**Module 12 Final Case Study: M57.biz**

Alice Mace

Computer Information Systems, Bellevue University

CIS 607: Computer Forensics

Professor Anthony Geron

August 7, 2022

1. **Abstract**

In the case of M57.biz, a web start-up company developing a body art catalog, a spreadsheet containing confidential corporate information was posted as an attachment on the "technical support" page of a competitor's website. The spreadsheet “m57.biz.xls” was found on the CFO’s computer, Jean. An important client, one of the first-round funders, requested an investigation to determine answers to the following questions:

* + - * When did Jean create this spreadsheet?
      * How did it get from her computer to competitor's website?
      * Who else from the company is involved?

The following conclusions were found upon completion of the investigation and analysis of results. The “m57biz.xls” file was created on 2008-07-19 20:28:03 CDT following the request from a spoofed email that appeared to have come from the account of Alison, the President. It is likely that Jean did not realize Alison’s email address was being spoofed and that when she sent her reply with the spreadsheet attachment, the recipient was the one who posted it on the competitor’s website. There is no evidence of involvement among any other employees of M57.biz in the creation or sharing of the spreadsheet. Analysis and findings in this report were generated using the Autopsy 4.17.0 software.

1. **Table of Contents**
2. Abstract……………………………………………………………………......2
3. Table of Contents……………………………………………………….........3
4. Investigation………………………………………………...…………………4

3.1 Introduction…………………………………………………………..…....4

3.2 When did Jean create this spreadsheet?...........................................5

3.3 How did it get from her computer to competitor's website?................7

3.4 Who else from the company is involved?.........................................10

IV. Conclusion………………………………………………………………………..10

V. References…………………………………………………………………..……11

VI. Glossary……………………………………………………………………..……11

1. **Investigation**
   1. **Introduction**

In the case of M57.biz, a web start-up company developing a body art catalog, a spreadsheet containing confidential corporate information was posted as an attachment on the "technical support" page of a competitor's website. The spreadsheet “m57.biz.xls” was found on the CFO’s computer, Jean. The President, Alison, stated that she was not aware of the spreadsheet, did not ask for it to be created, and never received it by email. Jean stated that she was asked by Alison to prepare the spreadsheet as part of a new funding round and to email it to her. An important client, one of the first-round funders, requested an investigation be conducted to determine answers to the following questions:

* + - * When did Jean create this spreadsheet?
      * How did it get from her computer to competitor's website?
      * Who else from the company is involved?

The structure of this report will follow the order of the above questions in the Investigation section, followed by a Conclusion with a summary of the findings and analytical results. Analysis and findings in this report were generated using the Autopsy 4.17.0 software. Two image files were provided for analysis; however, Autopsy would not allow the “nps-2008-jean.E02” file to be added as a data source and will therefore not be included in this analysis. An image of the spreadsheet referenced throughout the report is shown in Figure 3.1.1 below.

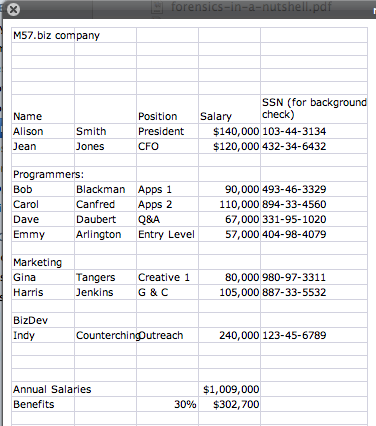


Figure 3.1.1. m57biz.xls

* 1. **When did Jean create this spreadsheet?**

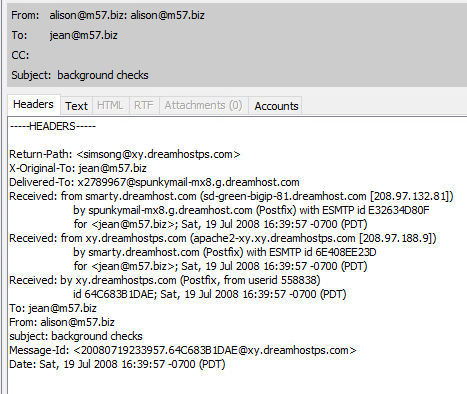
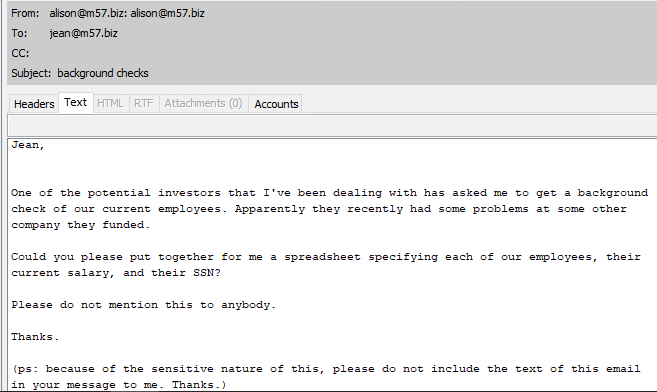
I identified two files titled “m57biz.xls” while searching the image of Jean’s computer. I found that one was saved on the desktop and the other was in Jean’s Outlook files from an email attachment she sent in a reply to alison@m57.biz upon looking at the metadata. Alison’s email address had been spoofed and would actually send the email to the simsong@xy.dreamhostps.com address, shown in the email header information in Figure 3.2.2. The original email (Figure 3.2.1) received on 19 July 2008 at 16:39:57 PDT requested that Jean build a spreadsheet with specific employee information to support background checks.Figure 3.2.1. Initial request for spreadsheet

Figure 3.2.2. Header information from Figure 3.2.1

The “m57biz.xls” desktop file was created on 2008-07-19 20:28:03 CDT and has the same date/time stamp for its last modified date/time. This also matched the date/time stamps on the file in the email. No evidence of manipulation was found, so it is unlikely any date/time stamp modification occurred. Both files, on the desktop and in the email attachment, share the same MD5 hash of “e23a4eb7f2562f53e88c9dca8b26a153” which ensures that there were no modifications between the file created and saved on the desktop and the file that was emailed.

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

On 19 July 2008 at 18:22:45 PDT another email was sent to Jean from the spoofed address requesting the information in the spreadsheet immediately (Figure 3.3.1).

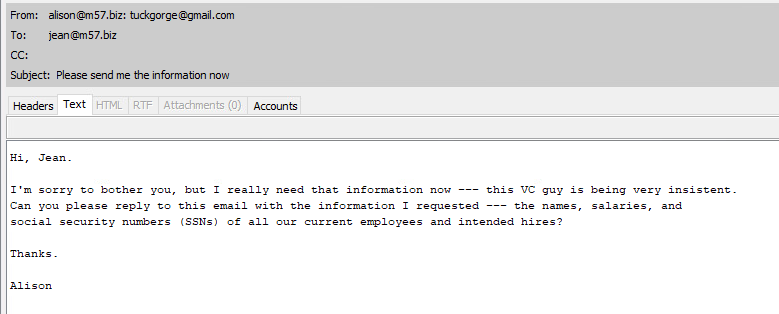


Figure 3.3.1. Spoofed email urgently requesting information in the spreadsheet

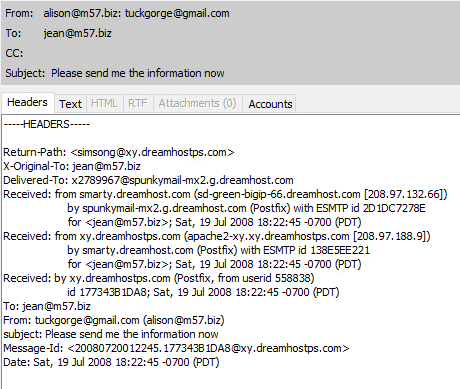


Figure 3.3.2. Header information from Figure 3.3.1

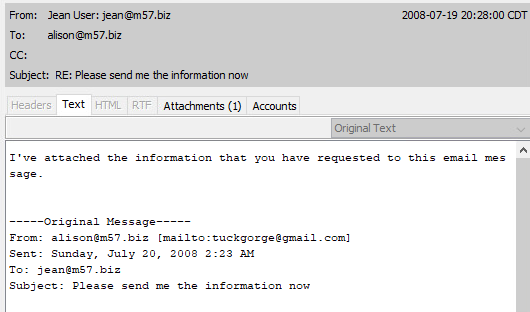
Jean replied to the email with the spreadsheet attachment, as shown in Figure 3.3.3.

Figure 3.3.3. Jean’s email with the spreadsheet attachment

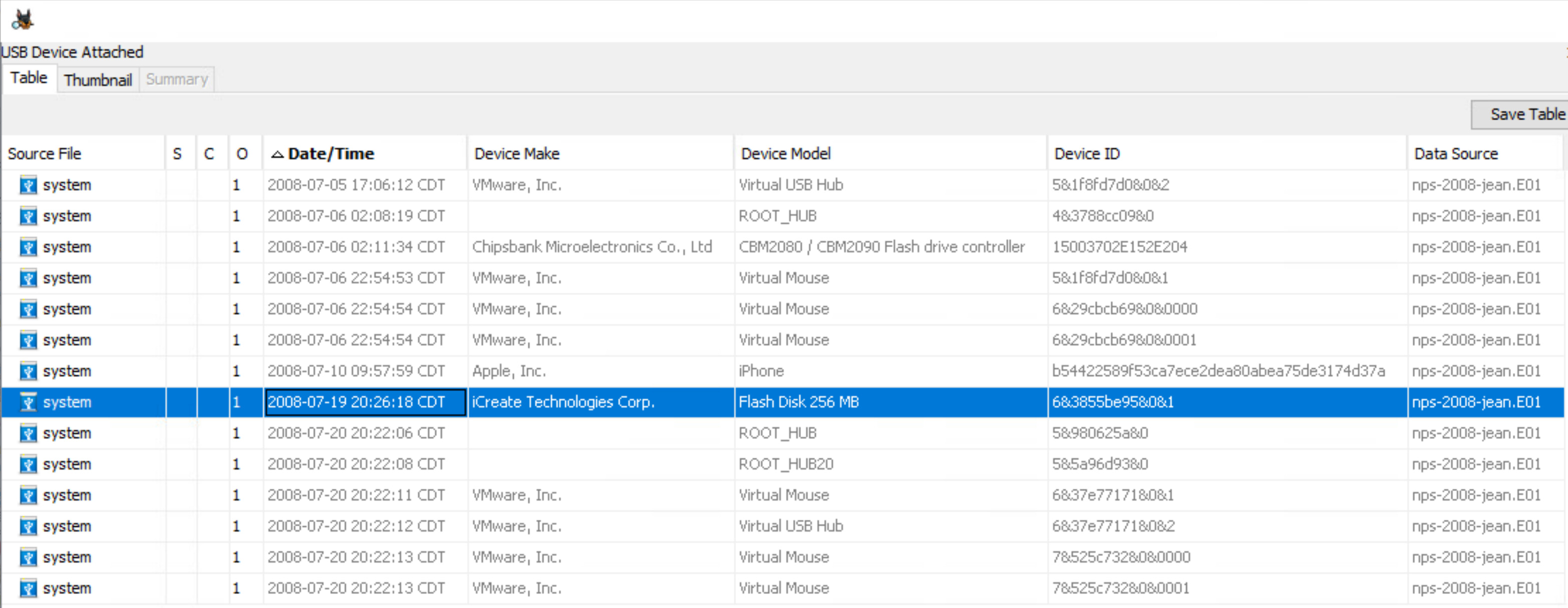
A USB device was attached to the device while logged in under Jean’s account approximately two minutes before Jean sent the email containing the spreadsheet (Figure 3.3.4). It is possible that the spreadsheet was saved to the USB, but it is unknown for certain if the file was saved there or where the USB resides now. Other USB devices connected were before the spreadsheet was created or appear to support a virtual mouse connection.

Figure 3.3.4. USB device connection history

I detected an additional user profile named “Devon” on this device, but there is no evidence that this user had access to the “m57biz.xls” spreadsheet. No evidence was found of the spreadsheet being embedded in another file that could have been shared. The web history of this device image did not show any evidence of potential competitors websites visited. No evidence was found of a virtual machine being used on this device that could have been used to share the spreadsheet.

* 1. **Who else from the company is involved?**

No evidence was found of the spreadsheet or information it contains being shared with any employee or other individual other than the email chain documented in section 3.3. The only correspondence regarding the information in the spreadsheet was found after it had been posted on the competitors website. As employees began to find out, Bob, Carol, and Alison, all M57.biz employees, emailed Jean asking for information of what was going on and confirming if the information they found was accurate.

1. **Conclusion**

The M57.biz confidential corporate spreadsheet created by Jean, the CFO, was posted on a competitor’s website. Several employees were concerned about the situation and one of the first-round funders of M57.biz requested an investigation be conducted to determine details of the spreadsheet’s creation and release. The following conclusions were found upon completion of the investigation and analysis of results.

The “m57biz.xls” file was created on 2008-07-19 20:28:03 CDT following the request from a spoofed email that appeared to had come from Alison’s account. It is likely that Jean did not realize Alison’s email address was being spoofed and that when she sent her reply with the spreadsheet attachment, the recipient was the one who posted it on the competitors website. There is no evidence of any other employees of M57.biz being involved in the creation or sharing of the spreadsheet.

1. **References**

Autopsy. (2020, October). *Autopsy User Documentation* (4.17.0). Basis Technology.

Nelson, B., Phillips, A., & Steuart, C. (2018). Guide To Computer Forensics and

Investigations - Standalone Book (6th ed.). Cengage Learning.

1. **Glossary**

CFO – Chief Financial Officer

MD5 hash – Message Digest 5 – An algorithm that produces a hexadecimal value of a file or storage media. Used to determine whether data has been changed.

Metadata – Information stored in the Master File Table that contains information about access rights, date and time stamps, system attributes, and other information about files.

Virtual machine – Emulated computer environments that simulate hardware and can be used for running operating systems separate from the physical computer.