

DIGITAL FORENSICS & INCIDENT RESPONSE.

DFIR reconstructs what actually happened on a compromised system from the artifacts it left behind — **evidence that isn't captured before it's overwritten or powered away is gone permanently, no matter how skilled the analyst.**

- ORDER OF VOLATILITY
- FORENSIC IMAGING
- CHAIN OF CUSTODY
- TIMELINE RECONSTRUCTION

01 THE MECHANISM



Order of Volatility

Live-response collection follows a strict sequence (RFC 3227) from most to least volatile — memory and process state before disk, disk before archival logs — because **evidence not captured immediately can be gone forever.**



Forensic Imaging & Hashing

Investigators create a bit-for-bit image of storage media through a write-blocker, then hash it before and after to **cryptographically prove the copy wasn't altered** during collection.



Timeline Reconstruction

Artifacts from disparate sources — file system metadata, registry keys, event logs, memory — get correlated into **a single timeline of what an intruder actually did**, in order.

02 THE FLOW

The Preserved, Documented Investigation

CONTAINED

1

Volatile evidence — memory, running processes, network connections — is captured **before the machine is powered off or touched further**, per the order of volatility.

2

Every action and every artifact collected is logged with who, what, and when, maintaining an **unbroken chain of custody** from acquisition through analysis.

3

Findings are corroborated across multiple independent artifact sources before conclusions are presented, so **one ambiguous log entry doesn't drive the narrative.**

The Rushed, Unpreserved Response

EXPOSED

1

A compromised machine is powered off or reimaged before volatile evidence is captured, **permanently destroying memory-resident artifacts** like fileless malware.

2

Responders work directly on the original evidence instead of a forensic image, and an investigative action **alters timestamps or overwrites** the data being examined.

3

Without a documented chain of custody, findings can't be corroborated for litigation or a regulatory report — the **conclusions carry no evidentiary weight.**

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Evidence Preservation	Write-blocking, forensic imaging, and volatile-data capture procedures that guarantee original evidence is never altered during collection.
Chain of Custody	Documented handling from acquisition to presentation, establishing who touched evidence, when, and what was done to it.
Artifact Analysis	Correlating file system metadata, registry data, memory dumps, and logs into a coherent timeline of attacker activity.
Reporting & Legal Defensibility	Findings documented to a standard that holds up in litigation, regulatory reporting, law enforcement referral, or insurance claims.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Powering Off the Machine Immediately	No	Destroys volatile memory-resident evidence — fileless malware, injected code, active connections — that never touches disk.
Working Directly on Original Media	No	Any investigative action risks altering timestamps or overwriting the evidence being examined.
Log Review Alone, No Memory or Disk Forensics	No	Attackers routinely clear or tamper with logs; a single evidence source misses what the deletion was meant to hide.
Analysis Without Documented Chain of Custody	No	Findings may be technically correct but carry no evidentiary weight in litigation or a regulatory proceeding.
Order-of-Volatility Collection + Forensic Imaging + Chain of Custody + Cross-Source Correlation	Yes	Preserves evidence integrity end-to-end and produces conclusions that hold up under scrutiny.

DIGITAL FORENSICS & IR.

PRESERVE · ANALYZE · REPORT

05

PROGRAM OPERATIONS

Volatile evidence has to be captured first or not at all. Memory contents, active connections, and running processes don't survive a reboot or a wipe.

Hashing before and after imaging isn't a formality — it's the cryptographic proof that the working copy matches the original evidence.

Attackers use anti-forensics deliberately. Timestomping, log clearing, and living-off-the-land binaries are designed to defeat the artifact types investigators rely on most.

A finding from a single artifact source is a hypothesis, not a conclusion. Corroborating across disk, memory, network, and logs is what makes a timeline defensible.

06

CONTROL MAPPING

NIST SP 800-86

Guide to Integrating Forensic Techniques into Incident Response, the primary US federal reference for applying forensic methodology within IR.

ISO/IEC 27037

International guidelines for the identification, collection, acquisition, and preservation of digital evidence.

RFC 3227

Guidelines for Evidence Collection and Archiving, source of the order-of-volatility principle governing live-response collection order.

SWGDE BEST PRACTICES

Scientific Working Group on Digital Evidence guidance widely referenced for forensic methodology and evidentiary standards.

07

WHAT THIS DOES NOT SOLVE

Prevention

DFIR investigates and reconstructs what already happened; it **doesn't stop the next intrusion**, only informs how to prevent a repeat of this one.

Attribution Certainty

Artifacts establish what happened on a system with confidence. **Identifying who was behind the keyboard** is a much harder, often impossible, bar.

Real-Time Containment

Forensic soundness takes time investigators don't always have. **Containment decisions can't wait** for a complete investigation while active damage continues.

Anti-Forensics-Proof Evidence

A determined attacker using memory-only tooling and log wiping can still **deny investigators clean artifacts**, no matter how sound the methodology.

08

MYTHS VS. REALITY

MYTH

"Powering off a compromised machine is always the safe move."

REALITY

It permanently destroys volatile evidence like memory-resident malware and active network state — **order of volatility says capture that first**.

MYTH

"Deleted files and cleared logs are gone for good."

REALITY

File system metadata, memory artifacts, and other sources often still hold traces after deletion — **which is why single-source analysis misses so much**.

MYTH

"Any competent analyst's findings will hold up if challenged."

REALITY

Without a documented chain of custody, technically correct findings can still be **inadmissible or unpersuasive** in litigation or a regulatory proceeding.

MYTH

"Forensics can always tell you exactly who the attacker was."

REALITY

Artifacts establish what happened on a system with confidence; **attribution to a specific person is a much higher, often unreachable bar**.

MYTH

"DFIR is the same discipline as incident response planning."

REALITY

IR planning designs the process in advance; DFIR is the **technical evidence-collection and analysis work** performed during and after an actual incident.

09

SPEAK THE PROGRAM — KEY TERMS

ORDER OF VOLATILITY

The principle that evidence should be collected **most to least perishable** — memory before disk, disk before archival logs.

CHAIN OF CUSTODY

A documented, unbroken record of who handled evidence, when, and what was done to it, **required for evidentiary defensibility**.

FORENSIC IMAGING

Creating a bit-for-bit copy of storage media through a write-blocker, verified by hashing, so **analysis never touches original evidence**.

TIMESTOMPING

An anti-forensics technique that **alters file timestamps** to disguise when a file was actually created, modified, or accessed.

MEMORY FORENSICS

Analysis of a system's RAM contents to recover **running processes, injected code, and network state** that never touches disk.

LIVING-OFF-THE-LAND BINARIES (LOLBINS)

Legitimate, pre-installed system tools an attacker repurposes for malicious ends, **avoiding the artifacts a dropped binary would leave**.