

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

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

Student:

Jose Cruz

Email:

jose.cruz2@udc.edu

Time on Task:

9 hours, 48 minutes

Progress:

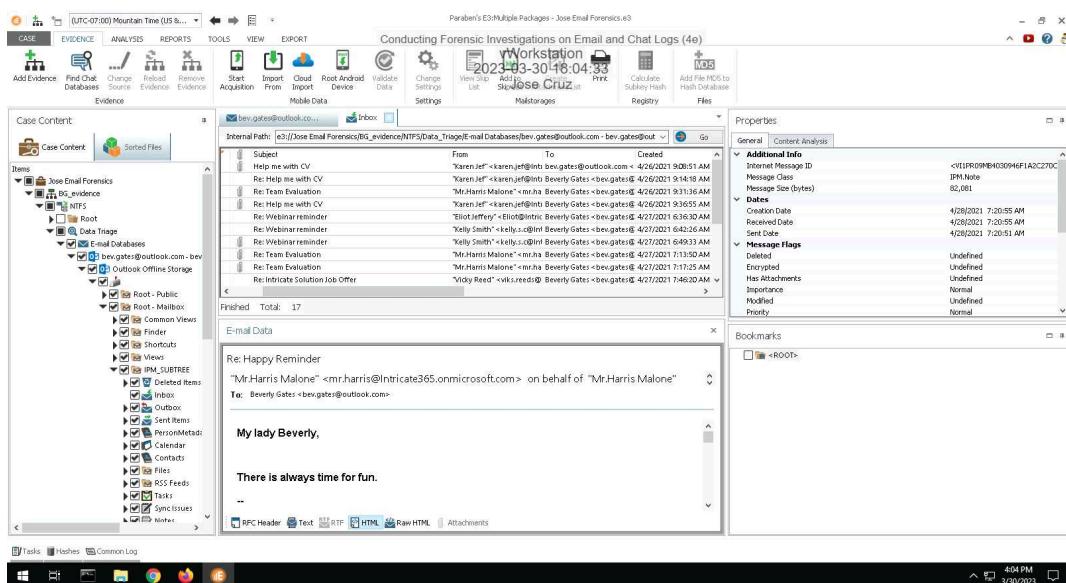
100%

Report Generated: Monday, April 10, 2023 at 10:35 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.

The screenshot shows the EnCase Evidence interface. The top menu bar includes CASE, EVIDENCE, ANALYSIS, REPORTS, TOOLS, and VIEW. The evidence tab is selected. The main pane displays an email inbox from 'bev.gates@outlook.com'. The left sidebar shows a tree view of the evidence structure, including 'Data Triage', 'E-mail Databases' (selected), and 'Outlook Offline Storage'. The right pane shows the properties of an email message, specifically focusing on the 'Sender' section which lists 'Vicky Reed' as the recipient. The bottom status bar shows the date as 3/30/2023 and the time as 4:35 PM.

Part 2: Search for Evidence in an Outlook Database

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

The screenshot shows the EnCase Evidence interface with a search query for 'Graphics' in progress. The top menu bar and evidence tabs are identical to the previous screenshot. The main pane displays a list of files found in the 'Graphics' category, with 9 items listed. The left sidebar shows the evidence structure. The right pane shows the properties of one of the files, 'CV1.jpg', including its type (JPEG image data JFIF standard), size (673,377 bytes), MD5 hash, and SHA1 hash. The bottom status bar shows the date as 3/30/2023 and the time as 4:42 PM.

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 software interface. The main window displays an email message from "Beverly Gates" to "Karen.Jeffrey@Intric86.onmicrosoft.com". The message subject is "RE: Team Evaluation". The body of the email contains the text: "I might report you to the actual Captain, aka Mr. Big Boss. Beware of his wrath!" Below the email, there is a preview pane showing the raw HTML code of the message.

From	To	Created
"Beverly Gates" <bev.gates@outlook.com>	Karen.Jeffrey@Intric86.onmicrosoft.com	4/26/2021 9:13:00 AM
"Beverly Gates" <bev.gates@outlook.com>	Karen.Jeffrey@Intric86.onmicrosoft.com	4/26/2021 9:15:23 AM
"Beverly Gates" <bev.gates@outlook.com>	mr.harris@intric86.onmicrosoft.com	4/26/2021 9:25:06 AM
"Beverly Gates" <bev.gates@outlook.com>	kelly.s.cooper2008@gmail.com	4/27/2021 6:19:20 AM
"Beverly Gates" <bev.gates@outlook.com>	Flint.Leffery<Flint.Leffery@Intric86.onmicrosoft.com>	4/27/2021 6:37:46 AM

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 software interface with a "Members List" view. The table displays the following information for each member:

Member ID	Real Name	Display Name	Email	Title	Phone	Skype	Team	Status
USLACKBOT	Slackbot	Slackbot	bgates.genius.2045@outlook.com				T01V1BN6VFF	Online
U01UPHJU729	Beverly Gates	bogates.genius.2045@outlook.com					T01V1BN6VFF	Online
U01UPM5Y179	Kelly Cooper	Kelly Cooper	kelly.s.cooper2008@gmail.com				T01V1BN6VFF	Online
U01UMK3T6CE	Karen Jeffery (HR)	Karen Jeffery (HR)	Karen.Jeffery9@gmail.com				T01V1BN6VFF	Online
U01VAKD8P1Q	July Riley (Sales)	July Riley (Sales)	july.riley.245678@gmail.com				T01V1BN6VFF	Online
U01VAKHTG1Q	Alan Super Harris	Alan Super Harris	alan.harris197070@gmail.com				T01V1BN6VFF	Online
U02039P4M7	Leo DF (Analyst)	Leo DF (Analyst)	fosterleo85@gmail.com				T01V1BN6VFF	Online
U020E854ILQ	Eliot Just Eliot	Eliot Just Eliot	eliot.jeffery@gmail.com				T01V1BN6VFF	Online

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.

The screenshot shows the Paraben's E3:Multiple Packages - Jose Email Forensics interface. The main window displays the 'Channels List' tab under the 'Evidence' tab. The left sidebar shows the 'Case Content' tree, which includes 'Jose Email Forensics', 'BG_evidence', 'Beverly_Gates_evidence_Cloud Import_04-29-2...', and 'E3 data case'. The 'E3 data case' node has a 'Cloud Data Import' folder containing a 'bgates.genius:2345632@gmail.com' folder, which further contains an 'IntricateSolutions' folder and a 'Channels' folder. The 'Channels' folder lists four channels: 'random', 'announcements', 'general', and 'team-leaders'. The 'general' channel has 8 members. The 'Channels List' table shows the following data:

ID	Name	Date Created	Creator	Members Count	Topic	Topic Co
CO1UPLLUV7	general	4/22/2021 6:38:36 AM	U01UPLLU739	7		
CD1VAL4Q9TM	random	4/22/2021 6:38:28 AM	U01UPLLU739	7		
CO20E8RPSMN	announcements	4/22/2021 6:44:19 AM	U01UPLLU739	7		
CO20E9BQ8M6	team-leaders	4/22/2021 6:49:39 AM	U01UPLLU739	7		

13. Make a screen capture showing the conversation contents.

The screenshot shows the Paraben's E3:Multiple Packages - Jose Email Forensics interface. The main window displays the 'Main channel' tab under the 'Evidence' tab. The left sidebar shows the 'Case Content' tree, similar to the previous screenshot. The 'E3 data case' node has a 'Cloud Data Import' folder containing a 'bgates.genius:2345632@gmail.com' folder, which further contains an 'IntricateSolutions' folder and a 'Channels' folder. The 'Channels' folder lists four channels: 'random', 'announcements', 'general', and 'team-leaders'. The 'general' channel has 8 members. The 'Main channel' table shows the following conversation logs:

Date Sent	Username	ID	Message Preview	Team
4/29/2021 8:58:31 AM	Beverly Gates	U01UPLLU739	Use discord	T01V1BN6VF
4/29/2021 8:58:15 AM	Beverly Gates	U01UPLLU739	NOT HERE	T01V1BN6VF
4/29/2021 8:56:53 AM	Eliot Just Eliot	U020E854UQ	Brings people back to life. You know. Just one time and then...	T01V1BN6VF
4/29/2021 8:56:18 AM	Eliot Just Eliot	U020E854UQ	Thank you so much! That woman is perfect. She knows all about star dust!	T01V1BN6VF
4/26/2021 10:46:53 AM	Beverly Gates	U01UPLLU739	No problem! Talk soon	T01V1BN6VF
4/26/2021 10:45:53 AM	Eliot Just Eliot	U020E854UQ	Thank you!	T01V1BN6VF
4/26/2021 10:45:14 AM	Beverly Gates	U01UPLLU739	Hi Eliot No worries, I'll update the invitation.	T01V1BN6VF
4/26/2021 10:44:43 AM	Eliot Just Eliot	U020E854UQ	:disappointed:	T01V1BN6VF
4/26/2021 10:44:26 AM	Eliot Just Eliot	U020E854UQ	Sorry, I just realized I have a conflict...	T01V1BN6VF
4/26/2021 10:43:56 AM	Eliot Just Eliot	U020E854UQ	Can we push our tomorrow's 1-1 back 15 minutes?	T01V1BN6VF
4/26/2021 10:42:59 AM	Eliot Just Eliot	U020E854UQ	Hi Beverly!	T01V1BN6VF

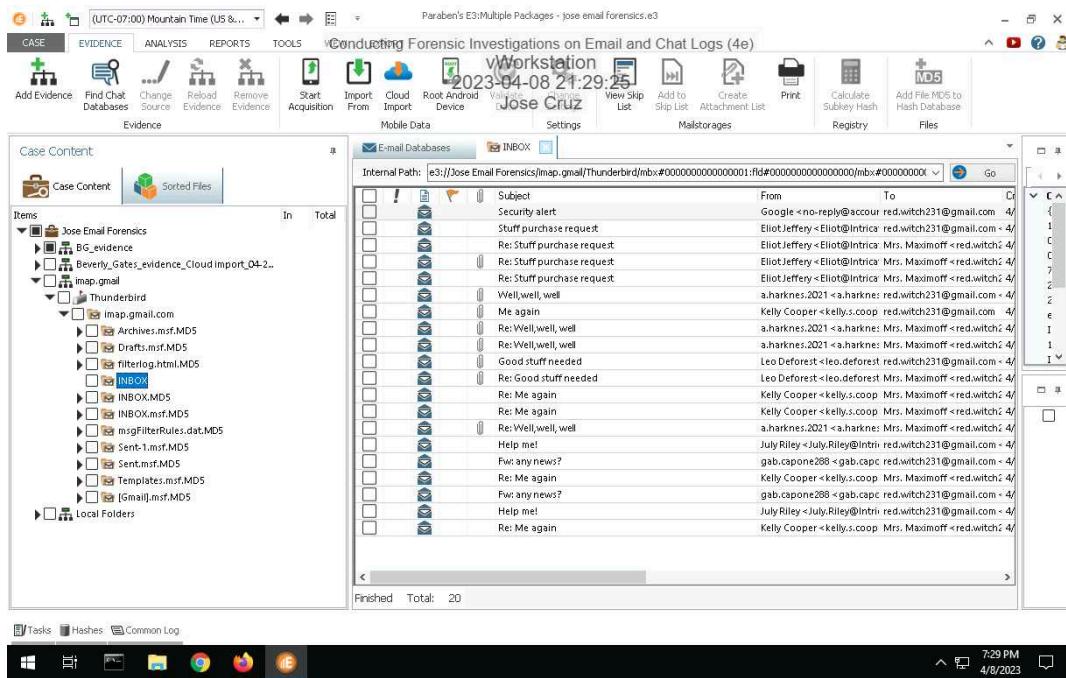
Conducting Forensic Investigations on Email and Chat Logs (4e)

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.

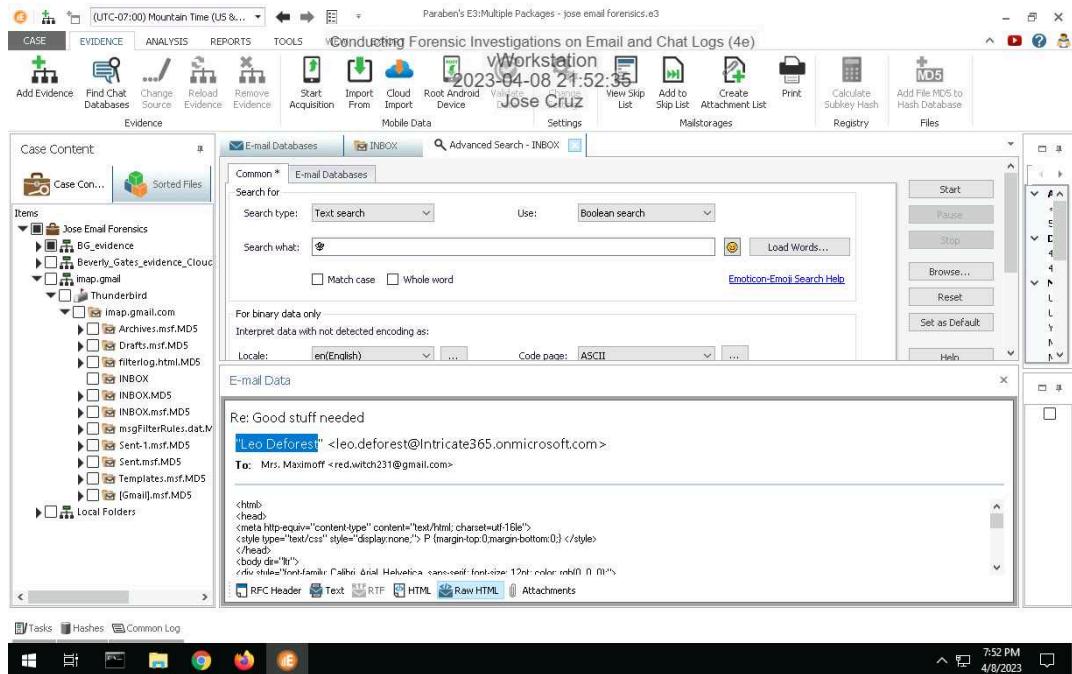
The senders email address is, a.harknes.2021@protonmail.com. Mail server name is "a.harknes.2021". Finally, the mail server IP address is, 185.70.40.132.

Part 2: Search for Evidence in a Thunderbird Database

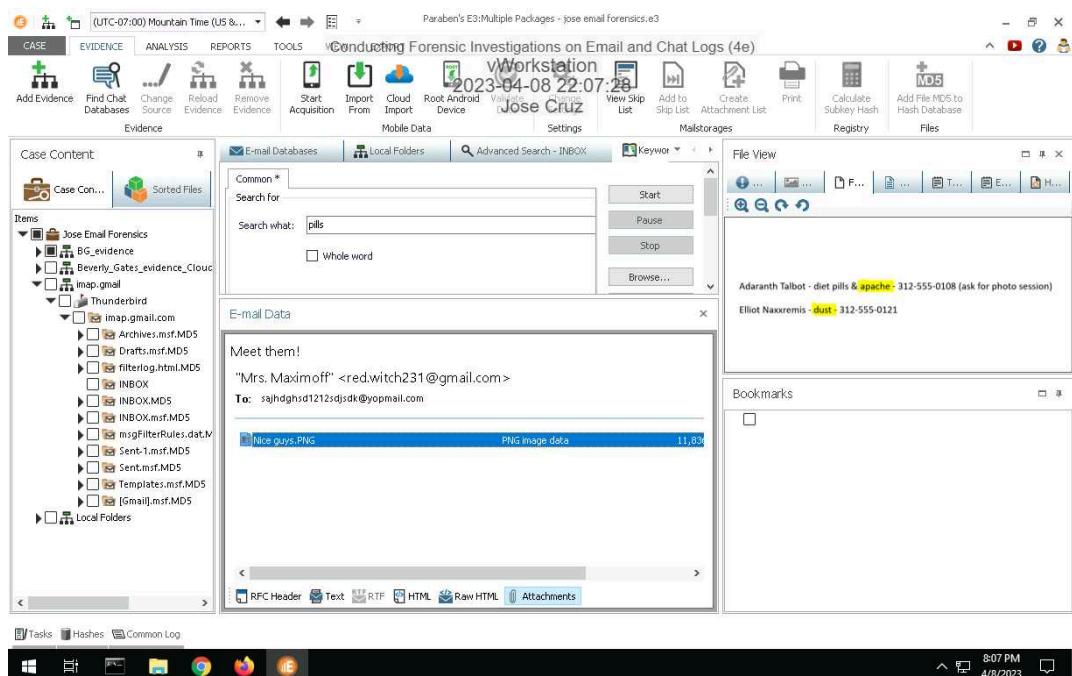
Conducting Forensic Investigations on Email and Chat Logs (4e)

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.

The screenshot shows the Paraben's E3 forensic tool interface. The main window displays a 'Members List' for a specific Slack workspace. The table includes columns for Member ID, Real Name, Display Name, and Email. The list contains several entries, including Beverly Gates, Kelly Cooper, Karen Jeffery (HR), July Riley (Sales), Alan Super Harris, Leo DF (Analyst), and Eliot Just Eliot. The left sidebar shows the case content structure, including 'Beverly_Gates_evidence_Cloud import_04-29-2023'. The bottom status bar indicates the date as 4/10/2023 and the time as 8:24 PM.

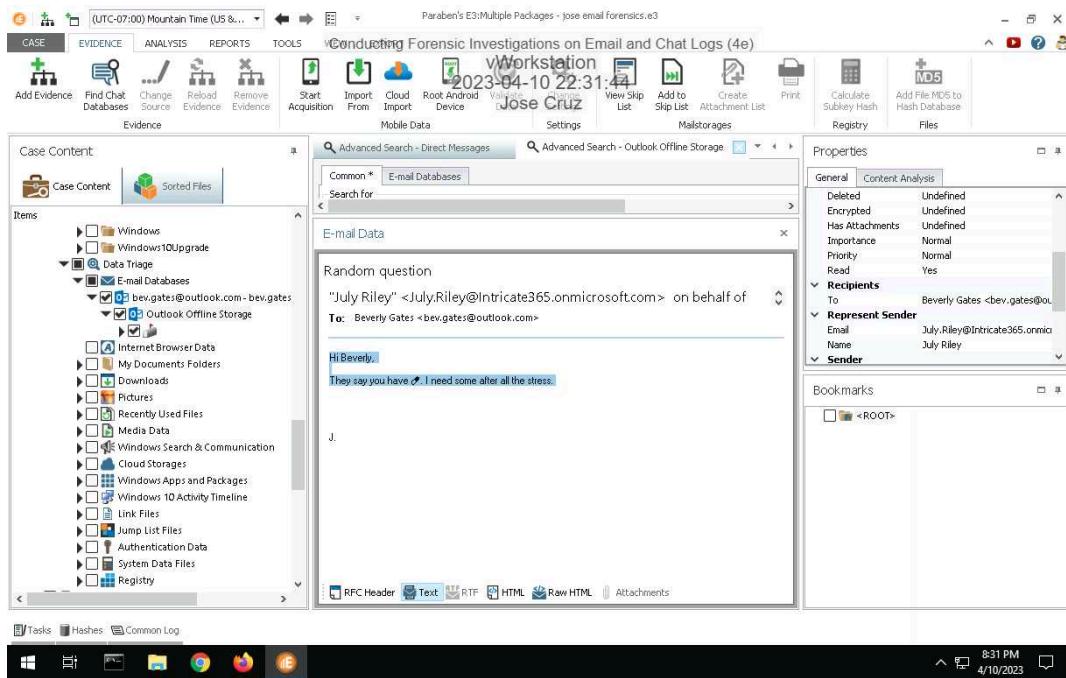
8. Make a screen capture showing the Lena Goodwin conversation.

The screenshot shows the Paraben's E3 forensic tool interface with a search function active. The search term 'Lena Goodwin' is entered in the 'Search what:' field under the 'Advanced Search - Direct Messages' tab. The results pane shows '0 Hits in 0 Places'. The left sidebar shows the case content structure, including 'Beverly_Gates_evidence_Cloud import_04-29-2023'. The bottom status bar indicates the date as 4/10/2023 and the time as 8:28 PM.

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

