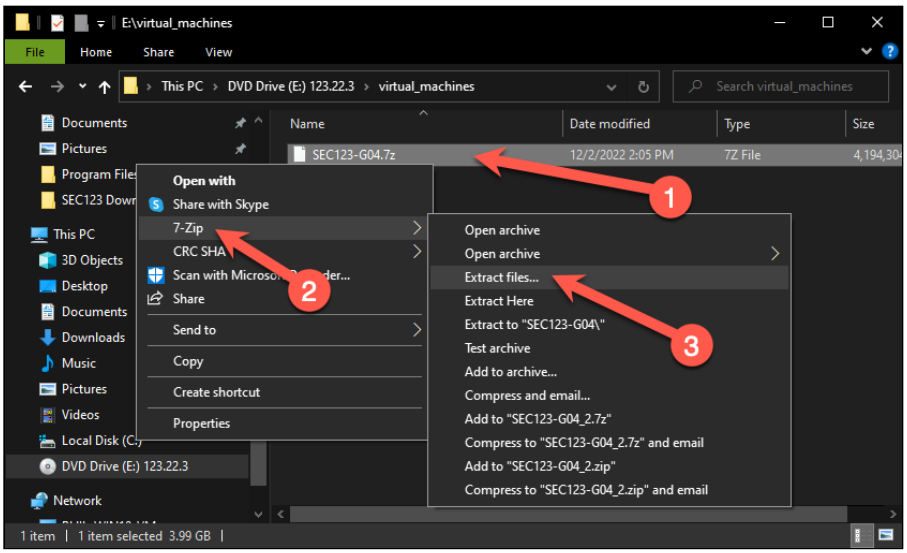
1. Due to the significant size and the dynamic nature of virtual machine files, **do not** extract your virtual machine(s) to a directory that synchronizes with a cloud storage service such as OneDrive or Dropbox.
2. Extract virtual machines contained within the mounted ISO volume. Do not copy 7zip archives from the mounted ISO volume to your host, then extract the virtual machines. Doing so will use significantly more disk space than needed and will take extra unnecessary time.

Notice

Content and screenshots in this section are examples and do not reflect your specific course ID and name.

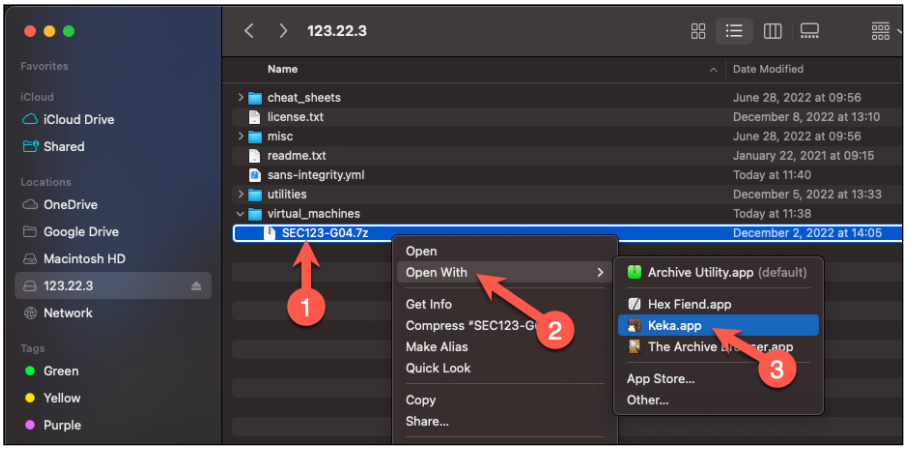
Using 7zip on Microsoft Windows

Right-click the filename of the archive you want to extract. Select "7-Zip" and then "Extract files...". Choose the desired destination directory.



Using Keka on Apple macOS

Right-click the filename of the archive you want to extract. Select "Open With" and then "Keka". Choose the desired destination directory.



Booting Virtual Machines

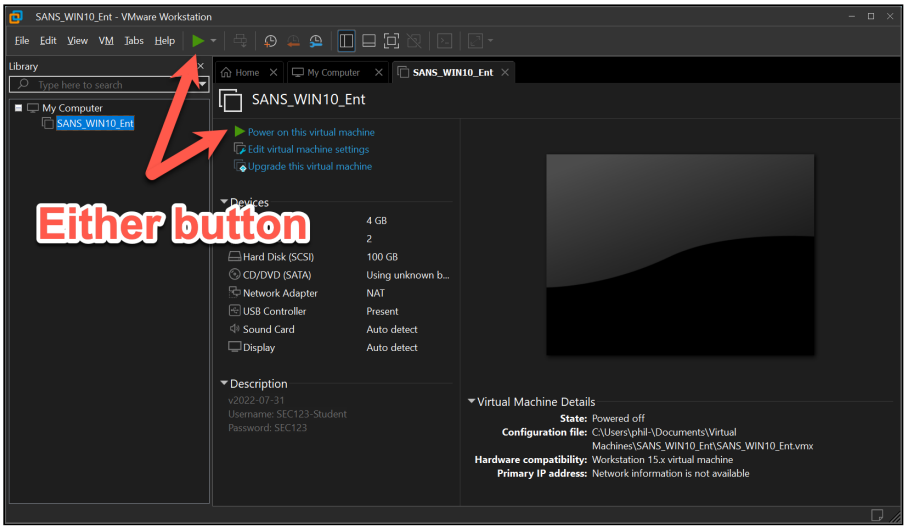
Note

Screenshots in this section depict VMware Workstation Pro 17.0.0 on a Microsoft Windows 10 host and VMware Fusion 13.0.0 on an Apple macOS Ventura 13.1 host. Your view may differ slightly with a different host operating system, VMware product, or VMware product version. All core concepts should be reasonably equivalent. If in doubt, ask your instructor, TA, or SME for assistance in getting the VMs set up.

Your course may have more than one virtual machine. If so, they may need to be used individually or together. The lab instructions for your course will indicate the virtual machine(s) to use at the appropriate time.

VMware Workstation Pro on Microsoft Windows

1. Run the VMware Workstation Pro application and open the `*.vmx` file for the virtual machine you wish to load. You must "Open" the existing virtual machine(s) that you have extracted - **do not** use VMware's "Create" or "Import" functions. Note that the `.vmx` extension may be hidden, so the Windows File Explorer may reflect a filename without an extension and a type of "VMware virtual machine configuration".
   - Alternatively, locate the `*.vmx` file in the Windows Explorer interface and double-click that file to open the virtual machine in VMware Workstation Pro. Note that this may automatically boot the virtual machine.
2. Recommended: Take a snapshot of the virtual machine prior to making any changes or booting the virtual machine for the first time. This feature is only available in VMware Workstation Pro and VMware Fusion. VMware Workstation Player does not offer this feature.
3. Optional: If you wish, you may increase the CPU and RAM resources allocated to your virtual machines. This is not necessary, as all virtual machines are tested with the resources with which they are distributed. However, if your host system has more capabilities than the minimum stated requirements, you might benefit from the increased performance that additional resources can provide.
4. Click the "Power on this virtual machine" link.

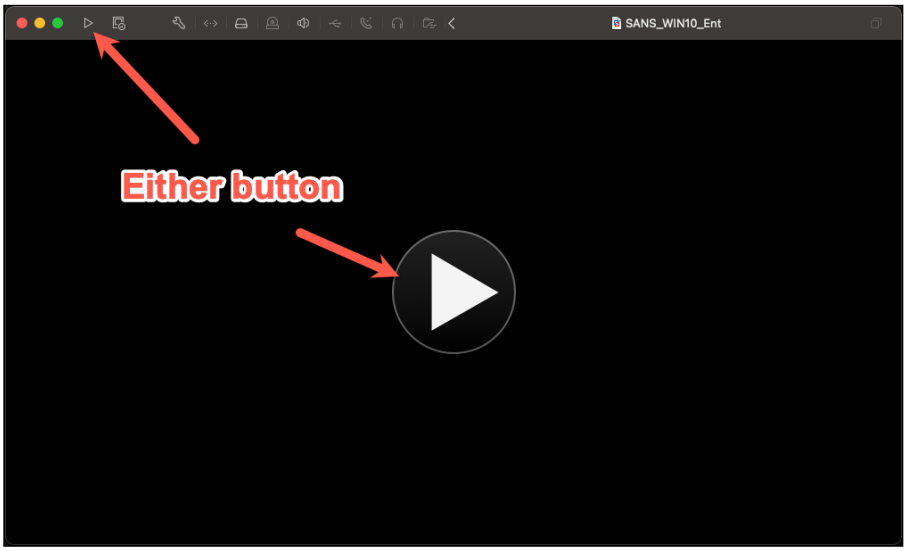


Depending on your software version, VMware may prompt you to "Upgrade this virtual machine". Click "Upgrade" if you see this dialog.

When asked if you "moved or copied" the virtual machine, click "I copied it".

VMware Fusion on macOS

1. Run the VMware Fusion application and open either the `*.vmwarevm` bundle, which looks like a file or the `*.vmx` file that you extracted. You must "Open" the existing virtual machine(s) that you have extracted. **Do not** use VMware's "Create" or "Import" functions. Note that the `.vmwarevm` or `.vmx` extension may be hidden.
    - Alternatively, locate the `*.vmwarevm` bundle in the macOS Finder interface and double-click that bundle to open the virtual machine in VMware Fusion. Note that this will automatically boot the virtual machine.
2. Recommended: Take a snapshot of the virtual machine prior to making any changes or booting the virtual machine for the first time. This feature is only available in VMware Workstation Pro and VMware Fusion. The VMWare Player products do not offer this feature.
3. Optional: If you wish, you may increase the CPU and RAM resources allocated to your virtual machines. This is not necessary, as all virtual machines are tested with the resources with which they are distributed. However, if your host system has more capabilities than the minimum stated requirements, you might benefit from the increased performance that additional resources can provide.
4. Click the "Play" icon to start the virtual machine.



Depending on your software version, VMware may prompt you to "Upgrade this virtual machine". Click "Upgrade" if you see this dialog.

When asked if you "moved or copied" the virtual machine, click "I copied it".

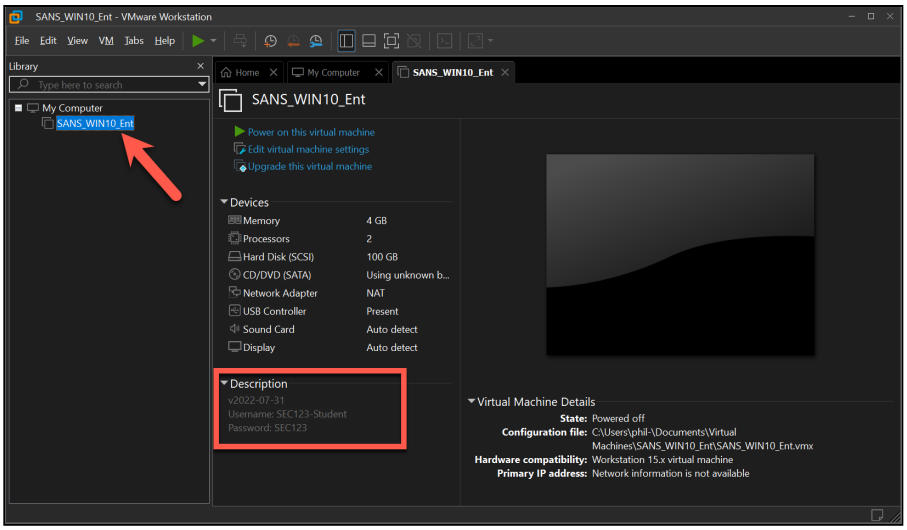
Troubleshooting error messages that may appear when Booting a VM

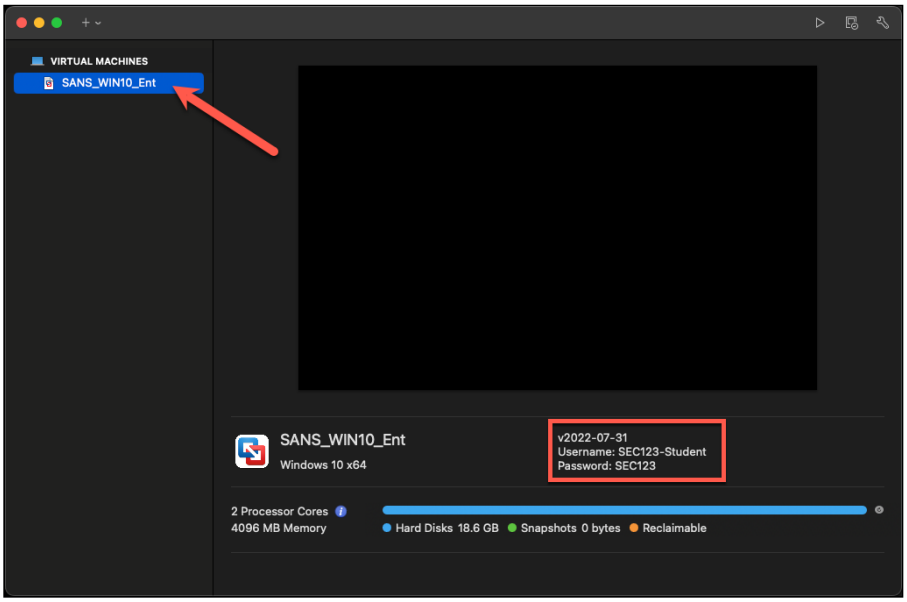
If you see an error message when attempting to power on the virtual machine, some of the following sections in this section may provide useful assistance.

Error Message	Troubleshooting Section Title
Device or Credential Guard	VMware Workstation/Credential Guard Incompatibility
This host is VT-capable, but VT is disabled	Enabling Virtualization Technology Extensions (VTx) in Intel and AMD BIOS
Hyper-V (Windows hosts only)	VMware Workstation/Hyper-V Incompatibility
Side Channel Mitigations, Virtualized Performance Counters, or Nested Virtualization (macOS hosts only)	VMware Fusion Issues with macOS 11 (Big Sur)

Logging Into Virtual Machines

After the virtual machine boots, you may need to provide login credentials or the virtual machine may automatically log you in. If credentials are needed, see the "Virtual Machine Credentials" section for details. All login credentials are also displayed in the respective virtual machine's information panel. Below are screenshots showing the login credentials under VMware Workstation and VMware Fusion, respectively.



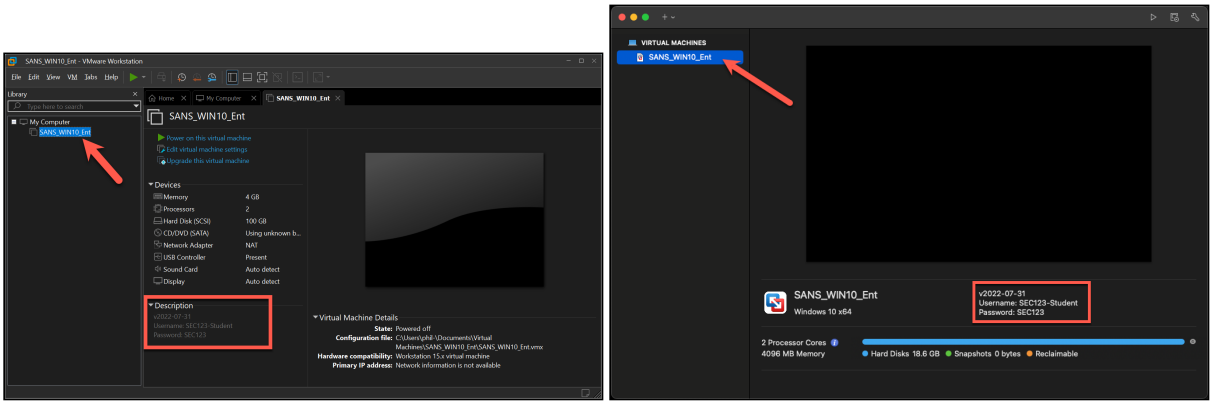


It is critical that you **do not** upgrade software within the virtual machine unless specifically directed to do so in the lab instructions. Your virtual machine has been extensively tested in the configuration which it was distributed. SANS cannot ensure your labs will function properly if the software is updated.

Virtual Machine Credentials

The login credentials for all virtual machines used in this class are listed below for quick reference.

All login credentials are also displayed in the respective virtual machine's information panel. Below are screenshots showing the login credentials under VMware Workstation and VMware Fusion, respectively.



1. FOR508 SIFT Linux Workstation
   - Username: `sansforensics`
   - Password: `forensics`

   This user has `sudo` access for all commands on the virtual machine.
2. FOR508 Windows VM
   - Username: `SANSDFIR`
   - Password: `forensics`

   This user has local administrative rights on the virtual machine.

VMware Workstation/Credential Guard Incompatibility

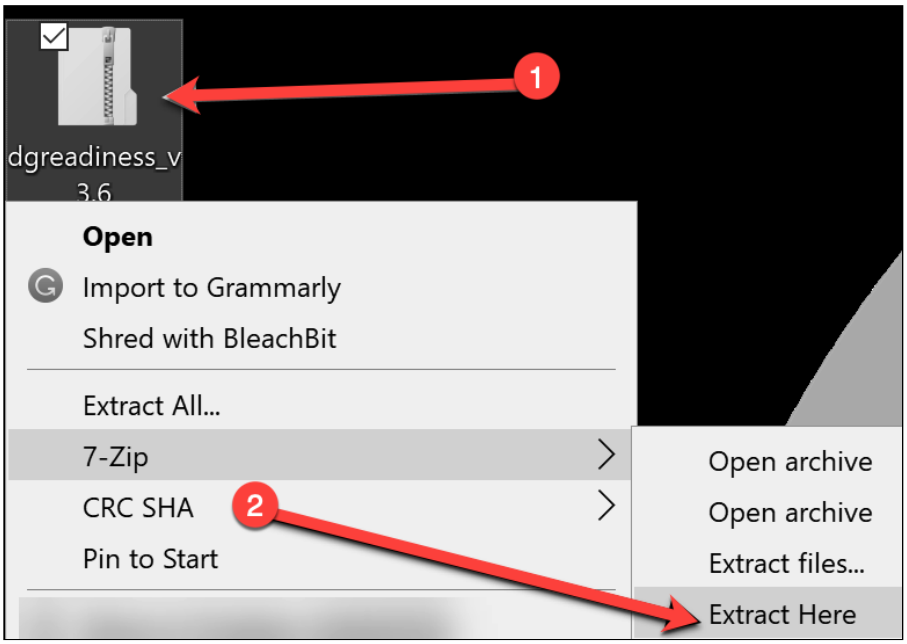
If your Windows host system has Credential Guard enabled and you attempt to run VMware Workstation, there is an issue that may prevent you from using your VMware in class..

Upon running VMware Workstation, you may encounter a dialog such as below. You will not be able to start the application.

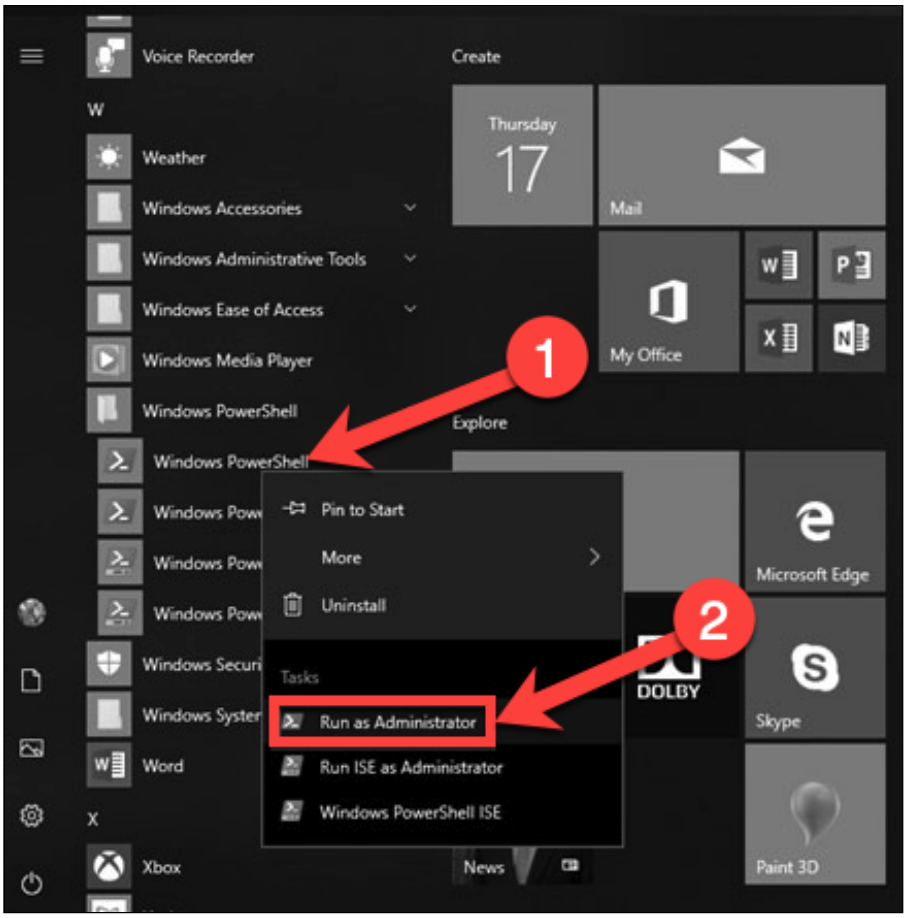
To correct this, take the following steps.

Disabling Credential Guard for Class

1. From your **host operating system**, Download the "Device Guard and Credential Guard hardware readiness tool" from Microsoft.
2. Move the downloaded zip file to your desktop and extract the zip file to your Desktop.



3. Run PowerShell as Administrator.



4. In the PowerShell window, change the directory to the folder where the script is extracted and run the following PowerShell commands. For example, in the command below, the zip file was extracted to the Desktop folder. You may need to reboot your host system for the changes to take effect.

> **Note:**
>
> The exact version might change over time. In this example, the version is 3.6, but that might change if Microsoft updates the tool. If it does, in each command below, the folder path might change slightly based on the version number.

Command lines

```
cd ~\Desktop\dgreadiness_v3.6\
Set-ExecutionPolicy Unrestricted
```

Expected results

```
PS C:\Users\sansforensics> cd ~\Desktop\dgreadiness_v3.6\
PS C:\Users\sansforensics\Desktop\dgreadiness_v3.6> Set-ExecutionPolicy Unrestricted
Execution Policy Change
...
Do you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"):
```

Type `A` and press the Enter/Return key.

Command lines

```
.\DG_Readiness_Tool_v3.6.ps1 -Disable
```

Expected results

```
PS C:\Users\sansforensics\Desktop\dgreadiness_v3.6> .\DG_Readiness_Tool_v3.6.ps1 -
Disable
Security Warning
...
Do you want to run C:
\Users\<%YOUR_USERNAME%>\Desktop\dgreadiness_v3.6\DG_Readiness_Tool_v3.6.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (Default is "D"):
```

Type `R` and press the Enter/Return key.

Expected results

```
...

################################################################################
Readiness Tool Version 3.4 Release
Tool to check if your device is capable to run Device Guard and Credential Guard
################################################################################
Disabling Device Guard and Credential Guard
Deleting RegKeys to disable DG/CG

...

Disabling Hyper-V and IOMMU
Disabling Hyper-V and IOMMU successful

Please reboot the machine, for settings to be applied.
```

Reboot as directed and your system should be ready for use.

Re-enabling Credential Guard After Class

When class is over, if you no longer need to use VMware Workstation and/or require Credential Guard to be enabled, follow these steps.

1. Run PowerShell as Administrator as shown above.
2. Run the following commands. You may need to reboot your host system for the changes to take effect.

Note:

The exact version might change over time. In this example, the version is 3.6, but that might change if Microsoft updates the tool. If it does, in each command below, the folder path might change slightly based on the version number.

Command lines

```
cd ~\Desktop\dgreadiness_v3.6\
.\DG_Readiness_Tool_v3.6.ps1 -Enable -CG
```

Expected results

```
PS C:\Users\sansforensics> cd ~\Desktop\dgreadiness_v3.6\
PS C:\Users\sansforensics\Desktop\dgreadiness_v3.6> .\DG_Readiness_Tool_v3.6.ps1 -
Enable -CG
Security warning
...
Do you want to run C:
\Users\<%YOUR_USERNAME%>\Desktop\dgreadiness_v3.6\DG_Readiness_Tool_v3.6.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (Default is "D"):
```

Type `R` and press the Enter/Return key.

Expected results

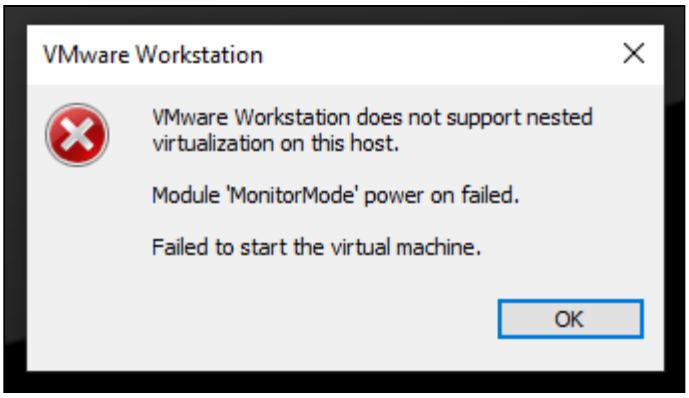
```
###############################################################################
Readiness Tool Version 3.4 Release
Tool to check if your device is capable to run Device Guard and Credential Guard
###############################################################################
###############################################################################
OS and Hardware requirements for enabling Device Guard and Credential Guard
    1. OS SKUs: Available only on these OS Skus - Enterprise, Server, Education,
Enterprise IoT, Pro, and Home
    2. Hardware: Recent hardware that supports virtualization extension with SLAT
To learn more, please visit: https://aka.ms/dgwhcr
###############################################################################

Enabling Device Guard and Credential Guard
Setting RegKeys to enable DG/CG
Enabling Hyper-V and IOMMU
Enabling Hyper-V and IOMMU successful
Please reboot the machine, for settings to be applied.
```

Reboot as directed and your system should be ready for use.

VMware Workstation/Hyper-V Incompatibility

If your Windows host system has Hyper-V enabled and you are running Windows 10 version 2004, there is an issue that may prevent you from using your class VM(s) in VMware Workstation 15.5.5.

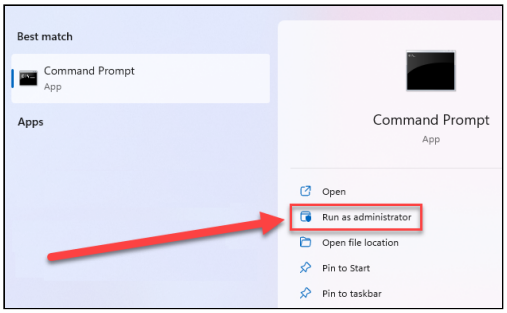
Upon starting your class virtual machine(s), you may encounter a dialog such as below. You will not be able to start the virtual machine.



To correct this, take the following steps.

Disabling Hyper-V Features for Class

1. If needed, disable Credential Guard using instructions in the "Credential Guard" section
2. Click the Windows button and type `cmd`. Then click on `Run as administrator`.



3. In the command-line windows type the following command and then reboot your computer to ensure the changes take effect.

Command lines

```
bcdedit /set hypervisorlaunchtype off
```

Expected results

```
Microsoft Windows [Version 10.0.19042.1466]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32> bcdedit /set hypervisorlaunchtype off
The operation completed successfully.
```

Your VM should now run as expected.

Re-enabling Hyper-V Features After Class

1. When class is over and you no longer need to use the class virtual machine, follow the same steps as above to open the administrative command prompt, then type the following command and then reboot your computer.

Command lines

```
bcdedit /set hypervisorlaunchtype auto
```

Expected results

```
Microsoft Windows [Version 10.0.19042.1466]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32> bcdedit /set hypervisorlaunchtype auto
The operation completed successfully.
```

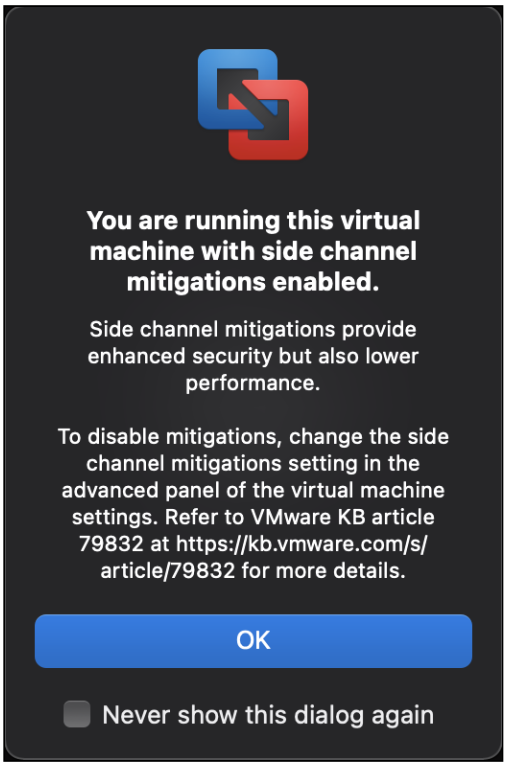
2. If you disabled Credential Guard, re-enable it with the instructions in the "Credential Guard" section.

VMware Fusion Issues with macOS 11 (Big Sur)

With the update to macOS 11 (Big Sur), there are a few issues that may prevent you from using your class VM(s) in VMware Fusion 12. This section addresses these issues.

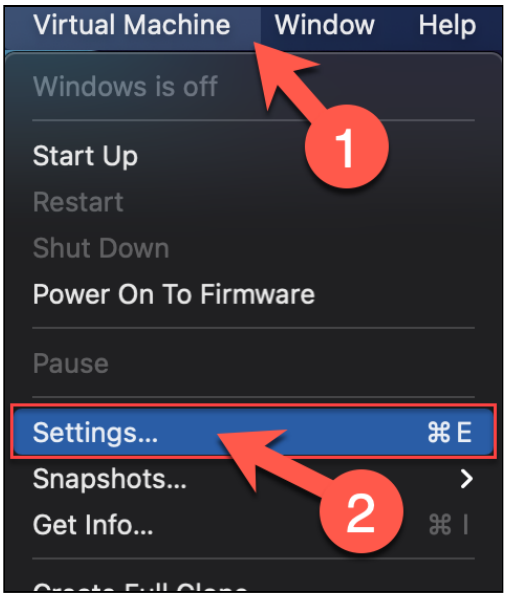
"Side Channel Mitigations" Error Message

Upon starting your class virtual machine(s), you may encounter a dialog such as below. You can safely click OK in order to continue running the affected virtual machine, however you may see degraded performance as a result.



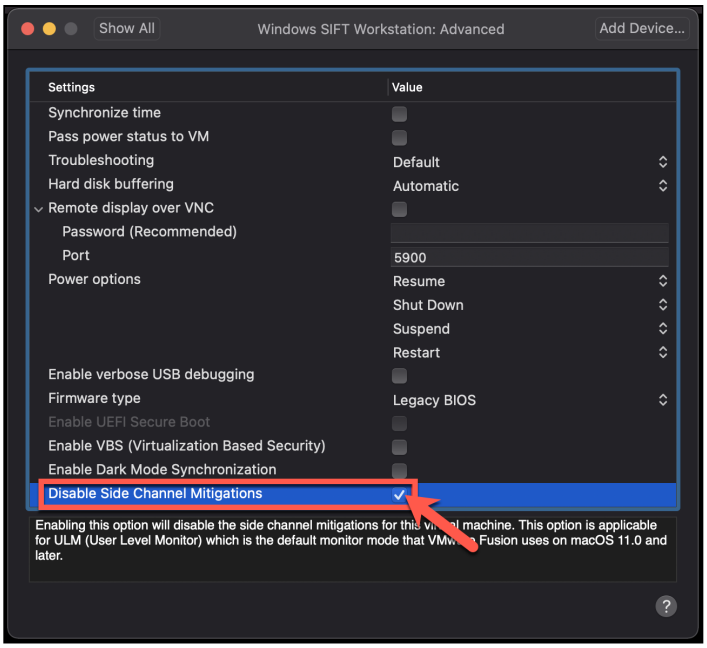
To overcome any performance issues take the following steps.

1. Shut down the virtual machine. (Not "Suspend".)
2. Click on the `Virtual Machine` menu item. Then click `Settings...`.



3. Click the `Advanced` icon.

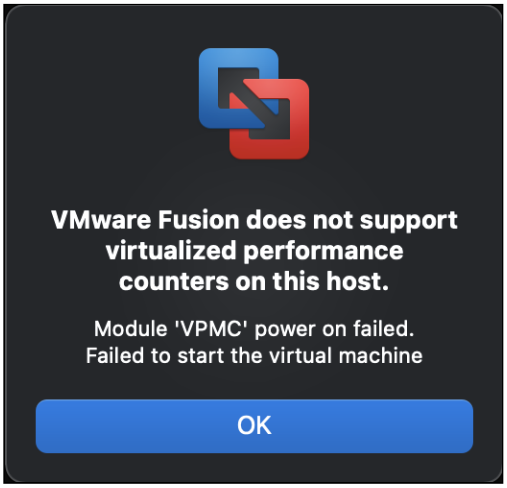
4. Check the box next to `Disable Side Channel Mitigations`



5. Close the Settings dialog and start the virtual machine.

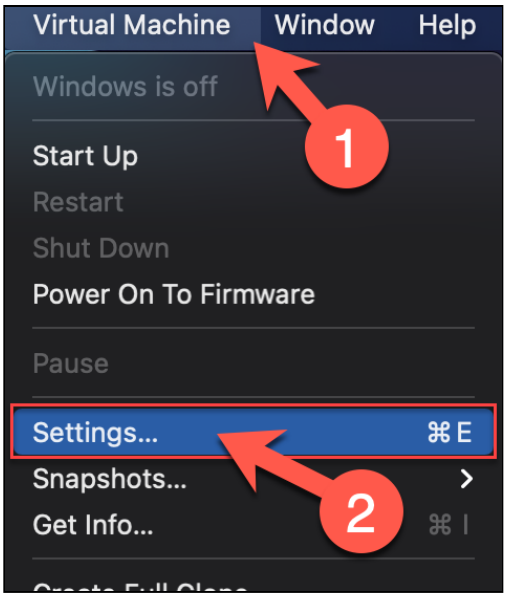
"Virtualized Performance Counters" Error Message

Upon starting your class virtual machine(s), you may encounter a dialog such as the one below. You will not be able to start the virtual machine.



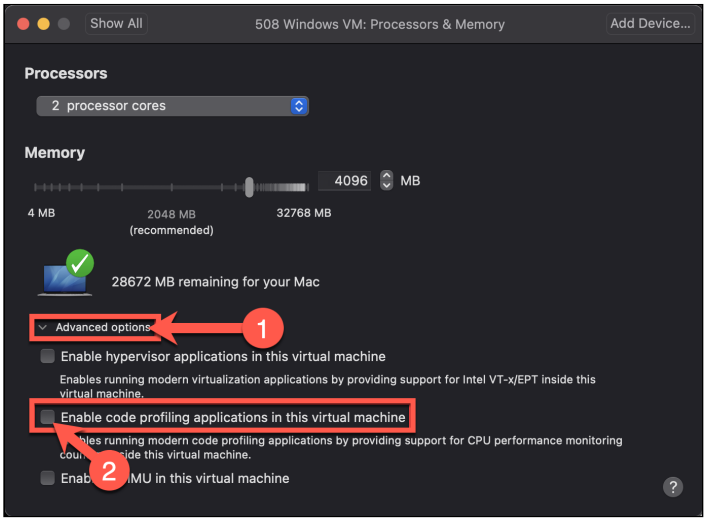
To correct this, take the following steps.

1. Click on the `Virtual Machine` menu item. Then click `Settings...`.



2. Click the `Processors & Memory` Icon.

3. Click the arrow to expand the `Advanced options` section. Then un-check the box next to `Enable code profiling applications in this virtual machine`.



4. Close the Settings dialog and start the virtual machine.

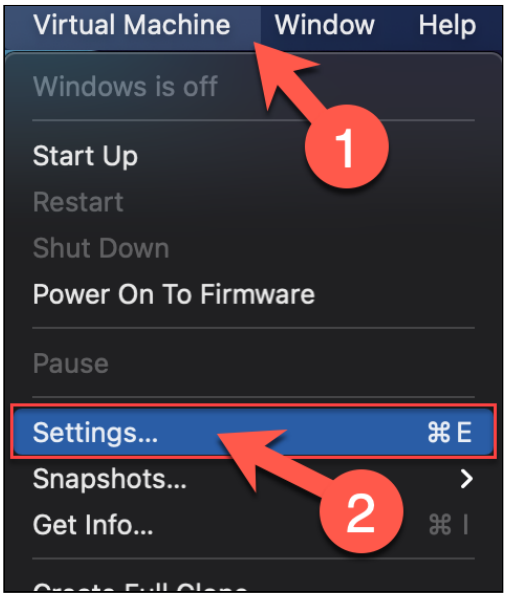
"Nested Virtualization" Error Message

Upon starting your class virtual machine(s), you may encounter a dialog such as the one below. You will not be able to start the virtual machine.

To correct this, take the following steps.

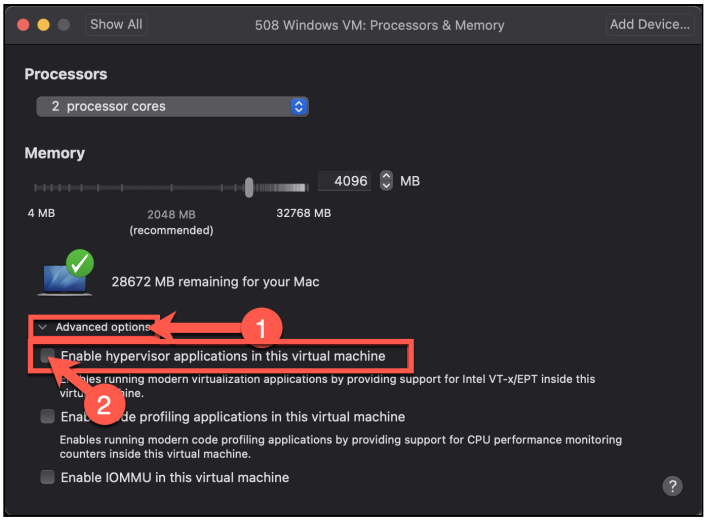
> **WARNING!**
>
> While taking these steps will allow you to boot the virtual machine, you may not be able to complete any labs that rely on nested virtualization features. Contact your instructor or OnDemand support to determine if this affects your class.

1. Click on the `Virtual Machine` menu item. Then click `Settings...`.



2. Click the `Processors & Memory` Icon.

3. Click the arrow to expand the `Advanced options` section. Then un-check the box next to `Enable hypervisor applications in this virtual machine`.

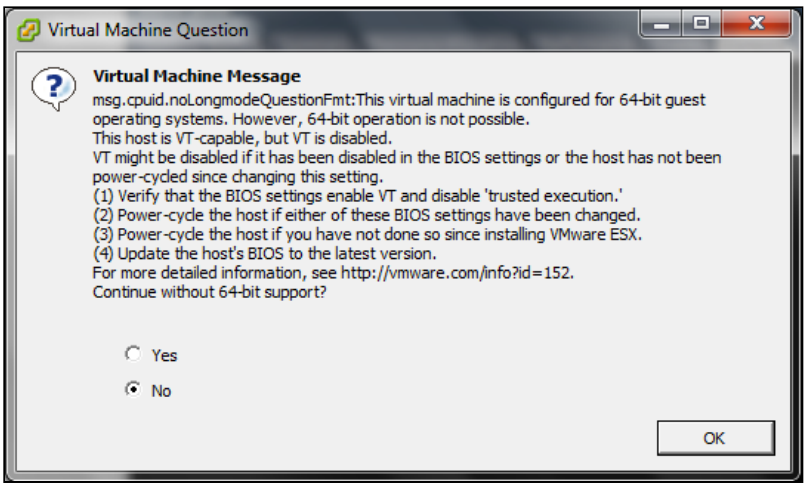


4. Close the Settings dialog and start the virtual machine.

Enabling Virtualization Technology Extensions (VTx) in Intel and AMD BIOS

On Intel and AMD systems, there is a BIOS extension that must be enabled or you will not be able to boot your class VM(s) in VMware.

Upon starting your class virtual machine(s), you may encounter a dialog similar to the one below. Starting the virtual machine without 64-bit support will result in a non-functional VM.



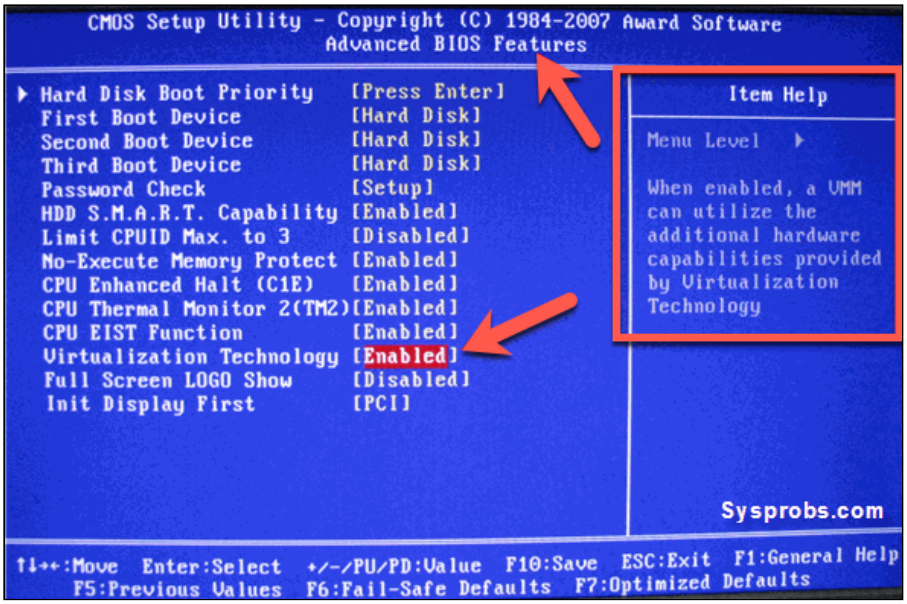
To correct this, take the following steps.

Enabling VTx for Class

1. Enter your system's BIOS configuration menus. This requires pressing a designated key immediately upon booting/rebooting your system, but the exact key depends on the system and BIOS manufacturers. Most systems use one of the following five keys:
    - F1
    - F2
    - DEL
    - ESC
    - F10
    - Older computers may require multiple keys to be pressed simultaneously, or keys other than those listed above:
        - CTRL+ALT+ESC
        - CTRL+ALT+INS
        - CTRL+ALT+ENTER
        - CTRL+ALT+S

- PGUP
- PGDN

2. Identify the BIOS menu that controls the VTx settings. This is also dependent on the specific version of BIOS that your system uses. The screenshots below represent the Award BIOS, but you may need to explore the various BIOS menus on your system to find the proper menu and setting. Different BIOS versions also have varying keyboard controls - some use the space bar to change settings, others use the PGUP and PGDN keys, etc.



Saving the settings may require pressing F10 or other keys or menu sequences.

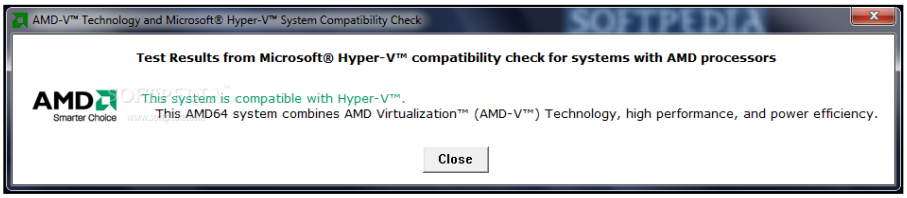
3. Exit the BIOS settings and reboot the system. Ideally, keep the power off for approximately one minute before powering it on to clear any residual configuration settings. The reboot is critical, as the BIOS settings are essentially a configuration file that is only read at boot time.

Verifying That VTx Settings are Correct

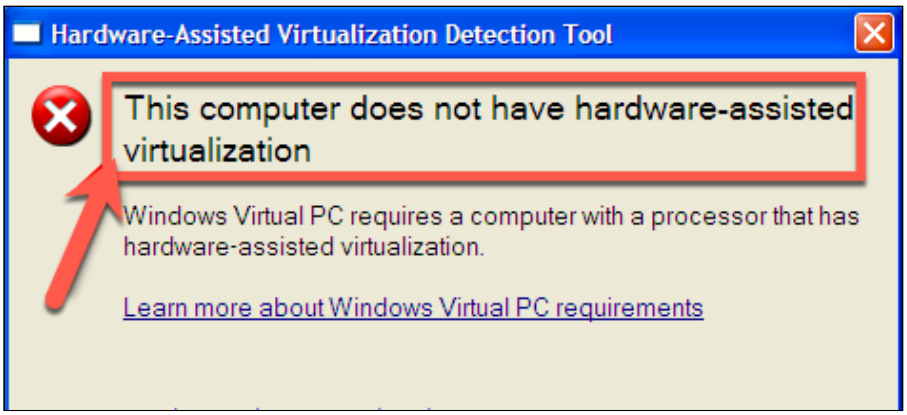
There are several ways to verify that the VTx settings above have been set correctly.

1. Boot your class VM(s) to ensure the VTx error at the beginning of this section is not displayed.
2. For Intel processors, you may download the Intel Processor Identification Utility. Run the utility and click the `CPU Technologies` tab to confirm if VTx is enabled or not.

3. For AMD processors, you may download the AMD Virtualization Technology and Microsoft Hyper-V System Compatibility Check Utility. Run the utility to confirm if VTx is enabled or not.



4. For both Intel and AMD processors, you may download Microsoft's Hardware-Assisted Virtualization Detection Tool. Run the utility to confirm if VTx is enabled or not.



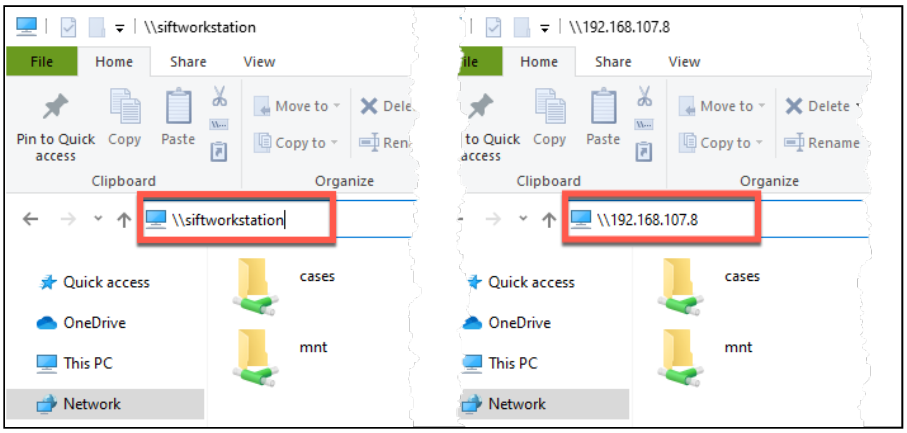
Windows File Sharing Issues

During your class, you may wish to share or copy files between your host system and a virtual machine or between virtual machines. One method of doing this is to use Microsoft Windows's native file sharing features, known as SMB. Tools that provide SMB functionality are available for Windows, macOS, and Linux operating systems. If you wish to use SMB to share files from a Windows client system, you'll need to follow the steps in this section to adjust the security settings. Using a macOS or Linux client system does not require these measures.

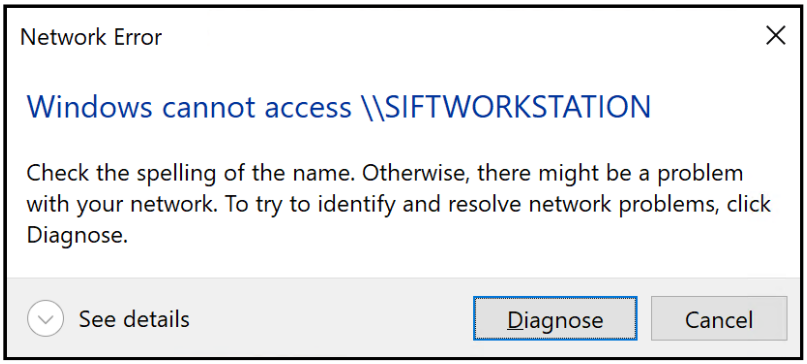
Using UNCs for SMB Sharing

To connect from one Windows system to another running SMB, you'll use UNC syntax with the destination system's hostname or IP address:

- `\\<%DESTINATION_SYSTEM_HOSTNAME%>\`
- `\\<%DESTINATION_SYSTEM_IP_ADDRESS%>\`



If, after attempting to access the destination system using both the hostname and IP address UNCs, you receive the following error message, you will need to change your settings on the Microsoft Windows client system to enable SMB functionality.



First Troubleshooting Approach

The following PowerShell one-liner is often all that is needed to fix the above error. Run this command before doing moving forward with any other steps.

Run this command from an Administrator PowerShell Terminal.

Command lines

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters"
AllowInsecureGuestAuth -Type DWORD -Value 1 -Force
```

If the command runs successfully, no results will be displayed in the PowerShell terminal.

Close and restart Windows Explorer and re-test your connection to file share. If you still receive the error message, see the additional troubleshooting steps below.

Additional Troubleshooting Approaches

If SMB sharing still is not working after running the above PowerShell one-liner, one or more of the following steps may be required.

1. Verify Lanman Workstation `AllowInsecureGuestAuth` Setting This PowerShell command will display the current Lanman Workstation `AllowInsecureGuestAuth` registry key. This MUST be set to `1` for Windows File Sharing to function.

   Run this command from an Administrator PowerShell Terminal.

   Command lines

   ```
   Get-ItemProperty -Path "HKLM:
   \SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters" | format-list -property
   AllowInsecureGuestAuth
   ```

   Expected results

   ```
   PS C:\Users\sansforensics> Get-ItemProperty -Path "HKLM:
   \SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters" | format-list -
   property AllowInsecureGuestAuth
   AllowInsecureGuestAuth : 1
   ```

   If this returns a value of `0` instead, run the PowerShell one-liner in the First Troubleshooting Approach section above.

2. Verify the destination machine's IP address

The network interface name can vary from system to system, and some systems will have more than one interface. You will need to know which interface is being used for SMB access. Your TA, SME, or instructor can assist you if you're unsure which interface is being used.

Log in to the destination system.

a. If the destination system is running Linux:

Command lines

```
ip address
```

Notional results

```
sansforensics@siftworkstation: ~
$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
default qlen 1000
    link/ether 00:0c:29:3a:47:73 brd ff:ff:ff:ff:ff:ff
    inet 192.168.107.8/24 brd 192.168.107.255 scope global dynamic noprefixroute
ens33
    valid_lft 85518sec preferred_lft 85518sec
    inet6 fd15:4ba5:5a2b:1008:35c7:81c:372d:e121/64 scope global temporary dynamic
    valid_lft 604786sec preferred_lft 86054sec
    inet6 fd15:4ba5:5a2b:1008:76b7:6100:3d57:95e9/64 scope global dynamic
mngtmpaddr noprefixroute
    valid_lft 2591985sec preferred_lft 604785sec
    inet6 fe80::ceae:7a20:f025:62b6/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN
group default
    link/ether 02:42:24:25:69:75 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
    valid_lft forever preferred_lft forever
```

In this case, the interface `ens33` is the only one used for the VM's services and its IP address is `192.168.107.8`, indicated by the highlighted line:

```
inet 192.168.107.8/24 ...
```

b. If the destination system is running Windows:

Command lines

```
ipconfig
```

Notional results

```
C:\Users\sansforensics> ipconfig
Ethernet adapter Ethernet:

Connection-specific DNS Suffix  . : sansgear.com
IPv6 Address. . . . . . . . . . . : fd15:4ba5:5a2b:1008:9c14:e101:232:5a1c
Temporary IPv6 Address. . . . . . : fd15:4ba5:5a2b:1008:8b4:b370:203b:a766
Temporary IPv6 Address. . . . . . : fd15:4ba5:5a2b:1008:a426:af82:6efc:488
Link-local IPv6 Address . . . . . : fe80::9c14:e101:232:5a1c%12
IPv4 Address. . . . . . . . . . . : 192.168.107.2
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : fe80::472:1446:5c3d:7670%12
                                    192.168.107.1
```

In this case, the IP address is `192.168.107.2`, indicated by the highlighted line:

```
IPv4 Address. . . . . . . . . . . : 192.168.107.2
```

3. Allow File and Print Sharing through the firewall

The simplest approach is to turn off the Windows Firewall entirely while you are in the classroom environment. The following command will accomplish this.

Run this command from an Administrator PowerShell Terminal or Administrator Command Prompt.

Command lines

```
netsh advfirewall set allprofiles state off
```

Expected results

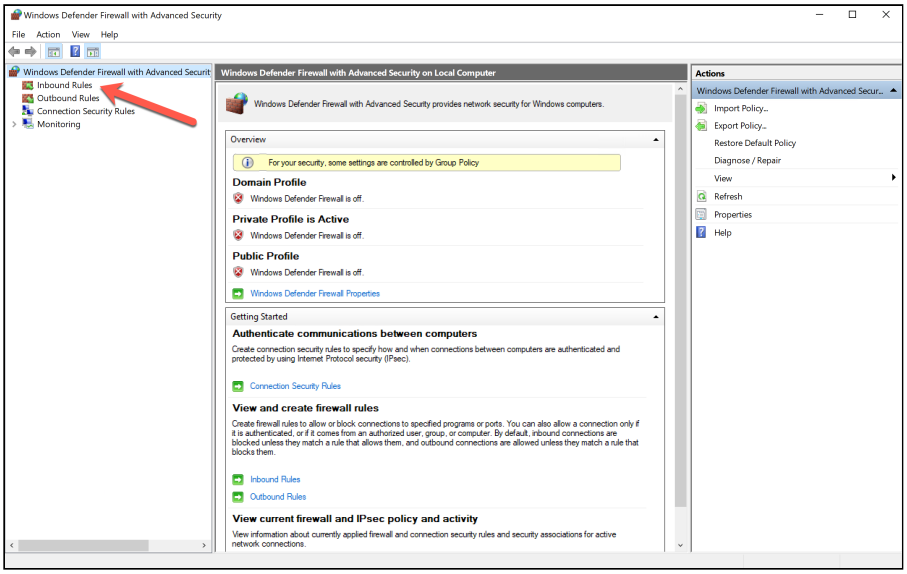
```
PS C:\Users\sansforensics> netsh advfirewall set allprofiles state off
Ok.
```

To re-enable the firewall after class, run the same command with `on` instead of `off`.

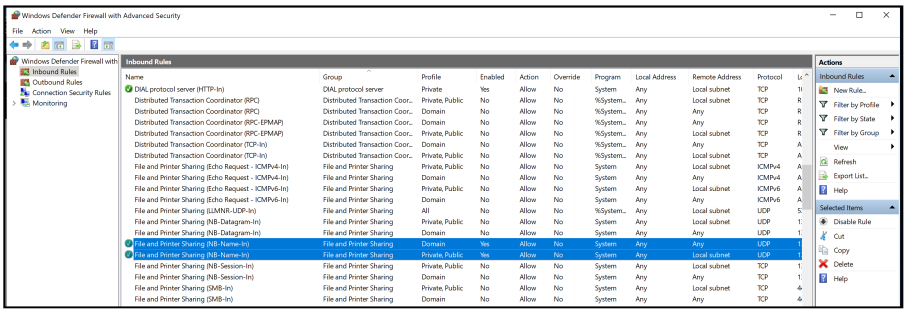
If you are not able to disable the firewall completely, you can open only the file and print sharing ports.

a. Open Control Panel, click System and Security, and then click Windows Firewall.

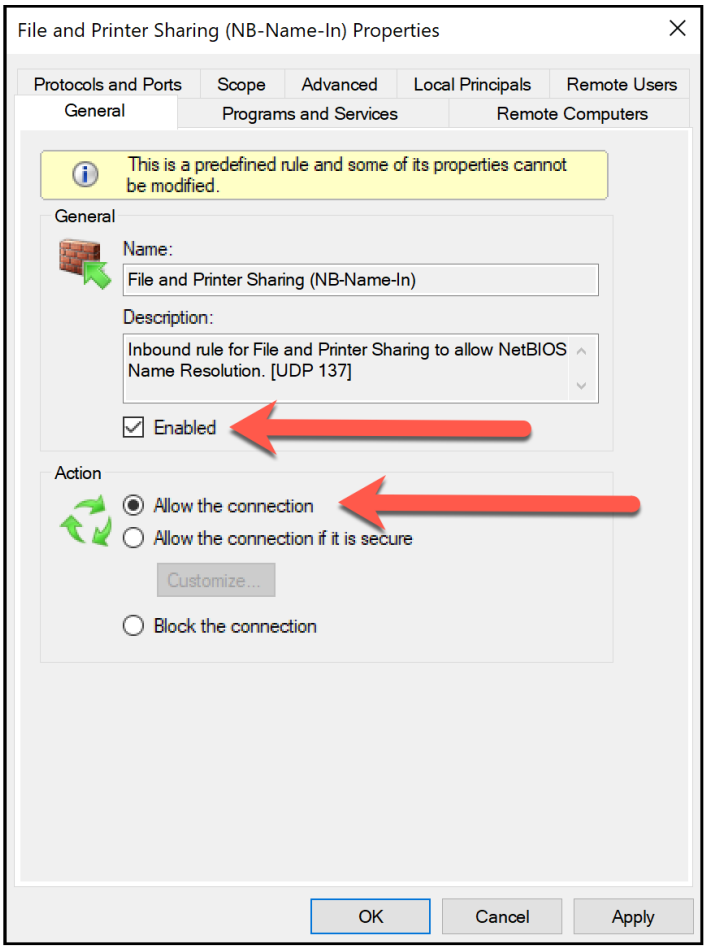
b. In the left pane, click Advanced settings, and in the console tree, click Inbound Rules.



c. Under Inbound Rules, locate the rules `File and Printer Sharing (NB-Session-In)` and `File and Printer Sharing (SMB-In)`.



d. For each rule, right-click the rule, and then click `Enabled` checkbox and `Allow the connection` option. Click the "OK" button.



4. Ensure SMB2 is enabled

   SMB version 2 (SMB2) is required for file sharing and is typically enabled by default. The following command will ensure SMB2 is enabled and will have no effect if it is already enabled.

   Run this command from an Administrator PowerShell Terminal.

   Command lines

   ```
   Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
   SMB2 -Value 1 -Force
   ```

   If the command runs successfully, no results will be displayed in the PowerShell terminal.

5. Verify all SMB configuration options

   If you have completed all of the steps above and are still unable to use the SMB service, the following command will produce output that may be helpful in more exhaustive troubleshooting.

   Run this command from an Administrator PowerShell Terminal.

Command lines

```
Get-SMBServerConfiguration
```

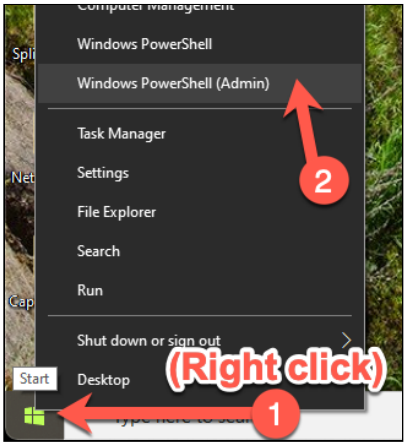
Notional results

```
PS C:\Users\sansforensics> Get-SMBServerConfiguration
AnnounceComment                   :
AnnounceServer                    : False
AsynchronousCredits               : 64
AuditSmb1Access                   : False
AutoDisconnectTimeout             : 15
AutoShareServer                   : True
AutoShareWorkstation              : True
CachedOpenLimit                   : 10
DurableHandleV2TimeoutInSeconds   : 180
EnableAuthenticateUserSharing     : True
EnableDownlevelTimewarp           : False
EnableForcedLogoff                : True
EnableLeasing                     : True
EnableMultiChannel                : True
EnableOplocks                     : True
EnableSecuritySignature           : False
EnableSMB1Protocol                : True
EnableSMB2Protocol                : True
EnableStrictNameChecking          : True
EncryptData                       : False
IrpStackSize                      : 15
KeepAliveTime                     : 2
MaxChannelPerSession              : 32
MaxMpxCount                       : 50
MaxSessionPerConnection           : 16384
MaxThreadsPerQueue                : 20
MaxWorkItems                      : 1
NullSessionPipes                  :
NullSessionShares                 :
OplockBreakWait                   : 35
PendingClientTimeoutInSeconds     : 120
RejectUnencryptedAccess           : True
RequireSecuritySignature          : False
ServerHidden                      : True
Smb2CreditsMax                    : 2048
Smb2CreditsMin                    : 128
SmbServerNameHardeningLevel       : 0
TreatHostAsStableStorage          : False
ValidateAliasNotCircular          : True
ValidateShareScope                : True
ValidateShareScopeNotAliased      : True
ValidateTargetName                : True
```

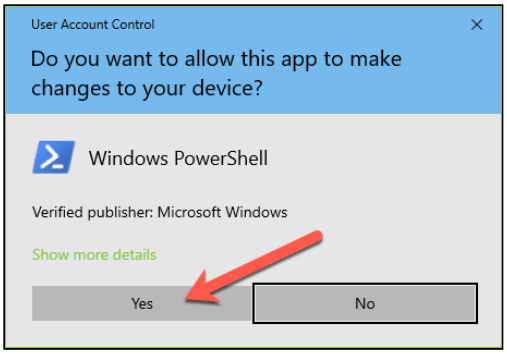
Running Administrator Terminal/Prompt

The steps in this section may require either an Administrator PowerShell Terminal or a Windows Command Prompt. To access these, use the following instructions.

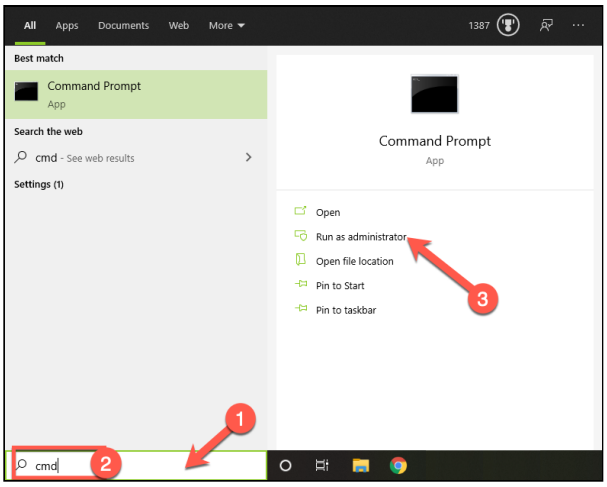
1. Administrator PowerShell Terminal
   a. Right click the Windows Start Icon on the bottom left of your Task Bar.
   b. Select Windows PowerShell (Admin) from the Menu.



   c. You may see a dialog requesting permission to make changes on your device. Click `Yes`.



2. Administrator Command Prompt
   a. Click the Windows search box or the Windows search icon (magnifying glass) on the bottom left of your Task Bar.
   b. Type `cmd` in the search box.
   c. Select `Run as Administrator`.



d. You may see a dialog requesting permission to make changes on your device. Click **`Yes`**.