Creating new .qcow2 file for the disk image

1) Run the ansible script to create a windows VM using KVM. The VM would boot up from the CD and install Windows 10. The --ask-become-pass is used to run the commands as root to prevent errors.
ansible-playbook playbook_createWin10.yaml --ask-become-pass

   The script below creates a new VM with 2 CD rom 1 for the drive 1 for the bootable disk :

```
- name: use virt-install to create VM
  become: yes
  command: >
    virt-install
    --name {{ vm_name }}
    --vcpus={{vcpus}}
    --memory {{ vm_memory }}
    --os-variant {{ vm_os_variant }}
    --disk pool={{ pool_name }},size=60,bus=scsi,format=qcow2
    --disk /data1/libvirt/images/en-us_windows_10_consumer_editions_version_21h2_updated_sep_2022_x64_dvd_bdec96d8.iso,device=cdrom
    --disk /data1/libvirt/images/virtio-win-0.1.240.iso,device=cdrom
    --network bridge={{ vm_network_bridge }},model=virtio
    --vnc
    --boot hd,cdrom,menu=on
```

Fig 1. The virt-install command to create the initial analysis VM

2) When the VM boots up, set the time zone to the local time zone and click on next to continue.

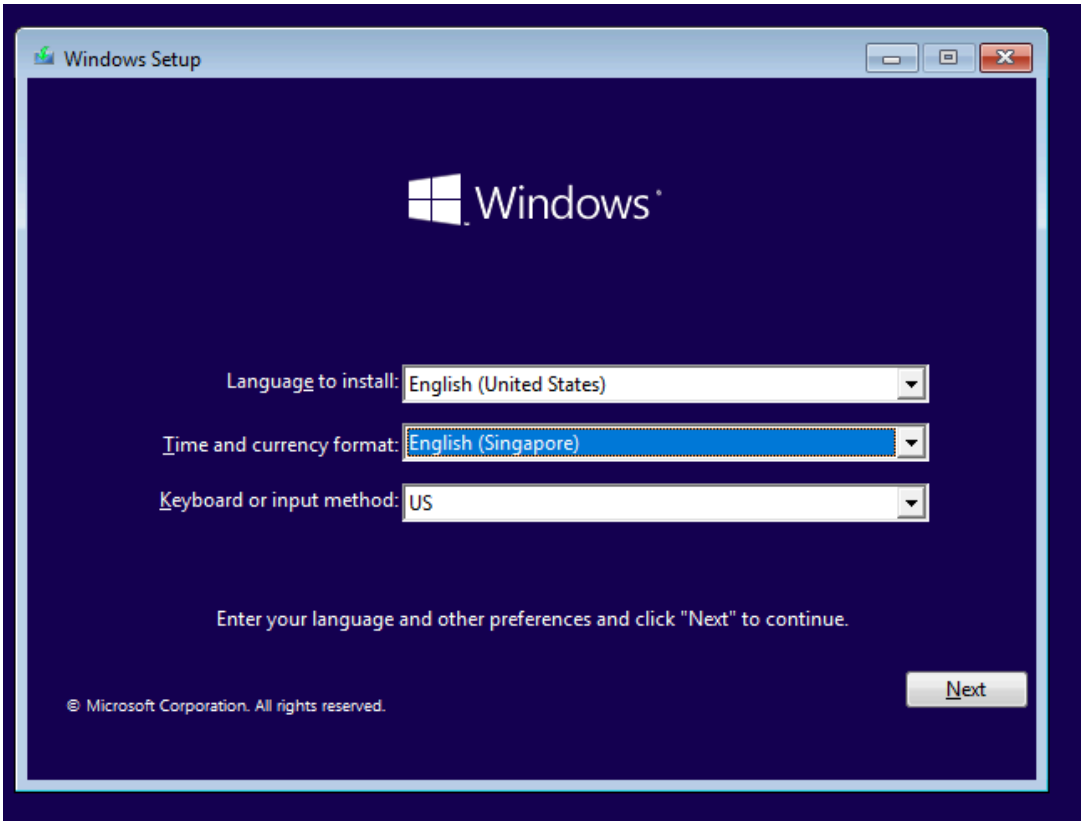

Fig 2. Set the Time and currency format to English (Singapore)

Then, click on Install Now to install windows 10:

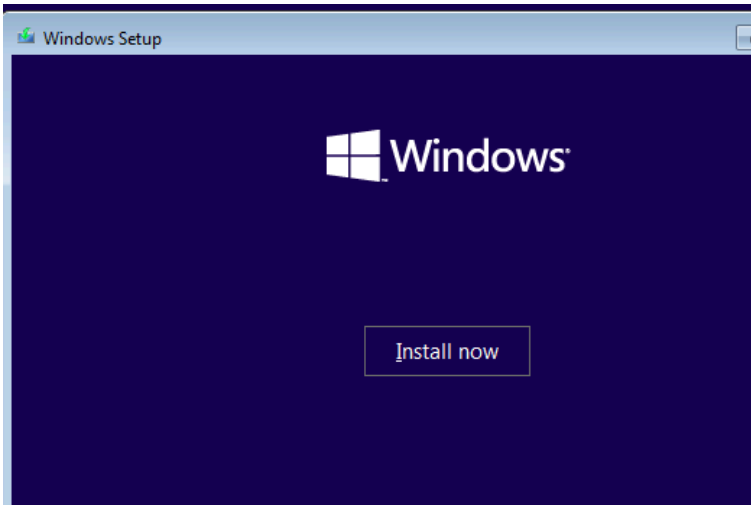

Fig 3. Install now button

Click on I don’t have a product key to continue:

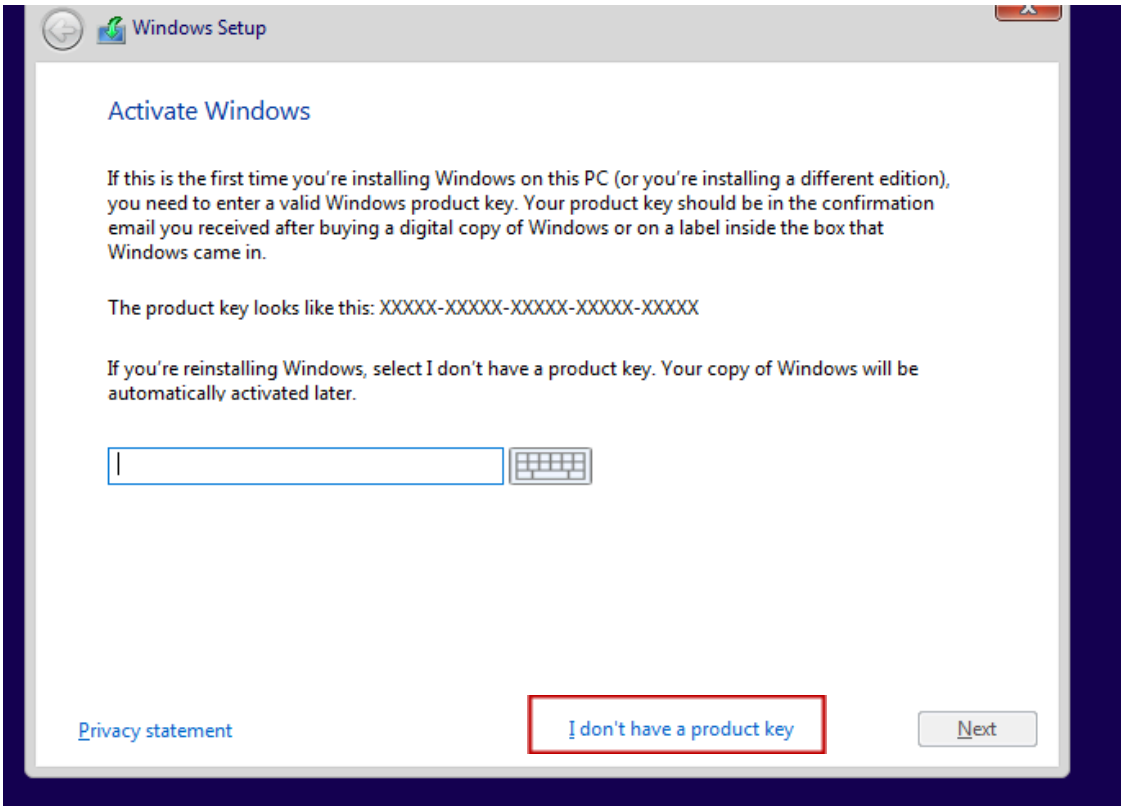

Fig 4. Click on I don’t have a product key.

Select Windows 10 Pro as the OS to install and Accept the license terms:

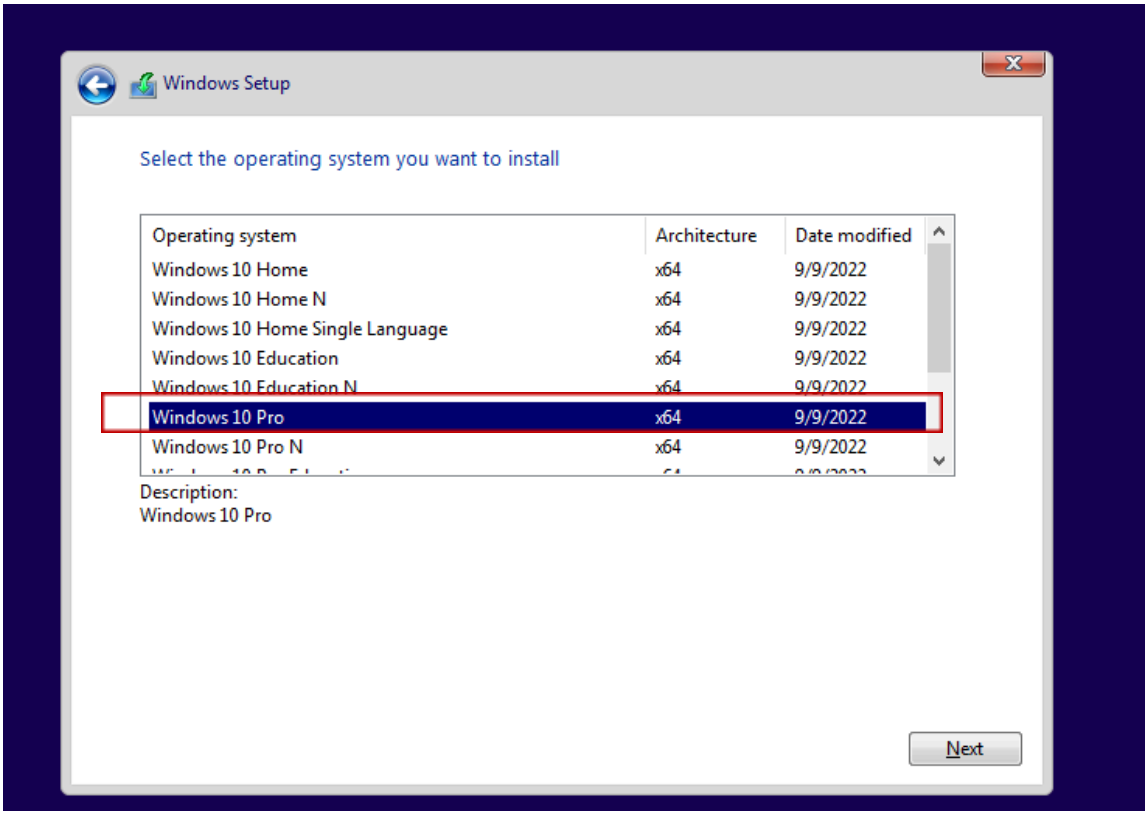

Fig 5. Select Windows 10 Pro

Next, Click on Custom and the hard disk will not be visible as the driver needs to be installed into the disk:

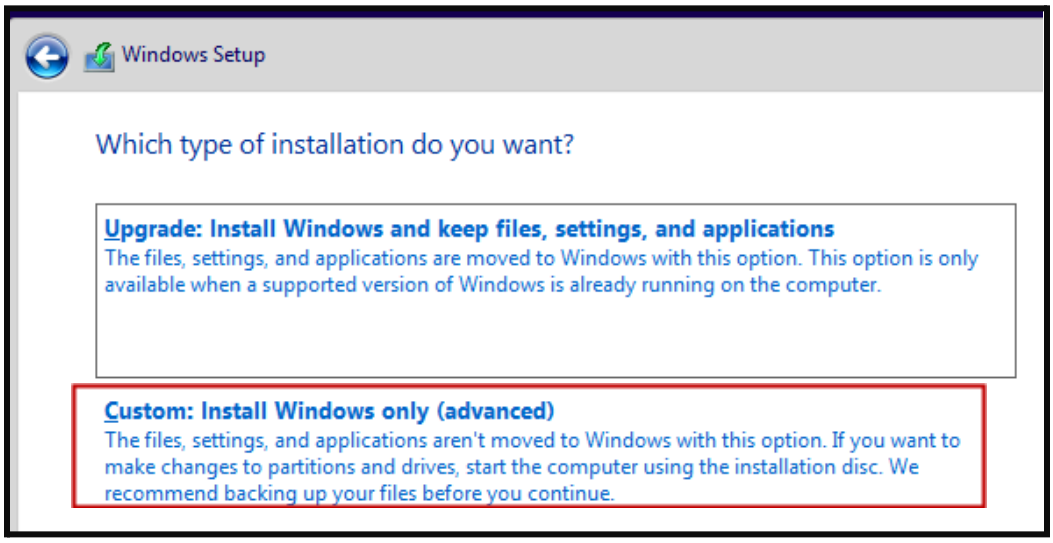

Fig 6. Click on Custom to install the Virtio Drivers

Click on Load Driver and then browse and navigate to the Virtio iso file.

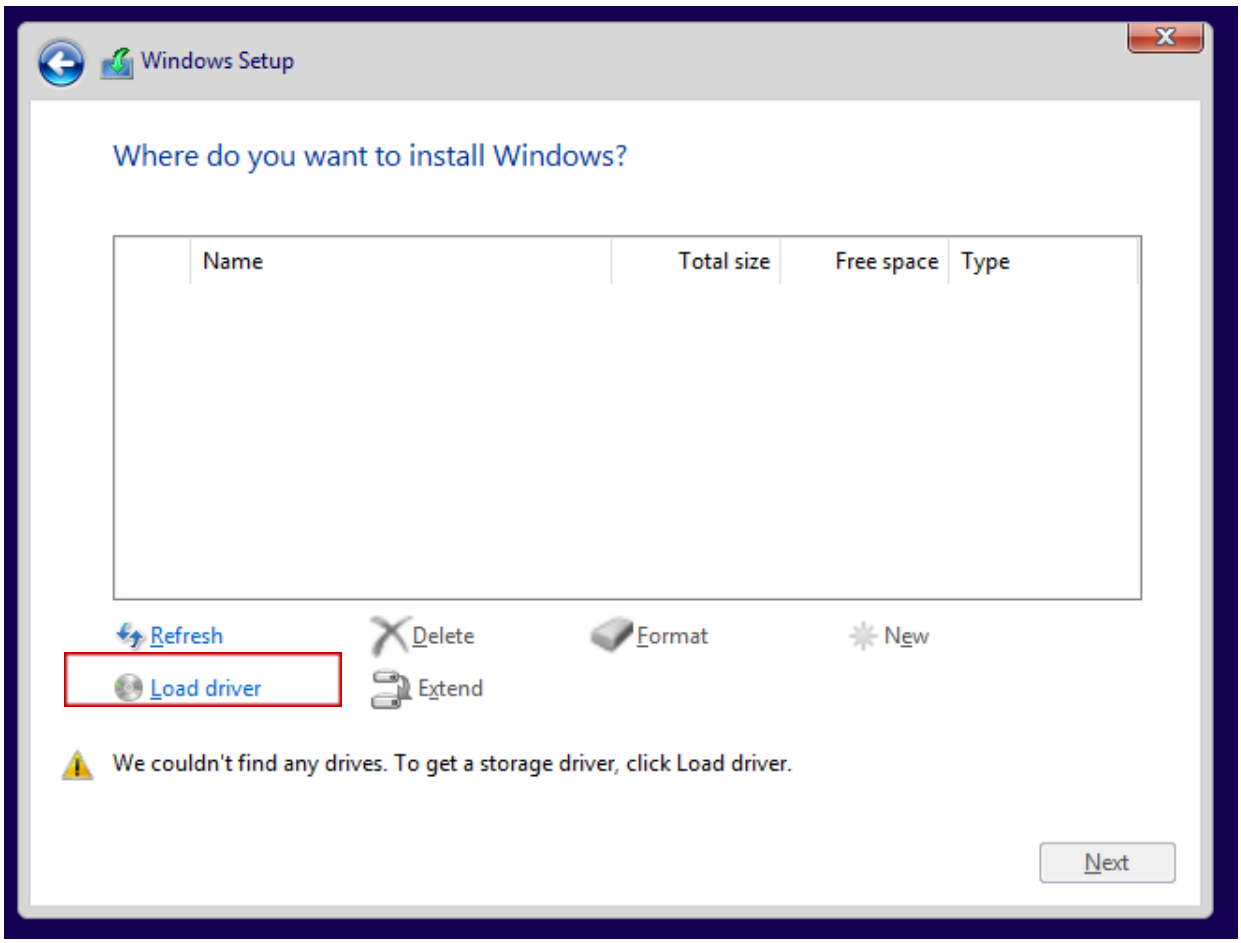

Fig 7. Select Load driver to install the Virtio Drivers

Click on Browse

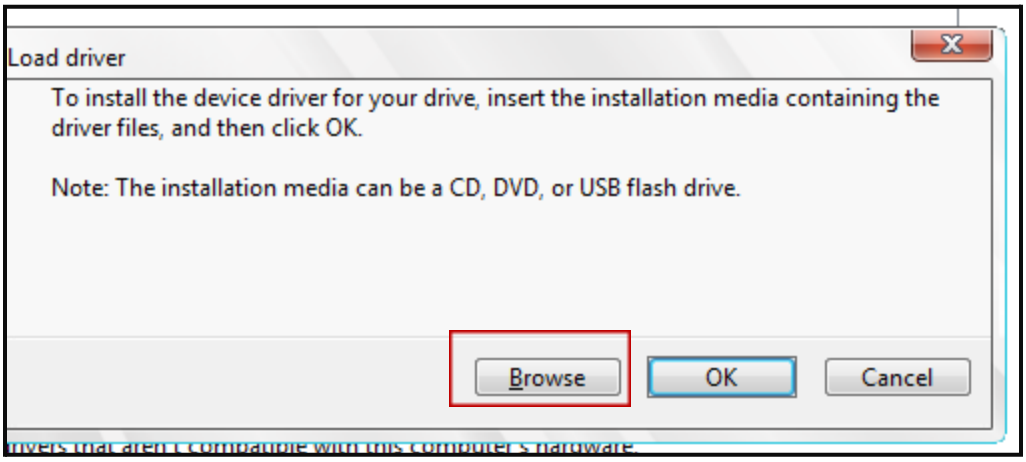

Fig 8. Select Browse

Click on the Virtio ISO file

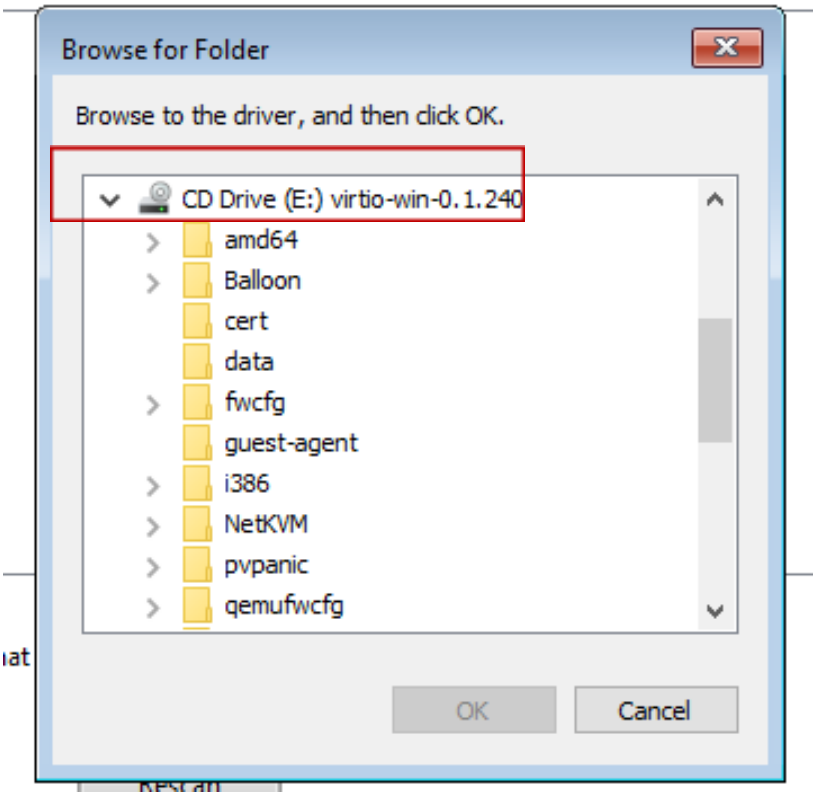

Fig 9. Select Virtio ISO disk

Scroll down to viostor -> w10 -> amd64. Click on Ok to continue

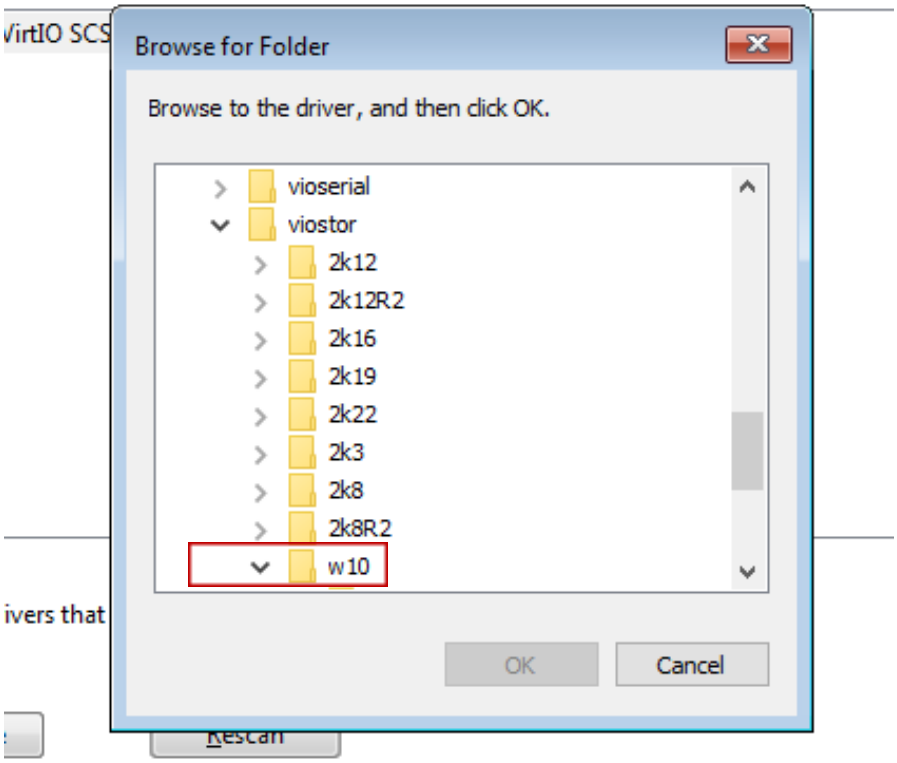

Fig 10. Select the w10 folder under the viostor folder

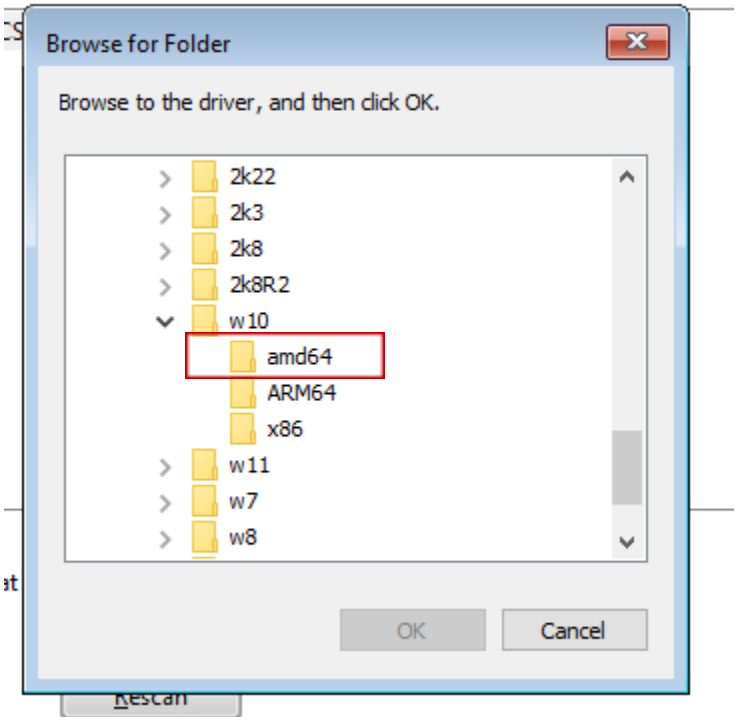

Fig 11. Select the amd64 folder

Selected driver viostor will appear as shown below. Click on Next to fully install the driver:

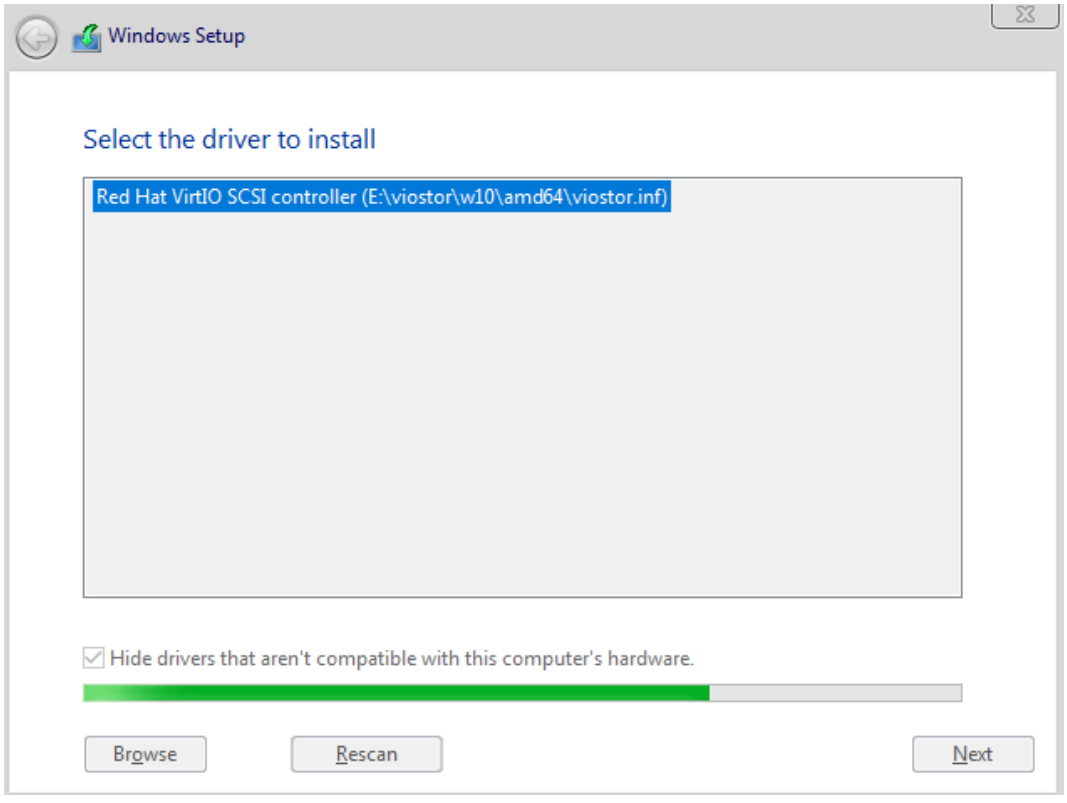

Fig 12. Select the driver for the hard disk.

3) The hard disk should now be visible. Click on Load Driver to install the driver for NetKVM for the network adapter to work:

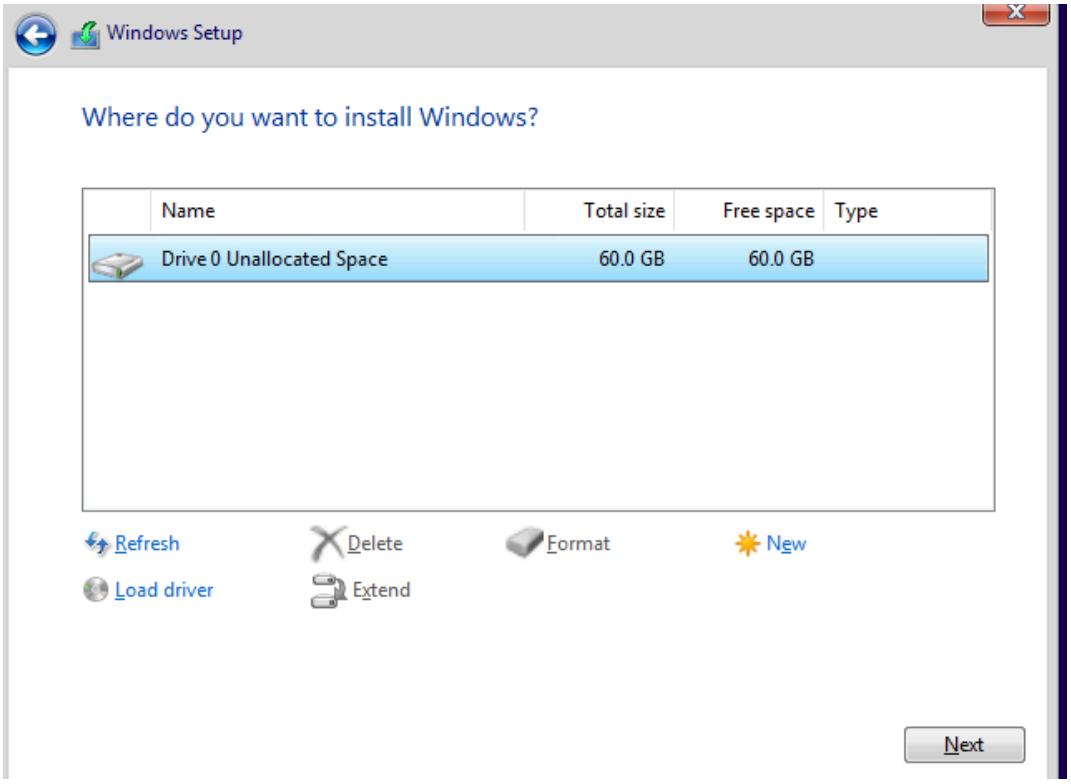

Fig 13. The hard disk of the kvm Virtual machine

4) Select driver netkvm for network communication. To get to this page click on Custom -> Install Drivers -> Browse -> Select the virtio disk -> select NetKVM folder -> w10 -> amd64 -> netkvm.inf

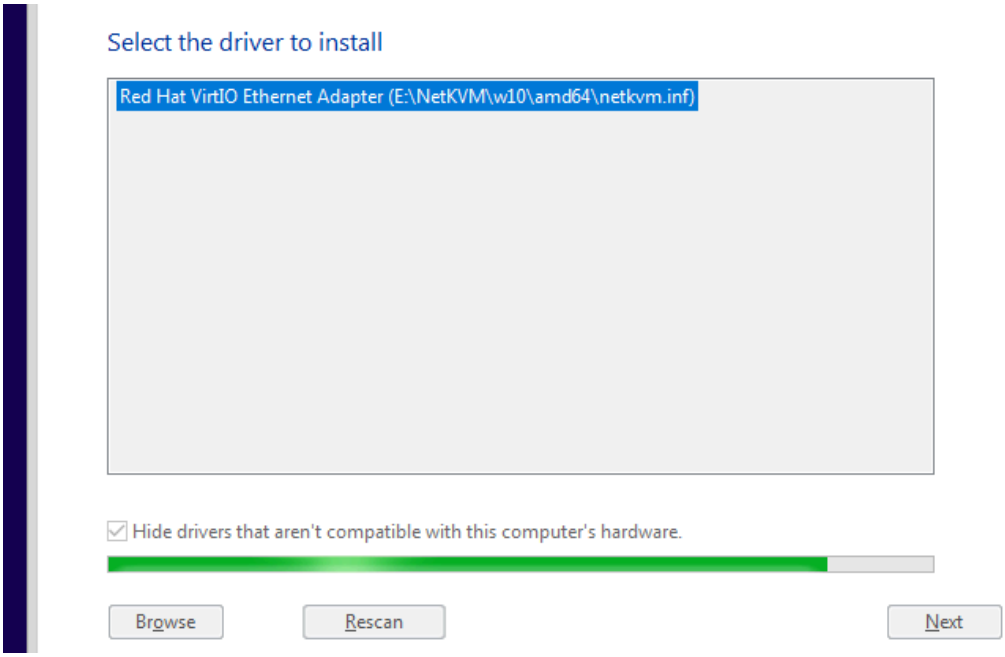

Fig 14. Select the driver for the network adapter

Upon returning to this page, click on Next to begin the installation of Windows 10 OS:

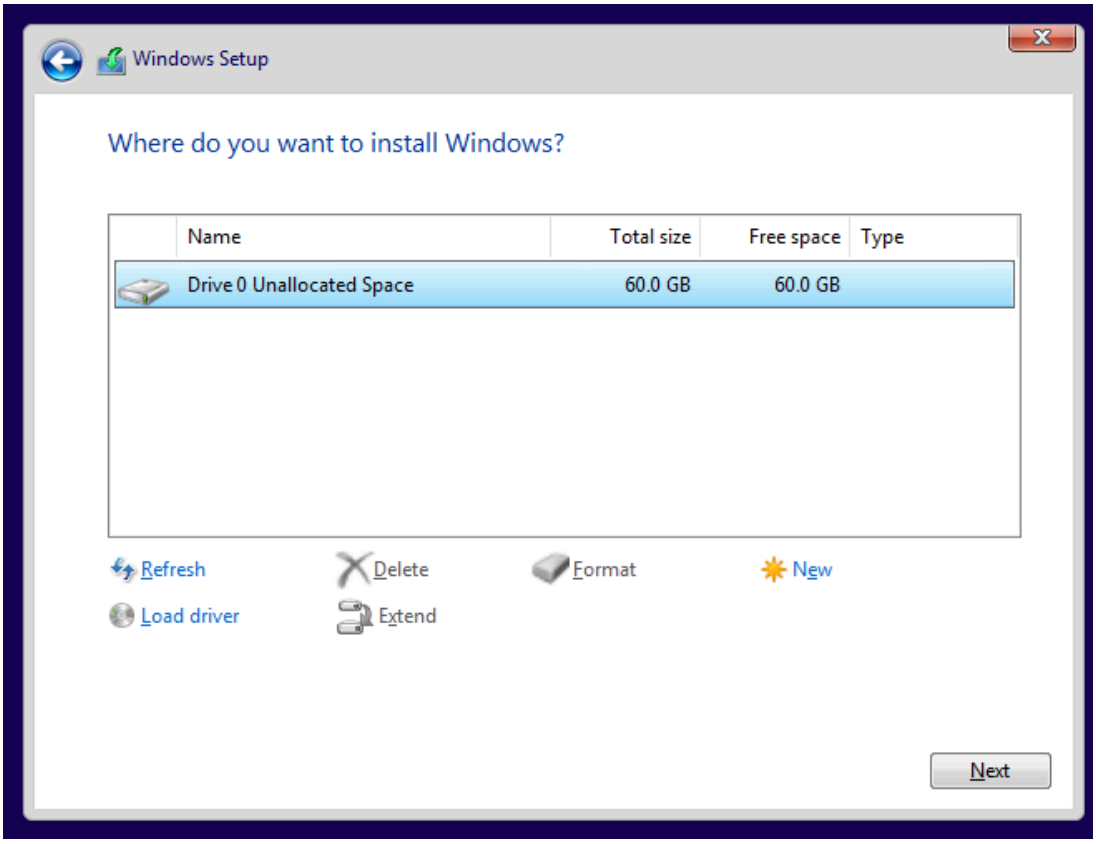

Fig 15. Click on Next to Continue

The installation of the OS should begin:

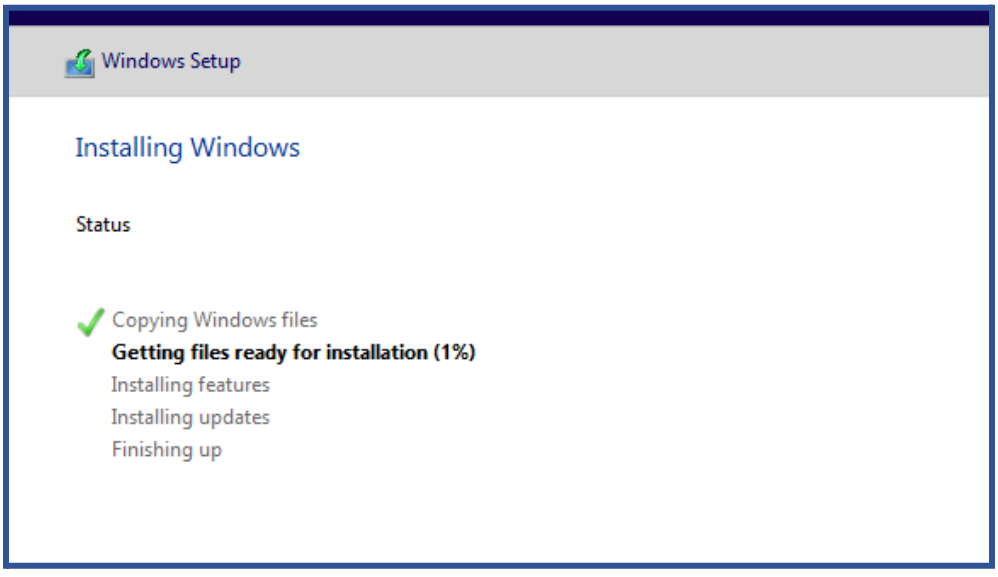

Fig 16. The Installing Windows Page

5) During Installation Process, upon reaching this page continue on the prompts until the screen asks for a Username.

Click on Continue with limited setup

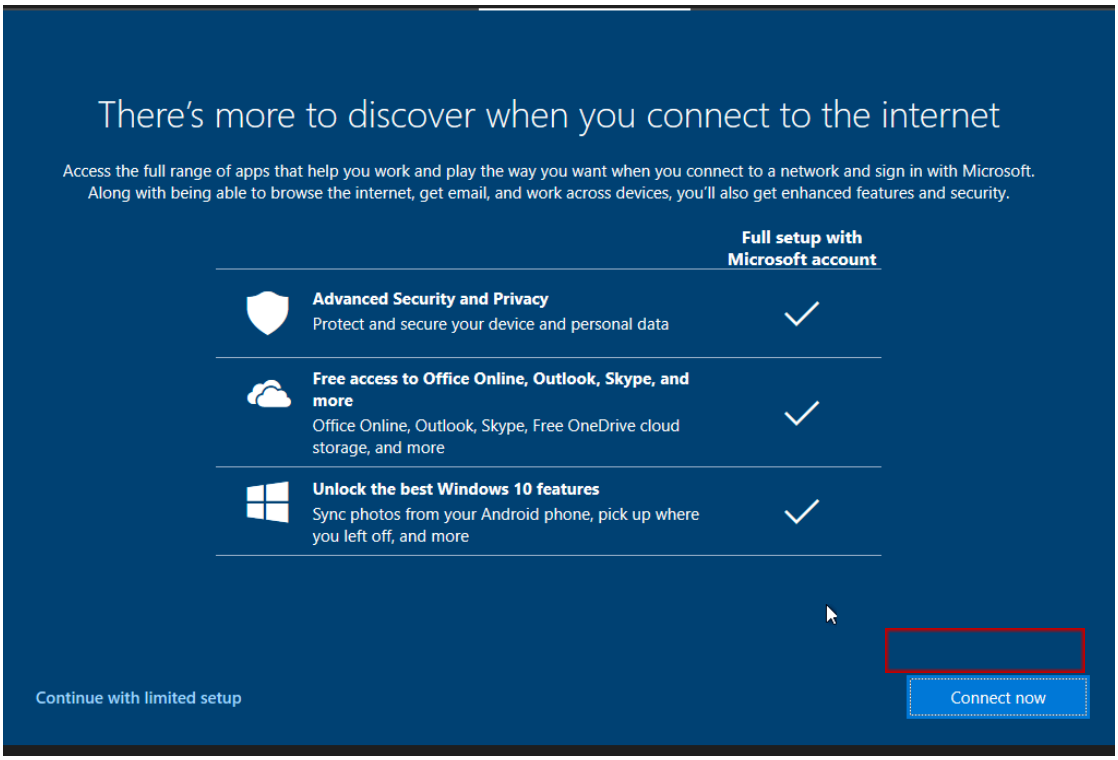

Fig 17. Continue with limited Setup

6) Enter the username to student18 as shown below:

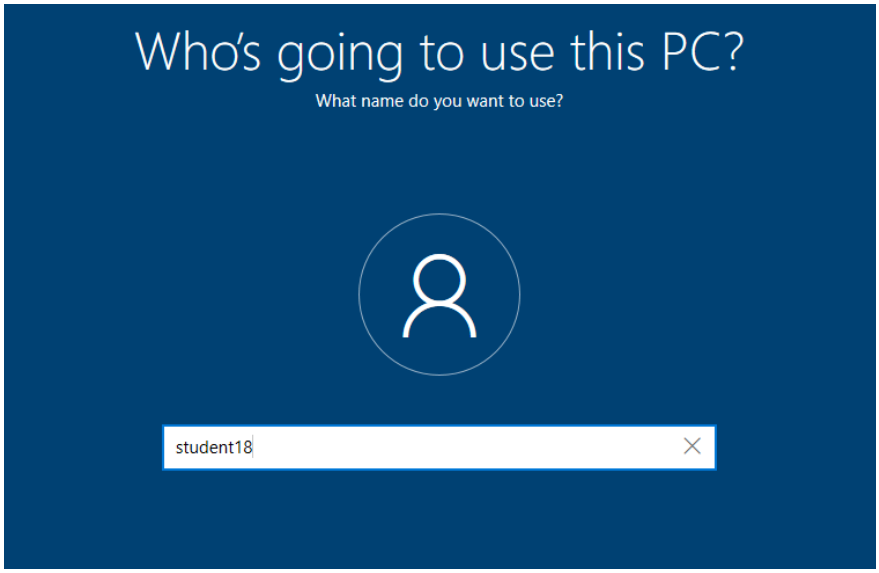

Fig 18. Set the username to student18

7) Set the password to toor

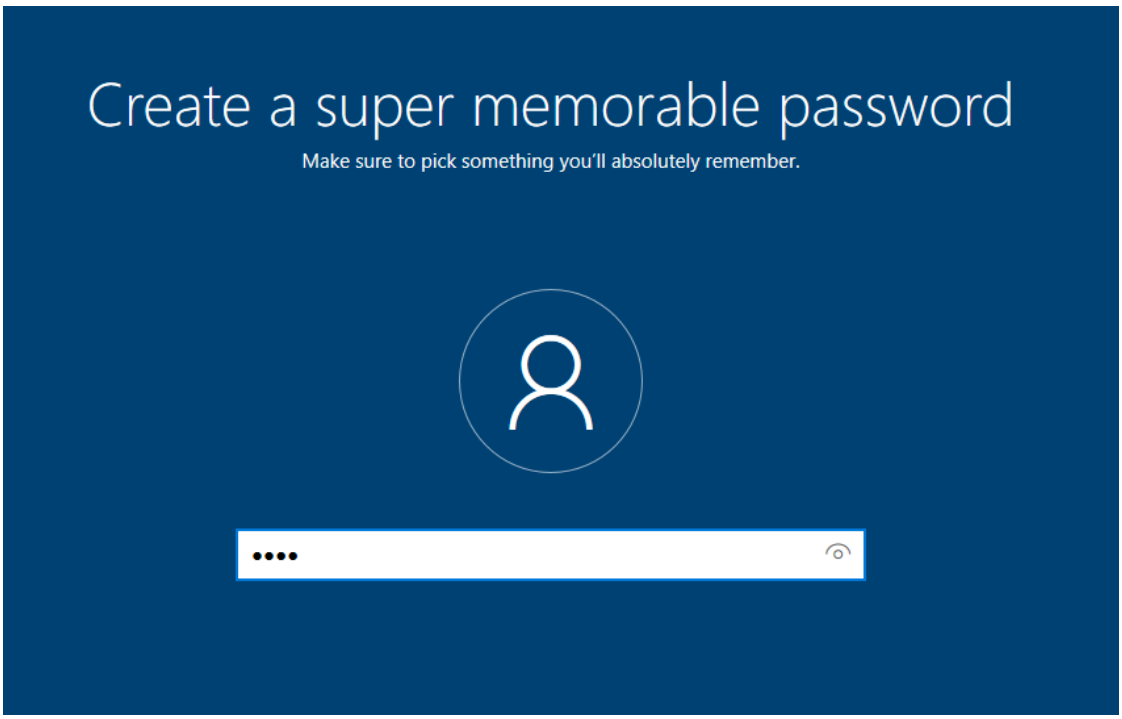

Fig 19. Set the password for student18

8) Disable all settings below to prevent background processes for analysis. Click on Accept to proceed:

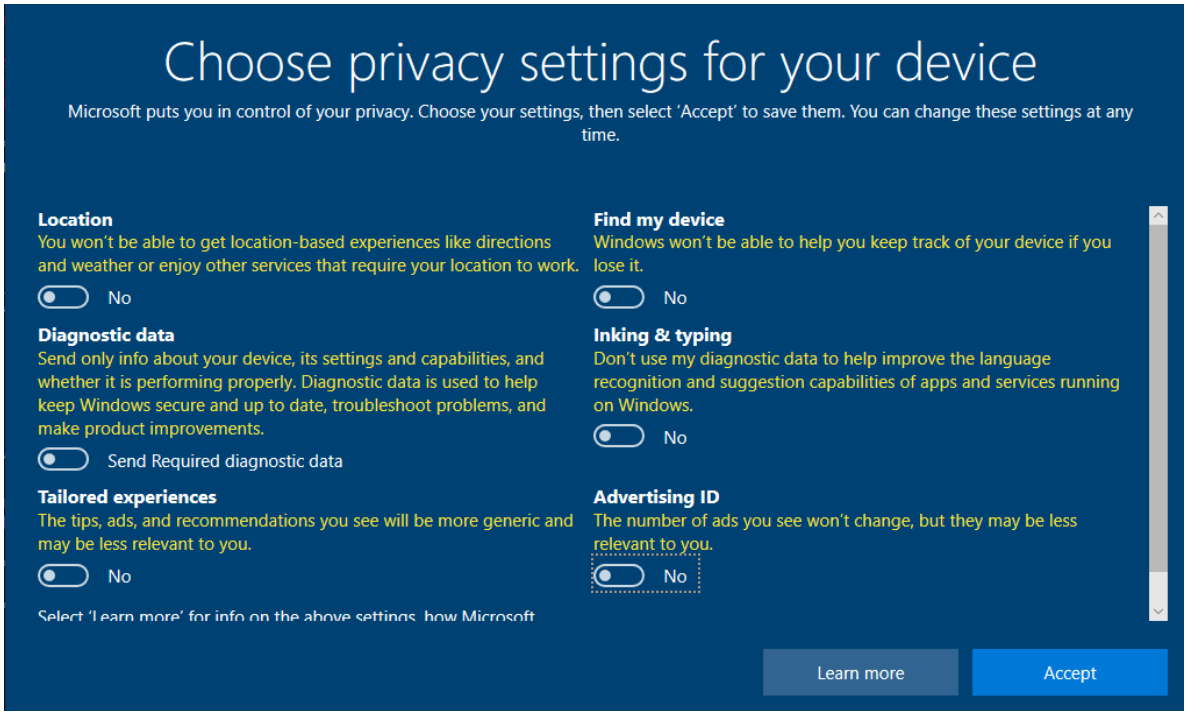

Fig 20. Turn off additional settings

9) The final step for the installation will take place if no errors:

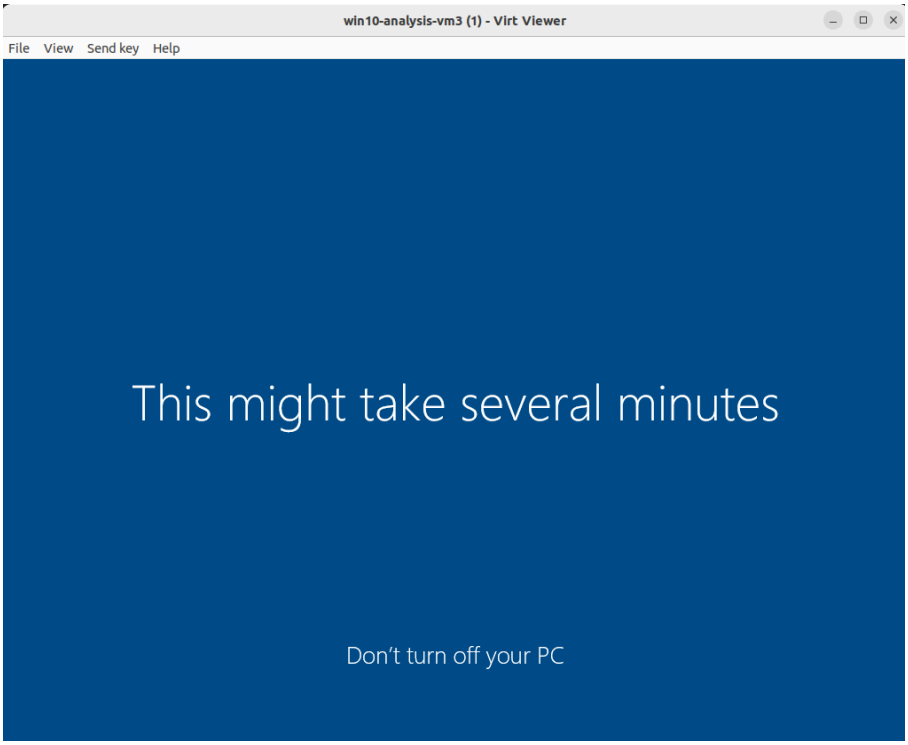

Fig 21. Windows 10 Installation in Progress

10) Once the OS has finished installing, Install the required software beginning with python 3.10:

Create a python server on the Ubuntu Virtual machine using the command below:
python3 -m http.server 3000

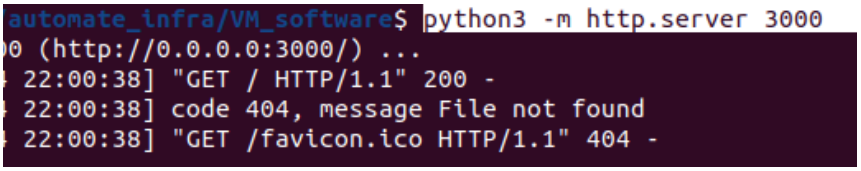

Fig 22. Python server on Ubuntu virtual machine

Run the command in the same directory as the installed software. Open up the web browser on the Analysis machine in KVM and go the URL for the python http server to check if the software installers are visible (http://192.168.100.1:3000).

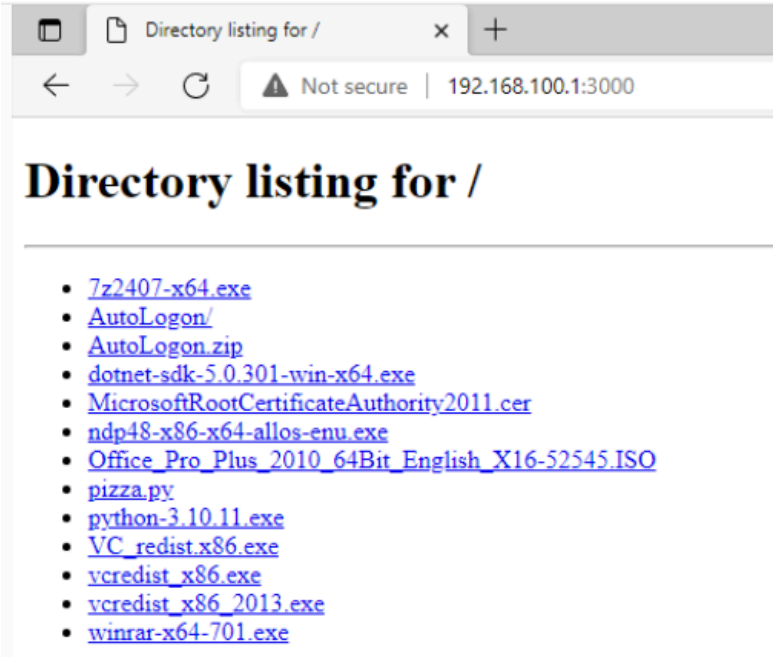

Fig 23. Python server on Ubuntu virtual machine with necessary software to install on KVM VM

Download the software files from the python HTTP server and begin installing the software beginning with python.

Install python 3.6 (32 bit) for the CAPE server to communicate with Analysis Machine

Python 3.6 or above 32-bit (CAPE Agent.py requires 32 bit python to run)

Fig 24. Python Installation Page in KVM virtual machine

Next Install the remaining software listed below:

- python 3.10.11(32-bit)
- Microsoft Root Certificate 2011
- Install Visual C++ (2012, 2013, 2015-2019)
- 7z
- WinRAR
- Office 2010

Install certificate in this directory:

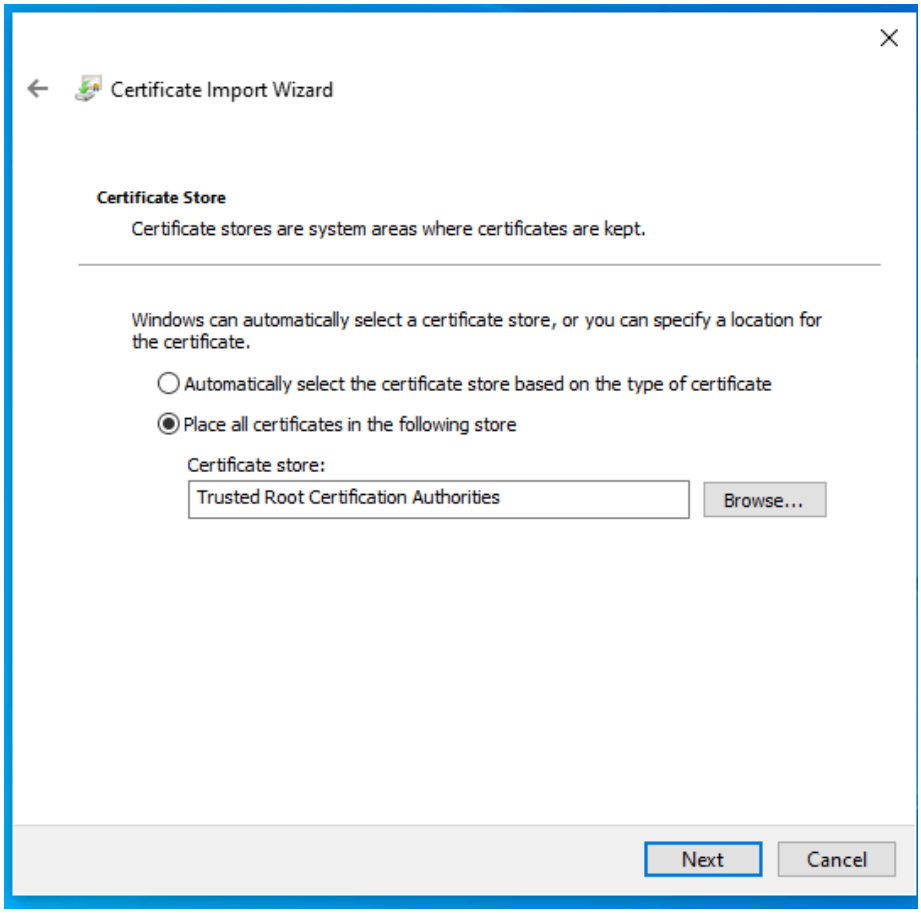

Fig 25. Installing the Windows Certificate.

To install Word2010 download the ISO file first and transfer to the analysis machine using the python server hosted on the CAPE host machine. Click on the ISO file to mount the file and click on setup.exe to install Office 2010:

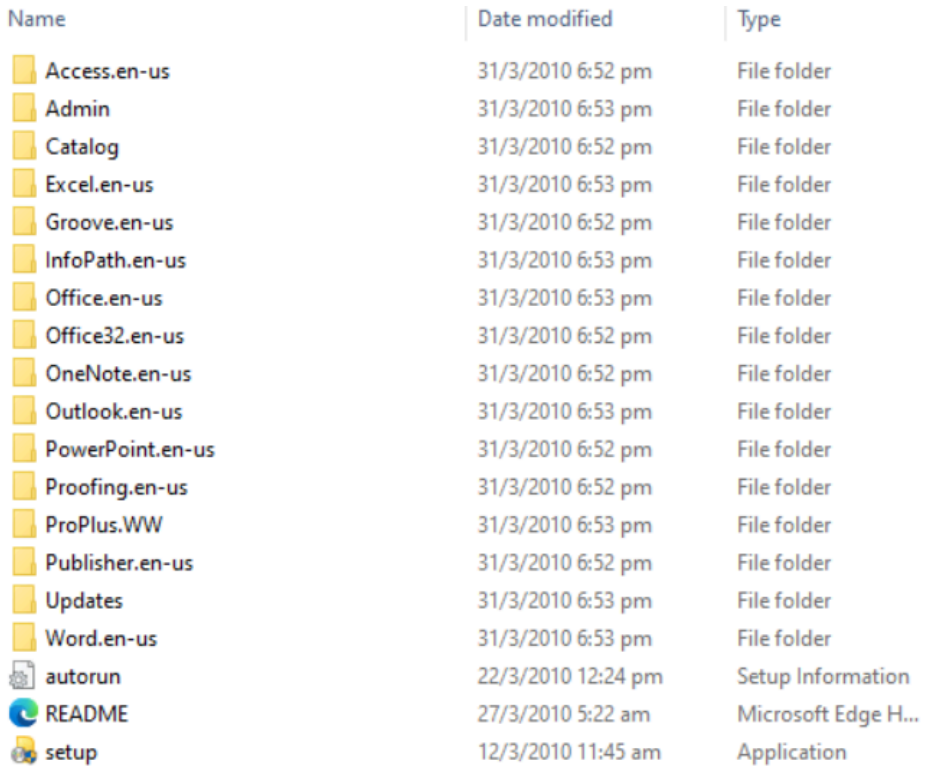

Fig 26. Image of Office2010 ISO files for installation office 2010

11) After installing Office 2010, disable Windows firewall and windows defender in the analysis machine. Open Windows defender firewall and click on Advanced settings

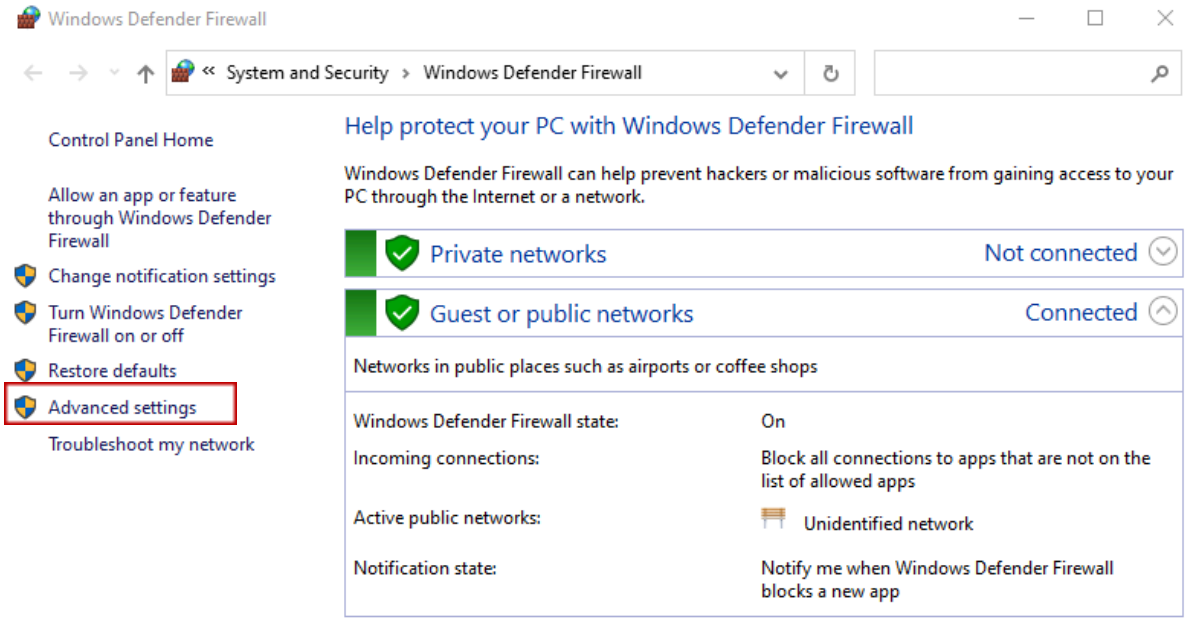

Fig 27. Click on Advanced settings in Windows Defender Firewall in Control Panel

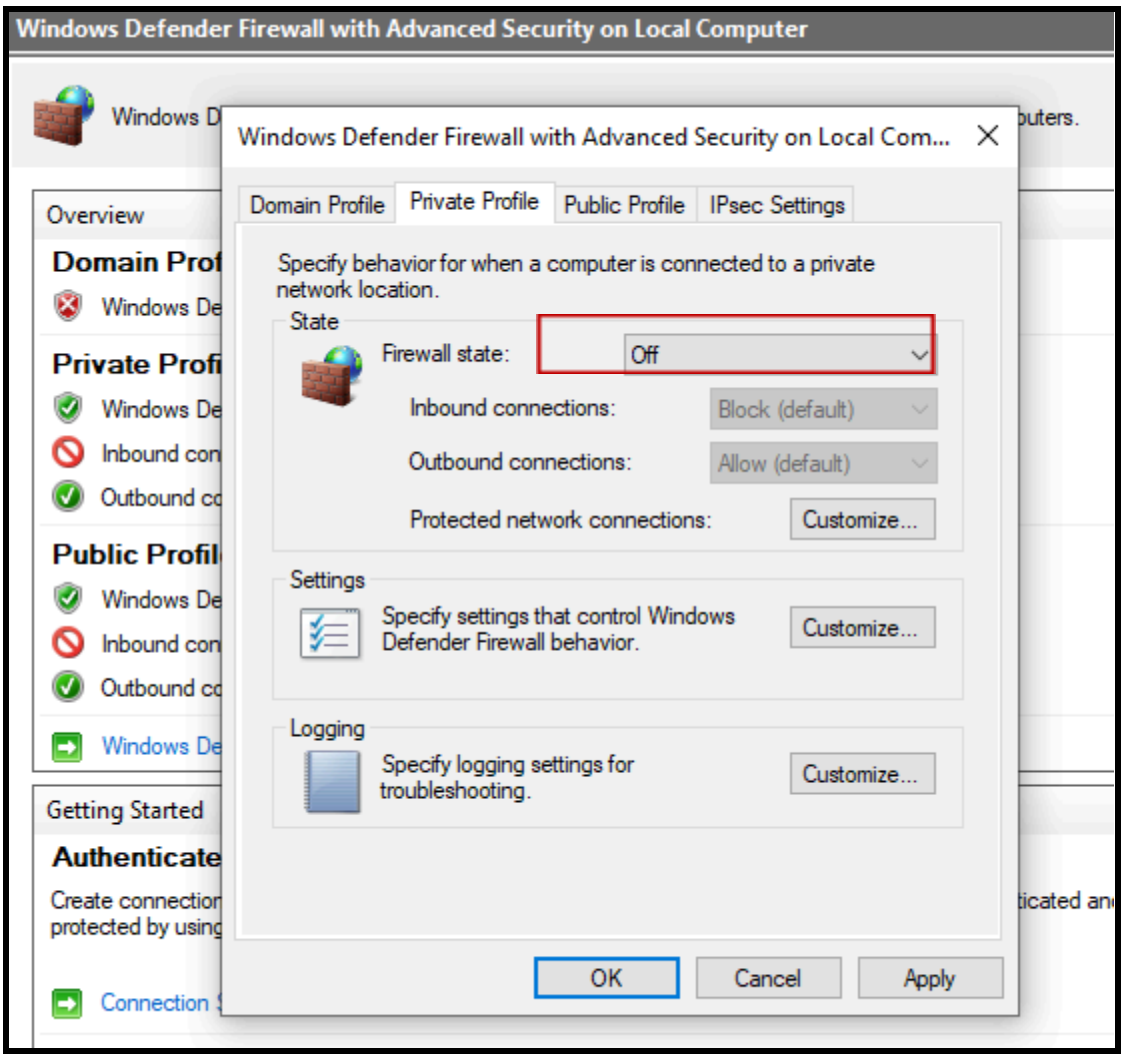

Fig 28. Set the Firwall State to off for Domain, Private and Public Profile

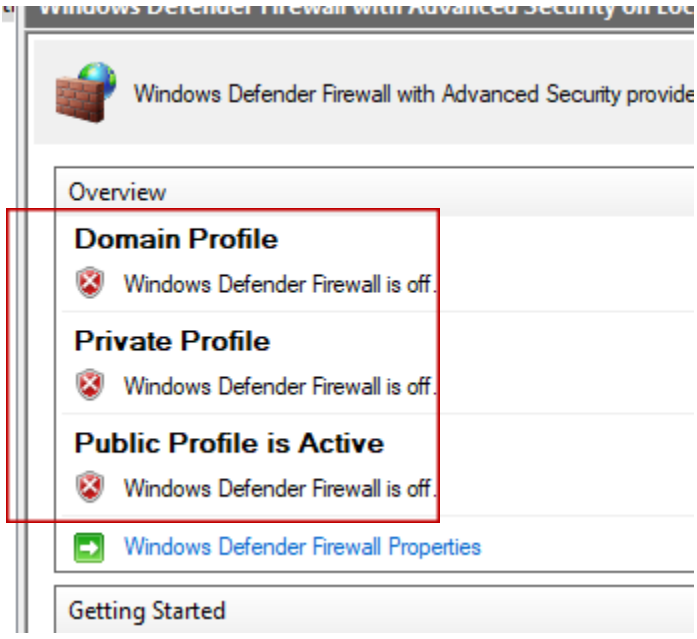

Fig 29. Set Windows Defender Firewall to off for Public, Private and Domain Profile.

12) Disable windows defender in settings. Turn off all settings listed below:

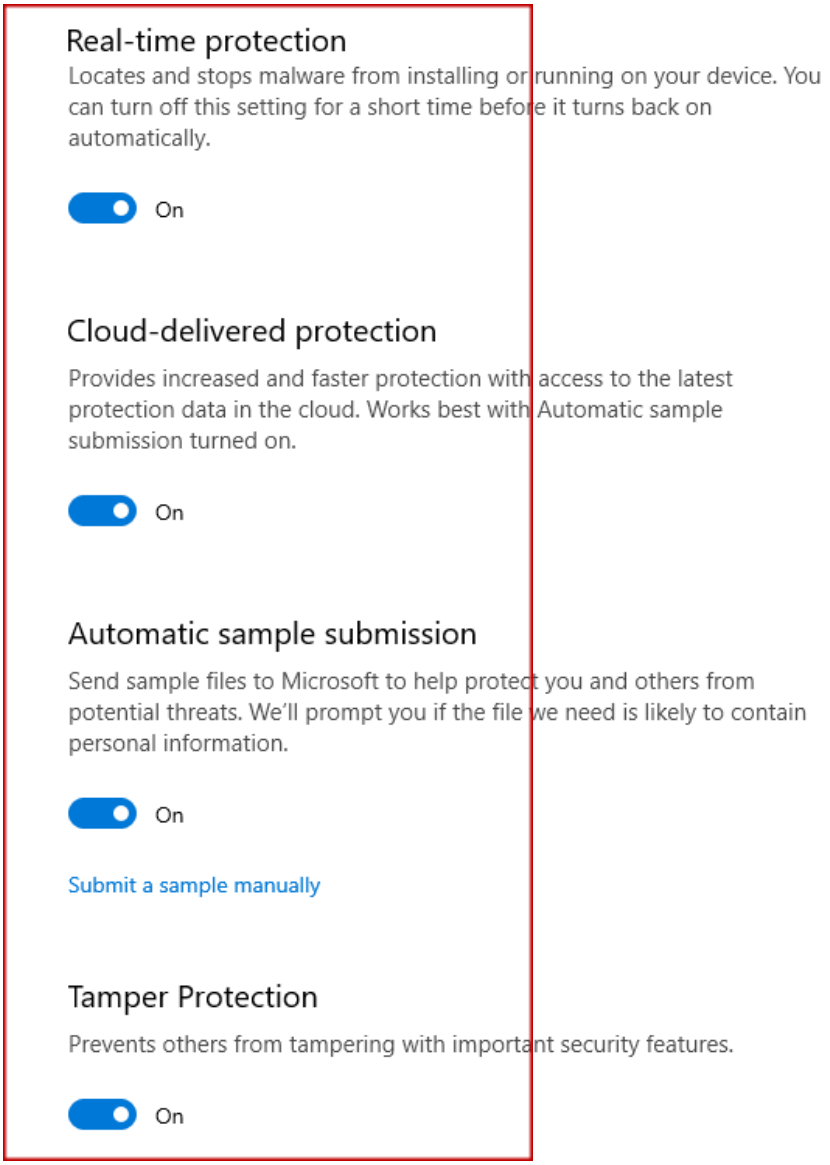

Fig 30. List of Windows Defender settings to disable.

13) Click on Windows security Browser and click on Reputation-Based protection. Disable smart screen by turning off all settings below:

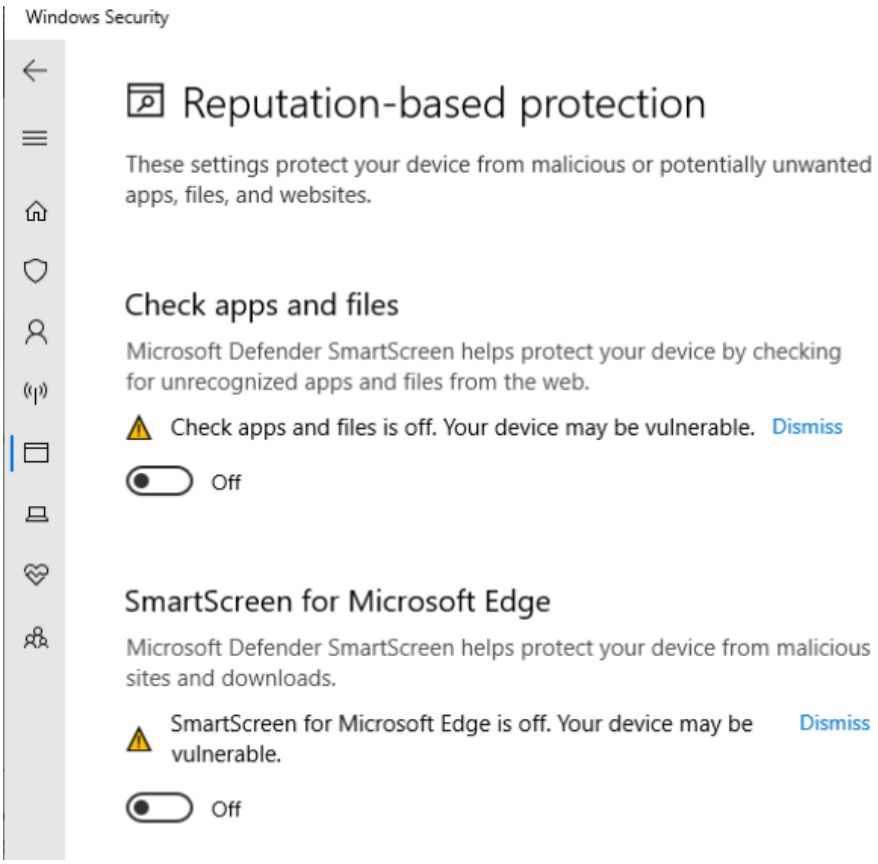

Fig 31. Disable Reputation-based protection to prevent interfering with the analysis

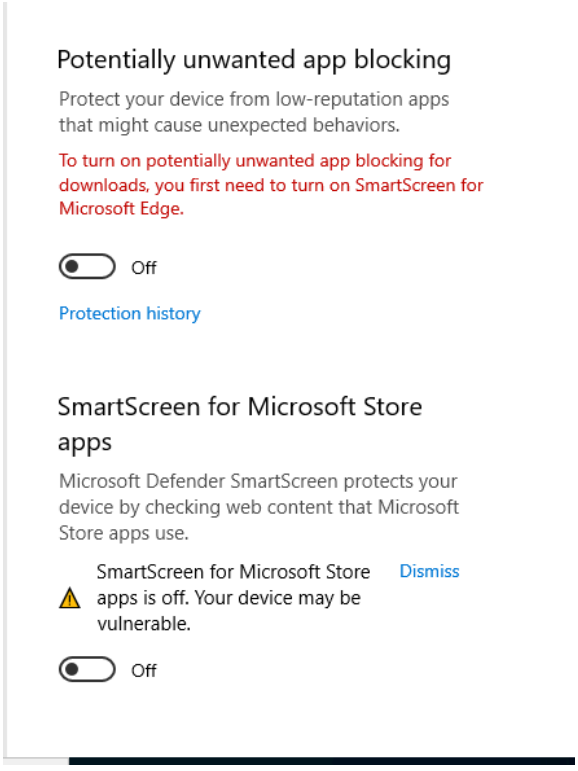

Fig 32. Disable SmartScreen settings for Microsoft store.

14) Next, Disable Windows Defender Real-Time monitoring in Registry. Open regedit and go to Windows Defender as shown below:

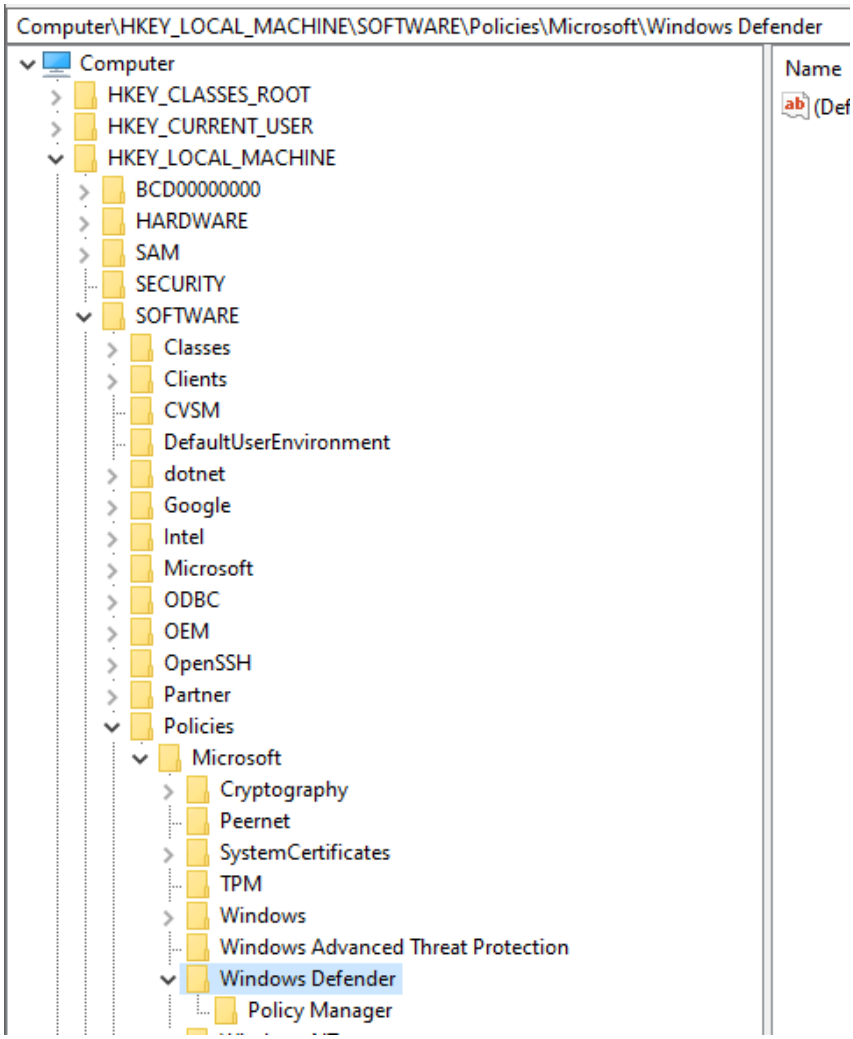

Fig 33. Windows Defender in Registry.

15) Right-click on Windows Defender and create a new key Real-Time Protection. Click on Real-time Protection and add a new DWORD key. Rename to DisableRealTimeMonitoring and set the value to 1.

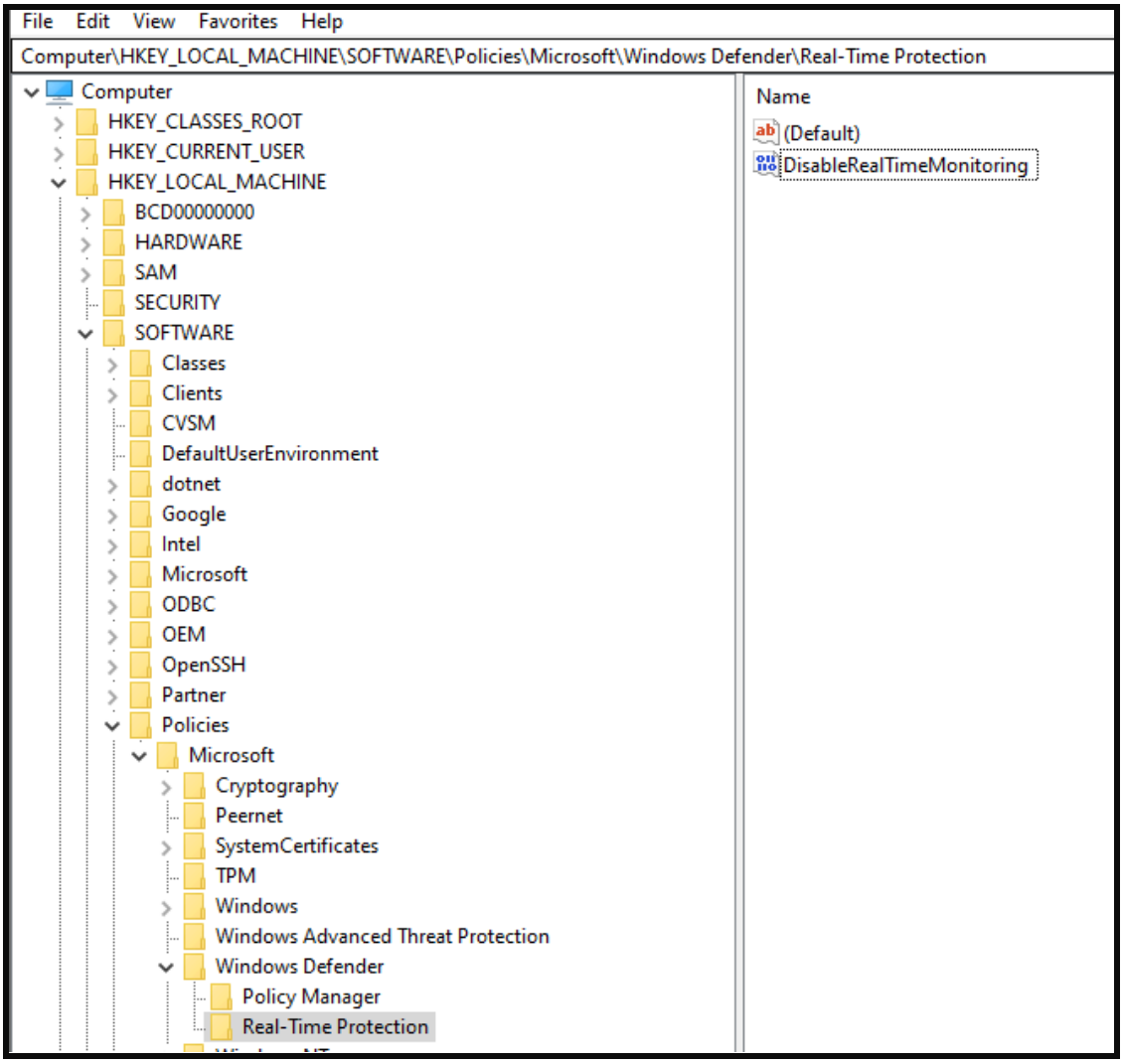

Fig 34. Real-TimeProtection key with value DisableRealTimeMonitoring.

16) Disable Smart Screen using Group Policy. Go to the policy Computer Configuration > Administrative Templates > Windows Components > File Explorer. Right-click on Configure Windows Defender SmartScreen policy and select Edit and select Disable

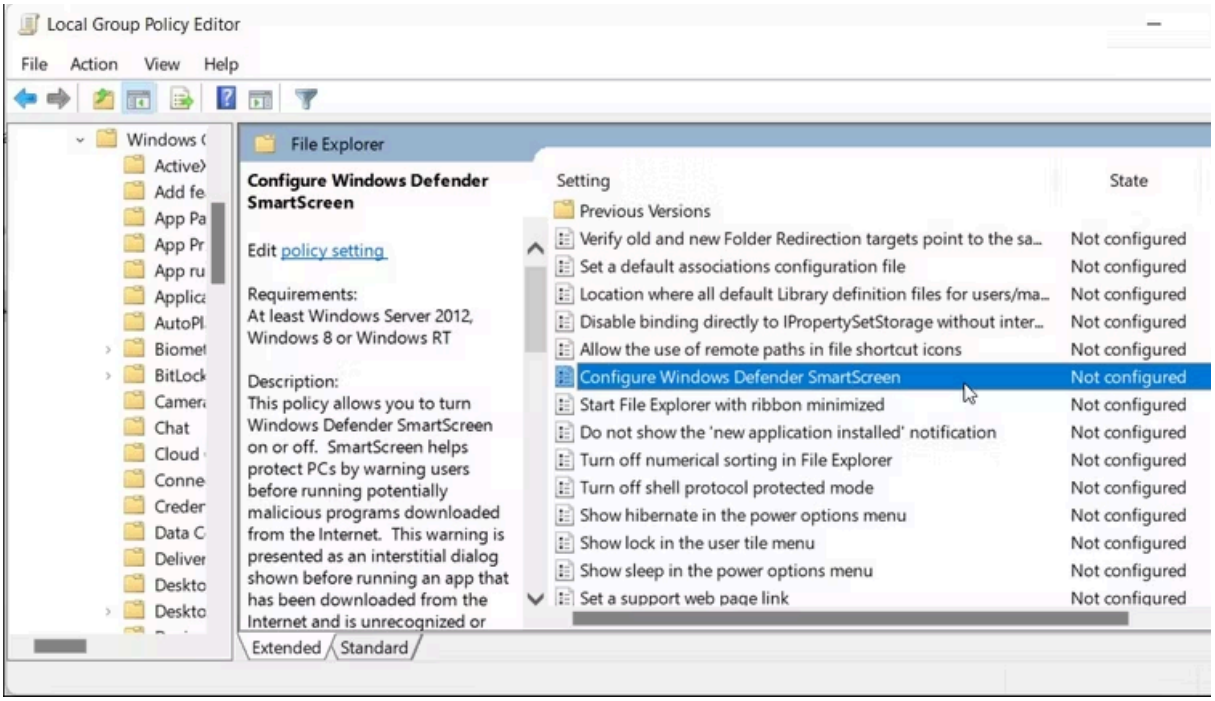

Fig 35. Policy for Windows Defender SmartScreen

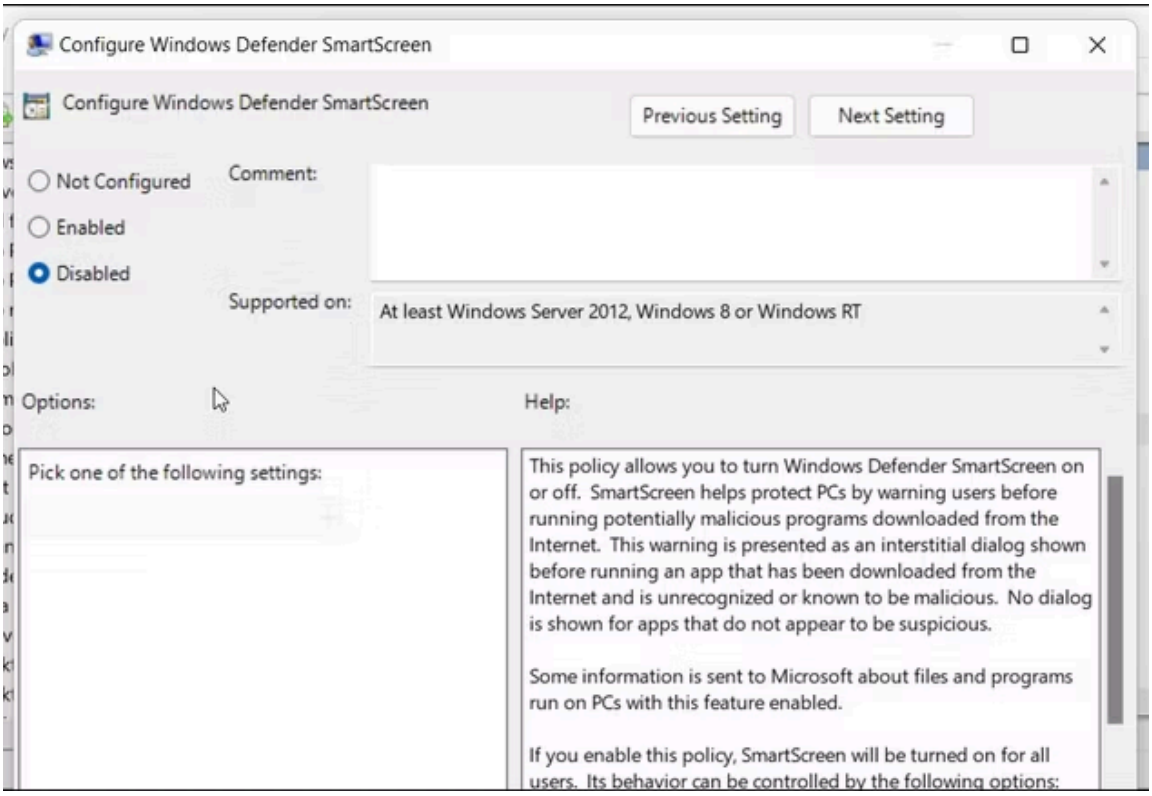

Fig 36. Set Window Defender SmartScreen Policy to Disabled

17) Disable Microsoft Defender (anti-virus). Open the Group Policy editor then navigate to Computer Configuration -> Administrative Templates -> Windows Components -> Microsoft Defender Antivirus, and open Turn off Microsoft Defender Antivirus. Set the policy to Enabled.

18) Turn off LLMNR. Open the Group Policy editor by typing gpedit.msc into the Start Menu search box, and press Enter. Then navigate to Computer Configuration > Administrative Templates > Network > DNS Client, and open Turn off multicast name resolution. Set the policy to Enabled.

19) Enable Restrict Internet communication. Open the Group Policy editor by typing gpedit.msc into the Start Menu search box, and press Enter. Then navigate to Computer Configuration > Administrative Templates > System > Internet Communication Management, and open Restrict Internet Communication. Set the policy to Enabled.

20) Disable Microsoft Defender (anti-virus). Open the Group Policy editor by typing gpedit.msc into the Start Menu search box, and press Enter. Then navigate to Computer Configuration > Administrative Templates > Windows Components > Microsoft Defender Antivirus, and open Turn off Microsoft Defender Antivirus. Set the policy to Enabled.

21) Disable Read-time Protection. Open the Group Policy editor by typing gpedit.msc into the Start Menu search box, and press Enter. Then navigate to Computer Configuration > Administrative Templates > Windows Components > Microsoft Defender Antivirus > Real-time Protection, and open Turn off real-time protection. Set the policy to Enabled.

22) Next, Disable windows updates in services. Open services and look for the service Windows Update. Click on stop to stop the Windows Update service.

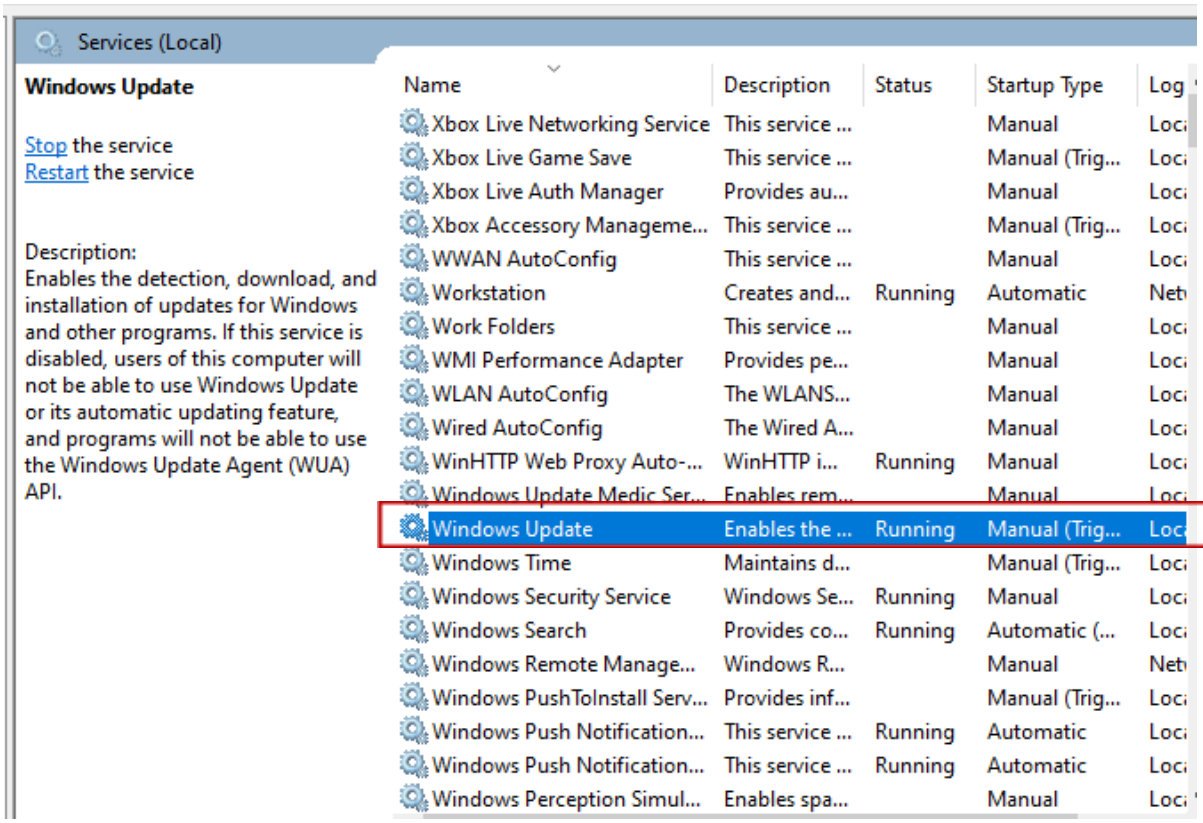

Fig 37. Windows Update in Services

Next, right-click on windows update and click on properties. Set the startup type to disabled. Click on Apply and then OK:

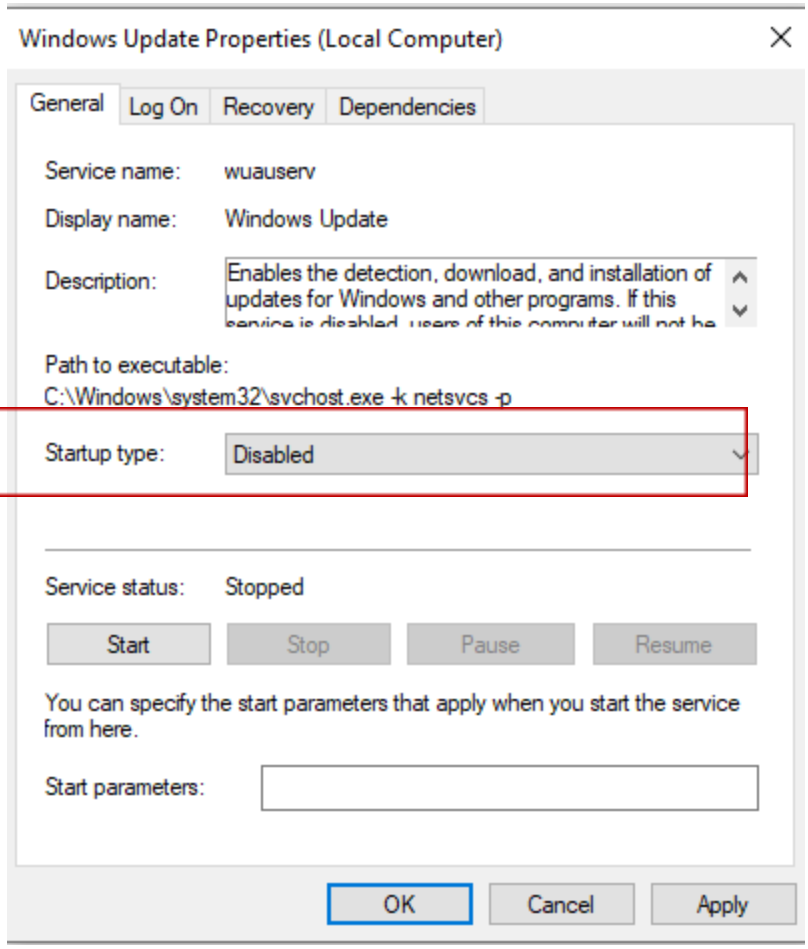

Fig 38. Windows Update set to Disabled

Repeat the Steps to disable Microsoft Edge Update services shown below:

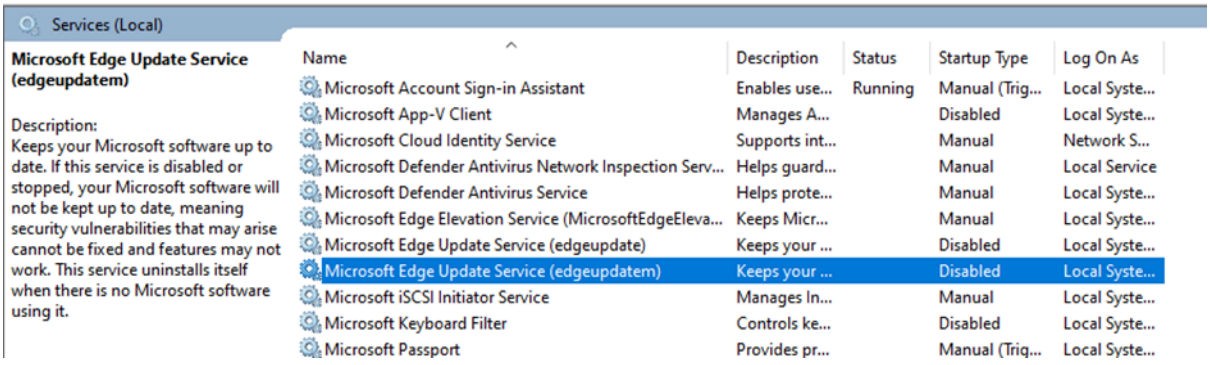

Fig 39. Windows Update set to Disabled

23) Next, disable the teredo interface to prevent teredo from interfering with analysis. Open PowerShell windows as Administrator, and run the following command to disable the teredo interface to avoid teredo from interfering with the analysis:

netsh interface teredo set state disabled

24) Next, Disable Microsoft store by removing Microsoft store from the PATH variable in environment variables. This is to prevent Microsoft store from interfering with the analysis. Click on Environment Variables:

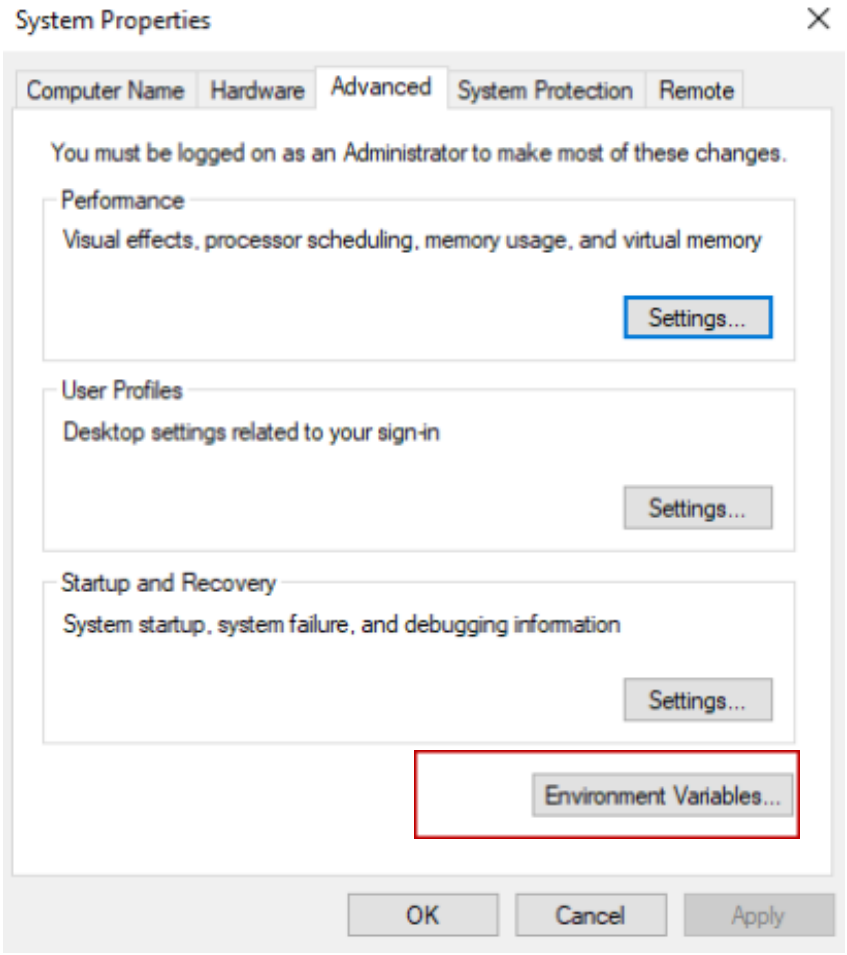

Fig 40. Environment Variables.

Then, click on Path and then Edit

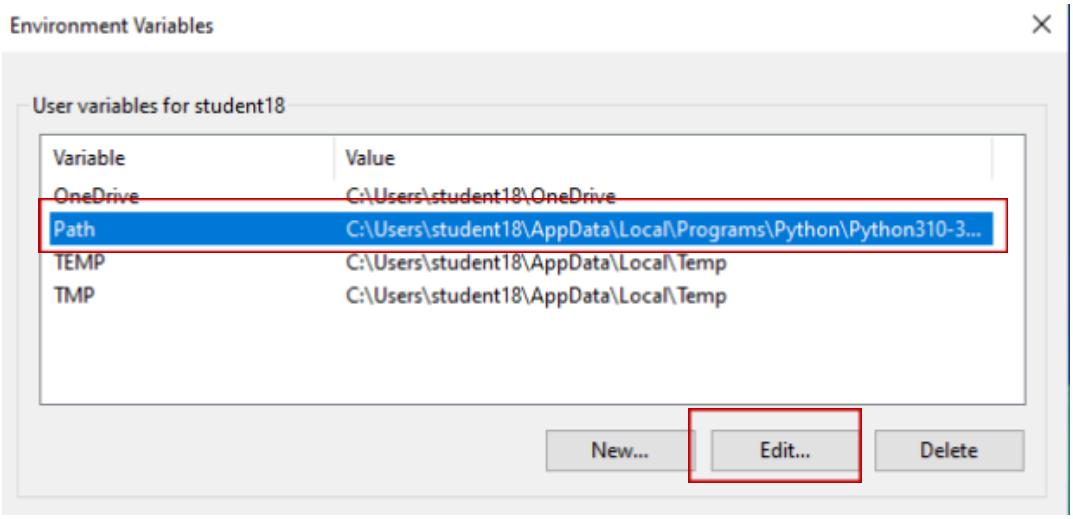

Fig 41. Select the Path variable

Click on WindowsApps and click on delete then click on okay:

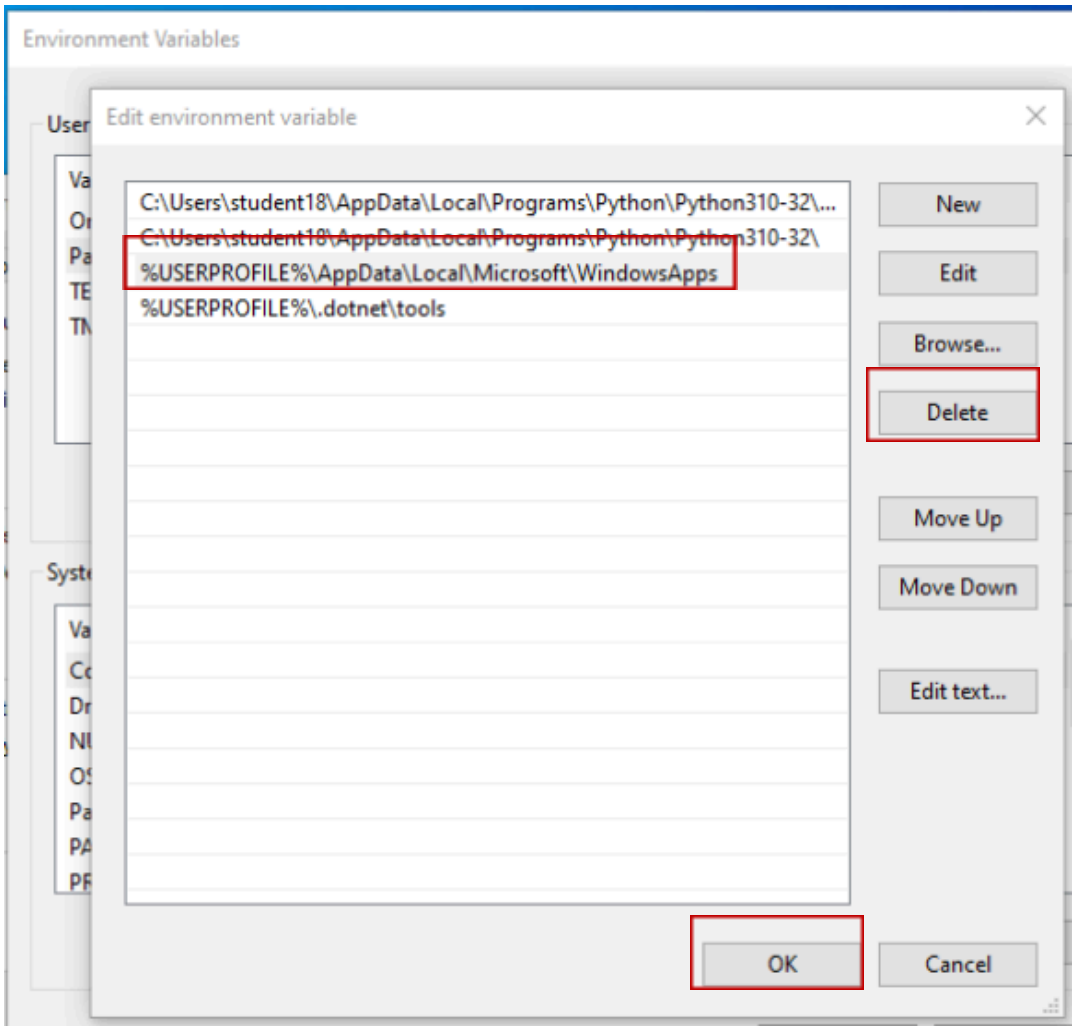

Fig 42. Remove WindowsApps from the PATH environment variable

25) Connect the VM to the internet vibr0 (NAT network). Power up the analysis machine when done, open Powershell and download the python packages. This is to install python packages necessary to Conduct analysis and the VM requires internet to install the packages:

To connect VM to the internet run the command:
virt-manager

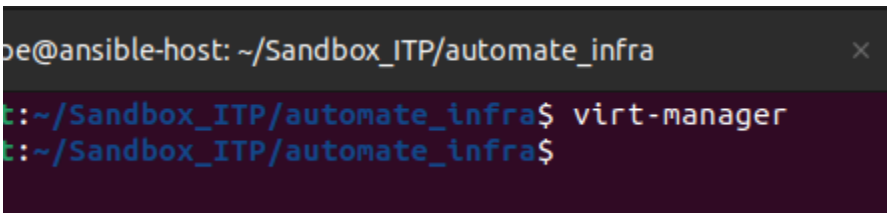

Fig 43. Virt-manager

Open the VM hardware details and then select the NIC and set it to NAT default

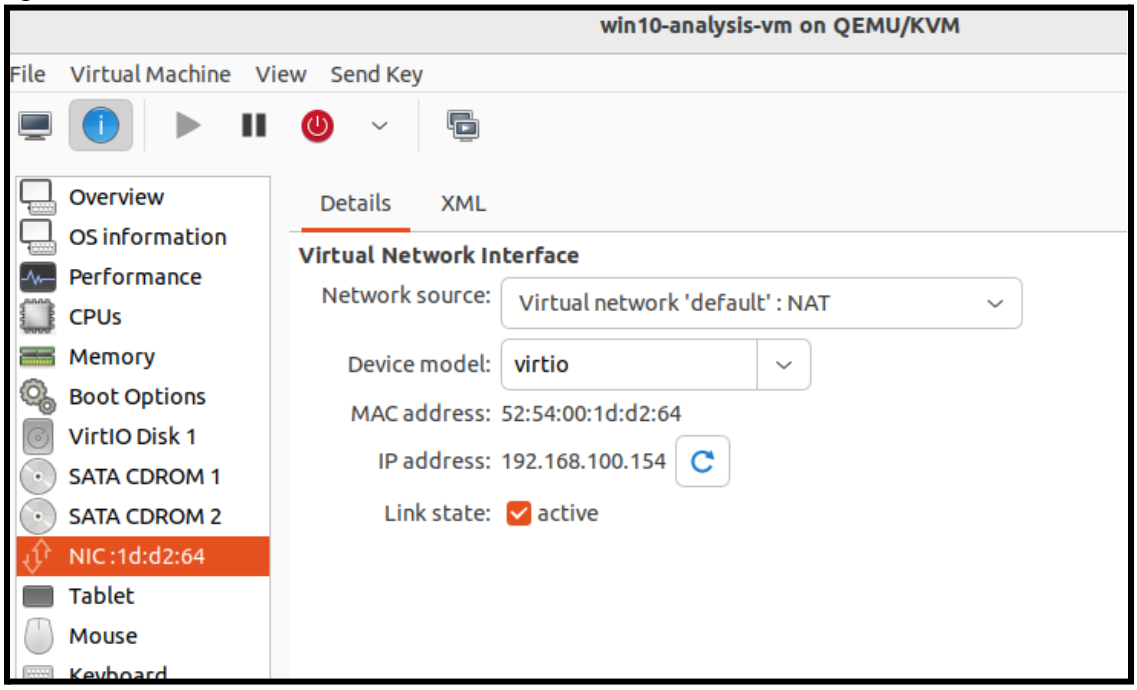

Fig 44. Set the Virtual Netowork Interface of the VM to NAT to connect to the internet to install python packages

Turn on the VM, login to student18 and open up Powershell to install python packages.

Install the python packages using the commands below:
python -m pip install Pillow==9.5.0
python -m pip install rarfile

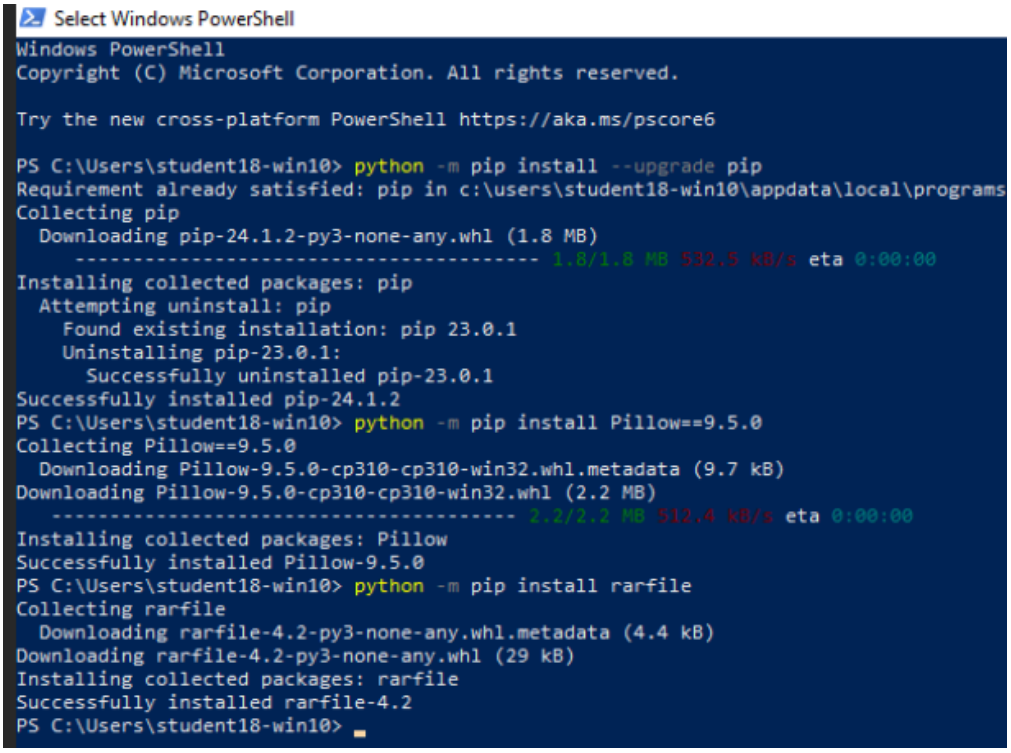

Fig 45. Installing Python Packages

After installing the python packages, powerdown and switch to the isolated host-only network to prevent malware samples from escaping.

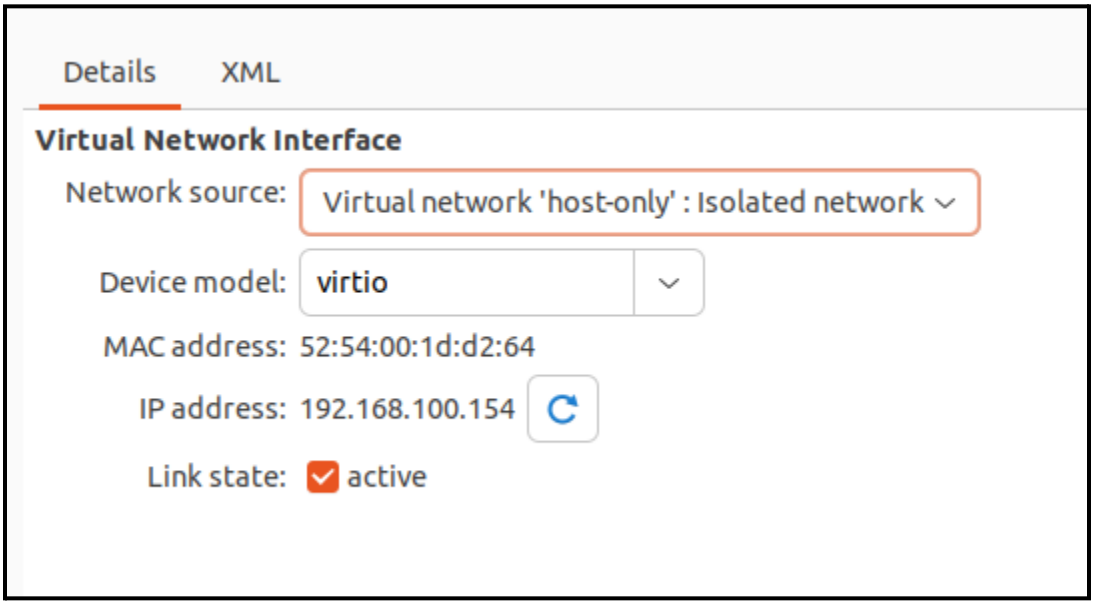

Fig 46. Set the Virtual network interface to host-only

Bootup the VM again and setup the CAPE agent.

26) Download pizza.py (the CAPE agent) from the python HTTP server in CAPE to the Documents folder and save the file as a .pyw file using PowerShell. Change the filename to pizza.

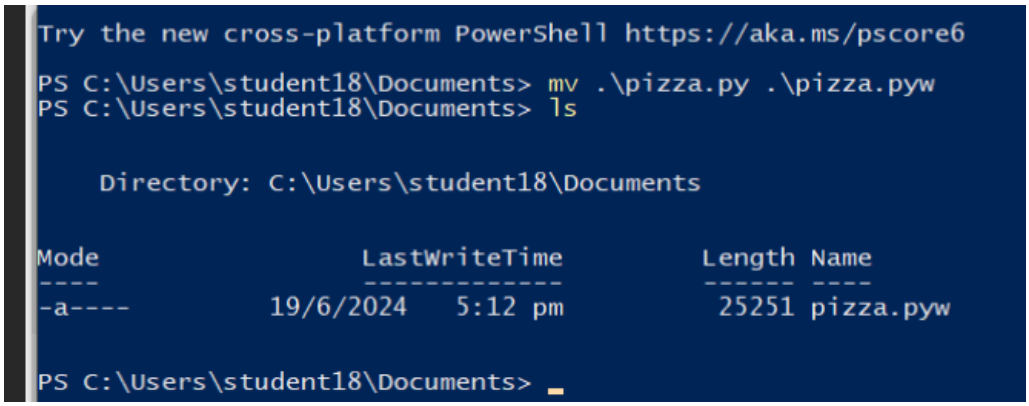

Fig 47. Move pizza.py to pizza.pyw in documents

27) Next open task scheduler and create a task to run the CAPEv2 agent. Create a Basic task with the name pizza:

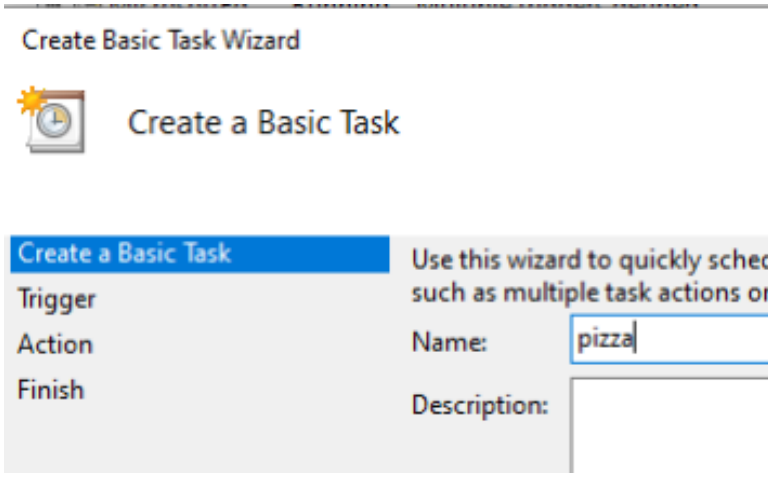

Fig 48. Create Basic Task

28) Set the task Trigger to “when I log on”:

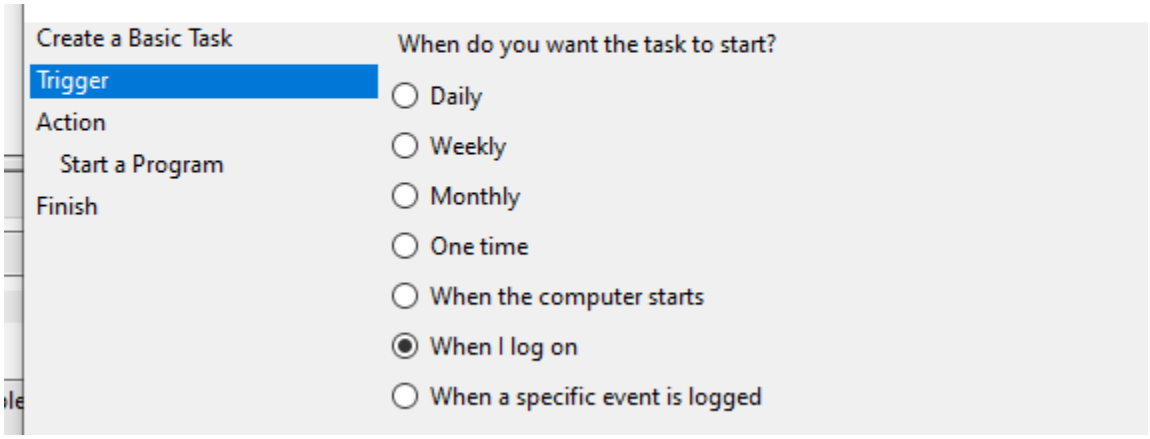

Fig 49. Set Trigger to When I log on

Click on Start a program:

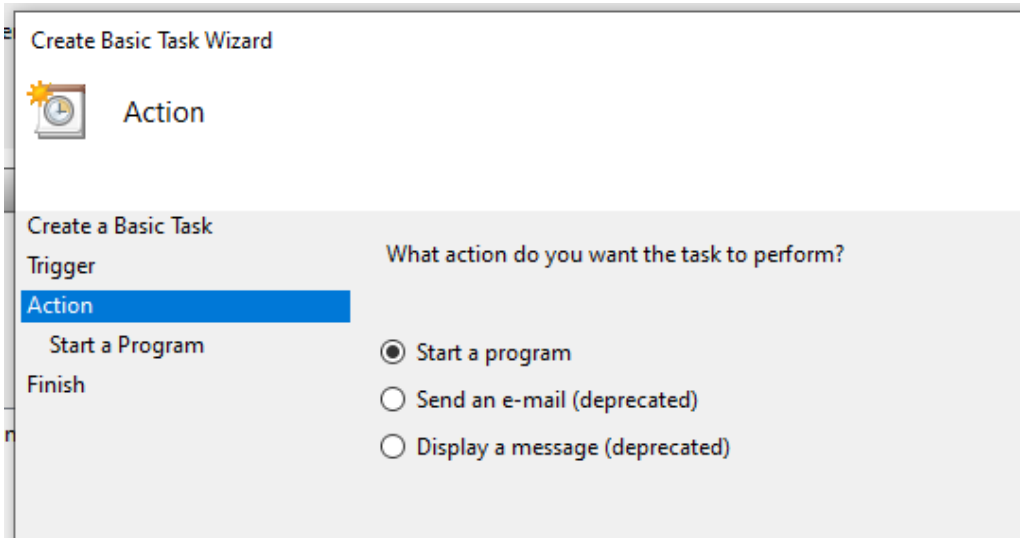

Fig 50. Set action to Start a Program

Click on Browse and select the file pizza.pyw file created earlier.

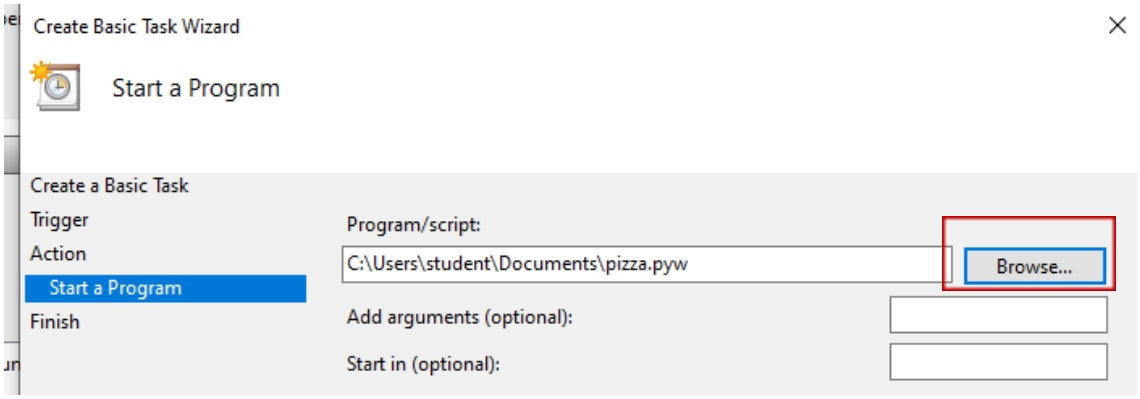

Fig 51. Click on Browse and select the pizza.pyw file in Documents folder

Next, go to the task properties and check the option run with the highest privileges

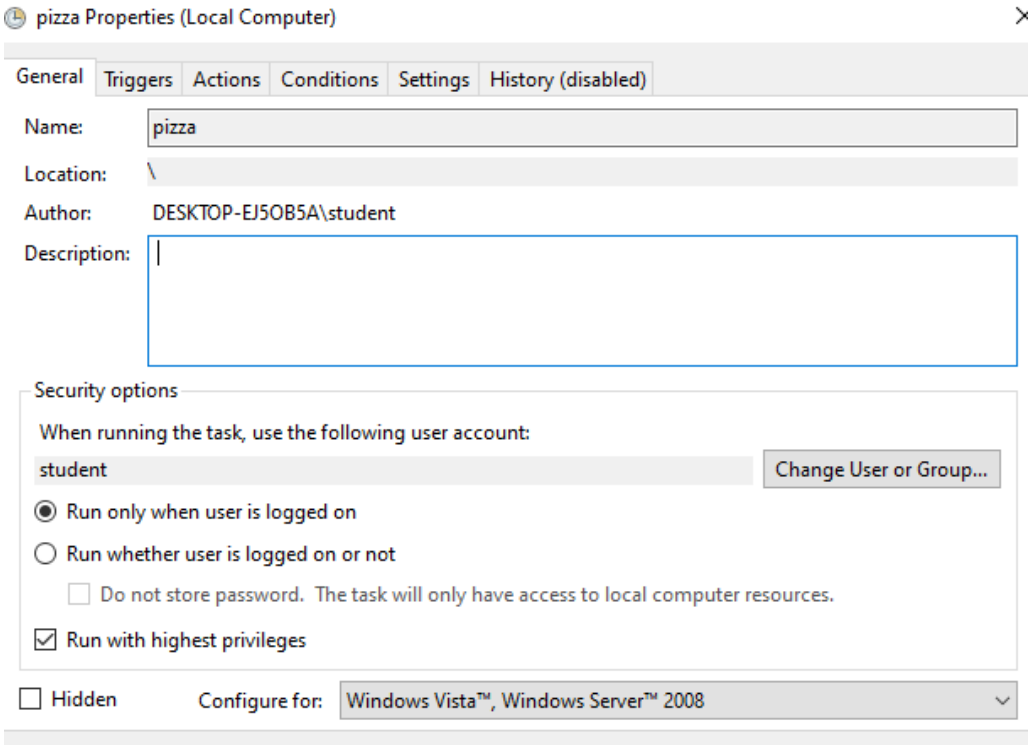

Fig 52. Set Cape agent task to run with the highest Privileges

29) After setting up the CAPE agent, setup autologon to automatically log in the analysis machine. AutoLogon64.exe into the Documents folder. Run autologon.exe and enter student18 password (toor). Once enabled, reboot the VM to test if auto logon is working.

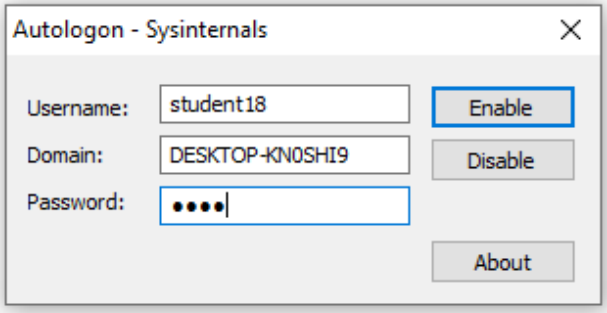

Fig 53. Enable Autologon in the analysis machine.

30) If Autologon is working powerdown the kvm VM. Next create a copy of the .qcow2 file inside the same directory. The .qcow2 file needs to be in the same directory as it needs to be in the same storage pool or else the new main analysis VM will fail to import the .qcow2 file.