

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.

The screenshot shows the Registry Explorer application interface. The title bar reads "Registry Explorer v1.6.0.0". The menu bar includes File, Tools, Options, Bookmarks (1/0), View, and Help. The left pane displays a tree view of registry keys under "Registry hives (1) Available bookmark". A search bar at the top left contains "Enter text to search..." and a "Find" button. The main pane has tabs "Values" and "User accounts" (which is selected). A header row allows dragging column headers. Below is a table of user account data:

Key name	# values	Total Logon...	User Name	Password	Groups	Comment
C:\Users\THM-4n6\...	0	0 2...	Administrator	Administrator	Built-in account for administering the computer/domain	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
ROOT	0	0 2...	Guest	Guests	Built-in account for guest access to the computer/domain	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
SAM	1	0 2...	DefaultAcco...	System Managed Accounts Group	A user account managed by the system.	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Domains	1	0 2...	WDAGUtility Account		A user account managed and used by the system for Windows Defender Application Guard scenarios.	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Account	1	19 2...	THM-4n6	count	Administrators	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Aliases	1	2 2...	thm-user	null	Users	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Groups	1	0 2...	thm-user2	null	Users	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Users	1					
000001F4	1					
000001F5	1					
000001F7	1					
000001F8	1					
000003E9	1					
000003EA	1					
000003EB	1					
Names	1					
Admin	1					
Defa...	1					
Guest	1					
THM...	1					
thm-u...	1					
thm-u...	1					
WDA...	1					
BuiltIn	1					
LastSkuUpgrade	1					
RVACT	1					

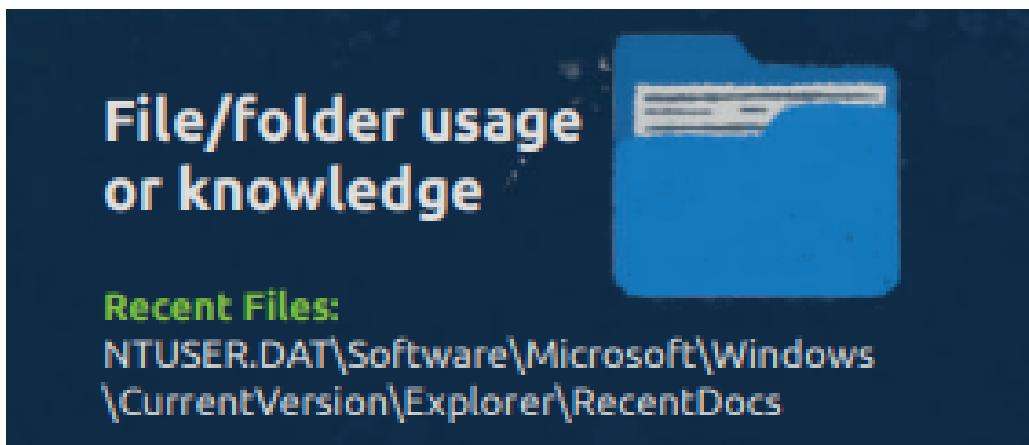
Bottom status bar: Total rows: 7

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.

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (30/0) View Help

Registry hives (3) Available bookmarks >

Values Recent documents

Drag a column header here to group by that column

Extension Value Name Target Name Lnk Name Mru Position Opened On Extension Last Opened

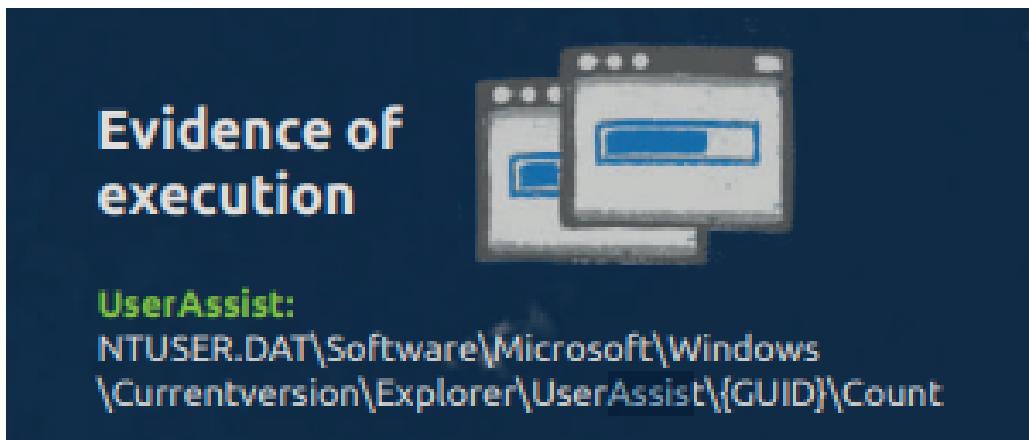
Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension	Last Opened
RecentDocs	7	EZtools	EZtools.lnk	=	=	=	=
RecentDocs	6	Settings	Settings.lnk	1	2021-11-30 10:56:23		
RecentDocs	5	WallpaperSettings.xml	WallpaperSettings.lnk	2	2021-11-30 10:56:21		
RecentDocs	4	System and Security	System and Security.lnk	3			
RecentDocs	3	::{BB06CCE4-D293-4F75-B490-CB9B8477EE}	System.lnk	4			
RecentDocs	1	KAPE	KAPE.lnk	5			
RecentDocs	0	Get-KAPEUpdate.ps1	Get-KAPEUpdate.lnk	6	2021-11-24 18:18:48		
RecentDocs	2	ChangeLog.txt	ChangeLog.lnk	7	2021-11-24 18:18:48		
Folder	2	Settings	Settings.lnk	0	2021-11-30 10:56:23		
Folder	1	System and Security	System and Security.lnk	1			
Folder	0	KAPE	KAPE.lnk	2			
.xml	0	WallpaperSettings.xml	WallpaperSettings.lnk	0	2021-11-30 10:56:21		
.txt	0	ChangeLog.txt	ChangeLog.lnk	0	2021-11-24 18:18:48		
.ps1	0	Get-KAPEUpdate.ps1	Get-KAPEUpdate.lnk	0	2021-11-24 18:18:48		

Total rows: 14 Export ?

Type viewer

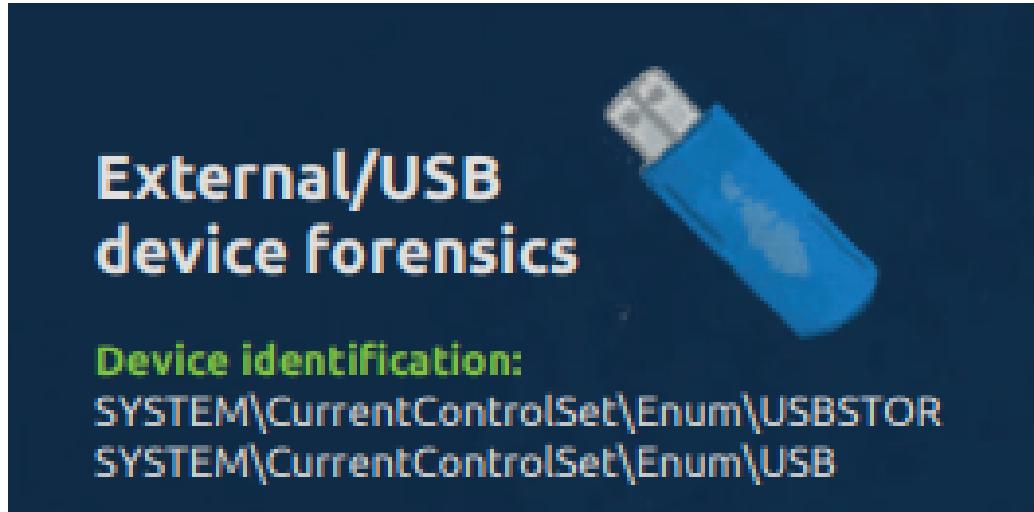
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19
00000000 07 00 00 00 06 00 00 00 05 00 00 04 00 00 00 03 00 00 00 01 00 00 00 00 00 00 yyyy
0000001A 00 00 02 00 00 FF FF FF FF

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: USBT0R list.