Seizure Lab

IT566-001

Dane Morgan

Aaron Cowley

25 January 2019

Table of Contents

[1. Executive Summary 1](#_Toc536197250)

[2. Background 2](#_Toc536197251)

[3. Preperation 2](#_Toc536197252)

[3.1 Documentation 2](#_Toc536197253)

[3.2 Tools 2](#_Toc536197254)

[3.3 Lab Sign Up 2](#_Toc536197255)

[4. Methodology 3](#_Toc536197256)

[4.1 Access 3](#_Toc536197257)

[4.2 Visual Scan 4](#_Toc536197258)

[4.3 Volatile Memory Capture 4](#_Toc536197259)

[4.4 Device Identification 5](#_Toc536197260)

[4.5 Chain of Custody Release 5](#_Toc536197261)

[4.6 Evidence Authentication 5](#_Toc536197262)

[4.6.1 Digital Evidence Hash Table 5](#_Toc536197263)

[4.6.2 Document Description and Hash Table 6](#_Toc536197264)

[5. Investigator Bio 6](#_Toc536197265)

[5.1 Dane Morgan 6](#_Toc536197266)

[5.2 Aaron Cowley 6](#_Toc536197267)

[References i](#_Toc536197268)

[Appendices ii](#_Toc536197269)

[Appendix A: Search Warrant 1.4.4 ii](#_Toc536197270)

[Appendix B: Evidence Chain of Custody Tracking Form 1.4.0 ii](#_Toc536197271)

[Appendix C: Consent To Search Electronic Media 1.4.1. ii](#_Toc536197272)

[Appendix D: Notes 1.4.3 ii](#_Toc536197273)

[Appendix D: Workstation 1.1.0 ii](#_Toc536197274)

[Appendix E: Family Photo 1.1.2 ii](#_Toc536197275)

[Appendix F: Kittens Photo 1.1.3 ii](#_Toc536197276)

[Appendix G: Computer Desktop 1.1.1 ii](#_Toc536197277)

[Appendix H: Digital Evidence Hash Table ii](#_Toc536197278)

[Appendix I: Document Description and Hash Table iii](#_Toc536197279)

[Appendix J: Devices Evidence Table iii](#_Toc536197280)

[Appendix K: Investigator Dane Morgan CV iii](#_Toc536197281)

[Appendix L: Investigator Aaron Cowley CV iii](#_Toc536197282)

# Executive Summary

On 24. January 2019, we Dane Morgan and Aaron Cowley, carried out the seizure and digital evidence collection of an iMac 5. We were able to successfully obtain several pieces of evidence, including a volatile memory capture, several photos of the crime scene, and MD5 checksums for each piece of evidence. In addition to the evidence we collected; we, to the best of our knowledge have prepared and completed all necessary documents for the seizure of computer equipment and of digital media.

# Background

On 18. January 2019, Dr. Justin Giboney informed us that we would be performing a digital evidence collection and seizure lab. Additionally, Giboney informed us that for the scope of this lab we could use our smart phones to take pictures of evidence.

On 21. January 2019, we received an email from Dr. Justin Giboney instructing to do the following:

* + 1. Come prepared with everything we need to do a criminal investigation.
    2. Sign up for a time on Google Sheets to come to room CTB 350 to perform our lab

On 22. January 2019, we received email from Dr. Justin Giboney with instructions on how to perform volatile memory collection on OSX and to bring a device to collect volatile memory.

# Preperation

## 3.1 Documentation

To prepare for evidence collection we submitted a request1 for a search warrant from the United States Department of the Treasury. We received our warrant on 24. January 2019 (see Appendix A).

We printed copies of NIST’s “Evidence of Chain Custody Tracking” form2 (see Appendix B) and a copy of the United States Secret Service “Consent to Search Electronic Media” form3 (see Appendix C).

## 3.2 Tools

As instructed, we brought a USB flash drive (evidence no. 1.0.3) to collect volatile memory. We ensured that our USB drive was exFAT formatted so that the drive could be mounted on OSX. In case of drive failure, we bought an additional USB drive (evidence no 1.0.4).

We brought Dane Morgan’s iPhone 7 to take pictures of evidence at the scene.

To take notes, we prepared ample graph paper.

## 3.3 Lab Sign Up

As instructed in Dr. Giboney’s email, we signed up a time slot at 1:00PM on 24. January 2019 at 1:00PM

# Methodology

## 4.1 Access

We arrived at CTB 350 at 12:53PM and were greeted by Dr. Giboney. We presented Dr. Giboney our search warrant (Appendix A) and search consent (Appendix C) form. Dr. Giboney signed our consent form and Aaron Vivian signed as a witness.

Giboney informed us that he is the lab technical showed us to Workstation 1 and informed us that we were welcome to ask him any questions, should we need help. Upon arrival, we took pictures of Workstation 1(See Appendix D) and took pictures of the photos that were taped to the desk (See Appendix E and Appendix F).

The devices at Workstation 1 are the following:

1 iMac 24-inch, Early 2008 (evidence no. 1.0.0)

1 Generic HP Keyboard (evidence no. 1.0.1)

1 Generic HP Optical Mouse (evidence no. 1.0.2)

Figure 4.1.1 Workstation upon arrival (evidence no. 1.1.0)

As shown above, the computer 1.0.0 was asleep. At 12:55PM we hit the space bar to wake it up. A login screen appeared with the user’s name as “Local Admin” with a blank password field. We tried various common password to try and login. After four or five failed login attempts, we tried switching users, this was not helpful because the both username field and password field were both blank.

We asked Dr. Giboney what the username for computer is and if he knew what the password was. Dr. Giboney told us that the username was “ladmin” and the password probably related to the type of cats in the picture.

At 1:00 PM we successfully login with the following credentials:

username: ladmin

password: kittens

Figure 4.1.2 Kittens picture (evidence no. 1.1.3)

## 4.2 Visual Scan

Once logged in, the desktop showed that following applications were open:

Finder

Safari

Sublime Text (version not known)

Terminal

We could see that this computer was not connected to any internal or external network by checking the network status icons in macOS’s Menu Bar.

Figure 4.1.2 Kittens picture (evidence no. 1.1.3)

## 4.3 Volatile Memory Capture

Once we were done with our initial visual scan of the desktop, we proceed to capture and save volatile memory. We inserted USB drive 1.0.3., opened Terminal.app, then signed is as the root user with password we had obtained earlier with the following command:

$ sudo su

Now with root access, we changed directories to mountpoint of USB drive 1.0.3 with the following command:

$ cd /Volumes/sandisk

With our current working directory set properly, we then captured volatile live memory with the following command:

$ /Users/ladmin/Desktop/osxpmem.app/osxpmem -o ./24\_january\_2019\_memcap\_ \_\_tests-iMac-5-evno-1-2-0.aff4

At 1:14PM, our memory capture was successfully saved to USB drive 1.0.3.

## 4.4 Device Identification

To find out more details about computer 1.0.0 we opened “About This Mac” on the Menu Bar, then clicked “More Information”. From there were able to find the following information:

Model: iMac 5 (24-inch, Early 2008)

Serial Number: QP220NWZE7

## 4.5 Chain of Custody Release

At 1:22PM, we released the computer 1.0.0 to Justin Giboney and completed the appropriate chain of custody form (Appendix B), then left the premise.

## 4.6 Evidence Authentication

Back at our lab, we inserted USB drive 1.0.3 and made a copy to our machine of the volatile memory capture (1.2.0), all photos (1.1.0-3), and documents (1.4.0-4).

To ensure the integrity of our evidence and documentation of this case, we obtained MD5 checksums of each file. We obtained the MD5 checksums for the memory capture and photos with the following command:

$ md5sum ./\* > seizure-lab-hashes.chk

Below are the evidence and documentation hash tables.

### 4.6.1 Digital Evidence Hash Table

|  |  |  |  |
| --- | --- | --- | --- |
| Digital Evidence Description and Hash Table | | | |
| Description | Evidence No. | Filename | MD5 Hash |
| iMac-5 Memory Capture | 1.2.0 | 24\_january\_2019\_memcap\_tests-iMac-5-evno-1-2-0.aff4 | ef4b5c1418ad2d2db8c0b0c485e20840 |
| Workstation | 1.1.0 | workstation-1.1.0.jpg | d4e389fd54a6ec9867e2ec5f7c690195 |
| Computer Desktop | 1.1.1 | desktop-1.1.1.jpg | d47af00d7e438d30dafb9ae0506ec27c |
| Family Photo | 1.1.2 | family-picture-1.1.2.jpg | ff2bd31bf17f2b79fd61ca68e27efb19 |
| Kittens Photo | 1.1.3 | kittens-1.1.3.jpg | 0db009274b6cef9002765cdb68c28e45 |

### 4.6.2 Document Description and Hash Table

|  |  |  |  |
| --- | --- | --- | --- |
| Document Description and Hash Table | | | |
| Description | Evidence No. | Filename | MD5 Hash |
| Evidence of Chain of Custody Tracking Form | 1.4.0 | evidence-of-chain-of-custody-tracking-form-1.4.0.pdf | 2bb5c939adecb6249921af99c27f2d11 |
| Consent to Search Electronic Media Form | 1.4.1. | conset-to-search-electronic-media-1.4.1.pdf | 9ceac6c0cbfbbdaf213b6a69bf5f4ef3 |
| Search Warrant | 1.4.2 | search-warrant-1.4.2.pdf | d837901ec913f31addb93b57c33f0d3e |
| Hand Written Notes | 1.4.3 | notes-1.4.3.pdf | 6cd5a711842e8887a05cf686893d652c |

To ensure that our evidence could not be lost via data corruption or system failure, we made two copies of each piece of evidence. We saved one copy to Dane Morgan’s lab computer, and second on USB drive 1.0.4.

# Lessons Learned

Looking back, there are two mistakes that we can do better on the lab:

* 1. Take more detailed time series notes.

Next time, we just need to be more diligent about writing down everything we do with the corresponding time. Having detailed time-series notes is essential to writing a valid forensic report.

* 1. Pay attention to what applications are open on the machine we are examining.

Next time, after we perform the memory capture, we need to look at all the applications that are open. We missed some evidence because we didn’t look at the pages that were open on Safari and Sublime Text.

# Bio

## 6.1 Dane Morgan

I work in the CSRL as a research assistant and am currently senior in the Cybersecurity major. I am planning on attending graduate school at BYU to earn my master’s degree in Technology. I am a skilled programmer and am a member PyPI, I have published several security related packages to their repository. I am part of BYU’s CCDC Team, I typically lead the hardening Unix-based systems and setting up and IDS/IPS. While I am skilled with Unix-based systems, my knowledge and skill with Windows systems is shallow and limited.

## 6.2 Aaron Cowley

I am a undergrad student in Cybersecurity in the cybersecurity major and currently work as a research assistant for the BYU Cybersecurity Research Lab. I am an avid cybersecurity student and have gained a lot of experience in cybersecurity as a research assistant. I also compete in CCDC competitions that help train me in defensive cybersecurity and incident response.

# References

*Best Practices for Seizing Electronic Evidence.* n.d. https://www.crime-scene-investigator.net/SeizingElectronicEvidence.pdf (accessed January 24, 2019).

IRS. *9.7.2 Civil Seizure and Forfeit | Internal Revenue Service.* n.d. https://www.irs.gov/irm/part9/irm\_09-007-002 (accessed January 24, 2019).

*Sample Chain of Custody Form.* n.d. https://www.nist.gov/document/sample-chain-custody-formdocx (accessed January 24, 2019).

# Appendices

## Appendix A: Search Warrant 1.4.4

See attached file: search-warrant-1.4.2.pdf

## Appendix B: Evidence Chain of Custody Tracking Form 1.4.0

See attached file: evidence-of-chain-of-custody-tracking-form-1.4.0.pdf

## Appendix C: Consent to Search Electronic Media 1.4.1.

See attached file: conset-to-search-electronic-media-1.4.1.pdf

## Appendix D: Notes 1.4.3

See attached file: notes-1.4.3.pdf

## Appendix D: Workstation 1.1.0

See attached file: workstation-1.1.0.jpg

## Appendix E: Family Photo 1.1.2

See attached file: desktop-1.1.1.jpg

## Appendix F: Kittens Photo 1.1.3

See attached file: kittens-1.1.3.jpg

## Appendix G: Computer Desktop 1.1.1

See attached file: desktop-1.1.1.jpg

## Appendix H: Digital Evidence Hash Table

|  |  |  |  |
| --- | --- | --- | --- |
| *Digital Evidence Description and Hash Table* | | | |
| *Description* | *Evidence No.* | *Filename* | *MD5 Hash* |
| *iMac-5 Memory Capture* | 1.2.0 | 24\_january\_2019\_memcap\_tests-iMac-5-evno-1-2-0.aff4 | ef4b5c1418ad2d2db8c0b0c485e20840 |
| *Workstation* | 1.1.0 | workstation-1.1.0.jpg | d4e389fd54a6ec9867e2ec5f7c690195 |
| *Computer Desktop* | 1.1.1 | desktop-1.1.1.jpg | d47af00d7e438d30dafb9ae0506ec27c |
| *Family Photo* | 1.1.2 | family-picture-1.1.2.jpg | ff2bd31bf17f2b79fd61ca68e27efb19 |
| *Kittens Photo* | 1.1.3 | kittens-1.1.3.jpg | 0db009274b6cef9002765cdb68c28e45 |

See also attached seizure-lab-hashes.chk for MD5 checksum validation file

## Appendix I: Document Description and Hash Table

|  |  |  |  |
| --- | --- | --- | --- |
| Document Description and Hash Table | | | |
| Description | Evidence No. | Filename | MD5 Hash |
| Evidence of Chain of Custody Tracking Form | 1.4.0 | evidence-of-chain-of-custody-tracking-form-1.4.0.pdf | 2bb5c939adecb6249921af99c27f2d11 |
| Consent to Search Electronic Media Form | 1.4.1. | conset-to-search-electronic-media-1.4.1.pdf | 9ceac6c0cbfbbdaf213b6a69bf5f4ef3 |
| Search Warrant | 1.4.2 | search-warrant-1.4.2.pdf | d837901ec913f31addb93b57c33f0d3e |
| Hand Written Notes | 1.4.3 | notes-1.4.3.pdf | 6cd5a711842e8887a05cf686893d652c |

See attached file seizure-lab-doc-hashes.chk MD5 checksum validation file

## Appendix J: Devices Evidence Table

|  |  |  |  |
| --- | --- | --- | --- |
| Device Description and Serial Number Table | | | |
| Description | Evidence No. | Serial Number | Quantity |
| iMac 5 24-Inch; Early 2008; | 1.0.0 | QP220NWZE7 | 1 |
| Generic HP Keyboard | 1.0.1 | - | 1 |
| Generic HP Optical Mouse | 1.0.2 | - | 1 |
| SanDisk Cruzer Glide 3.0 256GB; USB drive | 1.0.3 | BQ171225913B | 1 |
| SanDisk USB Flair USB 3.0 16GB; USB drive | 1.0.4 | MSIP-REM-TAD-SDCZ73 | 1 |

## Appendix K: Investigator Dane Morgan CV

See attached file: DANE\_MORGAN\_ResumeSep2018.pdf

## Appendix L: Investigator Aaron Cowley CV

See attached file: AARON\_COWLEY\_Resume.pdf