

# Collecting and Analyzing Artifacts from Active Systems

Unlocking Digital Evidence in Real Time

# Chapter 1

## Understanding Artifacts in Active Systems

In the dynamic landscape of digital forensics, understanding what artifacts are and how they behave in live systems forms the foundation of modern investigative techniques. This chapter explores the fundamental concepts that enable investigators to capture critical evidence while systems remain operational.



# What Are System Artifacts?

## The Nature of Digital Artifacts

System artifacts are the digital breadcrumbs left behind by every action, transaction, and operation that occurs within a computing environment. These data remnants serve as silent witnesses to user behavior, system processes, and application interactions. Think of them as the digital equivalent of fingerprints at a crime scene—each one tells a story about what happened, when it happened, and often who was responsible.

Artifacts are created and modified constantly as users interact with systems, applications execute tasks, and operating systems manage resources. They exist across multiple layers of the technology stack, from the deepest system-level operations to user-facing application behaviors.

## Live System Characteristics

In active, running systems, these artifacts maintain a dual existence across both volatile and persistent storage mediums. Volatile artifacts reside in random access memory (RAM), processor caches, and network buffers—locations that lose their contents when power is removed. Persistent artifacts live on hard drives, solid-state drives, and other non-volatile storage that retains information even after shutdown.

This real-time snapshot capability is what makes live artifact collection so powerful: it captures the system in its current operational state, preserving evidence of active connections, running processes, and in-memory data structures that would otherwise vanish upon system shutdown.

# Why Analyze Artifacts from Active Systems?



## Critical Incident Response

During active security incidents, shutting down systems can destroy valuable evidence and disrupt business operations. Live artifact analysis allows investigators to gather intelligence without interrupting critical services, enabling organizations to maintain continuity while simultaneously investigating threats. This approach is particularly vital in enterprise environments where downtime translates directly to revenue loss and operational disruption.



## Capturing Volatile Evidence

Some of the most valuable forensic evidence exists only in volatile memory—the contents of RAM, active network connections, running processes with their associated memory spaces, encryption keys, and cached credentials. This data provides unprecedented insight into what a system was doing at the exact moment of collection. Once power is lost or a system is shut down, this information disappears forever, taking with it crucial evidence about attacker techniques, malware behavior, and system compromises.



## Accelerated Investigation Timelines

Live forensic techniques dramatically compress investigation timelines by enabling on-site, real-time evidence gathering and analysis. Investigators can quickly triage systems, identify indicators of compromise, and make informed decisions about response actions without waiting for traditional forensic imaging and offline analysis. This speed advantage often makes the difference between containing an incident early or watching it spread across an entire network infrastructure.

# Types of Artifacts in Active Systems

Understanding the taxonomy of artifacts helps investigators know where to look and what evidence can reveal about system and user activities. Each category serves distinct investigative purposes and requires different collection methodologies.

1

## Execution Artifacts

These artifacts provide irrefutable evidence of program execution and usage patterns:

- **LNK Files (Windows Shortcuts):** Created automatically when files are opened, containing metadata about target files, access times, and file locations—even if the original file has been deleted.
- **Prefetch Files:** Windows optimization files that record application execution history, including the number of times run and the last execution timestamp, invaluable for timeline reconstruction.
- **Jump Lists:** Recent items lists for applications showing recently accessed documents and frequently used files, revealing user workflow patterns.
- **AmCache and ShimCache:** Registry-based execution tracking mechanisms that record program paths and execution metadata.

2

## Attribution Artifacts

These connect actions to specific users and establish accountability:

- **User Account Information:** Login records, account creation times, group memberships, and privilege escalation events.
- **Log Files:** Security logs, application logs, and system event logs documenting user authentication, failed login attempts, and privileged operations.
- **Registry Keys:** User-specific registry hives containing personalized settings, recently used files, and application configurations that definitively link activities to individual accounts.
- **User Profile Data:** Desktop contents, document folders, and application-specific user data directories.

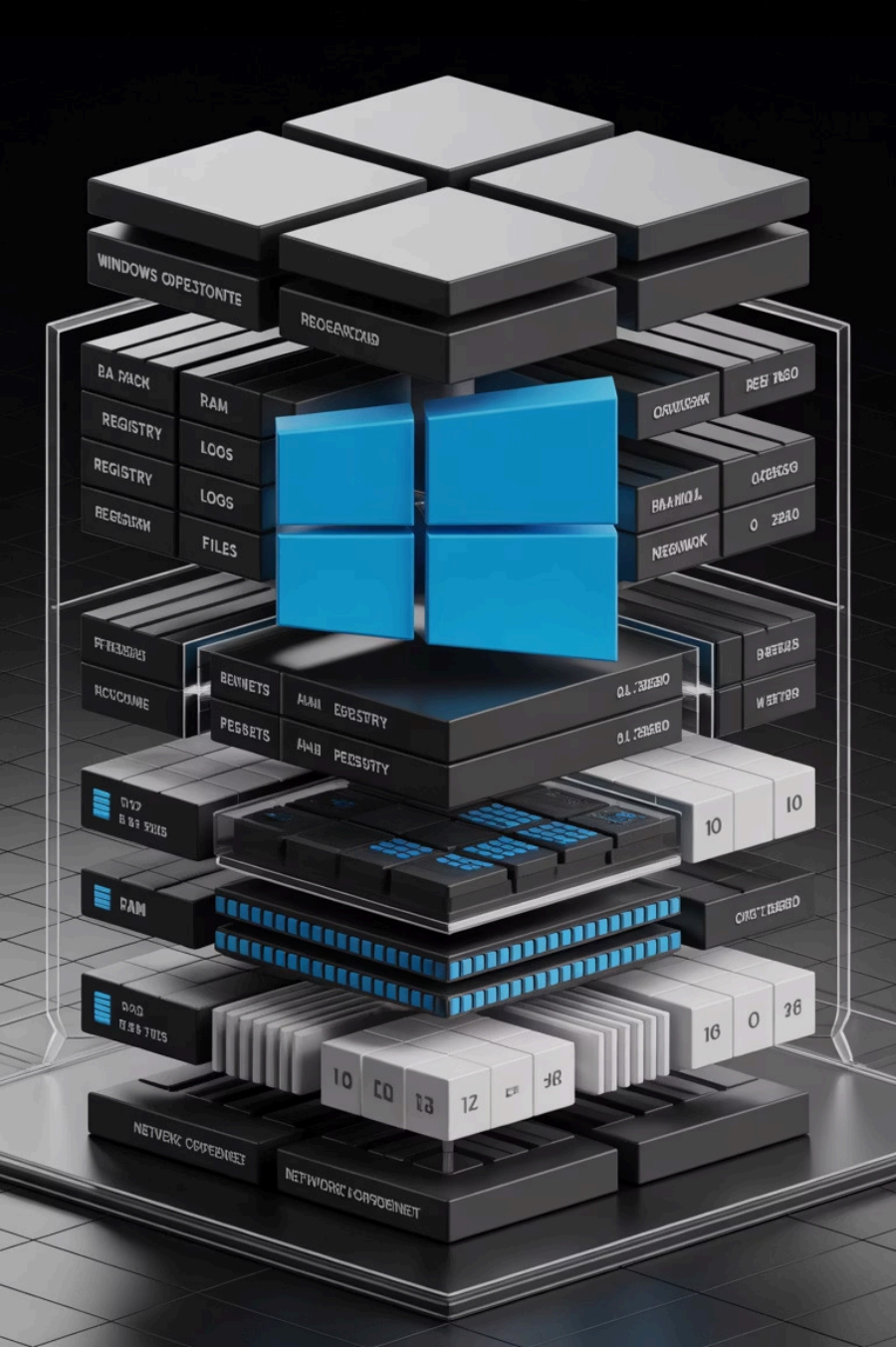
3

## System Metadata

These provide context about the system environment and network activity:

- **Event Logs:** Comprehensive Windows Event Logs or Linux system logs (syslog, auth.log) documenting system-level activities, service starts/stops, and error conditions.
- **Shellbags:** Registry artifacts tracking folder access and Windows Explorer view preferences, showing which directories users browsed—even on external drives.
- **Network Connections:** Active TCP/UDP connections, listening ports, routing tables, and DNS cache revealing communication patterns and potential command-and-control channels.
- **Memory Dumps:** Complete or targeted snapshots of RAM containing process memory, kernel structures, and cached file contents.





# The Digital Artifact Ecosystem

System artifacts don't exist in isolation—they form an interconnected ecosystem where each component provides context for others. This visualization shows the primary sources of artifacts within an active Windows system and how they relate to different layers of system operation.

## Memory Layer

Volatile artifacts residing in RAM, including process memory, network connections, encryption keys, and cached credentials. Most time-sensitive evidence exists here.

## Registry & Logs

Semi-persistent artifacts tracking system configuration, user activity, and historical events. The Windows Registry serves as a treasure trove of timeline data.

## File System

Persistent artifacts including execution traces, user documents, application data, and metadata. These survive reboots but may be altered or deleted by adversaries.

# Chapter 2

## Challenges and Considerations in Live Artifact Collection

While live forensics offers tremendous advantages, it also introduces unique challenges that investigators must navigate carefully. Understanding these complexities is essential for maintaining evidence integrity and investigative credibility.



# Challenges in Collecting Artifacts from Live Systems



## The Volatility Problem

Active systems are dynamic environments where data constantly changes. Memory contents are overwritten as new processes launch and existing ones execute. Log files rotate, temporary files are deleted, and cache contents are purged. Network connections open and close in milliseconds. This constant state of flux means that artifacts captured at one moment may be gone or altered the next. Investigators face a race against time—the longer a compromised system remains active, the more likely critical evidence will be overwritten by normal system operations or deliberately destroyed by attackers who realize they've been detected.

## Anti-Forensics Techniques

Sophisticated threat actors deploy anti-forensics techniques specifically designed to evade detection and thwart investigation efforts. These include timestomping (altering file timestamps to hide when files were actually created or modified), log clearing utilities that wipe event logs, memory-resident malware that leaves no disk artifacts, encrypted or packed executables that hide malicious code, and the use of legitimate system administration tools (living-off-the-land binaries) that blend in with normal activity. Some advanced persistent threat groups employ rootkits that hide processes and files from standard forensic tools, requiring specialized detection techniques.

## Minimizing System Impact

Every action taken during live forensics has the potential to alter the very evidence being collected—a phenomenon known as the Observer Effect in digital forensics. Collection tools consume system resources (CPU, memory, disk I/O), potentially affecting system performance and user experience. More critically, the act of accessing files updates their access timestamps, running forensic tools creates new process artifacts, and writing collected data to disk can overwrite unallocated space containing deleted files. Investigators must carefully select collection methods and tools that minimize these alterations while still gathering comprehensive evidence. This often involves using write-blocking techniques, storing collected data on external media, and employing tools specifically designed to have minimal system footprints.



# Principles of Live Forensics

Successfully navigating the challenges of live artifact collection requires adherence to fundamental forensic principles adapted for active system environments.



## **Evidence Integrity: Acquire Without Altering**

The cardinal rule of digital forensics applies with even greater importance in live environments: collect evidence in a manner that preserves its original state to the greatest extent possible. This means using forensically sound tools that minimize system modifications, documenting any unavoidable changes that occur during collection, employing hash verification to ensure data integrity, and utilizing read-only access methods whenever feasible. Tools should be validated and tested before use in actual investigations to understand their system impact. When possible, use trusted, digitally signed tools stored on write-protected media to prevent tampering.



## **Strategic Prioritization: Collect What Matters Most First**

In the time-sensitive environment of live forensics, not all artifacts are created equal. Investigators must follow the Order of Volatility principle, collecting the most volatile and time-sensitive evidence first before it disappears. This typically means capturing network connections and process memory first, followed by system memory dumps, then running process information, temporary file systems, and finally persistent disk-based artifacts. Understanding which artifacts answer your investigative questions helps focus collection efforts on high-value targets rather than attempting to grab everything (which may be impossible within time constraints).



## **Meticulous Documentation: Maintain Chain of Custody**

Comprehensive documentation transforms raw data into admissible evidence. Every step of the collection process must be documented with precision: exact timestamps of collection activities, tools used (including version numbers and hash values), command-line parameters and collection configurations, observed system state and any anomalies, names of personnel involved, and environmental conditions. This documentation establishes chain of custody—the paper trail proving that evidence has been properly handled and not tampered with from collection through analysis to presentation. In legal proceedings, poor documentation can render otherwise valuable evidence inadmissible, regardless of its technical merit.

# Chapter 3

## Tools and Techniques for Artifact Collection

Modern digital forensics relies on sophisticated tools that automate and streamline the artifact collection process. This chapter examines leading solutions that empower investigators to efficiently gather comprehensive evidence from live systems.



# ArtifactCollector: A Modern Tool for Live Artifact Gathering



## Universal Compatibility

ArtifactCollector represents the next generation of cross-platform forensic tools, providing consistent artifact collection capabilities across Windows, Linux, and macOS environments. This universal approach is increasingly critical in heterogeneous enterprise networks where investigators encounter diverse operating systems and need reliable tools that work everywhere.

## Comprehensive Collection Capabilities

ArtifactCollector excels at gathering multiple artifact types through a unified interface:

- **File System Artifacts:** Collects files based on configurable path specifications, supporting wildcards and recursive directory traversal to capture execution artifacts, user documents, and system configuration files.
- **Registry Data:** Extracts Windows Registry keys and values relevant to forensic investigation, including user activity tracking, program execution evidence, and system configuration data.
- **Command Output:** Executes system commands and captures their output, enabling collection of live system state information like running processes, network connections, and service status that exists only in volatile memory.
- **WMI Queries:** Leverages Windows Management Instrumentation to gather detailed system information, hardware inventory, installed software, and running services without direct file system access.

### Configurable Artifact Definitions

Built on proven methodologies from SANS FOR500 training, ArtifactCollector uses human-readable YAML configuration files defining which artifacts to collect. Investigators can customize collections for specific investigation types, add new artifact definitions as forensic knowledge evolves, and share configurations across teams to standardize collection procedures.

### Portable Evidence Packages

The tool produces comprehensive, self-contained evidence packages that bundle all collected artifacts with metadata and collection logs. These packages maintain file structure and metadata, include hash values for integrity verification, and can be easily transported for offline analysis, making them ideal for incident response scenarios requiring evidence collection from remote locations.

# Automated Live Artifact Collection: The e-Triage Tool Example

The e-Triage tool exemplifies how automation accelerates incident response by collecting comprehensive artifact sets with minimal investigator intervention.



## System Information Extraction

Automatically gathers complete system profiles including hardware specifications, installed operating system details, patch levels, system uptime, and environmental variables. This information establishes the technical context for all other artifacts and helps investigators understand system capabilities and potential vulnerabilities.



## Registry Hive Collection

Extracts critical registry hives containing user activity evidence, program execution history, system configuration, and persistence mechanisms used by malware. The tool intelligently targets high-value registry keys known to contain forensically relevant information, avoiding the need to collect entire multi-gigabyte registry files.



## Event Log Harvesting

Collects Windows Event Logs or Linux system logs documenting security events, application activities, system errors, and administrative actions. These logs provide timeline reconstruction data and often contain the first indicators of compromise or unauthorized access attempts.



## Memory Acquisition

Captures complete physical memory dumps or targeted process memory, preserving volatile evidence that would be lost upon shutdown. Memory analysis can reveal running malware, encryption keys, credentials, and network connections that leave no persistent disk artifacts.




## Browser History and Cache

Extracts web browsing history, cached pages, cookies, and download records from all major browsers. This data reveals user research activities, visited malicious websites, downloaded files, and web-based command-and-control communications used by attackers.



## Rapid On-Site Evidence Gathering

Designed for speed and efficiency, e-Triage enables investigators to quickly collect comprehensive evidence during active cyber incidents without requiring specialized forensic expertise. The tool's automated approach ensures consistent collection procedures and reduces the risk of missing critical artifacts during high-pressure incident response situations.

 **Prioritization Advantage:** By collecting the most valuable artifacts quickly, tools like e-Triage allow investigators to begin analysis and response actions while collection is still in progress, dramatically accelerating the investigation lifecycle and reducing attacker dwell time.

# Real-World Impact: Using Artifacts to Investigate Cyber Incidents

Theory becomes practice when we examine how artifact analysis solves real-world security incidents. These scenarios demonstrate the investigative power of live artifact collection.

## Ransomware Binary Identification

**The Challenge:** An organization's file servers begin encrypting files, but the ransomware executable has been deleted or obfuscated. Traditional file system searches find no obvious malware.

**The Solution:** Investigators examine execution artifacts including Prefetch files showing recently executed programs, AmCache entries recording program paths even after deletion, and Windows Defender logs capturing detection attempts. These artifacts reveal the ransomware's original filename, execution path, and launch timestamp—even though the malware itself has been removed.

**The Outcome:** With the binary name and hash identified from artifacts, security teams can scan all systems for indicators of compromise, determine the infection scope, and deploy appropriate remediation measures.

## Attack Timeline Reconstruction

**The Challenge:** Following a data breach, leadership needs to understand exactly when the compromise occurred, what data was accessed, and what actions the attacker took.

**The Solution:** Investigators correlate multiple artifact sources: Prefetch timestamps showing tool execution, Jump Lists revealing accessed documents, event logs documenting authentication events, and network artifacts recording data exfiltration. By triangulating these diverse artifact types, investigators build a comprehensive timeline spanning the initial compromise through lateral movement to ultimate data theft.

**The Outcome:** The detailed timeline supports legal proceedings, regulatory reporting, and board-level communications. It also provides crucial threat intelligence about attacker tactics, techniques, and procedures that inform future defensive measures.

1

2

## Persistence Mechanism Discovery

**The Challenge:** Despite repeated malware removal attempts, a sophisticated threat actor maintains access to compromised systems, suggesting hidden persistence mechanisms.

**The Solution:** Deep analysis of registry artifacts reveals modified Run keys, scheduled tasks, and Windows service configurations pointing to attacker implants. Log artifacts show repeated execution of suspicious processes at system startup. ShimCache and AmCache entries document the full execution history of these persistent components.






**The Outcome:** Understanding the complete persistence strategy allows defenders to remove all attacker footholds, breaking the reinfection cycle and genuinely cleaning compromised systems.

3



# Visualizing the Investigation: Attack Timeline Reconstruction

One of the most powerful applications of artifact analysis is the ability to reconstruct attacker activity into a clear, chronological timeline. This visualization approach transforms disparate data points into a coherent narrative of compromise.

		
<b>Initial Access</b> <p>Artifacts reveal how attackers first entered the network—whether through phishing emails (email logs, browser history), exploited vulnerabilities (application logs, patch status), or stolen credentials (authentication logs).</p>	<b>Discovery &amp; Reconnaissance</b> <p>Execution artifacts show attacker tool usage for network scanning, privilege enumeration, and data discovery. Registry and log artifacts document which systems and accounts were queried.</p>	<b>Lateral Movement</b> <p>Network artifacts, authentication logs, and execution traces on multiple systems reveal how attackers spread through the environment, compromising additional systems and escalating privileges.</p>
		
<b>Collection &amp; Staging</b> <p>File access artifacts, Jump Lists, and ShellBags show which sensitive data was accessed. Execution artifacts reveal archiving tools used to package data for exfiltration.</p>	<b>Exfiltration</b> <p>Network connection artifacts, browser history, and execution traces document how data left the network—via cloud storage, FTP, email, or command-and-control channels.</p>	

By correlating artifact timestamps across these attack phases, investigators create a precise timeline showing not just what happened, but when it happened and in what sequence. This timeline becomes the foundation for understanding attack sophistication, determining breach scope, and supporting legal and regulatory response requirements.

# Conclusion: Harnessing Live Artifact Analysis for Faster, More Effective Forensics



## Bridging Detection and Response

Live artifact collection represents a critical bridge between the moment a security incident is detected and when effective response actions can be taken. Traditional forensic approaches that require system shutdown and offline analysis introduce unacceptable delays in today's fast-paced threat landscape. By collecting and analyzing artifacts from active systems, investigators gain immediate insight into ongoing attacks, enabling rapid containment and remediation decisions that minimize damage and reduce attacker dwell time.

### The Power of Integration

Effective artifact analysis isn't just about collecting data—it's about combining forensic knowledge with the right tools and methodologies. Understanding which artifacts reveal specific types of evidence, knowing how to interpret artifact contents in context, and having reliable collection tools creates a powerful investigative capability that transforms raw system data into actionable intelligence.

### Uncovering Hidden Truths

Artifacts serve as digital witnesses that can't be intimidated, coerced, or silenced. They faithfully record system and user activities, often capturing evidence that attackers don't realize exists. Even when adversaries attempt anti-forensics techniques to cover their tracks, artifact correlation and analysis frequently reveals inconsistencies and traces that expose malicious activity. This investigative power empowers defenders to understand exactly what happened during security incidents, who was responsible, and what needs to be done to prevent recurrence.

### Essential for Modern Cybersecurity

As systems grow more complex, attacks become more sophisticated, and business demands for always-on availability intensify, the ability to perform forensics on active systems isn't optional—it's essential. Organizations that master live artifact collection and analysis gain decisive advantages in incident response speed, investigation quality, and overall security resilience. The future belongs to defenders who can extract truth from running systems without disrupting critical operations.

*"In digital forensics, artifacts are the breadcrumbs that lead us through the forest of data to the truth. On live systems, those breadcrumbs are still warm—we just need to know where to look and how to preserve them before they disappear."*

The journey from artifact discovery to incident resolution requires continuous learning, tool proficiency, and methodological discipline. As threat actors evolve their techniques and system architectures advance, forensic investigators must evolve alongside them—mastering new artifact types, adapting collection methodologies, and refining analytical approaches. The principles outlined in this presentation provide a solid foundation for that ongoing journey toward forensic excellence in the age of always-on systems.