COMPUTER FORENSICS AND CYBER CRIME ANALYSIS

Thats a lot of words in the title

Fabio Lorenzato

Contents

Part I

Legal part

Chapter 1

Introduction

Back in the days, it was really easy to analyze the communication between two people, because the technology was easier and know, meaning that the technology is *between us*. Nowadays the technology is more *about us*, for example we use AI for facial recognition. Another example are the social network algorithms that track our activity online. This means that we use the technology to be "analyzed" instead of using it only to communicate. Most likely, the technology will be *in us*, which not only means robotics, but also be more integrated with human beings.
In those scenarios, computer forensics became more complex, having to take in account no only the quality of data(ie: a voice call), but also the quantity, which makes mistakes more likely to happen in some instances. Another aspect of computer forensics will be to discern what is human from what is a machine(ie: deep fakes, generative ai), and in particular where the liability lies. Furthermore, it is necessary to handle the legal aspect of different countries, which is quite difficult because of natural language limitations. An ideal solution would be to translate laws in code, which is basically impossible, so we can approximate this solution with **legal design** This has still to deal with two issues, which are information overloading(too much information), and the fact that laws are written by lawyers for lawyers, which makes them difficult to understand.
Another aspect to consider is the GDPR, and the still to come AI act, for example the article 22 prevents automatic systems to make decisions having legal weight without the control of a human. An example of this is the Lex Machina framework, which was able to predict the decisions of the judges via ML methodologies, which was banned because it could influence the decisions of people and judges. After all, false positives in digital forensics **can change people lives**.

Chapter 2

Foundations of digital forensics

Chapter 3

Cybercrime Convention

Part II

Technical part

Chapter 4

Introduction to digital forensics

First of all, we need to understand some basic concepts.
Forensics analysis is the process of investigating and analyzing information to gather evidence to solve legal problems. In order to do that, the collections, preservation and analysis or presentation of digital evidence is required to support the investigation. **Computer forensics** does just that.
Forensic science is not a new field, it has been around since the ancient times. The first recorded use of forensic science was around 1900 BC in Babylon, where fingerprints were used to identify the author of a clay tablet. Digital forensics is a relatively new field, it started in the 1980s with the advent of personal computers, for example the first convicted person for digital crimes was Robert Tappan Morris, who created the Morris Worm in 1988, and found out by analyzing computer logs and network activity.

> **Computer Forensics** is the **discipline** that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.

In general, when carrying out a forensic investigation, the following questions are important to keep in mind to fully understand the crime scene:

- **What** happened? What is the timeline of events?
- **Who** was involved?
- **When** did it happen?
- **Where** did it happen?
- **How** did it happen?
- **Why** did it happen?
- **How** did the incident occur?

All this questions allow to **support legal proceedings**, the mitigation of damages and mature future prevention strategies.

4.1 Computer forensics goals

The main goals of computer forensics are:

1. **retrieve** the **input** data(ie: what has been typed)
2. **determine** the **actions** performed by the user (ie: what programs have been run)
3. **analyze** the **used files** (ie: what files have been modified)
4. **identify** the **damage** done to the system (ie: what files have been deleted)

> In essence, the goal of computer forensics is to **gain conprehansion** of **what happened**, at least technically speaking.