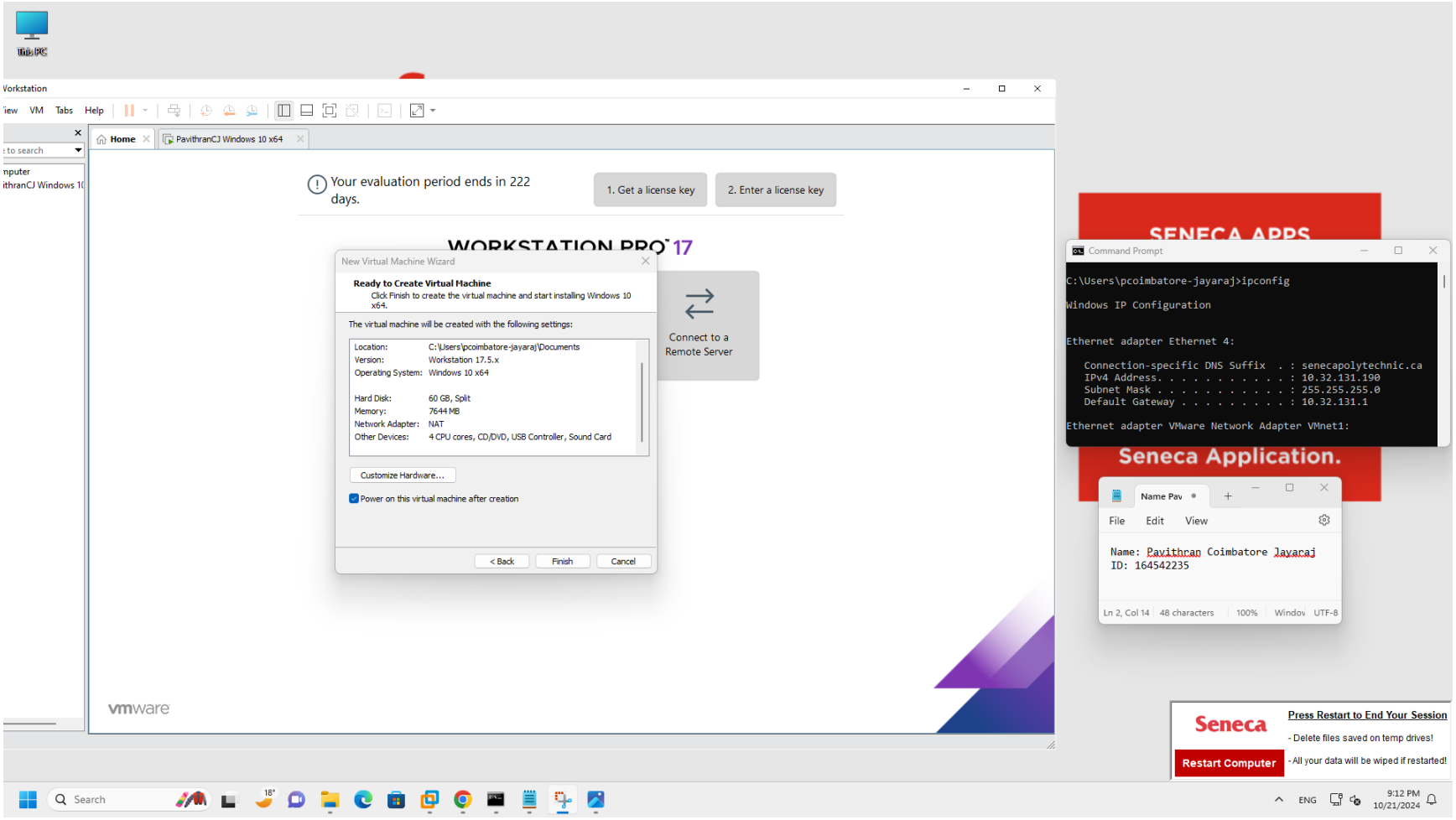
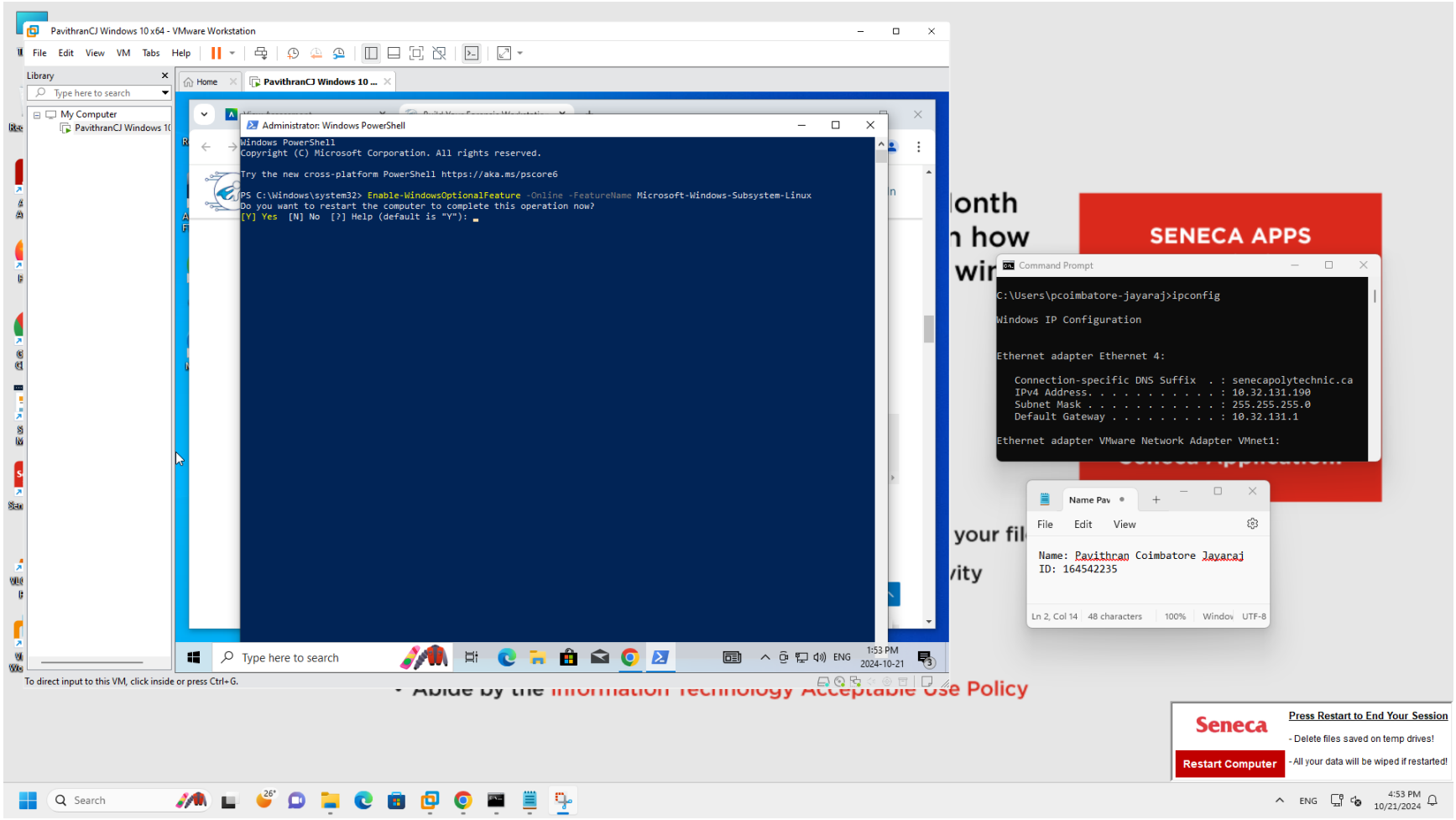
Part1:Setting up my Forensic Workstation

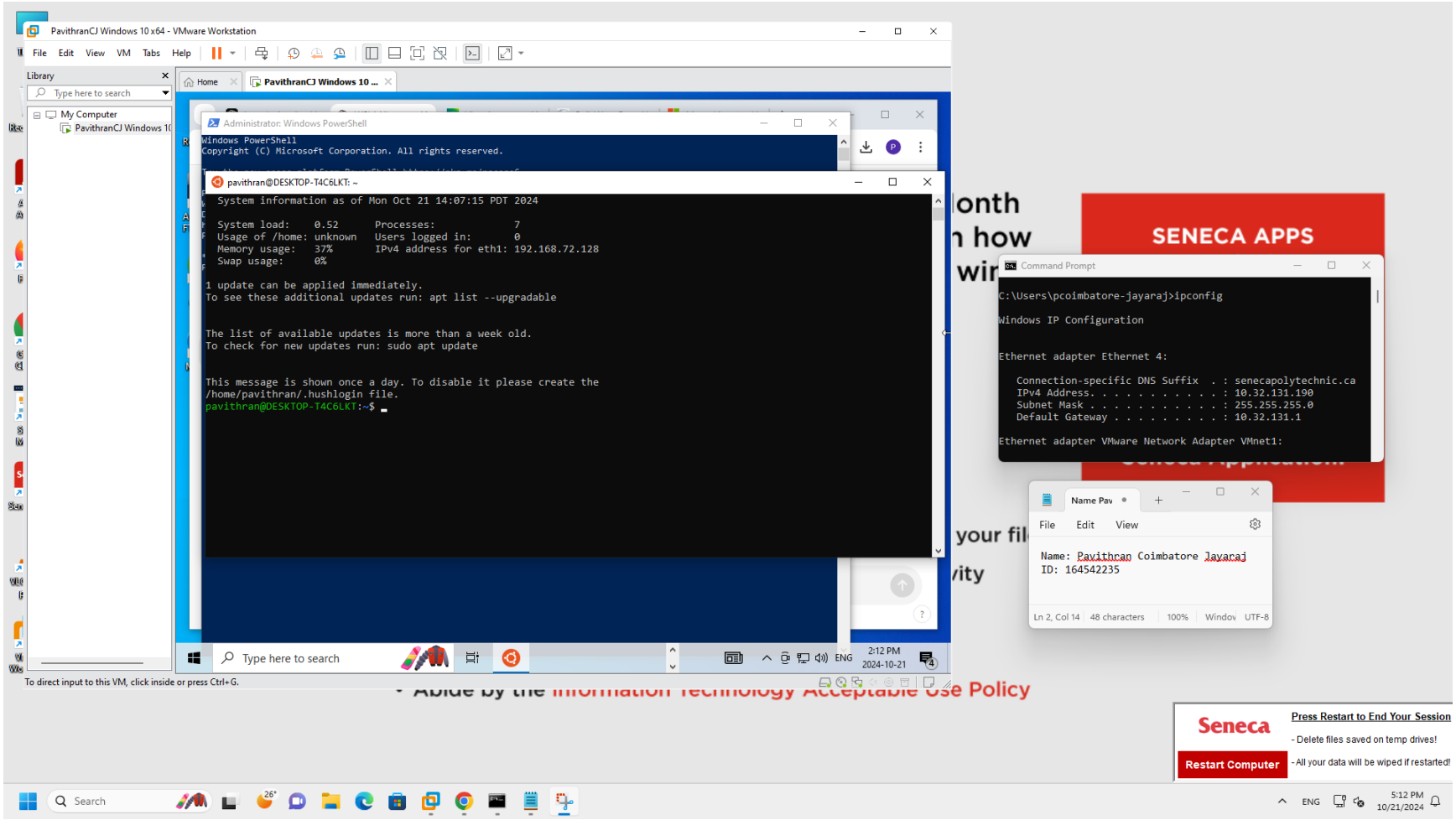
1. Install Windows 10 using VMware Workstation.



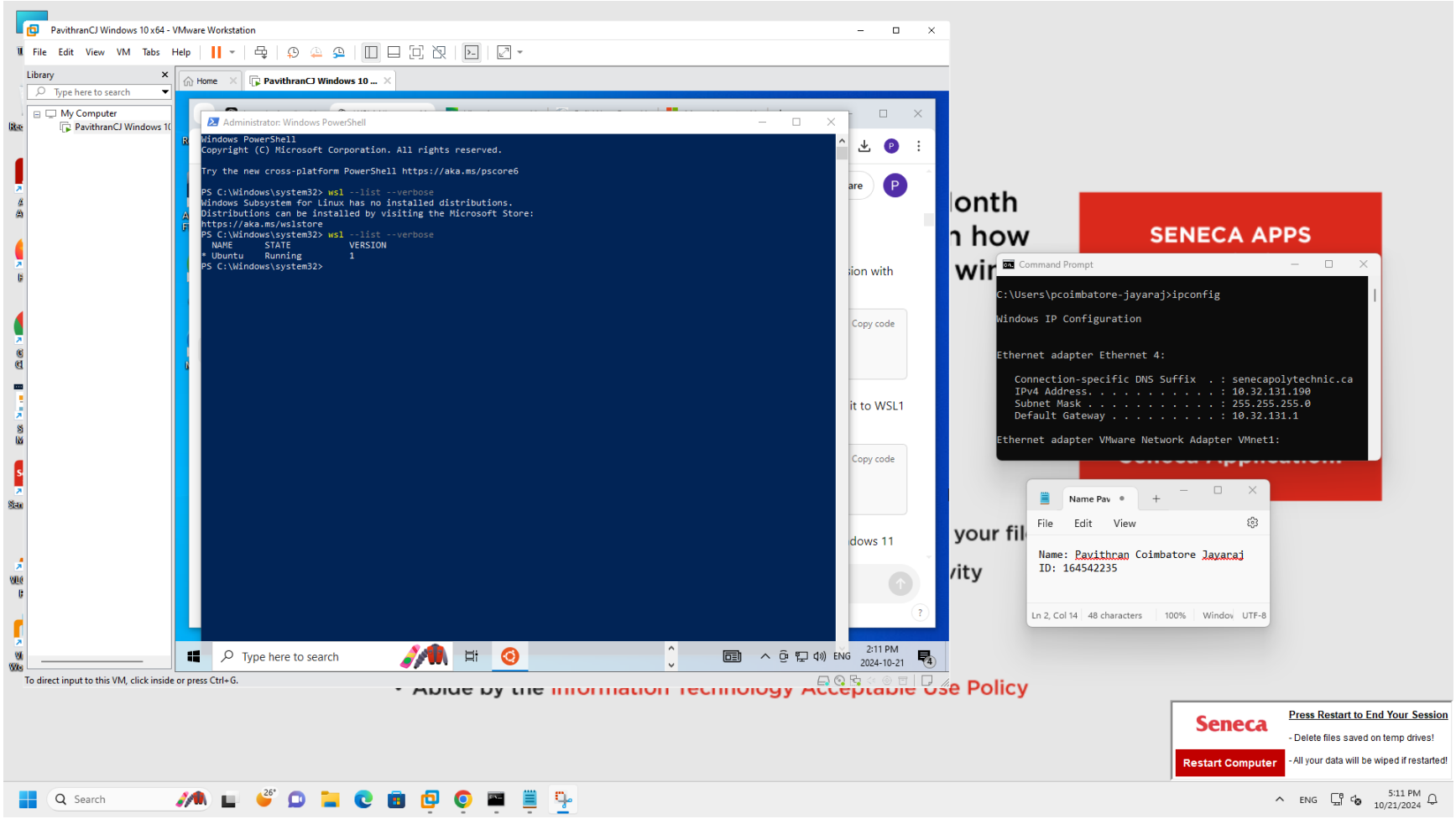
2. Enabling Windows Subsystem for Linux.



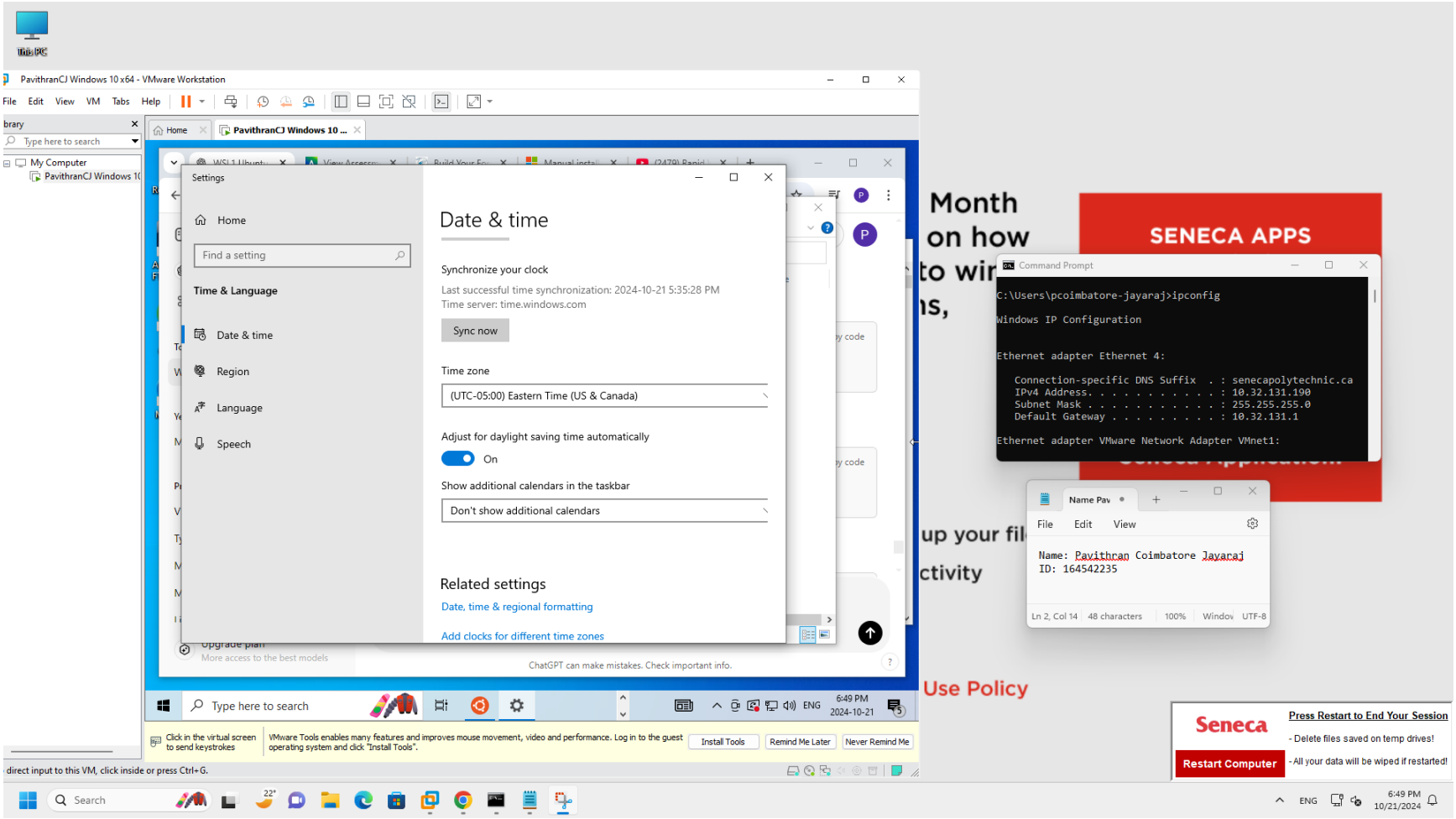
3. Setup username and Password after Installing Ubuntu 20.04.



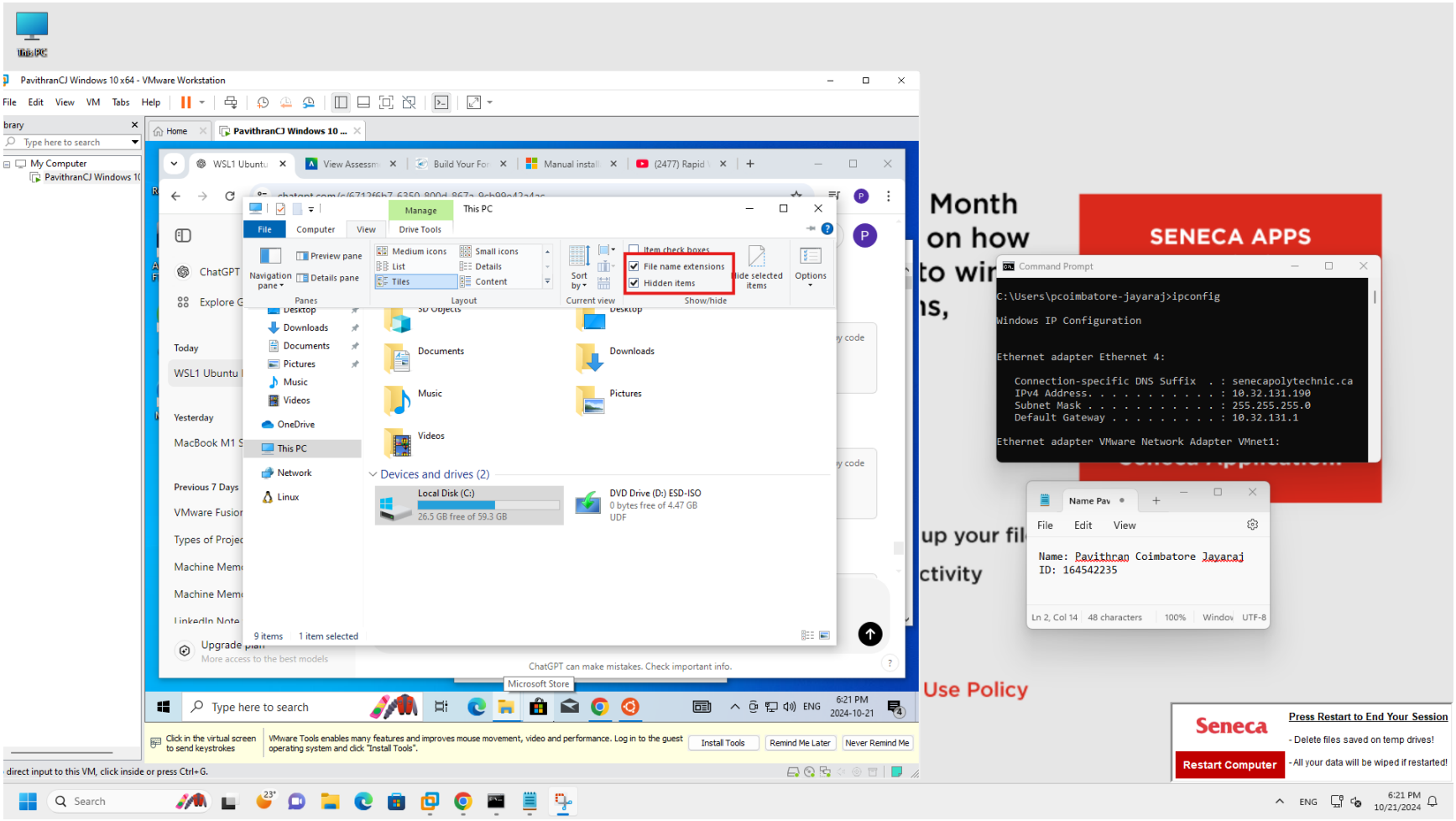
4. Proof that WSL1 is the version we are using, and Ubuntu is running.



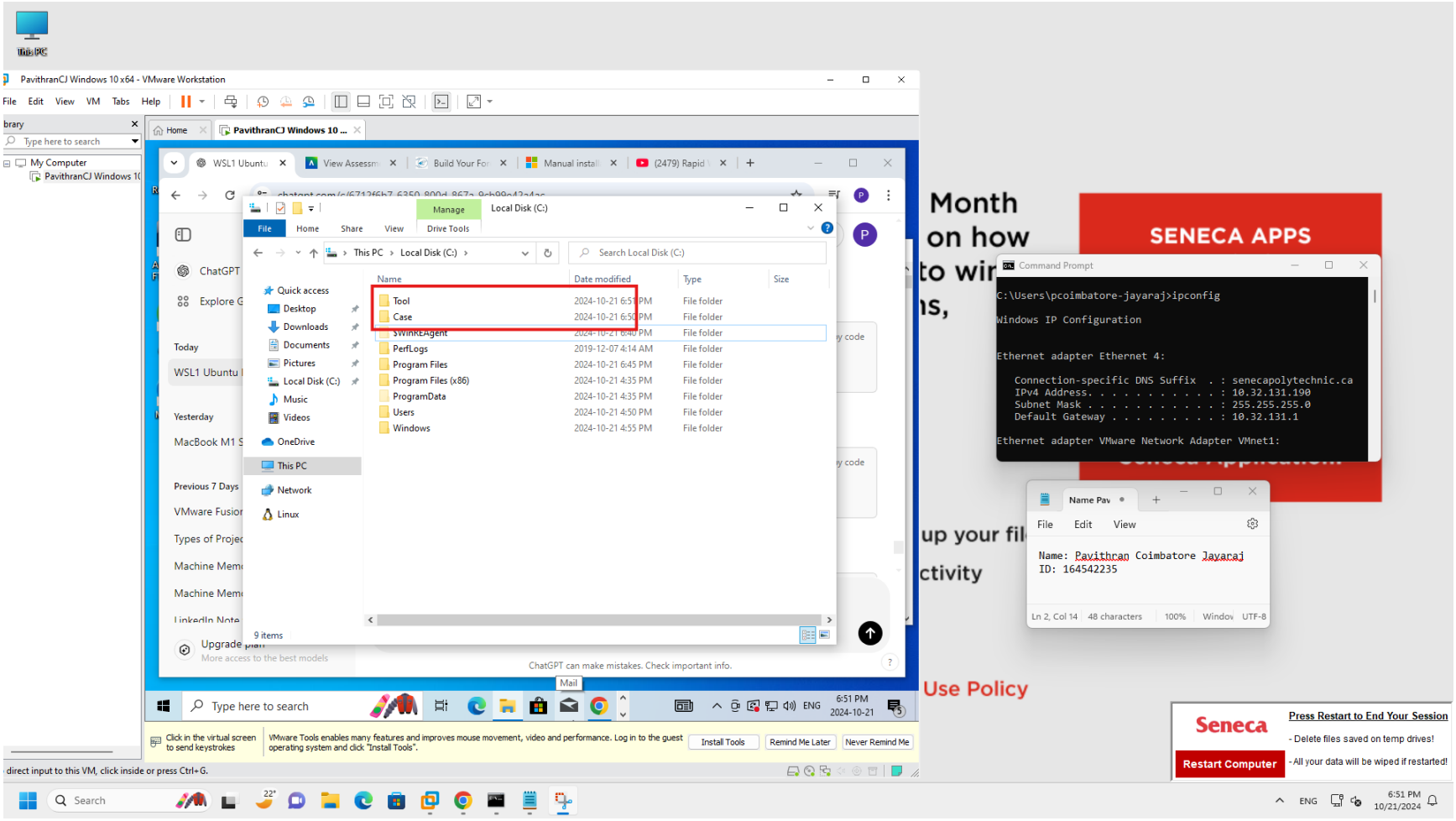
5. Configuring the windows environment by setting time zone to UTC.



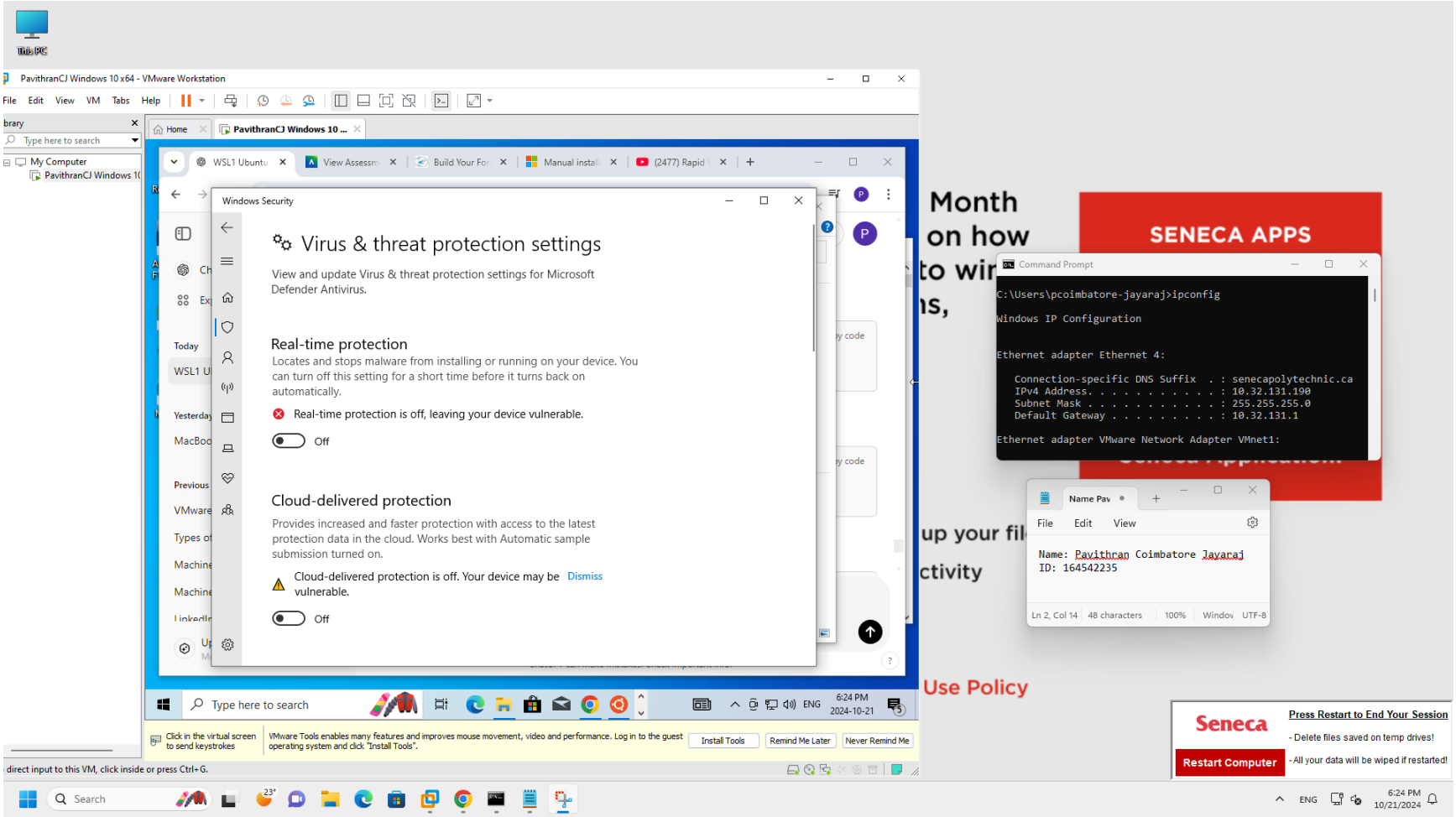
6. Check file name extension and hidden files for better visibility for crucial files.



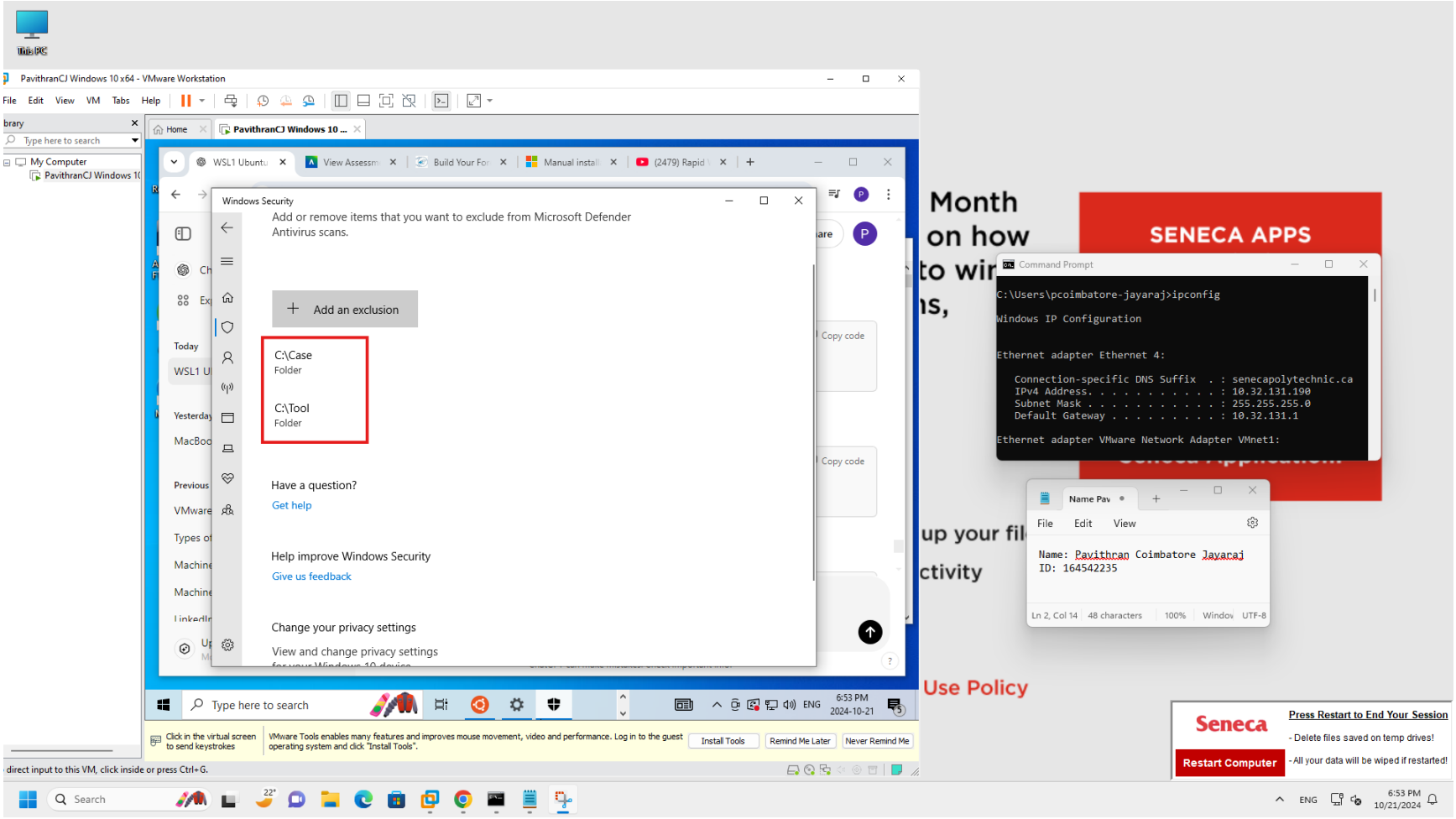
7. Create separate folders for case and tools for forensic evidence and tool storage.



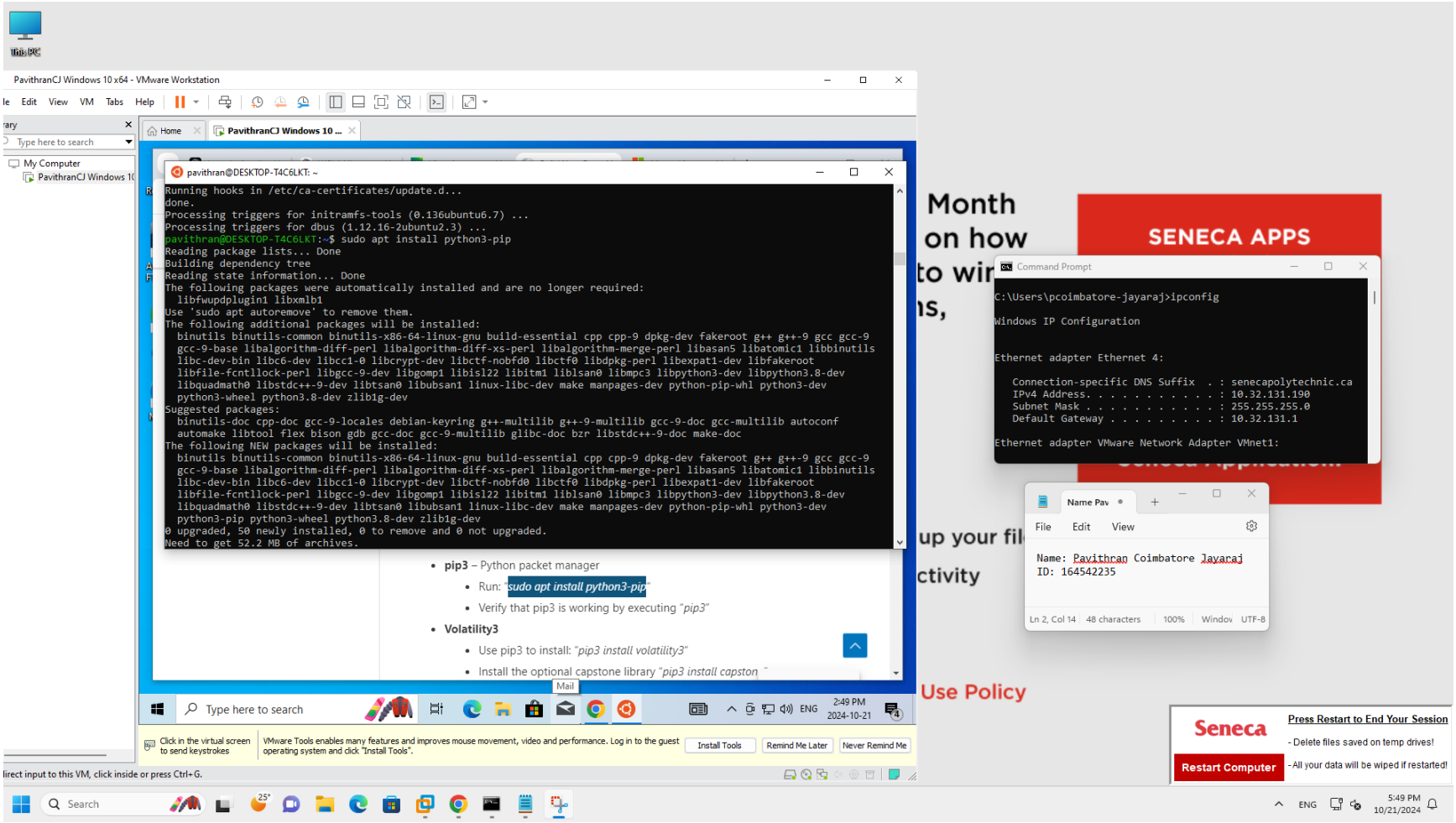
8. Configure Microsoft Defender to avoid interference with evidence or tools by Disableling Defender's "Real-time protection" and "Cloud-delivered protection" and "Automatic sample submission".



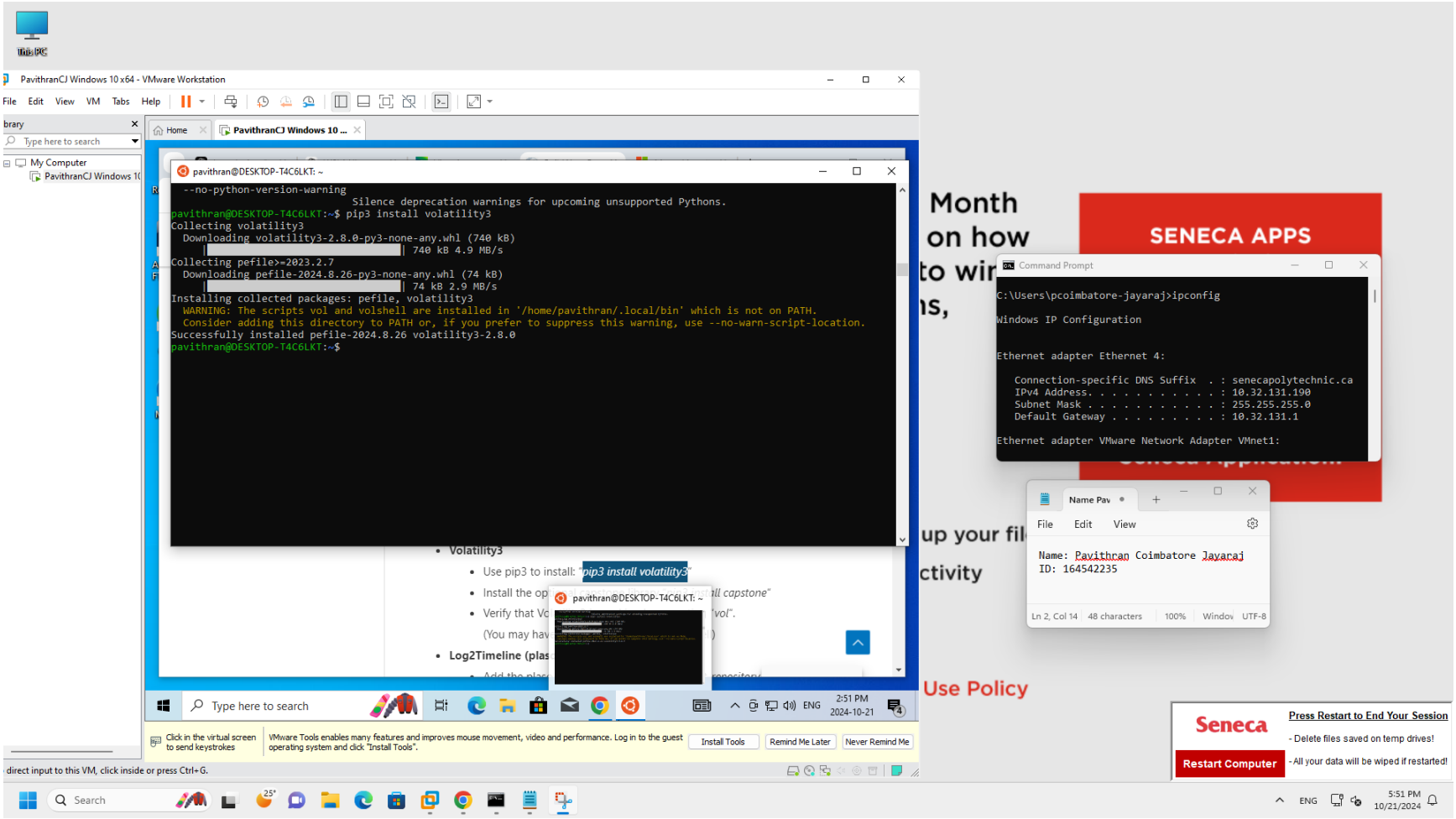
9. Exclude your working directories e.g. “C:\Cases” and “C:\Tools” from Defender’s virus and threat protection scanning. That way Defender won’t detect and remove important files during an investigation.

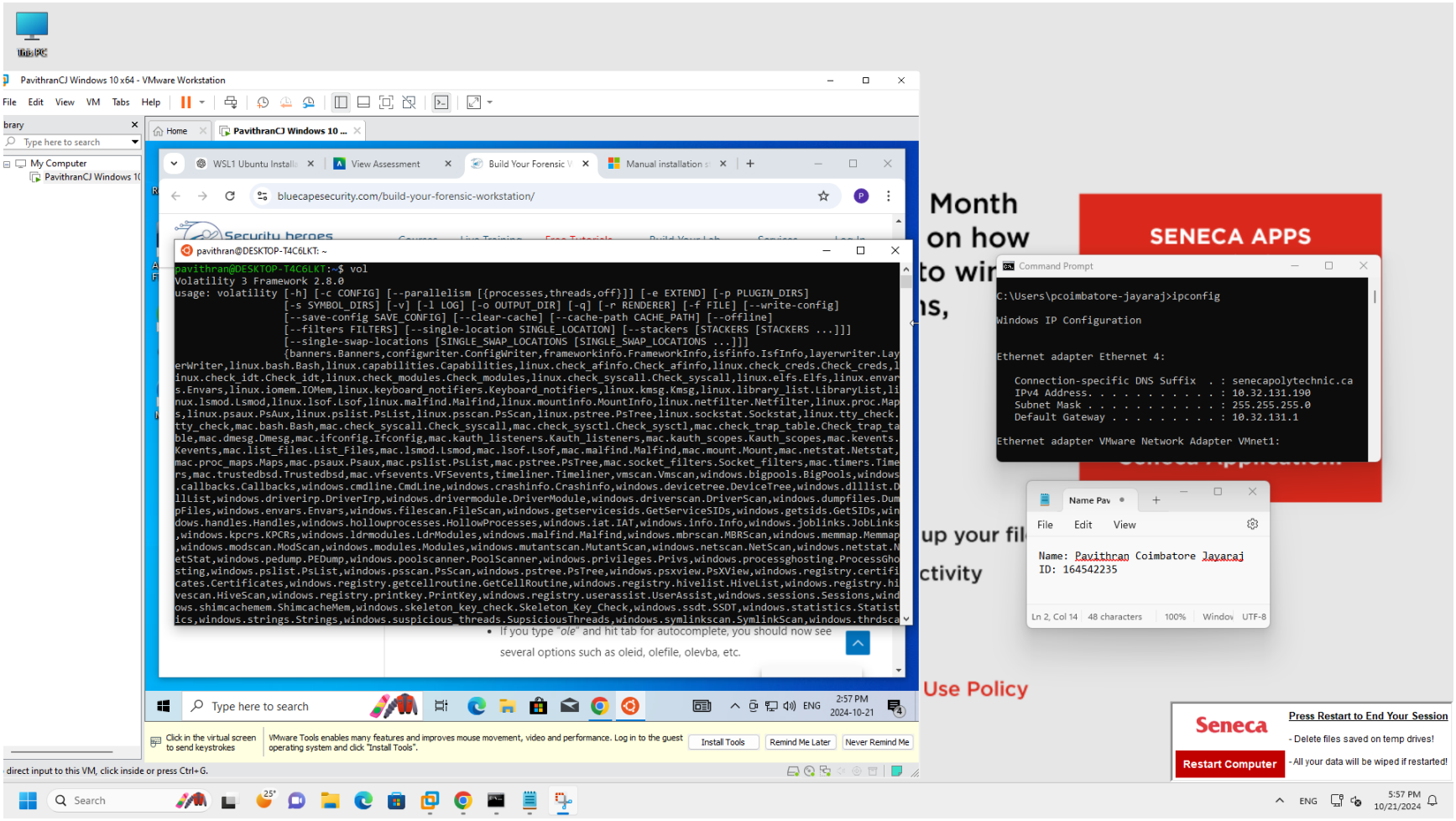


10. Install Forensic tools (Linux based)
    - pip3 – Python packet manager

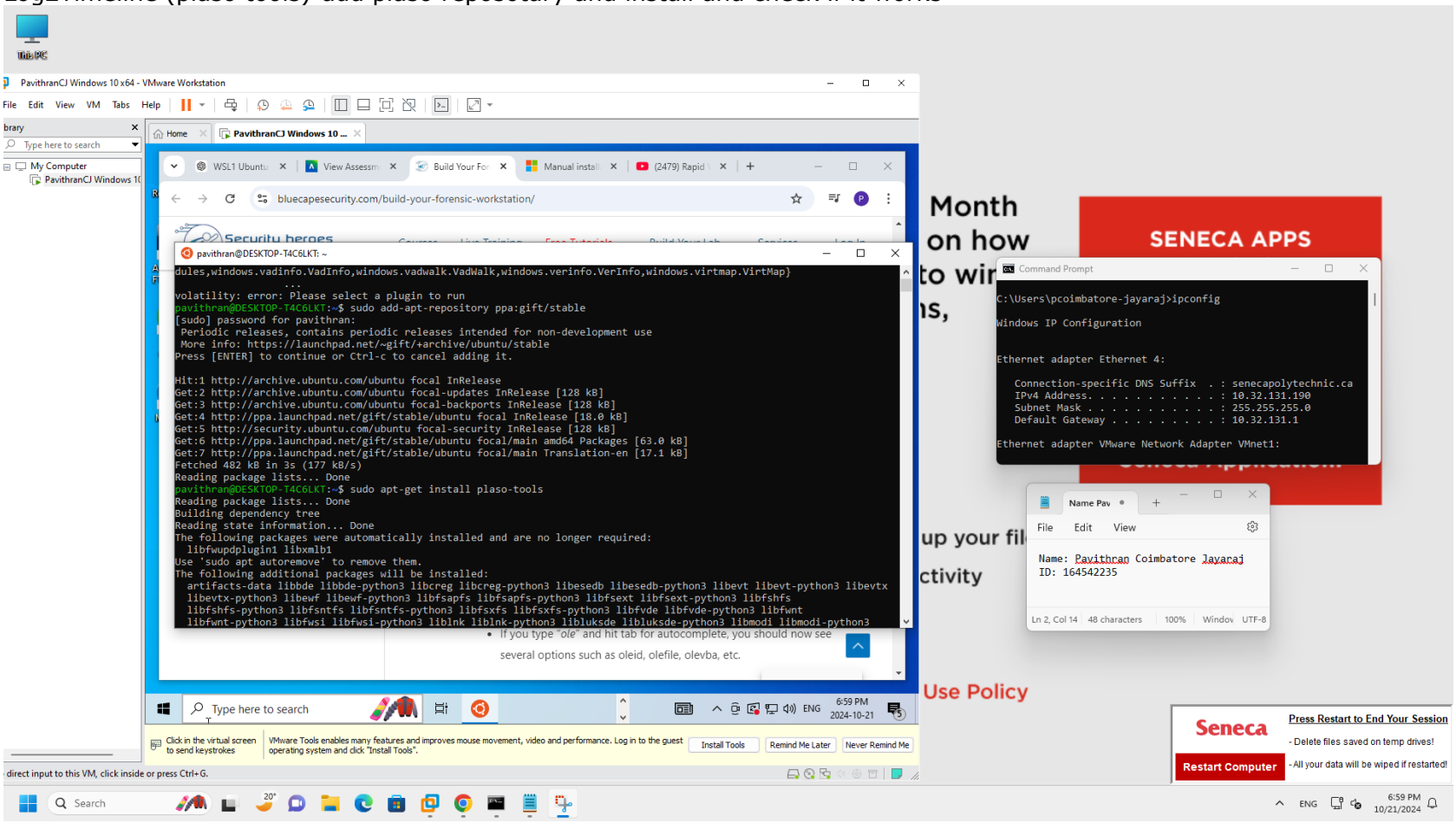


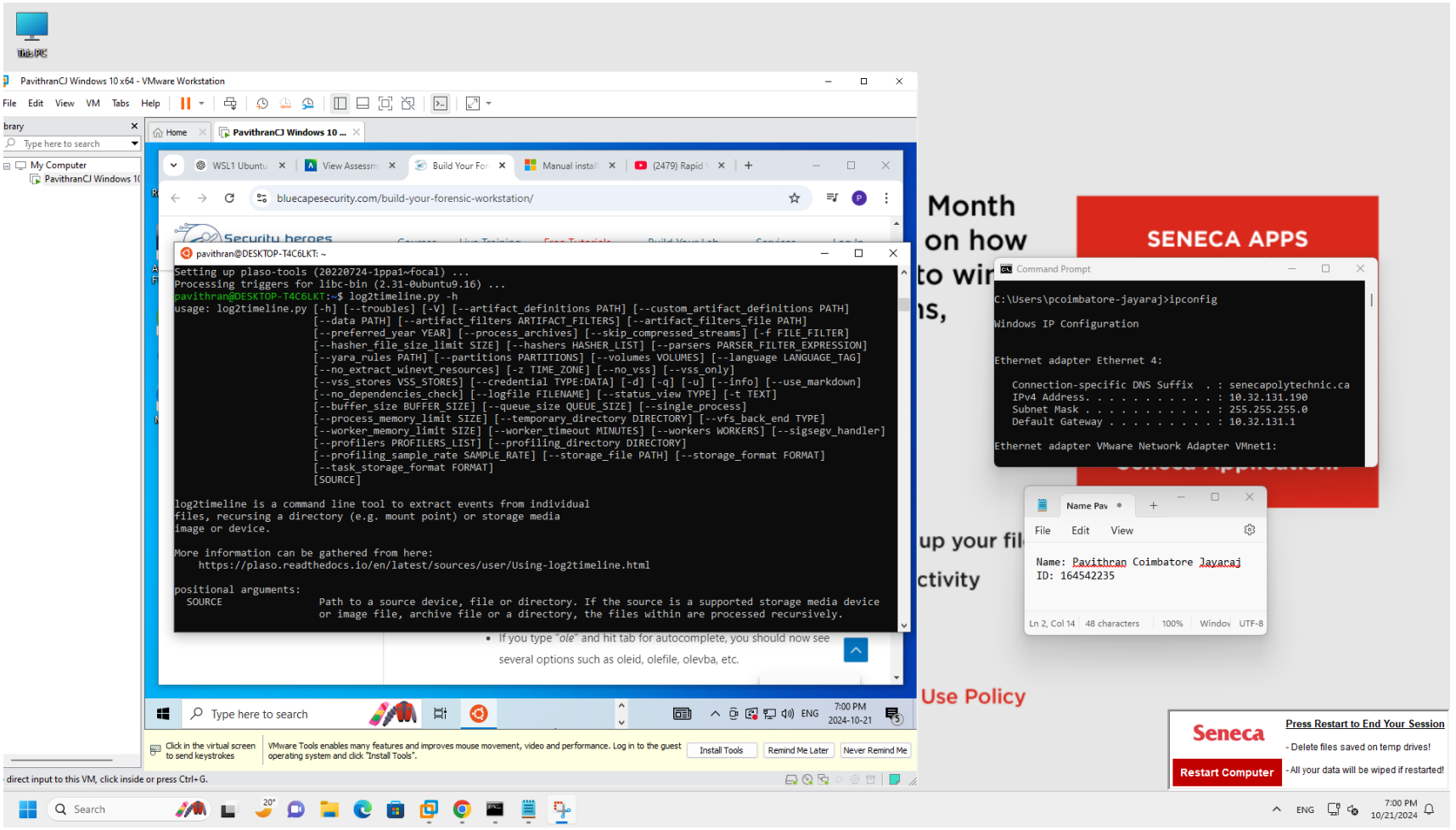
- Volatility3- install and check if its working



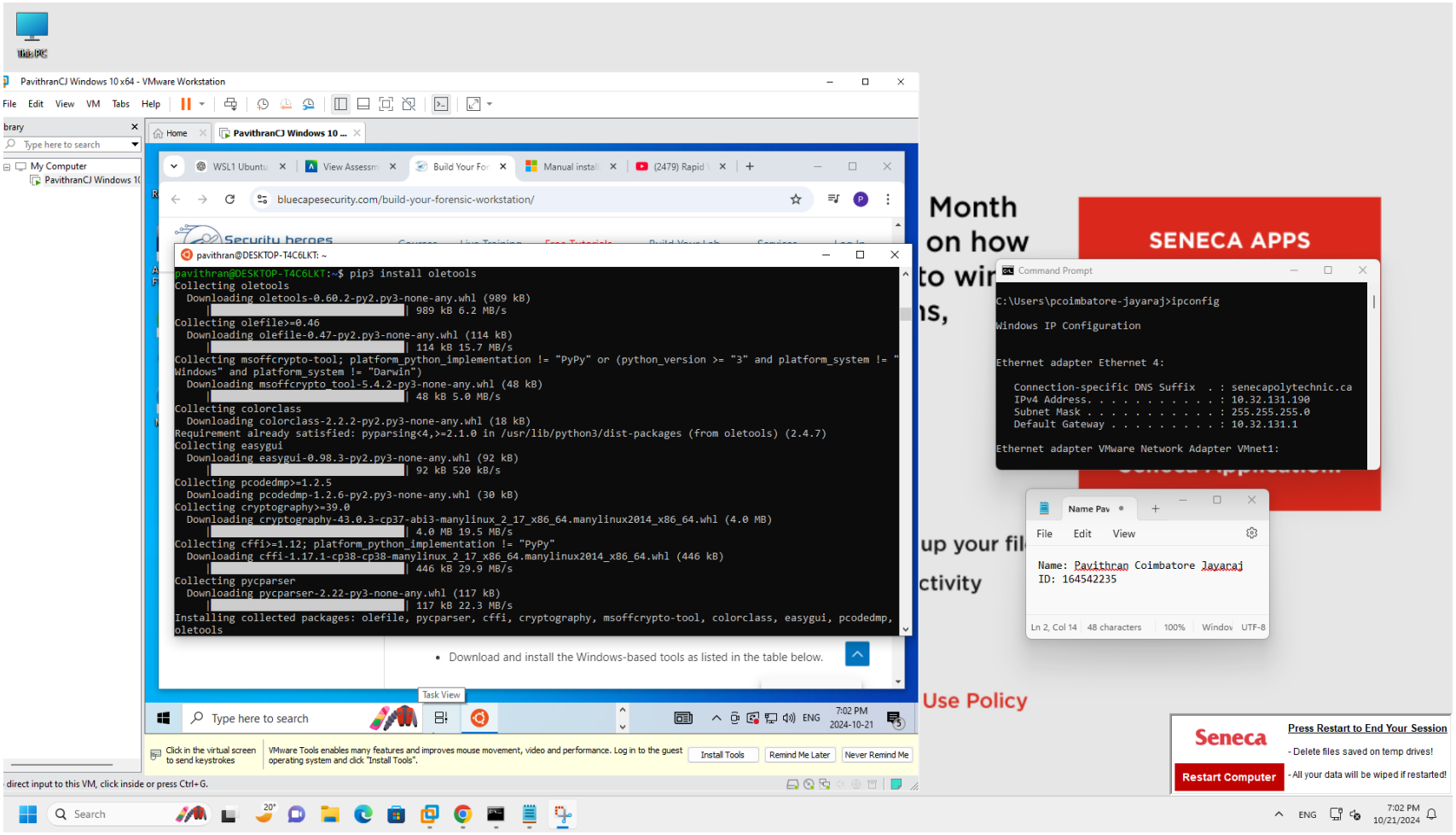

This PC
PavithranCJ Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Home
PavithranCJ Windows 10 ...
WSL1 Ubuntu Install
View Assessment
Build Your Forensic
Manual installation
bluecapesecurity.com/build-your-forensic-workstation/
pavithran@DESKTOP-T4C6LKT: ~
pavithran@DESKTOP-T4C6LKT:~$ vol
Volatility 3 Framework 2.8.0
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]
[--filters FILTERS] [--single-location SINGLE_LOCATION] [--stackers [STACKERS [STACKERS ...]]]
[--single-swap-locations [SINGLE_SWAP_LOCATIONS [SINGLE_SWAP_LOCATIONS ...]]]
{banners.Banners,configwriter.ConfigWriter,frameworkinfo.FrameworkInfo,isfinfo.IsfInfo,layerwriter.LayerWriter,linux.bash.Bash,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.elfs.Elfs,linux.envars.Envars,linux.iomem.IOMem,linux.keyboard_notifiers.Keyboard_notifiers,linux.kmsg.Kmsg,linux.library_list.LibraryList,linux.lsmod.Lsmod,linux.lsof.Lsof,linux.malfind.Malfind,linux.mountinfo.MountInfo,linux.netfilter.Netfilter,linux.proc.Maps,linux.psaux.PsAux,linux.pslist.PsList,linux.psscan.PsScan,linux.pstree.PsTree,linux.sockstat.Sockstat,linux.tty_check.tty_check,mac.bash.Bash,mac.check_syscall.Check_syscall,mac.check_sysctl.Check_sysctl,mac.check_trap_table.Check_trap_table,mac.dmesg.Dmesg,mac.ifconfig.Ifconfig,mac.kauth_listeners.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.Timeliner,vmscan.Vmscan,windows.bigpools.BigPools,windows.callbacks.Callbacks,windows.cmdline.CmdLine,windows.crashinfo.Crashinfo,windows.devicetree.DeviceTree,windows.dlllist.DllList,windows.driverirp.DriverIrp,windows.drivermodule.DriverModule,windows.driverscan.DriverScan,windows.dumpfiles.DumpFiles,windows.envars.Envars,windows.filescan.FileScan,windows.getservicesids.GetServiceSIDs,windows.getsids.GetSIDs,windows.handles.Handles,windows.hollowprocesses.HollowProcesses,windows.iat.IAT,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.Modules,windows.mutantscan.MutantScan,windows.netscan.NetScan,windows.netstat.NetStat,windows.pedump.PEDump,windows.poolscanner.PoolScanner,windows.privileges.Privs,windows.processghosting.ProcessGhosting,windows.pslist.PsList,windows.psscan.PsScan,windows.pstree.PsTree,windows.psxview.PsXView,windows.registry.certificates.Certificates,windows.registry.getcellroutine.GetCellRoutine,windows.registry.hivelist.HiveList,windows.registry.hivescan.HiveScan,windows.registry.printkey.PrintKey,windows.registry.userassist.UserAssist,windows.sessions.Sessions,windows.shimcachemem.ShimcacheMem,windows.skeleton_key_check.Skeleton_Key_Check,windows.ssdt.SSDT,windows.statistics.Statistics,windows.strings.Strings,windows.suspicious_threads.SuspiciousThreads,windows.symlinkscan.SymlinkScan,windows.thrdscan
If you type "ole" and hit tab for autocomplete, you should now see several options such as oleid, olefile, olevba, etc.
Type here to search
ENG 2:57 PM 2024-10-21
Click in the virtual screen to send keystrokes
VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".
Install Tools
Remind Me Later
Never Remind Me
direct input to this VM, click inside or press Ctrl+G.
Month
on how
to wir
ns,
SENECA APPS
Command Prompt
C:\Users\pcoimbatore-jayaraj>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet 4:
Connection-specific DNS Suffix . : senecapolytechnic.ca
IPv4 Address. . . . . : 10.32.131.190
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.32.131.1
Ethernet adapter VMware Network Adapter VMnet1:
Name Pav
File Edit View
Name: Pavithran Coimbatore Jayaraj
ID: 164542235
Ln 2, Col 14 48 characters 100% Windov UTF-8
up your fil
ctivity
Use Policy
Seneca
Press Restart to End Your Session
- Delete files saved on temp drives!
Restart Computer
- All your data will be wiped if restarted!
Search
ENG 5:57 PM 10/21/2024

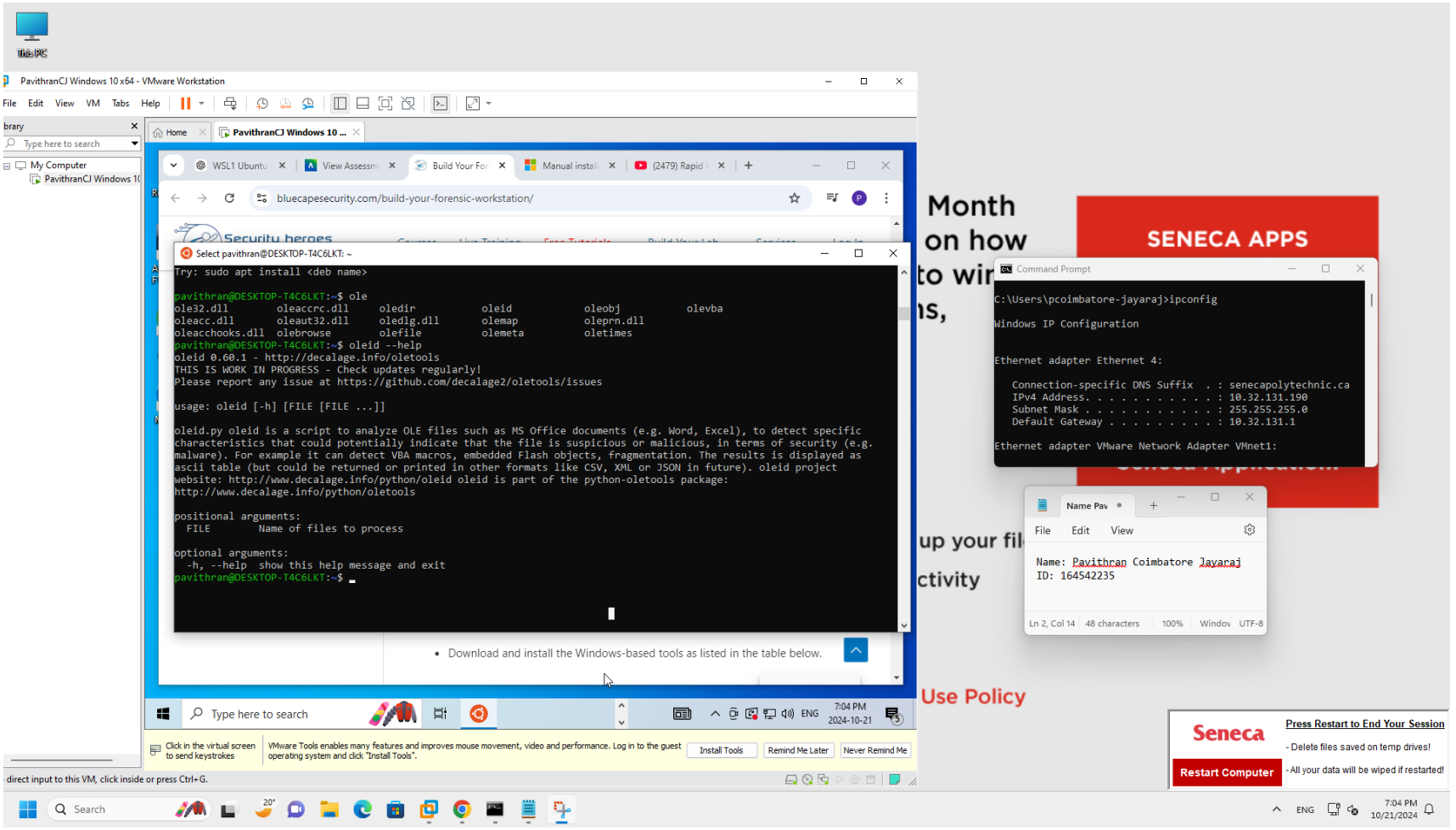
- Log2Timeline (plaso tools)-add plaso reposotary and install and check if it works



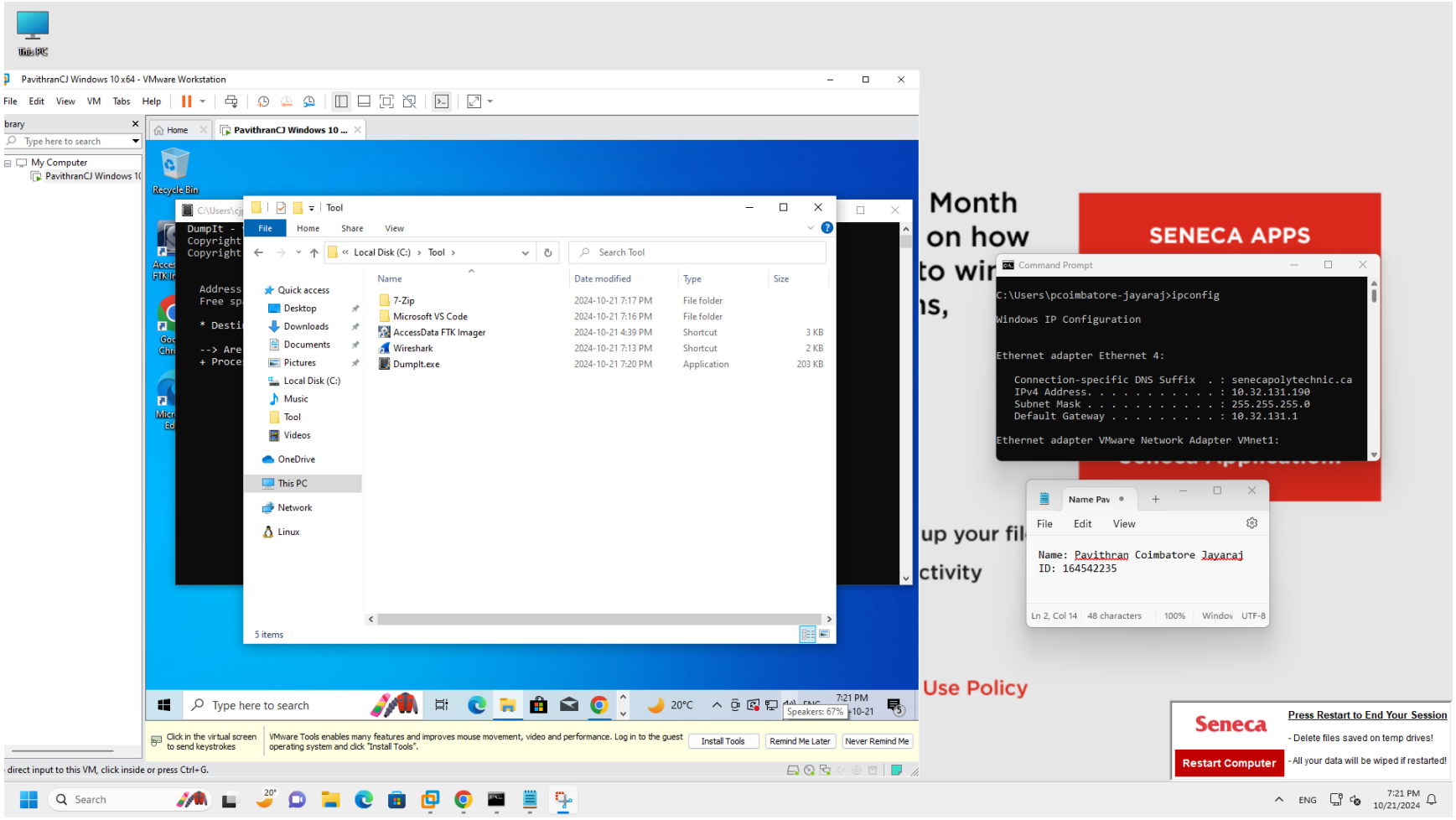

This PC
PavithranCJ Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Home
PavithranCJ Windows 10 ...
bluecapesecurity.com/build-your-forensic-workstation/
pavithran@DESKTOP-T4C6LKT: ~
Setting up plaso-tools (20220724-1ppa1~focal) ...
Processing triggers for libc-bin (2.31-0ubuntu9.16) ...
pavithran@DESKTOP-T4C6LKT:~$ log2timeline.py -h
usage: log2timeline.py [-h] [--troubles] [-V] [--artifact_definitions PATH] [--custom_artifact_definitions PATH]
[--data PATH] [--artifact_filters ARTIFACT_FILTERS] [--artifact_filters_file PATH]
[--preferred_year YEAR] [--process_archives] [--skip_compressed_streams] [-f FILE_FILTER]
[--hasher_file_size_limit SIZE] [--hashers HASHER_LIST] [--parsers PARSER_FILTER_EXPRESSION]
[--yara_rules PATH] [--partitions PARTITIONS] [--volumes VOLUMES] [--language LANGUAGE_TAG]
[--no_extract_winevt_resources] [-z TIME_ZONE] [--no_vss] [--vss_only]
[--vss_stores VSS_STORES] [--credential TYPE:DATA] [-d] [-q] [-u] [--info] [--use_markdown]
[--no_dependencies_check] [--logfile FILENAME] [--status_view TYPE] [-t TEXT]
[--buffer_size BUFFER_SIZE] [--queue_size QUEUE_SIZE] [--single_process]
[--process_memory_limit SIZE] [--temporary_directory DIRECTORY] [--vfs_back_end TYPE]
[--worker_memory_limit SIZE] [--worker_timeout MINUTES] [--workers WORKERS] [--sigsegv_handler]
[--profilers PROFILERS_LIST] [--profiling_directory DIRECTORY]
[--profiling_sample_rate SAMPLE_RATE] [--storage_file PATH] [--storage_format FORMAT]
[--task_storage_format FORMAT]
[SOURCE]
log2timeline is a command line tool to extract events from individual
files, recursing a directory (e.g. mount point) or storage media
image or device.
More information can be gathered from here:
https://plaso.readthedocs.io/en/latest/sources/user/Using-log2timeline.html
positional arguments:
SOURCE Path to a source device, file or directory. If the source is a supported storage media device
or image file, archive file or a directory, the files within are processed recursively.
Type here to search
ENG
7:00 PM
2024-10-21
Click in the virtual screen to send keystrokes
VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".
Install Tools
Remind Me Later
Never Remind Me
direct input to this VM, click inside or press Ctrl+G.
Search
Month
on how
to wir
ns,
SENECA APPS
Command Prompt
C:\Users\pcoimbatore-jayaraj>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet 4:
Connection-specific DNS Suffix . : senecapolytechnic.ca
IPv4 Address. . . . . : 10.32.131.190
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.32.131.1
Ethernet adapter VMware Network Adapter VMnet1:
Name Pav
File Edit View
Name: Pavithran Coimbatore Jayaraj
ID: 164542235
Ln 2, Col 14 48 characters 100% Windov UTF-8
up your fil
ctivity
Use Policy
Seneca
Press Restart to End Your Session
- Delete files saved on temp drives!
- All your data will be wiped if restarted!
Restart Computer
ENG
7:00 PM
10/21/2024

- Oletools


PavithranCJ Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
PavithranCJ Windows 10 ...
bluecapesecurity.com/build-your-forensic-workstation/
pavithran@DESKTOP-T4C6LKT: ~
pavithran@DESKTOP-T4C6LKT:~$ pip3 install oletools
Collecting oletools
Downloading oletools-0.60.2-py2.py3-none-any.whl (989 kB)
| 989 kB 6.2 MB/s
Collecting olefile>=0.46
Downloading olefile-0.47-py2.py3-none-any.whl (114 kB)
| 114 kB 15.7 MB/s
Collecting msoffcrypto-tool; platform_python_implementation != "PyPy" or (python_version >= "3" and platform_system != "Windows" and platform_system != "Darwin")
Downloading msoffcrypto_tool-5.4.2-py3-none-any.whl (48 kB)
| 48 kB 5.0 MB/s
Collecting colorclass
Downloading colorclass-2.2.2-py2.py3-none-any.whl (18 kB)
Requirement already satisfied: pyparsing<4,>=2.1.0 in /usr/lib/python3/dist-packages (from oletools) (2.4.7)
Collecting easygui
Downloading easygui-0.98.3-py2.py3-none-any.whl (92 kB)
| 92 kB 520 kB/s
Collecting pcodedmp>=1.2.5
Downloading pcodedmp-1.2.6-py2.py3-none-any.whl (30 kB)
Collecting cryptography>=39.0
Downloading cryptography-43.0.3-cp37-abi3-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (4.0 MB)
| 4.0 MB 19.5 MB/s
Collecting cffi>=1.12; platform_python_implementation != "PyPy"
Downloading cffi-1.17.1-cp38-cp38-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (446 kB)
| 446 kB 29.9 MB/s
Collecting pycparser
Downloading pycparser-2.22-py3-none-any.whl (117 kB)
| 117 kB 22.3 MB/s
Installing collected packages: olefile, pycparser, cffi, cryptography, msoffcrypto-tool, colorclass, easygui, pcodedmp, oletools
Download and install the Windows-based tools as listed in the table below.
Task View
Type here to search
ENG 7:02 PM 2024-10-21
Click in the virtual screen to send keystrokes
VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".
Install Tools
Remind Me Later
Never Remind Me
direct input to this VM, click inside or press Ctrl+G.
Month
on how
to wir
ns,
SENECA APPS
Command Prompt
C:\Users\pcoimbatore-jayaraj>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet 4:
Connection-specific DNS Suffix . : senecapolytechnic.ca
IPv4 Address. . . . . : 10.32.131.190
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.32.131.1
Ethernet adapter VMware Network Adapter VMnet1:
Name Pav
File Edit View
Name: Pavithran Coimbatore Jayaraj
ID: 164542235
Ln 2, Col 14 48 characters 100% Windov UTF-8
up your fil
ctivity
Use Policy
Seneca
Press Restart to End Your Session
- Delete files saved on temp drives!
- All your data will be wiped if restarted!
Restart Computer
Search
ENG 7:02 PM 10/21/2024


This PC
PavithranCJ Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Home
PavithranCJ Windows 10 ...
bluecapesecurity.com/build-your-forensic-workstation/
Select pavithran@DESKTOP-T4C6LKT: ~
Try: sudo apt install <deb name>
pavithran@DESKTOP-T4C6LKT:~$ ole
ole32.dll oleaccrc.dll oledir oleid oleobj olevba
oleacc.dll oleaut32.dll oledlg.dll olemap oleprn.dll
oleacchooks.dll olebrowse olefile olemeta oletimes
pavithran@DESKTOP-T4C6LKT:~$ oleid --help
oleid 0.60.1 - http://decalage.info/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues
usage: oleid [-h] [FILE [FILE ...]]
oleid.py oleid is a script to analyze OLE files such as MS Office documents (e.g. Word, Excel), to detect specific characteristics that could potentially indicate that the file is suspicious or malicious, in terms of security (e.g. malware). For example it can detect VBA macros, embedded Flash objects, fragmentation. The results is displayed as ascii table (but could be returned or printed in other formats like CSV, XML or JSON in future). oleid project website: http://www.decalage.info/python/oleid oleid is part of the python-oletools package: http://www.decalage.info/python/oletools
positional arguments:
FILE Name of files to process
optional arguments:
-h, --help show this help message and exit
pavithran@DESKTOP-T4C6LKT:~$
Download and install the Windows-based tools as listed in the table below.
Type here to search
ENG 7:04 PM 2024-10-21
Click in the virtual screen to send keystrokes
VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".
Install Tools
Remind Me Later
Never Remind Me
direct input to this VM, click inside or press Ctrl+G.
Command Prompt
C:\Users\pcoimbatore-jayaraj>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet 4:
Connection-specific DNS Suffix . : senecapolytechnic.ca
IPv4 Address. . . . . : 10.32.131.190
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.32.131.1
Ethernet adapter VMware Network Adapter VMnet1:
Name Pav
File Edit View
Name: Pavithran Coimbatore Jayaraj
ID: 164542235
Ln 2, Col 14 48 characters 100% Windov UTF-8
Month
on how
to wir
ns,
SENECA APPS
up your fil
ctivity
Use Policy
Seneca
Press Restart to End Your Session
- Delete files saved on temp drives!
- All your data will be wiped if restarted!
Restart Computer
Search
ENG 7:04 PM 10/21/2024

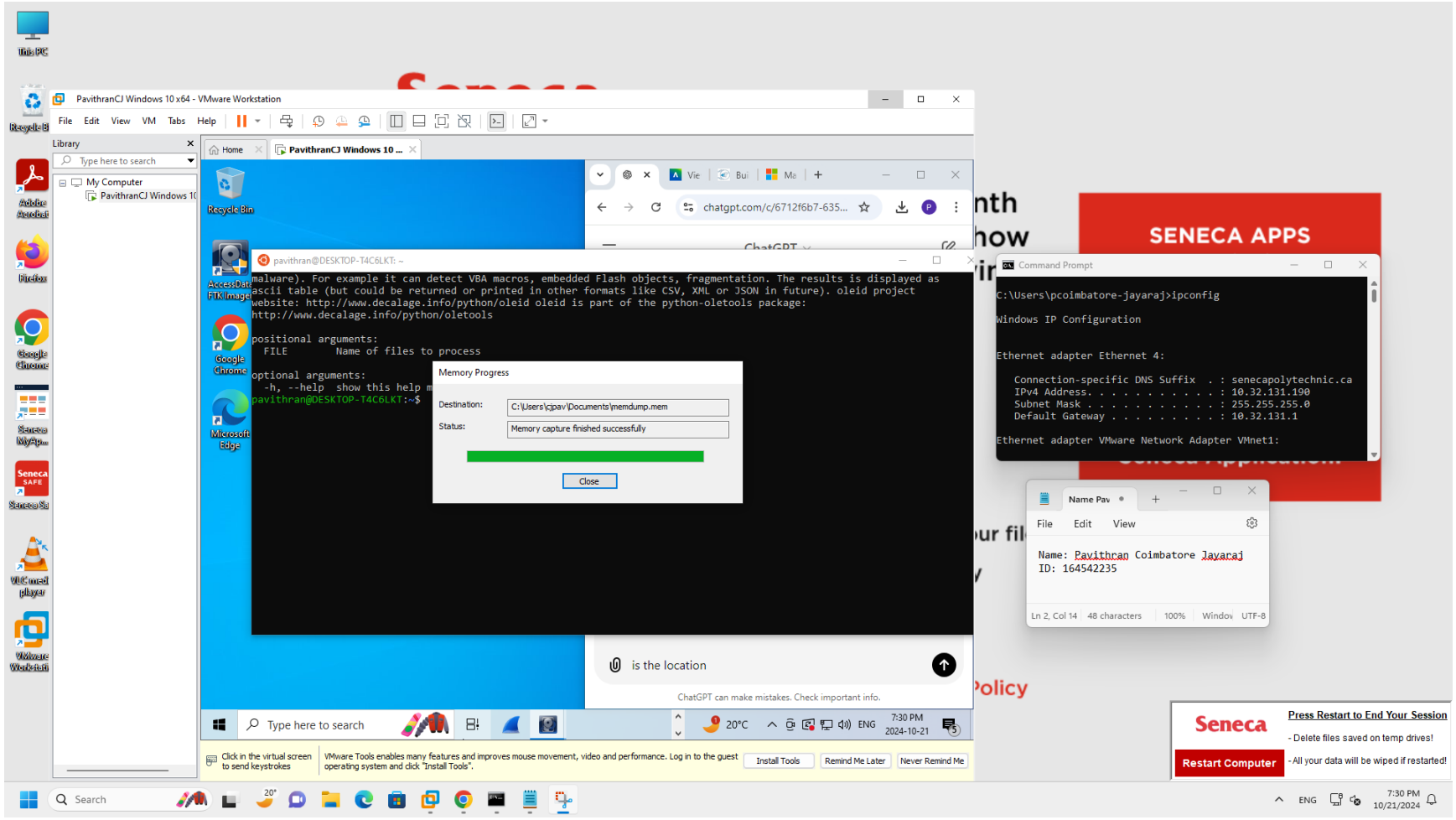
11. Install Forensic tools (windows based)
    - 7-Zip
    - Microsoft VS Code
    - FTK Imager
    - Wireshark
    - Dumpit



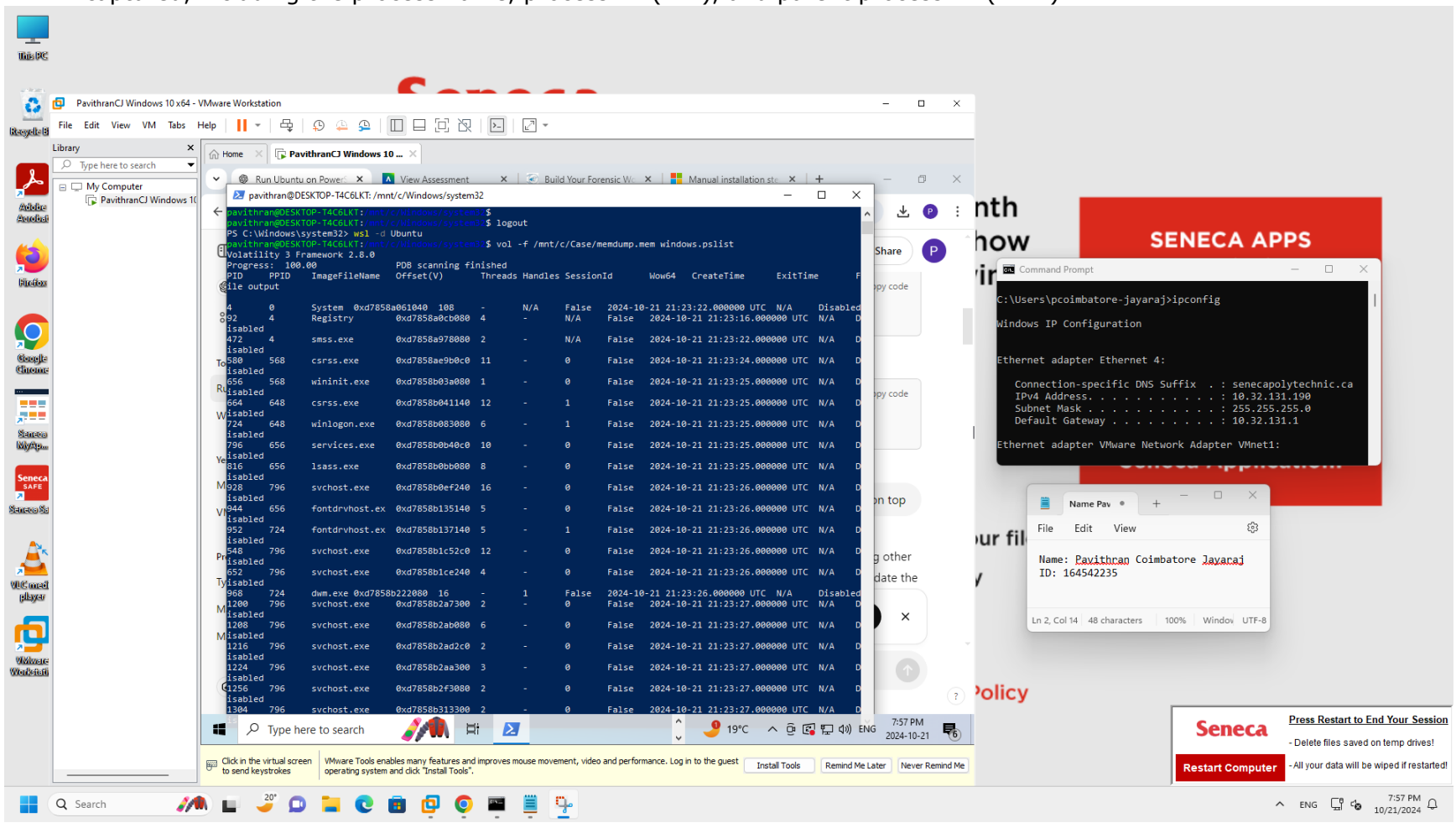
Part 2: Memory Analysis

1. Voaltility

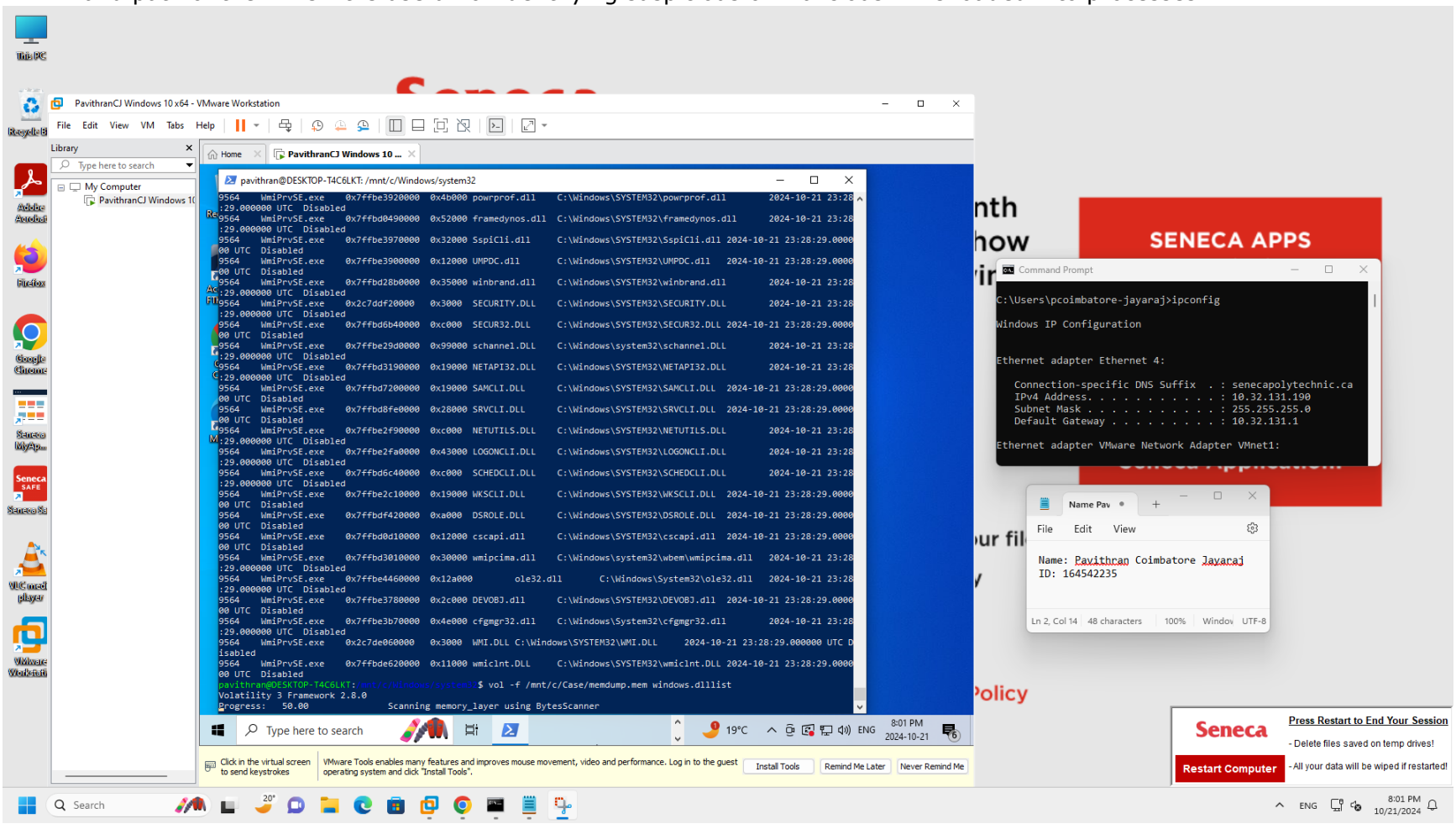
- Use FTK Imager to capture memory Image.



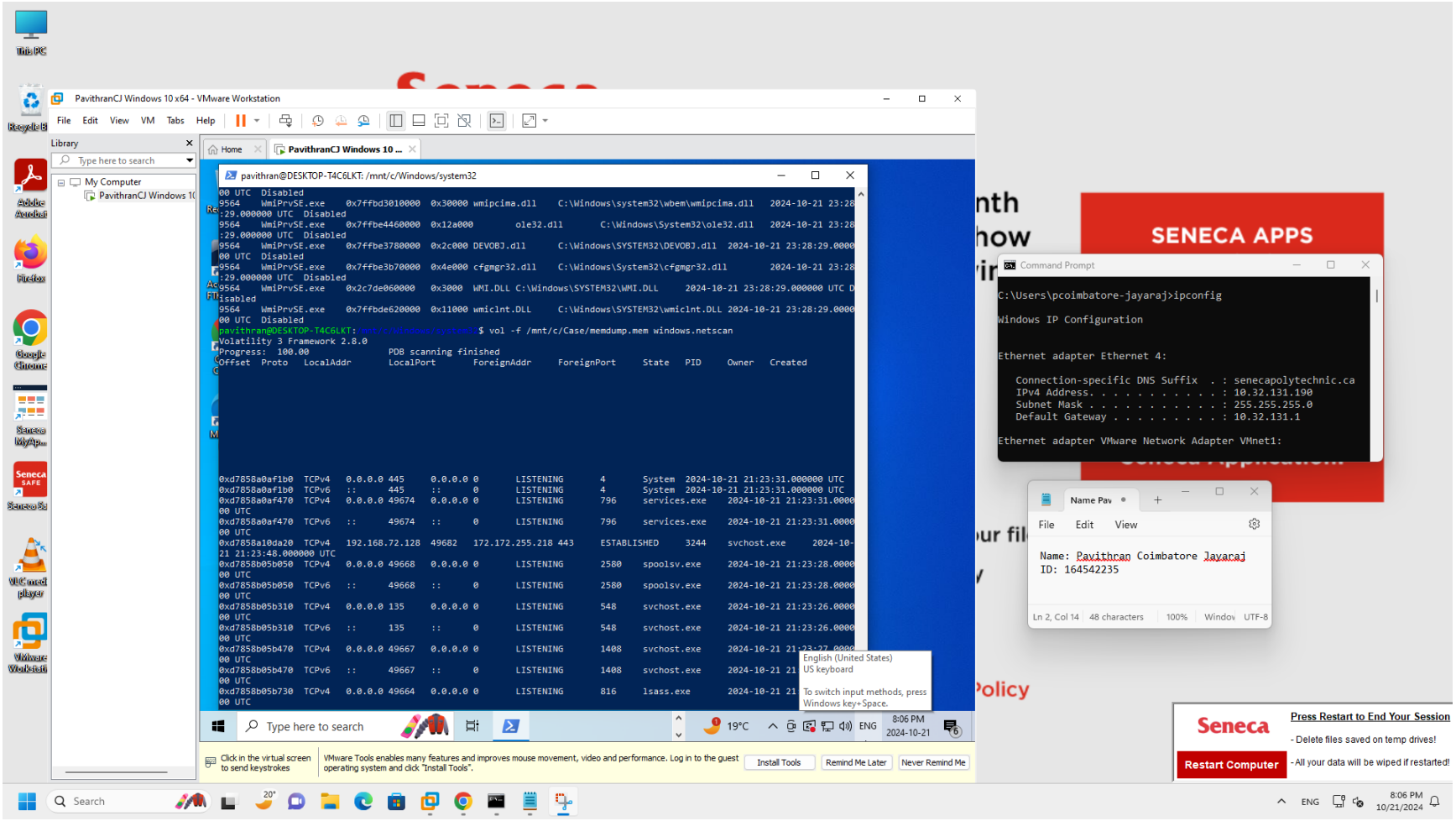
- Pslist command will show you a list of active processes in the system at the time the memory dump was captured, including the process name, process ID (PID), and parent process ID (PPID).



- dlllist command will provide a list of all DLLs loaded into each process's memory, including the base address, size, and path of the DLLs. It is useful for identifying suspicious or malicious DLLs loaded into processes.

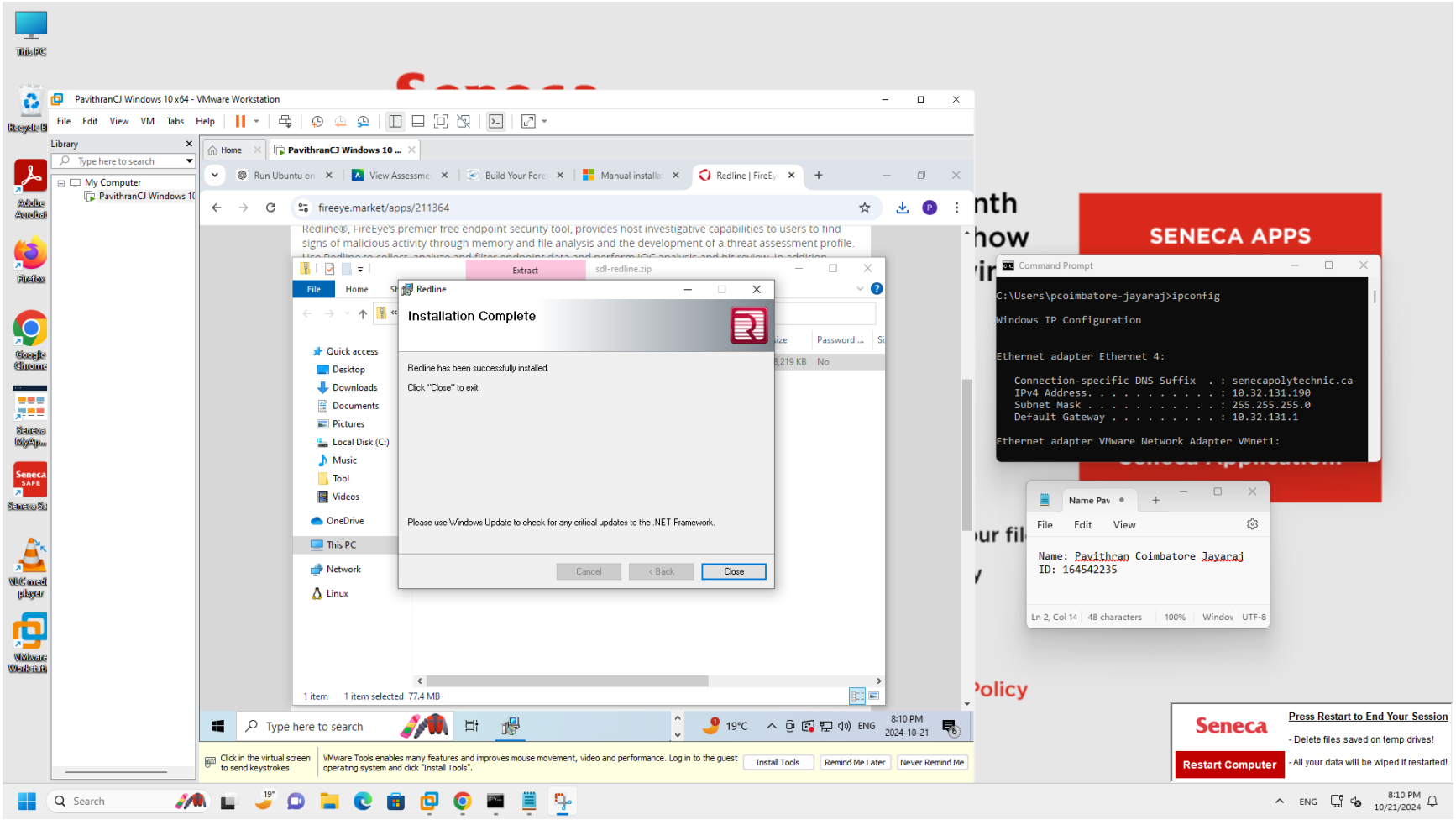


- The netscan plugin scans for TCP and UDP endpoints, along with listening sockets, and provides details

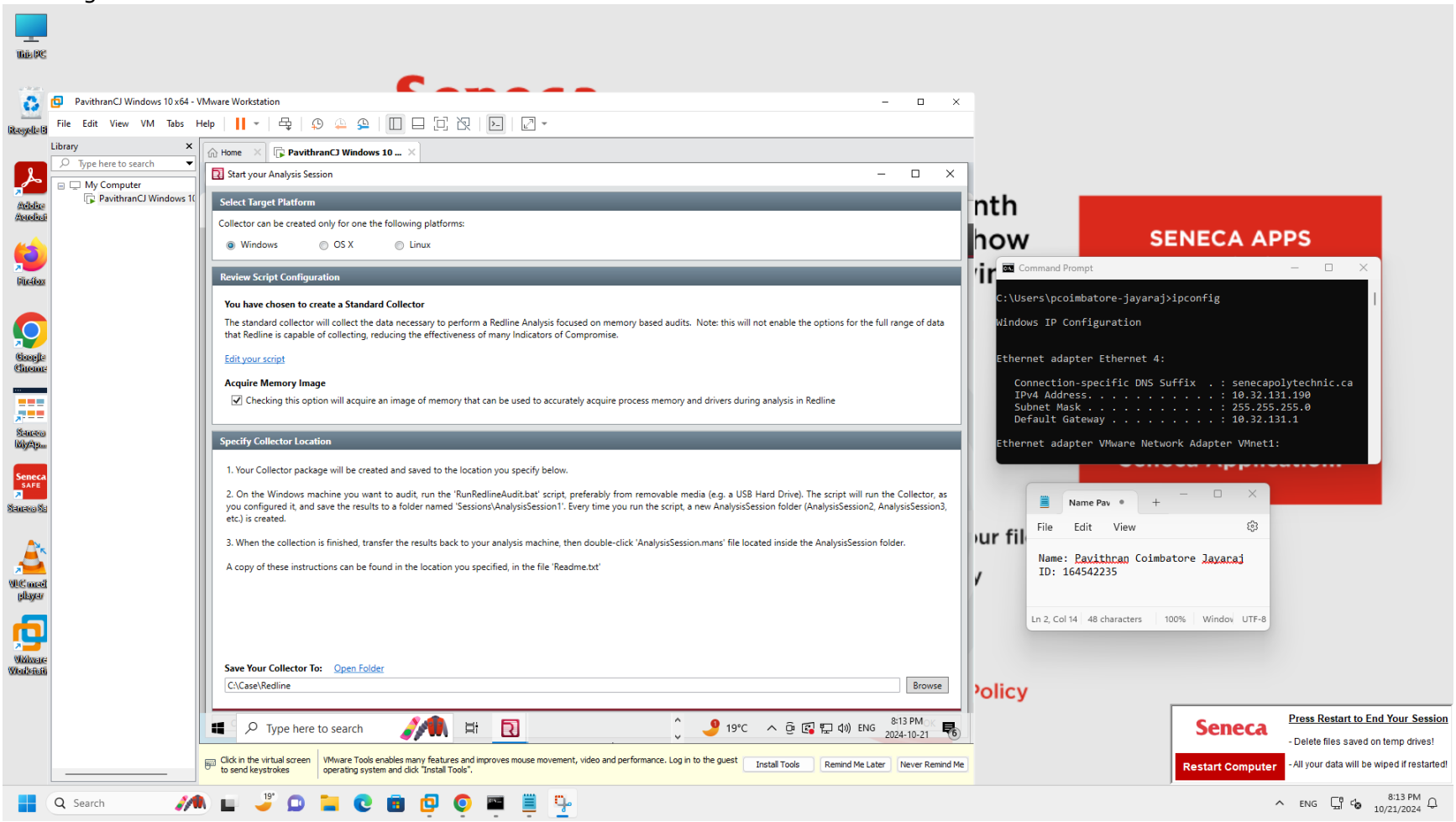


2. Redline

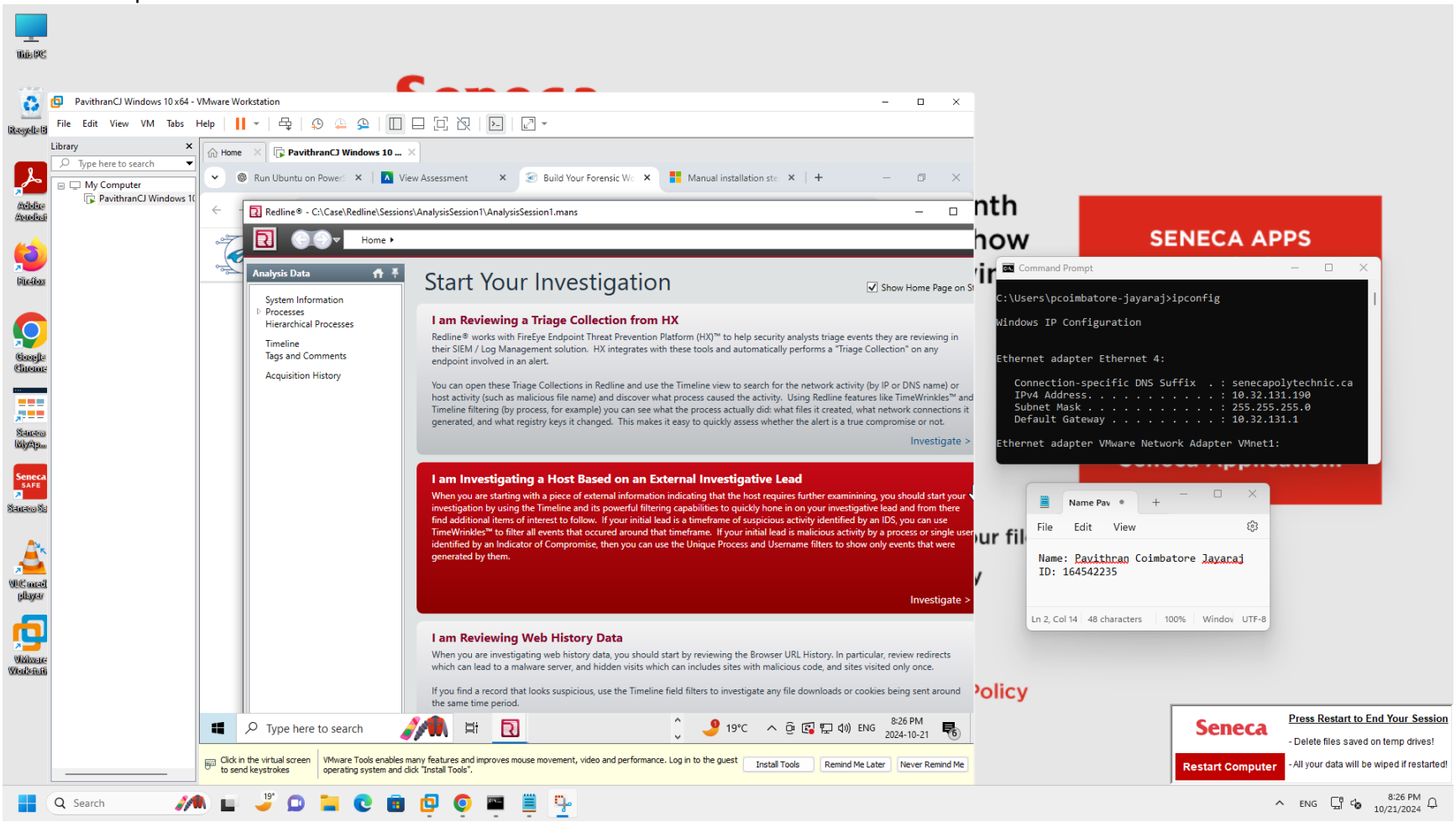
- Download and install redline from the website.



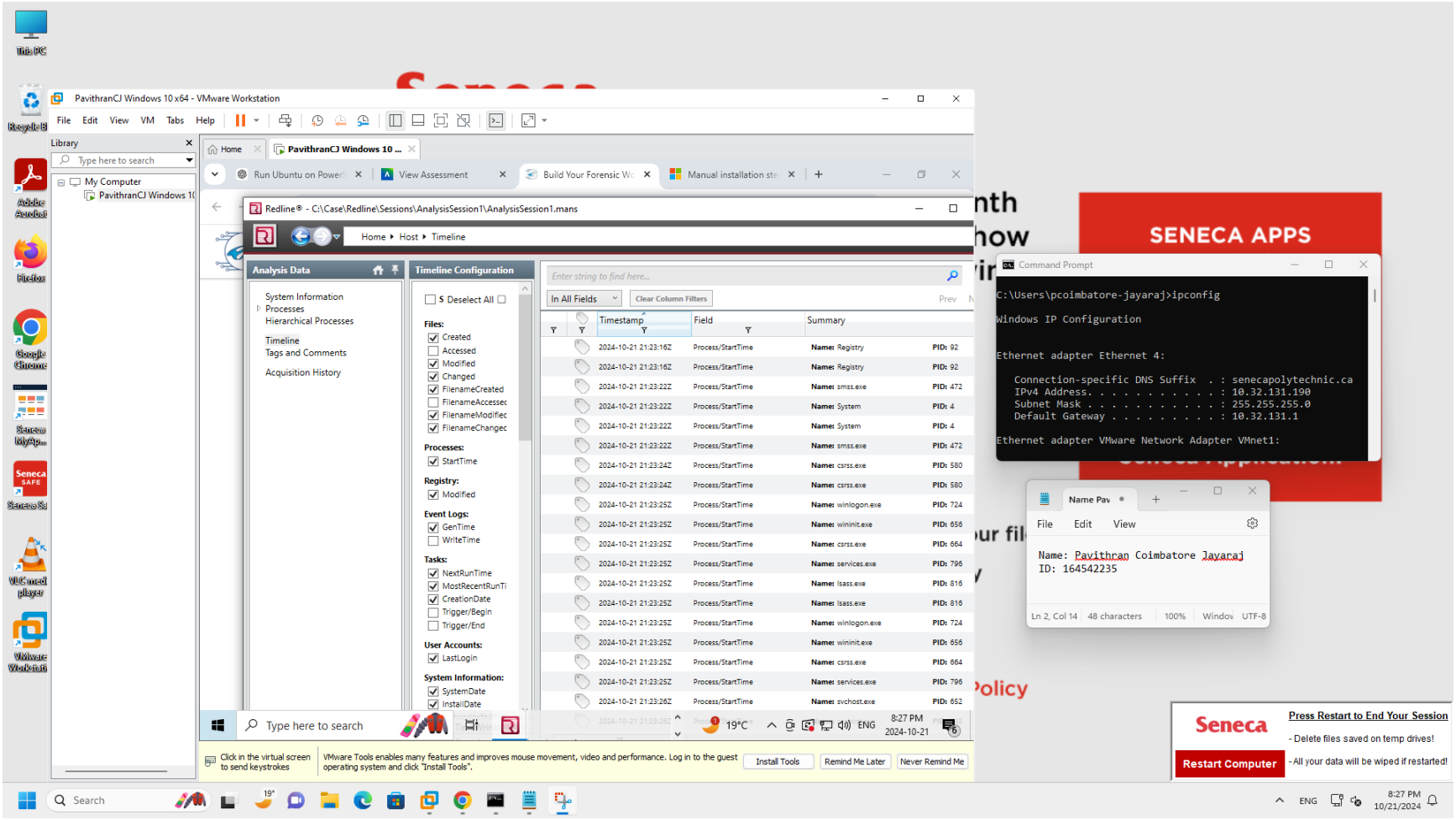
- Capture Image first by giving target platform as windows and check the acquire memory image checkbox and give a location for it to be stored.



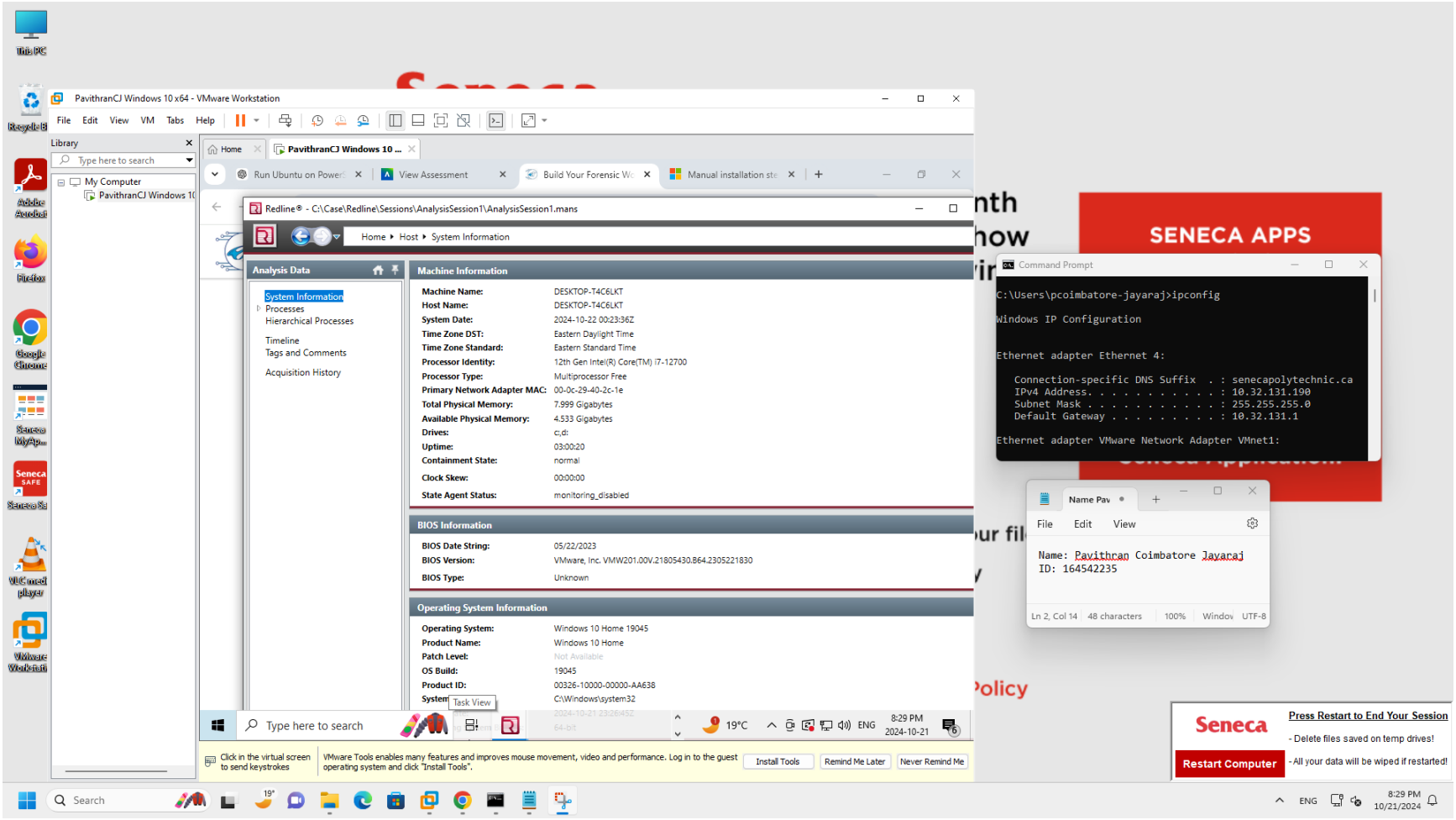
- Run the redline analysis session and click on host base based on an external investigative lead to see if external subspinous or malicious activities exists.



- Used timeline configuration to filter files, process, registry etc based on timestamps.

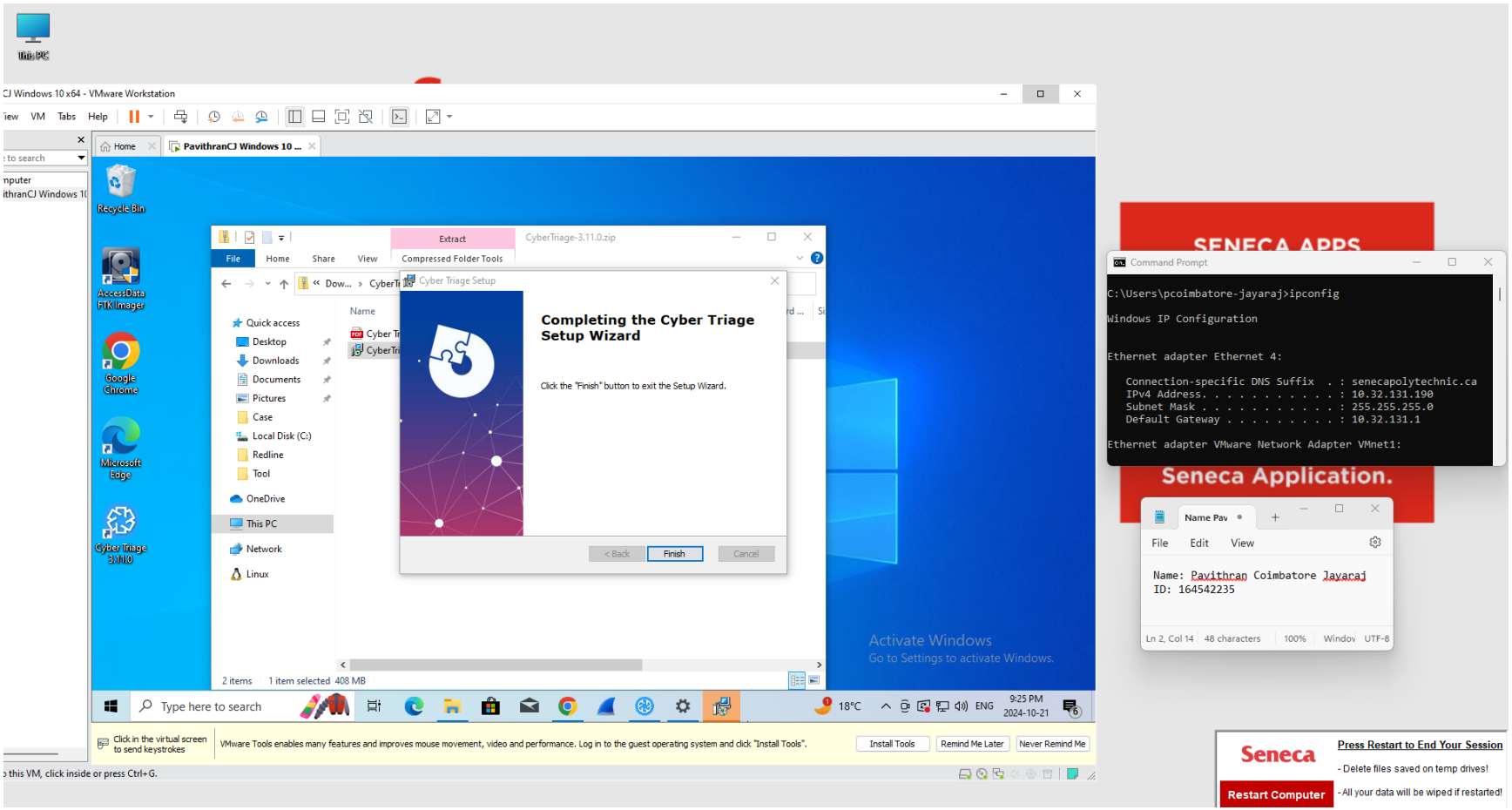


- The system Information gives the details of the system as shown below.

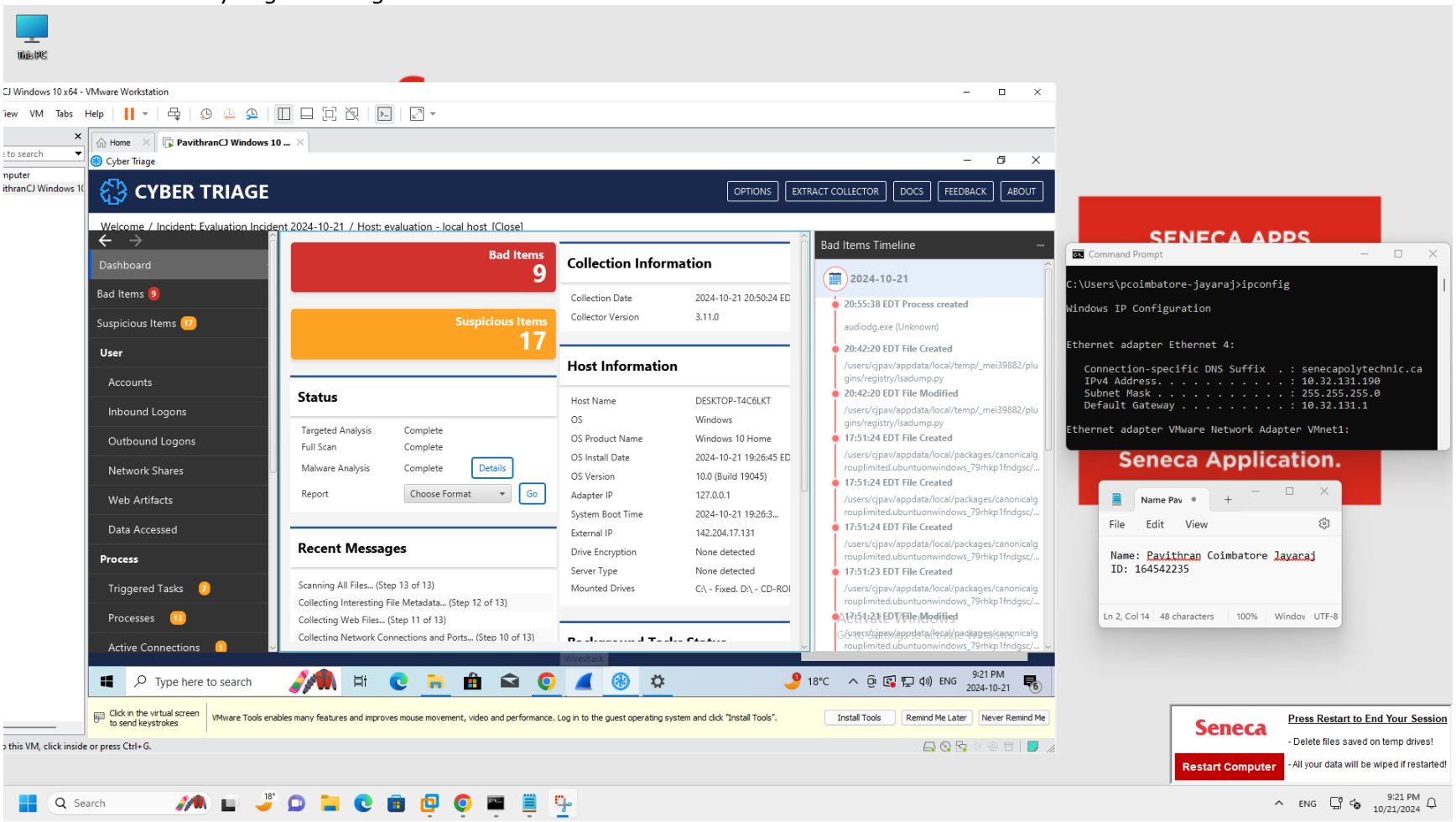


3. Cyber Triage

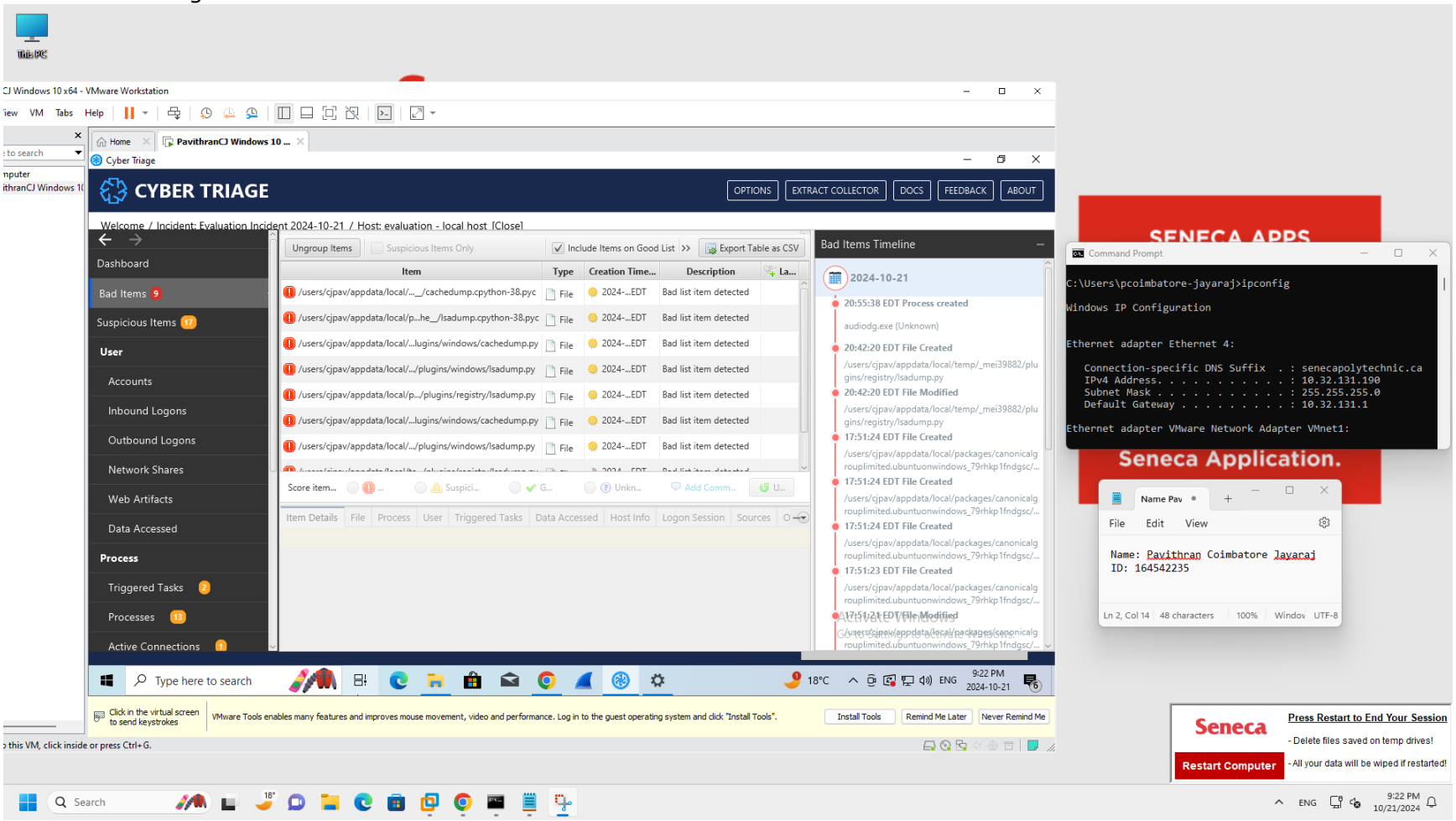
- Download and install the tool



- Cyber Triage was used here to evaluate the state of a Windows 10 machine, detect potential security threats, and flag bad or suspicious items based on file behaviors and system activity logs. I loaded the memory image and started analysing the image.



- The result shows all the bad and subspinous items we can investigate. Each of them by going into the directory and taking a look at it.



Part 3: Personal Learning experience.

Establishing the forensic workstation on the MacBook was quite a challenging journey, but it definitely came with its own set of obstacles. At first, my intention was to utilize VMware Fusion in order to establish the virtual environment for analyzing memory and malware. Regrettably, my VMware Fusions Windows 11 became corrupted, causing a significant setback for me. I needed to change to UTM, but I encountered a problem when I was unable to disable the secure boot feature, which was crucial for capturing the memory image correctly. Finding a Windows 10 ARM ISO file proved to be much harder than anticipated, which made it impossible to use VirtualBox. At that moment, it dawned on me that I had no other option but to go to our college and utilize the computers there to continue with my tasks.

After arriving at the college, I started arranging the forensic environment which led to a smoother workflow. I focused on setting up important tools such as Volatility, Redline, and Cyber Triage. Both Volatility and Redline were easier to understand compared to other tools, each with its own individual learning curve. Nonetheless, the analysis of Cyber Triage required more time than expected. However, the process provided me with a valuable opportunity to gain practical experience in the time-consuming nature of forensic investigations, especially when faced with extensive data sets or complex situations.

In spite of the challenges, this project provided valuable lessons on establishing a forensic workstation from the beginning and utilizing various tools to examine memory dumps for potential malware or malicious behavior. I gained a complete grasp of memory analysis by utilizing the unique capabilities of each tool: Volatility, Redline, and Cyber Triage. Reflecting on the past, I acknowledge how these obstacles have enhanced my comprehension of the technical and logistical elements of forensic investigation. Overall, despite the challenging nature of the process, it was highly gratifying.