**Digital Forensic Report**



Student Assignment Submission Form

=====================================================================================

I/we declare that the attached assignment is wholly my/our own work in accordance with Seneca Academic Policy. No part of this assignment has been copied manually or electronically from any other source (including websites) or distributed to other students.

Name(s): Ajay Jiwanand, Miguel Gonzales

Student ID(s): 028-942-134,

=====================================================================================

**Report prepared by**: Ajay Jiwanand and Miguel Gonzales

**Investigator(s)**: Ajay Jiwanand and Miguel Gonzales

**Report prepared for**: I.M.A. Lawyer

**Case**: SPR401-Assignment2

**Report Created**: April 15th, 2015

**Reference Case**: SPR401-Assignment1

**Table of Contents**

[Introduction](#Introduction)..........................................................................................................3

[Results/Comments](#ResultsComments)................................................................................................3

[Conclusions/Opinion](#Conclusions).............................................................................................3

[Data Acquisition and Media Analysis](#DataAcquisition)…………….......................................................4

[Exhibits](#Exhibits)..................................................................................................................6

[Image](#Image)...........................................................................................................6

[List by File Path](#EvidenceFilePath)............................................................................................6

[Additional evidence recovered](#AdditionalEvidence)...................................................................7

[Appendixes](#Apendixes)............................................................................................................8

**Introduction**

We were given a laptops hard drive from Mr. Lawyer to examine for any evidence that suggest Mia hacker is committing financial fraud. In addition to primary investigation we were also instructed to look for any evidence pertaining to the previous case that we were given. The attorney for Seneca College also required us to examine the disk for evidence supporting the school violation of cheating and any other infractions constituting a violation of Seneca’s [Information Technology Acceptable Use Policy](http://www.senecac.on.ca/policies/itau.html). All evidence must be copied and stored in report format.

**Results and Comments**

The investigation was conducted according to the attorney directions. All types of files (normal, temporary, deleted, fragmented) were examined. All parts of the hard drive were searched as well which included allocated and unallocated space. The examiners used Autopsy to carry out their investigations. Upon investigation we found that there were many instances of violation of Seneca’s policy. 4 of them being child porn and 2 of adult porn. There was also 3 instances in which files were found that linked to the previous case which shows interactions to achieve answers for the test as well as the answers. As far as the main case is concerned we did not find so much evidence against Mia. Thus we cannot confirm that she has committed any financial fraud. However we do suggest that an authorized person look into the New Zealand bank account number we found. As well as lookup the numbers in the address book and enquire if they are real account numbers. If any of this further investigation is deemed successful we suggest that a more inclusive investigation be done on Mia and her actions.

**Conclusions and Opinion**

The evidence found during the investigation does not support the accusation that Ms. Hacker was involved with fraudulent acts, or with the loss of the student council’s $25 000. There was some suspicious activity which we found on the hard drive but are unable to conclusively conclude that she committed financial fraud without any further investigation on the evidence that we did find. However, there is evidence to support that the accused was in violation of Seneca’s Information and Technology Use Policy on multiple occasions, as well as ownership and quite possibly the distribution of child pornography.

**Data Acquisition and Media Analysis**

The hard drive make/model/geometry are as follows:

Maxtor Diamond Max VL 40 Hard drive

4.87 GB internal 3.5" ATA

5400 RPM Model 32049H2

2491 cylinders

255 heads

63 sectors/track

The hard drive was examined for files and evidence. Files searched included normal, temporary, and deleted files. File fragments were also searched in the *HPA* [[1]](#footnote-1)and unallocated space.

Licensed software authorized to investigator used in the examination consisted of:

* Autopsy, Version 2.24., a web-based GUI for Sleuth kit
* Sleuth Kit Version 4.13, programs used in digital forensic investigation
* md5sum Version 8.13, tool used to calculate MD5 hash value for a file
* hdparm Version 9.30, tool to test for existence of HPA/DCO on hard drive.

Hardware used in examination consisted of:

* Tableau Forensic SATA/IDE Bridge, Model T35E. Serial #000ECC2000358026

Information about the write blocker can be accessed following this [link](https://www.guidancesoftware.com/products/Pages/tableau/products/forensic-bridges.aspx). Write blockers are required in investigations to keep the integrity of the examined hard drive intact and accurate.

Examination of hard drive occurred on February, 26, 2015 at 12:15pm. Examination details consist of:

1. Investigators receive and begin examining process of hard drive.

2. Hard drive connected to write blocker.

3.  *Sha1 Hash* of hard drive calculated.

4. *Image* acquired from hard drive and stored on *sanitized media*.

5. Sha1 *hash* was calculated from the image and compared to *hash* value of hard drive. Both values were: 9b42fa2d3ff86eaaaa36a06eed628fc380f349ce. It can be concluded drive and image have exact same information.

6. *Host Protected Area* (HPA) and *Device Configuration Overlay* (DCO) were inspected. None were found.

7. Hard drive was given back to Lab monitor on February, 26, 2015 at 12:40pm.

8. Forensics inspection began on *image file*, which was imported into Autopsy on March.03 at 10:15pm.

4. Hard drive inspection determined that there was 4 *allocated* volumes and 5 unallocated spaces that we will refer to as unallocated volumes for this report. The arrangement of the hard drives consisted of: Volume 1 (unallocated 0-62 physical disk sectors). Volume 2 (allocated DOS FAT 16 C:/ 63-1028159 physical disk sectors). Volume 3 (unallocated 1028160-1092419). Volume 4 (DOS FAT 16 D:/ 1092420-3084479). Volume 5 (unallocated 3084480-3084605). Volume 6 (DOS FAT 16 E:/ 30845606-4128704). Volume 7 (unallocated 4128705-4128767). Volume 8 (Linux 4128768-7422029). Volume 9 (unallocated 7422030-40021631). Hard drive inspection stopped on March.03, at 11:30pm.

5. Examination of the file system began on March.04, at 7:45am and it was concluded that the hard drive contained 10 separate files that contained some form of answers to test questions that seem relevant to the case. 3 of the files were deleted, 2 files were not deleted, and 5 were stored in allocated spaces. The location of each message is stated as follows: Vol1Unallocated.txt (physical disk address 1 in unallocated space), Vol2Unallocated.txt(), q7.txt (physical disk address 2070, logical volume address 2007 in volume 2), Desktopini.txt (physical address 1878, logical volume address 1815 in volume 2), Reso~1.doc (physical add 615, logical add 552 in volume 2), Hacker-Answers.txt/gedit-save-KZ5C1U.txt (physical 1093005, logical 585 in volume 4), Vol7Unallocated.txt (physical 4128705 in unallocated space), Vol9Unallocated.txt (physical 7422050 in unallocated space), BBT No 200.doc (physical 3526, logical volume address 3442 in volume2), Beethoven.mp3.txt/Gedit-save-B (physical1862 , logical volume address 3303 in volume2). Chuck.jpg/\_.JPG (physical 2313, logical 903 in volume 2), Spot.txt/\_.GIF (physical 742, logical 695 in volume 2)

6. The investigation of hard disk *unallocated space* and *slack space* was conducted. Forensic searches consisted of trying to find matches of string words such as “question”, “answer”, “test”. Disk locations can be manipulated to include unallocated space for the purpose of hiding information and because non-forensic software usually doesn’t have any reason to look at these non-used spaces, it gives the opportunity to hide data in these places.

7. Foremost and autopsy were used on the unallocated space in an attempt to find files, emails, and pictures that could be imperative to the case. Searching for string matches and any information in these unallocated spaces were conducted. Due to the fact that the un-allocated space was chosen in a specific spots as the beginning/end and in between partitions, and due to the very nature of unallocated space not being used for anything but the intent to hide data or be non-written over data, it would be objective to conclude they were used for the intent to hide information.

8. Messages were also found on the hard drive that are in direct violation of Seneca’s Information Technology Acceptable Use Policy. Specifically, 4 instances of an email message that contained a conversation about a student being paid to do another students work. There were also 4 instances of pornographic images found on the drive. Examination stopped on March.04, at 5:30 pm.

**Exhibits**

The investigation has produced results in the form of files and autopsy reports found below. The following links will show what was found on the hard drive and a corresponding report giving more detailed information such as size and location of file.

**Image**

The image was obtained by using the dd image command in Linux. 9 test answer case related messages were found. There were also 4 instances of emails and 4 instances of pornographic pictures found on the hard drive, which are in violation of Seneca IT policy. Information about the image of the hard drive is contained in this report found [here](file:///C:\Users\Sharlene\Downloads\DiskImage).

**Evidence File Path**

The following is a list of hard drive contents relevant to this case found

|  |  |  |  |
| --- | --- | --- | --- |
| ***Name*** | ***Report*** | ***MFT Entry*** | ***Notes*** |
| [images[2].jpg](Evidence/images%5b2%5d.jpg) | [Report](Evidence/images%5b2%5d.jpg) | 11094 | Account information from what looks to be a new Zealand bank account purposely hidden by changing the file extension |
| [miahacker.wab](Evidence/Mia%20Hacker.wab) | [Report](Autopsy%20Reports/miahackerwab.txt) | 10939 | An address book which contains some of the people that mia hacker used to communicate with. It also contains some numbers formulated like account numbers. Although we cannot confirm these are actual account numbers they are very suspicious |
| [mia hacker-old.wa~](Evidence/Mia%20Hacker-old.wa~) | [Report](Autopsy%20Reports/miahackeroldwa.txt) | 11076 | Another address book which seems to be an older one |
| [accounts.ink](Evidence/Accounts.LNK) | Report |  | A shortcut to a file which suspiciously named accounts. We did not find this file however we felt obligated to mention this shortcut. |
| [fun.zip](Evidence/fun.zip) | [Report](Autopsy%20Reports/funzip.txt) | 9428 | An encrypted zip file containing some files. This is highly suspicious which it is placed under main case evidence |

**Additional Evidence**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Item Recovered*** | ***Reports*** | ***MFT Entry*** | ***Notes*** |
| [AC391B80BB828EF97 D96A43D34B2A4[1].jpg](Additional%20Evidence/AC391B80BB828EF97D96A43D34B2A4%5b1%5d.jpg) | [Report](Autopsy%20Reports/AC.txt) | 9434 | A file containing evidence suggesting that Mia was offering bachelor degrees for a price however this may be spam and we cannot confirm this |
| [c1[1].jpg](Additional%20Evidence/c1%5b1%5d.jpg) | [Report](Autopsy%20Reports/c1.txt) | 9432 | Deleted Adult porn picture that violates Seneca policy |
| [c2[1].jpg](Additional%20Evidence/c2%5b1%5d.jpg) | [Report](Autopsy%20Reports/c2.txt) | 9434 | Deleted Child porn picture that violates Seneca policy |
| [c3[1].jpg](Additional%20Evidence/c3%5b1%5d.jpg) | [Report](Autopsy%20Reports/c3.txt) | 9432 | Deleted Child porn picture that violates Seneca policy |
| [c4[1].jpg](Additional%20Evidence/c4%5b1%5d.jpg) | [Report](Autopsy%20Reports/c4.txt) | 9433 | Deleted Child porn picture that violates Seneca policy |
| [c5[1].jpg](Additional%20Evidence/c5%5b1%5d.jpg) | [Report](Autopsy%20Reports/c5.txt) | 9435 | Deleted Child porn picture that violates Seneca policy |
| [images[9].jpg](Additional%20Evidence/images%5b9%5d.jpg) | [Report](Autopsy%20Reports/image9AP.txt) | 9432 | Deleted Adult porn picture that violates Seneca policy |
| [images[3].jpg](Additional%20Evidence/images%5b3%5d.jpg) | [Report](Autopsy%20Reports/images3.txt) | 9434 | Deleted Adult porn picture that violates Seneca policy |
| [Deleteditems.dbx](Additional%20Evidence/Deleted%20Items.dbx) | [Report](Autopsy%20Reports/deleteditemsdbx.txt) | 10962 | Shows an exchange of email between Karen and Mia which contains the answers to the test from the previous case |
| [sentitems.dbx](Additional%20Evidence/Sent%20Items.dbx) | [Report](Autopsy%20Reports/sentitemsdbx.txt) | 10959 | Also shows an exchange of email pertaining to the previous case |
| [Sp7.dll](Additional%20Evidence/sp7.dll) | [Report](Autopsy%20Reports/sp7dll.txt) | 9619 | A file containing the answers of the test in the previous case hidden by changing the extension to dll |

**Appendixes**

* **[Hardware Inventory](C:\\Users\\Ajay\\Documents\\SPR401\\Apendixes\\Hardware Inventory.pdf)**
* [**Chain of Custody**](file:///C:\Users\Ajay\Documents\SPR401\Apendixes\Chain%20of%20Custody.pdf)
* [**Glossary of Terms**](file:///C:\Users\Ajay\Documents\SPR401\Apendixes\Glossary.pdf)
* [**Technical Background Topics**](file:///C:\Users\Ajay\Documents\SPR401\Apendixes\TechnicalBackgroud.pdf)

1. All words that are in *italics* can be found in the glossary.

   [↑](#footnote-ref-1)