Computer Forensics: Investigations of the Future

Spencer Hanson

Contents

I Introduction 1

II What is Computer Forensics? 1
- II-A Acquire . . . 2
- II-B Authenticate . . . 2
- II-C Analysis . . . 2

III Technical Analysis 2
- III-A Hard Drives . . . 2
  - III-A1 Forensic Imaging . . . 3
- III-B Data Hiding . . . 3
- III-C Hashing . . . 4
  - III-C1 MD5 and SHA Algorithms . . . 5

IV Future Trends 6
- IV-A New Technologies . . . 6
  - IV-A1 Cloud Storage . . . 6
  - IV-A2 Solid-State Drives . . . 6
- IV-B The Future of the Field . . . 6

V Conclusion 7

Appendix 7

References 7

List of Tables

I Passwords and Their Hashes . . . 5

***Abstract*—Computer Forensics is a new field that uses traditional investigation processes and applies them to investigating a computer for digital evidence. In this paper, we will discuss the background of computer forensics and process of a digital investigation of a computer. Technical topics such cryptographic hashing and data hiding will be covered as well. Additionally, we will perform a demonstration of a basic computer investigation on a forensic image of a hard drive. To conclude the paper, we will discuss the future implications of cloud storage and solid-state drives on the field of computer forensics, and where the field will head in the coming years.**

I. Introduction

Computers are an integral part of our lives. A significant amount of transactions and processes take place using the computer and the Internet. With new types of technology, comes new types of crimes. To combat these crimes, a type of digital forensics has slowly become more prominent in the criminal justice world. Computer forensics emerged in response to the rising number of crimes committed that involves computers. There are two types of computer-related crimes: either a computer is used to commit a crime, or the computer itself is the target of a crime [1]. Computer crime brings forth many new issues that conservative legal processes have never been exposed it. Additionally, cyber lawyers have to deal with a greater level of ambiguity than many of their legal peers. The number of complaints that the FBI received that involve Internet crime was roughly 17,000 in 2000. In 2013, that same number was 262,000, and it nearly reached 340,000 in 2009 [4]. Computer Forensics involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis [9]. Although cloud storage offers new challenges for computer forensics, evidence is mostly found within the physical hard drive of a computer. Thus, it is critical for an investigator to understand where data can be hidden inside of the hard drive. It's also important for the hard drive to maintain honesty and integrity in order for any evidence found to be inadmissible in a court of law. Cryptographic hashing is used in an investigation to maintain such a level of integrity. There are both theoretical and technical areas of computer forensics that are crucial to understand and we will cover those areas in this paper.

II. What is Computer Forensics?

Computer Forensics involves the preservation, identification, extraction, documentation and interpretation of computer data. The computer investigation process is very similar to a traditional, criminal investigation process, but it is also different enough that it needed to have it's own methodologies developed. The three main aspects of all computer forensic methodologies include the three A's: Acquire, Authenticate and Analyze. In this

section, I will go into greater detail on each one of those aspects.

A. Acquire

The acquire phase of an investigation involves the acquisition of the evidence without altering or damaging the original [9]. When acquiring a computer or hard drive, it isn't as simple as turning the machine off and taking it back to the lab. If there was software left behind by the criminal that would destroy all data the next time an administrator logged on, then turning the computer off wouldn't be the right move. In this case, it would be better to pull the plug and freeze the computer; however, the criminal could have an attack running in progress. In that case, pulling the plug would result in a loss of data and evidence from the attack. All of this information just means that every case and situation needs to be approached differently. There isn't a clear way to go about the process. Every attack, crime, and computer is different. The most ideal way to examine a system and maintain the most defensible evidence is to freeze it and examine a copy of the original data [9]. It's important to collect as much evidence as you can. In a computer case, some of the most important evidence is digital log files kept by various systems. For example, if you are a dealing with an Internet-related attack, then you should try to obtain the logs kept by the Internet service provider (ISP).

B. Authenticate

The authentication phase involves making sure your recovered evidence is the same as the originally seized data [9]. Crime scenes age over time, and the same is true for computers. A hard drive deteriorates over time, and it can be harmed by mold, dust, or insects. The evidence itself (text files or pornographic images) never appear at random through any form of wear and tear; they are placed there by human action. Proof of integrity and timestamping are provided by calculating a value that functions as an electronic fingerprint for a specific file, or even a hard drive. This cryptographic technique is called *hashing*, and the value itself is a *hash*. I will go into more detail on hashing in a later section. For now, it's important to understand that the first thing to do when evidence or data is collected, is to create a hash value and record it. Then you can prove that the data you are using for your examination is identical to the original data.

C. Analysis

The final phase, analysis, involves analyzing the data without modifying it [9]. Before you can begin the analysis, it's very important to create back ups of the original hard drive: one master back up, and then a second one which you perform the analysis on. You want to create a forensic back-up of the data, not a "normal" back up. The difference is that a forensic backup is a bit-for-bit back-up, also known as Raw Image Format [1]. A normal backup doesn't copy deleted files, hidden partitions, or other parts of a hard drive that are important to investigate. One of the first things to do in the investigation is to search for terms related to the case. There are powerful forensic programs with sophisticated search capabilities so it essential to use one of these. Next, try to retrieve any deleted files. There are four main categories of files, and it's important to understand their differences. The four types are user created files, user protected files, computer-created files, and then other data areas [15]. User created files are address books, e-mail files, spreadsheets, text files, etc. User protected files are compressed files, misnamed files, encrypted and password protected files, and hidden files. Computer-created files are backups, log files, configuration files, cookies, Internet history and cache, etc. Other areas include deleted files, free space, hidden partitions, meta-data, software registration data, and more. To retrieve deleted files, there is software that exists to help you. To manually do it, you need to use a hex editor, but that is a long and complex process. Next, you can check unallocated space in the hard drive for any hidden data or partitions. These are just a few of the things you can do when investigating a hard drive.

III. Technical Analysis

Computer Forensics is a discipline that involves many different types of technical areas of computer science since an investigator will encounter many different ways a computer can be used in a crime. Some of these areas include encryption, Internet security, programming, knowledge of operating and file systems, and more. In this paper I will go over some of the areas that are more relevant to my project and give an in-depth description of each. The technical aspects included in this paper are hard drives, the process of hiding data, and cryptographic hash functions as a method of data integrity. The paper will then conclude with a discussion on what I have done for my demonstration thus far.

A. Hard Drives

A hard drive is the core of a forensic investigation; it's what contains the digital evidence. There are many layers of hard drive, from the partition all the way down to the records and fields within a file. Understanding the hardware and software layers and how they inter-relate are important to being an effective investigator.

In this section I will discuss the different layers of a hard drive important to an investigation. The first layer of a hard drive is the partitions. A partition is the segment of the hard drive that is separate from the other portions of the hard drive for a purpose such as multiple operating systems using the same hard drive, each with their own partition. Firmware of the hard drive can be manipulated such that partitions can be hidden from the investigator. This can be done by using the software released by the manufacturer to update drivers or by other software designed for drive repair and data recovery purposes [12]. The partitions are what contain the file systems of the hard drive. The process of turning a partition into a recognizable file system is called *format command* [9]. The file system is the layer of the hard drive where an investigator will spend most of their time. The file system is the place where an operating system stores files, making it easy for you to access them by name, location, date, or other characteristics [9]. Like a database, a file system has one or more indexes, or tables. The tables have a unique identifier for each object and contain location information so that the system can find objects when their access is requested. Furthermore, a file system operates on data in specifically sized unites. On Windows, these units are called clusters. Slack space, also known as Disk Slack, is the name given to space that is left over between the end of the data and the end of the last cluster. This means that every file that isn't an even multiple of the block size has some slack space associated with it. Slack space can be used by criminals to hide data because the host file that is associated with the hidden data is not affected by it. A file-level copy of a hard drive will not contain slack space, which means that a forensic image of a hard drive must be an exact copy.

1) Forensic Imaging: One of the first things an investigator does when they encounter a computer is create a copy of the hard drive. The copy must be a forensic image of the hard drive, meaning it is a bit-for-bit copy of the data [1]. A normal backup doesn't copy deleted files, hidden partitions, or other parts of a hard drive that are important to investigate such as slack space. A forensic image is also known as Raw Image Format, the most common way to achieve such a copy is using the *dd* command in Linux, or other forensic software. A piece of software known as FTK Imager is a powerful forensic tool used to create ram images, and I will discuss the use of this software later in this paper.

B. Data Hiding

The practice of hiding digital data is as old as the computer systems they are hidden on. Various methods exist in the modern computing world to hide data, and they all share the theme of storing information in places where the data is not expected. Hidden data is known as "dark data", and it's possible for light data and dark data to coexist [3]. For example, watermarking and encrypting a file is the production of light data that contains a dark message. There are many areas that contain deleted data within a hard drive, and they all can contain hidden data. When a hard drive has empty space, it is known as unallocated clusters [9]. Even though they don't contain data, these unallocated clusters have more than likely been used to store deleted or overwritten blocks of data. Thus, the more empty space on a hard drive, the more room there is for hidden data. As mentioned earlier hidden data can be contained inside slack space, unallocated blocks of data on the hard drive, inside of unused partitions, or application data within a file, such as Microsoft Word. All the structures within a hard drive can contain hidden data, as illustrated in **Figure 1**.

Many hard drive manufacturers have been creating partitions to store recovery data for years. These partitions are known as "Host Protected Areas." (See figure 1, item 1) These host protected areas (HPAs) are hidden from operating systems to ensure it cannot be accidentally formatted [12]. It's possible to identify the presence of an HPA, access it to write data to it, and then return it to an HPA format. Most hard drive partitions have space reserved at the beginning of the drive known as a Master Boot Record (MBR) [3]. (See figure 1, item 2) The MBR contains code necessary to begin the initial program load of an operating system and it contains a partition table that defines the size and location of up to four partitions. The implication of the existence of this table is that there are many sectors of empty space within it that data can hide in. Another example of hiding data is if there is a 100GB partition on a 500GB hard drive. The extra 400GB of space is known as *volume slack* (see figure 1, item 3), not to be confused with the slack space mentioned earlier in a specific file. It's possible to create another partition in the volume slack, put data on it, and then delete the partition. This partition may have been deleted, but the data is still there and now it is hidden. Every partition contains a boot sector, even if that partition is not bootable. The boot sectors in non-bootable partitions (Figure 1, item 5) can contain hidden data as well. Next, any space in a partition that is not currently allocated to a particular file (Figure 1, item 6) cannot be accessed by the operating system. Until the space has been allocated to a file, it can contain hidden data. Finally, it is possible to manipulate the file system metadata that identifies bad blocks so that the usable blocks are marked as bad too. Those blocks will no longer be able to be accessed by the operating system, thus making it possible to hide data within them.

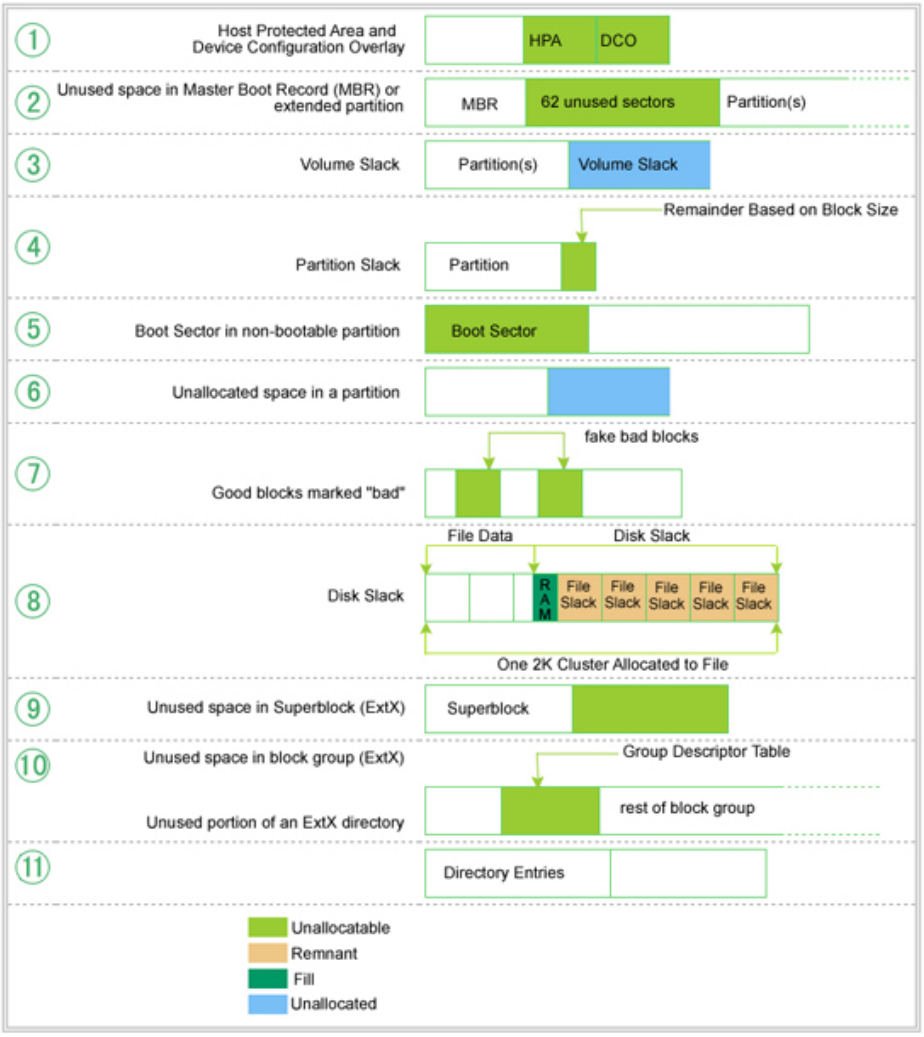

Figure 1. A graphical illustration of the digital sectors of a hard drive. In each example, the shaded area represents space within the structures where hidden data could reside. It starts at the level of the hard drive itself, and then works down through the set of nested data structures.

All the methods of data hiding discussed so far has been within the media and file system structures. There are others data hiding methods such as altering BIOS parameters, swapping files, binding an executable file to another, steganography, encrypted and compressed files, and renaming files [3]. Renaming a file is a simple, but extremely effective approach to data hiding. By changing a file's extension, you can quickly and easily hide it from an inexperienced analyst. For example, changing a MS Word document to have a .jpg extension instead of a .doc extension.

The process of hiding data inside a hard drive and then retrieving that data are important to understand for a computer forensic investigator. There are many, complex ways a criminal can hide evidence on their hard drive, but there are also sound methods to retrieve that data. Later in this paper I will go over how to retrieve data that has been deleted, a process that will be involved in the demonstration portion of my project.

C. Hashing

Digital encryption techniques are used to protect data in two ways: to maintain privacy and to prove integrity [9]. Encryption and cryptography are both related terms, but are different in scope. Encryption is the process of obscuring the content of a message. Cryptography is the practice of protecting the messages. The form of encryption I will focus on in this paper is what is known as a hash function. Data can become distorted in transit or during the investigation, so there

has to be some form of accuracy testing for the data. Hashing is a process that aims to maintain the integrity of the data by taking files, strings, or even full hard drives and running them through an algorithm, and receiving it's own hash value that is completely unique to itself. You can then compare the hash value of a file before and after you have analyzed it in order to ensure it hasn't been compromised [16]. The hashing algorithms that are most commonly used today are the Message Digest 5 algorithm (MD5), and the Secure Hashing Algorithm (SHA) [9]. A cryptographic hash algorithm is a one-way form of encryption, which means that is extremely hard to reverse the process [10]. It is statistically impossible for cryptographically secure hash algorithms to allow two different source files to have the same values. That is what makes a hash value the digital fingerprint of the file. Hash functions can be used in two ways. First, they can verify that a file has been altered. If you think that the binaries on a system may have been compromised, you have to assume that they have been so carefully compromised that their access times, sizes, and checksums have been manipulated to match the original files. Hashing provides a reliable way to confirm that the file has been changed. The other use of hash functions is to verify that files are intact and have not changed. Below is an example of how a hash functions works:

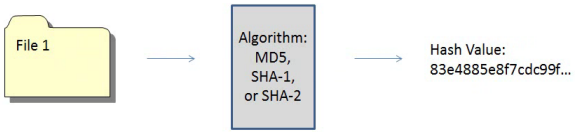

Figure 2. A visual representation of how hashing works. A file is run through an algorithm and then that algorithm outputs a hash value that is entirely unique to that file. The hash value is that files digital fingerprint.

1) MD5 and SHA Algorithms: As mentioned earlier, the two main algorithms that are involved in creating a hash value are the MD5 and SHA algorithms. In this section, I will go into greater detail about each of these algorithms. First I will go over the MD5 algorithm. The MD5 algorithm is extremely useful for forensic purposes, but it is not good for security. MD5 will be reliable in ensuring the integrity of a hard drive by calculating the hash value before and after the investigation, but if it is used for something like password security, it's not as effective because it is prone to brute force attacks [17]. MD5 has also proven to be effected by *collision*. A collision occurs when the hash algorithms creates a hash value that is the same for two documents [9]. Although collision is extremely rare, it has happened with MD5. As for the algorithm itself: The message is first "padded" so that it's length in bits is divisible by 512 [13]. This is done by adding a single bit, 1, to the end of the message. The 1 is followed by as many zeros required so that the length of the message is up to 64 bits fewer than a multiple of 512. The remaining 64 bits represent the length of the original message. Next, a 128 bit message digest is created from the message that was just padded. Then 128-bit digest is divided into four 32-bit words, and each word is initialized to a certain fixed constant. Next, there are four rounds, one for each 32-bit message. Every round uses one of four functions (F) to perform 16 similar operations based on F. The four possible functions for F are as follows:

$$F(B, C, D) = (B \wedge C) \vee (\neg B \wedge D)$$
$$G(B, C, D) = (B \wedge D) \vee (C \wedge \neg D)$$
$$H(B, C, D) = B \oplus C \oplus D$$
$$I(B, C, D) = C \oplus (B \vee \neg D)$$

Each of the 16 operations performed in each round are based on modular addition and left-bit rotation. Table 1 shows samples for passwords and then their corresponding MD5 hash digest.

TABLE I
PASSWORDS AND THEIR HASHES

Password	Hash
Ali99	b91f419b5388b5df94804ed640914471
Ashraf10	c16ffe25368eaddba046ca3ef4c71fd0
abcdef	e80b5017098950fc58aad83c8c14978e

The SHA algorithm is a lot like MD5, except that it produces 160-bit message digest. This is what makes SHA much more secure than MD5, and also what makes it the US federal standard hash algorithm [6]. That means that is required to be used whenever a cryptographic hash algorithm is needed for federal applications. The 160-bit message digest makes SHA more secure because, although its theoretically possible, collision is highly unlikely and it has never happened on the application level. The SHA algorithm is more complex, so I won't go into great detail. It involves two buffers that each consist of five 32-bit words, and a sequence of eighty 32-bit words. The message digest is generated by processing blocks of the 512-bit message in a method that involves 80 steps, where each step involves bitwise rotation and modular addition like the MD5 algorithm.
Hashing is a valuable tool used in forensic investigations to provide a form of integrity for the evidence after an investigation has been performed on it. Later, in the demonstration portion of this paper, I will describe how I plan to use hashing in a "dummy" investigation.

IV. Future Trends

The field of computer forensics is a young field that is undergoing rapid changes. Currently, computer forensics is a discipline that is becoming a science; a skill that's becoming it's own field. New technologies such as cloud storage and solid-state drives are causing the field to rework already existing methodologies. Not only is the technical side of computer forensics changing, but the academic side as well: more classes and certifications are being offered. In this paper I will go over the implications of new technologies for the future of computer forensics, along with predicting where the field will be at as a whole in the coming years.

A. New Technologies

Digital forensics has long been about the retrieval of evidence stored in a digital format, often on a hard-drive or a USB. Both of these things are still common today, but the emergence of new technologies to store data on have provided new hurdles for computer forensics to jump over. The specific technologies that I will talk about in this section are cloud storage and solid-state drives.

1) Cloud Storage: Cloud storage is becoming increasingly popular among individuals and businesses. The retrieval of evidence from cloud storage can be extremely challenging during an investigation. Factors such as virtualization, lack of knowledge on location of digital evidence, privacy issues, and legal or jurisdictional boundaries are all things that need to be addressed when conducting an investigation with cloud-based data [11]. When a user accesses data on the cloud, what are known as artifacts are left behind [8]. These traces of data can be found in the hard drive in places such as the installation network, database files, log files, uninstallation data, and more [5]. Most cloud storage services provide a client application for the user for convenience. When one of these applications are installed on a Windows system, traces of it are left inside the registry, log files and database files [8]. These files contain information on whether logins to a cloud service were successful or not, and the actions of the user. In a smartphone, most important artifacts are found in database files [8]. Database files are created to manage files and folders that are designated for synchronization.

One of the hardest aspects of investigating a cloud storage service is that it is difficult to find out what a user did from the moment of subscribing to the service until the end of their use of the service. Additionally, hosting companies are not willing to release information and logs about their users to protect clients' personal information. This is something the field of computer forensics has never seen, so it will make the investigation process longer and more difficult. In the future, we will start to see more thought-out methodologies and processes for an investigation that involves cloud storage. Although hard-drives are still popular, the emergence of technologies such as cloud storage are going to cause a decrease in the use of physical storage of data, causing many computer investigation techniques to be obsolete. Such an implication might hinder computer forensics in the short-term, but help it grow and adapt in the long-term.

2) Solid-State Drives: The transition from magnetic hard drives to solid-state drives inside modern computers is important to the computer forensics world. It's sometimes possible for solid-state drives (SSDs) to destroy evidence under their own volition, in the absence of specific instructions to do so from the computer [2]. With normal hard drives (HDDs), almost all files containing file system metadata and data are preserved after a quick format, and all of those files can be recovered perfectly at a later time. In contrast, with an SSD, almost all of those same files are damaged and purged completely shortly after a reboot [2]. Solid-state drives are capable of derailing a digital investigation before it even begins. If an investigator is unable to retrieve anything from the SSD, then any potential evidence is lost forever. Thus, new approaches and precautions need to be taken and adopted in the future. Until drive and data behavior of solid-state drives are more extensively studied, they are considered a 'gray area' in forensic recovery and legal validation. SSDs are an even larger hurdle than cloud storage for computer forensics to jump over, and it doesn't help that computer forensics is still trying to establish itself as a field at the same time. I think SSDs may potentially slow the growth of the field until solutions and methodologies are established in regards to the approach of SSDs in an investigation.

B. The Future of the Field

In 2009, there were 336,000 reported Internet crime complaints and that number was down to 262,000 in 2013. With computer forensics becoming more important and necessary, the number of computer crimes will still be very large but it will become relatively manageable. As noted before, computer forensics is still a new field; there is room for growth in many directions. There is currently a lack of national framework for certification and curricula to be a computer forensics investigator. In the world of computer forensics, there is more of a focus on the applied aspects, and less on the development of a theoretical foundation. In 2004, the most reported issue with computer forensics was the lack of education, certification, and training [14]. In the coming years, it will only become more necessary for a national framework for an academic curriculum of computer forensics to be developed. More computer forensic classes will be

offered at schools, along with an overarching standard for certification. All the certification that exists today is for particular technologies and software. For example, you can obtain certification for the software suite known as EnCase, which is the global standard in digital investigation technology [7]; however, there is no general certification for a digital forensics investigator.

V. Conclusion

Computer Forensics is a growing field; it's only as old as the personal computer itself. New technologies such as cloud storage and solid-state drives help challenge it in a way that promotes advancement, but the core foundation that was laid still remains. Even with these new technologies, understanding some of the core technological concepts such as hard-drives, data hiding and cryptographic hashing is important. A computer investigation is not much different than a traditional, criminal investigation. The key difference is the computer itself, so understanding and treating the computer as if it were a suspect is the key to being an effective investigator.

Appendix

Throughout my years at CSB/SJU, I have acquired a lot of skills and knowledge that greatly aided me in my research endeavors. From learning effective research techniques, to becoming a better writer, and to learning through my computer science classes, this project reflects how far I have come as a student. The greatest thing I have to take away from this project is the technical writing and presenting skills. I took pride in being an effective writer previous to this project, but my technical writing skills were lacking. I now feel much more confident in my abilities to write in a way that future employers may require of me. Additionally, I've never been a great presenter, especially in a technical sense. By the time I gave my final presentation, I felt like I had come a long way. There was an enormous amount of constructive criticism and tips that I had the privilege of receiving. In particular, using presentation slides as supplements to my presentation and not as note cards is something I feel I have a good grasp on now.

Things I learned in my computer science classes also helped me understand particular areas of research. The classes that come to mind are computer networks, algorithms and computer organization. In my computer networks class, we learned a fair amount about cryptography and hashing. The combination of learning that inside the classroom and learning it through research really helped me understand an area of my project that may have been more confusing otherwise. In addition to learning about hashing in networks, my knowledge on algorithms helped me understand the algorithms for MD5 and SHA hashing. Another class that was important to my project was computer organization. In that class I learned how hard drives work and how things operate on a bit-by-bit level. Understanding those things was key to my entire project, especially the research done on hard drives and hidden data. In a broader sense, various other classes helped me become a better writer and researcher. Classes like symposium and psychology were key in the strength of my skills at the start of my project. Getting a very solid start on my research and learning how to effectively use sources helped me tremendously in the initial weeks of the semester.

This project has been a very rewarding experience for me. I've acquired skills that I will carry with me for the rest of my professional life, not to mention that knowledge and grasp of my research topic as well. Computer Forensics is one of the most interesting things I've learned in regards to computer science. I even applied to an entry-level computer forensics job with a company in Minneapolis. Through this research, I may have discovered my passion inside of my major, and that really excites me. This has been one of the few times that I feel like I've gotten absolutely everything I could get out of a class.

References

[1] Ankit Agarwal, Megha Gupta, Saurabh Gupta, and SC Gupta. Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS)*, 5(1):118–131, 2011.

[2] Graeme B Bell and Richard Boddington. Solid state drives: the beginning of the end for current practice in digital forensic recovery? *Journal of Digital Forensics, Security and Law*, 5(3):1–20, 2010.

[3] Hal Berghel, David Hoelzer, and Michael Sthultz. Data hiding tactics for windows and unix file systems. *Advances in Computers*, 74:1–17, 2008.

[4] Internet Crime Complaint Center. 2013 internet crime report.

[5] Hyunji Chung, Jungheum Park, Sangjin Lee, and Cheulhoon Kang. Digital forensic investigation of cloud storage services. *Digital investigation*, 9(2):81–95, 2012.

[6] Donald Eastlake and Paul Jones. Us secure hash algorithm 1 (sha1), 2001.

[7] Lee Garber. Encase: A case study in computer-forensic technology. *IEEE Computer Magazine January*, 2001.

[8] Jason S Hale. Amazon cloud drive forensic analysis. *Digital Investigation*, 10(3):259–265, 2013.

[9] Warren G Kruse II and Jay G Heiser. *Computer forensics: incident response essentials*. Pearson Education, 2001.

[10] Ralph C Merkle. One way hash functions and des. In *Advances in CryptologyCRYPTO89 Proceedings*, pages 428–446. Springer, 1990.

[11] Darren Quick and Kim-Kwang Raymond Choo. Google drive: Forensic analysis of data remnants. *Journal of Network and Computer Applications*, 40:179–193, 2014.

[12] Huw Read, Konstantinos Xynos, Iain Sutherland, Gareth Davies, Tom Houiellebecq, Frode Roarson, and Andrew Blyth. Manipulation of hard drive firmware to conceal entire partitions. *Digital Investigation*, 10(4):281–286, 2013.

[13] Ronald Rivest. The md5 message-digest algorithm. 1992.

[14] Marcus K Rogers and Kate Seigfried. The future of computer forensics: a needs analysis survey. *Computers & Security*, 23(1):12–16, 2004.

[15] KK Sindhu, Rupali Kombade, Reena Gadge, and BB Meshram. Forensic investigation processes for cyber crime and cyber space. In *Proceedings of International Conference on Internet Computing and Information Communications*, pages 193–206. Springer, 2014.
[16] Lecture Snippets. Ubuntu 12.04 forensics - hashing overview.
[17] Systems and Al-Azhar University Cairo Egypt Computers Engineering Dept, Faculty of Engineering. Analysis of md5 algorithm safety against hardware implementation of brute force attack.