Assignment 1

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

Reece Hugo Zunino

28 June 2022

**Question 1.**

The three locations where data can be stored are internal storage, external storage, and cloud storage. Local storage is what is available within the device a user is using. This data is also available for offline use since the information is stored locally on the device. This is also known as direct data storage; This includes mechanical hard drives, solid-state drives(SSD), CD drives, flash drives, and any other physical drive attached internally to the device. The most common devices found for internal storage are mechanical hard drives and SSDs.

SSDs are the most popular form of disk drives and commonly have faster read and write speeds which means that these devices can store and access information much more quickly than their mechanical counterpart. However, they can malfunction just as easily as hard drives. They can wear out over time and are susceptible to external damage like spilling a liquid over it or physical damage like dropping the device. Some more of the cons of the SSD is that it can be more expensive than standard hard drives. SSDs are also more challenging to recover data if the drive malfunctions or becomes damaged. When it comes to hard drives, they have mechanical parts that tend to wear out more quickly than SSDs. With standard hard drives, you tend to have more storage space and are cheaper than SSDs (Kline, 2021).

External storage usually consists of USB drives, CDs, and external hard drives. These storage devices can be peripherally connected to the primary device. Some of the issues with using these devices are they can be lost or broken since they are not safe within the case and protected from an outside force. The information on these devices is portable but not always accessible (CDW, 2022).

Cloud storage is the next location where data can be stored. This storage location can only be accessed via the internet or network, and companies or government agencies commonly use cloud storage. Cloud storage can be accessed from any device connected to the internet or network that is allowed access to the servers. However, the data cannot be accessed if the user has no internet or access to the network.

**Question 2.**

Hashing data is passing data through a formula and producing a result. When the information is sent through the decryption formula, whether a string of text, file, or storage media, it will give that information a hash value, which is unique to that information sent through the formula, like DNA. This means that the same input will always produce the same output regarding the hash value given to that information (Forensics Digest, 2021).

Two types of hash values are typically used in discovery for data forensics. Message-Digest algorithm 5 (MD5 Hash) and Secure Hash Algorithm 1 (SHA-1). The file format does matter when using the algorithm to generate the hash values, and the same content will have different values based on the file format, whether a PDF file or a word document (Zola, 2021).

The primary way hash values are used is through evidence authentication. Since the hash value is used as the file's fingerprint/DNA, it represents its authenticity. If a file has been run through the algorithm and was given a specific hash value, but later that hash value was changed will show that the file has been tampered with (Forensic Discovery, 2021).

**Question 3**

A digital forensics analyst can find lost files in the recovery sectors of a storage device within an electronic device. Most investigations start with an investigator searching a computer for files belonging to the device's previous user. It is not easy to underestimate the value of digital forensics. Many different types of digital evidence can be found within electronic devices during an investigation; however, there is only one place these files are stored, and this is where they need to be extracted. Digital forensics experts need the knowledge and experience to be able to perform an extraction of this information from these devices (Gubanov, 2019).

Digital forensics experts rely on a specific set of tools and techniques. These tools and techniques can help identify devices found at the scene of crimes or during other investigations to help out victims, suspects, and bystanders involved with the crime or incident. When it comes to an analyst, there needs to be a basic understanding of how information is stored on electronic devices. Understanding these inner workings of the electronic devices is key to how data is recovered accurately and having the ability to retain that information during the extraction (Garfinkel, 2017).

Allocated files are files that, under normal circumstances, will not be overwritten by the computer's operating system. Allocated means the sectors where files are typically stored on a system's hard drive. These sectors are where these particular files are, and no other files cannot be assigned to the same sectors (Garfinkel, 2017).

When it comes to cyber law and the 4th Amendment, the analyst usually does not need to worry about violating these because they will not start an extraction or procedure until the authorities have given them the order with the proper documentation. As long as there is a search warrant for the analyst to be able to search the electronic device given to him, he should be free and clear of all liability (Law Enforcement Cyber Center, 2018).

When it comes to the time that an examiner has to extract evidence from a device, the courts have said that, unlike the search warrant that gives typically investigators ten days to execute the warrant, digital forensics experts have what they call reasonable time for them to be able to extract the information from the device instead of a specific period (Law Enforcement Cyber Center, 2018).

**Question 4**

The three laws that come to mind regarding digital and computer crimes are the Computer fraud and abuse act(CFAA), the Children's online privacy Protection Act(COPPA), and the Electronic Communications Privacy Act(ECPA).

The CFAA was enacted in 1986 and is one of the founding laws for cyber crimes. The CFAA has been amended over the years, most recently in 2008. The CFAA prohibits intentionally accessing a computer without authorization or more approval than is necessary for one to have access to a network or device. The computer fraud and abuse act, however, the act does not clarify what "without authorization" means (National Association of Criminal Defense Lawyers, n.d.). The CFAA gives a basis for all minimum sentences for each crime covered by the act under the amendments.

The COPPA was enacted in 1998 and was set forth to keep the information of children under the age of 13 safe from criminal activity and sets the standard and guidelines for websites to follow. It imposes specific requirements on companies of online services or websites directed towards children under 13 years of age and on company managers of these websites or services that have actual knowledge that they are collecting personal information online from a child under 13 years of age (Federal Trade Commission, 2020).

The Electronic Communications Privacy Act, commonly known as the ECPA, was enacted in 1998 to revise the federal wiretapping and electronic eavesdropping provisions. The ECPA also included amendments to the Wiretap Act, created the Stored Communications Act, and created the Pen Register Act. Individuals who violate the ECPA could serve up to 5 years in prison and incur fines if any damages were incurred due to the violation (Electronic Privacy Information Center, n.d.).

References

Bureau of Justice Assistance. (n.d.). *Electronic Communications Privacy Act of 1986 (ECPA)*. [https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285](about:blank)

CDW. (2022). *What is data storage? - Data storage types & attributes | CDW*. Welcome to CDW. [https://www.cdw.com/content/cdw/en/articles/datacenter/what-is-data-storage.html](about:blank)

Department of Justice. (2020, January 29). *9-48.000 - Computer Fraud and Abuse Act*. U.S. Department of Justice. [https://www.justice.gov/jm/jm-9-48000-computer-fraud](about:blank)

Electronic Privacy Information Center. (n.d.). *Electronic Communications Privacy Act (ECPA)*. EPIC – Electronic Privacy Information Center. [https://epic.org/ecpa/](about:blank)

Federal Trade Commission. (2020, December 1). *Children's online privacy protection rule ("COPPA")*. [https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa](about:blank)

Forensic Discovery. (2021, December 29). *Hash values are the DNA of digital evidence*. [https://forensicdiscovery.expert/hash-values-are-the-dna-of-digital-evidence/#:~:text=Just%20like%20law%20enforcement%20uses,the%20evidence%20in%20your%20case!](about:blank#:~:text=Just%20like%20law%20enforcement%20uses,the%20evidence%20in%20your%20case!)

Forensics Digest. (2021, February 20). *Hashing and data imaging*. [https://forensicsdigest.com/hashing-and-data-imaging/](about:blank)

Garfinkel, S. (2017, September 19). *Digital forensics*. American Scientist. [https://www.americanscientist.org/article/digital-forensics#:~:text=Forensics%20tools%20allow%20investigators%20to,damaged%20or%20are%20password%20protected](about:blank#:~:text=Forensics%20tools%20allow%20investigators%20to,damaged%20or%20are%20password%20protected)

Gubanov, Y. (2019, April 25). *Retrieving digital evidence: Methods, techniques and issues*. Forensic Focus. [https://www.forensicfocus.com/articles/retrieving-digital-evidence-methods-techniques-and-issues/](about:blank)

Kline, A. (2021, December 23). *A look at the differences between SSD and HDD*. Backblaze Blog | Cloud Storage & Cloud Backup. [https://www.backblaze.com/blog/hdd-versus-ssd-whats-the-diff/](about:blank)

Law Enforcement Cyber Center. (2018, September 13). *Digital search warrants*. [https://www.iacpcybercenter.org/prosecutors/digital-search-warrants/](about:blank)

National Association of Criminal Defense Lawyers. (n.d.). *Computer Fraud and Abuse Act (CFAA)*. NACDL - National Association of Criminal Defense Lawyers. [https://www.nacdl.org/Landing/ComputerFraudandAbuseAct](about:blank)

Zola, A. (2021, June 3). *What is hashing and how does it work?* SearchDataManagement. [https://www.techtarget.com/searchdatamanagement/definition/hashing](about:blank)