What Are the 5 Stages of a Digital Forensics Investigation?

By ERMProtect Staff

Digital forensics deals with the recovery, investigation and analysis of electronic data, and is often used to unearth evidence in litigation cases, criminal cases, or in internal investigations. Electronic data can provide critical evidence and clues in many cases, and aid in the discovery of cybercrime, data theft, crypto crimes, security breaches, instances of hacking, and more. Digital forensics play an instrumental role in getting to the bottom of complex data challenges.

Digital forensic investigators use a variety of tools and software to conduct investigations that can help to:

- Discover the source and cause of a cyberattack
- Identify whether a hack was perpetrated and how long the hacker had access to the system
- Create a timeline of criminal events, such as unauthorized access or altering of data
- Secure digital evidence

A digital forensic investigation can help identify and prove different kinds of wrongdoing, including data theft or disclosure, internet abuse, network or system breaches, espionage, and financial fraud.

In civil or criminal cases, it is crucial to carry out a structured and process-driven digital forensics investigation, to ensure the integrity of the data and its admissibility in a court of law. The core stages of a digital forensics investigation include:

1. Identification of resources and devices involved in the investigation
2. Preservation of the necessary data
3. Analysis
4. Documentation
5. Presentation

Data acquired in this way is permissible in court, and can be used as evidence to support litigation cases. Digital forensics investigators are trained in extracting and handling evidence in a way that is permissible in court, and their expertise can be invaluable in a litigation case involving digital data.

The Stages of a Digital Forensics Investigation

Digital Forensics Investigation Stage 1: Identification

The very first step in a digital forensics investigation is to identify the devices and resources containing the data that will be a part of the investigation. The data involved in an investigation could be on organizational devices such as computers or laptops, or on users' personal devices like mobile phones and tablets.

These devices are then seized and isolated, to eliminate any possibility of tampering. If the data is on a server or network, or housed on the cloud, the investigator or organization needs to ensure that no one other than the investigating team has access to it.

Digital Forensics Investigation Stage 2: Extraction and Preservation

After the devices involved in an investigation have been seized and stored in a secure location, the digital forensics investigator or forensics analyst uses forensic techniques to extract any data that may be relevant to the investigation, and stores it securely.

This phase can involve the creation of a digital copy of the relevant data, which is known as a "forensic image." This copy is then used for analysis and evaluation, while the original data and devices are put in a secure location, such as a safe. This prevents any tampering with the original data even if the investigation is compromised.

Digital Forensics Investigation Stage 3: Analysis

Once the devices involved have been identified and isolated, and the data has been duplicated and stored securely, digital forensic investigators use a variety of techniques to extract relevant data and examine it, searching for clues or evidence that points to wrongdoing. This often involves recovering and examining deleted, damaged or encrypted files, using techniques such as:

- **Reverse Steganography**: a technique used to extract hidden data by examining the underlying hash or string of characters representing an image or other data item
- **File or Data Carving**: identifying and recovering deleted files by searching for the fragments that deleted files may leave
- **Keyword Searches**: using keywords to identify and analyze information relevant to the investigation, including deleted data

These are just some of the many techniques digital forensic investigators to unearth evidence.

Digital Forensics Investigation Stage 4: Documentation

Post analysis, the findings of the investigation are properly documented in a way that makes it easy to visualize the entire investigative process and its conclusions. Proper documentation helps to formulate a timeline of the activities involved in wrongdoing, such as embezzlement, data leakage, or network breaches.

Digital Forensics Investigation Stage 5: Presentation

Once the investigation is complete, the findings are presented to a court or the committee or group that will determine the outcome of a lawsuit or an internal complaint. Digital forensics investigators can act as expert witnesses, summarizing and presenting the evidence they discovered, and disclosing their findings.

Selecting a Strong Digital Forensics Team

Digital forensics investigations are not just useful to law enforcement agencies or companies suspecting fraud on a large scale. They can also help corporations who suspect an employee is leaking data to an external party, or to determine the scope of and recovery from a cyberattack.

In case of a cyberattack, an investigation can help identify the source of the attack and secure systems against further breach, ensuring attackers no longer have access to the system. An investigation also helps take stock of the data that has been accessed, distributed or altered, and may even help in getting the original data restored.

A qualified and experienced digital forensics company like ERMProtect can help unearth evidence in cases of security breaches, data leaks or cyberattacks, and help win litigation cases. We are a worldwide leader in cybersecurity solutions and digital forensics, and can help mitigate your cybersecurity risk.

For information about how ERMProtect's digital forensics investigators can help, email

Get a curated briefing of the week's biggest cyber news every Friday.

This content isn’t available. Contact the owner of this site for help.

STOP THE PHISH

Turn your employees into a human firewall with our innovative Security Awareness Training.

Our e-learning modules take the boring out of security training.

Request A Demo

Intelligence and Insights

How To Test for PCI Compliance

October 26, 2023

PCI Compliance tests are a critical step in protecting yo outline the importance of PCI Compliance tests here ..

5 Types of Cybersecurity Penetra

October 18, 2023

If you are looking for ways to improve your comp five types of cybersecurity penetration testing ...

VIEW ALL INSIGHTS

Learn More About Our Services:

PCI Compliance
Penetration Testing
SOC 2 Reports
Digital Forensics & Incident Response
Comprehensive Security Assessments & Remediation
Regulatory Compliance
Chainalysis Demo
PCI PFI Credit Card Investigations

Free Guides
Our Company
ERMProtect Security Awareness Training
Blog
News Room
Careers
Privacy Policy – ERMProtect Cybersecurity Solutions
Terms Of Service

ERMProtect
800 S. Douglas Road
North Tower 940
Miami, FL 33134
Phone: (305) 447 – 6750
Email:
info@ermprotect.com