

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:

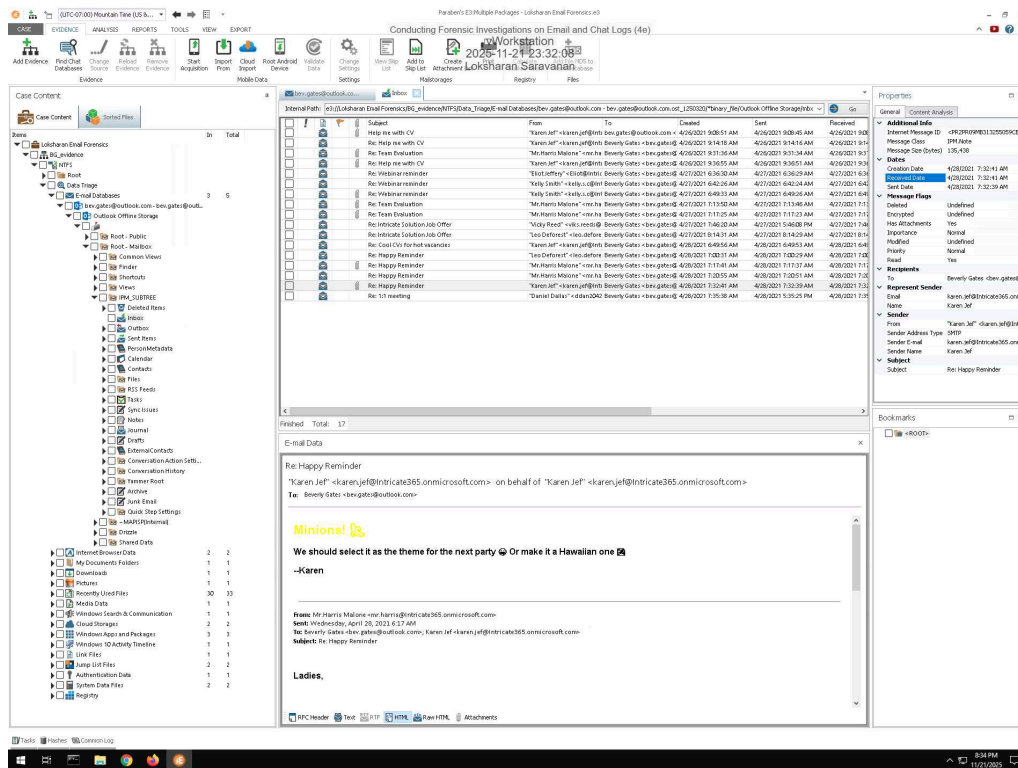
100%

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

Section 1: Hands-On Demonstration

Part 1: Analyze Email Headers

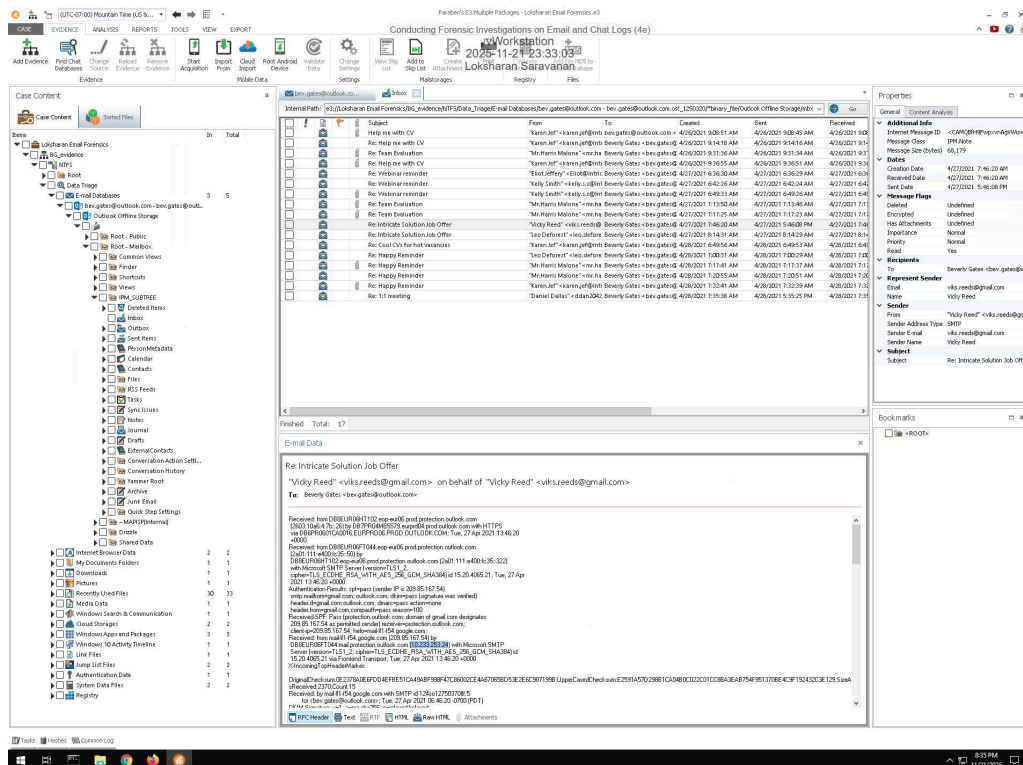
17. Make a screen capture showing the **Happy Reminder** email in the Text Viewer and Timestamp in the Properties pane.



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.

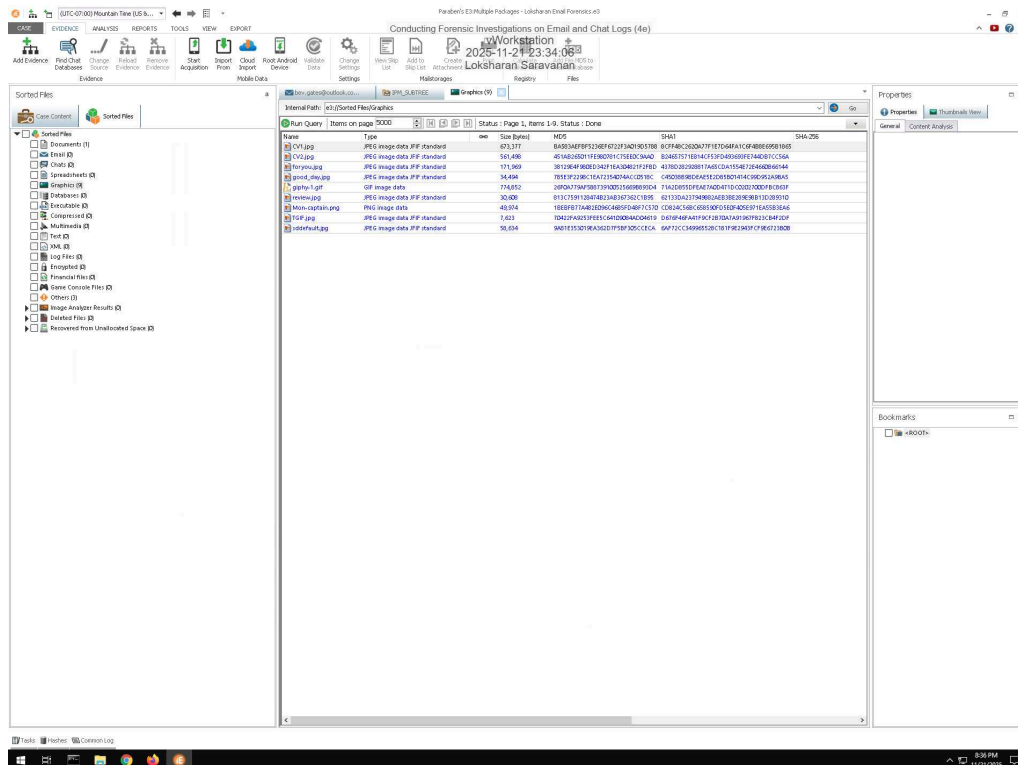


Part 2: Search for Evidence in an Outlook Database

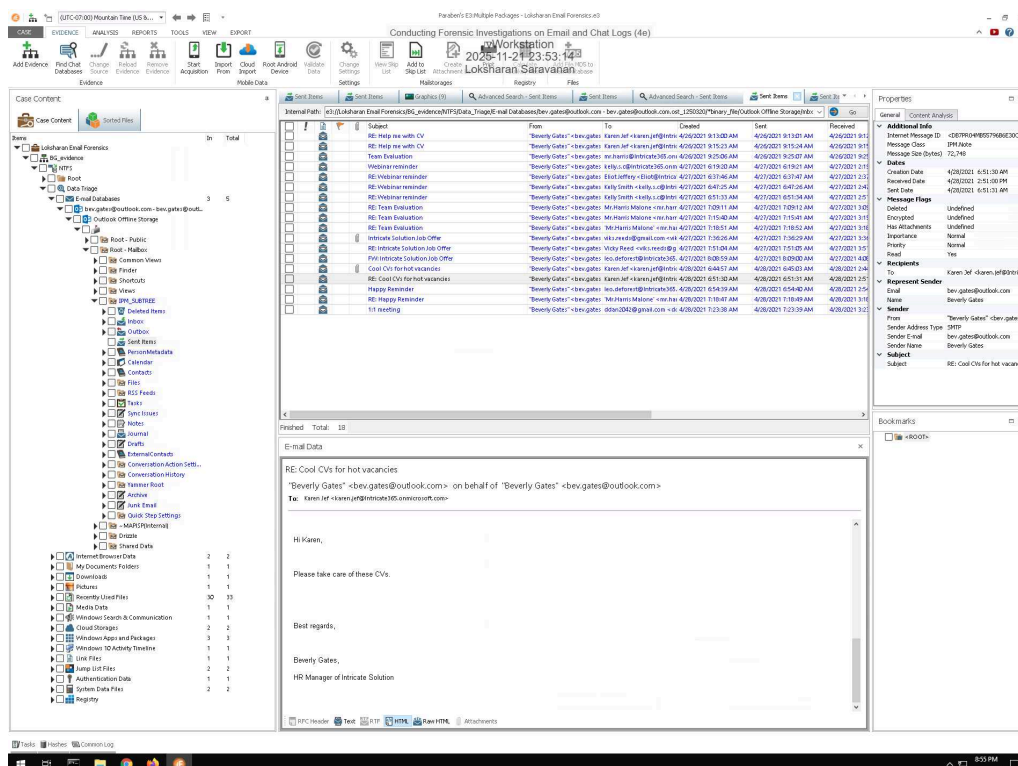
Conducting Forensic Investigations on Email and Chat Logs (4e)

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.

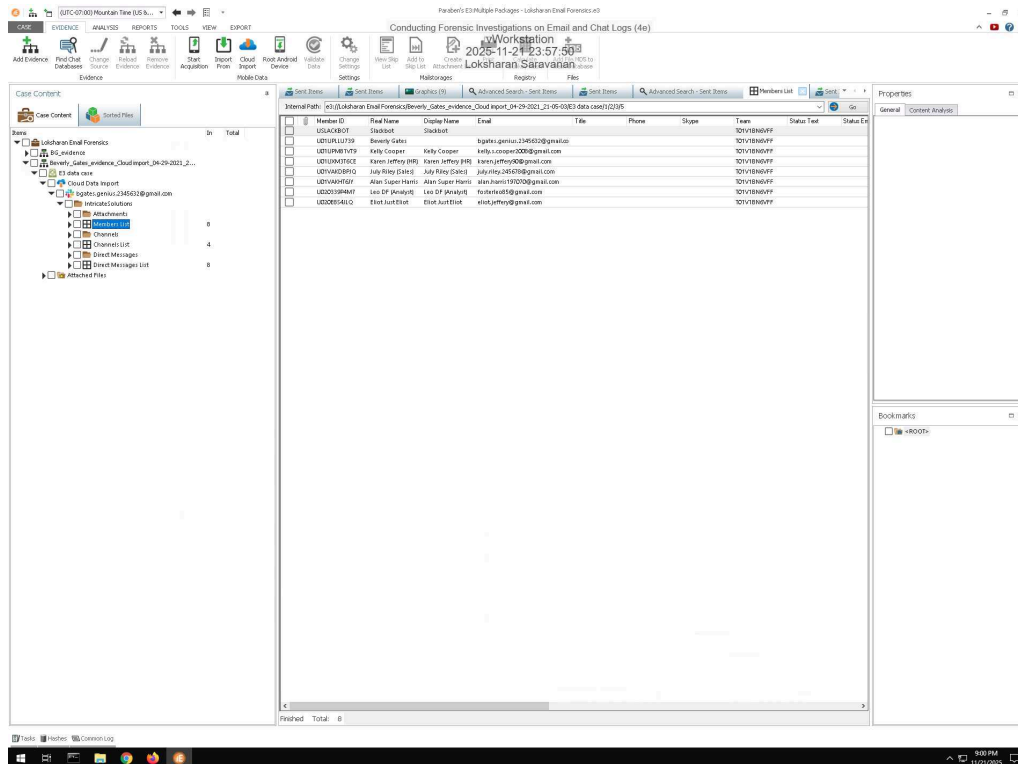


Conducting Forensic Investigations on Email and Chat Logs (4e)

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

Part 3: Search for Evidence in a Slack Database

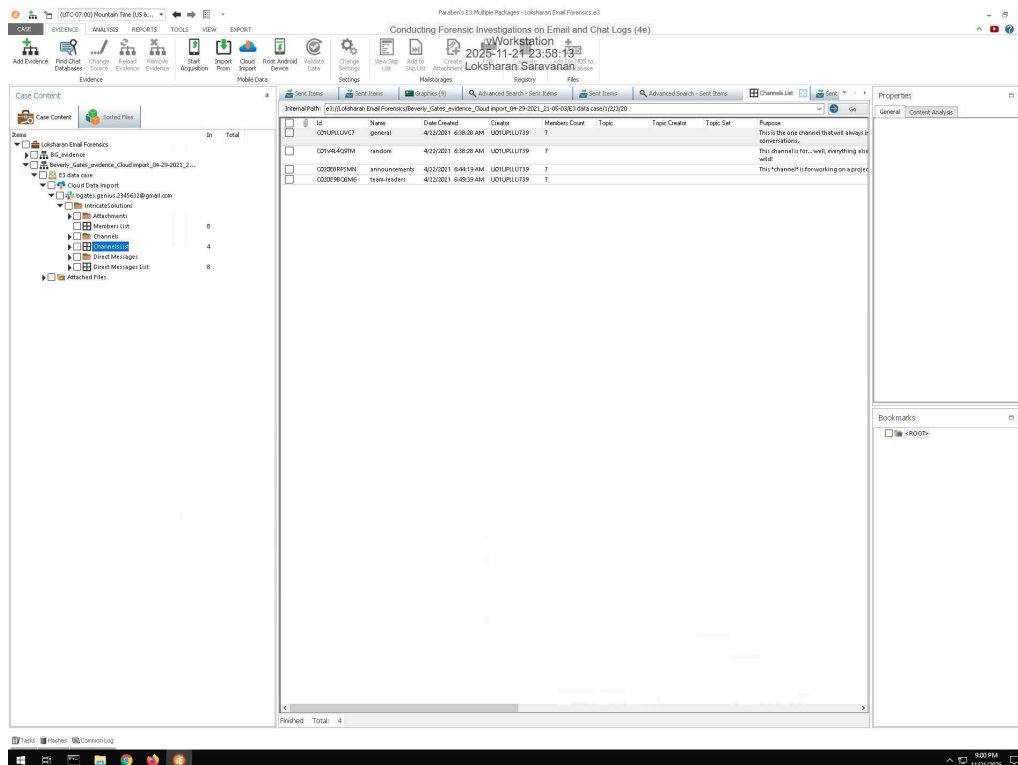
7. Make a screen capture showing the members of the IntricateSolutions workspace.



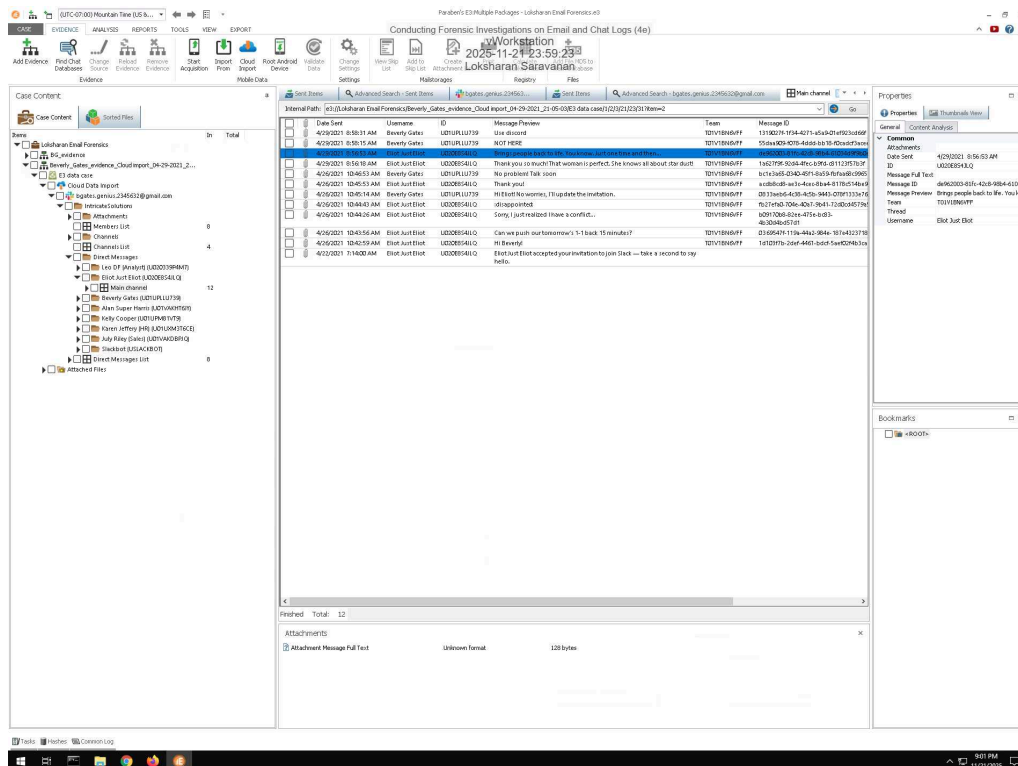
Conducting Forensic Investigations on Email and Chat Logs (4e)

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

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



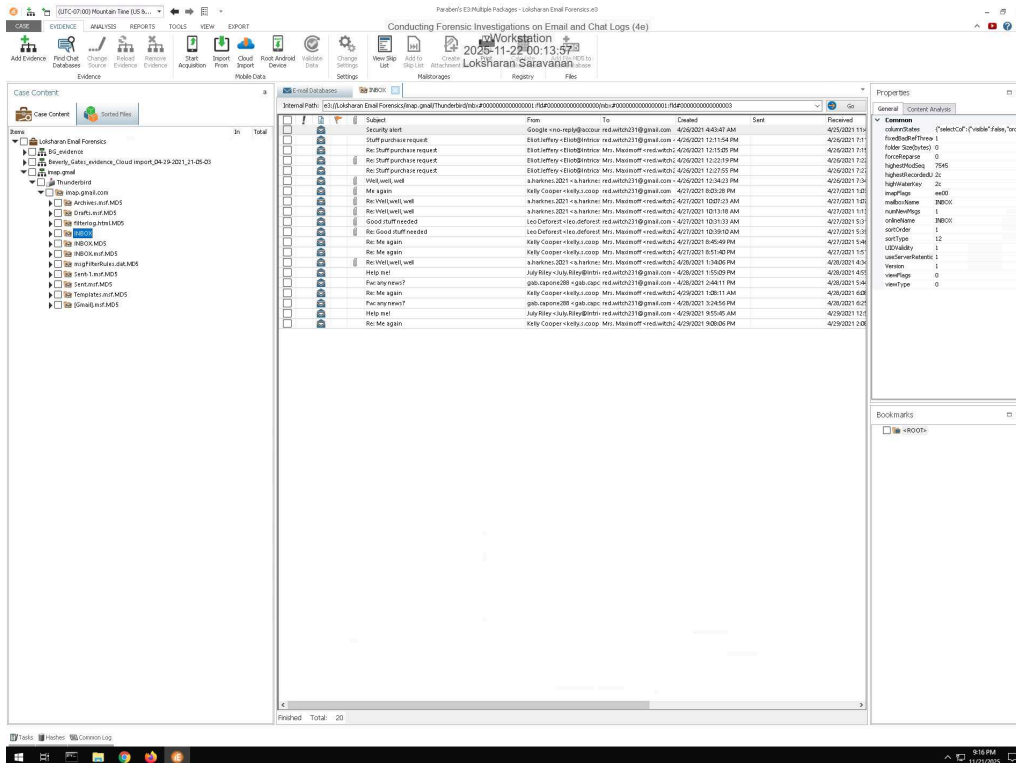
13. Make a screen capture showing the conversation contents.



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

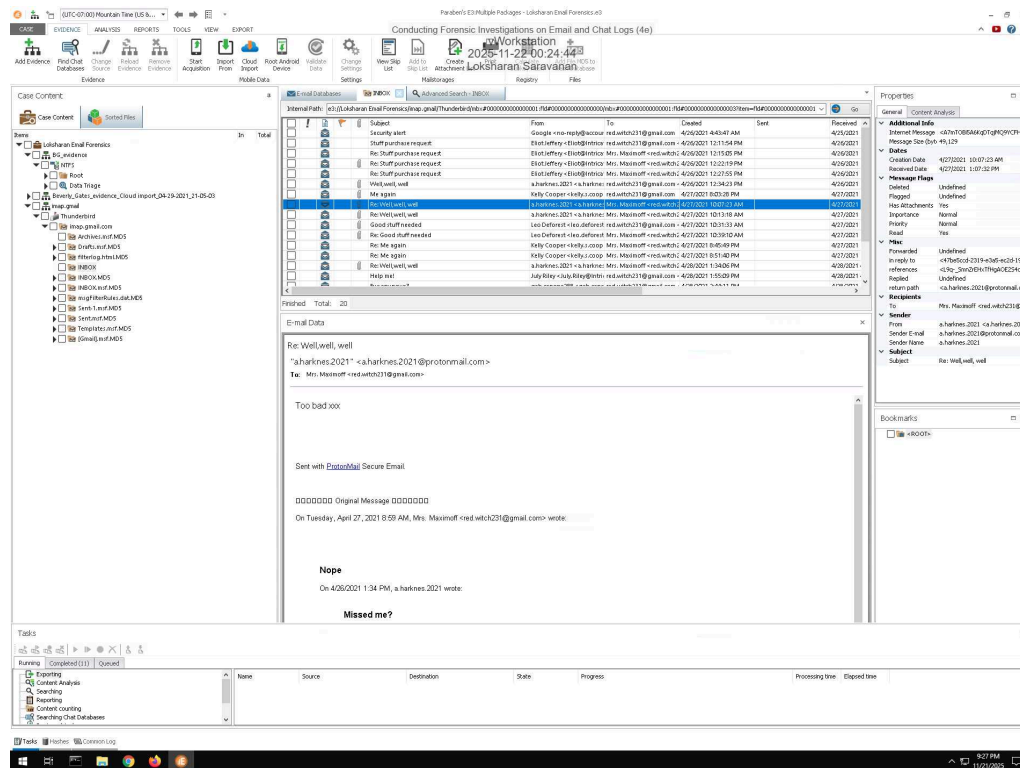
Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

[illegible]

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.

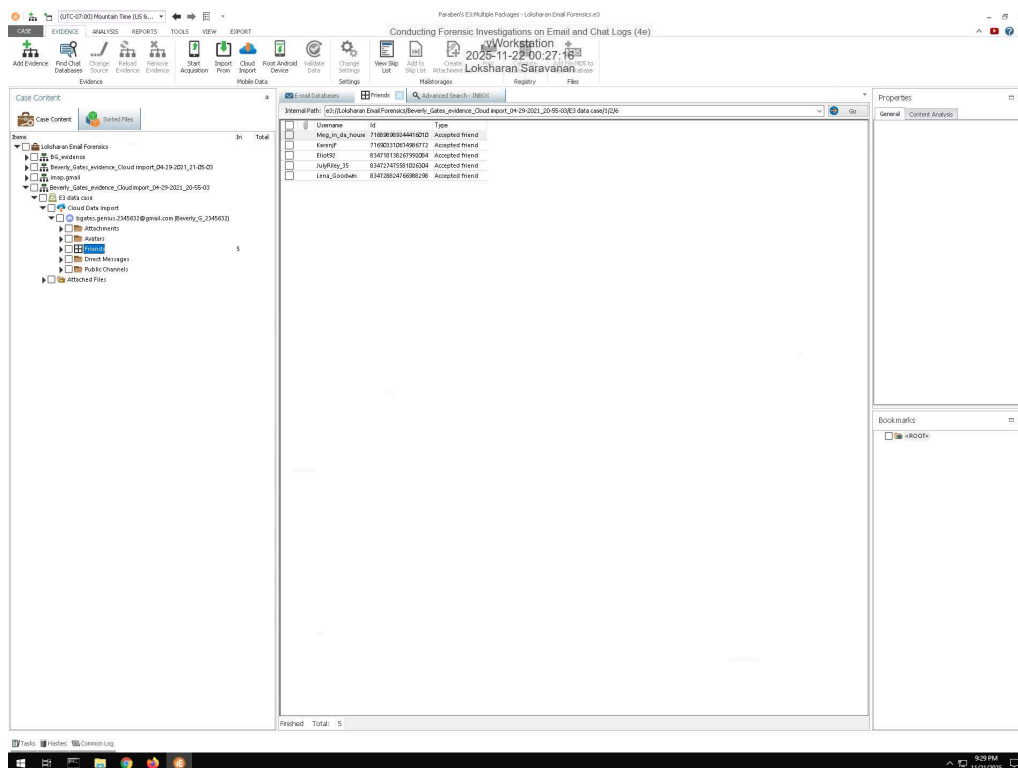


Part 3: Search for Evidence in a Discord Database

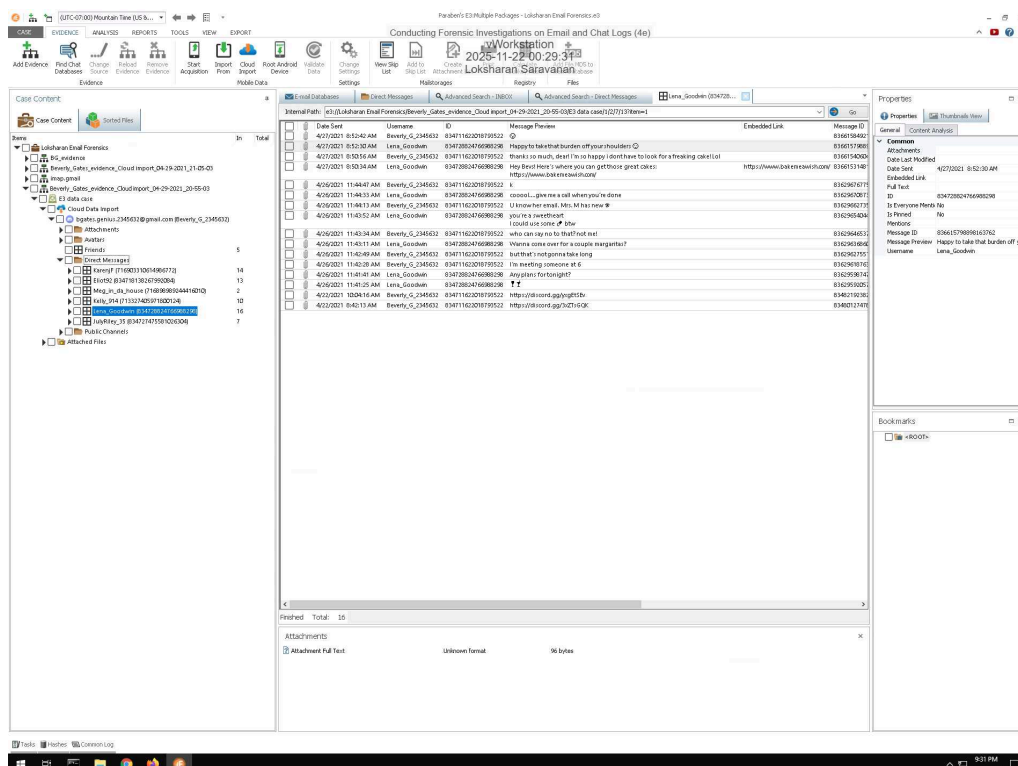
Conducting Forensic Investigations on Email and Chat Logs (4e)

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

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



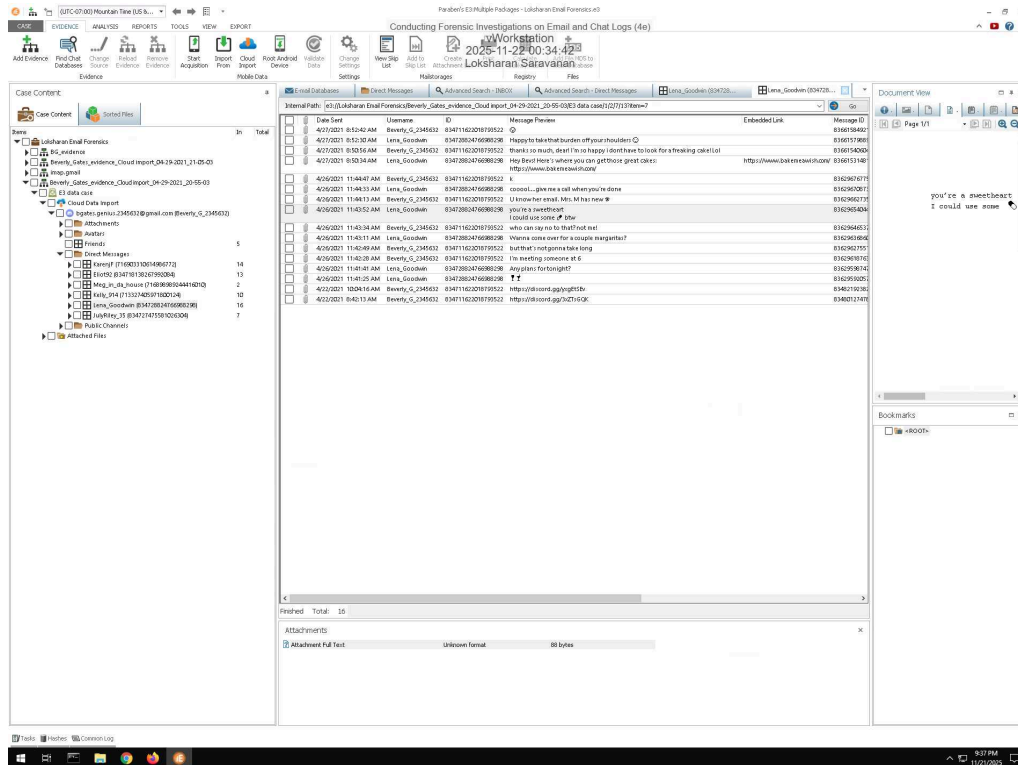
8. Make a screen capture showing the Lena Goodwin conversation.



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

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

Case Content:

Case Content | **Sorted Files**

Items:

- Loksharan Email Forensics
 - FFS_evidence
 - Beverly_Gates_evidence_Cloud import_04-29-2021_11-26-01
 - img.png
 - Beverly_Gates_evidence_Cloud import_04-29-2021_20-55-03
 - Cloud Chat
 - chatgptgpt2345632@gmail.com (Beverly_G_2345632)
 - Attachments
 - Avatar
 - Friends
 - Direct Messages
 - chatgpt (116033100486072) 14
 - chatgpt (134719130247692036) 13
 - chatgpt_p_02_27009171609050441002 2
 - chatgpt_p_01_1713224023619200154 10
 - chatgpt_p_03_1713224023619200154 10
 - chatgpt_p_04_1713224023619200154 16
 - chatgpt_p_05_1713224023619200154 7
 - Public Channels
 - Attached Files

Internal Path: (x) \Loksharan Email Forensics\Beverly_Gates_evidence_Cloud import_04-29-2021_20-55-03\FFS_evidence\chatgpt (116033100486072)\Items\6

Item	Date Sent	Username	ID	Message Preview	Embedded Link
<input type="checkbox"/>	4/27/2021 8:52:42 AM	Beverly_G_2345632	63471162201979552	0	
<input type="checkbox"/>	4/27/2021 8:52:42 AM	Lenix_Soodhan	63472882474680298	Happy to talk that burden off your shoulder ☺	
<input type="checkbox"/>	4/27/2021 8:52:46 AM	Beverly_G_2345632	63471162201979552	thanks to meet, dear! I'm happy ident have to look for a healing cake (a)	
<input type="checkbox"/>	4/27/2021 8:52:46 AM	Lenix_Soodhan	63472882474680298	Hey Bro! Here's where you can get those great cakes: https://www.bakessnack.com/	
<input type="checkbox"/>	4/26/2021 11:44:47 AM	Beverly_G_2345632	63471162201979552	x	
<input type="checkbox"/>	4/26/2021 11:44:23 AM	Lenix_Soodhan	63472882474680298	cool... give me a call whenever you're done	
<input type="checkbox"/>	4/26/2021 11:44:13 AM	Beverly_G_2345632	63471162201979552	U know her said. No..M..has new W	
<input type="checkbox"/>	4/26/2021 11:43:52 AM	Lenix_Soodhan	63472882474680298	you're a sweetheart I could use some #ther	
<input type="checkbox"/>	4/26/2021 11:43:34 AM	Beverly_G_2345632	63471162201979552	who can say no to that not met	
<input type="checkbox"/>	4/26/2021 11:43:17 AM	Lenix_Soodhan	63472882474680298	Wanna come over for a couple margaritas?	
<input type="checkbox"/>	4/26/2021 11:42:49 AM	Beverly_G_2345632	63471162201979552	but that's not going to take long	
<input type="checkbox"/>	4/26/2021 11:42:28 AM	Beverly_G_2345632	63471162201979552	I'm meeting someone at 6	
<input type="checkbox"/>	4/26/2021 11:41:45 AM	Lenix_Soodhan	63472882474680298	Am not for tonight	
<input type="checkbox"/>	4/26/2021 11:41:25 AM	Lenix_Soodhan	63472882474680298	👋👋	
<input type="checkbox"/>	4/26/2021 10:04:16 AM	Beverly_G_2345632	63471162201979552	https://www.crowdfunder.co/	
<input type="checkbox"/>	4/26/2021 9:42:13 AM	Beverly_G_2345632	63471162201979552	http://www.sandp.co.uk/	

Refresh Total: 15

Attachments

Attachment Full Text

Unknown format

56 bytes