Introduction to Digital Forensics

Brady Nielsen

Table of Contents

Introduction

Welcome to the world of computer forensics. This textbook is an Open Education Resource (OER) written under Creative Commons (CC). This book is designed to be an introduction to a very in depth and complex topic. In general investigating digital evidence is a labor intensive manual process. The target device and motivation behind the investigation can vary, the underlying principals are similar across all types investigations.

The target audience for this textbook are students and technical professionals. As a student you may be studying at a high school, college or independently. As a technical professional you may be a beginner or a seasoned veteran looking to master a new skill. The fact you have made it this far indicates you have sufficient interest and motivation.

Throughout this book I will try to keep the need for technical expertise to a minimum. We will be working on a Windows® computer in a sample case. The decision to investigate a full computer running a copyrighted OS was not taken lightly. In order to have the most familiarity with the operating system, Windows® was an easy decision.

Students should have a basic understanding of file structure and navigation of a file system. These are entry level skills. Other aspects of Windows will be discussed, but if you cannot locate files on a hard drive if you are given a path, you will not be successful in understanding this basic investigation.

We will look at common types of investigations and the data that helps to prove or disprove the allegations. This leads us the basic concept of investigating a computer. Evidence we are tasked to locate are inside of files. They may be easy to access, understand and explain to lay persons, or they may be very difficult to locate and interpret.

Ultimately you will discover throughout this book that you will be asked to conduct an investigation. You will be given guidance and you will follow a rigid set of guidelines. When you have completed the investigation you will provide any supporting evidence back to the requestor in a language they can understand. You collect and present. You are not the judge or the jury. The items you locate will rarely prove anything directly. Almost all evidence located inside of a computer is circumstantial evidence. It cannot associate an actual person with an action or evidence item.

Hopefully as you work your way through this book you will build the skills of an investigator and learn the ins and outs of investigations. Unfortunately, none of the activities you will encounter are like what you might have seen in a movie or on television. The process is not glamourous or exciting. This doesn’t mean that investigations can’t be gratifying and fulfilling. The skills developed in this book are very marketable. The ability to locate, interpret and explain data is a specialty many technical professionals lack.

The original target for this text was the students in the Information Technology AAS degree program as Spokane Falls Community College in Spokane, Washington. The author felt bad asking his students to pay $200 or more dollars for a textbook used in one course. He was awarded a grant to develop this text. It was not worth the money on an hourly scale, but the reward of being able to control the content of the book and tell his students the book is free was worth every second of his time.

Please enjoy the content. The author is always willing to discuss content and welcomes feedback to the content on both a technical and editing level. nielsen.brady@gmail.com

Chapter One Computer Forensics

Computer Forensics

Computer forensics is a rapidly growing and changing field. There are many opportunities to apply the techniques we will discuss in this book. One does not need to desire to be a full time digital forensic investigator to benefit from the content of this book and the concepts of computer forensics. The ubiquity of computers in today's society provides frequent opportunities to investigate the operation and content of devices in our everyday lives. Throughout this book I will use the term computer, but realize that any device that can create, modify, send, receive or store digital signals can probably be considered a computer. Because of the range of devices that one might investigate the term digital forensics is often used interchangeably with the term computer forensics.

There are a significant number of types of computers in our lives. Many we don't even notice them as computers. Cell phones are a small portable computer. Digital video recorders, such as a TiVo®, are a specialized computer. Onboard computers in modern cars control and record actions of the driver and the automated prcesses of the car itself sucha s automated braking. The type of device can dictate how or what can be investigated, but any potential device can be a target of investigation in today's society. The first task for learning any new topic is almost always a definition. Computer forensics is the collection, preservation and preparation of evidence contained inside a computer for presentation in court.

My target audience for this book is students and technical professionals. Most of you will never prepare evidence for presentation for court proceedings. Any investigation could potentially lead to a criminal or civil proceeding. As an investigator you should always keep in mind that your actions could be scrutinized in the future, often time two or more years after your investigation, and may have a significant impact on an outcome of a trial. First and foremost, don't panic. The process will be described and practiced throughout this book. No inspector is perfect in every investigation. The keys are going to be preparation, execution and documentation. We will examine all of these as we progress through this text. By reading this book and doing the labs you are working diligently on preparation.

As a technical professional most investigations you conduct will not lead to any type of law suit or criminal case. They are most often identifying what has occurred to a system to repair any damage and prevention of a reoccurrence of the disruption to business. As a full time forensic investigator most of your cases will be pursued to be presented in court. A significant number of cases with substantial evidence are pled out before they are heard by a judge and jury. Collection, preservation and presentation of evidence are significant factor in this process. These are not the only types of investigations that could occur. While this is not an exhaustive list of organizations and types of investigations here are some that can benefit from a computer forensic investigation.

Businesses might require investigating violation of company policies such as acceptable use of computers, sexual harassment or possible unauthorized access to corporate computers. Law enforcement investigates many potential types of crimes that involve computers. We will discuss this topic more throughout this book. Lawyers might require the services of a forensic investigator for civil cases such as stalking, harassment, divorce, or intellectual property infringement. Government intelligence agencies and military agencies conduct forensic examinations to collect and verify potential intelligence and information to support operations. Security firms frequently conduct forensic investigations for other organizations as part of incident response. They try to identify how intruders gained access to their systems or data, what they accessed and what data they might have exfiltrated.

This list is far from exhaustive. In an introductory text we cannot cover all of these types of investigations and the nuances of each. Instead we will cover the most likely and most beneficial uses of computer forensics. In general, we will start with law enforcement processes and relate other common investigations to their practice. This the most logical approach. This is based on the fact that almost all investigations could ends up as law suits and their practices and philosophies work with almost all other types of investigations. Where relevant, the differences in the types of investigations will be noted for you to be aware of potential differences.

Computers are used in crimes in three different ways. They are used in the commission of a crime and without a computer would not exist. Crimes like hacking fall into this category. Computers can be used in the commissioning of a crime that is still a crime without the existence of computers, but might make committing the crime easier. Crimes like harassment or fraud fall into this category. The last type of crime where computers are involved, computers act as a repository of information or evidence about a crime. Something such as a picture taken with a cell phone at the scene of a crime or a journal where someone details their crimes fall into this category.

I also feel compelled to mention the use of a computer or peripheral as a physical object. Assaulting someone with a computer is often a question I receive in class when discussing this topic. Sometimes the question is a legitimate question, but most often it is in jest. This type of crime is not one we will discuss. This would be no different than a knife or brick as a weapon in an assault case. This is a more traditional forensic science, not digital forensics.

We can relate these three types of crimes back to almost all of the other types of investigations. I will not usually talk about the types of crimes, but if I do they will often relate to more than just criminal cases. The sending of harassing messages via corporate email is not necessarily a criminal act, but is something a technical professional might be tasked to investigate. It falls under the second category, it is against the rules to harass fellow employees. This violation could occur in person, over the phone, on paper or with the aid of a computer via email.

Understanding computer forensics is all about understanding the process of identifying, preserving and presenting evidence. Your role as an investigator, whether it is a full time duty or as needed, is often as a leader or director versus a practitioner. You might be tasked to investigate a technology that you are not familiar with its internal working. This is not an impossible task. You likely won’t have the time or resources to learn the technology enough to investigate it properly. You will have to work with a subject matter expert to help navigate the technology and identify the best available evidence. Despite my years of experience in enterprise technology roles, education and forensic back ground, if I was tasked to investigate an Oracle® database, I would be lost. No investigator can be a subject matter expert in all technologies that you will be asked to investigate.

Despite the fact that you don’t need to be an expert on the technology you are investigating, I have elected to use Microsoft Windows 7® as our baseline for learning computer forensics. It should help in the process of learning if you do not need to learn about the technology you are investigating as well. If you are not proficient in any current version of Windows® you may have to struggle with the additional burden of learning that operating system in addition to computer forensics. My justification for using a closed source, proprietary operating system to accompany a creative commons book is two-fold. The first is common usage. Windows® is still the most common operating system used by businesses. The second is that most technical professionals and technology students should be familiar enough with this technology to be able to focus on the computer forensic aspect of this book.

I entertained using Linux® or Android® as they are both open source operating systems. In my experience as an instructor, far too few students are knowledgeable of these two operating systems for me to not spend time explaining the content of the operating system versus focusing on our true topic, computer forensics. In general, if you learn the computer forensics process and can understand one operating system, you can apply the process towards almost any technology. There are aspects or details that are unique to each technology that might require some new learning or techniques. The process to locating, preserving and presenting the evidence is still consistent through all technologies and type of investigations.

The content of this textbook will focus on the technical aspects of building knowledge of digital forensics, understanding the process and developing the skills to build an environment to have a sound forensic process. I will not discuss specifics of computer based laws. I am not a lawyer and I cannot take into consideration every jurisdiction in the world where a potential reader might reside or investigate.

I will however assume that you have a general knowledge of your legal system and you can understand basic legal terms. If you are not familiar or find terms you do not absolutely know, I strongly suggest you do some addition fact finding via sources such as Wikipedia or Youtube. I am also going to assume that you have some familiarity of investigations. It is also a reasonable leap that most people old enough to read in the United States have been exposed to certain types of investigate processes through popular media. I might make references or comparisons to physical evidence investigations and procedures. I will try to make the simple, understandable and not too graphic. If you have not been exposed to police shows or articles, most CSI, NCIS, or other police investigation shows are relatively accurate and informational. I can’t belive I just said “Go watch TV”, but I did.

I will not discuss the ethics behind the topic of forensics investigations. While most laws are intended to reflect the ethics of the group that is subject to the law, the process isn’t always easy from an ethical perspective. Corporate investigations involve people’s livelihoods or might even send someone to prison for an action the perpetrator didn’t fully comprehend. You will be asked to do work that could very significantly impact a person or a business for the rest of their life. Worse yet, you might be asked to alter your findings to include or omit information based on the wishes and motives of your employer.

At first glance laws and ethics might not seem significant. The more time I spent investigating the more these two influences led me to stop the practice of conducting investigations. I now teach other people to handle this burden in my place. The role of a digital forensics investigator is to find the evidence, preserve that evidence and present it to the person or group that requested in investigation. This is the long description. From here on I will summarize this process by using the phrase conducting an investigation or investigating. One thing I have noticed students struggle with is, they feel compelled to be the judge and jury. Avoid judgment and focus on collecting all of the relevant evidence for the appropriate people to judge. When I present the theory early in the course all students nod their head and agree that this is what should be done. At the end of the course when I read their findings, seldom is there a lack of bias or judgment. This is human nature to put the pieces together and form conclusions. You must resist this temptation. You will put your professional opinion into the investigation. You will interpret what you find and try to articulate what you think happened based on your knowledge of common computer usage. An easy example of this would be finding and email message in the sent folder of an email client. It would be my opinion that an email was composed and sent from that computer account at that date and time. I would not be able to definitively prove that a specific person wrote and sent the email unless I witnessed it. I would not comment on the content unless there quest a need to explain a technical aspect, such as it might have been stored in 64 bit code instead of plaintext. There might be other methods to associate a person with an activity, but most evidence you will find will not be absolute proof that any one person did any specific activity. Let the persons that requested the investigation make those decisions. Let the judge and jury do their job, focus on yours.

Chapter Two Evidence Acquisition

Evidence Acquisition

Evidence collection is a significant portion of a digital forensic investigation. Like most types of criminal investigations, digital forensics investigations have physical evidence. The unique aspect of computer forensic investigations is the digital evidence. You as an investigator have to address both aspects of an investigation, physical and digital. Each aspect has challenges, pitfalls and best evidence practices. == Investigation Basics We will start with physical evidence aspects first. Acquiring or gaining access the devices that contain digital evidence is similar to other physical evidence. The most significant rule for both physical and digital evidence is “preserve the evidence” or to me “don’t modify the evidence”. Alteration of the evidence might create two potential issues in the investigation.

First issue might be the destruction of information that might be valuable evidence. This might be a finger print or the email that has all of the details of a crime. The second issue involves the introduction of doubt of the validity of your evidence. If the person being investigated can generate doubt revolving around the accuracy of your findings, it might be considered as in accurate, fraudulent or outright dismissed as invalid evidence because it is tainted. If a crime scene has a bloody knife laying next to a corpse it is important that the knife not be altered. It might contain DNA evidence and finger prints of the perpetrator. If the person responding to the scene drops the knife into a bucket of industrial solvent, the evidence might be completely gone. If anything survives it is likely to be dismissed as tainted or not able to be verified as unaltered evidence.

Similarly if you approach the computer used by a person alleged to be browsing pornography and it is logged on with the person in question’s account, you shouldn’t open a browser and check your Facebook account. The new files might overwrite older cached items, or the defendant might claim that this is how all of the evidence you found ended up on their computer, by your actions not theirs. This might be an obvious example, but similar pitfalls exist.

When collecting physical evidence and when investigating digital evidence you need to have a legal right to do so. We will discuss this process and concept more in-depth later in this chapter, but remember this is not a legal guide or law book. If we are considering collection of evidence for an intelligence agency or military entity the situation might dictate and the rules resort to physical control is all that is needed to confiscate evidence with or without legal right. All other scenarios follow rules of search and seizure.In order to continue to discuss the acquisition and handling of physical evidence we will concede that you do have legal right to seize and search the evidence in question. If not modifying the evidence is rule number one for forensic investigators, rule number two is document everything you do in careful detail. This helps to prove that the evidence is the original unaltered evidence and helps to protect your reputation by providing a step-by-step recounting of your actions so that anyone else with the appropriate skills can recreate your findings. Even if you make a mistake, such as forgetting a step, you should keep detailed notes. Omitting an error indicates that you might be covering up other mistakes or intentional modifications of evidence or findings. You are a human being and will occasionally do something erroneous. If you admit to it, you are less likely to have your findings or the process questioned for accuracy and validity.

As a general note to potential investigators, you will spend far more time documenting your actions than you will conducting the investigation. I generally use an 80/20 reference, but there are many variables involved. You will spend 80 percent of your time documenting and 20 percent of your time doing. Be prepared to become very verbose in your writing. Failure to be thorough in your documentation can cause evidence to become inadmissible, dismissed as potentially flawed or even call your competence as an investigator into question. Writing is an essential function to the investigation process.

Collecting Physical Evidence

When collecting physical evidence the most important thing is to have a safe environment to be able to collect the evidence properly without any risk to you or anyone else. While this might not always be the case in all situations, where ever possible do not place yourself in danger to collect evidence. If you are part of a team executing a search warrant, ensure that the officers assigned to remove threats have done so.

The first consideration once the area is secure and safe is to document the environment. All investigations should have a very specific purpose and scope. You should in your own words, as detailed as you can, describe the physical area you collecting evidence from. You might write it down with a pencil on a notepad, record it with a video camera, take photos or take audio notes dictating as you go. Ultimately it is best to have consistent, typed notes when you complete your investigation. Most important information will be specific details about the physical evidence and anything in the environment that is abnormal or notable. Abnormal or notable might help prosecutors to further document their allegations by associating the area with things that can be associated with the suspect.

The unique aspects of physical evidence include details such as manufacturer, model, physical description such as color, stickers, damage, and customization. Serial numbers are an absolute essential when present as a unique identifier, but should not be the only identifier. For example, if the area is surrounded with images of Legos® and multiple building sets, this would indicate that the person who spends time in this area appears to be a fan of building blocks. You would make a note of this fact in as much detail as you can differentiate as possible. If you are conducting an investigation where other physical evidence will be collected, such as finger prints or foot prints, you need to ensure you wait for the individuals that will be collecting other physical evidence have completed that collection before you move forward.

When collecting a computer you must access it before you seize it. If it is turned on and the user interface is visible, without creating any input that would modify the evidence observe any running programs or content. Document everything you see including the system time of computer with a comparison to another reliable device. If the computer is running the user interface blank, such as sleep mode, moving the mouse does not alter any volatile evidence or hard drive contents. If the mouse doesn't make the computer resume, press the left or right direction arrow on the keyboard. If there is no display or you have documented everything visible you should remove the power cord from the back of the computer and if it is a laptop, pull the battery and unplug the power adapter. If it is a laptop and the battery is not removable, press and hold the power button until the system shuts down. If you know that the computer contains encryption or cannot be removed for any reason you will need to conduct a live investigation which will be discussed later in this book. Time is a very important aspect to the evidence items we will be collecting and analyzing. You should make every effort to document the system time. If the computer is powered on and the user interface is unlocked, check the logical location. In Windows®, the clock is usually displayed in the system tray in the lower left hand corner of the screen. If the system is powered off or you forcibly shut the system down, you can collect the system time from the BIOS or UEFI without booting the operating system. If the system is off you should avoid at all costs of booting the operating system as it will modify the contents of the hard drive.

Collection of physical evidence begins a process called the chain of evidence. It is imperative that all evidence once seized be kept in an environment where it cannot be accessed by unauthorized individuals. If unauthorized access is obtained to evidence an individual could alter, destroy or steal the evidence. As part of the chain of custody process a dedicated form is used to document where evidence is located and who has control of it at all times from the time it is collected until it is destroyed or returned to the rightful owner. A chain of custody form is needed for each evidence item. Additionally each item of evidence must be prepared or packaged to provide easy visible proof that it has not be tampered with or modified.

The methods used for this can vary dramatically depending on the type of item and the resources available to the person seizing the evidence. Some investigators use specialized materials, such as tamper evident bags. Some investigators use brown paper bags, duct tape and a sharpie to seal an item. The purpose is to identify tampering, not prevent access. Physical security from unauthorized access is obtained by locked rooms, vaults, alarms, cameras, safes, personnel to monitor the evidence, or a combination of those solutions.

Almost all of the forms, environments and processes in computer forensics are not standardized. There is no standard universal form used for documenting your investigation or one for chain of custody. There are many public documents made available by organizations like NIST and SANS that you can use or create your own. Creating a forensic investigation program from the ground up is a significant investment in time.

A chain of custody evidence form typically tracks physical location, person who is protecting the evidence or transporting it, dates, times, and a description of the evidence item. It can contain other information, but these are a bare minimum. If you collect evidence and do not track it with a chain of custody form, a defender can easily argue that an evidence item was left unattended, accessible to anyone to modify the evidence. This then progresses to all negative evidence located were aledgedly planted by that unauthorized person. A chain of custody allows a paper trail to prove that the preceding scenario was not possible. Once you have successfully seized the equipment to be investigated it needs to be transported back to location where the investigations will take place. It is important that the individual transporting the evidence not leave it unattended. It should be secured where the transporter can see if anyone attempts to gain access to the evidence. Leaving it in a locked trunk and going out of line of sight is not keeping it secure. It can be left under the surveillance of a known trusted individual if it is documented in your notes. It is best practice to take evidence directly from the scene where it is seized to a secure location.

The collection of evidence listed up to this point is the best possible scenario. There are some additional considerations that might need to be applied when seizing evidence. Volatility and availability of digital evidence is a significant consideration. If simply owning a hard drive was the crime, the instructions that precede this would always be perfect. There are some scenarios where exceptions are needed.

If a suspect started running a program that was destroying data, it would be more important to stop that process first than to document the physical surrounding. If a computer’s hard drive is encrypted turning it off would prevent locating any evidence. If the computer being investigated is a company’s enterprise web server, under most circumstances you can’t unplug it and take it with you. We will discuss most of these scenarios more throughout this book. Under rare circumstances, collection of physical evidence might not be possible or viable. You might be forced directly to collection of digital evidence. The processing of the physical evidence which is not a container for digital evidence, such as a computer, is beyond the scope of digital forensics. We, as investigators, handle the physical evidence for collection and processing of the digtial contents. The steps between poscessing the physical and examining the digital contents can very dramatically on a case by case basis. The general process is usually similar.

Collecting Digital Evidence

Investigators of digital evidence use specialized hardware and software to ensure that where ever possible rule number one, “Do not modify the evidence” is observed. The most common method used to apply this rule is the use of write blocking technologies. Write block hardware and write block software are manufactured by multiple companies and readily available in most jurisdictions including the United States.

The effectiveness of the write blocker must tested and documented in a process known as validation. Validating hardware and software write blocking can be an involved and time consuming process. An investigator must test a known piece of evidence, such as a hard drive, proving that a write block device does not allow any alterations of the evidence. The testing process and the results are recorded and kept as record that the validation was conducted and proved the write blocking works as intended. Testing a USB to SATA write blocker might include connecting a known hard drive to your forensic workstation and attempting to modify files, delete files, copy additional files to the drive. The examiner will then verify after each documented attempt that the write blocker prevented any alteration of the digital evidence. We will discuss the use of hash values that assist in this process later in the book.

The investigator documents the ability of each write block device or software before it is used to conduct an investigation. The validation of the technology only needs to be conducted before initial use or after significant change to the device or environment occurs. For physical hardware modifications such as a firmware update, inclusion of a new feature, use on a new workstation or dropping the device should prompt a new validation. A written, dated record is kept on hand or even included in each individual investigation report.

The validation process is a written documentation that substantiates your efforts to prove your procedure does not modify the evidence. A failure to validate or prove you have validated your write blocking process may cause your process or the evidence to be drawn into question. This doubt may lead to your investigation or evidence being discredited or barred from admission in court.

Investigating the original digital evidence is best conducted on a forensically sound copy of the original. Using the original evidence may lead to contamination, damage, destruction or loss of the evidence physically or the digital contents. Many devices or methods can be used to write block digital evidence. Once a method has been validated, creating a copy of the digital evidence for conducting your investigation where ever possible is important.

Collecting evidence, processing evidence and investigating evidence all require structure to ensure that all cases and evidence are easy to identify and navigate. Naming of physical and digital evidence as well as the investigation cases need to be clearly named. Most organizations that conduct regular or frequent investigations use a naming convention. Using a sequential numbering is the most common method because it helps prevent confusion or exposing information about a case. Using names or types of investigations can lead to unintentional disclosure of information, confusion between cases and difficulty in storing cases long term. A naming convention that starts with calendar year followed by an incrementing number makes tracking and storing cases and their evidence easy. A case named 2015-0012 with evidence 2015-0012A is an example of a naming convention that facilitates ease of storage and retrieval. A case named 'Nielsen Porn' and evidence named hard drive might reveal too much information in a Human Resources investigation or lead to issues if there is another Nielsen investigated for browsing porn at work. Additionally most cases could contain a hard drive. Differentiating between 15 hard drives with no additional detail or differentiation is not easy.

Legal Right to Search and Seize

It is important that we address this topic of legal search and seizure. I can’t emphasize enough that, I am not a lawyer and this is not a legal text. This is not legal advice, it is technical advice. When in doubt, ask a lawyer.

Investigating digital evidence can be a very involved task. It is in your best interest that before you seize anything or begin investigating you have the legal right to do so. I immediately think of the US Constitution and the Bill of Rights when this topic is brought to my attention. If you are assisting law enforcement with an investigation in the United States, they need to either have consent of the owner or a warrant issued by a judge to search or seize anything. An owner or possibly even a third party can consent to a search or surrender an item for seizure. This a very rigid principal with a few quirks and some interesting 'what ifs'. In the corporate world it is a little easier. All equipment and services provided by an employer is the legal property of the the employer; this includes the devices, such as computers, the network and network traffic, the files, the emails, the phone calls place over VoIP. The employer can surrender or has the legal right to examine for any or no right without the employee’s knowledge or consent. There are a few rare and unlikely to encounter circumstances, but I will not even attempt to address or explain, where an employer cannot consent to or investigate the conents of their own equipment.

If your employer tasks you with investigating a work computer, they have the legal right. If they ask you to examine network traffic, from their network, they have the right. They can surrender it to law enforcement without the employee’s involvement or knowledge. It is wise to always ask for requests to investigate in writing. This helps protect investigators from allegations of wrong-doing if they are acting on the behalf of their employer.

If you are involved in an investigation and it is discovered you didn’t have the legal right to search or seize, all evidence collected and analized is not admissible in court. Additionally any derivitive evidence located because of the unlawful search is also inadmissable. This

principle is known as fruit of the poison tree. If during your investigation of a hard drive you discover a location of additional hidden evidence that is a derivitive finding. If there was no legal right to search the hard drive, the additional evidence is also not legally investigated and cannot be used in a court proceding.

This segment is far too brief to complete and adequately discuss legal right to search and seize. It is important to know that you as an investigator will need to be aware of legal issues surrounding search and seizure. I strongly encourage further learning on this topic beyond the scope of this book.

Chapter Three Digital Evidence

Digital Evidence

The aspect of computer forensics that is unique is the nature of digital data. Ultimately, we still conduct an investigation just like a physical crime investigation. We do need to learn and understand the unique challenges of digital evidence. In this chapter we will start with physical aspects and follow logically from hardware to the bits stored inside. There are many reasonable places to start this endeavor, but we will start with binary digits. Binary digits, better known as bits, are the language computers use. All the digital evidence we locate inside of a computer is stored in bits. A bit can have two values, one or zero. A computer takes large strings of 1s and 0s and does that awesome things we all know and love. Photos, emails, text messages and everything else we use computers for is all done in 1s and 0s. Programmers have designed and manipulated those 1s and 0s into brilliant configurations that allows humans to interact with the data without having to deal with any of the machine code. When we investigate a hard drive or the content of a cell phone, we are ultimately looking at the 1s and 0s represented as documents, images, emails or other files. One of the most important aspects of digital is that every 1 or 0 is significant. If any single bit is modified, it might render the evidence useless. We must remember and comply with the first rule of investigation, "Do not modify the evidence". Have you ever lost a file? Had a power failure that 'ate your homework'? Have you ever experienced the dreaded 'crashed hard drive'? Bits are fragile. We are very fortunate, and all of the pioneers of this field have developed means and methods to protect us as best possible from these disasters. It is important that we use the tools available to us to ensure we stick to our first rule.

Spinning Platter Hard Drives

The most logical place for us to start down the path of digital evidence will start with a physical hard drive. A typical hard drive we might find in the average workplace desktop. It is probably 3.5" or 2.5" spinning platter hard drive (HDD). We will eventually discuss solid state drives (SSD) later in this chapter, but for starting concepts, we are starting with traditional hard drives.

When we start our investigation, we seize a physical desktop. We take the desktop back to our lab and extract the physical HDD. We would hook our HDD up to some write block device and use specialized software to make a copy. The software, such as Access Data FTK Imager ®, is designed to make a bit-by-bit copy known as a bit stream image. The software verifies that each bit is the same in the copy as the original. The file(s) created during the bit stream image process typically included multiple verification mechanisms and fail-safes to ensure that all the bits are identical. We take our bit stream image and add it into an examination suite to look at the contents. We will examine this process in more detail in a subsequent chapter. We just need to know there is a method to take the physical evidence and copy the bits without making any changes to the evidence. How a spinning platter hard drive works is an important aspect to investigating a computer and knowing how data is stored and retrieved from a HDD. The way a HDD works has some aspects that apply to all types of storage and key forensic impact. We need to start with a description of the physical aspects of a HDD. Inside of a HDD you will find one or more physical discs known as platters. They are typically plastic or ceramic disks coated with a ferrous coating. The center of the disc is a motor that spins the disks at rates of between 4,500 and 12,000 rotations per minute depending on the model of the drive. The drive has an arm that moves across the surface. This arm is mechanical in nature and has a read/write heads on the end of the arm on both sides of each disk. The arm moves to the appropriate location to access the correct physical spot to read or write as needed. The disks have a series of magnetic tracks, like concentric circles, and dividers placed on the disks to hold bits. The areas place on the disks during the manufacturing process are known a sector. Sectors are 512 bits for drives up to 2TB in capacity and 2048 bits for drives larger than 2TB. The bits are recorded as a positive or negative charge and written to the correct sector. The drive has a chip to associate a physical location to each sector. image::https://lh7-rt.googleusercontent.com/docsz/AD_4nXfVCe4kVqlDm8qqEFpS0p95Qq9KNjxDYLqinC-nkGCtMXRHxeXhlTHeHyVtgm1igWPoQLHCpL_Um2fweVjtMavSLlINNnalX-17tQpp-CKt20ncd5LdHLMPeTwEtNJcFItmCRvJPkpCxbXDCV405UkFE54?key=sowrcUWignI3XSpATxH3kQ)

Image courtesy of Wikipedia.org

File Systems

The operating system of the computer, for us we are using Windows 7®, does not interface directly to the hard drive for reads and writes for normal operations. The drive is formatted with a file system. The files system acts as an intermediary between the physical disk and the operating system. In Windows ® the default file system is NTFS. There are some aspects of NTFS that are unique, but we will start with the general 'most file systems' and discuss NTFS specifics as needed. The file system tracks files. Formatting a HDD creates clusters. Clusters are logical and where possible, physical grouping of sectors. 4 kilobit (kb) clusters are very common amongst most file systems and the default for NTFS for drives under 2TB in size. The size of a cluster can be customized during the format process ranging from 512 bits to 64 kb in NTFS. The formatting process creates a table of clusters and what is stored in that specific cluster. The files system communicates to the HDD to read or write to a specific cluster. The command comes to the HDD to start at a specific sector and the drive moves the arm to the correct physical location. You may have noticed when you format a hard drive, the available size is less than the physical drive size. When a drive is formatted with a file system, that file system requires space to track each location and what is in that specific spot, even when empty. Additionally, the file system can record information specific to the file such as the date and time the file was created, lasted accessed, last modified and even in NTFS which user account owns the file. These supplemental pieces of information, created and maintained by the file system, is called metadata and can be invaluable to investigators. The useful information that will help us prove or disprove the allegations we are investigating lies inside the files stored on the HDD. The physical evidence gives us access to the bits. The bits give us files. The files contain the artifacts that we can interpret and report. Hopefully you are super sharp, and you are thinking, "Hey! What about files that are larger than 64 kb, the maximum size of a single cluster in NTFS?". The answer is easy! We use more than one cluster. The HDD and the file system break the file into fragments that fit into clusters and the file system tracks each fragment. When the file is being written to the drive into multiple clusters it is common for the clusters to be in physically separated areas. This by product of writing a large file into physically separated clusters is known as fragmentation. Fragmentation can slow down the read or write process significantly. Most operating systems have a utility to try and re-arrange files, so they are less fragmented. When we look at this from a forensic perspective, it is neither a positive or a negative, merely a fact we must be aware happens.

Sectors and clusters functionality and how file systems interact with the physical drive create some interesting forensic possibilities. The most common and useful quirk of hard drives is deleted files. When a user deletes a file and in Windows® empties the Recycle Bin, the file is not gone. You have likely seen or heard of undeleting files. This concept of restoring deleted files in the forensic world is known as data carving. The process of deleting a file is the key to understanding how it is possible. This process is in general identical for all operating systems and file systems. When the operating system deletes a file, it tells the file system the file is no longer needed. The file system then marks the cluster(s) as empty and available to be written to again as needed. Clusters that are not associated with a file are unallocated. The file system does not do anything with the actual cluster contents. Data carving looks at each cluster trying to identify files that might be physically present, but not listed in the file system. The results of data carving can provide great results or nothing of value.

The file system clustering system also has issues surrounding contents of a cluster. The most file systems, including NTFS, only track one file or fragment of a file per cluster. This leaves the possibility of empty space inside of a cluster. If you save a 5 kb file on a hard drive with 64 kb clusters, 59 kb of the cluster is unused. This unused space is known as slack space. If we also consider that a deleted file is not overwritten or removed, that slack space could contain 59 kb of another file. It is possible that the remnant of a partially overwritten file might contain useful information that might be evidence to support the allegations we are investigating. NTFS has some unique characteristics. The study of the forensic aspects of NTFS warrants a complete textbook to itself as a standalone topic. There are some things we must know for our introductory purposes. NTFS is a journaling file system. This simply means it tracks changes in a log. This log file is $MFT and sits on the root of the drive. Unfortunately, we cannot just open it up and read it as Windows® is running. If we could, it wouldn’t be very people friendly to look at the contents. This journalling aspect helps the process of data carving to be more successful. The contents of $MFT indicates recent writes and deletes along with where the files are or were. NTFS also handles small files uniquely. The file can be stored inside $MFT if it is a small file. This prevents a cluster from being allocated to a small file and wasting space as each cluster can only be associated with one file or fragment of a file.

Data Destruction

It is also important we discuss data destruction in this section. If a HDD is physically damaged the normal read process is not possible. Specialized equipment might be able to read data from the platter of a disk that has a bullet hole in it or a platter that is bent. The data recovered from a physically damaged disk might not contain any intelligent content or it might recover evidence that supports the allegations. This is an extraordinary effort, but plausible for the right scenario. It is not realistic for an average investigator to be able to attempt to recover data from a damaged drive. The cost and time involved in attempting to recover data from a damaged disk prevents most organizations from attempting to use damaged HDD as evidence. A common method to erase HDDs is to use a powerful magnet to remove the magnetic tracks that separate and contain the positive or negative charges that represent 1s and 0s. This process is known as degaussing. If the magnet is powerful enough the data is gone, and the drive can no longer retain any data.

Deleting data can be accomplished by overwriting the current data. This is for all practical purposes unrecoverable with a single over-write. The ability to see the last seven states of a bit can be achieved if the platter is examined with an electron microscope. It is theoretically possible to read all seven previous states of all bits on a drive and reconstruct any data that was on the drive for the past seven writes. This process is not realistic because of the resources needed to accomplish this task and find useful information is not possible. The process of reads all the bits in each of the seven previous states then attempting to reassemble them in order is mathematically unachievable with modern computing power. It is however considered by entities with very sensitive data, such as military secrets, to be a possibility. As a result of this there are data erasure standards and utilities that will over-write each bit seven times to ensure that no data can ever be recovered. All methods of examining that do not include the use of an electron microscope, a very expensive piece of equipment, over-writing a bit one time makes it truly deleted.

Data destruction is a common occurrence on modern drives without users knowing that it has occurred. Defects in disk surface is a common problem. The precision of a physical disk with platters is phenomenal. It can read, write and move to .005mm at speeds of 10,000 rpms! Drives have trillions of bits. This is truly amazing. But the manufacturing process is not perfect and areas on the platters might not be high enough quality to endure that type of environment. Bad sectors happen on modern drives regularly. When a drive cannot read or write to a specific sector, it will identify that as a bad sector and substitute it with one of many spare sectors on the drive. Most drives ship with as much as ten percent extra space reserved for replacing bad sectors. These spare sectors are not accessible by normal means and are not part of the calculated available or used space in a drive. This technology is known as S.MA.R.T technology. It doesn’t change our approach but know that the tools we will use address these bad sectors. The software will attempt to read all accessible areas. Solid State Drives Solid state drives (SSD) have most of the same aspects as a spinning platter drive. Instead of platters, it has memory cells etched in silicon with a membrane that allows the charge to pass into the cell. This membrane has a limited life span and can deteriorate with use. Most modern drives can be written constantly for years before they fail, but it is a consideration in some technological respects. The cells are grouped together physically and logically. SSDs have sectors and is formatted by a file system into clusters. They are faster in read and writing times and less prone to mechanical failure as there are no moving parts. The cell and membrane aspect does create one phenomenon, known as write amplification, that does have a potential impact on digital forensics.

Over time SSD cells fill up with data. As the data is deleted by the file system the charges remain in the storage cells, just like on a spinning platter drive. When the drive attempts to write to an area that has remnants of previous files, it must negate what is there to a neutral state before it can write the data desired. This effect is compounded in multi-layer storage because charges may have to be submitted several layers deep before it can write. The speed of drives slows dramatically the longer it is used. SSD manufacturers developed an ATA protocol standard to address this phenomenon. The protocol is known as Trim support. Most modern solid-state storage, including storage in phones and tablets, support Trim. Trim support initiates a request from the operating system to the drive to clean up unallocated space before it is needed again. This effectively erases any files that we previously would have been able to successfully use data carving to recover. The implementation of this is non-standard at the operating system level and can occur at any time. Once the command is sent to the SSD it is executed 'as drive activity is available'. It is possible that you might remove an SSD from a suspect computer, hook it to a write blocker and begin to copy the contents as the Trim is activated. It is highly unlikely this will happen, but deleted files tend to be gone for good quickly in SSDs where Trim support is enabled, and the operating system supports Trim. Hashing Functions Now that we have discussed where the 1s and 0s are, how we access them and some of the quirks of data on drives, we need to go back to rule number one, 'Don’t modify the evidence'. We are fortunate that there is an established technology in use by investigators today that helps prove that the 1s and 0s are unmodified. The technology is known as hashing functions or hash functions. The most common hash function used in digital forensics is the MD5 hashing function. A hashing function performs a mathematical manipulation of data in fixed lengths. MD5 calculates 128-bit blocks. It is an iterative process that starts with a fixed length value of 128 bits, does bit level math and generates a result of 128 bits. The result is then used as the value to compare to the next 128-bit block of data that is being hashed. That result is used to compute the next block. The process repeats until the end of the file. The final mathematical calculation will add zeros to the end of the data until it is equal to 128 bits. The result is 128-bit string that is unique to that file. A practitioner can verify that all the 1s and 0s are identical between the original and the copy (or before and after) if the values match. Hashing functions are one-way functions. This means that you cannot recreate or predict the original content. The result of a hash function will always give the same result if you put in the same input. A single modification of one bit or character give a dramatically different 128-bit value. The results are not predictive. Any length of data can go into the function and will receive a unique 128-bit result. We can perform a hash value calculation on an 8 TB hard drive or a 6 KB digital image. Both will have 128-bit values that are unique.

Mathematically it is possible for two different chunks of data to have the same resulting hash value. This is known as a collision. There are only 340 billion-billion-billion-billion possible MD5 hash values. If I have 340 billion-billion-billion-billion and one files, two will have the same MD5 hash value. Forensic software and investigators also have used SHA-1 hashing function to calculate a second unique value for each file. It is mathematically infeasible for two files to have collisions with both algorithms as SHA-1 is 160-bits and MD5 is 128-bits. Sadly SHA-1 has recently been cracked by a group of researchers and they have developed a method to manipulate the content of data and generate the same SHA-1 value, so it is no longer considered a trustworthy hashing function. It is likely another hashing function will replace it soon. Identical hash values verify that all the bits of both data items are identical. This concept is proven and accepted as fact in a court of law. Ultimately all the 1s and 0s are what we work on. What we see, what we collect, what we interpret and what we present is in a far friendlier format, files. The key to every investigation is to locate files, look at what is inside the files and explain it to our requestor what is present in the drive. Files and how they are composed is dependent on the type of file or the type of application that use the files. A digital image might have one of many formats. Each of those formats is unique. The same would be true for text documents or audio clips. The formatting or type of file in Windows® is often identified by extension. Extensions allow Windows® to associate a type of file with a specific application. All files have data near the beginning of the file, known as file headers, that identifies the type of file that it is. Most other operating systems use file headers to associate a file type with an application. Learning which files contain the artifacts we need to locate and interpret to provide evidence to the requestors is the key to a successful investigation. In subsequent chapters we will look at some specific files and if you are following with the hands-on labs, you will have the opportunity to learn some useful files and their contents.

Chapter Four Investigating Digital Evidence

Investigating Digital Evidence

Investigating the digital content of a computer is unique. The ones and zeroes previously discussed have a lot of frailty and challenges. Pioneers in this industry have helped us with tools and methodologies that take away most of the true challenges. We as investigators still need to understand what we are looking for and how to find it to be successful. When we simplify the much larger concept of digital forensics, we are talking about files and the tools to locate, open and view the contents of files.

Files

The name 'file system' gives us the insight of the role of a file system. It helps a computer to store and locate files. Operating systems and applications are comprised of files. They both use files to store data to make the user experience more pleasant and useful. We as investigators cannot know every type of file ever created nor should we be expected to know every file included in the Windows® operating system. There are several informational items about files that can help us to better understand, locate and view the content of files where possible.

Structure

All files have similar structures. They all have a beginning, content and an end. The content is what we most often seek to obtain. In a text document, the content is text of some type. The text might be a grocery list or a manifesto. The content may be easy to view or may require an application. Some files such as binary files are not intended to have to contents viewed, but instead are intended to be executed and perform some function, such as a calculator application.

Files are typically identified as one of two types, binaries or data files. Binaries can be executables or dynamically linked libraries. They can be data files can be a vast number of possible types of files. Some common types of data files can include user created storage for an application, an archive of multiple files, or information for an application or operating system to use.

When an operating system or application creates a new file, it uses the appropriate format for that specific type of file. The start of a file is the file header. The file header is unique to each file type. The first four or five bytes of a file identify the file type. In Windows®, file types are identified by the extension of a file. The file example.bmp has an extension of bmp, a common digital image format. The first four bytes of a bmp file would be represented in hexadecimal as 42 4D F8 A9. This unique value is associated with bmp files. Operating systems such as Linux or MacOS associate a file by the header, not the extension. It is a common approach to examine the header of files in a forensic investigation. It helps in the data carving process as well as identifies file that might have been altered by an end user in an attempt to hide data from a casual user. Extension mismatch is the practice of changing a file extension in Windows® to prevent the correct application from opening a file.

If we take the same example.bmp and rename it to example.docx, Windows® will try to open the file with Microsoft Word®. The application will not be able to open the file properly and a casual user would think the file corrupted or broken. Most forensic investigation suites will identify the example.docx with the header of 42 4D F8 A9 as a mislabeled bmp file and likely highlight it for an investigator to examine as a suspicious file.

Headers start a file, the content of the file the computer uses is in the middle and the End of File (EoF)sequences end a file. Most files have a simple EoF character. This character is also used in data carving. The carving process looks for the header and the EoF. The carving utility then takes everything in between and places it all back together as a single file. As discussed earlier, the process is not always reliable. The header and the EoF may be from two separate deleted files. The size of data in between header and EoF could be Terrabytes of data.

File Uniqueness

Identifying or locating files and examining their contents is the key to a successful investigation. The ability to examine a file and determine when it was created, last modified, and to identify that it is a copy of an original file are all valuable pieces of information an investigator should collect during an investigation. Metadata is information about specific data. Metadata is created and stored in many ways in a computer. Information such as file creation date and time is generated and kept by the file system for every file. Information such as the make and model of a camera used to take a digital photograph can be embedded into the save image. This embedded data is also metadata.

Hash Values

We discovered hash values in the Digital Evidence Chapter. Each 'chunk' of data has a unique hash value when a hashing function is applied to that 'chunk' of data. If the 'chunk' is modified in anyway, the hash value of the 'chunk' changes as well. This concept is true with files, folders and drives. Each file has a unique hash value. The most used hashing function is MD5 in the digital forensic industry. We established that we could use a hash value of a drive or file to prove it has not been modified. We can also use that idea to prove an unmodified file is not of interest to us as investigators or that the existence of a file that matches a known value is important. When a software publisher, such as Microsoft, releases an application or operating system, their software can be comprised of hundreds or thousands of individual files that are copied to your computer. The installed software has the exact same files for every installation. They will have the same hash values after every install. We can use a database of known files to hide files that came from the publisher and have not been altered. How that is achieved is different in each software suite, but most advanced forensics tools have identifying known files as an option. The National Institute for Standards and Technology maintains a database of known files from major publishers. This database is known as the National Software Reference Library (NSRL) and is available for free download. The NSRL is updated and published approximately every six months.

The presence of a known bad or problematic file is also something that can be very beneficial to investigators. The gruesome example is the database maintained for law enforcement that contains hash values of all previously confiscated files containing child pornography. If the investigation suite has this database, the software can identify child pornography by hash value without having to view the contents of the offensive material. The same concept is often used for viruses and malicious software.

The hash value of a file will be the same for every exact copy, even on different computers. The content of the file is the portion that is processed by the hashing function. Some of the metadata can be changed without altering the contents of the file. We can rename the file, and the hash value of the contents will remain the same. We can copy the file to another computer. This process will give the file a new created date on the target computer. This will not change the hash value either.

Metadata

As previous mentioned files can have multiple types of metadata. The types and amount of metadata varies by the application that creates or modifies the file.

There are two primary types of metadata that you will encounter. The first type is embedded in files the second type is created and maintained by file systems. When you start to look at files many of them have data embedded in them there are several types of metadata embedded there are descriptive metadata fields, technical metadata fields, and rights metadata fields. Descriptive metadata might contain information such as the title of the document, the author, creation date, and keywords. Technical metadata might contain information such as a file type, file format, resolution, bit depth, codec information. Technical metadata might also include data such as program modified or created with, data rate, the model of a camera that took a picture, the GPS coordinates of where an image was snapped with a smartphone, file size, and time last modified. Rights metadata might contain copyright usage right licensing information and watermarking to identify ownership.

It is worth noting that some applications will modify file metadata as a method of tracking changes, such as MS Word documents the amount of time that a document has been opened for modifications or when it was last saved. This is important to note as something as simple as viewing a document in a method that can read and write might modify the contents of a file. In general, most metadata inside files is write-once read-many.

File system metadata is generated and tracked by the file system in which the file resides. Each file system tracks file information such as file name, logical location, physical location, file size, date and time created as well as date and time last modified. Some file systems can be customized to track other data that the administrator identifies as important. Most modern file systems also include data about ownership of a file, permissions to a file, dates and times accessed, and even tags or comments. One common question that I have received when conducting hands-on labs is “How can a file be modified before it was created?" Based on file system metadata, a copy of a file from one disk to another is creating a new file at the time of the copy. The file system may copy the remaining metadata of the original file. If the file was modified yesterday and copied from drive C: to drive D: today, it was modified before it was created according to the file system. This means that investigators must understand how to interpret metadata correctly.

Investigation Tools

Investigation requires specialized tools made for forensic investigation as well as non-forensic tools that can be used for forensic purposes. We will discuss some of the most common tools used in the industry. We will start with forensic suites of specialized software. Multiple organizations have developed forensic suites that are used by law enforcement, government agencies, and private industry. These suites are designed to be used by trained forensic investigators. The suites are designed to be used in a forensically sound manner. This means that the software does not alter the original data and that the software can be used to testify in court. The suites are designed to be used in a forensically sound manner. This means that the software does not alter the original data and that the software can be used to testify in court. The suites are typically multiple tools that are integrated into a single interface to aid in the consistent and expedient investigation of digital evidence.

Software for investigations

There are many software tools that can be used to investigate digital evidence. Some of the most common tools are discussed below. It is very important for students and potential practitioners to understand a few important aspects of digital forensic software and investigations. Software is not a replacement for a trained investigator. The software is a tool that can be used to assist in the investigation. The software is not a magic bullet that will solve all problems. Investigators should never learn how to use a software or conduct and investigation on a technology for the first time on a real, formal investigation. You may be forced to delay an investigation while you learn a software or environment you will be investigating by conducting practice investigations to develop a formal process, but in the long run it will preven mistakes or introduce the possibility that your skill and integrity into quesiton in court. It is also critical that investigators strictly adhere to software licensing. Over my many years of instruction, I have had many students that have a dislike for comercial software. They often ask if they can use a pirated version of the software. The answer is always no. If your invesgtigation would ever be used in legal proceeding all evidence could be ruled as inadmissible as it was obtained unlawfully or even potentially obtained illegally. Futhermore, the investigators involved might be personally liable for copyright violations that could result in extremely large monitary penalties and potential criminal processecution. The last item of noteworthiness is that not all tools used in a forensic investigation are designed to be used as forensic tools. It is possible that some element of your investigation will require that you use non-forensic tools to conduct the investigation into a specific evnidence type. This is not ideal, but it is a reality of the field. It is important that you document the use of non-forensic tools and the results of their use. This documentation will be critical if the investigation is ever used in a legal proceeding.

Forensic suites

In this category we examine software that tries to provide a complete solution for digital forensic investigations. The software is designed to be used by trained forensic investigators. The software is designed to be used in a forensically sound manner. This means that the software does not alter the original data and that the software can be used to testify in court. The suites are typically multiple tools that are integrated into a single interface to aid in the consistent and expedient investigation of digital evidence. Some of the most common forensic suites are discussed below. In general the software in these categories have been validated and vetted in the legal system. Expert technical witnesses have testified to the validity of the software and the results of the software. Once a software and how it is used is on record as vetted by a technical expert, an investigator should not be questioned regarding the software and the results of the software. This is a critical aspect of the forensic process. The legal team only need to reference the prior case where the resutls were established as valid.

The original commercially available digital forensic software was EnCase. It was and in general is still considered to be the baseline for crimial investigations. The software has evolved of the years and is now integraded with other case management tools owned by OpenText. It can perform almost all typical forensic investigative tasks and has a large user base. The software is expensive and requires training to use effectively. The software is used by law enforcement, government agencies, and private industry. The software is used to investigate a wide range of crimes and infractions.

Another longstanding forensic suite is the Forensics Toolkit or FTK. AccessData developed FTK as a series of tools that were an early competitor to EnCase. The software is also used by law enforcement, government agencies, and private industry. Similarly, it has merged into a larger bundle that includes case management tools and is now developed by eXterro Softare. This software is also expensive.

Autopsy is an open-source forensic suite that can be used in lieu of the other expensive commercial forensic suites. The software is free and has a large user base. This suite does lack some features that are found in the commercial suites, but it is built on a framework that allows for anyone to develop and implement tools. New tools might fall under scrutiny in a legal proceeding, but the software is still a viable option for many investigations. Typically the creator of the tool would be called as an expert witness to testify to the validity of the tool and the results of the tool. If you develop the tool and use it in an investigation, you would be the expert witness.

Specialty software

There are many types of tools available to assist in forensic investigations that are specialized for a specific type of investigation or evidence type. Some of the most common types of tools are discussed below. The following list is far from complete, but it does provide a good starting point for an investigator to begin to understand the types of tools that are available.

Browser software

Many investigations might focus on a suspect’s internet browsing activities. There are specialty tools that can be used to examine a suspect’s browsing history. Since web browsing involves downloading and viewing of files from web servers, it would be logical that the files would be stored on the suspect’s computer. The files would be stored in methods consistent with the browser in question. The larger suites listed above have tools that will look at individual files related to web browsing, but none of them provide a complete solution for web browsing. The tools in this category are designed to provide a complete solution for web browsing investigations.

Chat software

Some investigations might include chat conversations that occur on private or corporate networks. There are specialty tools that can be used to examine chat logs. The tools in this category are designed to provide a complete solution for chat log investigations. The larger suites listed above have tools that will look at individual files related to chat logs, but none of them provide a complete solution for chat logs. The tools in this category are designed to provide a complete solution for chat log investigations.

Text message software

some investigations might include text messages that occur on private or corporate networks. There are specialty tools that can be used to examine text messages. The tools in this category are designed to provide a complete solution for text message investigations. The larger suites listed above have tools that will look at individual files related to text messages, but none of them provide a complete solution for text messages. The tools in this category are designed to provide a complete solution for text message investigations.

Investigative Hardware

The key element of digital forensic investigation hardware is the concept of read-only. The effort to ensure that evidence is not modified, is achieved using write blocking technologies. In general there are solutions for all types of media that an investigator might encounter. An easy example of a media that might be investigated is a hard drive from a desktop computer. Depending on the model the drive could be connected via SATA, SAS, IDE, USB, Firewire, Thuderbolt, PCIe, or even older interfaces depending on the age of the device being investigated. It is commonplace to use a write blocker that is connected between the drive and the computer that is conducting the investigation. The write blocker is a device that is designed to prevent any writes to the drive. The write blocker is a critical piece of hardware that is used in every investigation.

It is also worth noting that an investigator will typically have a workstation that is build of commercial off-the-shelf computer parts in addition to the write blocking devices.

Forensic investigation workstations

This is a dedicated computer that can be used to capture evidence, process the evidence, and investigate the case while adhering to forensic principles of not modifying the evidence. It is possible on a limited budget to purchase a standard PC and use it as a forensic workstation. The key is to ensure that the workstation is not connected to the internet and that the workstation is not used for any other purpose. Collection or acquisition of evidence can be completed using a write blocker and a forensic suite. The workstation can be used to process the evidence and investigate the case. It is noteworthy that forensic suites process the bits on an evidence drive looking a all bits to identify data a low level to ensure all potential evidencie is identified. This process is extremely time consuming and requires a powerful workstation. Resources such as CPU, RAM, and GPUs are critical to the performance of the workstation. It is not uncommon for workstations built for forensic investation to cost over $8,000.00 without any software. I typically recommend that student look at 'F.R.E.D' from Digitial Intelligence as a good example of what a digital forensic workstation look like.

Mobile Forensics

I have opted to keep this section separate. Mobile devices are a unique challenge for forensic investigators. The devices have a wide range of proprietary hardware and firmware. Additionally as mentioned in the anti-forensic chapter, encryption can stop an investigation in its tracks. Most modern cellphones are encrypted by default. Therefore obtaining evidence from a locked device is extremely difficult. The process of obtaining evidence from a locked device is called unlocking. Few tools are available to unlock a device. The primary solution in this area is Cellibrite. It is an all-in-one solution that is primarily used by law enforcement and government agencies. The software is expensive and requires training to use effectively. Cellibrite is selective as to who it will sell their solution. If an academic entity to aquire a Cellibrite solution, we are required to attend a trining bootcamp and purchase the device at retail cost in excess of $12,000.00 as of the writing of this text. For this reason, we will not be discussing mobile investigations.

Chapter Five Anti-Forensics

Anti-Forensics and Data Hiding

Most people who knowingly break the rules don't think they will get caught. This is also true for most computer users. The handful of rule breakers and troublemakers rarely take into consideration they might get caught. If they are careful enough to try and cover their steps. When these attempts at countermeasures are applied to a computer, it is generally considered to be anti-forensics. I like to use the term data hiding as it is often a more realistic description. The popularity of shows like NCIS, CSI and Criminal Minds have exposed most of the people you might investigate to some of the ways they might get caught or how investigators locate evidence. They might Google how to delete data or hide photos. In general, most computer users lack the technical understanding to truly prevent a successful investigation.

When a person is using a computer and are worried, they might be caught doing something they shouldn't be they typically apply some common, simple protective measures. Often these measures will stop other simple users, but very few can avoid an educated investigator and standard forensic investigation software such as EnCase, FTK or Autopsy. The number of individuals that might take anti-forensic measures is small, I have often heard low single digit percentages. This small percentage might be some of the worst offenders or at the least, for most of us geeks, the exciting part of investigating. The presence of data hiding techniques is an evidence item in and of itself. It usually indicates that a user is doing something they know they shouldn't be taking measures to hide their actions. This might be significant for someone that has requested an investigation to determine if the person being investigated is acting intentionally.

Data hiding or anti-forensics is also very commonly seen in incident response involving complex hacks. In this book I will not spend notable time discussing this portion of forensic investigation, it is a very rapidly growing career and high demand skill set.

When we try to identify data hiding, we have multiple factors to consider. The first and most effective method is to understand the person being investigated. User skill level and motivations are the two most significant indicators of possible anti-forensics. Most users have limited knowledge of computers and how they operate beyond the normal use, such as web browsing and using applications. Some individuals have a much stronger understanding of how data is stored on a computer. The stronger their technical understanding the more likely they can identify advanced and effective techniques and apply them properly. Most individuals that break the rules are not facing prison time, at worst an upset spouse or supervisor. Their motivation is based on not getting caught and the severity of the penalty if caught might directly impact their effort to hide. Another factor in their motivation is the entity that they are preventing from locating their activities. If they are hiding data from a nosy neighbor or snooping spouse with basic computer knowledge, their efforts will be far different than trying to hide data from law enforcement.

We might examine the average computer abuser. They call for help when their shortcut disappears because the application is "broken". Their infraction might be using their work email to sign up for and use the web site Ashley Madison. They would rather risk their job than the wrath of their significant other if they are found out.

My favorite example on the other end of the spectrum is Joseph E. Duncan III, convicted murder, kidnapper and child predator. Duncan studied computer science at North Dakota State University. He kept a journal of his act ivies for his own perverse reasons. He knew enough to encrypt the content with a strong passphrase to keep it safe from everyone, including the FBI. He had the knowledge of what and how to protect the information and the motivation to do so.

Another indicator or limiting factor for the deployment of anti-forensics is the available resources. An advanced user can easily leverage tools to help hide data. The presence of software that is used primarily for data hiding is a clue for investigators that they need to keep their eyes open to possible anti-forensics. In law enforcement this might process might extend to warrant requests as well as altering search and seizure tactics. Some environments users might not have the luxury of installing software or using tools that require superuser permissions. This might not prevent the attempts to hide data, but it helps us to rule out certain types of data hiding. One of the last items to consider with anti-forensics is time. Does the person being investigated have the time to enact countermeasures? Does your investigation identify a timeline indicate or rule-out the likelihood of data-hiding? It is entirely possible that even if certain data-hiding techniques are possible, other supporting evidence eliminates the need to recover or unhide data if their actives and timeline can substantively provide adequate evidence. Passwords are the most common way for a computer user to try and hide data. Given their limited understanding of how data can be accessed, their belief that data is secured if hidden behind a password. In some instances, this is true, in other instances it is not true. It is directly related to the type of method of hiding that the password is associated with.

The most prevalent password, or in the case of many portables a pin, is the operating system password. Microsoft Windows prompts users to create a password during initial setup of a computer. They encourage the use of an online account for several reasons. This action of setting up and account with a password doesn’t indicate intent to hide data, but it can easily be leveraged for the purpose of perceived hiding. To a regular user, the data inside of a computer is only accessible if another person knows their password. In a home environment with only one enabled administrator account this may be closer to true if the computer and drive is only available through the operating system. Investigators do not use the operating system, except in cases where copying the drive might be impacted by encryption or failing equipment. We will use a third-party solution, hardware or software, to copy the drive or investigate it as a secondary drive using write blockers or bit-stream copies. Standard users do not know that the data on a drive can be accessed outside of the computer or via alternate boot method.

Passwords can also be used to protect folders and files. Typically, this associated with a third-party application such as PGP, GPG, or 7-Zip to achieve password protection of a file or folder. These programs use encryption and provide a near-unbreakable protection of the protected files or folders. Without knowledge of the password or passphrase, properly applied encryption is undefeatable. A weak password or passphrase is the only feasible method to recover these items. These protected items might also still be present on the device in an unprotected state. Duplicate files are a common user mistake that defeats their encryption efforts. Folder and file encryption applied at the file system level is tied back to the operating system (OS) authentication. It can be effective at preventing unauthorized access, but is tied directly to the OS level password, which may be susceptible to password recovery software more readily than decryption attacks against applications such as PGP, GPG or 7-Zip. Passwords are also a method to protect files and applications. A program such as Peachtree Accounting to prevent users from opening a file without the correct password. The application may or may not include or incorporate encryption. It is dependent on the application and possibly the options selected during file creation or save time. Correctly implemented encryption will prevent recovery, other than weak password guessing or recovery. Most modern applications that include a password protection solution for privacy will include encryption.

Most users will select a password that is easy to remember, such as something personal. It is likely that the password or a minor variant, such as the addition of a number to the end of the word, will also be present on the computer. Creation of a dictionary from the bit-stream copy is possible and advisable. FTK has a function integrated into the suite to generate a list of every string of characters between whitespaces to create a dictionary to guess passwords. Another common method of data hiding is file name and attribute manipulation. Users with general understanding of computer files can engage in several methods to hide data. Most of these methods are ineffective when investigated with common digital forensic tools. Users that are knowledgeable enough to deploy these anti-forensic countermeasures will frequently thwart other limited skill users.

Power users with file attribute knowledge might employ a tactic known as file extension mismatch. The simple action of changing a file extension makes the file unusable on a Windows computer. The reason this effort is successful is rooted in how Windows associates files by their extension to a default application. A change of extension will change the default application that will attempt to open the file. A double click of a file will initialize the application that is associated with the extension of that file. If the application does not know how to open the true file type it will generate an error, and the contents of the file will not be displayed. A more skilled user can open the file with the appropriate application or rename the extension. Forensic software identifies the type of file based on the file header and compares the extension. If there is a mismatch the software will identify it as a potential item of interest.

Additional methods used to hide files is to use the file system to identify files as hidden or system files. To an average user, these files would become invisible. A technically astute person would simply know how to unmask or unhide these files. Forensic investigation software ignores these attributes. A simple method of data hiding includes file naming and location. A deceptive name may throw off many nosy spouses or bosses. The ability to search by key words or examine dates accessed or modified help investigators to easily locate files of interest.

A knowledgeable user may try to hide files by placing it in locations that other, non-technical users would not likely look. Locations such as the system directory or program files folder might be areas that will be safe hiding locations. Another common type of hiding includes creating multiple sub-folders from a common or uncommonly used folder. This approach often couples well with hiding files in locations with large numbers of similar files. A determined user may combine multiple methods to further hide files from other common users. Depending on the content or data that a motivated user might be trying to hide, embedding data or files into other existing files is a possible attempt. Data such as images can easily be embedded into text documents, presentations or archive files. They can be files created just to hide or files that had other purposes when created can be used to help hide from normal users. Investigation software helps to identify files by filtering by dates accessed, created, key word searches or file sizes.

Common users as well as advanced users might use the ability to take their data with them to help hide it from prying eyes. Removable storage such as USB thumb drive is an easy method to take the evidence with you. This might not be a sign of hiding, so much as a method of convenience and control of their documents. This concept extends to cloud or online storage solutions. A note to examiners. Online storage is protected from investigation without a warrant or consent if it is a personal account. Even if an employee accesses it from a work computer on the work network, you cannot access their account legally without consent or search warrant. Frequently I have students that will discover a password for an online resource. They expand their search to include that online resource. Their actions are potentially criminal, violating the Computer Fraud and Abuse Act.

More advanced techniques of data hiding include using specialized tools to place data into files or on unused locations of a storage media. The most discussed method is steganography. Hiding data in plain sight is a basic definition of steganography. The ability to place data into another file without modifying its appearance to the naked eye is not uncommon. Modern digital cameras embed metadata into images. The quality of the image is not impacted, but the data is easily viewed with metadata reading software. Steganography has a much more complex method.

Almost any type of file can have data embedded into it using steganography techniques. To explain it I will give a simple explanation of how text might be embedded into a digital image without modifying the visible appearance of that image. A digital image has 32-bit color depth. A ten-megapixel camera has ten million 32-bit color dots. The human eye can identify color at roughly a 24-bit depth. The last eight bits have no impact or value to a person viewing the image. A program can simply overwrite the last eight bits with hidden data. You could potentially have 80 million bits to use for data hiding. This is a very simplified explanation, there are a notable number of potential issues, such as compression, that I will not factor into this basic explanation of steganography. Compression in modern digital image formats has an impact on applying this concept but doesn't prevent it. I have already covered this when discussing passwords, but encryption is worth a quick recap. Users with something to hide or a significant interest in protecting their privacy will select encryption to hide their data. Appropriately applied encryption with a strong passphrase is for all practical purposes undefeatable. Even with this fact, few people can use encryption to protect against entities like intelligence agencies and law enforcement.

Chapter Six Report Writing

Report Writing

The culmination of an investigator's efforts is presenting their findings to the entity that requested the investigation. The process of synthesizing all your findings into a refined easy to understand yet detailed enough to provide all the details of the investigation is a daunting task. Most incidents that evolve into an investigation have potential impacts for the entities being investigated, the entity requesting the investigation and you as an investigator. The best tool to ensure that the facts you discovered and preserved are conveyed to the requester. This transfer of knowledge allows the requesting entity to make informed decisions about how to proceed with the investigation.

The challenges faced by most technical professionals involve taking very technical information and providing it to a non-technical person without losing the value of the findings. When writing a report or presenting your findings most entities do not have a form or template. Usually, it is up to the investigator to craft this document from scratch or based on previous reports. The ability to find data in an investigation is important, but a truly skilled investigator is one that can put their findings into a format that anyone can read and understand the results of your investigation.

In addition to providing your results to a non-technical requester, they will often share the report with other entities, such as a prosecutor sharing the report with the defense, to review or critique. The investigator should also include in the report the technical information for another investigator to be able to replicate your findings from the same evidence.

Composing the report is a balancing act of sorts. You should take care to avoid including editorials, showing bias, drawing conclusions or providing any information other than the facts you have located in the evidence. The challenge to this task is often what you locate during your investigation is often interpreted or explained using your expertise as a professional.

An example of this process might be when looking at browser artifacts from a hard drive you are tasked with investigating. You might locate images from the cache files and URLs from the history files. You can piece together where a person might have been browsing and identify some content of the pages they were visiting. You are expected to piece this information together and present it as what likely occurred when someone was using the computer being investigated. Based on that evidence alone you cannot identify the actual person that was using the computer. You cannot identify their intent or motivation. You only have evidence to support the facts that someone used that computer to go to a website and what kind of content was present during that session. The investigation is requested and directed by an entity, typically your employer, your client, or perhaps even an organization that you are volunteering to assist. The very nature of the relationship between you and the requester, creates an interest in supporting this organization. This bias that might be present is a source of scrutiny for opposition. It is important that your findings you do not present option or material that can be discredited based on potential bias. You can present your professional opinion of the interpretation of the evidence present.

Structure of a report

I have already indicated there isn't always a correct way to present content in a report. You may be fortunate enough to work for an organization that has a template or a form to fill in to present your findings. Most investigators do not have that luxury. The layout or structure of a report can come in many formats. I will recommend one layout. You can customize or alter it to fit your environment or investigation. After many years of conducting investigations, teaching many courses and reading every book and text I could get my hands on, I have opted to support a three plus format. Provide three distinct sections and supporting information as appendices. Other professionals, investigators or authors may lobby for slightly different layouts, but in general they all try to include all the pertinent information and limit the volume of data in a report. In some circumstances I strongly support appendices as attachments or supporting files.

Executive Summary

The first full section of a report should be a summary of your findings, an Executive Summary. The content is an overview written in non-technical language. It is written for a lawyer, a Human Resources Manager or typical computer user. Acronyms and jargon are included in this section only when no other method to explain the findings is available and should be defined or explained before or as the topic is introduced.

This section is almost exclusively a written explanation of your findings. This portion is often the only portion that a requester will truly be able to comprehend, so it must be detailed and thorough without including content that will be unintelligible for them to be able to understand. It is very common to start your summary with a description of the investigation such as requestor, entity being investigated, allegations, and a description of your investigation process. When composing the Executive Summary, you should include all items of interest you located during your investigation. Depending on the volume of findings you have, you may need to group evidence into summations and include examples or the most relevant findings.

If we return to our example of investigating web browser history from a hard drive. the volume of findings could be too large to identify each website visited. You could summarize the activity by presenting the number of different sites visited, the frequency of visits, the length of visits, and common themes of websites. As a point of emphasis, you might specify several URLs that are most identifiable or most exemplary of the general activity.

“An individual using the computer in question, browsed to 125 different websites that are related to interlocking bricks. They averaged 18 sites lasting approximately 45 minutes every day for the past seven months. Sites such as brickbuildinghowtos.org and ilovetobuildbrickseveryday.net were included in the list are a good representation of the typical content of the sites visited by this user. “

Technical Details

The second section of a report should be description of what you found, how you found it and where another investigator can locate the same information. This portion is written for a more technically astute audience. If written properly a non-technical person may be able to understand the process or findings. You should include any user-friendly content where possible. The contents of an email message or of a memorandum can be understood be everyone that reads the report. Not all of the files you locate will have user friend content but including it where possible is very important. Think of it in terms of you told the boss what you found, now you will be explaining it to the person that does the job and understands the process. Using jargon and acronyms in this section is acceptable and where it expedites the reading without introducing ambiguity or confusion should be used.

In this section you include each item of interest you located during your investigation. The content is less focused on writing about what you found, more concentrated on what you found and how you found it and what it contains if the content can be placed into a report. For large volumes of information, the use of tables is strongly recommended. If the volume is significant, a sample of the data can be included in this section and the full contents can be added as an appendix at the end of the document. You should preface any documents or list with what the content is, where it is located inside the evidence, and any special process that is required to be able to reproduce the process of making the content human consumable. You should also include any description of the evidence that might have significant impact or provide additional insight. Items that are hidden, encrypted, abnormal or of significant content should be documented in this section.

We can return to our web browsing investigation example for clarification. The URL history of Internet Explorer is located inside of index.dat file, located inside a user profile. It is not viewable by double clicking without specialized software. We must inform the reader that this file in the specific location houses the browsing history in Internet Explorer but must be opened with a special software for the history to be easily viewed by a person. We then should include a table of the URLS, time(s) visited, view count, page titles and other information that could be extracted. If the number of entries is large, say more than 100, we should put the table in an appendix, tell the reader which appendix it is in and include a sample of 5-10 entries.

“I located browsing history in Internet Explorer [IE] located in the index.dat file in the user Steve’s profile. The file is located logically on the drive at

C:\users\steve\appdata\local\microsoft\windows\temporary internet files\index.dat We extracted the file from our bit-stream copy of the hard drive to examine the file in IE History Viewer by Nirsoft Industries. Using IE History Viewer I was able to extract the browser history for the user account Steve’s IE history. This table is a sample of the findings. I have place the entire contents into Appendix C “IE History Results”.

URL Date/Time Visits Page Title Referal

www.msn.com 3/4/15 12:34pm 16 Welcome to MSN

Www.geek.com 3/4/15 12:37pm 19 Home of Geeks Msn.com

Apple.com/store 3/16/15 1:45pm 4 Apple Store Home typed

You should have entries for all items you have located. You do not always include all content of all items located in this section, where viable a copy of the easy-to-read content. You might summarize the content in addition to where it is and how to read it.

Technical information

In this section you include the specific technical details for items you have identified as of interest. The information in this section will help any technical investigator to recreate your findings. The information about the item is dictated by type of evidence and the type of investigation. Generally, you will include the details of a file, such as dates and times created, modified, accessed, logical location, hash values, and where viable a copy of the easy-to-read content. Not all files have all attributes. Some evidence such as archive files, mailbox files or slack space may have a notable number of items of interest inside of one file. You do not have to relist the file and attributes for each item of interest.

For listing these details, it is often preferable to place them into an easy-to-read table. If needed multiple tables to sort and display data in a consistent and logical fashion. The content listed is at your discretion. You should be thorough and complete. The list of items could be very lengthy. It may all serve value and importance to the requestor of the report. The data you include should identify what items you located, proof they haven't been modified, and relevant data for any skilled investigator to find them given the same evidence to investigate.

Appendices

There are many items that you may opt to include in your report. The list can include but not limited to, your procedures, your validations, your investigation logs, detailed lists too long to place inside other portions of the report, supporting conversations such as the request to conduct the investigation or images retrieved during the investigations.

Organization and layout

General Description

This document represents you and your organization. It should be professional, reviewed, refined, neat and should be easy to read. Professionals compose and deliver professional quality documents. A poor document discredits your professional skill, even if your ability to find and synthesize information is extraordinary.

Cover Sheet

I don't consider a coversheet a portion of a report; it is a very important aspect of the report. Almost all investigations will involve sensitive content. Whether is legal, civil, or business sensitive, covering your findings is a smart move. The entity requesting the investigation should be responsible enough to ensure their copy of a report is not easily visible by unauthorized parties. To help ensure the confidentiality of the report a cover sheet with basic information that doesn't indicate the party(ies) being investigated, the alleged activity or any findings, you should include your name, the requesters' name, a case number [if assigned], date presented, and label such as "Investigation Report".

Pagination

Placing page numbers in a report is very easy to overlook, but very unprofessional to forget. Bottom of the page, top of the page, corners or center are all acceptable. Consistency of the placement is the only real requirement. It is also a very common requirement. It is a great practice to list the items in the paper and where they are located. If you use a modern word processing application, it will automatically generate and update a table of contents if you use the layout functions such as headers.

Boarders, Spacing and Fonts

Reasonable defaults of a word processor are acceptable. You should avoid large margins or narrow margins. Spacing between lines in business presentations is typically single-spaced with a line between paragraphs or sections. Font selection should be business professional. Times New Roman is almost always a safe selection. Avoid busy, flashy or non-standard fonts. They may appear business professional, but if the person reading the electronic version of the report doesn’t have the font you specified, it will use a default. Substituting fonts can alter the appearance and spacing of a document.

Chapter Seven Windows Artifacts

Windows Artifacts

One of the key aspects of investigation is locating the artifacts, or file remnants, that provide inculpatory or exculpatory; More simply put, if you find files that support or disprove the allegation you are successful in your investigation. Your job as an investigator is knowing where the files are in a Windows hard drive that will provide evidence. During your career, you may be asked to investigate many types of activities. Each case may have separate types of evidence files to locate or recover. In general, this is true for a Windows computer and just as true for an Android phone. Locating relevant files is the primary objective of investigating.

For this book we are only including a small section related to Windows. The concepts and specifics can be applied to any other type of investigation. It is the intent to provide a basic understanding of process and details for a few basic evidence items so you as an investigator and learn more on your own as needed. The key to success is learning what files or locations contain the types of evidence you are seeking. General file structure knowledge and the ability to navigate folders is essential in almost all digital investigations. File types and locations can change based on the version of a software or operating system, so investigators must be ready to learn about a different environment with every investigation. It is important that you take the time before a real live investigation to learn how to locate the types of files and evidence you will need. This might mean doing a mock investigation before you start your real investigation. You don’t want to 'learn as you go' because this can lead to errors, oversights or missed evidence. While you could under extreme circumstance 'learn as you go', but ensure you document everything in detail for your benefit.

A very common item that might be involved in a Windows investigation are documents. In a simple case everything in a case would hinge on finding work related documents, such as MS Word documents or an MS Excel spreadsheet. Average computer users will have a default location they store their work documents. This might be in the Documents folder. When we investigate Ableforth, locating these files may be as easy as looking in 'C:\users\abelforth\documents\work' directory inside of our investigation software. The files located contain far more evidence that what we might first realize. A novice inspector will rush to view the contents, locate inculpatory evidence and stop investigating. They would be overlooking some very valuable information that helps support the case. Each file on a Windows computer has file system attributes. The important values are date and time created date and time last modified, and date and time last accessed. When we look at digital evidence from a computer, creating a timeline to associate a user with an activity or piece of evidence is vital to making the circumstantial evidence more substantive.

MS Office documents such as MS Word and MS Excel embed a significant amount of information about the file. This metadata can also be a huge benefit to investigators. The metadata may contain the name or account name of the person that created the file, last modified the file, organization that registered the software when the document was created, modified dates and times, creation dates and times as well as changes made to the content of the document throughout the life of the document.

As you locate artifacts you should mark them as important in your investigation software as well as document them in your notes. It is common to assign evidence numbers to each file located for easy reference. Some files may contain multiple items of interest. A good example might be a mailbox file from an email application such as MS Outlook. All of the emails sent and received are stored in a single file, such as ableforth.ost. Using appropriate software to open the .ost file might provide hundreds of emails relevant to the investigation. Identifying each one with a unique evidence number is a daunting task, but each email may have significance. Your job as the investigator is to locate as much evidence as you can to help the individual or group that requested the investigation make the most informed decision about proceeding with their duties and roles. Email and communications have some unique aspects that we will study in another section of this book.

Windows has extensive logging capability. A computer can be configured to record actions or activities that take place on a computer automatically. Most corporate environments have specific types of events recorded by Windows for auditing and diagnostic purposes. Such as when a user account logs onto a Windows computer, an event is added to the security log. When a service is started, it is recorded in a log. A common type of evidence requested in corporate investigations, is examining for violations of work policies. This might be sexual harassment or using a computer for personal use. You may also be tasked to investigate to provide supporting evidence that an employee is not doing their assigned duties. The supporting evidence needed may be something as simple as examining the Windows security events and providing the dates and times a user's account logged onto the computer. You may be asked to examine web activity, which we will study in another section of this book. You may be tasked to identify if a user's account was used on a computer which was not authorized. Examining the security.evtx file in the

'C:\windows\system32\winevt\logs' folder. It is imperative that the examiner know how to read and filter the content of the .evtx file. Locating a logon or logoff event takes some understanding and practice. There are many resources available to assist an examiner, but they shouldn't be 'learning as they go'. The last item we will examine in the Windows specific arena is the registry. Windows' registry is a database of computer and user specific settings and configurations. It was built as a single repository for configurations. It records many aspects of a Windows computer in one nice, neat location. 'C:\windows\system32\config\' hosts the files: SAM, SECURITY, SOFTWARE and SYSTEM. These files comprise the setting for the computer and some configurations that applied or accessed by all users of the computer. Each user has their own registry file NTUSER.DAT that stores their specific information. If we were examining Ableforth, his file would be 'C:\users\ableforth\NTUSER.DAT'.

Closing

Thank you for reading this book. I hope you have learned something new and useful. If you have any questions or comments, please feel free to contact me at nielsen.brady@gmail.com