FOXY | MCC ALUMNI 2024

CSLU IIUM

UNLOCKING THE COMPUTER'S LIVE THOUGHTS:

MEMORY ANALYSIS

A Beginner's Journey from RAM Basics to Live Analysis

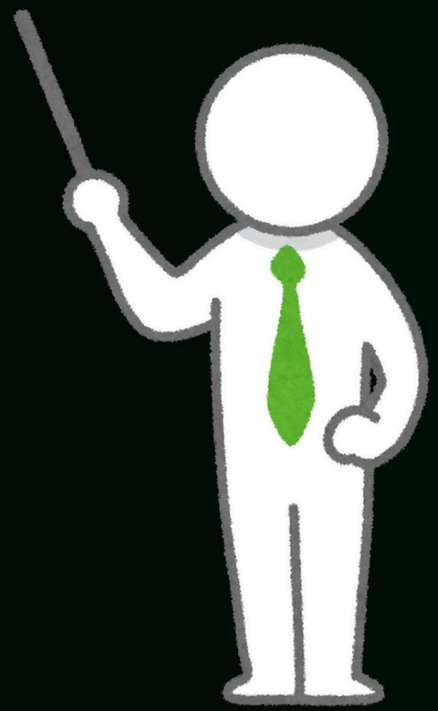
HI, I'm Foxy!

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

MCC
MALAYSIA CYBERSECURITY CAMP

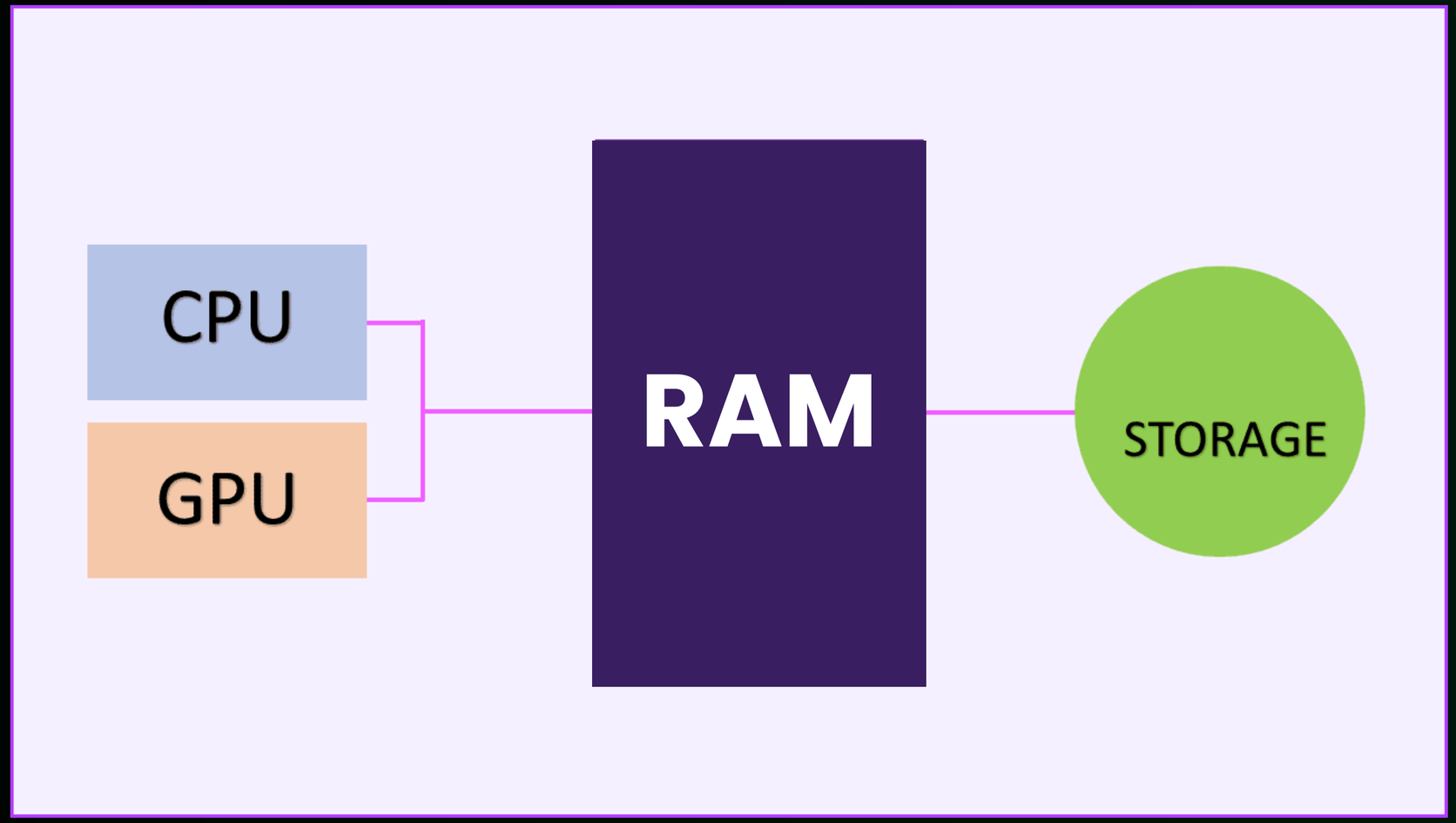
RE:UN1ON
WE PLAY WE LEARN

Before we start....

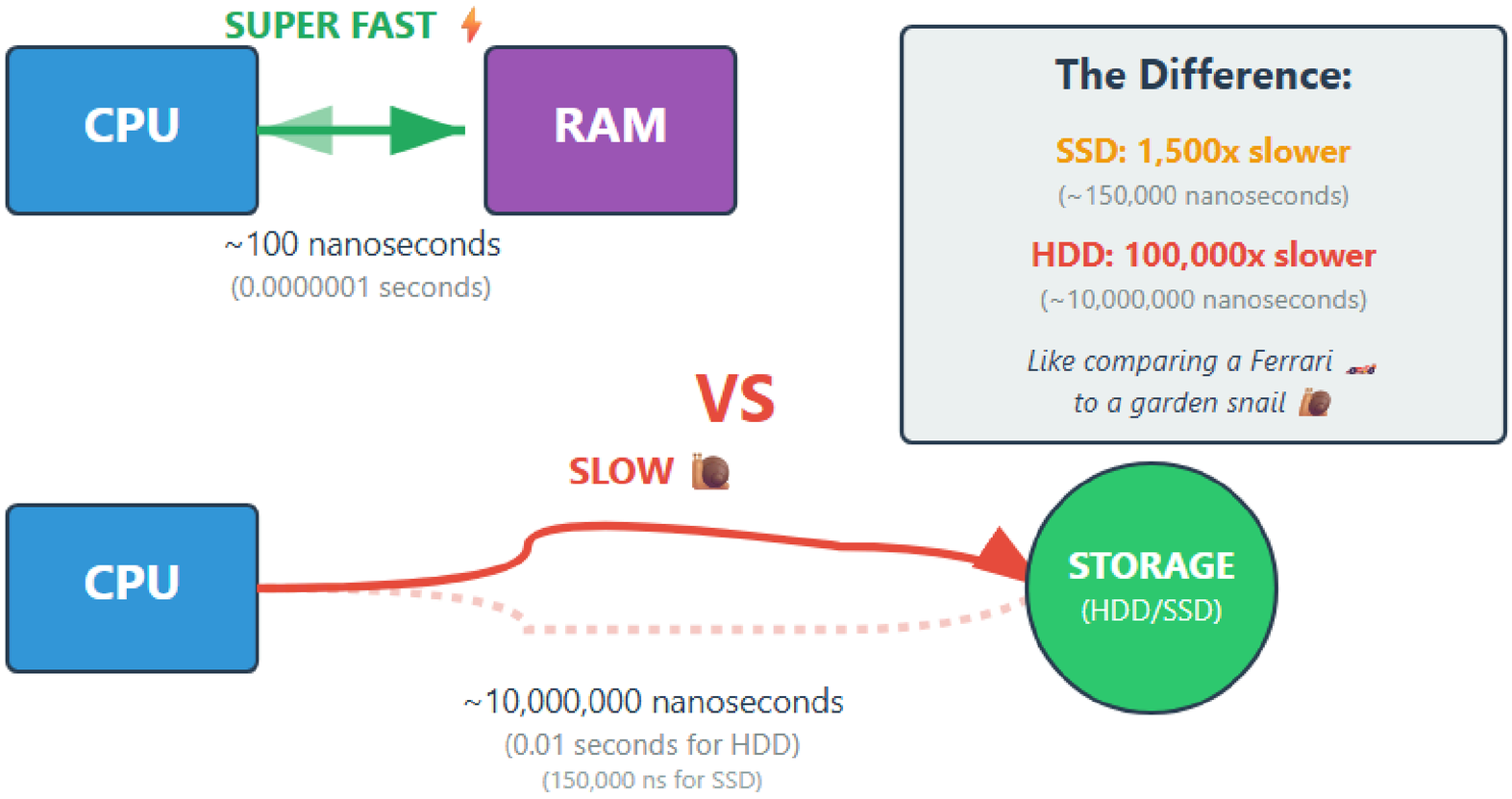


CTF vs Industry
What’s the difference?

Computer Fundamental



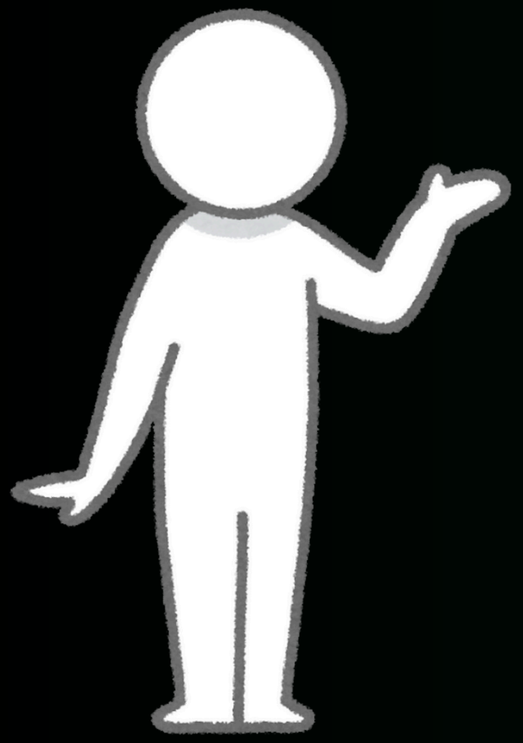
Speed Comparison: How Fast Can CPU Access Data?



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.

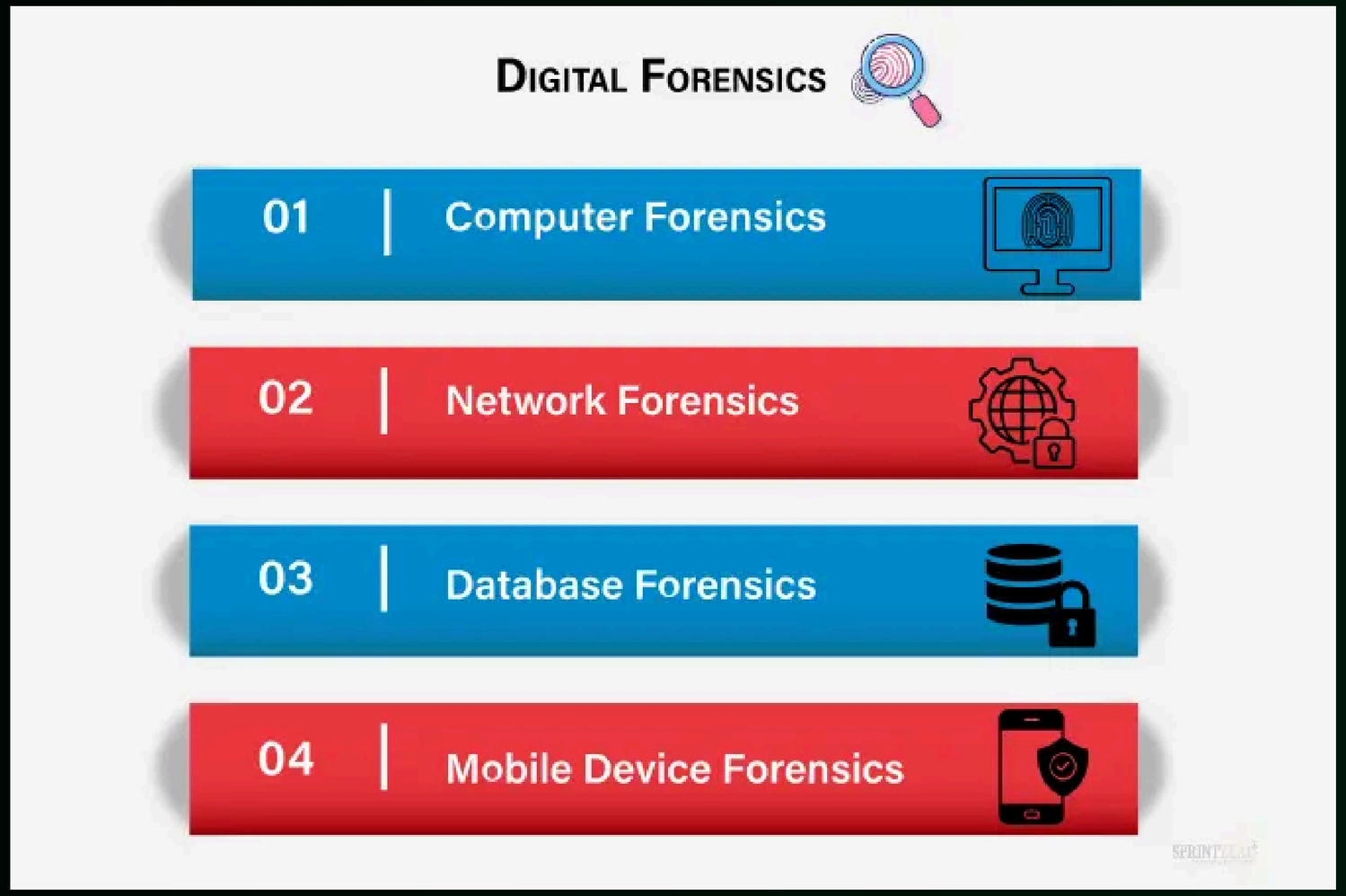
So... What is inside RAM?

When a system is running, RAM may contains:

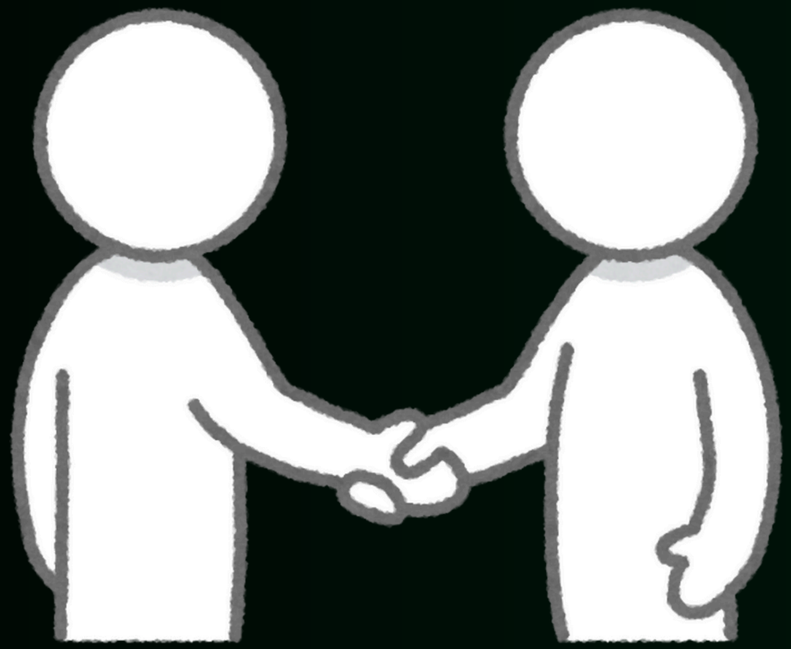
- Running processes
- Passwords in PLAINTEXT
- Active network connections
- Command history
- Encryption keys
- Recently typed data


DIGITAL FORENSIC

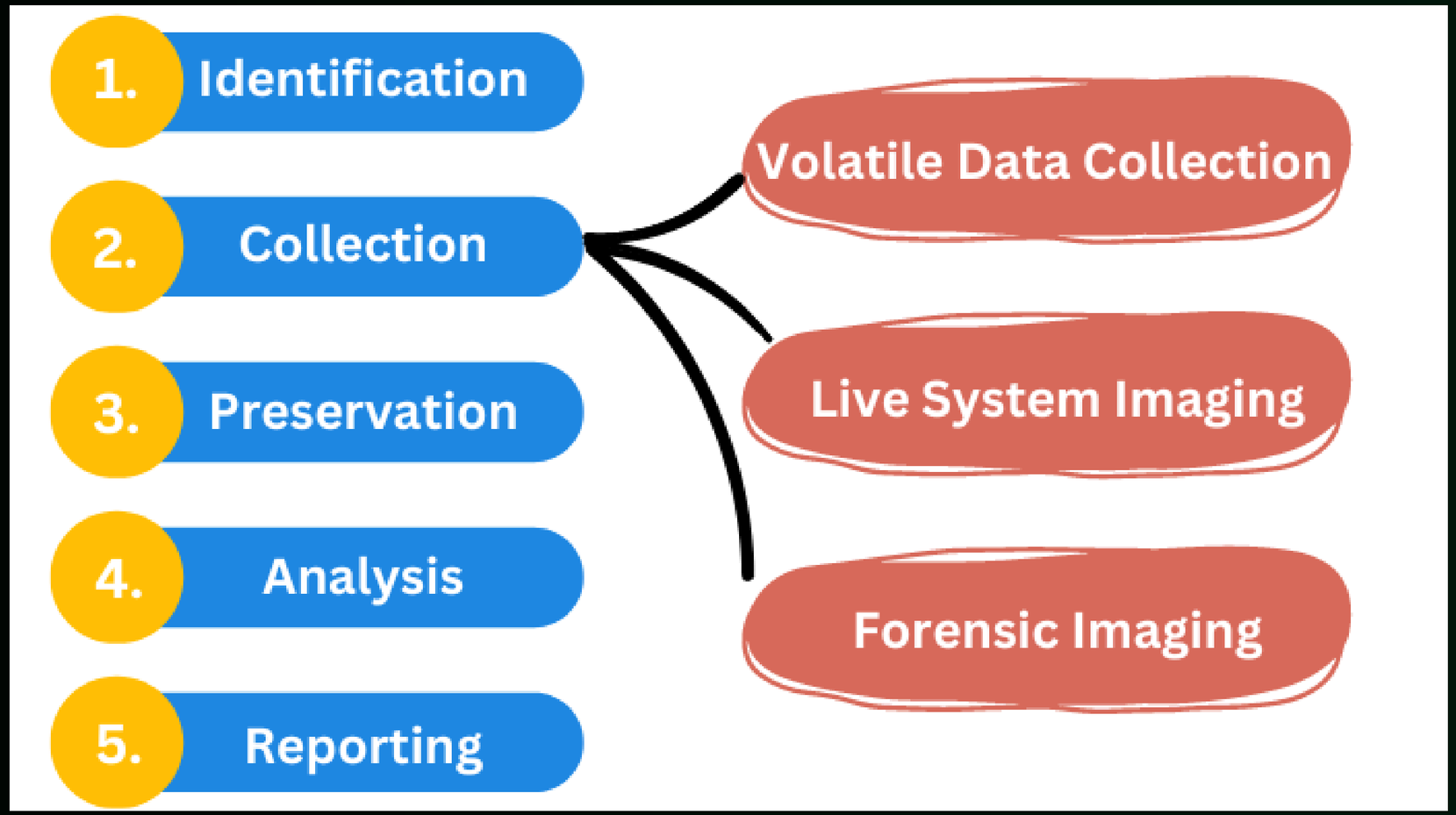
Introduction to digital forensic



All the components working together.



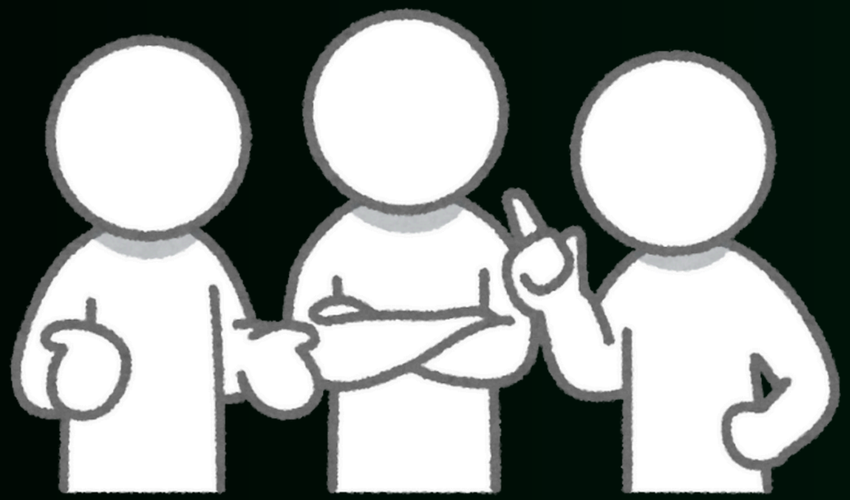
Investigation Framework, ICPAR



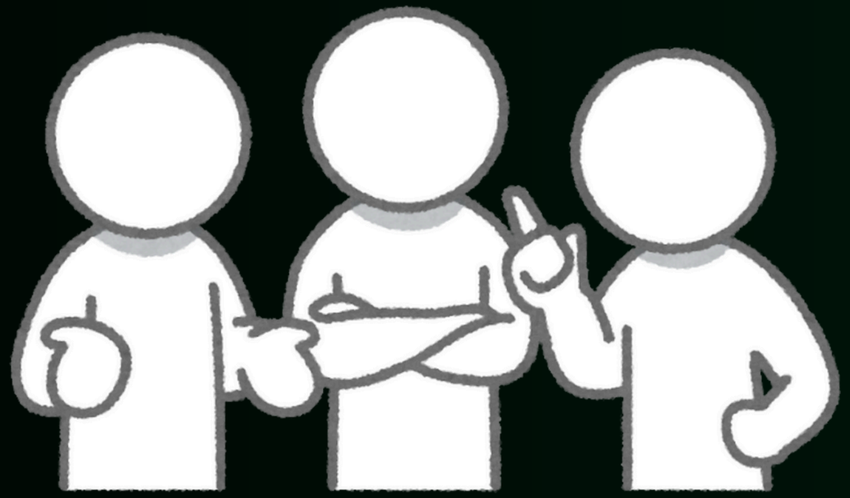

MEMORY FORENSICS

So what is memory forensic?

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



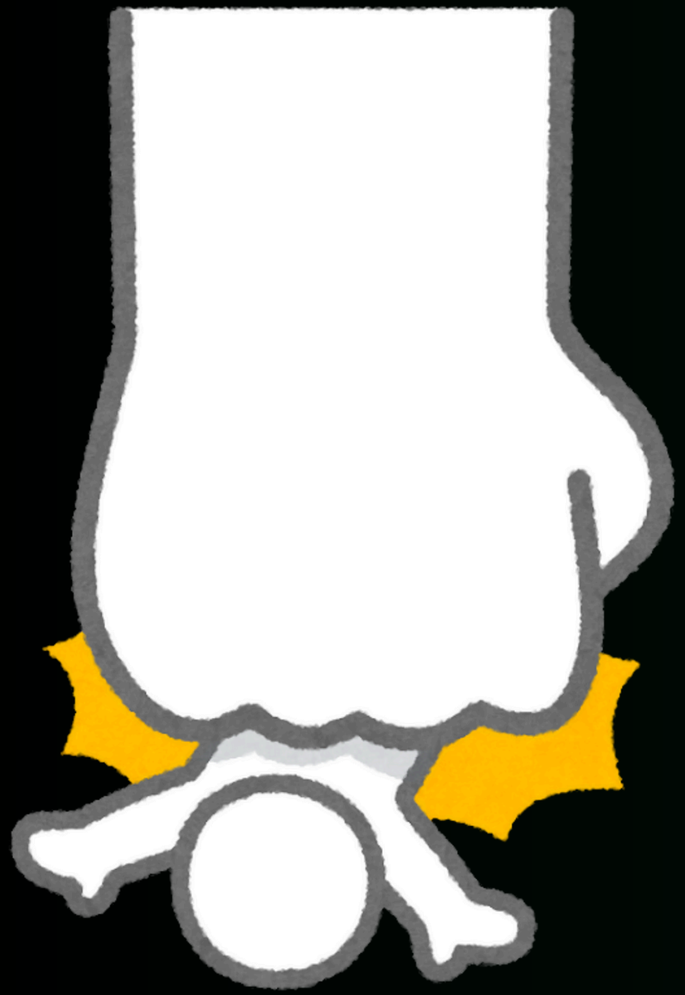
Attackers know about disk forensics. They know their files might get recovered. So **modern attackers** are getting **sneaky** so they're **living in memory**.



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

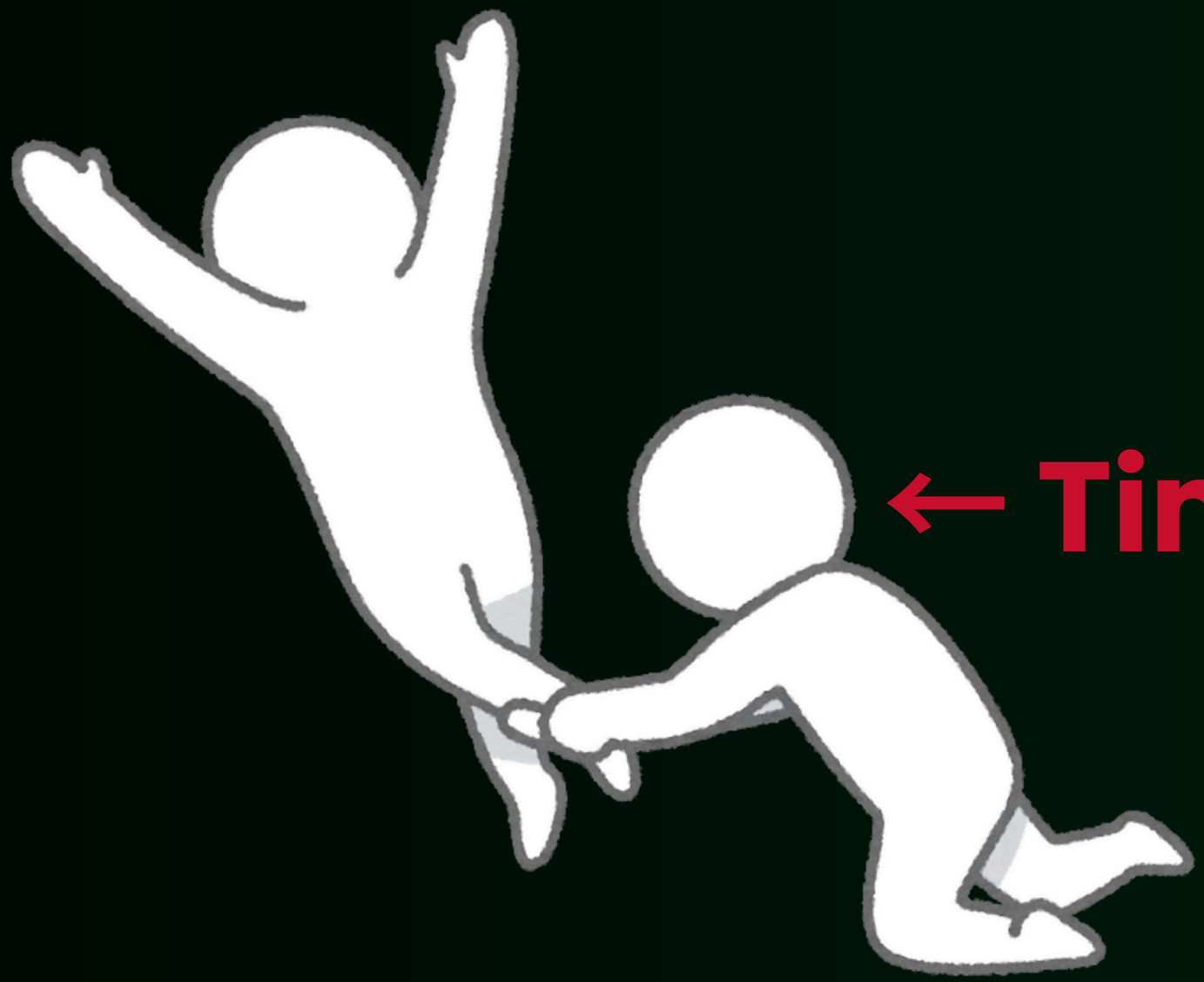
← Attackers

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



Challenges of memory forensic

Digital Forensic investigators ->



Example case:

gbhackers. HOME THREATS CYBER ATTACK DATA BREACH VULNERABILITY WHAT IS D

Cyber Security News | Tools 2 min. Read

EDR-Freeze: Technical Mechanics and Forensic Artifacts Exposed

Example case:

Forensic case study (memory image indicators) by tracepoint :

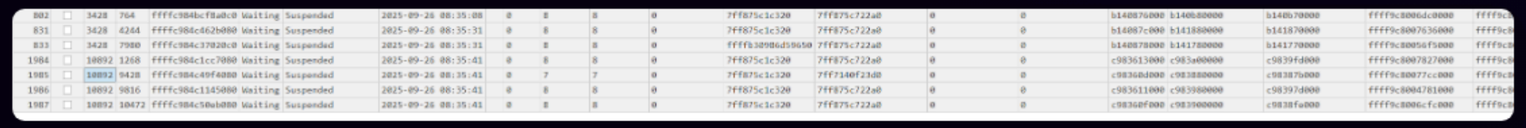
This section documents the memory artifacts you should expect when **EDR-Freeze** is applied to a security process such as `MsMpEng.exe` (Windows Defender). All example commands are memory-analysis oriented and use **Volatility 3/MemProcFS.**

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



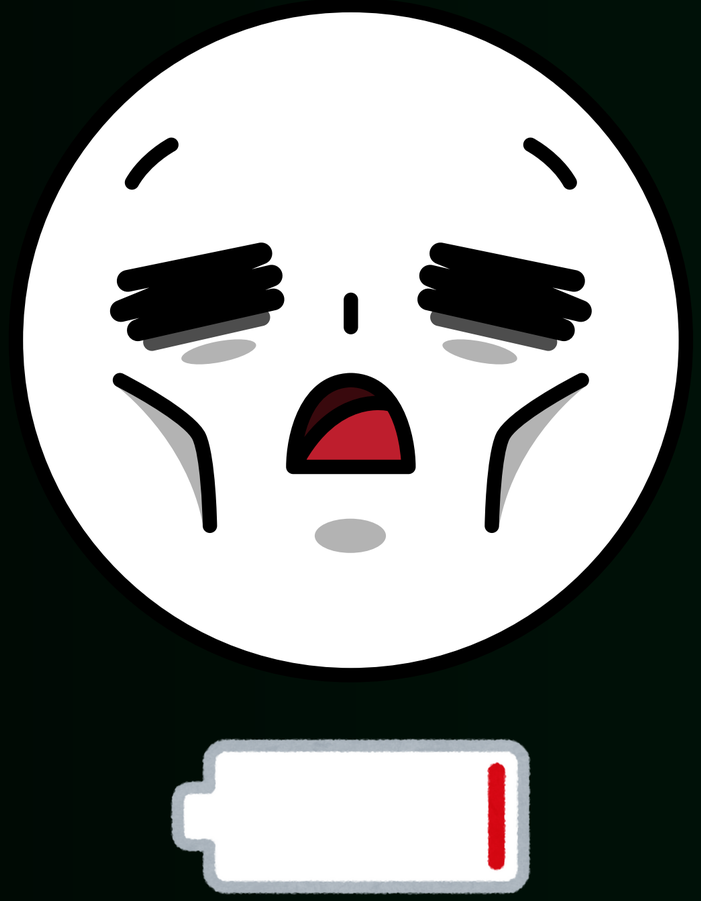
suspended_threads

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

CONGRATS!

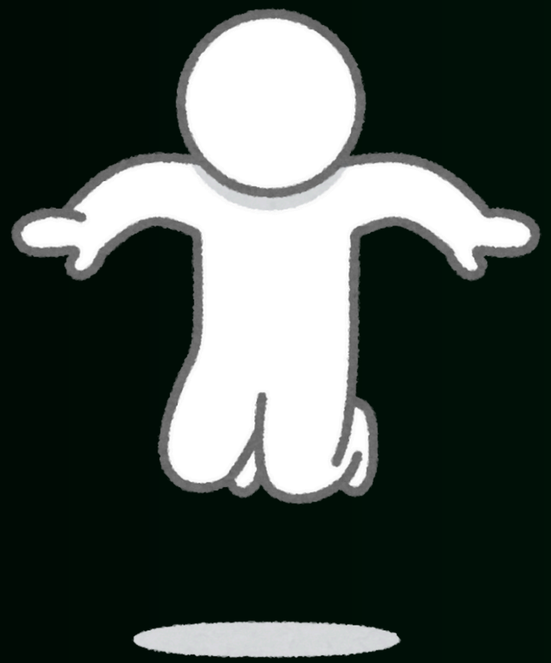
NOW YOU KNOW THE THEORIES IN MEMORY FORENSIC

5 MIN BREAK



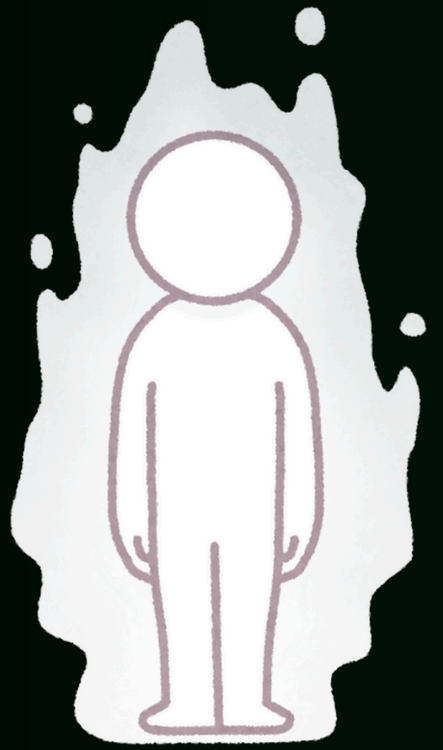
LET’S DO IT

LET’S DO 1 CHALLENGE TOGETHER USING VOLATILITY3!



PRIZE!

FOR THE BEST WRITEUP.

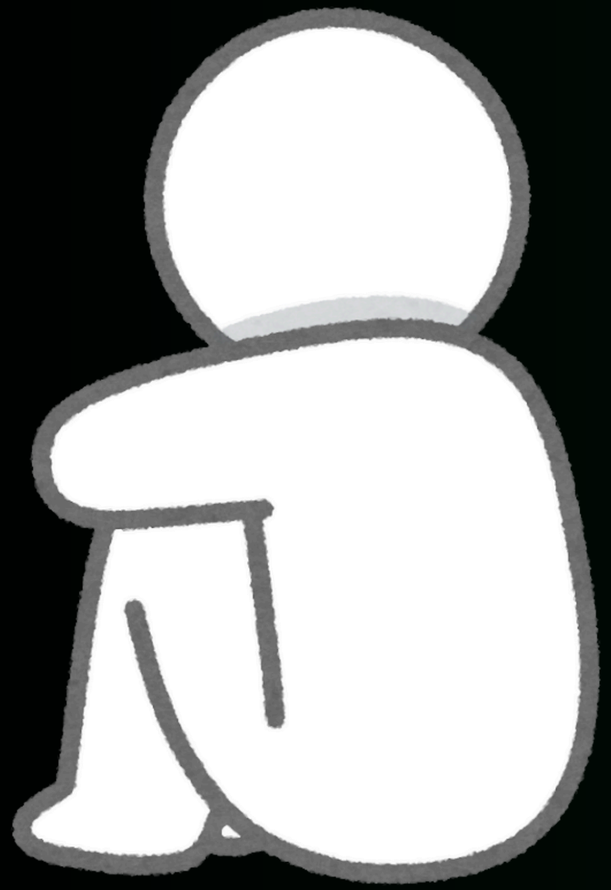


GROUND RULES!

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

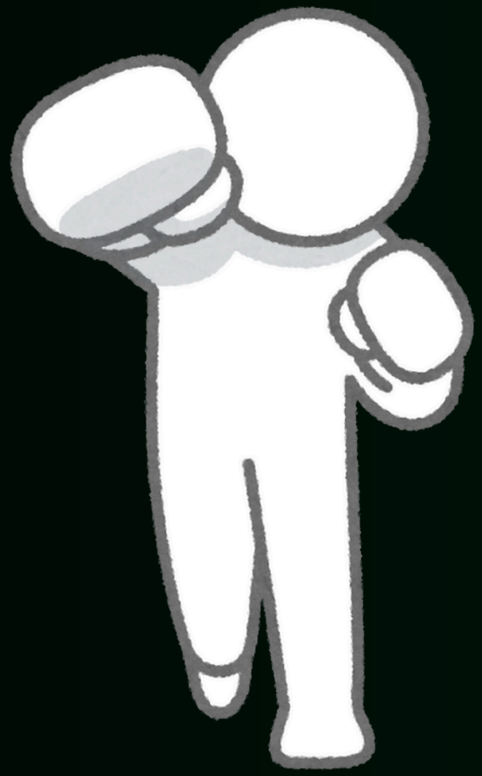
WINNER GETS....

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