

M57.biz Forensic Investigation Report

Keith M. Hall

College of Science and Technology, Bellevue University

CIS607-T302: Computer Forensics

Professor Gary Amerson

August 12, 2023



Table Of Contents

| | |
|---|-----------|
| I. Abstract..... | 5 |
| II. Introduction..... | 6 |
| Project Overview | |
| Purpose | |
| III. Disk Analysis..... | 7 |
| Tools..... | 7 |
| Procedures..... | 7 |
| Verification | |
| Passwords | |
| Carving | |
| Recent Activity | |
| Evidence Acquisition..... | 11 |
| M57.biz Confidential File | |
| Email Examination | |
| V. Results..... | 11 |
| When did Jean create this spreadsheet? | |
| How did it get from her computer to competitor's website? | |
| Who else from the company is involved? | |
| VI. Conclusion..... | 14 |
| VII. Limitations..... | 17 |

| | |
|------------------------------|-----------|
| VIII. References..... | 18 |
|------------------------------|-----------|

| | |
|--------------------------|-----------|
| IX. Glossary..... | 19 |
|--------------------------|-----------|

Appendix I

Appendix II

Appendix III

ABSTRACT

This report contains the results of a digital forensic examination of a disk image, jean57.E01,E02 (EnCase format), in response to a request by M57.biz, a start-up firm that reports having had a spreadsheet containing proprietary information uploaded as an attachment on a competitor's "technical support" forum. The disk image was placed in our custody, along with a copy of the spreadsheet with instructions to analyze it and answer three essential questions.

INTRODUCTION

Project Overview

M57.biz is a startup firm that produces an online body art catalog. The company is virtual and conducts most of its business operations across the internet. In and around July 20, 2008, an employee reported having seen a spreadsheet containing proprietary information uploaded as an attachment on a competitor's "technical support" forum. The incident was reported, and a digital forensic examiner was assigned to the case. After interviewing the parties involved, it was determined that 1) Jean, the CFO (Chief Financial Officer) admitted to having prepared the document but claims she did so in response to an email request from the company's president, Allison, where it was sent. Jean ended her statement with, "That's all I know." Allison, however, insists that she never made such a request nor received the spreadsheet via email as Jean claimed.

Purpose

A forensic copy of Jean's computer was made and placed in our custody as a disk image file, "nps-2008-jean," (E01-EnCase) by a co-founder with instructions to answer the following: 1) When did Jean create this spreadsheet? 2) How did it get from her computer to competitor's website? 3) Who else from the company is involved? The examiner assigned collected the appropriate tools, followed established protocols, and began analysis of the disk. Documentation of the procedures can be found in Appendix IV. The results of what was found, as well as limitations, are also discussed.

DISK ANALYSIS

Tools

The main forensic tools used for validation and verification protocols were OSForensics and Autopsy. FTK was initially chosen for timeline analysis and recent computer activity, but the examiner was unable to verify the results. Instead, autopsy was employed. In addition to verifying results, Autopsy was used for metadata analysis, encryption detection, and recovering any deleted files. OSForensics was only used to investigate emails.

Procedures

Validation and verification of the disk image and forensic tools was accomplished by retrieving and examining data with OSForensics and verifying the results by performing the same task with Autopsy. First, the disk image was verified using Autopsy to display the hash values calculated for the original hard drive to see if it matched the copy investigators were given. Both MD5 and SHA1 hash values matched the original values. (Fig.1)

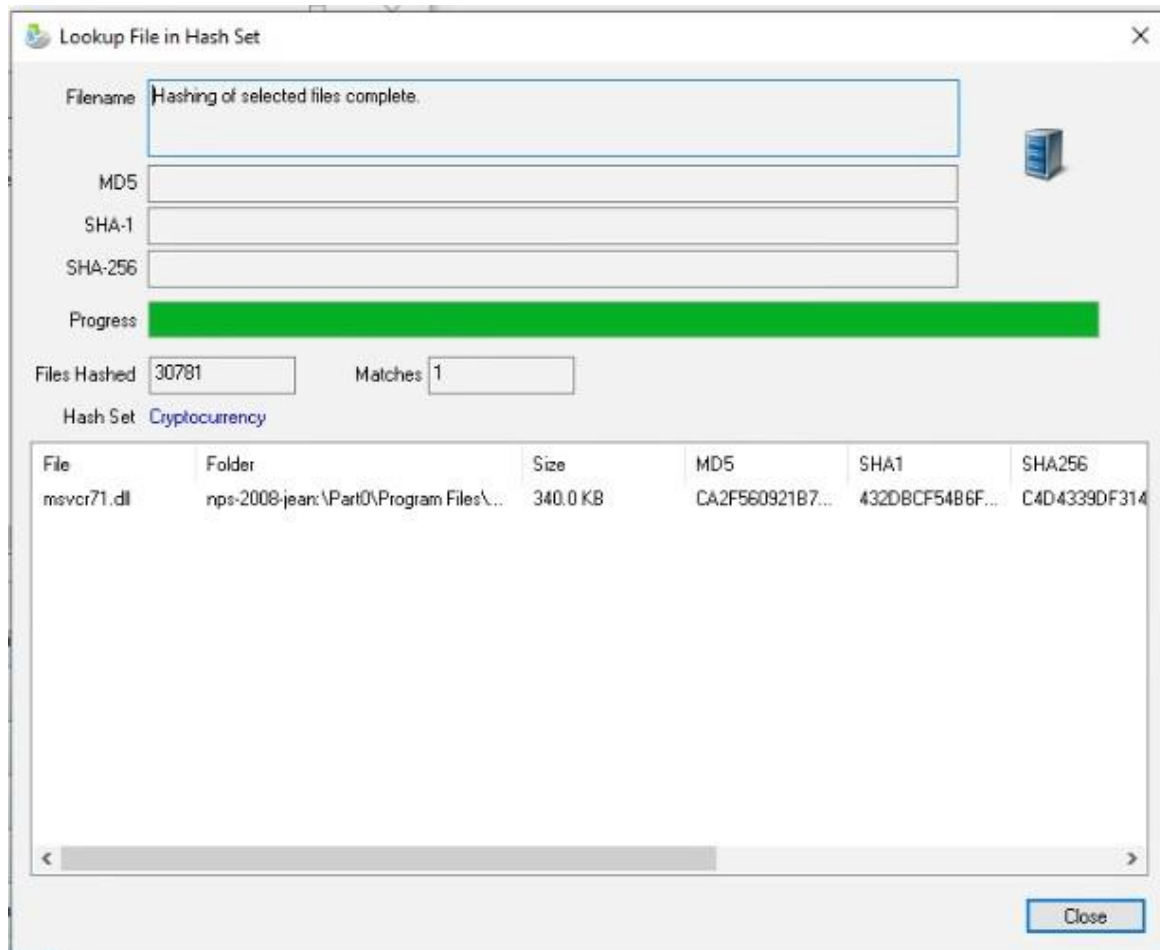


Fig. 1

The most crucial evidence extracted concerning the focal point of the investigation, the email files, was verified with Autopsy. The email investigation with Autopsy (Fig.2) led to the same results as was obtained with OSForensics. (Fig. 3)

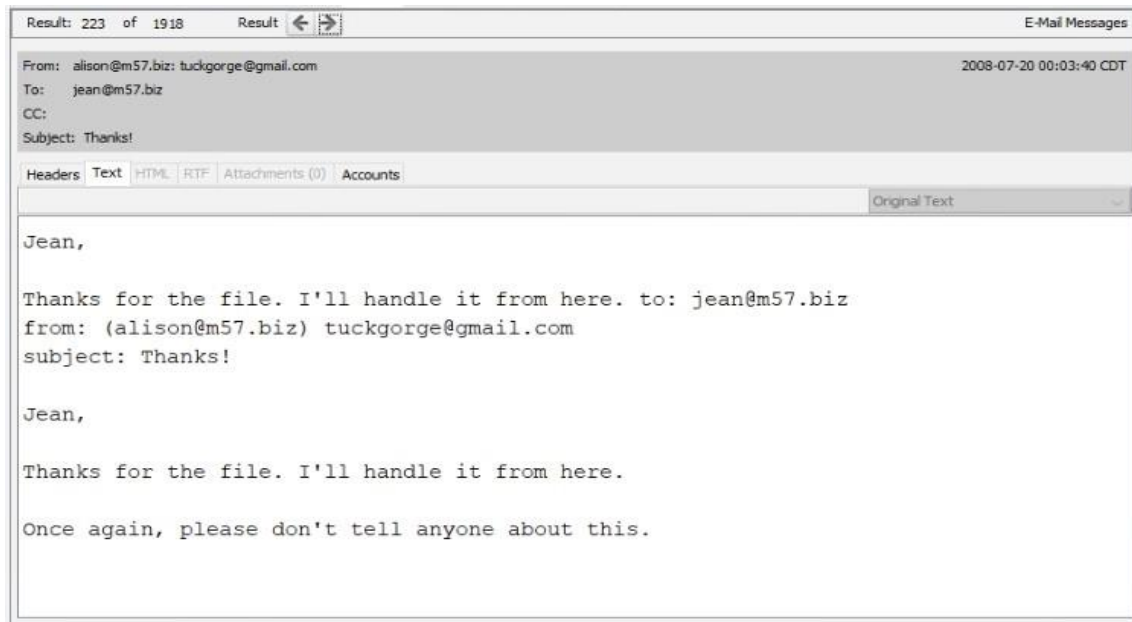


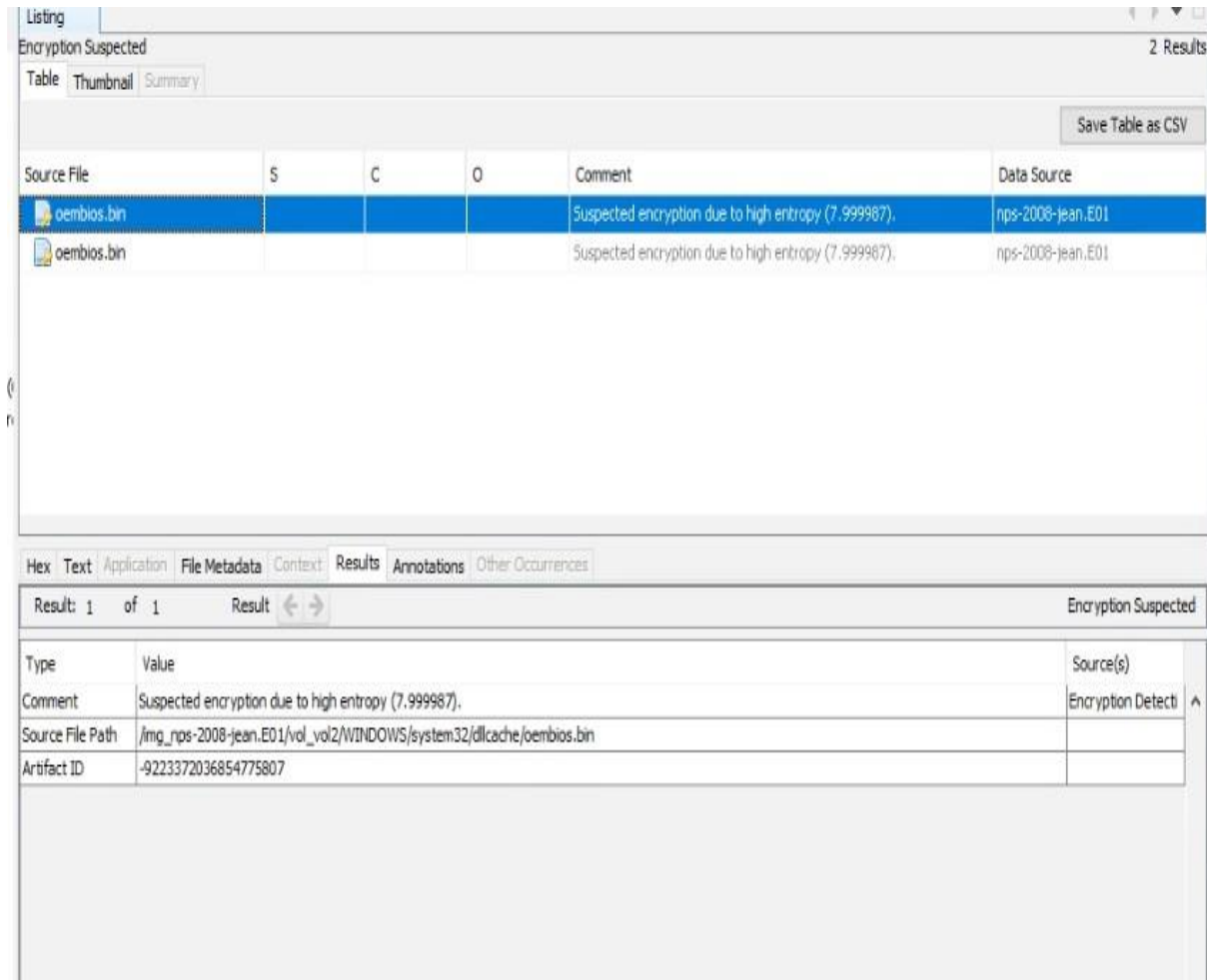
Fig. 2



Fig. 3

Encryption/Password Protected Files- Autopsy's encryption/password detection modules were used to see if any files were encrypted/password protected. There were 2

files listed as “encryption suspected,” since the test was based on the entropy of the file. The files' location suggests they are not encrypted, however.



The screenshot displays a forensic analysis interface. At the top, a 'Listing' tab is active, showing a table of results under the heading 'Encryption Suspected' with '2 Results'. The table has columns for 'Source File', 'S', 'C', 'O', 'Comment', and 'Data Source'. Two entries for 'oembios.bin' are listed, both with a comment 'Suspected encryption due to high entropy (7.999987)' and data source 'nps-2008-jean.E01'. Below this, a 'Results' tab is active, showing 'Result: 1 of 1'. The results table has columns for 'Type', 'Value', and 'Source(s)'. The first row shows a 'Comment' with the same entropy-based suspicion and source. The second row shows the 'Source File Path' as '/img_nps-2008-jean.E01/vol_vol2/NTFINDOWS/system32/dllcache/oembios.bin'. The third row shows an 'Artifact ID' of '-9223372036854775807'.

| Source File | S | C | O | Comment | Data Source |
|-------------|---|---|---|--|-------------------|
| oembios.bin | | | | Suspected encryption due to high entropy (7.999987). | nps-2008-jean.E01 |
| oembios.bin | | | | Suspected encryption due to high entropy (7.999987). | nps-2008-jean.E01 |

| Type | Value | Source(s) |
|------------------|---|--------------------|
| Comment | Suspected encryption due to high entropy (7.999987). | Encryption Detecti |
| Source File Path | /img_nps-2008-jean.E01/vol_vol2/NTFINDOWS/system32/dllcache/oembios.bin | |
| Artifact ID | -9223372036854775807 | |

Fig. 4

Carving- The image was examined scanned for deleted files. There were 2015 deleted files. Upon examination of the file extensions, it was clear none were related to this case.

Evidence Acquisition

M57.biz Confidential File- A spread sheet containing confidential information was discovered and extracted from the disk image. (See appendix 1) The file was an exact

match with the document provided by the co-founder and was discovered on Jean's desktop.

Email Examination- There were 4 key emails found that were relevant to the purpose set forth in this case: 1) An email requesting the confidential information that was sent to Jean by Allison, 2) A plea sent by Allison to Jean to send the information right away, 3) An email with an attachment identified as the confidential spreadsheet, that was sent by Jean, and 4) An email expressing thanks sent to Jean.

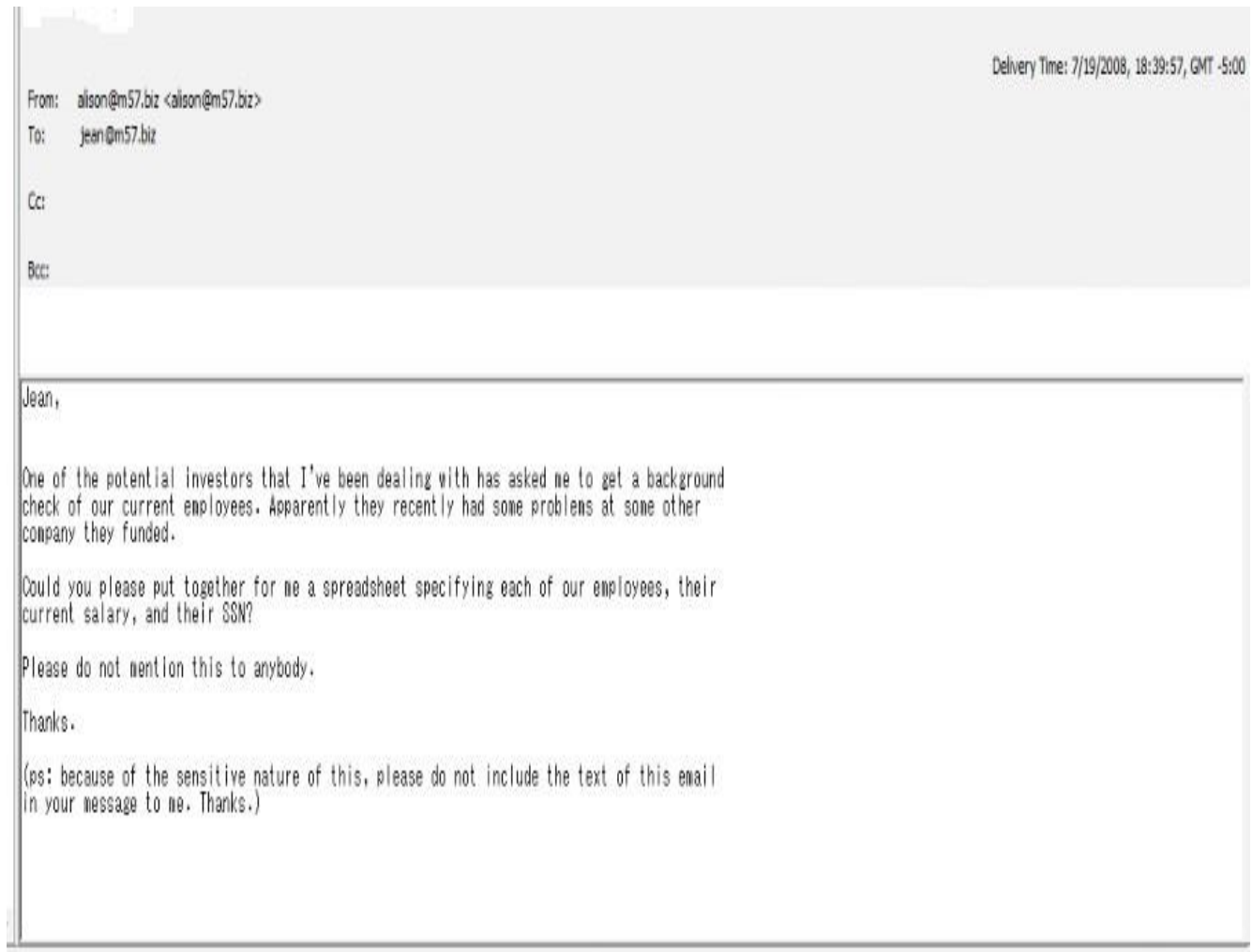
RESULTS

Chronology of events

Based on the evidence provided, the following timeline of events is likely to have occurred:

On July 19, 2008, at 18:39:57 (GMT);

I. An email from Alison@m57.biz was sent to jean@m57.biz stating that a potential investor wanted to conduct background checks on M57.biz employees and that a spreadsheet with employee salaries and SSNs were required, (Fig. 5)



Saturday, July 19, 2008, 20:22:45 (GMT)

2. jean@m57.biz receives another email. This time from alison@m57.biz/tuckergorge@gmail.com requesting that the information be sent now.
3. Jean sends the spreadsheet to alison@m57.biz/tuckergorge@gmail.com as an attachment to the email. (Fig. 6) Autopsy shows the location of the attachment.

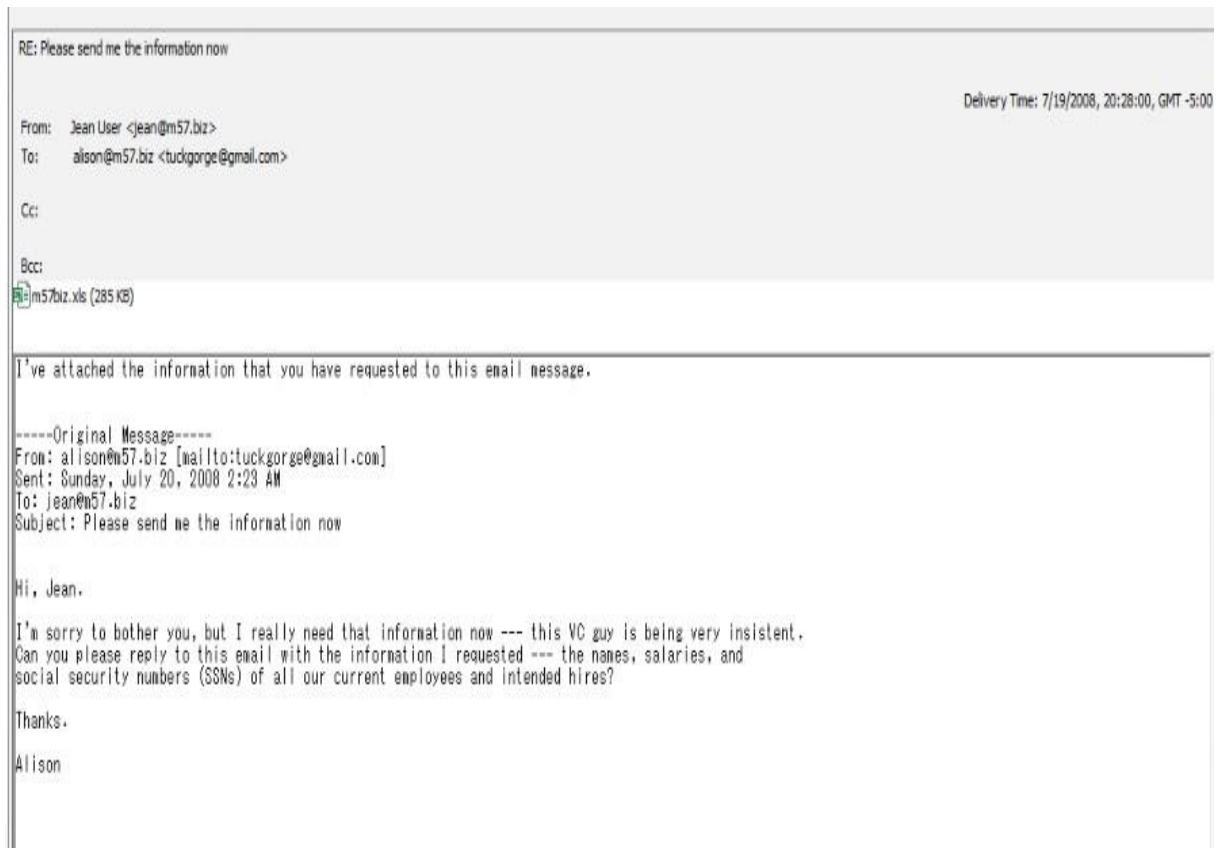




Fig. 6.1 OSForensics

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Result: 261 of 1918 Result  

E-Mail Messages

From: Jean User: jean@m57.biz 2008-07-19 20:28:00 CDT
To: alison@m57.biz
CC:
Subject: RE: Please send me the information now

Headers Text HTML RTF Attachments (1) Accounts

[View in New Window](#)

1 Results

Table Thumbnail Summary

[Save Table as CSV](#)


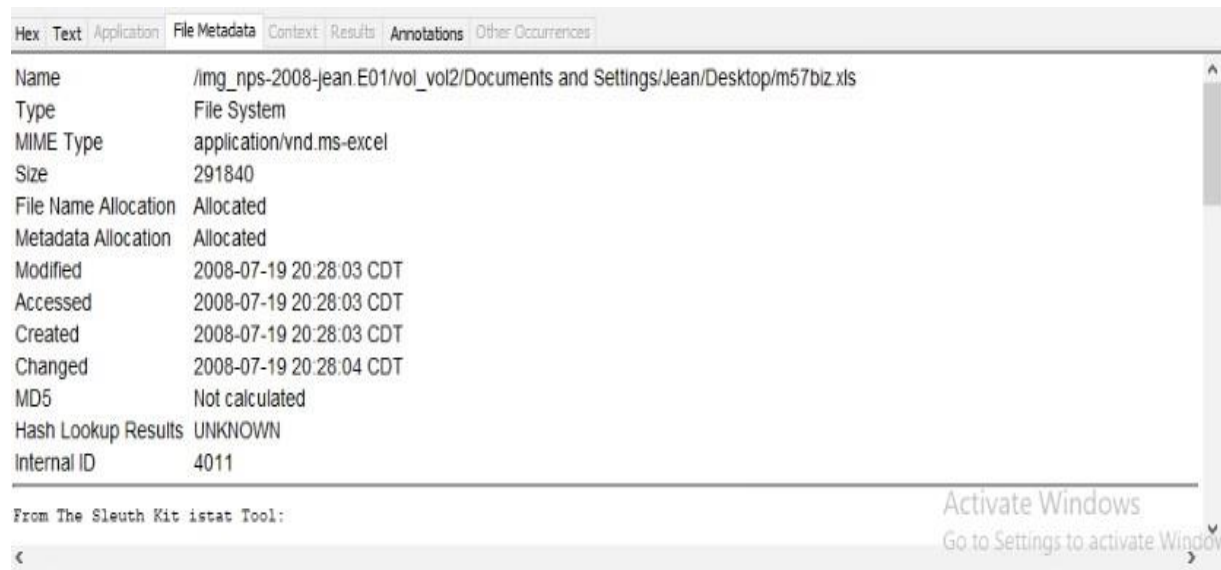
| Location | Size | Mime type | Known |
|--|--------|--------------------------|---------|
|  /img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst/m57biz.xls | 291840 | application/vnd.ms-excel | unknown |

Fig. 6.2 Autopsy

CONCLUSION

When did Jean create this spreadsheet?

According to a metadata analysis of the spreadsheet discovered on Jean's desktop, she created it July 19, 2008, 20:28:03 CDT.



| Hex | Text | Application | File Metadata | Context | Results | Annotations | Other Occurrences |
|----------------------|--|-------------|---------------|---------|---------|-------------|-------------------|
| Name | /img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Desktop/m57biz.xls | | | | | | |
| Type | File System | | | | | | |
| MIME Type | application/vnd.ms-excel | | | | | | |
| Size | 291840 | | | | | | |
| File Name Allocation | Allocated | | | | | | |
| Metadata Allocation | Allocated | | | | | | |
| Modified | 2008-07-19 20:28:03 CDT | | | | | | |
| Accessed | 2008-07-19 20:28:03 CDT | | | | | | |
| Created | 2008-07-19 20:28:03 CDT | | | | | | |
| Changed | 2008-07-19 20:28:04 CDT | | | | | | |
| MD5 | Not calculated | | | | | | |
| Hash Lookup Results | UNKNOWN | | | | | | |
| Internal ID | 4011 | | | | | | |

From The Sleuth Kit istat Tool:

Activate Windows
Go to Settings to activate Windows

Fig. 7

How did it get from her computer to competitor's website?

It appears to have been posted there by a threat actor posing as Allison. The email headers of 1) the request for the spread sheet, 2) the email with the attached spreadsheet, and 3) the thank you response were examined. In each instance Jean was communicating with tuckergorge@gmail.com @ IP 208.97.132.81 where the spreadsheet was sent. This IP address is not associated with M57.biz. In addition, the return path of all three emails was simsong@xy.dreamhostps.com and not M57.biz.

(Fig. 8)

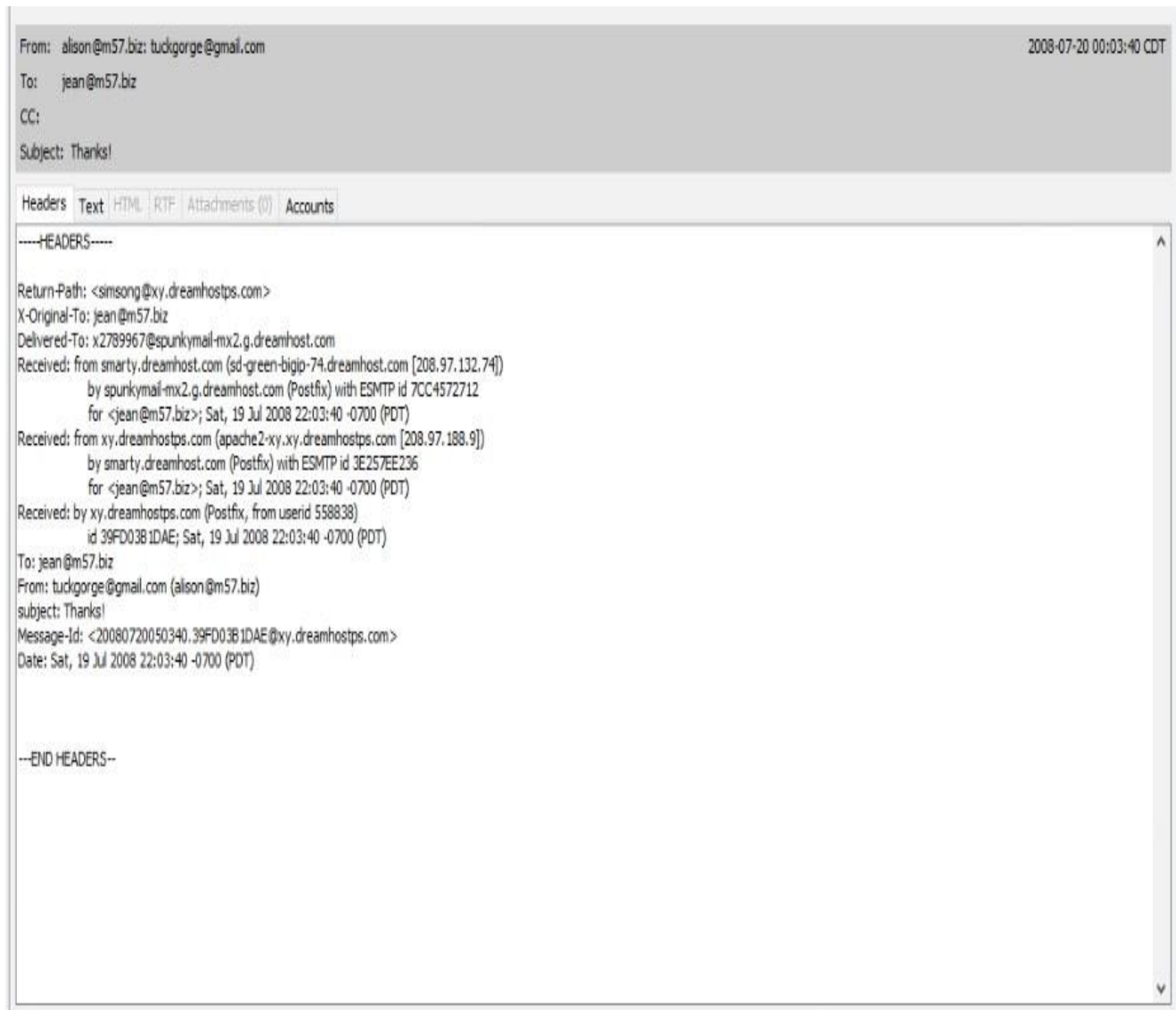


Fig. 8- Autopsy

Who else from the company is involved?

The results were inconclusive. There was no evidence that anyone else was involved

LIMITATIONS

Since the hash value associated with the spreadsheet file was not verified, it cannot be stated as fact that the spreadsheet found on Jean's desktop was the same as the file

attached to the email. The investigation resulted in more questions than answers and was not definitive in several aspects.

REFERENCES

Autopsy user documentation: Email Parser module. (n.d.-b).

http://sleuthkit.org/autopsy/docs/user-docs/4.20.0/email_parser_page.html

DFIRScience. (2022, February 15). *Data artifacts, analysis results and reporting in autopsy 4.19+* [Video]. YouTube.

<https://www.youtube.com/watch?v=5SHB4HwkX28>

Guide to Computer Forensics and Investigations, Nelson, B., Phillips, A., Steuart, C., 6th Ed (2019), Cengage Learning ISBN: 978-1-337-56894-4

GLOSSARY OF TERMS AND DEFINITIONS

2.1. Hashes Values- As evidence is being removed from a device, forensic examiners use tools that calculate **hash values**- a series of numbers representing the content within a file which is used to identify it. Once calculated, the values are stored in the file and remain part of it throughout its custody as evidence in a case. Because no two files will have the same hash values, digital evidence presented in court should have the same hash values that were calculated by the investigator during removal. With a few rare exceptions, any modification to a file result in an entirely different hash value, even if only one character is switched from capital to lowercase.

2.2. A Drive Image is an exact copy of a device's hard drive- the part of an electronic device that stores the operating system, applications, and all digital content such as text files, documents, folders, pictures, videos, and music. The image will include the original drive's empty or unused spaces.

2.3. Live Data Acquisition of Drives- Data acquisition is how forensic investigators recover and collect evidence from a digital device (computers, laptops, tablets, smart phones). There are two types of data acquisition: static, and live acquisitions. Static Acquisition is the more common approach in which the machine is shut down normally and then the disk image is acquired. Live acquisition is the process of capturing the contents of a disk while the computer is running, which must be done to obtain any evidence that is in the computer's immediate memory. When the computer is switched off, this memory is erased.

2.4. Data carving- Allocated space is the area on a hard drive where files already exist until the user deletes them. The space filled by the deleted files then becomes

unallocated space, often known as free space, which can be used to store new files.

Data carving, also known as file carving, is a forensic technique for recovering files in unallocated space. In other words, deleted files.

2.5 Digital forensics tool validation- Tool validation refers to the procedures that forensic analysts must follow to ensure that their tools function as intended. Examiners can utilize forensic drive images made for desktop and mobile devices to evaluate a tool; these images are put online and describe what the tool should uncover as evidence. Another procedure is to carry out the same operations with comparable forensics tools to see whether the same results are obtained.

APPENDIX I

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
|----|---------------------------|-------------|-------------|-----------|----------------------------|---|---|---|---|---|---|---|---|---|---|---|
| 1 | M57.biz company | | | | | | | | | | | | | | | |
| 2 | | | | | | | | | | | | | | | | |
| 3 | | | | | | | | | | | | | | | | |
| 4 | | | | | | | | | | | | | | | | |
| 5 | | | | | | | | | | | | | | | | |
| 6 | Name | | Position | Salary | SSN (for background check) | | | | | | | | | | | |
| 7 | Alison | Smith | President | \$140,000 | 103-44-3134 | | | | | | | | | | | |
| 8 | Jean | Jones | CFO | \$120,000 | 432-34-6432 | | | | | | | | | | | |
| 9 | | | | | | | | | | | | | | | | |
| 10 | Programmers: | | | | | | | | | | | | | | | |
| 11 | Bob | Blackman | Apps 1 | 90,000 | 493-46-3329 | | | | | | | | | | | |
| 12 | Carol | Canfred | Apps 2 | 110,000 | 894-33-4560 | | | | | | | | | | | |
| 13 | Dave | Daubert | Q&A | 67,000 | 331-95-1020 | | | | | | | | | | | |
| 14 | Emmy | Arlington | Entry Level | 57,000 | 404-98-4079 | | | | | | | | | | | |
| 15 | | | | | | | | | | | | | | | | |
| 16 | Marketing | | | | | | | | | | | | | | | |
| 17 | Gina | Tangers | Creative 1 | 80,000 | 980-97-3311 | | | | | | | | | | | |
| 18 | Harris | Jenkins | G & C | 105,000 | 887-33-5532 | | | | | | | | | | | |
| 19 | | | | | | | | | | | | | | | | |
| 20 | BizDev | | | | | | | | | | | | | | | |
| 21 | Indy | Counterchir | Outreach | 240,000 | 123-45-6789 | | | | | | | | | | | |
| 22 | | | | | | | | | | | | | | | | |
| 23 | | | | | | | | | | | | | | | | |
| 24 | | | | | | | | | | | | | | | | |
| 25 | Annual Salaries | | | ### | | | | | | | | | | | | |
| 26 | Benefits | | 30% | \$302,700 | | | | | | | | | | | | |
| 27 | | | | | | | | | | | | | | | | |
| 28 | Total Salaries + Benefits | | | ### | | | | | | | | | | | | |
| 29 | Monthly burn | | | ### | | | | | | | | | | | | |
| 30 | | | | | | | | | | | | | | | | |
| 31 | | | | | | | | | | | | | | | | |
| 32 | | | | | | | | | | | | | | | | |
| 33 | | | | | | | | | | | | | | | | |
| 34 | | | | | | | | | | | | | | | | |
| 35 | | | | | | | | | | | | | | | | |
| 36 | | | | | | | | | | | | | | | | |
| 37 | | | | | | | | | | | | | | | | |
| 38 | | | | | | | | | | | | | | | | |



Activate Windows
Go to Settings to activate Windows

APPENDIX II

Thanks!

Delivery Time: 7/20/2008, 0:03:40, GMT -5:00

From: alison@m57.biz <tuckgorge@gmail.com>

To: jean@m57.biz

Cc:

Bcc:

Jean,

Thanks for the file. I'll handle it from here. to: jean@m57.biz
from: (alison@m57.biz) tuckgorge@gmail.com
subject: Thanks!

Jean,

Thanks for the file. I'll handle it from here.

Once again, please don't tell anyone about this.

The screenshot displays the 'User Activity' application interface. On the left, a sidebar lists various system analysis tools, with 'User Activity' currently selected. The main window shows a list of activity categories and their counts, such as 'Most Recently Used (36)', 'Installed Programs (23)', and 'Event Logs (0)'. A 'Summary' dialog box is open, providing a detailed breakdown of the 302 total items, including counts for 'Most Recently Used', 'Installed Programs', 'Event Logs', 'UserAssist', 'Shellbags', 'Recycle Bin', 'Browser History', 'Website Logins', 'Bookmarks', 'USB', and 'Mounted Volumes'. The 'User Activity' list is sorted by time, showing entries for 'Administrator' and 'Jean' with timestamps ranging from 7/20/2008 to 7/20/2009.