Assignment 2

[CCJS 321 6981 Digital Forensics in the C](about:blank)riminal Justice System

Reece Hugo Zunino

10 July 2022

A search warrant is a warrant signed by a judge or a magistrate that authorizes law enforcement officials to search your home or business, including any property listed on the warrant. This warrant gives law enforcement the legal ability to obtain evidence they believe necessary to charge you or other individuals with a crime or even prove your innocence in the matter they are investigating. When filling out a search warrant, the officer must also support that evidence of illegality will or could be found in the areas they are trying to search (Cornell Law School, 2022).

A search warrant is necessary to protect the individual being searched and the officers involved in the investigation. If any officer searched your home without a warrant, the evidence would be non-admissible in a court of law since it wasn't obtained legally. The only contrary to this would be an exigent circumstance. Exigent circumstance allows officers to in certain situations where people or persons are in immediate threat, the possibility of evidence being destroyed, or to prevent a suspect from escaping the scene of a crime (Cornell Law School, 2017). If a search warrant is obtained through proper channels and is signed off by a judge or magistrate, the officers involved could be charged with violating your 4th amendment rights.

A search warrant to obtain digital evidence is similar to a typical search warrant but more specific to what is being seized in the search. When it comes to electronic devices or digitally stored media being captured, the warrant should focus on the relevant files more than the physical devices that are being seized by law enforcement (LAW ENFORCEMENT CYBER CENTER, 2018).

The three items that hold digital information or media I would like to discuss are laptops, USB memory sticks, and cellphones. A laptop is a mobile personal computer system capable of storing copious amounts of data depending on how it is built and configured, anything from email messages to full-length videos. The laptop would also give the investigators access to any email accounts saved on the devices, any protected financial information, internet browsing history, and the list. A laptop or any computer system can be extremely valuable in an investigation when intact and accessible. The data in a computer can be found anywhere, and the data you are looking for could be in raw files, software, and even within the apps on the laptop.

When it comes to acquiring a laptop during an investigation, you have to follow the step in basic forensics and more for the digital side. When arriving at the scene, I would ensure that you document where the laptop was found and take lots of notes and photos of how it was found and its state. You need to take different routes based on whether the laptop is on or not. If you want to leave the laptop off, do not power it back on. If the computer is on, photograph the screen before packaging the laptop. When handling the laptop, I would ensure to stay away from any magnets or areas that could potentially damage the laptop or risk the integrity of the information on the device. When it comes to packaging materials, make sure that all digital evidence is in antistatic packaging. Only paper bags, envelopes, cardboard boxes, and antistatic containers should be used to package digital evidence.

You should never use plastic materials when collecting digital evidence because plastics can produce or convey static electricity and allow humidity and condensation to develop, damaging or destroying the evidence (Gilbert Police Department, 2010). If I were the site examiner, I would consider making a volatile memory acquisition so that any information on the RAM can be saved before the device losses power or is turned off. After going through the steps of documenting the scene and noting everything, I can package it into a box marked fragile. If available, use a faraday bag around the laptop so that it cannot be manipulated remotely by an outside entity. I would make sure that all evidence collected was labeled correctly. I would then look for any instruction manuals or like items or devices with the laptop, such as peripheral devices, and make sure they are packaged into evidence bags. I would note in detail on the chain of custody form all necessary information that is needed to ensure the integrity of the evidence.

A USB memory stick, also known as a thumb drive or removable media, is small and light and can be hidden anywhere you can imagine. These days there are USB drives that can hold up to 4TB of data, that's as much as some home computers. This information isn't always readily accessible without a computer. Still, it is a good way for those trying to hide their information or pass on it without sending it digitally. The information stored on this external device is software, emails, applications, digital media chat logs, and more. However, most of these devices have an event log that can be very valuable during the investigation and prosecution.

A USB memory stick would follow the same basic principles as the laptop. You would document where the item was found and take plenty of pictures of the state of the thing and how it was found. When handling the USB, you would also want to take the same precautions as the laptop to ensure the integrity of the information stays intact before packaging. Once the scene has been documented, I would place the USB memory stick into a faraday bag and ensure that it is appropriately labeled and tagged as digital evidence. I would also follow the same steps and guidelines of the chain of custody form to ensure the integrity of the evidence while being transported.

A cellphone is a treasure trove of digital evidence if kept intact and accessible. These days a cellphone stores a person's whole life in the palm of their hand. The information that can be stored on a smartphone and even some older cellphones are valuable. Access to a person's financial information, location data of cellphone towers they have been in the vicinity of, GPS data of their locations, emails, phone calls, text messages, and even encrypted messages from certain messaging apps and the list is seldom ending when it comes to smartphones. Almost everyone has a smartphone these days, and having evidence and access to it can help an investigation tremendously when trying to accumulate data against the person who committed the illegal act.

When it comes to living vs. dead data acquisition, Live acquisition is when an investigator receives a powered system, and the information can be easily accessed and altered. With a live system, a lot more valuable data can be retrieved from the system. Still, the investigator has to decide if they want to make a volatile memory acquisition to the system's RAM before shutting it down. From there, you would eventually use the tools available to place the system into a read-only mode and attach external memory devices to capture the device's image for the data acquisition (Kolhe & Ahirao, 2017).

When handling a dead system or a system that has been powered off, there is still information that can be retrieved off the system similarly. However, you won't be able to recover all the data, especially the data on the system's RAM, since it purges all memory once it has more power. When collecting the data of a dead system, you must capture all the data stored on the device, including the metadata and the unallocated space(Kolhe & Ahirao, 2017).

References

Cornell Law School. (2017, June). Fourth Amendment. LII / Legal Information Institute. https://www.law.cornell.edu/wex/fourth\_amendment

Cornell Law School. (2022, May). Search warrant. LII / Legal Information Institute. https://www.law.cornell.edu/wex/search\_warrant

Gilbert Police Department. (2010, July 26). Electronic Evidence Collection and Preservation. Town of Gilbert, Arizona. https://www.gilbertaz.gov/Home/ShowDocument?id=13765

Kolhe, M., & Ahirao, P. (2017). Live Vs Dead Computer Forensic Image Acquisition. INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGIES. https://ijcsit.com/docs/Volume%208/vol8issue3/ijcsit2017080331.pdf

LAW ENFORCEMENT CYBER CENTER. (2018, September 13). Digital search warrants. Law Enforcement Cyber Center. https://www.iacpcybercenter.org/prosecutors/digital-search-warrants/#:~:text=A%20search%20warrant%20may%20be,an%20instrumentality%20of%20a%20crime

Mahalik, H. (2021, March 3). How to lawfully collect, examine and analyze data from computers. News | On the Scene and in the Lab - Forensic®. https://www.forensicmag.com/3425-Featured-Article-List/573794-How-to-Lawfully-Collect-Examine-and-Analyze-Data-from-Computers/

US Secret Service. (n.d.). Best Practices for Seizing Electronic Evidence. www.cwagweb.org | CWAG Conference of Western Attorneys General. https://www.cwagweb.org/wp-content/uploads/2018/05/BestPracticesforSeizingElectronicEvidence.pdf