Windows Forensics 1

-

Room Walkthrough

Paweł Murdzek, Piotr Szewczyk

Warsaw University of Technology

26 stycznia 2026

Spis treści

Introduction

This document provides a walkthrough for the challenge category "Windows Forensics 1" on the TryHackMe platform.

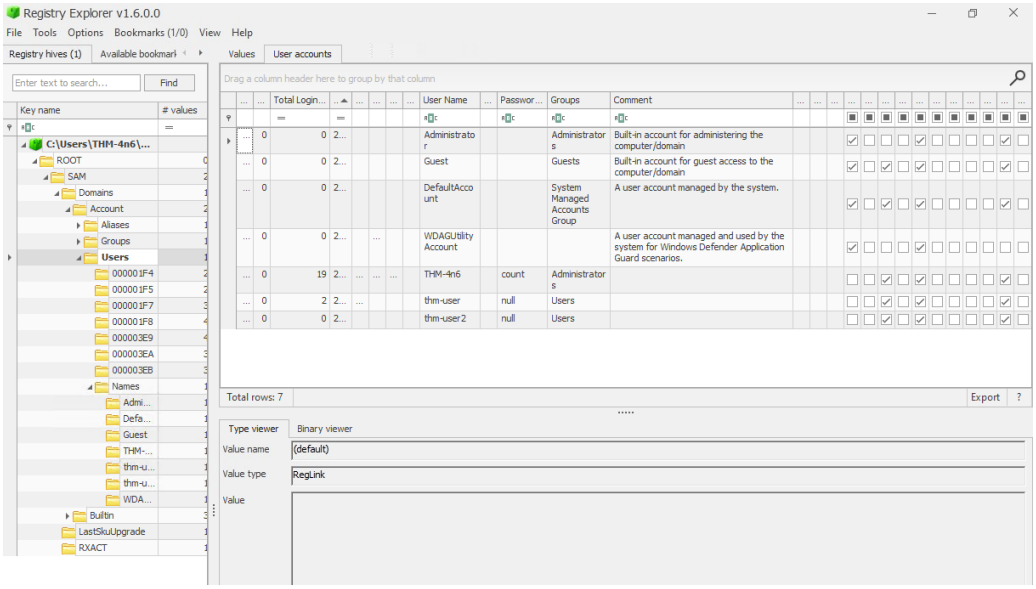
1. Windows Forensics 1 (TryHackMe)

1.1. Lab Description

The task involved learning tools for investigation in Windows system other than Autopsy.

1.2. Analysis and Answers

1. **How many user created accounts are present on the system?**
   Answer: 3 - 1 administrator and 2 users.

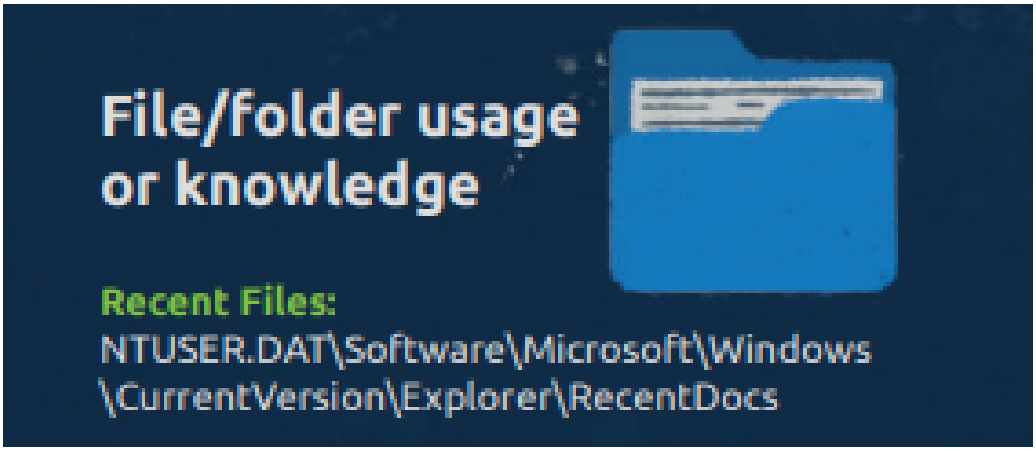


Rysunek 1: User registry from SAM profile.

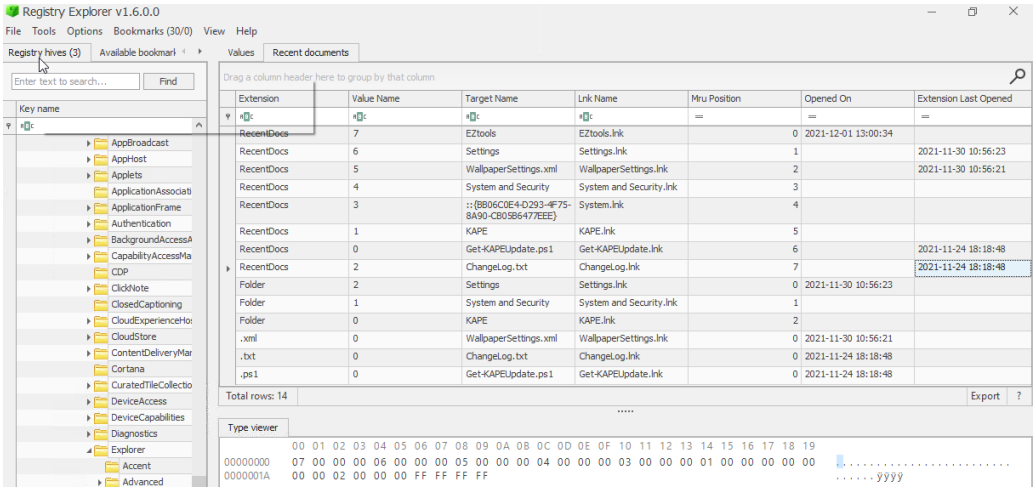
2. **What is the username of the account that has never been logged in?**
   Answer: thm-user2
3. **What's the password hint for the user THM-4n6?**
   Answer: count
4. **When was the file 'Changelog.txt' accessed?**
   Answer: 2021-11-24 18:18:48
5. **What is the complete path from where the python 3.8.2 installer was run?**
   Answer: z:
   setups
   python-3.8.2.exe
6. **When was the USB device with the friendly name 'USB' last connected?**
   Answer: 2021-11-24 18:40:06

1.3. Conclusions

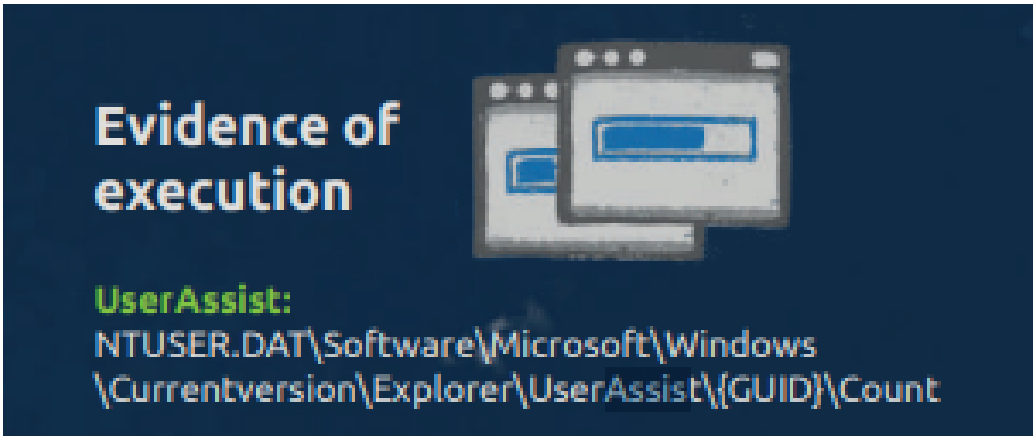
The analysis allowed identifying recent activity on the device. Registry Explorer handles log reproduction well. The tool works quite similarly to Autopsy, although personally



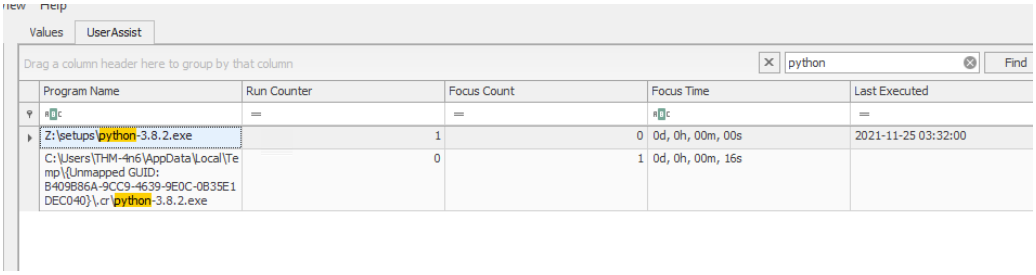
Rysunek 2: Hint on where to search for recently used files.



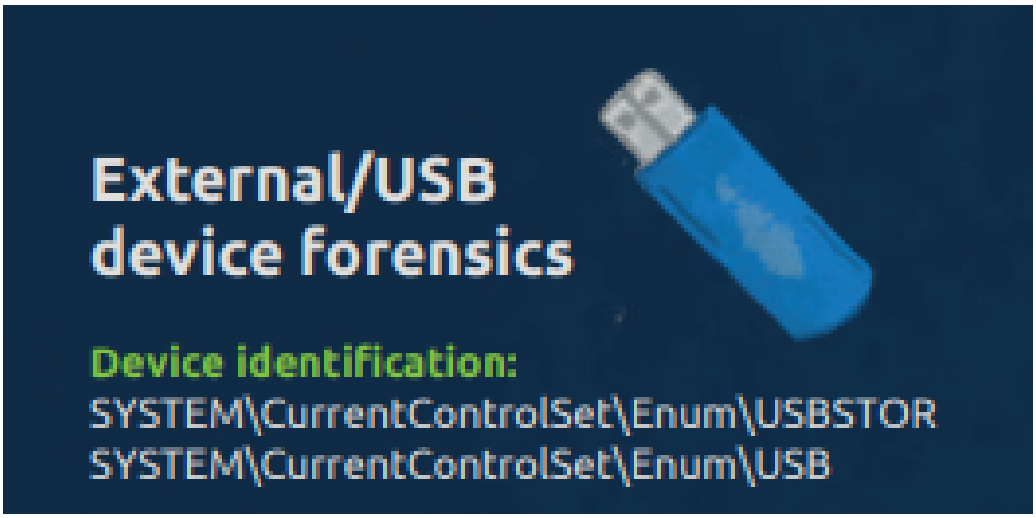
Rysunek 3: Registry of recent files.



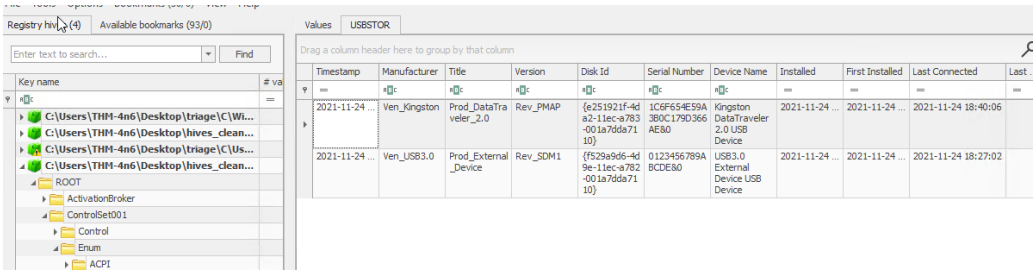
Rysunek 4: Hint on where to search for recently executed files.



Rysunek 5: Searching for Python application.



Rysunek 6: Hint on where to search for recently connected USBs.



Rysunek 7: USBTOR list.