NFI developing tools to extract data from counterfeit phones

News item | 01-07-2022 | 09:14

Criminals use mobile phones to communicate, coordinate, organise and execute illegal activities. Mobile phones present a unique challenge to law enforcement agencies worldwide due to the large numbers and variants in circulation. This means that the way to extract the data stored on these mobile devices will be different in each individual case.

In order to establish the truth of events in criminal cases, it is critical that law enforcement agencies are able to access relevant information stored in mobile devices. Digital traces stored on mobile phones can help officials reconstruct crimes and serve as incriminating or exculpatory evidence. 'Everyone is familiar with the major mobile phone brands – however, equally, there are thousands of counterfeit phones on the market. Just as branded clothing is counterfeited, iPhones are likewise counterfeited,' says Coert Klaver, a forensic researcher who was in charge of this Formobile sub-project, on behalf of the NFI. 'We analysed hundreds of counterfeit phones. All of these phones work in slightly different ways and as such the data always has to be extracted in slightly different ways.' The counterfeit phones are particularly common in Eastern European countries, but are also found by the police in the Netherlands. 'We have now developed software with the Swedish mobile forensic technology company MSAB that the police can use to copy data from the different types of counterfeit telephones, which makes the work of law enforcement agencies a whole lot easier at an international level.

Decoding and analysis

Within the Formobile project, the NFI also assisted on the development of an analysis tool that records data from various sources and makes it searchable. The tool is called the 'Joint Semantic Analyser' (JSA)

and is able to capture information from various Apps (such as Signal, Mail and Telegram) as well as capture information in text from a variety of forms (photos, videos) and make it searchable. JSA will record anything that is visible on photographs and videos and is audible in audio files in text, such as 'the person is armed'. All data is placed on a timeline, which makes it searchable.

In addition, the NFI has developed a tool with TU Delft as part of Formobile to be able to read the working memory (RAM) of mobile phones. Working memory is a form of temporary data storage. 'Not everything that is stored in the working memory is stored in the ordinary memory. Working memory will sometimes contain data that can be interesting from a forensic point of view, such as drafts of emails or search queries that someone might have put in.'

Tools to acquire, visualise and analyse

The research within Formobile focused on several sub-areas: the initial objective of the Formobile project was the development of innovative technology (hardware and software) for the acquisition, analysis and visualisation of data from mobile phones. The data from the phone must first be copied unaltered from the phone after the relevant phone has been seized, after which the information from the phone must be decrypted and decoded. The third step relates to the analysis and interpretation of the data, which includes establishing who the data belongs to, how it got there and what it means in the context of a specific case.

A new standard and a training programme

The project likewise involved an examination of legal and ethical issues. 'These days, the contents of someone's phone tell us more about a person than how they furnish their home. The greater the infringement of someone's privacy, the more types of permission are needed. Occasionally, the permission of the Public Prosecution Service will suffice – however, if the extent of the infringement increases, permission from the court is likewise required', Klaver explains. For that reason, a standardised forensic process has been developed to extract data from mobile phones in a manner that is technically as well as legally and ethically sound. Work also took place on the development of a European standard for Digital Forensics, ↗CWA 17865:2022. Various forensic laboratories work with the ISO standard 17025. 'However, this standard is not quite suitable for digital forensics. As yet there is no standard for digital forensics carried out on mobile phones. Digital forensics is highly dynamic and the ISO 17025 is not really suited to that.' A precursor to the ISO for digital forensics on mobile phones was published by Austrian Standards International this past March. 'Basically, an ISO 17025 for digital forensics, which now can be used to move forward.' Finally, Formobile provides a training programme to teach law enforcement agencies to use the tools effectively and follow the established procedures.

'International collaboration is crucial'

The three-year Formobile project involved nineteen European organisations working together to facilitate research into (crypto)phones that can be linked to crimes – from the crime scene to the courtroom. 'The field of digital technology moves very rapidly', says Klaver. 'It cannot be compared to a field like forensic pathology, in which, naturally, developments likewise take place, however, the research object itself – the human body – is not prone to much change over the years. The converse is the case for us – we're studying phones today that will be obsolete tomorrow.' International collaboration and knowledge sharing is therefore crucial, which is a fact that was highlighted by the German university that led the initiative to set up Formobile in 2018.

Pride

'When I look at everything the project yielded, I feel extremely proud', says Klaver, looking back on the project. 'Even companies that develop tools to read mobile phones and that would normally compete with one another took part and collaborated within this project to help advance their field. These various parties collaborated on the development of a new digital standard – regardless of which tool will ultimately be used to read mobile phones. It was great to witness.'