**UWW Cyber - Investigations Division**
**LAB REPORT**

**REPORTED BY**
Gunnar Yonker

**LAB NUMBER**
2

**START DATE**
2/11/2023

**COMPLETED DATE**
2/12/2023

**COURSE**
CYBER 742

**SEMESTER**
SPRING 23

**INSTRUCTOR**
Schoeneck

**TYPE OF INVESTIGATION**

**SUSPECT**

**LAB REPORT SUMMARY:**

## 21-0211 Forensic Acquisition Report

**--------------------------------------------------------------------------------**

**EVIDENCE**

**Evidentiary Item #1.1 – 23-0211**
**Item:** Memory capture - DESKTOP-VT2D789_mem.raw
**Acquisition MD5 Hash: 0efc5e0f8dd4047edb62e8c269856441**
**Acquisition SHA1 Hash:**
**d4cfe8b74de0e401f29f6508f5e409e4d0744a24**

**Evidentiary Item #1.2 – 23-0211**
**Item:** KAPE capture - DESKTOP-VT2D789_KAPE-cap.zip
**Acquisition MD5 Hash: c4efe6be7afdf2b568ef73c6d4efeab9**
**Acquisition SHA1 Hash:**
**0d8b38b972b470d1c2f4a7c3627ac2897d152341**

**Evidentiary Item #2 – 23-0211**
**Item:** AVML capture - gunnar-VirtualBox_mem.lime
**Acquisition MD5 Hash: 87623fee260f45edd09372c9adf74edb**
**Acquisition SHA1 Hash:**
**50d111ddb1fb797d61d7e6fad02beb2c73c35ef5**

**Evidentiary Item #3 – 23-0211**
**Item:** Memorex 32GB USB flash drive
**Acquisition MD5 Hash: c7a5108ab98eda180be66d03db43225d**
**Acquisition SHA1 Hash:**
**ef4216f2f03ef59d745f1ab359c34a08b4cfbc3d**

**--------------------------------------------------------------------------------**
**---NARRATIVE**

On Saturday, February 11 2023, I, UWW Cyber Investigations Division Digital Forensic Examiner Gunnar Yonker, conducted a forensic acquisition of the follwing devices: Lenovo laptop - Windows, Lenovo laptop - Linux(Ubuntu), and a Memorex 32GB flash drive.

I used Magnet RAM Capture v.120 to capture the RAM from the Lenovo laptop - Windows device. The evidence collected is evidence item #1.1, DESKTOP-VT2D789_mem.raw.
Following the acquisition, I used my home forensic device cmd line with the certutil technique to generate the MD5 and SHA1 hash values of evidence item #1.1. The memory capture was hashed with MD5/SHA1 to verify the integrity of the data and ensure that the data has not been tampered with during the acquision. They are

| | |
|---|---|
| **REPORTED BY**<br>Gunnar Yonker | 0 |
| **LAB NUMBER** | 2 |

**SUMMARY CONTINUED:**

I used Kroll Artifact Parser and Extractor (KAPE) v. 1.3.0.2 to locate and extract target system data and logs based on the !SANS-Triage Module. I encapsulated the extraction into a ZIP archive documented as evidence item #1.2 named DESKTOP-VT2D789_KAPE-cap.zip.

Following the acquisition, I used my home forensic device cmd line with the certutil -hashfile command to generate the MD5/SHA1 hash values of  the DESKTOP-VT2D789_KAPE-cap.zip data to ensure the integrity of the data during the acquision. The hash values are documented above under evidence item #1.2 with the KAPE capture.

In addition to capturing RAM and extracting data, I also collected Windows volatile data using the command line. This information was collected by running various commands such as "netstat" and "tasklist" to gather information about the system's running processes, network connections, and other relevant data. The output of these commands were then saved as text files in the case folders for each device. The collected volatile data provides valuable information about the state of the system at the time of the examination and can be used to reconstruct any actions that took place on the system. By storing the volatile data as text files in the case folders, I ensured that the information has been preserved and is easily accessible for further analysis. The files are clearly labeled with the system name, and what data was collected.

I used AVML v. 0.11.0 to capture the RAM from the Lenovo laptop - Linux(Ubuntu) device. The evidence was collected as evidence item #2 and documented as gunnar-VirtualBox_mem.lime. I used my home forensic device cmd line with the certutil -hashfile command to generate the MD5/SHA1 hash values of the gunnar-VirtualBox_mem.lime file to ensure the integrity of the data during the acquisition. The hash values are documented above under evidence item #2 with the AVML capture.

I used FTK Imager v. 4.7.1 and EnCase Forensice v. 8.10 write blocker to acquire a forensice image of the Memorex flash drive documented as evidence item #3. The write blocker was used to ensure that the data on the flash drive was not tampered with and would not be written to during the acquisition of the evidence. FTK Imager was used to create the forensic image of the USB flash drive.

(CONTINUES ON LAB SUPPLEMENTAL REPORT)

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

| | | | |
|---|---|---|---|
| **Evidence Number:** | 1 | **Evidence Number:** | 2 |
| **Device Type:** | Laptop | **Device Type:** | Laptop |
| **Make:** | Lenovo | **Make:** | Lenovo |
| **Model:** | Windows | **Model:** | Linux-Ubuntu |
| **Serial Number:** | R9-015NR1 | **Serial Number:** | R9-015NR1 |
| **Capacity (GB):** | 80GB | **Capacity (GB):** | 50GB |
| **Comments:** | Windows 10 VM, 8GB of RAM, Black colored laptop, Thinkpad on cover | **Comments:** | Ubuntu VM, 4GB of RAM, Black colored laptop, Thinkpad on cover |
| **Exam Method:** | Live Forensics | **Exam Method:** | Live Forensics |
| **Date:** | 2/11/2023 | **Date:** | 2/11/2023 |
| **Forensic Software:** | Magnet RAM, KAPE | **Forensic Software:** | AVML |
| **Forensic Hardware:** | Forensic Flash Drive | **Forensic Hardware:** | Forensic Flash Drive |

| | | | |
|---|---|---|---|
| **Evidence Number:** | 3 | **Evidence Number:** | |
| **Device Type:** | USB Flash Drive | **Device Type:** | |
| **Make:** | Memorex | **Make:** | |
| **Model:** | USB Flash Drive USB Device | **Model:** | |
| **Serial Number:** | 027912862 | **Serial Number:** | |
| **Capacity (GB):** | 32GB | **Capacity (GB):** | |
| **Comments:** | Red and White colored USB Stick, Memorex 32GB printed on outside | **Comments:** | |
| **Exam Method:** | Live Forensics | **Exam Method:** | |
| **Date:** | 2/11/2023 | **Date:** | |
| **Forensic Software:** | EnCase Forensic, FTK Imager | **Forensic Software:** | |
| **Forensic Hardware:** | Forensic Flash Drive | **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:** | |

**REPORTED BY**
Gunnar Yonker
0

**LAB NUMBER**
2

**START DATE**

**COMPLETED DATE**

**SUBMITTING AGENCY**
CYBER 742

**SEMESTER**
SPRING 23

**INSTRUCTOR**
Schoeneck

**TYPE OF INVESTIGATION**
0

**SUSPECT**
0
1/0/1900

**SUPPLEMENTAL INFORMATION:**

Following the acquisition, I compared the MD5/SHA1 hash values generated by FTK Imager and observed that there were no bad blocks found in the image, and that the MD5 and SHA1 hash values were a match. This verifies the integrity of the foresnic image when compared to the seized evidence that they are a 1:1 match. The hash values will help to ensure that the original evidence has not been tampered with. The write blocker also helps to ensure the original evidence is not written to during the forensic imaging.
I documented the hash values above for the MD5/SHA1 hashes under evidence item #3 for the Memorex flash drive.

I also collected the volatile data from the Lenovo laptop - Linux (Ubuntu) device using the command line. I used commands such as "lsof" and "ps ef" to gather information about the currently open files and running processes. The output of these commands were saved as text files and stored into the case folder for further analysis.

I stored the forensic acquisition evidentiary files on a secure and encrypted external hard drive pending further analysis. I also archived the evidentiary files in a tamper-evident container for safekeeping and to maintain their authenticity as evidence. The external hard drive and the archive containers have been labeled with the case number and a description of the contents for easy identification. To ensure the integrity of the data, I have taken hash values of the original data and the archived files and documented them above in this report.

**REPORTED BY**
Gunnar Yonker
0

**LAB NUMBER**
2

**SUMMARY CONTINUED:**