REPORTED BY
Gunnar Yonker

LAB NUMBER
4

START DATE
3/11/2023

COMPLETED DATE
3/14/2023

COURSE
CYBER 742

SEMESTER
SPRING 23

INSTRUCTOR
Schoeneck

TYPE OF INVESTIGATION
Policy Violation

SUSPECT
Warren Hamilton

LAB REPORT SUMMARY:

EXECUTIVE SUMMARY

On Saturday, March 11, 2022, I, Digital Forensic Examiner Gunnar Yonker, received a request to conduct a digital forensic examination and analysis of forensic images of computer media related to a investigation of…. The forensic images were acquired on 4/22/20 by the DFIR team from a previous unrelated litigation hold and provided to me on 2/13/2023. As part of the forensic analysis, I utilized Autopsy forensic software to process and examine the forensic images, tag significant content, and export artifacts for inclusion with the forensic analysis report.

NARRATIVE

On Saturday, March 14th, 2022, I, Digital Forensic Examiner (DFE) Gunnar Yonker, used Autopsy v.4.20.0 to process, parse through, and examine the data contained within the verified forensic images of the [Seagate 1TB HDD] (23-0213_1). During the forensic examination and analysis, I observed files and/or artifacts of interest. I selected the following information included below from the entries and artifacts contained within the forensic images and Autopsy cases and did not include the entire contents of the date from the computer media. I tagged data of interest, exported a report from Autopsy to document them, and later copied the files, artifacts and examination report to the evidence folder. The following is a brief synopsis of the information with the records, separated by evidence item and/or type.

Device Information – 23-0213_1
Operating System: Windows 7 Enterprise Service Pack 1
Installed/Updated Date/Time: 2020-02-13 20:10:21 CST
Owner: Warren Hamilton
Computer Name: WIN-9H6J4FBP8F7
Last Shutdown Time: 2020-02-13 23:00:31 CST
Volume Serial Number: A2F8DF74F8DF44E7
File System: NTFS/exFAT
Total Capacity: Approx. 59.98 GBs = ~ 60 GBs
Unallocated Area: 2,097,152 bytes

Autopsy Parsed Sections
Data Artifacts
Alex Index Caches (5)
Chrome Saved Passwords Identifier - TODO: ACCOUNT (1)
Communication Accounts (2)
Installed Programs (696)
Jump List Auto Dest (14)
NTFS Usr Jrnl entries (91035)

REPORTED BY
Gunnar Yonker
0

LAB NUMBER
4

SUMMARY CONTINUED:

Run Programs (87)
Shell Bags (67)
USB Device Attached (14)
Web Accounts (10)
Web Bookmarks (19)
Web Cache (79)
Web Cookies (825)
Web Downloads (119)
Web Form Addresses (1)
Web Form Autofill (49)
Web History (3073)
Web Search (129)
WebcacheV01 CONTENT (1430)

I noted the following .xlsx file of interest pertaining to the the investigation:

File Name: LoanBook4.xlsx
Full Path to file:
/img_DFA_Windows.E01/vol_vol2/Users/Warren/Documents/Loan Tracking/LoanBook4.xlsx
Size: 10064 bytes
Created Date/Time: 2020-02-18 14:00:35 CST
Last Accessed Date/Time: 2020-02-18 14:39:23 CST
Last Modified Date:Time: 2020-02-18 14:39:23 CST
Hash Value (MD5): f4ebeae447d549811859b717c62e5fd1
Comments/Description: This file was found along with 4 other loanbooks(1-5), however the contents of this file were pertaining to gambling debts that were owed.

I noted the following .pptx file of interest pertaining to the investigation:

File Name: Student Loans and Other Financial Markets.pptx
Full Path to file:
/img_DFA_Windows.E01/vol_vol2/Users/Warren/Documents/Mallie Sae/Student Loans and Other Financial Markets.pptx
Size: 459379 bytes
Created Date/Time: 2020-03-19 18:23:01 CDT
Last Accessed Date/Time: 2020-03-19 18:31:44 CDT
Last Modified Date:Time: 2020-03-19 18:31:44 CDT
Hash Value (MD5): ca02441f92308a690ab0473702f1f6e9
Comments/Description: This file was found as a presentation to give to college students to provide them with student loans that the suspect could then use to generate more income.

** Continued on Supplement Page**

This section contains details on the items examined for this case.

Evidence Number:	1	**Evidence Number:**	
Device Type:	Forensic Image	**Device Type:**	
Make:		**Make:**	
Model:		**Model:**	
Serial Number:		**Serial Number:**	
Capacity (GB):	60 GBs	**Capacity (GB):**	
Comments:	Forensic Image provided to me for the investigation	**Comments:**	
Exam Method:	Acquisition (File System)	**Exam Method:**	
Date:	3/14/20223	**Date:**	
Forensic Software:	Autopsy	**Forensic Software:**	
Forensic Hardware:	Forensic Workstation	**Forensic Hardware:**	
Evidence Number:		**Evidence Number:**	
Device Type:		**Device Type:**	
Make:		**Make:**	
Model:		**Model:**	
Serial Number:		**Serial Number:**	
Capacity (GB):		**Capacity (GB):**	
Comments:		**Comments:**	
Exam Method:		**Exam Method:**	
Date:		**Date:**	
Forensic Software:		**Forensic Software:**	
Forensic Hardware:		**Forensic Hardware:**	
Evidence Number:		**Evidence Number:**	
Device Type:		**Device Type:**	
Make:		**Make:**	
Model:		**Model:**	
Serial Number:		**Serial Number:**	
Capacity (GB):		**Capacity (GB):**	
Comments:		**Comments:**	
Exam Method:		**Exam Method:**	
Date:		**Date:**	
Forensic Software:		**Forensic Software:**	
Forensic Hardware:		**Forensic Hardware:**	

This section contains additional details about the examination.

FOUNDATIONAL ANALYSIS MEDIA:

The details of the investigation and the forensic imaging file was provided to me to conduct an analysis on pertaining to the investigation at hand. The image that was provided to me was ceated using AcceessData FTK Imager v.4.2.1.4 on April 22nd 2020. The image files were provided to me in the zipped file called 2020 CTF - Windows, once extracted I used Autopsy to conduct my analysis and search for evidence pertaining to the investigation. Autopsy was also used to ensure the authenticity and to validate the forensic image.

STEPS TAKEN:

From the analysis there were 4 files(png, xlsx, pptx, txt) that were of specific interest for the investigation. These files are attached and outlined in this report. This evidence is being securely kept on my forensic machine hardware.

ADDITIONAL INFORMATION:

Verified forensic image hash is located in the provided evidence folder as the file "VerificationHash.png"

REPORTED BY
Gunnar Yonker
0

LAB NUMBER
4

START DATE
3/11/2023

COMPLETED DATE
3/14/2023

SUBMITTING AGENCY
CYBER 742

SEMESTER
SPRING 23

INSTRUCTOR
Schoeneck

0

TYPE OF INVESTIGATION
Policy Violation

SUSPECT
Warren Hamilton

SUPPLEMENTAL INFORMATION:

The following evidence of interest was a png file:
File Name: really hang in there.png
Full Path to file:
/img_DFA_Windows.E01/vol_vol2/Users/Warren/Documents/Cats/really hang in there.png
Size: 306674 bytes
Created Date/Time: 2020-04-22 16:54:00 CDT
Last Accessed Date/Time: 2020-04-22 16:54:00 CDT
Last Modified Date:Time: 2020-04-22 16:54:00 CDT
Hash Value (MD5): 799c7c8714bcbb74c126f7fbf0b5e8b4
Comments/Description: The size of this png file was suspicious and I suspected that it may contain another file. Using OpenSteno I was able to recover the text file document titled "Hang in there.txt".

I noted the following web searches during the investigation:

Search Query: "they see gambling sites on vpn?"
Created Date/Time: 2020-02-14 09:39:50 CST
Hash Value (MD5): 0ab29a09c30c976d946f8abcfec7e6e6
Comments/Description: This search implies that the suspect may have been using a VPN service to hide their activities from their organization.

Search Query: "online poker for money"
Created Date/Time: 2020-02-14 09:39:50 CST
Hash Value (MD5): 0ab29a09c30c976d946f8abcfec7e6e6
Comments/Description: This search implies that the suspect was searching for ways to gamble online through poker.

Ending….No further information was documented at this time.

In this investigation, I followed a meticulous procedure to store and archive the items pending analaysis. Once the data had been identified and collected, I transferred the evidence to my forensic workstation's dedicated drive. To ensure that the original forensic image of the suspect's system had not been altered, the hashes were verified and documented which is included in the attached evidence folder. Through the use of the forensic tool Autopsy I was able to analyze the above digital evidence and ensure that it was valid and authentic through the MD5 and SHA hashes.

REPORTED BY
Gunnar Yonker
0

LAB NUMBER
4

SUMMARY CONTINUED: