CSCI-6638-01, Small-Scale Digital Forensic Science

**Applying the Digital Forensics Methodology**

September 13, 2023

TC

Table of Contents

[Intake 4](#_Toc145500668)

[Forms 4](#_Toc145500669)

[Identification 4](#_Toc145500670)

[Preparation 6](#_Toc145500671)

[Isolation 6](#_Toc145500672)

[Processing 6](#_Toc145500673)

[Verification 7](#_Toc145500674)

[Documenting/Reporting 7](#_Toc145500675)

[Presentation 8](#_Toc145500676)

[Archiving 8](#_Toc145500677)

Intake

* Fill out a request for processing form to begin the investigation by first receiving Kohberger and the victims’ devices requesting phones and IoT devices that were located at the crime scene.
* Reason: To begin the DF investigation, you must request the phones and other items associated with the crime and anything that could prove that Kohberger was there.

Forms

* Once the request form is fulfilled and I have access to the users phones and IoT devices I would begin with the chain of custody this would include documenting who collected it, how it was collected, where it was collected, who has taken possession of these items, at what time the possession was transferred, how was it stored and protected, and lastly who took it out of storage and why.
* Reason: The reason for the importance of this is insurance policy for the person who take the data and the sanctity of the data more specifically the validity of the data to be held up in court as in order to be admissible evidence it needs to be well documented everything that has happened to this device in question to assure that the most upmost care was taken and no digital information was tampered with or corrupted in any way.
* Specifically there are multiple things that are required for this to be used as evidence in the case it must be related to the incident in a relevant way, there must be enough data to describe the entire story or provide the missing details of the main story in this case to prove that Kohberger was at the victims residency, and lastly it must be Believable particularly easy to understand and have the jury be able to make a well-educated decision as well
* Reason: This is very important as this will determine the validity of the evidence in court and if it even is admissible as evidence, you need a proper chain of custody document to ensure the Integrity of the data. If these requirements are met, you can pass the information and evidence you find on the phone to the court.

Identification

Case Type/Legal Authority:

* For this case it would be digital information recovery (not sure the proper terms for the case)
* After This determine the amount of authority that was permitted to access the information in this case since it was required to search through Kohberger’s phone and the victims IoT devices with the instruction to prove that Kohberger was in fact there I would assume that this information should be proven by going through the phones and devices and nothing else in order to prove that Kohberger was in fact at the crime scene.
* Reason: The reason for these two items is one to clarify exactly what you are searching and ensure that no legal repercussions can be enacted on you for going over the boundary of investigation or just ensuring that you only process the required items that have been provided. Identifying the Case type will also help to show what tools to use or a good starting point for this type of case and what to look for.
* Examination Goals
* The defined set of goals specifically search through Kohbergers phone and the victims IoT devices in order to prove that Kohberger was In fact there at the scene of the crime and find evidence that is admissible in court from the devices provided.
* Reason: Always define the goals so that way you can save as much time as possible when conducting the investigation and ensure that you are able to investigate efficiently and ensure a clear and concise pathway to your goal for the device

Device Specifications

* This would involve taking down everything that was given over to myself and would be placed in the chain of custody information as well I presume. To identify each of the devices, for this scenario it would be noted each of the devices Manufacturers, specifications, Operating System, How much and what type of storage is used, and lastly anything that can identify the device such as marks scratches.

Reason: This will aid in the research aspect as knowing this information will help speed up the tool selection process and narrow down the best tools for the job.

Any external drives or storage

* It is worthwhile to take note of the type of storage that is being used, whether it is NAND Flash memory (the technology used in SSD technology) Hard Disk Drive (HDD) or USB/External Disks
* For this investigation Kohberger’s phone was an iPhone device, this uses flash memory or SSD technology this will make it easy to generate a forensic image later as we can determine what type of read write blocker to use and what settings to set the forensics tools to

Organizational Impact

* The organization in this case would be the families of the victims and how they would be impacted is emotionally and with the evidence found in the phone.

Preparation

* Consideration of the device to be examined for the purpose of this investigation the devices under investigation will be. For this stage the proper procedures taken would involve one identifying the software and the programs to be used, how the forensics workstation will be maintained and created, and lastly taking into consideration the devices to be analyzed.
* The use of SATA Read Write Blockers to plug into examiners computer to block any data being written to the forensic investigator’s computer and aligning/setting up mobile image extraction and the proper cabling to be used for mobile device image extractions’
* Preparing the proper environment besides the physical setup is vital as well, for this I will be utilizing a virtual box and a virtual windows 10 machine this will be marked as well as the computer specifications. This environment has been set up to have autopsy, forensic toolkit, Nmap, Wireshark, pwdump7, and Belkasoft.
* Reason: With the forensic software and physical deployment properly setup it allows for the proper safety precautions to be taken physically and since this is in a virtual machine/ environment it allows for the safety of the software as well. Along with that having all the software preinstalled into a virtual environment allows for quicker assessment.

Isolation

* Isolation of Kohbergers iPhone and the speaker in question that was connected to or the IoT device. These will be then placed individually into faraday bags to negate the Signal to Noise ratio interference/EMAG Interference or any radio frequency communication frequency tampering. This will ensure the validity and integrity of the data being gathered. Once this is bagged access to this or any other permitted person but if someone else partakes in the investigation before anything occurs on the device or they touch the device it will be noted on the chain of custody the date, time, and what was done/accessed.
* Reason: This will help in case someone wants to tamper with the device or locate the device. This will also protect against further attacks as when placed in a faraday bag it is entirely cut off form the internet and everything surrounding it and thus ensures that the isntegrity of the data is preserved.

Processing

* Before the processing ensure that there are copies of the evidence two is one and one is none. Remember to also keep in mind the goal of the examination and implement the proper tools that will be used for this specific task.
* The tools to be used for image extraction will be Forensic Tool Kit and Autopsy. Once the mobile device image is extracted autopsy will be used to upload the image and then compile all documents and logs recorded within the phone to be searched through for evidence pertaining to the case. In this sense Wi-Fi and Bluetooth traffic logs are to be analyzed for any sign of a connection between the phone and the Bluetooth device.
* Reason: Since we are trying to prove digitally that Kohberger was at the crime scene since the speaker (IoT Device) will automatically connect to devices within range that have been previously connected. Along with the range of Bluetooth based devices operating at 3Ghz this high frequency cannot travel far distances, only allowing for 10 meters. Due to the walls, doors, and rooms of the environment of the speaker Kohberger would have to be on the premises to connect to the speaker.
* Remind self about what is needed and what is necessary and once the information is proved and securely stored on a flash drive or any other format. The only other move should be to analyze the speaker device and download the generated logs of the Bluetooth device and ensure that the handshake between Kohbergers phone and the speaker took place from the speakers end as well also proving the validity of the data from two standpoints.

Verification

* Once proper data is extracted, the test to ensure its validity and integrity was not compromised accomplishing this through hash code verification and analyzing the hex code to ensure data integrity. This will be done through comparing the data extracted with the analyzed copy of the mobile device image and ensuring hash codes and hex codes are verified to be the exact same to ensure nothing has been tampered with.
* Reason: This is of the most upmost importance if you cannot prove the data’s validity and integrity it is not surmisable in court and cannot be used as evidence. With the data verification this will ensure it can be used to help the case and complete the task assigned.

Documenting/Reporting

* This will entail a detailed description of every action taken on the device, such as when the device was plugged into the workstation, the exact specifications of the workstation used such as storage, manufacturers, and the workstations operating system.
* Reason: So other investigators or people look at the documentation they know exactly what I was working with just in case something goes bad, and the need arises to determine what the cause of the hiccup could have been.
* Next move onto the devices that were gathered from the crime scene and begin documenting the physical condition of all the devices received, along with the make, model, and lastly taking pictures of the devices to be analyzed. Along with this the state in which the device was given such as ON/OFF and whether it is connected to the internet.
* Reason: In case something happens to the phone the original state can be verified to ensure that something in fact did change with the device being accessed.
* Following the table of the tools being used along with the data analyzed, acquired, and tagged for potential evidence and evidence alike.

Presentation

* Report format that follows normal procedures for presenting digital forensic works such as title page, table of contents, executive summary, apparatus, methodology, procedure, problem solving and troubleshooting, conclusion, and final remarks, and lastly references.
* Reason: With this lab report format I will be able to show and demonstrate everything that was done in the digital investigation in a clean and concise format.
* Along with this it will be in an electronic and printed out to be handed out so that other people on the case may mark it up and down and make their own notes on the paper. This is also useful for the intended audience of this report as it is geared to not go too in depth on the technical details as the experience of everyone in this subject is limited. Keep it clear and concise while showing the evidence and demonstrating its integrity to be used in court either to lawyer, jury, or judge.

Archiving

* It is important to keep good track of the forensic image, data associated with the investigation and all documentation and other things organized and archived properly. To ensure this, the lab report will be saved as a pdf electronically and stored somewhere secure whether on the cloud or on a secure external drive physically protected as well with other evidence.