MANUSCRIPT

When software leads to false judgments.

In criminal trials, investigators must rely on forensics software that extracts data from cell phones, for example. But the programs are not transparent, sometimes overlooking data or misinterpreting traces. The result can be wrongful convictions.

By Piotr Heller

Aired on 3.3.2021 at Deutschlandfunk

Online Version:

https://www.deutschlandfunk.de/probleme-bei-digitalen-ermittlungen-wenn-forensik-software.684.de.html?dram:article_id=495189

MP3 File:

https://ondemand-mp3.dradio.de/file/dradio/2021/04/03/wenn_schlechte_forensik_software_kriminalisten_auf_falsche_dlf_20210403_1631_1a7ed524.mp3

Christian Hummert

"Personally, I have a bigger problem with security agencies buying tools from some company somewhere abroad and these tools are an intrusion on fundamental rights and no one has looked at what those tools actually do."

-- Start of the first on air conversation --

Manfred Kloiber - Presenter

That's what Christian Hummert from the Central Office for Information Technology in the Security Sector, or ZITiS for short, says. Piotr Heller is with me in the studio. Piotr, what kind of tools are we talking about?

Piotr Heller

That's about IT forensics tools. This is software that investigators use in criminal proceedings, i.e. to crack confiscated cell phones and to bypass encryption. They also use it to extract pictures or chat logs, even if they have already been deleted.

Manfred Kloiber - Presenter

And they cause problems?

Piotr Heller

Let me tell you about a case. An IT forensics expert from a public prosecutor's office in Bavaria recently described it at a conference. It happened in 2016, when a mother discovered an abuse video of her daughter on her partner's smartphone. The man snatches the phone from her, flees, the police catch him, but of course the video is deleted. The forensic experts now use such a commercial tool to copy the entire memory of the cell phone to their computer. This works completely. No error message. They then search for traces of the video. But they find nothing. Only because the mother is

so convincing, they go one step further. They open the smartphone. Only then do they see: This particular model has two memory chips. But the software didn't recognize the second one. On the second chip, they then find the video. The problem here was: It was not obvious even to the expert what exactly the software does and what it can miss.

Manfred Kloiber - Presenter

So you can't rely on their results?

Piotr Heller

You shuld not, but investigators often have to. Just a few figures: Last year, there were over 100,000 cases of cybercrime in Germany, and 300,000 cases in which the Internet was used as a means of committing the crime. And we're not even talking about robberies or traffic accidents, where there are also digital traces. In order to be able to process these many cases at all, the evaluation must be automated to a certain extent. Another case the forensic scientist told us about shows how this works. It was again about images of child abuse. The forensic scientist analyzed the defendant's cell phone with a processing tool. Among other things, it showed him which terms the man had entered into a search engine. And there were terms there that, according to this forensic scientist, you really only know if you are entrenched in this "child pornography" scene. It came to the trial and then it was suddenly revealed that the search engine had suggested these terms to the defendant. He didn't know them at all, which was a bit exculpatory in the end. He selected them from the suggestions and did not enter them himself. But the tool did not distinguish that. But these are important details in a criminal trial.

Manfred Kloiber - Presenter

Let's take a look at how big the problem really is and how they are working to prevent it.

-- Start of the first narrated element --

Tobias Eggendorfer

"We have cases like that every now and then, where tools don't detect it correctly or misjudge it."

Narrator

Explains Tobias Eggendorfer. The computer scientist teaches at Ravensburg-Weingarten University and is an expert in IT forensics. One fundamental problem is that investigators have to hand over some of their forensic tasks to the tools, otherwise they can't keep up. However, the tools' errors are sometimes not noticed in the subsequent criminal proceedings.

Tobias Eggendorfer

"We then have miscarriages of justice as a logical consequence because, of course, the wrong evaluation of evidence leads to wrong results."

Narrator

" Miscarriage of justice" sounds theoretical. But the bottom line is that a person is wrongly convicted or a criminal gets away with it because the specialists at the police and public prosecutor's office may not know how their digital tools work. To some extent, this lack of transparency is even deliberate. After all, the manufacturers of forensics software want to keep the security loopholes they use to crack smartphones to themselves for as long as possible.

Tobias Eggendorfer

"I consider that to be very, very problematic in forensic proceedings. Because if I can't say how I got the data, I'm depriving the judge of the opportunity to evaluate the evidence. In order to do this, the procedures would have to be fully documented, the terms would have to be defined in a

meaningful way, and, if necessary, manual traceability would have to be ensured. That's where we actually have the problem with many commercial providers that they naturally hold back on the other hand, it's a matter of protecting business secrets."

Narrator

This has gone so far that some forensics companies no longer even include the function to crack the latest cell phones in their software. Instead, they offer paid data extraction, which they perform in their own labs. So an investigator has to give away a potential piece of evidence.

Tobias Eggendorfer

"This kind of approach is familiar. I think it is highly problematic. Because at that moment you might have signatures in which they say: We have handled the evidence carefully. But you don't know what really happened in the meantime. And that is naturally something where you can ask in a trial: Does it fit together? Or were the incriminated images or something like that possibly added in the course of the preservation of evidence?"

Narrator

The largest provider of such services is the Israeli company Cellebrite.

Tobias Eggendorfer

"I know that the company Cellebrite also supports German investigative agencies."

Narrator

The company itself left our questions about the process of its service and its customers unanswered. Christian Hummert, who heads digital forensics at the Central Office for

Information Technology in the Security Sector, or ZITiS for short, takes a similarly critical view of such services.

Christian Hummert

"There are many companies that do the digital evaluation, digital forensics for the security agencies. But these are private providers. But this is an original state task. That is an encroachment on civil rights. If your cell phone is confiscated, we have certain institutions that are allowed to do that: The police and the Federal Criminal Police Office, not companies that act on behalf of public prosecutors."

Narrator

ZITiS, founded in 2017, is to develop its own such forensics methods for the German authorities as a centaral body. However, these are mainly special solutions to crack systems used by criminal groups in Germany for which there are no solutions on the market. They do not develop their own tools to read, for example, chat logs of widely used programs such as Whatsapp.

Christian Hummert

"So if we were to start developing our own Celebrite now.... That would be relatively expensive for the German taxpayer. So what's important, though, is that these products are reviewed and evaluated. And that's what we're doing."

Narrator

In addition, ZITiS is collaborating on the European "Formobile" project. One of the goals is to standardize digital forensics for cell phones in criminal proceedings.

Christian Hummert

„We actually want to describe the process from the first moment a police officer touches a cell phone - We call him

the first responder - ro the moment when the expert witness gives his presentation in court."

-- Start of the second narrated element --

Manfred Kloiber - Presenter

Piotr, what exactly should these standards from the Formobile project describe?

Piotr Heller

First of all, the handling of the evidence: How is the cell phone stored? How is it packed? and so on. Then it's about the tools. They have to have been checked. That's a point shared by many experts: Clearly, manufacturers can't disclose their methods....

Manfred Kloiber - Presenter

... because they are using things that - I would say - come from this gray market for security vulnerabilities.

Piotr Heller

... exactly. And those are just secrets. But they should at least open up more to external audits that check the software.

Manfred Kloiber - Presenter

What happens to these standards then?

Piotr Heller

These will now be published and discussed, and then the European Institute for Standardization CEN can make something like this an official standard. This will allow such forensics laboratories and tools to be given a seal of

approval: "I function according to this standard". And then there may also be a change in the criminal procedure code that says: Digital traces must be secured according to this standard.

Manfred Kloiber - Presenter

So that should still take a little while, and even then it wouldn't be impossible for mistakes like the ones you described at the beginning to happen, would it?

Piotr Heller

Something could still slip through, of course. That also happens in trials, where you're not dealing with digital traces. But somehow it's special here because judges and lawyers and all of us, have a kind of understanding of things in the real world. You understand a car accident or malpractice at the doctor's office. You still need expert witnesses to judge that, but you have an understanding. In the digital world, things are sometimes so abstract that that understanding isn't there. This Formobile project aims to change that. One very important point is to develop training concepts for investigators and lawyers by 2022 so that they can gain an understanding of digital traces, assess them correctly and ask the right questions.