

Crime Scene Investigation report

Jason Rodriguez

Champlain college

CFDI-240-45

Digital Forensics Investigation Techniques

Crime Scene Investigation report

Introduction

On August 1, 2018, at approximately 6:00 am, police responded to a call at 7521 River Parkway. Arnold Harding a white Caucasian of 45 of age at the time of deceased from a gunshot wound at his place of business. Detective Martin contacted me at approximately 8:30 am describing that the medical examiner Dr. Brain who performed the autopsy had found a thumb drive on the victims right front pocket. He later submitted the thumb drive to the forensic laboratory for fingerprint and DNA analysis. The laboratory technician PDK#1234 provided a forensic copy of the thumb drive on a DVD. The DVD label read the .dd file

MD5: 95b28650816b0e06c07b5f0aae59f60f

Detective Martin obtained a search warrant from the court to obtain the USB thumb drive found on the victim's right front pocket, cell phone found next to the victim and a computer that was powered off at the scene.

Observations at the scene

Environmental conditions at the scene: Ambient exterior temperature approximately 80°F, interior temperature approximately 75°F. It is a small building painted white with a small sign on top that reads Harding Enterprises. I was directed through the main door of the office which had the window shade still closed, but all the lights in the office were on. With just to computers in the office it is a small business that looks like an E-commerce business. I spoke to the initial officer responder, and he states that nothing in the scene has been moved, contaminated and that the scene is properly secure.

Actions at the scene

First Evidence: Dell 780 desktop computer

To obtain the Dell 780 volatile memory I proceeded with this steps:

1. I first took a picture of the computer from the front as well as from the back. As well as anything displayed on the monitor.
2. I disconnected the computer from its network.
3. I made sure the computer had stable power.
4. I mounted an external drive consisting of the memory module.
5. Executed the FTK Imager lite on the host machine.
6. Goto File >Capture memory and enter the memory capturing module. Enter the destination location.
 - FTK also acquire the system RAM dump and the pagefile.sys
 - The AD1 image file contains the memory dump and pagefile
 - FTK also created MD5 checksum hashes and stored the acquisition starting as well as the ending time.
7. Next, I acquire the Hiberfil.sys as well as the Swapfile.sys from the local disk storage.

After gathering all the volatile data I proceeded with unplugging the power cord from the back tower, I diagram all the cords as well as lace labels on them. I documented all of its parts by writing down the model number as well as serial number. I then disconnected all the cords, package all components (using anti-static evidence bags). I made sure to keep all the components from any magnets, radio transmitters. Finally, I documented all my steps in the seizure and transported all the evidence back to the lab for further analyzing.

Samsung Galaxy S8+



Samsung Galaxy S8+

IMEI:355979080525824

Samsung Galaxy S8+ color black with a Samsung cover on the back. I initiated by taking pictures of the device of the front as well as the back as well as the home screen. I notice the cell phone was still on and proceeded to turn off the mobile. I couldn't remove the battery because it's built-in on the device, I then check to see if the sim card was still in place, I removed it. I placed the mobile phone in a Faraday bag. I then placed my mobile device on an evidence bag. Where then I transported to a lab.

Recommendations



Next step in analyzing the evidence is to make sure the MD5 hash is the same from the report and make sure it hasn't been tamper with in any way. Because the search warrant has a time deadline, it is crucial to analyze the image gather from the hard drive. I will conduct this by utilizing FTK imager and Autopsy to analyze the evidence.

I will also clone the sim card of the mobile phone with a tool name: Mobiledit forensic.

Another evidence in which I did not collect was a USB thumb drive found on the victim front right pocket. Detective Martin provided me with a DVD copy of the thumb drive. The label read .dd and also included the hash value and the technician ID who perform the copy.

Appendices

Crime Scene Investigation report5

 Evidence Item Recovery Log	Incident #: 0001	
---	------------------	---

Item #	Description	Recovered By	Date/Time
1	Dell 780 Desktop computer	Jason	Aug1/9:55a
2	Samsung Galaxy S8+	Jason	Aug1/10:00a
3	USB Thumb Drive	Jason	Aug1/10:09a

AFFIDAVIT FOR SEARCH WARRANT

Commonwealth of Virginia V.A. CODE § 19.2-54

The undersigned Applicant states under oath:

1. A search is requested in relation to ☐ an offense substantially described as follows:
☐ a person to be arrested for whom a warrant or process for arrest has been issued identified as follows:

Violation of FL state code 782.04, robbery

☐ CONTINUED ON ATTACHED SHEET

2. The place, person or thing to be searched is described as follows:

The residence of Arnold Harding and Lilian Harding located in 7521 River Parkway.

☐ CONTINUED ON ATTACHED SHEET

3. The things or persons to be searched for are described as follows:

Any cell phones, telephone logs, computers, emails, data, media storage devices, zip drives, dvd's, cd's or any electronic data of the aforementioned devices showing a means, motive, opportunity for the related crime and the relationship between suspect and the victim.

☐ CONTINUED ON ATTACHED SHEET

(OVER)

FORM DC-338 (MASTER, PAGE ONE OF TWO) 07/17

FILE NO.
AFFIDAVIT FOR SEARCH WARRANT
APPLICANT:
Martin
NAME
Detective
TITLE (IF ANY)
6130 Sunset Drive
ADDRESS
Miami, FL 33143
Certified to Clerk of
Circuit Court
CITY OR COUNTY
ON DATE
TITLE SIGNATURE
Original Delivered <input type="checkbox"/> in person <input type="checkbox"/> by certified mail <input type="checkbox"/> by electronically transmitted facsimile <input type="checkbox"/> by use of filing/security procedures defined in the Uniform Electronic Transactions Act
to Clerk of Circuit Court
CITY OR COUNTY WHERE EXECUTED
ON DATE
TITLE SIGNATURE

References

Henry, P. (2009, September 12). SANS Digital Forensics and Incident Response Blog. Retrieved

from

<https://digital-forensics.sans.org/blog/2009/09/12/best-practices-in-digital-evidence-colle>

[ction/](https://digital-forensics.sans.org/blog/2009/09/12/best-practices-in-digital-evidence-colle)

Warrington, D. (2016, June 14). Crime Scene Documentation: Start to Finish. Retrieved

from <https://www.forensicmag.com/article/2016/02/crime-scene-documentation-start-finish>