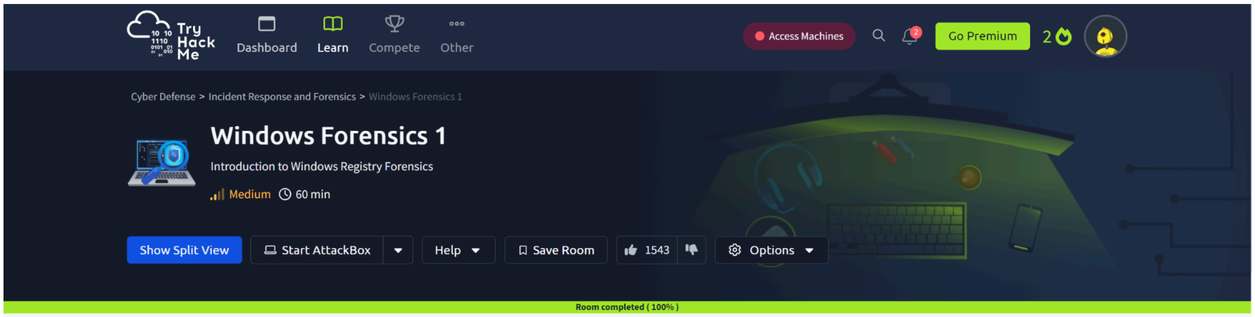
WINDOWS FORENSICS 1

ASSIGNMENT REPORT



Cyber Defense > Incident Response and Forensics > Windows Forensics 1

Windows Forensics 1

Introduction to Windows Registry Forensics

Room completed (100%)

Peter Kinyumu,
cs-sa07-24067,
July 20th, 2024

1. INTRODUCTION

This room teaches how to perform Windows registry forensics. It explains why the registry is a rich source of forensics evidence, then goes ahead to show how to access the different registry hives, tools used and the different artefacts like system information, program execution and external devices that were connected to the victim machine.

2. ANSWERS TO QUESTIONS

Introduction to Windows Forensics

a. **What is the most used Desktop Operating System right now?**
   - `Microsoft Windows`

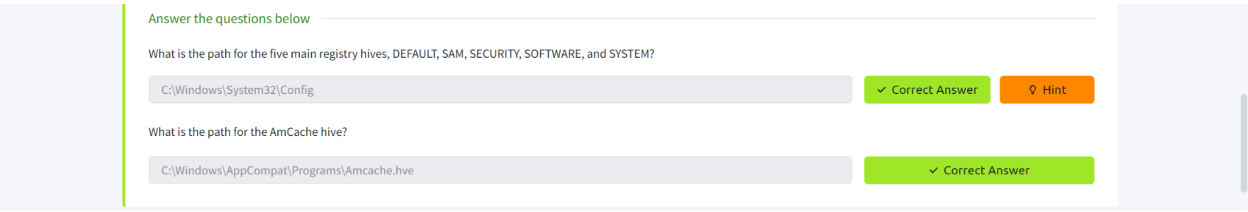
Windows Registry and Forensics

a. **What is the short form for HKEY_LOCAL_MACHINE?**
   - `HKLM`

Accessing Registry hives offline

a. **What is the path for the five main registry hives, DEFAULT, SAM, SECURITY, SOFTWARE, and SYSTEM?**
   - `C:\Windows\System32\Config`

b. **What is the path for the AmCache hive?**
   - `C:\Windows\AppCompat\Programs\Amcache.hve`



Answer the questions below

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

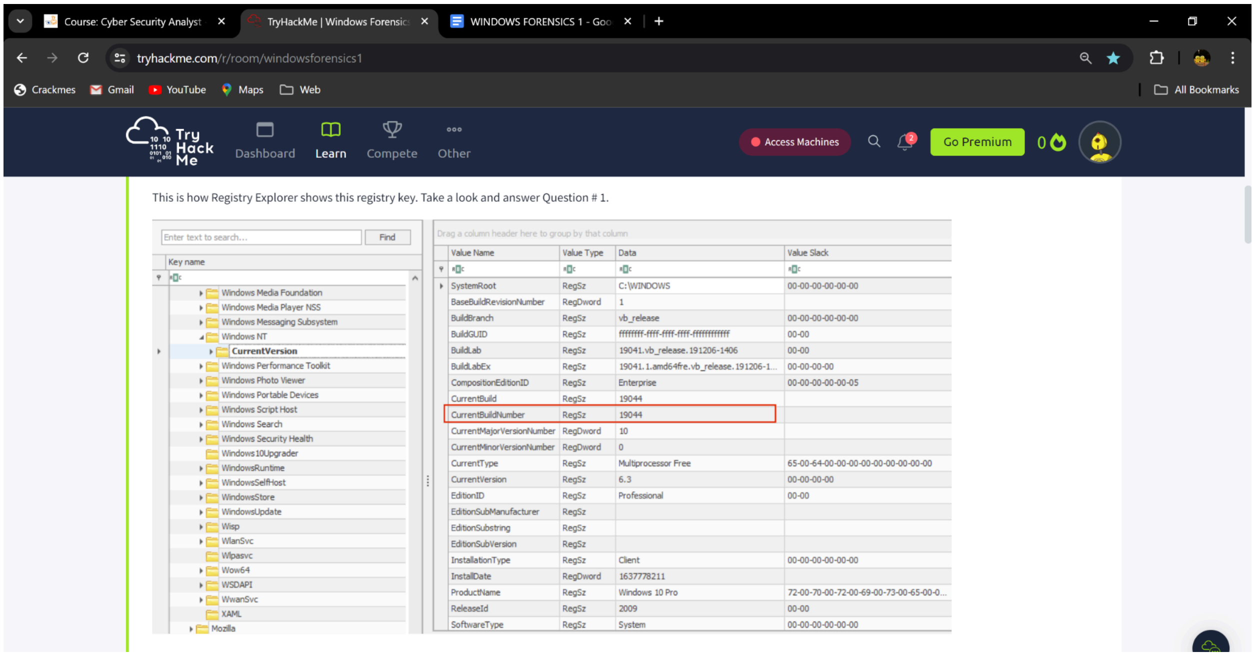
C:\Windows\System32\Config

What is the path for the AmCache hive?

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

System Information and System accounts

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

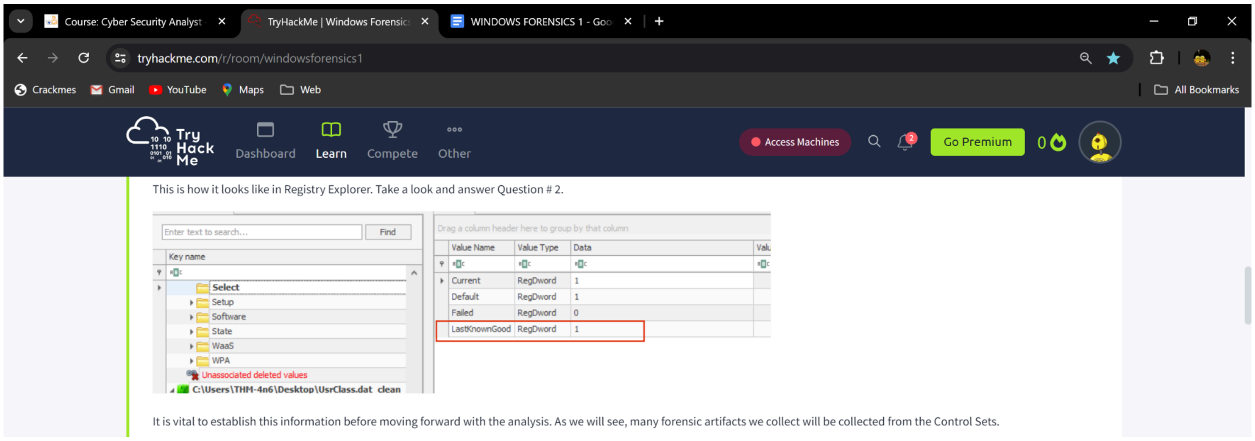


This is how Registry Explorer shows this registry key. Take a look and answer Question # 1.

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

b. Which ControlSet contains the last known good configuration?

- 1


Course: Cyber Security Analyst
TryHackMe | Windows Forensic
WINDOWS FORENSICS 1 - Goo
tryhackme.com/r/room/windowsforensics1
Crackmes
Gmail
YouTube
Maps
Web
All Bookmarks
Dashboard
Learn
Compete
Other
Access Machines
Go Premium
0
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

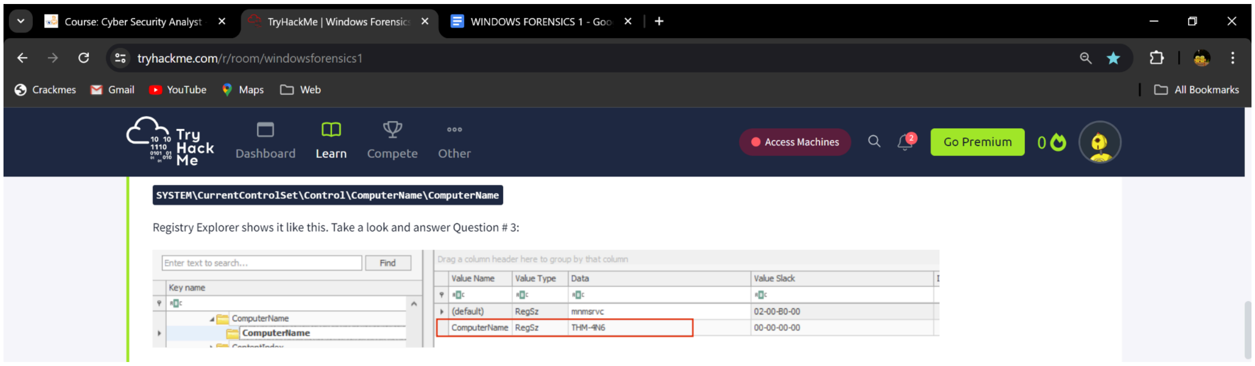
This is how it looks like in Registry Explorer. Take a look and answer Question # 2.

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

It is vital to establish this information before moving forward with the analysis. As we will see, many forensic artifacts we collect will be collected from the Control Sets.

c. What is the Computer Name of the computer?

- THM-4n6



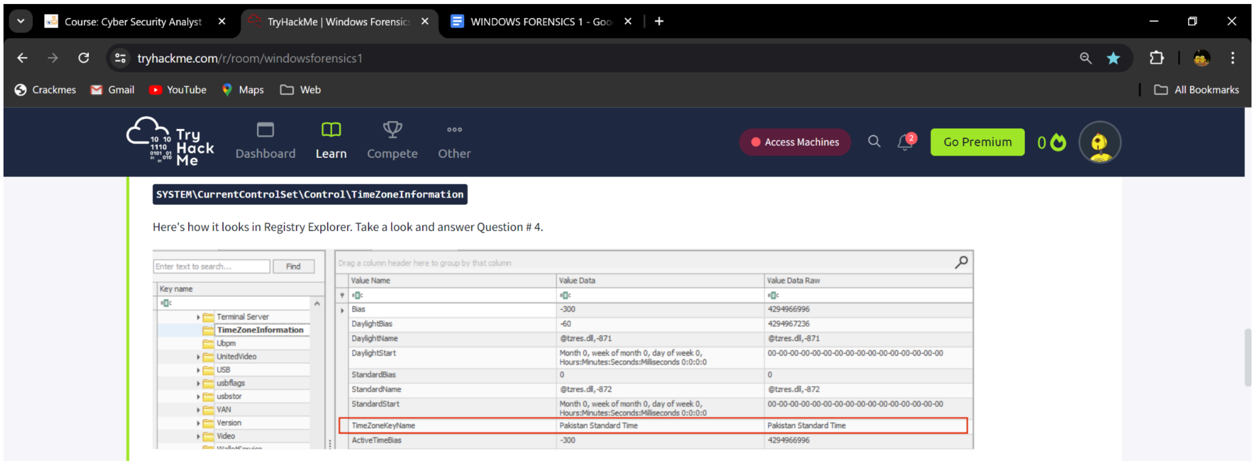
```
SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName
```

Registry Explorer shows it like this. Take a look and answer Question # 3:

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

d. What is the value of the TimeZoneKeyName?

- Pakistan Standard Time



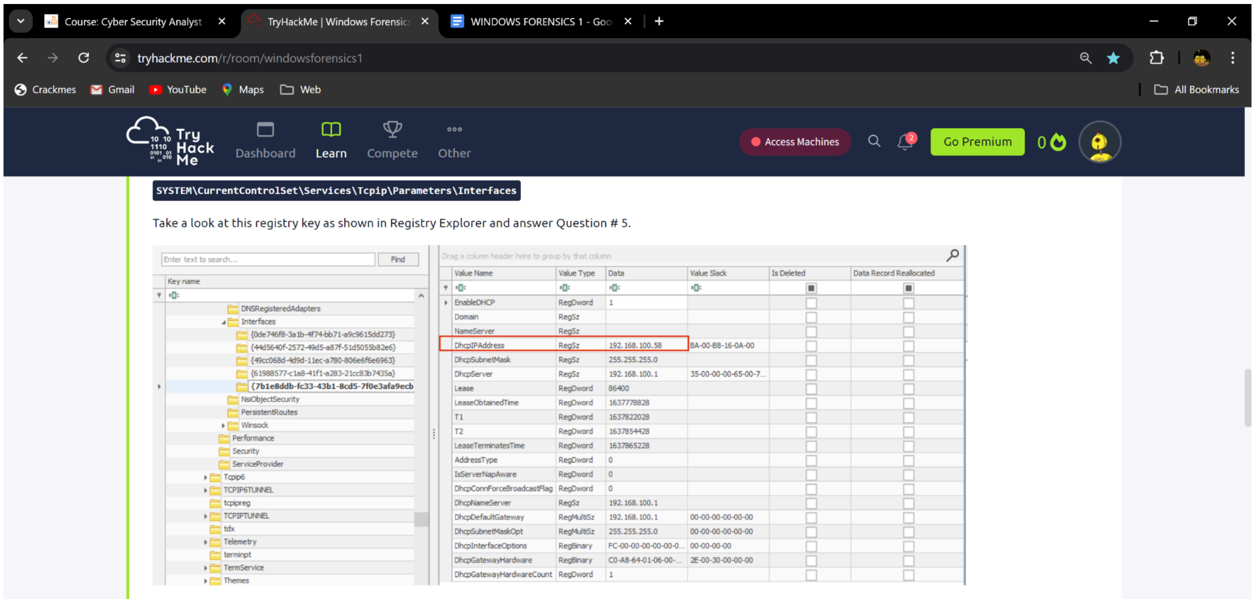
```
SYSTEM\CurrentControlSet\Control\TimeZoneInformation
```

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

e. What is the DHCP IP address

- 192.168.100.58



Course: Cyber Security Analyst
TryHackMe | Windows Forensic
WINDOWS FORENSICS 1 - Goo
tryhackme.com/r/room/windowsforensics1
Crackmes
Gmail
YouTube
Maps
Web
All Bookmarks
Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
Go Premium
0
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

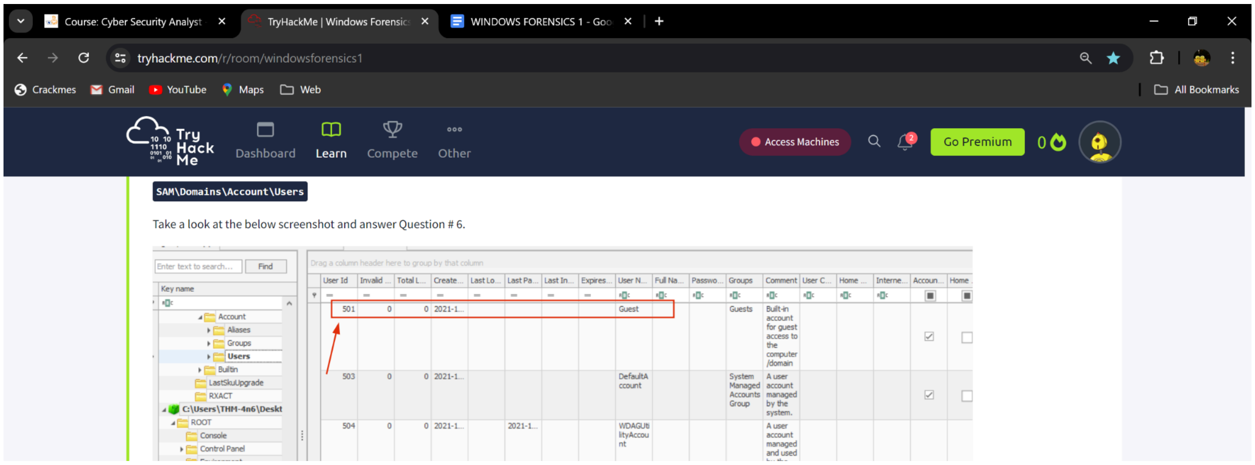
```
SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
```

Take a look at this registry key as shown in Registry Explorer and answer Question # 5.

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		□	□

f. What is the RID of the Guest User account?

- 501



Course: Cyber Security Analyst
TryHackMe | Windows Forensics
WINDOWS FORENSICS 1 - Goo
tryhackme.com/r/room/windowsforensics1
Crackmes
Gmail
YouTube
Maps
Web
All Bookmarks
Dashboard
Learn
Compete
Other
Access Machines
Go Premium

`SAM\Domains\Account\Users`

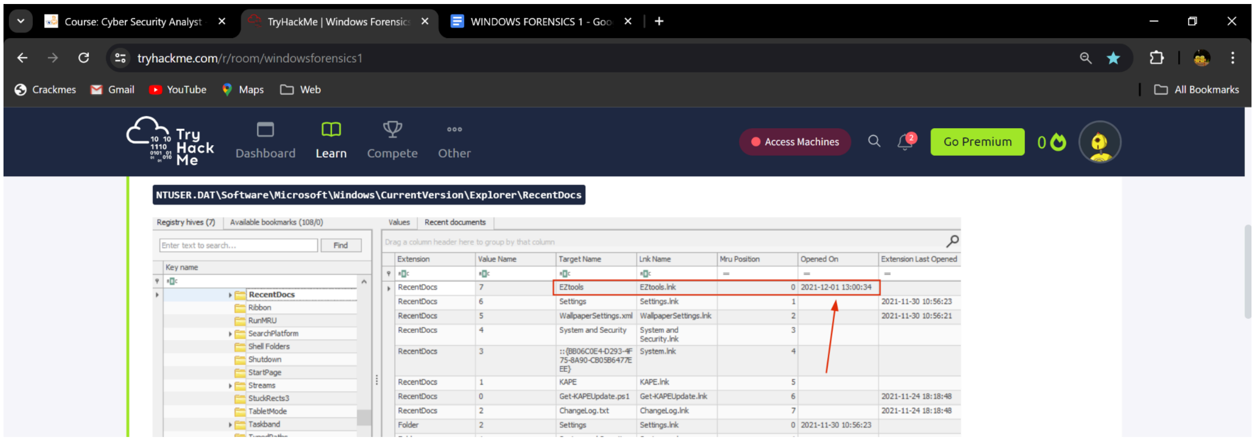
Take a look at the below screenshot and answer Question # 6.

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					

Usage or Knowledge of files/folders

a. When was EZtools opened?

- 2021-12-01 13:00:34



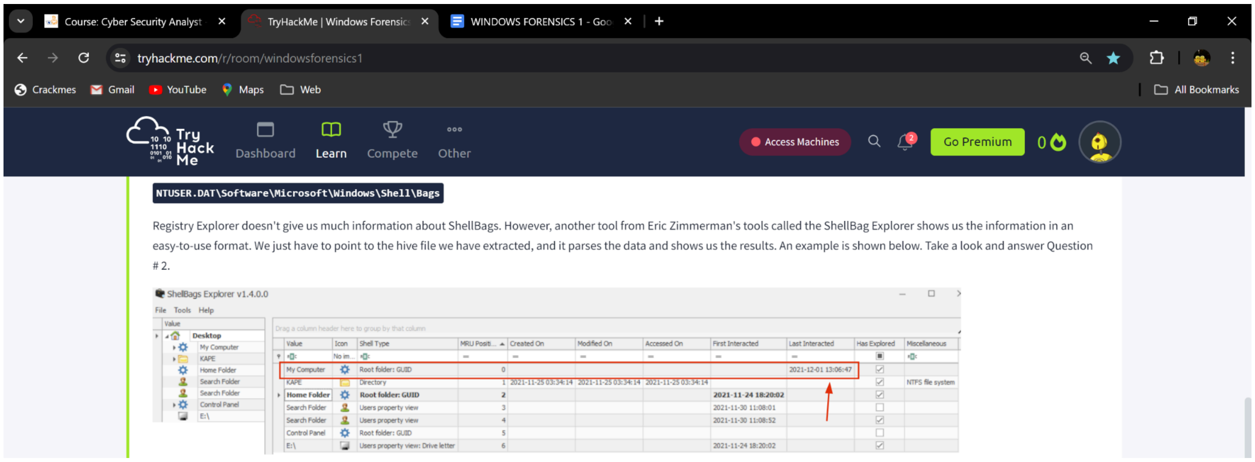
Course: Cyber Security Analyst
TryHackMe | Windows Forensics
WINDOWS FORENSICS 1 - Goo
tryhackme.com/r/room/windowsforensics1
Crackmes
Gmail
YouTube
Maps
Web
All Bookmarks
Dashboard
Learn
Compete
Other
Access Machines
Go Premium

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

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	

b. At what time was My Computer last interacted with?

- 2021-12-01 13:06:47


Course: Cyber Security Analyst
TryHackMe | Windows Forensic
WINDOWS FORENSICS 1 - Goo
tryhackme.com/r/room/windowsforensics1
Crackmes
Gmail
YouTube
Maps
Web
All Bookmarks
Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
2
Go Premium
0

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

Registry Explorer doesn't give us much information about ShellBags. However, another tool from Eric Zimmerman's tools called the ShellBag Explorer shows us the information in an easy-to-use format. We just have to point to the hive file we have extracted, and it parses the data and shows us the results. An example is shown below. Take a look and answer Question # 2.

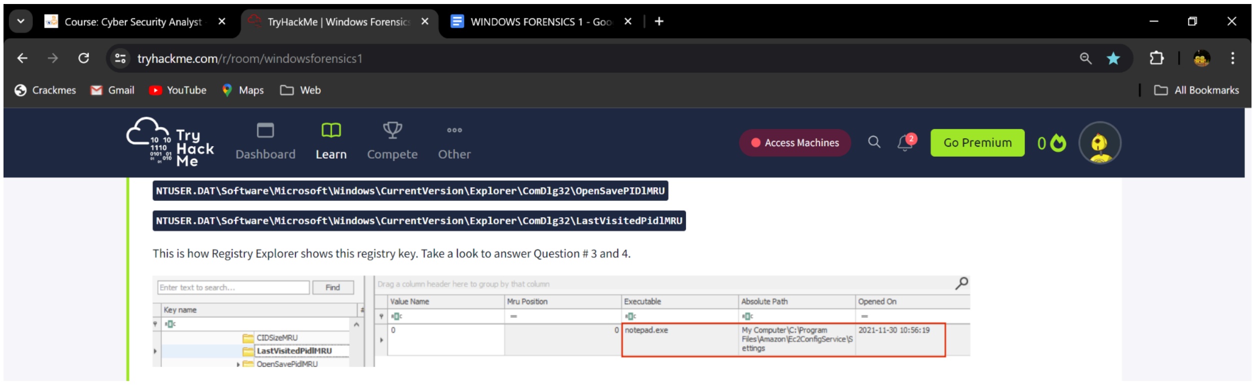
Value	Icon	Shell Type	MRU Positi...	Created On	Modified On	Accessed On	First Interacted	Last Interacted	Has Explored	Miscellaneous
My Computer		Root folder: GUID	0					2021-12-01 13:06:47	☑	
KAPE		Directory	1	2021-11-25 03:34:14	2021-11-25 03:34:14	2021-11-25 03:34:14			☑	NTFS file system
Home Folder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

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

- `C:\Program Files\Amazon\Ec2ConfigService\Settings`

d. **When was this file opened?**

- `2021-11-30 10:56:19`


Course: Cyber Security Analyst
TryHackMe | Windows Forensic
WINDOWS FORENSICS 1 - Goo
tryhackme.com/r/room/windowsforensics1
Crackmes
Gmail
YouTube
Maps
Web
All Bookmarks
Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
2
Go Premium
0

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

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

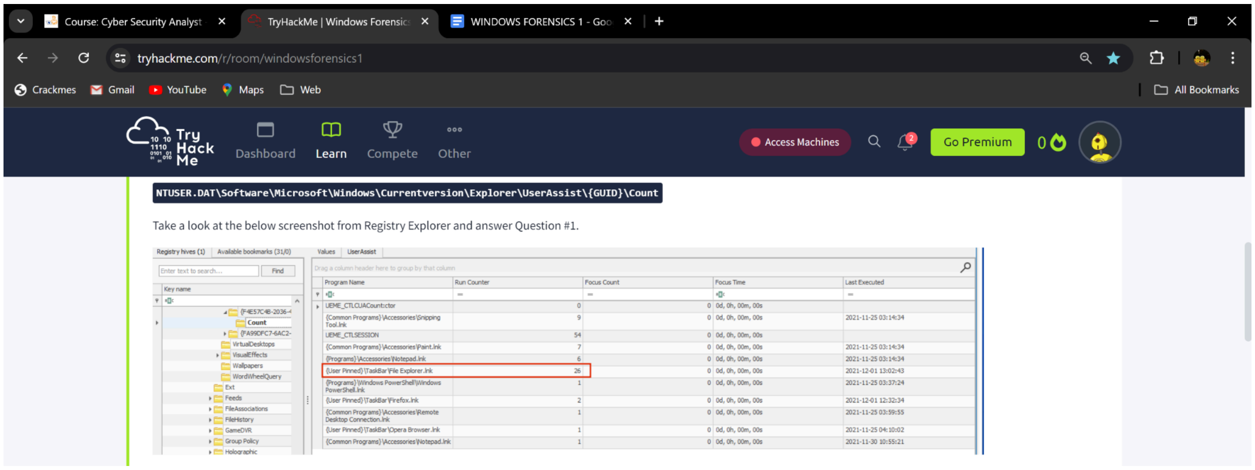
This is how Registry Explorer shows this registry key. Take a look to answer Question # 3 and 4.

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

Evidence of Execution

a. **How many times was the File Explorer launched?**

- `26`



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

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

b. **What is another name for ShimCache?**
   - AppCompatCache

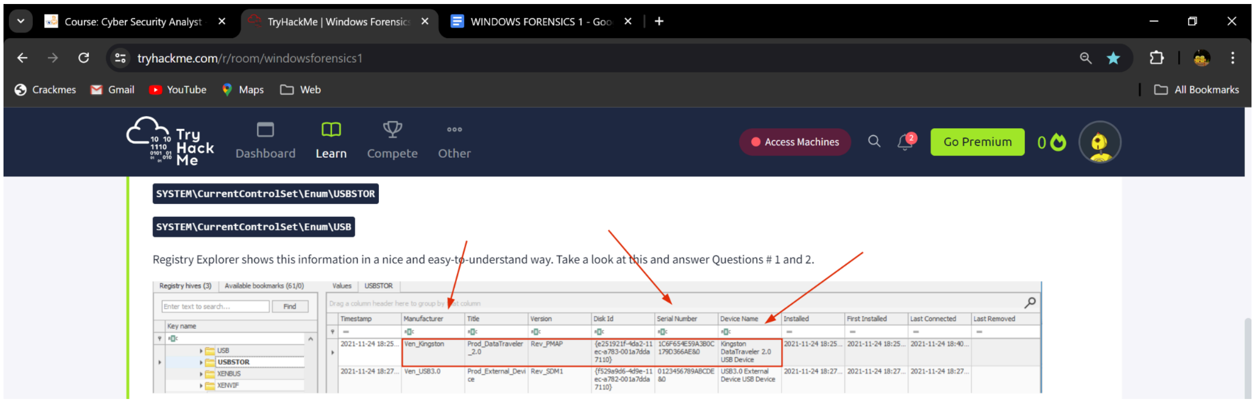
c. **Which of the artifacts also saves SHA1 hashes of the executed programs?**
   - AmCache

d. **Which of the artifacts saves the full path of the executed programs?**
   - BAM/DAM

External Devices/USB device forensics

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

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


Course: Cyber Security Analyst
TryHackMe | Windows Forensic
WINDOWS FORENSICS 1 - Goo
tryhackme.com/r/room/windowsforensics1
Crackmes
Gmail
YouTube
Maps
Web
All Bookmarks
Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
Go Premium
0
Registry hives (3)
Available bookmarks (61/0)
Enter text to search...
Find
Key name
USB
USBSTOR
XENBUS
XENVIF
Values
USBSTOR
Drag a column header here to group by that column

`SYSTEM\CurrentControlSet\Enum\USBSTOR`

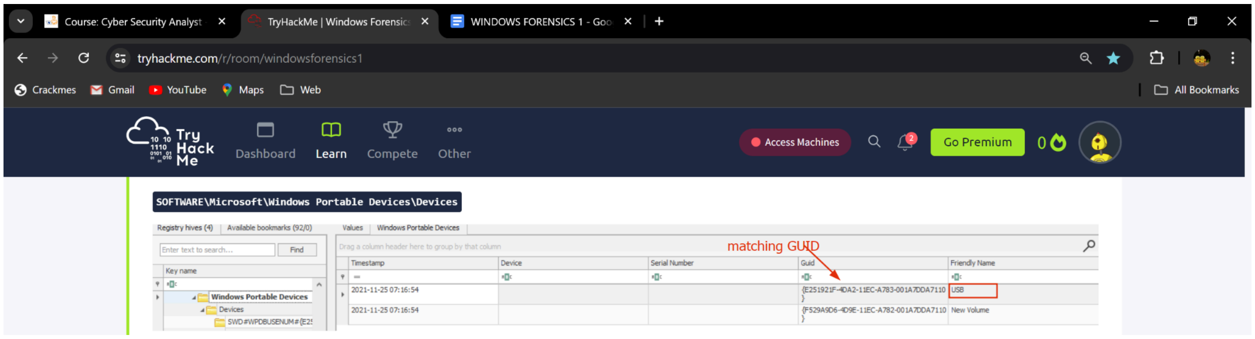
`SYSTEM\CurrentControlSet\Enum\USB`

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

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...	

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

- USB


Course: Cyber Security Analyst
TryHackMe | Windows Forensic
WINDOWS FORENSICS 1 - Goo
tryhackme.com/r/room/windowsforensics1
Crackmes
Gmail
YouTube
Maps
Web
All Bookmarks
Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
Go Premium
0

`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#{E25

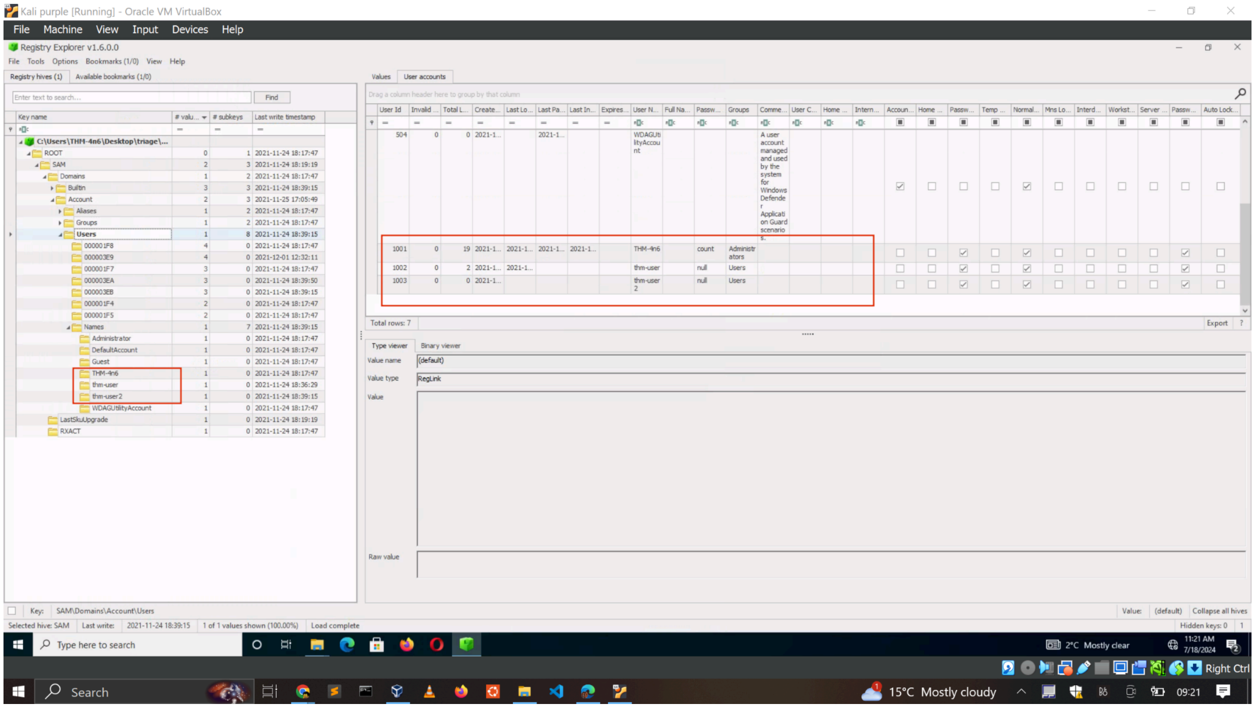
matching GUID

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

a. **How many user created accounts are present on the system?**

- 3


Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Registry Explorer v1.6.0.0
File Tools Options Bookmarks (1/0) View Help
Registry hives (1)
Available bookmarks (1/0)
Enter text to search...
Find
Values
User accounts
Drag a column header here to group by that column
Type viewer
Binary viewer
Export
Type here to search
2°C Mostly clear
11:21 AM 7/18/2024
Right Ctrl
Search
15°C Mostly cloudy
09:21

Key name	# valu...	# subkeys	Last write timestamp
C:\Users\THM-4n6\Desktop\triage\...			
ROOT	0	1	2021-11-24 18:17:47
SAM	2	3	2021-11-24 18:19:19
Domains	1	2	2021-11-24 18:17:47
Builtin	3	3	2021-11-24 18:39:15
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
000001F8	4	0	2021-11-24 18:17:47
000003E9	4	0	2021-12-01 12:32:11
000001F7	3	0	2021-11-24 18:17:47
000003EA	3	0	2021-11-24 18:39:50
000003EB	3	0	2021-11-24 18:39:15
000001F4	2	0	2021-11-24 18:17:47
000001F5	2	0	2021-11-24 18:17:47
Names	1	7	2021-11-24 18:39:15
Administrator	1	0	2021-11-24 18:17:47
DefaultAccount	1	0	2021-11-24 18:17:47
Guest	1	0	2021-11-24 18:17:47
THM-4n6	1	0	2021-11-24 18:17:47
thm-user	1	0	2021-11-24 18:36:29
thm-user2	1	0	2021-11-24 18:39:15
WDAGUtilityAccount	1	0	2021-11-24 18:17:47
LastSkuUpgrade	1	0	2021-11-24 18:19:19
RXACT	1	0	2021-11-24 18:17:47

User Id	Invalid ...	Total L...	Create...	Last Lo...	Last Pa...	Last In...	Expires...	User N...	Full Na...	Passw...	Groups	Comme...	User C...	Home ...	Intern...	Accoun...	Home ...	Passw...	Temp ...	Normal...	Mns Lo...	Interd...	Workst...	Server ...	Passw...	Auto Lock...
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	Administrators					☐	☐	☑	☐	☑	☐	☐	☐	☐	☑	☐
1002	0	2	2021-1...	2021-1...				thm-user		null	Users					☐	☐	☑	☐	☑	☐	☐	☐	☐	☑	☐
1003	0	0	2021-1...					thm-user2		null	Users					☐	☐	☑	☐	☑	☐	☐	☐	☐	☑	☐

Total rows: 7

Value name: (default)

Value type: RegLink

Value:

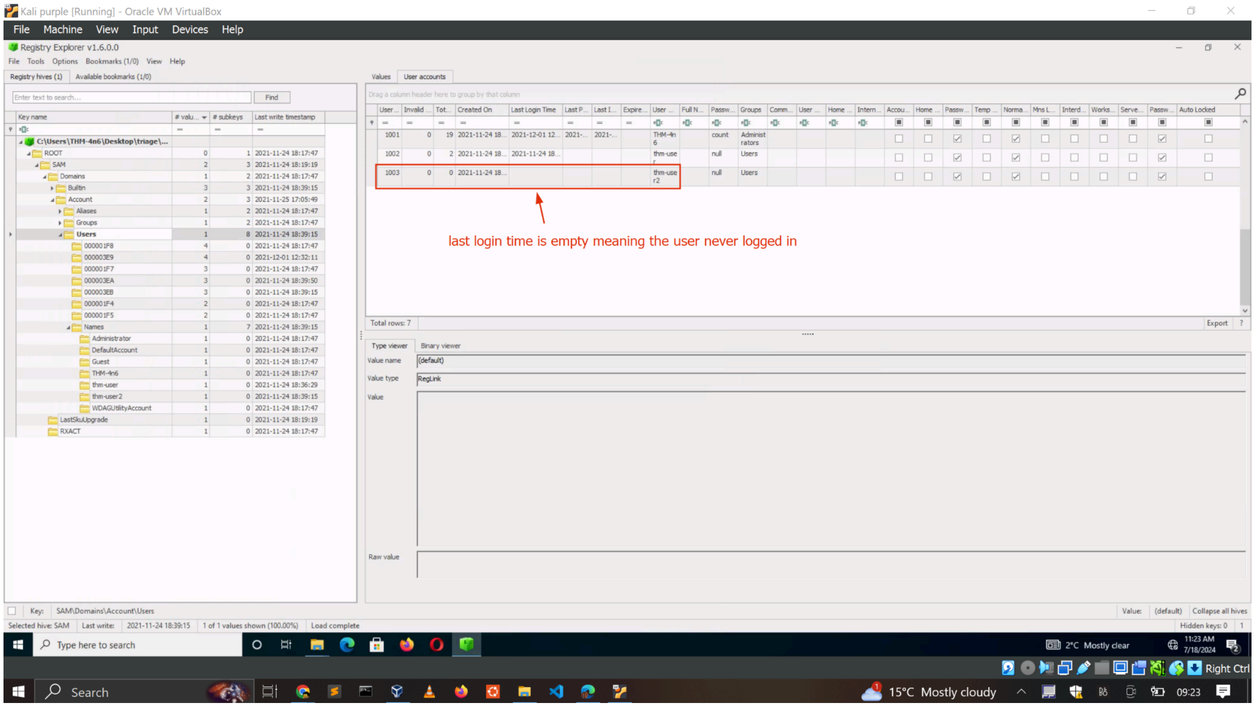
Raw value:

Key: SAM\Domains\Account\Users   Value: (default)   Collapse all hives

Selected hive: SAM   Last write: 2021-11-24 18:39:15   1 of 1 values shown (100.00%)   Load complete   Hidden keys: 0

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

- thm-user2



Kali purple [Running] - Oracle VM VirtualBox

Registry Explorer v1.6.0.0

Key name	# values	# subkeys	Last write timestamp
C:\Users\THM-4n6\Desktop\triage\...			
ROOT	0	1	2021-11-24 18:17:47
SAM	2	3	2021-11-24 18:19:19
Domains	1	2	2021-11-24 18:17:47
Builtin	3	3	2021-11-24 18:39:15
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
000001F8	4	0	2021-11-24 18:17:47
000003E9	4	0	2021-12-01 12:32:11
000001F7	3	0	2021-11-24 18:17:47
000003EA	3	0	2021-11-24 18:39:50
000003EB	3	0	2021-11-24 18:39:15
000001F4	2	0	2021-11-24 18:17:47
000001F5	2	0	2021-11-24 18:17:47
Names	1	7	2021-11-24 18:39:15
Administrator	1	0	2021-11-24 18:17:47
DefaultAccount	1	0	2021-11-24 18:17:47
Guest	1	0	2021-11-24 18:17:47
THM-4n6	1	0	2021-11-24 18:17:47
thm-user	1	0	2021-11-24 18:36:29
thm-user2	1	0	2021-11-24 18:39:15
WDAGUtilityAccount	1	0	2021-11-24 18:17:47
LastSkuUpgrade	1	0	2021-11-24 18:19:19
RXACT	1	0	2021-11-24 18:17:47

User...	Invalid ...	Tot...	Created On	Last Login Time	Last P...	Last I...	Expire...	User ...	Full N...	Passw...	Groups
1001	0	19	2021-11-24 18...	2021-12-01 12...	2021-...	2021-...		THM-4n6		count	Administrators
1002	0	2	2021-11-24 18...	2021-11-24 18...				thm-user		null	Users
1003	0	0	2021-11-24 18...					thm-user2		null	Users

last login time is empty meaning the user never logged in

Total rows: 7

Value name: (default)

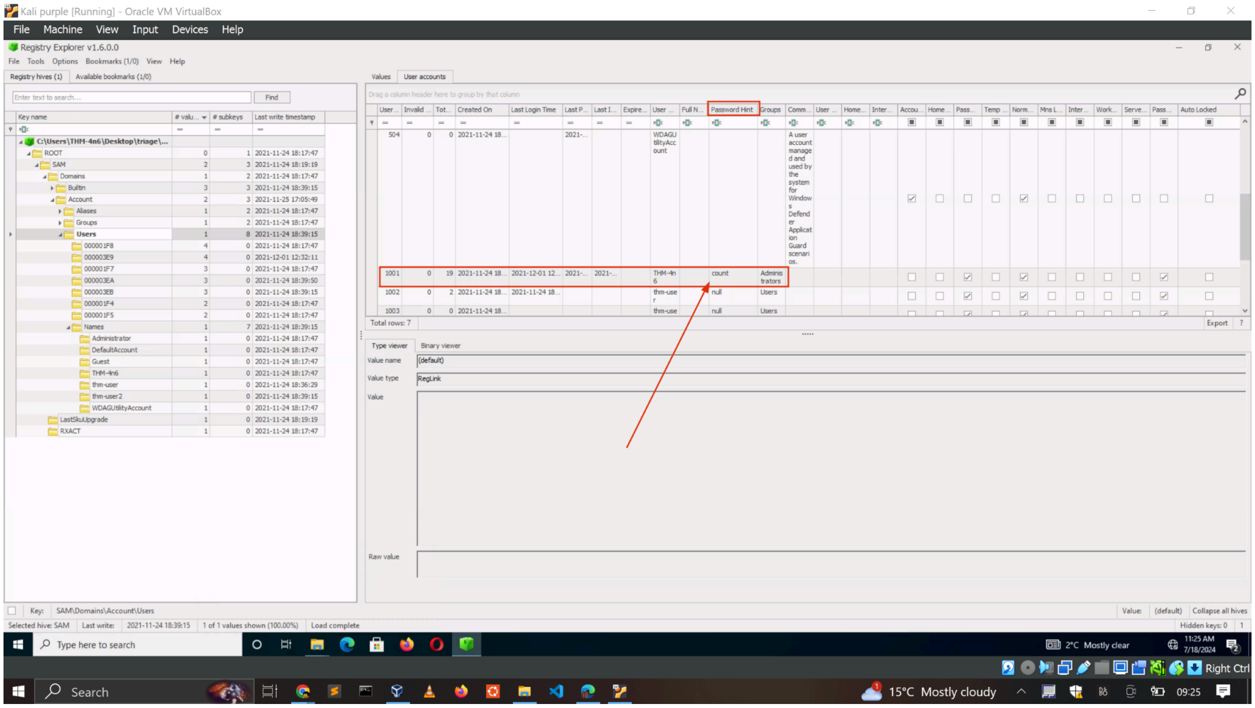
Value type: RegLink

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

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

- count



Kali purple [Running] - Oracle VM VirtualBox

Registry Explorer v1.6.0.0

Key name	# values	# subkeys	Last write timestamp
C:\Users\THM-4n6\Desktop\triage\...			
ROOT	0	1	2021-11-24 18:17:47
SAM	2	3	2021-11-24 18:19:19
Domains	1	2	2021-11-24 18:17:47
Builtin	3	3	2021-11-24 18:39:15
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
000001F8	4	0	2021-11-24 18:17:47
000003E9	4	0	2021-12-01 12:32:11
000001F7	3	0	2021-11-24 18:17:47
000003EA	3	0	2021-11-24 18:39:50
000003EB	3	0	2021-11-24 18:39:15
000001F4	2	0	2021-11-24 18:17:47
000001F5	2	0	2021-11-24 18:17:47
Names	1	7	2021-11-24 18:39:15
Administrator	1	0	2021-11-24 18:17:47
DefaultAccount	1	0	2021-11-24 18:17:47
Guest	1	0	2021-11-24 18:17:47
THM-4n6	1	0	2021-11-24 18:17:47
thm-user	1	0	2021-11-24 18:36:29
thm-user2	1	0	2021-11-24 18:39:15
WDAGUtilityAccount	1	0	2021-11-24 18:17:47
LastSkuUpgrade	1	0	2021-11-24 18:19:19
RXACT	1	0	2021-11-24 18:17:47

User...	Invalid ...	Tot...	Created On	Last Login Time	Last P...	Last I...	Expire...	User ...	Full N...	Password Hint	Groups	Comm...
504	0	0	2021-11-24 18...		2021-...			WDAGUtilityAccount				A user account managed and used by the system for Windows Defender Application Guard scenarios.
1001	0	19	2021-11-24 18...	2021-12-01 12...	2021-...	2021-...		THM-4n6		count	Administrators	
1002	0	2	2021-11-24 18...	2021-11-24 18...				thm-user		null	Users	
1003	0	0	2021-11-24 18...					thm-use		null	Users	

Total rows: 7

Value name: (default)

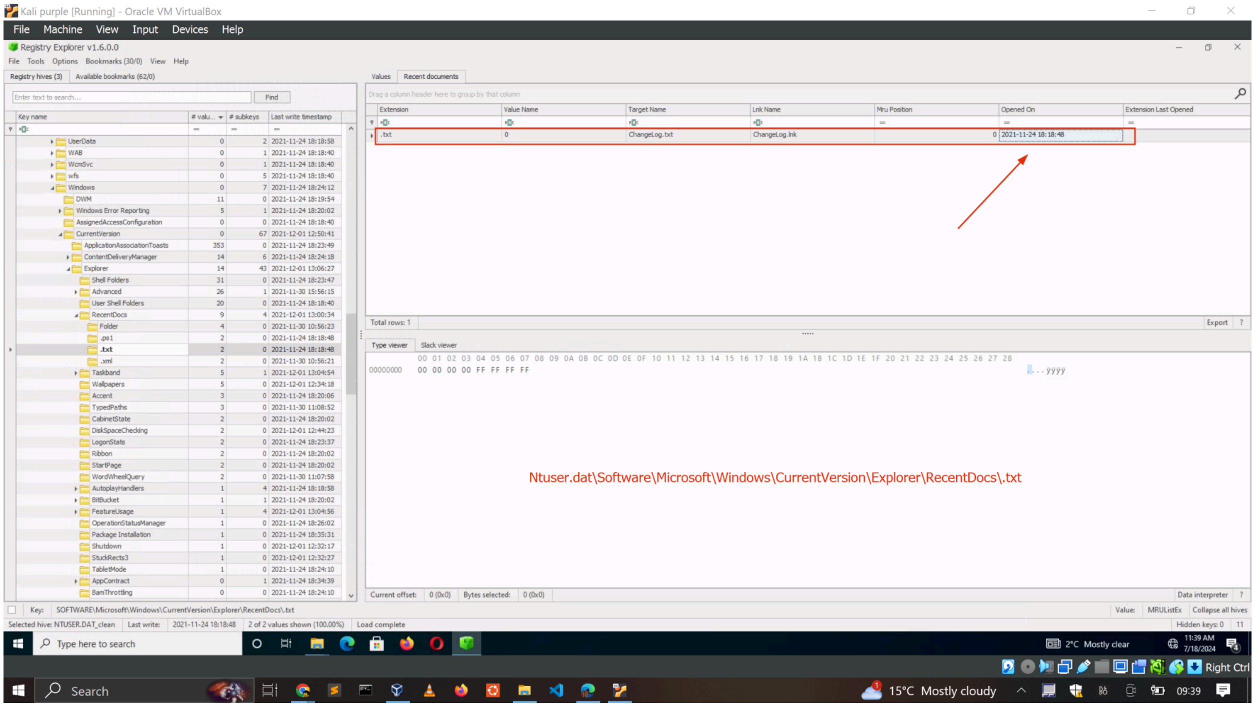
Value type: RegLink

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

d. **When was the file 'Changelog.txt' accessed?**

- 2021-11-21 18:18:48



Values | Recent documents

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

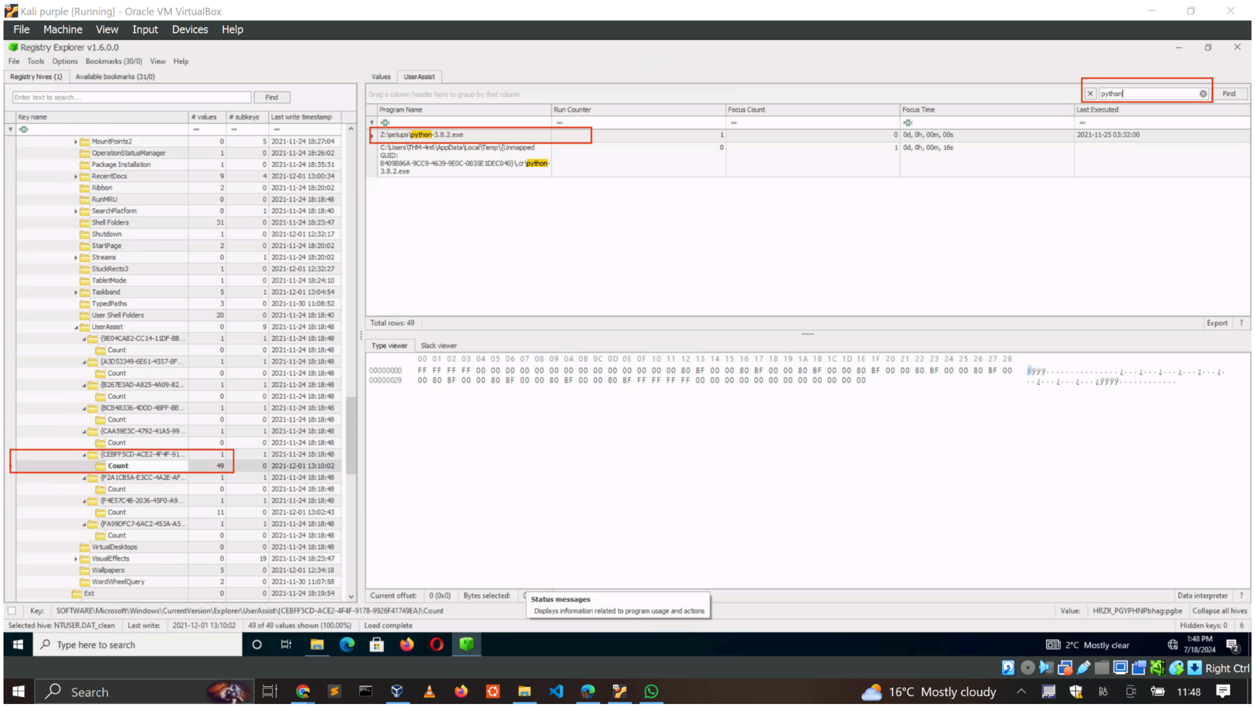
Ntuser.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt

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

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

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

- `Z:\setups\python-3.8.2.exe`



Values | UserAssist

python

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
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

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

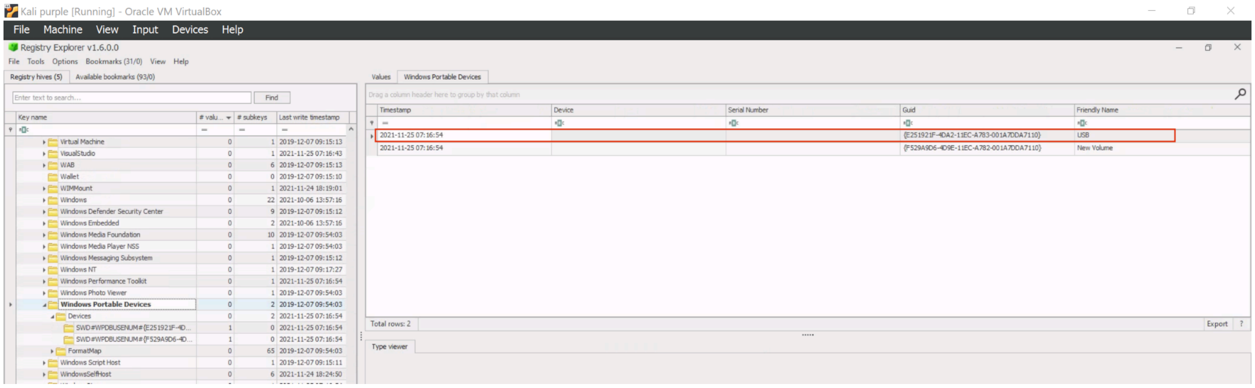
Selected hive: NTUSER.DAT_clean Last write: 2021-12-01 13:10:02 49 of 49 values shown (100.00%) Load complete

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

- We start by looking at the USB with the said friendly name from `SOFTWARE\Microsoft\Windows Portable Devices\Devices`

- Then we match the GUID to the devices in `SYSTEM\CurrentControlSet\Enum\USBSTOR`

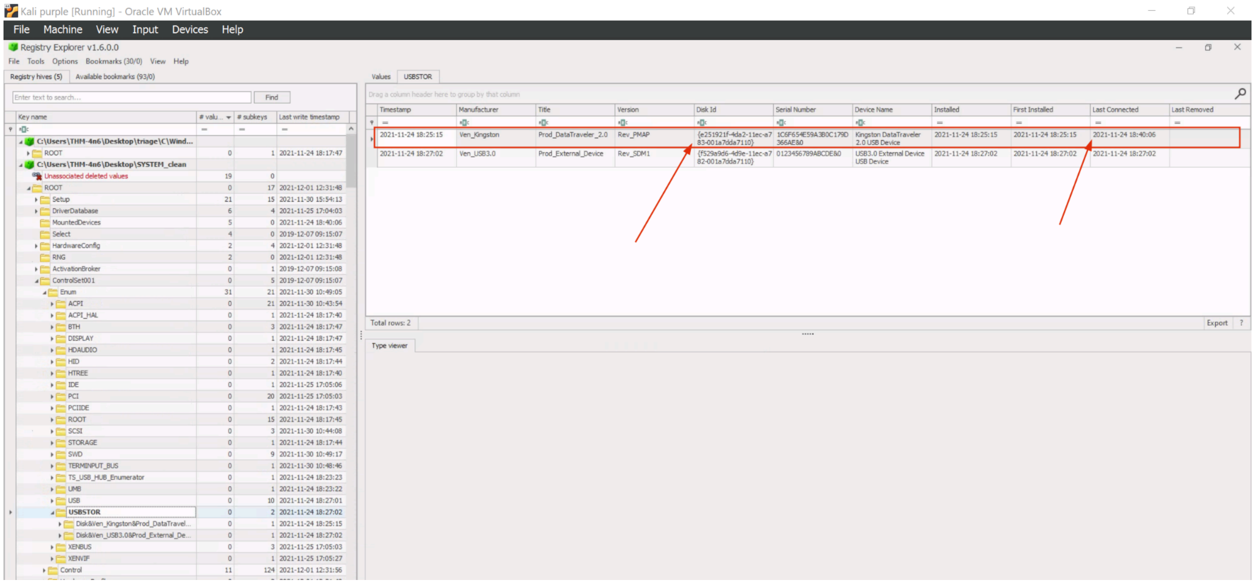
- `2021-11-24 18:40:06`


Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Registry Explorer v1.6.0.0
File Tools Options Bookmarks (31/0) View Help
Registry hives (5) Available bookmarks (93/0)
Enter text to search...
Find
Values
Windows Portable Devices
Drag a column header here to group by that column
Export
Type viewer

Key name	# valu...	# subkeys	Last write timestamp
Virtual Machine	0	1	2019-12-07 09:15:13
VisualStudio	0	1	2021-11-25 07:16:43
WAB	0	6	2019-12-07 09:15:13
Wallet	0	0	2019-12-07 09:15:10
WIMMount	0	1	2021-11-24 18:19:01
Windows	0	22	2021-10-06 13:57:16
Windows Defender Security Center	0	9	2019-12-07 09:15:12
Windows Embedded	0	2	2021-10-06 13:57:16
Windows Media Foundation	0	10	2019-12-07 09:54:03
Windows Media Player NSS	0	1	2019-12-07 09:54:03
Windows Messaging Subsystem	0	1	2019-12-07 09:15:12
Windows NT	0	1	2019-12-07 09:17:27
Windows Performance Toolkit	0	1	2021-11-25 07:16:54
Windows Photo Viewer	0	1	2019-12-07 09:54:03
Windows Portable Devices	0	2	2019-12-07 09:54:03
Devices	0	2	2021-11-25 07:16:54
SWD#WPDBUSENUM#{E251921F-4D...	1	0	2021-11-25 07:16:54
SWD#WPDBUSENUM#{F529A9D6-4D...	1	0	2021-11-25 07:16:54
FormatMap	0	65	2019-12-07 09:54:03
Windows Script Host	0	1	2019-12-07 09:15:11
WindowsSelfHost	0	6	2021-11-24 18:24:50

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

Total rows: 2


Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Registry Explorer v1.6.0.0
File Tools Options Bookmarks (30/0) View Help
Registry hives (5) Available bookmarks (93/0)
Enter text to search...
Find
Values
USBSTOR
Drag a column header here to group by that column
Export
Type viewer

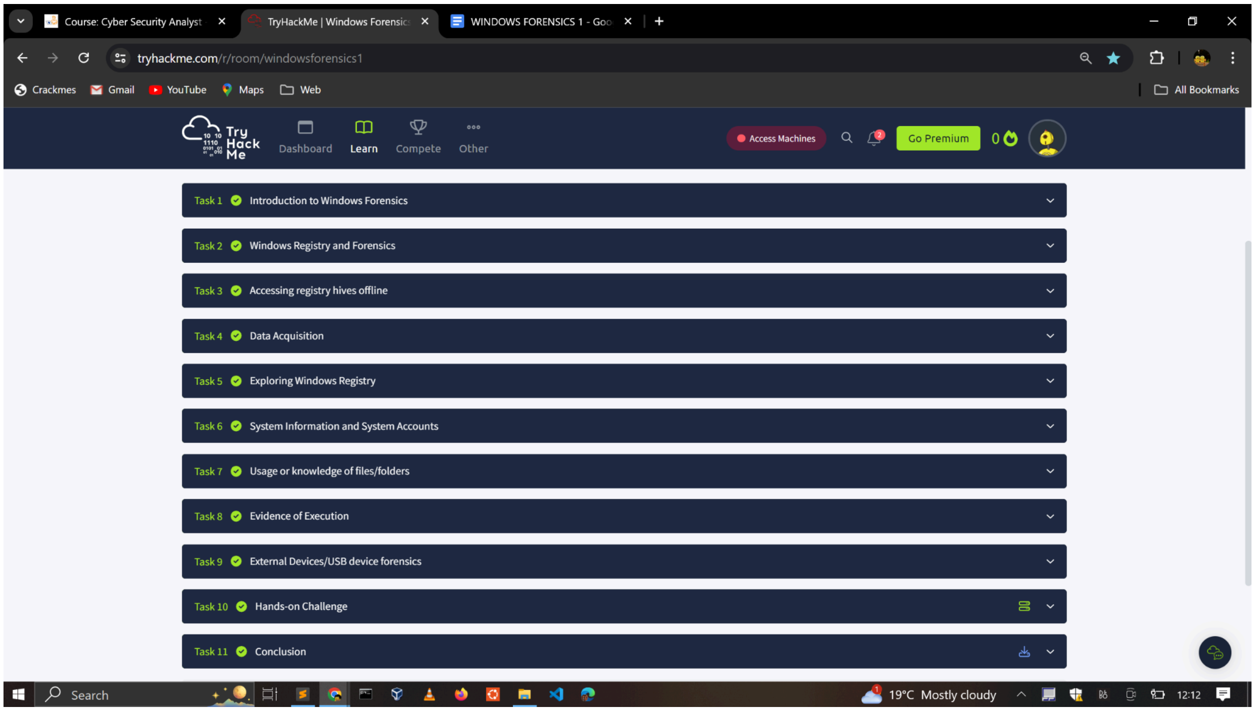
Key name	# valu...	# subkeys	Last write timestamp
C:\Users\THM-4n6\Desktop\triage\C\Wind...			
ROOT	0	1	2021-11-24 18:17:47
C:\Users\THM-4n6\Desktop\SYSTEM_clean			
Unassociated deleted values	19	0	
ROOT	0	17	2021-12-01 12:31:48
Setup	21	15	2021-11-30 15:54:13
DriverDatabase	6	4	2021-11-25 17:04:03
MountedDevices	5	0	2021-11-24 18:40:06
Select	4	0	2019-12-07 09:15:07
HardwareConfig	2	4	2021-12-01 12:31:48
RNG	2	0	2021-12-01 12:31:48
ActivationBroker	0	1	2019-12-07 09:15:08
ControlSet001	0	5	2019-12-07 09:15:07
Enum	31	21	2021-11-30 10:49:05
ACPI	0	21	2021-11-30 10:43:54
ACPI_HAL	0	1	2021-11-24 18:17:40
BTH	0	3	2021-11-24 18:17:47
DISPLAY	0	1	2021-11-24 18:17:47
HDAUDIO	0	1	2021-11-24 18:17:45
HID	0	2	2021-11-24 18:17:44
HTREE	0	1	2021-11-24 18:17:40
IDE	0	1	2021-11-25 17:05:06
PCI	0	20	2021-11-25 17:05:03
PCIIDE	0	1	2021-11-24 18:17:43
ROOT	0	15	2021-11-24 18:17:45
SCSI	0	3	2021-11-30 10:44:08
STORAGE	0	1	2021-11-24 18:17:44
SWD	0	9	2021-11-30 10:49:17
TERMINPUT_BUS	0	1	2021-11-30 10:48:46
TS_USB_HUB_Enumerator	0	1	2021-11-24 18:23:23
UMB	0	1	2021-11-24 18:23:22
USB	0	10	2021-11-24 18:27:01
USBSTOR	0	2	2021-11-24 18:27:02
Disk&Ven_Kingston&Prod_DataTravel...	0	1	2021-11-24 18:25:15
Disk&Ven_USB3.0&Prod_External_De...	0	1	2021-11-24 18:27:02
XENBUS	0	3	2021-11-25 17:05:03
XENVIF	0	1	2021-11-25 17:05:27
Control	11	124	2021-12-01 12:31:56

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

3. MODULE COMPLETION

https://tryhackme.com/p/c1ph3rbnuk



Task 1 ✓ Introduction to Windows Forensics

Task 2 ✓ Windows Registry and Forensics

Task 3 ✓ Accessing registry hives offline

Task 4 ✓ Data Acquisition

Task 5 ✓ Exploring Windows Registry

Task 6 ✓ System Information and System Accounts

Task 7 ✓ Usage or knowledge of files/folders

Task 8 ✓ Evidence of Execution

Task 9 ✓ External Devices/USB device forensics

Task 10 ✓ Hands-on Challenge

Task 11 ✓ Conclusion

4. CONCLUSION

This assignment has taught me how to perform registry forensics with tools like the Zimmerman Registry explorer. I have learned how to extract artefacts like programs set to run on startup, mounted devices, and user accounts from various registry keys and their values. As a security analyst this knowledge will help me gather more evidence of an attack when performing a diigtal forensic investigation.