Bellevue University

Eric Wellmaker

Week 12 Writing Assignment

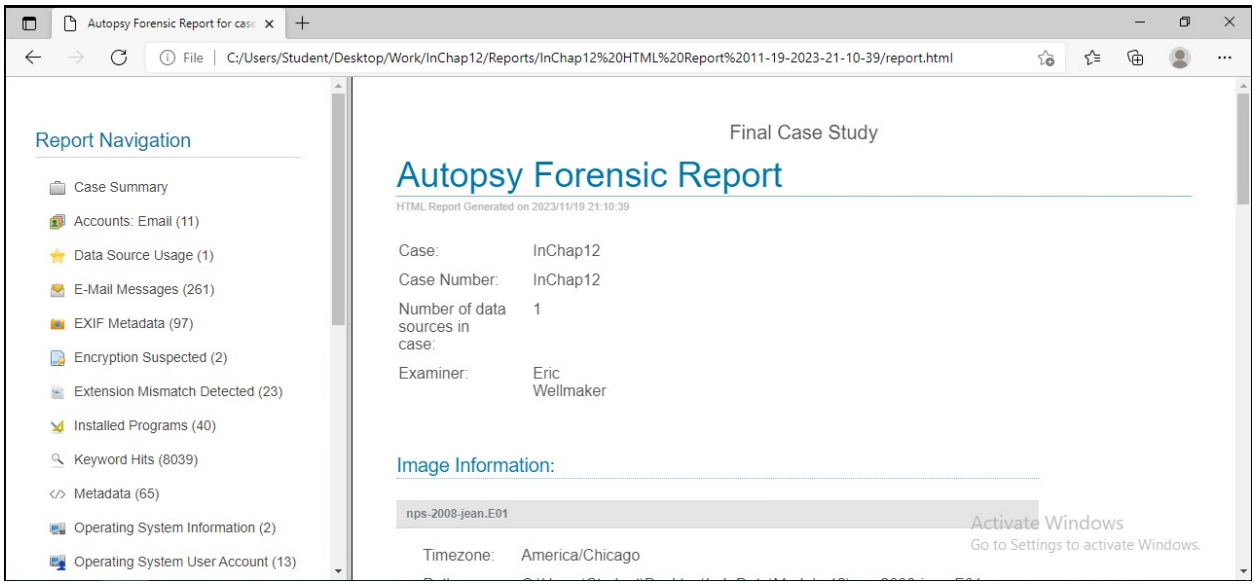
Computer Forensics

November 15th, 2023

For this presentation, a fictitious scenario was given to determine how company information was leaked to a competitor's website. Jean, a company secretary, was instructed to email out confidential company information from her boss. Alison, the president of the company, mentioned that it was Jean who leaked the information. Accessing the virtual lab, I utilize Autopsy and research all findings. Also in this case study, I will disclose when Jean created the spreadsheet file listing company data, how the company information appeared on the competitor's website and close with who else within the company was involved.

Company Spreadsheet

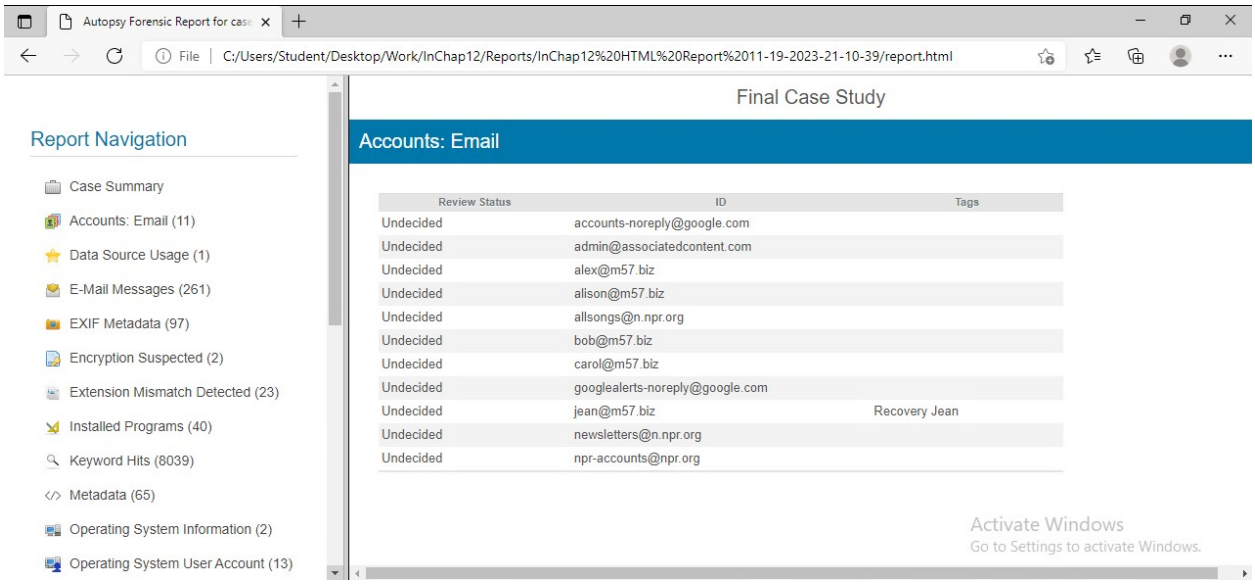
Based on the Autopsy data source, the created time for the excel spreadsheet file is 2008-07-19 20:28:03 CDT for the creation of m57biz.xls which listed company confidential secrets. The Modified time & Access Time are: 2008-07-19 20:28:03 CDT. The Change Time was 1 second later on the time date. All this means is this data was pulled from Jeans hard drive, and the evidence shows that it was her that created the spreadsheet file. In the next section, I will discuss how the spreadsheet information got leaked to another competitor's website.



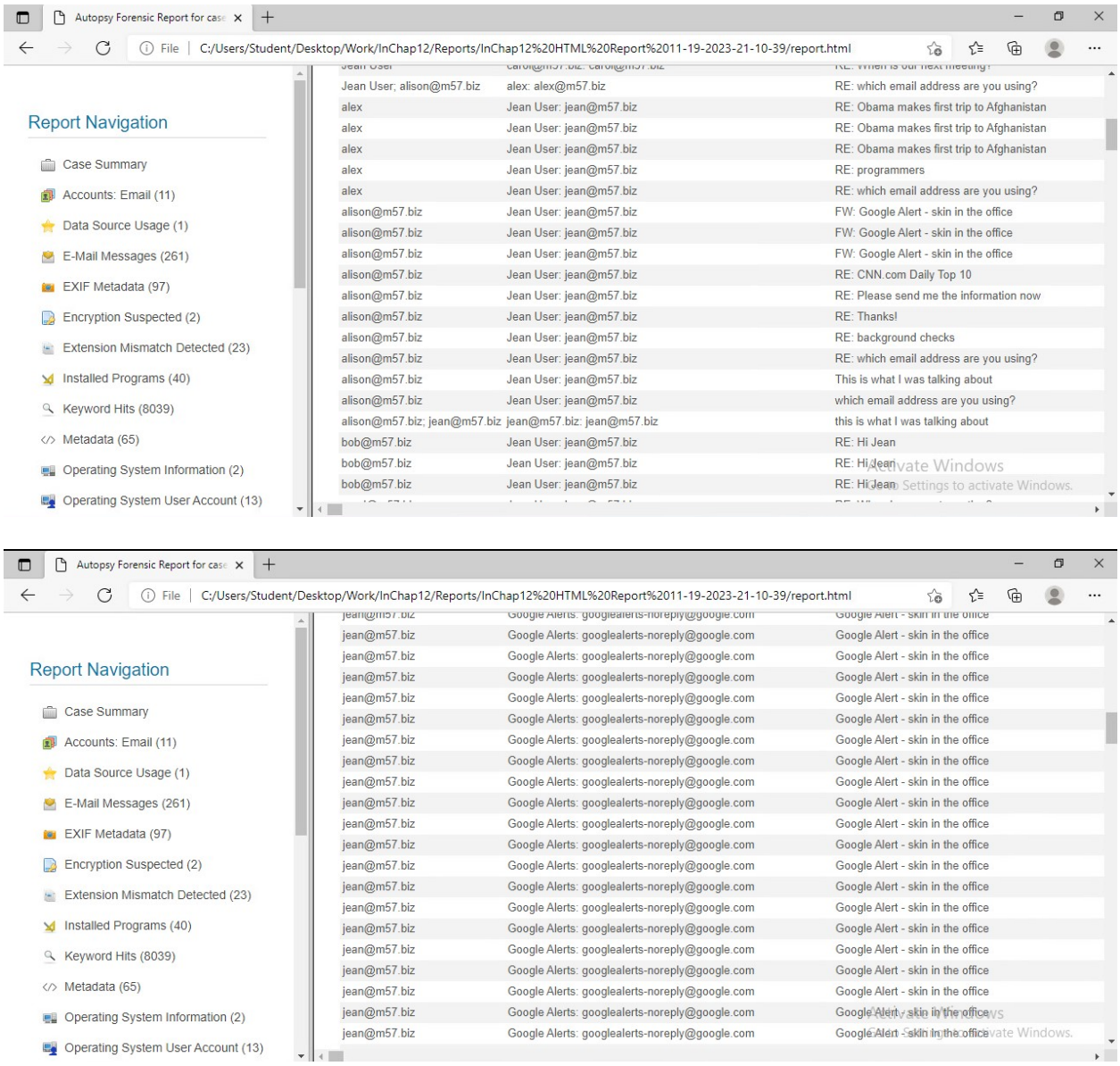
Information on Competitor's Website

On the Extracted content, USB Device Attached, there is a Flash Disc 256 MB that was used 2008-07-19 20:26:18 CDT which overlaps the creation time of the m57biz.xls file. For this segment, I had to review the email traffic between Alison, Jean and the other employees to fully understand how data Jean created was leaked to another company's site. The data shows Jean thought she was talking to Alison and vice-versa. The attack called a "whaling attempt", or highly targeted phishing attack aimed at senior executives of the company like President Alison. The attacker infiltrated their way through the company by convincing Alison and Jean they were each other. This man-in-the-middle attack is what lead Jean to submitting a highly sensitive file to a cyber attacker. Another thing to note was that the email traffic showed the security protocols notifying that there was a skin alert, but that message was ignored. There were reports of the server slowing down which also coincides with a DDOS (Distributed Denial of Service) which slowed down the company server. The employees thought they were talking to each other like admin support but instead talking to bots which simultaneously

sent the valuable information to tuckgeorge@gmail.com the cyber attacker. Once the hacker received the file they were looking for, that person uploaded it to the competitor's website. The final section, I will discuss all those involved with the company secrets being leaked.



All involved in leaking company secrets. I believe (alison@m57.biz) tuckgorge@gmail.com was the one who hacked their email server and conducted a man-in-the-middle attack to obtain the Excel file sheet. Page three of the email traffic for Alison@m57.biz can prove this case further. As stated in the previous section, the google automated system was saying skin alert several times throughout the conversation between Alison and Jean. On page 4 of Alison@m57.biz email traffic lists information of value to this case. <2008071923957.64C683B1DAE@xy.dreamhostps.com is the attacker or bot that requested the spreadsheet listing the employees, current salary and SSNs. This request was sent to Jean. The workers were talking to bots simultaneously and sent the valuable information to tuckgeorge@gmail.com.



The small startup company M57.biz received a cyber-attack resulting in the leaking of confidential company information. After searching the data from Jean's laptop drive, I was able to come to the conclusion that the chain of events started with the president and ended with Jean submitting information to a cyber attacker.

References

Nelson, B., Phillips, A., & Steuart, C. (2019). *Guide to Computer Forensics and Investigations* (6th ed.).