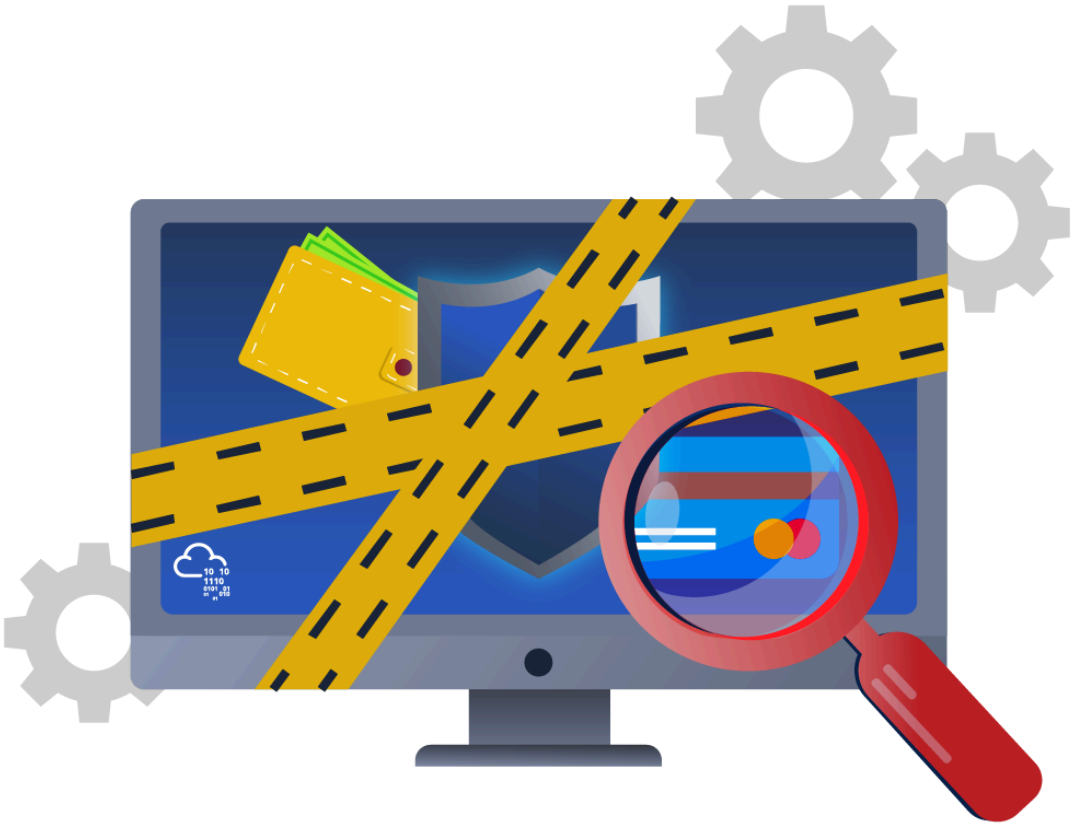
Windows Forensics 1

Task 1 Introduction to Windows Forensics

Introduction to Computer Forensics for Windows:



Computer forensics is an 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. The applications of digital and computer forensics are wide-ranging, from the legal sphere, where it is used to support or refute a hypothesis in a civil or criminal case, to the private sphere, where it helps in internal corporate investigations and incident and intrusion analysis.

A perfect example of Digital Forensics solving a criminal case is the BTK serial killer case. This case had gone cold for more than a decade when the killer started taunting the police by sending letters. The case took a major turn when he sent a floppy disk to a local news station

that was later taken to into evidence by the police. The police were able to recover a deleted word document on the drive, and using the metadata and some other evidence, they pinpointed and arrested him.

Microsoft Windows is by large the most used Desktop Operating System right now. Private users and Enterprises prefer it, and it currently holds roughly 80% of the Desktop market share. This means that it is important to know how to perform forensic analysis on Microsoft Windows for someone interested in Digital Forensics. In this module, we will learn about the different ways we can gather forensic data from the Windows Registry and make conclusions about the activity performed on a Windows system based on this data.

Forensic Artifacts:

When performing forensic analysis, you will often hear the word 'artifact'. Forensic artifacts are essential pieces of information that provide evidence of human activity. For example, during the investigation of a crime scene, fingerprints, a broken button of a shirt or coat, the tools used to perform the crime are all considered forensic artifacts. All of these artifacts are combined to recreate the story of how the crime was committed.

In computer forensics, forensic artifacts can be small footprints of activity left on the computer system. On a Windows system, a person's actions can be traced back quite accurately using computer forensics because of the various artifacts a Windows system creates for a given activity. These artifacts often reside in locations 'normal' users won't typically venture to. For our purposes, these artifacts can be analyzed to provide the trial of activity for an investigation.

So is my computer spying on me?

What do you think?

A Windows system keeps track of a lot of activity performed by a user. But is all that tracking for malicious purposes, or is there another reason for that? As we'll see in this room, the filesystem components that forensic experts deem artifacts primarily originated from Microsoft's efforts to improve the user's experience.

Assuming the same build of Windows is installed on a system, excluding the actions taken during installation, the out-of-the-box experience is similar for all users. However, with time, each user personalizes their computer according to their preferences. These preferences include the Desktop layout and icons, the bookmarks in the internet browser, the name of the user, installing of different applications, and logging in to different accounts for each of these applications and other accounts using the internet browser.

Windows saves these preferences to make your computer more personalized. However, forensic investigators use these preferences as artifacts to identify the activity performed on a system. So while your computer might be spying on you, it is not for the explicit reason of spying, instead to make it more pleasant to use the computer according to your taste. But that

same information is used by forensic investigators to perform forensic analysis. As we move through this room, we'll see that Windows stores these artifacts in different locations throughout the file system such as in the registry, a user's profile directory, in application-specific files, etc.

In the next task, we will learn about the Windows Registry and how it can help us in forensic analysis of a Windows system.

Note: Except for Task #10, which has a VM attached, the questions for all the upcoming tasks can be answered using the concepts and evidence presented in the text and images.

Answer the questions below
What is the most used Desktop Operating System right now?
Microsoft Windows

Task 2 Windows Registry and Forensics

Windows Registry:

The Windows Registry is a collection of databases that contains the system's configuration data. This configuration data can be about the hardware, the software, or the user's information. It also includes data about the recently used files, programs used, or devices connected to the system. As you can understand, this data is beneficial from a forensics standpoint. Throughout this room, we will learn ways to read this data to identify the required information about the system. You can view the registry using regedit.exe, a built-in Windows utility to view and edit the registry. We'll explore other tools to learn about the registry in the upcoming tasks.

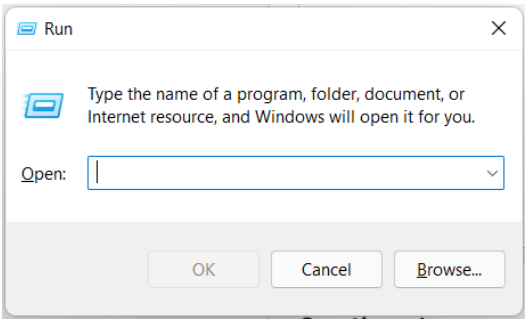
The Windows registry consists of Keys and Values. When you open the regedit.exe utility to view the registry, the folders you see are Registry Keys. Registry Values are the data stored in these Registry Keys. A Registry Hive is a group of Keys, subkeys, and values stored in a single file on the disk.

Structure of the Registry:

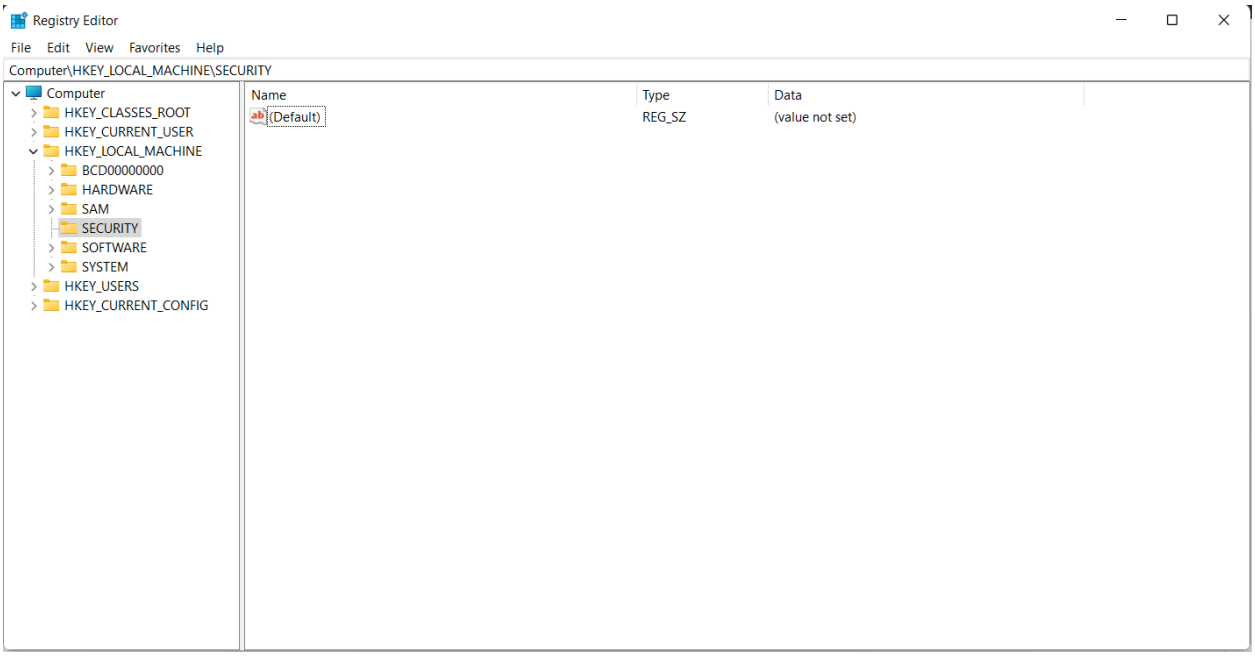
The registry on any Windows system contains the following five root keys:

1. HKEY_CURRENT_USER
2. HKEY_USERS
3. HKEY_LOCAL_MACHINE
4. HKEY_CLASSES_ROOT
5. HKEY_CURRENT_CONFIG

You can view these keys when you open the utility. To open the registry editor, press the Windows key and the R key simultaneously. It will open a prompt that looks like this:



In this prompt, type , and you will be greeted with the registry editor window. It will look something like this:



Here you can see the root keys in the left pane in a tree view that shows the included registry keys, and the values in the selected key are shown in the right pane. You can right-click on the value shown in the right pane and select properties to view the properties of this value.

Here is how Microsoft defines each of these root keys. For more detail and information about the following Windows registry keys, please visit Microsoft's documentation .

Folder/predefined key	Description

HKEY_CURRENT_USER	Contains the root of the configuration information for the user who is currently logged on. The user's folders, screen colors, and Control Panel settings are stored here. This information is associated with the user's profile. This key is sometimes abbreviated as HKCU.
HKEY_USERS	Contains all the actively loaded user profiles on the computer. HKEY_CURRENT_USER is a subkey of HKEY_USERS. HKEY_USERS is sometimes abbreviated as HKU.
HKEY_LOCAL_MACHINE	Contains configuration information particular to the computer (for any user). This key is sometimes abbreviated as HKLM.

HKEY_CLASSES_ROOT	Is a subkey of . The information that is stored here makes sure that the correct program opens when you open a file by using Windows Explorer. This key is sometimes abbreviated as HKCR. Starting with Windows 2000, this information is stored under both the HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER keys. The key contains default settings that can apply to all users on the local computer. The key has settings that override the default settings and apply only to the interactive user. The HKEY_CLASSES_ROOT key provides a view of the registry that merges the information from these two sources. HKEY_CLASSES_ROOT also provides this merged view for programs that are designed for earlier versions of Windows. To change the settings for the interactive user, changes must be made under instead of under HKEY_CLASSES_ROOT. To change the default settings, changes must be made under .If you write keys to a key under HKEY_CLASSES_ROOT, the system stores the information under . If you write values to a key under HKEY_CLASSES_ROOT, and the key already exists under , the system will store the information there instead of under .
HKEY_CURRENT_CONFIG	Contains information about the hardware profile that is used by the local computer at system startup.

Answer the questions below

What is the short form for HKEY_LOCAL_MACHINE?

HKLM

Task 3 Accessing registry hives offline

If you are accessing a live system, you will be able to access the registry using regedit.exe, and you will be greeted with all of the standard root keys we learned about in the previous task. However, if you only have access to a disk image, you must know where the registry hives are located on the disk. The majority of these hives are located in the directory and are:

1. **DEFAULT** (mounted on)
2. **SAM** (mounted on)
3. **SECURITY** (mounted on)
4. **SOFTWARE** (mounted on)
5. **SYSTEM** (mounted on)

Hives containing user information:

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 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 .

The NTUSER.DAT hive is located in the directory .

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 . 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 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 directory. These hives are copied to the 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 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 4 Data Acquisition

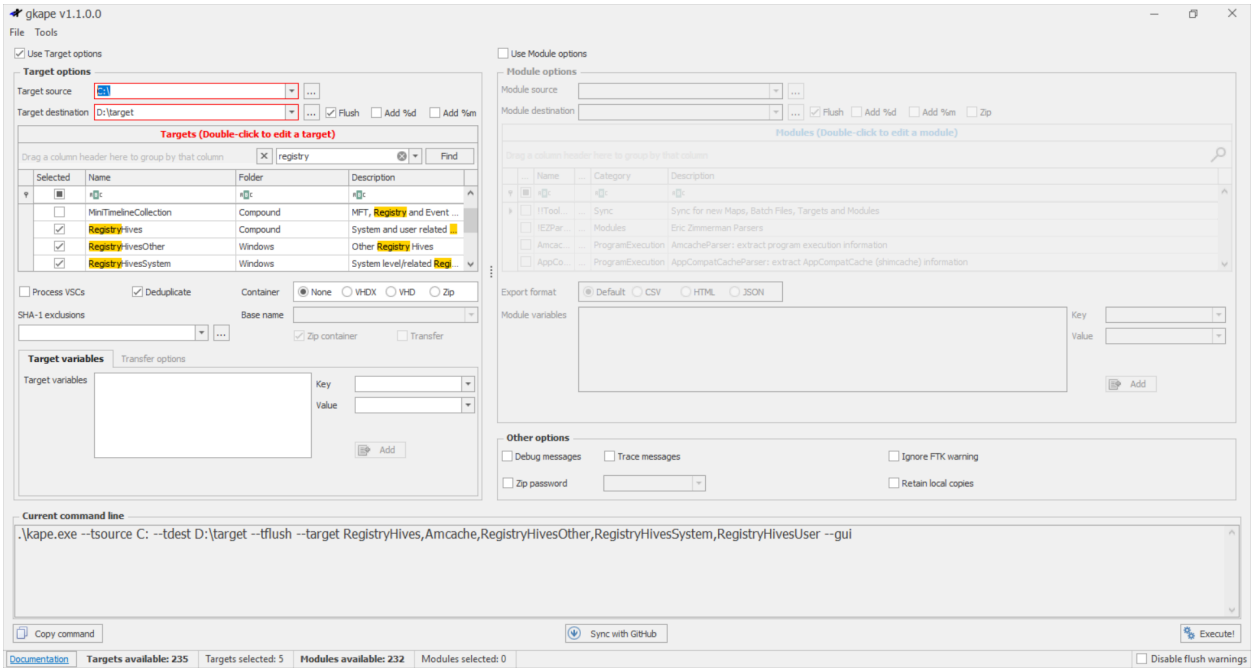
When performing forensics, we will either encounter a live system or an image taken of the system. For the sake of accuracy, it is recommended practice to image the system or make a copy of the required data and perform forensics on it. This process is called data acquisition. Below we discuss different ways to acquire registry data from a live system or a disk image:

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 , 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:

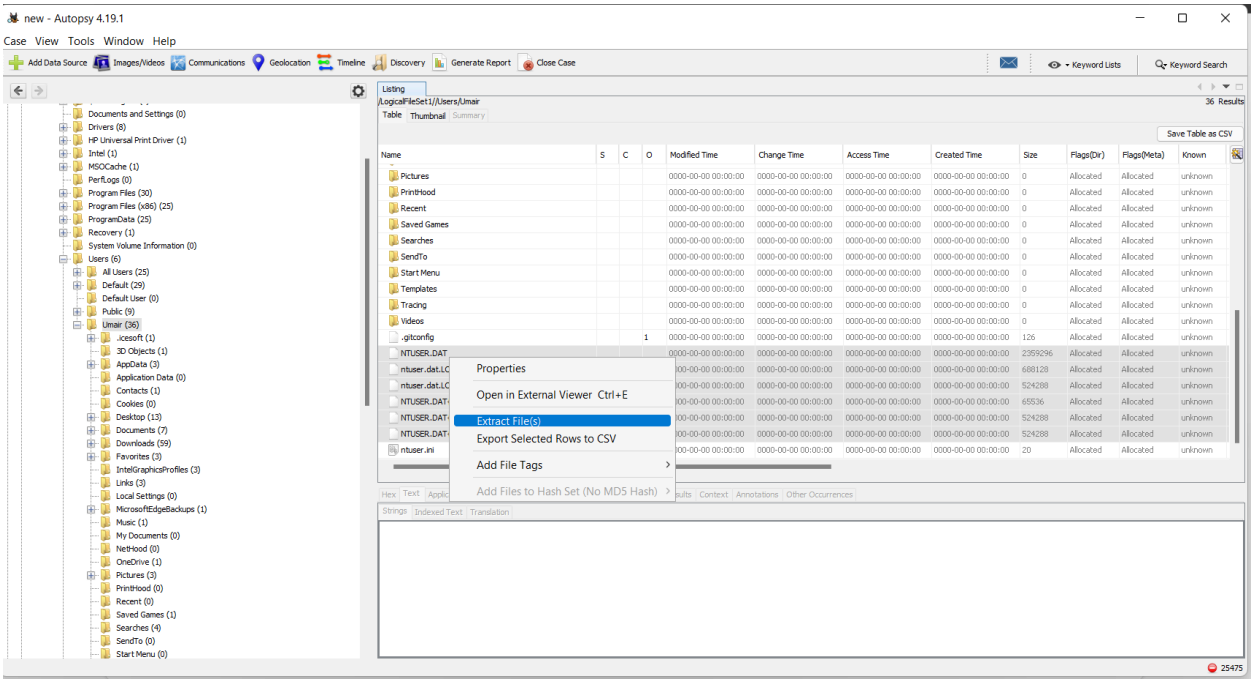
KAPE:

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. We will learn more about collecting forensic artifacts using KAPE in a dedicated KAPE room.



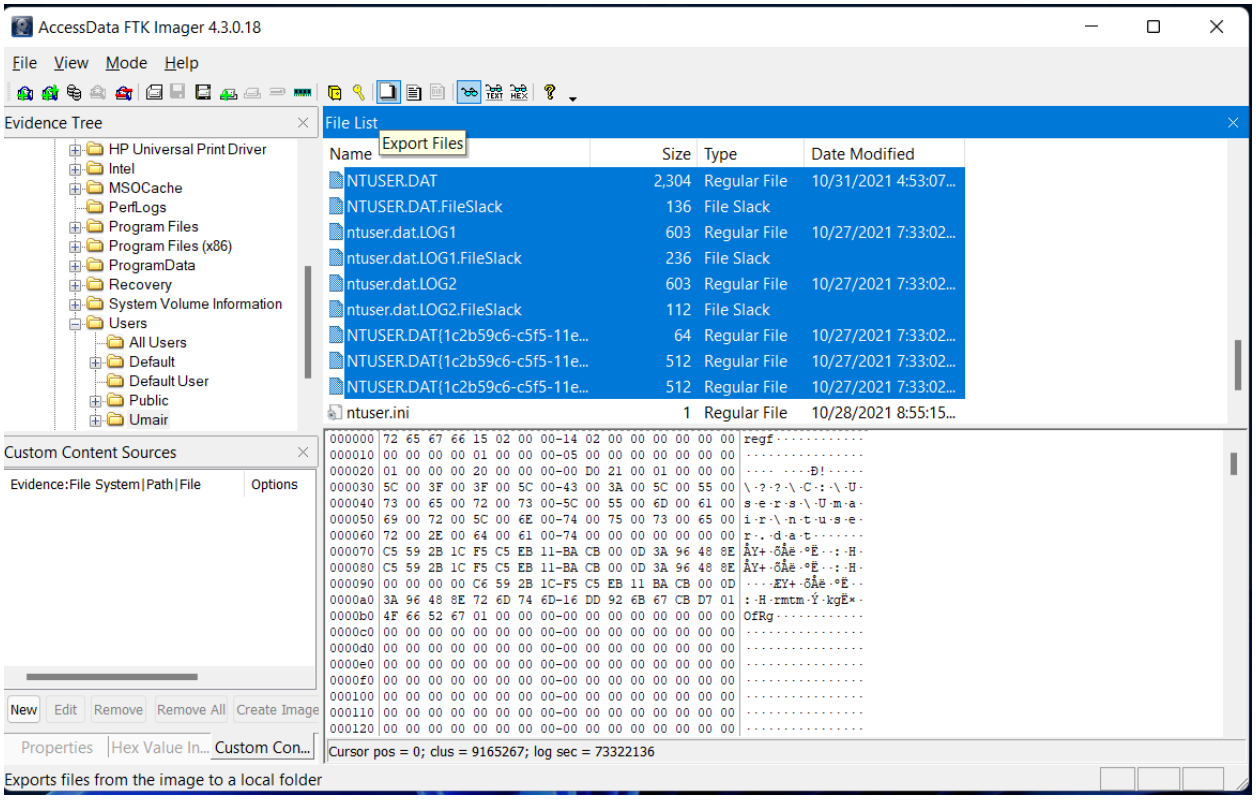
Autopsy:

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.

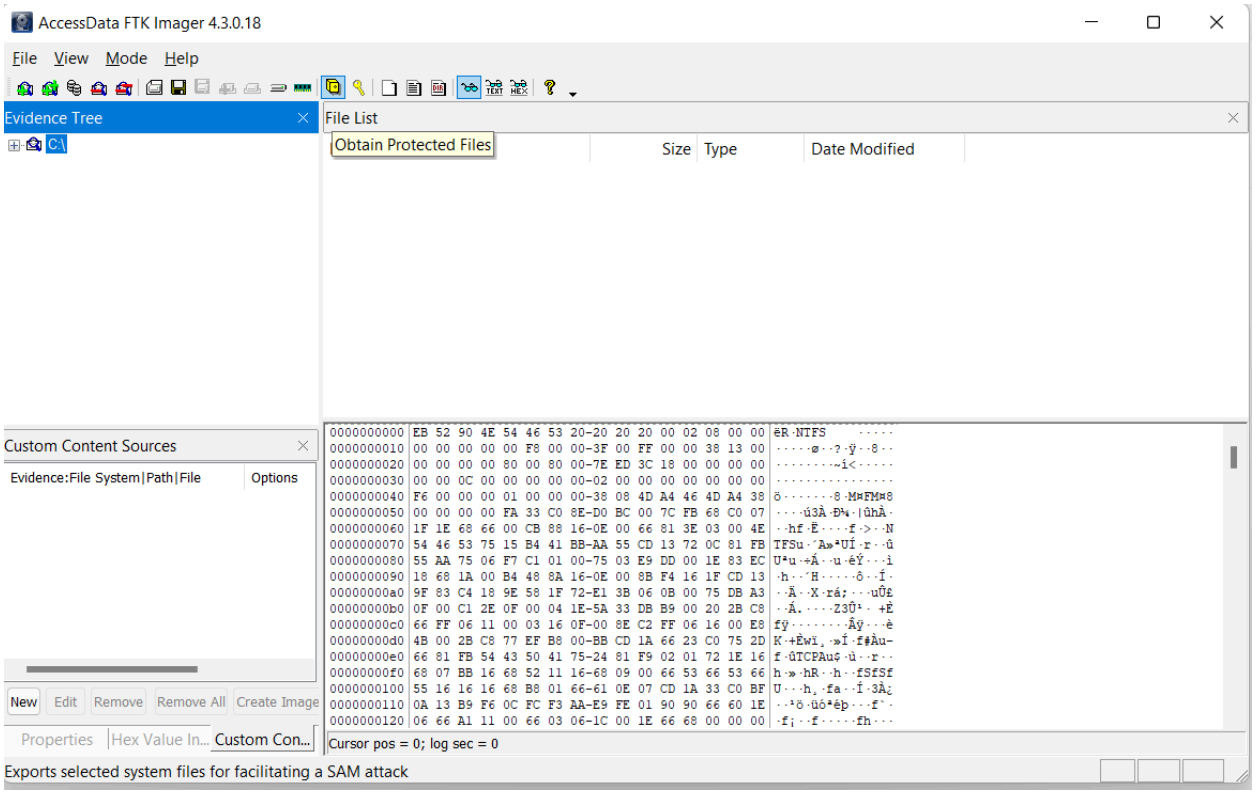


FTK Imager:

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.



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 file, which is often necessary to investigate evidence of programs that were last executed.



For the purpose of this room, we will not be acquiring data ourselves, but instead, we will work with the attached VM that already has data.

Task 5 Exploring Windows Registry

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:

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.

Task 6 System Information and System Accounts

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 7 Usage or knowledge of files/folders

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 8 Evidence of Execution

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