Incident Response - Order of Volatility

Taz Wake | Halkyn Consulting Ltd | Originally published 2023-10-29

The concept of the "order of volatility" plays a pivotal role in digital forensics and incident response, shaping the systematic approach to gathering digital evidence. This principle revolves around prioritizing the collection and preservation of volatile data — information residing in a computer's memory or temporary storage — based on its susceptibility to rapid change or loss. This methodology is critical for maintaining the integrity and admissibility of digital evidence in legal proceedings, emphasizing a methodical collection process from the most volatile to the least stable data sources.

In digital forensics, the order of volatility categorizes data based on its volatility, moving from the most ephemeral to relatively stable forms. These categories encompass registers and cache, RAM, temporary file systems, disk storage, and archival media. Each level holds distinct types of data crucial for investigations; for instance, RAM contains active network connections, running processes, open ports, and cached credentials. Understanding these categories empowers forensic investigators to strategize their data collection methods effectively.

RFC 3227, titled "Guidelines for Evidence Collection and Archiving," provides essential direction for digital forensics and incident response practitioners. It outlines best practices for collecting and preserving digital evidence, emphasizing documenting the entire process, from collection to analysis, and preserving the chain of custody. Adhering to these guidelines ensures a standardized and accountable approach to digital evidence preservation.

1. **Registers and Cache:** This category encompasses data stored in processor registers and CPU cache — the fastest and most volatile types of memory, containing temporary data used by the processor during operations.

2. **RAM (Random Access Memory):** RAM holds the operating system and application data in current use. Highly volatile, its contents are lost when the system is powered off. Forensic tools such as FTK Imager and EnCase can capture RAM snapshots for analysis.

3. **Temporary File Systems:** These include temporary file systems like /tmp and /run on Linux. Such file systems often contain temporary files created during system operation. It can also include temporary data stored in the %TEMP% folder on Windows as it often stores short-lived data, but it is rare for Windows to mount *truly* temporary filesystems. In Windows IR, mounted optical media (CD/BluRay) or mounted ISO files could be considered a temporary filesystem if you do not have access to the source media.

4. **Disk Storage:** Disk storage encompasses hard drives, SSDs, and other persistent storage devices. While less volatile than RAM, disk storage can still be altered if the system continues to run after an incident. Collection can be performed with tools like dd (on Linux) or applications like FTK Imager, dcfldd, dc3dd, ewfacquire, etc.

5. **Archival Media:** This category involves long-term storage like backups and log files. These are the least volatile and are preserved for historical reference.

The meticulous collection of volatile data is paramount in the context of cyber intrusions. Volatile data, residing in a computer's memory or temporary storage, holds critical evidence about ongoing cyber incidents. Active network connections can reveal suspicious communications, running processes indicate active applications (some potentially malicious), and open ports and cached credentials offer insights into potential vulnerabilities and unauthorized access, aiding investigators in understanding the attacker's tactics and intrusion points.

Collecting volatile data promptly is essential for understanding the intrusion's current state and reconstructing the digital crime scene comprehensively. It enables incident responders to uncover the attacker's tactics, techniques, and procedures (TTPs), aiding in building a robust case for legal proceedings. By demonstrating a comprehensive understanding of the intrusion's timeline, tools used, and the impact on the victim's system, incident responders can provide accurate, reliable, and admissible evidence. Prioritizing volatile data collection ensures that digital investigators possess the necessary context and evidence to effectively respond to cyber incidents, significantly contributing to the pursuit of justice in the face of cybercrime.

You can find out more about DFIR and the effect of collecting volatile data (or conducting live response) on the following SANS Institute courses:

Windows: https://sans.org/for500 and https://sans.org/for508

Linux: https://sans.org/for577

macOS: https://sans.org/for518

About Halkyn Consulting

Halkyn Consulting Ltd is a UK-based security and risk management consultancy providing 24/7 incident response, digital forensics, threat hunting, virtual security leadership (vCISO) and security compliance support to organisations worldwide. We deliver clear, practical, vendor-independent advice based on real-world threats — no hype, no upsell.

More free security resources are available at www.halkynconsulting.co.uk/security-resources.

Web: www.halkynconsulting.co.uk | **Email:** info@halkynconsulting.co.uk | **Tel:** +44 1244 940858