Yuval Ben-Moshe looks at the part played by mobile digital forensics in identifying criminals, arresting them and bringing them to justice, and argues there is now nowhere to hide for terrorists and criminals

DIGITAL HIDE AND SEEK

Mobile digital forensics is changing the way police forces and security agencies are approaching investigative processes. But criminals are evolving as well. The use of the Internet to commit crimes warrants an entirely different approach from investigators, as does the use of mobile phones to organise and execute sometimes very detailed criminal activity.

Police in the UK are fighting a two-front battle, however. On the one hand they have to deal with the threat of government cuts, and on the other they are fighting a continual battle with smarter, increasingly tech-savvy criminals. Thankfully the tools available to the police, to help with catching the "mobile criminal", are increasing in both volume and effectiveness.

The London riots in 2011 were a stark reminder of how the "unruly mob" is wising up to developments in mobile technology. The calls to arms that many gangs sent out were orchestrated via messaging services, such as Blackberry Messenger (BBM). Co-ordinating meeting times and planning the rioting became all too easy for criminals, and a large number of them were never brought to justice.

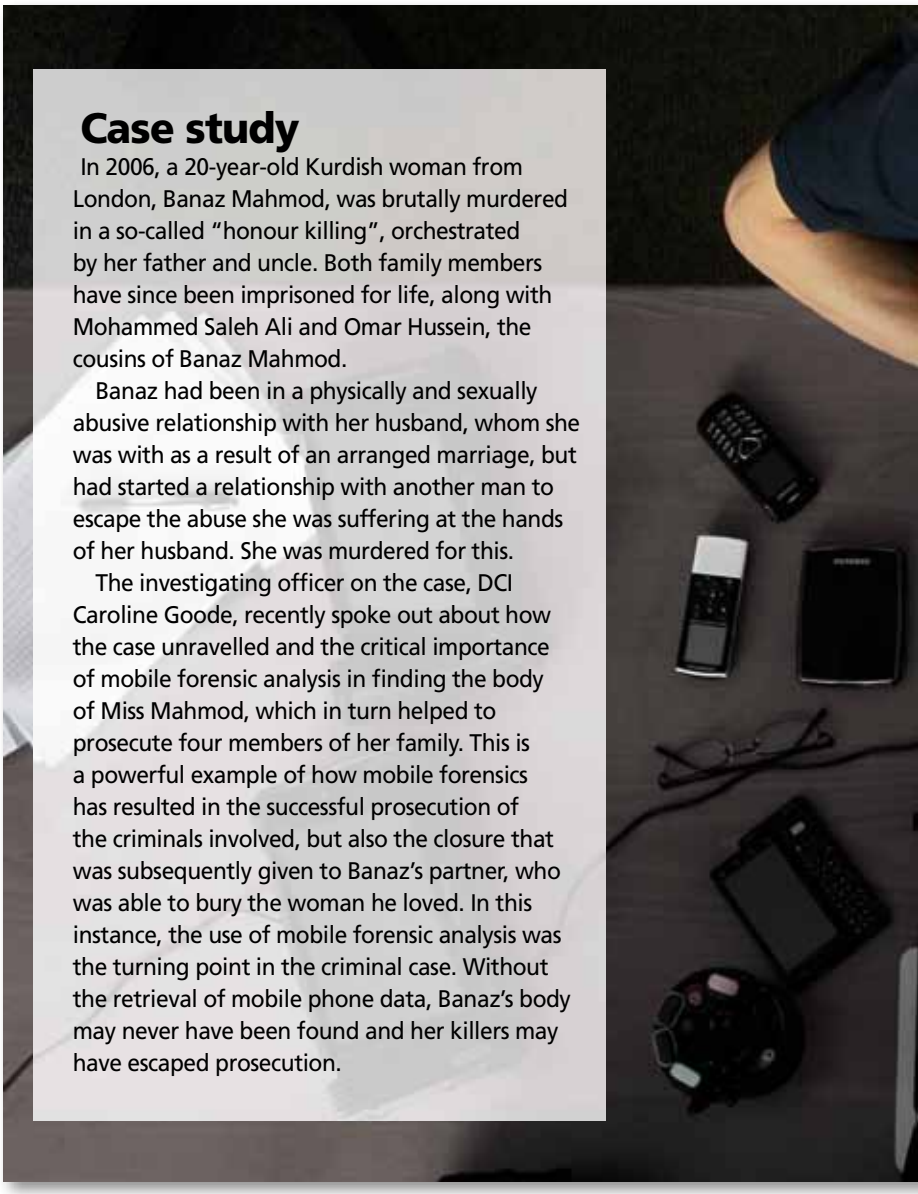
Subsequent reports stressed the need for greater family and community support to discourage youths from falling into the vicious circles of gang violence. But this only deals with the problem on a social level. Support needs to be given to the police in the form of cutting-edge technology to prevent gang-related crime and help to ensure that the perpetrators stand trial for the crimes they commit. In an age where criminal communication is extremely advanced, law enforcement agencies across the country must have a digital toolbox at their disposal to combat smarter criminal activity.

One major area of technological communication that criminals are exploiting is the use of mobile devices. Messaging applications, mobile calls, SMS and emails are all ways in which criminal networks stay connected, and this is an area that must warrant considerable attention from the police.

There is a three-part process for effective mobile data collection. The first part is the actual extraction of the data. This involves connecting the phone with an extraction device to access the phone's storage. After the extraction has taken place, the decoding of data from the mobile phone is designed to convert the data into its native format so that it can be analysed by the forensic team. The final stage is the analysis of the mobile data. This stage allows police to read patterns of communications between criminals and put pieces of the investigative puzzle together.

The mobile forensic process will improve their chances of obtaining evidence that can prevent a potential crime from occurring or to bring a criminal to justice. But there is no rule of thumb when it comes to mobile forensic investigation. Every case is different and, for

With so many digital devices available, forensic software and hardware tools must be highly adaptable



©Cellebrite

Case study

In 2006, a 20-year-old Kurdish woman from London, Banaz Mahmod, was brutally murdered in a so-called "honour killing", orchestrated by her father and uncle. Both family members have since been imprisoned for life, along with Mohammed Saleh Ali and Omar Hussein, the cousins of Banaz Mahmod.

Banaz had been in a physically and sexually abusive relationship with her husband, whom she was with as a result of an arranged marriage, but had started a relationship with another man to escape the abuse she was suffering at the hands of her husband. She was murdered for this.

The investigating officer on the case, DCI Caroline Goode, recently spoke out about how the case unravelled and the critical importance of mobile forensic analysis in finding the body of Miss Mahmod, which in turn helped to prosecute four members of her family. This is a powerful example of how mobile forensics has resulted in the successful prosecution of the criminals involved, but also the closure that was subsequently given to Banaz's partner, who was able to bury the woman he loved. In this instance, the use of mobile forensic analysis was the turning point in the criminal case. Without the retrieval of mobile phone data, Banaz's body may never have been found and her killers may have escaped prosecution.

that reason, varying approaches may be needed to fully optimise the forensic technology. Creativity among investigators is essential because mobile devices are not meant to be interrogated. They were not designed to have police teams rip data from them, and so a level of experimentation is required by investigators for more challenging cases.

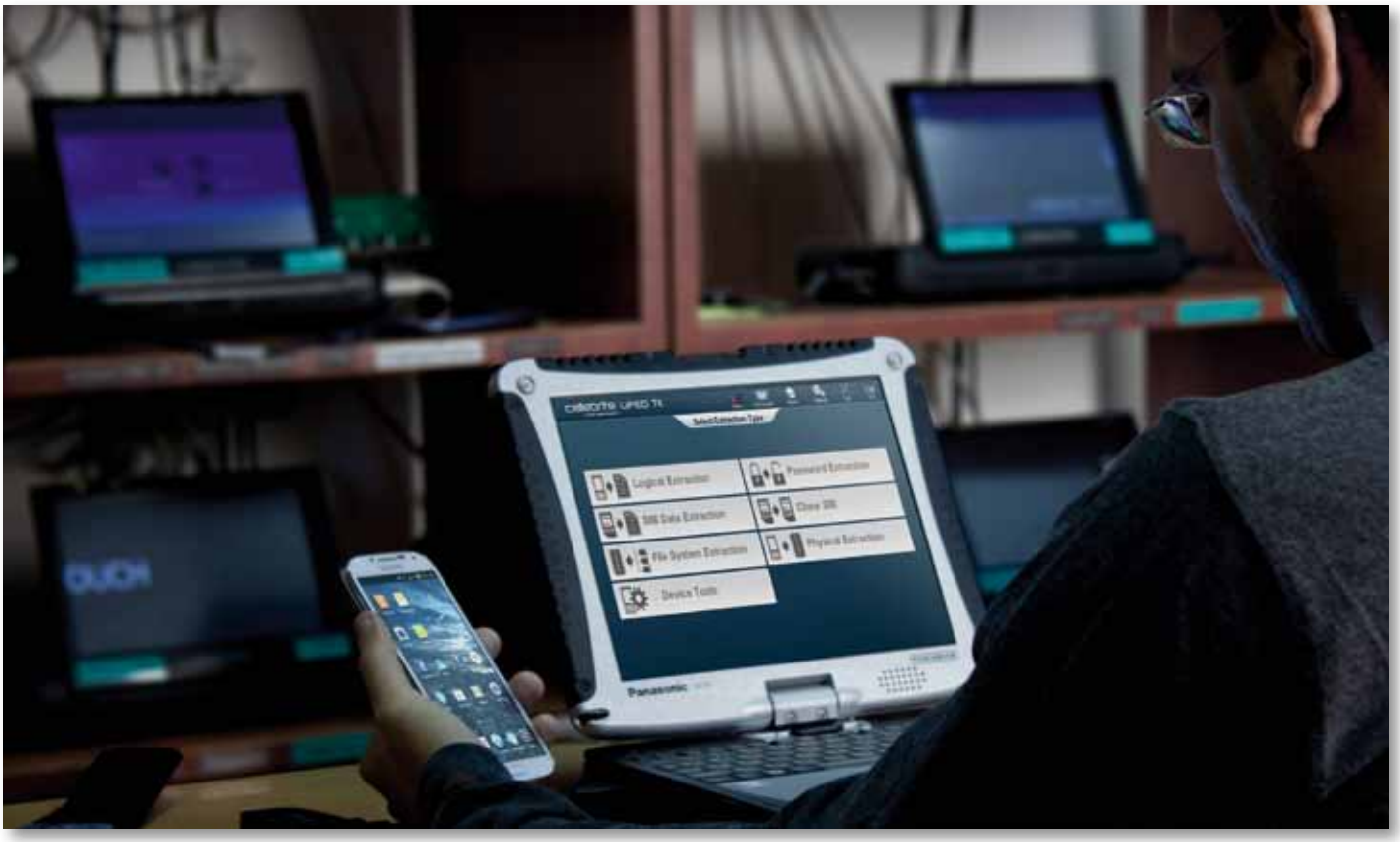
The latest mobile forensic equipment can drill deep into mobile data. Investigators can now use such software to identify how long communication between criminals has being going on for and who they are talking to on a regular basis. These forensic tools can deal with all three processes in mobile data collection: extraction, decoding and analysis, and the latest tools can help police gain all the mobile data they require for any investigation, for example by enabling investigators to securely and accurately extract decode and analyse mobile data on their existing laptop or PC. They can enable access to a vast number of locked mobile devices, with the capability to bypass the user's lock code.

Ruggedised systems are also available that have been designed for the tougher conditions that investigators face. Such systems can be used in conflict zones where terrain is likely to be rough or significantly damaged and with time restricted by the urgency of the situation. As with standard forensic equipment, every case differs so investigators have to choose the right tool in order to effectively extract mobile data from a suspect's phone.

In a case where time is of the essence, perhaps in a kidnapping incident, a quicker analysis of mobile data will be needed. What is called a "logical extraction" gives general data, rather than an in-depth breakdown,

"There is no rule of thumb when it comes to mobile forensic investigation; every case is different."

DIGITAL HIDE AND SEEK



©Cellebrite

in a much quicker time. A "physical extraction" provides a detailed history of data in a suspect's phone and takes more time to extract and analyse. In a murder investigation, where lots of evidence needs to be collated and triple-checked, the physical extraction option would be the most effective.

Any investigation is about gathering information and building up a picture. Just as biological forensics helps to put pieces of the puzzle together, mobile forensics can give more information about people and their habits. In addition, this can help identify alternative leads for the police and can help to identify key facts within an investigation.

On a macro-scale, mobile forensics has a significant role in protecting the public. As an application for counter-terrorism and homeland security, the technology can prove to be a necessity for the prevention of terrorist activity. Mobile forensic technology is critical in the conviction process, but it's equally as important in the initial stages of an investigation. Terrorist activity is frequently planned months, if not years, in advance, so a build-up of intel is needed to unravel any planned attacks and ultimately prevent them.

Although mobile forensic analysis works well in time-limited situations, with the correct technology it's also a powerful tool in cases where information needs to be built up over the course of a longer period of time. In July this year, for example, a joint investigation between Spanish and Belgian police resulted in the seizure of over five tonnes of hashish and multiple assets, as well as the arrest of more than 40 members of an organised crime ring. Mobile forensics played a vital part in the solving of this case, and Cellebrite's UFED devices were used by analysts from the European security agency, Europol, to extract mobile data from the suspects' phones and to analyse it.

This case shows the importance of mobile forensics when it comes to dismantling organised crime, and there are few limitations when it comes to the size of the investigation. It's in cases such as these that mobile forensic technology really comes into its own. Working in tandem with other investigative processes, it helps the authorities to drill down deeper into investigations.

The process of examining data is a science but, as with all sciences, changes occur that need updated solutions. Just as viruses mutate, forcing scientists to develop remedies to combat the bacteria, methods of communication mature, meaning investigators have to think outside the box in order to stay one step ahead.

And it is not just police and security forces that have to stay in the loop with technological developments. The mobile forensics industry must ensure it is also one step ahead of criminal operations, and provide law enforcement agencies with the latest software to fight the constantly evolving advances in criminal communications.

Mobile technology is on a steep upward curve and most criminals now operate using mobile devices. To ensure no stone is left unturned, police forces need to not only have the correct forensic software in place, but also to have the knowhow to operate the equipment, and not just by simply reading the manual.

As criminals innovate, so must the police. Relying solely on technology can be detrimental to an investigation, and investigators should apply human rationale while operating the forensic technology to better understand the criminal and the patterns that manifest.

Secrets unlocked: data extracted from mobile devices can help build up a picture of the suspect's activity, contacts and habits

Yuval Ben-Moshe is senior forensics technical director at Cellebrite, a leading provider of forensic solutions for mobile devices including smartphones, tablets and portable GPS devices. In this role, Mr Ben-Moshe acts as subject matter expert for the company and as a central knowledge hub, assuring the company's tight and intimate connection with the forensics community of law enforcement agencies worldwide.