Windows Forensics 1: TryHackMe

Name: Daniel Mwendwa Mwithui

ADM NO. CS-SA04-23080

Program: Security Analyst

Date of submission:3rd August 2023

Introduction

In this Windows Forensics 1 assignment on TryHackMe Labs, we will delve into the world of digital investigation on Windows systems. This hands-on module focuses on registry forensics, providing insights into the significance of the Windows registry and its various keys. Through practical exercises, we learn how to analyze and extract crucial information related to system configuration, user accounts, program execution, and connected USB devices. The use of powerful tools like RegistryExplorer, EZViewer, and AppCompatCacheParser.exe enhances our understanding of conducting comprehensive digital forensics.

Task 1: Forensics for windows

Forensics for Windows involves the investigation of digital evidence on Windows-based systems to uncover potential cybercrimes or security breaches. We can use tools such as registry to find such digital evidence. Forensic artifacts refer to the digital traces left behind by user activities on a computer system. These artifacts can include log files, browser history, registry entries, temporary files, and more. Forensics experts use these artifacts to reconstruct events, user behavior, and potentially identify malicious activities. To complete this section, read through the notes. You find that the most used desktop operating system is Microsoft windows.

Task 2: Windows Registry and Forensics

The Windows Registry is a hierarchical database that stores configuration settings and options for the Windows operating system and installed applications. It is essential for the proper functioning of Windows and contains information about hardware, software, user profiles, and system settings.

The Registry is organized into five main keys, also known as Registry hives. Each key contains numerous subkeys and values that store specific configuration data. The five keys are:

- HKEY_CLASSES_ROOT (HKCR): This key contains information related to file associations and OLE (Object Linking and Embedding) objects.
- HKEY_CURRENT_USER (HKCU): This key store configuration data specific to the currently logged-in user. It includes settings for the desktop, environment variables, and application preferences.
- HKEY_LOCAL_MACHINE (HKLM): This key contains configuration data that applies to all users of the system. It includes hardware settings, software configurations, and system-wide preferences.
- HKEY_USERS (HKU): This key contains subkeys for each user profile on the system. Each user's settings are stored in their respective subkey within HKU.
- HKEY_CURRENT_CONFIG (HKCC): This key holds information about the current hardware profile used by the system.

Registry keys are essential for the proper functioning of Windows, and any incorrect modification can lead to system instability or malfunction. Hence, it is crucial to exercise caution when making changes to the Registry, and it is recommended to back up the Registry before making any modifications.

The Windows Registry is vital in digital forensics because it contains valuable information about a system's configuration, user activities, and installed software. Forensic investigators can analyze the Registry to reconstruct events, identify user actions, and uncover evidence of potential malicious activities. The Registry helps in understanding the system's state at different points in time, aiding in investigations related to cybercrimes, data breaches, and other security incidents. Answers to this question can be found on the notes.

Task 3: Accessing Registry Hives offline

Accessing registry hives offline involves examining the Windows Registry on a disk image without booting into the live system. The registry hives are critical sources of forensic data, and they are located in the ***C:\Windows\System32\Config*** directory on the disk image. The main hives in this directory are DEFAULT, SAM, SECURITY, SOFTWARE, and SYSTEM.

Additionally, user-specific hives, NTUSER.DAT, and USRCLASS.DAT, can be found in the user's profile directory, usually in ***C:\Users<username>.*** The AmCache hive, which contains information about recently run programs, is located in ***C:\Windows\AppCompat\Programs\Amcache.hve.*** Besides, registry transaction logs (.LOG files) and backups (found ***in C:\Windows\System32\Config\RegBack)*** are essential sources for forensic analysis as they may reveal recent changes to the registry. Read through the notes to complete on the questions in this section.

Task 4: Data Acquisition

During forensic investigations, we may encounter either a live system or an image of the system. For accuracy, it's best to make a copy of the required data and perform forensics on that copy, a process called data acquisition. However, copying the registry hives directly from %WINDIR%\System32\Config on the live system is restricted.

To acquire registry data, several tools can be used:

- KAPE: A live data acquisition and analysis tool that can acquire registry data. It offers both command-line and GUI options.

- Autopsy: Allows data acquisition from live systems or disk images. After adding the data source, you can extract files by navigating to the location and using the Extract File(s) option.
- FTK Imager: Similar to Autopsy, it enables file extraction from disk images or live systems. It offers options to export files or obtain protected files for live systems, including the registry hives.

These tools facilitate the acquisition of registry data, ensuring a proper and secure approach to forensic analysis.

Task 5: Exploring windows registry

After extracting the registry hives, we need tools to view these files, as the registry editor works only with live systems and cannot load exported hives. Some useful tools for this purpose are:

- Registry Viewer (by AccessData): Similar to the Windows Registry Editor, but it loads one hive at a time and doesn't consider transaction logs.
- Zimmerman's Registry Explorer: Developed by Eric Zimmerman, this tool allows loading multiple hives simultaneously, includes transaction log data, and has bookmarks for important registry keys.
- RegRipper: Extracts data from forensically significant keys and values in a hive, producing a sequential text report. However, it doesn't account for transaction logs, and to get more accurate results, Registry Explorer should be used before running RegRipper.

For this exercise, we will focus on Registry Explorer and some of Eric Zimmerman's tools, while other tools will be covered separately.

Task 6: System information and system accounts

When performing forensic analysis, the first step is to gather system information and account data from the registry. We can find the OS version in the registry key ***SOFTWARE\Microsoft\Windows NT\CurrentVersion***. The Control Sets used during system startup can be located in ***SYSTEM\ControlSet001*** and ***SYSTEM\ControlSet002***. The CurrentControlSet, found at ***HKLM\SYSTEM\CurrentControlSet***, contains the most accurate system information. The Computer Name is available in ***SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName***.

Time Zone Information which is useful in helping establish event chronology is found in ***SYSTEM\CurrentControlSet\Control\TimeZoneInformation***,. Network interface details are located in ***SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces***, and past networks can be found in ***SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures***. Autostart programs are listed in various registry keys under ***NTUSER.DAT*** and ***SOFTWARE\Microsoft\Windows\CurrentVersion***. The SAM hive contains user account information, including login details and group information, found in ***SAM\Domains\Account\Users***. Accessing and analyzing this system information is crucial for a thorough forensic investigation. To complete this section, read through the thumbnails attached.

Task 7: Usage or Knowledge of the Files/Folders

When performing forensics, it is necessary to know information about the files and folders that we will be interacting with. Below are ways to gain information about some of mostly used files and folders:

- Recent Files: Windows maintains a list of recently opened files for each user in the NTUSER hive. The key location is ***NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs.*** Registry Explorer allows us to view and sort this data, showing the most recently used (MRU) files at the top.

- Office Recent Files: Microsoft Office also keeps a list of recently opened documents in the NTUSER hive. The location varies depending on the Office version. For example, for Office 2013, it is ***NTUSER.DAT\Software\Microsoft\Office\15.0\Word***.

- ShellBags: ShellBags store information about the layout preferences of folders, including MRU files and folders. The keys are stored in the user hives, and locations include ***USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags*** and ***NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags.*** ShellBag Explorer, a tool from Eric Zimmerman's collection, helps analyze this data effectively.

- Open/Save and LastVisited Dialog MRUs: Windows remembers locations used to open or save files, and this information is stored in the registry keys ***NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU*** and ***NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU.***

- Windows Explorer Address/Search Bars: Paths typed in the Windows Explorer address bar and search queries are stored in the registry keys ***NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths*** and ***NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery***, respectively.

Analyzing registry data for recent files and user activity can provide valuable insights during a forensic investigation. The use of tools like Registry Explorer and ShellBag Explorer helps to efficiently interpret and extract information from the registry hives, aiding in the reconstruction of events and user behavior on the system. Answers to question in this section can be found in the notes above.

Task 8: Evidence of execution

During a forensic investigation, evidence of program execution can provide crucial insights into user activity and system behavior. This section covers various artifacts related to program execution found in the Windows Registry, including UserAssist, ShimCache, AmCache, and BAM/DAM.

- UserAssist: Windows stores information about applications launched by the user using Windows Explorer in the User Assist registry keys. This data includes the program names, launch times, and execution frequencies. The User Assist key is located in the NTUSER hive, mapped to each user's GUID. Accessing this information can reveal the history of programs executed by the user.

- ShimCache: ShimCache, also known as Application Compatibility Cache, tracks application compatibility with the operating system and records all launched applications. It resides in the SYSTEM hive at ***SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache.*** However, the data in ShimCache is not easily readable using Registry Explorer, and the AppCompatCache Parser tool from Eric Zimmerman's collection can help parse the data into a human-readable format.

- AmCache: The AmCache hive is another artifact related to program execution and is linked to ShimCache. It stores additional data such as execution paths, installation times, and SHA1 hashes of executed programs. The AmCache hive is located at ***C:\Windows\appcompat\Programs\Amcache.hve***, and information about last executed programs can be found in ***Amcache.hve\Root\File{Volume GUID}.*** Registry Explorer can assist in parsing the AmCache hive for examination.

- BAM/DAM: Background Activity Monitor (BAM) and Desktop Activity Moderator (DAM) are components of Microsoft Windows that monitor background application activity and optimize power consumption. Relevant information about last run programs, their paths, and execution times can be found in the registry at ***SYSTEM\CurrentControlSet\Services\bam\UserSettings{SID}*** and ***SYSTEM\CurrentControlSet\Services\dam\UserSettings{SID},*** respectively.

The examination of these artifacts provides valuable evidence of program execution on a Windows system. These findings can aid in establishing a timeline of events, understanding user activities, and identifying potential security incidents during forensic investigations. Read through the notes to answer question in this section.

Task 9: External Devices/USB device forensics

During forensic investigations, it's essential to identify any USB or removable drives connected to the system and gather information related to these devices. The registry provides valuable data for this purpose.

1. Device Identification: The registry locations ***SYSTEM\CurrentControlSet\Enum\USBSTOR*** and ***SYSTEM\CurrentControlSet\Enum\USB*** keep track of connected USB devices, storing details like vendor ID, product ID, version, and connection time. Using Registry Explorer, this information can be easily viewed and analyzed.

2. First/Last Times: The registry key ***SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USBSerial#\Properties{83da6326-97a6-4088-9453-a19231573b29}####*** tracks the first and last connection times and the last removal time of the USB device. Registry Explorer helps parse and present this data, facilitating investigations.

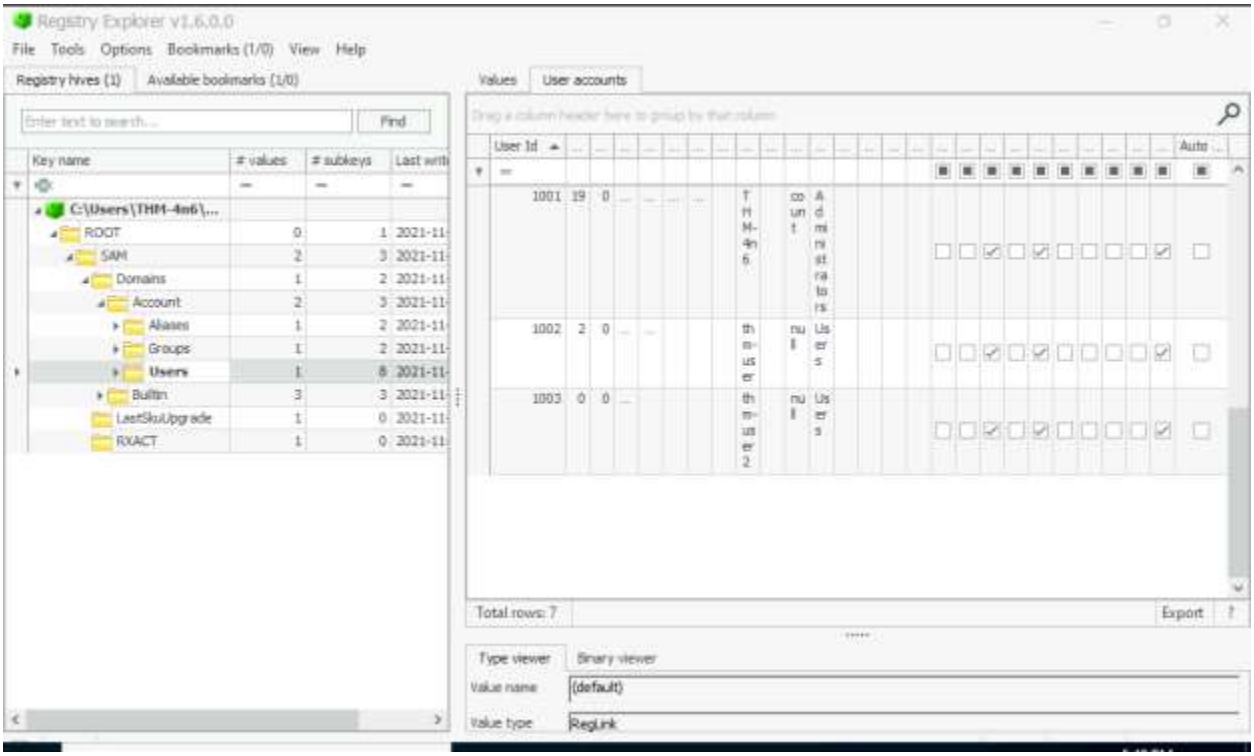
3. USB Device Volume Name: The device names of connected drives can be found in ***SOFTWARE\Microsoft\Windows Portable Devices\Devices***. By comparing the GUID from this registry key with the Disk ID obtained from device identification, unique devices can be correlated with their names.

By combining the information gathered from these registry locations, a comprehensive understanding of connected USB devices can be achieved during the forensic analysis. This data aids in building a timeline of events and identifying potential evidence related to USB activity on the system. Answers to this section are in the notes.

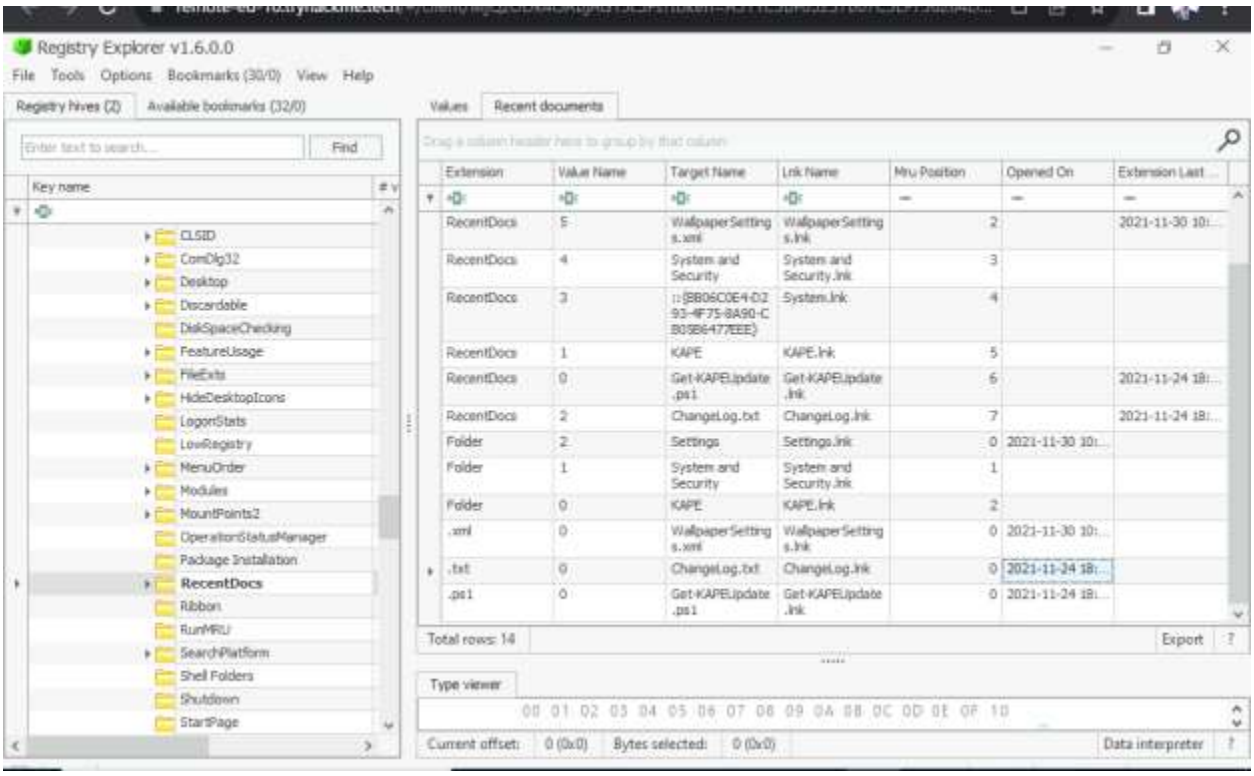
Task 10: Hands-on Challenge

The challenge presented in this challenge is a real-world scenario where we need to investigate a suspicious system at Organization X. Multiple user accounts and possible connections to network drives and USB devices are the focus of our investigation. We will utilize our knowledge of registry forensics and the provided tools like RegistryExplorer, EZViewer, and AppCompatCacheParser.exe to analyze the triage data and find answers to the questions. This exercise will put our registry forensics skills to the test and allow us to apply our learning in a practical context.

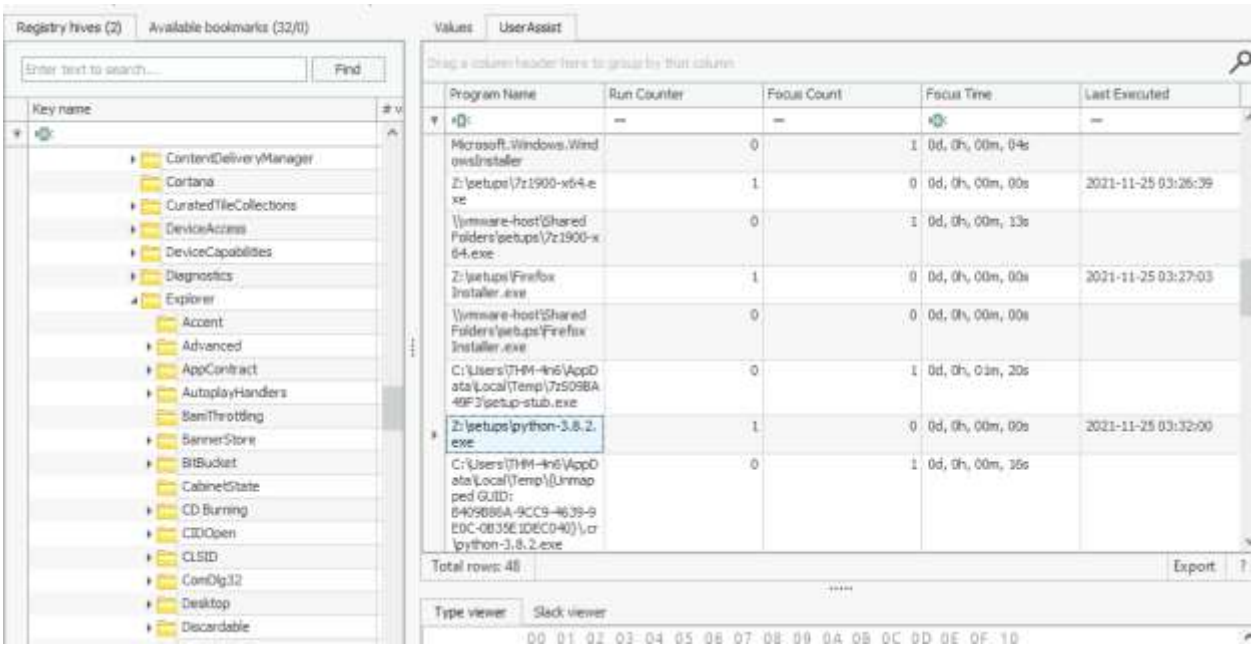
We are going to start by deploying the attached machine and after successful login we are going to start the registry explore and load the SAM hive. See the screenshot below to answer question 1, 2 and 3 in this section.



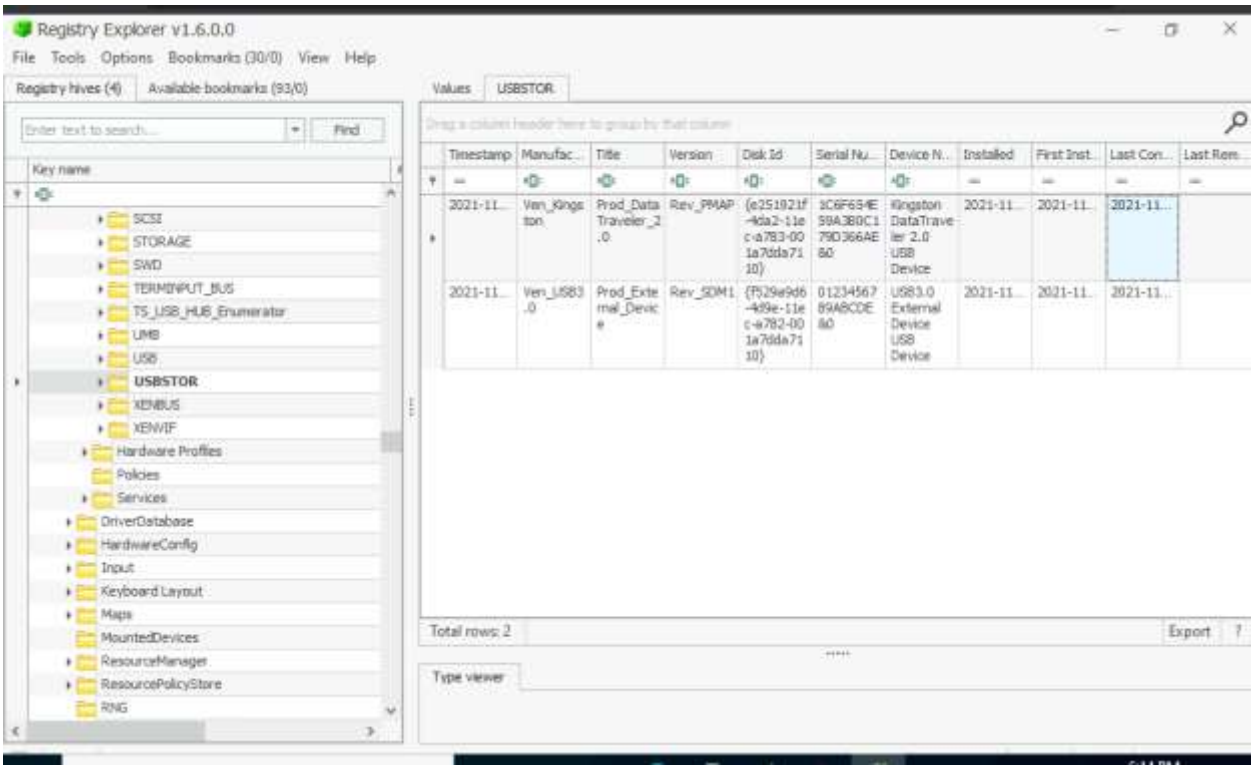
In question 4 we will be accessing the recent file located on ***NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs*** as described above.



To answer question 5, we are going to navigate to the userassist folder just below the recentdoc folder. Scroll down to find the path for python.exe.



For question 6, we are going to check the connected USB we can be found on ***SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USBSerial#\Properties.*** Since the system hive does not have the USB friendly name, load the software hive and check the friendly name with its Disk ID, which is available in the system hive.



Here is completion screenshot for this module.

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

Conclusion

Completing this Lab has been an enlightening experience. I have gained valuable insights into the intricacies of the Windows registry and its role in digital investigations. Learning how to identify and analyze important registry keys for system information, user accounts, and recent files has expanded my cybersecurity skillset. Additionally, exploring tools like RegistryExplorer and AppCompatCacheParser.exe has empowered me to efficiently extract and interpret valuable data.

This assignment has provided me with practical knowledge and confidence to tackle real-world scenarios in the field of digital forensics. I look forward to applying these skills to enhance cybersecurity practices and strengthen the security posture of organizations. The Windows Forensics 1 module has been an enriching journey, and I am excited to continue honing my expertise in this domain.