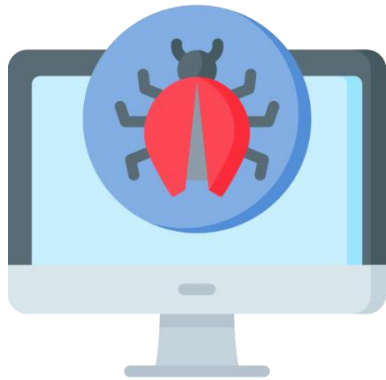


STEP BY STEP MALWARE ANALYSIS LABSET-UP



AMMAR HAKIM HARIS

Contents

HYPERVISOR INSTALLATION	2
WINDOWS 10 OS INSTALLATION	4
REMnux INSTALLATION	13
FLARE VM INSTALLATION	15
SPECIAL NETWORK CONFIGURATION	20
NETWORK CONFIGURATION FOR VM	22
Windows 10 - Flare VM.....	22
REMnux VM.....	23
SET UP INETSIM.....	25
References	30

HYPERVISOR INSTALLATION

1. Go to <https://www.virtualbox.org/wiki/Downloads> and choose the installer according to your host architecture.

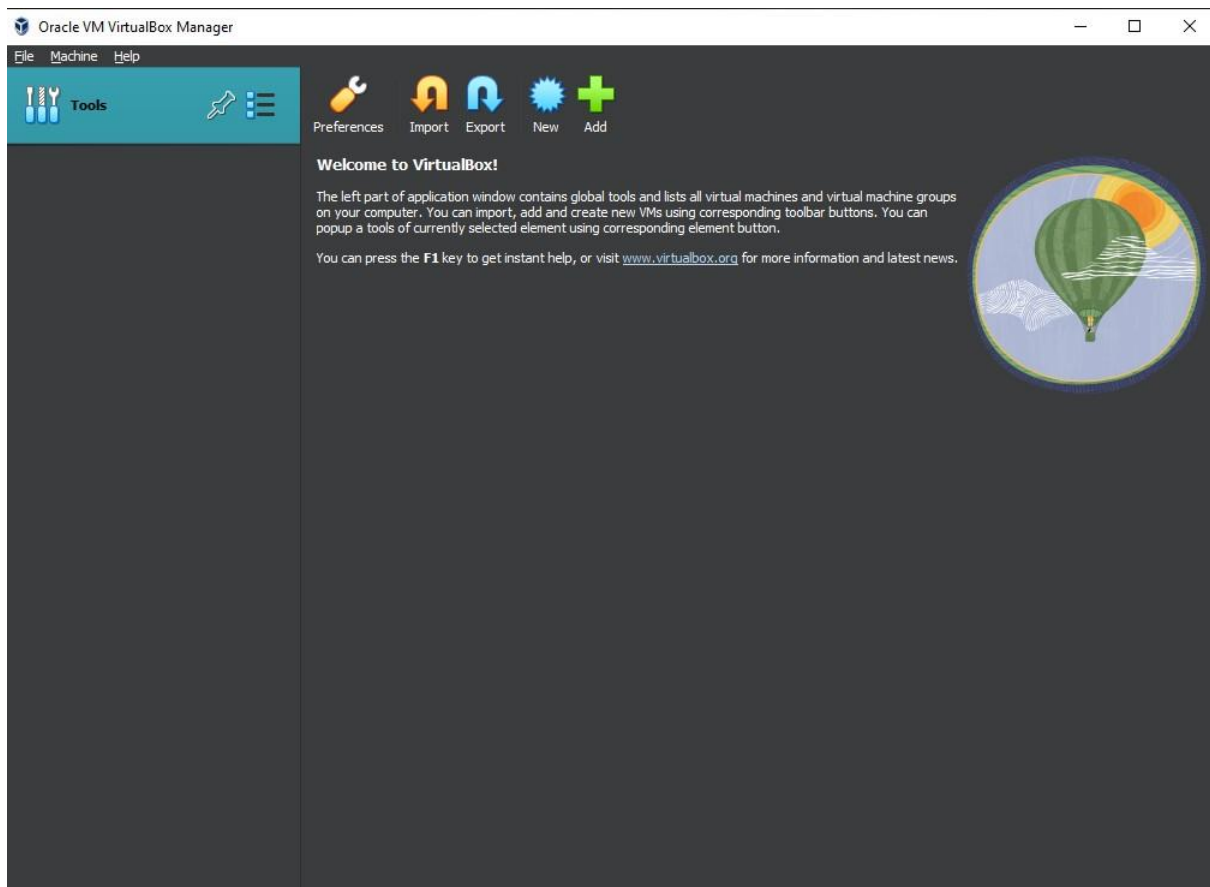


2. Once downloaded. Proceed with the installation with all default settings.



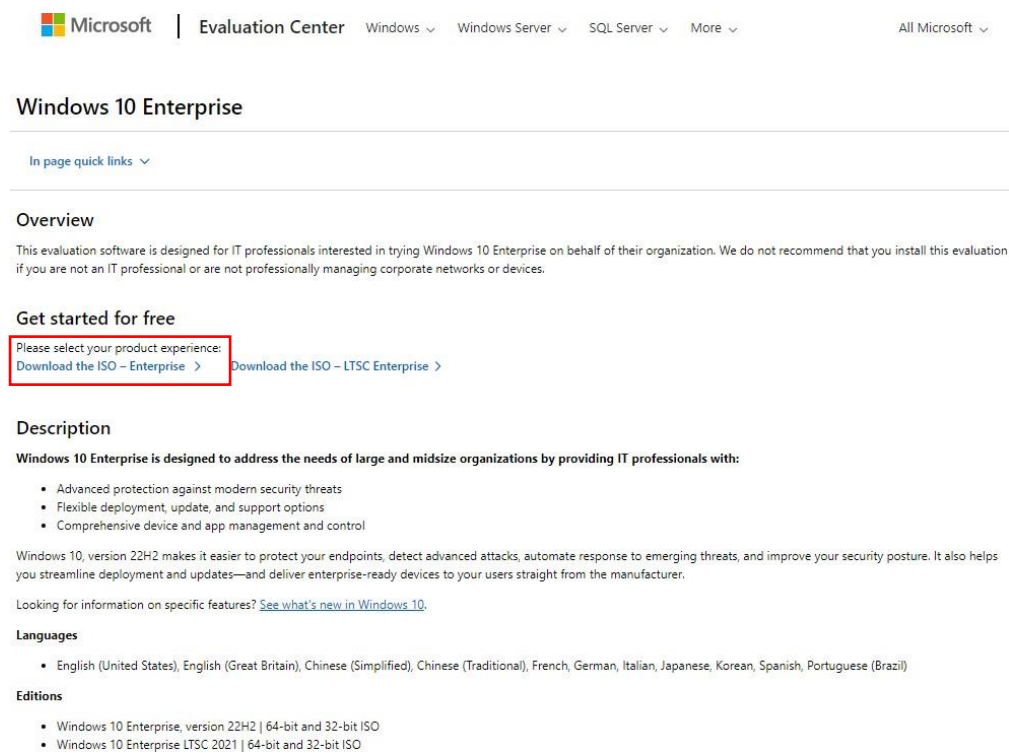
STEP BY STEP MALWARE ANALYSIS LAB SET-UP

3. VirtualBox should launch automatically.



WINDOWS 10 OS INSTALLATION

1. To install the first OS, go to <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise> to get the ISO.



The screenshot shows the Microsoft Evaluation Center page for Windows 10 Enterprise. The navigation bar includes the Microsoft logo, 'Evaluation Center', and links for 'Windows', 'Windows Server', 'SQL Server', and 'More'. The main heading is 'Windows 10 Enterprise'. Below it, there's a section for 'Overview' with a disclaimer. The 'Get started for free' section has a red box around the 'Download the ISO - Enterprise' link. The 'Description' section states that Windows 10 Enterprise is designed for large and midsize organizations. The 'Languages' section lists various languages, and the 'Editions' section lists different versions of the OS.

Microsoft | Evaluation Center Windows Windows Server SQL Server More All Microsoft

Windows 10 Enterprise

In page quick links

Overview

This evaluation software is designed for IT professionals interested in trying Windows 10 Enterprise on behalf of their organization. We do not recommend that you install this evaluation if you are not an IT professional or are not professionally managing corporate networks or devices.

Get started for free

Please select your product experience:
Download the ISO - Enterprise > Download the ISO - LTSC Enterprise >

Description

Windows 10 Enterprise is designed to address the needs of large and midsize organizations by providing IT professionals with:

- Advanced protection against modern security threats
- Flexible deployment, update, and support options
- Comprehensive device and app management and control

Windows 10, version 22H2 makes it easier to protect your endpoints, detect advanced attacks, automate response to emerging threats, and improve your security posture. It also helps you streamline deployment and updates—and deliver enterprise-ready devices to your users straight from the manufacturer.

Looking for information on specific features? [See what's new in Windows 10.](#)

Languages

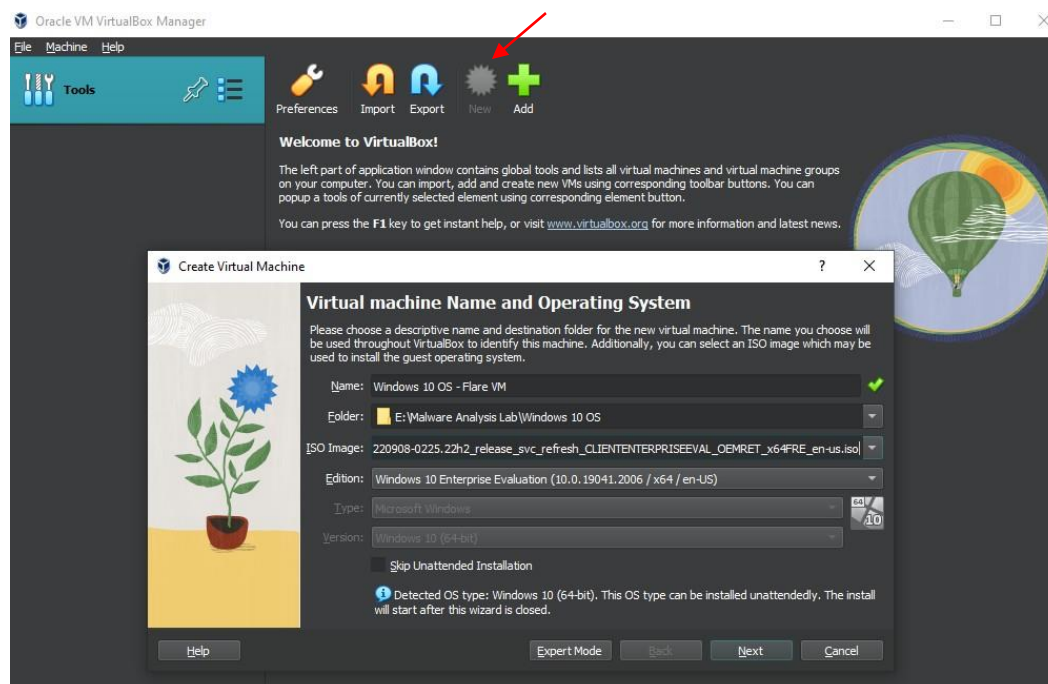
- English (United States), English (Great Britain), Chinese (Simplified), Chinese (Traditional), French, German, Italian, Japanese, Korean, Spanish, Portuguese (Brazil)

Editions

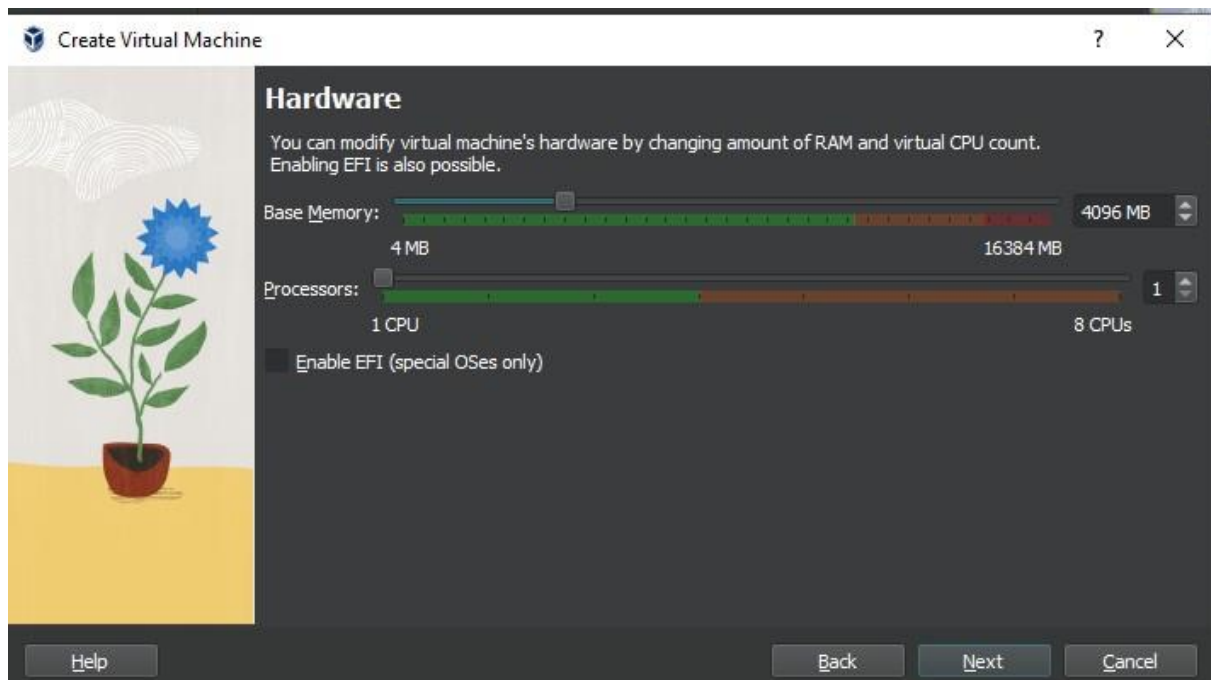
- Windows 10 Enterprise, version 22H2 | 64-bit and 32-bit ISO
- Windows 10 Enterprise LTSC 2021 | 64-bit and 32-bit ISO

2. It will request certain information from you. Register details for your free ISO.

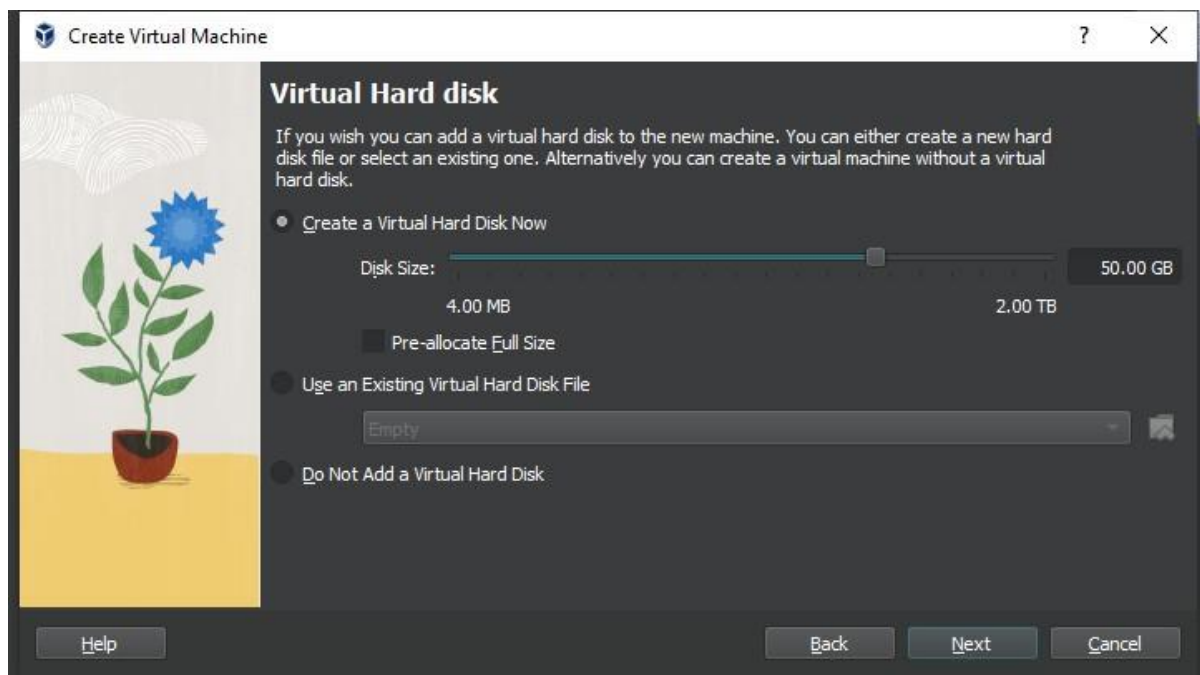
3. Once downloaded, go to VirtualBox - click New button to configure the VM details. Then click Next



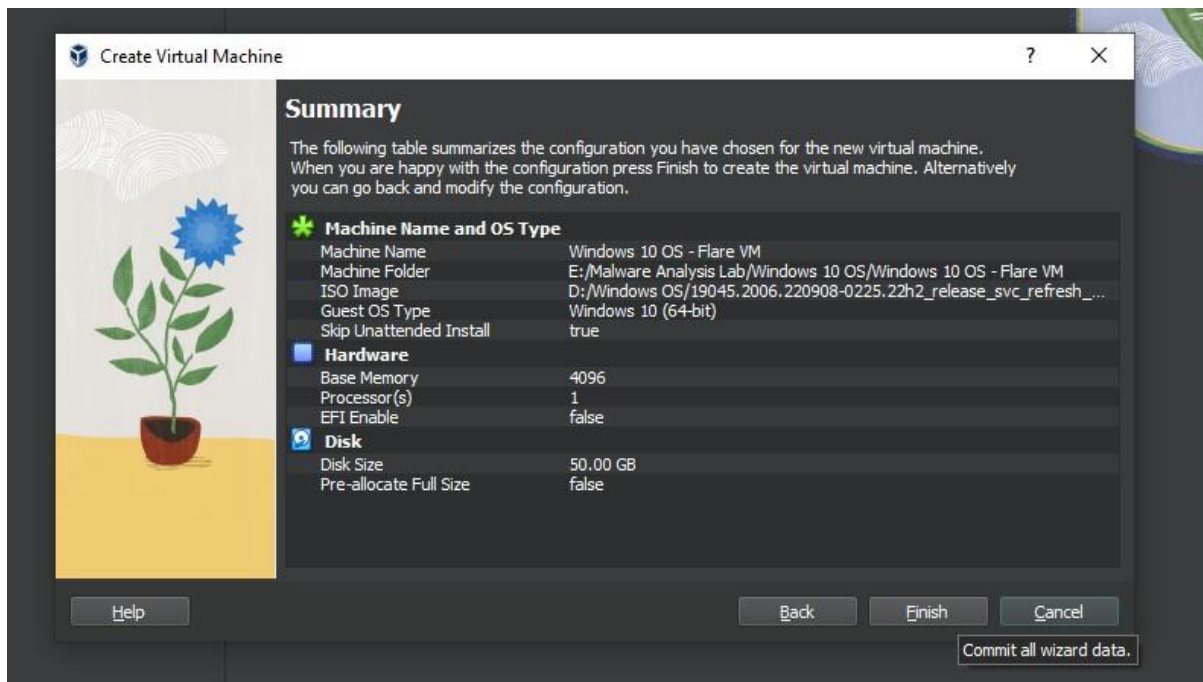
4. Configure your Memory and Processor amount.



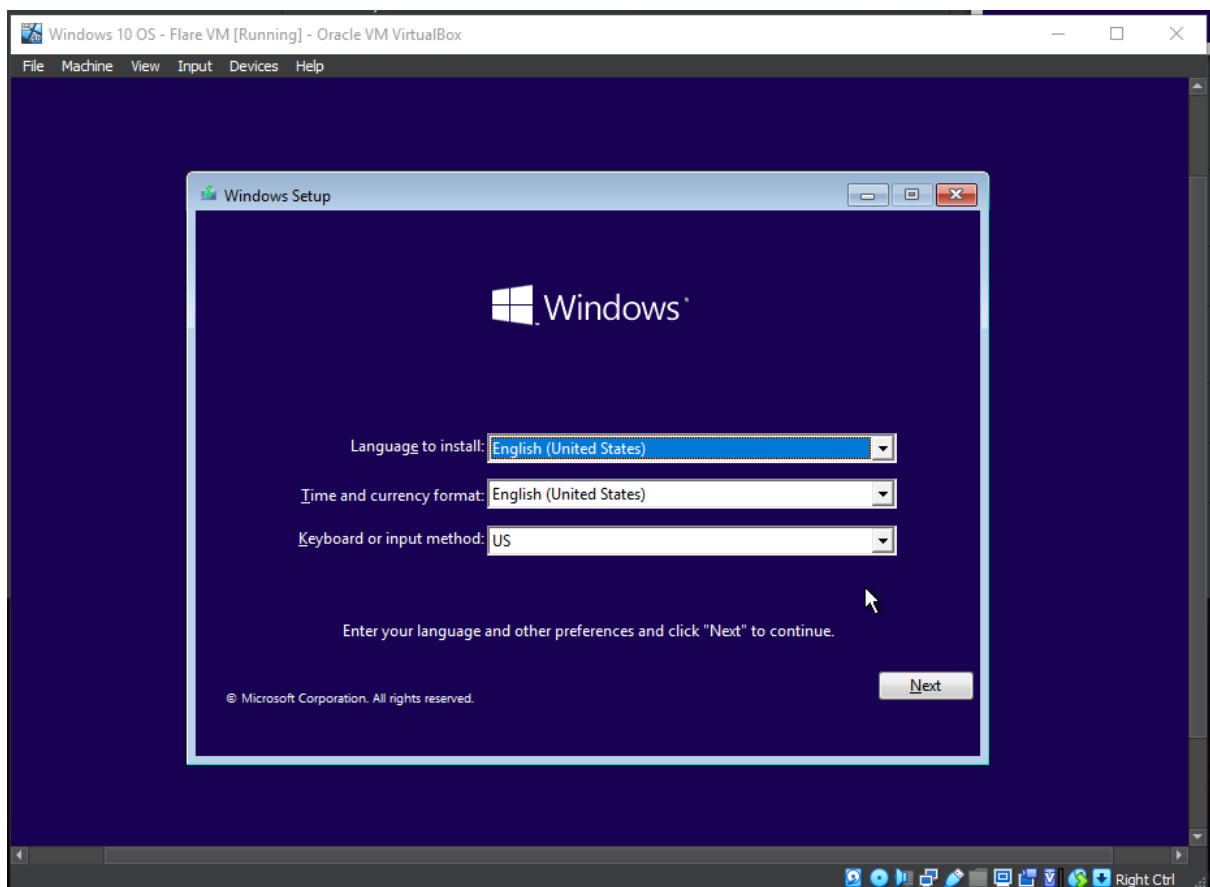
5. For Virtual Hard Disk - you can set it to default. Then click Next.



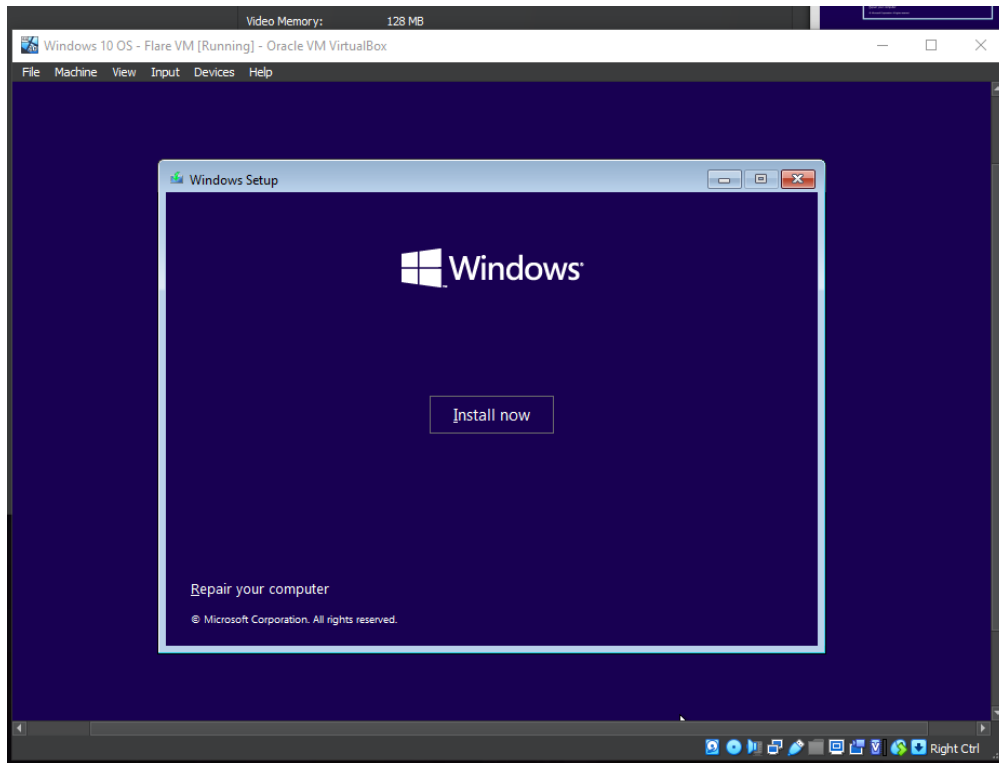
6. Check the details to confirm the configuration before click Finish.



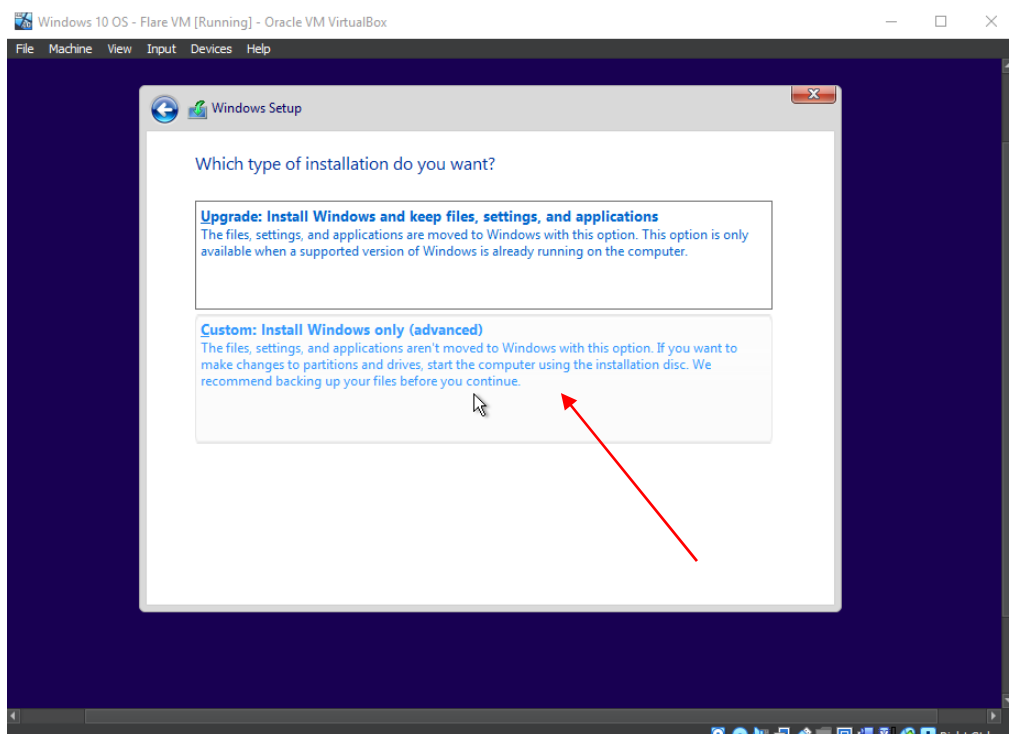
7. After click Finish, initialize it by clicking Start and the machine will start installation process.



STEP BY STEP MALWARE ANALYSIS LAB SET-UP

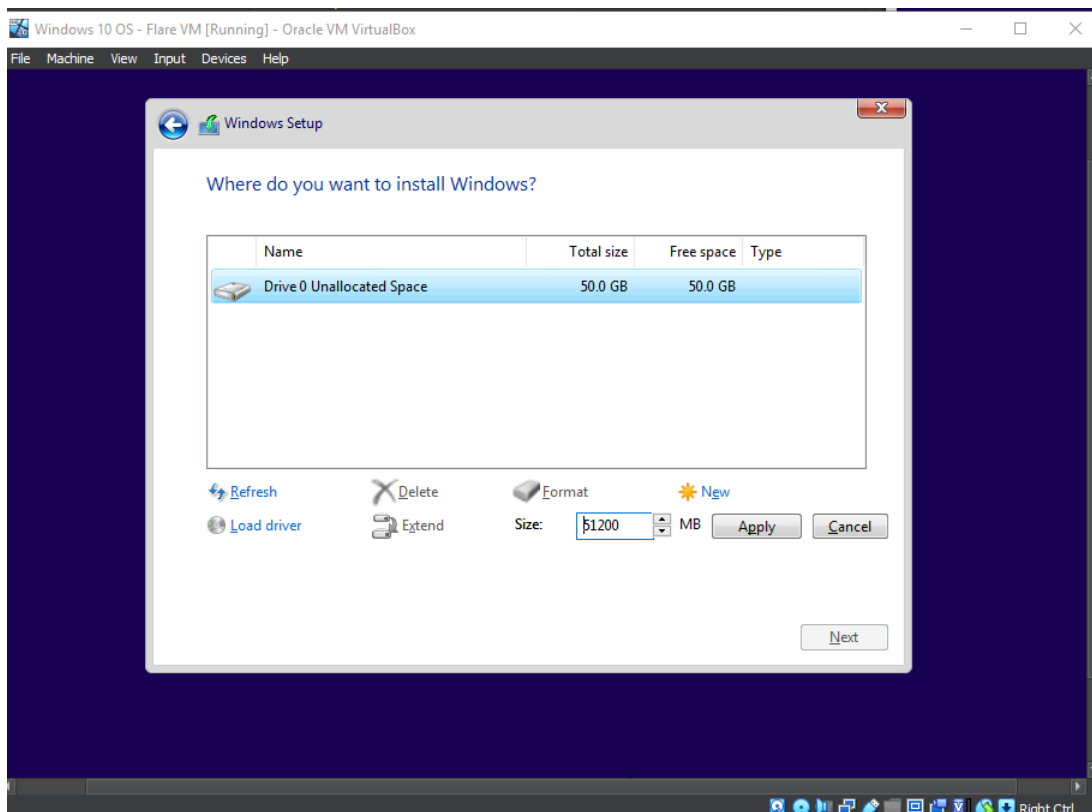


8. Choose Custom installation.

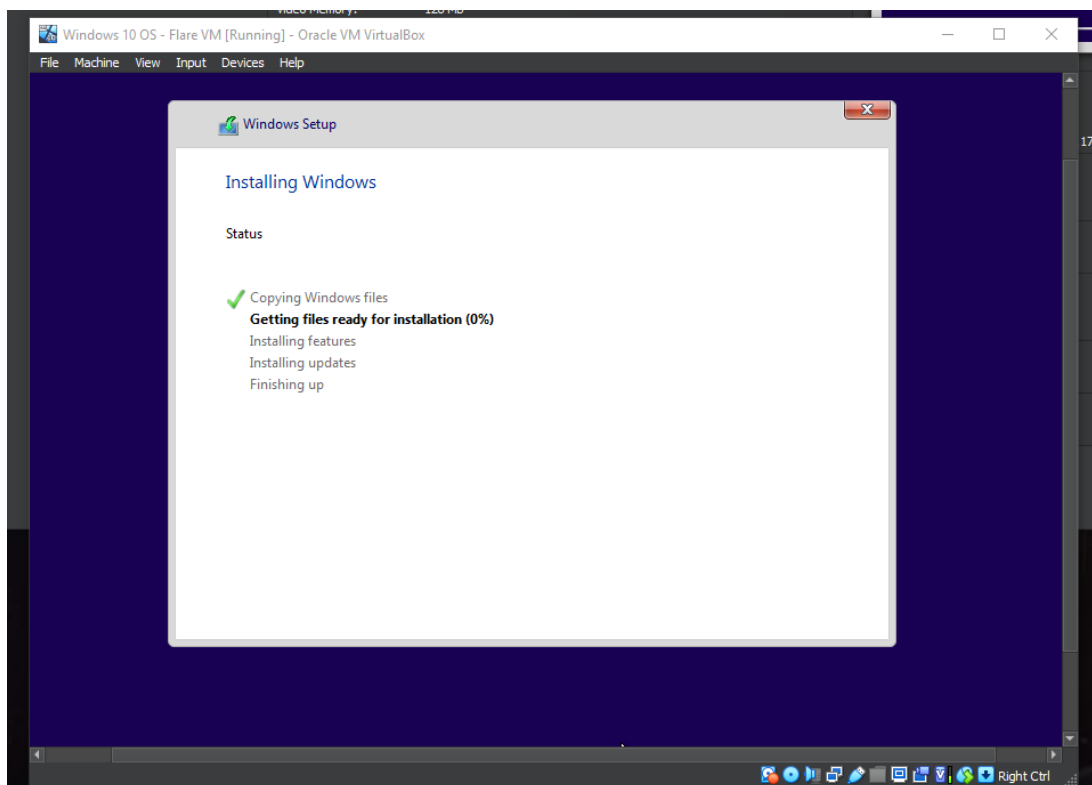


STEP BY STEP MALWARE ANALYSIS LAB SET-UP

9. Click New then Apply before you click Next.

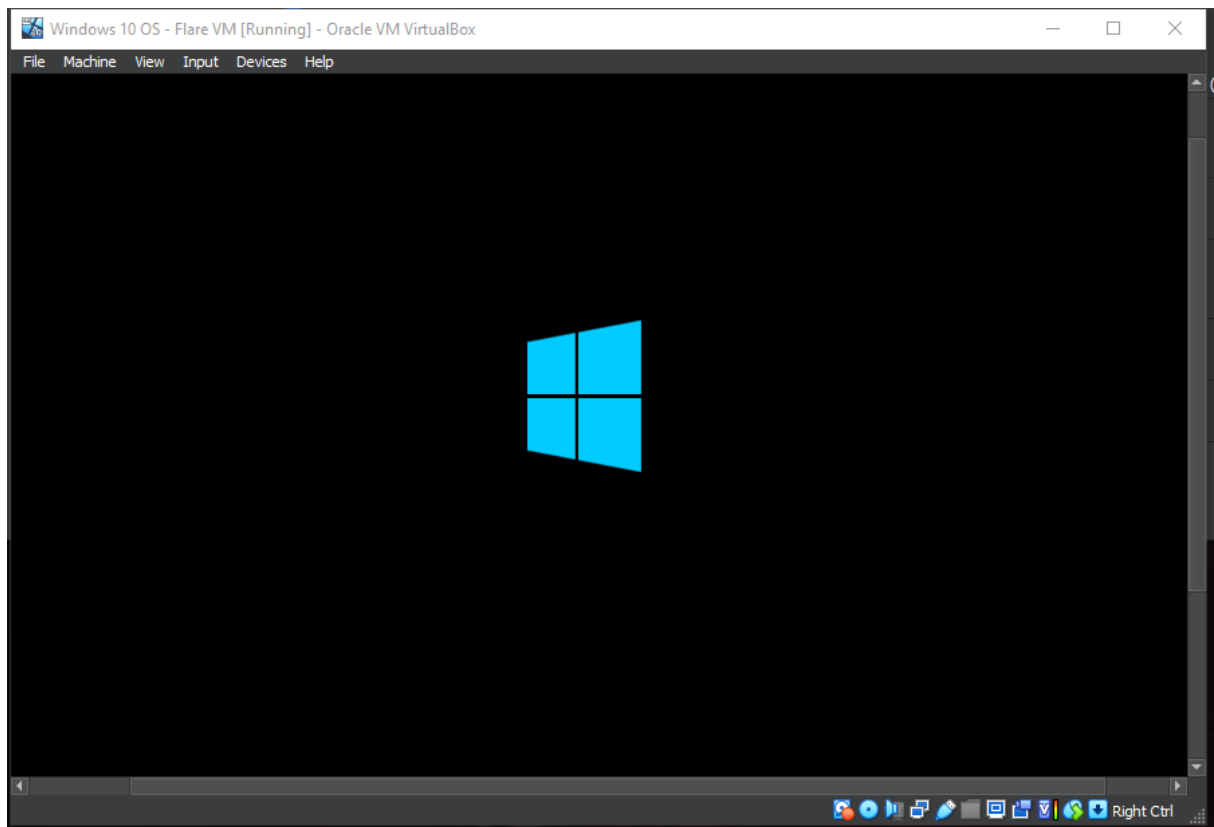


10. Let the installation process complete and this will takes sometimes depending on your resources.

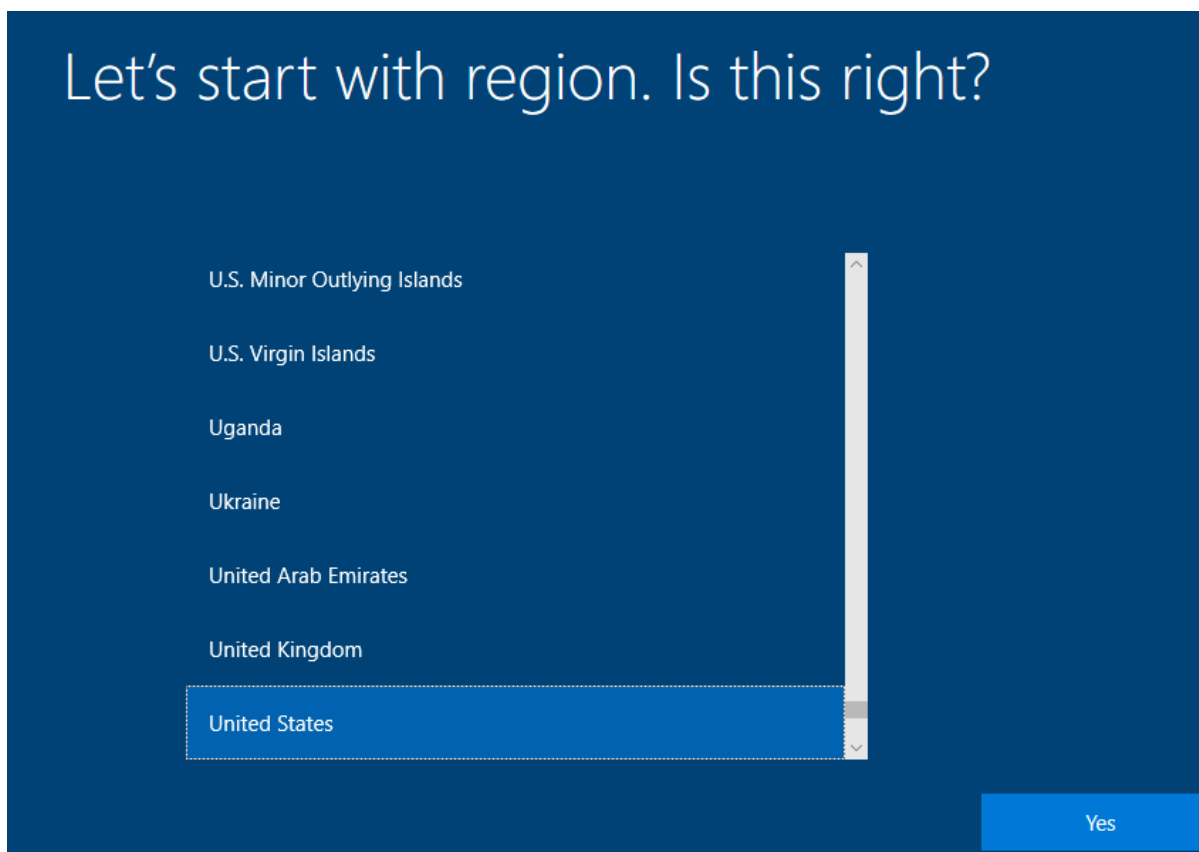


STEP BY STEP MALWARE ANALYSIS LAB SET-UP

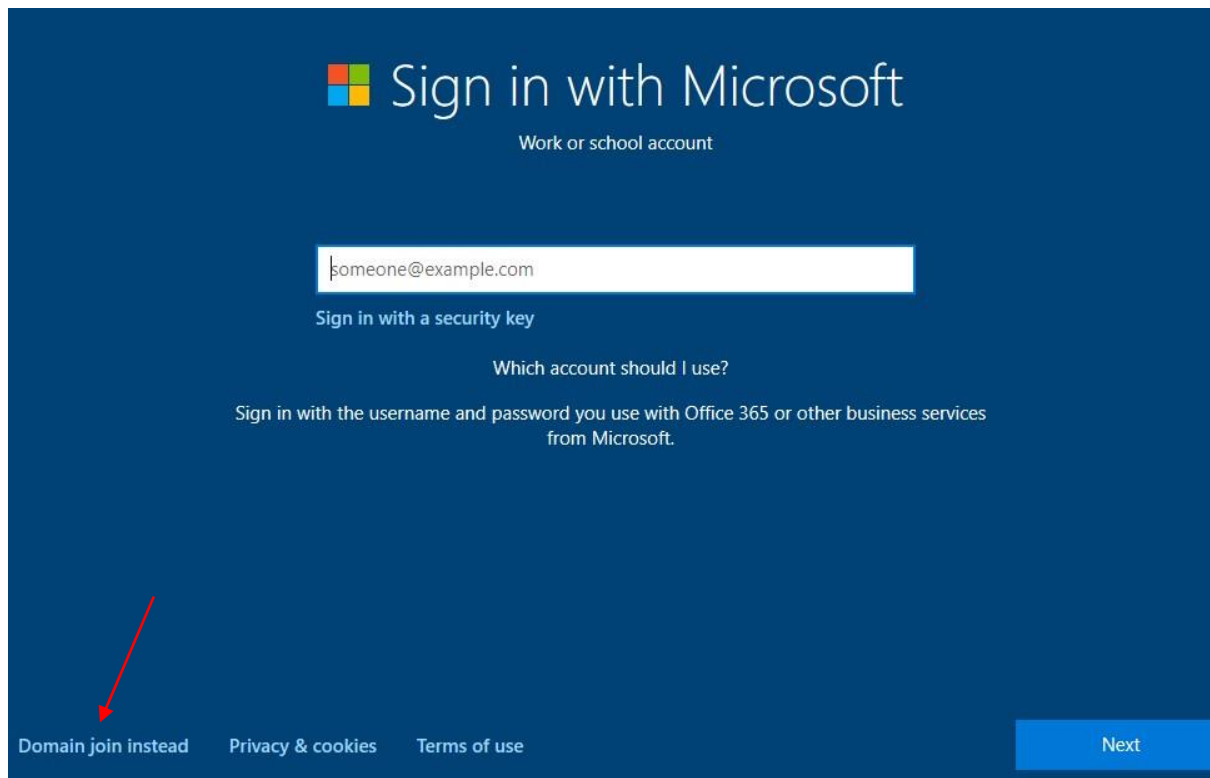
11. The machine will go into booting screen before next step.



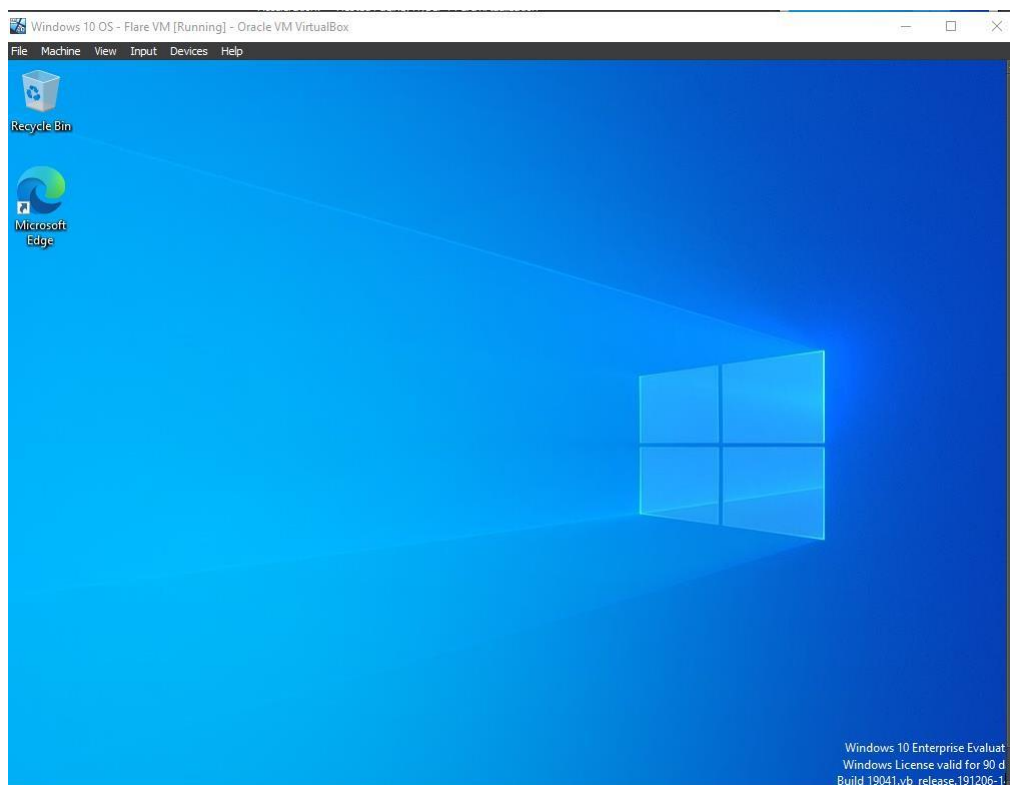
Select Region, Keyboard based on your preferences.



12. You don't have to sign in with Microsoft, select Choose Domain join instead before click Next

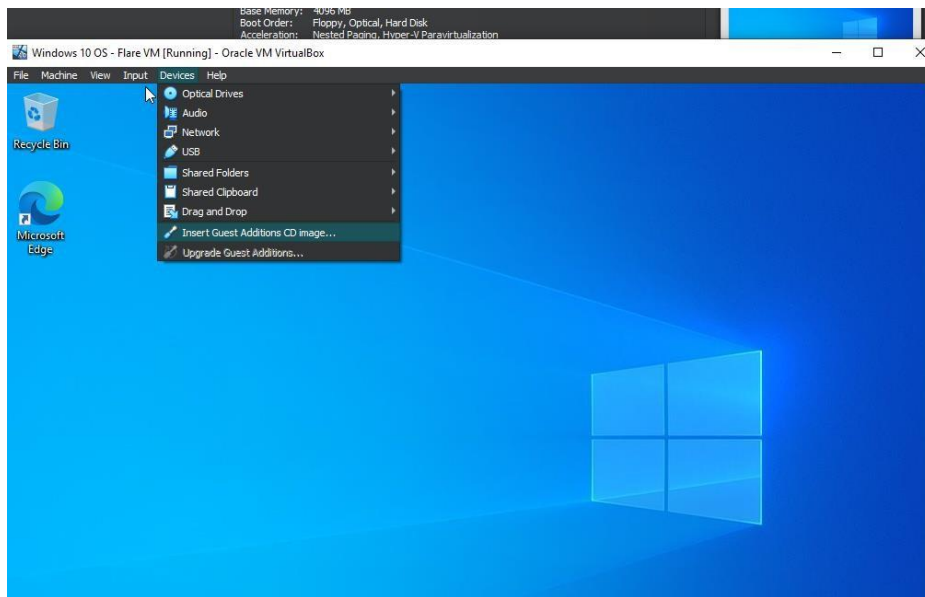


13. Complete the necessary set-up process until you see the Windows desktop.

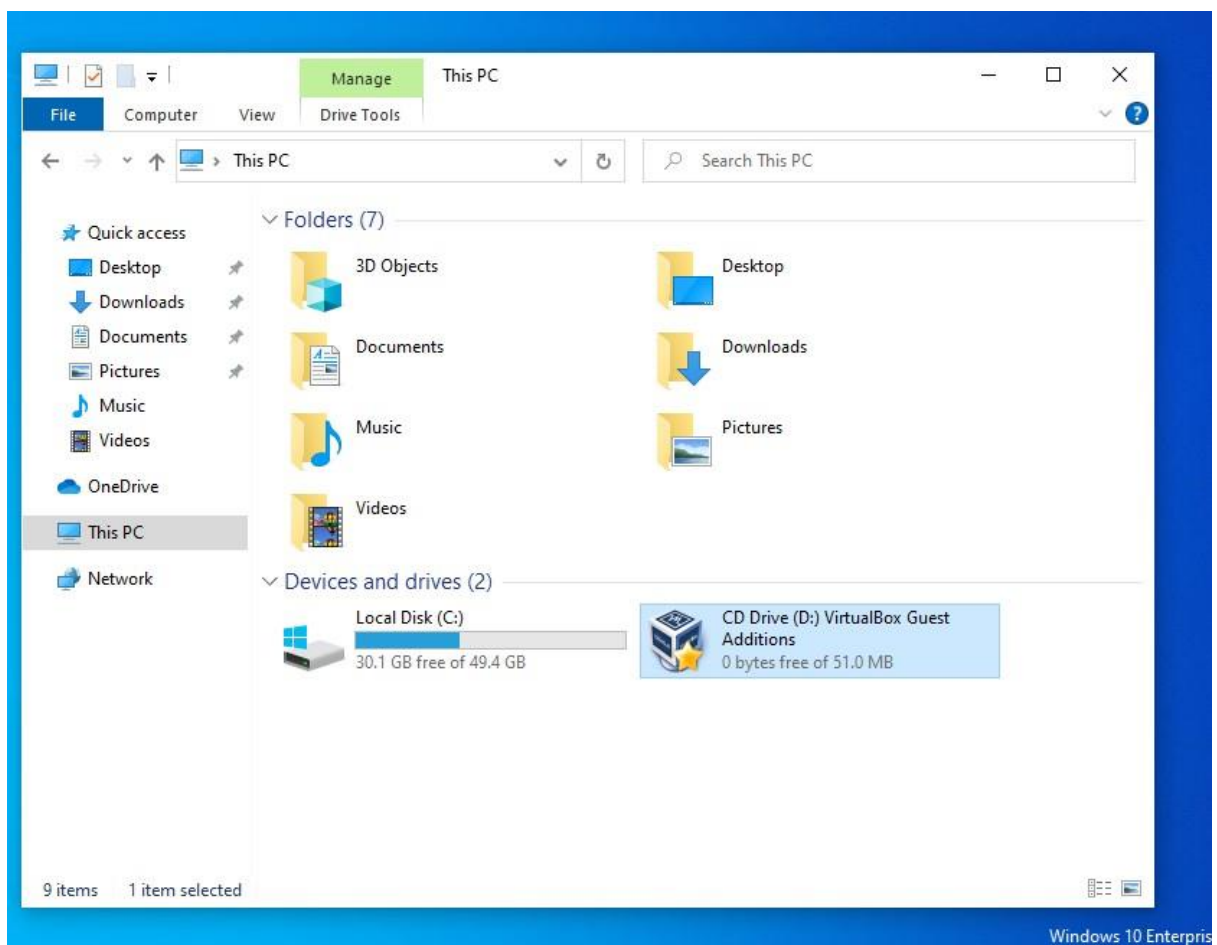


STEP BY STEP MALWARE ANALYSIS LAB SET-UP

14. Then, go to Devices - Insert Guest Edition Cd image to set up better viewing display of your VM.

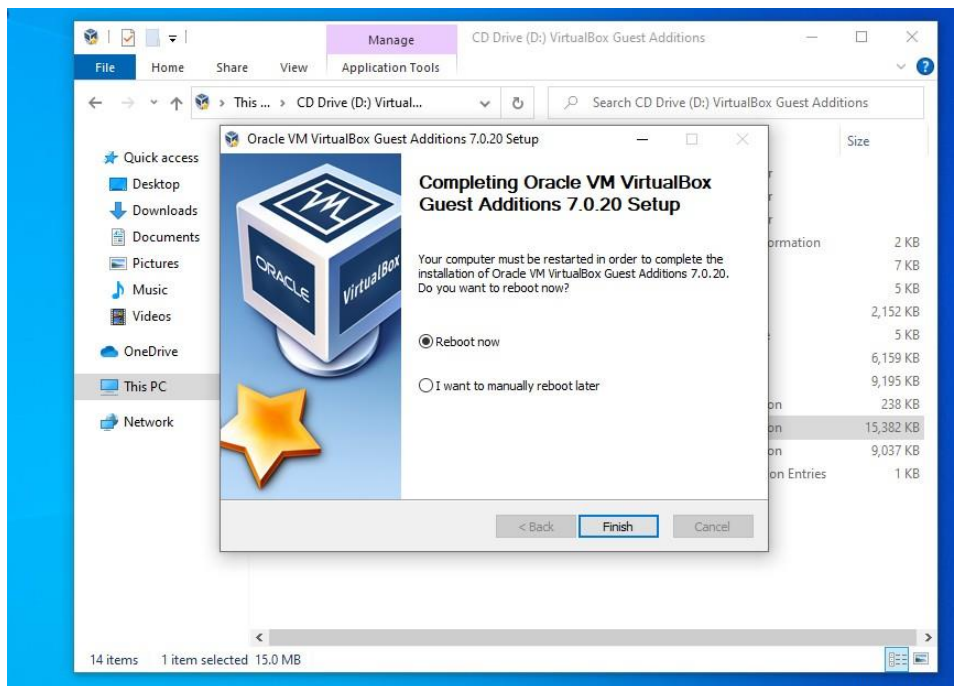


Go to This PC, and double click CD Drive then choose suitable configuration for the installation.

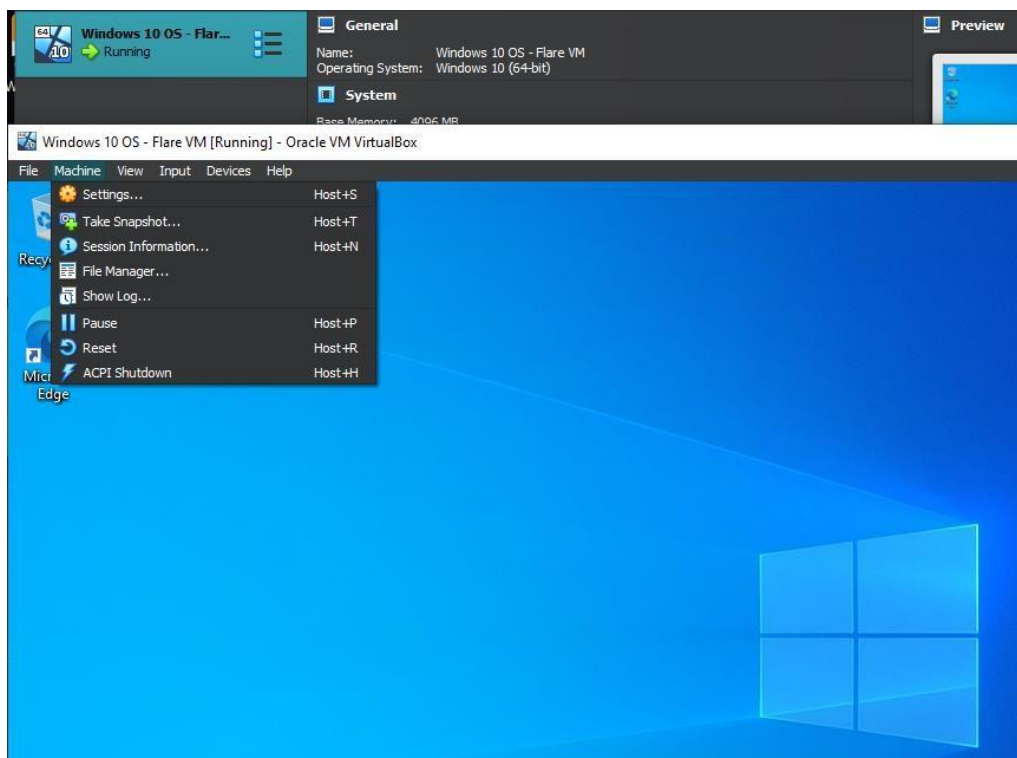


STEP BY STEP MALWARE ANALYSIS LAB SET-UP

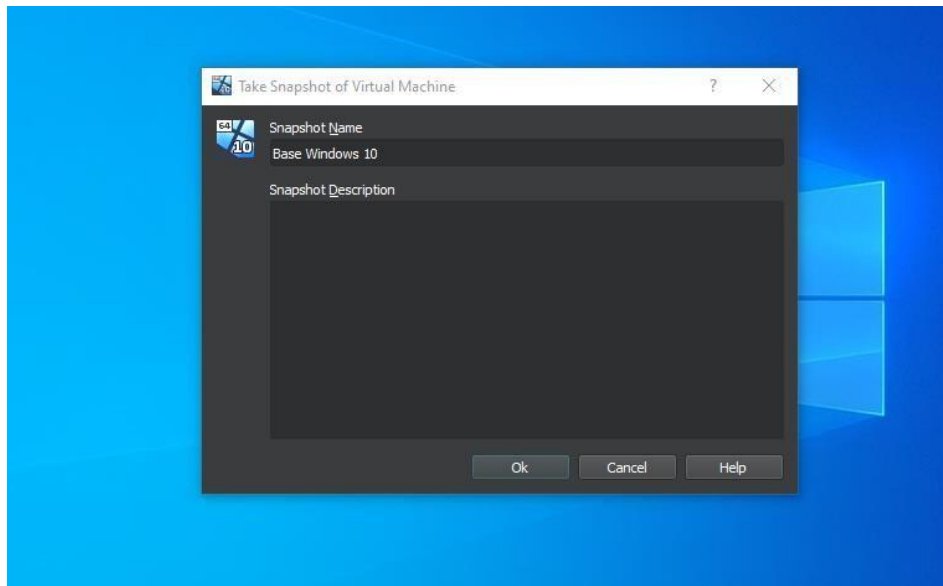
It will reboot once you click Finish.



15. Don't forget to take snapshot at this phase before you proceed with next step. Just go to the TaskBar and select Machine.



Name the snapshot accordingly. This will allow you to return to this base phase if there is error prompted during next configuration.



16. Then suspend your virtual machine to proceed with REMnux installation

REMnux INSTALLATION

17. Go to <https://docs.remnux.org/install-distro/get-virtual-appliance> , then select VirtualBox OVA. You will be able to download it from the Box.

M2.

Step 1: Download the Virtual Appliance File

The REMnux virtual appliance approximately 5 GB. It comes as an industry-standard OVA file, which you can import into your virtualization software. It's based on Ubuntu 20.04 (Focal).

Decide which OVA file to download. Unless you're using Oracle VM VirtualBox, get the general OVA file. If you're using VirtualBox, get the VirtualBox version. Download your preferred OVA file:

General OVA

VirtualBox OVA

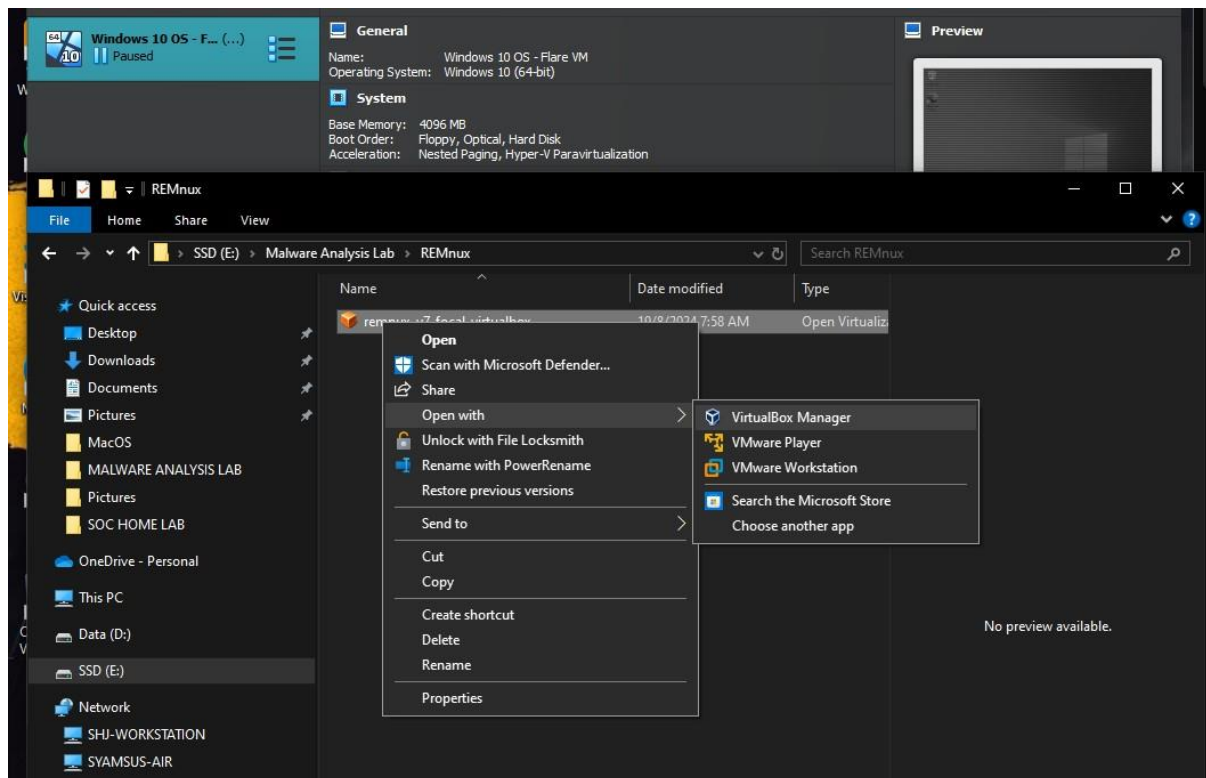
This VirtualBox OVA file is specifically for VirtualBox. Get the general version from the other tab if you're using other hypervisors:

Download the VirtualBox OVA file from [Box](#) (primary) or [SourceForge](#) (mirror)

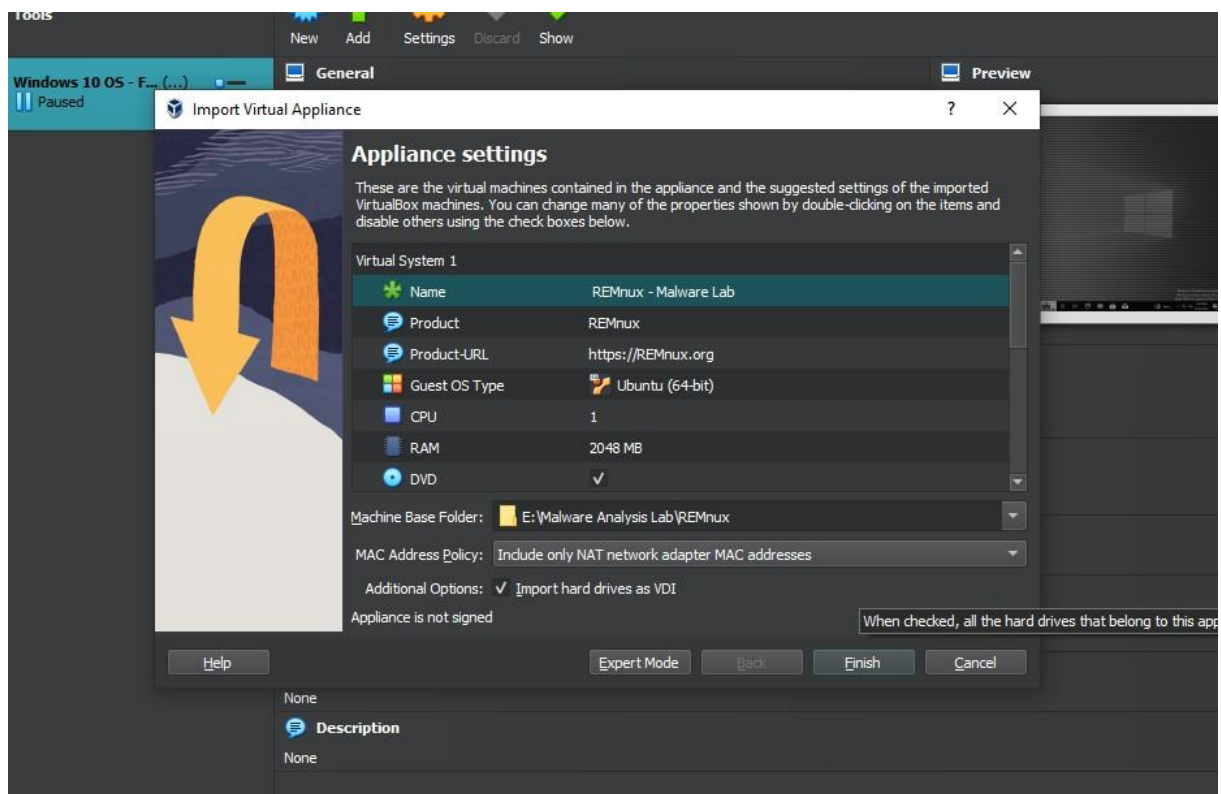
Some browsers (e.g., Brave) change the extension of the OVA file after downloading it, possibly giving it the incorrect .ovf extension. If that happens, rename the file so it has the .ova extension before proceeding.

STEP BY STEP MALWARE ANALYSIS LAB SET-UP

18. Download the file into the same directory created just now for easy access. Go to the installer once download completed and choose Open with VirtualBox Manager.

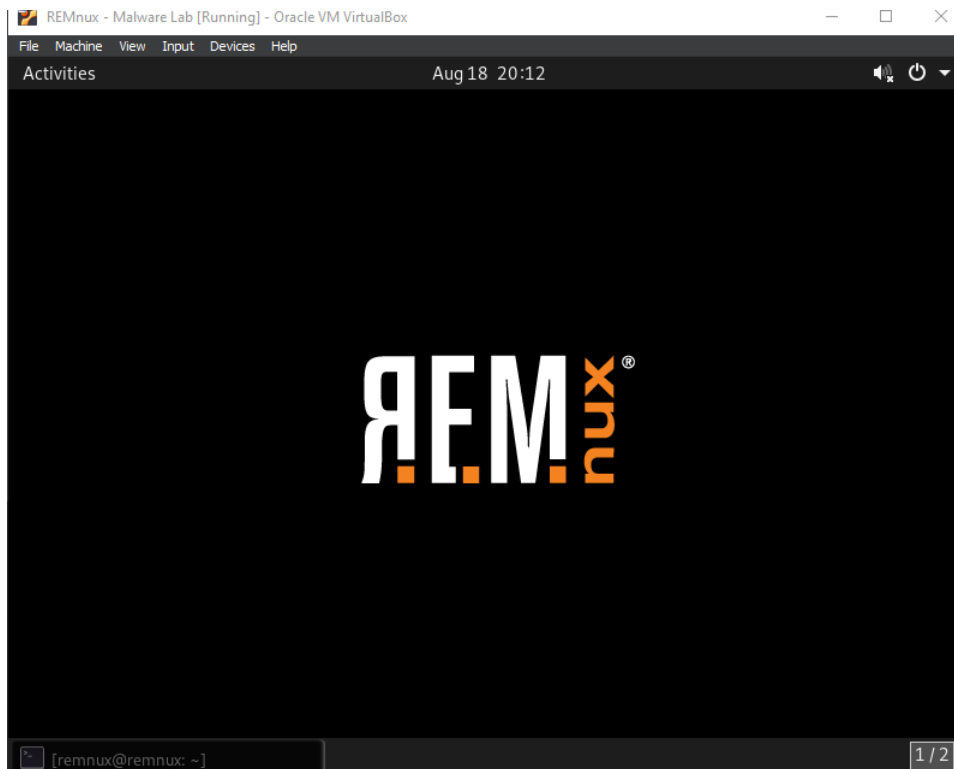


19. Set the VM accordingly before you click Finish.



Allow it to complete the set-up, then Power On the REMnux VM.

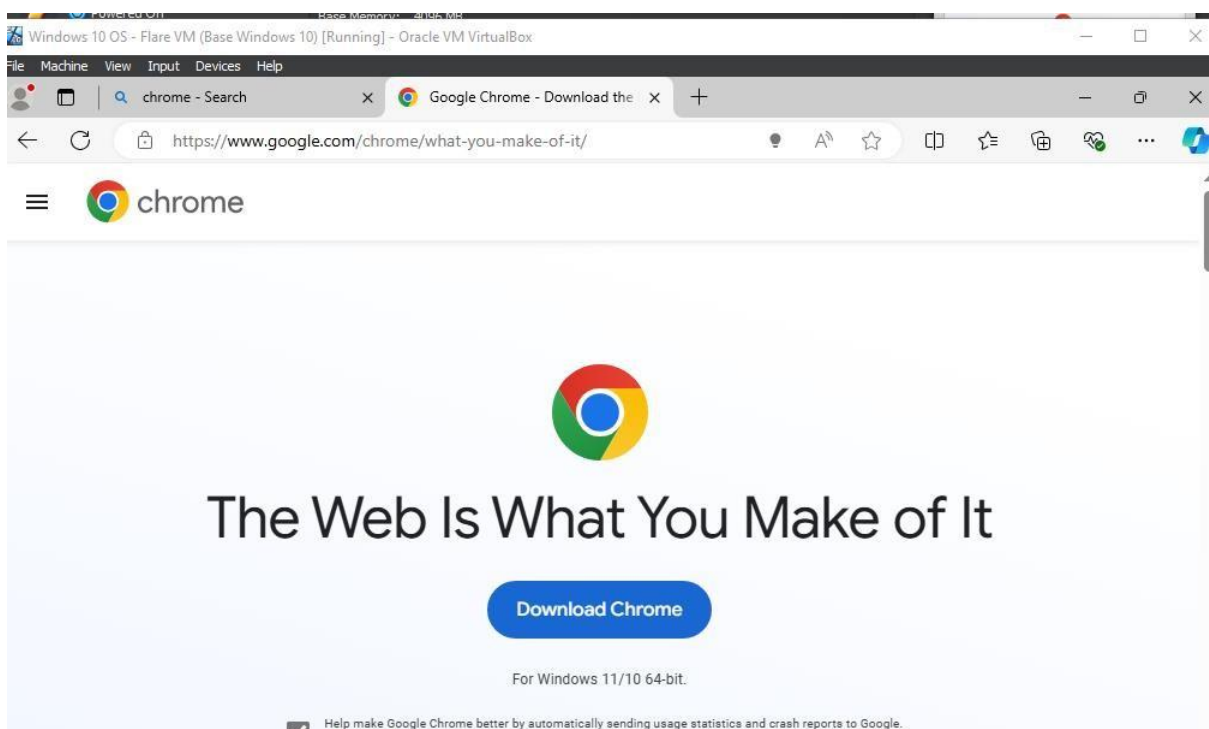
20. You should see REMnux VM running after the booting process completed.



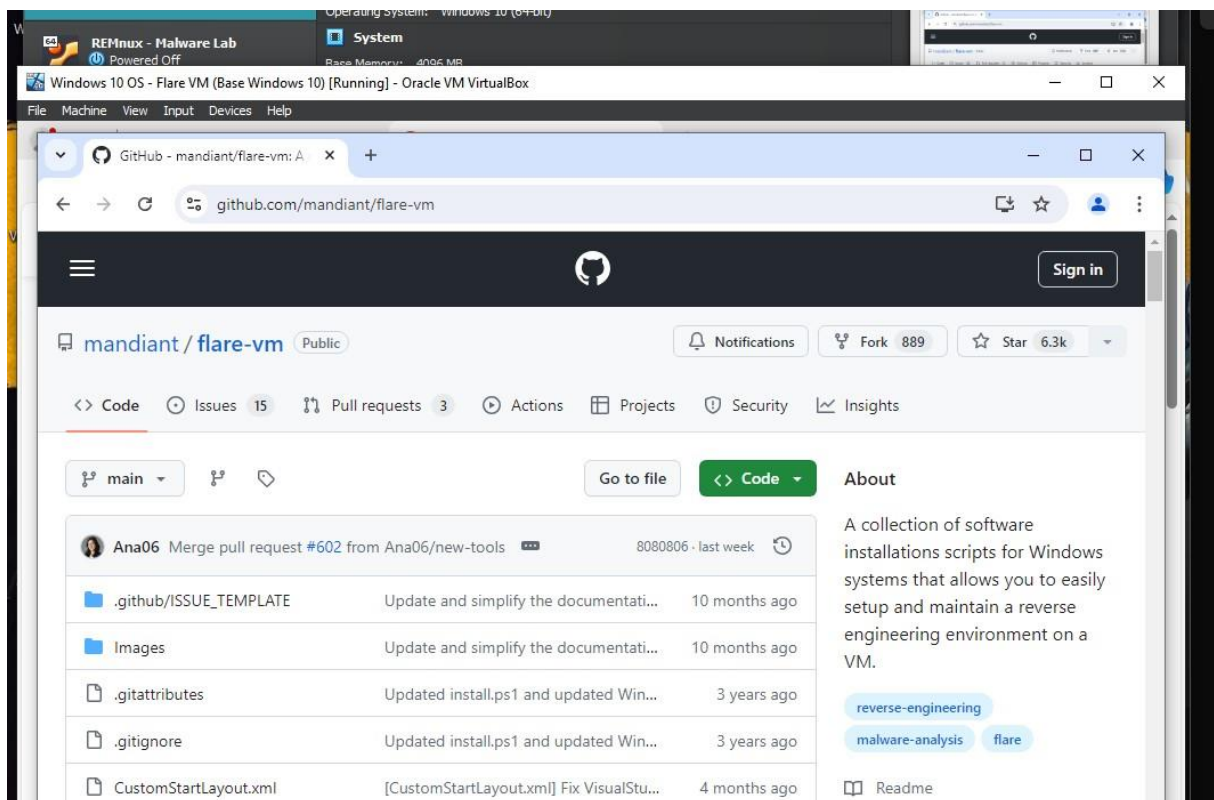
Power Off REMnux machine.

FLARE VM INSTALLATION

21. First install chrome browser into the Windows 10 OS VM.



22. Then go to <https://github.com/mandiant/flare-vm>



Copy link address of installer.ps1

automatically-windows-10

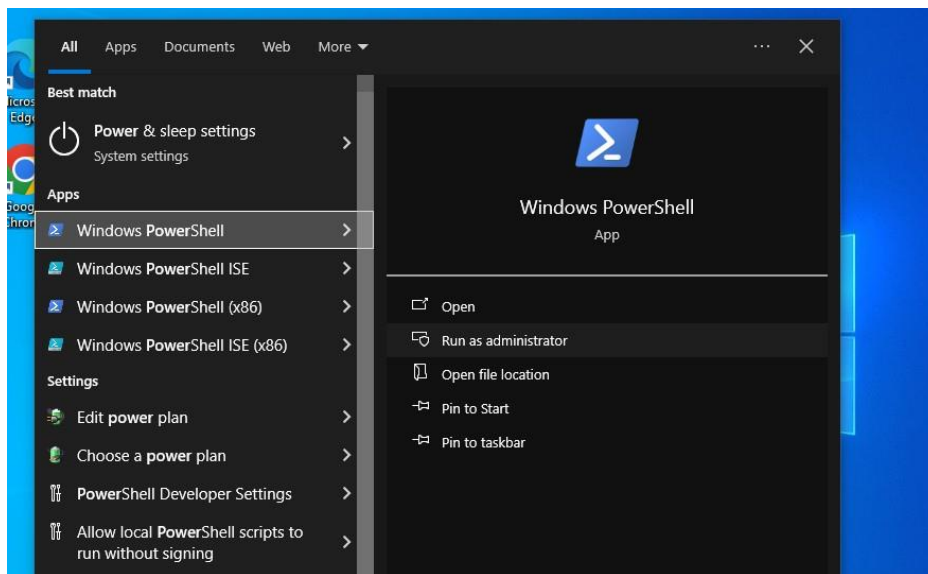
- Disable Tamper Protection and any Anti-Malware solution (e.g., Windows Defender), preferably via Group Policy.
 - <https://stackoverflow.com/questions/52174476/how-to-permanently-disable-win-with-gpo>
 - Open link in new tab
 - Open link in new window
 - Open link in incognito window
- Take a VM snapshot so you can always installation

FLARE-VM installation

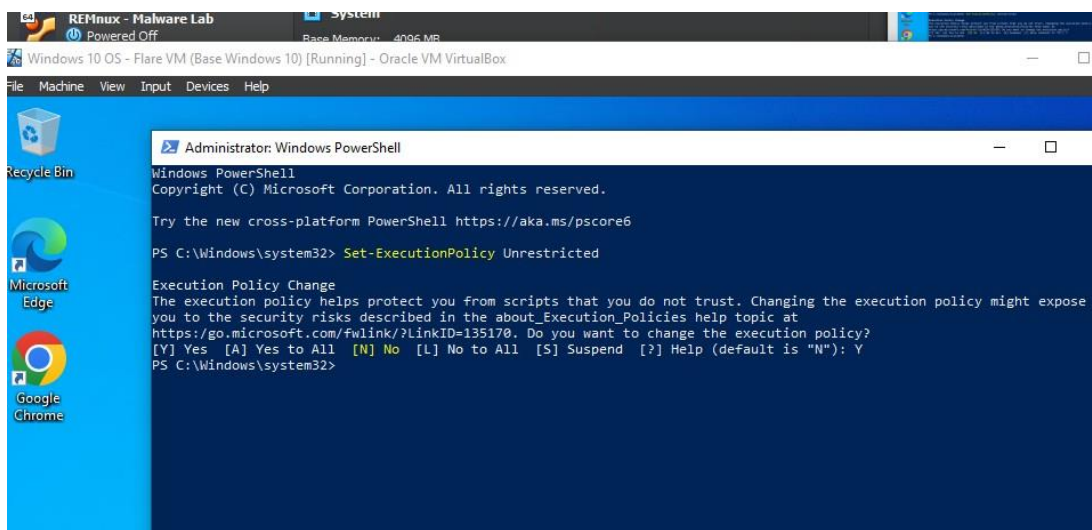
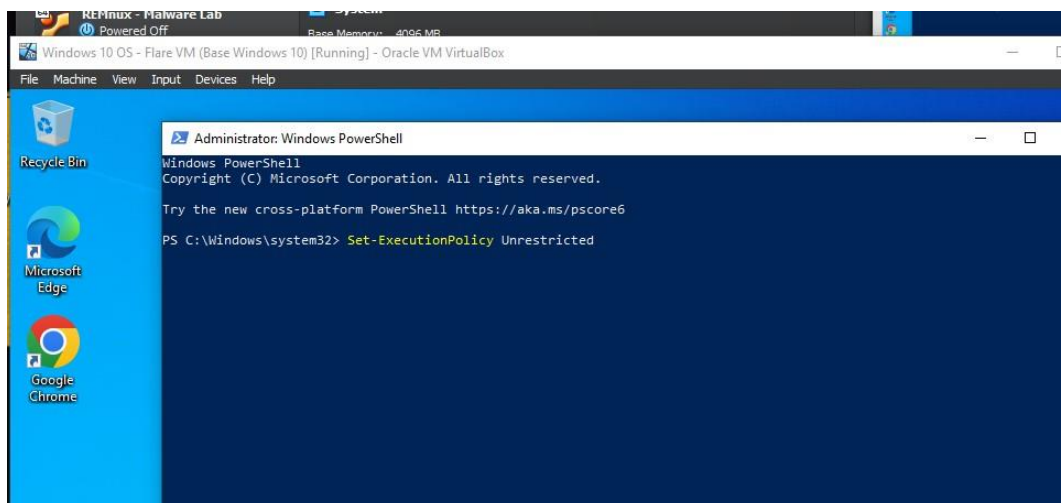
- Open a PowerShell prompt as administrator.
- Download the installation script `installer.ps1` to your Desktop.
 - `(New-Object net.webclient).DownloadFile('https://raw.githubusercontent.com/mandiant/flare-vm/main/install.ps1', '$([Environment]::GetFolderPath("Desktop"))\install.ps1')`
- Unblock the installation script:

STEP BY STEP MALWARE ANALYSIS LAB SET-UP

23. Open Windows PowerShell by run it as Administrator.

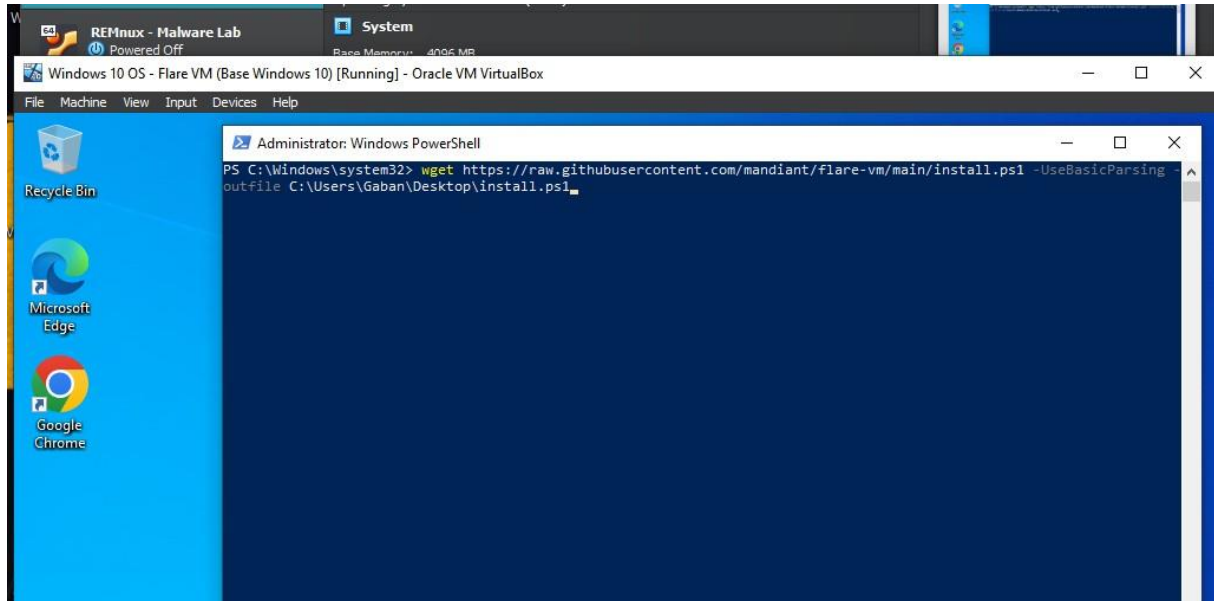


24. Then run this command Set-ExecutionPolicy Unrestricted



STEP BY STEP MALWARE ANALYSIS LAB SET-UP

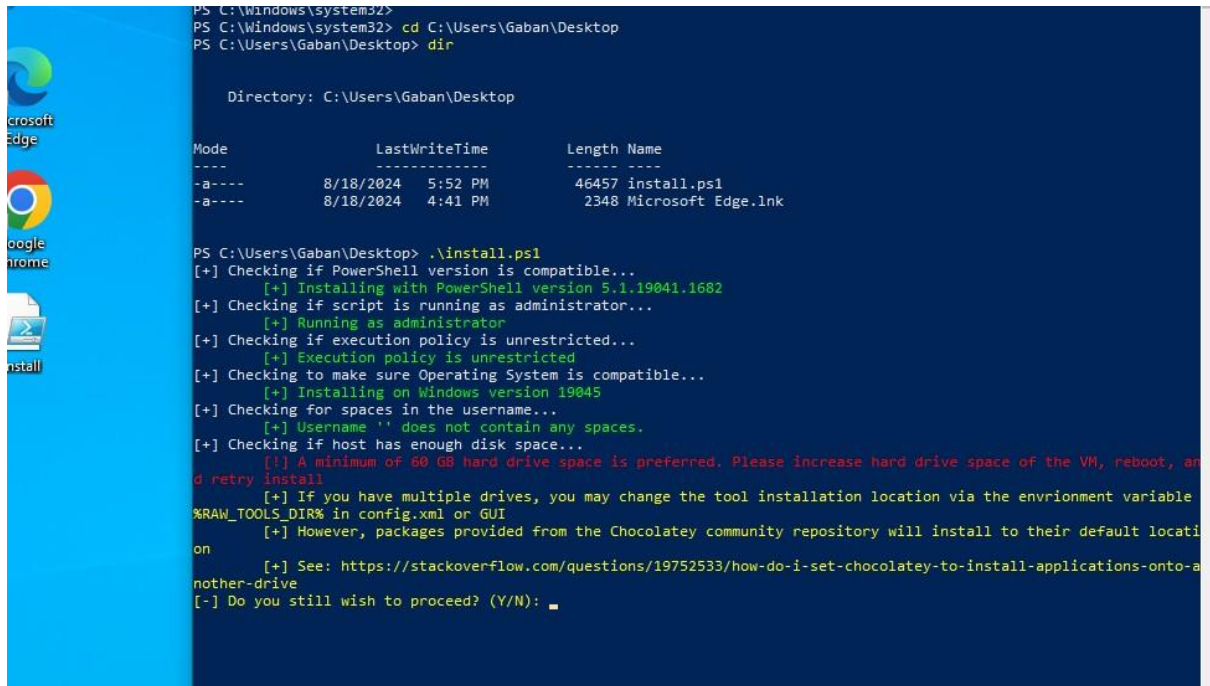
25. Run `wget https://raw.githubusercontent.com/mandiant/flare-vm/main/install.ps1 -UseBasicParsing -outfile <your desktop directory>`



After that you should see install file in the desktop.



26. Change directory to desktop - `cd <your desktop directory>` . Then run command `.\install.ps1`



```

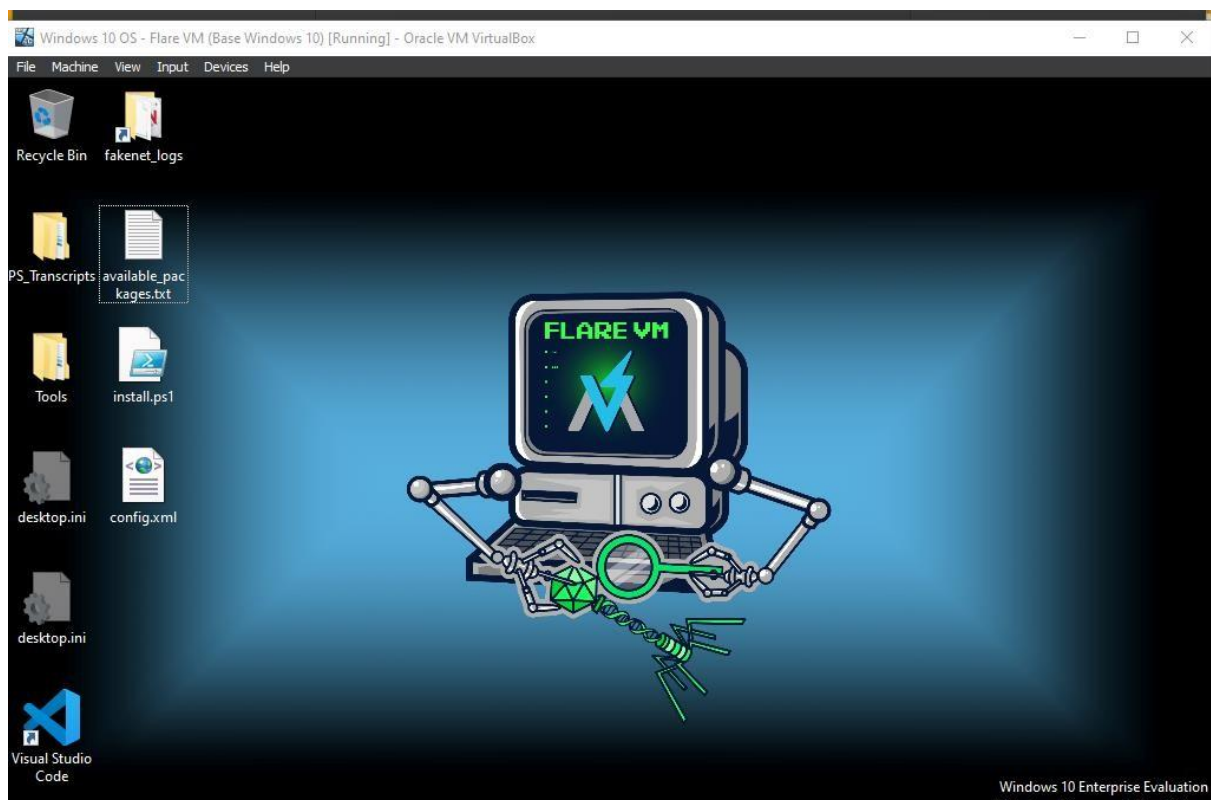
PS C:\Windows\system32>
PS C:\Windows\system32> cd C:\Users\Gaban\Desktop
PS C:\Users\Gaban\Desktop> dir

Directory: C:\Users\Gaban\Desktop

Mode                LastWriteTime         Length Name
----                -
-a----             8/18/2024   5:52 PM           46457 install.ps1
-a----             8/18/2024   4:41 PM           2348 Microsoft Edge.lnk

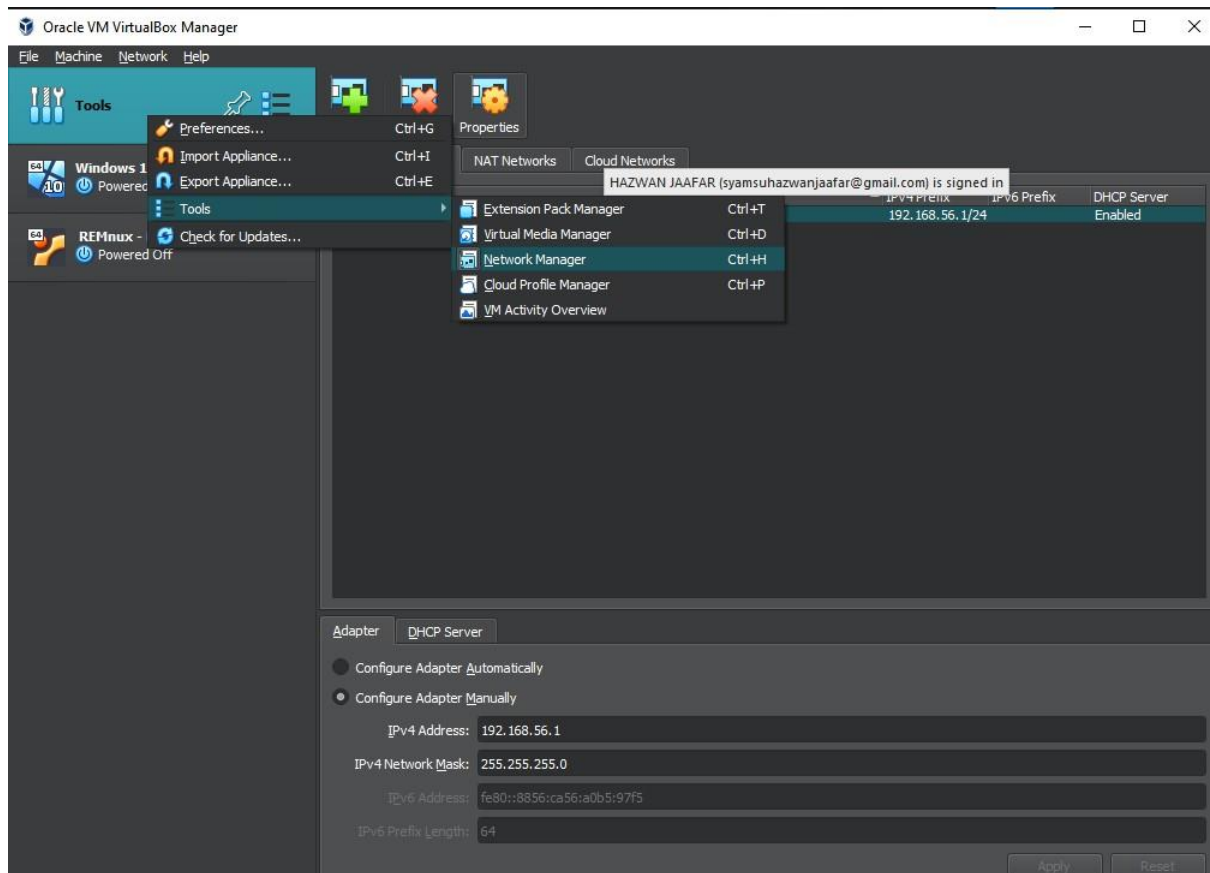
PS C:\Users\Gaban\Desktop> .\install.ps1
[+] Checking if PowerShell version is compatible...
[+] Installing with PowerShell version 5.1.19041.1682
[+] Checking if script is running as administrator...
[+] Running as administrator
[+] Checking if execution policy is unrestricted...
[+] Execution policy is unrestricted
[+] Checking to make sure Operating System is compatible...
[+] Installing on Windows version 19045
[+] Checking for spaces in the username...
[+] Username '' does not contain any spaces.
[+] Checking if host has enough disk space...
[!] A minimum of 60 GB hard drive space is preferred. Please increase hard drive space of the VM, reboot, and retry install
[+] If you have multiple drives, you may change the tool installation location via the environment variable %RAW_TOOLS_DIR% in config.xml or GUI
[+] However, packages provided from the Chocolatey community repository will install to their default location
[+] See: https://stackoverflow.com/questions/19752533/how-do-i-set-chocolatey-to-install-applications-onto-another-drive
[-] Do you still wish to proceed? (Y/N): _
  
```

27. This installation will take a long time, so allow it to complete the installation. Proceed with default installation till VM reboot and complete installation. Don't forget to take snapshot for base Flare VM. You should see new desktop feature once everything installed.



SPECIAL NETWORK CONFIGURATION

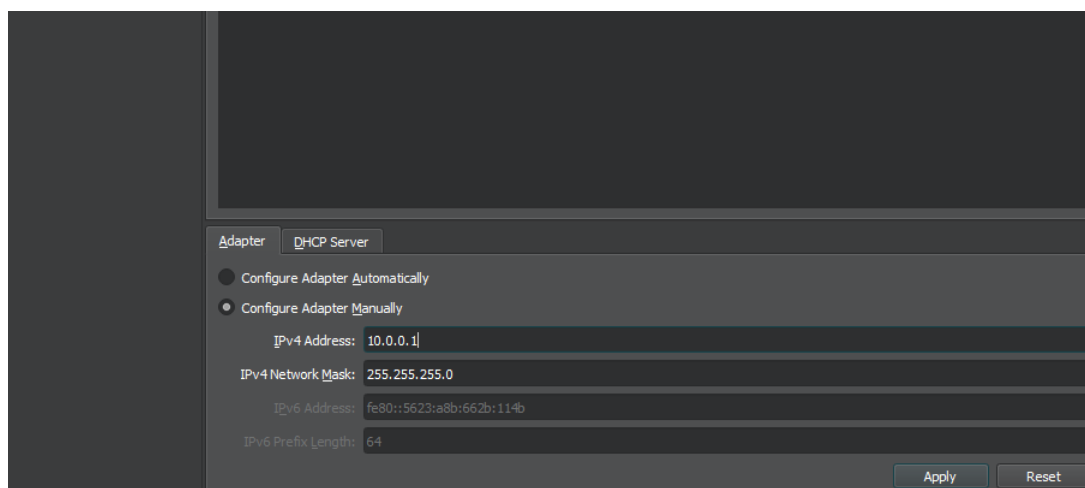
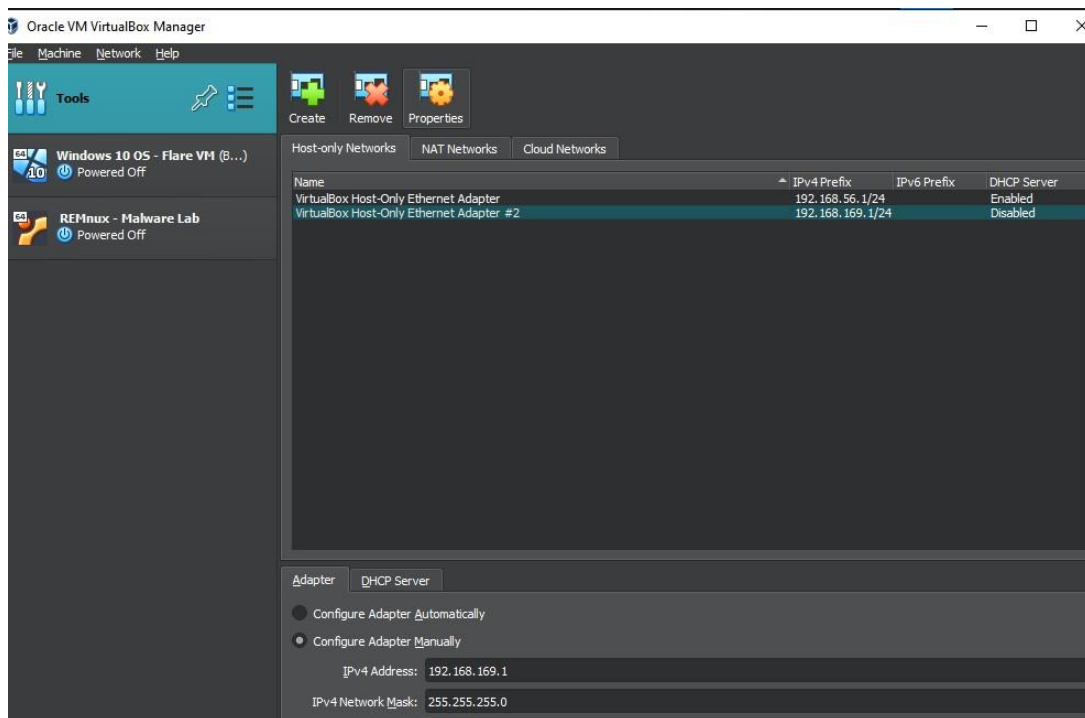
28. For special network configuration, go to VirtualBox - Tools - Network Manager.



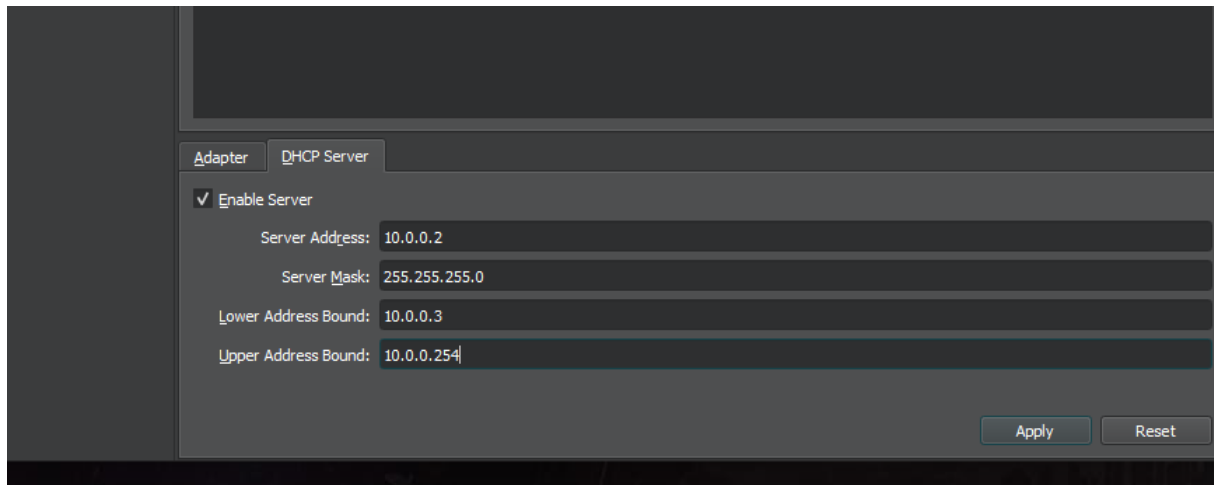
29. Then click Create to duplicate another adapter for this setting. So, both VM will only communicate with each other to prevent your host get infected with malware once detonated.

STEP BY STEP MALWARE ANALYSIS LAB SET-UP

30. Enable the DHCP Server and configure the adapter manually to 10.0.0.1 for IPV4



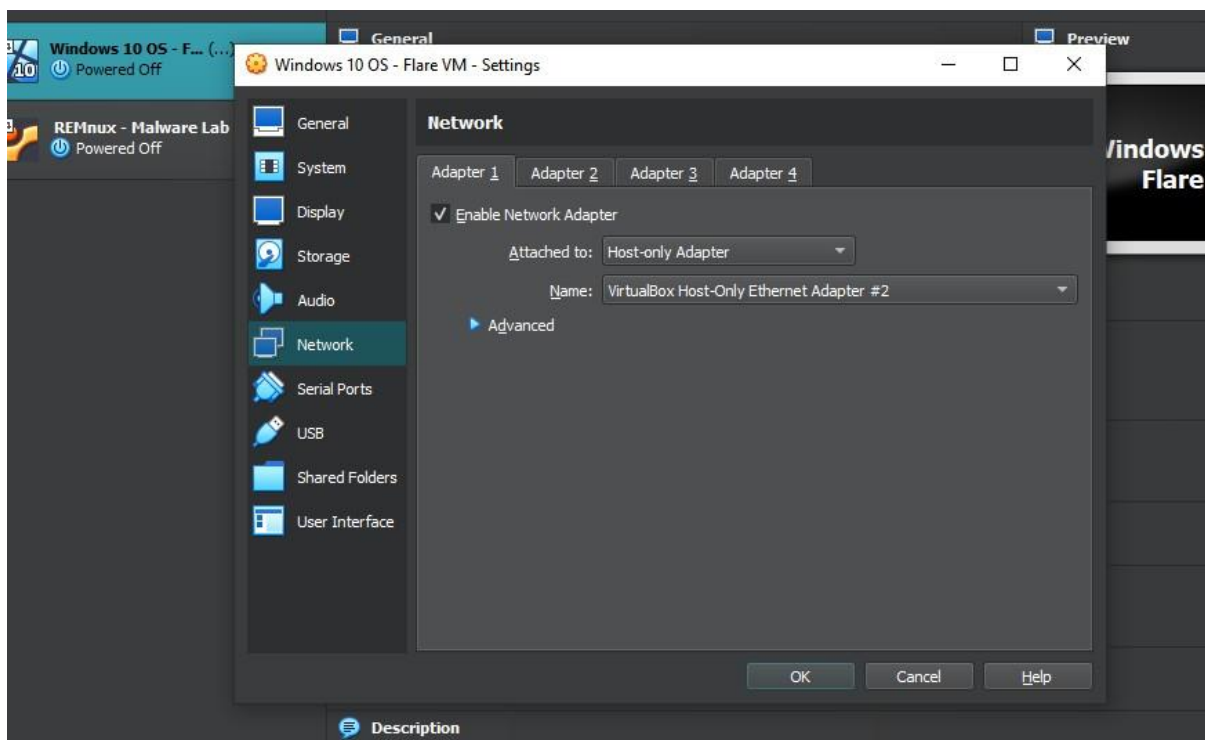
31. Then go to DHCP Server tab to change the Server Address to 10.0.0.2. Change Lower and Upper accordingly as well. Click apply



NETWORK CONFIGURATION FOR VM

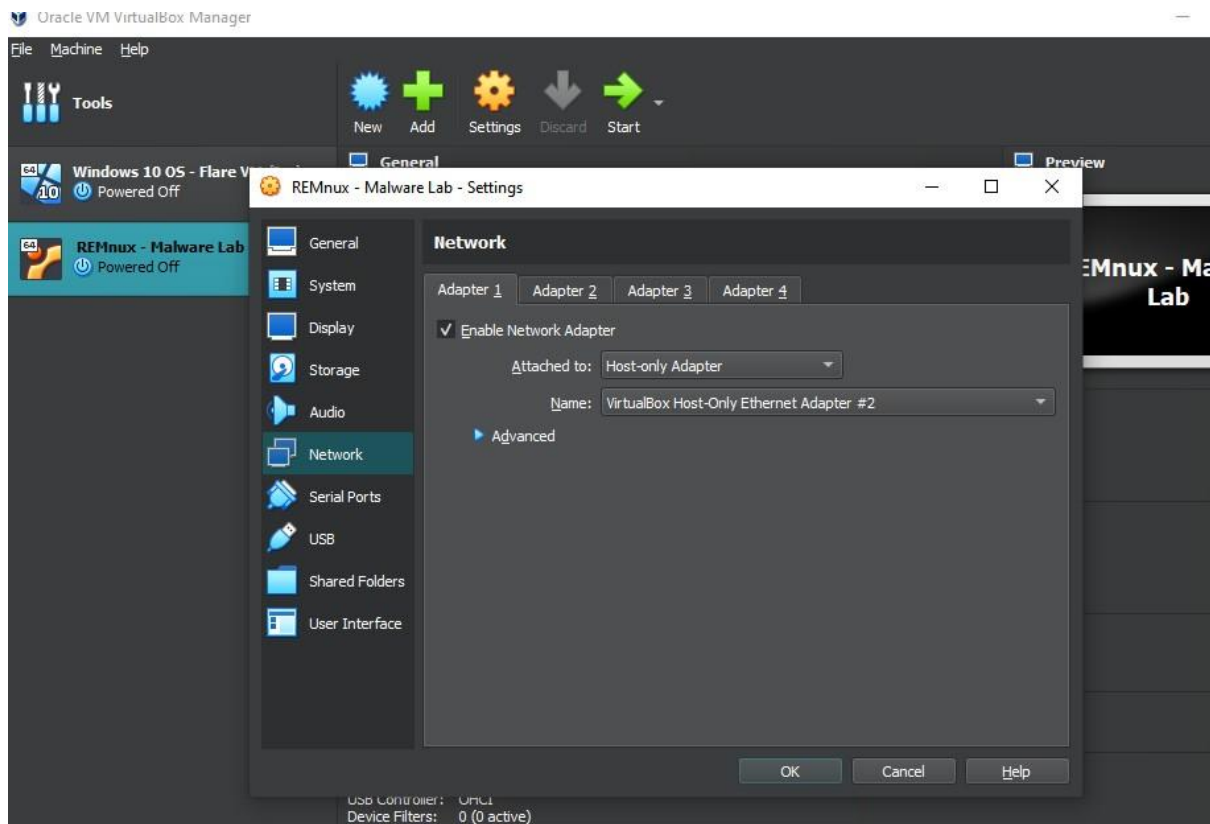
Windows 10 - Flare VM

32. Go to Settings then Network, change Attached to Host Only Adapter. For safety purpose check another Adapter as well. Then click OK

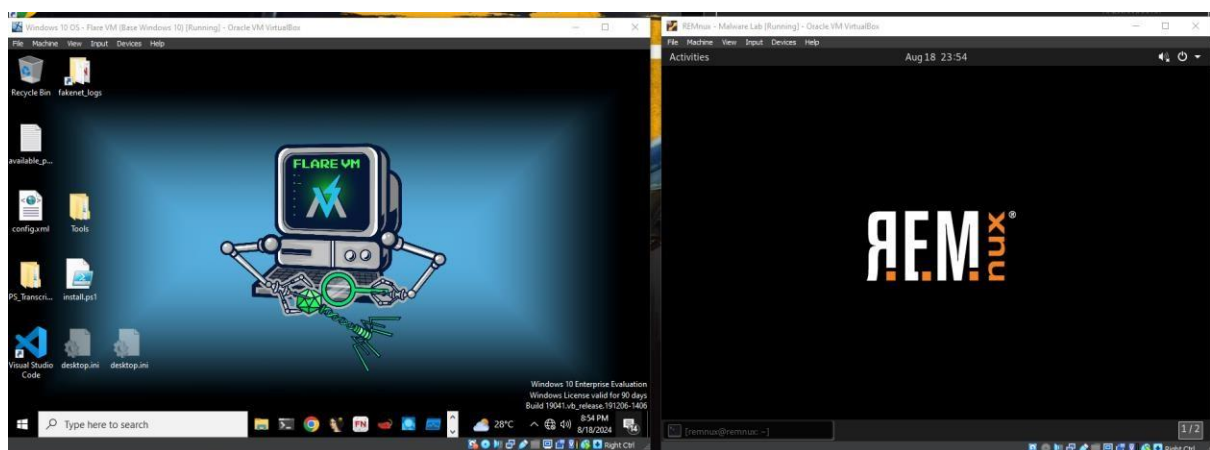


REMnux VM

33. Go to Settings then Network, change Attached to Host Only Adapter. For safety purpose check other Adapter as well. Then click OK



34. Power ON both VM to check their connectivity

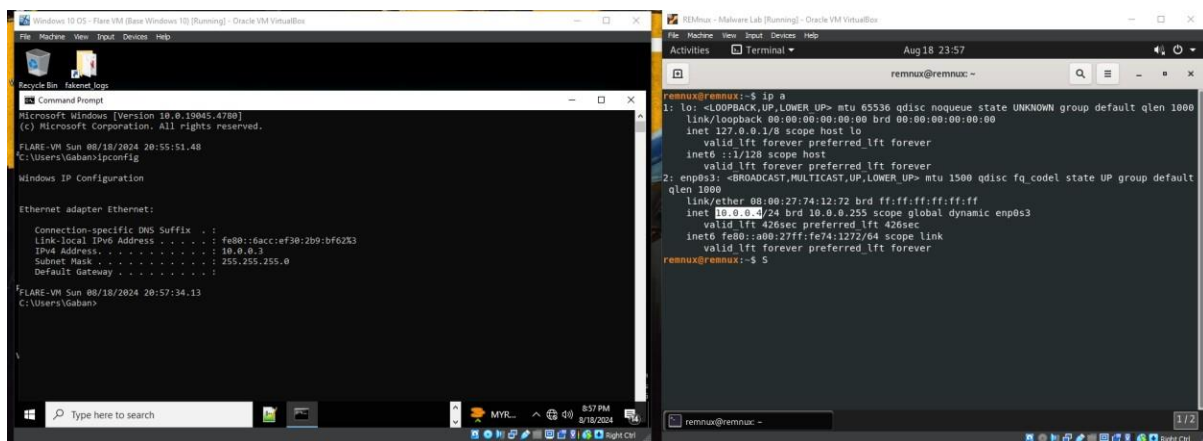


Launch Terminal for both VM

Check adapter internet setting in REMnux VM and Flare VM.

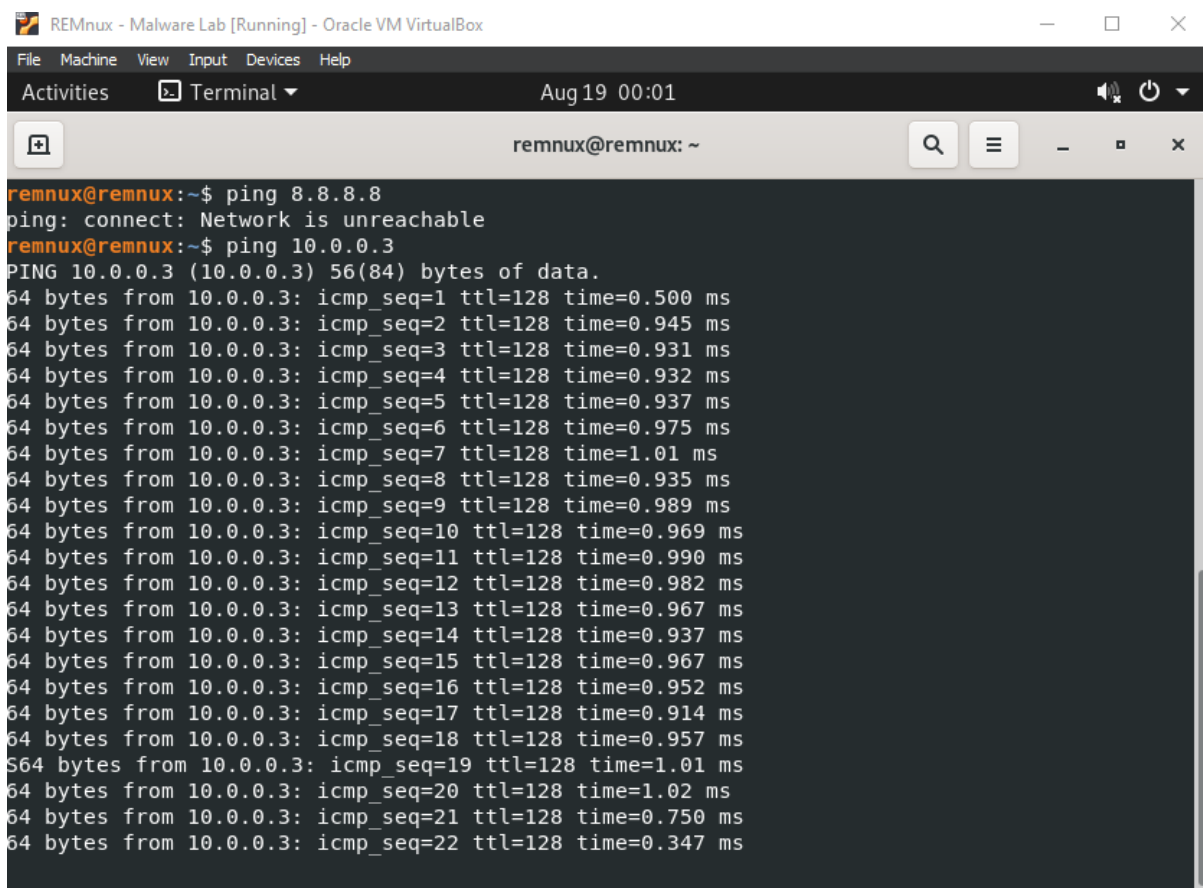
STEP BY STEP MALWARE ANALYSIS LAB SET-UP

By running the command `ip a` for REMnux VM and `ipconfig` for Flare VM.



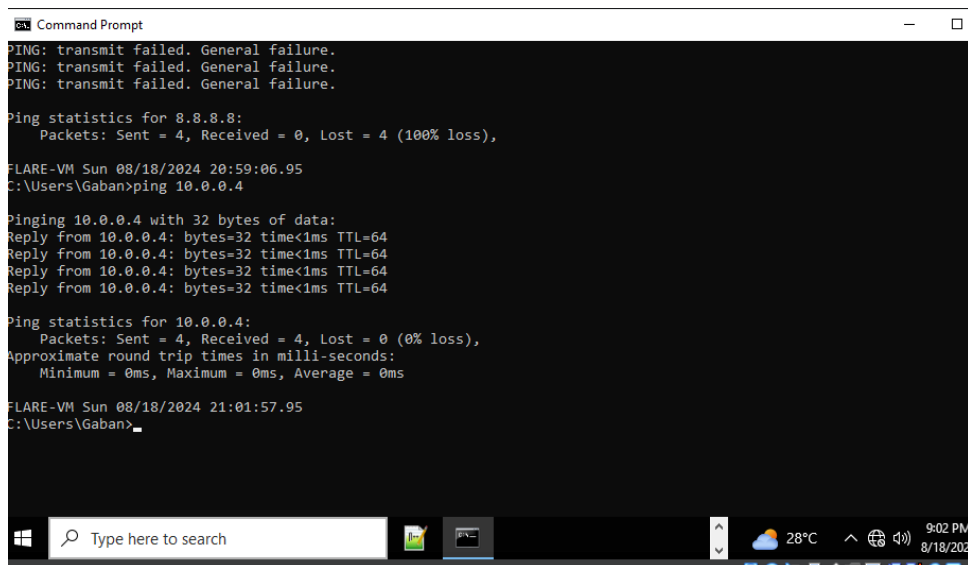
35. You also can try to run ping command for both VM to 8.8.8.8 to check the connection.

Then ping each other VM to see if they can communicate with each other



STEP BY STEP MALWARE ANALYSIS LAB SET-UP

Windows - Flare VM



```
Command Prompt
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

FLARE-VM Sun 08/18/2024 20:59:06.95
C:\Users\Gaban>ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:
Reply from 10.0.0.4: bytes=32 time<1ms TTL=64
Reply from 10.0.0.4: bytes=32 time<1ms TTL=64
Reply from 10.0.0.4: bytes=32 time<1ms TTL=64
Reply from 10.0.0.4: bytes=32 time<1ms TTL=64

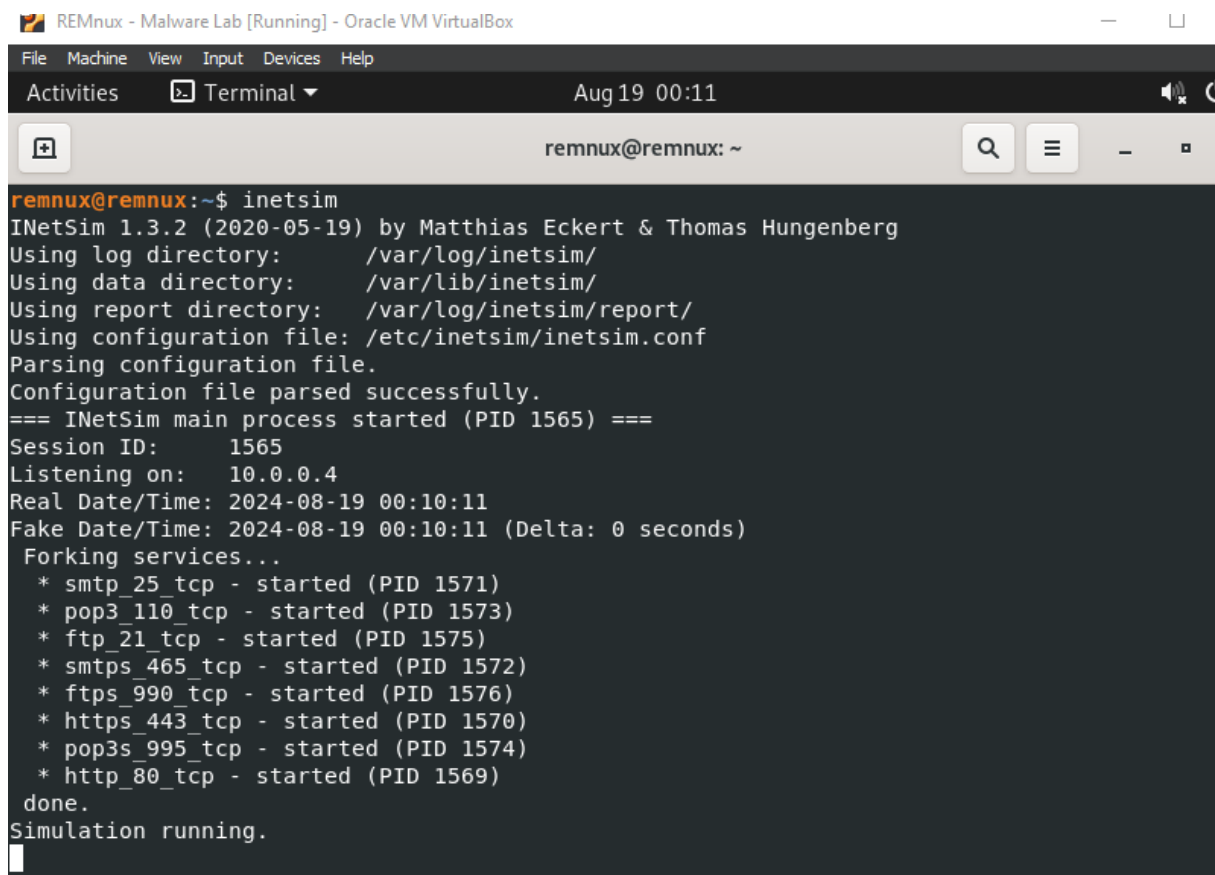
Ping statistics for 10.0.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

FLARE-VM Sun 08/18/2024 21:01:57.95
C:\Users\Gaban>
```

SET UP INETSIM

Internet Simulator

36. Open Terminal then run inetsim to check the services. All up and running except DNS server.



```
REMnux - Malware Lab [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Aug 19 00:11
remnux@remnux: ~

remnux@remnux:~$ inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 1565) ===
Session ID: 1565
Listening on: 10.0.0.4
Real Date/Time: 2024-08-19 00:10:11
Fake Date/Time: 2024-08-19 00:10:11 (Delta: 0 seconds)
Forking services...
* smtp_25_tcp - started (PID 1571)
* pop3_110_tcp - started (PID 1573)
* ftp_21_tcp - started (PID 1575)
* smtps_465_tcp - started (PID 1572)
* ftps_990_tcp - started (PID 1576)
* https_443_tcp - started (PID 1570)
* pop3s_995_tcp - started (PID 1574)
* http_80_tcp - started (PID 1569)
done.
Simulation running.
```

37. Hence terminate inetsim CTRL + C. Run sudo nano /etc/inetsim/inetsim.conf

```

REMnux - Malware Lab [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Aug19 00:16
remnux@remnux: ~
GNU nano 4.8 /etc/inetsim/inetsim.conf Modified
#####
#
# INetSim configuration file
#
#####
# Main configuration
#####
#####
# start_service
#
# The services to start
#
# Syntax: start_service <service name>
#
# Default: none
#
# Available service names are:
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
[ Read 1932 lines ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line
remnux@remnux: ~ 1/2

```

*Uncommented start_service dns and

```

#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 0.0.0.0
^G Get Help ^O Write Out ^W Where Is ^K Cut Text
^X Exit ^R Read File ^\ Replace ^U Paste Text

```

```
#####
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
dns_default_ip      10.0.0.4

^G Get Help      ^O Write Out     ^W Where Is      ^K Cut Text      ^J
^X Exit          ^R Read File     ^\ Replace       ^U Paste Text    ^T
```

38. Open another Terminal to run ip a to ensure the ip address of REMnux box.

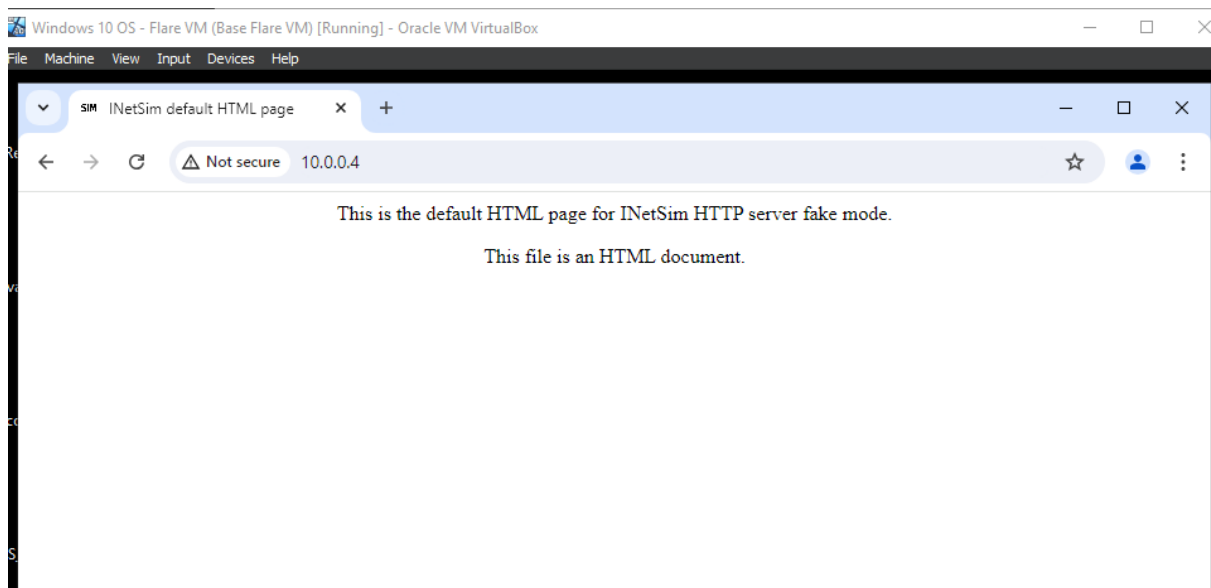
CNTRL + O then CNTRL + X to save and exit. Run inetsim again to see the changes.

```
remnux@remnux:~$ inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 1737) ===
Session ID:      1737
Listening on:    10.0.0.4
Real Date/Time:  2024-08-19 00:32:14
Fake Date/Time: 2024-08-19 00:32:14 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 1741)
* smtps_465_tcp - started (PID 1745)
* smtp_25_tcp - started (PID 1744)
* ftp_21_tcp - started (PID 1748)
* ftps_990_tcp - started (PID 1749)
* https_443_tcp - started (PID 1743)
* pop3s_995_tcp - started (PID 1747)
* pop3_110_tcp - started (PID 1746)
* http_80_tcp - started (PID 1742)
done.
Simulation running.
```

Go to Flare VM, then open browser key in the REMnux ip address to check.

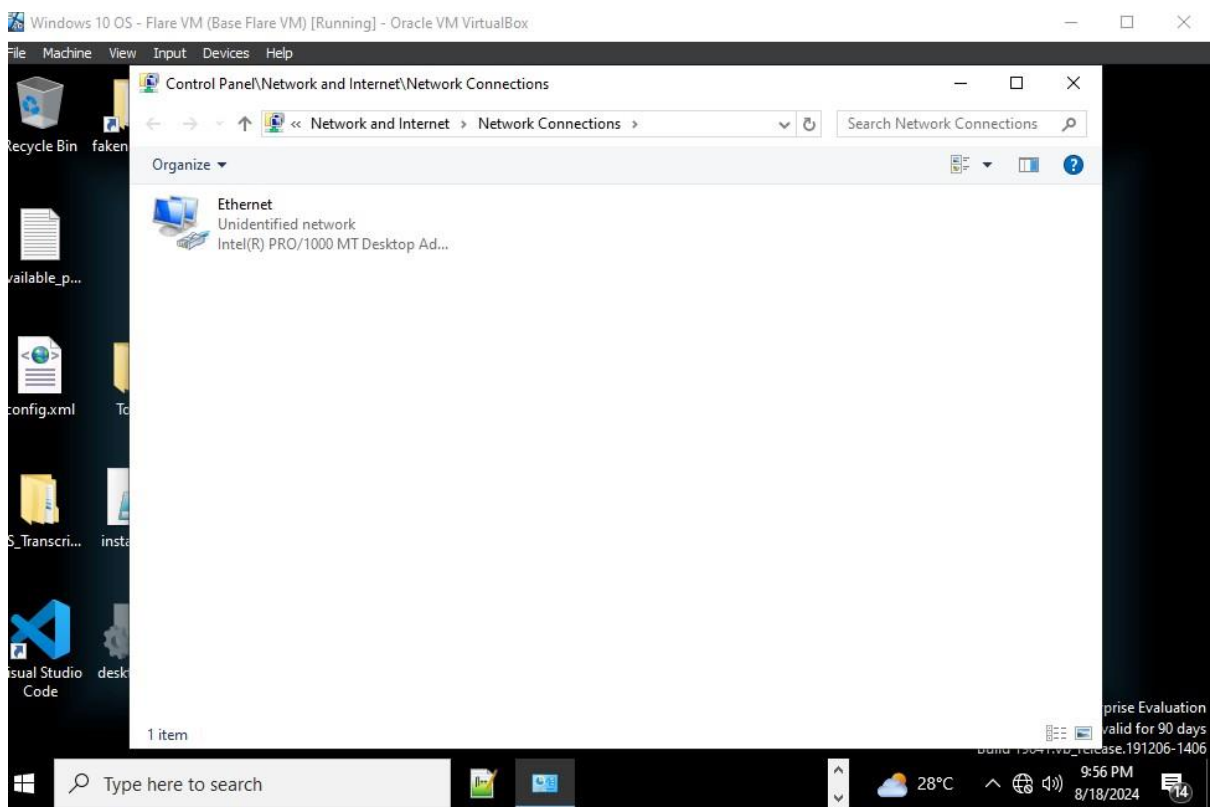
STEP BY STEP MALWARE ANALYSIS LAB SET-UP

39. It shows the default HTML page or HTTP server fake mode is successful.



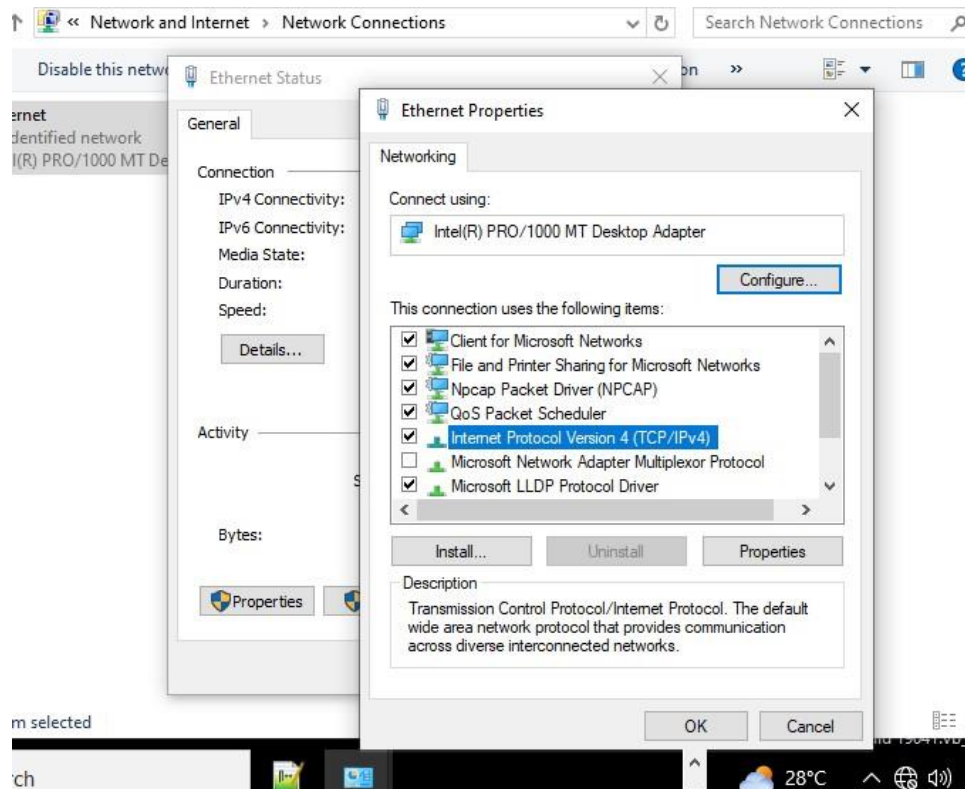
LAST STEP

40. In Flare VM, go to START menu and open Network Connection



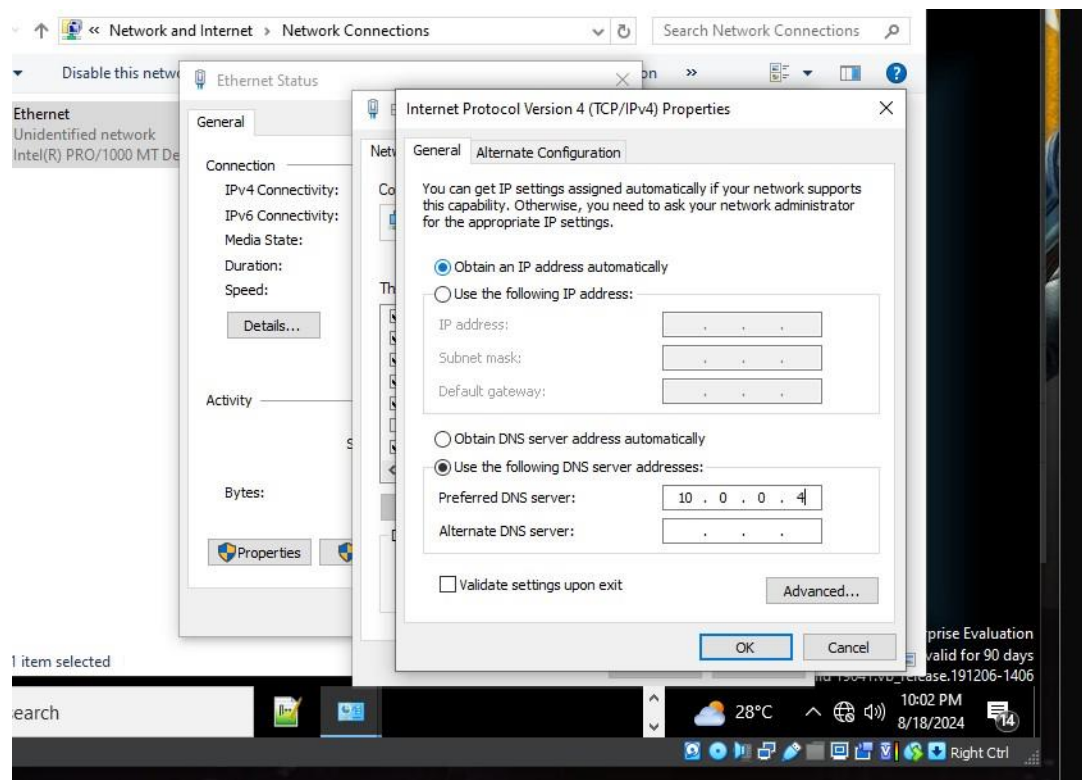
Double click then open Properties

STEP BY STEP MALWARE ANALYSIS LAB SET-UP



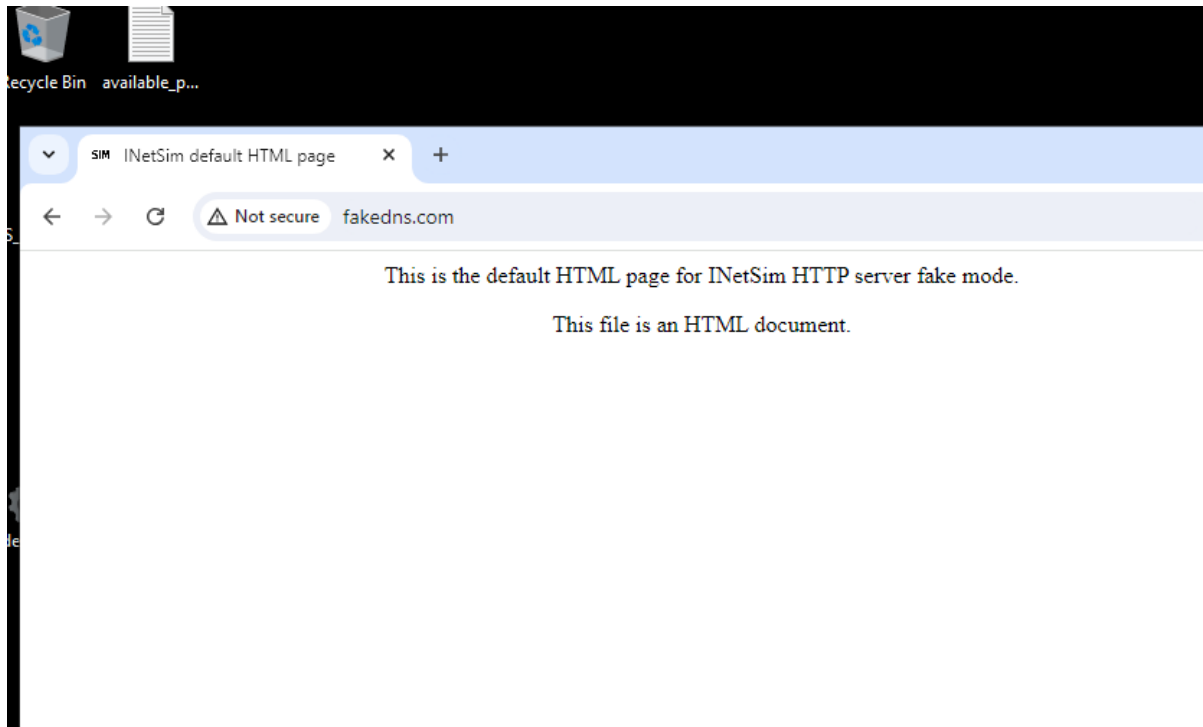
41. Choose Internet Protocol Version 4, click Properties. Configure as below picture:

Set the IP address for DNS server to the INETSIM in the REMnux Box.



Click OK and EXIT.

42. With this by typing any web address in browser, it will direct you to the Fake HTML page provided INETSIM is running in the REMnux Box.



Now you are ready to play with some malwares!!!

References:

<https://www.youtube.com/watch?v=qA0YcYMRWyl&t=3224s>

<https://www.youtube.com/watch?v=i8dCyy8WMKY>