

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

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

Student:

Loksharan Saravanan

Email:

loksharan.soc@gmail.com

Time on Task:

1 hour, 18 minutes

Progress:

100%

Report Generated: Friday, November 21, 2025 at 11:38 PM

Section 1: Hands-On Demonstration

Part 1: Analyze Email Headers

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

The screenshot shows the Paraben's E3 Multiple Platforms software interface. The main window displays a search results list for an email titled 'Re: Happy Reminder'. The properties pane on the right shows the following details for the selected email:

- General**:
 - Internet Message ID: <C2F919E9B11325205CBA0>
 - Message Class: IPM.Note
 - Message Sub-System: Microsoft
- Date**:
 - Creation Date: 4/26/2021 7:30:41 AM
 - Received Date: 4/26/2021 7:30:41 AM
 - Sent Date: 4/26/2021 7:30:39 AM
- Message Flags**: Undefined
- Recipients**: Beverly Gates <bever.gates@outlook.com>
- Represent Sender**: Karen Jeff <karen.jeff@intricate365.onmicrosoft.com>
- Sender**:
 - From: Karen Jeff <karen.jeff@intricate365.onmicrosoft.com>
 - Sender Address Type: Name
 - Sender E-mail: karen.jeff@intricate365.onmicrosoft.com
 - Sender Name: Karen Jeff
- Subject**: Re: Happy Reminder

The Text Viewer pane below shows the content of the selected email:

```
Re: Happy Reminder
[Karen Jeff] <karen.jeff@intricate365.onmicrosoft.com> - on behalf of [Karen Jeff] <karen.jeff@intricate365.onmicrosoft.com>
To: Beverly Gates <bever.gates@outlook.com>

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

From: Mr. Harris Malone <m.harris@intricate365.onmicrosoft.com>
Sent: Wednesday, April 28, 2021 6:17 AM
To: Beverly Gates <bever.gates@outlook.com>; Karen Jeff <karen.jeff@intricate365.onmicrosoft.com>
Subject: Re: Happy Reminder

Ladies,
```

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

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

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

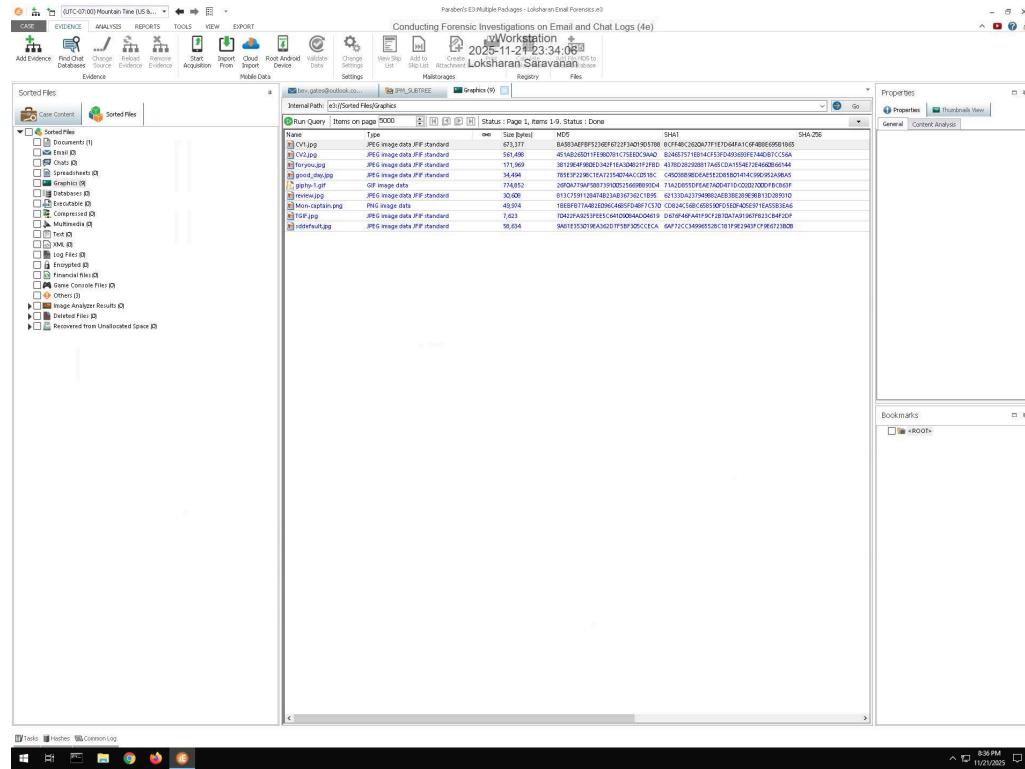
The screenshot shows the Paraben's E3 Multiple Packages software interface. The main window displays an email inbox from 'ber-gates@outlook.com' to 'ber-gates@outlook.com'. The subject of the email is 'Re: Intricate Solution Job Offer'. The message was received on 4/27/2021 at 7:35:33 AM. The properties pane on the right shows the recipient as 'berly.Gates-clm-gates@msn.com' with the name 'Vicky Reed'. The message flags indicate it is a draft. The message body contains the text: "Re: Intricate Solution Job Offer", "Subject: Re: Intricate Solution Job Offer", "From: Vicky Reed <vicks.reeds@gmail.com>", "To: ber-gates<ber-gates@outlook.com>". The message content includes several attachments, notably a PDF file named 'Re: Intricate Solution Job Offer.pdf' and a Microsoft Word document named 'Re: Intricate Solution Job Offer.docx'. The file paths for these attachments are visible in the left sidebar under 'Case Content'.

Part 2: Search for Evidence in an Outlook Database

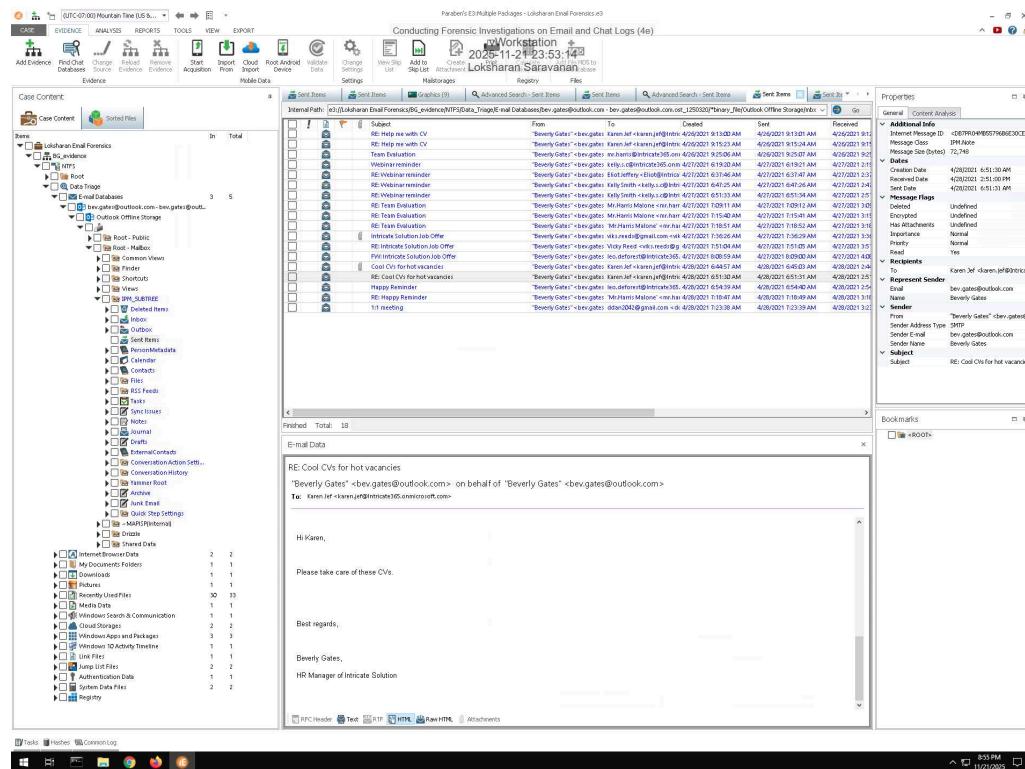
Conducting Forensic Investigations on Email and Chat Logs (4e)

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

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



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



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

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

Part 3: Search for Evidence in a Slack Database

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

The screenshot shows the Paraben's E3 Multiple Packages software interface. The main window title is "Conducting Forensic Investigations on Email and Chat Logs (4e)". The left sidebar shows a tree view of "Case Content" and "Case Details". The central pane displays a table of "Members" with the following data:

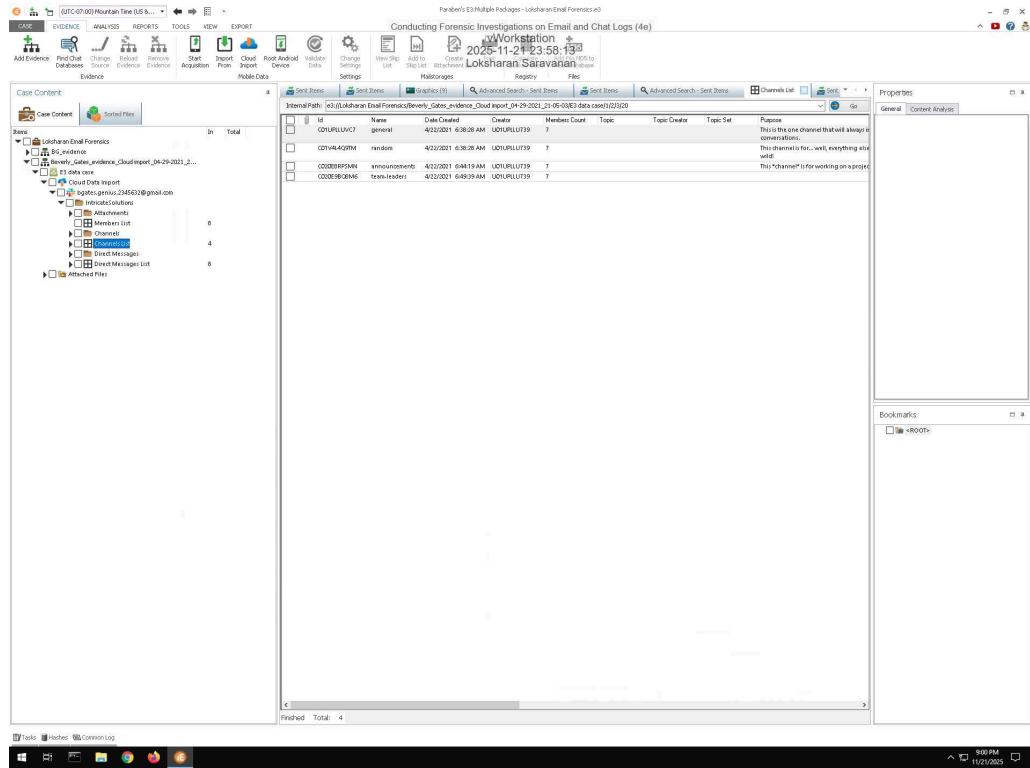
Member ID	Real Name	Display Name	Email	Type	Team	Status Text	Status Err
USACBOT	Slackbot	Slackbot	bot@slack.com	Bot	TO1	INB6wPF	
UDTULU739	Beverly Gates	Beverly Gates	beverly.gates.1970@gmail.com	User	TO1	INB6wPF	
UDTUPK1ZP	Kelly Cooper	Kelly Cooper	kelly.cooper.02@gmail.com	User	TO1	INB6wPF	
UDTVJYH7C	Karen Jeffrey Hrb	Karen Jeffrey Hrb	karen.jeffrey90@gmail.com	User	TO1	INB6wPF	
UDTVAM0B1Z	July Riley (Stand)	July Riley (Stand)	july.riley.3337@gmail.com	User	TO1	INB6wPF	
UDTVANH7F	Alan Super Herd	Alan Super Herd	alan.herd1970@gmail.com	User	TO1	INB6wPF	
UDT0519H4M	Lee DF Pavlyuk	Lee DF Pavlyuk	lee.pavlyuk@gmail.com	User	TO1	INB6wPF	
UDT0519G1Q	Ethan Justesen	Ethan Justesen	ethan.justesen@gmail.com	User	TO1	INB6wPF	

The bottom status bar shows the date and time as "11/21/2025 8:00 PM".

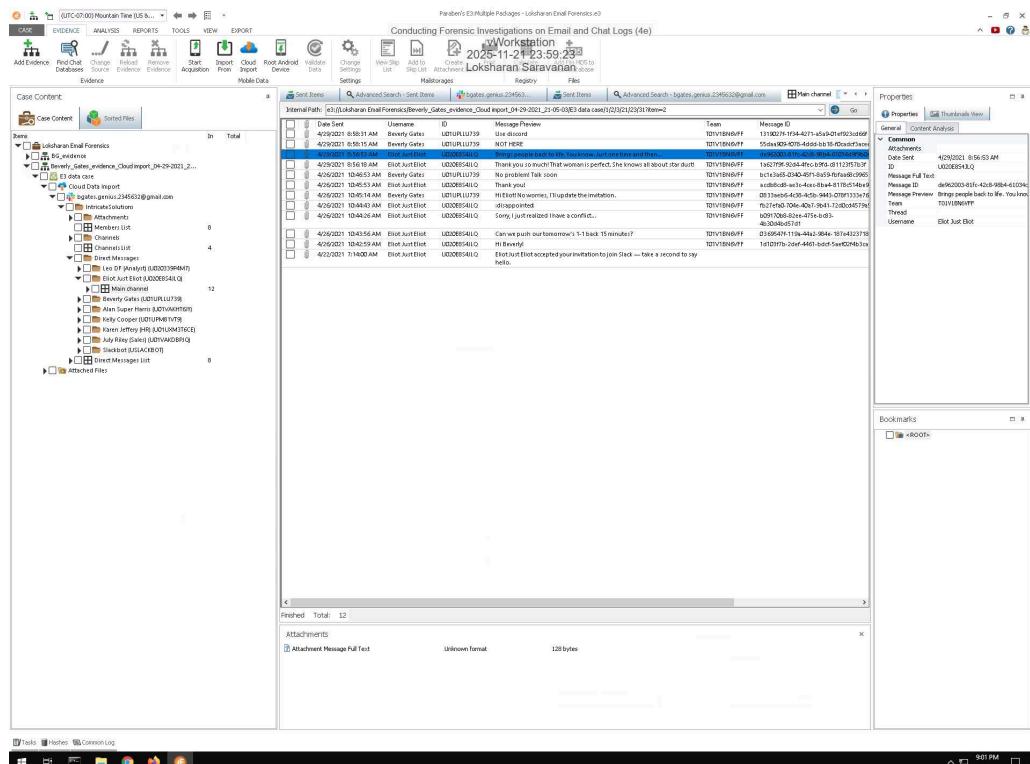
Conducting Forensic Investigations on Email and Chat Logs (4e)

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

9. Make a screen capture showing the channels in the IntricateSolutions workspace.



13. Make a screen capture showing the conversation contents



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

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

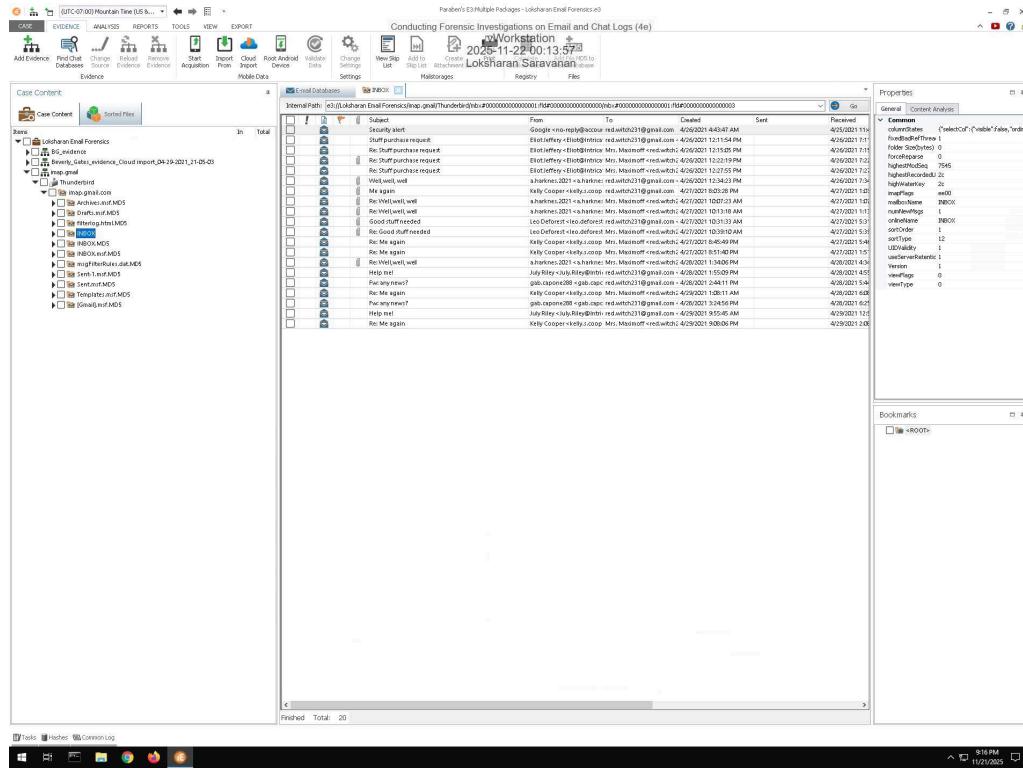
Conducting Forensic Investigations on Email and Chat Logs (4e)

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

Section 2: Applied Learning

Part 1: Import a Thunderbird Email Database

15. Make a screen capture showing the Thunderbird Inbox.



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

email address: red.witch@gmail.com
ip address: 185.70.40.132

Part 2: Search for Evidence in a Thunderbird Database

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.

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

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

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

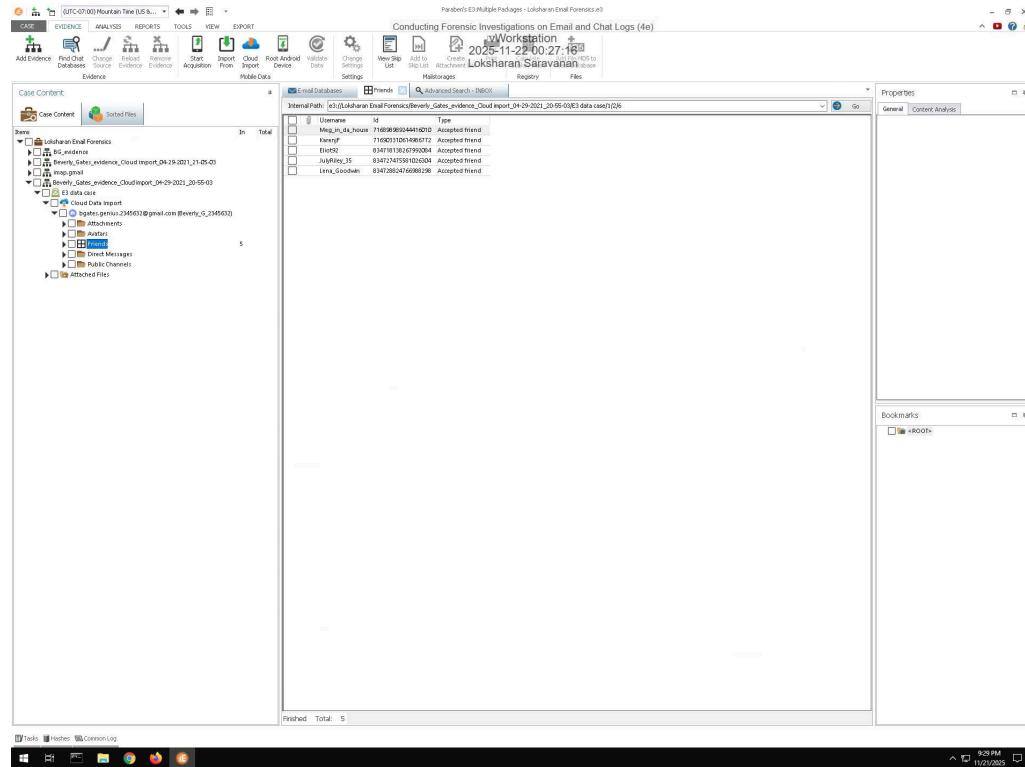
The screenshot shows the Paraben's ESI Multiple Plugins - Lab07 on Email Forensics v2 interface. The main window displays a search results table for 'Evidence' with 20 items found. One item is selected, showing its details in the 'Properties' panel. The selected item is an 'Internet Message' from 'red.with23@gmail.com' to 'a.harkness.2021 <aharkness.2021+aharkness:red.with23@gmail.com>' on 4/26/2021 at 1:45:47 AM. The message subject is 'Re: Well, well, well'. The Properties panel shows various fields like 'Message Size (Byte)', 'Creation Date', and 'Received Date'. The 'Recipients' section lists 'a.harkness.2021 <aharkness.2021+aharkness:red.with23@gmail.com>' and 'red.with23@gmail.com'. The 'Sender' section lists 'red.with23@gmail.com' and 'red.with23@gmail.com'. The 'Subject' section lists 'Re: Well, well, well'. The bottom right corner of the interface shows the date '4/27/2021' and time '8:27 PM'.

Part 3: Search for Evidence in a Discord Database

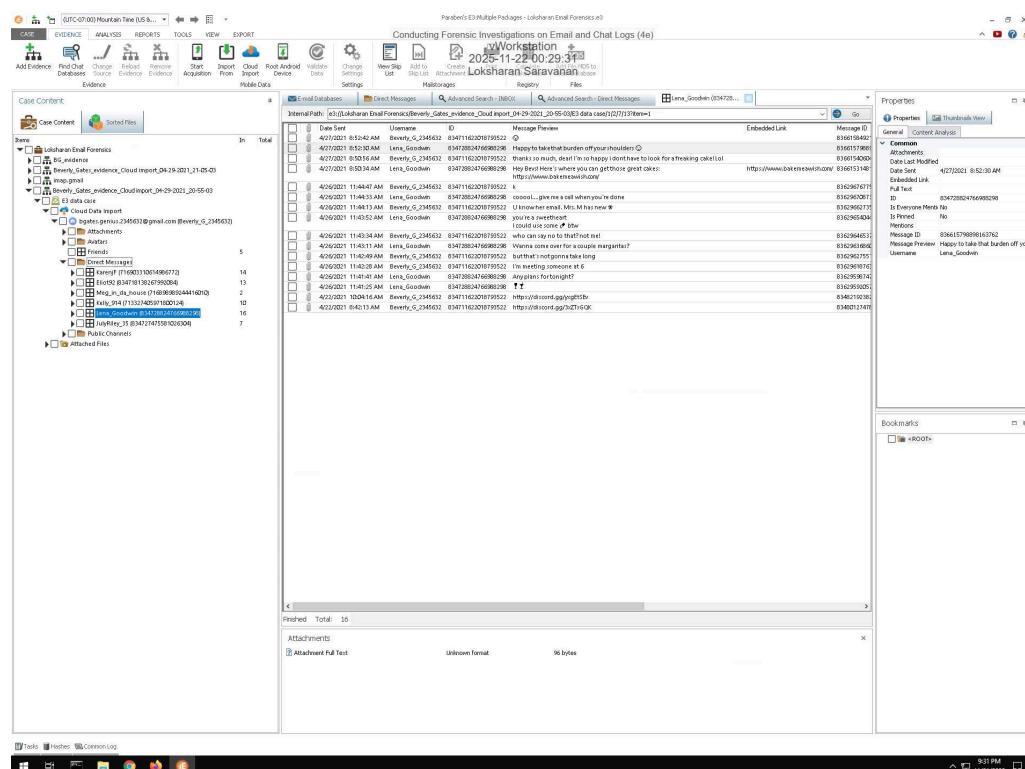
Conducting Forensic Investigations on Email and Chat Logs (4e)

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

4. Make a screen capture showing Beverly's Discord friend list.



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



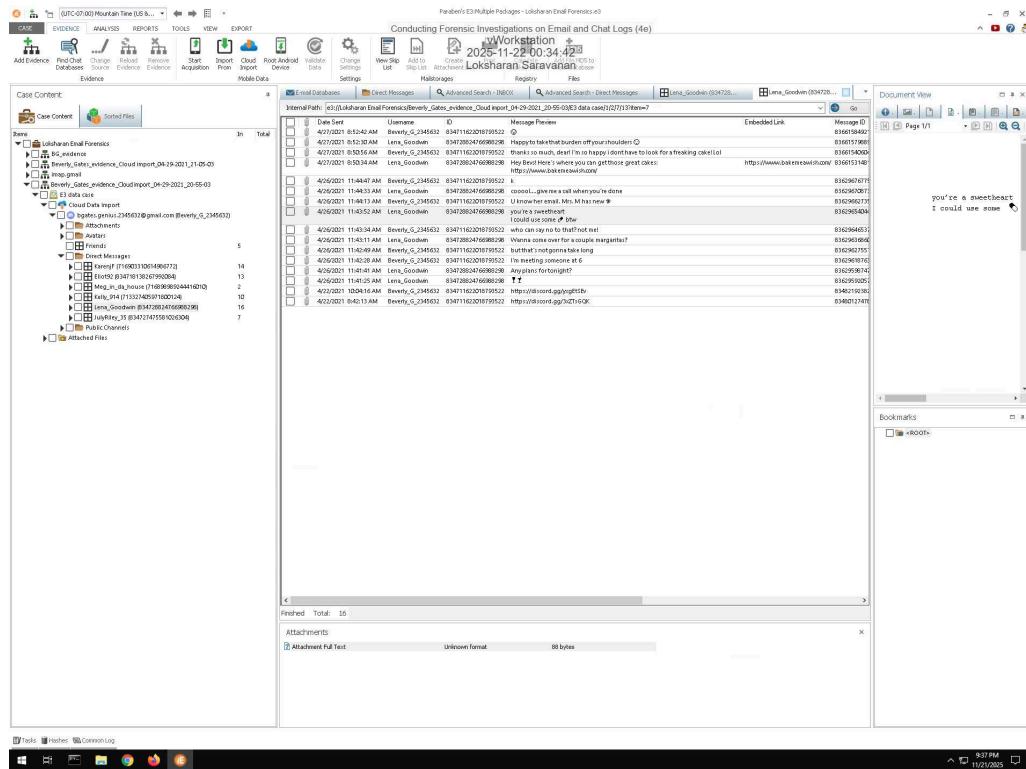
Conducting Forensic Investigations on Email and Chat Logs (4e)

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

Section 3: Challenge and Analysis

Part 1: Search for Additional Email Evidence

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



Part 2: Search for Additional Chat Evidence

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

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

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

The screenshot shows the Paraben's E3 Multiple Packages software interface. The main window displays a list of messages from a Discord channel named 'Loksharan_Saravanan'. The messages are listed by timestamp, showing conversations between users like 'Bevety_Goodkin' and 'Lena_Goodkin'. The interface includes a navigation bar with tabs for CASE, EVIDENCE, ANALYSIS, REPORTS, TOOLS, VIEW, and EXPORT. The EVIDENCE tab is selected. On the left, there is a sidebar for 'Case Content' and 'Evidentiary' categories. The bottom of the window shows a status bar with the date and time (2025-11-22 00:35:17) and a progress bar indicating 16 items finished.