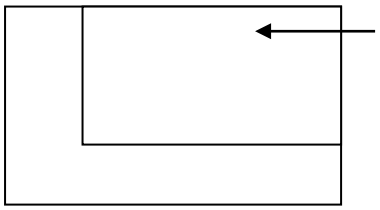
School of Computing
IT8003 Digital Forensics and Investigation

Practical 1A: VM Images Prep

Operating System Virtualization

A very simple explanation of a Virtual Machine (VM)

Most of our practical will be conducted within a virtual machine (VM). A virtual machine is like "a computer within a computer". You can start another operating system on your computer and run programs in that operating system while keeping your original operating system intact.



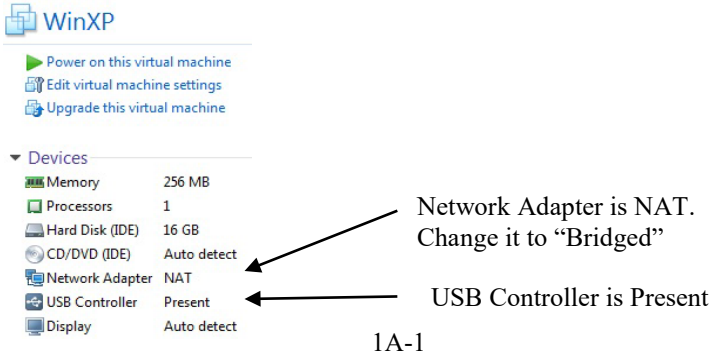
What can you do with Virtual Machines?

- Run multiple operating systems (Windows, Linux) on a single computer
- Discard changes to an operating system easily by creating snapshots. You can revert to a previous snapshot

We will be using VMware software in our practical. VMware Workstation Pro is a paid-software, while VMware Workstation Player is free for non-commercial, personal and home-use.

Exercise 1. Setting up your Windows image

1. Create a folder D:\DFI-*yourname,* eg D:\DFI-bernard
2. Go to My Computer. Go to C:\BaseImages (or D:\BaseImages). Copy the folder "Forensics" to D:\DFI-*yourname*" (eg after copying, you will have the folder D:\DFI-bernard\forensics).
3. Use VMware Workstation to open the "forensics" image in your DFI folder. Do not start it yet.



4. Check that you have a USB Controller listed under Devices for your "forensics" image (see image above).
5. If you do not have a USB Controller, do the following steps to add it:-
   a. Under Commands, click on Edit virtual machine settings.
   b. Under Hardware, click the Add button at the bottom.
   c. Select USB Controller and click Next. Click Finish. Click OK.

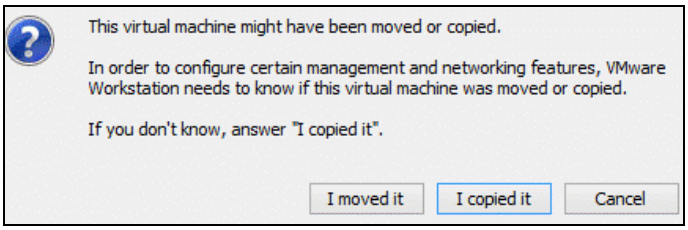
Adding a USB controller means you can access USB devices in your image.

6. Check that the Network Adapter is set to "**Bridged**" or **Network Address Translation [NAT]**.

Bridged networking means the virtual image is connected to the network using the Base PC's Ethernet adapter. It has access to other machines on the network and can be contacted by other machines on the network as if it were a physical computer on the network.

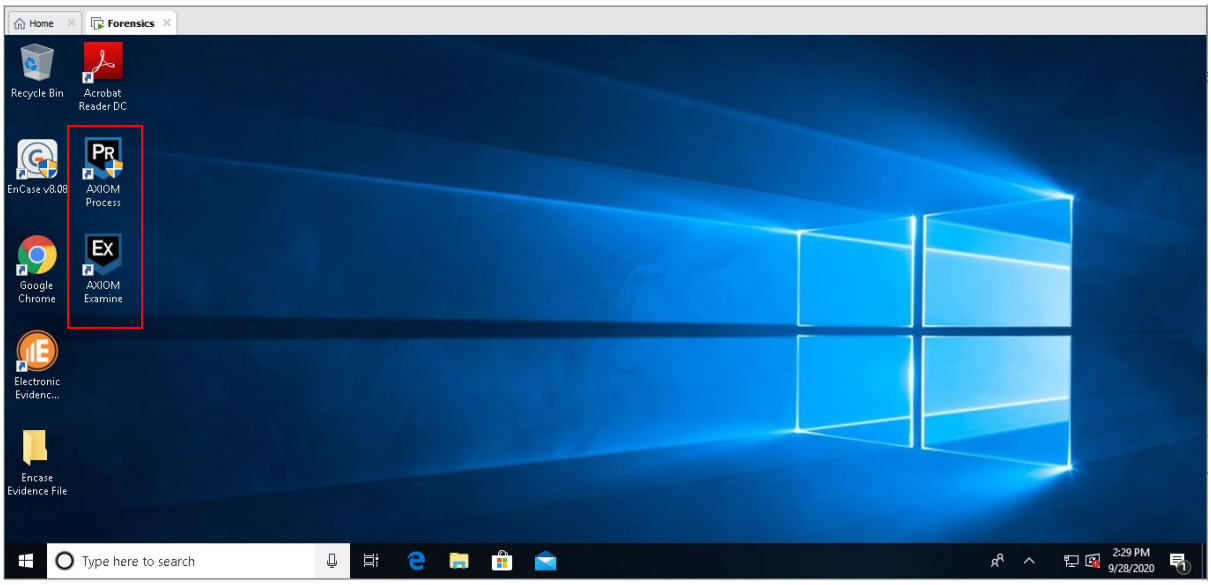
NAT networking means the virtual image is in a private network on the Base PC (or host system).

7. Start up the "forensics" image
8. Select "I copied it" when asked.

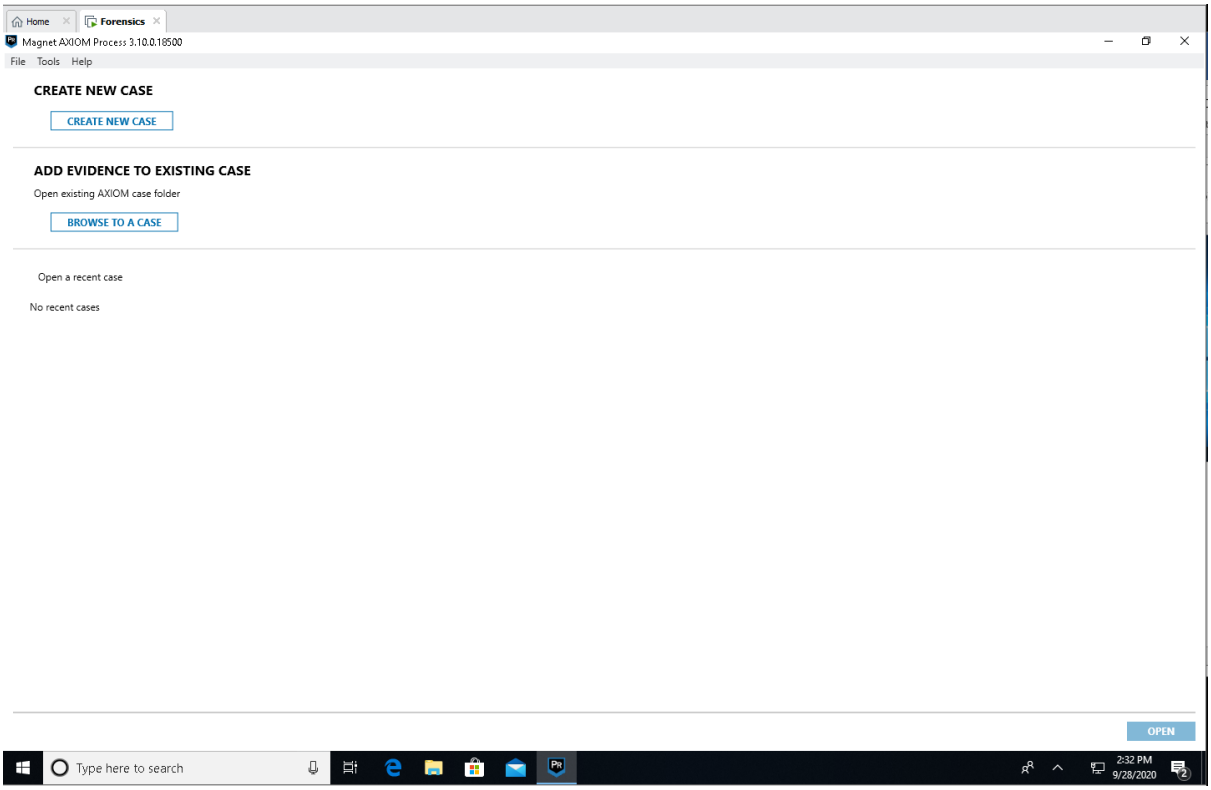


9. When the image has started up, you may want to install/update VMware Tools if it is not installed yet. Go to VM menu and choose Install VMware Tools or Update VMware Tools.
10. To adjust the size of the screen of the VM image, **right-click** on the desktop and choose **Properties**. Click on the **Settings** tab and select a Screen resolution that you prefer.

11. Check the software "**AXIOM Process**" and "**AXIOM Examine**" is available in the virtual machine.



12. Run "**AXIOM Process**"
13. Ensure that "**AXIOM Process**" is working properly



-- End --