Nulltack
Purple team bootcamp

DIGITAL FORENSICS

Prepared By:
Kazim Ali Obad

Supervisor:
Anmar Mohammed
Mohammed baqer

Contents

1. What is Digital Forensics?

Digital forensics is the science and art of collecting those footprints and turning them into evidence. Think of it like being the CSI team of cyberspace.

When hackers break into a system, our job is not just to kick them out. We need to:

- Collect the evidence
- Analyze it
- Understand what they did, how they did it, and how to stop them next time

2. Two Types of Digital Evidence

2.1 Volatile Data

Think of this like steam coming from your coffee cup. You can see it right now, but if you do not capture it immediately, it is gone.

Examples:

- RAM (Random Access Memory)
- Running processes
- Active network connections
- Open files and live sessions

Why is it volatile? It only exists while the system is powered on. The moment you shut down the machine poof all of that evidence disappears.

2.2 NonVolatile Data

This is like notes in a notebook they stay even after you close it. Even if the system shuts down, this data survives.

Examples:

- Hard drives (HDD)
- Solidstate drives (SSD)
- USB devices and flash drives

3. The Two Core Steps of Digital Forensics

Everything in digital forensics comes down to two steps:

Step 1 Acquisition: *Capturing evidence in a safe, unaltered way. Like taking fingerprints at a crime scene you capture without disturbing.*

Step 2 Analysis: *Digging into that evidence to figure out exactly what the attacker did, how they got in, and what they touched.*

4. Why Not Just Analyze the System While It Is Running?

You might think why not just jump straight in and analyze the live system? That sounds faster. But it is actually a bad idea, for two reasons:

Reason 1: You Could Destroy the Evidence

Running forensic tools directly on a live system can overwrite the very data you are trying to collect. Imagine walking through a muddy crime scene with white shoes you become part of the mess.

When you run tools on a live system, those tools write to the RAM, write to the hard disk, and can overwrite critical evidence that was sitting right there.

Reason 2: Time is Critical

Stopping the attack is always the first priority. You contain the threat first. Once things are secure, then you go back and analyze with clean, preserved copies of the evidence.

Golden Rule: *Always work on copies of the evidence. Never touch the original. The original must remain pristine.*

5. Why Digital Forensics Matters

Digital forensics is not just about catching hackers inside companies anymore. It plays a critical role in multiple areas:

- Incident Response understanding exactly how attackers broke in
- Legal and Compliance meeting requirements like HIPAA and PCI DSS
- Military and Cyber Warfare governments and militaries rely on forensic teams in real conflicts

6. Real World Cases

Let us look at some real cases that show just how powerful digital forensics is.

Case 1: Instagram Selfies That Exposed an Army

During the conflict in Ukraine, a Russian soldier named Alexander Sotkin posted selfies on Instagram. Seemed harmless, right?

Except those photos contained geotags location data embedded in the image metadata. Forensic analysis of the photos revealed the movement of Russian troops into Ukraine. A single selfie blew the cover off military operations.

Lesson: *Metadata is evidence. Even a selfie can trigger a geopolitical scandal.*

Case 2: The Fitbit That Solved a Murder

Connie Dabate was murdered at home. Her husband Richard claimed he was away and that an intruder attacked her. It sounded believable until police checked her Fitbit.

The Fitbit data showed Connie was alive and moving around the house for minutes after Richard claimed she was already dead. That data proved Richard was lying.

Lesson: *Wearable devices and IoT gadgets are evidence. Your steps, heart rate, and sleep data can testify in court.*

Case 3: The Apple Engineer Who Stole Secrets

Xiaolang Zhang was an engineer in Apple's autonomous car division. He resigned, saying he needed to go care for his mother in China. Before leaving, he downloaded gigabytes of data.

Suspicious network activity revealed:

- Bulk data transfers
- Secret files copied

When confronted, Zhang admitted to stealing trade secrets. The FBI got involved.

Lesson: *Network logs never lie. They showed exactly what the insider was doing, even when he tried to cover his tracks*.

7. Types of Digital Forensics

Digital forensics is not one single skill it covers multiple areas. Here are the four main types:

7.1 Disk Forensics

Extracting and analyzing data from storage drives hard drives, SSDs, USB sticks, and so on. Think of it like searching through a closet full of evidence boxes.

7.2 Memory Forensics

Analyzing the RAM to capture what is happening right now inside the system. This is critical for catching fileless malware malware that runs entirely in memory and never touches the disk.

Think of it like checking the suspect's brain in real time.

7.3 Network Forensics

Analyzing the traffic flowing between devices. Who talked to who? What data left the building? It is like reviewing security camera footage, but for network conversations.

7.4 Application Forensics

Digging into application logs, configurations, and databases to see how attackers interacted with software.

Important: *Real world attacks usually require more than one type. A hacker stealing data shows up in network logs. Tools dropped on the system show up in disk forensics. Stealthy malware is only revealed through memory forensics.*

8. The Evidence Acquisition Process

Before analysis, we must collect evidence safely and properly. Just like sealing a crime scene, digital evidence must be:

- Authentic it must be the real thing
- Untouched we do not alter the original
- Verifiable we can prove nothing was changed

Step by Step Acquisition

Step 1: Acquire the evidence (memory image or disk image) Do not touch the original. Make a copy.

Step 2: Hash it using two algorithms (MD5 + SHA1) A hash is a digital fingerprint. If even one single bit changes, the fingerprint will not match. This proves the evidence was never altered.

Step 3: Make another copy of the acquired evidence One copy goes to analysis, one copy goes to safe storage in case you need it later.

Golden Rule: *Always work on copies. Originals must remain pristine and untouched.*

9. Typical Investigation Order

When a cybercrime happens, professionals follow this order and there is a reason for it:

First: Memory Image Grab the RAM first. Volatile data disappears fast. This is always the first priority.

Second: Triage Image Quick capture of the most critical data on the system.

Third: Disk Image The full copy of everything on the hard drive.

This way, nothing is lost even if the system gets powered off later.

10. Memory (RAM) Acquisition

Why do we capture RAM from Windows systems? Because RAM holds evidence that exists nowhere else:

- Running programs and active processes
- Passwords stored temporarily in memory

- Malware running only in memory never written to disk
- Active network connections

If a system is hacked, a memory image is critical to understand what happened.

10.1 Challenges When Capturing RAM

Challenge 1: Footprint

The acquisition tool itself uses some RAM while it runs. This means it can accidentally overwrite the evidence you are trying to capture. A smaller footprint is always better the less the tool touches memory, the more evidence you preserve.

Analogy: Imagine you are copying notes from a chalkboard, but your hand erases some words as you write. A smaller hand erases less so you preserve more of the original notes.

Challenge 2: Mode of Operation (User Mode vs Kernel Mode)

Tools can run in two modes:

- User Mode Works like a normal program. Can only see parts of memory that are accessible to regular applications. Some hidden areas remain out of reach.
- Kernel Mode Works at the operating system level. Can access all memory, including protected regions. Can bypass protections like antidumping and anti debugging.

Analogy: Think of a building. User Mode means you are only allowed on the public floors. Kernel Mode means you have the master key and can open every locked room.

Challenge 3: Speed

RAM changes every second. Some malware is even designed to wipe itself if it detects you are investigating. The faster the tool captures memory, the more accurate and complete the evidence.

Analogy: It is like taking a photo of a whiteboard while someone is erasing it. Fast photo you capture everything. Slow photo half the board is already gone.

11. Memory Acquisition Tools Comparison

Here is a comparison of the most common memory acquisition tools, evaluated on footprint, mode, and speed:

Tool	Footprint	Mode	Speed (6GB)	Notes	Best For
DumpIt v1.3.2	0.66 MB	Kernel	~2 min	Single image	Speed + minimal footprint
Belkasoft RAM	2.1 MB	Kernel	~1214 min	Pause/Resume supported	Advanced protection bypass
Nigilant32 v1.1	1.5 MB	Kernel	~2 min	Single image	Good balance / fast
Magnet RAM	1.8 MB	User	~67 min	Splits output files	Chunked output needed
FTK Imager v3.1.1	17.4 MB	User	Slow	Part of FTK suite	Already using FTK

Practical Recommendations

- Dump It Best for speed and minimal footprint. Fast and safe.
- Belka soft RAM Capturer Best if you need pause/resume or need to bypass advanced protections.
- Nigilant32 Good balance. Fast but simple.
- Magnet RAM Capture Best if you need to split files into chunks.
- FTK Imager Best if you are already working within the FTK forensic suite.

How to Choose: The Three Factors

When picking a memory acquisition tool, ask yourself:

Factor 1 Footprint: Does it use as little RAM as possible? (smallest footprint)

Factor 2 Mode: Does it run in Kernel Mode so it can see everything, including hidden areas?

Factor 3 Speed: Does it capture memory quickly, before it changes or gets wiped?

12. The Forensic Investigator Mindset

Digital forensics is not just about running tools. You have to think like a detective. Every single artifact has meaning:

- Every process running on the system is a footprint
- Every network packet captured is a witness
- Every hard disk sector is a crime scene