Introduction

One legal standard that is key to forensics and too often overlooked in forensic books is the Daubert standard. This standard is used by a trial judge to make a preliminary assessment of whether an expert's scientific testimony is based on reasoning or methodology that is scientifically valid and can properly be applied to the facts at issue. Under this standard, the following factors may be considered in determining whether the methodology is valid:

1. Has the theory or technique in question been tested?
2. Has the theory or technique been subjected to peer review and publication?
3. Does the theory or technique have any known or potential errors?
4. Does the theory or technique adhere to the maintenance of standards controlling its operation?
5. Has the theory or technique attracted widespread acceptance within a relevant scientific community?

Established in 1993 as a result of the Supreme Court case *Daubert v. Merrell Dow Pharmaceuticals, Inc.* (509 U.S. 579), the Daubert standard is the test currently used in federal and most state courts. Because the Daubert standard requires that scientific evidence presented in court be generally accepted in the field, it is unlikely that new tools would be immediately approved for use in court. For this reason, it is important that a forensic investigator be familiar with emerging technologies and developments in the field of forensic techniques.

In this lab, you will act as a forensic specialist assisting the lead forensics investigator at the Cyber Crimes Division (CCD) of the Boston Police Department. You have been given a hard drive image taken from a seized computer that is suspected to contain evidence of a sophisticated drug trafficking operation. First, you will review the search warrant and complete the Chain of Custody form that accompanies the evidence drive. You will then prepare the contents of the seized hard drive image as evidence in accordance with the Daubert standard using a variety of forensic tools.

Lab Overview

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

1. In the first part of the lab, you will review a search warrant and complete a Chain of Custody form for seized evidence.

2. In the second part of the lab, you will use FTK Imager to create hash codes for suspicious files.

3. In the third part of the lab, you will validate the hash codes using Paraben's E3.

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 explore the suspect's drive image to locate additional evidence. You will also use Autopsy, another popular digital forensics tool, to validate the hash codes created during your preliminary investigation.

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. Prepare evidence for court and complete forms used in evidence handling.

2. Understand how a judge will determine the admissibility of evidence using the Daubert standard.

3. Import a drive image as evidence using digital forensics software.

4. Identify suspicious files as evidence using digital forensics software.

5. Create hash codes to verify the integrity of forensic evidence.

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.

- FTK Imager
- Paraben's E3
- Autopsy

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:

- Contents of the search warrant in Adobe Reader
- Completed Chain of Custody form in Adobe Reader
- Contents of the 0002665_hash.csv file
- Contents of the RecycleBinEvidence_hash.csv file
- Contents of the MyRussianMafiaBuddies_hash.csv file
- Contents of the Nice guys_hash.csv file
- MD5 and SHA1 values for the MyRussianMafiaBuddies.txt file
- MD5 and SHA1 values for the Nice Guys.png file

2. Any additional information as directed by the lab:

- Describe how the hash values produced by E3 for the incriminating files compare to those produced by FTK. Do they match?

SECTION 2

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

- Contents of the suspicious email file in the Display pane
- Two hash values for the suspicious email file
- MD5 field in the Result Viewer
- MD5 value produced by E3.

2. Any additional information as directed by the lab:

- Describe how the hash value produced by Autopsy compares to the values produced by FTK

Imager for the two .eml files.
- Describe how the hash value produced by E3 compares to the values produced by FTK Imager for the two .eml files and the value produced by Autopsy.

SECTION 3

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

- Hash values for the Evidence_drive1.001 file

2. Any additional information as directed by the lab:

- Define the original file names and file paths for each of the three files.

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**.

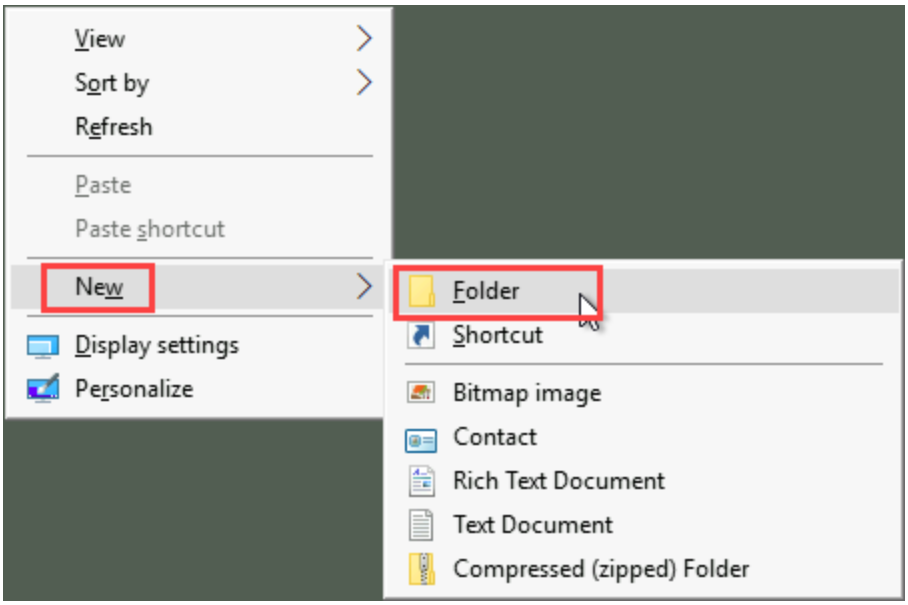
Part 1: Complete Chain of Custody Procedures

Note: The setting for this lab is an ongoing investigation into the activities of Beverly Gates, the HR Manager at Intricate Solutions, Inc. Senior leadership at Intricate Solutions has reason to believe that Beverly is involved in a sophisticated drug trafficking operation and has recently contacted the local police department to investigate the matter further. The police officer assigned to the case, Brendan O'Rourke, has already processed a search warrant and seized a hard drive at Beverly's home. The police department has assigned 10001-BPD-CCD as the case number for the Beverly Gates case. As a digital forensics specialist assigned to the case, the seized hard drive has been transferred to you for further investigation.

When a search warrant is issued, it is critically important to pay attention to what you are and are not allowed to examine or seize. A search warrant places specific boundaries around the evidence you can collect. Overstepping those boundaries can put the entire investigation in jeopardy. In conjunction with the search warrant, the chain of custody process will determine whether evidence may be considered admissible in court. Without following chain of custody and producing the appropriate documentation to support it, the opposing attorney can challenge or dismiss the evidence presented.

In the next steps, you will review the search warrant and complete the chain of custody form to take possession of the seized disk image.

1. On the vWorkstation desktop, **right-click anywhere** and **select New > Folder** from the context menu to create a new folder.



Create a new folder

2. In the folder name field, **type** `10001-BPD-CCD` and **press Enter** to name the new folder.

   You will save your work to this folder as the lab progresses.

3. On the vWorkstation taskbar, **click** the **File Explorer icon** to open a new File Explorer window.

File Explorer

4. In the File Explorer, **navigate** to **C:\Daubert Standard Evidence**.

5. In the Daubert Standard Evidence folder, **double-click** the **BG_warrant PDF** to open it in Adobe Reader.

6. In the Adobe Reader window, **review** the contents of the **BG_warrant PDF.**

7. **Make a screen capture** showing the **contents of the search warrant in Adobe Reader**.

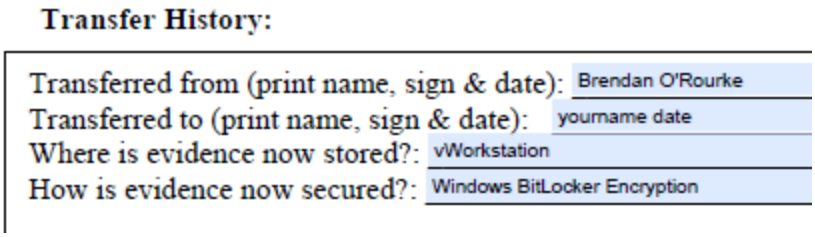
8. **Close** the **Adobe Reader window**.

9. In the Daubert Standard Evidence folder, **double-click** the **chain_of_custody_10001 PDF** to open it in Adobe Reader.

10. In the Transfer History section of the form, **type** the following information in the first block of entries to record the transfer of data.

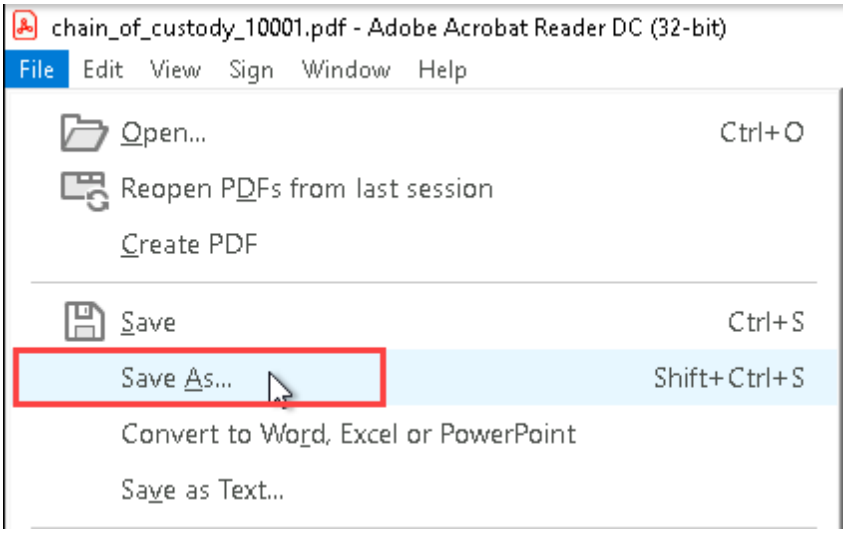
    - Transferred from: **`Brendan O'Rourke`**
    - Transferred to: ***`yourname`*** and ***`date`***, replacing *yourname* and date with your own name and the current date
    - Where is the evidence now stored: **`vWorkstation`**
    - How is the evidence now secured: **`Windows BitLocker Encryption`**

    Typically, this document would be signed by the investigator as well, but you will not be able to add an actual signature to this form.



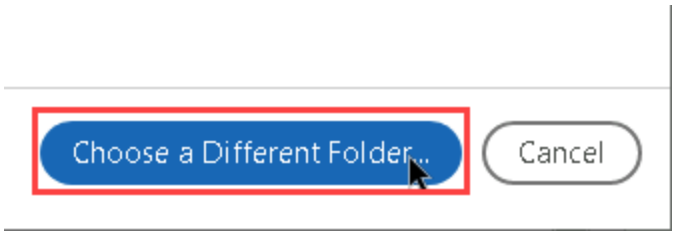
Transfer History

11. From the Adobe Reader menu bar, **click File** and **select Save As** from the drop-down menu.



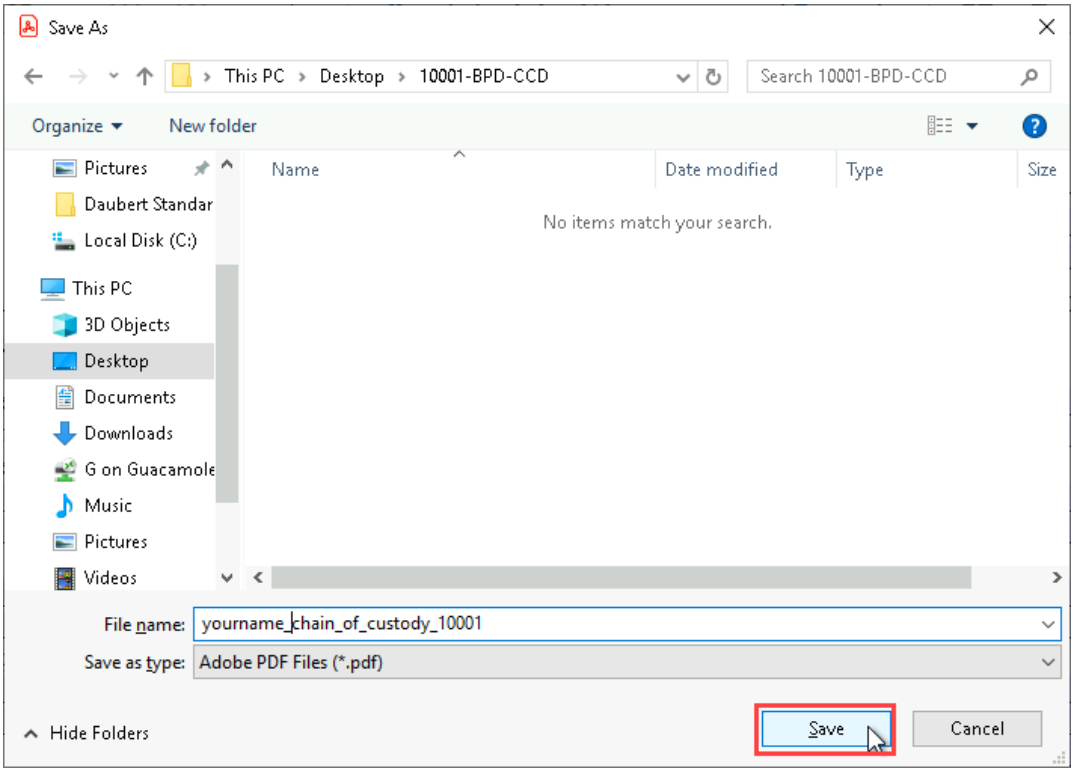
Save As

12. In the Save As dialog box, **click** the **Choose a Different Folder... button** to open another Save As dialog box.



Choose a Different Folder

13. In the second Save As dialog box, **navigate** to the 10001-BBD-CCD folder you created earlier in the lab (**This PC > Desktop > 10001-BPD-CCD**), then **type** ***yourname*_chain_of_custody_10001** in the File name field, replacing *yourname* with your own name, and **click Save** to save this file to the evidence folder.



Save As dialog box

14. **Make a screen capture** showing the **completed Chain of Custody form in Adobe Reader.**

15. **Close** the **Adobe Reader** and **File Explorer windows**.

Part 2: Extract Evidence Files and Create Hash Codes with FTK Imager

Note: To adhere to the Daubert standard, the prosecution must be able to show that evidence obtained during an investigation was not altered in any way during the process. To demonstrate the integrity of digital evidence, forensic investigators commonly employ sophisticated digital forensics software that allows them to efficiently analyze evidence, extract files, and generate hash codes for extracted evidence. These hash codes can later be compared to hash codes for the same files on the original drive image. Because hash codes for a given file will differ if the file is altered, if the hash codes match, this may be considered proof of integrity. That said, it is the job of the judge to assess the tools, processes, and evidence in full before determining if the evidence adheres to the Daubert standard and may be considered admissible.

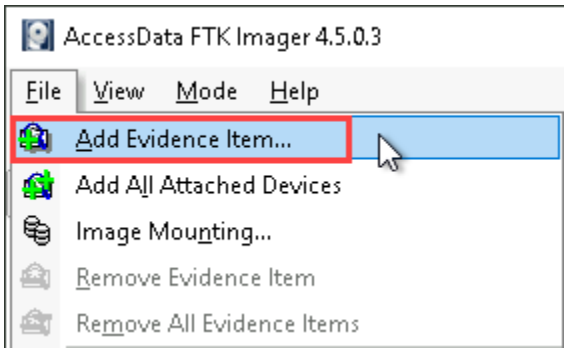
In this part of the lab, you will use FTK Imager to extract evidence from the seized drive image in a manner that adheres to the Daubert standard. In the next steps, you will use FTK Imager to acquire the seized drive image and search for suspicious files, extracting evidence and hash codes as you go along. The hash codes you create with FTK Imager will later be validated using another forensic tool in the next part of this lab.

1. On the vWorkstation desktop, **double-click** the **AccessData FTK Imager icon** to open the FTK Imager application.

FTK Imager icon

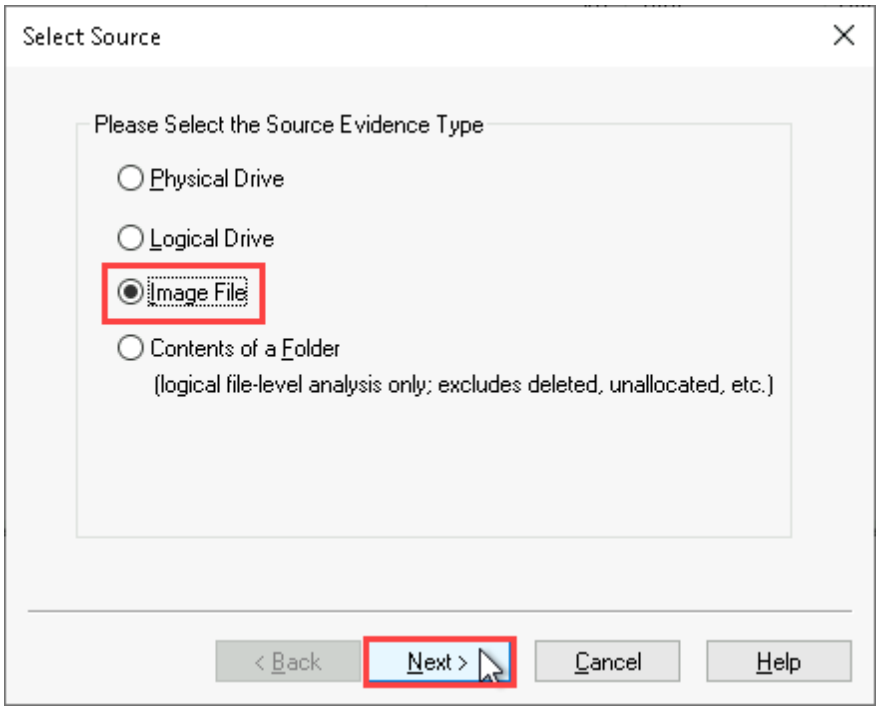
Note: FTK Imager is a free disk imaging and data preview tool developed by AccessData, now owned by Exterro. FTK Imager is a standalone utility associated with the Forensic Toolkit (FTK), a professional-grade digital forensics tool suite that offers enhanced search and analysis functionality for a variety of digital evidence formats. FTK Imager allows you to create forensic images, preview files and folders, mount an image for read-only viewing, recover deleted files, create hashes of files, and generate hash reports. In addition to the normal GUI, certain FTK Imager functions can be run from the command line.

2. From the AccessData FTK Imager menu bar, **select File > Add Evidence Item** to open the Select Source dialog box and begin adding evidence.



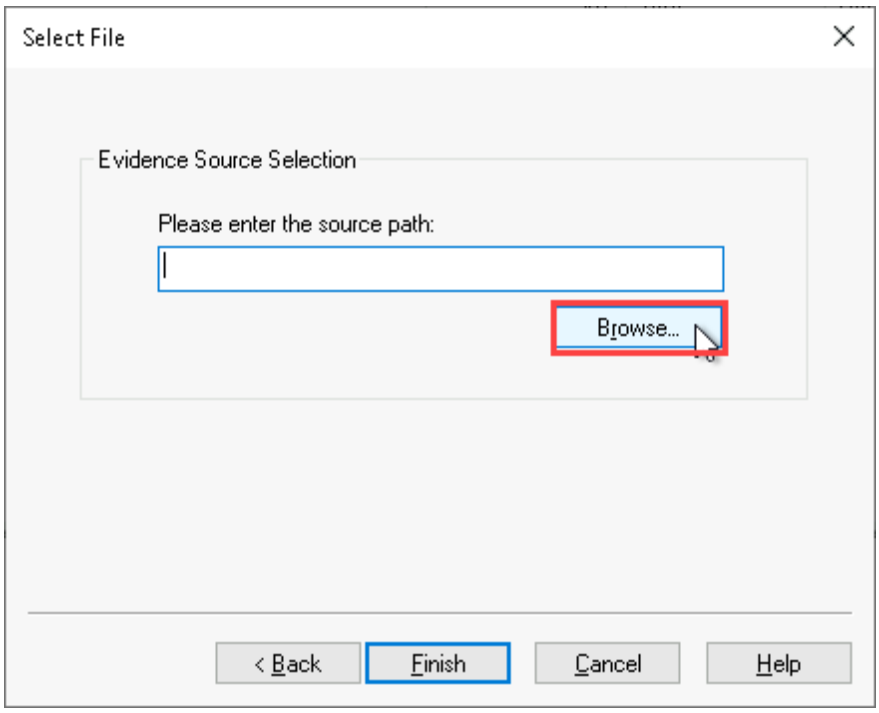
Add Evidence Item

3. On the Select Source page, **click** the **Image File radio button** and **click Next** to continue.



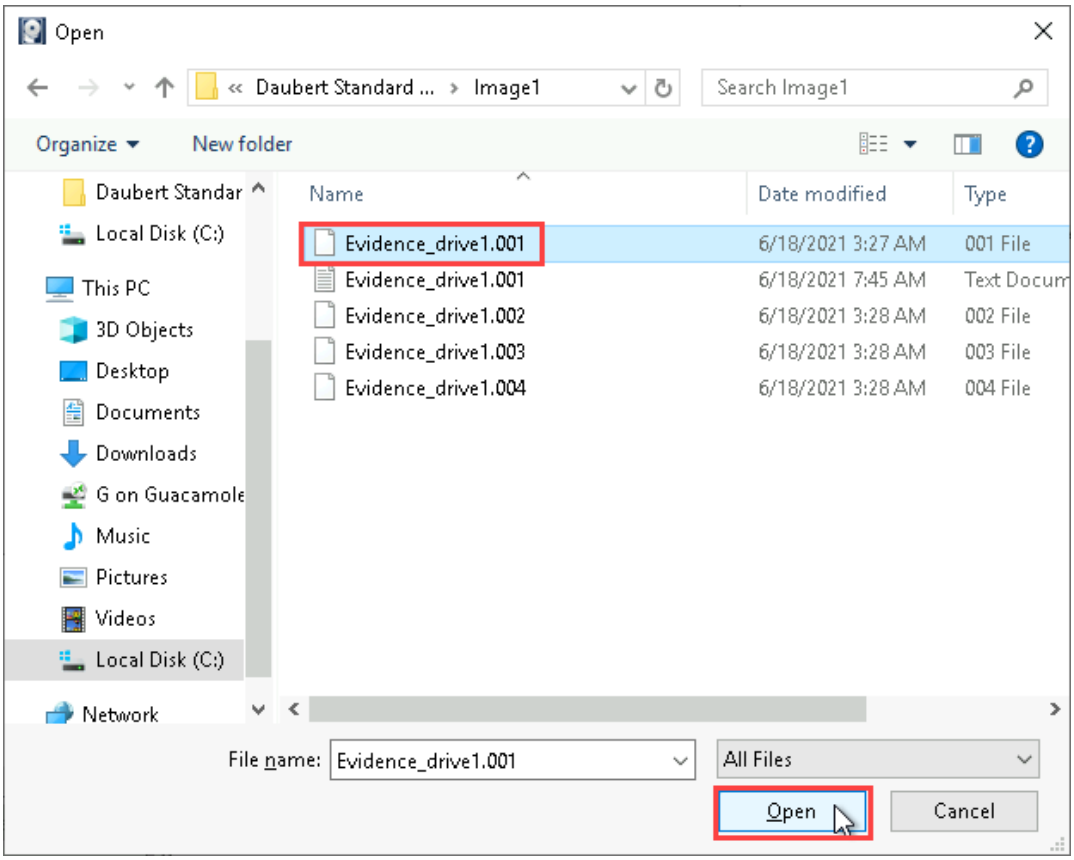
Select Source

4. On the Select File page, **click** the **Browse button** to open the Open dialog box.



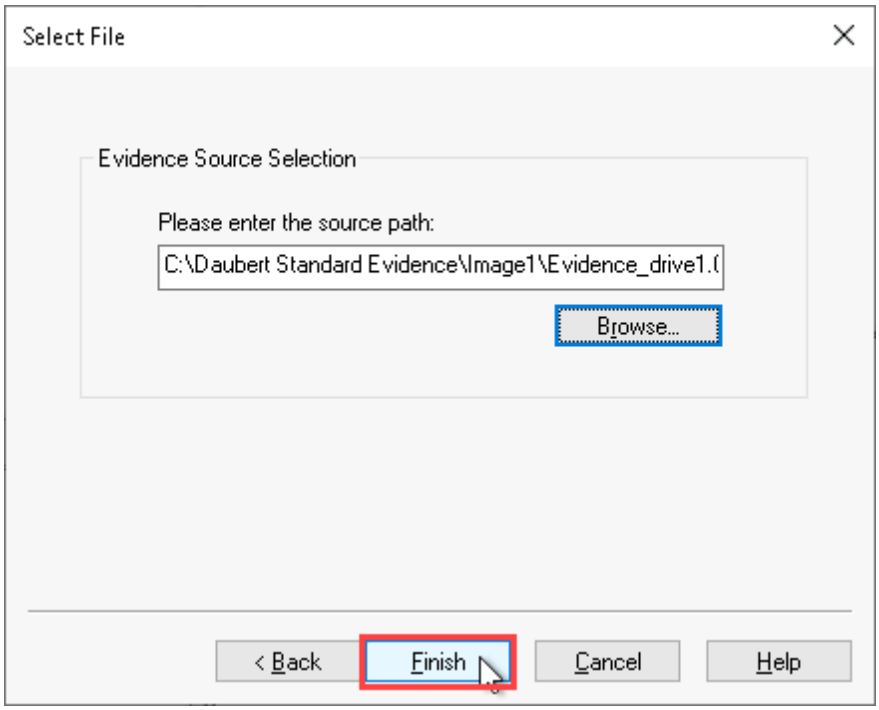
Click the browse button

5. In the Open dialog box, **navigate** to (**This PC > Local Disk (C:) > Daubert Standard Evidence > Image1**), then **select** the first **Evidence_drive1.001 file** and **click Open**.



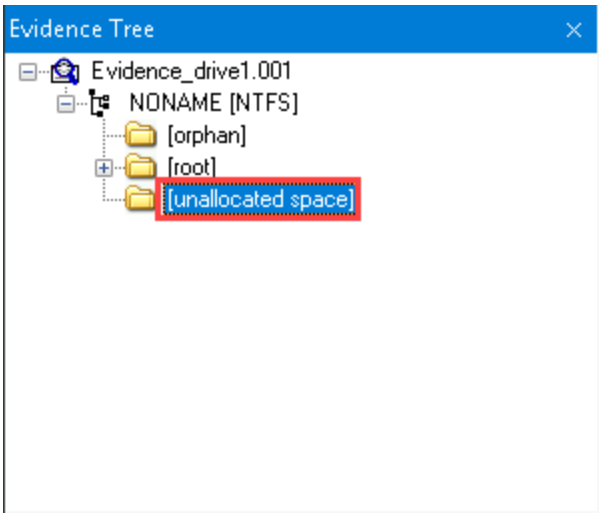
Open the Evidence_drive1.001 file

6. On the Select File page, **click Finish** to open the suspect's drive image in FTK Imager.



Finish adding evidence

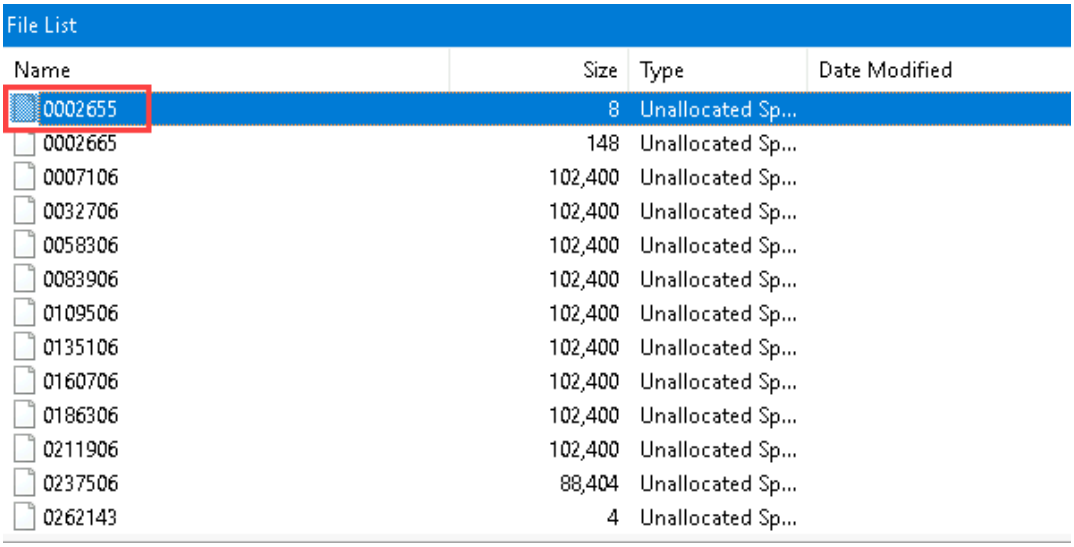
7. In the Evidence Tree pane, **navigate** to **Evidence_drive1.001 item > NONAME [NTFS] > [unallocated space]** to display its contents in the File List pane.



Evidence Tree

Note: In the Windows NTFS file system, deleted files are not actually deleted - they are retained in the unallocated space on the hard drive. This is often a very evidence-rich area of the evidence drive, as deleted files should always prompt investigators to explore motives. For the purposes of your investigation, the unallocated space on Beverly Gates's hard drive seems like a great place to begin looking for evidence.

8. In the File List pane, **select** the **first file (0002655)** to view the contents in the Display pane.



File List

Note: The File List pane displays files in alphabetical order based on the file name. The Display pane will show images, hex view, or clear text, depending on the file type.

9. In the Display pane, **review** the contents of the 0002655 file.

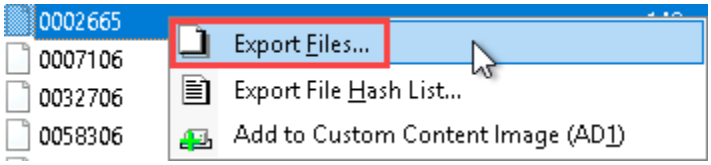
Note: The file appears to be an email between Beverly Gates and several Intricate Solutions employees about setting up a recurring meeting. Nothing suspicious about that - at least outside the context of additional evidence. Time to move to the next file.

10. In the File List pane, **select** the **second file (0002665)** to view the contents in the Display pane.

11. In the Display pane, **review** the contents of the 0002665 file.

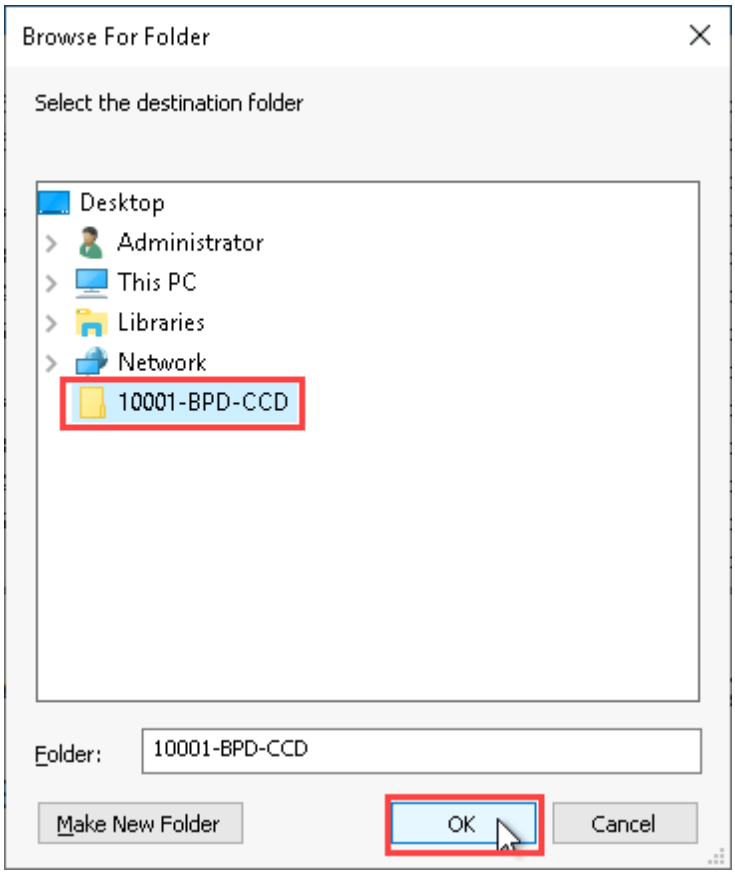
Note: Now this is a little more interesting. Given that Beverly is suspected of being involved in drug trafficking, this file looks an awful lot like an image containing a list of drug dealers, what they sell, and their phone numbers. You would be well-advised to save this file to your evidence folder for future reference.

12. In the File List pane, **right-click** the **0002665 file** and **select Export Files** from the context menu to extract this file as evidence.



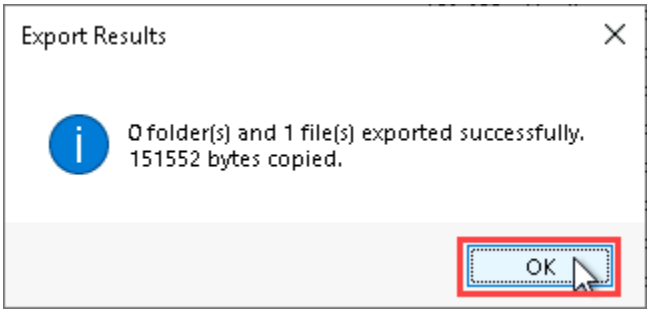
Export Files

13. In the Save As dialog box, **navigate** to the **10001-BPD-CCD folder** you created earlier in the lab, then **click OK** to save this file to the evidence folder.



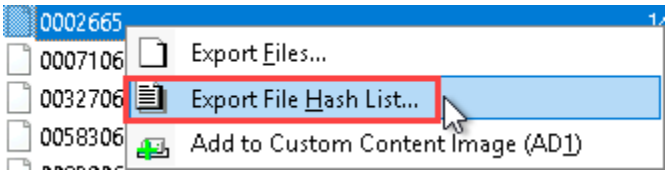
Browse for Folder

14. When prompted, **click OK** to close the Export Results dialog box.



Export Results

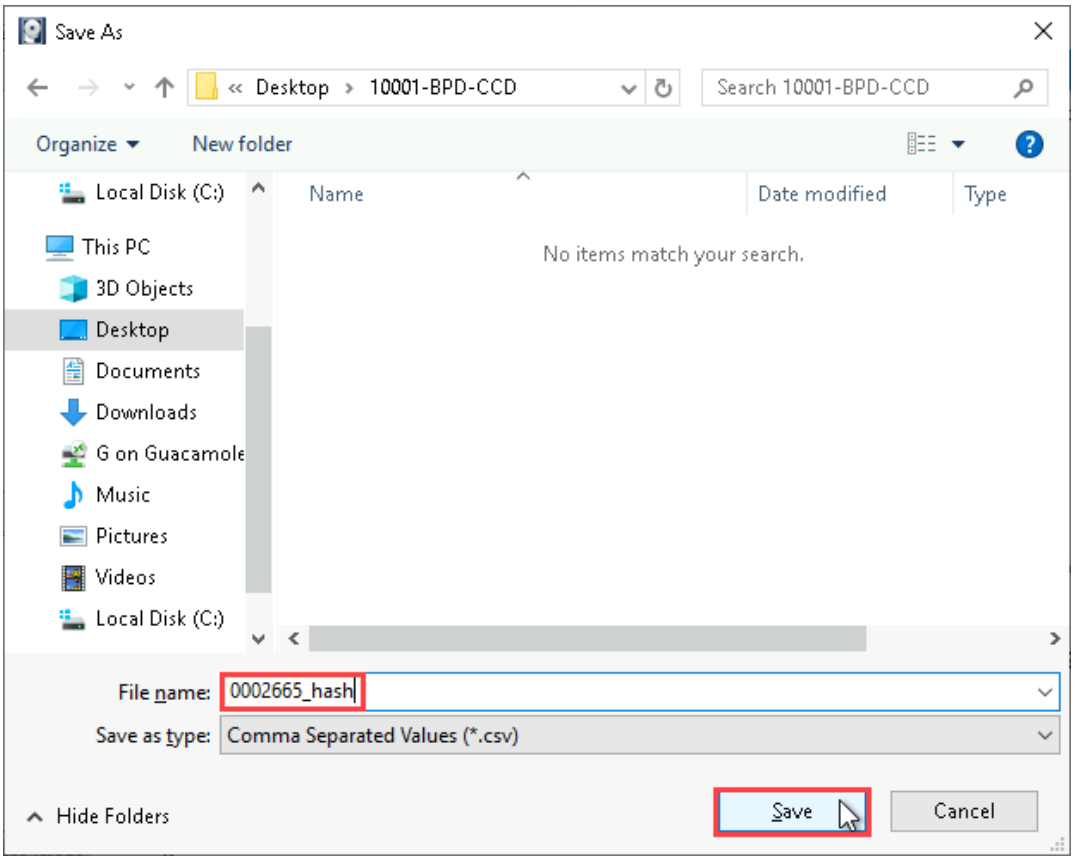
15. In the File List pane, **right-click** the **0002665 file** and **select Export File Hash List** from the context menu to create a hash code for this file.



Export File Hash List

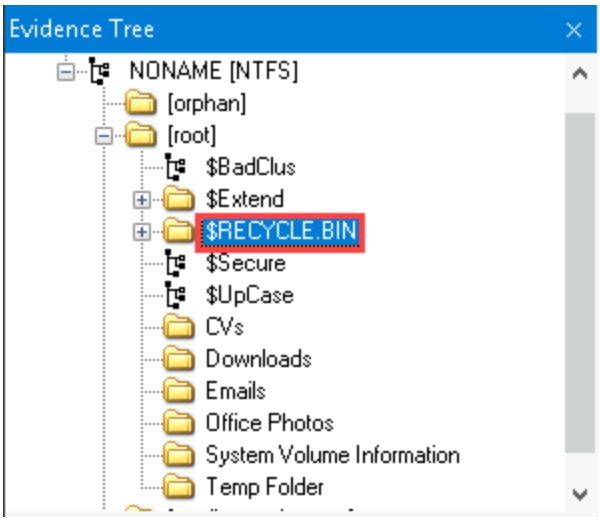
Note: When you use the Export File Hash List function, you are generating a human-readable file that contains three important fields: MD5, SHA1, and filename location. The MD5 and SHA1 are hash values for the file and the filename location is the name of the imaged/seized drive along with full-path name (within the drive image) of the file. When vetting and verifying evidence, as long as the file remains unchanged, these three fields will be the same regardless of the forensic tool (FTK Imager, Autopsy, E3, or others) used to view it.

16. In the Save As dialog box, **navigate** to the 10001-BPD-CCD folder (**This PC > Desktop > 10001-BPD-CCD**), then **type** `0002665_hash` in the File name field and **click Save** to save this file to the evidence folder.



Save As dialog box

17. In the Evidence Tree pane, **navigate** to **Evidence_drive1.001 item > NONAME [NTFS] > [root] > $RECYCLE.BIN** to view the contents in the Display pane.



Evidence Tree

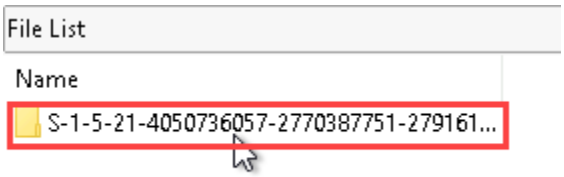
Note: In Windows systems, the Recycle Bin holds files that the user intends to delete. Like the unallocated space, it is one of the first places an investigator should explore. However, unlike the unallocated space, the contents of the Recycle Bin remain visible to the user and can be easily restored if required. When the Recycle Bin is emptied, any files in Recycle Bin are "deleted" and moved to the unallocated space.

When files are moved to the Recycle Bin in Windows 10, two files are created in the Recycle Bin. The first file is assigned a random alpha-numeric name beginning with $I. This file contains the original location of the deleted file. The second file is assigned the same random name, but beginning with $R. The second file is the actual deleted file.

In older versions of Windows (with the exception of Windows Vista), deleted files were renamed DC#.ext, where # is an incrementally increasing integer number (for example, DC1, DC2, DC3, etc.) and ext is the original file's extension (for example, .txt or .exe). The original locations of all deleted files are stored in a single file titled INFO2.

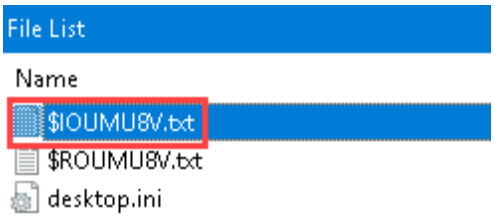
For forensic investigators, the fact that a file was deleted suggests that the owner of this computer may have wanted to hide it. This behavior is not inherently criminal, as deleting files from a computer is also simply good hygiene, but in the context of a forensic investigation, it is potentially suspicious.

18. In the File List pane, **double-click** the **S-1-5-21-4050736057-2770387751-2791612479-1001 folder** to open it.



File List

19. In the File List pane, **select** the **$IOUMU8V.txt file** to view the file contents in the Display pane.



File List

20. In the Display pane, **review** the contents of the $IOUMU8V.txt file.

Note: The $IOUMU8V.txt file contains the original file name and location of the deleted file, which is now stored as $ROUMU8V.txt in the Recycle Bin. In this case, $ROUMU8V.txt appears to be the Recycle Bin name for a file titled MyRussianMafiaBuddies.txt file that was deleted from the Downloads folder.

21. In the File List pane, **select** the **$ROUMU8V.txt file** to view the contents in the Display pane.

Note: As the original file name implies, this file appears to contain a list of Russian names and addresses. Given that Beverly Gates is under investigation for drug trafficking, it would seem reasonable to take the name of this file at face value. You should save this file as another piece of evidence.

21. In the File List pane, **click the $IOUMU8V.txt file while holding down the control key** to select both files.

22. **Repeat steps 12-14** to save the $IOUMU8V.txt and $ROUMU8V.txt files to the 10001-BPD-CCD folder.

23. **Repeat steps 15-16** to export the hash values for the $IOUMU8V.txt and $ROUMU8V.txt files to the 10001-BPD-CCD folder as a .csv file titled **`RecycleBinEvidence_hash`**.

Note: In the next steps, you will attempt to locate copies of the deleted files with their original file names on Beverly Gates' hard drive. FTK Imager does not have a search function, so searching for specific files must be done manually. A thorough investigation using FTK Imager can take days, but for the purpose of this lab, you can look through the folders available in the disk image, as it does not contain a lot of data. Because you know the contents of one deleted file and the original name of the other, you should be able to identify copies of the files fairly easily.

At a glance, you should see a few different folder in the root directory, including CVs, Downloads, Emails, Office Photos, System Volume Information, and Temp Folder. As far as folder names go, Temp Folder is a bit strange, which makes it as good a place as any to start.

24. In the Evidence Tree pane, **navigate** to **Evidence_drive1.001 item > NONAME [NTFS] > [root] > Temp Folder** to display its contents in the File List pane.

Note: Okay, that was a little too easy, but that sure looks like a copy of the MyRussianMafiaBuddies.txt file and an image file titled Nice Guys.png. This seems to be exactly what you're looking for.

25. **Review each file in the Display pane** to verify that they match the files you previously found in the Unallocated space and Recycle Bin.

26. **Repeat steps 12-14** to save the MyRussianMafiaBuddies.txt to the 10001-BPD-CCD folder.

27. **Repeat steps 15-16** to export the hash values for the MyRussianMafiaBuddies.txt file to the 10001-BPD-CCD folder as a .csv file titled **`MyRussianMafiaBuddies_hash`**.

28. **Repeat steps 12-14** to save the Nice Guys.png to the 10001-BPD-CCD folder.

29. **Repeat steps 15-16** to export the hash values for the Nice Guys.png file to the 10001-BPD-CCD folder as a .csv file titled **`Nice guys_hash`**.

30. **Close** the **FTK Imager window**.

31. On the vWorkstation Desktop, **double-click** the **10001-BPD-CCD folder** to open it.

32. In the 10001-BPD-CCD folder, **double-click** the **0002665_hash.csv file** to open the file in the Notepad application.

33. **Maximize** the **Notepad window** to ensure the MD5, SHA1, and file name are fully visible.

    If necessary, select Notepad > Format > Enable Word Wrap.

Note: The MD5, SHA1 hash codes generated by FTK Imager will remain the same, no matter which investigator, which program, or which day the files are touched. The hash codes will only change if the file itself is changed, thereby assuring the court that the evidence they are looking at has not been altered.

34. **Make a screen capture** showing the **contents of the 0002665_hash.csv file**.

35. **Close** the **Notepad window.**

36. **Repeat steps 32-35** for each .csv in the case folder.

37. **Make a screen capture** showing the **contents of the RecycleBinEvidence_hash.csv file**.

38. **Make a screen capture** showing the **contents of the MyRussianMafiaBuddies_hash.csv file**.

39. **Make a screen capture** showing the **contents of the Nice guys_hash.csv file**.

40. **Close** the **10001-BPD-CCD folder**.

Part 3: Verify Hash Codes with E3

Note: In this part of the lab, you will use Paraben's Electronic Evidence Examiner (E3) to verify the MD5 hashes generated by FTK. E3 is a tremendously powerful forensic investigation platform that provides end-to-end processing capabilities for all types of digital evidence. E3 also supports evidence triage, email analysis, smartphone acquisition and analysis, cloud acquisition and analysis, and IoT forensics.

In real-world investigations, the first responder and the forensic analyst are often different people, and sometimes the evidence can be forensically acquired weeks or months before an investigator begins to process it. The first responder may have FTK Imager or another forensic-grade imaging tool on hand for acquiring the evidence from the source, while the forensic analyst may use an entirely different tool for their in-depth investigation. In these situations, or cases involving multiple analysts or investigators, it is important to compare hash codes to ensure the evidence has not been altered in transit.

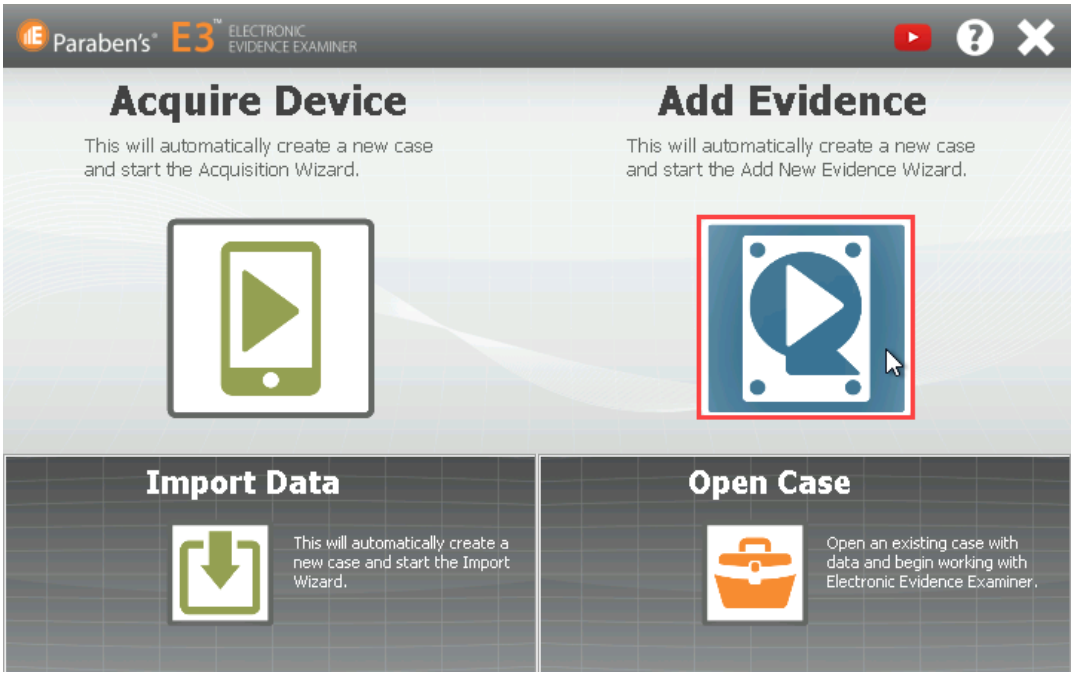
In the next steps, you will acquire the same evidence used in Part 2, generate hash codes, and compare them to the hash codes generated by FTK.

1. On the vWorkstation desktop, **double-click** the **Electronic Evidence Examiner icon** to open the E3 application.

E3 icon

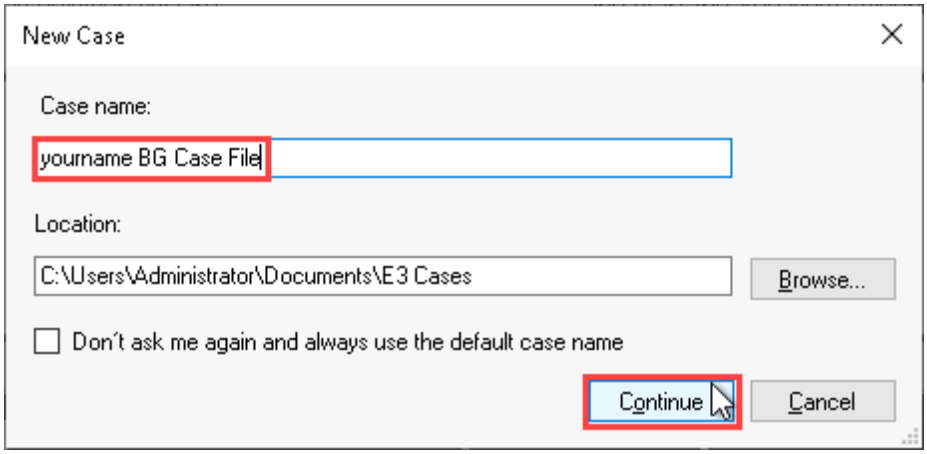
Note: E3 may take several minutes to load. The E3 welcome page opens with shortcuts to the most common activities that forensic investigators will perform within the tool.

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



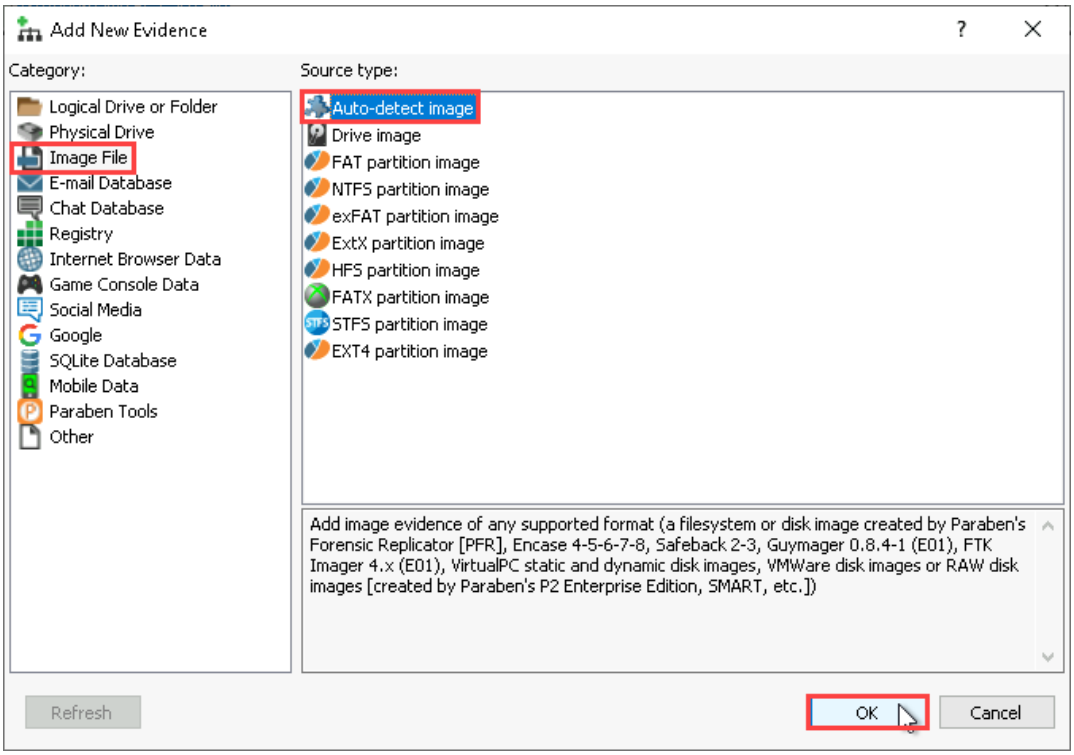
Welcome page - Add Evidence

3. In the New Case dialog box, **type** ***yourname*** **`BG 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.



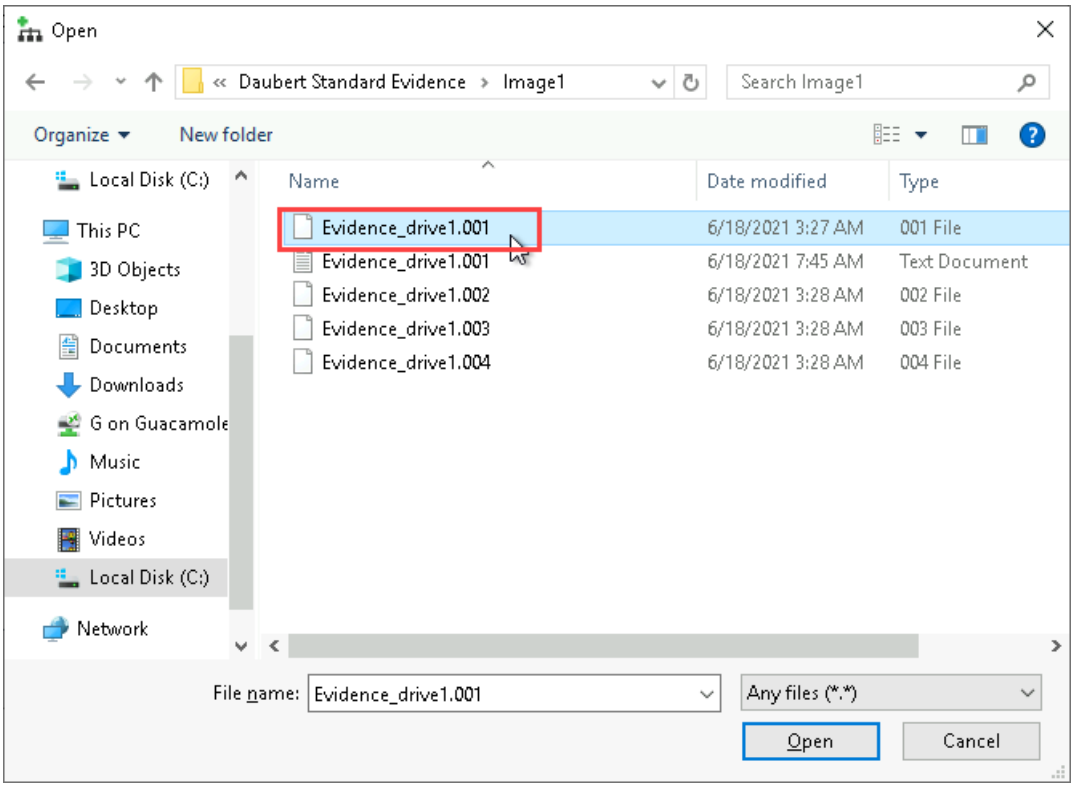
New Case dialog box

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.



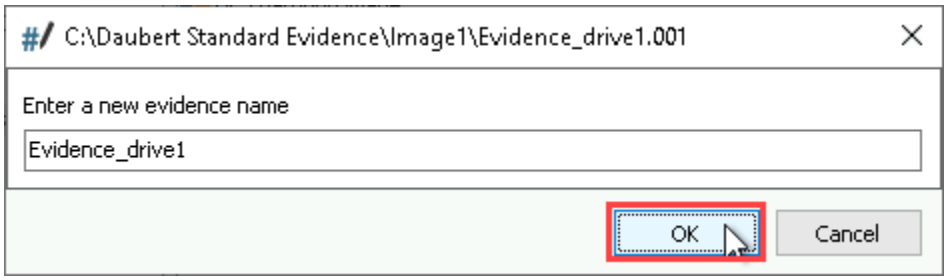
Add New Evidence - Auto-detect image

5. In the Open dialog box, **navigate** to **This PC > Local Disk (C:) > Daubert Standard Evidence > Image1** and **double-click** the first **Evidence_drive1.001 file** to select the digital drive image for this lab.



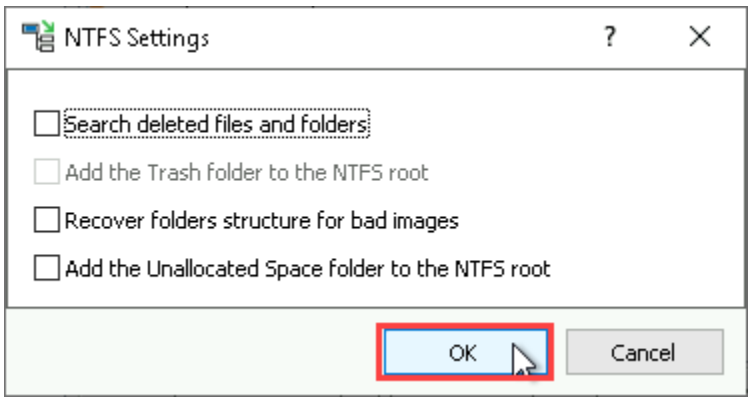
Open dialog box

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.



Evidence name

7. When prompted, **click OK** to close the NTFS Settings dialog box.

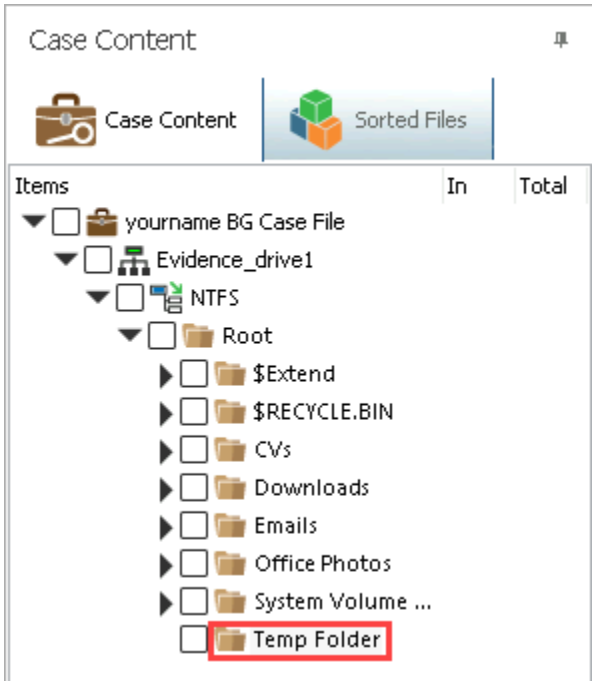


NTFS Settings dialog box

Note: The *yourname* BG 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.

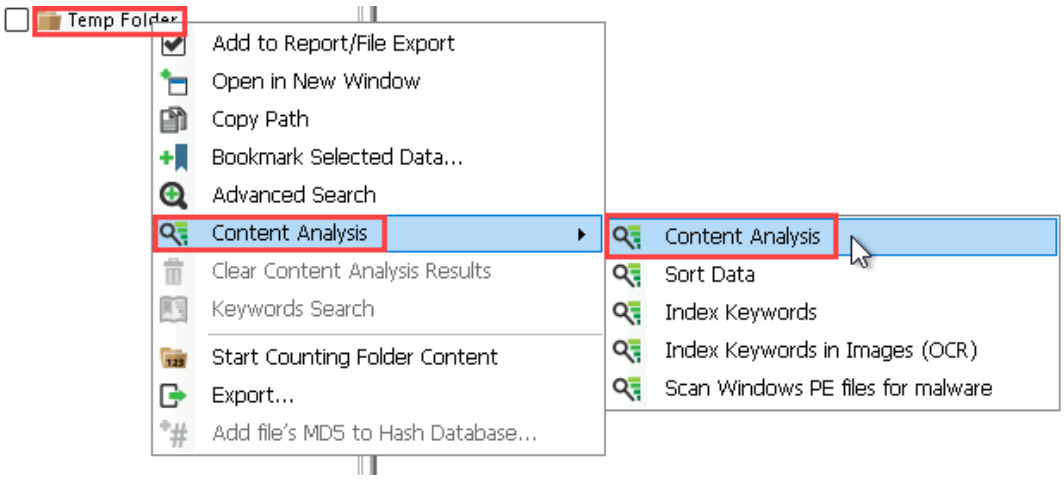
When you select a specific node or grid within the Case Content pane, the contents of the enclosing folder or database will be displayed in the Data Viewer in the center pane. Within the Data Viewer, you can select individual files, folders, and records. Additional information about the currently selected 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* BG Case File > Evidence_drive1 > NTFS > Root > Temp Folder** to display the contents in the center pane.



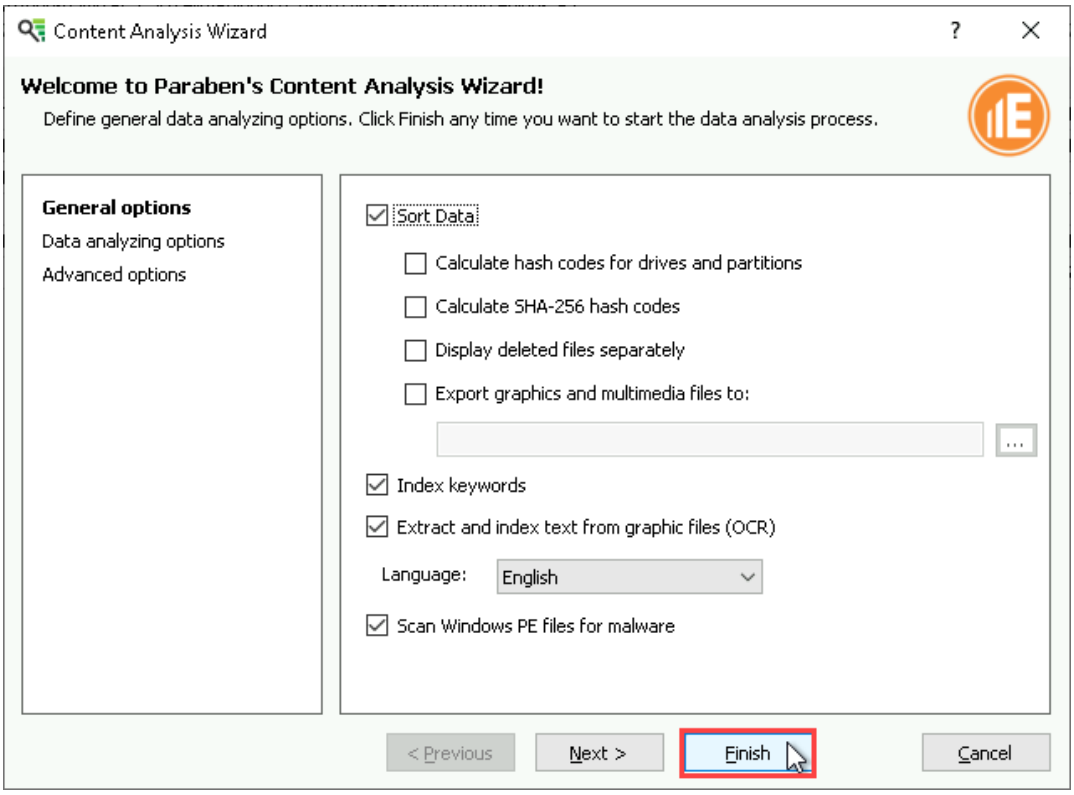
Case Content pane

9. In the Case Content pane, **right-click** the **Temp Folder node** and **select Content Analysis > Content Analysis** from the context menu to open the Content Analysis wizard.



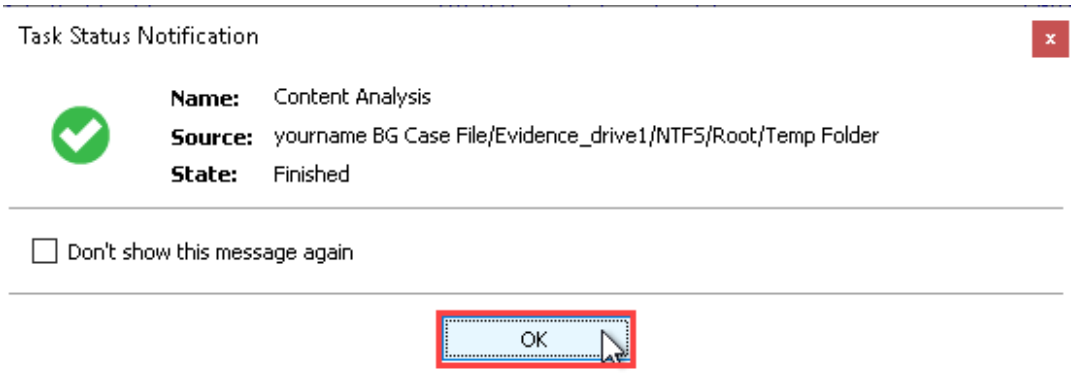
Content Analysis

10. In the Content Analysis wizard, **click Finish** to run the content analyzer with default settings.



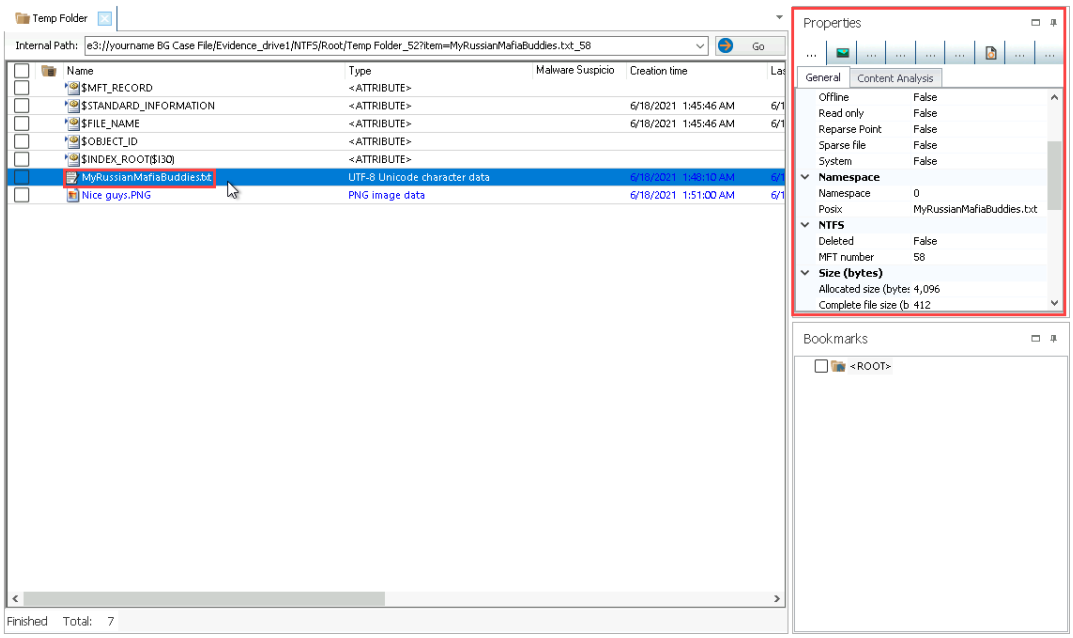
Content Analysis wizard

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



Task Status Notification dialog box

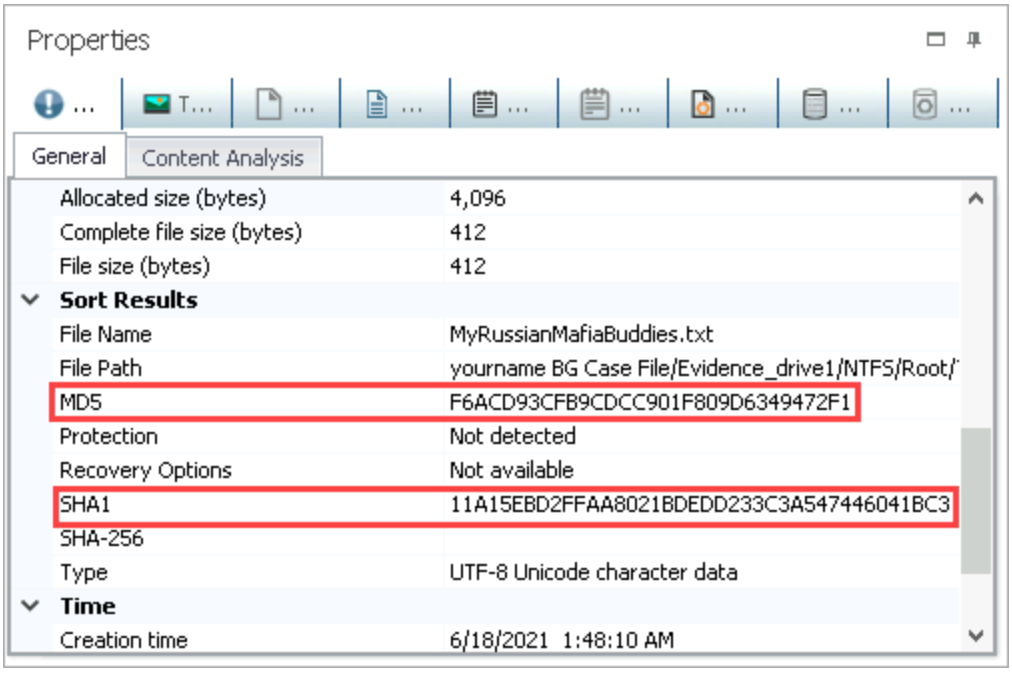
12. In the center pane, **select** the **MyRussianMafiaBuddies.txt file** to display information about the file in the Properties pane.



MyRussianMafiaBuddies.txt properties

13. In the Properties pane, **scroll down** to display the MD5 and SHA1 values.

    If necessary, expand the Properties pane.



MD5 and SHA1 values

14. **Make a screen capture** showing the **MD5 and SHA1 values for the MyRussianMafiaBuddies.txt file**.

15. **Repeat steps 11-12** for the Nice Guys.png file.

16. **Make a screen capture** showing the **MD5 and SHA1 values for the Nice Guys.png file**.

17. **Describe** how the hash values produced by E3 for the incriminating files compare to those produced by FTK. Do they match?

18. **Close** the **E3 window**.

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 explore the suspect's drive image to locate additional evidence. You will also use Autopsy, another popular digital forensics tool, to validate the hash codes created during your preliminary investigation.

Part 1: Extract Evidence Files and Create Hash Codes with FTK Imager

Note: In this part of the lab, you will continue your investigation of Beverly Gates's seized drive image and attempt to identify additional evidence. Your supervisor has reason to believe that Beverly may have exchanged some incriminating emails with her criminal partners and has recommended you search her drive image for email evidence. He has also requested that you demonstrate the efficacy of hash codes by altering a sample evidence file, then adding the altered file back into FTK Imager and exporting new hash codes. In the next steps, you will re-open the drive image in FTK Imager.

1. From the vWorkstation desktop, **launch** the **AccessData FTK Imager application**.

2. **Add** the **Evidence_drive1.001 drive image** as evidence.

3. In the Evidence Tree, **navigate** to **Evidence_drive1.001 > NONAME [NTFS] > root > Emails**.

4. **Identify** a **suspicious email file** in the Emails folder.

   Hint: It's the one that references stardust.

5. **Make a screen capture** showing the **contents of the suspicious email file in the Display pane**.

6. **Export** the **suspicious email file** to the 10001-BPD-CCD folder.

7. **Export** the **File Hash List** for the suspicious email file to the 10001-BPD-CCD folder.

8. **Minimize** the **FTK Imager window**.

9. From the 10001-BPD-CCD folder, **open** the **suspicious email file** in Notepad.

10. In Notepad, **delete** the **body of the suspicious email**, then **close** the file and **save** your changes.

11. **Restore** the **FTK Imager window**.

12. **Add** the **edited suspicious email file** as evidence.

    Hint: You can add the entire 10001-BPD-CCD folder as evidence.

13. **Export the File Hash List** for the edited suspicious email file to the 10001-BPD-CCD folder.

14. **Close** the **FTK Imager window**.

15. From the 10001-BPD-CCD folder, **open** the **csv files** for both the original and edited suspicious email file in Note pad, then **arrange** the windows side by side.

16. **Make a screen capture** showing the **two hash values for the suspicious email file**.

Note: The hash values for the two files should not match, demonstrating that changes made to an evidence file will result in a different hash code.

17. **Close** any **open windows**.

Part 2: Verify Hash Codes with Autopsy

Note: In this part of the lab, you will use Autopsy, another popular digital forensics tool. Autopsy is a simplified graphical front-end for The Sleuth Kit, an open-source collection of Windows and Unix-based command line utilities designed to extract and analyze data from drive images. Because of their plug-in architecture, Autopsy and The Sleuth Kit can be augmented with community-developed or custom-built modules to enhance their out-of-box functionality.

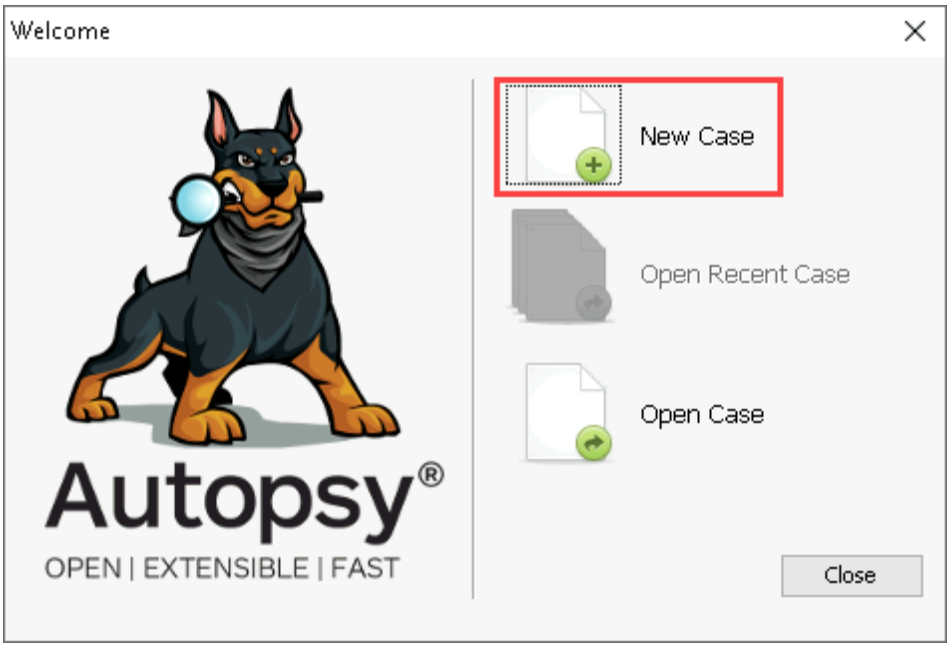
In the next steps, you will use Autopsy to validate the hash code for the suspicious email file you

extracted from the suspect's drive image in Part 1.

1. From the vWorkstation desktop, **launch** the **Autopsy application**.

Autopsy icon

2. In the Autopsy Welcome window, **click** the **New Case option** to create a new case file.



Welcome window

3. On the Case Information page, **enter** `BG_evidence` as the case name and **select** the **Documents folder** as the Base Directory, then **click Next** to continue.

4. On the Optional Information page, **click Finish** to save your case file and open the Add Data Source Wizard.

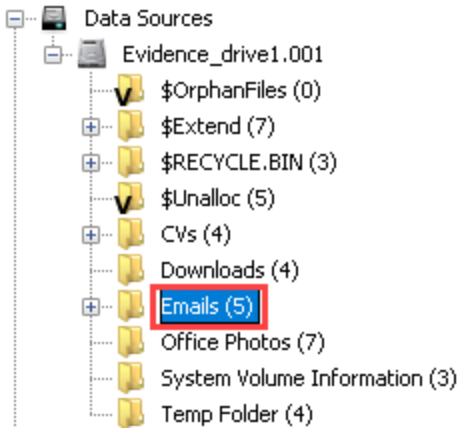
5. On the Select Type of Data Source To Add page, **click Next** to accept the default (Disk Image or VM File) and continue.

6. On the Select Data Source page, **click** the **Browse button**, then **navigate** to **This PC > Local Disk (C:) > Daubert Standard Evidence > Image1** and **double-click** the **Evidence_drive1.001 file**, then **click Next** to continue.

7. On the Configure Ingest Modules page, **click Next** to accept the default settings and continue.

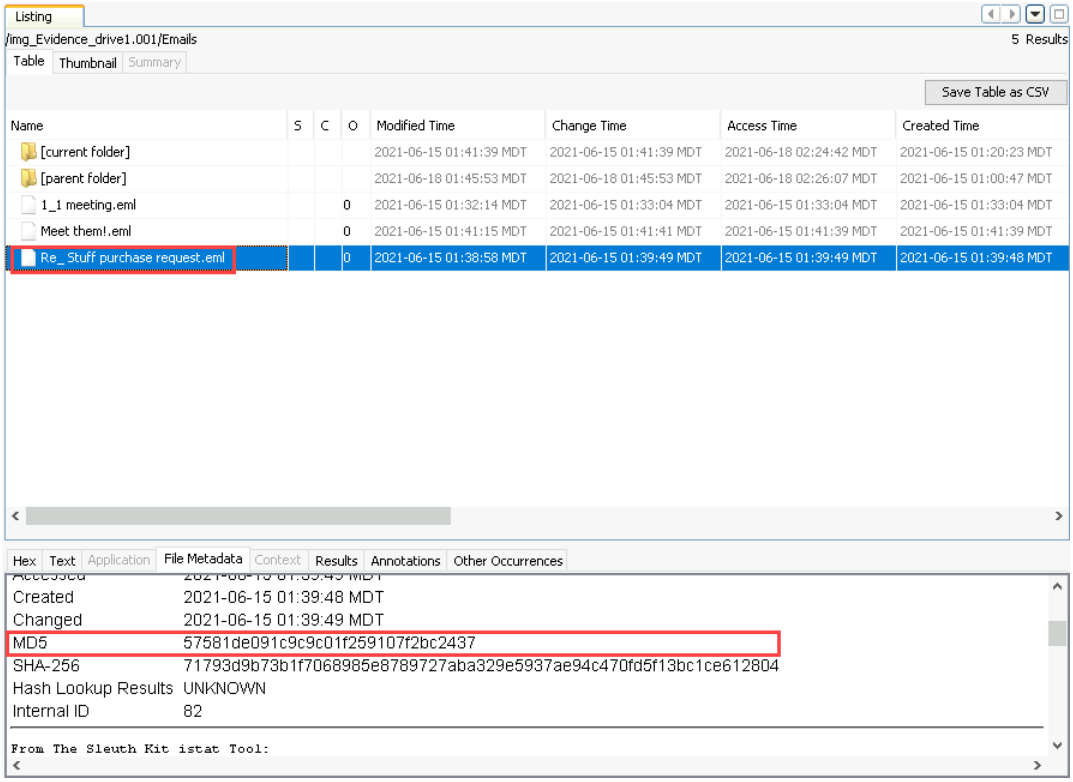
8. On the Add Data Source page, **click Finish** to continue.

9. In the Tree Viewer, **navigate** to **Data Sources > Evidence_drive1.001 > Emails** to display the contents in the Result Viewer.



Tree Viewer

10. In the Result Viewer, **select** the **Re_Stuff purchase request.eml file**, then **click** the **File Metadata tab** and **scroll down** to display the MD5 hash value.



Result Viewer

11. **Make a screen capture** showing the **MD5 field in the Result Viewer**.

12. **Describe** how the hash value produced by Autopsy compares to the values produced by FTK Imager for the two .eml files.

13. **Close** the **Autopsy window**.

Part 3: Verify Hash Codes with E3

Note: In this part of the lab, you will use Paraben's E3 to further validate the hash codes created for the suspicious email file using the other two digital forensics tools.

1. From the vWorkstation desktop, **launch** the **E3 application**.

2. From the Welcome screen, **open** the ***yourname* BG Case File** that you created in Section 1.

3. From the Case Content tree, **navigate** to the **Emails folder** and **locate** the **suspicious email file** that you identified in FTK Imager and Autopsy.

4. **Right-click** the **suspicious email file** and use the **Export function** to save the file to the 10001-BPD-CCD folder.

5. **Close** the **E3 window**.

6. From the 10001-BPD-CCD folder, **open** the **MD5 file** for the suspicious email file in Notepad.

7. **Make a screen capture** showing the **MD5 value produced by E3**.

8. **Describe** how the hash value produced by E3 compares to the values produced by FTK Imager for the two .eml files and the value produced by Autopsy.

9. **Close** the **Notepad 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: Verify Hash Codes on the Command Line

In this lab, you assumed the role of a forensic specialist investigating evidence associated with a drug trafficking case. While conducting your investigation with different digital forensics tools, you learned that certain FTK Imager functions can also be run from the command line. In the interest of expanding your own forensic toolkit, you have decided to learn more about this approach.

Using the Internet, research the command line version of FTK Imager and identify the command used to generate SHA1 and MD5 hashes for a specific file. Next, launch a Command Prompt window and navigate to the FTK Imager CMD tool (C:\Program Files\AccessData\FTK Imager\cmd\). Use the command you identified in your research to verify the SHA1 and MD5 hashes of the Evidence_drive1.001 file used in this lab.

Make a screen capture showing the **hash values for the Evidence_drive1.001 file**.

Part 2: Locate Additional Evidence

New information has emerged, suggesting that there may be additional evidence located on the seized drive image. Using any of the three forensic programs provided in this lab (FTK Imager, Autopsy, or E3), identify the initial location and names of the following files in the Evidence_drive2 disk image (located within the Daubert Standard Evidence / Image2 folder):

- $R354ELH.xlsx
- $RBQEOTL.doc
- $RX3177E.pdf

Define the original file names and file paths for each of the three files.

Note: This concludes Section 3 of the lab.