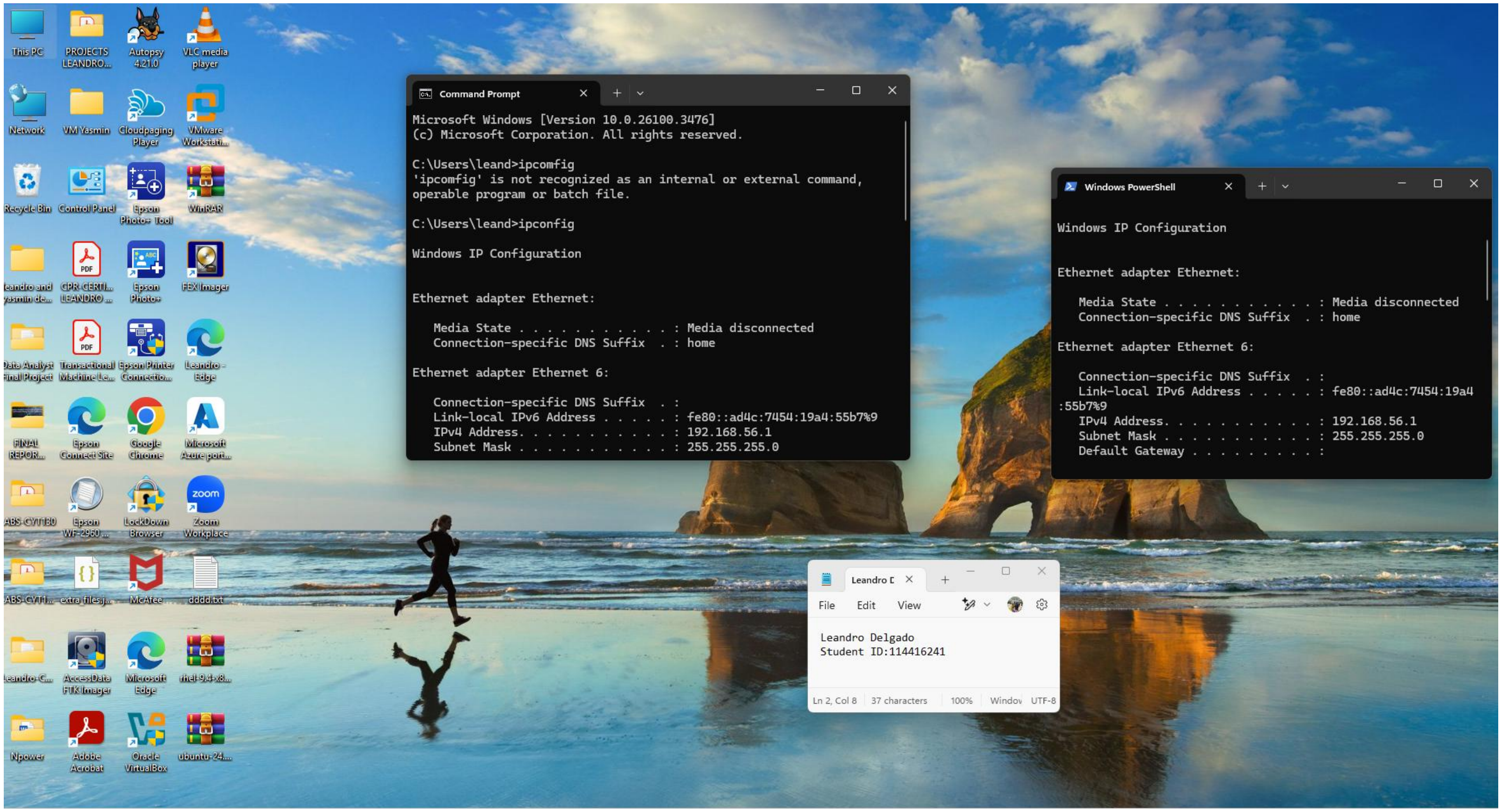
Put Student Name(s) ↓	Put Student IDs ↓	Due Date	Grade Weight
LEANDRO DELGADO	114416241	As Posted	12%

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	• It is an Individual assignment. Put your name + Student ID in the empty spaces above. • Submit via the BB relevant link ONLY. NO submission via email please. Be sure to submit the final version file ONLY. • Show me genuine signs of your work is done on your machine. This includes: ○ Screenshots that show your desktop background with Date/Time ○ Show me a pop-up bx that shows "your name + IP." ○ Show your logged in account, if applicable ○ Optional: Show your photo. • Use this same template to include your work in the specified fields below. Submit in PDF. • Submit your report name with the name: CYT215-Project1-Student Name & ID
Students Work required for this activity	1. You will follow instructions to setup your own forensics workstation on your machine. 2. You will check that your forensics workstation is functioning. 3. You will use your workstation for memory & malware analysis. 4. You will Prepare Your Target System (your own machine). You will Build Your basic Lab.
How to start	• Read thoroughly & follow the instructions mentioned in this link. The instructions will guide you to a step-by-step of how you complete your work successfully https://bluecapesecurity.com/build-your-forensic-workstation/ • Take an image of your machine memory. Use this link for guidance: https://dfirmadness.com/case-001-memory-analysis/ • You can use any installed tool or focus on common tools for memory analysis e.g.: Volatility; Cyber Triage; Rekall; Redline;
Important	• Your target system should be your own machine
Students Reports	



```
Microsoft Windows [Version 10.0.26100.3476]
(c) Microsoft Corporation. All rights reserved.

C:\Users\leand>ipcomfig
'ipcomfig' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\leand>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

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

Ethernet adapter Ethernet 6:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ad4c:7454:19a4:55b7%9
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

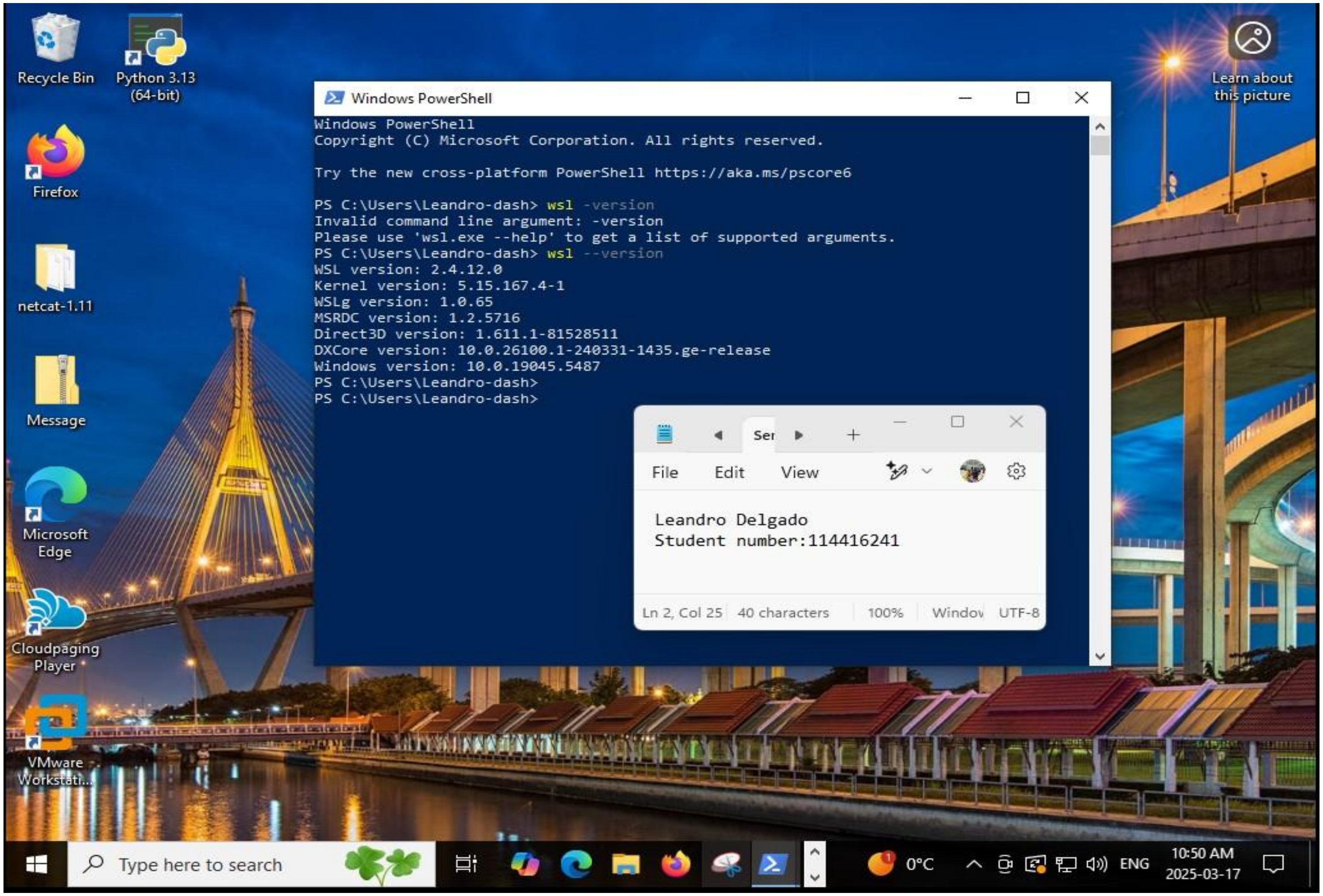
```
Windows IP Configuration


Ethernet adapter Ethernet:

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

Ethernet adapter Ethernet 6:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ad4c:7454:19a4
:55b7%9
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

```
Leandro Delgado
Student ID:114416241
```

Process of Forensics Workstations

Once I had installed the windows Vm on my systems, I proceed to install some tools mentioned on the instructions link provide by the instructor.

Installation of WSL was installed providing the version of the software on my Vm machine



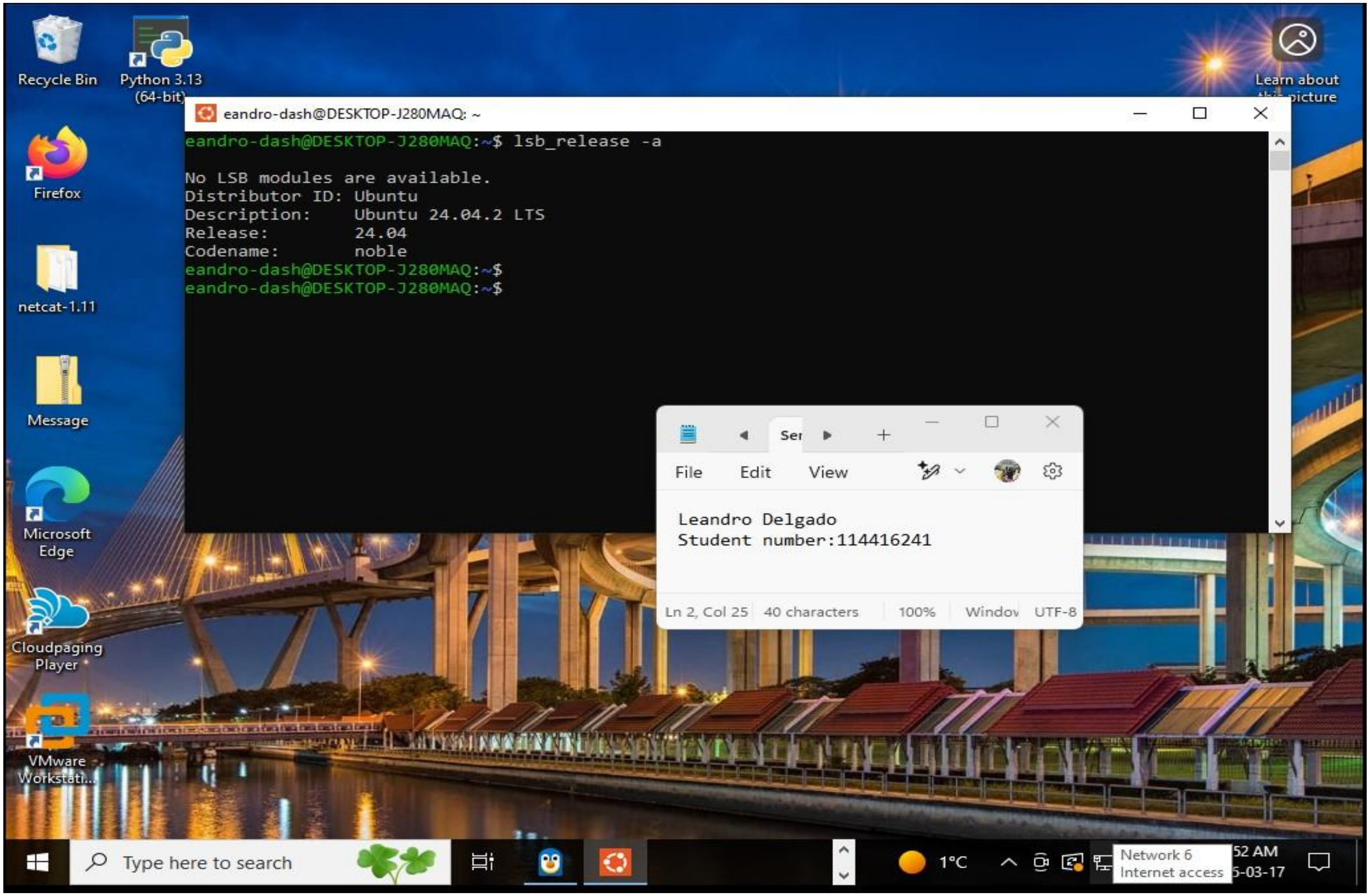
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Leandro-dash> wsl -version
Invalid command line argument: -version
Please use 'wsl.exe --help' to get a list of supported arguments.
PS C:\Users\Leandro-dash> wsl --version
WSL version: 2.4.12.0
Kernel version: 5.15.167.4-1
WSLg version: 1.0.65
MSRDC version: 1.2.5716
Direct3D version: 1.611.1-81528511
DXCore version: 10.0.26100.1-240331-1435.ge-release
Windows version: 10.0.19045.5487
PS C:\Users\Leandro-dash>
PS C:\Users\Leandro-dash>
```

```
Leandro Delgado
Student number:114416241
```

Ln 2, Col 25 | 40 characters | 100% | Windov | UTF-8

Figure 1.Installation of WSL ona windoms Vm

Ubuntu Installation

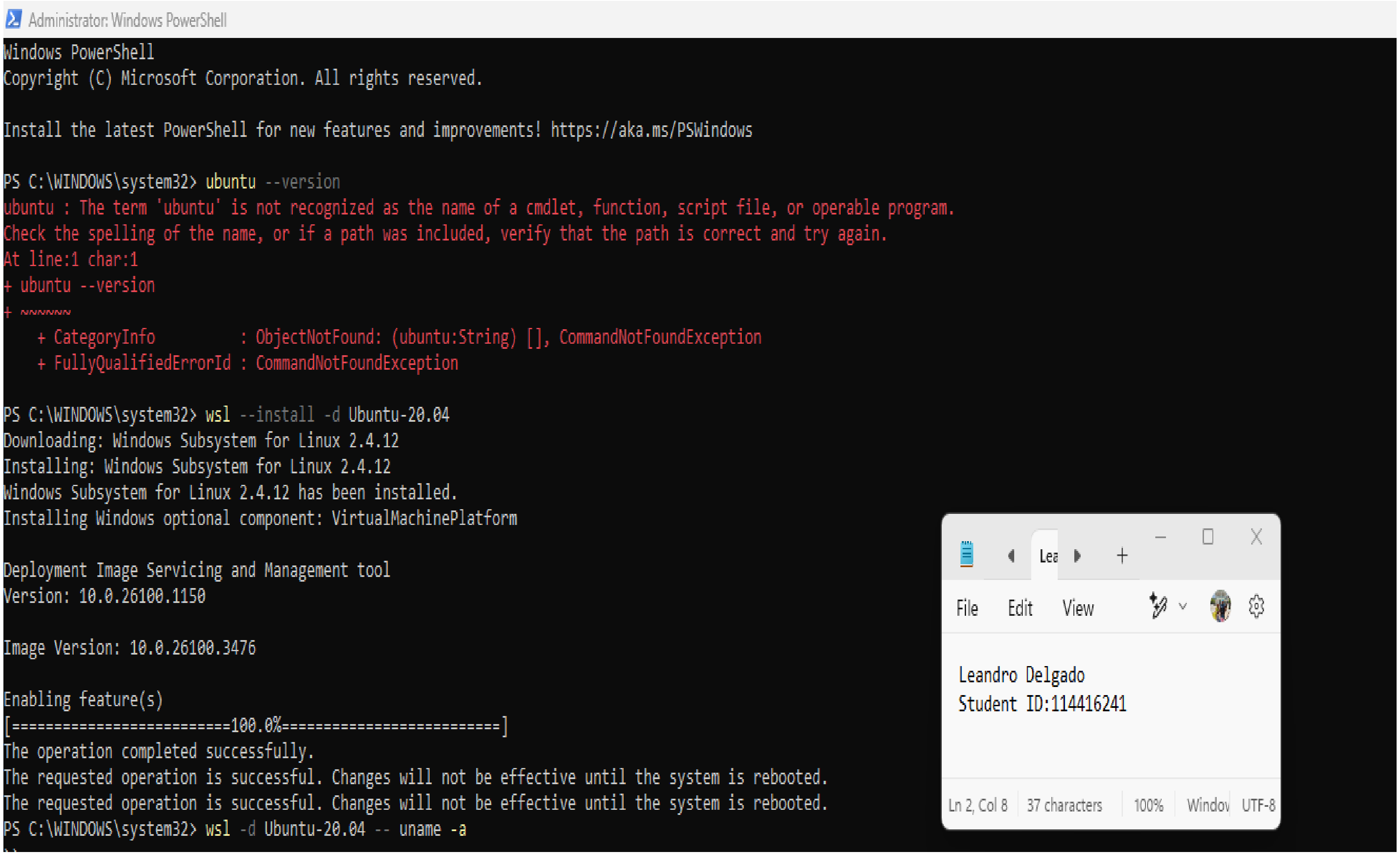


```
eandro-dash@DESKTOP-J280MAQ:~$ lsb_release -a

No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 24.04.2 LTS
Release:        24.04
Codename:       noble
eandro-dash@DESKTOP-J280MAQ:~$
eandro-dash@DESKTOP-J280MAQ:~$
```

Leandro Delgado
Student number:114416241

Figure 2.Ubuntu Installation

Process UBUNTU Installation

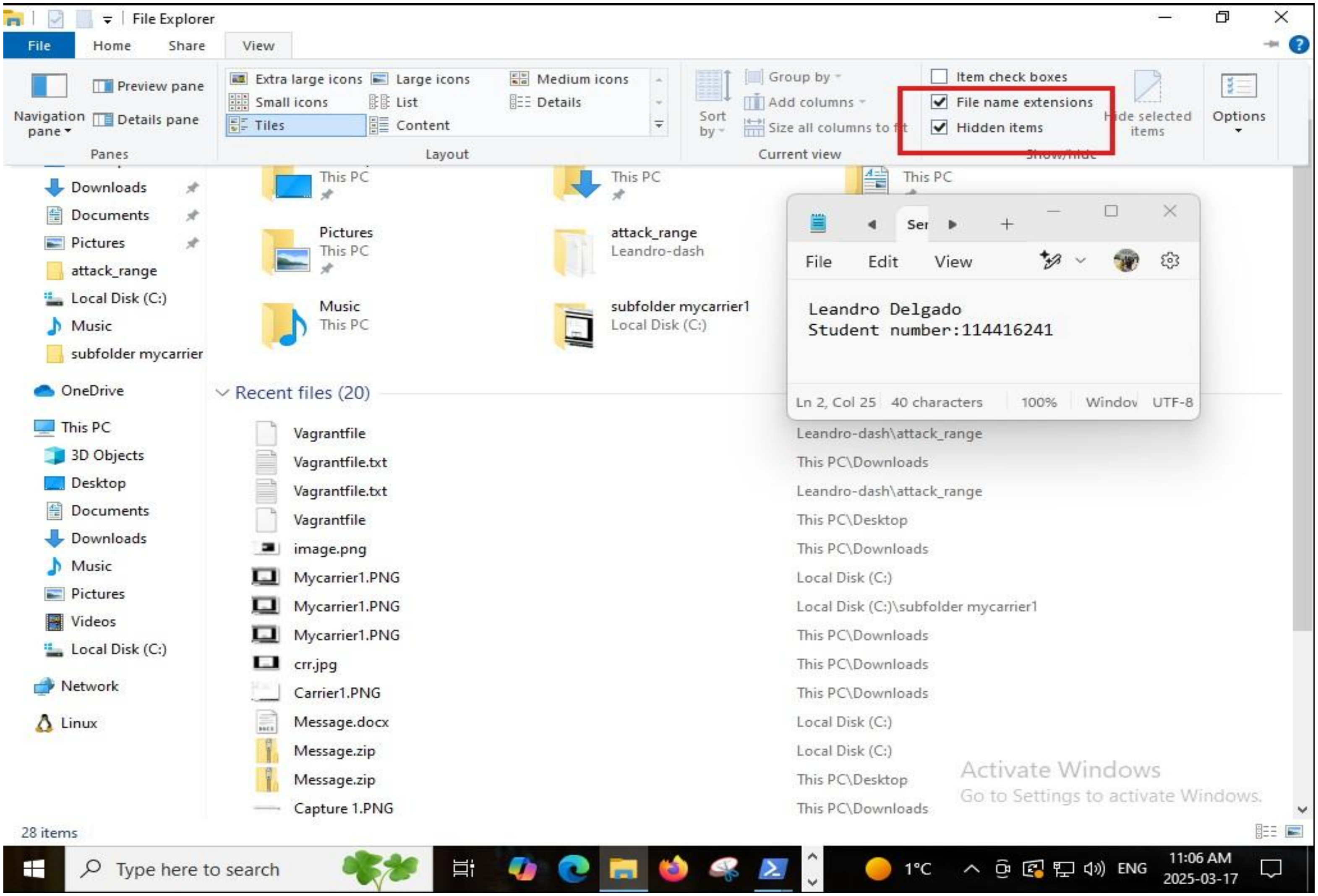


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\WINDOWS\system32> ubuntu --version
ubuntu : The term 'ubuntu' is not recognized as the name of a cmdlet, function, script file, or operable program.
Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ ubuntu --version
+ ~~~~~~
    + CategoryInfo          : ObjectNotFound: (ubuntu:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\WINDOWS\system32> wsl --install -d Ubuntu-20.04
Downloading: Windows Subsystem for Linux 2.4.12
Installing: Windows Subsystem for Linux 2.4.12
Windows Subsystem for Linux 2.4.12 has been installed.
Installing Windows optional component: VirtualMachinePlatform

Deployment Image Servicing and Management tool
Version: 10.0.26100.1150

Image Version: 10.0.26100.3476

Enabling feature(s)
[==========================100.0%==========================]
The operation completed successfully.
The requested operation is successful. Changes will not be effective until the system is rebooted.
The requested operation is successful. Changes will not be effective until the system is rebooted.
PS C:\WINDOWS\system32> wsl -d Ubuntu-20.04 -- uname -a
```

Leandro Delgado
Student ID:114416241

Figure 3.Process Ubuntu Installation

In the file explorer, we create a ‘Cases’ and ‘Tools’ folder and show all hidden folders.



□ Item check boxes
☑ File name extensions
☑ Hidden items

Leandro Delgado
Student number:114416241

Ln 2, Col 25 | 40 characters | 100% | Windov | UTF-8

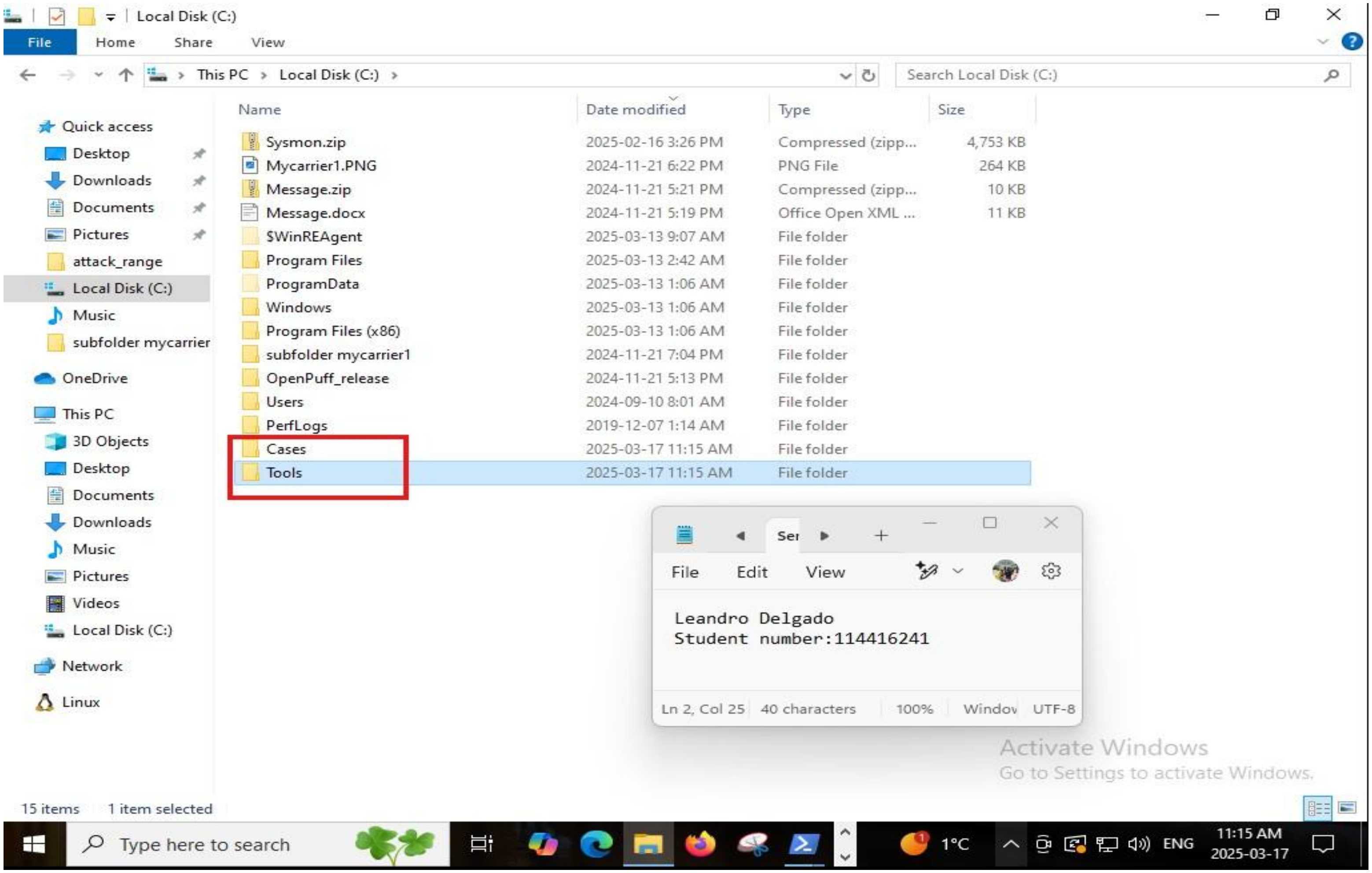
Vagrantfile	Leandro-dash\attack_range
Vagrantfile.txt	This PC\Downloads
Vagrantfile.txt	Leandro-dash\attack_range
Vagrantfile	This PC\Desktop
image.png	This PC\Downloads
Mycarrier1.PNG	Local Disk (C:)
Mycarrier1.PNG	Local Disk (C:)\subfolder mycarrier1
Mycarrier1.PNG	This PC\Downloads
crr.jpg	This PC\Downloads
Carrier1.PNG	This PC\Downloads
Message.docx	Local Disk (C:)
Message.zip	Local Disk (C:)
Message.zip	This PC\Desktop
Capture 1.PNG	This PC\Downloads

28 items

Figure 4.Creation of tools and cases folder.

Creation of tools and Folder

In the file explorer, we create a ‘Cases’ and ‘Tools’ folder and show all hidden folders.

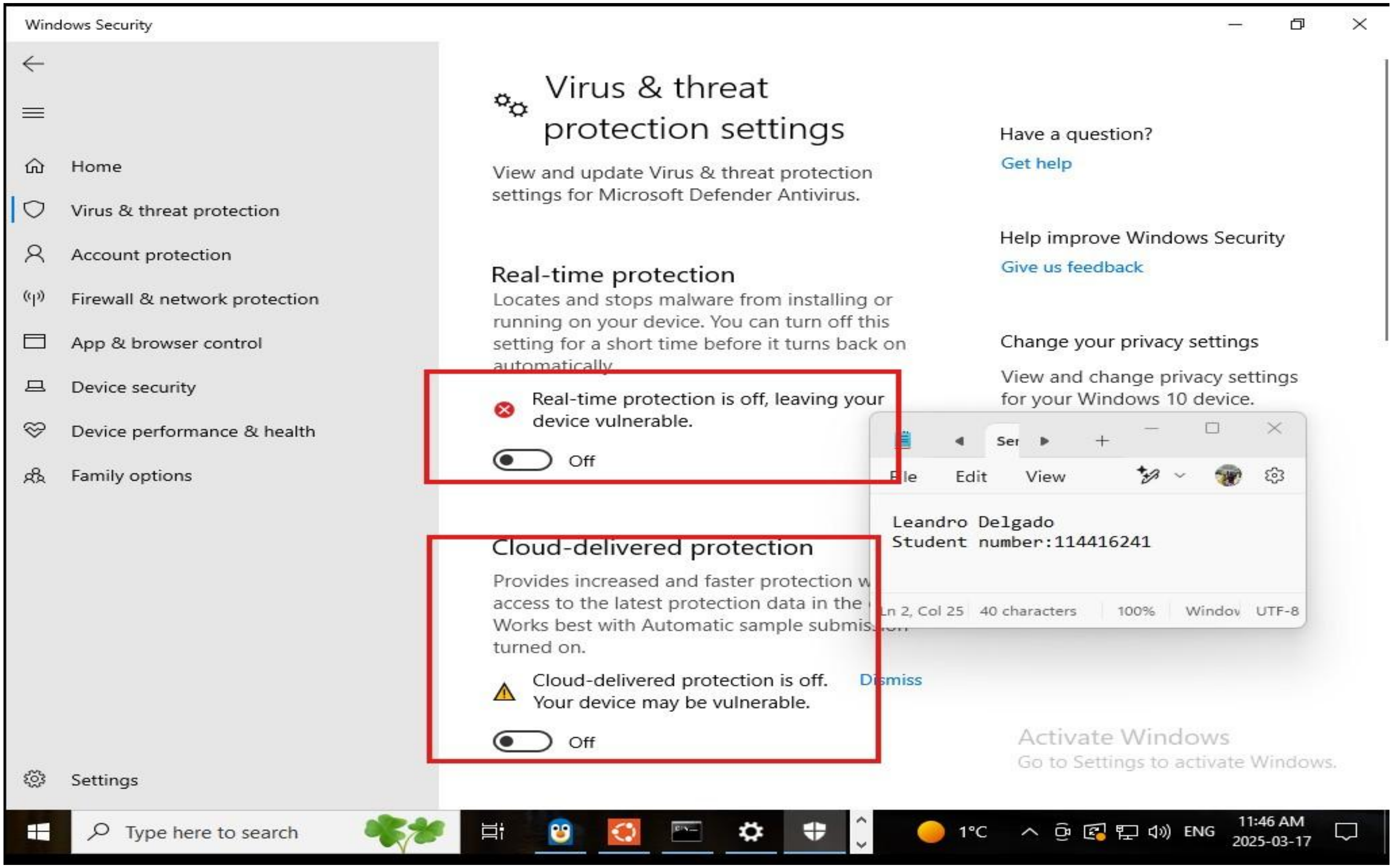


Name	Date modified	Type	Size
Sysmon.zip	2025-02-16 3:26 PM	Compressed (zipp...	4,753 KB
Mycarrier1.PNG	2024-11-21 6:22 PM	PNG File	264 KB
Message.zip	2024-11-21 5:21 PM	Compressed (zipp...	10 KB
Message.docx	2024-11-21 5:19 PM	Office Open XML ...	11 KB
$WinREAgent	2025-03-13 9:07 AM	File folder	
Program Files	2025-03-13 2:42 AM	File folder	
ProgramData	2025-03-13 1:06 AM	File folder	
Windows	2025-03-13 1:06 AM	File folder	
Program Files (x86)	2025-03-13 1:06 AM	File folder	
subfolder mycarrier1	2024-11-21 7:04 PM	File folder	
OpenPuff_release	2024-11-21 5:13 PM	File folder	
Users	2024-09-10 8:01 AM	File folder	
PerfLogs	2019-12-07 1:14 AM	File folder	
Cases	2025-03-17 11:15 AM	File folder	
Tools	2025-03-17 11:15 AM	File folder	

Leandro Delgado
Student number:114416241

Figure 5. Confirmation of folder creation

Setting process of Microsoft defender
For Microsoft Defender, we disable the protections enabled by default in Windows.



Windows Security

Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection w access to the latest protection data in the Works best with Automatic sample submis turned on.

Cloud-delivered protection is off. Your device may be vulnerable.

Off

Have a question?

Get help

Help improve Windows Security

Give us feedback

Change your privacy settings

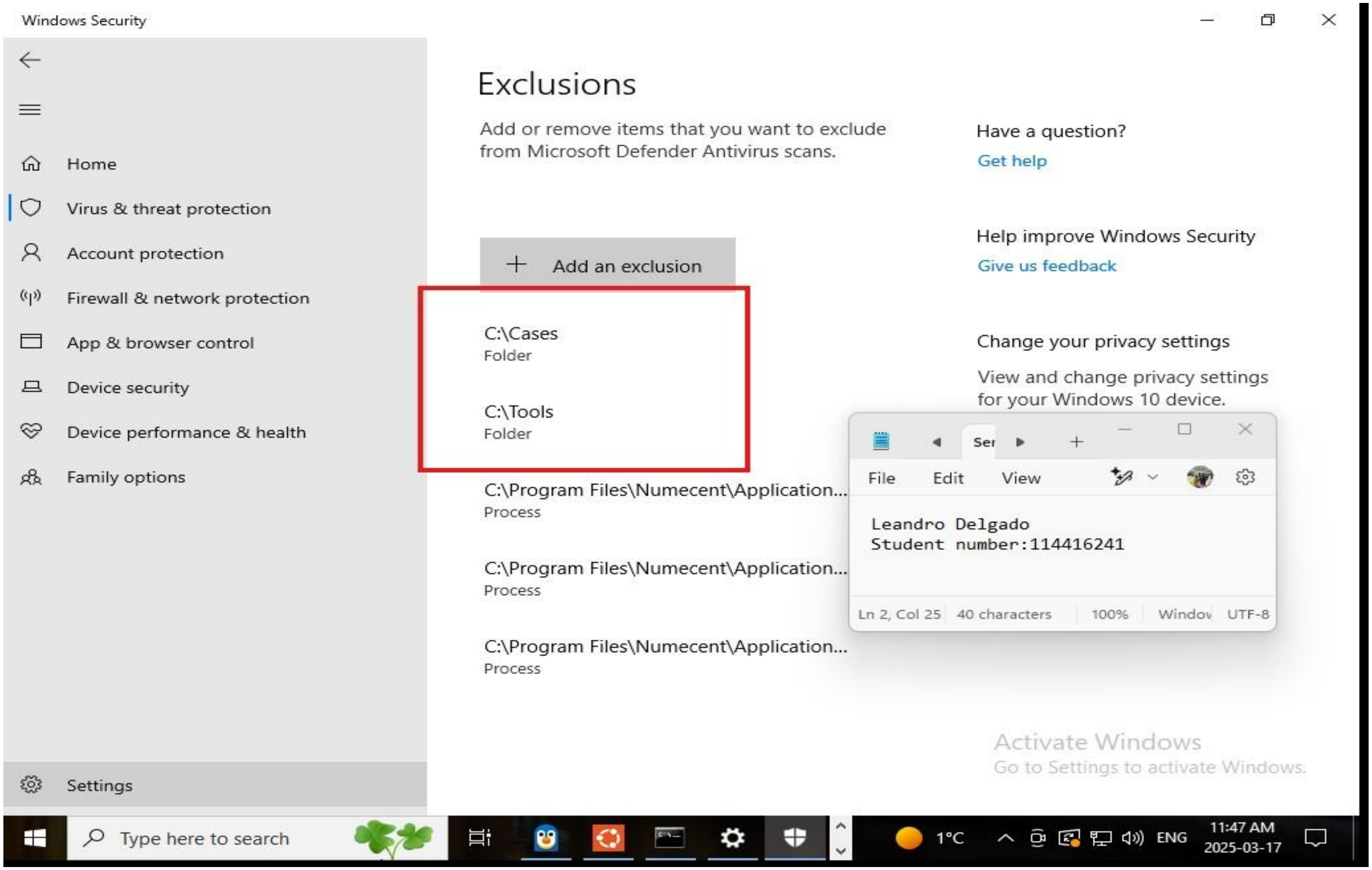
View and change privacy settings for your Windows 10 device.

```
Leandro Delgado
Student number:114416241
```

Activate Windows
Go to Settings to activate Windows.

Figure 6.Disable process on Microsoft Defender

Exclusion Of folders created



Exclusions

Add or remove items that you want to exclude from Microsoft Defender Antivirus scans.

C:\Cases
Folder

C:\Tools
Folder

C:\Program Files\Numecent\Application...
Process

C:\Program Files\Numecent\Application...
Process

C:\Program Files\Numecent\Application...
Process

Have a question?

Help improve Windows Security

Change your privacy settings

View and change privacy settings for your Windows 10 device.

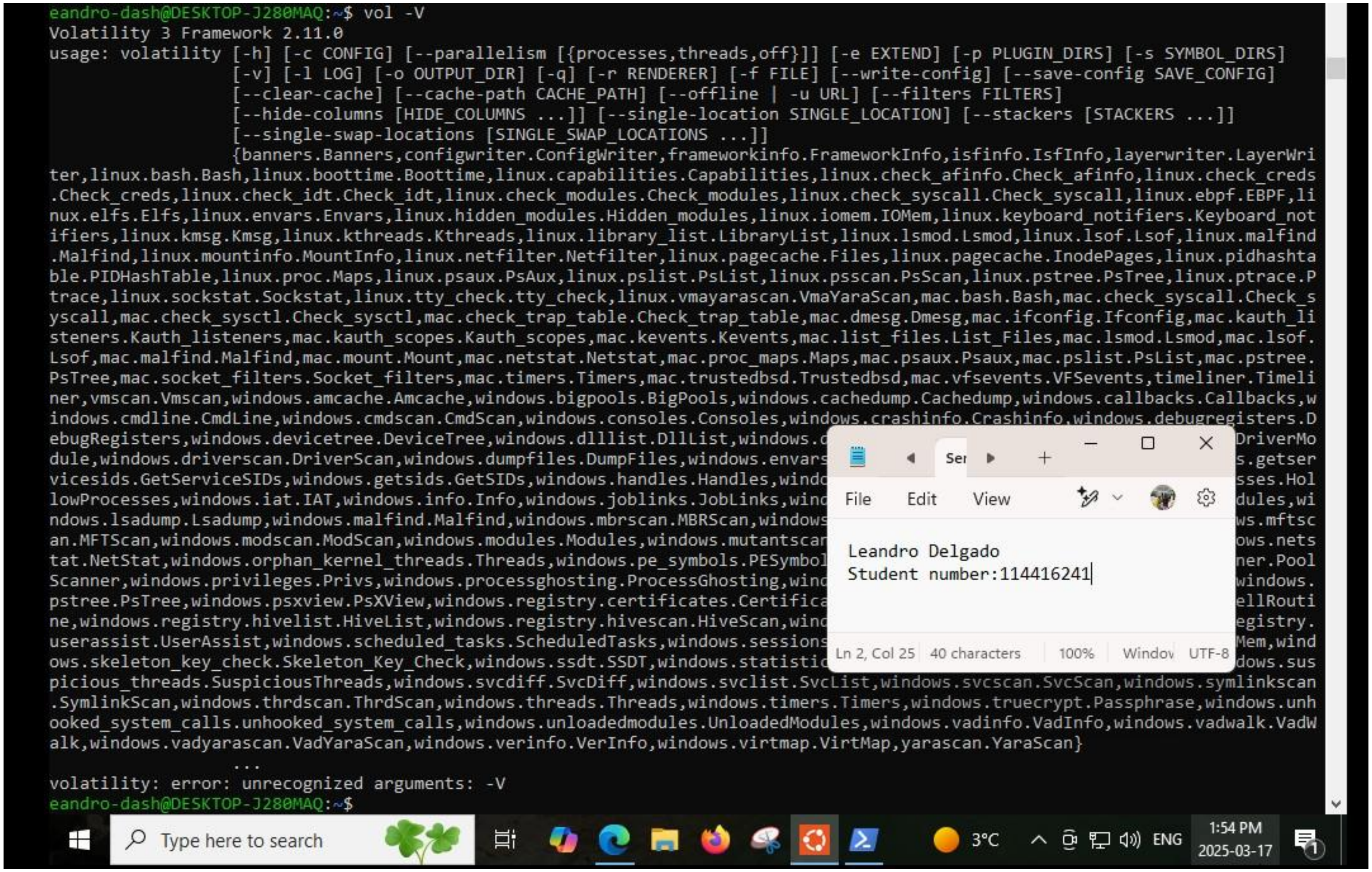
```
Leandro Delgado
Student number:114416241
```

Ln 2, Col 25 | 40 characters | 100% | Windov | UTF-8

Activate Windows
Go to Settings to activate Windows.

Figure 7. Exlusion of folder created on Vm

I installed a few tools for this step, theses are the results of the installation (volatility3, Log2timeline, python3):

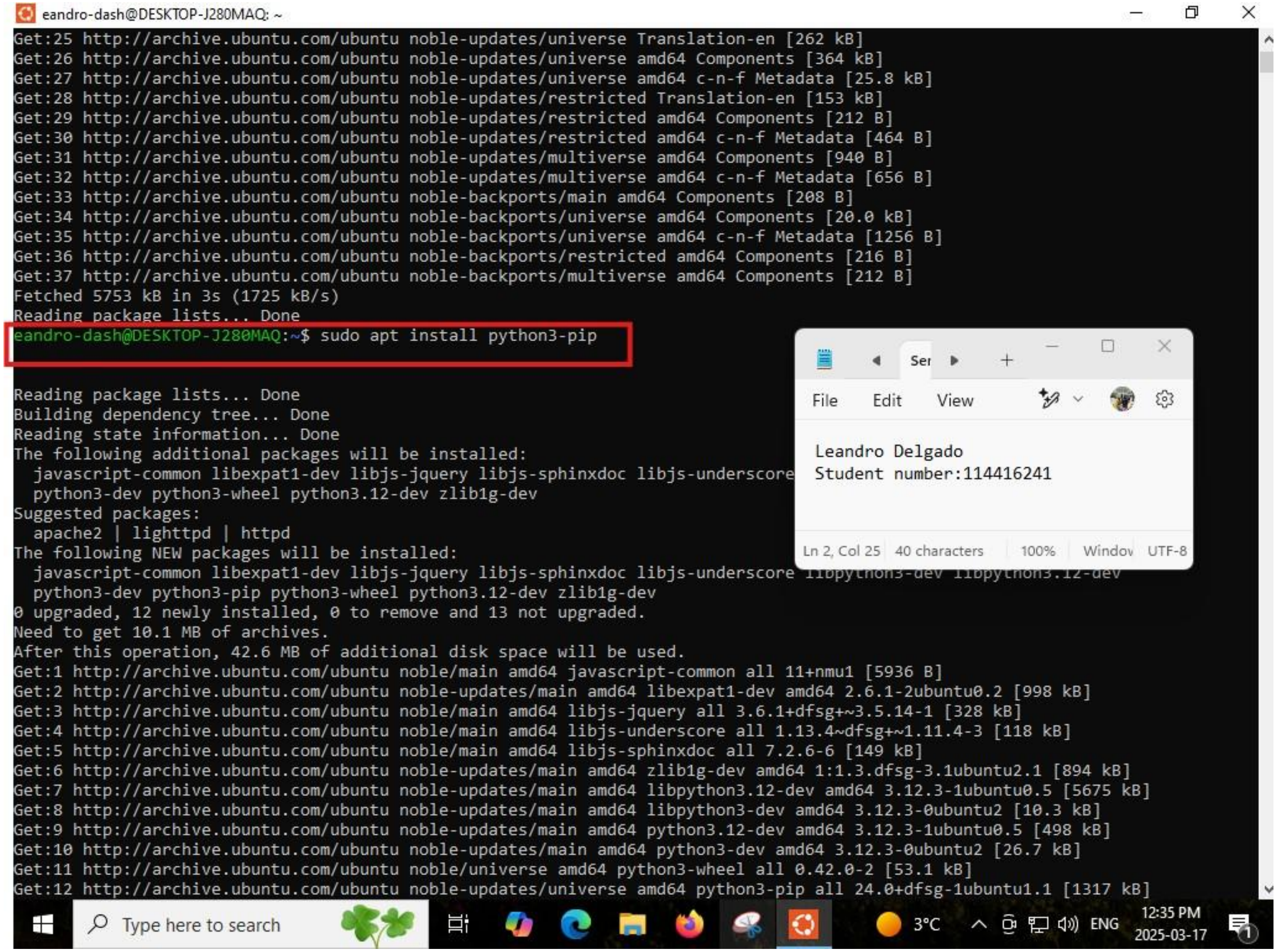


```
eandro-dash@DESKTOP-J280MAQ:~$ vol -V
Volatility 3 Framework 2.11.0
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS]
                  [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE_CONFIG]
                  [--clear-cache] [--cache-path CACHE_PATH] [--offline | -u URL] [--filters FILTERS]
                  [--hide-columns [HIDE_COLUMNS ...]] [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]]
                  [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
                  {banners.Banners,configwriter.ConfigWriter,frameworkinfo.FrameworkInfo,isfinfo.IsfInfo,layerwriter.LayerWri
ter,linux.bash.Bash,linux.boottime.Boottime,linux.capabilities.Capabilities,linux.check_afinfo.Check_afinfo,linux.check_creds
.Check_creds,linux.check_idt.Check_idt,linux.check_modules.Check_modules,linux.check_syscall.Check_syscall,linux.ebpf.EBPF,li
nux.elfs.Elfs,linux.envars.Envars,linux.hidden_modules.Hidden_modules,linux.iomem.IOMem,linux.keyboard_notifiers.Keyboard_not
ifiers,linux.kmsg.Kmsg,linux.kthreads.Kthreads,linux.library_list.LibraryList,linux.lsmod.Lsmod,linux.lsof.Lsof,linux.malfind
.Malfind,linux.mountinfo.MountInfo,linux.netfilter.Netfilter,linux.pagecache.Files,linux.pagecache.InodePages,linux.pidhashta
ble.PIDHashTable,linux.proc.Maps,linux.psaux.PsAux,linux.pslist.PsList,linux.psscan.PsScan,linux.pstree.PsTree,linux.ptrace.P
trace,linux.sockstat.Sockstat,linux.tty_check.tty_check,linux.vmayarascan.VmaYaraScan,mac.bash.Bash,mac.check_syscall.Check_s
yscall,mac.check_sysctl.Check_sysctl,mac.check_trap_table.Check_trap_table,mac.dmesg.Dmesg,mac.ifconfig.Ifconfig,mac.kauth_li
steners.Kauth_listeners,mac.kauth_scopes.Kauth_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_filters.Socket_filters,mac.timers.Timers,mac.trustedbsd.Trustedbsd,mac.vfsevents.VFSevents,timeliner.Timeli
ner,vmscan.Vmscan,windows.amcache.Amcache,windows.bigpools.BigPools,windows.cachedump.Cachedump,windows.callbacks.Callbacks,w
indows.cmdline.CmdLine,windows.cmdscan.CmdScan,windows.consoles.Consoles,windows.crashinfo.Crashinfo,windows.debugregisters.D
ebugRegisters,windows.devicetree.DeviceTree,windows.dlllist.DllList,windows.c                                      DriverMo
dule,windows.driverscan.DriverScan,windows.dumpfiles.DumpFiles,windows.envars                                      s.getser
vicesids.GetServiceSIDs,windows.getsids.GetSIDs,windows.handles.Handles,windo                                      sses.Hol
lowProcesses,windows.iat.IAT,windows.info.Info,windows.joblinks.JobLinks,wind                                      dules,wi
ndows.lsadump.Lsadump,windows.malfind.Malfind,windows.mbrscan.MBRScan,windows                                      ws.mftsc
an.MFTScan,windows.modscan.ModScan,windows.modules.Modules,windows.mutantscan                                      ows.nets
tat.NetStat,windows.orphan_kernel_threads.Threads,windows.pe_symbols.PESymbol                                      ner.Pool
Scanner,windows.privileges.Privs,windows.processghosting.ProcessGhosting,wind                                      windows.
pstree.PsTree,windows.psxview.PsXView,windows.registry.certificates.Certifica                                      ellRouti
ne,windows.registry.hivelist.HiveList,windows.registry.hivescan.HiveScan,wind                                      egistry.
userassist.UserAssist,windows.scheduled_tasks.ScheduledTasks,windows.sessions                                      Mem,wind
ows.skeleton_key_check.Skeleton_Key_Check,windows.ssdt.SSDT,windows.statistic                                      dows.sus
picious_threads.SuspiciousThreads,windows.svcdiff.SvcDiff,windows.svclist.SvcList,windows.svcscan.SvcScan,windows.symlinkscan
.SymlinkScan,windows.thrdscan.ThrdScan,windows.threads.Threads,windows.timers.Timers,windows.truecrypt.Passphrase,windows.unh
ooked_system_calls.unhooked_system_calls,windows.unloadedmodules.UnloadedModules,windows.vadinfo.VadInfo,windows.vadwalk.VadW
alk,windows.vadyarascan.VadYaraScan,windows.verinfo.VerInfo,windows.virtmap.VirtMap,yarascan.YaraScan}
                  ...
volatility: error: unrecognized arguments: -V
eandro-dash@DESKTOP-J280MAQ:~$
```

Leandro Delgado
Student number:114416241

Figure 8. Installation of Volatility

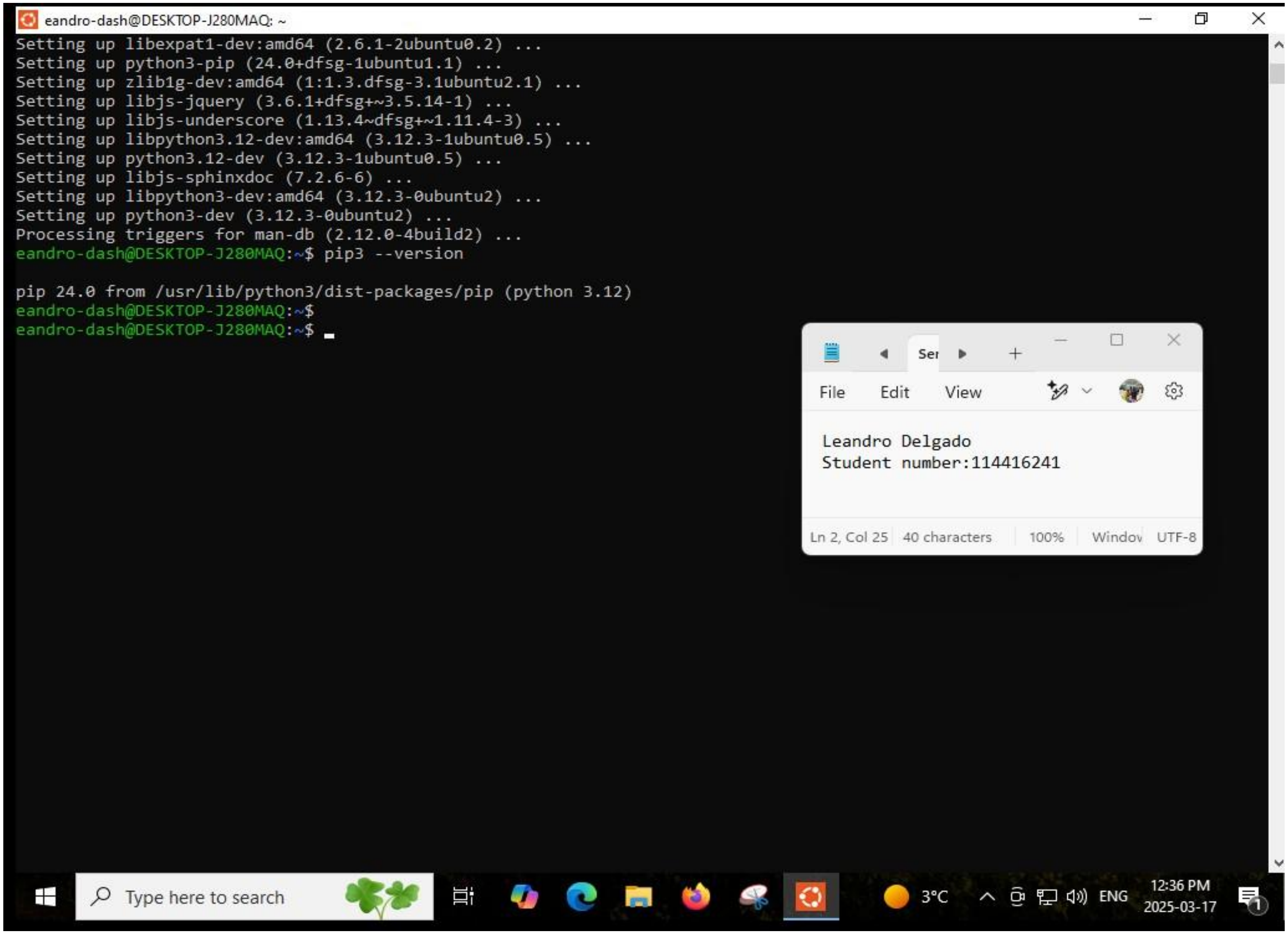
Installation Of Python3



```
Get:25 http://archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [262 kB]
Get:26 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [364 kB]
Get:27 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [25.8 kB]
Get:28 http://archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [153 kB]
Get:29 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:30 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 c-n-f Metadata [464 B]
Get:31 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Get:32 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 c-n-f Metadata [656 B]
Get:33 http://archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
Get:34 http://archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [20.0 kB]
Get:35 http://archive.ubuntu.com/ubuntu noble-backports/universe amd64 c-n-f Metadata [1256 B]
Get:36 http://archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:37 http://archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Fetched 5753 kB in 3s (1725 kB/s)
Reading package lists... Done
eandro-dash@DESKTOP-J280MAQ:~$ sudo apt install python3-pip

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  javascript-common libexpat1-dev libjs-jquery libjs-sphinxdoc libjs-underscore
  python3-dev python3-wheel python3.12-dev zlib1g-dev
Suggested packages:
  apache2 | lighttpd | httpd
The following NEW packages will be installed:
  javascript-common libexpat1-dev libjs-jquery libjs-sphinxdoc libjs-underscore libpython3-dev libpython3.12-dev
  python3-dev python3-pip python3-wheel python3.12-dev zlib1g-dev
0 upgraded, 12 newly installed, 0 to remove and 13 not upgraded.
Need to get 10.1 MB of archives.
After this operation, 42.6 MB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble/main amd64 javascript-common all 11+nmu1 [5936 B]
Get:2 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libexpat1-dev amd64 2.6.1-2ubuntu0.2 [998 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble/main amd64 libjs-jquery all 3.6.1+dfsg+~3.5.14-1 [328 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble/main amd64 libjs-underscore all 1.13.4~dfsg+~1.11.4-3 [118 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble/main amd64 libjs-sphinxdoc all 7.2.6-6 [149 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 zlib1g-dev amd64 1:1.3.dfsg-3.1ubuntu2.1 [894 kB]
Get:7 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libpython3.12-dev amd64 3.12.3-1ubuntu0.5 [5675 kB]
Get:8 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libpython3-dev amd64 3.12.3-0ubuntu2 [10.3 kB]
Get:9 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 python3.12-dev amd64 3.12.3-1ubuntu0.5 [498 kB]
Get:10 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 python3-dev amd64 3.12.3-0ubuntu2 [26.7 kB]
Get:11 http://archive.ubuntu.com/ubuntu noble/universe amd64 python3-wheel all 0.42.0-2 [53.1 kB]
Get:12 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 python3-pip all 24.0+dfsg-1ubuntu1.1 [1317 kB]
```

Leandro Delgado
Student number:114416241

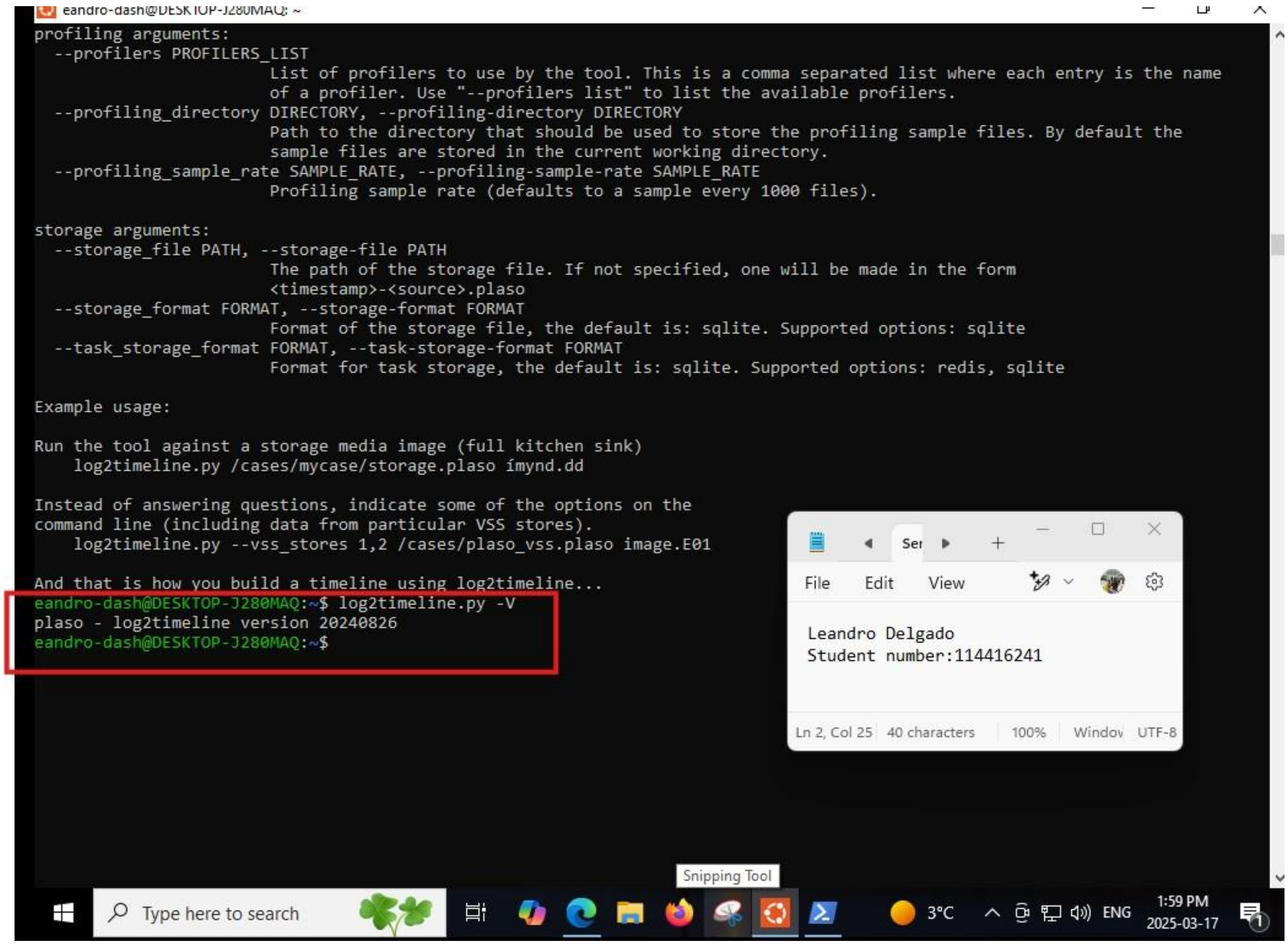
Confirmation of python Installation



```
Setting up libexpat1-dev:amd64 (2.6.1-2ubuntu0.2) ...
Setting up python3-pip (24.0+dfsg-1ubuntu1.1) ...
Setting up zlib1g-dev:amd64 (1:1.3.dfsg-3.1ubuntu2.1) ...
Setting up libjs-jquery (3.6.1+dfsg+~3.5.14-1) ...
Setting up libjs-underscore (1.13.4~dfsg+~1.11.4-3) ...
Setting up libpython3.12-dev:amd64 (3.12.3-1ubuntu0.5) ...
Setting up python3.12-dev (3.12.3-1ubuntu0.5) ...
Setting up libjs-sphinxdoc (7.2.6-6) ...
Setting up libpython3-dev:amd64 (3.12.3-0ubuntu2) ...
Setting up python3-dev (3.12.3-0ubuntu2) ...
Processing triggers for man-db (2.12.0-4build2) ...
eandro-dash@DESKTOP-J280MAQ:~$ pip3 --version

pip 24.0 from /usr/lib/python3/dist-packages/pip (python 3.12)
eandro-dash@DESKTOP-J280MAQ:~$
eandro-dash@DESKTOP-J280MAQ:~$ _
```

Leandro Delgado
Student number:114416241

Installation of log2timeline

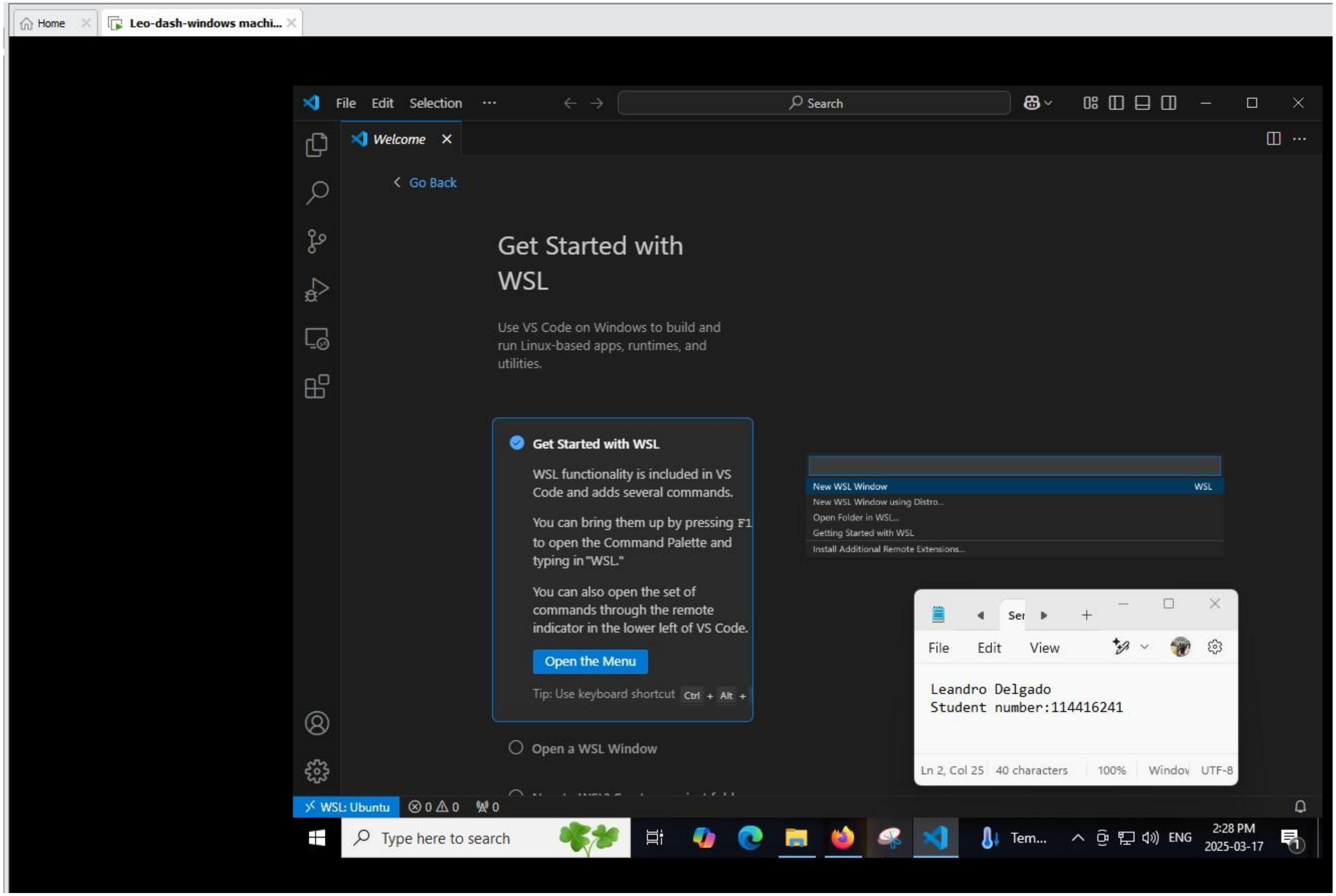


```
profiling arguments:
  --profilers PROFILERS_LIST
                        List of profilers to use by the tool. This is a comma separated list where each entry is the name
                        of a profiler. Use "--profilers list" to list the available profilers.
  --profiling_directory DIRECTORY, --profiling-directory DIRECTORY
                        Path to the directory that should be used to store the profiling sample files. By default the
                        sample files are stored in the current working directory.
  --profiling_sample_rate SAMPLE_RATE, --profiling-sample-rate SAMPLE_RATE
                        Profiling sample rate (defaults to a sample every 1000 files).

storage arguments:
  --storage_file PATH, --storage-file PATH
                        The path of the storage file. If not specified, one will be made in the form
                        <timestamp>-<source>.plaso
  --storage_format FORMAT, --storage-format FORMAT
                        Format of the storage file, the default is: sqlite. Supported options: sqlite
  --task_storage_format FORMAT, --task-storage-format FORMAT
                        Format for task storage, the default is: sqlite. Supported options: redis, sqlite

Example usage:

Run the tool against a storage media image (full kitchen sink)
    log2timeline.py /cases/mycase/storage.plaso ímynd.dd

Instead of answering questions, indicate some of the options on the
command line (including data from particular VSS stores).
    log2timeline.py --vss_stores 1,2 /cases/plaso_vss.plaso image.E01

And that is how you build a timeline using log2timeline...
eandro-dash@DESKTOP-J280MAQ:~$ log2timeline.py -V
plaso - log2timeline version 20240826
eandro-dash@DESKTOP-J280MAQ:~$
```

Leandro Delgado
Student number:114416241

Figure 9.Installation of Log2timeline on the system

Windows Tools installed



Get Started with WSL

Use VS Code on Windows to build and run Linux-based apps, runtimes, and utilities.

Get Started with WSL

WSL functionality is included in VS Code and adds several commands.

You can bring them up by pressing F1 to open the Command Palette and typing in "WSL."

You can also open the set of commands through the remote indicator in the lower left of VS Code.

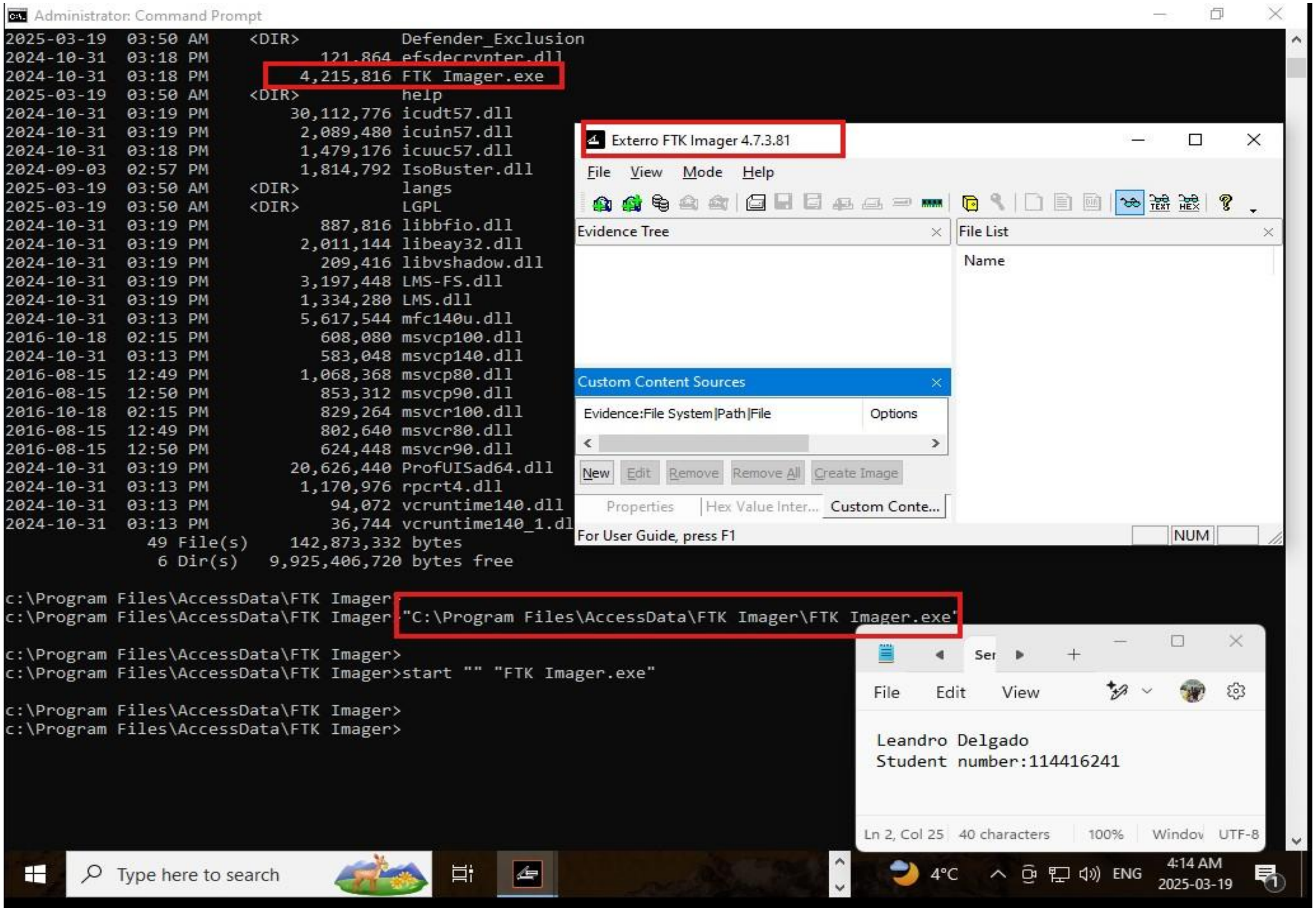
Tip: Use keyboard shortcut Ctrl + Alt +

```
Leandro Delgado
Student number:114416241
```

***F**igure 10. Installation of Visual studio Code*

Installation Of FTK image Tools

FTK Imager is a forensic imaging tool used to capture and analyze digital evidence while maintaining data integrity.

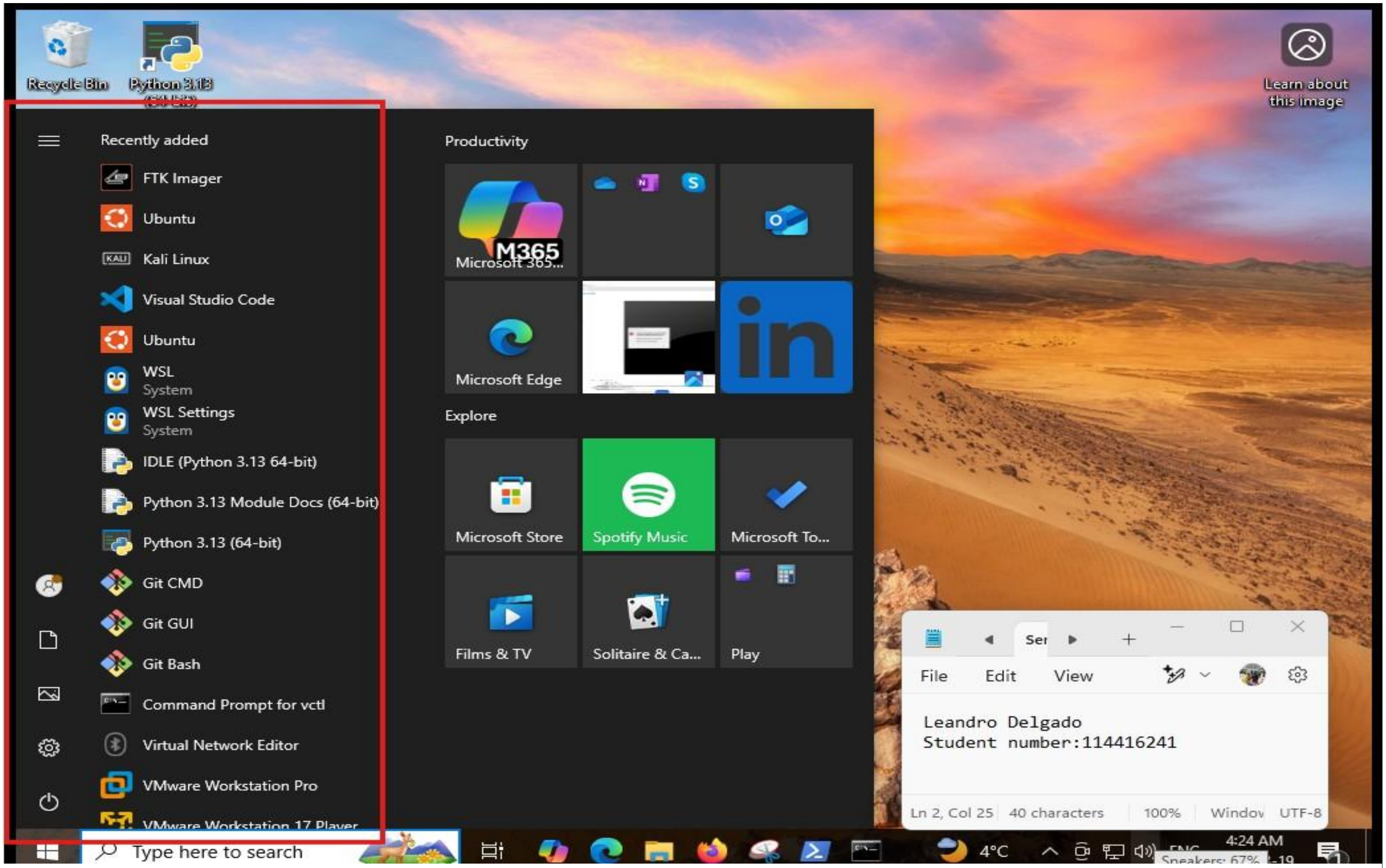


```
2025-03-19  03:50 AM    <DIR>          Defender_Exclusion
2024-10-31  03:18 PM           121,864 efsdecrypter.dll
2024-10-31  03:18 PM         4,215,816 FTK Imager.exe
2025-03-19  03:50 AM    <DIR>          help
2024-10-31  03:19 PM        30,112,776 icudt57.dll
2024-10-31  03:19 PM         2,089,480 icuin57.dll
2024-10-31  03:18 PM         1,479,176 icuuc57.dll
2024-09-03  02:57 PM         1,814,792 IsoBuster.dll
2025-03-19  03:50 AM    <DIR>          langs
2025-03-19  03:50 AM    <DIR>          LGPL
2024-10-31  03:19 PM           887,816 libbfio.dll
2024-10-31  03:19 PM         2,011,144 libeay32.dll
2024-10-31  03:19 PM           209,416 libvshadow.dll
2024-10-31  03:19 PM         3,197,448 LMS-FS.dll
2024-10-31  03:19 PM         1,334,280 LMS.dll
2024-10-31  03:13 PM         5,617,544 mfc140u.dll
2016-10-18  02:15 PM           608,080 msvcp100.dll
2024-10-31  03:13 PM           583,048 msvcp140.dll
2016-08-15  12:49 PM         1,068,368 msvcp80.dll
2016-08-15  12:50 PM           853,312 msvcp90.dll
2016-10-18  02:15 PM           829,264 msvcr100.dll
2016-08-15  12:49 PM           802,640 msvcr80.dll
2016-08-15  12:50 PM           624,448 msvcr90.dll
2024-10-31  03:19 PM        20,626,440 ProfUISad64.dll
2024-10-31  03:13 PM         1,170,976 rpcrt4.dll
2024-10-31  03:13 PM            94,072 vcruntime140.dll
2024-10-31  03:13 PM            36,744 vcruntime140_1.dl
              49 File(s)    142,873,332 bytes
               6 Dir(s)   9,925,406,720 bytes free

c:\Program Files\AccessData\FTK Imager
c:\Program Files\AccessData\FTK Imager "C:\Program Files\AccessData\FTK Imager\FTK Imager.exe"

c:\Program Files\AccessData\FTK Imager>
c:\Program Files\AccessData\FTK Imager>start "" "FTK Imager.exe"

c:\Program Files\AccessData\FTK Imager>
c:\Program Files\AccessData\FTK Imager>
```

```
Leandro Delgado
Student number:114416241
```

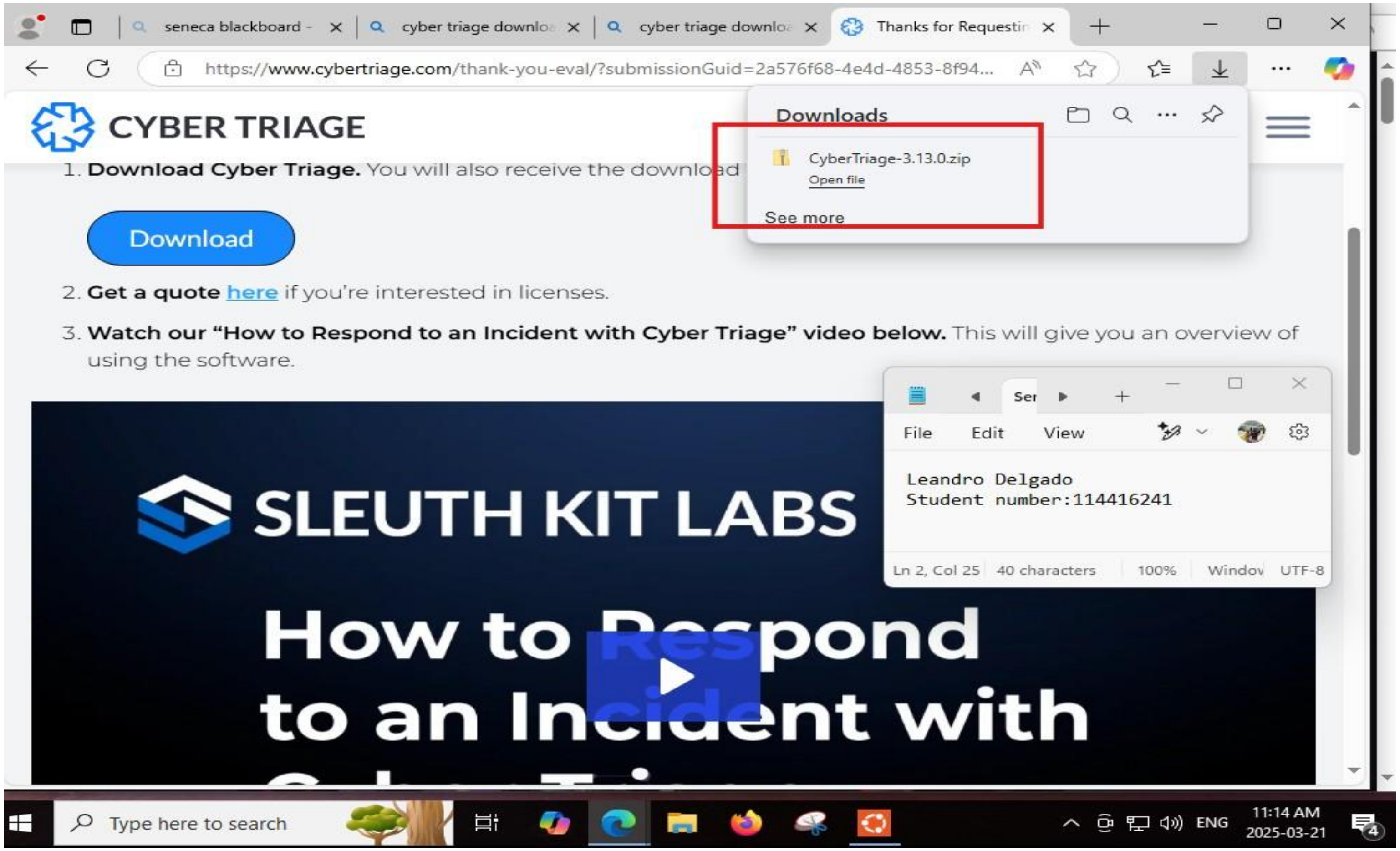
Figure 11. Installation of FTK image

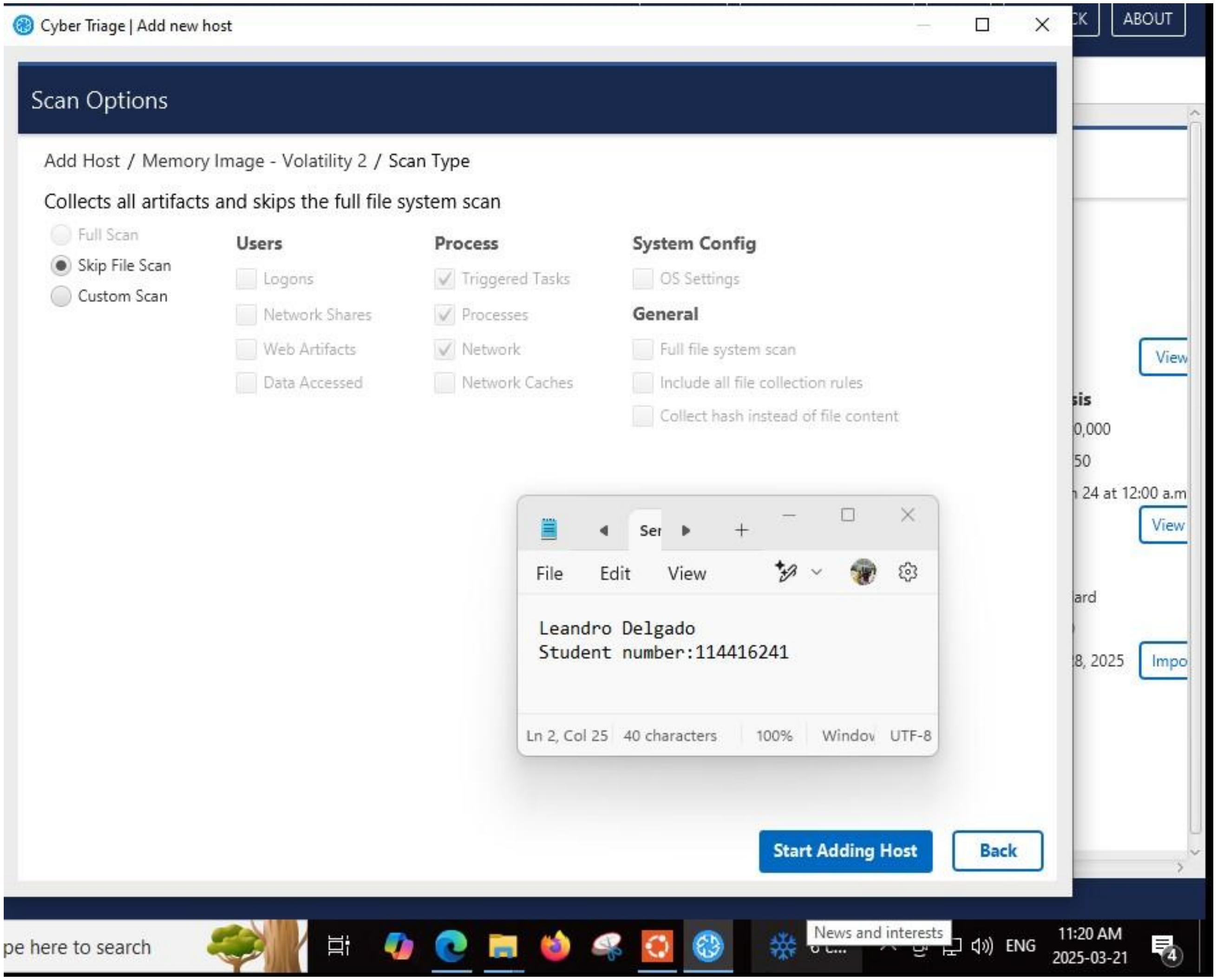
Tools Installed on my workstation



```
Leandro Delgado
Student number:114416241
```

Figure 12.Corfirmation of tools installed

	Cyber Triage This commercial tool facilitates live response and triage investigations, offering a user-friendly interface for endpoint data collection and malware detection. It is primarily designed for Windows environments.  1. **Download Cyber Triage.** You will also receive the download 2. **Get a quote** here if you're interested in licenses. 3. **Watch our "How to Respond to an Incident with Cyber Triage" video below.** This will give you an overview of using the software. Downloads CyberTriage-3.13.0.zip Open file See more Leandro Delgado Student number:114416241 seneca blackboard - cyber triage downlo cyber triage downlo Thanks for Requestin https://www.cybertriage.com/thank-you-eval/?submissionGuid=2a576f68-4e4d-4853-8f94... CYBER TRIAGE Download SLEUTH KIT LABS How to Respond to an Incident with Ser File Edit View Ln 2, Col 25 40 characters 100% Windov UTF-8 Type here to search ENG 11:14 AM 2025-03-21 **Figure 13. Intallation of Cyber Triage**



Cyber Triage | Add new host

Scan Options

Add Host / Memory Image - Volatility 2 / Scan Type

Collects all artifacts and skips the full file system scan

○ Full Scan
● Skip File Scan
○ Custom Scan

Users

□ Logons
□ Network Shares
□ Web Artifacts
□ Data Accessed

Process

☑ Triggered Tasks
☑ Processes
☑ Network
□ Network Caches

System Config

□ OS Settings

General

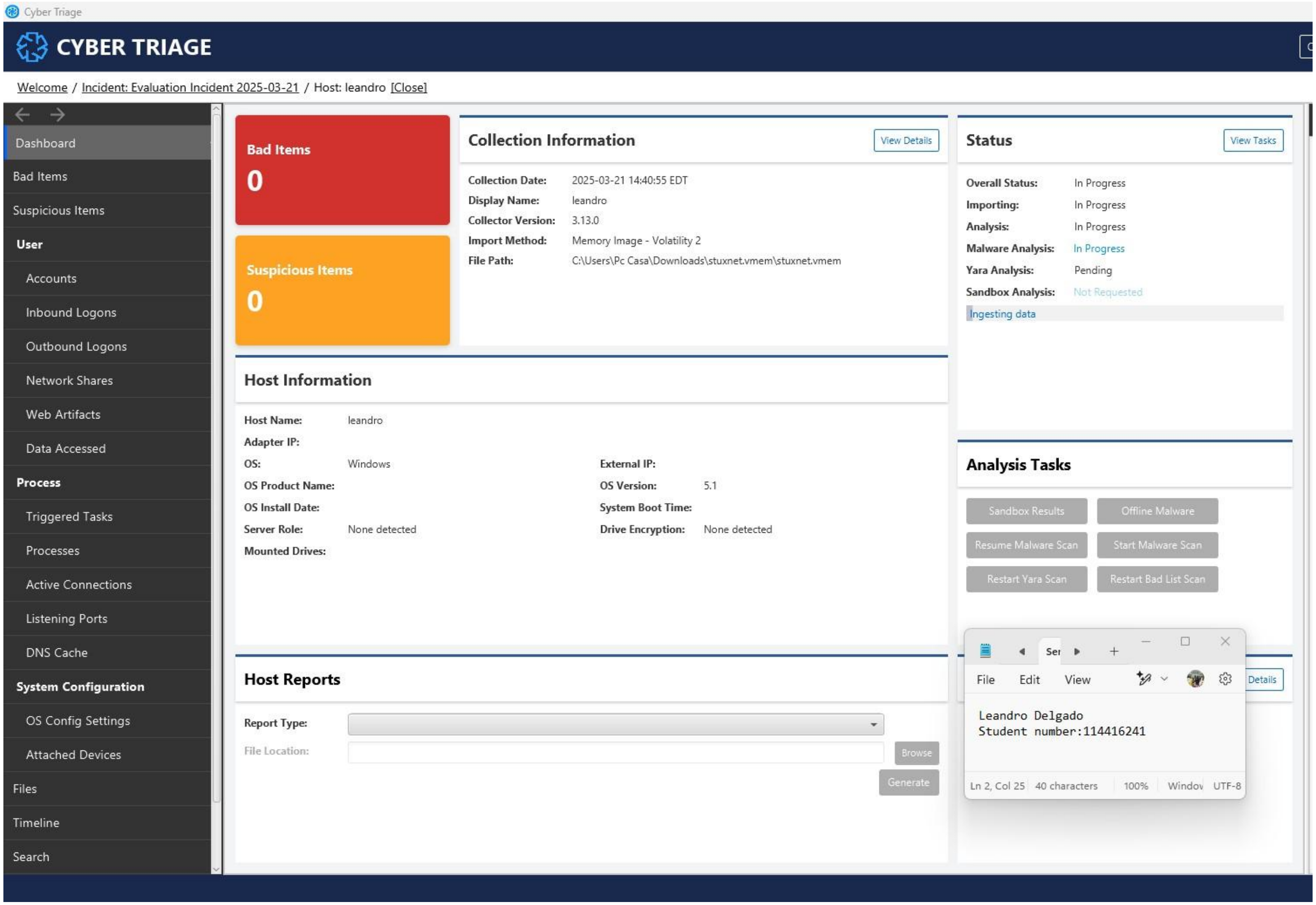
□ Full file system scan
□ Include all file collection rules
□ Collect hash instead of file content

```
Leandro Delgado
Student number:114416241
```

Ln 2, Col 25 | 40 characters | 100% | Windov | UTF-8

Figure 14.Cyber Triage Interfaces

Image memory-Cyber Triage Dashboard



Welcome / Incident: Evaluation Incident 2025-03-21 / Host: leandro [Close]

Bad Items 0

Suspicious Items 0

Collection Information

Collection Date: 2025-03-21 14:40:55 EDT
Display Name: leandro
Collector Version: 3.13.0
Import Method: Memory Image - Volatility 2
File Path: C:\Users\Pc Casa\Downloads\stuxnet.vmem\stuxnet.vmem

Status

Overall Status: In Progress
Importing: In Progress
Analysis: In Progress
Malware Analysis: In Progress
Yara Analysis: Pending
Sandbox Analysis: Not Requested
Ingesting data

Host Information

Host Name: leandro
Adapter IP:
OS: Windows
External IP:
OS Product Name:
OS Version: 5.1
OS Install Date:
System Boot Time:
Server Role: None detected
Drive Encryption: None detected
Mounted Drives:

Analysis Tasks

Host Reports

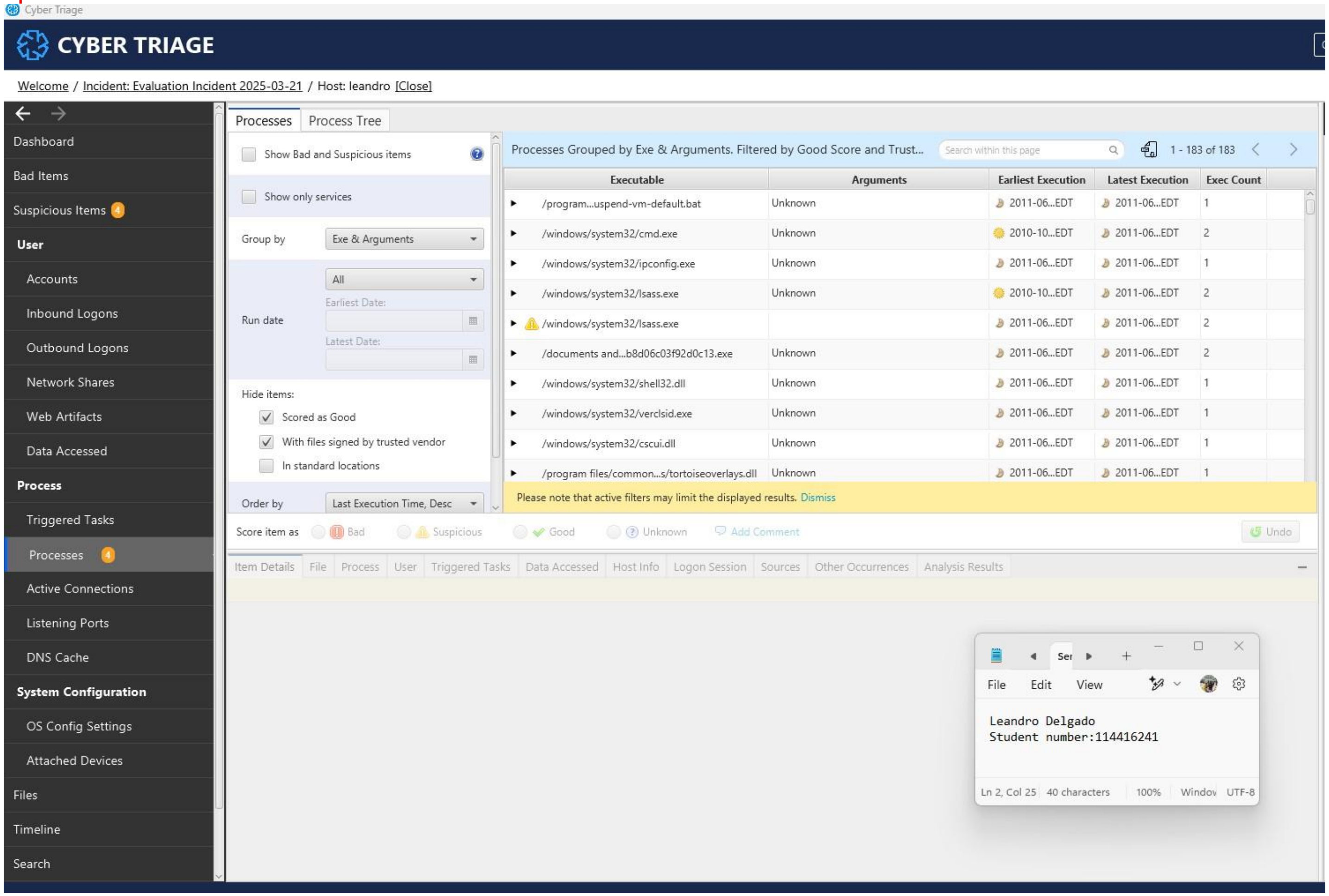
Report Type:
File Location:

```
Leandro Delgado
Student number:114416241
```

Ln 2, Col 25 40 characters 100% Windov UTF-8

Figure 15.Cyber Triage Outcome from image memory lecture

In this part, Cyber Triage Provide the process in the memory image lecture. In this section I can apply filter and tags to get specific information



☐ Show Bad and Suspicious items

☐ Show only services

Group by: Exe & Arguments

Run date: All

Earliest Date:

Latest Date:

Hide items:

☑ Scored as Good

☑ With files signed by trusted vendor

☐ In standard locations

Order by: Last Execution Time, Desc

Processes Grouped by Exe & Arguments. Filtered by Good Score and Trust...

1 - 183 of 183

Executable	Arguments	Earliest Execution	Latest Execution	Exec Count
/program...uspend-vm-default.bat	Unknown	2011-06...EDT	2011-06...EDT	1
/windows/system32/cmd.exe	Unknown	2010-10...EDT	2011-06...EDT	2
/windows/system32/ipconfig.exe	Unknown	2011-06...EDT	2011-06...EDT	1
/windows/system32/lsass.exe	Unknown	2010-10...EDT	2011-06...EDT	2
⚠ /windows/system32/lsass.exe		2011-06...EDT	2011-06...EDT	2
/documents and...b8d06c03f92d0c13.exe	Unknown	2011-06...EDT	2011-06...EDT	2
/windows/system32/shell32.dll	Unknown	2011-06...EDT	2011-06...EDT	1
/windows/system32/verclsid.exe	Unknown	2011-06...EDT	2011-06...EDT	1
/windows/system32/cscui.dll	Unknown	2011-06...EDT	2011-06...EDT	1
/program files/common...s/tortoiseoverlays.dll	Unknown	2011-06...EDT	2011-06...EDT	1

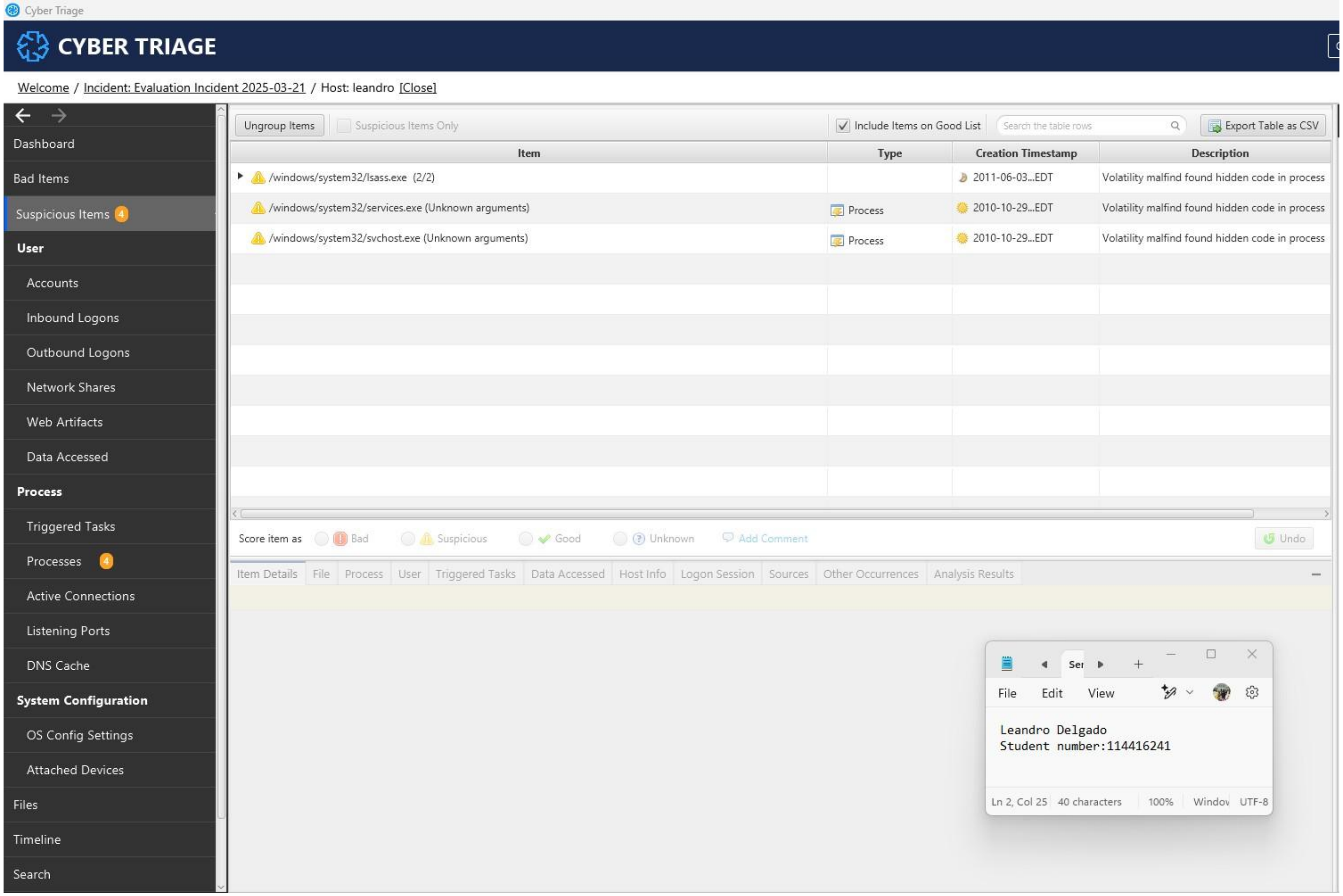
Please note that active filters may limit the displayed results. Dismiss

Leandro Delgado
Student number:114416241

Ln 2, Col 25 | 40 characters | 100% | Windov | UTF-8

Figure 16.Result from Memory image

In this section, Cyber triage demonstrates the suspicious items that can affect the memory image. Analyzing this information, we can have a roughly idea about the current situation on the system



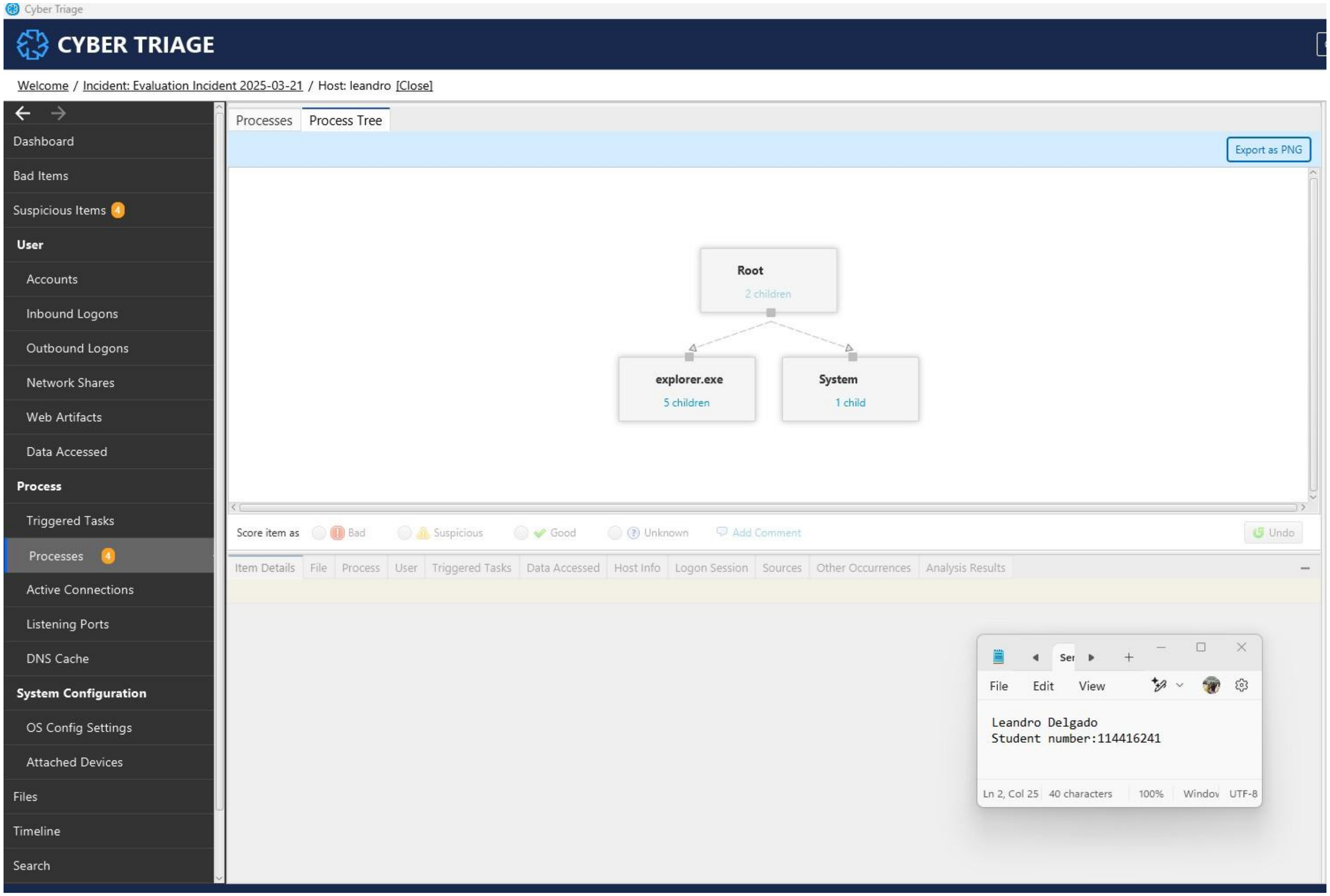
Welcome / Incident: Evaluation Incident 2025-03-21 / Host: leandro [Close]

Item	Type	Creation Timestamp	Description
/windows/system32/lsass.exe (2/2)		2011-06-03...EDT	Volatility malfind found hidden code in process
/windows/system32/services.exe (Unknown arguments)	Process	2010-10-29...EDT	Volatility malfind found hidden code in process
/windows/system32/svchost.exe (Unknown arguments)	Process	2010-10-29...EDT	Volatility malfind found hidden code in process

```
Leandro Delgado
Student number:114416241
```

Figure 17.Suspicious Items

The tree process showed inside the memory image systems helps to understand the performance of the system and get more information

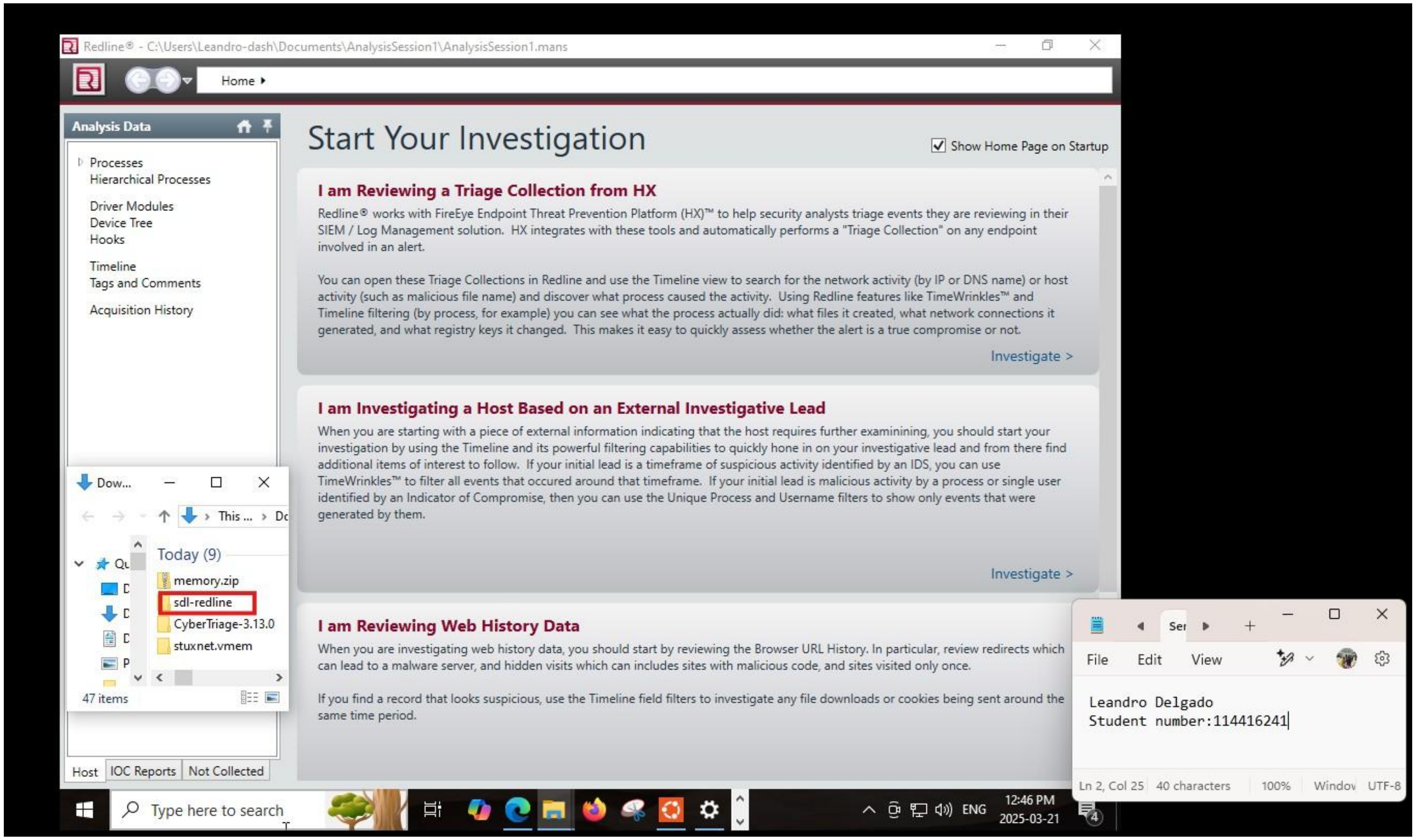


Leandro Delgado
Student number:114416241

Figure 18.Cyber Triage Process Tree

Red Line

This tool is good for memory and malware analysis. Its performance offers a good visual representation of all memory aspects keeping active the process and systems configurations.


Redline® - C:\Users\Leandro-dash\Documents\AnalysisSession1\AnalysisSession1.mans

Start Your Investigation

I am Reviewing a Triage Collection from HX

Redline® works with FireEye Endpoint Threat Prevention Platform (HX)™ to help security analysts triage events they are reviewing in their SIEM / Log Management solution. HX integrates with these tools and automatically performs a "Triage Collection" on any endpoint involved in an alert.

You can open these Triage Collections in Redline and use the Timeline view to search for the network activity (by IP or DNS name) or host activity (such as malicious file name) and discover what process caused the activity. Using Redline features like TimeWrinkles™ and Timeline filtering (by process, for example) you can see what the process actually did: what files it created, what network connections it generated, and what registry keys it changed. This makes it easy to quickly assess whether the alert is a true compromise or not.

Investigate >

I am Investigating a Host Based on an External Investigative Lead

When you are starting with a piece of external information indicating that the host requires further examinining, you should start your investigation by using the Timeline and its powerful filtering capabilities to quickly hone in on your investigative lead and from there find additional items of interest to follow. If your initial lead is a timeframe of suspicious activity identified by an IDS, you can use TimeWrinkles™ to filter all events that occured around that timeframe. If your initial lead is malicious activity by a process or single user identified by an Indicator of Compromise, then you can use the Unique Process and Username filters to show only events that were generated by them.

Investigate >

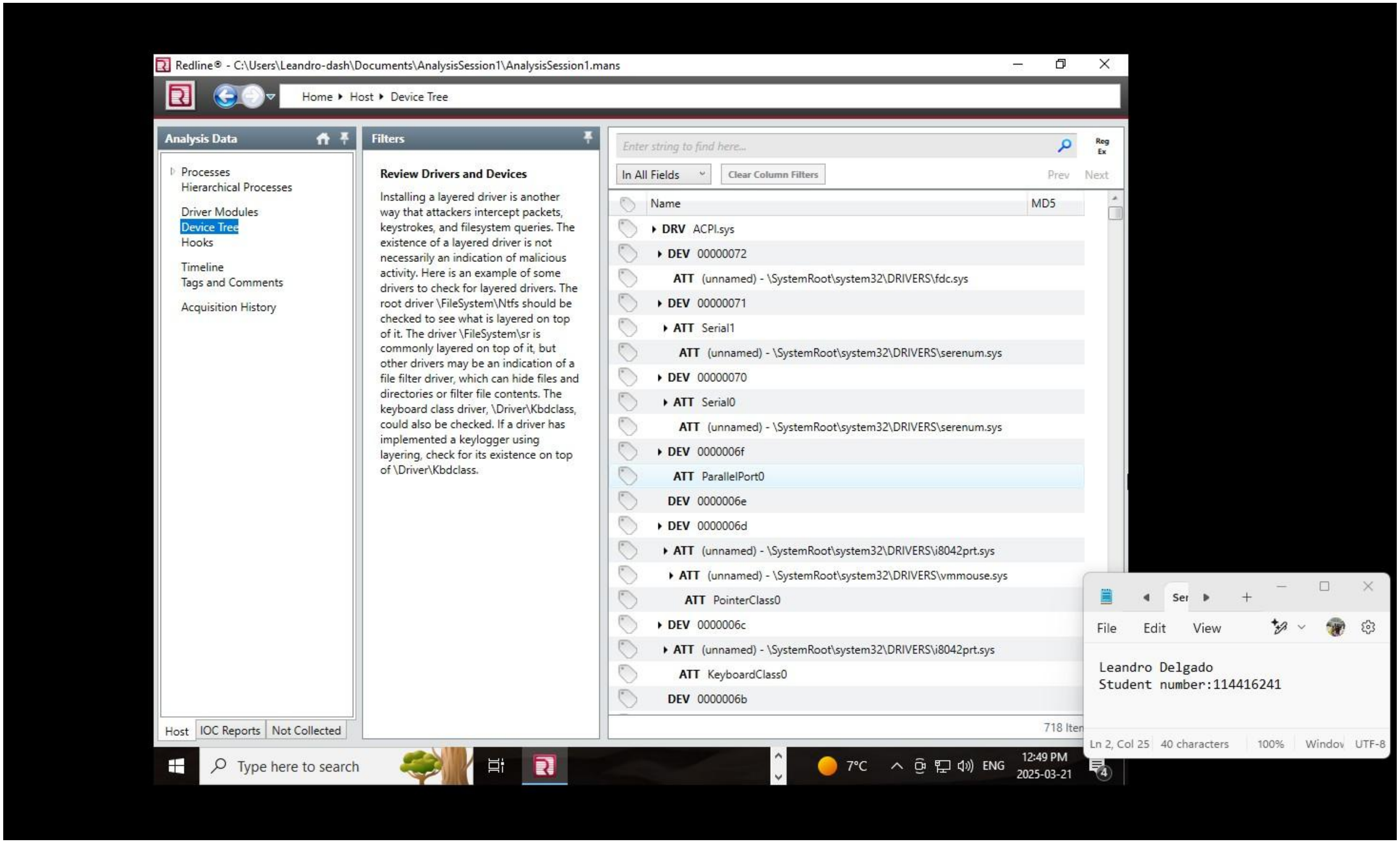
I am Reviewing Web History Data

When you are investigating web history data, you should start by reviewing the Browser URL History. In particular, review redirects which can lead to a malware server, and hidden visits which can includes sites with malicious code, and sites visited only once.

If you find a record that looks suspicious, use the Timeline field filters to investigate any file downloads or cookies being sent around the same time period.

Leandro Delgado
Student number:114416241

Figure 19. Redline Installation



Redline® - C:\Users\Leandro-dash\Documents\AnalysisSession1\AnalysisSession1.mans

Home ▸ Host ▸ Device Tree

Review Drivers and Devices

Installing a layered driver is another way that attackers intercept packets, keystrokes, and filesystem queries. The existence of a layered driver is not necessarily an indication of malicious activity. Here is an example of some drivers to check for layered drivers. The root driver \FileSystem\Ntfs should be checked to see what is layered on top of it. The driver \FileSystem\sr is commonly layered on top of it, but other drivers may be an indication of a file filter driver, which can hide files and directories or filter file contents. The keyboard class driver, \Driver\Kbdclass, could also be checked. If a driver has implemented a keylogger using layering, check for its existence on top of \Driver\Kbdclass.

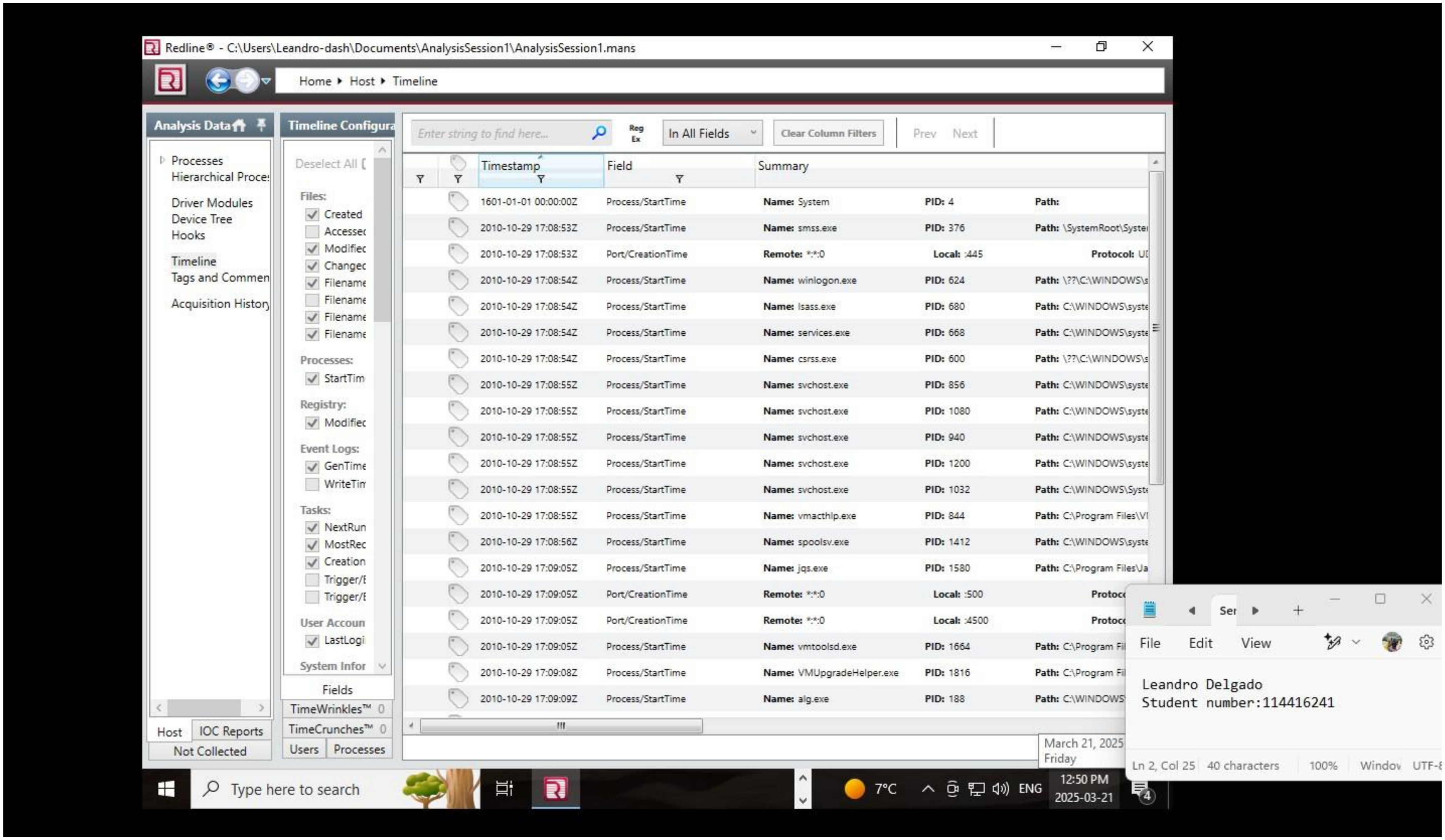
```
▸ DRV  ACPI.sys
 ▸ DEV  00000072
   ATT  (unnamed) - \SystemRoot\system32\DRIVERS\fdc.sys
 ▸ DEV  00000071
  ▸ ATT  Serial1
    ATT  (unnamed) - \SystemRoot\system32\DRIVERS\serenum.sys
 ▸ DEV  00000070
  ▸ ATT  Serial0
    ATT  (unnamed) - \SystemRoot\system32\DRIVERS\serenum.sys
 ▸ DEV  0000006f
   ATT  ParallelPort0
   DEV  0000006e
 ▸ DEV  0000006d
  ▸ ATT  (unnamed) - \SystemRoot\system32\DRIVERS\i8042prt.sys
   ▸ ATT  (unnamed) - \SystemRoot\system32\DRIVERS\vmmouse.sys
     ATT  PointerClass0
 ▸ DEV  0000006c
  ▸ ATT  (unnamed) - \SystemRoot\system32\DRIVERS\i8042prt.sys
    ATT  KeyboardClass0
   DEV  0000006b
```

```
Leandro Delgado
Student number:114416241
```

Ln 2, Col 25 | 40 characters | 100% | Windov | UTF-8

Figure 20.Devices Tree

In this section, redline shows the list of all items with its descriptions. Provide in detail a very clear information



Timestamp	Field	Summary		
1601-01-01 00:00:00Z	Process/StartTime	**Name:** System	**PID:** 4	**Path:**
2010-10-29 17:08:53Z	Process/StartTime	**Name:** smss.exe	**PID:** 376	**Path:** \SystemRoot\Syster
2010-10-29 17:08:53Z	Port/CreationTime	**Remote:** *:*:0	**Local:** :445	**Protocol:** UI
2010-10-29 17:08:54Z	Process/StartTime	**Name:** winlogon.exe	**PID:** 624	**Path:** \??\C:\WINDOWS\s
2010-10-29 17:08:54Z	Process/StartTime	**Name:** lsass.exe	**PID:** 680	**Path:** C:\WINDOWS\syste
2010-10-29 17:08:54Z	Process/StartTime	**Name:** services.exe	**PID:** 668	**Path:** C:\WINDOWS\syste
2010-10-29 17:08:54Z	Process/StartTime	**Name:** csrss.exe	**PID:** 600	**Path:** \??\C:\WINDOWS\s
2010-10-29 17:08:55Z	Process/StartTime	**Name:** svchost.exe	**PID:** 856	**Path:** C:\WINDOWS\syste
2010-10-29 17:08:55Z	Process/StartTime	**Name:** svchost.exe	**PID:** 1080	**Path:** C:\WINDOWS\syste
2010-10-29 17:08:55Z	Process/StartTime	**Name:** svchost.exe	**PID:** 940	**Path:** C:\WINDOWS\syste
2010-10-29 17:08:55Z	Process/StartTime	**Name:** svchost.exe	**PID:** 1200	**Path:** C:\WINDOWS\syste
2010-10-29 17:08:55Z	Process/StartTime	**Name:** svchost.exe	**PID:** 1032	**Path:** C:\WINDOWS\Syste
2010-10-29 17:08:55Z	Process/StartTime	**Name:** vmacthlp.exe	**PID:** 844	**Path:** C:\Program Files\VI
2010-10-29 17:08:56Z	Process/StartTime	**Name:** spoolsv.exe	**PID:** 1412	**Path:** C:\WINDOWS\syste
2010-10-29 17:09:05Z	Process/StartTime	**Name:** jqs.exe	**PID:** 1580	**Path:** C:\Program Files\Ja
2010-10-29 17:09:05Z	Port/CreationTime	**Remote:** *:*:0	**Local:** :500	**Protoco**
2010-10-29 17:09:05Z	Port/CreationTime	**Remote:** *:*:0	**Local:** :4500	**Protoco**
2010-10-29 17:09:05Z	Process/StartTime	**Name:** vmtoolsd.exe	**PID:** 1664	**Path:** C:\Program Fi
2010-10-29 17:09:08Z	Process/StartTime	**Name:** VMUpgradeHelper.exe	**PID:** 1816	**Path:** C:\Program Fi
2010-10-29 17:09:09Z	Process/StartTime	**Name:** alg.exe	**PID:** 188	**Path:** C:\WINDOWS

```
Leandro Delgado
Student number:114416241
```

Figure 21. Red line all Items

	This project used a very interesting combination of open-source and commercial tools to analyze computer memory and find malware. 1. Redline (Windows-based) specializes in detailed audits and visual memory analysis but relies on a manual workflow. 2. Volatility (Linux)- this open-source memory analysis tool is quite powerful and has so many plugins, but it really requires manual installation. 3. Cyber Triage is simple and gives a fully automated outcome instead of very user-friendly two clicks to start the triage analysis on Windows. Yes, for at least commercial cost, it is required, and natively under Linux, it is absent. Conclusion: All in all, this project has empowered the user by allowing him to obtain actual experience in the fields of forensic investigation and evidence interpretation while comparing tools across platforms, ramping overall skills in digital forensics. 1. Take screenshots of all your works steps 2. Show you have practiced 3 relevant tools to investigate memory. 3. Write a detailed report of personal learning experience (free writing).
Grading Rubrics	• 5 Marks for completing the setup of your forensics workstation successfully. • 5 Marks for using your workstation for memory analysis. Ate least, use 3 tool/memory analysis. • 2 Marks for your detailed personal learning experience (free writing)
Grading Alerts	• If you do NOT use this template or delete anyart of it or use any other template, you will be degraded. • If you do NOT follow the fie naming convention, you will be degraded. • If you do submit your file in in PDF; you will be degraded. • If you do NOT show your account real name (when applicable); you will be degraded. • If you do NOT show your machine desktop background (with date & time) and IP, you will be degraded. • If you do NOT write (in your own words) your learning experience for the activity practices, you will be degraded.