Contents

Abstract

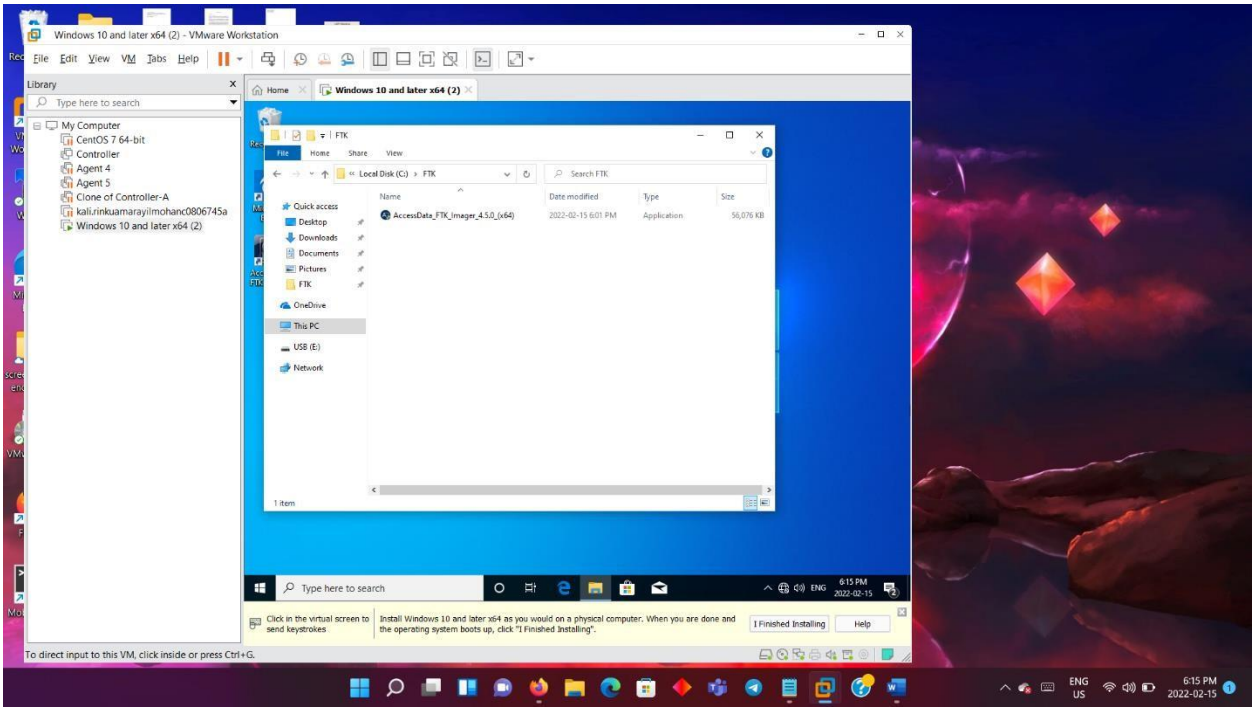
In this lab we work on various tools like FTK imager, creating image with the help of USB, host forensics registry analysis, PSRECON tool, NTUSER.DAT. These are mainly digital forensics tools that help in research and finding of computer evidence with the extracted report to understand the step-by-step procedure that has taken place. It in fact makes the process simple and easy to understand. The output is justified with solid evidence.

Part 1a

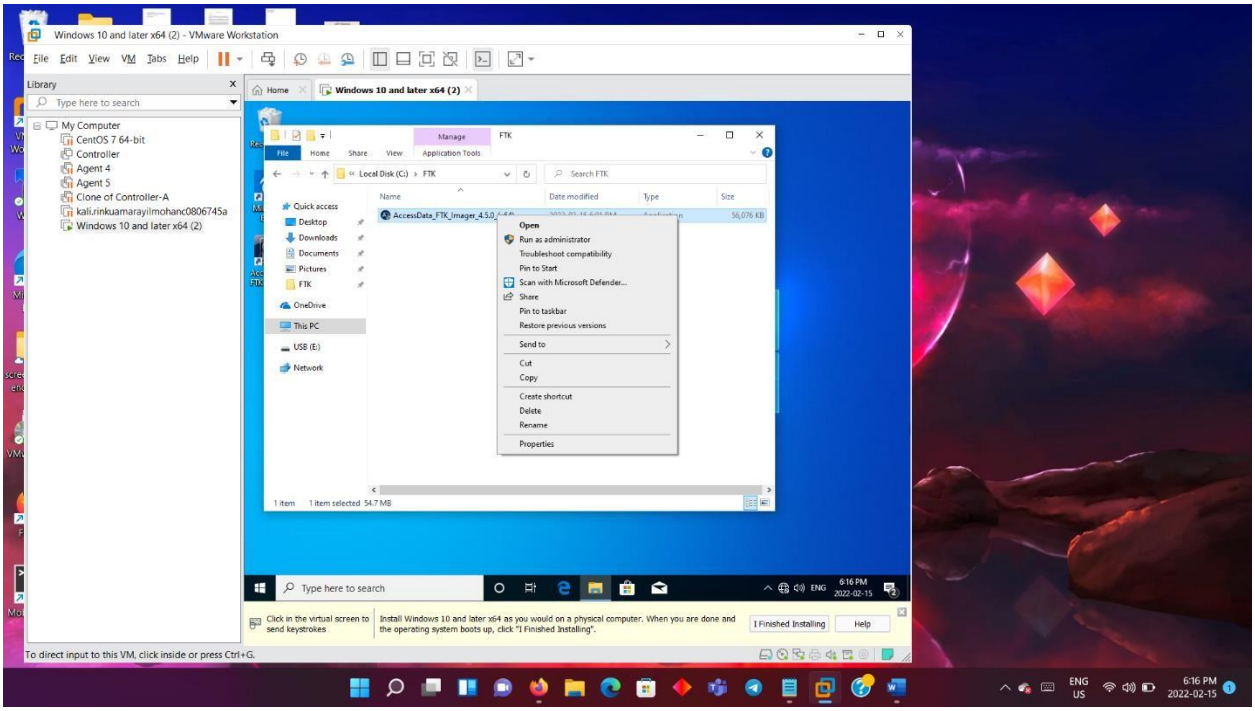
FTK Imager

Basically, a computer forensics software manufactured by access data. It can acquire and analyze computer forensic data for volatile and non-volatile memory.

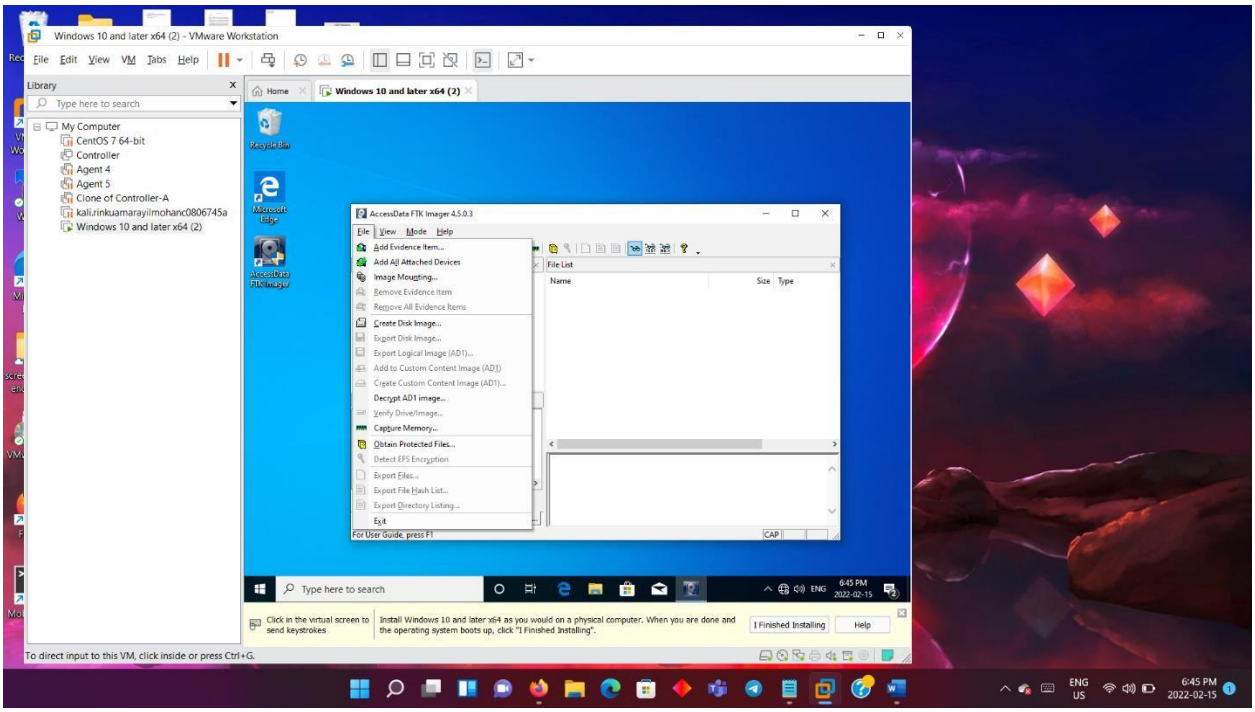
- Move the AccessData_FTK_Imager_4.5.0 exe file to windows virtual machine



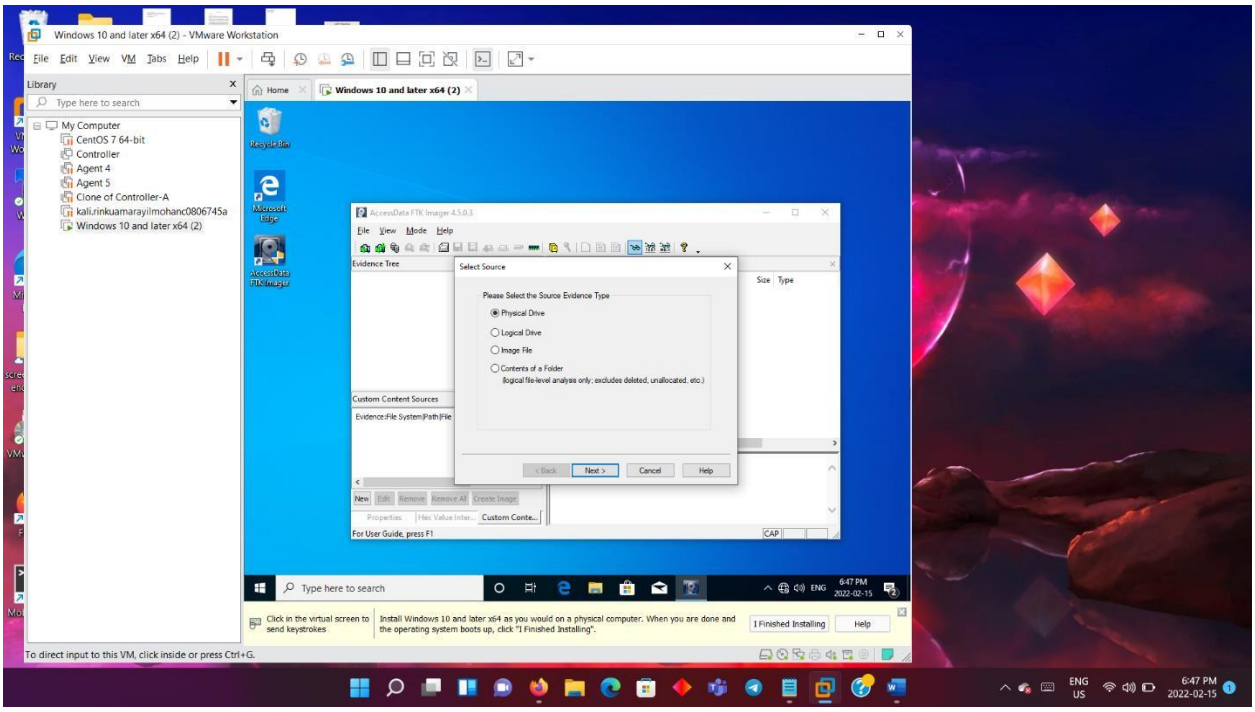
- Run the file as administrator.



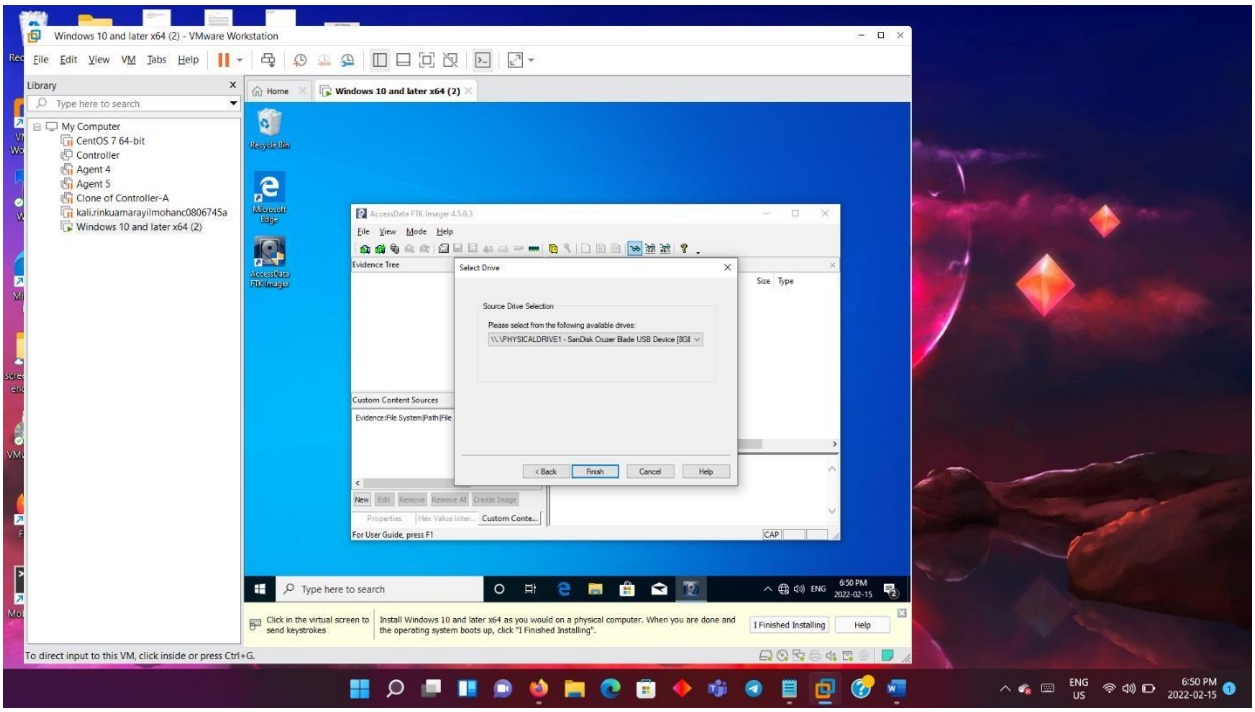
- Installed the file in the C drive.



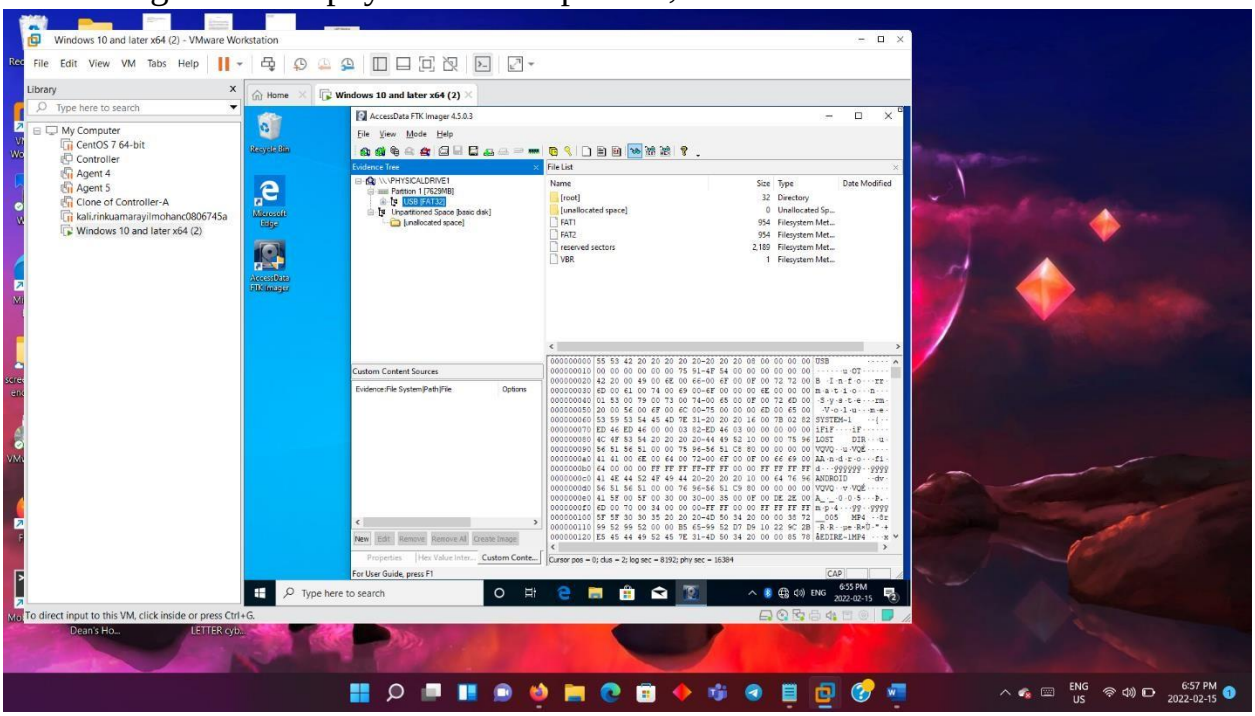
- Select File > Add evidence item



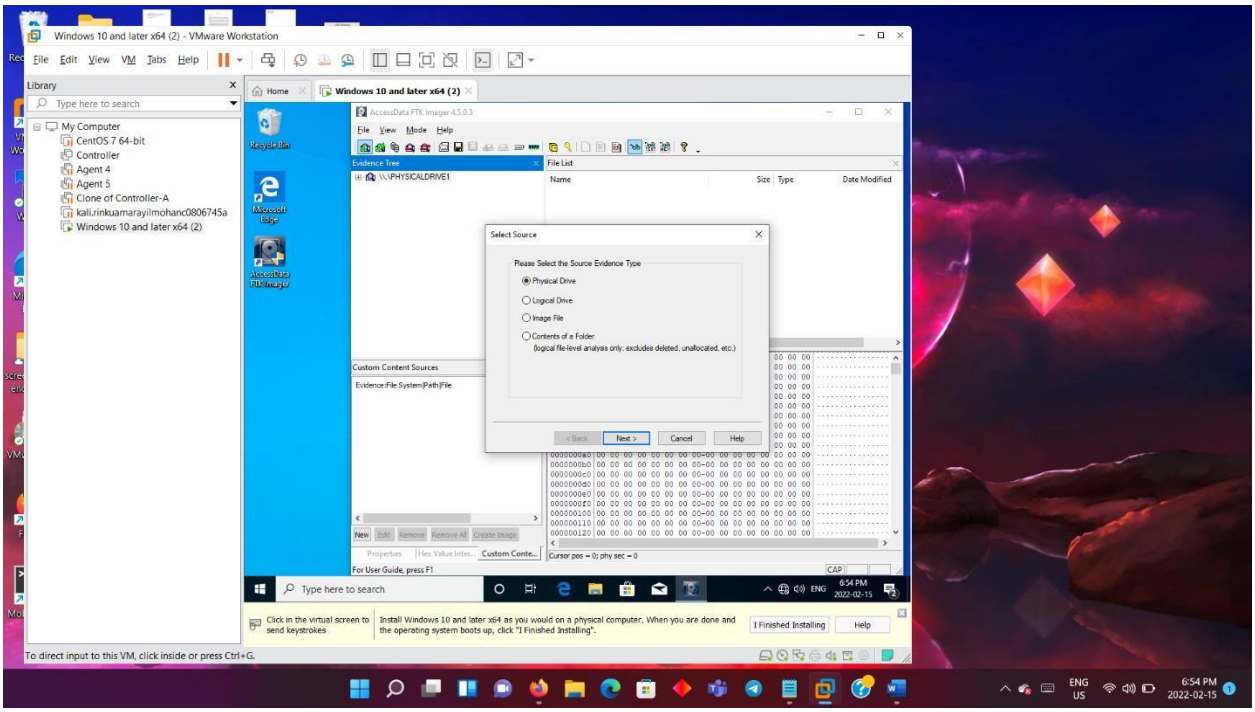
- Select Physical Drive and select next.



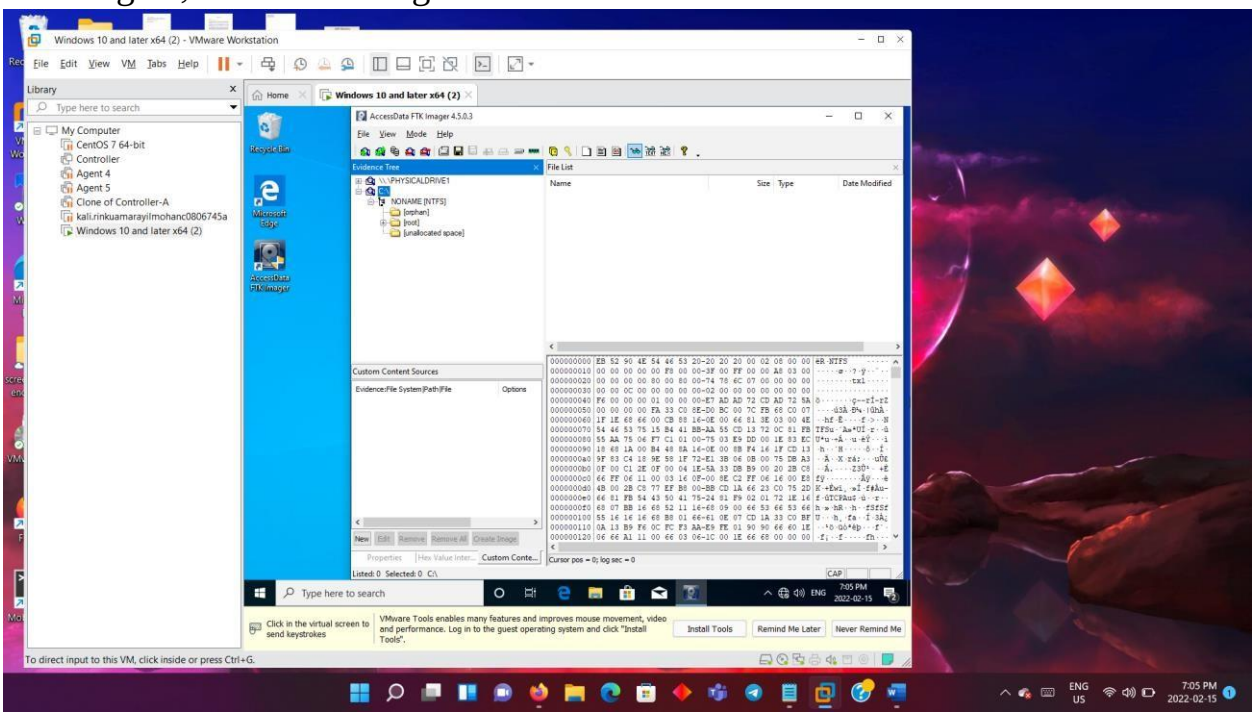
- We get a list of physical drives present, select one and click on finish.

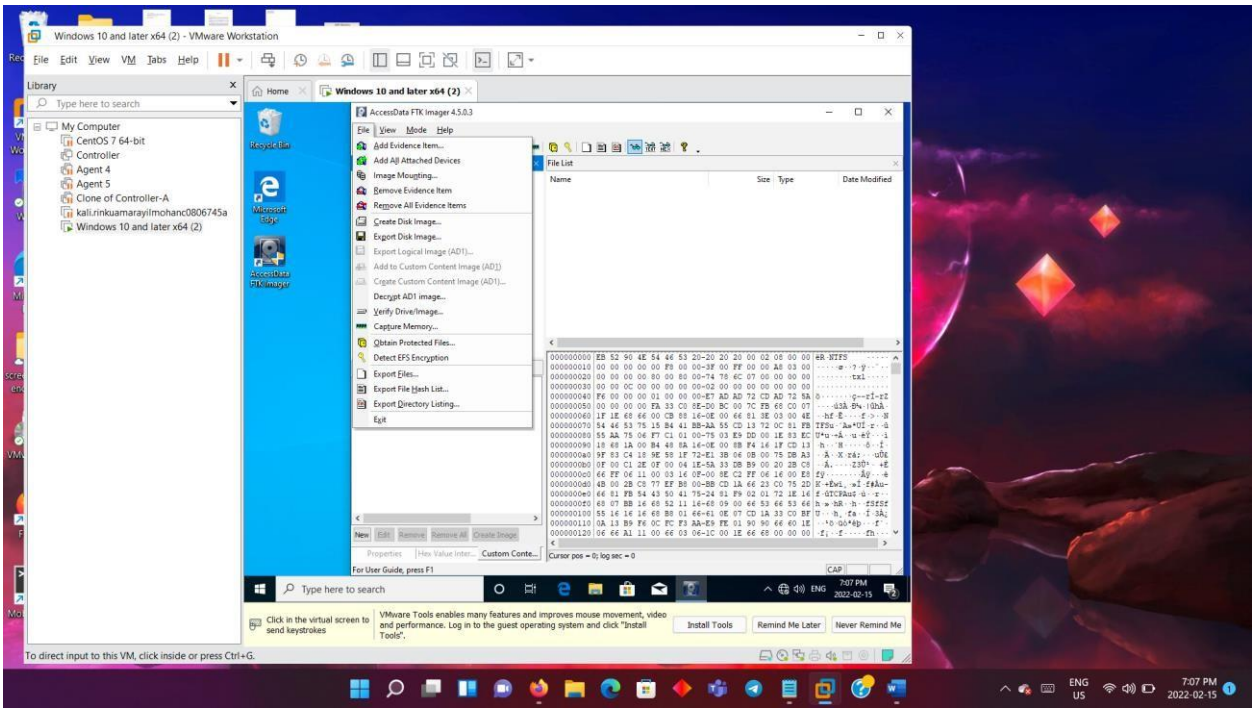


- We are able to expand all the subfolders and files present as shown in the picture above.

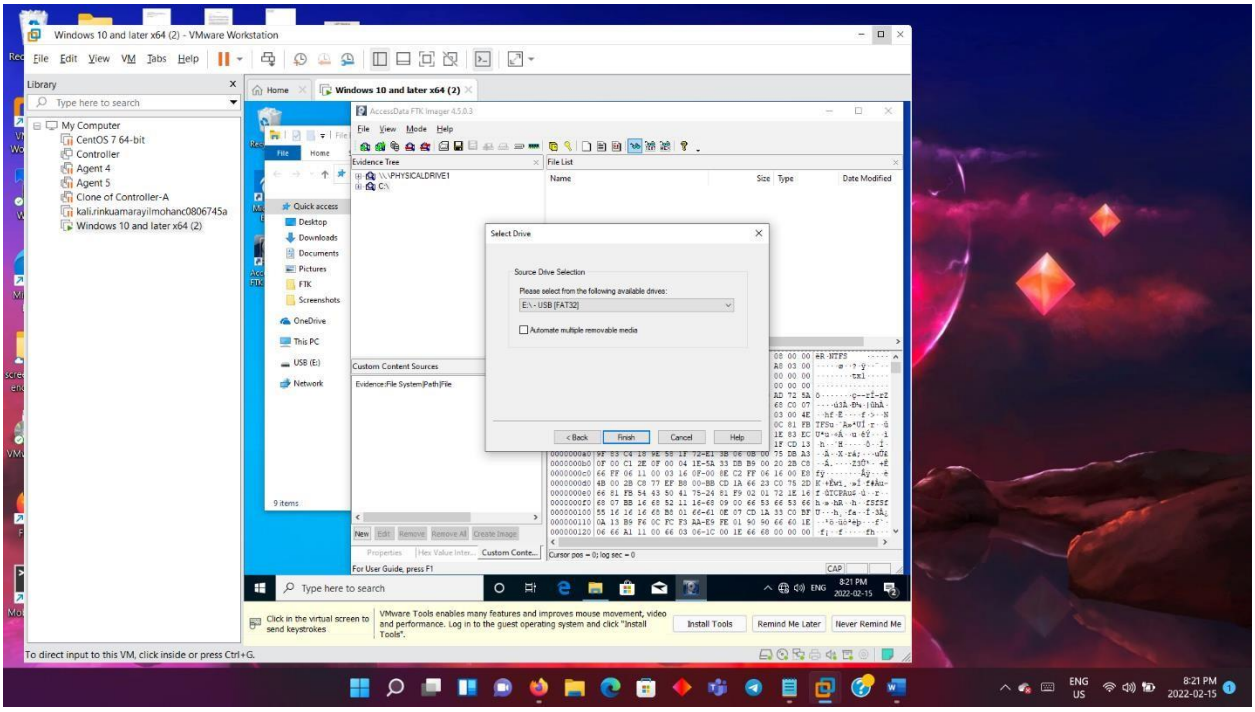


- Again, select file > logic drive this time.

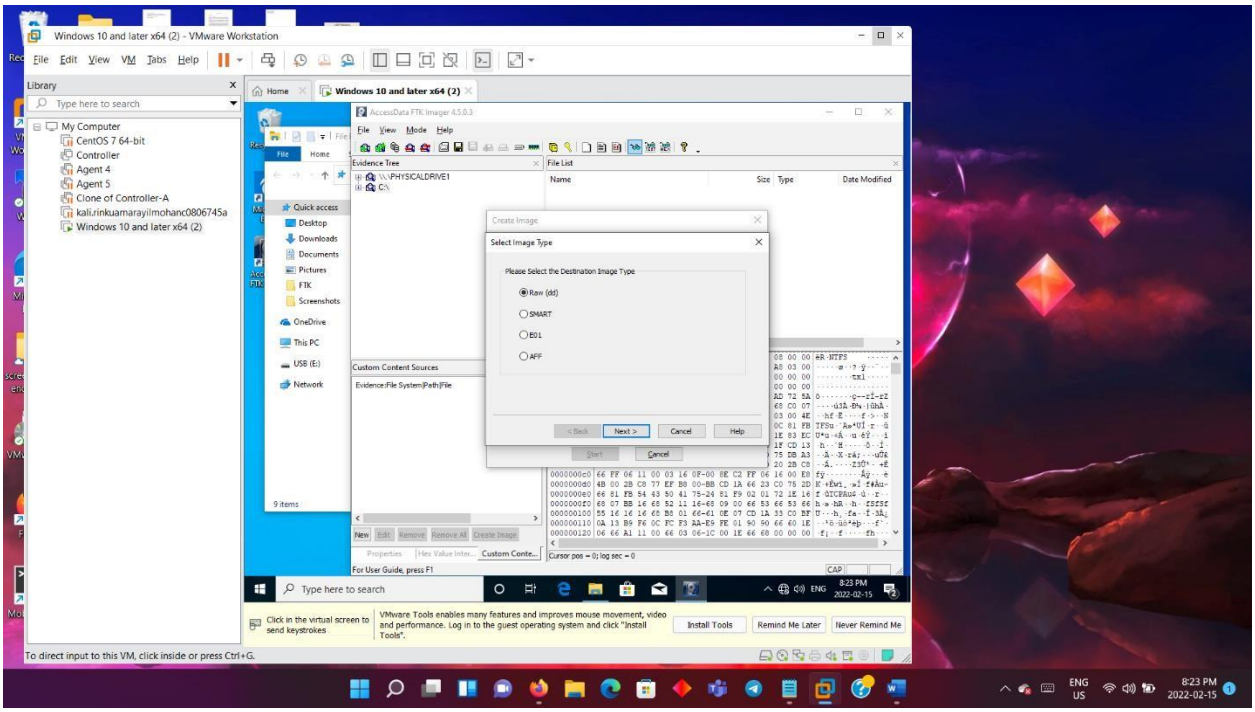




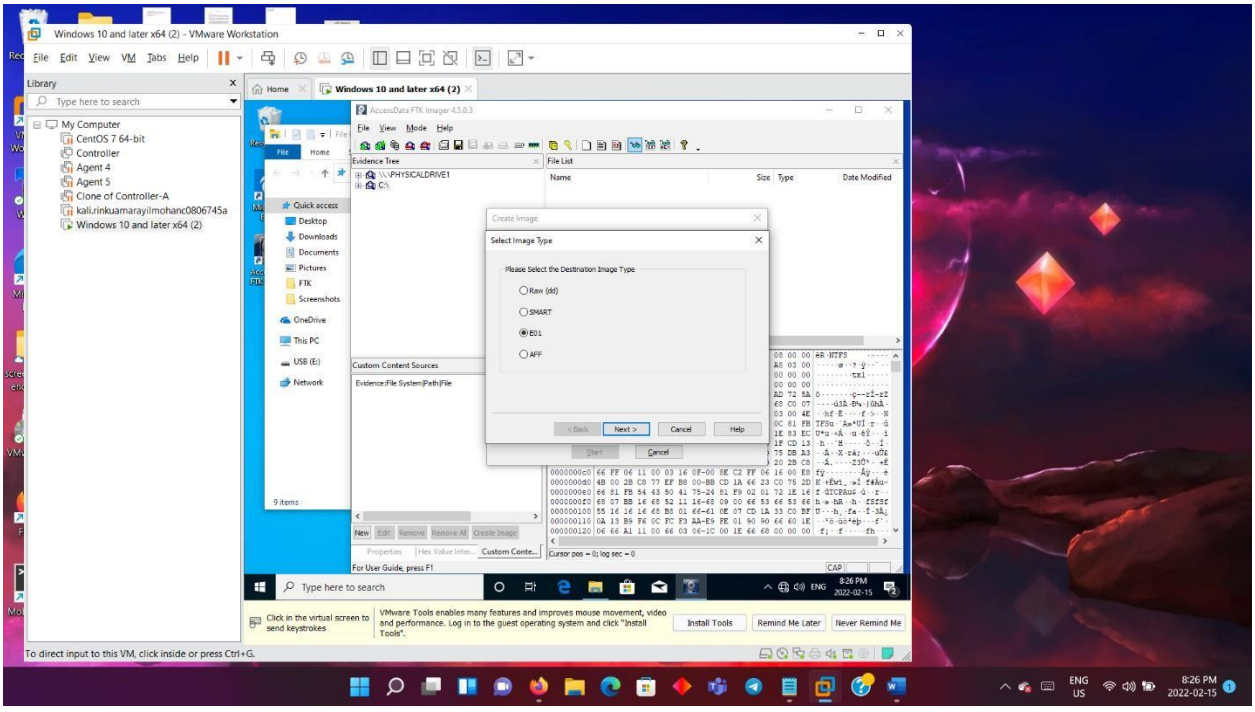
- To create a disk image, select File > Create Disk Image



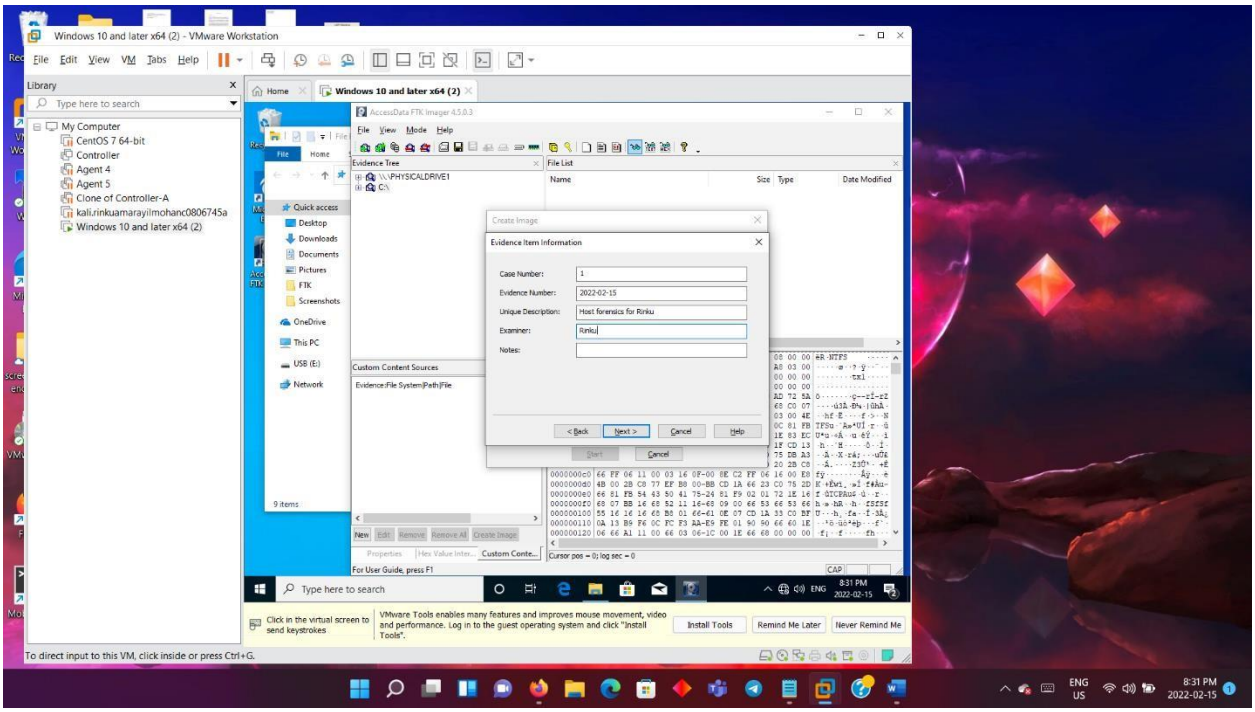
- Select logic drive>choose the USB drive



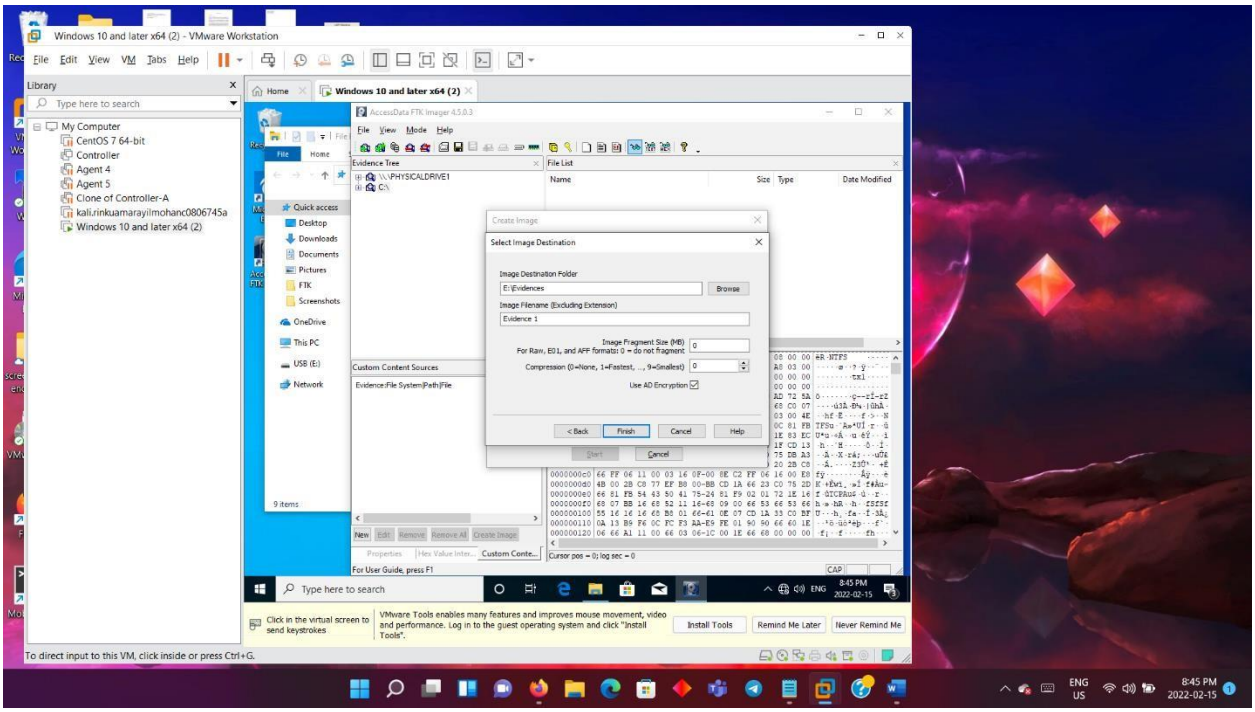
- Select image destination by selecting Add



- Select E01-compress the image file with MD5 hash

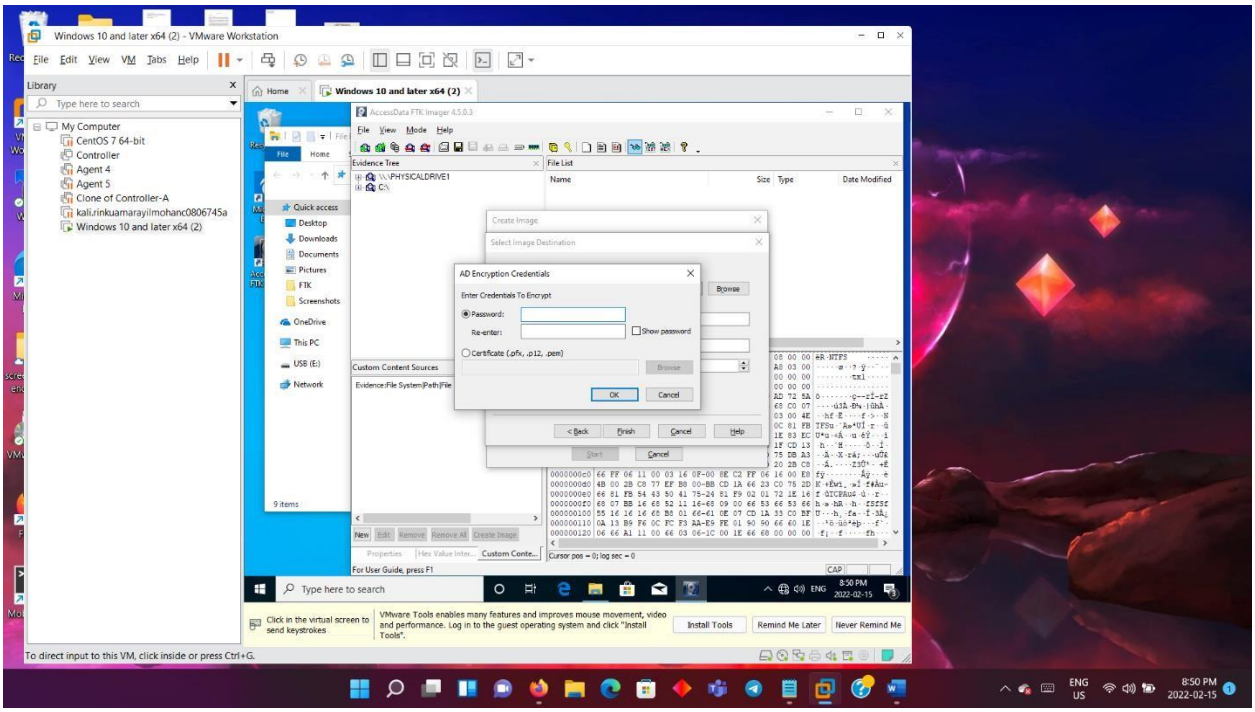


- Provide the evidence item information as shown above and select next.

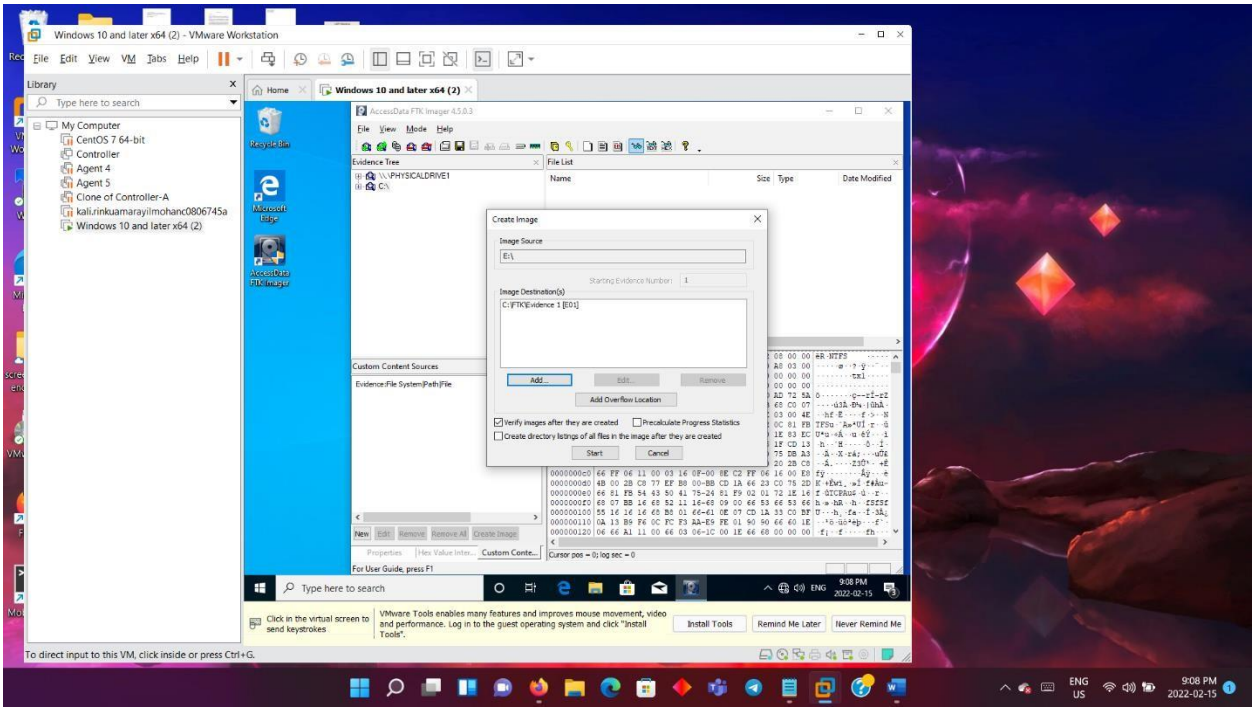


- Provide the destination folder and folder name, if we do not want fragmentation and want a single file, then change the value to 0.

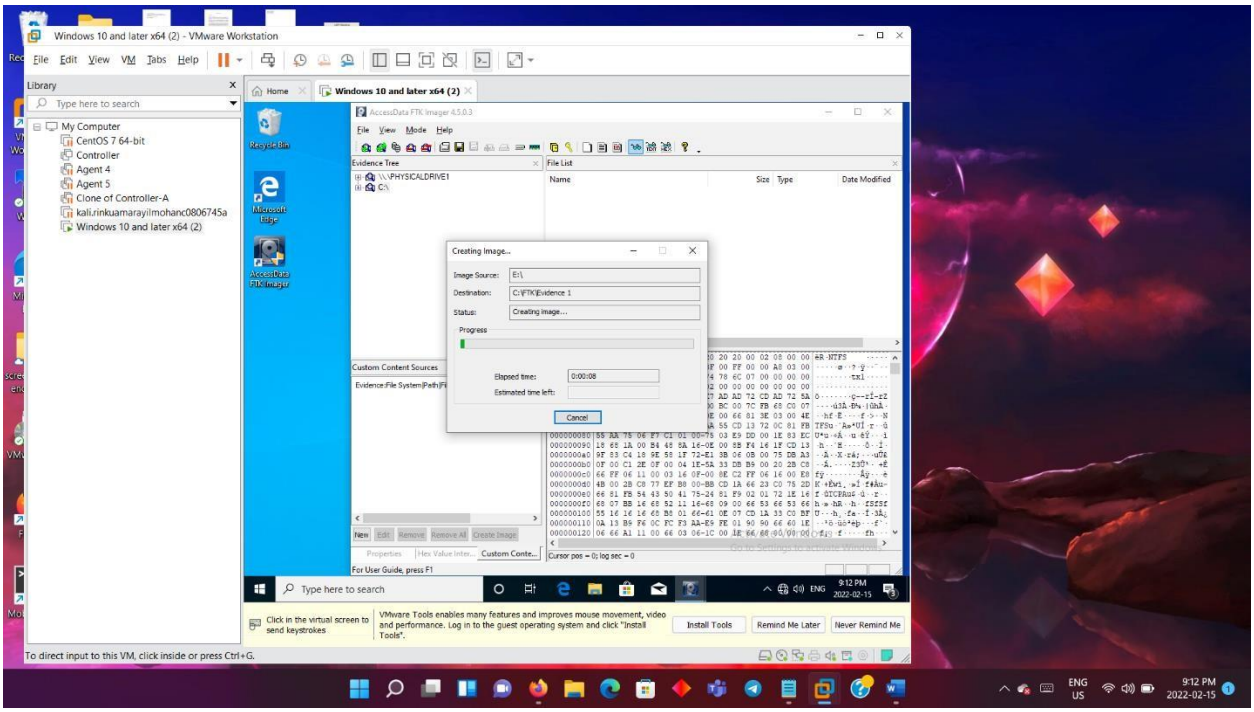
Encryption can be enabled if required. Select finish.

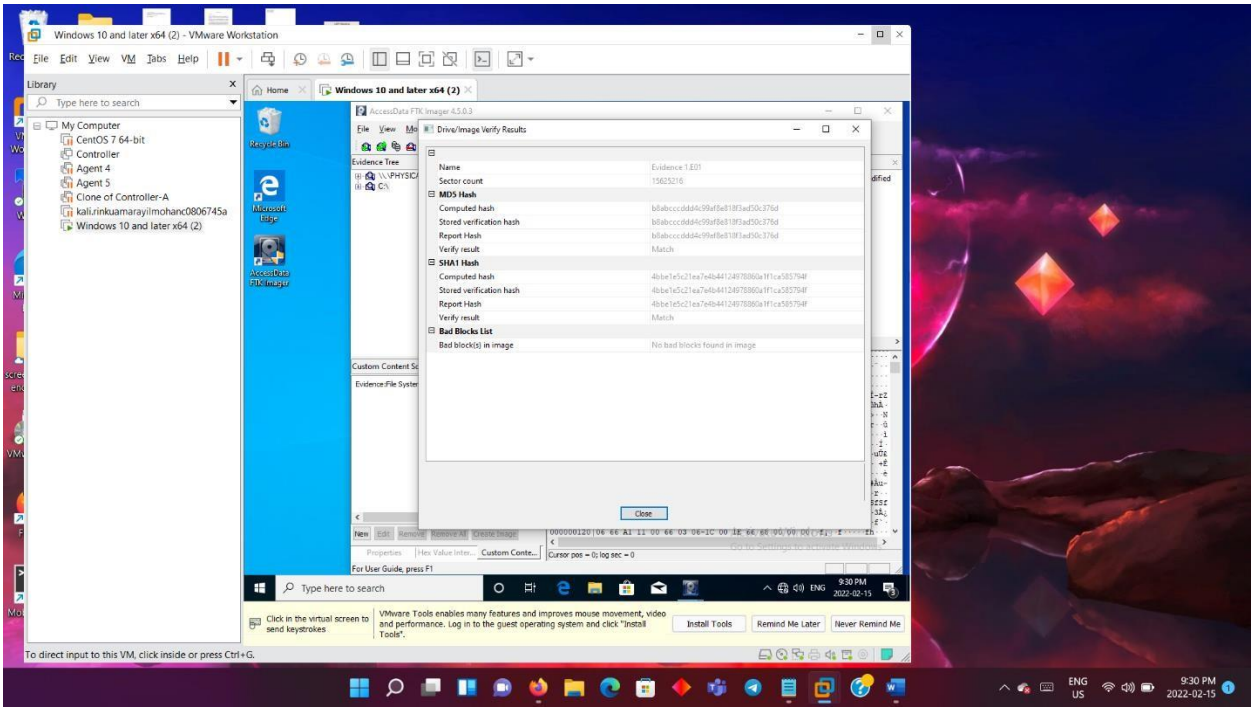


- Create password.

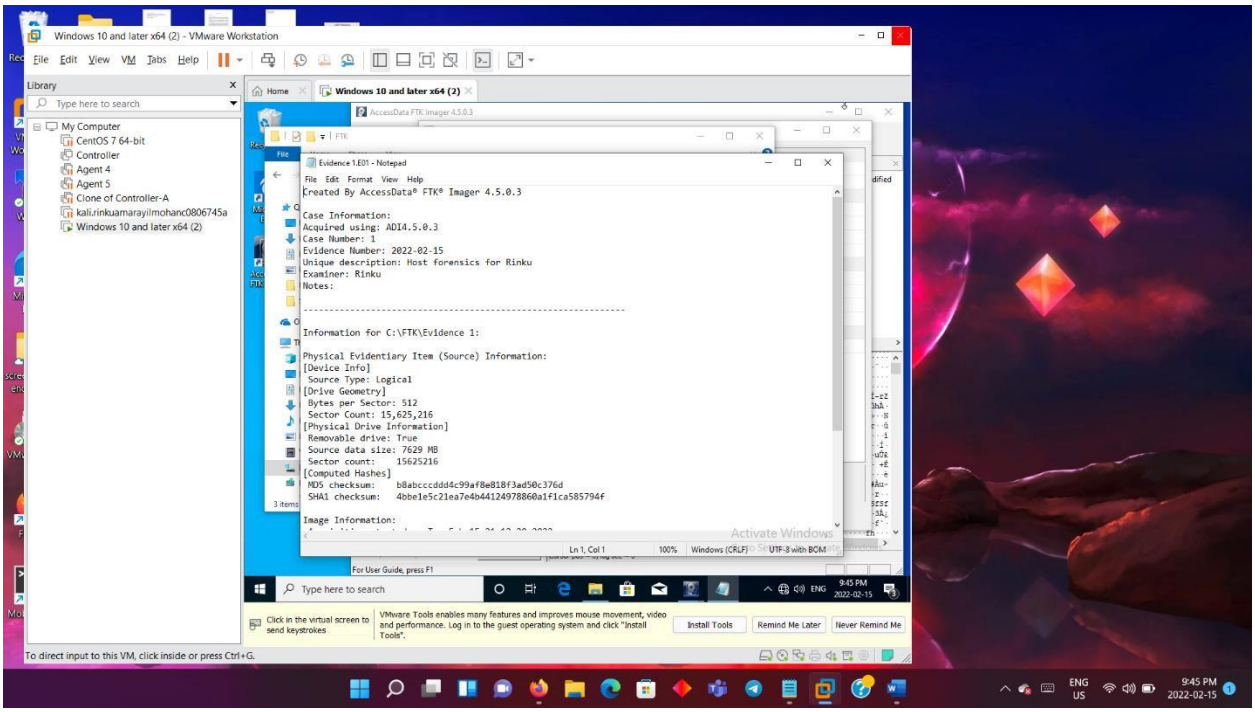


- Click on start. The process starts.

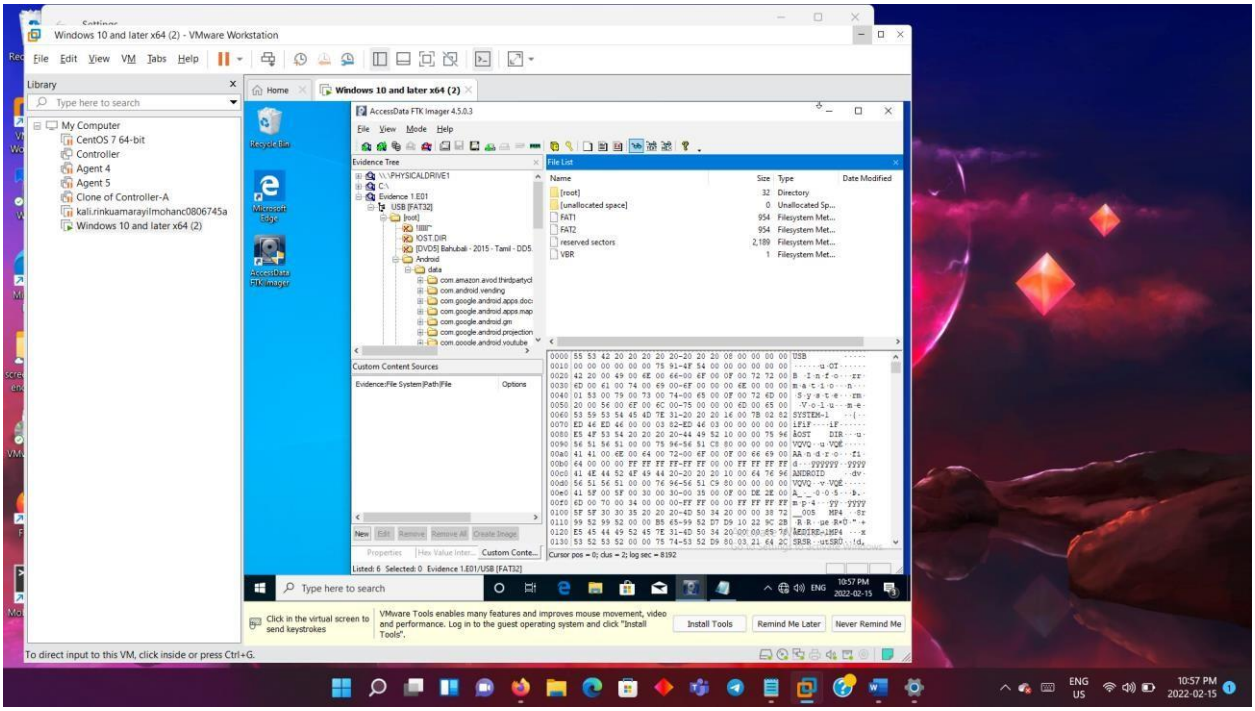




- The result displays MD5 hash, SHA1 hash, both of which shows match, which means there is no modification of data.



- Now we access the file path to check the data created. Open the notepad to get the details. It provides Case information.

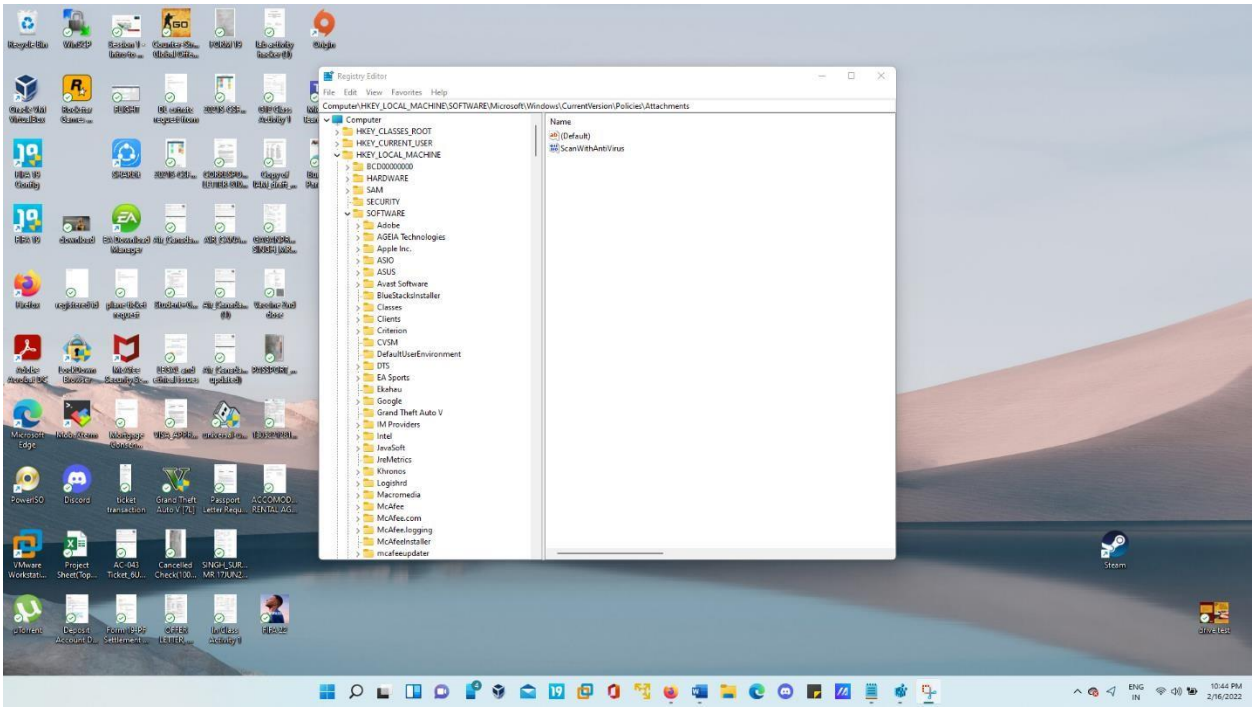


- We can also access the image file of this folder created. As shown above.

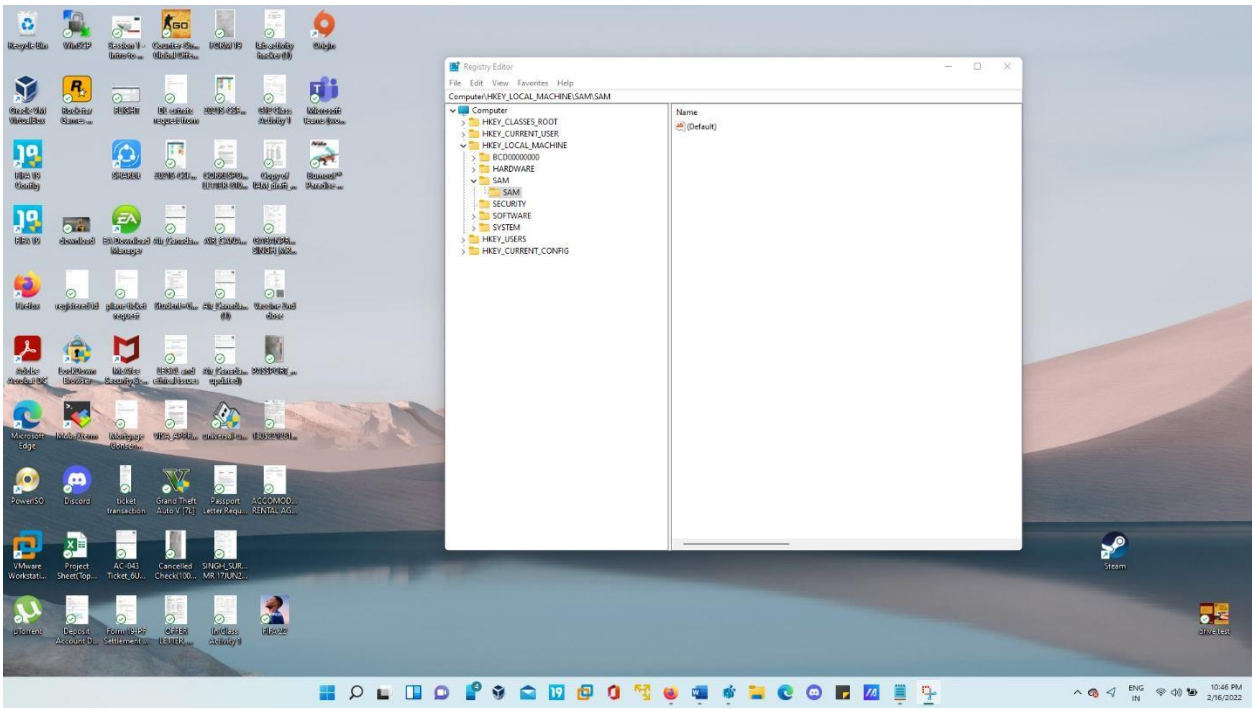
Part 1b

Host Forensic – Registry Analysis

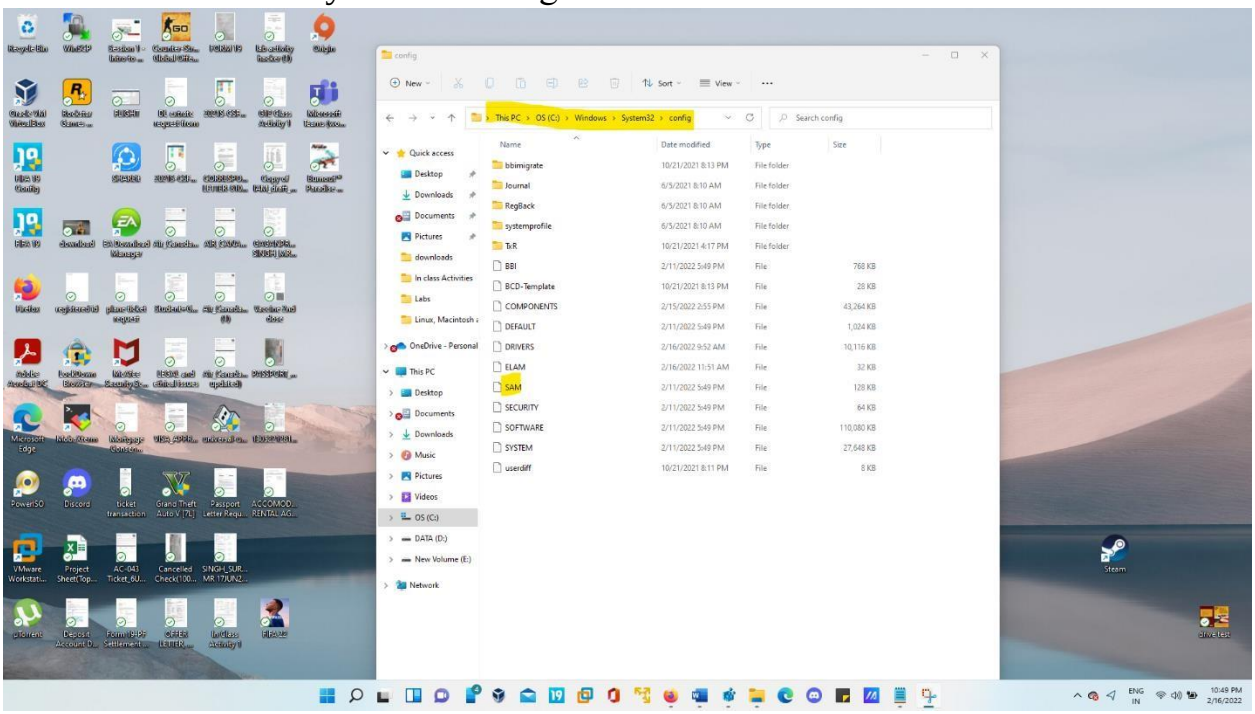
- Click on Windows icon and type registry editor to open it.



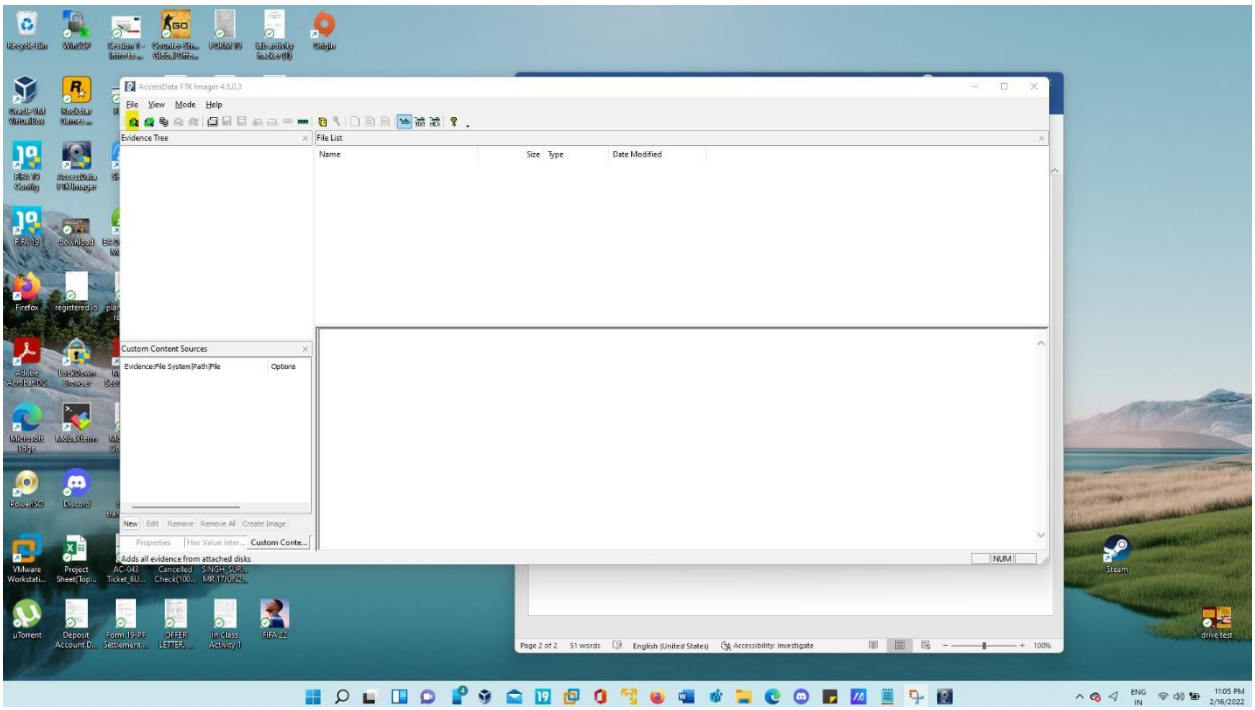
- Expand HKEY_LOCAL_MACHINE. Expand SAM. This SAM key hold user information.



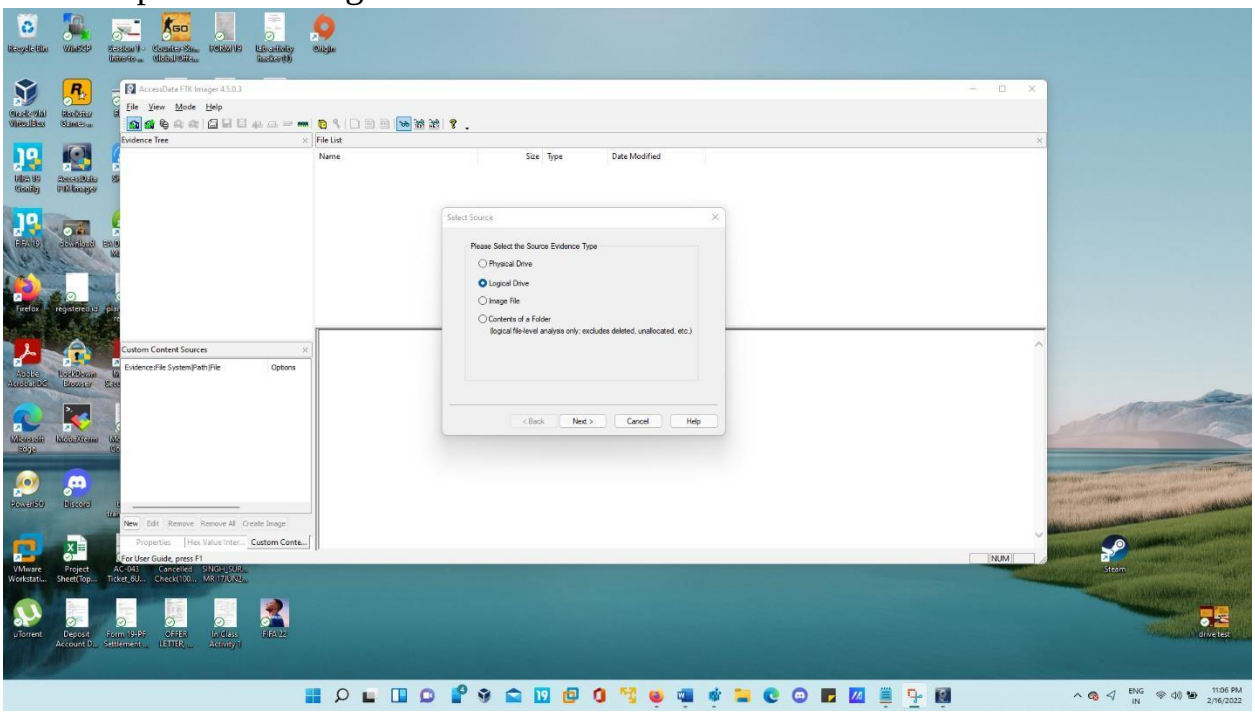
- Another way of finding SAM file is navigating to the location "C:\Windows\System32\config".

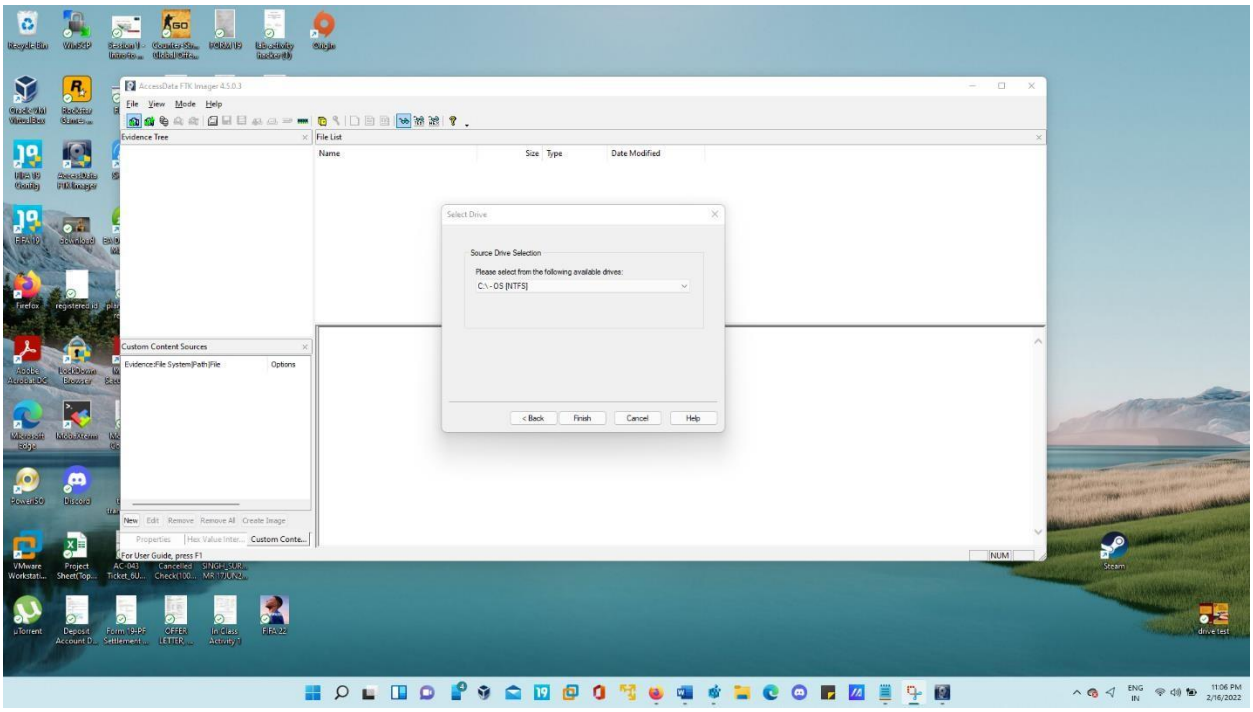


- Install and launch AccessData FTK imager application and click on add Evidence item.

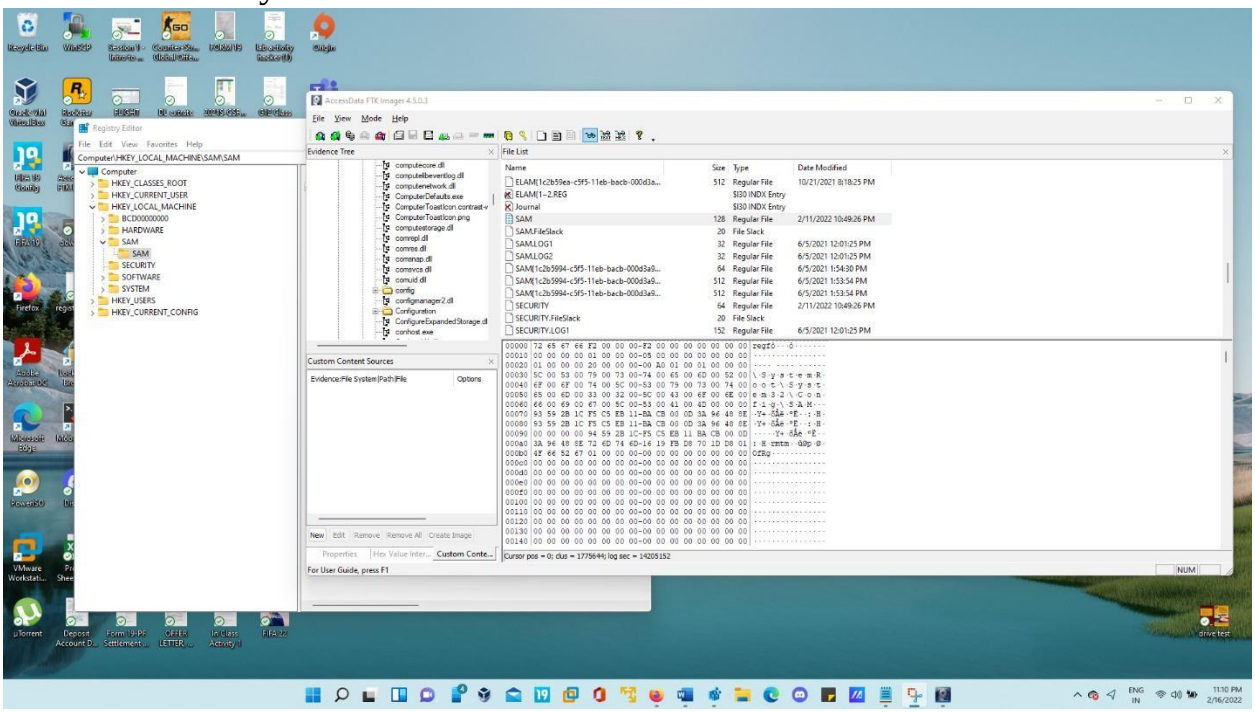


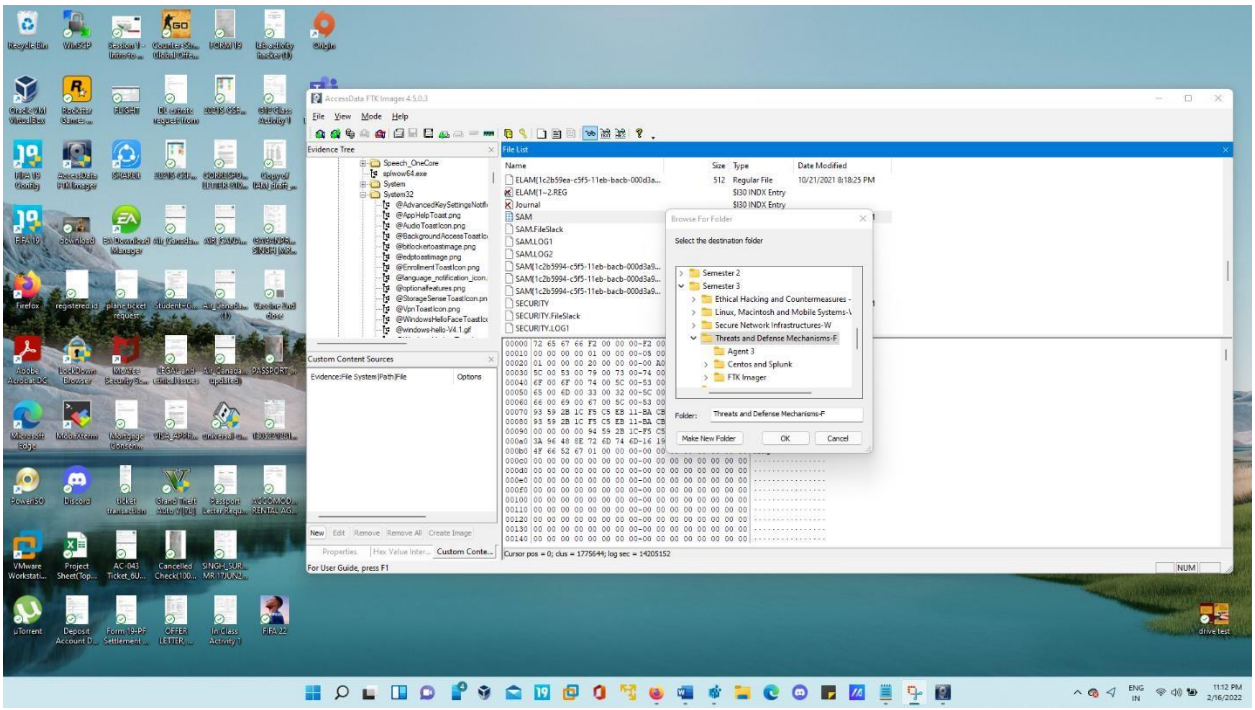
- Step 5: Select Logical drive and select C: and wait till it is loaded.



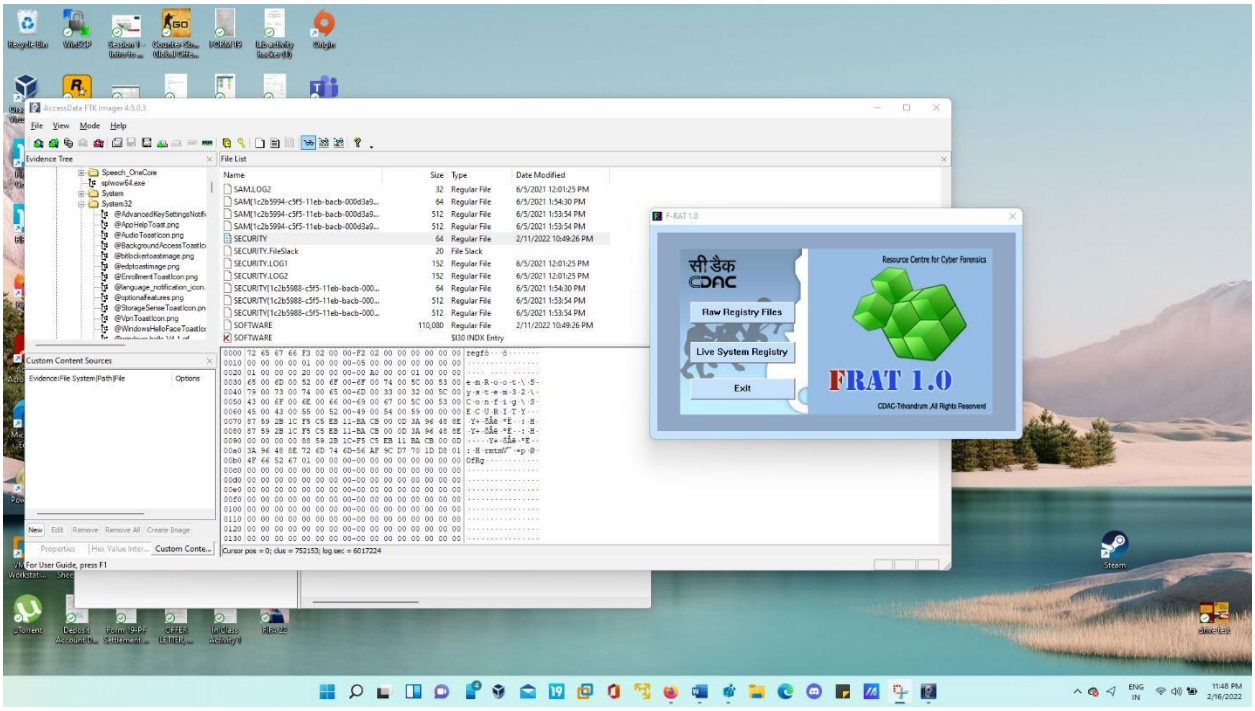


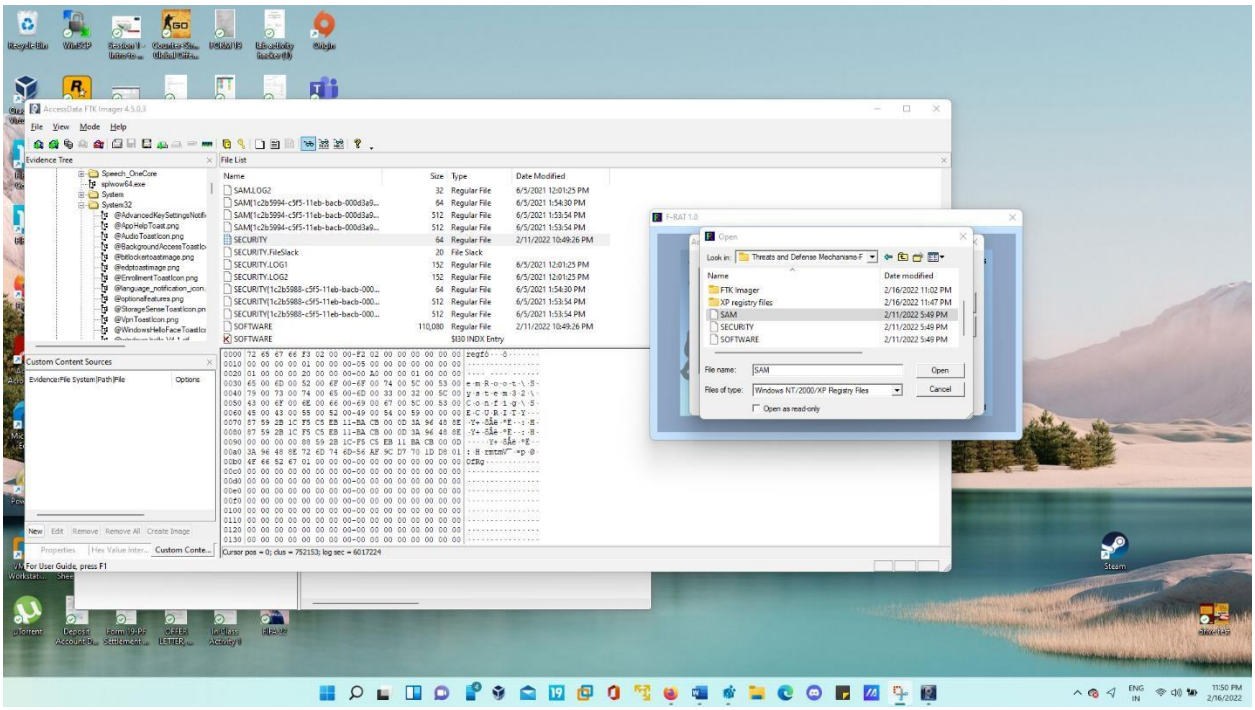
- Expand root->Windows->system32->SAM. Click and export SAM file to location of your choice.



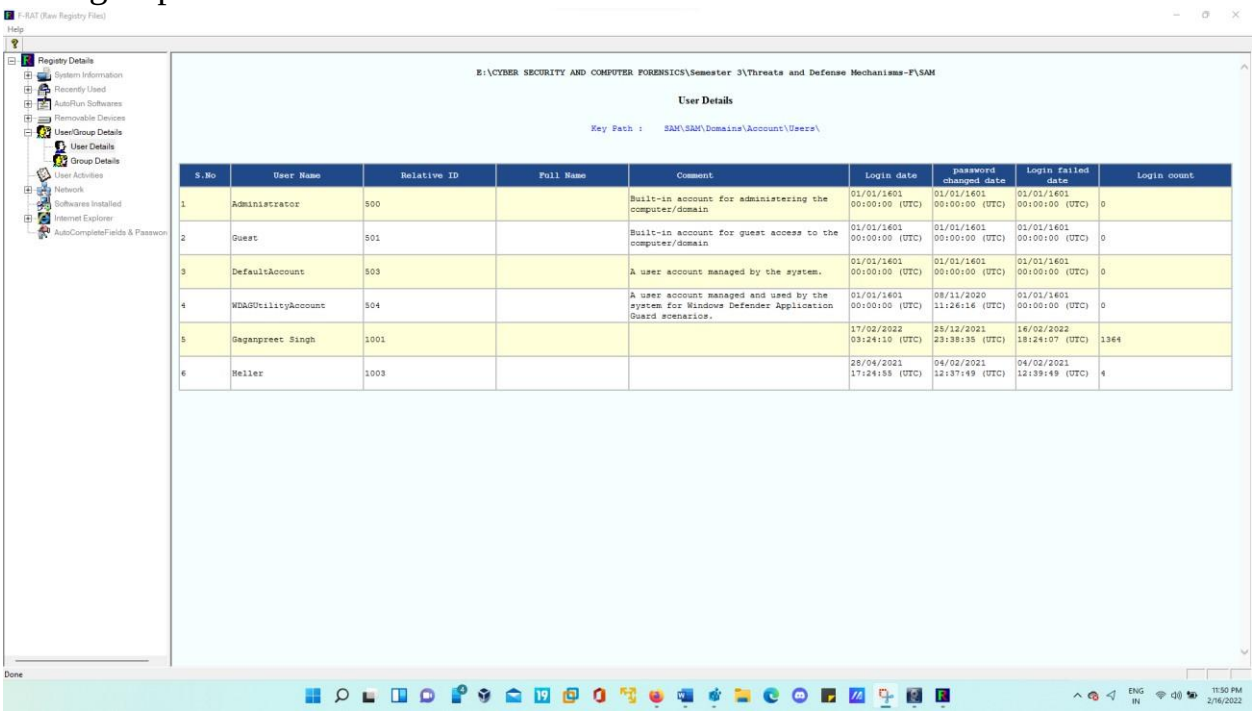


- Install F-RAT 1.0 from C-DAC(India) and open it. Click on Raw Registry files and add them.





- Expanding User/Group details will provide more details of users as well as group details.

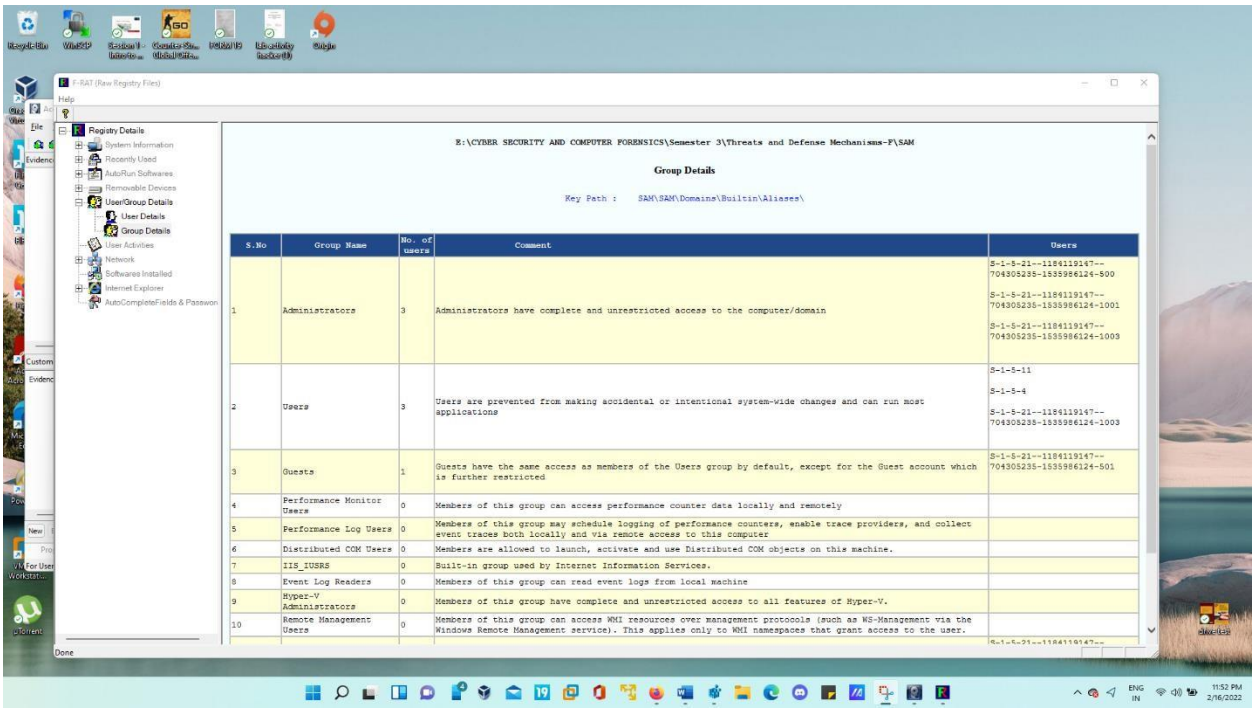


E:\CYBER SECURITY AND COMPUTER FORENSICS\Semester 3\Threats and Defense Mechanisms-F\SAM

User Details

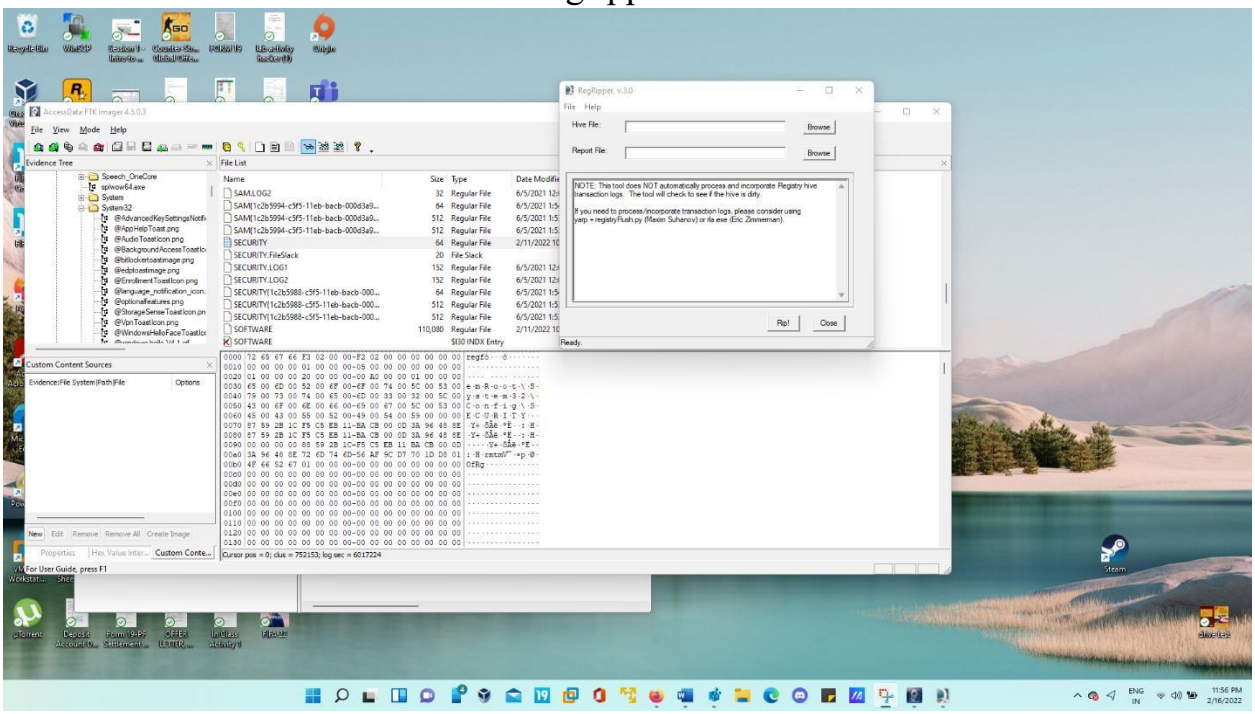
Key Path : SAM\SAM\Domains\Account\Users\

S.No	User Name	Relative ID	Full Name	Comment	Login date	password changed date	Login failed date	Login count
1	Administrator	500		Built-in account for administering the computer/domain	01/01/1601 00:00:00 (UTC)	01/01/1601 00:00:00 (UTC)	01/01/1601 00:00:00 (UTC)	0
2	Guest	501		Built-in account for guest access to the computer/domain	01/01/1601 00:00:00 (UTC)	01/01/1601 00:00:00 (UTC)	01/01/1601 00:00:00 (UTC)	0
3	DefaultAccount	503		A user account managed by the system.	01/01/1601 00:00:00 (UTC)	01/01/1601 00:00:00 (UTC)	01/01/1601 00:00:00 (UTC)	0
4	WDAGUtilityAccount	504		A user account managed and used by the system for Windows Defender Application Guard scenarios.	01/01/1601 00:00:00 (UTC)	08/11/2020 11:26:16 (UTC)	01/01/1601 00:00:00 (UTC)	0
5	Gaganpreet Singh	1001			17/02/2022 03:24:10 (UTC)	25/12/2021 23:38:35 (UTC)	16/02/2022 18:24:07 (UTC)	1364
6	Heller	1003			28/04/2021 17:24:55 (UTC)	04/02/2021 12:37:49 (UTC)	04/02/2021 12:39:49 (UTC)	4

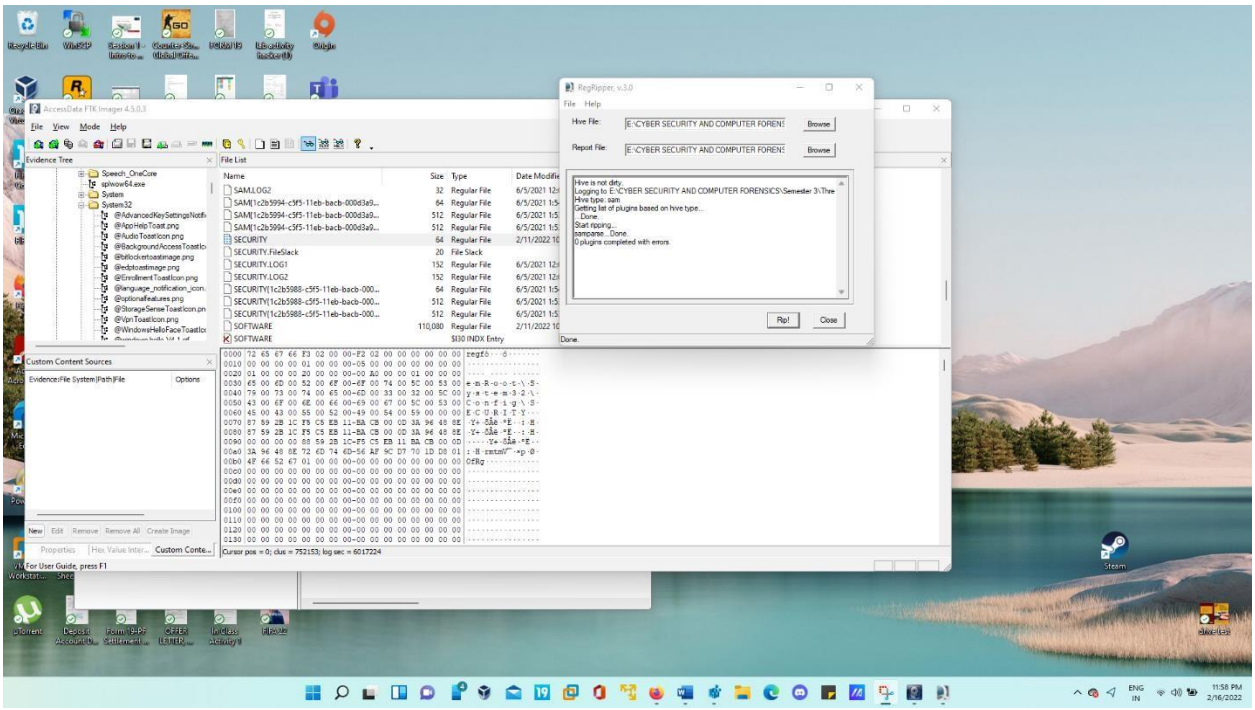


S.No	Group Name	No. of users	Comment	Users
1	Administrators	3	Administrators have complete and unrestricted access to the computer/domain	S-1-5-21--1184119147--704305235-1535986124-500 S-1-5-21--1184119147--704305235-1535986124-1001 S-1-5-21--1184119147--704305235-1535986124-1003
2	Users	3	Users are prevented from making accidental or intentional system-wide changes and can run most applications	S-1-5-11 S-1-5-4 S-1-5-21--1184119147--704305235-1535986124-1003
3	Guests	1	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted	S-1-5-21--1184119147--704305235-1535986124-501
4	Performance Monitor Users	0	Members of this group can access performance counter data locally and remotely	
5	Performance Log Users	0	Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via remote access to this computer	
6	Distributed COM Users	0	Members are allowed to launch, activate and use Distributed COM objects on this machine.	
7	IIS_IUSRS	0	Built-in group used by Internet Information Services.	
8	Event Log Readers	0	Members of this group can read event logs from local machine	
9	Hyper-V Administrators	0	Members of this group have complete and unrestricted access to all features of Hyper-V.	
10	Remote Management Users	0	Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user.	

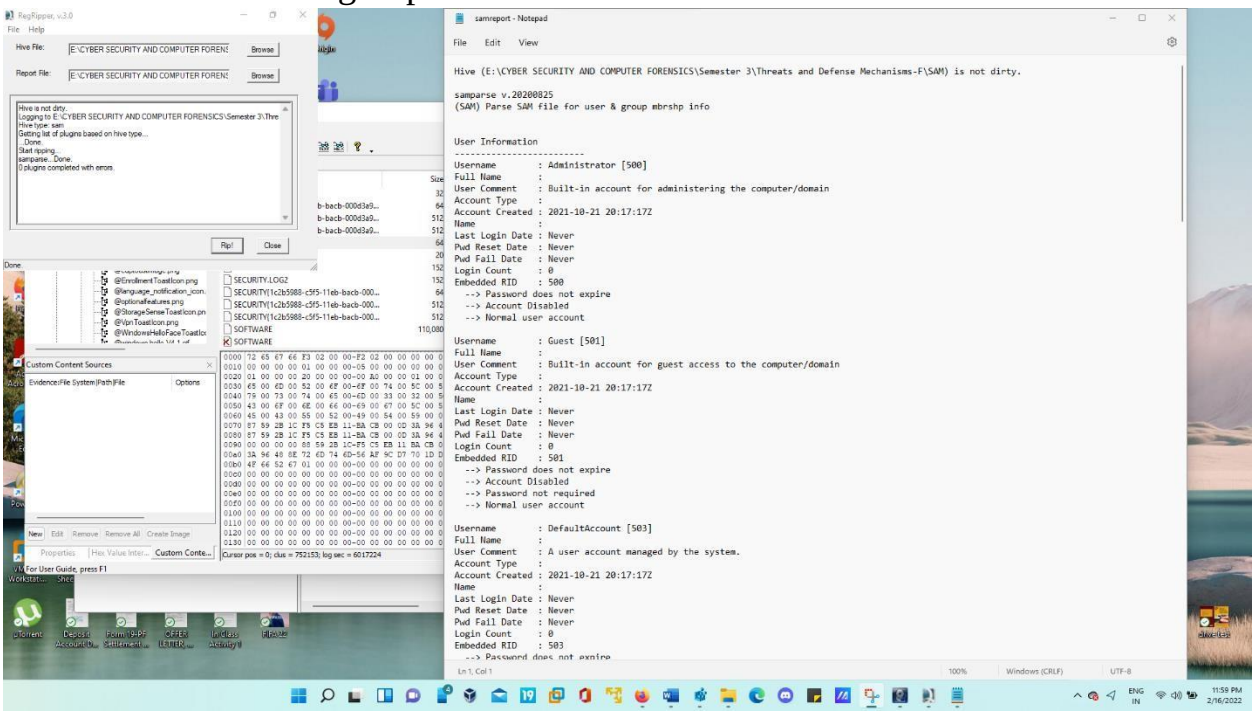
- Now we will run tool name “Regripper”.



- Choose SAM file and create a report.



- Open the report file and it will provide more details regarding user information and group information.

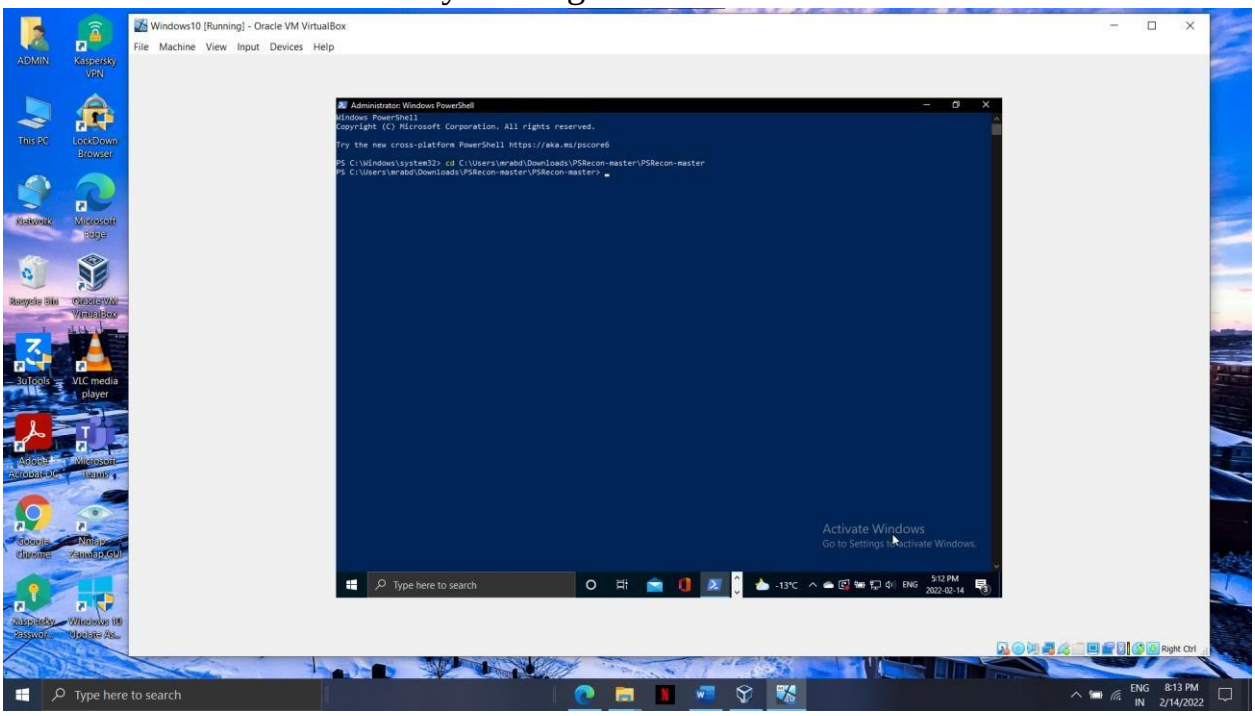


.

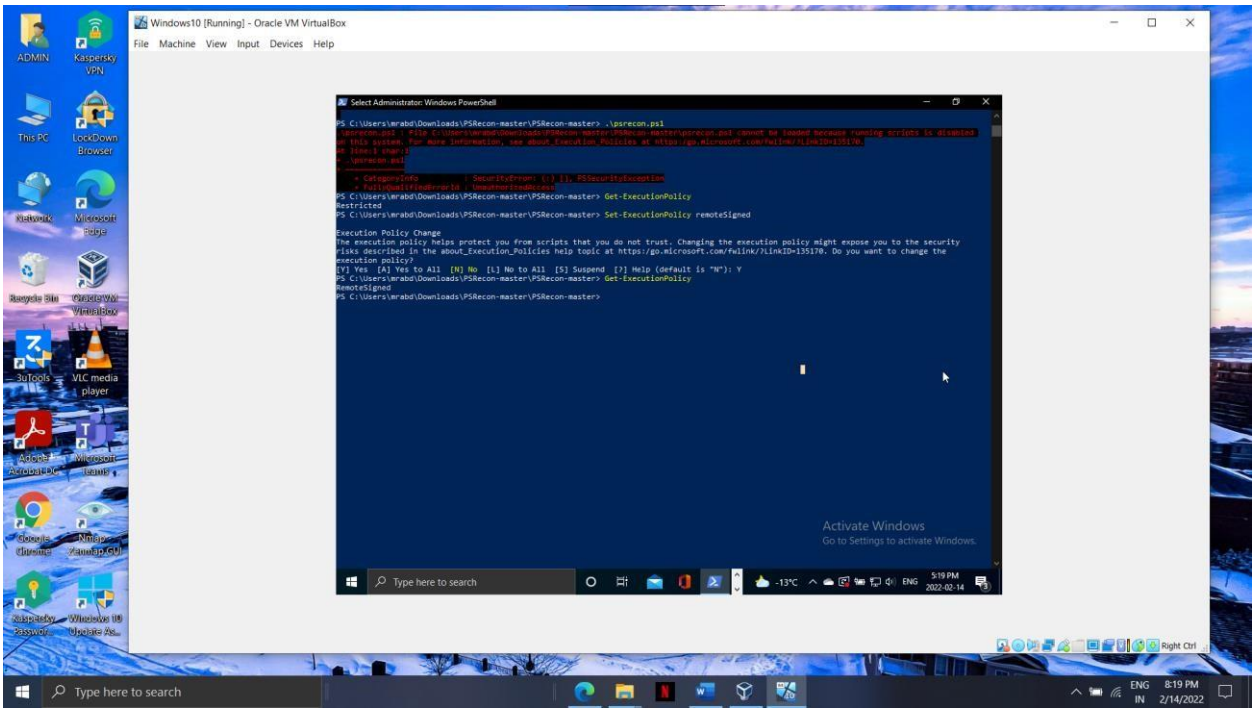
Part 1c

Host Forensic - PSRECON

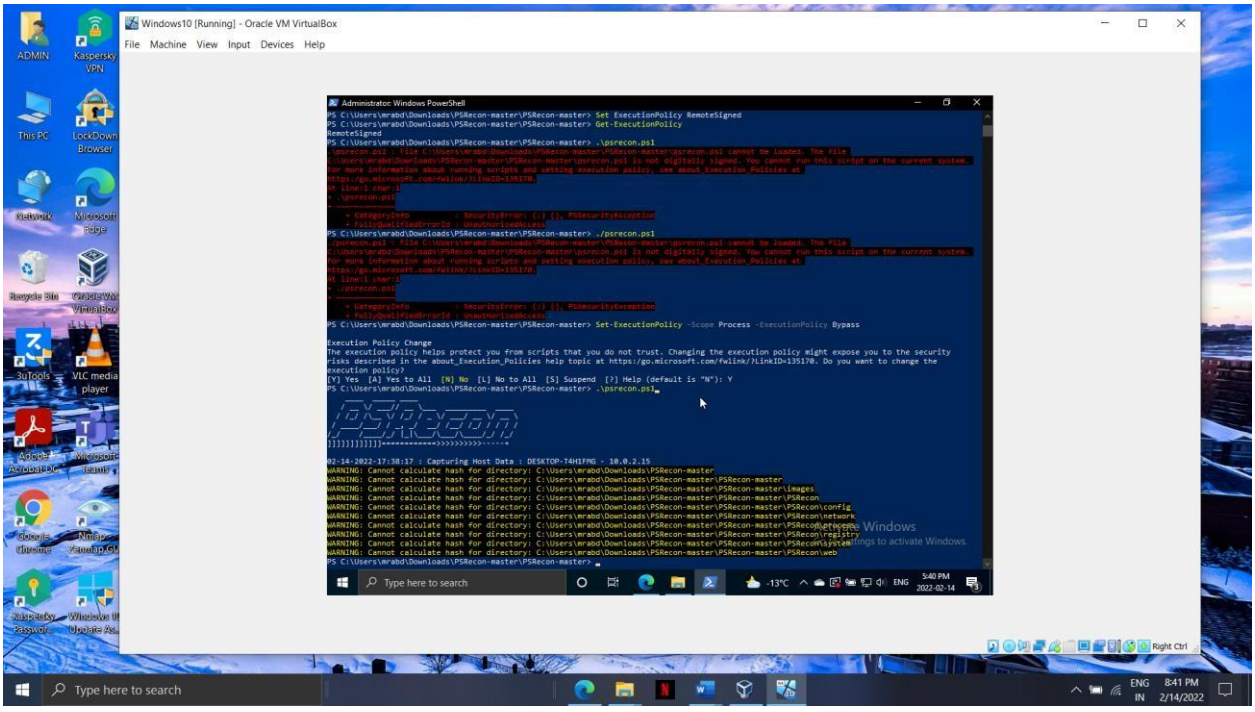
- First download the Zip file from GitHub. Then extract and navigate it in Windows PowerShell by running it in Administrator mode.



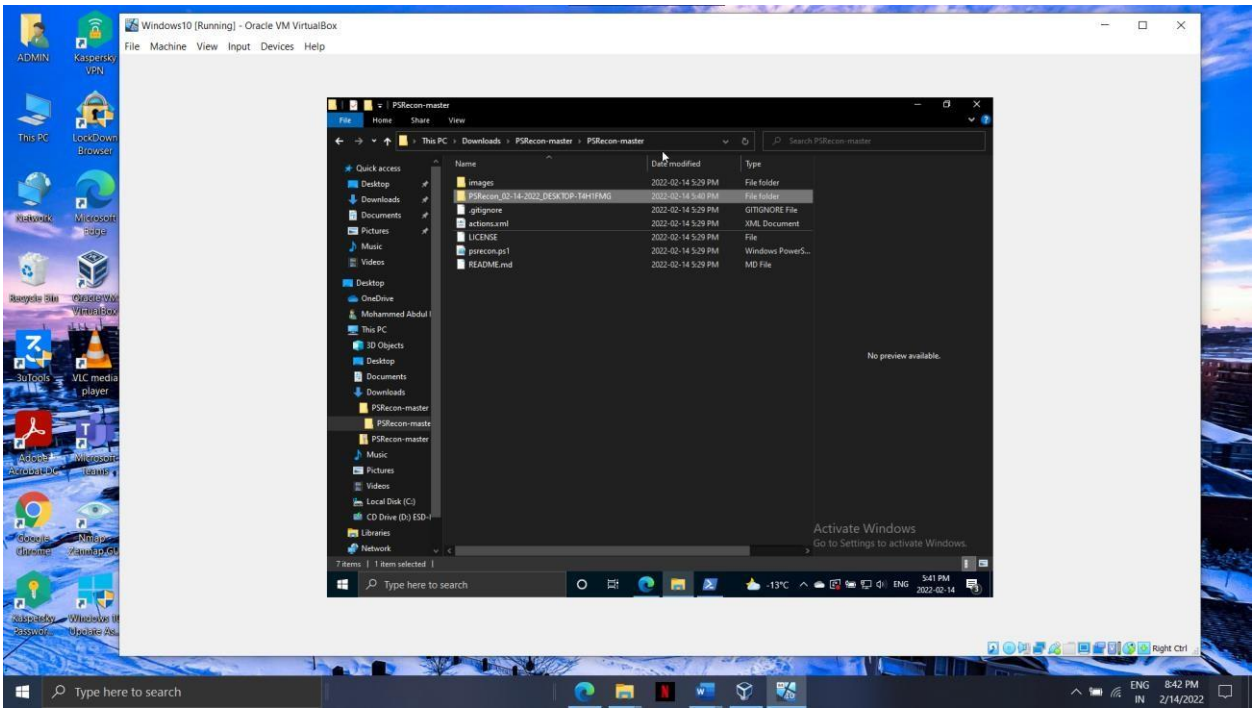
- Changing the execution policy



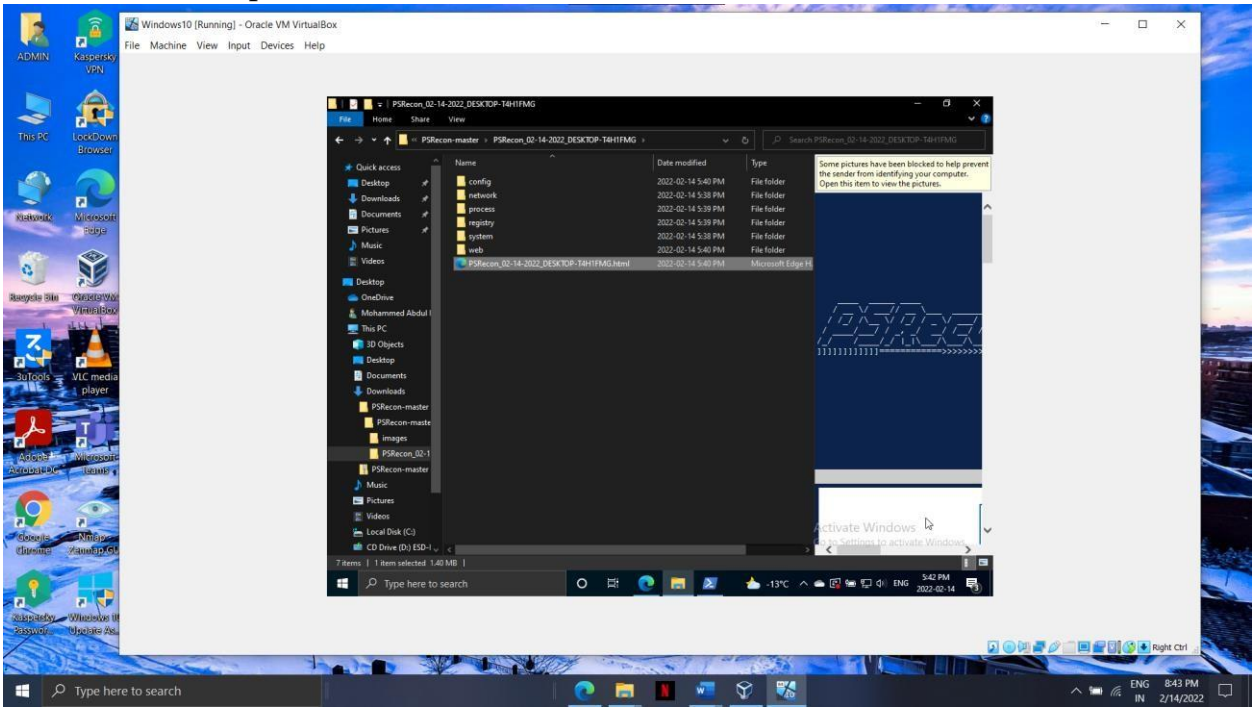
- PSRecon is running and capturing data

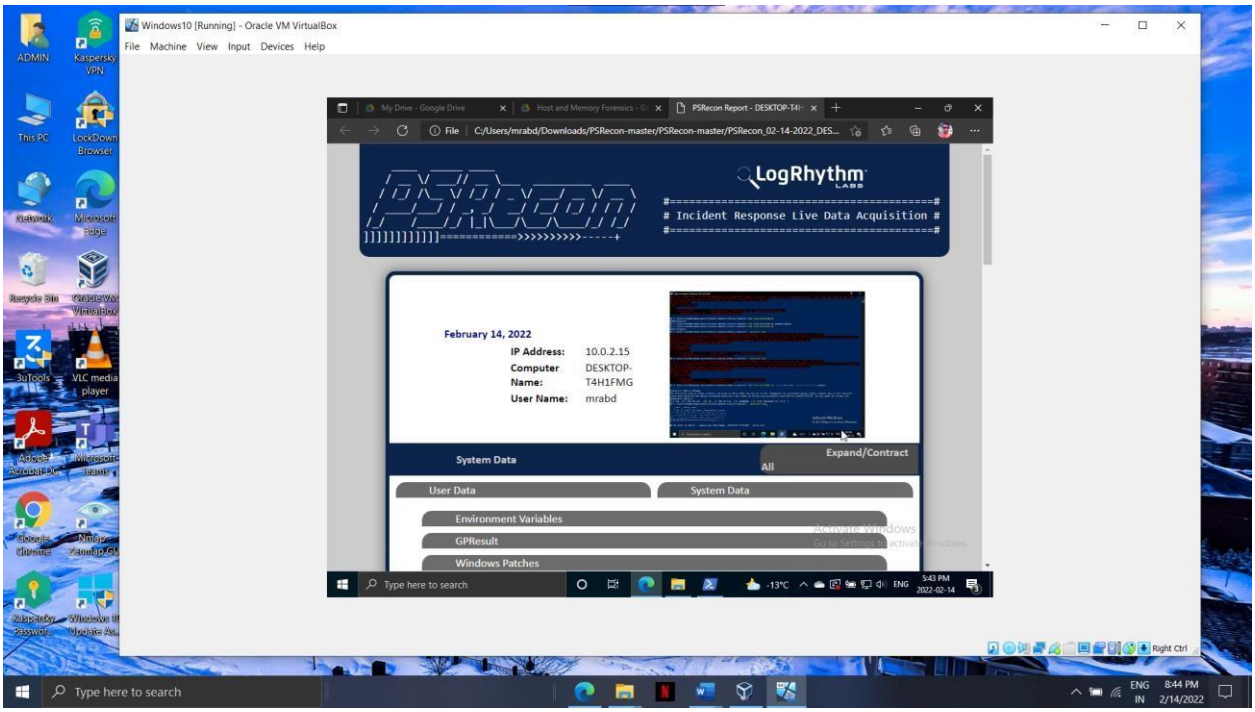


- File created by PSRecon



- We shall open this file to view detailed information

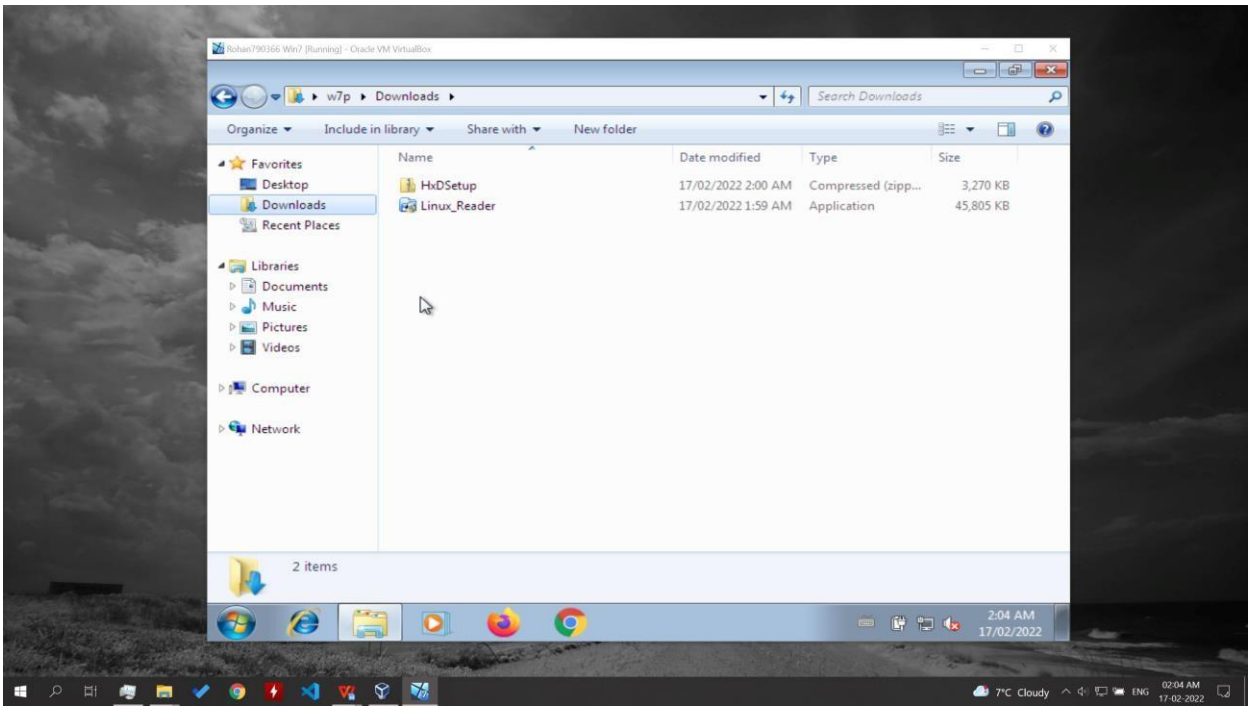




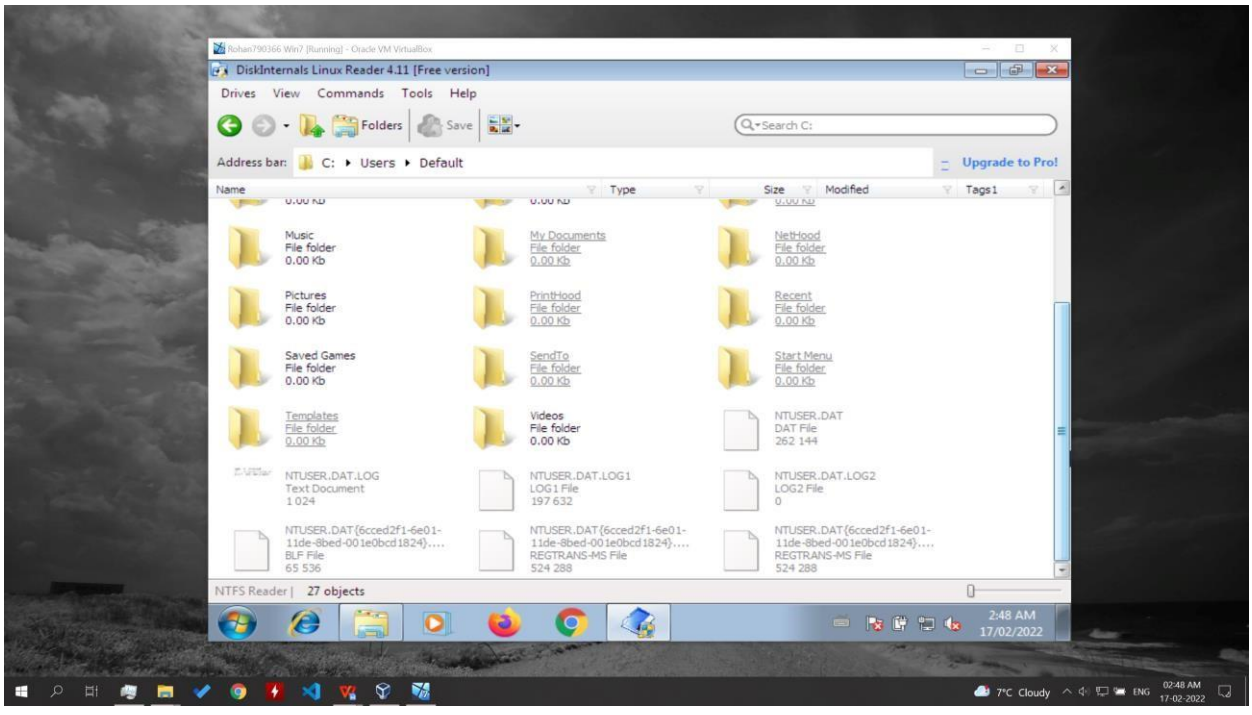
Part 1d

Host Forensic NTUSER.DAT

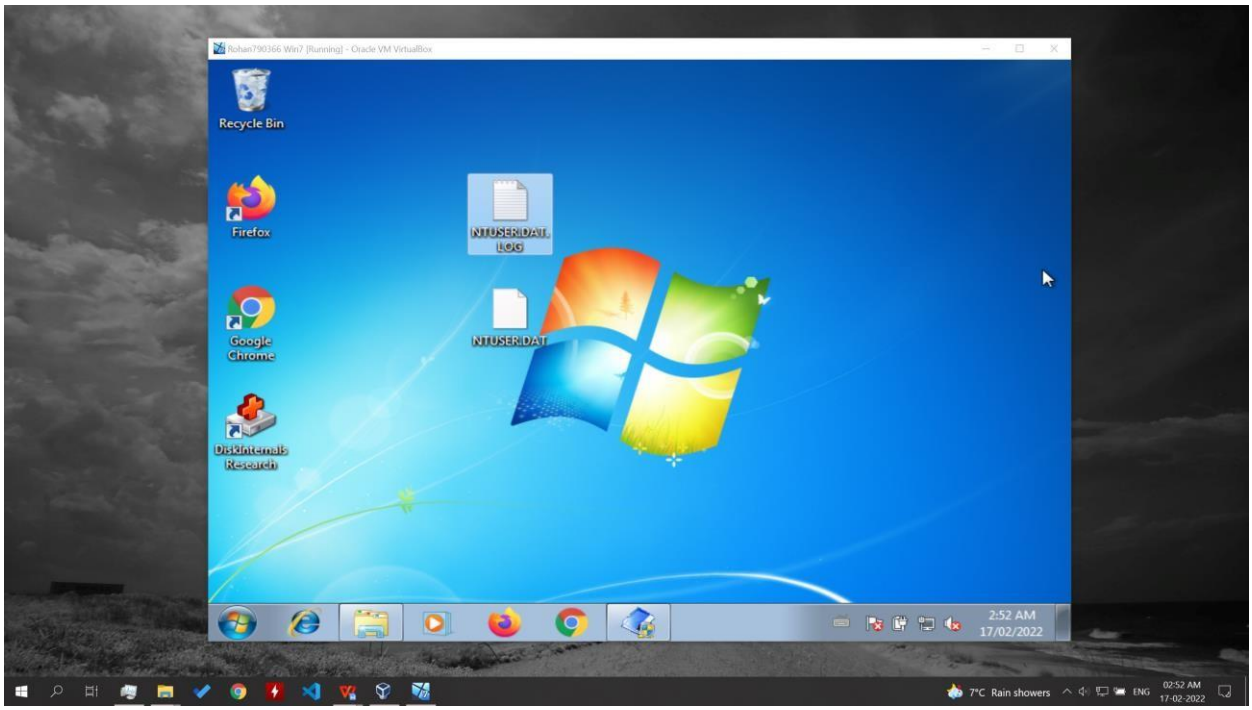
- Install HxD and Linux Reader (Disk Internal Linux Reader)



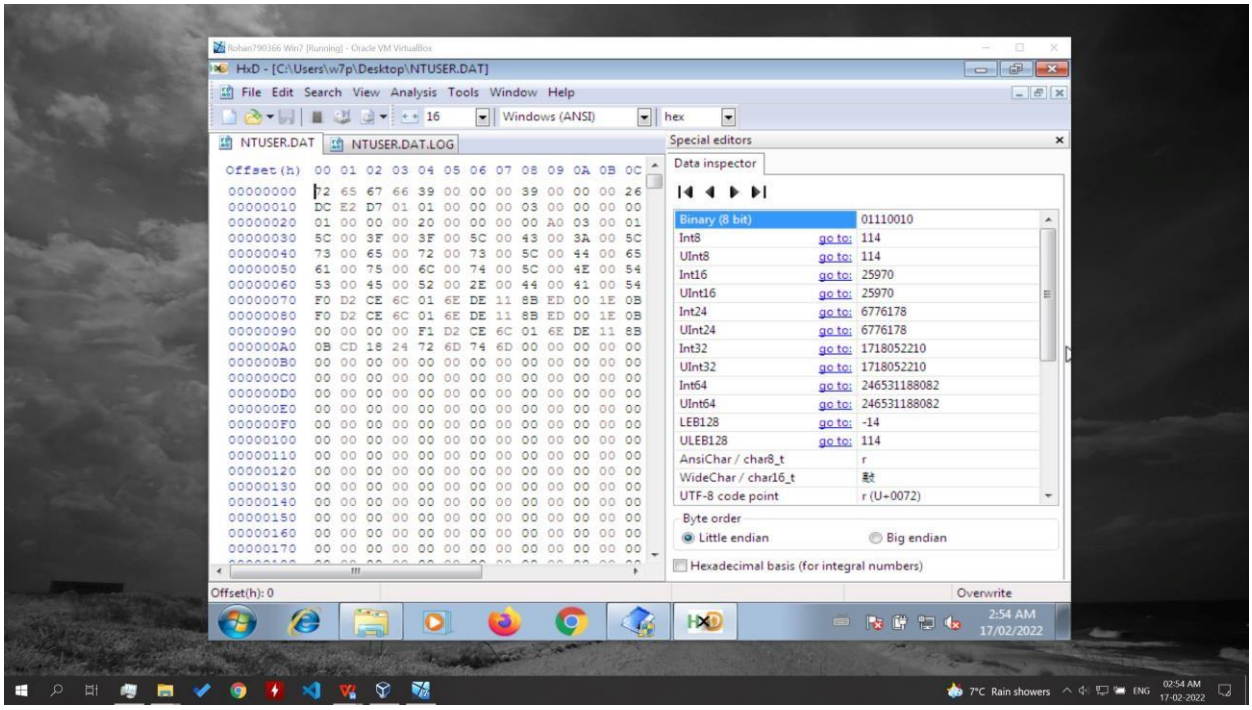
- Use Linux Read to find NTUSER.DAT and NTUSER.LOG (under C -users -defaults)



- Save them in your desktop



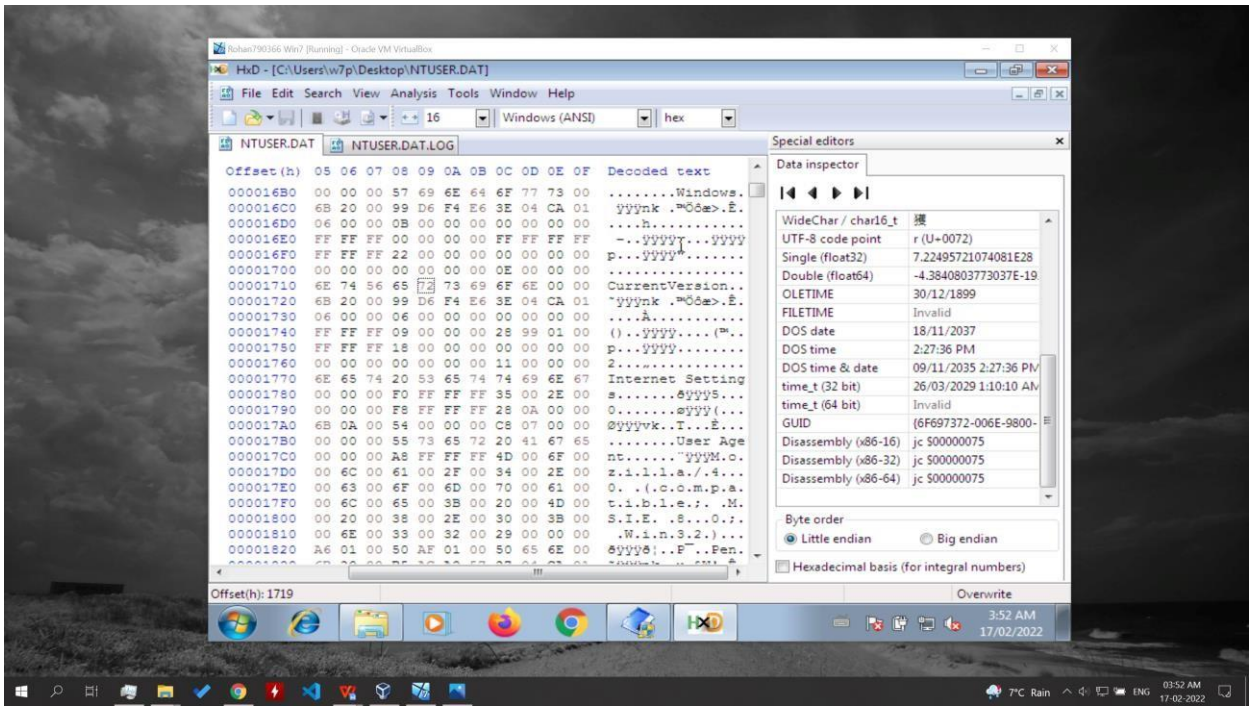
- Open them with HxD



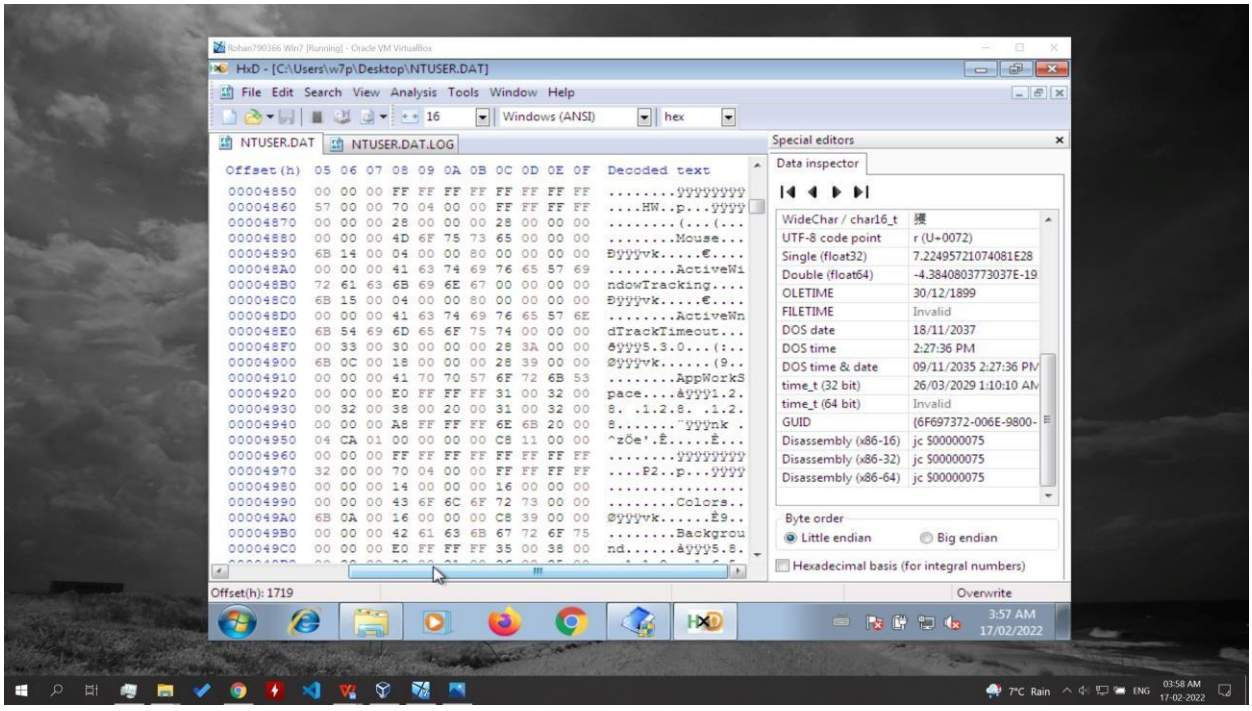
- Write down about your finding

NTUSER.DAT file saves any changes made to the operating system. They are usually stored in the registry but on restart the changes are updated to NTUSER.DAT file.

As seen in screenshot the decoded text in NTUSER.DAT file contains Windows/Internet settings

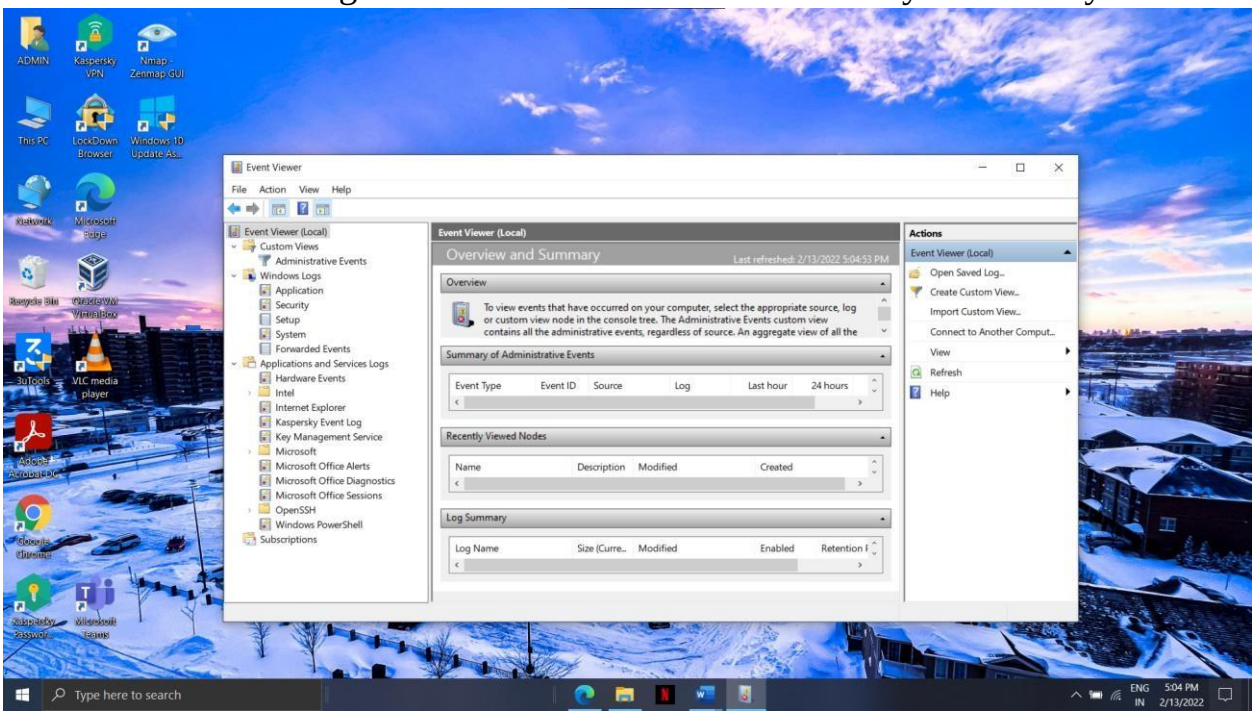


- Further Windows Tracking, Timeout and colors are also recorded in this file.



Part 1e

- **Event Viewer**: It is a tool in Windows OS that is used by Administrators and users to views logs and events within a Network locally or remotely.



- **Custom Views**: If an Administrator wants to track information about a specific issue on a system, it can be done by creating a custom view. It shows events that ADMIN has requested to.
- **Windows Logs**: Events in windows logs has been categorized into Application, Security and System.
- **Application**: Any type of information or warnings about different applications that are running in your system. Drivers or built-in system element events also shows in this tab.
- **Security**: This tab shows us anytime someone has successfully logged into a system or anytime someone successfully failed to log in to a system. Users or Administrators can go further deep into the reason of what was the reason behind those events.
- **Setup**: All the events or errors occurred during installation of windows are recorded here.
- **System**: All the events related to programs which are installed in the system are logged in this tab with its Event ID and timestamp.

- **Forwarded Events**: This log keeps track of records or events that have been sent to the system (which can also be called as a Collector system) from other systems in the same network. We can maintain track of events from numerous machines from one centralized location using this log.
- **Application and services log**: Windows applications services log enables administrator and users to track individual applications and services logs on windows devices. Subcategories in this log are detailed below.
- **Hardware events**: To use this service user must be subscribed to it to monitor events. But this only works on Windows Server 2008.
- **Internet Explorer**: All the events by Internet explorer are stored in this tab. As by default it is disabled by Microsoft, so no events are visible here.
- **Key Management Service**: KMS (Key Management Service) is an activation feature that lets enterprises to manage the activation of their Windows systems and Office without having to connect individual PCs to Microsoft for product activation. All the logs related to KMS clients are logged here.
- **Media Center**: It contains all the events related to any media service on the windows machine.
- Microsoft: It contains logs related to proprietary services provided by Microsoft such as Bluetooth, AppLocker, BitLocker and many more.
- **ThinPrint Diagnostics**: Events from ThinPrint Diagnostic utility are logged in this tab.
- **Windows PowerShell**: It is a task automation system that consists of a command-line shell, a scripting language, and a configuration management framework that works across different platforms. Events related to all these are stored here with Event IDs and timestamps.

Conclusion

To conclude, with this we get to know about FTK imager is an imaging tool which helps to create image and more about host forensic through registry analysis, PSRECON which collects information from Windows and arrange data in folders, NTUSER.DAT which created by MS windows OS. The extension DAT refers to the data files which stores information about program This helps to save the changes which we have made into account.

Summary

To summarize, we have learned how to create a forensic evidence drive using FTK Imager. For the second part, we learnt how to dissect internal registry files of a system using F-RAT. We utilized PSRecon to conduct a passive reconnaissance on a remote Windows environment using PowerShell and gathering details such as IP addresses and Firewall configuration, which cou ld be detrimental to the systems integrity. After this we looked at NTUSER.DAT file which contains information about the user profile and preferences including any changes to the visual settings. For this we used Linux Disk Reader to extract the hidden files and HxD to read the .DAT files. Lastly we looked at all the components in the event viewer and discuss about them, hence learning about their functions in our daily usage.

Achievement

Achievement for this activity is that we have learned about SAM files and with the help of these tools we can get more information about all the users and group present in the machine for example login counts, last password changes etc. With the help of Internal Linux Reader and HxD we were able to locate hidden files and access them. This provided us with the state of machine and any new changes made to it before last restart.

References

- Dysert, B. (n.d.). *What is the Purpose of the Forwarded Events Event Log? (Tips.Net)*. Windows.Tips.Net. Retrieved February 13, 2022, from https://windows.tips.net/T012878_What_is_the_Purpose_of_the_Forwarded_Events_Event_Log.html
- Hoffman, C. (2018, November 12). *What Is the Windows Event Viewer, and How Can I Use It?* How-To Geek. Retrieved February 13, 2022, from https://www.howtogeek.com/123646/htg-explains-what-the-windows-event-viewer-isand-how-you-can-use-it/
- K. (n.d.). *Creating Hardware Event Subscriptions - Win32 apps*. Microsoft Docs. Retrieved February 13, 2022, from https://docs.microsoft.com/enus/windows/win32/wec/creating-hardware-event-subscriptions
- S. (2021, October 6). *What is PowerShell? - PowerShell*. Microsoft Docs. Retrieved February 13, 2022, from https://docs.microsoft.com/enus/powershell/scripting/overview?view=powershell-7.2
- *StackPath*. (n.d.). Maketecheasier. Retrieved February 13, 2022, from https://www.maketecheasier.com/windows-custom-views-event-viewer/
- *TechNet Wiki*. (n.d.). Social.Technet.Microsoft. Retrieved February 13, 2022, from https://social.technet.microsoft.com/wiki/contents/articles/26939.getting-started-withkms-key-management-service.aspx

Name of students who has not participated in the assignment.
Student name:
Student name:
Student name:
Student name:
Student name:

All members of this group has participated in this activity