TRYHACKME ROOM = WINDOWS FORENSICS 1

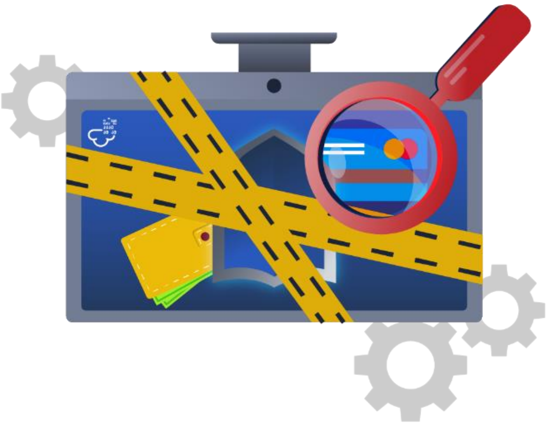
Introduction:

This report presents the findings and analysis of the Windows Forensics 1 room from TryHackMe, which covers the fundamentals of Windows registry forensics. The Windows registry is a vital source of evidence for digital forensic investigators, containing critical information about the system and user activities.

https://tryhackme.com/p/Damiano254

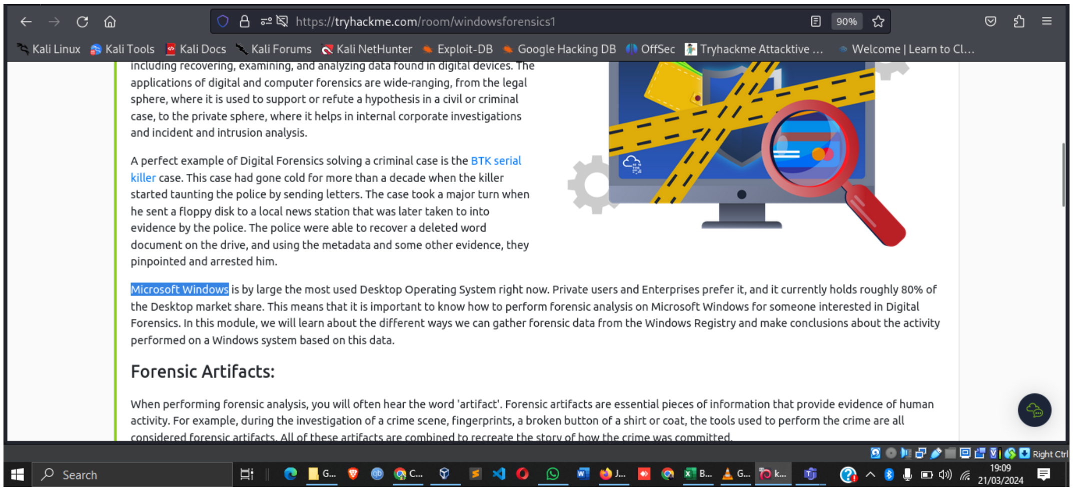
Task 1: Introduction to Windows Forensics

- Microsoft Windows is the most widely used desktop operating system, making knowledge of Windows forensics essential for digital forensic investigations. Forensic artifacts in Windows systems are the residual evidence of human activity that can be used to recreate the actions performed on a system. Computer forensics deals with the examination of digital devices and their data for evidence in civil, criminal, or internal investigations.
- Forensic artifacts are the pieces of information that provide evidence of human activity.
- Windows forensics involves analysing the artifacts in the Windows operating system to gather evidence of activities performed on the system.



What is the most used Desktop Operating System right now?

- **Microsoft Windows**



https://tryhackme.com/room/windowsforensics1

including recovering, examining, and analyzing data found in digital devices. 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.

A perfect example of Digital Forensics solving a criminal case is the BTK serial killer case. This case had gone cold for more than a decade when the killer started taunting the police by sending letters. The case took a major turn when he sent a floppy disk to a local news station that was later taken to into evidence by the police. The police were able to recover a deleted word document on the drive, and using the metadata and some other evidence, they pinpointed and arrested him.

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:

When performing forensic analysis, you will often hear the word 'artifact'. Forensic artifacts are essential pieces of information that provide evidence of human activity. For example, during the 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. All of these artifacts are combined to recreate the story of how the crime was committed.

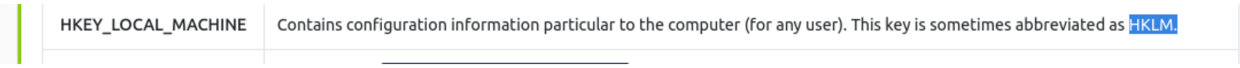
Task 2: Windows Registry and Forensics

- The Windows Registry is a collection of databases that stores configuration data for the Windows operating system.

- The registry consists of keys and values, where keys are the folders and values are the data stored in the keys.
- A registry hive is a single file that contains one or more keys, subkeys, and values.
- The Windows Registry Editor (regedit.exe) is a built-in Windows utility to view and edit the registry.

What is the short form for HKEY_LOCAL_MACHINE?

- **HKLM**



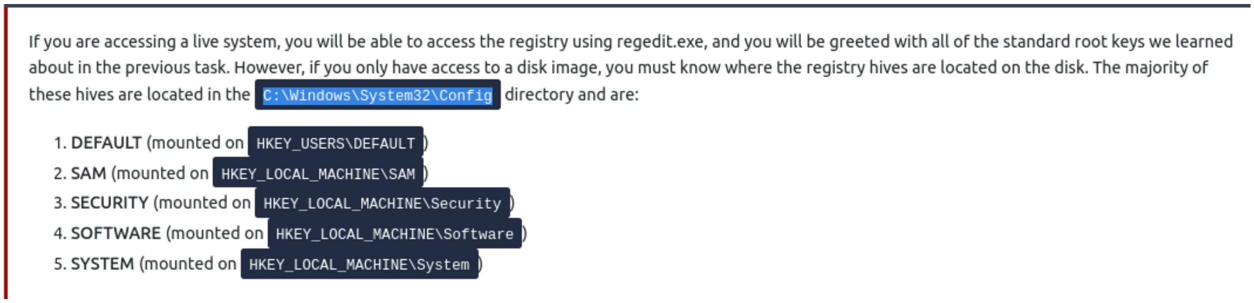
HKEY_LOCAL_MACHINE Contains configuration information particular to the computer (for any user). This key is sometimes abbreviated as HKLM.

Task 3: Accessing Registry Hives Offline

- When analysing a Windows system, forensic investigators often deal with disk images. To perform forensics on a Windows system using disk images, it is essential to know the location of the registry hives.

Path for the five main registry hives (DEFAULT, SAM, SECURITY, SOFTWARE, and SYSTEM):

- **C:\Windows\System32\Config**



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`)

Path for the AmCache hive:

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

Task 4: Data Acquisition

- Data acquisition involves creating a copy of the system or the required data and performing analysis on that.
- KAPE, Autopsy, and FTK Imager are popular tools to acquire registry data.

Tool	**Description**
KAPE	A live data acquisition and analysis tool for Windows systems.
Autopsy	An open-source digital forensics platform for Windows, macOS, and Linux systems.
FTK Imager	A forensic imaging tool for Windows, macOS, and Linux systems.

Task 5: Exploring Windows Registry

- Various tools can be used to view and analyze the Windows Registry.
- Registry Viewer, Registry Explorer, and RegRipper are popular tools to view and analyze the Windows Registry.

Tool	**Description**
Registry Viewer	A Windows registry viewer developed by Access Data.

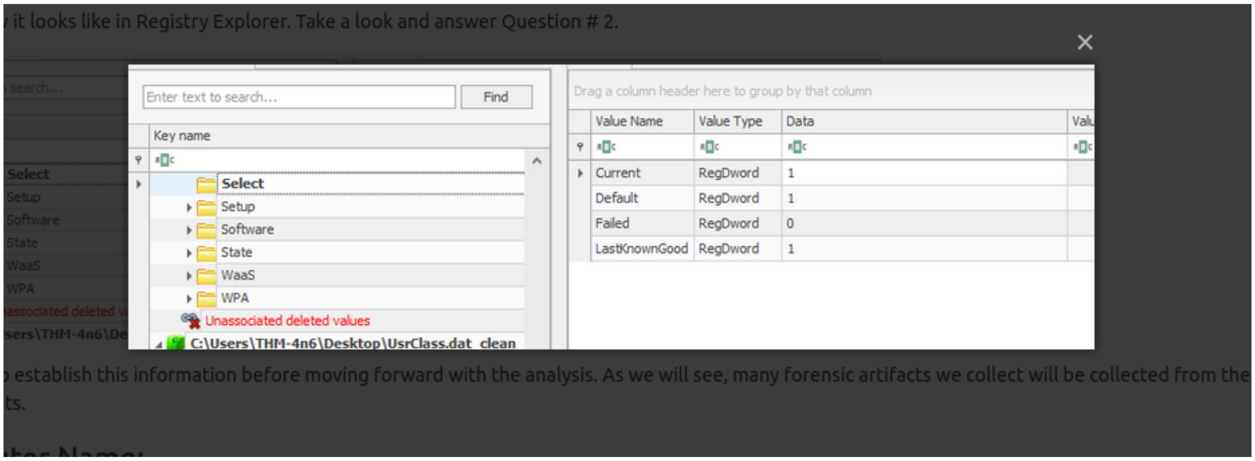
Tool	Description
Registry Explorer	A Windows registry viewer developed by Eric Zimmerman, which can load multiple hives and merge transaction logs.
RegRipper	A utility that takes a registry hive as input and outputs a report that extracts data from some of the forensically important keys and values.

Task 6: System Information and System Accounts

- The SYSTEM hive contains the system's configuration data required for controlling system start-up.
- The Select key (HKEY_LOCAL_MACHINE\SYSTEM\Select) contains the most accurate system information.
- The Computer Name can be found in the SYSTEM hive at HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ComputerName.

1. What is the Current Build Number of the machine whose data is being investigated?
    - **19044**

2. Which ControlSet contains the last known good configuration?
    - **1**



it looks like in Registry Explorer. Take a look and answer Question # 2.

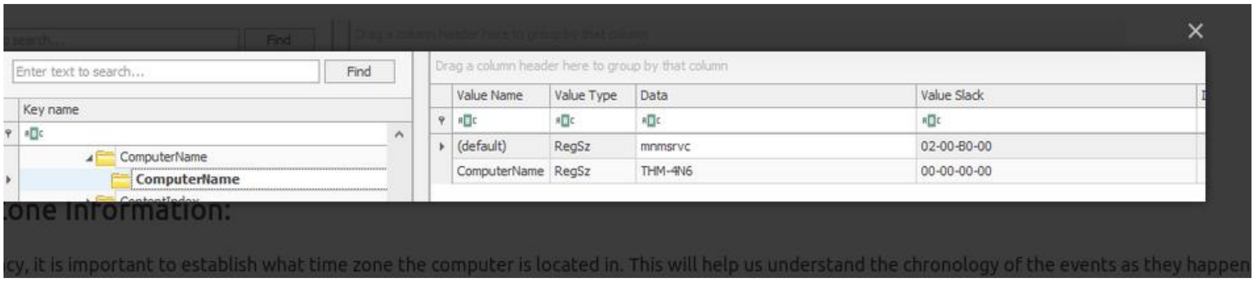
Value Name	Value Type	Data
Current	RegDword	1
Default	RegDword	1
Failed	RegDword	0
LastKnownGood	RegDword	1

establish this information before moving forward with the analysis. As we will see, many forensic artifacts we collect will be collected from the

ts.

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

3. What is the Computer Name of the computer?
    - **THM-4n6**

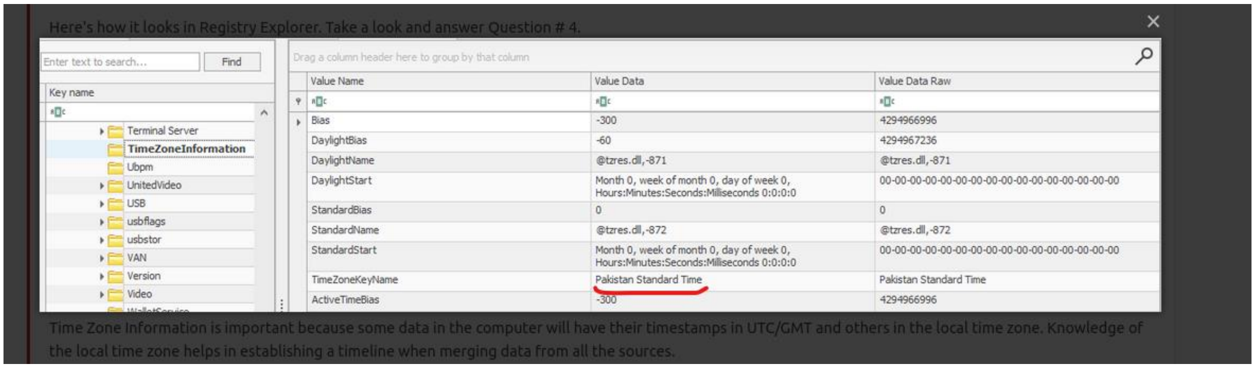


Value Name	Value Type	Data	Value Slack
(default)	RegSz	mnmsrvc	02-00-B0-00
ComputerName	RegSz	THM-4N6	00-00-00-00

one Information:

cy, 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 happen

4. What is the value of the TimeZoneKeyName?
    - **Pakistan Standard Time**

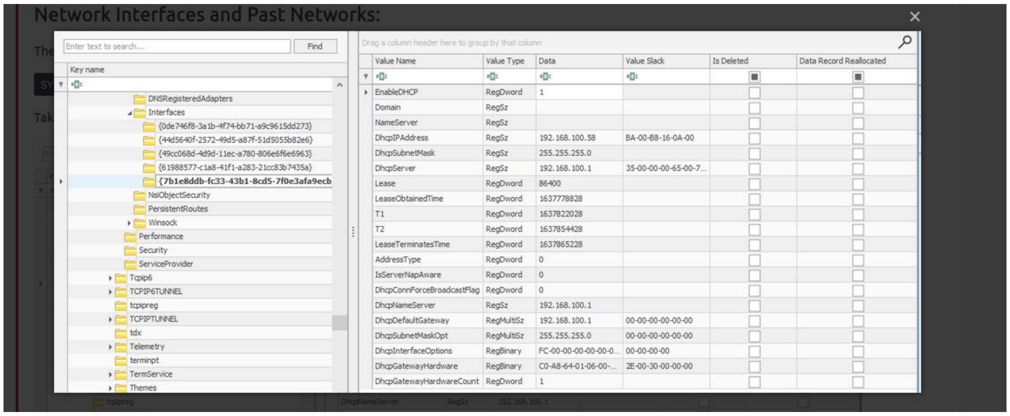


Here's how it looks in Registry Explorer. Take a look and answer Question # 4.

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

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.

5. What is the DHCP IP address?
   - **192.168.100.58**

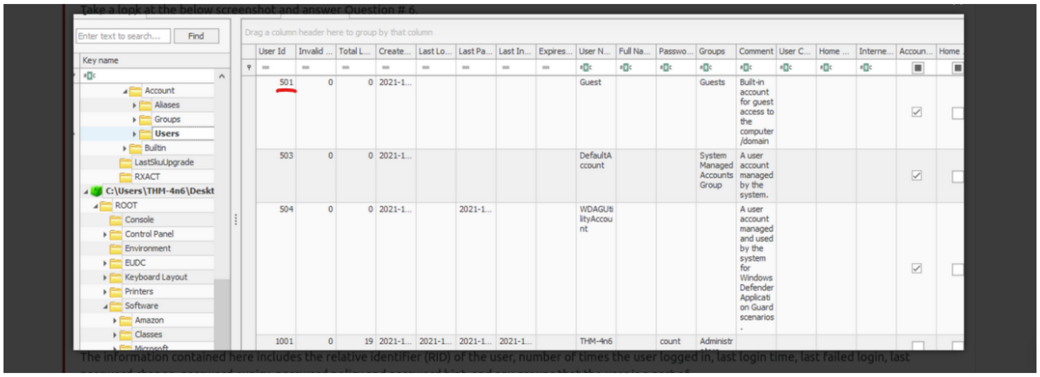


Network Interfaces and Past Networks:

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		□	□

6. What is the RID of the Guest User account?
   - **501**



Take a look at the below screenshot and answer Question # 6.

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					□	□

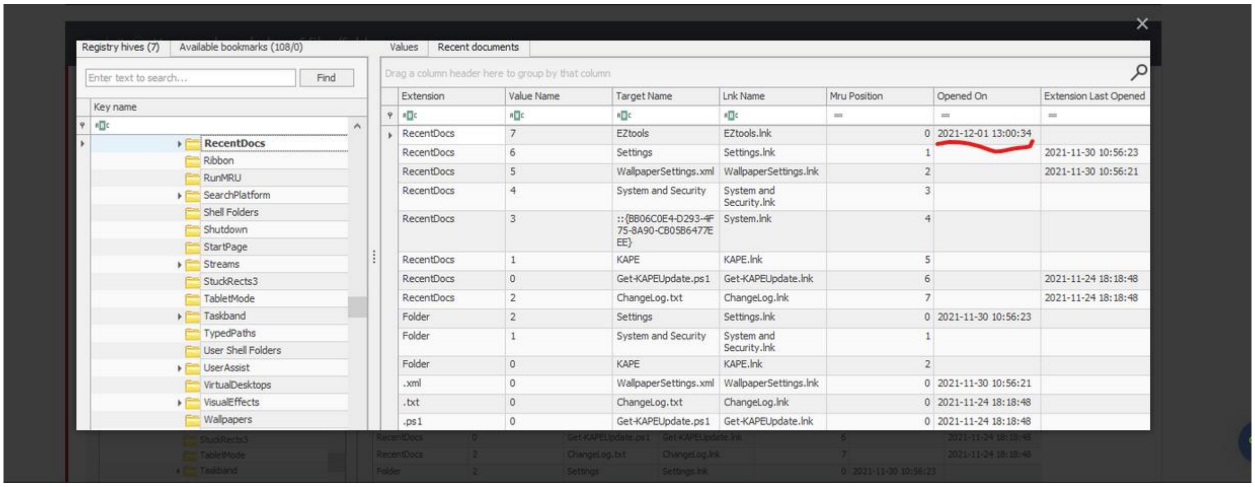
The information contained here includes the relative identifier (RID) of the user, number of times the user logged in, last login time, last failed login, last

Task 7: Usage or Knowledge of Files/Folders

- The Windows operating system maintains a list of recently opened files for each user.
- The SYSTEM hive contains the system's configuration data required for controlling system startup.
- Various registry keys are available to extract information about recently opened files and USB devices.

When was EZtools last accessed?

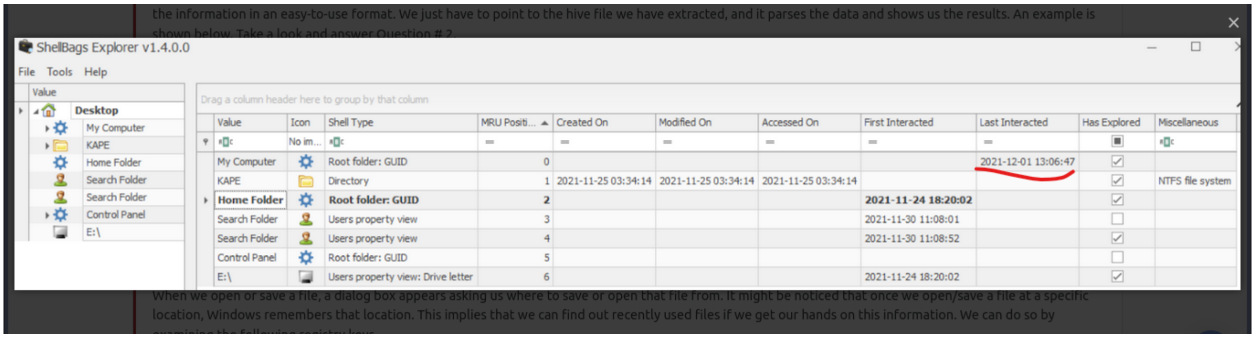
- **EZtools was last accessed on 2021-12-01 at 13:00:34.**



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-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	

When was My Computer last interacted with?

- **My computer was last interacted with on 2021-12-01 at 13:06:47.**

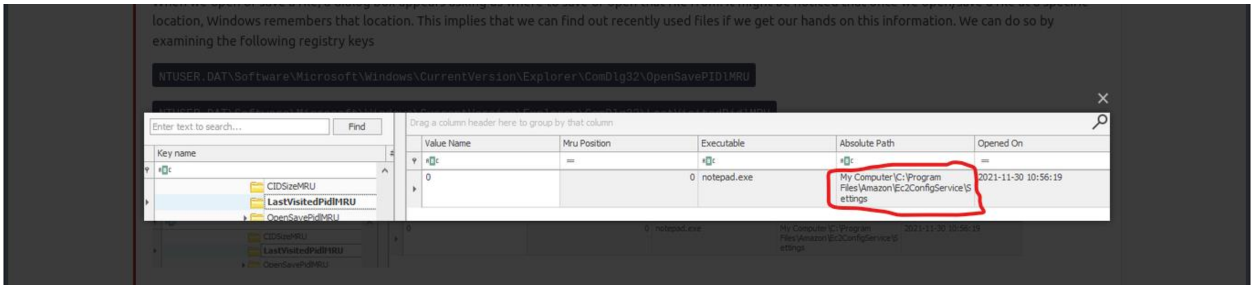

the information in an easy-to-use format. We just have to point to the hive file we have extracted, and it parses the data and shows us the results. An example is shown below. Take a look and answer Question # 2.

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		☑	

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

What is the absolute path of the file opened using notepad.exe?

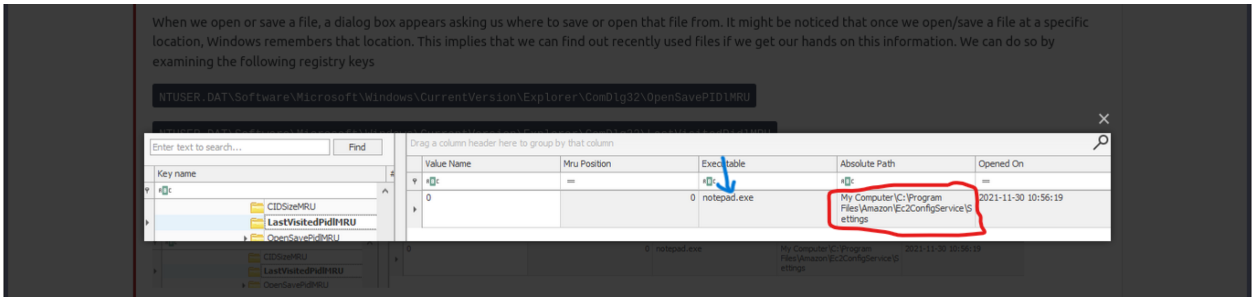
- **Absolute Path: C:\Program Files\Amazon\Ec2ConfigService\Settings**


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
```

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

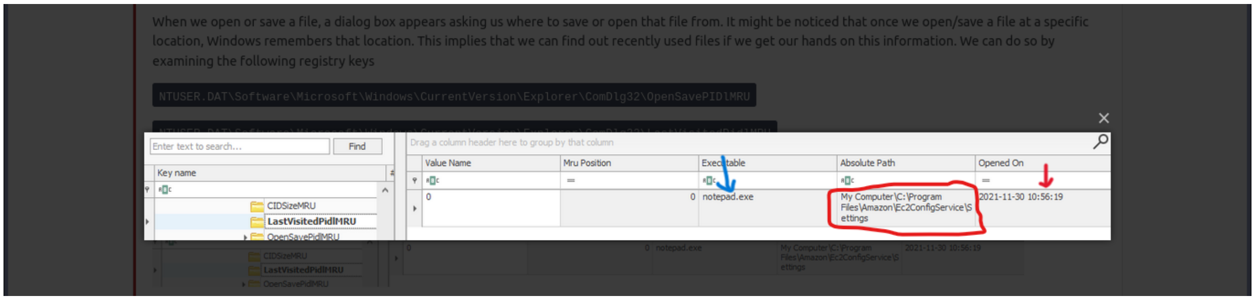
- **File Opened: Using notepad.exe**


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
```

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

- **Access Time: 2021-11-30 at 10:56:19**


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
```

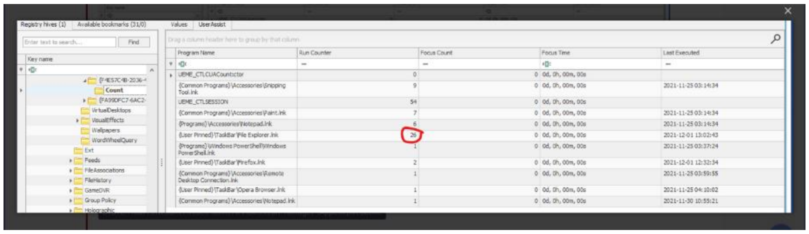
Value Name	Mru Position	Executable	Absolute Path	Opened On
0	0	notepad.exe	My Computer\C:\Program Files\Amazon\Ec2ConfigService\Settings	2021-11-30 10:56:19

Task 8 Evidence of Execution

1. User Assist: Tracks programs launched by users via Windows Explorer.
2. ShimCache: Stores data about all launched applications for OS compatibility.
3. AmCache: Similar to ShimCache, but with additional data like execution paths and SHA1 hashes.
4. BAM/DAM: Monitor background application activity, recording last run programs and execution times.

How many times was File Explorer launched?

- **File Explorer was launched 26 times.**



Registry Hives (1) Available bookmarks (31/0)

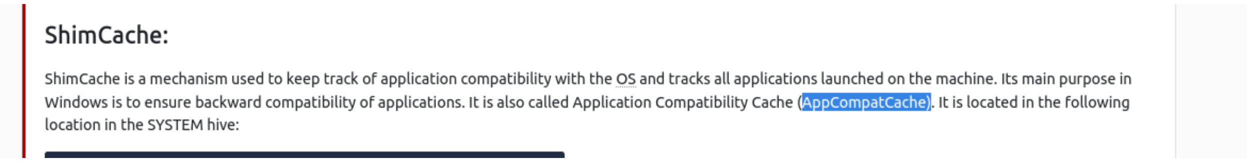
Values UserAssist

Drag a column header here to group by that column

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
UEME_CTLCUACountctor	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?

- **Another name for ShimCache is AppCompatCache**.

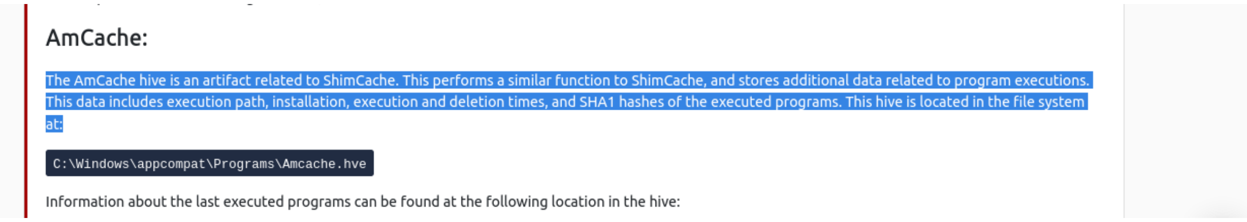


ShimCache:

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 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:

Which artifact also saves SHA1 hashes of the executed programs?

- **The artifact that also saves SHA1 hashes of executed programs is AmCache.**



AmCache:

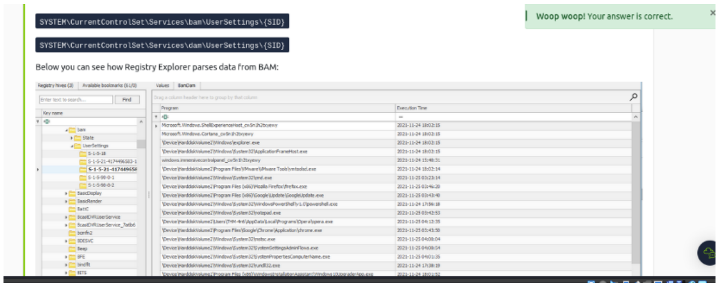
The AmCache hive is an artifact related to ShimCache. This performs a similar function to ShimCache, and stores additional data related to program executions. This data includes execution path, installation, execution and deletion times, and SHA1 hashes of the executed programs. This hive is located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

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

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

Which artifact saves the full path of executed programs?

- **BAM/DAM saves the full path of executed programs**.



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

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

Woop woop! Your answer is correct.

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

Registry hives (2) Available bookmarks (61/0)

Values BamDam

Drag a column header here to group by that column

Program	Execution Time
Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy	2021-11-24 18:02:15
Microsoft.Windows.Cortana_cw5n1h2txyewy	2021-11-24 18:02:15
\Device\HarddiskVolume2\Windows\explorer.exe	2021-11-24 18:02:15
\Device\HarddiskVolume2\Windows\System32\ApplicationFrameHost.exe	2021-11-24 18:02:15
windows.immersivecontrolpanel_cw5n1h2txyewy	2021-11-24 15:40:31
\Device\HarddiskVolume2\Program Files\VMware\VMware Tools\vmtoolsd.exe	2021-11-24 18:02:14
\Device\HarddiskVolume2\Windows\System32\cmd.exe	2021-11-25 03:23:14
\Device\HarddiskVolume2\Program Files (x86)\Mozilla Firefox\firefox.exe	2021-11-25 03:46:20
\Device\HarddiskVolume2\Program Files (x86)\Google\Update\GoogleUpdate.exe	2021-11-25 03:43:40
\Device\HarddiskVolume2\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	2021-11-24 17:56:18
\Device\HarddiskVolume2\Windows\System32\notepad.exe	2021-11-25 03:42:53
\Device\HarddiskVolume2\Users\THM-4n6\AppData\Local\Programs\Opera\opera.exe	2021-11-25 04:12:35
\Device\HarddiskVolume2\Program Files\Google\Chrome\Application\chrome.exe	2021-11-25 03:43:50
\Device\HarddiskVolume2\Windows\System32\mstsc.exe	2021-11-25 04:00:04
\Device\HarddiskVolume2\Windows\System32\SystemSettingsAdminFlows.exe	2021-11-25 04:00:54
\Device\HarddiskVolume2\Windows\System32\SystemPropertiesComputerName.exe	2021-11-25 04:01:35
\Device\HarddiskVolume2\Windows\System32\rundll32.exe	2021-11-24 17:38:19
\Device\HarddiskVolume2\Program Files (x86)\WindowsInstallationAssistant\Windows10UpgraderApp.exe	2021-11-24 18:01:52

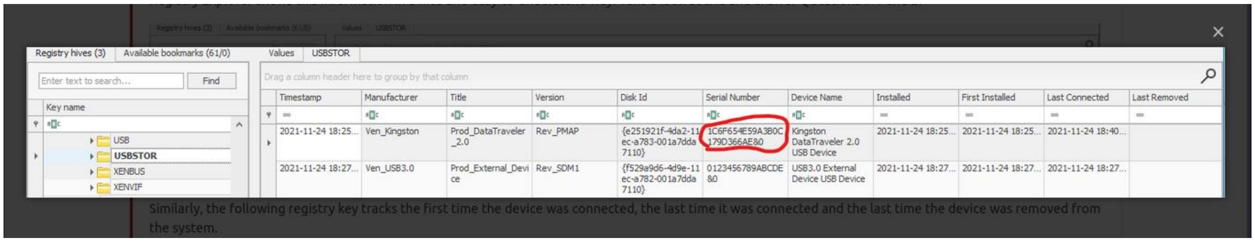
Task 9: External Devices/USB Device Forensics

- Windows maintains various registry keys to extract information about connected devices.
- The USBSTOR key in the SYSTEM hive can be used to extract information about USB devices.

SYSTEM\CurrentControlSet\Enum\USBSTOR	Stores information about the USB devices plugged into a system. The key contains subkeys for each USB device, which can be used to identify unique devices.
SYSTEM\CurrentControlSet\Enum\USB	Stores information about the USB controllers on the system. The key contains subkeys for each USB

	controller, which can be used to identify the device and its settings.
SOFTWARE\Microsoft\Windows	Portable Devices\Devices Stores information about the external devices connected to the system. The key contains subkeys for each device, which can be used to identify the device and its properties.

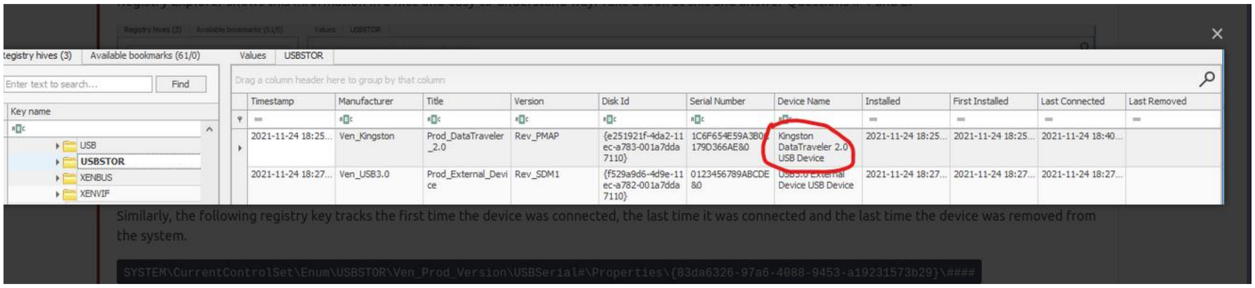
1. What is the serial number of the device from the manufacturer 'Kingston'?
   - **Serial Number: 1C6f654E59A3B0C179D366AE&0**



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...	

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.

2. What is the name of this device?
   - **Device Name: Kingston Data Traveler 2.0 USB Device**

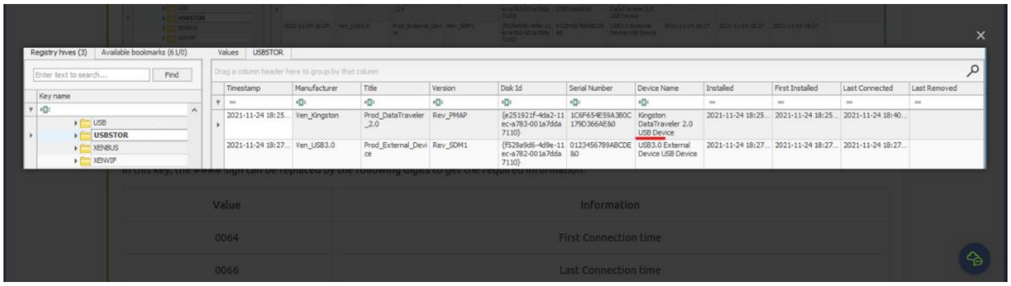


Timestamp	Manufacturer	Title	Version	Disk Id	Serial Number	Device Name	Installed	First Installed	Last Connected	Last Removed
2021-11-24 18:25...	Ven_Kingston	Prod_DataTraveler _2.0	Rev_PMAP	{e251921f-4da2-11ec-a783-001a7dda7110}	1C6F654E59A3B0C179D366AE&0	Kingston DataTraveler 2.0 USB Device	2021-11-24 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...	

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}\####
```

3. What is the friendly name of the device from the manufacturer 'Kingston'?
   - **Friendly Name: USB**

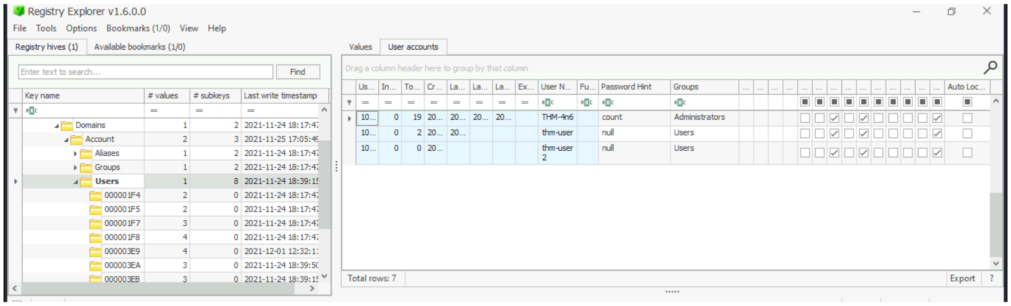


Timestamp	Manufacturer	Title	Version	Disk Id	Serial Number	Device Name	Installed	First Installed	Last Connected	Last Removed
2021-11-24 18:25...	Ven_Kingston	Prod_DataTraveler _2.0	Rev_PMAP	{e251921f-4da2-11ec-a783-001a7dda7110}	1C6F654E59A3B0C179D366AE&0	Kingston DataTraveler 2.0 USB Device	2021-11-24 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...	

Value	Information
0064	First Connection time
0066	Last Connection time

Task 10: Hands-on Challenge

1. How many user-created accounts are present on the system?
   - **There are 3 user-created accounts on the system.**

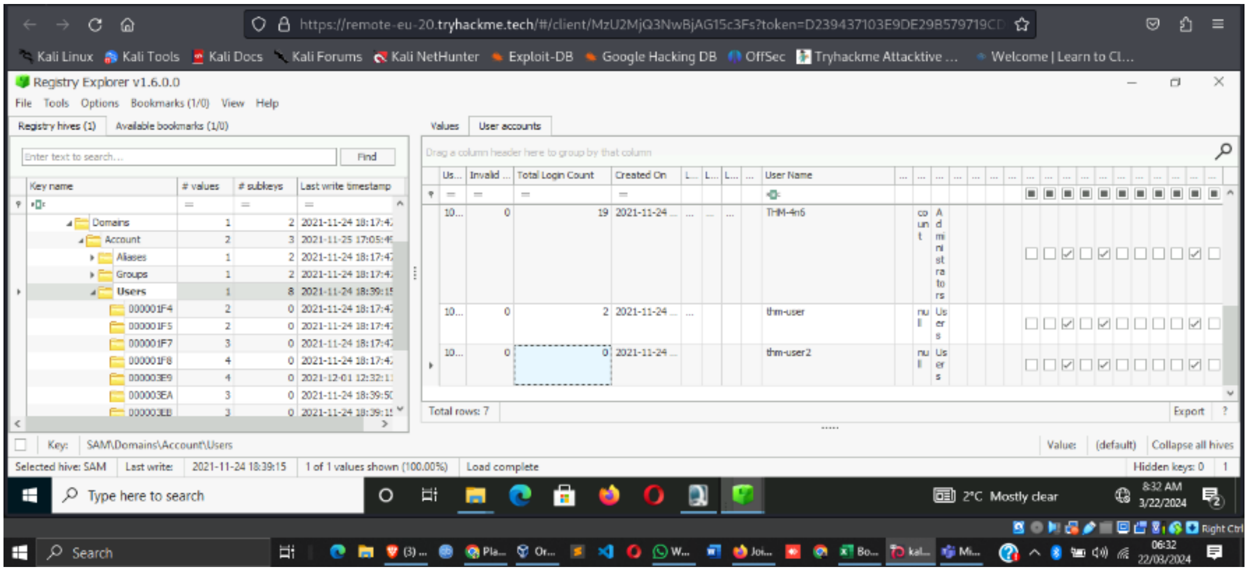


Key name	# values	# subkeys	Last write timestamp
Domains	1	2	2021-11-24 18:17:47
Account	2	3	2021-11-25 17:05:49
Aliases	1	2	2021-11-24 18:17:47
Groups	1	2	2021-11-24 18:17:47
Users	1	8	2021-11-24 18:39:15
000001F4	2	0	2021-11-24 18:17:47
000001F5	2	0	2021-11-24 18:17:47
000001F7	3	0	2021-11-24 18:17:47
000001F8	4	0	2021-11-24 18:17:47
000003E9	4	0	2021-12-01 12:32:11
000003EA	3	0	2021-11-24 18:39:50
000003EB	3	0	2021-11-24 18:39:15

Us...	In...	To...	Cr...	La...	La...	La...	Ex...	User N...	Fu...	Password Hint	Groups	...	...	...	...	...	...	...	...	...	...	...	...	...	...	Auto Loc...
10...	0	19	20...	20...	20...	20...		THM-4n6		count	Administrators					☐	☐	☑	☐	☑	☐	☐	☐	☐	☑	☐
10...	0	2	20...	20...				thm-user		null	Users					☐	☐	☑	☐	☑	☐	☐	☐	☐	☑	☐
10...	0	0	20...					thm-user2		null	Users					☐	☐	☑	☐	☑	☐	☐	☐	☐	☑	☐

Total rows: 7

2. What is the username of the account that has never been logged in?
   - **The username of the account that has never been logged in is 'thm-user2'.**



Key name	# values	# subkeys	Last write timestamp
Domains	1	2	2021-11-24 18:17:4:
Account	2	3	2021-11-25 17:05:4!
Aliases	1	2	2021-11-24 18:17:4:
Groups	1	2	2021-11-24 18:17:4:
Users	1	8	2021-11-24 18:39:1!
000001F4	2	0	2021-11-24 18:17:4:
000001F5	2	0	2021-11-24 18:17:4:
000001F7	3	0	2021-11-24 18:17:4:
000001F8	4	0	2021-11-24 18:17:4:
000003E9	4	0	2021-12-01 12:32:1:
000003EA	3	0	2021-11-24 18:39:5(
000003EB	3	0	2021-11-24 18:39:1!

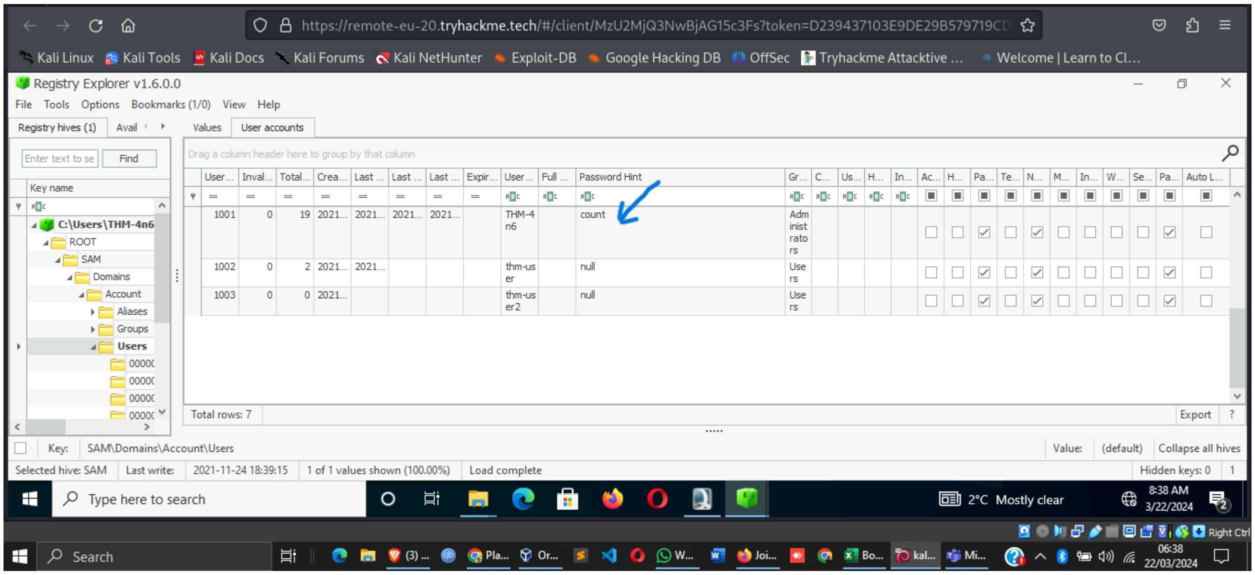
Us...	Invalid ...	Total Login Count	Created On	L...	L...	L...	...	User Name	...	...	...	...	...	...	...	...	...	...	...	...	...
10...	0	19	2021-11-24 ...	...	...	...		THM-4n6	count	Administrators	□	□	☑	□	☑	□	□	□	□	☑	□
10...	0	2	2021-11-24 ...	...				thm-user	null	Users	□	□	☑	□	☑	□	□	□	□	☑	□
10...	0	0	2021-11-24 ...					thm-user2	null	Users	□	□	☑	□	☑	□	□	□	□	☑	□

Total rows: 7

Key: SAM\Domains\Account\Users

Selected hive: SAM | Last write: 2021-11-24 18:39:15 | 1 of 1 values shown (100.00%) | Load complete

3. What's the password hint for the user THM-4n6?
    - **Password Hint: count**



Key name
C:\Users\THM-4n6
ROOT
SAM
Domains
Account
Aliases
Groups
Users
0000(
0000(
0000(
0000(

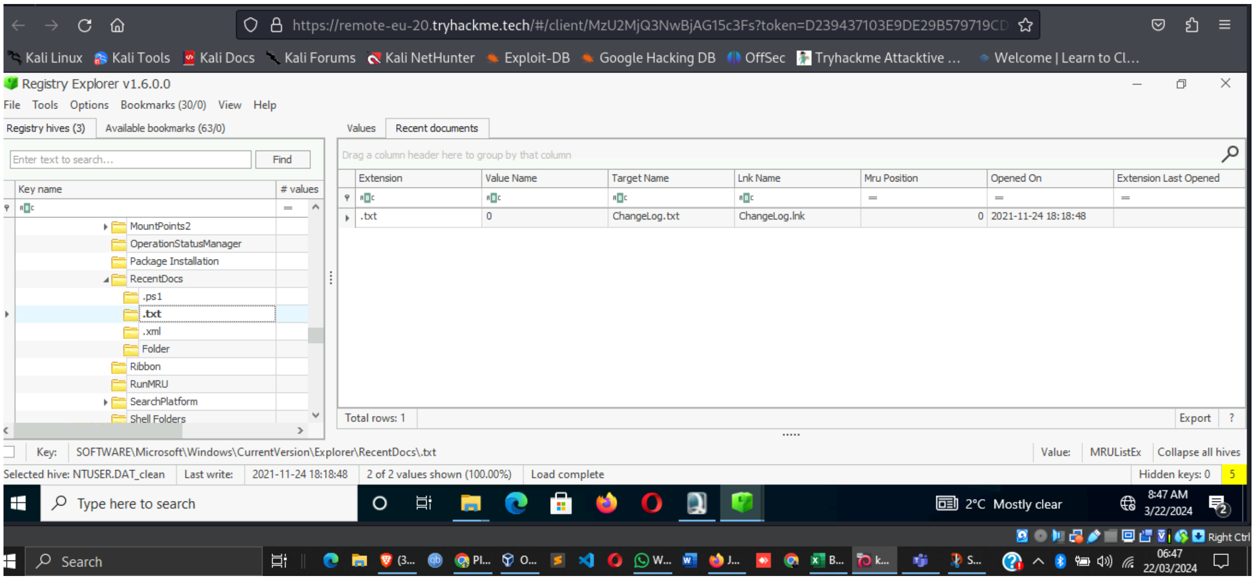
User...	Inval...	Total...	Crea...	Last ...	Last ...	Last ...	Expir...	User...	Full ...	Password Hint	Gr...	C...	Us...	H...	In...	Ac...	H...	Pa...	Te...	N...	M...	In...	W...	Se...	Pa...	Auto L...
1001	0	19	2021...	2021...	2021...	2021...		THM-4n6		count	Administrators					□	□	☑	□	☑	□	□	□	□	☑	□
1002	0	2	2021...	2021...				thm-user		null	Users					□	□	☑	□	☑	□	□	□	□	☑	□
1003	0	0	2021...					thm-user2		null	Users					□	□	☑	□	☑	□	□	□	□	☑	□

Total rows: 7

Key: SAM\Domains\Account\Users

Selected hive: SAM | Last write: 2021-11-24 18:39:15 | 1 of 1 values shown (100.00%) | Load complete

4. When was the file 'Changelog.txt' accessed?
    - **The file 'Changelog.txt' was accessed on 2021-11-21 at 18:18:48.**



Key name	# values
MountPoints2	
OperationStatusManager	
Package Installation	
RecentDocs	
.ps1	
.txt	
.xml	
Folder	
Ribbon	
RunMRU	
SearchPlatform	
Shell Folders	

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
.txt	0	ChangeLog.txt	ChangeLog.lnk	0	2021-11-24 18:18:48	

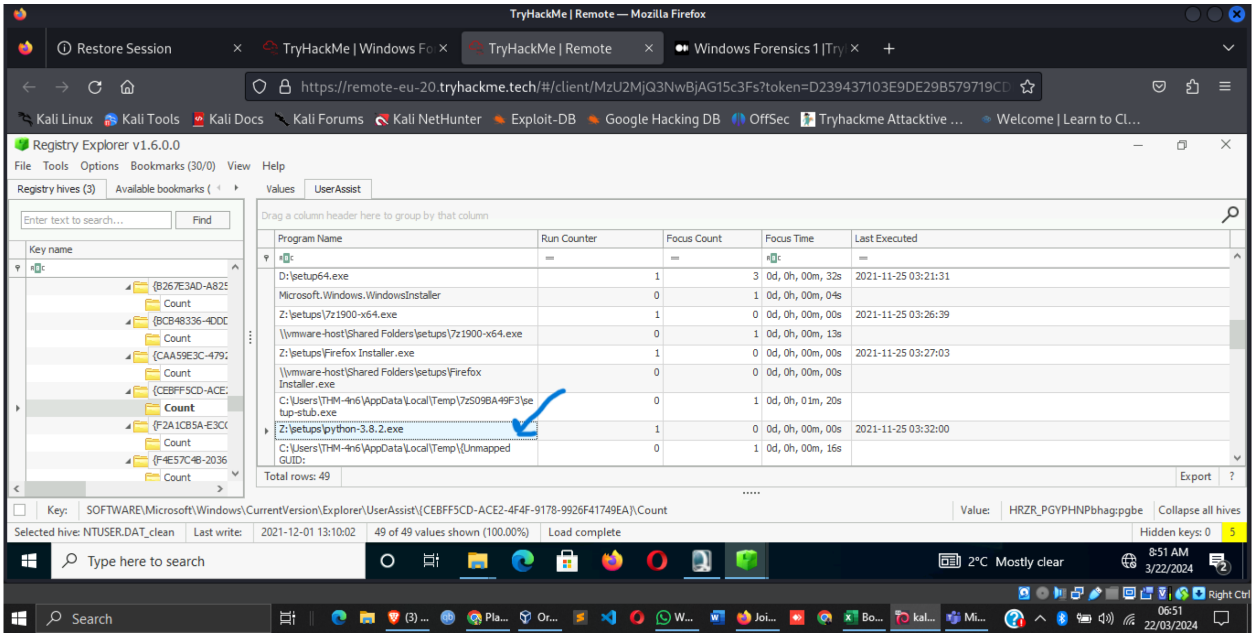
Total rows: 1

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

Value: MRUListEx

Selected hive: NTUSER.DAT_clean | Last write: 2021-11-24 18:18:48 | 2 of 2 values shown (100.00%) | Load complete

5. What is the complete path from where the Python 3.8.2 installer was run?
    - **Complete Path: Z:\setups\python-3.8.2.exe**



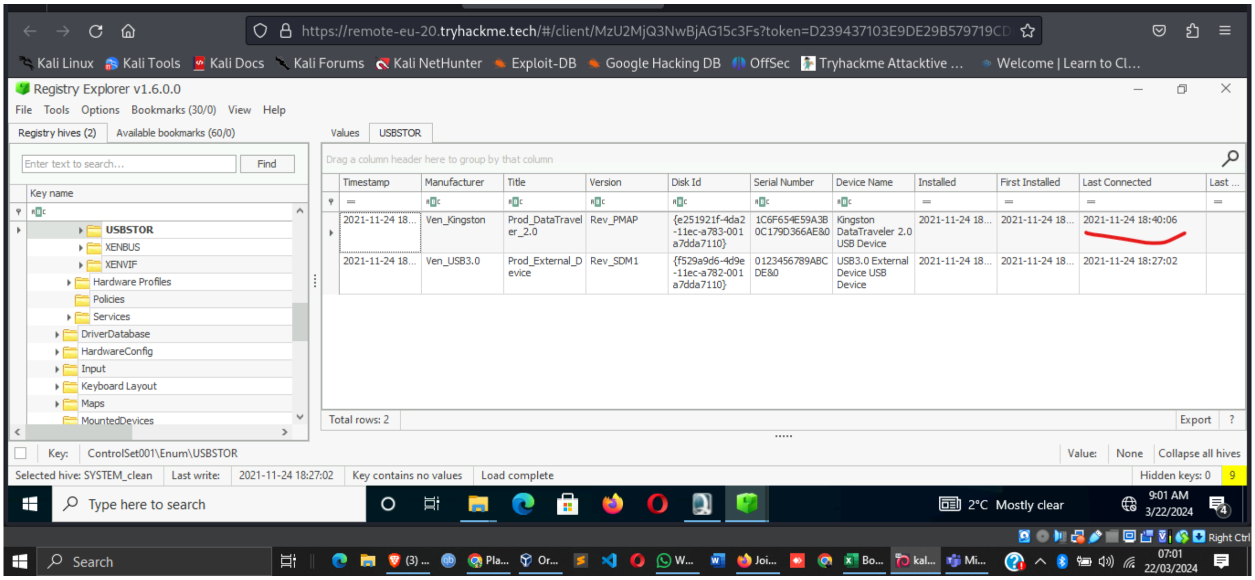
Program Name	Run Counter	Focus Count	Focus Time	Last Executed
D:\setup64.exe	1	3	0d, 0h, 00m, 32s	2021-11-25 03:21:31
Microsoft.Windows.WindowsInstaller	0	1	0d, 0h, 00m, 04s	
Z:\setups\7z1900-x64.exe	1	0	0d, 0h, 00m, 00s	2021-11-25 03:26:39
\\vmware-host\Shared Folders\setups\7z1900-x64.exe	0	1	0d, 0h, 00m, 13s	
Z:\setups\Firefox Installer.exe	1	0	0d, 0h, 00m, 00s	2021-11-25 03:27:03
\\vmware-host\Shared Folders\setups\Firefox Installer.exe	0	0	0d, 0h, 00m, 00s	
C:\Users\THM-4n6\AppData\Local\Temp\7zS09BA49F3\setup-stub.exe	0	1	0d, 0h, 01m, 20s	
Z:\setups\python-3.8.2.exe	1	0	0d, 0h, 00m, 00s	2021-11-25 03:32:00
C:\Users\THM-4n6\AppData\Local\Temp\{Unmapped GUID:	0	1	0d, 0h, 00m, 16s	

Total rows: 49

Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count Value: HRZR_PGYPHNPbhag:pgbe

Selected hive: NTUSER.DAT_clean Last write: 2021-12-01 13:10:02 49 of 49 values shown (100.00%) Load complete Hidden keys: 0

6. When was the USB device with the friendly name 'USB' last connected?
   - **The USB device with the friendly name 'USB' was last connected on 2021-11-24 at 18:40:06.**



Timestamp	Manufacturer	Title	Version	Disk Id	Serial Number	Device Name	Installed	First Installed	Last Connected	Last ...
2021-11-24 18...	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...	2021-11-24 18...	2021-11-24 18:40:06	
2021-11-24 18...	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...	2021-11-24 18...	2021-11-24 18:27:02	

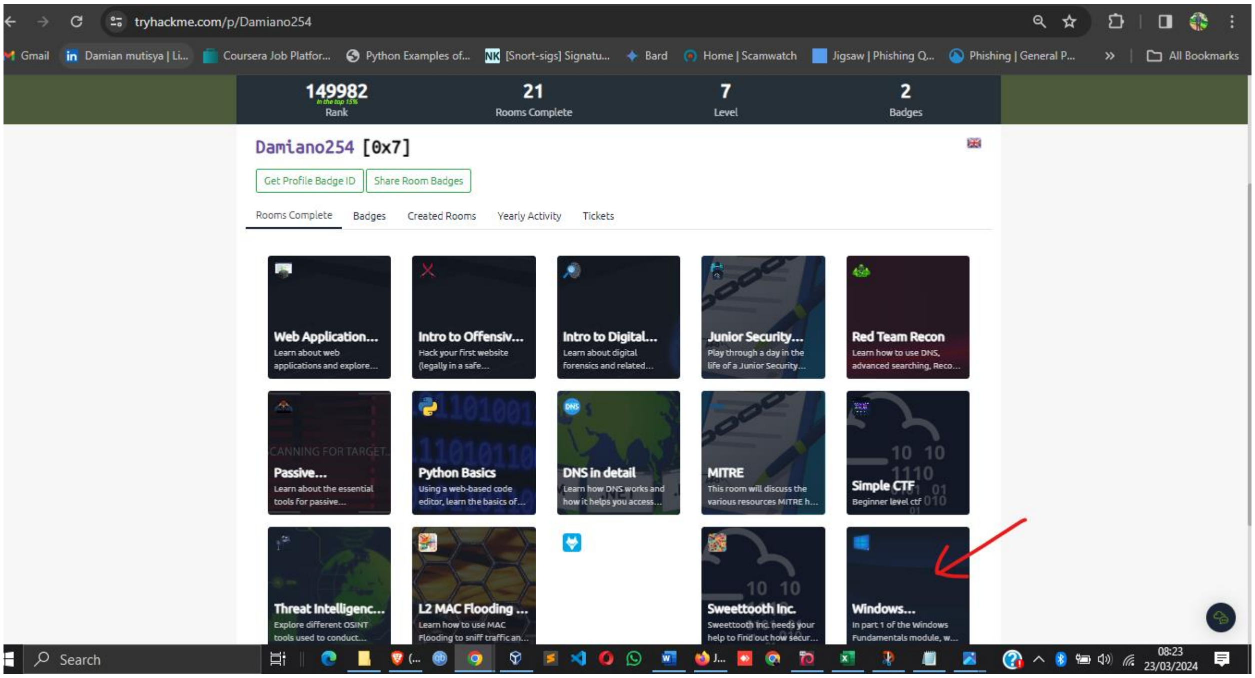
Total rows: 2

Key: ControlSet001\Enum\USBSTOR Value: None

Selected hive: SYSTEM_clean Last write: 2021-11-24 18:27:02 Key contains no values Load complete Hidden keys: 0

Conclusion:

In conclusion, understanding the Windows registry and its importance in forensic investigations is crucial for digital forensic experts. The Windows Forensics 1 room has provided an insightful examination of Windows registry forensics, covering the structure of the Windows registry, accessing registry hives offline, system and user account information, and registry analysis. By understanding the concepts discussed, investigators can extract valuable information from Windows-based systems to aid in their investigations**.**



149982
in the top 15%
Rank

21
Rooms Complete

7
Level

2
Badges

Damiano254 [0x7]

Get Profile Badge ID

Share Room Badges

Web Application...
Learn about web applications and explore...

Intro to Offensiv...
Hack your first website (legally in a safe...

Intro to Digital...
Learn about digital forensics and related...

Junior Security...
Play through a day in the life of a Junior Security...

Red Team Recon
Learn how to use DNS, advanced searching, Reco...

Passive...
Learn about the essential tools for passive...

Python Basics
Using a web-based code editor, learn the basics of...

DNS in detail
Learn how DNS works and how it helps you access...

MITRE
This room will discuss the various resources MITRE h...

Simple CTF
Beginner level ctf

Threat Intelligenc...
Explore different OSINT tools used to conduct...

L2 MAC Flooding ...
Learn how to use MAC Flooding to sniff traffic an...

Sweettooth Inc.
Sweettooth Inc. needs your help to find out how secur...

Windows...
In part 1 of the Windows Fundamentals module, w...