Introduction

Microsoft Windows is the most widely used operating system for both personal and business use. Originally released in 1985 as a graphical operating system shell for MS-DOS, Windows rapidly became the dominant personal computing operating system over the course of the 1980's and 1990's. Despite the resurgent popularity of Apple's Mac OS in the 2000s, today Windows still maintains more than 75% market share for desktop and laptop computers (among smartphones and similar devices, Android is similarly dominant). For this reason, the relevance of Windows in the field of digital forensics cannot be understated. As a forensics investigator, encountering cases involving Windows-based evidence is all but inevitable.

Within the realm of Windows-based digital forensics, there are multiple forms of analysis that an investigator can perform, most of which intersect with other types of digital forensics. For example, data recovery, network packet capture, and malware analysis are all types of forensic activities that a professional might conduct within a Windows environment. In some situations, the knowledge and skills required may transfer readily from one operating system to another, but in many cases, the mode of forensic analysis and background required will be unique to Windows. The most obvious example of the latter is conducting live analysis directly on a Windows system, which requires an investigator to use Windows-specific utilities and explore Windows-specific artifacts.

In this lab, you will use several Windows utilities to perform live analysis on a Windows Server 2019 system. You will explore one of the most evidence-rich areas of the Windows operating system - the Windows Registry. In Section 2, you will shift your attention to a Windows drive image and conduct forensic analysis using Paraben's E3.

Lab Overview

SECTION 1 of this lab has two parts, which should be completed in the order specified.

1. In the first part of the lab, you will use various tools and commands to gather information from a live Windows system.

2. In the second part of the lab, you will use regedit to explore the Windows Registry.

SECTION 2 of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods. You will use Paraben’s E3 to gather forensic evidence from a Windows drive image.

Finally, you will explore the virtual environment on your own in **SECTION 3** of this lab to answer a set of questions and challenges that allow you to use the skills you learned in the lab to conduct independent, unguided work - similar to what you will encounter in a real-world situation.

Learning Objectives

Upon completing this lab, you will be able to:

1. Use Windows utilities to gather forensic evidence on a live Windows system.
2. Use the Windows Registry to gather forensic evidence on a live Windows system.
3. Use Paraben's E3 to explore the NTFS file system.
4. Use Paraben's E3 to analyze the Windows Registry on a Windows 10 drive image.
5. Use Paraben's E3 to analyze Windows artifacts, including link files and browser history.

Topology

This lab contains the following virtual machines. Please refer to the network topology diagram below.

- vWorkstation (Windows: Server 2019)

Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- Task Manager
- Resource Monitor
- Fsutil
- Registry Editor (regedit)
- Paraben's E3

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

SECTION 1

1. Lab Report file, including screen captures of the following:

- Properties window for the process you selected
- Listening Ports list

- Information about the C: drive
- Information about the vWorkstation's usn journal
- File path for the *yourname*.txt file
- vWorkstation Windows installation timestamp in a human-friendly format
- Key values for the vWorkstation's default network interface
- Winlogon key values
- ShellBag key values
- RecentDocs key values

2. Any additional information as directed by the lab:

- None

SECTION 2

1. Lab Report file, including screen captures of the following:

- Sorted Files
- Contents of the 777.jpg file in the Document View
- 777.lnk file contents, including the path to the file in the system
- Installation files for suspicious apps in the Downloads category
- VPN application (Speedify) in the Uninstall folder
- Users list
- Contents of the Beverly Gates / Run folder
- At least one suspicious browsing record found in the History sub-node
- At least one suspicious keyword found in the Keywords sub-node

2. Any additional information as directed by the lab:

- None

SECTION 3

1. Lab Report file, including screen captures of the following:

- Contents of the suspicious file
- At least one registry key with information associated with Tor and Firefox

2. Any additional information as directed by the lab:

- None

Section 1: Hands-On Demonstration

Note: In this section of the lab, you will follow a step-by-step walk-through of the objectives for this lab to produce the expected deliverables.

1. **Review** the **Tutorial**.

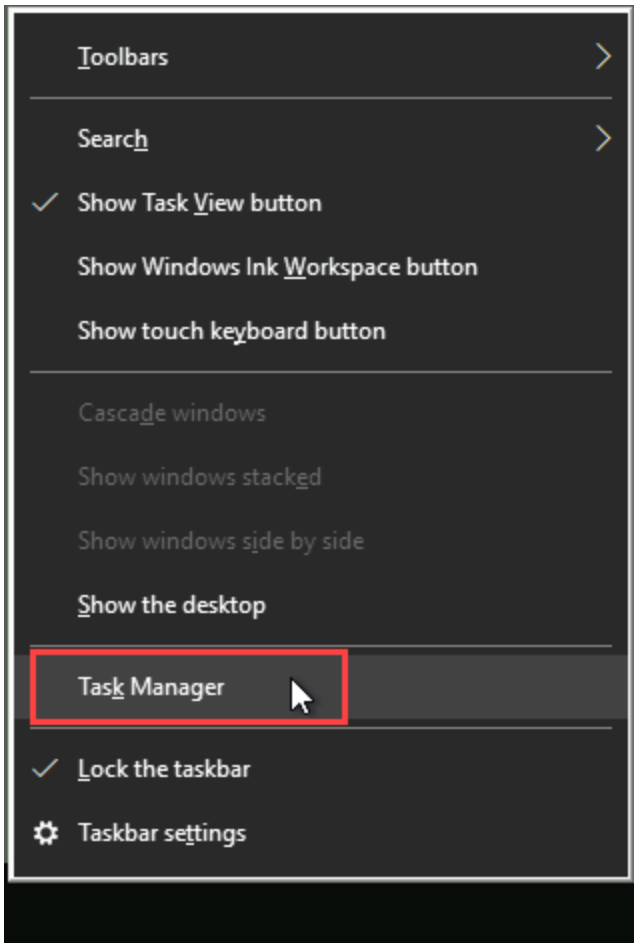
   Frequently performed tasks, such as making screen captures and downloading your Lab Report, are explained in the Cloud Lab Tutorial. The Cloud Lab Tutorial is available from the User menu in the upper-right corner of the Student Dashboard. You should review these tasks before starting the lab.

2. **Proceed** with **Part 1**.

Part 1: Gather Basic System Information

Note: In this part of the lab, you will use a variety of different tools to gather forensically relevant information about a Windows system.

1. From the vWorkstation desktop, **right-click** anywhere on the **taskbar**, then **select Task Manager** from the context menu to open the Task Manager.



Open the Task Manager

Note: From the Task Manager, you can review all the applications, processes, and services that are active at the moment. You can even attempt to shut down specific processes, if necessary.

Among the many processes displayed in the Task Manager, you should be able to identify the following core Windows processes:

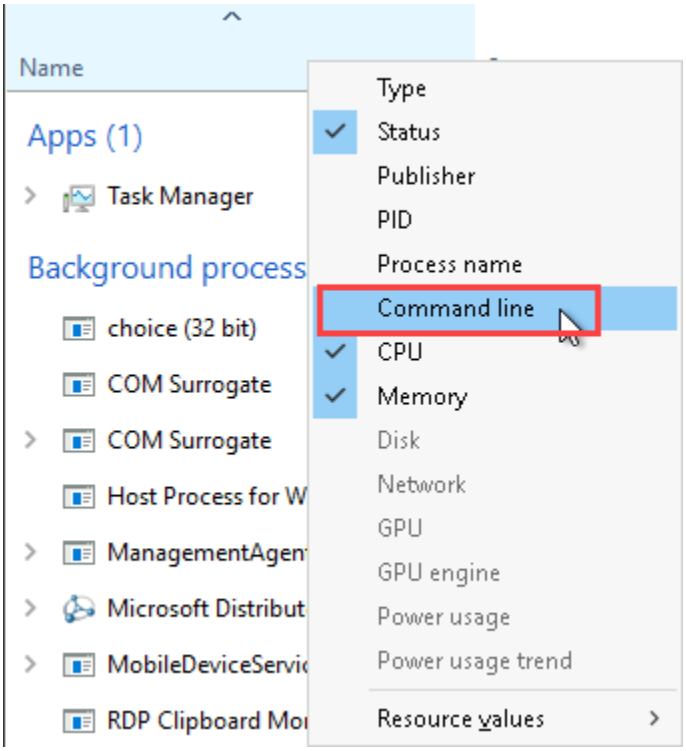
- **System (ntoskrnl.exe):** The core of the Windows operating system.
- **Windows Session Manager (smss.exe):** A program that manages services.
- **Windows Logon Application (winlogon.exe):** The program that logs you on.

- **Local Security Authority Process (lsass.exe):** The program that handles security and logon policies.

- **Windows Explorer (explorer.exe):** The interface the user interacts with, such as the desktop, Windows Explorer, and so on.

- **Client Server Runtime Process (crss.exe):** The program that handles tasks like creating threads and console windows.

2. In the Task Manager, **right-click** the **Name column header**, then **select Command line** from the context menu to add the Command line column.

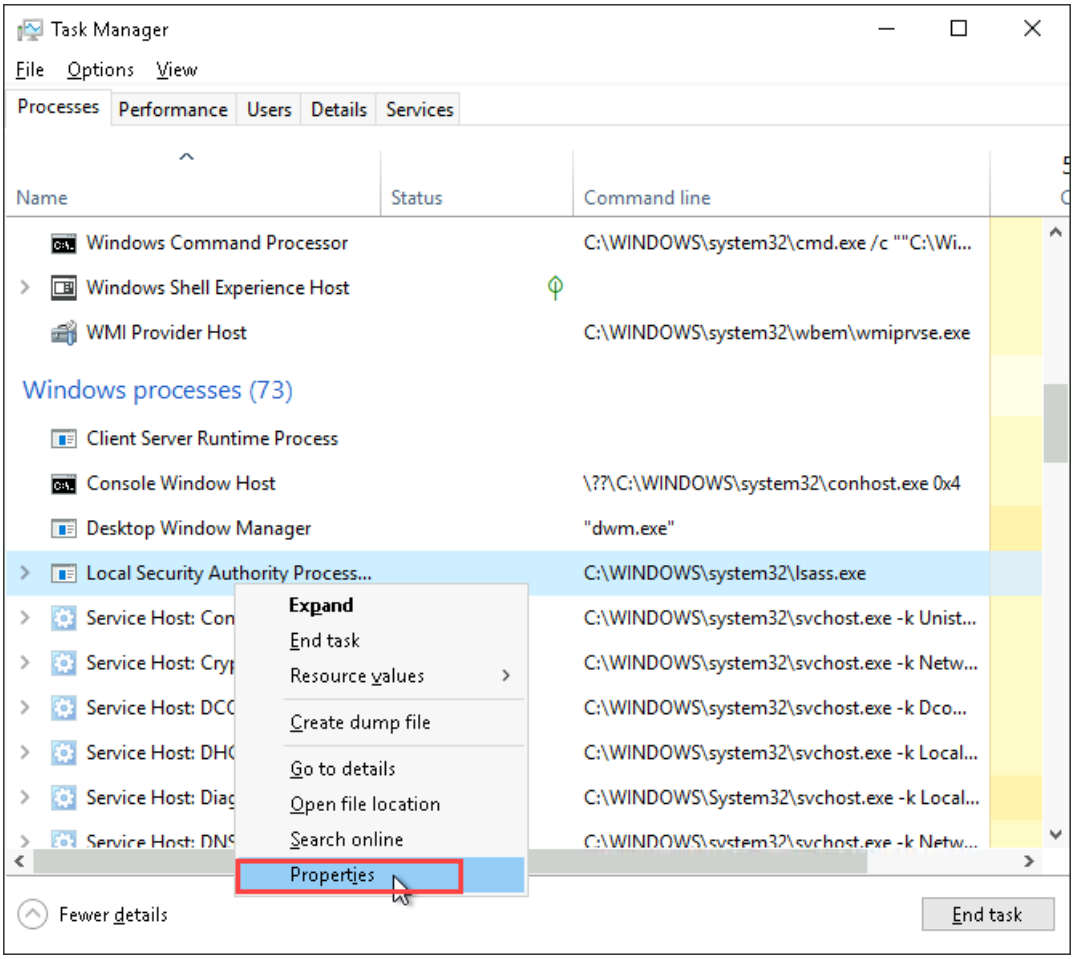


Add the Command line column

Note: By adding the Command line column, you can observe the file path for each process's executable file, as well as any command line options that were used to launch the program. While even casual Windows users often know how to use the Task Manager to shut down applications that

are slowing down their computers, for forensic investigators it can be a valuable source of detailed information when attempting to analyze and isolate malware that has been running since the start of the system.

3. In the Task Manager, **identify** one of the **core Windows processes** listed above, then **right-click** the **process** and **select Properties** from the context menu to display additional information about the process in the Properties window.

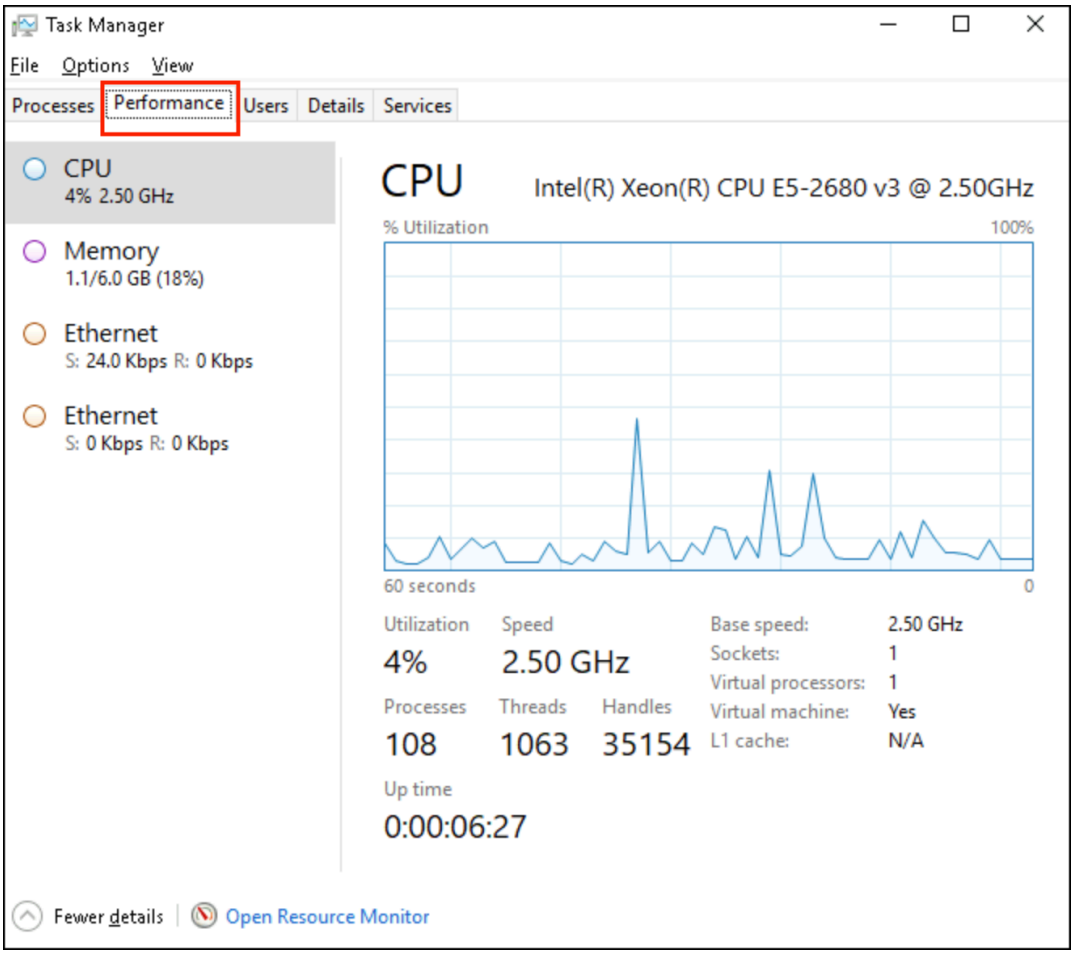


Open the Properties window

4. **Make a screen capture** showing the **Properties window for the process you selected**.

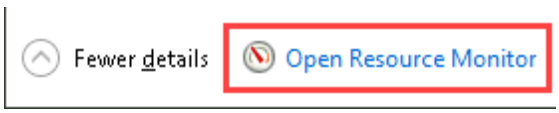
5. **Close** the **Properties window**.

6. In the Task Manager, **click** the **Performance tab** to display information about resource usage.



Performance tab

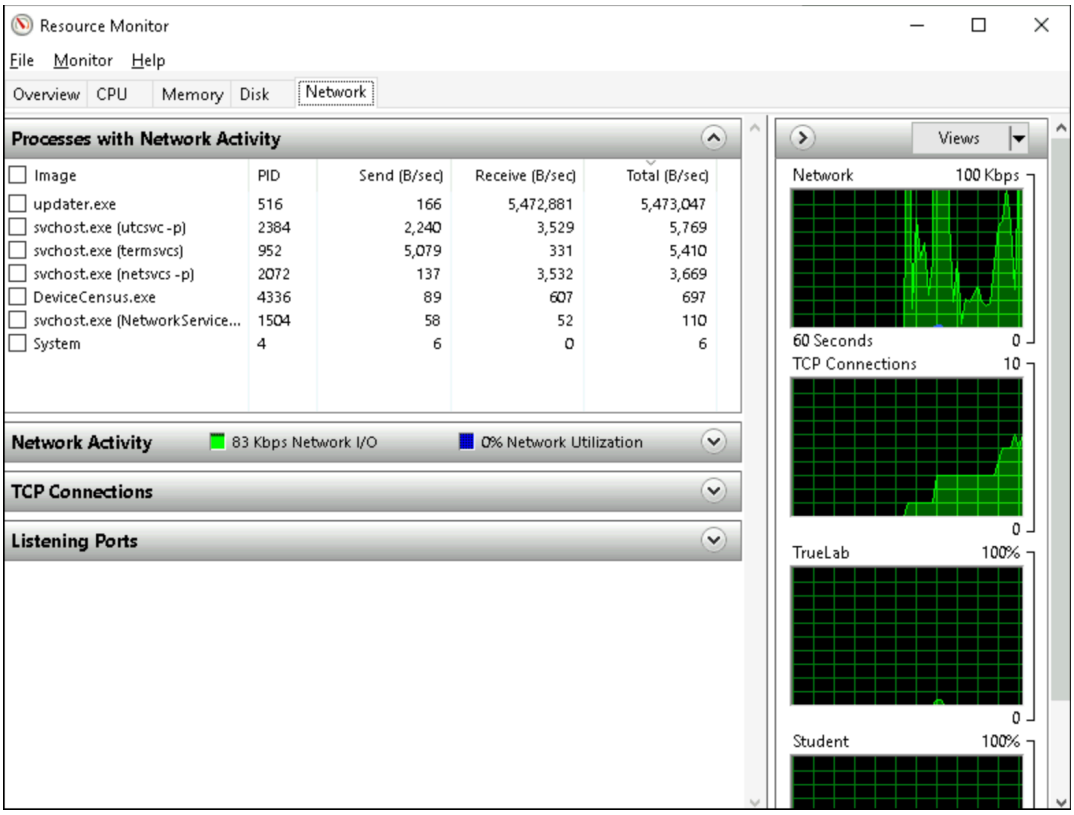
7. From the bottom of the Task Manager, **click** the **Open Resource Monitor link** to launch the Resource Monitor.



Open Resource Monitor

Note: The Resource Monitor is a dedicated utility for monitoring system resource usage in real time, including CPU, memory usage, disk utilization, and network use. While the Resource Monitor contains many of the same metrics as the Performance tab of the Task Manager, it allows knowledgeable users to drill deeper into the underlying data.

8. In the Resource Monitor, **click** the **Network tab** to display a list of processes that are currently generating network activity.

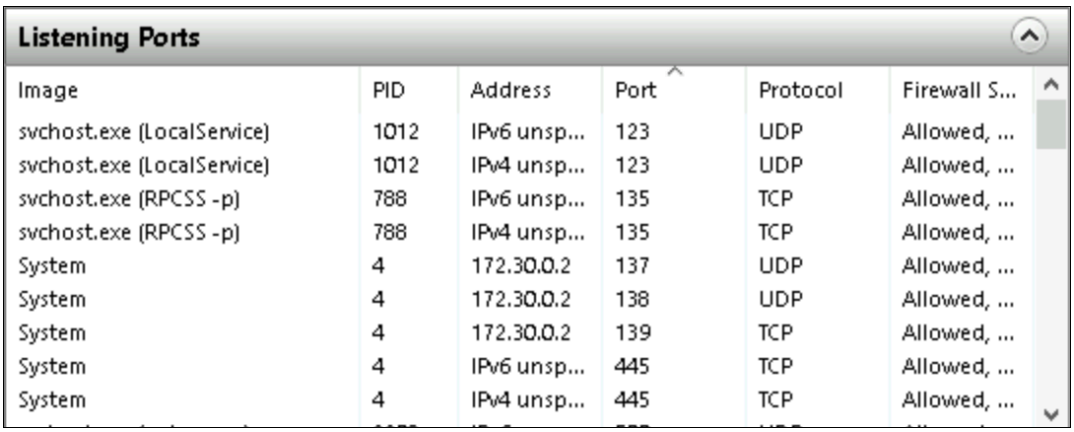


Network tab

Note: The Network tab displays network activity, TCP connections, and listening ports for any running process. As a forensic investigator, this information can be essential to identifying spyware, botnets,

and other forms of malware that require network connectivity.

9. On the Network tab, **expand** the **Listening Ports header** to display a list of ports that are actively listening and the processes that are using them.



Listening Ports

10. **Make a screen capture** showing the **Listening Ports list**.

11. **Close** the **Resource Monitor** and **Task Manager windows**.

Note: In the next steps, you will use the fsutil utility to gather information about the Windows file system. Fsutil can perform a variety of tasks related to FAT and NTFS file systems. It can be used to obtain drive lists for a computer, obtain the drive type, display some general volume information, and determine the amount of free space on a drive.

12. On the vWorkstation taskbar, **click** the **Command Prompt icon** to open a new Command Prompt window.

Command Prompt icon

13. At the command prompt, **type** `fsutil fsinfo ntfsinfo C:` and **press Enter** to display information about the C: drive.

```
C:\Users\Administrator>fsutil fsinfo ntfsinfo C:
NTFS Volume Serial Number :        0xe8f46c07f46bd5fa
NTFS Version   :                   3.1
LFS Version    :                   2.0
Number Sectors :                   0x0000000011569ff8
Total Clusters :                   0x00000000022ad3ff
Free Clusters  :                   0x00000000002d59ab
Total Reserved :                   0x000000000000126e
Bytes Per Sector  :                512
Bytes Per Physical Sector :        512
Bytes Per Cluster :                4096
Bytes Per FileRecord Segment    :  1024
Clusters Per FileRecord Segment :  0
Mft Valid Data Length :            0x0000000020740000
Mft Start Lcn  :                   0x00000000000c0000
Mft2 Start Lcn :                   0x0000000000000002
Mft Zone Start :                   0x00000000004c7ac0
Mft Zone End   :                   0x00000000004cf320
Max Device Trim Extent Count :     0
Max Device Trim Byte Count :       0x0
Max Volume Trim Extent Count :     62
Max Volume Trim Byte Count :       0x40000000
Resource Manager Identifier :      83BA1061-A635-11E6-BB74-D7C204107C12

C:\Users\Administrator>
```

Display information about the C: drive

Note: The output of this command provides information about the C drive, including the NTFS volume serial number, version, number of total clusters, number of free clusters, total number of sectors, and much more. In the context of a forensic investigation, this information can be used to determine if there is hidden data in a boot file or boot record of the drive. It can also be used to determine if there are faked bad clusters, which are areas of the drive that the file system ignores due to damage, but are in fact viable and used to hide data. To calculate the total number of clusters that are currently

used by the system, you can use the following formula: Total Clusters minus Free Clusters minus Total Reserved (however, you must first convert the hexadecimal values to conventional decimal notation.

14. **Make a screen capture** showing the **information about the C: drive**.

15. At the command prompt, **type** `fsutil usn queryjournal C:` and **press Enter** to display information related to the update sequence number changes journal.

Display information related to the update sequence number changes journal

Note: The update sequence number (usn) change journal provides visibility into filesystem activity going back several days or even weeks. As files, directories, and other NTFS objects are added, deleted, and modified, NTFS enters records into the usn change journal, one for each volume on the computer. Each record indicates the type of change that occurred, such as file creation or deletion, and the filename that was changed.

16. **Make a screen capture** showing the **information about the vWorkstation's usn journal**.

Note: Now that you have gathered some general information about the usn journal, you will directly inspect the contents.

17. At the command prompt, **type** `fsutil usn readjournal C:` and **press Enter** to display all records in the usn journal.

    After allowing the command to run for about 10 seconds, **press Ctrl + c** to terminate it.

Display all records in the usn journal

Note: This information can be useful for several reasons. First, when a program is run, typically you will be able to see the modified prefetch files, which will give you a timestamp for execution. Second, the usn journal can provide evidence of deleted files. Third, you can see file modifications and the creation of specific particular file extensions, such as executables, which in some contexts can be indicative of a system compromise. Many compromises occur after a piece of file-based malware is initially run, such as from a macro or PDF. The usn journal can provide a timeline of initial infection.

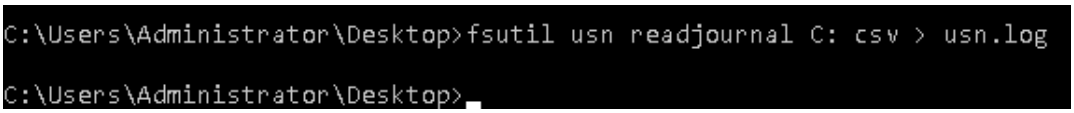
In the next steps, you will generate a new record for the usn journal and export the contents of the usn journal to the vWorkstation desktop. Using the exported usn journal, you will identify the file ID for your record, then use the fsutil utility to look up the location of the associated file.

18. On the vWorkstation desktop, **right-click any empty space** and **select New > Text Document** to create an empty text file on the desktop.

19. In the filename field, **type *`yourname`***, where *yourname* is your own name, and **press Enter** to name the new file.

20. At the command prompt, **type `cd Desktop`** and **press Enter** to change the current directory to the desktop.

21. At the command prompt, **type `fsutil usn readjournal C: csv > usn.log`** and **press Enter** to save the contents of the usn journal to the vWorkstation desktop as a .csv file.



Export the usn journal

22. From the vWorkstation desktop, **double-click** the **usn.log file** to open it in Notepad.

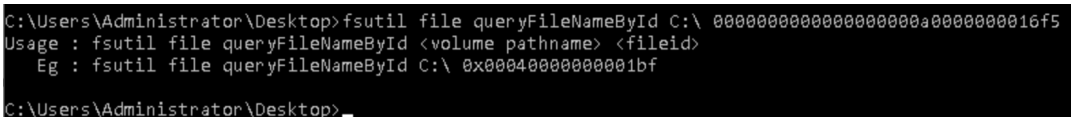
23. In the Notepad window, **scroll down** to the bottom of the file and **locate** the record referencing the ***yourname*.txt file**.

24. In the Notepad window, **highlight** the **File ID value** for the *yourname*.txt file, then **press Ctrl+c** to copy it to the clipboard.

    The File ID should be the long hexadecimal number directly to the right of the word "Archive."

File ID

25. At the command prompt, **type** `fsutil file queryFileNameById C:\ 0x`***`File ID`***, where *File ID* is the value you copied from the previous command output (**press Ctrl + v** to paste), then **press Enter** to retrieve the file path associated with the file ID.



Retrieve the file path

26. **Make a screen capture** showing the **file path for the *yourname*.txt file**.

27. **Close** any **open windows**.

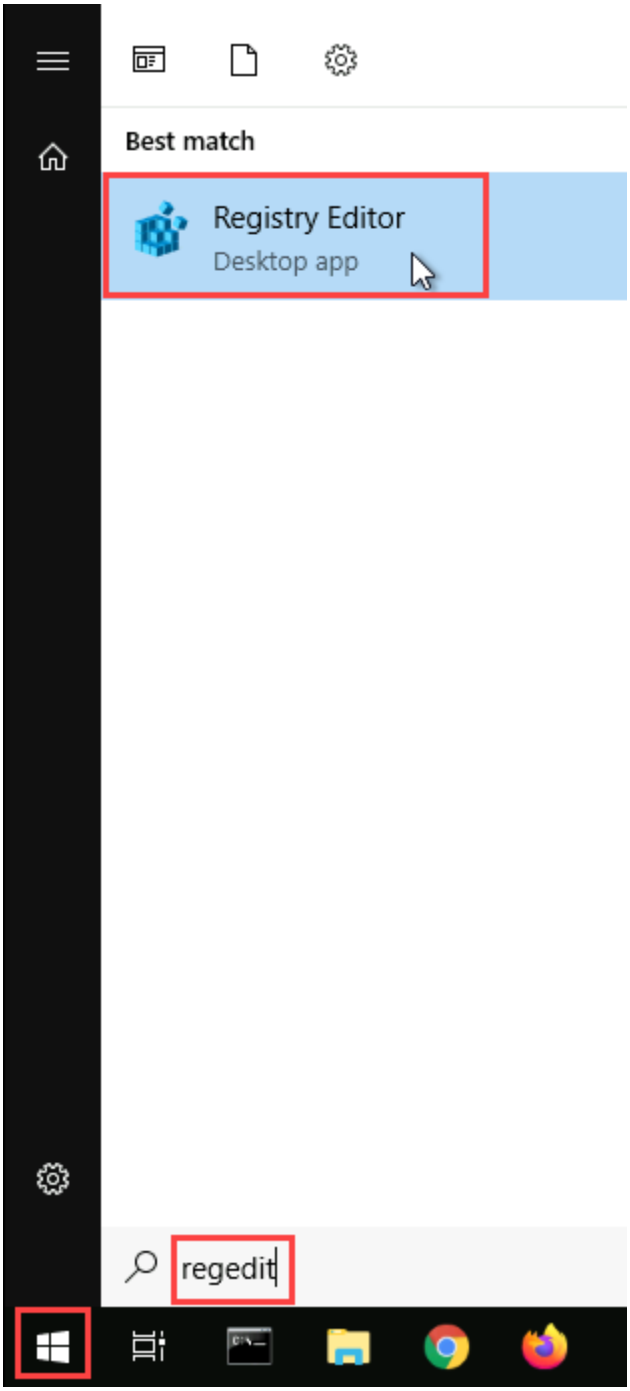
Part 2: Explore the Registry

Note: The Windows Registry is one of the key components of the Windows operating system. This hierarchical database contains Windows settings, application settings, device driver info, and user passwords. When an application is installed in a Windows environment, some part of the software is stored in the Registry. For this reason, registry analysis is often a critical component of conducting forensics investigations on Windows systems.

In the next steps, you will open the Registry Editor and get acquainted with the organizational

structure.

1. From the vWorkstation taskbar, **click** the **Start icon**, then **type** `regedit` and **press Enter** to search for and launch the Registry Editor.



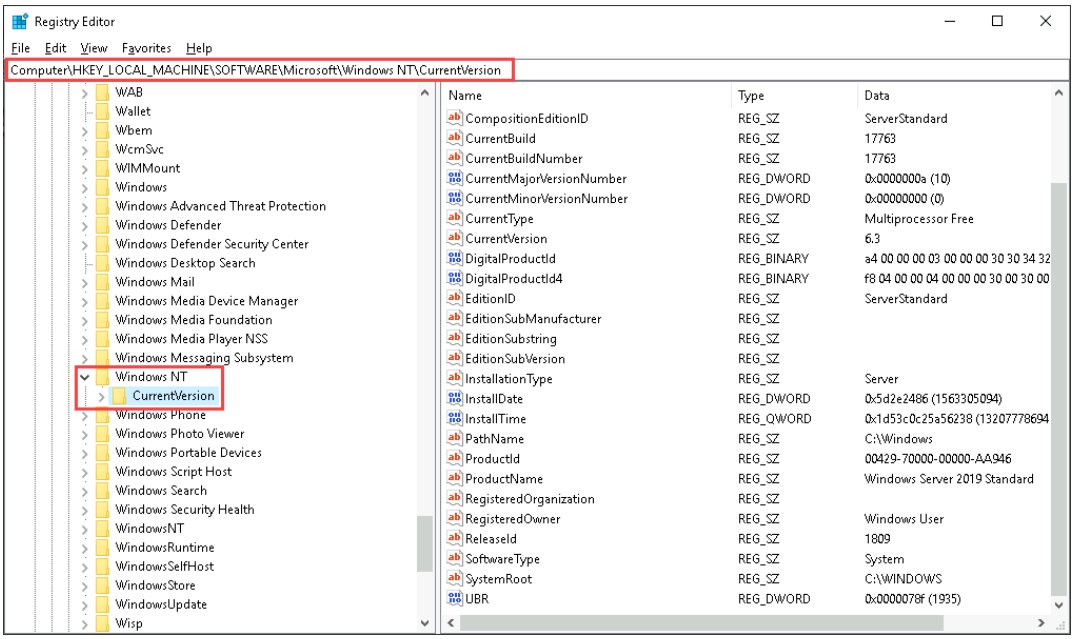
Open the Registry Editor

Note: As a database, the Windows Registry is composed of two basic components: Keys and Values. You can essentially think of Keys as folders and Values as files, where Values are stored in Keys. Like folders, Keys can contain other Keys, which are typically referred to as Sub-keys. Keys typically contain multiple Values, each of which has a Name, Type, and Data attribute.

At the top-most level of the hierarchy, Registry Keys are organized into the following Hives.

- **HKEY_CLASSES_ROOT** (HKCR) contains file extension associations, programmatic identifiers (ProgIDs), Class IDs (CLSIDs), and Interface IDs (IIDs).
- **HKEY_CURRENT_USER** (HKCU) stores information about the currently logged-on user, including desktop settings, user folders, and so forth.
- **HKEY_LOCAL_MACHINE** (HKLM) contains configurations for installed applications and Windows itself.
- **HKEY_USERS** (HKU) contains user-specific configuration information for all active users on the machine.
- **HKEY_CURRENT_CONFIG** (HCU) contains the current system configuration.

2. In the Registry Editor, **navigate** to the following key: **HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion**.



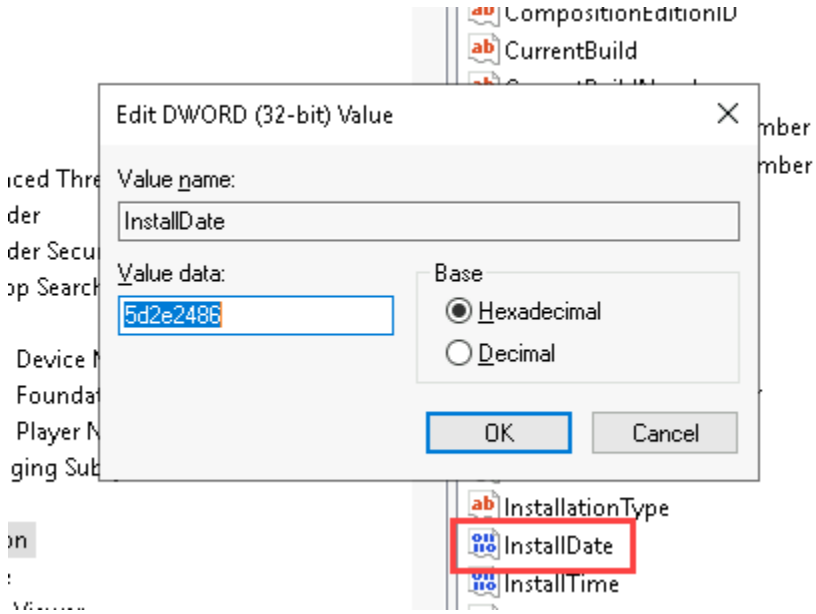
CurrentVersion key

Note: The HKEY_LOCAL_MACHINE Registry hive contains the majority of the configuration information for the software installed on the system, as well as for the Windows operating system itself. In addition to software configuration data, the HKEY_LOCAL_MACHINE hive also contains valuable information about currently detected hardware and device drivers.

In this case, the current key stores multiple values related to the version of Windows that is currently installed on the vWorkstation. Within this key, you will find values related to current major version of Windows, the current minor version of Windows, the current build, the installation date, the registered organization, and much, much more.

While the value of a specific piece of information is largely determined by the context of the investigation at hand, this Key contains multiple data points that could be immensely useful to an investigator who has obtained a drive image as evidence, but does not know the exact version of Windows that was installed on it. If the drive image was taken from a recently compromised system, this information could help corroborate evidence of an exploit that might be unique to that specific version of Windows.

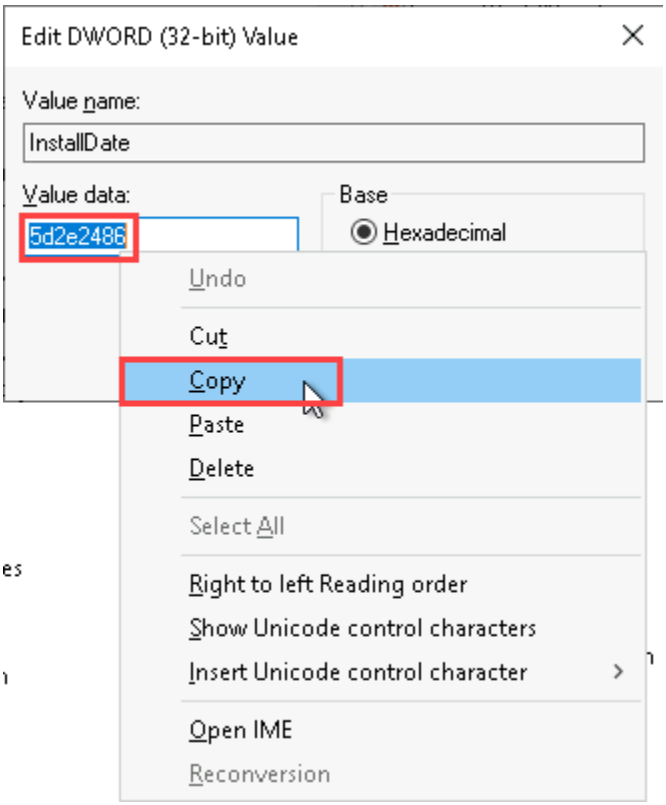
3. In the right pane, **double-click** the **InstallDate value** to open the Edit DWORD (32-bit) Value dialog box.



InstallDate value and dialog box

Note: Value data in the Windows Registry is commonly stored in hexadecimal notation. In the next steps, you will use a hexadecimal converter to convert the install date to a more human-friendly notation.

4. In the dialog box, **right-click** the **Value data field**, then **select Copy** from the context menu to copy the hex value to the clipboard.



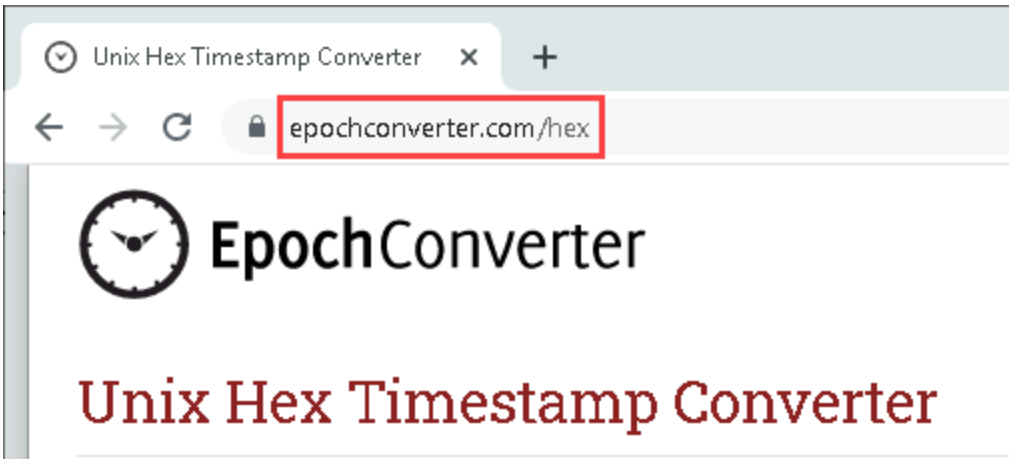
Copy the hex value

5. **Click OK** to close the dialog box.

6. From the vWorkstation taskbar, **click** the **Chrome icon** to open a new Chrome browser window.

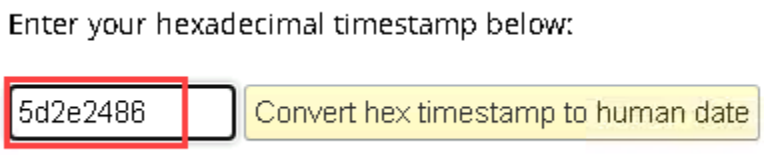
Chrome icon

7. In the Chrome navigation bar, **type** `epochconverter.com/hex` and **press Enter** to navigate to the hexadecimal converter.



Hexadecimal converter website

8. In the hexadecimal converter, **delete** the **existing hexadecimal timestamp value**, then **right-click** the **empty hex field** and **select Paste** from the context menu to paste the hex value into the converter.



Paste the hex value

9. **Click** the ***Convert hex timestamp to human date*** **button** to perform the conversion.

10. **Make a screen capture** showing the **vWorkstation Windows installation timestamp in a human-friendly format**.

11. **Close** the **Chrome browser window**.

12. In the Registry Editor, **navigate** to the following key: **HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ Tcpip \ Parameters \ Interfaces \ {39007c8a-d2a1-4c34-bb9d-e9c1bce829b3}**.

Note: This key contains information about the default network interface for the vWorkstation, including the IP address and default gateway. The other sub-keys within the Interfaces key are other network interfaces for the vWorkstation. If you take the time to examine the other interface keys, you will find that two contain very little information. This typically means the network interface is disconnected. The fourth interface key contains as much information as the first key. This is the second active network interface on the vWorkstation, where the first is used to connect within the self-contained lab environment, while the second is used to facilitate your remote connection from your local machine.

13. **Make a screen capture** showing the **key values for the vWorkstation's default network interface**.

14. **Navigate** to the following key: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon**.

Note: Winlogon is the component of Microsoft Windows operating systems that is responsible for handling the secure attention sequence, loading the user profile on logon, and optionally locking the computer when a screensaver is running. The actual obtainment and verification of user credentials is left to other components. Winlogon is a common target for several threats that could modify its function and memory usage. Signs of increased memory usage for this process might indicate that it has been compromised.

15. **Make a screen capture** showing the **Winlogon key values**.

Note: At this point, you have examined registry keys related to the system version, network interfaces and the windows login function. In the final steps, you will review registry keys related to the current user account.

16. **Navigate** to the following key: **HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ Shell \ Bags**.

17. Within the Shell\Bags key, **expand** any of the **sub-keys** until key values appear in the right pane.

Note: The ShellBags keys provide records that a specific folder was accessed by the current user. While reading the contents of these key values, including the folder names and file paths, requires a specialized ShellBags parser such as ShellBags Explorer, the information they contain can be instrumental to providing non-repudiation of claims that a defendant was not aware of a particular folder on their computer.

18. **Make a screen capture** showing the **ShellBags key values**.

19. **Navigate** to the following key: **HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Explorer \ RecentDocs**.

Note: As the name implies, this registry key is related to the Recent Files function in the File Explorer. Within this key, you can see hexadecimal records for the last 10 files that the current user accessed through the File Explorer.

20. **Make a screen capture** showing the **RecentDocs key values**.

21. **Close** any **open windows**.

Note: This concludes Section 1 of the lab.

Section 2: Applied Learning

Note: SECTION 2 of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods. You will use Paraben's E3 to gather forensic evidence from a Windows drive image.

Part 1: Create and Sort a New Case File

Note: Forensic investigations of Windows systems also commonly use evidence extracted from a live system, such as drive images. For this purpose, investigators typically use specialized tools to acquire, explore, and catalog evidence in accordance with forensically sound principles and procedures. In this part of the lab, you will use Paraben's E3 to create a new case file and import a Windows drive image. You will then use E3's Content Analysis feature to analyze and sort the files on the drive image into different categories that will streamline your search for evidence.

The setting of this lab is an ongoing investigation into the activities of Beverly Gates, the HR Manager at Intricate Solutions, Inc. Senior leadership has reason to believe that Beverly is involved in a sophisticated drug trafficking operation with ties to the Russian mafia and has recently brought contacted the authorities to investigate the matter further. As a forensic analyst assigned to the case, you have been given a drive image taken from Beverly's work laptop and tasked with reviewing its contents for forensic evidence of suspicious activity.

In the next steps, you will add the drive image to E3.

1. From the vWorkstation desktop, **launch** the **Electronic Evidence Examiner (E3) application**.

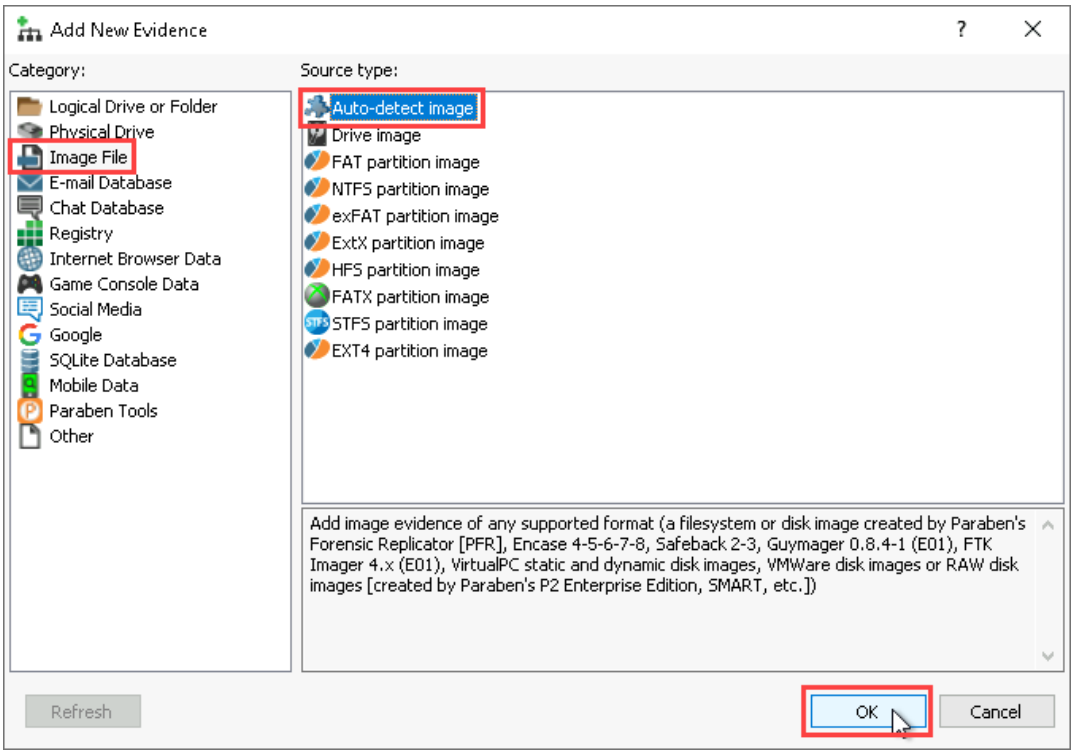
E3 icon

Note: E3 may take several minutes to load. The E3 welcome screen opens with shortcuts to the most common activities that forensic investigators will perform within the tool.

2. On the Welcome screen, **click** the **Add Evidence button** to open the New Case dialog box.

3. In the New Case dialog box, **type** ***yourname*** **`Windows Case File`** in the Case name field, replacing *yourname* with your own name, then **click Continue** to create your new case file and open the Add New Evidence dialog box.

4. In the Add New Evidence dialog box, **click** the **Image File category**, then **select** the **Auto-detect image Source type** and **click OK** to continue.



Add New Evidence

5. In the Open dialog box, **navigate** to **This PC > Local Disk (C:) > Beverly Gates Evidence** and **double-click** the **BG_evidence.001 file** to select the first chunk of the digital drive image for this lab.

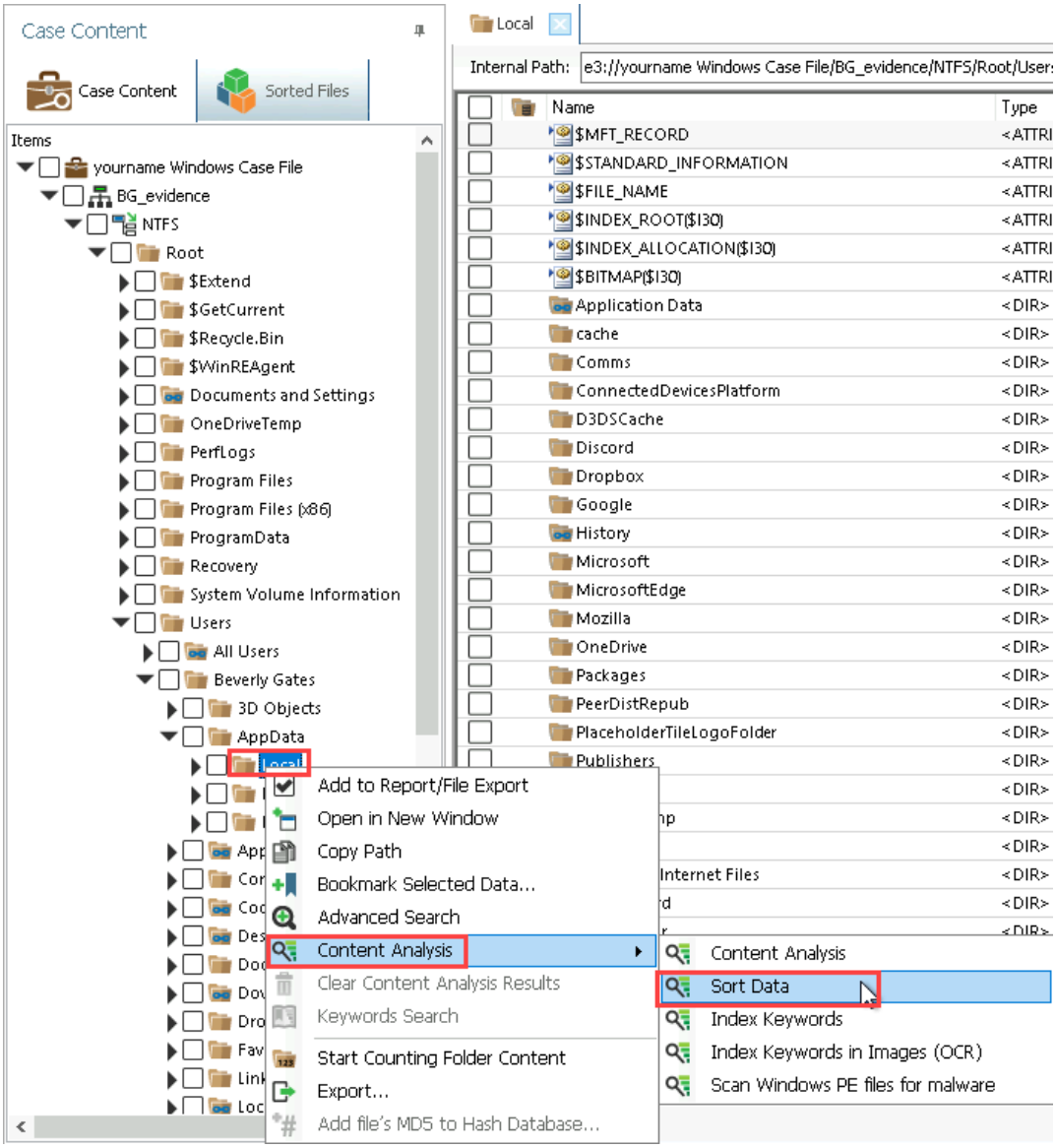
6. When prompted, **click OK** to accept the default name for the drive image and add the data from the drive image to your case file.

7. When prompted, **click OK** to close the NTFS Settings dialog box without making any changes.

Note: The *yourname* Windows Case File case will appear in the Case Content pane. The Case Content pane is the primary display and navigation area for all evidence in the open case file. Within the Case Content pane's tree-view structure, you can access case nodes, evidence nodes, evidence type nodes, folder nodes, and data grids/streams. Technically, the Case Content pane does not store the actual evidence, but provides a series of links to elements within the physical evidence.

When you select a specific node or grid within the Case Content pane, the contents of the enclosing folder or database will be displayed in the Data Viewer in the center pane. Within the Data Viewer, you can select individual files, folders, and records. Additional information about the currently selected node, grid, file, folder, or record will be displayed in the Viewers pane on the right, which provides multiple ways to view your current selection.

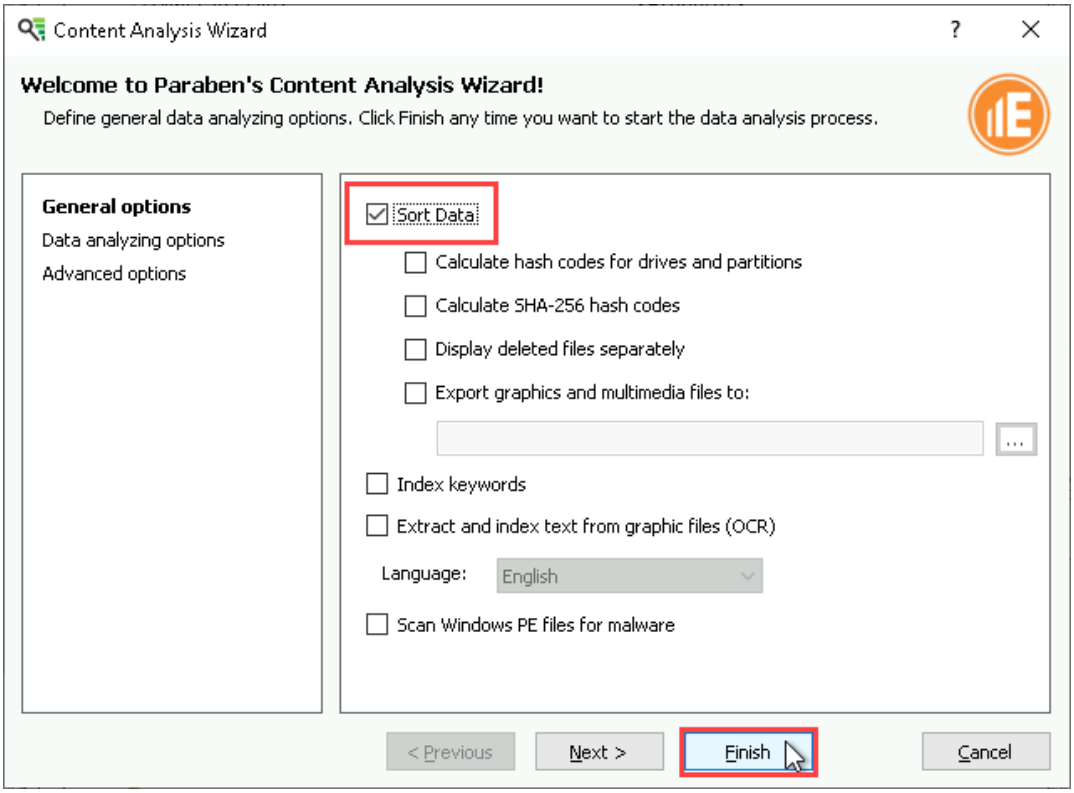
8. In the Case Content pane, **navigate** to ***yourname* Windows Case File\BG_evidence\NTFS\Root\Users\Beverly Gates\AppData**, then **right-click** the **Local folder** and **select Content Analysis > Sort Data** from the context menu to open the Content Analysis Wizard.



Case Content

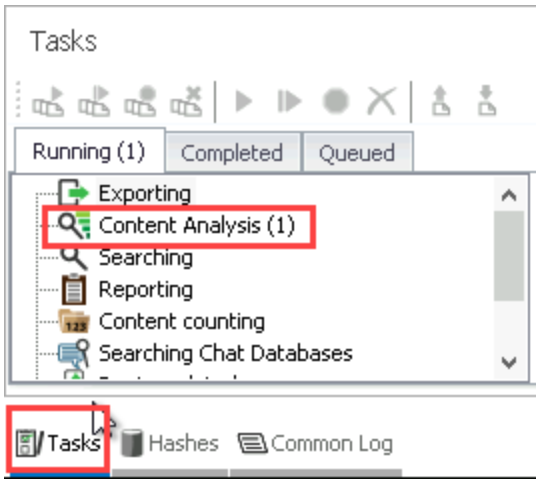
Note: You could run content analysis and sorting on the whole case file, but it would take too much time. To speed up the sorting process, you will limit content analysis to the Local folder. In this case, the process will take about 30 minutes. For comparison, sorting the entire evidence drive could take upwards of 2-3 hours, which is typical (if not low) for many drive images.

9. In the Content Analysis Wizard, **confirm** the Sort Data option is selected, then **click Finish** to launch the content analysis process.



Content Analysis Wizard

10. In the E3 window, **click** the **Tasks tab** and **select Content Analysis** to check the status of the content analysis process.



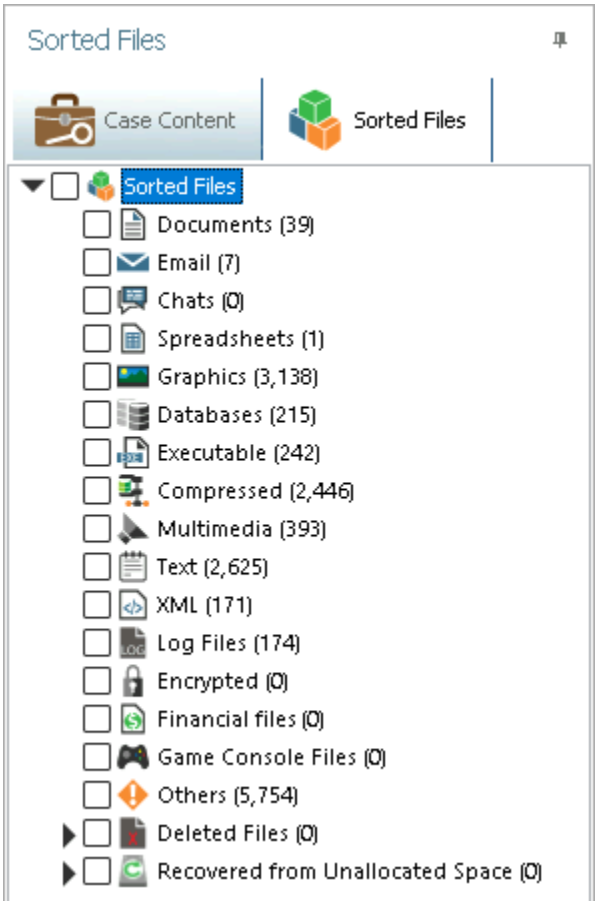
Tasks tab

Note: This process will take about 30 minutes. While running, the Tasks pane will show a (1) flag in the Running tab. When the task is finished, E3 will generate a notification.

11. When prompted, **click OK** to close the Task Status Notification dialog box.

12. In the left pane, **click** the **Sorted Files tab** to switch to the Sorted Files view.

13. In the Sorted Files pane, **double-click** the **Sorted Files node** to display the categories that E3 uses to sort files on the disk image.



Sorted Files categories

Note: Next to each category name, E3 indicates the number of files sorted into that category. The center pane now includes the complete list of all items identified during the Content Analysis and a total count of the items in the status line.

14. **Make a screen capture** showing the **Sorted Files**.

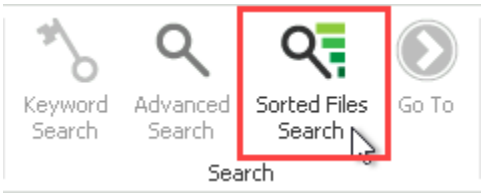
Part 2: Perform Forensic Analysis on a Windows Drive Image

Note: In this part of the lab, you will analyze the Windows drive, file system, and files to discover any potentially incriminating evidence against Beverly Gates.

1. In the Sorted Files pane, **select** the **Compressed category** to display a list of archive files on the suspect's drive in the Data Viewer.

Note: In the interest of time, you will limit this first part of your investigation to the Compressed category only. In a real-world investigation, you would likely need to examine all files.

2. On the E3 toolbar, **click** the **Analysis tab**, then **click** the **Sorted Files Search button** to open the Sorted Files Search tab in the center console.



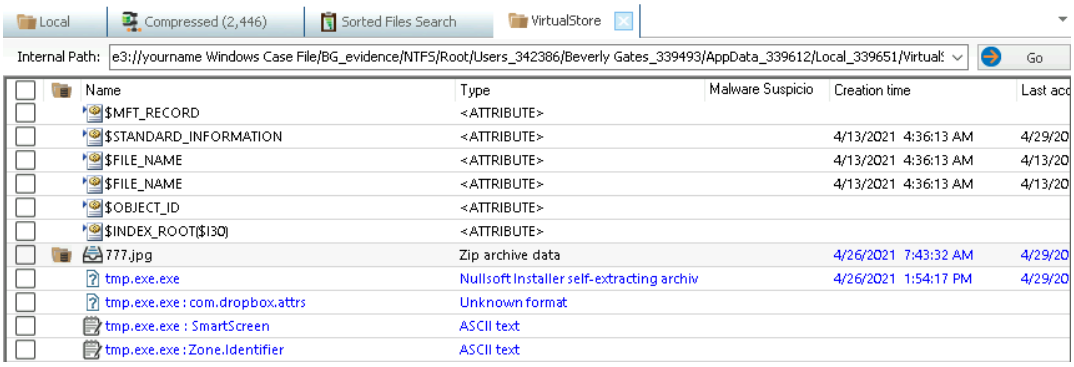
Sorted Files Search

3. On the Sorted File Search tab, **type** `.jpg` in the Filename field and **click** the **Only files with extension mismatch checkbox**, then **click Run Query** to run a search on the sorted evidence for files incorrectly identified as .jpg files.

Note: In the interest of time, you will limit your search to .jpg files only, as they are among most common file types. In a real-world investigation, you would likely need to examine all the files.

The search should return 11 results. Most of the files returned in the search appear to be PNG files that are improperly labelled as .jpg files, which is a reasonably common mistake among image files. However, the last file appears to be a .zip archive that's been mis-labeled as a .jpg, which seems like a strange and possibly deliberate decision – perhaps made with the intention of concealing the file's true nature.

4. In the Data Viewer, **double-click** the **777.jpg file** to display the file's location in the Case Content pane and open a new tab showing the contents of the enclosing folder.

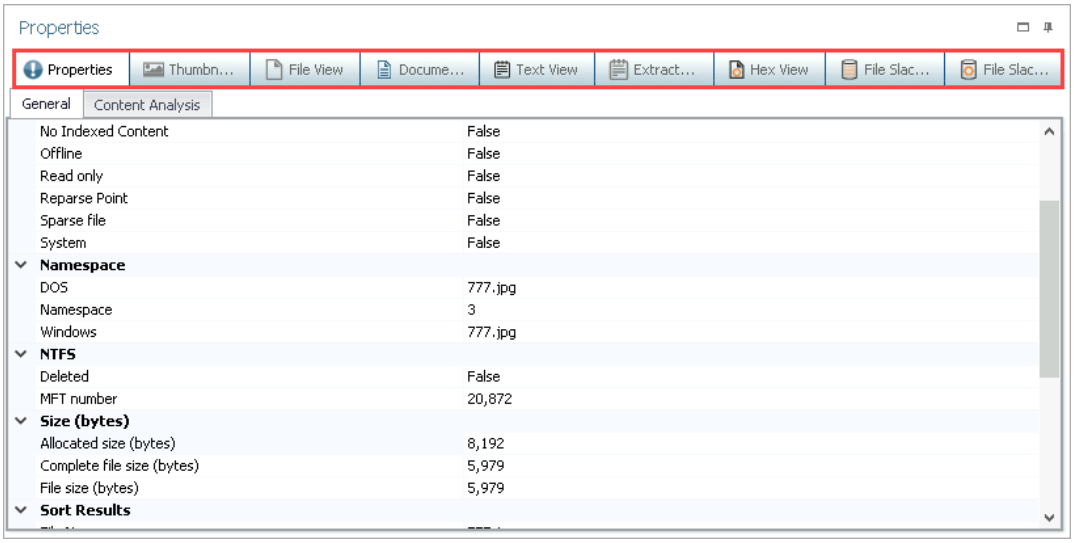


777.jpg file in the VirtualStore folder

Note: The file is located in the VirtualStore folder (Root\Users\BeverlyGates\AppData\Local\VirtualStore). This folder contains internal application data and is usually hidden in the system. In Windows, the hidden VirtualStore folder was intended as a compatibility feature to allow old programs to continue working in newer versions of Windows. However, because it is a hidden folder, it can be used to hide data.

When you select a file, E3 will display the file in different viewers in the right pane. You may need to expand this pane to see the name of each viewer tab, which includes Properties, Thumbnails View, File View, Document View, Text View, Extracted Text View, Hex View, File Slack: Text View, and File Slack: Hex View.

5. In the right pane, **click each tab** to gather more information about the 777.jpg file.



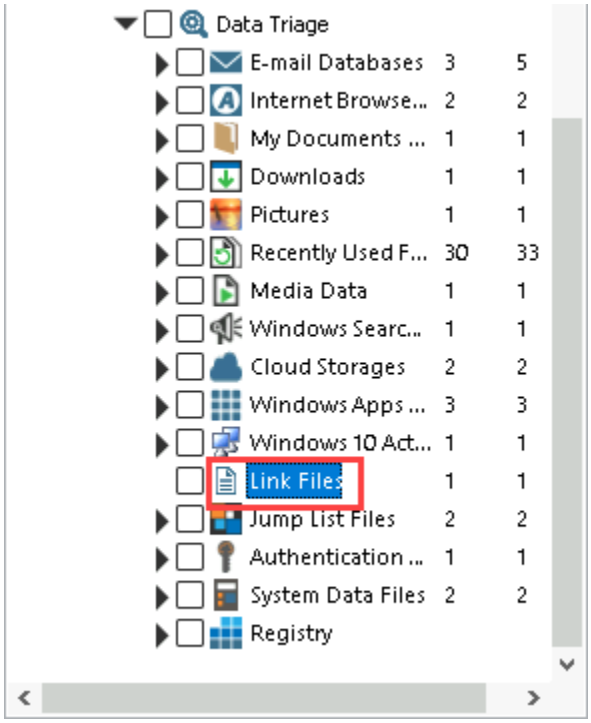
E3 file views

6. **Make a screen capture** showing the **contents of the 777.jpg file in the Document View.**

Note: Although E3 identified 777.jpg as a mislabeled .zip file, based on the Document View, it actually appears to be a spreadsheet. So which one is it? Actually, both. Excel spreadsheet files (.xls and .xlsx) are actually a compressed package of XML files. If you were change the defined file format of an Excel file on your local computer, you could un-zip it and inspect the internal folder and file structure. Fun facts about file formats aside, the contents of this spreadsheet definitely looks like a list of customers, amounts owed, and drugs.

Now that you have the first piece of potentially incriminating evidence, including the file's location on the suspect's computer, it is time to dig deeper and look for additional evidence. This file is likely the first of many potentially incriminating files on the suspect's computer. Because actions are rarely done in isolation when interacting with a computer, you will explore some other likely places where incriminating actions could have taken place and incriminating files could be stored.

7. In the Case Content pane, **scroll down** to the bottom and **expand** the **Data Triage header**, then **expand** the **Link Files category** to display the contents of this category in a new tab in the Data Viewer.



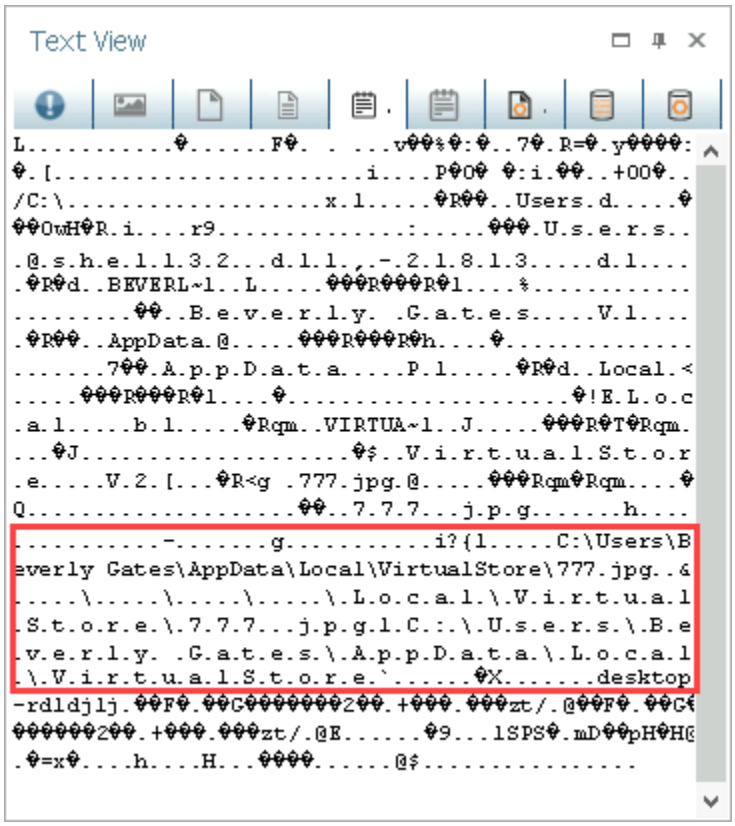
Data Triage > Link Files

Note: You should see that the Link Files category contains one folder – the Recent folder. This folder contains several links to files located throughout the filesystem. In E3, the Link Files category is part of the Data Triage functionality, and it contains not only the user-created links, but the automatically-created links that appear as a user works with files. These links allow investigators to identify a user's recent activity and serve as irrefutable proof that a file has been recently accessed.

8. In the Data Viewer, **double-click** the **Recent folder** to open it.

9. In Data Viewer, **locate** and **select** the **777.lnk file**, then **click** the **Text View tab** on the right to view the contents of this file.

   The 777.lnk file contains the file path to 777.jpg in the system, which should match the file path you observed earlier.



File path in .lnk file

10. **Make a screen capture** showing the **777.lnk file contents including the path to the file in the system**.

11. In the Case Content pane, **select** the **Data Triage / Downloads category** to display the contents of this category in the Data Viewer.

12. In the Data Viewer, **double-click** the **Downloads folder** to open it.

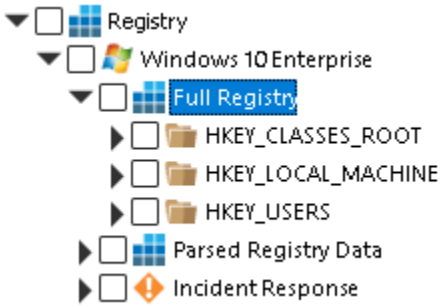
13. **Review** the **Downloads folder** to identify traces of suspicious activity (for example, the downloaded installation files for Speedify VPN and Tor browser).

Note: The Tor network disguises your identity by encrypting your traffic and moving it across different Tor relays within the network. The Tor browser is one of the most popular browsers for enabling

anonymous communications on the Internet (for example, when accessing the darknet). VPN solutions are typically used in conjunction with Tor to further conceal traces of the activity in the web. Most companies prohibit any Tor software from being installed on their systems for security reasons. Evidence of this type of software is often an indication of unauthorized, covert communication.

14. **Make a screen capture** showing the **installation files for suspicious apps in the Downloads category**.

15. In the Case Content pane, **expand** the **Data Triage / Registry category**, then **expand** the **Windows 10 Enterprise / Full Registry sub-categories**.



Full Registry

Note: The Registry category in E3 shows the contents of the Windows Registry in the same format as the Registry Editor on a live system. In the disk image, there are three main registry hives present:

- **HKEY_CLASSES_ROOT** (HKCR)
- **HKEY_LOCAL_MACHINE** (HKLM)
- **HKEY_USERS** (HKU)

Two of the hives that you investigated in Section 1 are absent, because there is no current user or current configuration for the disk image. The data from the HKEY_CURRENT_USER hive is a part of the HKEY_USERS hive and data from the HKEY_CURRENT_CONFIGURATION hive is a part of the HKEY_LOCAL_MACHINE hive.

Based on the evidence you have collected so far, the Parsed Registry Data category likely contains registry values that might be important for investigation.

16. **Expand** the **Parsed Registry Data / Programs sub-categories**, then **select** the **Uninstall folder** to see what programs generated registry keys related to deinstallation on the suspect's machine.

Note: This function automatically searches the Registry for any programs that were installed on the target system and generated registry keys linking them to the Windows uninstall feature. Pay attention to the suspicious applications listed here. You should see additional evidence that the Speedify VPN application was not only downloaded but installed.

17. **Make a screen capture** showing the **VPN application (Speedify) in the Uninstall folder**.

18. In the Case Content pane, **select** the **Users Info sub-category** to see the list of users on the suspect's machine.

19. **Make a screen capture** showing the **users list**.

20. In the Data Viewer, **open** the **Beverly Gates user record**, then **open** the **Run folder** to see the applications that are set to run automatically on start-up.

    When prompted, **click OK** to close the notification.

21. **Make a screen capture** showing the **contents of the Beverly Gates / Run folder**.

Note: Your evidence list now includes an incriminating spreadsheet with drug prices and inventory, as well as multiple records of the use of an anonymized browser and VPN, including the installers and registry records. In the next steps, you will extend your search to the Chrome browser.

22. In the Case Content pane, **select** the **Data Triage / Internet Browser Data category**, then **navigate** to the **Default / History folder** in the Data Viewer.

23. **Review** the **History sub-node** and **locate** an example of suspicious browsing activity.

24. **Make a screen capture** showing **at least one suspicious browsing record found in the History sub-node**.

25. **Review** the **Keywords sub-node** and **locate** the **suspicious keywords**.

26. **Make a screen capture** showing **at least one suspicious search found in the Keywords sub-node**.

27. **Close** the **E3 window**.

Note: This concludes Section 2 of the lab.

Section 3: Challenge and Analysis

Note: The following exercises are provided to allow independent, unguided work using the skills you learned earlier in this lab - similar to what you would encounter in a real-world situation.

Part 1: Use Advanced Search to Locate Additional Evidence

Your investigation of Beverly Gates has progressed well and you now have several pieces of incriminating digital evidence. However, as a seasoned investigator, you have learned a few tricks for surfacing well-concealed evidence over the years. One such trick is the use of E3's Advanced Search functionality combined with your own custom word lists of commonly used terms found in drug trafficking cases.

From the Case Content pane, right-click the Users\Beverly Gates\AppData\Local\Packages folder and select the Advanced Search option. In the Advanced Search pane, click the Load Words button and open the Drug Search Term List1.txt file in the Beverly Gates Evidence folder. Next, select the Whole word option and click Start.

From the Advanced Search results, locate a suspicious file that contains suspicious addresses.

Make a screen capture showing the **contents of the suspicious file in the Document View**.

Part 2: Identify Suspicious Browser Activity

Given your recent success with surfacing new evidence using E3's Advanced Search functionality, it occurs to you that it may be worth running an Advanced Search in areas that you previously explored in your initial investigation. You know that the Registry is deep well of potential evidence, and you have reason to believe that Beverly was both interested in the Tor browser and careless enough to run incriminating web searches from her work computer. You decide to revisit the Registry and look for additional evidence related to Tor .

In the Data Triage / Registry / Windows 10 Enterprise / Parsed Registry Data category, go to the Users Info > Beverly Gates > Applications, right-click the Applications folder and select Advanced Search. Use the Advanced Search feature to search for the keyword *Tor* with the Whole word option selected. Review the results and locate evidence that suggests that Tor was run as an extension in Firefox.

Make a screen capture showing **at least one registry key with information associated with Tor and Firefox**.

Note: This concludes Section 3 of the lab.