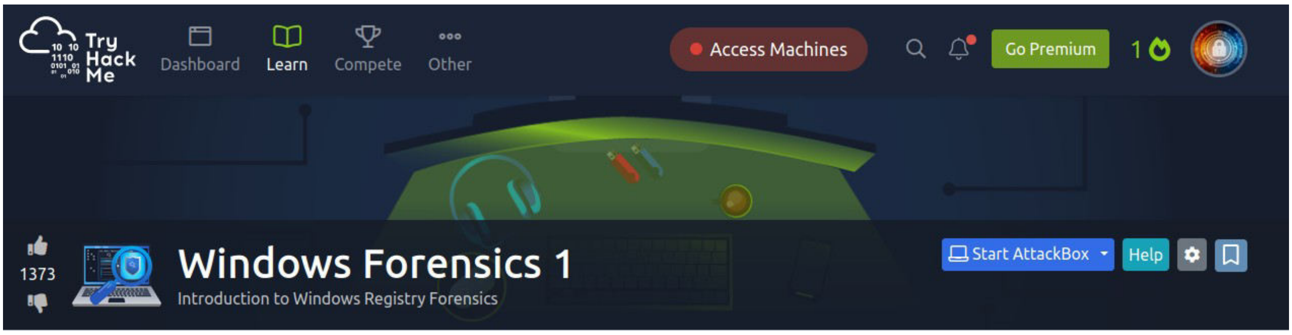
**Eric Mwenda**

**Windows Forensics 1**

https://tryhackme.com/p/Ericm



Windows Forensics 1

Introduction to Windows Registry Forensics

## Introduction to Windows Forensics.

Computer forensics is an essential field of cyber security that involves gathering evidence of activities performed on computers.

The applications of digital and computer forensics are wide-ranging, from the legal sphere, where it is used to support or refute a hypothesis in a civil or criminal case, to the private sphere, where it helps in internal corporate investigations and incident and intrusion analysis.

Digital Forensics field, which deals with forensic analysis of all types of digital devices, including recovering, examining, and analyzing data found in digital devices.

Microsoft Windows is by large the most used Desktop Operating System right now. Private users and Enterprises prefer it, and it currently holds roughly 80% of the Desktop market share. This means that it is important to know how to perform forensic analysis on Microsoft Windows for someone interested in Digital Forensics.

## Forensic Artifacts.

Forensic artifacts are essential pieces of information that provide evidence of human activity

Forensics artifact example during an investigation of a crime scene, fingerprints, a broken button of a shirt or coat, the tools used to perform the crime are all considered forensic artifacts.

## Is my computer spying on me?

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.

## Answer the questions below

What is the most used Desktop Operating System right now?

**Microsoft Windows**

## Windows Registry and Forensics.

The Windows Registry is a collection of databases that contains the system's configuration data. This configuration data can be about the hardware, the software or the user's information. It also includes data about the recently used files, programs used or devices connected to the system.

We view the registry using regedit.exe, a built-in Windows utility to view and edit the registry.

The Windows registry consists of Keys and Values. When you open the regedit.exe utility to view the registry, the folders you see are Registry Keys. Registry Values are the data stored in these Registry Keys. A Registry Hive is a group of Keys, subkeys, and values stored in a single file on the disk.

### Structure of the Registry:

The registry on any Windows system contains the following five root keys:

- HKEY_CURRENT_USER
- HKEY_USERS
- HKEY_LOCAL_MACHINE
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_CONFIG

**HKEY_CURRENT_USER (HKCU)** - Contains the root of the configuration information for the user who is currently logged on. The user's folders, screen colors, and Control Panel settings are stored here. This information is associated with the user's profile.

**HKEY_USERS (HKU)** - Contains all the actively loaded user profiles on the computer. HKEY_CURRENT_USER is a subkey of HKEY_USERS.

**HKEY_LOCAL_MACHINE (HKLM)** - Contains configuration information particular to the computer (for any user).

**HKEY_CLASSES_ROOT (HKCR)** - Is a subkey of HKEY_LOCAL_MACHINE\Software. The information that is stored here makes sure that the correct program opens when you open a file by using Windows Explorer.

**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**

## Accessing registry hives offline.

If you are accessing a live system, you will be able to access the registry using regedit.exe, and you will be greeted with all of the standard root keys we learned about in the previous task. However, if you only have access to a disk image, you must know where the registry hives are located on the disk. The majority of these hives are located in the C:\Windows\System32\Config directory.

This directories are:-

- DEFAULT (mounted on HKEY_USERS\DEFAULT)

- SAM (mounted on HKEY_LOCAL_MACHINE\SAM)

- SECURITY (mounted on HKEY_LOCAL_MACHINE\Security)

- SOFTWARE (mounted on HKEY_LOCAL_MACHINE\Software)

- SYSTEM (mounted on HKEY_LOCAL_MACHINE\System)

## The Amcache Hive.

This hive is located in C:\Windows\AppCompat\Programs\Amcache.hve. Windows creates this hive to save information on programs that were recently run on the system.

## 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/modified 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**

What is the path for the AmCache hive?

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

## Data Acquisition.

This is the process carried out when performing forensics, we will either encounter a live system or an image taken of the system. For the sake of accuracy, it is recommended practice to image the system or make a copy of the required data and perform forensics on it.

The forensically correct method is to acquire a copy of this data and perform analysis on that copy.

Hives from %WINDIR%\System32\Config, we cannot because it is a restricted file. So, what to do now?

For acquiring these files, we can use one of the following tools:

### 1. KAPE:

KAPE is a live data acquisition and analysis tool which can be used to acquire registry data. It is primarily a command-line tool but also comes with a GUI.

### 2. Autopsy:

Autopsy gives you the option to acquire data from both live systems or from a disk image. After adding your data source, navigate to the location of the files you want to extract, then right-click and select the Extract File(s) option.

### 3. FTK Imager:

FTK Imager is similar to Autopsy and allows you to extract files from a disk image or a live system by mounting the said disk image or drive in FTK Imager.

Another way you can extract Registry files from FTK Imager is through the Obtain Protected Files option. This option is only available for live systems and is highlighted in the screenshot below. This option allows you to extract all the registry hives to a location of your choosing. However, it will not copy the Amcache.hve file, which is often necessary to investigate evidence of programs that were last executed.

## Exploring Windows Registry.

Once we have extracted the registry hives, we need a tool to view these files as we would in the registry editor. Since the registry editor only works with live systems and can't load exported hives, we can use the following tools:

### 1. Registry Viewer:

AccessData's Registry Viewer has a similar user interface to the Windows Registry Editor. There are a couple of limitations, though. It only loads one hive at a time, and it can't take the transaction logs into account.

### 2. Zimmerman's Registry Explorer:

Eric Zimmerman has developed a handful of tools that are very useful for performing Digital Forensics and Incident Response. One of them is the Registry Explorer.

It can load multiple hives simultaneously and add data from transaction logs into the hive to make a more 'cleaner' hive with more up-to-date data. It also has a handy 'Bookmarks' option containing forensically important registry keys often sought by forensics investigators. Investigators can go straight to the interesting registry keys and values with the bookmarks menu item.

## RegRipper:

RegRipper is a utility that takes a registry hive as input and outputs a report that extracts data from some of the forensically important keys and values in that hive. The output report is in a text file and shows all the results in sequential order.

RegRipper is available in both a CLI and GUI form.

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.

## System Information and System Accounts.

When we start performing forensic analysis, the first step is to find out about the system information. This task will cover gathering information related to a machine's System and Account information.

### OS Version:

If we only have triage data to perform forensics, we can determine the OS version from which this data was pulled through the registry.

To find the OS version, we can use the following registry key: **SOFTWARE\Microsoft\Windows NT\CurrentVersion**

### Current Control Set:

The hives containing the machine’s configuration data used for controlling system startup are called Control Sets. Commonly, we will see two Control Sets, ControlSet001 and ControlSet002, in the SYSTEM hive on a machine. In most cases, ControlSet001 will point to the Control Set that the machine booted with, and ControlSet002 will be the last known good configuration. Their locations will be:

**SYSTEM\ControlSet001**

**SYSTEM\ControlSet002**

Windows creates a volatile Control Set when the machine is live, called the CurrentControlSet **(HKLM\SYSTEM\CurrentControlSet).** For getting the most accurate system information, this is the hive that we will refer to

We can find out which Control Set is being used as the CurrentControlSet by looking at the following registry value: **SYSTEM\Select\Current**

Similarly, the last known good configuration can be found using the following registry value:

**SYSTEM\Select\LastKnownGood**

### Computer Name:

It is crucial to establish the Computer Name while performing forensic analysis to ensure that we are working on the machine we are supposed to work on. We can find the Computer Name from the following location: **SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName**

## Time Zone Information:

For accuracy, it is important to establish what time zone the computer is located in. This will help us understand the chronology of the events as they happened. For finding the Time Zone Information, we can look at the following location: **SYSTEM\CurrentControlSet\Control\TimeZoneInformation**

Time Zone Information is important because some data in the computer will have their timestamps in UTC/GMT and others in the local time zone. Knowledge of the local time zone helps in establishing a timeline when merging data from all the sources.

## Network Interfaces and Past Networks:

The following registry key will give a list of network interfaces on the machine we are investigating: **SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces**

Each Interface is represented with a unique identifier (GUID) subkey, which contains values relating to the interface's TCP/IP configuration. This key will provide us with information like IP addresses, DHCP IP address and Subnet Mask, DNS Servers, and more. This information is significant because it helps you make sure that you are performing forensics on the machine that you are supposed to perform it on.

The past networks a given machine was connected to can be found in the following locations:

**SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged**

**SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed**

## Autostart Programs (Autoruns):

The following registry keys include information about programs or commands that run when a user logs on.

**NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run**

**NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce**

**SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce**

**SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run**

**SOFTWARE\Microsoft\Windows\CurrentVersion\Run**

The following registry key contains information about services: **SYSTEM\CurrentControlSet\Services**

In this registry key, if the start key is set to 0x02, this means that this service will start at boot.

## SAM hive and user information:

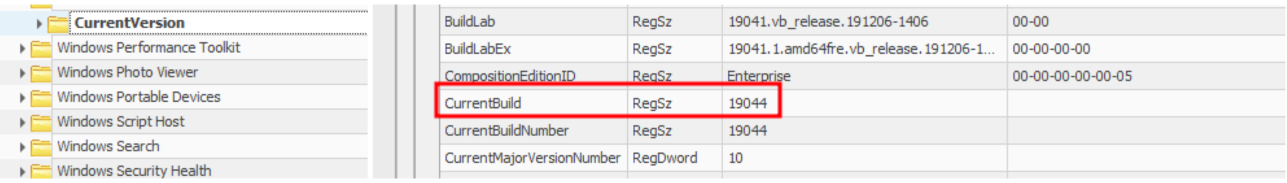
The SAM hive contains user account information, login information, and group information. This information is mainly located in the following location: **SAM\Domains\Account\Users**

The information contained here includes the relative identifier (RID) of the user, number of times the user logged in, last login time, last failed login, last password change, password expiry, password policy and password hint, and any groups that the user is a part of.

## Answer the questions below

What is the Current Build Number of the machine whose data is being investigated?

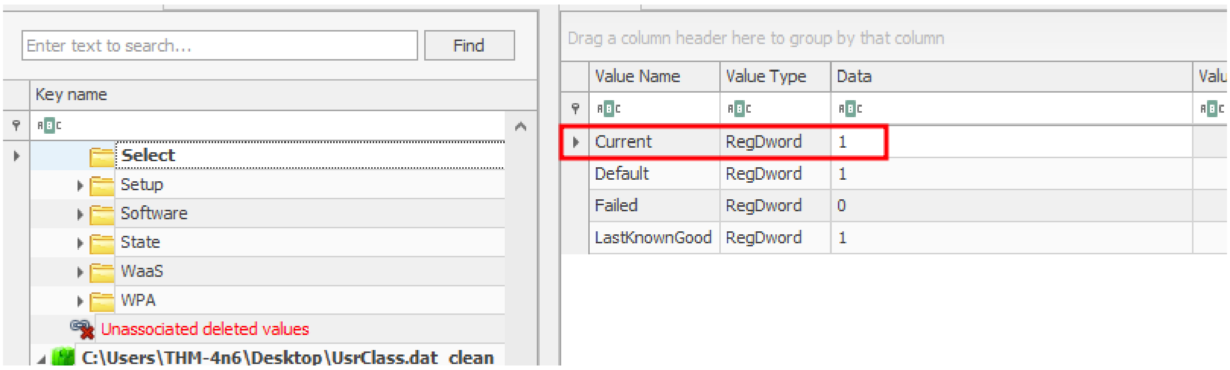
**Ans: 19044**



| | | | |
|---|---|---|---|
| BuildLab | RegSz | 19041.vb_release.191206-1406 | 00-00 |
| BuildLabEx | RegSz | 19041.1.amd64fre.vb_release.191206-1... | 00-00-00-00 |
| CompositionEditionID | RegSz | Enterprise | 00-00-00-00-00-05 |
| CurrentBuild | RegSz | 19044 | |
| CurrentBuildNumber | RegSz | 19044 | |
| CurrentMajorVersionNumber | RegDword | 10 | |

Which ControlSet contains the last known good configuration?

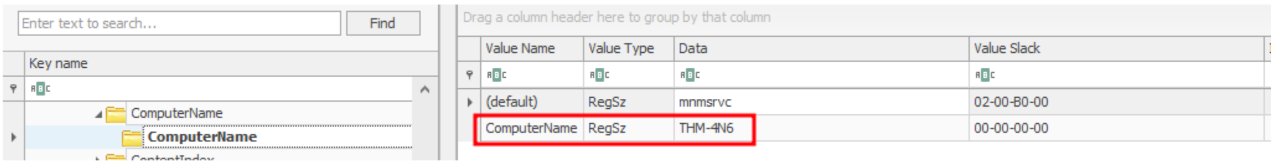
**Ans: 1**


Enter text to search...
Find
Key name
Select
Setup
Software
State
WaaS
WPA
Unassociated deleted values
C:\Users\THM-4n6\Desktop\UsrClass.dat clean
Drag a column header here to group by that column

| Value Name | Value Type | Data | Valu |
|---|---|---|---|
| Current | RegDword | 1 | |
| Default | RegDword | 1 | |
| Failed | RegDword | 0 | |
| LastKnownGood | RegDword | 1 | |

What is the Computer Name of the computer?

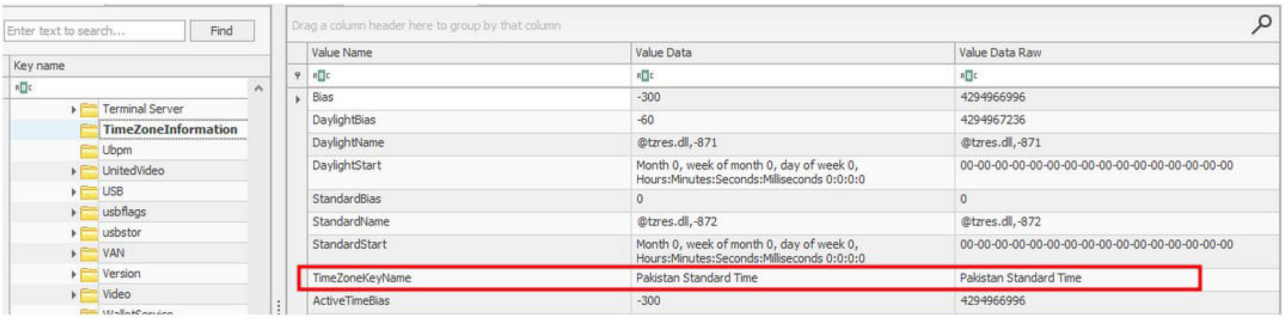
**Ans: THM-4N6**



| Value Name | Value Type | Data | Value Slack |
|---|---|---|---|
| (default) | RegSz | mnmsrvc | 02-00-B0-00 |
| ComputerName | RegSz | THM-4N6 | 00-00-00-00 |

What is the value of the TimeZoneKeyName?

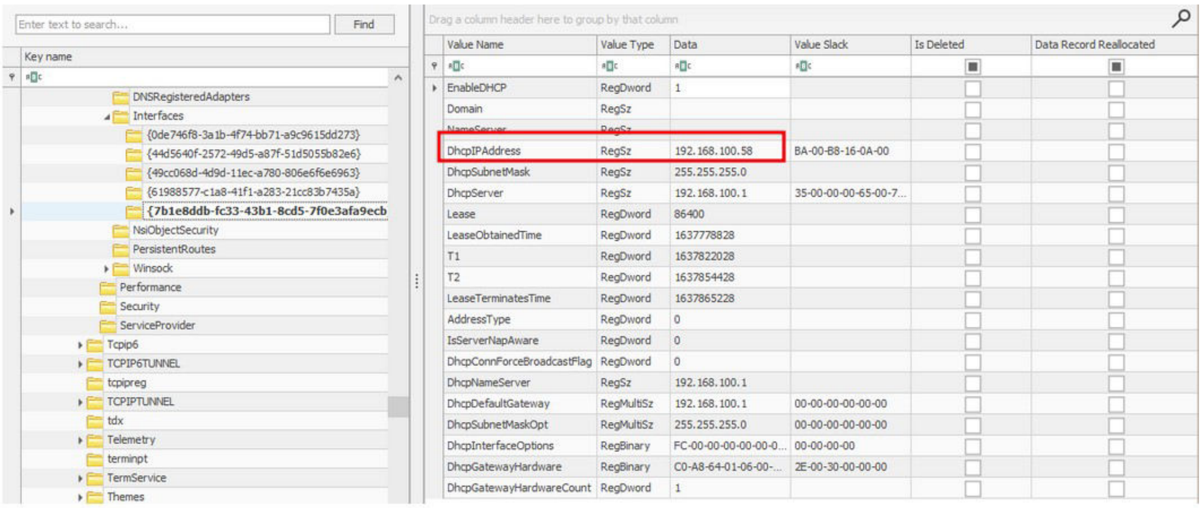
**Ans: Pakistan Standard Time**



| Value Name | Value Data | Value Data Raw |
|---|---|---|
| Bias | -300 | 4294966996 |
| DaylightBias | -60 | 4294967236 |
| DaylightName | @tzres.dll,-871 | @tzres.dll,-871 |
| DaylightStart | Month 0, week of month 0, day of week 0,<br>Hours:Minutes:Seconds:Milliseconds 0:0:0:0 | 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 |
| StandardBias | 0 | 0 |
| StandardName | @tzres.dll,-872 | @tzres.dll,-872 |
| StandardStart | Month 0, week of month 0, day of week 0,<br>Hours:Minutes:Seconds:Milliseconds 0:0:0:0 | 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 |
| TimeZoneKeyName | Pakistan Standard Time | Pakistan Standard Time |
| ActiveTimeBias | -300 | 4294966996 |

What is the DHCP IP address

**Ans: 192.168.100.58**



Enter text to search... Find

Key name

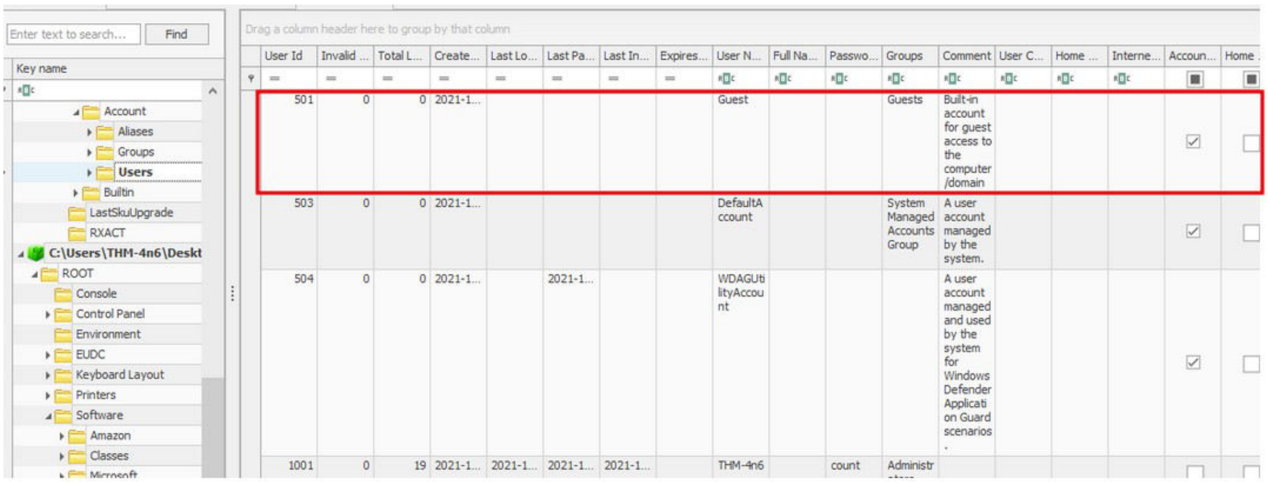
DNSRegisteredAdapters
Interfaces
{0de746f8-3a1b-4f74-bb71-a9c9615dd273}
{44d5640f-2572-49d5-a87f-51d5055b82e6}
{49cc068d-4d9d-11ec-a780-806e6f6e6963}
{61988577-c1a8-41f1-a283-21cc83b7435a}
**{7b1e8ddb-fc33-43b1-8cd5-7f0e3afa9ecb**
NsiObjectSecurity
PersistentRoutes
Winsock
Performance
Security
ServiceProvider
Tcpip6
TCPIP6TUNNEL
tcpipreg
TCPIPTUNNEL
tdx
Telemetry
terminpt
TermService
Themes

Drag a column header here to group by that column

| Value Name | Value Type | Data | Value Slack | Is Deleted | Data Record Reallocated |
|---|---|---|---|---|---|
| EnableDHCP | RegDword | 1 | | □ | □ |
| Domain | RegSz | | | □ | □ |
| NameServer | RegSz | | | □ | □ |
| DhcpIPAddress | RegSz | 192.168.100.58 | BA-00-B8-16-0A-00 | □ | □ |
| DhcpSubnetMask | RegSz | 255.255.255.0 | | □ | □ |
| DhcpServer | RegSz | 192.168.100.1 | 35-00-00-00-65-00-7... | □ | □ |
| Lease | RegDword | 86400 | | □ | □ |
| LeaseObtainedTime | RegDword | 1637778828 | | □ | □ |
| T1 | RegDword | 1637822028 | | □ | □ |
| T2 | RegDword | 1637854428 | | □ | □ |
| LeaseTerminatesTime | RegDword | 1637865228 | | □ | □ |
| AddressType | RegDword | 0 | | □ | □ |
| IsServerNapAware | RegDword | 0 | | □ | □ |
| DhcpConnForceBroadcastFlag | RegDword | 0 | | □ | □ |
| DhcpNameServer | RegSz | 192.168.100.1 | | □ | □ |
| DhcpDefaultGateway | RegMultiSz | 192.168.100.1 | 00-00-00-00-00-00 | □ | □ |
| DhcpSubnetMaskOpt | RegMultiSz | 255.255.255.0 | 00-00-00-00-00-00 | □ | □ |
| DhcpInterfaceOptions | RegBinary | FC-00-00-00-00-00-0... | 00-00-00-00 | □ | □ |
| DhcpGatewayHardware | RegBinary | C0-A8-64-01-06-00-... | 2E-00-30-00-00-00 | □ | □ |
| DhcpGatewayHardwareCount | RegDword | 1 | | □ | □ |

What is the RID of the Guest User account?

**Ans: 501**



Enter text to search... Find

Key name

Account
Aliases
Groups
**Users**
Builtin
LastSkuUpgrade
RXACT
**C:\Users\THM-4n6\Deskt**
ROOT
Console
Control Panel
Environment
EUDC
Keyboard Layout
Printers
Software
Amazon
Classes
Microsoft

Drag a column header here to group by that column

| User Id | Invalid ... | Total L... | Create... | Last Lo... | Last Pa... | Last In... | Expires... | User N... | Full Na... | Passwo... | Groups | Comment | User C... | Home ... | Interne... | Accoun... | Home ... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 501 | 0 | 0 | 2021-1... | | | | | Guest | | | Guests | Built-in account for guest access to the computer /domain | | | | ☑ | □ |
| 503 | 0 | 0 | 2021-1... | | | | | DefaultAccount | | | System Managed Accounts Group | A user account managed by the system. | | | | ☑ | □ |
| 504 | 0 | 0 | 2021-1... | | 2021-1... | | | WDAGUtilityAccount | | | | A user account managed and used by the system for Windows Defender Application Guard scenarios . | | | | ☑ | □ |
| 1001 | 0 | 19 | 2021-1... | 2021-1... | 2021-1... | 2021-1... | | THM-4n6 | | count | Administr | | | | | □ | □ |

## Usage or knowledge of files/folders

### Recent Files:

Windows maintains a list of recently opened files for each user. As we might have seen when using Windows Explorer, it shows us a list of recently used files. This information is stored in the NTUSER hive and can be found on the following location:

**NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs**

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.

Another interesting piece of information in this registry key is that there are different keys with file extensions, such as .pdf, .jpg, .docx etc. These keys provide us with information about the last used files of a specific file extension. So if we are looking specifically for the last used PDF files, we can look at the following registry key:

**NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf**

**Office Recent Files:**

Similar to the Recent Docs maintained by Windows Explorer, Microsoft Office also maintains a list of recently opened documents. This list is also located in the NTUSER hive. It can be found in the following location: **NTUSER.DAT\Software\Microsoft\Office\VERSION**

The version number for each Microsoft Office release is different. An example registry key will look like this: **NTUSER.DAT\Software\Microsoft\Office\15.0\Word**

Here, the 15.0 refers to Office 2013. A list of different Office releases and their version numbers can be found on this link.

Starting from Office 365, Microsoft now ties the location to the user's live ID. In such a scenario, the recent files can be found at the following location.

**NTUSER.DAT\Software\Microsoft\Office\VERSION\UserMRU\LiveID_####\FileMRU**

In such a scenario, the recent files can be found at the following location. This location also saves the complete path of the most recently used files.

**ShellBags:**

When any user opens a folder, it opens in a specific layout. Users can change this layout according to their preferences. These layouts can be different for different folders. This information about the Windows 'shell' is stored and can identify the Most Recently Used files and folders. Since this setting is different for each user, it is located in the user hives. We can find this information on the following locations:

**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**

**NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags**

Registry Explorer doesn't give us much information about ShellBags. However, another tool from Eric Zimmerman's tools called the **ShellBag Explorer** shows us the information in an easy-to-use format. We just have to point to the hive file we have extracted, and it parses the data and shows us the results.

**Open/Save and LastVisited Dialog MRUs:**

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\ComDlg32\OpenSavePIDlMRU**

**NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU**

**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.

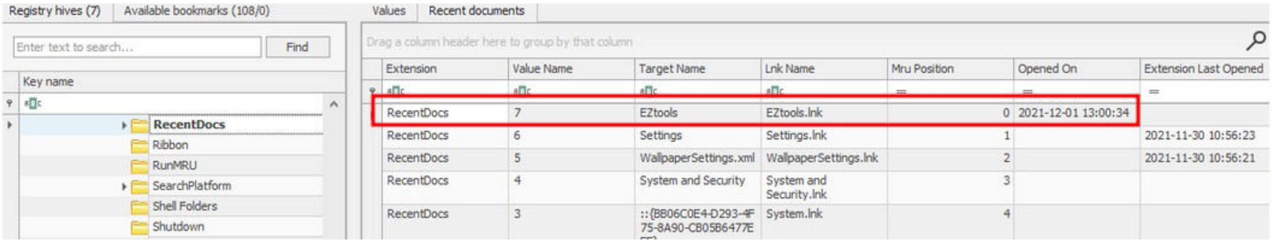
**NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths**

**NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery**

## Answer the questions below

When was EZtools opened?

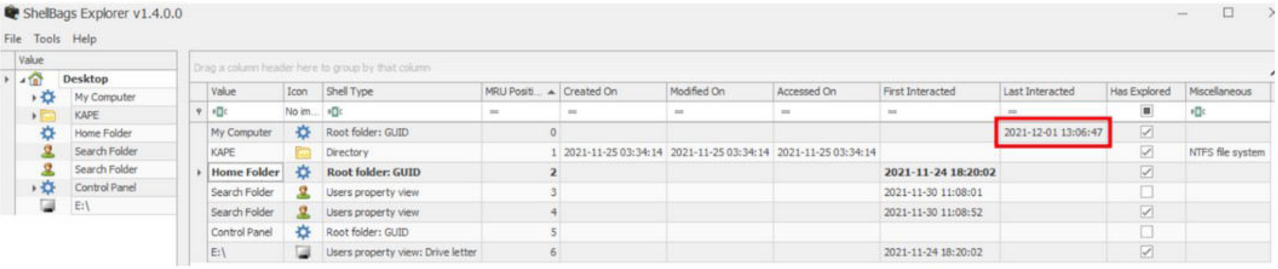
**Ans: 2021-12-01 13:00:34**



| Extension | Value Name | Target Name | Lnk Name | Mru Position | Opened On | Extension Last Opened |
|---|---|---|---|---|---|---|
| RecentDocs | 7 | EZtools | EZtools.lnk | 0 | 2021-12-01 13:00:34 | |
| 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 | ::{BB06C0E4-D293-4F75-8A90-CB05B6477E | System.lnk | 4 | | |

At what time was My Computer last interacted with?

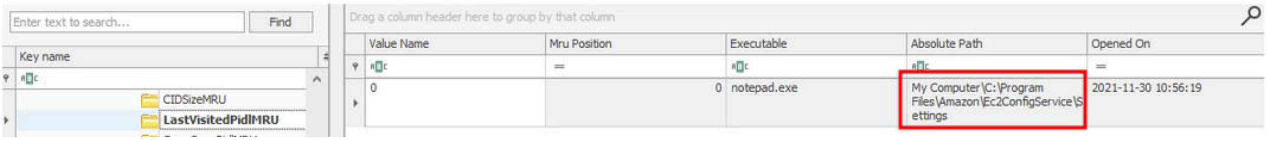
**Ans: 2021-12-01 13:06:47**



| Value | Icon | Shell Type | MRU Positi... | Created On | Modified On | Accessed On | First Interacted | Last Interacted | Has Explored | Miscellaneous |
|---|---|---|---|---|---|---|---|---|---|---|
| My Computer | | Root folder: GUID | 0 | | | | | 2021-12-01 13:06:47 | ☑ | |
| KAPE | | Directory | 1 | 2021-11-25 03:34:14 | 2021-11-25 03:34:14 | 2021-11-25 03:34:14 | | | ☑ | NTFS file system |
| **Home Folder** | | **Root folder: GUID** | **2** | | | | **2021-11-24 18:20:02** | | ☑ | |
| Search Folder | | Users property view | 3 | | | | 2021-11-30 11:08:01 | | ☐ | |
| Search Folder | | Users property view | 4 | | | | 2021-11-30 11:08:52 | | ☑ | |
| Control Panel | | Root folder: GUID | 5 | | | | | | ☐ | |
| E:\ | | Users property view: Drive letter | 6 | | | | 2021-11-24 18:20:02 | | ☑ | |

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

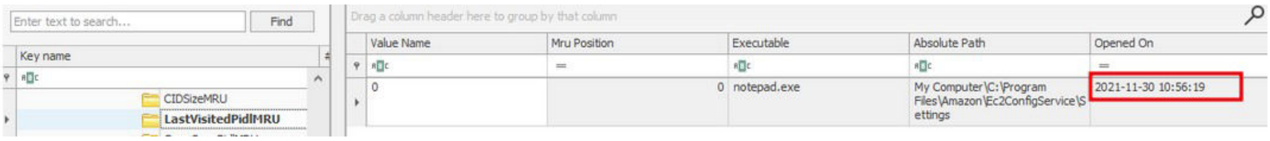
**Ans: C:\Program Files\Amazon\Ec2ConfigService\Settings**



| 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 |

When was this file opened?

**Ans: 2021-11-30 10:56:19**



| 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 |

## Evidence of Execution

### UserAssist:

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**

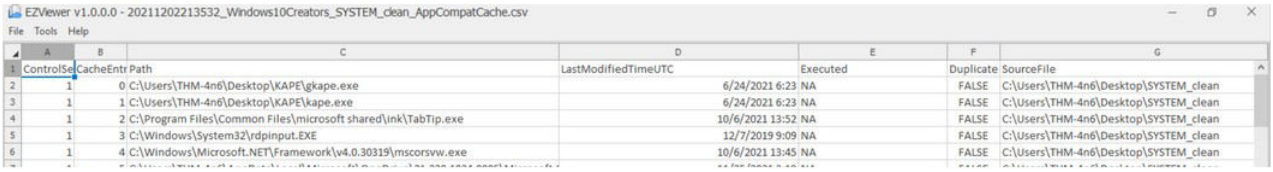
**<u>ShimCache:</u>**

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.

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.



EZViewer v1.0.0.0 - 20211202213532_Windows10Creators_SYSTEM_clean_AppCompatCache.csv

|  | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | ControlSe | CacheEntr | Path | LastModifiedTimeUTC | Executed | Duplicate | SourceFile |
| 2 | 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 | 1 | C:\Users\THM-4n6\Desktop\KAPE\kape.exe | 6/24/2021 6:23 | NA | FALSE | C:\Users\THM-4n6\Desktop\SYSTEM_clean |
| 4 | 1 | 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 | 1 | 3 | C:\Windows\System32\rdpinput.EXE | 12/7/2019 9:09 | NA | FALSE | C:\Users\THM-4n6\Desktop\SYSTEM_clean |
| 6 | 1 | 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 |

We can use the following command to run the AppCompatCache Parser Utility:

**AppCompatCacheParser.exe --csv <path to save output> -f <path to SYSTEM hive for data parsing> -c <control set to parse>**

The output can be viewed using EZviewer, another one of Eric Zimmerman's tools.

**<u>AmCache:</u>**

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.hve

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

**Amcache.hve\Root\File\{Volume GUID}**

**<u>BAM/DAM:</u>**

Background Activity Monitor or BAM keeps a tab on the activity of background applications. Similar Desktop Activity Moderator or DAM is a part of Microsoft Windows that optimizes the power consumption of the device. Both of these are a part of the Modern Standby system in Microsoft Windows.

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.

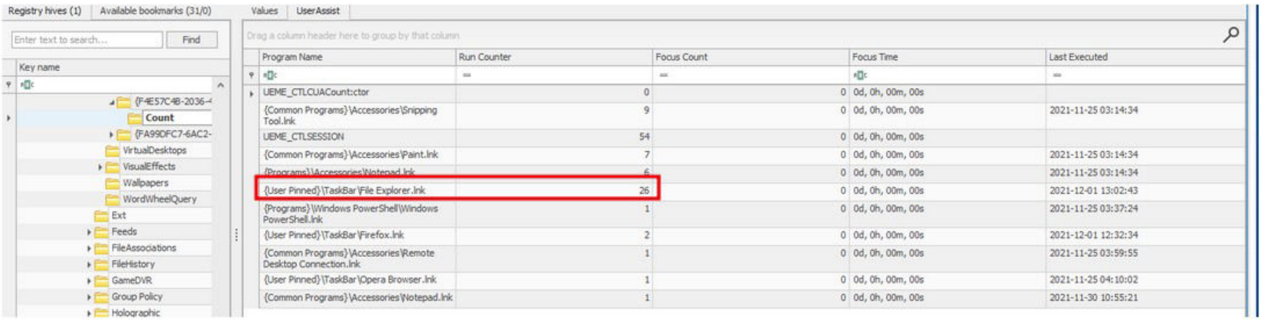
**SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}**

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

## Answer the questions below

How many times was the File Explorer launched?

**Ans: 26**



| Program Name | Run Counter | Focus Count | Focus Time | Last Executed |
|---|---|---|---|---|
| UEME_CTLCUACount:ctor | 0 | 0 | 0d, 0h, 00m, 00s | |
| {Common Programs}\Accessories\Snipping Tool.lnk | 9 | 0 | 0d, 0h, 00m, 00s | 2021-11-25 03:14:34 |
| UEME_CTLSESSION | 54 | 0 | 0d, 0h, 00m, 00s | |
| {Common Programs}\Accessories\Paint.lnk | 7 | 0 | 0d, 0h, 00m, 00s | 2021-11-25 03:14:34 |
| {Programs}\Accessories\Notepad.lnk | 6 | 0 | 0d, 0h, 00m, 00s | 2021-11-25 03:14:34 |
| {User Pinned}\TaskBar\File Explorer.lnk | 26 | 0 | 0d, 0h, 00m, 00s | 2021-12-01 13:02:43 |
| {Programs}\Windows PowerShell\Windows PowerShell.lnk | 1 | 0 | 0d, 0h, 00m, 00s | 2021-11-25 03:37:24 |
| {User Pinned}\TaskBar\Firefox.lnk | 2 | 0 | 0d, 0h, 00m, 00s | 2021-12-01 12:32:34 |
| {Common Programs}\Accessories\Remote Desktop Connection.lnk | 1 | 0 | 0d, 0h, 00m, 00s | 2021-11-25 03:59:55 |
| {User Pinned}\TaskBar\Opera Browser.lnk | 1 | 0 | 0d, 0h, 00m, 00s | 2021-11-25 04:10:02 |
| {Common Programs}\Accessories\Notepad.lnk | 1 | 0 | 0d, 0h, 00m, 00s | 2021-11-30 10:55:21 |

What is another name for ShimCache?

**AppCompatCache**

Which of the artifacts also saves SHA1 hashes of the executed programs?

**AmCache**

Which of the artifacts saves the full path of the executed programs?

**Bam/Dam**

## External Devices/USB device forensics

When performing forensics on a machine, often the need arises to identify if any USB or removable drives were attached to the machine. If so, any information related to those devices is important for a forensic investigator. In this task, we will go through the different ways to find information on connected devices and the drives on a system using the registry.

### 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.

**SYSTEM\CurrentControlSet\Enum\USBSTOR**

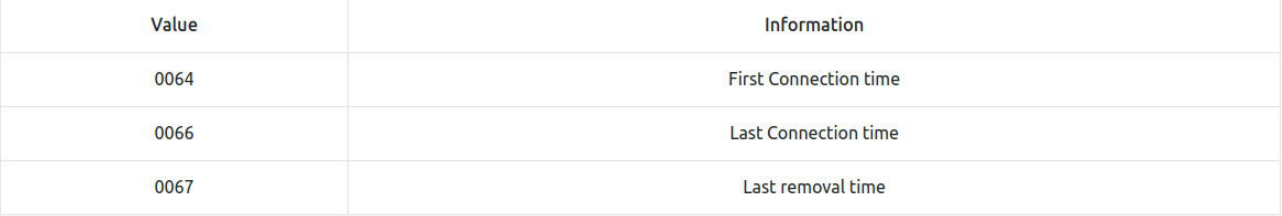
**SYSTEM\CurrentControlSet\Enum\USB**

### 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.

SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USBSerial#\Properties\{83da6326-97a6-4088-9453-a19231573b29}\####

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



| Value | Information |
|---|---|
| 0064 | First Connection time |
| 0066 | Last Connection time |
| 0067 | Last removal time |

USB device Volume Name:

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

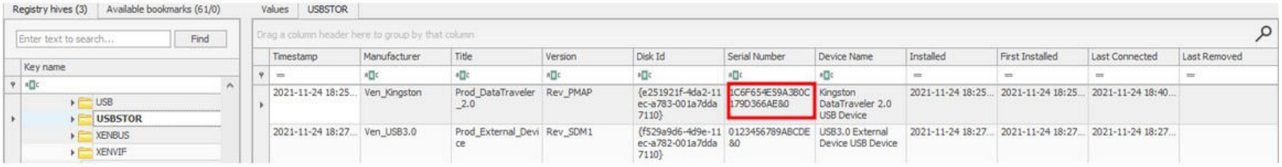
**SOFTWARE\Microsoft\Windows Portable Devices\Devices**

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

## Answer the questions below

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

**Ans: 1C6F654E59A3B0C179D366AE&0**



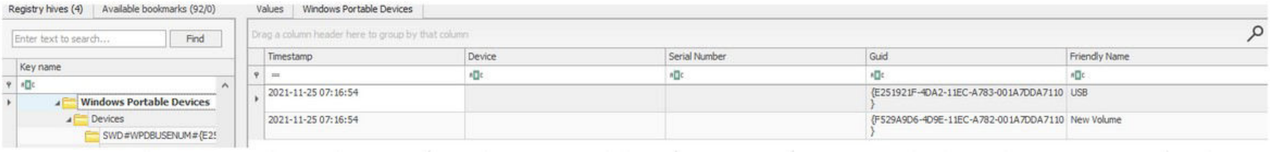
| Timestamp | Manufacturer | Title | Version | Disk Id | Serial Number | Device Name | Installed | First Installed | Last Connected | Last Removed |
|---|---|---|---|---|---|---|---|---|---|---|
| 2021-11-24 18:25... | Ven_Kingston | Prod_DataTraveler_2.0 | Rev_PMAP | {e251921f-4da2-11ec-a783-001a7dda7110} | 1C6F654E59A3B0C179D366AE&0 | Kingston DataTraveler 2.0 USB Device | 2021-11-24 18:25... | 2021-11-24 18:25... | 2021-11-24 18:40... | |
| 2021-11-24 18:27... | Ven_USB3.0 | Prod_External_Device | Rev_SDM1 | {f529a9d6-4d9e-11ec-a782-001a7dda7110} | 0123456789ABCDE&0 | USB3.0 External Device USB Device | 2021-11-24 18:27... | 2021-11-24 18:27... | 2021-11-24 18:27... | |

What is the name of this device?

**Kingston Data Traveller**

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

Ans: USB



| Timestamp | Device | Serial Number | Guid | Friendly Name |
|---|---|---|---|---|
| 2021-11-25 07:16:54 | | | {E251921F-4DA2-11EC-A783-001A7DDA7110} | USB |
| 2021-11-25 07:16:54 | | | {F529A9D6-4D9E-11EC-A782-001A7DDA7110} | New Volume |

## Hands-on Challenge

The Setup:

If preferred, use the following credentials to log into the machine:

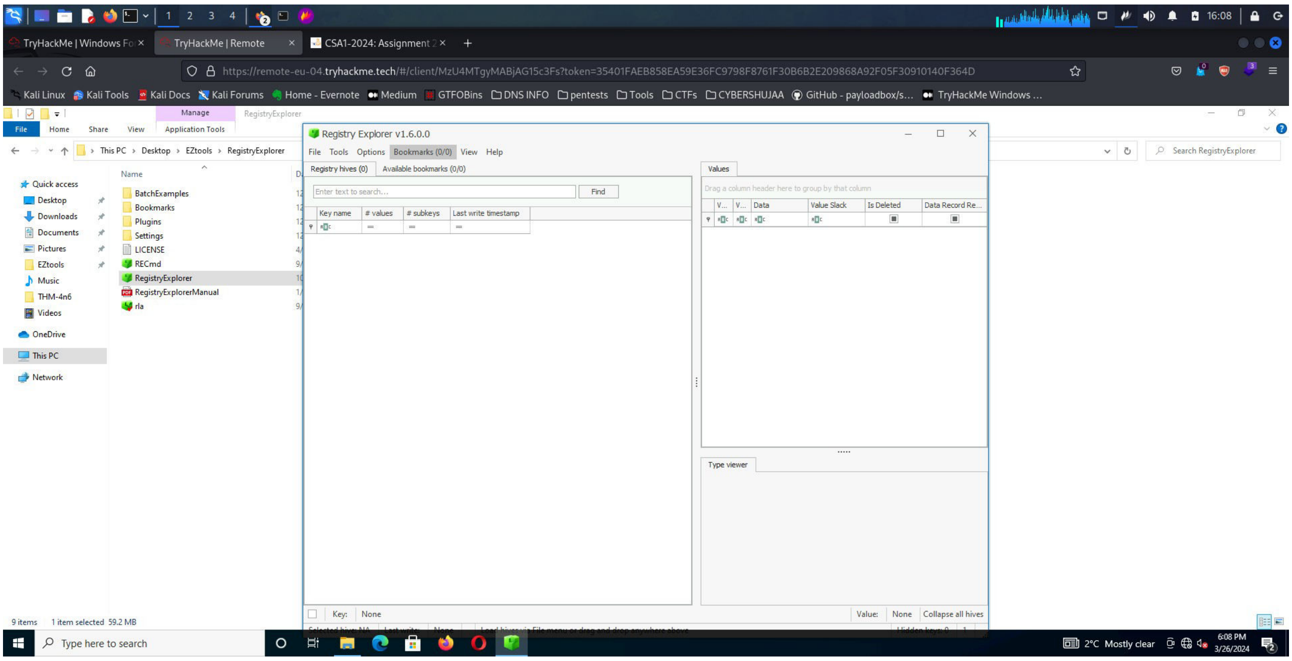
**Username: THM-4n6**

**Password: 123**

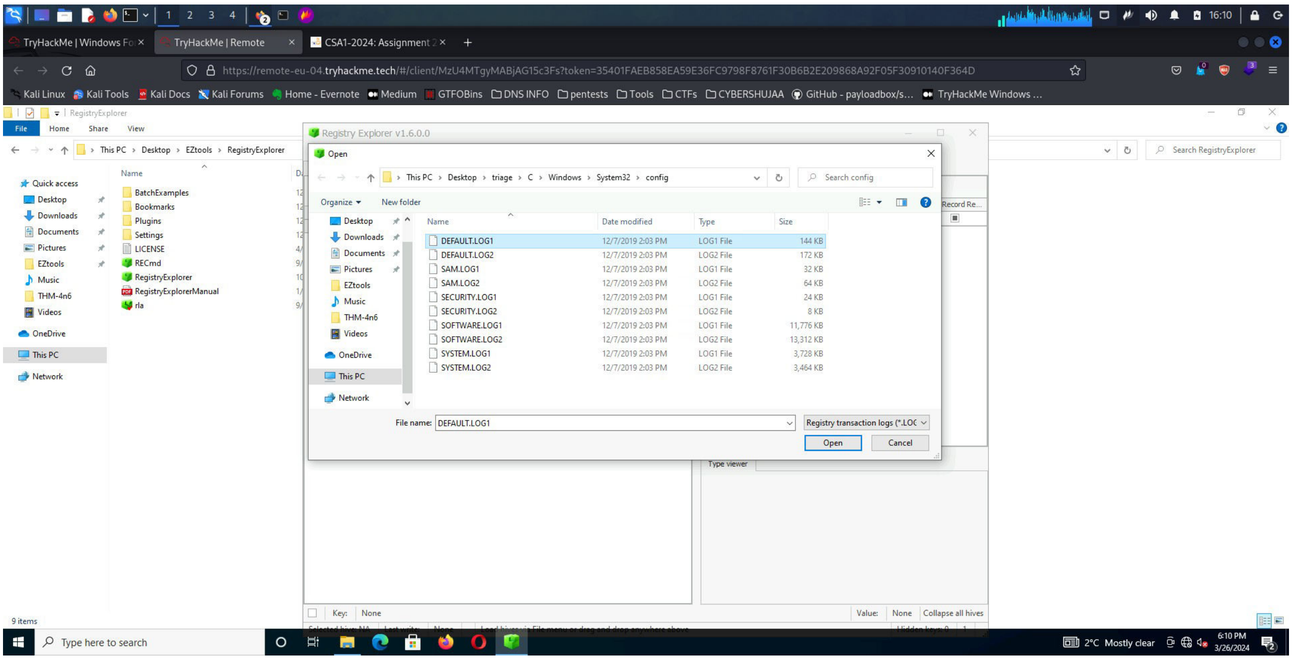
One of the Desktops in the research lab at Organization X is suspected to have been accessed by someone unauthorized. Although they generally have only one user account per Desktop, there were multiple user accounts observed on this system. It is also suspected that the system was connected to some network drive, and a USB device was connected to the system. The triage data from the system was collected and placed on the attached VM. Can you help Organization X with finding answers to the below questions?

## Answer the questions below

First was to open Registry Explore and load hive



Loading hives.


Registry Explorer v1.6.0.0
Open
This PC › Desktop › triage › C › Windows › System32 › config
Search config
Organize ▾
New folder
Open
Cancel
Registry transaction logs (*.LOG

| Name | Date modified | Type | Size |
|---|---|---|---|
| DEFAULT.LOG1 | 12/7/2019 2:03 PM | LOG1 File | 144 KB |
| DEFAULT.LOG2 | 12/7/2019 2:03 PM | LOG2 File | 172 KB |
| SAM.LOG1 | 12/7/2019 2:03 PM | LOG1 File | 32 KB |
| SAM.LOG2 | 12/7/2019 2:03 PM | LOG2 File | 64 KB |
| SECURITY.LOG1 | 12/7/2019 2:03 PM | LOG1 File | 24 KB |
| SECURITY.LOG2 | 12/7/2019 2:03 PM | LOG2 File | 8 KB |
| SOFTWARE.LOG1 | 12/7/2019 2:03 PM | LOG1 File | 11,776 KB |
| SOFTWARE.LOG2 | 12/7/2019 2:03 PM | LOG2 File | 13,312 KB |
| SYSTEM.LOG1 | 12/7/2019 2:03 PM | LOG1 File | 3,728 KB |
| SYSTEM.LOG2 | 12/7/2019 2:03 PM | LOG2 File | 3,464 KB |

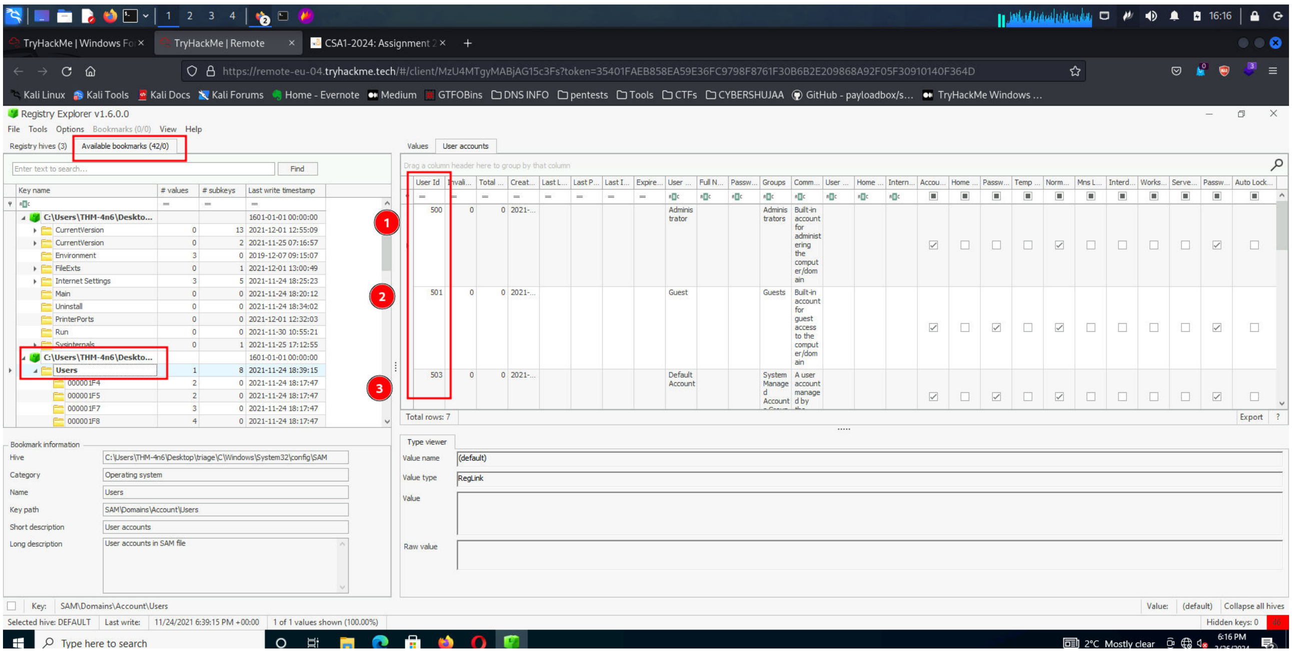
File name: DEFAULT.LOG1

How many user created accounts are present on the system?

**Ans: 3**

Once I was done with loading hives, on the top left, I clicked on “Available bookmarks” and then clicked on “Users” which should display the list of users associated on this computer.

There are 3 User ID meaning there are 3 users.



Registry Explorer v1.6.0.0

Registry hives (3) | Available bookmarks (42/0)

| Key name | # values | # subkeys | Last write timestamp |
|---|---|---|---|
| C:\Users\THM-4n6\Deskto... | | | 1601-01-01 00:00:00 |
| CurrentVersion | 0 | 13 | 2021-12-01 12:55:09 |
| CurrentVersion | 0 | 2 | 2021-11-25 07:16:57 |
| Environment | 3 | 0 | 2019-12-07 09:15:07 |
| FileExts | 0 | 1 | 2021-12-01 13:00:49 |
| Internet Settings | 3 | 5 | 2021-11-24 18:25:23 |
| Main | 0 | 0 | 2021-11-24 18:20:12 |
| Uninstall | 0 | 0 | 2021-11-24 18:34:02 |
| PrinterPorts | 0 | 0 | 2021-12-01 12:32:03 |
| Run | 0 | 0 | 2021-11-30 10:55:21 |
| Sysinternals | 0 | 1 | 2021-11-25 17:12:55 |
| C:\Users\THM-4n6\Deskto... | | | 1601-01-01 00:00:00 |
| Users | 1 | 8 | 2021-11-24 18:39:15 |
| 000001F4 | 2 | 0 | 2021-11-24 18:17:47 |
| 000001F5 | 2 | 0 | 2021-11-24 18:17:47 |
| 000001F7 | 3 | 0 | 2021-11-24 18:17:47 |
| 000001F8 | 4 | 0 | 2021-11-24 18:17:47 |

Bookmark information

Hive: C:\Users\THM-4n6\Desktop\triage\C\Windows\System32\config\SAM
Category: Operating system
Name: Users
Key path: SAM\Domains\Account\Users
Short description: User accounts
Long description: User accounts in SAM file

Values | User accounts

| User Id | Invali... | Total ... | Creat... | Last L... | Last P... | Last I... | Expire... | User ... | Full N... | Passw... | Groups | Comm... | User ... | Home ... | Intern... | Accou... | Home ... | Passw... | Temp ... | Norm... | Mns L... | Interd... | Works... | Serve... | Passw... | Auto Lock... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 500 | 0 | 0 | 2021-... | | | | | Administrator | | | Administrators | Built-in account for administering the computer/domain | | | | ☑ | □ | □ | □ | ☑ | □ | □ | □ | □ | ☑ | □ |
| 501 | 0 | 0 | 2021-... | | | | | Guest | | | Guests | Built-in account for guest access to the computer/domain | | | | ☑ | □ | ☑ | □ | ☑ | □ | □ | □ | □ | ☑ | □ |
| 503 | 0 | 0 | 2021-... | | | | | Default Account | | | System Managed Account | A user account managed by | | | | ☑ | □ | ☑ | □ | ☑ | □ | □ | □ | □ | ☑ | □ |

Total rows: 7

1

2

3

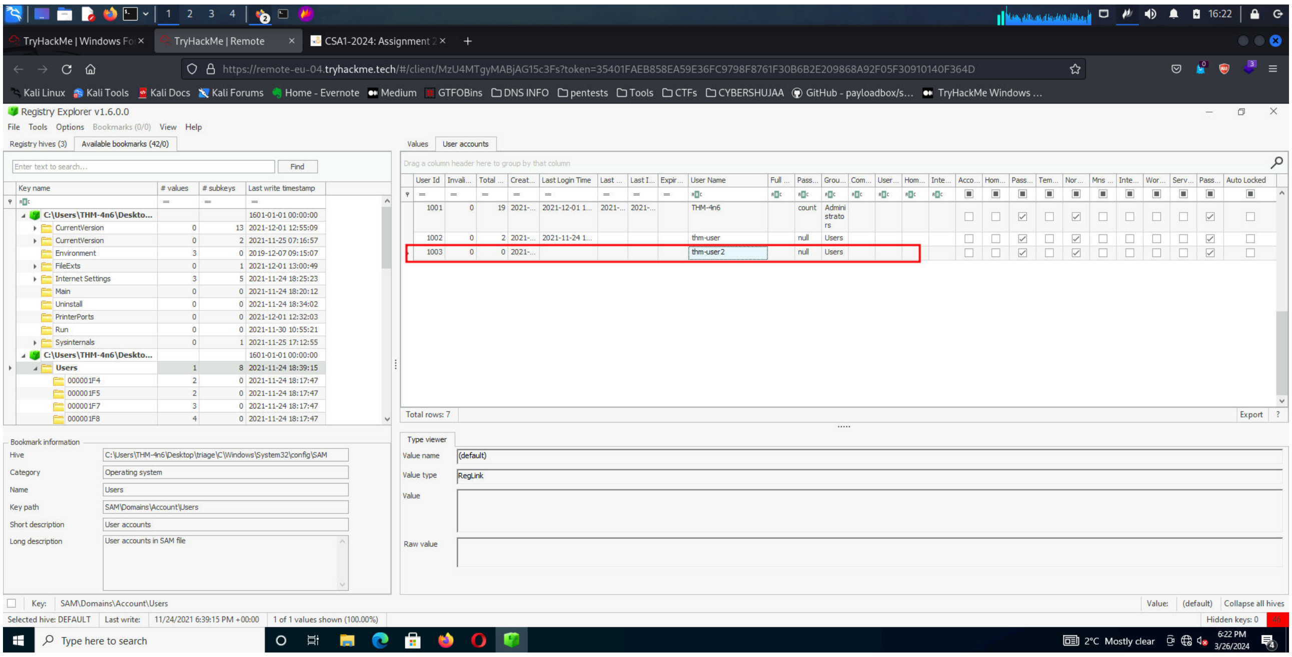
Type viewer
Value name: (default)
Value type: RegLink

Key: SAM\Domains\Account\Users
Selected hive: DEFAULT Last write: 11/24/2021 6:39:15 PM +00:00 1 of 1 values shown (100.00%)

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

Ans: THM-user2

This user was created but has no record of login.



Registry Explorer v1.6.0.0

Values | User accounts

| User Id | Invali... | Total ... | Creat... | Last Login Time | Last ... | Last I... | Expir... | User Name | Full ... | Pass... | Grou... | Com... | User... | Hom... | Inte... | Acco... | Hom... | Pass... | Tem... | Nor... | Mns ... | Inte... | Wor... | Serv... | Pass... | Auto Locked |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1001 | 0 | 19 | 2021-... | 2021-12-01 1... | 2021-... | 2021-... | | THM-4n6 | | count | Administrators | | | | | □ | □ | ☑ | □ | ☑ | □ | □ | □ | □ | ☑ | □ |
| 1002 | 0 | 2 | 2021-... | 2021-11-24 1... | | | | thm-user | | null | Users | | | | | □ | □ | ☑ | □ | ☑ | □ | □ | □ | □ | ☑ | □ |
| 1003 | 0 | 0 | 2021-... | | | | | thm-user2 | | null | Users | | | | | □ | □ | ☑ | □ | ☑ | □ | □ | □ | □ | ☑ | □ |

Total rows: 7

Bookmark information

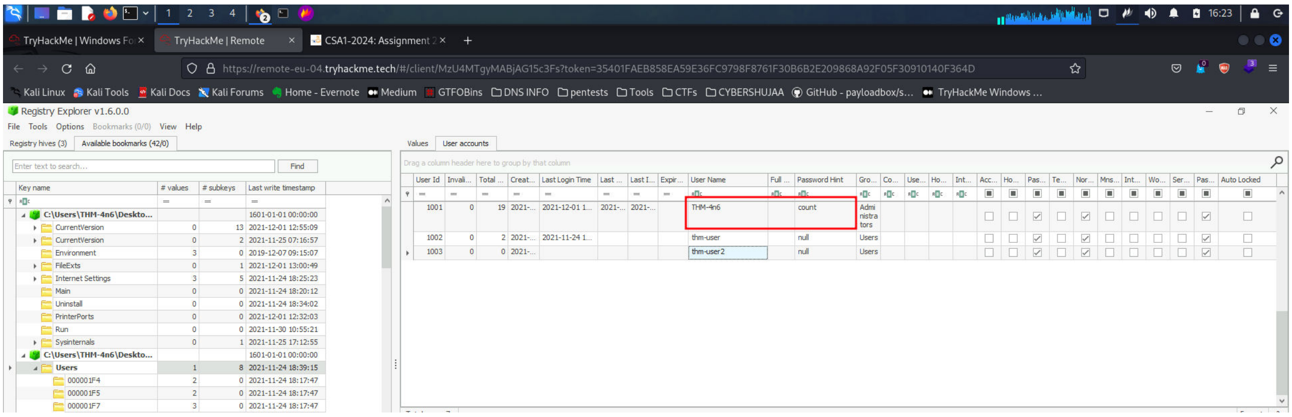
Hive: C:\Users\THM-4n6\Desktop\triage\C\Windows\System32\config\SAM
Category: Operating system
Name: Users
Key path: SAM\Domains\Account\Users
Short description: User accounts
Long description: User accounts in SAM file

Type viewer
Value name: (default)
Value type: RegLink

Key: SAM\Domains\Account\Users
Selected hive: DEFAULT Last write: 11/24/2021 6:39:15 PM +00:00 1 of 1 values shown (100.00%)

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

Ans: count



Registry Explorer v1.6.0.0

Registry hives (3) | Available bookmarks (42/0)

| Key name | # values | # subkeys | Last write timestamp |
|---|---|---|---|
| C:\Users\THM-4n6\Deskto... | | | 1601-01-01 00:00:00 |
| CurrentVersion | 0 | 13 | 2021-12-01 12:55:09 |
| CurrentVersion | 0 | 2 | 2021-11-25 07:16:57 |
| Environment | 3 | 0 | 2019-12-07 09:15:07 |
| FileExts | 0 | 1 | 2021-12-01 13:00:49 |
| Internet Settings | 3 | 5 | 2021-11-24 18:25:23 |
| Main | 0 | 0 | 2021-11-24 18:20:12 |
| Uninstall | 0 | 0 | 2021-11-24 18:34:02 |
| PrinterPorts | 0 | 0 | 2021-12-01 12:32:03 |
| Run | 0 | 0 | 2021-11-30 10:55:21 |
| Sysinternals | 0 | 1 | 2021-11-25 17:12:55 |
| C:\Users\THM-4n6\Deskto... | | | 1601-01-01 00:00:00 |
| Users | 1 | 8 | 2021-11-24 18:39:15 |
| 000001F4 | 2 | 0 | 2021-11-24 18:17:47 |
| 000001F5 | 2 | 0 | 2021-11-24 18:17:47 |
| 000001F7 | 3 | 0 | 2021-11-24 18:17:47 |

Values | User accounts

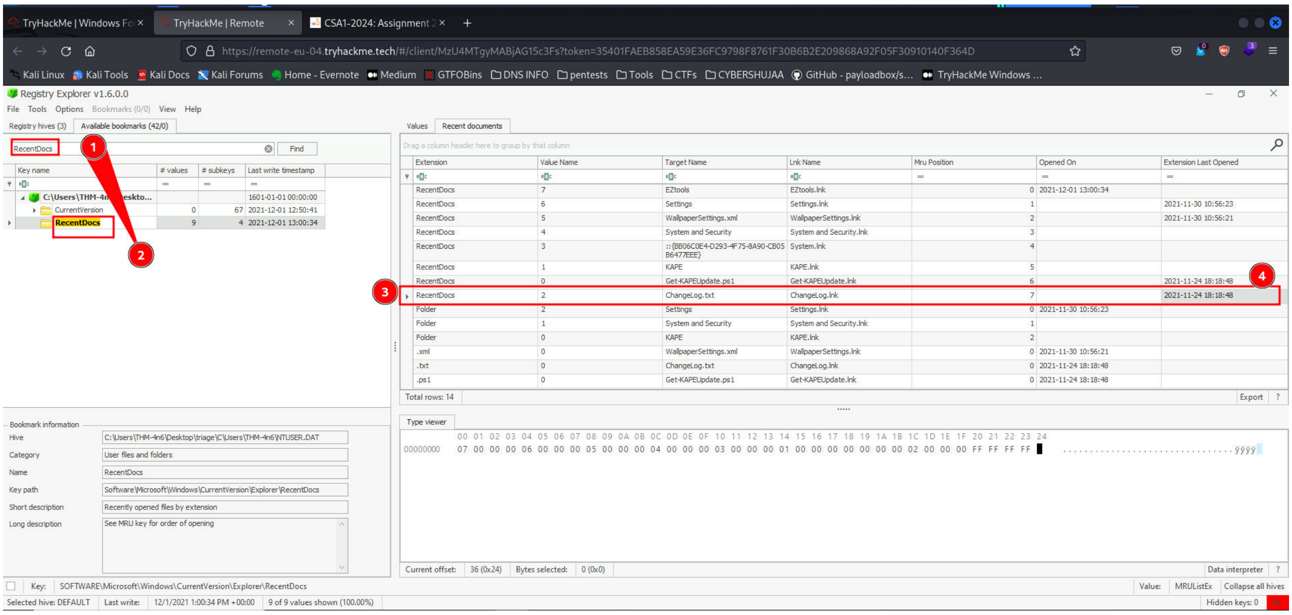
| User Id | Invali... | Total ... | Creat... | Last Login Time | Last ... | Last I... | Expir... | User Name | Full ... | Password Hint | Gro... | Co... | Use... | Ho... | Int... | Acc... | Ho... | Pas... | Te... | Nor... | Mns... | Int... | Wo... | Ser... | Pas... | Auto Locked |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1001 | 0 | 19 | 2021-... | 2021-12-01 1... | 2021-... | 2021-... | | THM-4n6 | | count | Administrators | | | | | □ | □ | ☑ | □ | ☑ | □ | □ | □ | □ | ☑ | □ |
| 1002 | 0 | 2 | 2021-... | 2021-11-24 1... | | | | thm-user | | null | Users | | | | | □ | □ | ☑ | □ | ☑ | □ | □ | □ | □ | ☑ | □ |
| 1003 | 0 | 0 | 2021-... | | | | | thm-user2 | | null | Users | | | | | □ | □ | ☑ | □ | ☑ | □ | □ | □ | □ | ☑ | □ |

When was the file 'Changelog.txt' accessed?

**Ans: 2021-11-24 18:18:48**

First was to search on the find bar for Recent Docs, for easier navigation.

Once I had a hint I clicked on the folder to view more information.



Registry Explorer v1.6.0.0

Search: RecentDocs

| Key name | # values | # subkeys | Last write timestamp |
|---|---|---|---|
| C:\Users\THM-4n6\Deskto... | | | 1601-01-01 00:00:00 |
| CurrentVersion | 0 | 67 | 2021-12-01 12:50:41 |
| RecentDocs | 9 | 4 | 2021-12-01 13:00:34 |

Values | Recent documents

| Extension | Value Name | Target Name | Lnk Name | Mru Position | Opened On | Extension Last Opened |
|---|---|---|---|---|---|---|
| RecentDocs | 7 | EZtools | EZtools.lnk | 0 | 2021-12-01 13:00:34 | |
| 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 | ::{BB06C0E4-D293-4F75-8A90-CB05B6477EEE} | 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

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 1A 1B 1C 1D 1E 1F 20 21 22 23 24
00000000  07 00 00 00 06 00 00 00 05 00 00 00 04 00 00 00 03 00 00 00 01 00 00 00 00 00 00 00 02 00 00 00 FF FF FF FF      ................................ÿÿÿÿ
```

Current offset: 36 (0x24) | Bytes selected: 0 (0x0)

Bookmark information

Hive: C:\Users\THM-4n6\Desktop\triage\C\Users\THM-4n6\NTUSER.DAT

Category: User files and folders

Name: RecentDocs

Key path: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Short description: Recently opened files by extension

Long description: See MRU key for order of opening

Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Selected hive: DEFAULT | Last write: 12/1/2021 1:00:34 PM +00:00 | 9 of 9 values shown (100.00%)

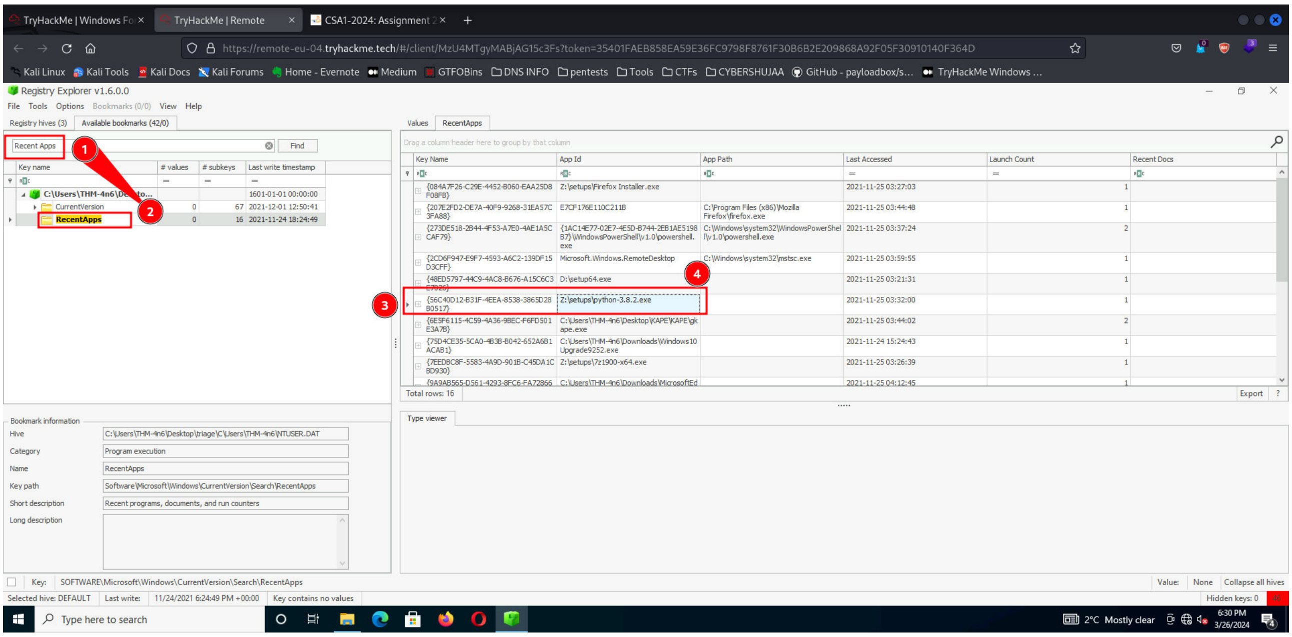
Value: MRUListEx

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

**Ans: Z:\setups\python-3.8.2.exe**

To also find the complete path, first was to search on the find bar for Recent Apps, for easier navigation.

Once I had a hint on the folder I clicked on it to view more information.



1
2
3
4
Registry Explorer v1.6.0.0
File Tools Options Bookmarks (0/0) View Help
Registry hives (3) Available bookmarks (42/0)
Recent Apps
Find
Values RecentApps
Drag a column header here to group by that column
Type viewer
Export

| Key name | # values | # subkeys | Last write timestamp |
|---|---|---|---|
| C:\Users\THM-4n6\Deskto... | | | 1601-01-01 00:00:00 |
| CurrentVersion | 0 | 67 | 2021-12-01 12:50:41 |
| RecentApps | 0 | 16 | 2021-11-24 18:24:49 |

| Key Name | App Id | App Path | Last Accessed | Launch Count | Recent Docs |
|---|---|---|---|---|---|
| {084A7F26-C29E-4452-B060-EAA25D8F08FB} | Z:\setups\Firefox Installer.exe | | 2021-11-25 03:27:03 | 1 | |
| {207E2FD2-DE7A-40F9-9268-31EA57C3FA88} | E7CF176E110C211B | C:\Program Files (x86)\Mozilla Firefox\firefox.exe | 2021-11-25 03:44:48 | 1 | |
| {273DE518-2B44-4F53-A7E0-4AE1A5CCAF79} | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\WindowsPowerShell\v1.0\powershell.exe | C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe | 2021-11-25 03:37:24 | 2 | |
| {2CD6F947-E9F7-4593-A6C2-139DF15D3CFF} | Microsoft.Windows.RemoteDesktop | C:\Windows\system32\mstsc.exe | 2021-11-25 03:59:55 | 1 | |
| {48ED5797-44C9-4AC8-B676-A15C6C3E7026} | D:\setup64.exe | | 2021-11-25 03:21:31 | 1 | |
| {56C40D12-B31F-4EEA-8538-3865D28B0517} | Z:\setups\python-3.8.2.exe | | 2021-11-25 03:32:00 | 1 | |
| {6E5F6115-4C59-4A36-9BEC-F6FD501E3A7B} | C:\Users\THM-4n6\Desktop\KAPE\KAPE\gkape.exe | | 2021-11-25 03:44:02 | 2 | |
| {75D4CE35-5CA0-4B3B-B042-652A6B1ACAB1} | C:\Users\THM-4n6\Downloads\Windows10Upgrade9252.exe | | 2021-11-24 15:24:43 | 1 | |
| {7EEDBC8F-5583-4A9D-901B-C45DA1CBD930} | Z:\setups\7z1900-x64.exe | | 2021-11-25 03:26:39 | 1 | |
| {9A9AB565-D561-4293-8FC6-FA72866 | C:\Users\THM-4n6\Downloads\MicrosoftEd | | 2021-11-25 04:12:45 | 1 | |

Total rows: 16

Bookmark information

| | |
|---|---|
| Hive | C:\Users\THM-4n6\Desktop\triage\C\Users\THM-4n6\NTUSER.DAT |
| Category | Program execution |
| Name | RecentApps |
| Key path | Software\Microsoft\Windows\CurrentVersion\Search\RecentApps |
| Short description | Recent programs, documents, and run counters |
| Long description | |

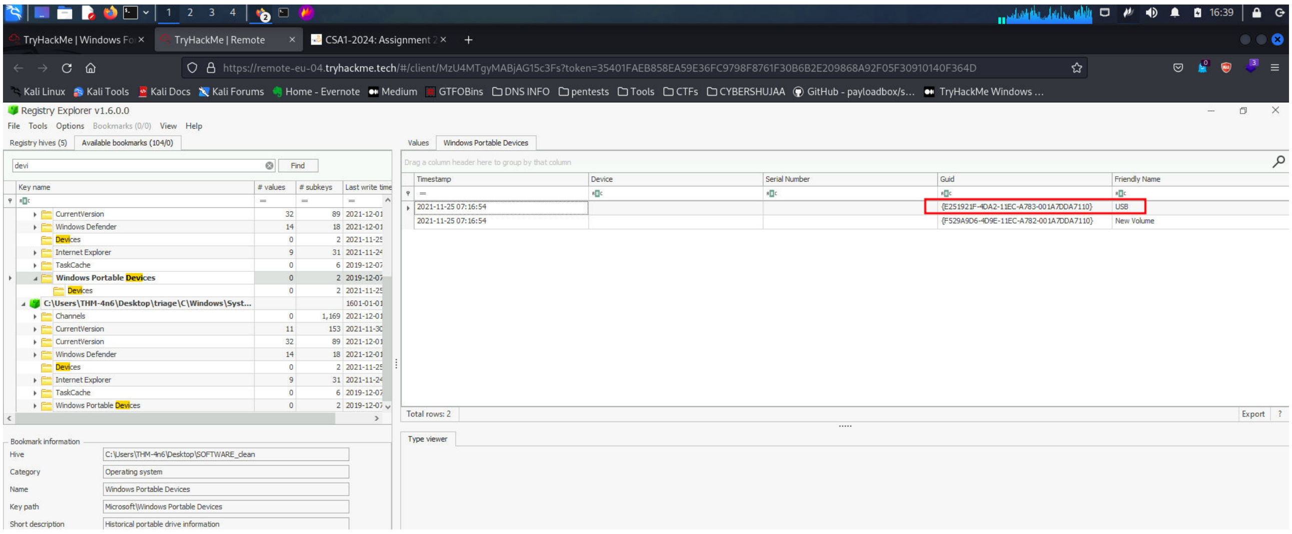
Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Search\RecentApps

Selected hive: DEFAULT | Last write: 11/24/2021 6:24:49 PM +00:00 | Key contains no values

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

**Ans: 2021-11-24 18:40:06**

First was to check the GUID for Friendly name USB so as to double check with the name of the device with this same ID as well.



Registry Explorer v1.6.0.0
File Tools Options Bookmarks (0/0) View Help
Registry hives (5) Available bookmarks (104/0)
devi
Find
Values Windows Portable Devices
Drag a column header here to group by that column
Type viewer
Export

| Key name | # values | # subkeys | Last write time |
|---|---|---|---|
| CurrentVersion | 32 | 89 | 2021-12-01 |
| Windows Defender | 14 | 18 | 2021-12-01 |
| Devices | 0 | 2 | 2021-11-25 |
| Internet Explorer | 9 | 31 | 2021-11-24 |
| TaskCache | 0 | 6 | 2019-12-07 |
| Windows Portable Devices | 0 | 2 | 2019-12-07 |
| Devices | 0 | 2 | 2021-11-25 |
| C:\Users\THM-4n6\Desktop\triage\C\Windows\Syst... | | | 1601-01-01 |
| Channels | 0 | 1,169 | 2021-12-01 |
| CurrentVersion | 11 | 153 | 2021-11-30 |
| CurrentVersion | 32 | 89 | 2021-12-01 |
| Windows Defender | 14 | 18 | 2021-12-01 |
| Devices | 0 | 2 | 2021-11-25 |
| Internet Explorer | 9 | 31 | 2021-11-24 |
| TaskCache | 0 | 6 | 2019-12-07 |
| Windows Portable Devices | 0 | 2 | 2019-12-07 |

| Timestamp | Device | Serial Number | Guid | Friendly Name |
|---|---|---|---|---|
| 2021-11-25 07:16:54 | | | {E251921F-4DA2-11EC-A783-001A7DDA7110} | USB |
| 2021-11-25 07:16:54 | | | {F529A9D6-4D9E-11EC-A782-001A7DDA7110} | New Volume |

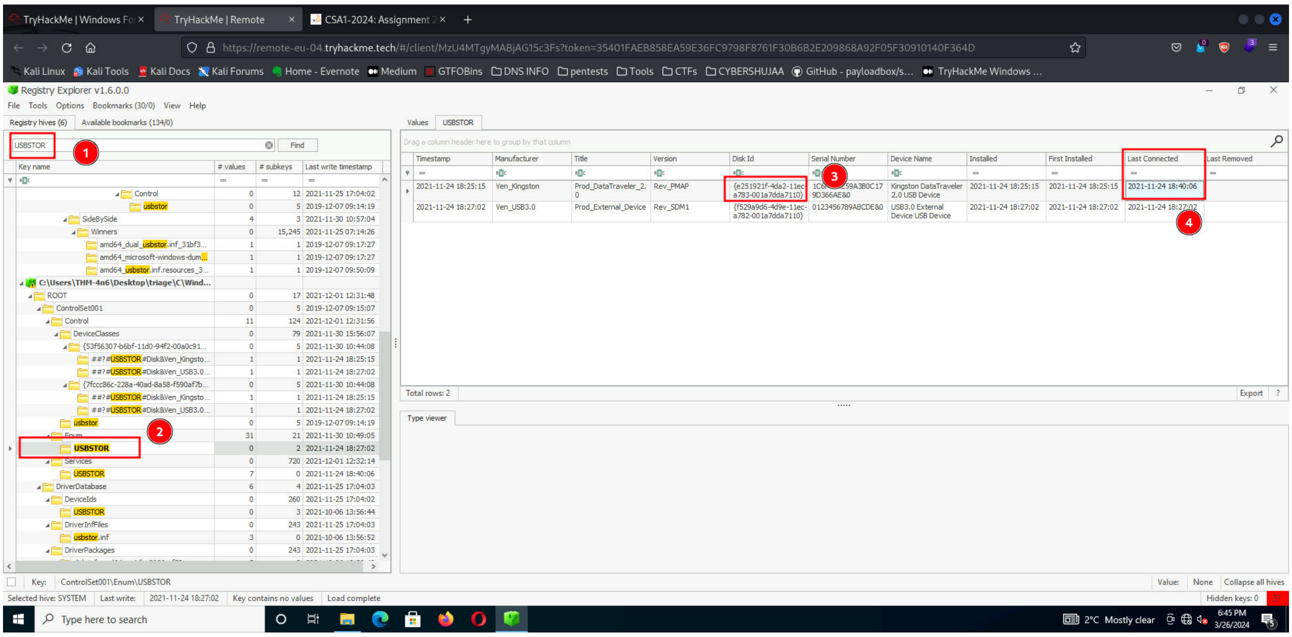
Total rows: 2

Bookmark information

| | |
|---|---|
| Hive | C:\Users\THM-4n6\Desktop\SOFTWARE_clean |
| Category | Operating system |
| Name | Windows Portable Devices |
| Key path | Microsoft\Windows Portable Devices |
| Short description | Historical portable drive information |

Double checking the Disk ID and checking Last Connection Time

To do this I searched for “USBSTOR” and looked at the right side to compare values.



USBSTOR

| Key name | # values | # subkeys | Last write timestamp |
|---|---|---|---|
| Control | 0 | 12 | 2021-11-25 17:04:02 |
| usbstor | 0 | 5 | 2019-12-07 09:14:19 |
| SideBySide | 4 | 3 | 2021-11-30 10:57:04 |
| Winners | 0 | 15,245 | 2021-11-25 07:14:26 |
| amd64_dual_usbstor.inf_31bf3... | 1 | 1 | 2019-12-07 09:17:27 |
| amd64_microsoft-windows-dum... | 1 | 1 | 2019-12-07 09:17:27 |
| amd64_usbstor.inf.resources_3... | 1 | 1 | 2019-12-07 09:50:09 |
| C:\Users\THM-4n6\Desktop\triage\C\Wind... | | | |
| ROOT | 0 | 17 | 2021-12-01 12:31:48 |
| ControlSet001 | 0 | 5 | 2019-12-07 09:15:07 |
| Control | 11 | 124 | 2021-12-01 12:31:56 |
| DeviceClasses | 0 | 79 | 2021-11-30 15:56:07 |
| {53f56307-b6bf-11d0-94f2-00a0c91... | 0 | 5 | 2021-11-30 10:44:08 |
| ##?#USBSTOR#Disk&Ven_Kingsto... | 1 | 1 | 2021-11-24 18:25:15 |
| ##?#USBSTOR#Disk&Ven_USB3.0... | 1 | 1 | 2021-11-24 18:27:02 |
| {7fccc86c-228a-40ad-8a58-f590af7b... | 0 | 5 | 2021-11-30 10:44:08 |
| ##?#USBSTOR#Disk&Ven_Kingsto... | 1 | 1 | 2021-11-24 18:25:15 |
| ##?#USBSTOR#Disk&Ven_USB3.0... | 1 | 1 | 2021-11-24 18:27:02 |
| usbstor | 0 | 5 | 2019-12-07 09:14:19 |
| Enum | 31 | 21 | 2021-11-30 10:49:05 |
| USBSTOR | 0 | 2 | 2021-11-24 18:27:02 |
| Services | 0 | 720 | 2021-12-01 12:32:14 |
| USBSTOR | 7 | 0 | 2021-11-24 18:40:06 |
| DriverDatabase | 6 | 4 | 2021-11-25 17:04:03 |
| DeviceIds | 0 | 260 | 2021-11-25 17:04:02 |
| USBSTOR | 0 | 3 | 2021-10-06 13:56:44 |
| DriverInfFiles | 0 | 243 | 2021-11-25 17:04:03 |
| usbstor.inf | 3 | 0 | 2021-10-06 13:56:52 |
| DriverPackages | 0 | 243 | 2021-11-25 17:04:03 |

Key: ControlSet001\Enum\USBSTOR

Selected hive: SYSTEM | Last write: 2021-11-24 18:27:02 | Key contains no values | Load complete

| Timestamp | Manufacturer | Title | Version | Disk Id | Serial Number | Device Name | Installed | First Installed | Last Connected | Last Removed |
|---|---|---|---|---|---|---|---|---|---|---|
| 2021-11-24 18:25:15 | Ven_Kingston | Prod_DataTraveler_2.0 | Rev_PMAP | {e251921f-4da2-11ec-a783-001a7dda7110} | 1C6[illegible]59A3B0C17 9D366AE&0 | Kingston DataTraveler 2.0 USB Device | 2021-11-24 18:25:15 | 2021-11-24 18:25:15 | 2021-11-24 18:40:06 | |
| 2021-11-24 18:27:02 | Ven_USB3.0 | Prod_External_Device | Rev_SDM1 | {f529a9d6-4d9e-11ec-a782-001a7dda7110} | 0123456789ABCDE&0 | USB3.0 External Device USB Device | 2021-11-24 18:27:02 | 2021-11-24 18:27:02 | 2021-11-24 18:27:02 | |

## conclusion:

In my conclusion, the Windows Forensics 1 room has been beneficial to me by providing insights about the fundamentals of digital forensics within a Windows environment. Through practical exercises and challenges, I have gained hands-on experience in analyzing disk images, examining system artifacts and identifying potential security incidents. This room has equipped me with essential skills in forensic analysis, empowering me to uncover valuable insights and evidence crucial for incident response and digital investigations. As a foundational resource, this room has served an excellent starting point in digital forensics.

**Thank You.**