

Windows Forensics 1

-

Room Walkthrough

Paweł Murdzek, Piotr Szewczyk

Warsaw University of Technology

26 stycznia 2026

Spis treści

| | |
|---|---|
| Introduction | 2 |
| 1. Windows Forensics 1 (TryHackMe) | 2 |
| 1.1. Lab Description | 2 |
| 1.2. Analysis and Answers | 2 |
| 1.3. Conclusions | 2 |

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.

| Total Login... | User Name | Password... | Groups | Comment |
|----------------|---------------------|-------------|-------------------------------|---|
| 0 | Administrator | | Administrators | Built-in account for administering the computer/domain |
| 0 | Guest | | Guests | Built-in account for guest access to the computer/domain |
| 0 | DefaultAcco... | | System Managed Accounts Group | A user account managed by the system. |
| 0 | WDAGUtility Account | | | A user account managed and used by the system for Windows Defender Application Guard scenarios. |
| 19 | THM-4n6 | count | Administrators | |
| 2 | thm-user | null | Users | |
| 0 | thm-user2 | null | 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

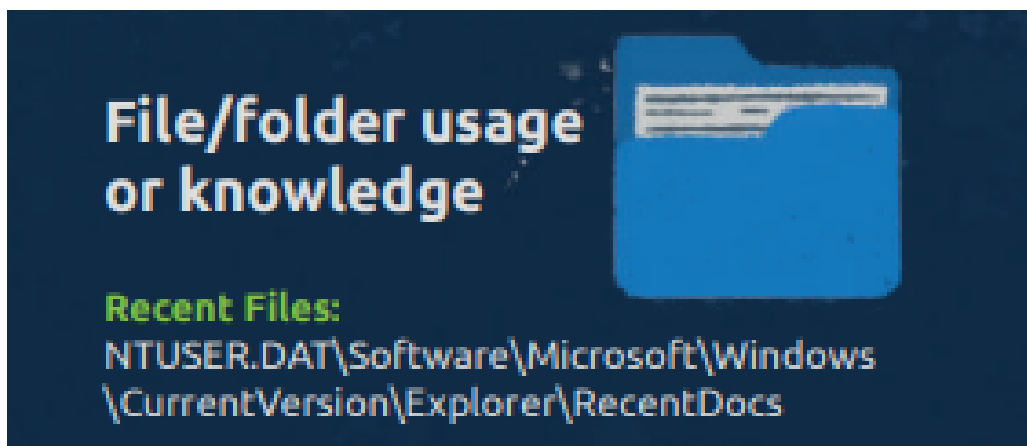
python-3.8.2.exe

6. When was the USB device with the friendly name 'USB' last connected?

Answer: 2021-11-24 18:40:06

1.3. Conclusions

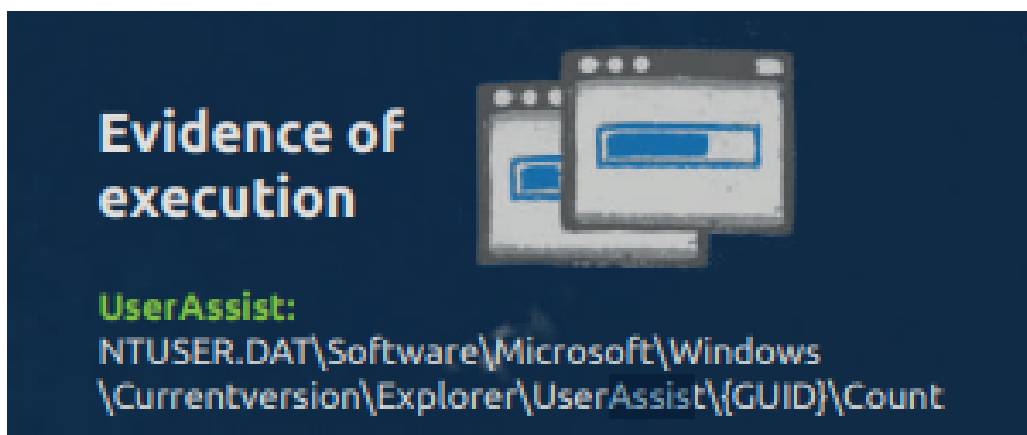
The analysis allowed identifying recent activity on the device. Registry Explorer handles log reproduction well. The tool works quite similarly to Autopsy, although personally



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

| Extension | Value Name | Target Name | Link Name | Mru Position | Opened On | Extension Last Opened |
|------------|------------|--|--------------------------|--------------|---------------------|-----------------------|
| RecentDocs | 7 | EZtools | EZtools.Link | 0 | 2021-12-01 13:00:34 | |
| RecentDocs | 6 | Settings | Settings.Link | 1 | | 2021-11-30 10:56:23 |
| RecentDocs | 5 | WallpaperSettings.xml | WallpaperSettings.Link | 2 | | 2021-11-30 10:56:21 |
| RecentDocs | 4 | System and Security | System and Security.Link | 3 | | |
| RecentDocs | 3 | ::(BB06C0E4-D293-4F75-8A90-CB05B6477EEE) | System.Link | 4 | | |
| RecentDocs | 1 | KAPE | KAPE.Link | 5 | | |
| RecentDocs | 0 | Get-KAPEUpdate.ps1 | Get-KAPEUpdate.Link | 6 | | 2021-11-24 18:18:48 |
| RecentDocs | 2 | Changelog.txt | Changelog.Link | 7 | | 2021-11-24 18:18:48 |
| Folder | 2 | Settings | Settings.Link | 0 | 2021-11-30 10:56:23 | |
| Folder | 1 | System and Security | System and Security.Link | 1 | | |
| Folder | 0 | KAPE | KAPE.Link | 2 | | |
| .xml | 0 | WallpaperSettings.xml | WallpaperSettings.Link | 0 | 2021-11-30 10:56:21 | |
| .txt | 0 | Changelog.txt | Changelog.Link | 0 | 2021-11-24 18:18:48 | |
| .ps1 | 0 | Get-KAPEUpdate.ps1 | Get-KAPEUpdate.Link | 0 | 2021-11-24 18:18:48 | |

Rysunek 3: Registry of recent files.



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

new help

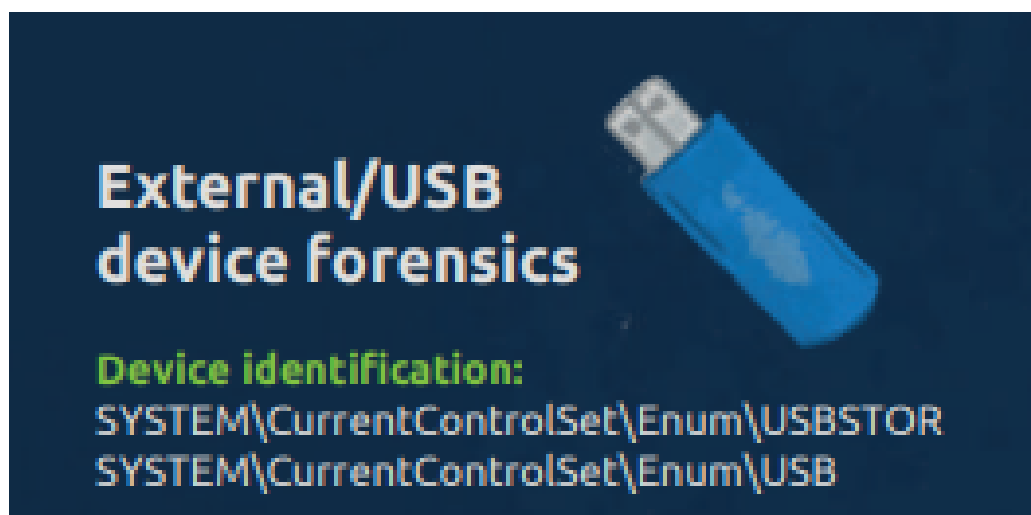
Values UserAssist

Drag a column header here to group by that column

X python Find

| | Program Name | Run Counter | Focus Count | Focus Time | Last Executed |
|---|--|-------------|-------------|--------------------|---------------------|
| ▼ | •C: | = | = | •C: | = |
| ▶ | Z:\setups\python-3.8.2.exe | | 1 | 0 0d, 0h, 00m, 00s | 2021-11-25 03:32:00 |
| | C:\Users\THM-4n6\AppData\Local\Temp\{Unmapped GUID: B409886A-9CC9-4639-9E0C-0B35E1DEC040}\c\python-3.8.2.exe | | 0 | 1 0d, 0h, 00m, 16s | |

Rysunek 5: Searching for Python application.



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

Registry hrv (4) Available bookmarks (93/0)

Enter text to search... Find

Key name # va

▼ •C:

▶ C:\Users\THM-4n6\Desktop\trriage\C\Wl...

▶ C:\Users\THM-4n6\Desktop\hives_clean...

▶ C:\Users\THM-4n6\Desktop\trriage\C\Us...

▶ C:\Users\THM-4n6\Desktop\hives_clean...

ROOT

ActivationBroker

ControlSet001

Control

Enum

ACPI

Values USBSTOR

Drag a column header here to group by that column

| | Timestamp | Manufacturer | Title | Version | Disk Id | Serial Number | Device Name | Installed | First Installed | Last Connected | Last |
|---|----------------|--------------|----------------------|----------|--|------------------------------|--------------------------------------|----------------|-----------------|---------------------|------|
| ▼ | = | •C: | •C: | •C: | •C: | •C: | = | = | = | = | = |
| ▶ | 2021-11-24 ... | Ven_Kingston | Prod_DataTra | Rev_PMAP | {e251921f-4d a2-11ec-a783 -00 1a76da71 10} | 1C6F654E59A 360C1790366 AEB0 | Kingston DataTraveler 2.0 USB Device | 2021-11-24 ... | 2021-11-24 ... | 2021-11-24 18:40:06 | |
| | 2021-11-24 ... | Ven_USB3.0 | Prod_External Device | Rev_SDM1 | {f529a9d6-4d 9e-11ec-a782 -00 1a76da71 10} | 0123456789A 8CDE80 | USB3.0 External Device USB Device | 2021-11-24 ... | 2021-11-24 ... | 2021-11-24 18:27:02 | |

Rysunek 7: USBTOR list.