

Forensic Analysis of Mobile Phones

A white paper on the nature of mobile phone evidence and how to secure it

John Butler, Geode Forensics Ltd.

8 May 2008

By 2006 91% per cent of adults in the United Kingdom owned or used a mobile phone.

In the UK we are increasingly relying on our mobile phones. By the end of 2006 there were more than twice the number of mobile connections than landline connections. More UK households now rely just on a mobile phone (9%) than rely just on a landline (7%) and in 2006 total mobile call minutes accounted for over one third of all call minutes.

Today's consumers are using their mobiles for much more than just making phone calls. Some 41% of mobile phone users regularly use their phone as a digital camera, 13% use it for internet access, 10% listen to FM radio broadcasts and 21% use it as a mini games console. In 2006 mobile users in the UK sent 20% more texts than the previous year¹. Mobile users make on average 20 mobile calls/week and send 28 text messages (27 calls and 70 texts for 16-24 year olds²).

Nearly every one of us therefore carries with us a record of who we spoke to and who spoke to us, what we sent and received text messages about, photographs we took and even calendars of what we did and when. The younger we are the more complete this record can be.



Modern phones can carry data equivalent to 12 Encyclopaedia Britannicas on a chip the size of a fingernail. If we use the phone to take photographs or browse the World Wide Web this will be recorded and much of what is recorded about our activities persists even after we think we have deleted it.

Forensically the phone can be a vital tool in demonstrating guilt or innocence if secured soon enough. Though the phone's capacity is huge, the way information is organised means that some items are overwritten very quickly. Most phones only record details of the last 40 or so calls after which time older entries may be overwritten. For average users phone call logs will start to wrap around in a week or so and text message stores will fill every few weeks.

¹ http://www.ofcom.org.uk/media/news/2007/08/nr_20070823

² www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/medialit_audit/medialit_audit.pdf

Unlike PCs each make and model of phone has its own standards, characteristics and quirks. Most can be read via a compatible cable, Infra-Red or Bluetooth though some older or budget phones have no means of acquisition and data extraction has to be done 'manually' – a euphemism for punching up the data on the phone keypad screen by screen and photographing the results. At all times the phone must be kept isolated from any contact with any network since the moment it gains contact with the service provider information will be lost.

A number of tools exist for interrogating phones, the most popular being XRY, CellDEK, PhoneBase, Paraben Cell Seizure and MobilEdit! Forensic. All have their advantages and disadvantages and it is often necessary to read the phone on two or more applications and check the results manually to ensure nothing was missed.

One difference between a phone and a PC is that the phone has much greater control over access to memory than does a PC and some phones encrypt memory. A result of this is that though information may be present within the phone the phone may not allow access to all of it and *in extremis* the only way of getting at it is to break the phone open and read the memory directly. This is rarely necessary and the facilities to do this are restricted to a very small number of large forensic companies. Reading the phone this way may result in destruction of the phone.

The mobile phone is a combination of a handset plus a SIM card and often a memory card. The SIM contains all information necessary to identify the subscriber plus a limited number of text messages and call logging records. In a modern phone most information is recorded in the handset. The memory card if present will tend to be used to store pictures, games, applications and music tracks and is generally much easier to read than the phone.

Information that can be expected to be present on a mobile phone

This includes

- Serial numbers of the SIM (the *ICCID*) and the handset (the *IMEI*) though not necessarily the phone's own caller ID (07xxx-xxxxxx).
- A date and time. This will usually have been supplied by the phone's owner and will be used to timestamp call records and outgoing text messages. Incoming text messages are time-stamped by the service provider.
- Details of previous calls made, received and missed.
- The Abbreviated Dialling Numbers list (the contact list or phone book)
- Text messages received, saved and draft copies, though probably not sent messages. Where sent text messages are vital then these may need to be obtained from the recipient's phone.
- Some deleted text messages of all categories.
- The IMEI number of previous handsets that have been used with the SIM.
- The last cell the phone was attached to.
- Any photographs present plus some deleted photographs. Many digital images contain information embedded within them such as when a photograph was taken

and this information can also include the make, model and even serial number of the phone or camera that took the photograph. This means that even if images are found away from a phone it may be possible to say something about their origin.

- Calendar entries

In addition to the phone itself, under the terms of the Data Retention (EC Directive) Regulations 2007³ service providers are obliged to keep information for all connected calls for 12 months from the date of communication, namely:

- The caller and called telephone numbers of each call, the details of the registered users of those telephones plus the International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity (IMEI) of both phones.
- The date and time of the start and end of the call or text message.
- The telephone service used.
- In the case of pre-paid anonymous services, the date and time of the initial activation of the service and the cell ID from which the service was activated, the cell ID at the start of the communication and data identifying the geographic location of cells by reference to their cell ID.

This information can be important as it may cover a longer period than the phone's own record and will be time-stamped by the service provider unlike calls in the phone handset which will be time-stamped by a time set by the phone user. Phone companies will not give this information out freely however and in all likelihood the phone's owner will need to request it him or herself.

Securing phone evidence

If phone evidence is likely to be of value then it is essential that a phone is secured at the first opportunity and either switched off or wrapped in several layers of tinfoil to isolate it from its network. PINs should be recorded along with the phone's caller ID (07xxx ..) and the owner should be asked to state whether the phone was loaned out or another SIM used with it during the time of interest. If possible a custody receipt should be made out and added to as the phone changes hands⁴. To most people a phone is an essential item and the owner should be reassured that forensic analysis will be conducted with the utmost urgency and returned as soon as possible (this can usually be completed within a day or two).

Where a phone has been seized as a Crown production and a defence opinion is required it is still advisable to arrange this as soon as possible – if the phone is in storage more than a month or two the battery can discharge at which point the clock is no longer valid. In certain phones this can affect the dates and times displayed for entries in the call logs.

³ H.M. Government: <http://www.opsi.gov.uk/si/si2007/20072199.htm>

⁴ e.g. <http://www.geodeforensics.com/docs/custody.pdf>

Summary

Recommendations concerning phone evidence including additional points from the ACPO Good Practice Guide for Computer based Electronic Evidence⁵:

- Secure mobile phone evidence at the first opportunity
- If you are certain you know the PIN for the phone ensure that the phone is switched off and remains off until it can be examined under controlled conditions.
- If you don't have the PIN or otherwise aren't sure that the phone can be restarted after being switched off then wrap the phone in a couple of layers of tinfoil and send it to a forensic service by courier or special delivery. If the phone charge level is low then it may be worth trying to charge the phone first.
- Obtain any relevant PINs and the phone number.
- Establish who is the registered owner if there is one.
- Establish the recent history of the phone and whether SIMs have been swapped between phones.
- Consider whether additional evidence is required from the service provider or other phones and arrange to obtain this where possible.
- When dispatching the phone for analysis then pack it securely so that it cannot be turned on or off accidentally in transit.
- Record details of custody of the phone on a form that accompanies the phone. Though this may be unnecessary, in our opinion it can't hurt and may help forestall some issues about admissibility of evidence.

VI.3 8/5/2008

Geode Forensics has facilities to examine mobile phones and extract data under controlled conditions and uses XRY, PhoneBase 2 and Mobicedit! Forensic.

Fees for a straightforward examination and report are based (2008) on a charge for 2 hours of SLAB time and for most common phones can be completed and the phone returned within 2 business days. Examinations can be undertaken 'in the field' at a somewhat higher charge plus travel.

Geode Forensics Ltd.

3 High Buckstone

Edinburgh EH10 6XS

Tel: 0131 445 3705

Mob: 07775 791396

<http://www.geodeforensics.com>



⁵ www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf