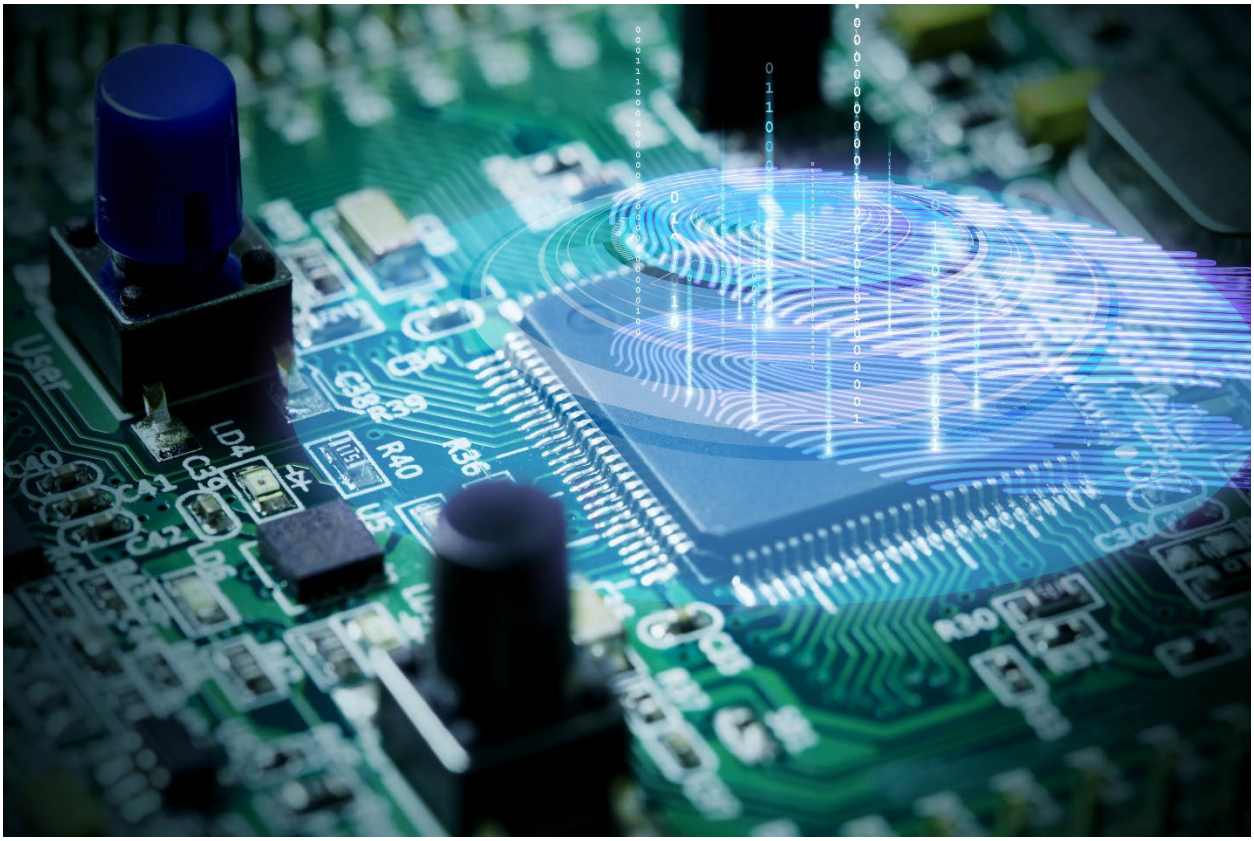
CSS350 Computer Forensics I



Forensics Research Report on “Murder by Text”

Joshua Powell

16OCT2022

Contents

Electronic Evidence and Crime

Digital Evidence Used

1. Taped recordings of taps (Kushner, 2011)
2. 1.4 billion pages of paper evidence including Facebook and MSN messages. Text messages, and chat histories of Cam and Kruse (Kushner, 2011)
3. Search History of Cam and Kruse (Kushner, 2011)

How Evidence was Acquired

The evidence acquired in Kimberly's murder was not acquired immediately. They started off assessing the evidence at hand. They had search parties out looking for her and a pot head smoking his daily fix stumbled across burnt remains. Due to the state of the body, they ended up having to rely on dental records. From the dental records, they were able to confirm that it was indeed Kimberly's remains that were found. The investigators started off monitoring the social media sites where the friends and family created support pages

for Kimberly's family and friends. This was to no avail. The investigators were able to acquire a court order to monitor Kruse and Cameron, however, whether it is to keep the public from knowing or just to keep it private it is not clear as to how they acquired this judicial authorization other than they had enough evidence to acquire it. This may have been from someone who pointed them in their direction and to protect that person from the scrutiny they left it out of public knowledge as there were a few who knew of their actions. After getting the court order they were able to monitor the two and acquire 1.4 billion pages of paper evidence through Facebook and MSN messages, text messages, and chat histories. This also included their search histories and all they had been doing on the internet with porn sites and such (Kushner, 2011)

Analyzing of the Data

The data acquired were analyzed and sifted through. The investigators found that in their analysis of the data Kruse and Cameron were feeding off each other's desires. The two had been going through and looking into dark porn that consisted of rape, gagging, and mutilating the victims. They also found that through their search history the two were looking for places to dump a body through google maps so that it would go unnoticed. The evidence became overwhelming, and they were able to get a warrant for Kruse and Cameron's arrest (Roberts, 2011)

The Crime Scene

Crucial electronic evidence for this case.

The most crucial evidence in this case was the messages between the two of them on MSN and Facebook due to the ill decision from either thinking they were secure from being found. It was found also during the investigation that Kruse's father was convicted of sexually assaulting a 16-year-old female and that Kruse had bragged about in a blog of having all the characteristics of a serial killer. Both boys Kruse and Cameron both conversed between each other about certain topics pertaining to the dark porn they were watching. This consisted of them both fantasizing about committing such acts in real time and how they would carry them out. They started figuring out the best way to commit such an act. Their first and only victim ended up being Kimmy a female friend of theirs. This friendship started with Kruse and Cameron becoming a sort of brotherly friendship in that they both yearned for the darker side of sexual activity and Fed off each other. Kruse was the leader of the two and Cameron followed along with Kruse. When Kimmy was transferred to Pacific Secondary after being ridiculed and picked on at her current school do to ADHD and lack of attention in class. It was at Pacific Secondary that Kimmy met both Kruse and Cam and they hit off as good friends. Where cam developed a liking for Kimmy, but Kimmy who had recently broken up wanted Kruse Instead. They all ended up trading messages on up until ultimately leading to Kimmy's Untimely death (Robert, 2011).

How the police obtained the electronic evidence.

The police obtained the evidence in this case first was a body that they could not ID due to the burning of the body they only knew that It was human remains. They then ran the victim's dental structure against a database of digital dental prints. It was found the burnt body found was indeed Kimmy's body. From there the police through tactics not stated for public consumption were able to acquire enough evidence to bring both cam and Kruse in for questioning. After the questioning, there was evidence given that the police were able to get a court order to monitor and get records on the two boys. From there the police were able to gather 1.4 billion pages of digital footprints that both boys left through their Facebooks and MSN's. It was from this information that the cops were finally able to arrange an arrest and apprehend the two perpetrators. (Roberts, 2011).

The electronic crime scene is in this case.

The electronic crime scene is vast for this criminal case and has an obscene amount of evidence pointing toward the two perps and their victim. This included the searching of dark porn sites and other dark categories of dark sexual pleasure. This ultimately led to Kruse and Carmon carrying out these acts on Kimmy leading to her death by suffocation after they raped, gagged, and committed other horrendous malicious acts on her (Roberts, 2011).

Electronic evidence you believe was admissible in court from this case.

The evidence I believe to be admissible in this case was the 1.4 billion pages they got from the social media sites that the two were using. This was a huge turnaround point for the case and rest assured sealed the fate of the two young perpetrators (Roberts, 2011)

Chain of Custody Concerns

What physical and electronic evidence can you as the investigator obtain?

So, in any case there are many factors that come into evidence being used. First off, the evidence must be admissible. This means that the evidence must either prove a fact or be in conjunction with the charges being placed on the defendant. There are also the details of the evidence obtained. What I mean is that there is a wide range of evidence that can be used, however it must pertain to the case. The evidence can be put into four categories; 1. Demonstrative, 2. Documentary, 3. Real Evidence, and 4. Testimonial. They all have their role to play in any case. Demonstrative evidence can be anything that shows or demonstrates a truth at issue in the case (1). Documentary Evidence is basically like it sounds, any documents that specifically pertain to the facts and issues within the case. Real Evidence is evidence such as the device used to break into the ATM that the defendant stole money from. Then there is testimonial evidence is when a person has an actual testimony before the court that pertains to the facts of the case.

Then there are two major sources of laws that dictate what is admissible and what is not admissible when it comes to electronic evidence. The first one is the Fourth Amendment. In accordance with the Fourth Amendment, Law Enforcement can obtain computers and other electronic evidence given they have a valid warrant. There are also cases that Law Enforcement can search a computer without a warrant and that is through permission by the owner of the computer. The next Source is Statutory Privacy Laws. This basically governs how and when electronically evidence can be obtained. Electronic Communications Privacy Act is one such law that regulates how law enforcement is permitted to obtain the following: stored account records

from network providers, Internet Service Providers (ISP), Telephone Companies, Cell phone service providers, and satellite service providers. Then there is the Patriot Act that expanded the power of law enforcement and gave them more ease when dealing with Electronically Stored Information (ESI) (LaMance, 2022).

How would you safeguard that evidence?

Safeguarding evidence starts before and it is apprehended. First and foremost, the investigator must inform the person in question of their rights. This will lead to either the defendant waiting on an attorney or the defendant giving the investigator what is they asked for without cohesion and they also must get a signature on a written document stating that they were not swayed to wave the rights in giving them the information without an attorney present. Another way to safeguard evidence is to adhere to the process of the chain of custody by making sure that the evidence is documented correctly. This means from the time the evidence is dated, coded, and bagged, to the conviction of the defendant. One of the key processes in ensuring the safeguarding of evidence is by keeping written records of the handling and movement of evidence, and who has access to it. It is not always possible but keeping the evidence out of as many hands as possible is ideal, as it ensures the less chance of the evidence being corrupted or messed with (Handling of Evidence —, n.d.).

How would you create a chain of custody for this evidence?

Creating a chain of custody should be mandatory and the best way to get the process started is using Custody forms. This way anyone who has access or needs access to the evidence has the proper clearance to see the evidence and fills out a custody form to document them getting the evidence. Another aspect to this is making sure the custody form is filled out properly ie: What is the evidence, a description of the evidence, name of person accessing this evidence,

employee ID number, their contact info and organization, date and time the evidence was gotten by the person, and any intermediaries who make take part in the evidence such as secretaries (Stride, 2017).

What are the limitations when protecting evidence only found online or in the cloud?

The issue we run into with evidence only online or in the cloud is the fact that it is challenging to preserve said data. The main issue here is that there are many different forms of digital evidence found online and in the cloud. This means that there must be practitioners that can go in a preserve and obtain this evidence to be able to keep and hold. Then we run into the issue of virtual machines being used by a lot of people. When it comes to criminal if they are using a virtual machine then the data can be deemed inadmissible due to its nature making it useless. So, it would behoove of us to make sure that we find tools and regulations that will back us up on virtual machines and cloud based as you cannot not take a server and run forensics on it like you used to and it takes a real extensive process to get this data. Not to mention ensure it is admissible in court as well (Lomer, 2016).

Digital Evidence and Admissibility

Spoliation

When it comes to criminal and civil cases Spoliation is when the other party i.e., the plaintiff or defendant have found that they have in some way shape or form messed with the evidence. What this means is that the party in question has in some way found that the opposing party has in some way shape or form intentionally or negligently withholding, hiding, alteration or destruction of evidence relevant to the legal proceedings. This could mean that during the proceedings it was found that for example the plaintiff knew that he had evidence that could have been used in the case that they destroyed evidence to avoid persecution from the evidence. One could say that even deleting a file after being found guilty of a digital crime could be considered grounds for spoliation (Keheley, n.d.). One example of a spoliation example is when in the 1980's Lt. Col. Oliver North deleted emails relating to the Iran-Contra affair (Keheley, n.d.). The issue yes is the fact that he deleted the emails, but also the fact that we all do things we think are right, but in turn that event alone could be the difference between an espionage charge or a felony depending on the circumstances. Given if he deleted them, they more than likely were incriminating, but if he knew he was caught and to save his behind he thought it better to delete them when it might have been better to work out a plea deal than to delete something that can be recovered.

Tampering

This is the most notorious as it comes up the most when it comes to cases involving digital evidence. The thing is with tampering it is when you are without a doubt guilty of tampering with evidence, whether it intentional or accidental. With tampering the courts have enough evidence to say that the party in question without a doubt had something to do with

altering the evidence whether it was to intentionally mislead the defendant or just out of pure accident which would in turn would dictate the severity of the offense. When it comes to tampering with evidence this could be as simple as changing a name on a digital document to photo shopping a photo of an event that did not take place. One thing to keep in mind in the world of digital evidence is given the right tools one could figure out whether evidence was tampered with, but that does not mean they will. There are several cases out there that were thrown out because one could not prove that the defendant had committed the act due to a lack of an IP address which could have been tampering but one cannot be sure, as it was never proven (Law, 2020).

Fruit of the poisonous tree

I know for me this type of evidence is like it sounds and comes from the bible version of eating from the tree that they were forbade from eating from. Much like the tree of knowledge and good and evil that was eaten from when it comes to evidence obtaining evidence without using the proper channels and jurisdiction one could wind up being in contempt themselves. One such way is obtaining evidence without the permission of the holder. Like let's say a person takes a video of a law enforcement officer doing something they should not. This does not give the law enforcement agent the right to take that person's phone. The law enforcement officer would first have to get approval from their first line leader and then proceed to get a warrant. Then and only then can a law enforcement agent take the alleged persons phone if there is just cause to do so. This could also be a situation where a First Responder responded to a call and found evidence at the scene but failed to document it and it was still used in the case against the

plaintiff. Which would render it fruit of the poisonous tree as it was not documented properly and thus makes it inadmissible in court (Fruit of the Poisonous Tree, n.d.).

Process for Evidence Used in Legal Proceedings

Collect electronic evidence

There are a lot of tools in existence to help get data from a hard drive on the scene so that way if anything happens one can make sure that they have the evidence at hand. One such way is through what is known as Forensic Cloning. This is where you take the hard drive and basically create a clone of the data present inside of it. This type of procedure is also referred to as a bit-stream image and it basically captures everything from the beginning to the end. It is not like a "copy and paste" you would perform from a hard drive to a jump drive, but all the active and latent data inside the hard drive. This is the best type of data imaging as it allows to catch of any data that may have been deleted by the criminal. This also allows hard drives in a business setting to be restored back to service and allows the investigators to go over the clone with a fine-tooth comb without interrupting the business. Another aspect to keep in mind is that forensic analysis is most often done on the clone as most hard drives are sensitive in nature and can be corrupted or destroyed very easily so taking a forensic data clone of the hard drive on the scene is vital in preserving the data. This process is time-consuming so for a crime scene unless it is a business with its data hard drives it would be more visible to bring an individual hard drive of one individual back to the lab to be analyzed rather than spending hours at the crime scene trying to gather the data plus it would be in more of a controlled environment (Wright, 2022).

Store electronic evidence

When it comes to storing and processing digital evidence there must be a check and balances that ensure that the said evidence is not compromised in anyway shape or form. The gathering of this evidence is in constant fluctuation and must adapt according to new shifts in the

digital world. That said, digital evidence needs to be collected based on its' life expectancy. The gathering of such data is not a particularly new nor old tradition in the world of digital forensics.

When there is a crime scene the first thing is always to secure that crime scene. Then next thing is to mark and document the evidence at the crime scene by those who are qualified to do so. When it comes to digital evidence those steps are very thorough and should be followed to the "T". It starts with photographing the computer (whatever type it may be) and the scene. Followed by protocols that need to be followed 1. If the computer is off leave it off, 2. If the computer is on take a picture of the computer screen, 3. Collect any live data – Start with RAM followed by network connection state, Users that are logged on, currently existing hard drives that are connected, etc., 4. When evaluating the computer when using a tool such as Zero-view and encryption is detected such as a PGP disk collect a local image of the hard disk using dd.exe, Helix- locally or remotely via F-Response., 5. Remove the power chord from the computer and if it is a laptop remove the battery, 6. Diagram and label all cords, 7. Document all device model numbers and serial numbers, 8. Disconnect all cords and devices, 9. Check for High-Performance Addressing (HPA) then image hard drives using a write blocker, Helix or a hardware imager, 9. Package all components with anti-static bags, 10. Seize all additional storage bags, 11. Keep all media away from magnets as this can compromise any data stored on them, 12. This is one of the most important and that is to document every step in the seizure of the evidence.

When it comes to collecting this evidence there is a need to be very thorough in that any digital evidence that may be volatile there have to be protocols in place to protect it. When the seizure of evidence starts assessing that evidence is a necessity to make sure you collect the data properly. The order of volatile data seizure is as follows; getting cache and registers, 2. Routing

Table, ARP Cache, process table, Kernel Statistics, Memory, 3. Temporary File systems, 4. Disk, 5. Remote logs and Monitored data that is in question to the digital data, 6. Physical Configuration i.e., network topology, and 7. Archival Media.

The world is full of digital evidence and cannot be taken for granted when it comes to obtaining said evidence if needed. There are a lot of things in this world in the time we live in that cannot be taken for granted as a level of importance. We all want to assume that the evidence is physical and understandable, but that does not mean that it is. We can presume that all is well, but in the end the analyzing of digital evidence can paint an even bigger and more extravagant picture of what unfolded than anything else (Wright, 2022).

Analyze electronic evidence

In the analyzing of this data, it is essential to be able to gather this data. When it comes to investigators, they have a tremendous chip on there shoulder as it takes a forensic investigators ability to obtain the data collected and put it into a format that is understandable to the court room. Several tools exist to help these forensic data analyzers to do their jobs more efficiently. One tool or should I say thing is resourceful. Digital investigators have remained simple and complex when analyzing data. It can go from just sifting through the common OS to using tools that dig into the binary of the OS. In most cases the simplest of resources can be rewarding. When it comes to Microsoft i.e., Windows you only need to remember that there is a recycle bin that stores all deleted data unless it was completely deleted. You can also use things such as Data Carving that can basically be used to analyze all non-deleted, deleted and files that were deleted to piece together the digital trail of the criminal (Just a Moment. . ., n.d.).

References

1. Kushner, D. (2011, October 27). *Murder, They Messaged: The Story of a Brutal Crime, Hatched Online*. Vanity Fair. Retrieved October 2, 2022, from https://www.vanityfair.com/culture/2011/10/world-of-warcraft-text-murder-201110
2. Roberts, H. (2011, November 9). *Teenage killer left digital trail of sick fantasies and World of Warcraft confession*. Mail Online. Retrieved October 3, 2022, from https://www.dailymail.co.uk/news/article-2057868/Teenage-killer-left-digital-trail-sick-fantasies-World-Warcraft-confession.html
3. LaMance, K. (2022, March 28). *Electronic evidence*. LegalMatch Law Library. Retrieved October 7, 2022, from https://www.legalmatch.com/law-library/article/electronic-evidence.html
4. *Handling of Evidence —*. (n.d.). Retrieved October 7, 2022, from https://aceproject.org/ace-en/topics/ei/eie/eie03/eie03d
5. Stride, J. D. (2017, December 7). *Creating a Chain of Custody for Your Documents*. In Confidence. Retrieved October 7, 2022, from https://www.inconfidence.com.au/creating-chain-custody-documents/
6. Lomer, D. (2016, September 14). Digital Evidence in the Cloud: A Challenge for Investigators. *I-Sight*. Retrieved October 9, 2022, from https://www.i-sight.com/resources/digital-evidence-in-the-cloud-a-challenge-for-investigators/
7. Keheley, P. (n.d.). *What Is Spoliation Of Evidence, And How Can You Prevent It?* Retrieved October 17, 2022, from https://www.digitalwarroom.com/blog/what-is-digital-spoliation

8. Law, B. (2020, May 26). *What Qualifies as Evidence Tampering?* Berry Law. Retrieved October 17, 2022, from https://jsberrylaw.com/blog/what-qualifies-as-evidence-tampering/
9. *fruit of the poisonous tree*. (n.d.). LII / Legal Information Institute. Retrieved October 17, 2022, from https://www.law.cornell.edu/wex/fruit_of_the_poisonous_tree
10. Wright, J. (2022, July 16). *Month of PowerShell - Working with the Event Log, Part 3 - Accessing Message Elements*. Retrieved October 23, 2022, from https://www.sans.org/blog/best-practices-in-digital-evidence-collection/
11. *Just a moment. . .* (n.d.). Retrieved October 23, 2022, from https://www.forensicfocus.com/articles/retrieving-digital-evidence-methods-techniques-and-issues/
12.