

# 1

## Types of Computer-Based Investigations

Welcome to the 21st century, where almost everything in life is connected to an electronic device. There are digital cameras inside doorbells; your smartphone tracks your daily progress from work to home and back again; you get social media updates when you go to the gym, a show, or travel to a new city.

Your phone calls, bank access, and medical appointments are tracked via digital technology. If it tracks your mundane daily activity, what about criminal or unethical behavior? Of course, that activity is also followed, and if you are a digital forensic investigator, you must know the repositories of the digital evidence and how to analyze it. All activity, benign or criminal, will most likely generate some sort of digital evidence. As an investigator, it is your job to locate all data of interest, process it, and present the evidence to the finder of fact. This chapter will introduce you to the different topics of computer-based investigations, from criminal acts investigated by the police to civil and potentially illegal actions performed by an employee, and an external third party examined by a nongovernmental investigator.

While the goal is the same, to present evidence related to an incident, the methods for evidence gathering and for evidence presentation are slightly different. Therefore, you need to understand where there are similarities and where there are differences.

The topics that will be covered in this chapter are as follows:

- Differences in computer-based investigations
- Criminal investigations

- Corporate investigations

# Introduction to computer-based investigations

This book is all about introducing a beginner to the realm of digital forensics. What is digital forensics? It is a division of forensics involving the recovery and analysis of data that has been recovered from digital devices. At one time, the term *digital forensics* was treated as a synonym for computer forensics, but now it involves all devices capable of storing digital data. No matter what term is used, the goal is to identify, collect, and examine/analyze digital data while preserving its integrity. Digital forensics is not only about finding the artifact; it is a formal examination/analysis of the digital evidence to prove or disprove whether the accused committed the violation.

It is not always about demonstrating that the suspect is guilty; as a forensic examiner, you also have that ethical obligation to find **exculpatory** evidence that will prove the subject's innocence. In addition, you must be an unbiased third party in presenting the investigation's findings. In a criminal examination, your findings could deprive someone of their liberty, and in a corporate investigation, your findings may lead to a criminal investigation or cost someone their livelihood. As a digital forensic examiner, your conclusions can have an extraordinary impact on the subjects of the investigation.

To be a digital forensic examiner, you need to have a desire to ask questions, have specialized equipment, and have the required training. From teaching people interested in the field, I have found the best students can critically examine the facts and circumstances being presented and, using that ability, can focus their efforts on efficiently reaching an accurate conclusion. Unfortunately, I find many students want to use a "find evidence" button, find all the artifacts, and print up a thousand-page report and call it a day. That is not digital forensics.

Digital forensics is not finding the artifact. By artifact, I am talking about an incriminating Google search in browser history, an incriminating email between the subject and a co-conspirator, and illicit images found in the filesystem. Artifacts are breadcrumbs leading to the identity of the person conducting the illegal activity. However, on their own, they do not identify the user who created these artifacts or the one who is responsible for their creation indirectly. One of the biggest challenges in this field is identifying the user who is physically operating the device. You want to tie the user to the specific subject, and to do that, you have to analyze – that is the keyword – the digital evidence to associate it with a particular user.

If you are in the IT field, you will understand networking and computer operating systems, but you will lack knowledge of how to preserve evidence, maintain a chain of custody, and present it in criminal/administrative proceedings.

If you are an investigator, you will understand the chain of custody, evidence preservation, and testifying in criminal/administrative proceedings. However, you may lack experience in the digital field. To be an effective digital forensic examiner, you must be part of both those worlds. You must understand how data is created, shared, and saved in the digital realm and preserve that evidence in a forensically sound manner and be able to testify in proceedings. Sometimes, the ability to talk in front of a large group while answering challenging questions posed to you by attorneys from both sides is the hardest part of the field.

As with any field, the way you get better and more effective is to practice, conduct real and mock examinations, receive training, and have the willingness to reach out to your peers for advice. Since you are reading this book, you are taking that first step. You could be reading the text on your own, using it as a textbook for a college course you are taking, or using it in a corporate training session. The reason does not matter. Reading this book will put you on the road to becoming a more effective digital forensic examiner.

What is cybercrime? What crimes does a digital forensic examiner investigate? A digital forensic examiner may investigate any alleged wrongdoing that touches the digital world. Nearly everyone possesses a

mobile device. Sometimes, a person owns or uses multiple mobile devices, laptops, and the traditional desktop. All of these sources can maintain a significant amount of information related to the investigation. For example, I investigated a crime against a person where the victim was physically unable to communicate with the police. How does that become a crime that requires the use of a digital forensic examiner?

Well, in this case, she had maintained communication with the suspect of that crime via a website and instant messaging on her mobile device. So, while they did not directly have evidence relating to the crime being investigated, they had evidence about the relationship between the victim and the suspect. In the 21st century, almost any crime may have evidence stored in a digital format. Now, there are some crimes where someone will have used their computer as a tool to commit the crime, such as sending harassing emails, fraud and forgery, hacking, corporate espionage, or the trafficking of illicit images. Your occupation will dictate your response to a situation; if you are law enforcement, you will have one set of procedures to follow, while if you are in the corporate world, you will have a different set of procedures to follow. While some processes may overlap in different fields, each one has its unique differences, which is what we will discuss next.

## Criminal investigations

As a law enforcement professional, your first consideration will be officer safety. Is the scene **safe and secure** to process and secure evidence? When the investigation starts, you may participate in one or more roles. The most basic positions are as follows:

- The first responder
- The investigator
- Crime scene technician

Depending on the size of your agency, you may fill one position or all three, and you may report to one or more supervisors. Now, with digital evidence, the person in charge of the crime scene should know the fragility

of digital evidence. That allows personnel to enact the proper procedures to ensure that the evidence is not corrupted.

Let's talk about what each role does.

## **First responders**

The first responders are the first ones on the scene. They secure what may be a chaotic scene. They will identify the following:

- Potential victims
- Witnesses
- Potential suspects
- How best to maintain control

They will do this until the investigator arrives. The first responder's primary mission is to make the scene safe and secure and ensure that no one can contaminate the evidence. As you can imagine, crime scenes can vary from a dynamic crime scene to a relatively static crime scene, depending on the nature of the crime. In both scenarios, the first responder must have basic knowledge of what items could contain digital evidence when they secure the scene. We would not want subjects grabbing cell phones or laptops and using them for any activity.

So, how does a first responder protect the crime scene? Like you see in TV shows and movies, yellow crime scene tape is the most common method. It is the most straightforward visible sign of a crime scene barrier, and in our culture, people recognize the barrier being presented by that thin piece of yellow plastic. One or more personnel will have to monitor the crime scene to regulate who can cross that line and enter the scene.

## **Investigators**

The investigator will respond to the scene after being requested by the first responder. Upon arriving at the scene, the first responder and the investigator will coordinate, and information sharing will now start. The

first responder will provide the basic information, which typically involves the five Ws and one H, specifically the who, what, when, where, why, and how, about the incident.

The first responder will also provide information about any actions they or anyone else had taken before the arrival of the investigator. For example, the investigator will want to know whether the first responder(s) touched anything, moved anything, or changed anything within the crime scene. This could be a physical action such as applying first aid to a victim or turning a computer on or off. I remember an examination I did where the first responders did not reveal that they had accessed the victim's computer. While conducting my examination, I did a timeline analysis and saw an abnormality in the activity after the victim had died. The abnormality was caused by the unreported actions of the first responders. What's important to understand here is that the first responders' actions were not wrong. What created complications was that they did not report the actions, which led to additional work and explanations.

The investigator takes charge of the scene and directs all activity. They will direct the other team members' investigative efforts to ensure the proper documentation is completed regarding the seizure of evidence. Sometimes, the first responder will seize evidence and turn it over to the investigator. A chain of custody document must be completed and maintained showing who found the item and who maintained control until the completion of the judicial or administrative proceedings.

## **Crime scene technician**

Finally, we come to the crime scene technician. This can be a sworn or unsworn position within the law enforcement agency. They have specialized training in the collection of evidence. This could be physical evidence, such as fingerprints, tool comparison, the collection of biological fluids, and crime scene photography, all of which require specialized training and equipment. The collection of digital evidence requires the same level of expertise that the collection of physical evidence does.

### **Note**

We can put law enforcement jobs into two basic groups.

**Sworn:** May take an oath to support the laws in their jurisdiction; they have the power to make arrests and carry firearms.

**Unsworn:** May take an oath but do not have powers to arrest. These positions are typically crime scene analysts or law enforcement support technicians (this will be dependent on your jurisdiction).

The crime scene technician is responsible for preserving evidence and starting the chain of custody. Some actions they could carry out include acquiring the volatile memory of a computer system, creating forensic images of the storage devices, or creating the logical forensic image of logical files from a server. Next, the evidence will be bagged, tagged, and transported to a secure location. What do I mean by *bagged and tagged*? They will place the physical evidence or the items holding the digital evidence in the appropriate storage container. A tag will then be filled out with identifiers to specify which investigation the evidence belongs to, who collected it, and what evidence is contained within the container.

As we go through the rest of this book, we will cover the duties of the crime scene technician in greater detail.

A law enforcement officer may be a first responder, investigator, or crime scene technician and, in all roles, is an agent of the government. Depending on your jurisdiction, the government may restrict how and when the property can be seized and searched. I will discuss the judicial process in the United States; your locality may have different laws and procedures.

In the United States, a citizen's rights to privacy are protected by the fourth amendment of the US Constitution, which states the following:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

At a basic level, this means that before the government can seize any evidence, there must be (a) a search warrant based upon probable cause or (b) the owner's consent. The consent given by the owner must be willingly given and must be able to be revoked, which can create an issue in some jurisdictions where the processing of digital evidence can take months and, in some jurisdictions, years. If the owner revokes their consent or refuses to give it, what options does law enforcement have? A search warrant.

How does a member of law enforcement get a warrant? As we learned from the preceding passage, it must be based on probable cause. The definition of probable cause is a reasonable standard that the applicant must reasonably believe that the items being searched for are at that location. Who determines what is reasonable? This would be the judicial official, such as a judge, Justice of the Peace, and so on.

The law enforcement officer makes the written request while the judge reviews it and will approve/disapprove it. If approved, the law enforcement officer can seize and search the property within the guidelines specified by the judicial official. The law requires only agents of the government to get a search warrant to seize and search property. This process will not pertain to you if you work in the corporate world.

Now, let's talk about some potential crimes someone might call you to investigate. This will be a high-level overview of the crime itself. Later in this book, we will address the specific artifacts we should analyze to determine whether criminal actions occurred.

## **Illicit images**

Nearly everyone is connected to the many different forms of digital networks via our mobile devices, tablets, laptops, and computers—we are always connected in one manner or another. Depending on who you ask, it is either the best thing in the world or the worst. There are some excellent aspects; social media allows people/family members to stay in contact, no matter where they are in the world. The totality of the world's knowledge is just a few clicks away. You can read news reports from portions of the world that you previously did not know existed. It is an adventure waiting



to happen. Now, it is not all unicorns and rainbows out there. Like any society, there are dark and dangerous portions of the internet where you should be hesitant to travel. That includes the sourcing and sharing of illicit images. For our purposes, an illicit image is an image whose subject matter is offensive or illegal, depending on your cultural or legal landscape.

Before the advent and widespread use of the internet, trafficking in illicit images was almost eradicated, so what changed? The consumer of illicit images no longer had to be physically present to pick up the physical images. The internet allows the user to be relatively anonymous and access illicit images with minimal exposure. I have read reports stating that the high-speed data network that most of us enjoy is because the consumer wants faster throughput speeds to download illicit images.

Consumers of illicit images have free access to terabytes of data with simple clicks of the mouse. If the consumer wants higher quality or a specific subject matter, then it is not a complicated process to find a vendor to meet the consumer's needs for a price.

Your jurisdiction will determine what is or is not an illicit image and the level of criminality associated with the contraband images' possession and/or distribution. I will not differentiate or specify a subject to define illicit images. Instead, I will discuss them using the generic title of illicit images or contraband images. You can use either phrase depending on what may be legal/illegal in your jurisdiction.

How do people share contraband images? At a basic level, a file is a file. A JPEG image of a sunset does not differ from a JPEG image of a contraband subject. Anyone can use any aspect of the internet to share files—the content of the files is irrelevant. If the system allows the user to share data, then the contents of those shared files can be legal or illegal content. Let's look at some media through which illicit images could be exchanged.

## **Email-based communications**

Email is one of the easiest ways to share information through files between two or more people. An email address does not automatically point to a

specific user. Some service providers actively advertise anonymity for users of their email accounts. The service provider states that they do not save transactional information, such as source IP, dates and times of connection, or billing information. The service provider may be located outside of the jurisdiction investigating the contraband, which will allow the service provider to ignore the judicial paperwork requesting the subscriber information.

## **Newsgroups/USENET**

This is one of the first components of the internet and has fallen off the radar for the everyday user. Initially, the internet comprised the World Wide Web, with components such as web browsing, email, and USENET. Web browsing and email are known by nearly every internet user, while USENET has faded out of public perception. However, this does not mean it is not being used. USENET is like the old bulletin board system, where you had specific groups, and users could post messages, attach files, and other users could download the files and comments. The user can post just a text message or attach a file to the message. This attached file is known as a binary.

This USENET attachment will be a file type, such as digital images, video, audio software, or any other file type a user can access. The user must use a newsreader to access USENET. There are free and paid versions of newsreaders available in which the user can subscribe to a USENET service. Just like the email service providers that we discussed earlier, one selling point for USENET service providers is anonymity; they explicitly state that they maintain no user transactional data or billing records or they are in jurisdictions whose laws may not adequately address the contraband contained on the server:

 Graphical user interface, application Description automatically generated

Figure 1.1: Unison application

The preceding screenshot shows you the Unison program running on macOS and accessing the service provider Astraweb.

Looking from left to right, you can see the hierarchical system used by USENET. I have selected **alt** in the far-left column, which then populates the next column with many named folders. The folders' naming convention shows the subject of the group. I have selected **binaries**, which means I am looking for attached files to the postings. We can see folder icons in the third column and a brown folder icon with papers coming out the top. The folder icon shows that additional groups are contained within, while the brown folder icon indicates a newsgroup.

As you can see from the preceding screenshot, there are a variety of subjects for the user to explore; some groups may or may not contain contraband images/files. Your jurisdiction will determine what is legal or not as you conduct your investigation.

## **Peer-to-Peer file sharing**

**Peer-to-Peer (P2P)** file-sharing is a decentralized method of file sharing. In traditional file sharing, a server hosts the file, and the client accesses the server to download the file. In the early days of Napster and music sharing, this became a liability for copyright violations. The service provider was served with judicial processes and was liable for hosting a directory of copyrighted files.

In response, the P2P method was changed; no longer was a centralized database created, but instead, users were able to directly search for other users' shared folders on the network. Users connected to a shared network and acted as servers and clients. In P2P file sharing, when users identify a file they want to download, the software reaches out to the other users who possess the desired file. Each user then provides a piece of the file to the recipient. When all the pieces are collected, the software returns them to the original configuration. The user could then participate as a node (the term "node," when discussing P2P, refers to the user's system connected to the P2P network and sharing files) and start sharing the file they just downloaded:

 Graphical user interface, application Description automatically generated

Figure 1.2: Transmission application

The preceding screenshot shows the **Transmission** program running on macOS. I am downloading a movie from the public domain ([archive.org](http://archive.org)), and in the bottom portion of the preceding screenshot, you can see that the file has been broken into much smaller bits. The highlighted bits show which parts of the file I have downloaded. Later, we will go into much greater detail about P2P file sharing and the artifacts left in the filesystem.

## The crime of stalking

For all of the good that the internet provides, it also provides a conduit for people to exploit, harass, and bully others. The victim could be known to the subject or could have interacted with the victim's online persona in some manner and felt the victim had wronged them. A lot of the bad behavior we see with online activities is because of the anonymity that the internet provides the attacker/subject. When eyes are watching or when we know the attacker's true identity, they change their behavior to conform to societal norms. Unfortunately, it takes time for society to recognize the criminality of specific actions via the digital medium.

Cyberstalking or cyberbullying is now being regulated and considered an actual crime. Depending on your jurisdiction, the definition will vary, and what resources the government will spend on prosecuting these crimes will differ. Remember, the user's identity at the other end of the digital world can be challenging to prove to the high standard required by a court of law.

According to the National Center for Victims of Crime, <https://web.archive.org/web/20201028110630/https://members.victimsofcrime.org/our-programs/past-programs/stalking-resource-center/stalking-information>, historically, in the United States, almost 1,500,000 people, the majority of them women, have been victimized, harassed, and bullied via the digital medium, with the attacks lasting more than two years. In

addition, the attacks increased in length if the participants had been intimate partners.

The impact of this criminal behavior is immense; the victim may lose time from work, may have to move residences (several times, sometimes), and potentially suffer from the physical and mental effects such as the anxiety and depression that come from being targeted. In addition, the ability to stalk a former intimate partner in the digital world opens the door to the ability to inflict significant violence on a former partner and, in some cases, bring about their death.

What behaviors can make up cyberstalking? Generally cyberstalking is where the stalker engages in a series of actions, which can cause the subject of the efforts to be fearful and concerned about their well-being. An example of this is where a terminated employee has sent manipulated, compromising images of their supervisor to members of the organization and the general public. This activity continued for months before it was stopped. Despite the harassment ending and the perpetrator being identified, the supervisor still felt the need to leave their job, change their name, and move to another community.

So, where do we begin in our attempts to investigate this crime? The interview will be the best starting place. Asking the victim if they know or suspect who may be behind the harassment is the first question asked.

In my experience and most of the time, the victim will have a general idea of who the harasser is, especially if it is a former intimate partner. Now, some victims may suffer from mental health issues that could complicate the assessment. As an investigator, you must listen to the whole story to understand the totality of events. Just because someone may appear paranoid does not mean that their concerns or fears are unfounded. As an investigator, you must have an open mind and not allow your preconceptions to make you miss evidence or indicators that may be visible.

If the victim has an idea of who the harasser may be, make sure you record all the pertinent information they can provide you. Names, addresses,

usernames, email addresses, screen names, and social media locations will all give you valuable information so that you can start your investigation.

Establish the method of the harassment and when it started. For example, was it a Facebook group? Snapchat? Text messages? Chat rooms? Is a mobile device involved in text messages, missed calls, and more? Has the harassment gone old-school with the use of the post office with physical letters?

Threats of violence may increase the severity of the crime and should not be discounted.

The investigator will need to ensure they get forensically sound copies of the digital evidence to start the investigation. This creates the chain of custody of the digital evidence and is the beginning of the investigation.

We will go into much greater detail about the specific artifacts found in digital evidence, but once you have account usernames and IP addresses that the attacker is using to facilitate their attacks, you have a starting point to identify them.

In the United States, a subpoena is required to obtain subscriber information. This information includes the user's first and last names, physical address, how often they access the account, and the IP address used to access the account. It varies between service providers as to how long this information is maintained. Sometimes, it could be as little as weeks or as much as years, depending on the provider. You can also submit legal paperwork asking them to "freeze" the account so that the user cannot disable it or delete any incriminating information.

To gain access to the information contained within the account, such as email content, contents of messages, or anything having to do with content, a search warrant signed by a judge will have to be served on the service provider. If the service provider is within the same jurisdiction as the judicial authority, there are typically no issues. However, when the service provider is in another jurisdiction within the United States or a jurisdiction outside the borders of the United States, this is when the process becomes much more difficult, and sometimes it's impossible to proceed.

Some subscriber information you get may or may not be accurate. It is not unusual for a user to complete the registration forms with false information. But what you can do, for example, if you have an email address, is you can do an open-source search and see whether the user used the email address anywhere else. For example, some online forums will use the email address as a username, and if so, the user may post identifying information in their communications with the other users. That forum now becomes a source of information for which you can issue a subpoena to get the subscriber information.

As you can see, following breadcrumbs of information may lead you to sources you never even considered. Moreover, it can be quite complicated and time-consuming.

## **Criminal conspiracy**

Criminal conspiracy and digital forensics: how do these aspects intersect in the world of the digital forensic investigator? First, let's define what a conspiracy is: when two or more people agree to commit an illegal act. However, just deciding to commit the unlawful act is not enough; actions also have to be taken to further the conspiracy. What does all that mean? For the physical crime of robbery, criminal A contacts criminal B to discuss robbing victim C. The conversation between criminals A and B does not meet the statutory definition of a conspiracy. However, suppose criminal A paid criminal B and agreed on the amount of funds in exchange for the service of the robbing of victim C. In that case, we have an act in furtherance of the conspiracy to commit robbery. So, what crimes can the digital forensic investigator find within the digital realm? Almost any crime imaginable. Let's take a look at an example of such a crime:

"Michelle Theer was convicted of a crime against a person. She conspired with John Diamond to commit the crime against her husband, Marty. Investigators had no direct evidence, no physical evidence, and no eyewitness evidence, but they had digital evidence showing the conspiracy to commit the crime. Investigators recovered over 80,000 emails and instant messages between Diamond and Theer that showed a personal relationship

between the two and the messages showing the conspiracy between them to commit the crime.”

You can read about this case in more detail at <https://caselaw.findlaw.com/nc-court-of-appeals/1201672.html>.

Now more than ever, people are connected to their devices for their everyday activities. It is not a stretch of the imagination that criminals also use their devices to help organize their criminal activities. The digital forensic investigator has to know of all potential sources of digital evidence and recognize that the **Internet of Things (IoT)** is an untapped bonanza of digital evidence. What is the Internet of Things?

Home assistance programs such as Siri and Alexa, smartwatches, home security systems, and GPS devices – anything that has an app – might contain evidence and show the criminals’ intent to commit the crime. Failure to recognize digital devices can result in significant damage to your investigation. For example, there have been instances where the subject of an investigation was placed in the interrogation room, and the investigator did not recognize the suspect was wearing a smartwatch. While they left the subject unattended in the interrogation room, the subject was able to communicate with their co-conspirators and direct their efforts to destroy evidence and interfere with the investigation. Once the investigators caught on to the subject’s actions, they used the smartwatch to show the criminal conspiracy. They used the evidence to generate additional charges for the suspect in custody and their co-conspirators.

Social media is also a source of digital evidence for showing a conspiracy. For example, take the case of Larry Jo Thomas. The government convicted Thomas of committing a crime against Rito Llamas-Juarez. Initially, investigators only knew that a specific type of item harmed Llamas-Juarez. However, as investigators processed the crime scene, a bracelet that was “distinctive” was found and collected as evidence. The investigators examined Thomas’s Facebook page and saw a photo of Thomas posing with an item similar to what was used at the crime scene. In a different photo, they found the “distinctive” bracelet being worn by Thomas. While the digital evidence did not directly impact the criminality being



investigated, it showed how the subject had the means and had been at the crime scene.

Vehicles are also a source of evidence to prove the conspiracy. New vehicles are connected to the network and have their own Wi-Fi connection and sync data between mobile devices, GPS data, and the vehicle's black box. Potentially, the investigator can show the subjects performing reconnaissance on their targets, meetings between the conspirators at a shared location, or where they have traveled to and returned from using toll passes.

Technology is rapidly changing and advancing as the general population uses technology, and so do the criminals. The general population plans out their day by utilizing technology; criminals also plan out their day of criminal activity using the same technology. I am always amazed when criminals use their mobile devices to plan and execute criminal activity and then take pictures to memorialize their illegal business.

Now that we have learned about criminal investigations, the roles, and the means by which information is being shared, let's move on to the next type of investigation, which is corporate investigations.

## **Corporate investigations**

We will now discuss computer forensics from a civilian or non-law enforcement perspective. Since you are not an agent of the government, the search warrant requirement does not pertain to you. (Your specific jurisdiction may be different.) While you may not have the search warrant requirement, you cannot seize and analyze private property. What do I mean by that? You are the investigator for a large multinational corporation; you have an employee you believe is harassing other employees and may have viewed illicit images on their company laptop. What is the legal requirement for you to examine the contents of the employee's laptop? If you are an agent of the government, the employee has an expectation of privacy. However, as an employee utilizing the

company's equipment, in the United States the courts have held that the employee has a limited expectation of privacy on the data in the device.

### **Important note**

This may differ, depending on your local jurisdiction. I was teaching a class in Germany and as I was teaching, the students explained that German law gave an employee a high expectation of privacy. In their jurisdiction, there were specific requirements that had to be met before they could examine an employee's computer.

Other than the search warrant requirement, the corporate investigator's duties are similar to law enforcement's. They still must acquire the evidence, analyze the evidence, and present their findings. They could present their findings in an administrative proceeding or, if necessary, forward them to law enforcement, where they may have to testify in a judicial proceeding. In either case, the digital forensic investigator must ensure that the digital evidence was collected in a forensically sound manner while maintaining the chain of custody of the digital evidence.

If the digital forensic examiner cannot authenticate the evidence, they cannot testify or present it in the administrative/judicial proceeding. The corporate digital forensic investigator also investigates a wide variety of allegations. Typically, they will not be investigating a crime where a person was hurt or killed. However, they can still investigate fraud, forgery, a violation of the company's policies and procedures, corporate espionage, or if they believe an employee has stolen intellectual property or is trying to harm the corporation itself. So, let's now talk about employee misconduct.

## **Employee misconduct**

As a condition of the employee's employment, they must abide by the policies created by their organization. Typically, an employer has an "Employee Handbook" or has a set of policies and procedures that dictate what behaviors are acceptable and which ones are not acceptable. Such policies also include laying out specifications to ensure that the organization treats all employees with dignity and respect in the

organization's daily operations. There may be rules that specify an acceptable use of the organization's desktop and laptop computers, and a violation of those rules could result in an investigation analyzing those devices, as we mentioned earlier.

Now, I use the term "policy and procedures," and I have found a large amount of confusion with those two terms, primarily when used together. A policy is a statement from the organization addressing a specific issue, while the procedure is the specific instructions regarding how to accomplish the goals of the policy. For example, the organization could enact a policy to restrict employees from accessing non-organizational emails using the organization's computers. The procedure would have two audiences: all the employees and the IT staff. The procedure would inform the employees of how to access the organization's email while directing the IT staff regarding how to block non-organizational emails from being accessed.

You need to follow some general guidelines as your organization drafts and implements policies and the accompanying procedures, as follows:

- The policy should be simple to understand. Short and sweet – do not overcomplicate it. If there is a way for an employee to "misunderstand" the policy, then they will dispute whether their actions violated the policy.
- The procedure should specify all the steps needed to implement the task outlined in the policy. Don't assume the reader will understand if you are not specific in what you want them to do.
- The organization must inform the employee of the potential consequences of violating the policy.
- The organization cannot implement policies that violate the law.
- The organization must enforce the policies. There have been many investigations I have conducted where multiple employees have violated the policy, but the organization never enforced the policy. If they do not enforce the policy for 51 weeks and then, during the 52nd week, the organization enforces the policy against some employees and not others, how can the employees be held accountable during week 52?

- There must be documentation that the employee knew and understood that the organization implemented the policy and the penalties for violating the policy.

If an employee violates the organizations' policies or procedures, does law enforcement have to get involved? Of course not. It would depend on the violation, whether it was a criminal act, and whether the organization had a responsibility to notify law enforcement. Sometimes, the law may mandate the organization to notify law enforcement if they discover the employee has committed a criminal violation. Make sure you know the statutory requirements in your jurisdiction and communicate with in-house counsel during the investigation.

As a digital forensic investigator, it is not typically your decision to notify law enforcement. Instead, after you consult the organization's legal counsel and C-level executives, they will make that decision. It does not matter whether the investigation relates to a criminal or non-criminal matter for the digital forensic investigator's purposes.

Remember, we treat *every* investigation as if we may have to go to court and testify. While the initial investigation may deal with policy violations, you may discover there have been criminal violations that mandate law enforcement involvement in the inquiry. The prosecution and defense will scrutinize all of your investigative endeavors before law enforcement involvement. If you do not maintain the standards of the investigative process, it could weaken the prosecution.

As a digital forensic investigator for a corporate organization, there are a variety of violations the organization may call on you to investigate. One of the more common incidents is the complaint of harassment or a hostile work environment. This is where one person causes one or more people to be intimidated, harassed, physically threatened, humiliated, or any other activity that makes the workplace offensive. How would you investigate someone for a hostile work environment? After conducting the interviews with the complaining employees, they may provide statements on how the subject created the harassment/hostile work environment, if at all.

Your investigation will determine whether the actions were physical, verbal, or carried out on digital media and the frequency of the offending conduct. Was there a single employee whose behavior was offensive, or is there a culture within the organization? If a supervisor was notified or asked the offender to stop, what resulted from the efforts to stop the offending behavior? The offending employee could send offensive text messages, emails, or instant messages utilizing the organization's communication network. Suppose the alleged behavior occurred on or was facilitated with the organization's devices. In that case, you should be conducting your examination to determine whether there is any digital evidence to support or refute the allegations since the property belongs to the organization, limiting the employee's expectation of privacy. (Remember, this may vary by jurisdiction.)

The investigation can proceed once you have supervisory approval to conduct the digital forensic examination. With the information at hand, you can filter out a large amount of additional data that may be contained on the storage device. To be efficient while dealing with the extraordinarily large datasets in today's high-capacity devices, you have to filter out data that is not pertinent to your investigation. For example, if we deal with harassing emails, you may restrict your examination to only email traffic.

Now, your investigation may grow based on your findings on the initial exam. For example, while viewing emails, you observe the subject sending illicit images to other employees. Your investigation has now increased based on the violation and the potential number of violators. Do not limit yourself to only the suspect's computer; you need to examine both the suspect and the complaining witness.

The complaining witness may have evidence of the offending email, while the suspect may have used anti-forensic techniques to remove the source email from their computer. Or you may find the complaining witness had changed the email to contain offensive material. You want to be as thorough as possible, which dictates an examination of the emails from both the sender and the recipient.

You are not typically called upon to determine whether the conduct was offensive – that is a very subjective determination. What one employee

considers offensive, another employee may not. Your job will be to recover the artifacts to allow the fact finder to make a well-informed decision on whether the complaining witness' statement can be substantiated. Human resources or in-house legal counsel will determine whether the employee's conduct was offensive. Your job is to be an impartial third party and present the findings. This could be through an administrative proceeding such as a hearing, or you could make a presentation to a senior executive. Remember that the organization may be held liable when they have been informed of the employee's offensive behavior and did not take action.

## **Corporate espionage**

In the corporate environment, no matter how large or small, there are specifics about your organization you don't want to share with the entire world. For example, you could provide a proprietary widget to another organization or have an exclusive recipe for a consumer food product. In almost every case, your organization provides a service, and they get paid to provide that service. If a competitor could look inside the organization's internal workings, that look may mitigate any advantage the organization has over the competition.

We can define corporate espionage as one organization spying on another to achieve commercial or financial gain. The same tactics that nation-states use against each other are utilized by corporate actors against each other; for example:

- Physical or digital trespassing to gain access to data or information
- Impersonating any employee to gain physical access to an organization's buildings or other facilities
- Intercepting voice or data communications or manipulating a competitor's website
- Manipulating social media against a competitor

Some actions I just listed are not in the digital realm, so how can a digital forensic investigator determine what occurred?

## **Security**

It comes down to physical and digital security. The organization has to be proactive and identify the critical infrastructure that needs protection. Once the critical infrastructure has been identified, the organization can then implement controls for security and documentation. If an attacker is successful, the digital forensic investigator will have to determine how the attacker got past the established protocols. The organization's physical and digital defenses should be multifaceted and not rely on a single aspect. I mean that there should be a mixture of physical and digital mitigation efforts to protect the organization. For example, access control is essential; a locked door could be access control, such as controlling access to the server room. Now, the door could be locked and unlocked with biometrics or a physical token. The organization should maintain the access control logs at an off-site facility.

If the attacker compromised and used an employee's access control token, a digital forensic investigator can analyze the logs and determine which user identity accessed the server room. Implementing digital surveillance recordings will allow the investigator to observe the compromise and decide whether or not it was the employee or an unknown third party. With a digital attack, you will have to analyze the logs from the network security devices, for example, antivirus logs, authentication servers, routers, and firewalls, all of which are detective controls. While a detective control allows you to investigate what occurred, it doesn't prevent the incident, nor is it a deterrent. Access control is about protecting an asset; you control users and prevent unauthorized access.

## **Threat Actors**

You may be the victim of an attack from a threat actor. What is a threat actor? Typically, it's a malicious user gaining access to information systems that belong to another.

You may see the terms "black hat" or "white hat" threat actor, where the color of the hat determines the threat actor's intent.

A "white hat" threat actor is a positive actor. This is a person or persons whose goal is to identify vulnerabilities in the system so that the

organization's owner or vendor may correct them. A "black hat" threat actor is someone who is attacking the system with malicious intent; their goal is to violate and exploit the organization's data system. Finally, there is also the "activist threat actor," who is looking to exploit vulnerabilities in the system for political reasons. The attack could be compromising information maintained in the system or a distributed denial-of-service attack on the organization. The following is a table to help highlight the differences:

<b>White Hat</b>	<b>Black Hat</b>	<b>Activist</b>
They hack into systems to discover the liabilities before the bad actors.	They hack into systems for their own personal gain.  (Bad actor)	They hack into the system to expose activities, harass the owner, or to promote a political agenda.  (Bad actor)

A bad actor will not only rely on accessing the system through technical means; they will also attack an organization through the employees. This is known as using social engineering, which is what we will discuss next.

## **Social engineering**

Social engineering is another attack that is relatively common in the corporate environment. One aspect is a "phishing attack," where the attacker attempts to trick the user into gaining access to confidential information such as a username and password. Typically, this attack is made via email, where the sender purports to be a bank, or someone in authority, where they're asking the user to provide biographical information, name, date of birth, governmental identification number, username, and passwords.



If the user believes the email and provides that information, the attacker can impersonate the user and attempt to gain a foothold into the organization's data systems.

There are automated tools designed to use social engineering, such as a phishing attack, against organizations. These tools do not require a significant amount of specialized knowledge to implement. The users of these tools are referred to as “script kiddies” and could attack your organization using these automated tools.

The vendors of the tools state they are to be used by the organization to test their defenses, but there is no method to control what the user does with the software once downloaded.

## Gophish

Gophish is one such automated tool. It works on all three of the major operating systems and is freely available for anyone to download. It does not require significant installation skills; you can extract it and run the executable, and the program will be up and running. The following screenshot shows the initial login screen when the software is up and running:


 A picture containing graphical user interface Description automatically generated

Figure 1.3: Gophish login

Once you log in, you will be presented with the **Dashboard** of the service.

### Note

This book is not about running Gophish or any other program; it is merely to give you an idea of what is available out there.

Please follow all applicable laws and regulations.

You can create email templates that you can send out to organizations. You can capture members of the organization's emails using **open source intelligence techniques (OSINTs)** and import them into the program:


 Graphical user interface, text Description automatically generated

Figure 1.4: Gophish import emails

A common theme when it comes to phishing the user's credentials is to send them an email asking them to reset their password, and when they do so, it directs them to a clone of the official landing page. After the attackers capture the username and password, the user is redirected to the official page, and they never know what occurred.

## Real-world experience

One time, I was hired to conduct a vulnerability analysis of an organization. As part of the scenario, they did not provide me with any information about the data network's internal workings or the building's physical security. The building had public access during regular business hours. During normal business hours, I walked around the organization and conducted my reconnaissance to see whether I could identify any vulnerabilities.

To go to the executive levels of the building, I was required to sign in at the security desk and receive a **radio frequency identification (RFID)** pass. As I signed in, they did not require me to show any identification or state my business or my destination. I signed in and was given a visitor RFID card and was sent on my way. I took the elevator to the top floor and walked around the executive level. I was dressed in the typical business casual clothing, carrying my laptop case. I found an unlocked training room where I entered and set up my laptop. I plugged into the network and accessed the system. Several employees walked in while I was inside the training room, but none of them questioned why I was there, sitting alone, typing furiously at my computer. I stayed in the room until four hours after the building closed. During that time, no one questioned why I was in there.

I packed up my laptop and had full access to the executive level for the rest of the evening.

If I was an actual attacker, how would you be able to investigate what happened? What sources of evidence, maintained by the organization, could you process? The first step would be to identify a potential timeline for what occurred. One control for this vulnerability test was not to damage the network and to access the control file. A control file is a plain document of no value and can be safely manipulated to show unauthorized access. The manipulated file will contain the timestamps to show when the unauthorized access happened. The timestamps will give the investigator a starting point for starting the investigation.

This will be achieved by examining server logs and firewall logs and identifying my digital footprints within the network. Once they identify the physical device location where the compromise occurred, they can review the surveillance footage to work backward on how I gained access to the executive level, the RFID-protected elevator, and the physical security log I completed. Typing out the reaction to the compromise in the system does not address the enormity of the task facing the digital forensic investigator.

If the organization identifies the compromise within a timely fashion, that makes the investigation more straightforward, but consider if the compromise isn't recognized for days, weeks, or months. How hard would it be to determine what occurred months later, after the compromise?

Consider the compromise of Sony Pictures in 2014. While the exact duration of the attack is unknown, the attackers spent at least two months inside the network copying files, with some reports saying the attackers had access to the internal network for a year. Although it has never been confirmed, the attackers claim to have compromised and transferred over 100 TB of data from Sony Pictures. The compromise of information was not the only vector of attack; they made employees' computers inoperable and compromised some of the organization's social media accounts. In addition, the organization's employees were also victimized by the compromising of their personal information by the attackers.

# Insider threat

An organization cannot assume the attack will come from an external threat. While the design of most protocols and mitigations is to safeguard the organization from the external threat, the internal threat can be more dangerous than the external threat. No longer can the organization rely upon outward-facing security such as firewalls, building access control systems, intrusion prevention systems, or intrusion detection systems; they must also assess and monitor internal vulnerabilities to mitigate the threat from the inside. This is not an easy task; the insider threat has knowledge of the security protocols, policies, and potential vulnerabilities that the external threat does not.

In 2016, almost 1/3 of all electronic crimes were known/suspected to be caused by an insider threat. The damage caused by the insider was more significant than an external attack. No sector is protected from the internal attacker; if you are a US federal agency or a defense contractor, the government requires you to create a formal insider threat program, which is not surprising since there have been nearly 100 insider threat incidents within the last ten years. (We are not talking about espionage incidents.) Almost 3/4 of the insider attackers were actively employed by the federal agency, while 1/3 were not directly employed, such as a contractor or an employee of another agency. Most of the federal cases dealt with fraud and were committed by the insider for financial gain.

Who typically commits insider attacks? Is it a new employee? A veteran? Remember, for an insider attack to be effective, the insider must be trusted. If we look at the federal government sector, nearly half of the insiders had been with the organization for over five years, with most of them abusing their access and creating fraudulent documents.

Now, in the information technology sector, the demographics of an insider attack are a bit different. Nearly 75 percent were former employees and were with the organization for less than a year. In addition, almost 20 percent did not have their accounts deactivated when they left the organization. That means they could use their credentials to access the confidential information, despite leaving their employment.

As an investigator, this should be a warning that there is an issue with that organization's policies and procedures that must be immediately corrected.

Having a procedure at hand to deactivate an employee's account either before termination or shortly after they give their resignation would have stopped 1/5 of the documented attacks.

Investigating an insider threat will be difficult. You are dealing with people/employees who, at some level, have gained the trust of the organization. The investigator has to try and determine what the insider's mindset is underneath the persona that is being shown every day. Are they an opportunist? Are they a disgruntled employee? Are they someone out for revenge against an executive? Those are the potential attackers you may have to deal with. You want to create the groundwork before the attack happens.

Various sections of the organization – Human Resources, Legal, and IT – will be part of planning any potential response as well as being part of the response. The response team will identify who may be involved in an insider threat, such as the following:

- Executive staff
- Directors
- Employees with access to data

If you have to identify any potential data source(s) for when we have an investigation, you will need to examine the following:

- Company-issued laptops
- Company-issued tablets
- Cell phones or mobile devices
- Any cloud account access

You will have to correlate the user and the user's devices with access to the critical data, and the team will have to identify the critical data beforehand. When should insider threat investigation be initiated? Typically, this will start with a notification from Legal or Human Resources. The organization

could also implement a policy investigating when an employee leaves the organization.

If the employee's position gives them access to sensitive or privileged information, then a review of their activities within the organization should be conducted. This could start in a broad sense; you are looking to gather data from mobile devices, laptops, desktops, and potentially the cloud. Then, you take that dataset and filter it to reflect access to the critical information.

Once the employee has resigned or the organization has decided to terminate the employee, the data collection process should start. The data collection process should begin before the employee is told they will be terminated. I recommend that the organization collects between 30 and 90 days' worth of activity for the employee. The more data is acquired, the better informed the investigator will be of the employee's actions. Some of the artifacts that may help determine whether the employee has exfiltrated data are as follows:

- USB devices
- Cloud accounts
- Sharing of files via social media
- Burning a CD/DVD

You will also analyze the activity around the critical data. This should be a standard activity so that there is an understanding of what is normal. Then, you must monitor the data to get that normal baseline to understand when the unusual traffic occurs. For example, you could monitor the traffic to the critical data, and suddenly, access to that data spikes. Does an attack cause this spike, or is it normal because it is the end of the pay period and accountants access the data as part of standard processing?

Another example could be whether the data is accessed after regular business hours. Is there a legitimate reason for that access? These are the circumstances that need to be identified before the investigation starts. This foreknowledge will allow you to filter out all the baseline information and focus only on that data outside of the norms.

The investigation may show no malicious intent or indicate there was malicious intent. Either way, you report the findings to the team to determine the next steps. This could lead to a review of policies and procedures and new controls to mitigate future attacks.

How effective is digital evidence when used in criminal or civil proceedings? There are many variables in play during the trial, from the jury members (if there is one) to the ability of the lawyers to present the digital evidence in the most favorable light to help them accomplish their goal. Then you must consider the expert witnesses that will testify about the digital evidence.

The effectiveness of the expert witness to explain a highly technical subject to a non-technical audience is going to be critical.

## Case studies

The following case studies are snapshots of what you may see during administrative or judicial proceedings. Be advised that there will be many proceedings where the court (or an official of the proceeding) will not release the digital evidence to anyone outside of the proceeding. Potential explanations can include the digital evidence that will contain contraband, such as **child exploitation material (CEM)**, also known as **child sexual abuse material (CSAM)**, or it may contain sensitive information, and the court has ruled to keep the material private.

### Dennis Rader

One of the first national cases dealing with digital evidence I became aware of when I started my forensic training was the **Bind Torture Kill (BTK)** serial killer Dennis Rader.

Initially, as a youth Rader had sexual fantasies about women that he considered trapped and helpless. Rader also exhibited other troubling behavior such as killing and torturing small animals and voyeuristic

behavior by spying on female neighbors. When Rader reached adulthood, he dropped out of college and joined the United States Air Force for four years. After being released from active duty, he moved to the Wichita, Kansas area. Rader was soon married and ultimately had two children with his wife.

Rader had a variety of employment types, including a security system installer for ADT, an animal compliance officer for Park City, Kansas, and an operations supervisor for the U.S. Census. In addition, Rader was involved in the community as a Cub Scout leader and was elected president of his Church Council.

Rader started his killing spree in January 1974, when he killed four members of the Otero family. The killings were discovered when the children returned home from school. In October 1974, Rader described the killings in great detail in a handwritten letter he placed in an engineering book in the public library. Rader continued his killing during the spring of 1974 until the end of 1977. During this timeframe, he killed three more women. In 1978, the television station KAKE received a letter written by Rader that claimed responsibility for the deaths of the Otero family and of the three women (Kathryn Bright, Shirley Relford, and Nancy Fox). The letter's contents included suggestions for a nickname that the new station could use when reporting on the murders. This is where the BTK nickname originated. A second letter was received by the television station, which demanded greater media attention. Rader killed his last victim, Dolores Davis, in January 1991.

In 2004, Rader started communicating with the local media. Numerous letters and packages were sent to the television station and placed in the community. Some items included identification cards, threats to law enforcement, and dolls posed with the limbs bound in a plastic bag over its head. One item left by Rader included a cereal box that he placed in the bed of a pickup truck that was parked in the parking lot of a Home Depot store. When Rader asked law enforcement about the cereal box, he realized they had not found the box. The pickup truck owner had thrown the cereal box into the trash. When law enforcement went to the parking lot, they were able to recover the cereal box, which contained a question that Rader had



about using a floppy disk in his communications with law enforcement. Rader asked if he stored his writings on a floppy disk, would law enforcement be able to trace its origins. Rader told law enforcement to respond by posting a message in the local newspaper with the words “Rex, it will be okay.” Law enforcement was able to find security CCTV footage that showed an unidentified man driving a black Jeep Grand Cherokee that stopped near the pickup truck and then the driver walking around the truck.

In February 2005, a television station, KSAS, received a package that contained a Memorex floppy disk, a letter, a necklace, and a copy of the cover for the book “Rules of Prey.”

When the investigators conducted a forensic examination of the floppy disk, they were able to recover a previously deleted Microsoft Word document. The embedded metadata contained information about the organization that registered this version of Microsoft Word; in this case, the examiners found “Christ Lutheran Church” in the organization name in the embedded metadata. The metadata also included the last user to modify the document, which was identified as “Dennis.” An Internet search identified Dennis Rader as the church council president for the Christ Lutheran Church.

Physical surveillance revealed that Rader owned a black Jeep Grand Cherokee. Law enforcement was able to get a search warrant to collect Rader’s daughter’s DNA from a Pap smear and compare the DNA found on the victims. The test showed there was a family relationship between the two samples. Rader was then arrested, tried, and convicted. Rader was sentenced to ten consecutive life sentences.

## **Silk Road**

Silk Road was the first online black market hosted on the dark web. This required the use of the Tor browser, which allowed anonymous users to access the vendors without fear of their traffic being monitored by a third-party. The founder of Silk Road was known by the pseudonym “Dread Pirate Roberts,” later identified as Robert Ulbricht.

In February 2011, Ulbricht launched Silk Road, taking its name from the historical trade routes between India, China, and Europe and using the Tor network combined with the cryptocurrency Bitcoin for anonymous transactions between anonymous users.

The success of Silk Road led to an article written by Adrian Chen titled “The Underground Website Where You Can Buy Any Drug Imaginable” and published on the website Gawker. As the public noticed, so did law enforcement and the federal government. First, multiple different agencies started their investigations, and the **Federal Bureau of Investigation (FBI)** started a deep examination of the Tor network to identify potential vulnerabilities. Next, the **Internal Revenue Service (IRS)** began to follow the money to understand how anonymous users could purchase services being offered on Silk Road. Finally, the **Drug Enforcement Administration (DEA)** and the **Department of Homeland Security (DHS)** focused their efforts on interdiction by identifying the packages of illegal drug shipments being sent to the country.

The IRS dug deep into the origins of Silk Road. Investigators started researching internet traffic, such as posts to message boards, newsgroups, and discussion forums, looking for information that a user or administrator may have posted at the same time as when Silk Road was open to the public. They were able to unearth a posting about Silk Road to a discussion forum by a user with the username “Altoid.” As the investigators started following the history of Altoid, they found a posting that listed a Google Plus account that the investigators traced back to Robert Ulbricht. Unfortunately, there was no evidence linking Ulbricht to Silk Road or even that Ulbricht had computer systems or networking background.

In July 2013, **Homeland Security Investigations (HSI)** intercepted a package that contained counterfeit identification cards that had Ulbricht’s picture. The intercepted package was intended to be delivered to Ulbricht’s address in San Francisco, California. HSI agents followed up on the counterfeit identification investigation and spoke to Ulbricht. At that time, the agents were unaware of the connection between the Silk Road investigation and Ulbricht.

The FBI continued its investigative efforts to identify any vulnerabilities that could lead to other investigative endeavors to identify the operators and users of Silk Road. The agents were able to locate an IP address that a coding error exposed on the Silk Road website. The IP address returned to geolocation within the country of Iceland. The Icelandic government agreed to cooperate with the FBI and created a clone backup of the server, but unfortunately, the server's contents were encrypted. Ultimately, the FBI broke the encryption, and the server's contents were now available to be examined. Armed with this information, the FBI created a mirror of the Silk Road servers and identified employee information, accounting information, and copies of chats between users.

One chat included the user "Dread Pirate Roberts." The chat contained information that Dread Pirate Roberts had agreed to pay for the murder of an adversary. Additional chats found that Dread Pirate Roberts had often engaged with individuals to pay for them to kill people that were considered to be a danger to Dread Pirate Roberts.

Finally, in July 2013, the different agencies investigating the Silk Road website sat down and shared information. When the IRS brought up Robert Ulbricht's name, the four agencies were able to conduct a thorough background check. The background check identified that Ulbricht had traveled to Dominica, which is used by individuals wishing to hide their monetary proceeds from the US government. They were also able to locate an email address used by Ulbricht, which also matched a user account on the servers.

The FBI then started physical surveillance of Ulbricht and was able to match Dread Pirate Roberts's activity with Ulbricht's activities. In October 2013, they decided it was time to arrest Ulbricht.

There was a concern that Ulbricht could destroy the digital evidence before they took Ulbricht into custody. The FBI waited until Ulbricht went to the public library and opened his computer. The Silk Road had hired an FBI undercover agent as a new employee and sent Dread Pirate Roberts a message to check a post from an admin account that had been flagged. When the undercover agents saw Ulbricht interfacing with his computer, they created a distraction. A male and female undercover agent started a

verbal argument that turned physical. When Ulbricht was distracted, an undercover agent came up and took the open laptop and immediately passed it to another agent. They then took Ulbricht into custody without further incident. When the investigators examined the laptop, the investigators found that full disk encryption was active. When agents completed the examination of the computer, the investigators had found nearly 150,000 bitcoins, accounting information for the Silk Road web page, a listing of all the Silk Road servers, and diary entries made by Ulbricht listing the creation and operational details of Silk Road.

The FBI then took down the Silk Road website, and Ulbricht was tried and convicted.

## **San Bernardino terror attack**

Terrorists carried out a coordinated attack in San Bernardino, California, on December 2, 2015. The attack was a coordinated attack using semiautomatic rifles and explosives. A training event and Christmas party hosted by the Department of Public Health was the target of the attack conducted by Syed Farook and Tashfeen Malik. Farook and Malik were married and lived in Redlands, CA. The death count was 14, and 22 people were critically injured in the attack. Farook was born in the United States and was an employee of the Department of Public Health. Malik was born in Pakistan and was a legal resident of the United States.

The investigation labeled Farook and Malik as “homegrown violent extremists.” They were not a member of any terrorist cell or terror network. It is believed that Farook and Malik became radicalized before the assault, declaring their devotion to jihadism and martyrdom in private conversations with each other before the incident took place. Farook and Malik had accumulated weapons, ammo, and bomb-making material in their house.

On February 9, 2016, a report from the FBI stated they could not unlock an iPhone 5C, which belonged to the county and was issued to Farook as a part of his employment. The **National Security Agency (NSA)** was asked to break into the phone, but they could not do so. The FBI then asked

Apple to create a RAM-based operating system to bypass the iPhone's security. Apple declined the request because of its policy never to undermine the security elements of the software. Apple's response caused the FBI to request a United States magistrate judge issue a court order requiring Apple to develop and furnish the software to the FBI. The magistrate judge granted the request.

Apple considered constructing a backdoor of this type a significant security concern to its users and challenged the ruling.

The United States **Department of Justice (DOJ)**, in response to Apple's denial, then requested the court to force Apple to comply with the court's order. The DOJ informed the court the FBI would deploy the software and would allow Apple to remove the software via a remote connection on the phone.

Apple reported they presented other options to the FBI to access the data stored in the iPhone. However, the FBI's actions had removed one of the more promising methods because of an operational error. When the FBI recovered the shooter's phone, they asked San Bernardino County to reset the user's iCloud account password. This would allow them to access the data stored in the iCloud backup. However, when the county reset the password, the phone could not be backed up to iCloud unless the user entered the passcode on the phone.

On March 28, the DOJ withdrew the lawsuit against Apple because it reported they had unlocked the iPhone. Several scenarios were reported on how access was granted to the phone's data: the Israeli business Cellebrite agreed to assist the FBI, or the FBI paid threat actors to exploit a zero-day vulnerability in iOS.

Apple's refusal to comply with the court order elicited a mixed response from the public. A CBS poll showed that 50 percent backed the FBI, and 45 percent supported Apple.

## **Theft of intellectual property**

It is not only criminal matters that you may come across; civil matters also require a forensic investigator. The following case study is from the firm Cyber Diligence, Inc.

The firm was hired to assist the legal team of a world-renowned scientist who was accused of stealing intellectual property from his previous employer, with the matter being filed in federal court. This matter had a large amount of discovery dealing with computer forensics. There was a concern that the previous employer was abusing the process to keep the client from working with another employer. The previous employer did not have a non-compete agreement with the client. The previous employer wanted to get an injunction because they believed the client had stolen intellectual property. The client's law firm provided copies of all the court documents and discovery, including transcripts of depositions and expert statements. A review of the documents showed the previous employer did not suspect intellectual property theft before they filed the case.

The previous employer did not conduct a forensic analysis on the workstations used by the client before they filed in federal court. The statements of the forensic expert contained inaccurate information, such as the client removed emails from the employer because the modified date time stamps of the OST file showed the file had been modified the day before the client left the organization.

An OST file (.ost) is used with Microsoft Outlook. This file allows users to work offline. When the user regains connectivity, they can synchronize any changes with the Exchange server

The expert statement related that this was proof that the client had extracted emails that belonged to the organization. The expert could not think of a valid reason a user would create an OST file other than for illegal purposes. Outlook creates OST files when the client connects to the Exchange server. This is an automated process and not user-initiated. The modified timestamp indicates when the contents of the OST file have been changed, such as receiving and sending emails. An interview with the client was conducted to understand the network configuration of the previous employer. Consultations with the client's legal team helped develop a plan

to address the expert statements, which were prolonging the matter and draining the client's financial resources.

The client's legal team requested the digital evidence for examination by the forensic team. The forensic team performed their analysis in preparation to depose the opposing forensic expert. It was also noted that the previous employer's legal team filed the expert's statements, which lacked a digital or physical signature of the expert. When the forensic images of the workstations used by the client were examined and compared to the "facts" presented in the six statements of the expert, they found the findings to be inaccurate. The next step was to interview the defense expert, which was much harder than it should have been. Ultimately, the federal judge, hearing the matter, ordered the previous employer to produce the expert and to make them available to the client's legal team.

Their expert stated he did not make the conclusions found in the reports, nor were they the reports he created. The expert reports filed by the previous employer's legal team were fabricated. The district judge threw out the case on a summary judgment, and they ordered the previous employer to pay for the client's legal fees.

## Summary

In this chapter, you have gained an understanding of the different types of issues you may encounter during a digital forensic examination. You have learned how the digital world and the physical world interact and how to use the digital world to help prove or disprove allegations. You have gained an understanding of different procedures and how to collect and manage evidence when investigating allegations of wrongdoing.

In the next chapter, we will discuss the forensic analysis process to maximize the efficiency of your investigation.

## Questions

1. Peer-to-Peer filesharing is used to share illegal files only.
  1. True
  2. False
2. What does a first responder identify?
  1. Potential victims
  2. Witnesses
  3. Subjects
  4. All of the above
3. You may find digital evidence in every type of investigation.
  1. True
  2. False
4. Which amendment of the U.S. Constitution protects the rights of citizens from unlawful search and seizure?
  1. First
  2. Second
  3. Third
  4. Fourth
5. What is a “binary”?
  1. A star
  2. An attached file
  3. A USENET post
  4. A web browsing artifact
6. What is required in the United States to obtain subscriber information?
  1. A search warrant
  2. A subpoena
  3. Consent
  4. Hacking
7. Criminals use social media for illegal purposes.
  1. True
  2. False

The answers can be found in the back of this book, under *Assessments*.

## Further reading



John Vacca and Michael Erbschloe. *Computer Forensics: Computer Crime Scene Investigation*. Charles River Media, 2002 (available at <https://www.amazon.com/Computer-Forensics-Investigation-CD-ROM-Networking/dp/1584500182>)

## Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

<https://packt.link/CyberSec>