Chapter 4 Topics

This chapter covers the following topics and concepts:

- Using proper forensic procedure
- Handling evidence appropriately
- Different storage formats
- The process of forensically imaging a drive
- Acquiring RAID

Chapter 4 Goals

When you complete this chapter, you will be able to:

- Properly seize a suspect computer
- Prepare that computer for forensic examination
- Understand the various storage formats
- Image a drive
- Acquire RAID drives

Handling a Suspect Computer

The primary goal when handling a computer for forensic analysis is to preserve evidence and maintain its integrity. This involves a strict, documented procedure from seizure to analysis.

Key Takeaways

1. Don't Immediately Shut Down

Valuable evidence exists in the computer's live memory (RAM), which is **volatile data** that is lost when the power is cut. Before powering down, an investigator should:

- **Check for running processes and network connections** using commands like `netstat`, `net sessions`, and `openfiles`. This helps identify malware, unauthorized access, or open files.
- **Perform a memory capture** if necessary. Tools like OSForensics or FTK can create a "dump" of the system's memory, preserving the live state for later analysis.

- When shutting down, it is often better to **pull the plug** rather than performing a standard shutdown, as the normal process can alter or delete temporary files and other evidence.

---

2. Maintain a Strict Chain of Custody

The **chain of custody** is the most critical concept. It's a detailed log that tracks the evidence from the moment it's collected.

- **Documentation is essential:** Everything must be photographed and documented before being touched, including cable connections, peripheral devices, and the system's hardware configuration (noting BIOS/UEFI time).
- **Secure transport is mandatory:** Evidence must be transported directly to a secure lab without any stops. Any period where the evidence is unaccounted for breaks the chain of custody and can render the evidence inadmissible.
- **Every item needs a form:** Each piece of evidence (like a hard drive) must have its own chain of custody form.

---

3. Ensure Evidence Integrity with Hashing

To prove that no data was altered after collection, forensic investigators rely on **hashing**.

- **Create a forensic image:** A bit-for-bit copy of the original storage device is made. The original device is then secured and not worked on directly.
- **Generate a hash:** A hashing algorithm (like MD5 or SHA2) is used to create a unique digital fingerprint (a hash value) for both the original drive and the forensic copy.
- **Verify the copy:** If the hash values of the original and the copy match, it provides mathematical proof that the copy is an exact, unaltered duplicate. This is crucial for verifying the integrity of the evidence presented in court.

The Hunt for Digital Evidence 🕵️‍♀️

After securing a device, the core of the investigation begins. The main tasks are to **find, preserve, and prepare** evidence. Investigators must look beyond the obvious files and folders, as incriminating data is often hidden, deleted, or stored in temporary locations.

Key Takeaways

1. Know Where to Look for Hidden Data

Evidence resides in many places, not just in user-created files. The most forensically valuable data is often found in the system's operational areas:

- **Volatile Data:** This is the first priority as it disappears when the computer is shut down. It includes currently running processes and active network connections.
- **The Swap File (pagefile.sys):** This acts as virtual RAM on the hard drive. It can contain fragments of documents, passwords, browsing history, and other data that was recently in active memory. This data often persists even after a reboot.
- **Unallocated Space:** When a file is deleted, the data isn't immediately erased. It remains in "unallocated space" on the drive until new data overwrites it. Forensic tools can often recover partial or complete files from this space.
- **File Metadata:** This is "data about data." It includes file creation and modification dates/times, which are crucial for building a timeline. For images, **Exif data** can reveal the camera used, the date and time the photo was taken, and even the **GPS location**.

---

2. Build the Story with a Timeline

The goal is to reconstruct a sequence of events. This is done by creating a **timeline** that logically orders actions based on the timestamps and metadata recovered from files, system logs, and different devices. A clear timeline turns isolated pieces of data into a coherent narrative of what happened, when it happened, and who was involved. This step-by-step reconstruction is essential for explaining the events of a crime.

---

3. Present the Evidence Clearly and Simply

Finding the evidence is only half the battle. The forensic examiner must be able to present their technical findings in a way that is **logical, compelling, and easily understood** by a non-technical audience, such as a judge and jury. The ability to explain complex topics like recovering deleted files or interpreting network logs in plain English is a critical skill that can ultimately determine the outcome of a case.

Understanding Digital Storage in Forensics

A forensic investigator must be familiar with various types of physical storage media and the specialized file formats used to preserve digital evidence. Each storage type has unique characteristics and vulnerabilities that affect how evidence is handled and analyzed.

Key Takeaways

1. Know Your Storage Media

Different storage types require different handling procedures. The fundamental rule is to always create a forensic copy and work from that copy, never the original.

- **Magnetic Media (HDDs):** The traditional spinning hard drive.
    - **Vulnerability:** Susceptible to physical shock (from moving parts) and magnetic fields, which can destroy data. Requires careful handling and transport in anti-static bags.
- **Solid-State Drives (SSDs):** The modern standard using flash memory with no moving parts.
    - **Advantage:** Faster and much more resistant to physical damage than HDDs. Found in most modern computers, laptops, and tablets.
- **Optical Media (CDs, DVDs, Blu-ray):**
    - **Vulnerability:** Easily damaged by scratches, which can make data unreadable.
- **Tape Drives (DAT, DLT):** Primarily used for archival backups.
    - **Forensic Process:** Data from tapes must be restored to a forensically wiped hard drive before it can be analyzed.
- **USB Drives:** Use solid-state technology.
    - **Critical Handling:** Must be accessed in **read-only mode** or with a hardware write-blocker to prevent accidentally altering the data.

---

2. Data Hides in Unseen Places

A significant amount of evidence can be found in areas of a drive that are not visible to the operating system. An investigator must know where to look for intentionally or unintentionally hidden data.

- **Host Protected Area (HPA):** A hidden section of the drive reserved by the manufacturer, which can be used to hide data.
- **Slack Space:** This refers to unused space that can contain residual data.
    - **File Slack:** The space between the end of a file's actual data and the end of the last storage block (cluster) assigned to it.
    - **Volume Slack:** Space on a hard drive that exists outside of any defined partition.
- **"Bad" Blocks:** A user can manipulate the file system to mark healthy blocks as "bad," making the operating system ignore them. These blocks can then be used to store hidden information.

---

3. Use Standard Forensic File Formats

When a forensic image (a bit-for-bit copy) of a drive is created, it is saved in a special, verifiable format.

- **Advanced Forensic Format (AFF):** An open-source, flexible format supported by tools like Autopsy.
- **EnCase Format:** A proprietary format that includes a hash value to verify the image's integrity and prove it hasn't been altered.
- **Generic Forensic Zip (Gfzip):** Another open-source format used to store evidence from an examination.

Forensic Imaging: Creating a Digital Duplicate for Analysis

Forensic imaging is the process of creating a forensically sound, bit-for-bit copy of a storage device (like a hard drive). The core principle of digital forensics is to **never work on the original evidence**. Instead, all analysis is performed on this exact, verifiable copy.

Key Takeaways

1. The Process Requires Two Key Steps

Before imaging, you must:

1. **Use a Write Blocker:** The original evidence drive must be connected to a forensic workstation using a hardware **write blocker**. This device prevents the computer from making any changes (even accidental ones) to the original drive, thus preserving its integrity.
2. **Forensically Wipe the Destination:** The drive where the image will be stored must be "forensically wiped." This involves overwriting every single bit on the drive to ensure no old data can contaminate the new evidence image.

---

2. There are Manual and Automated Imaging Methods

While investigators should understand the manual process, most now use automated tools for efficiency and reliability.

- **Manual Method (Linux `dd` and `netcat`):** This foundational technique uses the `dd` command to perform a low-level, bit-for-bit copy of the drive. The data is then piped through `netcat` to transfer it over a network to a forensic server. This demonstrates the core principles of data acquisition.
- **Automated Method (FTK Imager & EnCase):** Tools like FTK Imager provide a user-friendly interface to perform the same task. The typical workflow is:
    1. Select "Create Disk Image."
    2. Choose **"Physical Drive"** as the source type to ensure a complete copy that includes deleted files and unallocated space.
    3. Select the source drive and the wiped destination drive.

3. Verification is the Most Critical Step

The most important part of the imaging process is **verification**. Automated tools like FTK Imager will create a **cryptographic hash** (e.g., MD5, SHA-1) of both the original drive and the newly created image file. If the two hash values match, it provides mathematical proof that the copy is a perfect, unaltered duplicate of the original evidence. This verification is essential for the evidence to be admissible in court.

Imaging with OSForensics

OSForensics is another graphical tool used to perform **forensic imaging**. The process is straightforward and emphasizes the critical need for evidence verification.

Key Takeaway: Verification is Mandatory

Like other professional forensic tools, OSForensics simplifies the creation of a bit-for-bit disk image. The user selects "Drive Imaging," chooses the **source drive** to be copied, and specifies a **target location** for the image file.

The most crucial feature, highlighted in the instructions, is that the **"verify image"** option is checked by default. The text explicitly warns the user not to uncheck this box. This feature automates the **hashing** process, creating a digital fingerprint of both the original drive and the new image and comparing them to guarantee an exact, unaltered copy. This verification is essential for ensuring the integrity and admissibility of the digital evidence.

Acquiring RAID in Digital Forensics

RAID (Redundant Array of Independent Disks) is a technology that combines multiple physical hard drives into a single logical unit. This is done to improve performance or provide redundancy against drive failure. Understanding the type of RAID is crucial for proper forensic acquisition. 💾

Common RAID Levels

- **RAID 0 (Striping):** Data is split across multiple disks. This is fast but has **no redundancy**. If one drive fails, all data is lost.
- **RAID 1 (Mirroring):** Data is duplicated, with an identical copy on each disk. This provides full redundancy.

- **RAID 5 (Striping with Parity):** Data is striped across multiple disks, but it also includes special data called **parity**. This parity information allows the array to be completely rebuilt if any single drive fails.

How Parity Works

Parity is calculated using a simple mathematical operation called **exclusive OR (XOR)**. By performing an XOR operation on the data from two drives, a parity value is created and stored on a third. If one of the data drives fails, you can simply perform the XOR operation again on the *surviving* data drive and the *parity* drive to perfectly reconstruct the lost data.

The Golden Rule of RAID Acquisition

How you image a RAID array depends entirely on its configuration.

- For **RAID 1 (Mirroring)**, it's acceptable to image each drive separately, as they are identical copies.
- For any array that uses **striping (RAID 0, RAID 5, etc.)**, you **must not** image the drives individually. Each drive only contains a fraction of the total data.
- **The correct procedure is to image the entire RAID array as a single logical volume.** This creates one large forensic image file that represents the complete, assembled data. Modern forensic tools like **FTK, EnCase, and OSForensics** have built-in functions to handle this complex acquisition process correctly.