Forensics

> [!toc] Table of Contents

Introduction

Forensics is a collective term for fields of work in which “criminal acts” are systematically investigated. In short: **when cops try to find evidence**.

Relevant subfields

Many forensic measures pose relevant threats to activists. These include:

- **Forensic linguistics**: Examines written language to identify the author of a text, for example. *Relevant for anonymous letters of confession, instructions, etc.*.
- **Physical forensics**: Examines fiber traces, DNA, tire or shoe prints, and fingerprints, among other things, to identify people who were present at a specific “crime scene” or who used a specific tool, for example. *Relevant for anonymous actions*.
- **Digital forensics**: Examines data on IT systems such as cell phones, PCs, servers, printers, etc.

> [!warning] {static}
>
> Digital forensics is almost always a threat, as digital devices store an enormous amount of information!

Digital Forensics

E.g. in the words of the German Federal Police Office:

"*In addition to traditional evidence such as files (paper), images, tools, or weapons, digital evidence is playing an increasingly important role in criminal investigations. Evidence includes data*

carriers in countless formats: PCs, e-book readers, printers, chip cards, optical media, mobile phones/smartphones, and SIM cards."

There are many things that can unexpectedly become (digital) evidence. Another thing that one should keep in mind is that digital forensic investigators can often restore files that were "deleted" a long time ago, which is why encrypting and securely deleting your stuff is so important.

Look at our countermeasure article about deleting data securely for more information on how to securely delete data and why it is so important.

> [!technical] How does a digital forensic investigation work?
>
> A forensic investigation is usually requested by prosecutors or courts and carried out by a “forensic expert.” Usually, the cops carry out the forensic analysis.
>
> Many forensic tools are offered to the authorities by external companies, e.g. Cellebrite for mobile phone forensics.
>
> Laptops and data carriers are usually not examined directly. Instead, an “image,” i.e., a copy, of the data carrier/hard drive is made, which is then examined. This is to ensure that no digital evidence has been falsified or corrupted.

Physical Forensics

We will not go into detail about physical forensics here. In general, classic forensic methods used in criminal investigations may also be relevant for activists. These include tracing:

- Fiber traces
- Shoe prints
- Fingerprints
- DNA
- *and more*

It is very difficult not to leave any physical traces. Physical forensic analysis is usually very time-consuming and costly. Nevertheless, individual case studies show that confused cops have ordered this even for minor offenses, even for simple ad busting actions.

Version #2
Erstellt: 2026-02-15 16:17:01 UTC von ESC-IT Migration Bot
Zuletzt aktualisiert: 2026-03-18 13:28:42 UTC von ESC-IT Migration Bot