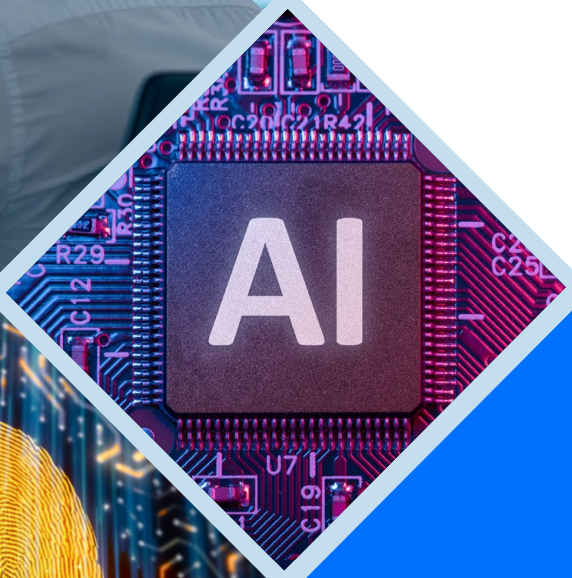
ERMProtect
Cybersecurity Solutions



The Complete Guide to Digital Forensics

ERMProtect
Cybersecurity Solutions

Introduction to Digital Forensics

Digital forensics focuses on identifying, collecting, preserving, analyzing, and presenting digital evidence in a manner that is legally admissible and technically sound. It operates at the intersection of technology, law, and investigative methodology. As digital systems are embedded in business operations, government functions, and personal life, digital forensics has evolved from a niche specialty into a core pillar of cybersecurity, incident response, litigation support, and regulatory compliance.

The purpose of digital forensics is not just to recover deleted files or identify malware. It seeks to reconstruct events: who did what, when did they do it, how did they do it, and what systems or data were affected or breached.

Through careful analysis of digital artifacts and logs, investigators can build a timeline of activities, attribute actions to specific users or systems, determine scope and impact of breaches, and provide defensible findings to courts, regulators, and executives. These findings are formally documented in a forensic report, which contains only verified facts derived from the investigation — free from assumptions or unsupported statements.

What Types of Cases Benefit from Digital Forensics

Following digital trails, forensic examiners can uncover critical evidence in all types of fraud — wire fraud, embezzlement, and theft, for example. Digital forensics also plays a key role in identifying the cause of data

305-447-6750 | info@ermprotect.com

breaches, so that they can be contained and remediated. Further, forensic analysis is a key source of evidence in litigation cases involving commercial disputes, IP theft, and employee misconduct may rise or fall depending on forensic analysis. Real-life examples of the wide range of cases handled by a digital forensics firm can be found here.

The Evolution of Digital Forensics

Digital forensics emerged in the late 20th century alongside the proliferation of personal computers. In the 1980s and early 1990s, investigations focused primarily on standalone machines and floppy disks. Law enforcement agencies began developing procedures for imaging hard drives and recovering deleted files, and the field was often referred to as "computer forensics."

Today, digital forensics covers a vast variety of systems such as endpoints, network forensics, cloud, smartphones, memory and in the coming few years, artificial intelligence systems. The discipline has evolved from standalone machines to entire networks and interconnected systems.

Digital Forensic Methodology Steps

Digital forensics follows a detailed, methodical process where strict adherence is vital. There are five broad steps that a digital forensic investigation follows:

1 Identification

Investigators identify all potential sources of digital evidence such as computers, mobile devices, hard drives, USBs, and even SaaS platforms such as Teams or cloud workloads. The scope may range from a single laptop to an entire network.

2 Preservation

Evidence identified in Step 1 is isolated, secured, and preserved to maintain authenticity. Next, an image of the evidence is created. An image is a bit-by-bit copy of the evidence (hard drive, USB device, shared network folder, etc.). For cloud environments, "Live Response" tools capture snapshots of systems before reboot or termination.

3 Examination

Investigators perform an in-depth analysis of the image. The examination phase is never carried out on the original evidence to preserve integrity. This phase focuses on identifying relevant data types, such as:

- **Saved Data -** Regular files and system files present on the image.
- **Temporary Data -** Files created by programs (e.g., .TMP or ~ files) that capture snapshots of original files.
- **Deleted Data -** Data marked for deletion but not yet overwritten which is often recoverable.
- **Metadata -** Information about files (creation date, modification date, location) that helps reconstruct activity.
- **Slack Space Data -** Unused storage space within file clusters that may contain remnants of valuable data.

4 Documentation

Investigators document every action taken during their investigation, including methods used for retrieving, copying, storing, and analyzing data. A detailed timeline of events is created to support findings. Proper documentation demonstrates data integrity, adherence to policies, and court admissibility. Poor reporting can compromise the entire case.

5 Reporting

A good report can serve as the invaluable link between the technical and non-technical elements of a case. A report should be comprehensive yet clear, explaining case-relevant evidence in simple terms. At minimum, a forensic report should identify the data analyzed, an independent evaluation of the sequence of events, and a conclusion or opinion at the end.

305-447-6750 | info@ermprotect.com

What are the Procedures for Evidence Handling?

Proper evidence handling ensures admissibility in court. Evidence must be authentic, reliable, and complete to meet legal standards. Here are some key elements to keep in mind in relation to evidence handling:

Preparation

Computer forensic examiners must thoroughly understand case objectives to determine where relevant evidence resides and how it can be collected. They must also devise an approach that takes into consideration industry-standard protocols and applicable regulatory requirements for acquiring evidence. In addition, they must determine the method that will be used to make a copy of the original evidence.

Collection

After identifying evidence sources, investigators create bit-stream or "mirror image" backups that replicate every sector of the device or media. To preserve volatile data, they follow an order of volatility, starting with capturing RAM, then collecting cloud metadata, and finally imaging physical disks. For cloud environments, API-integrated tools are used to generate point-in-time snapshots of virtual machines or database instances, ensuring the data is isolated from the live environment and preventing the loss of critical information such as encryption keys.

Hashing

Hashing is a method to ensure the integrity of data acquired by an investigator. A one-way algorithm is created and applied when the investigator images evidence. If the hash value of the data before starting the imaging process matches the hash value of the copy, this demonstrates that the evidence has not been tampered with during the process to ensure its integrity and admissibility in court.

Chain of Custody

A chain of custody is a paper trail or sequential documentation of every step in the evidence-handling process, including collection, control, transfer, and analysis. It ensures the integrity of evidence and its admissibility in court.

Handling and Transportation

Each piece of electronic evidence should be stored in its own electronic evidence bag/box for transportation. Smaller devices could be stored together provided they are first labeled and logged. When transporting evidence, extra caution should be taken so that there is no damage or adverse effect from extreme weather conditions.

Encryption

All collected electronic data should be encrypted and secured at all times – during collection, in transit, and at its destination. Evidence must be encrypted using AES-256 at rest and TLS 1.3 in transit. Additionally, sensitive PII (Personally Identifiable Information) within the evidence may be tokenized or masked during the examination phase to comply with privacy-by-design principles while the investigation is ongoing.

305-447-6750 | info@ermprotect.com

Core Principles of Digital Forensics

Despite technological change, several core principles remain constant. They include:

1 **Preservation:** Evidence must be collected in a way that prevents alteration. This typically involves creating forensic images using write blockers and calculating cryptographic hashes to ensure integrity.

2 **Documentation:** Every action taken must be logged to maintain chain of custody. Chain of custody is a document that details all individuals who the evidence passed through, along with the hashes to ensure no one tampers with the evidence.

3 **Repeatability:** Another qualified examiner should be able to reproduce the findings.

Finally, analysis must be objective and defensible, free from bias or speculation. These principles ensure that digital evidence can withstand scrutiny in legal proceedings, internal investigations, or regulatory review.

Types of Digital Artifacts and What They Reveal

Digital artifacts are traces left behind by user activities, system processes, or malicious actions performed by an attacker. They exist across endpoints, networks, mobile devices, cloud systems, and applications. Each category of artifact provides insight into different aspects of activity.

File System Artifacts

File systems store information about files, directories, and metadata. This includes timestamps such as creation time, last access time, and last modification time. These timestamps can reveal when a file was downloaded, opened, modified, or deleted. File system metadata often forms the backbone of a forensic timeline, enabling reconstruction of events in sequence.

File system artifacts may also include remnants of deleted files, temporary files, and contents of recycle bins. Investigators can piece together these artifacts to recover deleted files. Forensic investigators can also use file system artifacts to state whether a USB was inserted, when it was inserted, and the make and model of the USB device. In addition, investigators can identify whether logs were deliberately cleared to conceal malicious activities.

Registry and System Configuration Artifacts

The registry artifacts contain information about which user installed malicious software, when it was installed, and how it was installed. This helps forensic examiners reconstruct events, develop a timeline, and try to determine the root cause of a security incident. System configuration artifacts also help investigators understand the persistence mechanisms established by the malware which help the attacker maintain access to the system, even after the system restarts.

Memory (RAM) Artifacts

Memory artifacts contain information on active processes, open network connections, encryption keys, and in-memory-only malware. Using these techniques, investigators can find out whether the attacker ran code in memory, without creating any files on the system. In addition, these artifacts can help investigators find the attacker's IP address.

Network Artifacts

Network artifacts include firewall logs, intrusion detection alerts, proxy logs, VPN logs, and packet captures. These artifacts help answer whether the attacker jumped from one machine to another, how many devices were compromised, and whether the attacker still has access to the network. They can also reveal evidence of whether data exfiltration has occurred and from which system. Further, in some cases, the network artifacts can reveal attacker IP addresses, domains that were accessed, and how much data was exfiltrated (in GBs).

305-447-6750 | info@ermprotect.com

Email Artifacts

Email artifacts contain timestamps, sender IP addresses, and authentication information. These details can help identify whether an email is a phishing email and the IP address from where it was sent. They can be used to determine if an email account has been compromised and then misused. They also help identify whether authentic emails are being diverted to another mailbox controlled by the hacker, a common technique.

Browser Artifacts

Web browsers store the history of websites visited, cookies, cache files, download logs, and autofill entries. These artifacts can reveal user browser searches, websites visited, file downloads, and timestamps.

Mobile Device Artifacts

Mobile devices contain call logs, SMS messages, application data, geolocation records, Wi-Fi connection history, voice mail, and cloud synchronization artifacts. These provide valuable evidence for investigations.

Cloud Artifacts

In cloud environments, artifacts are typically log-based rather than file-based. These include authentication logs, API call records, object storage access logs, and administrative activity logs. These logs can reveal who accessed a cloud resource, the IP address, and the actions undertaken, such as read, edit, or delete. Cloud artifacts help determine whether credentials were misused, whether data was downloaded in bulk, or whether new instances were spun up for malicious activity.

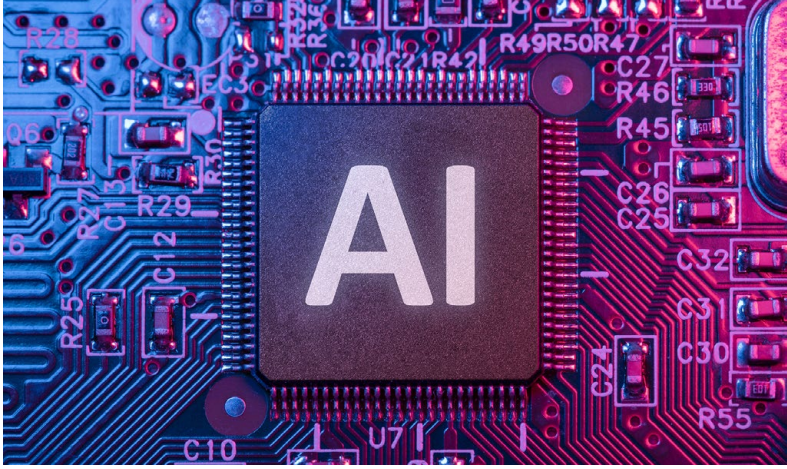
Application and Database Artifacts

Enterprise applications and databases maintain their own logs and transaction histories. These may include user login records, configuration changes, query histories, export activities, and access permission changes. These artifacts may prove critical in an investigation.

305-447-6750 | info@ermprotect.com

ERMProtect
Cybersecurity Solutions

Looking into the Future: Forensic Investigations of AI Misuse



As artificial intelligence becomes more common in business, mistakes and misuse are likely to happen. For example, an AI system can produce harmful content, leak sensitive data, or be used for malicious purposes. Forensic investigators can use system records and logs to determine what happened, how it happened, and who was involved.

Investigators can piece together a clear timeline. They can see what commands were entered into the system, what the AI produced as a result, and whether anyone interfered with or manipulated the process. This helps determine whether the issue was a genuine mistake, a system flaw, poor oversight, or deliberate misuse.

Investigators can also determine whether proper safeguards were in place. For example, they can identify whether access controls and monitoring tools were deployed. They can identify whether data used to train the AI may have been biased or inappropriate. And, if needed, they can often identify the specific user, insider, or external party connected to a security incident.

How do you Pick a Digital Forensics Company?

Choosing the right digital forensics provider is critical to the success and credibility of an investigation. Here are key factors to consider:

- **Analyze** if the computer forensics company or expert has experience with the platforms and systems relevant to the scope of the investigation. Even highly skilled examiners may not be the right fit if it is their first time working with the specific technology in your environment.
- **Assess** the computer forensic team's and company's qualifications. There are several digital forensics certifications that demonstrate expertise in forensic techniques, standards of practice, and legal principles. Common certifications include PCI Forensic Investigator (PFI), EnCase Certified Examiner (ENCE), EC Council Certified Incident Handler (ECIH), Certified Computer Forensic Examiner (CCFE), Certified Cyber Forensics Professional, and GIAC credentials such as GCFE, GCFA, GNFA, and Advanced Smartphone Forensics. It is also wise to confirm whether the team has experience providing expert witness testimony.
- **Check** to see if the computer forensic company has good references. Ask for client references and request a redacted forensic report to evaluate quality. A strong report should be "bi-lingual" — highly technical for IT teams yet clear and narrative-driven for judges or executives.
- **Verify** if the company has experience testifying in court in criminal or civil cases, before the investigation begins.
- **Examine** the company's security infrastructure. A professional lab should not be connected to corporate resources. It should be equipped with biometric access controls and monitored 24/7 to maintain physical chain of custody. Evidence storage should include fireproof, climate-controlled safes within a secure evidence room, and the company should regularly update its forensic tools and technology.

305-447-6750 | info@ermprotect.com

ERMProtect
Cybersecurity Solutions

800 S. Douglas Rd. Suite 940
Coral Gables, FL 33134

305-447-6750

info@ermprotect.com

ermprotect.com

Proven Protection.
Peace of Mind.