

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

Copyright © 2022 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Senior Publishing Product Manager: Aaron Tanna

Acquisition Editor – Peer Reviews: Saby Dsilva

Project Editor: Amisha Vathare

Content Development Editor: Liam Thomas 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: <...>

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, Middle East, 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 (catchapredator.org) to combat the Sexual Exploitation of Children in a way that has never been done in all of history.

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 RAM? How many SSD drives? Which processor? Which operating system? 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 will 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 servers log from AD001
HD-001	1	Samsung SSD 1TB Ser#ABC9876
HD-002	1	Samsung SSD 512 MB Ser# DEF4567
CP-001	1	Pixel XL 128 MB Ser# A5 12 D3 AC FD
TD-001	1	Generic Thumb drive 32MB (green) unknown SN
MD-001	1	Apple iPad 512mb 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:

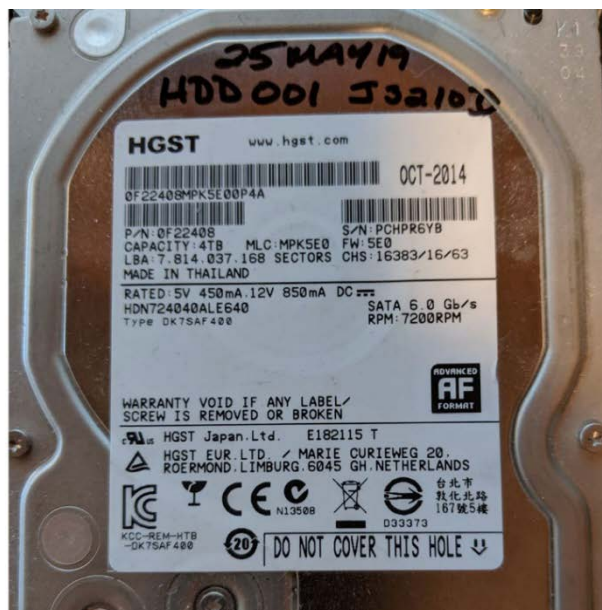


Figure 2.3: A hard drive

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`:

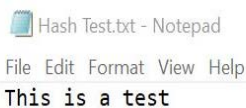
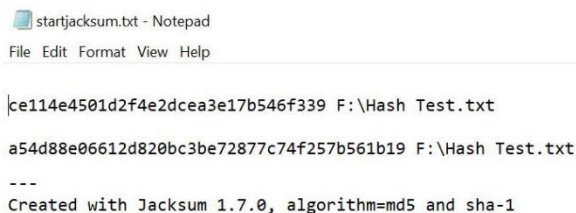


Figure 2.4: The hash text

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



```
startjacksum.txt - Notepad
File Edit Format View Help

ce114e4501d2f4e2dcea3e17b546f339 F:\Hash Test.txt
a54d88e06612d820bc3be72877c74f257b561b19 F:\Hash Test.txt
---
Created with Jacksum 1.7.0, algorithm=md5 and sha-1
```

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:



```
Hash Test change.txt - Notepad
File Edit Format View Help
This is a test!
```

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:



```
changejacksum.txt - Notepad
File Edit Format View Help

702edca0b2181c15d457eacac39de39b F:\Hash Test change.txt
8b6ccb43dca2040c3cfbcd7bfff0b387d4538c33 F:\Hash Test change.txt
---
Created with Jacksum 1.7.0, algorithm=md5 and sha-1
```

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 ASCII
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:

3 Results Found For JPG File Extension		
Extension	Signature	Description
☆ JPG	FF D8 FF E0 ASCII	JPEG IMAGE Size: 4 Bytes Offset: 0 Bytes
☆ JPG	FF D8 FF E1 ASCII	Digital camera JPG using Exchangeable Image File Format (EXIF) Size: 4 Bytes Offset: 0 Bytes
☆ JPG	FF D8 FF E8 ASCII	Still Picture Interchange File Format (SPIFF) Size: 4 Bytes Offset: 0 Bytes

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:

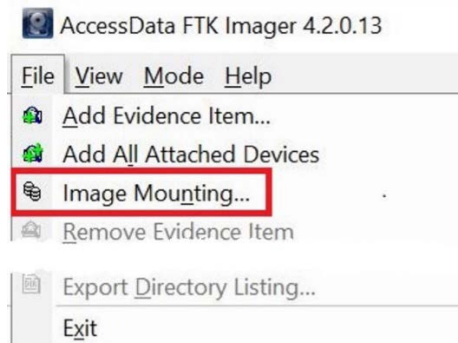


Figure 2.12: Image mounting

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

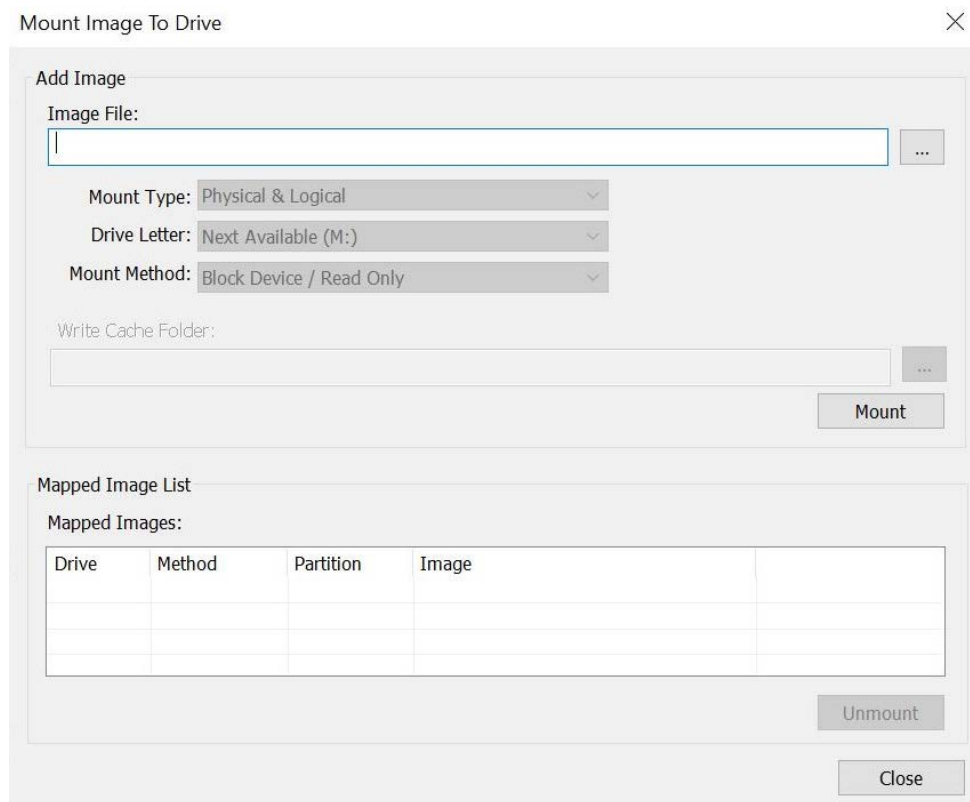


Figure 2.13: Mount the image

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:

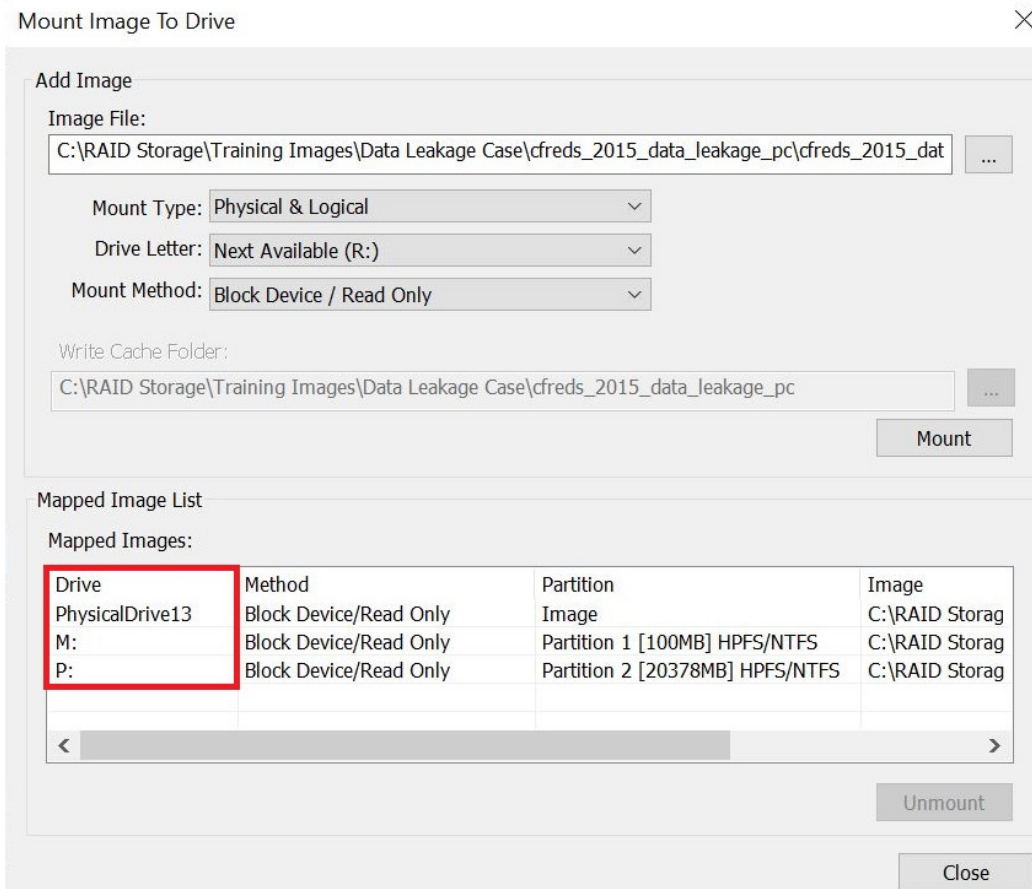


Figure 2.14: A mounted image

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. To clarify, the **operating system (OS)** is the system 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. 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>.