Memory Forensics - What it is, what it finds, and how responders use it

Gridinsoft Help Center

What it is

Memory forensics is the practice of analyzing a computer’s RAM to see what is happening right now or just happened. By capturing and examining memory, investigators can spot active processes, network connections, passwords in use, and stealthy malware that may never touch the disk.

Why it matters

Many modern threats hide in memory to dodge file scans. Looking at RAM lets you catch live attacks, rebuild timelines, and confirm exactly what ran, even if the attacker tried to clean up.

What you can find - quick tour

- Running processes and threads that don’t appear in Task Manager
- Network sockets and connections tied to suspicious programs
- Loaded modules and drivers that reveal rootkits or injectors
- Credentials, keys, and commands left in memory by tools and scripts

If you need to run it - basics

- Isolate the system and avoid heavy use that overwrites memory.
- Capture RAM with a trusted tool and preserve hashes for integrity.
- Analyze with Volatility/Velociraptor or similar frameworks.
- Correlate with logs, EDR, and disk artifacts to confirm scope.

Tips

- Practice on test hosts so you can work fast under pressure.
- Prefer cold captures when possible; document every step.
- Automate extraction of IoCs and feed them to SIEM and EDR blocklists.