

## Digital Forensics: Core Terms and Investigative Capabilities

### Case Assessment

Not all digital investigations are created equal. The nature of the concern, the number and type of devices, and the background of the user all influence the likelihood of locating relevant evidence. Rather than offer guarantees, Swailes investigators provide realistic expectations based on years of practical experience. s, IP theft, misconduct, harassment, or breach of policy.

### Device Imaging

This refers to the forensic acquisition of a digital device. Imaging captures a full bit-for-bit copy of a system, regardless of platform (Windows, Mac, Linux, Unix), to preserve data in a court-admissible format. Devices imaged include desktops, laptops, servers, smartphones (iPhone, Android), tablets, external drives, and backup media.

### Evidentiary Snapshot

When full forensic imaging isn't feasible, due to active systems, damaged devices, or volatile data, an evidentiary snapshot captures the current state of a system for preservation or future analysis. This is often used when a device must remain in service but future evidence preservation is required.

### Backup Tape Restoration

Backup tapes often hold critical evidence. Whether restoring data from legacy media or fulfilling court-ordered email production, Swailes has deep expertise across formats such as LTO, DLT, DDS, Travan, AIT, ZIP, and JAZZ. This allows full restoration of archived data for investigative review.

### Email Search and Processing

Whether email is sourced from a forensic image, backup tape, Exchange server, or PST file, Swailes can process, index, and extract messages based on keywords, time ranges, or data types, supporting eDiscovery, litigation, and internal investigations.

### Deleted File Recovery

Even when data is "deleted," remnants often remain. Swailes investigators use forensic tools, scripts, and investigative logic to recover files believed permanently lost, even from formatted or damaged devices.



### Swailes Differentiators

- Extensive Civil & Criminal Case Expertise
- Certified Forensic Examiners
- Experienced Expert Witness in Federal & State Courts
- State Licensed Investigators
- Proven Testimony Experience
- Expertise in Digital Evidence Preservation
- Veteran-Owned and Houston-Based
- InfraGard/FBI Member

## Digital Forensics: Core Terms and Investigative Capabilities

### Metadata Analysis

Digital files often store embedded details: who created them, who edited them last, when they were printed, and how long they've been modified. Swailes examiners extract metadata from documents, images, and system files to reveal facts often missed in standard reviews.

### Log File Review

Activity logs from operating systems, servers, apps, or network hardware (e.g., routers, switches) often hold critical information. Swailes investigators analyze these logs to identify timelines, trace activity, or uncover anomalies.

### Keyword & Search Terms Analysis

Searches based on names, phrases, or company terms remain a cornerstone of forensic review. While not always conclusive alone, keyword matches often lead to other critical data points and are foundational in timeline development and behavior reconstruction.

### Data Carving

When a file is deleted or corrupted, forensic carving can extract or reassemble content from system caches, memory dumps, swap files, or hibernation files. This method can recover files thought to be unrecoverable.

### Tailored Reporting

Swailes produces customized reports based on audience, whether legal teams, HR professionals, executives, or courtroom presentation. While the core evidence remains the same, the delivery is tailored for clarity, strategy, and legal defensibility.

### Cloud & SaaS Platform Forensics

As more business operations move to the cloud, evidence increasingly resides in services like Microsoft 365, Google Workspace, Slack, Dropbox, and Salesforce. Swailes investigators are experienced in accessing and analyzing data from cloud-hosted systems, including webmail, collaboration logs, and cloud file activity.



### Swailes Differentiators

- Extensive Civil & Criminal Case Expertise
- Certified Forensic Examiners
- Experienced Expert Witness in Federal & State Courts
- State Licensed Investigators
- Proven Testimony Experience
- Expertise in Digital Evidence Preservation
- Veteran-Owned and Houston-Based
- InfraGard/FBI Member

## Digital Forensics: Core Terms and Investigative Capabilities

### Mobile Application Artifacts

Beyond messages and call logs, apps such as WhatsApp, Signal, TikTok, and Instagram can store valuable data including message threads, media, contacts, and hidden usage artifacts. Swailes can recover and interpret this app-specific data even after deletion or obfuscation.

### Behavioral Pattern Analysis

By combining timestamps, logs, metadata, and usage artifacts, Swailes examiners can reconstruct a subject's behavior, habits, and intent, often crucial in matters involving insider threats, harassment, or intellectual property misuse.

### Link & Timeline Correlation

Individual artifacts rarely tell the whole story. Swailes investigators correlate data from multiple sources, devices, emails, cloud accounts, logs, to build cohesive, defensible timelines of activity that connect people, devices, and events.

### Validation & Chain of Custody

Swailes adheres to rigorous validation protocols and maintains strict chain-of-custody procedures for all evidence. This ensures defensibility in court and protects against evidence tampering or disqualification.

### Expert Witness Support & Testimony

In cases that proceed to litigation, Swailes examiners can serve as qualified expert witnesses, providing sworn affidavits, deposition support, or live courtroom testimony. Our professionals explain technical findings in plain language that is clear, credible, and admissible under state and federal evidentiary standards.

### Structured & Unstructured Data Review

Digital evidence exists in many forms, from structured data like databases and logs to unstructured content like documents, images, chat threads, and handwritten notes in scanned files. Swailes examiners are trained to extract, classify, and contextualize both structured and unstructured evidence sources across complex systems.



### Swailes Differentiators

- Extensive Civil & Criminal Case Expertise
- Certified Forensic Examiners
- Experienced Expert Witness in Federal & State Courts
- State Licensed Investigators
- Proven Testimony Experience
- Expertise in Digital Evidence Preservation
- Veteran-Owned and Houston-Based
- InfraGard/FBI Member