Windows-Forensics-1

INTRODUCTION

Computer forensics is vital in cybersecurity, uncovering evidence from digital devices. A prime example is the BTK killer case, solved through data recovery from a floppy disk. With Windows dominating the desktop OS market, mastering forensic analysis on this platform is crucial.

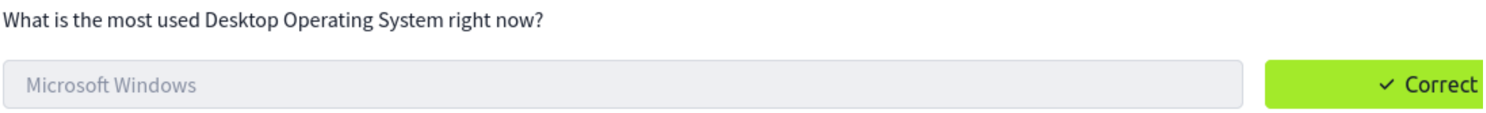
Forensic Artifacts

Forensic artifacts are digital traces of user activity. Like physical evidence at a crime scene, these artifacts tell a story. Windows creates numerous artifacts to enhance user experience, but they also provide critical evidence for investigators.

Is My Computer Spying on Me?

Windows tracks user activity, not to spy, but to improve personalization. However, this same data is invaluable for forensic analysis, helping investigators trace user actions and uncover evidence.

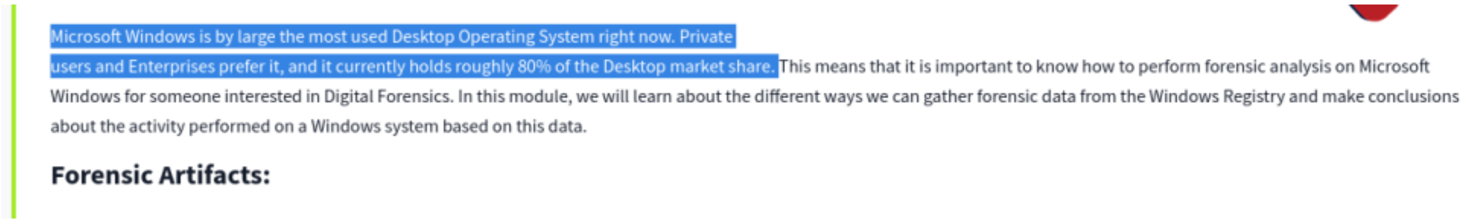
Let me walk you through on how I tackled each task.



What is the most used Desktop Operating System right now?

Microsoft Windows

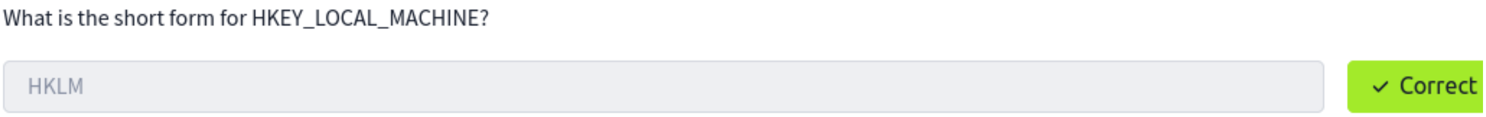
Microsoft Windows is by large the most used Desktop Operating System right now.
In this module, we will learn about the different ways we can gather forensic data from the Windows Registry and make conclusions about the activity performed on a Windows system based on this data.



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. In this module, we will learn about the different ways we can gather forensic data from the Windows Registry and make conclusions about the activity performed on a Windows system based on this data.

Forensic Artifacts:

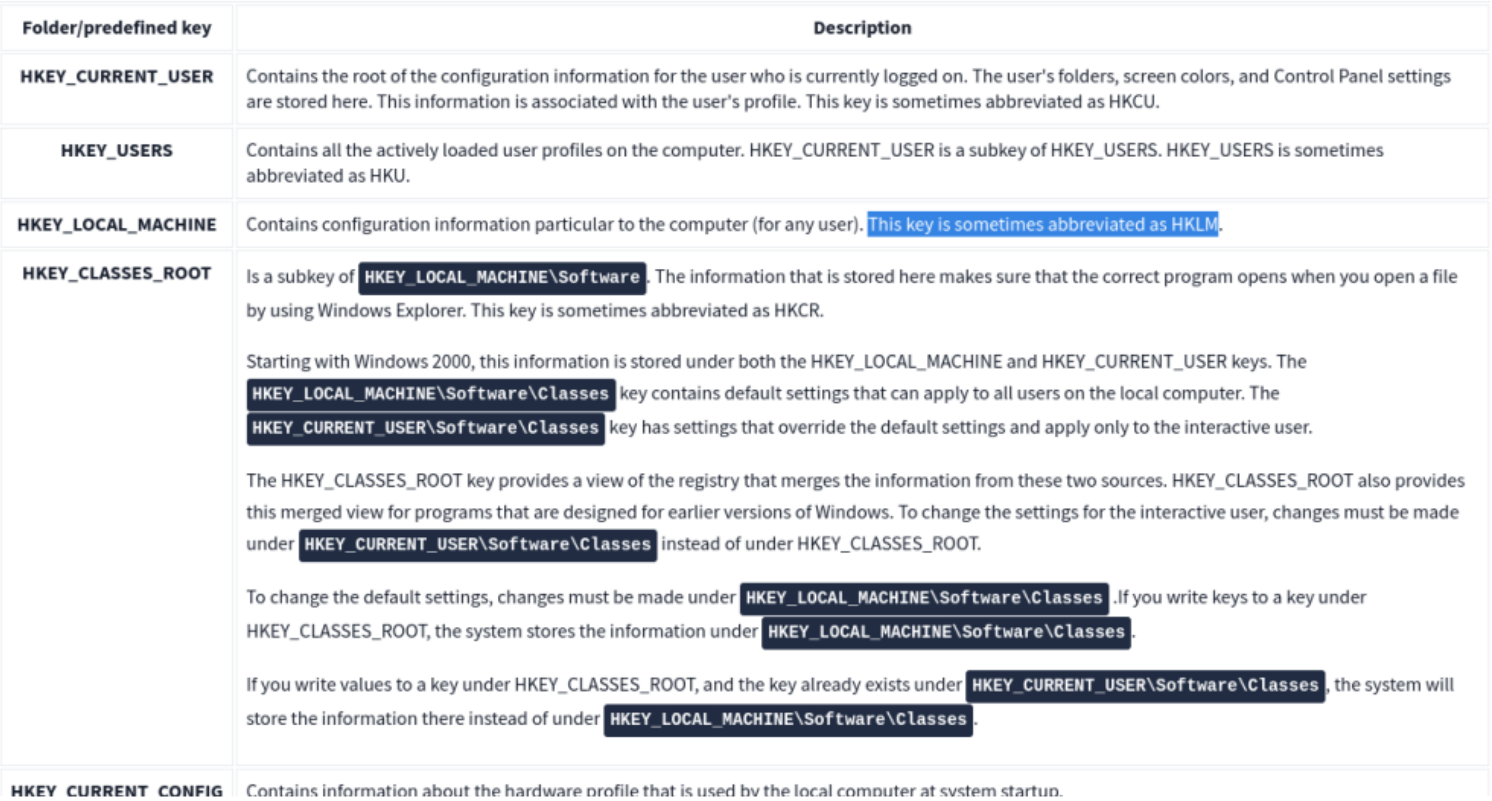
The registry on any Windows system contains the following five root keys:
1. HKEY_CURRENT_USER
2. HKEY_USERS
3. HKEY_LOCAL_MACHINE
4. HKEY_CLASSES_ROOT
5. HKEY_CURRENT_CONFIG



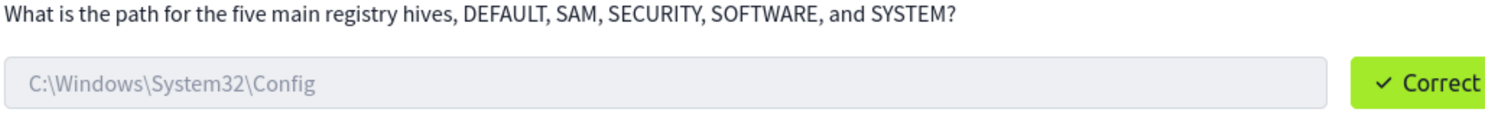
What is the short form for HKEY_LOCAL_MACHINE?

HKLM

This can be found in the reading. Also quite good information as to what the information in each of the five root keys hold. The image below is the sample section where I read this information.



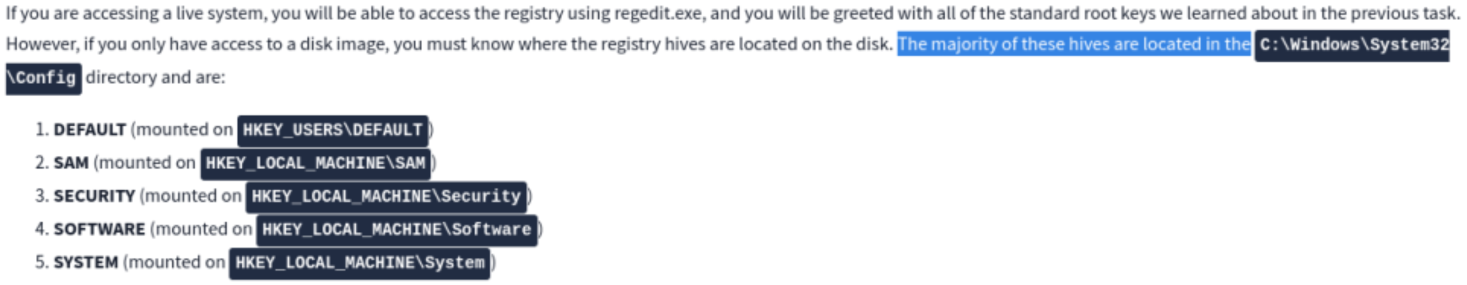
Folder/predefined key	Description
HKEY_CURRENT_USER	Contains the root of the configuration information for the user who is currently logged on. The user's folders, screen colors, and Control Panel settings are stored here. This information is associated with the user's profile. This key is sometimes abbreviated as HKCU.
HKEY_USERS	Contains all the actively loaded user profiles on the computer. HKEY_CURRENT_USER is a subkey of HKEY_USERS. HKEY_USERS is sometimes abbreviated as HKU.
HKEY_LOCAL_MACHINE	Contains configuration information particular to the computer (for any user). This key is sometimes abbreviated as HKLM.
HKEY_CLASSES_ROOT	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. This key is sometimes abbreviated as HKCR. 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.



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

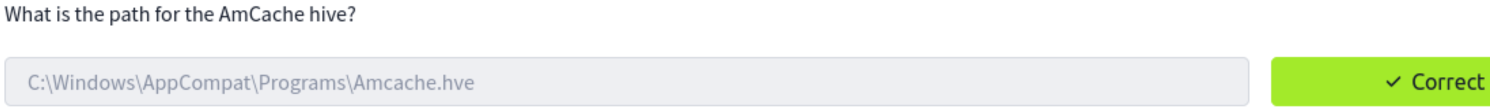
C:\Windows\System32\Config

C:\Windows\System32\Config is the path to the five main registry hives as shown from the information in the image below.



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 and are:

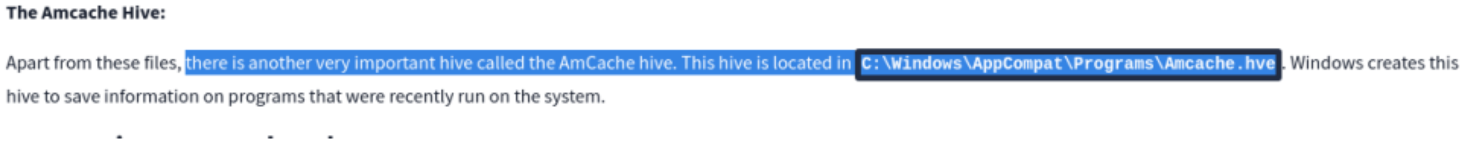
1. **DEFAULT** (mounted on `HKEY_USERS\DEFAULT`)
2. **SAM** (mounted on `HKEY_LOCAL_MACHINE\SAM`)
3. **SECURITY** (mounted on `HKEY_LOCAL_MACHINE\Security`)
4. **SOFTWARE** (mounted on `HKEY_LOCAL_MACHINE\Software`)
5. **SYSTEM** (mounted on `HKEY_LOCAL_MACHINE\System`)



What is the path for the AmCache hive?

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

Going through the reading, I came accross this information as it can be seen in the image below.



The Amcache Hive:

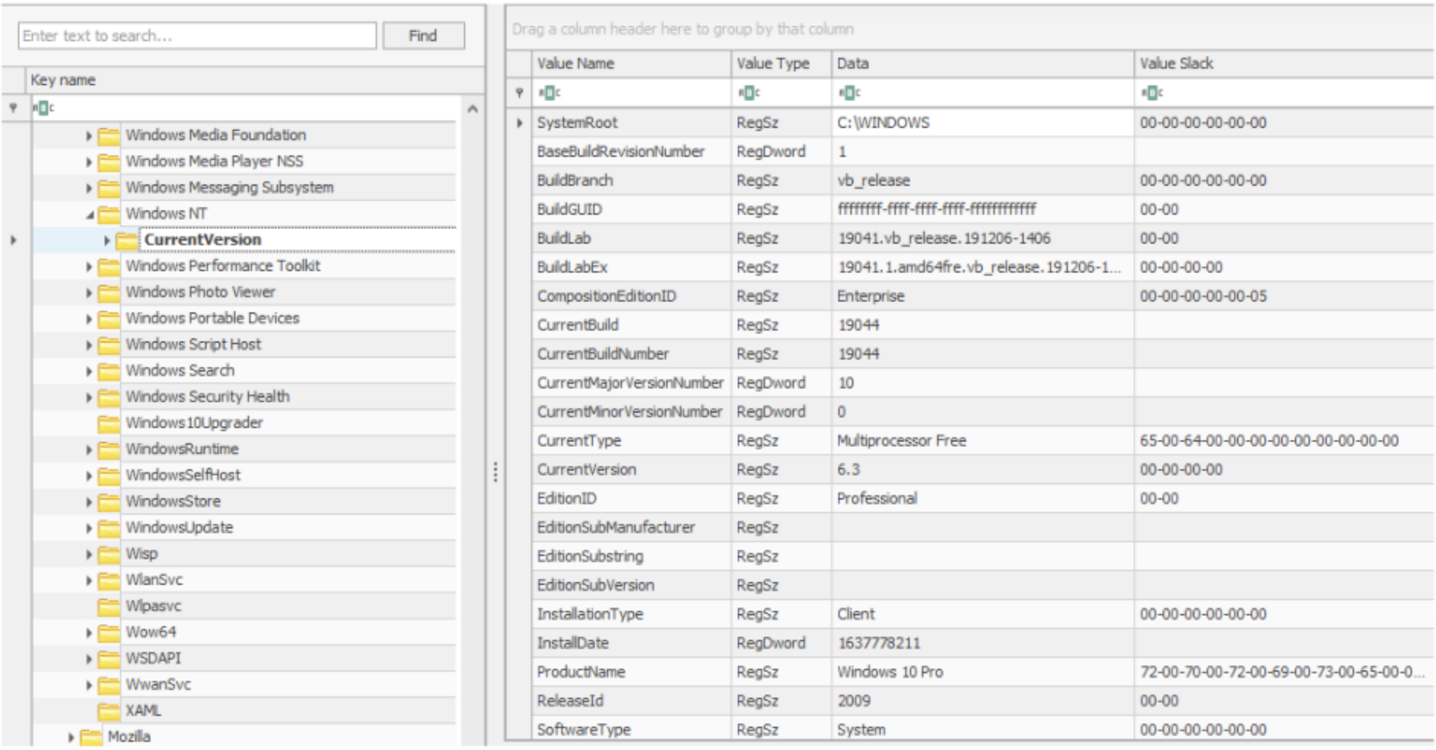
Apart from these files, there is another very important hive called the AmCache hive. This hive is located in `C:\Windows\AppCompat\Programs\Amcache.hve`. Windows creates this hive to save information on programs that were recently run on the system.

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

19044

✓ Correct

We will be using the screenshot provided in the reading. The OS Version section tells us to use the screenshot to answer question 1, as seen below.



Enter text to search... Find

Key name

- Windows Media Foundation
- Windows Media Player NSS
- Windows Messaging Subsystem
- Windows NT
  - **CurrentVersion**
- Windows Performance Toolkit
- Windows Photo Viewer
- Windows Portable Devices
- Windows Script Host
- Windows Search
- Windows Security Health
- Windows10Upgrader
- WindowsRuntime
- WindowsSelfHost
- WindowsStore
- WindowsUpdate
- Wisp
- WlanSvc
- Wlpasvc
- Wow64
- WSDAPI
- WwanSvc
- XAML
- Mozilla

Drag a column header here to group by that column

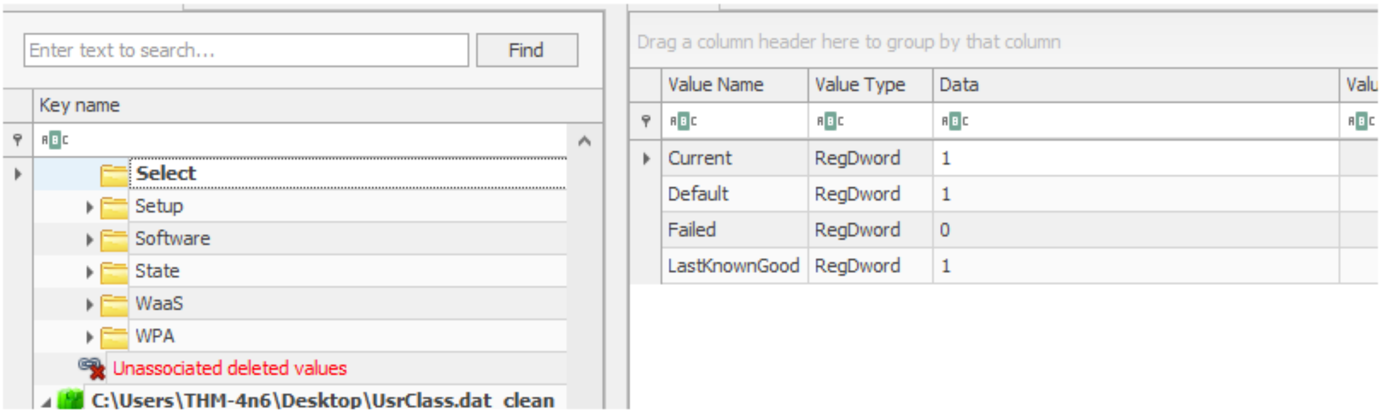
Value Name	Value Type	Data	Value Slack
SystemRoot	RegSz	C:\WINDOWS	00-00-00-00-00-00
BaseBuildRevisionNumber	RegDword	1	
BuildBranch	RegSz	vb_release	00-00-00-00-00-00
BuildGUID	RegSz	ffffffff-ffff-ffff-ffff-ffffffffffff	00-00
BuildLab	RegSz	19041.vb_release.191206-1406	00-00
BuildLabEx	RegSz	19041.1.amd64fre.vb_release.191206-1...	00-00-00-00
CompositionEditionID	RegSz	Enterprise	00-00-00-00-00-05
CurrentBuild	RegSz	19044	
CurrentBuildNumber	RegSz	19044	
CurrentMajorVersionNumber	RegDword	10	
CurrentMinorVersionNumber	RegDword	0	
CurrentType	RegSz	Multiprocessor Free	65-00-64-00-00-00-00-00-00-00-00-00
CurrentVersion	RegSz	6.3	00-00-00-00
EditionID	RegSz	Professional	00-00
EditionSubManufacturer	RegSz		
EditionSubstring	RegSz		
EditionSubVersion	RegSz		
InstallationType	RegSz	Client	00-00-00-00-00-00
InstallDate	RegDword	1637778211	
ProductName	RegSz	Windows 10 Pro	72-00-70-00-72-00-69-00-73-00-65-00-0...
ReleaseId	RegSz	2009	00-00
SoftwareType	RegSz	System	00-00-00-00-00-00

Which ControlSet contains the last known good configuration?

1

✓ Correct

The screenshot in Current Control Set section will contain the answer we need, the image below is the screenshot image from the task.



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

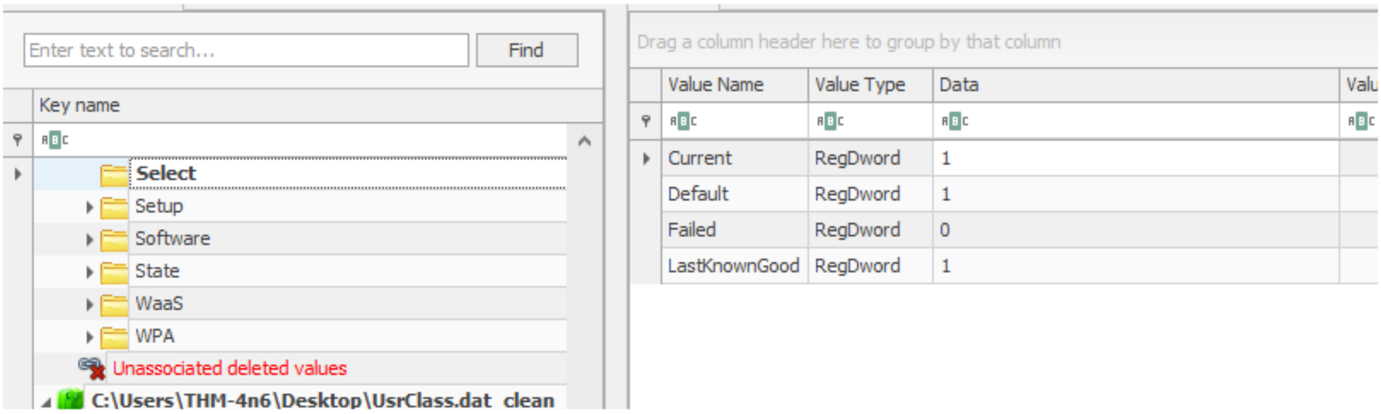
Value Name	Value Type	Data	Valu
Current	RegDword	1	
Default	RegDword	1	
Failed	RegDword	0	
LastKnownGood	RegDword	1	

What is the Computer Name of the computer?

THM-4n6

✓ Correct

The screenshot in Computer Name section will contain the answer we need.



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

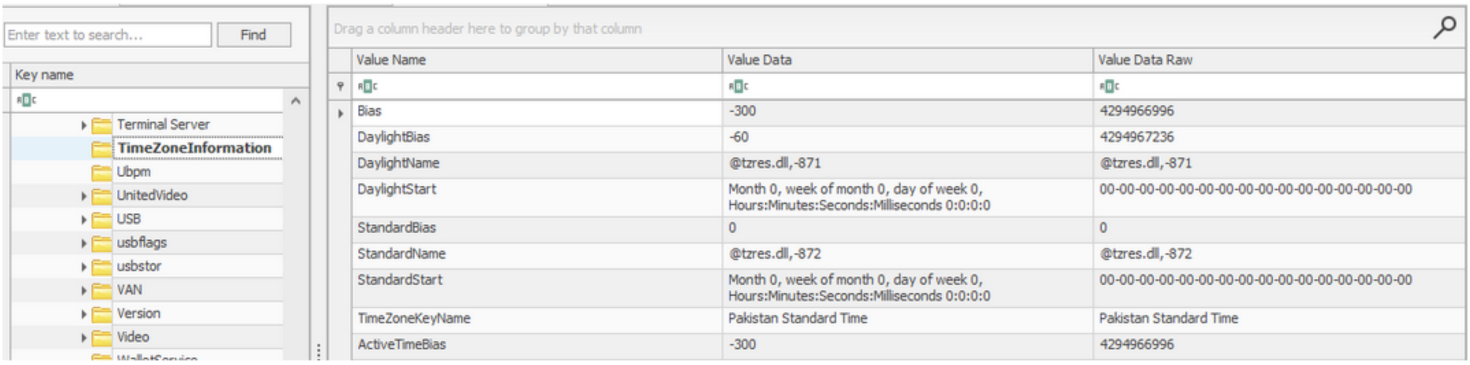
Value Name	Value Type	Data	Valu
Current	RegDword	1	
Default	RegDword	1	
Failed	RegDword	0	
LastKnownGood	RegDword	1	

What is the value of the TimeZoneKeyName?

Pakistan Standard Time

✓ Correct

The screenshot in Time Zone Information section will contain the answer we need.



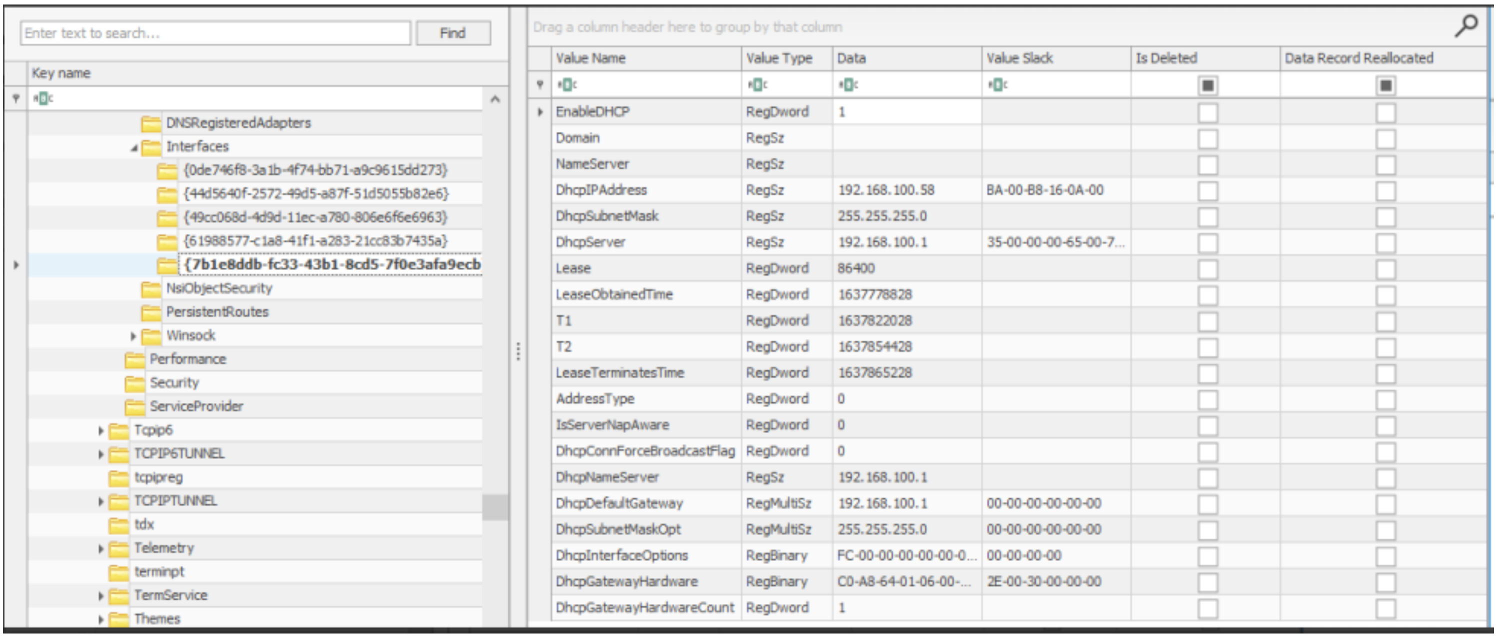
Value Name	Value Data	Value Data Raw
Bias	-300	4294966996
DaylightBias	-60	4294967236
DaylightName	@tzres.dll,-871	@tzres.dll,-871
DaylightStart	Month 0, week of month 0, day of week 0, Hours:Minutes:Seconds:Milliseconds 0:0:0:0	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
StandardBias	0	0
StandardName	@tzres.dll,-872	@tzres.dll,-872
StandardStart	Month 0, week of month 0, day of week 0, 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

192.168.100.58

✓ Correct

The screenshot in Network Interface and Past Networks will contain the answer we need. And this can be seen from the image below.


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

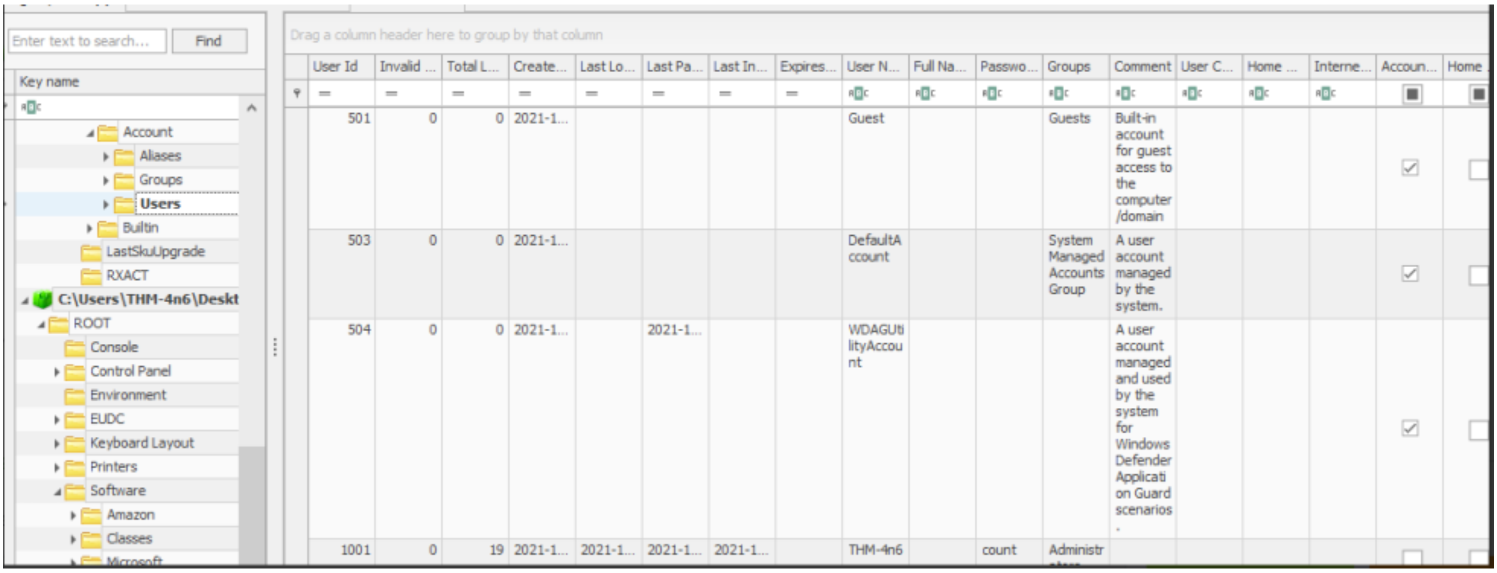
Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
EnableDHCP	RegDword	1		□	□
Domain	RegSz			□	□
NameServer	RegSz			□	□
DhcpIPAddress	RegSz	192.168.100.58	BA-00-B8-16-0A-00	□	□
DhcpSubnetMask	RegSz	255.255.255.0		□	□
DhcpServer	RegSz	192.168.100.1	35-00-00-00-65-00-7...	□	□
Lease	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?

501

✓ Correct

The screenshot in SAM Hive and User Information section just as seen below will contain the answer we need.



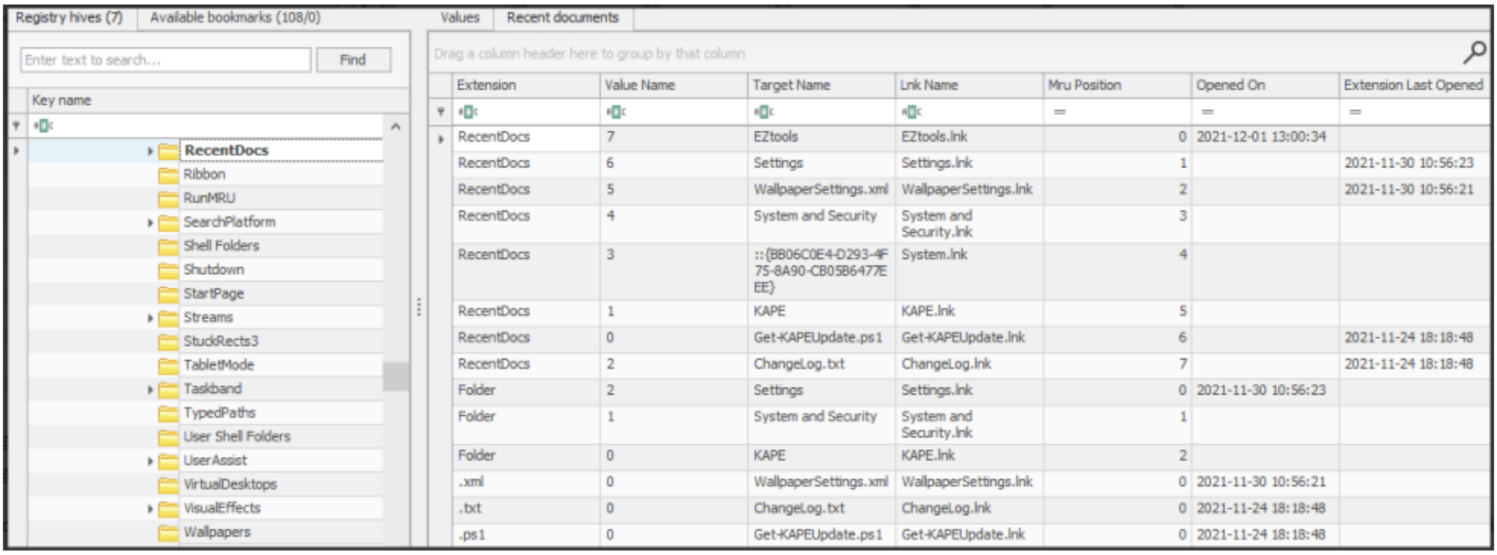
User Id	Invalid ...	Total L...	Create...	Last Lo...	Last Pa...	Last In...	Expires...	User N...	Full Na...	Passwo...	Groups	Comment	User C...	Home ...	Interne...	Accoun...	Home
501	0	0	2021-1...					Guest			Guests	Built-in account for guest access to the computer /domain				☑	□
503	0	0	2021-1...					DefaultAccount			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					□	□

When was EZtools opened?

2021-12-01 13:00:34

✓ Correct

Looking closely at the screenshot in Recent Files section, I found the answer to this question as shown in the image below.



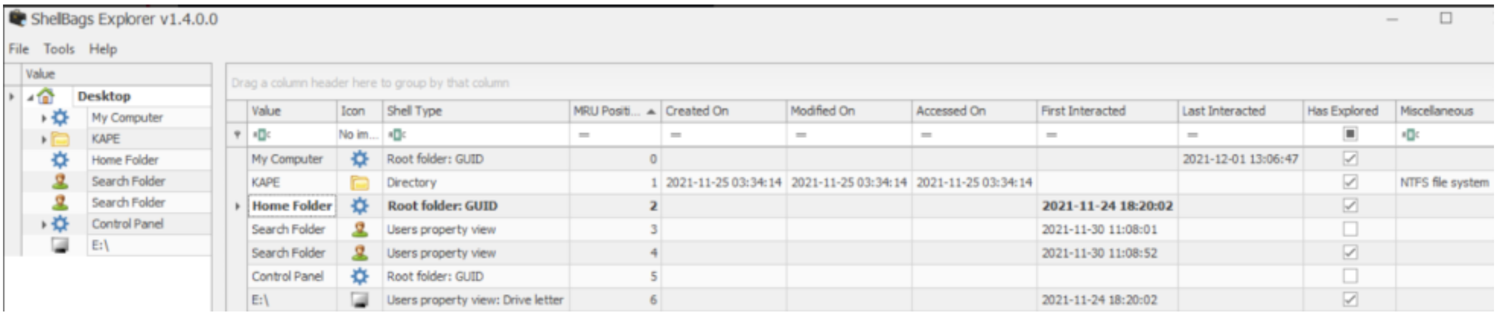
Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
RecentDocs	7	EZtools	EZtools.lnk	0	2021-12-01 13:00:34	
RecentDocs	6	Settings	Settings.lnk	1		2021-11-30 10:56:23
RecentDocs	5	WallpaperSettings.xml	WallpaperSettings.lnk	2		2021-11-30 10:56:21
RecentDocs	4	System 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	

At what time was My Computer last interacted with?

2021-12-01 13:06:47

✓ Correct

The screenshot in ShellBags section as shown below contained the response needed.



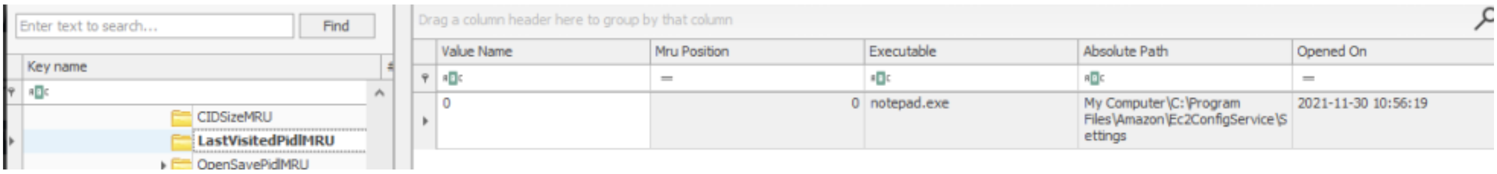
Value	Icon	Shell Type	MRU Positi...	Created On	Modified On	Accessed On	First Interacted	Last Interacted	Has Explored	Miscellaneous
My Computer	⚙	Root folder: GUID	0					2021-12-01 13:06:47	☑	
KAPE	📁	Directory	1	2021-11-25 03:34:14	2021-11-25 03:34:14	2021-11-25 03:34:14			☑	NTFS file system
Home Folder	⚙	**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?

C:\Program Files\Amazon\Ec2ConfigService\Settings

✓ Correct

The screenshot in Open/Save and LastVisited Dialog MRUs section will contain the answers needed just as shown from image below.



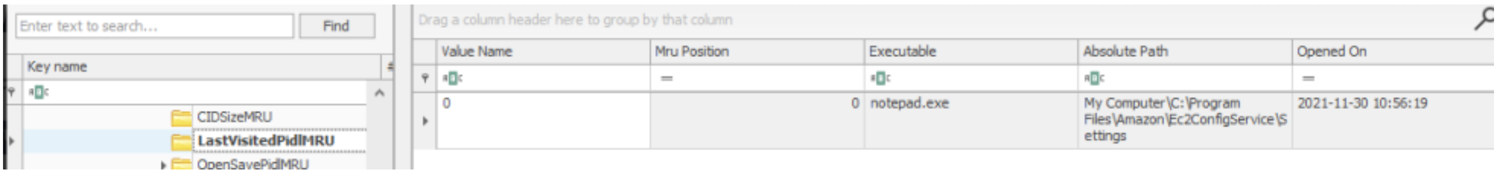
Value Name	Mru Position	Executable	Absolute Path	Opened On
0	0	notepad.exe	My Computer\C:\Program Files\Amazon\Ec2ConfigService\Settings	2021-11-30 10:56:19

When was this file opened?

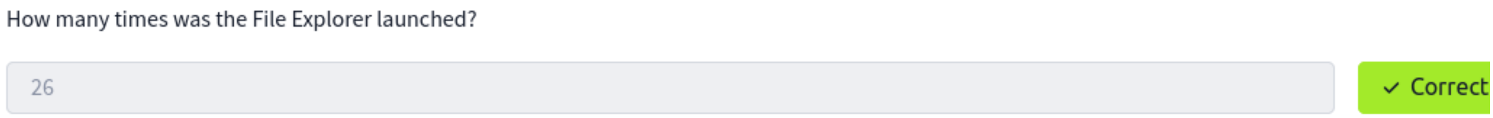
2021-11-30 10:56:19

✓ Correct

Checking on the “Open On” tab in the image below, I found the date.



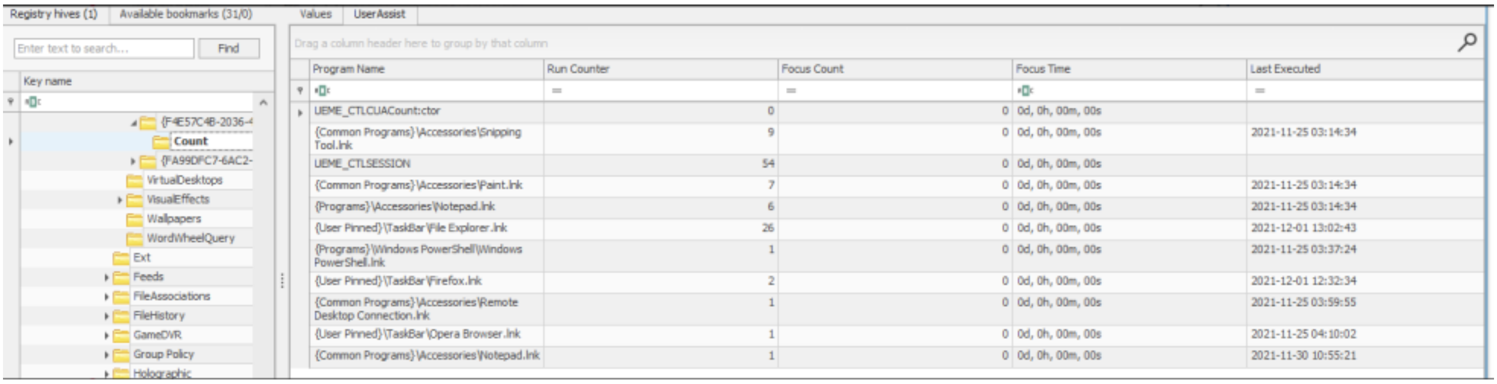
Value Name	Mru Position	Executable	Absolute Path	Opened On
0	0	notepad.exe	My Computer\C:\Program Files\Amazon\Ec2ConfigService\Settings	2021-11-30 10:56:19



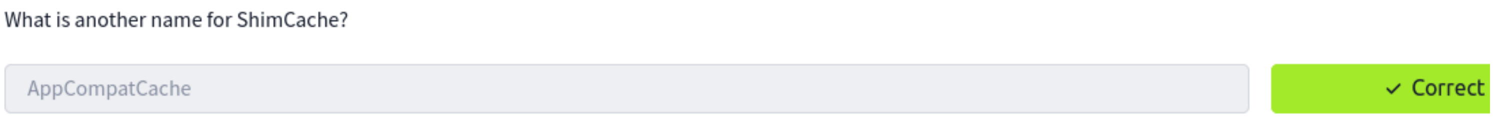
How many times was the File Explorer launched?

26

The screenshot in UserAssist section will contain the answer we need just as seen in the image below.



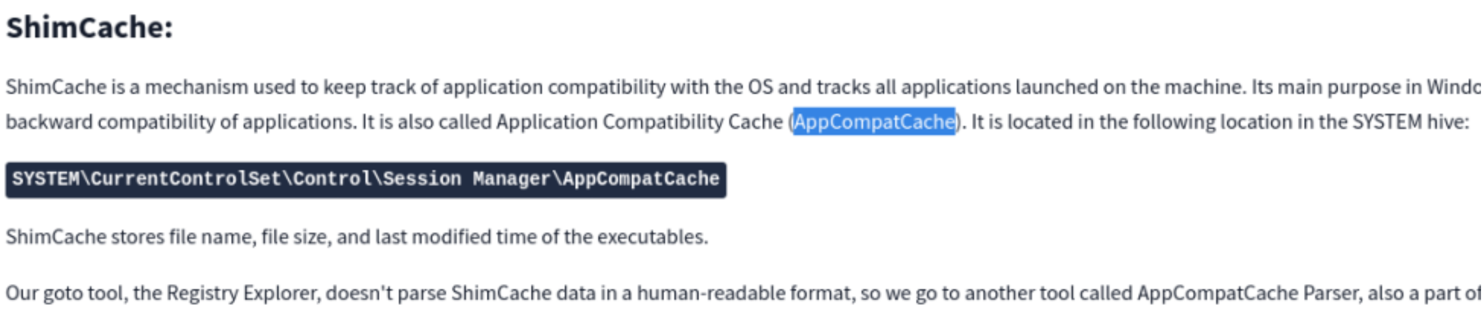
Program Name	Run Counter	Focus Count	Focus Time	Last Executed
UEME_CTLCUACount:ctor	0	0	0d, 0h, 00m, 00s	
{Common Programs}\Accessories\Snipping Tool.lnk	9	0	0d, 0h, 00m, 00s	2021-11-25 03:14:34
UEME_CTLSESSION	54	0	0d, 0h, 00m, 00s	
{Common Programs}\Accessories\Paint.lnk	7	0	0d, 0h, 00m, 00s	2021-11-25 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

The answer can be found in the reading-image below.



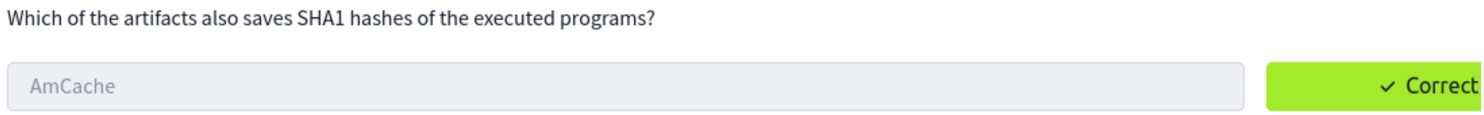
ShimCache:

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 Windo 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



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

AmCache

The image below, shows a section of the reading where I came across the answer to the above question.

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.hve
```

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

BAM/DAM

✓ Correct

The answer to this also can be found in the reading as shown below.

BAM/DAM:

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.

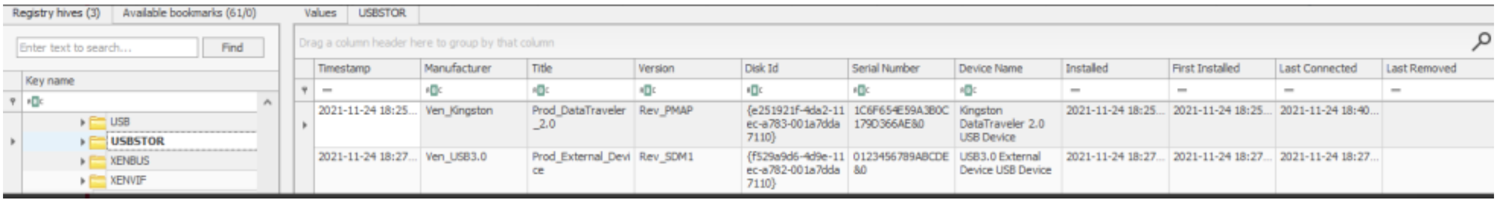
In the Windows registry, the following locations contain information related to BAM and DAM. This location contains information about last run programs, their full paths, and last execution time.

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

1C6f654E59A3B0C179D366AE&0

✓ Correct

The screenshot in Device Identification section will contain the answers needed for this question and the next just as shown from the images below.

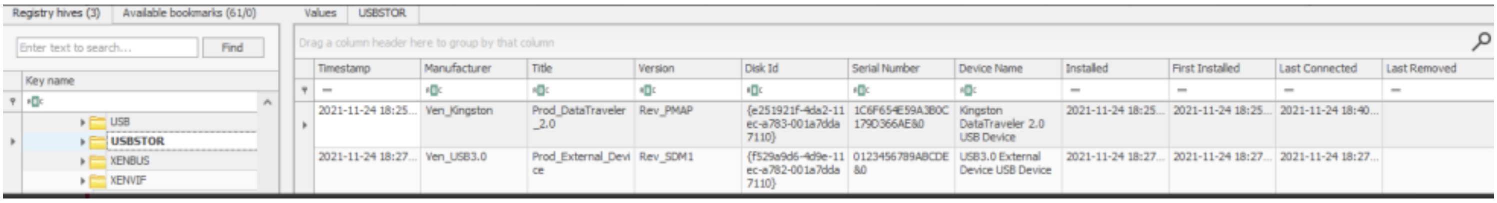


Timestamp	Manufacturer	Title	Version	Disk Id	Serial Number	Device Name	Installed	First Installed	Last Connected	Last Removed
2021-11-24 18:25...	Ven_Kingston	Prod_DataTraveler_2.0	Rev_PMAP	{e251921f-4da2-11ec-a783-001a7dda7110}	1C6F654E59A3B0C179D366AE&0	Kingston DataTraveler 2.0 USB Device	2021-11-24 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 Traveler 2.0 USB Device

✓ Correct


Registry hives (3)
Available bookmarks (61/0)
Values
USBSTOR
Enter text to search...
Find
Key name
USB
USBSTOR
XENBUS
XENVIF
Drag a column header here to group by that column

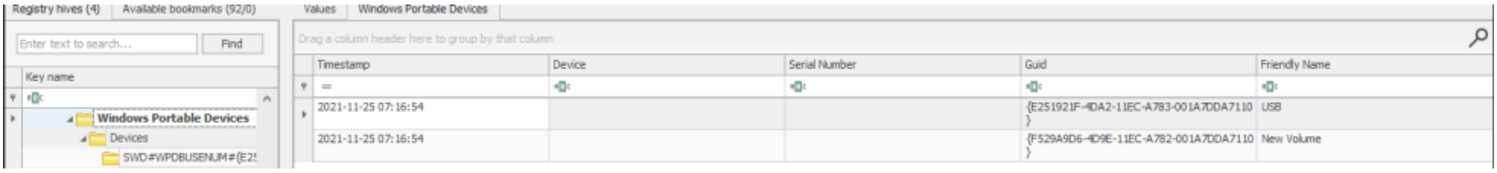
Timestamp	Manufacturer	Title	Version	Disk Id	Serial Number	Device Name	Installed	First Installed	Last Connected	Last Removed
2021-11-24 18:25...	Ven_Kingston	Prod_DataTraveler_2.0	Rev_PMAP	{e251921f-4da2-11ec-a783-001a7dda7110}	1C6F654E59A3B0C179D366AE&0	Kingston DataTraveler 2.0 USB Device	2021-11-24 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 friendly name of the device from the manufacturer 'Kingston'?

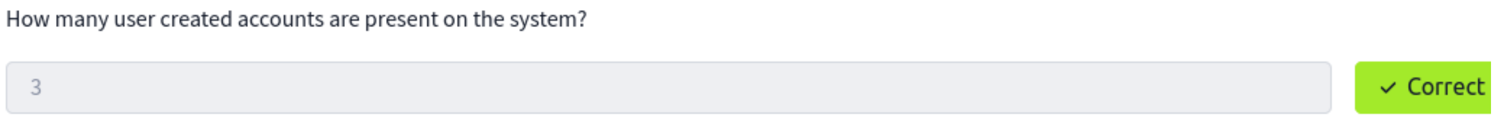
USB

✓ Correct

Combining the information from both the first screenshot and the third from the reading, I can see the Disk Id from the first screenshot and Guid from the third screenshot shows a match. So the device name is Kingston DataTraveler 2.0 USB Device and the friendly name is USB.



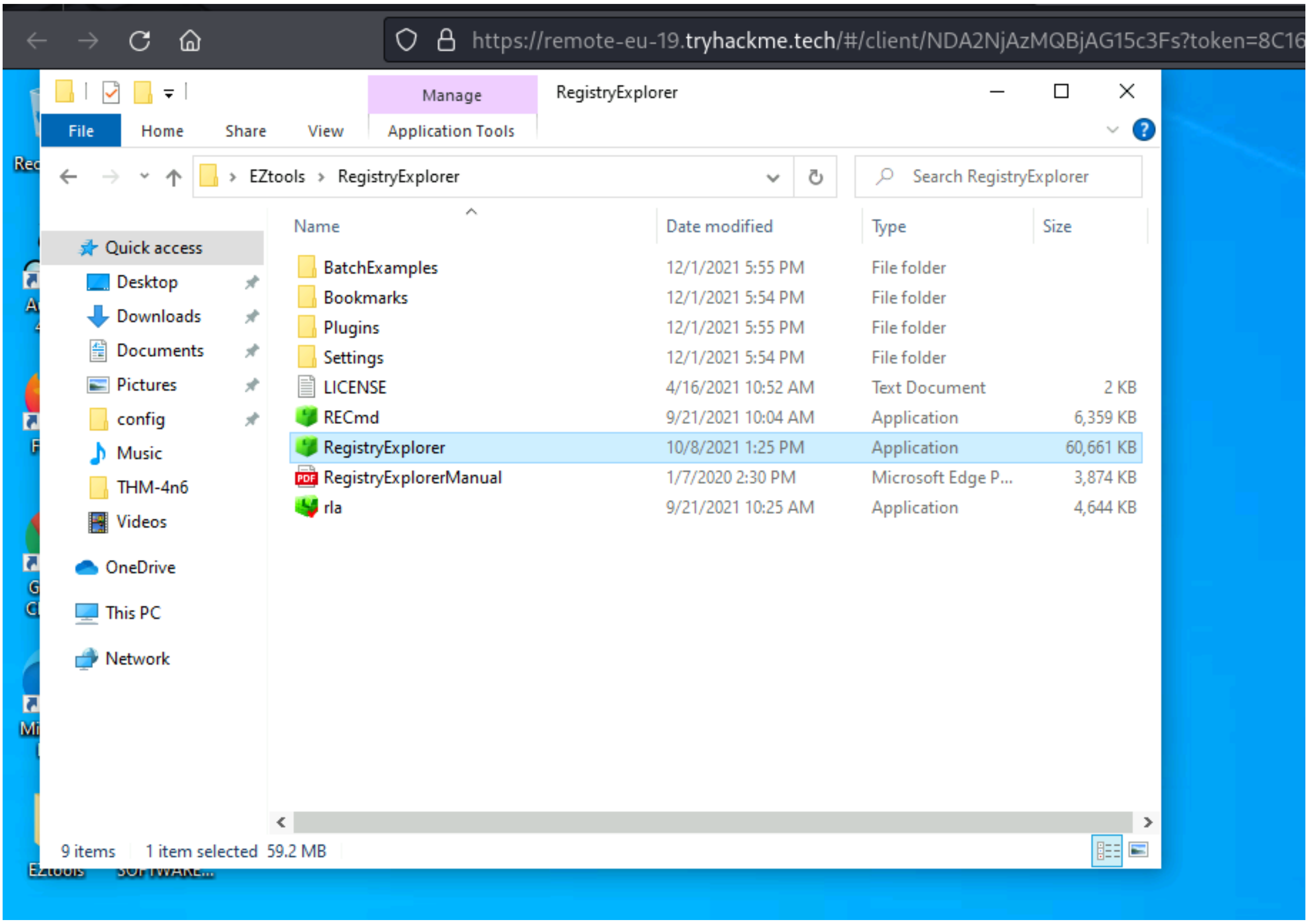
Timestamp	Device	Serial Number	Guid	Friendly Name
2021-11-25 07:16:54			{E251921F-4DA2-11EC-A783-001A7DDA7110 }	USB
2021-11-25 07:16:54			{F529A9D6-4D9E-11EC-A782-001A7DDA7110 }	New Volume



How many user created accounts are present on the system?

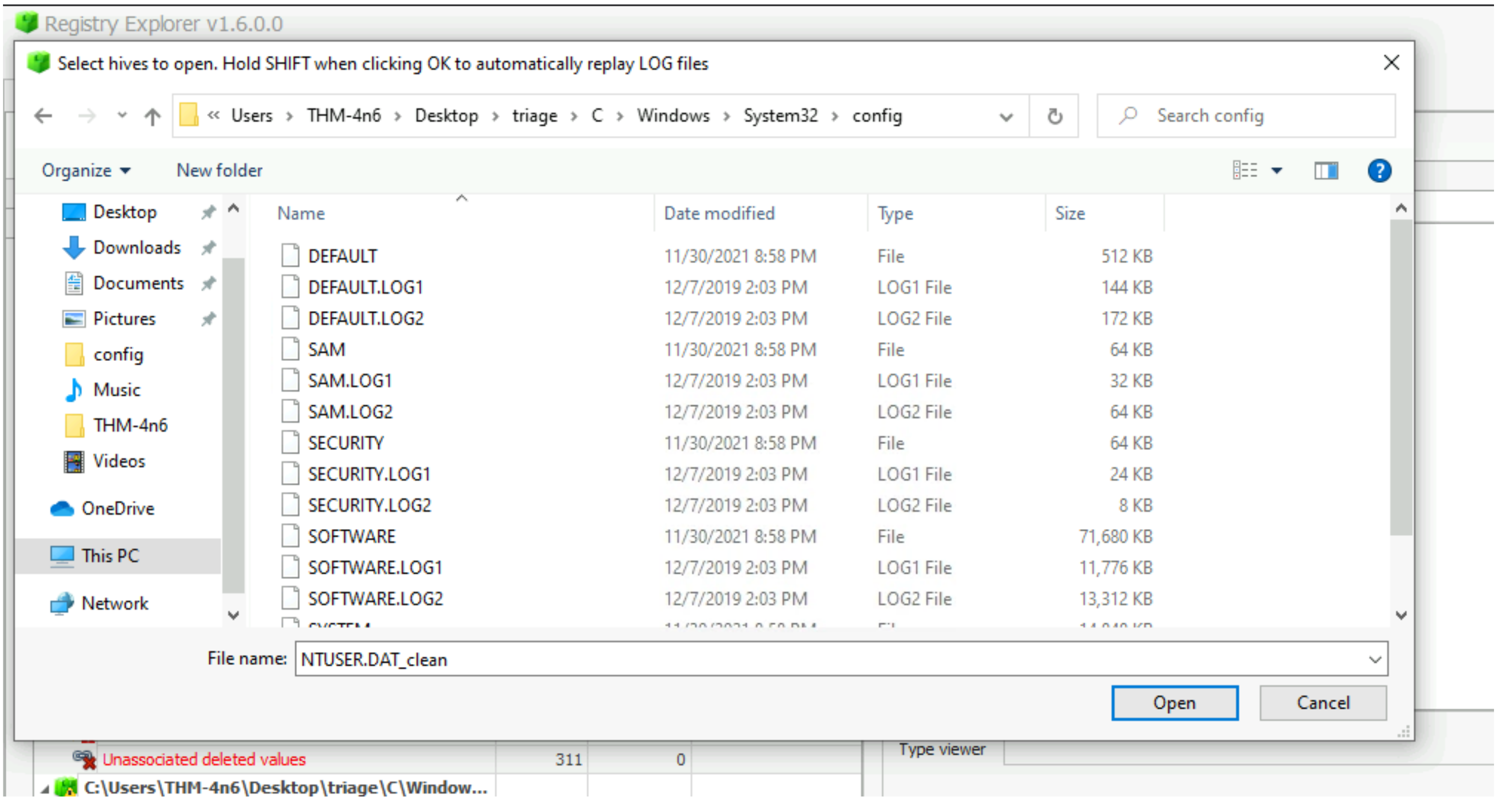
3

I will be RDPing into the machine. I wrote the instructions here on how I did it.
Loading the hives into RegistryExplorer took me about 20 minutes of searching and messing around with the interface. It was difficult when I didnâ€™t even start on the actual questions yet! To load the hives into RegistryExplorer, we need to open it first. RegistryExplorer is located by going to EZTools folder -> RegistryExplorer -> RegistryExplorer. It may take a while for the application to load.



Name	Date modified	Type	Size
BatchExamples	12/1/2021 5:55 PM	File folder	
Bookmarks	12/1/2021 5:54 PM	File folder	
Plugins	12/1/2021 5:55 PM	File folder	
Settings	12/1/2021 5:54 PM	File folder	
LICENSE	4/16/2021 10:52 AM	Text Document	2 KB
RECmd	9/21/2021 10:04 AM	Application	6,359 KB
RegistryExplorer	10/8/2021 1:25 PM	Application	60,661 KB
RegistryExplorerManual	1/7/2020 2:30 PM	Microsoft Edge P...	3,874 KB
rla	9/21/2021 10:25 AM	Application	4,644 KB

Once Registry Explorer loads, I loaded the hive. I did this by going to File -> Load hive
From here, I navigated to triage -> C -> Windows -> System 32 -> config to access the registry files.



Select hives to open. Hold SHIFT when clicking OK to automatically replay LOG files

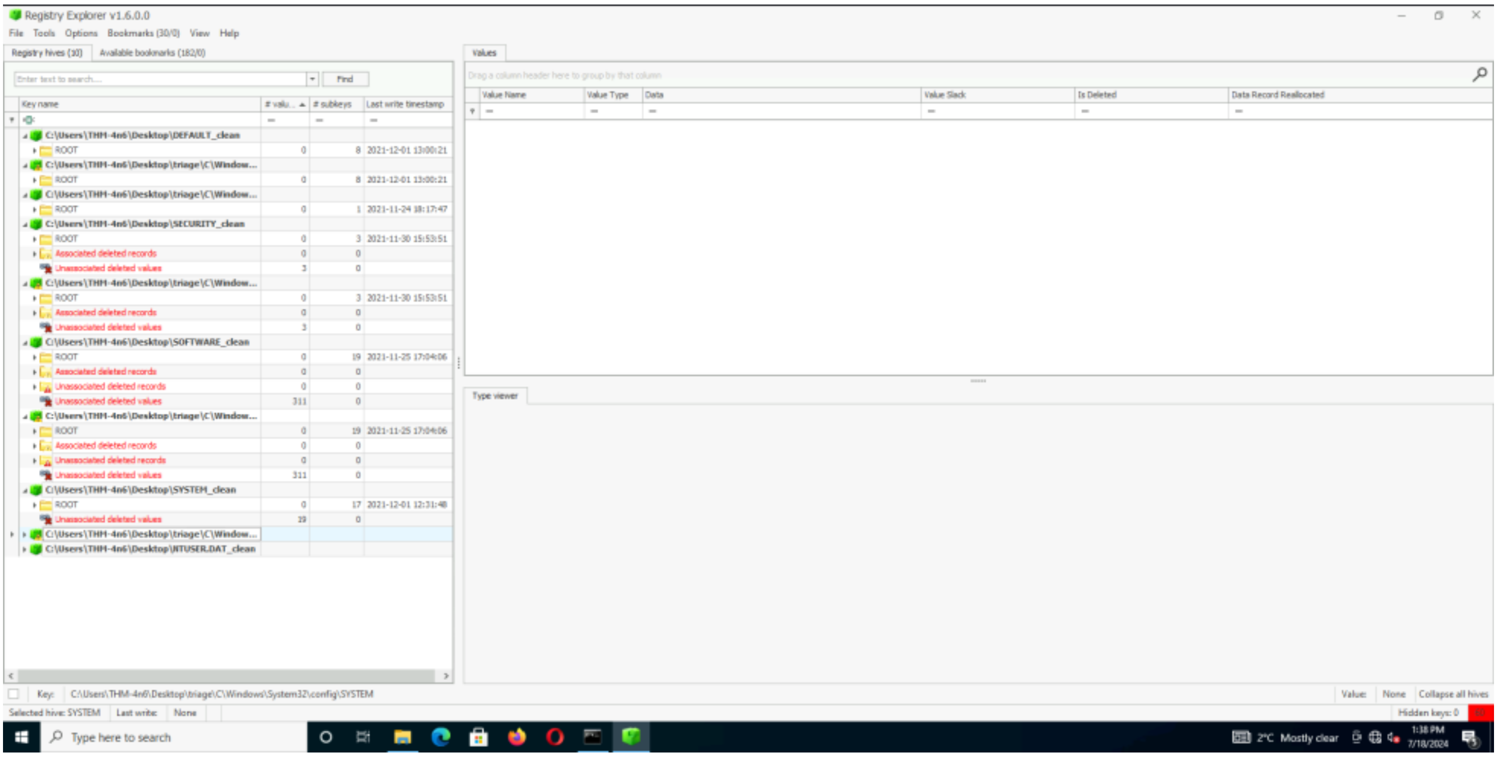
Registry Explorer v1.6.0.0
« Users › THM-4n6 › Desktop › triage › C › Windows › System32 › config
Search config
Organize
New folder
Desktop
Downloads
Documents
Pictures
config
Music
THM-4n6
Videos
OneDrive
This PC
Network
Open
Cancel
Unassociated deleted values
311
0
C:\Users\THM-4n6\Desktop\triage\C\Window...
Type viewer

Name	Date modified	Type	Size
DEFAULT	11/30/2021 8:58 PM	File	512 KB
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	11/30/2021 8:58 PM	File	64 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	11/30/2021 8:58 PM	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	11/30/2021 8:58 PM	File	71,680 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

File name: NTUSER.DAT_clean

I loaded each file one at a time starting with "DEFAULT." A warning should pop up about sequence numbers not matching. Do not worry. Just press Yes. Next, it says select transaction logs. We will select both DEFAULT.LOG1 and DEFAULT.LOG2 files. To select more than one file, you can click on the first file, then hold CTRL and click on the second file.

After I successfully loaded my first hive, now I did it again for the hives, which are SAM, SECURITY, SOFTWARE, and SYSTEM. The image below is the final image after loading all the hives.



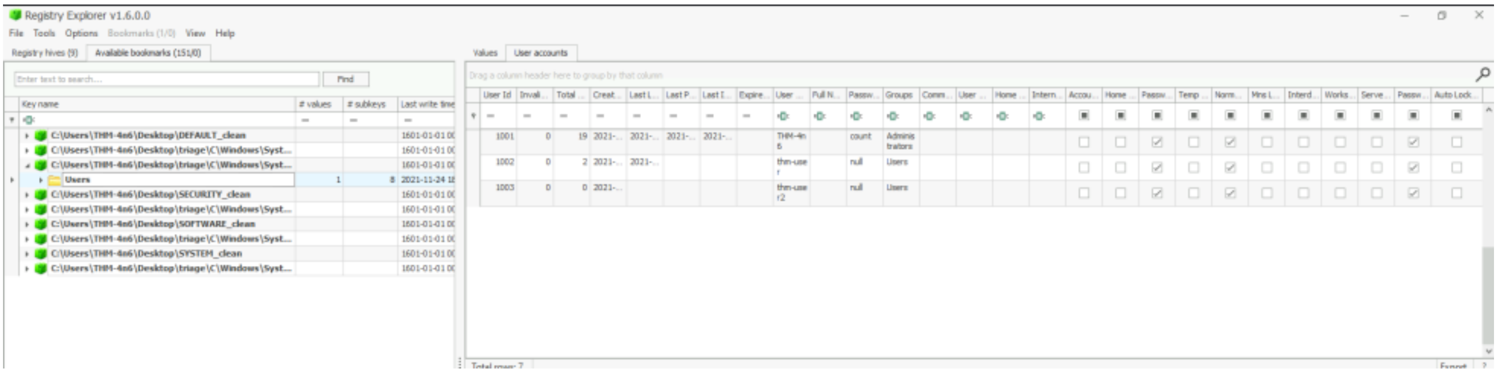
Key name	# valu...	# subkeys	Last write timestamp
C:\Users\THM-4n6\Desktop\DEFAULT_clean			
ROOT	0	8	2021-12-01 13:00:21
C:\Users\THM-4n6\Desktop\triage\C\Window...			
ROOT	0	8	2021-12-01 13:00:21
C:\Users\THM-4n6\Desktop\triage\C\Window...			
ROOT	0	1	2021-11-24 18:17:47
C:\Users\THM-4n6\Desktop\SECURITY_clean			
ROOT	0	3	2021-11-30 15:53:51
Associated deleted records	0	0	
Unassociated deleted values	3	0	
C:\Users\THM-4n6\Desktop\triage\C\Window...			
ROOT	0	3	2021-11-30 15:53:51
Associated deleted records	0	0	
Unassociated deleted values	3	0	
C:\Users\THM-4n6\Desktop\SOFTWARE_clean			
ROOT	0	19	2021-11-25 17:04:06
Associated deleted records	0	0	
Unassociated deleted records	0	0	
Unassociated deleted values	311	0	
C:\Users\THM-4n6\Desktop\triage\C\Window...			
ROOT	0	19	2021-11-25 17:04:06
Associated deleted records	0	0	
Unassociated deleted records	0	0	
Unassociated deleted values	311	0	
C:\Users\THM-4n6\Desktop\SYSTEM_clean			
ROOT	0	17	2021-12-01 12:31:48
Unassociated deleted values	19	0	
C:\Users\THM-4n6\Desktop\triage\C\Window...			
C:\Users\THM-4n6\Desktop\NTUSER.DAT_clean			

Key: C:\Users\THM-4n6\Desktop\triage\C\Windows\System32\config\SYSTEM

Selected hive: SYSTEM Last write: None

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.

The right handed side should then show something similar to this. Look at "User Id" column and look for IDs starting with 10. That means it's a user created account. I only knew that because I checked the hint.


Registry Explorer v1.6.0.0
File Tools Options Bookmarks (1/0) View Help
Registry hives (9) Available bookmarks (151/0)
Enter text to search... Find
Values User accounts
Drag a column header here to group by that column

Key name	# values	# subkeys	Last write time
C:\Users\THM-4n6\Desktop\DEFAULT_clean			1601-01-01 00
C:\Users\THM-4n6\Desktop\triage\C\Windows\Syst...			1601-01-01 00
C:\Users\THM-4n6\Desktop\triage\C\Windows\Syst...			1601-01-01 00
Users	1	8	2021-11-24 18
C:\Users\THM-4n6\Desktop\SECURITY_clean			1601-01-01 00
C:\Users\THM-4n6\Desktop\triage\C\Windows\Syst...			1601-01-01 00
C:\Users\THM-4n6\Desktop\SOFTWARE_clean			1601-01-01 00
C:\Users\THM-4n6\Desktop\triage\C\Windows\Syst...			1601-01-01 00
C:\Users\THM-4n6\Desktop\SYSTEM_clean			1601-01-01 00
C:\Users\THM-4n6\Desktop\triage\C\Windows\Syst...			1601-01-01 00

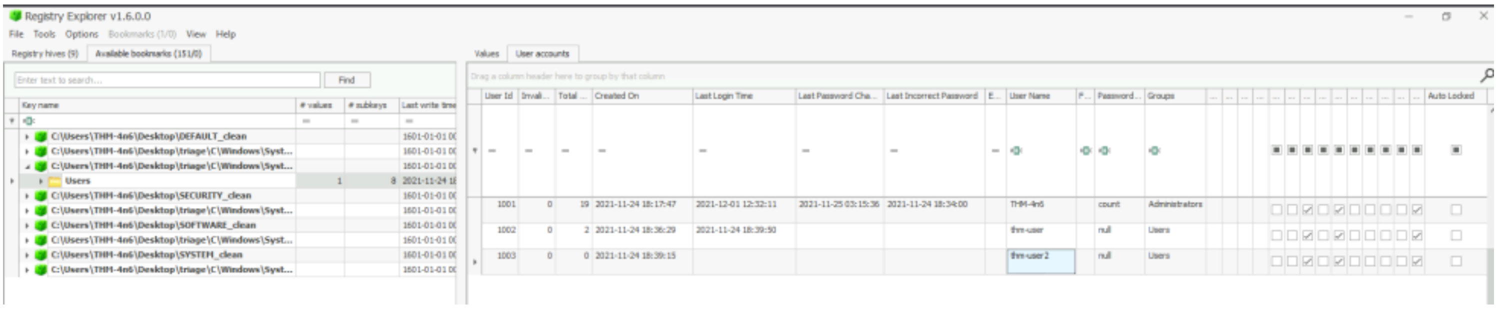
User Id	Invali...	Total ...	Creat...	Last L...	Last P...	Last I...	Expire...	User ...	Full N...	Passw...	Groups	Comm...	User ...	Home ...	Intern...	Accou...	Home ...	Passw...	Temp ...	Norm...	Mns L...	Interd...	Works...	Serve...	Passw...	Auto Lock...
1001	0	19	2021-...	2021-...	2021-...	2021-...		THM-4n6		count	Administrators					☐	☐	☑	☐	☑	☐	☐	☐	☐	☑	☐
1002	0	2	2021-...	2021-...				thm-user		null	Users					☐	☐	☑	☐	☑	☐	☐	☐	☐	☑	☐
1003	0	0	2021-...					thm-user2		null	Users					☐	☐	☑	☐	☑	☐	☐	☐	☐	☑	☐

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

thm-user2

✓ Correct

After the above, I extended some of the columns so I can see what the column headers were. From here, we can see one user never logged on.


Registry Explorer v1.6.0.0
File Tools Options Bookmarks (1/0) View Help
Registry hives (9) Available bookmarks (151/0)
Enter text to search... Find
Values User accounts
Drag a column header here to group by that column

Key name	# values	# subkeys	Last write time
C:\Users\THM-4n6\Desktop\DEFAULT_clean			1601-01-01 00
C:\Users\THM-4n6\Desktop\triage\C\Windows\Syst...			1601-01-01 00
C:\Users\THM-4n6\Desktop\triage\C\Windows\Syst...			1601-01-01 00
Users	1	8	2021-11-24 18
C:\Users\THM-4n6\Desktop\SECURITY_clean			1601-01-01 00
C:\Users\THM-4n6\Desktop\triage\C\Windows\Syst...			1601-01-01 00
C:\Users\THM-4n6\Desktop\SOFTWARE_clean			1601-01-01 00
C:\Users\THM-4n6\Desktop\triage\C\Windows\Syst...			1601-01-01 00
C:\Users\THM-4n6\Desktop\SYSTEM_clean			1601-01-01 00
C:\Users\THM-4n6\Desktop\triage\C\Windows\Syst...			1601-01-01 00

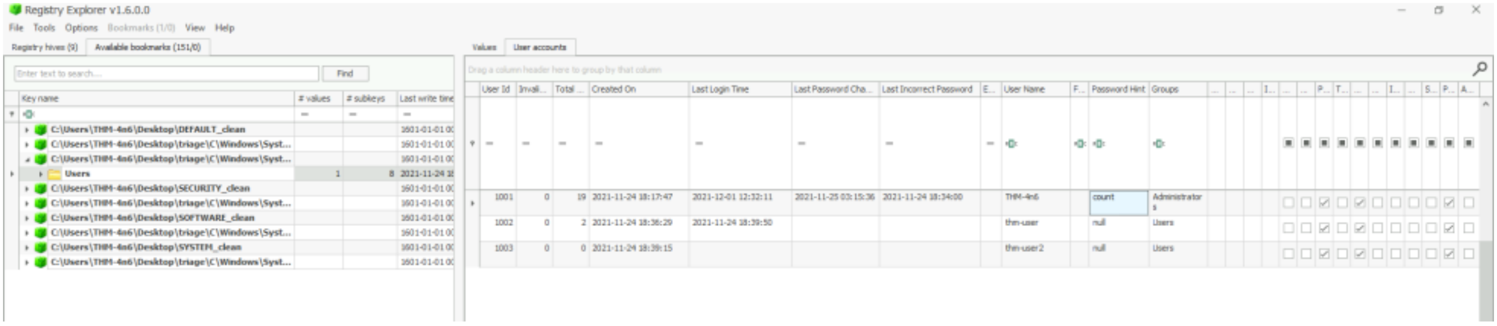
User Id	Invali...	Total ...	Created On	Last Login Time	Last Password Cha...	Last Incorrect Password	E...	User Name	F...	Password...	Groups	...	...	...	...	...	...	...	...	...	...	...	...	...	...	Auto Locked
1001	0	19	2021-11-24 18:17:47	2021-12-01 12:32:11	2021-11-25 03:15:36	2021-11-24 18:34:00		THM-4n6		count	Administrators					☐	☐	☑	☐	☑	☐	☐	☐	☐	☑	☐
1002	0	2	2021-11-24 18:36:29	2021-11-24 18:39:50				thm-user		null	Users					☐	☐	☑	☐	☑	☐	☐	☐	☐	☑	☐
1003	0	0	2021-11-24 18:39:15					thm-user2		null	Users					☐	☐	☑	☐	☑	☐	☐	☐	☐	☑	☐

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

count

✓ Correct

Similar to question 2, I looked at the columns to see which one gives me the answer I need and extended it for better visibility.


Registry Explorer v1.6.0.0
File Tools Options Bookmarks (1/0) View Help
Registry hives (9) Available bookmarks (151/0)
Enter text to search... Find
Values User accounts
Drag a column header here to group by that column

Key name	# values	# subkeys	Last write time
C:\Users\THM-4n6\Desktop\DEFAULT_clean			1601-01-01 00
C:\Users\THM-4n6\Desktop\triage\C\Windows\Syst...			1601-01-01 00
C:\Users\THM-4n6\Desktop\triage\C\Windows\Syst...			1601-01-01 00
Users	1	8	2021-11-24 18
C:\Users\THM-4n6\Desktop\SECURITY_clean			1601-01-01 00
C:\Users\THM-4n6\Desktop\triage\C\Windows\Syst...			1601-01-01 00
C:\Users\THM-4n6\Desktop\SOFTWARE_clean			1601-01-01 00
C:\Users\THM-4n6\Desktop\triage\C\Windows\Syst...			1601-01-01 00
C:\Users\THM-4n6\Desktop\SYSTEM_clean			1601-01-01 00
C:\Users\THM-4n6\Desktop\triage\C\Windows\Syst...			1601-01-01 00

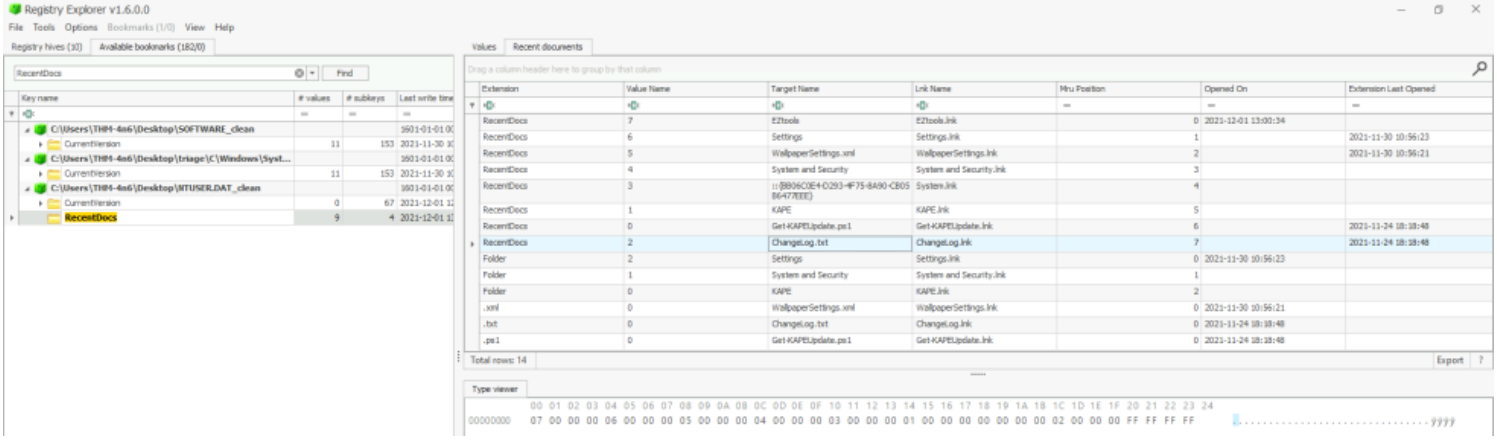
User Id	Invali...	Total ...	Created On	Last Login Time	Last Password Cha...	Last Incorrect Password	E...	User Name	F...	Password Hint	Groups	...	...	...	I...	...	...	P...	T...	...	...	I...	...	S...	P...	A...
1001	0	19	2021-11-24 18:17:47	2021-12-01 12:32:11	2021-11-25 03:15:36	2021-11-24 18:34:00		THM-4n6		count	Administrators					☐	☐	☑	☐	☑	☐	☐	☐	☐	☑	☐
1002	0	2	2021-11-24 18:36:29	2021-11-24 18:39:50				thm-user		null	Users					☐	☐	☑	☐	☑	☐	☐	☐	☐	☑	☐
1003	0	0	2021-11-24 18:39:15					thm-user2		null	Users					☐	☐	☑	☐	☑	☐	☐	☐	☐	☑	☐

When was the file 'Changelog.txt' accessed?

2021-11-21 18:18:48

✓ Correct

I went back to one of the reading sections as I recalled learning where to find recent files. It's in Task 7. The location to find where a file was last accessed is at NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs. Alternatively, you can type "RecentDocs" in the search bar and then look for the result that is under NTUSER.DAT. I was practicing navigating it and didn't use the search bar.


Registry Explorer v1.6.0.0
File
Tools
Options
Bookmarks (1/0)
View
Help
Registry hives (10)
Available bookmarks (182/0)
RecentDocs
Find
Values
Recent documents
Drag a column header here to group by that column

Key name	# values	# subkeys	Last write time
C:\Users\THM-4n6\Desktop\SOFTWARE_clean			1601-01-01 00
CurrentVersion	11	153	2021-11-30 1
C:\Users\THM-4n6\Desktop\triage\C\Windows\Syst...			1601-01-01 00
CurrentVersion	11	153	2021-11-30 1
C:\Users\THM-4n6\Desktop\NTUSER.DAT_clean			1601-01-01 00
CurrentVersion	0	67	2021-12-01 1
RecentDocs	9	4	2021-12-01 1

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

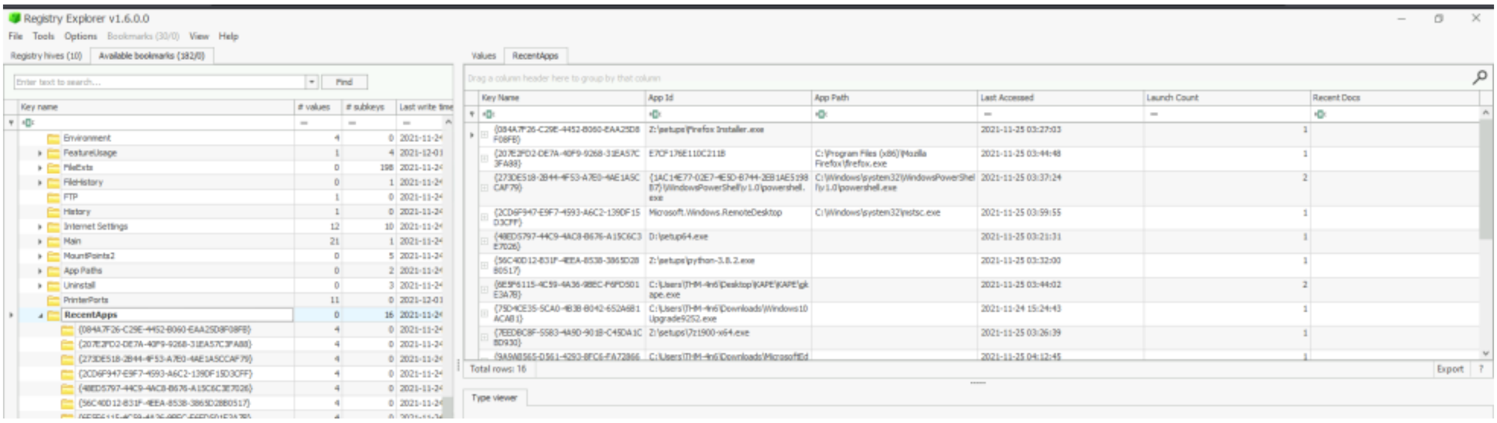
```
         00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24
00000000 07 00 00 00 06 00 00 00 05 00 00 00 04 00 00 00 03 00 00 00 01 00 00 00 00 00 00 00 02 00 00 00 FF FF FF FF    ..............................ÿÿÿÿ
```

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

Z:\setups\python-3.8.2.exe

✓ Correct

I checked the hint to see how to do this section properly. It said to look at UserAssist to look for any execution artifacts. I ended up doing that and looking through each of the folder in UserAssist. Found python as shown below.


Registry Explorer v1.6.0.0
File
Tools
Options
Bookmarks (30/0)
View
Help
Registry hives (10)
Available bookmarks (182/0)
Enter text to search...
Find
Values
RecentApps
Drag a column header here to group by that column

Key name	# values	# subkeys	Last write time
Environment	4	0	2021-11-24
FeatureUsage	1	4	2021-12-01
FileExts	0	198	2021-11-24
FileHistory	0	1	2021-11-24
FTP	1	0	2021-11-24
History	1	0	2021-11-24
Internet Settings	12	10	2021-11-24
Main	21	1	2021-11-24
MountPoints2	0	5	2021-11-24
App Paths	0	2	2021-11-24
Uninstall	0	3	2021-11-24
PrinterPorts	11	0	2021-12-01
RecentApps	0	16	2021-11-24
{084A7F26-C29E-4452-B060-EAA25D8F08FB}	4	0	2021-11-24
{207E2FD2-DE7A-40F9-9268-31EA57C3FA88}	4	0	2021-11-24
{273DE518-2B44-4F53-A7E0-4AE1A5CCAF79}	4	0	2021-11-24
{2CD6F947-E9F7-4593-A6C2-139DF15D3CFF}	4	0	2021-11-24
{48ED5797-44C9-4AC8-B676-A15C6C3E7026}	4	0	2021-11-24
{56C40D12-831F-4EEA-8538-3865D28B0517}	4	0	2021-11-24

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	
{56C40D12-831F-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	
{7EED8C8F-5583-4A9D-901B-C45DA1C8D930}	Z:\setups\7z1900-x64.exe		2021-11-25 03:26:39	1	
{9A9A8565-D561-4293-8FC6-FA72866	C:\Users\THM-4n6\Downloads\MicrosoftEd		2021-11-25 04:12:45	1	

Total rows: 16

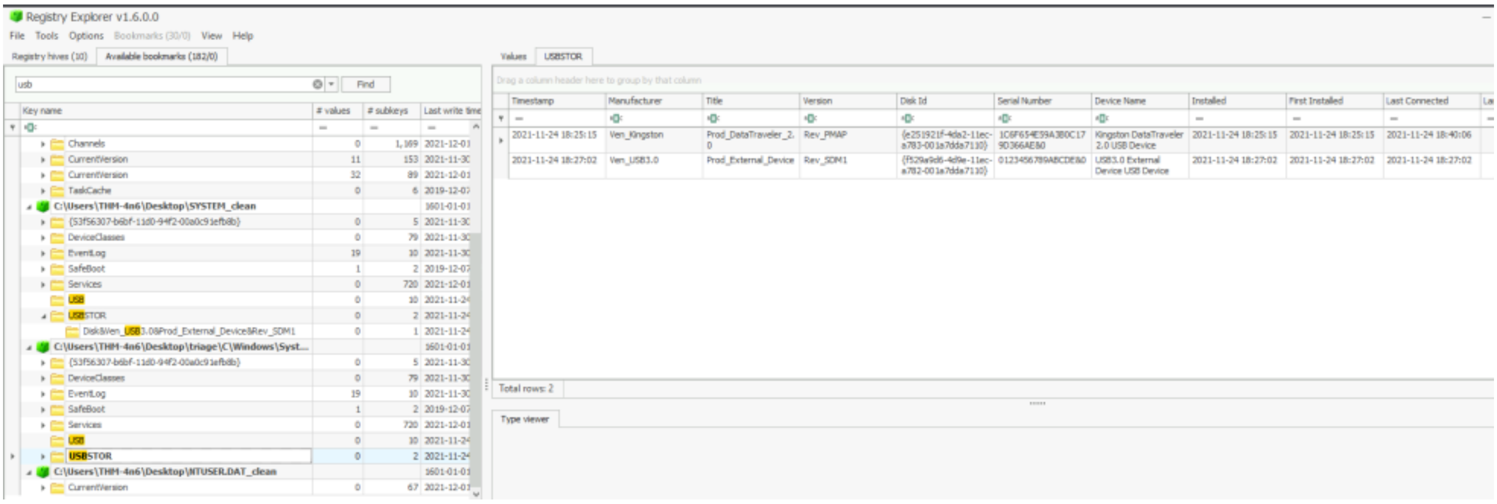
When was the USB device with the friendly name 'USB' last connected?

2021-11-24 18:40:06

✓ Correct

I reread task 9 to jog my memory on how to get the device name. I went to SOFTWARE\Microsoft\Windows Portable Devices\Devices first. Unfortunately, Microsoft folder didnâ€™t exist, so the path I used was SOFTWARE\Windows Portable Devices\Devices. I saw that one of the two folders had a FriendlyName value of USB. I took note of, what I

believe to be, the serial number in the folder name.
Now I searched for "USBSTOR" and looked at the right side to compare values. It looks like the value I took note of wasn't the serial number but disk ID instead.



Registry Explorer v1.6.0.0

File Tools Options Bookmarks (30/0) View Help

Registry hives (10) | Available bookmarks (182/0)

usb | Find

Key name	# values	# subkeys	Last write time
Channels	0	1,169	2021-12-01
CurrentVersion	11	153	2021-11-30
CurrentVersion	32	89	2021-12-01
TaskCache	0	6	2019-12-07
C:\Users\THM-4n6\Desktop\SYSTEM_clean			1601-01-01
{53f56307-b6bf-11d0-94f2-00a0c91efb8b}	0	5	2021-11-30
DeviceClasses	0	79	2021-11-30
EventLog	19	10	2021-11-30
SafeBoot	1	2	2019-12-07
Services	0	720	2021-12-01
USB	0	10	2021-11-24
USBSTOR	0	2	2021-11-24
Disk&Ven_USB3.0&Prod_External_Device&Rev_SDM1	0	1	2021-11-24
C:\Users\THM-4n6\Desktop\triage\C\Windows\Syst...			1601-01-01
{53f56307-b6bf-11d0-94f2-00a0c91efb8b}	0	5	2021-11-30
DeviceClasses	0	79	2021-11-30
EventLog	19	10	2021-11-30
SafeBoot	1	2	2019-12-07
Services	0	720	2021-12-01
USB	0	10	2021-11-24
USBSTOR	0	2	2021-11-24
C:\Users\THM-4n6\Desktop\NTUSER.DAT_clean			1601-01-01
CurrentVersion	0	67	2021-12-01

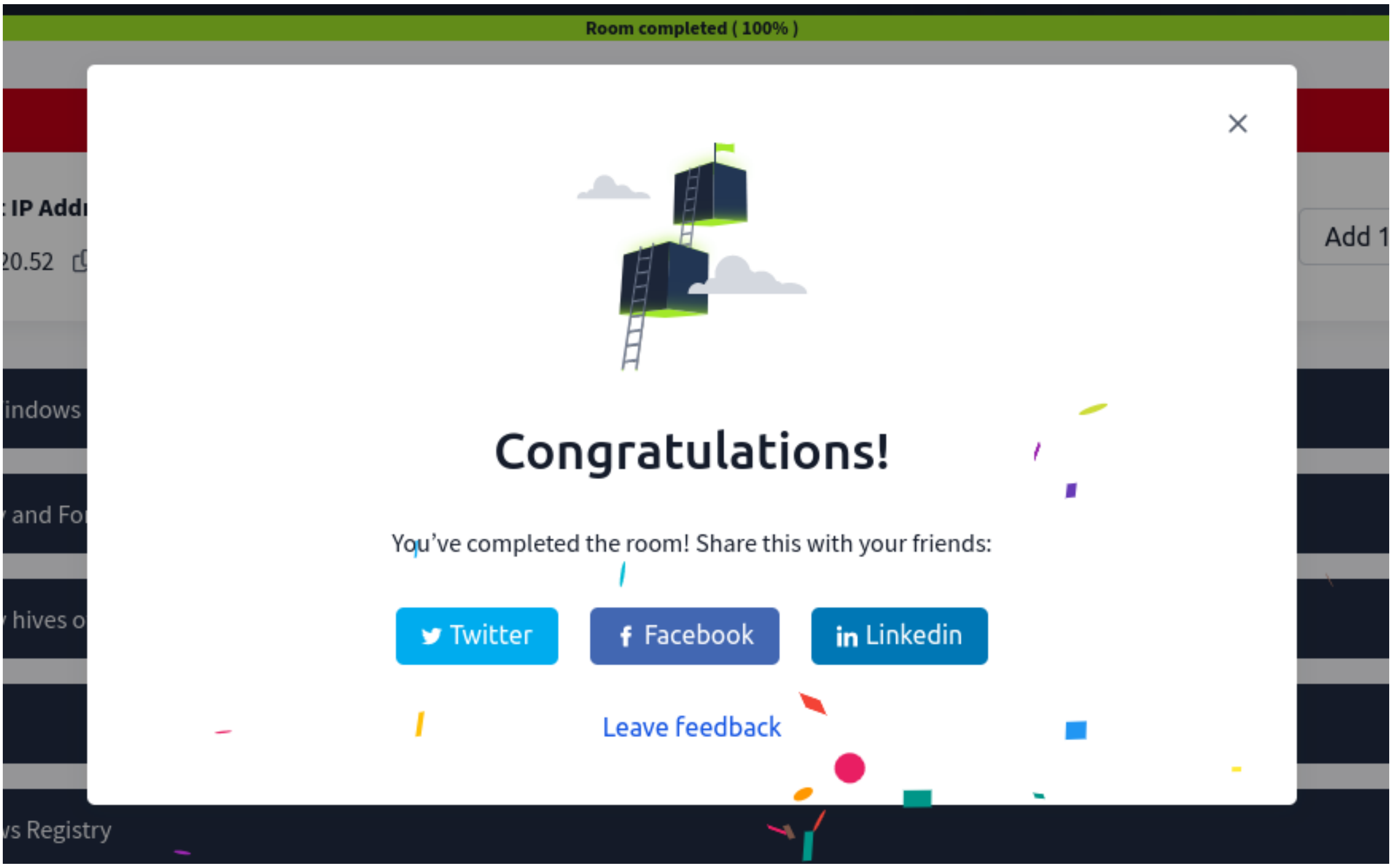
Values | USBSTOR

Drag a column header here to group by that column

Timestamp	Manufacturer	Title	Version	Disk Id	Serial Number	Device Name	Installed	First Installed	Last Connected
2021-11-24 18:25:15	Ven_Kingston	Prod_DataTraveler_2.0	Rev_PMAP	{e251921f-4da2-11ec-a783-001a7dda7110}	1C6F654E59A3B0C179D366AE&0	Kingston DataTraveler 2.0 USB Device	2021-11-24 18:25:15	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

Total rows: 2

Type viewer



Room completed (100%)

Congratulations!

You've completed the room! Share this with your friends:

Twitter | Facebook | in Linkedin

Leave feedback

https://tryhackme.com/r/room/windowsforensics1

CONCLUSION
I personally felt like this was the right difficulty for me. I've used EnCase and Autopsy before but never even heard of Registry Explorer. I love getting exposed to more tools as you'll never know what your organization will be using. Definitely took me a while to get started as the hardest part for me was understanding how to load the files into Registry Explorer. I enjoyed digging around trying to look for the answer. I even saved the cheat sheet that was given at the end of the room. There is absolutely no way I remembered everything I've read so the cheat sheet will definitely be useful.