

# Windows Forensics 1

## Introduction

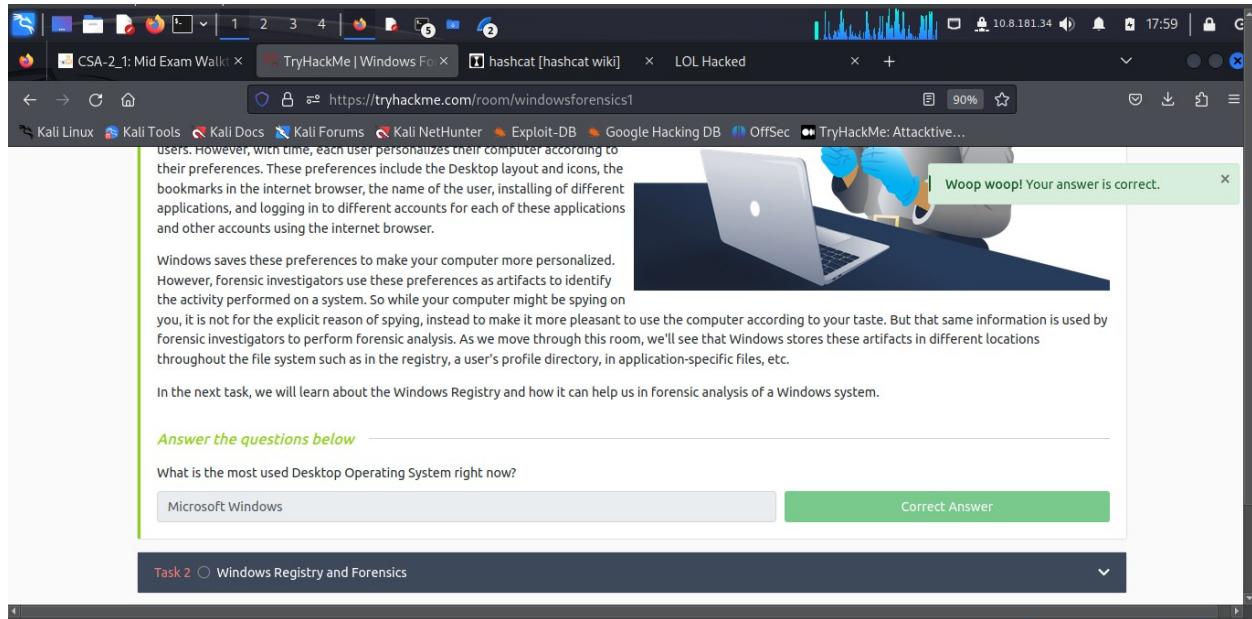
In this chapter the learner is expected to go through Windows registry forensic and cover ten tasks that solidifies his knowledge and skills in Security Analysis.

## Activities

### **Task 1: Introduction to Windows Forensics**

#### **Introduction to Computer Forensics for Windows:**

Essential field of cyber security that involves gathering evidence of activities performed on computers. It is a part of the wider Digital Forensics field, which deals with forensic analysis of all types of digital devices, including recovering, examining, and analyzing data found in digital devices.



### **Task 2: Windows Registry and Forensics**

The screenshot shows a web browser window with the URL <https://tryhackme.com/room/windowsforensics1>. The page content discusses registry keys under HKEY\_CLASSES\_ROOT, mentioning that changes made there affect the HKEY\_LOCAL\_MACHINE\Software\Classes key. It also notes that writing to HKEY\_CURRENT\_USER\Software\Classes will override existing values. A sidebar on the left lists various Kali Linux tools and forums. At the bottom, there's a section for answering questions, a dropdown for Task 3 (Accessing registry hives offline), and another for Task 4 (Data Acquisition). A green notification bar at the top right says "Woop woop! Your answer is correct."

### Task 3: Accessing registry hives

The path for the five main registry hives, DEFAULT, SAM, SECURITY, SOFTWARE, and SYSTEM is: `c:\Windows\System32\Config`

This screenshot shows a continuation of the challenge. It discusses transaction logs (.LOG files) located in the `C:\Windows\System32\Config` directory, which are backups of the registry hives. It also mentions Registry backups in the `C:\Windows\System32\Config\RegBack` directory. A sidebar on the left shows Kali Linux tools and forums. The question section asks for the path to the five main registry hives. A dropdown for Task 4 (Data Acquisition) is shown. A green notification bar at the top right says "Woop woop! Your answer is correct." A progress bar at the bottom right indicates a streak increase and proximity to a badge.

The path for the AmCache hive is: C:\Windows\AppCompat\Programs\Amcache.hve

Woop woop! Your answer is correct.

Some other very vital sources of forensic data are the registry transaction logs and backups. The transaction logs can be considered as the journal or the changelog of the registry hive. Windows often uses transaction logs when writing data to registry hives. This means that the transaction logs can often have the latest changes in the registry that haven't made their way to the registry hives themselves. The transaction log for each hive is stored as a .LOG file in the same directory as the hive itself. It has the same name as the registry hive, but the extension is .LOG. For example, the transaction log for the SAM hive will be located in C:\Windows\System32\Config in the filename SAM.LOG. Sometimes there can be multiple transaction logs as well. In that case, they will have .LOG1, .LOG2 etc., as their extension. It is prudent to look at the transaction logs as well when performing registry forensics.

Registry backups are the opposite of Transaction logs. These are the backups of the registry hives located in the C:\Windows\System32\Config directory. These hives are copied to the C:\Windows\System32\Config\RegBack directory every ten days. It might be an excellent place to look if you suspect that some registry keys might have been deleted/modifed recently.

*Answer the questions below*

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

C:\Windows\System32\Config

Correct Answer Hint

What is the path for the AmCache hive?

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

Correct Answer

Task 4 Data Acquisition

#### Task 4: Data Acquisition

This refers to the process of imaging the system or making a copy of the required data and perform forensics on it.

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

##### KAPE:

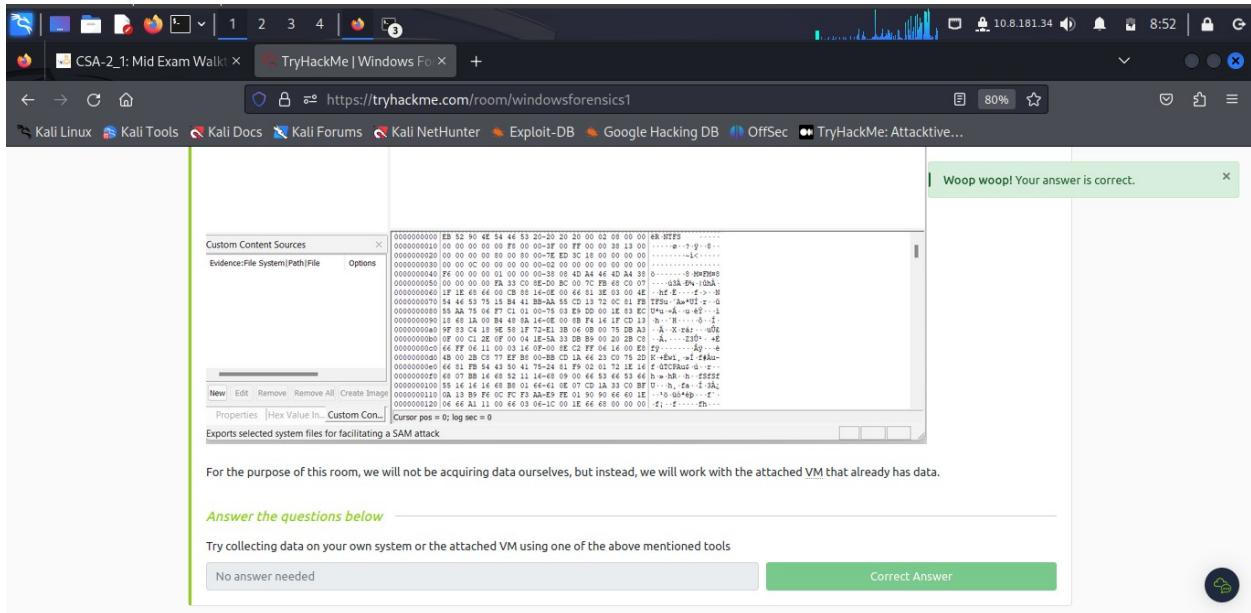
**KAPE** is a live data acquisition and analysis tool which can be used to acquire registry data. It is primarily a command-line tool but also comes with a GUI.

##### Autopsy:

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

##### FTK Imager:

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



## Task 5: Exploring Windows Registry

A tool to view registry hives is needed since the registry editor only works with live systems and can't load exported hives.

### Registry Viewer:

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

### Zimmerman's Registry Explorer:

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

### RegRipper:

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

One shortcoming of RegRipper is that it does not take the transaction logs into account. Registry Explorer must be used to merge transaction logs with the respective registry hives before sending the output to RegRipper for a more accurate result.

One shortcoming of RegRipper is that it does not take the transaction logs into account. We must use Registry Explorer to merge transaction logs with the respective registry hives before sending the output to RegRipper for a more accurate result.

Even though we have discussed these different tools, for the purpose of this room, we will only be using Registry Explorer and some of Eric Zimmerman's tools. The other tools mentioned here will be covered in separate rooms.

**Answer the questions below**

Study the above material to understand the difference between the different tools

No answer needed      Correct Answer

Task 6 System Information and System Accounts

Task 7 Usage or knowledge of files/folders

Task 8 Evidence of Execution

## Task 6: System Information and System Accounts

Value Name	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
BuildID	RegSz	ffffffff-ffff-ffff-ffff-ffffffffffff	00-00
BuildLab	RegSz	19041.vb_release.191206-1406	00-00
BuildLabEx	RegSz	19041.1-and64fe.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		
InstallOnType	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...
ReleaseId	RegSz	2009	00-00
SoftwareType	RegSz	System	00-00-00-00-00-00

Current control set:

The Current Build Number of the machine whose data is being investigated is: **19044**.

Similarly, the `last Known Good` configuration can be found using the following registry value:

`SYSTEM\Select\LastKnownGood`

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

Value Name	Value Type	Data	Value Slack
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.

**Computer Name:**

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

`SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName`

ControlSet contains the last known good configuration as **1**.

Control Sets.

**Computer Name:**

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

`SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName`

Value Name	Value Type	Data	Value Slack
(default)	RegSz	mmmsrvc	02-00-80-00
ComputerName	RegSz	THM-4N6	00-00-00-00

**Time Zone Information:**

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

`SYSTEM\CurrentControlSet\Control\TimeZoneInformation`

The Computer Name of the computer is **THM-4N6**.

Time Zone Information:

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

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

Network Interfaces and Past Networks:

The value of the TimeZoneKeyName is **Pakistan Standard Time**.

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-00-0B-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	1637779828			
T1	RegDword	1637822028			
T2	RegDword	1637854408			
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		
DhcpGatewayHardwareCount	RegDword	1			

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

The DHCP IP address is **192.168.100.58**

The screenshot shows a browser window with the URL <https://tryhackme.com/room/windowsforensics1>. The page displays a table titled "SAM\Domains\Account\Users". The table has columns: User Id, Invalid..., Total L..., Create..., Last Lo..., Last Pa..., Expires..., User N..., Full Na..., Passwo..., Groups, Comment, User C..., Home..., Interne..., Accoun..., Home. There are five rows of data:

User Id	Invalid...	Total L...	Create...	Last Lo...	Last Pa...	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...							DefaultAcount	System Accounts Group	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	Administrator							

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

The RID of the Guest User account is **501**.

The screenshot shows a browser window with the URL <https://tryhackme.com/room/windowsforensics1>. A green message bar at the top right says "Woop woop! Your answer is correct." Below it, there is a section titled "Answer the questions below" with several questions and their answers:

- What is the Current Build Number of the machine whose data is being investigated? Answer: 19044
- Which ControlSet contains the last known good configuration? Answer: 1
- What is the Computer Name of the computer? Answer: THM-4n6
- What is the value of the TimeZoneKeyName? Answer: Pakistan Standard Time
- What is the DHCP IP address? Answer: 192.168.100.58
- What is the RID of the Guest User account? Answer: 501

## Task 7: Usage or knowledge of files/folders

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

Extension	Value Name	Target Name	Link Name	MrU Position	Opened On	Extension Last Opened
	RecentDocs	EZtools	EZtools.lnk	=	0 2021-12-01 13:00:34	=
	RecentDocs	Settings	Settings.lnk	1	2021-11-30 10:56:23	
	RecentDocs	WallpaperSettings.xml	WallpaperSettings.lnk	2	2021-11-30 10:56:21	
	RecentDocs	System and Security	System and Security.lnk	3		
	RecentDocs	::(B006C0E4-D293-4F75-8A90-CB05B6477EEE)	System.lnk	4		
	RecentDocs	KAPE	KAPE.lnk	5		
	RecentDocs	Get-KAPEUpdate.ps1	Get-KAPEUpdate.lnk	6	2021-11-24 18:18:48	
	RecentDocs	ChangeLog.txt	ChangeLog.lnk	7	2021-11-24 18:18:48	
	Folder	Settings	Settings.lnk	0	2021-11-30 10:56:23	
	Folder	System and Security	System and Security.lnk	1		
	Folder	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	

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

The EZTools was opened on: 2021-12-01 13:00:34.

NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU

Value	Icon	Shell Type	MRU Positi...	Created On	Modified On	Accessed On	First Interacted	Last Interacted	Has Explored	Miscellaneous
No im...			=	=	=	=	=	=	<input checked="" type="checkbox"/>	<input type="checkbox"/>
My Computer	Root folder: GUID		0					2021-12-01 13:06:47	<input checked="" type="checkbox"/>	
KAPE	Directory		1	2021-11-25 03:34:14	2021-11-25 03:34:14	2021-11-25 03:34:14			<input checked="" type="checkbox"/>	NTFS file system
Home Folder	Root folder: GUID		2				2021-11-24 18:20:02		<input checked="" type="checkbox"/>	
Search Folder	Users property view		3				2021-11-30 11:08:01		<input type="checkbox"/>	
Search Folder	Users property view		4				2021-11-30 11:08:52		<input checked="" type="checkbox"/>	
Control Panel	Root folder: GUID		5						<input type="checkbox"/>	
E:\	Users property view: Drive letter		6				2021-11-24 18:20:02		<input checked="" type="checkbox"/>	

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

The last time My Computer interacted with was on 2021-12-01 at 13:06:47

The screenshot shows a browser window with the URL <https://tryhackme.com/room/windowsforensics1>. The page content discusses "Open/Save and LastVisited Dialog MRUs". It includes a screenshot of the Windows Registry Editor showing the key `NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDMRU`. The table lists entries for "CIDSizeMRU", "LastVisitedPidMRU", and "OpenSavePidMRU". One entry for "notepad.exe" is highlighted, showing the absolute path `C:\Program Files\Amazon\Ec2ConfigService\Settings` and the timestamp `2021-11-30 10:56:19`.

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

When we open or save a file, a dialog box appears asking us where to save or open that file from. It might be noticed that once we open/save a file at a specific location, Windows remembers that location. This implies that we can find out recently used files if we get our hands on this information. We can do so by examining the following registry keys

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDMRU

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

**Windows Explorer Address/Search Bars:**

Another way to identify a user's recent activity is by looking at the paths typed in the Windows Explorer address bar or searches performed using the following registry keys, respectively.

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

The Absolute Path of the file opened using notepad.exe is: `C:\ProgramFiles\Amazon\Ec2ConfigService\Settings`

The screenshot shows a challenge interface on TryHackMe. The user has answered the following questions correctly:

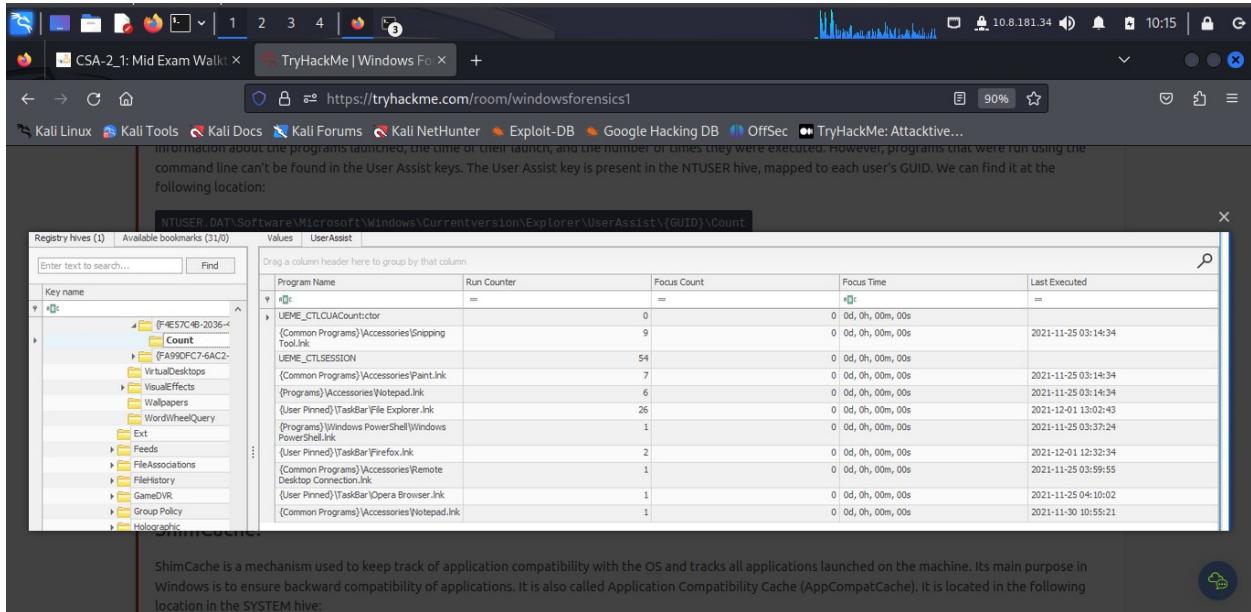
- When was EzTools opened? Answer: 2021-12-01 13:00:34
- At what time was My Computer last interacted with? Answer: 2021-12-01 13:06:47
- What is the Absolute Path of the file opened using notepad.exe? Answer: `C:\ProgramFiles\Amazon\Ec2ConfigService\Settings`
- When was this file opened? Answer: 2021-11-30 10:56:19

The interface also shows three tasks listed below the answers:

- Task 8: Evidence of Execution
- Task 9: External Devices/USB device forensics
- Task 10: Hands-on Challenge

## Task 8: Evidence of Execution

The number of times the File Explorer was launched is: **26**.

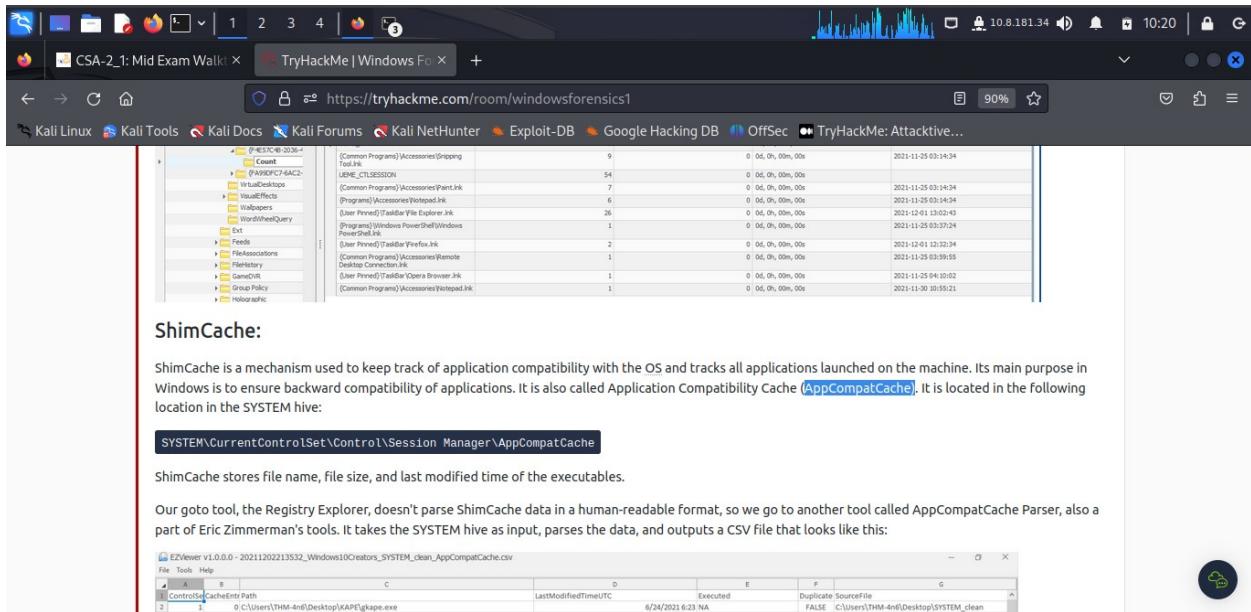


The screenshot shows the Registry Explorer interface on a Kali Linux system. The left pane displays the registry tree under 'Registry hives (1)'. The right pane shows a table titled 'UserAssist' with columns: Program Name, Run Counter, Focus Count, Focus Time, and Last Executed. The table lists various applications and their execution counts. The 'File Explorer' entry has a 'Run Counter' of 26.

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
UEME_CTLCLIAutoRun	0	0	00:00,00m,00s	2021-11-25 03:14:34
UEME_CTLSESSION	54	0	00:00,00m,00s	2021-11-25 03:14:34
File Explorer	26	0	00:00,00m,00s	2021-12-01 13:02:43
PowerShell	1	0	00:00,00m,00s	2021-11-25 03:37:24
Firefox	2	0	00:00,00m,00s	2021-12-01 12:32:34
Opera Browser	1	0	00:00,00m,00s	2021-11-25 04:10:02
Notepad	1	0	00:00,00m,00s	2021-11-30 10:55:21

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:

Another name for ShimCache is **AppCompatCache**.



The screenshot shows the Registry Explorer interface on a Kali Linux system. The left pane displays the registry tree under 'Registry hives (1)'. The right pane shows a table titled 'AppCompatCache' with columns: Program Name, Run Counter, Focus Count, Focus Time, and Last Executed. The table lists various applications and their execution counts. The 'File Explorer' entry has a 'Run Counter' of 26.

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
File Explorer	26	0	00:00,00m,00s	2021-11-25 03:14:34
PowerShell	1	0	00:00,00m,00s	2021-11-25 03:14:34
Firefox	2	0	00:00,00m,00s	2021-12-01 12:32:34
Opera Browser	1	0	00:00,00m,00s	2021-11-25 04:10:02
Notepad	1	0	00:00,00m,00s	2021-11-30 10:55:21

**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:

**SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache**

ShimCache stores file name, file size, and last modified time of the executables.

Our goto tool, the Registry Explorer, doesn't parse ShimCache data in a human-readable format, so we go to another tool called AppCompatCache Parser, also a part of Eric Zimmerman's tools. It takes the SYSTEM hive as input, parses the data, and outputs a CSV file that looks like this:



A	B	C	D	E	F	G
ControlCacheEntryPath	LastModifiedTimeUTC	Executed	Duplicate	SourceFile		
0 C:\Users\THM-4n\Desktop\KAP\lgkape.exe	6/24/2021 6:23 NA	TRUE	FALSE	C:\Users\THM-4n\Desktop\SYSTEM_clean		

Artifacts that saves SHA1 hashes of the executed programs is **AmCache**.

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

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

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

**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:

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

This is how Registry Explorer parses the AmCache hive:

The artifacts that saves the full path of the executed programs is **bam/dam**.

Answer the questions below

How many times was the File Explorer launched?

 Correct Answer Hint

What is another name for ShimCache?

 Correct Answer

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

 Correct Answer

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

 Correct Answer

Task 9 ○ External Devices/USB device forensics

Task 10 ○ Hands-on Challenge

## Task 9: External Devices/USB device forensics

The serial number of the device from the manufacturer 'Kingston' is **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	Rev_PMAP	<0>	(e251921f-4da2-11)	1C6f654E59A3B0C0	Kingston	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_Dev	Rev_SDM1	<0>	(f5269d66-49e-11)	0123456789ABCDEF	USB3.0 External Device	2021-11-24 18:27...	2021-11-24 18:27...	2021-11-24 18:27...

The name of the device is **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	Rev_PMAP	<0>	(e251921f-4da2-11)	1C6f654E59A3B0C0	Kingston	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_Dev	Rev_SDM1	<0>	(f5269d66-49e-11)	0123456789ABCDEF	USB3.0 External Device	2021-11-24 18:27...	2021-11-24 18:27...	2021-11-24 18:27...

The friendly name of the device from the manufacturer 'Kingston' is **USB**.

**USB device Volume Name:**

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

Software\Microsoft\Windows Portable Devices\Devices

Timestamp	Device	Serial Number	Guid	Friendly Name
2021-11-25 07:16:54			{E251921F-DAZ-1EC-A7B3-001A7DDA7110}	USB
2021-11-25 07:16:54			{F529A006-409E-1EC-A7B2-001A7DDA7110}	New Volume

*Answer the questions below*

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

What is the name of this device?  
Kingston Data Traveler 2.0 USB Device

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

We can compare the GUID we see here in this registry key and compare it with the Disk ID we see on keys mentioned in device identification. We can also look at these two screenshots and answer Question # 3.

Combining all of this information, we can create a fair picture of any USB devices that were connected to the machine we're investigating.

*Answer the questions below*

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

What is the name of this device?  
Kingston Data Traveler 2.0 USB Device

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

Task 10 ○ Hands-on Challenge

Task 11 ○ Conclusion

## Task 10: Hands-on Challenge

The screenshot shows a web browser window with two tabs: "CSA-2\_1: Mid Exam Walkthrough" and "TryHackMe | Windows Forensics". The main content area displays a challenge from tryhackme.com. The challenge asks for the number of user-created accounts (3), the username of the account that has never been logged in (thm-user2), the password hint for user THM-4n6 (count), the date when 'Changelog.txt' was accessed (2021-11-21 18:18:48), and the date when a USB device was last connected (2021-11-21 18:40:06). Below the challenge is a "Correct Answer" button and a "Hint" button.

On the right side of the screen, a Windows desktop environment is visible. It includes a taskbar with icons for Autopsy, Firefox, Google Chrome, Microsoft Edge, and File Explorer. A file explorer window titled "RegRipper v.3.0" is open, showing the results of a scan on a file named "test1.txt". The results indicate that the hive is not dirty and lists several registry keys and their details. The desktop background is blue, and the system tray shows the date and time as 11/29/2023 at 1:10 PM.

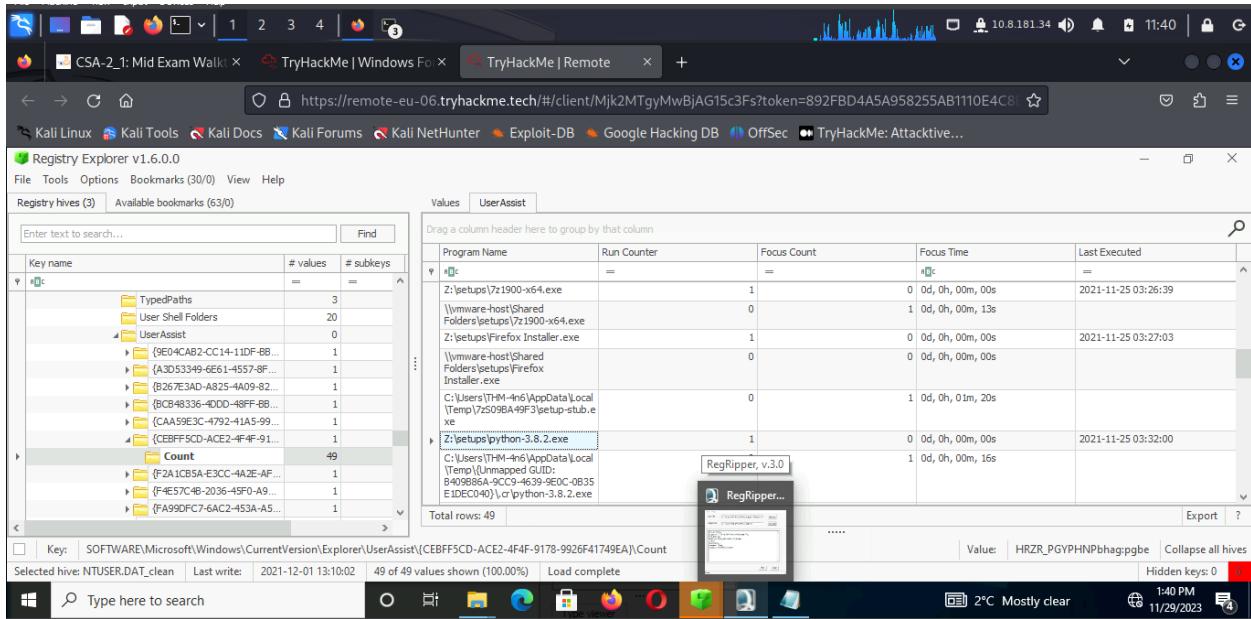
The username of the account that has never been logged in is **thm-user2**.

The screenshot shows a Registry Explorer window titled "Registry Explorer v1.6.0.0". The left pane displays a tree view of registry keys under "C:\Users\THM-4n6\...". The "Users" key is expanded, showing subkeys like "000001F4", "000001F5", "000001F7", "000001F8", and "000003E9". The right pane shows a table with columns: Key name, # values, # subkeys, Last write timestamp, Total, Created On, Last Logon, Last Write, Expires On, User Name, Full Name, Password, etc. One row in the table corresponds to the user "thm-user2", which is highlighted. The status bar at the bottom indicates "Total rows: 7" and "Load complete".

The password hint for the user THM-4n6 is **count**.

The file 'Changelog.txt' was accessed on 2021-11-21 18:18:48

The complete path from where the python 3.8.2 installer was run is Z:\setups\python-3.8.2.exe



The USB device with the friendly name 'USB' last connected on **2021-11-21 18:40:06**

**Answer the questions below**

How many user created accounts are present on the system?  
3 Correct Answer Hint

What is the username of the account that has never been logged in?  
thm-user2 Correct Answer Hint

What's the password hint for the user THM-4n6?  
count Correct Answer Hint

When was the file 'Changelog.txt' accessed?  
2021-11-21 18:18:48 Correct Answer Hint

What is the complete path from where the python 3.8.2 installer was run?  
Z:\setups\python-3.8.2.exe Correct Answer Hint

When was the USB device with the friendly name 'USB' last connected?  
2021-11-21 18:40:06 Correct Answer Hint

**Woop woop! Your answer is correct.**

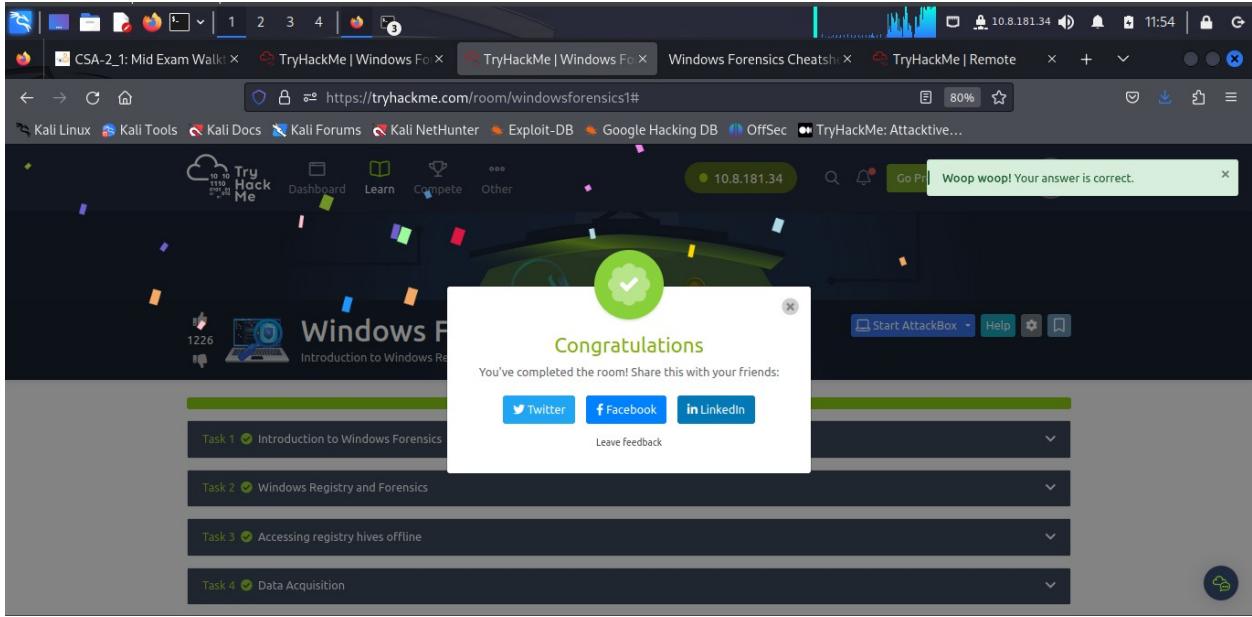
Name	Date modified	Type
Default	12/1/2021 6:10 PM	File folder
Public	12/1/2021 6:09 PM	File folder
THM-4n6	12/1/2021 6:11 PM	File folder
thm-user	12/1/2021 6:09 PM	File folder

### Task 11: Conclusion

I have learned how to gather basic information about a computer and its users, identify which files they used, which programs they ran, and any external devices connected to the system.

### Conclusion

Using the registry access is important part of a security analyst in that it gives me the power to know which user made which type of configuration and collecting relevant information that can be used in digital forensic.



Completion Link: <https://tryhackme.com/room/windowsforensics1#>