FORENSICS V2 LAB SERIES

Lab 04: Registry Forensics

Document Version: 2021-01-14

Contents

Introduction

Forensic artifacts can be found in many areas of the Windows operating system. The registry hives are a hierarchical database that stores user settings and configuration data from installed software. The registry files hold some of the most valuable artifacts that can be used to identify user activity. The data can also be correlated with files found on the source device or other related evidence items.

Objectives

- Identify the location of the most common registry files
- Learn what type of data each one stores
- Learn how to parse them
- Understand how to corroborate findings in the registry with files on the source device

Lab Topology

Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	**IP Address / Subnet Mask**	**Account** (if needed)	**Password** (if needed)
Caine	172.16.16.30	caine	Train1ng$
CSI-Linux	172.16.16.40	csi	csi
DEFT	172.16.16.20	deft	Train1ng$
WinOS	172.16.16.10	Administrator	Train1ng$

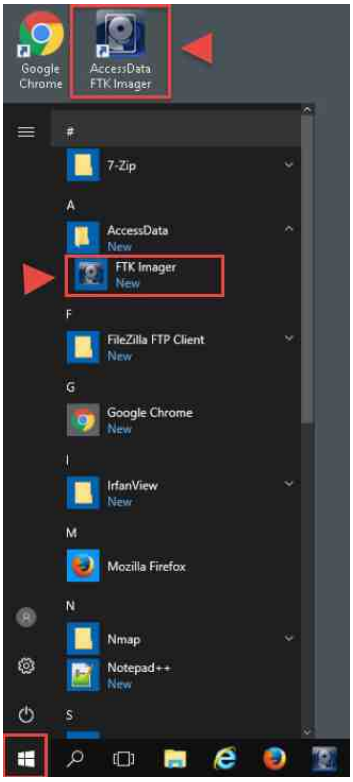
1 Find Out How to Manually Locate Windows' Registry Files

Not many cyber forensic examinations are performed without the assistance of data found in the registry files. This lab will explore the six most common registry hives, how to find them, and show you how to extract data from each of them. These registry files are called SAM, SECURITY, SYSTEM, SOFTWARE, NTUSER.DAT, and UsrClass.dat. We will get into their details in later exercises. For now, the important thing to note is that the SAM, SECURITY, SYSTEM, and SOFTWARE registry files contain data for the entire system and for all users. Alternatively, there is an NTUSER.DAT and UsrClass.dat file for each user account on the operating system. Now, let us find out where the files are stored in Windows' folder structure.

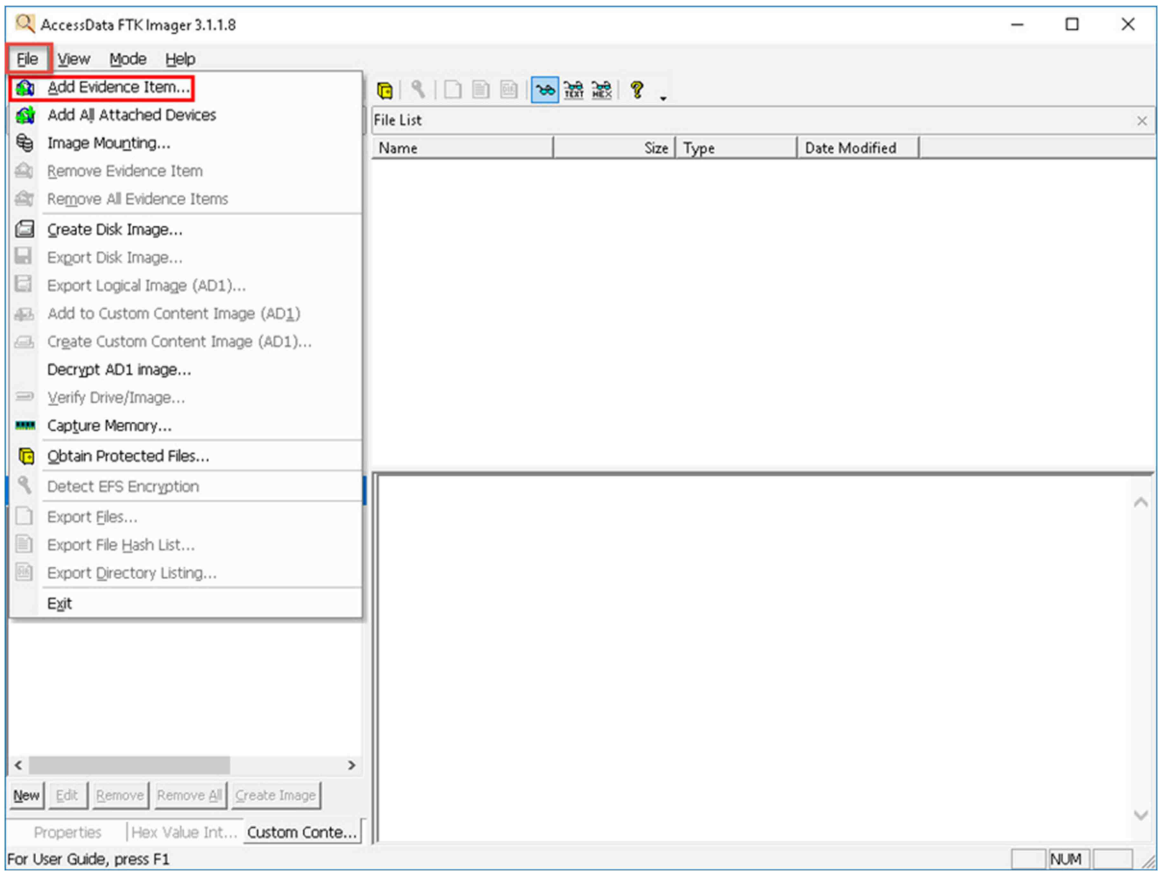
1. To begin, launch the WinOS virtual machine to access the graphical login screen.
   a. Select Send CTRL+ALT+DEL from the dropdown menu to be prompted with the login screen.

   b. Log in as `Administrator` using the password: `Train1ng$`

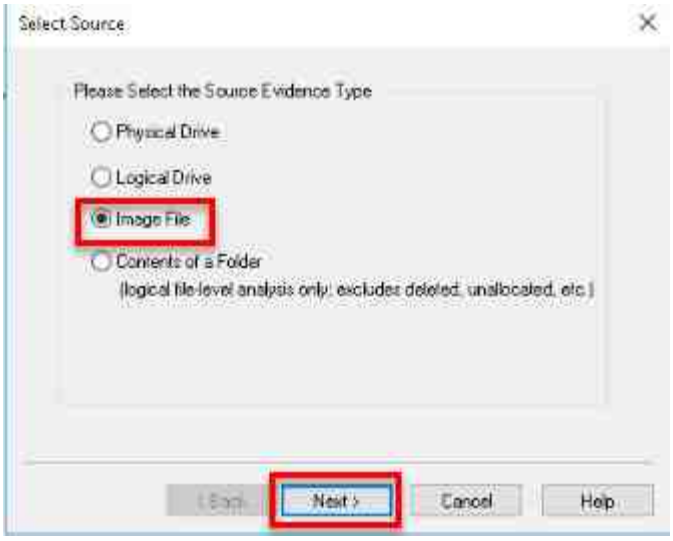
2. Once you are logged into the VM, launch the FTK Imager program from the windows menu by navigating to Start Menu > AccessData > FTK Imager. Alternatively, you can open FTK Imager from the Desktop by clicking the icon called AccessData FTK Imager:



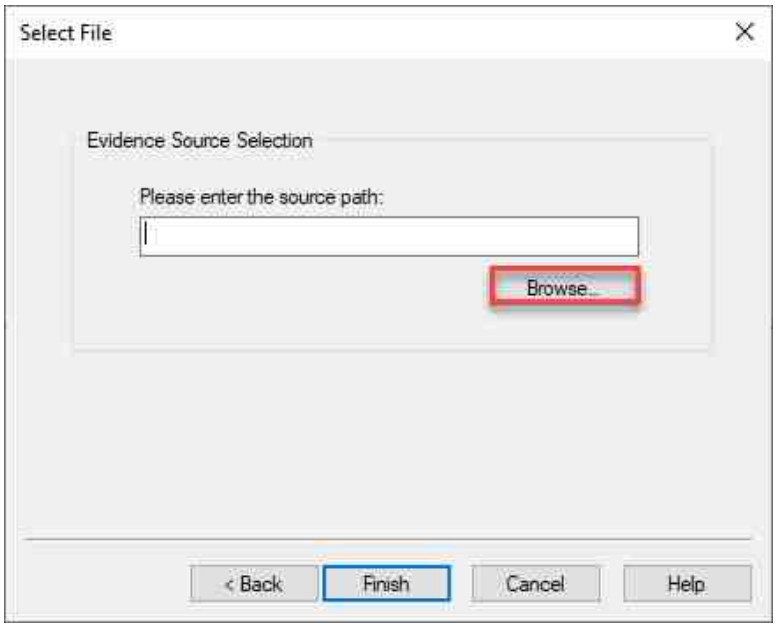
3. You should already be familiar with FTK Imager from our previous labs. In this exercise, we will learn how to navigate to the registry files' locations using some preconfigured Forensic Evidence Files (FEF). Let us begin by loading an FEF. To do this, click the File menu option to open the File dropdown, then click the Add Evidence Item option from the dropdown menu. It is the first item on the menu, as highlighted below.



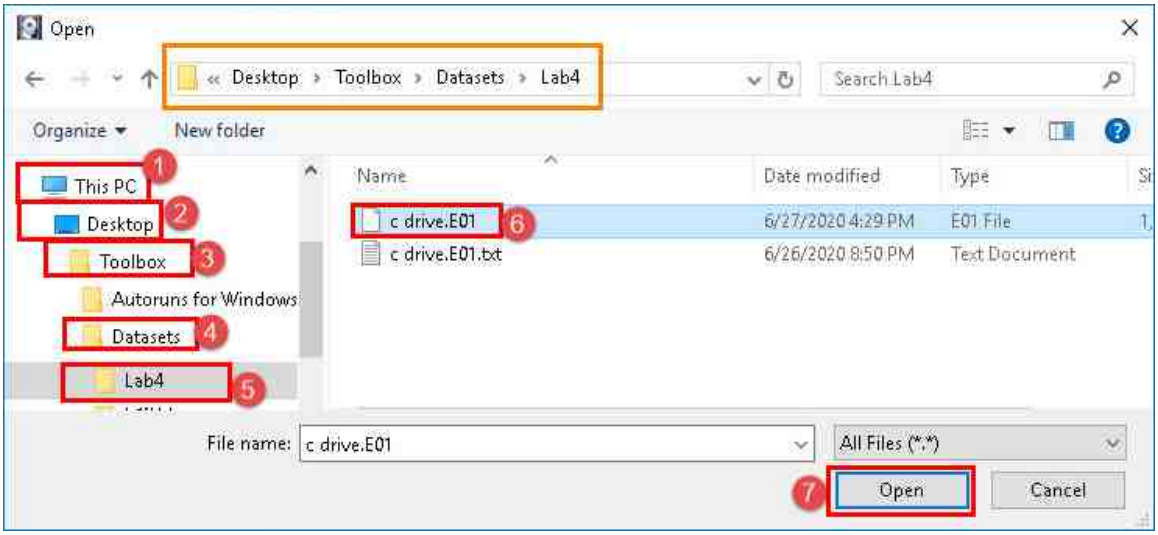
4. You will be brought to the Select Source window. Let us select Image File and click Next as highlighted below.



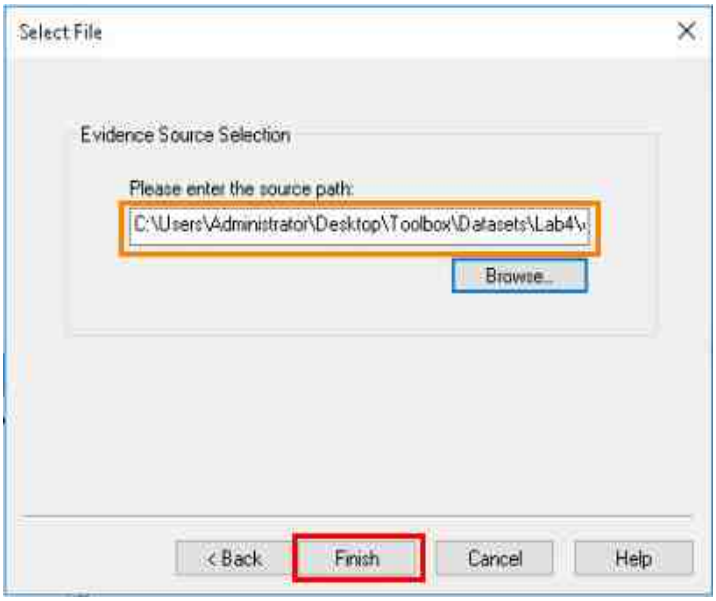
5. In the Select File window, click Browse highlighted in the screenshot below. This will open the Open window, which will allow you to browse to the appropriate FEF.



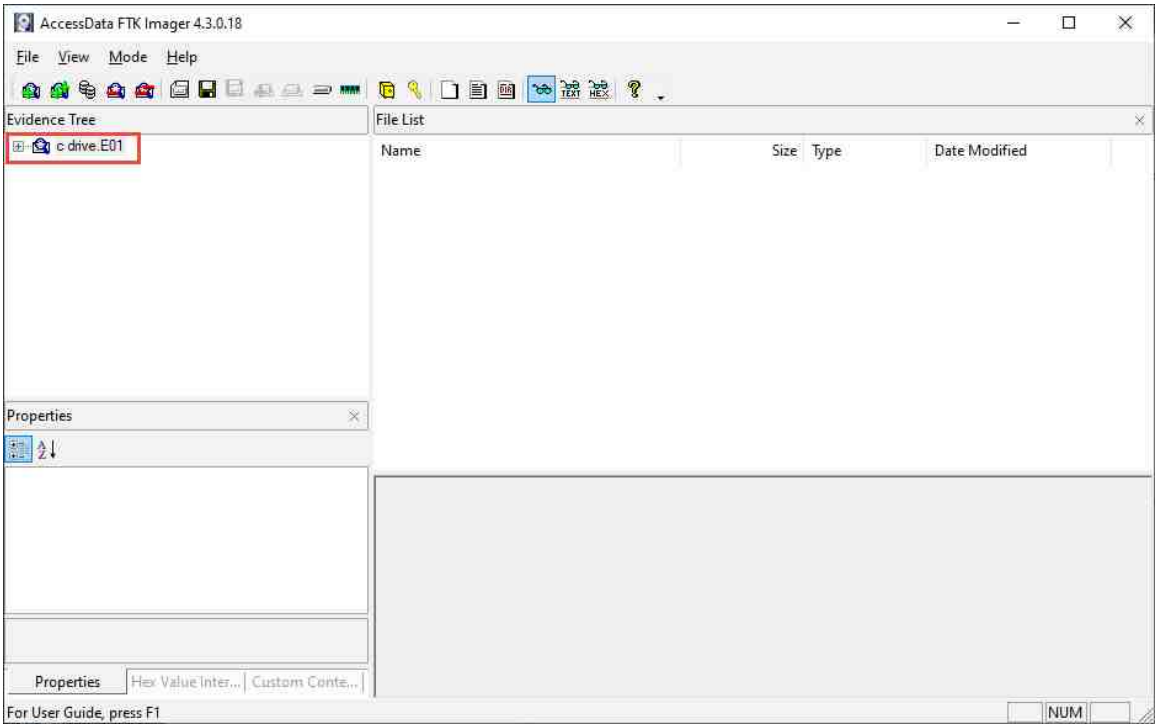
6. You are now at the Select File window. Browse to This PC > Desktop and double-click the folder Toolbox > Datasets > Lab4. This will open the folder revealing the FEF called C Drive.E01. Select the file called C Drive.E01 and click the Open button as highlighted in items 1 - 7 below.



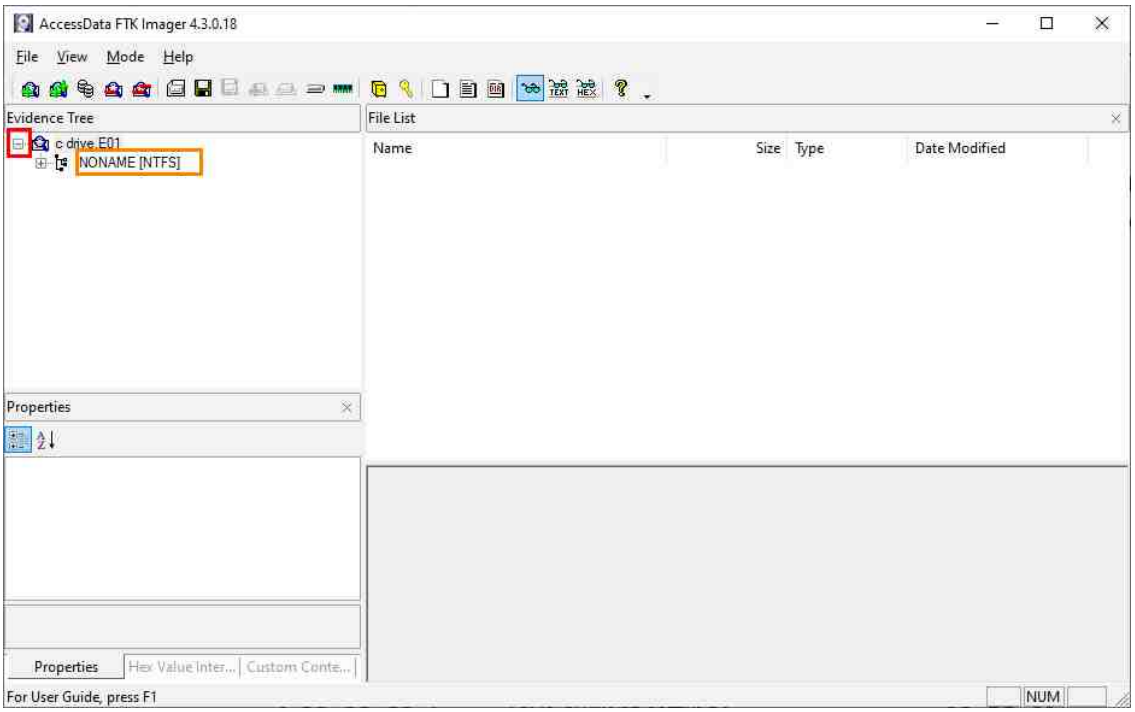
7. Review the source path of the file called C Drive.E01. In the Select File window, click Finish highlighted in red in the screenshot below. This will take you back to the FTK Imager's main window.



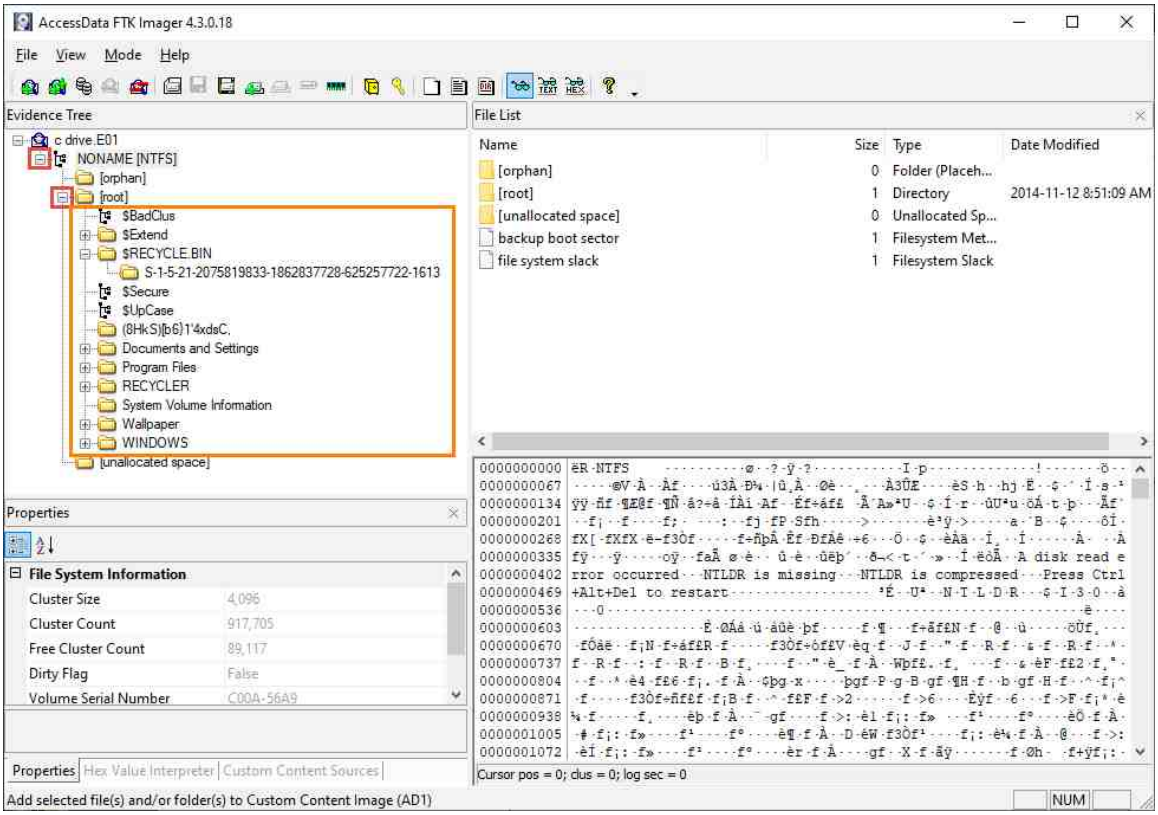
8. If you did everything correctly, you will now be back at FTK Imager's main window with C Drive.E01 listed under the Evidence Tree Pane. From the Evidence Tree pane, click the tree item C Drive.E01 highlighted below. This will select the image you are going to peruse.



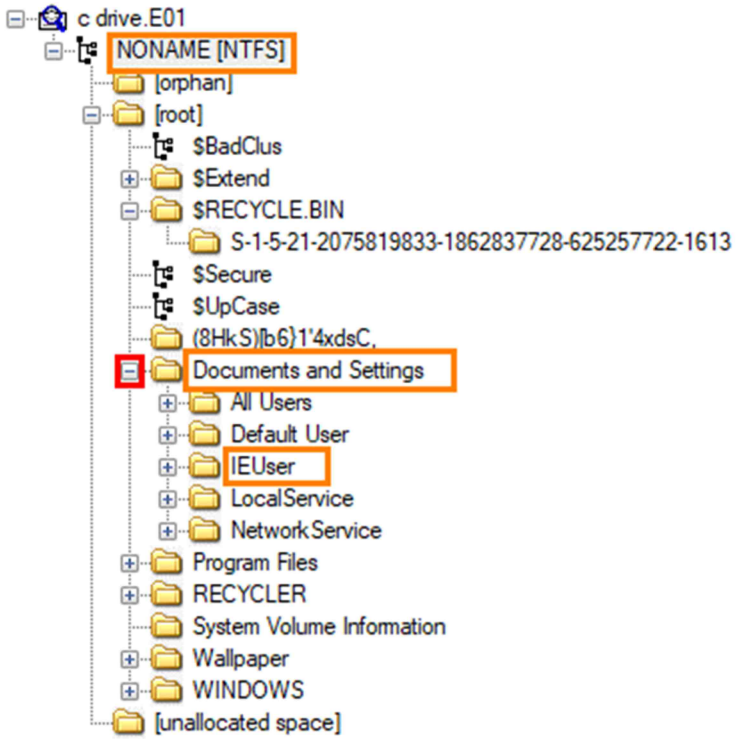
9. We will now browse the FEF and view its contents. To begin, click the + sign beside the hard drive you added called C Drive.E01, as seen below. This will expand the tree and display the partition on the drive. Now that you can see the partition, let us learn how to identify the operating system files on a normal installation of Microsoft Windows.



10. You will now be presented with the file system that is being used on the partition. The file system in the screenshot below is called NONAME [NTFS], which indicates that the partition uses the New Technology File System (NTFS) file system. Let us expand the partition by clicking the + beside NONAME [NTFS]. This will reveal three folders. The first folder is the orphan folder, and it contains deleted files that were recovered but have no parent folder. Next, there is the root folder that contains the operating system. The last folder is called unallocated space and represents free space as files. Let us expand the folder called root by clicking the + sign beside it.

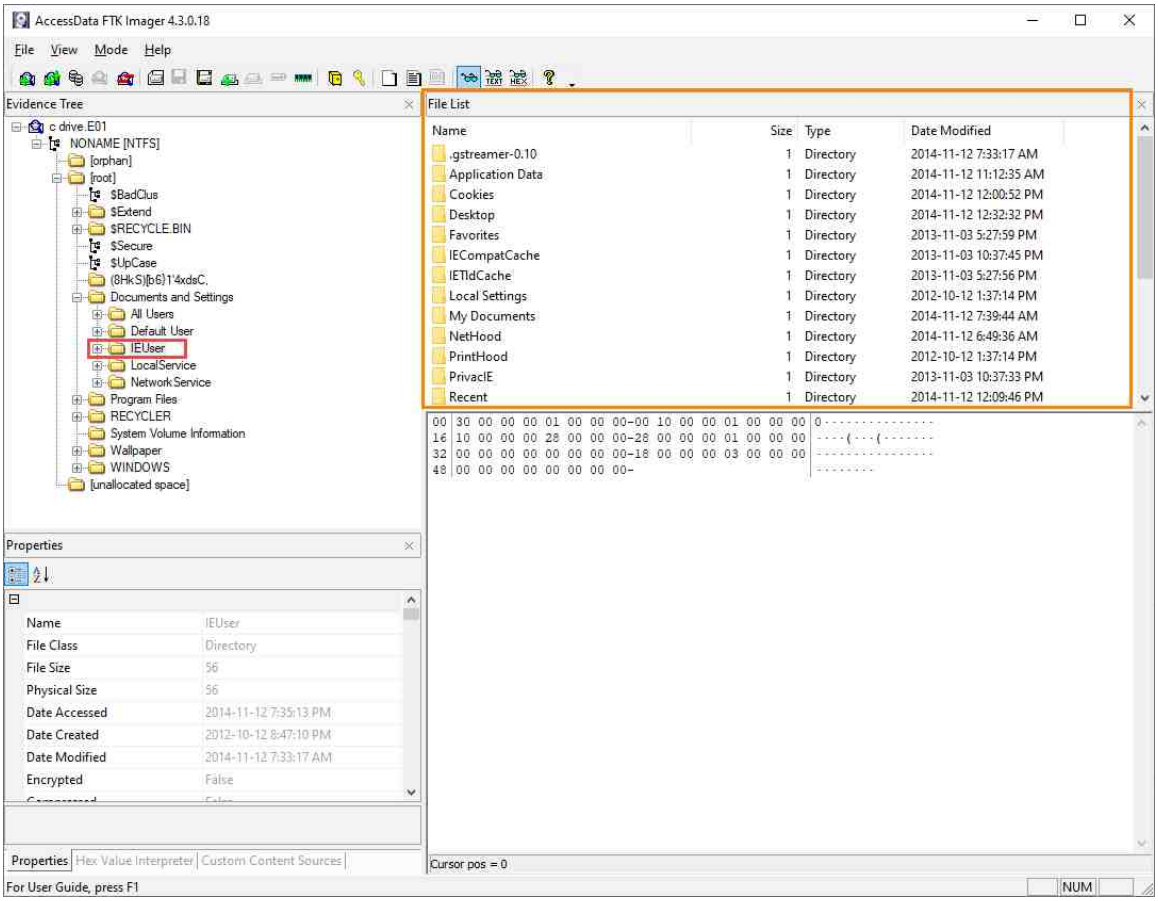


11. As we saw in the last lab, this root directory contains the Microsoft Windows operating system files and is represented as the C:\ drive in Windows File Explorer. The first registry file we will locate is the NTUSER.DAT file. As mentioned earlier, there are NTUSER.DAT files for each user account. In practice, it is always best to capture all the registry files available. In this exercise, we will only identify the NTUSER.DAT file for the IEUser account. Begin by clicking the + sign beside the Documents and Settings folder as highlighted below.

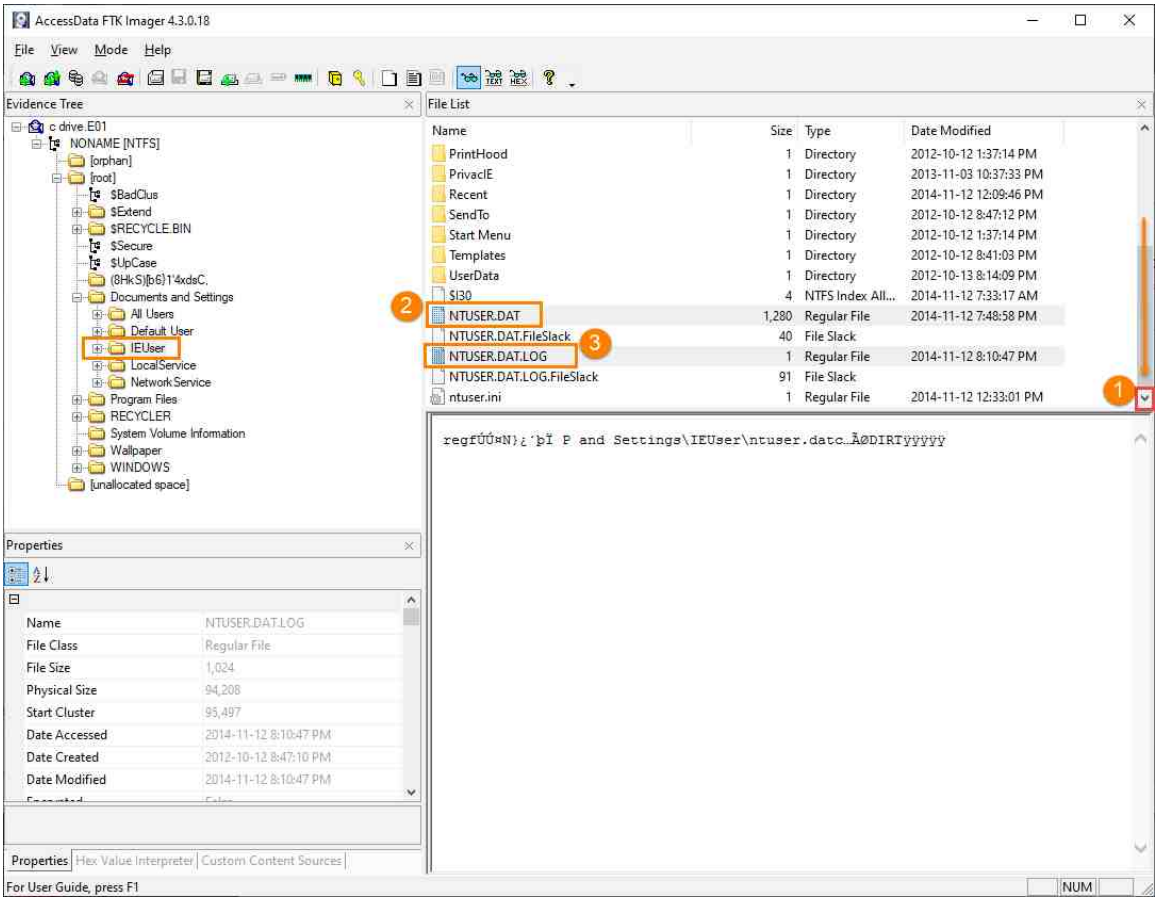


The folder that contains user data is called Documents and Settings in editions of Microsoft Windows XP and earlier versions of the Microsoft Windows operating systems. Since Microsoft Windows Vista, the Documents and Settings folder has been renamed to Users.

12. Now that you have expanded the Documents and Settings folder, you will see the list of user folders bearing the name of their associated user. The NTUSER.DAT file we are after is stored in the root of the IEUser folder. To access it, click the IEUser folder as seen below; this will reveal its contents in FTK Imager's File List pane.

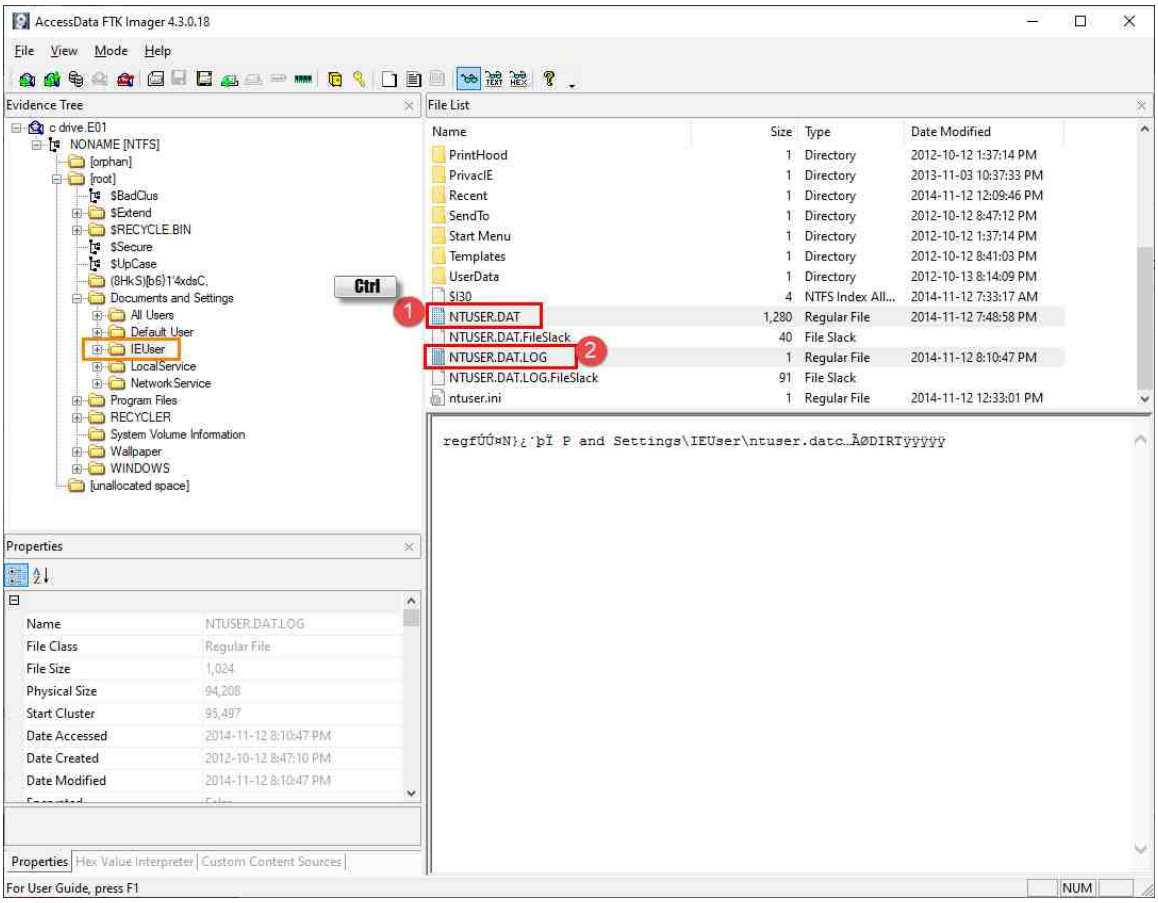


13. The File List pane will show all the IEUser's user files and folders. Normally the folders are shown first and the files after. Let us scroll to the bottom of the file list to see the files. You can scroll by placing your mouse in the File List pane and spinning the mouse wheel down or by clicking the down arrow highlighted in red. Scroll until you see the highlighted files below. The file labeled 2 called NTUSER.DAT is the registry file. The other file 3 is the transaction log file; It stores data that has been changed or deleted from the NTUSER.DAT registry file.



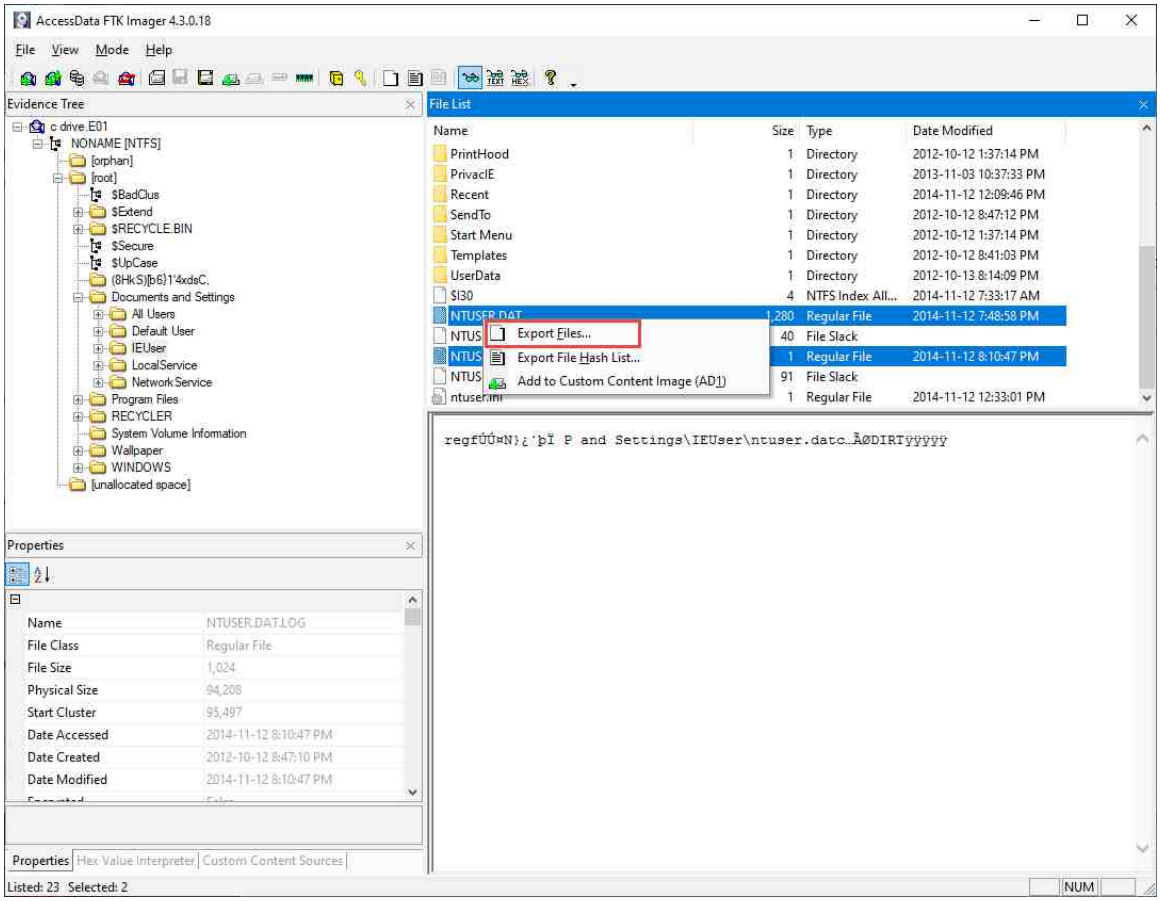
In practice, you should export the NTUSER.DAT file and any ntuser.dat.LOG* files to ensure you have the most complete data set.

14. To export the NTUSER.DAT and its associated log files, highlight them. This can be done by holding the Ctrl key and left-clicking on each of them. An example can be seen below.

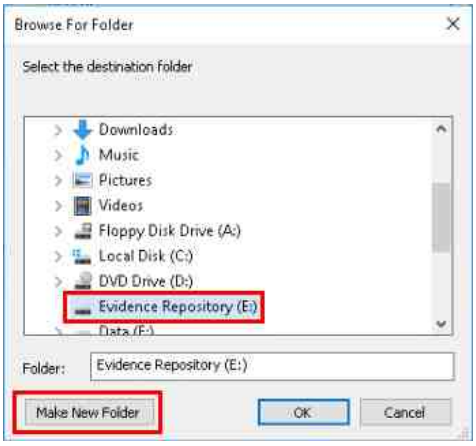


If this were a Live Examination, we could not export most registry files from a live system using FTK Imager's export function (or copying the files in Windows File Explorer).

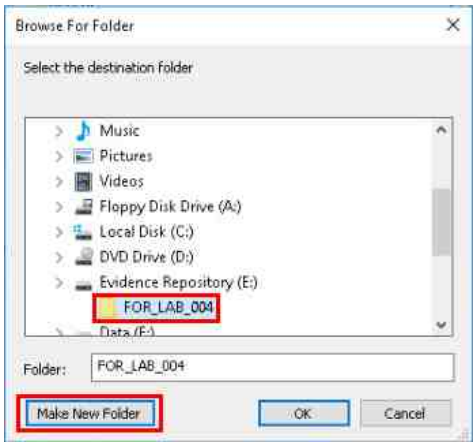
15. Now that they are selected, let us export them. To do this, right-click on one of the highlighted files and select the Export Files... option from the context menu that appears as highlighted below. This will bring up the Browse For Folder window.



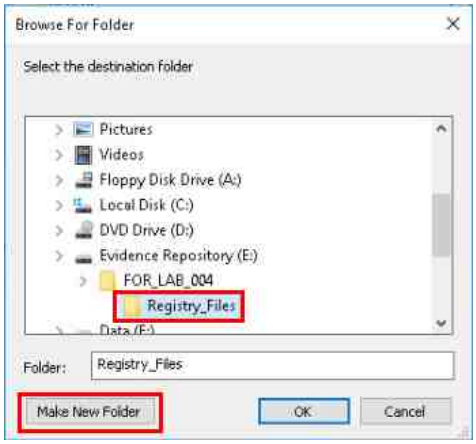
16. In the Browse For Folder window, navigate to the (E:) drive labeled Evidence Repository and click the Make New Folder button.



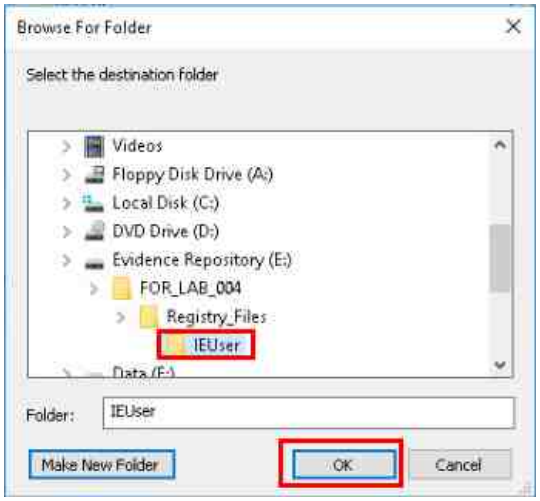
17. Name the folder `FOR_LAB_004` and create another folder within it by clicking on the folder you just created and click the Make New Folder button again.



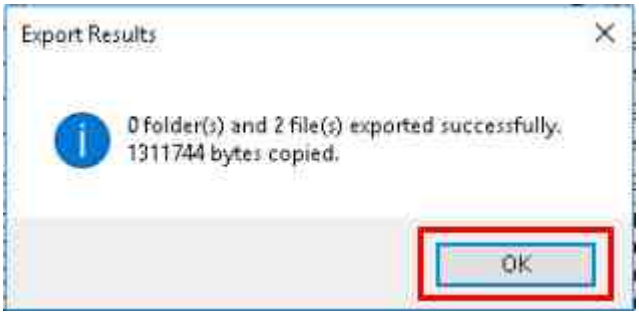
18. Name this new folder `Registry_Files` and then click Make New Folder to make one final sub-folder to identify the user that this file came from.



19. Name the final folder `IEUser` and then click OK; this will export the NTUSER.dat file to the specified folder for further analysis.



20. Now that you have exported the NTUSER.dat file. This will bring up the Export Results window. Click the OK button again to close the window and let us continue to learn where to find these files.

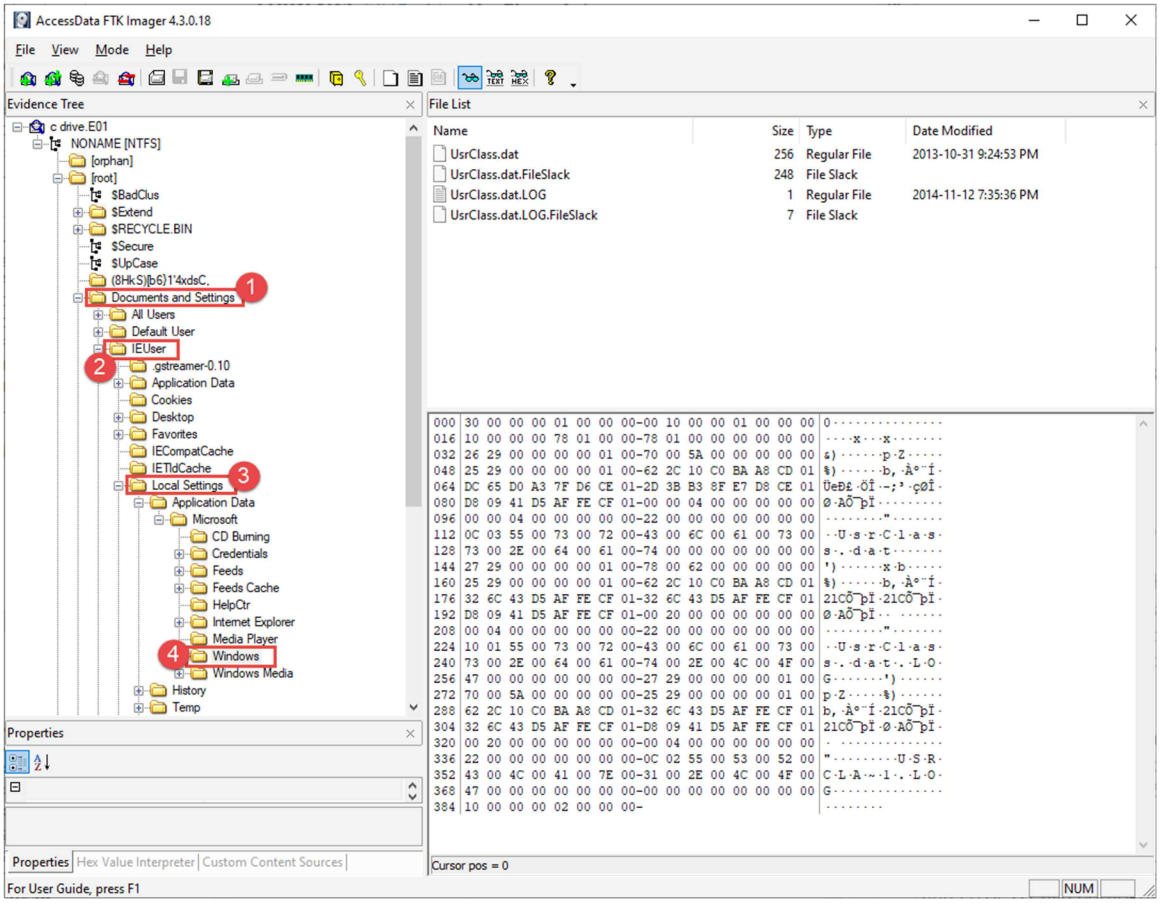


Each export performed will prompt a confirmation. Simply click out to continue.

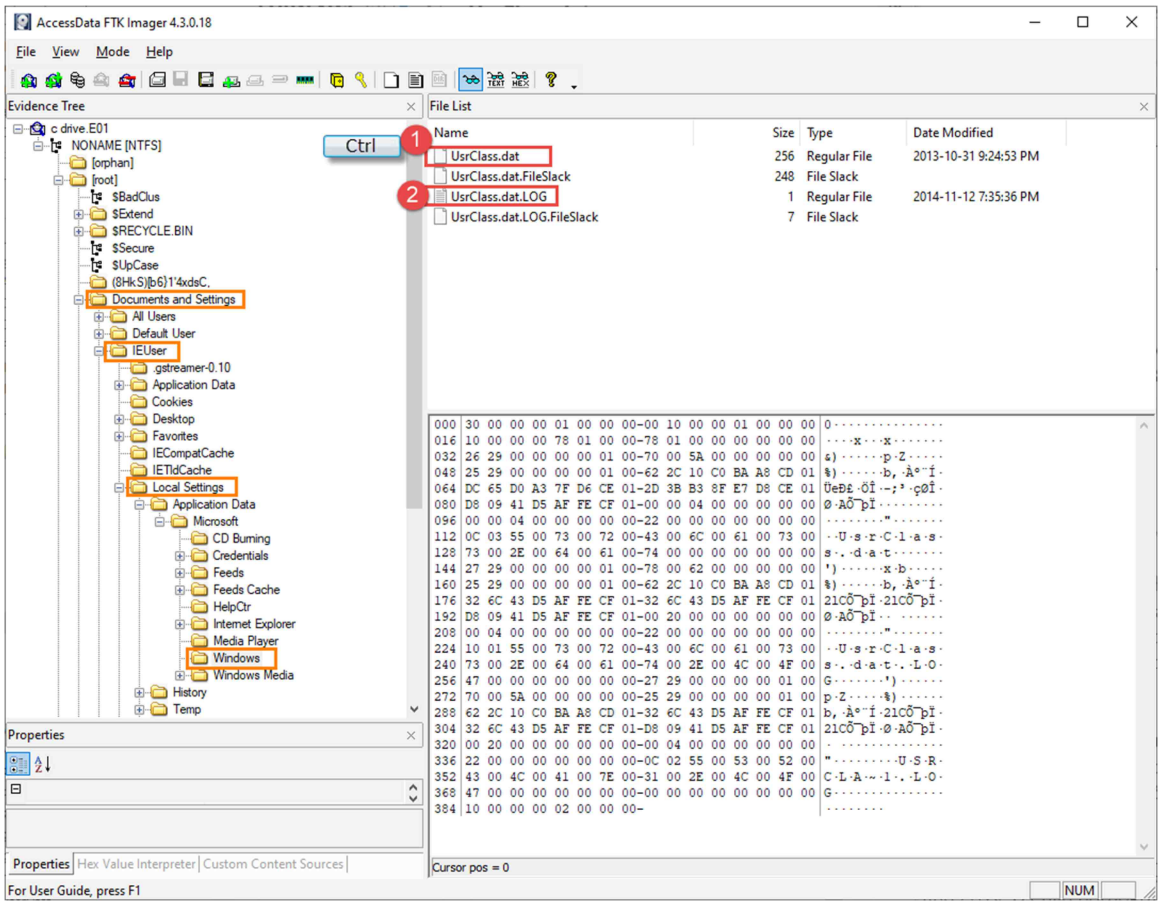
21. The next user-specific registry file is the UsrClass.dat file. This file contains, among other things, Shellbags, which are a set of registry keys that store configuration settings for Windows File Explorer. Shellbags store information about the size and positions of File Explorer windows and can help determine different folders that a user navigated and provide dates and times that they were accessed.

Since we are examining a FEF, we can export the registry files by right-clicking on them and selecting Export Files. Remember, this is not possible when examining a live system, however, the only hive that can be exported on a live system is the UsrClass.dat.

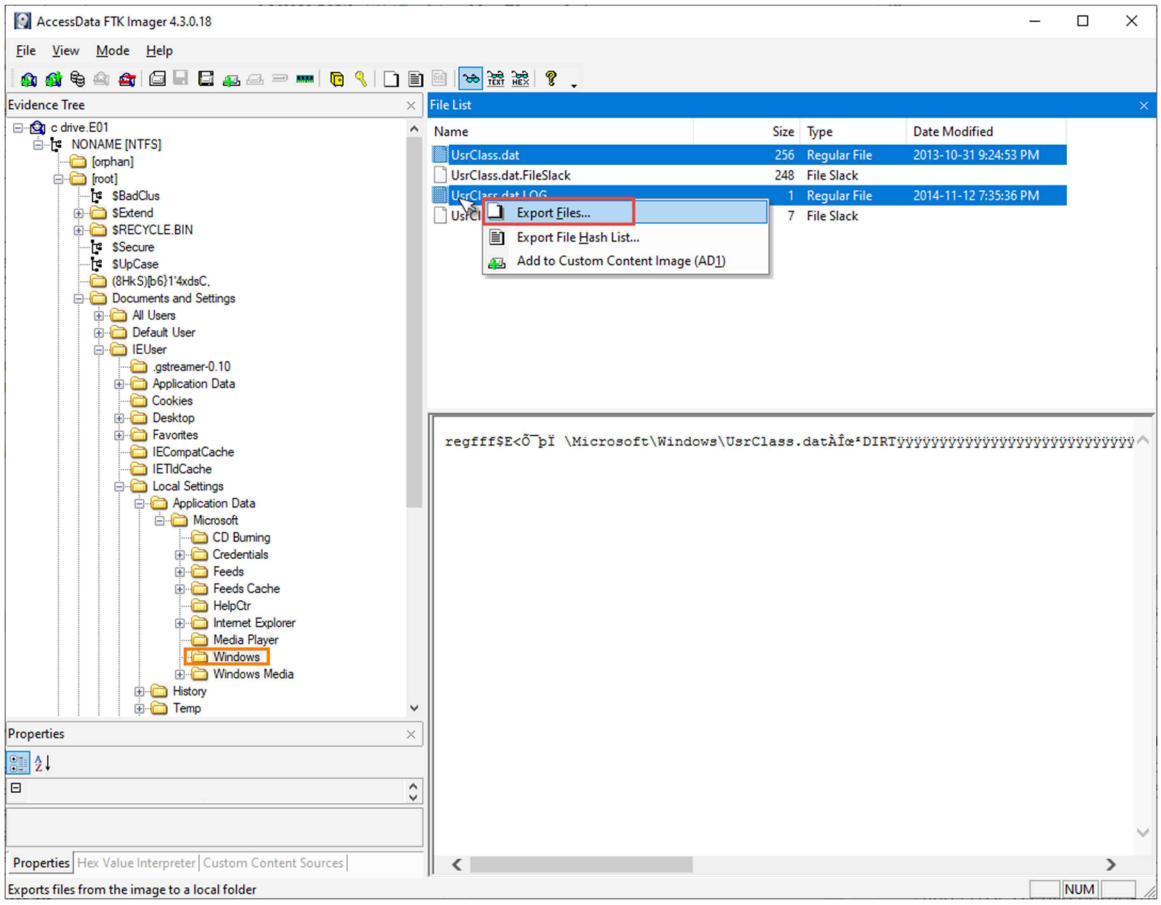
22. The UsrClass.dat file is in a subdirectory within the user's AppData folder. To get to this registry file, we need to navigate to Documents and Settings> IEUser > Local Settings > Application Data > Microsoft > Windows by clicking the + sign beside the folders as highlighted in 1,2,3, and 4 below.



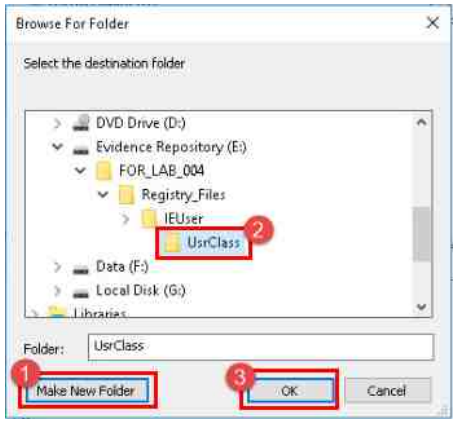
23. You will find the UsrClass.dat file in the root of the directory called Windows highlighted below. Click it to view its contents in the File List pane. The UsrClass.dat file and the associated transaction log files will appear. Now, let us export the UsrClass.dat and associated files. To export the UsrClass.dat and its associated log files, highlight them. This can be done by holding the Ctrl key and left-clicking on each of them. An example can be seen below, highlighted in items 1 and 2.



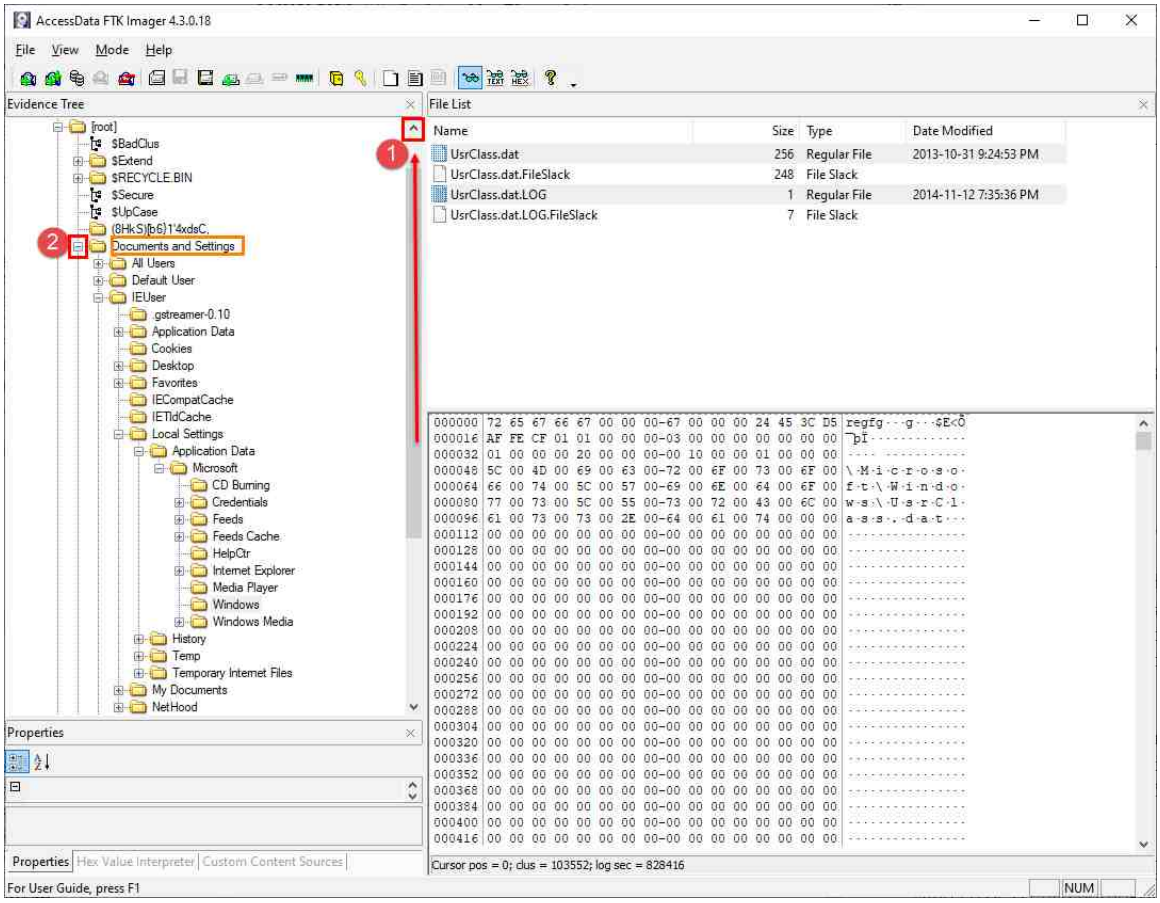
24. Now that they are selected, let us export them. To do this, right-click on one of the highlighted files and select the Export Files... option from the context menu that appears as highlighted below. This will bring up the Browse For Folder window.



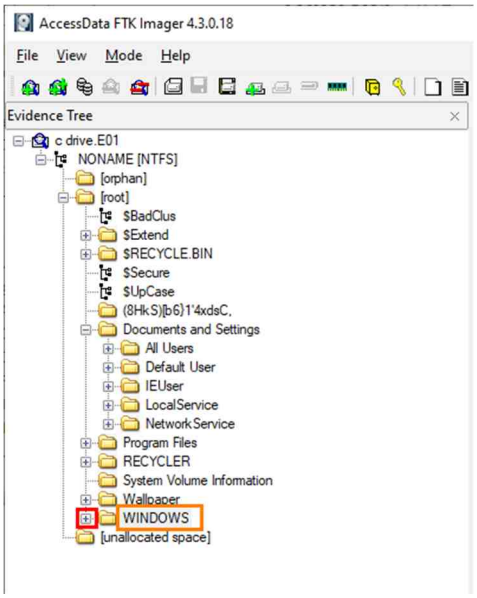
25. Navigate to the (E:) drive labeled Evidence Repository and save the registry file in the location FOR_LAB_004 > Registry_Files > IEUser > and click the Make New Folder button, highlighted in item 1. Name the folder `UsrClass` as shown in item 2 and then click OK as highlighted in item 3. This will export the UsrClass.dat file to the specified folder for further analysis.



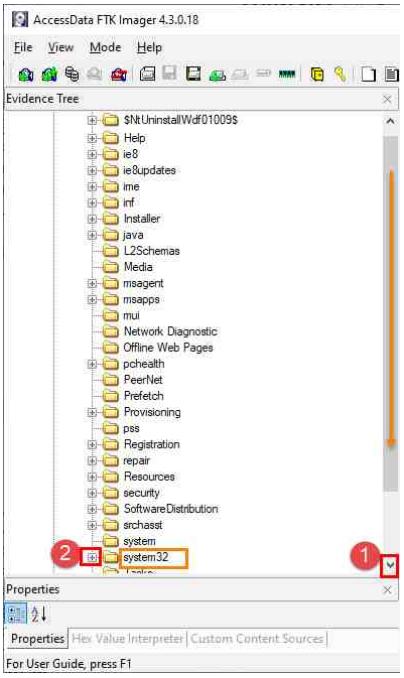
26. Let us continue to the remaining registry files. These are the universal registry files called SAM, SECURITY, SYSTEM, and SOFTWARE, and they are all located in the same folder. We must do some backtracking to get to these files. First, let us contract the folders we previously expanded just to make the folder tree easier to navigate. Do this by scrolling up in the Tree Pane until you see the Documents and Settings folder. Click the - sign beside the Documents and Settings folder to contract the folder tree as highlighted in item 2 below.



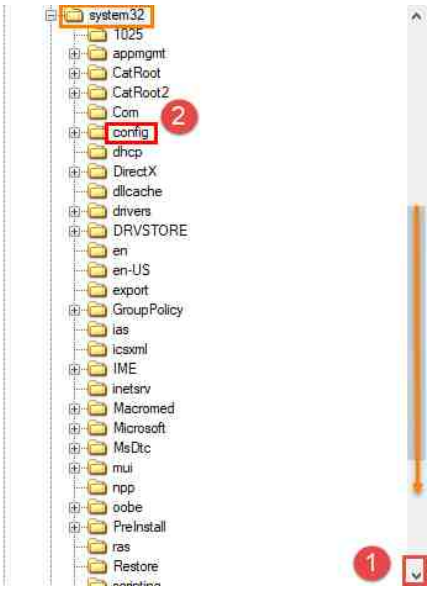
27. Now that the folder tree is contracted, we can see the folder called Windows that is in the operating systems root directory as highlighted below. Click the + beside the Windows folder to expand it.



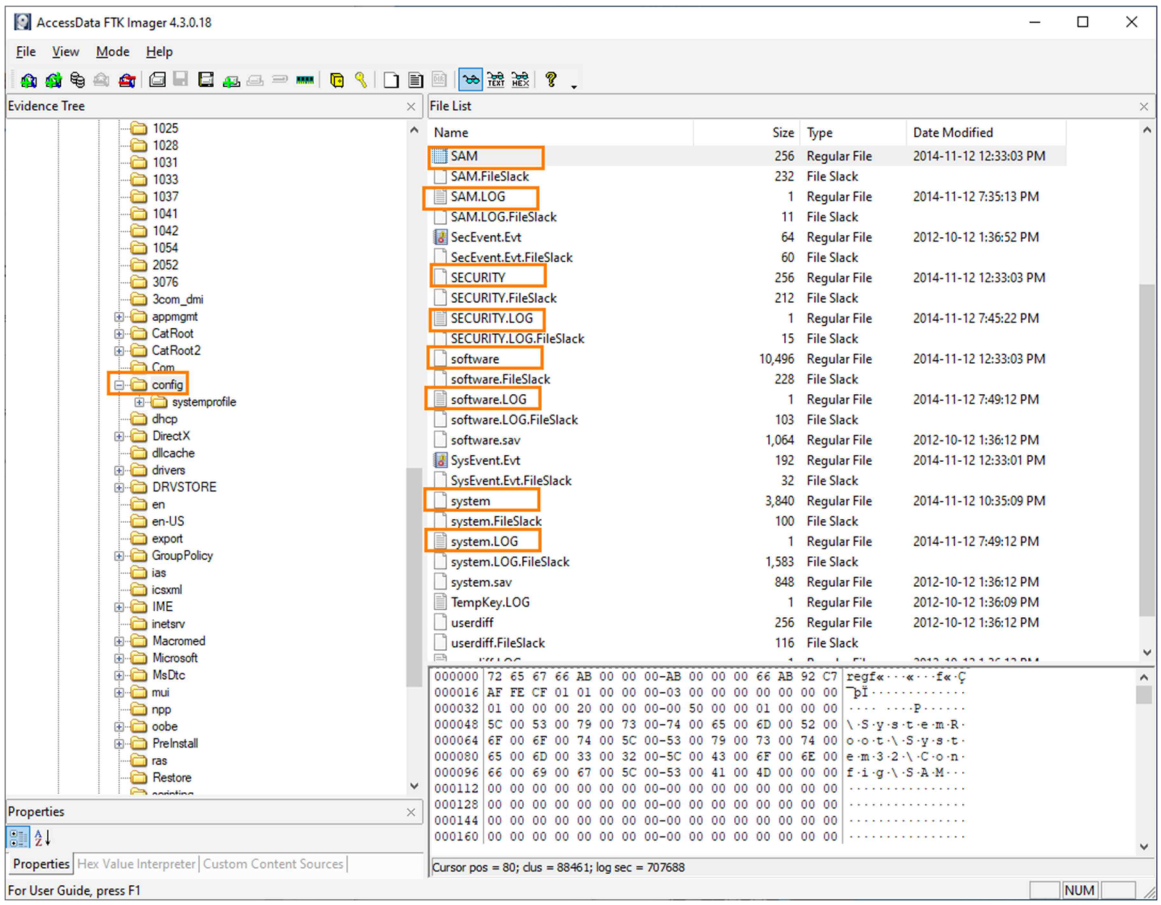
28. The Windows folder has many files and folders. The folder that contains the registry files is in the System32 folder and may require scrolling down to see it. Scroll until you see the System32 folder and click the + sign beside it, highlighted as item 2 below.



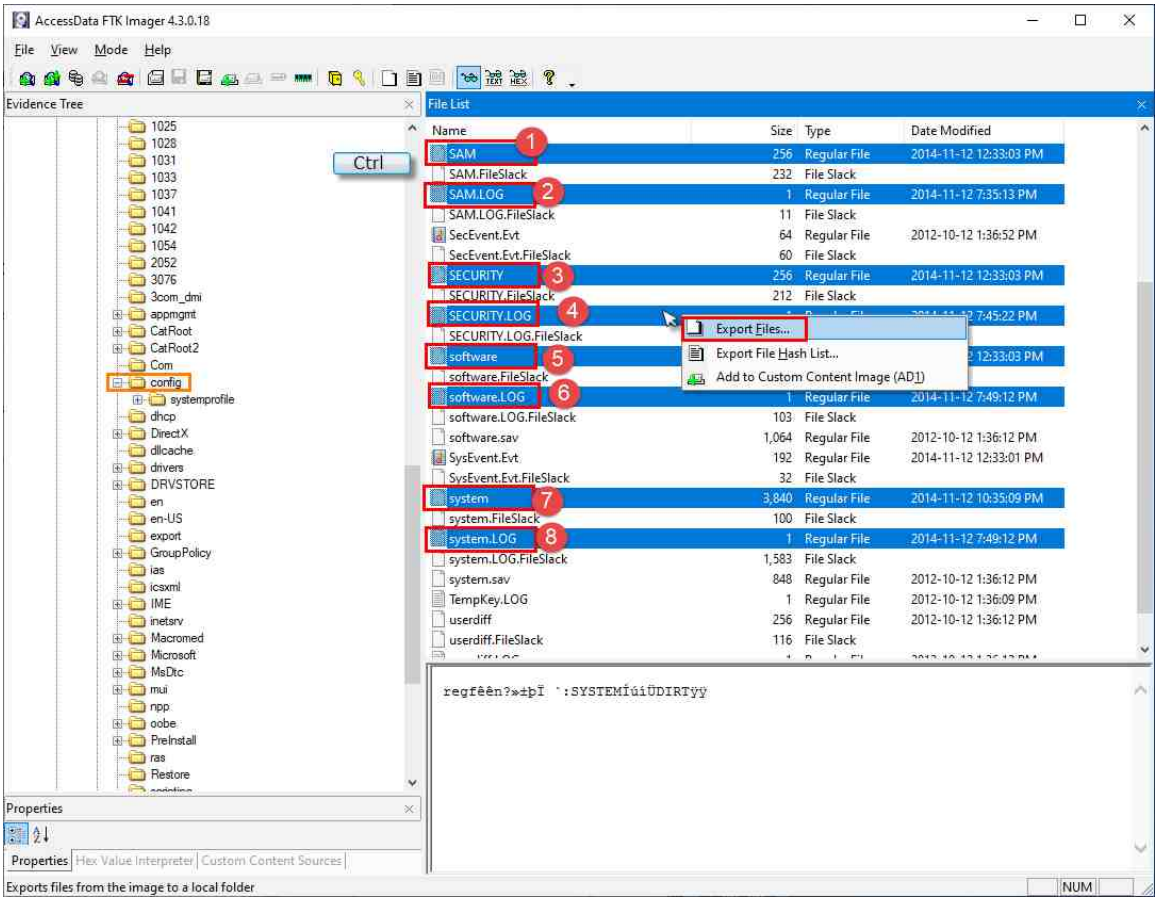
29. The System32 folder is another folder that has many files and folders. We are looking for the folder called config. To get to it, you may need to scroll down in the File Tree pane. Once you see the config folder, click it as highlighted below.



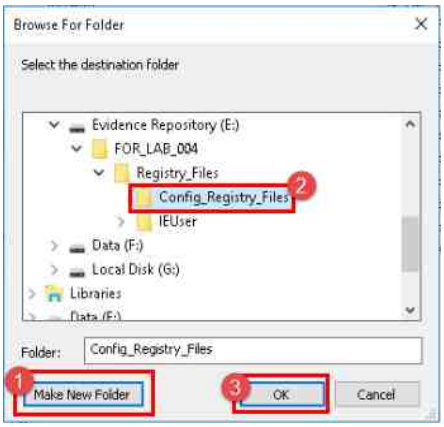
30. Now, let us look in the File List pane to identify the registry files. The system-wide registry files are unique in that they do not have file extensions. Scroll down in the File List pane to see each file and its transaction logs. The screenshot below lists the different registry files on this system.



31. Now, let us export the Registries and their associated files. To export them, highlight each by holding the Ctrl key and left-clicking on each. An example can be seen below, highlighted in items 1 through 8. Now that they are selected, let us export them. To do this, right-click on one of the highlighted files and select the Export Files… option from the context menu that appears as highlighted below. This will bring up the Browse For Folder window.



32. Navigate to the (E:) drive labeled Evidence Repository, open the folders FOR_LAB_004 > Registry_Files, and click the Make New Folder button. Name the folder `Config_Registry_Files` and then click OK this will export the SAM, SECURITY, SYSTEM, and SOFTWARE registry files and their respective transaction logs to the specified folder for further analysis.

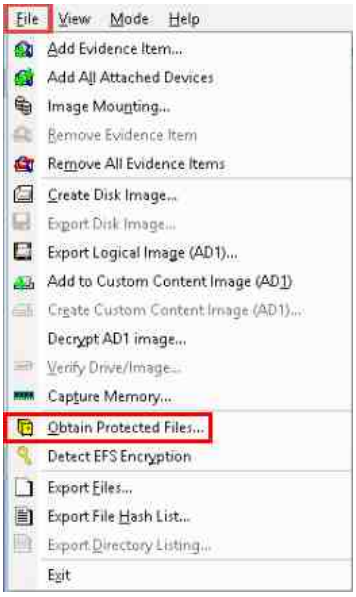


33. In this lab, we learned how to navigate to the Windows folder tree and locate the six common registry hives. Remembering how to find these files will help make cyber forensic examinations easier and more transparent.
34. We will now move on to the next exercise. Close FTK Imager and any other open windows by clicking the X at the top-right corner.

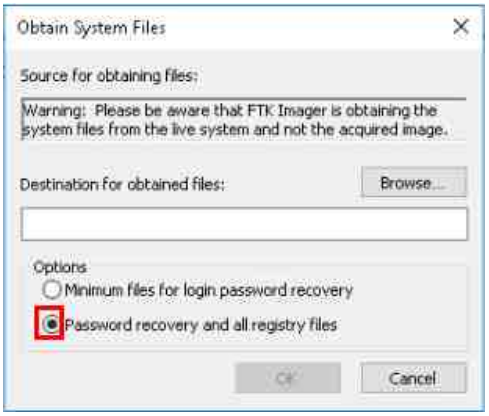
2 Exporting Registry Files from a Live System (General Knowledge)

Now that you know how to find and identify the files, let us learn how to export them from a live system.

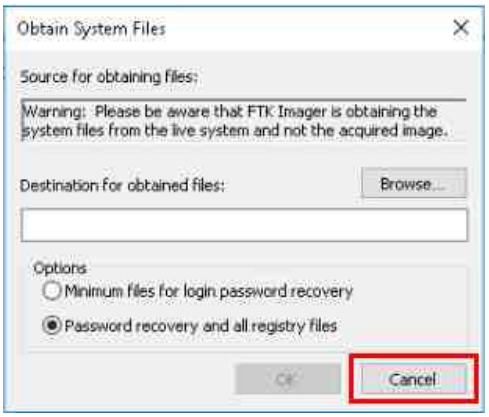
1. FTK Imager should still be open. If not, reopen it and click the File menu option from the Menu bar. Once the dropdown menu appears, click the Obtain Protected Files option as highlighted below. This will bring up the Obtain System Files window.



2. The Obtain System Files option gives the user the ability to export files that are normally locked by the operating system. To get all the registry files (except the UsrClass.dat), click the radio button beside Password recovery and all registry files as highlighted below.



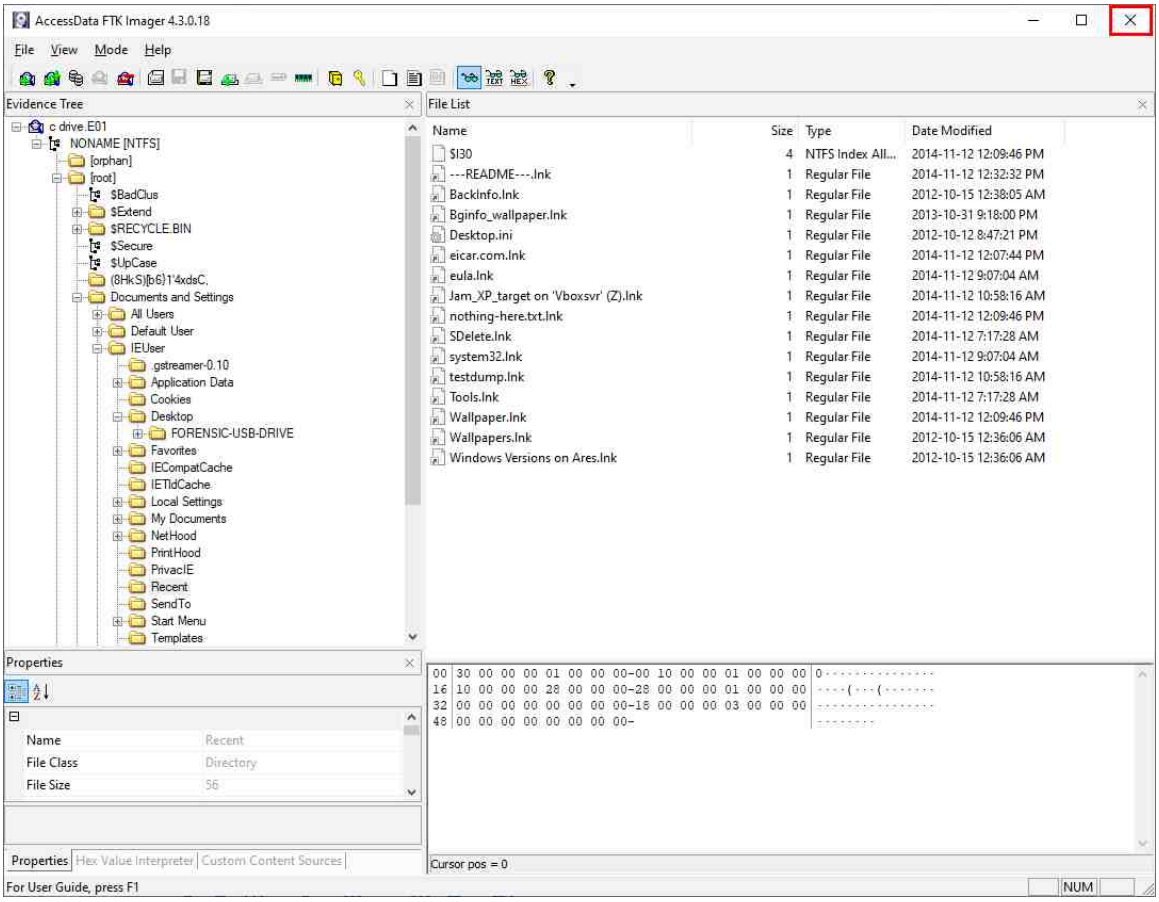
3. Next, you would normally click the Browse button to open the Browse For Folder window, which allows you to select a location to store the registry files; however, we are using a Forensics Evidence File. Let us move forward in the lab by clicking Cancel, as highlighted below.



Please Note

We will not export these registry files in this lab, but it is important to know how to export them while in the field.

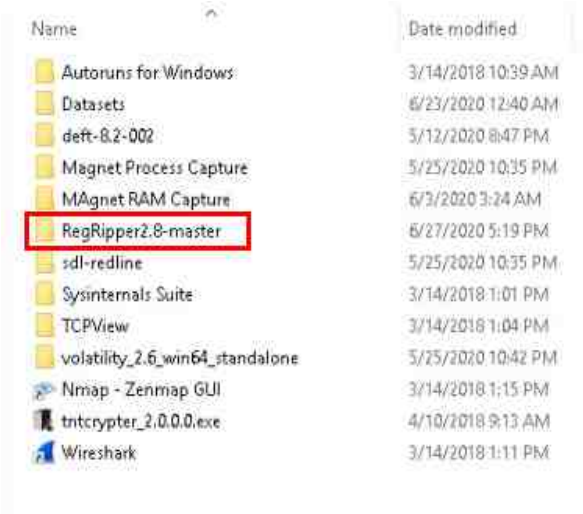
4. We will not be using FTK Imager for the rest of this exercise so let us close it by clicking the X at the top-right corner of the main window.



3 Getting Familiar with RegRipper

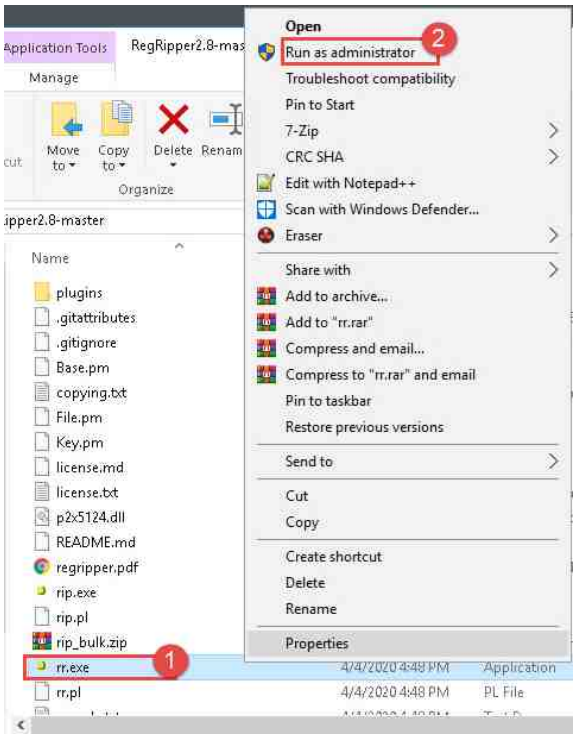
Once you have exported all the registry files, the next task will be to review the data within them. You can achieve this by using one of the many different tools available for examining the Windows registry. In this exercise, we will be using one such tool called RegRipper[1]. RegRipper is a lightweight, portable software that ingests registry files and provides a text-based report. The parsing of the registry is done using several plugins that come with the tool.

1. Let us begin by opening RegRipper. To do this, open File Explorer and browse to Desktop > Toolbox. Double-click the folder called RegRipper2.8-master highlighted below.

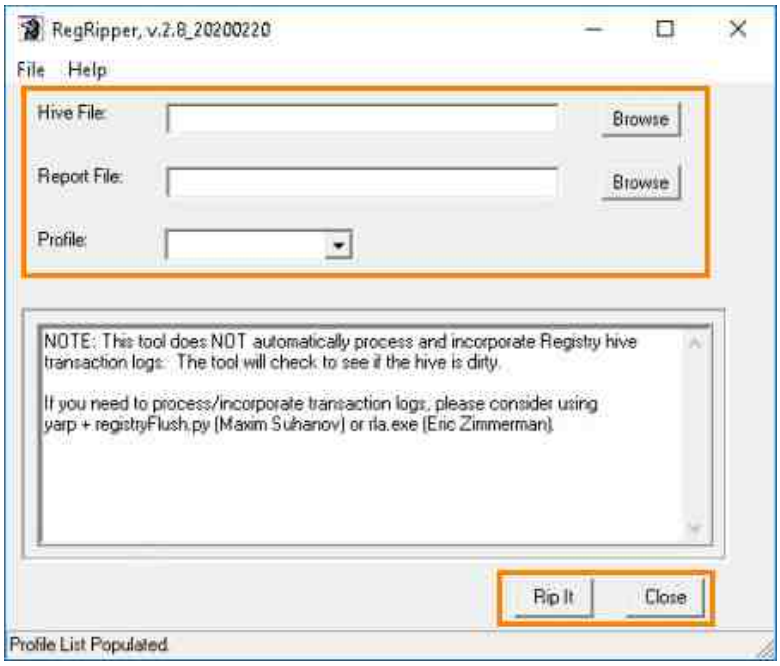


[1]https://github.com/keydet89/RegRipper2.8

2. In the RegRipper2.8-master folder, look for the file called rr.exe. This is RegRipper's executable. Right-click on rr.exe and then click Run as administrator from the context menu as highlighted in items 1 and 2 below.



3. The RegRipper v2.8 main window will appear. It is a very simple interface. The table below outlines the functions of the GUI interface.

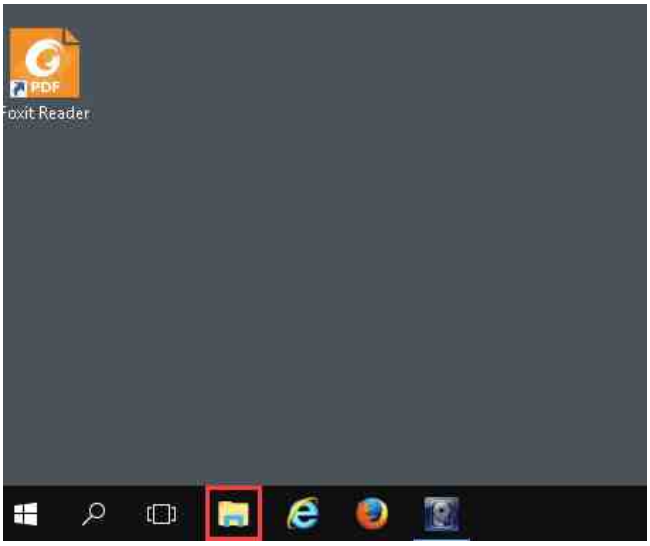


Hive File	The Hive File field is for the path of the registry file that you want to parse. Click the browse button beside it to locate the file.
Report File	The Report File field is for the path of the report for the registry file you selected in the Hive File field. Click the Browse button beside it to locate a destination for the report.
Profile	The Profile field is a dropdown menu that contains a list of profiles. Each profile contains plugins that are unique to each registry file. When using RegRipper, ensure that the registry file you selected in the Hive File field is the same as the profile.
Rip it	The Rip it button is the option that starts the registry parsing process.
Close	The Close button closes RegRipper.

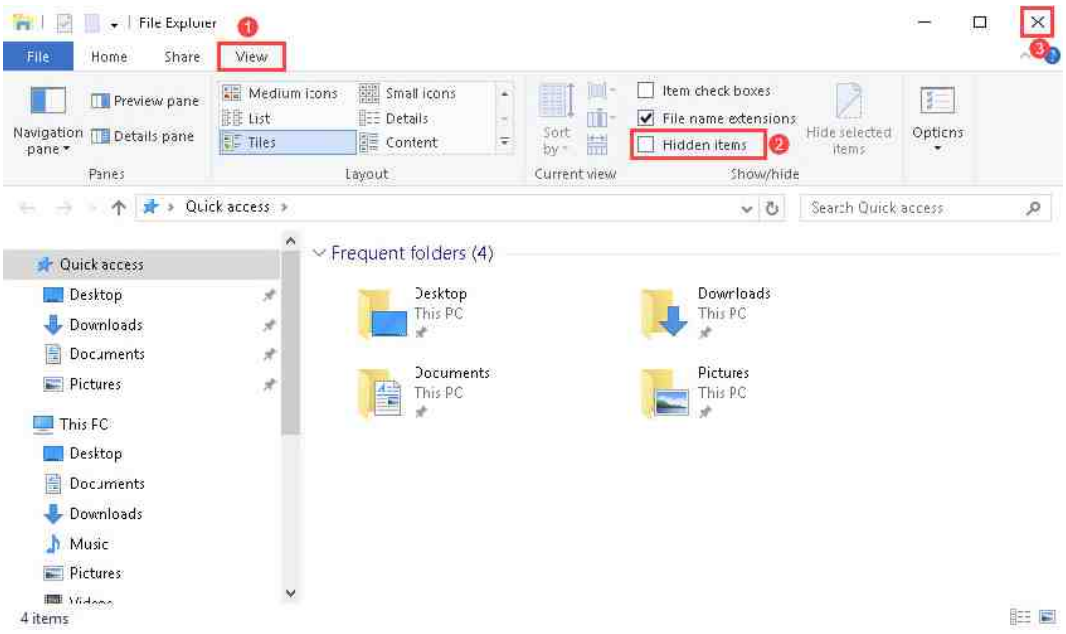
4 Parsing Registry Files with RegRipper

Now that you are familiar with the interface, let us begin parsing some registry files.

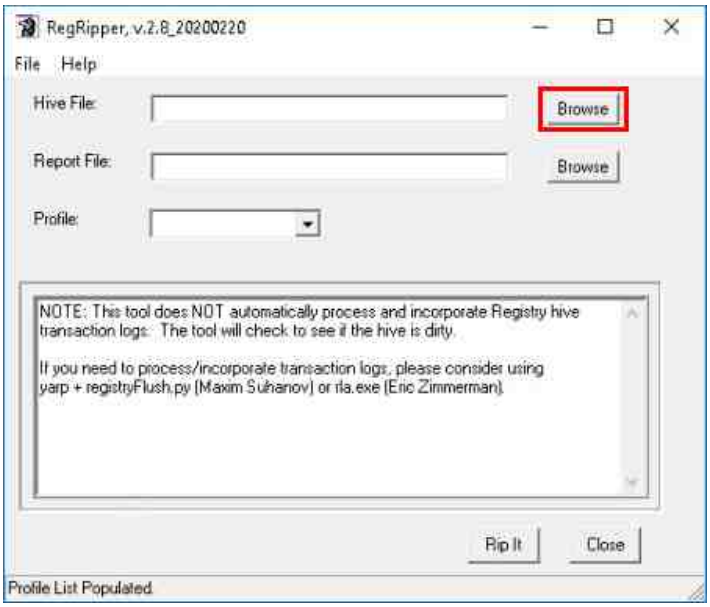
1. Before we begin, it is important to note that registry files are hidden by default. To view them, we need to enable Hidden Items in Windows File Explorer. To do this, click the Windows File Explorer icon from the taskbar as highlighted in the screenshot below.



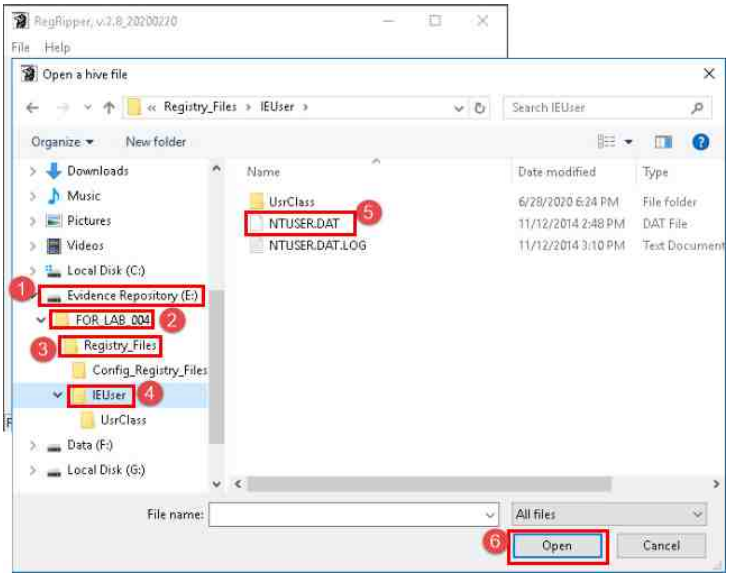
2. In the Windows File Explorer window that appears, click the View tab highlighted in item 1 below and then click the Hidden items checkbox, as seen in item 2, to reveal hidden files. Once you are done, close the window by clicking the X at the top-right corner of the window, as seen in item 3 below.



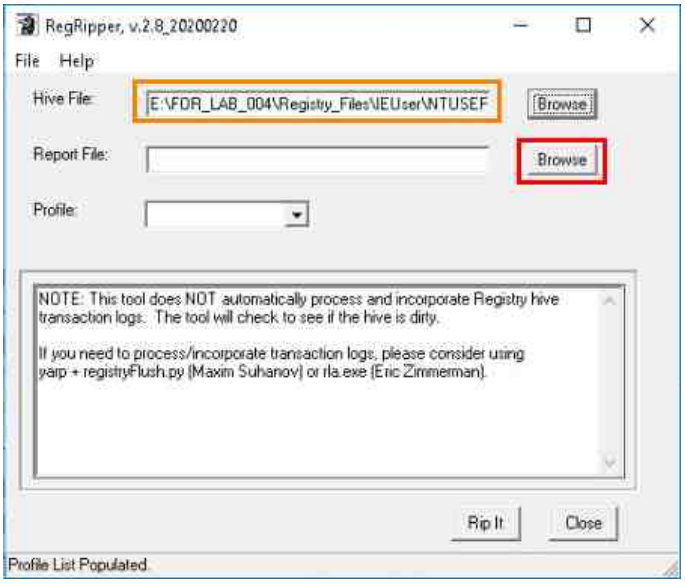
3. Now let us begin using Regripper. You should have RegRipper open already; if not, reopen it. Now let us click the Browse button beside the Hive File field. This will open the Open a hive file window.



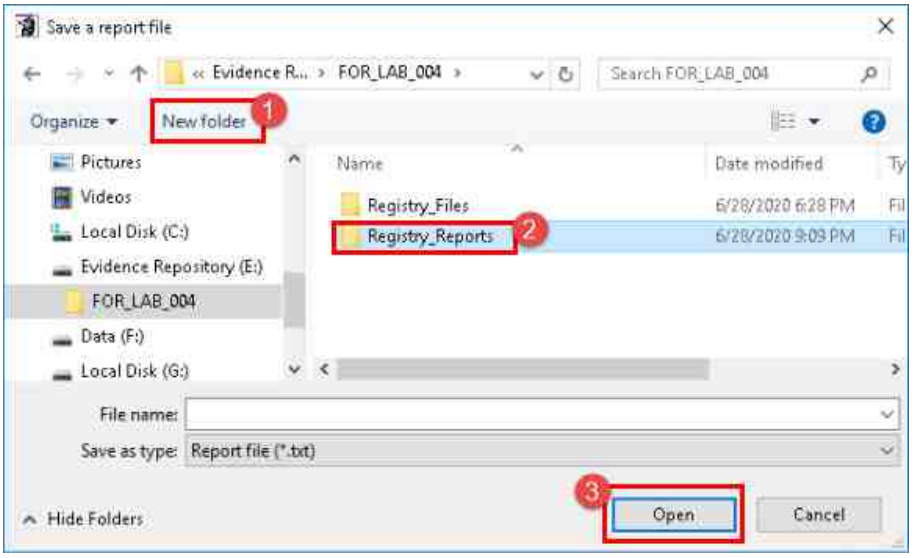
4. In the Open a hive file window, navigate to the NTUSER.DAT file we exported in the exercise earlier. Do this by clicking the folders Evidence Repository (E:) > FOR_LAB_004 > Registry_Files > IEUser as highlighted in items 1, 2, 3, and 4 below. Once there, it should reveal the NTUSER.DAT file in the view pane on the right. Now that you have located the NTUSER.DAT file, click it and then click the Open button as highlighted in items 5 and 6 to load the hive and return to the RegRipper main window.



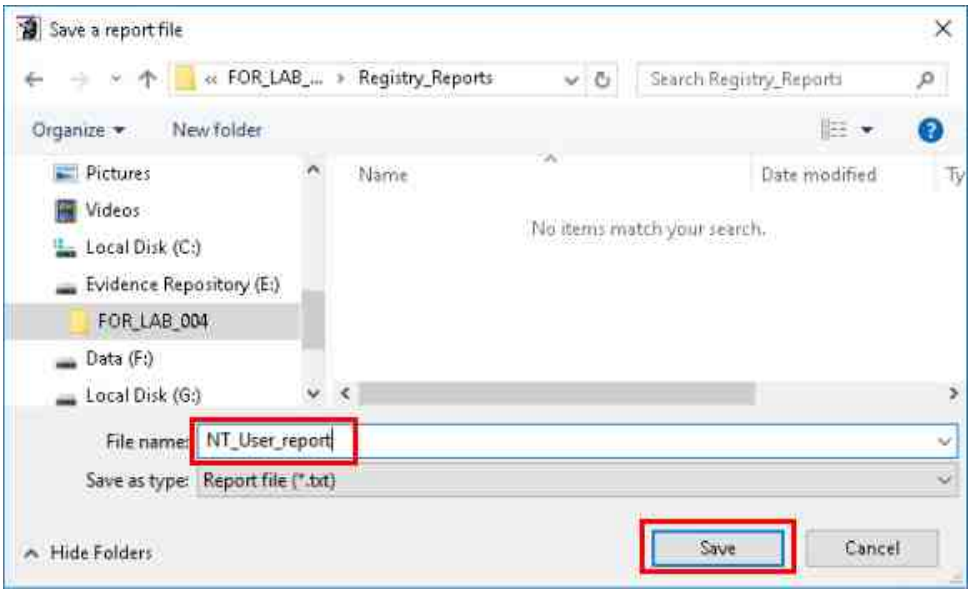
5. Now you should be back at the RegRipper main window, and the Hive File field should be populated with the path for the NTUSER.DAT file. Next, let us select a path for the report file. Do this by clicking the Browse button beside the Report File field as highlighted below. This will open the Save a report file window.



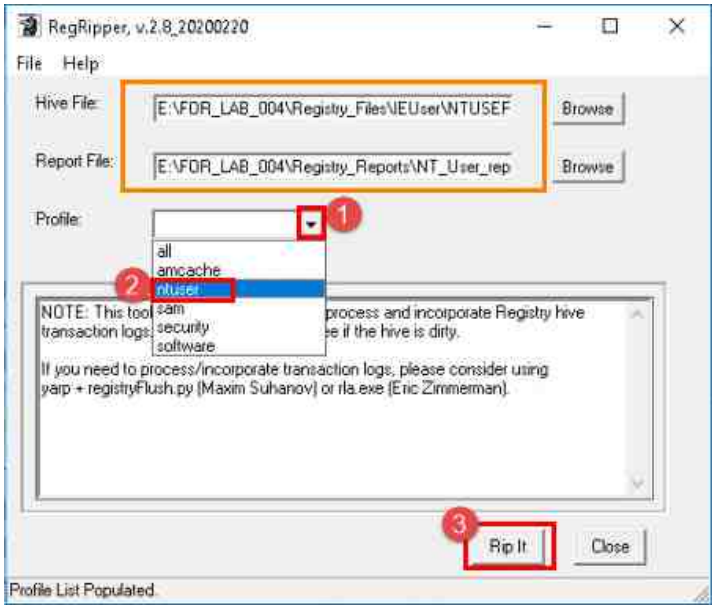
6. In the Save a report file window, browse to the FOR_LAB_004 folder you created on the Evidence Repository (E:) volume and click the New folder button. Name the new folder `Registry_Reports` highlighted below in items 1 and 2 and then item 3 by clicking Open.



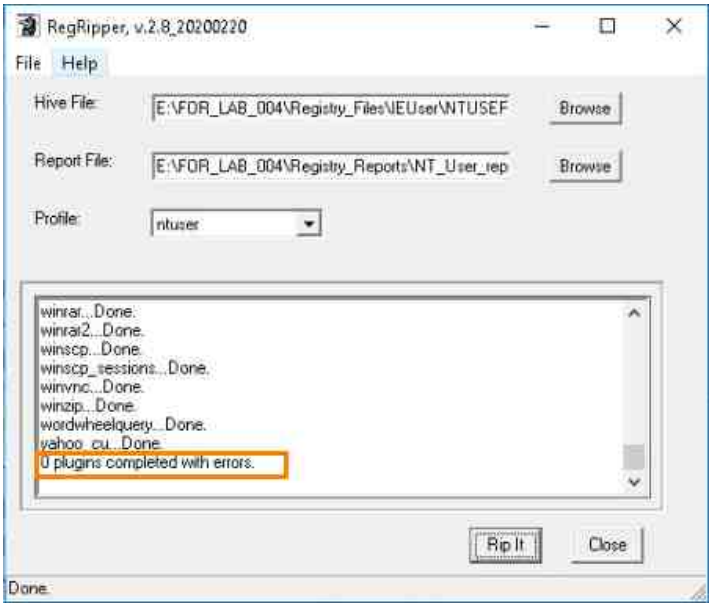
7. Let us give our registry report a name. Since this is the NTUSER.DAT file, let us call it `NT_User_report`. Once you have created the name, click the Save button highlighted below.



8. Now let us not forget the Profile field. As mentioned earlier, this is how RegRipper knows what type of registry file it is parsing. To select the profile for the NTUSER.DAT file, click the arrow beside the Profile dropdown field and then click the ntuser option from the dropdown menu highlighted below in items 1 and 2. Now, verify that you have all the correct settings selected before proceeding. Once you have verified that everything is correct, click the Rip it button highlighted below at item 3.



9. You will see the display area become populated as each plugin runs. You will see a message, plugins completed with errors once the parsing is complete.



The errors encountered in RegRipper can be reviewed in the log file to determine what exactly happened and whether you must manually review the registry to access the necessary data.

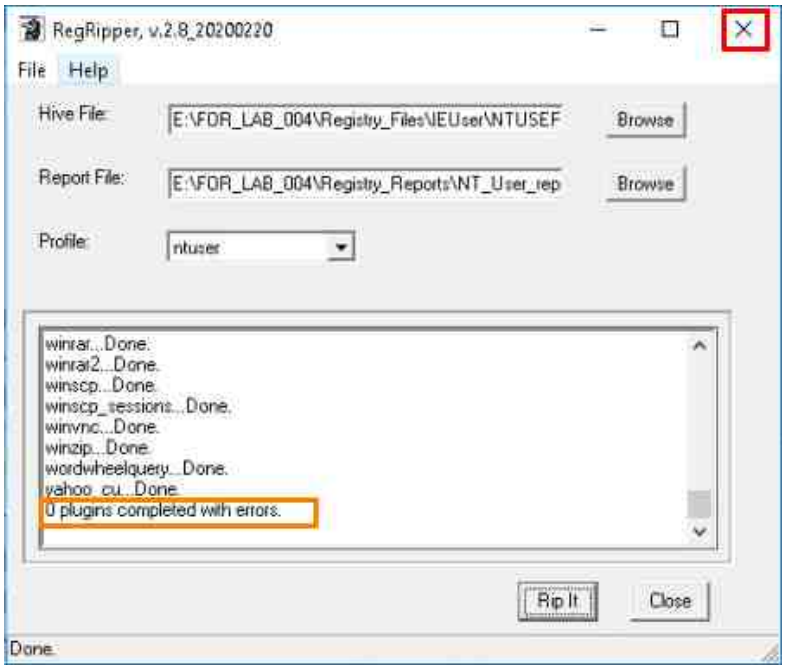
10. Now that you have parsed the NTUSER.DAT file, let us parse the remaining registry files. This can be done by repeating steps 1 - 9 using the registry files located at the following locations:

Be sure to name registry reports appropriately so you can identify them later. For example, SAM_report, SYSTEM_Report, etc.

11. Evidence Repository (E:) > FOR_LAB_004 > Registry_Files > Config_Registry_Files > SAM
12. Evidence Repository (E:) > FOR_LAB_004 > Registry_Files > Config_Registry_Files > SYSTEM
13. Evidence Repository (E:) > FOR_LAB_004 > Registry_Files > Config_Registry_Files > SOFTWARE
14. Evidence Repository (E:) > FOR_LAB_004 > Registry_Files > Config_Registry_Files > SECURITY
15. Evidence Repository (E:) > FOR_LAB_004 > Registry_Files > IEUser > UsrClass > UsrClass.dat

Please complete steps 11 – 15 before proceeding. Then close the application and let us move to the next step.

16. Now that you are done parsing the registry files, click the Close button on RegRipper to close the software.

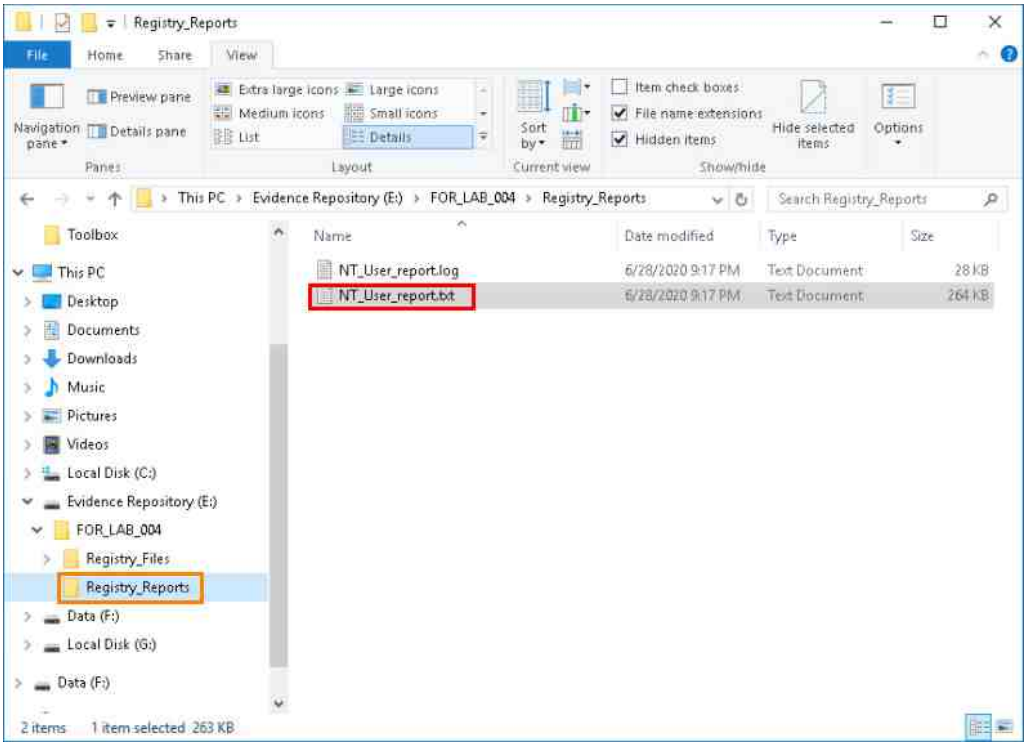


5 NTUSER.DAT File

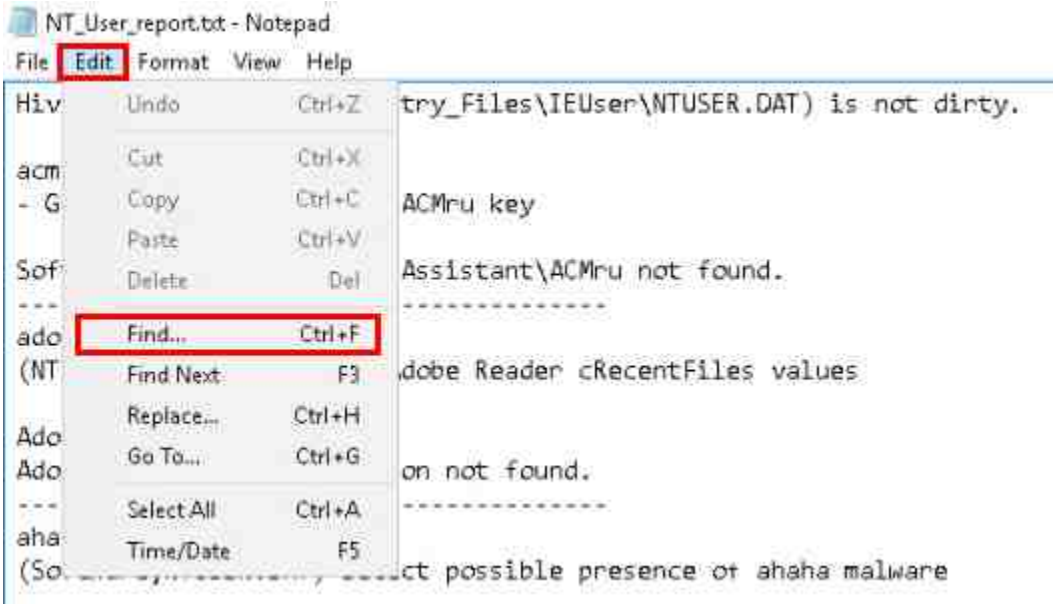
Now that you have generated the reports for the registry files, let us review the four (4) most common ones to see what kind of data each one stores. We will review the NTUSER.DAT, SYSTEM, SAM, and SOFTWARE. Let us start with the NTUSER.DAT report. Before we begin, it is important to note a few things. The first is that data in the registry is stored in two ways. There is the registry key, which can be compared to a folder, and there is the registry value, which can be compared to a file. Each registry key can have one or more values as well as sub-keys, which are synonymous to sub-folders.

Registry values sometimes have a number or letter before the value. This is known as the MRUListex order, which places the value for the most recently accessed file at the top of the list. It can be confusing at times because they do not necessarily have to be in alphabetical or numerical order. The number or letter associated with the value refers to the first time the file was accessed. For example, if there are two values, a = office.doc and b = office2.doc, then it means that office.doc was the first file opened. If a = office.doc is at the top of the list, it means that office.doc was the first one opened, then office2.doc was opened sometime after, and then office.doc was opened again after that. This bumps office.doc back to the top of the list because it was the most recently used file. Let us look at the data to get a better understanding.

1. To access this report, browse to the folder called Registry_Reports located at Evidence Repository (E:) > FOR_LAB_004 > Registry_Reports. Once you get to the folder, double-click the file we named NT_User_report.txt to open it in Notepad, as seen below.

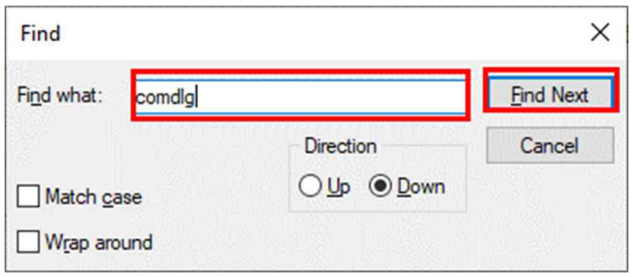


2. The registry report may seem overwhelming at first but do not be daunted; it is easy to use if you know what data you are looking for. In the NT User registry hive, you can find things like Recent Files, programs and services opened from the RUN feature and URLs typed by the user. You can also find data about the programs that were run and the last time they were run as well as many other things. Let us look at a few of these artifacts.
3. The first one we will check out is the Comdlg32 registry key. You can find this registry key by scrolling down until you see the heading or by searching the document for the term comdlg32. To search for the term, click Edit from the Menu bar and click the Find option from the dropdown menu as highlighted below.



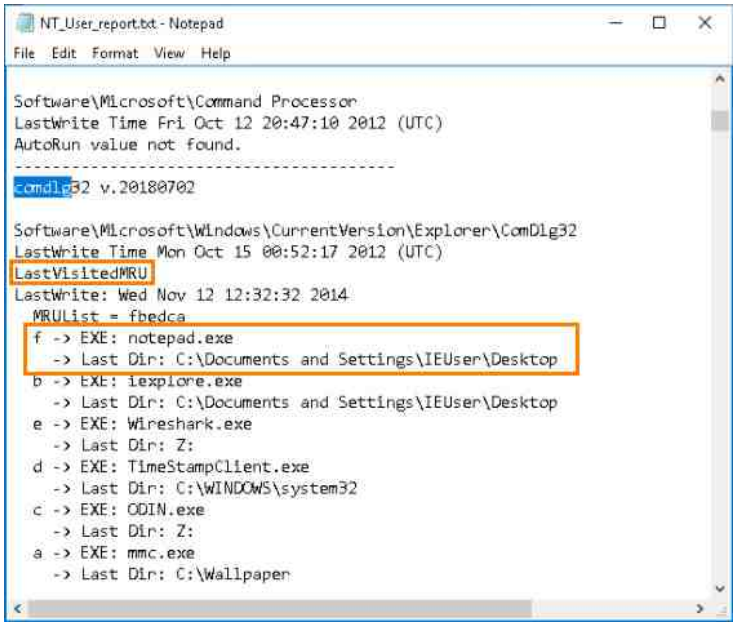
It might be easier to navigate if you maximize the notepad window.

4. When the Find window appears, type the term `Comdlg` and click Find Next as seen below.

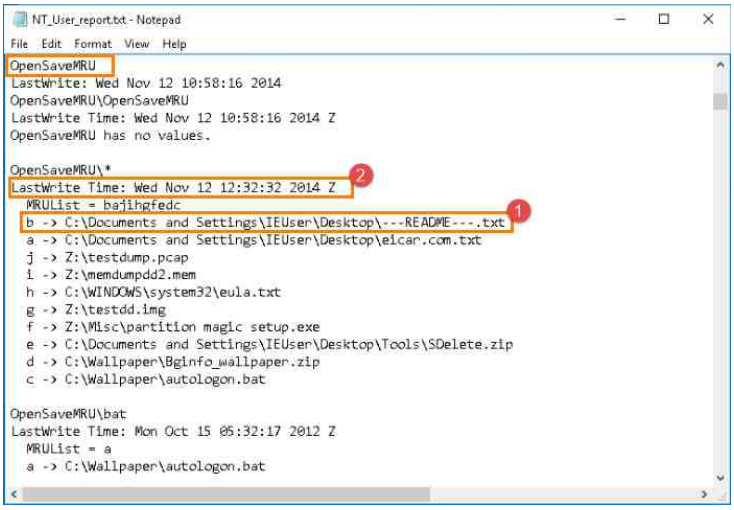


If the search does not find the term, then change the radio button beside the direction from Down to Up or vice versa. If it still does not work, then check that you typed it correctly.

5. Once you found the comdlg32 artifact, scroll down and look at the entries as highlighted below. The comdlg32 stands for Common Dialogue and is a registry key that contains the list of LastVisitedMRU (Most Recently Used) and OpenSaveMRU files. The OpenSaveMRU provides data about files that have been opened or saved within most Windows dialog boxes. The LastVisited MRU compliments the Open/Save MRU as it lists the specific location of the application used to open the files listed in the OpenSaveMRU.



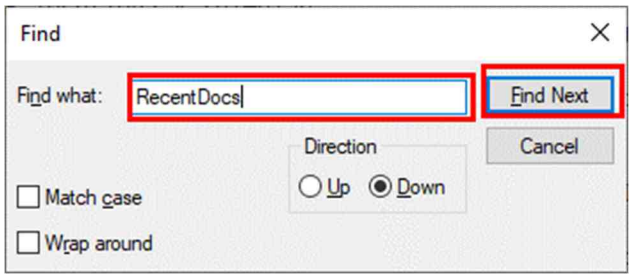
6. As you can see from the screenshot below, the path and the name of the last file reported in the OpenSaveMRU is C:\Documents and Settings\IEUser\Desktop\---README---.txt highlighted as item 1. If you look now on the LastVisited MRU, you will see that the last program used was notepad.exe, and the same path that is listed for the ---README---.txt file is listed beneath notepad.exe in the LastVisited MRU (listed in step 5 above). The LastWrite Time is highlighted as item 2 and reflects the date and time the registry key was last updated and is normally the same date and time that the item at the top of the list was opened.



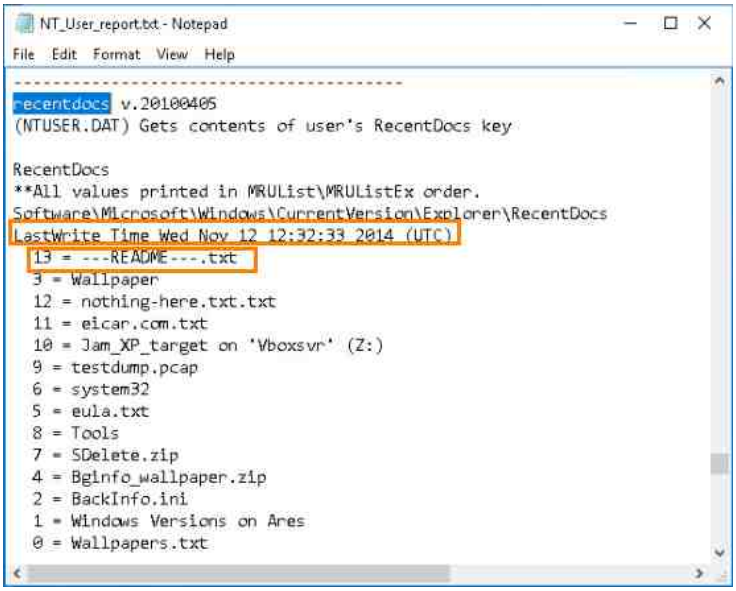
The parsed registry files will show a 'Z' when referencing time. This indicates Zulu time, generally as a term for Universal Coordinated Time (UCT).

7. Also, note the letters beside each value. The notepad.exe has f beside it and is the highest letter sequentially. This means that it was the last item that was added to the list and was the most recently opened one as well. Alternatively, the ---README---.txt file in the OpenSaveMRU has the letter b beside it. This indicates that it was the second file added to the list and means all the files listed between c to j were opened sometime after. The fact that the ---README---.txt file is at the top of the list, however, means that it was the one that was opened most recently.

8. The next artifact we will look at is the RecentDocs registry key. As the name suggests, a list of the recently opened documents can be found here. Let us use Find again to locate the artifact. You should still have the Find window open, if not, reopen it. Once you are in the window, type `RecentDocs` and click Find Next.

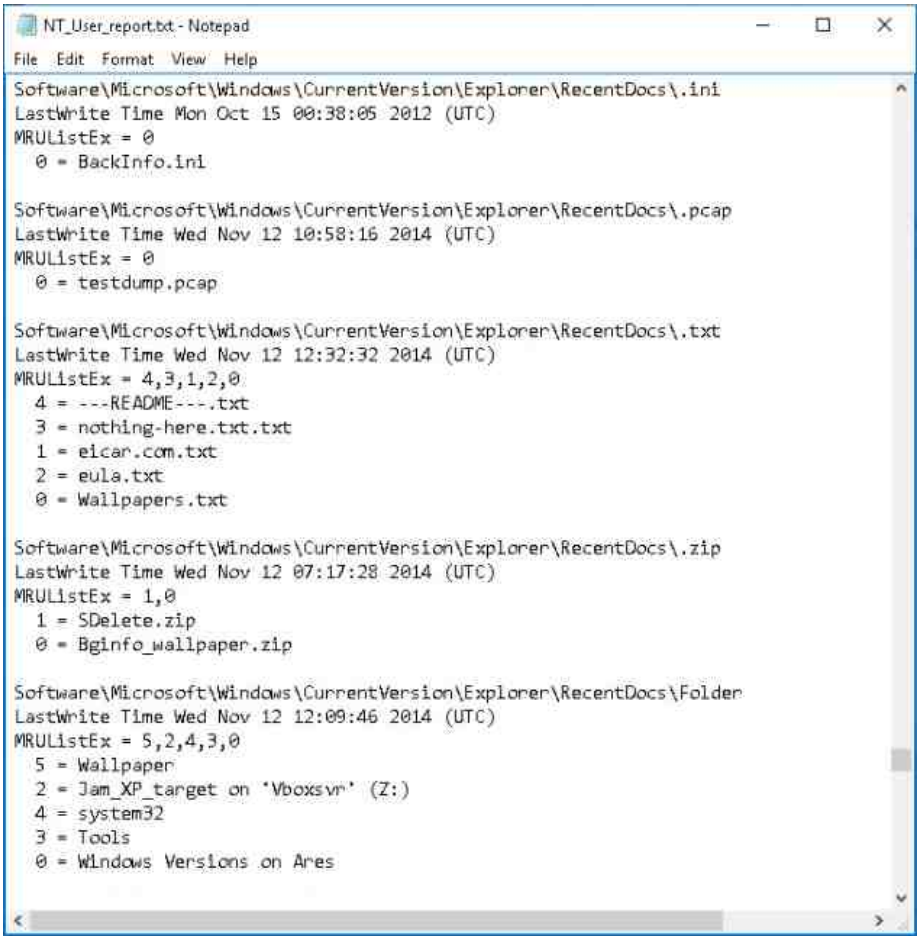


9. Once Find reveals the RecentDocs registry key, look at the values. As seen in the screenshot below, there are fourteen (14) filenames listed as recent documents. As with the other registry keys, the LastWrite Time highlighted below is the same as the time that the most recent file was opened (The last time the key was updated). As seen in the screenshot below, the same file called ---README---.txt is at the top of the list, which means it was the last file opened by this user.



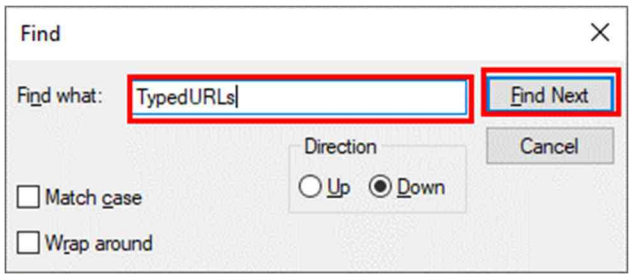
This can be very valuable in determining what files were last accessed and find files that would not normally stand out (Like the one called nothing-here.txt.txt).

10. Let us scroll down to the registry sub-keys for RecentDocs. The lists in these sub-keys are recent documents, but they are sorted based on extension. This is helpful when trying to focus on a specific filetype, to get a LastWrite Time for a specific file, or sorting through large lists.

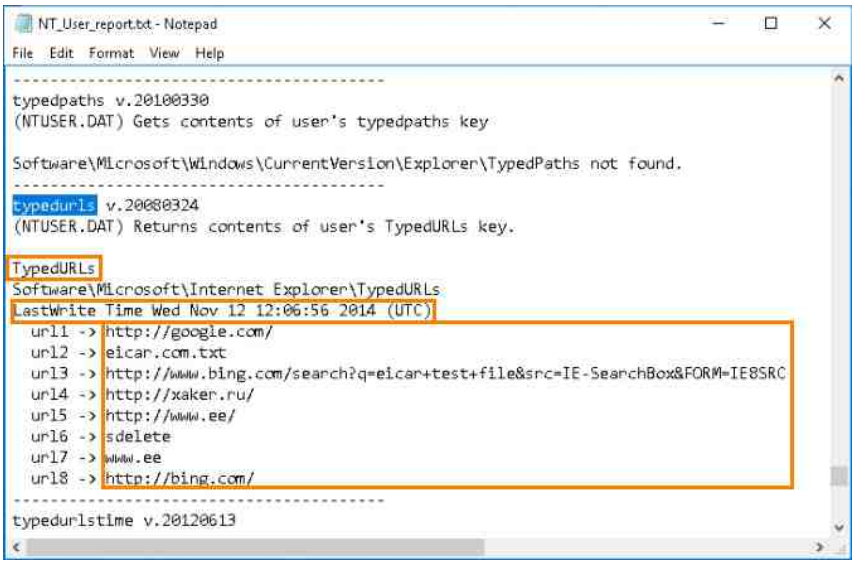


The dates and times in RegRipper's reports are in the UTC time zone. Be sure to pay attention to this and convert the times to the appropriate time zone.

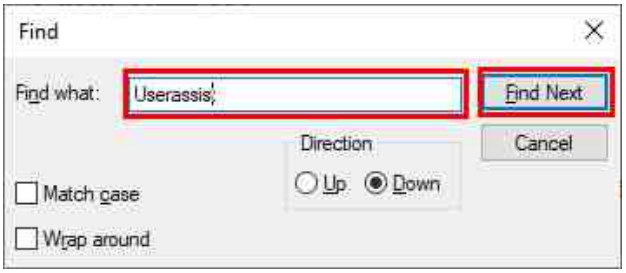
11. Let us look at another useful registry key in the NTUSER.DAT file. This one is the TypedURLs, which, as the name suggests, contains a list of URLs that were typed by the user. You should have the Find Window still open; if not, reopen it and type TypedURLs as the search term, then click Find Next.



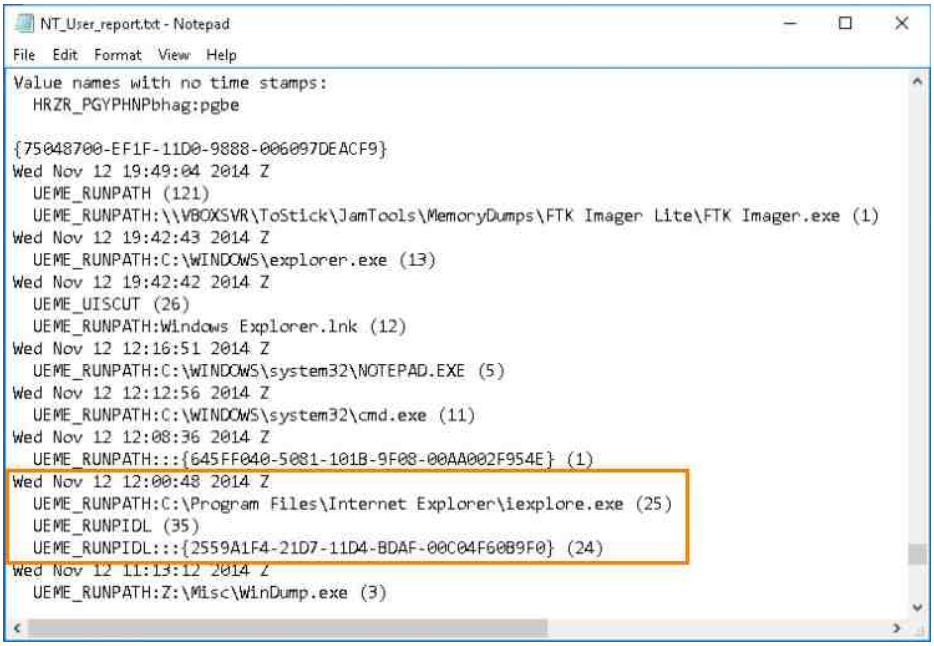
12. Once you get to the TypedURLs registry key, look at the values in the list. This registry key lists URLs that were typed in the Internet Explorer web browser. As with the other lists, it is in the order of most recently typed and has a LastWrite Time that is updated each time a new entry is typed as well. Unlike the other registry values, the item at the top of this list will always be URL1. When a new URL is typed, the old one gets the number URL2, and all the other URLs in the list are updated as well. As with the others, the LastWrite Time is the same as the time the URL was typed.



13. The last one we will look at is the UserAssist. You should have the Find Window still open; if not, reopen it and type `UserAssist` as the search term, then click Find Next.

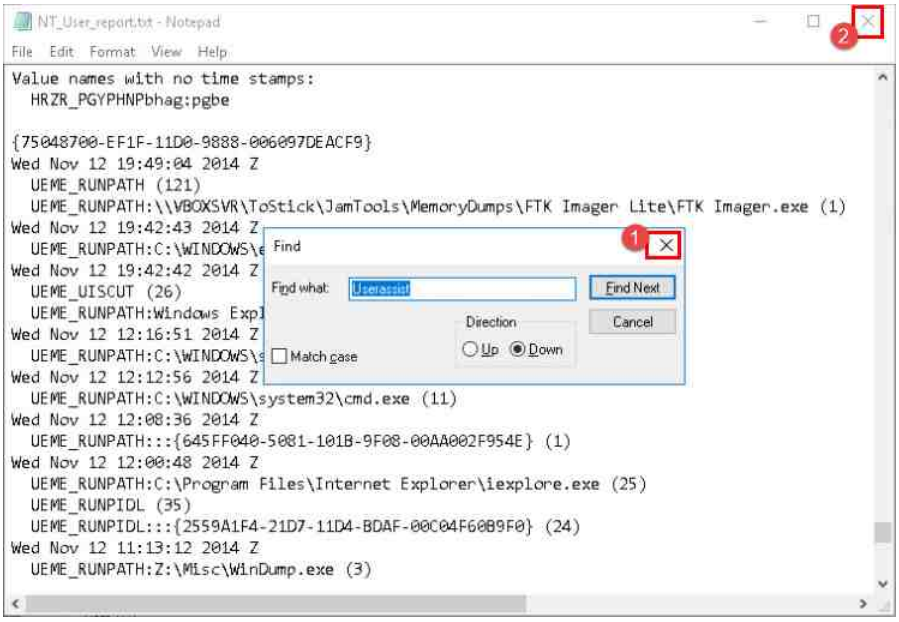


14. Once you are at the UserAssist key, you will see a list of programs that were run on the system. This key contains the date and time that each software was last used and the number of times it was run. The run count is represented as the number in brackets in the report below.



15. The UserAssist key is great for showing that a user ran certain programs and how often they did. It can also differentiate between whether the program was run using a shortcut or the executable.
16. The NTUSER.DAT file has many more useful artifacts, but we cannot touch them in this exercise. We will now move on to another useful registry file.

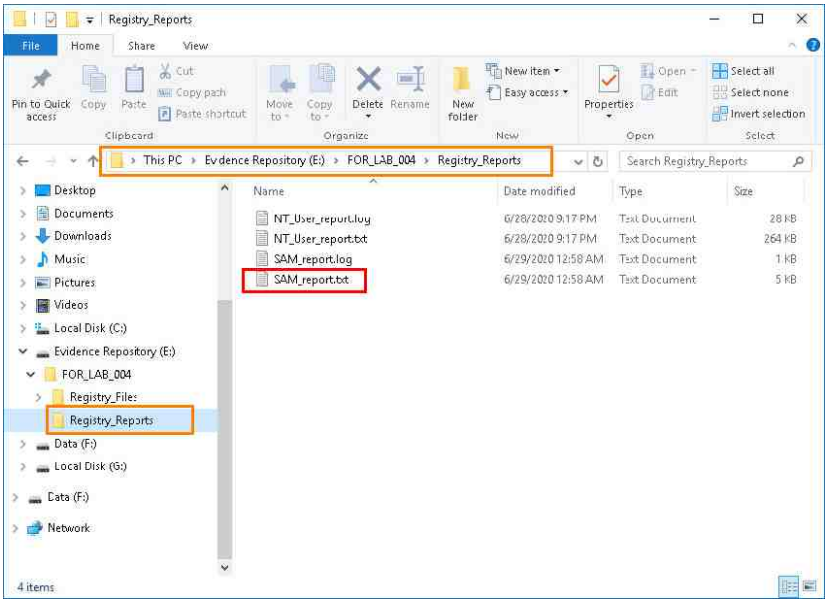
17. Now that you are done, close the Find window and the Notepad program by clicking the X at the top-right corner as highlighted below.



6 SAM Registry File

Now let us look at the SAM report that you created. The SAM registry hive stores data about each user account and can be used to help attribute physical users with their user account.

1. To access this report, browse to the folder called Registry_Reports located at Evidence Repository (E:) > FOR_LAB_004 > Registry_Reports. Once you get to the folder, double-click the file we named SAM_report.txt to open it in Notepad.



2. The SAM registry report is normally very short, so we can use the scroll feature to navigate it. The first artifact we will look at is the list of user accounts, their login counts, and their relative identifiers. Using the down arrow or mouse wheel, scroll until you get to the User Information registry key as highlighted below.

```
Username        : IEUser [1003]
SID             : S-1-5-21-776561741-308236825-1417001333-1003
Full Name       :
User Comment    :
Account Type    : Default Admin User
Account Created : Fri Oct 12 20:47:08 2012 Z
Name            :
Last Login Date : Wed Nov 12 19:35:13 2014 Z
Pwd Reset Date  : Thu Oct 31 21:26:00 2013 Z
Pwd Fail Date   : Thu Oct 31 21:30:48 2013 Z
Login Count     : 76
   --> Password does not expire
   --> Normal user account
```

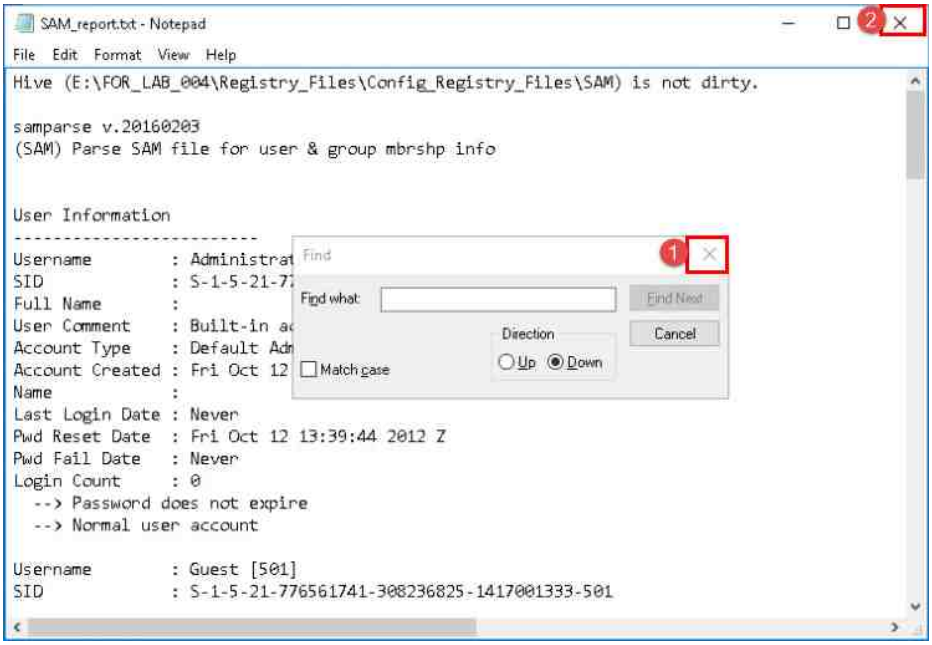

3. As you can see in the User Information registry key, each username is listed. The number beside the username highlighted below is known as a relative identifier (RID) and is unique for each account. Every time an account is created, it gets a new RID. If an account is deleted, then the associated RID will be discarded and will never be reused. It can therefore be used to determine if user accounts were deleted. RIDs are also unique in that the 500 and 501 RIDs are reserved for the built-in Administrator user account and the Guest account, respectively. Any user-created account will receive a RID of 1000 and up.

```
Username        : IEUser [1003]
SID             : S-1-5-21-776561741-308236825-1417001333-1003
Full Name       :
User Comment    :
Account Type    : Default Admin User
Account Created : Fri Oct 12 20:47:08 2012 Z
Name            :
Last Login Date : Wed Nov 12 19:35:13 2014 Z
Pwd Reset Date  : Thu Oct 31 21:26:00 2013 Z
Pwd Fail Date   : Thu Oct 31 21:30:48 2013 Z
Login Count     : 76
  --> Password does not expire
  --> Normal user account
```

4. We can also determine if the user's password was ever reset and when by looking at the Pwd Reset Date highlighted as item 1 below. There is also the Account Type that will tell whether the user is an administrator, guest, or regular user, highlighted as item 2. Finally, the Login Count and Pwd Fail Date outline the number of times the user logged in and the last time a login failed. These are highlighted as item 3 below.

```
Username        : IEUser [1003]
SID             : S-1-5-21-776561741-308236825-1417001333-1003
Full Name       :
User Comment    :
Account Type    : Default Admin User
Account Created : Fri Oct 12 20:47:08 2012 Z
Name            :
Last Login Date : Wed Nov 12 19:35:13 2014 Z
Pwd Reset Date  : Thu Oct 31 21:26:00 2013 Z
Pwd Fail Date   : Thu Oct 31 21:30:48 2013 Z
Login Count     : 76
  --> Password does not expire
  --> Normal user account
```

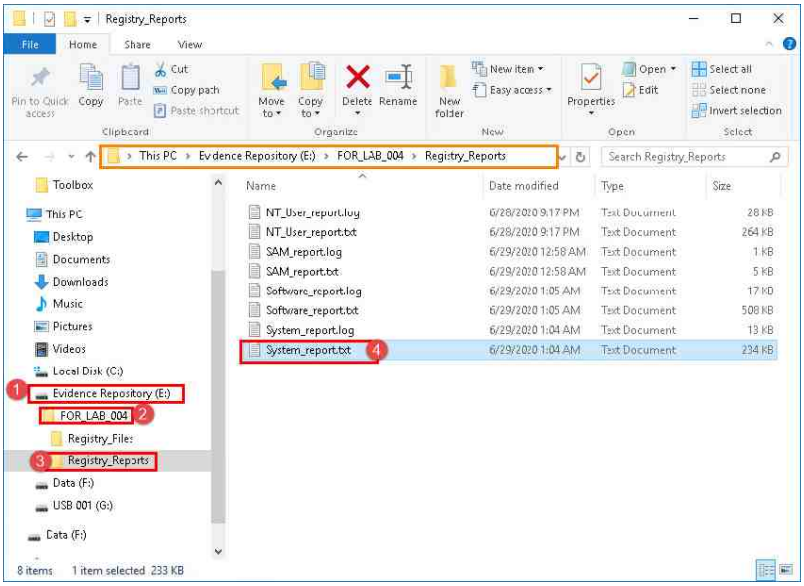

5. The SAM registry hive also provides details about user group memberships, but we will not cover that in this exercise. Let us move on to the last registry file we will cover in this lab.
6. Now that you are done, close the Find window and the Notepad program by clicking the X at the top-right corner as highlighted below.



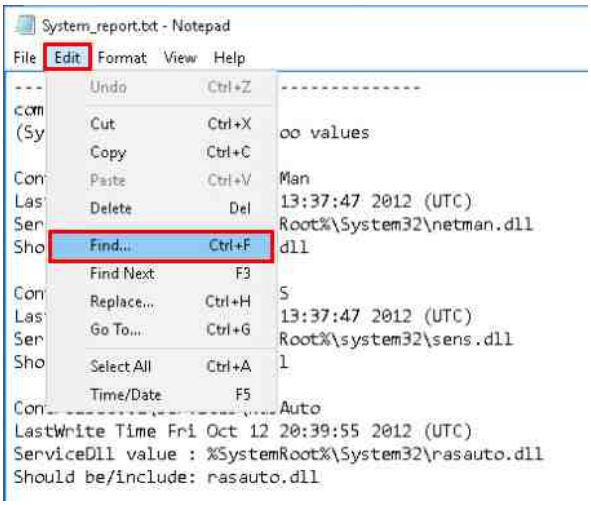
7 SYSTEM Registry File

Now that you see the valuable data that can be found in the registry, let us dig a little deeper by looking at another registry file. This time we will review the SYSTEM report that you created. The SYSTEM registry hive stores data about the physical devices connected to the computer and some operating system data.

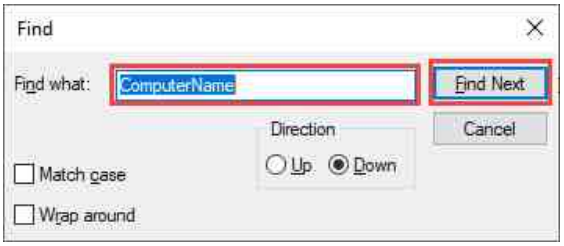
1. To access this report, browse to the folder we created called Registry_Reports located at Evidence Repository (E:) > FOR_LAB_004 > Registry_Reports as highlighted at items 1, 2, and 3. Once you get to the folder, double-click the file we named System_report.txt to open it in Notepad as indicated at item 4.



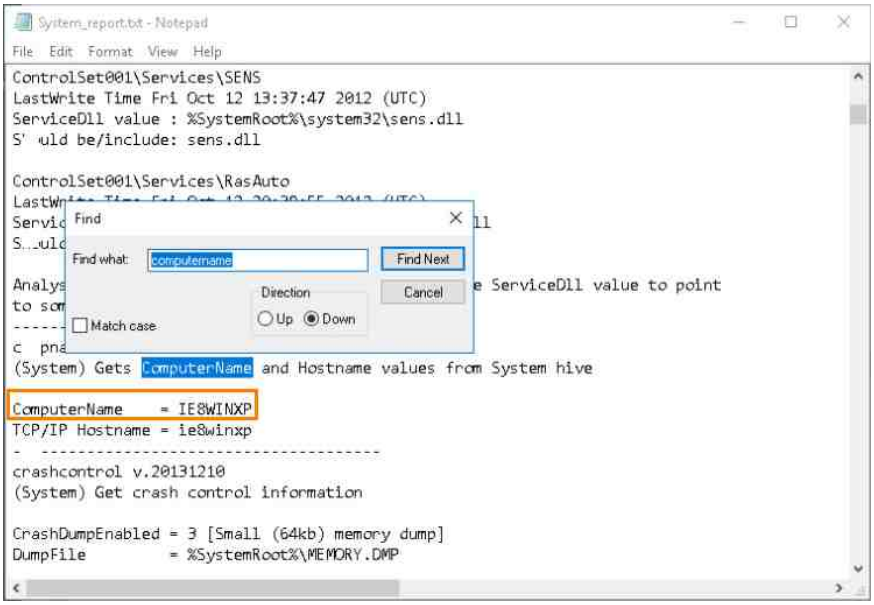
2. Since we are already used to the format of the document, let us use Find to locate the first artifact, the computername. This artifact will provide the hostname for the computer, which is useful in identifying a specific system. To search for the term, click Edit from the Menu bar and click the Find option from the dropdown menu as highlighted below.



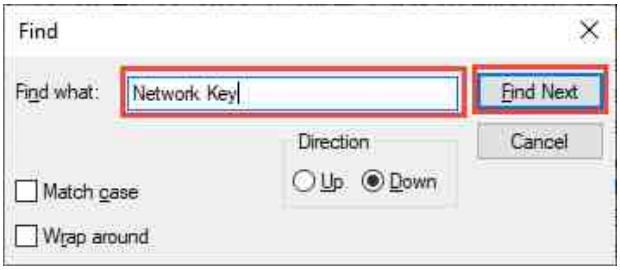
3. Once the Find window appears, type the term `Computername` and click Find Next as seen below.



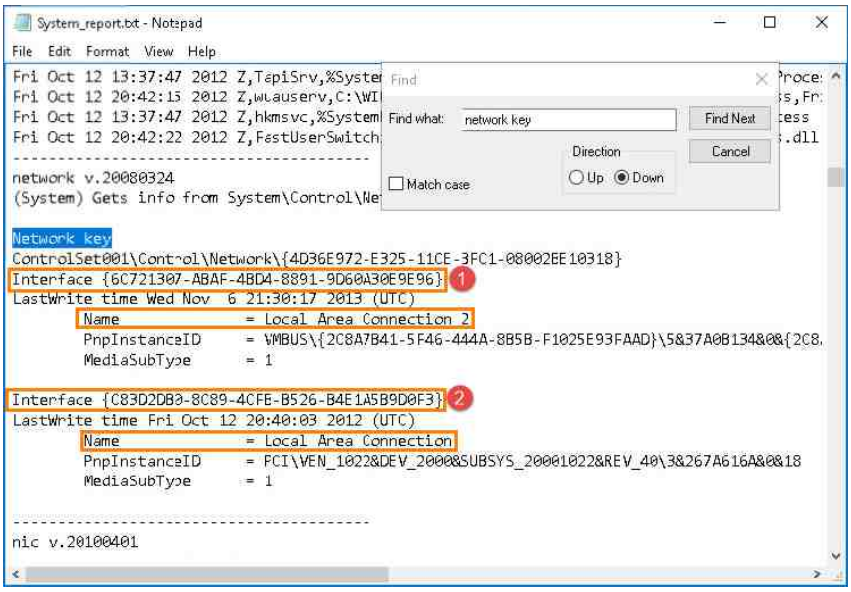
4. If successful, you will be taken to the ComputerName as highlighted below.



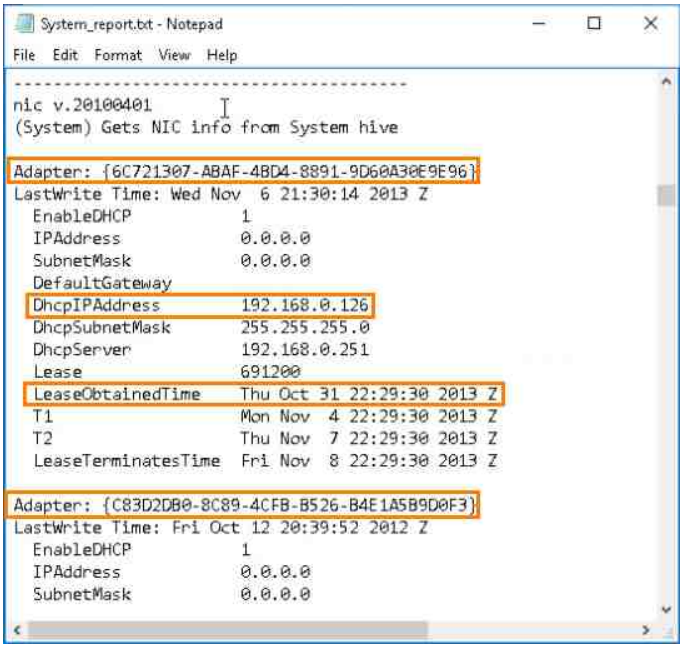
5. Now let us look at the network interfaces and IP address that was assigned to the computer. You should still have the Find window open, if not, reopen it. Once Find is open, type the term `Network Key` and click Find Next as seen below.



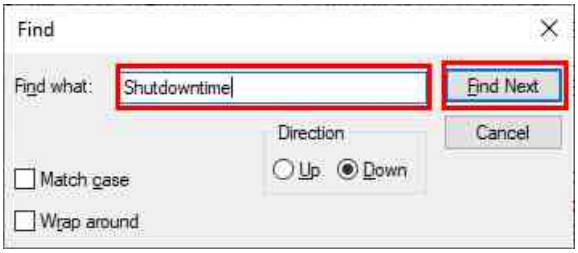
6. You will be taken to the Network Key that details the types of network interfaces available on the computer, highlighted as item 1 below. The value called Interface highlighted as item 2 is the Globally Unique Identifier (GUID) and is used to uniquely identify information on computer systems. In this case, the GUID is identifying each network adapter:



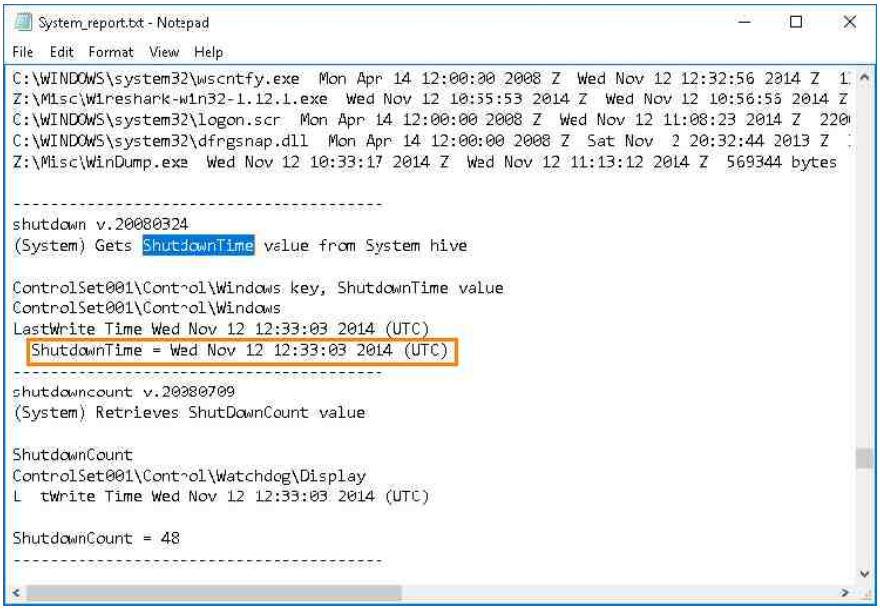
7. Let us scroll down by using the mouse wheel or clicking the down arrow until you get to the NIC configuration, as seen below. This registry key will detail the last IP address that was assigned to each of the network interfaces you saw above. You can match the name of the network above with the GUID below.



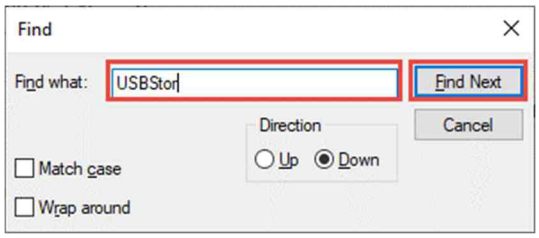
8. Let us look at another registry key; this one is the ShutdownTime registry value and, as the name suggests, provides the date and time of the last clean shutdown of the computer. This means the user intentionally shut down the computer, and it was not shut down due to a power outage or other similar accident. Let us use Find once again to locate this registry. If you do not have the Find window open, reopen it and type the term `Shutdowntime` then click Find Next as seen below.



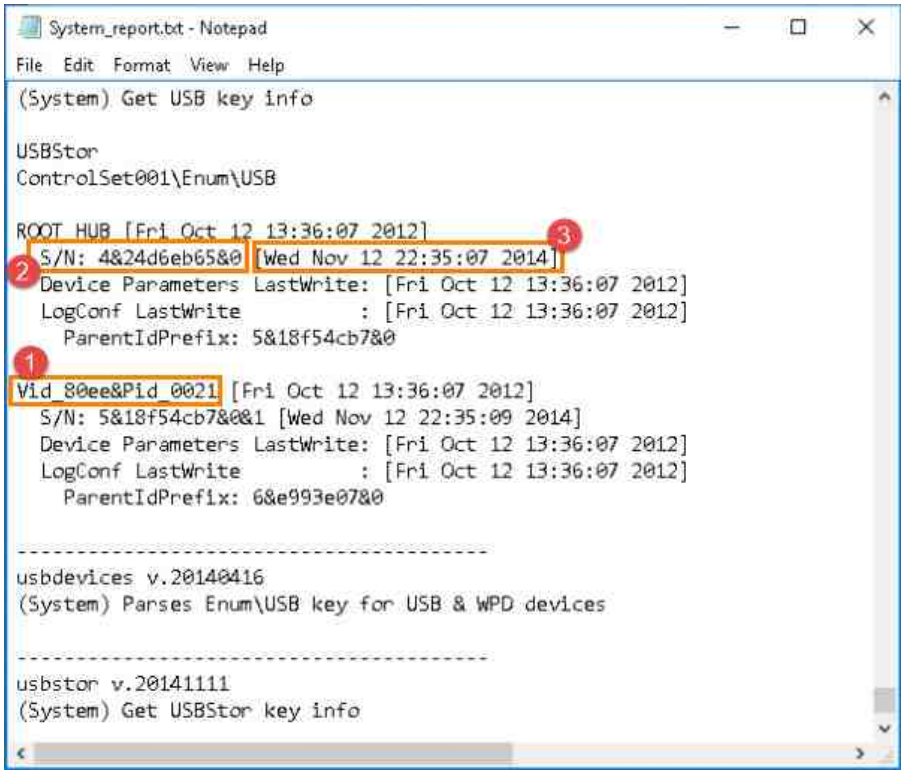
9. You will be taken to the following registry value. As seen below, this computer was last shut down on November 12, 2014 at 12:33:03 (UTC).



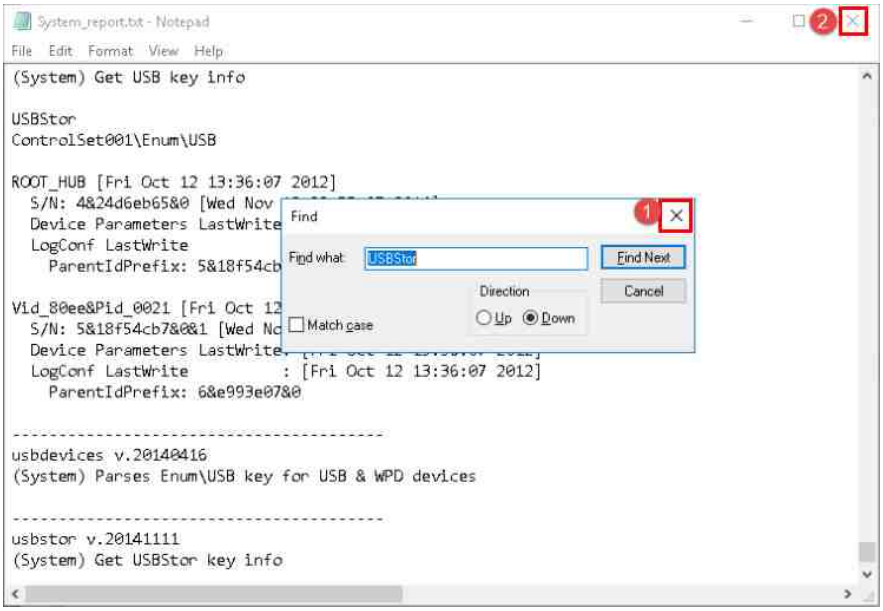
10. The last thing we will look at in the SYSTEM hive is the connected USB drives. The computer will keep a record of every USB device ever connected to it and provide the date and time it was last connected. Let us use Find once again to locate this registry. If you do not have the Find window open, reopen it and type the term `USBStor` then click Find Next as seen below.



11. You will be taken to the USBStor registry key, as seen below. Each entry provides the Vendor ID of the USB drive highlighted as item 1, the serial number highlighted as item 2, and the last time the drive was connected highlighted as item 3.



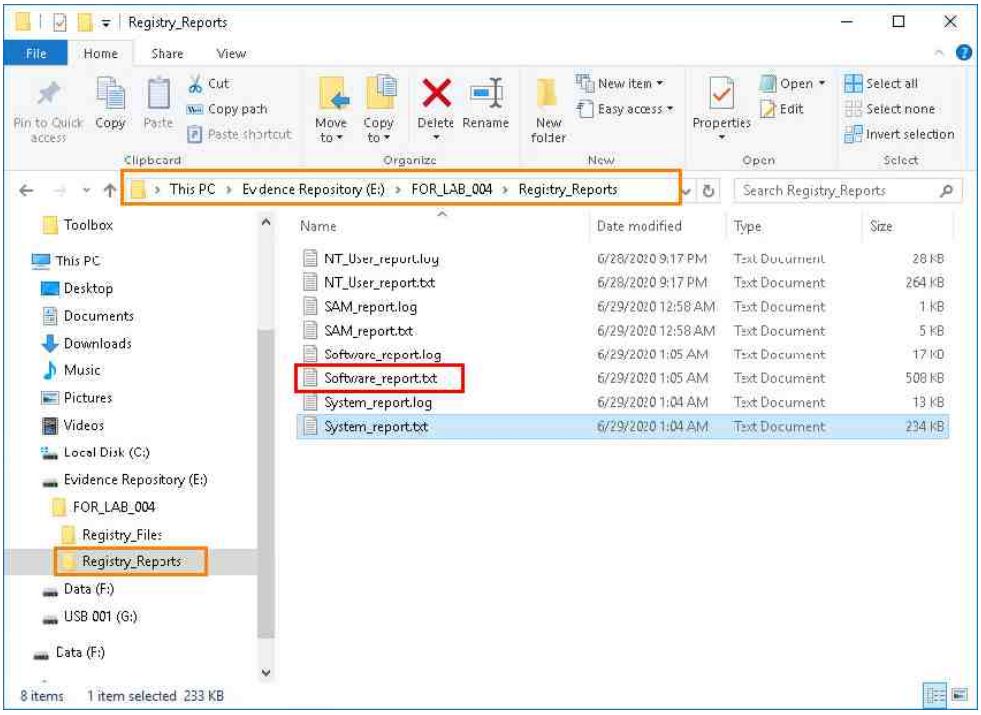
12. As with the other registry hives, the SYSTEM registry hive is a treasure trove of data. Explore it further to find interesting artifacts. When you are ready to move on, we will cover the SAM registry hive.
13. Now that you are done, close the Find window and the Notepad program by clicking the X at the top-right corner as highlighted below.



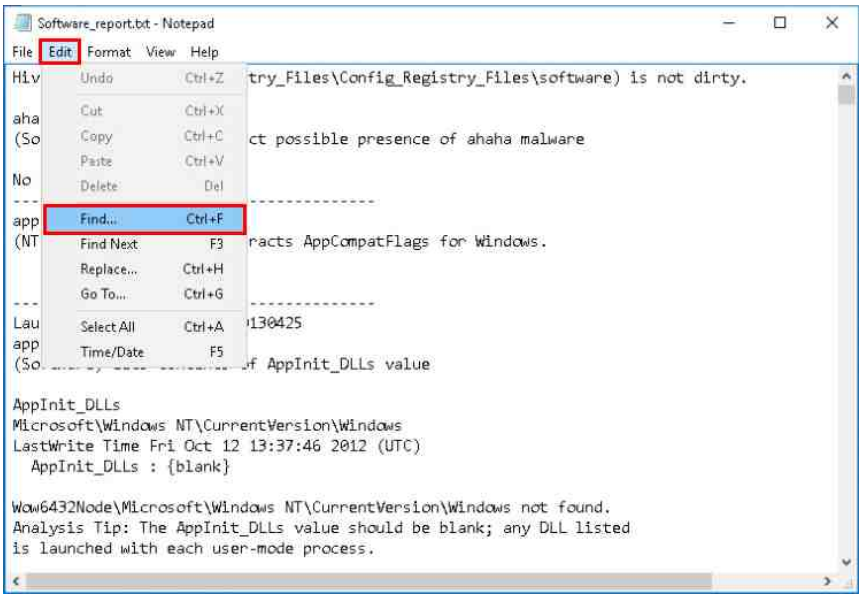
8 SOFTWARE Registry File

The SOFTWARE registry file stores data about the software installed on the computer and is usually the largest of the hives (This is not a rule, though). Let us begin by opening the SOFTWARE report you created.

1. To access this report, browse to the folder called Registry_Reports located at Evidence Repository (E:) > FOR_LAB_004 > Registry_Reports. Once you get to the folder, double-click the file we named Software_report.txt to open it in Notepad, as seen below.

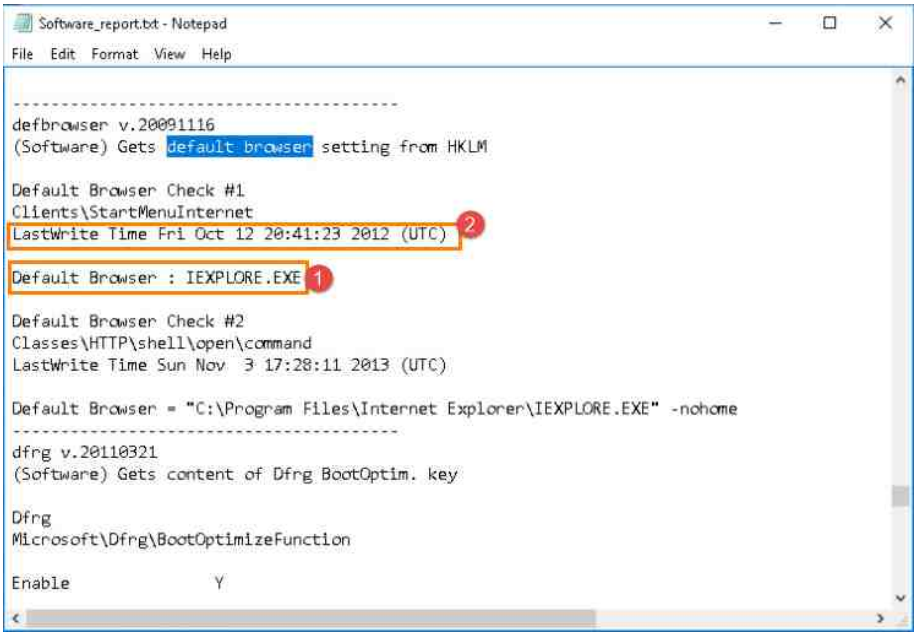


2. Let us use Find to locate the first artifact, the Default Browser Check. This artifact can tell you what the default browser is. This is very useful when you want to narrow your focus on browser artifacts and would like to determine the main browser. To search for the term, click Edit from the Menu bar and click the Find option from the dropdown menu as highlighted below.

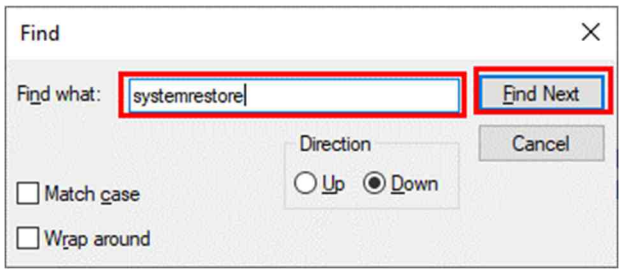


3. Once the Find window appears, type the term `Default Browser Check`, and click Find Next as seen below.

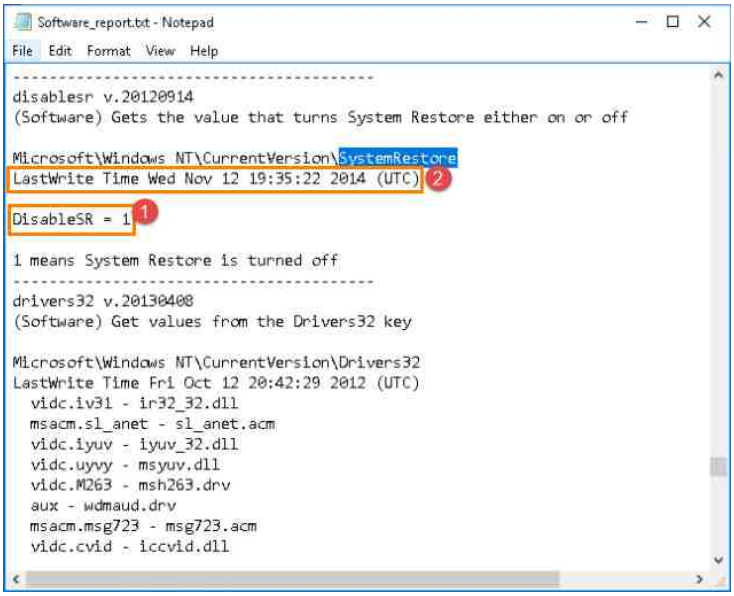
4. If successful, you will be taken to the Default Browser Check, as seen below. This registry file indicates that the default browser is IEXPLORE.EXE (Internet Explorer) as highlighted as item 1. The LastWrite Time value indicates the date the software was made the default highlighted as item 2:



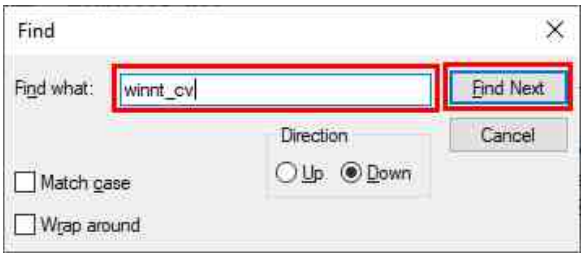
5. Next, let us look at the SystemRestore state. This registry key will tell you whether the System Restore feature is enabled. If System Restore is enabled, then that means backups of user files and activities are being made and stored on the computer in files called shadow files and is a goldmine for forensic examiners. There is no question why knowing whether it is enabled is important. Let us use Find to locate the SystemRestore key. You should have Find open, if not, reopen it and type the term `Systemrestore` and click Find Next as seen below.



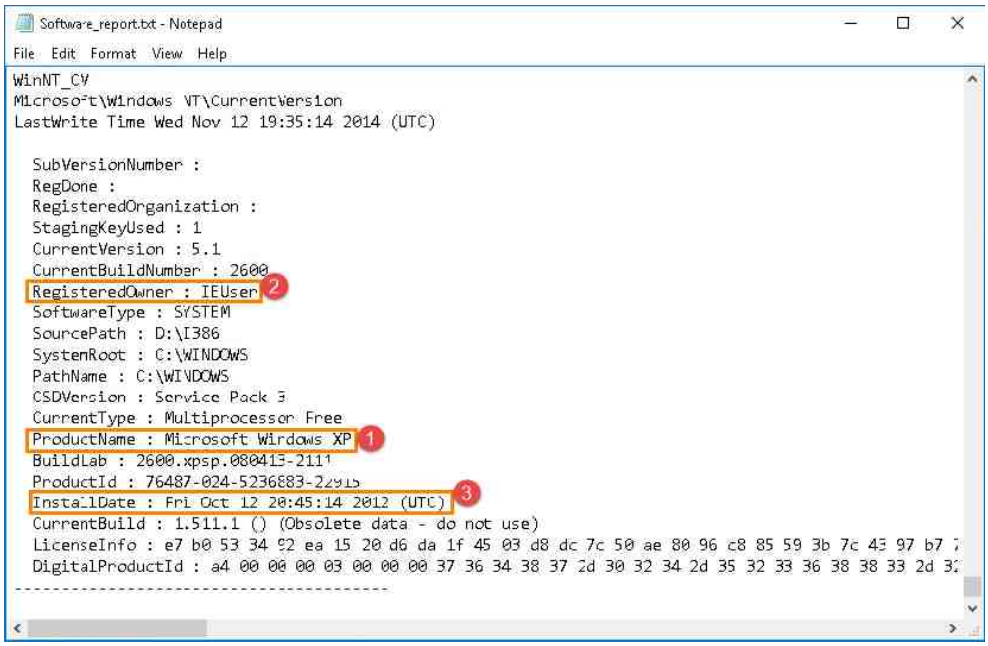
6. You will be taken to the System Restore key as seen below. As seen below, the DisableSR = 1 value, highlighted as item 1, indicates that System Restore was disabled. If it were 0 instead of 1, then it would mean that it was still enabled. The LastWrite Time, highlighted as item 2, indicates when it was disabled.



7. Let us look at one last registry key. This is the Operating System Information registry key, and it provides details about the operating system version, install date, the registered owner, and other useful information. Let us use Find to locate the Operating System Information. You should have Find open, if not, reopen it and type the term Winnt_cv and click Find Next as seen below.



8. You will be taken to the WinNT_CV registry key, where you will find the Operating System Information. This registry key can provide the Product Name and build number, which refers to the version of Microsoft Windows operating system installed as highlighted in item 1 below. The RegisteredOwner field will tell you the name entered when the computer was being installed and is highlighted as item 2 below. Finally, highlighted as item 3 is the InstallDate. This provides the date and time that the operating system was installed.



9. As you can see, the registry hives are extremely useful in learning about the system and tracking user activity. We will not cover any other registry files, but please feel free to open and review them all to become more familiar with their contents.
10. Now that you are done, close the Find window and the Notepad program by clicking the X at the top-right corner as highlighted below.