Forensic extraction of electronic evidence from GSM mobile phones

Dr A J Goode, CEng MIEE [1] (ajg@fss.org.uk)
The Forensic Science Service

1.0 Introduction

At the scene of a crime, traces of evidence can be recovered which can be used to help identify the crime which occurred, the perpetrators and the victims involved. Forensic investigation aims to recover these traces so that scientific evaluation can be applied to assist the court in reaching a fair verdict.

At a modern crime scene it is likely that a mobile phone will be recovered. Although it may be possible to recover traditional forms of trace evidence (such as fingerprints, DNA) from such a device, equally important evidence can potentially be retrieved from electronic data stored on the phone. For example, in the case of a murder, the murderer's identity could be available as one of the 'last dialled numbers', or 'last calls received' recorded on the device. The extraction of hi-tech evidence such as this requires care, because (as with traditional crime scene investigation) careless handling can destroy evidence.

Evidence extraction and recovery is a vital part of forensic investigation. It is handled through standard operating procedures (SOPs) which govern the collection, preservation and analysis of evidence. Because of the rapidly changing nature of modern technology, procedures for handling hi-tech evidence must be continually updated, but the underlying approach for handling evidence remains similar. This approach aims to ensure thoroughness and consistency of forensic examination [ACPO 1999].

Mobile phones are as useful to criminals as they are to the general population. In using a mobile phone a surprisingly large amount of personal data is supplied by the user, and significant data is recorded by the network provider. In criminal investigation the data available from a phone represents important forensic information about the phone user and their network of contacts. It is vitally important that forensic science develops techniques and procedures to recover electronic trace evidence robustly and with forensic integrity. It is also important that the privacy of this personal data is protected by law from misuse.

This paper will consider the types of electronic evidence that are available from a mobile phone, and introduce a forensic procedure for extracting them. Network information and phone tracking are also discussed. The paper concludes by considering aspects of future development, and the problems and opportunities such developments will potentially bring forensic investigations.

2.0 Forensic electronic evidence available from a mobile phone

A mobile phone is a complex communication device which communicates with other phones through the radio access network via RF links, but which also has substantial capability for data storage in the device itself. Mobile phones are rich in information which can provide extremely useful forensic data if the phone is involved in the planning or execution of criminal activity.

The mobile phone memory and subscriber information module (SIM) card hold phone number lists (such as address book numbers and last dialled numbers) which may contain critical evidence for an investigator. For example, a stalker may harass their victim by making repeated calls to their mobile phone. The call list on the victim's phone may have registered the number used by the perpetrator recorded in the 'received calls' list, and similarly the victim's number may be registered on the perpetrators call records.

There is normally a list of calls recently dialled on a mobile phone, unless this list has been cleared by the user. The phone also has the capability of storing names and phone numbers from which the user can choose to dial. Extracting this information yields valuable information about the user's network of contacts, and may provide links to other phones involved in the investigation.

[1] ajg@fss.org.uk

2.1 Location of stored information on a mobile phone

The SIM card is a smart card which contains an embedded microprocessor with ROM and RAM memory It may contain the subscriber's phone number and personal identification number (PIN) where this is set up. The subscriber using a SIM card is identified by the IMSI (international mobile subscriber identity), a 15 digit number globally unique to the subscriber which indicates the subscriber's country and network operator. Not all the information stored on a SIM card is known to or easily accessible by the subscriber. The SIM can easily be transferred to another mobile phone. Removing the card can have important implications forensically since for certain devices some data from the handset memory is deleted in this event.

Phone number lists can be stored in either the SIM card or the handset memory. In some devices, this is under control of the user. The handset may support a more comprehensive extended character set than the SIM card which is limited to 128 characters under the present standard. This extended character set is available for use with the address lists and text messages stored on the handset, although transmitted text messages collapse the characters into the standard set.

SMS (short messaging service) text messages are another source of useful forensic information. These messages can be stored on the SIM card, or in the handset memory. SIM cards adhere to the present smart card standard (ISO 7816), which limits the character set to 128 standard characters, but handsets are able to extend this character set to include for example animations and unusual character types.

2.2 Identification information from a mobile phone

A GSM (global system for mobile communications) mobile phone is marked with a unique identifier, the IMEI (international mobile equipment identity). This number is marked on the handset, and is also stored in electronically on the device. As a result of the recent alarming levels of theft of mobile phones, the UK government has encouraged network operators to prevent modification of the IMEI by subscribers, so that stolen phones can be more successfully barred from the network. The GSM standard GSM09.02 2.1.8) defines an equipment identity register (EIR) to enable the management of equipment identities for mobile stations.

The question of who owns a mobile phone is linked to the IMEI number. The question of who pays the bill is linked to who owns the SIM card that made a call (IMSI number). A helpful analogy is that the IMEI is like the chassis number of a car; whereas the IMSI is like the registration number of the car. Both these identifiers are important in criminal investigation.

It should be noted that none of this information can be definitely linked to the individual who was actually using the phone when a suspect call was connected, since mobile phones and SIM cards can easily be transferred or stolen. Linking an individual with a series of events involving mobile phones requires careful investigation, and may eventually involve extraction of individualising trace evidence (e.g. fingerprints, DNA , voice recognition) from the device itself.

2.3 Network information available for forensic investigation

Network information is monitored by the network operator and may be highly significant in forensic investigation. For example the IMSI and IMEI of the caller; the number called; the date, time and duration of the call; and the transmitting cells where the call began and ended are all items of information available to the service provider. In general however, service providers have different data available, and store it for different amounts of time.

When the mobile phone is switched on but no calls are in progress the phone is in a standby mode. In this quiescent state it will still enter or attempt to enter communication with the network, for example to perform a location area update. In this way the network normally maintains information on the location of the phone, whether it is in its home network, or roaming in another network or in another country.

Location information is available through the HLR (home location register) or the VLR (visitor location register), and is used to locate the subscriber and connect calls to or from the phone. This information is available to the network operator, and can be made available to the forensic examiner under certain legally controlled conditions.

Billing records also contain information about the calls made by a subscriber, such as call timing and duration. It can be important in forensic investigation to establish whether a call shown in the 'last numbers dialled' list was actually connected. This information can be obtained from billing records.

Maps of signal strength measurement can be important for reconstruction of the use of mobile phones at or near a crime scene. This type of evidence can be difficult (both physically and legally) to obtain. Physically, because a trained forensic reporting officer must capture and analyse the data at the level of the radio and signalling links. Legally the difficulties arise from the Regulation for Investigatory Powers Act 2000 (RIPA) legislation designed to protect personal privacy.

Because of the very large amounts of data continuously available to the network operators, detailed records are not maintained for long. In an investigation, it is important to capture what information might be helpful as quickly as possible.

3.0 Forensic procedure for hi-tech evidence extraction

Evidence extraction and recovery are handled through standard operating procedures (SOPs) which govern the collection, preservation and analysis of evidence. Because of the rapidly changing nature of technology, procedures for handling hi-tech evidence must be continually updated. The forensic approach to this aims to ensure thoroughness and consistency of forensic examination. The Association of Chief Police Officers' good practice guide [ACPO 1999]builds upon principles that were developed in collaboration with the International Organisation of Computer Evidence [SWGDE 1999]. These principles are summarised below.

- *No data should be changed by the investigator which may subsequently be relied on in court*
- *Where original data must be accessed on a target computer, the operator must be competent to do so, and must be able to give evidence explaining the relevance and implications of their actions*
- *An audit trail of all processes applied to the evidence must be created and preserved. An independent third party should be able to examine those processes and achieve the same result*
- *The officer in charge of the case is responsible for ensuring that the law and these principles are followed. This applies to the possession of and access to information contained in a computer. They must be satisfied that anyone accessing the computer or using a copying device complies with these laws and principles.*

Existing guidelines and procedures focus on the collection of digital evidence, but provide little guidance on the forensic analysis of the evidence these systems and devices may contain. As technology has developed devices have emerged which are not directly covered by the guidelines.

Crime reconstruction is traditionally used to gain a more complete understanding of the crime using the available evidence. This technique can be adapted for use in assessing forensic evidence present in digital systems [Casey 2002]. The clues used in crime reconstruction may be categorised as

- *relational* - where an object is in relation to another object, and how the objects interact with each other
- *functional* - the way something works or how it was used
- *temporal* - the times related to evidence and events

For example, in an investigation involving mobile phones, significant information is elicited by establishing which phones communicated with the telecommunication network, their location and the times of the events which occurred.

3.2 Evidence interpretation

An important aspect of forensic investigation is evidence interpretation. Even with physical evidence such as DNA the result of the evidence analysis process is statistical rather than deterministic in nature, and this is no less the case with evidence available from mobile phones. The problem of interpretation with mobile phone evidence arises because of the nature of the data available to the investigation. Data from the network operator may not be available; data on phone location based on signal strength available at the phone may vary depending on the weather and the environment; and the identity of the person using the phone at the time in question may be different from the subscriber or owner of the phone.

An important part of the evidence interpretation process is to form hypotheses of how the evidence could have come to exist on the phone, which may be different from the most obvious explanation. For example, the presence of a specific phone number in the LDN list on a suspect's phone may not be definite evidence of contact between the two phones, since the call may not have been connected, or it may have been dialled in error. However, if the suspect's phone number appears in the address book of the other phone, this is more suggestive (although not necessarily definitive evidence) of contact. In forensic evidence interpretation, the hypothesis that person X was involved in the criminal activity given the evidence E must be weighed against the hypothesis that X was not involved given this evidence. The ratio of these two quantities provides the likelihood ratio, which is a measure of the weight of the evidence E. [Evett 1998]

In general, evidence involving data extracted from mobile phones is built up of a number of facts, which like any criminal event are open to the interpretation of the judge and jury. The role of the forensic scientist is to assist the court in the process, and this may involve the formulation of possible alternative hypotheses.

3.3 Evidence extraction from mobile phone handsets

Mobile phones show a large variability in performance and functionality between devices, and between 'generations' of technology. A standard forensic procedure for evidence extraction from mobile phones to assist in criminal investigations is highly desirable, since it would enable evidence to be recovered rapidly and consistently. The standards to which GSM devices conform are helpful in the development of a standard procedure, as they enable tools for extraction of data from SIM cards and handsets to be implemented.

3.4 Validation of tools and techniques

When a tool is selected for evidence recovery and analysis, it must be validated to demonstrate that its application consistently gives accurate results. When an exhibit is examined, the first step is to identify the device involved. The preferred approach is then to obtain an example of the same type of device which can be compared to the exhibit, an example which can provide guidance on how to access relevant areas for data retrieval; and on device specific information such as the character set available to the phone.

In order to comply with the principles of evidence handling described above, a standard test data set is defined and loaded on to the example device. This data is then extracted using the recommended tools and standard operating procedures developed for the device, and the result compared with the original test data to determine any changes introduced by the procedure. The standard test data set should be comprehensive enough to test functionality of the device. The behaviour of fully loaded phones; phones from which data has been deleted; sparsely loaded phones; and the full character set for SMS text messages stored on both the SIM card and handset memory should be tested.

Data recovery from the SIM card and the handset memory of the device is tested, using recovery from the handset via a data cable; via the IR port; or by hand. The test data are loaded using tools normally available to the user, i.e. manually and also automatically via a data connection from a lap top computer. The behaviour of data which has been transmitted to the phone being examined from another phone was also tested.

3.5 Data extraction from the exhibit

It is necessary to extract as much data as possible without changing any data on the exhibit. A suitable comtrolled procedure has to be used in removing the data from an exhibit, since data can easily be added accidentally to the phone during this process. The procedure is performed by a trained forensic reporting officer. The safest procedure is to first extract data from the exhibit through its data port. Certain data must be removed from the device manually, for example such lists as 'missed calls'. Removal of the SIM card can alter data on the device, so this step is performed last.

The data are read through the data port for equipment that supports the AT command collection for mobile GSM equipment (ETSI standards GSM07.07 and GSM07.05). A log file is created which records all communication between the computer and the phone so that it can be satisfactorily demonstrated that no data has been written to the phone during the extraction process. Not all the data on the phone can be extracted using this method however, for full data extraction the SIM card must also be read.

The SIM card is read using a standard smart card reader. The card may be protected by a PIN (personal identification number). This number is stored in a dedicated area of the card, and is not easy to read or overwrite without authorisation; normally only 3 attempts to enter the PIN are allowed. Access to the PIN is protected under RIPA legislation, but in certain circumstances it can be over-ridden by the network operator who can supply the PUK (pin un-blocking key) to enable a new PIN to be set by the investigator. Because files can be read directly via the smart card operating system, it is possible to retrieve deleted information. In practice only deleted SMS messages can feasibly be recovered.

3.5 Evidence preservation

The evidence submitted for examination must be preserved from change. This preservation process consists of the following steps.

- ***Maintaining power supply***
  Electronic devices will lose data if the power supply is interrupted. This is less critical for mobile phones, because the devices are able to maintain their data for a significant period in the absence of external power. However, in a forensic unit for mobile phone investigation a range of power supply units and cables should be available, preserving the power supply like this minimises damage to the phones by inadvertently supplying the wrong power profile or connection.
- ***Unwanted electromagnetic contact***
  As mentioned in the previous section, mobile phones can be in contact with the GSM network even in an idle state. This contact destroys potentially useful evidential information such as SMS messages and missed calls. The phone must therefore be shielded for electromagnetic contact during examination.
- ***Security***
  If enabled the PIN number must be removed. Normally the owner of the phone is invited to unlock it during the investigation, but in certain circumstances the PIN can be overwritten by the network operator.
- ***Repair***
  It is not unusual to receive phones which have been damaged. Repair of an exhibit conflicts with the requirement to maintain the original state of the exhibit, so that repair of the device should not be undertaken unless the current state of the device makes data extraction impossible. The forensic unit must have the capability for repairing those modules of the phone which still contain data.

4.0 Future developments

Interpretation of mobile phone evidence is still developing. It is apparent that the large amount of data typically stored in a phone potentially represents very valuable information in criminal investigation. Evidence retrieved from phones already plays a critical part in investigation of crime, and as devices develop in complexity the digital traces of crime become more difficult to hide.

The development of the mobile phone towards a mobile desktop has already begun, such devices will be characterised by even greater amounts of memory. The personal character of these devices make them particularly interesting for forensic investigations, but all the more worthy of the privacy protection afforded by the law.

Bluetooth technology can potentially make the devices more personal and better targeted to individual preferences. It also leaves a clearer trail of digital evidence for use in investigation.

References

ACPO1999	*The Good Practice Guide For Computer Based Evidence,* Association of Chief Police Officers (UK), 1999
SWGDE1999	*Digital Evidence: Standards and Principles.* www.fbi.gov/hq/lab/fsc/backissu/april 2000/swgde.htm
Casey 2002	*The Handbook of computer Crime Investigation*, Casey ed., Academic Press, 2002
Evett 1998	Evett, I, *Toward a uniform framework for reporting opinions in forensic science casework*, Science & Justice, 1998. 38(3): : pp198 - 202

Printed and published by the IEE, Savoy Place, London WC2R 0BL, UK.