Windows Forensics 1

Introduction

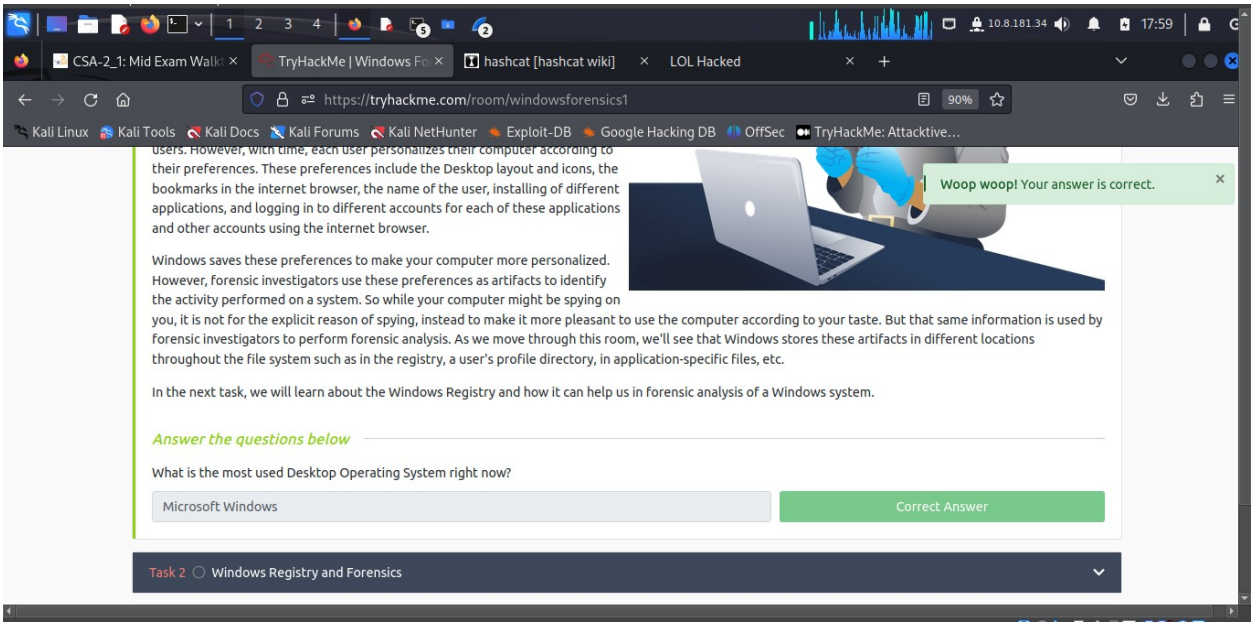
In this chapter the learner is expected to go through Windows registry forensic and cover ten tasks that solidifies his knowledge and skills in Security Analysis.

Activities

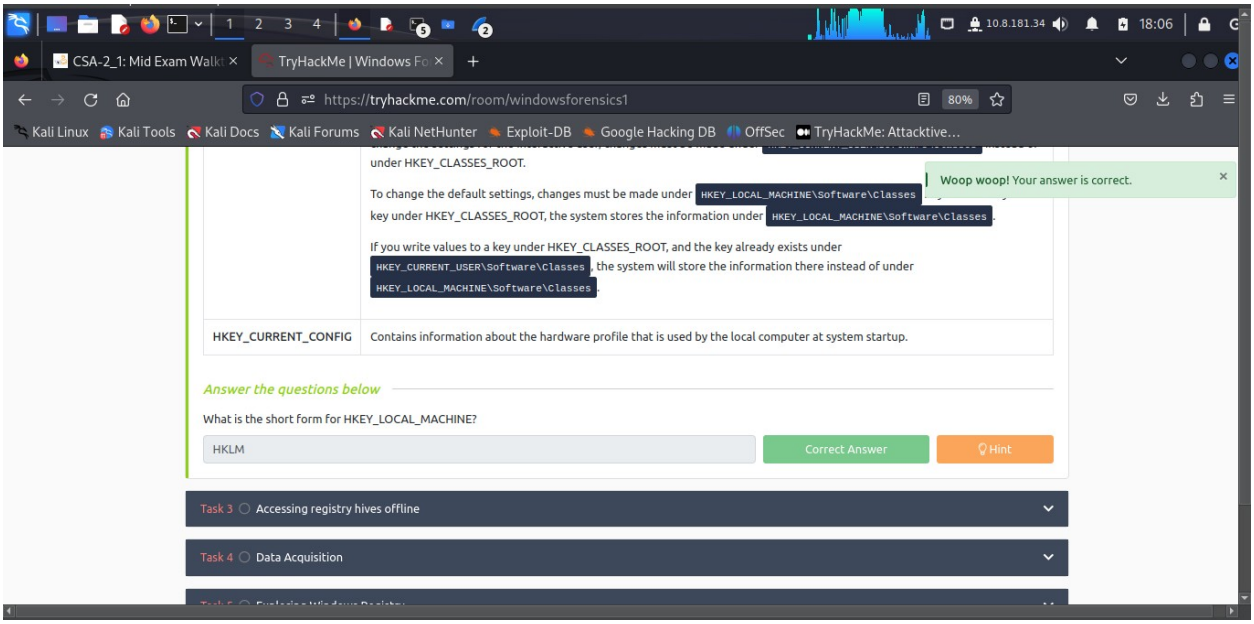
Task 1: Introduction to Windows Forensics

Introduction to Computer Forensics for Windows:

Essential field of cyber security that involves gathering evidence of activities performed on computers. It is a part of the wider Digital Forensics field, which deals with forensic analysis of all types of digital devices, including recovering, examining, and analyzing data found in digital devices.

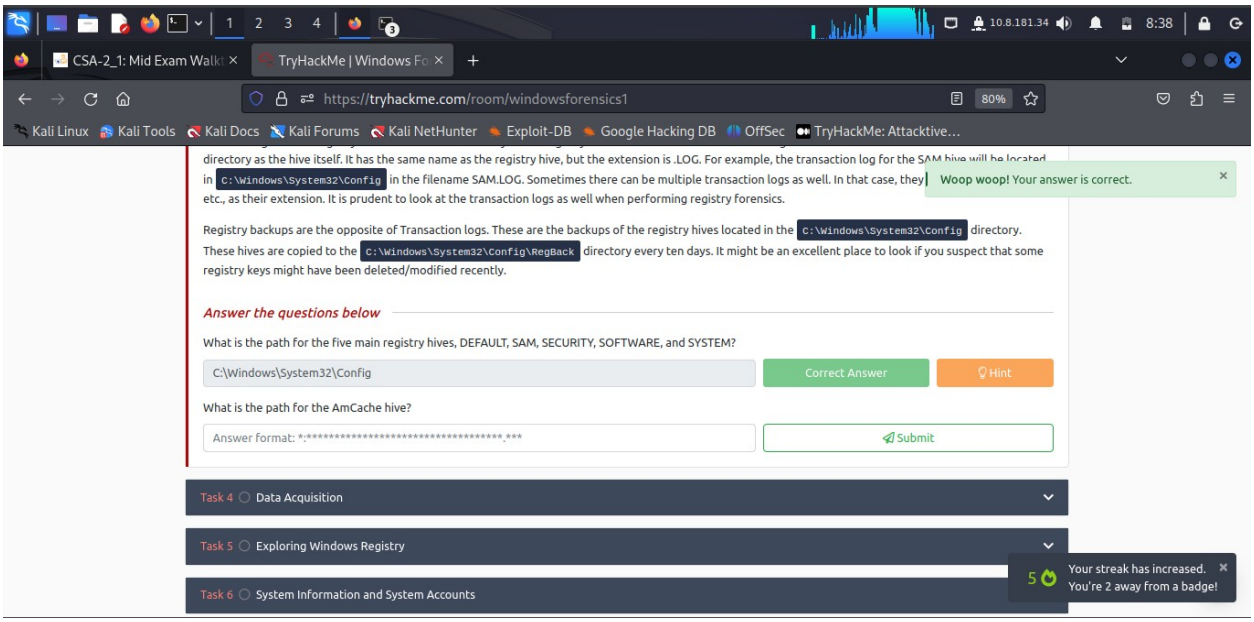


Task 2: Windows Registry and Forensics

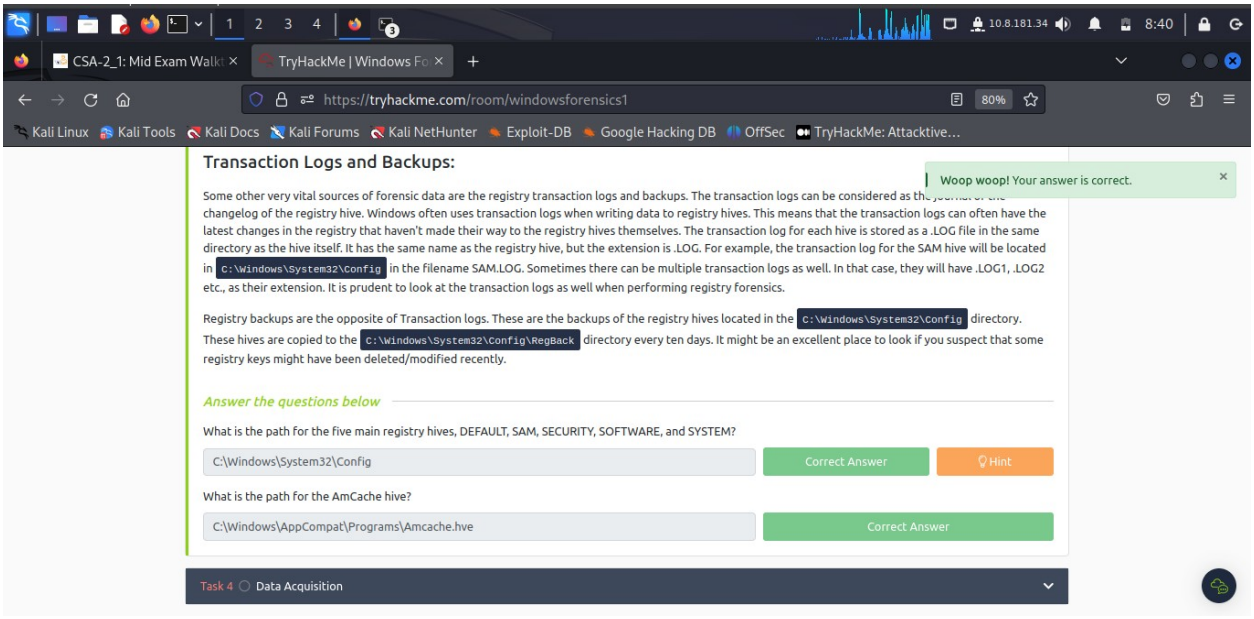


Task 3: Accessing registry hives

The path for the five main registry hives, DEFAULT, SAM, SECURITY, SOFTWARE, and SYSTEM is: **C:\Windows\System32\Config**



The path for the AmCache hive is: **C:\Windows\AppCompat\Programs\Amcache.hve**



Task 4: Data Acquisition

This refers to the process of imaging the system or making a copy of the required data and perform forensics on it.

For acquiring registry files, we can use one of the following tools:

KAPE:

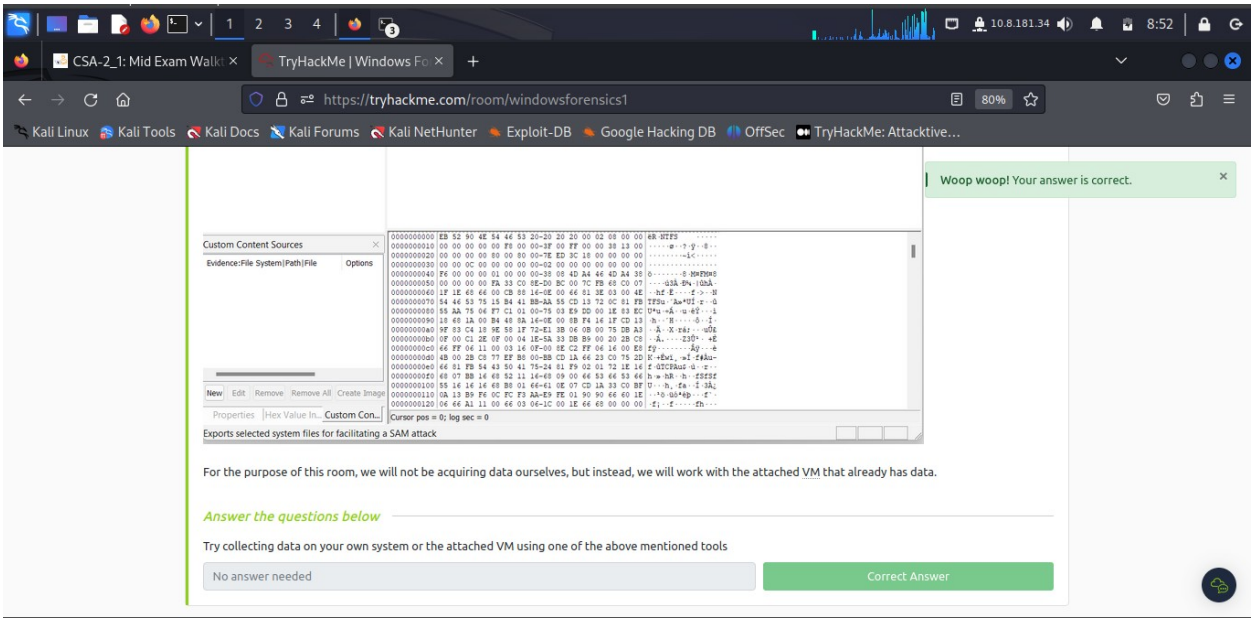
KAPE is a live data acquisition and analysis tool which can be used to acquire registry data. It is primarily a command-line tool but also comes with a GUI.

Autopsy:

Autopsy gives you the option to acquire data from both live systems or from a disk image. After adding your data source, navigate to the location of the files you want to extract, then right-click and select the Extract File(s) option.

FTK Imager:

FTK Imager is similar to Autopsy and allows you to extract files from a disk image or a live system by mounting the said disk image or drive in FTK Imager.



Task 5: Exploring Windows Registry

A tool to view registry hives is needed since the registry editor only works with live systems and can't load exported hives.

Registry Viewer:

AccessData's Registry Viewer has a similar user interface to the Windows Registry Editor. There are a couple of limitations, though. It only loads one hive at a time, and it can't take the transaction logs into account.

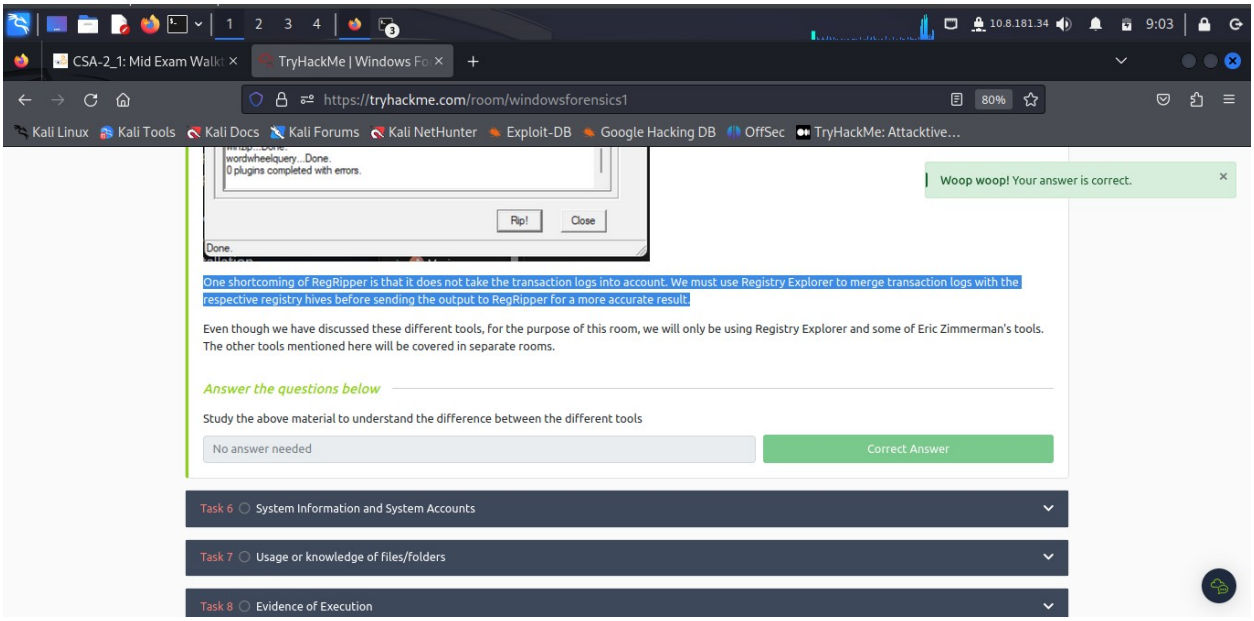
Zimmerman's Registry Explorer:

It can load multiple hives simultaneously and add data from transaction logs into the hive to make a more 'cleaner' hive with more up-to-date data. It also has a handy 'Bookmarks' option containing forensically important registry keys often sought by forensics investigators. Investigators can go straight to the interesting registry keys and values with the bookmarks menu item.

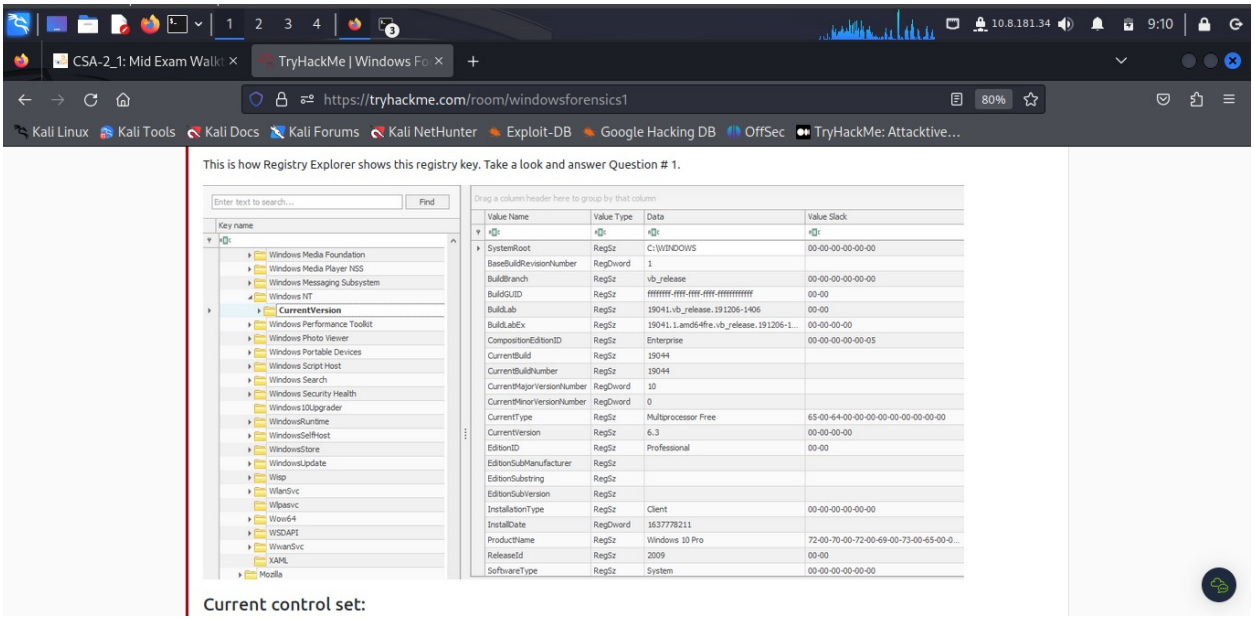
RegRipper:

RegRipper is a utility that takes a registry hive as input and outputs a report that extracts data from some of the forensically important keys and values in that hive. The output report is in a text file and shows all the results in sequential order.

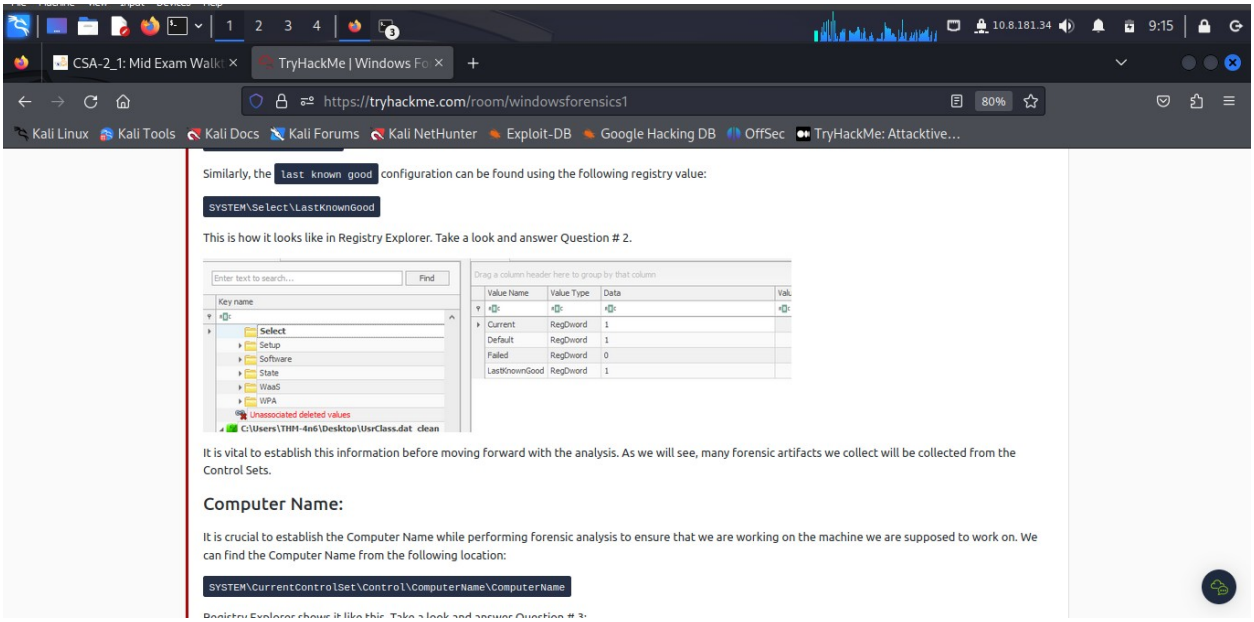
One shortcoming of RegRipper is that it does not take the transaction logs into account. Registry Explorer must be used to merge transaction logs with the respective registry hives before sending the output to RegRipper for a more accurate result.



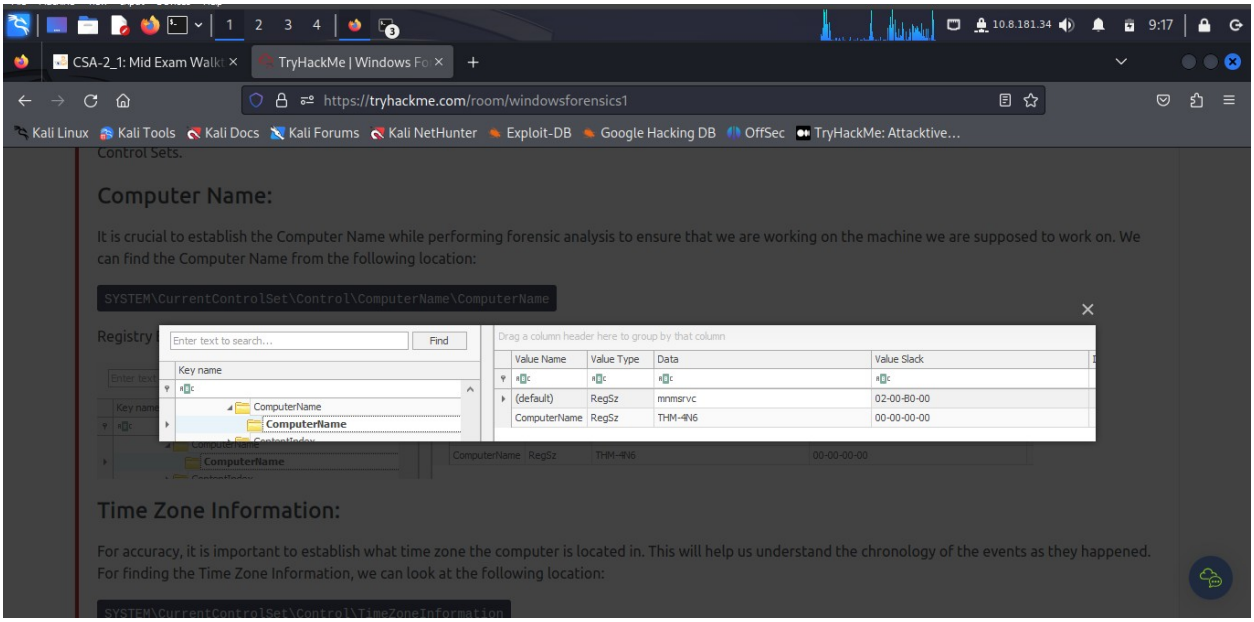
Task 6: System Information and System Accounts



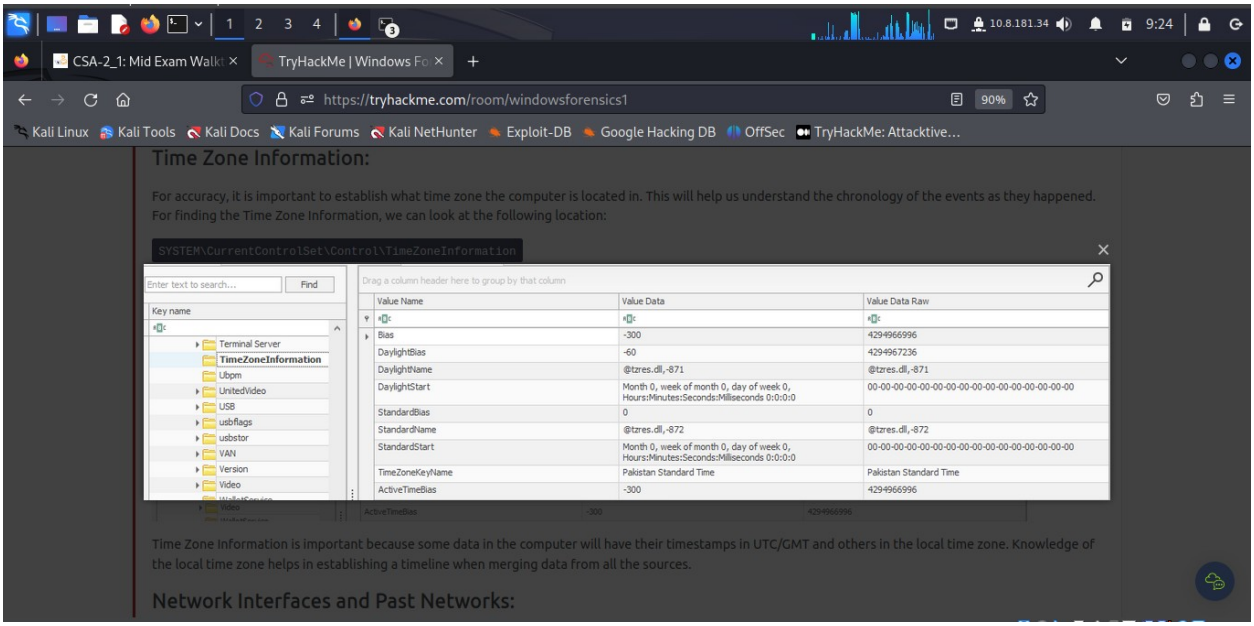
The Current Build Number of the machine whose data is being investigated is: **19044**.



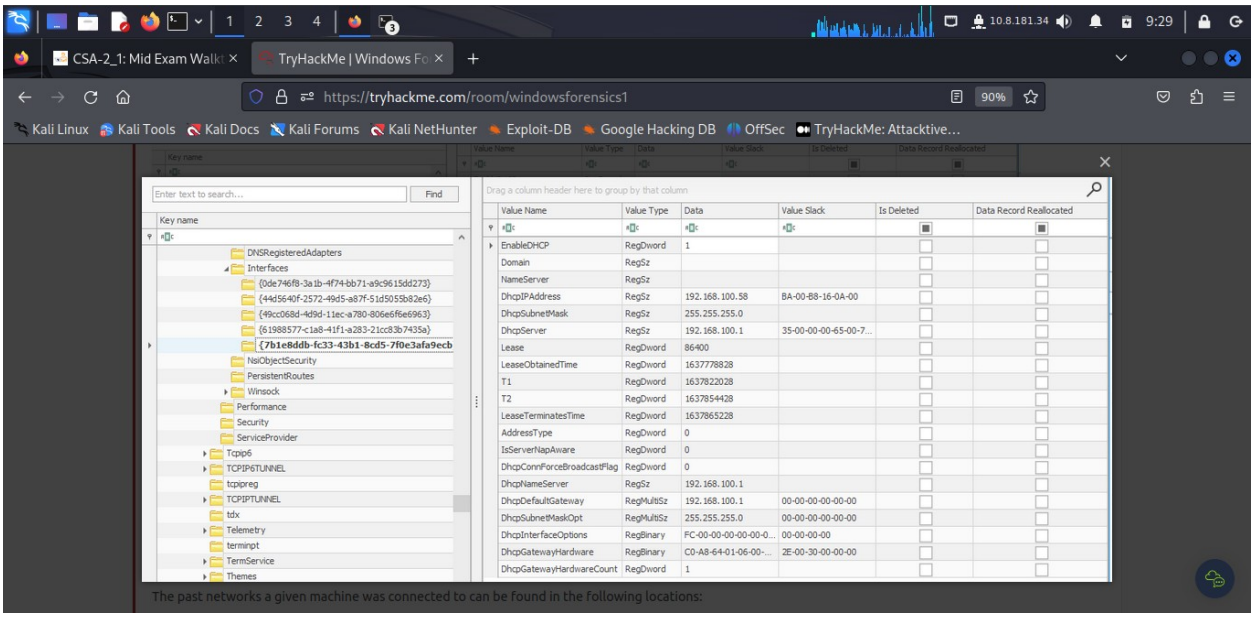
ControlSet contains the last known good configuration as **1**.



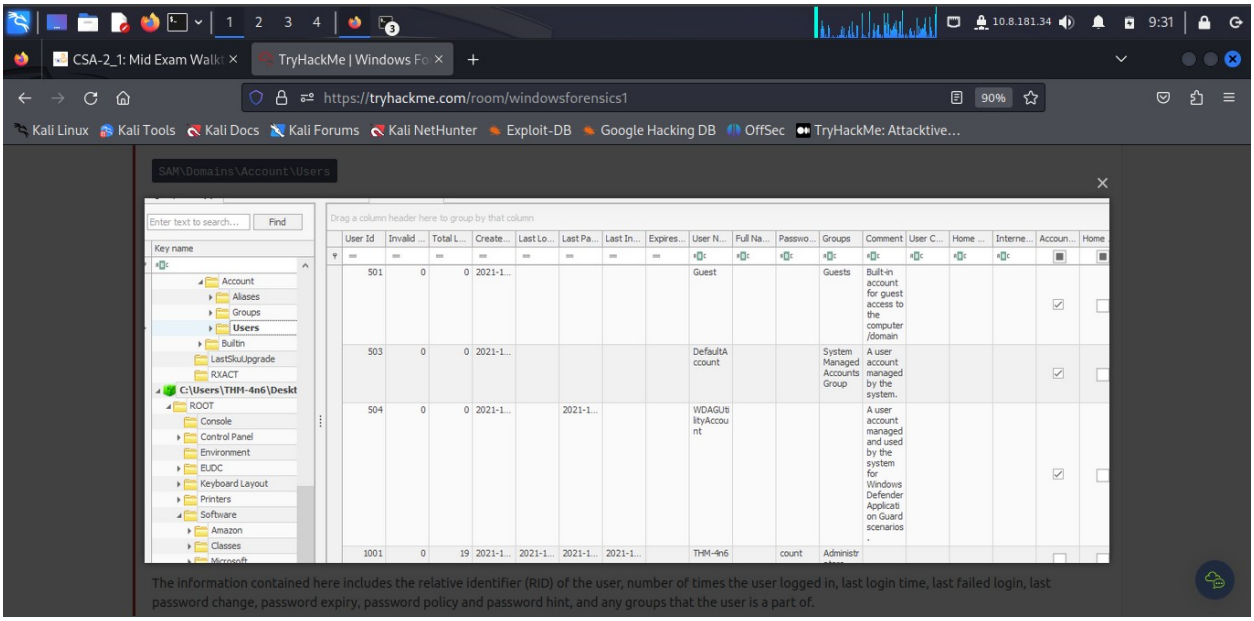
The Computer Name of the computer is **THM-4N6**.



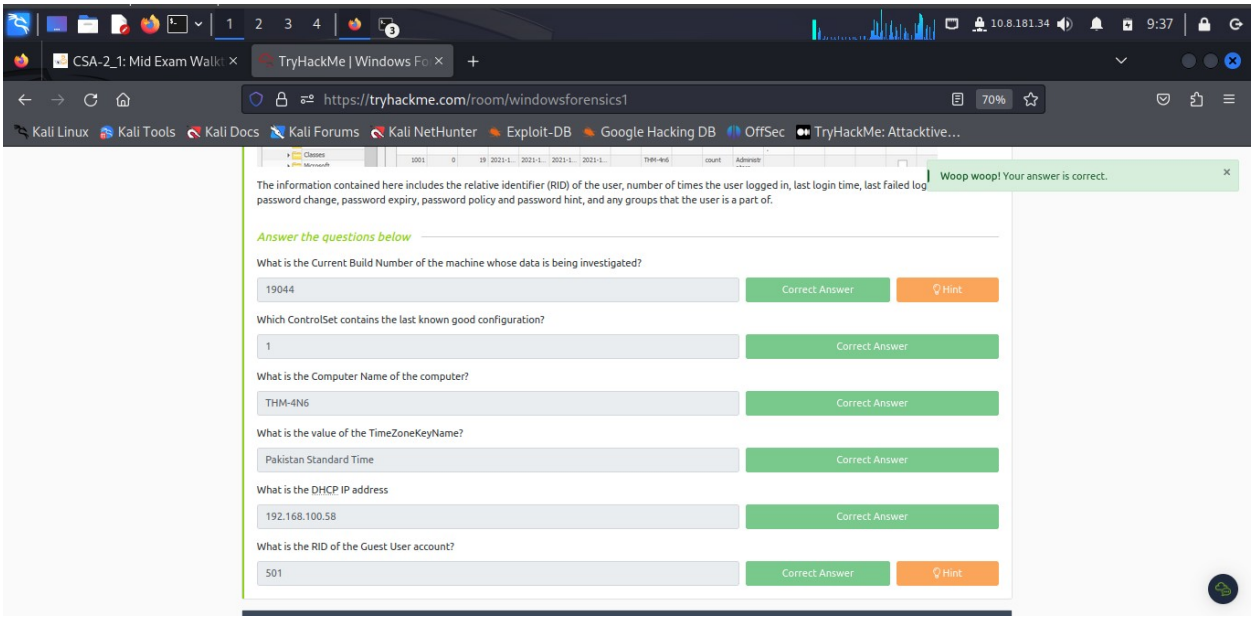
The value of the TimeZoneKeyName is **Pakistan Standard Time**.



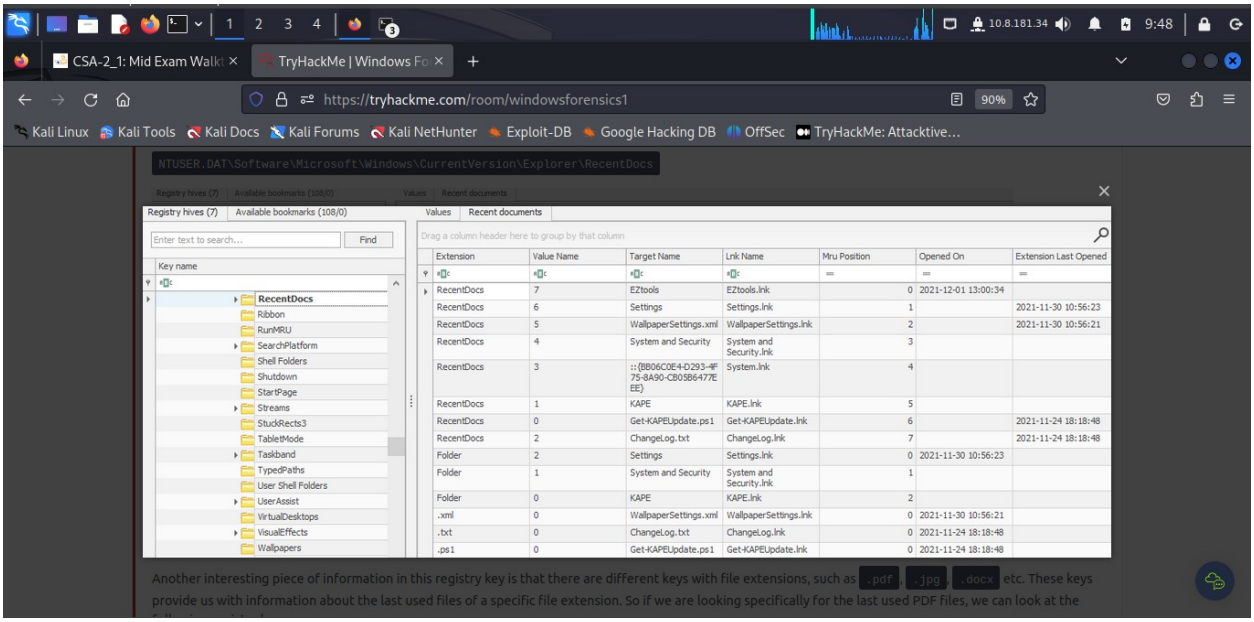
The DHCP IP address is **192.168.100.58**



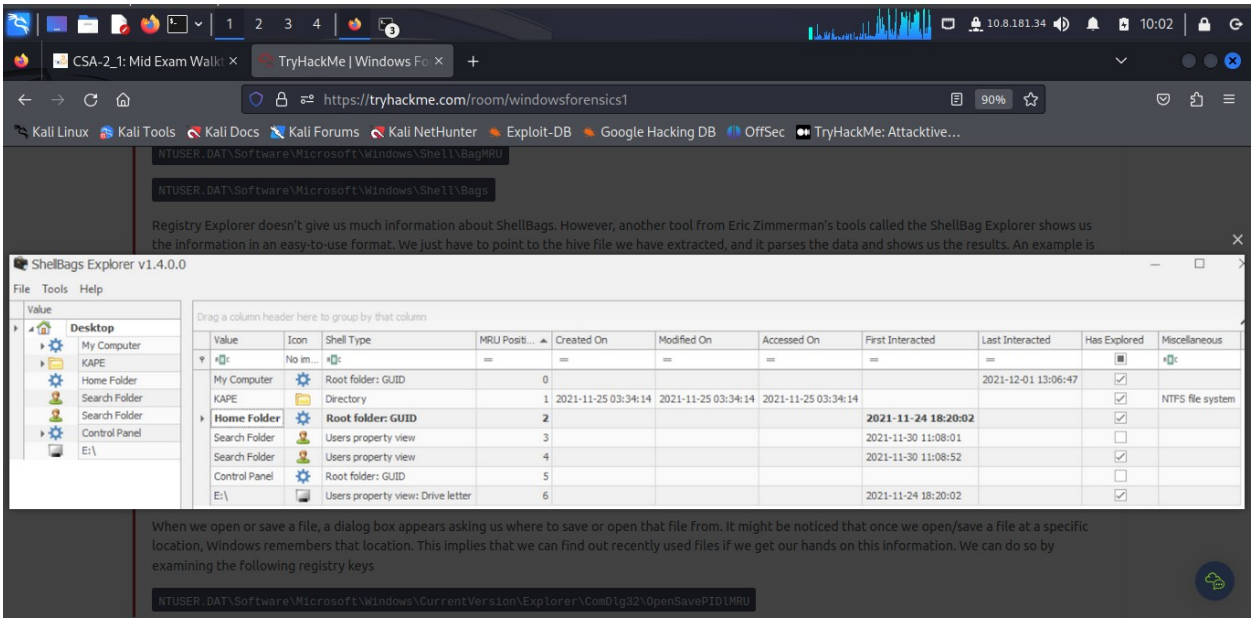
The RID of the Guest User account is **501**.



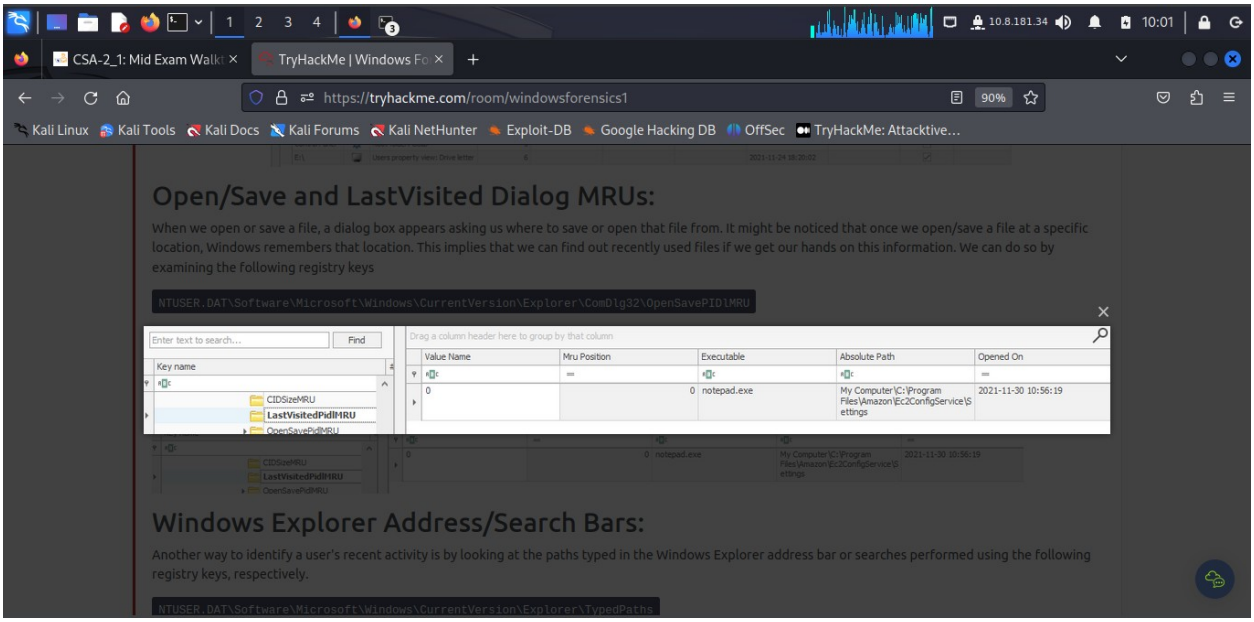
Task 7: Usage or knowledge of files/folders



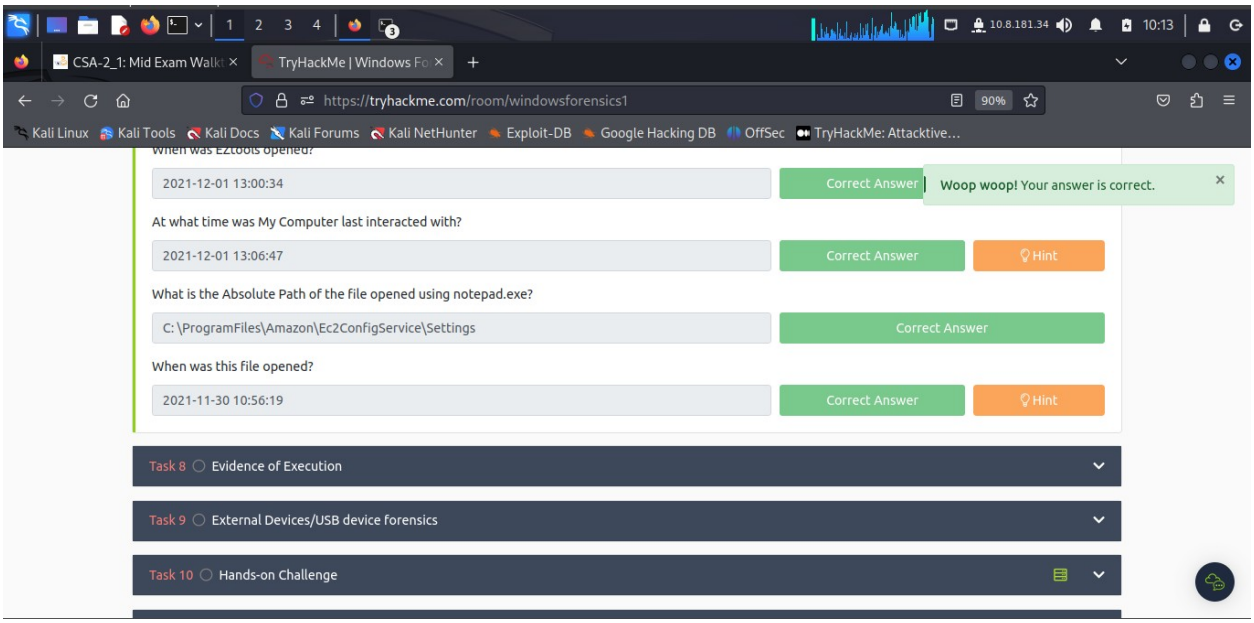
The EZTools was opened on: **2021-12-01 13:00:34**.



The last time My Computer interacted with was on **2021-12-01** at **13:06:47**

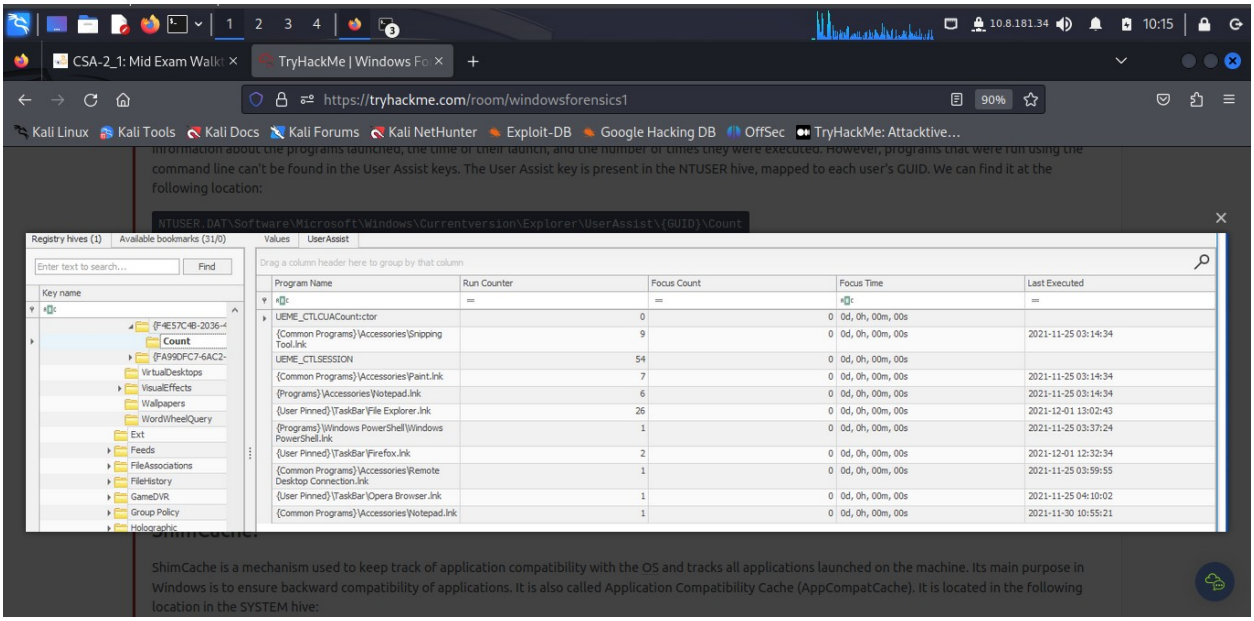


The Absolute Path of the file opened using notepad.exe is: **C: \ProgramFiles\Amazon\Ec2ConfigService\Settings**

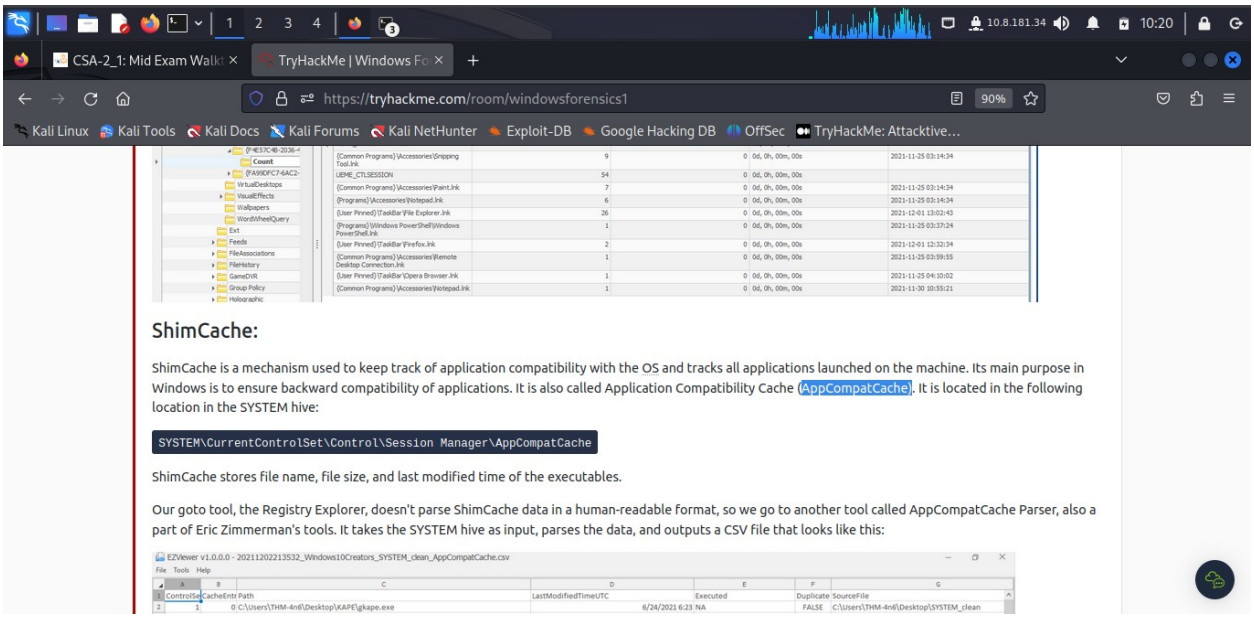


Task 8: Evidence of Execution

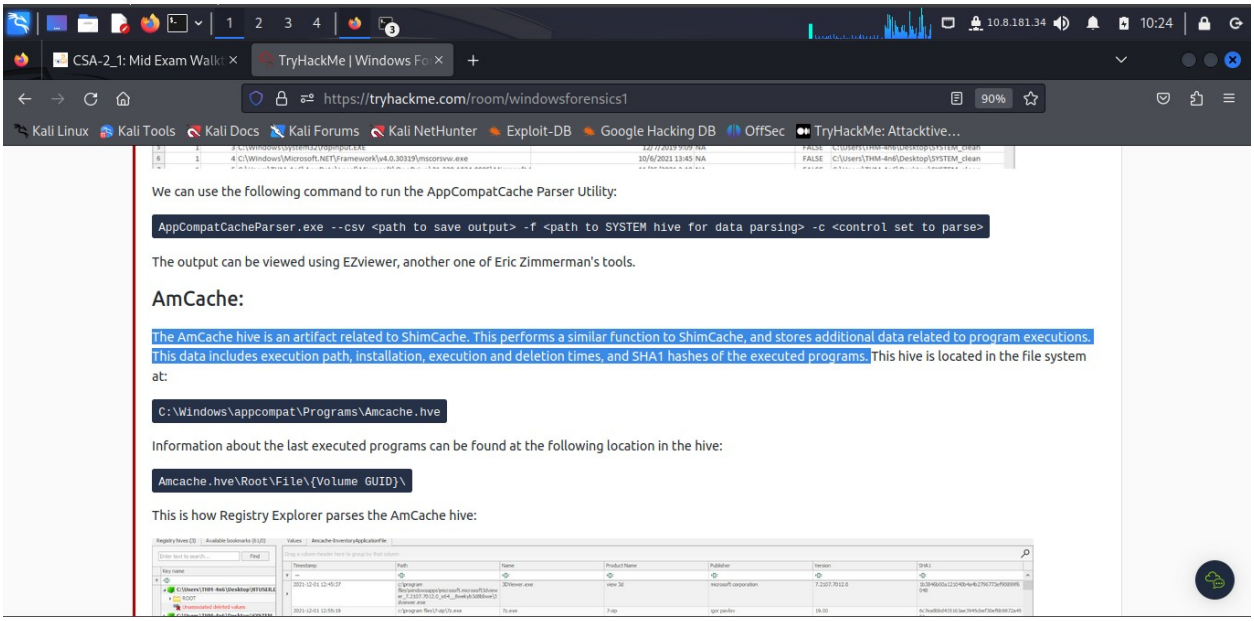
The number of times the File Explorer was launched is: **26**.



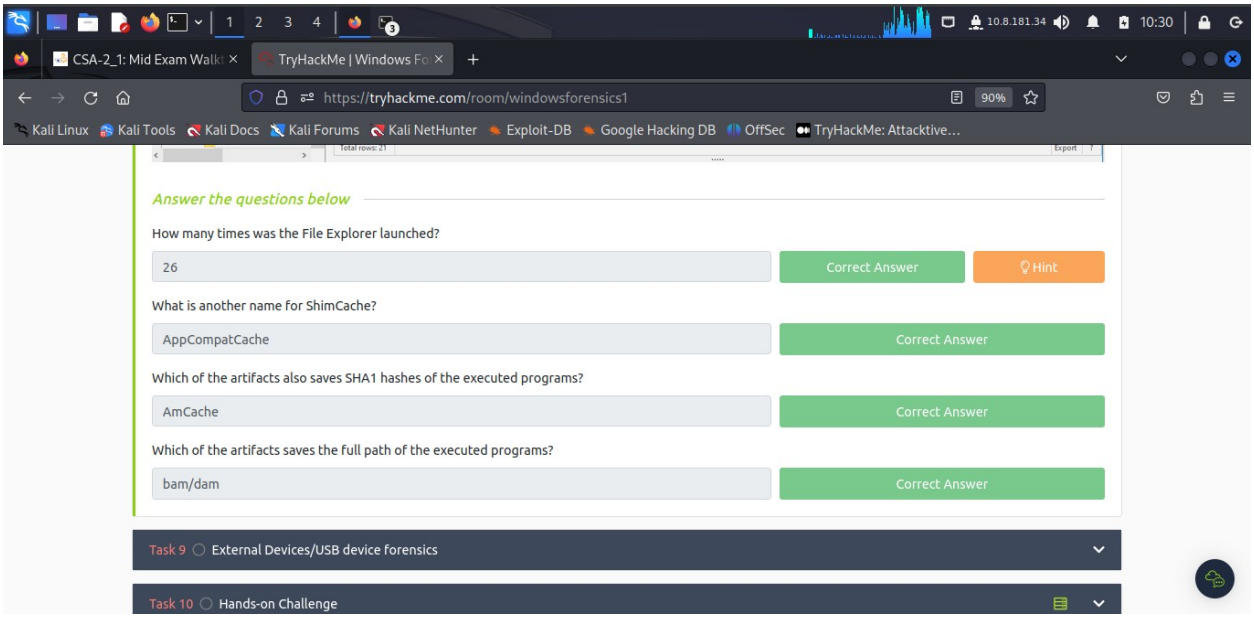
Another name for ShimCache is **AppCompatCache**.



Artifacts that saves SHA1 hashes of the executed programs is **AmCache.**

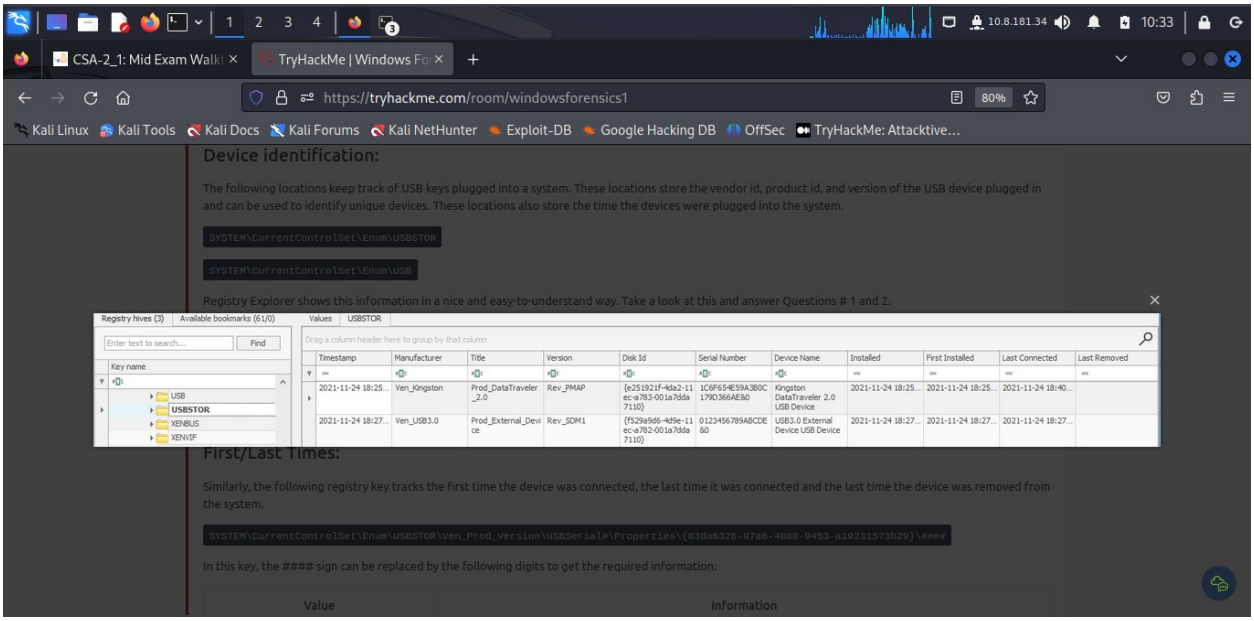


The artifacts that saves the full path of the executed programs is ***bam/dam***.

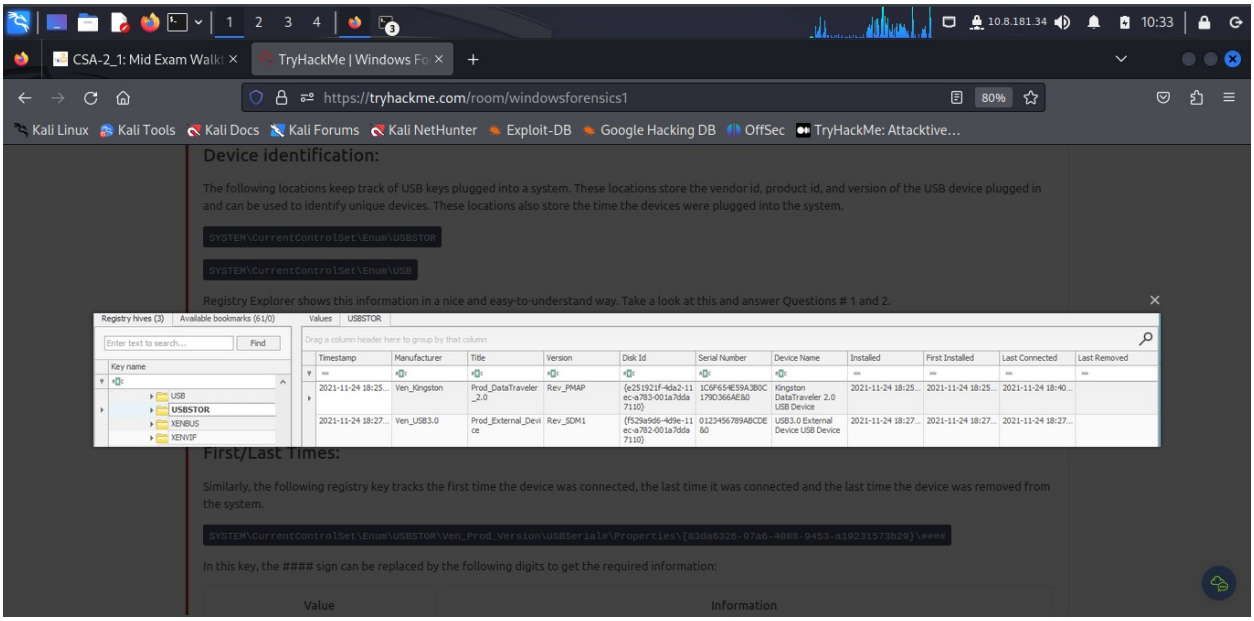


Task 9: External Devices/USB device forensics

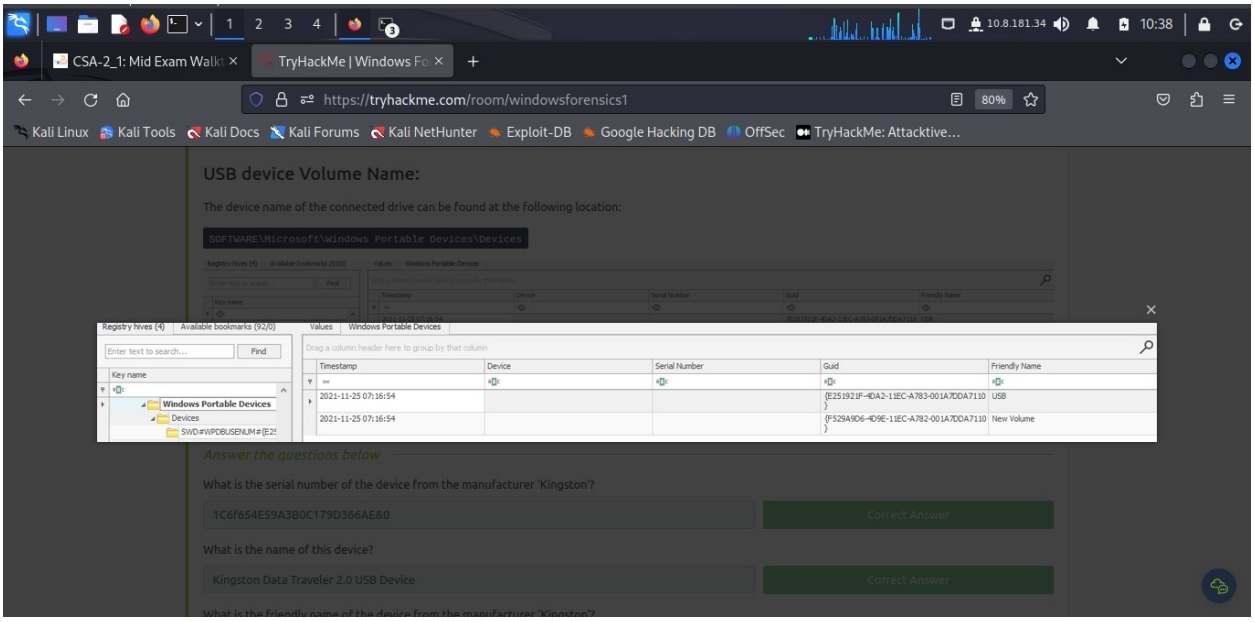
The serial number of the device from the manufacturer 'Kingston' is **1C6f654E59A3B0C179D366AE&0**

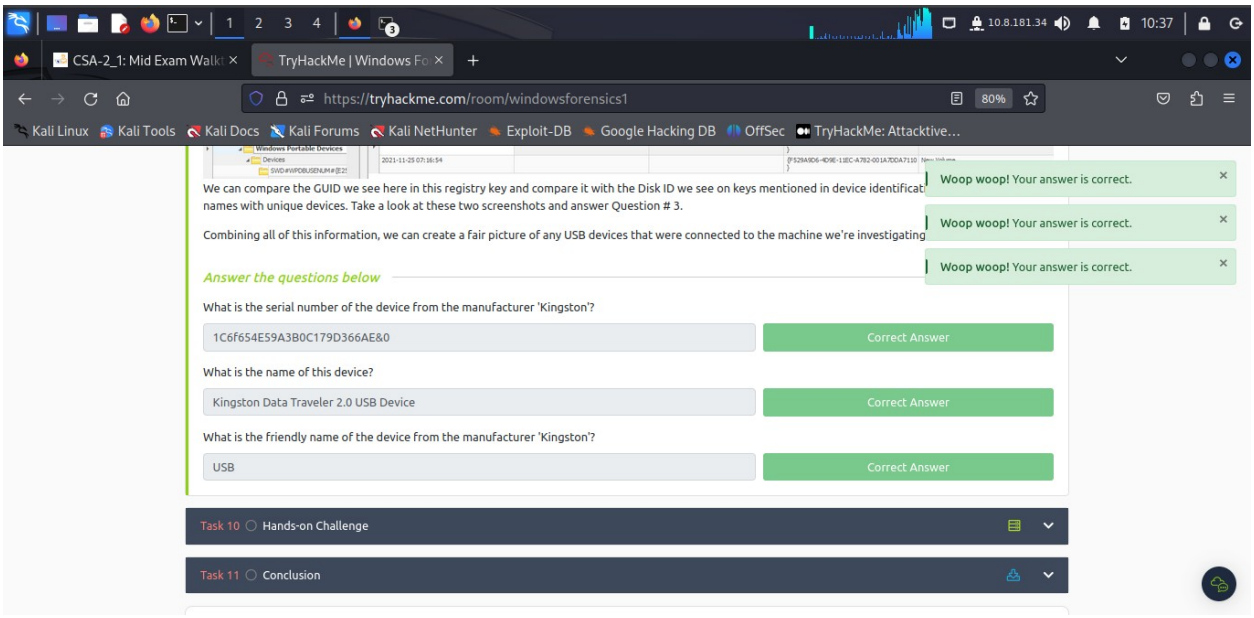


The name of the device is **Kingston Data Traveler 2.0 USB Device**.

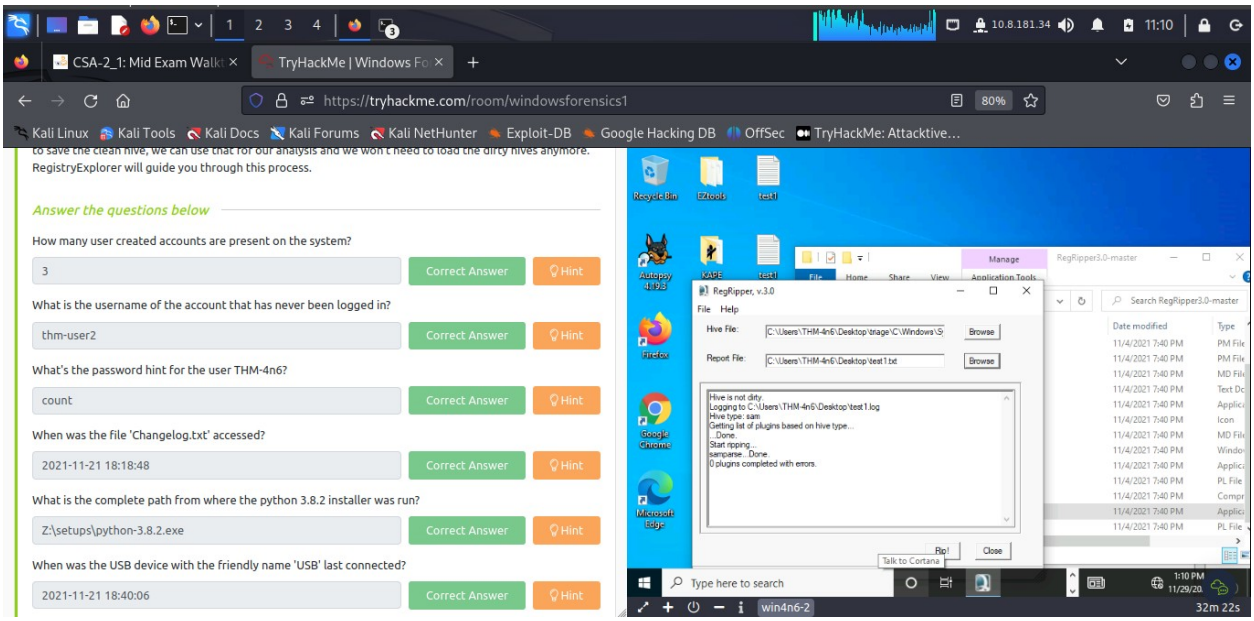


The friendly name of the device from the manufacturer 'Kingston' is **USB**.

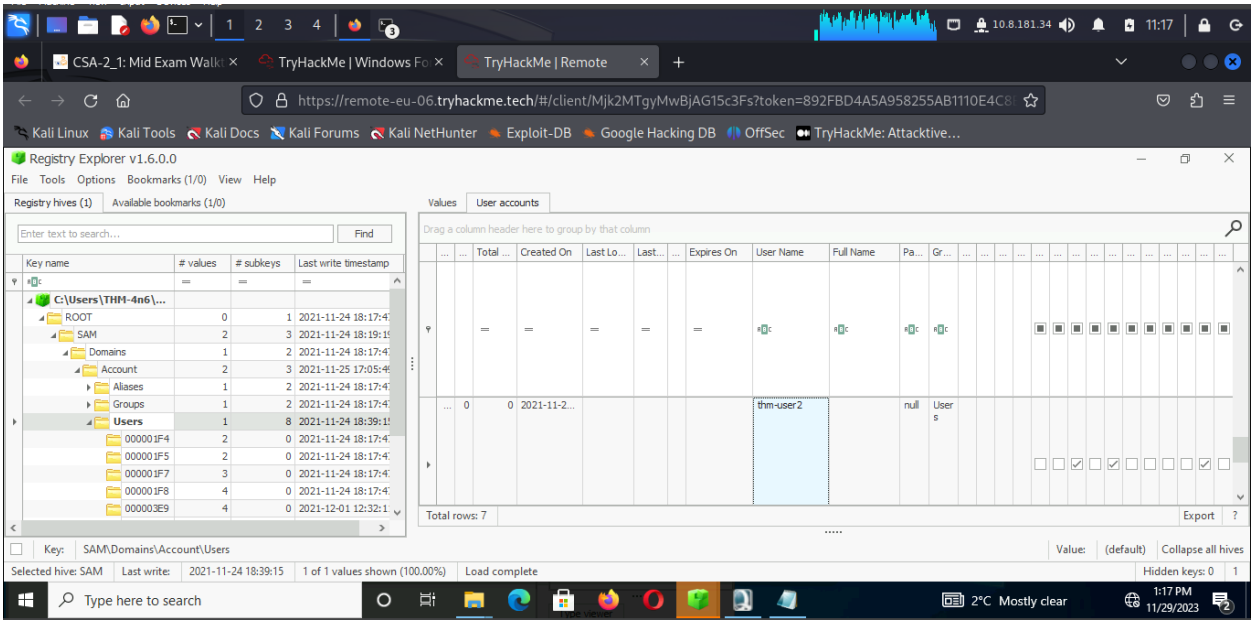




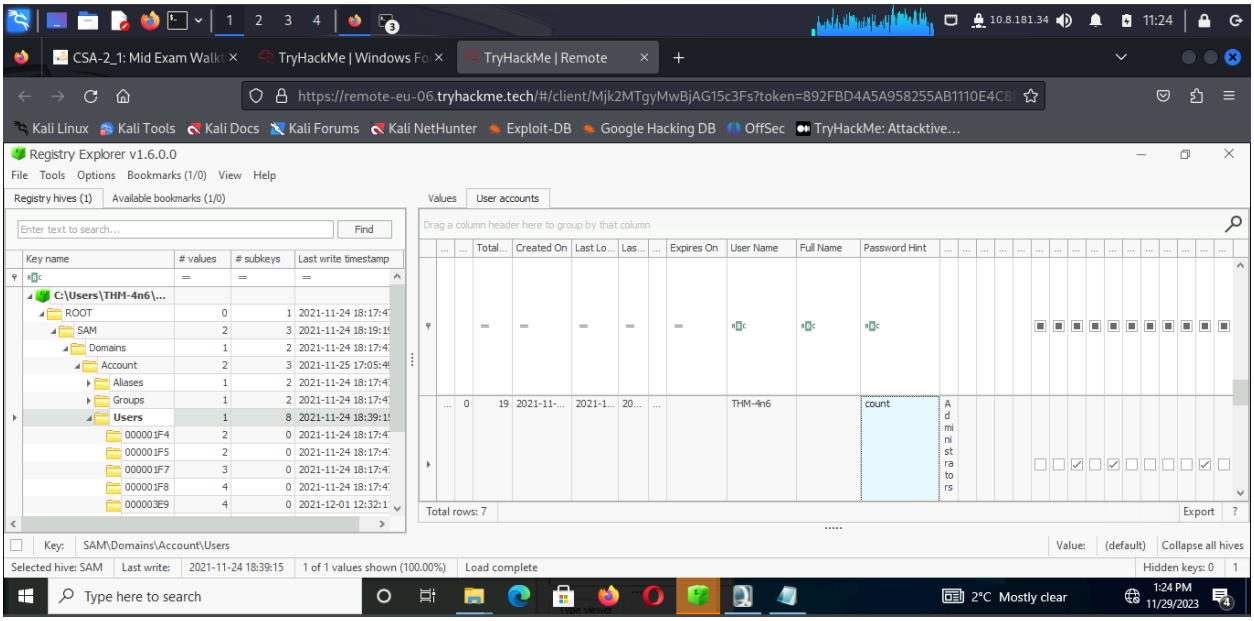
Task 10: Hands-on Challenge



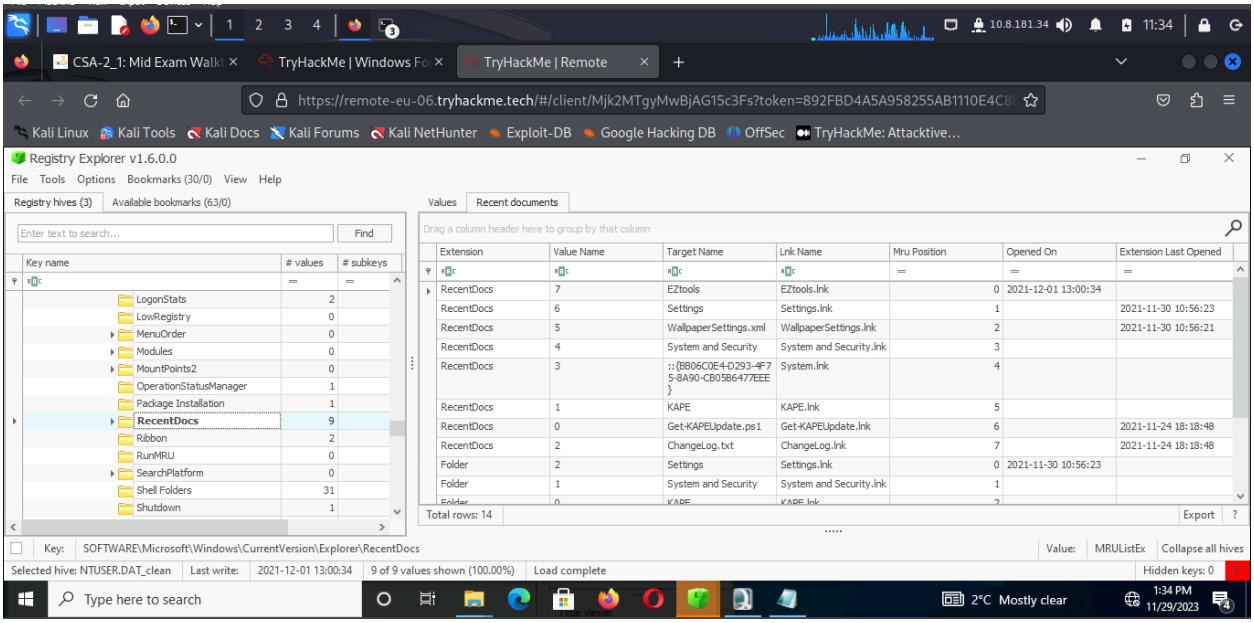
The username of the account that has never been logged in is **thm-user2**.



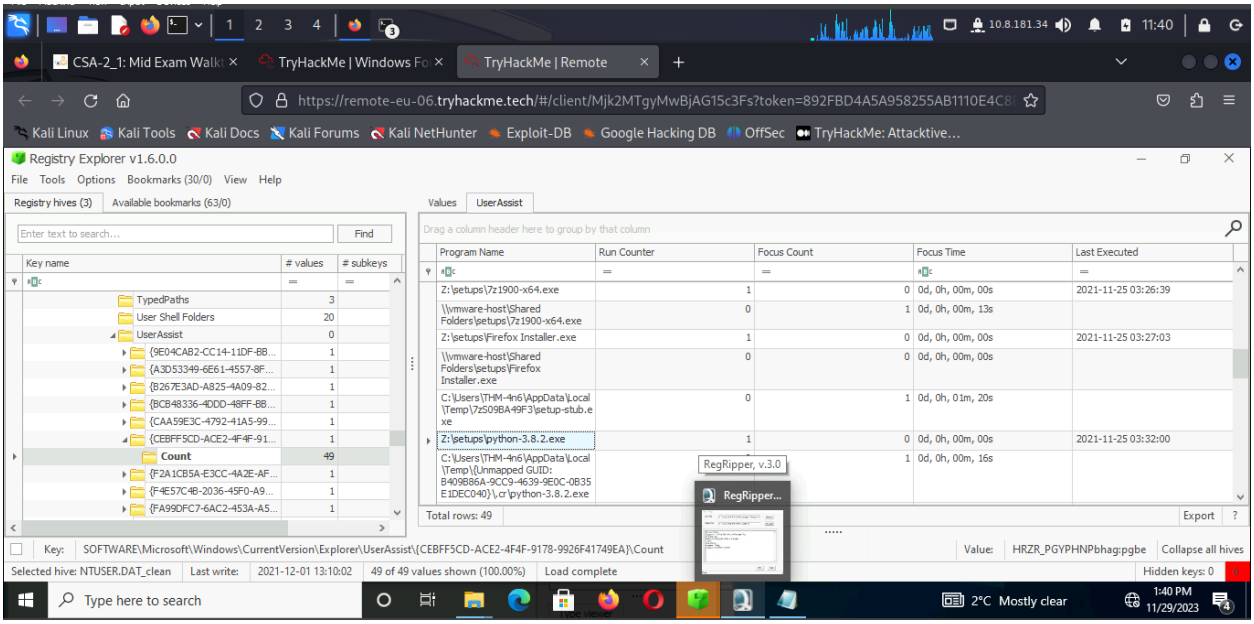
The password hint for the user THM-4n6 is **count**.



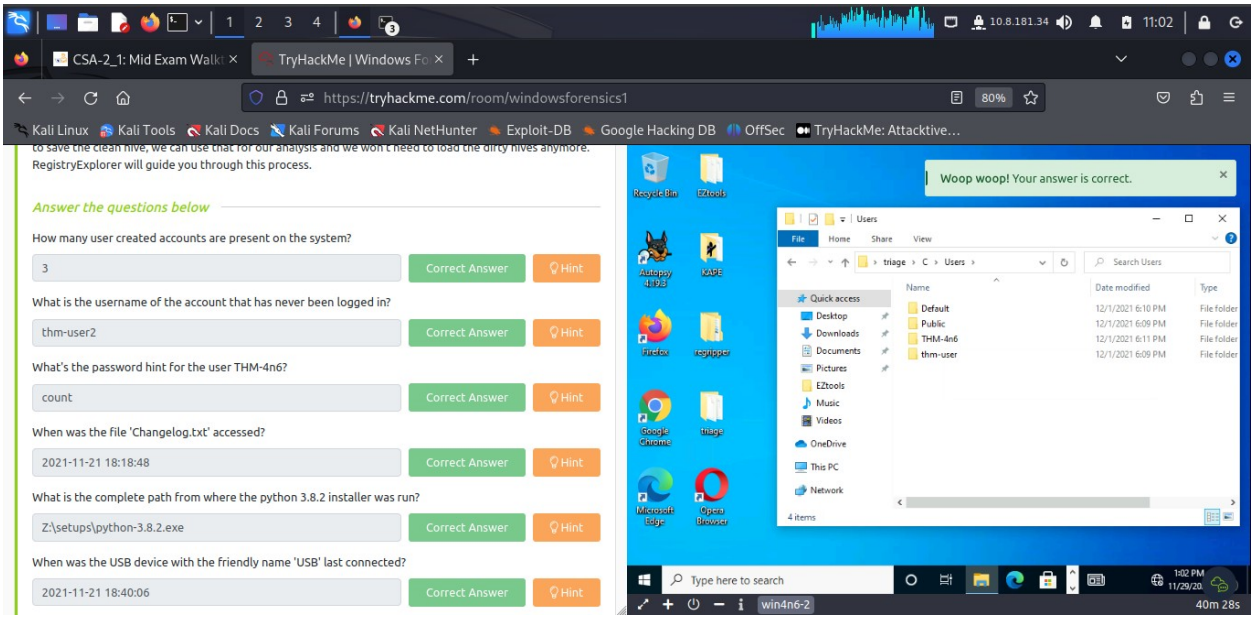
The file 'Changelog.txt' was accessed on **2021-11-21 18:18:48**



The complete path from where the python 3.8.2 installer was run is **Z:\setups\python-3.8.2.exe**



The USB device with the friendly name 'USB' last connected on **2021-11-21 18:40:06**

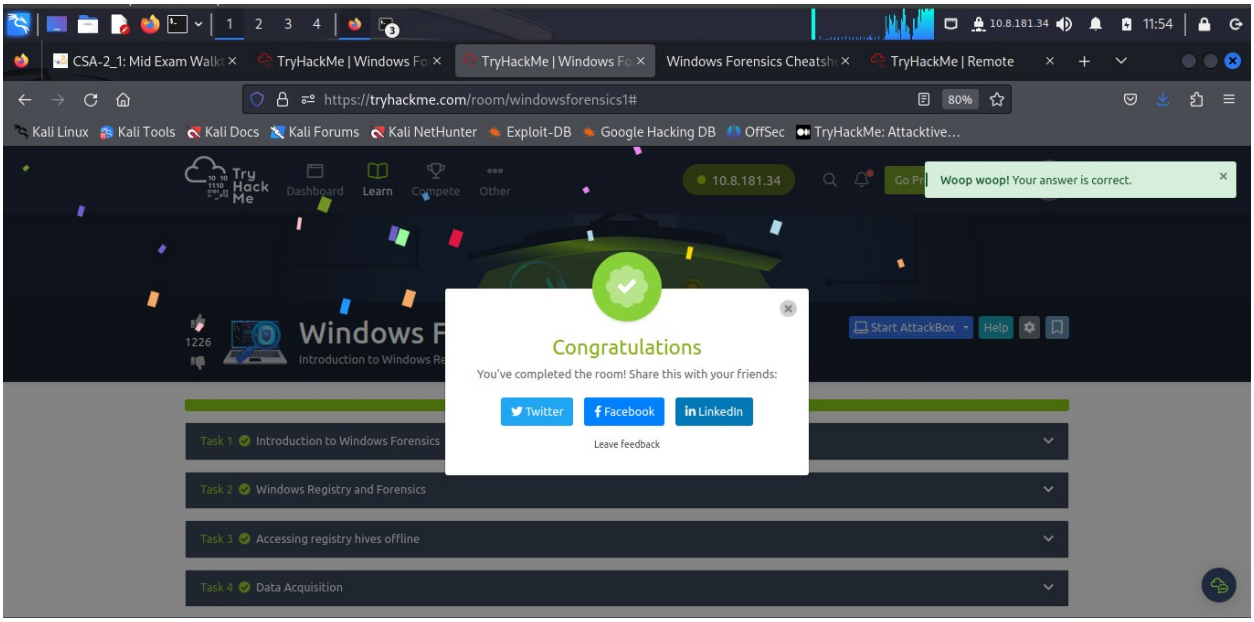


Task 11: Conclusion

I have learned how to gather basic information about a computer and its users, identify which files they used, which programs they ran, and any external devices connected to the system.

Conclusion

Using the registry access is important part of a security analyst in that it gives me the power to know which user made which type of configuration and collecting relevant information that can be used in digital forensic.



Completion Link: https://tryhackme.com/room/windowsforensics1#