EXPERT INSIGHT

Learn Computer Forensics

Your one-stop guide to searching, analyzing, acquiring, and securing digital evidence

Second Edition

William Oettinger

‹packt›

Learn Computer Forensics

Second Edition

Your one-stop guide to searching, analyzing, acquiring, and securing digital evidence

William Oettinger

‹packt›

BIRMINGHAM—MUMBAI

Learn Computer Forensics

Second Edition

Senior Publishing Product Manager: Aaron Tanna

Acquisition Editor – Peer Reviews: Saby Dsilva

Project Editor: Amisha Vathare

Content Development Editor: Liam Draper

Copy Editor: Safis Editing

Technical Editor: Aniket Shetty

Proofreader: Safis Editing

Indexer: Manju Arasan

Presentation Designer: Pranit Padwal

First published: April 2020

Second edition: July 2022

Production reference: 1220722

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham
B3 2PB, UK.

ISBN 978-1-80323-830-2

www.packt.com

Contributors

About the author

William Oettinger is a veteran technical trainer and investigator. He is a retired police officer with the Las Vegas Metropolitan Police Department and a retired CID agent with the United States Marine Corps. He is a professional with over 20 years of experience in academic, local, military, federal, and international law enforcement organizations, where he acquired his multifaceted experience in IT, digital forensics, security operations, law enforcement, criminal investigations, policy, and procedure development. He has earned an MSc from Tiffin University, Ohio. When not working, he likes to spend time with his wife and his three miniature schnauzers.

This book is dedicated to IACIS and the pioneers of this field whom I have had the privilege of meeting and learning from. Mike Anderson and Will Docken were some of the first professionals I met, and they had a significant impact on me as I started in this field. I want to thank Eric Zimmerman, Harlan Carvey, Brett Shavers, and Steve Whalen for their work for the forensics community. Your information sharing and work have impacted me and helped me grow as an examiner. There is a long list of people who contributed to my success that I want to thank: Larry Smith, David Papargiris, Tom Keller, Dave McCain, Steve Williams, Scott Pearson, Scot Bradeen, Matt Presser, Mike Webber, and everyone else who has helped me along the way.

About the reviewer

Steve Whalen is a Certified Computer Forensic Examiner (CFCE) with degrees in Psychology and Sociology and served as a Delaware State Trooper. As a state trooper, Steve worked as a detective with the Criminal Investigations Unit and served as their first full-time forensic examiner for digital evidence. Building off this experience, Steve helped the Delaware State Police develop its first High Technology Crimes Unit in 2001, where he processed thousands of electronic devices and media containing digital evidence from hundreds of cases relating to intrusion, financial crimes, child sexual exploitation, narcotics, stalking and homicides.

After retiring from law enforcement, Steve co-founded SUMURI, a leading provider of hardware, software, training and services relating to digital evidence and computer forensics worldwide. Steve was the designer of the successful Macintosh Forensic Survival Courses, RAPTOR, PALADIN, CARBON and RECON forensic software, and TALINO workstations.

Steve has developed and delivered forensic training to thousands of investigators and examiners around the world through organizations such as the International Association of Computer Investigative Specialists (IACIS), the High Technology Crimes International Association (HTCIA) and the US Department of State Anti-Terrorism Assistance Program. Steve has over 20 years of experience in computer forensics and has provided training throughout North America, Asia, Europe, the Middle East, the Caribbean, Africa and Oceania.

Wanting to do more, Steve founded the non-profit company Red Stapler Inc. and used his knowledge of digital forensics, psychology, sociology to create a “first of its kind” software solution (`https://www.catchapredator.org/`) to combat the sexual exploitation of children in a way that has never been done in all of history.

Join our community on Discord

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

`https://packt.link/CyberSec`

Table of Contents

Preface

Welcome to the world of digital forensics! In this book, you will be going into the depths of the Windows operating system to determine the user's actions on the system. You will also learn about the different filesystems used by the Windows operating system. The role of the examiner is not only about the examination, but also about the report you generate and how you explain your findings. You will learn how to prepare for a digital investigation, including equipment selection, training, and planning a response to the crime scene. It is my hope that this book will be your resource if you are a novice examiner or an experienced examiner.

This book teaches forensic examiners and those who want to become forensic examiners about the various skills and tasks required to be a forensic examiner, completing forensic analyses in either criminal or civil matters. This book will deliver information through the lens of the author's experience in the United States of America so references to criminal matters will involve American law.

Who this book is for

This book is for the novice and experienced examiner in private or public employment sectors. While an understanding of operating systems, file systems is helpful, it is not required.

What this book covers

Chapter 1, *Types of Computer-Based Investigations*, introduces to the reader the different topics of computer-based investigations, from criminal acts investigated by the police to potentially illegal actions performed by an employee or third parties and examined by a non-governmental investigator. While the goal is the same—to present evidence about an incident—the methods of the two slightly differ. It is essential for the reader to understand the similarities, that is, being able to present evidence in judicial proceedings, and recognize the differences, that is, search warrant requirements for a government agent.

Chapter 2, *The Forensic Analysis Process*, details the critical thinking in the planning of providing digital investigative services. This topic will allow the reader to create a strategy to conduct an efficient investigation. The reader will learn to offer different approaches to conduct an investigation depending on the unique set of circumstances for each matter.

Chapter 3, *Acquisition of Evidence*, explains that digital evidence is one of the most volatile pieces of evidence an investigator can handle. The mishandling of digital evidence can severely impact an investigation. Additionally, you may destroy the entire dataset. This chapter will address how to minimize or eliminate these issues when using a validation process to create a forensic image.

Chapter 4, *Computer Systems*, explains that the investigator must control the computer processes while acquiring digital evidence. When dealing with the many combinations of operating systems and hardware, you must implement controls to protect the integrity of the evidence. This chapter will discuss the boot process in detail and identify the most commonly used filesystems.

Chapter 5, *Computer Investigation Process*, explains that being a forensic examiner is much more than pushing a button. Once the evidence has been collected, you have to analyze the dataset. It is not about finding artifacts but rather examining the data and putting it into a context that will either support or not support the hypothesis about the user's actions on the system.

Chapter 6, *Windows Artifact Analysis*, explains that Microsoft Windows is by far the most common operating system today. In this chapter, we will look at the different versions of Windows and will show the reader how to identify and recover common artifacts based on the release of Windows being examined.

Chapter 7, *RAM Memory Forensic Analysis*, covers the analysis of RAM, which is a source of evidence that has recently been recognized as containing vital information about the user's actions on the system. RAM is very volatile evidence and can provide data that cannot be found anywhere else on the computer system.

Chapter 8, *Email Forensics – Investigation Techniques*, discusses email, which is a part of everyday life. This communication vector can be one of the primary communication tools for the majority of the population. These communications can contain incredible amounts of data related to an investigation. The investigator must be able to reconstruct the path that email took from the source to the destination to determine its validity.

Chapter 9, *Internet Artifacts*, explains that using the internet is a daily activity for the majority of the population. Like any other activity, the internet can be used for legal, law-abiding business, or for criminal activity. The internet can be accessed in a variety of ways. The forensic investigator must be able to analyze all these different aspects of the internet to get to the truth of the matter.

Chapter 10, *Online Investigations*, discusses how to use open-source intelligence techniques to learn about the target of the investigations. Also discussed are the steps an investigator can take to hide their true identity and create an undercover online persona.

Chapter 11, *Networking Basics*, explains some of the common network protocols, hardware and models that are being used to connect devices and share information. The ability to understand how information is shared between devices is a critical skill for the online investigator.

Chapter 12, *Report Writing*, covers report writing, which is not the most exciting portion of the forensic exam process. The forensic examiner must be able to explain a technical topic to a non-technical user. As a forensic examiner, you must be able to place that artifact into a context that the audience understands. This ability is a critical skill that you need to master to be a competent forensic examiner.

Chapter 13, *Expert Witness Ethics*, explains that a forensic examiner must be objective, truthful, honest, and perform their due diligence when conducting an examination. The examiner will be providing testimony that may result in someone losing their freedom. The ultimate goal of the investigation conducted by the forensic examiner is to provide testimony or evidence in a judicial or administrative proceeding to stop the cybercriminal's activity.

Download the exercise files

You can download exercise files for this book from at `https://github.com/bill-lcf/Learn-Computer-Forensics`.

Employed academic faculty can also download PowerPoints for each chapter and a question bank after validation. Send an email to `verify@learncomputerforensics.com` from an `.edu` email address requesting access. If you do not have an `.edu` email address, please send proof that you are an instructor.

Once the files are downloaded, please make sure that you unzip or extract the folder using the latest version of:

- WinRAR / 7-Zip for Windows
- Zipeg / iZip / UnRarX for Mac
- 7-Zip / PeaZip for Linux

We also have other code bundles from our rich catalog of books and videos available at `https://github.com/PacktPublishing/`. Check them out!

Download the color images

We also provide a PDF file that has color images of the screenshots/diagrams used in this book. You can download it here: `https://static.packt-cdn.com/downloads/9781803238302_ColorImages.pdf`.

Conventions used

There are a number of text conventions used throughout this book.

`CodeInText`: Indicates code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles. For example: "Outlook stores email information in several file types, such as `.pst`, `.mdb`, and `.ost`."

A block of code is set as follows:

```
MIME-Version: 1.0
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit
```

When we wish to draw your attention to a particular part of a code block, the relevant lines or items are set in bold:

```
{"endpoint_info_list":[{"endpoint":"smtp:badguy27@yahoo.com",
"c_id":"d24c.2d00",
"c_name":"Joe Badguy Smith"},
{"endpoint":"smtp:badguyneedslove@gmail.com",
"c_id":"e80f.5b71","c_name":"John Badguy Smith"},
{"endpoint":"smtp:yahoo@mail.comms.yahoo.net",
"c_id":"624f.10f0","c_name":"Yahoo! Inc."}]}
```

Any command-line input or output is written as follows:

```
$USER$\AppData\Local\Google\Chrome\User Data\Default
```

Bold: Indicates a new term, an important word, or words that you see on the screen. For instance, words in menus or dialog boxes appear in the text like this. For example: "The **MSF** files are **Mail Summary files**, one part of the email."

Warnings or important notes appear like this.

Tips and tricks appear like this.

Get in touch

Feedback from our readers is always welcome.

General feedback: Email `feedback@packtpub.com` and mention the book's title in the subject of your message. If you have questions about any aspect of this book, please email us at `questions@packtpub.com`.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you reported this to us. Please visit `http://www.packtpub.com/submit-errata`, click **Submit Errata**, and fill in the form.

Piracy: If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at `copyright@packtpub.com` with a link to the material.

If you are interested in becoming an author: If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit `http://authors.packtpub.com`.

Share your thoughts

Once you've read *Learn Computer Forensics, Second Edition*, we'd love to hear your thoughts! Please `click here to go straight to the Amazon review page` for this book and share your feedback.

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

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:

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:

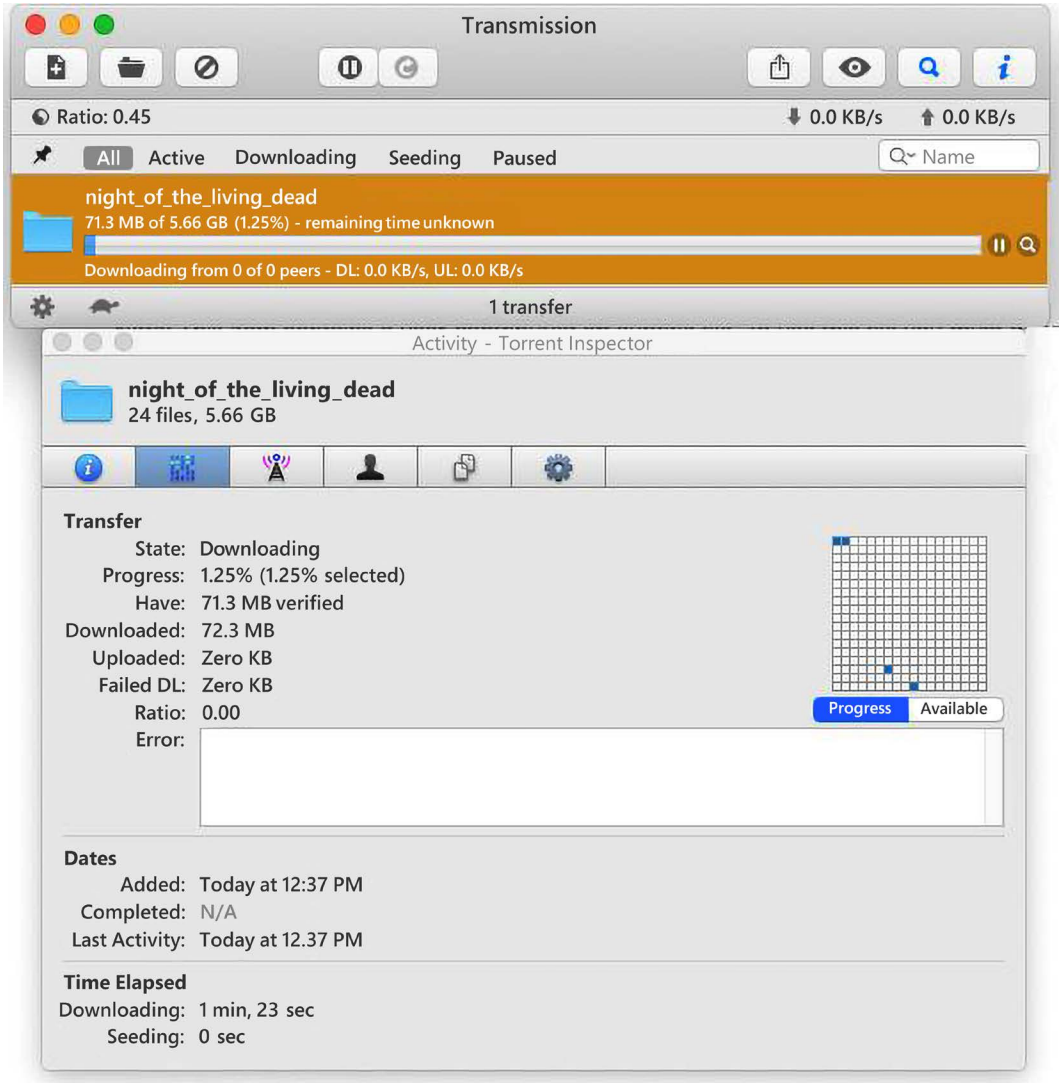


Figure 1.2: Transmission application

The preceding screenshot shows the **Transmission** program running on macOS. I am downloading a movie from the public domain (`archive.org`), 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:

White Hat	**Black Hat**	**Activist**
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:

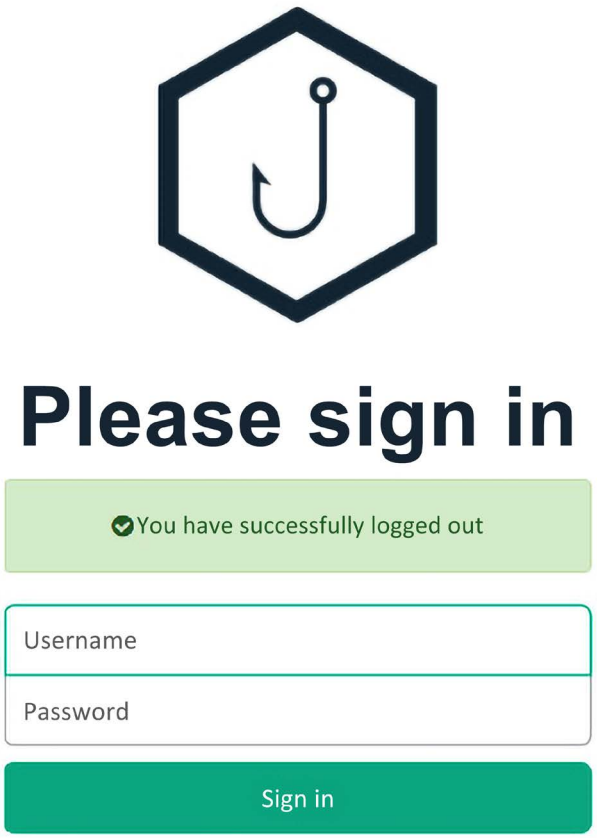


Figure 1.3: Gophish login

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:

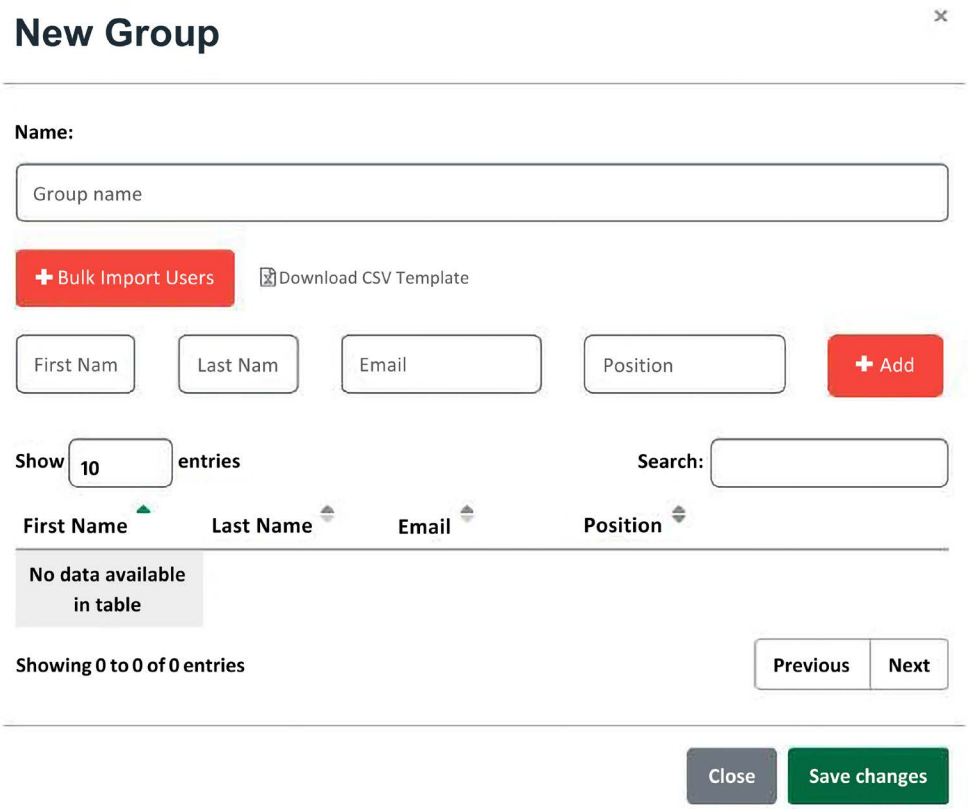


Figure 1.4: Gophish import emails

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.

   a. True

   b. False

2. What does a first responder identify?

   a. Potential victims

   b. Witnesses

   c. Subjects

   d. All of the above

3. You may find digital evidence in every type of investigation.

   a. True

   b. False

4. Which amendment of the U.S. Constitution protects the rights of citizens from unlawful search and seizure?

   a. First

b. Second

c. Third

d. Fourth

5. What is a “binary”?

a. A star

b. An attached file

c. A USENET post

d. A web browsing artifact

6. What is required in the United States to obtain subscriber information?

a. A search warrant

b. A subpoena

c. Consent

d. Hacking

7. Criminals use social media for illegal purposes.

a. True

b. False

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

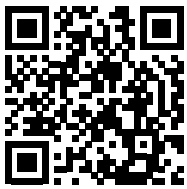
Further reading

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`



2

The Forensic Analysis Process

We will now discuss the forensic analysis process. As a forensic investigator, you will need to create a strategy that will enable you to conduct an efficient investigation. You also need to make sure you are familiar with your tools and the results that they will provide. Without a process, you will waste time examining data that will not impact your investigation, and you will not be able to rely on your tools. In addition, you want to make sure you get valid results from the tools you deploy. Finally, to be thorough and efficient, you must use critical thinking to determine the best investigation or exam method.

While there are similarities in every investigation, you will find differences that will require you to have an exam strategy to be efficient. I am not a fan of keeping an examination checklist because there will be areas that aren't relevant, such as different operating systems, physical topography of the network, criminal elements, and suspects. These variables ensure that no two examinations or investigations are the same and will require the investigator to execute a different strategy for each of them.

The forensic analysis process is made up of five subsets:

- Pre-investigation considerations
- Understanding case information and legal issues
- Understanding data acquisition
- Understanding the analysis process
- Reporting your findings

The upcoming sections will discuss each of these in greater detail.

Pre-investigation considerations

The pre-investigation is where you determine your capabilities and equipment specifications to conduct a forensic exam, regardless of whether it is in the field or a lab environment. Now is the time to determine your hardware, personnel, and training budget. Some of those costs will not be a one-time expenditure but will be an ongoing budget expenditure. The equipment must be updated, personnel training must be maintained, and the purchase of new technology as it becomes available.

Being a digital forensic investigator is not about buying the equipment, going to a training class, and never updating either of these afterward. As technology changes, so do the methods of hiding data or conducting criminal activities, so the investigator must be ready to adjust to these changes.

Before you are ready to begin the investigation, you must prepare yourself. This will allow for greater efficiency and a better work product. This includes preparing your equipment and becoming familiar with the current laws and legal decisions and the organization's policies and procedures.

Some equipment will be reusable, and some will not. For the single-use items, make sure someone replaces them as soon as the incident concludes.

Note

I cannot tell you how many times I have responded to the scene with my "to go" kit only to find that another detective had already used it and not replaced the consumable equipment. It was my mistake for not checking it before I departed to go to the crime scene, and it was my partner's mistake for not replacing the items.

We will now discuss the equipment you will use as an investigator.

The forensic workstation

Whenever you get forensic investigators together, a common topic of conversation is the forensic workstation. How much **Random Access Memory (RAM)**? How many **Solid State Drives (SSD)** drives? Which **Central Processing Unit (CPU)**? Which **Operating System (OS)**? These are all questions that you might commonly hear. There is always a difference of opinion about the configuration of a forensic workstation. None of the views are incorrect because the investigator's workstation configuration depends on their budget and the cases that are being investigated.

Forensic workstations are not cheap. Depending on the skill level of the investigator, they can either build their own or purchase a pre-made forensic workstation. Several vendors will configure a workstation to your specification. For example, consider the vendor SUMURI (`https://sumuri.com`) and their TALINO workstations. The base model costs approximately $8,000 and comes with:

- Intel Core i9-10900X 3.7 GHz 10-Core LGA 2066 processor
- 32GB of DDR4 2666 MHz RAM
- 500GB M.2 NVMe SSD

That is a basic forensic workstation, and you still must add storage for the forensic images. The high-end version costs over $18,000 and comes with:

- Dual Intel Xeon Gold 5220 18-Core processors
- 128GB DDR4 RAM
- 1TB SSD for the operating system
- 1TB M.2 NVMe SSD for temporary files and processing
- 2TB M.2 NVMe SSD for databases
- Eight 6TB hard drives configured in RAID 10 for evidence
- A 30-series GDDR6 **Graphics Processing Unit (GPU)** such as the NVIDIA RTX 3070 or 3080

One bottleneck that a forensic investigator may face with their forensic workstation is data transfer. I suggest using SSDs because they have much higher throughput than the typical spinning disk does. A fast CPU and a large amount of RAM enable maximum performance for forensic analysis. However, these machines are not portable, and you are not always able to perform the analysis or to acquire the data from the relative comfort of your workstation. A forensic laptop is also an expensive piece of equipment. At the time of printing, the TALINO OMEGA comes with:

- Intel Core i9-11900K processor
- 64GB DDR4 2933 MHz RAM
- 500GB M.2 NVMe SSD for the operating system
- 250GB M.2 NVMe SSD for temporary files and processing
- 1TB M.2 NVMe SSD for database
- 2TB M.2 NVMe SSD for evidence files
- NVIDIA GeForce RTX 3080 GPU with 16GB GDDR6 video memory

Note

You will need to include Gigabit Ethernet on both workstations to communicate on the local area network.

As you can see, you can never have too much CPU, RAM, or storage space on your forensic workstations. The equipment I described is on the higher end; you can conduct digital forensic examinations with less expensive equipment and still achieve the same results. In addition, the more high-end equipment will decrease the time involved. If you are a member of a multinational corporation or a large law enforcement agency, you may have the budget for high-end equipment. A smaller law enforcement agency, a smaller organization, or a single practitioner will have to determine what cost is more appropriate for their situation.

Sometimes you must leave the lab, which means you need additional portable equipment. We will now discuss the equipment required in your response kit.

The response kit

The digital evidence is not always delivered to your workspace. Sometimes, you may have to respond to a third-party location to acquire that evidence. The collection of that evidence is the basic building block for any digital forensic examination you may conduct. Like conducting an examination in your workspace, you need the proper tools and supporting equipment to accomplish this task. You need to create a response kit that includes documentary paperwork, pens, and storage containers to store digital evidence.

A response kit is unique to each digital forensic investigator. No kit is perfect; all kits are always subject to improvement. The goal of your response kit is to have everything you need to collect digital evidence, and we will go over some equipment that, in my experience, I have found helpful:

- **Digital camera**: Capable of still and video recording. You need to document the scene as it was when you arrived. If you testify in official proceedings, you will show the fact-finder precisely what you saw as you arrived. Some organizations also video record all the actions of the digital forensic investigator's activities as they collect digital evidence.

Note

A word of advice: I would disable the microphone so as not to record audio. You may have extended discussions about how to proceed using language that may be regarded as less professional. These discussions and use of language could be used as a distraction by the opposing side in the presentation of evidence.

- **Latex or nitrile gloves**: These protect several aspects of the evidence collection — you are not leaving your fingerprints, and you are also protecting yourself from potential biohazards that may be on the scene. I am talking about blood, urine, feces, and any other biological fluid you can think of.
- **Notepads**: You need to document your actions on the scene. A notepad is a perfect repository to maintain that information. You can take notes about who you talk to, who secured the scene, and the basic facts of the case. When you begin the investigation, a lot of information will come at you, and it could be easy for you to forget a specific action if you do not record it. Some organizations also make a hand-written sketch of where the digital evidence is being collected. Your organization's policies and procedures will determine whether a sketch is required.
- **Organizational paperwork**: This could be a property report for seizing evidence, and it lists exactly what was taken, where it was taken from, and any specific identifying marks or serial numbers on the item being taken. You can also include labels or tags to identify items that contain digital evidence.
- **Paper storage bags/antistatic bags**: You have to put the containers of digital evidence somewhere to prevent any unauthorized access. Digital evidence is very fragile, and you want to make sure you do not store it in a manner where static electricity can be generated. Static electricity can render the storage media inoperative, and you will lose access to any data.
- **Storage media**: Hard drives can be a traditional spinning disk or SSD and USB devices. A corporate digital forensic investigator will not shut down a server to create a forensic image. Instead, they will collect the specific datasets in the form of log files, RAM, or user directories and store them on the appropriately sized storage media.

- **Write blocking devices**: This could be a hardware device, such as the Tableau TK8u USB 3.0 forensic bridge (`https://security.opentext.com/tableau/hardware/details/t8u`), which allows you to access a storage device without changing its contents. We will discuss the acquisition of evidence in much greater detail in *Chapter 3*, *Acquisition of Evidence*. Alternatively, you can use a forensic boot disk, such as SUMURI's PALADIN, a Linux distribution based on Ubuntu that allows the collection of digital evidence in a forensically sound manner. SUMURI offers PALADIN as a free download at `https://sumuri.com/software/paladin`.
- **Frequency shielding material**: This could include commercial aluminum foil, Faraday bags, or any container that will block radio transmissions. You will use this when you seize a mobile device to prevent the user from remotely wiping or resetting the device. Be aware, however, that when you place the device in these containers, the battery will quickly deplete, as it will attempt to reconnect to the network. If you have access to the mobile device's menu, you can put the device into airplane mode. Then, the device will no longer attempt to connect to the network. Ensure you document any changes you make to the device.
- **A toolkit**: A small precision toolkit with multiple screwdriver bits is used to disassemble laptops, desktops, or mobile devices to access the digital storage container. You want to make sure you have a variety of screw heads to match what the various manufacturers use. Sometimes, the manufacturers will use two or three different screw heads when assembling their devices.
- **Miscellaneous items**: This can include extra power cables, data cables, USB hubs, screws, or anything else that might be difficult to acquire when you are at the subject's location in the middle of the night, and no stores are available for you to purchase the missing item. If you are responding to a commercial site, keep a spare mouse and keyboard in case you need to access a server and they are not available. (If you are conducting network-based investigations, you may also want to include a network tap.) This subset comprises items you don't think are needed until you are onsite and need them.
- **A forensic laptop**: Make sure all your software is up to date. I recommend creating a folder containing digital versions of any forms you will use, any processes you need to document, and any applications you find helpful in carrying out your tasks.
- **Encryption**: If you are traveling out of the country to get to the target site, you might want to encrypt the target drives that contain the acquired data you need to analyze. It is not uncommon for security services or customs to seize devices. This will ensure the data you acquired will not be compromised.

- **Software security keys**: This is also referred to as a dongle. You will find commercial versions of software that require you to insert a USB-based security key to use it. You want to make sure you have them with you because the software cannot be used without the security key inserted.

Note

A program called VirtualHere (`http://virtualhere.com/home`) allows you to use your USB devices remotely. This will require a network connection at your destination and at your home location where the USB keys are plugged in. If you are unsure about the quality of your network connection, I recommend taking the keys with you.

Now, the important question is this: how do you carry all of this from one location to another?

My recommendation is a Pelican-type case that is watertight and crush-proof to protect the equipment. Also, include a TSA-compliant locking device if you must travel via commercial air in the United States.

The list of items we have just discussed is only a recommendation. You will add/subtract from this list to meet the needs of the task at hand. There is no right or wrong answer when stocking your response kit. The budget, the organization, and the task at hand will dictate what equipment is needed.

A government/law enforcement digital forensic investigator may acquire full forensic images at the scene, and they will need larger storage capacity devices. As you become more experienced, you will accurately determine what equipment you need to perform your duties.

The result is that you need to have a response kit when leaving the office to acquire digital data or respond to any incident. How you stock that kit is entirely up to you as the forensic investigator. This is all about making your job easier and more efficient.

That has covered some of the hardware and physical items needed. We will now move on to discussing software.

Forensic software

This is the software that you will use to analyze data. You have a choice of utilizing commercial software designed for the forensic process or open-source tools. You want to make sure that you use fully licensed software in your work environment.

There is nothing more embarrassing than an organization using pirated software to investigate and have that fact come out in the administrative or judicial proceeding. It will be a severe hit to your reputation if you use pirated software to conduct your investigation, and it will call into question your integrity, your ethics, the results of your inquiry, and the results provided by the forensic tool. I cannot stress this enough: you must use fully licensed software in the forensic process. So, what is the difference between open-source and commercially available tools?

Vendors make open-source software freely available for anyone to use. Typically, there are no restrictions on its use; you can use it for educational, profit, or testing purposes. The positive aspect is that it is available at no cost in most situations. The downside is that you will have little or no technical support if something goes wrong. It will depend entirely on your skillset and level of comfort working with these tools. In addition, many open-source tools use a **command-line interface** (**CLI**) and not a **graphical user interface** (**GUI**), which can intimidate new users.

A commercial tool will typically have better customer support, documentation, and timely updates. The downside is that you are paying for those services. In reality, most of the time anything that a commercial forensic tool can do, an open-source tool can do the same thing. A commercial tool may carry out multiple functions, while with an open-source framework you may have to use different open-source tools to accomplish the same task.

Neither choice is wrong. As a digital forensic investigator, you must know where the data came from and ensure that the tool provides an accurate representation of the data. It does not matter if the tool is an open-source or commercial version; you must validate the results provided by any tool. We will talk about validation a little further on in this chapter.

I often get questions about whether a particular piece of software is court-approved. Forensic software is not court-approved, but you need to explain in the administrative/judicial process whether the tool you used produces reliable results and is accepted within the forensic community.

In the United States, this is known as the Daubert standard, which comes from the Supreme Court case Daubert v. Merrell Dow Pharmaceuticals Inc., 509 U.S. 579 (1993). This standard is used to determine whether an expert witness's testimony is based on scientifically valid reasoning and can be appropriately applied to the facts of the matter. The factors the court considered are as follows:

- Whether the theory or technique can be or has been tested
- Whether it has been subjected to peer review and publication
- The known or potential error rate
- The existence and maintenance of standards
- Its acceptance within the scientific community

Initially, the courts only used the standard for scientific testimony. That changed with the Kumho Tire Co. v. Carmichael 526 U.S. 137 (1999) case; the Supreme Court clarified that the factors used in the Daubert decision could also apply to non-scientific testimony, that is, the testimony of engineers and other experts who are not scientists. So, as you can see, it is not so much the software being used but the expertise of the digital forensic investigator. Commercial forensic tools simplify the process and sometimes have a **find evidence** button. However, as the digital forensic investigator, you still must know where the forensic tool extracted the artifact from within the filesystem. (Your local jurisdiction may have different opinions.)

The **National Institute of Standards and Technology** (**NIST**) has sponsored the **Computer Forensic Tool Testing Project** (**CFTT**) (`https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt`), which has established a methodology for testing computer forensic software tools through the development of general tool specifications, test procedures, test criteria, test sets, and test hardware. This project provides a source for testing the results of forensic tools on its website. They also offer a collection of testing media to conduct your validation of forensic software. It is part of your best practices to validate the results of your forensic tools at least annually or whenever the tool is updated. It does not matter whether you are a government or private sector digital forensic investigator: you need to have confidence in your tools and be able to testify that you have tested and validated the process.

In 2011, this validation process was called into question during the trial of Casey Anthony. Casey Anthony was being tried on the following charges: first-degree murder, aggravated child abuse, aggravated manslaughter of a child, and four counts of providing false information to police, who were investigating the death of her child. During the trial there was a significant assertion by the prosecution was that someone searched for the term “chloroform” 84 times on Anthony’s computer. While the trial was ongoing, it was discovered that the forensic tool used by the digital forensic investigators had misinterpreted the values in the internet history database. The user had only visited the site one time, not 84 as reported. The software designer of the forensic tool realized the mistake while the trial was ongoing and notified the trial team of the error. My recommendation is that you have multiple forensic tools to validate your findings. For example, you could have two commercial forensic tools, one commercial and one open-source forensic tool, or two open-source forensic tools, but you need to validate your findings.

Some open-source forensic tools include the following:

- **Autopsy**: Autopsy is a fully functioning suite of forensic tools that allows you to conduct a complete forensic examination. It costs nothing and can be found at `https://www.autopsy.com`.

- **SIFT Workstation**: SIFT is a virtual machine that uses the Ubuntu operating system with multiple forensic tools pre-installed. It is free and can be found at `https://digital-forensics.sans.org/community/downloads`.
- **PALADIN Forensic Suite**: PALADIN is a live Linux distribution based on Ubuntu and has implemented several open-source forensic tools in a user interface called the PALADIN toolbox. It is free and can be found at `https://sumuri.com/software/paladin/`.
- **CAINE**: **Computer-Aided Investigative Environment (CAINE)** is a digital forensics project that provides a GUI and many open-source forensic tools for free. You can find it at `https://www.caine-live.net/`.

These are just a few of the open-source forensic suites available. There may be others out there that I haven't mentioned, or you may wish to use single-purpose tools. As long as you achieve the goal of finding the artifact to reveal the truth about the matter being investigated, it does not matter which tool you use. The key is to use your training and experience to explain the pertinence of the artifact and how you determined the tool is providing reliable results.

Here are some commercial forensic tools available for Windows-based users:

- **X-Ways Forensics**: `https://www.x-ways.net/`
- **EnCase**: `https://www.guidancesoftware.com/encase-forensic`
- **Forensic Toolkit (FTK)**: `https://accessdata.com/products-services/forensic-toolkit-ftk`
- **Forensic Explorer (FEX)**: `http://www.forensicexplorer.com/`
- **Belkasoft Evidence Center**: `https://belkasoft.com/ec`
- **Axiom**: `https://www.magnetforensics.com/products/magnet-axiom/`

Here are some Macintosh-based tools:

- **Cellebrite Inspector**: `https://cellebrite.com/en/inspector/`
- **RECON LAB**: `https://sumuri.com/software/recon-lab/`
- **RECON ITR**: `https://sumuri.com/software/recon-itr/`

A Linux-based tool is **SMART** (`http://www.asrdata.com/forensic-software/smart-for-linux/`).

This is just a sample of the commercial forensic tools available for use. Each tool will have its strengths and weaknesses, which can be debated endlessly with your fellow practitioners.

Right now, I prefer X-Ways as my primary tool, and I supplement it with FEX and Belkasoft Evidence Center.

You can have all the tools, software, and hardware, but how effective will you be without training? So next up are some training options for you to consider.

Forensic investigator training

If you travel on the path of a career in digital forensics, you will need to continually upgrade your skills and training, which must be considered an ongoing expense. Just because someone goes through a 40-hour course does not automatically make them a digital forensic investigator. Instead, they are taking the first steps down that career path, but they will need to continue to attend training sessions and associate with other like-minded peers.

Certification is not a guarantee that the user knows what they are doing. Instead, certification shows that the user met the minimum level to achieve that certification. There are many certifications available, and some are more worthwhile than others. Before joining an organization and participating in its certification process, you must do your due diligence and research the costs, availability, and whether that certification is accepted within the forensic community. Most certifying organizations will require annual dues and a yearly training requirement to recertify the certification. There are tool- and vendor-specific certifications where you are being tested on your ability to use the vendor's forensic tool and an understanding of the fundamentals of digital forensics. At the other end of the spectrum is tool-agnostic certifications. You can use any tool to complete the certification process.

This is a list of some of the certifications available:

- **Certified Forensic Computer Examiner (CFCE) (Tool-Agnostic)**: `https://www.iacis.com/`
- **EnCase Certified Examiner** (**EnCE**) (tool-specific): `https://www.Opentext.com/products-and-solutions/services/training-and-learning-services/encase-training/certifications`
- **ACE** (tool-specific): `https://training.accessdata.com/exams`
- **Computer Hacking Forensic Investigator** (**CHFI**) (tool-agnostic): `https://www.eccouncil.org/programs/computer-hacking-forensic-investigator-chfi/`
- **Global Information Assurance Certification** (**GIAC**) (tool-agnostic): `https://www.giac.org/certifications`
- **Certified Forensic Mac Examiner (CFME)** (tool-agnostic): `https://sumuri.com/mac-training/`

Now that we have explored the equipment and training options, you still must prepare by understanding the legal and case information pertaining to the specifics of an investigation. So, we will discuss legal issues next.

Understanding case information and legal issues

Let's talk about case information and legal issues. You must get this information before you even power up your workstation to look at the digital evidence. You will have to gather information from the person requesting your services. It would be best if you asked the following questions:

- What is the nature of the investigation? For example, is it a narcotics case, homicide, or employee misconduct? As you listen to this information, you formulate your plan on how you want to proceed.
- What digital evidence do you expect to find at the scene? I've had responses where the investigator was only looking for a single laptop, and once we were at the scene, we found multiple laptops, multiple desktops, and many mobile devices. Just remember the information you get may not always be accurate, so you also must be prepared for that eventuality.
- What is the legal justification? For law enforcement—what is the rationale behind the search? Consent? A search warrant? It doesn't matter whether it is written consent or a written search warrant: you need to read the search warrant and consent to understand the limits placed on the search. It may be physical limits within the scene or digital limits on what you can search for on digital devices.
- As a government and corporate digital forensic investigator, I have had limits on what I can search for or view on digital devices many times. Be aware of those limits; if you find relevant artifacts outside of the scope of the search authority, they cannot be used in the proceedings, and you may face sanctions if you do use them.
- Who are the subjects and suspects, and what roles do they play in the investigation? Now, depending on your role, you may or may not have any contact with the subjects and suspects involved. However, if you do have that ability, try talking to them. If you can have a civil conversation with them, you may get additional information about the digital containers and the data.

If you're thinking, "We have gathered information from the first respondents, and we have gathered information on the other subjects involved; now we can jump right in and collect evidence!"—well, not yet. You want to make sure the crime scene has been adequately documented and safe. For law enforcement, this will include removing extraneous personnel from the scene, restricting access, and allowing someone to record the scene.

The easiest way is to photograph everything. They may call you to testify in a proceeding 12, 18, 24, or even more months in the future. Lawyers may ask you where a specific item was and, unless you have a photograph (or sketch) of the scene, you may not be able to answer the question.

For a corporate investigation—for example, a hidden camera found in a confidential location—what do you do? The finder's actions may hamper your ability. For example, I investigated a hidden camera in a unisex restroom. A restroom user found the camera when the tape holding it to the bottom of the shelf released, and the camera fell to the ground. The user gave the camera to their supervisor. The supervisor opened the camera and removed the digital storage card. They then placed it into a card reader and plugged it into their computer. At least five other people handled the camera and the SD card, putting it into multiple computers before contacting me. Every time they plugged the SD card into a computer system, they changed the evidence. When you access the data on an SD card, you change the date and time stamps on the files you access. An organization has to train its members not to look at digital evidence when there is an incident and to call a professional. This will ensure that the evidence is contained in a state that allows it to be presented in a judicial or administrative proceeding.

This case required interviewing all the people involved, processing the digital camera and the SD card, and examining the five workstations. Since this was a corporate environment and, initially, law enforcement would not be involved, I took photographs of the workstations and the connections to identify the specific workstations and their users. Remember, we are in a corporate environment, and there are multiple versions of the same make and model of computers everywhere.

There will be times when you have been presented the digital evidence after someone else collected it. You still must ask questions, and the source of your answers may only be the investigative reports. You will want to know the following:

- Why was this item seized?
- Does it contain evidence of criminal activity or evidence considered exculpatory?
- Is there a chain of custody for this item?
- How many people have had access to it?
- Where was the item found?
- Was it found in a secured location or a common area of the site?
- Are there any date and time references?
- What should the investigation focus on?
- When does the investigator need the findings of the digital forensic exam?

You need to review the documentation before you start the evidence-collection process. When investigators bring you digital evidence containers such as computers, you need to ensure the search warrant authorized its seizure. There have been several cases where devices containing digital evidence were seized, but there was a grey area around the use of digital evidence.

The search warrant will come with limitations on your search. For example, if it is an illicit images investigation, you may be restricted to only viewing images. It is your responsibility to read all the judicial paperwork and understand what it authorizes and does not. Only then can you create a plan for how you stay within limits.

You also must anticipate what problems you may encounter as you conduct the digital forensic examination. For example, is there an aspect of the investigation where your training and experience could be lacking? This is not something to be ashamed of but should be acknowledged so you can reach out for help to increase your training and experience. What resources do you have available to assist you?

Once the legal portion of your preparation is done, we can move on to the next portion of the process. You must now deal with acquiring the data in a forensically sound manner.

Understanding data acquisition

So, let's recap: you have received training as a digital forensic investigator and may have received certification. You have built or purchased a digital forensic workstation and a forensic laptop and have created your response kit. You have responded to the scene and ensured that it had been made secure. You have verified that no one has altered the scene, and you have documented the scene with photographs. Now, it is time to process the scene and collect that digital evidence. We will now discuss the acquisition of data, otherwise known as evidence.

There are multiple scenarios where someone may call on you to acquire data for a digital forensic investigation. For example, as a law enforcement officer, you may respond to the scene, identify potential sources of digital forensic evidence, and then seize those items. As a private sector or corporate investigator, you may be called on to take an employee's workstation or respond to the server room (either physically or remotely) to collect the data you need to analyze. The procedures we will discuss in the next section can be utilized in every environment.

A source of potential evidence is volatile memory. In the past, the data contained within volatile memory was ignored with a "pull the plug" mentality. This was based on whether officers responded to a scene and the computer was up and running. Best practice required officers to pull the plug to shut the system down.

However, volatile memory is only available while a system is up and running. Therefore, when the investigator pulled the plug, they lost all that data, including any potential evidence. As the field of digital forensics has matured, we have learned that what we once considered best practice was, in reality, not.

To collect volatile evidence, we should start from the most to the least volatile. This is called the **order of volatility**, and it goes like this:

1. Live system
2. Running
3. Network
4. Virtual
5. Physical

We approach volatile data collection with the same mindset as creating forensic images. You must document the steps you take because you will interact with the machine to collect volatile data, which will change the evidence. In reality, the changes you make typically do not affect what you are investigating. But you should know that changes are being made to the system; you may get asked a question about potential changes to the evidence while testifying at the administrative or judicial proceeding. If you don't know the answer, it could be professionally embarrassing.

The changes you make while collecting the volatile data will impact the processes found in RAM. That is why you need to take notes and document everything you do. Some examples of volatile data we collect are the current state of the system networking information (the ARP table, connections, routing table, and name cache), the logged-on users, running services, running processes, shared drives, remote activity, and open encrypted containers.

We have to balance our changes versus the evidence that may be potentially lost forever. The term "forensically sound manner" means leaving the smallest possible footprint during collection to minimize the amount of data being changed with the collection. The order of collecting volatile data is significant because if you collect volatile data in the wrong order, you may destroy the evidence you are looking for. RAM is considered to be the most volatile of all volatile data, so we would want to collect that first.

Keep the following in mind:

- Collecting the volatile data may not always be possible, depending on the specific set of circumstances you encounter on the scene.

- If you find there is a destructive process running on the machine and the information you want to collect is being altered or overwritten, you may not want to take the time to collect the RAM as evidence is being manipulated.
- If it is a remote connection causing the destructive process, you need to document the connection, sever the connection, and then collect the RAM. Again, it depends on your investigation and the information you are trying to acquire.
- If the attacker is connected remotely and is accessing highly sensitive data, do you want the attacker to maintain access while you collect the RAM, or do you want to interrupt the connection? What if it is not critical information?
- Do you want to let the attacker continue to have access while you continue your processing?

Ultimately, the goal of digital forensics is to create a forensic image for analysis. Therefore, under normal circumstances, it is not appropriate to change digital evidence during collection.

In today's environment, that is not always possible. Due to the easy availability of full disk encryption or full volume encryption, it is no longer acceptable to pull the plug on computer systems.

Let's take a slight detour and talk about what encryption is. At a basic level, encryption is encoding information to protect the confidentiality of the information and allow only the person with the decryption key to access it. All encryption can be broken if the attacker has enough time.

With today's level of equipment, that time factor is measured in hundreds of years. As technology advances with increases in processing power, the time taken to decrypt top-level encryption decreases. So, what was considered secure encryption in the 1990s is now regarded as weak. That is why it is imperative not to pull the plug on a system where it is possible that encryption is being used. Without gaining access to the decryption key, you cannot get to the data.

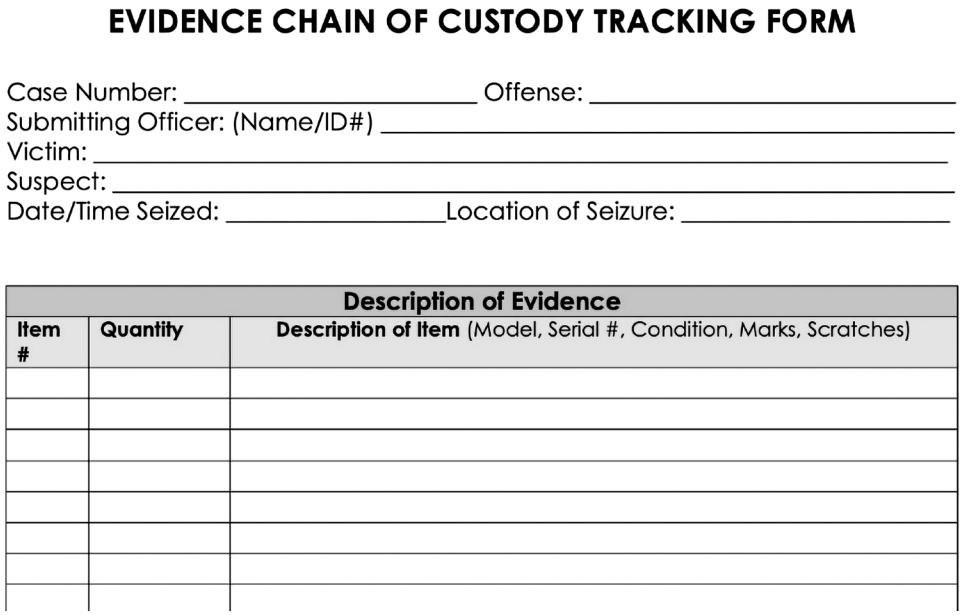
Every situation, every crime scene, and investigation will be different, which means the actions you take will be based on the specific set of circumstances you encounter. Utilize your problem-solving skills and make quick decisions based on the limited information you have available.

Now we have the evidence, how do we keep control of it? Let's talk about the chain of custody.

Chain of custody

Maintaining the **chain of custody** is an integral part of preserving and authenticating physical and digital evidence for an administrative or judicial proceeding. The chain of custody documents all access to the evidence, who accessed it, when it was accessed, and for what purpose it was accessed.

NIST provides a chain-of-custody document, shown in the following figure. It is a generic chain-of-custody form for you to use and adjust as needed and can be downloaded at `https://www.nist.gov/document/sample-chain-custody-formdocx`. The form is used to track the chain of custody and will be maintained every time evidence changes hands:



EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____
Submitting Officer: (Name/ID#) _____
Victim: _____
Suspect: _____
Date/Time Seized: _____Location of Seizure: _____

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)

Figure 2.1: An evidence form

As you can see, some fields may not be pertinent to you. For example, as a corporate digital forensic investigator, you may not need the **Victim** field, so you can change it or remove it altogether.

The goal of this form is to track the digital evidence and maintain control so that you may authenticate the evidence later. In the **Description of Evidence** field, you describe the container holding the digital evidence. It could be non-reusable media, such as a DVD with log files burned for later examination.

In the following figure, you can see the **Description of Evidence** section. The **Item** number refers to a sequential numbering system to help track the items. **Quantity** is the physical number of items, and the **Description of Item** field is self-explanatory:

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)
CD-001	1	Ultimate DVD contains server logs from AD001
HDD-001	1	Samsung SSD 1TB Ser#ABC9876
HDD-002	1	Samsung SSD 512 MB Ser#DEF4567
CP-001	1	Pixel XL 128 GB Ser# A5 12 D3 AC FD
TD-001	1	Generic Thumb drive 32GB (green) Unknown Serial Number
MD-001	1	Apple iPad 512 GB Ser# 09 E3 4D AB Rose Gold

Figure 2.2: A description of the evidence

For example, in the previous figure, a DVD is listed as item **CD-001**. You might impound several CDs or DVDs and have the problem of trying to differentiate one disk from another. It's not just CDs or DVDs but also hard drives. It won't often be that you will impound a single item of a specific media type.

I use the following numbering system as a part of my process:

- CD/DVD: **CD-XXX**
- Hard drive: **HD-XXX**
- Thumb drive: **TD-XXX**
- Cell phone: **CP-XXX**
- Mobile device (not a cell phone): **MD-XXX**

Note

As a side note, you also need to make a permanent mark on the items being seized, but you should try to do so in a manner that will not reduce the value of the item.

You can see in the following figure that the hard drive is marked as **HDD001** with the date and the initials of the officer seizing the device:

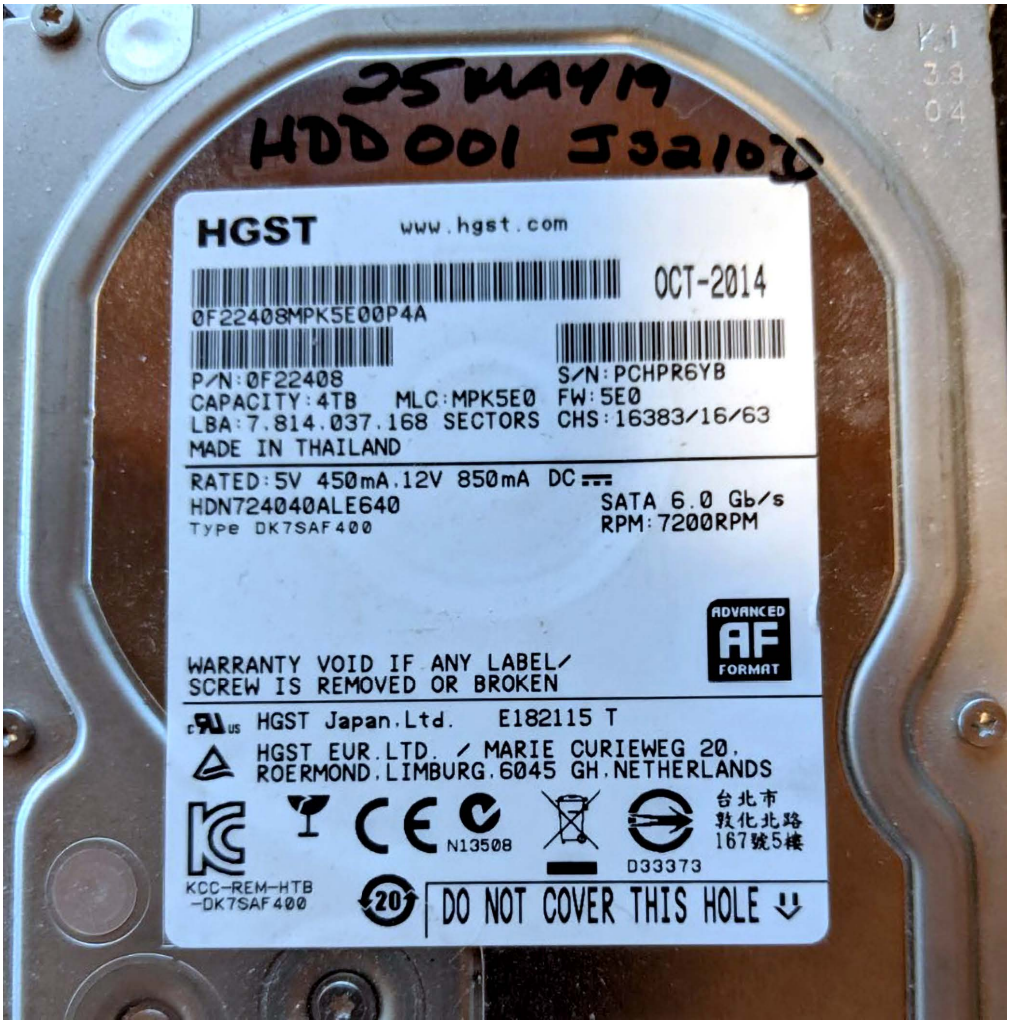


Figure 2.3: A hard drive

When the forensic image is created, the device will be referred to as **HDD001** for the rest of the process.

If you cannot write on a device without permanently reducing its value, such as an iPad, do not use a permanent marker to write **MD-XXX**. Instead, use an adhesive label to mark the information.

Note

Use a system that works for you. When you have developed your system, make sure you use it every time. It will save you from losing evidence or mismarking evidence.

When we are on the scene and seizing evidence and containers containing digital evidence, we want to make sure we do so in a forensically sound manner. Therefore, we do not analyze the original evidence; we create a copy to do the exam to ensure we do not make any changes to the original evidence.

We have three choices for making a working copy:

- **A forensic copy**: This is a straight bit-for-bit copy of the source to the destination. This is not common in today's environment. Ensure that your destination device has no old data from previous investigations. You do not want to cause cross-contamination between the current digital forensic investigation and a past investigation. We will recover deleted files, file slack, and partition slack. We will discuss wiping hard drives later on in this book.
- **A forensic image or forensic evidence file**: We create a bit-for-bit copy of the source device, but we store that data in a forensic image format. This could be a **DD** image, an **E01** image, or an **AFF** image. We take that source data and wrap it in a protective wrapper of the forensic image. We will recover deleted files, file slack, and partition slack.
- **A logical forensic image**: Sometimes, we are restricted to only accessing specific datasets. They do not allow us to access the entire container. We cannot create a bit-for-bit copy forensic image/forensic evidence file or a forensic copy. This can be used when we extract data from a server, and we cannot shut the server down to create a forensic image from the source hard drives. So, we can make logical copies of the files and folders pertinent to the investigation. We will not recover deleted files, the file slack, and partition slack.

Later on in *Chapter 3*, *Acquisition of Evidence*, we will address creating a forensic image from the devices we have seized or the data seized at the scene.

Now that we have discussed what you need to consider when acquiring a dataset, we will discuss what you need to understand when analyzing data.

Understanding the analysis process

Once you have collected data from the scene, you return to your lab, and it is now time to start your forensic analysis. You will find yourself quickly overwhelmed by the sheer amount of data you will find in storage devices. You must promptly determine whether the information contained within the storage containers is pertinent to your investigation.

This is where the information gathering in the case information and legal issues step of the process will play an essential part.

Therefore, you must capture the five Ws of the investigation (previously mentioned in *Chapter 1*, *Types of Computer-Based Investigations*). First, associate the activity on the computer system with a specific user and identify that user as a real-life person.

If the investigation already has a live suspect identified, you correlate that suspect with the user on the computer system. We will discuss some guidelines that can be used with commercial or open-source forensic tools. The goal is to understand the process without resorting to any specific forensic tool.

Now that we have discussed what you need to consider when acquiring a dataset, we will discuss what you need to understand when analyzing the data.

Dates and time zones

Dates and time zones can cause issues for the digital forensic investigator if they forget to consider them. For example, if you only conduct exams in a specific time zone and all your seized data comes from the same time zone, the issues you face are minor. But if the data comes from multiple time zones or you travel to various time zones, they can cause some confusion if you do not consider the time zone issue.

Setting the forensic machine and tools to use **universal time** (**UTC**) as a standard frame of reference helps solve this problem. Also, ensure that you adjust any timeframe where the criminal activity occurred in UTC. It does not help that operating/file systems save metadata in different time zone formats. You also must consider that the suspect may have changed the time zone settings on the computer to hide their illicit activity. Timeline analysis is critical when conducting a forensic exam.

Next, we will need to be able to identify files we know are irrelevant, as well as instantly identify contraband images. We can do that with hash analysis.

Hash analysis

What is a hash value? A hash is a digital fingerprint for a file or piece of digital media. It is generated using a one-way cryptographic algorithm.

The standard cryptographic algorithms used in digital forensics are **Message Digest 5** (**MD5**) and the **Secure Hashing Algorithm** (**SHA-1**). MD5 creates a 128-bit digital fingerprint, while SHA-1 produces a 160-bit digital fingerprint. Using a hashing algorithm allows using a variable input to create a fixed-length output.

If one bit changes in the variable input, it will cause a different output. Additional hashing information will be provided later in the book. Let's see how this works in the following exercise:

1. Create a text file containing the words `This is a test` with a filename of `Hash Test.txt`:

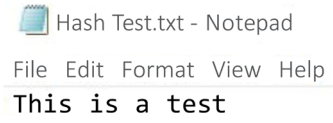


Figure 2.4: The hash text

2. Use the free Jacksum utility (`https://jacksum.loefflmann.net/en/index.html`) to obtain the hash values:

Figure 2.5: The Jacksum values

As you can see in the preceding figure, the `ce114e4501d2f4e2dcea3e17b546f339` value is the MD-5 standard length output for the `F:\Hash Test.txt` file.

The second value, `a54d88e06612d820bc3be72877c74f257b561b19`, is the SHA-1 output. It doesn't matter which forensic tool I use—these values are the digital fingerprint for this specific file.

3. Change a single part of the contents of the file:

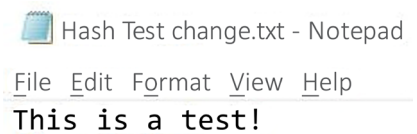


Figure 2.6: The change in the text

I have added an exclamation point to the end of the sentence—a very small change—but any change will change the hash values.

4. Use Jacksum again and you will get a totally different hash value:

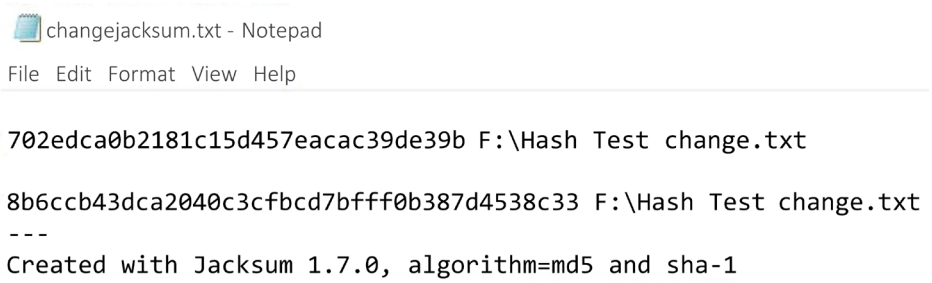


Figure 2.7: The change in the Jacksum values

The MD5 value is now `702edca0b2181c15d457eacac39de39b`, which is different from the original value of `ce114e4501d2f4e2dcea3e17b546f339`.

The standard output generated by the hashing algorithm is a one-way process. You cannot input the alphanumeric value to reverse the process to get the original dataset used in the hashing process. If you have a hash set of known illicit images, the values within that hash set cannot be used to re-create the illicit images.

There are hash sets (sets of multiple hash values) that identify known good files. These are files that are of no interest to an investigator. These can be the standard files used in an operating system or application. Using a known good hash set allows you to filter out files with no evidentiary value. On the other hand, if you have identified files of interest, such as illicit images or known documents that have been stolen, any data that may interest the investigator can also be highlighted. For the known bad files, someone needs to have access to the original file to create the hash value used to identify the file.

Using hash analysis can save you some time and effort during your investigation:

- You can use it to verify the evidence has not changed.
- It can be used to exclude files.
- It can be used to identify files of interest.

NIST has created the **National Software Reference Library** (**NSRL**) (`https://www.nist.gov/software-quality-group/national-software-reference-library-nsrl`), where they have collected software from many sources and created a **Reference Data Set** (**RDS**).

The RDS is a large hash set to help identify known good files when conducting your examination. The RDS is freely available to law enforcement, the government, and private industries. Some files identified in the RDS may be considered malicious, such as hacking tools. The investigator still has to put the files in context to see if they were being used for an unlawful purpose. The RDS does not contain hash values of illicit data, such as illegal images.

A collision occurs when two different variable inputs result in the same fixed-length output. This means that two different files have the same hash value, which you will realize is not good for identifying evidence based on our previous discussions. However, nation-states have manipulated variable inputs to create the same fixed-length output, and they have been successful.

Does that mean hashing is dead? No, it isn't. There have been no two different files found in the wild with the same hash value. All the collisions that have occurred have been files that have been manipulated. When independent examiners analyzed the manipulated files, they did not have any user-readable content. While there has been concern that this would negatively affect the admissibility of digital evidence, in 2009, the court case of US versus Schmidt ruled that the odds of a collision of two files were insignificant and were not an issue.

Now that we have determined the digital fingerprint, let's make sure the files are correctly identified.

File signature analysis

Your next step is to carry out a file signature analysis to ensure the file extension matches the file type. Many file types you will find in the filesystem have been standardized and possess unique file signatures to identify themselves to the filesystem. This is not the file extension, such as a Microsoft Word document with a file extension of `.doc` or `.docx`.

A user can change the file extension to hide incriminating evidence. The intention behind carrying out a file signature analysis is to determine whether the file signature and file extension match.

The following screenshot shows how X-Ways flags a file when the file extension does not match the file signature:

Name	10534.gif
Type	jpg
Description	existing
Existent	✓
Size	3.0 KB (3,081)
Modified	07/12/2008 21:51:38 +0
Ext.	gif
Type status	mismatch detected, OK
Type descr.	JPEG

Figure 2.8: A file signature mismatch

The file extension identifies the file as a GIF, but X-Ways has identified the file as a JPEG. The next figure shows the file header for the GIF file in question:

```
Offset    0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15      ANSI ASCIT
00000000  FF D8 FF E0 00 10 4A 46  49 46 00 01 01 00 00 01  ÿØÿà JFIF
```

Figure 2.9: A file header

A GIF file should have a hexadecimal **47 49 46 38** file signature, not hexadecimal **FF D8 FF E0**. In some cases, the mismatch is through normal usage of the filesystem and not from user interaction. You must examine the data to ensure the mismatch can be attributed to a specific user.

Gary Kessler has created a website that allows you to search a database based on the file extension or signature. You can refer to this website at `https://filesignatures.net/`:

Figure 2.10: filesignatures.net

You can search by file extension or file signature. Once you input the file extension, in this case JPG, you will be returned the file signatures associated with the JPEG standard:

Figure 2.11: The results for a JPG file signature

After we have ensured that the files have been properly identified, we need to identify any malware that may be on the system. We can do that with antivirus.

Antivirus

A common claim of innocence from a subject accused of wrongdoing that "a virus did it" has occurred in nearly every investigation I have done. Have you determined whether that is a valid claim? For example, is there malware on the system, and did it cause the behavior you are investigating without the user's interaction or knowledge?

This is one reason we collect the volatile data to see what was occurring on the system at the time of collection. If someone else has collected the evidence and all you have is a forensic image, you can still scan that forensic image to help determine whether someone has installed malware. Several forensic tools allow you to "mount" the forensic image as a read-only drive, and you can then scan the filesystem to help determine whether there is malware installed.

FTK Imager is a free tool offered by AccessData, available at `https://accessdata.com/product-download/ftk-imager-version-4.2.0`, which allows you to mount the forensic image.

Image mounting allows you to mount a forensic image as a drive or physical device. Your viewing is in read-only mode. You will find many benefits to mounting a forensic image, such as using the file explorer to view it as if it were a device attached to the computer. In addition, you can natively view different file types, use antivirus against the forensic image, share the mounted forensic image over a network, and copy files from the mounted forensic image.

We will now cover how to mount a forensic image with FTK Imager in the following exercise:

1. To mount a forensic image in FTK Imager, you need to select the **File** menu and then select **Image Mounting...** from the menu, as in the following screenshot:

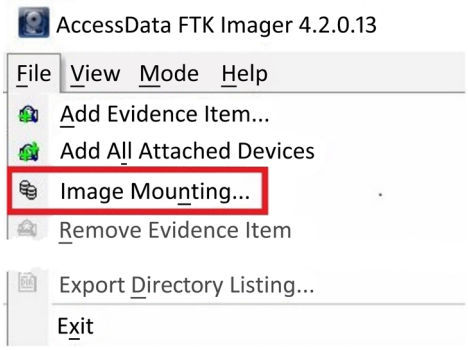


Figure 2.12: Image mounting

2. It will then present you with the **Mount Image to Drive** menu:

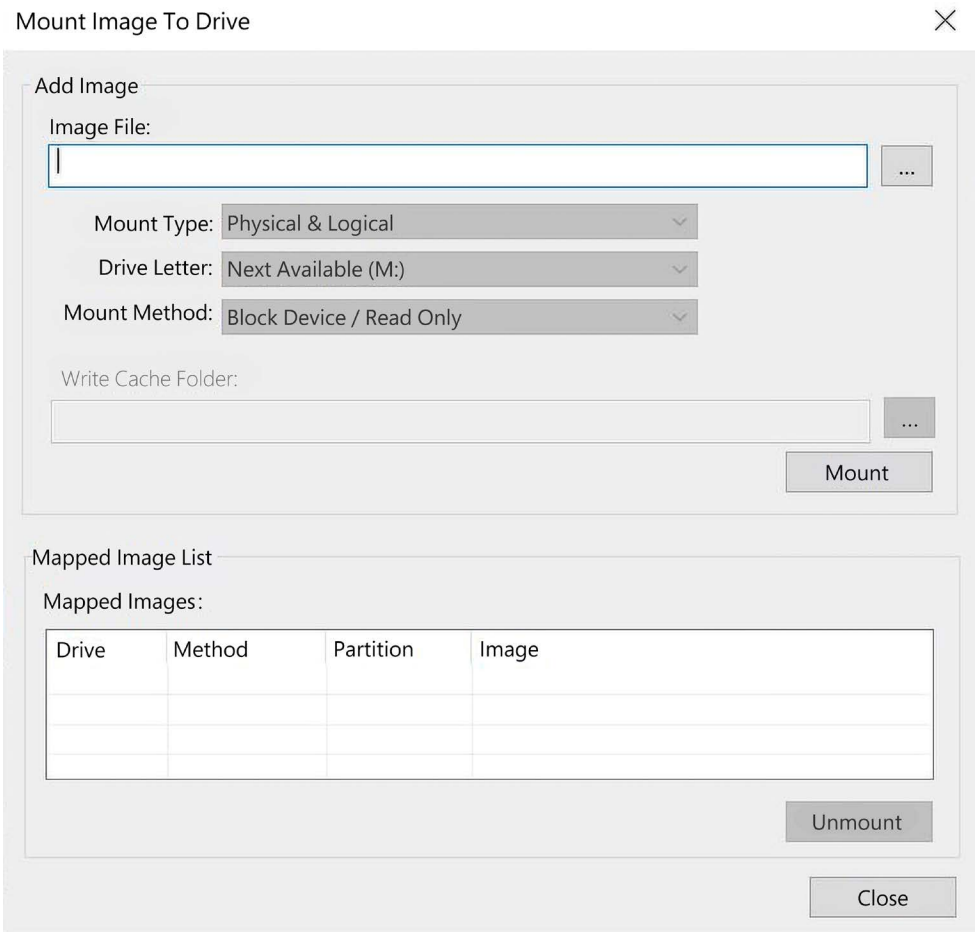


Figure 2.13: Mount the image

In the dialog box, you will have to select the forensic image you want to mount. If this is a segmented forensic, you only need to point it at the first segment:

- **Mount Type**: You have a choice of **Physical & Logical**, just **Physical**, or just **Logical**. If you select **Physical & Logical**, the software will mount the forensic image as a physical device and mount any logical partitions.
- **Drive Letter**: This is where you want to see the forensic image. In the previous figure, it shows that the next available drive letter is **M**. You can select any open drive letter you desire.

- **Mount Method**: You have the following choices:
    - **Block Device / Read Only**: This will read the device as a block device, which means a Windows application that performs physical name querying can view the mounted device.
    - **Block Device / Writable**: No changes are made to the original evidence. It will save any changes you attempt to make in a cache file.
    - **File System / Read-Only**: The device as a read-only device that someone can view using Windows Explorer.

In the following screenshot, you can see we have mounted a forensic image and the forensic image has partitions in it:

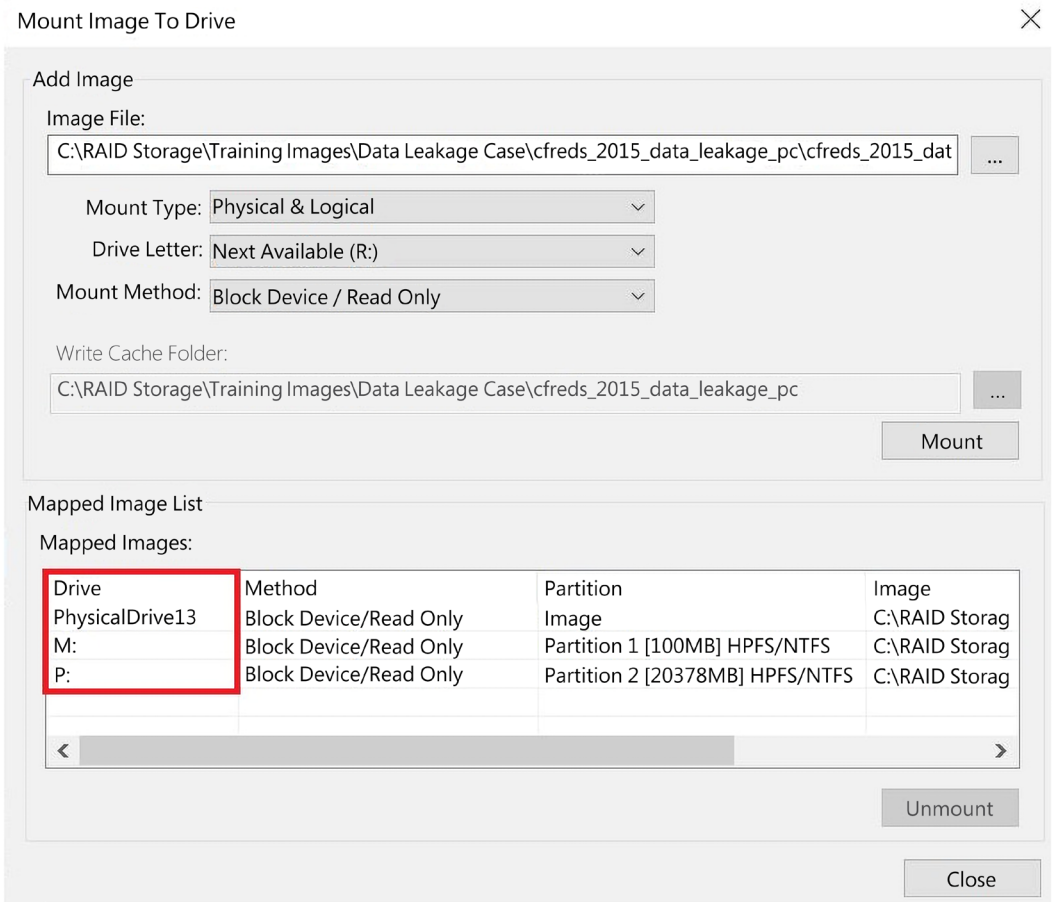


Figure 2.14: A mounted image

The system has mounted the partitions as drive **M** and drive **P**. Now, you can run the antivirus of your choice against those volumes to see whether they have installed any malware.

If malware has been installed, that is still not an alibi for the suspect. Determine whether the found malware can do the actions the suspect claims. I have investigated many illicit images investigations where the accused claims the malware downloaded the images. I have yet to find any malware that searches, finds, downloads, and sorts by content the illicit images found on a subject's computer. You still must analyze the content to determine the context of the digital evidence.

Now, you can begin your analysis of the filesystem and operating system. We will discuss the specific artifacts in the rest of this book. The OS is in place to communicate between the applications and the hardware. Some common operating systems are Microsoft Windows, Macintosh, and Linux. Almost every action conducted within an OS, whether user- or machine-generated, will leave a footprint somewhere within the OS. You want to analyze these artifacts controlled by the OS to determine whether the user committed any wrongdoing.

A filesystem is the storage mechanism for the data. A filesystem is independent of the OS. The filesystem tracks where the data is stored and what space is available. There are many filesystems, such as NTFS, HFS+, FAT 32 and Ext 4. Some formats are compatible with multiple operating systems, and some are not. For example, NTFS is utilized by Microsoft Windows as the filesystem of choice.

Once we are sure there is no malware on the system, we can then move on to report the investigation findings.

Reporting your findings

We are at the final step of the process: your report. You did all the work of preparing, purchasing the equipment, going to training, and creating your response kit, and when the call came, you responded to the scene. You successfully got the case information and navigated any potential legal issues when you arrived. You collected the volatile data, identified containers of digital evidence, and duly seized the digital evidence while maintaining the chain of custody when transporting it back to your lab. You then conducted your analysis and found artifacts that show that the suspect did or did not do what they were accused of.

Now what? You must be able to explain your findings to a non-technical person. You must take a very technical topic and talk about it in a manner that a non-technical person will understand. This is one of the most challenging aspects of being a digital forensic investigator to master.

You may have to create different report versions depending on the audience. Your intended audience will read and interpret your report, and a third party might question you on it in a judicial or administrative hearing.

Details to include in your report

You need to include enough details so that you can remember what occurred. Taking notes as you traverse the process will be your friend. There have been many times where I have failed to take that advice and had to go back and redo the process because I did not write something down. Your notes can take many forms, such as handwritten notes, typed notes, screenshots, or notes made with the built-in blogging function of your favorite forensic tool. There is no right or wrong rule on how to take notes, only that you take notes during the process.

So, what do you want to document? The following gives you an idea:

- Communication between the primary investigator and prosecutor/C-Suite executives
- The condition of the evidence containers
- The specifics of the storage device (the make, model, serial number, and condition)
- Personal identifiers of the suspect, victim, and witness (if a criminal matter)
- Personal identifiers of the witness(es), response team, responsible executive (if a civil matter)
- The forensic hardware used
- The forensic software used
- What you examined (even if the examination turned up nothing of evidentiary value)
- Your findings
- Glossary (to define technical terms)

Take all the pieces and put them together so that a non-technical reader will understand the investigations, the steps you have taken, and why you made the conclusions you did. As with everything else in digital forensics, there is not a set standard for the format of your report. Instead, you will have input from your employer, the recipients of the report, and your personal preferences.

I would recommend you include the following in your report. You should break your report into three primary sections:

- Your narrative
- Pertinent exhibits
- Supporting documentation

The narrative is what it sounds like. This is where you explain what occurred, what you did, and what it means. You should include an executive summary to hit the key points and conclusions and then move on to a detailed narrative. In your narrative, you should provide screenshots of the artifact you are talking about. Do not add a screenshot without an accompanying narrative. Do not assume the reader will understand what is pertinent about the screenshot. You will have to explain it to the reader. Make sure you focus your screenshot on the artifact you are discussing.

Suppose your report contains screenshots of contraband, such as illicit images. In that case, you will need to maintain control of that report to not cause an accidental release of the contraband images. You will also need to create a second report with the contraband images redacted for readers who cannot legally possess the contraband images.

After the executive summary, you should include basic administrative information. Next, identify the subjects involved, including the victim, suspect, witness, and other investigators.

Document facts and circumstances

You have two options regarding listing the evidence that you analyzed. In some larger cases, the listing of digital evidence can take two or more pages. Having a long, drawn-out list does not help the reader understand your report. More likely, the reader will skip the evidence listing and move on. If the investigation does not have a large number of digital devices being examined, then you can list them here, including the devices where you found nothing of evidentiary value. If you have many digital devices, I recommend you only list the devices with artifacts of evidentiary value while listing the entire evidence list at the end of the report.

You should also list details about the creation of the forensic images. I typically include a summary of the acquisition details in the narrative portion. I then create a detailed step-by-step process of the forensic image's creation as an exhibit. Once again, having a step-by-step process in the report's narrative does not help the reader understand the process. Giving the reader the high-level details of the forensic image process and then providing the details at a different location improves the readability of the report.

The analysis of the digital evidence will make up the bulk of your report. This is where you will walk the reader through the step-by-step process of the incriminating artifacts you found and why the artifact is important. I have often seen reports where a specific image is highlighted as important, but then it never explains why the image is important. Is it the location of where the image was found, or is it the image itself? Explain why that specific artifact is important and how you determined it was important.

Note

Remember, you are taking a technical subject and explaining it to a non-technical reader. Do not create a list of important files and assume the reader will know what is important.

I find that it's best to present the artifacts in chronological order. For example, if you are examining the illegal downloading of copyright-protected material, you would start by potentially identifying the owner of the computer and any artifacts that can identify a specific user. You can then show any browser searches the user performed when looking for the copyright-protected material and then the steps taken to download that material. Suppose the user had any ongoing communications with other users about the copyright-protected material. In that case, you could then use these communications to support your hypothesis about the user's activity of downloading the copyright-protected material.

You can also present the artifacts by subject. For example, if you are investigating the possession and distribution of illicit images, you can present the artifacts showing that the user viewed the images. This will show that the user knew about the images on their system and whether the user actively shared them with other users. Just the image alone is not enough; you must also find the OS artifacts to support your hypothesis about the image. When creating the analysis section, you will need to avoid making any absolute statements. I have seen forensic reports dealing with illicit images where the investigator made the unequivocal statement that the user knew about the illegal image. They found the image in question in the thumb cache database. The location of an image in a thumb cache database is not absolute proof that the user knew about the image. The system can include images in the thumb cache database without the user's knowledge. So, you want to be very careful with your language. Do not include opinions—only provide factual information.

I have seen reports describing artifacts as "a disturbing image of a child." The term "disturbing image" is not factually based—it is an opinion. It would be best to describe the artifact as it is without projecting your feelings about it. A better description could be "an image depicting a young-looking male, nude, standing in a wooded area." Be careful how you describe the artifacts attributed to a specific user or person. The most challenging item to prove is who is behind the keyboard. You can never say with 100 percent certainty that suspect **A** did the criminal activity unless you have a video showing suspect **A** was at the keyboard at that specific time. This is not the place for you to offer your opinion; do not assume ownership of an item or the identification of a user.

The report conclusion

The final portion of your narrative is your conclusion. This is the section where you can offer your opinion based on the artifacts you described in the analysis section of the report. You must still be careful about presenting your opinions. Try to look at the artifacts with no preconceived notions and determine whether the facts again meet your hypothesis. If you cannot decide, include that opinion. Remember, it is not always about proving the subject's guilt or liability. You must also provide evidence if the subject did not do what they are being accused of.

You will probably create an electronic report for distribution; a standard format is PDF. No matter what format you use, make sure you digitally sign the report. The digital signature will show that no one has altered the report since you signed it.

Note

Remember, the report is a representation of you and the investigation. If you create a poor report, that will reflect poorly on you, the investigation, and your organization.

Proofreading is essential. Do not proofread the report yourself, use the peer review process. You will miss typographical errors, poor sentence structures, and unclear findings. What may be clear to you in your mind may not always be accurately transcribed in written form. Suppose the investigation proceeds to administrative or judicial proceedings. In that case, I can guarantee the opposition will dissect your report line by line, looking for inconsistencies and places where you were not objective.

Remember, if the reader does not understand what you are saying about the artifacts you found, your entire investigation effort has been wasted.

Summary

In this chapter, we have discussed the forensic analysis process. You now know how to prepare to conduct a digital forensic examination, from getting the proper equipment to the training and getting certification. In addition, you now understand the importance of obtaining information before seizing digital evidence and ensuring you talk to other investigators or personnel involved in the situation.

I cannot stress the importance of collecting volatile data enough; if you do not, you will lose a large amount of potential evidence. Next, we discussed some strategies for conducting your examination and the differences between an OS artifact and a filesystem artifact. Lastly, we discussed reporting your findings so that the reader easily understands them.

The next chapter will go into the specifics of the acquisition of evidence and how to validate your tools to create an error-free forensic image.

Questions

1. Which of the following should be included in your response kit?
    a. A digital camera
    b. Latex gloves
    c. A write-blocking device
    d. All of the above
2. You must use commercial software to perform a valid forensic examination.
    a. True
    b. False
3. What questions need to be asked when you receive digital evidence?
    a. Why was the digital evidence seized?
    b. Where is the chain of custody?
    c. Who has accessed the evidence?
    d. All of the above.
4. RAM is the most volatile of evidence.
    a. True
    b. False
5. The chain of custody documents _____.
    a. Who controlled the evidence
    b. Who witnessed the crime
    c. The suspect's fingerprints
    d. None of the above
6. Which of the following is best for a digital forensic exam?
    a. A forensic copy
    b. A forensic image
    c. A logical forensic image
    d. Both B and C

7. Which of the following is a hashing algorithm?

    a. CDC
    b. FBI
    c. MD5
    d. LSD

The answers can be found at the end of the book in the *Assessments* section.

Further reading

Warren Kruse and Jay Heiser, Computer Forensics: Incident Response Essentials (*Addison Wesley, 2001*)

You can purchase the book from `https://www.amazon.com/Computer-Forensics-Incident-Response-Essentials/dp/0201707195`.

Join our community on Discord

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

`https://packt.link/CyberSec`

3

Acquisition of Evidence

Digital evidence is one of the most volatile pieces of evidence an investigator can handle, and the slightest error or mishandling on the investigator's part can severely affect the investigation. For example, you may lose the data forever or lose pieces of it. In addition, the unintentional manipulation of data can cast doubt on your ability to investigate or question the integrity of the data in the investigation. This chapter will address minimizing or eliminating any of these issues by using a tool validation process to create an error-free and validated forensic image.

We will cover the following topics in this chapter:

- Exploring evidence
- Understanding the forensic examination environment
- Tool validation
- Creating sterile media
- Defining forensic imaging

Exploring evidence

What is evidence? The dictionary definition is the available body of facts or information indicating whether a belief or proposition is true or valid. Now that seems to be a short, simple, common-sense answer to a simple question. In reality, the question becomes far more convoluted when you consider regulations, the law, and rules of evidence in one jurisdiction, which grows exponentially when considering multiple jurisdictions. Evidence is a determination made by the trier of fact. The trier of fact will determine if the evidence meets the standards for that proceeding and jurisdiction.

I offer the following example: Let's say you are investigating a murder and you find the victim's and suspect's blood in the suspect's vehicle; the victim's blood on the suspect's socks; and a bloodied glove at the scene, and its matching mate found in the suspect's house.

You could believe the government had an airtight case against the suspect based on this evidence. But in this case, the defense was able to successfully argue and challenge the evidence, which resulted in the suspect's acquittal. As you can see, just because something is evidence, if it cannot withstand the challenge of the opposition, then it becomes a liability.

I have worked on both sides of the judicial process regarding digital evidence, and every time, the sheer amount of digital evidence that never sees the light of day amazes me. If we do not present the evidence to the trier of fact, it does not exist as far as the proceedings are concerned. Neither side will reference it or offer it during the proceedings. It simply will not exist.

How does the opposition attack evidence that the trier of fact has admitted? Either by attacking the evidence itself and/or by attacking the process and personnel associated with collecting and analyzing the evidence.

Consider the following example:

An examiner analyzes the thumb cache of the system and sees a URI (the **URI** is a **uniform resource identifier** based on the standard created by the Internet Engineering Task Force; in this instance, it is a file path) pointing to the location of the original image. The original destination folder no longer exists on the system, nor does the source image for the thumbnail in the cache.

As shown in the following screenshot, the source image for the thumbnail in the cache was located in the **New** folder on the **Picture Drive** of the user account of **bob**. *Figure 3.1* displays the URI that was found in the thumbnail's metadata:

```
URI: file:///media/bob/Picture Drive/New
```

Figure 3.1: URI from thumbnail

In the following screenshot, you can see the URI found in the metadata of a different thumbnail in the same thumb cache. The path is very similar to the one found in the URI image. However, there are significant differences here–the user account is **bobby**, not **bob**, and the **New** folder does not exist:

```
URI: file:///media/bobby/Picture Drive/
```

Figure 3.2: URI image: bobby

On the system that was being analyzed, there was not a **bob** user account, nor were there any artifacts showing the **bob** account was ever created or deleted from that system. The digital forensic examiner amended their report and incorrectly stated that the **Picture Drive** was the same in both instances based on the similarities of the URIs. Initially, the digital forensic examiner noted that the metadata's URIs represent file paths that cannot be verified.

The digital forensic examiner conducted a second exam and found a deleted folder called **New** on the **Picture Drive** and amended the report to reflect that. The URIs found within the metadata represent evidence item HDD 001. The **New** folder was deleted on this date and time. (I am not using exact names or dates for obvious reasons.)

Based on the file path and the current users, there was no way to determine if the **New** folder referenced in the URI was the same as the deleted **New** folder. When the lawyer confronted the digital forensic examiner about these discrepancies, they admitted they had made an error. I believe they made the error because of the similarities of the file paths and not paying attention to the specific details. I absolutely believe the error was not malicious or intentional but an honest mistake by the opposition's digital forensic examiner. As you can see, sometimes, a simple mistake can lead to additional questions being asked about the collection of the evidence and the process used to generate the report and the evidence.

In a different case that I was brought in on, the subject was charged with attempting to lure a child. In this specific set of circumstances, the subject communicated with an **undercover agent (UC)** and sent many illicit images to the UC. When law enforcement took the subject into custody, the subject was interrogated, confessed, and wrote an apology letter.

The confession, over 400 pages of chats, and a dozen illicit images were submitted as evidence in the judicial proceedings. Once again, you would expect that there would be a conviction based upon this evidence.

During the trial, it was revealed the government had deleted some text messages and edited the video file of the recording of the confession. The judicial authority informed the jury of the manipulated evidence. Additionally, the jury was told the only conclusion they could consider was that the government's agents altered the digital evidence to hide facts that would hinder the government's prosecution. The jury then found the subject not guilty of all charges.

If you do not follow your organization's best practices, policies, and procedures, the evidence will not see the inside of the courtroom. If the flawed evidence is admitted, the opposition's attacks will mitigate its effectiveness. These attacks can create enough reasonable doubt to generate an acquittal.

So, what can we do to mitigate the attack of the opposition? First, it does not matter which side of the matter you are on; the opposing counsel will attack your findings if it is harmful to their case.

Do not forgo proper evidence-handling procedures. Proper evidence handling does not end with collecting evidence in the field. As the evidence is transported from the field to the secure location, and whenever someone checks over the evidence, you must maintain the evidence's chain of custody and security.

Do not forgo utilizing proper procedures, methodologies, or processes when conducting your digital forensic investigation. Do not take shortcuts.

Validate any procedure, methodology, or processes. You must go through the validation process; you cannot rely on third-party validation. Your validation must repeatedly reproduce the same results when performed by you or anyone else.

Prepare and conduct your digital forensic examination with the mindset that someone will go through every step you take and question every finding you make. With this mindset, you should be able to mitigate any attack against your digital forensic examination. The key is that you must prepare. If you are unprepared for the attack, then you may be made to look incompetent while testifying in judicial/administrative proceedings.

We have discussed the evidence, but what about the environment in which you will conduct the investigation? We will now discuss how you should control the examination environment.

Understanding the forensic examination environment

A term that has been pounded into my head since I first went to training with IACIS is the *forensically sound examination environment*. While it sounds complicated, it is a relatively simple concept:

- The digital forensic examiner controls the working environment of the digital forensic examination
- No actions will occur unless the digital forensic examiner intends the action to occur
- When the action has been completed, the examiner will reasonably know what the expected outcome is

This concept does not merely apply to a physical location, but anywhere we complete a digital forensic examination or perform actions to support the digital forensic investigation. This could be a lab, office, or in the field where the digital evidence has been collected.

The forensically sound examination environment is a mindset of the digital forensic examiner. You want to be methodical and thorough to support the digital forensic examination. This mindset will help eliminate some mistakes that may occur during the process.

For example, the organization sent two colleagues to a remote location to acquire several workstations. They were able to complete data acquisition within 2 to 3 days. The investigators did not perform triage on the dataset or examine the dataset while on the scene, but it was expected to be completed when they returned to the central lab. The remote location was several hundred miles away, and once my colleagues left, they could not return to gain access to the source devices. Upon arrival at the central lab, my colleagues started to conduct their digital forensic examination. Colleague A started to examine one of the forensic images, and as a part of their process, they viewed the folder structure of the filesystem. As they were looking at the installed programs, they were shocked to find a commercial forensic tool installed on the suspects' system. As they drilled down further into the filesystem, they started to find documents with their names on them. Again, they were shocked; how did the suspect gain access to Colleague A's information?

The suspect didn't have access to the information.

Colleague A made an error when creating a forensic image. Instead of imaging the suspects' device, they imaged the system drive of their forensic laptop. They ignored the details as they were creating a forensic image. Luckily, the procedure was for each colleague to make a forensic image of the source device, for a total of two forensic images.

While this story is embarrassing, there were no lasting repercussions because we could use the second copy. Imagine how you would feel if you were Colleague A, and there was no second backup to use. How do you explain to your supervisor or the client that you could not complete the task as given, and now you do not have access to the source device?

To help stop that from occurring, we will look at tool validation.

Tool validation

Earlier, we discussed potential attacks on you, your exam, and your findings. The opposing counsel will focus on how you did the exam and what tools you used to perform the exam. Your ability to mitigate the opposing counsel attacks is directly related to your preparation and the documentation you created during the exam. Being aware and following best practices is critical in your ability to defend your actions successfully. How do you do this? By continuing your education. The field is constantly changing, and you must keep aware of those changes.