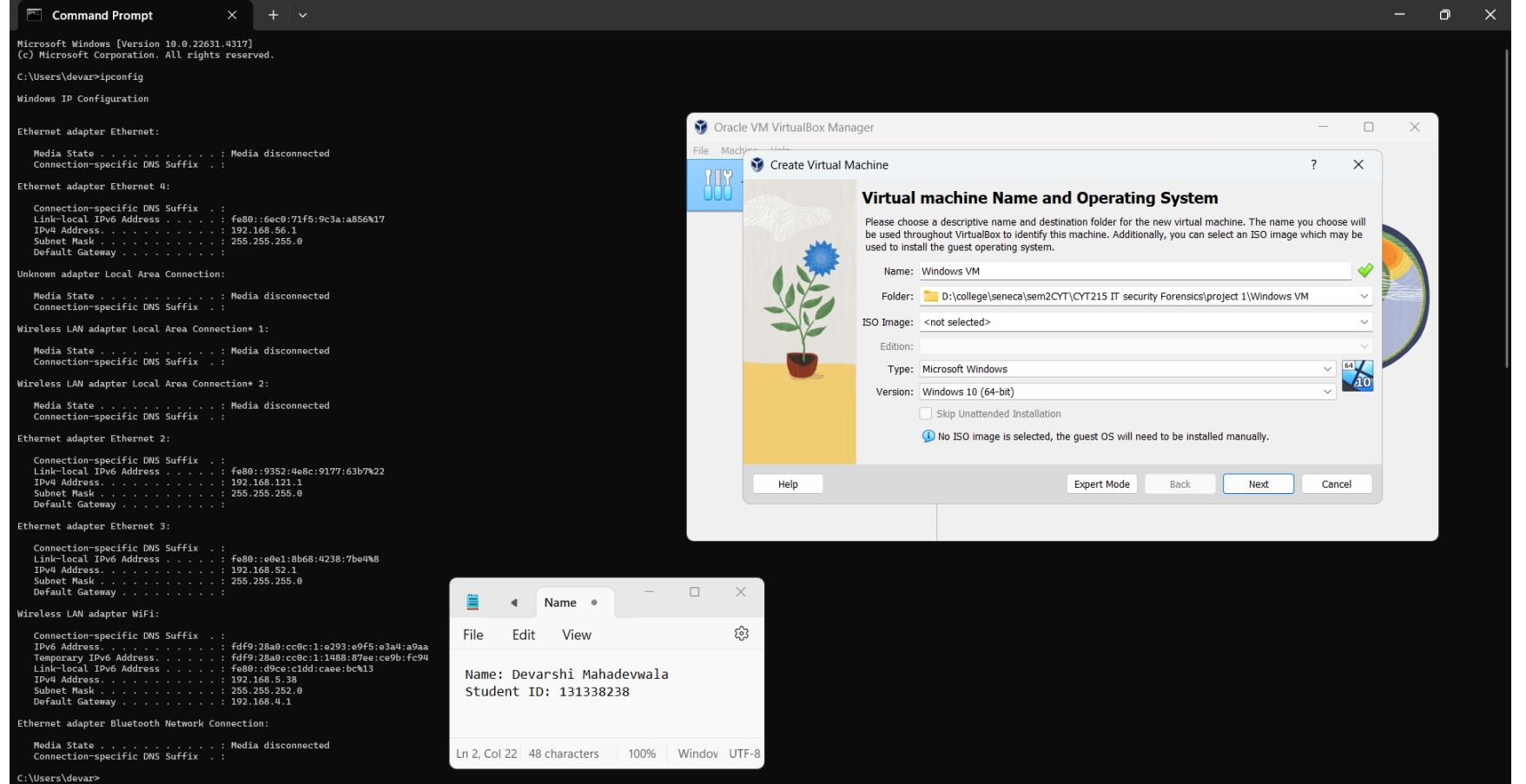


Name ↓				
Devarshi Mahadevwala				
Name	Project1: Build Your own Forensic Workstation			
Main Goal	Set up your functional forensic workstation to conduct forensics investigations using variety of popular tools			
Instructions	<ul style="list-style-type: none"> <li>• It is an Individual assignment. Put your name + Student ID in the empty spaces above.</li> <li>• Submit via the BB relevant link ONLY. NO submission via email please. Be sure to submit the final version file ONLY.</li> <li>• Show me genuine signs of your work is done on your machine. This includes: <ul style="list-style-type: none"> <li>◦ Screenshots that show your desktop background with Date/Time</li> <li>◦ Show me a pop-up bx that shows "your name + IP."</li> <li>◦ Show your logged in account, if applicable</li> <li>◦ Optional: Show your photo.</li> </ul> </li> <li>• Use this same template to include your work in the specified fields below. Submit in PDF.</li> <li>• Submit your report name with the name: CYT215-Project1-Student Name &amp; ID</li> </ul>			
Students Work required for this activity	<ol style="list-style-type: none"> <li>1. You will follow instructions to setup your own forensics workstation on your machine.</li> <li>2. You will check that your forensics workstation is functioning.</li> <li>3. You will use your workstation for memory &amp; malware analysis.</li> <li>4. You will Prepare Your Target System (your own machine). You will Build Your basic Lab.</li> </ol>			
How to start	<ul style="list-style-type: none"> <li>• Read thoroughly &amp; follow the instructions mentioned in this link. The instructions will guide you to a step-by-step of how you complete your work successfully <a href="https://bluecapesecurity.com/build-your-forensic-workstation/">https://bluecapesecurity.com/build-your-forensic-workstation/</a></li> <li>• Take an image of your machine memory. Use this link for guidance: <a href="https://dfirmadness.com/case-001-memory-analysis/">https://dfirmadness.com/case-001-memory-analysis/</a></li> <li>• You can use any installed tool or focus on common tools for memory analysis e.g.: Volatility; Cyber Triage; Rekall; Redline;</li> </ul>			
Important	<ul style="list-style-type: none"> <li>• Your target system should be your own machine</li> </ul>			
Students Reports	<ol style="list-style-type: none"> <li>1. Take screenshots of all your works steps</li> <li>2. Show you have practiced 3 relevant tools to investigate memory.</li> <li>3. Write a detailed report of personal learning experience (free writing).</li> </ol>			
Grading Rubrics	<ul style="list-style-type: none"> <li>• 5 Marks for completing the setup of your forensics workstation successfully.</li> <li>• 5 Marks for using your workstation for memory analysis. At least, use 3 tool/memory analysis.</li> <li>• 2 Marks for your detailed personal learning experience (free writing)</li> </ul>			

Student work	<p>First, we need to setup the forensics lab along with the tools and necessary applications to conduct memory analysis. For this, I have setup a windows virtual machine environment. I have downloaded FTK imager to capture memory image from my windows machine and run memory analysis on that image from several applications like volatility, cyber triage, and redline. I have used windows VM in VMware, but below are the steps to setup windows VM in virtualbox.</p>  <p>The screenshot displays three windows:</p> <ul style="list-style-type: none"> <li><b>Command Prompt</b>: Shows the output of the ipconfig command, listing various network adapters (Ethernet, Wireless LAN, WiFi, Bluetooth) with their connection status, IP addresses, and subnet masks.</li> <li><b>Oracle VM VirtualBox Manager</b>: A dialog box for creating a new virtual machine. It asks for the VM name (Windows VM), folder (D:\college\seneca\sem2CYT\CYT215 IT security Forensics\project 1\Windows VM), ISO image (not selected), edition (Microsoft Windows), and version (Windows 10 (64-bit)).</li> <li><b>Notepad</b>: A text editor containing student information: Name: Devarshi Mahadevwala and Student ID: 131338238.</li> </ul>
--------------	--

Command Prompt

```
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Users\devar>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : 

Ethernet adapter Ethernet 4:
  Connection-specific DNS Suffix . . . . . :
  Link-local IPv6 Address . . . . . : fe80::6ec0:71f5:9c3a:a856%17
  IPv4 Address . . . . . : 192.168.56.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 

Unknown adapter Local Area Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : 

Wireless LAN adapter Local Area Connection* 1:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : 

Wireless LAN adapter Local Area Connection* 2:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : 

Ethernet adapter Ethernet 2:
  Connection-specific DNS Suffix . . . . . :
  Link-local IPv6 Address . . . . . : fe80::9352:4e8c:9177:63b7%22
  IPv4 Address . . . . . : 192.168.121.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 

Ethernet adapter Ethernet 3:
  Connection-specific DNS Suffix . . . . . :
  Link-local IPv6 Address . . . . . : fe80::e0e1:8b68:4238:7be4%8
  IPv4 Address . . . . . : 192.168.52.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 

Wireless LAN adapter WiFi:
  Connection-specific DNS Suffix . . . . . :
  IPv6 Address . . . . . : fdf9:28a0:cc0c:1:e293:e9f5:e3a4:a9aa
  Temporary IPv6 Address . . . . . : fdf9:28a0:cc0c:1:1488:87e0:ce9b:fc94
  Link-local IPv6 Address . . . . . : fe80::d9ce:c1dd:caee:bc%13
  IPv4 Address . . . . . : 192.168.5.38
  Subnet Mask . . . . . : 255.255.252.0
  Default Gateway . . . . . : 192.168.4.1

Ethernet adapter Bluetooth Network Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : 

C:\Users\devar>
```

Oracle VM VirtualBox Manager

Create Virtual Machine

**Hardware**

You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

Base Memory: 4096 MB (4 MB to 8192 MB)

Processors: 3 (1 CPU to 12 CPUs)

Enable EFI (special OSes only)

Help Back Next Cancel

Name: Devarshi Mahadevawala  
Student ID: 131338238

Ln 2, Col 22 48 characters 100% Window UTF-8

Specify the details of the virtual machine hardware. I have selected 3 processors and 4GB RAM for my windows virtual machine.

Microsoft Windows [Version 10.0.22631.4317]  
 (C) Microsoft Corporation. All rights reserved.

```
C:\Users\devar>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 4:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::6ec0:71f5:9c3a:a856%17
  IPv4 Address . . . . . : 192.168.56.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Unknown adapter Local Area Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 1:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 2:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 2:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::9352:4e8c:9177:6b7%22
  IPv4 Address . . . . . : 192.168.121.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Ethernet adapter Ethernet 3:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::e0e1:8b68:4238:7b%4
  IPv4 Address . . . . . : 192.168.52.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Wireless LAN adapter WiFi:
  Connection-specific DNS Suffix . :
  IPv4 Address . . . . . : fdf9:28a0:cc0c:1:e293:e9f5:e3a4:a9aa
  Temporary IPv6 Address . . . . . : fdf9:28a0:cc0c:1:1488:87e:ce9b:fc%13
  Link-local IPv6 Address . . . . . : fe80:d9ce:c1d:caee:bc%13
  IPv4 Address . . . . . : 192.168.5.38
  Subnet Mask . . . . . : 255.255.252.0
  Default Gateway . . . . . : 192.168.4.1

Ethernet adapter Bluetooth Network Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :
```

C:\Users\devar>

**Virtual Hard disk**

If you wish you can add a virtual hard disk to the new machine. You either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

Create a Virtual Hard Disk Now

Disk Size:  50.00 GB

Pre-allocate Full Size

Use an Existing Virtual Hard Disk File

17763.737.amd64fre.rs5\_release\_svc\_refresh.190906-2324\_server\_serverdatacentereval\_e

Do Not Add a Virtual Hard Disk

Back Next Cancel

A virtual hard disk needs to be specified so that the virtual machine has memory storage.

Oracle VM VirtualBox Manager

Create Virtual Machine

**Summary**

The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.

Machine Name and OS Type	Windows VM
Machine Name	D:\college\seneca\sem2CYT\CYT215 IT security Forensics\project 1\Wind...
Machine Folder	
ISO Image	
Guest OS Type	Windows 10 (64-bit)
<b>Hardware</b>	
Base Memory	4096
Processor(s)	3
EFI Enable	false
<b>Disk</b>	
Attached Disk	D:\college\seneca\sem2CYT\CYT215 IT security Forensics\project 1\Wind...

Help Back Finish Cancel

```

Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Users\devar>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 4:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::6ec0:71f5:9c3a:a856%17
  IPv4 Address . . . . . : 192.168.56.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Unknown adapter Local Area Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection 1:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection 2:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 2:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::9352:4e8c:9177:6b7%22
  IPv4 Address . . . . . : 192.168.121.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Ethernet adapter Ethernet 3:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::e0e1:8b68:4238:7be4%8
  IPv4 Address . . . . . : 192.168.52.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

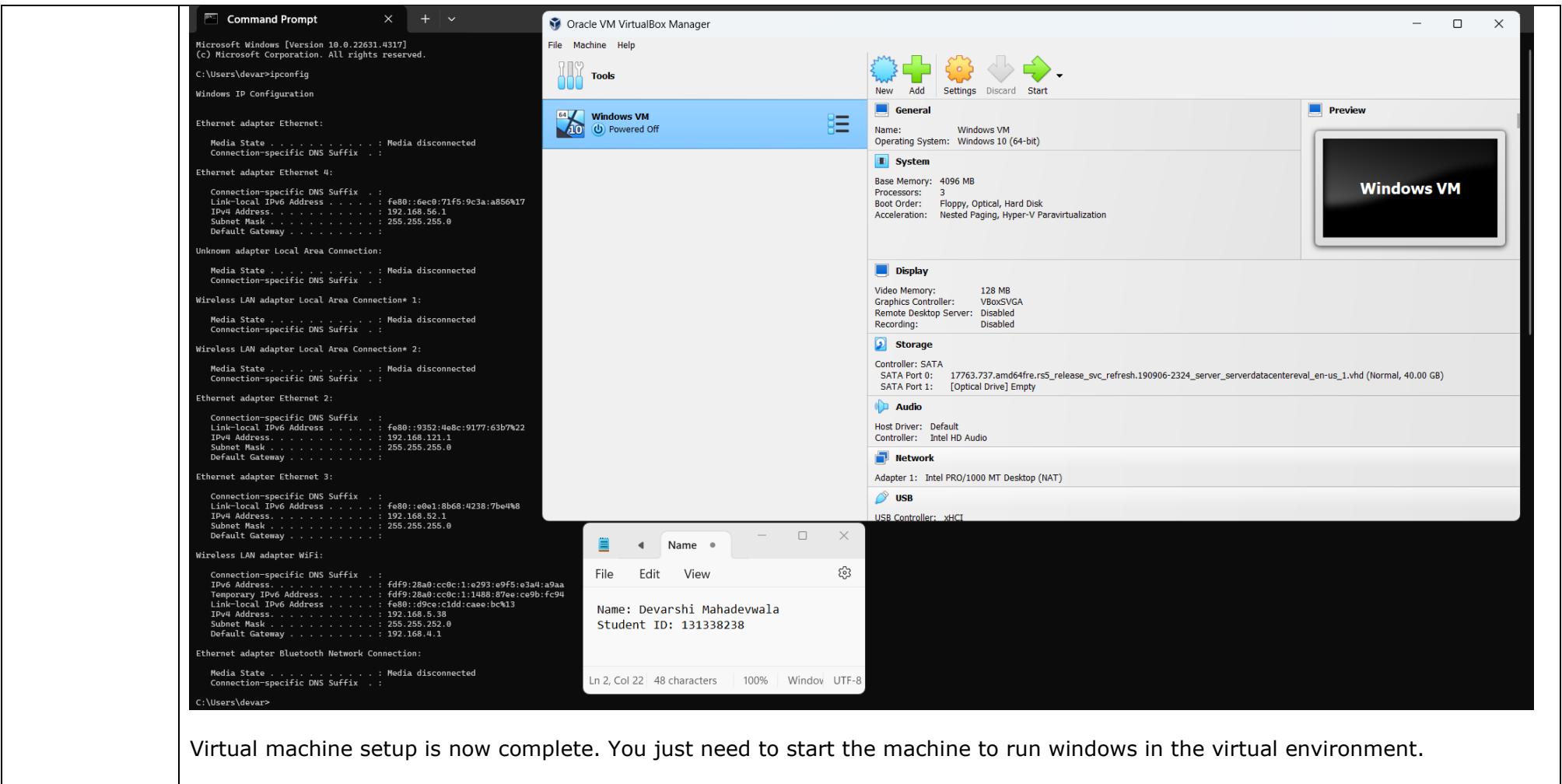
Wireless LAN adapter WiFi:
  Connection-specific DNS Suffix . :
  IPv6 Address . . . . . : fdf9:28a0:cc0c:1:e293:e9f5:e3a4:a9aa
  Temporary IPv6 Address . . . . . : fdf9:28a0:cc0c:1:1488:87ee:ce9b:fc94
  Link-local IPv6 Address . . . . . : fe80::d9ce:11dd:caee:bc%3
  IPv4 Address . . . . . : 192.168.5.38
  Subnet Mask . . . . . : 255.255.252.0
  Default Gateway . . . . . : 192.168.4.1

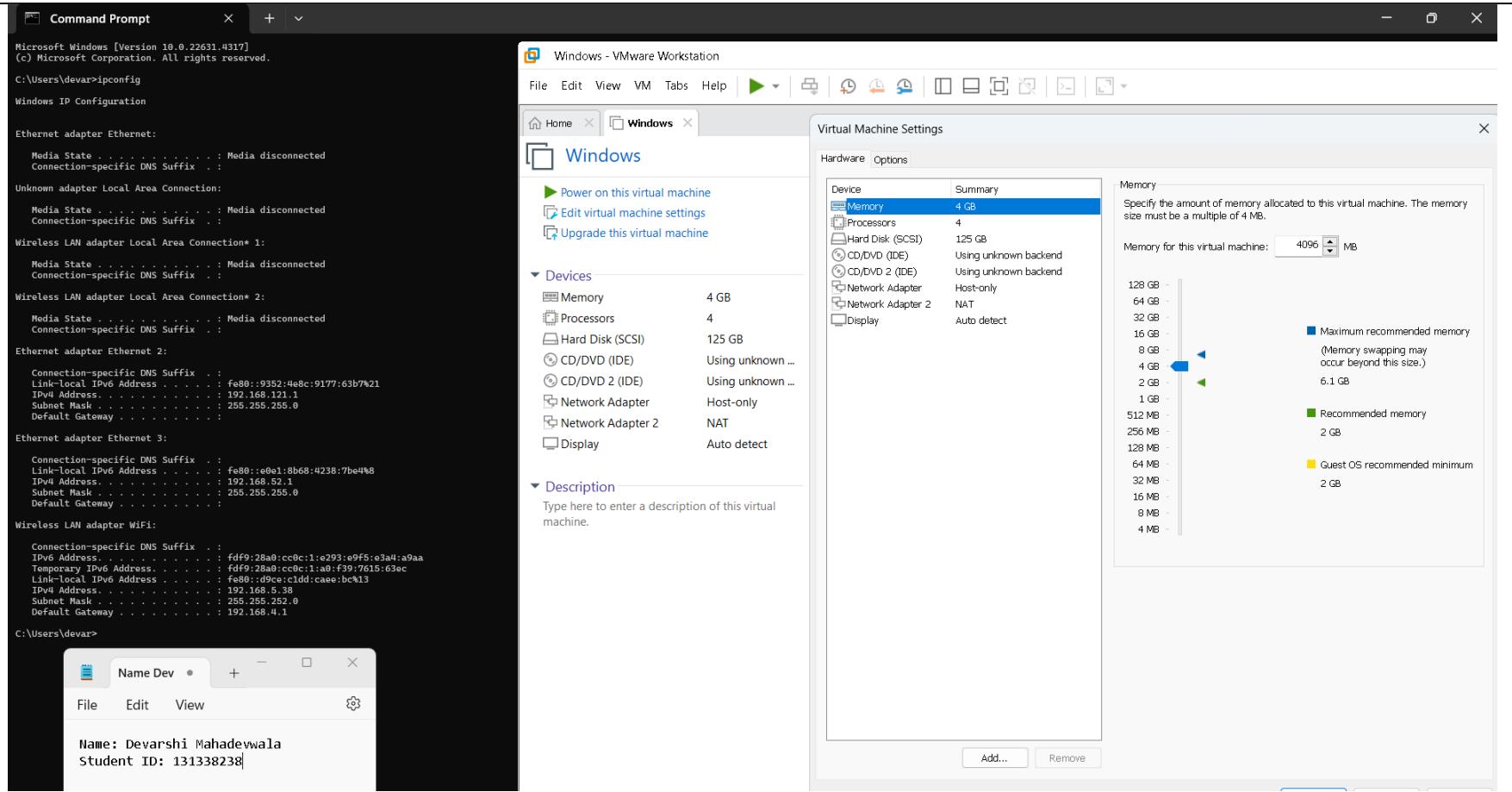
Ethernet adapter Bluetooth Network Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

C:\Users\devar>

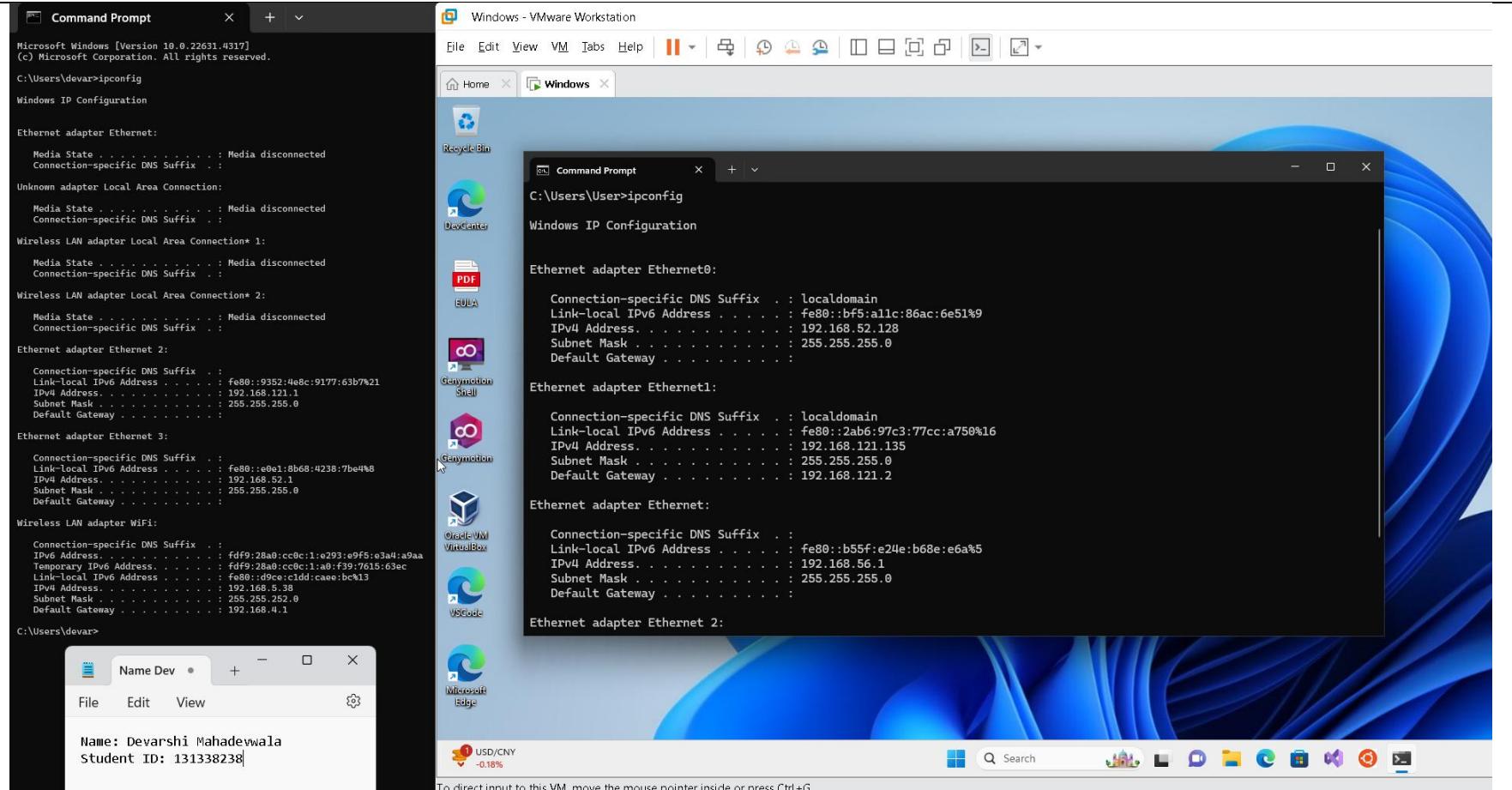
```

Finally, check the specifics of the virtual machine in the summary and if it is to your liking, finish the setup.





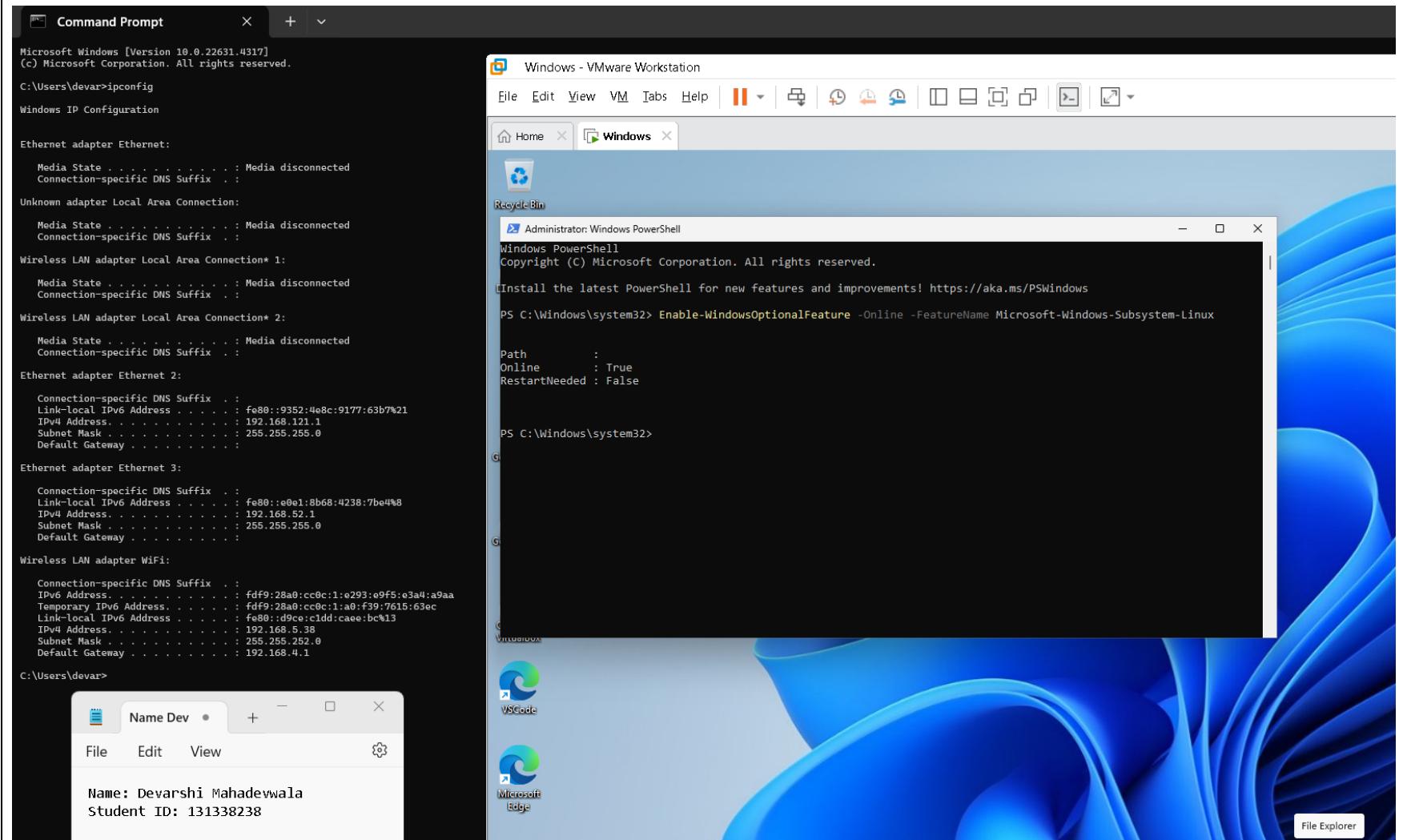
Before starting the virtual machine, check out the settings of the virtual machine and make changes you feel fit for your liking.



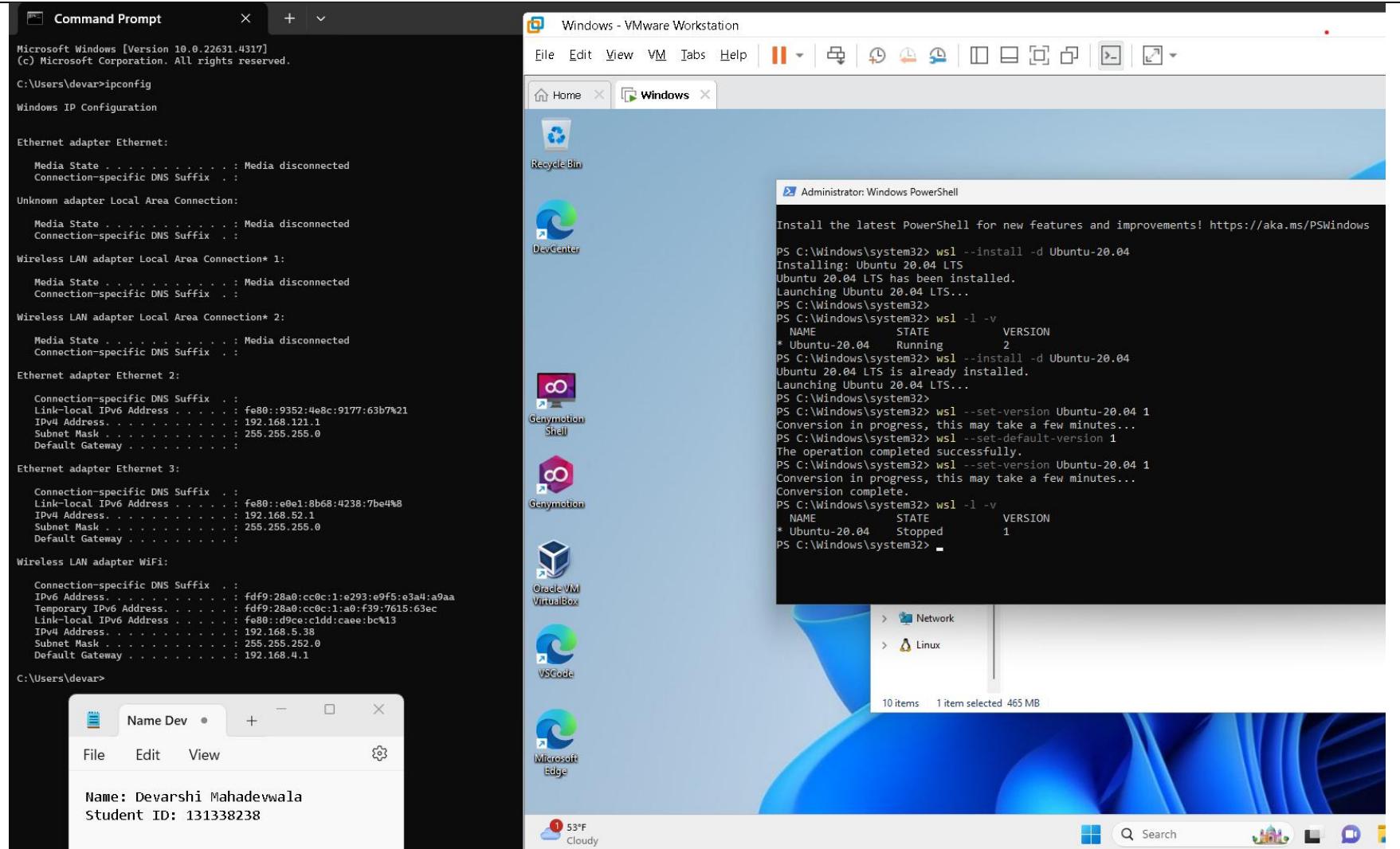
The windows machine has been powered up and above states my virtual machine's IP address.

Note: The virtual machine is working on VMware as it is the application I prefer to run my virtual environments.

We need to setup a WSL ubuntu environment on windows machine.

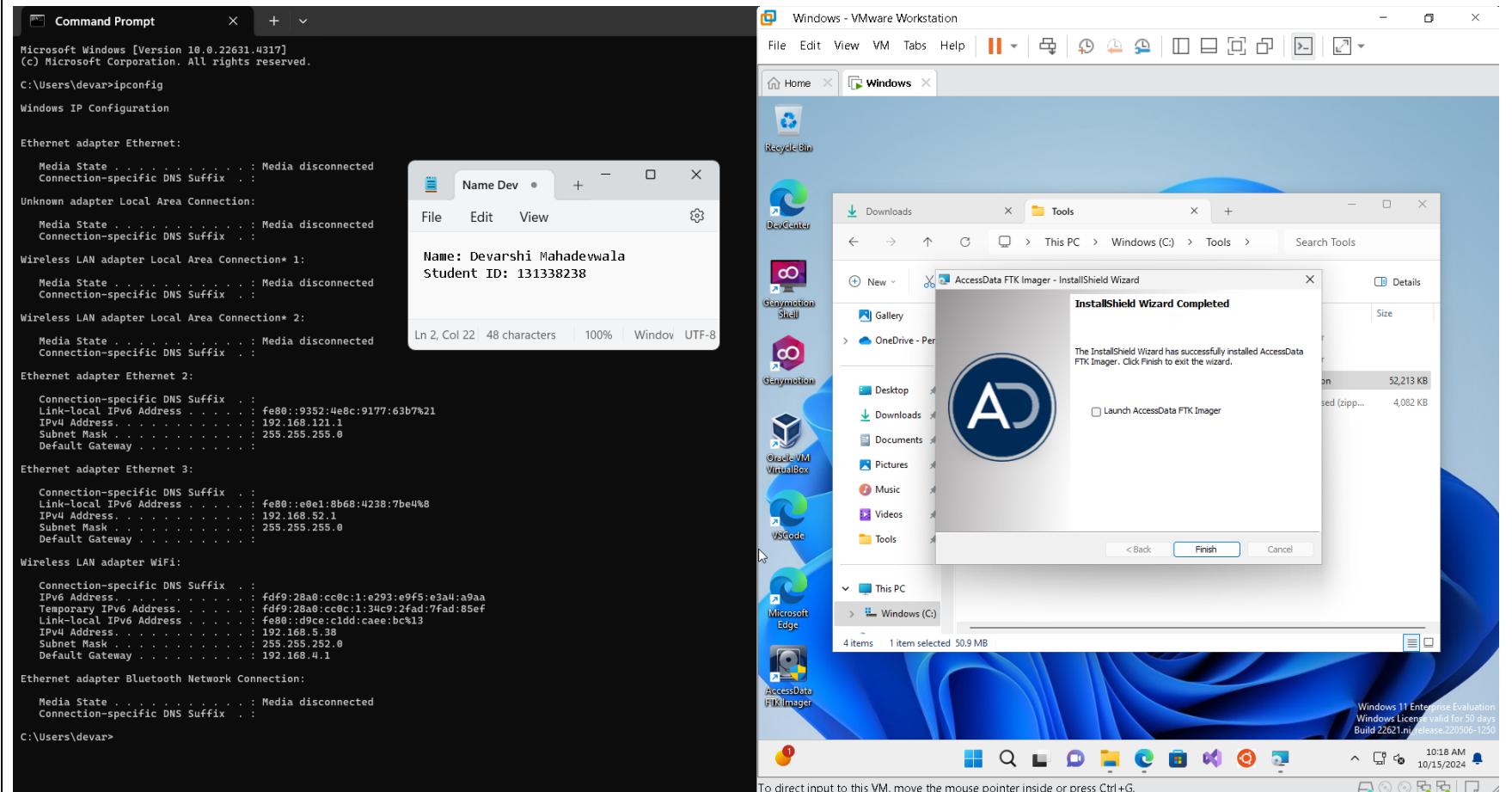


We enable the feature of using ubuntu terminal environment on windows virtual machine.



WSL environment download and setup is now complete and the version we are using for this lab is version 1.

Now, we need to setup some tools on the virtual machine to create our virtual forensics lab. Let us start with FTK imager which will help us capture a memory image file on which we will run our memory analysis operations.



FTK imager has a GUI application. Above is the photo which shows that FTK imager has been successfully downloaded on our virtual windows machine.

Microsoft Windows [Version 10.0.22631.4317]  
 (C) Microsoft Corporation. All rights reserved.

```
C:\Users\devar>ipconfig
```

Windows IP Configuration

Ethernet adapter Ethernet:

```
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
```

Unknown adapter Local Area Connection:

```
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
```

Wireless LAN adapter Local Area Connection 1:

```
  Media State . . . . . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . . . . . :
```

Wireless LAN adapter Local Area Connection 2:

```
  Media State . . . . . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . . . . . :
```

Ethernet adapter Ethernet 2:

```
  Connection-specific DNS Suffix . . . . . : fe80::9352:4e8c:9177:63b7%21
  Link-local IPv6 Address . . . . . : fe80::e8e1:8b68:4238:7be4%
  IPv4 Address . . . . . : 192.168.121.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :
```

Ethernet adapter Ethernet 3:

```
  Connection-specific DNS Suffix . . . . . : fe80::e8e1:8b68:4238:7be4%
  Link-local IPv6 Address . . . . . : fe80::d9c0:cc0c:1:e293:e9f5:e3a4:a9aa
  IPv4 Address . . . . . : 192.168.52.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :
```

Wireless LAN adapter WiFi:

```
  Connection-specific DNS Suffix . . . . . : fdf9:28a0:cc0c:1:e293:e9f5:e3a4:a9aa
  IPv6 Address . . . . . : fdf9:28a0:cc0c:1:e293:e9f5:e3a4:a9aa
  Temporary IPv6 Address . . . . . : fdf9:28a0:cc0c:1:34c9:2fad:7fad:85ef
  Link-local IPv6 Address . . . . . : fe80::d9c0:c1dd:caee:bc%13
  IPv4 Address . . . . . : 192.168.5.38
  Subnet Mask . . . . . : 255.255.252.0
  Default Gateway . . . . . : 192.168.4.1
```

Ethernet adapter Bluetooth Network Connection:

```
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
```

```
C:\Users\devar>
```

Administrator: Windows PowerShell

Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! <https://aka.ms/PSWindows>

```
PS C:\Windows\system32> Invoke-WebRequest -Uri "https://github.com/volatilityfoundation/volatility3/archive/refs/heads/main.zip" -OutFile "C:\Tools\volatility3.zip"
Invoke-WebRequest : 404: Not Found
At line:1 char:1
+ Invoke-WebRequest -Uri "https://github.com/volatilityfoundation/volat ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebException
+ FullyQualifiedErrorMessage : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand
PS C:\Windows\system32> Invoke-WebRequest -Uri "https://github.com/volatilityfoundation/volatility3/archive/refs/heads/develop.zip" -OutFile "C:\Tools\volatility3.zip"
PS C:\Windows\system32> Expand-Archive -Path "C:\Tools\volatility3.zip" -DestinationPath "C:\Tools\volatility3"
PS C:\Windows\system32>
```

Downloads

volatility3-develop

Name Date modified Type Size

Name	Date modified	Type	Size
.github	10/15/2024 10:26 AM	File folder	
development	10/15/2024 10:26 AM	File folder	
doc	10/15/2024 10:26 AM	File folder	
test	10/15/2024 10:26 AM	File folder	
volatility3	10/15/2024 10:26 AM	File folder	
.gitignore	10/13/2024 2:32 PM	GITIGNORE File	1 KB

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

For volatility, I cloned the github repository of volatility 3 and expanded the archive of volatility in C:\Tools in my C drive.

Microsoft Windows [Version 10.0.22631.4317]  
 (C) Microsoft Corporation. All rights reserved.

```
C:\Users\devar>ipconfig
```

Windows IP Configuration

Ethernet adapter Ethernet:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . .
```

Unknown adapter Local Area Connection:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . .
```

Wireless LAN adapter Local Area Connection 1:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . .
```

Wireless LAN adapter Local Area Connection 2:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . .
```

Ethernet adapter Ethernet 2:

```
Connection-specific DNS Suffix . . . . . : fe80::9352:4e8c:9177:63b7%21
Link-local IPv6 Address . . . . . : fe80::e0e1:8b68:4238:7be4%8
IPv4 Address . . . . . : 192.168.121.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Ethernet adapter Ethernet 3:

```
Connection-specific DNS Suffix . . . . . : fe80::e0e1:8b68:4238:7be4%8
Link-local IPv6 Address . . . . . : fe80::d9c0:cc0c:1:e293:9ef5:e3a4:a9aa
IPv4 Address . . . . . : 192.168.52.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Wireless LAN adapter WiFi:

```
Connection-specific DNS Suffix . . . . . : fdf9:28a0:cc0c:1:e293:9ef5:e3a4:a9aa
IPv6 Address . . . . . : fdf9:28a0:cc0c:1:a973:49ab:452c:1637
Temporary IPv6 Address . . . . . : fdf9:28a0:cc0c:1:cidd:caee:bc13
Link-local IPv6 Address . . . . . : fe80::d9c0:c1dd:caee:bc13
IPv4 Address . . . . . : 192.168.5.38
Subnet Mask . . . . . : 255.255.252.0
Default Gateway . . . . . :
```

Ethernet adapter Bluetooth Network Connection:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . .
```

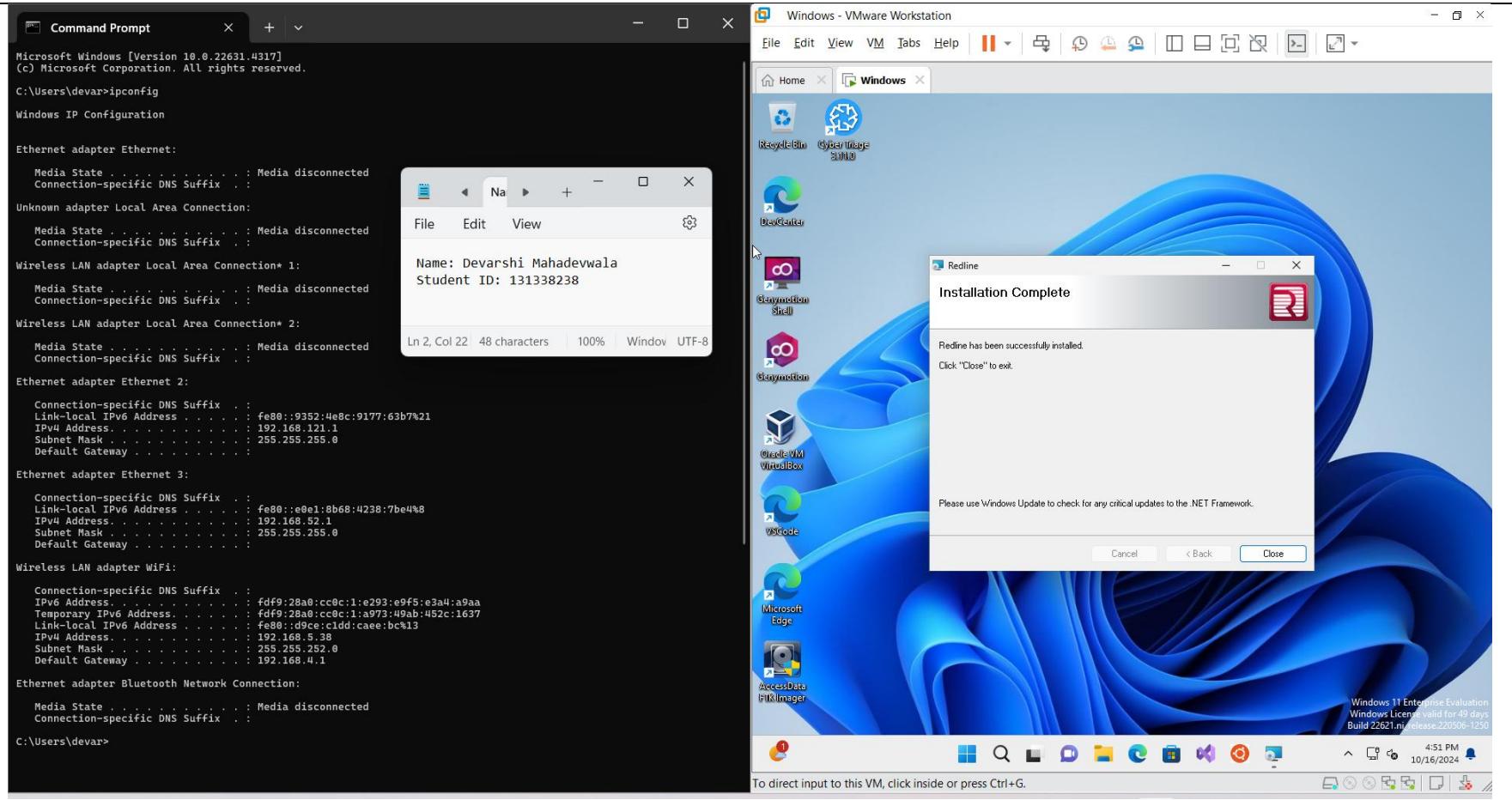
Name: Devarshi Mahadevwalla  
 Student ID: 131338238

Administrator: Windows PowerShell

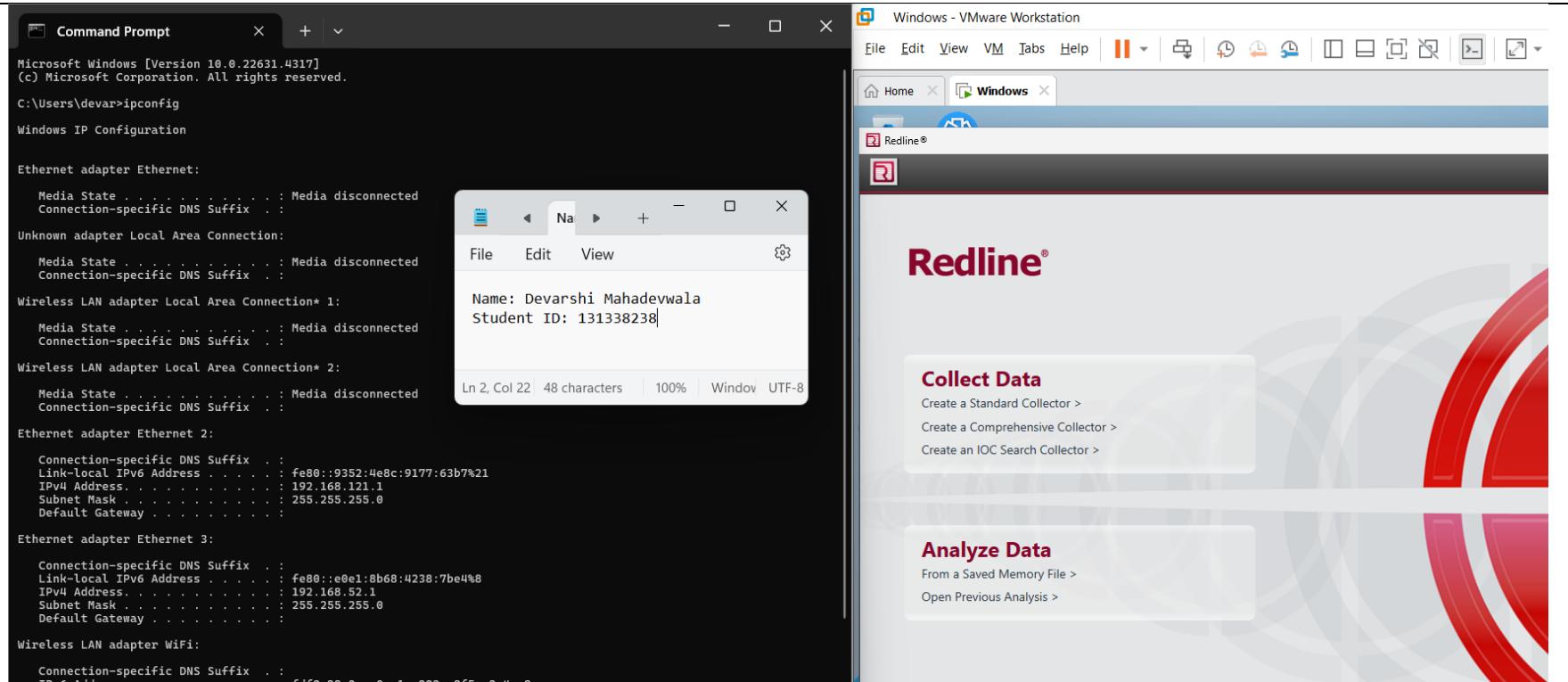
```
PS C:\Windows\system32> cd C:\Tools\volatility3\volatility3-develop
PS C:\Tools\volatility3\volatility3-develop> python vol.py --help
Volatility 3 Framework 2.11.0
usage: volatility [-h] [-c CONFIG] [--parallelism [(processes,threads,off)]] [-e EXTEND] [-p PLUGIN_DIRS]
                  [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [-w write-config]
                  [-s save-config SAVE_CONFIG] [--clear-cache] [--cache-path CACHE_PATH] [-o offline] [-u URL]
                  [-f filters FILTERS] [-h hide-columns [HIDE_COLUMNS ...]] [--single-location SINGLE_LOCATION]
                  [-stackers [STACKERS ...]] [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
                  [-banners Banners,configwriter,ConfigWriter,frameworkInfo,IsfInfo,layerwriter,
                   LayerWriter,linux,bash,Bash,linux,capabilities,Capabilities,linux,check,afinfo,Check_afinfo,linux,check,creds,Che
                   ck_creds,linux,check_idt,Check_idt,linux,check_modules,Check_modules,linux,check,syscall,Check_syscall,linux,ebpf,E
                   BPF,linux,elfs,Elf,linux,envars,Envvars,linux,iomem,IoMem,linux,keyboard,notifiers,Keyboard,notifiers,linux,kmsg,Km
                   sg,linux,library,lib,Library,lib,lsmod,Lsmod,linux,lsof,Lsof,linux,malfind,Malfind,linux,mountinfo,MountInfo
                   ,linux,netfilter,Netfilter,linux,pagecache,Files,linux,pagecache,InodePages,linux,pidhashtable,PIDHashTable,linux,p
                   rot,Maps,linux,psaux,Psaux,linux,pslist,PsList,linux,pscan,PsScan,linux,pstree,Pstree,linux,sockstat,Sockstat,linu
                   x,tty,check_tty,check,mac,bash,Bash,mac,check_syscall,Check_syscall,mac,check_sysctl,Check_sysctl,mac,check_trap_ta
                   ble,Check_trap_table,mac,osmsg,mac,ifconfig,Ifconfig,mac,auth_listeners,MacAuthListeners,mac,auth_scopes,Kau
                   th_scopes,mac,Kevents,Kevents,mac,list_files,List_Files,mac,lsmod,Lsmod,mac,lsof,Lsof,mac,malfind,Malfind,mac,mount
                   ,Mount,mac,netstat,Netstat,mac,proc_maps,Maps,mac,psaux,Psaux,mac,pslist,PsList,mac,psTree,PsTree,mac,socket_filter
                   ,Socket_filters,mac,timers,Timers,mac,trustedbsd,Trustedbsd,mac,vsevents,VSEvents,timerline,Timerline,vmscan,Vm
                   scan,Windows,amcache,Amcache,Windows,bigpools,BigPools,Windows,callbacks,Callbacks,Windows,cmdline,Cmdline,Windows,c
                   rashinfo,CrashInfo,Windows,devicetree,DeviceTree,Windows,dllist,DllList,Windows,driverirp,DriverIrp,Windows,driver
                   module,DriverModule,Windows,driverscan,DriverScan,Windows,dumpfiles,DumpFiles,Windows,envars,Envvars,Windows,filesc
                   a,n,FileScan,Windows,getservicesids,GetServicesIDs,Windows,handles,Handles,Windows,hollowpro
                   cesses,HollowProcesses,Windows,info,Info,Windows,joblinks,JobLinks,Windows,kpcrs,KPCRS,Windows,ldrmodules,LdrModules
                   ,Windows,malfind,Malfind,Windows,mbrscan,MbrScan,Windows,memmap,Memmap,Windows,modscan,ModScan,Windows,modules,Modu
                   les,Windows,mutantscan,MutantScan,Windows,orphan,Orphan,Kernel_Threads,Threads,Windows,pedump,PEdump,Windows,poolsc
                   anner,PoolScanner,Windows,privileges,Privs,Windows,processghosting,ProcessGhosting,Windows,pslist,PsList,Windows,psscan,Ps
                   Scan,Windows,psTree,PsTree,Windows,psxview,PsxView,Windows,registry,Certificates,Windows,registry,GetC
                   ellroutine,GetCellRoutine,Windows,registry,HiveList,Windows,registry,Hivescan,Windows,registry,VirtualBox
```

Windows 11 Enterprise Evaluation  
 Windows License valid for 49 days  
 Build 22621.1700 / Release 220506-1250

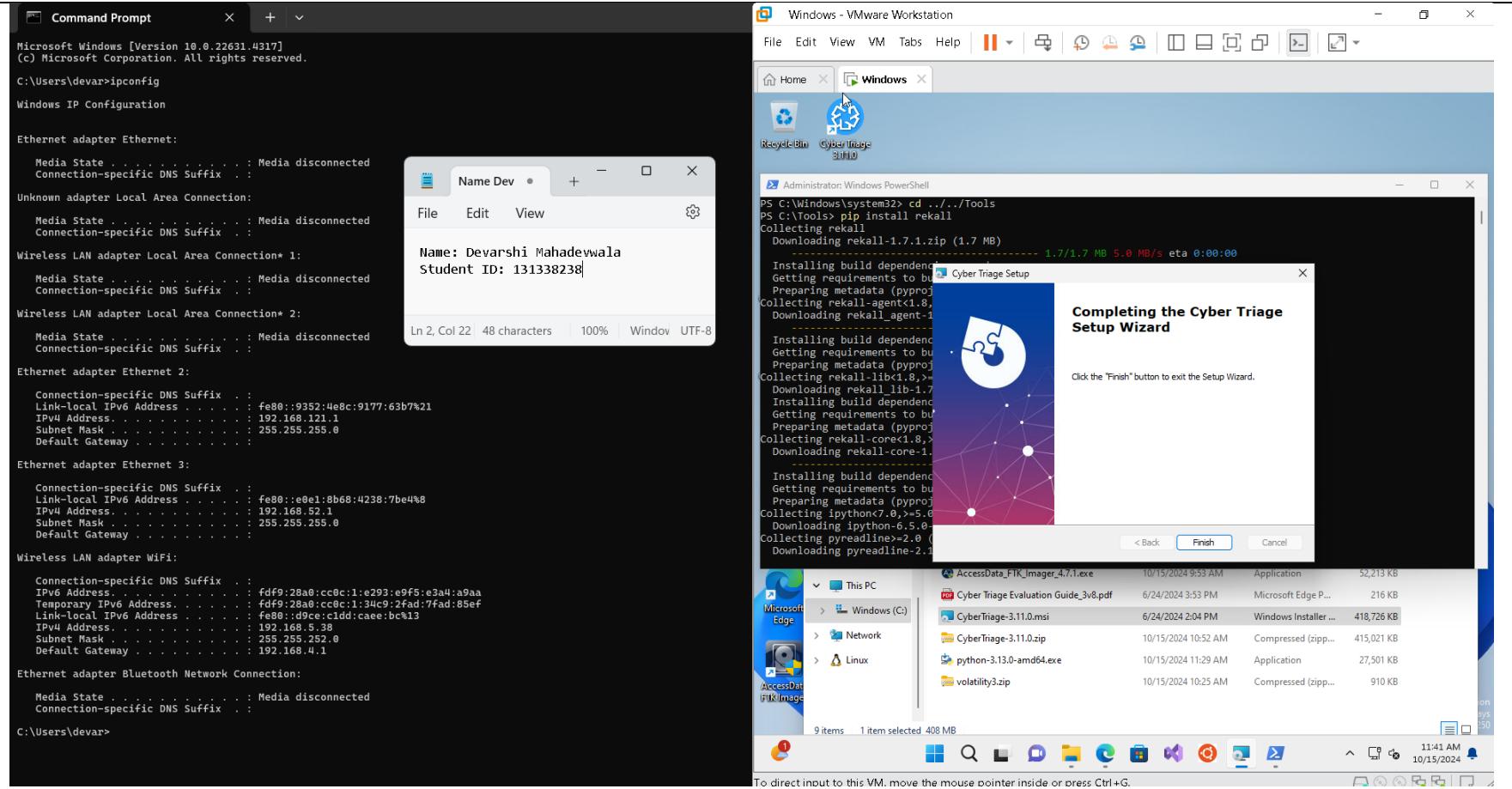
In PowerShell, from the folder where volatility was expanded, we run a help function to check if volatility has been successfully downloaded and is working on our system. Now we can use volatility to conduct scans on our image file.



Redline is a GUI application where we can run analysis on our memory image. As it a GUI application, above is the screenshot showing that redline has been successfully downloaded on our virtual environment.



Above is the successful running environment of redline where we can collect data and analyze it.



Cyber triage wizard setup complete. It is again a GUI application that you can easily download from the internet.

```
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Users\devar\ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Unknown adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix . . .
    Link-local IPv6 Address . . . . . : fe80::9352:4e8c%9177:63b7%1
    IPv4 Address . . . . . : 192.168.121.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.121.1

Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix . . .
    Link-local IPv6 Address . . . . . : fe80::e0e1:8b68%4238:7be4%1
    IPv4 Address . . . . . : 192.168.52.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.52.1

Wireless LAN adapter WiFi:

    Connection-specific DNS Suffix . . .
    IPv6 Address . . . . . : fdf9:28a0:cc0c:1:e293:e9f5%1
    Temporary IPv6 Address . . . . . : fdf9:28a0:cc0c:1:34c9:2fac%1
    Link-local IPv6 Address . . . . . : fe80::d9ce:cld%1
    IPv4 Address . . . . . : 192.168.5.38
    Subnet Mask . . . . . : 255.255.252.0
    Default Gateway . . . . . : 192.168.4.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

C:\Users\devar>
```

Windows - VMware Workstation

File Edit View VM Tabs Help

Home Windows Recycle DevCer GenMyShell GenMyConfig OracleVirtualBox VSCode Microsoft Edge AccessData FITKImager

dbmahadevvala@WinDev24C ~

```
Setting up libpython3.8:amd64 (3.8.10-0ubuntu1~20.04.12) ...
Setting up python3-pip (20.0.2-5ubuntu1.10) ...
Setting up cpp-9 (9.4.0-1ubuntu20.04.2) ...
Setting up libc6-dev:amd64 (2.31-0ubuntu9.16) ...
Setting up binutils-x86_64-linux-gnu (2.34-6ubuntu1.9) ...
Setting up binutils (2.34-6ubuntu1.9) ...
Setting up dpkg-dev (1.19.7ubuntu3.2) ...
Setting up libgcc-9-dev:amd64 (9.4.0-1ubuntu1~20.04.2) ...
Setting up libexpat1-dev:amd64 (2.2.9-1ubuntu0.7) ...
Setting up libpython3.8-dev:amd64 (3.8.10-0ubuntu1~20.04.12) ...
Setting up zlib1g-dev:amd64 (1:1.2.11.dfsg-2ubuntu1.5) ...
Setting up cpp (4:9.3.0-1ubuntu2) ...
Setting up gcc-9 (9.4.0-1ubuntu1~20.04.2) ...
Setting up libpython3-dev:amd64 (3.8.2-0ubuntu2) ...
Setting up libstdc++9-dev:amd64 (9.4.0-1ubuntu1~20.04.2) ...
Setting up gcc (4:9.3.0-1ubuntu2) ...
Setting up g++-9 (9.4.0-1ubuntu1~20.04.2) ...
Setting up python3.8-dev (3.8.10-0ubuntu1~20.04.12) ...
Setting up g++ (4:9.3.0-1ubuntu2) ...
Setting up alternatives: using /usr/bin/g++ to provide /usr/bin/c++ (c++) in auto mode
Setting up build-essential (12.8ubuntu1.1) ...
Setting up python3-dev (3.8.2-0ubuntu2) ...
Processing triggers for libc-bin (2.31-0ubuntu9.9) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for mime-support (3.64ubuntu1) ...
dbmahadevvala@WinDev2407Eval:/mnt/c/Windows/system32$ python3 --version
Python 3.8.10
dbmahadevvala@WinDev2407Eval:/mnt/c/Windows/system32$ pip3 --version
pip 20.0.2 from /usr/lib/python3/dist-packages/pip (python 3.8)
dbmahadevvala@WinDev2407Eval:/mnt/c/Windows/system32$ |
```

Windows 11 Enterprise Evaluation  
Windows License valid for 50 days  
Build 22621.ni RELEASE.220506-1250

10:44 AM 10/15/2024

Microsoft Windows [Version 10.0.22631.4317]  
 (C) Microsoft Corporation. All rights reserved.

```
C:\Users\devar>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .
  Unknown adapter Local Area Connection:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .
  Wireless LAN adapter Local Area Connection 1:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .
  Wireless LAN adapter Local Area Connection 2:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .
Ethernet adapter Ethernet 2:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::9352:4e8c:9177:63b%21
  IPv4 Address . . . . . : 192.168.121.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :
Ethernet adapter Ethernet 3:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::e8e1:8b68:4238:7be%8
  IPv4 Address . . . . . : 192.168.52.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :
Wireless LAN adapter WiFi:
  Connection-specific DNS Suffix . . .
  IPv6 Address . . . . . : fdf9:28a0:cc0c:1:e293:9ef5:e3a4:a9aa
  Temporary IPv6 Address . . . . . : fdf9:28a0:cc0c:1:a973:49ab:452c:1637
  Link-local IPv6 Address . . . . . : fe80::d9ce:c1dd:cae:bc%13
  IPv4 Address . . . . . : 192.168.5.38
  Subnet Mask . . . . . : 255.255.252.0
  Default Gateway . . . . . : 192.168.4.1
Ethernet adapter Bluetooth Network Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

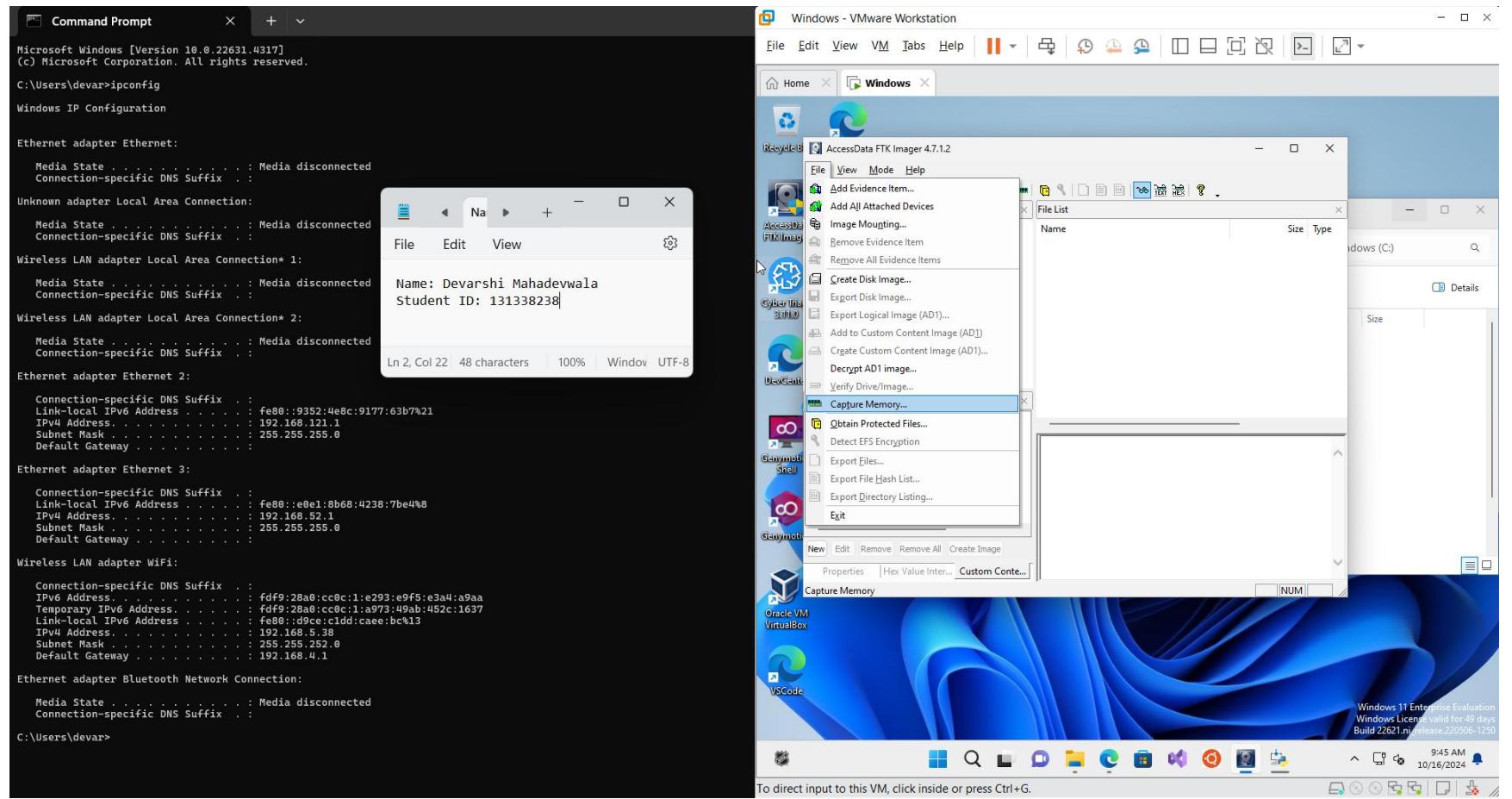
C:\Users\devar>
```

Using cached pyParsing-2.1.5-py2.py3-none-any.whl (42 kB)
 Collecting python-dateutil==2.6.1
 Using cached python\_dateutil-2.6.1-py2.py3-none-any.whl (194 kB)
 Collecting pytsk3==20170802
 Using cached pytsk3-20170802.tar.gz (2.9 MB)
 Collecting pytz==2017.3
 Using cached pytz-2017.3-py3-none-any.whl (511 kB)
 Collecting rekal-capstone==3.0.5.post2
 Using cached rekal-capstone-3.0.5.post2.zip (1.8 MB)
 Collecting rekal-efilter<1.7,>=1.6
 Using cached rekal\_efilter-1.6.0.zip (112 kB)
 Collecting rekal-yara==3.6.3.1
 Using cached rekal\_yara-3.6.3.1.tar.gz (1.2 MB)
 ERROR: Could not find a version that satisfies the requirement pypiwin32==220 (from rekal-core<1.8,>=1.7.0rc1->rekal)
 ERROR: No matching distribution found for pypiwin32==220 (from rekal-core<1.8,>=1.7.0rc1->rekal)
 PS C:\Users\User> python -m pip install pypiwin32==220
 DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this functionality.
 ERROR: Could not find a version that satisfies the requirement pypiwin32==220 (from versions: 219, 223)
 ERROR: No matching distribution found for pypiwin32==220
 PS C:\Users\User> python -m pip install pywin32==223
 DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this functionality.
 Requirement already satisfied: pywin32==223 in c:\python27\lib\site-packages (223)
 PS C:\Users\User>

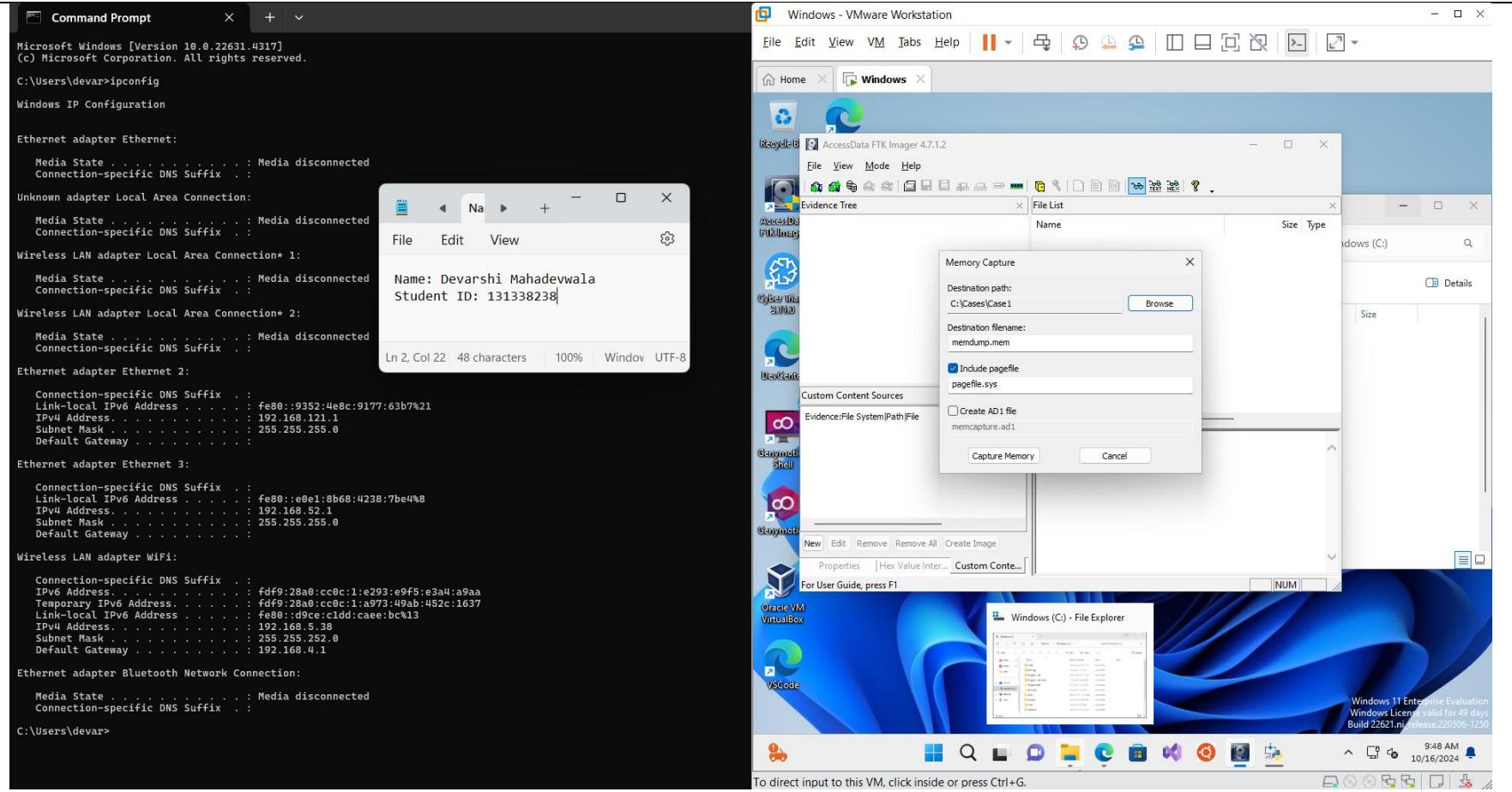
I also tried downloading rekal on the virtual environment. But there is a package named pypiwin32 which need to have the version 220 for recall to download, install, and run successfully. That package has been deprecated and there are currently no vendors that distributes that package, so I needed to scrape using rekal here.

The forensics lab has been setup with FTK imager, cyber triage, redline and volatility along with WSL ubuntu environment and python installed and up and running on our virtual environment. You can also download other tools like Belka soft to run memory image analysis.

Now, we can start conducting the memory image analysis. But before that, let us capture a memory image from FTK imager.



Start the FTK imager application and click on file on the taskbar. We need to select capture memory from it.



The memory capture wizard will ask us the name we want for our memory file and the destination of our memory image. I am storing my memory image in C:\Cases\Case1 as it is the dedicated directory where I will create cases for memory analysis.

```
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Users\devar>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Unknown adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix . . .
    Link-local IPv6 Address . . . . . : fe80::9352:4e8c:9177:63b7%21
    IPv4 Address . . . . . : 192.168.121.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix . . .
    Link-local IPv6 Address . . . . . : fe80::e8e1:8b68:4238:7be4%8
    IPv4 Address . . . . . : 192.168.52.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

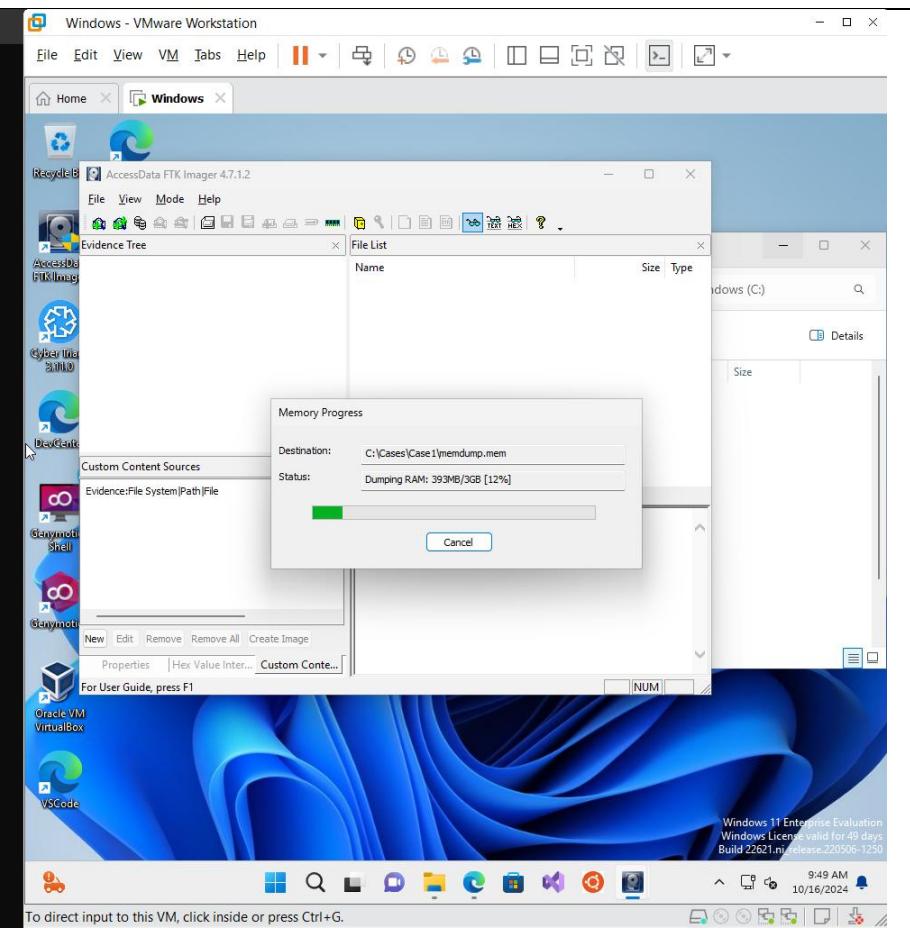
Wireless LAN adapter WiFi:

    Connection-specific DNS Suffix . . .
    IPv6 Address . . . . . : fdf9:28a0:cc0c:1:e293:e9f5:e3a4:a9aa
    Temporary IPv6 Address . . . . . : fdf9:28a0:cc0c:1:a973:49ab:452c:1637
    Link-local IPv6 Address . . . . . : fe80::d9ce:c1dd:cae:bc%13
    IPv4 Address . . . . . : 192.168.5.38
    Subnet Mask . . . . . : 255.255.252.0
    Default Gateway . . . . . : 192.168.4.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

C:\Users\devar>
```



After clicking on capture memory, FTK imager will start capturing the image.

```
Command Prompt + v
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Users\devar>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

Unknown adapter Local Area Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

Wireless LAN adapter Local Area Connection* 1:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

Wireless LAN adapter Local Area Connection* 2:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

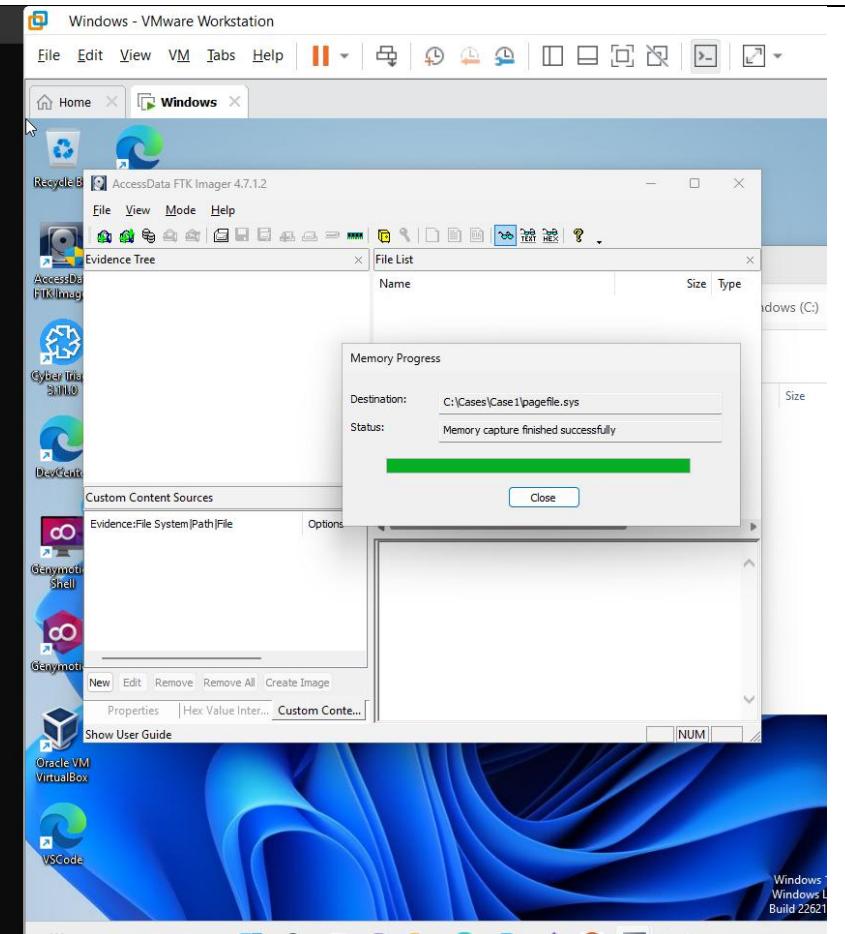
Ethernet adapter Ethernet 2:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::9352:4e8c:9177:63b7%21
  IPv4 Address . . . . . : 192.168.121.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Ethernet adapter Ethernet 3:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::e0e1:8b68:4238:7be4%8
  IPv4 Address . . . . . : 192.168.52.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

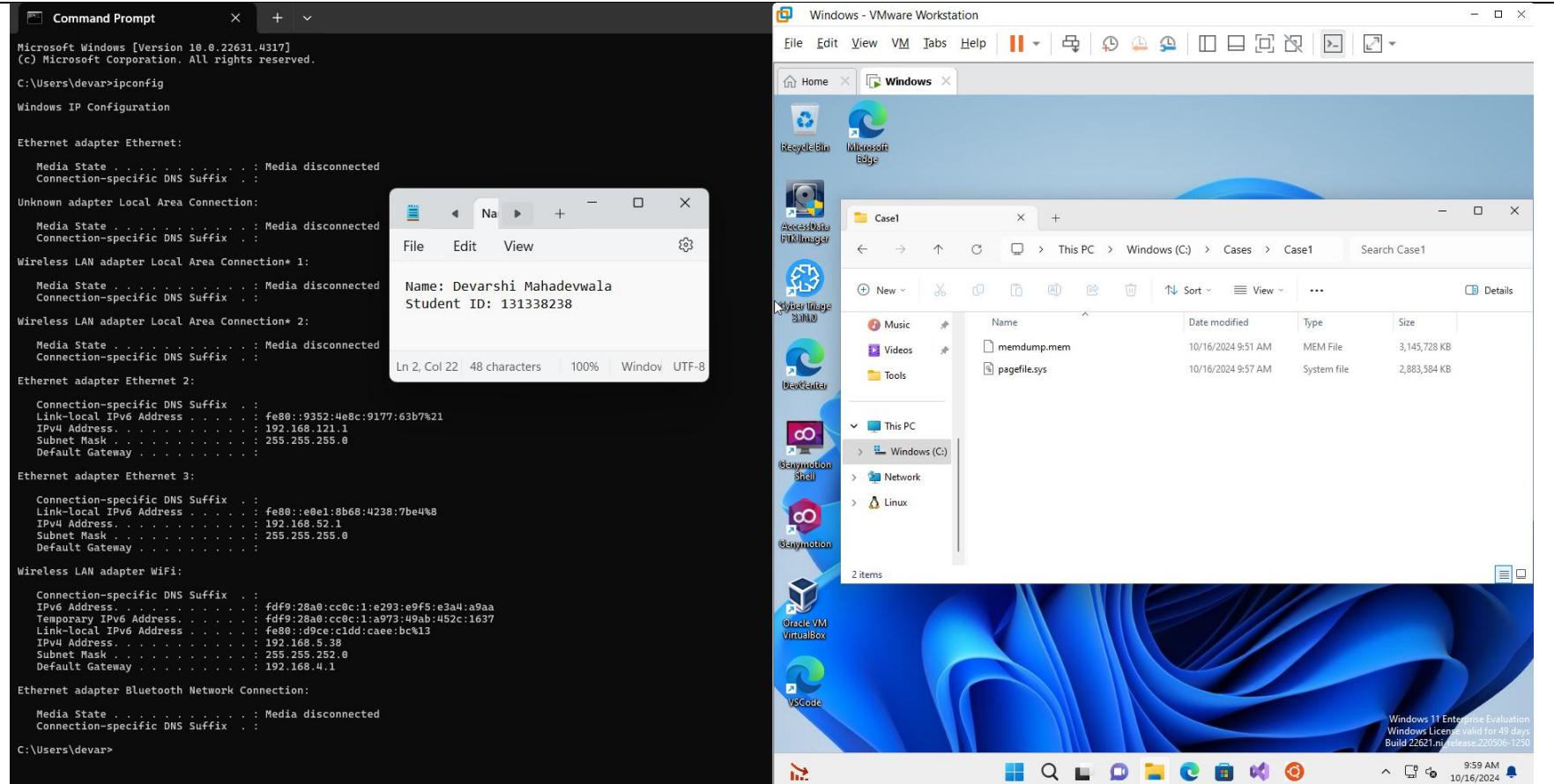
Wireless LAN adapter WiFi:
  Connection-specific DNS Suffix . . .
  IPv6 Address . . . . . : fdf9:28a0:cc0c:1:e293:e9f5:e3a4:a9aa
  Temporary IPv6 Address . . . . . : fdf9:28a0:cc0c:1:ca973:49ab:452c:1637
  Link-local IPv6 Address . . . . . : fe80::d9ce:c1d:cae:bc%13
  IPv4 Address . . . . . : 192.168.5.38
  Subnet Mask . . . . . : 255.255.252.0
  Default Gateway . . . . . : 192.168.4.1

Ethernet adapter Bluetooth Network Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

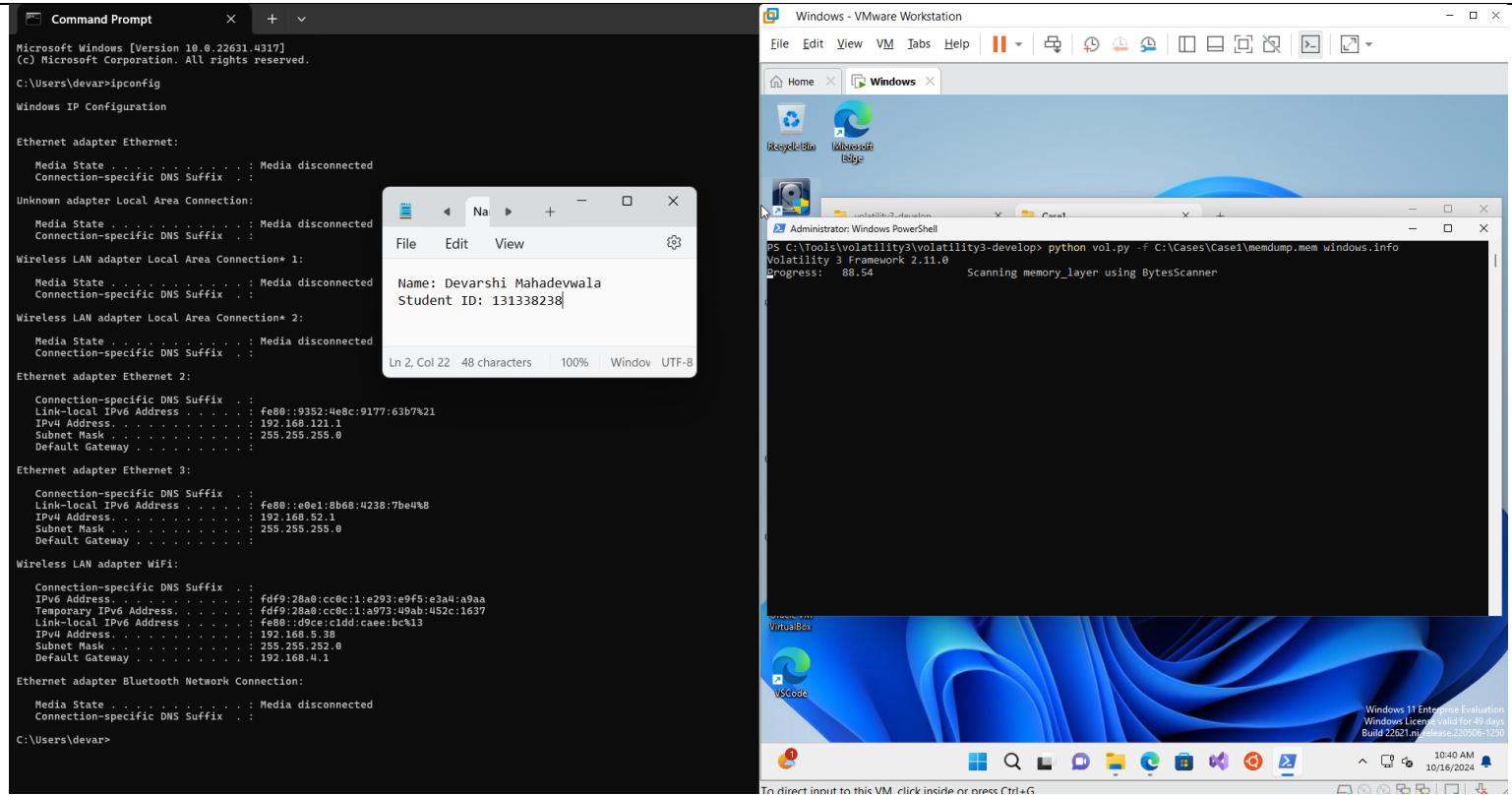
C:\Users\devar>
```



Memory has been captured, click on close and check up if the memory image has been captured at the specified location.



In C:\Cases\Case1, we can see the memdump.mem file indicating that memory capture was successful. Now let us run our tools for memory image analysis.



Let us run our first scan from volatility on the image file that we captured. Starting off with a basic scan, I ran a simple windows information step. When you run the 'windows.info' plugin in Volatility on a memory image from FTK Imager, it extracts and displays various details about the Windows operating system. This includes:

- The version and build number of Windows
- The service pack level installed
- The system root directory
- The username of the logged-in user
- The current process ID and name
- The system uptime
- Information about any system crashes or blue screens

This plugin provides a quick and easy way to gather essential information about the Windows system from the memory image, which can be useful in digital forensics and incident response investigations.

Microsoft Windows [Version 10.0.22631.4317]  
 (C) Microsoft Corporation. All rights reserved.

```
C:\Users\devar>ipconfig
```

Windows IP Configuration

Ethernet adapter Ethernet:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . .
```

Unknown adapter Local Area Connection:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . .
```

Wireless LAN adapter Local Area Connection 1:

```
Media State . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . . . . .
```

Wireless LAN adapter Local Area Connection 2:

```
Media State . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . . . . .
```

Ethernet adapter Ethernet 2:

```
Connection-specific DNS Suffix . . . . . : fe80::9352:4e8c:9177:63b7%21
Link-local IPv6 Address . . . . . : fe80::e8e1:8b68:4238:7be4%8
IPv4 Address . . . . . : 192.168.121.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Ethernet adapter Ethernet 3:

```
Connection-specific DNS Suffix . . . . . : fe80::e8e1:8b68:4238:7be4%8
Link-local IPv6 Address . . . . . : fe80::d9c0:cc0c:1:e293:9ef5:e3a4:a9aa
IPv4 Address . . . . . : 192.168.52.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Wireless LAN adapter WiFi:

```
Connection-specific DNS Suffix . . . . . : fdf9:28a0:cc0c:1:e293:9ef5:e3a4:a9aa
IPv6 Address . . . . . : fdf9:28a0:cc0c:1:a973:49ab:452c:1637
Temporary IPv6 Address . . . . . : fdf9:28a0:cc0c:1:a973:49ab:452c:1637
Link-local IPv6 Address . . . . . : fe80::d9c0:c1dd:caee:bc%13
IPv4 Address . . . . . : 192.168.5.38
Subnet Mask . . . . . : 255.255.252.0
Default Gateway . . . . . :
```

Ethernet adapter Bluetooth Network Connection:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . .
```

Administrator: Windows PowerShell

```
Progress: 100.00          Reading Symbol layer
Progress: 100.00          PDB scanning finished

Variable           Value
Kernel Base        0xf0055b400000
DTB               0x1ae000
Symbols file:///C:/Tools/volatility3/volatility3-develop/volatility3/symbols/windows/ntkrnlmp.pdb/9074FC2B82ED2B7E1
CB3366964BE62F9-1.json.xz
Is64bit True
IsPAE False
layer_name         0 WindowsIntel32e
memory_layer       1 FileLayer
KdVersionBlock    0xf0055c0099a0
Major/Minor        15.22621
MachineType       34404
NumberOfProcessors 2
SystemTime        2024-10-16 13:51:01+00:00
NtSystemRoot      C:\Windows
NtProductType     NtProductWinNT
NtMajorVersion    10
NtMinorVersion    0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine        34404
PE TimeDateStamp   Fri Jul 2 05:18:00 1993
PS C:\Tools\volatility3\volatility3-develop>
VirtualBox
VSCode
```

To direct input to this VM, click inside or press Ctrl+G.

First scan has been completed and the details of those scans can be clearly visible from the above screenshot.

Command Prompt

```
Microsoft Windows [Version 10.0.22621.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Users\devar

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Unknown adapter Local Area Connection:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 1:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 2:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 2:
    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::9352:4e8c:9177:63b7%21
    IPv4 Address . . . . . : 192.168.121.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter Ethernet 3:
    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::e0e1:8b68:4238:7be4%8
    IPv4 Address . . . . . : 192.168.52.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter WiFi:
    Connection-specific DNS Suffix . :
    IPv6 Address . . . . . : fd9f:28a0:cc0c:1:e293:e9f5:e3a4:a9aa
    Temporary IPv6 Address . . . . . : fd9f:28a0:cc0c:1:a973:49ab:452c:1637
    Link-local IPv6 Address . . . . . : fe80::e0e1:8b68:4238:c9e:bc%13
    IPv4 Address . . . . . : 192.168.5.38
    Subnet Mask . . . . . : 255.255.252.0
    Default Gateway . . . . . : 192.168.4.1

Ethernet adapter Bluetooth Network Connection:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

C:\Users\devar>
```

File Explorer

```
Name: Devarshi Mahadevawala
Student ID: 131338238
```

Windows - VMware Workstation

```
Administrator: Windows PowerShell
PS C:\Tools\volatility3\volatility3-develop> python vol.py -F C:\Cases\Case1\memdump.mem windows.pslist
Volatility 3 Framework 2.11.0
Progress: 4.17 Scanning memory_layer using BytesScanner
```

Now, I am running a windows.pslist scan on the memory image. The windows.pslist plugin in Volatility generates a list of processes running on the Windows system at the time the memory dump was captured. This includes:

- Process ID (PID)
- Process name
- Parent process ID (PPID)
- Process start time
- Process exit time (if applicable)
- Thread count
- Handle count
- Memory usage (private bytes, working set, and peak working set)

This plugin provides a comprehensive view of the system's process landscape, allowing investigators to identify and analyze running processes, including potential malware or suspicious activity.

Microsoft Windows [Version 10.0.22631.4317]  
 (C) Microsoft Corporation. All rights reserved.

```
C:\Users\devar>ipconfig
```

Windows IP Configuration

Ethernet adapter Ethernet:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . .
```

Unknown adapter Local Area Connection:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . .
```

Wireless LAN adapter Local Area Connection 1:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . .
```

Wireless LAN adapter Local Area Connection 2:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . .
```

Ethernet adapter Ethernet 2:

```
Connection-specific DNS Suffix . . . . .
Link-local IPv6 Address . . . . . : fe80::9252:4e8c:9177:63b%21
IPv4 Address . . . . . : 192.168.121.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Ethernet adapter Ethernet 3:

```
Connection-specific DNS Suffix . . . . .
Link-local IPv6 Address . . . . . : fe80::e0e1:8b68:4238:7be4%8
IPv4 Address . . . . . : 192.168.52.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Wireless LAN adapter WiFi:

```
Connection-specific DNS Suffix . . . . .
IPv6 Address . . . . . : fdf9:28a0:cc0c:1:e293:e9f5:e3a4:a9aa
Temporary IPv6 Address . . . . . : fdf9:28a0:cc0c:1:a973:49ab:452c:1637
Link-local IPv6 Address . . . . . : fe80::d9ce:c1dd:caee:bc%13
IPv4 Address . . . . . : 192.168.5.38
Subnet Mask . . . . . : 255.255.252.0
Default Gateway . . . . . :
```

Ethernet adapter Bluetooth Network Connection:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . .
```

Administrator: Windows PowerShell

Process ID	Process Name	Start Address	Priority	Session ID	Creation Time	Last Write Time	Exit Status	User
3800	msedgewebview2	0xc508f7b62080	14	-	1	2024-10-16 13:37:46.000000 UTC	N/A	
5200	msedgewebview2	0xc508f40ad080	8	-	1	2024-10-16 13:37:46.000000 UTC	N/A	
7484	msedgewebview2	0xc508f7eca080	14	-	1	2024-10-16 13:37:46.000000 UTC	N/A	
872	svchost.exe	0xc508f8630080	7	-	0	2024-10-16 13:41:32.000000 UTC	N/A	
4904	ApplicationFra	0xc508f8659080	3	-	1	2024-10-16 13:41:41.000000 UTC	N/A	
8260	svchost.exe	0xc508f8b84080	2	-	1	2024-10-16 13:41:45.000000 UTC	N/A	
8392	MoUsaCoreWork	0xc508f8666080	8	-	0	2024-10-16 13:41:46.000000 UTC	N/A	
8520	MoNotification	0xc508f9bbe0c0	0	-	1	2024-10-16 13:41:51.000000 UTC	202	
7700	msiexec.exe	0xc508f9d82180	4	-	0	2024-10-16 13:42:49.000000 UTC	N/A	
8324	msiexec.exe	0xc508f91430c0	0	-	1	2024-10-16 13:42:54.000000 UTC	202	
3456	OneDriveSetup.	0xc508f94060c0	8	-	1	2024-10-16 13:46:51.000000 UTC	N/A	
5588	OneDriveSetup.	0xc508f54df1c0	11	-	1	2024-10-16 13:47:08.000000 UTC	N/A	
5924	Microsoft.Shar	0xc508f95cd0c0	12	-	1	2024-10-16 13:48:59.000000 UTC	N/A	

PS C:\Tools\volatility3\volatility3-develop>

To direct input to this VM, click inside or press Ctrl+G.

We can see all the specified list on the result of the scan when completed in the screenshot above. It gives us a very detailed list of processes and their specifics which we can go through to run an analysis later.

Microsoft Windows [Version 10.0.22631.4317]  
 (C) Microsoft Corporation. All rights reserved.

```
C:\Users\devar>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

Unknown adapter Local Area Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

Wireless LAN adapter Local Area Connection 1:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

Wireless LAN adapter Local Area Connection 2:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

Ethernet adapter Ethernet 2:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::9252:4e8c:9177:63b7%21
  IPv4 Address . . . . . : 192.168.121.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Ethernet adapter Ethernet 3:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::e0e1:8b68:4238:7be4%8
  IPv4 Address . . . . . : 192.168.52.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Wireless LAN adapter WiFi:
  Connection-specific DNS Suffix . . .
  IPv6 Address . . . . . : fdf9:28a0:cc0c:1:e293:e9f5:e3a4:a9aa
  Temporary IPv6 Address . . . . . : fdf9:28a0:cc0c:1:a973:49ab:452c:1637
  Link-local IPv6 Address . . . . . : fe80::d9ce:c1dd:caee:bc%13
  IPv4 Address . . . . . : 192.168.5.38
  Subnet Mask . . . . . : 255.255.252.0
  Default Gateway . . . . . : 192.168.4.1

Ethernet adapter Bluetooth Network Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

C:\Users\devar>
```

Name: Devarshi Mahadevwalla  
 Student ID: 131338238

Ln 2, Col 22	48 characters	100%	Window	UTF-8

Administrator: Windows PowerShell

```
PS C:\Tools\volatility3\volatility3-develop> python vol.py -f C:\Cases\Case1\memdump.mem windows.pslist
Volatility 3 Framework 2.11.0
Progress: 100.00          PDB scanning finished
PID      PPID     ImageFileName   Offset(V)    Threads Handles SessionId   Wow64  CreateTime       ExitTime
File output
```

File output	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime
4	0	System	0xc508f16e4040	156	-	N/A	False	2024-10-16 13:26:22.000000 UTC	N/A
60	4	Secure System	0xc508f17de080	0	-	N/A	False	2024-10-16 13:26:01.000000 UTC	N/A
92	4	Registry	0xc508f171a080	4	-	N/A	False	2024-10-16 13:26:01.000000 UTC	N/A
392	4	smss.exe	0xc508f370b040	2	-	N/A	False	2024-10-16 13:26:23.000000 UTC	N/A
520	520	csrss.exe	0xc508f3791140	11	-	0	False	2024-10-16 13:27:03.000000 UTC	N/A
628	620	csrss.exe	0xc508f4136140	14	-	1	False	2024-10-16 13:27:12.000000 UTC	N/A
676	620	winlogon.exe	0xc508f418c0c0	5	-	1	False	2024-10-16 13:27:13.000000 UTC	N/A
696	520	wininit.exe	0xc508f4192080	2	-	0	False	2024-10-16 13:27:13.000000 UTC	N/A
740	696	services.exe	0xc508f41a3080	7	-	0	False	2024-10-16 13:27:15.000000 UTC	N/A
764	696	LsaIso.exe	0xc508f41a2080	2	-	0	False	2024-10-16 13:27:16.000000 UTC	N/A
804	696	lsass.exe	0xc508f4121080	10	-	0	False	2024-10-16 13:27:25.000000 UTC	N/A
920	740	svchost.exe	0xc508f42d6080	16	-	0	False	2024-10-16 13:27:31.000000 UTC	N/A

VirtualBox

VSCode

To direct input to this VM, click inside or press Ctrl+G.

Windows 11 Enterprise Evaluation  
 Windows License Valid for 49 days  
 Build 22621.1962.1962.220506-1250

10:51 AM  
 10/16/2024

Above we can see the resulting column wise specification of windows.pslist analysis.

Command Prompt

```
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Users\devar>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Unknown adapter Local Area Connection:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Wireless LAN adapter Local Area Connection 1:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Wireless LAN adapter Local Area Connection 2:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Ethernet adapter Ethernet 2:
    Connection-specific DNS Suffix . . .
    Link-local IPv6 Address . . . . . : fe80::9252:4e8c:9177:63b%21
    IPv4 Address . . . . . : 192.168.121.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter Ethernet 3:
    Connection-specific DNS Suffix . . .
    Link-local IPv6 Address . . . . . : fe80::e8e1:8b68:4238:7be4%8
    IPv4 Address . . . . . : 192.168.52.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter WiFi:
    Connection-specific DNS Suffix . . .
    IPv6 Address . . . . . : fdf9:28a0:cc0c:1:e293:e9f5:e3a4:a9aa
    Temporary IPv6 Address . . . . . : fdf9:28a0:cc0c:1:a973:49ab:452c:1637
    Link-local IPv6 Address . . . . . : fe80::d9ce:c1dd:caee:bc%13
    IPv4 Address . . . . . : 192.168.5.38
    Subnet Mask . . . . . : 255.255.252.0
    Default Gateway . . . . . : 192.168.4.1

Ethernet adapter Bluetooth Network Connection:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

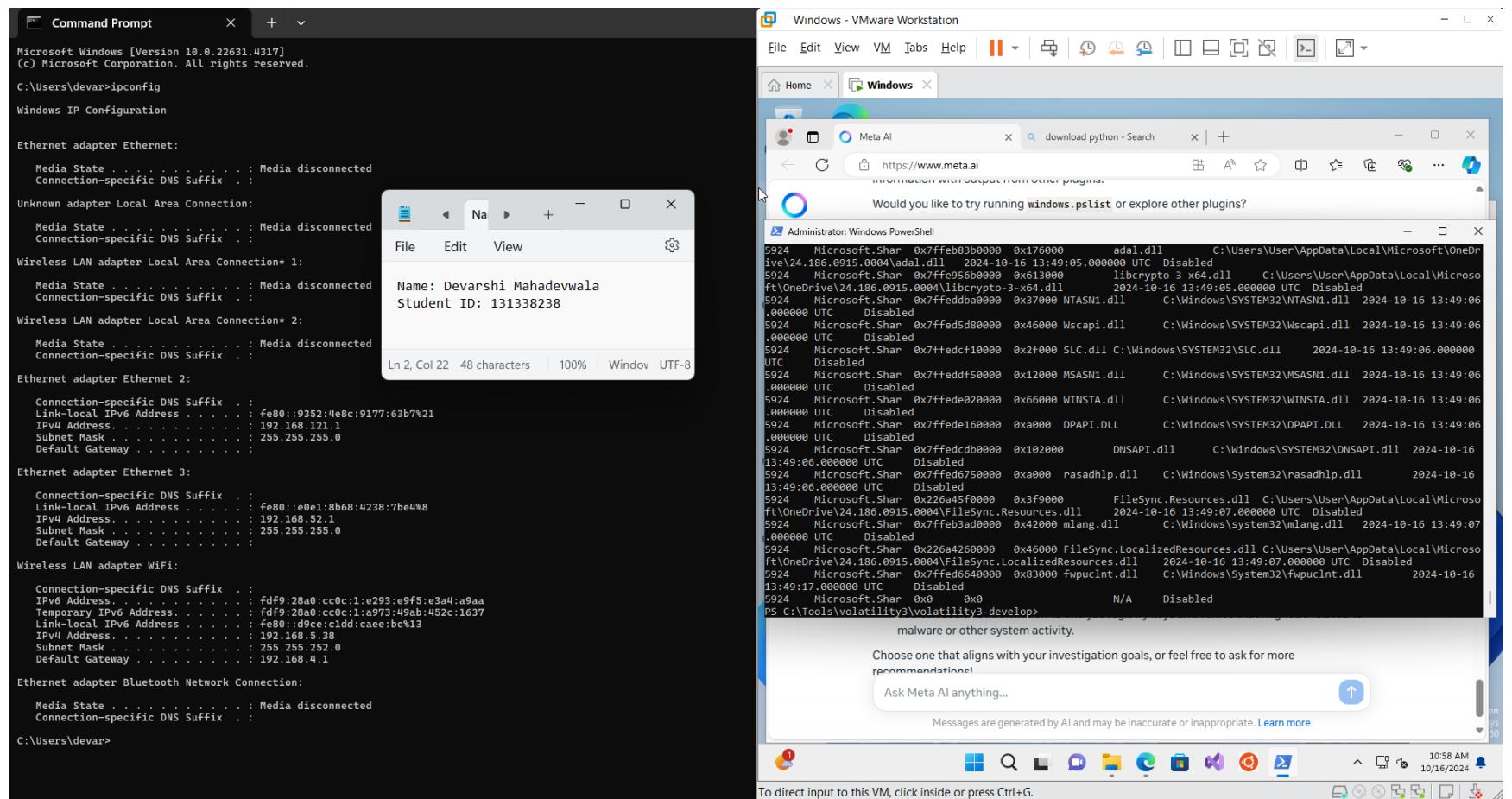
C:\Users\devar>
```

Next scan that we will conduct is a dll list scan. The windows.dlllist plugin in Volatility enumerates the DLLs (Dynamic Link Libraries) loaded by each process running on the Windows system at the time the memory dump was captured. This includes:

- Process ID (PID)
- Process name
- DLL name
- DLL base address
- DLL size
- DLL load count
- DLL load time

This plugin provides a detailed view of the DLLs used by each process, allowing investigators to:

- Identify potentially malicious or unknown DLLs
  - Analyze DLL load patterns and dependencies
  - Detect potential DLL hijacking or injection attacks
  - Investigate DLL-related system crashes or instability



We can see all of the specific details of each **dll** process running on windows in the above screenshot.

The screenshot shows a Windows desktop environment with three main windows:

- Command Prompt**: A terminal window displaying the output of the command `ipconfig`. It lists network adapters, their connection status (Media State), and IP configuration details (IPv4 Address, Subnet Mask, Default Gateway).
- Windows - VMware Workstation**: A browser window showing a search result for "download python". Below the search bar, it says "Would you like to try running windows.pslist or explore other plugins?". A PowerShell window titled "Administrator: Windows PowerShell" is open, showing the command `python vol.py -f C:\Cases\Case1\memdump.mem windows.malfind` being run.
- Meta AI**: An AI interface from Microsoft. It displays a message: "malware or other system activity. Choose one that aligns with your investigation goals, or feel free to ask for more recommendations! Ask Meta AI anything...".

Final scan we conduct is the `windows.malfind`. The `windows.malfind` plugin in Volatility is designed to detect and identify potential malware artifacts in the memory dump of a Windows system. This includes:

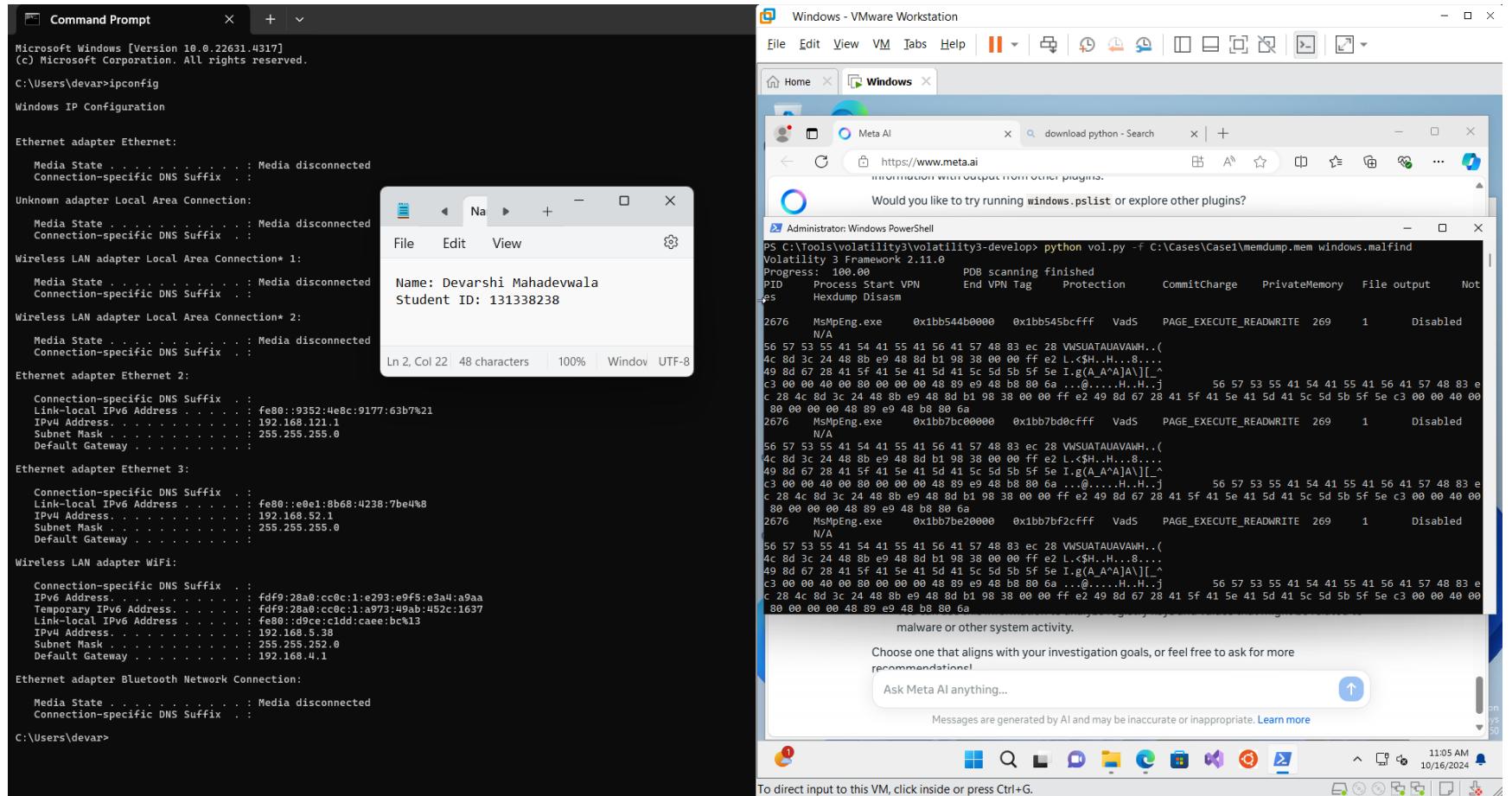
- Suspicious memory allocations
- Unusual API hooks
- Hidden or masked processes
- Mysterious system calls
- Anomalies in system memory

This plugin uses various techniques to identify potential malware, including:

- Heuristics-based detection

- Signature-based detection
- Anomaly-based detection

By running windows.malfind, investigators can quickly identify potential malware activity and take further action to contain and eradicate the threat.



The resulting screenshot shows us the potential malware artifacts of the memory dump with PID process and other details.

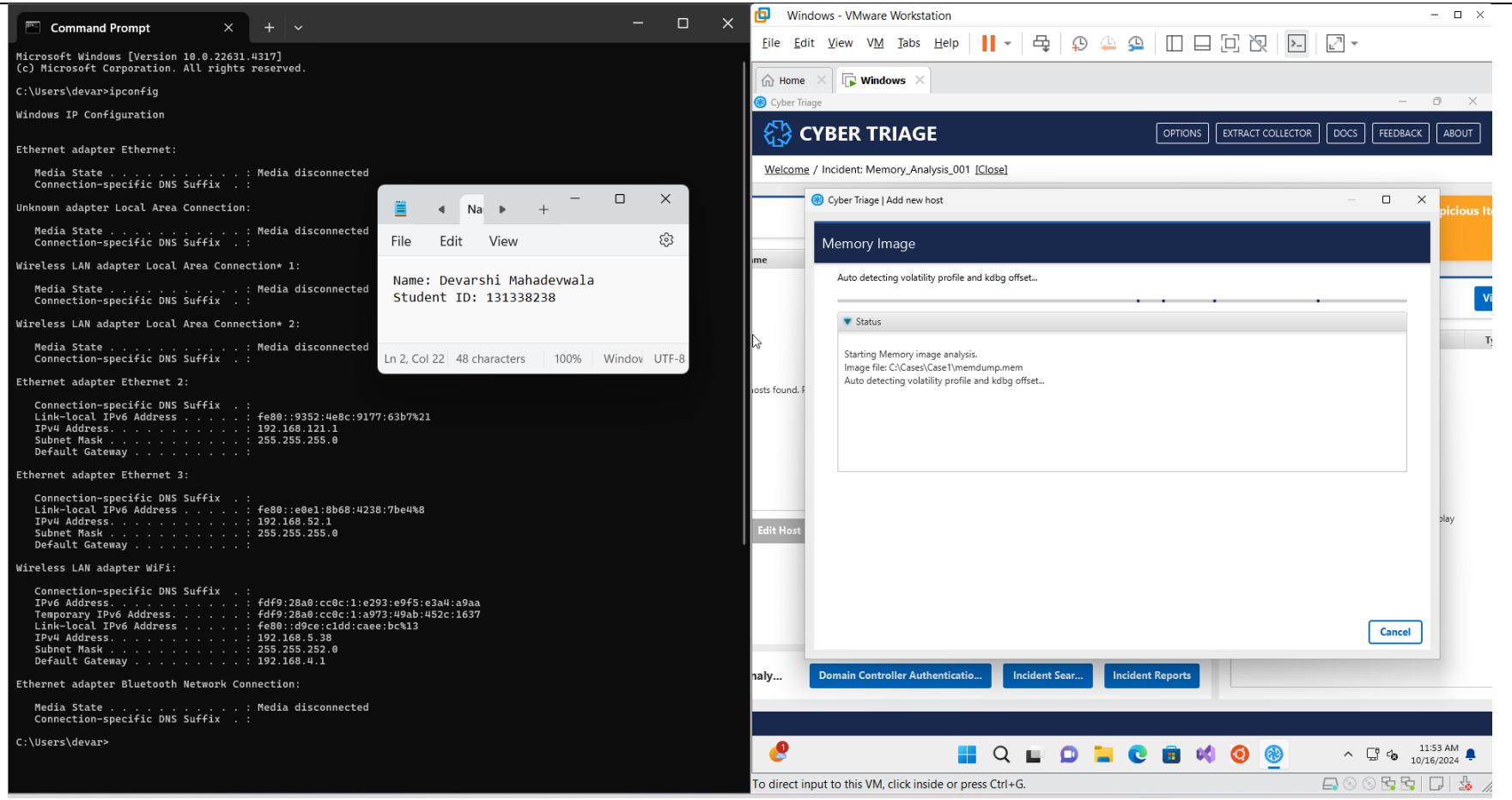
Let us now look at cyber triage.

The screenshot shows a Windows desktop environment. In the foreground, a Command Prompt window displays network configuration details for various adapters, including Ethernet, Local Area Connection, and WiFi. A small modal window is overlaid on the Command Prompt, showing user information: Name: Devarshi Mahadevwalla and Student ID: 131338238. In the background, a VMware Workstation window titled "Windows - VMware Workstation" is open, showing a virtual machine named "Cyber Triage". The Cyber Triage interface has a red header bar with the text "CYBER TRIAGE". Below it, a message says "Welcome / Incident: Evaluation Incident 2024-10-16 / Host: evaluation - demo data [Close]". The main interface is divided into sections: "Collection Information" (Bad Items: 0, Suspicious Items: 17), "Host Information" (listing host details like Host Name, OS, and Adapter IP), "Status" (listing analysis tasks like Targeted Analysis, Full Scan, and Malware Analysis), and "Recent Messages" (listing log entries such as "Collecting Network Connections and Ports... (Step 11 of 13)"). At the bottom of the Cyber Triage window, there is a status bar with the text "To direct input to this VM, click inside or press Ctrl+G." and a system tray with icons for power, volume, and date/time (11:32 AM, 10/16/2024).

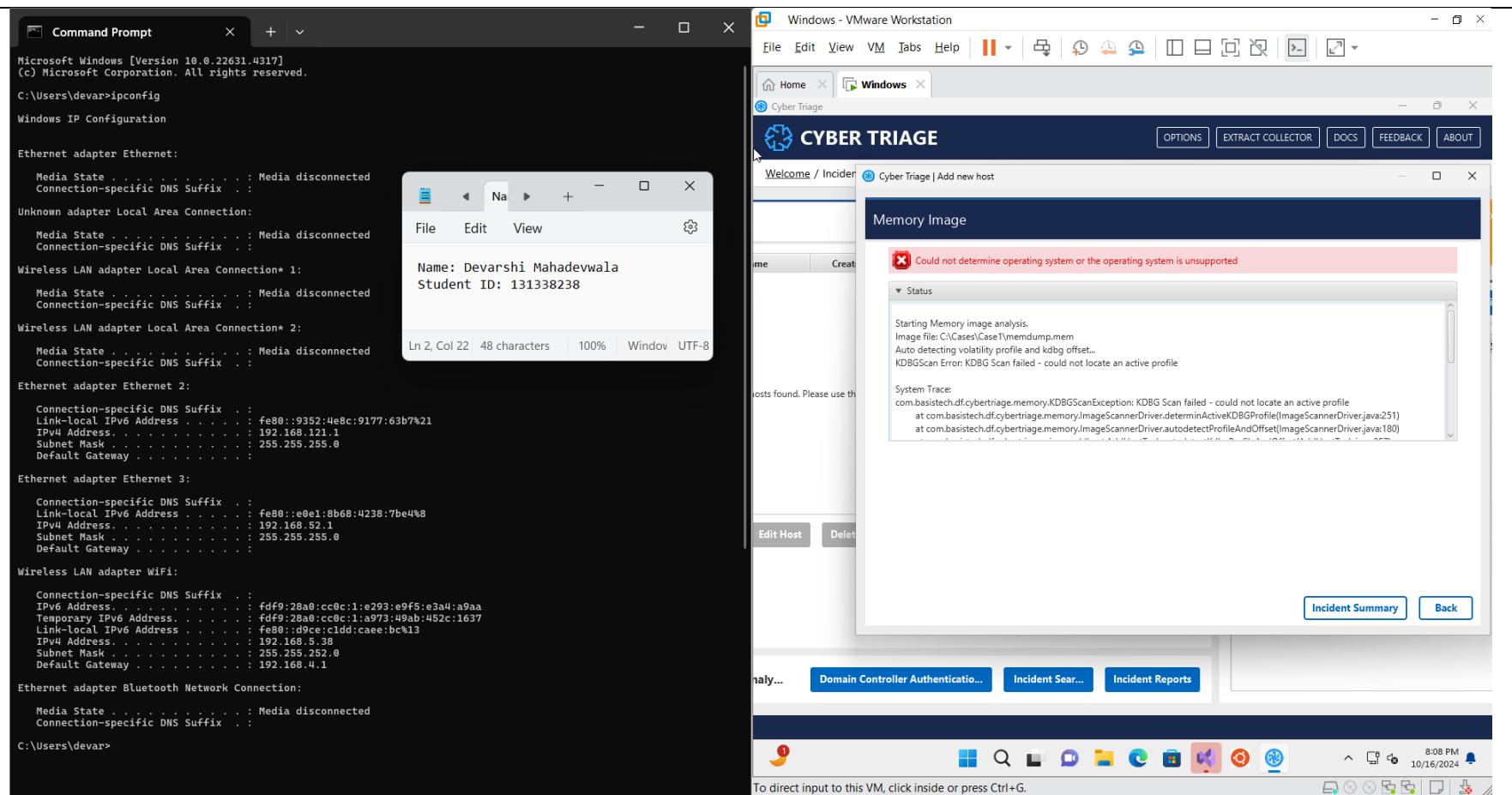
Here, cyber triage is running a scan on the host to find any bad or suspicious items.

The screenshot displays a Windows environment within a VMware Workstation window. On the left, a Command Prompt window shows the results of the ipconfig command, listing network adapter details including MAC addresses and IP configurations. A small file viewer window is overlaid on the Command Prompt, displaying a text file with the user's name and student ID. On the right, the Cyber Triage application is open, showing a 'New Incident' dialog box. The dialog box contains fields for 'Incident Name' (Memory\_Analysis\_001) and 'Description' (This is for a IT forensics Project that we have been assigned). Below the dialog, the Cyber Triage interface shows a system status summary with metrics like 'Hosts analyzed' (1), 'Hosts not analyzed' (0), and an 'Automatically generated evaluation' section.

We need to create a new incident to conduct analysis as this will create a proper pathway for us to navigate to the scans we have conducted.

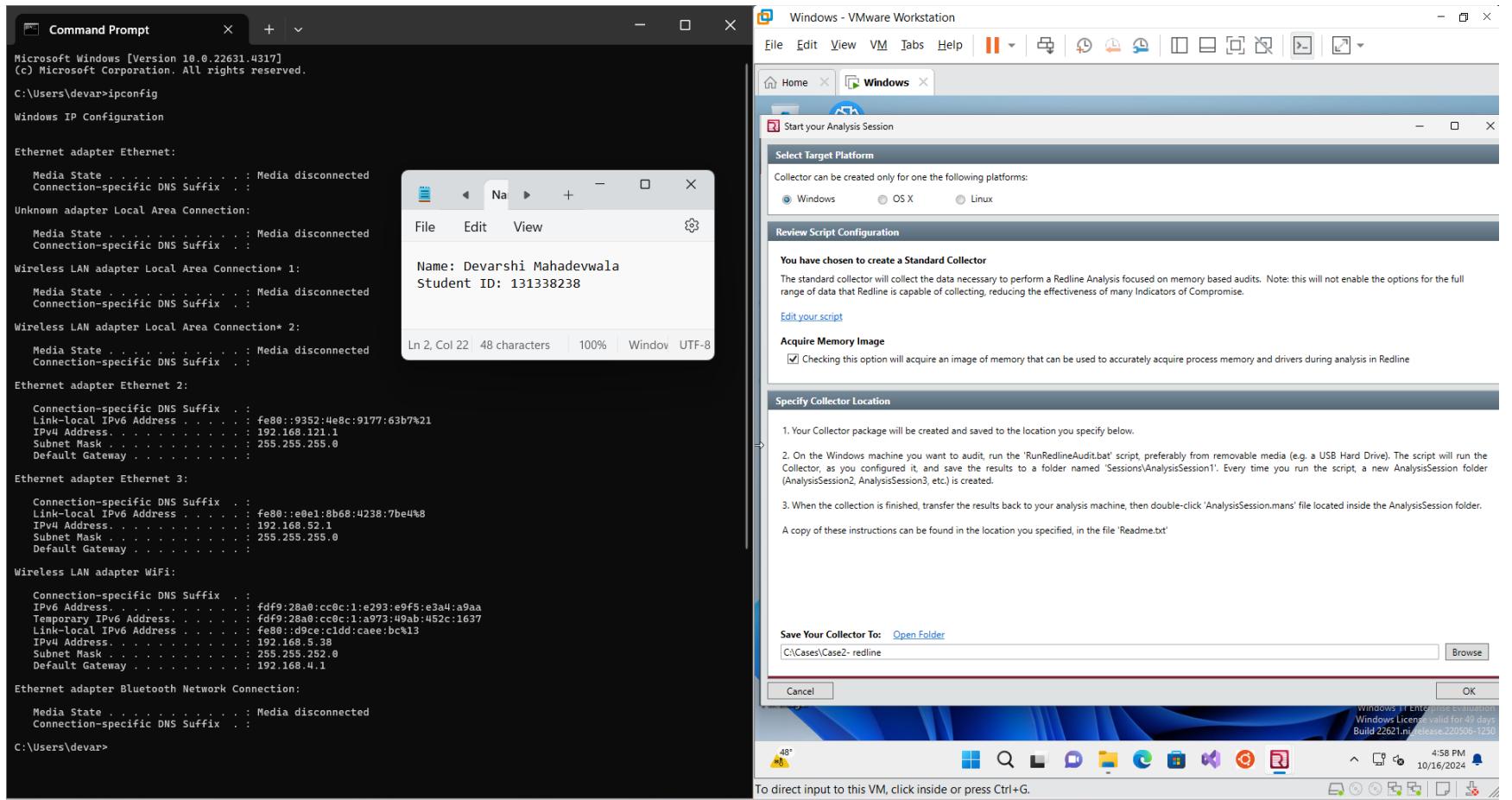


Now, we start our scan on the FTK image file. The application is currently running the scan on our image file.

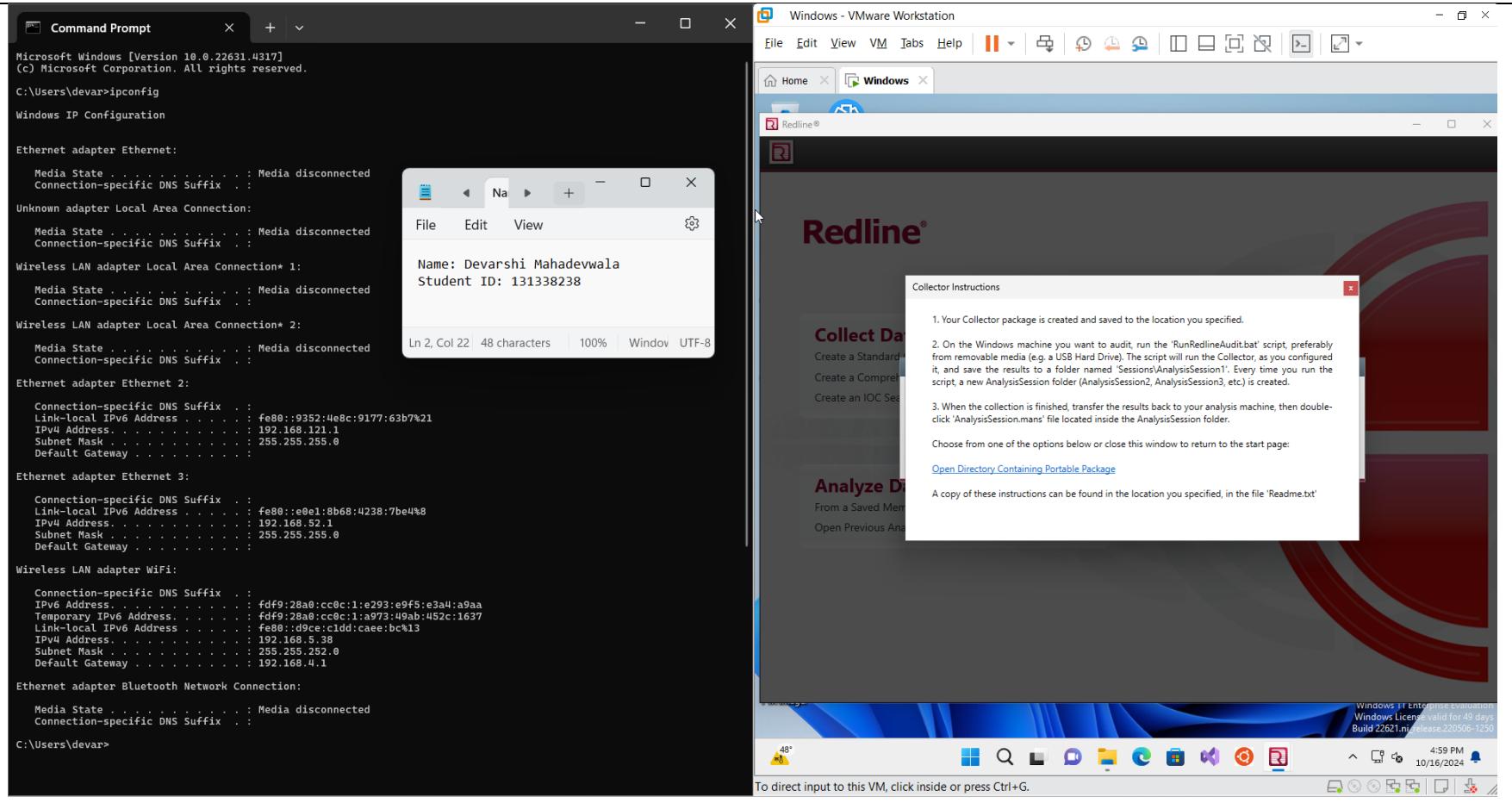


Usually, at this point the memory image analysis should be complete and give you a detailed report about your image file. But I was getting some error about which operating system is supported. I tried this for 5-6 times with every bug fix that I can conduct but it gave me the same result every time.

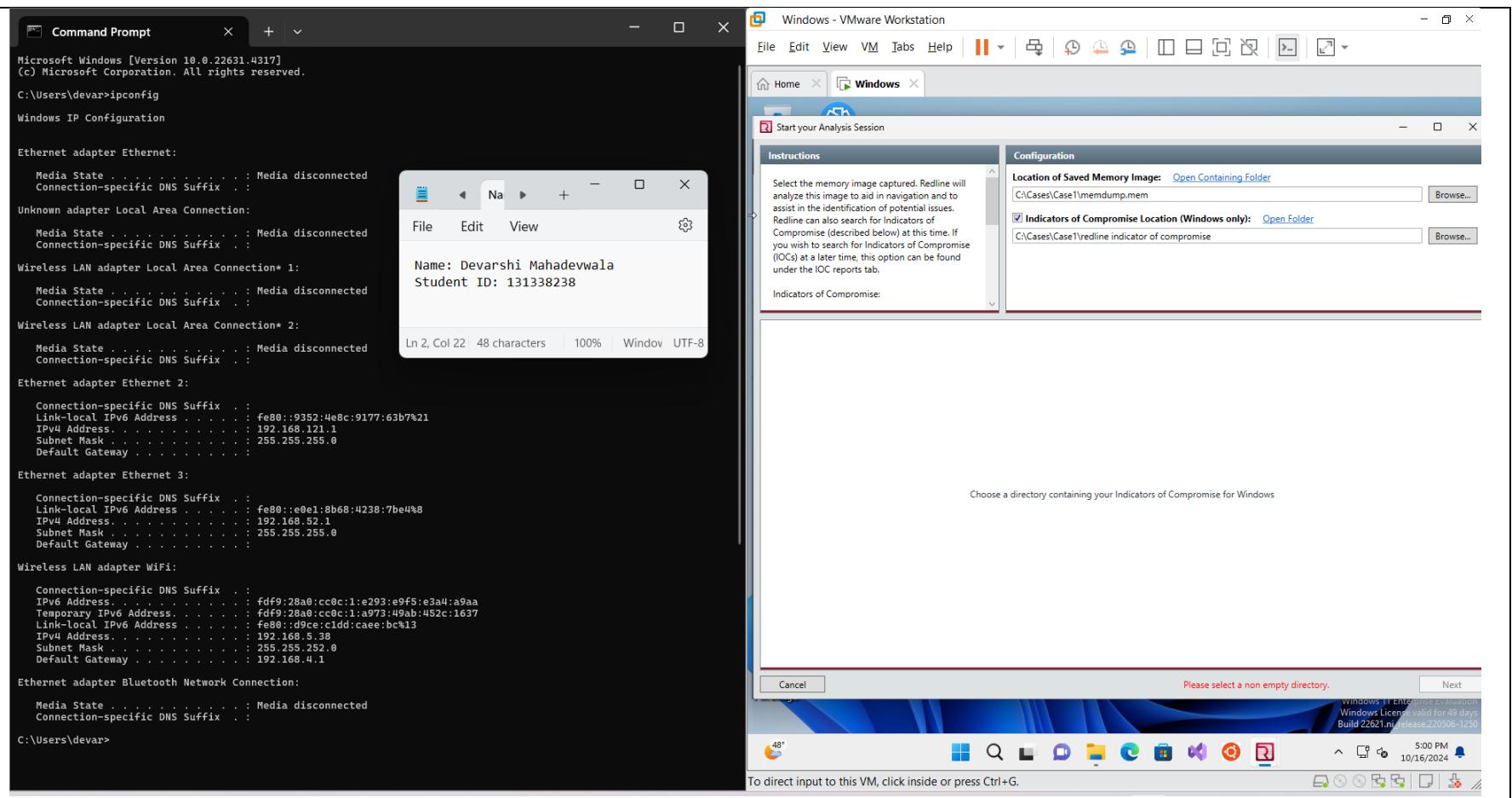
Now, let us move on to redline.



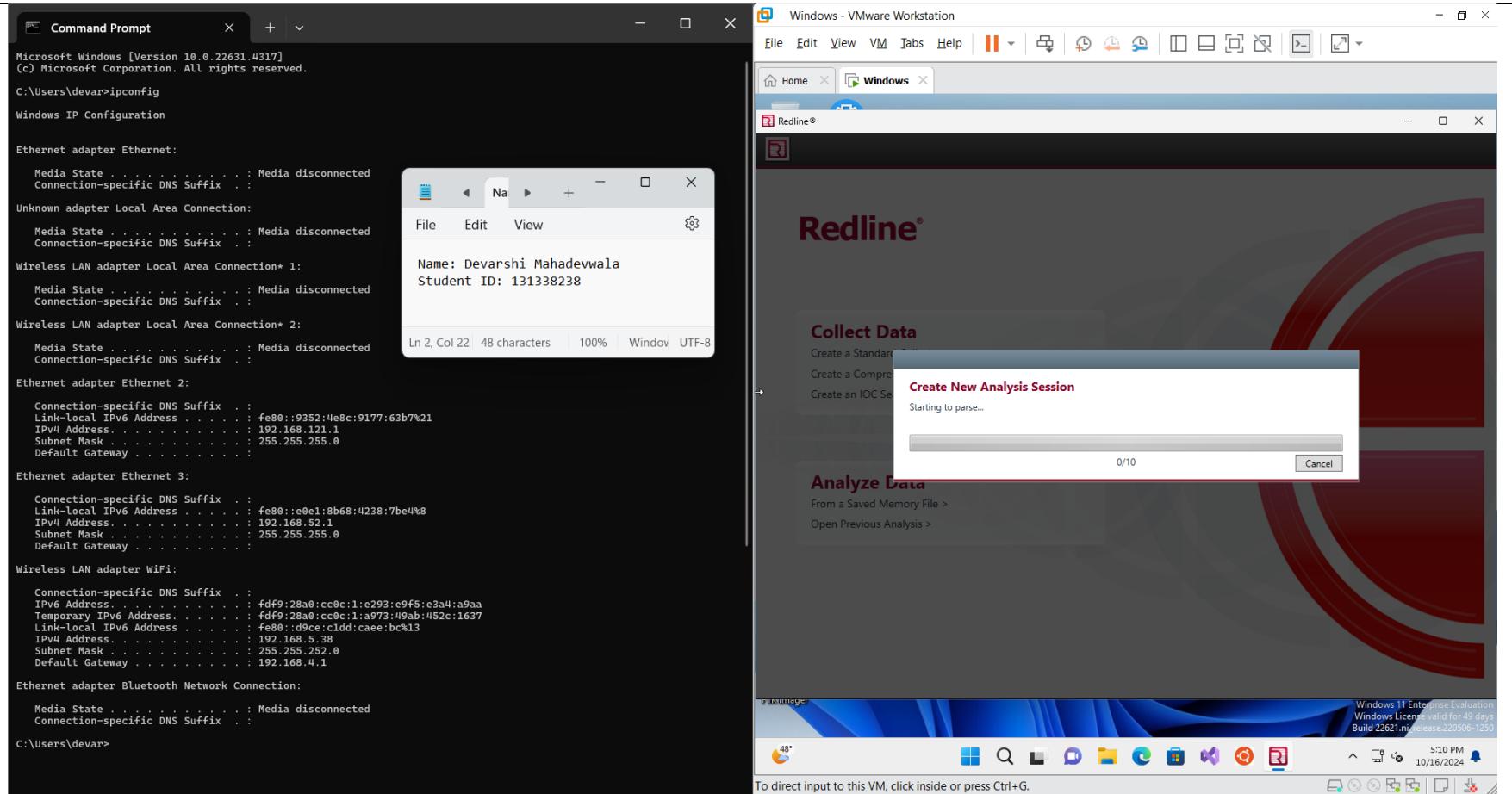
We can collect data from redline so we will create a new case in our C:\Cases to store our data.



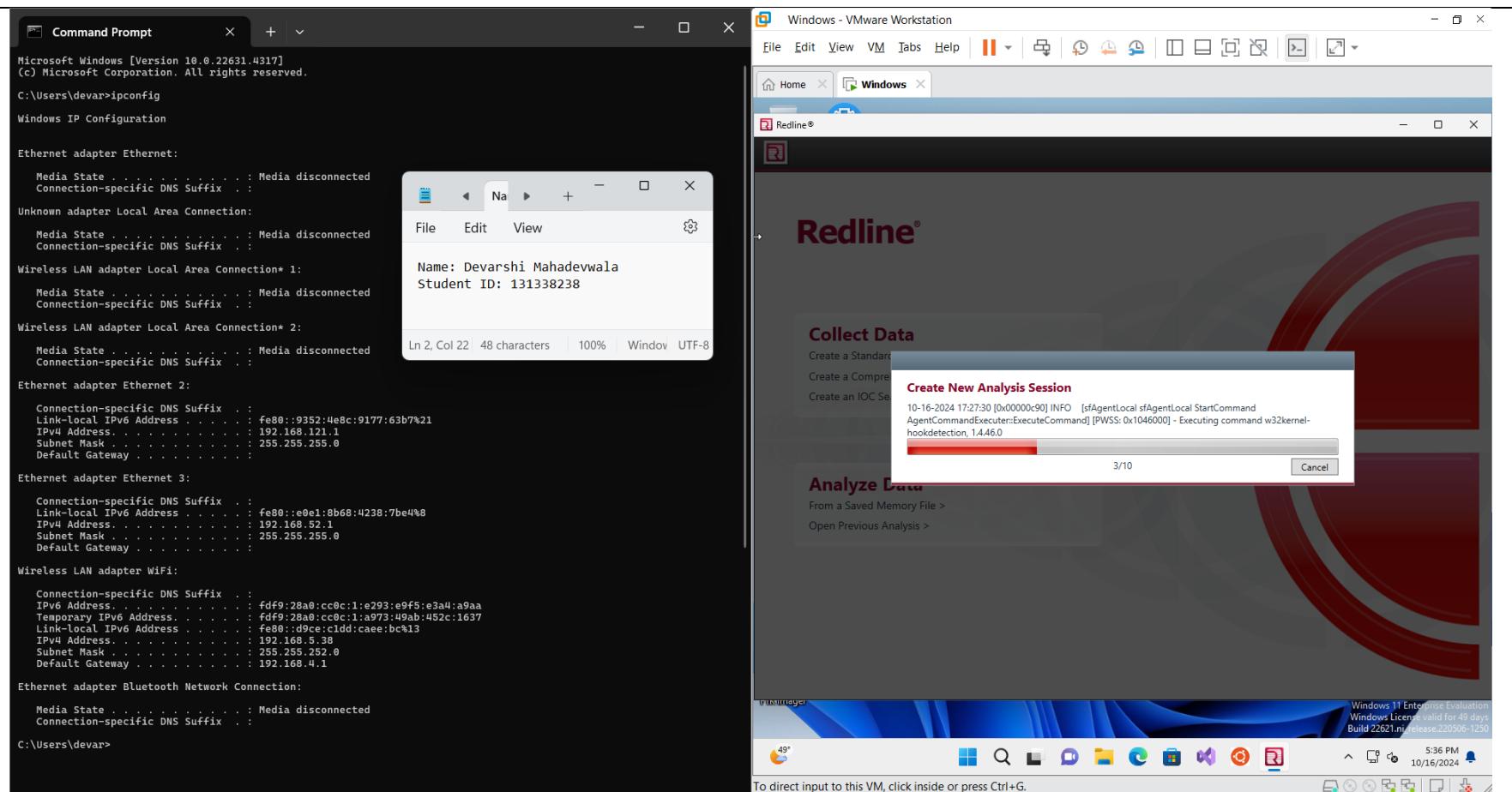
The package has been collected and stored at the specified destination.



Now to conduct a memory analysis on our memory image, we need to start our analysis and specify the file on which we need to conduct our analysis.



Our analysis is running, and this will create a new session for us to analyse our packages.



The scan is in process, it will take some time.

I faced a problem. When the analysis completed, I needed to include some indicators of compromise (IOC) which I tried solving but I found no way around this as the IOC needed was specifically for the memory image. Thus, I couldn't get redline to work too.

## **Personal Learning Experience Report on Memory Analysis Workstation Setup**

### **1. Introduction to Memory Analysis**

Setting up a forensics workstation was an enlightening experience, providing insight into the tools and techniques used for memory analysis. Memory forensics is critical for uncovering malicious activity and gaining a deeper understanding of an incident. The process allowed me to experiment with tools like Redline, Cyber Triage, and Volatility, offering hands-on experience in real-world digital forensics.

### **2. Building the Workstation**

The first step involved setting up a forensic workstation following a guide from Blue Cape Security. The process included configuring the necessary software, setting up the hardware, and ensuring a stable environment. This setup was essential for preparing a dedicated machine for forensic analysis, providing a controlled environment for working on memory analysis tasks without compromising the system's integrity.

Challenges included navigating software configurations and troubleshooting dependencies. For example, installing Python for Volatility required specific library versions. Despite these hurdles, configuring the workstation taught me the importance of meticulous preparation and checking for compatibility with the software.

### **3. Memory Image Acquisition**

I followed guidance from DFIR Madness to capture a memory image of my machine. The process required using tools like FTK Imager to generate a .mem file. This experience emphasized the importance of maintaining the integrity of the data, ensuring no alterations were made during acquisition.

Capturing memory from a live system proved to be an engaging task, as it required careful handling to avoid tampering with potentially volatile data. The .mem file provided a complete snapshot of system memory, allowing for in-depth analysis using various forensic tools.

### **4. Memory Analysis Using Redline, Cyber Triage, and Volatility**

Exploring multiple tools helped to understand different capabilities and approaches to memory analysis.

**Redline:** I used this tool for comprehensive memory analysis, which involved scanning the captured memory image for potential indicators of compromise. Its user-friendly interface and detailed reports made it easier to identify suspicious processes and anomalies.

**Cyber Triage:** This tool allowed for automated analysis, which quickly highlighted potentially malicious activities. The incident-based approach of Cyber Triage streamlined the investigation process, providing quick insights into various artifacts.

**Volatility:** As an open-source tool, Volatility provided more control over memory analysis through command-line usage. Running specific commands to detect malicious processes, network connections, and registry keys provided a deeper understanding of how memory artifacts correlate with potential threats.

	<p>Each tool had its strengths; for instance, Redline was efficient for initial triage, while Volatility offered more granular analysis capabilities.</p> <p><b>5. Personal Insights and Learning Outcomes</b></p> <p>This experience highlighted the complexity and necessity of memory forensics in cybersecurity. Understanding how to navigate different tools and handle the nuances of memory data was challenging but rewarding. Key takeaways included:</p> <ul style="list-style-type: none"> <li>Tool Capabilities and Limitations: Each tool provides different insights based on its approach to memory forensics. It's essential to understand their capabilities to utilize them effectively.</li> <li>Challenges in Data Interpretation: Memory analysis often yields large volumes of data, requiring the use of filters and advanced techniques to identify significant indicators of compromise.</li> <li>Importance of Documentation and Reporting: Keeping detailed records of each step during the analysis process helps in tracking progress, troubleshooting issues, and ensuring accurate reporting.</li> </ul> <p><b>6. Conclusion</b></p> <p>Overall, setting up the forensic workstation and conducting memory analysis provided a comprehensive learning experience in digital forensics. Using multiple tools demonstrated the strengths and weaknesses of various approaches to memory analysis. The practical application of these tools to detect potential threats greatly improved my understanding of cybersecurity practices and prepared me for future forensic tasks.</p>
Grading Alerts	<ul style="list-style-type: none"> <li>• If you do NOT use this template or delete any part of it or use any other template, you will be degraded.</li> <li>• If you do NOT follow the file naming convention, you will be degraded.</li> <li>• If you do NOT submit your file in PDF; you will be degraded.</li> <li>• If you do NOT show your account real name (when applicable); you will be degraded.</li> <li>• If you do NOT show your machine desktop background (with date &amp; time) and IP, you will be degraded.</li> <li>• If you do NOT write (in your own words) your learning experience for the activity practices, you will be degraded.</li> </ul>