

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

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

Student:

Matias Kun

Email:

rvh4zx@virginia.edu

Time on Task:

10 hours, 0 minutes

Progress:

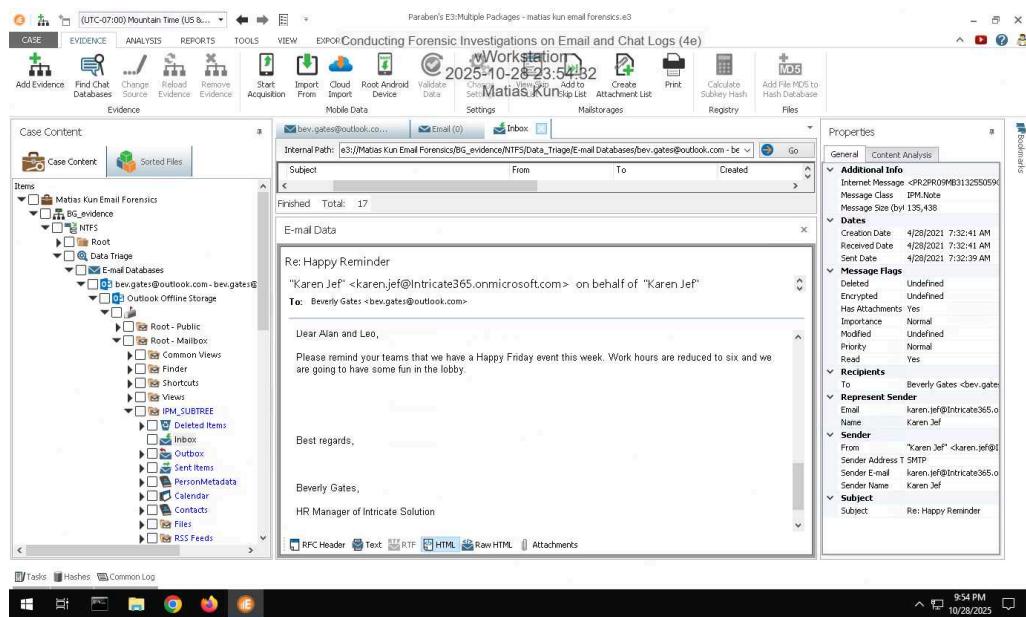
100%

Report Generated: Wednesday, October 29, 2025 at 12:09 AM

Section 1: Hands-On Demonstration

Part 1: Analyze Email Headers

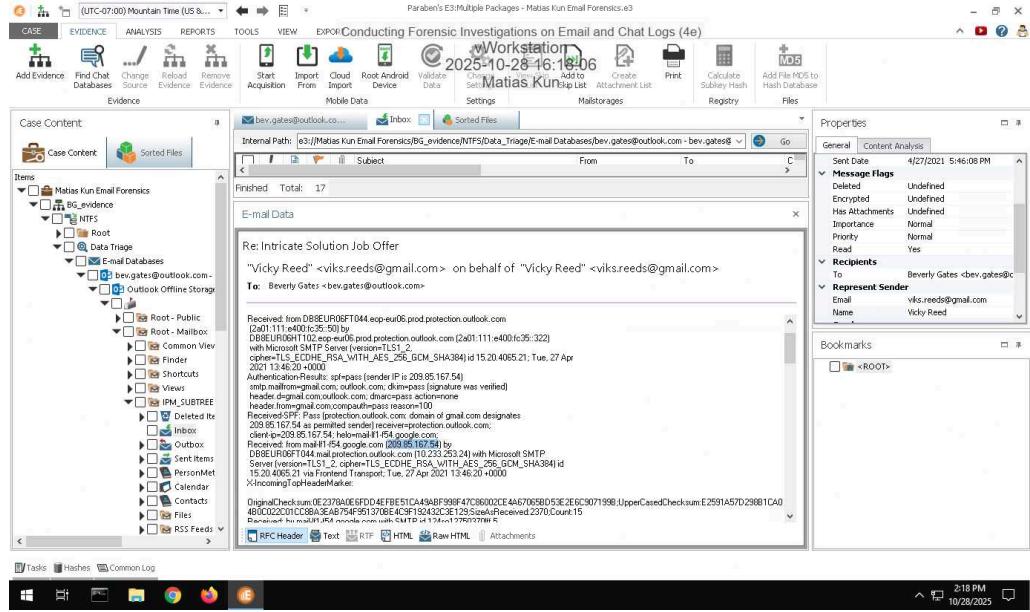
17. Make a screen capture showing the Happy Reminder email in the Text Viewer and Timestamp in the Properties pane.



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

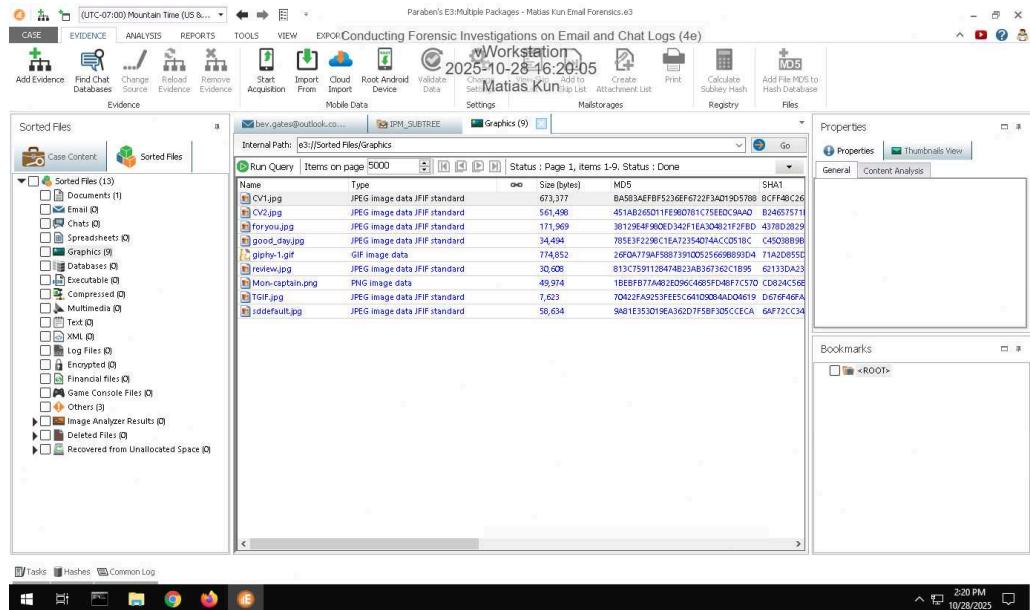
Digital Forensics, Investigation, and Response, Fourth Edition - Lab 07

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.

The screenshot shows the Paraben's E3 Forensic tool interface. The main pane displays an email message titled "RE: Team Evaluation". The message body contains the text: "I might report you to the actual Captain, aka Mr. Big Boss. Beware of his wrath!". The recipient is listed as "Mr. Harris Malone <mr.harris@intricate365.onmicrosoft.com>". The properties pane on the right shows the following details:

General	Content Analysis
Sent Date	4/27/2021 7:18:52 AM
Message Flags	Deleted: Undefined, Encrypted: Undefined, Importance: Normal, Priority: Normal, Read: Yes
Recipients	To: Mr. Harris Malone <mr.harris@intricate365.onmicrosoft.com>
Represent Sender	Email: bev.gates@outlook.com, Name: bev.gates@outlook.com

Part 3: Search for Evidence in a Slack Database

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

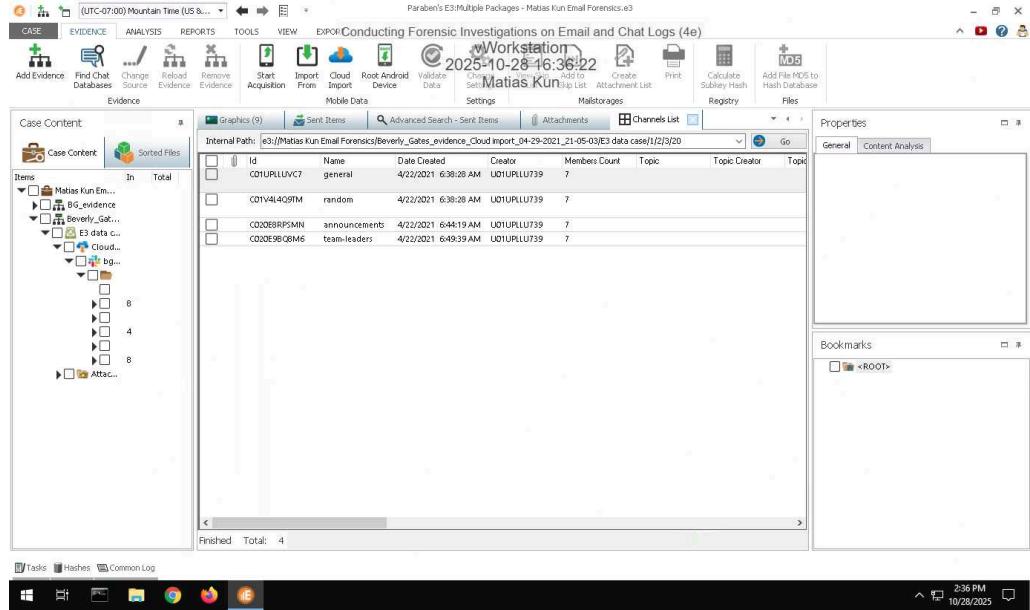
The screenshot shows the Paraben's E3 Forensic tool interface. The main pane displays a table titled "Members List" showing the following data:

Member ID	Real Name	Display Name	Email	Title	Phone	Skype
U01WFLU739	Beverly Gates	Stackbot	bgates.genius+2345672@gmail.co			
U01WFLW0179	Kelly Cooper	Kelly Cooper	kelly.cooper+2000@gmail.co			
U01WFLM37CE	Karen Jeffrey (HR)	Karen Jeffrey (HR)	karen.jeffrey00@gmail.co			
U01WFLA8PQ	Judy Riley (Sales)	Judy Riley (Sales)	judy.riley+245769@gmail.co			
U01WFLH1RQ	Asha Super Hamz	Asha Super Hamz	ashaham1970D@gmail.co			
U0203394MT	Leo DF Analyst	Leo DF Analyst	fosterled85@gmail.co			
U020654ULQ	Elliot Just Elliot	Elliot Just Elliot	elliot.jeffery@gmail.co			

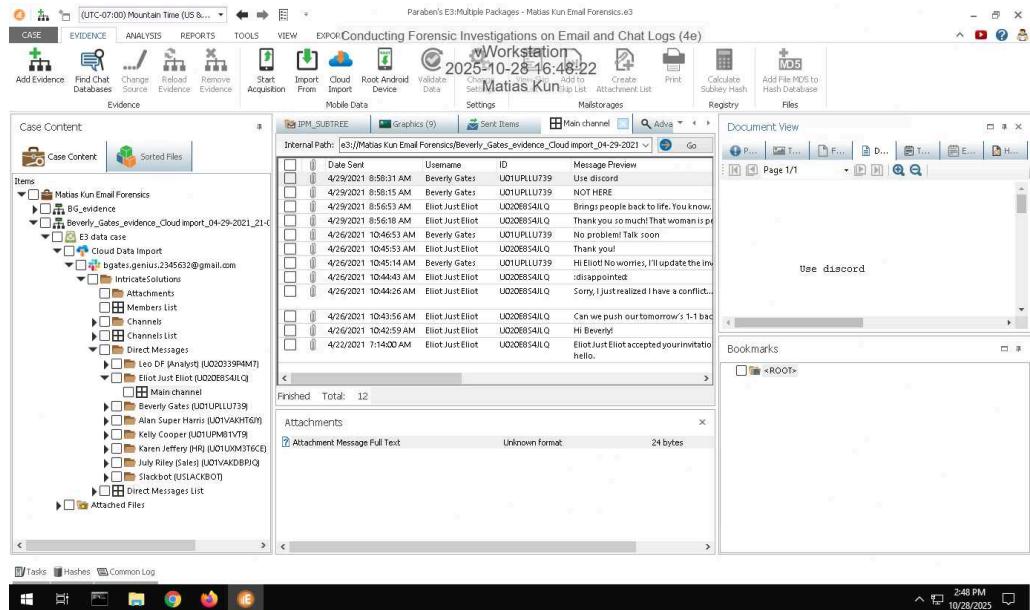
Conducting Forensic Investigations on Email and Chat Logs (4e)

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.



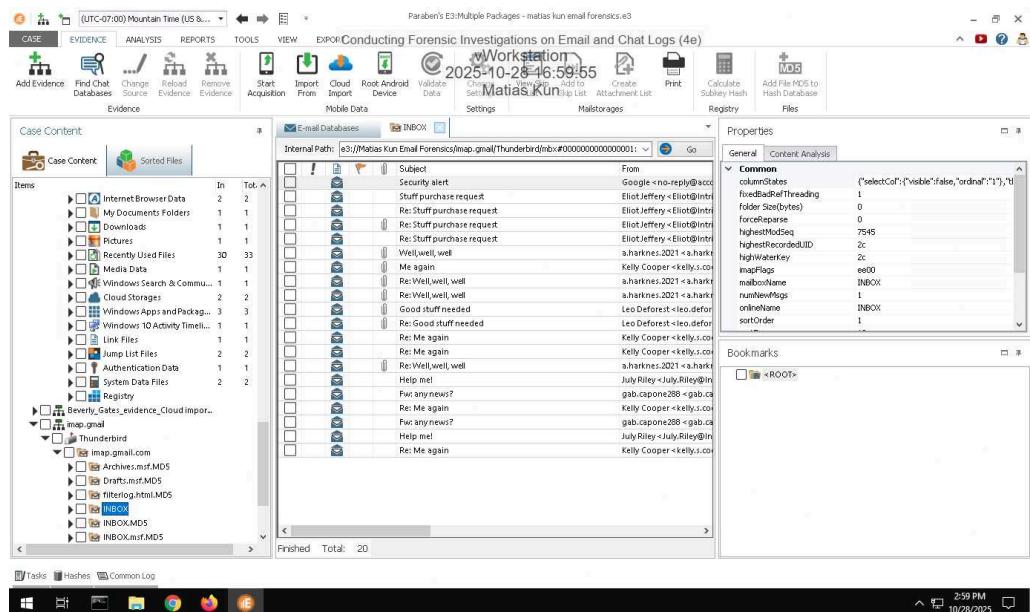
Conducting Forensic Investigations on Email and Chat Logs (4e)

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

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.

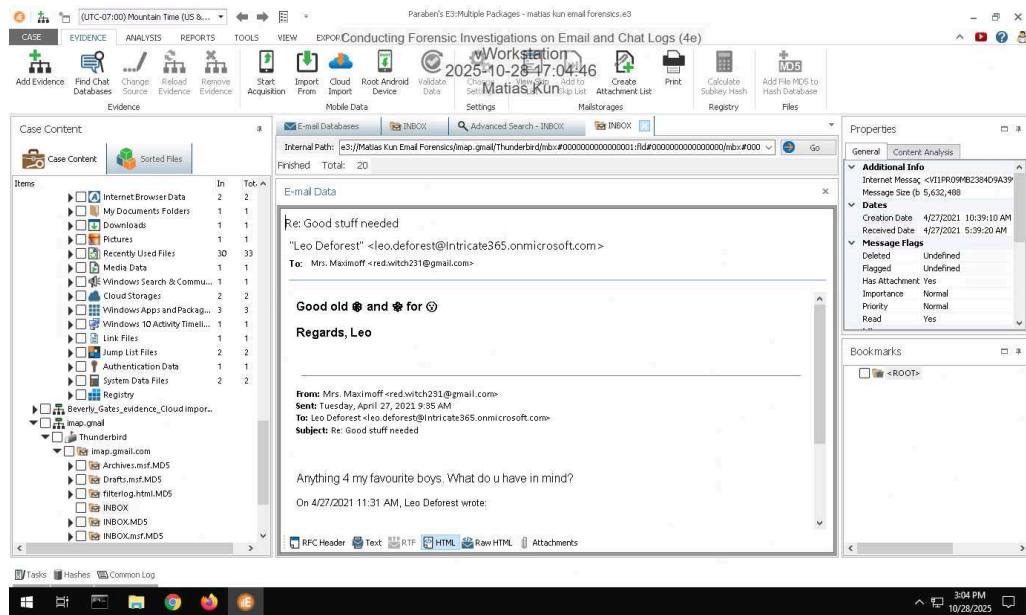
The sender's email is a.harknes.2021@protonmail.com, and the email service provider is Proton Mail. The IP address from the sender is 185.70.40.132.

Part 2: Search for Evidence in a Thunderbird Database

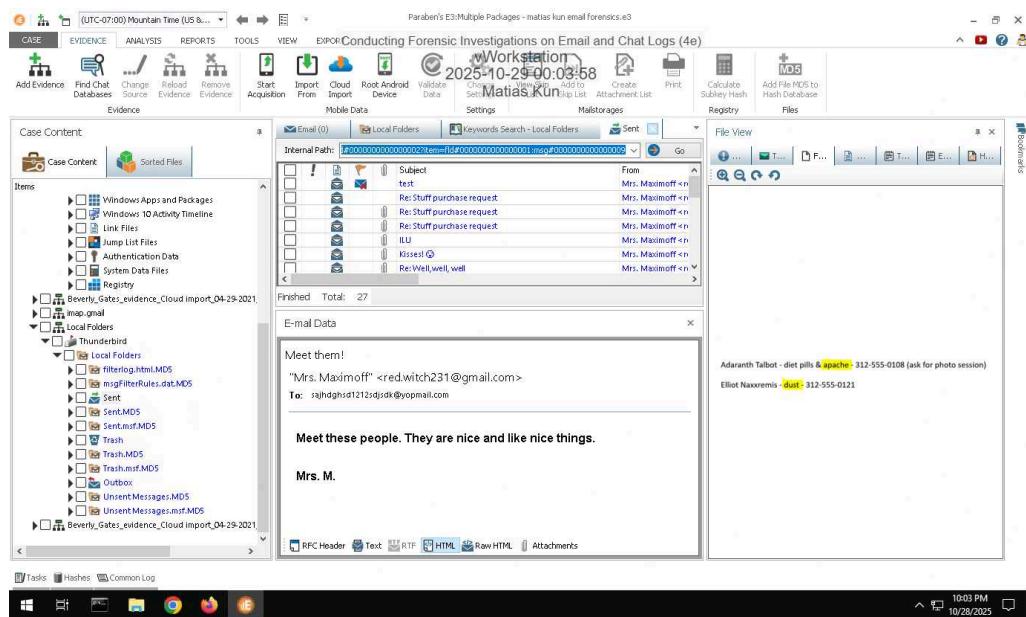
Conducting Forensic Investigations on Email and Chat Logs (4e)

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

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



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.

UTC-07:00 Mountain Time (US & Canada) Paraben's E3:Multiple Packages - matias.kun@email.forensics.e3

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

Add Evidence Find Chat Databases Change Source Reload Evidence Remove Evidence Start Acquisition Import From Cloud Root Android Validate Data Change Settings Mailstorages Registry Files

Evidence

Case Content

Case Content Sorted Files

Items

- Matias Kun Email Forensics
 - B6_evidence
 - Beverly_Gates_evidence_Cloud import...
 - imap.gmail
 - Local Folders
 - Beverly_Gates_evidence_Cloud imp...
 - E3 data case
 - Cloud Data Import
 - bgtates.genius.2345632@g...
 - Attachments
 - Avatars
 - Friends
 - Direct Messages
 - Public Channels
- Attached Files

Friends

Internal Path: es_evidence_Cloud import_04-29-2021_20-55-03/E3 data case/1/2/6

	Username	Id	Type
	Meg_in_da_house	716898989244416010	Accepted friend
	KarenJF	716903310614986772	Accepted friend
	Eliot92	834718138267992064	Accepted friend
	JulyRiley_35	834727475581026304	Accepted friend
	Lena_Goodwin	834728624766988298	Accepted friend

Finished Total: 5

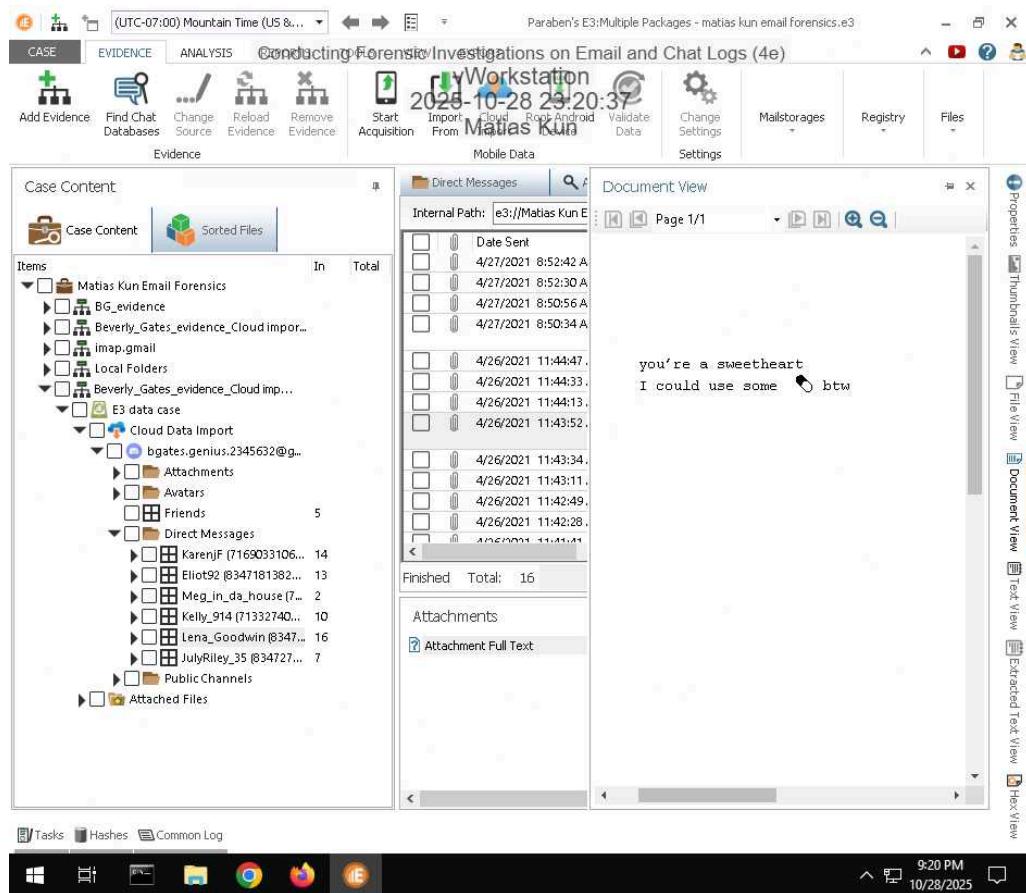
Tasks Hashes Common Log

9:15 PM 10/28/2025

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

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

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



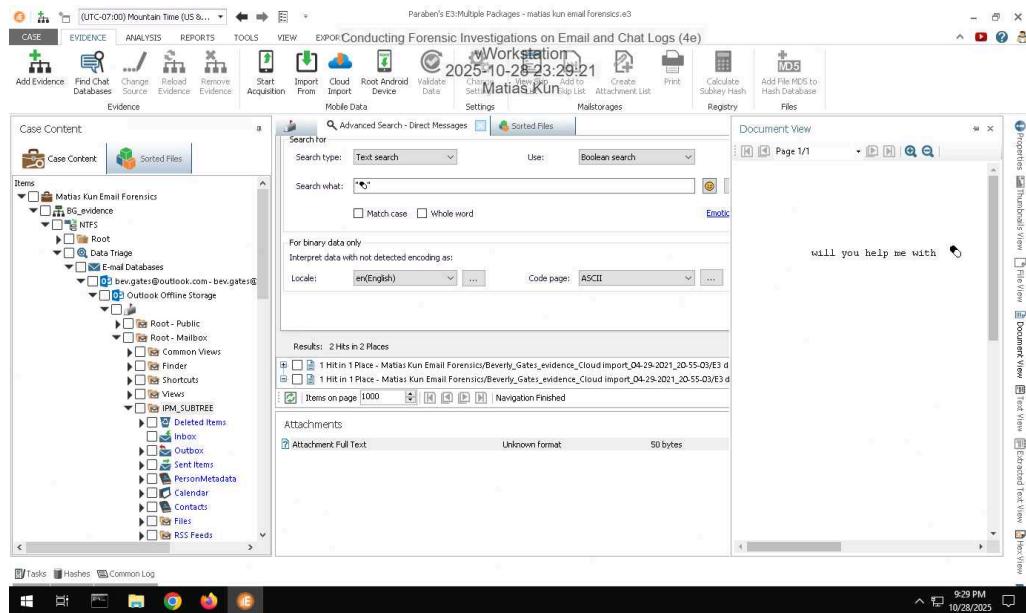
Conducting Forensic Investigations on Email and Chat Logs (4e)

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

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

