DIGITAL FORENSICS CORP

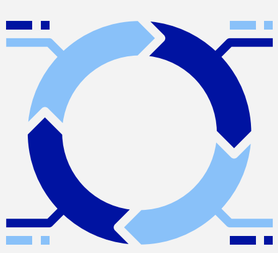
Windows Operating System Forensic Analysis

Introduction to Windows Forensics & Key Artifacts

Windows Forensics: A Guide to Digital Evidence Analysis

WHAT IS WINDOWS FORENSICS?

Brief definition: Windows forensics is the discipline of collecting, preserving, analyzing, and reporting on evidence found on Windows operating system devices (desktops, laptops, servers). It is critical for incident response and digital investigations (e.g., intellectual property theft, malware analysis, or regulatory compliance).



THE FORENSIC PROCESS (A 4-STEP OVERVIEW)

Highlight the core steps:

1. Preservation & Acquisition: Creating a forensically sound image of the storage media.
2. Examination: Using tools to analyze the raw data.
3. Analysis: Interpreting the data to reconstruct events.
4. Reporting: Documenting the findings for legal or internal review.

CRITICAL EVIDENCE: KEY WINDOWS ARTIFACTS

Registry: Contains system configuration, user activity, and executed programs.

Event Logs: Record system, security, and application events (e.g., login attempts, service changes).

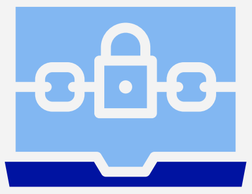
Prefetch & ShimCache: Show evidence of program execution and usage history.

Recycle Bin: Contains details on deleted files.

LNK Files (ShellBags): Shortcuts that reveal recently accessed files and folders, even if deleted.

Investigative Tools and Cyber Threat Focus

Tools of the Trade & Investigating Common Cyber Threats



Essential Windows Forensics Tools

Acquisition (Imaging): FTK Imager, X-Ways Forensics, EnCase.
Analysis (Parsing/Viewing): Volatility (for memory analysis), Registry Explorer, Event Log Explorer.
Open-Source Utilities: Autopsy, The Sleuth Kit (TSK).
Note: Proper tool usage ensures the integrity and admissibility of evidence.

Investigating Common Threats

1. Malware/Ransomware:
Focus: Identifying initial infection vectors (email, downloaded files), persistence mechanisms (Registry Run keys, Scheduled Tasks), and communication with C2 servers.

2. Data Theft/Exfiltration:
Focus: Analyzing USB/External Device connection logs, recent file access (LNK/Jump Lists), and network activity logs showing large uploads.

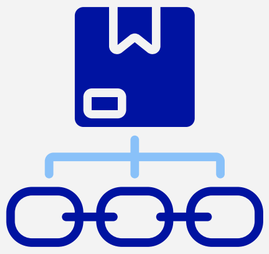
3. Unauthorized Access:
Focus:Scrutinizing failed and successful login events, RDP usage history, and account creation/modification logs.

Threat Removal & Remediation (Forensic Output)
The investigation provides the evidence needed to:

Containment: Immediately isolate affected systems.
Eradication: Pinpoint and remove malicious files, registry entries, and user accounts.
Recovery: Restore systems using clean backups and implement stronger security controls.

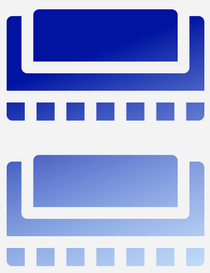
Best Practices and Your Forensic Partner

Maintaining Integrity & Partnering for Expertise



Chain of Custody: Non-Negotiable

Digital evidence is fragile. The Chain of Custody is a documented process showing who had possession of the evidence and when, ensuring it hasn't been tampered with. A forensically sound acquisition using write-blockers is the first critical step.



Memory (RAM) Analysis

The most volatile evidence: RAM holds currently running processes, network connections, and sometimes decryption keys or passwords. It must be captured before the system is shut down, as its contents are lost on power loss.

Partner with Digital Forensics Corp.

Don't go it alone. Digital evidence is complex, and errors can invalidate an entire case. Our certified experts use court-approved methodologies and proprietary tools to ensure evidence is legally sound. We provide the critical analysis needed for legal proceedings or internal investigations.

Contact us!

Contact us today for a confidential consultation.
Phone: 1-800-849-6515
Email: info@digitalforensics.com
Website: https://www.digitalforensics.com/