Alexandre Fernandes Costa

Master of Science in Cyber Security Operations and Leadership

CSOL-590-02-SU20 - Cyber Incident Resp/Forensics

Module 5: Computer Forensic Tools

University of San Diego

Author Note

In Dedication to Services Pentest (SERPENT) Team

Abstract

The computer forensic examination report is a thorough analysis going through all phases of the digital forensic readiness process model and with an additional ad-hoc section that analyzes the digital forensic presented for this case.

Introduction

The computer forensic examination report presents a compelling forensic analysis of the case of the start-up company.

Digital Forensic Report

During this engagement, the complete details of the forensic expert are presented below. The engagement length is about two weeks of engagement from receiving the digital forensic data and going through all phases presented in this report.

It is essential to highlight that it includes an evidence package presentation that will be used in court.

Forensics Engineer	Alexandre Fernandes Costa
	Digital Forensics Examiner or Expert
	Redmond, Washington
	(425) 301-0700
Subject	Computer Forensic Examination Report
Offense	Confidential data breach and personally identifiable information (PII)
Accused	Jane Jones
Engagement request	6/15/2020
Engagement conclusion	6/29/2020

Executive Summary

The involvement of a highly capable forensic expert, in this case of the start-up company named M57.biz, where highly confidential and personally identifiable information was leaked.

An external forensic investigator was hired to investigate the case, gather evidence, and determine the attack-path that resulted in the document being exfiltrated to a foreign threat actor or even a presence of advanced persistent threat (APT).

Background of the Case

M57.biz is a start-up company developing a body art catalog. The start-up company had $3 million in seed money and is closing in on a $10 million funding round with two founders or owners, and ten employees hired in the first year.

In theory, the spreadsheet originated from the CFO named Jean and the associated computer.

Objectives

The objectives assigned to this engagement and resulting in this report are to:

- Analyze the forensics data presented.
- Determine and investigate multiple hypotheses based on the forensic data presented.
- Extract useful evidence data.
- Leverage the best tools in the market to analyze the forensic data.
- Investigate and prove the industrial espionage case and if there is an insider threat of external threat collaboration.
- Investigate the involvement or presence of an Advanced Persistent Threat (APT).
- Bring to resolution the hypothesis defined.

In order to fulfill the objectives mentioned, two tools were used to conduct a practical and productive investigation. The tools employed were Forensic Toolkit Imager (FTK Imager) and Autopsy. The Forensic Toolkit Imager is a software toolkit made by AccessData. The Autopsy is an open-source leveraged by the military, law enforcement, and corporate examiners to investigate evidence images.

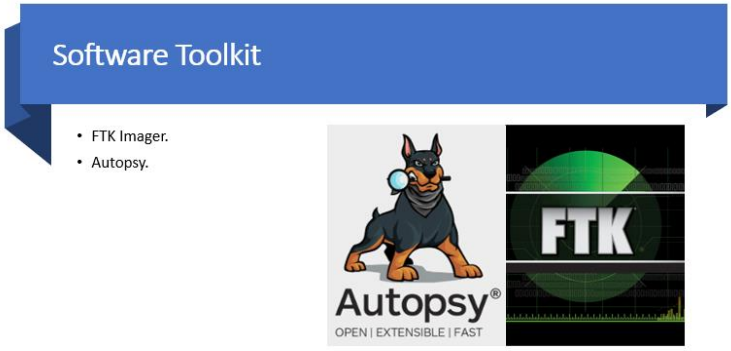

Figure 1: Software Toolkit employed in the analysis of the case.

Forensic Practice Principles

In any digital forensics investigation, investigators, legal advisors should consider the core principles of a digital forensics investigation. The goals of the forensics practices principles are to:

- Find as much as evidence as possible – reconnaissance.
- Preserve the evidence as good as possible – reliability.
- Identity-related evidence as close as possible – relevancy

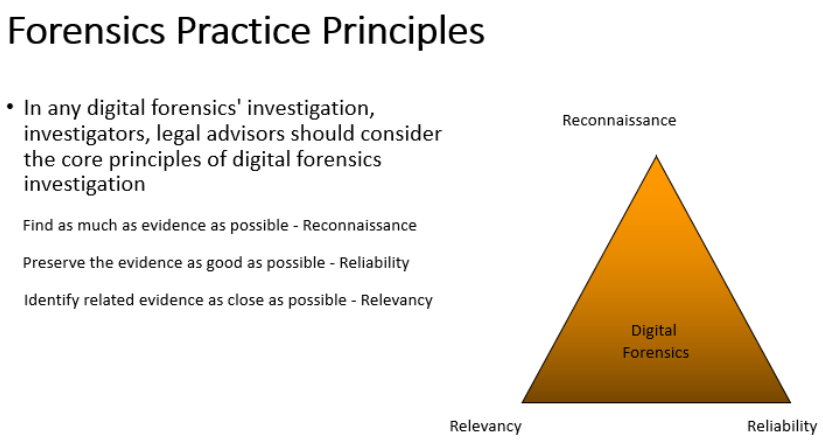

Figure 2: Forensics Practice Principles.

Legal Considerations

For the start-up in this case being investigated, there is a liability concerning a data breach. It is essential to highlight that it is not the core question in the investigation, nor is the criminality of actions.

The culpability is the court's duty and role to determine after the presentation of the evidence package.

The concerns for the investigator are the collection and, above all, the secure handling of evidence to ensure that it is admissible in court and the determination of facts. Throughout the investigation, there was care taken to ensure that evidence was collected and analyzed in a manner recommended by the Scientific Working Group on Digital Evidence (SWGDE). Standard forensics tools were used to examine the data.

Chain of Custody

The Chain of Custody was monitored carefully to ensure that it was properly documented for verification.

The image file has the .E01 extension, and both FTK Imager and the Autopsy were used to analyze and verify the integrity of the digital forensic evidence received.

The first evidence was kept in a secure vault, and any access to the file was registered manually and automatically via internal systems.

The device forensic image integrity can be seen in the screenshot below.

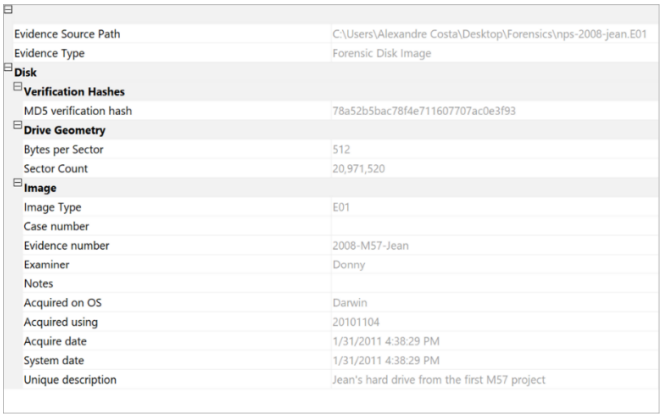

Figure 3: Checking the integrity of the image and the result of the verification hash.

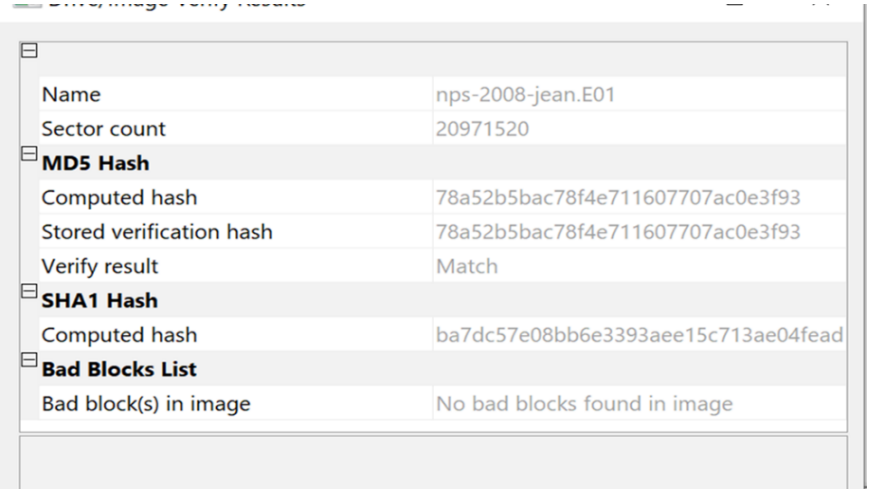

Figure 4: The results of the computed hash and the stored verification hash.

Readiness

A well-defined process model built to support digital forensic readiness is different from a process model developed for the digital forensic investigative process.

The digital forensic readiness process is not a linear process where activities and steps are executed sequentially.

A process model for digital forensic readiness consists of activities and steps within a circular and redundant hierarchy.

The initiation of the digital forensic readiness process model can originate from any activity or steps and subsequently lead to any other phase.

The digital forensics readiness process model must establish administrative, technical, and physical foundations to effectively support the activities and tasks performed in phases of the digital forensic process model by:

- Maximizing the potential use of digital evidence.
- Minimizing the costs of digital forensic investigations.
- Minimizing the interference disruption of business processes.
- Preserving and improving information security posture.

An example of the digital forensics readiness process model is exhibited in figure 5.

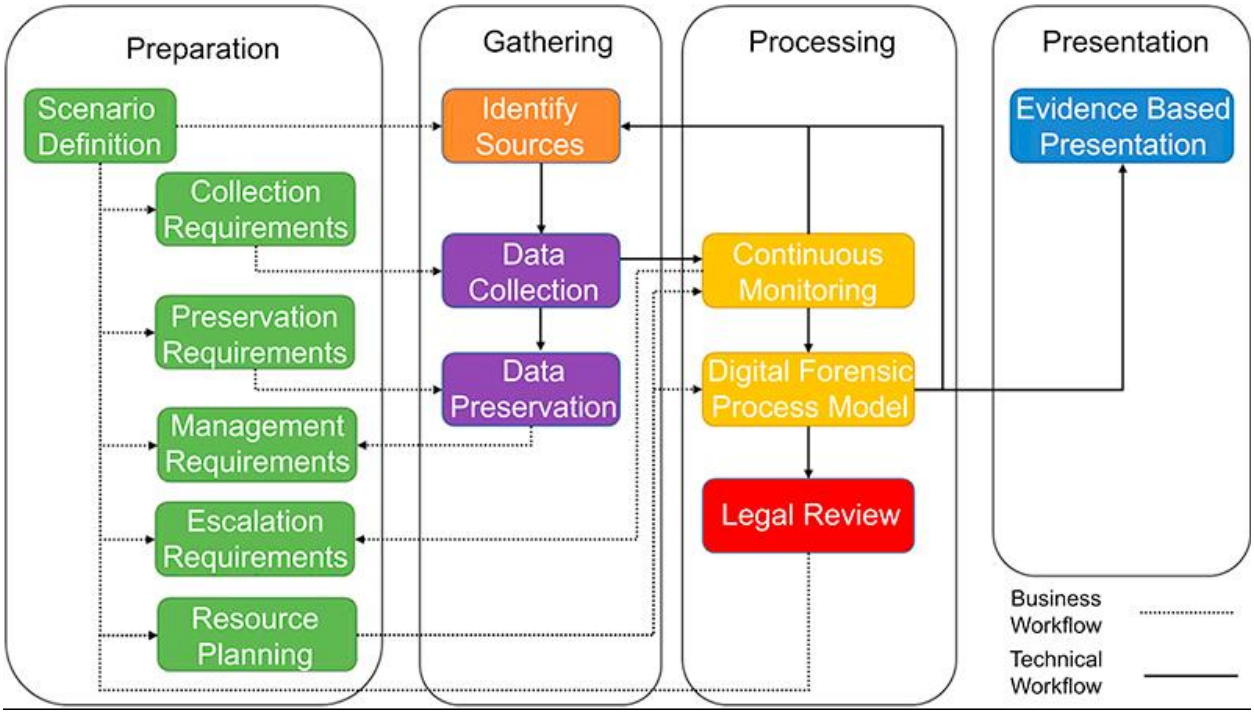

Figure 5: Digital Forensics Process Model

Evaluation

As part of the analysis of the evidence, Alexandre Fernandes Costa has been assigned to this case. The instructions are clear and aligned with the objectives described in the objectives section of this report. Throughout the evaluation, the phase is vital to evaluate the results of the interviews conducted, elaborate hypothesis, and formulate to potential answers.

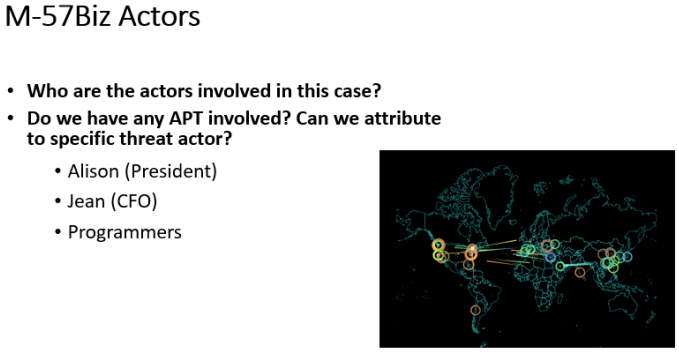

Figure 6: M-57Biz Actos and potential hypothesis

Collection

From legacy to modern systems, it is essential to understand the requirements for practicing digital forensics.

Today, there is a range of modern systems such as mobile devices, cloud environments, or game consoles that are potential sources of evidence.

Independent of legacy or modern systems, there are two types of digital evidence where information can be gathered, including non-volatile or volatile data.

The only digital forensic evidence presented was ***nps-2008-jean.E01.***

Life Span	Storage Type	Data Type
As short as a single clock cycle	CPU Storage	Registers
	Video	Caches
Until Host is shut down	System Storage	RAM
	Kernel Tables	Network Connections
		Login sessions
		Running processes
		Open files
		Network configurations
		System date/time
Until overwritten or erased	Non-volatile data	Paging/swap files
		Temporary/cache files
		Configuration/log file
		Hibernation files
		Dump files
		Registry
		Account profile or information
		Data files
		Slack space
		Storage devices
	Removable Media	Floppy Disks
		Tapes
		Optical Disc (read/write only)
Until physically destroyed		Optical Disc (write-only)
	Outputs	Paper printouts

Analysis

In this phase of the investigation, and it involves processing the activities and steps performed by the investigator to examine the image provided in this case as a piece of digital evidence.

The activities and steps are used by examiners or investigators to examine duplicated evidence forensically to identify meaningful data and subsequently reduce the volume of data based on the contextual and content relevance. The idea behind this activity is to reduce the number of hours used by the investigator.

In theory, all activities and steps delivered during the analysis should occur inside a secure facility due to the COVID-19 situation. The investigation took place in safe operational security at the home of the forensic examiner.

The main reasons for this requirement are to ensure the digital evidence is appropriately controlled and the access authorization to the digital evidence and, most importantly, avoid the contamination of the digital proof.

In this case, the level of forensic investigators engaged in ensuring the due diligence proving the integrity of the data and using secure equipment, including inspecting malicious software, verifying wiped media, and certifying the host operating system. Up to this phase, many procedure have been followed, and it is vital to highlight them in figure 7.

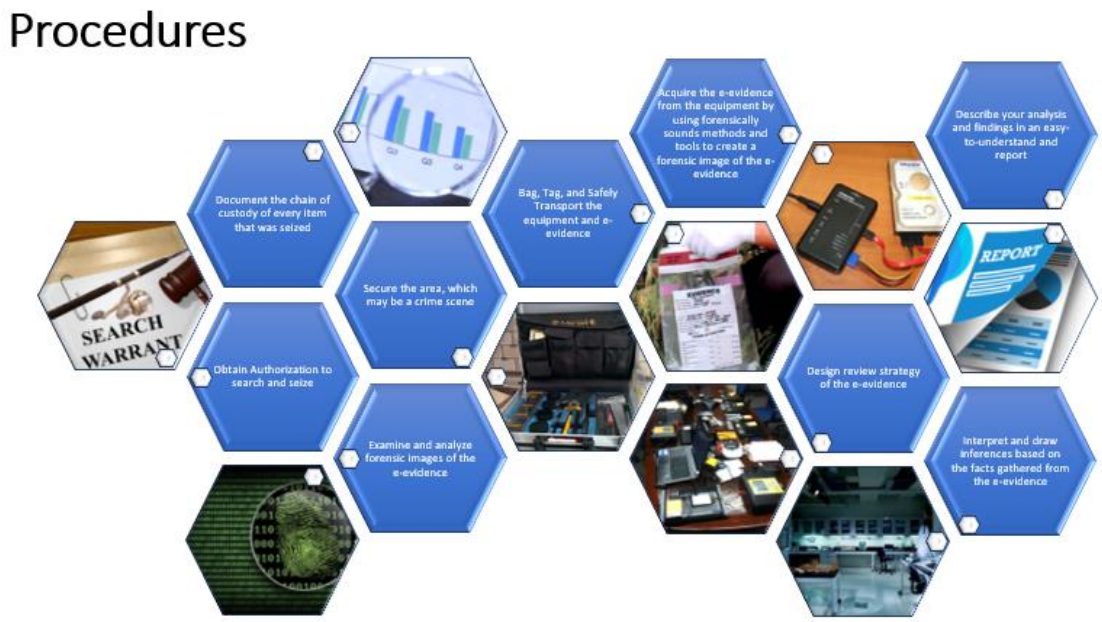

Figure 7: Summary of all procedures followed by the investigation.

Presentation

In the presentation, the phase involves all the activities and steps performed to produce all the deliverables that are all evidence-based of the investigation.

The activities and all associated steps provide forensic investigators with a venue of presenting a compelling set of processes, techniques, tools, equipment, and interactions that maintained the authenticity, reliability, and trustworthiness of digital evidence throughout the investigative process.

The examination and analysis of all case files and evidence must be stored in secure lockers, and the chain of custody must be kept up to date. If not instructed directly by the legal authorities, the criteria for retaining digital evidence must comply with, and not exceed, the timelines established through policies, standards, and procedures.

Proper disposal of digital evidence must be done so using the existing chain of custody form. Documentation is a critical element of an investigation. In alignment with established operating procedures, each phase of the investigative workflow requires different documentation to be maintained that is as complete, accurate, and comprehensive as possible. From the details captured in these documents, investigators can demonstrate the continuity in custody and interactions with authorized personnel for all digital evidence.

This section will be used to show the activities and the results of the analysis as part of the evidence package.

The file being part of the data breach is ***M57biz.xls***.In figure 8, it is showing all the results for the ***M57biz.xls***.

Name	Location	Modified Time	Char
Recent Documents Artifact	/img_nps-2008-jean.E01/vol_vol2/Documents and Settings...	2008-07-20 18:18:00 PDT	2008
EXCEL.EXE-1C75F8D6.pf	/img_nps-2008-jean.E01/vol_vol2/WINDOWS/Prefetch/EX...	2008-07-19 18:27:50 PDT	2008
NTUSER.DAT	/img_nps-2008-jean.E01/vol_vol2/Documents and Settings...	2008-07-20 18:18:00 PDT	2008
m57biz.xls	/img_nps-2008-jean.E01/vol_vol2/Documents and Settings...	2008-07-19 18:28:03 PDT	2008
m57biz.xls-slack	/img_nps-2008-jean.E01/vol_vol2/Documents and Settings...	2008-07-19 18:28:03 PDT	2008
Recent Documents Artifact	/img_nps-2008-jean.E01/vol_vol2/Documents and Settings...	2008-07-19 18:28:04 PDT	2008
Recent Documents Artifact	/img_nps-2008-jean.E01/vol_vol2/Documents and Settings...	2008-07-19 18:28:04 PDT	2008
f0286464.reg	/img_nps-2008-jean.E01/vol_vol2//$CarvedFiles/f0286464...	0000-00-00 00:00:00	0000
RegRipper /img_nps-2008-jean.E01/vol_vol2/Documents and Setti	RegRipper /img_nps-2008-jean.E01/vol_vol2/Documents a...		
outlook.pst	/img_nps-2008-jean.E01/vol_vol2/Documents and Settings...	2008-07-20 18:17:54 PDT	2008
Layout.ini	/img_nps-2008-jean.E01/vol_vol2/WINDOWS/Prefetch/Lay...	2008-07-20 17:28:21 PDT	2008
index.dat	/img_nps-2008-jean.E01/vol_vol2/Documents and Settings...	2008-07-20 16:49:55 PDT	2008
index.dat	/img_nps-2008-jean.E01/vol_vol2/Documents and Settings...	2008-07-19 17:00:42 PDT	2008
m57biz.lnk	/img_nps-2008-jean.E01/vol_vol2/Documents and Settings...	2008-07-19 18:28:04 PDT	2008
m57biz.xls	/img_nps-2008-jean.E01/vol_vol2/Documents and Settings...	2008-07-19 18:28:03 PDT	0000
$MFT	/img_nps-2008-jean.E01/vol_vol2/$MFT	2008-05-13 15:18:43 PDT	2008
_REGISTRY_USER_NTUSER_S-1-5-21-484763869-796845957-839	/img_nps-2008-jean.E01/vol_vol2/System Volume Informat...	2008-07-19 19:00:13 PDT	2008
Unalloc_56309_40448_2907565568	/img_nps-2008-jean.E01/vol_vol2//$Unalloc/Unalloc_56309...	0000-00-00 00:00:00	0000
Unalloc_56309_4328603136_6097866240	/img_nps-2008-jean.E01/vol_vol2//$Unalloc/Unalloc_56309...	0000-00-00 00:00:00	0000
Unalloc_56309_6793707008_8345808384	/img_nps-2008-jean.E01/vol_vol2//$Unalloc/Unalloc_56309...	0000-00-00 00:00:00	0000
_REGISTRY_USER_NTUSER_S-1-5-21-484763869-796845957-839	/img_nps-2008-jean.E01/vol_vol2/System Volume Informat...	2008-07-20 18:18:00 PDT	2008
m57biz.LNK	/img_nps-2008-jean.E01/vol_vol2/Documents and Settings...	2008-07-19 18:28:04 PDT	2008

Figure 8: The result of the search to show where the M57biz.xls is present.

In figure 9, it is possible to see the M57biz.xls present at Jean's desktop.

Flags(Meta)	MD5 Hash	MIME Type	Extension	Keyword Preview
Allocated	ec0e1ebf93facfbb732a031c26ad228d	application/x.windows-registry	dat	Settings\Jean\Desktop\«m57biz.xls«Program Name : Exce
Allocated	c7172b8375adcd5c2797237be5657be8	application/octet-stream	pf	\JEAN\LOCALS~1\TEMP\«M57BIZ.XLS«\DEVICE\HARDDIS
Allocated	ec0e1ebf93facfbb732a031c26ad228d	application/x.windows-registry	dat	aim.com/music «m57biz.xls««m57biz.xls«# AIM6~1.LNKA
Allocated	e23a4eb7f2562f53e88c9dca8b26a153	application/vnd.ms-excel	xls	«m57biz.xls«
Allocated		application/octet-stream	xls-slack	«m57biz.xls«-slack
Allocated	e0250a439c4b606dbb982c2902ff672c	application/octet-stream	lnk	Settings\Jean\Desktop\«m57biz.xls«Path ID : 4036Date/T
Allocated	267c4ad8a74c278fa0d5013342b43b64	application/octet-stream	lnk	Settings\Jean\Desktop\«m57biz.xls«Path ID : 4036Date/T
Unallocated	c0e2ef97c046a88321acbef3fb8b519e	application/x.windows-registry	reg	\outlook.pstGoogle«m57biz.xls«m57biz.lnkm57biz.lnk
				Settings\Jean\Desktop\«m57biz.xls«Software\Microsoft\C
Allocated	8c862a8c7ad8b7aff1df4d44fbf1fe95	application/vnd.ms-outlook-pst	pst	information now«m57biz.xls««m57biz.xls«Sheet1
Allocated	192516d18b7c20d97e6a34b00eafdaf1	application/octet-stream	ini	\JEAN\LOCALS~1\TEMP\«M57BIZ.XLS«C:\WINDOWS\SYS
Allocated	2a56c7bbdc9880aedbcbaffc1d231711	application/octet-stream	dat	ttings/Jean/Desktop/«m57biz.xls«URL Visited: Jean@http
Allocated	c81a1f45fc246f613b496d792142df27	application/octet-stream	dat	ttings/Jean/Desktop/«m57biz.xls«URL :200807202008072
Allocated	267c4ad8a74c278fa0d5013342b43b64	application/octet-stream	lnk	m57biz.lnk «m57biz.xls««m57biz.xls«C:\Documents and
Allocated	e23a4eb7f2562f53e88c9dca8b26a153	application/vnd.ms-excel	xls	«m57biz.xls«
Allocated	0f3096cc3681cbfd00497fd084feb483	application/octet-stream		Tunes.urlAIMTUN~1.URL«m57biz.xls«FILE0Cookies$I300
Allocated	337b8f9992350ec245cfc1f1404bf6d2	application/x.windows-registry		\outlook.pstGoogle«m57biz.xls«m57biz.lnkm57biz.lnk
Unallocated		application/octet-stream		\JEAN\LOCALS~1\TEMP\«M57BIZ.XLS«C:\WINDOWS\SYS
Unallocated		application/octet-stream		\JEAN\LOCALS~1\TEMP\«M57BIZ.XLS«C:\WINDOWS\SYS
Unallocated		application/octet-stream		\outlook.pstGoogle«m57biz.xls«m57biz.lnkm57biz.lnk
Allocated	ec0e1ebf93facfbb732a031c26ad228d	application/x.windows-registry		aim.com/music «m57biz.xls««m57biz.xls«# AIM6~1.LNKA
Allocated	e0250a439c4b606dbb982c2902ff672c	application/octet-stream	lnk	m57biz.lnk «m57biz.xls««m57biz.xls«C:\Documents and

Figure 9: M57biz.xls shows the file on Jean's desktop folder.

In figure 10, we can search and analyze e-mail content.

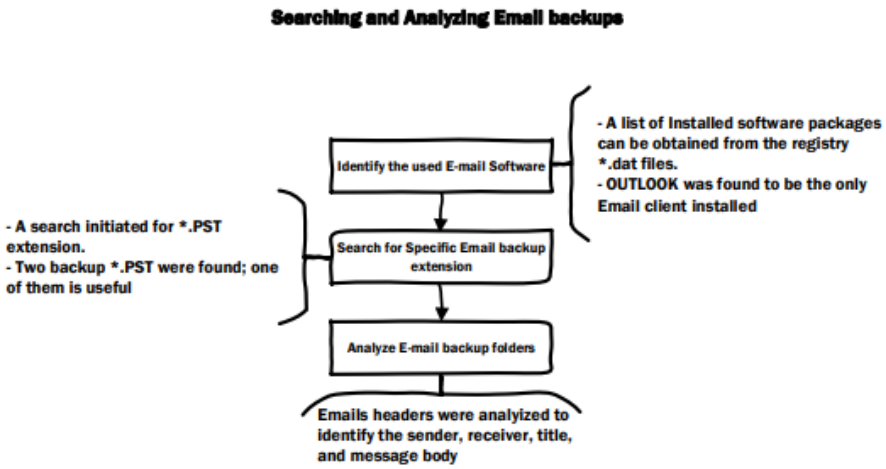

Figure 10: Searching and analyzing e-mails.

In figure 11, it is possible to the real identity of the e-mail received by Jean at 18:22. The sender spoofed the e-mail alias from Alison. The actual sender was tuckgorge@gmail.com.

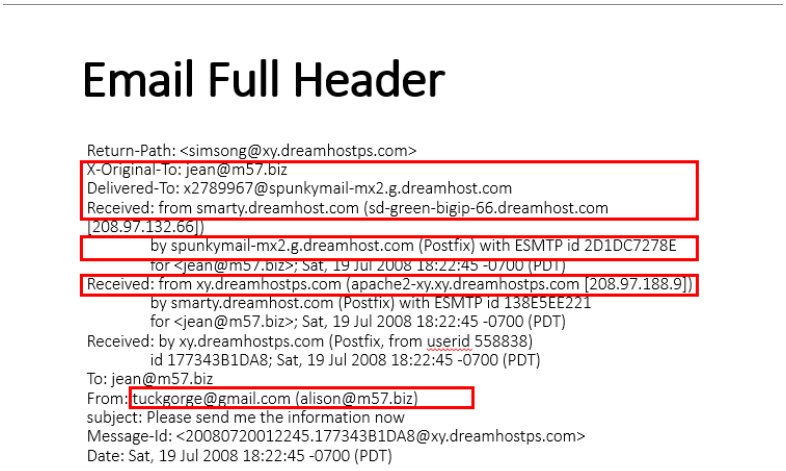

Figure 11: Analysis of the full e-mail header.

In figure 12 shows the presence of the all DNS records for the 208.97.188.9. The IP is still active and still open for the relay. This could be checked via telnet.

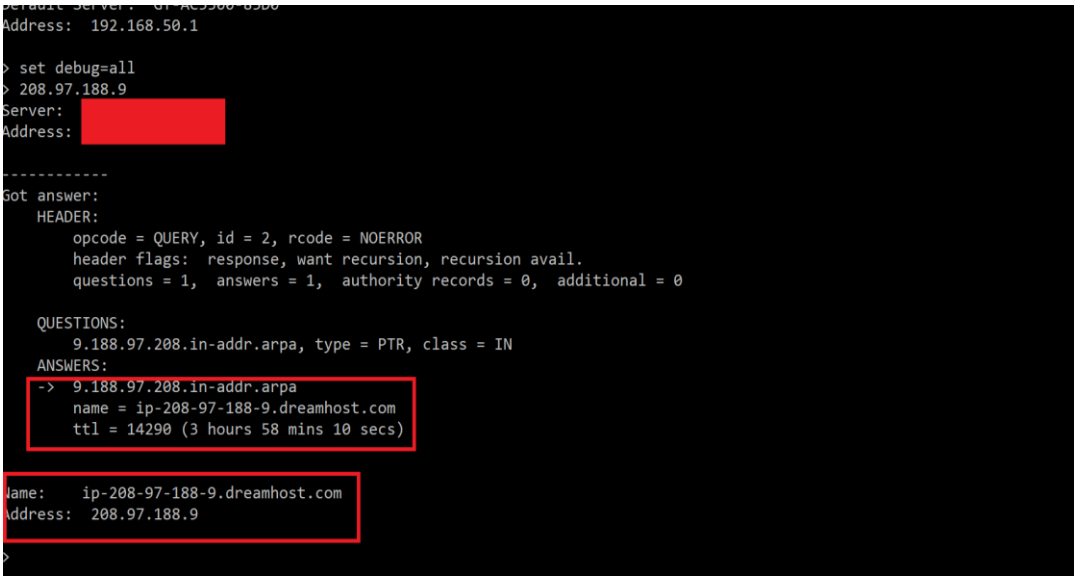

Figure 12: Nslookup and complete DNS address resolution of the 208.97.188.9

In figure 13, with all the evidence collected so far, it helps to illustrate the most probable attack path by the external threat actor.

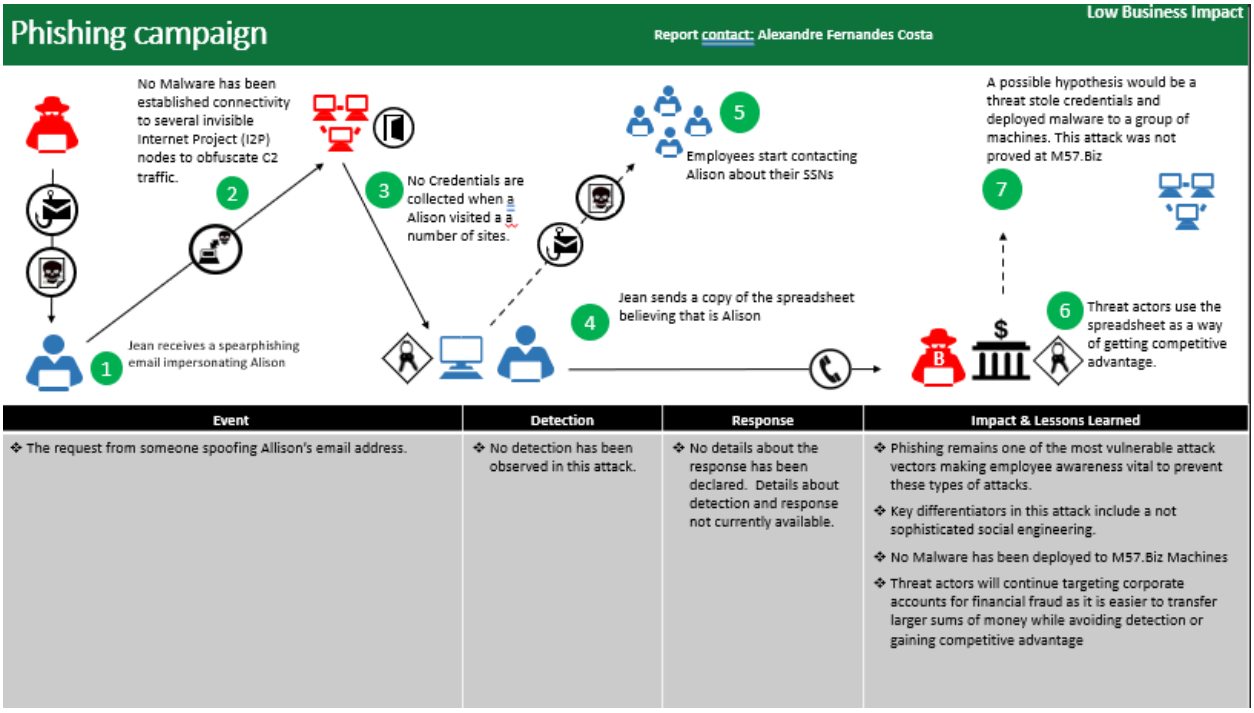

Figure 13: Illustration of the attack-path against Jean.

In figure 13, it is also possible to summarize the steps executed by the external threat actor:

1. Jean receives a spearphishing e-mail impersonating Alison.
2. No Malware has been established connectivity to several invisible nodes to obfuscate C2 Traffic.
3. No credentials harvesting has been observed, meaning no password has been collected or gathered.
4. Jean sends a copy of the spreadsheet, believing that it is Alison.
5. Employees (Developers) start contacting Alison about their SSNs being on the internet.
6. Threat Actors use the spreadsheet as a way of getting a competitive advantage.
7. A possible hypothesis would be a threat stole credentials and deployed malware to a group of machines. This attack was not proved at M57.Biz. That's the reason that we have a dotted line.

In figure 14, it is a complete timeline of all events collected during this forensic analysis.

Date	Time	Event
07-06-2008	12:25 PM	Alison asks for a Business Plan update for Jean
07-06-2008	12:25 PM	Alison replies to Jean stating do not see emails with links
07-19-2008	04:33 PM	Jean receives an e-mail to follow-up on the financial projection
07-19-2008	04:33 PM	Misunderstanding with regards the emails to use or potential previous spoof attempts
07-19-2008	04:40 PM	Alison requests for a spreadsheet with the information of all employees
07-19-2008	06:23 PM	The request from someone spoofing Allison's email address
07-19-2008	06:28 PM	Jean replies to the spoofed Tuckgorge@gmail.com
07-19-2008	10:04 PM	Spoofed address replies to Jean saying thank you!
07-20-2008	04:41 PM	Alison states to Jean: "What are you doing?"
07-20-2008	04:57 PM	Jean replies to the e-mail of 04:41 PM
07-20-2008	04:48 PM	Alison states to Jean: "Something very strange is going. Do you know anything about it?"
07-20-2008	04:53 PM	Bob sends an e-mail to Jean saying that his SSN is online
07-20-2008	05:04 PM	Jean replies saying she does not know what is going and Alison has asked the same question
07-20-2008	05:46 PM	Bob asks Jean to reply an e-mail to be in used in the court of law

Figure 14: Timeline built based on Jean's inbox and analysis of the image.

Review

Digital forensics science has been long established to be a discipline that adheres to consistency, repeatability, and defensible protocols. The phases mentioned throughout this report shows the consistency through all the stages and, most importantly, the capability of implementing a repeatable process and defensible protocols that can be used to analyze any forensic investigation.

Conclusion

In conclusion to this case, it is possible to attest to the steps taken by the foreign actor resulting in the data breach.

The final recommendations and review of all steps analyzed throughout this case resulted in a set of statements:

- The integrity of the evidence was checked with its hash values.
- A complete examination of the full e-mail header was useful from the forensics and the end-user point of view.
- End-user training security awareness is necessary.
- An e-mail system that stores all inbound and outbound e-mails.
- Files metadata are crucial for in-depth forensics analysis.
- Endpoint protection software could have avoided this attack.
- Gateway security solutions could have avoided this attack.
- The importance of maintaining software up-to-date on all PCs.

References

HAYES, DARREN R. Practical Guide to Digital Forensics Investigations. PEARSON, 2019.

Sachowski, Jason. Implementing Digital Forensic Readiness: From Reactive to Proactive Process. Syngress, 2016.