**Computer Forensics**

## What is computer forensics?

Computer forensics, also called digital or cyber forensics, is a field of technology that uses investigation techniques to help identify, collect, and store evidence from an electronic device. Oftentimes computer forensics professionals uncover evidence that can be used by law enforcement agencies or by businesses and individuals to recover lost and damaged data. Read on to learn about the computer forensics types, techniques, career paths, and more.

### Why is computer forensics important?

As the world becomes more connected digitally, digital evidence for solving crimes is becoming more relevant every day. A computer forensics investigator’s job is to collect, examine, and safeguard this evidence to help solve cybercrimes and to recover important compromised data.

## Types of computer forensics

Computer forensics always involves gathering and analysing evidence from digital sources. Some common types include:

* **Database forensics:** Retrieval and analysis of data or metadata found in databases
* **Email forensics:** Retrieval and analysis of messages, contacts, calendars, and other information on an email platform
* **Mobile forensics:** Retrieval and analysis of data like messages, photos, videos, audio files, and contacts from mobile devices
* **Memory forensics:** Retrieval and analysis of data stored on a computer's RAM (random access memory) and/or cache
* **Network forensics:** Use of tools to monitor network traffic like intrusion detection systems and firewalls
* **Malware forensics:** Analysis of code to identify malicious programs like viruses, ransomware, or Trojan horses

## Common computer forensics techniques

When conducting an investigation and analysis of evidence, computer forensics specialists use various techniques; here are four common ones:

* **Deleted file recovery.** This technique involves recovering and restoring files or fragments that are deleted by a person—either accidentally or deliberately—or by a virus or malware.
* **Reverse-steganography.** The process of attempting to hide data inside a digital message or file is called steganography. Reverse-steganography happens when computer forensic specialists look at the hashing of a message or the file contents. A hashing is a string of data, which changes when the message or file is interfered with.
* **Cross-drive analysis.** This technique involves analysing data across multiple computer drives. Strategies like correlation and cross-referencing are used to compare events from computer to computer and detect anomalies.
* **Live analysis.** This technique involves analysing a running computer's volatile data stored in RAM (random access memory) or cache memory. This helps pinpoint the cause of abnormal computer traffic.