# 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, Bernard Adamski
Student ID(s): 028-942-134, 069-983-138
==================================================================================

**Report prepared by**: Ajay Jiwanand and Bernard Adamski
**Investigator(s)**: Ajay Jiwanand and Bernard Adamski
**Report prepared for**: I.M.A. Lawyer
**Case**: SPR401-1
**Report Created**: March 3rd, 2015
**Reference Case**: N/A

# Table of Contents

## Introduction

Seneca College lab technician gave us a hard disk drive on February 26.2015 to be forensically investigated. The hard disk was confiscated from a student who was accused of cheating on a final exam. The attorney for Seneca College requires 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. 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 (forensic toolkit analyzing disk image) and Foremost (raw data recovery tool) software to assist in the investigation. The circumstantial evidence found consisted of various messages and files that contained answers to test questions found throughout the hard drive. These messages were found in suspicious areas that would suggest they were being used to hide data that would impede the college's non-cheating policy. In addition, an email message was found where it suggest that a student was being paid to do work for another student. Finally, there were many pornographic images found on the hard drive that is a direct violation of Seneca's IT policy.

## Conclusions and Opinion

The evidence found in the investigation does support the accusation of the student using their hard drive to store answers to be used during the examination. It further goes to support that the student was in 2 additional violation of school policy in the form pornography and recruiting other students to do personal work.

# Data Acquisition and Media Analysis

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

Maxtor Diamond Max VL 40 Hard drive
20.5 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]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
- dd, Version 8.13, tool used to create file image from storage device
- 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.
- Foremost, Version 1.5.7, tool used to support digital forensic investigation

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. Write blockers are required in investigations to keep the integrity of the examined hard drive intact and accurate.

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

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.

## Evidence File Path

The following is a list of hard drive contents relevant to this case found and when possible, an autopsy report giving more detailed information.

| *Name* | *Report* | *Notes* |
|---|---|---|
| Vol1Unallocated.txt | Autopsy Report | This information was purposely hidden in unallocated space and could only be saved there manually. |
| Vol2Unallocated.txt | | Purposely hidden information unallocated space. |
| q7.txt | Autopsy Report | Deleted file “q7” had answer to question 7. |
| Desktopini.txt | Autopsy Report | Question 6 answer found in Desktop.ini file. |
| MyDoc~1.txt | Autopsy Report | Deleted MyDoc~1 file had quest 5 answer. |
| Vol3Unallocated.txt | | Quest 4 answer found in unallocated space. |
| Hacker-Answers.txt<br>gedit-save-KZ5C1U.txt | Autopsy Report | All answers were found in Hacker – Answers and deleted file gedit-save-KZ5C1U also had same copy of all answers to questions. |
| Vol7Unallocated.txt | Autopsy Report | Q2 answer found in unallocated space. |
| Vol9Unallocted.txt | Autopsy Report | Q3 answer found in unallocated space. |

## Additional Evidence

| *Item Recovered* | *Reports* | *Notes* |
|---|---|---|
| BBT No 200.doc<br>beethhoven.txt<br>Beethoven.mp3<br>Gedit-save-B | Autopsy Report<br>Autopsy Report | This email conversation violates Seneca’s college policy on having another student hand in another students work. |
| spot.txt | Autopsy Report | Porn picture that violates Seneca policy |
| _.GIF | | Deleted porn picture spot.txt file |
| _.JPG | | Deleted porn picture chuck.jpg file |
| chuck.JPG | Autopsy Report | Porn picture that violates Seneca policy |

# Appendixes

- Hardware Inventory
- Chain of Custody
- Glossary of Terms
- Technical Background Topics