**Digital Forensic Report**

Prepared By: Abby Gopal

Date of Report:04-30-2024

Week 8

Table of Contents

[Background Information 2](#_Toc143444665)

[Summary of Findings 2](#_Toc143444666)

Methodology…………………………………………………………………………………….2

[Collection Methodology 3](#_Toc143444667)

[Analysis 4](#_Toc143444668)

[Findings 5](#_Toc143444669)

[References 6](#_Toc143444670)

[Appendix A: Verification Information 7](#_Toc143444671)

[Appendix B: Examiner Machine Specifications 8](#_Toc143444672)

[Appendix C: Tools Used 9](#_Toc143444673)

Glossary………………………………………………………………………………………….9

Background Information

The provided email logs were extracted from the client's system and preserved in a ZIP file labeled "email.zip" for examination. The logs contain a series of email communications between various users detailing discussions, interactions, and system activities.

Summary of Findings

The examination of the email logs extracted from the client's system revealed extensive communication among various users, including 'tracysumtwelve,' 'terrysumtwelve,' 'loginwindow', and others. These communications encompassed a wide range of topics such as office affairs, personal matters, technical discussions, and financial issues. Notable findings include discussions about seeking financial assistance for private school tuition, speculation on the value of a rare stamp collection, plans for attending a summer concert. Additionally, there were mentions of interactions and references to legal matters and financial advice. Attachments, including documents possibly in zip files, were also exchanged during the communication. Of particular significance is the mention of a password linked to an old dog's name on July 10th, 2012. This detail raises concerns about potential security vulnerabilities, as the use of easily guessable passwords could pose risks to the integrity and confidentiality of sensitive information.

Methodology

Collection Methodology

The integrity of the email logs extracted from the client's system and preserved in a ZIP file was maintained throughout the process. This preservation was verified by both pre and post-analysis MD5/SHA1 hash comparisons. No alterations were detected in the original logs, ensuring the fidelity of the forensic data.

Analysis

Each log entry was carefully examined, noting timestamps, sender and recipient information, message content, and any attachments mentioned. Participants' identities, timing of communications, topics of conversation, attachments, and significant details were recorded for further analysis.

Findings

**Participants**

System Administrator (root@Tracys-MacBook-Air.local)

Joe Sum (joe.sum.twelve@gmail.com)

Other participants (e.g., Coral, unknown individuals with email addresses like coralbluetwo@hotmail.com)

**Timing of Communications:**

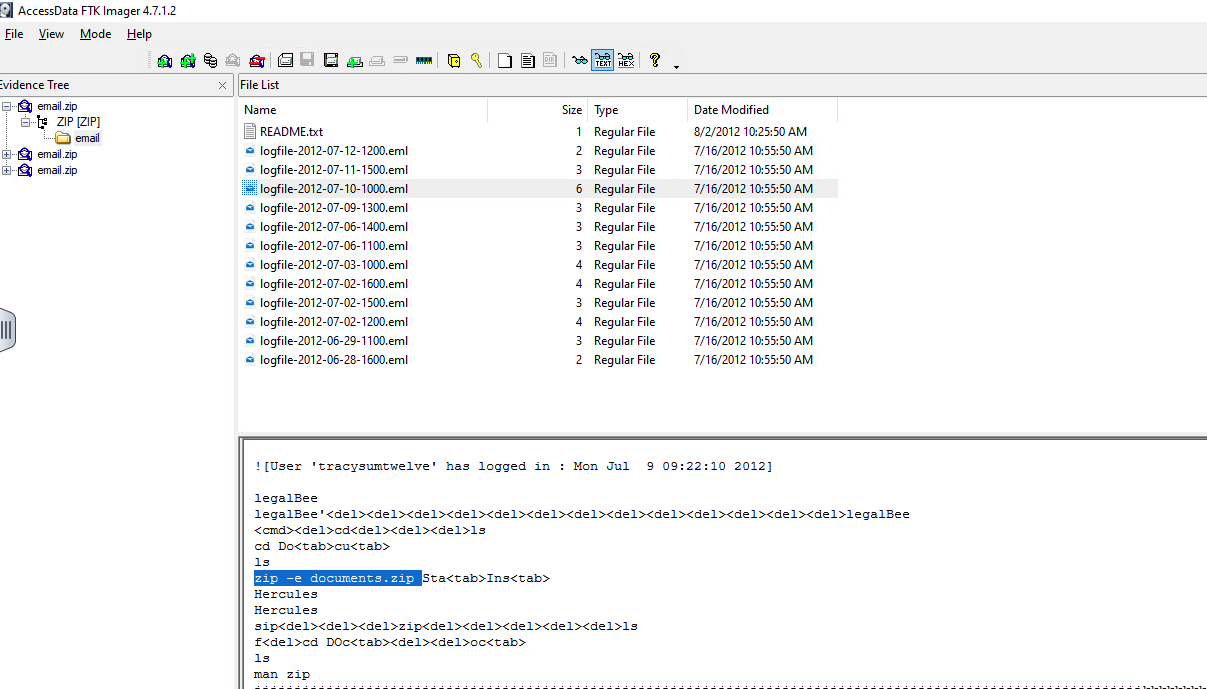
* **Friday, June 29, 2012**
  + 9:14 AM: User 'tracysumtwelve' logged in.
  + 10:33 AM: User 'tracysumtwelve' logged in.
* **Thursday, June 28, 2012**
  + 3:42 PM: User 'tracysumtwelve' logged in.
* **Monday, July 2, 2012**
  + 11:18 AM: User 'terrysumtwelve' logged in.
  + 12:00 PM: Logfile creation.
  + 2:23 PM: LogKext Daemon started up.
  + 2:50 PM: User 'tracysumtwelve' logged in.
  + 4:02 PM: LogKext Daemon created a new logfile.
* **Tuesday, July 3, 2012**
  + 9:18 AM: LogKext Daemon started up.
  + 9:40 AM: User 'tracysumtwelve' logged in.
* **Thursday, July 5, 2012**
  + 2:05 PM: User 'tracysumtwelve' logged in.
  + 2:15 PM: LogKext Daemon started up.
  + 2:16 PM: User 'tracysumtwelve' logged in.
  + 10:51 AM (Friday, July 6): LogKext Daemon started up.
  + 10:51 AM (Friday, July 6): User 'terrysumtwelve' logged in.
* **Friday, July 6, 2012**
  + 11:11 AM: Logfile creation.
  + 1:34 PM: LogKext Daemon started up.
  + 1:34 PM: User 'tracysumtwelve' logged in.
* **Monday, July 9, 2012**
  + 9:22 AM: User 'tracysumtwelve' logged in.
  + 10:41 AM: LogKext Daemon started up.
  + 10:42 AM: User 'tracysumtwelve' logged in.
* **Tuesday, July 10, 2012**
  + 9:15 AM: Logfile creation.
  + 9:15 AM: User 'tracysumtwelve' logged in.
  + 9:50 AM: LogKext Daemon started up.
  + 9:50 AM: User 'terrysumtwelve' logged in.
* **Thursday, July 12, 2012**
  + 11:41 AM: LogKext Daemon started up.
  + 11:42 AM: User 'tracysumtwelve' logged in.
  + 2:00 PM: Logfile creation.

**Topics of Conversation**

1. Tracy emails Joe Sum seeking help with Terry's school tuition due to financial strain. She expresses reluctance but hopes for assistance.
2. Tracy discusses receiving a rare stamp collection, noting its potential value. She speculates on its significance and its potential as a financial opportunity.
3. Tracy suggests attending a concert during the summer and discusses this with one of the participants, possibly Terry or Joe Sum.
4. Mention of unusual shipping information prompts speculation about the nature of the shipment.
5. Mention of a conversation with Coral, who has received positive news about her job. Tracy suggests catching up with Coral to learn more.
6. The emails contain logs of system activities, including LogKext Daemon starting up and user logins, indicating technical monitoring or troubleshooting.
7. The System Administrator notes office excitement about a foreign exhibit. There's anticipation despite no official confirmation.
8. Coral expresses concern about her child possibly switching schools due to financial constraints. Tracy suggests keeping an eye out for opportunities.
9. Tracy mentions receiving insurance documents with value assessments for certain objects. She suggests keeping an eye out for anything notable.
10. Tracy discusses financial aid for private school tuition, indicating financial strain.
11. Tracy mentions "tablet access" in one of the emails, suggesting a discussion or consideration regarding access to tablet devices, possibly for work-related purposes or personal use.
12. Tracy mentions receiving or handling various documents, including insurance documents with value assessments for certain objects. This suggests professional duties or responsibilities related to document management.
13. Plans or discussions about watching a scary movie are mentioned, indicating social or leisure activities among the participants.
14. There's a mention of a short story, although the context or content of the discussion is not detailed.
15. Coral expresses concern about her child's potential absence from school, indicating personal or family-related matters that could affect her child's education.
16. Mentioned in relation to the shipping exhibit, there's discussion about dealing with paperwork, suggesting organizational efforts or logistical challenges associated with the event.
17. A password for accessing documents is mentioned, linked to an old dog's name.
18. Technical commands related to file management are present, including navigation and zipping files.
19. Various mentions of web searches and discussions related to legal matters and financial advice.
20. There's also a cautionary message about avoiding trouble at work.
21. Mention of "legalBee”,"google.com" “Yahoo.com” and VM.

**Attachments/Files Transferred**:

**Date: July 9th, 2012 (Monday) Documents** shared, possible zip files.



**Pertinent Details/Significant Findings**:

1. Mention of a Password Linked to an Old Dog's Name (July 10th, 2012):

This could indicate the use of a potentially weak password, which may pose security risks or suggest inadequate security practices.

1. Discussion About Private School Tuition Help and Office Matters (July 6th, 2012):

Conversations related to financial matters, especially those involving requests for help with tuition or concerns about school switching, may indicate financial stress or potential vulnerabilities that could be exploited.

1. Mention of Coral's Email Address (June 29th, 2012):

The repeated mention of specific email addresses, especially if they are associated with multiple conversations or activities, could indicate a focus on individuals or entities, potentially raising questions about the nature of the relationship or communication.

1. Cautionary Message About Avoiding Trouble at Work (June 29th, 2012):

While this message may appear innocuous on the surface, its presence suggests awareness of potential risks or misconduct in the workplace, prompting the need for further investigation into the context and circumstances surrounding this cautionary advice.

1. Mention of Various Web Searches Related to Legal Matters and Financial Advice (July 2nd, 2012):

Depending on the specifics of the searches, such as queries related to legal issues, financial aid, or private school tuition, these activities may indicate specific interests, concerns, or potential motives.

6. Technical Commands Related to File Management (July 10th, 2012):

The use of technical commands for file management, particularly if they involve accessing, modifying, or organizing sensitive data or documents, may raise questions about the purpose or intent behind these actions.

Attachments of Screenshots:

A white background with black text

Description automatically generated

A white background with black lines

Description automatically generatedA white screen with black text

Description automatically generatedA white and black line

Description automatically generated with medium confidenceA white background with black text

Description automatically generated

A close-up of a computer screen

Description automatically generated

**Timeline of Events**

June 28th, 2012 (Thursday):

3:41 PM EDT: LogKext Daemon starts up.

3:42 PM EDT: User 'tracysumtwelve' logs in.

Mention of "legalBee" and various email addresses.

June 29th, 2012 (Friday):

New Logfile Created: Thursday, June 28th, 2012, at 4:09 PM EDT.

9:04 AM EDT: LogKext Daemon starts up.

9:14 AM EDT: User 'tracysumtwelve' logs in.

Mention of Coral's email address: coralbluetwo@hotmail.com

Conversation with "legalBee" regarding office matters and concerns about switching schools.

10:33 AM EDT: LogKext Daemon starts up.

10:33 AM EDT: User 'tracysumtwelve' logs in.

Additional mention of "legalBee" with cautionary advice regarding work trouble.

July 2nd, 2012 (Monday):

New Logfile Created: Friday, June 29th, 2012, at 11:26 AM EDT (Timestamp likely incorrect).

11:18 AM EDT (Timestamp likely incorrect): User 'terrysumtwelve' logs in.

11:87 AM EDT (Timestamp likely incorrect): User 'tracysumtwelve' logs in.

Mention of "legalbee" and "national gallery exhibit."

Various web searches related to legal matters, financial aid, and private school tuition.

12:00 PM EDT: LogKext Daemon starts up. (Possibly a duplicate entry from December 5th, 2006)

1:23 PM EDT: LogKext Daemon starts up.

2:50 PM EDT: User 'tracysumtwelve' logs in.

Office buzz about a foreign exhibit, paperwork discussions, and Coral's financial aid for private school.

July 3rd, 2012 (Tuesday):

9:18 AM EDT: LogKext Daemon starts up.

9:18 AM EDT: User 'tracysumtwelve' logs in.

Discussion regarding Terry's school tuition and a request for financial help.

Mention of receiving a rare collection of stamps and their potential value.

Discussion about good news from Coral regarding her job and catching up with her.

Looking for alternatives to private school.

July 5th, 2012 (Thursday):

1:41 PM EDT: LogKext Daemon starts up (possibly from July 4th).

2:05 PM EDT: User 'tracysumtwelve' logs in.

2:15 PM EDT: LogKext Daemon starts up.

2:15 PM EDT: User 'tracysumtwelve' logs in.

10:51 AM EDT (Friday, July 6th): LogKext Daemon starts up.

10:51 AM EDT (Friday, July 6th): User 'terrysumtwelve' logs in.

References to Google, images.google.com, "Buick," "value of international," private school, and helping parents afford it.

Mention of an MLA formal event and summer concert plans.

July 6th, 2012 (Friday):

11:00 AM EDT: LogKext Daemon starts up (possibly from July 5th).

2:05 PM EDT: User 'tracysumtwelve' logs in.

1:34 PM EDT: LogKext Daemon starts up.

1:34 PM EDT: User 'tracysumtwelve' logs in.

Mentions watching YouTube videos, adobe.com, google.com, and thanking someone named "Carrym" for lunch.

July 9th, 2012 (Monday):

New Logfile Created: Friday, July 6th, 2012, at 2:01 PM EDT.

9:04 AM EDT: LogKext Daemon starts up.

9:22 AM EDT: User 'tracysumtwelve' logs in.

Technical commands related to file management.

July 10th, 2012 (Tuesday):

9:50 AM EDT: User 'terrysumtwelve' logs in.

Mention of a password for accessing documents linked to an old dog's name.

9:15 AM EDT: LogKext Daemon starts up.

9:50 AM EDT: User 'tracysumtwelve' logs in.

Technical commands related to file management, navigation, and zipping files.

10:00 AM EDT: LogKext Daemon starts up.

12:00 PM EDT: LogKext Daemon starts up.

2:02 PM EDT: User 'tracysumtwelve' logs in.

Discussion about private school tuition help and a message exchange regarding office matters.

2:15 PM EDT: LogKext Daemon starts up.

4:00 PM EDT: LogKext Daemon starts up.

July 11th, 2012 (Wednesday):

12:00 PM EDT: LogKext Daemon starts up.

2:45 PM EDT: LogKext Daemon starts up.

2:54 PM EDT: User 'tracysumtwelve' logs in.

Discussion about a short story review and disappointment with the ending.

Mention of attaching a writeup of the short story for review.

3:00 PM EDT: LogKext Daemon starts up.

July 12th, 2012 (Thursday):

11:41 AM EDT: LogKext Daemon starts up.

11:42 AM EDT: User 'tracysumtwelve' logs in.

**Recommendations for Further Analysis**:

1. Perform a deeper analysis of the email logs to identify any additional participants or conversations.
2. Investigate the content of attachments, if any, for potential insights.
3. Conduct keyword searches to uncover hidden or sensitive information.
4. Explore the metadata of emails for more context and understanding of communication patterns.

References

Allen, T. (2017, May 8). *Computer Forensics Tool Testing Program (CFTT)*. NIST. <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cf>

# Appendix A: Verification Information

| Designation | File Type | File Name | MD5/SHA1 Hash |
| --- | --- | --- | --- |
| PRE-ANALYSIS |  |  |  |
|  | Preservation Copy |  |  |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-07-12-1200.eml | a224f7fdf6af727a16bc4d7ae0bb9125 |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-06-28-1600.eml | df2f439f28af342ca8a8fd9f0b740f53 |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-06-29-1100.eml | c891901bb05b6a65228d6709a8e27173 |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-07-82-1200.eml | 88061c1ea9c7feb5ee2a4ff76c305a21 |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-87-82-1500.eml | d5d2132926e1dc71c4f477dcSf02f74f |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-07-82-1600.eml | a4f064444a8c62443e03e8e29735dcd2 |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-87-83-1000.eml | 68e9fa3bb0716a10a9021cf77bc5a0e7 |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-07-06-1100.eml | 630dd4a71d4e8a082dS7a6eb7d8a168d |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-07-06-1400.eml | 970ab8abcSGeSeF1a1241488c3b41adb |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-07-09-1300.eml | 7479cdc87ae4f8d96d4e692828e380d7 |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-07-10-1000.eml | dd23022018c86f474ba6c2961fdae35e |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-87-11-1500.eml | 59469076816371618619a028948df12a |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-07-12-1200.eml | a224f7fdf6af727a16bc4d7ae0bb9125 |

|  | File Type | File Name | MD5/SHA1 Hash |
| --- | --- | --- | --- |
| POST-ANALYSIS |  |  |  |
|  | Preservation Copy |  |  |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-07-12-1200.eml | a224f7fdf6af727a16bc4d7ae0bb9125 |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-06-28-1600.eml | df2f439f28af342ca8a8fd9f0b740f53 |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-06-29-1100.eml | c891901bb05b6a65228d6709a8e27173 |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-07-82-1200.eml | 88061c1ea9c7feb5ee2a4ff76c305a21 |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-87-82-1500.eml | d5d2132926e1dc71c4f477dcSf02f74f |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-07-82-1600.eml | a4f064444a8c62443e03e8e29735dcd2 |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-87-83-1000.eml | 68e9fa3bb0716a10a9021cf77bc5a0e7 |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-07-06-1100.eml | 630dd4a71d4e8a082dS7a6eb7d8a168d |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-07-06-1400.eml | 970ab8abcSGeSeF1a1241488c3b41adb |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-07-09-1300.eml | 7479cdc87ae4f8d96d4e692828e380d7 |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-07-10-1000.eml | dd23022018c86f474ba6c2961fdae35e |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-87-11-1500.eml | 59469076816371618619a028948df12a |
|  | Working Copy | emai1.zip\ZIP [ZIP]\emai1\10gfile-2012-07-12-1200.eml | a224f7fdf6af727a16bc4d7ae0bb9125 |

Appendix B: Examiner Machine Specifications

Computer Name: Dell VSI

Operating System: Microsoft Windows

OS Version: 10

Time Zone: Eastern

The system date/time is consistent with the time zone listed above, as verified by <http://nist.time.gov>

Appendix C: Tools Used

|  |  |
| --- | --- |
| Tool Name | Version |
|  |  |
| FTK Imager | 4.7.1.2 |

Glossary

Email. Zip - Refers to compressing or "zipping" email attachments to reduce file size before sending them via email. This process involves using software to compress one or more files into a single archive file with the ".zip" extension.