

Introduction

Of the many services we use over the Internet, email is among the most common. In the years since Internet usage began gaining widespread popularity in the 1990s, email has become a primary means of communication for companies, government, and individuals. Consequently, email is one of the most common sources of evidence that a forensic investigator can examine during an investigation.

In its simplest form, email forensics consists of analyzing the source and content of an email message, which enables an investigator to identify the sender, receivers, date, and time. As a source of forensic evidence, email has the power to document a suspect's activities with immense detail. Proper email analysis can prove guilt, innocence, or at least that something happened.

However, email is not the only way that people communicate electronically. For personal usage, applications such as Facebook Messenger, WhatsApp, and Discord are immensely popular services that allow individuals to exchange messages over the Internet. Meanwhile, in professional environments, applications such as Slack and Microsoft Teams have gained traction as complements and even replacements for email. As with email, digital artifacts left by instant messaging (IM) and chat applications can hold immense forensic value. This is particularly true if it is possible to recover entire databases containing complete conversation transcripts.

In this lab, you will perform forensic analysis on a variety of email and IM services, including Outlook, Thunderbird, Slack, and Discord. You will analyze email headers and search for forensic evidence using Paraben's E3.

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 perform basic email header analysis.

2. In the second part of the lab, you will search for forensic evidence in email using targeted search techniques.

3. In the third part of the lab, you will search for forensic evidence in a chat application database.

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

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 new evidence in different email clients and chat applications.

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. Navigate the structure of common email client databases, including Outlook and Thunderbird.
2. Read and understand the contents of email headers.
3. Use E3's Content Analysis function to sort email attachments.
4. Use E3's Advanced Search function to apply custom search filters.
5. Navigate the structure of common chat application databases, including Slack and Discord.

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.

- 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:

- Happy Reminder email in the Text Viewer and Timestamp in the Properties pane
- IP address of the sender
- List of files in the Graphics category
- Email that references the Big Boss
- Members of the IntricateSolutions workspace
- Channels in the IntricateSolutions workspace

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

- Conversation contents

2. Any additional information as directed by the lab:

- None

SECTION 2

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

- Thunderbird Inbox
- Email from Leo Deforest
- Pills evidence and Beverly Gates corresponding as Natasha "Red" Maximoff
- Beverly's Discord friend list
- Lena Goodwin conversation

2. Any additional information as directed by the lab:

- Document the sender's email address, mail server name, and mail server IP address in the Well, Well, Well email header

SECTION 3

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

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

- Email thread returned in the search results
- Additional evidence within the Discord database

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: Analyze Email Headers

Note: In this part of the lab, you will perform some basic email header analysis using Paraben's E3 and a drive image. The standard format for email structure, including header fields and the message body, are defined in RFC 822, RFC 2822, and RFC 5322. Within an email, header fields serve as the email's delivery metadata, describing the email's source, destination, and the path that it took between the two. For forensic investigators, any email investigation should include a thorough examination of the email headers.

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

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07



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.

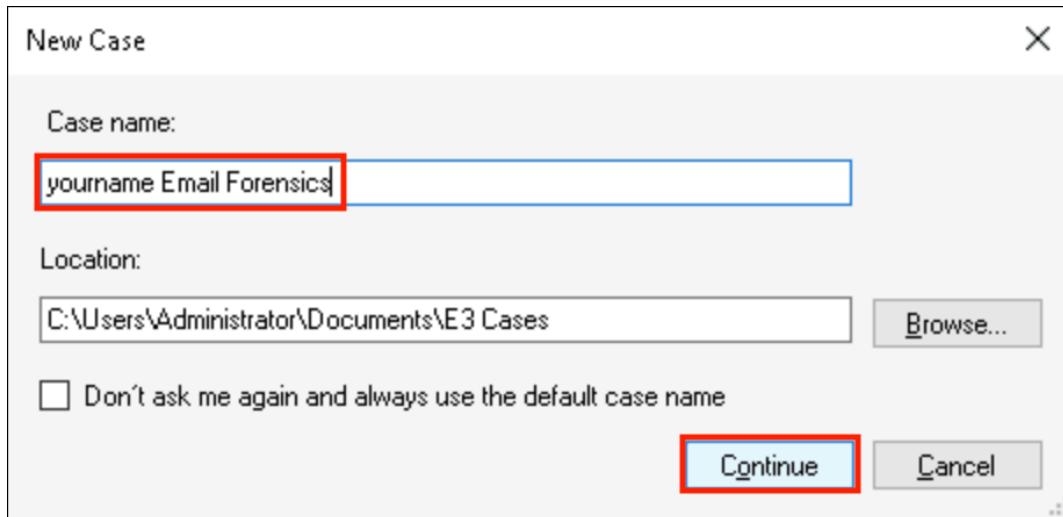


Welcome page - Add Evidence

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

3. In the New Case dialog box, type **yourname Email Forensics** 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.

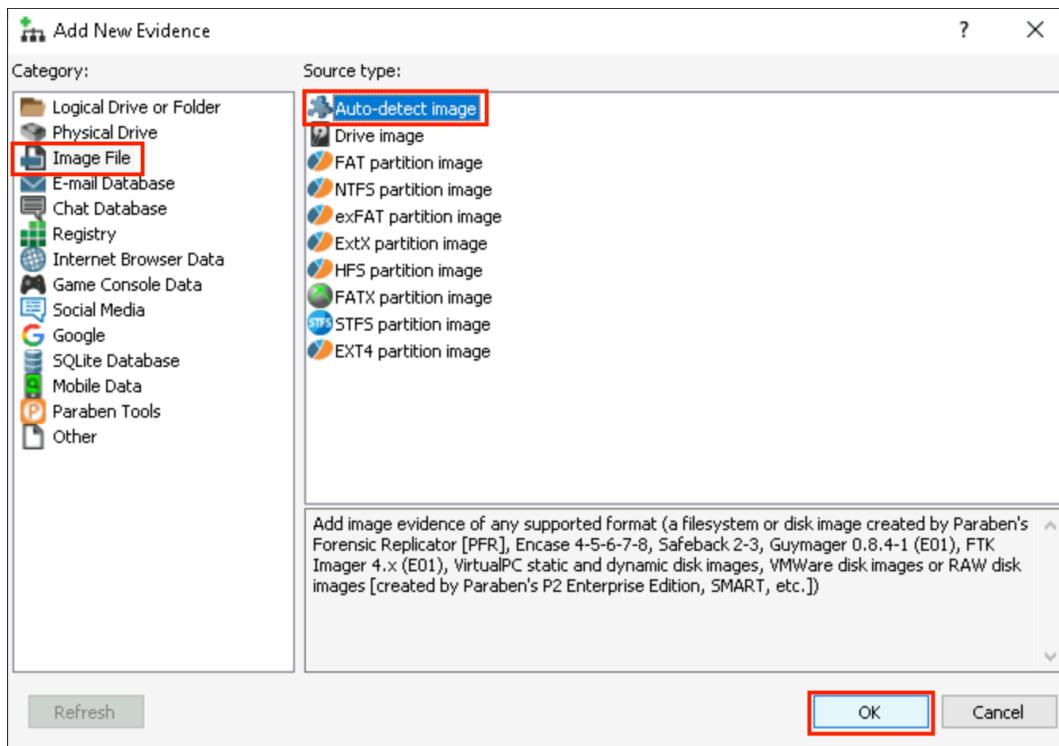


New Case dialog box

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.

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

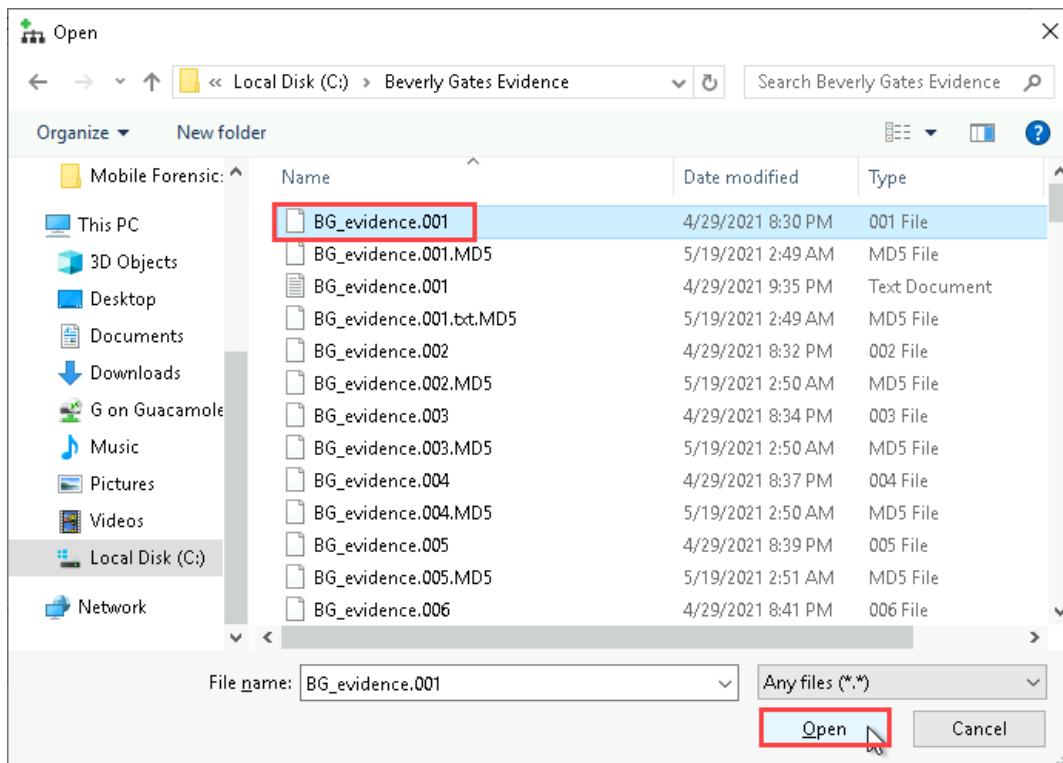


Add New Evidence - Auto-detect image

5. In the Open dialog box, **navigate to C:\Beverly Gates Evidence and select the first BG_evidence.001 file**, then **click Open** to import the digital drive image for this lab.

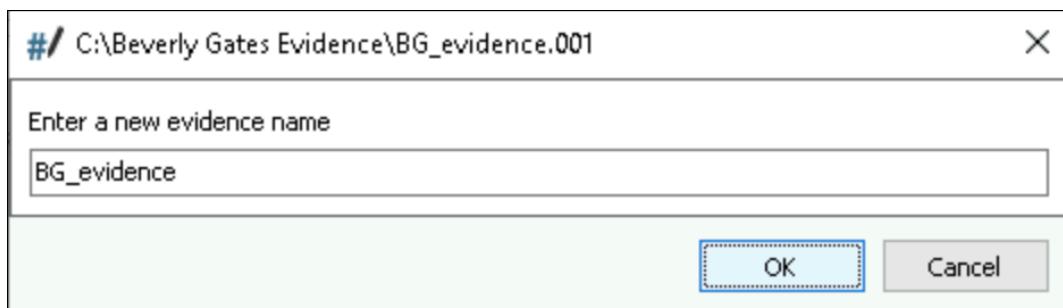
Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07



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

Note: The *yourname* Email Forensics 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

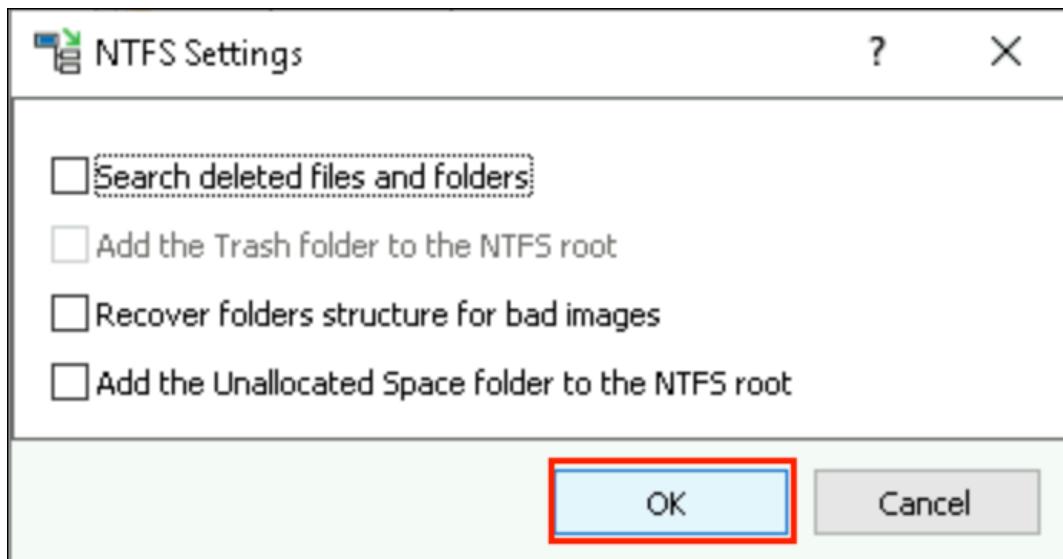
Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

Content pane's tree-view structure, you can access case nodes, evidence nodes, evidence type nodes, folder nodes, and data gridsstreams. 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 console. 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.

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



NTFS Settings dialog box

- In the Case Content pane, **navigate to *yourname* Email Forensics / BG_evidence / NTFS**, then **expand the Data Triage node** to display the Data Triage categories.

Case Content



Case Content



Sorted Files



Items

In

Total

▼	□	💼	yourname Email Forensics		
▼	□	💻	BG_evidence		
▼	□	📁	NTFS		
▶	□	📁	Root		
▼	□	🔍	Data Triage		
▶	□	✉️	E-mail Databases	3	5
▶	□	🌐	Internet Browse...	2	2
▶	□	📁	My Documents ...	1	1
▶	□	⬇️	Downloads	1	1
▶	□	📸	Pictures	1	1
▶	□	⌚	Recently Used F...	30	33
▶	□	▶	Media Data	1	1
▶	□	🔊	Windows Searc...	1	1
▶	□	☁️	Cloud Storages	2	2
▶	□	GridLayout	Windows Apps ...	3	3
▶	□	📅	Windows 10 Act...	1	1
▶	□	📄	Link Files	1	1
▶	□	📅	Jump List Files	2	2
▶	□	🔑	Authentication ...	1	1
▶	□	💻	System Data Files	2	2
▶	□	🌐	Registry		

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

Data Triage

Note: The Data Triage function in E3 allows you to quickly view potentially high-value evidence, such as email databases, recently used files, and parsed registry data.

9. In the Case Content pane, **select the E-mail Databases category** to display all email databases detected on the drive image in the Data Viewer pane.

Name	Physical Path	User Name	Status	Size [bytes]
bev.gates@outlook.com - bev.gates@outlook.com.ost	BG_evidence\NTFS\Root\use BEVERLY GATES r\beverly gates\appdata\local\micros ost\outlook\bev.gates@outlook.com.ost	BEVERLY GATES	Available	16,818,176
bev.gates@outlook.com.ost	BG_evidence\NTFS\Root\use BEVERLY GATES r\beverly gates\appdata\local\micros ost\outlook\bev.gates@outlook.com.ost	BEVERLY GATES	Moved/Deleted	
bevi.gates@outlook.com.ost	BG_evidence\NTFS\Root\use BEVERLY GATES r\beverly gates\appdata\local\micros ost\outlook\bev.gates@outlook.com.ost	BEVERLY GATES	Moved/Deleted	
dfb7v5vd.default-release	BG_evidence\NTFS\Root\use BEVERLY GATES r\beverly gates\appdata\roaming\thu nderbird\profile\dfb7v5vd. default-release	BEVERLY GATES	Available	
ltsphysz.default	BG_evidence\NTFS\Root\use BEVERLY GATES r\beverly gates\appdata\roaming\thu nderbird\profile\ltsphysz.d efault	BEVERLY GATES	Available	

E-mail Databases

10. In the Data Viewer pane, **double-click** the **bev.gates@outlook.com – bev.gates@outlook.com.ost** database to open it.

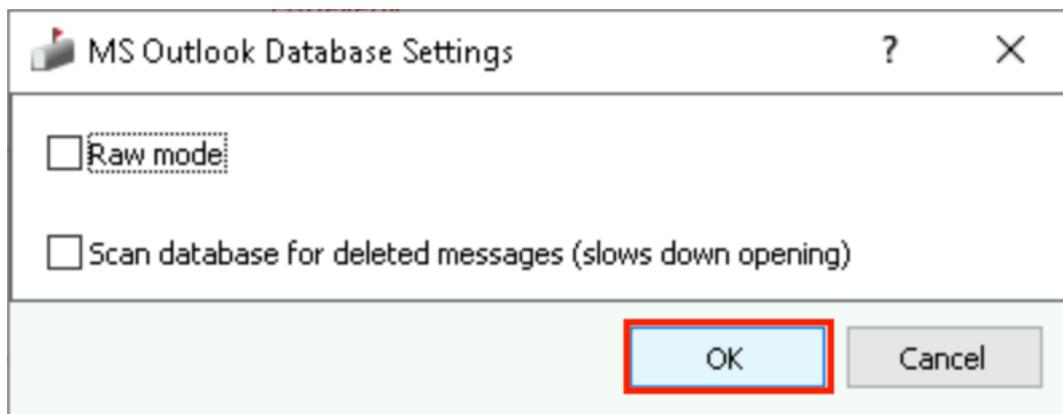
Name	Physical Path	User Name	Status	Size [bytes]
bev.gates@outlook.com - bev.gates@outlook.com.ost	BG_evidence\NTFS\Root\use BEVERLY GATES r\beverly gates\appdata\local\micros ost\outlook\bev.gates@outlook.com.ost	BEVERLY GATES	Available	16,818,176
bev.gates@outlook.com.ost	BG_evidence\NTFS\Root\use BEVERLY GATES r\beverly gates\appdata\local\micros ost\outlook\bev.gates@outlook.com.ost	BEVERLY GATES	Moved/Deleted	

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

Bev.gates@outlook.com database

- When prompted, **click OK** to close the MS Outlook Database Settings dialog box without making any changes.



MS Outlook Database Settings dialog box

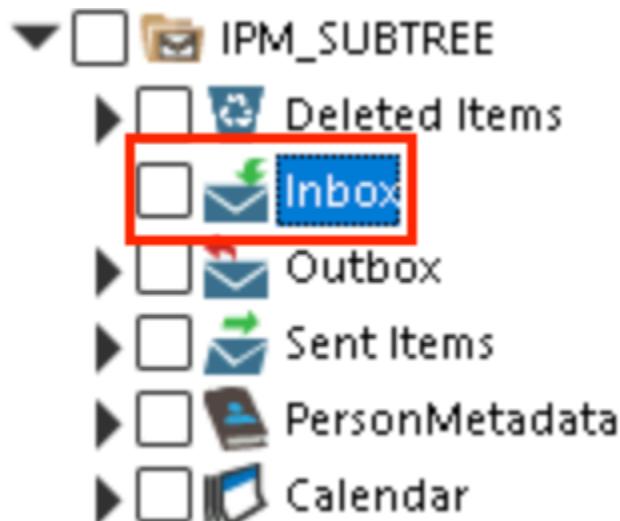
- In the Case Content pane, **navigate to bev.gates@outlook.com\Outlook Offline Storage\Root - Mailbox**, then **expand the IPM_SUBTREE folder node** to display the structure of the email database.

IPM_SUBTREE folder

Note: IPM stands for "InterPersonal Message." Within an Outlook email database, the IPM Subtree is used to store all messages between human recipients (hence, *interpersonal*). From here, you can access the Inbox, Outbox, Sent Items, and Deleted Items. Within Microsoft Outlook Office, the IPM Subtree also contains folders for Calendar, Contacts, Tasks, Notes, and more.

In a real-world situation, you might need to review all the components of the email database, but in this lab, you will narrow your investigation to the Inbox.

13. In the Case Content pane, **select the **Inbox** folder node** to display the contents in the Data Viewer.



Inbox

14. In the Data Viewer pane, **select the **email** from *Karen Jef* with the subject *Re: Happy Reminder* to display its contents in the E-mail Data pane.**

You may need to adjust the pane sizes to view the information in the E-mail Data pane.

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

The screenshot shows the E3 Data Triage interface. At the top, there's a navigation bar with 'Inbox' and other icons. Below it is a search bar with the internal path: 'e3:///yourusername Email Forensics/BG_evidence/NTFS/Data_Triage/E-mail Databases/bev.gates@outlook.com - bev.gates@outlook.com.' A 'Go' button is next to the search bar. The main area is a grid of email items:

	Subject	From	To	Created
1	Re: Team Evaluation	"Mr.Harris Malone" <mr.ha	Beverly Gates <bev.gates@	4/27/2021 7:1
2	Re: Team Evaluation	"Mr.Harris Malone" <mr.ha	Beverly Gates <bev.gates@	4/27/2021 7:1
3	Re: Intricate Solution Job Offer	"Vicky Reed" <viks.reeds@	Beverly Gates <bev.gates@	4/27/2021 7:4
4	Re: Intricate Solution Job Offer	"Leo Deforest" <leo.defore	Beverly Gates <bev.gates@	4/27/2021 8:1
5	Re: Cool CVs for hot vacancies	"Karen Jef" <karen.jef@lntric	Beverly Gates <bev.gates@	4/28/2021 6:4
6	Re: Happy Reminder	"Leo Deforest" <leo.defore	Beverly Gates <bev.gates@	4/28/2021 7:C
7	Re: Happy Reminder	"Mr.Harris Malone" <mr.ha	Beverly Gates <bev.gates@	4/28/2021 7:1
8	Re: Happy Reminder	"Mr.Harris Malone" <mr.ha	Beverly Gates <bev.gates@	4/28/2021 7:2
9	Re: Happy Reminder	"Karen Jef" <karen.jef@lntric	Beverly Gates <bev.gates@	4/28/2021 7:3
10	Re: 1:1 meeting	"Daniel Dallas" <ddan2042	Beverly Gates <bev.gates@	4/28/2021 7:3

Below the grid, it says 'Finished Total: 17'. The bottom part of the interface is the 'E-mail Data' pane, which shows the selected email's details:

Re: Happy Reminder
"Karen Jef" <karen.jef@lntric365.onmicrosoft.com> on behalf of "Karen Jef"
To: Beverly Gates <bev.gates@outlook.com>

Minions! 🎉
We should select it as the theme for the next party 😊 Or make it a Hawaiian one 🏝
--Karen

At the bottom of the pane are buttons for RFC Header, Text, RTF, HTML, Raw HTML, and Attachments.

Re: Happy Reminder

Note: When you select an individual email in an email database, E3 will display the file in different viewers in the E-mail Data pane, including RFC Header, Text, RTF, Raw HTML, and Attachments.

15. Review the contents of the email.

Note: Recall that the setting for this lab is an investigation into Beverly Gates for suspected drug trafficking. While the content of the email thread seems to indicate some of the Intricate Solutions employees may be partying on the clock, it does not provide any obvious evidence of illegal activity.

16. In the Properties pane, locate the timestamps for this email.

Properties

General Content Analysis

Additional Info

Internet Message ID <PR2PR09MB313255059CE>
Message Class IPM.Note
Message Size (bytes) 135,438

Dates

Creation Date 4/28/2021 7:32:41 AM
Received Date 4/28/2021 7:32:41 AM
Sent Date 4/28/2021 7:32:39 AM

Message Flags

Deleted Undefined
Encrypted Undefined
Has Attachments Yes
Importance Normal
Modified Undefined
Priority Normal
Read Yes

Recipients

To Beverly Gates <bev.gates@Intricate365.oni>

Represent Sender

Email karen.jef@Intricate365.oni
Name Karen Jef

Sender

Properties pane

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

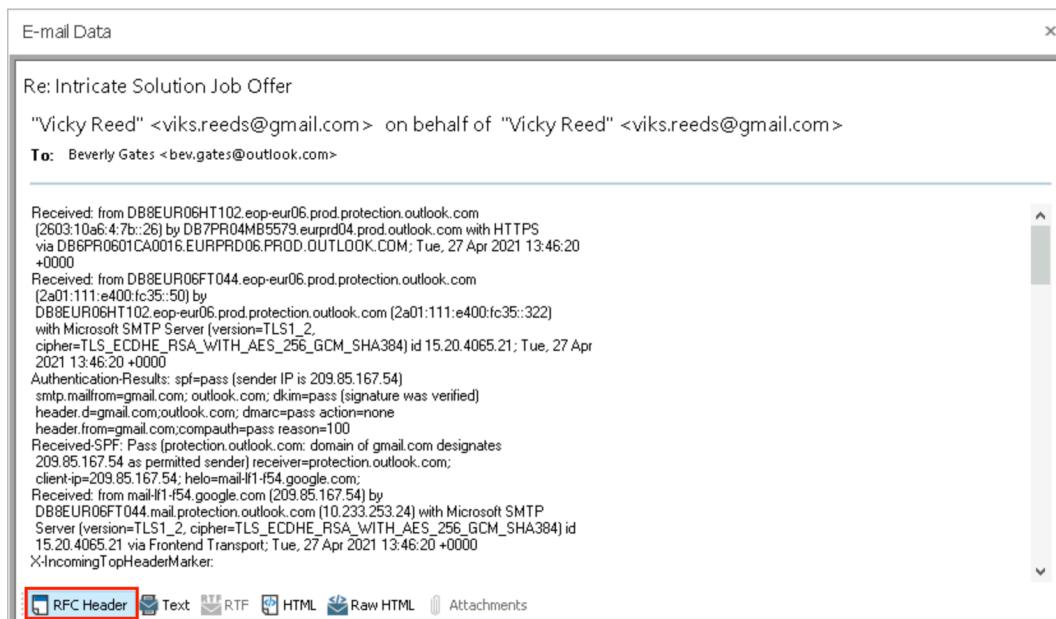
Note: The Properties pane displays basic information about the currently selected email, including size, times/dates, flags, recipients, and the sender.

17. Make a screen capture showing the Happy Reminder email in the Text Viewer and Timestamp in the Properties pane.

18. In the Data Viewer pane, select the email from Vicky Reed with the subject *Re: Intricate Solution Job Offer* to display its contents in the E-mail Data pane.

19. Review the contents of the email in the Text viewer.

20. In the E-mail Data pane, click the **RFC Header tab** to view the email headers.



RFC Header

Note: RFC Header refers to the RFC 822, RFC 2822, and RFC 5322 standards that define a standard email format consisting of header fields and the message body. Email headers contain information associated with the sender, the recipient, the email's route to the inbox, as well as different authentication details.

Every e-mail, regardless of the software that generated it, follows this standard format. The header keeps a record of the message's journey as it travels through the communications network. As the

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

message is routed through one or more mail servers, each server adds its own information to the message header, providing an audit trail of every machine through which the e-mail has passed. This information can be immensely valuable to a forensic investigator. For example, in cases of email spoofing, the email header may contain headers that provide the true sender and originating IP address for the email. Using the IP addresses, you may even be able to determine a geographical location for the sender of the email message.

21. Review the **email header** and locate the IP address of the sender.

Once located, **select** the IP address to highlight it.

22. Make a screen capture showing the **IP address of the sender**.

Part 2: Search for Evidence in an Outlook Database

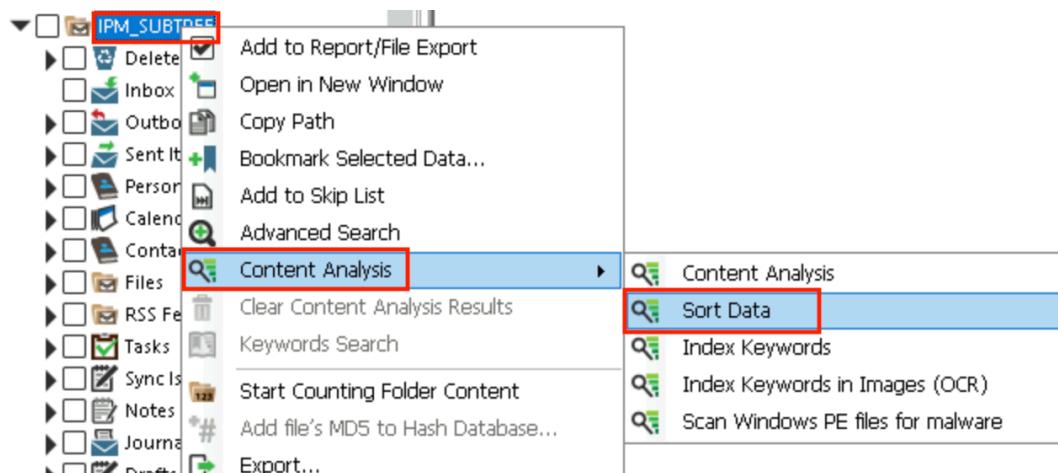
Note: In this part of the lab, you will use E3's Sort Data and Search functions to continue your search for incriminating evidence in Beverly Gates's Outlook database. Due to the volume of emails that most email users send and receive each day in both personal and professional capacities, combing through individual emails one by one is rarely a viable strategy for a forensic investigator. Fortunately, dedicated forensics tools like E3 offer advanced sort and search functionalities to automatically parse the contents of email databases and empower an investigator to quickly identify relevant conversations and files.

In the next steps, you will use E3's Content Analysis engine to identify and sort any attachment files stored within the IPM_SUBTREE directory.

1. In the Case Content pane, **right-click** the **IPM_SUBTREE folder**, then **select Content Analysis > Sort Data** from the context menu to open the Content Analysis Wizard.

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07



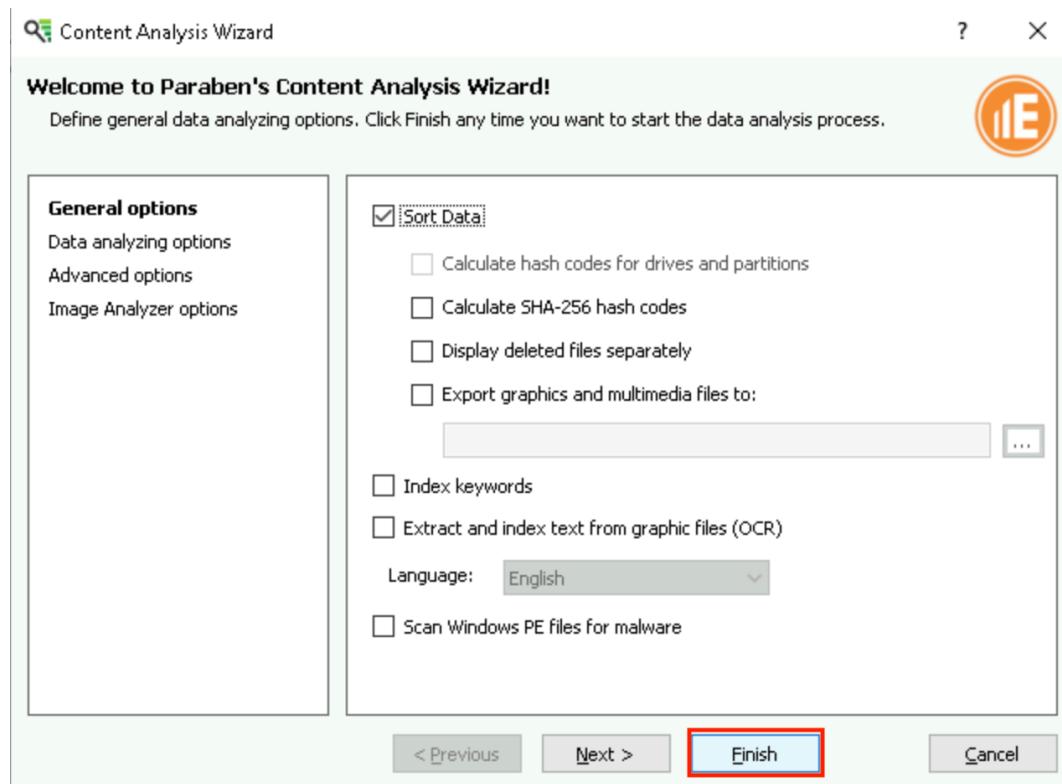
Sort Data

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

This process should take less than 30 seconds to run.

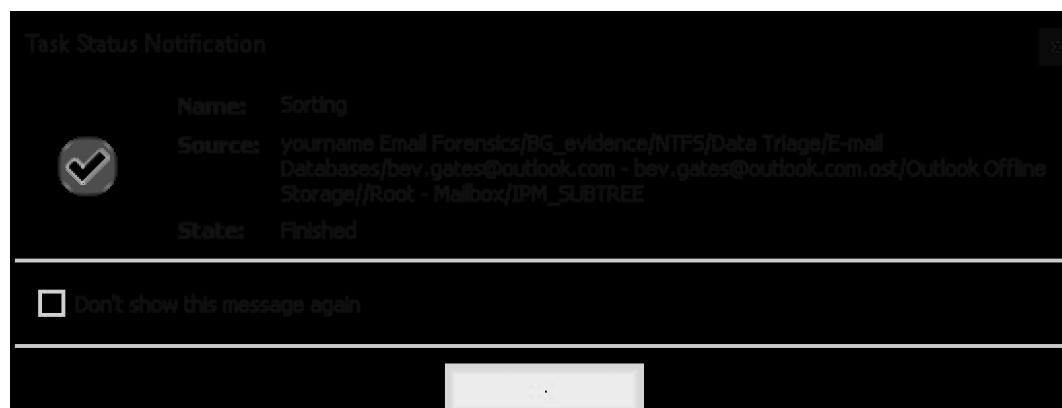
Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07



Content Analysis Wizard

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

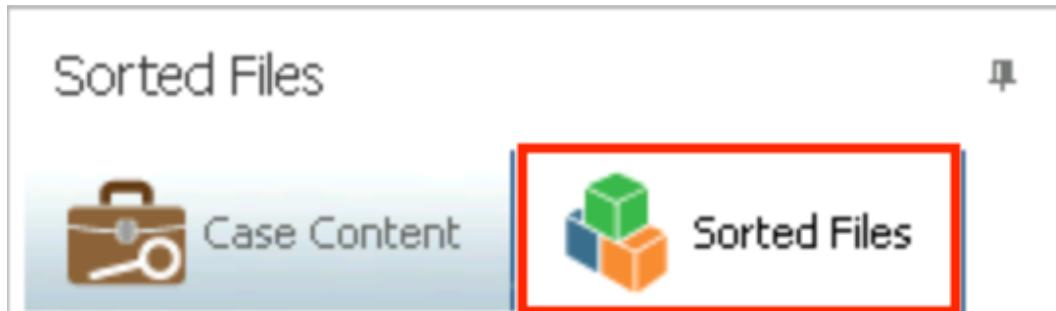


Task Status Notification

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

4. In the Case Content pane, **click the Sorted Files tab** to switch to the Sorted Files view.



Sorted Files tab

5. 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



Case Content



Sorted Files



Sorted Files

- Documents (1)
- Email (0)
- Chats (0)
- Spreadsheets (0)
- Graphics (9)
- Databases (0)
- Executable (0)
- Compressed (0)
- Multimedia (0)
- Text (0)
- XML (0)
- Log Files (0)
- Encrypted (0)
- Financial files (0)
- Game Console Files (0)
- Others (3)
 - ▶ Image Analyzer Results (0)
 - ▶ Deleted Files (0)
 - ▶ Recovered from Unallocated Space (0)

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

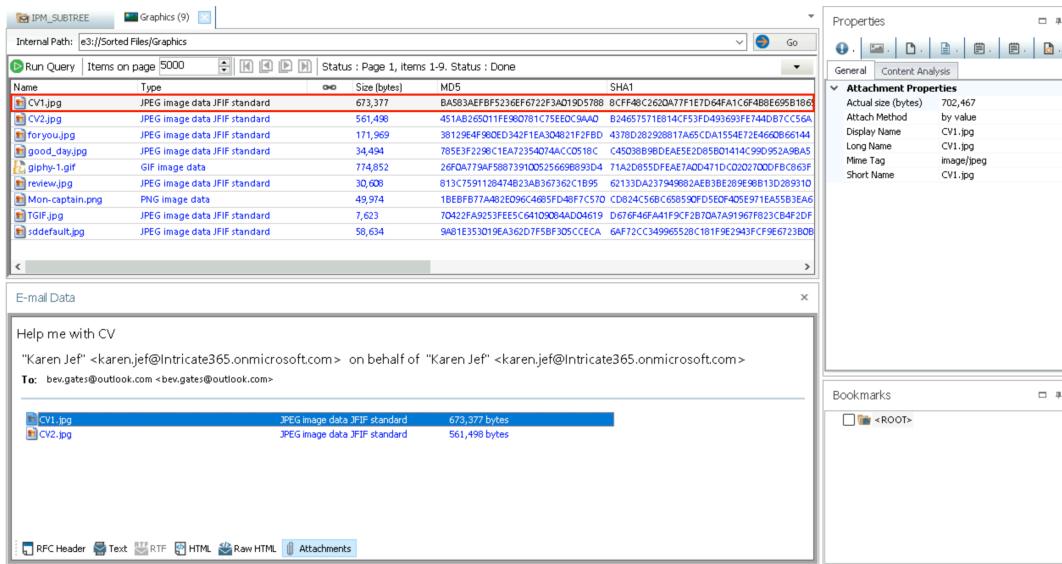
Sorted Files categories

Note: In this context, the Sorted Files view contains all email attachments that E3 identified in the IPM_SUBTREE directory, sorted by file type. For forensic investigators, approaching an email investigation by reviewing the attachments first can help to elevate the most useful or informative evidence. From this view, you can easily identify any interesting files, then review the associated email threads for additional context and evidence.

6. In the Sorted Files pane, **select the Graphics category** to display a list of identified graphics files in the Data Viewer.

7. **Make a screen capture showing the list of files in the Graphics category.**

8. In the Data Viewer, **select the CV1.jpg file** to display the source email in the E-mail Data pane and the file properties in the Properties pane.



The screenshot shows the E3 Data Viewer interface. The top navigation bar includes 'IPM_SUBTREE' and 'Graphics (9)'. The 'Sorted Files' pane displays a list of attachments with columns for Name, Type, Size (bytes), MD5, and SHA1. A red box highlights the 'CV1.jpg' entry. The 'E-mail Data' pane shows an email message from 'Karen Jef' to 'bev.gates@outlook.com'. The 'Properties' pane is open, showing the 'Attachment Properties' tab with details like Actual size (bytes), Attach Method, Display Name, Long Name, Mime Tag, and Short Name. The 'Bookmarks' pane shows a single entry for '<ROOT>'.

Name	Type	Size (bytes)	MD5	SHA1
CV1.jpg	JPEG image data JFIF standard	673,377	BA583A9FB5236F672F23D019D57B8	8CF4FAC2620A77F1E7D04FA1C6F4B8E6959186
CV2.jpg	JPEG image data JFIF standard	561,498	451AB265D11FFEB02781C75EEDC94A0	B24657571B614C5F53FD0493693F7440B7C56A
foryou.jpg	JPEG image data JFIF standard	171,969	3812964F380ED342F1EA304821F2BD	437B282928B17A65CDAA1554E72E4660B66144
good_boy.jpg	JPEG image data JFIF standard	34,494	78513F2298C1EA27354074AC0C516C	C49D39B9D0EAE5E2D6B501414C990952A9BAS
giphy-1.gif	GIF image data	774,852	26F0A773A9F5887391005256698893D4	71A2D855D0EAE7A0D4710C020700FB6363F
review.jpg	JPEG image data JFIF standard	30,608	613C759128474B23AB367362C1B9	62133A237949892AEB3E28E9E8B13D289310
Mon-captain.png	PNG image data	49,974	1BEBF77A4B26096C4685FD48F7C57D	CD624C56B0C695950FD5ED405E971EA5B3E46
tGif.jpg	JPEG image data JFIF standard	7,623	70422FA9253FEE5C64109084AD04619	D676F46FA1F9CF2B70A7A91967F823CB4F2D
sddefault.jpg	JPEG image data JFIF standard	58,634	9481E353019E362D7F5BF305CCECA	6AF72CC349965528C181F9E2943FCF9E6723B0B

CV1.jpg

9. In the E-mail Data pane, **click the HTML button** to display the HTML view of the email that the

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

file was attached to.



HTML view

10. In the right pane, **click the File View tab** to display the contents of the attachment.

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

File View

The screenshot shows a digital resume for Anakin Skywalker. At the top, there's a navigation bar with icons for Home, About, Portfolio, Services, Contact, and a search bar. Below the header, there's a large portrait of Anakin Skywalker.

ANAKIN SKYWALKER
The Chosen One

EDUCATION

Jedi Initiate # Youngling
The Jedi Academy
BB-8000 - BB-8001

• Helped the Jedi's attack and preservation had their place in the Jedi Assembly (Year 2000).

• Drafted in Separatist as a member of the academy (Year 2001).

JEDI EXPERIENCE

Obi-Wan Kenobi's Padawan
The Jedi Academy
BB-8000 - BB-8001

• Prevented Senator Amidala's assassination attempt by capturing Darth Maul.

• Rescued the captured Obi-Wan Kenobi from the Separatist Death Army.

• Maintained his services in secret with others being his master (Darth Vader and Palpatine).

Jedi Knight # Grand Army General
Jedi Order
BB-8000 - BB-8001

• Won over 200 battles in the Clone Wars and became known as the "leader of the Troopers of the Year".

• Appointed by the Chancellor to be his personal representative on the Council.

• Resposed the dark side of Palpatine and converted it to the Jedi Order.

TALENTS

Flying, Tricycling, Engineering, Piloting, Telekinesis, Mind Control, Saber Throw.

LIFE PHILOSOPHY

"Ensuring the most powerful Jedi and bringing order to the Republic."

MOST PROUD OF

- Chosen to destroy the Sith and bring balance to the Force.
- Defeated Darth Tyranus and reward Character Purpose.
- Stopped the Invasion of Naboo.
- Won the Senate five times protecting.
- Built the greatest shield C-090.

FORCE STRENGTHS

- Lightaber Combat: Mastering from the best Jedi Masters over the last 10 years.
- Force Sense: power to feel another being's feelings and other forces.

www.CIO.com

File View

Conducting Forensic Investigations on Email and Chat Logs (4e)

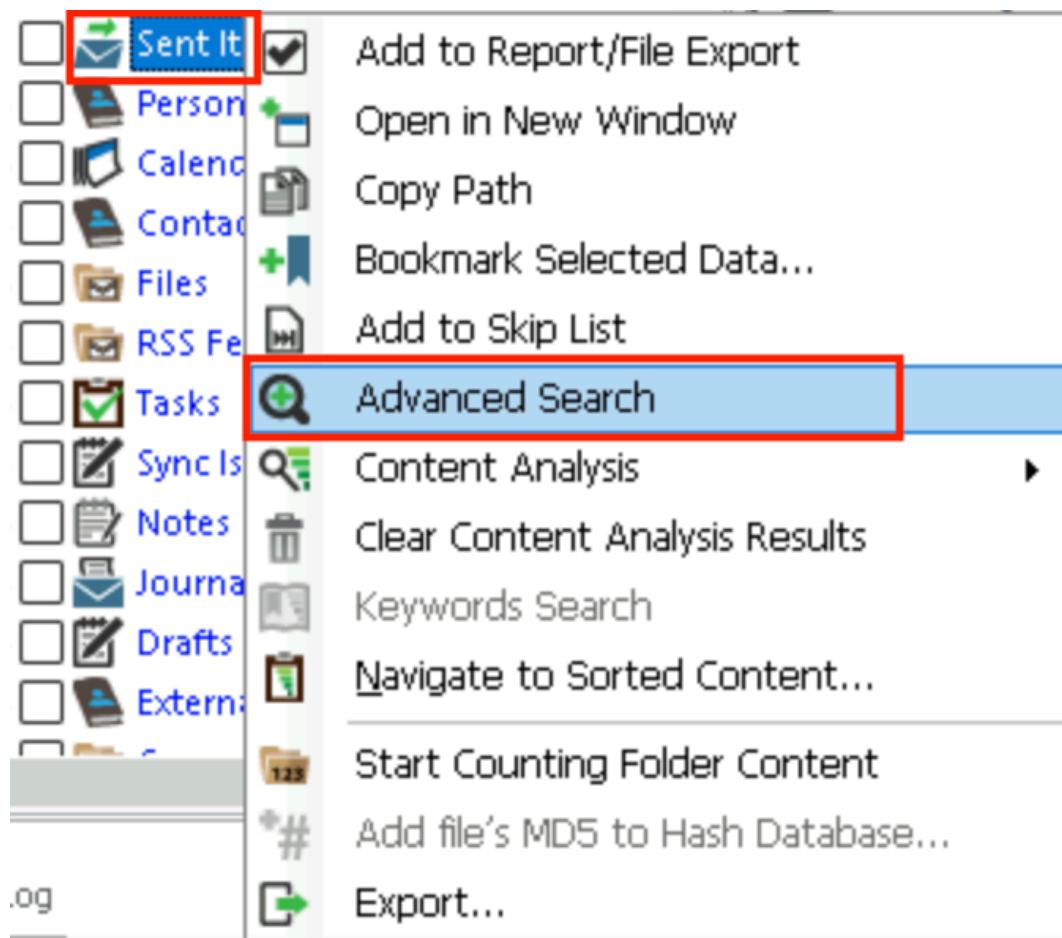
Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

11. **Repeat steps 8-10** to review each file in the Graphics category and the email it was attached to, looking for anything that could be construed as suspicious.

Note: Overall, the contents of the files and emails should appear to be largely normal conversations among office workers. However, you should notice that Alan's – or Mr. Harris Malone's – choice of words and behavior toward Beverly is rather informal for a professional environment, as well as strangely subservient. His conversations with Beverly also reference an urgent deadline that Beverly has set at midnight on April 26, 2021.

Now, Alan (or Harris) may just be an odd duck, but as a forensic investigator in search of patterns and clues in digital evidence, you must often act as a student of human behavior as much as computer behavior. Now, suppose senior leadership has reason to believe that Alan is actually a collaborator in Beverly's drug trafficking operation. In this case, you would be well-advised to further focus your search to emails exchanged between Beverly and Alan on the 26th and 27th of April. To accomplish this, you will use E3's Advanced Search function.

12. In the Case Content pane, **click the Case Content tab** to switch to the Case Content view.
13. In the Case Content pane, **expand the IPM_SUBTREE node**, then **right-click the Sent Items folder** and **select Advanced Search** to open the Advanced Search pane in the center console.

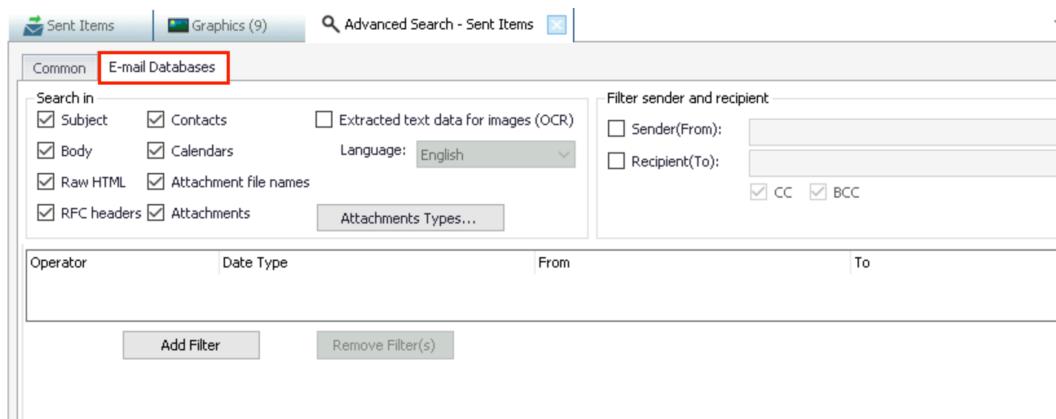


Advanced Search

14. In the Advanced Search pane, **click the E-mail Databases tab** to open the advanced search options for email databases.

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07



E-mail Databases tab

15. In the Advanced Search pane, **select the Sender (From) checkbox**, then **type `bev.gates@outlook.com`** in the Sender (From) field.
16. In the Advanced Search pane, **select the Recipient (To) checkbox**, then **type `mr.harris@Intricate365.onmicrosoft.com`** in the Recipient (To) field.



Sender and Recipient fields

17. In the Advanced Search pane, **click the Add Filter button**, then **change the From and To fields** to the following dates: **4/26/2021 12:00:00 AM** to **4/27/2021 12:00:00 PM**.

Conducting Forensic Investigations on Email and Chat Logs (4e)

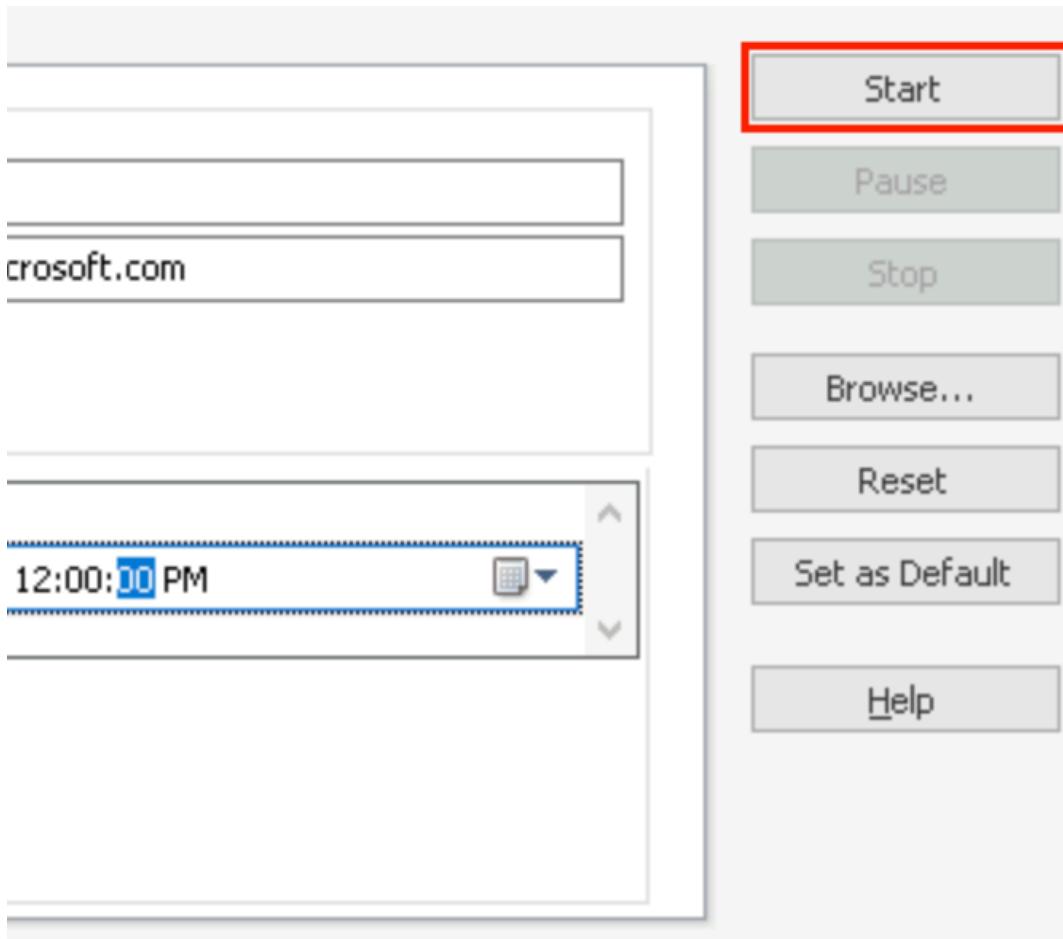
Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

A screenshot of a search interface. At the top, there is a blue header bar with the text "Date Type" and "Any date between:". Below this, there are two input fields: "From" containing "4/21/2021 12:00:00 AM" and "To" containing "4/27/2021 12:00:00 PM". Both of these input fields are highlighted with a red box. Below the input fields are two buttons: "Add Filter" and "Remove Filter(s)".

Add Filter

18. Click the **Start button** to run the search.

You may need to scroll to the right to see the Start button.



Start button

19. When prompted, **click OK** to close the Task Status Notification dialog box.
20. In the Search Results area, **double-click** each **search result** to display the email and its location in a new tab.

Note: As you review the search results, you should find several of the same emails that you encountered while reviewing the Graphics category. However, the results on the Advanced Search in the Sent box should also reveal a final email that Beverly sent to Alan, referencing a Big Boss. Although none of this evidence is explicitly incriminating, it should register as suspicious within the broader context of the investigation.

21. **Make a screen capture** showing the **email that references the Big Boss**.

Part 3: Search for Evidence in a Slack Database

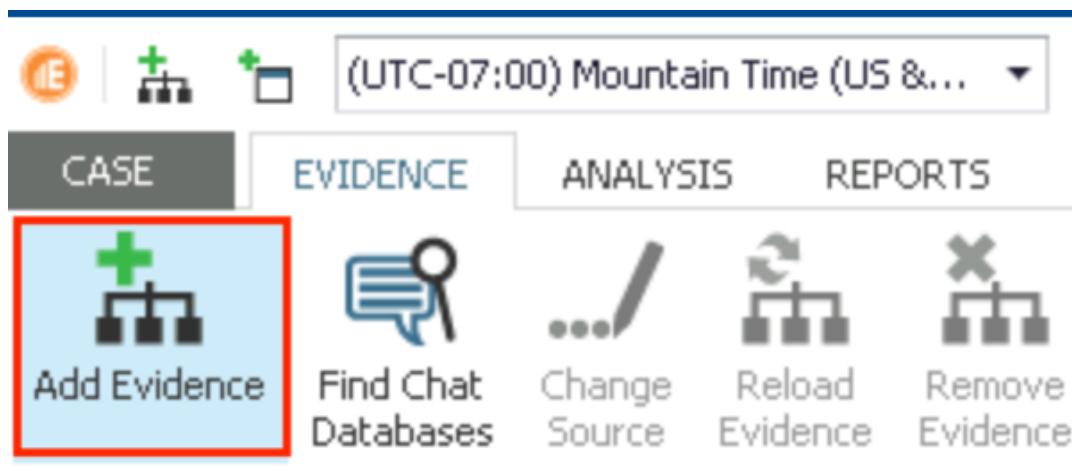
Note: In this part of the lab, you will extend your search to a different type of communications-based evidence – chat databases, specifically a Slack database. Slack is used as the primary instant messaging application at Intricate Solutions, which makes it a potential source of evidence in the investigation of Beverly Gates.

In the next steps, you will import an existing E3 data case that contains a copy of the chat database from Beverly Gates's Slack account.

1. On the E3 toolbar, **click** the **Add Evidence button** to open the Add New Evidence window.

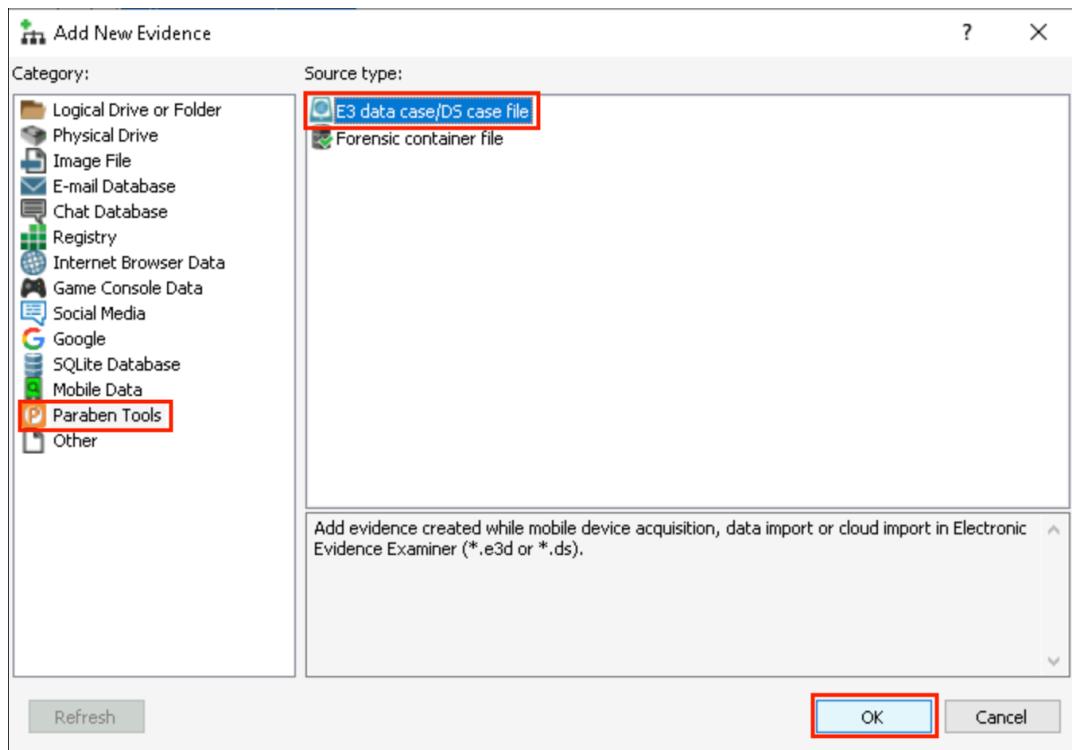
Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07



Add Evidence

2. In the Add New Evidence window, click the **Paraben Tools** category, then select the **E3 data case/DS case file** Source type and click OK to continue.



Add New Evidence

3. In the Open dialog box, **navigate to C:\Email Forensics** and **double-click** the **Beverly_Gates_evidence_Cloud import_04-29-2021_21-05-03** file to open the existing E3 case file with Slack data.
4. When prompted, **click OK** to accept the default name for the evidence and add the data from the existing case file to your current case file.
5. In the Case Content pane, **navigate to *yourname* Email Forensics / Beverly_Gates_evidence_Cloud import_04-29-2021_21-05-03/ E3 data case / Cloud Data Import / bgates.genius.2345632@gmail.com**, then **expand the Intricate Solutions folder** to display the contents of the Slack database.

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

The screenshot shows the 'Case Content' pane of a digital forensic tool. At the top, there are two tabs: 'Case Content' (selected) and 'Sorted Files'. Below the tabs, the title 'Items' is displayed. The main area shows a hierarchical tree structure of evidence items:

- yourname Email Forensics
 - BG_evidence
 - Beverly_Gates_evidence_Cloud import_04-29-2021_21-05-
 - E3 data case
 - Cloud Data Import
 - bgates.genius.2345632@gmail.com
 - IntricateSolutions
 - Attachments
 - Members List
 - Channels
 - Channels List
 - Direct Messages
 - Direct Messages List
 - Attached Files

Slack database

Note: The Slack application allows users to communicate in multiple channels. As a forensic investigator, identifying the users and channels in a Slack database can help guide your investigation. In the next steps, you will document the users and channels associated with Beverly's Slack account – or in other words, the users and channels that Beverly communicated with.

6. In the Case Content pane, **select the Members grid node** to display the list of Slack users that Beverly has communicated with in the Data Viewer.

7. **Make a screen capture showing the members of the IntricateSolutions workspace.**

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

8. In the Case Content pane, **select** the **Channels grid node** to display the list of Slack channels in the Data Viewer.
9. **Make a screen capture** showing the **channels in the IntricateSolutions workspace**.

Note: Now that you have determined who Beverly has been communicating with via Slack, you will again use E3's Advanced Search feature to narrow your search and attempt to surface relevant evidence. Suppose senior leadership suspects that Beverly has been using specific code words to covertly discuss her drug trafficking operation, including the term "star dust". In the next steps, you will run a search against the Slack database for any conversations that reference star dust.

10. In the Case Content pane, **right-click** the **bgates.genius.2345632@gmail.com sub-node** and **select Advanced Search** from the context menu to open a new Advanced Search pane in the center console.
11. In the Advanced Search pane, **type star AND dust** in the Search What field, then **click** the **Start button** to run a search for both words.
12. When the search is complete, **double-click** the **result** to display the conversation and its location in a new tab.

Note: The only search result should be a conversation between Beverly and Eliot "Just Eliot" in the Main Channel that explicitly references "star dust." Based on Beverly's strong reaction to Eliot's mention of star dust, the term clearly means something specific to her. She also tells Eliot to "use discord," which implies that there may be more explicitly incriminating evidence to be had elsewhere.

13. **Make a screen capture** showing the **conversation contents**.
14. **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 new evidence in different email clients and chat applications.

Part 1: Import a Thunderbird Email Database

Note: In this part of the lab, you will continue your investigation into Beverly Gates using a Thunderbird database. Mozilla Thunderbird is a free, open-source email client. Using one account, users can manage multiple email addresses and support multiple identities. By analyzing Beverly Gates Thunderbird account, you may be able to uncover other identities that she is using in her drug trafficking operation.

In the next steps, you will import the Thunderbird database to your E3 case file.

1. From the vWorkstation desktop, **launch the E3 application**.
2. From the Welcome screen, **open the *yourname* Email Forensics case file** that you created in Section 1.
3. In the Case Content pane, **navigate to BG_evidence / NTFS**, then **expand the Data Triage node** and **select the E-mail Databases category** to display its contents in the Data Viewer pane.
4. In the Data Viewer pane, **open the dfb7v5vd.default-release database**.

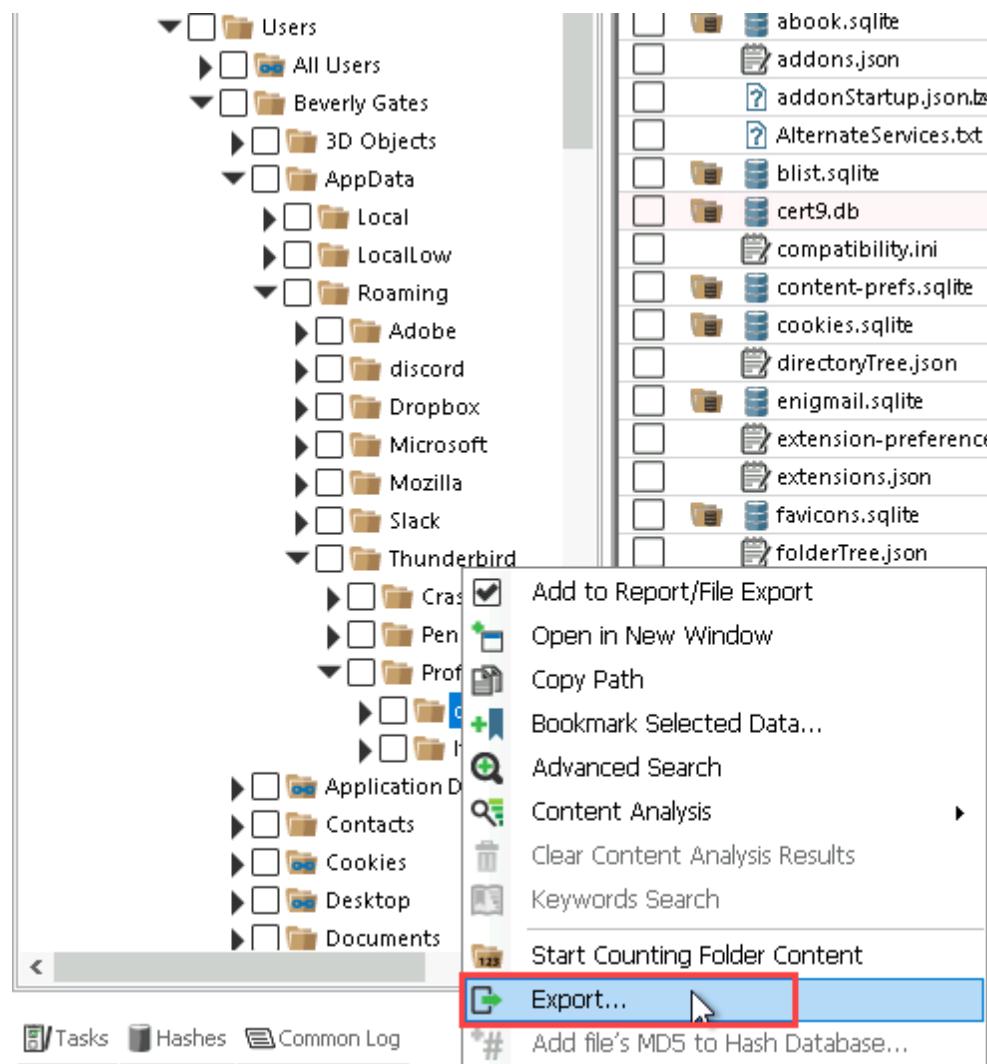
Note: At this point, you will be prompted with a message stating that because this is a Thunderbird email database, it will need to be exported from the drive image, and then reimported as an email database. In the next steps, you will do exactly that.

5. In the Data Viewer pane, **right-click the Thunderbird database (dfb7v5vd.default-release)** and **select Go to Source** to locate the database within the filesystem.

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

6. In the Case Content pane, **right-click** the **dfb7v5vd.default-release** folder and **select Export** from the context menu to open the Export Options window.



Export

7. In the Export Options window, **click the Export button** to save the Thunderbird database to the E3 case folder.
8. When prompted, **close the Task Status Notification dialog box**.

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

- Once the database is exported, **click the Add Evidence button** to open the Add Evidence window.



- In the Add New Evidence window, **select the E-mail Database category**, then **select the Thunderbird database source type**.

Note: In this database, the emails are stored in separate folders. Specifically, Inbox emails are available in the imap.gmail.com folder, whereas the Sent, Deleted and Outbox emails are in the Local Folders folder. You need to add both folders to the case, then analyze the whole Thunderbird database.

- In the Folder selection window, **click Browse** and **navigate to C:\Users\Administrator\Documents\E3 Cases\yourname Email Forensics\dfb7v5vd.default-release\imapMail\imap.gmail.com**, then **click Open** and **OK** to continue.
- When prompted, **click OK** to accept the default evidence name.
- Repeat steps 9-12 to import dfb7v5vd.default-release\Mail\Local Folders.**
- In the Case Content pane, **navigate to imap.gmail / Thunderbird / image.gmail.com / INBOX** to display the contents of the Inbox in the Data Viewer pane.
- Make a screen capture showing the Thunderbird Inbox.**

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

15. In the Data Viewer, **open** the email with the **subject: Well, well, well** in the E-mail Data pane.
16. In the E-mail Data pane, **open** the **RFC Header viewer**.
17. **Document** the sender's email address, mail server name, and mail server IP address in the Well, Well, Well email header.

Part 2: Search for Evidence in a Thunderbird Database

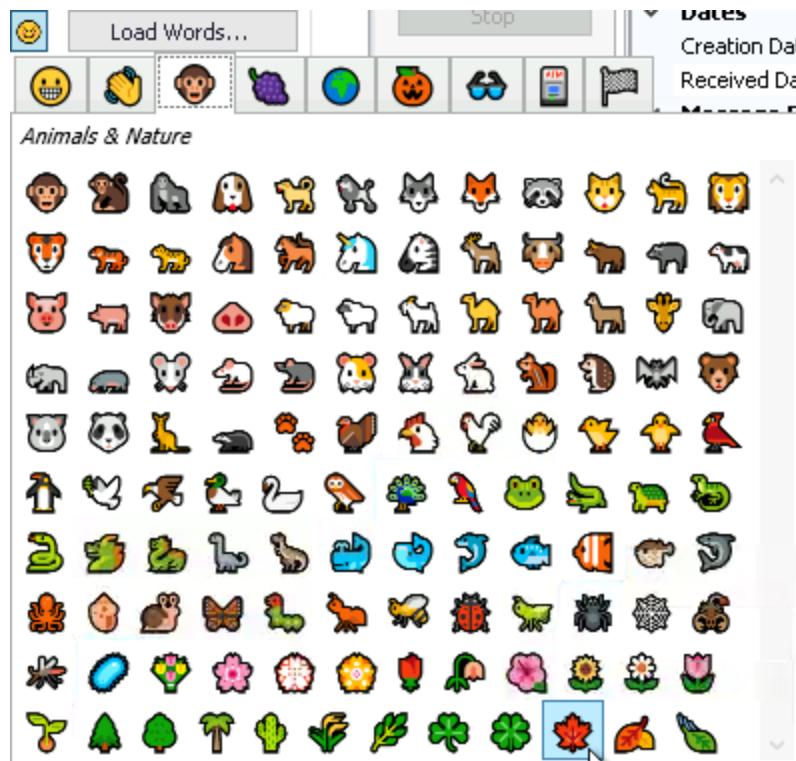
Note: According to senior management, Beverly Gates is suspected of using emojis as code for drugs. Fortunately, E3's Advanced Search functionality allows users to use emojis as search terms.

In the next steps, you will search for emails containing specific emojis within the Thunderbird database.

1. In the Case Content pane, **right-click** the **INBOX folder** and **select Advanced Search** from the context menu to open an Advanced Search pane within the center console.
2. In the Advanced Search pane, **click** the **Emoji Picker button**, then **select** the **maple leaf** on the Animals and Nature tab as your search criteria.

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07



Emoji Picker

Note: As a means of communication, many emojis have transcended the objects that they literally represent to take on a much broader and ever-evolving web of alternative meanings. This ambiguity also makes them an ideal means of communicating about illicit activities. For example, the maple leaf is a common symbol for drugs, [given its passing resemblance to a marijuana leaf](#).

3. In the Advanced Search pane, **click the Start button** to start the searching process.
4. When the search is complete, **review the results**.

Note: Your search has identified an email sent by one Leo Deforest, who appears to be requesting different types of drugs, represented as emojis. You now have the name of a likely buyer and potential witness.

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

5. Make a screen capture showing the email from Leo Deforest.

Note: In the next steps, you will use E3's Keyword Search feature to search for additional evidence of drug trafficking. According to senior management, Beverly Gates is suspected of selling a variety of pills and powders, so you will use "pills" as your next search term. To expand your search beyond the text in Beverly's emails, you will use E3's Content Analyzer to extract text from image files and save the text as indexed keywords. When you run your Keyword Search, E3 will include any graphics files that contain the search term in the results.

6. In the Case Content pane, **right-click** the **Local Folders** evidence node and **select Content Analysis > Index Keywords in Images (OCR)** to open the Content Analysis Wizard.
7. In the Content Analysis Wizard, **confirm** the **Extract and index text from graphic files (OCR) checkbox** is selected, then **click Finish** to index the keywords identified in any graphics files found within the Local Folders database.
8. When the indexing process is complete, **right-click** the **Local Folders** node and **select Keywords Search** to perform a search using the indexed keywords.
9. In the Keywords Search pane, **type pills** in the Search what field, then **click Start** to run the search.
10. When the search is complete, **review** the results.

You will need to use the File View in the Viewers pane to display the contents of any image files returned in the results.

Note: Your search should return one result - a PNG file that contains the word *pills*. The email itself does not contain any reference to pills, which means that this evidence would have eluded your grasp without the keyword index that you generated with the Content Analyzer.

By now, you should have also noticed that the email account associated with the Thunderbird database is redwitch321@gmail.com and that Beverly has signed many of these emails as Natasha "Red" Maximoff. As you may recall, senior leadership at Intricate Solutions has suggested that Beverly might have connections to the Russian mafia. Is it possible that Beverly is not her real name? Or is Natasha "Red" Maximoff the alias? Either way, you now have additional evidence that makes explicit references to drug sales.

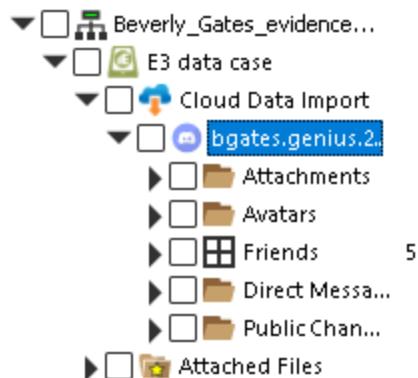
11. Make a screen capture showing the **pills** evidence and Beverly Gates corresponding as Natasha "Red" Maximoff.

Part 3: Search for Evidence in a Discord Database

Note: Discord is a free chat service that is accessible from mobile devices and computers. Discord allows users to talk to friends and strangers using chat, voice, or video. It was initially created as a way for people to communicate while playing video games, but its popularity has since exploded, opening it up to millions of users. In Section 1, you discovered evidence where Beverly made reference to using Discord. The security team at Intricate Solutions has since confirmed that Discord was installed on Beverly Gates's company laptop, which means it may have been used as part of her criminal activity.

In the next steps, you will add a copy of Beverly's Discord database to E3 and perform an advanced search in the chat database.

1. Add the **Beverly_Gates_evidence_Cloud import_04-29-2021_20-55-03** file as new evidence using the E3 data case/DS case file source type.
2. In the Case Content pane, expand the **bgates.genius.2345632@gmail.com (Beverly_G_2345632)** account to view the structure of the Discord database.



Discord cloud data import

Conducting Forensic Investigations on Email and Chat Logs (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

3. Open the **Friends** grid node and review the contents.
4. Make a screen capture showing Beverly's Discord friend list.
5. In the Case Content pane, right-click the Direct Messages folder and select Advanced Search.
6. In the Advanced Search pane, open the **Emoji Picker** and select the following emojis for the search, then click Start to launch the search process: pill, wine glass, and cocktail glass.

You will need to separate each emoji with the word OR.
7. Review the search results

Note: The search should return multiple hits in conversation between Beverly and one Lena Goodwin. Within the conversation, Lena requests pills using the pill emoji, to which Beverly replies with a reference to Mrs. M – presumably the Mrs. Maximoff that Beverly goes by in her other email account.

8. Make a screen capture showing the **Lena Goodwin** conversation.

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: Search for Additional Email Evidence

At this point in your investigation, you have identified multiple email and chat communications between Beverly Gates and likely customers discussing the sale and distribution of illegal drugs. In Section 2, while investigating her secondary email database, you learned that Beverly has been selling pills and using emojis to communicate about her drug sales. In this part of the lab, you will return to Beverly's original Outlook account and run a similar search.

Using the Advanced Search feature on the Outlook database, run a search for messages containing the pill emoji.

Make a screen capture showing the email thread returned in the search results.

Part 2: Search for Additional Chat Evidence

In Section 2 of the lab, you identified a conversation between Beverly and Lena Goodwin in a Discord chat database that Beverly was apparently using as the preferred means of discussing drug sales. However, your review of the Discord database was limited to the results of the emoji search, and you wonder if there might be additional evidence that you could identify by manually reviewing some of the other chat logs.

Using E3, explore the other conversations in the Discord data to identify another conversation related to drug trafficking.

Make a screen capture showing the additional evidence within the Discord database

Note: This concludes Section 3 of the lab.