**What is Forensic Analysis and Why is it Important for the Security of Your Infrastructure**

With the advent of cybercrime in recent years, tracking malicious online activities has become imperative for protecting operations in national security, public safety, law and government enforcement along with protecting private citizens. Consequently, the field of **computer forensics** is growing, now that legal entities and law enforcement has realized the value IT professionals can deliver.

# What is Forensic Analysis

**Forensic analysis definition** can be described as a detailed process of detecting, investigating, and documenting the reason, course, and consequences of a security incident or violation against state and organization laws. Forensic analysis is often used for providing evidence in court hearings, especially in criminal investigations. It employs wide range of investigative procedures and technologies.

# The Steps for Conducting Forensic Analysis

By tracking digital activity, investigators can relate digital information to physical evidence. Digital forensics can also allow investigators to discover planned attacks and prevent a crime from occurring. There are five critical **forensic analysis components** involved in conducting a detailed forensic analysis, all of which are involved in contributing towards a successful investigation.

## Developing Policy and Procedures

Whether it’s about a criminal conspiracy, cyber activity, or an intention to commit a crime, forensic evidence can be highly sensitive and delicate. **Cybersecurity experts** know how valuable the information is, and understand that if it’s not properly handled and protected, it can be compromised easily.

For this reason, it is important to develop and follow strict **policies and procedures** for all activities related to forensic analysis. These procedures may include instructions on how to prepare systems for retrieving evidence, where to store the retrieved evidence, when to authorize forensic investigators to recover potential evidence, and how to document the activities.

## Assess the Evidence

The second key step in the forensic investigation is assessing **potential evidence** in a cybercrime. This assessment involves classifying the cybercrime in question, such as one related to identity theft, social engineering, phishing, etc. The investigator then needs to determine the integrity and source of data before entering it as an evidence.

## Acquire Evidence

This involves devising a detailed, rigorous plan to acquire evidence. All information should be recorded and preserved, and documented before, during, and after the evidence acquisition. The policies regarding preserving the **integrity of potential evidence** mainly apply to this step, since without evidence, the forensic analysis may be considered futile.

The general guidelines to **preserve evidence** include using controlled boot discs for retrieving critical data, physically removing storage devices, and taking required steps to copy and shift the evidence to the forensic investigation team. It is important to document and authenticate all the evidence when in a court case.

## Examining the Evidence

To examine a potential evidence, there should be procedures to retrieve, copy, and store evidence within the appropriate database. It can include a number of approaches and methods for analyzing information, such as using an **analysis software** to look for data archives with specific file types or keywords, or retrieving recently-deleted files.

Data that is **tagged with dates and times** is of particular importance to the investigators, along with any encrypted or hidden files. It is also useful to analyze file names, since it can help identify when the data was created, uploaded, or downloaded. It can also send files on a storage device to an online data transfer.

## Documenting and Reporting

Lastly, forensic investigators need to keep a record of not only software and hardware specifications, but also include all **methods used in the investigation**, including methods to test system functionality and copying, retrieving, and storing data. Documentation and reporting not only demonstrate how user integrity was preserved, but also ensures that all parties adhere.

# **Tools for Forensic** Analysis

Whether you require forensic analysis for an investigation into unauthorized server access, a human resource case, or a high-profile data breach investigation, these open-source digital forensic tools can help carry out memory forensic analysis, forensic image exploration, hard drive analysis, and mobile forensics. The tools give ability to retrieve **in-depth information** about an infrastructure.

Here are some of them:

* **Autopsy** – It is an open-source GUI-based tool that analyzes smart phones and hard drives. It is used worldwide for investigating what happened in a computer.
* **Wireshark** – It is a network capture and analyzer software tool that sees what happens in the network.
* **Encrypted Disk Detector** – It helps in checking encrypted physical drives and supports Bitlocker, TrueCrypt, and Safeboot.
* **Magnet RAM Capture** – It is used to capture physical memory of a computer to analyze memory artifacts.
* **Network Miner** – It is a network forensic analyzer for Linux, Windows, and Mac OS X for detecting operating systems, hostname, open ports and sessions by PCAP file or through packet sniffing.

# Importance of Forensic Analysis for the Security of Your Infrastructure

Forensic analysis importance can be understood by knowing the benefits it provides to your infrastructure’s security.

## Preventing Hackers

With digital forensics, cyber security companies have been able to **develop technology** that prevents hackers from accessing a website, network, or device. By knowing the trends of how cyber criminals steal or exploit data, cyber security software firms are able to protect relevant data and scan networks to ensure that outside parties cannot access it.

## Preventing Malware

Antimalware software is one of the biggest benefits resulting from digital forensics. Forensic analysis helps identify how a virus enters and behaves in a network infrastructure. The software developed as a result can detect **malware and spyware** and remove it before a vulnerability can be exploited.

## Retrieving Deleted Information

For any digital investigation, it is crucial to recover deleted information – especially in a data breach or in case of identity theft. Digital forensics uses **complex tools and techniques** to recover information and present it in the court of law or even in situations without court cases where recovery of data is essential.

## Identifying Vulnerabilities

Vulnerabilities are often not apparent, thus making it easy for hackers to exploit them. Forensic analysis techniques provide valuable information to present **typical weak areas** in an infrastructure, application, or website. Based upon this information, security software can pay attention to fix these vulnerable areas.

[VirtualMetric](https://www.virtualmetric.com/trial) provides **monitoring and analysis tools** to help you ensure performance and reliability of your infrastructure. Get a free [30-day trial](https://www.virtualmetric.com/trial) today to find out how our products work.