

THM__Windows Forensics 1 [Introduction to Windows Registry Forensics]

<https://tryhackme.com/room/windowsforensics1>

Task 1 Introduction to Windows Forensics

TLDR: Mostly a summary of how digital forensics has been used, defining what an "artifact" is, and how Windows keeps tabs on users to provide a more personalized experience.

Answer the questions below

What is the most used Desktop Operating System right now?

Microsoft Windows

What is the term used to define a piece of evidence of human activity?

Artifact

Task 2 Windows Registry and Forensics

TLDR: Windows registry contains config data; consist of keys and values; a **registry hive** is a group of keys, subkeys and values stored in a single file

regedit.exe

The registry on any Windows system contains the following five root keys:

1. HKEY_CURRENT_USER
2. HKEY_USERS
3. HKEY_LOCAL_MACHINE
4. HKEY_CLASSES_ROOT--this information is stored under both the HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER keys
5. HKEY_CURRENT_CONFIG

Hives (OFFLINE)

Now, 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 these standard root keys. 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)

Apart from these hives, two other hives containing user information can be found in the User profile directory. For Windows 7 and above, a user's profile directory is located in C:\Users\<username>\ where the hives are:

1. **NTUSER.DAT** (mounted on HKEY_CURRENT_USER when a user logs in)
2. **USRCLASS.DAT** (mounted on HKEY_CURRENT_USER\Software\CLASSES)

The USRCLASS.DAT hive is located in the directory C:\Users\<username>\AppData\Local\Microsoft\Windows.

The NTUSER.DAT hive is located in the directory C:\Users\<username>\.

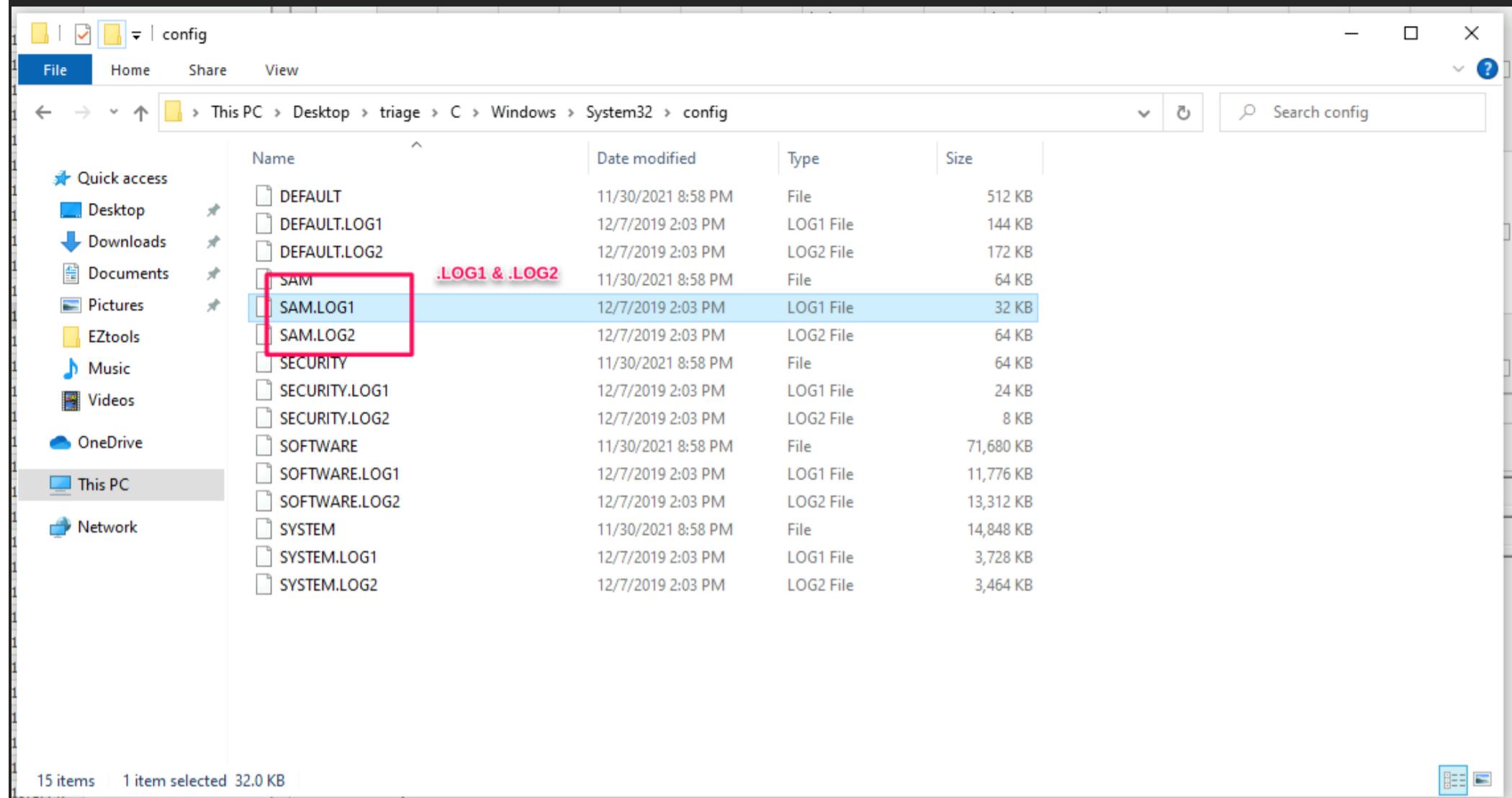
Remember that NTUSER.DAT and USRCLASS.DAT are hidden files.

The Amcache Hive:

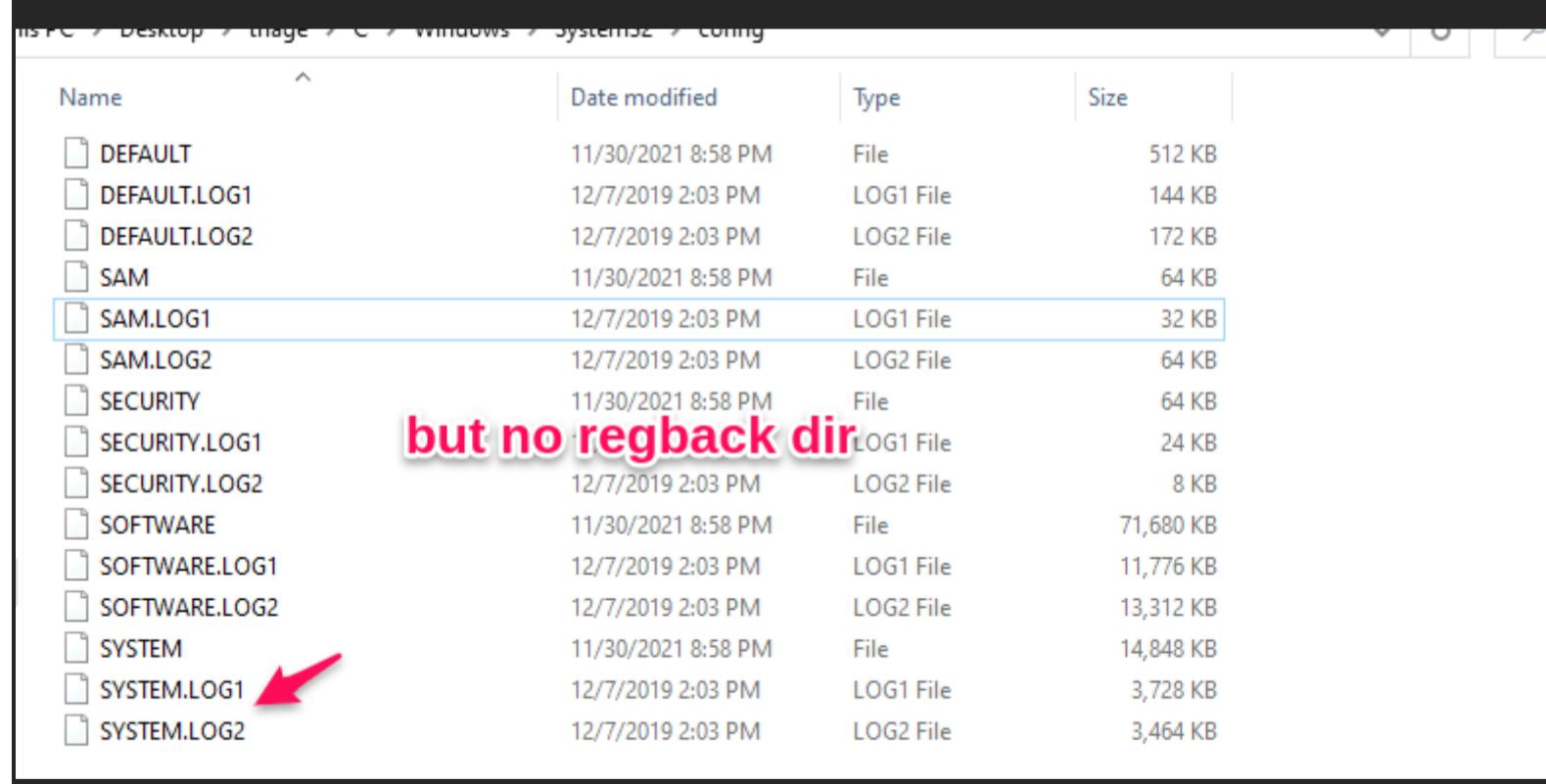
Apart from these files, there is another very important hive called the AmCache hive. This hive is located in C:\Windows\AppCompat\Programs\Amcache.hve. Windows creates this hive to save information on programs that were recently run on the system.

Transaction Logs and Backups:

Some other very vital sources of forensic data are the registry transaction logs and backups. The transaction logs can be considered as the journal of 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/modified recently.**



Answer the questions below

What is the short form for HKEY_LOCAL_MACHINE?

HKLM

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
```

Task 3 Exploring Windows Registry

Data Acquisition:

Though we can view the registry through the registry editor, the forensically correct method is to acquire a copy of this data and perform analysis on that. However, when we go to copy the registry hives from %WINDIR%\System32\Config, we cannot because it is a restricted file. So, what to do now?

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

KAPE:

<https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-cape/training>

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. The below screenshot shows what the KAPE GUI looks like. We have already selected all the settings to extract the registry data using KAPE in this screenshot.

Tried to download for free, link in email did not work. I'll look into this later.

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. It will look similar to what you see in the screenshot below.

Honestly, there are too many hoops to install autopsy on Linux

Used this to install it

```
sudo dpkg -i --force-overwrite [filename]
```

Then run:

```
sudo apt -f install
```

to fix if any broken packages.

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. Below you can see the option to Export files as highlighted in the screenshot.

Windows only, it seems!

Another way you can extract Registry files from FTK Imager is through the Obtain Protected Files option. This option is only available for live systems and is highlighted in the screenshot below. This option allows you to extract all the registry hives to a location of your choosing. However, it will not copy the Amcache.hve file, which is often necessary to investigate evidence of programs that were last executed.

Exploring the extracted files:

Once we have extracted the registry hives, we need a tool to view these files as we would in the registry editor. Since the registry editor only works with live systems and can't load exported hives, we can use the following tools:

Registry Viewer:

As we can see in the screenshot below, 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:

 Get-ZimmermanTools.zip 15 kB

Eric Zimmerman has developed a handful of [tools](#) that are very useful for performing Digital Forensics and Incident Response. One of them is the Registry Explorer. It looks like the below screenshot. 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. We will explore these in more detail in the upcoming tasks.

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.

RegRipper is available in both a CLI and GUI form which is shown in the screenshot below.

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.

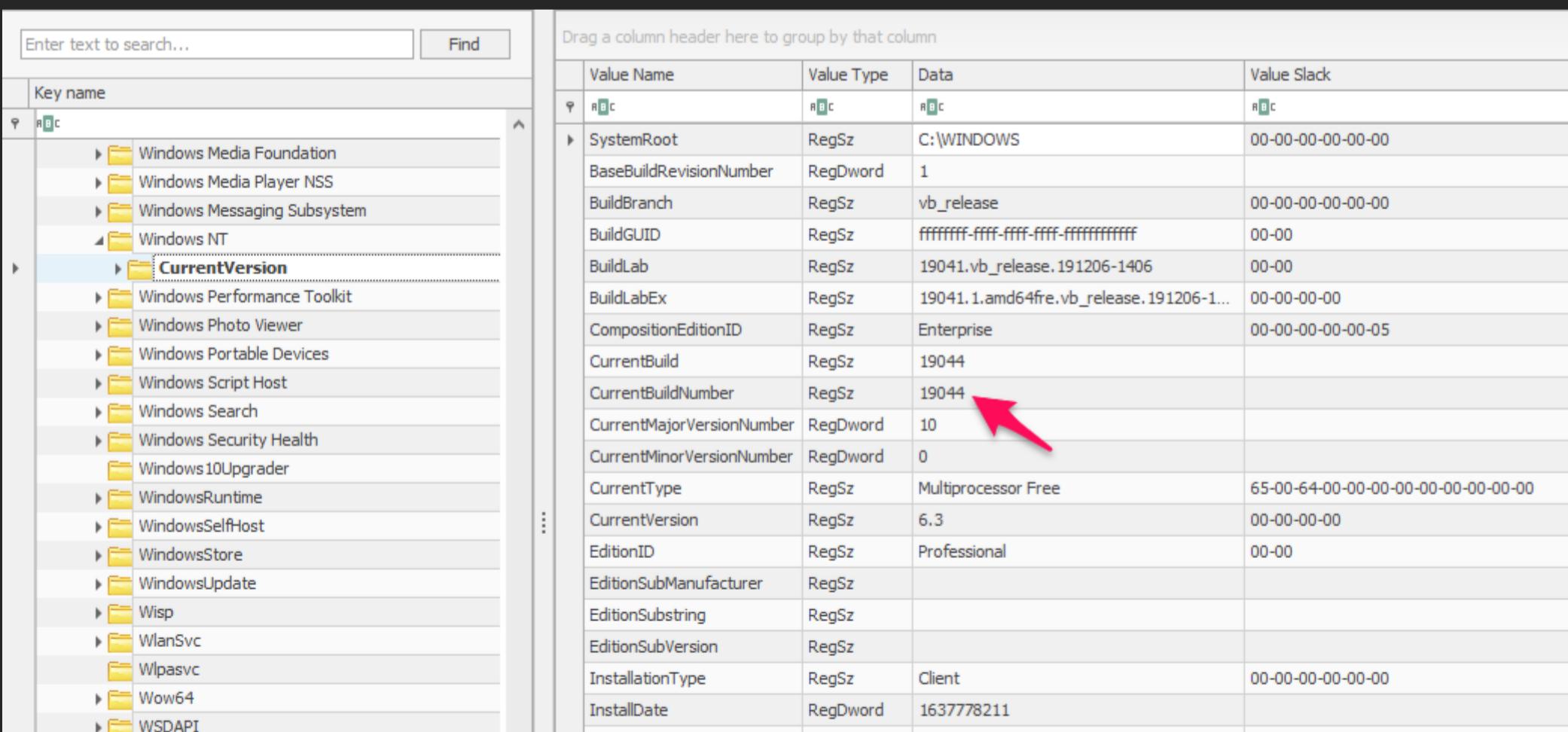
NO QUESTIONS**Task 4 System Information and System Accounts**

Step 1: gather system information and account info

To find the OS version, we can use the following registry key:

SOFTWARE\Microsoft\Windows NT\CurrentVersion

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



Drag a column header here to group by that column				
	Value Name	Value Type	Data	Value Slack
▼ RBC	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	65-00-64-00-00-00-00-00-00-00-00-00-00-00-00-00
	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

WwanSvc
XAML
Mozilla

TryHackMe - Evernote			
ReleaseId	RegSz	2009	00-00
SoftwareType	RegSz	System	00-00-00-00-00-00

Current control set:

The hives containing the machine's configuration data used for controlling system startup are called Control Sets. Commonly, we will see two Control Sets, ControlSet001 and ControlSet002, in the SYSTEM hive on a machine. In most cases, ControlSet001 will point to the Control Set that the machine booted with, and ControlSet002 will be the last known good configuration. Their locations will be:

SYSTEM\ControlSet001

SYSTEM\ControlSet002

Windows creates a volatile Control Set when the machine is live, called the CurrentControlSet (HKLM\SYSTEM\CurrentControlSet). For getting the most accurate system information, this is the hive that we will refer to. We can find out which Control Set is being used as the CurrentControlSet by looking at the following registry value:

SYSTEM\Select\Current

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

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

Value Name	Value Type	Data	Value Slack
(default)	RegSz	mmmsrvc	02-00-B0-00
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

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

Enter text to search... Find

Key name

Terminal Server
TimeZoneInformation
Ubpmp
UnitedVideo
USB
usbflags
usbstor
VAN
Version
Video
WalletService

Drag a column header here to group by that column

Value Name	Value Data	Value Data Raw
RBC	RBC	RBC
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	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	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.

Network Interfaces and Past Networks:

The following registry key will give a list of network interfaces on the machine we are investigating:

SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces

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

Enter text to search... Find 🔍

Key name R C

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
EnableDHCP	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
Domain	RegSz			<input type="checkbox"/>	<input type="checkbox"/>
NameServer	RegSz			<input type="checkbox"/>	<input type="checkbox"/>
DhcpIPAddress	RegSz	192.168.100.58 BA-00-B8-16-0A-00		<input type="checkbox"/>	<input type="checkbox"/>
DhcpSubnetMask	RegSz	255.255.255.0		<input type="checkbox"/>	<input type="checkbox"/>
DhcpServer	RegSz	192.168.100.1	35-00-00-00-65-00-7...	<input type="checkbox"/>	<input type="checkbox"/>
Lease	RegDword	86400		<input type="checkbox"/>	<input type="checkbox"/>
LeaseObtainedTime	RegDword	1637778828		<input type="checkbox"/>	<input type="checkbox"/>
T1	RegDword	1637822028		<input type="checkbox"/>	<input type="checkbox"/>
T2	RegDword	1637854428		<input type="checkbox"/>	<input type="checkbox"/>
LeaseTerminatesTime	RegDword	1637865228		<input type="checkbox"/>	<input type="checkbox"/>
AddressType	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
IsServerNapAware	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
DhcpConnForceBroadcastFlag	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
DhcpNameServer	RegSz	192.168.100.1		<input type="checkbox"/>	<input type="checkbox"/>
DhcpDefaultGateway	RegMultiSz	192.168.100.1	00-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
DhcpSubnetMaskOpt	RegMultiSz	255.255.255.0	00-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
DhcpInterfaceOptions	RegBinary	FC-00-00-00-00-00-0...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
DhcpGatewayHardware	RegBinary	C0-A8-64-01-06-00-...	2E-00-30-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
DhcpGatewayHardwareCount	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>

Each Interface is represented with a unique identifier (GUID) subkey, which contains values relating to the interface's TCP/IP configuration. This key will provide us with information like IP addresses, DHCP IP address and Subnet Mask, DNS Servers, and more. **This information is significant because it helps you make sure that you are performing forensics on the machine that you are supposed to perform it on.**

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

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed

Registry hives (7)		Available bookmarks (108/0)		Find	
Enter text to search...				Values	
Key name	Value Name	Value Type	Data	Value Slack	Is Deleted
past networks connect to can be found here	R&C	R&C	R&C	R&C	<input checked="" type="checkbox"/>
	ProfileGuid	RegSz	{A3D7C922-7D34-4688	CA-63-7F-00-CA-99	<input type="checkbox"/>

Unmanaged
010103000F0000F0080000000F0000F04
010103000F0000F0080000000F0000F05D50DC
010103000F0000F0080000000F0000F0744CC
010103000F0000F0080000000F0000F07BEDES

Description	RegSz	Network 2				
Source	RegDword	8				
DnsSuffix	RegSz	eu-west-1.compute.int...	F5-48-B1-00-F5-57			
FirstNetwork	RegSz	Network 2				
DefaultGatewayMac	RegBinary	02-D4-DB-FF-33-74	87-01-C0-51-87-01			

These registry keys contain past networks as well as the last time they were connected. The last write time of the registry key points to the last time these networks were connected.

Autostart Programs (Autoruns):

The following registry keys include information about programs or commands that run when a user logs on.

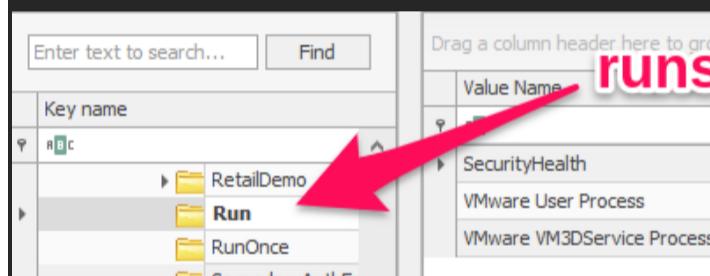
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce

SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run

SOFTWARE\Microsoft\Windows\CurrentVersion\Run



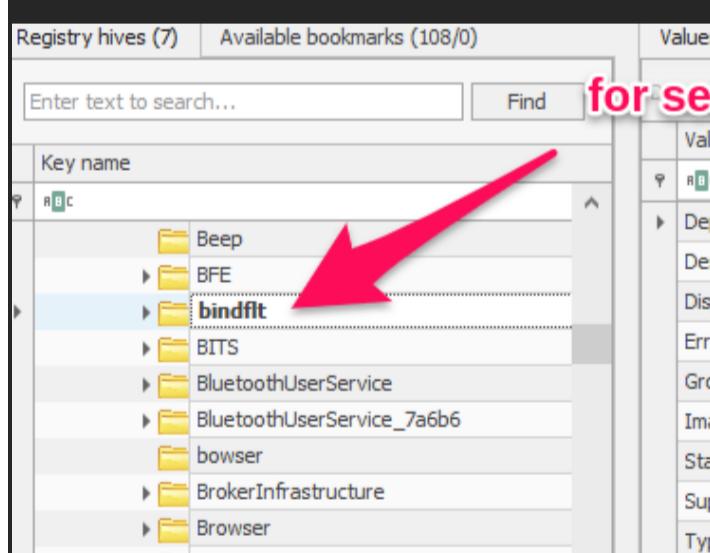
runs on logon

Value Name	Type	Data	Value Slack	Is Deleted	Data Record Reallocated
RetailDemo	RegDword	00000000	00-00-00-00		
Run	RegExpandSz	%windir%\system32\Secu...	00-00-00-00		
RunOnce	RegSz	"C:\Program Files\VMware...	00-00		
SecondaryAuthE...	RegSz	"C:\WINDOWS\system32\...	47-00		

The following registry key contains information about services:

SYSTEM\CurrentControlSet\Services

Notice the Value of the Start key in the screenshot below.



for services, look for bindfit

Value Name	Type	Data	Value Slack	Is Deleted	Data Record Reallocated
DependOnService	RegMultiSz	FltMgr	00-00-00-00		
Description	RegSz	@%systemroot%\system...	00-00-00-00		
DisplayName	RegSz	@%systemroot%\system...	00-00-00-00		
ErrorControl	RegDword	1			
Group	RegSz	FSFilter Top	00-00		
ImagePath	RegExpandSz	\SystemRoot\system32\d...	00-00		
Start	RegDword	2			
SupportedFeatures	RegDword	7			
Type	RegDword	2			

In this registry key, if the start key is set to 0x02, this means that this service will start at boot.

SAM hive and user information:

The SAM hive contains user account information, login information, and group information. This information is mainly located in the following location:

SAM\Domains\Account\Users

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

Enter text to search...	Find	Drag a column header here to group by that column
-------------------------	------	---

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				<input checked="" type="checkbox"/>	<input type="checkbox"/>
503	0	0	2021-1...					DefaultA ccount			System Managed Accounts Group	A user account managed by the system.				<input checked="" type="checkbox"/>	<input type="checkbox"/>
504	0	0	2021-1...		2021-1...			WDAGUti lityAccou nt				A user account managed and used by the system for Windows Defender Application Guard scenarios				<input checked="" type="checkbox"/>	<input type="checkbox"/>
1001	0	19	2021-1...	2021-1...	2021-1...	2021-1...		THM-4n6		count	Administr				<input type="checkbox"/>	<input type="checkbox"/>	

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.

Answer the questions below

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

19044

Which ControlSet contains the last known good configuration?

1

What is the Computer Name of the computer?

THM-4N6

What is the value of the TimeZoneKeyName?

Pakistan Standard Time

What is the DHCP IP address

192.168.100.58

What is the RID of the Guest User account?

501

Task 5 Usage or knowledge of files/folders

Recent Files:

Windows maintains a list of recently opened files for each user. As we might have seen when using Windows Explorer, it shows us a list of recently used files. This information is stored in the NTUSER hive and can be found on the following location:

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

Registry hives (7)		Available bookmarks (108/0)		Values	Recent documents										
				Enter text to search...	Find										
				Drag a column header here to group by that column											
Key name	RBC	Extension	RBC	Value Name	RBC	Target Name	RBC	Mru Position	RBC	Opened On	RBC	Extension	RBC	Last Opened	RBC
RecentDocs	RBC	RBC	RBC	RBC	RBC	RBC	RBC	=	RBC	RBC	RBC	RBC	RBC	RBC	RBC
RecentDocs	RBC	RBC	RBC	RBC	RBC	EZtools	RBC	RBC	RBC	RBC	RBC	RBC	RBC	RBC	RBC
RecentDocs	RBC	RBC	RBC	RBC	RBC	Settings	RBC	RBC	RBC	RBC	RBC	RBC	RBC	RBC	RBC
RecentDocs	RBC	RBC	RBC	RBC	RBC	WallpaperSettings.xml	RBC	RBC	RBC	RBC	RBC	RBC	RBC	RBC	RBC
RecentDocs	RBC	RBC	RBC	RBC	RBC	System and Security	RBC	RBC	RBC	RBC	RBC	RBC	RBC	RBC	RBC
RecentDocs	RBC	RBC	RBC	RBC	RBC	::{B806C0E4-D293-4F75-8A90-CB05B6477E}	RBC	RBC	RBC	RBC	RBC	RBC	RBC	RBC	RBC

			EE}				
RecentDocs	1	KAPE	KAPE.Ink	5			
RecentDocs	0	Get-KAPEUpdate.ps1	Get-KAPEUpdate.Ink	6			2021-11-24 18:18:48
RecentDocs	2	ChangeLog.txt	ChangeLog.Ink	7			2021-11-24 18:18:48
Folder	2	Settings	Settings.Ink	0	2021-11-30 10:56:23		
Folder	1	System and Security	System and Security.Ink	1			
Folder	0	KAPE	KAPE.Ink	2			
.xml	0	WallpaperSettings.xml	WallpaperSettings.Ink	0	2021-11-30 10:56:21		
.txt	0	ChangeLog.txt	ChangeLog.Ink	0	2021-11-24 18:18:48		
.ps1	0	Get-KAPEUpdate.ps1	Get-KAPEUpdate.Ink	0	2021-11-24 18:18:48		

Registry Explorer allows us to sort data contained in registry keys quickly. For example, the Recent documents tab arranges the Most Recently Used (MRU) file at the top of the list. Registry Explorer also arranges them so that the Most Recently Used (MRU) file is shown at the top of the list and the older ones later.

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 following registry key:

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

Registry Explorer also lists the Last Opened time of the files. Answer Question # 1 by looking at the above screenshot.

Office Recent Files:

Similar to the Recent Docs maintained by Windows Explorer, Microsoft Office also maintains a list of recently opened documents. This list is also located in the NTUSER hive. It can be found in the following location:

NTUSER.DAT\Software\Microsoft\Office\VERSION

The version number for each Microsoft Office release is different. An example registry key will look like this:

NTUSER.DAT\Software\Microsoft\Office\15.0\Word

Here, the 15.0 refers to Office 2013. A list of different Office releases and their version numbers can be found on [this link](#).

Starting from Office 365, Microsoft now ties the location to the user's [live ID](#). In such a scenario, the recent files can be found at the following location.

NTUSER.DAT\Software\Microsoft\Office\VERSION\UserMRU\LiveID_####\FileMRU

In such a scenario, the recent files can be found at the following location. This location also saves the complete path of the most recently used files.

ShellBags:

When any user opens a folder, it opens in a specific layout. Users can change this layout according to their preferences. These layouts can be different for different folders. This information about the Windows 'shell' is stored and can identify the Most Recently Used files and folders. Since this setting is different for each user, it is located in the user hives. We can find this information on the following locations:

USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags

USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU

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

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
Desktop										
My Computer	No im...		=	=	=	=	=	=	<input checked="" type="checkbox"/>	
KAPE										
Home Folder		Root folder: GUID	0					2021-12-01 13:06:47	<input checked="" type="checkbox"/>	
Search Folder		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
Search Folder		Root folder: GUID	2				2021-11-24 18:20:02		<input checked="" type="checkbox"/>	
Control Panel		Users property view	3				2021-11-30 11:08:01		<input type="checkbox"/>	
E:\		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"/>	

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

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

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

Enter text to search...		Find	Drag a column header here to group by that column				
Key name			Value Name	Mru Position	Executable	Absolute Path	Opened On
	RBC	=	RBC	=	RBC	RBC	=
	CIDSizeMRU		0	0	notepad.exe	My Computer\{C:\Program Files\Amazon\Ec2ConfigService\Settings	2021-11-30 10:56:19
	LastVisitedPidlMRU						
	OpenSavePidlMRU						

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

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

Here is how the TypedPaths key looks like in Registry Explorer:

Enter text to search...		Find	Drag a column header here to group by that column					
Key name		#	Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
	RBC		RBC	RBC	RBC	RBC	<input type="checkbox"/>	<input type="checkbox"/>
▶	TypedPaths		url1	RegSz	C:\	72-00-6F-00-67-00-72-00-61...	<input type="checkbox"/>	<input type="checkbox"/>
▶	User Shell Folders		url2	RegSz	C:\Program Files	33-00-32-00-00-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
▶	UserAssist		url3	RegSz	C:\Windows\System32	60-53-09-00	<input type="checkbox"/>	<input type="checkbox"/>

Answer the questions below

When was EZtools opened?

2021-12-01 13:00:34

At what time was My Computer last interacted with?

2021-12-01 13:06:47

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

C:\Program Files\Amazon\Ec2ConfigService\Settings

When was this file opened?

2021-11-30 10:56:19

Task 6 Evidence of Execution

UserAssist:

Windows keeps track of applications launched by the user using Windows Explorer for statistical purposes in the User Assist registry keys. These keys contain information about the programs launched, the time of their launch, and the number of times they were executed. However, **programs that were run using the command line can't be found in the User Assist keys.** The User Assist key is present in the NTUSER hive, mapped to each user's GUID. We can find it at the following location:

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
Notepad.lnk	=	=	Notepad.lnk	=
UEME_CTLCUACount:ctor	0	0	0 0d, 0h, 00m, 00s	2021-11-25 03:14:34
{Common Programs}\Accessories\Snipping Tool.lnk	9	0	0 0d, 0h, 00m, 00s	
UEME_CTLSESSION	54	0	0 0d, 0h, 00m, 00s	
{Common Programs}\Accessories\Paint.lnk	7	0	0 0d, 0h, 00m, 00s	2021-11-25 03:14:34
{Programs}\Accessories\Notepad.lnk	6	0	0 0d, 0h, 00m, 00s	2021-11-25 03:14:34
{User Pinned}\TaskBar\File Explorer.lnk	26	0	0 0d, 0h, 00m, 00s	2021-12-01 13:02:43
{Programs}\Windows PowerShell\Windows PowerShell.lnk	1	0	0 0d, 0h, 00m, 00s	2021-11-25 03:37:24
{User Pinned}\TaskBar\Firefox.lnk	2	0	0 0d, 0h, 00m, 00s	2021-12-01 12:32:34
{Common Programs}\Accessories\Remote Desktop Connection.lnk	1	0	0 0d, 0h, 00m, 00s	2021-11-25 03:59:55
{User Pinned}\TaskBar\Opera Browser.lnk	1	0	0 0d, 0h, 00m, 00s	2021-11-25 04:10:02
{Common Programs}\Accessories\Notepad.lnk	1	0	0 0d, 0h, 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
1	ControlSet	CacheEntry Path	LastModifiedTimeUTC	Executed	Duplicate	SourceFile
2	1	0 C:\Users\THM-4n6\Desktop\KAPE\gkape.exe	6/24/2021 6:23	NA	FALSE	C:\Users\THM-4n6\Desktop\SYSTEM_clean
3	1	1 C:\Users\THM-4n6\Desktop\KAPE\kape.exe	6/24/2021 6:23	NA	FALSE	C:\Users\THM-4n6\Desktop\SYSTEM_clean
4	1	2 C:\Program Files\Common Files\microsoft shared\ink\TabTip.exe	10/6/2021 13:52	NA	FALSE	C:\Users\THM-4n6\Desktop\SYSTEM_clean
5	1	3 C:\Windows\System32\rdpinput.EXE	12/7/2019 9:09	NA	FALSE	C:\Users\THM-4n6\Desktop\SYSTEM_clean
6	1	4 C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe	10/6/2021 13:45	NA	FALSE	C:\Users\THM-4n6\Desktop\SYSTEM_clean
7	1	5 C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe	11/25/2021 2:18	NA	FALSE	C:\Users\THM-4n6\Desktop\SYSTEM_clean

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.

<https://www.evernote.com/client/web#?b=b05d125c-53d4-3cd8-8d27-1dcf82175d5d&n=2b81adfe-aba7-0c16-162e-bd45d8052723&>

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:

Registry hives (3) Available bookmarks (61/0)						
Values Amcache-InventoryApplicationFile						
Drag a column header here to group by that column						
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_8wekyb3d6bbw\3dviewer.exe	3DViewer.exe	view 3d	microsoft corporation	7.2107.7012.0	1b384b00a12104b4a62796773ef90899f6048
2021-12-01 12:55:19	c:\program files\7-zip\7z.exe	7z.exe	7-zip	igor pavlov	19.00	6c7ea8bb435163ae3945bef30ef6b9872a4591
2021-12-01 12:55:19	c:\program files\7-zip\7zfm.exe	7zFM.exe	7-zip	igor pavlov	19.00	e45e198607c8d7398745baa71780e3e7a2fd6eca
2021-12-01 12:55:19	c:\program files\7-zip\7zg.exe	7zG.exe	7-zip	igor pavlov	19.00	df2612647e9404a515d48ebad49034965250de
2021-12-01 13:00:29	c:\program files\{x86}\google\update\download\b8a69d345-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	e2b82e677152fab11f14d1e192184ca05166e0f
2021-12-01 12:55:49	c:\program files\amazon\ssm\amazon-ssm-agent.exe	amazon-ssm-agent.exe				e57d619197d5937d85d8d702385fd45707a30809
2021-12-01 12:57:38	c:\programdata\package\71aad047-faef-4dc7-8d46-60f211aa9f6\amazonssmagentsetup.exe	AmazonSSMAgentSetup.exe	amazon ssm agent	amazon web services	3.1.338.0	9194f54f615d43875ed093b94da70ea59682816a
2021-12-01 13:00:20	c:\users\thm-4n6\desktop\amcacheparser.exe	AmcacheParser.exe	amcacheparser	eric zimmerman	1.4.0.0	13ab20217dff43326642d9a224e5405db00b3c7

BAM/DAM:

Background Activity Monitor or BAM keeps a tab on the activity of background applications. Similar Desktop Activity Moderator or DAM is a part of Microsoft Windows that optimizes the power consumption of the device. Both of these are a part of the Modern Standby system in Microsoft Windows.

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

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

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

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

Registry hives (3) Available bookmarks (61/0)	
Values BamDam	
Drag a column header here to group by that column	
Program	Execution Time
Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy	=
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\undll32.exe	2021-11-24 17:38:19
\Device\HarddiskVolume2\Program Files (x86)\WindowsInstallationAssistant\Windows10UpgraderApp.exe	2021-11-24 18:01:52
\Device\HarddiskVolume2\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	2021-11-24 15:21:35
\Device\HarddiskVolume2\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	2021-11-24 15:23:43

Answer the questions below

How many times was the File Explorer launched?

26

What is another name for ShimCache?

AppCompatCache

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?

BAM/DAM

Task 7 External Devices/USB device forensics**Device identification:**

The following locations keep track of USB keys plugged into a system. These locations store the vendor id, product id, and version of the USB device plugged in and can be used to identify unique devices. These locations also store the time the devices were plugged into the system.

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.

Registry hives (3)		Available bookmarks (61/0)												
		Values	USBSTOR											
		Drag a column header here to group by that column												
Key name		Timestamp	Manufacturer	Title	Version	Disk Id	Serial Number	Device Name	Installed	First Installed	Last Connected	Last Removed		
USB	USB	2021-11-24 18:27...	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...	=		
USBSTOR	USBSTOR	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...	=		

First/Last Times:

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}\####

In this key, the ##### sign can be replaced by the following digits to get the required information:

Value	Information
0064	First Connection time
0066	Last Connection time
0067	Last removal time

Although we can check this value manually, as we have seen above, Registry Explorer already parses this data and shows us if we select the USBSTOR key.

USB device Volume Name:

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

SOFTWARE\Microsoft\Windows Portable Devices\Devices

Key name	Timestamp	Device	Serial Number	Guid	Friendly Name
Windows Portable Devices	2021-11-25 07:16:54			{E251921F-4DA2-11EC-A783-001A7DDA7110}	USB
Devices	2021-11-25 07:16:54			{F529A9D6-4D9E-11EC-A782-001A7DDA7110}	New Volume
SWD#WPDBUSENUM#{E2!					

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 to correlate the names with unique devices. Take a 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 DataTraveler 2.0 USB Device

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

USB

Task 8 Hands-on Challenge**Answer the questions below**

How many user created accounts are present on the system?

Hint: Check the SAM hive. Accounts with RIDs starting with 10xx are user created accounts

Here I opened RegistryExplorer and opened up the SAM hive, C:\Windows\System32\Config\SAM

000001F5
000001F7
000001F8
000003E9
000003EA
000003EB
Names
Administrator
DefaultAccount
Guest
THM-4n6
thm-user
thm-user2
WDAGUtilityAccount

In the details I find

User ID	Invalid Logins	Total Logins	Created	Last Logon	Last Passwd Chg	Last Inact	Expires	User Name	Full Name	Password Hint	Groups	Comment	User Type
=	=	=	=	=	=	=	=	RBC	RBC	RBC	RBC	RBC	RBC
503	0	0	2021-11...					DefaultAccount			System Managed Accounts Group	A user account managed by the system.	
504	0	0	2021-11...	2021-11...				WDAGUtilityAccount				A user account managed and used by the system for Windows Defender Application Guard scenarios.	
1001	0	19	2021-11...	2021-12...	2021-11...	2021-11...		THM-4n6		count	Administrators		
1002	0	2	2021-11...	2021-11...				thm-user		null	Users		
1003	0	0	2021-11...					thm-user2		null	Users		

Total rows: 7

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

Hint: Check the account that does not have a last logged in time

User ID	Invalid Logins	Total Logins	Created	Last Logon	Last Passwd Chg	Last Inact	Expires	User Name	Full Name	Password Hint	Groups	Comment	User Type
=	=	=	=	=	=	=	=	RBC	RBC	RBC	RBC	RBC	RBC
503	0	0	2021-11...					DefaultAccount			System Managed Accounts Group	A user account managed by the system.	
504	0	0	2021-11...	2021-11...	2021-11...			WDAGUtilityAccount				A user account managed and used by the system for Windows Defender Application Guard scenarios.	
1001	0	19	2021-11...	2021-12...	2021-11...	2021-11...		THM-4n6		count	Administrators		
1002	0	2	2021-11...	2021-11...				thm-user		null	Users		
1003	0	0	2021-11...					thm-user2		null	Users		

Total rows: 7

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

Hint: Check the Password Hint column

User Name	Full Name	Password Hint	Groups	Comments
DefaultAccount			System Managed Accounts Group	A user account managed by the system.
WDAGUtilityAccount				A user account managed and used by the system for Windows Defender Application Guard scenarios.

		count	Administrators
THM-4n6		null	Users
thm-user		null	Users

When was the file 'Changelog.txt' accessed?

Hint: Format: yyyy-mm-dd hh:mm:ss Check in evidence of file/folder opening

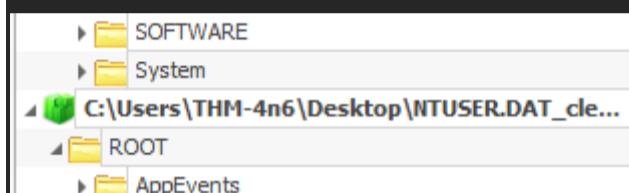
WOW! This one took me nearly 20 minutes to figure out how to look for it and where to find it!!!!

Still using Registry Editor, load up a new hive.

Task 5 teaches us to look here for recent file activity:

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

You just need to find which user.



2021-11-24 18:18:48 --And now I realized it is the username for the current user 😊

Values								Recent documents
Drag a column header here to group by that column								Values
Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension	Last Opened	Values
.txt	0	ChangeLog.txt	ChangeLog.lnk	=	=	=	=	
					0 2021-11-24 18:18:48			

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

Hint: Check the evidence of execution artifacts

I'm going to assume this was done on command line and will not be found in User Assist registry keys; let's try the ShimCache
SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

But Registry Explore can't help us here; we need AppCompatCache Parser--But I can't seem to get this to work. Looking back, I see I can find the info on AmCache, too.

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}\

I had to look at the screenshot when it talks about AmCache; it's not "File" but "InventoryApplicationFile\"

Amcache.hve\Root\InventoryApplicationFile\python-3.8.2.exe

File Tools Options Bookmarks (0/0) View Help						
Registry hives (2)		Available bookmarks (0/0)				
Enter text to search...						
Key name	# values					
=						
C:\Users\THM-4n6\Desktop\Amcach...						
{11517B7C-E79D-4e20-961B-75A811715...						
Root						
DeviceCensus						
DriverPackageExtended						
InventoryApplication						
InventoryApplicationAppV						
InventoryApplicationFile						
python-3.8.2.exe c75eb509...	19	0	2021-12-01 13:00:10			
pyw.exe 5f03342bb9a9928a	21	0	2021-12-01 12:57:44			
rawie.exe db5ff357ed867187	21	0	2021-12-01 13:00:29			
rbcmd.exe 6c45b9be22ffca56	19	0	2021-12-01 13:00:22			
rbcmd.exe c158d99ba47dbaf6	21	0	2021-12-01 13:00:29			
rebin.exe 18ea81dc270698ec	21	0	2021-12-01 13:00:29			
recentfilecachep ad2a90d3ade8...	19	0	2021-12-01 13:00:22			

c:\users\thm-4n6\appdata\local\package cache\{3182483d-078b-48fa-92c2-798baa1fe27d}\python-3.8.2.exe

Registry file: C:\Users\THM-4n6\Desktop\Amcache.hve_clean

Key: Root\InventoryApplicationFile\python-3.8.2.exe|c75eb5095c91ccff

Last write: 2021-12-01 13:00:10

Value: LowerCaseLongPath (RegSz)

Data: c:\users\thm-4n6\appdata\local\package cache\{3182483d-078b-48fa-92c2-798baa1fe27d}\python-3.8.2.exe

Slack: 00-00

c:\ appdata\python-3.8.2.exe

Values						
Drag a column header here to group by that column						
Value Name	Value Type	Data			Value Slack	Is Deleted
Value Name	Value Type	Data	Value Slack	Is Deleted	Value	Is Deleted
ProgramId	RegSz	0000698aecae48db708e3c40f46dc402e1c00000ffff	00-00			
FileId	RegSz	00005ac9b7b0f46e289809878c5055978842ba017e7a	6E-00			
LowerCaseLongPath	RegSz	c:\users\thm-4n6\appdata\local\package cache\{3182483d-078b-48fa-92c2-798baa1fe27d}\python-3.8.2.exe	00-00			
LongPathHash	RegSz	python-3.8.2.exe c75eb5095c91ccff				
Name	RegSz	python-3.8.2.exe	00-00			
OriginalFileName	RegSz	python-3.8.2.exe	00-00			
Publisher	RegSz	python software foundation	00-00-00-00-00-00			
Version	RegSz	3.8.2150.0	00-00-00-00-00-00			
BinFileVersion	RegSz	3.8.2150.0	23-00-08-C6-23-00			
BinaryType	RegSz	pe32_i386				
ProductName	RegSz	python 3.8.2 (32-bit)				
ProductVersion	RegSz	3.8.2150.0	00-00-00-00-00-00			
LinkDate	RegSz	11/18/2017 22:00:38	00-00-00-00			
BinProductVersion	RegSz	3.8.2150.0	00-00-00-00-00-00			
AppxPackageFullName	RegSz					
AppxPackageRelativeId	RegSz		****			

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

Answer format: ~~*****~~ c:\python-3.8.2.exe

8 char remaining

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

I honestly can't answer this after 40 minutes of smashing my head in.

File Tools Options Bookmarks (0/0) View Help				
Registry hives (2)		Available bookmarks (0/0)		
3.8.2				Find
	Key name	# values	# subkeys	Last write timestamp
?	RBC	=	=	=
▲	C:\Users\THM-4n6\Desktop\Amcache...			2021-11-25 03:13:59
▲	{11517B7C-E79D-4e20-961B-75A811715...	0	1	2021-11-24 18:23:15
▲	Root	0	25	2021-11-24 18:25:42
▲	InventoryApplicationFile	2	596	2021-12-01 13:04:49
▲	python-3.8.2.exe c75eb5095c91...	19	0	2021-12-01 13:00:10
✖	python-3.8.2.exe 4d23dde6fea9...	17	0	2021-11-24 18:23:15
▲	Associated deleted records	0	0	
▲	{11517B7C-E79D-4e20-961B-75A8117...	0	0	
▲	Root	0	0	
▲	InventoryApplicationFile	0	0	
✖	python-3.8.2.exe 4d23dde6fea9...	17	0	2021-11-24 18:23:15
▲	Associated deleted records	0	0	
▲	{11517B7C-E79D-4e20-961B-75A811715...	0	1	2021-11-24 18:23:15
▲	Root	0	25	2021-11-24 18:25:42
▲	InventoryApplicationFile	2	596	2021-12-01 13:04:49
▲	python-3.8.2.exe c75eb5095c91...	19	0	2021-12-01 13:00:10
✖	python-3.8.2.exe 4d23dde6fea9...	17	0	2021-11-24 18:23:15
▲	Associated deleted records	0	0	
▲	{11517B7C-E79D-4e20-961B-75A8117...	0	0	
▲	Root	0	0	
▲	InventoryApplicationFile	0	0	
✖	python-3.8.2.exe 4d23dde6fea9...	17	0	2021-11-24 18:23:15

A new day. New tactics.

Going to

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

I had no idea what the guid would be so I just opened them all to see the "count"

Two entries have values: 11 and 4%

Looking under the 49 one--

Shell Folders	31	0	2021-11-24 1:		
Shutdown	1	0	2021-12-01 1:		
StartPage	2	0	2021-11-24 1:		
Streams	0	1	2021-11-24 1:		
StuckRects3	1	0	2021-12-01 1:		
TabletMode	1	0	2021-11-24 1:		
Taskband	5	1	2021-12-01 1:		
TypedPaths	3	0	2021-11-30 1:		
User Shell Folders	20	0	2021-11-24 1:		
UserAssist	0	9	2021-11-24 1:		
{9E04CAB2-CC14-11DF-BB8C-A2F1DE... Count	1	1	2021-11-24 1:		
{A3D53349-6E61-4557-8FC7-0028EDC... Count	1	1	2021-11-24 1:		
{B267E3AD-A825-4A09-82B9-EEC22A... Count	1	1	2021-11-24 1:		
{BCB48336-4DDD-48FF-BB0B-D3190D... Count	1	1	2021-11-24 1:		
{CAA59E3C-4792-41A5-9909-6A6A8D... Count	1	1	2021-11-24 1:		
{CEBFF5CD-ACE2-4F4F-9178-9926F41... Count	1	1	2021-11-24 1:		
49	0	2021-12-01 1:			
{F2A1CB5A-E3CC-4A2E-AF9D-505A70... Count	1	1	2021-11-24 1:		
{F4E57C4B-2036-45F0-A9AB-443BCFE... Count	1	1	2021-11-24 1:		
11	0	2021-12-01 1:			
{FA99DFC7-6AC2-453A-A5E2-5E2AFF... Count	1	1	2021-11-24 1:		
0	0	2021-11-24 1:			
VirtualDesktops	0	0	2021-11-24 1:		
VisualEffects	0	19	2021-11-24 1:		
Wallpapers	5	0	2021-12-01 1:		
WordWheelQuery	2	0	2021-11-30 1:		
Ext	0	0	2021-11-24 1:		
Feeds	7	1	2021-12-01 1:		

FINALLY!!!

Z:\setups\firefox_installer.exe					
\vmware-host\Shared Folders\setups\Firefox					
Installer.exe					
C:\Users\THM-4n6\AppData\Local\Temp\7zS09BA					
49F3\setup-stub.exe					
Z:\setups\python-3.8.2.exe					
C:\Users\THM-4n6\AppData\Local\Temp\{Unmapp					
ed GUID: B409B86A-9CC9-4639-9E0C-0B35E1DEC040}\,cr\					
python-3.8.2.exe					
E7CF176E110C211B					
Z:\setups\chromesetup.exe					
Program Files					
Total rows: 49					

Type viewer Slack viewer

00000000	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D
00000024	FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00
	00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 00 00

FINALLY!!!

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

Hint: Format: yyyy-mm-dd hh:mm:ss

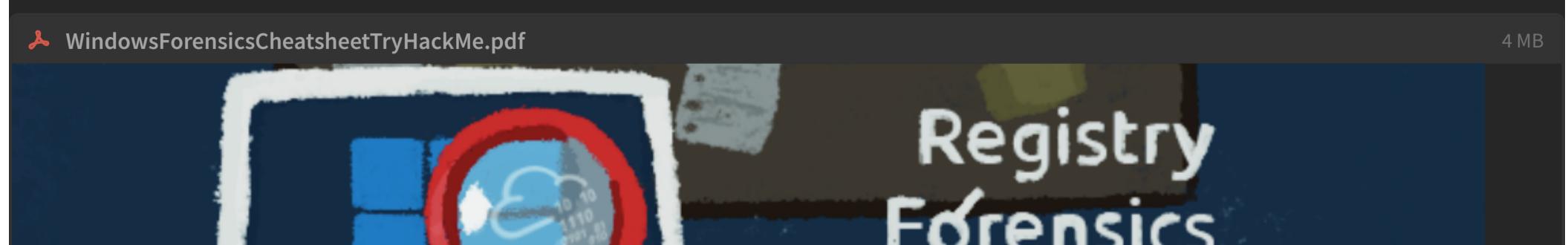
Having opened the SYSTEM hive, I see two USB devices, however I do not know how to determine their friendly names.

That said, I enter the second date into THM but it is wrong: the first one works.

I don't know why that is the right answer which bothers me because I want to link the device to the friendly name

USBSTOR											
Drag a column header here to group by that column											
	Timestamp	Manufacturer	Title	Version	Disk Id	Serial Number	Device Name	Installed	First Installed	Last Connected	Last Rem
▼	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	

Conclusion



Cheatsheet

System info and accounts



OS Version:

SOFTWARE\Microsoft\Windows NT\CurrentVersion

Current Control set:

HKLM\SYSTEM\CurrentControlSet
SYSTEM\Select\Current
SYSTEM\Select\LastKnownGood

Computer Name:

SYSTEM\CurrentControlSet\Control\ComputerName
\ComputerName

Time Zone Information:

SYSTEM\CurrentControlSet\Control
\TimeZoneInformation

Network Interfaces and Past Networks:

SYSTEM\CurrentControlSet\Services\Tcpip
\Parameters\Interfaces

Autostart Programs (Autoruns):

NTUSER.DAT\Software\Microsoft\Windows
\CurrentVersion\Run
NTUSER.DAT\Software\Microsoft\Windows
\CurrentVersion\RunOnce
SOFTWARE\Microsoft\Windows\CurrentVersion
\RunOnce
SOFTWARE\Microsoft\Windows\CurrentVersion
\policies\Explorer\Run
SOFTWARE\Microsoft\Windows\CurrentVersion\Run

SAM hive and user information:

SAM\Domains\Account\Users

External/USB device forensics



Device identification:

SYSTEM\CurrentControlSet\Enum\USBSTOR
SYSTEM\CurrentControlSet\Enum\USB

First/Last Times:

SYSTEM\CurrentControlSet\Enum\USBSTOR
\Ven_Prod_Version\USBSerial#\Properties
\{83da6326-97a6-4088-9453-a19231573b29}\####
0064=first connection
0066=last connection
0067=last removal

USB device Volume Name:

SOFTWARE\Microsoft\Windows Portable Devices
\Devices

File/folder usage or knowledge



Recent Files:

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

Office Recent Files:

NTUSER.DAT\Software\Microsoft\Office\VERSION
NTUSER.DAT\Software\Microsoft\Office\VERSION
\UserMRU\LiveID_####\FileMRU

ShellBags:

USRCLASS.DAT\Local Settings\Software\Microsoft
\Windows\Shell\Bags
USRCLASS.DAT\Local Settings\Software\Microsoft
\Windows\Shell\BagMRU
NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU
NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags

Open/Save and LastVisited Dialog MRUs:

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

Windows Explorer Address/Search Bars:

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

Evidence of execution



UserAssist:

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

ShimCache:

SYSTEM\CurrentControlSet\Control\Session Manager
\AppCompatCache

AmCache:

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

BAM/DAM:

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