

UNLOCKING THE COMPUTER'S LIVE THOUGHTS:

MEMORY ANALYSIS

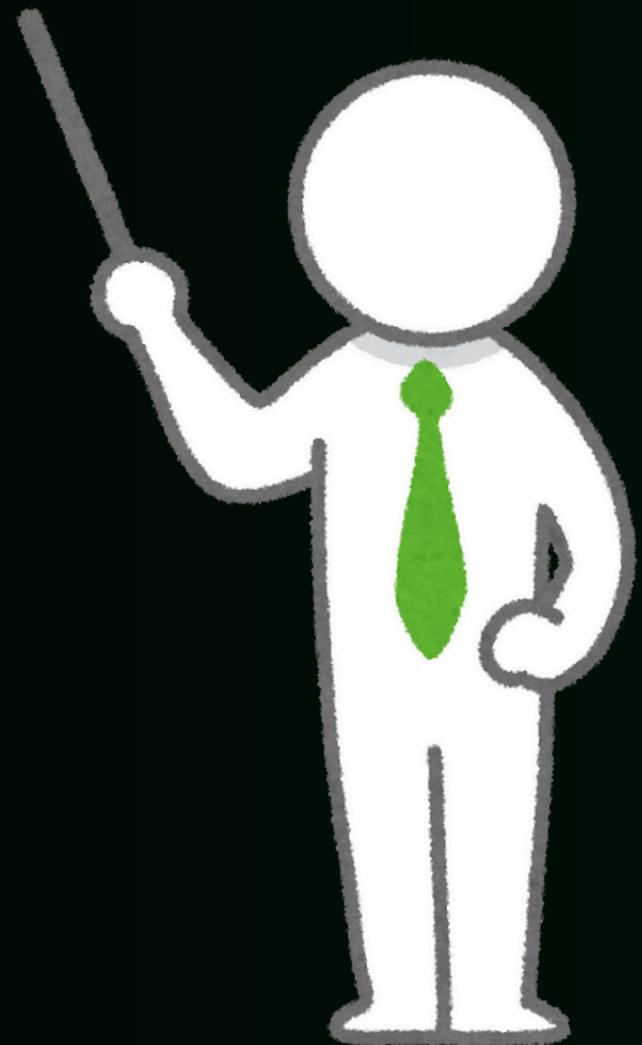
A Beginner's Journey from RAM Basics to Live Analysis

HI, I'm Foxy!

- 2nd year Degree IT (Computer Forensic)
- Seasonal CTF player
- MCC 2024 alumni
- RE:UN10N member

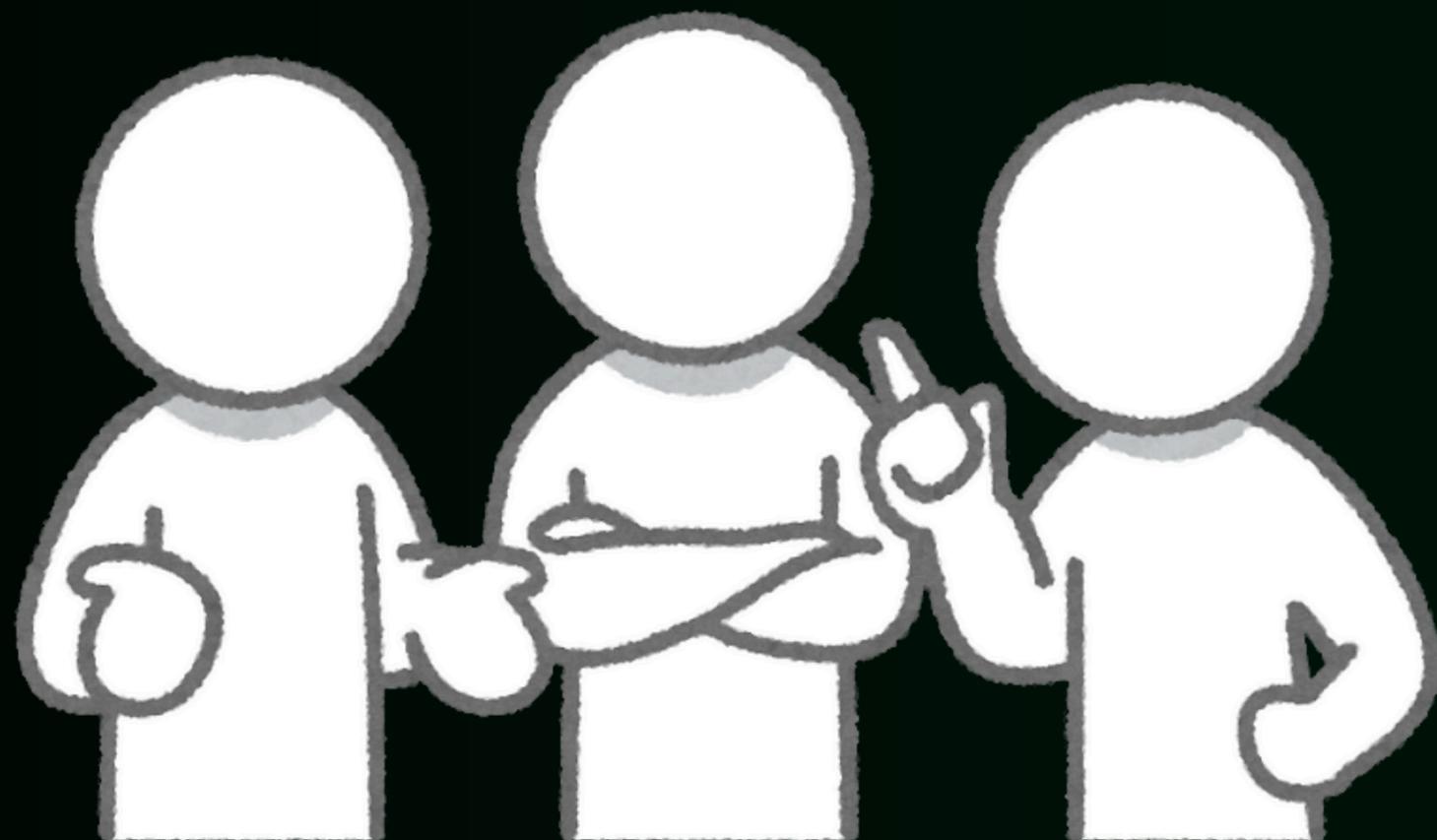


Before we start....

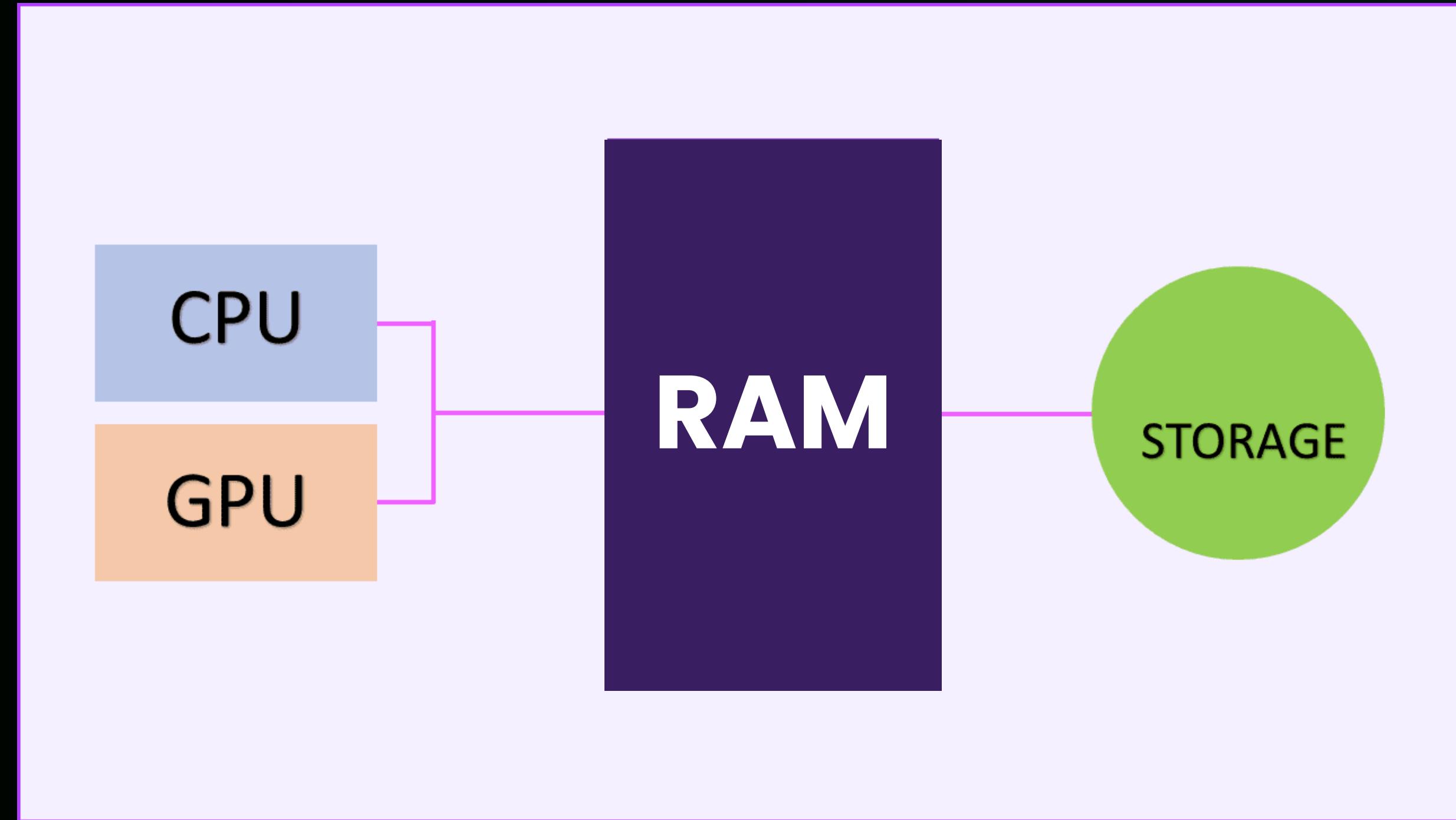


CTF vs Industry

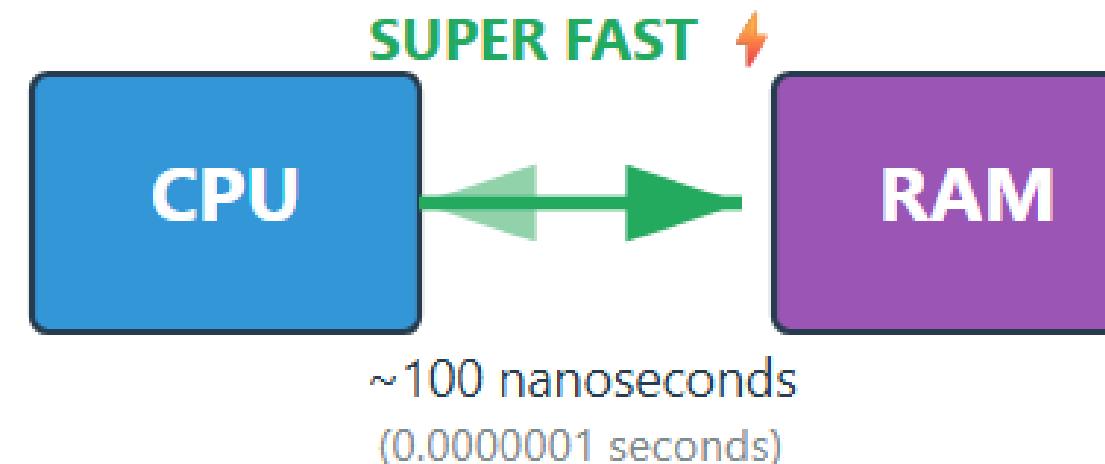
What's the difference?



Computer Fundamental



Speed Comparison: How Fast Can CPU Access Data?

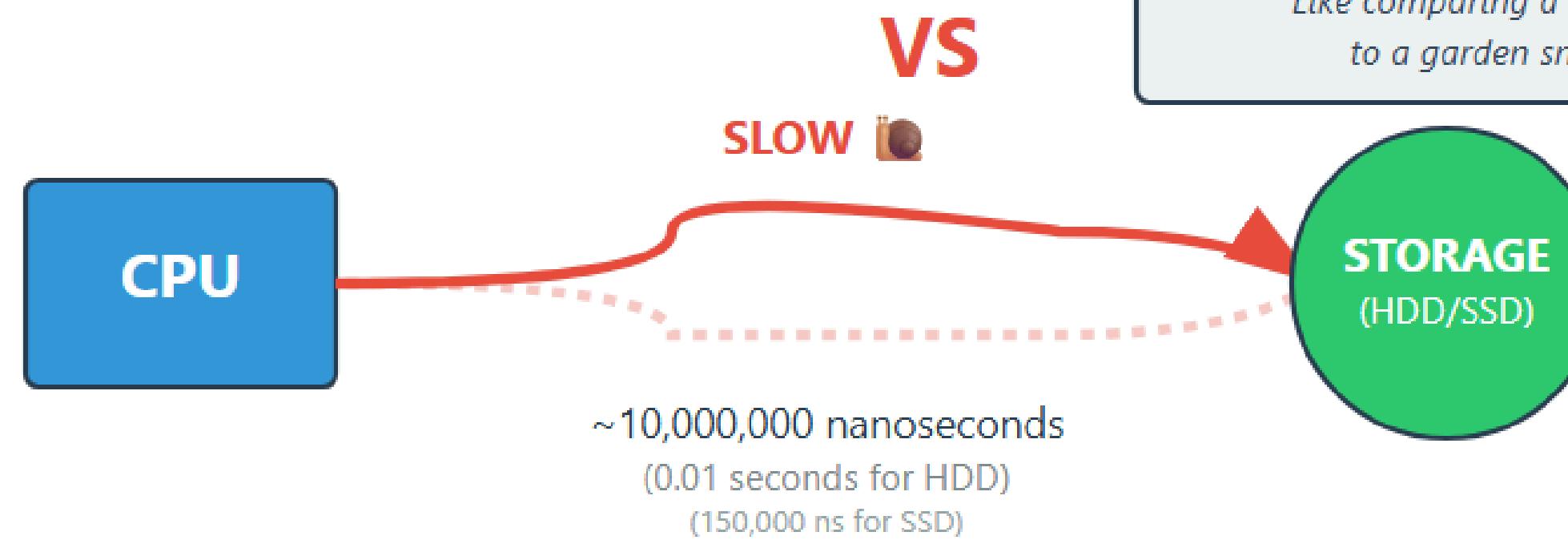


The Difference:

SSD: 1,500x slower
(~150,000 nanoseconds)

HDD: 100,000x slower
(~10,000,000 nanoseconds)

Like comparing a Ferrari 🚗 to a garden snail 🐌



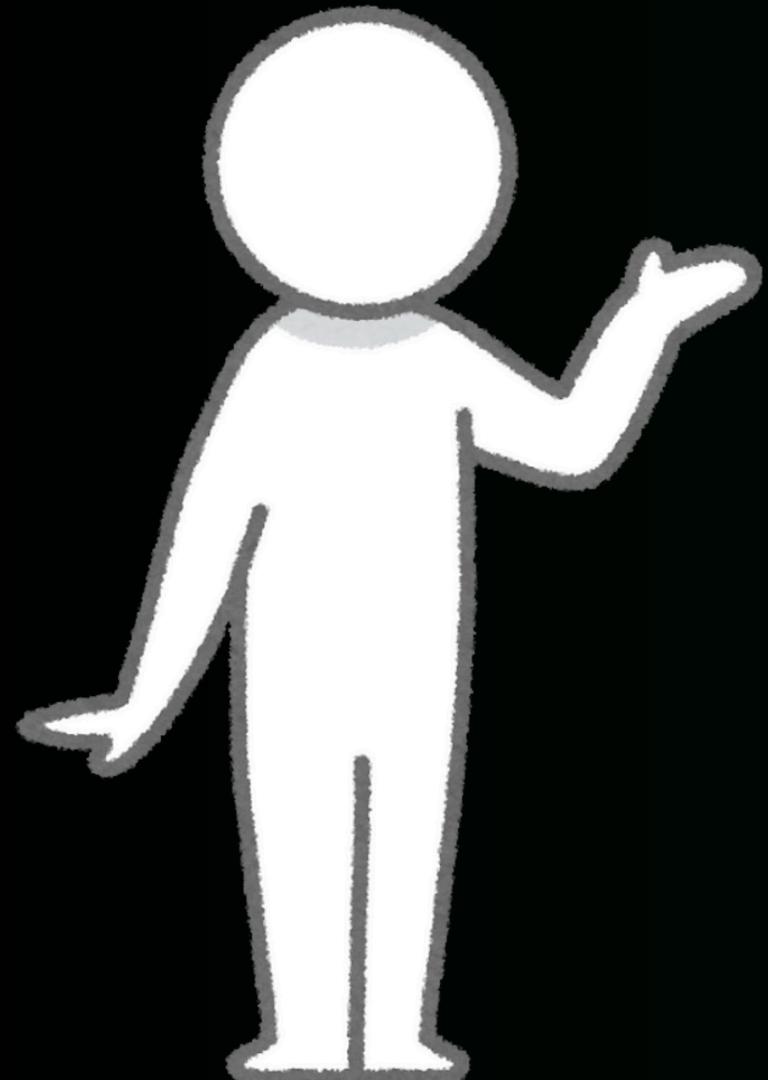
Source: "Latency Numbers Every Programmer Should Know" (Jeff Dean, Google)



**RAM is fast.
WHY?**

It's by design.





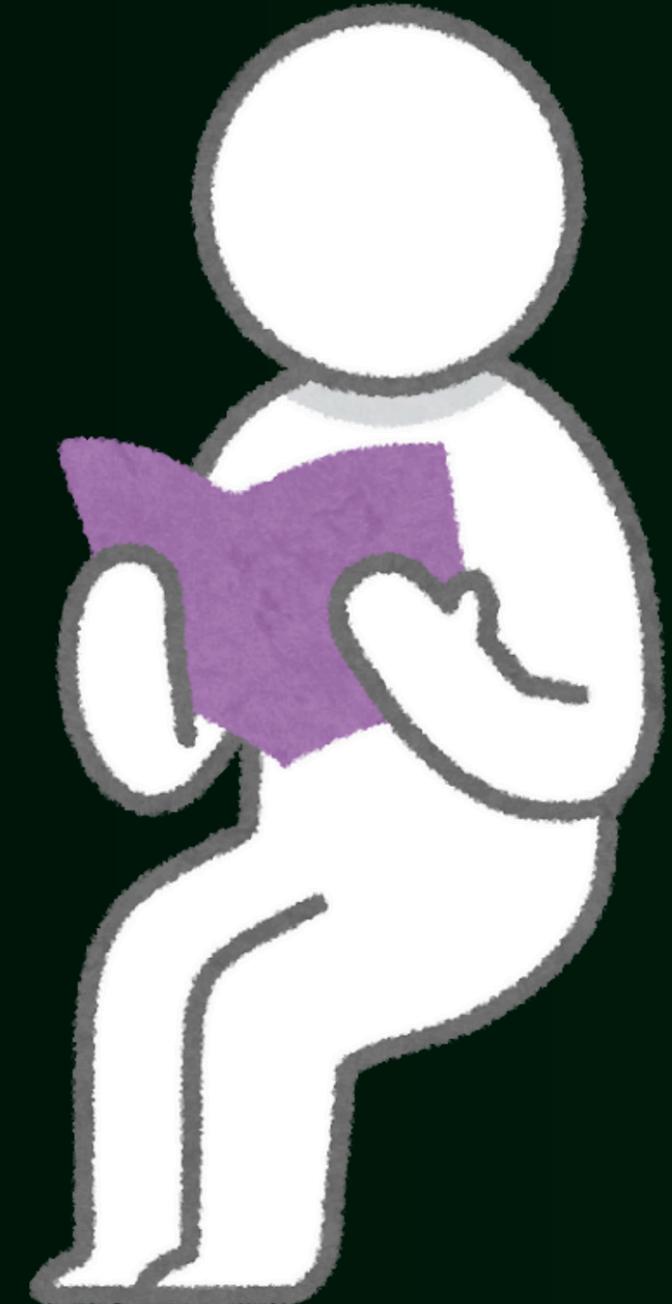
This is what we call **volatile memory**. THIS is why memory forensics exists and why we need to act FAST during incidents.



So... What is
inside **RAM**?

When a **system** is running, **RAM** may contains:

- Running processes
- Passwords in PLAINTEXT
- Active network connections
- Command history
- Encryption keys
- Recently typed data



DIGITAL FORENSIC

Introduction to digital forensic

DIGITAL FORENSICS



01 | Computer Forensics



02 | Network Forensics



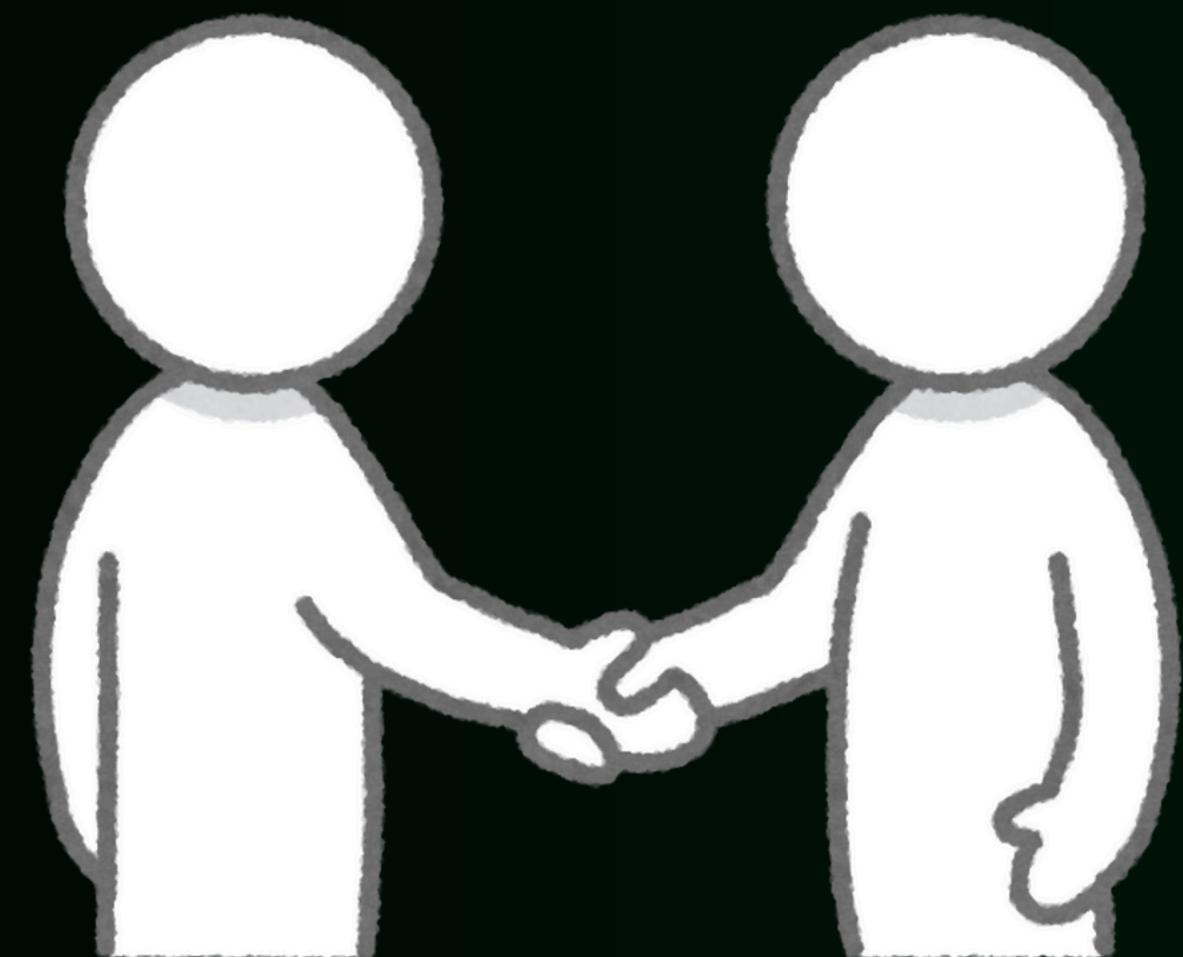
03 | Database Forensics



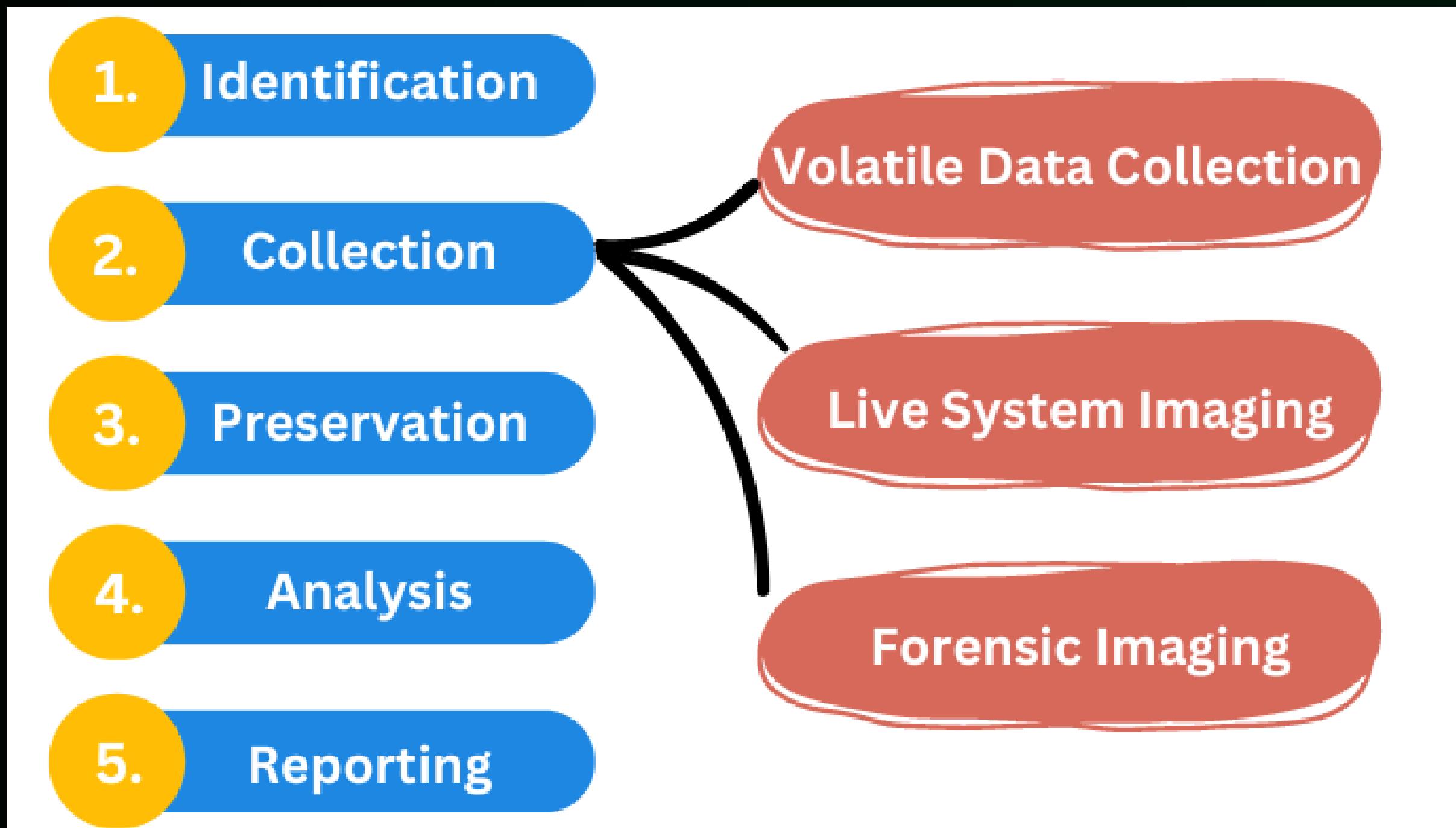
04 | Mobile Device Forensics



All the components
working together.



Investigation Framework, ICPAR

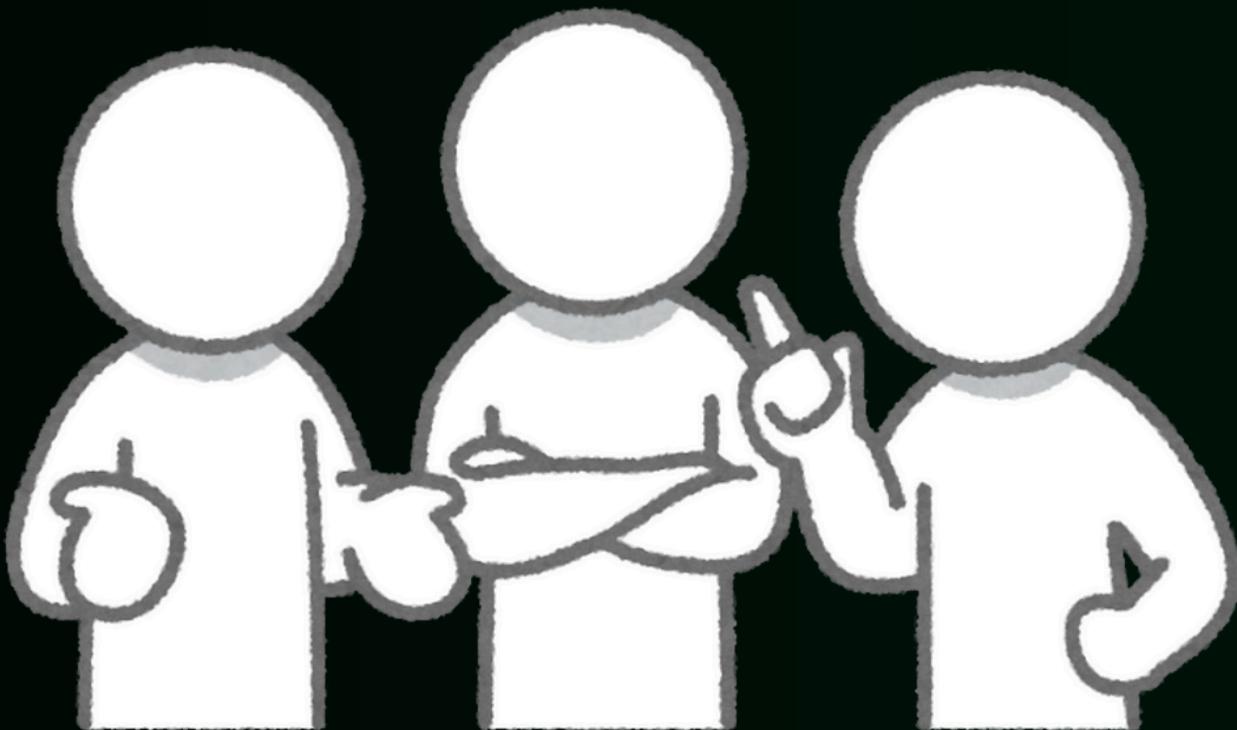


MEMORY FORENSICS

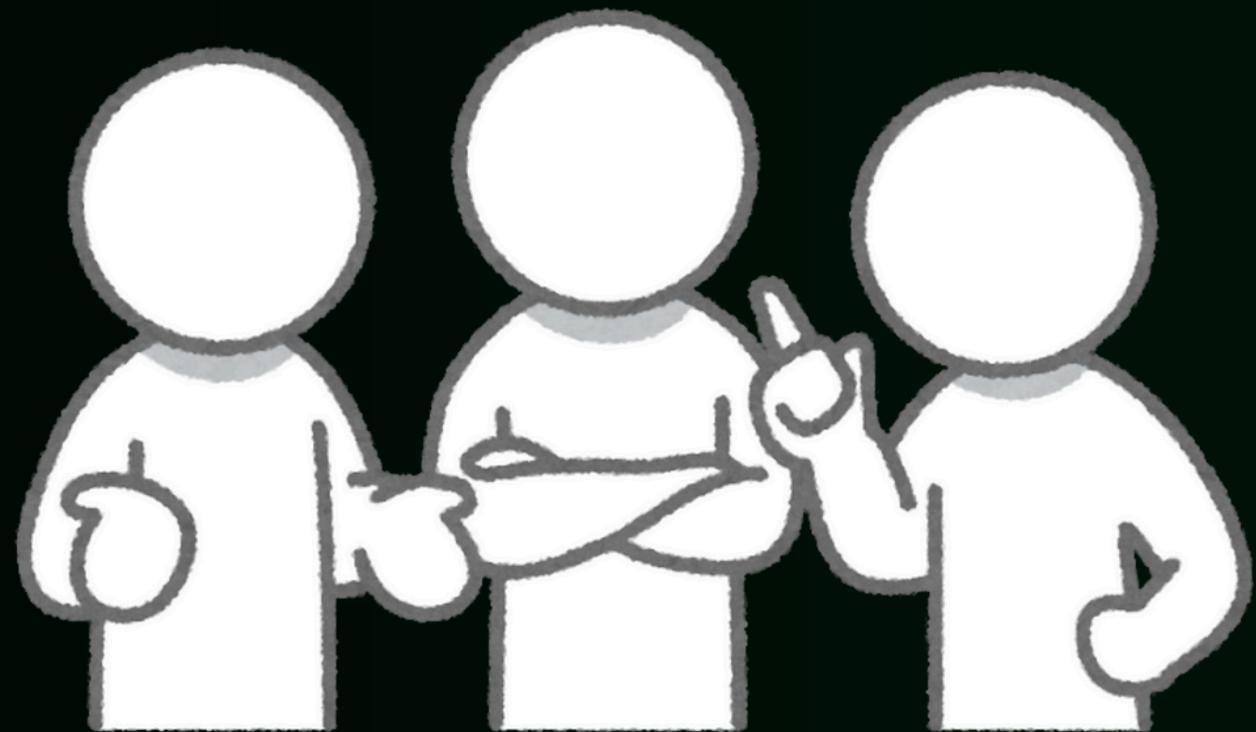


So what is
memory forensic?

Simply put: it's **analyzing RAM** to **find evidence** of what was **running** at a **specific moment** in **time**.



Attackers know about disk forensics. They know their files might get recovered. So **modern attackers** are getting **sneaky** so they're **living in memory**.



You know how **attackers**
look like when they
discover **fileless malware**
is a thing?



← Attackers

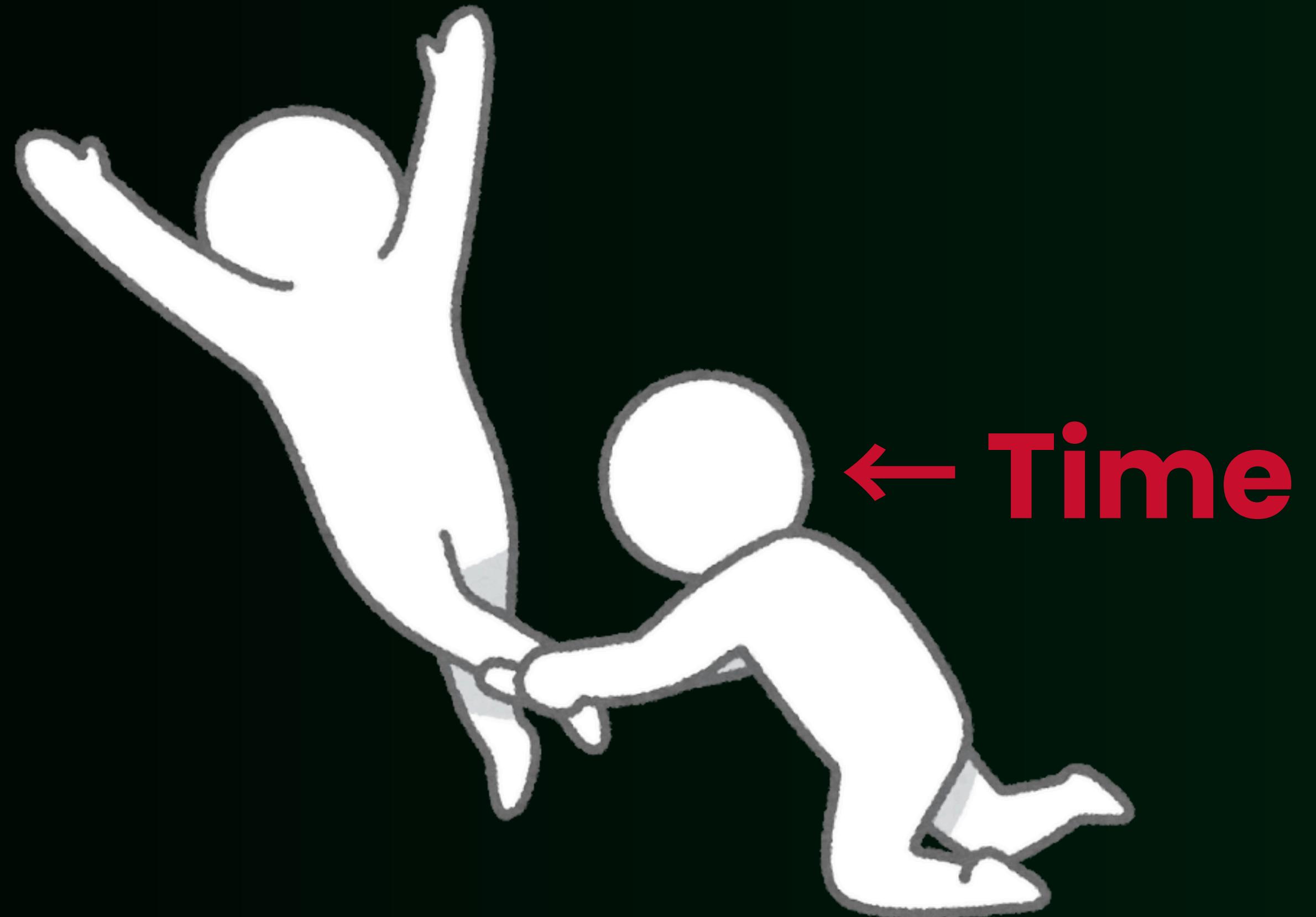
JK. Dear attackers,
Plez don't attack me..





Challenges of memory forensic

Digital Forensic investigators ->



Example case:

The screenshot shows a web page from the website [gbhackers.com](#). The header features the site's logo in red text "gbhackers." followed by a navigation menu with links to "HOME", "THREATS", "CYBER ATTACK", "DATA BREACH", "VULNERABILITY", "WHAT IS", and "D". Below the header is a large graphic of a blue shield with the letters "EDR" in red. The main content area includes a timestamp "Cyber Security News | Tools" and a "2 min. Read" indicator. The main title of the article is "EDR-Freeze: Technical Mechanics and Forensic Artifacts Exposed".

Cyber Security News | Tools 2 min. Read

EDR-Freeze: Technical Mechanics and Forensic Artifacts Exposed

Example case:

The screenshot shows a website with a dark purple header. The header features the word "Tracepoint" in large white letters. Below it is a navigation bar with links: Home, About, Blog, Projects, Certifications, and Contact. To the right of the navigation bar is a circular profile picture of a person with short hair. The main content area has a dark background with white text. It includes a link to "Back to Writeups". Below this, there is a section titled "EDR-Freeze - Forensic Analysis of an EDR Coma Attack" with two blue circular tags below it labeled "DFIR" and "Memory Forensics". A descriptive paragraph follows, and at the bottom, there is a question "What is "EDR-Freeze""?

Tracepoint

Home About Blog Projects Certifications Contact

- Back to Writeups

EDR-Freeze - Forensic Analysis of an EDR Coma Attack

DFIR Memory Forensics

This analysis walks through the inner workings of the EDR-Freeze technique - from thread suspension and handle manipulation to the forensic artifacts it leaves in memory - and highlights how defenders can detect and investigate such activity.

What is "EDR-Freeze"?

Forensic case study (memory image indicators) by tracepoint:

This section documents the memory artifacts you should expect when **EDR-Freeze** is applied to a security process such as `MsMpEng.exe` (Windows Defender). All example commands are memory-analysis oriented and use **Volatility 3/MemProcFS**.

Context: this was a controlled environment where the only action performed was suspending `MsMpEng.exe`. I intentionally skip basic enumeration plugins (`pslist`, `psscan`, `filescan`) – we already know the process exists and how the PoC was executed. Instead we focus on the *underlying mechanisms and forensic signals* that memory forensics uniquely reveals.

Correlated thread evidence - MsMpEng ← WerFaultSecure

Our PIDs of interest are: 1) 3428 -> MsMpEng.exe 2) 10892 -> WerFaultSecure.exe 3) 5648 -> EDR-Freeze 1.0 4) 10724 -> PowerShell.exe (to some extent)

Starting with enumerating suspended threads, I attempted to utilize the `windows.suspended_threads` plugin for Volatility3, but it returns an error and no results are printed so I shifted to MemProcFS.

B82	□	3428	764	fffffc984bcf8a0c0	Waiting	Suspended	2025-09-26 08:35:08	0	0	0	0	ffff875c1c320	ffff875c722a0	0	0	b140876000	b140880000	b140870000	ffff9c8000dc0000	ffff
831	□	3428	424d	fffffc984c462b000	Waiting	Suspended	2025-09-26 08:35:31	0	0	0	0	ffff875c1c320	ffff875c722a0	0	0	b14887c000	b141880000	b141870000	ffff9c80076356000	ffff
B83	□	3428	7980	fffffc984c37020c0	Waiting	Suspended	2025-09-26 08:39:31	0	0	0	0	fffffb30986d59650	fffffb795c722a0	0	0	b140878000	b141780000	b141770000	ffff9c8005af5000	ffff
1984	□	18982	1268	fffffc984c1cc7000	Waiting	Suspended	2025-09-26 08:35:41	0	0	0	0	ffff875c1c320	ffff875c722a0	0	0	c983613000	c983a00000	c9839fd000	ffff9c8007287000	ffff
1985	□	18982	9428	fffffc984c49f4000	Waiting	Suspended	2025-09-26 08:35:41	0	0	0	0	ffff875c1c320	ffff7346f23d0	0	0	c98360d000	c983800000	c983875000	ffff9c80077cc000	ffff
1986	□	18982	9816	fffffc984c1145000	Waiting	Suspended	2025-09-26 08:35:41	0	0	0	0	ffff875c1c320	ffff875c722a0	0	0	c983611000	c983980000	c98397d000	ffff9c8004781000	ffff
1987	□	18982	30472	fffffc984c50ab000	Waiting	Suspended	2025-09-26 08:35:41	0	0	0	0	ffff875c1c320	ffff875c722a0	0	0	c98360f000	c983900000	c9838fe000	ffff9c8006cf000	ffff



**THIS CASE IS FASCINATING
BECAUSE IT SHOWS HOW
SOPHISTICATED ATTACKERS
HAVE BECOME AND HOW
MEMORY FORENSICS CAUGHT
THEM ANYWAY.**

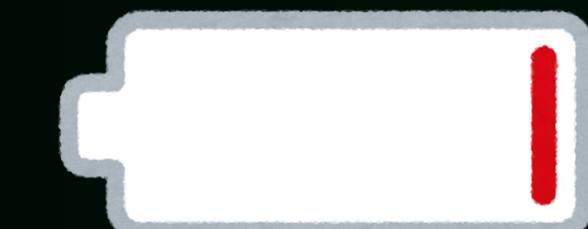
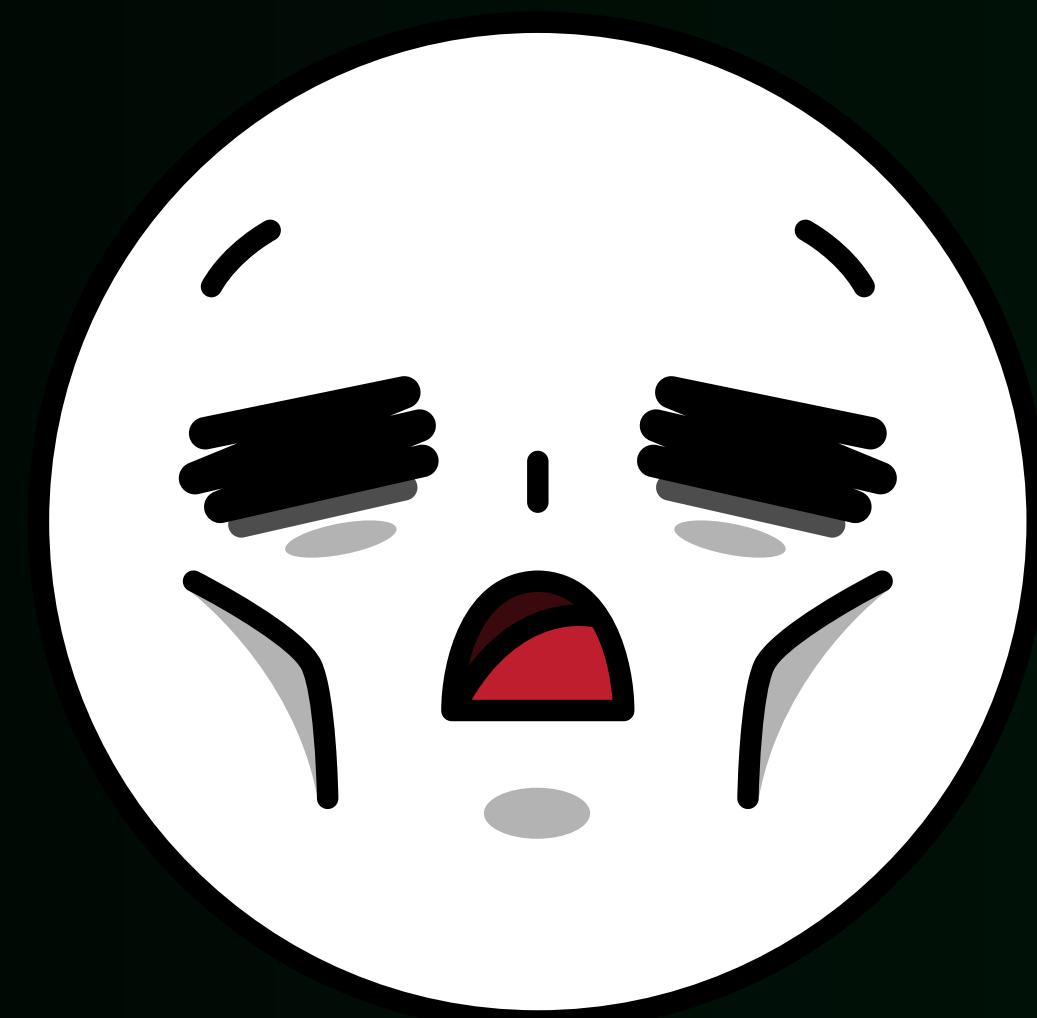


CONGRATS!



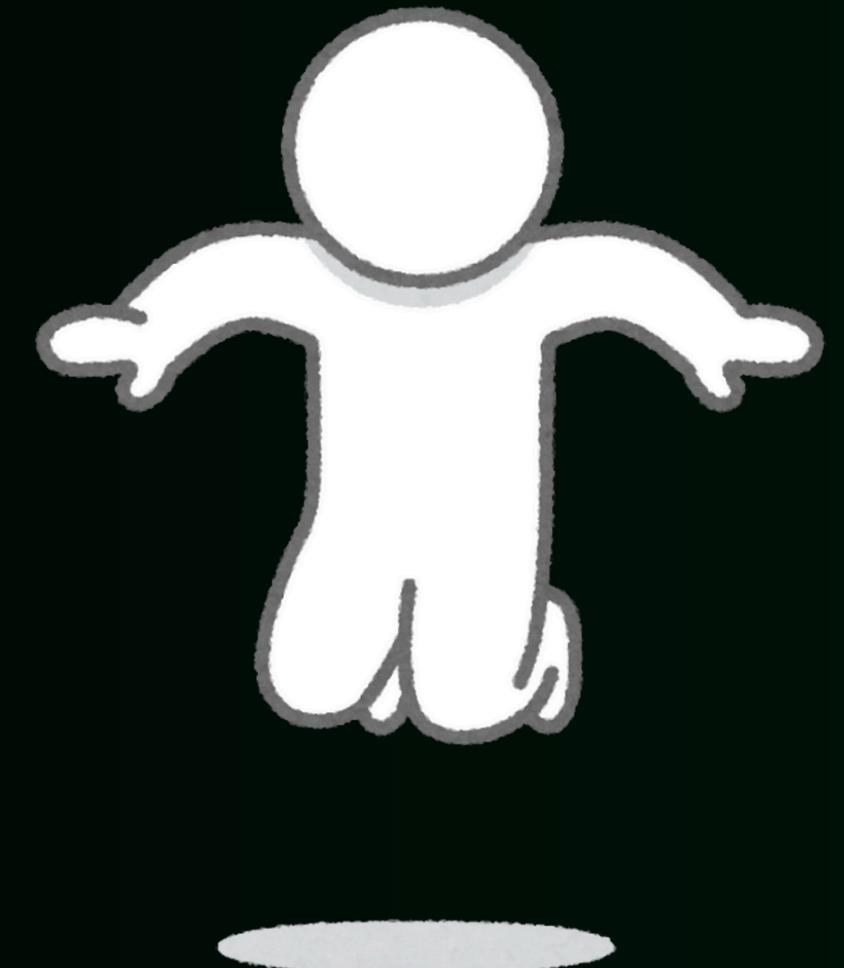
**NOW YOU KNOW
THE THEORIES IN
MEMORY FORENSIC**

5 MIN BREAK

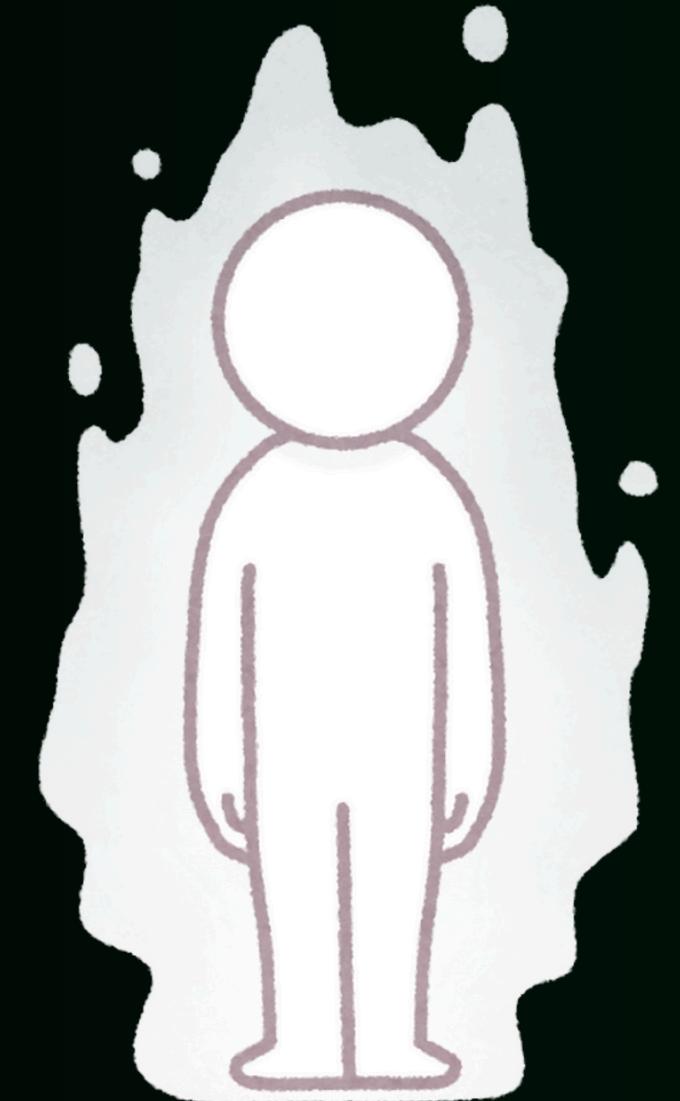


LET'S DO IT

LET'S DO 1 CHALLENGE TOGETHER USING VOLATILITY 3!



PRIZE!
FOR THE BEST WRITEUP.



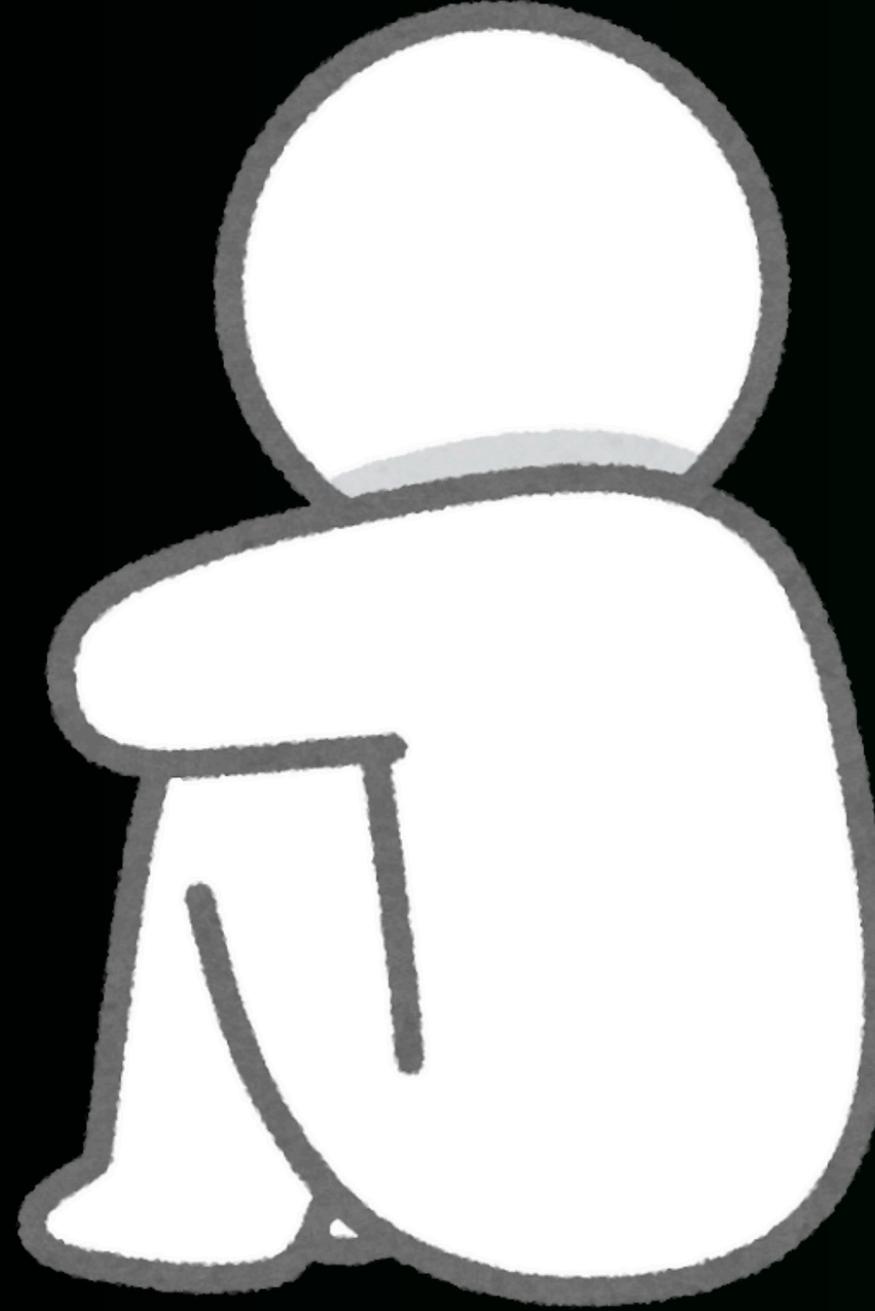
GROUND RULES!

1. NO GPT
2. NO COPYING OFF OTHER PEOPLE'S WRITING
3. ABLE TO DESCRIBE THINKING PROCESS

WINNER GETS...



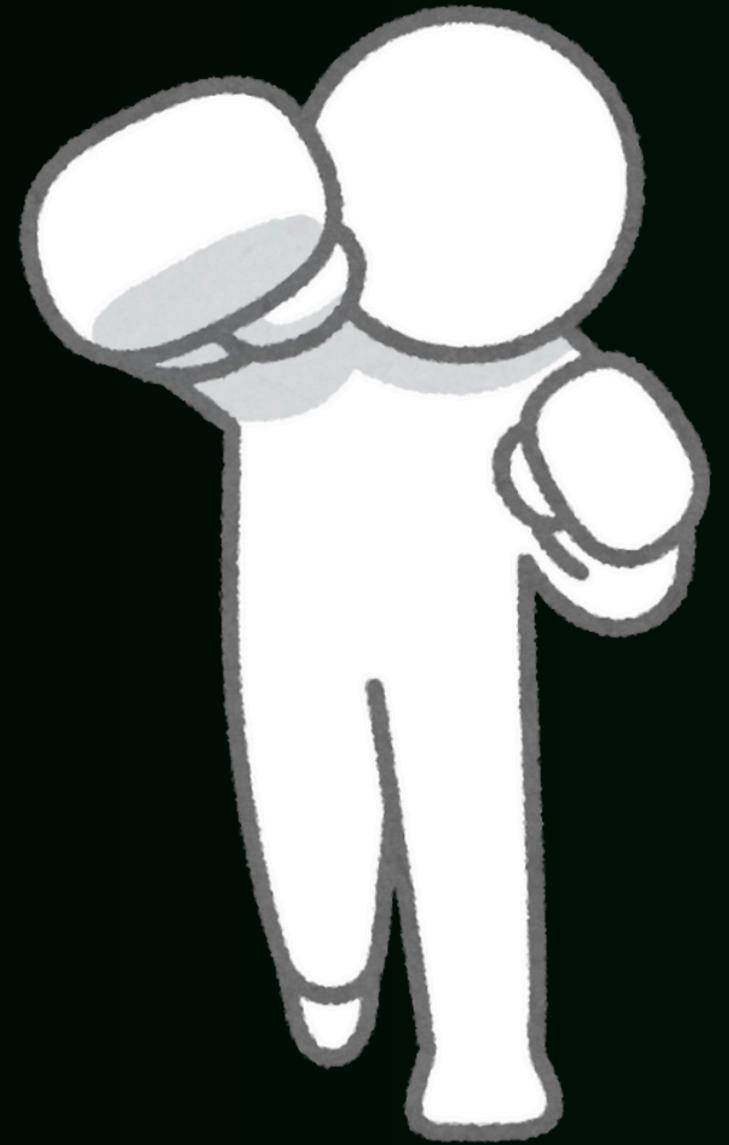
SOME KIND OF VOUCHER....
I THINK...



WIN FIRST THEN
YOU'LL KNOW.



**SUBMIT
WRITEUP LINK
TO FOXY BEFORE
4.20PM**



THANK YOU

FOR YOUR ATTENTION