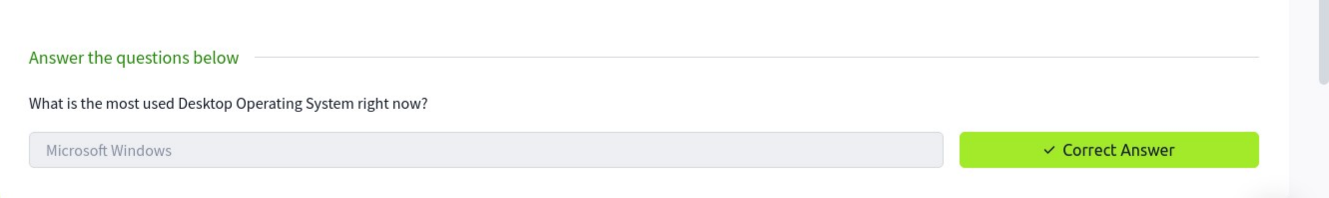
ISSACK WAITHAKA
cs-sa07-24085

Introduction to computer forensics for windows

- Forensics involves gathering evidence of activities performed on a computer.
- Forensic artifacts are essential pieces of information that provide evidence of human activity
- Windows saves your activities to make the computer more personalized

Questions

1.



Answer the questions below

What is the most used Desktop Operating System right now?

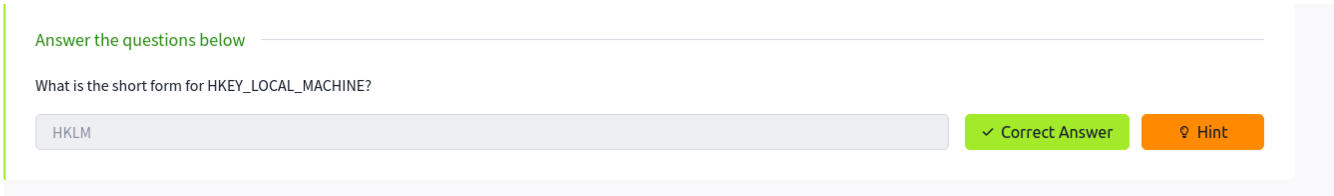
Microsoft Windows

Windows Registry and Forensics

- Windows registry is a collection of databases that contains the system’s configuration data, which could be about the hardware, software or data about recent used files.
- Windows Registry consists of keys and values.
- Windows Registry has five root keys which include:
  - HKEY_CURRENT_USER -
  - HKEY_USERS
  - HKEY_LOCAL_MACHINE
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_CONFIG
- We can find these keys on regedit.exe

Questions

1.



Answer the questions below

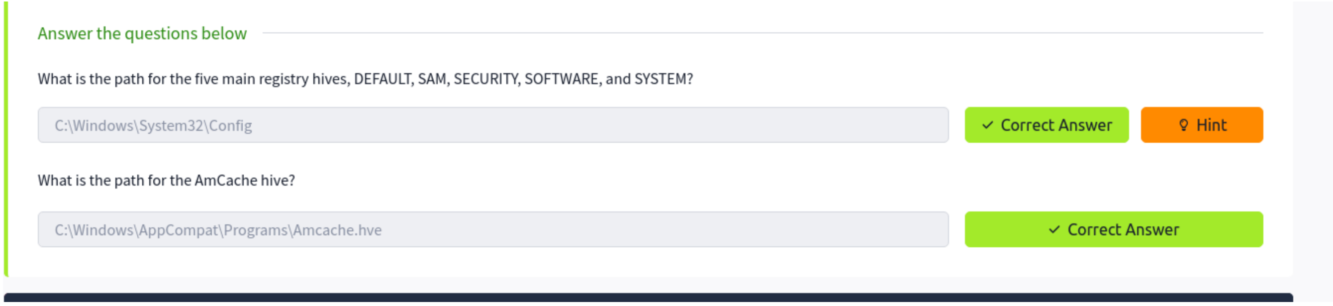
What is the short form for HKEY_LOCAL_MACHINE?

HKLM

Accessing registry hives offline

- Majority of hives are located in c:\windows\System32\Config\……
- There is also another two hives containing user information that can be found in user profile directory.
- The transaction log is also a vital source of forensic data. It can be considered as the journal of the changelog of the registry hive.
- They are stored as a .LOG file and are located in c:windows\system32\config

Questions



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

- Acquisition involves making a copy of required data or use the image of the system and perform forensics on it.
- KAPE is a live data acquisition tool that which can be used to acquire registry data.
- Autopsy allows us to either acquire data from live systems or from disk image.
- FTK imager works like autopsy but this allows us to mount the disk image or drive in FTK imager

Exploring Windows Registry

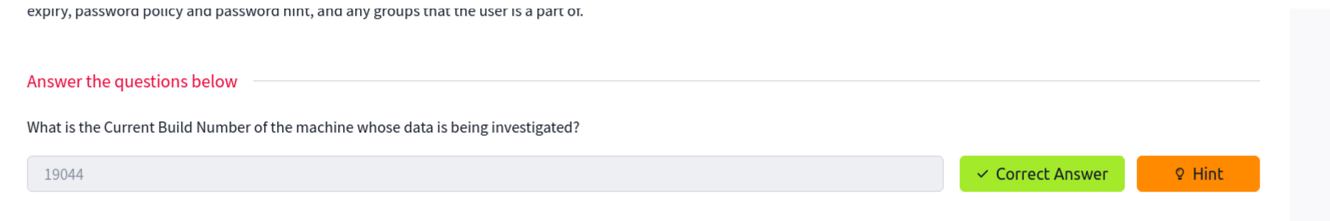
- Registry viewer loads one hive at a time
- Registry explorer, can load multiple hive simultaneously and add data from transaction logs into the hive.
- RegRipper a tool that takes registry as input and output report that extracts data from some of the important keys.

System information and System Account

- We can find the OS version from the data that was pulled through Software\Microsoft\windows NT\currentVersion
- Current Control sets are hives containing machines configuration data used for controlling system startup
- location is system\controlset...
- Current control is set when machine is live.
- We can find the computer name from
  SYSTEM\CurrentControlSet\Control\ComputerName\computerName
- To find the time zone location
  SYSTEM\CurrentControlSet\Control\TimeZoneInformation
- To find network Interface
  SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
- Information about services are found inSYSTEM\CurrentControlSet\Service

Questions

1.

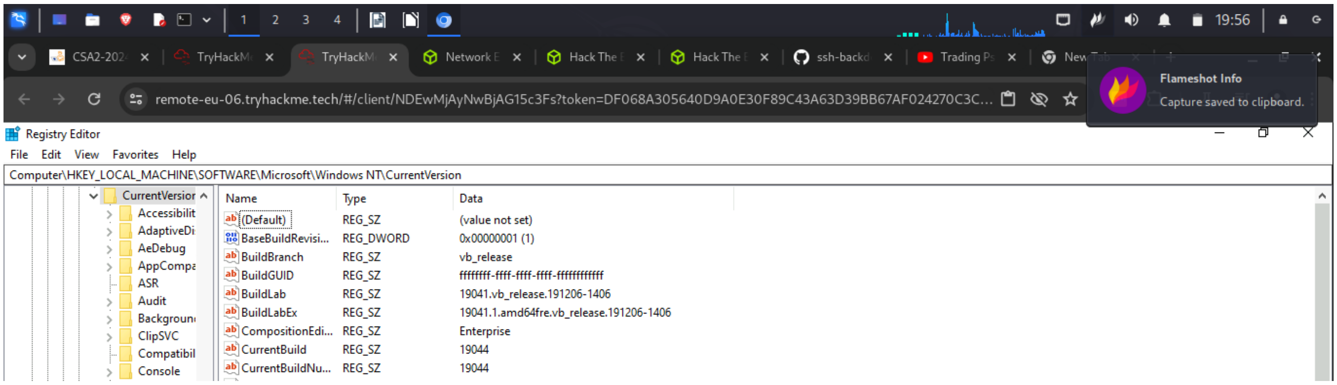


expiry, password policy and password hint, and any groups that the user is a part of.

Answer the questions below

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

19044



remote-eu-06.tryhackme.tech/#/client/NDEwMjAyNwBjAG15c3Fs?token=DF068A305640D9A0E30F89C43A63D39BB67AF024270C3C...

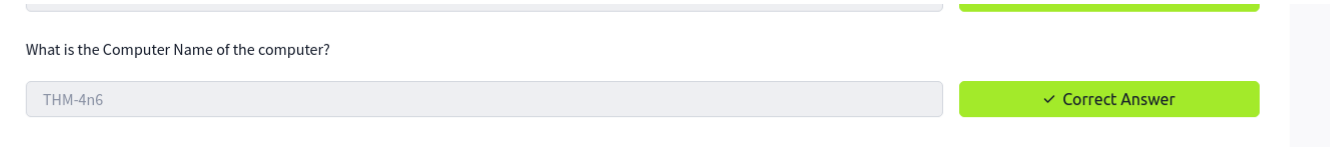
Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

Name	Type	Data
(Default)	REG_SZ	(value not set)
BaseBuildRevisi...	REG_DWORD	0x00000001 (1)
BuildBranch	REG_SZ	vb_release
BuildGUID	REG_SZ	ffffffff-ffff-ffff-ffff-ffffffffffff
BuildLab	REG_SZ	19041.vb_release.191206-1406
BuildLabEx	REG_SZ	19041.1.amd64fre.vb_release.191206-1406
CompositionEdi...	REG_SZ	Enterprise
CurrentBuild	REG_SZ	19044
CurrentBuildNu...	REG_SZ	19044

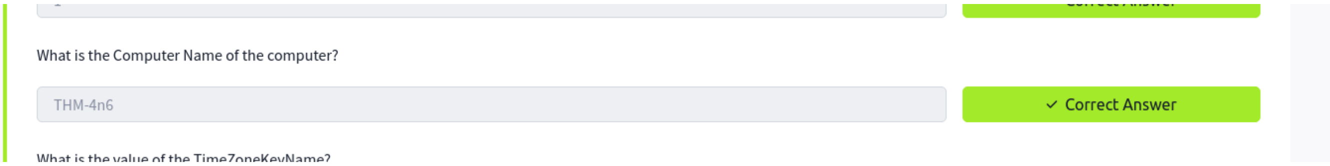
2.



What is the Computer Name of the computer?

THM-4n6

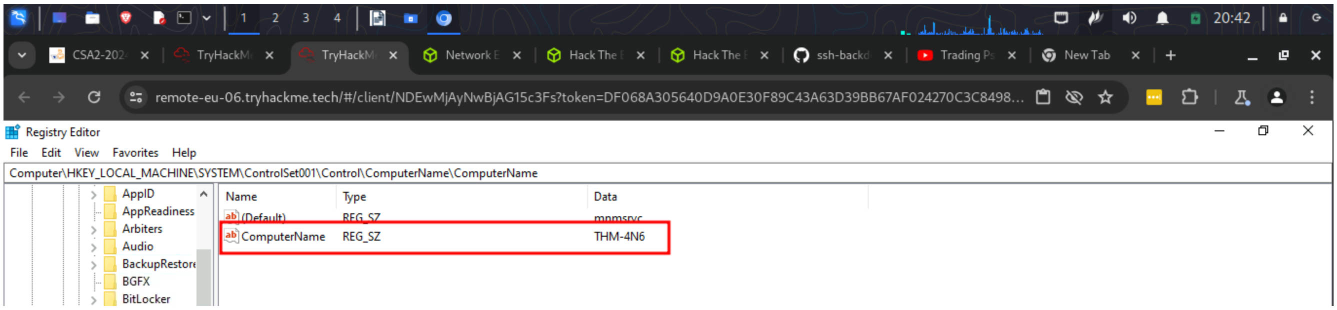
3.



What is the Computer Name of the computer?

THM-4n6

What is the value of the TimeZoneKeyName?



remote-eu-06.tryhackme.tech/#/client/NDEwMjAyNwBjAG15c3Fs?token=DF068A305640D9A0E30F89C43A63D39BB67AF024270C3C8498...

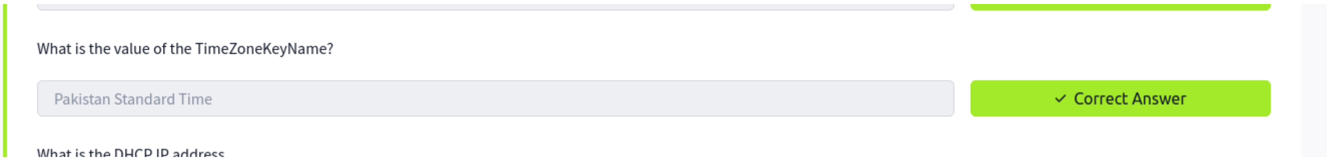
Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ComputerName

Name	Type	Data
(Default)	REG_SZ	mnmsrvc
ComputerName	REG_SZ	THM-4N6

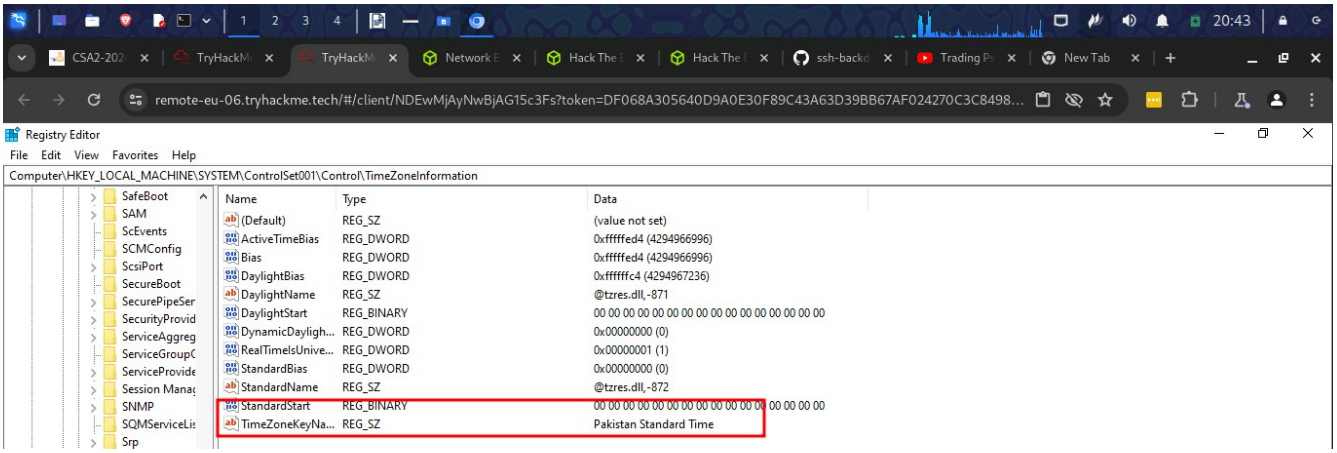
4.



What is the value of the TimeZoneKeyName?

Pakistan Standard Time

What is the DHCP IP address



remote-eu-06.tryhackme.tech/#/client/NDEwMjAyNwBjAG15c3Fs?token=DF068A305640D9A0E30F89C43A63D39BB67AF024270C3C8498...

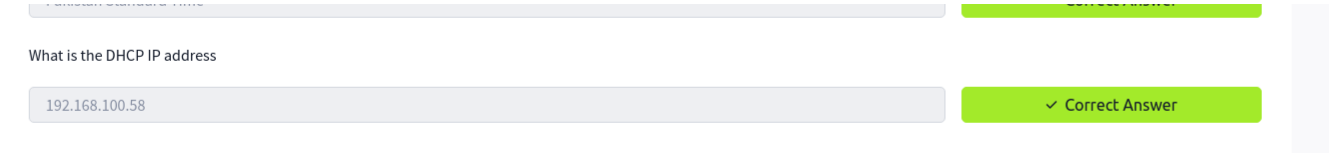
Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\TimeZoneInformation

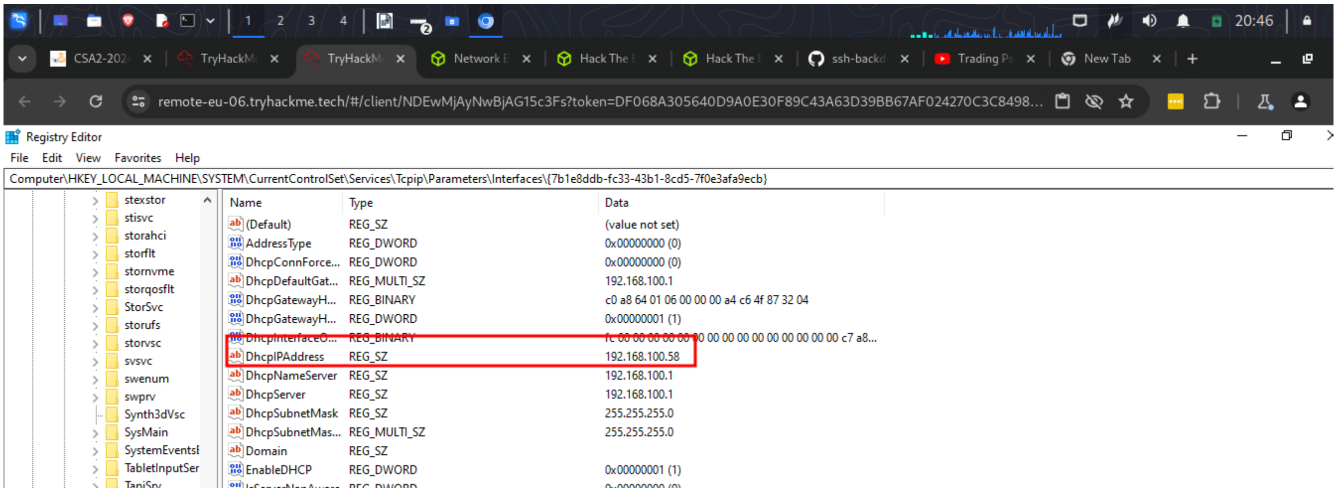
Name	Type	Data
(Default)	REG_SZ	(value not set)
ActiveTimeBias	REG_DWORD	0xfffffed4 (4294966996)
Bias	REG_DWORD	0xfffffed4 (4294966996)
DaylightBias	REG_DWORD	0xffffffc4 (4294967236)
DaylightName	REG_SZ	@tzres.dll,-871
DaylightStart	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
DynamicDayligh...	REG_DWORD	0x00000000 (0)
RealTimeIsUnive...	REG_DWORD	0x00000001 (1)
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-872
StandardStart	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
TimeZoneKeyNa...	REG_SZ	Pakistan Standard Time

5.



What is the DHCP IP address

192.168.100.58

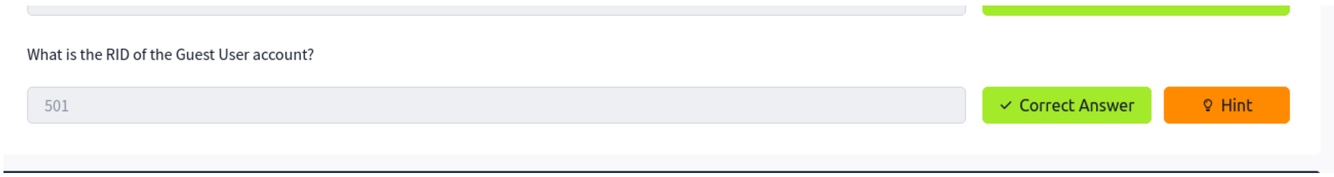


Registry Editor

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{7b1e8ddb-fc33-43b1-8cd5-7f0e3afa9ecb}

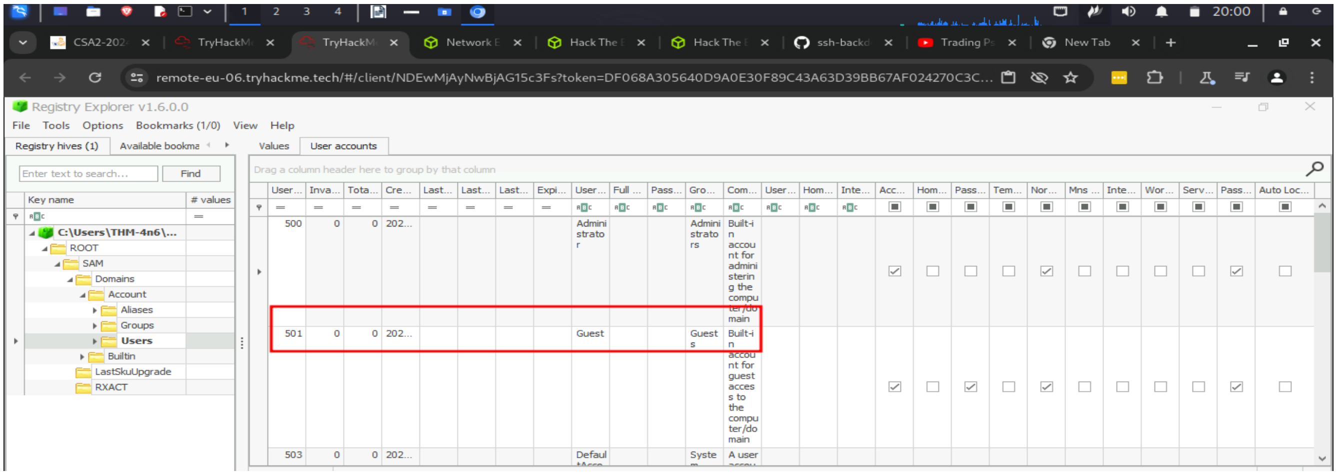
Name	Type	Data
(Default)	REG_SZ	(value not set)
AddressType	REG_DWORD	0x00000000 (0)
DhcpConnForce...	REG_DWORD	0x00000000 (0)
DhcpDefaultGat...	REG_MULTI_SZ	192.168.100.1
DhcpGatewayH...	REG_BINARY	c0 a8 64 01 06 00 00 00 a4 c6 4f 87 32 04
DhcpGatewayH...	REG_DWORD	0x00000001 (1)
DhcpInterfaceO...	REG_BINARY	fc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c7 a8...
DhcpIPAddress	REG_SZ	192.168.100.58
DhcpNameServer	REG_SZ	192.168.100.1
DhcpServer	REG_SZ	192.168.100.1
DhcpSubnetMask	REG_SZ	255.255.255.0
DhcpSubnetMas...	REG_MULTI_SZ	255.255.255.0
Domain	REG_SZ	
EnableDHCP	REG_DWORD	0x00000001 (1)

6.



What is the RID of the Guest User account?

501



Registry Explorer v1.6.0.0

User...	Inva...	Tota...	Cre...	Last...	Last...	Last...	Expi...	User...	Full ...	Pass...	Gro...	Com...	User...	Hom...	Inte...	Acc...	Hom...	Pass...	Tem...	Nor...	Mns ...	Inte...	Wor...	Serv...	Pass...	Auto Loc...
500	0	0	202...					Administrator			Administrators	Built-in account for administering the computer/domain				☑	□	□	□	☑	□	□	□	□	☑	□
501	0	0	202...					Guest			Guests	Built-in account for guest access to the computer/domain				☑	□	☑	□	☑	□	□	□	□	☑	□
503	0	0	202...					Defaul			Syste	A user														

Usage or knowledge of files/folders

- Registry allows us to sort data contained in registry keys quickly, so recent document tab arranges the most recent used file at the top of the list (mru)

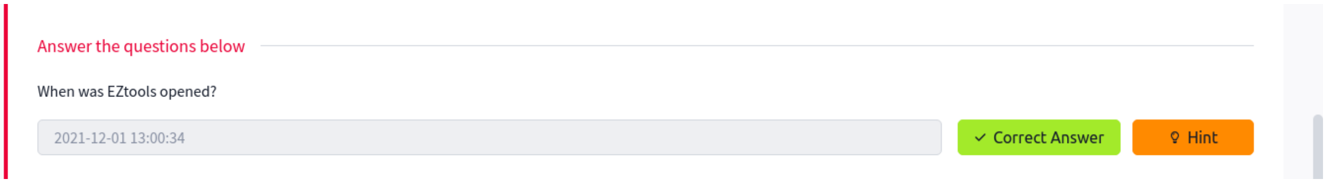
- Windows maintains a list of recently opened files for each user. It is stored in the NTUSER hive.

NTUSER.DAT\Software\microsot\windows\currentVersion\Explorer\RecentDocs

- Registry explorer allows us to sort data contained in registry keys quickly.
- Arranges files such that the most recent file is shown at the top of the list.
- There are extension keys like .pdf, .jpg which provide information about the lst used files of a specific file extension
- Microsoft office also provide list of recent accessed documents.
-

Questions

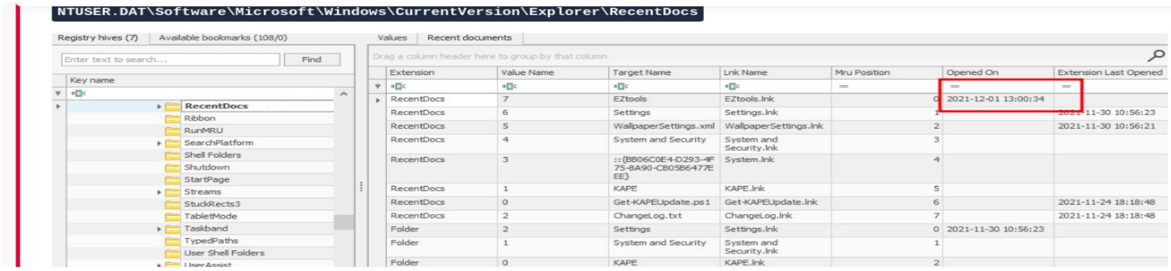
1.



Answer the questions below

When was EZtools opened?

2021-12-01 13:00:34



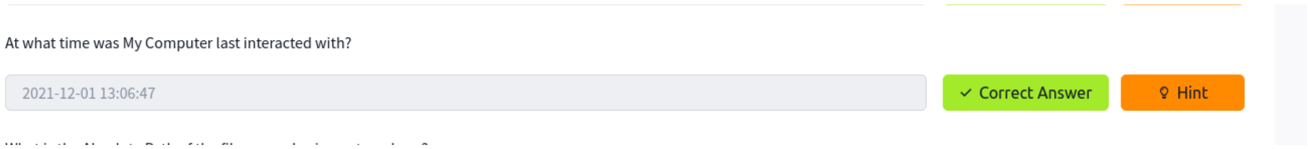
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Registry hives (7)
Available bookmarks (108/0)
Enter text to search...
Find
Key name
Values
Recent documents
Drag a column header here to group by that column

RecentDocs
Ribbon
RunMRU
SearchPlatform
Shell Folders
Shutdown
StartPage
Streams
StuckRects3
TabletMode
Taskband
TypedPaths
User Shell Folders
UserAssist

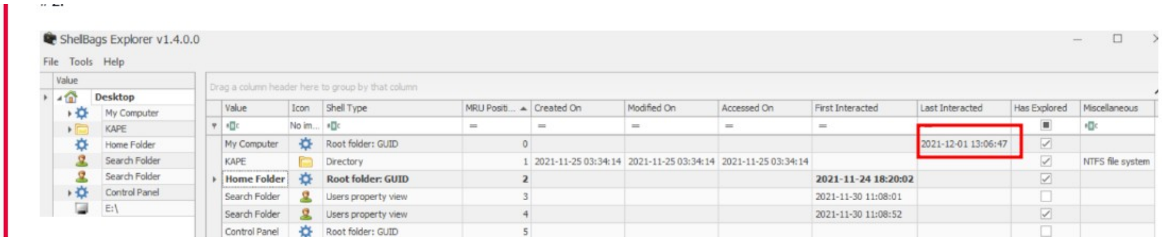
Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
RecentDocs	7	EZtools	EZtools.lnk	0	2021-12-01 13:00:34	
RecentDocs	6	Settings	Settings.lnk	1		2021-11-30 10:56:23
RecentDocs	5	WallpaperSettings.xml	WallpaperSettings.lnk	2		2021-11-30 10:56:21
RecentDocs	4	System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

2.



At what time was My Computer last interacted with?

2021-12-01 13:06:47

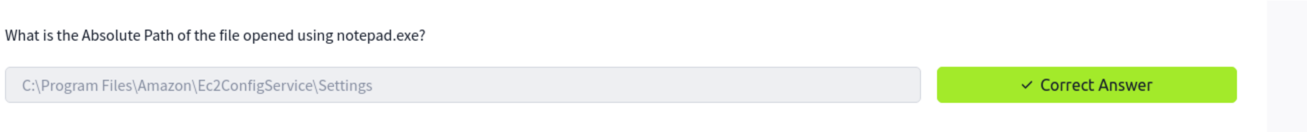


ShellBags Explorer v1.4.0.0
File
Tools
Help
Value
Drag a column header here to group by that column

Desktop
My Computer
KAPE
Home Folder
Search Folder
Search Folder
Control Panel
E:\

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						☐	

3.

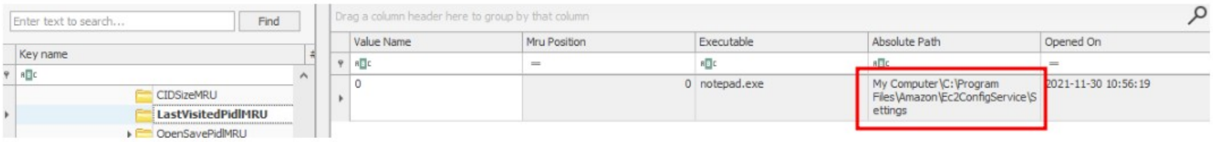


What is the Absolute Path of the file opened using notepad.exe?

C:\Program Files\Amazon\Ec2ConfigService\Settings

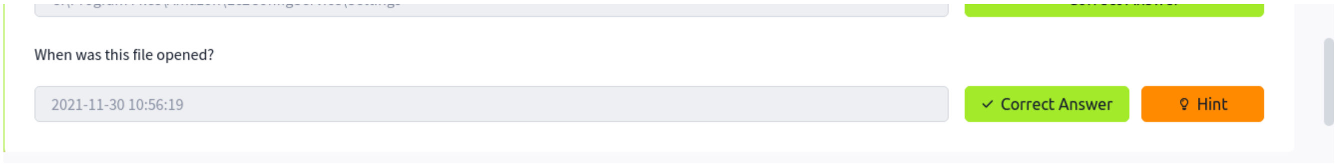
```
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU
```

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



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

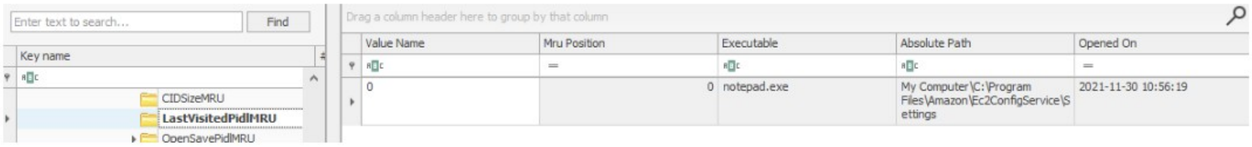
4.



When was this file opened?

2021-11-30 10:56:19

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



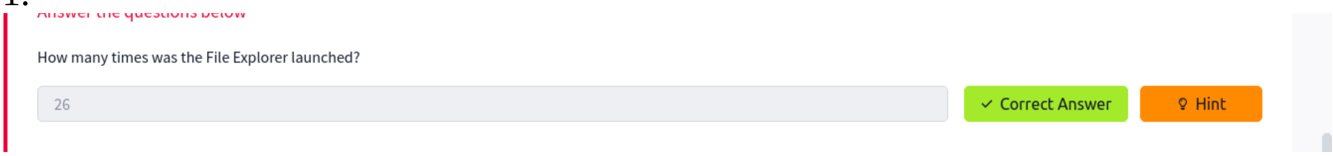
Value Name	Mru Position	Executable	Absolute Path	Opened On
0	0	notepad.exe	My Computer\C:\Program Files\Amazon\Ec2ConfigService\Settings	2021-11-30 10:56:19

Evidence of Execution

- Windows keeps track of applications launched by the user using windows Explorer for statistical purposes in the user Assist registry keys
- ShimCache is a mechanism used to keep track of applications compatibility with OS and track all applications launched on the machine
- AmCache – perform similar functions like ShimCache
- BAM/DAM – Background Activity Monitor keeps a tab on the activity of background applications
- Desktop Activity Moderator is a part of windows that optimizes power consumption

Questions

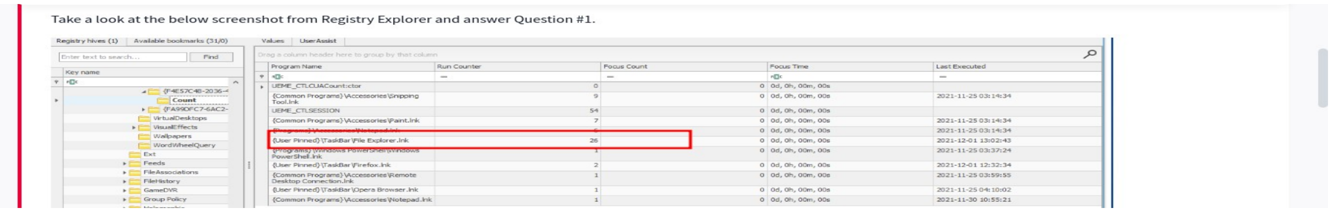
1.



How many times was the File Explorer launched?

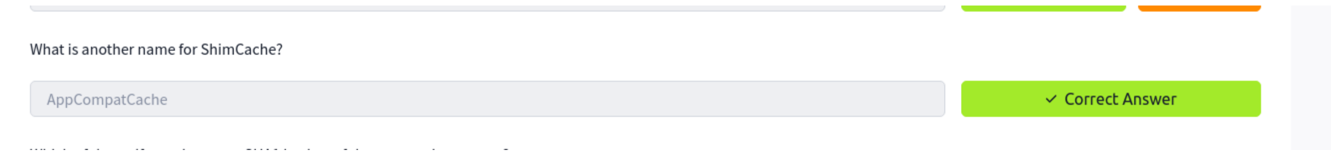
26

Take a look at the below screenshot from Registry Explorer and answer Question #1.



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

2.

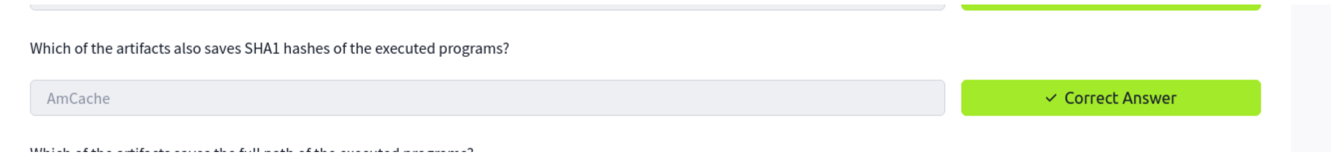


What is another name for ShimCache?

AppCompatCache

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

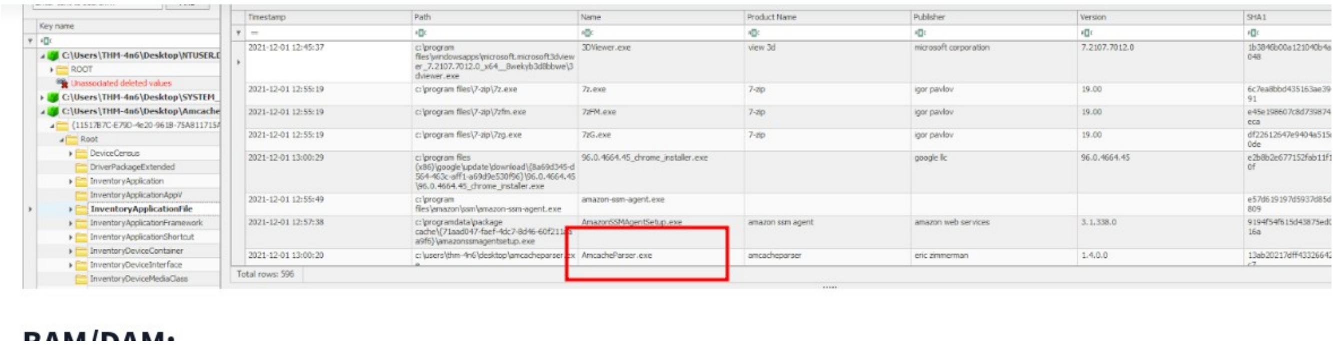
3.



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?



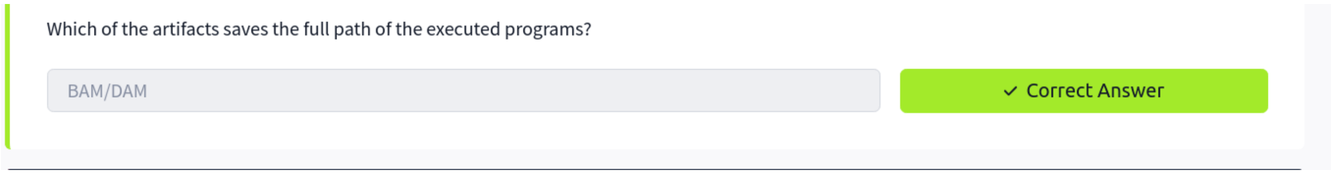
Key name
C:\Users\THM-4n6\Desktop\NTUSER.D
ROOT
Unassociated deleted values
C:\Users\THM-4n6\Desktop\SYSTEM_
C:\Users\THM-4n6\Desktop\Amcache
{11517B7C-E79D-4e20-961B-75A811715A
Root
DeviceCensus
DriverPackageExtended
InventoryApplication
InventoryApplicationAppV
InventoryApplicationFile
InventoryApplicationFramework
InventoryApplicationShortcut
InventoryDeviceContainer
InventoryDeviceInterface
InventoryDeviceMediaClass

Timestamp	Path	Name	Product Name	Publisher	Version	SHA1
2021-12-01 12:45:37	c:\program files\windowsapps\microsoft.microsoft3dviewer_7.2107.7012.0_x64__8wekyb3d8bbwe\3dviewer.exe	3DViewer.exe	view 3d	microsoft corporation	7.2107.7012.0	1b3846b00a121040b4a 048
2021-12-01 12:55:19	c:\program files\7-zip\7z.exe	7z.exe	7-zip	igor pavlov	19.00	6c7ea8bbd435163ae39 91
2021-12-01 12:55:19	c:\program files\7-zip\7zfm.exe	7zFM.exe	7-zip	igor pavlov	19.00	e45e198607c8d739874 eca
2021-12-01 12:55:19	c:\program files\7-zip\7zg.exe	7zG.exe	7-zip	igor pavlov	19.00	df22612647e9404a515 0de
2021-12-01 13:00:29	c:\program files (x86)\google\update\download\{8a69d345-d564-463c-aff1-a69d9e530f96}\96.0.4664.45\96.0.4664.45_chrome_installer.exe	96.0.4664.45_chrome_installer.exe		google llc	96.0.4664.45	e2b8b2e677152fab11f1 0f
2021-12-01 12:55:49	c:\program files\amazon\ssm\amazon-ssm-agent.exe	amazon-ssm-agent.exe				e57d619197d5937d85d 809
2021-12-01 12:57:38	c:\programdata\package cache\{71aad047-faef-4dc7-8d46-60f211a a9f6}\amazonssmagentsetup.exe	AmazonSSMAgentSetup.exe	amazon ssm agent	amazon web services	3.1.338.0	9194f54f615d43875ed 16a
2021-12-01 13:00:20	c:\users\thm-4n6\desktop\amcacheparser.ex e	AmcacheParser.exe	amcacheparser	eric zimmerman	1.4.0.0	13ab20217dff43326642 c7

Total rows: 596

BAM/DAM:

4.



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

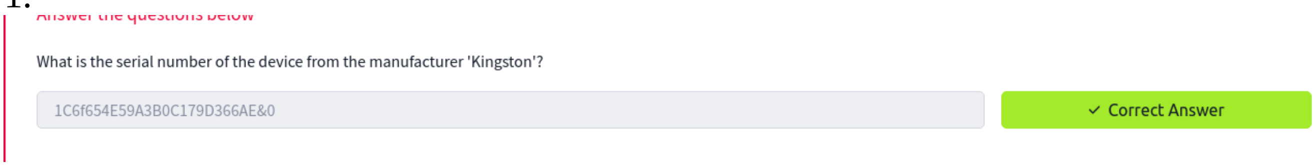
BAM/DAM

External Devices/USB devices forensics

- Usb keys plugged into a system are kept in system\currentcontrol\enum\usb

Questions

1.

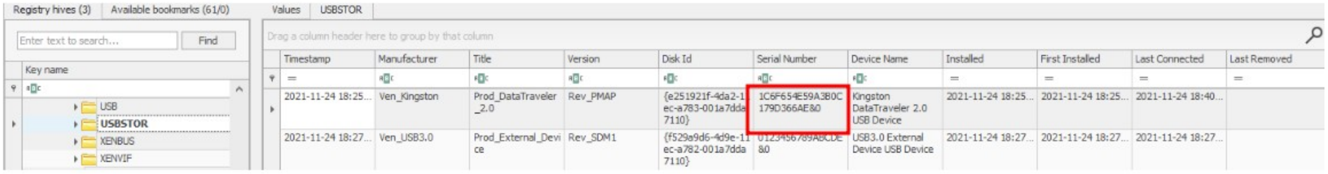


Answer the questions below

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

1C6f654E59A3B0C179D366AE&0

Registry Explorer shows this information in a nice and easy-to-understand way. Take a look at this and answer Questions # 1 and 2.



Registry hives (3) | Available bookmarks (61/0) | Values | USBSTOR

Key name: USB, **USBSTOR**, XENBUS, XENVIF

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-4da2-1 ec-a783-001a7dda 7110}	1C6F654E59A3B0C 179D366AE&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-11 ec-a782-001a7dda 7110}	0123456789ABCDE &0	USB3.0 External Device USB Device	2021-11-24 18:27...	2021-11-24 18:27...	2021-11-24 18:27...	

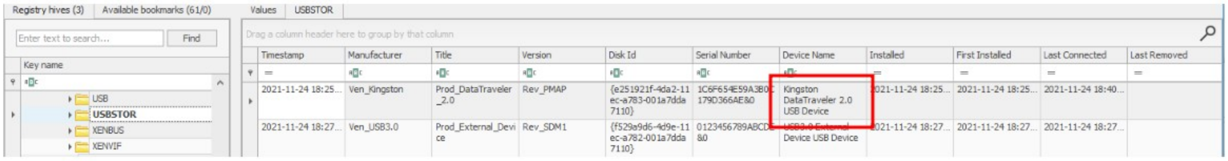
2.

What is the name of this device?

Kingston Data Traveler 2.0 USB Device

✓ Correct Answer

Registry Explorer shows this information in a nice and easy-to-understand way. Take a look at this and answer Questions # 1 and 2.



Registry hives (3) | Available bookmarks (61/0) | Values | USBSTOR

Key name: USB, **USBSTOR**, XENBUS, XENVIF

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-4da2-11 ec-a783-001a7dda 7110}	1C6F654E59A3B0C 179D366AE&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-11 ec-a782-001a7dda 7110}	0123456789ABCD &0	USB3.0 External Device USB Device	2021-11-24 18:27...	2021-11-24 18:27...	2021-11-24 18:27...	

First/Last Times:

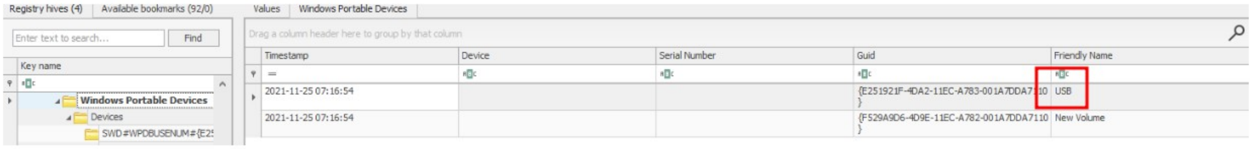
3.

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

USB

✓ Correct Answer

```
SOFTWARE\Microsoft\Windows Portable Devices\Devices
```



Registry hives (4) | Available bookmarks (92/0) | Values | Windows Portable Devices

Key name: **Windows Portable Devices** > Devices > SWD#WPDBUSENUM#{E2!

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

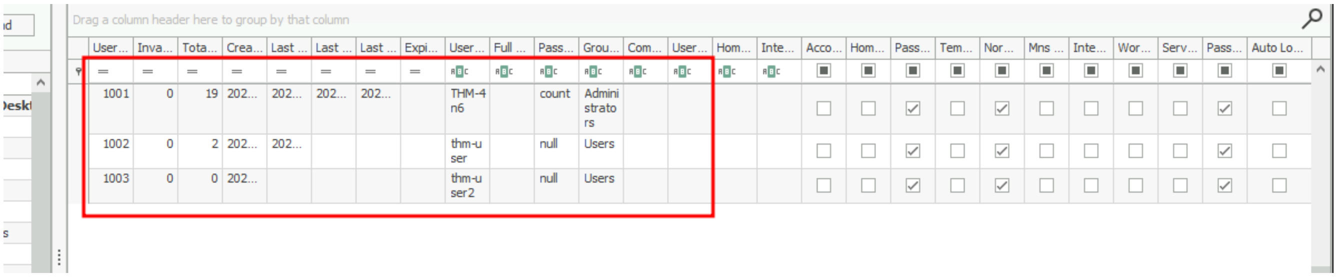
1.

Answer the questions below

How many user created accounts are present on the system?

3

✓ Correct Answer | Hint



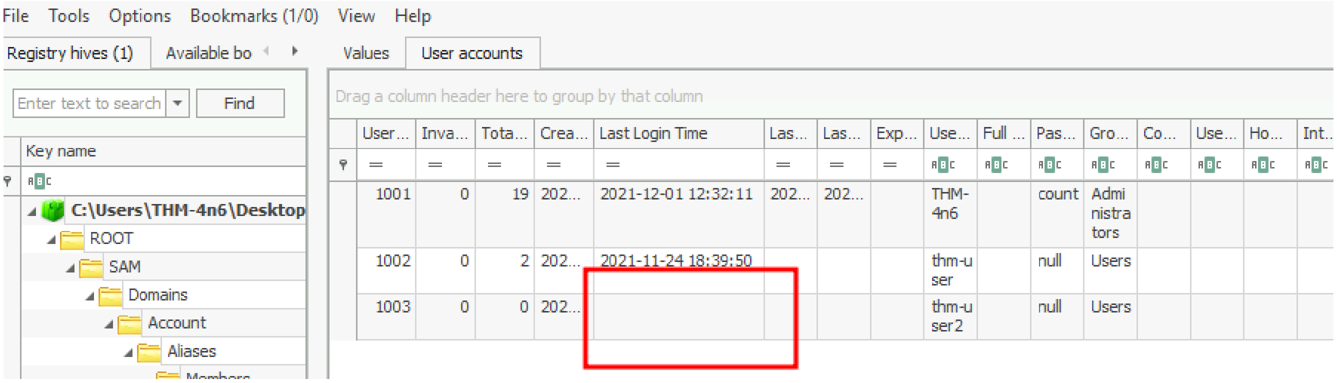
User...	Inva...	Tota...	Crea...	Last ...	Last ...	Last ...	Expi...	User...	Full ...	Pass...	Grou...	Com...	User...	Hom...	Inte...	Acco...	Hom...	Pass...	Tem...	Nor...	Mns ...	Inte...	Wor...	Serv...	Pass...	Auto Lo...
1001	0	19	202...	202...	202...	202...		THM-4n6		count	Administrators					□	□	☑	□	☑	□	□	□	□	☑	□
1002	0	2	202...	202...				thm-user		null	Users					□	□	☑	□	☑	□	□	□	□	☑	□
1003	0	0	202...					thm-user2		null	Users					□	□	☑	□	☑	□	□	□	□	☑	□

2.

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

thm-user2

✓ Correct Answer | Hint



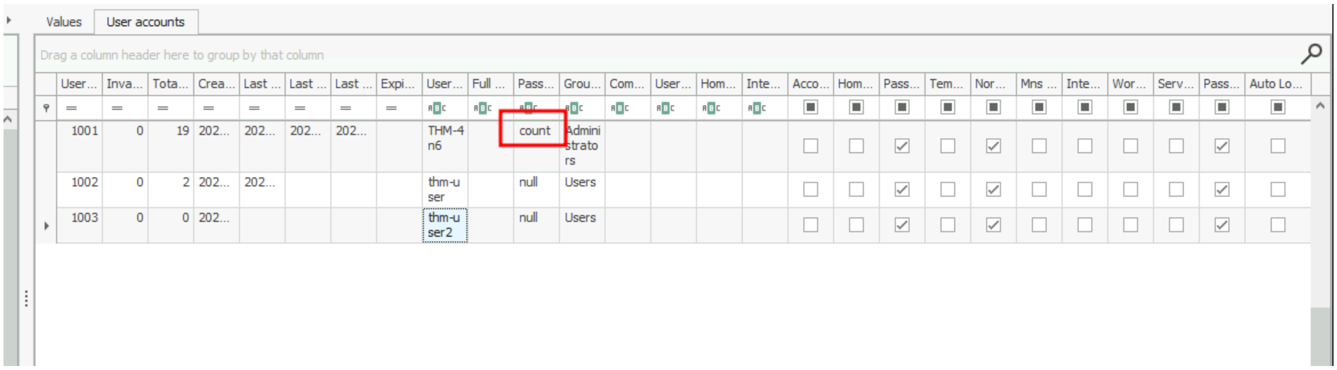
User...	Inva...	Tota...	Crea...	Last Login Time	Las...	Las...	Exp...	Use...	Full ...	Pas...	Gro...	Co...	Use...	Ho...	Int...
1001	0	19	202...	2021-12-01 12:32:11	202...	202...		THM-4n6		count	Administrators				
1002	0	2	202...	2021-11-24 18:39:50				thm-user		null	Users				
1003	0	0	202...					thm-user2		null	Users				

3.

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

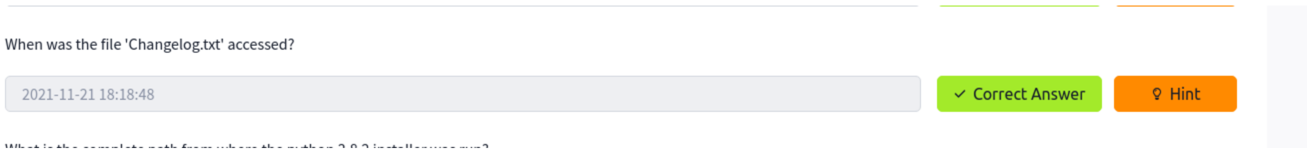
count

✓ Correct Answer | Hint



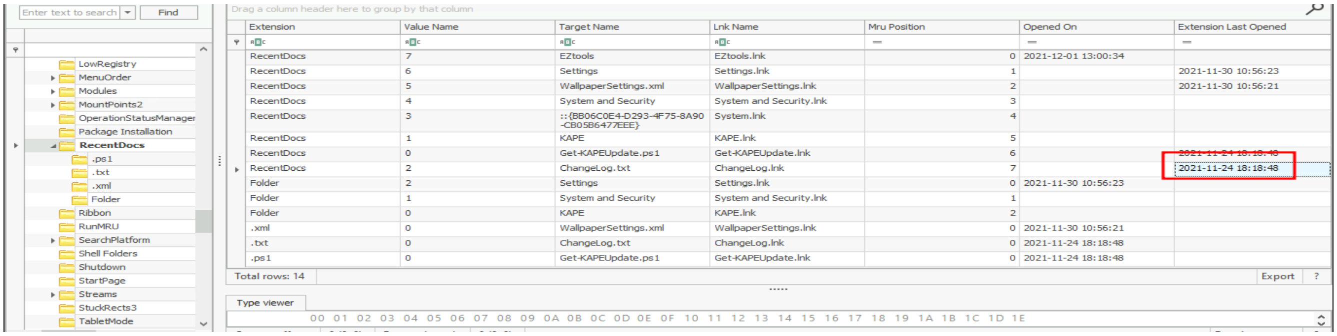
User...	Inva...	Tota...	Crea...	Last ...	Last ...	Last ...	Expi...	User...	Full ...	Pass...	Grou...	Com...	User...	Hom...	Inte...	Acco...	Hom...	Pass...	Tem...	Nor...	Mns ...	Inte...	Wor...	Serv...	Pass...	Auto Lo...
1001	0	19	202...	202...	202...	202...		THM-4n6		count	Administrators					□	□	☑	□	☑	□	□	□	□	☑	□
1002	0	2	202...	202...				thm-user		null	Users					□	□	☑	□	☑	□	□	□	□	☑	□
1003	0	0	202...					thm-user2		null	Users					□	□	☑	□	☑	□	□	□	□	☑	□

4.



When was the file 'Changelog.txt' accessed?

2021-11-21 18:18:48

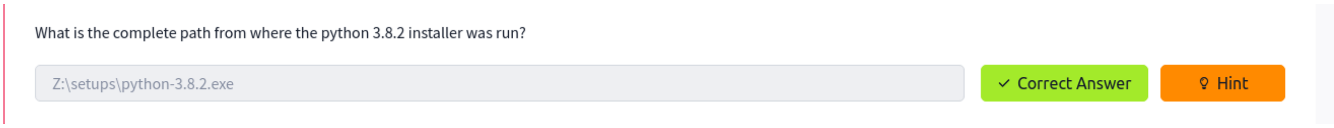


Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
RecentDocs	7	EZtools	EZtools.lnk	0	2021-12-01 13:00:34	
RecentDocs	6	Settings	Settings.lnk	1		2021-11-30 10:56:23
RecentDocs	5	WallpaperSettings.xml	WallpaperSettings.lnk	2		2021-11-30 10:56:21
RecentDocs	4	System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

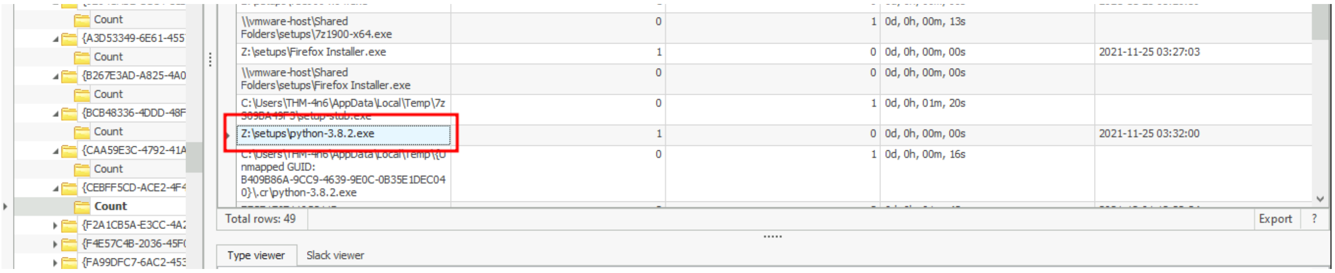
Export
?
Type viewer
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E

5.



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

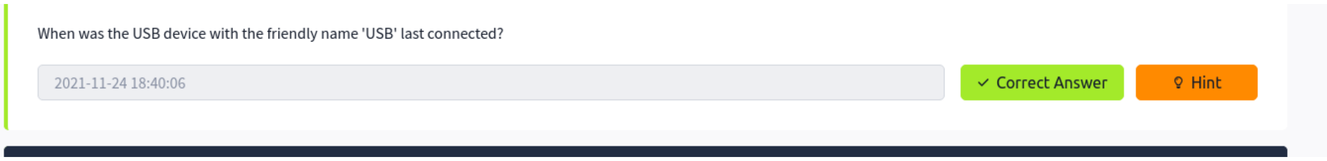
Z:\setups\python-3.8.2.exe



\\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\7z S09BA49F5\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: B409B86A-9CC9-4639-9E0C-0B35E1DEC040}\.cr\python-3.8.2.exe	0	1	0d, 0h, 00m, 16s	

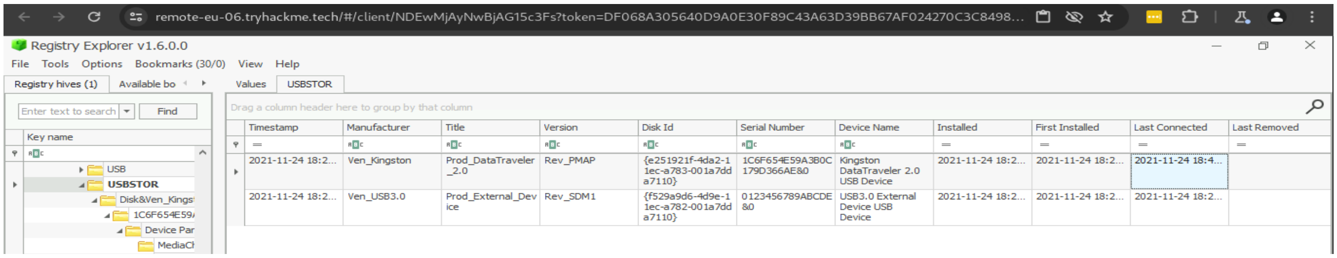
Total rows: 49

6.



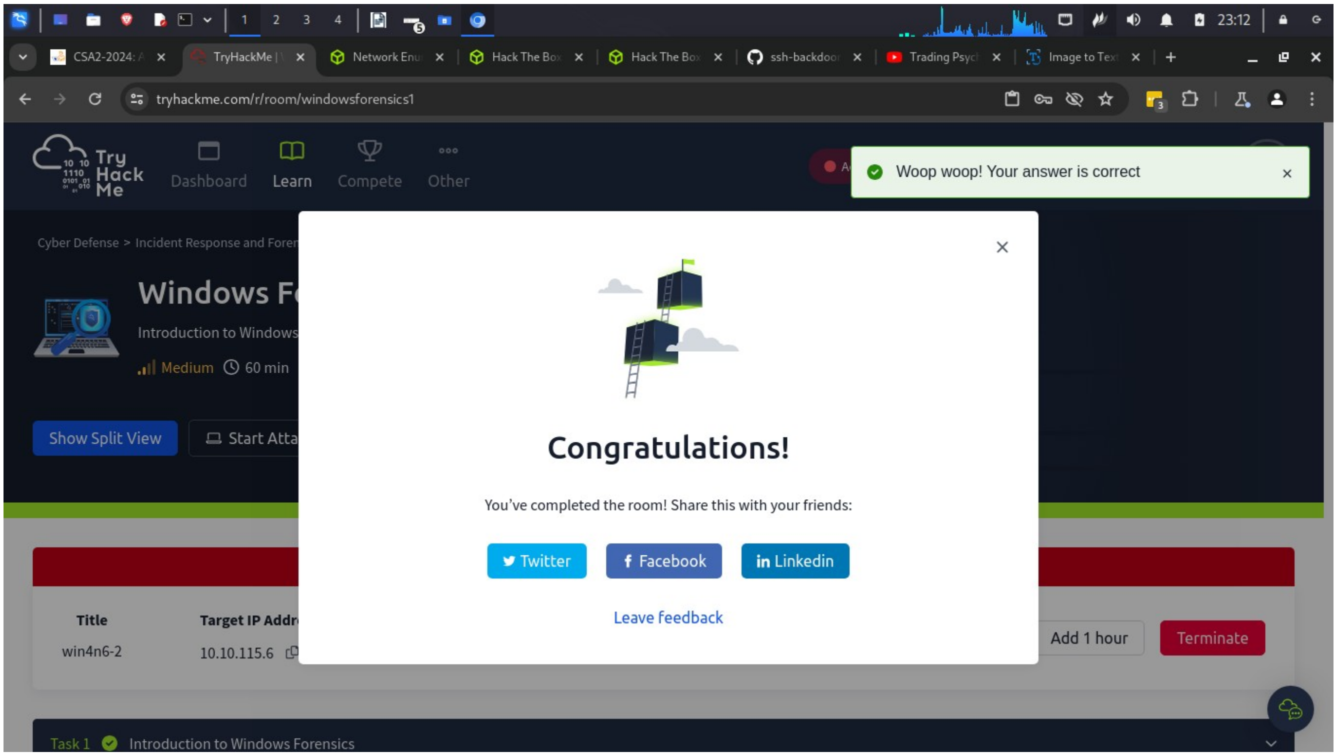
When was the USB device with the friendly name 'USB' last connected?

2021-11-24 18:40:06



remote-eu-06.tryhackme.tech/#/client/NDEwMjAyNwBjAG15c3Fs?token=DF068A305640D9A0E30F89C43A63D39BB67AF024270C3C8498...

Timestamp	Manufacturer	Title	Version	Disk Id	Serial Number	Device Name	Installed	First Installed	Last Connected	Last Removed
2021-11-24 18:2...	Ven_Kingston	Prod_DataTraveler_2.0	Rev_PMAP	{e251921f-4da2-11ec-a783-001a7dda7110}	1C6F654E59A3B0C179D366AE&0	Kingston DataTraveler 2.0 USB Device	2021-11-24 18:2...	2021-11-24 18:2...	2021-11-24 18:4...	
2021-11-24 18:2...	Ven_USB3.0	Prod_External_Device	Rev_SDM1	{f529a9d6-4d9e-11ec-a782-001a7dda7110}	0123456789ABCDE&0	USB3.0 External Device USB Device	2021-11-24 18:2...	2021-11-24 18:2...	2021-11-24 18:2...	



Woop woop! Your answer is correct

Congratulations!

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

Conclusion

In this room I have learnt a lot about windows registry. I have learnt how to gather information about a windows computer and its users, to identify which files they used, Which program they ran and any external devices connected to them. I also downloaded the cheat sheet that I will be using to practice what I have learn.