



Searching for mobile gold

Mobile forensics is becoming widely established as a vital component of modern policing with forces across the country embracing the technology and increasingly “doing it for themselves” rather than relying on third party outsourcing – something that actually makes economic sense. And interestingly, the more complicated that mobile phones become the better a source of potentially incriminating data they are. Jose Sanchez de Muniain finds out what the fuss is about and uncovers how the latest smart phones are – literally – forensic gold mines.

Mike Dickinson is the Country Manager (UK and Ireland) of Micro Systemation, a leading manufacturer and global supplier of mobile forensic examination hardware and software. He remembers how only a few years ago the involvement of mobile phones evidence in crime investigations was minimal. Forces would typically outsource the devices for examination by third parties – and that worked fine at a time when most forces didn’t know when the next device would come in. Today the situation has changed radically to the extent the majority of investigations involve mobile phones in some way or another. “It is almost impossible for the police not to have the phone examined as part of any serious investigation,” he says.

The sheer volume of handsets involved has tipped the balance of cost to the point that for many forces it no

longer makes financial sense to outsource every device to a specialist company. Many police forces are now doing it for themselves, setting up specialist units that can carry out the same type of work as commercial service providers, and using the same mobile forensics devices. And with budgets being cut and forces looking at saving money, many are realising that training and equipping themselves to do the examination is economically viable.

The picture today, believes Dickinson, is that around 90% of the UK police is equipped with mobile forensics technology to some extent.

Lancashire Constabulary

Trevor Pollard heads up the mobile phones examination unit within the scientific support department of Lancashire police. The unit is relatively new – just 18

months old – and prior to that phones were either examined by two officers who sat within the major investigation team, or outsourced to a number of third parties: “We realised that the cost of outsourcing mobile phones coupled with the results we were expecting were not adding up. We realised we could do it in-house just as well and also at a lower cost.”

More importantly, Trevor and his team understood that the plethora of mobile phones in the market meant no one organisation could be expected to hold all the answers – but on the other hand the collective knowledge and experience of all police forces could do just that.

Today the unit runs a triage system consisting of a central unit of four technicians, two admin staff and Trevor Pollard as head. The central unit trains a further six divisions who are capable of screening the phones under the triage system. “The triage involves basic screening of phones to see if there is anything of evidential value, using a piece of nominated kit,” explains Trevor.

If more in-depth screening is necessary, phones are passed on to the central unit for further examination.

Trevor is very clear about the importance of mobile forensics. “These days the fingerprint of someone’s life is on their phone, and the more complicated the phone the more stuff they put in them. They are a goldmine of information.”

The system in Lancashire is still in its infancy but Trevor says it seems to be working: “I think we saw the opportunity earlier than other forces and now they are following suit in some way – but of course each will have its own policy to operate under.” For forces that are thinking of setting up a similar structure, Trevor recommends that they visit a number of local forces already operating a system and take the best bits from each one: “The main challenge is going to be the number of phones versus the number of staff you’ve got.

“We anticipated in Lancashire for the first year 2,500 mobile examinations. Today it looks like we will have done 4,000+ phones. And if you think if you outsource these, on average it would be around £200 each, we are talking nearly one million pounds in Lancashire alone.”

Some outsourcing is still carried out in Lancashire (a dozen perhaps in the last six to eight months), but not due to volume but the type of requirements that were

called for: “And in any case they couldn’t do what was required anyway.”

The technology

So what does mobile forensics actually entail? Mike Dickinson from Sweden-headquartered Micro Systemation is one of the two main global players that manufacture the devices that extract the data from the phones. He explains how there are two ways of extracting details from a mobile: either doing a so-called “logical” analysis or a “physical” analysis – and the two are very different with only a few companies worldwide being able to comprehensively offer the latter.

“The logical analysis is the automated equivalent of a person scrolling over every screen on the mobile and taking a photograph of each one. The positive side of this is that a logical analysis is probably good enough for 80% of cases.”

On the downside, explains Dickinson, for the majority of handsets this type of examination won’t provide deleted data, and it cannot bypass security protocols eg if a phone is locked.

“Then you have the physical approach, where the operating system is bypassed and the real memory is examined to make sense of the binary code on the chips – this is called the ‘hex dump’.”

Dickinson provides a useful analogy of the difference between the two: “A logical analysis is the equivalent of a suspect walking into a police station with a big folder under his arm and saying, ‘here is the evidence’, you are too good for me’.

“Physical analysis is the equivalent of getting a search warrant and going to a suspect’s house and going through his filing cabinet, dumping the contents on the floor and then finding the missing bit of paper that was at the back of the drawer and which even the suspect had forgotten about.

“And then to your horror you find that that bit of paper that will incriminate the suspect is not only shredded, but also written in Swedish. So to make sense of it you have to tape it back together and get someone to translate it back into English – and that is called decoding.”

A physical analysis is a two-step process that involves first “dumping” the real binary data – which is basically gibberish due to the fact that it has been written in the operating system of that particular phone – and then decoding to make sense of it.

“But what that gives you is the opportunity to recover deleted data – which is the holy grail of mobile forensics; deleted images and text messages,” says Dickinson.

So how is it possible to recover data that has been deleted? Interestingly, Dickinson puts it down to lazy programming. “When you press the ‘delete’ button on the screen, it doesn’t actually destroy the data but it just flags it up saying that this is now available for overwriting. If the operating system has not written over it before it is examined then it can potentially be recovered.”

There is a caveat however – whether or not an operating system has written over data is anybody’s guess. It may be possible to gain data from five years ago, but not from five months ago.



“A logical analysis is the equivalent of a suspect walking into a police station with a big folder under his arm and saying, ‘here is the evidence’, you are too good for me’.”

➤ *Mike Dickinson, Country Manager, UK and Ireland, Micro Systemation.*



The tailoring strategy of Radio Tactics is in evidence in the latest release of the Aceso v5, launched in May this year. Aceso v5 is Radio Tactics’ flagship mobile forensics suite, which provides information on 2,800 handsets, including what information can be extracted from them.

Mobile forensics



Geotagging is becoming very popular – where satellite coordinates are stored within data. Below right: the CelleBrite Universal Forensic Extraction Device (UFED).



“We are very much aimed at the front line of law enforcement and this is an important distinction. We offer the immediate possibility to access information, by ensuring the user experience is such that the process of the examination of the devices is as easy as possible, without prejudicing the forensic value of the information being recovered.”

➔ **Andy Gill,**
Co-founder,
Radio Tactics.

“In the world of computers and operating systems there are Windows, Apple, and Linux – only three systems – therefore only three system standards,” explains Dickinson. “But in mobile phones it is like having 1,000 Bill Gates and they are all successful. And each one has a different operating system, which means manufacturers of mobile forensics have to write specific code for every phone in the market.”

The physical examination of handsets is still relatively new and forensic devices that can do it have only been commercially available for around two years. This means the levels of support for physical examination ie technical support from the manufacturers, is lower than logical support, mainly because each phone has to be reversed engineered to allow it.

The growth in smart phones is an important driving factor too – in Dickinson’s words, they are “cannibalising the rest of the electronics sector” (think digital cameras and sat nav features increasingly available for free on mobile phones): “That means there is more and more data stored in them and a higher need to interpret that information. Geo-tagging is becoming very popular, where satellite coordinates are stored within data. When you take a picture it also embeds in the file the geodata of where you were standing at that moment. Now you can retrieve that information from smart phones.”

Forensics on the front line

Andy Gill is co-founder of Radio Tactics, a UK-based manufacturer of front-line mobile phone forensic equipment ie equipment that can extract data from the operating system of mobile phones, but not recover and interpret data that has been deleted – ie logical examinations as opposed to physical examinations.

“We are very much aimed at the front line of law enforcement and this is an important distinction. We offer the immediate possibility to access information, by ensuring the user experience is such that the process of the examination of the devices is as easy as possible, without prejudicing the forensic value of the information being recovered.”

Typical installations vary from custody suites where property is being confiscated and examined – and where it may be useful to present certain evidence to a suspect as soon as possible – to office-based installations such as

in CID units where there is a need to have fast access to the information contained in mobile phones. “In some cases a customer wants the equipment to be static, such as when there is an element of security and a dedicated room. In other instances portability is key, for example in a vehicle, for transportation to a crime scene.”

There is no off-the-shelf solution for law enforcement, and certainly not in the UK. Gill explains that 43 different police forces in the UK translates into 43 different views on how even basic operations should be conducted, which means each mobile forensic device has to be very much tailored to each force. “The various features are tailored depending on the culture of that constabulary and the level of control or freedom they want to give to the end user. It can range from one extreme to another – from just permitting the end user to print off a report without any electronic media, even excluding images; to creating a report that contains all the information but is only created in output format like pdfs.”

The tailoring strategy of Radio Tactics is in evidence in the latest release of the Aceso v5, launched in May this year. Aceso v5 is Radio Tactics’ flagship mobile forensics suite, which provides information on 2,800 handsets, including what information can be extracted from them. This latest version allows for the easy examination of handsets that don’t have SIM cards – and Gill sees this as somewhat of a technical breakthrough: “It packages a number of well-understood techniques that would be used in the laboratory environment by an expert user. We have packaged it in a safe auditable way that can be used at the sharp end without prejudicing any subsequent examination by an expert.”

The new technology allows the examiner to create a SIM card for the relevant handset whilst providing very clear guidelines on the limitation on the type of data that is recoverable. “In general terms examining a handset without a SIM card can very much restrict the data that can be recorded.”

Radio Tactics’s Aceso solutions for front-line mobile forensics are installed in nearly 30 forces in England, and while this could be in various specialist policing units, for Gill the most effective use of this technology would be in the custody suite environment. “It is there where the biggest opportunity lies to gather information from devices – whilst processing people. Within our customer base only a handful have them at that particular point.”



Mobile forensics

The ISO 17025 standard could be introduced as early as 2012 in order to ensure a standard set of operating procedures throughout the country

Below right: Cellebrite's devices allow users to extract data in the field.



Evidence

Dan Williams is a mobile phone forensics investigator at CY4OR, a global computer forensics company that conducts investigations on a broad range of digital media, including computers, PDAs and mobile phones. Williams' duties involve acquisition of handsets, examination, reports, and witness statements, plus appearances at court as an expert witness if required. While traditionally CY4OR's workload would mostly entail law enforcement work, the company has noticed a shift away from this work and now there is a 70-30% split in favour of commercial cases. Such cases may relate for instance to the examination of company handsets used by a departing employee (eg to check no data has been lifted): "There is a rise in IP theft because the plethora of small devices such as thumb drives means it is much simpler, and therefore perhaps more tempting. But it does leave footprints we can investigate." Today, explains Williams, the trend in the police is towards "civilianising" many of their units. "Traditionally officers could have served two years in the cybercrime unit, and then gone back on the street. But they realised that it didn't make sense to train them up and spend all that money to then do that."

Williams handles between 10 and 20 devices per week. "Most investigations ask for a logical examination, but often the Defence is more interested in a physical examination in order to get deleted information. Often a client may feel that deleted text messages may turn the case in their favour. Or they may want to get hold of call logs that are no longer viewable on the handset as they may have been deleted."

So what kind of issues require clarification in court? Williams says most court appearances relate to technical clarification. "With mobile phones dates and times are often called into question – the log of when a text was sent, for example, may differ from a billing record.

That's often down to date and time changes on a handset, and how that could have happened. If a battery dies the phone may reset the time and date. Also, the only completely accurate times on phones are actually on inbound text messages, because those dates and times are put on by the telephone network – other dates and times are taken from the handset locally. So sometimes the Court needs more detailed explanation."

Market developments

Cellebrite is a main player in the global market of mobile forensics. Last month it unveiled the Universal Forensic Extraction Device (V1.1.3.8), which supports over 2,500 mobile devices including TomTom Navigation as well as the new Apple iPad device.

Yossi Carmil Co-CEO of Cellebrite, explains how in the UK alone Cellebrite has over 400 devices in use, mostly in the law enforcement arena but also in the military. In addition there are more than 1,500 cellular points of sale equipped with the Universal Memory exchanger device on the commercial side, in mobile device shops (for unlocking phones and retrieving data etc).



"In different countries you see a different typology of handset users. In some countries criminals are typically using low-end phones, in others they are using high-level or smart phones."

➤ *Yossi Carmil,
Co-CEO,
Cellebrite.*

Mobile forensics

Trevor Pollard opening the UK Law Enforcement Mobile Phone Examiners' Conference in Blackpool. The next event will be held around April 2012.



"One of our largest customer segments is on the military side. As you can imagine, having arrested a suspected terrorist and having the capacity to extract data on the field and put it on a USB stick to begin data analysis to identify terror suspects is a huge advantage.

"As regards law enforcement, at the beginning mobile forensic devices were primarily purchased by cybercrime units but today we are seeing it as something that is wanted by every unit – regardless of country," points out Carmil.

That there is currently a global trend in mobile forensics is clear. Cellebrite itself is an Israeli-headquartered company that was bought by a Japanese firm two years ago and today it has subsidiaries in China and Japan. "We have discovered that mobile forensics is only at the start phase in these countries, very much like in many other developed Western nations. We have caught the trend very quickly and created support and user interfaces, but more importantly, started supporting highly complex Japanese handsets. A year and a half ago Japan didn't have any support but today they have more than 50 Cellebrite devices in use there," says Carmil.

The need for mobile forensics equipment that can support as many devices as possible is driven by many factors. "In different countries you see a different typology of handset users. In some countries criminals are typically using low-end phones, in others they are using high-level or smart phones. In Japan, however, only smart phones are used, which offers the possibility of lots of content – deleted or not."

Manufacturers such as Cellebrite are often able to support a mobile device at the point of launch into the market. "Based on our dominating position in the civil market where more than 140 operators are customers, we are receiving the handsets up to three months before the launch."

A developing sector: standards

There is a standard that could be introduced as early as

2012 (ISO 17025) by the UK Forensic Science Regulator Andrew Rennison. Indeed throughout 2012 a number of workshops were organised in the UK to raise awareness on accreditation in the forensic sector. "It will be a challenge to introduce the standard but if we want to have credibility in evidence within all the sector – whether private or law enforcement – then regulations will have to be adhered to," believes Trevor. He adds that "credibility" in this sense refers to having a standard set of operating procedures – including quality assurance – as regards how mobile phones are handled as evidence.

What is clear is that this branch of forensics is moving forward at a fast pace and becoming highly organised. It now even enjoys its own annual event, the UK Law Enforcement Mobile Phone Examiners' Conference, organised by Trevor and which includes a mini exhibition too (the next one will be held around April 2012). "It is more about workshops than presentations, and we cover areas such as how to set up a mobile forensics unit, how it has been achieved in different forces, sharing problems and experience, as well as putting facts and figures forward."

Micro Systemation's XRY Logical and/or XRY Physical Office Version is delivered in a briefcase to ensure that the system stays complete and organised.

