**Computer Forensics Process Report**

Maks Miketa N0945100

**Case Introduction**

On the 1st of July 2004, I have been called in by an organisation called Sebra that suspects one of its staff members is breaking organisational policy. I was informed that the staff member has joined a strange religious group that considers geometric shapes to be very important and that the staff member was warned in May 2004 against using organisational resources to create, store, search the internet for or disseminate pictures of such shape. My job as an investigator for this case was to identify relevant evidence that can be proved towards this case, ensuring that the provided evidence within this report is the same as the one originally seized and credible.

**Search and Seizure**

I was authorised from a signed letter of approval from a senior person within Sebra to conduct a search and seize procedure at the suspected scene where evidence could be found for the case. Before arriving to the scene, I prepared for the investigation by asking Sebra where the equipment is so I can locate it on arrival, and the type of equipment to arrive prepared with all the tools required for the procedure. After being told the type of equipment and items at the scene, I prepared many faraday bags, a screwdriver set, a box for storing items, a phone charger with multiple cable ports, risk assessment paper for checking volatile data and a camera with photo and video functionality, I asked the organisation for the suspected staff member’s password to aid with the investigation when identifying for evidence on the organisation’s machine and I was provided with it.

Upon arrival to the scene, I started a video recording to record everything I did within the scene as well as around the scene that can be used for evidence of my procedure in court. At the scene, a windows computer was turned on and logged in so I instantly checked the computer’s hard disk light on the computer’s case to see if it was flashing rapidly as this would indicate that a destructive program would be running which would require me to turn the computer off. The computer had the disk light was flashing but, it was not flashing rapidly so turning the computer off was unnecessary.

I looked and took pictures of anything that could contain relevant information and evidence to the case within and around the scene. I identified a mobile phone with its display off behind the keyboard. I checked to see if it was turned on by looking for any lights indicating that the phone is on which there were not any, so I identified and pressed the power button once to see if the display would light up. The phone’s screen did not light up therefore, it was turned off, so I placed it in a faraday bag and attached an evidence label.

I identified three unlabelled memory sticks that were: A silver bottle opener memory stick, a memory stick with a black case and transparent lid and a white and blue memory stick. There was also one 32MB FUJIFILM SD card and a SIM card that were on the desk inside. I placed each item inside a faraday bag and labelled the bags. I looked through the book “catch me if you can” and the A4 paper behind it for any passwords and evidence related to the case. I could not find relevant information from the A4 paper and book so I did not seize them but, I took a photograph of them in case there may be relevant information required from them at a later stage in the investigation. The book was about criminal activity, but it did not contain information about violating organisational policy through using the organisations resources, so it was unnecessary to seize it.

I looked at the back of the computer to see where all the cables were running and to see if any external media devices were connected. The computer was only connected to the monitor, keyboard, and mouse, I then proceeded to perform a risk assessment to gather volatile data which was successful, so I performed capturing volatile data. I made sure the recording captured the monitor screen before doing anything on the computer. I manually collected mandatory volatile data in order from: CPU, cache, register content, physical memory, virtual memory, network state and running processes. I then checked to see if there were any open files, minimised windows, the user that is logged on, chat messages, clipboard contents, visits to websites and other domains, web history on browser and software that could have been used to create images. I concluded the volatile search and powered off the machine through windows power settings. I used a pin to check if there was a CD inside the CD Drive which there was not. I used a screwdriver to open the computer case, I unplugged the hard drives power and data cable, I unscrewed the hard drive mounting bracket, and I placed the hard drive from the computer in a faraday bag and labelled the bag. I photographed all the faraday bags with their labels and finished the search and seize procedure.

**Image Acquisition**

I used the T35u SATA/IDE Forensic Bridge hardware write blocker to create the forensic image of the hard drive in the forensic lab. The purpose of the write blocker was to ensure integrity of all the data on the seized hard drive by preventing any write operations to the original drive and avoid any unintentional changes to the evidence, thus preserving the hard drives authenticity. I connected the power cable to the write blocker to power it on and connected an ESATA cable to the forensic workstation. I connected the SATA and power cable from the write blocker to a test hard drive first to ensure the write block and host detection functions worked and then I connected the seized hard drive. I created a forensic copy of the seized hard drive using FTK imager v4.7.1 (documentation: https://d1kpmuwb7gvu1i.cloudfront.net/Imager/4\_7\_1/FTKImager\_UserGuide.pdf) on a forensically wiped hard drive. After completing the copy, I computed a hash function using the same algorithm on both drives which does not write anything to the seized drive to confirm the values of the two drives are the same. I noted down the hashed function in case I would have to justify the integrity of the forensic image in court.

**Analysis**

I analysed the silver bottle opener memory stick using Autopsy v4.21.0 (software’s documentation: https://sleuthkit.org/autopsy/docs/user-docs/4.21.0//) to investigate the forensic image. I firstly checked to see if the drive had multiple partitions and it only had one. I analysed deleted data on the drive first by looking into the Recycle bin as there might have been data that was not emptied. I then investigated the hidden System Volume information folder which is a snapshot which the System Restore tool in windows uses for its information and restore points. I then investigated the Volume Shadow Copies folder to look for backed up copies/snapshots of the computer. I lastly looked in unallocated space, slack space (carved files) and shadow data within the software. The table below shows the analysis organised based on the BST timeline.

|  |  |  |
| --- | --- | --- |
| Timeline (BST), Born(created) = B, Modified = M, Changed = C, Accessed = A | File/Folder | Analysis |
| N/A | Carved File:  f0000000.jpg | Image:  Has jpg hex header at start and trailer at the end of the file. |
| N/A | Carved File:  f0000639.jpg | Image:  Has jpg hex header start and trailer at the end of the file. |
| N/A | Carved File:  f00033372.db | Database file extension but ms office hex header. File only openable in a word processor which contains unreadable text, and no data is shown when opened in db. opener. Text in hex contains: |
| N/A | Unallocated File:  Unalloc\_4\_545792\_10289152 | Contains jpg hex header start and trailer but not at end of the file. Opened in jpg and has same image as f0000000.jpg and hex data from the other carved files. |
| M at 2004-06-09 21:52:20 | file8.jpg | Image:    Has jpg hex header at start and trailer at the end of the file. |
| M at 2004-06-09 21:53:32 | file9.jpg | Image:    Has jpg hex header at start and trailer at the end of the file. |
| M at 2004-06-09 22:06:22 | random8.dat | Contains unreadable hex text. |
| M 2004-06-09 22:17:38 | random9.dat | Contains unreadable hex text. |
|  |  | Word file only containing image9.jpg:    Has jpg hex header at start and trailer at the end of the file.  Metadata contains creator and Author Brian Carrier.  File directory:  “lillet:Users:bcarrier:proj:dftt:8-jpeg-search:files:pict9.jpg”, “ X-TIKA:origResourceName: lillet:Users:bcarrier:proj:dftt:8-jpeg-search:files:file12.doc” |
| M at 2004-06-10 02:54:53 | file10.jpg | Image:    Has jpg hex header at start and trailer at the end of the file. |
| M 2004-06-10 03:18:41 | random10.dat | Contains unreadable hex text. |
|  |  | NTFS file system was created on the memory stick at 04:22:22  $Boot appears the drive was attempted to be booted with errors.  The $MFT and $LogFile includes a file called FILE0 and e3.jpg that do not appear in autopsy results. SID found in $LogFile: S-1-5-21-1757981266-484763869-1060284298-1003 |
|  |  | file1.jpg image:  Has jpg hex header at start and trailer at the end of the file.  File2.dat has an extension mismatch as it contains jpg hex header at start of file and trailer at the end of the file but has the .dat extension. Image after opening the file in jpg |
|  |  | file6.jpg is a deleted file that is the same as carved file f0000639.jpg as it contains the same image, file size and hex data |
| B at 2004-06-10 04:28:00 | File7.hmm | Deleted file7.hmm has an extension mismatch (.hmm) as contains jpg hex header at start and trailer at the end of the file. Contains the same image and size as carved file f0000000.jpg. |
|  |  | File3.jpg unopenable as image. File contains hex converted into text which contains steganography:  File3.jpg contains no file extension header or footer.  File4.jpg unopenable. Contains jpg hex header at start but trailer not at the end of the file. Unopenable after removing data after jpg footer so can be corrupted/encrypted.  File5.rtf does not contain rtf hex header and two matches for footer hex within file but not at the end of file. Unreadable text when opened in MS word and notepad. |
| |  | | --- | |  | |  | Archive folder contains 3 compressed files in different compressed file extensions.  .boo extension may belong to ZipZag program. |
|  |  | File11.dat contains a jpg hex header not at the start of file and footer at the end of file. Image after removing hex before the jpg header and opening the file as jpg:  The .dat extension is not found and hex code before jpg header is unreadable.  File12.doc created yet created earlier.    File13.dll does not contain .dll hex header and hex header and footer are unidentifiable. File is unreadable when opened.  File13.dll:here has extension mismatch and contains jpg hex header and footer at the end of file. Opened image in jpg: |
|  |  | tracking.log file created. |
| /del2 B at 2004-06-10 04:43:19 BST  File7.hmm A 19s later, then C 6s later. | /del2  /file7.hmm | File7.hmm moved to del folder. |
|  |  | Log file modified. Only contains “Thorntons” in hex. |
| A, C, B, M at 2004-06-10 04:59:31 BST | /RECYCLER/S-1-5-21-1757981266-484763869-1060284298-1003  Desktop.ini  INFO2 | INFO2 has no available text.  Desktop.ini is a windows configuration file. |
| A, C, M /del1 at 2004-06-10 04:59:15 BST then /del2 8s later. | /del1  /del2 | Modified folders. |
| A, C, M at 2004-06-10 04:59:31 BST | INFO2 | Modified file. |
|  |  | Modified the files. |

Table - Autopsy Analysis

**Evidence Reporting**

After analysing the memory stick with Autopsy software, several key findings have been uncovered:

1. The memory stick contains 10 distinct geometric shaped images thus, establishing clear evidence of geometric shapes stored on the memory stick.
2. The memory stick contains deliberate effort to conceal certain geometric shapes and files through renaming of file extensions rendering the files unopenable from the modified file extensions. Additionally, steganography was applied to “file3.jpg” where it should open as an image file but contains hexadecimal digits that translate to human readable text.
3. The “tracking.log” file within the System Volume Information which is a system folder that tracks changes to file paths was modified. This modification aimed to obscure critical information from removing the system’s logs.
4. On the 10th of June at 02:20:00 BST, a Microsoft Word file (file12.doc) was created and saved, as per the word file's metadata. However, conflicting timeline dates identified during the autopsy process suggest potential modifications to the file's metadata. Although the creator, author, and name within the document's directory appear as Brian Carrier, the varying timelines raise the possibility of intentional file modifications by the user, showcasing their ability to manipulate file attributes. The document itself contains solely an image file of a geometric shape. While Microsoft Word is capable to create geometric shapes such as the one within the document, the evidence falls short of establishing conclusive proof of the software being used to create the shapes, as the shape within the document could have been imported. No other software was identified as being used to create these images.
5. A Windows Security Identifier (SID) labelled as “S-1-5-21-1757981266-484763869-1060284298-1003” has been identified in the Recycler folder and within the NTFS hidden system files. This SID is integral for checking the Windows user/group within a domain and holds significance in verifying against Sebra's Windows domain, potentially identifying the owner of the memory stick.

In summary, the evidence clearly indicates the presence of geometric shapes on the memory stick, coupled with attempts to conceal certain shapes through file extension modifications and log file alterations. The user demonstrates knowledge in concealing information using steganography and manipulating files. However, there remains insufficient evidence to definitively link the creation of these shapes to Sebra's organisational resources. Further investigation, specifically matching the directory from file12.doc to the suspected staff member's organisation's machine, organisation's SID, or verifying the individual as Brian Carrier, is necessary for conclusive attribution. Notably, there is no evidence indicating internet usage on the memory stick. Consequently, a thorough investigation is warranted to conclusively ascertain the individual responsible for the contents on the memory stick, given that its location on the member's desk does not guarantee it as the suspect's memory stick until ownership is proven.

**Parallel Reports**

***General Case Documentation***  
Case ID: 2004-4567

Investigation Start Date: 01/07/2004

Investigator: Mark Jobs

Investigator’s Phone Number: 07606510885

Investigator’s email address: markjobs@bestdetectives.com

Type: Digital Forensics

Case Description: Investigation into a potential violation of organisational policies by a staff member at Sebra, associated with a peculiar religious group. The primary focus is on the use of geometric shapes and unauthorised activities involving organisational resources. The case aims to ascertain the extent of the violation, gather relevant evidence, and determine appropriate remedial actions.

***Notebook – Record of Actions***

Case ID: 2004-4567

Procedure ID: S&S-ORG-2004-4567

Date Executed: 03/07/2004

Description: Search and Seizure at Suspected Scene

1. Obtained an authorisation letter from a senior person within Sebra, granting permission for the search and seizure procedure.

2. Coordinated with Sebra to gather detailed information on the location of equipment and specific devices related to the suspected staff member.

3. Requested and secured the suspected staff member’s password from Sebra to facilitate the identification of evidence on the organisation’s machine.

4. Upon arrival at the scene, initiated video recording to comprehensively document all actions and surroundings, ensuring admissibility in court.

5. Checked the powered-on Windows computer for any signs of malicious activity by observing the hard disk light for rapid flashing, indicating potential destructive programs.

6. Systematically surveyed the scene for potential evidence, capturing photographs and identifying relevant items such as a powered-off mobile phone and unlabelled storage devices.

7. Secured the powered-off mobile phone in a faraday bag, attaching an evidence label for proper documentation.

8. Identified, bagged, and labelled three unlabelled flash drives, one 32MB FUJIFILM SD card, and a SIM card found on the desk.

9. Conducted a thorough examination of the book "Catch Me If You Can" and the A4 paper behind it for any passwords or evidence related to the case.

10. If no relevant information was found in the A4 paper, documented it with photographs for potential future reference.

11. Inspected the back of the computer to assess cable connections and external media devices. Performed a risk assessment to guide the collection of volatile data.

12. Manually collected mandatory volatile data, including information from CPU, cache, register content, physical memory, virtual memory, network state, and running processes.

13. Checked for open files, minimised windows, logged-on user details, chat messages, clipboard contents, website visits, and software related to image creation.

14. Concluded the volatile data search and powered off the machine through Windows power settings.

15. Used a pin to check the CD Drive for any inserted CDs, noting the absence of any.

16. Utilised a screwdriver to open the computer case, disconnected the hard drive's power and data cables, unscrewed the hard drive mounting bracket, and secured the hard drive in a faraday bag. Labelled the bag appropriately.

17. Photographed all faraday bags with their respective labels to maintain a comprehensive record of the search and seizure procedure.

18. Concluded the search and seizure process, ensuring adherence to established protocols and chain of custody procedures.

***Chain of Custody***

Case ID: 2004-4567

Item: 32MB FUJIFILM SD Card

Date Collected: 04/07/2004 11:30 BST

Date Returned: 05/07/2004 14:00 BST

Collector: Detective Michael Silverbridge

Description: Performing Forensic Image Copy on SD Card

Chain of Custody: Collected SD card from seized isle in the forensic laboratory storage area to perform a forensic image copy on the SD card then returned to the storage area in the seized isle.

***Process Documentation***

Case ID: 2004-4567

Analysis ID: IA-2004-4567-002

Date Conducted: 08/07/2004

Analysis Type: Image Acquisition

Software Versions: FTK Imager v4.7.1, Autopsy v4.21.0

Details:

Created a forensic copy of the seized hard drive using FTK Imager v4.7.1 on a forensically wiped hard drive. Software documentation: https://d1kpmuwb7gvu1i.cloudfront.net/Imager/4\_7\_1/FTKImager\_UserGuide.pdf

Computed hash values using the same algorithm on both drives without writing anything to the seized drive.

Noted down the hashed function for court justification of the forensic image integrity.

Conducted analysis using Autopsy v4.21.0. Software’s documentation: https://sleuthkit.org/autopsy/docs/user-docs/4.21.0//

**References**

fileinfo.com. (n.d.). BOO File - What is a .boo file and how do I open it? [online] Available at: https://fileinfo.com/extension/boo [Accessed 13 Dec. 2023].

Kessler, G. (2019). File Signatures. [online] Garykessler.net. Available at: https://www.garykessler.net/library/file\_sigs.html.