

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

Screenshot Overview of the Task

The screenshot shows a web browser window with multiple tabs open. The active tab is 'tryhackme.com/r/room/windowsforensics1'. The page content discusses how users personalize their Windows experience and how forensic investigators use these preferences as artifacts. It includes a sidebar for answering questions and a task navigation bar at the bottom.

Assuming the same build of Windows is installed on a system, excluding the actions taken during installation, the out-of-the-box experience is similar for all users. However, with time, each user personalizes their computer according to their preferences. These preferences include the Desktop layout and icons, the bookmarks in the internet browser, the name of the user, installing of different applications, and logging in to different accounts for each of these applications and other accounts using the internet browser.

Windows saves these preferences to make your computer more personalized. However, forensic investigators use these preferences as artifacts to identify the activity performed on a system. So while your computer might be spying on you, it is not for the explicit reason of spying, instead to make it more pleasant to use the computer according to your taste. But that same information is used by forensic investigators to perform forensic analysis. As we move through this room, we'll see that Windows stores these artifacts in different locations throughout the file system such as in the registry, a user's profile directory, in application-specific files, etc.

In the next task, we will learn about the Windows Registry and how it can help us in forensic analysis of a Windows system.

Answer the questions below

What is the most used Desktop Operating System right now?

Microsoft Windows

✓ Correct Answer

Task 2 0 Windows Registry and Forensics

9:33 PM
7/22/2024

cs-sa07-24019

John_Mbithi_Mutave

The screenshot shows a completed task window titled "RegRipper". The window displays a list of completed tasks: "typeutils... Done.", "vadutilsh... Done.", "uninstall... Done.", "userassist... Done.", "wc_shares... Done.", "winrar... Done.", "winscp... Done.", "winzip... Done.", "wordwheelquery... Done.". Below the list, it says "0 plugins completed with errors." with "Done." underneath. At the bottom are "Rip!" and "Close" buttons.

One shortcoming of RegRipper is that it does not take the transaction logs into account. We must use Registry Explorer to merge transaction logs with the respective registry hives before sending the output to RegRipper for a more accurate result.

Even though we have discussed these different tools, for the purpose of this room, we will only be using Registry Explorer and some of Eric Zimmerman's tools. The other tools mentioned here will be covered in separate rooms.

Answer the questions below

Study the above material to understand the difference between the different tools

No answer needed ✓ Correct Answer

The screenshot shows a task titled "Task 6 System Information and System Accounts". It features a "Custom Content Sources" interface with a table of file paths and their hex values. The table includes columns for "Evidence", "File System Path", and "File". The "File" column contains large amounts of hex data. A status bar at the bottom says "Exports selected system files for facilitating a SAM attack".

For the purpose of this room, we will not be acquiring data ourselves, but instead, we will work with the attached VM that already has data.

Answer the questions below

Try collecting data on your own system or the attached VM using one of the above mentioned tools

No answer needed ✓ Correct Answer

The screenshot shows a task titled "Task 5 Exploring Windows Registry". It features a "Custom Content Sources" interface with a table of file paths and their hex values, similar to the previous task. The table includes columns for "Evidence", "File System Path", and "File". The "File" column contains large amounts of hex data. A status bar at the bottom says "Exports selected system files for facilitating a SAM attack".

Transaction Logs and Backups:

Some other very vital sources of forensic data are the registry transaction logs and backups. The transaction logs can be considered as the journal of the changelog of the registry hive. Windows often uses transaction logs when writing data to registry hives. This means that the transaction logs can often have the latest changes in the registry that haven't made their way to the registry hives themselves. The transaction log for each hive is stored as a .LOG file in the same directory as the hive itself. It has the same name as the registry hive, but the extension is .LOG. For example, the transaction log for the SAM hive will be located in `C:\Windows\System32\Config` in the filename SAM.LOG. Sometimes there can be multiple transaction logs as well. In that case, they will have .LOG1, .LOG2 etc., as their extension. It is prudent to look at the transaction logs as well when performing registry forensics.

Registry backups are the opposite of Transaction logs. These are the backups of the registry hives located in the `C:\Windows\System32\Config` directory. These hives are copied to the `C:\Windows\System32\Config\RegBack` directory every ten days. It might be an excellent place to look if you suspect that some registry keys might have been deleted/modifed recently.

Answer the questions below

What is the path for the five main registry hives, DEFAULT, SAM, SECURITY, SOFTWARE, and SYSTEM?

`C:\Windows\System32\Config`

✓ Correct Answer ⓘ Hint

What is the path for the AmCache hive?

`C:\Windows\AppCompat\Programs\Amcache.hve`

✓ Correct Answer

Task 4 Data Acquisition

Starting with Windows 2000, this information is stored under both the HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER keys. The `HKEY_LOCAL_MACHINE\Software\Classes` key contains default settings that can apply to all users on the local computer. The `HKEY_CURRENT_USER\Software\Classes` key has settings that override the default settings and apply only to the interactive user.

The HKEY_CLASSES_ROOT key provides a view of the registry that merges the information from these two sources. HKEY_CLASSES_ROOT also provides this merged view for programs that are designed for earlier versions of Windows. To change the settings for the interactive user, changes must be made under `HKEY_CURRENT_USER\Software\Classes` instead of under HKEY_CLASSES_ROOT.

To change the default settings, changes must be made under `HKEY_LOCAL_MACHINE\Software\Classes`, if you write keys to a key under HKEY_CLASSES_ROOT, the system stores the information under `HKEY_LOCAL_MACHINE\Software\Classes`.

If you write values to a key under HKEY_CLASSES_ROOT, and the key already exists under `HKEY_CURRENT_USER\Software\Classes`, the system will store the information there instead of under `HKEY_LOCAL_MACHINE\Software\Classes`.

HKEY_CURRENT_CONFIG Contains information about the hardware profile that is used by the local computer at system startup.

Answer the questions below

What is the short form for HKEY_LOCAL_MACHINE?

`HKLM`

✓ Correct Answer ⓘ Hint

Task 3 Accessing registry hives offline

cs-sa07-24019

John_Mbithi_Mutave

The screenshot shows a web browser window for the TryHackMe platform. The URL is `tryhackme.com//room/windowsforensics1`. The interface includes a navigation bar with links for Dashboard, Learn, Compete, and Other, along with a 'Access Machines' button and a user icon. A progress bar at the top indicates completion of Task 7.

Task 7: Usage or knowledge of files/folders

- Question: Which ControlSet contains the last known good configuration?
Answer: 1
Feedback: ✓ Correct Answer
- Question: What is the Computer Name of the computer?
Answer: THM-4n6
Feedback: ✓ Correct Answer
- Question: What is the value of the TimeZoneKeyName?
Answer: Pakistan Standard Time
Feedback: ✓ Correct Answer
- Question: What is the DHCP IP address?
Answer: 192.168.100.58
Feedback: ✓ Correct Answer
- Question: What is the RID of the Guest User account?
Answer: 501
Feedback: ✓ Correct Answer

At the bottom of the screen, the Windows taskbar is visible, showing icons for File Explorer, Search, Task View, and various pinned applications like Microsoft Edge, Google Chrome, and File Explorer. The system tray shows the date and time as 7/22/2024 9:34 PM, and connectivity status.

cs-sa07-24019

John_Mbithi_Mutave

This is how Registry Explorer parses the AmCache hive:

Information about the last executed programs can be found at the following location in the hive:
Amcache.hive\Root\file\{Volume GUID}\

| Timestamp | Path | Name | Product Name | Publisher | Version | DHash |
|---------------------|------------------------------------------------------------------------------------------|-----------------------------------|-----------------------------------|-----------------------|---------------|----------------------------------------|
| 2021-12-01 12:45:37 | C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_7.7.112.0_12.0_3008be\Amcache.exe | view3d.exe | view3d | microsoft corporation | 7.1207.7012.0 | 2b384b00a12104b4a2796772e90889f6 |
| 2021-12-01 12:55:19 | c:\program files\7-zip\7z.exe | 7z.exe | 7-zip | igor pavlov | 29.00 | 6c7ea8bbd435163ee3945cfe730ef9b9872a45 |
| 2021-12-01 12:55:19 | c:\program files\7-zip\7zfm.exe | 7zfm.exe | 7-zip | igor pavlov | 29.00 | 45e1986672d87398349aa71760e3e398d |
| 2021-12-01 12:55:19 | c:\program files\7-zip\7zg.exe | 7zg.exe | 7-zip | igor pavlov | 29.00 | d7261294949494931549eb8ba49314968523 |
| 2021-12-01 13:00:29 | c:\program files\google\update\SharedData\6af\3d45-d54-494a-8330-23030a4a4a4-45 | 96.0.4664.45_chrome_installer.exe | 96.0.4664.45_chrome_installer.exe | google inc | 96.0.4664.45 | c29826577152fb1b137141e1e152184a05566e |
| 2021-12-01 13:55:49 | c:\program files\amazon\amazon\agent.exe | amazon-sea-agent.exe | amazon-sea-agent | amazon inc | 5.1.538.0 | e576b1970709373875d847302385845707a30 |
| 2021-12-01 13:57:38 | c:\program files\amazon\amazon\agent\cache\13adbf1-fae-467-8d46-6ff711aa | AmazonSMAgentSetup.exe | Amazon Sma agent | amazon web services | 5.1.538.0 | 9134549515d43075e0393b94da70ea356828 |
| 2021-12-01 13:00:20 | c:\users\bri\desktop\amcache\amcache\amcacheParser.exe | amcacheParser.exe | amcacheParser | eric zimmerman | 5.4.0.0 | 13b202170ff423266429fe224e5405fb0b3c |

In the Windows registry, the following locations contain information related to BAM and DAM. This location contains information about last run programs, their full paths, and last execution time.

SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}

SYSTEM\CurrentControlSet\Services\dam\UserSettings\{SID}

Below you can see how Registry Explorer parses data from BAM:

ShimCache stores file name, file size, and last modified time of the executables.

Our goto tool, the Registry Explorer, doesn't parse ShimCache data in a human-readable format, so we go to another tool called AppCompatCache Parser, also a part of Eric Zimmerman's tools. It takes the SYSTEM hive as input, parses the data, and outputs a CSV file that looks like this:

| ControlSet | CacheEntryPath | LastModifiedTimeUTC | Executed | Duplicate | SourceFile |
|------------|-----------------------------------------------------------------|---------------------|----------|---------------------------------------|------------|
| 1 | 0 C:\Users\THM-4n6\Desktop\KAPE\gkape.exe | 6/24/2021 6:23 NA | FALSE | C:\Users\THM-4n6\Desktop\SYSTEM_clean | |
| 3 | 1 C:\Users\THM-4n6\Desktop\KAPE\gkape.exe | 6/24/2021 6:23 NA | FALSE | C:\Users\THM-4n6\Desktop\SYSTEM_clean | |
| 4 | 2 C:\Program Files\Common Files\Microsoft shared\ink\TabTip.exe | 10/6/2021 13:52 NA | FALSE | C:\Users\THM-4n6\Desktop\SYSTEM_clean | |
| 5 | 3 C:\Windows\System32\rdpinput.EXE | 12/7/2019 9:09 NA | FALSE | C:\Users\THM-4n6\Desktop\SYSTEM_clean | |
| 6 | 4 C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe | 10/6/2021 13:45 NA | FALSE | C:\Users\THM-4n6\Desktop\SYSTEM_clean | |

AmCache:

The AmCache hive is an artifact related to ShimCache. This performs a similar function to ShimCache, and stores additional data related to program executions. This data includes execution path, installation, execution and deletion times, and SHA1 hashes of the executed programs. This hive is located in the file system at:

C:\Windows\appcompat\Programs\Amcache.hive

Information about the last executed programs can be found at the following location in the hive:

Amcache.hive\Root\file\{Volume GUID}\

cs-sa07-24019

John_Mbithi_Mutave

The screenshot shows a web-based interface for Windows forensics, specifically focusing on User Assist registry keys. The URL is tryhackme.com/r/room/windowsforensics1. The interface includes a sidebar with links like Dashboard, Learn, Compete, and Other. The main content area displays a table of User Assist keys from the NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count key. The table has columns: Program Name, Run Counter, Focus Count, Focus Time, and Last Executed. Key entries include UME_CTLUICountctor, UME_CTLSESSION, and various Snipping Tool, Paint, Notepad, and Taskbar links.

| Program Name | Run Counter | Focus Count | Focus Time | Last Executed |
|-------------------------------------------------------------|-------------|-------------|---------------|---------------------|
| UME_CTLUICountctor | = | 0 | 0, 0h, 0m, 0s | |
| [Common Programs]\Accessories\Snipping Tool.lnk | 9 | 0 | 0, 0h, 0m, 0s | |
| UME_CTLSESSION | 54 | 0 | 0, 0h, 0m, 0s | |
| [Common Programs]\Accessories\Paint.lnk | 7 | 0 | 0, 0h, 0m, 0s | 2021-11-25 03:14:34 |
| [Programs]\Accessories\Notepad.lnk | 6 | 0 | 0, 0h, 0m, 0s | 2021-11-25 03:14:34 |
| (User Pinned) Taskbar File Explorer.lnk | 26 | 0 | 0, 0h, 0m, 0s | 2021-12-01 13:02:43 |
| [Programs]\Windows PowerShell\Windows PowerShell.lnk | 1 | 0 | 0, 0h, 0m, 0s | 2021-11-25 03:37:24 |
| (User Pinned) Taskbar \Firefox.lnk | 2 | 0 | 0, 0h, 0m, 0s | 2021-12-01 12:32:34 |
| [Common Programs]\Accessories\Remote Desktop Connection.lnk | 1 | 0 | 0, 0h, 0m, 0s | 2021-11-25 03:59:55 |
| (User Pinned) Taskbar \Opera Browser.lnk | 1 | 0 | 0, 0h, 0m, 0s | 2021-11-25 04:10:02 |
| [Common Programs]\Accessories\Notepad.lnk | 1 | 0 | 0, 0h, 0m, 0s | 2021-11-30 10:55:21 |

ShimCache is a mechanism used to keep track of application compatibility with the OS and tracks all applications launched on the machine. Its main purpose in Windows is to ensure backward compatibility of applications. It is also called Application Compatibility Cache (AppCompatCache). It is located in the following location in the SYSTEM hive:

`SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache`

ShimCache stores file name, file size, and last modified time of the executables.

The screenshot shows a web-based interface for Windows forensics, specifically focusing on Open/Save and LastVisited Dialog MRUs. The URL is tryhackme.com/r/room/windowsforensics1. The interface includes a sidebar with links like Dashboard, Learn, Compete, and Other. The main content area displays a table of Open/Save and LastVisited Dialog MRU keys from the INTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidMRU and INTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidMRU keys. The table has columns: Value Name, Mru Position, Executable, Absolute Path, and Opened On. One entry is shown: notePad.exe was opened on My Computer\Program Files\Amazon\Ec2ConfigService\Settings at 2021-11-30 10:56:19.

| Value Name | Mru Position | Executable | Absolute Path | Opened On |
|------------|--------------|-------------|------------------------------------------------------------|---------------------|
| 0 | 0 | notePad.exe | My Computer\Program Files\Amazon\Ec2ConfigService\Settings | 2021-11-30 10:56:19 |

Windows Explorer Address/Search Bars:

Another way to identify a user's recent activity is by looking at the paths typed in the Windows Explorer address bar or searches performed using the following registry keys, respectively.

`INTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths`

`INTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery`

Here is how the TypedPaths key looks like in Registry Explorer:

The screenshot shows a web-based interface for Windows forensics, specifically focusing on TypedPaths. The URL is tryhackme.com/r/room/windowsforensics1. The interface includes a sidebar with links like Dashboard, Learn, Compete, and Other. The main content area displays a table of TypedPaths keys from the INTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths key. The table has columns: Enter text to search... and Find. One entry is shown: C:\Program Files\Amazon\Ec2ConfigService\Settings.

| Enter text to search... | Find |
|---------------------------------------------------|------|
| C:\Program Files\Amazon\Ec2ConfigService\Settings | |

cs-sa07-24019

John_Mbithi_Mutave

The screenshot shows a web browser window with multiple tabs open. The main content area displays a table titled "Open/Save and LastVisited Dialog MRUs:".

Table Headers:

| Value Name | MRU Position | Executable | Absolute Path | Opened On |
|------------|--------------|------------|---------------|-----------|
|------------|--------------|------------|---------------|-----------|

Table Data:

| | | | | |
|---|---|-------------|------------------------------------------------------------|---------------------|
| 0 | 0 | notepad.exe | My Computer\Program Files\Amazon\Ec2ConfigService\Settings | 2021-11-30 10:56:19 |
|---|---|-------------|------------------------------------------------------------|---------------------|

Text Below Table:

This is how Registry Explorer shows this registry key. Take a look to answer Question # 3 and 4.

The taskbar shows the following recent file paths:

- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths
- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagBags
- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU
- NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU

The screenshot shows the "ShellBags Explorer v1.4.0.0" application window. It displays a table of MRU items, similar to the one above.

Table Headers:

| Value | Icon | Shell Type | MRU Posit... | Created On | Modified On | Accessed On | First Interacted | Last Interacted | Has Explored | Miscellaneous |
|-------|------|------------|--------------|------------|-------------|-------------|------------------|-----------------|--------------|---------------|
|-------|------|------------|--------------|------------|-------------|-------------|------------------|-----------------|--------------|---------------|

Table Data:

| | | | | | | | | | | |
|---------------|----------|---------------|---|---------------------|---------------------|---------------------|---------------------|---------------------|-------------------------------------|------------------|
| No im... | File | Desktop | 0 | 2021-11-25 03:34:14 | 2021-11-25 03:34:14 | 2021-11-25 03:34:14 | 2021-12-01 13:06:47 | 2021-11-24 18:20:02 | <input checked="" type="checkbox"/> | NTFS file system |
| My Computer | Computer | My Computer | 1 | 2021-11-25 03:34:14 | 2021-11-25 03:34:14 | 2021-11-25 03:34:14 | 2021-12-01 13:06:47 | 2021-11-30 11:08:01 | <input checked="" type="checkbox"/> | NTFS file system |
| KAPE | Folder | KAPE | 2 | 2021-11-25 03:34:14 | 2021-11-25 03:34:14 | 2021-11-25 03:34:14 | 2021-12-01 13:06:47 | 2021-11-30 11:08:01 | <input checked="" type="checkbox"/> | NTFS file system |
| Home Folder | Folder | Home Folder | 3 | | | | 2021-11-24 18:20:02 | 2021-11-30 11:08:01 | <input type="checkbox"/> | |
| Search Folder | User | Search Folder | 4 | | | | 2021-11-24 18:20:02 | 2021-11-30 11:08:01 | <input type="checkbox"/> | |
| Control Panel | Folder | Control Panel | 5 | | | | 2021-11-24 18:20:02 | 2021-11-30 11:08:01 | <input type="checkbox"/> | |
| E:\ | File | E:\ | 6 | | | | 2021-11-24 18:20:02 | 2021-11-30 11:08:01 | <input type="checkbox"/> | |

Text Below Table:

When we open or save a file, a dialog box appears asking us where to save or open that file from. It might be noticed that once we open/save a file at a specific location, Windows remembers that location. This implies that we can find out recently used files if we get our hands on this information. We can do so by examining the following registry keys

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComObj32\OpenSavePIDMRU

The taskbar shows the same recent file paths as the first taskbar:

- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths
- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagBags
- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU
- NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU

cs-sa07-24019

John_Mbithi_Mutave

Registry hives (3) Available bookmarks (61/0)

Key name

Program Execution Time

| Program | Execution Time |
|-----------------------------------------------------------------------------------------------------|---------------------|
| Microsoft.Windows.ShellExperienceHost_cw5n1h2tbyevy | 2021-11-24 18:02:15 |
| Microsoft.Windows.Cortana_cw5n1h2tbyevy | 2021-11-24 18:02:15 |
| [Device]HarddiskVolume2\Windows\explorer.exe | 2021-11-24 18:02:15 |
| [Device]HarddiskVolume2\Windows\System32\ApplicationFrameHost.exe | 2021-11-24 18:02:15 |
| window.immersivecontrolpanel_cw5n1h2tbyevy | 2021-11-24 15:40:11 |
| [Device]HarddiskVolume2\Program Files\VMware\Tools\lmtoolsd.exe | 2021-11-24 18:02:14 |
| [Device]HarddiskVolume2\Windows\System32\cmd.exe | 2021-11-25 03:23:14 |
| [Device]HarddiskVolume2\Program Files (x86)\Mozilla\Firefox\firefox.exe | 2021-11-25 03:46:20 |
| [Device]HarddiskVolume2\Program Files (x86)\Google\Update\GoogleUpdate.exe | 2021-11-25 03:43:40 |
| [Device]HarddiskVolume2\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | 2021-11-24 17:56:18 |
| [Device]HarddiskVolume2\Windows\System32\notepad.exe | 2021-11-25 03:42:53 |
| [Device]HarddiskVolume2\Users\TH-M-41d\AppData\Local\Programs\Opera\opera.exe | 2021-11-25 04:12:31 |
| [Device]HarddiskVolume2\Program Files\Google\Chrome\Application\chrome.exe | 2021-11-25 03:43:50 |
| [Device]HarddiskVolume2\Windows\System32\instc.exe | 2021-11-25 04:00:04 |
| [Device]HarddiskVolume2\Windows\System32\sysentersettings\AdminPowers.exe | 2021-11-25 04:00:54 |
| [Device]HarddiskVolume2\Windows\System32\systemPropertiesComputerName.exe | 2021-11-25 04:01:35 |
| [Device]HarddiskVolume2\Windows\System32\wind32.exe | 2021-11-24 17:38:19 |
| [Device]HarddiskVolume2\Program Files (x86)\Windows Installation Assistant\Windows10UpgraderApp.exe | 2021-11-24 18:01:52 |
| [Device]HarddiskVolume2\Program Files (x86)\Microsoft\Edge\Update\MicrosoftEdgeUpdate.exe | 2021-11-24 15:21:35 |
| [Device]HarddiskVolume2\Program Files (x86)\Microsoft\Edge\Application\msedge.exe | 2021-11-24 15:23:43 |

Total rows: 21

Answer the questions below

How many times was the File Explorer launched?

tryhackme.com//room/windowsforensics1

Answer the questions below

When was EZTools opened?

2021-12-01 13:00:34

✓ Correct Answer ⚡ Hint

At what time was My Computer last interacted with?

2021-12-01 13:06:47

✓ Correct Answer ⚡ Hint

What is the Absolute Path of the file opened using notepad.exe?

C:\Program Files\Amazon\Ec2ConfigService\Settings

✓ Correct Answer

When was this file opened?

2021-11-30 10:56:19

✓ Correct Answer ⚡ Hint

Task 8 Evidence of Execution

cs-sa07-24019

John_Mbithi_Mutave

The screenshot shows a web browser window with multiple tabs open. The main content area displays a table titled "Open/Save and LastVisited Dialog MRUs:".

Table Headers:

| Value Name | MRU Position | Executable | Absolute Path | Opened On |
|------------|--------------|------------|---------------|-----------|
|------------|--------------|------------|---------------|-----------|

Table Data:

| | | | | |
|---|---|-------------|------------------------------------------------------------|---------------------|
| 0 | 0 | notepad.exe | My Computer\Program Files\Amazon\Ec2ConfigService\Settings | 2021-11-30 10:56:19 |
|---|---|-------------|------------------------------------------------------------|---------------------|

Text Below Table:

This is how Registry Explorer shows this registry key. Take a look to answer Question # 3 and 4.

The taskbar shows the following recent file paths:

- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths
- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags
- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU
- NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU

The screenshot shows the "ShellBags Explorer v1.4.0.0" application window. It displays a table of MRU items, similar to the one above.

Table Headers:

| Value | Icon | Shell Type | MRU Posit... | Created On | Modified On | Accessed On | First Interacted | Last Interacted | Has Explored | Miscellaneous |
|-------|------|------------|--------------|------------|-------------|-------------|------------------|-----------------|--------------|---------------|
|-------|------|------------|--------------|------------|-------------|-------------|------------------|-----------------|--------------|---------------|

Table Data:

| | | | | | | | | | | |
|---------------|----------|---------------|---|---------------------|---------------------|---------------------|---------------------|---------------------|-------------------------------------|------------------|
| No im... | File | Desktop | 0 | 2021-11-25 03:34:14 | 2021-11-25 03:34:14 | 2021-11-25 03:34:14 | 2021-12-01 13:06:47 | 2021-11-24 18:20:02 | <input checked="" type="checkbox"/> | NTFS file system |
| My Computer | Computer | My Computer | 1 | 2021-11-25 03:34:14 | 2021-11-25 03:34:14 | 2021-11-25 03:34:14 | 2021-12-01 13:06:47 | 2021-11-30 11:08:01 | <input checked="" type="checkbox"/> | NTFS file system |
| KAPE | Folder | KAPE | 2 | 2021-11-25 03:34:14 | 2021-11-25 03:34:14 | 2021-11-25 03:34:14 | 2021-12-01 13:06:47 | 2021-11-30 11:08:01 | <input checked="" type="checkbox"/> | NTFS file system |
| Home Folder | Folder | Home Folder | 3 | | | | 2021-11-24 18:20:02 | 2021-11-30 11:08:01 | <input type="checkbox"/> | |
| Search Folder | User | Search Folder | 4 | | | | 2021-11-24 18:20:02 | 2021-11-30 11:08:01 | <input type="checkbox"/> | |
| Control Panel | Folder | Control Panel | 5 | | | | 2021-11-24 18:20:02 | 2021-11-30 11:08:01 | <input type="checkbox"/> | |
| E:\ | File | E:\ | 6 | | | | 2021-11-24 18:20:02 | 2021-11-30 11:08:01 | <input type="checkbox"/> | |

Text Below Table:

When we open or save a file, a dialog box appears asking us where to save or open that file from. It might be noticed that once we open/save a file at a specific location, Windows remembers that location. This implies that we can find out recently used files if we get our hands on this information. We can do so by examining the following registry keys

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComObj32\OpenSavePIDMRU

cs-sa07-24019

John_Mbithi_Mutave

The screenshot shows a Registry Explorer interface on a browser. The left pane displays a tree view of registry keys under 'Recent Docs'. The right pane shows a table titled 'Recent documents' with columns: Extension, Value Name, Target Name, Link Name, Mru Position, Opened On, and Extension Last Opened. The table lists various files and their details.

| Extension | Value Name | Target Name | Link Name | Mru Position | Opened On | Extension Last Opened |
|-----------|------------|------------------------------------------|-------------------------|--------------|-----------------------|-----------------------|
| .ini | 7 | EZTools | EZTools.lnk | == | 0 2021-12-01 13:00:34 | |
| .ini | 6 | Settings | Settings.lnk | 1 | 2021-11-30 10:56:23 | |
| .xml | 5 | WallpaperSettings.xml | WallpaperSettings.lnk | 2 | 2021-11-30 10:56:21 | |
| .ini | 4 | System and Security | System and Security.lnk | 3 | | |
| .ini | 3 | c:\BBB5CCE4-D293-4F7E-75-8A90-CB305647EE | System.lnk | 4 | | |
| .ini | 1 | KAPE | KAPE.lnk | 5 | | |
| .ps1 | 0 | Get-KAPEUpdate.ps1 | Get-KAPEUpdate.lnk | 6 | 2021-11-24 18:18:48 | |
| .txt | 2 | ChangeLog.txt | ChangeLog.lnk | 7 | 2021-11-24 18:18:48 | |
| .ini | 2 | Settings | Settings.lnk | 0 | 2021-11-30 10:56:23 | |
| .ini | 1 | System and Security | System and Security.lnk | 1 | | |
| .ini | 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 | |
| .ini | 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 | |

Registry Explorer allows us to sort data contained in registry keys quickly. For example, the Recent documents tab arranges the Most Recently Used (MRU) file at the top of the list. Registry Explorer also arranges them so that the Most Recently Used (MRU) file is shown at the top of the list and the older ones later.

The screenshot shows a Registry Explorer interface on a browser. The left pane displays a tree view of registry keys under 'LastVisitedPidMRU'. The right pane shows a table with columns: Value Name, Mru Position, Executable, Absolute Path, and Opened On. The table lists a single entry for 'notepad.exe'.

| Value Name | Mru Position | Executable | Absolute Path | Opened On |
|------------|--------------|-------------|----------------------------------------------------------------|---------------------|
| 0 | 0 | notepad.exe | My Computer\{C:\Program Files\Amazon\Ec2ConfigService\Settings | 2021-11-30 10:56:19 |

Windows Explorer Address/Search Bars:

Another way to identify a user's recent activity is by looking at the paths typed in the Windows Explorer address bar or searches performed using the following registry keys, respectively.

INTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths
INTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

Here is how the TypedPaths key looks like in Registry Explorer:

The screenshot shows a Registry Explorer interface on a browser. The left pane displays a tree view of registry keys under 'TypedPaths'. The right pane shows a table with columns: Enter text to search... and Find. The table lists a single entry for 'notepad.exe'.

| Enter text to search... | Find |
|-------------------------|------|
| notepad.exe | |

cs-sa07-24019

John_Mbithi_Mutave

The screenshot shows a browser window with the URL tryhackme.com/room/windowsforensics1. The page title is "Task 9 External Devices/USB device forensics". The main content area displays a file search interface with a sidebar showing file paths like 'Device\HarddiskVolume2\Program Files (x86)\Windows Installation Assistant\Windows 10 Logon\orderApp.exe'. Below this is a section titled "Answer the questions below". It contains four questions with input fields and "Correct Answer" buttons:

- How many times was the File Explorer launched? (Answer: 26)
- What is another name for ShimCache? (Answer: AppCompatCache)
- Which of the artifacts also saves SHA1 hashes of the executed programs? (Answer: AmCache)
- Which of the artifacts saves the full path of the executed programs? (Answer: BAM/DAM)

The bottom of the screen shows a task bar with various icons and the system tray indicating the date and time.

cs-sa07-24019

John_Mbithi_Mutave

This is how Registry Explorer parses the AmCache hive:

Information about the last executed programs can be found at the following location in the hive:
Amcache.hive\Root\file\{Volume GUID}\

| Timestamp | Path | Name | Product Name | Publisher | Version | DHash |
|---------------------|-------------------------------------------------------------------------------------------------------------|-----------------------------------|-----------------------------------|-----------------------|---------------|----------------------------------------|
| 2021-12-01 12:45:37 | C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_7.7.112.0_12.0_364_0_neutral\shell\Start\Amcache.exe | Amcache.exe | view 3d | microsoft corporation | 7.1207.7012.0 | 2b384b00a12104b4a2796772e90889f6 |
| 2021-12-01 12:55:19 | c:\Program Files\7-zip\7z.exe | 7z.exe | 7-zip | igor pavlov | 29.00 | 6c7ea1bbd435163ee3945cfe730ef9b9872a45 |
| 2021-12-01 12:55:19 | c:\Program Files\7-zip\7zfm.exe | 7zfm.exe | 7-zip | igor pavlov | 29.00 | 45e1986672d87398349aa71760e3e398d |
| 2021-12-01 12:55:19 | c:\Program Files\7-zip\7zg.exe | 7zg.exe | 7-zip | igor pavlov | 29.00 | d7261294949494541549ebab949314968523 |
| 2021-12-01 13:00:29 | c:\Program Files\google\update\SharedData\0af3d245-d544-464a-a203-23030a2a064-45 | 96.0.4664.45_chrome_installer.exe | 96.0.4664.45_chrome_installer.exe | google inc | 96.0.4664.45 | c29826577152fb1b137141e1e152184a05566e |
| 2021-12-01 13:55:49 | c:\Program Files\amazon\amazon\agent.exe | amazon-sea-agent.exe | amazon-sea-agent | amazon inc | 5.1.538.0 | e576b1970709373875d847302385845707a30 |
| 2021-12-01 13:57:38 | c:\ProgramData\Amazon\AmazonSSM\Setup\AmazonSSMSetup.exe | AmazonSSMSetup.exe | amazon ssm agent | amazon web services | 5.1.538.0 | 9134549515d43075e0393b94da70ea356828 |
| 2021-12-01 13:00:20 | c:\Users\bri-06\Desktop\amcache\amcacheParser.exe | amcacheParser.exe | eric zimmerman | eric zimmerman | 5.4.0.0 | 13b202170ff423266428fe224e5405fb0b3c |

In the Windows registry, the following locations contain information related to BAM and DAM. This location contains information about last run programs, their full paths, and last execution time.

SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}

SYSTEM\CurrentControlSet\Services\dam\UserSettings\{SID}

Below you can see how Registry Explorer parses data from BAM:

ShimCache stores file name, file size, and last modified time of the executables.

Our goto tool, the Registry Explorer, doesn't parse ShimCache data in a human-readable format, so we go to another tool called AppCompatCache Parser, also a part of Eric Zimmerman's tools. It takes the SYSTEM hive as input, parses the data, and outputs a CSV file that looks like this:

| ControlSet | CacheEntryPath | LastModifiedTimeUTC | Executed | Duplicate | SourceFile |
|------------|-----------------------------------------------------------------|---------------------|----------|---------------------------------------|------------|
| 1 | 0 C:\Users\THM-4n6\Desktop\KAPE\gkape.exe | 6/24/2021 6:23 NA | FALSE | C:\Users\THM-4n6\Desktop\SYSTEM_clean | |
| 3 | 1 C:\Users\THM-4n6\Desktop\KAPE\kape.exe | 6/24/2021 6:23 NA | FALSE | C:\Users\THM-4n6\Desktop\SYSTEM_clean | |
| 4 | 2 C:\Program Files\Common Files\Microsoft Shared\ink\TabTip.exe | 10/6/2021 13:52 NA | FALSE | C:\Users\THM-4n6\Desktop\SYSTEM_clean | |
| 5 | 3 C:\Windows\System32\rdpinput.EXE | 12/7/2019 9:09 NA | FALSE | C:\Users\THM-4n6\Desktop\SYSTEM_clean | |
| 6 | 4 C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe | 10/6/2021 13:45 NA | FALSE | C:\Users\THM-4n6\Desktop\SYSTEM_clean | |

AmCache:

The AmCache hive is an artifact related to ShimCache. This performs a similar function to ShimCache, and stores additional data related to program executions. This data includes execution path, installation, execution and deletion times, and SHA1 hashes of the executed programs. This hive is located in the file system at:

C:\Windows\appcompat\Programs\Amcache.hive

Information about the last executed programs can be found at the following location in the hive:

Amcache.hive\Root\file\{Volume GUID}\

tryhackme.com//room/windowsforensics1

Windows keeps track of applications launched by the user using Windows Explorer for statistical purposes in the User Assist registry keys. These keys contain information about the programs launched, the time of their launch, and the number of times they were executed. However, programs that were run using the command line can't be found in the User Assist keys. The User Assist key is present in the NTUSER hive, mapped to each user's GUID. We can find it at the following location:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count

| Program Name | Run Counter | Focus Count | Focus Time | Last Executed |
|-------------------------------------------------------------|-------------|-------------|---------------|---------------------|
| UEME_CTLUICountctor | = | 0 | 0, 0h, 0m, 0s | |
| [Common Programs]\Accessories\SnippingToolLink | 9 | 0 | 0, 0h, 0m, 0s | |
| UEME_CTLSESSION | 54 | 0 | 0, 0h, 0m, 0s | 2021-11-25 03:14:34 |
| [Common Programs]\Accessories\PaintLink | 7 | 0 | 0, 0h, 0m, 0s | 2021-11-25 03:14:34 |
| [Programs]\Accessories\NotepadLink | 6 | 0 | 0, 0h, 0m, 0s | 2021-11-25 03:14:34 |
| (User Pinned) Taskbar File Explorer Link | 26 | 0 | 0, 0h, 0m, 0s | 2021-12-01 13:02:43 |
| [Programs]\Windows PowerShell\WindowsPowerShellLink | 1 | 0 | 0, 0h, 0m, 0s | 2021-11-25 03:37:24 |
| (User Pinned) Taskbar FirefoxLink | 2 | 0 | 0, 0h, 0m, 0s | 2021-12-01 12:32:34 |
| [Common Programs]\Accessories\RemoteDesktop Connection Link | 1 | 0 | 0, 0h, 0m, 0s | 2021-11-25 03:59:55 |
| (User Pinned) Taskbar\Opera Browser Link | 1 | 0 | 0, 0h, 0m, 0s | 2021-11-25 04:10:02 |
| [Common Programs]\Accessories\NotepadLink | 1 | 0 | 0, 0h, 0m, 0s | 2021-11-30 10:55:21 |

ShimCache is a mechanism used to keep track of application compatibility with the OS and tracks all applications launched on the machine. Its main purpose in Windows is to ensure backward compatibility of applications. It is also called Application Compatibility Cache (AppCompatCache). It is located in the following location in the SYSTEM hive:

SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

ShimCache stores file name, file size, and last modified time of the executables.

tryhackme.com//room/windowsforensics1

Answer the questions below

How many times was the File Explorer launched?

| Program | Execution Time |
|---------------------------------------------------------------------------------------------------------|---------------------|
| Microsoft.Windows.ShellExperienceHost_cw5n1h2tbyewy | 2021-11-24 18:02:15 |
| Microsoft.Windows.Cortana_cw5n1h2tbyewy | 2021-11-24 18:02:15 |
| [Device HarddiskVolume2]\Windows\explorer.exe | 2021-11-24 18:02:15 |
| [Device HarddiskVolume2]\Windows\System32\ApplicationFrameHost.exe | 2021-11-24 18:02:15 |
| windows.immersivecontrolpanel_cw5n1h2tbyewy | 2021-11-24 15:40:31 |
| [Device HarddiskVolume2]\Program Files\VMware\VMware Tools\vmtoolsd.exe | 2021-11-24 18:02:14 |
| [Device HarddiskVolume2]\Windows\System32\cmd.exe | 2021-11-25 03:23:14 |
| [Device HarddiskVolume2]\Program Files (x86)\Mozilla Firefox\firefox.exe | 2021-11-25 03:46:20 |
| [Device HarddiskVolume2]\Program Files (x86)\Google\Update\GoogleUpdate.exe | 2021-11-25 03:43:40 |
| [Device HarddiskVolume2]\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | 2021-11-24 17:56:12 |
| [Device HarddiskVolume2]\Windows\System32\notepad.exe | 2021-11-25 03:42:53 |
| [Device HarddiskVolume2]\Users\TH-M-4n6\AppData\Local\Programs\Opera\opera.exe | 2021-11-25 04:12:35 |
| [Device HarddiskVolume2]\Program Files\Google\Chrome\Application\chrome.exe | 2021-11-25 03:43:50 |
| [Device HarddiskVolume2]\Windows\System32\msasn1.exe | 2021-11-25 04:00:04 |
| [Device HarddiskVolume2]\Windows\System32\systemsettings\AdminFlows.exe | 2021-11-25 04:00:54 |
| [Device HarddiskVolume2]\Windows\System32\sysmonPropertiesComputerName.exe | 2021-11-25 04:01:34 |
| [Device HarddiskVolume2]\Windows\System32\runnd32.exe | 2021-11-24 17:38:19 |
| [Device HarddiskVolume2]\Program Files (x86)\Windows Installation Assistant\Windows 10 Upgrader App.exe | 2021-11-24 18:01:52 |
| [Device HarddiskVolume2]\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe | 2021-11-24 15:21:35 |
| [Device HarddiskVolume2]\Program Files (x86)\Korusef\Edge\Application\imsedge.exe | 2021-11-24 15:23:43 |

cs-sa07-24019

John_Mbithi_Mutave

The screenshot shows a browser window for the TryHackMe website, specifically the Windows Forensics challenge. The main content area displays a registry key structure under 'Windows Portable Devices' and a table of device identification data.

Registry Key Structure:

- Key name: Windows Portable Devices
- Devices
 - SWD\#WP0BUSHUM# (22)

Device Identification Table:

| Timestamp | Device | Serial Number | Guid | Friendly Name |
|---------------------|--------|---------------|----------------------------------------|---------------|
| 2021-11-25 07:16:54 | | | {E251921F-4DA2-11EC-A783-001A700A7110} | USB |
| 2021-11-25 07:16:54 | | | {F529A906-4DE9-11EC-A782-001A700A7110} | New Volume |

We can compare the GUID we see here in this registry key and compare it with the Disk ID we see on keys mentioned in device identification to correlate the names with unique devices. Take a look at these two screenshots and answer Question # 3.

Combining all of this information, we can create a fair picture of any USB devices that were connected to the machine we're investigating.

Answer the questions below

What is the serial number of the device from the manufacturer 'Kingston'?

1C6f654E59A3B0C179D366AE&0 ✓ Correct Answer

What is the name of this device?

Kingston Data Traveler 2.0 USB Device ✓ Correct Answer

What is the friendly name of the device from the manufacturer 'Kingston'?

USB ✓ Correct Answer

Task 10 Hands-on Challenge

https://tryhackme.com/room/windowsforensics1

9:35 PM 7/22/2024

cs-sa07-24019

John_Mbithi_Mutave

Device identification:

The following locations keep track of USB keys plugged into a system. These locations store the vendor id, product id, and version of the USB device plugged in and can be used to identify unique devices. These locations also store the time the devices were plugged into the system.

First/Last Times:

Similarly, the following registry key tracks the first time the device was connected, the last time it was connected and the last time the device was removed from the system.

In this key, the ##### sign can be replaced by the following digits to get the required information:

| Value | Information |
|-------|-----------------------|
| 0064 | First Connection time |

USB device volume name:

The device name of the connected drive can be found at the following location:

Answer the questions below

What is the serial number of the device from the manufacturer 'Kingston'?

Answer format: *****

What is the name of this device?

Answer format: *****

What is the friendly name of the device from the manufacturer 'Kingston'?

cs-sa07-24019

John_Mbithi_Mutave

How many user created accounts are present on the system?

3 ✓ Correct Answer Hint

What is the username of the account that has never been logged in?

thm-user2 ✓ Correct Answer Hint

What's the password hint for the user THM-4n6?

count ✓ Correct Answer Hint

When was the file 'Changelog.txt' accessed?

2021-11-21 18:18:48 ✓ Correct Answer Hint

What is the complete path from where the python 3.8.2 installer was run?

Z:\setups\python-3.8.2.exe ✓ Correct Answer Hint

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

2021-11-24 18:40:06 ✓ Correct Answer Hint

Task 11 Conclusion

| Key name | # subkeys | Last write timestamp |
|-------------------------------------------|-----------|----------------------|
| RecentDocs | = | = |
| PolicyManager | 3 | 2019-12-07 09:15:12 |
| default | 245 | 2021-11-25 07:16:46 |
| ADMX_Desktop | 29 | 2021-10-06 13:57:16 |
| NoRecentDocsInHood | 0 | 2021-10-06 13:57:16 |
| ADMX_StartMenu | 67 | 2021-10-06 13:57:16 |
| ClearRecentDocsOnExit | 0 | 2021-10-06 13:57:16 |
| NoRecentDocsInMenu | 0 | 2021-10-06 13:57:16 |
| ADMX_WindowsExplorer | 71 | 2021-10-06 13:57:16 |
| MainRecentDocs | 0 | 2021-10-06 13:57:16 |
| Windows | 22 | 2021-10-06 13:57:16 |
| CurrentVersion | 153 | 2021-11-30 10:45:30 |
| Explorer | 79 | 2021-11-25 07:16:44 |
| CommandStore | 1 | 2019-12-07 09:17:23 |
| shell | 217 | 2021-11-25 07:16:05 |
| Windows.dearRecentDocs | 1 | 2019-12-07 09:15:12 |
| RecentDocs | 0 | 2019-12-07 09:17:23 |
| WOW6432Node | 9 | 2021-12-01 12:31:51 |
| Microsoft | 141 | 2021-12-01 12:31:51 |
| Windows | 12 | 2019-12-07 09:17:23 |
| CurrentVersion | 83 | 2021-12-01 12:31:51 |
| Explorer | 70 | 2021-12-01 12:31:51 |
| CommandStore | 1 | 2019-12-07 09:17:23 |
| shell | 196 | 2019-12-07 09:54:01 |
| Windows.dearRecentDocs | 1 | 2019-12-07 09:15:12 |
| RecentDocs | 0 | 2019-12-07 09:17:23 |
| C:\Users\THM-4n6\Desktop\WTUSER.DAT_clean | | |
| ROOT | 11 | 2021-12-01 12:32:14 |
| SOFTWARE | 12 | 2021-12-01 12:32:12 |
| Microsoft | 74 | 2021-12-01 12:32:15 |
| Windows | 7 | 2021-11-24 18:24:11 |

cs-sa07-24019

John_Mbithi_Mutave

The screenshot shows a completed room on TryHackMe. At the top, there's a navigation bar with links for Dashboard, Learn, Compete, and Other. A green banner at the top indicates "Room completed (100%)". Below this, a list of tasks is shown in a dark-themed card:

- Task 1: Introduction to Windows Forensics (Completed)
- Task 2: Windows Registry and Forensics (Completed)
- Task 3: Accessing registry hives offline (Completed)
- Task 4: Data Acquisition (Completed)
- Task 5: Exploring Windows Registry (Completed)
- Task 6: System Information and System Accounts (Completed)
- Task 7: Usage or knowledge of files/folders (Completed)
- Task 8: Evidence of Execution (Completed)
- Task 9: External Devices/USB device forensics (Completed)

The screenshot shows a room page on TryHackMe. At the top, there's a navigation bar with links for Dashboard, Learn, Compete, and Other. A green banner at the top indicates "Room completed (100%)". Below this, a list of tasks is shown in a dark-themed card:

- Task 1: Introduction to Windows Forensics (Completed)
- Task 2: Windows Registry and Forensics (Completed)
- Task 3: Accessing registry hives offline (Completed)
- Task 4: Data Acquisition (Completed)
- Task 5: Exploring Windows Registry (Completed)
- Task 6: System Information and System Accounts (Completed)
- Task 7: Usage or knowledge of files/folders (Completed)
- Task 8: Evidence of Execution (Completed)
- Task 9: External Devices/USB device forensics (Completed)

In the center, there's a terminal window showing a command prompt with the path: `USB device Volume Name: SOFTWARE\Microsoft\Windows Portable Devices\Devices`. To the right of the terminal, there's some text about using links to explore tools and playing with KAPE, regripper, and EZtools.

You can use the links provided within Task 3 to explore more about the tools we introduced. Furthermore, if you like, you can play around with KAPE, regripper, and EZtools in the VM attached with the room.

You can learn more about Windows Forensics in our [Windows Forensics 2](#) room, where we cover even more exciting ways to perform forensics on a Windows machine, and the [KAPE](#) room to understand how to perform forensics in a quick and efficient manner.

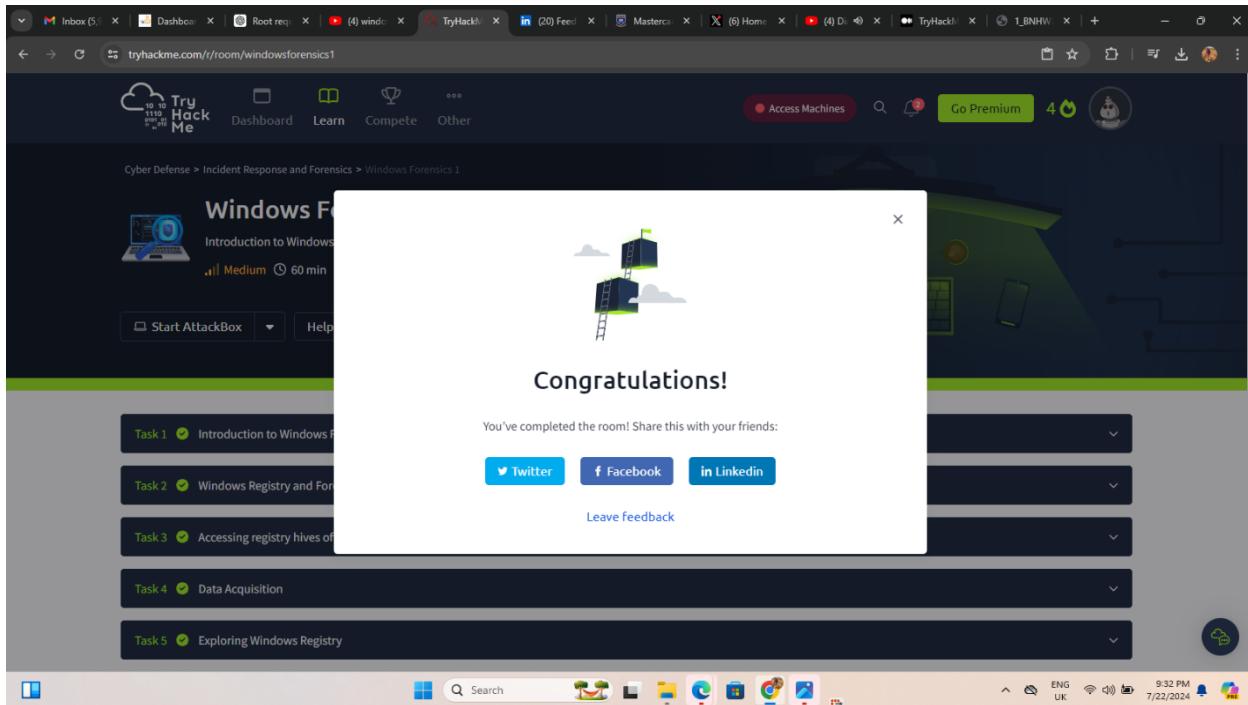
Answer the questions below

Review the provided resources.

No answer needed ✓ Correct Answer

| Created by | Room Type | Users in Room | Created |
|--------------------------|---------------------------------------------------------------------------------------|---------------|--------------|
| tryhackme umairalizafar | Free Room. Anyone can deploy virtual machines in the room (without being subscribed)! | 53,620 | 916 days ago |

Copyright TryHackMe 2018-2024



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.