cs-sa07-24019
John_Mbithi_Mutave

Windows Forensics 1

Introduction

The Windows Registry is a critical component of the Windows operating system that stores configuration settings and options. Windows Forensics involves the analysis of the Windows Registry to gather evidence for digital investigations. This comprehensive report covers the tasks involved in understanding and utilizing Windows Registry forensics, providing insights and methodologies for effective forensic analysis.

Task 1: Introduction to Windows Forensics

This task provided an overview of Windows Forensics, highlighting the importance of the Windows Registry in digital investigations. It introduced fundamental concepts and set the stage for in-depth exploration of Registry forensics.

Task 2: Windows Registry and Forensics

In this task, the structure and purpose of the Windows Registry were examined. The Registry is divided into several hives, each containing keys and values that store configuration settings. Understanding the layout and content of these hives is crucial for forensic analysis.

Key points covered:

- Structure of the Windows Registry
- Common Registry hives: HKEY_LOCAL_MACHINE (HKLM), HKEY_CURRENT_USER (HKCU), etc.
- Importance of Registry data in forensic investigations

Task 3: Accessing Registry Hives Offline

This task demonstrated methods to access Registry hives from an offline system. This is particularly useful when dealing with a compromised or non-bootable system. Techniques included using tools like RegRipper and mounting Registry hives on another system.

Key points covered:

- Tools for accessing offline Registry hives
- Steps to mount and analyze Registry hives on a different system

Task 4: Data Acquisition

Data acquisition is a critical step in any forensic investigation. This task focused on acquiring Registry hives from a target system. Methods for securely copying Registry hives and ensuring data integrity were discussed.

Key points covered:

- Techniques for acquiring Registry hives
- Ensuring data integrity during acquisition

Task 5: Exploring Windows Registry

This task involved hands-on exploration of the Windows Registry. Various tools and techniques for navigating and interpreting Registry data were introduced. Practical exercises helped solidify the understanding of Registry structure and content.

Key points covered:

- Tools for exploring the Windows Registry
- Practical exercises in navigating and interpreting Registry data

Task 6: System Information and System Accounts

Analyzing system information and user accounts stored in the Registry provides valuable insights into system configuration and user activity. This task covered methods for extracting and interpreting this information.

Key points covered:

- Extracting system information from the Registry
- Analyzing user accounts and related data

Task 7: Usage or Knowledge of Files/Folders

The Registry stores information about files and folders accessed by users. This task focused on identifying and interpreting this data to understand user behavior and potential evidence of malicious activity.

Key points covered:

- Identifying files and folders accessed by users
- Interpreting Registry data related to file and folder usage

Task 8: Evidence of Execution

Understanding what programs have been executed on a system can be critical in forensic investigations. This task explored how to find evidence of program execution within the Registry.

Key points covered:

- Identifying executed programs from Registry data
- Interpreting evidence of execution for forensic analysis

Task 9: External Devices/USB Device Forensics

Information about external devices, such as USB drives, is stored in the Registry. This task covered methods for identifying and analyzing data related to external devices to understand device usage and potential data transfer.

Key points covered:

- Identifying connected external devices from Registry data
- Analyzing data related to USB device usage

Task 10: Hands-on Challenge

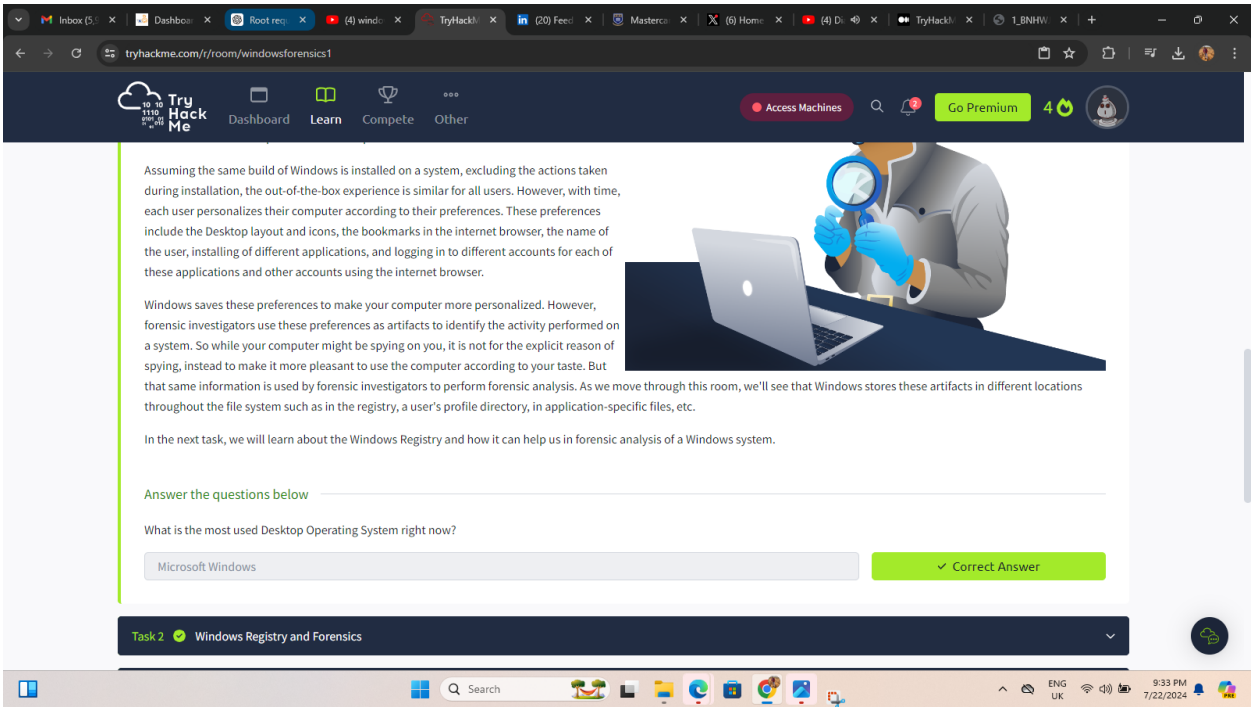
A hands-on challenge provided practical experience in applying the skills and knowledge gained from the previous tasks. This task involved real-world scenarios requiring forensic analysis of the Windows Registry to gather evidence.

Key points covered:

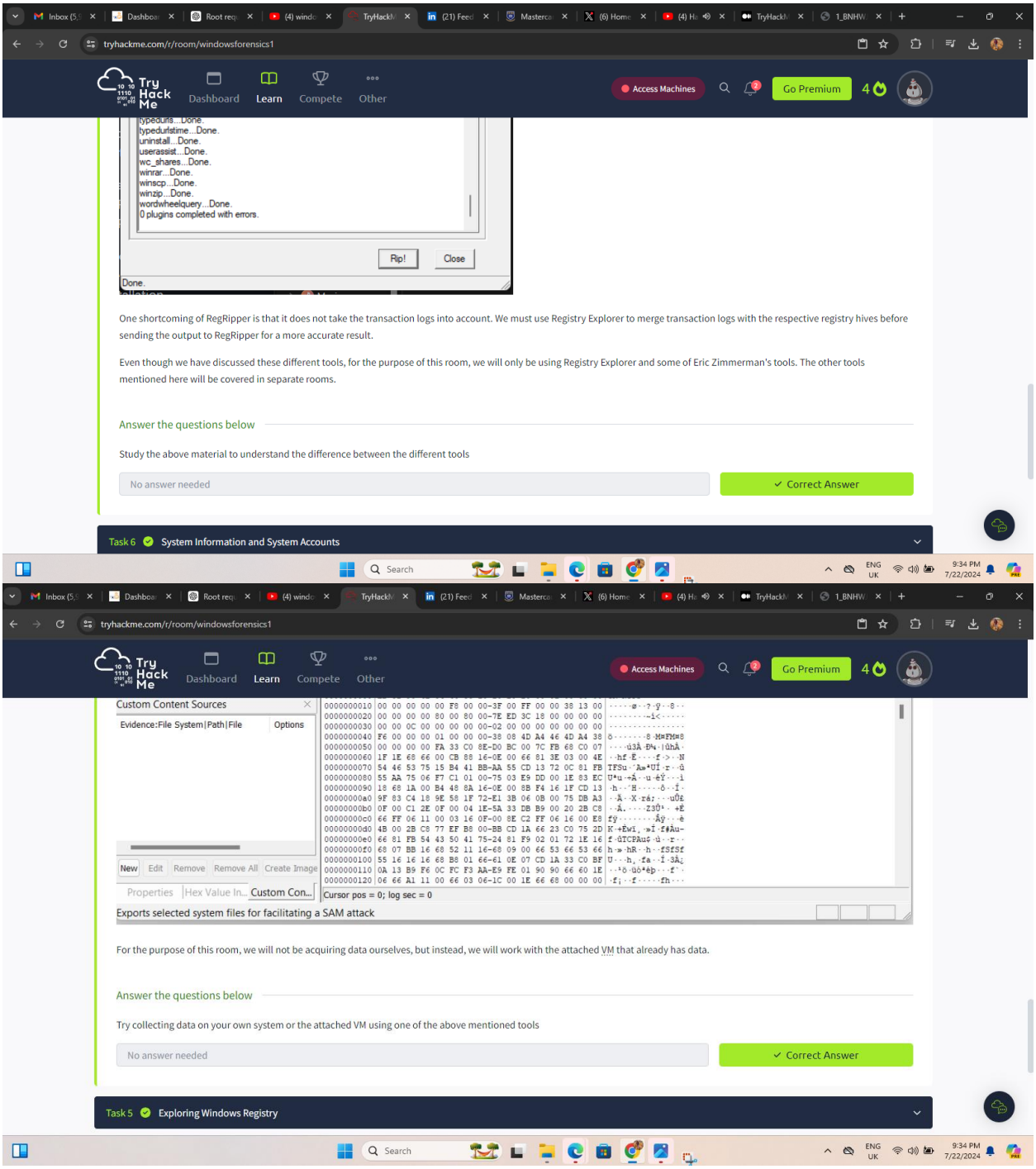
- Practical application of Registry forensic techniques
- Real-world scenarios for evidence gathering

cs-sa07-24019
John_Mbithi_Mutave

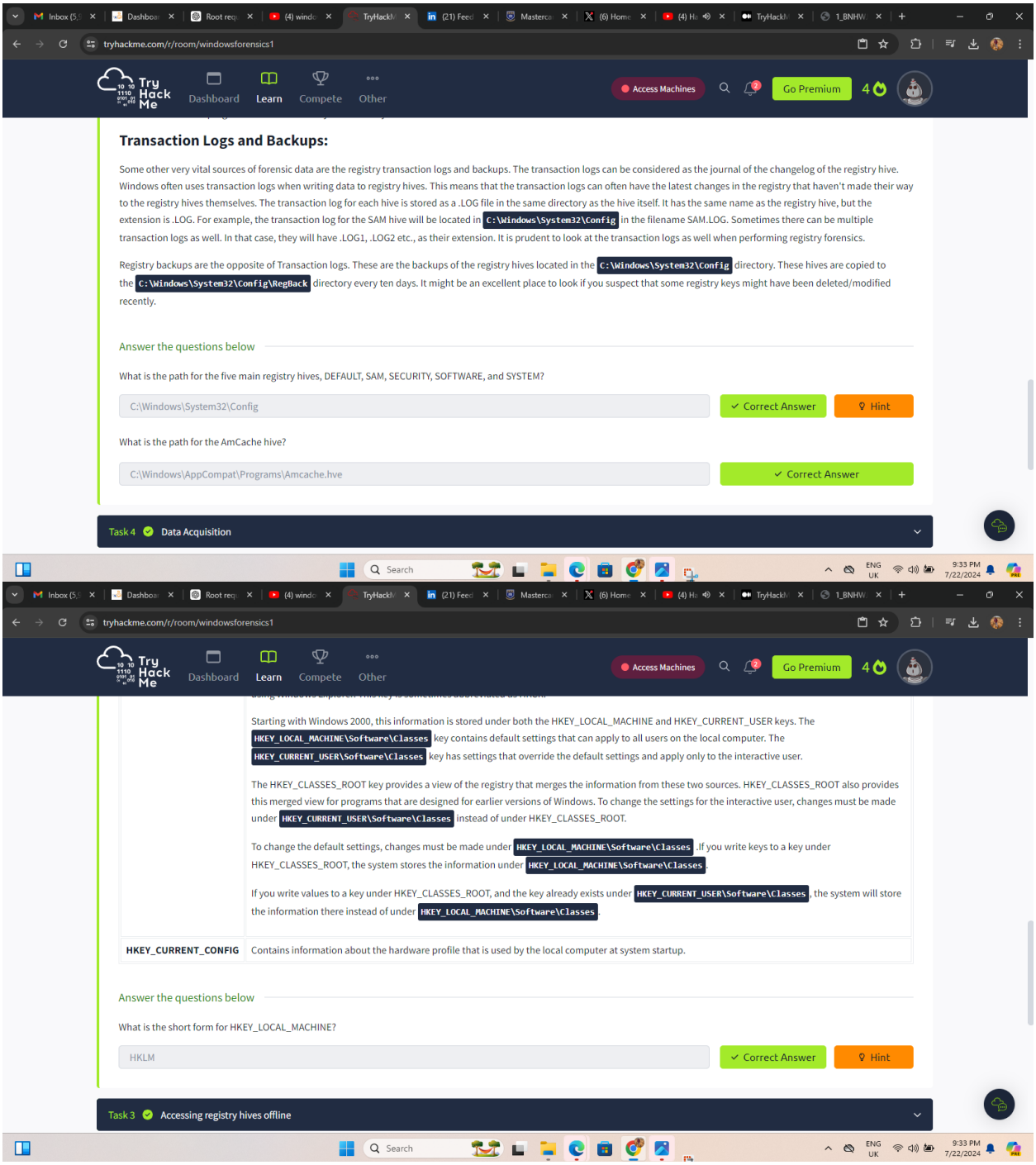
Screenshot Overview of the Task



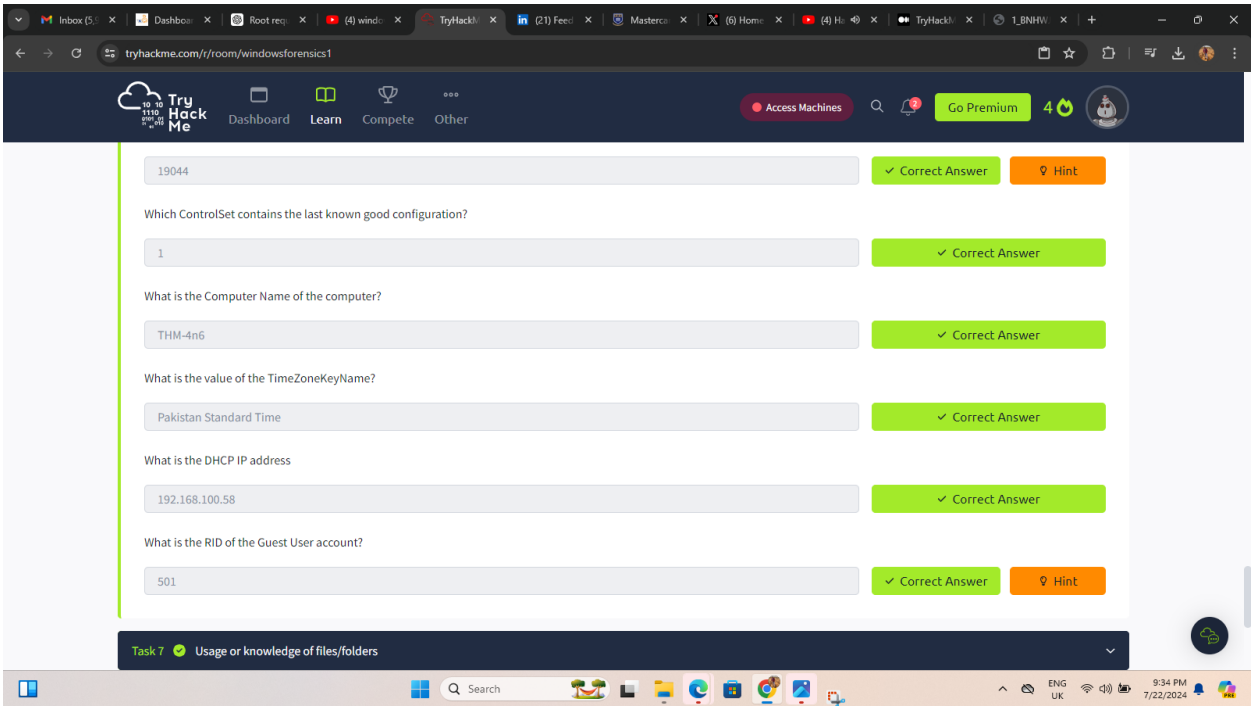
cs-sa07-24019
John_Mbithi_Mutave



cs-sa07-24019
John_Mbithi_Mutave

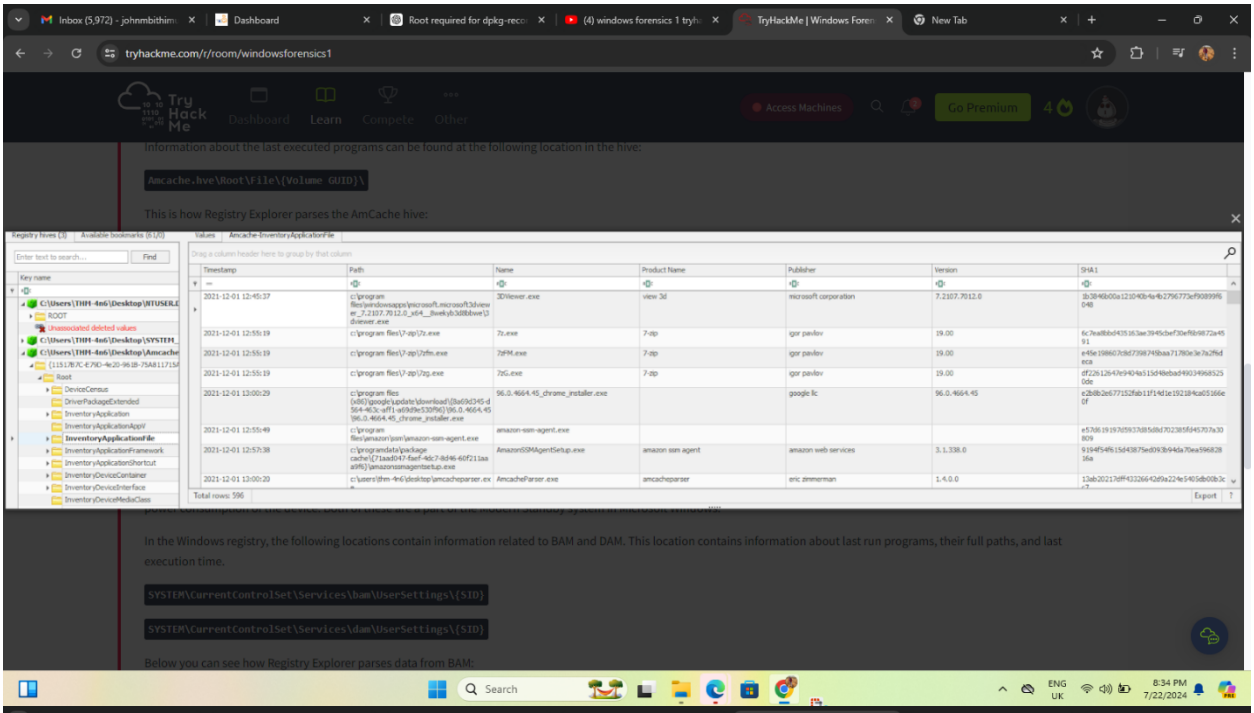


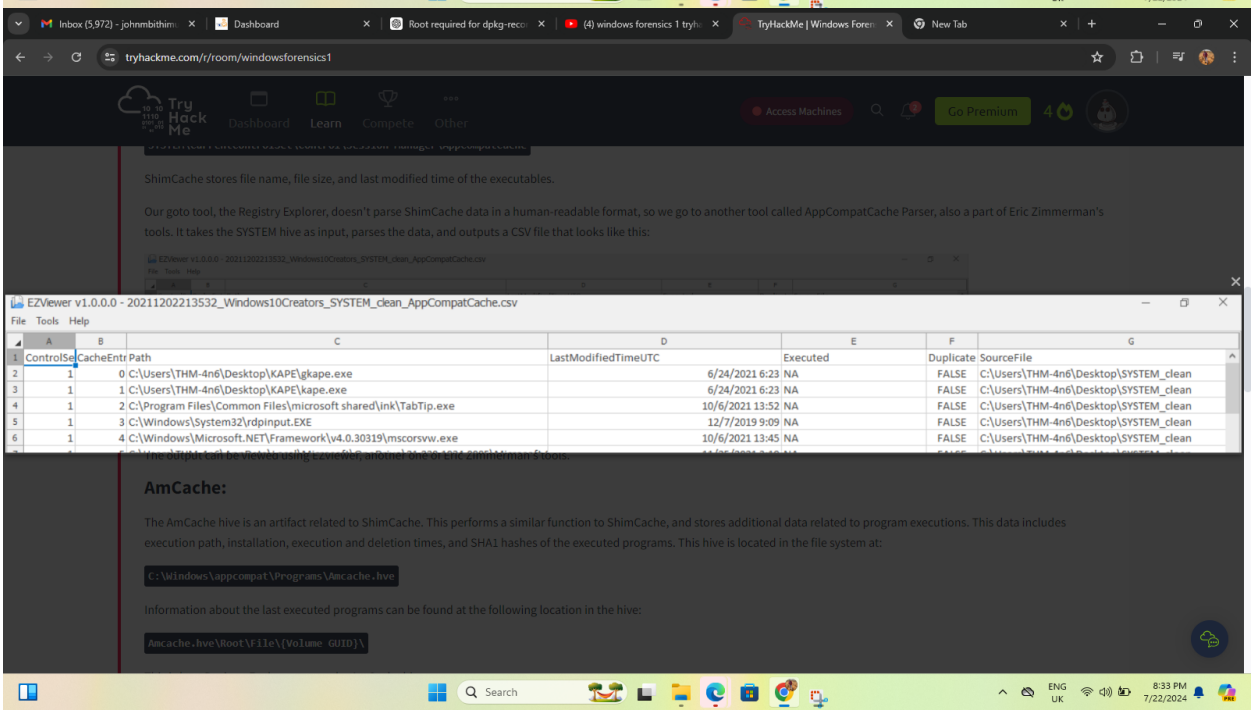
cs-sa07-24019
John_Mbithi_Mutave



cs-sa07-24019

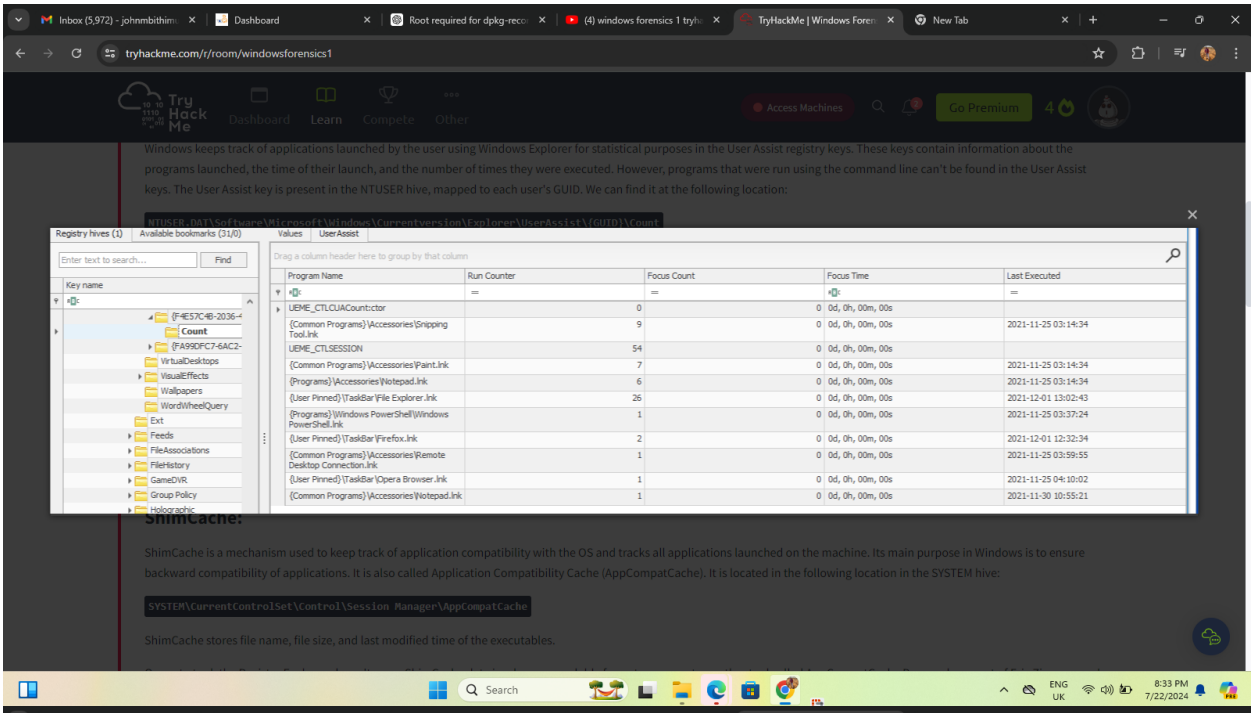
John_Mbithi_Mutave

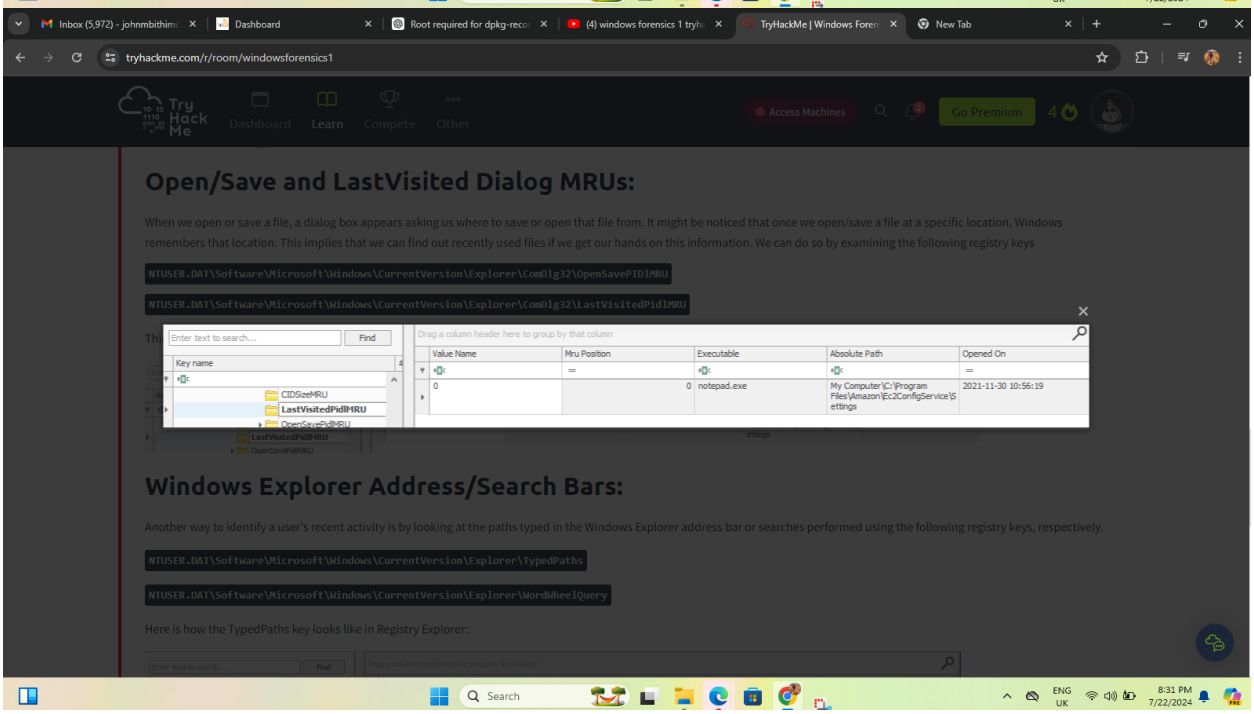




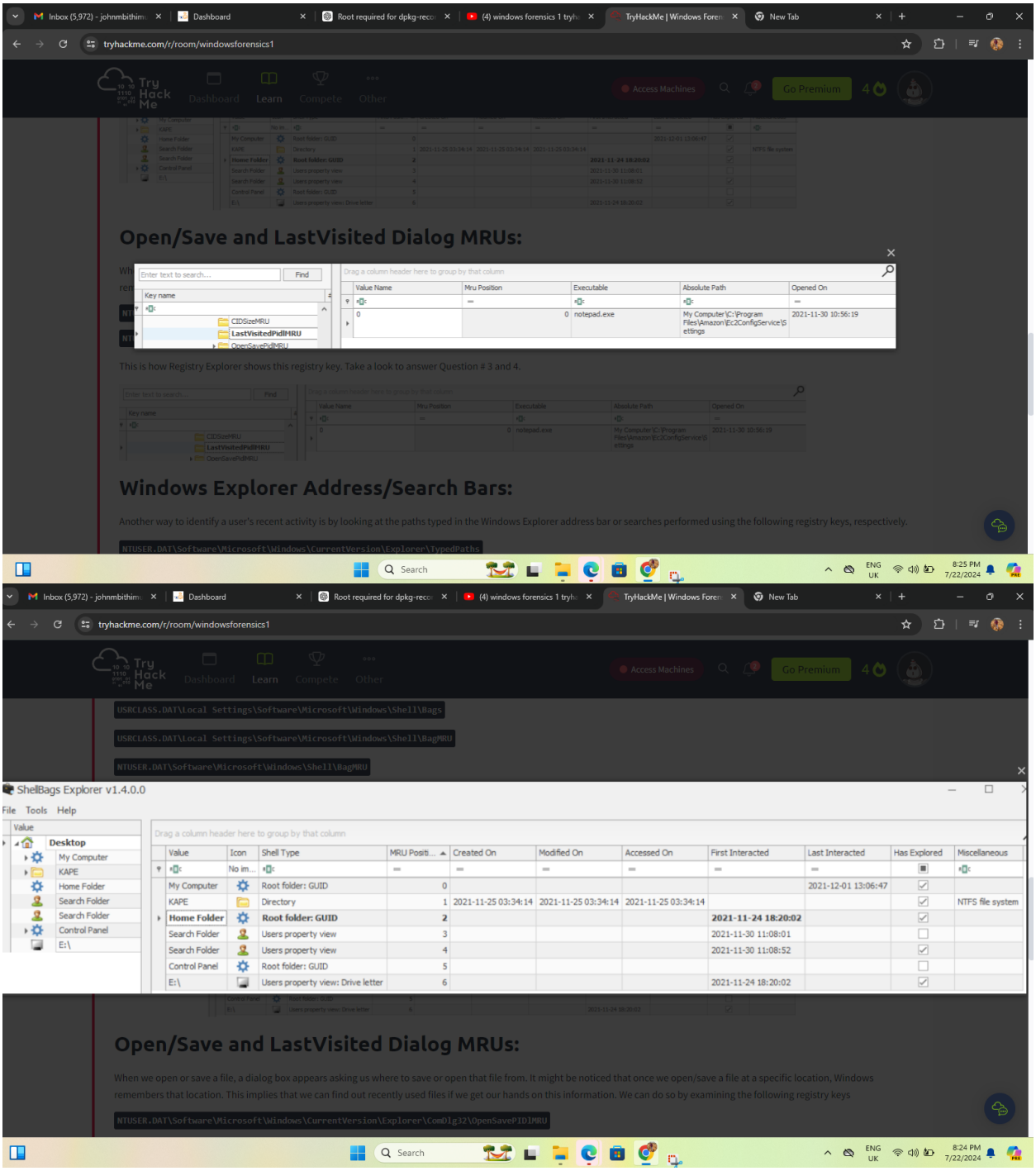
cs-sa07-24019

John_Mbithi_Mutave

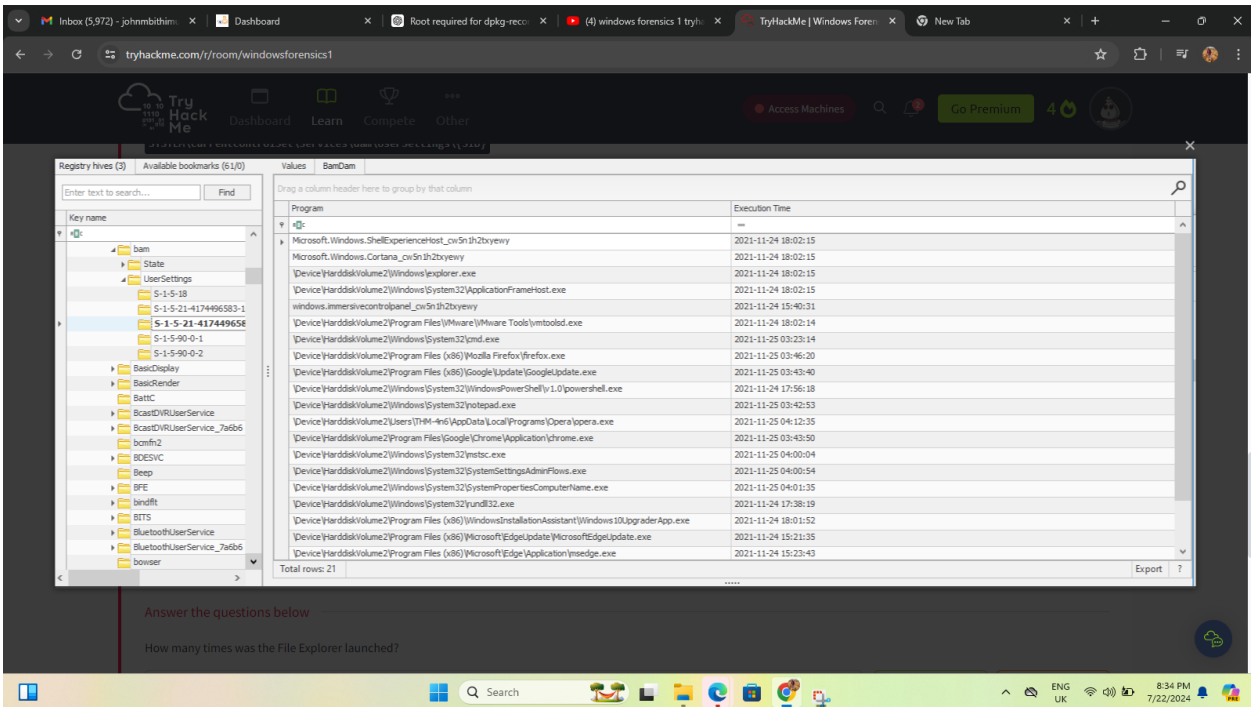


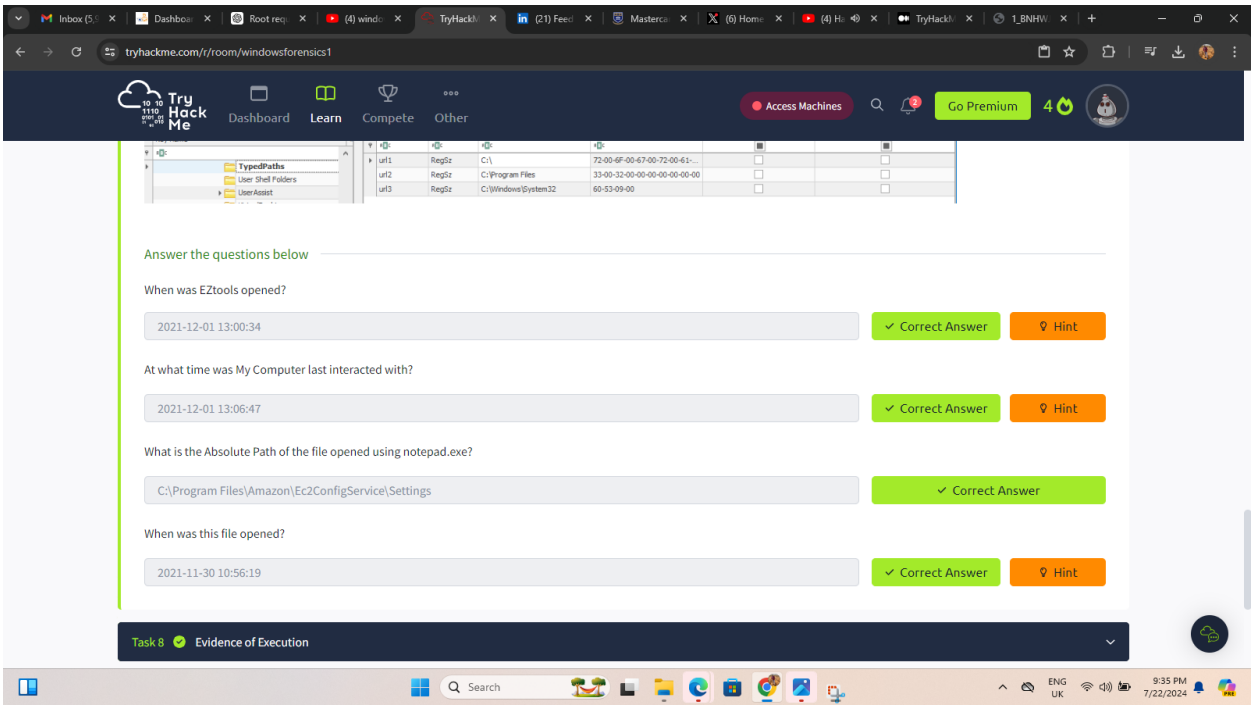


cs-sa07-24019
John_Mbithi_Mutave

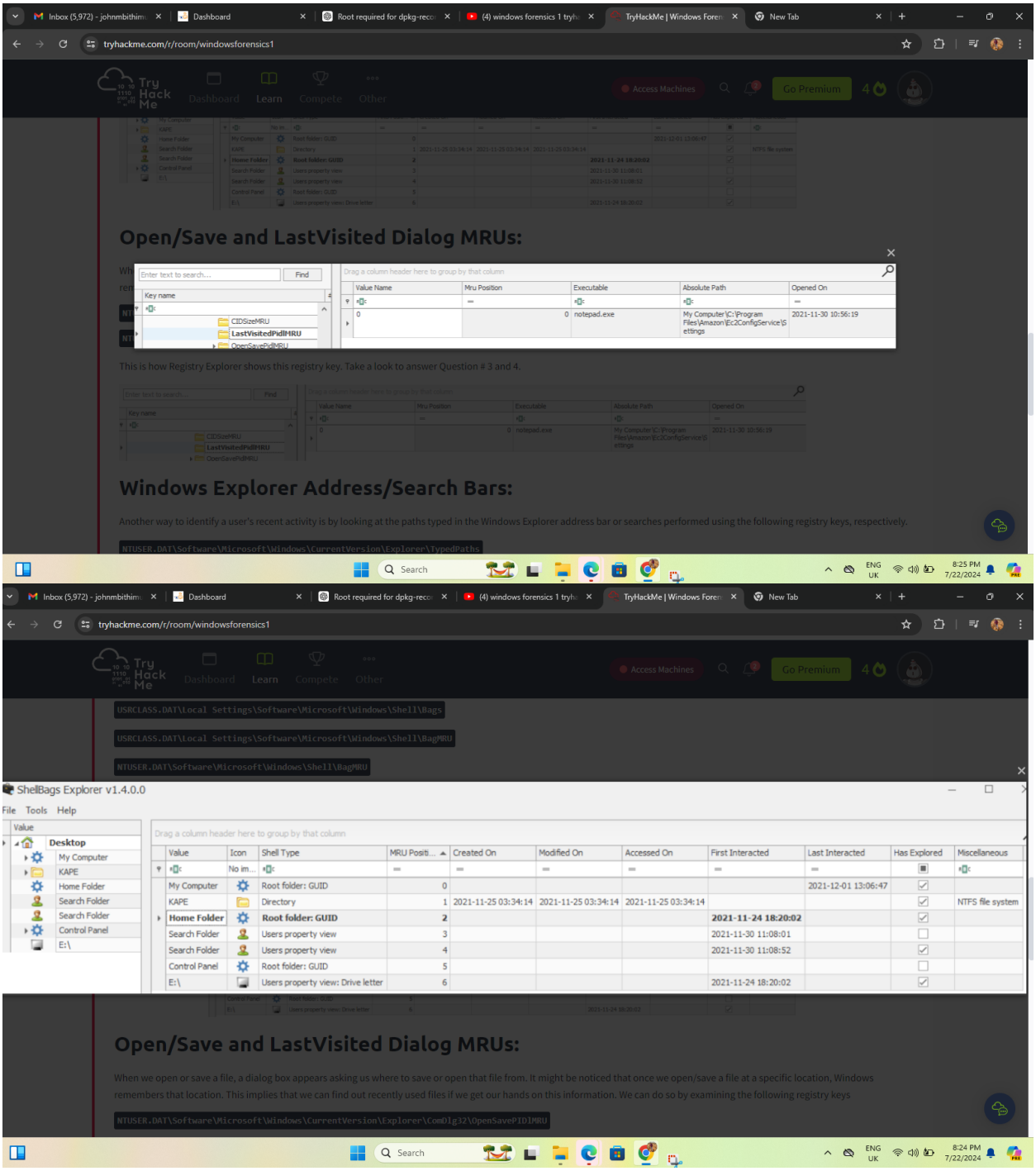


cs-sa07-24019
John_Mbithi_Mutave

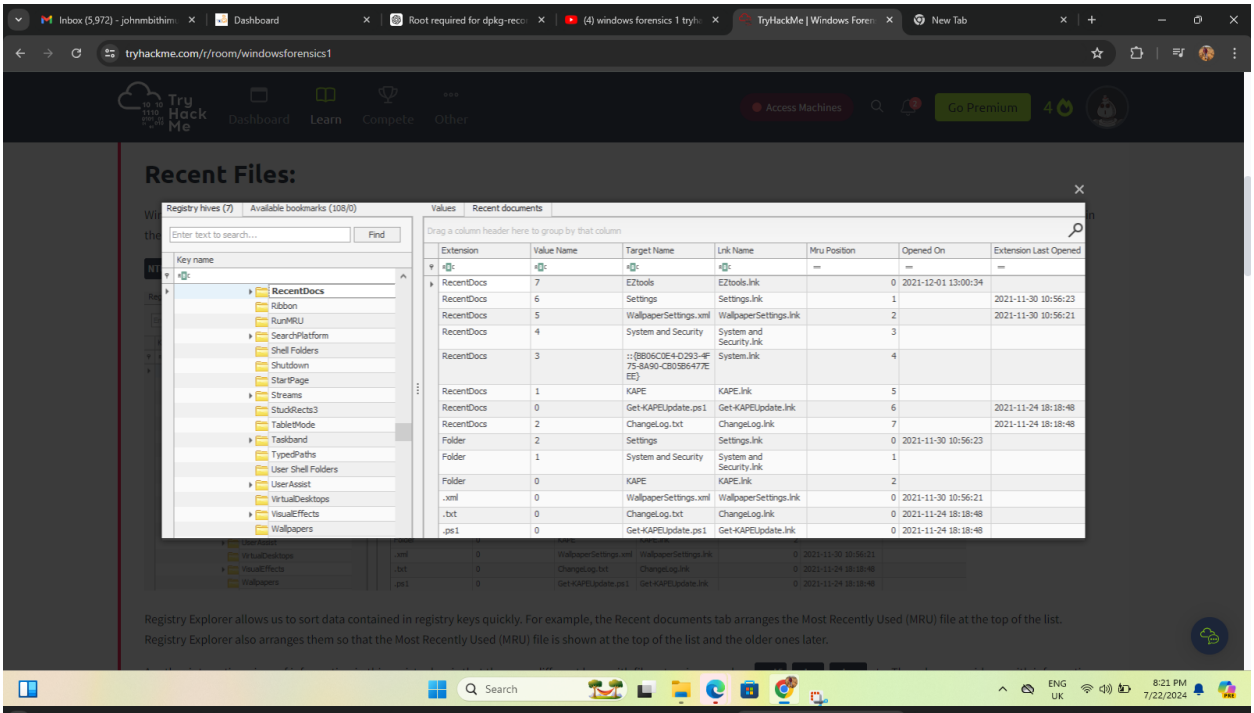


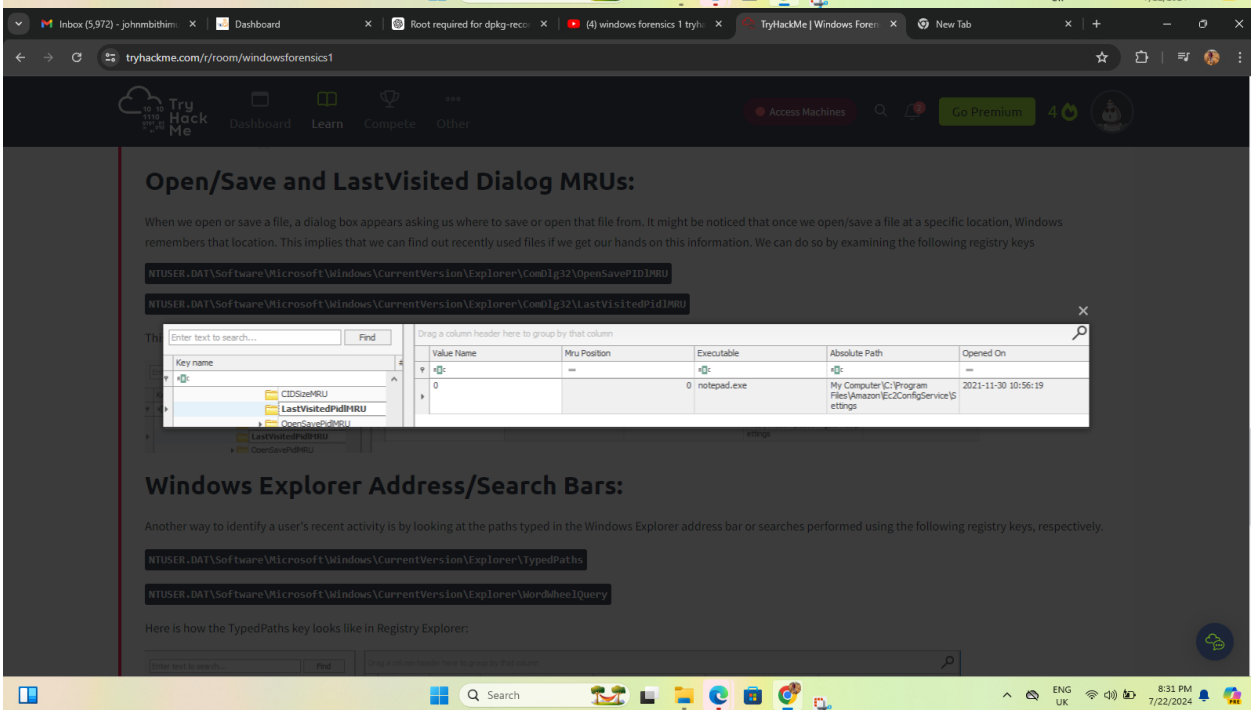


cs-sa07-24019
John_Mbithi_Mutave

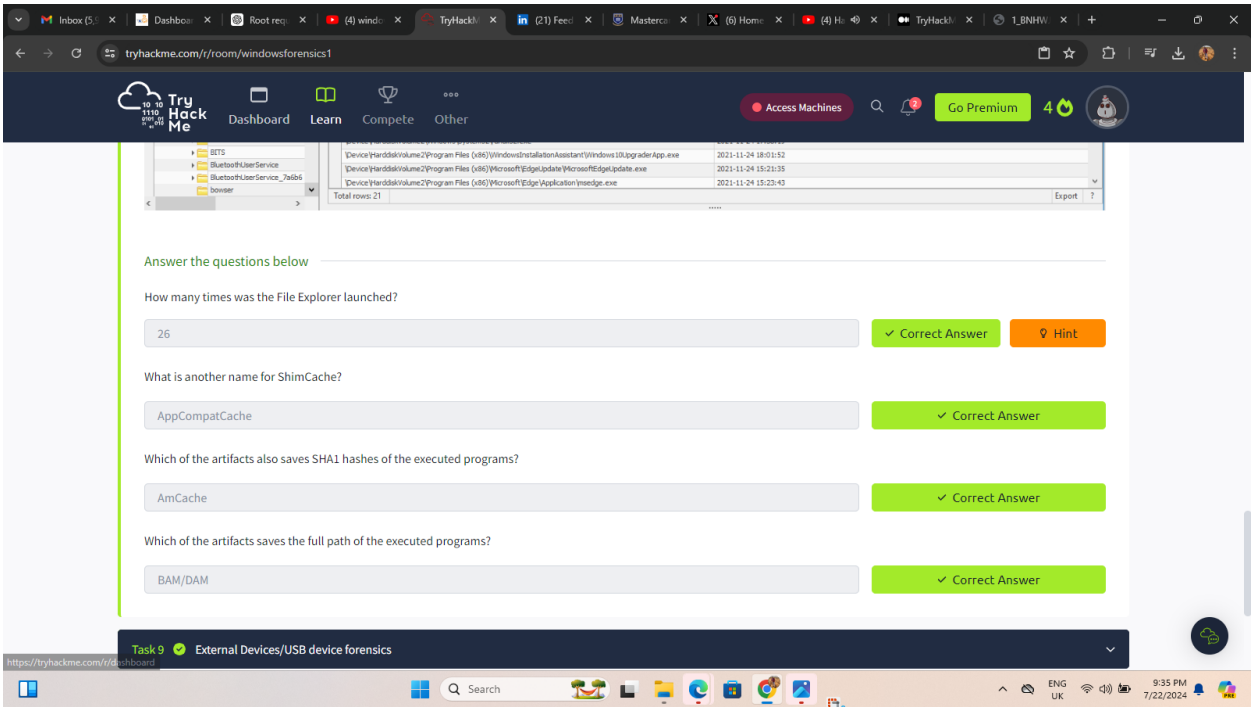


cs-sa07-24019
John_Mbithi_Mutave



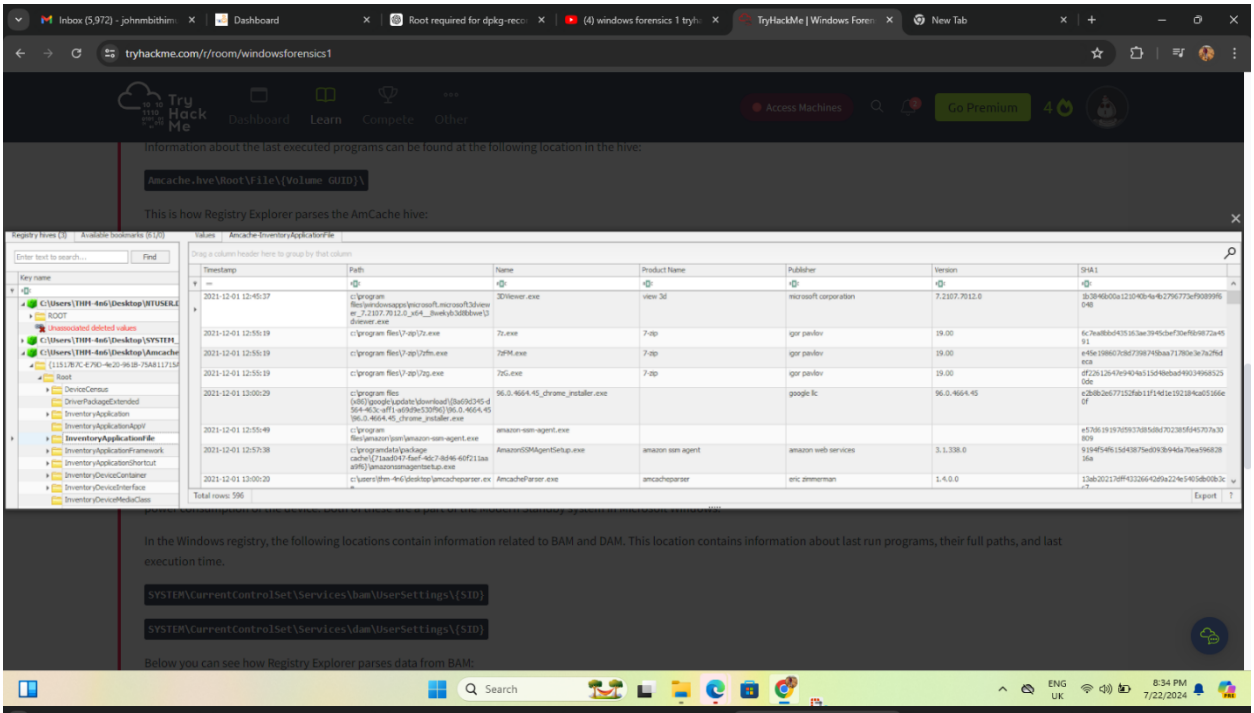


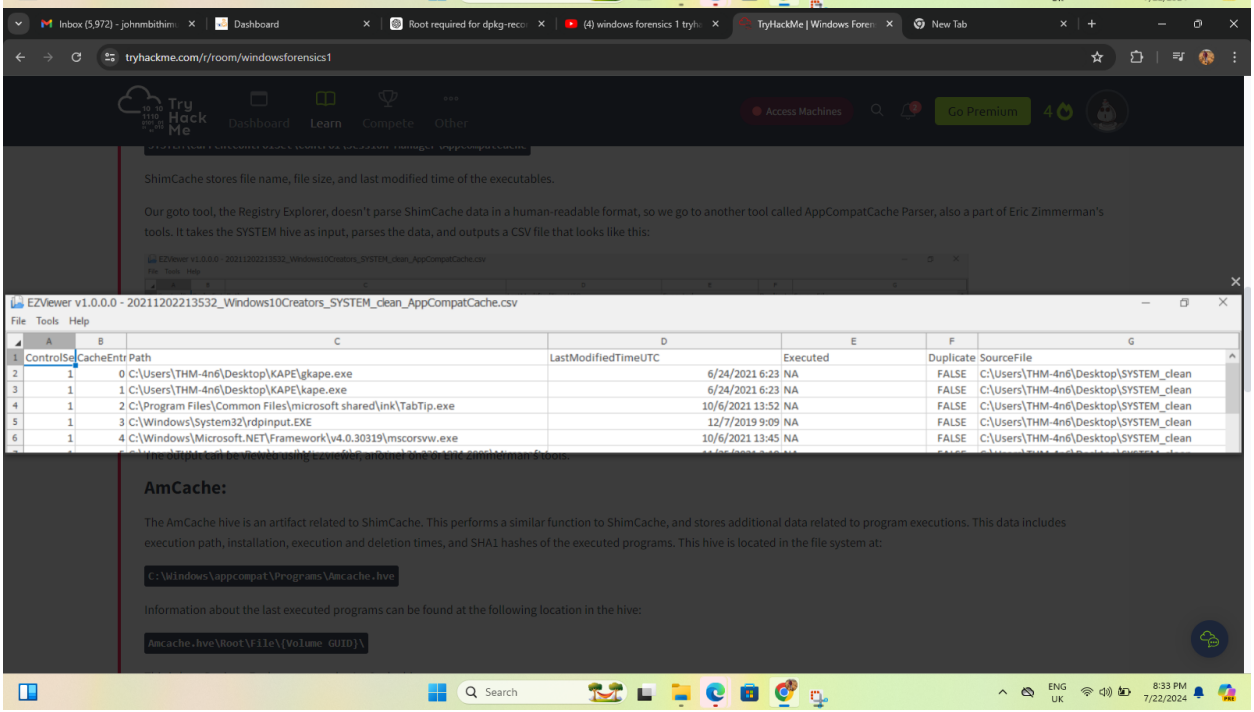
cs-sa07-24019
John_Mbithi_Mutave



cs-sa07-24019

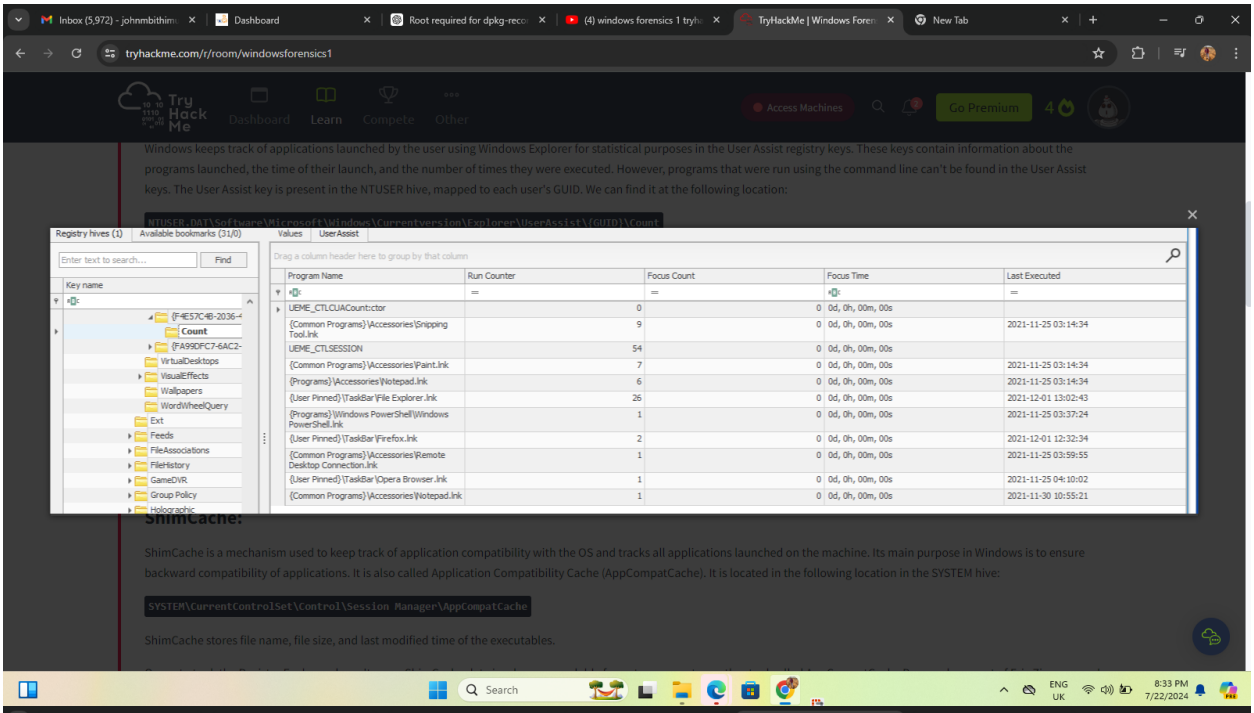
John_Mbithi_Mutave

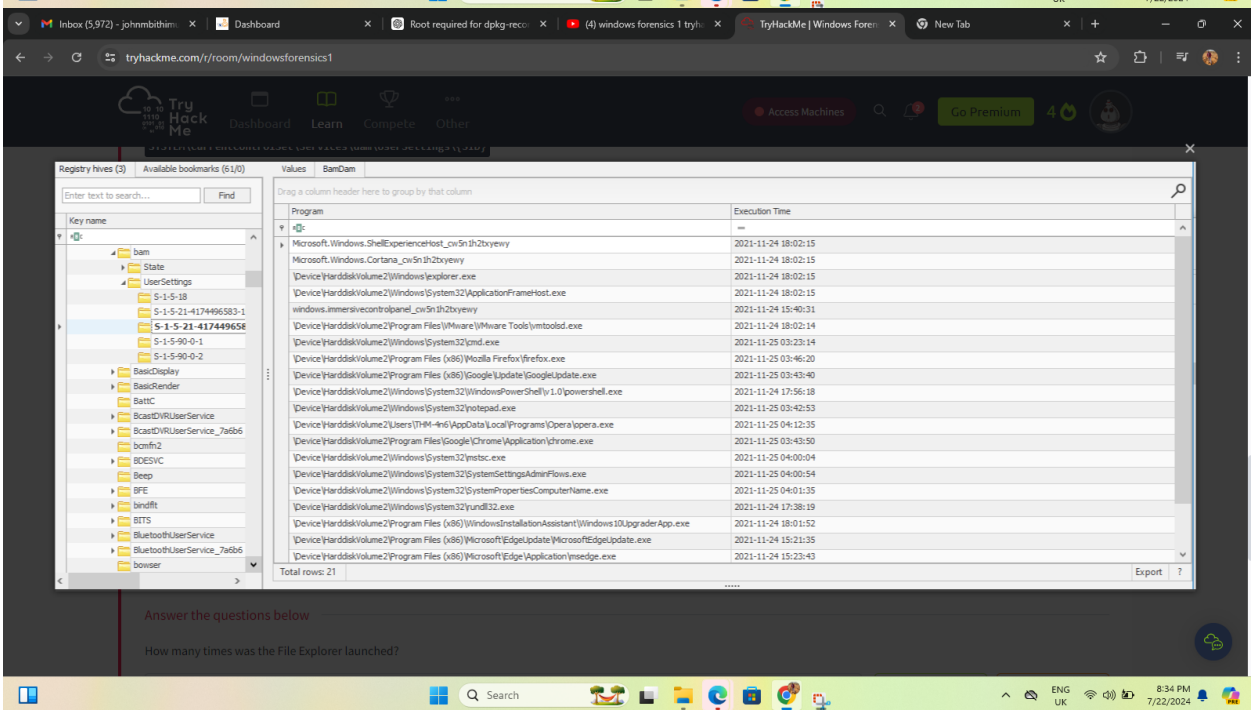




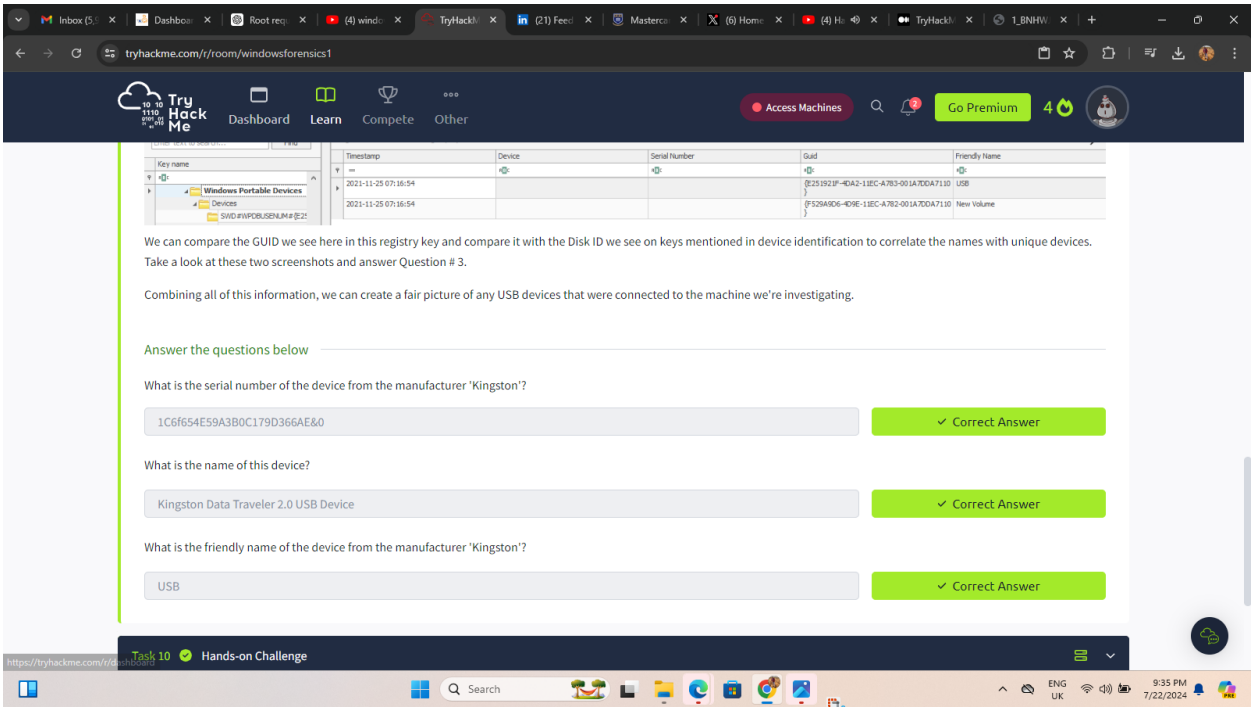
cs-sa07-24019

John_Mbithi_Mutave

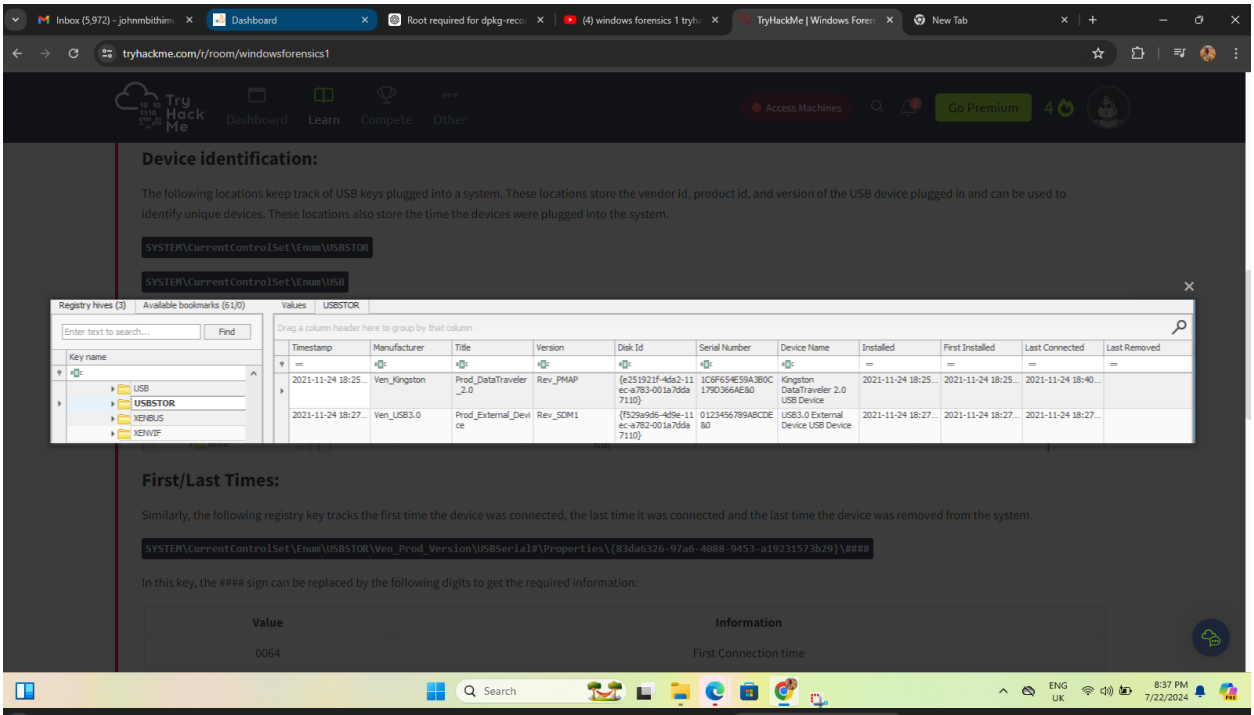


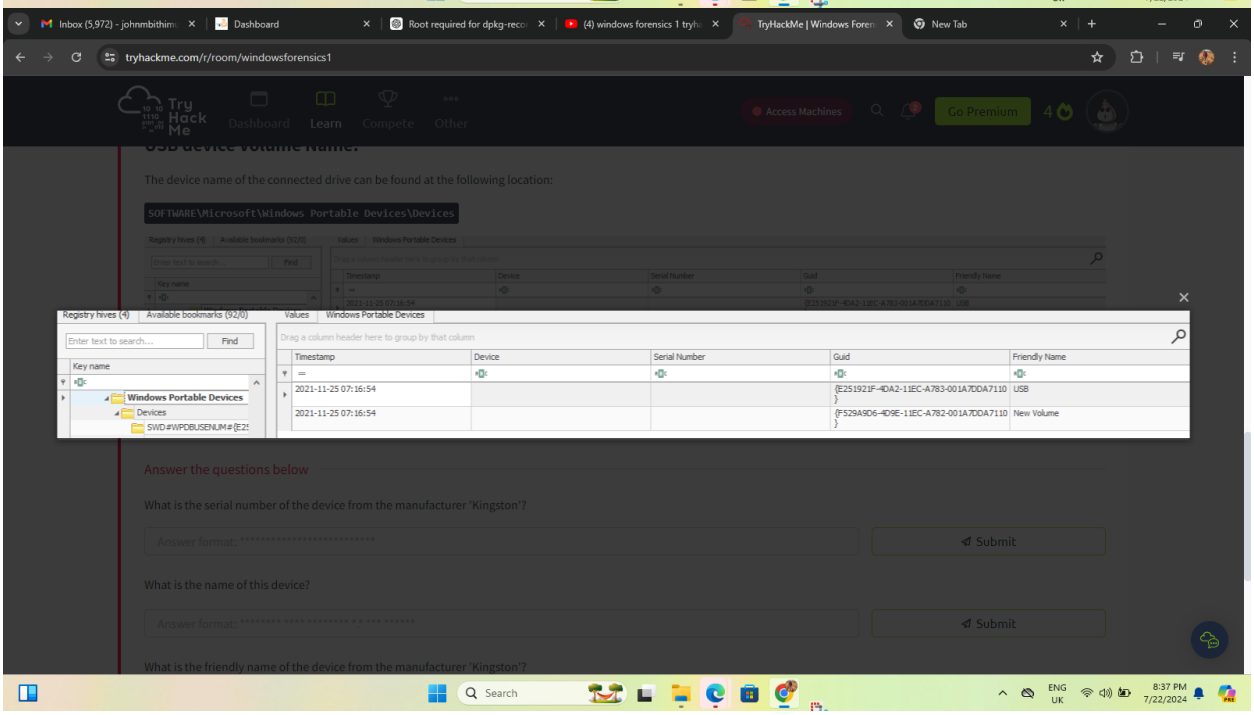


cs-sa07-24019
John_Mbithi_Mutave

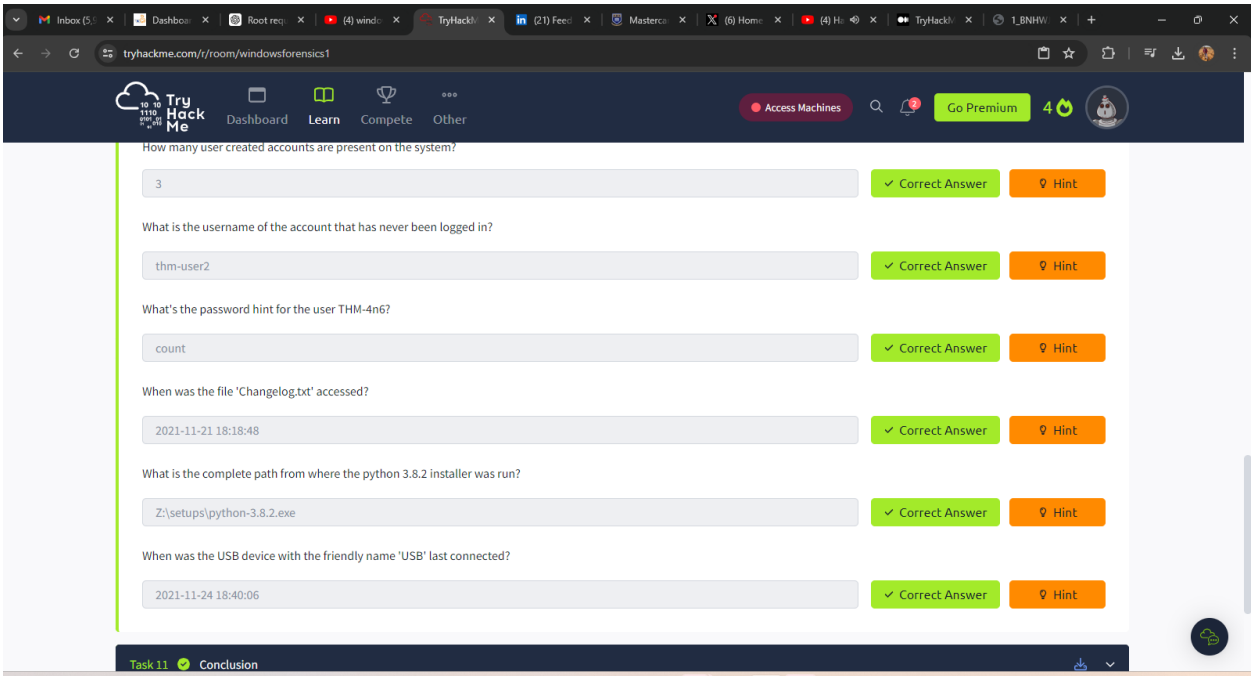


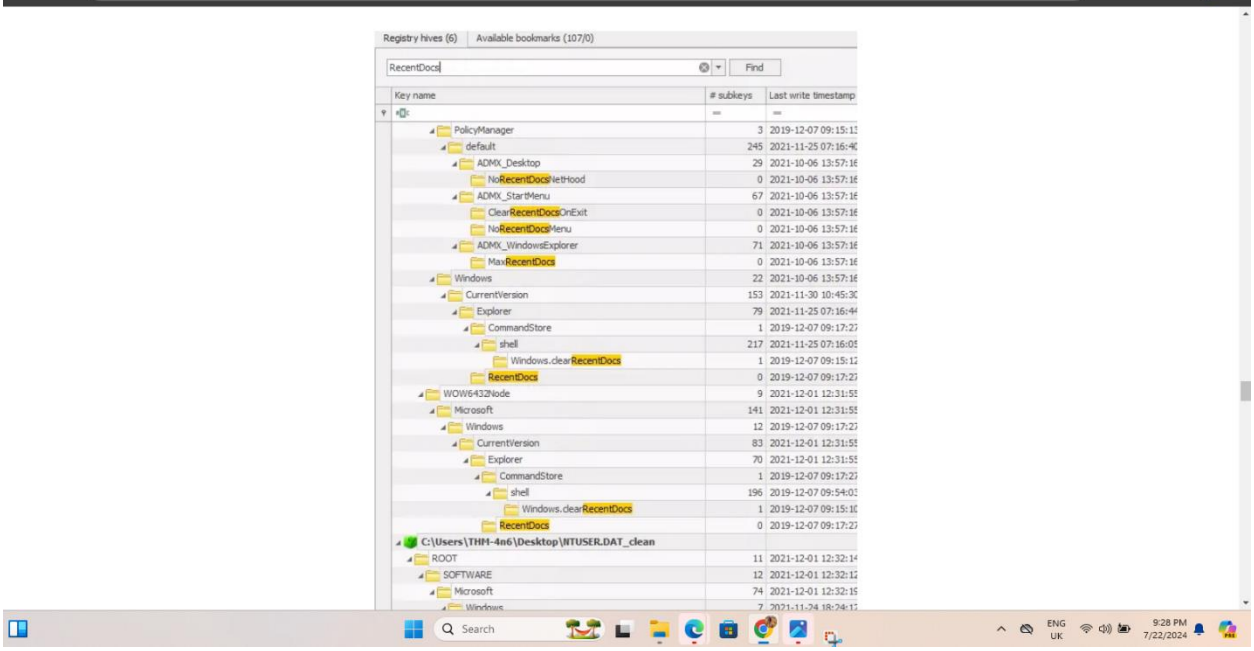
cs-sa07-24019
John_Mbithi_Mutave



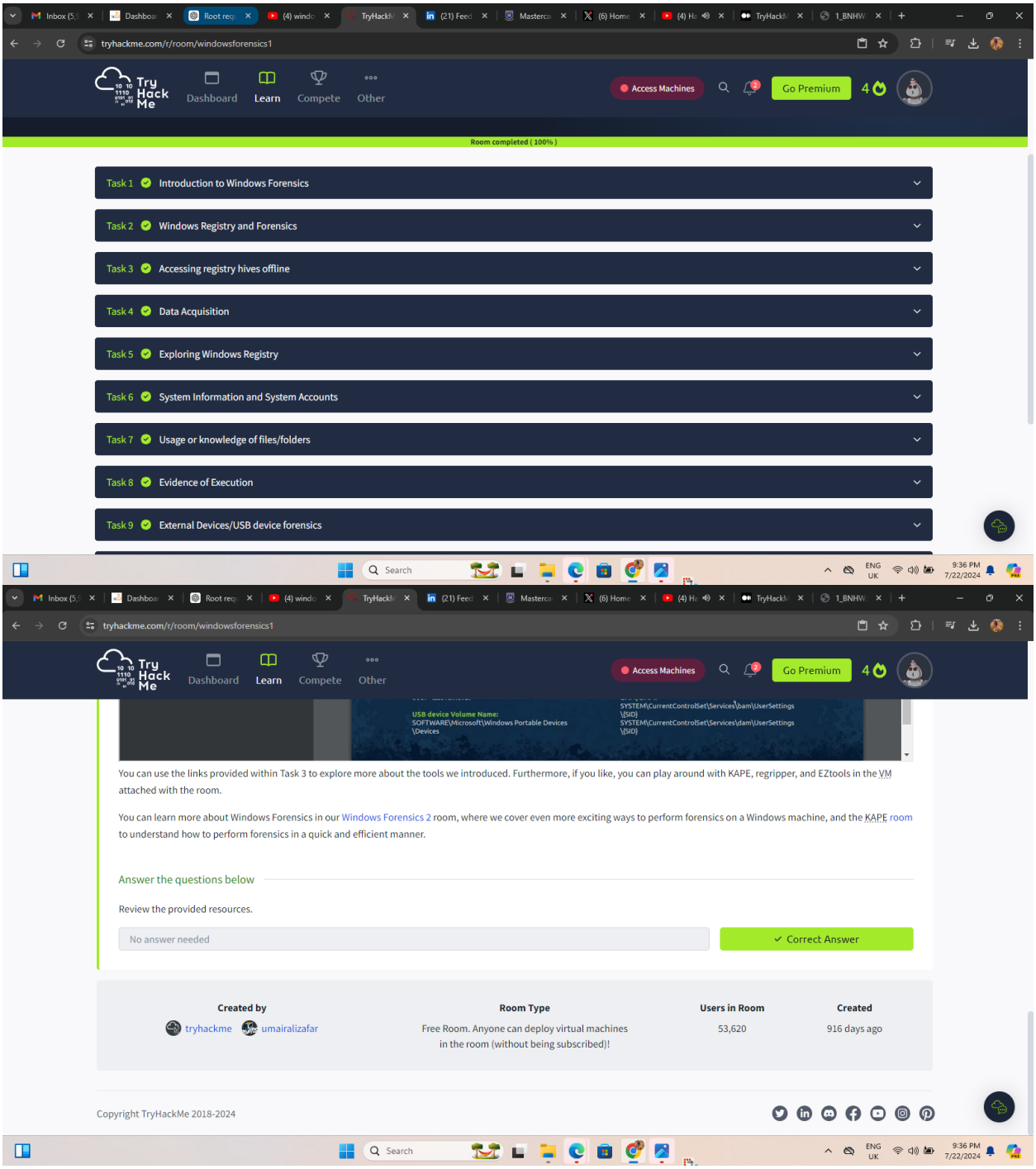


cs-sa07-24019
John_Mbithi_Mutave

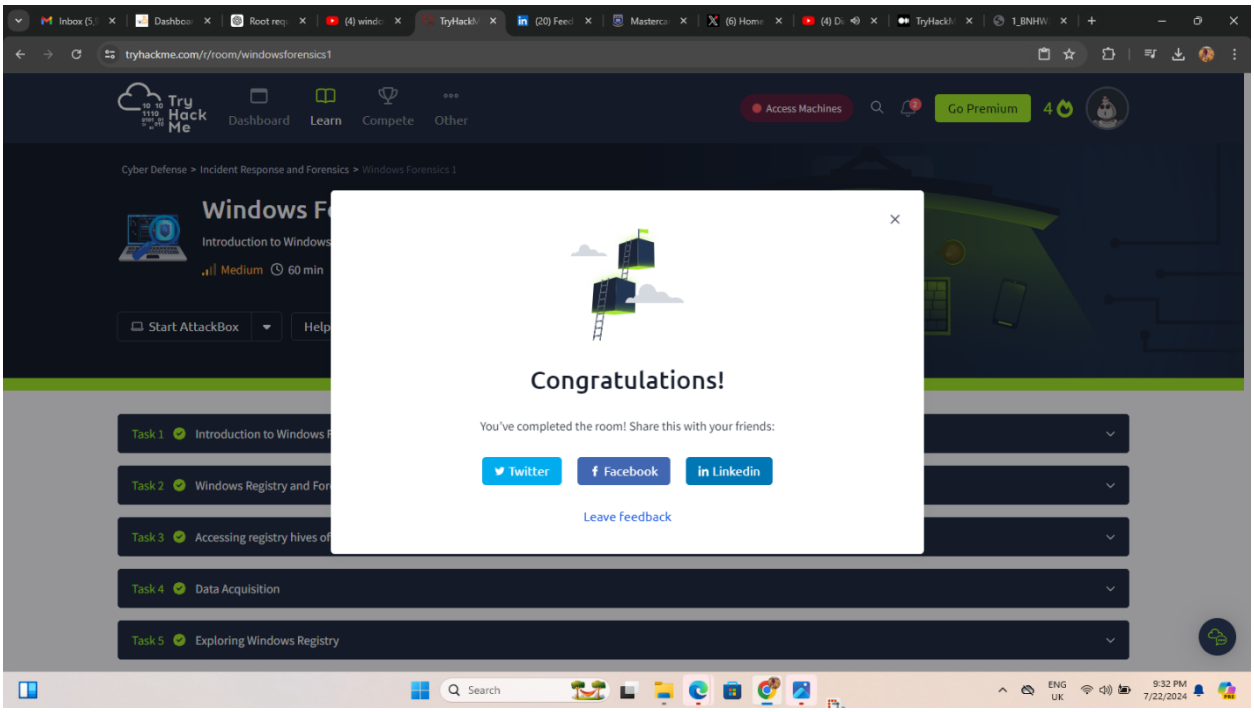




cs-sa07-24019
John_Mbithi_Mutave



cs-sa07-24019
John_Mbithi_Mutave



Shareable Link - https://tryhackme.com/r/room/windowsforensics1

Conclusion

The Windows Forensics 1 course provided a comprehensive understanding of the Windows Registry and its role in digital forensics. By exploring various tasks, participants gained valuable skills in accessing, analyzing, and interpreting Registry data. These skills are crucial for conducting thorough and effective forensic investigations, ultimately aiding in the pursuit of justice and cybersecurity.