| | |
|---|---|
| Student:<br>muhammad zahid | Email:<br>zahid1mz@cmich.edu |

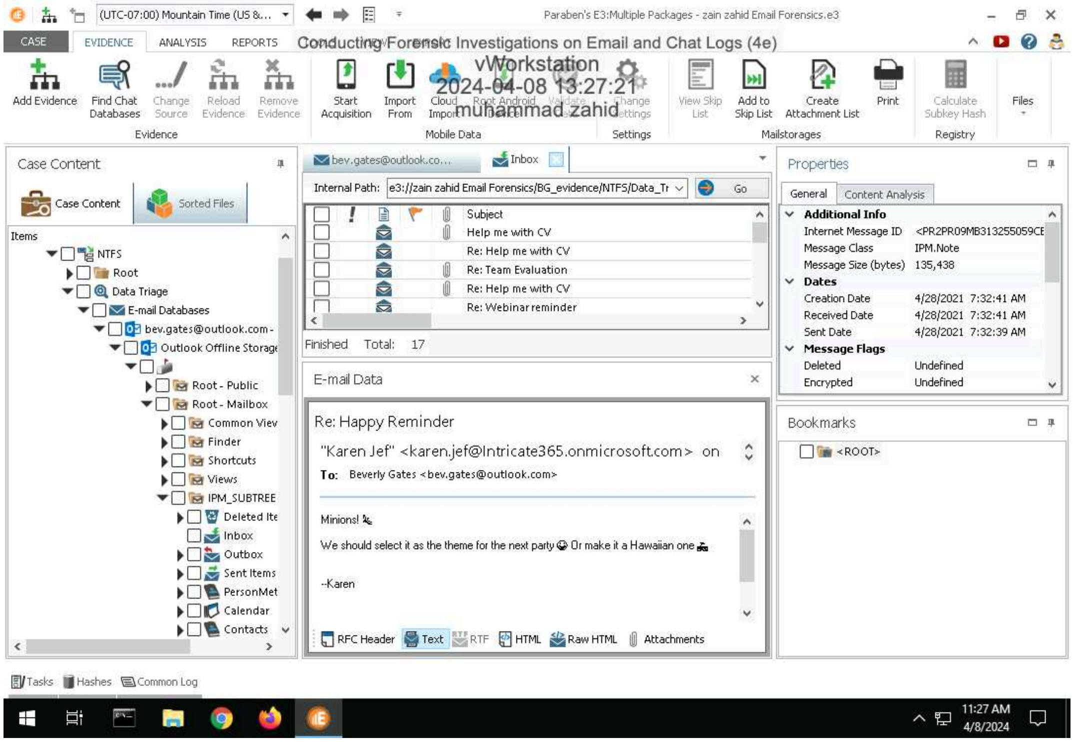
| | |
|---|---|
| Time on Task:<br>3 hours, 56 minutes | Progress:<br>100% |

Report Generated: Monday, April 8, 2024 at 3:15 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**.



Internal Path: e3://zain zahid Email Forensics/BG_evidence/NTFS/Data_Tr

| Subject |
|---|
| Help me with CV |
| Re: Help me with CV |
| Re: Team Evaluation |
| Re: Help me with CV |
| Re: Webinar reminder |

Finished Total: 17

| Additional Info | |
|---|---|
| Internet Message ID | <PR2PR09MB313255059CE |
| Message Class | IPM.Note |
| Message Size (bytes) | 135,438 |
| **Dates** | |
| Creation Date | 4/28/2021 7:32:41 AM |
| Received Date | 4/28/2021 7:32:41 AM |
| Sent Date | 4/28/2021 7:32:39 AM |
| **Message Flags** | |
| Deleted | Undefined |
| Encrypted | Undefined |

Re: Happy Reminder

"Karen Jef" <karen.jef@Intricate365.onmicrosoft.com> on

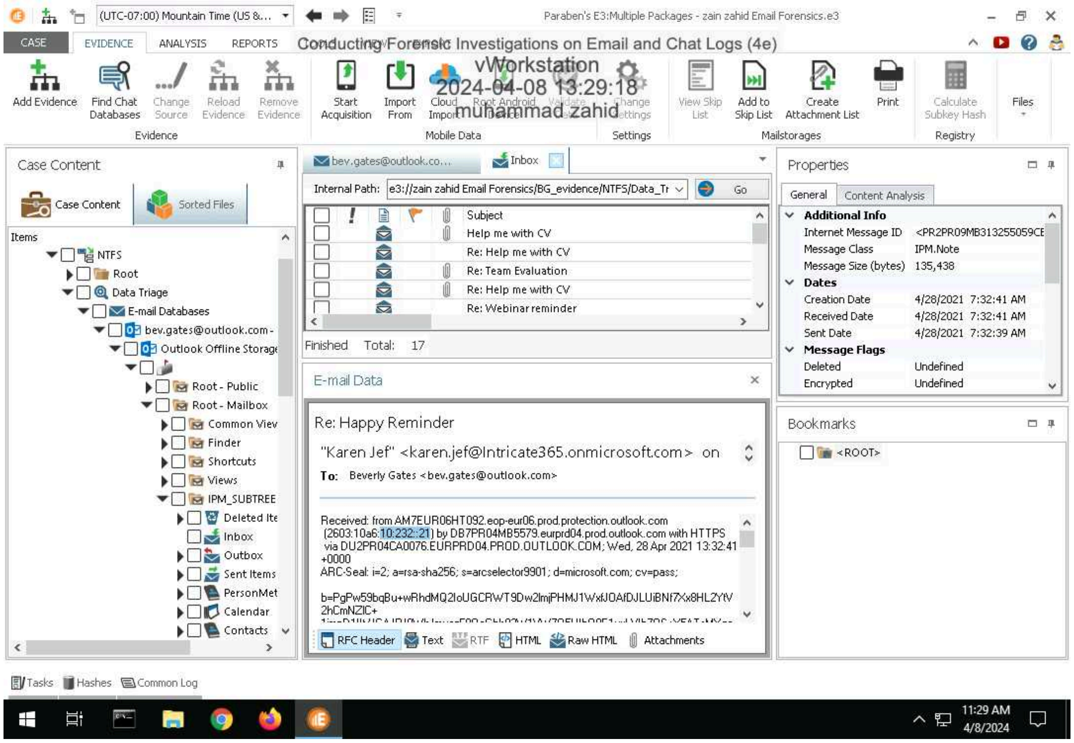
To: Beverly Gates <bev.gates@outlook.com>

Minions! 🦗

We should select it as the theme for the next party 😜 Or make it a Hawaiian one 🚣

--Karen

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



Internal Path: e3://zain zahid Email Forensics/BG_evidence/NTFS/Data_Tr

| Subject |
|---|
| Help me with CV |
| Re: Help me with CV |
| Re: Team Evaluation |
| Re: Help me with CV |
| Re: Webinar reminder |

Finished Total: 17

| | |
|---|---|
| **Additional Info** | |
| Internet Message ID | <PR2PR09MB313255059CE |
| Message Class | IPM.Note |
| Message Size (bytes) | 135,438 |
| **Dates** | |
| Creation Date | 4/28/2021 7:32:41 AM |
| Received Date | 4/28/2021 7:32:41 AM |
| Sent Date | 4/28/2021 7:32:39 AM |
| **Message Flags** | |
| Deleted | Undefined |
| Encrypted | Undefined |

Re: Happy Reminder

"Karen Jef" <karen.jef@Intricate365.onmicrosoft.com> on

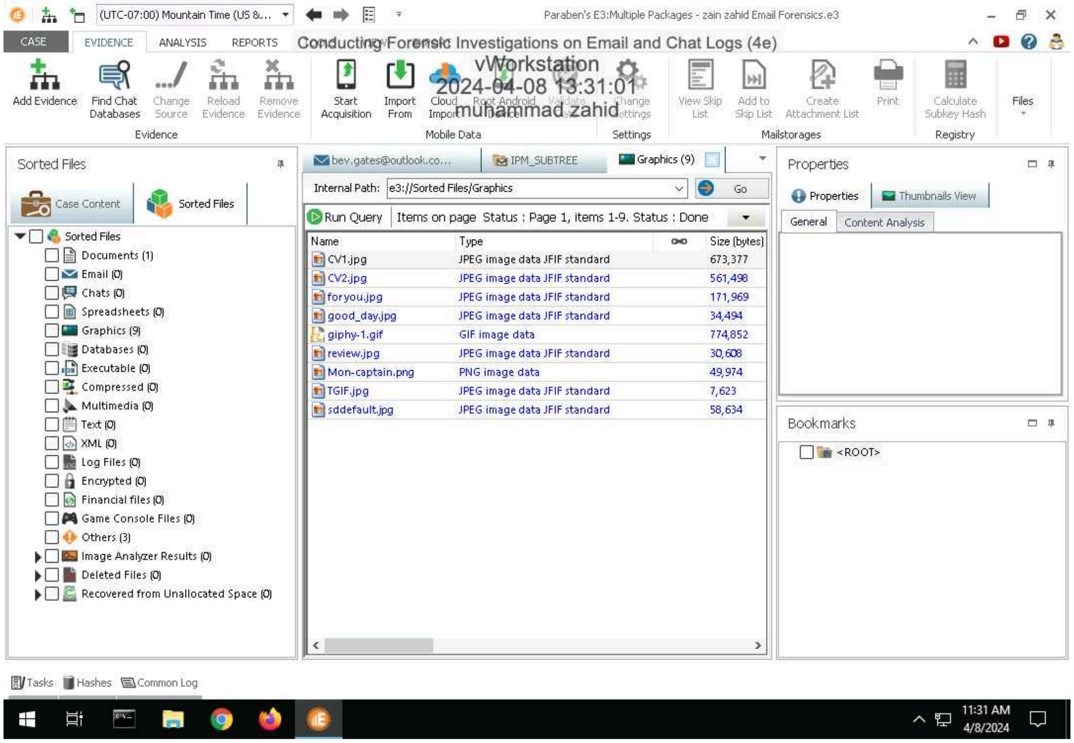
To: Beverly Gates <bev.gates@outlook.com>

```
Received: from AM7EUR06HT092.eop-eur06.prod.protection.outlook.com
 (2603:10a6:10:232::21) by DB7PR04MB5579.eurprd04.prod.outlook.com with HTTPS
 via DU2PR04CA0076.EURPRD04.PROD.OUTLOOK.COM; Wed, 28 Apr 2021 13:32:41
+0000
ARC-Seal: i=2; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cv=pass;

b=PgPw59bqBu+wRhdMQ2IoUGCRWT9Dw2lmjPHMJ1WxfJOAfDJLUiBNf7Xx8HL2YtV
2hCmNZIC+
```

## Part 2: Search for Evidence in an Outlook Database

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



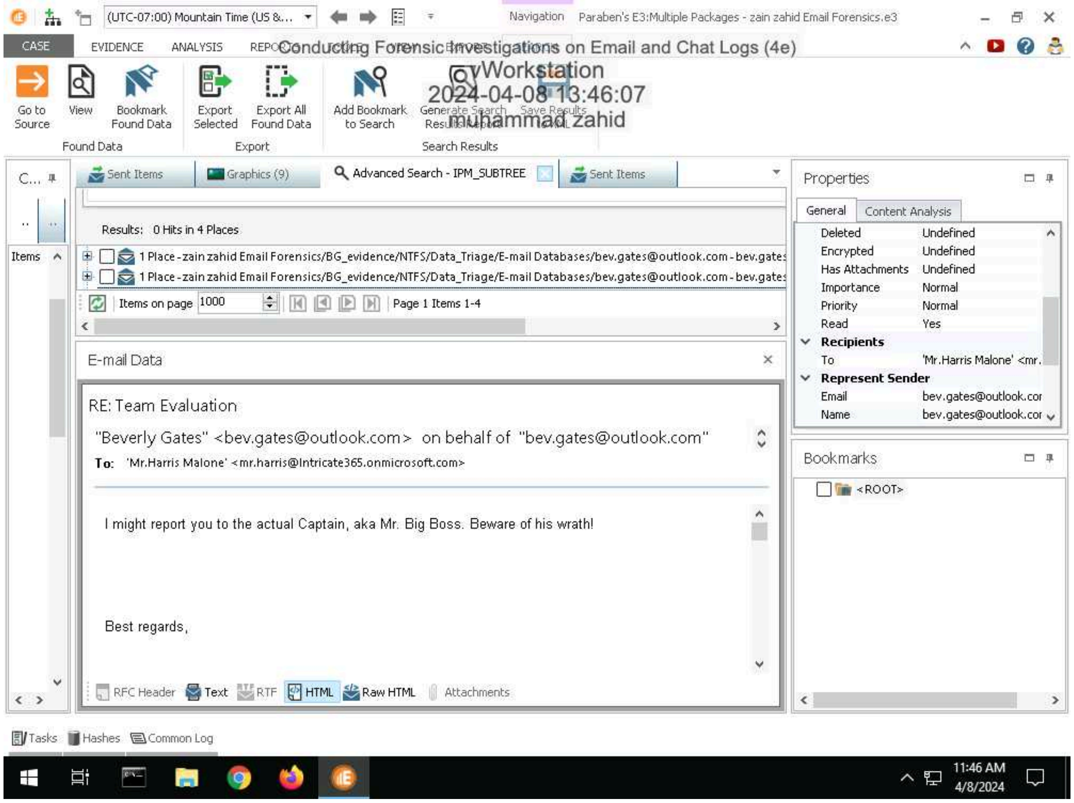
- □ Sorted Files
  - □ Documents (1)
  - □ Email (0)
  - □ Chats (0)
  - □ Spreadsheets (0)
  - □ Graphics (9)
  - □ Databases (0)
  - □ Executable (0)
  - □ Compressed (0)
  - □ Multimedia (0)
  - □ Text (0)
  - □ XML (0)
  - □ Log Files (0)
  - □ Encrypted (0)
  - □ Financial files (0)
  - □ Game Console Files (0)
  - □ Others (3)
  - □ Image Analyzer Results (0)
  - □ Deleted Files (0)
  - □ Recovered from Unallocated Space (0)

Internal Path: e3://Sorted Files/Graphics

Run Query | Items on page Status : Page 1, items 1-9. Status : Done

| Name | Type | | Size (bytes) |
|---|---|---|---|
| CV1.jpg | JPEG image data JFIF standard | | 673,377 |
| CV2.jpg | JPEG image data JFIF standard | | 561,498 |
| foryou.jpg | JPEG image data JFIF standard | | 171,969 |
| good_day.jpg | JPEG image data JFIF standard | | 34,494 |
| giphy-1.gif | GIF image data | | 774,852 |
| review.jpg | JPEG image data JFIF standard | | 30,608 |
| Mon-captain.png | PNG image data | | 49,974 |
| TGIF.jpg | JPEG image data JFIF standard | | 7,623 |
| sddefault.jpg | JPEG image data JFIF standard | | 58,634 |

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



Conducting Forensic Investigations on Email and Chat Logs (4e)
vWorkstation
2024-04-08 13:46:07
muhammad zahid

Results: 0 Hits in 4 Places

1 Place - zain zahid Email Forensics/BG_evidence/NTFS/Data_Triage/E-mail Databases/bev.gates@outlook.com - bev.gates

1 Place - zain zahid Email Forensics/BG_evidence/NTFS/Data_Triage/E-mail Databases/bev.gates@outlook.com - bev.gates

Items on page 1000 Page 1 Items 1-4

| | |
|---|---|
| Deleted | Undefined |
| Encrypted | Undefined |
| Has Attachments | Undefined |
| Importance | Normal |
| Priority | Normal |
| Read | Yes |
| **Recipients** | |
| To | 'Mr.Harris Malone' <mr. |
| **Represent Sender** | |
| Email | bev.gates@outlook.cor |
| Name | bev.gates@outlook.cor |

E-mail Data

RE: Team Evaluation

"Beverly Gates" <bev.gates@outlook.com> on behalf of "bev.gates@outlook.com"

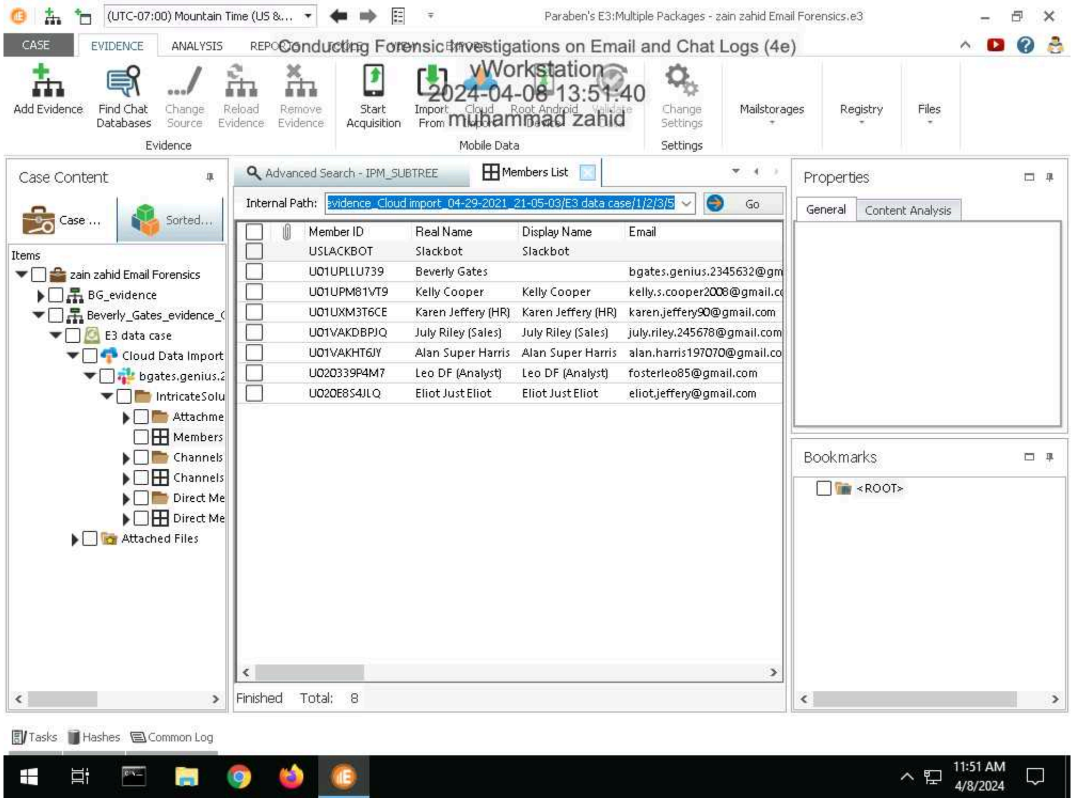
**To:** 'Mr.Harris Malone' <mr.harris@Intricate365.onmicrosoft.com>

I might report you to the actual Captain, aka Mr. Big Boss. Beware of his wrath!

Best regards,

## Part 3: Search for Evidence in a Slack Database

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

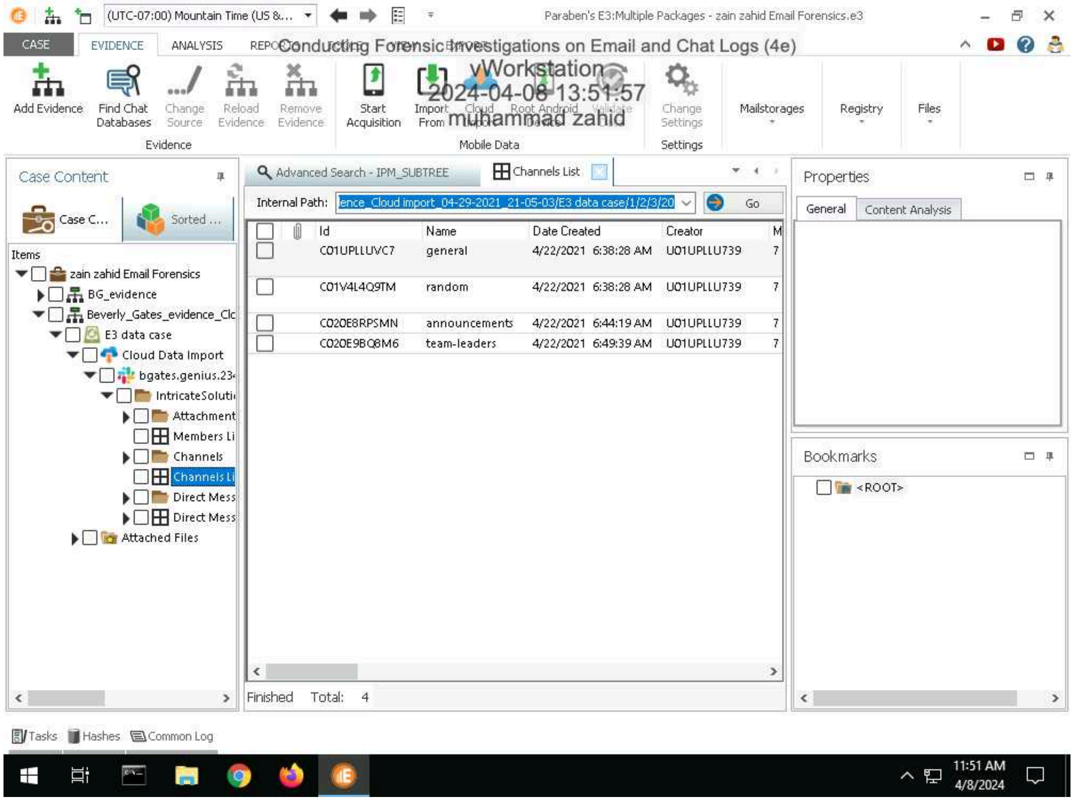


Internal Path: evidence_Cloud import_04-29-2021_21-05-03/E3 data case/1/2/3/5

| Member ID | Real Name | Display Name | Email |
|---|---|---|---|
| USLACKBOT | Slackbot | Slackbot | |
| U01UPLLU739 | Beverly Gates | | bgates.genius.2345632@gm |
| U01UPM81VT9 | Kelly Cooper | Kelly Cooper | kelly.s.cooper2008@gmail.c |
| U01UXM3T6CE | Karen Jeffery (HR) | Karen Jeffery (HR) | karen.jeffery90@gmail.com |
| U01VAKDBPJQ | July Riley (Sales) | July Riley (Sales) | july.riley.245678@gmail.com |
| U01VAKHT6JY | Alan Super Harris | Alan Super Harris | alan.harris197070@gmail.co |
| U020339P4M7 | Leo DF (Analyst) | Leo DF (Analyst) | fosterleo85@gmail.com |
| U020E8S4JLQ | Eliot Just Eliot | Eliot Just Eliot | eliot.jeffery@gmail.com |

Finished Total: 8

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

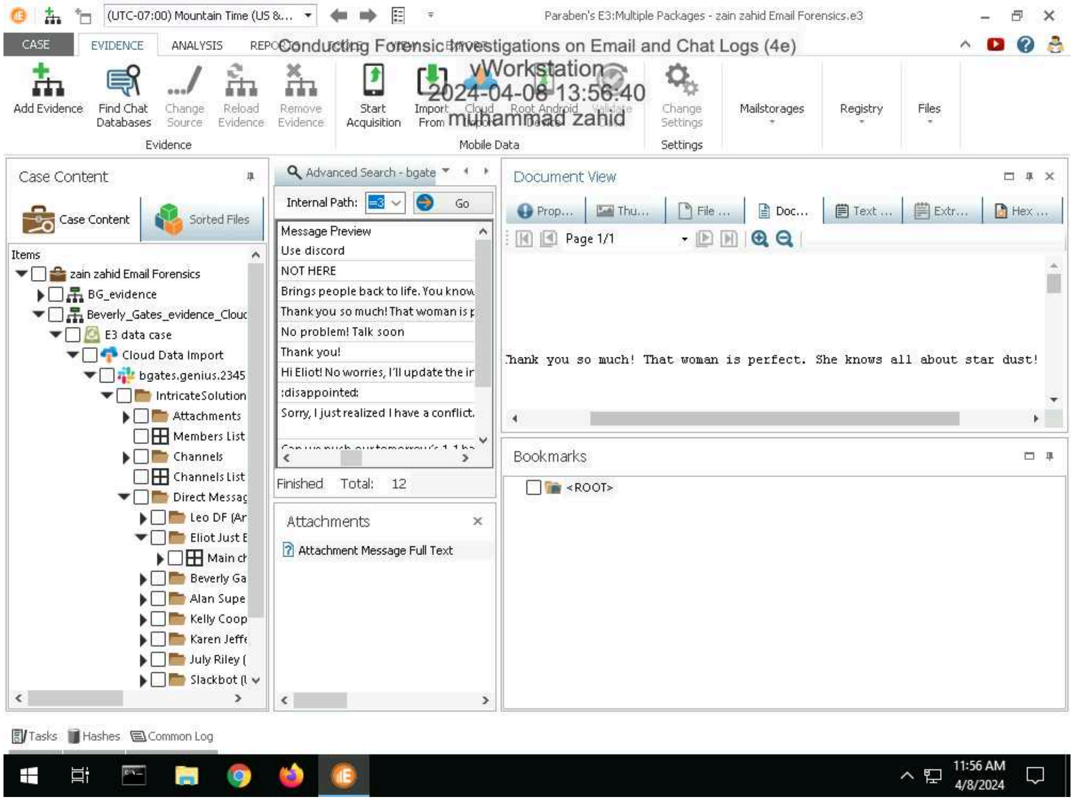


Internal Path: ence_Cloud import_04-29-2021_21-05-03/E3 data case/1/2/3/20

| □ | | Id | Name | Date Created | Creator | M |
|---|---|---|---|---|---|---|
| □ | | C01UPLLUVC7 | general | 4/22/2021 6:38:28 AM | U01UPLLU739 | 7 |
| □ | | C01V4L4Q9TM | random | 4/22/2021 6:38:28 AM | U01UPLLU739 | 7 |
| □ | | C020E8RPSMN | announcements | 4/22/2021 6:44:19 AM | U01UPLLU739 | 7 |
| □ | | C020E9BQ8M6 | team-leaders | 4/22/2021 6:49:39 AM | U01UPLLU739 | 7 |

Finished Total: 4

13. **Make a screen capture** showing the **conversation contents**.



Message Preview
Use discord
NOT HERE
Brings people back to life. You know
Thank you so much! That woman is p
No problem! Talk soon
Thank you!
Hi Eliot! No worries, I'll update the ir
:disappointed:
Sorry, I just realized I have a conflict.

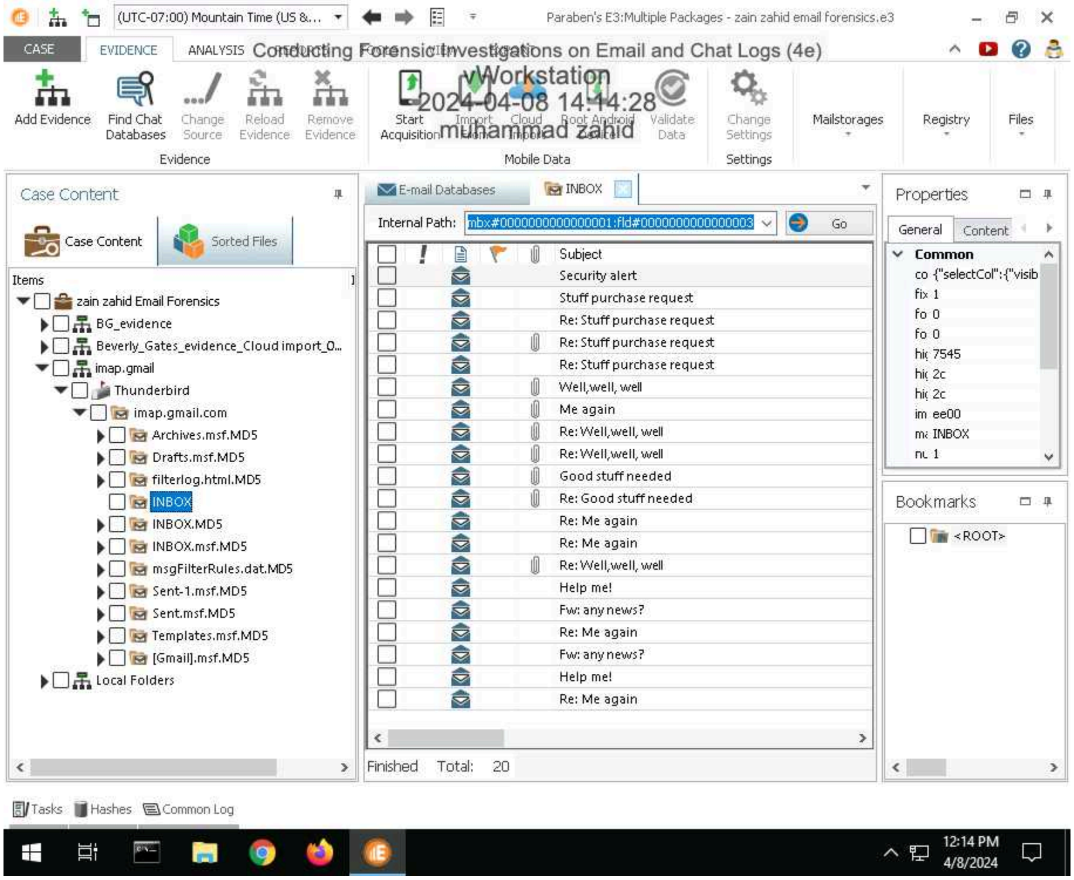
Finished Total: 12

hank you so much! That woman is perfect. She knows all about star dust!

# Section 2: Applied Learning

## Part 1: Import a Thunderbird Email Database

15. **Make a screen capture** showing the **Thunderbird Inbox**.



Internal Path: mbx#0000000000000001:fld#0000000000000003

- zain zahid Email Forensics
  - BG_evidence
  - Beverly_Gates_evidence_Cloud import_O...
  - imap.gmail
    - Thunderbird
      - imap.gmail.com
        - Archives.msf.MD5
        - Drafts.msf.MD5
        - filterlog.html.MD5
        - INBOX
        - INBOX.MD5
        - INBOX.msf.MD5
        - msgFilterRules.dat.MD5
        - Sent-1.msf.MD5
        - Sent.msf.MD5
        - Templates.msf.MD5
        - [Gmail].msf.MD5
  - Local Folders

| Subject |
|---|
| Security alert |
| Stuff purchase request |
| Re: Stuff purchase request |
| Re: Stuff purchase request |
| Re: Stuff purchase request |
| Well,well, well |
| Me again |
| Re: Well,well, well |
| Re: Well,well, well |
| Good stuff needed |
| Re: Good stuff needed |
| Re: Me again |
| Re: Me again |
| Re: Well,well, well |
| Help me! |
| Fw: any news? |
| Re: Me again |
| Fw: any news? |
| Help me! |
| Re: Me again |

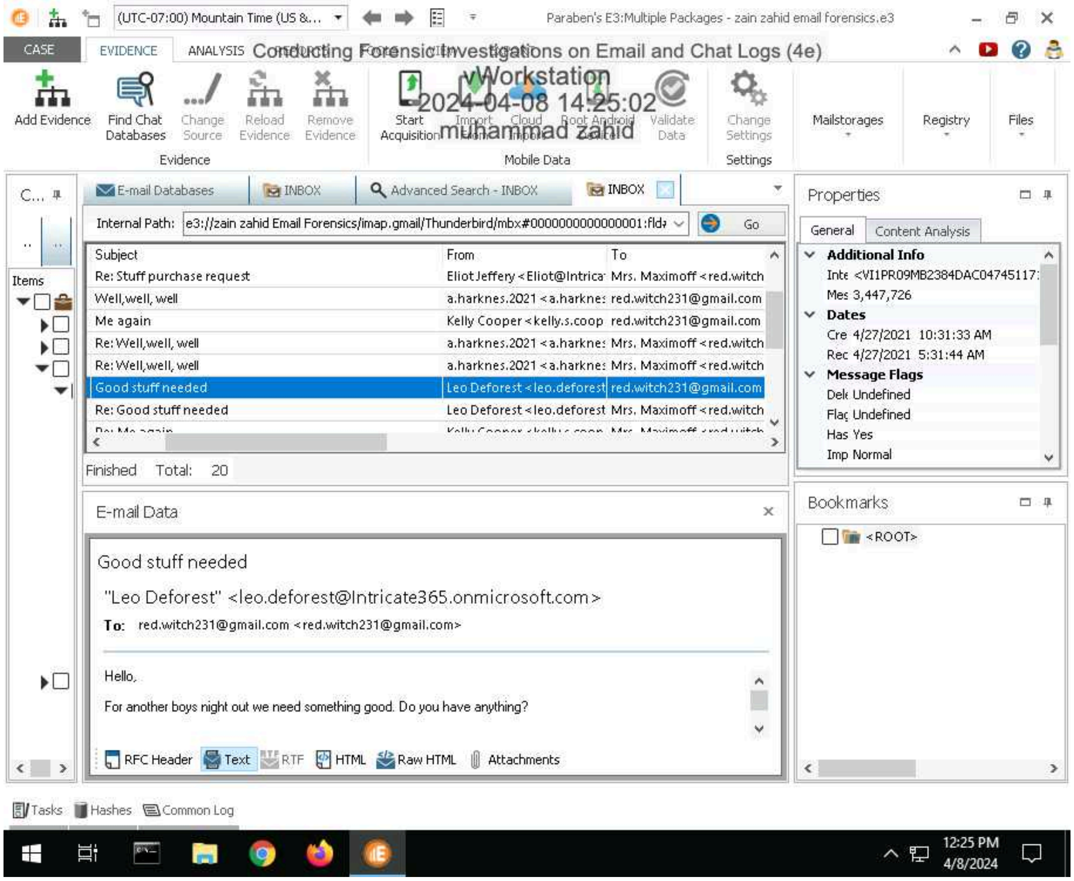
Common
co {"selectCol":{"visib
fix 1
fo 0
fo 0
hi( 7545
hi( 2c
hi( 2c
im ee00
m: INBOX
nu 1

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

from: a.harkness.2021@protonmail.comIP: 0:0:0:0Server Name: X-mozilla

## Part 2: Search for Evidence in a Thunderbird Database

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



Internal Path: e3://zain zahid Email Forensics/imap.gmail/Thunderbird/mbx#0000000000000001:fld

| Subject | From | To |
|---|---|---|
| Re: Stuff purchase request | Eliot Jeffery <Eliot@Intrica | Mrs. Maximoff <red.witch |
| Well,well, well | a.harknes.2021 <a.harknes | red.witch231@gmail.com |
| Me again | Kelly Cooper <kelly.s.coop | red.witch231@gmail.com |
| Re: Well,well, well | a.harknes.2021 <a.harknes | Mrs. Maximoff <red.witch |
| Re: Well,well, well | a.harknes.2021 <a.harknes | Mrs. Maximoff <red.witch |
| Good stuff needed | Leo Deforest <leo.deforest | red.witch231@gmail.com |
| Re: Good stuff needed | Leo Deforest <leo.deforest | Mrs. Maximoff <red.witch |
| Re: Me again | Kelly Cooper <kelly.s.coop | Mrs. Maximoff <red.witch |

Finished Total: 20

Properties

General | Content Analysis

**Additional Info**
Inte <VI1PR09MB2384DAC04745117
Mes 3,447,726
**Dates**
Cre 4/27/2021 10:31:33 AM
Rec 4/27/2021 5:31:44 AM
**Message Flags**
Dele Undefined
Flag Undefined
Has Yes
Imp Normal

Bookmarks

□ <ROOT>

E-mail Data

Good stuff needed

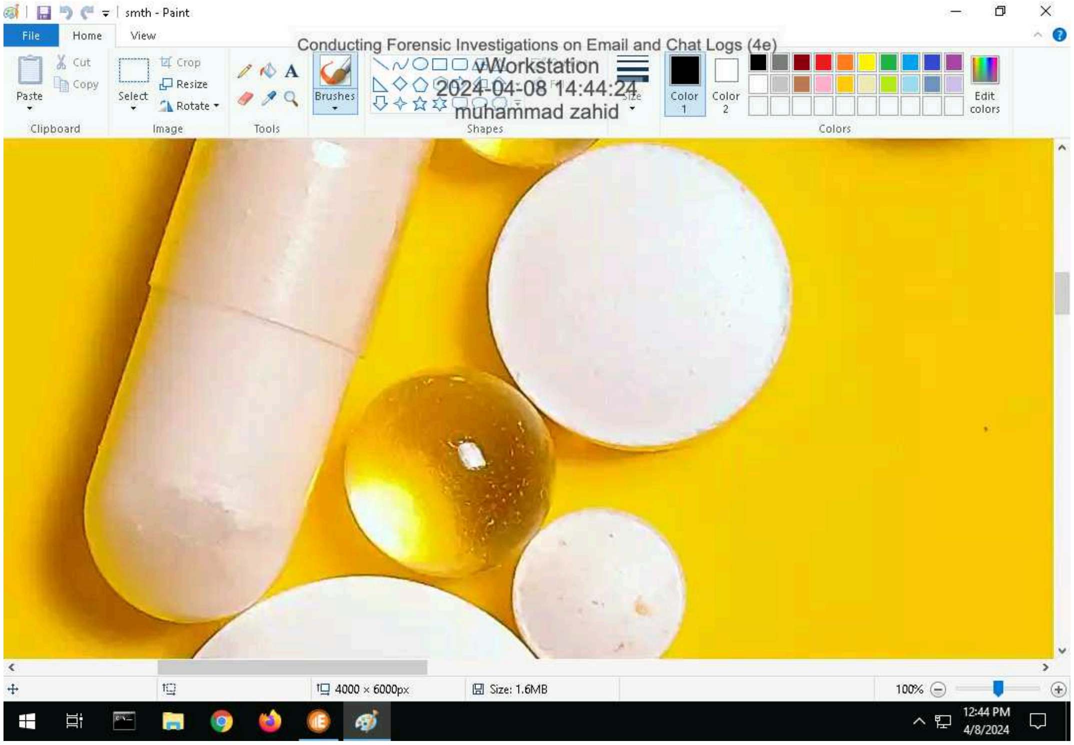
"Leo Deforest" <leo.deforest@Intricate365.onmicrosoft.com>

**To:** red.witch231@gmail.com <red.witch231@gmail.com>

Hello,

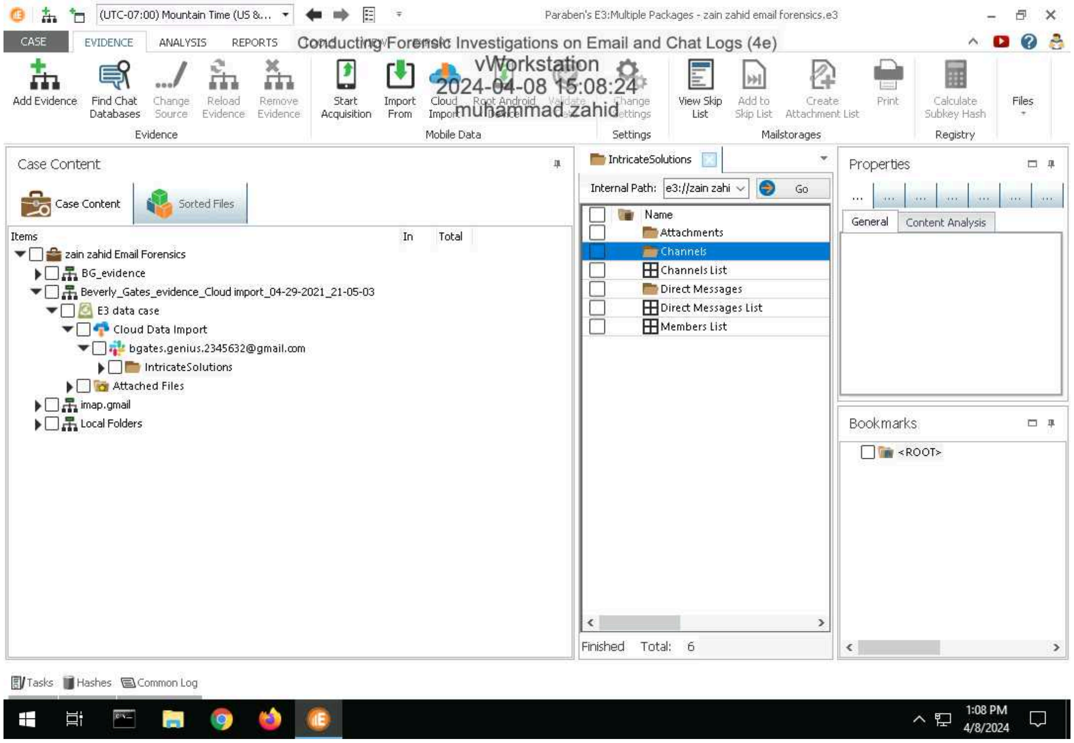
For another boys night out we need something good. Do you have anything?

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

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



Items | In | Total

- zain zahid Email Forensics
  - BG_evidence
  - Beverly_Gates_evidence_Cloud import_04-29-2021_21-05-03
    - E3 data case
      - Cloud Data Import
        - bgates.genius.2345632@gmail.com
          - IntricateSolutions
      - Attached Files
  - imap.gmail
  - Local Folders

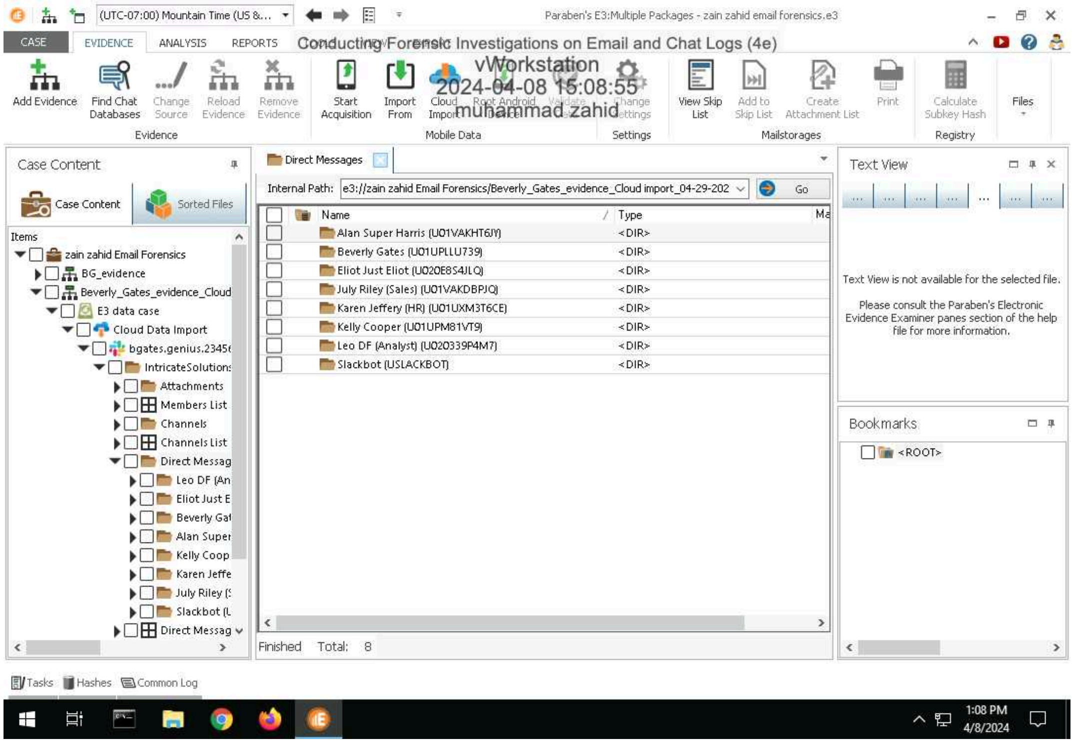
IntricateSolutions

Internal Path: e3://zain zahi

| Name |
|---|
| Attachments |
| Channels |
| Channels List |
| Direct Messages |
| Direct Messages List |
| Members List |

Finished Total: 6

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



Items

- zain zahid Email Forensics
  - BG_evidence
  - Beverly_Gates_evidence_Cloud
    - E3 data case
      - Cloud Data Import
        - bgates.genius.2345
          - IntricateSolutions
            - Attachments
            - Members List
            - Channels
            - Channels List
            - Direct Messag
              - Leo DF (An
              - Eliot Just E
              - Beverly Gat
              - Alan Super
              - Kelly Coop
              - Karen Jeffe
              - July Riley (S
              - Slackbot (U
            - Direct Messag

Direct Messages

Internal Path: e3://zain zahid Email Forensics/Beverly_Gates_evidence_Cloud import_04-29-202

| Name | Type |
|---|---|
| Alan Super Harris (U01VAKHT6JY) | <DIR> |
| Beverly Gates (U01UPLLU739) | <DIR> |
| Eliot Just Eliot (U020E8S4JLQ) | <DIR> |
| July Riley (Sales) (U01VAKDBPJQ) | <DIR> |
| Karen Jeffery (HR) (U01UXM3T6CE) | <DIR> |
| Kelly Cooper (U01UPM81VT9) | <DIR> |
| Leo DF (Analyst) (U020339P4M7) | <DIR> |
| Slackbot (USLACKBOT) | <DIR> |

Finished Total: 8

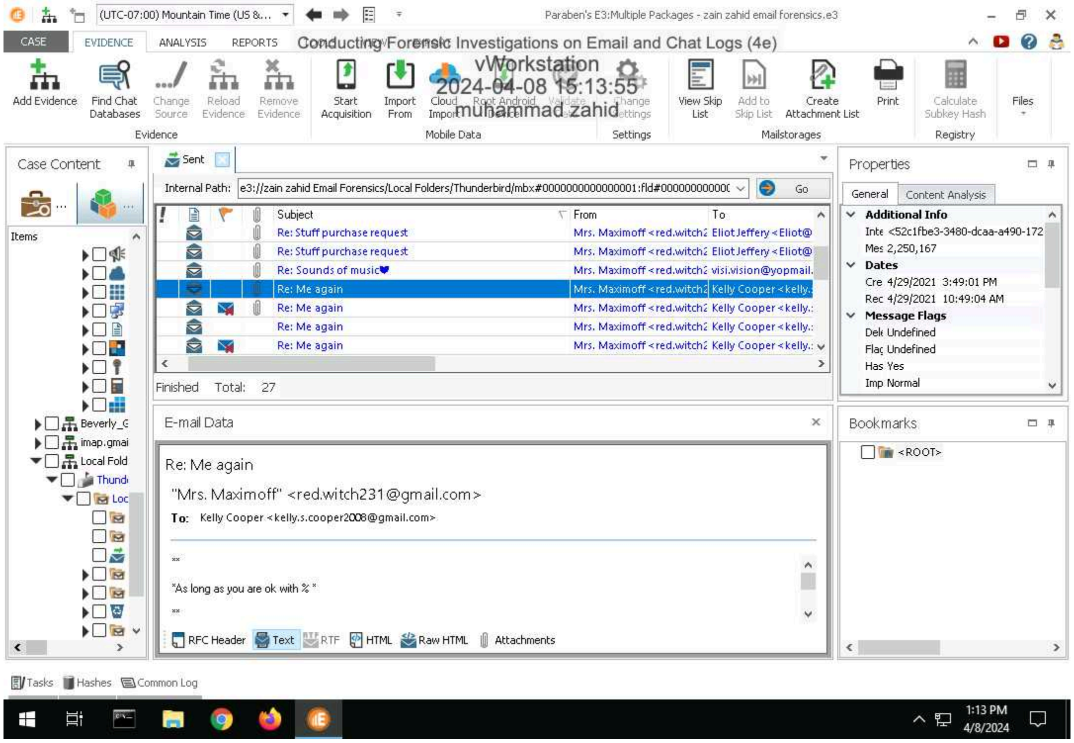
Text View is not available for the selected file.

Please consult the Paraben's Electronic Evidence Examiner panes section of the help file for more information.

# 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**.



Internal Path: e3://zain zahid Email Forensics/Local Folders/Thunderbird/mbx#0000000000000001:fld#00000000000C Go

| Subject | From | To |
|---|---|---|
| Re: Stuff purchase request | Mrs. Maximoff <red.witch2 | Eliot Jeffery <Eliot@ |
| Re: Stuff purchase request | Mrs. Maximoff <red.witch2 | Eliot Jeffery <Eliot@ |
| Re: Sounds of music♥ | Mrs. Maximoff <red.witch2 | visi.vision@yopmail. |
| Re: Me again | Mrs. Maximoff <red.witch2 | Kelly Cooper <kelly. |
| Re: Me again | Mrs. Maximoff <red.witch2 | Kelly Cooper <kelly.: |
| Re: Me again | Mrs. Maximoff <red.witch2 | Kelly Cooper <kelly.: |
| Re: Me again | Mrs. Maximoff <red.witch2 | Kelly Cooper <kelly.: |

Finished Total: 27

**Additional Info**
Inte <52c1fbe3-3480-dcaa-a490-172
Mes 2,250,167
**Dates**
Cre 4/29/2021 3:49:01 PM
Rec 4/29/2021 10:49:04 AM
**Message Flags**
Dele Undefined
Flag Undefined
Has Yes
Imp Normal

E-mail Data

Re: Me again
"Mrs. Maximoff" <red.witch231@gmail.com>
**To:** Kelly Cooper <kelly.s.cooper2008@gmail.com>

**

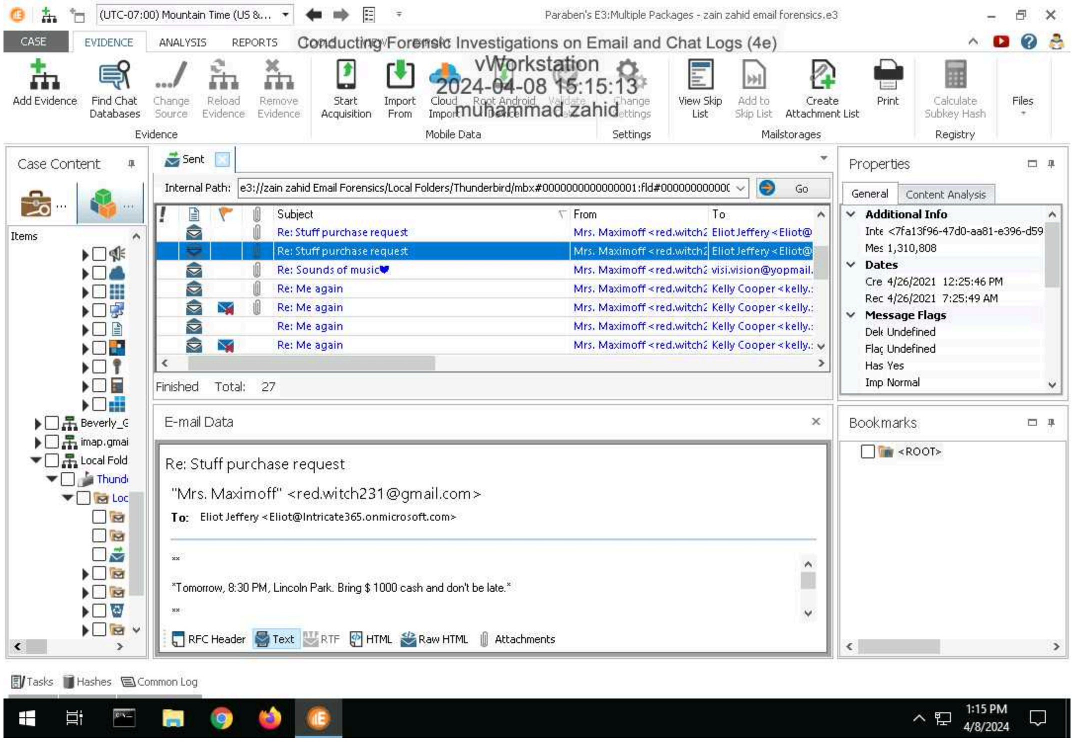
*As long as you are ok with % *

**

RFC Header | Text | RTF | HTML | Raw HTML | Attachments

## Part 2: Search for Additional Chat Evidence

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



Internal Path: e3://zain zahid Email Forensics/Local Folders/Thunderbird/mbx#0000000000000001:fld#00000000000(

| Subject | From | To |
|---|---|---|
| Re: Stuff purchase request | Mrs. Maximoff <red.witch2 | Eliot Jeffery <Eliot@ |
| Re: Stuff purchase request | Mrs. Maximoff <red.witch2 | Eliot Jeffery <Eliot@ |
| Re: Sounds of music♥ | Mrs. Maximoff <red.witch2 | visi.vision@yopmail. |
| Re: Me again | Mrs. Maximoff <red.witch2 | Kelly Cooper <kelly.: |
| Re: Me again | Mrs. Maximoff <red.witch2 | Kelly Cooper <kelly.: |
| Re: Me again | Mrs. Maximoff <red.witch2 | Kelly Cooper <kelly.: |
| Re: Me again | Mrs. Maximoff <red.witch2 | Kelly Cooper <kelly.: |

Finished Total: 27

Additional Info
Inte <7fa13f96-47d0-aa81-e396-d59
Mes 1,310,808
Dates
Cre 4/26/2021 12:25:46 PM
Rec 4/26/2021 7:25:49 AM
Message Flags
Dele Undefined
Flag Undefined
Has Yes
Imp Normal

Re: Stuff purchase request
"Mrs. Maximoff" <red.witch231@gmail.com>
To: Eliot Jeffery <Eliot@Intricate365.onmicrosoft.com>

""
"Tomorrow, 8:30 PM, Lincoln Park. Bring $ 1000 cash and don't be late."
""