

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

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

Student:

Vishal Singh Bhardvaj

Email:

Time on Task:

2 hours, 3 minutes

Progress:

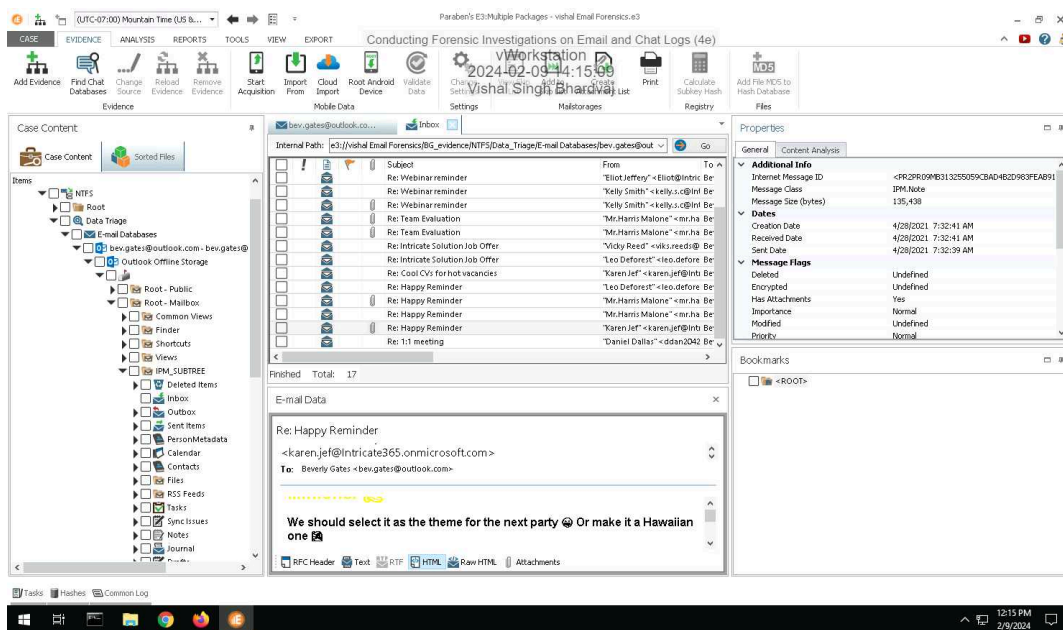
100%

Report Generated: Friday, February 9, 2024 at 4:08 PM

Section 1: Hands-On Demonstration

Part 1: Analyze Email Headers

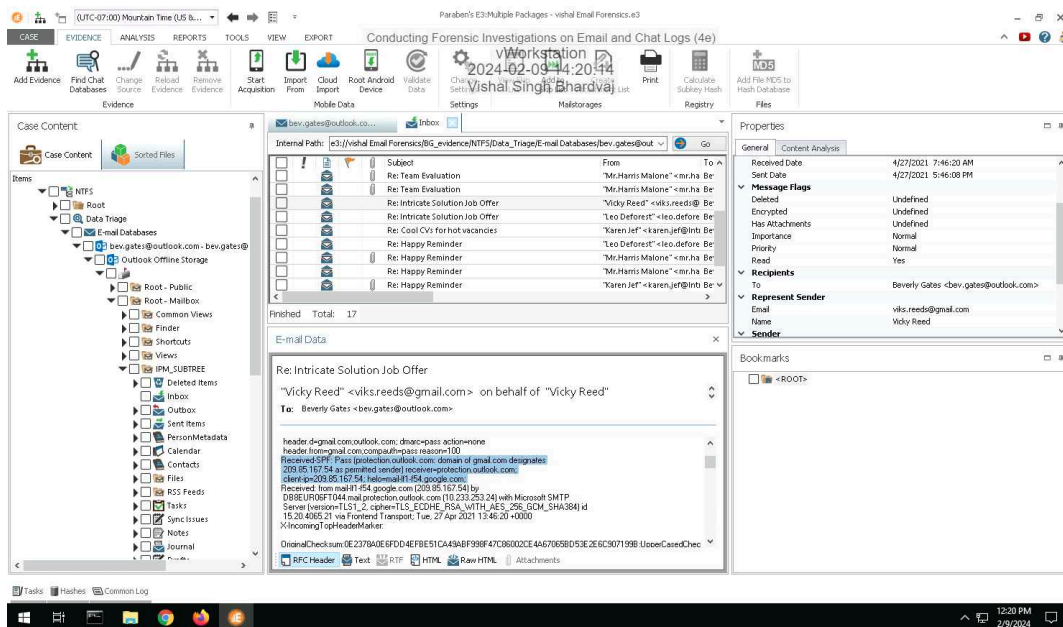
17. Make a screen capture showing the **Happy Reminder** email in the Text Viewer and Timestamp in the Properties pane.



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

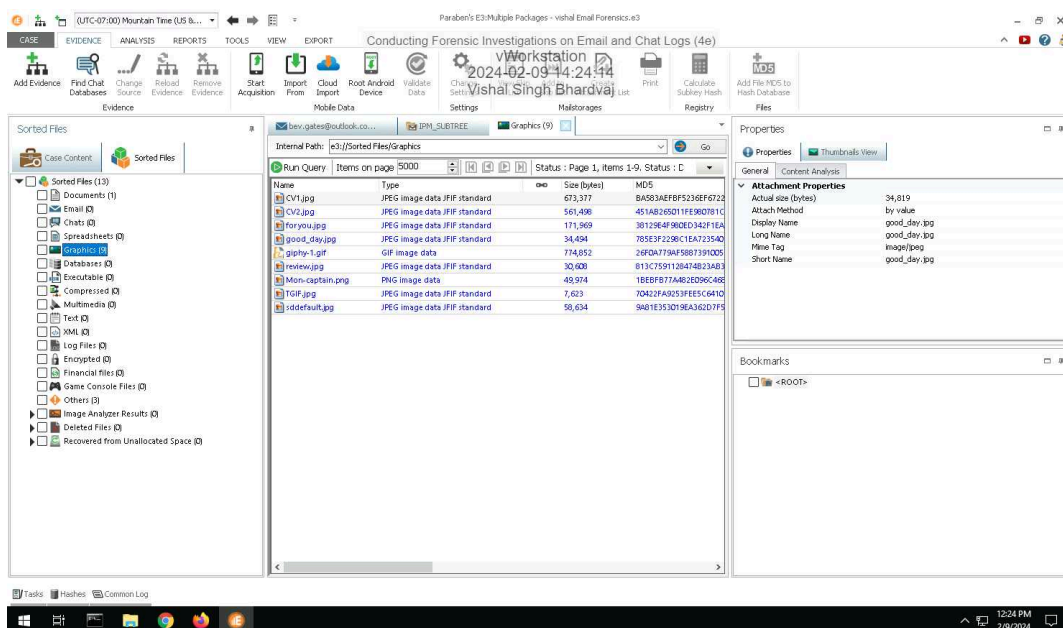
Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

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



Part 2: Search for Evidence in an Outlook Database

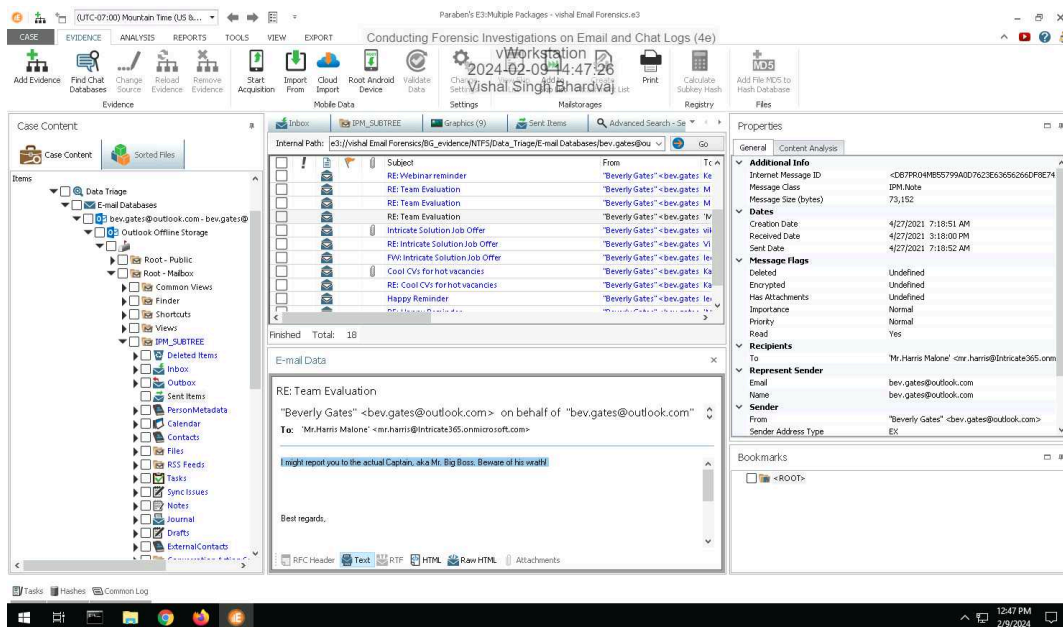
7. Make a screen capture showing the list of files in the Graphics category.



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

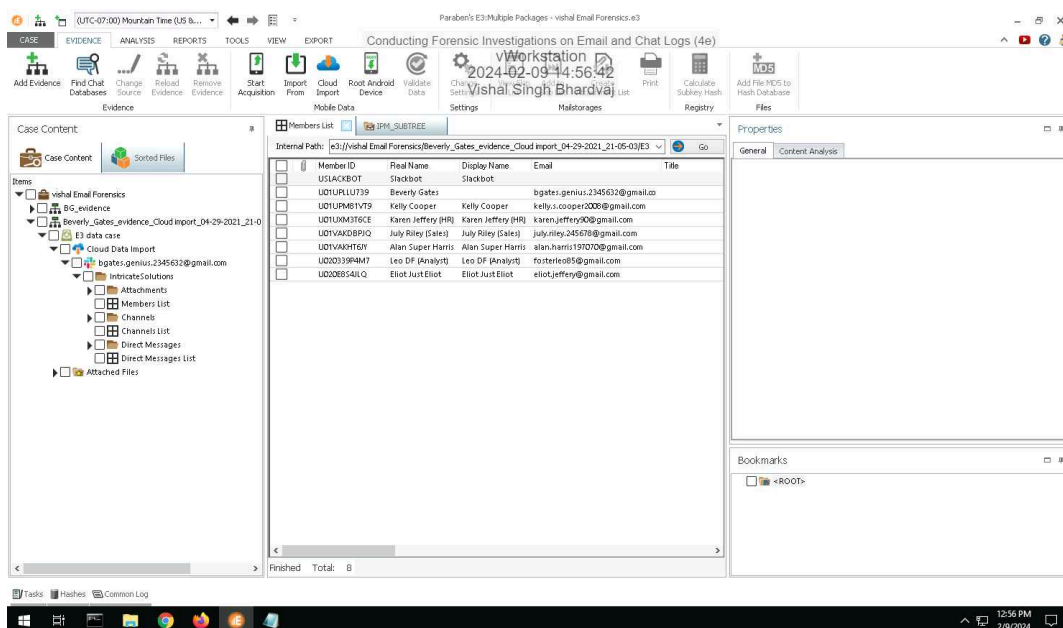
Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

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

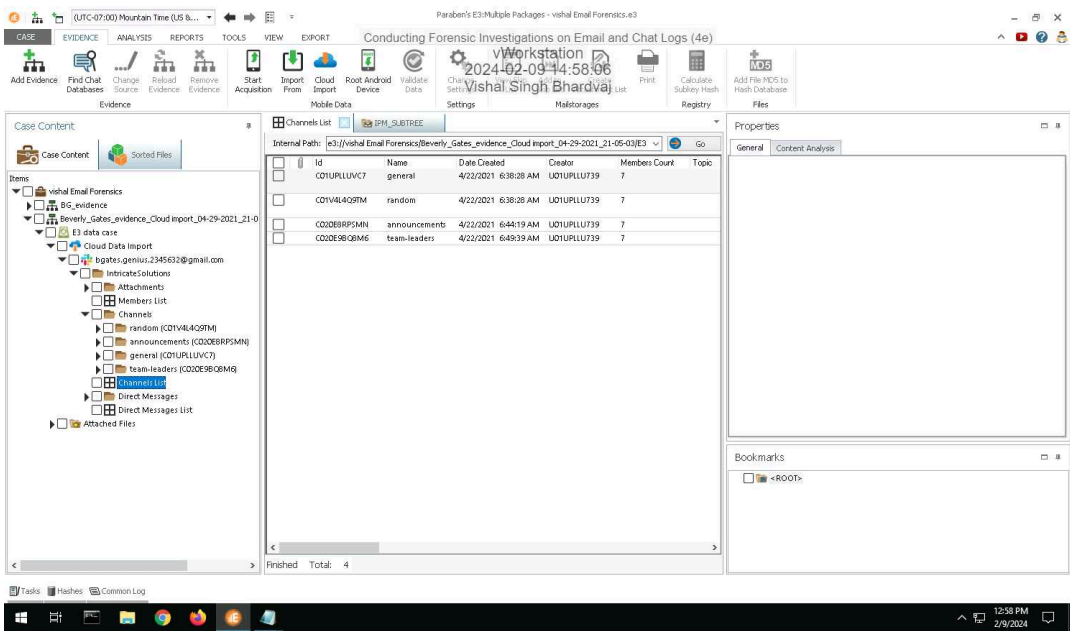


Part 3: Search for Evidence in a Slack Database

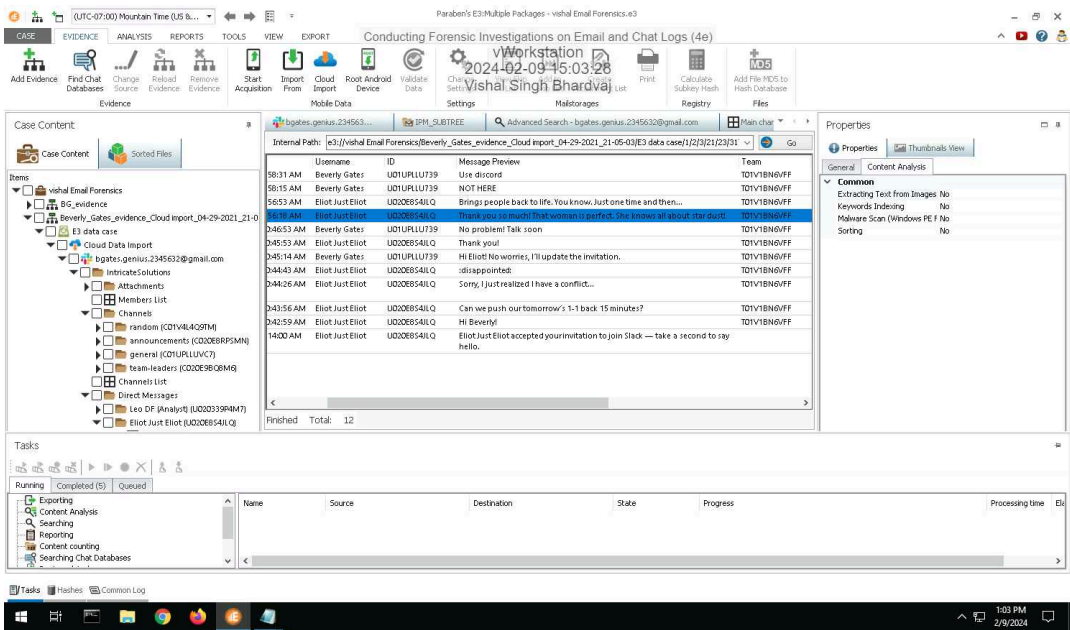
7. Make a screen capture showing the members of the IntricateSolutions workspace.



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



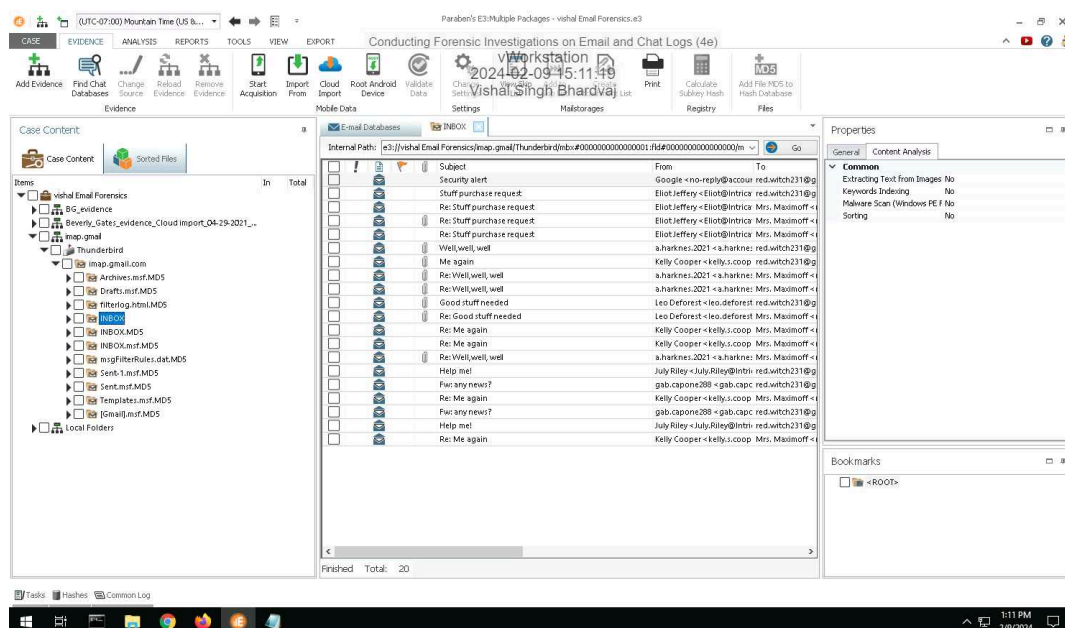
13. Make a screen capture showing the conversation contents.



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.

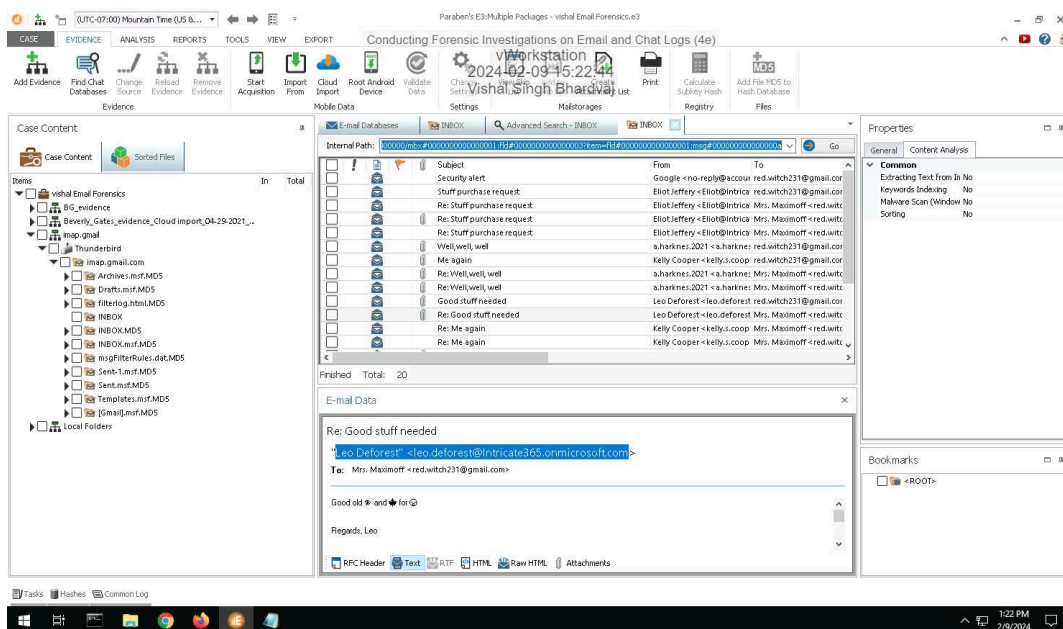
Sender's email address- a.harkens.2021@protonmail.com

mail server name - mail-40132.protonmail.ch(mail-40132.protonmail.ch)

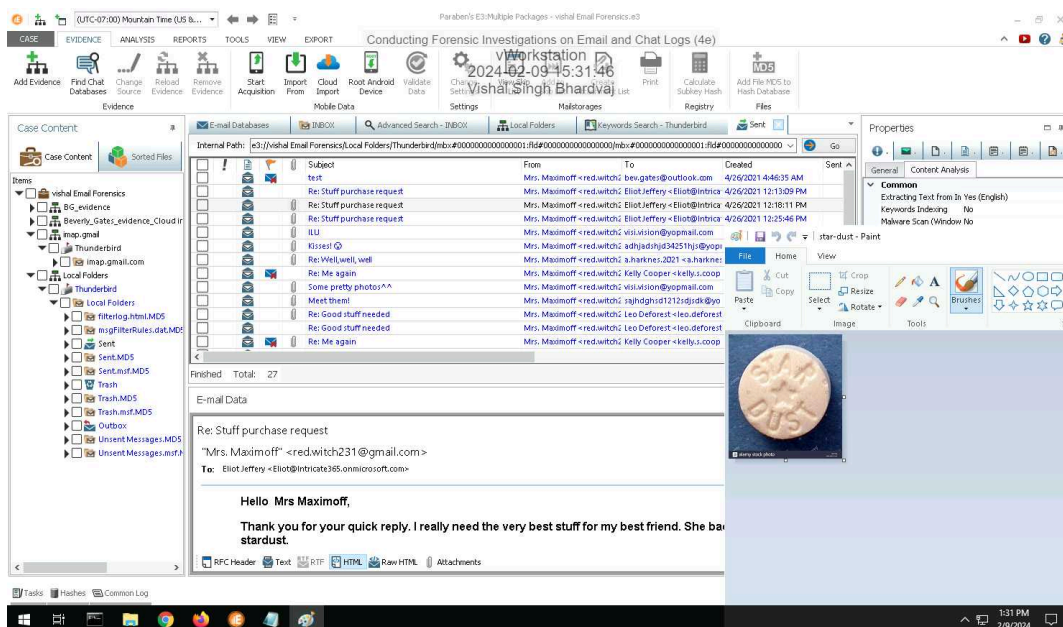
mail server IP address - 185.70.40.132

Part 2: Search for Evidence in a Thunderbird Database

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



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

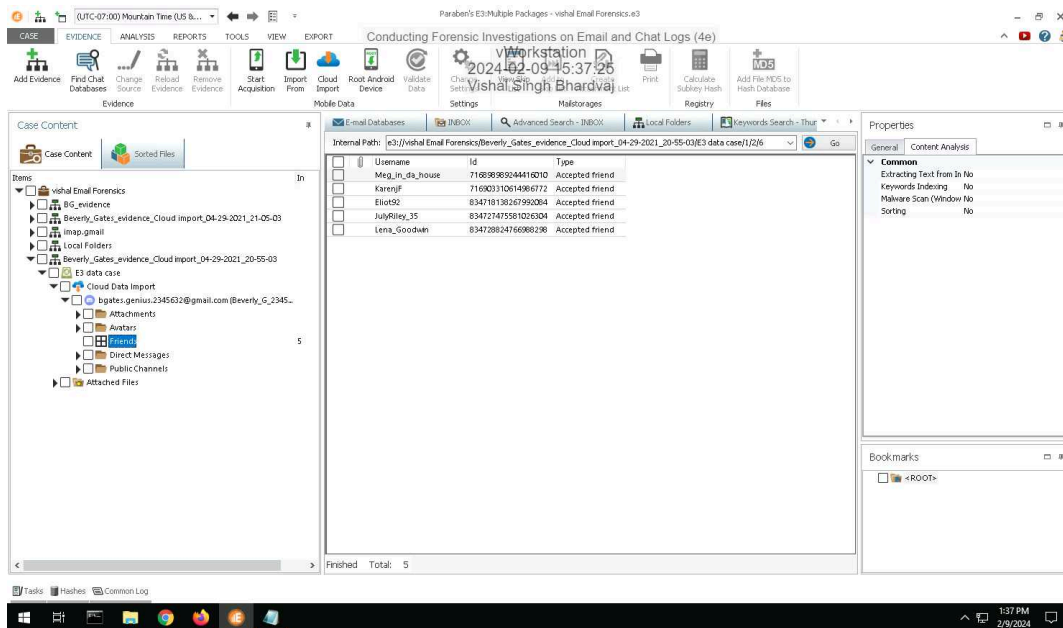


Part 3: Search for Evidence in a Discord Database

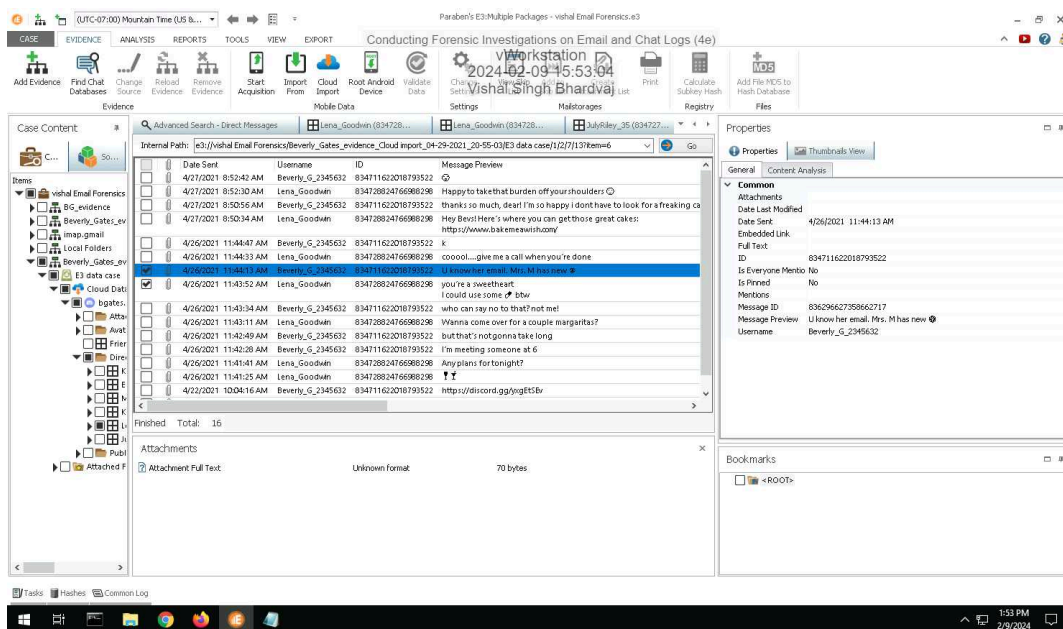
Conducting Forensic Investigations on Email and Chat Logs (4e)

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

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



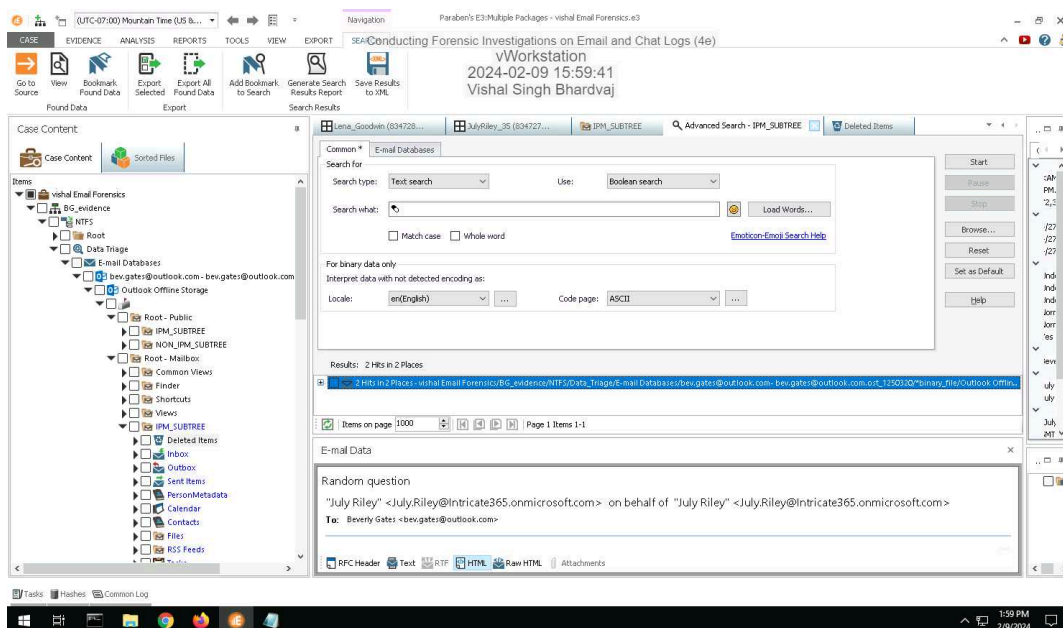
8. Make a screen capture showing the Lena Goodwin conversation.



Section 3: Challenge and Analysis

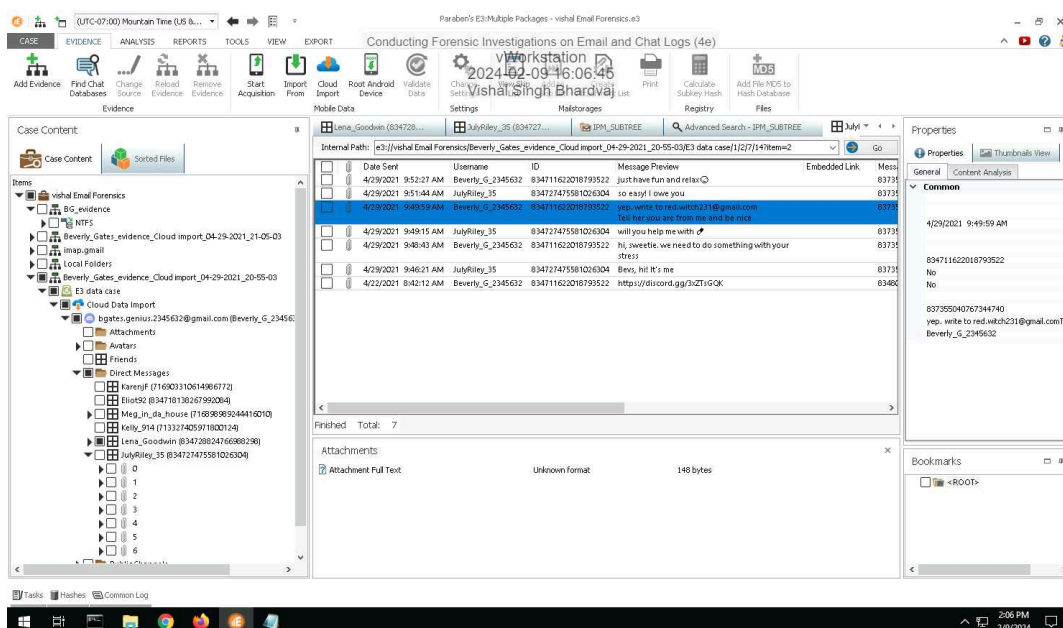
Part 1: Search for Additional Email Evidence

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



Part 2: Search for Additional Chat Evidence

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



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

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