# Digital Forensic Analysis and Examination

## Introduction

The purpose of digital forensics is to answer investigative or legal questions to prove or disprove a court case. To ensure that innocent parties are not convicted and that guilty parties are convicted, it is mandatory to have a complete forensic process carried out by a qualified investigator who implements quality and quality control measures and follows standards. In this context, this document can be used as a starting point to understand the major phases of a digital forensics process and the key methods and guidelines applied. Furthermore, it details the critical components of a forensic examination to obtain consistent results.

## What Are the Steps in Forensic Analysis?

Digital forensics is a computer forensic science that involves the process of seizure, acquisition, analysis, and reporting of evidence found in electronic devices and media to be used in a court of law. Following is a detailed description of each phase.

**1) Seizure**

The seizure step involves marking the elements that will be used in later processes. Photographs of the scene and notes are taken. An important question to answer in this phase is whether or not to pull the plug on the network. Leaving the system online while proceeding may alert the attacker, allowing him to wipe the attack traces and destroy evidences. The attacker may also leave a dead man switch, which destroys the evidence once the system goes offline. In such circumstances, it may be necessary or advisable for to gather evidence from the system while it is running or in a live state, being fully aware that this causes changes to the system and reasons for taking this approach must be explained.

**2) Acquisition**

After the seizure phase comes the data collection/acquisition. The data must be acquired without altering or damaging the source to be analyzed later. Notice that an illegal seizure or improper methodology can affect the admissibility of the evidence in court. Following the applicable rules of evidence, evidence is admitted into court when permitted by the judge. For this reason, methods of acquiring evidence should be forensically sound and verifiable. Acquisition can be physical or logical. In physical acquisition, a bit stream image is captured from a physical storage media, while in a logical acquisition, a sparse or logical image is captured from storage media. In both cases, write blockers are to be used to prevent the evidence from being modified. The duplicate image must be verified that is identical to the source by comparing the hash value of the acquired image/copy and the original media data.

It is always recommended to start capturing from the most to the least data. The order of volatility is:

* Registers, cache
* Network state (ARP cache and routing table)
* Running processes
* Kernel modules and statistics
* Main memory
* Temporary files on disk

There are several tools for acquiring data, most of which are software-based and require training to successfully perform the collection phase. InfoSec Institute offers hand-on labs to learn and practice data acquisition and evidence collection using popular commercial and open-source tools in a real forensics environment and real use-cases.

**3) Analysis**

In the analysis phase, evidence should be extracted by interpreting the acquired information.  
Appropriate methodologies and standards should be followed during this procedure (described in the next section). The investigator should examine the acquired copy/image of the media, not the original media.

The examiner may use additional tools to conduct special actions and help retrieve additional information, such as deleted files. Those tools must be validated to ensure their correctness and reliability, as noted above. Referring to the requestor documentation, the examiner extracts evidence from the collected data. Typically, there are two approaches: The examiner looks for something he doesn’t know within something he knows. This can be infected programs, opened programs, erased documents, Internet history, or chat/calls history. Otherwise, he looks for something he knows in something he don’t know, trying to extract meaningful information from unstructured data, such as URLs, email addresses, or cryptographic keys through the use of carving techniques. The evidence found is then assembled to reconstruct events or actions to provide facts. In the case of multiple sources, the evidence is aggregated and correlated together. The facts may identify the attack scenario, attacker identity, attacker location, or any other relevant information, which is provided to the requestor.

In contrast with the seizure phase (which can be conducted by non-experts), acquisition and analysis phases must be conducted by experts. Examiners must have knowledge and be properly trained. InfoSec Institute offers accelerated in-depth computer forensics boot camp sessions that include seminar-style lectures and hands-on labs focusing on identifying, preserving, extracting, analyzing, and reporting computer forensic evidence.

**4) Reporting**

After the examination is complete, the results are reported, along with a detailed description of the steps conducted during the investigation. An examination report typically includes the following details: information related to the acquisition phase (the person who did the examination, when it was done, what software/hardware tools were used, and what version numbers), the original data hash and the acquired data hash, photographs taken. Detailed information related to the examination phase, such as descriptions of the examined media (volatile memory, hard disk, etc.), are also included in the report. This allows another examiner to be able to identify what has been done and to access the findings independently. Further actions are determined after the report is reviewed.