**Jean, CFO, M57.biz Case Study**

CIS607 Forensic Case Study Assignment 12

By Daniel Carbajal

Bellevue University

November 19, 2022

Table of Contents

[**Abstract** 3](#_Toc119769679)

[**Analysis** 4](#_Toc119769680)

[**Introduction** 4](#_Toc119769681)

[**Background** 4](#_Toc119769682)

[**Detailed Analysis** 6](#_Toc119769683)

[**Conclusion** 11](#_Toc119769684)

[**Appendix** 13](#_Toc119769685)

# **Abstract**

This case involved a disclosure of sensitive employee information, at a small company called M57.biz, that appeared on a competitor’s website and was not known how it got there. The only person who had this information was named Jean, the CFO of M57.biz. She claims she emailed the information to her President based on the President’s request of which the President had no recollection of ever asking for this information. After analysis of Jean’s laptop image it was discovered that she was the victim of an email phishing campaign and accidentally sent out the sensitive information unknowingly thinking that she was sending it to her President. Below are the background and analysis conducted for this investigation in order to arrive at this conclusion.

# **Analysis**

## **Introduction**

The firm of Daniel Carbajal has been tasked to investigate Jean, the CFO, at M57.biz. M57.biz claims tha a spreadsheet containing confidential information was posted as an attachment in the "technical support" forum of a competitor's website. It is believed that the only person who had a copy of the spreadsheet was CFO Jean on her computer. Jean claims that she does not know how the information was leaked and that she sent the spreadsheet to her President, Alison, upon her President’s request. The President claims she never asked for a copy nor ever received a copy of the spreadsheet. The firm has retained a disk image of Jean’s computer in to conduct analysis and an investigation as to how the spreadsheet was leaked and whom, if any, was involved within the company.

## **Background**

Facts of the case:

* M57.biz is a hip web start-up developing a body art catalog
* $3M in seed funding; now closing $10M round
* 2 founder/owners
* 10 employees hired first year

Current staff:

* President: Alison Smith
* CFO: Jean
* Programmers: Bob, Carole, David, Emmy
* Marketing: Gina, Harris
* BizDev: Indy

M57.biz is a virtual corporation that develops a body art catalog. Its programmers work remote out of their houses and they have daily online chat session to cover the details. There is a weekly in-person meeting for the programmers at the office park. Marketing and Business Development are mostly on the road and work out of hotel rooms or public spaces like Starbucks. There are in-person meetings once every two weeks for these employees.

Most documents are exchanged by email, and somehow a spreadsheet containing confidential information was posted as an attachment in the "technical support" forum of a competitor's website. The spreadsheet came from CFO Jean's computer and the investigating firm has obtained a copy of the spreadsheet, "m57biz.xls" seen in *Figure 1* below and a disk image of Jean’s computer has been taken for further analysis.

Graphical user interface, application, table

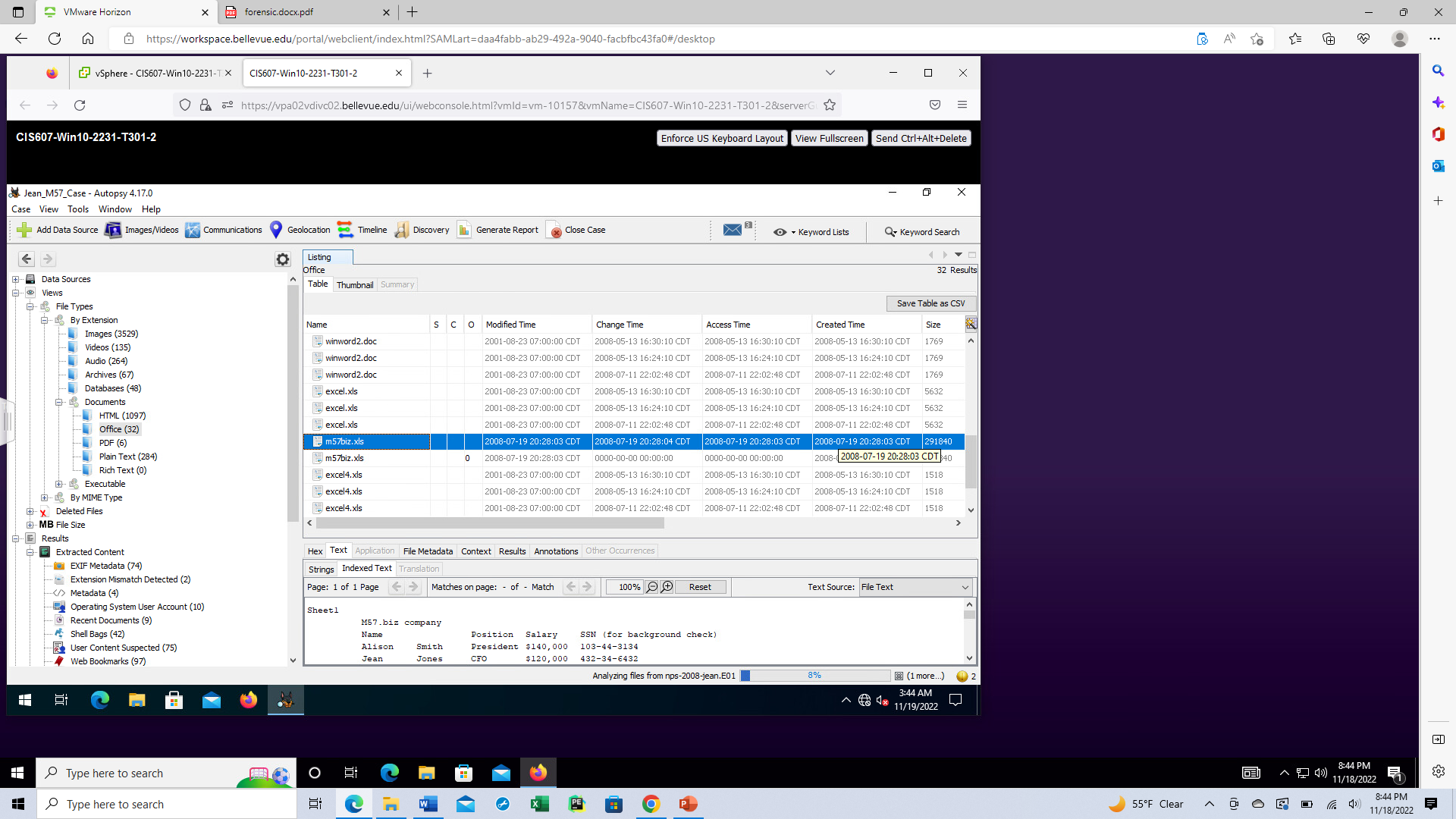
Description automatically generated

***Figure 1.*** Copy of the Spreadsheet Containing Sensitive Information

## **Detailed Analysis**

The analysis of the data is centered around the "m57biz.xls" spreadsheet. The first step was to use a well-known forensics tool that would perform the analysis needed to reach a conclusion. Autopsy was the chosen tool as it has everything needed for this analysis and it is a well-known and recognized tool. Autopsy was used to look at a disk image of Jean’s laptop to investigate how the spreadsheet was leaked from her computer an onto the competitor’s website. A disk image is an exact copy of Jean's laptop disk drive and is used to investigate analyzed the laptop without altering or causing harm to Jean's laptop during the investigation.

The first step was to locate the "m57biz.xls" file and find out when it was created and then examine the disk image to find out how it was leaked to a competitor's website. *Figure 2* shows the data from Autopsy showing the spreadsheet was located on Jean’s computer, and its created date is shown to be 07/19/2008 at 28:03 CDT.



***Figure 2.*** Spreadsheet found in Jean’s disk drive using Autopsy forensic tool.

For the second step, a search was made on this file to locate where on the Jean’s disk drive it was located and *Figure 3* shows that is was on her Desktop at data path as follows:

***C:\Documents and Settings\Jean\Desktop\m57biz.xls.***

A screenshot of a computer

Description automatically generated

***Figure 3.*** Datapath to Jean’s spreadsheet document.

The third step in the analysis is to look where the spreadsheet may have been copied or attached and delivered to the competitor’s website. It is also important to find out if anyone else was involved in this incident, so we can begin our investigation with the possible suspects. It is possible that the copy was pasted on the the competitor’s website, so looking at images or HTML code could be a possibility. However, this is a virtual company that relies primarily on email and chat services. So, it is more likely to start looking there, since there are a lot of potential places to start.

The next step was to do a search on the spreadsheet to see if it got somewhere is was not supposed to be. A list of words were used to search for the spreadsheet to include:

***Keywords***: spreadsheet, m57biz.xls, attachement, attached, attach, Excel sheet, salaries, and confidential.

During this search, an email file was found that included the word ‘**attached’**. Looking a

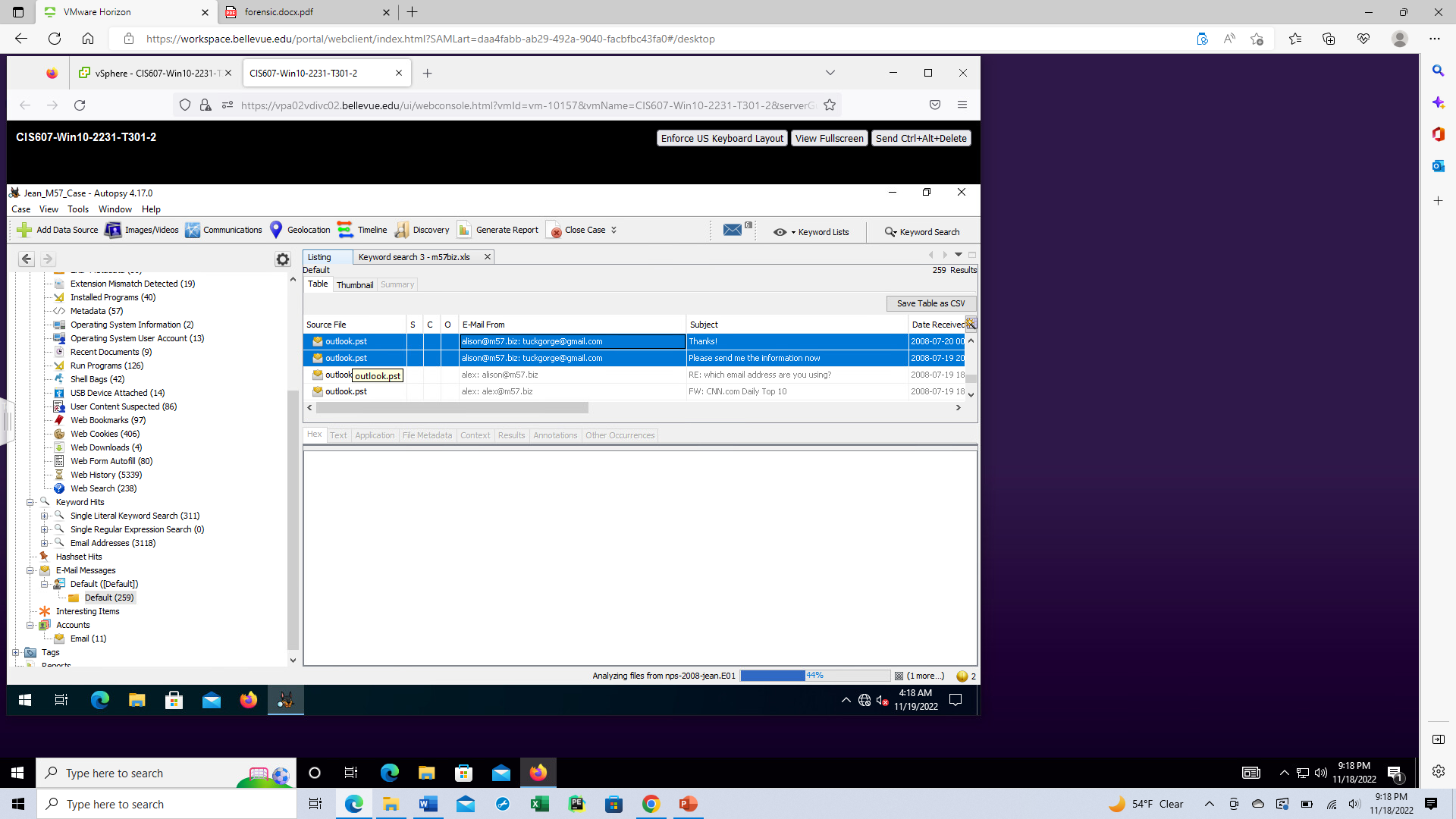
*Figure 4*, we found some discrepancies in the email. While, it appears that Jean, the CFO, whose email is [jean@m57.biz](mailto:jean@m57.biz) is sending and email to the President, Alison, whose email is [alison@m57.biz](mailto:alison@m57.biz) there appears to be a email address going to [tuckgeorge@gmail.com](mailto:tuckgeorge@gmail.com) . Thus, this appears there may be a spoofed email that Jean may have unknowingly sent an email to. Email spoofing is defined as impersonating, masquerading, or faking the sending address of an email transmission to gain illegal entry into a secure system or data. Further analysis is needed to reach a more conclusive result.

A screenshot of a computer

Description automatically generated

***Figure 4.*** Email with word ‘attached’ on it showing conflicting email addresses.

Thus, the immediate focus is on the emails sent between the CFO Jean and the President Alison A search on the unknown email is done and it is found that there were several emails between Jean and whom she though was President Alison. Two of these emails were found and highligted during the email search. *Figure 5* shows two emails found with the address [tuckgeorge@gmail.com](mailto:tuckgeorge@gmail.com), and these two emails need to be analyzed to discover what may have occurred between CFO Jean and this spoofed email account.



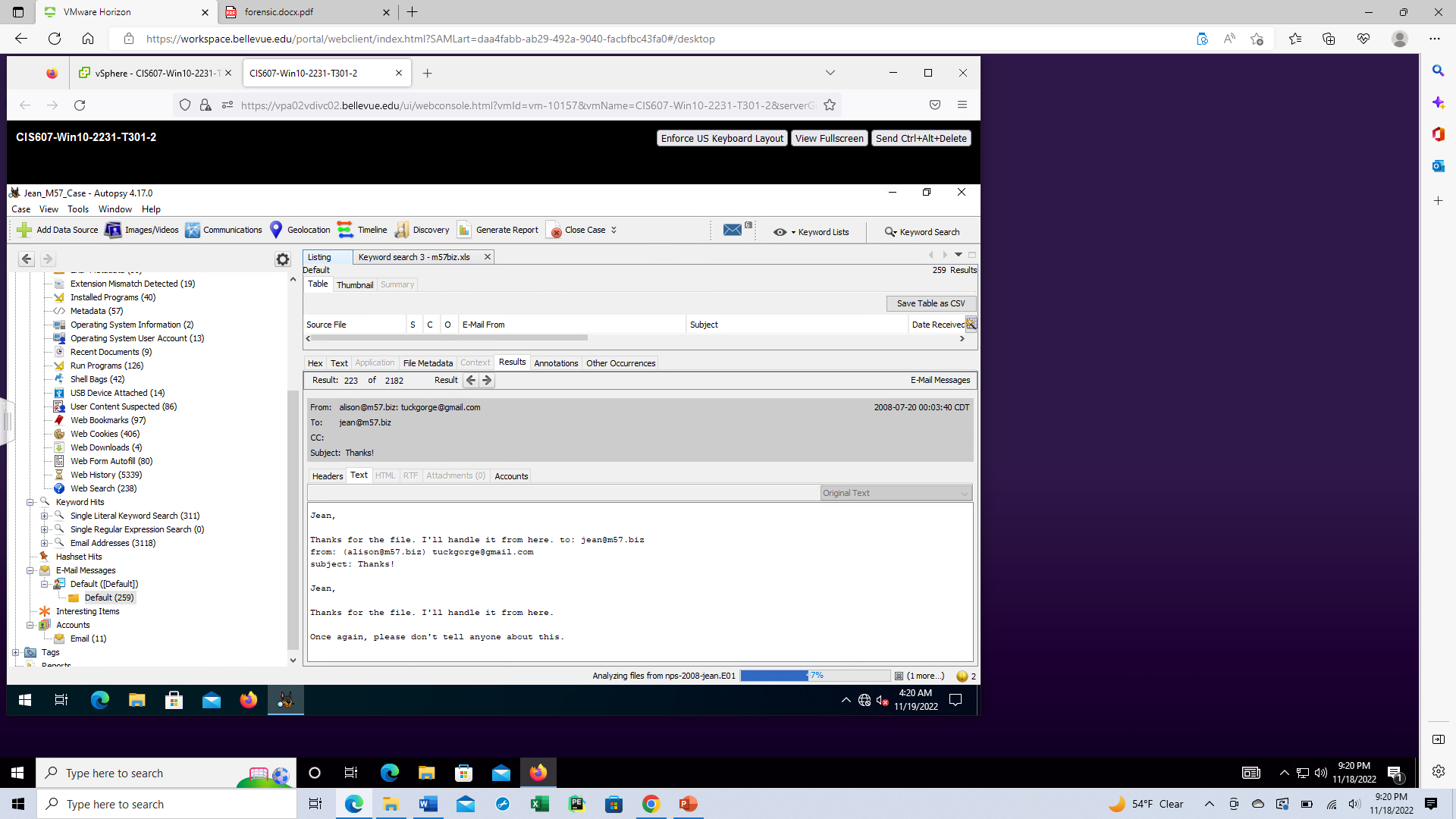
***Figure 5.* Two emails with** [**tuckgeorge@gmail.com**](mailto:tuckgeorge@gmail.com)**, found in CFO Jean’s disk drive.**

The first email seen in *Figure 6*, shows what appears to be [alison@57.biz](mailto:alison@57.biz) asking for the information contained in the spreadsheet that appeared in the competitor’s website. It appears that [tuckgeorge@gmail.com](mailto:tuckgeorge@gmail.com)somehow got a hold of President Alison’s email and spoofed his email with her name in order to get CFO Jean to send the sensitive information. The second *Figure 7*, shows that [tuckgeorge@gmail.com](mailto:tuckgeorge@gmail.com)has received the information from CFO Jean that was requested and asks CFO Jean not to mention this to anyone. Thus, CFO Jean appears to have been the victim of a spoofing campaign that got the information leaked and then somehow appeared on their competitor’s website.

A screenshot of a computer

Description automatically generated

***Figure 6.*** Email from [tuckgeorge@gmail.com](mailto:tuckgeorge@gmail.com) impersonating President Alison asks for data.



***Figure 7.*** Email from [tuckgeorge@gmail.com](mailto:tuckgeorge@gmail.com) acknowledging information was received.

# **Conclusion**

Upon further investigation both President Alison and CFO Jean are not involved in any wrongdoing. They both told the truth in both of their interviews. CFO Jean unfortunately sent sensitive information to [tuckgeorge@gmail.com](mailto:tuckgeorge@gmail.com)unknowingly think that President Alison was asking for the information. It appears that no other personnel were involved in any wrongdoing either. Based on this information it is the opinion of this firm that CFO Jean should not be charged with a crime as she was a victim of email spoofing. In summary the following was found during the investigation.

* CFO Jean was a victim of phishing in particular a term known as ‘spear phishing’.
* CFO Jean unkowingly sent sensitive information to an outside source
* President Alison and all other employees are clear of wrongdoing.

It is recommended that M57.biz increases their knowledge of email security, email integrity, and security of their email server and gateway. It is recommended that cybersecurity training is given to all employees, espcially on phising and email spoofing. It is also recommended that an investigation be conducted into whom [tuckgeorge@gmail.com](mailto:tuckgeorge@gmail.com) belongs to, and how they gained access to Alison and Jean’s email address and sensitive information. Also an investigation should be conducted to see if its possible to find a connection between [tuckgeorge@gmail.com](mailto:tuckgeorge@gmail.com) and the competitor who may have been involved in illegal activity. This concludes this investigation and further questions can be addressed via email or via phone. Attached is an Appendix following the references, which *Figure* 8 thru 21 shows a more detailed version of the steps taken using the forensic tool Autopsy to discover all information regarding this case.

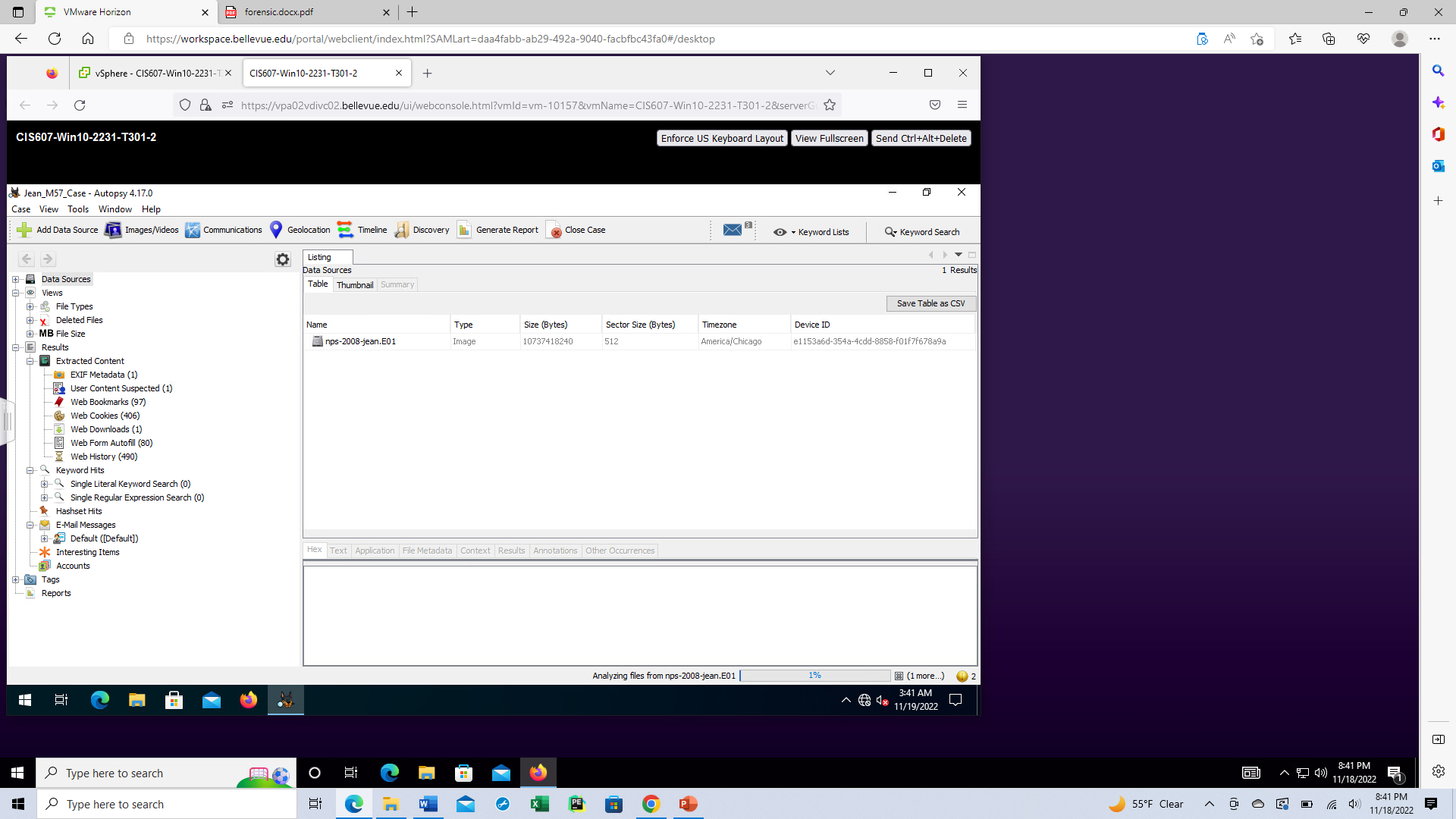
**References**

Autopsy, Forensic Tool, <https://sleuthkit.org/autopsy/>

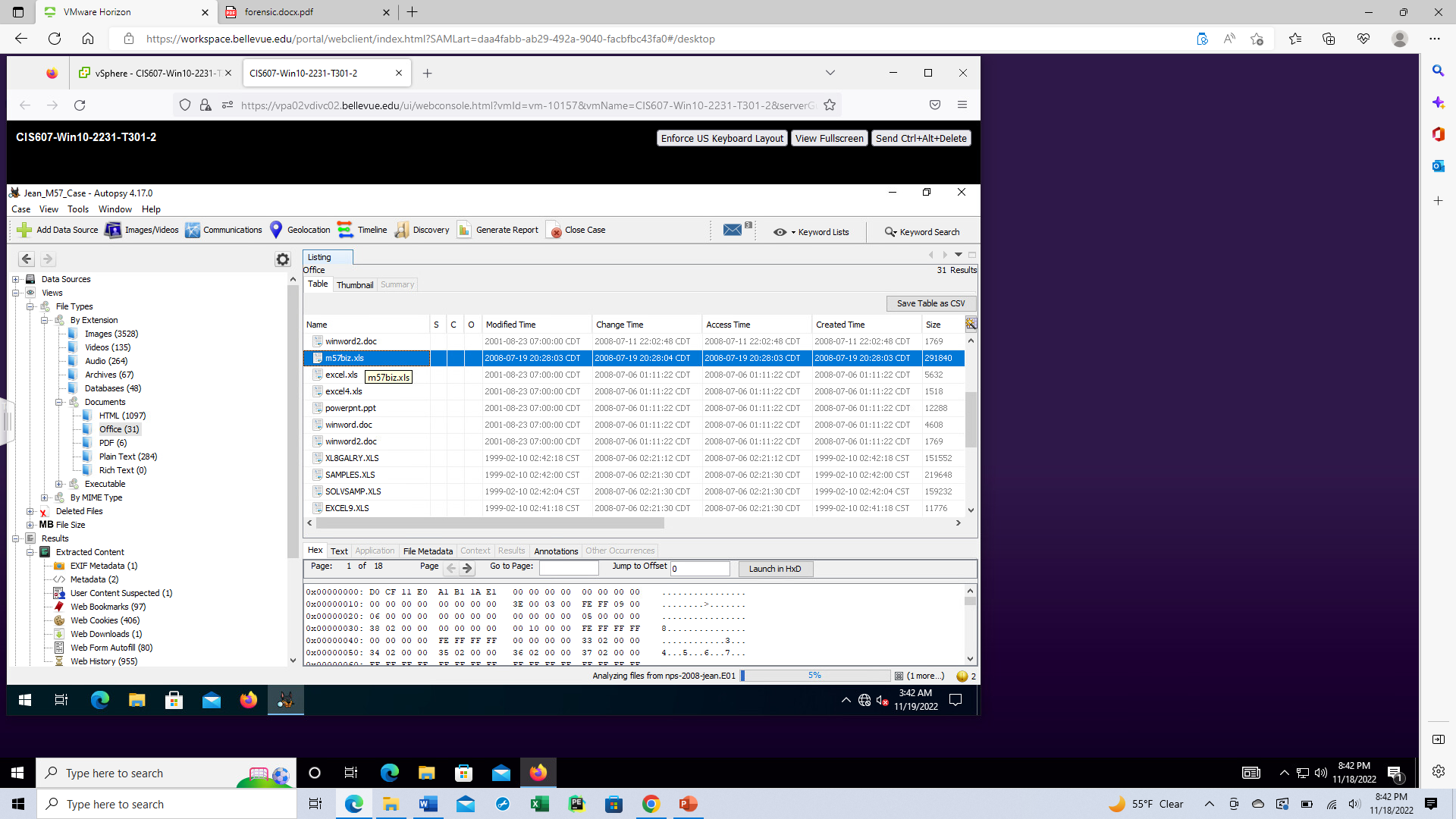
Nelson, B., Phillips, A., and Steuart, C.,(2018). Guide To Computer Forensics and Investigations, 6th Edition, Cengage, Boston, MA.

NIST, Phishing, <https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing>

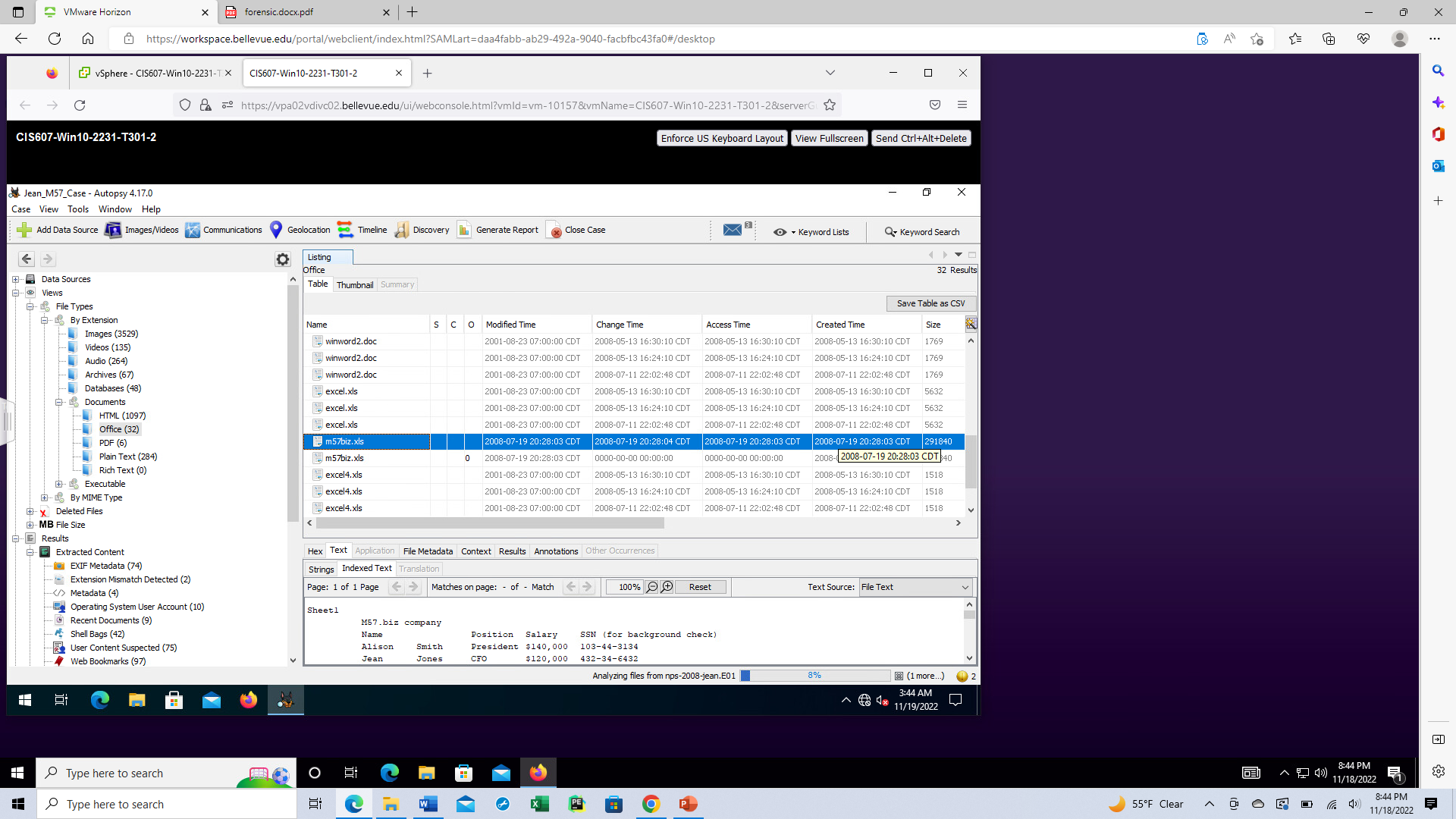
# **Appendix**



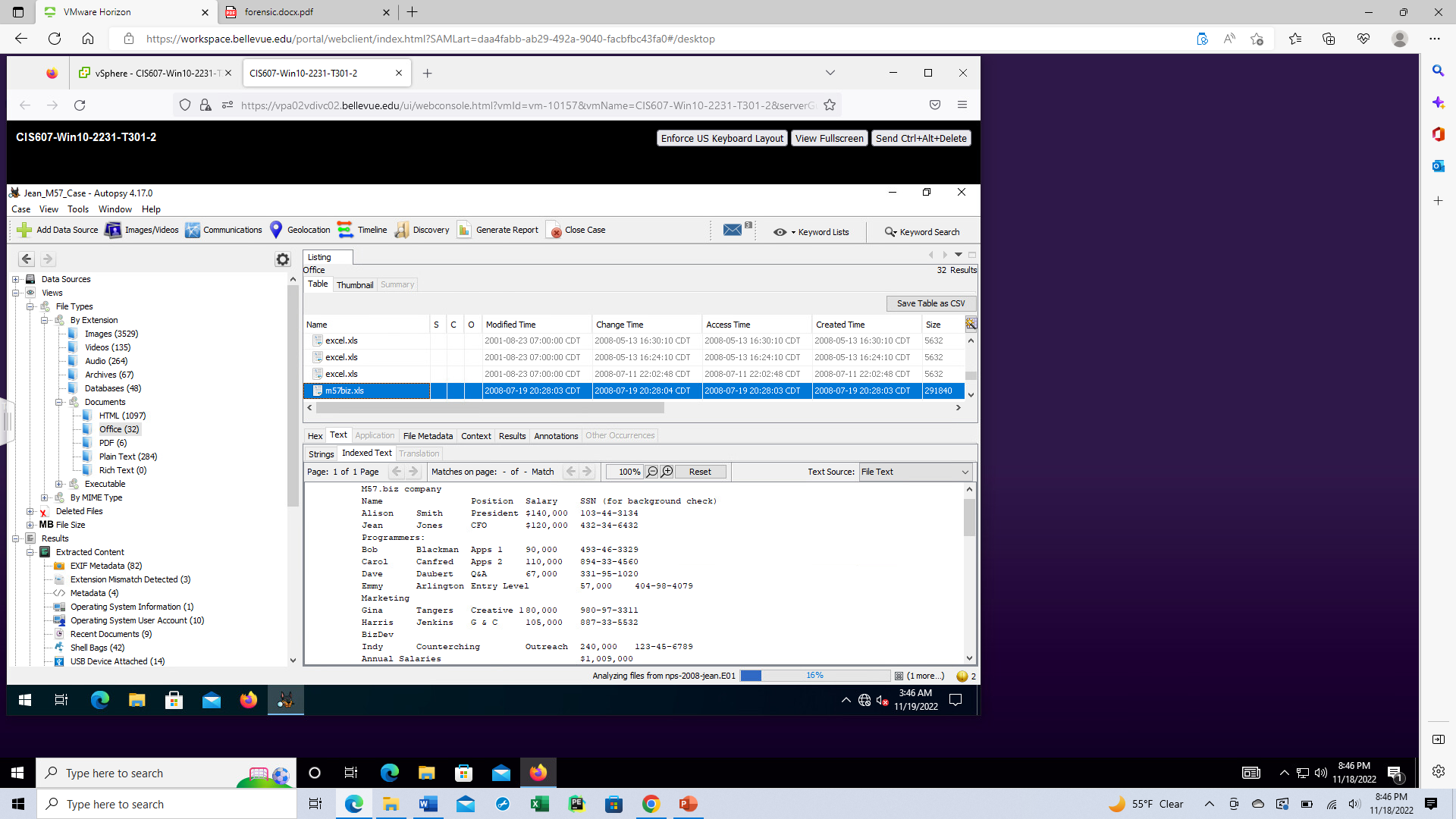
***Figure 8.*** Autopsy showing copy of CFO Jean disk image.



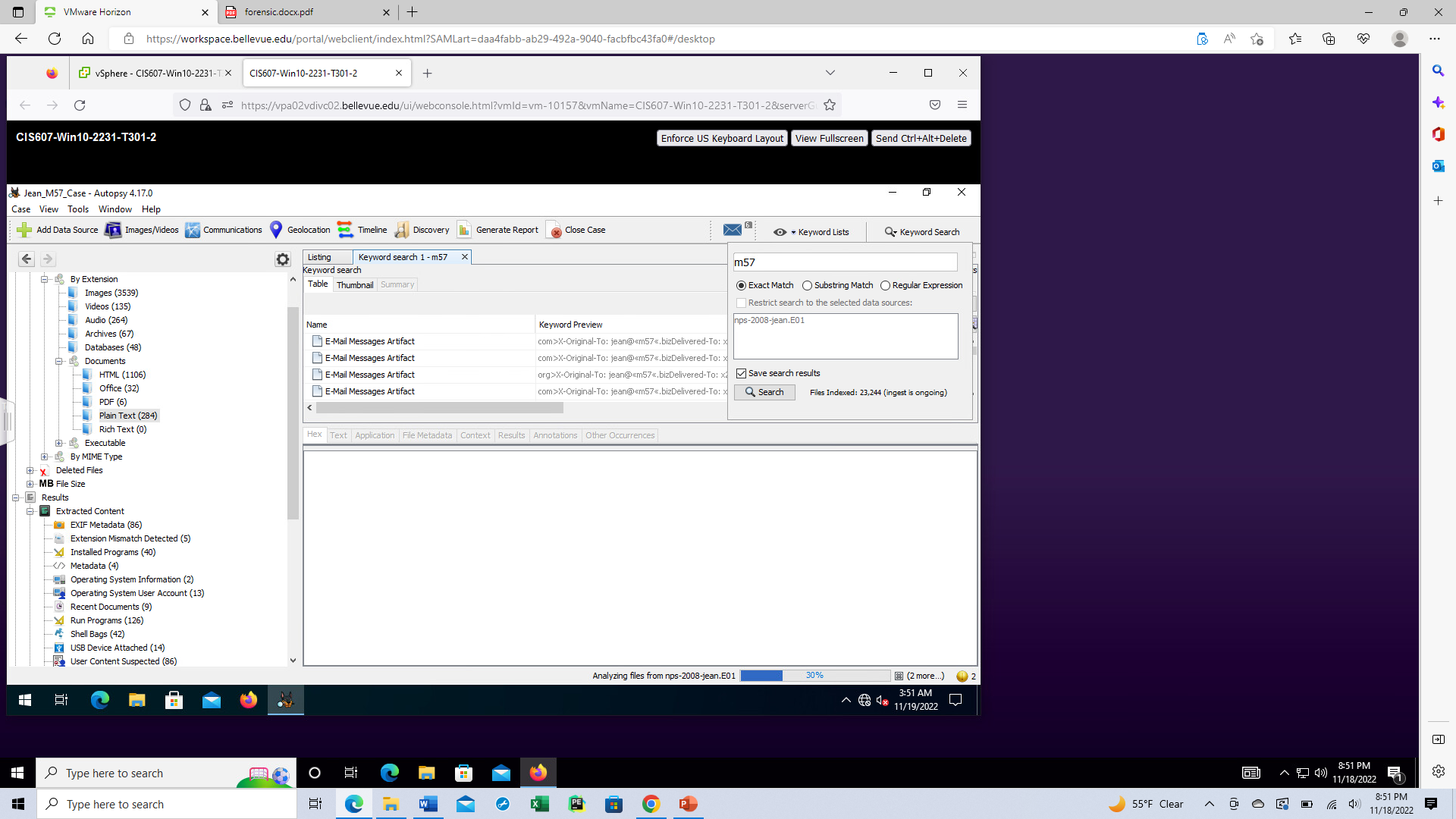
**Figure 9.** Initial search of ‘m57biz.xls’ using Autopsy



**Figure 10.** Initial Listing of Time that File was created.



**Figure 11.** Analyzing file to make sure it contains sensitive information.



**Figure 12.** Making a search on more files or media containing m57 in the data

A screenshot of a computer

Description automatically generated

**Figure 13**. Finding of location of spreadsheet on CFO Jean’s disk image.

A screenshot of a computer

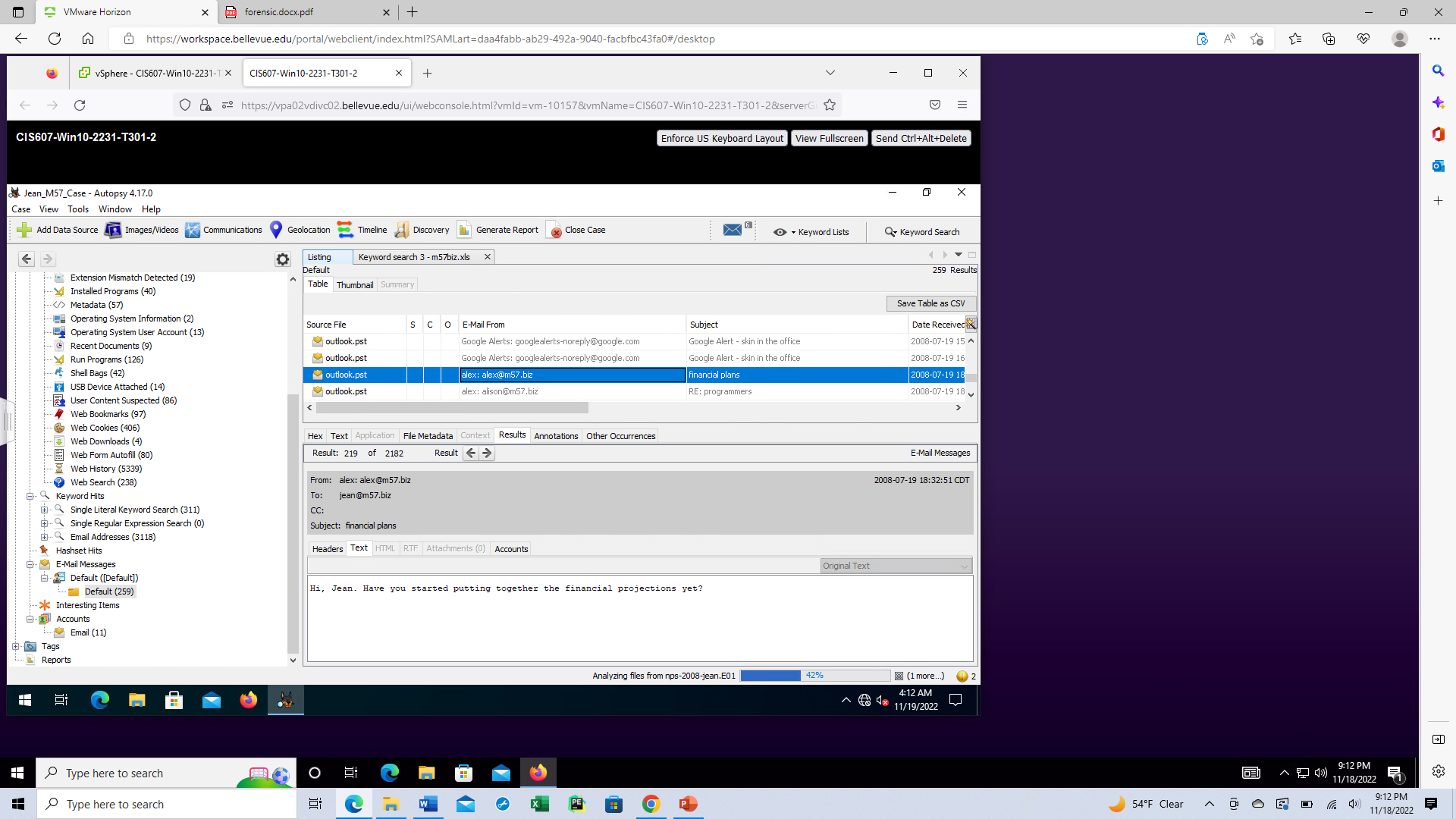
Description automatically generated

**Figure 14.** Using key word search of different terms for spreadsheet and attachment points to email trail.

A screenshot of a computer

Description automatically generated

**Figure 15.** Some emails showing Alison had two different emails which could have complicated CFO Jean into sending out information unknowingly

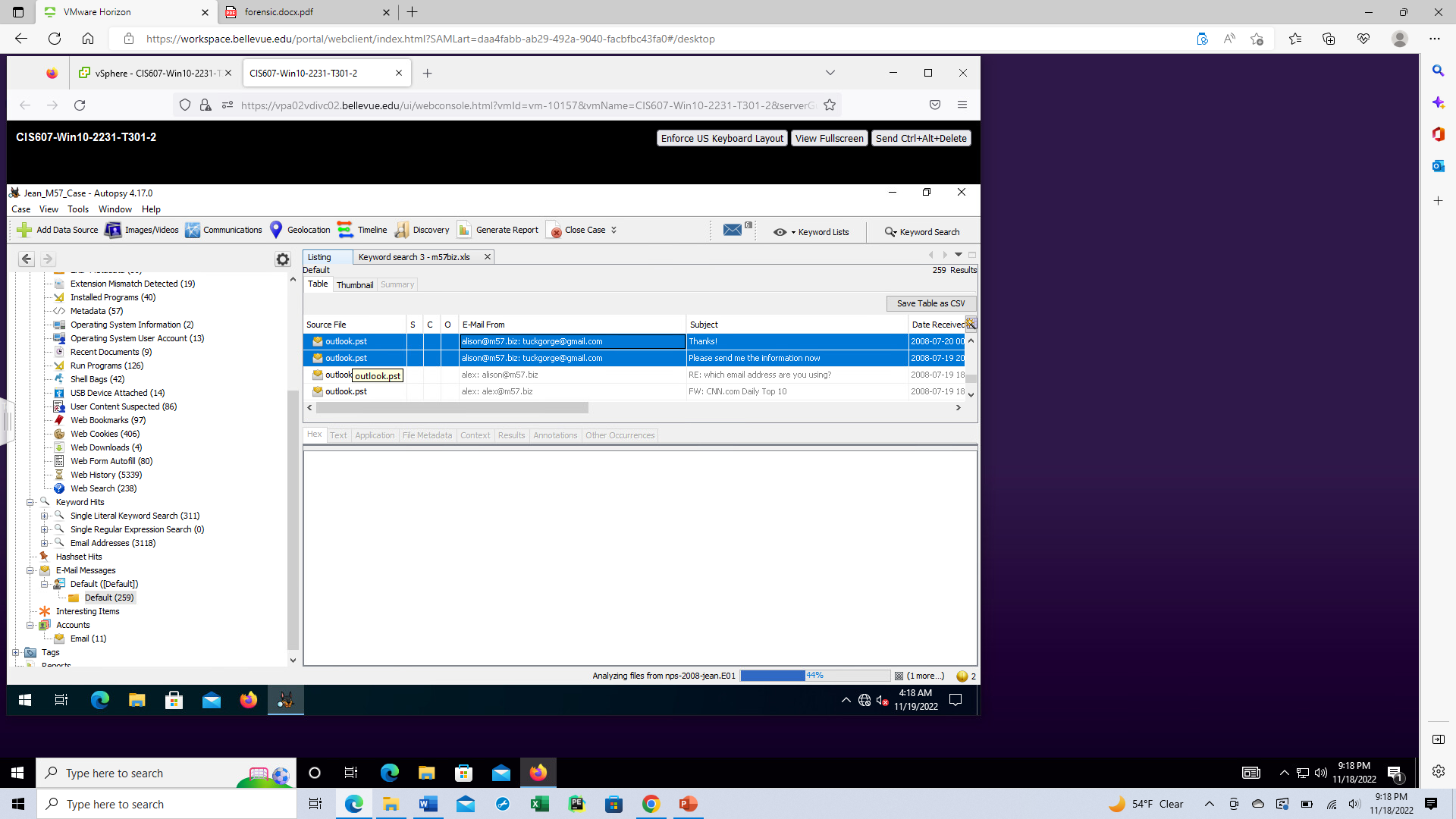


**Figure 16**. Email from Alison to Jean showing she did ask for other sensitive information before the incident.

A screenshot of a computer

Description automatically generated

**Figure 17.** Initial File showing the word attached with possible spoofed email.

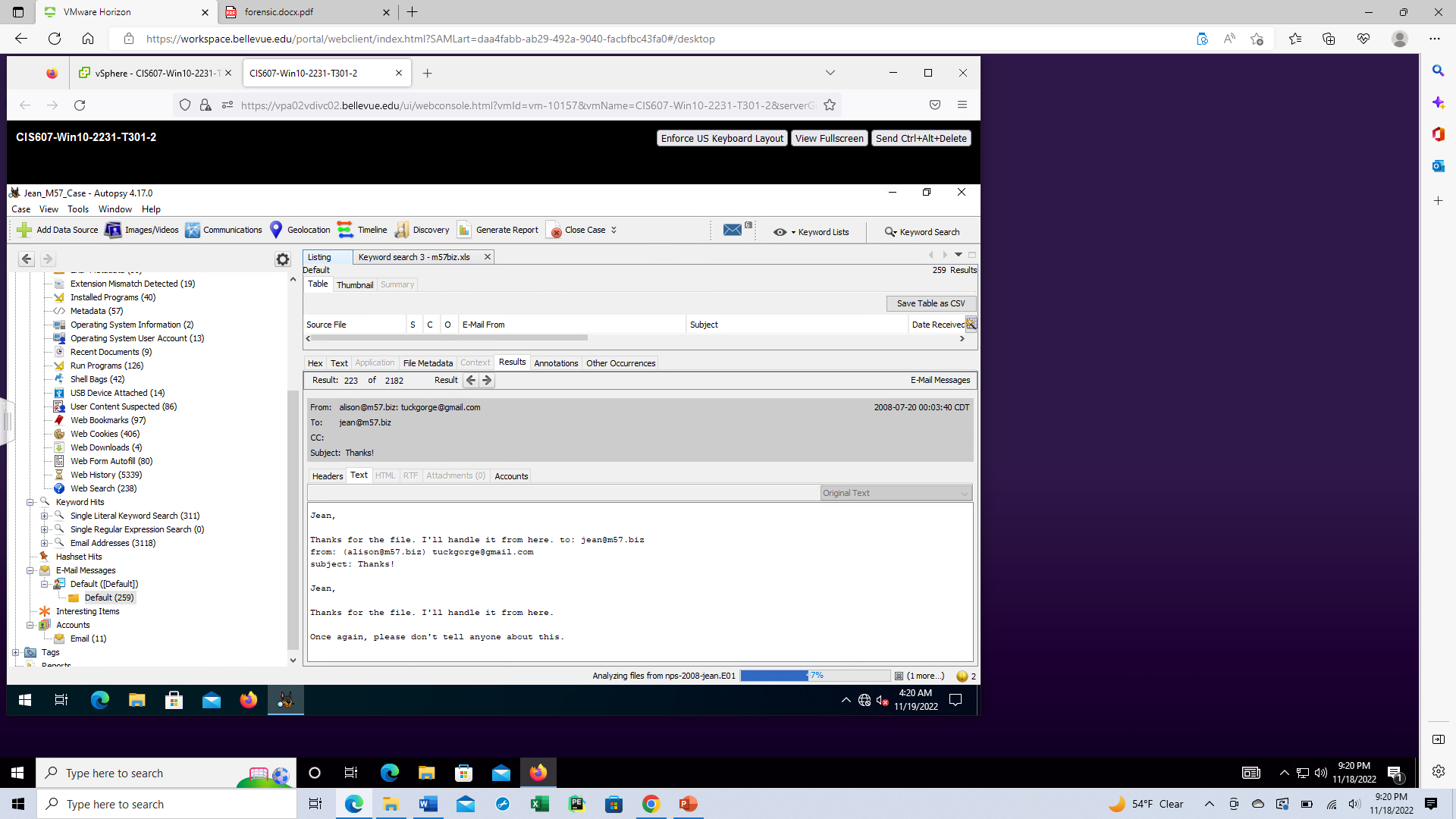


**Figure 18.** Finding of two possible spoofed emails

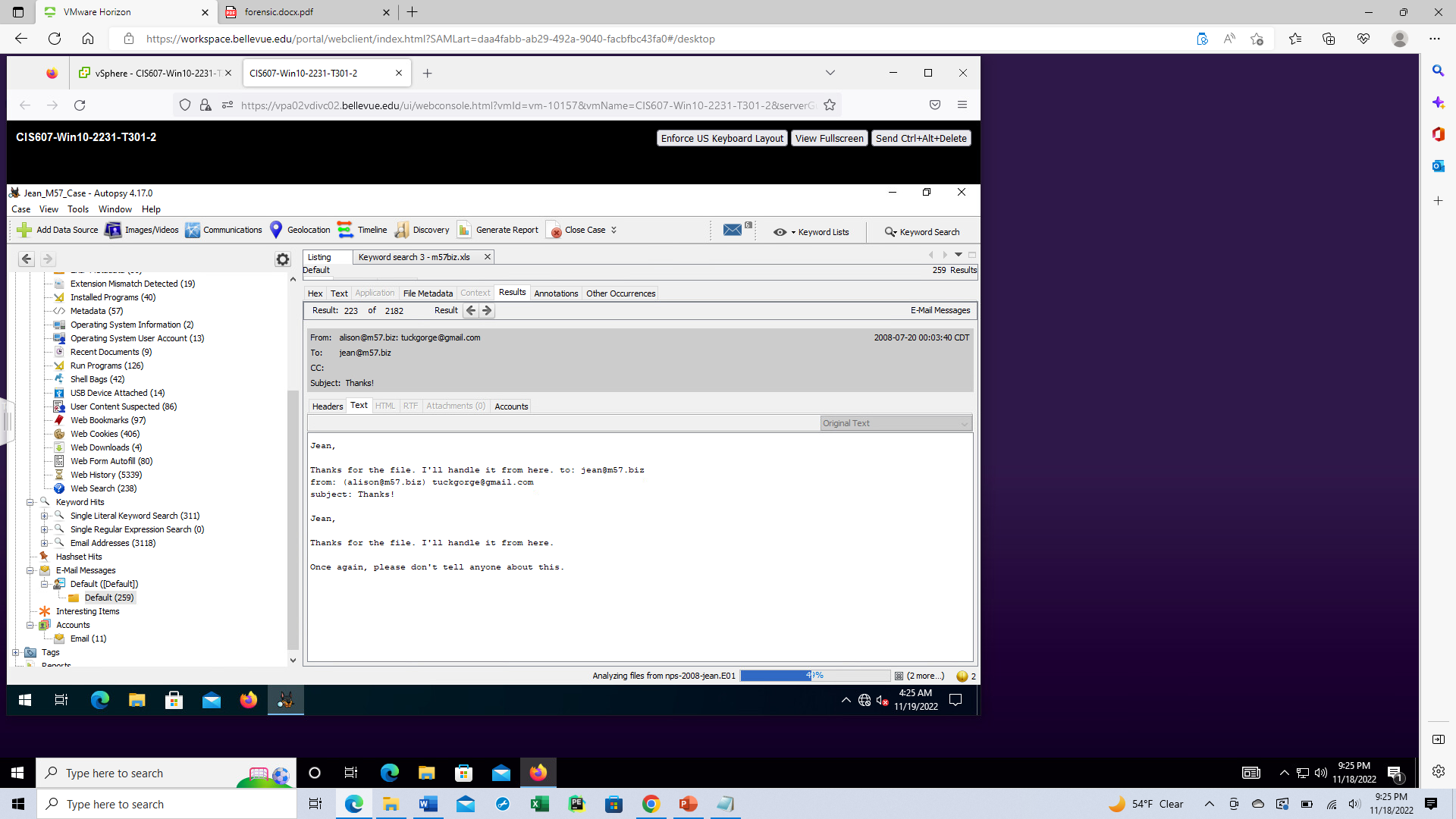
A screenshot of a computer

Description automatically generated

**Figure 19**. Spoofed email showing Alison impersonator asking for sensitive information from Jean



**Figure 20**. Showing where CFO Jean sends sensitive information to spoofed email



**Figure 21**. Showing where impersonator has received information and asks Jean not to mention it to anyone