Bellevue University

Eric Wellmaker

Week 12 Writing Assignment

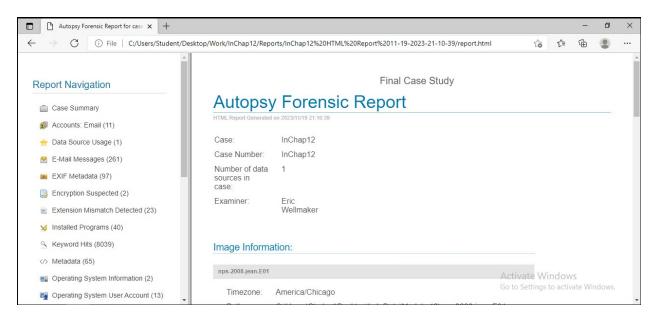
**Computer Forensics** 

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 <u>tuckgeorge@gmail.com</u> 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.

Autopsy Forensic Report for case × +					-	٥	×
$\leftarrow$ $\rightarrow$ $C$ (1) File   C:/Users/Student/D	)esktop/Work/InChap12/Reports/I	nChap12%20HTML%20Report%2011-19-2023	-21-10-39/report.html	°9 €≣	Ē		
A	Final Case Study						
Report Navigation	Accounts: Email						
Case Summary	Review Status	ID	Tags				
Accounts: Email (11)	Undecided	accounts-noreply@google.com	ingo				
- Data Source Usage (1)	Undecided	admin@associatedcontent.com					
Bata Source Usage (1)	Undecided	alex@m57.biz					
🖄 E-Mail Messages (261)	Undecided	alison@m57.biz					
👜 EXIF Metadata (97)	Undecided	allsongs@n.npr.org					
	Undecided	bob@m57.biz					
Encryption Suspected (2)	Undecided	carol@m57.biz					
Extension Mismatch Detected (23)	Undecided	googlealerts-noreply@google.com					
restrict a second se	Undecided	jean@m57.biz	Recovery Jean				
M Installed Programs (40)	Undecided	newsletters@n.npr.org					
Keyword Hits (8039)	Undecided	npr-accounts@npr.org					
Metadata (65)							
Operating System Information (2)			Activate Go to Setti				
Operating System User Account (13)	4		60 to setti	igs to acti	Value VVI	100 WS.	► F

#### 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 <u>Alison@m57.biz</u> 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 <u>Alison@m57.biz</u> 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.

→ C ① File   C:/Users/Student/	/Daskton/Mark/InChan12/Pans == //-	Chap12%20HTML%20Report%2011-19-2023-21-10-39/r	aport html	~	չ^≡	œ		
	Jesktop/work/inchap12/kepons/in	Chap 12%20HTML%20Kepol1%20T1-19-2025-21-10-59/1	RE. THOMAS	ε <u>ο</u>		Ψ		
	Jean User; alison@m57.biz	alex: alex@m57.biz	RE: which en			u usina'	2	
	alex	Jean User: jean@m57.biz	RE: Obama n					
Report Navigation	alex	Jean User: jean@m57.biz	RE: Obama n					
	alex	Jean User: jean@m57.biz	RE: Obama n			-		
Case Summary	alex	Jean User: jean@m57.biz	RE: programm			9		
Accounts: Email (11)	alex	Jean User: jean@m57.biz	RE: which em		s are vo	u usina'	2	
P Accounts. Email (11)	alison@m57.biz	Jean User: jean@m57.biz	FW: Google A			-		
🔶 Data Source Usage (1)	alison@m57.biz	Jean User: jean@m57.biz	FW: Google A					
E-Mail Messages (261)	alison@m57.biz	Jean User: jean@m57.biz	FW: Google A					
E-mail messages (201)	alison@m57.biz	Jean User: jean@m57.biz	RE: CNN.con					
i EXIF Metadata (97)	alison@m57.biz	Jean User: jean@m57.biz	RE: Please s			ation nov	N	
Encryption Suspected (2)	alison@m57.biz	Jean User: jean@m57.biz	RE: Thanks!					
	alison@m57.biz	Jean User: jean@m57.biz	RE: backgrou	ind checks				
Extension Mismatch Detected (23)	alison@m57.biz	Jean User: jean@m57.biz	RE: which en			u usina'	2	
M Installed Programs (40)	alison@m57.biz	Jean User: jean@m57.biz	This is what I					
	alison@m57.biz	Jean User: jean@m57.biz	which email a			ina?		
Keyword Hits (8039)		biz jean@m57.biz: jean@m57.biz	this is what I					
Metadata (65)	bob@m57.biz	Jean User: jean@m57.biz	RE: Hi Jean	indo tanting	about			
	bob@m57.biz	Jean User: jean@m57.biz	RE: Hi/Jean	into Mi	n d au			
Operating System Information (2)	bob@m57.biz	Jean User: jean@m57.biz	RE: Higlean					
Operating System User Account (13)     Autopsy Forensic Report for case × +	•					-	٥	
Autopsy Forensic Report for case x +	/Desktop/Work/InChap12/Reports/In	Chap12%20HTML%20Report%2011-19-2023-21-10-39/r	report.html	تو	£≡	- -	0	
Autopsy Forensic Report for case x +	/Desktop/Work/InChap12/Reports/In	Chap12%20HTML%20Report%2011-19-2023-21-10-39/r Google Alens: googlearens-riorepry@google.com	report.html Google Alert	τ <b>ο</b> - 5κm m un	ζ≡ eromice	-	5	
Autopsy Forensic Report for case x +				- skin in un	e onice	- -	5	
☐ Autopsy Forensic Report for case     x       →     C     ① File       C     ① File     C;/Users/Student,	jean@mor.biz	Google Alerts: googlealerts-horeply@google.com	Google Alen	- skin in the	e onice e office	Ð	0 •	
☐ Autopsy Forensic Report for case     x       →     C     ① File       C     ① File     C;/Users/Student,	jean@m57.biz	Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com	Google Alert	- sкin in un - skin in the - skin in the	e onice e office e office	Ð –	6	
Autopsy Forensic Report for case x +	jean@m57.biz jean@m57.biz	Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com	Google Alert Google Alert Google Alert	- skin in the - skin in the - skin in the - skin in the	e onice e office e office e office	- Ē	•	
☐ Autopsy Forensic Report for case     x       →     C     ① File       C     ① File     C;/Users/Student,	jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz	Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com	Google Alert Google Alert Google Alert Google Alert	- skin in the - skin in the - skin in the - skin in the - skin in the	e onice e office e office e office e office	Ð –	6	
Autopsy Forensic Report for case x +	▲ Jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz	Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com	Google Alert Google Alert Google Alert Google Alert Google Alert	- skin in the - skin in the	e onice e office e office e office e office e office	Ð	0	
Autopsy Forensic Report for case × + → C ① File C:/Users/Student, Report Navigation Case Summary Accounts: Email (11)	▲ Jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz	Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com	Google Alert Google Alert Google Alert Google Alert Google Alert Google Alert	- skin in the - skin in the	e office e office e office e office e office e office e office e office	Ð –	•	
Autopsy Forensic Report for case X + C T File C;/Users/Student, Report Navigation Case Summary	▲ Jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz	Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com	Google Alert Google Alert Google Alert Google Alert Google Alert Google Alert Google Alert	- skin in the - skin in the	e office e office e office e office e office e office e office e office	Ē	5	
Autopsy Forensic Report for case × + C  File C;/Users/Student, Case Summary Accounts: Email (11)	▲ Jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz	Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com	Google Alert Google Alert Google Alert Google Alert Google Alert Google Alert Google Alert Google Alert	- skin in the - skin in the	e office e office e office e office e office e office e office e office e office e office	Ð	6	
<ul> <li>Autopsy Forensic Report for case x +</li> <li>→ C ① File C:/Users/Student</li> <li>Case Summary</li> <li>Accounts: Email (11)</li> <li>Data Source Usage (1)</li> <li>E-Mail Messages (261)</li> </ul>	jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz	Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com	Google Alert Google Alert Google Alert Google Alert Google Alert Google Alert Google Alert Google Alert	skin in the skin in the	e office e office	Ē	6	
<ul> <li>Autopsy Forensic Report for case x +</li> <li>→ C ① File C:/Users/Student,</li> <li>Report Navigation</li> <li>Case Summary</li> <li>Accounts: Email (11)</li> <li>★ Data Source Usage (1)</li> </ul>	▲ Jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz	Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com	Google Alert Google Alert Google Alert Google Alert Google Alert Google Alert Google Alert Google Alert Google Alert	skin in the skin in the	e office e office	-	•	
<ul> <li>Autopsy Forensic Report for case x +</li> <li>→ C ① File C:/Users/Student</li> <li>Case Summary</li> <li>Accounts: Email (11)</li> <li>Data Source Usage (1)</li> <li>E-Mail Messages (261)</li> </ul>	Jean@nt57.biz jean@nt57.biz jean@nt57.biz jean@nt57.biz jean@nt57.biz jean@nt57.biz jean@nt57.biz jean@nt57.biz jean@nt57.biz jean@nt57.biz jean@nt57.biz	Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com	Google Alert Google Alert Google Alert Google Alert Google Alert Google Alert Google Alert Google Alert Google Alert Google Alert	skin in the skin in the	e office e office	-	0	
<ul> <li>Autoppy Forensic Report for case x +</li> <li>→ C ① File C:/Users/Student,</li> <li>Report Navigation</li> <li>Case Summary</li> <li>Accounts: Email (11)</li> <li>Data Source Usage (1)</li> <li>E-Mail Messages (261)</li> <li>EXIF Metadata (97)</li> <li>Encryption Suspected (2)</li> </ul>	Jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz	Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com	Google Alert Google Alert	skin in the skin in the	e office e office	- @	0	
<ul> <li>Autoppy Forensic Report for case x +</li> <li>→ C</li></ul>	<ul> <li>jean@m57.biz</li> </ul>	Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com	Google Alert Google Alert	skin in the skin in the	e office e office	- G	8	
<ul> <li>Autoppy Forensic Report for case x +</li> <li>→ C ① File C:/Users/Student,</li> <li>Report Navigation</li> <li>Case Summary</li> <li>Accounts: Email (11)</li> <li>Data Source Usage (1)</li> <li>E-Mail Messages (261)</li> <li>EXIF Metadata (97)</li> <li>Encryption Suspected (2)</li> </ul>	jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz	Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com	Google Alert Google Alert	skin in the skin in the	e office e office	- G	8	
<ul> <li>Autopsy Forensic Report for case x +</li> <li>→ C</li></ul>	jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz	Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com	Google Alert Google Alert	skin in the skin in the	e office e office	- @	6	
<ul> <li>Autopsy Forensic Report for case x +</li> <li>→ C</li></ul>	jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz	Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com	Google Alert Google Alert	skin in the skin in the	e office e office	- @	0	
<ul> <li>Autopsy Forensic Report for case x +</li> <li>→ C</li></ul>	Jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz	Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com	Google Alert Google Alert	skin in the skin in the	e office e office	- @	6	
<ul> <li>Autopsy Forensic Report for case x +</li> <li>→ C</li></ul>	Jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz jean@m57.biz	Google Alerts: googlealerts-noreply@google.com Google Alerts: googlealerts-noreply@google.com	Google Alert Google Alert	skin in the skin in the	e office e o		•	

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.).