



Introduction to Digital Forensics

Curriculum and Lesson Plans for Training

Kristie Arciszewski, KAIT Consulting

August 2023

Copyright © 2023 by KAIT Consulting, Greenfield, Wisconsin

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under sections 107 or 108 of the 1976 United States Copyright Act and with prior written permission of the publisher.

Limit of liability/Disclaimer of warranty: the author and publisher makes no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the author is not engaged in rendering other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising here from. The fact that an organization or website is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

Table of Contents

Chapter 1 — How to Handle Digital Evidence.....	1
Chapter 2 — Image and Tool Verification	10
Chapter 3 — Evidence Acquisition Process	20
Chapter 4 — Using FTK Imager	29
Chapter 5 — Proper Forensics Methodology and Standards	32
Chapter 6 — File Systems: Electronic Evidence Issues	41
Chapter 7 — Windows Registry Analysis.....	54
Chapter 8 — Windows File System Analysis	64
Chapter 9 — Forensic Tools	72
Chapter 10 — Incident Response	76
Chapter 11 — Introduction to Password Cracking	83
Chapter 12 — Introduction to Steganography.....	88
Chapter 13 — Introduction to Cryptocurrency	99
Chapter 14 — Introduction to Memory Forensics	106

Chapter 1 —

How to Handle Digital Evidence

Learning Objectives

- Understand what is considered digital evidence.
- Know the procedures for handling digital evidence.
- Understand why it's important to handle digital evidence properly.

Important Terms

digital evidence
digital forensic analyst
auditability
justifiability
reliability
chain of custody

INTRODUCTION

- Do you know what to do if you find yourself involved in a crime scene that has electronic devices in the immediate area?
- Are you a supervisor of people who process crime scenes?
- Do you work for an organization that requires digital evidence collection?

If you answered “yes” to any of these questions, then it is critical for you to understand the process and procedures to properly handle evidence. Without knowing what a bit, a byte, or a gig is, the average person is more than qualified to be aware of how to handle computer devices that may be part a potential incident or crime. That can be understood by knowing one important thing:

**Never turn off or power down any electronic device that
may be part of an incident or possible crime scene.**

Three prominent crimes in the recent past were solved as a result of digital evidence that was obtained according to digital evidence collection protocol. Consider these examples:

- **BTK Killer:** In 2005, the BTK killer inquired if police would be able to trace a floppy disk back to him. The police published an ad in the local newspaper assuring him that it would be untraceable. BTK believed them and sent a disk to the local Fox TV affiliate. On the disk, digital forensics professionals found metadata from a document that had been deleted. The metadata revealed the words “Christ Lutheran Church

- " and that the last edits were made by someone named Dennis. Further research by detectives found that there was a person named Dennis Rader that was the church's council president. Police surveillance verified that a vehicle believed to have been related to one of BTK's crimes matched a vehicle in the Christ Lutheran Church parking lot.
- Craigslist Killer: In 2009, medical student, Philip Markoff was discovered to be the Craigslist Killer. One of the victims was murdered and another reported an assault and robbery at gunpoint. The police found that both women were connected in that they both advertised personal services on Craigslist and both had an appointment with a man named "Andy". Investigators reviewed the email communications between the victims and Andy and discovered the IP addresses used. They traced back the IP addresses to Philip Markoff.
- Larry J. Thomas v. State of Indiana: In 2016 Larry J. Thomas was found guilty of murdering Rito Llamas-Juarez. Eyewitnesses confirmed that Thomas was in vicinity of the crime scene but digital forensics evidence provided an extra layer of confidence to their testimony. Cell phone records corroborated witnesses' claims that he was located at the crime scene. Investigators were also able to identify an application that was used to set up a meeting with the deceased victim.

But none of that evidence would have been admissible in court if proper procedures and protocols weren't followed.

DIGITAL EVIDENCE

Digital evidence is data that is transmitted to or from or stored on any electronic device. This includes, but is not limited to, devices such as computers, laptops, servers, USB or flash drives, mobile phones, digital cameras, and tablets.

According to the National Institute of Standards and Technology (NIST), there are four types of digital evidence: physical media, digital images/files, other digital objects, and law enforcement (LE)-generated evidence (Guttman et al., 2022, p. 1).

- Physical media are computer hard drives, mobile devices, USB drives, CDs, and DVDs.
- Digital images/files originate from physical media or systems.
- Other digital objects include online accounts.
- Law enforcement generated evidence are items such as body cameras, patrol car cameras, or electronic records.

Any actions taken with the devices that capture digital evidence, can change the state of the data on that device. For example, the mere act of moving a computer's mouse or inserting a USB drive creates records about these actions; the device is no longer in its original state. Therefore, it's imperative to ensure that, in situations where digital evidence is potentially part of a crime or incident, evidence is collected using proper techniques and accepted procedures that do not change the state of the device. A **digital forensic analyst** is a person who is trained in digital evidence collection and is the best option in these cases.

DIGITAL EVIDENCE HANDLING BEST PRACTICES

Having a qualified digital evidence collection professional is critical to ensuring that the integrity of digital evidence is maintained. This includes using proper techniques in capturing an image of the data and maintaining a chain of evidence.

To that end, the following best practices (Mountrakis & Ioannou, 2019) should be followed with regard to digital evidence handling:

- **Auditability** – Digital forensics professionals must document all actions taken such that an independent third party would be able to evaluate them.
- **Justifiability** – Digital forensics professionals must choose and justify all methods used and actions taken while handling digital evidence.
- **Repeatability** – An independent third party or different testing environment should be able to repeat or reproduce the actions performed by the digital forensics professional and get the same results.

ADMISSIBILITY OF EVIDENCE

According to the American Bar Association, the Federal Rules of Evidence are generally applied to digital evidence, just as they are for physical evidence (Battista Sozio, 2017). The key is that relevancy and authenticity must be established. It is common for email, texts, and social media posts to be used in court cases. Establishing their authenticity is where following digital forensics best practices becomes critical. If digital evidence cannot be shown to be authentic, it cannot be used in a court of law.

ESTABLISHING AUTHENTICITY

Fortunately, there are a variety of computer forensics tools that are used to maintain the integrity of the data. The following examples are just a sampling of the software and hardware tools are available.

COMMON DIGITAL FORENSICS SOFTWARE

- Disk and data capture tools
 - Magnet Forensics
 - X-Ways Forensics
 - AccessData FTK
 - EnCase
 - Mandiant RedLine
 - Paraben E3 Suite (processes data from smartphones, cloud, computers, email, and IoT devices)
 - Bulk Extractor
 - Volatility (used for memory forensics)
 - WindowsSCOPE (used for memory forensics)
- File viewers
- File analysis tools
 - Autopsy/The Sleuth Kit
- Registry analysis tools
 - Registry Recon
- Internet analysis tools
- Email analysis tools
- Mobile device analysis
 - Oxygen Forensic Detective
 - Cellebrite UFED
 - XRY
- Network forensics tools
 - Wireshark
 - Network Miner
 - Xplico
- Database forensics tools

COMMON DIGITAL FORENSICS HARDWARE



[Photo courtesy of TriTech Forensics](#)

Digital Forensics Workstation

Used for processing digital forensics data.



[Photo courtesy of TriTech Forensics](#)

Full Field Digital Forensics Laptop Workstation

Used for processing and storing digital forensics data in the field.



[Photo courtesy of TriTech Forensics](#)

Faraday Bags

- Used to block electromagnetic waves from reaching anything inside it
- Great for protecting SSD cards, RAM sticks, hard drives, mobile phones, and memory cards
- Can be purchased as disposable bags or as zippered pouches.



[Photo courtesy of TriTech Forensics](#)

Digital Forensics Storage Tower

- Used for storing digital evidence
- Expandable



[Photo courtesy of TriTech Forensics](#)

Portable Digital Forensics Kit

Includes forensic imaging drive and write-blocking device into one portable case.

- Allows digital investigator to create write-blocked disk clones, manage images, and log and maintain chain of custody.
- Kits can include the following equipment:
 - Write-blocking and duplicating imaging unit
 - Unitized SAS to eSATA + mini-fit power cable
 - IDE cable
 - 12V power supply
 - Power cord
 - Legacy power to mini-fit cable
 - Ethernet cable (RJ45)
 - 2.5 IDE to 3.5 IDE and mini-fit cable
 - Power adapter, legacy to SATA
 - Velcro cable wrap
 - eSATA cable
 - SD card
 - HD tool to assist in drive connection
 - Digital camera for pics and video record w/ 16 gig card
 - Pelican case

- eSATA portable 1 TB hard drive for evidence collection
- eSATA portable 2 TB hard drive for evidence collection



[Photo courtesy of CDW](#)

USB WriteBlocker USB Drive

- A tool designed to prevent write access to the hard disk, thus permitting read-only access to the data storage devices.
- Protects the integrity of the data.
- Protects the chain of custody.

CHAIN OF CUSTODY

Different activities are involved with maintaining **chain of custody**. It starts with the documentation of the original physical evidence. Photos are taken of the physical device. The source of the evidence is noted, as well as how it was created and who it was created by on a chain of custody document (Figure 1-1).



Chain of Custody Document			Sequence Number:	
Receiving Organization:			Location:	
Name of Person From Whom Received:			Address:	
Location from Where Obtained:			Reason:	Date/Time Obtained:
Item Number	Quantity	Description		
Item Number	Date	Released By:	Received By:	Reason for Change:
		Signature	Signature	
		Name & Title	Name & Title	
		Signature	Signature	
		Name & Title	Name & Title	
		Signature	Signature	
		Name & Title	Name & Title	
		Signature	Signature	
		Name & Title	Name & Title	

The American Society of
Digital Forensics & eDiscovery
Nonprofit 501(c)(3) corporation. For additional information, visit www.aspfd.com/links.

Download additional copies at
www.aspfd.com

Figure 1-1. Sample chain of custody form.

The next stage of the process is to generate a hash value from the data on the original device. Hashing is a process that converts the data of a file into a fixed-length string of letters and numbers. There are different lengths of hashes produced by different hash functions. The MD5 hashing function creates a representation of the data that is 32 characters long. The SHA-1 hash function produces a data representation of 40 characters. SHA-256 creates a data representation of 64 characters. SHA-512 creates a data string of 128 characters.

You will never conduct any forensic analysis on original device data. Instead, a write-protected, bit-by-bit copy of the device data is made using a write blocker and imaging software. A hashing function is applied to the copied image. To be deemed authentic, the hash value of the original data and the copy must be exactly the same. A single change to any of the data being hashed will

produce a different string of characters. Therefore, if they don't match, it is a sign that the file has been tampered with or has otherwise changed from the original.

When not in use, any data evidence collected must be locked and stored in a faraday storage box or cage to protect it from electromagnetic interference that can damage it.

WHERE TO FIND DIGITAL FORENSIC TOOLS

- X-Ways: <https://x-ways.net/forensics/>
- Magnet Forensics: <https://www.magnetforensics.com/resource-center>
- EnCase: <https://www.opentext.com/products/encase-forensic>
- FTK: <https://www.esecforte.com/products/forensic-toolkit-ftk/>
- Mandiant: <https://www.mandiant.com/resources/blog/mandiant-dfir-framework-ot>
- Paraben Suite: <https://paraben.com/>
- Bulk Extractor: https://downloads.digitalcorpora.org/downloads/bulk_extractor/
- Volatility: <https://www.volatilityfoundation.org/releases-vol3>
- WindowsSCOPE: <https://www.windowsscope.com/>
- Autopsy: <https://www.autopsy.com/>
- Registry Recon: <https://arsenalrecon.com/products>
- Oxygen Forensic Detective: <https://teeltech.com/mobile-device-forensic-tools/oxygen-forensic-detective/>
- Cellebrite UFED: <https://enterprise.cellebrite.com/cellebrite-ufed/>
- XRY: <https://www.msab.com/product/xry-extract/>
- Wireshark: <https://www.wireshark.org/download.html>
- Network Miner: <https://www.netresec.com/?page=Networkminer>
- Xplico: <https://www.xplico.org/>

Chapter 2 —

Image and Tool Verification

- Learning Objectives:**
- Understand the important properties of hash functions
 - Know the different families of hash functions
 - Learn how the commonly used SHA-1 hash works

- Important Terms:**
- hashing function
 - pre-image resistance
 - collision resistance
 - second preimage resistance

INTRODUCTION

Image and tool verification are extremely important in digital forensics. The necessity to prove the integrity of an image is just as important as the tools that are used to confirm it. It is our responsibility as digital forensic analysts to ensure we are verifying an image is a true bit-by-bit copy of the original drive. It is also our responsibility to make sure that the tool we are using to prove the integrity of the digital copy is done with a tool that is proven to be reliable and accurate.

In this unit we will explore the reasons for verifying digital forensic images and tools used to acquire and analyze the data reaped from all sorts of digital media. A significant part of verifying the integrity of a digital copy has to do with the use of hashing functions.

Some of the most important reasons for verifying digital forensic images:

- Ensure the data collected from a device is a true digital representation of the original. This is especially critical in a court of law where the data may be important to prove or disprove an illegal act. Rules of Evidence determined by the U.S. legal system are used to determine whether evidence can or cannot be admitted.
- Verify if there are corrupted or bad sectors on the device that did not transfer to the digital copy.
- Verify whether data may have gotten corrupted in the input or output of the acquisition process.
- Verify if cached data did not get copied over during the acquisition process.

- In a situation where digital evidence needs to be acquired at the scene of the incident, verifying ensures that the copy matches the original before leaving the scene. A digital analyst does not want to get back to the lab, only to realize that something has gone wrong with the copying process. Going back to the site to reacquire the image is almost pointless as the state of the device is likely to have changed by that time. A lot could have happened during that time. The opportunity to find quality evidence may be lost.
- Revalidate image files to ensure they are still viable if they have not been accessed for an extended period of time. Degradation or corruption can happen naturally the longer digital evidence sits without being used.
- In a court case, verifying the image helps refute claims by the defense that the data has bad sectors or isn't a true original. Both of those conditions would cause digital evidence to be invalid and not usable in a court of law.

Common tools used in the image discovery process primarily include write blockers and image acquisition software. If these tools are found to be faulty or unreliable, the integrity of the image cannot be trusted.

IMAGE VERIFICATION

In the image verification process, a value that is called a hash, is obtained from the original device data prior to obtaining the copy. In simple terms, a **hash** is a mathematical function that creates a unique fixed-length value string.

There are five major properties hashes must have to be considered secure: one-wayness, collision resistance, preimage resistance, second preimage resistance, and fixed lengths.

- An important property of a hash is that it is one-way, meaning that it is a mathematical function that generates an output value that cannot be reverted to its original input.
- **Pre-image resistance** means that if given a hash value, it is computationally infeasible to find out what its input originally was.
- **Collision resistance** means that two different message inputs cannot have the same hash output. In other words, the same input always produces the same hash value. Consequently, any modification to the original input will output a different hash.
- **Second preimage resistance** means that given a second hash value, it is "...computationally infeasible to find a second input that has the same hash value as any other specified input" (Computer Security Resource Center, 2023).
- Hash functions can be applied to any size file and will always generate a value output ranging between 128 and 512 bits depending on the type of hash function used (refer to Table 2-1 below).

The most common hash functions are called dedicated hashes. The family of Secure Hash Algorithms (SHA) are dedicated hashes. SHA-1 and its later versions were developed by the U.S. National Security Agency (NSA) and “...published as standards by the US National Institute of Science and Technology (NIST). It is the required algorithm for secure applications used by US government agencies” (Forensic Focus, 2017).

Table 2-1. Dedicated hash functions.

Hash Name	Secure	Input Block Length (in bits)	Output Bit Length (in bits)	Number of Rounds
MD5	No	512	128	N/A
SHA-1	No	512	160	80
SHA-256	Yes	512	256	64
SHA-512	Yes	1,024	512	80

Figure 2.2 below is a visual representation of how dedicated hashing functions generally work. The data to be hashed is segmented into blocks of equal sizes (refer to Table 2-1, Input Block Length). Extra bits are added at the end to pad the final block, if needed, to ensure it is the same size as all the other blocks.

The blocks are then processed sequentially by the hash function. To start the hashing process, an initial random value is used with the first block of data and is run through the function. The result of the first block that goes through the function is used as the value to hash with the second block. The result of the second block that goes through the function is used as the value to hash with the third block. This continues until all blocks have been input into the function. The last iteration (the last block which may be padded) becomes the final hash value.

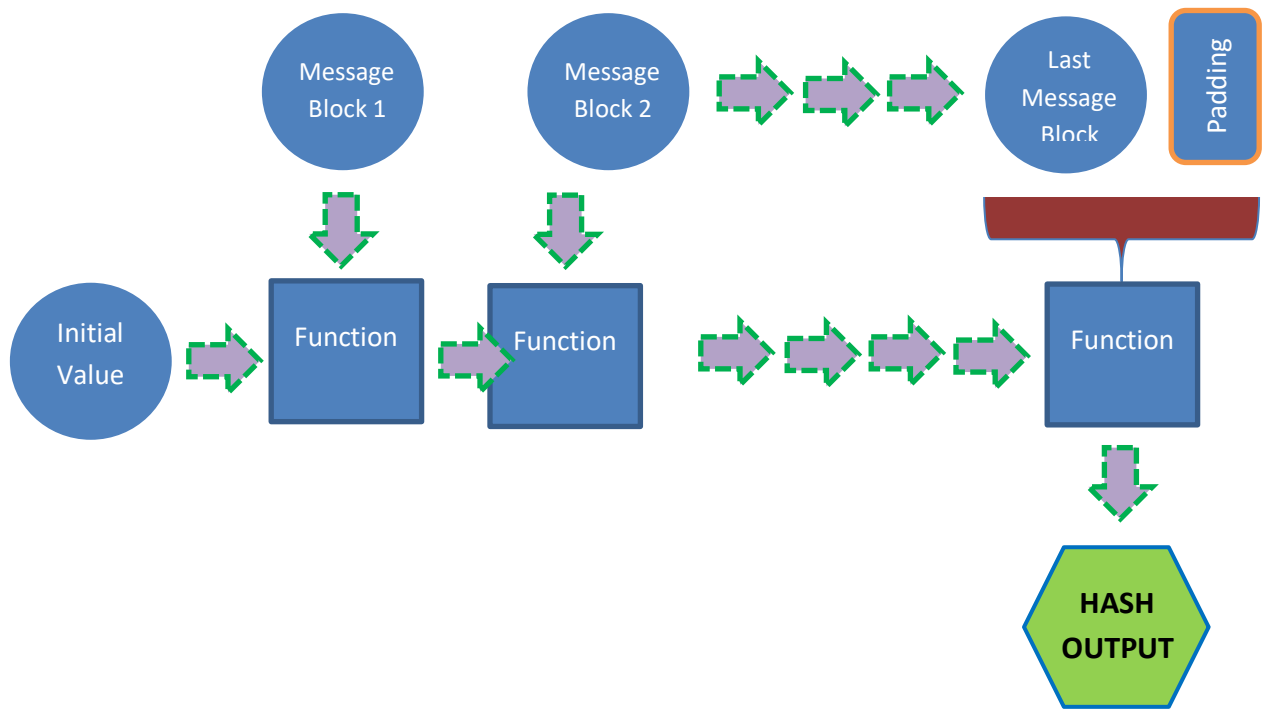


Figure 2-2. General dedicated hash function process

In conclusion, verification of an image happens when the hash value of the copy matches the hash that was derived from the original.

HASHING IN ACTION

The following is an example showing the hash value for the following phrase:

Luke, I am your father.

- **MD5:** fafc4ff240e0539cd6325989c881427d
- **SHA-256:** 5d8082c2eabfe36a513a644700155bc479ceee8533459e71678b689beabdd7d6

The following are the hash outputs for the same phrase but with an exclamation point at the end of the sentence (instead of a period) and an additional sentence has been added:

Luke, I am your father! You know this to be true.

- **MD5:** 519f262ae8ece8e6058d61fa1507b381
- **SHA-256:** 25161c33f745ab27551c2022f698a1526b4d0d070503d93f4169c86c7fc6fd30

Even though the original two messages have a different number of characters, the hash functions yield values that are the same length. That is, MD5 hashes will always yield a value that is 32 characters long and SHA-256 hashes will always yield a value that is 64 characters long no matter how many characters are hashed.

LEARNING ACTIVITY 2-1

1. Navigate to <https://hashingservice.com/>. It is an online hash generator.
Note: This online tool is used only for the purpose of this exercise. In a real scenario, you would use an installed application. Using an online generator exposes the submitted data to be being collected or recorded by the online tool.
2. Choose a hash function from the drop-down menu.
3. Enter each of the following phrases into the hash generator. Try different hash functions for the same phrase. How do they differ?
 - The quick brown fox jumps over the lazy dog.
 - Using the Force really tires Baby Yoda out.
 - Harley Quinn is the Clown Princess of Crime.
 - What do you call a fake noodle? An impasta!
 - “Nothing is impossible, the word itself says I’m possible.” – Audrey Hepburn

[Type the company name]

4. Enter one of the above phrases but substitute one of the characters with a different one.
Does the hash value match the original phrase?
5. Try using some of your own words and phrases.

THE IMAGE VERIFICATION PROCESS

There are many applications that provide utilities for obtaining the hash value of an entire file.
Some of the most popular are:

- [FTK Imager](#)
- [The Sleuth Kit and Autopsy](#)
- [OpenText EnCase](#)
- [Magnet Axiom](#)
- [CAINE](#)

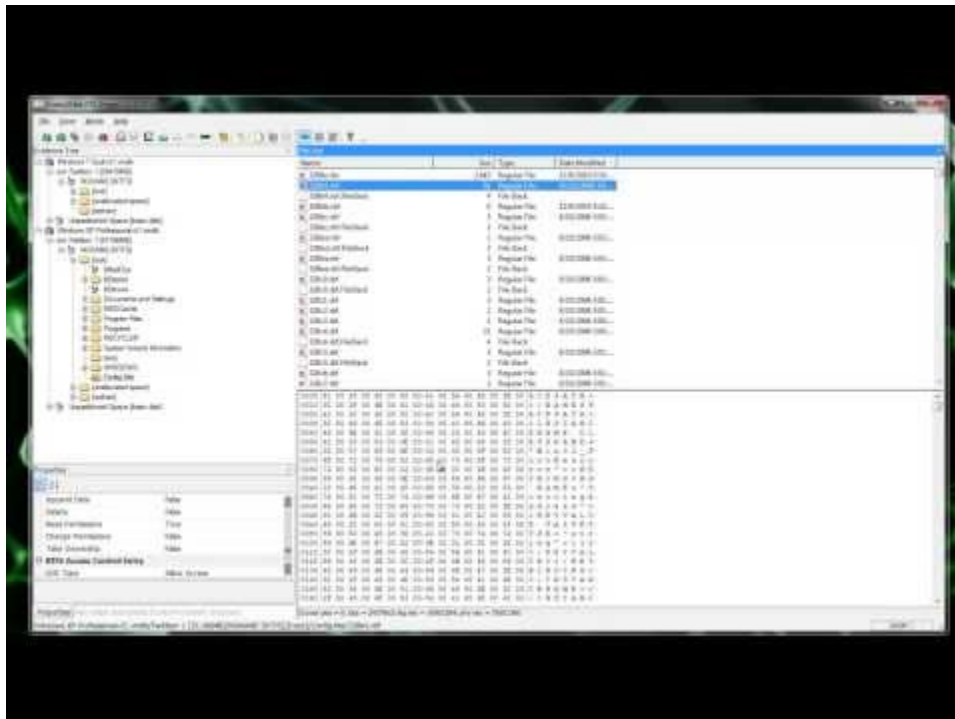
LEARNING ACTIVITY 2-2

1. [Download FTK Imager](#) and follow prompts for installation.
2. Learn how to open an image file for analysis.

[FTK Image Loading and Analysis](#)

Posted by H3xx Edit

Duration: 15 min. 51 sec.



3. Work on the M57-Jean Scenario as described below:

Adapted from Digital Corpora, <https://digitalcorpora.org/corpora/scenarios/m57-jean/>.

Introduction

The M57-Jean scenario is a single disk image scenario involving the exfiltration of corporate documents from the laptop of a senior executive. The scenario involves a small start-up company, M57.Biz. A few weeks into inception a confidential spreadsheet that contains the names and salaries of the company's key employees was found posted to the "comments" section of one of the firm's competitors. The spreadsheet only existed on one of M57's officers, Jean.

Jean says that she has no idea how the data left her laptop and that she must have been hacked.

You have been given a disk image of Jean's laptop. Your job is to figure out how the data was stolen, or if Jean isn't as innocent as she claims.

Materials:

- Jean's disk in EnCase E01 format:

- nps-2008-jean.E01
- nps-2008-jean.E02

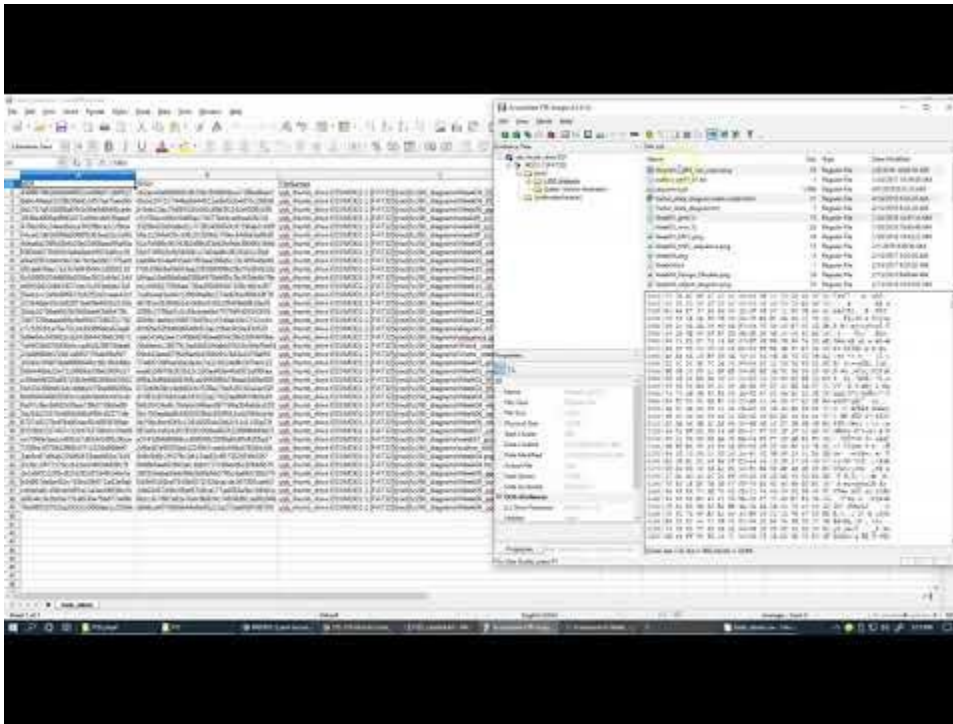
(Note: nps-2008-jean is a multi-volume Expert Witness file. You need to download both of the files and put them in the same directory, or else you will not be able to process the disk image.)

- Exercise Slides:

- M57-Jean.ppt (Microsoft PowerPoint format)
- M57-Jean.key (Apple keynote format)
- M57-Jean.pdf (Adobe Acrobat format)

- Make a new folder on your Desktop and make sure that you place the nps-2008-jean.E01 and nps-2008-jean.E02 files inside.
- Load image as instructed in video *FTK Image Loading and Analysis*.

4. Watch video, [2.9 Lab F17, FTK Imager, hash calculation and verification](#).
Posted by cjumpdotcom
Duration: 8 min. 11 sec.



5. Using the techniques shown in the [2.9 Lab F17, FTK Imager, hash calculation and verification](#), please respond to the following questions using the *nps-2008-jean.E01* image that you've previously loaded:
 - How would you calculate and save hash values of the files present in this evidence item?
 - What are the MD5 and SHA hashes for this image?
 - Choose a folder within the image and export the hashes for all files contained within the folder.
 - Are integrity checks logged by the FTK Imager?

UNDERSTANDING DIGITAL FORENSICS TOOL VERIFICATION

The acquisition of an image, including its hash generation, cannot be trusted if the tools that are used in digital forensics analysis are not effective. Therefore, it is important that tools be verified on a regular basis. That's where the Computer Forensics Tool Testing (CFTT) program comes in. The focus of the CFTT program is to "...establish a methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware. The results provide the information necessary for toolmakers to improve tools, for users to make informed choices about acquiring and using computer forensics tools, and

for interested parties to understand the tools capabilities” (Information Technology Laboratory / Software and Systems Division Software Quality Group, 2019).

The Federated Testing Project is an off-shoot program of the CFTT that focuses on disk imaging, forensic media preparation, forensic string search, hardware write blocking, and mobile forensics data extraction. The Federated Testing test suites have been developed to verify the reliability and accuracy of these digital forensics tools. CFTT adds new tests as functionalities and types of digital forensics tools evolve.

To use the Federated Testing test suites:

1. Download the latest Federated Testing live [Linux.iso file](#) and use it to create either a bootable flash drive or a bootable DVD. The [Rufus](#) tool can be used to create a bootable flash drive from an .iso file.
2. “Insert the bootable flash drive or DVD into your forensic workstation and boot to it (you may need to change your computer's boot options to select your flash drive or DVD drive as your boot device). NOTE: to test Hardware Write Blocking and Disk Imaging tools you must boot a computer using a Federated Testing flash drive or DVD; when testing other types of tools however, e.g., a Mobile Forensics Data Extraction tool, one may consider booting a virtual machine in lieu of a computer.
3. Use the user interface (Firefox Web browser) to select the type of tool you want to test. The user interface will tell you what items you will need to have on hand to get started.
4. Use the interface to generate the test cases for testing your tool and follow the instructions to run each test.
5. Use the interface to generate a test report for your tool” (Information Technology Laboratory / Software and Systems Division Software Quality Group, 2023).

LEARNING ACTIVITY 2-3

1. [Create a Federated Testing bootable flash drive or DVD.](#)
2. Choose a tool from the [Computer Forensics Tools & Techniques Catalog.](#)
3. Use the Federated Testing suite to check the tool you chose.
4. Print a report of the test.

LEARNING ACTIVITY 2-4

1. Choose three tools from the [Computer Forensics Tool & Techniques Catalog.](#)
2. Make a table that shows each tool’s vulnerabilities and what their strengths are.

WRITE BLOCKERS

Write blockers are used in the acquisition process to prevent the computer from being able to execute any programs that would modify the contents of the disk. Write blockers can be software or hardware based but no matter which format is used, it should be validated as being effective.

The [CRU WriteBlocking Validation Utility](#) is a tool used to test the functionality of the write blocker being used. A software-based write blocker is a tool that is installed on a forensic workstation. A hardware-based write blocker is a physical tool that contains built-in write blocking software and has different adapters based on the device being acquired.

LEARNING ACTIVITY 2-5

Watch a video demonstration about using a hardware write blocker.

[Tableau External Write Blocker Setup and Forensic Imaging Walkthrough](#)

Posted by DFIRScience

Duration: 15 min. 38 sec.



LEARNING ACTIVITY 2-6

Practice using a write blocker validation utility.

1. Download and install [SAFE Block Win8-10](#) software write blocker. NOTE: You will need to provide an email address before being allowed to download the application.
2. Download and install the [CRU WriteBlocking Validation Utility](#). NOTE: You will need to provide an email address to receive a link to the download file. Do not change any of the options during installation.
3. Open the CRU WriteBlocker Validation Utility.
4. Insert a test USB drive that has files on it.

5. Start CRU WriteBlocker Validation Utility.
6. Save the report that is output after validation is completed.

ADDITIONAL RESOURCES

- Download FTK Imager: <https://www.exterro.com/ftk-imager>
- Quick#GUI Simple Hashing Tool: <https://www.quickhash-gui.org/downloads/>
- Cryptographic Module Validation Program: <https://csrc.nist.gov/projects/cryptographic-module-validation-program>
- Block Cipher Techniques: <https://csrc.nist.gov/projects/block-cipher-techniques>
- Cryptographic Standards and Guidelines: <https://csrc.nist.gov/Projects/cryptographic-standards-and-guidelines/example-values>
- Cyber Security Tools: <https://www.sans.org/tools/>
- OpenText Encase Product Sheet: <https://www.opentext.com/assets/documents/en-US/pdf/opentext-po-encase-forensic-en.pdf>
- CAINE Forensics Tools: <https://www.caine-live.net/>
- The Sleuth Kit & Autopsy: <https://sleuthkit.org/>
- Computer Forensics Tools & Techniques Catalog: <https://toolcatalog.nist.gov/>
- SANS Digital Forensics Cheat Sheets: <https://www.sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/>
- Write Blocker Testing Download: <https://www.cru-inc.com/support/software-downloads/writeblocking-validation-utility/>
- Department of Homeland Security Write Blocker Test Results Reports: <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical/hardware>

Chapter 3 — Evidence Acquisition Process

- Learning Objectives:**
- Recognize digital evidence storage formats.
 - Understand the legal considerations related to digital forensics acquisitions.
 - Learn how to use acquisition tools.
 - Learn how to validate data acquisitions.
 - Learn about other forensic tools available for data acquisitions.

Important Terms:

Chain of custody
Exclusionary Rule
Digital contamination
Write protection
Electronic Communications Privacy Act of 1986
Privacy Protection Act of 1980
Static acquisition
Live acquisition
Digital contamination

INTRODUCTION

Digital forensics evidence acquisition is the variety of techniques, methods, and processes by which electronic data is retrieved from computers, mobile phones, and other types of devices while also maintaining the integrity of the extracted data. This is critical to ensure accurate analysis and results in investigations, legal or otherwise.

How data is handled can make or break an investigation. If the data extraction is done improperly, the reliability of any evidence found can be questioned. From a legal perspective, it can be the difference between allowing or disallowing evidence into a court of law.

DIGITAL FORENSICS EVIDENCE ACQUISITION BASICS

Before going into the steps for evidence acquisition, it is important to understand the legal implications surrounding it. For example, for digital forensic evidence to be admissible in a court of law, it must meet two conditions:

1. It must be relevant.
2. It must be discovered by using scientific methods and can be validated.

More than that, though, there are legal considerations to think about before acquiring digital evidence. This includes determining how much authority an investigator has for a search and addressing key concerns related to federal laws such as the Electronic Communications Privacy Act of 1986, Privacy Protection Act of 1980, and applicable state and local laws.

The **Electronic Communications Privacy Act of 1986** is concerned with the protection of electronic communications while it is in transit and outlines the requirements for obtaining a search warrant. It also provides protection for electronically stored communications. In addition, it prohibits the use of tracing devices without having a court order that allows it.

The **Privacy Protection Act of 1980** protects work products and documentary materials from being accessed without having a subpoena. From a digital forensics' perspective, investigators must be cognizant of the proprietary data that is on a device. Digital forensic analysts "...need to be sensitive to how a lawful authorization to search may subsequently implicate the rights of third parties, who may have a reasonable expectation of privacy that could be invaded..." ("Forensic Examination," 2016).

The **Exclusionary Rule** is any rule that is used to exclude evidence from being admitted into a court of law. As digital forensics professional, it is imperative that evidence acquisition is done to keep the Exclusionary Rule from being invoked. One reason digital evidence can be deemed inadmissible or unreliable in a court of law has to do with poor evidence preservation and lack of physical security protocols. Maintaining the integrity of the data is of the utmost importance. One strategy around this is to ensure that there is a **chain of custody** document (Figure 3-1) associated with each piece evidence and that the evidence is stored and located up in a secure area.

CHAIN OF CUSTODY FORM			
Your Logo Here		Your Address Here	
[Agency Name] Case #:			
Item #	Date/Time Removed	Reason for Removal of Evidence	Signature

Figure 3 - 1. Example of chain of custody form. Source: Moulin, 2015

A second strategy is to ensure that great care is taken during the transportation and storage of digital devices and media; it is easy to damage evidence without realizing it. For example, the digital media that the evidence is on could be exposed to a variety of environmental conditions, magnetic forces, and physical damage. Placing these devices in faraday bags, boxes, or cages greatly reduces the chances of that happening.

When digital evidence is acquired, it can be stored in one of three formats: raw, proprietary, and Advanced Forensics Format (AFF). As you can see from Table 3-1, each format has its own advantages and disadvantages.

Table 3-1. Digital Forensics Data Formats

Data Format	Advantages	Disadvantages
Raw	• Data is written bit by bit • Fast data transfers • Most computer forensics tools can read raw format	• Storage space is the same as the original disk • Bad sectors may be passed over
Proprietary	• Have an option to compress or not compress image files • An image can be split into smaller segmented files. • Metadata can be integrated into the image file.	• Data format can only be read by the application that created it. • Segmented volumes have a file size limit.
Advanced Forensics Format (AFF) File extensions used: - .afd (image files) - .afm (metadata)	• Can provide compressed and uncompressed image files. • No file size restriction for disk-to-image files. • Open source for multiple platforms and operating systems. • Offers internal consistency checks for self-authentication.	

Data acquisitions are static or live. **Static acquisitions** refer to non-volatile data obtained from internal and external hard drives, DVD-ROMs, USB drives, SD or flash cards, smartphones, and other physical digital media. Data acquired from these devices does not change with the state of the computer; the computer can be shut down and data remains unchanged.

There are four methods used to acquire data:

- bit-stream disk-to-image file;
- bit-stream disk-to-disk;
- logical disk-to-disk or disk-to-disk data; and
- sparse data copy of a file or folder.

Table 3 - 2. Data Acquisition Methods

Data Acquisition Method	Method Considerations
bit-stream disk-to-image file Related applications: ProDiscover, EnCase, FTK, SMART, Sleuth Kit, XWays, iLook	- Most common - More than one copy can be made - Copies are bit-by-bit representations of the original
bit-stream disk-to-disk Related applications: EnCase, SafeBack, SnapCopy	- Used when a disk-to-image copy is not possible - Disk geometry
logical disk-to-disk or disk-to-disk data	- Used when acquisition time is limited - Captures only specific files - Used for large disk acquisitions (e.g. RAID) - PST or OST email files
sparse data copy of a file or folder	- Used when acquisition time is limited - Captures specific files and unallocated data

EVIDENCE ACQUISITION PROCESS

Several types of electronic devices have data that can be extracted. Note that each type has its own specific procedures:

Table 3-3. Digital Device Types

Type	Description
Computer systems	Laptops, desktops, towers, mini-computers, servers, mainframes
Storage devices	Internal and external hard drives, RAID systems, flash drives, memory cards, and other removable media
Handheld devices	Digital cameras, mobile and smart phones, GPS devices
Peripherals	Equipment that can be connected to a computer such as printers, scanners, docking stations, routers
Computer networks	Two or more computer network segments connected by routers, switches, and/or hubs via cables or wireless to communicate with each other, share data, and other resources.
Other	Drones, IoT and smart devices

The U.S. Department of Justice recommends the following guidelines to prepare and conduct evidence acquisition. An abbreviated version of these guidelines can be found in the Evidence Acquisition Decision Matrix on page 26.

- Never conduct analysis on the original image.
- Always create duplicate copies of an image using different tools and techniques.
- Photograph, document and secure all digital evidence.

- Determine the state of the device:
 - If an electronic device is off, leave it off.
 - If you are not sure if it is on:
 - Look for LEDs lighting up.
 - Check if you can hear any noise coming from the device (i.e. fans or spinning drives).
 - Look at the monitor:
 - Is it on, off or sleeping?
 - Does the display indicate messages that data has been deleted, formatted, removed, copied, moved, cut, or wiped?
 - Look for signs that it might be being accessed remotely or other communication with the device is happening.
 - Note all available cameras. Are any of them on?
 - If it is on, do not power it off until data can be acquired from it.
- Remove all unauthorized personnel from the area where the evidence is located.
- Gather all electronic devices found, including personal ones.
- Look for other types of digital evidence (i.e. mobile/smartphones, drones, motor vehicles, video recorders, IoT/smart devices).
- Separate all people of interest and note the location of where they were located when you got to the scene.
- Interview all people of interest:
 - Ask about the purpose of the devices.
 - What internet service provider is being used?
 - Get logins, passwords, user account names, email addresses used for computer, social media, and website access.
 - Find out what software or applications might be in use.
 - Any other relevant information.
- Document the scene; note the following:
 - Type, location, position, condition, and power status for each device.
 - Activity and processes showing on the display.
 - All connections, including network cables, to/from the device to other devices and connected to the internet.
 - Take photos and videos, make sketches of the scene.
- Evidence collection:
 - Do not attempt to look through the information or screens on any of the collected devices.
 - Do not press any of the keys on the keyboard.
 - Do not move the mouse or touch the track pad.
 - Do not move a device that is still powered on.
 - Do not accept assistance from people that you do not know.
 - Request technical help if required.
- Assess the situation:
 - Double-check to make sure the device can be legally seized.
 - Follow Figure 3-2. Evidence Acquisition Decision Matrix on page 26 as a guide.

DIGITAL CONTAMINATION

Implementing write protection is an important process to make sure data on a device remains unchanged during a forensic analysis. Gruber, et al. (2023) defines **digital contamination** as “a transfer of traits to an object of relevance at any point in the forensic process without intent”. However, prior to starting any data acquisition, it is crucial to make sure that the digital forensic analyst’s storage device is not contaminated. Digital contamination can happen in the following ways:

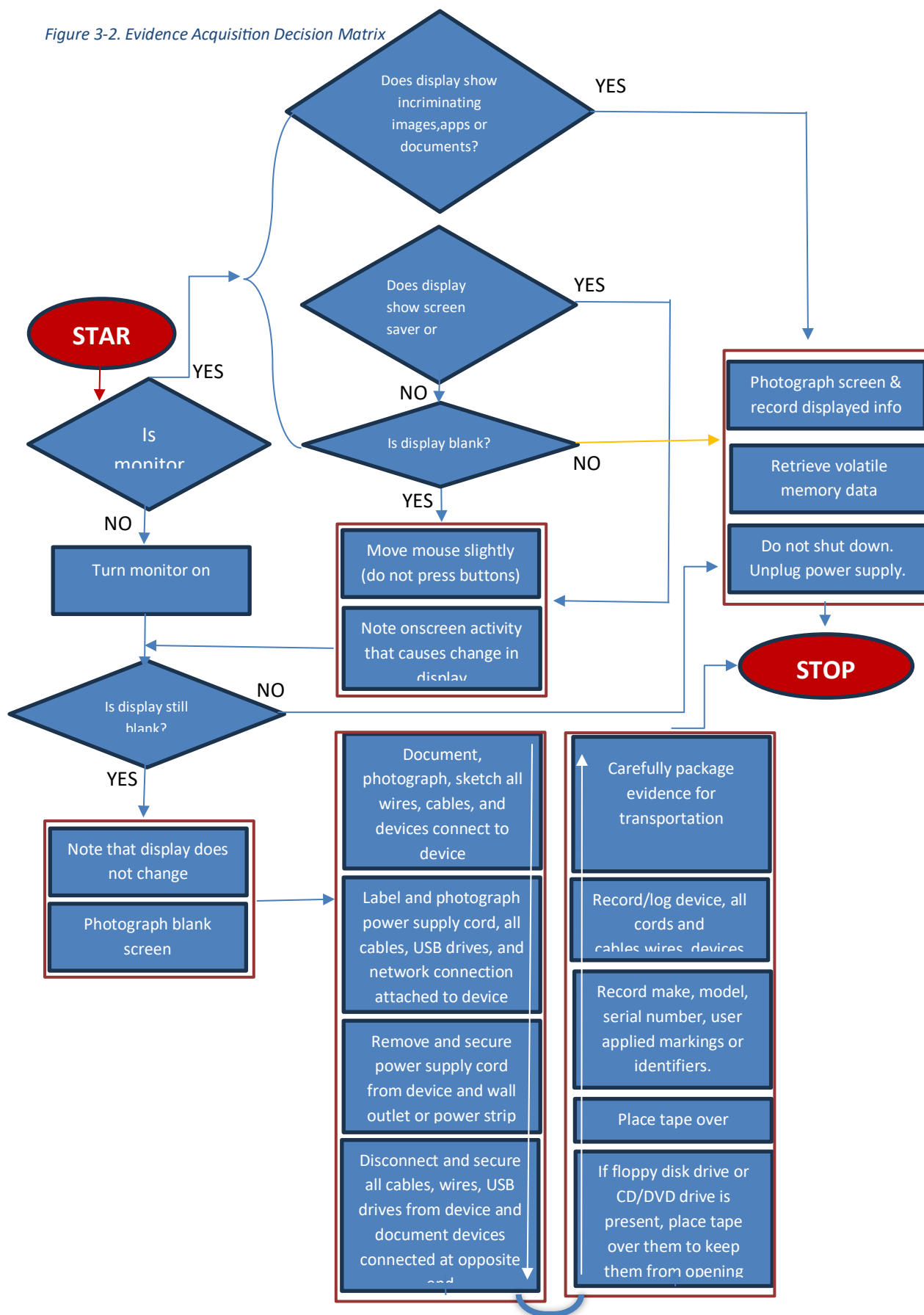
- Improper forensic booting into a device can cause changes to access timestamps, cache clean-ups, or other automatic process.
- Remote wiping of mobile devices may not be fully complete.
- SQLite write-ahead log modifications can inadvertently occur.
- Signal's RCE on Cellebrite UFED. A vulnerability found in a FFmpeg file which is used for file parsing in Cellebrite products exposes the device to being controlled by Remote Code Execution (RCE). A bad actor using RCE can contaminate the data.
- Storage devices not properly wiped may have residual data on it from a previous investigation.

DIGITAL ACQUISITION PROCEDURE FOR A COMPUTER

Adapted from *Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders*
U.S. Department of Justice National Institute of Justice, 2004, pp. 11-13

- Document hardware and software configuration and verify the operation of the examiner’s system.
- Making sure the area is protected from static electricity and magnetic fields, open the case of the computer that is going to be analyzed to gain access to its storage devices.
 - Use a Universal Digital Evidence Worksheet (Figure 3-3) to document all internal storage devices and note the hardware configuration. Also take note on the:
 - Drive condition (e.g., make, model, geometry, size, jumper settings, location, drive interface).
 - Internal components (e.g., sound card; video card; network card, including media access control (MAC) address; personal computer memory card international association (PCMCIA) cards).
- Disconnect storage devices (using the power connector or data cable from the back of the drive or from the motherboard) to prevent the destruction, damage, or alteration of data.
- Obtain configuration information from the suspect’s system through controlled boots.
 - Perform a controlled boot to capture CMOS/BIOS information and test functionality.
 - Boot sequence (change the BIOS to ensure the system boots from a flash drive, CD/DVD-ROM, or thumb drive).
 - Perform a second controlled boot to test the computer’s functionality and the forensic boot disk.
 - Ensure the power and data cables are properly connected and ensure the power and data cables to the storage devices are still disconnected.
 - Place the forensic boot disk into the CD/DVD-ROM or insert flash drive and boot the computer. Test to make sure you can boot from the forensic boot device.

Figure 3-2. Evidence Acquisition Decision Matrix



Universal Digital Evidence Worksheet

Fill in all sections as completely as possible. Attach additional documentation or information as needed.

Section 1. Case Information

Case Name:		Case/Docket Number:	
Attorney:		Contact Information:	
Investigator:		Contact Information:	

Section 2. Evidence Intake

Evidence Type:	Computer _____ Phone _____ GPS _____ Removable Storage _____ Other (Specify) _____ DVR _____ (Complete section 3)
Intake Date/Time:	Evidence Number:
Device Owner:	Contact Information:
Device Make/Model:	Serial Number:
Phone Number:	Carrier/Service Provider:
Operating System:	OS Version:
Screen name(s):	Passcode, passwords:
State of Device at Intake: (Powered on or off, detail any actions taken)	
Device Manual obtained?	
Physical Condition:	
Additional Components:	
Photograph Device:	Photograph Components:

Section 3. DVR System & Settings

DVR Make/Model/Serial No.	
Multiplexer Make/Model/Serial No.	
PC Based or Stand Alone?	Is system networked?
Number of hard drives:	Capacity of each:
Date of oldest recording:	
Are user manuals available?	
Native/Proprietary Format:	
Image Quality (High/Medium/Low)	
Frames Per Second:	
Aspect Ratio:	
System Firmware Version:	
System Password:	
Software password:	
Number of Cameras:	Active Camera Numbers:
Are any Cameras Infrared? (Y/N)	If yes, specify cameras:
Is Audio Recorded? (Y/N)	If yes, specify cameras:
Any Camera(s) Motion Triggered?	If yes, specify cameras:
Any Camera(s) Alarm Triggered?	If yes, specify cameras:
System Date/Time Displayed:	Actual Time/Date:
Sketch Scene	Note Camera Angles

Figure 3 - 3. Universal Digital Evidence Worksheet. Source: I.R.I.S. LLC

- Reconnect the storage devices and perform a third controlled boot to capture the drive configuration information from the CMOS/BIOS.
 - Ensure there is a forensic boot disk or flash drive connected to prevent the computer from accidentally booting from the storage devices.
 - Locate drive configuration information: logical block addressing (LBA); large disk; cylinders, heads, and sectors (CHS); or auto-detect.
- Power system down.
 - Whenever possible, remove the subject storage device and perform the acquisition using the examiner's system.
 - Exceptional circumstances may result in a decision not to remove the storage devices from the subject system:
 - RAID (redundant array of inexpensive disks). Removing the disks and acquiring them individually may not yield usable results.
 - Laptop systems. The system drive may be difficult to access or may be unusable when detached from the original system.
 - Hardware dependency (legacy equipment). Older drives may not be readable in newer systems.
 - Equipment availability. The examiner does not have access to necessary equipment.
 - Network storage. It may be necessary to use the network equipment to acquire the data.

When using the subject computer to acquire digital evidence, reattach the subject storage device and attach the examiner's evidence storage device (e.g., hard drive, tape drive, CD-RW).

- Ensure that your storage device is forensically clean when acquiring the evidence.
- Obtain hash value.
- Initiate write protection:
 - If hardware write protection is used:
 - Install the write protection device.
 - Boot system with the examiner's controlled operating system.
 - If software write protection is used:
 - Boot system with the examiner-controlled operating system.
 - Activate write protection.
- Investigate the geometry of any storage devices to ensure that all space is accounted for, including host-protected data areas (e.g., nonhost specific data such as the partition table matches the physical geometry of the drive).
- Capture the electronic serial number of the drive and other user-accessible, host-specific data.
- Acquire the subject evidence to the examiner's storage device using the appropriate software and hardware tools.
- Verify successful acquisition by comparing hash values of the original and the copy.

Chapter 4 — Using FTK Imager

Learning Objectives:

- Learn about what FTK Imager can do.
- Learn how to install FTK Imager.
- Understand how to use the most popular features of FTK Imager.
- Learn about the different forensic image formats.

Important Terms:

Open source
Raw dd file format
E01 file format
EX01 file format
AFF file format

INTRODUCTION

FTK Imager is an open-source tool used to image data for forensic analysis. **Open-source** tools are tools that do not require purchase or a paid subscription; they can be downloaded from the internet. As mentioned in the previous chapter, image data can come from digital media such as hard drives, USB flash drives, external drives, and other forms of media. FTK Imager version 4.7.1 (as of this writing) can be downloaded from [Exterro's website](#).



ACCESSDATA[®]
ForensicToolkit (FTK)



INSTALL AND CREATE A DISK IMAGE

LEARNING ACTIVITY 4-1

- A. Watch a video demonstration on [How to Install FTK Imager in Windows 10](#).
Posted by: Cyber Security – Purple Team
Duration: 2 min. 10 sec.



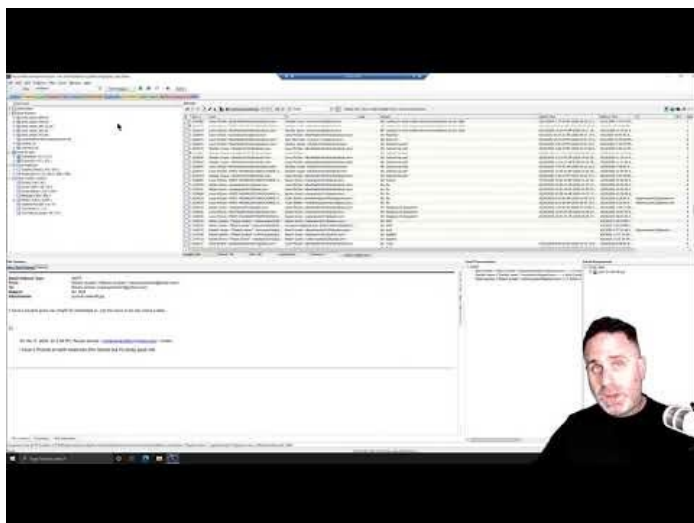
- B. Install FTK Imager on Windows 10 virtual machine.

LEARNING ACTIVITY 4-2

Watch [FTK Imager video demonstration](#).

Posted by: Justin Tolman

Duration: 43 min. 53 sec.

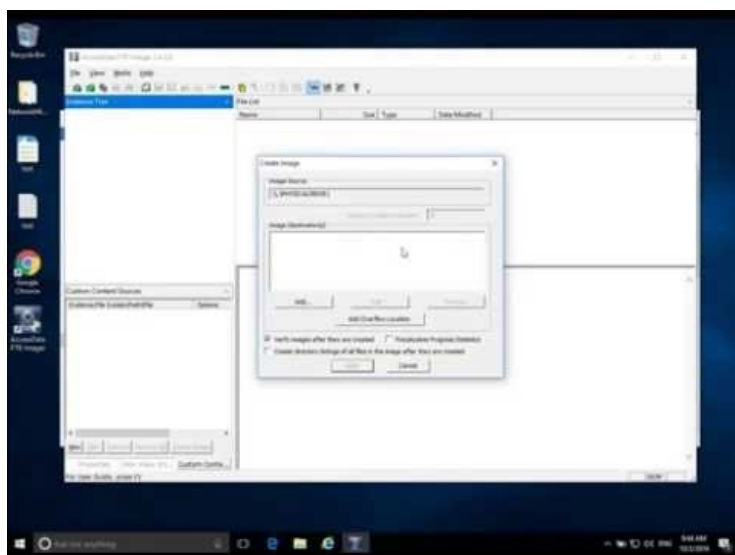


LEARNING ACTIVITY 4-3

Watch tutorial on [Forensic Acquisition in Windows – FTK Imager](#).

Posted By: DFIRScience

Duration: 29 min. 2 sec.



ADDITIONAL RESOURCES

- [Imager User Guide](#)
- [FTK Imager 4.7.1.2 – Release Notes](#)
- [Comprehensive Guide on FTK Imager](#)
- [Using FTK Imager](#)
- [How to create a forensic image of a physical hard drive using FTK Imager](#)
- [FTK Imager Command Line Physical Disk Hashing](#)

Chapter 5 —

Proper Forensics Methodology and Standards

- Learning Objectives:**
- Understand the legal and ethical considerations in digital forensics.
 - Know where to find the latest digital forensics standards and best practices.
 - Understand the four-step digital forensics methodology.
 - Know the most popular tools used in digital forensics.

Important Terms

- volatile memory
- trier of fact
- hashing

INTRODUCTION

According to the National Institute of Standards and Technology (NIST), digital forensics is “...the field of forensic science that is concerned with retrieving, storing and analyzing electronic data that can be useful in criminal investigations. This includes information from computers, hard drives, mobile phones and other data storage devices” (National Institute of Standards & Technology, n.d.). Using the proper digital forensics methodology involves a four-step process: collection, examination, analysis, and reporting. These steps help to ensure viable data is retrieved using accepted standards and within legal limits.

LEGAL AND ETHICAL CONSIDERATIONS

LEGAL FRAMEWORK AND REQUIREMENTS

The following laws are important for digital forensics analysts to understand:

- [Fourth Amendment](#) – Related to warrantless search and seizure of computers.
- [Protection Act, 42 U.S.C 2000aa](#) – Search warrant restrictions related to examining computers.
- [Stored Communications Act, 18 U.S.C 2701-12](#) – Provides protections around how digital forensics analysts get access to the account records from internet and mobile service providers.
- [Child Exploitation and Obscenity Section \(CEOS\)](#) of 1987 provides the laws around computer-related child pornography.
- [Article VII of the Federal Rules of Evidence](#) – Digital forensics experts may be called to testify to their findings in court. This Article encompasses six rules related to providing expert testimony.
 - Rule 701: Opinion Testimony by Lay Witnesses
 - Rule 702: Testimony by Expert Witnesses
 - Rule 703: Bases of an Expert’s Opinion Testimony

- Rule 704: Opinion on an Ultimate Issue
- Rule 705: Revealing the Facts Underlying an Expert's Opinion
- Rule 706: Court-Appointed Expert Witnesses
- [The Computer Fraud and Abuse Act of 1986](#) – This law is an amendment to the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, expanding on the offenses that qualify as a computer-related crime.

ETHICAL GUIDELINES & PROFESSIONAL CONDUCT

To help maintain the integrity of the digital forensics field, several professional organizations have developed their own versions of ethical conduct and rigorous standards. The three listed below are the most common but there definitely are others. Which organization you choose to belong to is a personal choice or can be mandated by your employer; read through the code of ethics, professional standards and select the organization that best aligns with your own beliefs and thoughts about how digital forensics should be surveilled.

- [International Society for Forensics Computer Examiners \(ISFCF\)](#) – ISFCF's code of ethics provides for maintaining objectivity; presenting accurate findings; using industry-accepted techniques; following accepted principles; being truthful in court; refraining from conflicts of interest; and maintaining confidentiality. In addition, a forensics examiner cannot misrepresent their credentials.
- [High Technology Crime Investigation Association \(HTCIA\)](#) – HTCIA is a non-profit organization. They have a Code of Ethics of Professional Standards of Conduct which includes using HTCIA-approved techniques and advanced technologies in their examinations to help decrease the number of wrongful convictions.
- [International Association of Computer Investigative Specialists \(IACIS\)](#) – The code of ethics for members of the IACIS includes maintaining objectivity during investigations; representing all facts and that they are presented accurately; examining evidence thoroughly; maintaining an unbiased opinion when analyzing evidence and coming to conclusions.

PRIVACY CONCERNS & DATA PROTECTION

Electronic devices contain all sorts of data. Being able to separate digital evidence from personal data requires the scrutiny of a digital forensic investigator. The nature of digital forensics investigation can be unavoidably invasive to a person's privacy.

There is a tradeoff between preserving privacy and effectively investigating a device. The concern with privacy in digital forensics is that the Fourth Amendment limits the type of information that can be searched or seized, but not the protocols used to conduct the search of information (Aminnezhad et al., 2015). This is where the importance of ethics fits in. It is up to digital forensics examiners to follow a code of ethics as they carefully examine data and make reasonable decisions to determine its relevancy to a case.

OTHER CONSIDERATIONS

Before conducting any analysis of data, it is critical to make sure there is documentation authorizing the activity. Depending on the type of investigation, documentation can be a search warrant, consent form, or other comparable instrument.

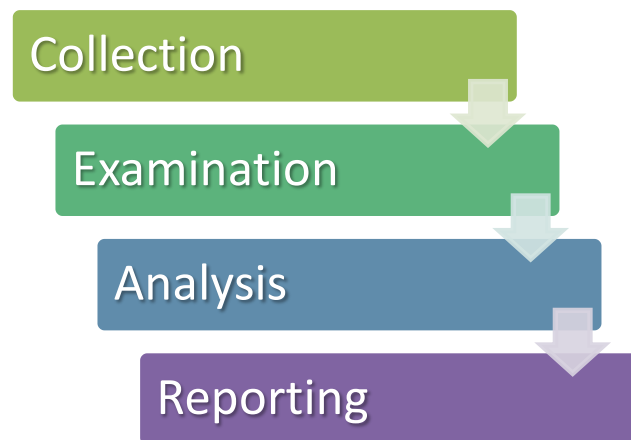
It's also important to validate tools to not only ensure their accuracy, but to further ensure the digital evidence extracted meets the requirements of 'trier of fact' to be admissible in a court of law. According to LegalDictionary.com:

"A **trier of fact** is a person, or group of people, tasked with determining – from the facts of a case – whether a certain thing is true, usually during the trial of the matter. Depending on the way in which the matter is tried, who is considered the trier of fact can vary. For example, the trier of fact during a jury trial is the jury itself. During a bench trial, the trier of fact is the judge, and during an administrative hearing, the administrative law judge serves as the trier of fact" (Trier of Fact, 2017).

PROPER DIGITAL FORENSICS METHODOLOGY

THE FOUR-STEP PROCESS

There are four steps to the digital forensics methodology: collection, examination, analysis, and reporting:



Collection. The data collection process begins with using a variety of specialized tools to gather volatile evidence first before approaching non-volatile evidence acquisition. **Volatile evidence** is any data that would be lost once the device is powered off. Examples of this include CPU, cache, and registry content; routing table, ARP cache, process table; memory; and the temporary file system and swap space.

By themselves, memory modules can contain information about processes, files, directories, network connections, open files, configuration parameters, encryption keys, commands that have

been used, memory-specific exploits, websites that have been visited, evidence of a rootkit, and more. Data located on the hard disk is considered non-volatile.

If the tools used to acquire the digital evidence are faulty, it calls the evidence to question and will likely be inadmissible in a court of law. To make sure the hardware and software tools used in the digital forensics process are working properly, they must be regularly validated.

Examination. Data that is uncovered is then categorized and organized. The digital evidence collected is examined to determine what is relevant to the case at hand.

Analysis. A systematic process is used to search for relevant evidence. Conclusions are drawn based on evidence that is found.

Reporting. In a digital forensic investigation, everything that is done with a device and any relevant evidence discovered must be documented. Documentation can, but is not limited to, include taking photographs, drawing sketches, and taking notes. A final report includes detailed information about the investigation, the steps taken to acquire the data, and conclusions made.

CHAIN OF CUSTODY AND EVIDENCE HANDLING

To keep digital evidence from being questioned in a court of law, great care must be taken to protect its authenticity. In digital evidence collection, cryptographic hashes and maintaining the chain of custody are the best way to ensure that.

As mentioned in Chapter 3, a chain of custody form (Figure 5-1) is used with each evidence item. Each time evidence is moved to a new location or submitted to a different person, the date and time, reason for taking possession of the evidence, and a signature of the person taking custody of the evidence must be documented.

CHAIN OF CUSTODY FORM			
Your Logo Here		Your Address Here	
[Agency Name] Case #:			
Item #	Date/Time Removed	Reason for Removal of Evidence	Signature

Figure 5- 1. Example of chain of custody form. Source: Moulin, 2015

DOCUMENTATION AND RECORDKEEPING

Any time a digital forensics examination is done on a device, a report must be prepared outlining the following, at minimum (Council of the Inspectors General on Integrity and Efficiency (CIGIE), 2019, p. 2):

- The organization creating the report.
- An assigned case number or identifier.
- The name of the person submitting the report.
- The date of the report and any other relevant date information.
- A description of the evidence.
- Name and signature of the person conducting the analysis.
- Results and conclusions of the examination.
- Any relevant work notes.

It is also recommended that a separate administrative and technical review be done of all digital forensics reports for quality assurance purposes.

ENSURING DATA INTEGRITY AND AUTHENTICITY

Hashing is a cryptographic algorithm function that is applied to digital evidence (e.g., a file, disk, or string of characters) to verify the copy is the same as the original data. The cryptographic algorithm produces a unique output based on the data that is input. The mere change of one character in a file will change the hash value output, making this the perfect tool to verify the integrity of a file or disk image.

For example, let's say that you downloaded a file from the internet. The person that posted the file will sometimes also post the file's hash value. Before you open the downloaded file, you input the file into the selected hashing algorithm (e.g., MD5, SHA-1, SHA-256). If your hash value is the same as what was posted on the webpage, the file has not been corrupted or tampered with. If the two values are not the same, the file has been altered.

DIGITAL FORENSICS TOOLS AND TECHNIQUES

Digital forensics tools can be categorized into the following classifications:

- *Disk and data acquisition* tools to pull data or create a copy from a Windows or Linux disk.
- *File viewers and analysis* tools to extract and analyze specific files.
- *Windows registry analysis* tools to uncover the computer user's activities.
- *Internet and network analysis* tools provide information about network activity.
- *Email analysis* tools to scrutinize emails.
- *Mobile device analysis* tools to extract data from mobile devices.
- *Mac operating system tools* for disk imaging, metadata extraction, and analysis.
- *Database forensics* tools to analyze and create reports.

Table 5-1 below shows a list of the most popular tools used today and what each is used for.

Table 5-1. Digital Forensics Tool Capabilities

Tool	Data Acquisition & Imaging	File System Analysis	Artifact & Metadata Analysis	Network Forensics & Log Analysis	Mobile Device Forensics	Cloud Forensics	IoT Forensics	Memory Forensics
Autopsy	X	X						
Cellebrite					X			
Datadog Security Monitoring				X				
FAW (Forensic Acquisition of Websites)					X			
FTK Imager	X	X	X		X			
Log Rhythm				X				
Magnet Axiom	X	X			X	X	X	
MSAB					X			
MVT					X			
NetworkMiner				X				
OpenText EnCase	X	X			X			
Paraben E3					X	X	X	
ProDiscover	X	X	X					
Query.ai				X		X		
SIFT Workstation	X	X	X	X	X	X	X	
SleuthKit	X	X						
SolarWinds Security Event Manager				X				
Volatility								X
Wireshark				X				
X-Plico				X				
X-Ways Investigator		X						

No matter what tool you choose to use in the digital forensics process, it is important to regularly perform validation testing on it to ensure it is working properly. A malfunctioning tool causes any data retrieved using it, to not be trusted; and will likely not be admissible in a court of law.

The following instruments are available for conducting tool validations:

- Cryptographic Algorithm Testing: <https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program>
- Digital Forensics Tool Testing: <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/federated-testing>

The National Institute of Standards and Technology (NIST) conducts its own testing and posts its own validation test results:

- [Disk Imaging Tool Test Reports](#)
- [Mobile Device Tool Test Reports](#)
- [Hardware Write Block Tool Test Reports](#)
- [Forensic String Search Tool Test Reports](#)
- [Forensic Media Preparation Tool Test Reports](#)

DIGITAL FORENSICS STANDARDS & BEST PRACTICES

The digital forensics community works hard to ensure that the field maintains its credibility. Several organizations have been formed to keep all interested parties informed of best practices and standards in digital forensics. The most prominent groups include the IOCE, SWGDE, NIST, and ISO as described below:

- The Scientific Working Group on Digital Evidence (SWGDE) connects organizations that conduct digital forensics investigations together in an effort to keep all of them informed and in sync on the latest digital forensics techniques, standards and best practices. [SWGDE has their established standards and best practices for digital forensics](#). They are regularly reviewed and updated as technology and techniques advance.
- The National Institute of Standards and Technology (NIST), founded in 1901, is an organization managed by the U.S. Department of Commerce. Their mission is to “...promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life” (National Institute of Standards and Technology, 2022). NIST offers their [Digital Forensics and Incident Response \(DFIR\) Framework for Operational Technology \(OT\)](#) as an established standard for digital forensics practices.
- The International Organization for Standardization (ISO) is an independent international organization made up of 168 different countries. Its purpose is to establish standards that are recognized worldwide. Their guidelines are published in the document, [ISO/IEC 27037:2012 - Guidelines for identification, collection, acquisition, and preservation of digital evidence](#).

CASE STUDIES AND REAL-WORLD EXAMPLES

Digital forensics has taken center stage in several prominent cases. Stories of how digital forensics has solved some very prominent cases were discussed in Chapter 1. Digital forensics has led to the identification of both the BTK Killer and the Craigslist Killer.

However, another case we can look at involves the death of Michael Jackson. It was determined that Michael Jackson died of excessive amounts of prescription medication. As a result, his personal physician, Dr. Conrad Murray was brought to trial. A digital forensics investigation uncovered documentation regarding the prescriptions the doctor ordered for Michael. It showed that the prescribed doses were lethal amounts.

Magnet Forensics, a digital forensics software company, published a case where a family business caught fire in February 2018 (Cadden, 2022). Arson was suspected but the business' DVR security camera system was operational. The fire severely damaged the DVR but the hard drive seemed to be intact. Using digital forensics software specifically for DVR devices, the camera footage was recovered, and it showed who started the fire and how.

LEARNING ACTIVITY 5-1

Case Study: Work on The HoneyNet Project's [Forensics Challenge](#).

LEARNING ACTIVITY 5-2

Linux Case Study: Work on [A Linux Forensics Starter Case Study](#).

FUTURE TRENDS AND CHALLENGES IN DIGITAL FORENSICS

As technology advances, it opens the door to exciting new trends and unexpected challenges. For example, with the increased demand by smartphone customers for more security, vendors are integrating stronger encryption technologies and other mobile device security. This is making it exceedingly difficult for digital forensics examiners to gain access to these devices. (Mahalik & Lorentz, 2022)

The technological advancement in microchips allows smartphone manufacturers to create devices that are smaller, lighter, and thinner. Unfortunately, this also makes these devices that much more fragile. The new chips are so small and thin that the chance of damaging them upon attempting to remove them is very high. (Mahalik & Lorentz, 2022)

The same complications have also yielded some positive trends:

- More online digital forensics communities are sharing information with each other. With so many people contributing their expertise, there are many more opportunities to find resolution to complicated digital forensics techniques.

- The positive outcomes of digital forensics investigations in the law enforcement community have inspired the need to train personnel better. Standard operating procedures need to be updated or created to integrate the digital forensics process.
- With the better digital forensics handling training that law enforcement is receiving, data acquisitions are being done with greater care. This is leading to more digital forensics evidence being admitted in a court of law and more cases being solved.

Artificial intelligence and machine learning also play a role in the forward progress of digital forensics technologies. Cyberattacks are becoming more complex and artificial intelligence (AI) can make use of its "...pattern detection and recognition capabilities to uncover hidden evidence in digital artifacts that would have been missed if conducted manually" (Solanke & Biasiotti, 2022, p. 143). With the excessive amounts of data that drives can store and that networks can process, AI can help classify data during digital forensics analysis very efficiently.

CONCLUSION

- Understanding the laws related to digital forensics is important because it can make the difference between evidence being admissible or being disqualified in a court of law.
- It is important to stay current with digital forensics standards and best practices to ensure analysts are working in a legal and ethical manner. It also makes certain that all digital forensics examiners are aligned to using the same procedures.
- The digital forensics methodology involves four stages: collection, examination, analysis, and reporting.
- There are so many facets to digital forensics and advances in the field are growing exponentially. Continuous learning is imperative to staying on top of it all.

ADDITIONAL RESOURCES

- Windows Incident Response Blog: <https://windowsir.blogspot.com/>
- Cryptographic Algorithm Validation Program: <https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program>
- Scientific Working Group on Digital Evidence (SWGDE) document repository: <https://www.swgde.org/documents/published-complete-listing>
- Digital Forensics Association: <http://www.digitalforensicsassociation.org/>

Chapter 6 —

File Systems: Electronic Evidence Issues

Learning Objectives:

- Know the common file systems in use today.
- Compare and contrast different file systems.
- Learn about the different file-system-specific digital forensics processes.
- Know the challenges and future trends in file system forensics.

Important Terms

Solid-state drive
File system
File Allocation Table
New Technology File System
Extended File System
Hierarchical File System
Apple File System

INTRODUCTION

Another aspect of a digital forensics investigation is the examination of the file system. Understanding how the files and folders are structured on a disk or solid-state drive (SSD) helps make looking for evidence easier. In Figure 6.1, you can see that the **file system** is the organizational structure of a computer where all files are compartmentalized into folders. Folders are organized into directories that exist on a partition. The files of an operating system such as Windows or MacOS are typically stored on their own partition. Other partitions can contain the various programs used and the files that a user creates from normal use.

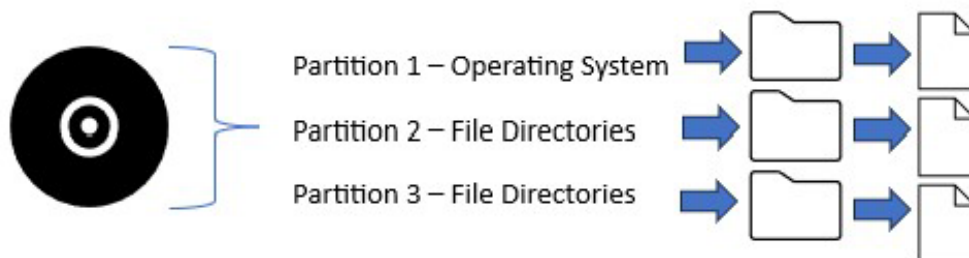


Figure 6 - 1. General NTFS file system hierarchy.

File systems are kept on a storage device such as a hard disk (Figure 6-2) or solid-state drive (SSD) (Figure 6-3). Older desktop computers and laptops had hard disks that were made of magnetic platters and had an arm that wrote data to them. Modern laptops and computers have a solid-state drive (SSD) which is made of semiconductors.



Figure 6 - 2. Antiquated desktop hard drive.
Source: <https://assets.website-files.com/>



Figure 6 - 3. External Solid-state Drives
Source: <https://static1.makeuseofimages.com/>

There are different types of file systems or organizational file structures as shown in Table 6-1 below.

Table 6 - 1. File Systems by Type

	Windows	MacOS	Linux
FAT (File Allocation Table)	X		
NTFS (New Technology File System)	X		
HFS+ (Hierarchical File System Plus)		X	
EXT (Extended File System)			X
APFS (Apple File System)		X	

As you can see, there are different file systems depending on the system you have. Below is a comparison of the advantages and disadvantages of various file systems:

Table 6 - 2. Advantages and Disadvantages of Different File Systems

File System	Advantages	Disadvantages
FAT16	Maximum partition size is 4TB	Maximum file size is 2GB
FAT32	- Compatible with USB flash drives and game consoles - Maximum partition size is 8 TB	- Maximum file size is 4GB - No file permissions available
exFAT	- Compatible with USB flash drives - Compatible with NTFS drives - Compatible with MacOS and Linux - Compatible with PlayStation 4 & 5 - Compatible with Xbox X, S, and One - Maximum file size is 128 TB - Maximum partition size is 128 TB	- Incompatible with PlayStation 3 - Incompatible with Xbox 360
NTFS	- It is faster than FAT - Has integrated security features - Uses file journaling - Automatic corruption correction - Supports file encryption - Compatible with Xbox X, S, and One - Maximum file size is 256 TB - Maximum partition size is 256 TB	- Compatible with operating system Windows XP and newer - Macs cannot write to a NTFS-formatted drive - Incompatible with PlayStation consoles - Incompatible with Xbox 360 - Linux OS can only read NTFS files but not write them to an NTFS-formatted drive.
HFS+	- Supported on all versions of MacOS X and MacOS - Best for older mechanical drives or with older versions of MacOS	- Incompatible with Windows file systems - No data integrity checking - Not recommended for SSDs
EXT	- Compatible with Windows and MacOS - Option to encrypt	
APFS	- Full disk encryption - Increased read/write speeds on SSDs - Increase storage space - Best for SSDs and flash drives - Option to encrypt	- No compression capability - Not compatible with MacOS earlier than High Sierra. - Incompatible with any Windows file systems - Encryption slows down performance

FILE TYPES

File Allocation Table (FAT)

FAT (File Allocation Table) was the default file system for Windows before the modern-day NTFS came out; by today's standards, it is very slow. FAT16 was the very first type of file system for Microsoft and later FAT32 was developed. The file structure is based on a file allocation table which is a type of index. The nature of writing a file to a disk is that it can be fragmented, with the different parts of the file being written to different parts of the disk. The file allocation table is what is used to chain those files together. It keeps track of where the various pieces of a file are on the disk. (Burn, 2022)

The basic FAT file system directory starts with three main folders: *Windows Operating System files*, *Program files* and *Documents and Settings*. The *Windows* folder has a subfolder *system32*. The *Program Files* folder is where applications and other programs reside. The *Documents and Settings* folder has two main folders: *All Users* and *{Username}*. *{Username}* indicates the username created by the owner of the computer system. The *All Users* and *{Username}* folders both consist of four main folders: *Desktop*, *Favorites*, *My Documents* or *Shared Documents*, and *StartMenu*. The *Shared Documents* folder in the *All Users* directory contains three folders: *Shared Music*, *Shared Pictures*, and *Shared Video*. The *My Documents* folder in the *{Username}* directory contains three folders: *My Music*, *My Pictures*, and *My Video*.

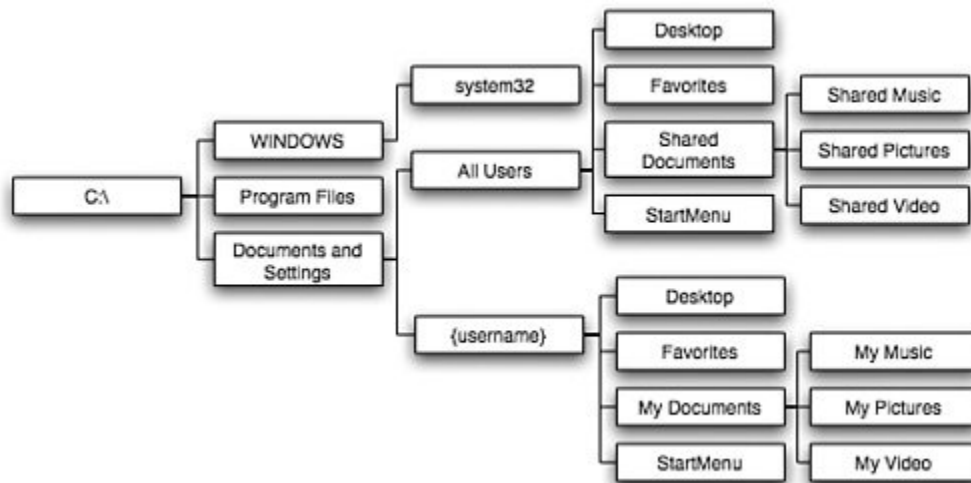


Figure 6 - 1. Basic FAT file system directory structure.

Source: <https://flylib.com/books/2/97/1/html/2/images/04fig07.jpg>

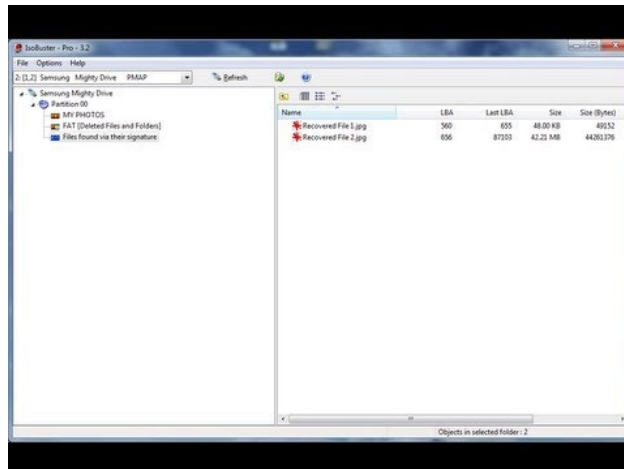
When a file is deleted off a FAT file system, the entry of that file in the file allocation table is what is deleted, not the file itself. The file itself remains on the computer until another file is written over it.

LEARNING ACTIVITY 6-1

Watch [Recover deleted files and folders from a FAT formatted disk \(Undelete FAT\)](#)

Posted by IsoBuster

Duration: 2 mins. 40 secs.



LEARNING ACTIVITY 6-2

Watch [011 FAT File Systems FAT32 and FAT16 forensics](#)

Posted by SystemForensics

Duration: 1 hour 5 mins.



NEW TECHNOLOGY FILE SYSTEM (NTFS)

NTFS (New Technology File System) is the current default Windows file system. It provides for increased reliability and security over FAT16 or FAT32. It is also capable of supporting larger volumes of data than FAT. Some of the distinctive features NTFS has is the capability of self-healing corrupt files, access control lists for files and folders, BitLocker encryption, large data volumes, longer file and path names, backwards compatibility, and file system compression. (*NTFS Overview*, 2023)

When a disk is formatted as NTFS it gets divided into partitions. The operating system is responsible for keeping track of the files on the various partitions utilizing a Master File Table (MFT) by recording each file's attributes (see Table 6 - 3). Up to 512 bytes are used for each file to record the set of attributes for that file.

Table 6 - 3. NTFS Attribute Types

Attribute Name	Description
\$ATTRIBUTE_LIST	Lists the location of all attribute records that do not fit in the MFT record
\$BITMAP	Attribute for Bitmaps
\$DATA	Contains the default file data
\$EA	Extended the attribute index
\$EA_INFORMATION	Extended attribute information
\$FILE_NAME	File name
\$INDEX_ALLOCATION	The type name for a Directory Stream. A string for the attribute code for index allocation
\$INDEX_ROOT	Used to support folders and other indexes
\$LOGGED_UTILITY_STREAM	Use by the encrypting file system
\$OBJECT_ID	Unique GUID for every MFT record
\$PROPERTY_SET	Obsolete
\$REPARSE_POINT	Used for volume mount points
\$SECURITY_DESCRIPTOR	Security descriptor stores ACL and SIDs
\$STANDARD_INFORMATION	Standard information, such as file times and quota data
\$SYMBOLIC_LINK	Obsolete
\$TXF_DATA	Transactional NTFS data
\$VOLUME_INFORMATION	Version and state of the volume
\$VOLUME_NAME	Name of the volume
\$VOLUME_VERSION	Obsolete. Volume version

Source: https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-fscc/a82e9105-2405-4e37-b2c3-28c773902d85



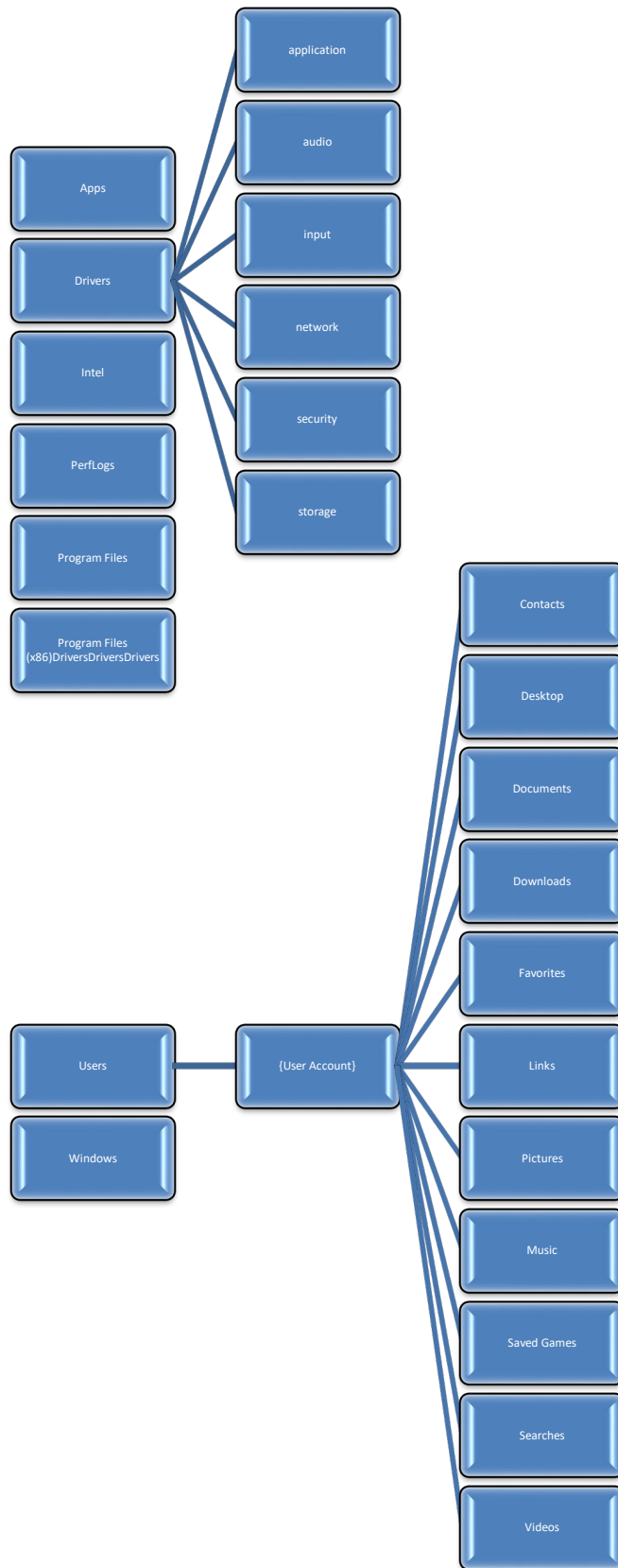


Figure 6 - 2. Diagram of basic Linux file structure.

LEARNING ACTIVITY 6-3

Watch [Introduction to Windows Forensics – Digital Forensics Course](#)

Posted by 13Cubed

Duration: 1 hour, 5 mins.



HIERARCHICAL FILE SYSTEM PLUS (HFS+)

HFS+ is the default operating system for older Mac computers. HFS+ “...(also known as Mac OS Extended or HFS Extended) is a journaling file system developed by Apple Inc. It replaced the Hierarchical File System (HFS) as the primary file system of Apple computers with the 1998 release of Mac OS 8.1. HFS+ continued as the primary Mac OS X file system until it was itself replaced with the Apple File System (APFS), released with macOS High Sierra in 2017. HFS+ is also one of the formats supported by the iPod digital music player.” (*HFS Plus*, 2023)

EXTENDED (EXT) FILE SYSTEM

EXT (Extended File System) has been the default operating system for Linux computers since the beginning. EXT originated from a different file system called Minix. The original EXT file system came out in 1992. Since then, there have been three upgrades from the original: EXT2 (1993), EXT3 (2001), and EXT4 (2008).

The EXT2 file system was created as an improvement of the original EXT file system and was the first commercial grade file system for Linux. The EXT3 file system was created to overcome the limitations of EXT2 and is the most common file system used in all the Linux distributions.

Compared to its predecessors, the latest EXT4 file system offers better performance, increased capacity, and better reliability (see Table 6-4 below for comparison). And compared to the FAT or NTFS file system, EXT4 has decreased the need for file fragmentation. (Both, 2017)

Table 6-4. Comparison of EXT File Systems (Adapted from "Difference Between," 2020)

File System	Advantages	Disadvantages
EXT2	• Best to use on SD cards and USB drives	• Does not support journaling. • Supports file sizes of 16GB-2TB. • File system size can be 2TB-32TB.
EXT3	• Supports journaling which is used to track file changes and reduce the chance of data loss. • Supports file system sizes between 4TB to 32TB. • Upgrading from EXT2 to EXT3 requires no down time.	• Supports file sizes of 16GB-2TB. • Upgrading from EXT2 to EXT3 is accomplished online.
EXT4	• Supports journaling and incorporates a checksum for extra security. • Backwards compatible with EXT2 and EXT3, so no upgrade is required. • Unlimited number of subdirectories. • Maximum file size increased from 2TB to 16TB. • Maximum file system size increased from 32TB to 1EB. • File time stamps are given to the nanosecond..	

Figure 6-6 (below) shows the general Linux file structure with short descriptions of each. Please note that the "/" indicates the root directory.

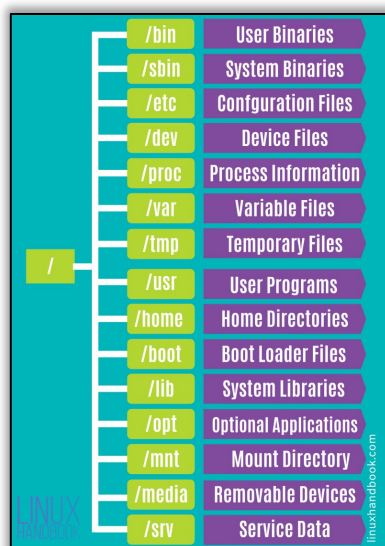


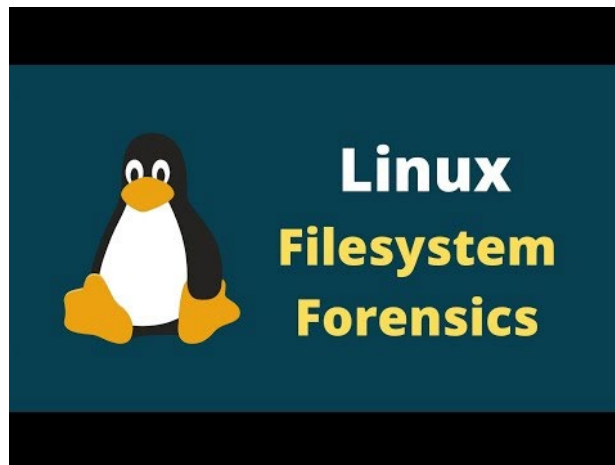
Figure 6 - 3. Simplified Linux file structure.

LEARNING ACTIVITY 6-4

Watch [Linux Forensics Tutorial || Linux file system forensics](#)

Posted by CS Lesson

Duration: 1 hour 50 mins.



LEARNING ACTIVITY 6-5

Watch [Linux Forensics Investigation | TryHackMe Linux Forensics](#)

Posted by Motasem Hamdan

Duration: 28 mins. 17 secs.



HIERARCHICAL FILE SYSTEM PLUS (HFS+) & APPLE FILE SYSTEM (APFS)

HFS+ “(also known as Mac OS Extended or HFS Extended) is a journaling file system developed by Apple Inc. It replaced the Hierarchical File System (HFS) as the primary file system of Apple computers with the 1998 release of Mac OS 8.1. HFS+ continued as the primary Mac OS X file system until it was itself replaced with the Apple File System (APFS), released with macOS High Sierra in 2017. HFS+ is also one of the formats supported by the iPod digital music player.” (*HFS Plus*, 2023)

APFS (APPLE FILE SYSTEM)

APFS (Apple File System) is the next version of Apple’s proprietary file system and first deployed with the Sierra (v.10.12) operating system in September 2016. As shown below in Table 6-5, APFS is an improvement over HFS+. Some of the more prominent features include optimization for solid-state drives and improved data integrity and encryption. (Vigo, 2018) To see a full timeline of Mac operating systems, visit [Wikipedia’s Mac operating systems page](#).

Table 6 - 5. Advantages and Disadvantages of the HFS+ and APFS File Systems

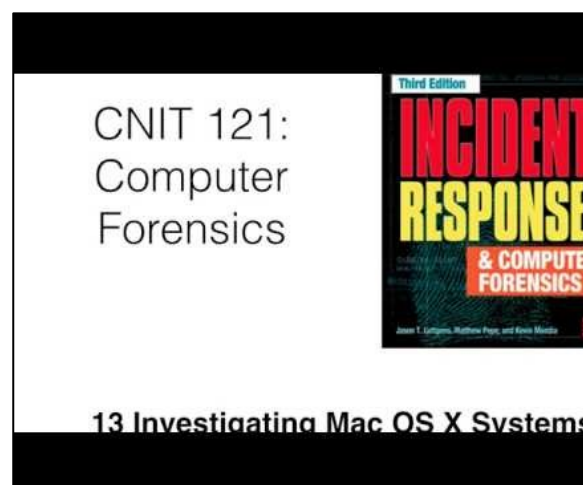
	Advantages	Disadvantages
HFS+	- Supported on all versions of Mac OS X and macOS. - Supports Fusion drives. - Capable of using NVRAM for data storage.	- No snapshot feature. - No support for dates later than February 6, 2040. - Does not use nanosecond-formatted file time stamps - Doesn't use checksums to ensure data integrity.
APFS	- Backwards compatibility for HFS+ file system. - Allows for snapshots. - Faster disk speeds. - Increased maximum of files. - Better crash protection. - Uses nanosecond file time stamps. - Maximum number of files is increased from 2^{32} to 2^{63}. - Utilizes checksums to ensure metadata integrity. - Supports full disk encryption. - Provides support for dates beyond February 6, 2040. - Backs up data more efficiently.	- Incompatible with any macOS earlier than Sierra - No support of directory hard links. - APFS files can only be read from a Windows (NTFS) computer and only by using third-party software. - Checksums are limited to metadata only, not user data. - Does not support Fusion drives

LEARNING ACTIVITY 6-5

Watch [CNIT 121:13 Investigating Mac OS X Systems \(Part 1 of 2\)](#)

Posted by Sam Bowne

Length: 25 mins. 5 secs.

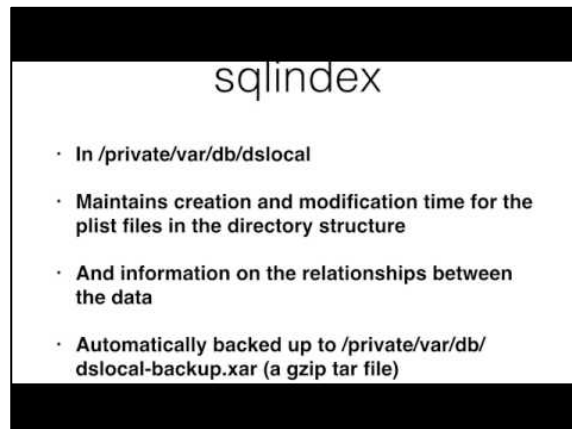


LEARNING ACTIVITY 6-6

Watch [CNIT 121: 13 Investigating Mac OS X Systems \(Part 2 of 2\)](#)

Posted by Sam Bowne

Length: 30 mins. 16 secs.

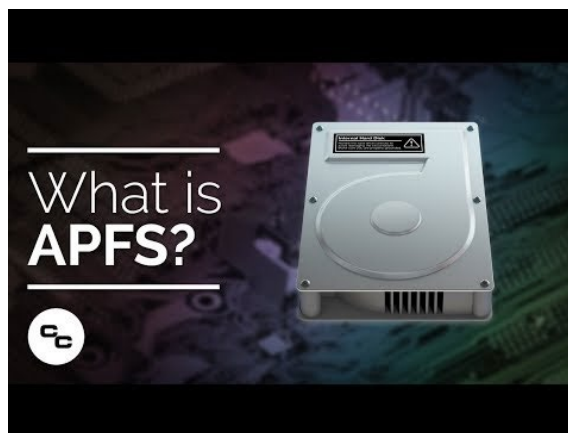


LEARNING ACTIVITY 6-7

Watch [What is APFS? The Apple File System Explained](#)

Posted by Computer Clan

Length: 19 mins. 52 secs.



LEARNING ACTIVITY 6-8

Watch [Imaging APFS – A Walkthrough for Starting Forensics on MacOS](#)

Posted by SEVN X

Length: 12 mins. 40 secs.



CHALLENGES & FUTURE TRENDS IN FILE SYSTEM FORENSICS

ENCRYPTION

Most computers now come with full disk encryption (FDE) which has produced some challenges for digital forensics examiners. Some of the problems that can occur are:

- Shutting down a running computer, not realizing that it is fully encrypted.
- Failure by digital forensics analysts to search the crime scene for possible clues to passwords or passphrases.
- If the computer is equipped with a Trusted Platform Module (TPM) chip, any change to the hardware of the system (e.g., removing the SSD card or hybrid drive) makes the data unretrievable or causes irreversible damage to the data.

CLOUD COMPUTING

Cloud computing technology has grown exponentially over the last decade and presents a unique set of challenges that revolve around “...data replication, location transparency, and multi-tenancy” (U.S. Department of Commerce, 2020). The NIST Cloud Computing Forensic Science Working Group uncovered 65 specific challenges. Among those challenges are:

- Deletion of data in the cloud.
- Recovering overwritten data.
- Correlating evidence between providers is difficult.
- Being able to reconstruct virtual storage.
- Timestamp synchronization.
- Inconsistent log formatting between devices.
- Capturing network logs is difficult in cases where dynamic IPs are used.
- Interoperability issues between providers

To see the complete list, please see pages 26-52 of the NIST Cloud Computing Forensic Challenges report. (U.S. Department of Commerce, 2020)

EMERGING FILE SYSTEMS

Technology is advancing all the time and with that, new file systems are beginning to emerge. This is necessitating the need for digital forensics investigators to keep informed on the different aspects of each file system to know where to locate the data they are looking for, what information is accessible, and other related aspects. It also requires new digital forensics software to be developed and continuous updating of existing software applications. The following are just a few of the most recent file systems that are still being explored:

- [PVFS \(Parallel Virtual File System\)](#)
- [\(HDFS\) Hadoop Distributed File System](#)

CONCLUSION

Having a good understanding of different computer file systems is necessary for a digital forensic professional to be able to find the different types of data they need for their investigations. It is also important to stay abreast of emerging file systems.

Chapter 7 — Windows Registry Analysis

Learning Objectives

- Understand the function and importance of the Windows registry.
- Become familiar with effective registry analysis tools.
- Learn how malware can be detected in a registry.

Important Terms

registry hive
registry value
registry keys
registry subkeys

INTRODUCTION

The concept of a Windows registry has been around since 1992 when it replaced the “.ini” files of older Windows systems (Windows 3.0 and earlier). The “.ini” files were essentially files that set up the configuration of the computer. The Windows registry is a hierarchical database of system configuration settings that tell the operating system and applications “...what to do, where to put things, and how to react to certain stimulus” (Carvey, 2011, p. 15).

The function of a registry can provide a wealth of details about security incidents, troubleshooting system issues, and understanding application behavior. It can also be used to optimize system performance.

Nearly every action a computer user takes is recorded to the registry. That is, when a computer user attaches a device such as a USB flash drive to a USB port, the registry will store data about the device, its serial number and manufacturer, the port it was connected to, and timestamp information indicating when it was connected and disconnected.

Modifying the registry should only be done by someone that understands its structure. An inexperienced user who makes changes to their registry settings risks making their computer inoperable. Fortunately, Windows protects itself by only allowing access to the Registry Editor GUI (graphical user interface) if the user has Administrator privileges. However, if any unwanted changes are made, there is a way to recover the data, although not always. That process will be discussed later in this module.

When opening the Registry Editor GUI, you will see that the registry consists of five essential “hives” (Liang et al., 2023).

- HKEY_CURRENT_USER (HKCU)
 - Contains configuration information about the currently logged-in user; this includes the user’s folders, user-defined screen colors and Control Panel settings.
- HKEY_USERS (HKU)
 - Contains information about what users have logged onto the machine.
- HKEY_LOCAL_MACHINE (HKLM)
 - Contains configuration information specific to that machine rather than the user settings information.
- HKEY_CLASSES_ROOT (HKCR)
 - Contains information that ensures the correct program opens depending on the file you open.
- HKEY_CURRENT_CONFIG (HKCC)
 - Contains information about the hardware profile when the computer starts up.

Table 7-1 (below) shows hive locations that have the most useful information for digital forensics analysis and their associated Windows system file names. These hives can be found in the Windows file directory at *\\%SystemRoot%\System32\config folder and each user account folder*.

Table 7-1. Registry Hives and Associated Windows System File Names

Registry Hive	Supporting System Files
HKEY_CLASSES_ROOT*	
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav
HKEY_CURRENT_USER*	Ntuser.dat, Ntuser.dat.log
HKEY_LOCAL_MACHINE\Hardware*	
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System*	System, System.alt, System.log, System.sav
HKEY_USERS\DEFAULT	Default, Default.log, Default.sav

Source: <https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry-hives>

Note: Asterisked (*) items are volatile.

Just as RAM has an element of volatility, so do some portions of certain registry hives. In Table 7-1 above, volatile registry hive locations are marked with an asterisk (*). They are volatile in the sense that the hive files are written over whenever a computer is shut down and restarted. Therefore, it is imperative that a live image of the machine be done before it is powered down.

REGISTRY STRUCTURE

It is important to explain some important terminology related to the elements that make up the registry: **key**, **subkey**, **value**, **type**, and data.

Figure 7-1 shows the components of the registry editor. “The data [in the registry] is structured in a tree-like format. Each node in the tree is called a key. Each key can contain both subkeys and data entries called values.

To illustrate this concept in simpler terms, let’s say that you have a basket of washed clothes; we could equate that to what a hive is. Now these clothes can be sorted out by type such as shirts, pants, and underclothes; we could equate that to what a key is. Next, the shirts can be sorted into types of shirts such as T-shirts, dress shirts, polo shirts and uniform shirts; these would be considered subkeys. Now the T-shirts are sorted even further based on their composition (e.g. cotton, polyester, rayon, or acrylic) and those would be considered values.

Sometimes, the presence of a key is all the data that an application requires; other times, an application opens a key and uses the values associated with the key” (White et al., 2021). A value can be a string or multiple strings or binary data.

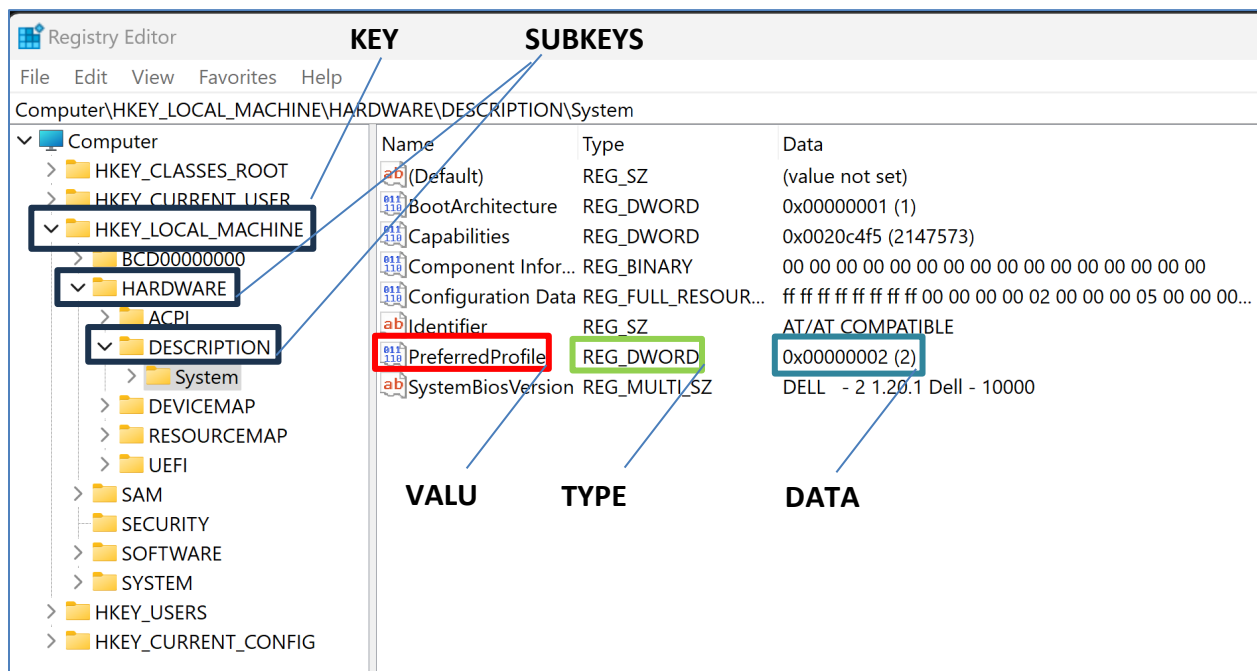


Figure 7- 1. Components of the Windows registry editor.

The 11 possible values available for “type” include:

- REG_SZ
- REG_DWORD
- REG_BINARY
- REG_DWORD_LITTLE_ENDIAN
- REG_DWORD_BIG_ENDIAN
- REG_EXPAND_SZ
- REG_LINK
- REG_MULTI_SZ
- REG_NONE
- REG_QWORD
- REG_QWORD_LITTLE_ENDIAN

REGISTRY ANALYSIS TOOLS

Table 7-2 (below) shows the options digital forensic professionals have for registry analysis tools. Windows has its own built-in tools but there are third-party tools that can be used as well. This is not an exhaustive list.

Table 7- 2. Resident Windows and Third-Party Registry Analysis Tools

Built-in	Third Party
Registry Editor (also known as regedit)	Registry Explorer
Reg.exe	RegRipper
	NirSoft's RegScanner

Selecting the best tool depends on what you are trying to accomplish or the data you are hoping to uncover.

Regedit is a command that is typed into the Windows search feature to open its resident Registry Editor. The Registry Editor allows you to create, manipulate, rename or delete registry keys, subkeys, values, and value data. It can also be used to import or export .REG files.

To start Registry Editor, type **run** in the Windows search box and then type **regedit** in the Run dialog box as shown in Figure 7-2 below.

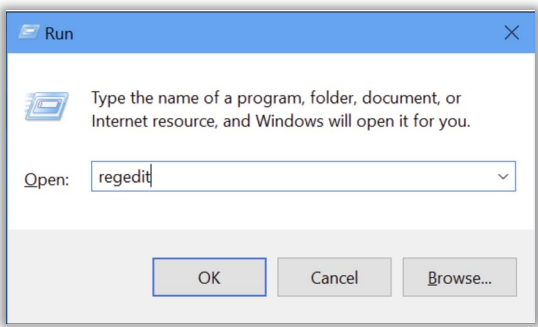


Figure 7- 2. Registry Editor dialog box.

A User Account Control (UAC) dialog box will appear asking if you want to open Registry Editor as an administrator. Click **Yes** and Registry Editor opens (Figure 7-3) to what you see below.

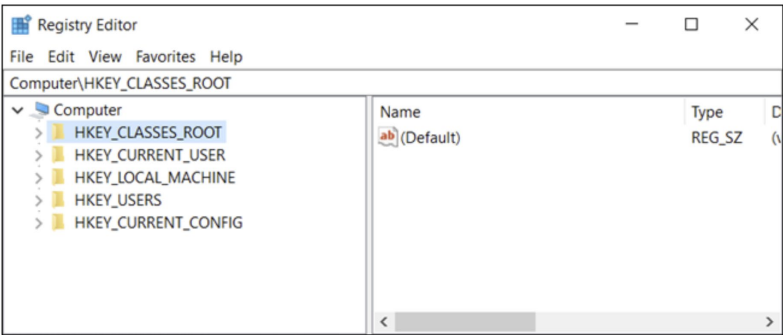


Figure 7-3. Registry Editor opening screen.

Another tool that can be used is **Reg.exe** which has the capability to set or remove permissions within the registry.

Nirsoft's RegScanner (Figure 7-4) "...is a small utility that allows you to scan the Registry, find the desired Registry values that match to the specified search criteria, and display them in one list...you can also export the found Registry values into a .reg file that can be used in RegEdit" (RegScanner V2.71, 2022).

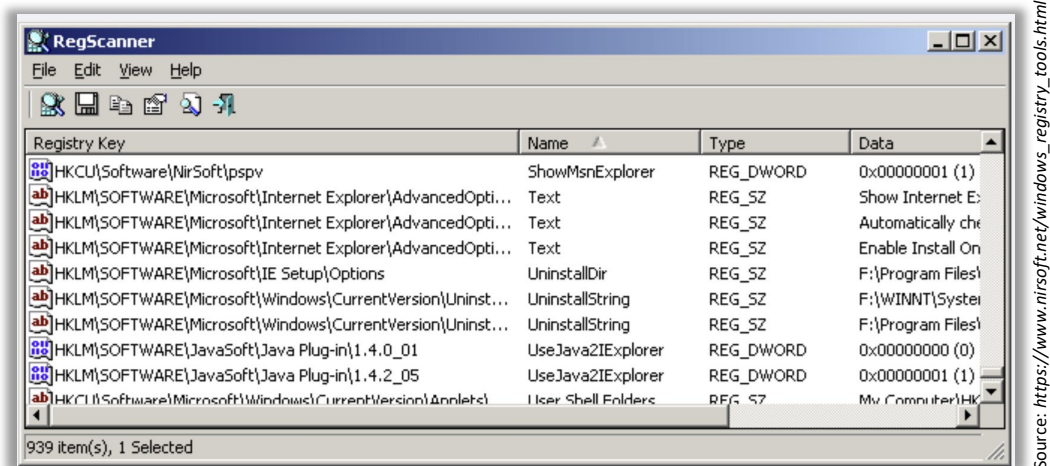


Figure 7-4. Sample output from NirSoft's RegScanner.

Registry Explorer (Figure 7-5) is a tool that functions like Registry Editor but has more capabilities. It was developed for the purpose of expanding the features of Windows Registry Editor since it had not been updated for several years. For example, it allows for key and advance searching; copying and pasting keys and values into different locations; and undoing and redoing actions. (Mills, 2021)



Figure 7-5. Sample output from Registry Explorer.

RegRipper is a tool that runs a registry file against a set of RegRipper search plugins and produces an output report (Figure 7-6). To see a complete list of the current RegRipper plugins go to <https://hexacorn.com/tools/3r.html>.

```

ComputerName = textbox
-----
ControlSet002\Control\Windows key, ShutdownTime value
ControlSet002\Control\Windows
LastWrite Time Mon Jan 19 23:03:52 2009 (UTC)
    ShutdownTime = Mon Jan 19 23:03:52 2009 (UTC)
-----
ShutdownCount
ControlSet002\Control\Watchdog\Display
LastWrite Time Mon Jan 19 23:03:52 2009 (UTC)
    ShutdownCount = 218
-----
TimeZoneInformation key
ControlSet002\Control\TimeZoneInformation
LastWrite Time Sun Nov  2 14:14:54 2008 (UTC)
    DaylightName -> Eastern Daylight Time
    StandardName -> Eastern Standard Time
    Bias -> 300 (5 hours)
    ActiveTimeBias -> 300 (5 hours)
-----
ControlSet002\Control\Terminal Server key, fDenyTSConnections value
LastWrite Time Fri Oct 24 20:53:51 2008 (UTC)
    fDenyTSConnections = 1
-----

```

Source: <https://www.sans.org/blog/regripper-ripping-registries-with-ease/>

Figure 7-6. Sample RegRipper report output.

In Table 7-7 below shows the common types of digital artifacts that can be found in the various hives within the registry. This is by no means an exhaustive list.

Artifact	Hive Location
Most recently used (MRU) list	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
Product and device ID values of any USB devices that have ever been connected to the system	HKEY_LOCAL_MACHINE\SYSTEM\controlset001\Enum\USBSTOR
Internet Explorer data	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TypedURLs
Product and device ID values of any devices that have been connected to the system	HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices
Last accessed applications	HKEY_CURRENT_USER\SOFTWARE\Microsoft\CurrentVersion\Search\RecentApps
Contains information about the network interfaces on the machine including assigned IP addresses, gateways, domains, DHCP leases	HKEY_LOCAL_MACHINE\SYSTEM\controlset00n\Services\Tcpip\Parameters\Interfaces\{INTERFACE ID}
Provides search terms used	HKEY_CURRENT_USER\SOFTWARE\Microsoft\SearchAssistant\ACMr\{5001, 5603, 5604, 5647}
Recent documents listing	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Artifact	Hive Location
Provides a list of most recently used audio and video files	HKEY_CURRENT_USER\SOFTWARE\Microsoft\MediaPlayer\Player\RecentFileList
Provides a list of the most recently accessed Adobe PDF files	HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\9.0\AVGeneral\cRecentFiles
Mapped network drives	HKEY_CURRENT_USER\SOFTWARE\Windows\CurrentVersion\Explorer\Map Network Drive MRU

Figure 7-7. Common types of digital artifacts that can be found in various hives within the Windows registry.

LEARNING ACTIVITY 7-1

Research on the Internet and locate three Windows artifacts and their corresponding hive locations. How might this information be useful in a digital forensic investigation?

WINDOWS REGISTRY AND MALWARE ANALYSIS

The registry can also be a useful repository of information when it comes to detecting malware. Malware has the capability of modifying the registry to remain undetectable. There are particular areas in the registry that are manipulated by malware than others. You may also notice services running on your computer that are not typical and those should be investigated as well.

LEARNING ACTIVITY 7-2

Running Windows Autoruns provides a thorough list of registry keys that are most susceptible to malware manipulation on your system. Autoruns covers over 30 different registry key sections (Grimes, 2017). The different tabs help sort the keys by function or application. By running this on a regular basis, anomalies are easier to detect.

Autoruns also has a feature to run all this output through VirusTotal.com. VirusTotal.com is a site that scans files, URLs, IP addresses, and domains for malware. This service “...runs every file hash against every participating antivirus software” (Grimes, 2017). This is the easiest way of detecting malware-infected registry keys.

1. Go to the Microsoft Sysinternals [Autoruns for Windows v14.1](#) webpage and use the link to download the Autoruns program. Extract the files into a folder you create.
2. Double-click on the .exe file for the type of system you are using (Figure 7- 8 below) and let it run.

Name	Status	Date modified	Type	Size
autoruns.chm	✓	7/1/2023 3:51 PM	Compiled HTML H...	25 KB
Autoruns.exe	✓	7/1/2023 3:51 PM	Application	1,742 KB
Autoruns64.exe	✓	7/1/2023 3:51 PM	Application	1,934 KB
Autoruns64a.exe	✓	7/1/2023 3:51 PM	Application	2,040 KB
autorunsc.exe	✓	7/1/2023 3:51 PM	Application	702 KB
autorunsc64.exe	✓	7/1/2023 3:51 PM	Application	785 KB
autorunsc64a.exe	✓	7/1/2023 3:51 PM	Application	808 KB
Eula.txt	✓	7/1/2023 3:51 PM	Text Document	8 KB

Figure 7- 8. List of Autoruns .exe files.

You should see output that looks similar to this:

Name	Description	Publisher	Image Path	Timestamp
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Wed Jun 28 14:00:59 20
Adobe Acrobat Synchronizer	Acrobat Collaboration Synchronizer 23.3	(Verified) Adobe Inc.	C:\Program Files\Adobe\Acrobat DC\Acrobat\AdobeCollabSync.exe	Wed Jun 14 15:40:30 20
CanvaAutoLaunch\AvailabilityCheckAgent	Canva	(Verified) Canva	C:\Users\zewsk\AppData\Local\Programs\Canva\Canva.exe	Sun Feb 5 17:59:54 202
GoogleChromeAutoLaunch_0ED248A133F4877B4F5C5221AB109EC	Google Chrome	(Verified) Google LLC	C:\Program Files\Google\Chrome\Application\chrome.exe	Fri Jun 23 23:57:47 202
GoogleDriveFS	Google Drive	(Verified) Google LLC	C:\Program Files\Google\Drive File Stream\77.0.3.0\GoogleDriveFS.exe	Wed Jun 28 14:00:42 20
MicrosoftEdgeAutoLaunch_80F1010DD80014760B711D091493D5C1	Microsoft Edge	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Thu Jun 29 02:04:16 202
NordVPN	NordVPN	(Verified) nordvpn s.a.	C:\Program Files\NordVPN\NordVPN.exe	Wed Jun 9 13:55:50 20
OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	C:\Program Files\Microsoft OneDrive\OneDrive.exe	Tue Jun 27 10:24:52 202
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Thu Jun 29 16:52:38 202
Acrobat Assistant 8.0	Acrobat Licensing Service	(Verified) Adobe Inc.	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrotray.exe	Wed Jun 14 15:40:24 20
AdobeGCInvoker-1.0	Adobe GC Invoker Utility	(Verified) Adobe Inc.	C:\Program Files (x86)\Common Files\Adobe\AdobeGCClient\AGCInvokerU...	Thu Jan 19 11:19:10 202
Bdagent	Bitdefender agent	(Verified) Bitdefender SRL	C:\Program Files\Bitdefender\Bitdefender Security\bdagent.exe	Sat May 27 13:41:29 20
BdVpnApp	Bitdefender Vpn App	(Verified) Bitdefender SRL	C:\Program Files\Bitdefender\Bitdefender VpnApp\BdVpnApp.exe	Thu Jan 12 00:08:31 202
RtkAudioService	Realtek HD Audio Universal Service	(Verified) Realtek Semiconductor C.	C:\WINDOWS\System32\DriverStore\FileRepository\realtek\realtek.inf_amd...	Mon Feb 20 11:26:24 2i
TechSmithSnagit	Snagit	(Verified) TechSmith Corporation	C:\Program Files\TechSmith\Snagit 2022\SnagitCapture.exe	Mon Feb 27 14:57:50 2i
WavesSvc	Waves MaxxAudio Service Application	(Verified) Waves Inc	C:\WINDOWS\System32\DriverStore\FileRepository\wavesapo10de.inf_am...	Wed Feb 15 21:32:50 2i
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				Sat May 7 00:25:14 202
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe	Tue May 9 19:15:26 20
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				Thu Jun 15 05:54:53 202
Google Chrome	Google Chrome Installer	(Verified) Google LLC	C:\Program Files\Google\Chrome\Application\114.0.5735.199\Installer\chr...	Thu Jun 29 00:11:25 202
Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\114.0.1823.67\Installer...	Sat Jul 1 06:22:57 2023
n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Sat May 7 00:20:30 202
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				Mon Oct 17 23:15:15 20
vmware-tray.exe	VMware Tray Process	(Verified) VMware, Inc.	C:\Program Files (x86)\VMware\VMware Workstation\vmware-tray.exe	Fri Feb 18 01:46:08 202
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				Thu Jun 15 05:54:53 202

Figure 7-9. Example of Sysinternals Autoruns program output.

5. Enable VirusTotal.com: Select it from the **Options** dropdown menu. Accept the Terms and Conditions and run the Autoruns program again by clicking on the VirusTotal button. (Figure 7-10)

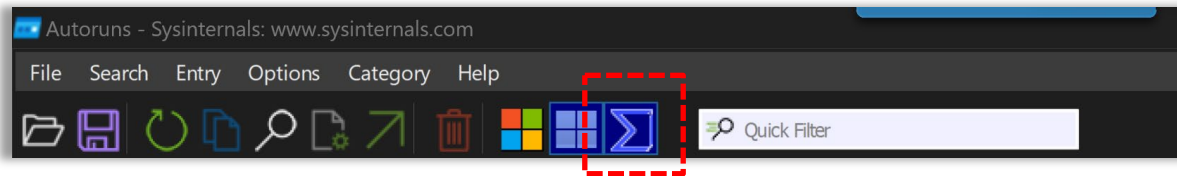


Figure 7-10. Location of VirusTotal button on Sysinternals Autoruns toolbar.

When clicking on the VirusTotal button (Figure 7-10) the registry files will pass through the service and point out potential issues with registry files by color coding them (Figure 7-11).

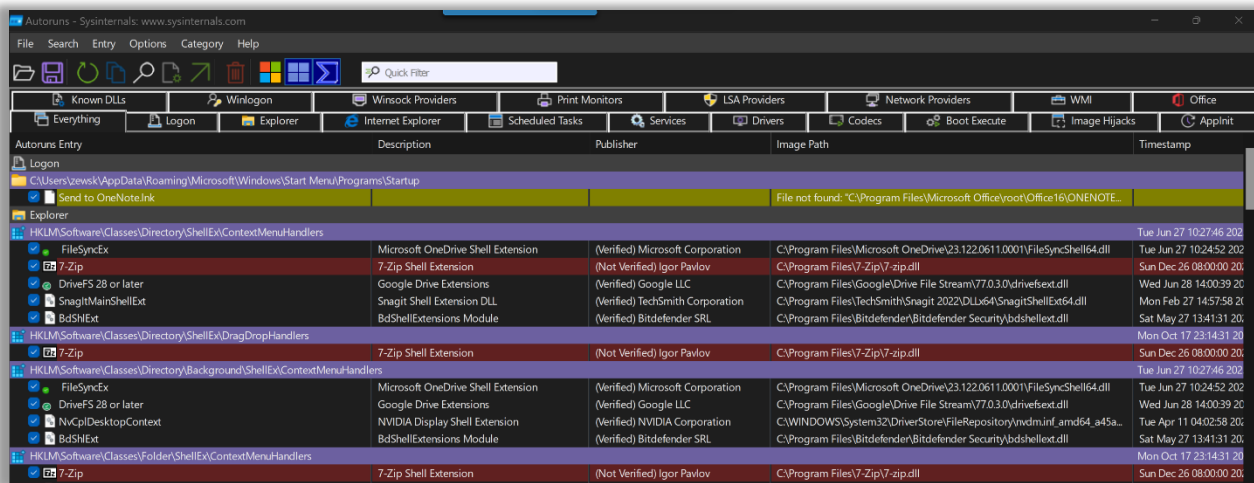


Figure 7- 11. View of registry file list with color-coded alerts.

6. Read [Autoruns for Windows 14.1](#).

RECOVERING DELETED REGISTRY FILES

Registry files can be recovered if they have been previously backed up.

LEARNING ACTIVITY 7-3

In this exercise you will create a registry backup file. For your knowledge, instructions are given on restoring a manual registry backup; you will not do this activity. The following instructions are directly from Microsoft's website and valid as of August 2023 for Windows 11, 10, and 8.1:

To back up the registry manually:

1. Select **Start**, type **regedit.exe** in the search box, and then press **Enter**. If you are prompted for an administrator password or for confirmation, type the password or provide confirmation.
2. In Registry Editor, locate and click the registry key or subkey that you want to back up.
3. Select **File > Export**.
4. In the Export Registry File dialog box, select the location to which you want to save the backup copy, and then type a name for the backup file in the File name field.
5. Select **Save**.

To restore a manual back up:

1. Select **Start**, type **regedit.exe**, and then press **Enter**. If you are prompted for an administrator password or for confirmation, type the password or provide confirmation.
2. In Registry Editor, click **File > Import**.
3. In the **Import Registry File** dialog box, select the location to which you saved the backup copy, select the backup file, and then click **Open**

CONCLUSION

The Windows registry is a plethora of information for digital forensics analysts. The registry is like a database in that it records all configuration settings and changes of a computer system. It can also be used to stop or start configurations for a system. The registry is organized into 5 general hives: HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, and HKEY_CURRENT_CONFIG. Within these hives are keys, subkeys, values, and types.

Registry files cannot be read like a text file. There are many applications that are capable of parsing registry files. In this module, five of the most reliable and popular applications were covered: Registry Editor, reg.exe, Registry Explorer, RegRipper, and RegScanner.

One must be careful when making changes to the registry as an incorrect configuration can render a computer system inoperable. It is always a good idea to regularly back up the registry so it can be restored if it becomes corrupt.

The Windows registry is also vulnerable to malware. As the registry is automatically loaded when booting up a computer, it is a popular location for threat actors to create backdoors or attack a system with malware. This is another area where registry backups can become a useful tool. From a cybersecurity perspective, conducting regular registry backups can help trace irregular or suspicious changes.

It is the responsibility of the digital forensics professional to stay on top of registry analysis techniques and latest applications. The Windows registry is a very meticulous, yet interesting concept that deserves further exploration. It is encouraged that learners new to digital forensics review the resources located in the appendix and to look for some of your own repositories for more information.

Chapter 8 — Windows File System Analysis

Learning Objectives:

- Understand the common file systems in use today.
- Compare and contrast different file systems.
- Learn about the different file-system-specific digital forensics processes.
- Know the challenges and future trends in file system forensics.

Important Terms

artifacts
partitions
file attributes
folder attributes
metadata

INTRODUCTION

A **file system** is a means of organizing data on a disk. In general, **partitions** (also known as “drives”) on a disk are broken down into directories, folders, and subfolders (Figure 8-1). What makes file systems different from each other is the manner in which files are formatted, characterized, and organized. As mentioned previously in Chapter 6 – Various File Systems, there are three categories of file systems: Windows, Mac, and Linux (Figure 8-2). This chapter will specifically focus on Windows files systems analysis and their artifacts, the nuggets of data unique to Windows. The registry is one category of Windows artifacts to investigate. Other artifacts to also examine are file attributes, folder attributes metadata, prefetch (.pf) files, event logs, and shortcuts (.lnk).

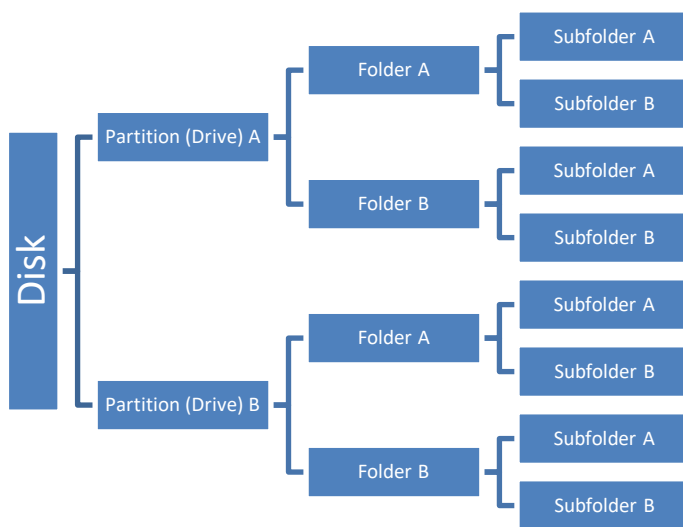


Figure 8-1. Simplified Windows file structure.

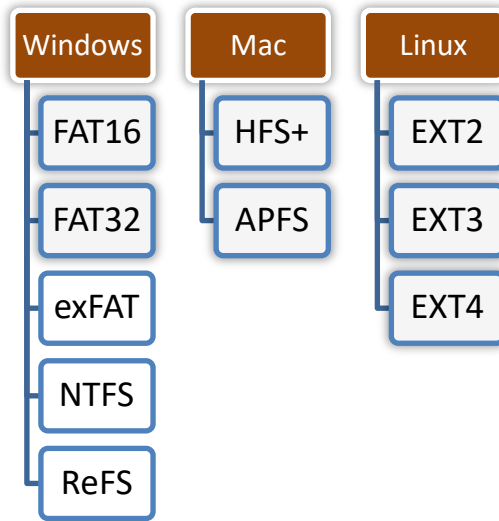


Figure 8- 2. General file system categories.

Chapter 6 covered two main Windows file systems, the File Allocation Table (FAT) and New Technology File System (NTFS). FAT had three iterations: FAT16, FAT32, and exFAT. However, there is a newer one that is gaining acceptance, called Resilient File System (ReFS). The differences between FAT, NTFS, and ReFS are shown in Table 8-1 below.

Table 8- 1. Windows File Systems Characteristics

File System	Advantages	Disadvantages
FAT16	Maximum partition size is 4 TB	Maximum file size is 2 GB
FAT32	- Compatible with USB flash drives and game consoles - Maximum partition size is 8 TB	- Maximum file size is 4 GB - No file permissions available
exFAT	- Compatible with USB flash drives - Compatible with NTFS drives - Compatible with MacOS and Linux - Compatible with PlayStation 4 & 5 - Compatible with Xbox X, S, and One - Maximum file size is 128 TB* - Maximum partition size is 128 TB*	- Incompatible with PlayStation 3 - Incompatible with Xbox 360
NTFS	- It is faster than FAT - Has integrated security features - Uses file journaling - Automatic corruption correction - Supports file encryption - Compatible with Xbox X, S, and One - Maximum file size is 256 TB* - Maximum partition size is 256 TB*	- Compatible with operating system Windows XP and newer - Macs cannot write to a NTFS-formatted drive - Incompatible with PlayStation consoles - Incompatible with Xbox 360 - Linux OS can only read NTFS files but not write them to an NTFS-formatted drive.

<i>File System</i>	<i>Advantages</i>	<i>Disadvantages</i>
ReFS	• Uses checksums for metadata and optionally for file data to detect data corruption. • Storage Spaces feature uses an alternate copy of the data that it has stored to automatically repair file corruption with no downtime. • In the instance that an alternate copy of the data does not exist, ReFS removes the corrupt data from the namespace without causing downtime. • Integrity scanner proactively and intermittently scans the data for corruption. If corruption is present, ReFS will automatically repair the corrupt data. • Maximum file size: 35 PB* • Maximum partition size is 35 PB*	• File system compression not available • File system encryption not available • No extended file attributes • No boot capability. • Not supported on removable media

*1 PB (Petabytes) = 1,000 TB (Terabytes)

WINDOWS FILE ATTRIBUTES

Understanding the concept of **file or folder attributes** is important. Examining a file's or folder's attributes provides extra information about its characteristics and behaviors. As shown in Figure 8-2 below, there are several file attribute types. However, the most common are:

- Read-only – File can be viewed but not modified.
- Hidden – Keeps the file from being shown in file explorer.
- System – File is used by the operating system and cannot be modified.
- Archive – File is identified as being modified and needs to be backed up.

One way this information can be useful to a digital forensic professional is knowing which file attributes can be changed and which cannot. For example, files can be made to be read only, hidden, or set as a system file. Changes to a file attribute can be made as a matter of preference to the user. However, from a digital forensics' perspective, it could be considered questionable behavior.

Table 8- 2. Windows File Attributes.

Value	Meaning
FILE_ATTRIBUTE_READONLY 0x00000001	A file or directory that is read-only. For a file, applications can read the file but cannot write to it or delete it. For a directory, applications cannot delete it, but applications can create and delete files from that directory.
FILE_ATTRIBUTE_HIDDEN 0x00000002	A file or directory that is hidden. Files and directories marked with this attribute do not appear in an ordinary directory listing.
FILE_ATTRIBUTE_SYSTEM 0x00000004	A file or directory that the operating system uses a part of or uses exclusively.
FILE_ATTRIBUTE_DIRECTORY 0x00000010	This item is a directory.
FILE_ATTRIBUTE_ARCHIVE 0x00000020	A file or directory that requires to be archived. Applications use this attribute to mark files for backup or removal.
FILE_ATTRIBUTE_NORMAL 0x00000080	A file that does not have other attributes set. This flag is used to clear all other flags by specifying it with no other flags set. This flag MUST be ignored if other flags are set.<161>
FILE_ATTRIBUTE_TEMPORARY 0x00000100	A file that is being used for temporary storage. The operating system can choose to store this file's data in memory rather than on mass storage, writing the data to mass storage only if data remains in the file when the file is closed.
FILE_ATTRIBUTE_SPARSE_FILE 0x00000200	A file that is a sparse file .
FILE_ATTRIBUTE_REPARSE_POINT 0x00000400	A file or directory that has an associated reparse point .
FILE_ATTRIBUTE_COMPRESSED 0x00000800	A file or directory that is compressed. For a file, all of the data in the file is compressed. For a directory, compression is the default for newly created files and subdirectories.
FILE_ATTRIBUTE_OFFLINE 0x00001000	The data in this file is not available immediately. This attribute indicates that the file data is physically moved to offline storage. This attribute is used by Remote Storage, which is hierarchical storage management software.
FILE_ATTRIBUTE_NOT_CONTENT_INDEXED 0x00002000	A file or directory that is not indexed by the content indexing service .

Value	Meaning
FILE_ATTRIBUTE_ENCRYPTED 0x00004000	A file or directory that is encrypted. For a file, all data streams in the file are encrypted. For a directory, encryption is the default for newly created files and subdirectories.
FILE_ATTRIBUTE_INTEGRITY_STREAM 0x00008000	A file or directory that is configured with integrity support. For a file, all data streams in the file have integrity support. For a directory, integrity support is the default for newly created files and subdirectories, unless the caller specifies otherwise. <162>
FILE_ATTRIBUTE_NO_SCRUB_DATA 0x00020000	A file or directory that is configured to be excluded from the data integrity scan. For a directory configured with FILE_ATTRIBUTE_NO_SCRUB_DATA, the default for newly created files and subdirectories is to inherit the FILE_ATTRIBUTE_NO_SCRUB_DATA attribute. <163>
FILE_ATTRIBUTE_RECALL_ON_OPEN 0x00040000	This attribute appears only in directory enumeration classes (FILE_DIRECTORY_INFORMATION, FILE_BOTH_DIR_INFORMATION, etc.). When this attribute is set, it means that the file or directory has no physical representation on the local system; the item is virtual. Opening the item will be more expensive than usual because it will cause at least some of the file or directory content to be fetched from a remote store. This attribute can only be set by kernel-mode components. This attribute is for use with hierarchical storage management software. <164>
FILE_ATTRIBUTE_PINNED 0x00080000	This attribute indicates user intent that the file or directory should be kept fully present locally even when not being actively accessed. This attribute is for use with hierarchical storage management software. <165>
FILE_ATTRIBUTE_UNPINNED 0x00100000	This attribute indicates that the file or directory should not be kept fully present locally except when being actively accessed. This attribute is for use with hierarchical storage management software. <166>
FILE_ATTRIBUTE_RECALL_ON_DATA_ACCESS 0x00400000	When this attribute is set, it means that the file or directory is not fully present locally. For a file this means that not all of its data is on local storage (for example, it may be sparse with some data still in remote storage). For a directory it means that some of the directory contents are being virtualized from another location. Reading the file or enumerating the directory will be more expensive than usual because it will cause at least some of the file or directory content to be fetched from a remote store. Only kernel-mode callers can set this attribute. This attribute is for use with hierarchical storage management software. <167>

Source: https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-fscc/ca28ec38-f155-4768-81d6-4bf8586fc9

WINDOWS FILE METADATA

In the simplest terms, file metadata is information about data. This is not the data itself such as text in a document or numbers in cells of an Excel spreadsheet. Table 8-3 below shows the different types of metadata a file or folder can have.

Table 8-3. Metadata Types

Metadata Type	Information Provided About File
Descriptive	title, abstract, author, keywords
Structural	types, versions, relationships, and other characteristics of digital materials
Administrative	type, permissions, and when and how it was created
Reference	contents and quality of statistical data
Statistical	processes that collect, process, or produce statistical data
Legal	creator, copyright holder, and public licensing

Source: <https://en.wikipedia.org/wiki/Metadata>

PREFETCH (.PF) FILES

The purpose of prefetch files is to store information necessary for executable files to run so that it takes less time for the program to start. For a digital forensic investigation, prefetch files can provide useful information about the programs a user ran on their computer. This includes the number of times a program is run, the additional files that were loaded, the prefetch version used, timestamps of the last time a program executed, and the file path where the program executed from. In the Windows file directory, prefetch files can be found at `C:\Windows\Prefetch\`.

WINDOWS SHORTCUTS (.LNK)

Windows offers a shortcuts feature to link or point to executable files, rather than navigating to the file to launch it. LNK is the file extension used for a shortcut file. LNK files contain information about when an executable is accessed, modified, and created. This can be useful when attempting to put a timeline of events together in an investigation.

WINDOWS EVENT LOGS

Any changes made to a computer or events that happen to the system are automatically recorded to event logs. This type of information can be useful to a digital forensics technician in that it shows activities that have been completed on the system such as threats against networks and systems; unauthorized logins; and can assist in troubleshooting specific software problems. Windows 10, for example, maintains three types of logs: event, security, and application (Figure 8- 2).

Table 8- 4. Types of Windows Event Logs.

Log Type	Information Recorded
System	Changes to hardware, device drivers, and all activities related to the machine itself
Security	Login and logoff activity for the operating system
Application	Application related events that are installed on the system

TOOLS FOR FILE SYSTEMS ANALYSIS

There are several tools that can be used to extract different types of Windows artifacts. Table 8- 5 shows a summary of what tools are currently available. However, this in no way is an exhaustive list. Some are paid tools and others are open-source (free) programs. Some of the tools are installed GUI-based programs and others are done via command line. Some of the tools may also be specific to certain operating systems.

Table 8- 5. Tools Used for File System Analysis.

Type of Digital Artifact	Windows File Path	Tool to use
Metadata from Recycle Bin files: \$I file contains contents of Recycle Bin before being permanently deleted	C:\\$Recycle.Bin\SID*\\$Ixxxxxx	\$I Parse
Recycle Bin: \$R file contains contents of deleted files in Recycle Bin	C:\\$Recycle.Bin\SID*\$Rxxxxxx	Autopsy
Remote Desktop Protocol Cache: processes bcache*.bmc and cache???.bin files	C:\Users\XXX\AppData\Local\Microsoft\Terminal Server Client\Cache	BMC-Tools
.lnk files: Windows shortcut files that point to other files or executables		LECcmd
Jump Lists: Information about recently accessed applications and files.	C:\Users\xxx\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations C:\Users\xxx\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations	JumpList Explorer
Prefetch Files: Application names, path, last execution timestamp, creation timestamp	C:\Windows\Prefetch\	WinPrefetchView
Analyze hard disks and smartphones		Autopsy
meta information from different types of files		Exif Tool
Linux-based file carving tool		Foremost
File system recovery tool for Windows and Linux		Scalpel

Table 8-6. Windows Error Reporting File Directory Locations.

Windows Error Reporting	C:\ProgramData\Microsoft\Windows\WER\ReportArchive C:\Users\XXX\AppData\Local\Microsoft\Windows\WER\ReportArchive C:\ProgramData\Microsoft\Windows\WER\ReportQueue C:\Users\XXX\AppData\Local\Microsoft\Windows\WER\ReportQueue
--------------------------------	--

Table 8-7. Open-Source Tools for Windows Digital Forensics Investigations.

Open Source Tool	Purpose
Magnet Encrypted Disk Detector	Checks for these encrypted drives: TrueCrypt, PGP®, VeraCrypt, Check Point related processes, SafeBoot, or Bitlocker®.
Magnet RAM Capture	Imaging tool designed to capture physical memory.
Wireshark	Network protocol analyzer
RAM Capturer	Extracts contents of computer's volatile memory.
Nmap	Scan IP addresses and ports in a network and detects installed applications.
NetworkMiner	Network sniffer that can capture or detect the operating system information, ports, sessions, hostnames of connected devices.
Autopsy	Used to analyze hard disks and smartphones
Forensic Investigator	Capable of VirusTotal and Metascan lookups; Base64, XOR, and HEX conversion.
HashMyFiles	Calculates SHA1 and MD5 hashes.
Crowd Response	Gathers system information for incident response.
Exif Tool	Reads, writes, and edits meta information from different types of files.
FAW (Forensic Acquisition of Websites)	Used to acquire web pages, images, HTML, source code of the web page.

CONCLUSION

There are several types of Windows artifacts that can be searched for in a digital investigation. Besides the registry, it is important to examine the directories within the file system. Windows, MacOS, and Linux are the most popular file systems. Within the Windows directory you can look for file attributes, metadata, prefetch (.pf) files, event logs, shortcuts (.lnk) and other relevant files. Several tools have been created to help gain access to or assist in reading the files.

Chapter 9 — Forensic Tools

Learning Objectives:

- Understand the factors involved in selecting digital forensics tools.
- Know the difference between open source and paid forensics software.
- Learn the basic components of a digital forensics laboratory.

Important Terms:

N/A

INTRODUCTION

Tools are at the heart of every digital forensic professional's investigation. As technology advances, new methods and approaches to accessing different types of digital artifacts are created out of necessity. The best tools to use can be a combination of hardware- and software-based equipment. Software-based tools can be paid or open-source. An open-source tool is an application or publicly accessible code designed through collaboration with others. This allows people with different skills and knowledge to create the best possible product and also keeps the code fresh.

A digital forensic laboratory houses all hardware and software tools and specialized equipment required to conduct effective investigations. The selection of tools is dependent on several factors, including budget, devices that will likely be analyzed, and the availability of facilities.

DESIGNING A DIGITAL FORENSICS LAB

Ultimately budget and available space are the main factors in designing a digital forensics laboratory., Secondary factors must also be considered such as: facilities, configuration, equipment, and software.

- **Facilities.** Aside from the size of the area, another major consideration is security. An effective access control system is necessary to maintain chain of custody. Data storage must also be secure and protected from physical damage.
- **Configuration.** Configuration has to do with the basic furnishing of the lab such as desktop area, bookcases, evidence safes or lockers, server stations, and storage shelves.
- **Equipment.** This depends on the operating systems that will be used, data storage requirements, and the type of forensic analysis that will be done. A basic list includes:
 - Forensic towers
 - Monitors
 - Uninterruptible Power Supplies (UPS)
 - Printers
 - Servers
 - Variety of device adapter and cable types

- NAS or other high-volume storage
- Mobile forensics kit
- Write blockers
- Digital cameras
- Computer hand tools

Whatever forensic tools are selected, it is best practice to have at least two tools of the same type. For example, if you use a hardware-based write protection device, there should also be a second one that could be used to validate the findings. Validation that these tools continue to work effectively is necessary.

Below is a list of recommended digital forensics tools for to consider when setting up an initial lab facility. This list is by no means an exhaustive catalog.

RECOMMENDED SOFTWARE

General Forensic Imaging and Analysis

[OpenText EnCase](#)
[Magnet Forensics Axion](#)
[Forensic Toolkit \(FTK\) by AccessData](#)
[XWays Forensics](#)
[Forensic Explorer \(FEX\)](#)

Mobile Device Forensics

[Cellebrite UFED4PC](#)
[MSAB XRY-XAMN](#)
[Paraben Electronic Evidence Examiner](#)
[Oxygen Forensics](#)
[SQLite Forensics Toolkit](#)
[Belkasoft](#)
[FinalMobile Forensics](#)
[Susteen Secure View](#)

Antivirus Software

[Bitdefender](#)
[Symantec](#)

Image File Viewing Software

[Magnet Axion](#)
[EnCase](#)
[Autopsy](#)

VLC Software

[VLC Media Player](#)

Registry Software

[Registry Explorer](#)
[RegRipper](#)

[NirSoft's RegScanner](#)

RECOMMENDED HARDWARE

Forensic Workstations

[Phantym product line](#)
[Digital Intelligence product line](#)
[Silicon Forensics product line](#)
[Forensic Store](#)

Forensic Imaging

[Atola TaskForce](#)

Cell Phone Forensic Workstations

[Silicon Forensics product line](#)

Write Blockers

Digital Intelligence [UltraKit v5](#)
 WiebeTech [Ultradock FUDv6](#)

Digital Camera

RF Shielding Device

[Ramsey STE3000](#)

Advanced Equipment

Teel Technologies [JTAG](#) (passcode bypass)
 Teel Technologies [SD Chip Reader Complete Kit](#)
 (chip reader kit)
[Atola Insight](#) (Forensic Data Recovery Tool)
[Atola TaskForce](#) (Forensic Imager)

[PC-3000](#) Data Recovery T

Data Storage

There are four options for digital forensics data storage: USB drives, Network Attached Storage (NAS), on-site data servers, and cloud storage. Table 9-1 below examines the advantages and disadvantages of the various data storage options.

Table 9-1. Data Storage Options: Advantages and Disadvantages

Storage Method*	Advantages	Disadvantages
USB drives and NAS	• Portability • Varied sizes • Cost effective • Easy to use	• Greater chance for hardware failure • Not as forensically sound as other storage methods
On-site server	• Permanent on-site storage • Typically more secure • More forensically sound than other storage methods • Redundant backups available	• High cost for implementation • Professional installation often required • Training required for all users
Cloud **	• Little to no cost to set up • Meets all federal laws and regulations* • Storage is off-site • Data security is the responsibility of the cloud provider • Training not required in most cases • Forensically sound environment • Unlimited storage	• No control over data security

Source: Lawrence et al., 2018

* For law enforcement, data security requirements must meet the following federal requirements: [Criminal Justice Information Security \(CJIS\)](#); [Federal Information Processing Standards \(FIPS\) Standard #197](#); [Health Insurance Portability and Accountability Act \(HIPPA\) Security Rule](#); [National Institute of Standards and Technology \(NIST\) SP 800-53 \(Rev. 5\)](#), and [SP 800-171](#).

** For cloud storage, additional requirements: [Federal Risk and Authorization Management Program \(FedRAMP\)](#) and [Department of Defense Cloud Computing Security Requirements Guidelines \(DoD SRG\)](#).

MISCELLANEOUS

- Faraday bags
- digital camera
- intake forms
- chain of custody paperwork
- evidence tape
- evidence envelopes
- removable media (CDs, DVDs, thumb drives)
- labels
- printer

LEARNING ACTIVITY 9-1

How would your ideal digital forensics lab be designed? Use the resources listed above and information from previous chapters to design a forensics laboratory suited for your current employer or favorite organization. For each component you include, provide your reasoning for the selection.

CONCLUSION

Many factors go into the selection of the hardware and software tools used in a digital forensics investigation. An organization's budget is usually the most influential element. Secondary, are the types of devices an organization intends to conduct digital forensics analyses on. Digital forensics analysts need to stay educated on new and updated hardware and software.

Chapter 10 — Incident Response

Learning Objectives:

- Learn about the Incident Life Cycle.
- Know what items to look for on a Windows system in an investigation.
- How to find suspicious processes on a Windows system.
- Learn about which Windows logs are useful for a digital forensics investigation.

Important Terms:

Indicators of compromise

INTRODUCTION

INCIDENT RESPONSE LIFE CYCLE

Cybersecurity incident response typically involves a systematic approach to effectively address and mitigate security breaches. While the exact steps may vary depending on the organization and the incident, the National Institute of Standards and Technology (NIST) (2012) has defined the following elements of the Incident Response Life Cycle: Preparation, Detection & Analysis, Containment, Eradication, Recovery, Post-Incident Activity (Figure 10-1).

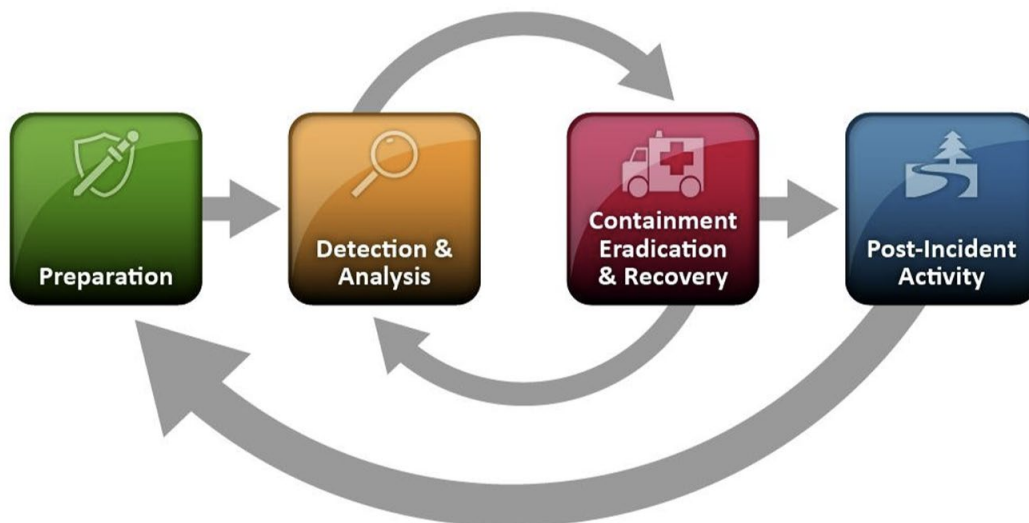


Figure 10- 1. NIST Incident Response Life Cycle.

Source: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

Preparation. This step involves establishing a well-defined incident response plan and assembling a team responsible for executing it. The plan should outline roles, responsibilities, communication protocols, and technical procedures to follow in case of an incident.

Detection & Analysis. Detecting and identifying cybersecurity incidents is critical. This step involves monitoring systems, networks, and logs for any suspicious activities, indicators of compromise (IOCs), or abnormal behavior that may indicate a security breach.

Containment. Once an incident is identified, it's essential to contain the situation to prevent further damage. This step may involve isolating affected systems, disconnecting from the network, or implementing temporary security measures to limit the incident's impact. Per Murdoch (2016), the digital forensics team needs to focus on obtaining data according to its volatility level (prior to disconnecting or shutting any devices down):

1. CPU, cache, registry, memory capture, processes/services;
2. Network routing tables, ARP cache, process table, and kernel statistics;
3. Main memory;
4. Temporary files and swap space;
5. Resident data on the hard disk (i.e., file system and slack space);
6. Data logged on a remote or central server;
7. Data on archival media.

Eradication. After containing the incident, the next step is to remove the cause of the breach, malware, or unauthorized access from the affected systems. This may involve patching vulnerabilities, removing malicious software, or taking other necessary actions to restore the system's integrity. From a digital forensics' perspective, this is the point at which analysis is done to define root cause.

Recovery. The recovery involves restoring the affected systems, networks, or data to their original functioning state. This is accomplished by restoring from backups, implementing security measures, and then verifying the integrity of the newly restored state.

Post-Incident Activity. After an incident is resolved, it is important to conduct a post-incident review. In this step, the incident is documented, areas of improvement are identified, security policies and procedures are updated, and lessons learned are communicated to the organization. The goal of this step is to use the incident as a means of improving future response.

INDICATORS OF COMPROMISE

Indicators of compromise are those characteristics that are signs that an attack is imminent. The following are examples (Murdoch, 2016):

- Unusual or unaccounted for outbound traffic and between networks;
- Abnormal privileged account use;
- Users logging in from multiple computers or IP addresses;
- Excessive failed login attempts (Windows event IDs 4625, 4771, and 4772);
- Database administrators running jobs they normally wouldn't;
- Abnormal increase in outbound web browser requests;

- Unusual Increase in web server queries;
- Application traffic doesn't coincide with the port information;
- Unplanned registry changes have been made;
- Increase in domain name requests, short TTL response times, packets that are larger than normal;
- UDP traffic followed by TCP traffic;
- Unexplainable files in odd locations;
- Large number of computer systems visiting the same website in a small window of time;
- Short bursts of traffic in every hour of the day;
- Excessively long URLs (> 6 slashes);
- Appearance of unexpected services installed on system; and
- Changes to user account permissions

WINDOWS DATA COLLECTION

Depending on the nature of the attack, you may need to gather any or all of the information about the system being investigated (Murdoch 2016):

- Prepare environment for collection.
- Collect physical memory data. Mandiant Redline and F-Response Tactical are excellent tools to use to collect memory data.
- Analyze volatile memory using the Volatility tool.
- Confirm operating system identity.
- Pull network information.
- Scan for hidden or terminated processes.
- Find and extract injected code.
- Capture live system state.
- Document system details.
- Network configuration and communication details.
- DNS information.
- MAC address
- Physical and logical NICs.
- Service information.
- Process information currently running.
- Process information at startup.
- Event logs.
- User and group information.
- Scheduled tasks.
- Find files for the specific timeframe for the incident being investigated.
- Collect disk image using FTK or other imager software.
- Collect supplemental system information.
- Patch/hotfix installation history.
- System manufacturer.
- List of installed software.
- Detect if an encryption file system is present.
- Verify system file integrity.
- Check most recently modified files.

FINDING WINDOWS SUSPICIOUS PROCESSES

Digital forensics professionals may need to extract the Windows processes that are running at a given time. For this kind of work, [Windows Process Explorer](#) (Mihaiuc et al., 2023) can be used to view processes on live machines or to have them pulled from an image of the device.

To understand what the abnormal processes are on a Windows machine, you need to know what processes you can expect to see. Some criteria include:

- Only one system can be seen.
- One instance of smss.exe running.
- One instance of Wininit.exe, services.exe, lsm.exe, and WinLogon.exe.
- Multiple taskhost.exe running by various users.
- One instance of explorer.exe per user logged in.

Figure 10-2 (below) presents evidence of the criteria above, highlighting processes with red dashed boxes:

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System	Susp...	188 K	82,300 K	172		
Registry		10,824 K	42,236 K	216		
System Idle Process	98.81	60 K	8 K	0		
System	< 0.01	132 K	33,644 K	4		
Interrupts	< 0.01	0 K	0 K		n/a Hardware Interrupts and DP...	
smss.exe		1,104 K	1,116 K	1076		
Memory Compression	< 0.01	3,748 K	1,623,336 K	5044		
csrss.exe	< 0.01	2,844 K	5,552 K	1624		
wininit.exe		1,508 K	5,588 K	1752		
services.exe	< 0.01	9,084 K	12,256 K	1824		
Lsalso.exe		2,288 K	3,768 K	1836		
lsass.exe	< 0.01	19,220 K	35,972 K	1860	Local Security Authority Pro...	Microsoft Corporation
fontdrvhost.exe		2,368 K	3,208 K	1104		
csrss.exe	< 0.01	3,764 K	7,108 K	1772		
winlogon.exe		2,644 K	49,104 K	1924		
fontdrvhost.exe		7,444 K	18,460 K	1096		
dwm.exe	< 0.01	1,135,172 K	233,924 K	2208		
GoogleCrashHandler.exe		3,412 K	1,084 K	5532		
GoogleCrashHandler64.exe		4,604 K	1,048 K	5440		
explorer.exe	< 0.01	324,184 K	289,236 K	17884	Windows Explorer	Microsoft Corporation

Figure 10- 2. Sample Windows Process Explorer output.

Indications of abnormal Windows processes can include the following:

- No visible icon or description.
- There's no company name or the company name is misspelled, all caps, or improper case.
- Software installed in the Windows directory or subdirectories.
- Processes that look like they are original Microsoft files but aren't in the directory they would typically be found.

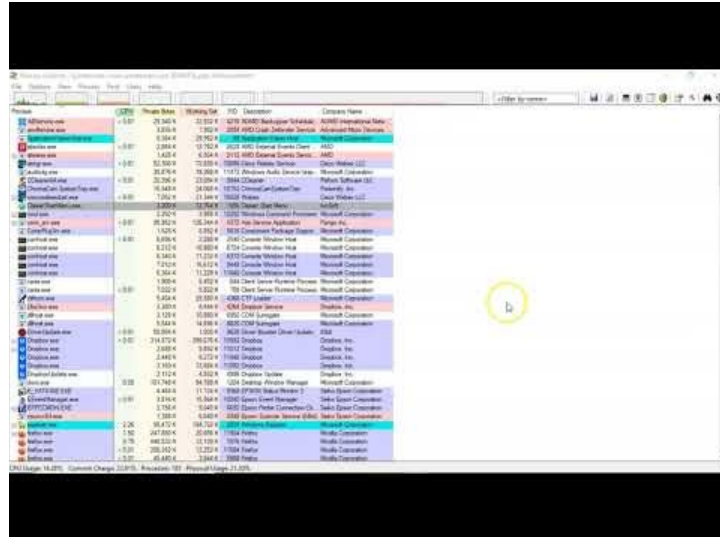
- Software with non-valid URLs in the process name.
- TCP and UDP endpoints that aren't associated with a service.
- Excessive number of compressed files.
- Files named something they're not.

LEARNING ACTIVITY 10-1

Watch [Overview of Sysinternals' Process Explorer](#)

Posted by Professor K

Duration: 17 mins. 40 secs.



LEARNING ACTIVITY 10-2

1. After watching the Overview of Sysinternals' Process Explorer video in Learning Activity 10-1, download and install [Process Explorer](#).
2. Open Process Explorer and find the following processes:
 - smss.exe
 - wininit.exe
 - services.exe
 - lsass.exe
 - winlogon.exe.
 - Multiple taskhost.exe running
 - explorer.exe for each user that is logged in

TIMELINE CONSTRUCTION

Murdoch (2016) provides a list of Windows logs that should be run during an incident (Table 10-1). Logs are at the crux of timeline construction. Knowing what events happened when is very useful in the Post Activities incident response life cycle. The chronology can help see where the failures may have occurred and find ways to keep the incident from reoccurring.

Table 10-1. Windows Logs Helpful for Incident Response.

LOG	FILE PATH
APPLICATION	%SystemRoot%\System32\Winevt\Logs\Application.evtx
FORWARDED EVENTS	%SystemRoot%\System32\Config\ForwardedEvents.evtx
SECURITY	%SystemRoot%\System32\Winevt\Logs\Security.evtx
SETUP	%SystemRoot%\System32\Winevt\Logs\Setup.evtx
DFS REPLICATION	%SystemRoot%\System32\Winevt\Logs\DfsReplication.evtx
DNS SERVER	%SystemRoot%\System32\Winevt\Logs\DNS Server.evtx
DNS SERVER	%SystemRoot%\System32\DNS\Dns.log
HARDWARE EVENTS	%SystemRoot%\System32\Winevt\Logs\HardwareEvents.evtx
IIS V6 AND EARLIER	C:\Windows\System32\LogFiles\W3SVC1
IIS V7 AND LATER	%SystemDrive%\inetpub\logs\LogFiles
FTP (WIN2012)	%SystemDrive%\inetpub\logs\LogFiles
IIS SMTP SERVICE	<SystemDrive>\Inetpub\Mailroot for the Badmail and Drop folder
SQL SERVER 2012	C:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\Log\ERRORLOG
SYSTEM CENTER 2012	C:\ProgramData\Microsoft System Center 2012\Orchestrator\ManagementService.exe\Logs

LEARNING FROM INCIDENTS

When the root cause of an incident is determined, it is a good idea to reflect on what was done well and determine what could be improved. Lambert (2022) provides guiding questions that can help find those opportunities for change:

- “How was this incident raised?”
- Could it have been identified earlier?
- Was this something you could have been alerted for?
- Did a customer notice it before we did?
- Were all internal and external stakeholders kept up to date at the right times with what was going on?
- Was it clear who was responsible for communication?
- Were the right people involved at the right moments?
- Did you find yourself in a “too many cooks” situation?
- Did it take a while for the relevant team to find out about the incident?”

LEARNING ACTIVITY 10-3

There are software tools (Table 10-2) that can be useful to identifying malicious traffic before it impacts a system or network. Choose 2 to 3 tools from the list below and create a table comparing their features.

Table 10- 2. Vulnerability Detection and Management Tools.

Tool	Purpose
<u>OpenVAS</u>	Vulnerability management software for finding security vulnerabilities before they can be exploited.
<u>Nessus</u>	Vulnerability management software for finding security vulnerabilities before they can be exploited.
<u>Nmap</u>	Open source software used for network discovery and security auditing, network inventory.
<u>Snort IDS</u>	Open source software used for defining and alerting malicious network activity
<u>Wireshark</u>	Open source software used for monitoring and analyzing network activity.

CONCLUSION

Incident response is critical to cybersecurity. The incident response cycle is important to a digital forensics analyst for the purpose of understanding their role in the process. Indicators of compromise are signs that a cybersecurity event is likely to happen. If an incident occurs, a digital forensics analyst can search in specific areas of a computer image to find evidence and help prepare a timeline for the incident response team to keep the same incident from happening again.

Chapter 11 — Introduction to Password Cracking

Learning Objectives:

- Understand what makes passwords complex.
- Learn about password cracking methodologies.
- Learn about the function of password salts.
- Learn about what tools can be used to decrypt passwords.
- Learn about what makes smartphones secure.

Important Terms:

password cracking
entropy
salts
data in motion
data at rest
password guessing

dictionary attack
brute force attack
credential stuffing
password spraying
password salts

INTRODUCTION

Password cracking is not just for hackers. It is also a very useful skill for a digital forensics analyst when it comes to accessing a password-protected drive or file. There are techniques and tools that can be leveraged to gain access to what could otherwise be considered an impossible task.

Cybersecurity efforts focus a lot on the strength of the password. Therefore, the start of a discussion about password cracking has to begin with what makes a password strong. Mathematically, the longer a password is, the greater the number of combinations a password could be (Chu, n.d.); this phenomenon is called entropy (Table 11-1).

For example, with a password of 8 numbers in length (no alphabetic characters or symbols), there are over 111 million possible combinations and that increases to 1.11 quadrillion combinations if the length of the password is increased to 15 numbers. However, with 1.11 quadrillion possible combinations, a password cracking application can still figure out the password in approximately 3 hours. (Chu, n.d.)

However, when the 26 letters of the alphabet are added-in with the numbers of 0 to 9, the number of 15-character combinations increases to 227 sextillion and will take an estimated 7 centuries to crack. Including common symbols with the letters of the alphabet and numbers of 0 to 9 yields 3.88 octillion password combinations and now would take approximately 12.34 million centuries to crack. (Chu, n.d.)

Table 11- 1. Entropy in Password Combinations.

	Numbers Only	Numbers & Letters	Numbers, Letters, & Common Symbols
4-Character Password	11,110	1,727,604	23,000,460
6-Character Password	1,111,110	2,238,876,116	109,505,194,890
8-Character Password	111,111,110	2,901,713,047,668	521,354,232,876,120
10-Character Password	11,111,111,110	3,760,620,109,779,060	2,482,167,502,723,212,150
15-Character Password	1.11 quadrillion	227.39 sextillion	3.88 octillion

Source: <https://dataoverhaulers.com/how-many-possible-passwords/>

With cybersecurity being top of mind, it's impossible for anyone to access anything digitally without a password. Rowe (2023) asserts that a single user can have as many as 100 passwords that they need to keep track of. Recalling 100 complex passwords, is quite a task considering the average person retains up to 7 items in their short-term memory (Mcleod & Evans, 2023).

This is a big problem from a cybersecurity perspective since writing passwords down is a taboo practice. Password requirements will continue to get complex and that will never change. To encourage users to follow good password hygiene, cybersecurity professionals have devised a number of mnemonic devices and software developers have created applications for secure password storage.

METHODOLOGIES

Password guessing. Random password guessing is rarely successful unless the password is something that is commonly used (e.g., passw0rd, qwerty789, or mermaidgirl) or a word that can be found in a dictionary. When hackers try to figure out what a password might be, the hacker will do reconnaissance; they look for related information about a person and make up password wordlists based on the person's favorite things, interests, friends, family members, pet names, or any other useful information they may find by trolling social media accounts or conducting general searches on the internet.

Dictionary attacks. Passwords can be cracked by using a dictionary attack tactic. This is largely using a password list that consists of common words that can be found in the dictionary. That list is then uploaded to a password cracking application that systematically goes through each word and checks against it.

Brute force attacks. This type of attack uses a list that is generated systematically by going through letter/number/symbol combinations until it finds a match.

Credential stuffing. Credential stuffing exploits the idea that a person will use the same password in other applications. The threat actor will harvest username and password combinations from lists found or sold on the internet and will try them in other attacks.

Password spraying. Password spraying is the opposite of the brute force technique. Instead of hitting several different passwords against a single user account, a single password is used against several different user accounts before moving to the next password combination.

PASSWORD SALTS

When a password is entered it automatically gets hashed and the hashed value is what is used by the system. A problem arises if two users happen to use the same password. To mitigate this issue, a password salt is used. **Salts** are snippets of random extra characters that are appended to the password. This changes the final hashed value of the password.

As shown in Figure 11-1, two people can have the exact same password but in the system, when a salt is added they are made to be different.

Person #1

Password	Salt	Salt Appended to Password	Resulting MD5 hash
HarleyQuinn	7!6j	HarleyQuinn7!6j	21e4e5993921483f8d891db29527d2

Person #2

Password	Salt	Salt Appended to Password	Resulting MD5 hash
HarleyQuinn	hI\$t	HarleyQuinnhI\$t	cf2ff07a8bae54e6486dbf80870cc0e9

Figure 11- 1. How a salt works.

PASSWORD CRACKING APPLICATIONS

Password cracking applications are critical to digital forensic investigations. [Passware](#) is the leader in password cracking and offers tools dedicated to different usage types:

- **Passware Kit** *Ultimate, Forensic, Mobile, Business, Lab Edition, Rainbow Tables for Windows, Rainbow Tables for Office Agent, Standard and Standard Plus;*
- **Windows Key** *Basic and Business;* and
- *Quickbooks Key, FileMaker Key, Excel Key, and Word Key.*

Other widely used password cracking applications include the following (Table 11-2):

Table 11- 2. Widely Used Password Cracking Tools.

Tool	Function
Hash Suite	Password hash crackers.
Hash Droid	Hash cracker for Android phones.
Hashcat	Advanced password recovery.
CrackStation	Online password hash cracker
Password Cracker	Cracks hidden passwords in Windows applications.
Aircrack-ng	Monitors, conducts attacks, tests, and cracks wireless network activity.

RainbowCrack	Cracks hashes using rainbow tables.
John the Ripper	Password cracking tool.
Cain & Abel	Sniffs the network to crack encrypted passwords using dictionary, brute-force and cryptanalysis attacks; records VoIP conversations; decodes scrambled passwords; reveals password boxes; uncovers cached passwords; and analyzes routing protocols.
ophCrack	Password cracker based on rainbow tables.

LEARNING ACTIVITY 11-1

Watch [Password Hacking Using Kali Linux](#)

Posted by John Hammond
Length: 24 mins. 22 secs.



SMARTPHONE SECURITY

As opposed to an Android phone, an Apple iPhone is extremely difficult, if not impossible, to crack. iPhones have several safeguards built in. There are two main types of data encryption when it comes to smartphones – one for data in motion and another for data at rest.

Encryption for **data in motion** provides “end to end” secure transmission of data between devices; it keeps application developers, phone manufacturers, and cellular service providers from being able to read messages. This type of encryption is the most difficult for law enforcement to crack. The encryption algorithm for the iPhone is created by the phone’s processor which, in turn, makes a complicated calculation to verify the code a user enters is correct (Guo, 2016). Therefore, only the iPhone knows what the passcode is and Apple cannot help in decrypting it.

Encryption for **data at rest** provides security for the data that resides on the smartphone itself. Law enforcement is more successful at finding tools to help decrypt mobile devices to recover text messages.



Specific barriers to successfully hacking into an iPhone include:

- Its self-preservation feature:
 - After five wrong guesses, you must wait a minute before you can try again.
 - After nine wrong guesses, you must wait an hour before you can try again.
 - The phone completely erases after ten incorrect tries.
- Older iPhones only had one passcode option – four digits – which allowed for over 11 thousand possibilities. Today's iPhones offer several options: 4-digits, 6-digits, custom digits, and alphanumeric. The possibilities of passcodes is increased exponentially.
- With the complexity of iPhone encryption, even law enforcement has difficulty getting into them which is becoming a cause for concern. More financially endowed law enforcement agencies can afford to spend hundreds of thousands of dollars on passcode cracking applications. However, this leaves smaller law enforcement agencies at a disadvantage.
- Despite the hefty price tag, decryption tools are not guaranteed success.

CONCLUSION

Password cracking is just as useful to digital forensics as it is to the digital analyst. The number of possible passwords is dependent on the number of characters and the type of characters (alpha, numeric, and/or symbols) used. The longer and more diverse the password is, the longer it will take to crack it. Using password salts increases the difficulty of cracking it.

Password cracking applications fall into one of the five basic password cracking methodologies: password guessing, dictionary attacks, brute force, password credentialing, and password spraying.

Cracking the codes on smartphones is becoming an issue for law enforcement. The encryption on these devices is highly complex but there are specialized tools available to assist in the effort.

Chapter 12 —

Introduction to Steganography

Learning Objectives:

- Learn about the history of steganography.
- Learn about the different types of steganography techniques.
- Learn how to convert between base 10 and base 2 numbers.
- Learn how to convert ASCII code to base 2.
- Learn about how least significant bit (LSB) insertion steganography works.
- Find out about recommended steganography tools.

Important Terms:

steganography	steganalysis
Least Significant Bit (LSB) insertion	base 2
spread spectrum	base 10
text steganography	byte
transfer domain techniques	

INTRODUCTION

Steganography is the art and science of hiding secret information within seemingly innocuous digital or physical objects. Unlike cryptography, which focuses on making information unintelligible through encryption, steganography aims to keep the existence of the information itself a secret.

Steganography can be traced back to ancient civilizations, where secret messages were hidden in various ways. One of the earliest documented instances is from around 440 BC when the Greek historian Herodotus mentioned in his Histories how a message was tattooed on a slave's shaved head, hidden beneath regrown hair, to communicate covert information.

In the era of the Roman Empire, steganography techniques were employed to hide messages in wax tablets, wooden tablets, and other forms of written communication. By the Middle Ages, techniques involved encoding messages into seemingly ordinary objects, such as invisible inks, hidden compartments, or variations in the arrangement of letters in a text. The greatest advancements, however, were seen during World War I and World War II as it was extremely important to keep messages from being readable by the enemy. It wasn't until the development of computers, that the digital version of steganography that we see today was realized.

The primary goal of steganography is to embed hidden data in such a way that it remains undetected by an observer, making it a form of security through obscurity. By concealing data within other files or media, steganography allows for covert communication and protection of sensitive information.

Steganography has a long history and has been used in various forms throughout different eras. In ancient times, secret messages were hidden within wax tablets or written in invisible ink. In modern times, with the widespread use of digital media, steganography has evolved to hide information within digital files such as images, audio, video, and even executable files.

DIGITAL STEGANOGRAPHY TECHNIQUES

There are several techniques used in digital steganography:

Least Significant Bit (LSB) Insertion. This method involves replacing the least significant bits of pixels in an image or audio file with secret data. Since changing the least significant bits don't significantly alter the appearance or sound of the media, the change is often imperceptible to the human eye or ear.

Spread Spectrum. In this technique, secret data is distributed across the entire frequency spectrum of an audio signal, making it hard to detect without knowing the exact spread spectrum key. Direct Sequence Spread Spectrum (DSSS) is a category of wideband techniques. This includes Frequency Hopping Spread Spectrum (FHSS) and Time Hopping Spread Spectrum (THSS). The specifics of these methods are beyond the scope of an introductory lesson on spread spectrum steganography techniques.

Text Steganography. Concealing information within text documents by applying various techniques like invisible character encoding, modified spacing, or even using synonyms to convey the hidden message.

Transform Domain Techniques. Hiding data in the frequency or wavelet domain of an image or audio file using mathematical transformations like Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT). "The DCT is in a class of mathematical operations that includes the well-known Fast Fourier Transform (FFT), as well as many others. The basic purpose of these operations is to take a signal and transform it from one type of representation to another" (J. Williams, lecture, n.d.).

Payload Embedding. This technique involves embedding malware (e.g., a rootkit) into a file. Often hackers will do this and then post it to a website where others download it. When opened it installs the malware. In the case of a rootkit, opening the file would install a backdoor that allows the hacker to gain control of the system it is installed on. Other examples of payload-related malware include:

- **NetTraveler** (Global Research and Analysis Team, 2013) (Axel F, 2016). "NetTraveler uses a side-loading technique. The payloads use the clean, signed executable fsguidll.exe (F-secure GUI component) to sideload fslapi.dll or the clean, signed executable RasTls.exe to sideload rastls.dll" (J. Williams, lecture, n.d.).
- **Zberp** (CyberWire, now N2K Cyber, 2017). "The Trojan disguises the configuration code in an image file through steganography. [Zberp] enables cyber criminals to grab basic information about the infected computer, including the Computer name, IP and more. It can take screen shots and send them to the attacker. It steals data submitted in HTTP forms, user SSL certificates and even FTP and POP account credentials. The Zberp Trojan also includes optional features that enable Web injections, dynamic Web injections, MITB/MITM attacks and VNC/RDP connections" (J. Williams, lecture, n.d.).
- **Shamoon** (Myrtus 0x0, 2019) (Albano & Kessem, 2017). Shamoon is implemented in stages. It starts with a spear phishing email that has a link or attachment (typically a Word document). Once the enclosed link is clicked or attachment is opened, PowerShell executes communication with threat actor. The threat actor works to get information about the network infrastructure, credentials, and critical systems and then uses that knowledge to deploy the Shamoon malware which disables systems and writes over drives.

- **ZeusVM (aka KinS)** (malwarebreakdown, 2017) (Segura, 2014). The threat actor resides in the browser and harvests personal and financial information that is used to conduct online activities as the victim.

If steganography is used for hiding data within digital files, then **steganalysis** is the process of detecting and recovering the hidden information from suspected steganographic content. Steganography and steganalysis often engage in a cat-and-mouse game, with steganography techniques becoming increasingly sophisticated to avoid detection by steganalysis methods.

While steganography has legitimate applications, such as covert communication and watermarking, it can also be misused for malicious purposes, such as concealing malware or facilitating cybercrime. As a result, steganography poses both challenges and opportunities in the fields of security, digital forensics, and data protection.

LEARNING ACTIVITY 12-1

Watch [Conceal Secret Messages or Data Through Steganography with Steghide \[Tutorial\]](#)

Posted by Null Byte

Duration: 9 mins. 28 secs.

- OR -

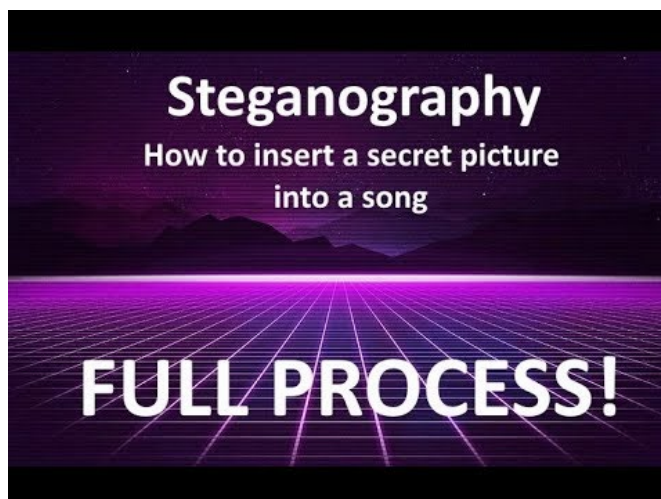
Read [Steganography: How to Hide Secret Data Inside an Image or Audio File in Seconds « Null Byte :: WonderHowTo.](#)



LEARNING ACTIVITY 12-2

Watch [How To Insert Secret Picture Into a Song \(Steganography\)](#) by RedBlue Labs

Duration: 7 mins. 16 secs.



FOUNDATION OF BINARY MATH

The least significant bit (LSB) is the lowest-order bit in a binary representation of a number. In binary, decimal numbers are expressed using only two digits: 0 and 1; this is also known as **base 2**. A decimal number is what we use in everyday basic mathematics; it also known as **base 10**.

Each digit in a binary number is called a **bit**. The position of each bit in a binary number carries a different weight (Table 12-1). The rightmost bit is considered the least significant bit because its weight compared to the other bits is the smallest.

Table 12-1. Binary Conversion Table.

1	2	3	4	5	6	7	8	← Digit position
128	64	32	16	8	4	2	1	← Bit position weight

Table 12-2. Example of Decimal to Binary Conversion.

1	2	3	4	5	6	7	8	← Digit position
128	64	32	16	8	4	2	1	← Bit position weight
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	← Exponential value
0	0	1	1	0	1	1	1	Example: 55 in decimal

When converting a decimal (base 10) number to a binary (base 2) number the goal is to get to zero, as demonstrated in the example (Table 12-3) below:

Table 12-3. Decimal-to-Binary Conversion Step by Step.

Step #	Value	Explanation
0	55	Start with the decimal number 55 that will be converted to binary.
1	55	The first digit position has a weight of 128 . The value 55 is less than 128 . Therefore, a zero (0) is entered in the first digit position. The value remains as 55 .
2	55	The second digit position has a weight of 64 . The value 55 is less than 64 . Therefore, a zero (0) is entered in the second digit position. The value remains at 55 .
3	-32 = 23	The third digit position has a weight of 32 . The value 55 is larger than 32 . Therefore, a 1 is entered in the third digit position. Subtracting 32 from 55 results in a new value: 23 .
4	-16 = 7	The fourth digit position has a weight of 16 . The value 23 is larger than 16 . Therefore, a 1 is entered in the fourth digit position. Subtracting 16 from 23 results in a new value: 7 .
5	7	The fifth digit position has a weight of 8 . The value 7 is less than 8 . Therefore, a zero (0) is entered in the fifth digit position. The value remains at 7 .
6	-4 = 3	The sixth digit position has a weight of 4 . The value 7 is larger than 4 . Therefore, a 1 is entered in the sixth digit position. Subtracting 4 from 7 results in a new value: 3 .
7	-2 = 1	The seventh digit position has a weight of 2 . The value 3 is larger than 2 . Therefore, a 1 is entered in the seventh position. Subtracting 2 from 3 results in a new value: 1 .

8	-1 = 0	The eighth digit position has a weight of 1 . The number 1 is larger than or equal to the value of 1 . Therefore, a 1 is entered in the eighth position. Subtracting 1 from 1 results in a new value: 0 .
9		Reading the digits from left to right, the binary representation of 55 is 00110111 .

To verify the binary value is correct, add the weights for each of the 1s in the binary number. Remember, the weights are based on the digit positions. In this example, there are “1” values in the third, fourth, sixth, seventh, and eighth positions (Table 12-4).

Table 12- 4. Binary 'on' Positions and Values.

1	2	3	4	5	6	7	8	← Digit position
128	64	32	16	8	4	2	1	← Bit position weight
0	0	1	1	0	1	1	1	<i>Example:</i> 55 in decimal

Adding the weights in each of the digit positions that have a “1” binary value equal 55 (Table 12-5).

Table 12-5. Binary Proof.

Position	Exponential Value	Weight
3	$2^5 = 32$	32
4	$2^4 = 16$	16
6	$2^2 = 4$	4
7	$2^1 = 2$	2
8	$2^0 = 1$	1
	TOTAL:	55

In the example above, the binary number is "**00110111**". The least significant bit is the rightmost bit, which has a value of 1 in this case. The weight of the least significant bit is $2^0 = 1$. The bit to its left has a weight of $2^1 = 2$, the next one has $2^2 = 4$, and so on. The leftmost bit, also known as the most significant bit (MSB), has the highest weight. A string of eight bits is called a **byte**.

Changing the least significant bit in a number will have the smallest impact on the value of the number. For example, if we change the least significant bit in the binary number "**00110111**" from 1 to 0, we get "**00110110**," which represents the decimal number 54. The change from 55 to 54 is minimal compared to changing other more significant bits in the number.

LEARNING ACTIVITY 12-3

Convert decimal numbers to binary:

1. Choose five numbers between 1 and 256 and convert them to binary. Show your work.
2. Identify the decimal value for each of the following binary numbers:
 - a. 10000111
 - b. 11011110
 - c. 00101110
 - d. 11001001
 - e. 10010010

THE ASCII TABLE

The American Standard Code for Information Interchange (ASCII) table (Table 12-6) consists of numerical representations of letters and numbers. A decimal and hexadecimal value is assigned to each uppercase letter (65 through 90), each lowercase letter (97 through 122), various symbols, and other characters.

Table 12- 6. Simplified ASCII Table.

Letter	ASCII Value
A	65
B	66
C	67
D	68
E	69
F	70
G	71
H	72
I	73
J	74
K	75
L	76
M	77

Letter	ASCII Value
N	78
O	79
P	80
Q	81
R	82
S	83
T	84
U	85
V	86
W	87
X	88
Y	89
Z	90

Letter	ASCII Value
a	97
b	98
c	99
d	100
e	101
f	102
g	103
h	104
i	105
j	106
k	107
l	108
m	109

Letter	ASCII Value
n	110
o	111
p	112
q	113
r	114
s	115
t	116
u	117
v	118
w	119
x	120
y	121
z	122

LEARNING ACTIVITY 12-4

In this exercise you will convert ASCII to binary.

Complete the table below following these steps:

1. Choose three words.
2. Determine the ASCII value for each letter of the word.
3. Determine the binary value for each ASCII value.

Word	ASCII Values for Each Letter	Binary Value for Each ASCII Value

LEAST SIGNIFICANT BIT (LSB) INSERTION STEGANOGRAPHY

Where binary and the ASCII table intersect is with the LSB insertion steganography technique.

The LSB has the least impact on the overall value of the number (e.g., 54 vs. 55). In LSB steganography, the idea is to replace the least significant bit of some or all of the pixels in an image (or the least significant bits of audio samples) with the bits of the secret message.

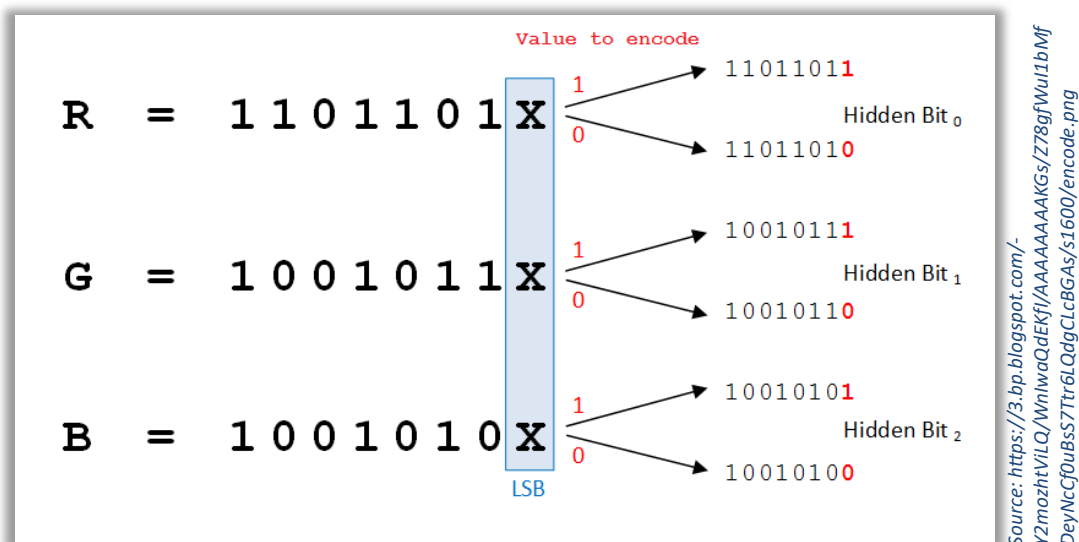


Figure 12-1. Altering a pixel's color value to hide a message.

This method is based on the fact that altering the least significant bit of a pixel's color value, as shown in Figure 12-1, is usually not noticeable to the human eye or ear.

Longer messages start to impinge into the second most right bit and that is where modifications to the image start to become noticeable visually and audibly.

The general steps in LSB insertion steganography are:

1. **Image selection.** Choose a cover image in which you want to hide the secret message.
2. **Convert the message to binary.** Convert the secret message (e.g., text, image, or any other data) into binary format.
3. **LSB replacement.** For each pixel in the image, replace the least significant bits of the color channels (typically Red, Green, and Blue in the case of RGB images) with the corresponding bits of the binary message. The number of LSBs used for hiding the message will determine the capacity and the invisibility of the hidden message.
4. **Message length and metadata.** Optionally, include the length of the secret message in the stego image metadata, so you know how many bits need to be extracted during the decoding process.
5. **Save stego image.** Save the modified image (stego image) with the hidden message.

The receiver of the stego image extracts the hidden message by reversing the steps.

1. **LSB Extraction.** For each pixel in the stego image, extract the least significant bits of the color channels.
2. **Combine Bits.** Concatenate the extracted bits to reconstruct the binary representation of the hidden message.
3. **Convert Binary to Message.** Convert the binary representation back into the original secret message.

Below is an example of an image that has been modified through LSB steganography:

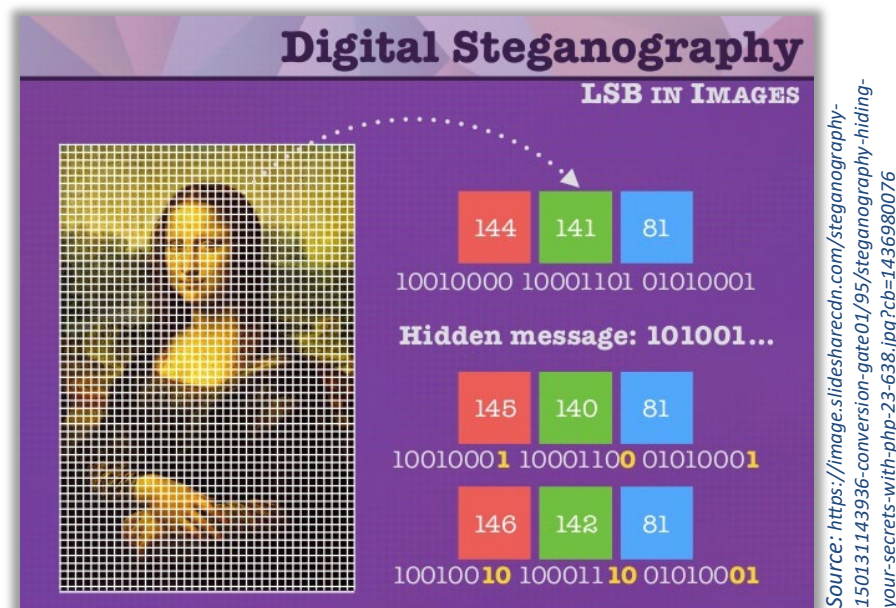


Figure 12- 2. LSB steganography in images.

Figure 12-2 contains an image of the Mona Lisa. The grid on top of the image is a representation of the pixels of the image. Each pixel is made up of a red, green, and blue component. A number value is assigned to each component signifying each color's intensity. In the example above, the pixel is made up of red (R) 144, green (G) 141, and blue (B) 81. Each of these numbers is then converted to binary.

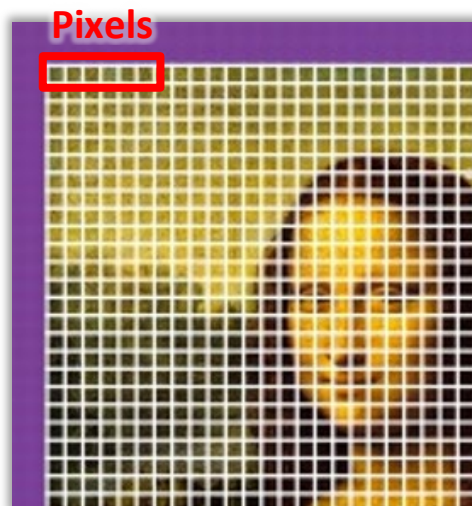


Figure 12-3. Pixels 1 through 6 from example.

To hide a message, each alphanumeric character is assigned its ASCII value. The value for each character is then converted to binary. Next, each bit in each binary number is placed into the least significant bit of each pixel.

Let's take the message LMK (let me know) as an example:

Table 12-7. Converting an ASCII Character to Binary.

Character	L	M	K
ASCII Value	76	77	75
Binary Value	01001100	01001101	01001011

Table 12-8. Converting a Color Value to Binary

	R	G	B
Color Value	144	141	81
Binary Value*	10010000	10001101	01010001

The red digit shown in Table 12-8 above is the least significant bit. This bit will be replaced with the binary value of each character in the secret message.

Start with the first letter (L) of the secret message. The binary digits for the letter L (shown in light blue in Table 12-7) are **0 1 0 0 1 1 0 0**.

When the binary values for the letters L, M, and K are placed next to each other from left to right, it looks like this (Figure 12-4):

L M K

01001100 01001101 01001011



010011000100110101001011

Figure 12-4. Binary values of L, M, and K concatenated.

The least significant bit is substituted with the message's binary digits in sequential order from left to right (Table 12-9).

Table 12- 9. Substitution of the least significant bit.

Pixel #		RGB Color Values Converted to Binary	Binary Digit of Secret Message	Binary Value with LSB Substituted with Secret Message
1	R	10010000	0	10010000
	G	10001101	1	10001101
	B	01010001	0	01010000
2	R	10001111	0	10001110
	G	11011101	1	11011101
	B	00100000	1	00100001
3	R	01100100	0	01100100
	G	01011000	0	01011000
	B	01000100	0	01000100
4	R	01001100	1	01001101
	G	10000111	0	10000110
	B	11011110	0	11011110
5	R	00101110	1	00101111
	G	11001001	1	11001001
	B	10010010	0	10010010
6	R	10011001	1	10011001
	G	01001101	0	01001100
	B	00100101	1	00100101

STEGANOGRAPHY TOOLS

There are several open-source (unpaid) steganography tools available to digital forensics analysts as seen in Table 12-10 below:

Table 12- 10. *Steganography Tools by Function.*

Tool	Function
<u>Xiao Steganography</u>	• Hides secret files in BMP images or WAV files • Can only decode BMP or WAV with embedded files that were produced with Xiao Steganography software.
<u>Image Steganography</u>	• Hides text messages or files inside an image file. • Can only decode a stego image file that was produced with Image Steganography software.
<u>Steghide</u>	• Hides secret files in an image or audio file. • Command line tool • Application is Windows 32-bit
<u>Crypture</u>	• Hides very small amounts of data inside a BMP image file. • Command line tool • Does not require installation
<u>SteganographX Plus</u>	• Hides very small amounts of data inside a BMP image file. • Command line tool • Does not require installation. • Can only decode a stego image file that was produced with SteganographX Plus.
<u>rsteg</u>	• Hides textual data inside an image • Can only decode a stego image file that was produced with SteganographX Plus.
<u>SSuite Picse!</u>	• Hides text inside an image file. • Windows 32- and 64-bit • Portable. Requires no installation. • Uses an image file as the key to open the stego file.
<u>OpenStego</u>	• Hides message file in an image file (BMP, GIF, JPEG, JPG, PNG and WBMP) • Uses a password to encrypt data along with hiding the message within the image file. • Windows

CONCLUSION

It is important to understand that LSB insertion is a basic and relatively easy steganographic technique. It offers limited security, and advanced steganalysis methods can detect hidden information in many cases. More sophisticated steganographic techniques may be used for higher levels of security and robustness.

Keep in mind that while steganography can be a fun to explore, it should always be used responsibly and ethically.

Chapter 13 — Introduction to Cryptocurrency

Learning Objectives:

- Understand the concept of cryptocurrency.
- Learn about the role of blockchains.
- Learn how different cryptocurrencies are purchased.
- Understand the different types of cryptocurrencies.

Important Terms:

fiat currency	centralized digital currency
cryptocurrency	decentralized digital
crypto exchange	miner
crypto wallet	currency
satoshi	proof of work
blockchain	node
hot wallet	Ethereum blockchain
cold wallet	smart contract protocol
closed virtual currency	ether
closed loop virtual currency	

INTRODUCTION

Cryptocurrency is a digital currency that can take different forms and is becoming an increasingly popular way to make purchases. Three cryptocurrencies (Bitcoin, Litecoin, and Ethereum) alone transact around 1.5 million transactions, and over \$12 Billion USD each day. Now take those numbers and multiply that by the 9,000+ different cryptocurrencies that are in circulation today and the numbers are staggering. (Ashford, 2023) Below is a simplified version of the Bitcoin transaction process:

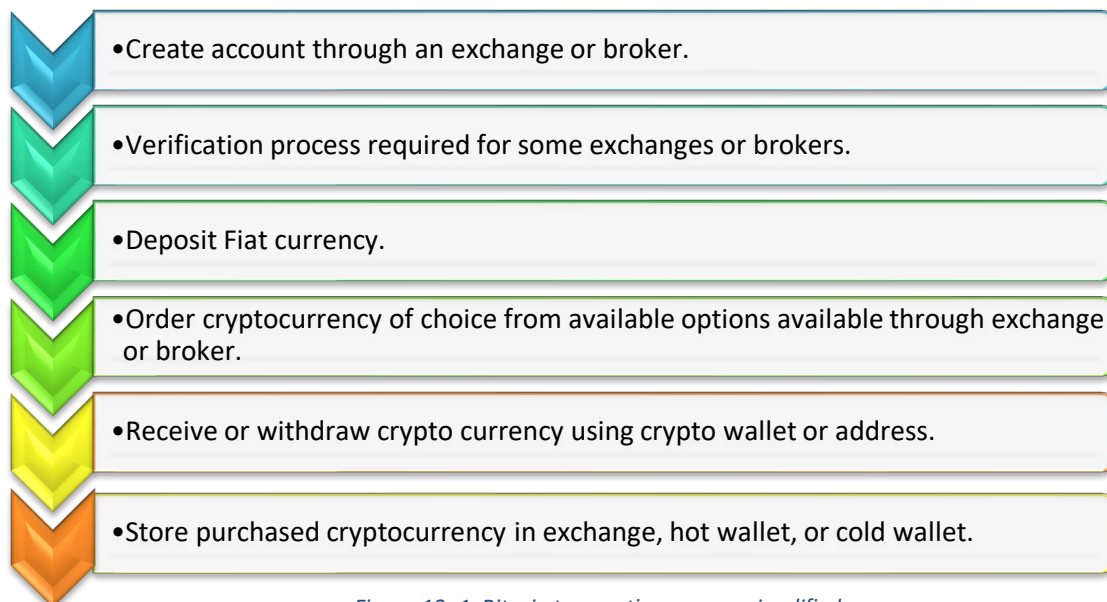


Figure 13- 1. Bitcoin transaction process simplified.

U.S. CURRENCY AND CRYPTOCURRENCY

Fiat money or currency is another term for *legal tender*, the paper and coin money that is controlled by a government such as U.S. dollars or the Euros used by the countries in the European Union. It is a term used to distinguish it from cryptocurrency. Whereas, the values of fiat money are defined by its respective government, cryptocurrency is digital currency that is not controlled by any bank.

Cryptocurrency is also known as digital money, electronic money, or cybercash; its currency is exclusively in electronic form. Cryptocurrency can be stored on an exchange (also known as a software wallet) or in a **crypto wallet**. There are two types of crypto wallets: hot and cold. A **hot wallet** is connected to the internet and a **cold wallet** is not, but you need a hot wallet to download Bitcoin to a cold wallet. A hot wallet refers to conducting transactions via the internet using a tablet, smartphone, or computer. A cold wallet is an independent piece of hardware that is used to conduct transactions.

CENTRALIZED VS. DECENTRALIZED DIGITAL CURRENCY

Digital currencies fall into one of two types: centralized and decentralized.

Centralized digital currencies are those that can be exchanged electronically between debit or credit cards using electronic funds transfer (EFT) or at point of sale (POS). Its value comes from the authority that issues the digital currency. Examples of this type are Venmo, Google Wallet, and ApplePay.

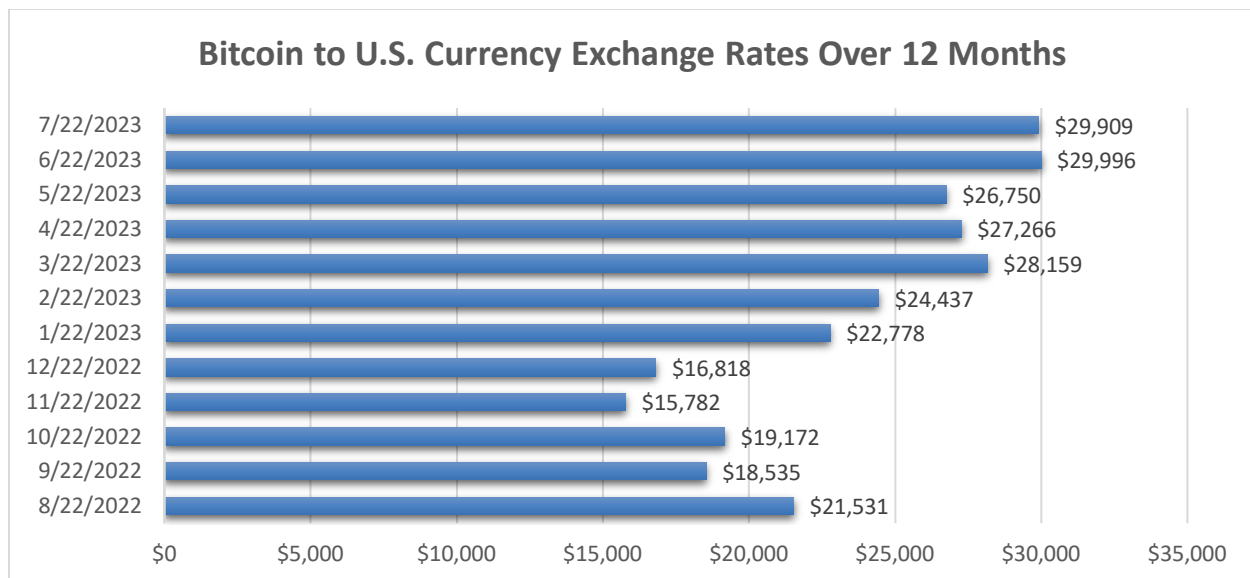
Decentralized digital currencies gain their value from the people who use it. It is not managed through banks or third-party companies to exist.

CRYPTO EXCHANGES

Crypto exchanges are the different routes cryptocurrency can be traded. There are three types of exchanges: retail, peer-to-peer, and decentralized. Rosen (2023) highlights the following as the best crypto exchanges available in 2023:

Bittrex Global	bitFlyer
Coinbase	Gemini
Bitfinex	Kraken
Bitstamp	Crypto.com
Binance	

The overall exchange rate of crypto currency can be highly volatile. For example, on July 22, 2023, the exchange rate for bitcoin to U.S. currency was 1 BTC = \$29,909. However, on November 22, 2022 its rate was \$15,782 (Figure 13-2). Just as stocks can be bought or sold in fractions of a whole, it is common for the sale or purchase of Bitcoin as well.



*Figure 13-2. Bitcoin exchange rates over 12-month period.
Source: [Yahoo Finance](#)*

The denominations between U.S. currency and Bitcoin are also strikingly different. While the smallest denomination of U.S. currency is one cent, the smallest unit of Bitcoin is a hundred millionth of one Bitcoin which is called **satoshi** (named after the creator of Bitcoin, Satoshi Nakamoto).

WHAT IS A BLOCKCHAIN?

“Bitcoin is powered by open-source code known as blockchain, which creates a shared public history of transactions organized into “blocks” that are “chained” together to prevent tampering. This technology creates a permanent record of each transaction, and it provides a way for every Bitcoin user to operate with the same understanding of who owns what” (Voigt et al., 2023).

Blockchain can be compared to an accountant’s ledger where you record all the money you spend. Each page in the ledger is analogous to a block and a ledger with pages full of transactions is like a blockchain. The entire ledger is distributed among the computers (also known as **nodes**) of the people who have transactions listed in the book and whenever it is updated, everyone gets the updated version. Conducting a transaction requires a crypto address and each blockchain has its own addressing system. Bitcoin addresses, for example, are 27 to 34 alphanumeric characters and begin with 1, 3, or bc1. Ethereum uses 40 hexadecimal characters and begins with “0x”.

BITCOIN BLOCKCHAIN

When a Bitcoin transaction is generated, it is not immediately added to the blockchain. The transaction is transmitted to the Bitcoin network through peer-to-peer nodes. Each available Bitcoin node will verify the transaction by confirming certain data such as the version, size, date, input, and output. After the transaction successfully passes verification by a node, the transaction is placed inside that node’s

“mempool” (memory pool). A **mempool** is similar to a holding area where unconfirmed or pending Bitcoin transactions are held before they are added to a block and incorporated into the blockchain. (J. Williams, lecture, n.d.)

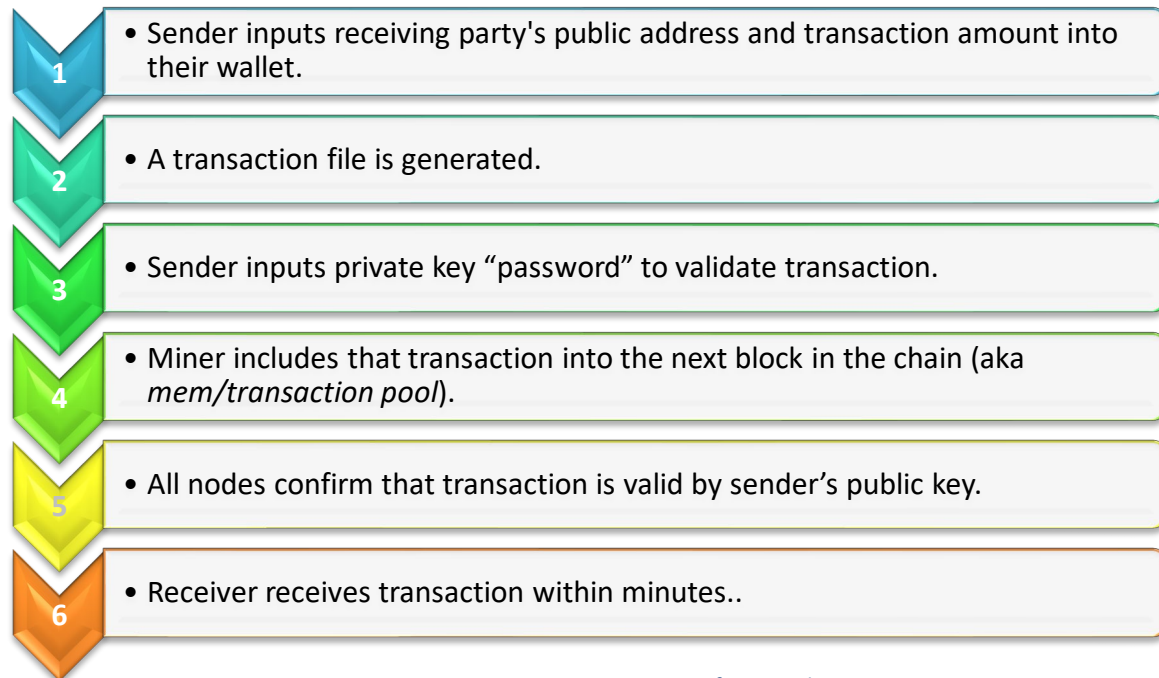


Figure 13-3. Bitcoin transaction process, from sender to receiver.

Each computer in the blockchain is called a miner. A **miner** node is connected to a cryptocurrency network and works to solve a random mathematical puzzle. The work to find the solution to the puzzle results in a block of cryptocurrency being created and added to the blockchain ledger. The miner can then sell the cryptocurrency earned for profit which is typically used to recoup the costs of the mining process.

TRANSACTION VALIDATION

There are two validation techniques to ensure that cryptocurrency transactions are legitimate: proof of work and proof of stake.

Proof of Work is a validation technique that verifies cryptocurrency transactions before they are committed to the blockchain. Due to the amount of processing, it can take an average of 10 minutes or more for a transaction to be verified, this is because as the blockchain increases in size, so does the amount of computing time and the energy required to process it. This technique does not require providing cryptocurrency as collateral such as the proof of stake technique does. (Ashford, 2023)

“Rather than requiring a network of miners racing to solve a puzzle, Proof of Stake requires a robust network of participants who are literally invested in the success of the enterprise” (J. Williams, lecture, n.d.). **Proof of Stake** is a validation technique where the number of transactions a stakeholder can verify is proportionate to the amount of cryptocurrency they are willing to deposit into the staking pool. The more cryptocurrency deposited by a stakeholder who wishes to mine, the greater the chances that

stakeholder may have to participate in the validation process. All participating stakeholders are rewarded with ETH (Ethereum) currency proportionate to the stake they committed.

The stakeholder who contributes the most cryptocurrency wins the opportunity to validate blocks of transactions. The runners-up are tasked with making sure the block is accurate (also referred to as attestation). When the number of attestations has reached its threshold, the block is then committed to the blockchain. The efficiency of this process results in approximately 3,000 transactions per second. (Ashford, 2023)

ETHEREUM BLOCKCHAIN

Ethereum (ETH) blockchain is a decentralized blockchain just as Bitcoin is, but processes transactions in a different way. Ethereum blockchain specifically uses **smart contract protocol**. The purpose of the smart contract protocol is the automation of the execution of agreements. If the terms of a smart contract are met, the transaction executes automatically. No intermediary is necessary. “Everything from financial tools and games to complex databases are already running on the Ethereum blockchain” (J. Williams, lecture, n.d.). A unit of ETH is called ether.

Transactions on the Ethereum network uses a currency denomination called ETH to pay the network to execute smart contracts. These fees are called gas. The price of gas varies depending on how busy the network is.

NON-FUNGIBLE TOKENS

Non-fungible tokens (NFT) are a special kind of crypto asset. Each token is unique, cannot be divided into smaller units, and is created to be scarce. In fact, NFTs are “...built using [ERC-721](#) and [ERC-1155](#) standards, allowing creators to issue unique crypto assets via smart contract” (J. Williams, lecture, n.d.). They are like certificates of authenticity for digital artifacts such as gaming “skins” (i.e., digital apparel for SIMs characters) or virtual real estate. A smart contract is used to embed the digital file into the blockchain which then becomes a non-fungible token.

Figure 13-4 shows just how easy it is to create your own NFT. To start, you must have currency deposited into a cryptocurrency wallet such as Metamask, Coinbase Wallet, WalletConnect, Fortmatic, etc. Next, join an NFT marketplace like [OpenSea](#) or [Enjin Marketplace](#) and connect the cryptocurrency wallet to the chosen marketplace account. Then create the image, video, audio, or 3D model you want to use to make your NFT, ensuring that its size is smaller than 100MB; OpenSea.io is a NFT marketplace that currently supports the following file formats: JPG, PNG, GIF, SVG, MP4, WEBM, MP3, WAV, OGG, GLB, and GLTF (Non-Fungible Token, n.d.). The last step in the process is to select the blockchain that you want to mint the NFT on.



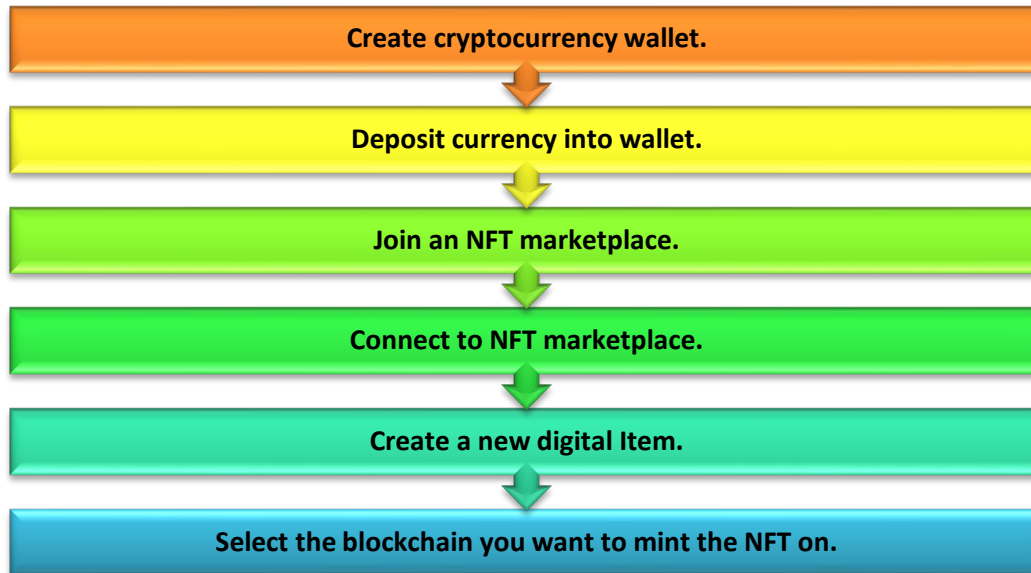


Figure 13-4. The NFT creation process.

CLOSED VIRTUAL CURRENCY

Closed virtual currency is a currency that exists in a controlled, private ecosystem; it cannot be used as legal tender. A **closed-loop virtual currency** is an electronic payment card or single purpose card that can only be used to make purchases from a single company. The card will have the company's logo and will not have a credit card processing logo (e.g., Visa, MasterCard, Discover). Examples of virtual currencies include frequent flyer miles, loyalty points, hotel rewards, in-world gaming tokens, and video arcade tokens.

ROLE OF DIGITAL FORENSICS IN CRYPTOCURRENCY

With the increased use of cryptocurrency, investigations in this realm are becoming more prominent. As we have learned earlier, every cryptocurrency transaction is saved as part of a blockchain and, therefore, transactions cannot be altered, and integrity is maintained.

"All cryptocurrency transactions start and end inside a cryptocurrency address or wallet. Addresses are similar to bank-account numbers and contain a balance and history of transactions undertaken in the past" (Rubin & Rega, 2021).

There are certain digital artifacts to look for when focusing on cases involving fraud or financial transactions:

- In a digital forensics investigation, finding crypto wallet addresses is of particular interest; accessing a crypto wallet requires a password or "seed phrase", making finding passwords very lucrative to a threat actor.
- Examination of the web browser history may uncover activities related to cryptocurrency transactions.
- Email and chat applications could expose communications about fraudulent or questionable cryptocurrency transactions.

“As noteworthy addresses and transactions are identified, blockchain explorers are valuable tools to explore the blockchain itself and track the flow of funds from one wallet to another” (Rubin & Rega, 2021).

CONCLUSION

The use of cryptocurrency is growing at an exponential rate. Similar to a stock exchange, there is a cryptocurrency exchange. Digital currency can be centralized or decentralized. Cryptocurrency is committed to a blockchain that acts as a digital ledger. Non-fungible tokens and closed virtual currency are different types of digital currency. In a digital forensics investigation, it is important to know what cryptocurrency digital artifacts look like in the event they come up in an analysis

.

Chapter 14 — Introduction to Memory Forensics

Learning Objectives:

- Understand the concept and importance of memory forensics.
- Learn how to capture computer memory.
- Get a brief introduction to memory for virtual machines, Windows, Linux, and Mac operating systems.

Important Terms

random access memory (RAM)	southbridge
central processing unit (CPU)	CPU register
computer busses	file system
memory controller	hypervisor
cache	kernel
memory management unit (MMU)	Executable and Linkable
northbridge	Format (ELF)
	strings

INTRODUCTION

Every action performed by the operating system or a computer's applications modifies a computer's memory. Digital artifacts such as running processes, open network connections, executed commands, disk encryption keys, passwords, chat messages, unencrypted e-mail messages or documents, and non-cacheable internet history are only a small part of what can be found in computer memory. But it can also contain malicious code of a virus. Several tools can be useful for obtaining and analyzing memory. The most notable of them all is an open-source tool called Volatility.

For a digital forensic analyst, the contents of a computer's memory can assist in correlating seemingly disconnected digital evidence and also corroborate evidence found on disk. In addition, it can be helpful for possibly locating password information to access encrypted drives.

COMPUTER MEMORY CONCEPTS

The foundation of conducting memory forensics activities requires an understanding of how memory works and understanding important terminology. To start, the functionality of devices connected to a computer relies upon both hardware and software. In the context of computer memory, it starts with the circuit board (Figure 14-2) and operating system.

The **random-access memory** (RAM) (Figure 14-1) temporarily stores code and data that the CPU actively uses such as executed programs and their associated data. Windows encryption supports password caching and key files in memory. In addition, master keys must remain in RAM while a disk volume is mounted. In the case of a fully encrypted partition, Windows caches any accessed files for a short period of time into memory. RAM is categorized as volatile memory because once the computer is powered down, any data stored in memory can be written over at the next boot. Since RAM itself requires power

for the data in the various memory registers to remain accessible. Keeping the RAM powered is then essential to keep these types of digital artifacts in memory.

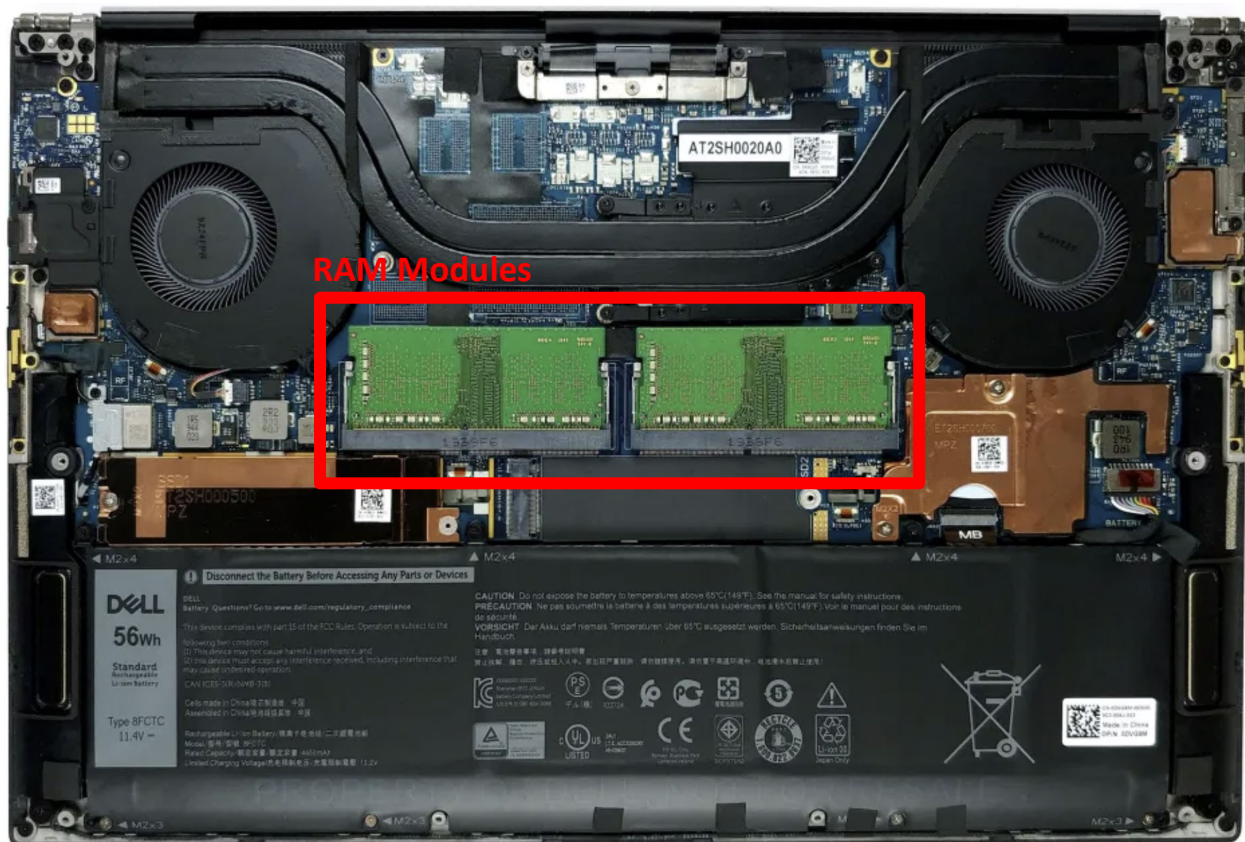


Figure 14-1. Dell XPS 15 9510 with back cover removed.

Source: [Gaur Open](#)

The **central processing unit (CPU)** (Figure 14-2, p. 108) executes programs and accesses the main memory to get and execute its instructions to process the data. CPU architecture is another phrase for describing the programming of a CPU. A CPU can have a 32-bit or 64-bit architecture. A CPU with a 32-bit or 64-bit architecture supports features such as virtual memory, paging, privilege levels, and segmentation.

CPUs have **registers** which are extremely fast memory cells that the CPU uses for temporary storage while instructions, logical and arithmetic operations are being processed. The processor core for a 32-bit CPU has 32-bit registers. The processor core for a 64-bit CPU has 64-bit registers.

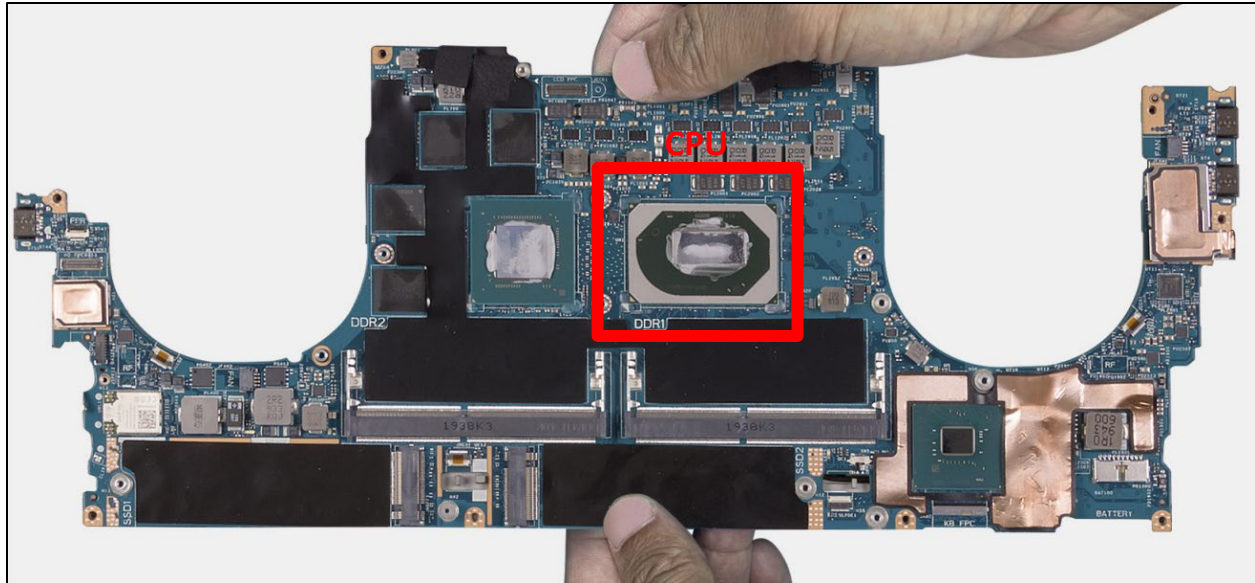


Figure 14- 2. Dell XPS 15 9510 laptop circuit board.
Source: [Dell XPS 15 9510 Service Manual](#)

Other components of memory that are good to know include:

- **Computer buses.** These are communication channels found on the motherboard.
- **Cache.** A cache is a placeholder for additional memory storage.
- **Memory management unit (MMU).** The MMU helps the CPU find where the data it needs is stored.
- **Memory controller.** The memory controller manages communication with the main memory. For example, it leverages the difference between a charged and discharged state of a capacitor to store a bit of data. This requires the capacitor to be periodically refreshed to maintain the memory. In modern day computers, the memory controller is integrated with the CPU.
- **Process.** A process is an instance of a program executing in memory; when a program executes, it is given a unique process ID (PID). A digital forensic analyst may examine process IDs that are suspect.

In older computers the circuit board had a northbridge and southbridge. The **northbridge**, also called a memory controller hub, is the part of the circuit board that the CPU and physical RAM is connected to. The **southbridge** is the secondary memory controller that any devices connected to the computer use; it also shares the northbridge to access the computer's main memory and the CPU.

THE OPERATING SYSTEM & MEMORY

"The **kernel** is a computer program at the core of a computer's operating system and generally has complete control over everything in the system.[1] It is the portion of the operating system code that is always resident in memory [2] and facilitates interactions between hardware and software components. A full kernel controls all hardware resources (e.g., I/O, memory, cryptography) via device drivers, arbitrates conflicts between processes concerning such resources, and optimizes the utilization of common resources (e.g., CPU and cache usage, file systems, and network sockets). On most systems, the kernel is one of the first programs loaded on startup (after the bootloader). It handles the rest of startup

as well as memory, peripherals, and input/output (I/O) requests from software, translating them into data-processing instructions for the central processing unit" (Kernel (operating, 2023)).

The operating system is software that manages a computer's hardware and software resources. It also provides services to computer programs. Within the structure of an operating system is the file system. The **file system** is an organizational structure similar to the old-school paper filing system and without it, a computer's storage device would be a big chunk of data stored line after line after line and be unreadable by the operating system.

Device drivers are small programs that help devices installed on a computer to communicate with the motherboard.

RISKS TO MEMORY ACQUISITION

The act of acquiring the memory from a computer system can lead to system instability and can corrupt or change the evidence itself. Therefore, memory acquisition is a careful decision to be made by the digital forensic analyst, as well as the acquisition method.

If collecting evidence from a suspect computer that is still running, it is important to do this while the suspect is online or logged in. This allows the digital analyst to access the suspect's login session, find information about connections to the cloud or remote data storage, and see the unencrypted documents the suspect is viewing.

If dumping memory to an external storage device connected to the computer, a digital forensic analyst must keep the following guidelines in mind prior to acquiring data from a disk or RAM:

- Never attach the same removable media to more than one possibly infected computer to avoid spreading the infection while you are gathering evidence.
- Do not plug potentially infected removable media directly into your forensic workstation.
- Always forensically sterilize removable media before using or re-using it to acquire evidence.

MEMORY ACCESS TOOLS

[Volatility](#) is an open-source collection of memory forensic tools used to extract digital artifacts from volatile memory. It is python-based and is command line oriented. It consists of several plugins for exploring the contents of extracted memory. An [extensive list of commands](#) is available for reference from VolatilityFoundation.org.

Ligh et al (2014) offers their list of memory acquisition tools to use in addition to Volatility. This is not an exhaustive list; current tools are regularly updated, and new ones are developed as technologies evolve. Each tool has its own special features and are worth exploring:

- [F-Response](#)
- [MAGNET RAM Capture](#)
- [Mandiant Memoryze](#)
- [AccessData FTK Imager](#)
- [EnCase/WinEn](#)
- [Belkasoft Live RAM Capture](#)
- [Winpmem](#)

VIRTUAL MACHINE MEMORY

Virtual machine memory can also be harvested. Virtual machines are run using a type of computer software, firmware, or hardware called a **hypervisor**. Memory acquisition tools collect memory from the

hypervisor used by the virtual machine. VMware Workstation, VM Player, Fusion and VirtualBox are all applications that support virtual machines. In VMware Workstation, VM Player, or Fusion, memory acquisition tools search for a virtual memory file extension such as .vmem, .vmsn, or .vmss. VirtualBox uses memory file formats such as .raw or as an ELF64 core dump binary.

EVENT RECONSTRUCTION

Data found on RAM can be in the form of strings. **Strings** are a sequence of bytes that contain human-readable characters, typically in ASCII and Unicode. Strings can be the password characters that have been cached, it can contain chat or email messages, documents, cryptocurrency addresses, system timestamps, and other digital artifacts.

Timestamps are very useful in event reconstruction. Some of the most common timestamps found in memory are:

- System time
- Process start and end times
- Thread start and end times
- Internet history URL access times
- Symbolic link creation times
- Registry key last-write times
- MFT entry timestamps
- UserAssist times
- Process working set trim times
- PE file compile time
- Library load times
- Socket/connection creation times
- Event log creation times
- Shimcache record times

LINUX MEMORY FORENSICS

Up to this point, Windows has been used as the frame of reference to explain digital forensics concepts. Linux also has its own memory acquisition tools and methods. Linux memory acquisition tools include: [Volatility](#), [fmem](#), [Linux Memory Extractor \(LiME\)](#), and [/proc/kcore](#). Volatility supports Linux kernels version 2.6.11 through the present.

The same types of information that can be found on RAM for a Windows computer can also be found on a Linux computer (e.g., files placed in the page cache when they are read or executed or most recently used files). The biggest difference is the types of files. The Linux operating system obviously uses different types of files with different file extensions. For example, an **Executable and Linkable Format** (.elf) file is the main executable file format used on Linux systems (e.g., user applications, shared libraries, kernel modules, the kernel itself). Other common file system types that may be seen in memory include: .ext3, .ext4, .sysfs, .proc, .tmpfs, .devpts, .devtmpfs, and .cifs.

MAC MEMORY FORENSICS

The Mac operating system is similar to Linux. Both MacOS and Linux are based on a version of UNIX called Berkeley Software Distribution (BSD). Some of the memory tools available to the Mac operating system include:

- Mac Memory Reader (MMR) which supports v.10.6.x through 10.8 on 32-bit and 64-bit Intel
- Mac Memoryze which supports v.10.6.x through 10.8 on 32-bit and 64-bit Intel
- OSXPmem is open source and support for v.10.7 and later
- Volafox
- Chainbreaker

Mach-O is the file format for all executable file types (e.g., application binaries, shared libraries, kernel binary, kernel extensions) on Mac OSX. Some other Mac-specific digital artifacts that can be found in memory are the operating system's cached copy of the login keychain file, unencrypted e-mail messages and attachments, Apple Contacts, Apple Calendar, Apple Notes, and Adium chat messages.

CONCLUSION

Memory forensics can be very useful in correlating the digital evidence found on disk. Computer RAM temporarily stores code and data that the CPU actively uses to execute instructions to process the data. The operating system's kernel is the portion of the "...operating system code that is always resident in memory and facilitates interactions between hardware and software components" (Kernel (operating, 2023). Windows, Linux, and Mac operating systems have their own unique types of operating system files. In addition, the memory of virtual machines can also be obtained but it is not in the same location as a hardware-based machine.

There are several memory forensic tools available, both as open-source and as paid or subscribed. A digital forensic analyst must be aware that the act of acquiring data from RAM may itself cause data on the RAM to be modified. Therefore, the decision to do it must be carefully weighed. Before proceeding with the acquisition of data, precautions must be taken to not taint any evidence extracted from RAM or a disk.

This section on memory forensics is just a small explanation on a topic that involves a vast amount of knowledge that a digital forensic analyst should have to be effective at performing memory data acquisition tasks. It is encouraged that you conduct additional research.

APPENDIX A

REFERENCES

Chapter 1 — How to Handle Digital Evidence

- Battista Sozio, M. (2017, April 27). *Authenticating Digital Evidence at Trial*. American Bar Association. Retrieved May 28, 2023, from https://www.americanbar.org/groups/business_law/resources/business-law-today/2017-april/authenticating-digital-evidence-at-trial/
- Computer Forensic Tool Testing (CFTT) Reports*. (2023, February 14). U.S. Department of Homeland Security - Science and Technology. Retrieved May 28, 2023, from <https://www.dhs.gov/science-and-technology/nist-cftt-reports>
- Drone forensics*. (n.d.). VTO Labs. Retrieved May 28, 2028, from <https://www.vtolabs.com/drone-forensics>
Drone forensic sample data sets and reports to use for testing and research.
- Eclipse Forensics. (2021, July 1). floppy disk used for investigation 3 Famous Cases Solved Through Digital Forensics. *Cybersecurity Exchange*. <https://eclipseforensics.com/3-famous-cases-solved-through-digital-forensics/>
- Finn, H. (2019, August 29). Who Is the BTK Killer? What 'Mindhunter' Doesn't Tell You About Dennis Rader. *Good Housekeeping*. <https://www.goodhousekeeping.com/life/entertainment/a28859869/btk-killer-dennis-rader/>
- FREE EBOOK: Best Practices for Handling Water Damaged Devices*. (2022). VTO Labs. Retrieved May 28, 2023, from <https://www.vtolabs.com/ebook-request>
- Guttman, B., White, D. R., & Walraven, T. (2022, September). *Digital Evidence Preservation: Considerations for Evidence Handlers* (NIST Interagency Report 8387). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8387>
- Hardware Write Block*. (2023, April 17). NIST. Retrieved May 28, 2023, from <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical/hardware>
DHS testing reports of write blocking devices.
- Injosoft AB. (2023). *ASCII table according to Windows-1252*. Retrieved May 28, 2023, from <https://www.ascii-code.com/>
- IoT Forensics*. (n.d.). VTO Labs. Retrieved May 28, 2023, from <https://www.vtolabs.com/iot-forensics>
IoT sample data sets for digital forensics research.

- Mountrakis, P., & Ioannou, M. (2019, July 2). *Admissibility of digital evidence in court* [Editorial]. Elias Neocleous & Co. LLC. Retrieved May 28, 2023, from <https://www.neo.law/wp-content/uploads/2019/07/Admissibility-of-digital-evidence-in-court-Newsletters-International-Law-Office.pdf>
- Poston, H. (2021, January 8). Popular computer forensics top 19 tools [updated 2021]. *Infosec*. <https://resources.infosecinstitute.com/topic/computer-forensics-tools/>
- Smith, T. (2021, November 5). Popular Case Studies in Digital Forensics. *Pro Digital Forensic Consulting*. <https://prodigital4n6.blogspot.com/2021/11/popular-case-studies-in-digital.html>
- U.S. Department of Justice National Institute of Justice. (2008, April). *Electronic Crime Scene Investigation: A Guide for First Responders, 2nd Edition* (D. W. Hagy, Author; Report No. NCJ 219941). <https://www.ojp.gov/pdffiles1/nij/219941.pdf>
- Vrchoticky, N., & Boone, B. (2022, July 12). The Disturbing Truth of Craigslist Killer Philip Markoff. *Grunge*. <https://www.grunge.com/657017/the-disturbing-truth-of-craigslist-killer-philip-markoff/>
- What is CFReDS?* (n.d.). Retrieved May 28, 2023, from <https://cfreds.nist.gov/> Digital forensic image datasets.

Chapter 2 — Image and Tool Verification

- Block Cipher Techniques*. (2023, May 9). NIST. Retrieved August 3, 2023, from <https://csrc.nist.gov/projects/block-cipher-techniques>
- Brunty, J. (2021, November 1). Validation of Forensic Tools- A Quick Guide for the DFIR Examiner. <https://joshbrunty.github.io/2021/11/01/validation.html>
- cjumpdotcom. (2020, August 28). *2.9 Lab F17, FTK Imager, hash calculation and verification* [Video]. YouTube. <https://www.youtube.com/watch?v=y4PszD1ajSA>
- Computer Security Resource Center. (2023, May 12). *Hash Functions*. NIST. Retrieved June 2, 2023, from <https://csrc.nist.gov/Projects/hash-functions>
- CRU Data Security Group, LLC. (2023). *Download CRU's WriteBlocking Validation Utility*. Retrieved August 3, 2023, from <https://www.cru-inc.com/support/software-downloads/writeblocking-validation-utility/>
- Cryptographic Module Validation Program CMVP*. (2016, October 11). NIST. Retrieved August 3, 2023, from <https://csrc.nist.gov/projects/cryptographic-module-validation-program>
- Cryptographic Standards and Guidelines*. (2023, May 8). NIST. Retrieved August 3, 2023, from <https://csrc.nist.gov/Projects/cryptographic-standards-and-guidelines/example-values>
- DFIRScience. (2022, May 17). *Tableau External Write Blocker Setup and Forensic Imaging Walkthrough* [Video]. YouTube. <https://www.youtube.com/watch?v=Kmm8iaa76rQ>

Digital Corpora. (n.d.). *2009 M57-Jean*. Digital Corpora. Retrieved June 3, 2023, from <https://digitalcorpora.org/corpora/scenarios/m57-jean/>
The M57-Jean scenario is a single disk image scenario involving the exfiltration of corporate documents from the laptop of a senior executive.

Forensic Focus. (2014). *FTK Image Loading and Analysis* [Video]. YouTube.
<https://www.youtube.com/watch?v=TKM7DZiHwVs>

Forensic Focus. (2017, June 9). A Method For Verifying Integrity And Authenticating Digital Media. <https://www.forensicfocus.com/articles/a-method-for-verifying-integrity-and-authenticating-digital-media/>

Image Verification: CSC 485/585 [Lecture transcript]. (n.d.). University of Rhode Island. Retrieved June 3, 2023, from <https://students.cs.uri.edu/~forensics/courses/CSC485/Week8/ImageVerification.pdf>
PowerPoint slides

Information Technology Laboratory / Software and Systems Division Software Quality Group. (2019, November 15). *Computer Forensics Tool Testing Program (CFTT)*. NIST. Retrieved June 3, 2023, from <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt>

Information Technology Laboratory / Software and Systems Division Software Quality Group. (2023, April 26). *Federated Testing Project*. NIST. Retrieved June 3, 2023, from <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/federated-testing>

Jarocki, J. (2009, June 18). Forensics 101: Acquiring an Image with FTK Imager. SANS.
<https://www.sans.org/blog/forensics-101-acquiring-an-image-with-ftk-imager/>

Megri Soft Limited. (2022). *Hashing Service*. Retrieved August 2, 2023, from <https://hashingservice.com/>

National Institute of Standards and Technology. (2023, February 7). *Computer Forensics Tools & Techniques Catalog*. Retrieved June 3, 2023, from <https://toolcatalog.nist.gov/>

Open Text. (2022). *PRODUCT OVERVIEW: OpenText™ EnCase™ Forensic* [PDF].
<https://www.opentext.com/assets/documents/en-US/pdf/opentext-po-encase-forensic-en.pdf>

SANS Institute. (2021, March 9). *The Ultimate List of SANS Cheat Sheets*. SANS. Retrieved August 3, 2023, from <https://www.sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/>

Ted Smith. (2020). *Download*. Quickhash#GUI. Retrieved August 3, 2023, from <https://www.quickhash-gui.org/downloads/>

U.S. Department of Commerce National Institute of Standards and Technology. (2015, August). *Secure Hash Standard (SHS)* (Federal Information Processing Standards Publication Series 180-4). <https://doi.org/10.6028/NIST.FIPS.180-4>

This standard specifies hash algorithms that can be used to generate digests of messages. The digests are used to detect whether messages have been changed since the digests were generated.

Chapter 3 — Evidence Acquisition Process

Forensic Examination of Digital Devices in Civil Litigation: The Legal, Ethical and Technical Traps. (2016, March 1). *American Bar Association*.

https://www.americanbar.org/groups/professional_responsibility/publications/professional_lawyer/2016/volume-24-number-1/forensic_examination_digital_devices_civil_litigation_legal_ethical_and_technical_traps/

Gruber, J., Hargreaves, C. J., & Freiling, F. C. (2023). Contamination of digital evidence: Understanding an underexposed risk. *Forensic Science International: Digital Investigation / DFRWS 2023 EURO - Proceedings of the Tenth Annual DFRWS Europe Conference*, 44(March). <https://doi.org/10.1016/j.fsidi.2023.301501>

Guides Related to Collecting and Using Digital Evidence. (n.d.). International Association of Chiefs of Police Law Enforcement Cyber Center. Retrieved June 9, 2023, from <https://www.iacpybercenter.org/prosecutors/litigation-resources/>

I.R.I.S. Investigations. (n.d.). [Universal Digital Evidence Worksheet]. http://www.irisinvestigations.com/wp-content/uploads/2018/06/IRIS_UDEW-1-400x501.png

Moulin, J. (2015, May 11). *Digital Forensics / Incident Response Forms, Policies, and Procedures* [Photograph]. <https://joshmoulin.com/wp-content/uploads/2015/05/Screen-Shot-2015-05-11-at-1.48.29-PM.png>

National Institute of Standards and Technology. (2023, February 7). *Computer Forensics Tools & Techniques Catalog*. Retrieved June 4, 2023, from <https://toolcatalog.nist.gov/>

University of Tennessee at Chattanooga. (n.d.). *Guide to Computer Forensics and Investigations Fourth Edition* [PowerPoint slides]. University of Tennessee at Chattanooga. Retrieved June 4, 2023, from <https://www.utc.edu/sites/default/files/2021-04/4680-ch04.pdf>

U.S. Department of Justice National Institute of Justice. (2004, April). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (S. V. Hart, Author; Report No. NCJ 199408). <https://www.ojp.gov/pdffiles1/nij/199408.pdf>

U.S. Department of Justice National Institute of Justice. (2009, November). *Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders* (K. Rose, Author; Report No. NCJ 227050). <https://www.ojp.gov/pdffiles1/nij/227050.pdf>

Chapter 4 — Using FTK Imager

AccessData Group, Inc. (2016, March 31). *Imager User Guide* [White paper]. Forensic Focus.

Retrieved August 3, 2023, from https://www.forensicfocus.com/stable/wp-content/uploads/2017/10/ftkimager_ug.pdf

AccessData Group, Inc. & Exterro, Inc. (2022, January 31). *FTK Imager 4.7.1.2 – Release Notes* [White paper]. Retrieved June 12, 2023, from

https://d1kpmuwb7gvu1i.cloudfront.net/Imager/Imager_4.7.1_RN.pdf

Chandel, R. (2020, November 6). Comprehensive Guide on FTK Imager. *Hacking Articles*.

<https://www.hackingarticles.in/comprehensive-guide-on-ftk-imager/>

Cyber Security - Purple Team. (2022, October 15). *How to install FTK Imager in Windows 10*

[Video]. YouTube. https://www.youtube.com/watch?v=l_hKrn2V4Dg

DFIRScience. (2016, October 3). *Forensic Acquisition in Windows - FTK Imager* [Video]. YouTube.

https://www.youtube.com/watch?v=TkG4JqUcx_U

DFIRScience. (2018, February 6). *FTK Imager Command Line Physical Disk Hashing* [Video].

YouTube. <https://www.youtube.com/watch?v=HZaQ7tXfYzA>

Forensic Focus. (2021, May 7). What The Tech? Using FTK Imager. *Forensic Focus*.

<https://www.forensicfocus.com/webinars/what-the-tech-using-ftk-imager/>

Imager User Guide [White paper]. (2016, March 31). Forensic Focus. Retrieved June 12, 2023, from https://www.forensicfocus.com/stable/wp-content/uploads/2017/10/ftkimager_ug.pdf

Regan, B. (2022, November 9). How to create a forensic image of a physical hard drive using FTK

Imager. *Medium*. <https://blueteamtactics.net/how-to-create-a-forensic-image-of-a-physical-hard-drive-using-ftk-imager-ef167729598f>

Tolman, J. (2021, May 6). *AccessData's Forensic Toolkit Product Demo* [Video]. YouTube.

<https://www.youtube.com/watch?v=oamL2eXw7rs>

Chapter 5 — Proper Forensics Methodology and Standards

- Aminnezhad, A., Dehghantanha, A., & Abdullah, M. T. (2015, May). *A Survey on Privacy Issues in Digital Forensics*. ResearchGate. Retrieved June 18, 2023, from https://www.researchgate.net/publication/267799382_A_Survey_on_Privacy_Issues_in_Digital_Forensics/link/552791510cf2e486ae410fbd/download
- [Basic FAT file system directory structure] [Chart]. (2017). Flylib.com. <https://flylib.com/books/2/97/1/html/2/images/04fig07.jpg>
- Cadden, J. (2022). *Magnet Forensics*. Retrieved June 19, 2023, from <https://www.magnetforensics.com/resources/making-the-case-from-a-fire-damaged-dvr/>
- Carvey, H. (n.d.). Windows Incident Response. <https://windowsir.blogspot.com/>
The Windows Incident Response Blog is dedicated to the myriad information surrounding and inherent to the topics of IR and digital analysis of Windows systems.
- Council of the Inspectors General on Integrity and Efficiency (CIGIE). (2019, June 18). *Quality Standards for Digital Forensics* (T. L. Whitcomb & M. J. Missal, Authors). https://www.ignet.gov/sites/default/files/files/Quality_Standards_for_Digital_Forensics_2019.pdf
- Cryptographic Algorithm Validation Program CAVP*. (2023, March 16). NIST. Retrieved August 4, 2023, from <https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program>
- [Desktop Hard Drive]. (n.d.). https://assets.website-files.com/5c895551cef9097fb47eaaa6/5c92ca099f6e07e342523667_35-Desktop-Hard-Drive.jpeg
- Digital Forensics Association*. (n.d.). Retrieved August 4, 2023, from <http://www.digitalforensicsassociation.org/>
- Digital forensics: what is it in 2021—2022?* (n.d.). RecFaces. Retrieved June 18, 2023, from <https://recfaces.com/articles/digital-forensics>
- Disk Imaging*. (2023, April 17). NIST. Retrieved August 4, 2023, from <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cfft/cfft-technical/disk>
Disk imaging tool testing reports
- Documents published by the Scientific Working Group on Digital Evidence*. (n.d.). SWGDE. Retrieved August 4, 2023, from <https://www.swgde.org/documents/published-complete-listing>
- Federated Testing Project*. (2023, April 26). NIST. Retrieved August 4, 2023, from <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cfft/federated-testing>

Forensic Focus. (2020, December 8). *A Linux Forensics Starter Case Study*. Retrieved June 20, 2023, from <https://www.forensicfocus.com/articles/a-linux-forensics-starter-case-study/>

Forensic Media Preparation. (2023, April 17). NIST. Retrieved August 4, 2023, from <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cfft/cfft-technical/forensic>
Forensic media preparation tool testing reports

Forensics Challenge (2001 Archive). (n.d.). The HoneyNet Project. Retrieved June 19, 2023, from <https://www.honeynet.org/challenges/forensic-challenge-2001-archive/>

Forensic String Search. (2022, September 8). NIST. Retrieved August 4, 2023, from <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cfft/cfft-technical-1>
Forensic string search tool testing reports

Hardware Write Block. (2023, April 17). NIST. Retrieved August 4, 2023, from <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cfft/cfft-technical/hardware>
Hardware write block tool testing reports

High Technology Crime Investigation Association. (n.d.). *HTCIA*. Retrieved August 4, 2023, from <https://www.htcia.org/>

Imam, F. (2017, September 29). *Computer Forensics: Legal and Ethical Principles*. Infosec. Retrieved June 18, 2023, from <https://resources.infosecinstitute.com/topic/computer-forensics-legal-ethical-principles/>

International Association of Computer Investigative Specialists (IACIS). (2023, April 20). *Code of Ethics and Professional Conduct Policy* [PDF]. <https://www.iacis.com/wp-content/uploads/2023/03/IACIS-Code-of-Ethics-and-Professional-Conduct-v1.6.pdf>

Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27. (n.d.). *Guidelines for identification, collection, acquisition and preservation of digital evidence*. ISO. Retrieved August 4, 2023, from <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27037:ed-1:v1:en>

Mahalik, H., & Lorentz, P. (2022, September 16). *The Future of Digital Forensics: The Good and the Bad*. Forensic. Retrieved June 19, 2023, from <https://www.forensicmag.com/3425-Featured-Article-List/590044-The-Future-of-Digital-Forensics-The-Good-and-the-Bad/>

Mobile Devices. (2023, April 17). NIST. Retrieved August 4, 2023, from <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cfft/cfft-technical/mobile>
Mobile device tool testing reports

National Institute of Standards and Technology. (2022, January 11). *About Us*. Retrieved June 18, 2023, from <https://www.nist.gov/about-nist>

National Institute of Standards & Technology. (n.d.). *Digital Evidence*. Retrieved June 17, 2023, from <https://www.nist.gov/digital-evidence>

Raytheon Technologies. (2023). *International Society of Forensic Computer Examiners*. Retrieved August 4, 2023, from <https://www.isfce.com/>

Salfati, E., & Pease, M. (2022, June). *Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)* (NISTIR 8428). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8428>

Solanke, A. A., & Biasiotti, M. A. (2022). Digital Forensics AI: Evaluating, Standardizing and Optimizing Digital Evidence Mining Techniques. *Künstliche Intelligenz*, 36, 143-161. <https://doi.org/10.1007/s13218-022-00763-9>

Trier of Fact. (2017, May 11). Legal Dictionary. Retrieved June 18, 2023, from <https://legaldictionary.net/trier-of-fact/>

Chapter 6 — Various File Systems: Electronic Evidence Issues

13Cubed. (2017, June 4). *Introduction to Windows Forensics - Digital Forensics Course* [Video]. YouTube. <https://www.youtube.com/watch?v=VYROU-ZwZX8&list=PLlv3b9B16ZadqDQH0ITRO4kqn2P1g9Mve>

Apple File System. (2023, March 29). Wikipedia. Retrieved June 24, 2023, from https://en.wikipedia.org/wiki/Apple_File_System

Both, D. (2017, May 25). An introduction to Linux's EXT4 filesystem. <https://opensource.com/article/17/5/introduction-ext4-filesystem>

Bowne, S. (2016, November 17). *CNIT 121: 13 Investigating Mac OS X Systems (Part 1 of 2)* [Video]. YouTube. <https://www.youtube.com/watch?v=7r5rF2ad1bo>

Bowne, S. (2016, November 17). *CNIT 121: 13 Investigating Mac OS X Systems (Part 2 of 2)* [Video]. YouTube. <https://www.youtube.com/watch?v=Py8GqmG2wag>

Burn, I. (2022, February 9). FAT16 and FAT32: characteristics and differences. <https://ccm.net/computing/hardware/9773-fat16-and-fat32-characteristics-and-differences/>

Casey, E., Fellows, G., Geiger, M., & Stellatos, G. (2011). The growing impact of full disk encryption on digital forensics. *Digital Investigation*, 8(2), 129-134. <https://doi.org/10.1016/j.diin.2011.09.005>

Computer Clan. (2017, October 12). *What is APS? The Apple File System Explained* [Video]. YouTube. <https://www.youtube.com/watch?v=9I7fg930Deg>

CS Lesson. (2020, September 23). *Linux Forensics Tutorial || Linux file system forensics* [Video]. YouTube. <https://www.youtube.com/watch?v=HTEj8UY2TA8>

Difference between ext2, ext3 and ext4. (2020, June 24). *KernelTalks*. <https://kerneltalks.com/disk-management/difference-between-ext2-ext3-and-ext4/>

Hamdan, M. (2022, June 24). *Linux Forensics Investigation / TryHackMe Linux Forensics* [Video]. YouTube. https://www.youtube.com/watch?v=gOg_h9fdgZE

HFS Plus. (2023, March 25). Wikipedia. Retrieved June 24, 2023, from https://en.wikipedia.org/wiki/HFS_Plus

Hoffman, C., & Lewis, N. (2023, February 10). FAT32 vs. exFAT vs. NTFS: What's the Difference? <https://www.howtogeek.com/235596/whats-the-difference-between-fat32-exfat-and-ntfs/>

IsoBuster. (2013, October 2). *Recover deleted files and folders from a FAT formatted disk (Undelete FAT)* [Video]. YouTube. <https://www.youtube.com/watch?v=nWQGC0Y9464>

[Linux Directory] [Chart]. (2023). Linux Handbook. <https://linuxhandbook.com/content/images/2020/06/linux-system-directories-poster.png>

Mac operating systems. (2023, July 29). Wikipedia. Retrieved August 4, 2023, from https://en.wikipedia.org/wiki/Mac_operating_systems

[NTFS Attribute Types] [Table]. (n.d.). Microsoft. https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-fscc/a82e9105-2405-4e37-b2c3-28c773902d85

NTFS overview. (2023, March 23). Retrieved June 24, 2023, from <https://learn.microsoft.com/en-us/windows-server/storage/file-server/ntfs-overview>

Parallel Virtual File System. (2023, March 25). Wikipedia. Retrieved June 25, 2023, from https://en.wikipedia.org/wiki/Parallel_Virtual_File_System

SEVNX. (2021, July 7). *Imaging APFS - A Walkthrough for Starting Forensics on MacOS* [Video]. YouTube. <https://www.youtube.com/watch?v=cThb0y5eNTs>

SystemForensics. (2022, December 30). *011 FAT File Systems FAT32 and FAT16 forensics* [Video]. YouTube. <https://www.youtube.com/watch?v=hv0grnkdqis>

U.S. Department of Commerce. (2020, August). *NIST Cloud Computing Forensic Science Challenges* (M. Herman, M. Iorga, A. M. Salim, R. H. Jackson, M. R. Hurst, R. Leo, . . . R. Sardinias, Authors; NIST Interagency Report 8006). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8006>

Vigo, J. (2018, January 8). HFS+ v. APFS: Which Apple file system is better? *TechRepublic*. <https://www.techrepublic.com/article/apfs-vs-hfs-which-apple-filesystem-is-better/>

What is HDFS? (n.d.). IBM. Retrieved June 25, 2023, from <https://www.ibm.com/topics/hdfs>

Chapter 7 — Windows Registry Analysis

Autoruns for Windows v14.1 [Autoruns for Windows 14.1]. (2023, June 7). <https://download.sysinternals.com/files/Autoruns.zip>

Belding, G. (2018, July 20). Threat Hunting for Suspicious Registry and System File Changes. *InfoSec*. <https://resources.infosecinstitute.com/topic/threat-hunting-for-suspicious-registry-and-system-file-changes/>

Carvey, H. A. (2011). *Windows Registry Forensics* (D. Hull, Ed.). Elsevier.

Ganesh, B. (2023, June 3). Windows Registry Analysis – Tracking Every Activity That You Do on the Windows System. <https://gbhackers.com/windows-registry-analysis-tracking-everything-you-do-on-the-system/>

Google Code Archive: regripper. (n.d.). Retrieved July 1, 2023, from <https://code.google.com/archive/p/regripper/downloads>
Download website for RegRipper application.

Grimes, R. (2017, November 9). Infected with malware? Check your Windows registry. *CSO*. <https://www.csoonline.com/article/550849/are-you-infected-with-malware-check-windows-registry-keys.html>

How to back up and restore the registry in Windows. (n.d.). *Microsoft | Support*. https://support.microsoft.com/en-us/topic/how-to-back-up-and-restore-the-registry-in-windows-855140ad-e318-2a13-2829-d428a2ab0692#ID0EBD=Windows_8.1

Liang, H., Harris, B., Cox, E., Zou, L., Anna-Li, & Xu, S. (2023, March 8). *Windows registry information for advanced users*. Retrieved July 1, 2023, from <https://learn.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users>

Mills, M. (2021, November 14). *Registry Explorer, alternative registry editor for Windows*. Retrieved July 1, 2023, from <https://itigic.com/registry-explorer-alternative-registry-editor-for-windows/>

Network Edition [Image]. (n.d.). Registry Explorer. <http://www.regxplor.com/screenshots.html>

Registry Explorer. (n.d.). Retrieved July 6, 2023, from <http://www.regxplor.com/download.html>

regripper. (2013). Google Code Archive. Retrieved July 6, 2023, from <https://code.google.com/archive/p/regripper/downloads>
Regripper download site.

RegRipper & keys parsed by plugins. (2020, May 27). Retrieved July 1, 2023, from <https://hexacorn.com/tools/3r.html>

[RegRipper report sample]. (2009, February 6). <https://www.sans.org/blog/regripper-ripping-registries-with-ease/>

RegScanner [Image]. (n.d.). NirSoft. https://www.nirsoft.net/windows_registry_tools.html

RegScanner v2.71 - find / search in the Registry of Windows. (2022). Retrieved July 1, 2023, from <https://www.nirsoft.net/utis/regscanner.html>

RegScanner v2.71 - find / search in the Registry of Windows. (2022). Retrieved July 1, 2023, from <https://www.nirsoft.net/utis/regscanner.html>
Download website for RegScanner.

Russinovich, M. (2023, June 27). *Autoruns for Windows v14.1*. Retrieved July 1, 2023, from <https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns>

VIRUSTOTAL. (n.d.). Retrieved July 1, 2023, from <https://www.virustotal.com/gui/home/upload>

White, S., Mozi, Sharkey, K., Coulter, D., Batchelor, D., & Satran, M. (2021, June 2). *Structure of the Registry*. Retrieved June 28, 2023, from <https://learn.microsoft.com/en-us/windows/win32/sysinfo/structure-of-the-registry>

White, S., Park, C. D., Partlow, J., Sharkey, K., Coulter, D., Batchelor, D., & Satran, M. (2023, February 8). *Registry value types*. Retrieved July 1, 2023, from <https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry-value-types>

White, S., Sharkey, K., Syroxieon, & Satran, M. (2021, January 7). *Registry Hives*. Microsoft. Retrieved August 4, 2023, from <https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry-hives>

Zimmerman, E. (n.d.). *Registry Explorer*. Retrieved July 1, 2023, from <https://www.sans.org/tools/registry-explorer/>

Download site for Registry Explorer.

Chapter 8 — Windows File System Analysis

[Autopsy Download Page]. (n.d.). Retrieved July 2, 2023, from <https://www.sleuthkit.org/autopsy/>

Belkasoft RAM Capturer. (n.d.). Retrieved July 2, 2023, from <https://belkasoft.com/ram-capturer>

Community Tools. (n.d.). CrowdStrike. Retrieved July 2, 2023, from <https://www.crowdstrike.com/resources/community-tools/>

Downloading Nmap. (n.d.). Retrieved July 2, 2023, from <https://nmap.org/download.html>

Eric Zimmerman's Tools. (n.d.). Retrieved July 2, 2023, from <https://ericzimmerman.github.io/#!index.md>

Site to download LECmd and JumpList Explorer programs

ExifTool by Phil Harvey. (n.d.). Retrieved July 2, 2023, from <https://exiftool.org/>

FAW - Forensics Acquisition of Websites. (n.d.). Retrieved July 2, 2023, from <https://www.fawproject.com/>

Forensic Investigator. (n.d.). Splunkbase. Retrieved July 2, 2023, from <https://splunkbase.splunk.com/app/2895/>

HashMyFiles v2.43 - Calculate MD5/SHA1/CRC32 hashes of your files. (n.d.). NirSoft. Retrieved July 2, 2023, from https://www.nirsoft.net/utils/hash_my_files.html

\$I Parse [\$I Parser]. (2023). <https://df-stream.com/download/321/>

Kornblum, J., Kendall, K., & Mikus, N. (2013, May 8). *Foremost*. SourceForge. Retrieved July 3, 2023, from <https://sourceforge.net/projects/foremost/>

MAGNET Encrypted Disk Detector. (2023). Retrieved July 2, 2023, from <https://www.magnetforensics.com/resources/encrypted-disk-detector/>

MAGNET RAM Capture. (2023). Retrieved July 2, 2023, from <https://www.magnetforensics.com/resources/magnet-ram-capture/>

Maschke, M., & Barnes, B. (2020, November 19). *A Lawyers Guide to Windows 10 and Evolving Digital Forensics Techniques* [PowerPoint slides]. Retrieved July 4, 2023, from <https://www.dcbarr.org/getmedia/db97b178-8aa6-4216-b7dd-8fc0888fde1a/A-Lawyers-Guide-to-Windows-10-and-Evolving-Digital-Forensics-Techniques-19Nov2020>

Metadata. (n.d.). Wikipedia. Retrieved July 3, 2023, from <https://en.wikipedia.org/wiki/Metadata>

Narzisi, G., Fang, H., & Schatz, M. (2019, January 11). *scalpel*. Retrieved July 3, 2023, from <https://sourceforge.net/projects/scalpel/>

NetworkMiner. (n.d.). Netresec. Retrieved July 2, 2023, from <https://www.netresec.com/?page=NetworkMiner>

NirSoft. (2021). *WinPrefetchView v1.37*. Retrieved July 2, 2023, from https://www.nirsoft.net/utils/win_prefetch_view.html

Nitorgenc. (n.d.). *ANSSI-FR / bmc-tools*. GitHub. Retrieved July 2, 2023, from <https://github.com/ANSSI-FR/bmc-tools>

RDP Bitmap Cache parser

rashi_garg. (2022, July 1). *Windows Forensic Analysis*. Retrieved July 2, 2023, from <https://www.geeksforgeeks.org/windows-forensic-analysis/#>

Smolen, B., Harwood, R., Dhiman, M., dknappettmsft, Downie, K., Leavitt, S., Sharkey, K., Wester-Ebbinghaus, K., Ross, E., Gerend, J., Knight, L., imba-tjd, Dardour, M., Poggemeyer, L., Hansen, A., Ainapure, K., & Watumull, G. (2023, February 15). *Resilient File System (ReFS) overview*. Microsoft. Retrieved July 3, 2023, from <https://learn.microsoft.com/en-us/windows-server/storage/refs/refs-overview>

2.6 File Attributes [Table]. (2022, April 27). Microsoft. https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-fscc/ca28ec38-f155-4768-81d6-4bfeb8586fc9

Wireshark. (n.d.). Retrieved July 2, 2023, from <https://www.wireshark.org/>

Chapter 9 — Forensic Tools

Accelerate Your DFIR Investigation. (n.d.). Belkasoft. Retrieved July 7, 2023, from <https://belkasoft.com/>

Atola Insight Forensic. (n.d.). Atola Technology. Retrieved July 7, 2023, from <https://atola.com/products/insight/>

Atola TaskForce Forensic Imager with 15 TB /Hour Performance. (n.d.). Retrieved July 7, 2023, from <https://atola.com/products/taskforce/>

Autopsy Digital Forensics. (n.d.). Retrieved July 6, 2023, from <https://www.autopsy.com/>

Bassetti, N., & Lehr, J. (n.d.). *C.A.IN.E. Computer Aided Investigative Environment*. CAINE Computer Forensics Linux Live Distro. Retrieved August 2, 2023, from <https://www.caine-live.net/>

Batard, P. (2023). *Rufus*. Retrieved August 2, 2023, from <https://rufus.ie/en/>

Bitdefender is a Global Leader in Cybersecurity. (n.d.). Bitdefender. Retrieved July 7, 2023, from <https://www.bitdefender.com/>

Cellebrite UFED. (n.d.). Retrieved July 6, 2023, from https://cellebrite.com/wp-content/uploads/2022/11/Solution_Overview_Cellebrite_UFED_LTR.pdf

cjumpdotcom. (2020, August 28). *2.9 Lab F17, FTK Imager, hash calculation and verification* [Video]. YouTube. <https://www.youtube.com/watch?v=y4PszD1ajSA>

Collins, C. E. (2023). *Cloud Storage & Digital Forensic Evidence: Understanding Misconceptions and Providing Answers*. Hexordia. Retrieved July 6, 2023, from <https://static1.squarespace.com/static/62ab5b933d903d4c55e5d716/t/645ae8f3839ee9684f2ed8f5/1683679477474/Cloud+Storage+and+Digital+Forensic+Evidence.pdf>

Computer Forensics Tool Testing (CFTT) Program. (n.d.). *CFTT Federated Testing 64-bit ISO beta version* [ISO image]. <https://s3.amazonaws.com/cftt.cfreds.nist.gov/cftt/federated-testing-version-6-1.iso>

CRU Data Security Group, LLC. (2023). *Download CRU's WriteBlocking Validation Utility*. CRU. Retrieved August 2, 2023, from <https://www.cru-inc.com/support/software-downloads/writeblocking-validation-utility/>

E3:Universal Software License. (n.d.). Paraben Corporation. Retrieved July 6, 2023, from <https://paraben.com/shopping/E3-Universal-Software-License-p446500535>

FCI Home Forensic Computers, Inc. (n.d.). Retrieved July 6, 2023, from <https://www.forensiccomputers.com/>

FINALMobile Forensics 4 Download. (n.d.). Retrieved July 6, 2023, from <http://fmf.finaldata.com/Download/fmf4.html>

Forensic Explorer (FEX)™. (n.d.). GetData Forensics. Retrieved July 7, 2023, from <https://getdataforensics.com/product/forensic-explorer-fex/>

ForensicSoft, Inc. (2023). *SAFE Block*. Retrieved August 3, 2023, from <https://www.forensicsoft.com/products/safe-block>

Forensics Software Tools for Mobile, Cell Phone, Cellular, Smartphone. (n.d.). Retrieved July 6, 2023, from <https://www.secureview.us/>

Forensic UltraDock, model FUDv6. (n.d.). WiebeTech. Retrieved July 6, 2023, from <https://wiebetech.com/products/forensic-ultradock-fudv6-0/>

FTK® Forensic Toolkit. (n.d.). exterro. Retrieved July 6, 2023, from <https://www.exterro.com/forensic-toolkit>

H3xx Edit. (2014, March 26). *FTK Image Loading and Analysis* [Video]. YouTube. <https://www.youtube.com/watch?v=TKM7DZiHwVs>

Health Insurance Portability and Accountability Act of 1996 (HIPAA). (n.d.). U.S. Department of Health & Human Services. Retrieved July 6, 2023, from <https://www.cdc.gov/phlp/publications/topic/hipaa.html>

Information Technology Laboratory / Software and Systems Division Software Quality Group. (2023, April 26). *Federated Testing Project*. NIST. Retrieved June 3, 2023, from <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cfft/federated-testing>

Lawrence, T., Karabiyik, U., & Shashidhar, N. (2018). Equipping a digital forensic lab on a budget. *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, (March), 1-7. <http://dx.doi.org/10.1109/ISDFS.2018.8355345>

Magnet AXIOM Cyber. (n.d.). Magnet Forensics. Retrieved July 6, 2023, from <https://www.magnetforensics.com/products/magnet-axiom-cyber/>

Norton AntiVirus Plus. (n.d.). Norton. Retrieved July 7, 2023, from <https://us.norton.com/products/norton-360-antivirus-plus>

OpenText EnCase Forensic. (n.d.). OpenText. Retrieved July 6, 2023, from <https://www.opentext.com/products/encase-forensic>

Our Featured Products. (n.d.). Forensic Store. Retrieved July 6, 2023, from <https://www.forensicstore.com/>

PC-3000 Data Recovery. (n.d.). Retrieved July 7, 2023, from <http://www.pc3000.com/>

Registry Explorer. (n.d.). Retrieved July 6, 2023, from <http://www.regxplor.com/download.html>

regripper. (2013). Google Code Archive. Retrieved July 6, 2023, from <https://code.google.com/archive/p/regripper/downloads>

Regripper download site.

RegScanner v2.71 - find / search in the Registry of Windows. (2022). Retrieved July 1, 2023, from <https://www.nirsoft.net/utis/regscanner.html>

Securing Cloud Services for the Federal Government. (n.d.). FedRAMP. Retrieved July 6, 2023, from <https://www.fedramp.gov/>

Simplify Your Investigations. (n.d.). Magnet Forensics. Retrieved July 6, 2023, from <https://www.magnetforensics.com/products/magnet-axiom-cyber/>

Simplify your workflow and strengthen your investigations. (n.d.). Oxygen Forensics. Retrieved July 7, 2023, from <https://oxygenforensics.com/en/solutions/federal-and-government/>

SQLite Forensic Tools That Make A Difference! (n.d.). Sanderson Forensics. Retrieved July 7, 2023, from <https://sqliteforensictoolkit.com/>

STE3000. (n.d.). Ramsey. Retrieved July 6, 2023, from <https://ramseytest.com/ste3000>

Teel Technologies Chip-off | ISP | JTAG. (n.d.). Retrieved July 6, 2023, from <https://teeltech.com/chip-off-isp-jtag/>

Teel Technologies Chip Reader Kits. (n.d.). Retrieved July 6, 2023, from <https://www.teeltech.com/mobile-device-forensic-hardware/chip-reader-kits/>

Tower Workstations. (n.d.). Retrieved July 6, 2023, from <https://siliconforensics.com/products/forensic-workstations/tower-workstations.html>

UltraKit | UltraBlock. (n.d.). Digital Intelligence. Retrieved July 6, 2023, from <https://digitalintelligence.com/products/ultrablock#overview>

U.S. Department of Commerce. (2020, February). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (R. Ross, V. Pillitteri, K. Dempsey, M. Riddle, & G. Guissanie, Authors; Special Publication 800-171, Revision 2). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-171r2>

U.S. Department of Commerce. (2020, September). *Security and Privacy Controls for Information Systems and Organizations* (Special Publication 800-53, Revision 5). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-53r5>

U.S. Department of Commerce. (2023, May 9). *Advanced Encryption Standard (AES)* (Federal Information Processing Standards 197). National Institute of Standards and Technology (NIST). <https://doi.org/10.6028/NIST.FIPS.197-upd1>
Originally published November 26, 2001

U.S. Department of Defense Defense Information Systems Agency. (2017, March 6). *Department of Defense Cloud Computing Security Requirements Guide* (Publication No. Version 1, Release 3). https://rmf.org/wp-content/uploads/2018/05/Cloud_Computing_SRG_v1r3.pdf

U.S. Department of Justice. (2020, June 1). *Criminal Justice Information Services (CJIS) Security Policy*. Federal Bureau of Investigation. https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

VLC media player. (n.d.). VideoLAN Organization. Retrieved July 6, 2023, from <https://www.videolan.org/vlc/>
Download site for VLC video media player.

X-Ways Forensics: Integrated Computer Forensics Software. (n.d.). Retrieved July 7, 2023, from <https://x-ways.net/forensics/>

Chapter 10 — Incident Response

Downloading Nmap. (n.d.). Nmap.org. Retrieved July 10, 2023, from <https://nmap.org/download.html>

Figure 3-1. Incident Response Life Cycle [Illustration]. (n.d.). NIST. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

F-Response TACTICAL. (n.d.). Retrieved July 9, 2023, from <https://www.f-response.com/software/tac>

Lambert, M. (2022, September 5). Why you need an incident timeline. *Incident.io*.
<https://incident.io/blog/why-you-need-incident-timelines>

Lee, R. (n.d.). *SIFT Workstation*. SANS Institute. Retrieved July 9, 2023, from
<https://www.sans.org/tools/sift-workstation/>

Mandiant Redline for Windows. (2020, May 7). Softpedia. Retrieved August 4, 2023, from
<https://www.softpedia.com/get/Security/Security-Related/Mandiant-Redline.shtml>

McCurdy, M. (2020, November 30). Win the hearts of incident responders with Windows logging. *accenture*. <https://www.accenture.com/us-en/blogs/cyber-defense/win-hearts-incident-responders-windows-logging>

Mihaiuc, A., markruss, Hewardt, M., Stephens, J., Buck, A., Peters, S., Jahiu, D., Bjorn, W., Maurer, H., Kim, L., analyze-v, & Tsarev, L. (2023, March 30). *Process Explorer v17.05*. Microsoft. Retrieved August 4, 2023, from <https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer>

Murdoch, D. (2016). *Blue Team Handbook: Incident Response Edition* (2.2 ed.).

Professor K. (2021, September 5). *Overview of Sysinternal's Process Explorer* [Video]. YouTube.
<https://www.youtube.com/watch?v=3UXhMpvATS0>

Release Downloads. (n.d.). Retrieved July 9, 2023, from <https://www.volatilityfoundation.org/>

Sava, A. (2016, September 1). *Mandiant Redline for Windows*. Softpedia. Retrieved July 8, 2023, from <https://www.softpedia.com/get/Security/Security-Related/Mandiant-Redline.shtml>

Snort 3 is available! (n.d.). Snort. Retrieved July 10, 2023, from <https://www.snort.org/>

Tenable Nessus®: The Global Gold Standard in Vulnerability Assessment Built for the Modern Attack Surface. (n.d.). Tenable. Retrieved July 10, 2023, from
<https://www.tenable.com/products/nessus>

U.S. Department of Commerce. (2012, August). *Computer Security Incident Handling Guide* (P. Cichonski, T. Millar, T. Grance, & K. Scarfone, Authors; Special Publication 800-61 Rev. 2). National Institute of Standards and Technology (NIST).
<https://doi.org/10.6028/NIST.SP.800-61r2>

Volatility Foundation. (2020). Retrieved August 4, 2023, from
<https://www.volatilityfoundation.org/>

Vulnerability Management: Your IT infrastructure's security is the most important thing to us. (n.d.). Greenbone AG. Retrieved July 10, 2023, from <https://www.greenbone.net/en/>

The world's most popular network protocol analyzer. (n.d.). Wireshark. Retrieved July 10, 2023, from <https://www.wireshark.org/>

Chapter 11 — Introduction to Password Cracking

- Aircrack-ng Download*. (n.d.). Retrieved July 17, 2023, from <https://www.aircrack-ng.org/>
- Cain & Abel 4.9.56*. (n.d.). TechSpot. Retrieved July 17, 2023, from <https://www.techspot.com/downloads/2416-cain-abel.html>
- Chu, M. (n.d.). *How Many Passwords Are Possible With 4, 6, 8, Or More Digits?* Data Overhauleders. Retrieved July 11, 2023, from <https://dataoverhauleders.com/how-many-possible-passwords/>
- CrackStation*. (n.d.). Retrieved July 15, 2023, from <https://crackstation.net/>
- Download*. (n.d.). Hashcat. Retrieved July 21, 2023, from <https://hashcat.net/hashcat/>
- Download ophcrack*. (n.d.). Ophcrack. Retrieved July 17, 2023, from <https://ophcrack.sourceforge.io/download.php>
- 11 Password Cracker Tools (Password Hacking Software 2023)*. (2023, June 29). Software Testing Help. Retrieved July 17, 2023, from <https://www.softwaretestinghelp.com/password-cracker-tools/>
- Free Your iPhone / iPad / iPod touch from Various Locks Instantly and Happily*. (n.d.). iMobie. Retrieved July 15, 2023, from <https://www.imobie.com/anyunlock/iphone-password-unlocker.htm>
- Guo, J. (2016, February 17). *Why even the FBI can't hack the iPhone*. The Washington Post. Retrieved July 18, 2023, from <https://www.washingtonpost.com/news/wonk/wp/2016/02/17/how-long-it-takes-to-crack-an-iphone/>
- Hammond, J. (2023, April 4). *Password Hacking in Kali Linux* [Video]. YouTube. https://www.youtube.com/watch?v=4X5aoQ8i-_g
- Hash Suite Droid (Hash Suite for Android)*. *Free and Open Source*. (n.d.). Hash Suite. Retrieved July 17, 2023, from <https://hashsuite.openwall.net/android>
- Home*. (n.d.). Hash Suite. Retrieved July 17, 2023, from <https://hashsuite.openwall.net/>
- John the Ripper*. (n.d.). TechSpot. Retrieved July 17, 2023, from <https://www.techspot.com/downloads/6970-john-the-ripper.html>
- McElhearn, K. (2020, August 28). If Hackers Crack a Six-Digit iPhone Passcode, They Can Get All Your Passwords. *The Mac Security Blog*. <https://www.intego.com/mac-security-blog/if-hackers-crack-a-six-digit-iphone-passcode-they-can-get-all-your-passwords/>
- Mcleod, S., & Evans, O. G. (2023, May 10). Short-Term Memory | Facts, Types, Duration & Capacity. *Simply Psychology*. <https://www.simplypsychology.org/short-term-memory.html>
- Miller, M. (2022, March 25). Password Cracking 101: Attacks & Defenses Explained. *BeyondTrust*. <https://www.beyondtrust.com/blog/entry/password-cracking-101-attacks-defenses-explained>

Nicas, J. (2020, October 21). *The Police Can Probably Break Into Your Phone*. The New York Times. Retrieved July 18, 2023, from <https://www.nytimes.com/2020/10/21/technology/iphone-encryption-police.html>

Passware. (n.d.). *Find. Decrypt. Open*. Passware. Retrieved July 21, 2023, from <https://www.passware.com/>

Password Cracker. (n.d.). cnet. Retrieved July 15, 2023, from https://download.cnet.com/Password-Cracker/3000-2092_4-10226556.html

RainbowCrack. (n.d.). Retrieved July 17, 2023, from <http://project-rainbowcrack.com/>

Rowe, A. (2023, March 21). Study Reveals Average Person Has 100 Passwords. *tech.co*. <https://tech.co/password-managers/how-many-passwords-average-person>

Wagenseil, P. (2016, February 29). Smartphone Encryption: What You Need to Know. *Tom's Guide*. <https://www.tomsguide.com/us/smartphone-encryption-faq,news-21915.html>

Chapter 12 — Introduction to Steganography

Albano, K., & Kessem, L. (2017, February 15). The Full Shamoan: How the Devastating Malware Was Inserted Into Networks. *Security Intelligence*. <https://securityintelligence.com/the-full-shamoan-how-the-devastating-malware-was-inserted-into-networks/>

Axel F. (2016, July 7). NetTraveler APT Targets Russian, European Interests. *proofpoint*. <https://www.proofpoint.com/us/threat-insight/post/nettraveler-apt-targets-russian-european-interests>

Berry, N. (2012, November 3). Discrete Cosine Transformations. *Data Genetics*. <http://datagenetics.com/blog/november32012/index.html>

[Binary representation of a pixel and the least significant bit]. (n.d.). Hacking Land. <https://3.bp.blogspot.com/-Y2mozhtViLQ/WnlwaQdEKfI/AAAAAAAAAKGs/Z78gfWu1bMfDeyNcCf0uBsS7Ttr6LQdgCLcBGAs/s1600/encode.png>

Black Slash. (2017, November 11). *How to Hide Secret Data Inside an Image or Audio File in Seconds*. Cyber Weapons Lab. Retrieved July 20, 2023, from <https://null-byte.wonderhowto.com/how-to/steganography-hide-secret-data-inside-image-audio-file-seconds-0180936/>

cpascoe95. (2014, July 3). *Image Steganography*. SourceForge. Retrieved July 21, 2023, from <https://sourceforge.net/projects/image-steg/>

CyberWire, now N2K Cyber (Host). (2017, December 9). Stealthy Zberp Banking Trojan — Research Saturday [Video podcast episode]. In *Research Saturday*. YouTube. <https://www.youtube.com/watch?v=8Z3uC4lxI3A>

The Discrete Cosine Transform (DCT). (n.d.). Retrieved July 21, 2023, from <https://cs.stanford.edu/people/eroberts/courses/soco/projects/data-compression/lossy/jpeg/dct.htm>

Download.com Staff (Ed.). (2009, February 27). *Xiao Steganography Editor's Review*. CNET. Retrieved July 21, 2023, from https://download.cnet.com/Xiao-Steganography/3000-2092_4-10541494.html
Download link provided on webpage.

Fraile, R. (2015, January 31). *Digital Steganography: LSB in Images* [Illustration]. SlideShare. <https://image.slidesharecdn.com/steganography-150131143936-conversion-gate01/95/steganography-hiding-your-secrets-with-php-23-638.jpg?cb=1436980076>

Global Research and Analysis Team. (2013). *The NeTTraveler (aka 'TravNeT')*. Kaspersky Lab. <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08080841/kaspersky-the-net-traveler-part1-final.pdf>

Go Green Software. (n.d.). *SSuite PicseL Security*. Retrieved July 21, 2023, from <https://www.ssuitesoft.com/ssuitepicseLsecurity.htm>

LeeLu Soft - official direct downloads. (2017, August 29). LeeLu Soft. Retrieved July 21, 2023, from <http://www.leelusoft.altervista.org/steganographx.html>

malwarebreakdown. (2017, April 3). Good Man Gate Leads to RIG EK, Drops ZeusVM (KINS). *Malware Breakdown*. <https://malwarebreakdown.wordpress.com/2017/04/03/good-man-gate-leads-to-rig-ek-drops-zuesvm-kins/>

Myrtus 0x0. (2019, December 21). Shamoon 2012 Complete Analysis. *MalwareInDepth*. <https://malwareindepth.com/shamoon-2012/>

Null Byte. (2018, September 16). *Conceal Secret Messages or Data Through Steganography with Steghide* [Tutorial] [Video]. YouTube. <https://www.youtube.com/watch?v=9UZh-4Er7BQ>

OpenStego. (n.d.). Retrieved July 21, 2023, from <https://www.openstego.com/>

RedBlue Labs. (2021, October 25). *How To Insert Secret Picture Into a Song (Steganography)* [Video]. YouTube. https://www.youtube.com/watch?v=yZBuwK_mh5A

rsteg for Windows. (2010, March 26). Softpedia. Retrieved July 21, 2023, from <https://www.softpedia.com/get/Security/Security-Related/rSteg.shtml>

Segura, J. (2014, February 17). Hiding in plain sight: a story about a sneaky banking Trojan. *Malwarebytes Labs*. <https://blog.malwarebytes.com/threat-analysis/2014/02/hiding-in-plain-sight-a-story-about-a-sneaky-banking-trojan/>

Shankdhar, P. (2020, July 8). Best tools to perform steganography [updated 2020]. *Infosec*. <https://resources.infosecinstitute.com/topic/steganography-and-tools-to-perform-steganography/>

Steghide - Download. (2003, December 24). SourceForge. Retrieved July 21, 2023, from <https://steghide.sourceforge.net/download.php>

the_land_baron. (2016, January 21). *Crypture*. SourceForge. Retrieved July 21, 2023, from <https://sourceforge.net/projects/crypture/>
Using OpenStego. (n.d.). OpenStego. Retrieved July 20, 2023, from <https://www.openstego.com/>
Williams, J. (Presenter). (n.d.). *Steganography: Conceal the Threat, Hide the Evidence!* [Lecture]. PowerPoint presentation

Chapter 13 — Introduction to Cryptocurrency

Ashford, K. (2023, February 16). *What Is Cryptocurrency?* (B. Curry, Ed.). Retrieved July 24, 2023, from <https://www.forbes.com/advisor/investing/cryptocurrency/what-is-cryptocurrency/>
Bitcoin USD (BTC-USD). (n.d.). Yahoo Finance. Retrieved July 25, 2023, from <https://finance.yahoo.com/quote/BTC-USD/history/>
Conflux Network. (2021, October 30). Centralized vs. Decentralized Digital Currency (and Why it Matters). *Medium*. <https://medium.com/conflux-network/centralized-vs-decentralized-digital-currency-and-why-it-matters-6df64df1736d>
NFTs for Everyone. (n.d.). Enjin. Retrieved July 26, 2023, from <https://enjin.io/>
[Non-Fungible Token Marketplace]. (n.d.). OpenSea. Retrieved July 26, 2023, from <https://opensea.io/>
Rosen, A. (2023, July 6). 11 Best Crypto Exchanges and Apps of July 2023. *Nerd Wallet*. <https://www.nerdwallet.com/best/investing/crypto-exchanges-platforms>
Rubin, R., & Rega, A. (2021, April 5). Forensic Analysis of Digital Currencies in Investigations. <https://www.americanbar.org/groups/litigation/committees/pretrial-practice-discovery/practice/2021/forensic-analysis-of-digital-currencies-in-investigations/>
Smith, C., Rutten, T., Wackerow, P., minimalism, J., Ashimine, I. E., & Londhe, S. (2023, April 7). *ERC-1155 Multi-token Standard*. Ethereum.org. Retrieved July 25, 2023, from <https://ethereum.org/en/developers/docs/standards/tokens/erc-1155/>
Voigt, K., Rosen, A., & Coombes, Editor, A. (2023, March 29). Bitcoin for Beginners: What You Need to Know about BTC. *Nerd Wallet*. <https://www.nerdwallet.com/article/investing/what-is-bitcoin>
Wackerow, P., Ponnann, J. P., Tarcan, H., superphiz, Smith, C., minimalism, J., Vianello, J., hugomd, H., Barda, V., Grimaud, P., Yilmaz, E. Y., Garske, V., Moen, K., Richards, S., Gontijo, A., & scrovy. (2023, June 23). *ERC-721 Non-Fungible Token Standard*. Ethereum.org. Retrieved July 25, 2023, from <https://ethereum.org/en/developers/docs/standards/tokens/erc-721/>
Williams, J. (Presenter). (n.d.). *Digital Assets and Cryptocurrency 101 Workshop* [Lecture]. PowerPoint presentation

Chapter 14 — Introduction to Memory Forensics

- 504ENSICS Labs. (2022, December 9). *LiME ~ Linux Memory Extractor* [Online forum post]. GitHub. <https://github.com/504ensicsLabs/LiME>
- baeldung. (2021, November 23). What Is an ELF File? <https://www.baeldung.com/linux/executable-and-linkable-format-file>
- Belkasoft RAM Capturer: Volatile Memory Acquisition Tool*. (2023). Belkasoft. Retrieved July 29, 2023, from <https://belkasoft.com/ram-capturer>
- [Dell XPS 15 9510 RAM Modules]. (2020, August 10). LaptopMedia.com. <https://laptopmedia.com/highlights/inside-dell-xps-15-9500-disassembly-and-upgrade-options/>
- Dell XPS 15 9510 with back cover removed* [Photograph]. (2020, August 11). Gear Open. <https://gearopen.com/wp-content/uploads/2020/08/Untitled-123.png>
- 5.2.14. */proc/kcore*. (2023). Red Hat. Retrieved July 29, 2023, from https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/4/html/reference_guide/s2-proc-kcore
- FTK® Imager*. (2023). Exterro. Retrieved July 29, 2023, from <https://www.exterro.com/ftk-imager>
- K, R. (2021, May 14). WinPmem : The Multi-Platform Memory Acquisition Tool. <https://kalilinuxtutorials.com/winpmem/>
- Kernel (operating system)*. (2023, July 19). Wikipedia. Retrieved July 29, 2023, from https://en.wikipedia.org/wiki/Kernel_%28operating_system%29
- [Laptop circuit board]. (n.d.). Dell Technologies. <https://dl.dell.com/content/manual21673621-xps-15-9510-service-manual.pdf?language=en-us>
XPS 15 9510 Service Manual
- Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory*. John Wiley & Sons, Inc.
- Live forensics, data recovery and eDiscovery over an IP network - using your choice of tools*. (n.d.). F-Response. Retrieved July 29, 2023, from <https://www.f-response.com/>
- MAGNET RAM Capture*. (2023). MAGNET Forensics. Retrieved July 29, 2023, from <https://www.magnetforensics.com/resources/magnet-ram-capture/>
- OpenText EnCase Forensic*. (2023). Opentext. Retrieved July 29, 2023, from <https://www.opentext.com/products/encase-forensic>
- Riofrio, M. (2020, January 8). *How Dell built 5G into the Latitude 9510* [Photograph]. PCWorld. <https://www.pcworld.com/article/3512880/dells-latitude-9510-shakes-up-corporate-laptops-with-5g-machine-learning-and-thin-bezels.html>

Tilbury, C. (2010, November 8). Digital Forensics How-To: Memory Analysis with Mandiant Memoryze. <https://www.sans.org/blog/digital-forensics-how-to-memory-analysis-with-mandiant-memoryze/>

Volatility Cheat Sheet (2.4 ed.). (2014). Retrieved July 28, 2023, from https://downloads.volatilityfoundation.org/releases/2.4/CheatSheet_v2.4.pdf

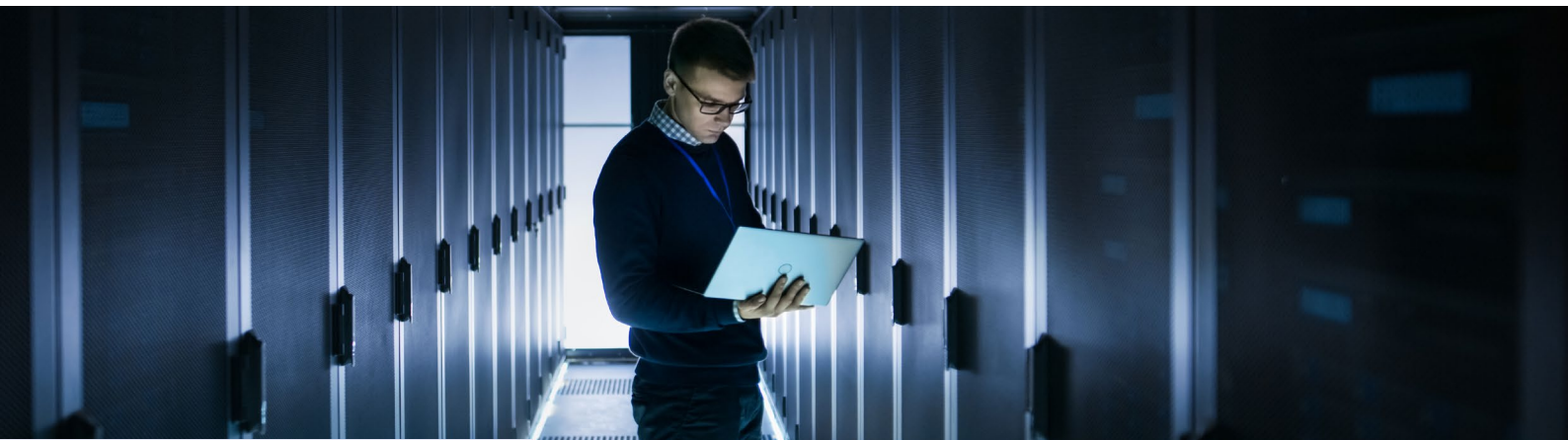
Digital Acquisition Tools

Disk Imaging Tool Name	Version	Download URL	OS				Evidence Device														Target Device								Methods		Supported image format																	
			Windows	Mac	Linux	Custom Boot	Standalone	Software	IDE	PATA	SATA	SCSI	SAS	PCle	Mini PCle	USB 2	USB 3	SCSI	Firewire	Thunderbolt	Compact Flash	Ethernet	SD Card	Software	IDE/PATA	SATA	PCle	SCSI	SAS	USB2	USB3	Thunderbolt	Compact Flash	Ethernet	Disk-to-Disk Copy	Disk-to-File Copy	Logical	Raw	Apple Disk Image	EX01	E01	AFF	ASB	Virtual Disk				
Atola Insight Forensic	4.8	http://atola.com/products/insight/	X					X	X	X		X	X			X					X	X		X	X							X	X	X	X	X			X									
Atola TaskForce	2020.7.1	https://atola.com/products/taskforce/					X		X	X	X		X	X		X	X			X	X	X		X	X							X	X	X	X	X					X							
Belkasoft Evidence Center	9.7	https://belkasoft.com/ec	X					X															X										X	X	X	X	X			X								
Cellebrite	3.2	https://www.cellebrite.com/en/digital-collector/	X	X			X	X	X														X											X	X	X	X	X		X	X							
Covert Forensic Imaging Device	3	http://www.sgcCanada.com/					X	X								X	X																	X	X	X	X	X		X	X							
Data Recovery System	16.7.1.122	http://www.salvationdata.com/drs-data-recovery-system.html	X						X	X	X					X	X							X	X		X	X	X	X	X	X	X	X	X	X	X	X		X								
DC3DD	7.2.646	http://www.dc3.mil	X	X	X			X															X											X	X	X	X	X										
Detego Ultimate Suite	3.4	http://www.teeltech.com/mobile-device-forensic-tools/detego-ultimate/	X	X		X					X					X	X			X														X	X	X	X	X		X								
Ditto DX Forensic FieldStation	2	https://wiebetech.com/products/ditto-dx-forensic-fieldstation/					X		X	X	X			X			X	X						X	X	X								X	X	X	X	X		X			X					
Ditto DX Forensic FieldStation	1	https://wiebetech.com/products/ditto-forensic-fieldstation/					X		X	X	X			X			X	X							X	X	X							X	X	X	X	X		X			X					
Ditto x86 BE		https://wiebetech.com/products/ditto-x86-be/				X		X															X											X	X	X	X	X		X			X					
Ditto x86 SE		https://wiebetech.com/products/ditto-x86-se/				X		X															X											X	X	X	X	X		X			X					
Fast Disk Acquisition System	2.0.1	http://www.cyanline.com					X		X	X					X				X	X	X					X								X	X	X	X	X		X			X					
Forensic Falcon	2.3	http://www.logicube.com/shop/falcon/					X		X	X		X	X			X	X	X			X		X		X	X		X	X	X	X	X	X	X	X	X	X	X	X		X	X		X				
Guymager		http://guymager.sourceforge.net/				X		X															X											X	X	X	X	X		X			X	X				
HardCopy 3P		https://www.voomtech.com/hardcopy-3p					X		X	X	X													X	X									X	X	X	X	X		X			X					
ILookIXimager	3.0/4.0	http://www.perlustro.com				X	X		X														X											X	X	X	X	X									X	
Magnet ACQUIRE	1.1	http://www.magnetforensics.com	X					X															X											X	X	X	X	X		X			X					
Magnet AXIOM	1.2.6	https://www.magnetforensics.com/magnet-axiom/	X					X																X										X	X	X	X	X		X			X					
MiniDAS	1	http://www.cyanline.com/minidas/				X		X																X										X	X	X	X	X		X			X					
OSForensics	8	http://osforensics.com/whatsnew.html	X					X															X											X	X	X	X	X		X			X	X	X	X		
PC-3000 Data Extractor	5.5.2	http://www.aceLab.eu.com/data-extractor-express.php	X					X	X	X	X	X	X								X		X	X	X	X		X	X					X	X	X	X	X		X			X				X	
SANAN Amphibious Incidence Response Utility		https://sananforensics.in/tools-catalog/	X					X															X											X	X	X	X	X		X	X							
Solo-101 Forensics	2011	http://www.ics-iq.com/Image-MASster-Solo-101-Forensic-Drive-Duplicator-p/f.gr-0054-000a.htm					X		X	X	X					X								X	X									X	X	X	X	X		X			X					
Solo-4 Forensics	2008	http://www.ics-iq.com/ImageMASster-Solo-4-Forensic-Hard-Drive-Duplicator-p/f.gr-0035-000e.htm					X		X	X	X		X			X			X		X			X	X		X							X	X	X	X	X		X			X				X	
SuperImager 7" Field Imaging and Triage Platform Unit	1.4.2.3	http://www.media-clone.com/cleanDS/SIM0001Brochures.pdf	X				X		X	X	X					X	X	X			X		X		X	X								X	X	X	X	X		X			X	X			X	
SuperImager 8" Field Unit	1.4.4.1	http://www.media-clone.net/SuperImager-8-Field-Unit-SAS-SATA-and-USB-3-0-p/sif-0017-00b.htm	X				X		X	X	X	X	X		X	X	X	X	X		X		X											X	X	X	X	X		X			X	X				
SuperImager Rugged 12" Field Computer Forensic Imaging and Field Platform	1.4.4.1	http://www.media-clone.net/SuperImager-Rugged-12-LCD-SAS-SATA-and-USB-3-0-p/sir-0024-00b.htm	X				X		X	X	X	X												X	X		X							X	X	X	X	X		X			X	X				
TD2	1	http://www.tableau.com/index.php?pageid=products&model=TD2					X		X	X	X		X			X								X										X	X	X	X	X		X			X					
TD3	1	http://www.tableau.com/index.php?pageid=products&model=TD3					X		X	X	X		X			X	X		X						X									X	X	X	X	X		X			X					
X-Ways Forensics	16.7	http://www.x-ways.com	X					X															X											X	X	X	X	X		X			X					
X-Ways Imager		http://www.x-ways.com	X					X															X											X	X	X	X	X		X			X					

PRODUCT OVERVIEW

OpenText™ EnCase™ Forensic

The industry standard for previewing, collecting, analyzing and reporting on digital forensic data for law enforcement, government agency and corporate investigations



Reliable acquisition of evidence



Deep forensic analysis



Mobile collection for 36,000+ profiles



Image analysis



Broad OS/decryption support



Connected to the cloud



Optical character recognition

For digital investigations, examiners need to be able to prioritize, collect and decrypt evidence from a wide variety of devices while maintaining its integrity. The process needs to be quick, efficient, repeatable and defensible, with the ability to create intuitive reports.

OpenText™ EnCase™ Forensic is recognized globally as the standard for digital forensics and is a court-proven solution built for deep-level digital forensic investigation, powerful processing and integrated investigation workflows with flexible reporting options. It is built with a deep understanding of the digital investigation lifecycle and the importance of maintaining evidence integrity. EnCase Forensic empowers any examiner to seamlessly complete any investigation, including investigations of mobile devices.

Reliable acquisition of evidence

With EnCase Forensic, examiners can be confident the integrity of the evidence will not be compromised. All evidence captured with EnCase Forensic is stored in the court-accepted EnCase evidence file formats.

Deep forensic analysis

EnCase Forensic has been used in thousands of court cases and is known for its ability to uncover evidence that may go unnoticed if analyzed with other solutions. EnCase Forensic doesn't just deliver an "artifacts first" approach but also lets investigators dive deep into the operating system to locate artifacts that would otherwise be well-hidden by bad actors.

"With EnCase Forensic, we see a significant improvement in our efficiency, allowing us to investigate more complaints and bring more offenders to justice."

Allen LaFontaine
Forensic Examiner
Southern Alberta Internet Child
Exploitation Unit

Mobile collection for 36,000+ profiles

EnCase Forensic supports the latest smartphones and tablets, including more than 36,000 mobile device profiles, all while empowering the examiner to conduct logical and physical acquisitions. From the new investigator to the seasoned examiner, each level of user can find the evidence they need with mobile acquisitions in EnCase Forensic.

Image analysis

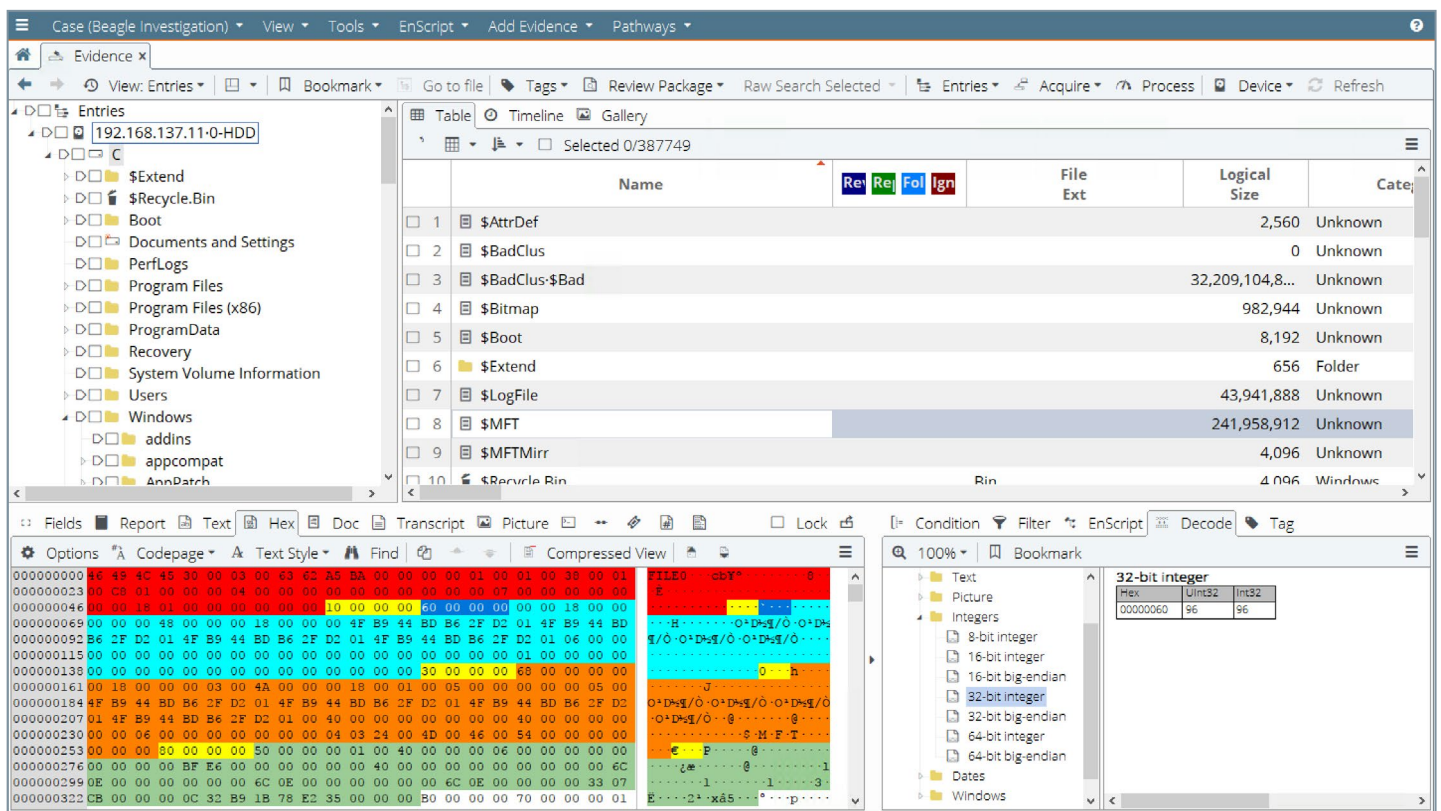
EnCase Forensic artificial intelligence capabilities process images into 12 categories using visual threat intelligence technology. Examiners can quickly filter by confidence level and identify previously unidentified contraband with near-zero false positives.

Broad OS/decryption support

Offering the broadest support of operating and file systems, artifacts and encryption types, EnCase Forensic enables the investigator to provide conclusive results with a detailed analysis of findings.

Connect to the cloud

With EnCase Forensic, digital forensic investigators can collect evidence from cloud-based applications, including social media, storage and communication tools.



Encase Forensic acquires data from a wide variety of devices, completes a forensically sound investigation and produces extensive reports.

OpenText offers a wide variety of professional training programs and certifications to help develop expertise in EnCase software and forensic security.

Police agencies, government agencies and corporations across the globe depend on EnCase Forensic for its functionality, flexibility and track record of court acceptance. Providing investigators with the information advantage needed to find the truth in data, EnCase Forensic makes the world a safer, more secure place.

OpenText EnCase Forensic features

Enhanced indexing engine	Empowers investigators to conduct investigations with powerful processing speeds, advanced index searching, comprehensive language support and optimized performance
Easy reporting	Provides customizable templates to help examiners create compelling, easy to read, professional reports that can be shared for every case
Extensibility	Offers extensibility through EnScripts, which are automated code commands that streamline and automate tasks and extend the capabilities of EnCase Forensic to help the examiners complete investigations more efficiently
Workflow automation	Delivers automated investigation workflows so examiners can easily navigate through EnCase Forensic to enhance how they uncover evidence
Updated encryption support	Provides encryption support for Microsoft® Windows® 10 Bitlocker XTS-AES, Dell® Data Protection 8.17 and Symantec® PGP v10.3; investigators can acquire encrypted evidence without worry about data corruption, damage or unnecessary delays
Apple File System (APFS) support	Supports APFS, the file system used in helping investigators conduct targeted data collections from APFS and send the output as an EnCase logical evidence file
Volume shadow copy capabilities	Examines Volume Shadow Snapshot (VSS) backups, also known as volume shadow copies, generated by Microsoft Windows, allowing investigators to recover deleted or modified files, as well as full volumes and learn what may have taken place on a system before the investigation
Apple T2 Security Bypass	Acquires machines equipped with Apple T2 Security chips without additional hardware, drive partitions, or hassle. And if the user is logged in, no credentials are required
AFF4 support	Provides physical and logical read capabilities to allow for ingestion of evidence from other investigative tools, enabling all relevant evidence to be collected within a single EnCase case file and helping investigators quickly gain a more comprehensive view of the evidence available to their case.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- [OpenText CEO Mark Barrenechea's blog](#)
- opentext.com/security