Assignment 3

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

Reece Hugo Zunino

July 25, 2022

Cloud storage is the modern way to store data accessible anywhere in the world via an internet connection. It is used to store all different types of data, from music to spreadsheets. Cloud storage works because it's a variety of digital services (essentially servers) that are stored in one or more locations and can be accessed via the internet. The cloud services users range from government to companies and even individual users. Cloud services are used for a variety of reasons. Some companies use it to streamline workflow and access the company's data to a person at home who is streaming a movie or TV show (Rembert, 2020). The Cloud works by data centers with large server networks physically storing the data that users or companies upload to it so that other users or companies can then download, work on, or stream that information live from that cloud storage center via their workstation, laptop or even their mobile device (Jethva, 2019).

Some of the challenges when it comes to Cloud based digital forensics is that different types of data can be collected. The data that can be obtained publicly, called "open source" data, can be obtained without a warrant because it can be seen and obtained publically. The other type of data is private data, and this data is usually found only on a cloud server and needs to be obtained via a warrant (Mahalik, 2021). There are many other challenges related to Cloud-based forensics. Other challenges include data integrity, decentralized data, deleted data, chain of custody, and data volatility, to name a few. Some of the solutions to these challenges can be simple or very complex. A key to decentralized data would be to obtain logs from the cloud service provider to determine where the data is stored, how it can be received, and even who uploaded and accessed that data. A solution for deleted information that is a challenging task would be utilizing information-cutting strategies (Arafat et al., 2017).

When protecting your data on your home computer, the first step would be to ensure that you have anti-virus software installed, like Norton or MacAfee. That would bolster the computer's defense and offense when it comes to intruders and the overall health of your computer. You should also ensure that all software on your computer stays up to date. This includes any apps on your computer and, most importantly, your operating system. There are always essential security updates and fixes that get pushed out over the life of your computer, and making sure it receives these fixes and updates helps ensure that any holes in the programs get fixed so that outside intruders aren't able to use them to their advantage (Nick, 2022).

Suppose you use your home computer for both personal and work business. In that case, you should think about setting up two different user profiles to separate the information on your device. When setting up these other profiles, ensure that you do not sync the information between the profiles or that sensitive work data could bleed over to your profile. One primary step you can and should take in securing your computer should be to encrypt your files. This option is available on most computers and can be toggled on through the device's settings (Nick, 2022). You should also always, if possible, back up your data. Programs like Norton offer a service that automatically backs up your device to their cloud network and can sync your data daily if set that way so that your information is always safe and secure off-site from your device. Finally, you should ensure your computer has a good firewall. Most programs like Norton already have this tool in tier program and manage your computer's firewall for you (Nick, 2022).

There are many ways digital forensics practitioner can display their ethical practices and understanding of ethics within their profession. However, there isn't currently a single governing body that gives digital forensics practitioners a code of ethics to go by. There is currently a draft drawn up by the Academy of Forensic Sciences, the Organization of Scientific Area Committee, and the National Institute of Standards and Technology that sets a code of ethics for the industry. Hopefully, one day will be the governing code for the profession (Crimmins, 2017). One way a practitioner can display their ethics is through their work. Ensuring the collected evidence is done legally and truthfully so that no evidence can be found illegitimate and thrown out of court due to bad practices or malicious intent on behalf of the practitioner. Another way digital forensics practitioner can show their ethics within their profession is through their knowledge. A digital forensics practitioners should stay current on current practices within their career and continue their education (NATIONAL COMMISSION ON FORENSIC SCIENCE, n.d.). They should also remain consistent in their training and certifications to ensure they align with the profession's norms. A final way a digital forensics practitioner can show their ethics through their work is to avoid participation in any case that would put them in a position where they would have a personal interest in the case. Personal interest in a case could lead to the defendant's attorney having evidence thrown out due to possible integrity issues. It is always best to avoid investigating places you are employed, invested in, or could have some personal gain in the investigation.

References

Arafat, Y., Mondal, B., & Rani, S. (2017, August). *Technical Challenges of Cloud Forensics and Suggested Solutions*. Menlo Security. [https://safe.menlosecurity.com/doc/docview/viewer/docN83ED197C5F6D32863d230322625e0a9454457b5409cb19d050ed3d3845157fa10687d7bfece2](about:blank)

Crimmins, D. M. (2017, May 16). *Development of a professional code of ethics in digital forensics. Scholarly Commons*. Menlo Security. [https://safe.menlosecurity.com/doc/docview/viewer/docN83ED197C5F6De76b76abdce6d317b73333426b418c018552ae98575948d19c001010f9c26d72](about:blank)

Imam, F. (2020, October 28). *Computer forensics: Legal and ethical principles*. Infosec Resources. [https://resources.infosecinstitute.com/topic/computer-forensics-legal-ethical-principles/](about:blank)

Jethva, H. (2019, October 22). *What is cloud storage and how does it work?* Alibaba Cloud Community. [https://www.alibabacloud.com/blog/what-is-cloud-storage-and-how-does-it-work\_595461](about:blank)

Mahalik, H. (2021, May 7). *How to lawfully collect and examine data in the Cloud*. News | On the Scene and in the Lab - Forensic®. [https://www.forensicmag.com/3425-Featured-Article-List/575758-How-to-Lawfully-Collect-and-Examine-Data-in-the-Cloud/](about:blank)

NATIONAL COMMISSION ON FORENSIC SCIENCE. (n.d.). *National Code of Ethics and Professional Responsibility for the Forensic Sciences*. U.S. Department of Justice. [https://www.justice.gov/archives/ncfs/page/file/788576/download](about:blank)

Nick, E. (2022, April 26). *How to protect your computer data*. Data Science Central. [https://www.datasciencecentral.com/how-to-protect-your-computer-data/](about:blank)

Rembert, L. (2020, February 28). *How the Cloud complicates the digital crime scene*. Infosecurity Magazine. [https://www.infosecurity-magazine.com/opinions/cloud-complicates-digital-crime/](about:blank)