communication@formobile-project.eu
Linkedin – Formobile-project
Twitter – @Formobile2019
www.formobile-project.eu

Mobile forensics needs a holistic approach

The Central Office for Information Technology in the Security Sector (ZITiS) works on several research projects. One of them is entitled "From Mobile Phones to Court" (FORMOBILE). The project is about mobile phone forensics by authorities and organizations with security tasks (BOS). Dr. Christian Hummert, the ZITiS business unit manager for digital forensic science talks about this project - the questions were asked by Behörden Spiegel's editor Marco Feldmann.

Behörden Spiegel: Dr. Hummert, what are the goals of the research project "From Mobile Phones to Court" (FORMOBILE), where ZITiS participates?

Dr. Christian Hummert: FORMOBILE is a major EU mobile forensics project that explores the entire investigation chain. This means for us that the project starts with the so-called first responder, i.e. the investigator who comes first into contact with a phone by securing it. The process then moves to a forensic laboratory – where data backup, data decoding and data analysis are covered. Finally, the evaluation report for a phone and the presentation of the results in court are considered. The project has three key pillars: 1) to create new tools that support investigators and forensic laboratories. 2) To create a European standardised process for mobile forensics and 3) to develop a modern training to expand and strengthen the skills of the parties involved in the field.

Behörden Spiegel: Who else is working on the project?

Hummert: In FORMOBILE, 19 partners from fifteen countries work together. The consortium covers a broad spectrum of different institutions. Next to five police authorities, who give a practical perspective to the project, there are also the Dutch Forensic Institute (NFI) and ZITiS - both with highly specialized laboratories of digital forensics. We are especially happy about the industrial partner MSAB. As a major manufacturer of products of mobile forensics they have the necessary know-how in order to exploit the project results- taking them to the market and thus to the street. Furthermore, we have first-class universities and colleges in the field of digital forensics in the team, but also an NGO and lawyers who check, that our tools and the standard are not violating applicable law or the restriction of civil rights.

Behörden Spiegel: Is there a need for a Europe-wide standard for the forensic examination of mobile phones?

Hummert: There is currently no European or international standard for mobile forensics. Although, mobile forensics is an essential element in the preservation of evidence and the investigation of criminal offences. Furthermore, the results must be admissible in court. In the project, we interviewed 49 European police authorities. Only 65 % said they had any standard to follow in their work. The most common standard applied is ISO 17025. That is a standard for laboratories for testing and calibration, and thus very different from the process of a mobile forensic examination.

Behörden Spiegel: How should the standard look like?

Hummert: Europe continues to grow together unfortunately, this also applies to the field of cross-border crime. The security authorities must face up to these challenges. For this purpose, it is essential that data from a smartphone, read out in France, are also accepted as evidence by a German court.

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme. H2020-SU-SEC-2018, under grant agreement no.832800

There is still plenty that has to be standardised, starting from procedural instructions to forms. FORMOBILE strives for a standard with a high level of acceptance by the security authorities and society. Therefore, we develop a so-called CEN workshop Agreement (CWA), which can be further developed into an EN or ISO standard after the project. To achieve results, we held large workshops with all stakeholders involved to ensure that all interests were taken into account. Currently, the CWA is publicly available and can be commented on by citizens of the EU.

Behörden Spiegel: What does the standard regulate?

Hummert: The new standard has four major sections: a) the people who are using the devices, b) the tools that are used, c) the process from the first responder to the court and (d) the legal framework by which mobile phone forensics is governed. Through this approach, various things are regulated from little things like packaging and transport of traces to the selection of appropriate forensic tools.

Behörden Spiegel: ZITiS leads a work package in the project that defines the requirements of European police authorities. What are the requirements of the police?

Hummert: First of all, we prepared a long questionnaire for the European police authorities and asked how they proceed in the field of mobile forensics, and where are their biggest issues? Of course, there are very different authorities, and it is difficult to compare a highly specialised security authority- such as the Forensic Institute in the Federal Criminal Police Office with a police station somewhere in the EU. However, only 52 % of the security authorities interviewed declared that they are optimally prepared in the field of mobile forensics.

Behörden Spiegel: What consequences have you drawn from this result?

Hummert: Of course, in the frame of the project, we do not want to rely on a single questionnaire. Therefore, we started an extensive ring trial, where sets from six specially prepared phones and wearables were sent to respective laboratories. We compared the evaluations afterwards. As a result, not only the approach of the various European authorities varied greatly from each other, there were also large differences in the quality of the evaluation.

Behörden Spiegel: And what happened then?

Hummert: From the results of the questionnaire and the ring trial, we concluded the requirements for the project results. This concerns the standard as well as tools and training. Overall, we elaborated 164 functional and non-functional requirements from the results. For the technical tools, which will be developed in the project, they were converted into technical specifications.

Behörden Spiegel: What challenges do you face when decoding mobile data?

Hummert: In many smartphones, the data are stored encrypted. Cryptography (encryption technology) was formerly reserved for the military or intelligence services; today, it is nearly omnipresent. Many users do not even know that their data in the smartphone are encrypted. On the other hand, there are special crypto phones that are mainly used in organized crime - making it additionally challenging for mobile forensics.

Behörden Spiegel: What other difficulties are there?

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme. H2020-SU-SEC-2018, under grant agreement no.832800

Hummert: There is an almost infinite number of different apps available to users. The data are not located in uniform file formats on the phone; conversely, each app has its own data format for which a dedicated decoder has to be developed. In FORMOBILE, we develop tools to bypass the encryption or to obtain the password. This is a hugely demanding work package, but so far, we are very successful with this.

Behörden Spiegel: The FORMOBILE project will continue until April next year. How should it go on afterwards?

Hummert: The European Commission has supported the FORMOBILE project as a part of the current HORIZON 2020 funding program initially with almost seven million euros for three years, we are very thankful for that. Of course, we are not just finished after three years – there are many more open questions in mobile forensics. In addition, ZITiS has further internal projects on mobile phone forensics, apart from the FORMOBILE project. Moreover, the consortium of the project will not drift apart immediately after the end of FORMOBILE. FORMOBILE is a big project with more than 70 people working; many of them are young people who write their PhD theses as part of the project. Despite COVID, the project has also brought Europe a little bit closer together. For me, it is normal now, for example, to just quickly call our partner in Bulgaria for certain questions. Before FORMOBILE, I would have never done that.

Behörden Spiegel: What remains to be done?

Hummert: After April 2022, there is still a lot to do such as developing the CWA into an EN or ISO standard or continuing the training. We will see if there are new funding opportunities or other possibilities for the project to move forward. FORMOBILE is very successful and has been recently evaluated favourably by the European Commission - we should definitely go on this important path in the future.

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme. H2020-SU-SEC-2018, under grant agreement no.832800