

## Mobile Telephones – the new fingerprints

Since the development of the [Global System for Mobile Communications](#) (GSM) standard in the early 1980's, the numbers of deployed mobile telephones have grown exponentially; with an estimated 2 billion handsets now in use throughout the world. There are now more mobile telephones in the UK than there are people – this pervasive technology impacts on almost all areas of industry and life. Unsurprisingly mobile communications have enabled old crime to be effected in new ways and evidence from such devices are increasingly forming an important part of criminal and civil proceedings.

Speaking at a recent lecture to the British Computer Society (BCS), Ross Patel, Director of Digital Evidence at AFENTIS Forensics, commented that “in almost every major fraud case or murder investigation, telephonic evidence proves crucial in placing the suspect in the locale at the time of the offence” [1]. Conspiracy charges are sometimes wholly based upon telephonic evidence, where linkages and contact between individuals is provided by an analysis of the digital evidence within the mobile phones and from the associated telecommunication network (e.g. T-mobile).

Modern communication devices of this form comprise of three distinct components: a finger-nail sized chip known as the 'Subscriber Identity Module' (SIM) that is responsible for service with the telecom network provider, the handset, which provides the user interface and memory capacity to store information, and removable memory modules that facilitate simple exchange of information and markedly improve the data storage capacities.

Many specialists argue that the mobile phone has become so valuable a tool to investigators that they have become known as “the new fingerprints”. A case in point being Ian Huntley's conviction for the Soham murders[2] which was based partly on crucial mobile phone evidence.

It is incumbent that advocates and legal specialists learn more about this sphere of forensics, ensuring that opportunities and avenues of recourse that would benefit their client are fully explored and exploited.

This article explores the digital evidence that can be found within a mobile telephone handset; follow-up features will examine the value of examining SIM cards and how Cell Site Analyses (mapping the geographic position of a handset).

### Digital Evidence

Mobile phones employ what is known as 'flash memory'[3] to store data and settings. Unlike the 'Random Access Memory' (RAM), which is found within computers, flash memory can continue to store information even in the absence of a power source. This resilient feature of mobile telephone memory means that devices that have been buried or even left damaged for considerable periods of time can still yield valuable evidence through careful forensic examination.

As mobile communication devices continue to evolve[4], with features like word processing and photo imaging applications becoming commonplace, the memory storage areas have become increasingly important silos of digital evidence.

The following materials can be recovered from the handset and can greatly assist in case preparations:

- Logged Incoming & Last Dialed numbers
- Text & Multimedia messages
- System Settings (including date/time/volume)
- Stored audio/visual materials
- Saved computer and data files
- Calendar and Alarm notifications
- Internet settings and websites accessed

## Common Questions

*Where does evidence reside - on the handset or on the SIM?*

Materials of evidentiary value are stored on both the SIM[5] and within the handset memory. Therefore it is recommended that comprehensive evaluations of both are undertaken. The SIM will tend to contain valuable user-specific information such as network identity, whilst the handset will contain large amounts of information relating to calls made/received, texts sent/received, images/video clips created etc. Most handsets now also feature the ability to connect to computers to expand functionality and allow data/media exchange – which should also be considered in the interests of a thorough and comprehensive investigation.

*Can indecent images such as child abuse material be stored on a handset?*

The prevalence of high resolution cameras integrated with most mobile telephones has led to an increase in the number of offences being committed in relation to creation, or attempted creation, of indecent/obscene images. Assuming a standard handset with 32MB of memory, close to 500 still images could be taken and stored. Through the use of removable memory devices, such as SD Cards, these media archives can be easily shared to other telephones or even with computers. In Italy the Data Protection Commissioner has issued stringent guidelines on the use of camera phones in public places – especially in places such as swimming baths.

### Did you know?

New mobile telephones have as much as 32 megabytes of internal memory - enough to comfortably store a document with over 2,000 pages of text!

Telephone handsets will typically store user defined words that are not in a normal dictionary. Names of individuals and places are often stored in this archive - a potentially valuable source of intelligence for investigators or legal support teams.

*Text messages and phonebook entries deleted six months ago - can they be recovered?*

Dependent upon a number of factors, such as how frequently the memory segments that store information are over-written with fresh data, it is possible to retrieve even the oldest materials committed to the phone - including text messages received by the user but never saved. In most cases a surprising amount of information can be retrieved, often going back several years.

*Does locking the handset keep information private and inaccessible?*

Personal Identification Numbers (PINs) and pass codes can be used to restrict access to the handset, but forensic assessments typically bypass such controls by interrogating the memory module directly[6]. At this time encrypted file-systems and data storage areas are not available in standard retail handsets.

*What else can the handset tell us?*

Aside from digital evidence the presence of DNA traces on the keypad, earpiece and mouthpiece can tie a user to device. Similarly, 'Call Detail Records' (CDRs)[7] can be retrieved from the network provider (e.g. O2 or T-Mobile), providing near post-code location information as to where and when the device was used for messaging or even picking up voicemail. This type of information can be retained by network providers for several years, allowing for even reconstruction and long after the incident.

*How do you identify the International Mobile Equipment Identity?*

The IMEI is a 15 digit Code used to identify the phone to the network. Whilst this code can often be found etched into the handset beneath the battery, it is also possible to identify the IMEI without the use of forensic technology. By entering \*#06# on the keypad the telephone screen should display the device IMEI. Caution: this approach to identifying the IMEI may affect valuable evidence in storage.

---

Mobile telephone devices and related portable communication exhibits are playing an increasingly important role in today's courtroom. Almost all murder, complex fraud and cases involving conspiracies, will have some degree of electronic evidence tendered. In extreme cases the proceedings will rise or fall based solely upon the digital evidence exhibits. According to Mike Rainford, Head of Fraud and Business Crime at Burton Copeland, "appreciating what is forensically possible and the type of evidence that can be recovered through careful examination is crucial to ensuring that opportunities and avenues of recourse that would benefit case preparations are fully explored and exploited".

## ABOUT THE AUTHOR

Ross Patel (BSc)Hons, MCSE, CCNA, CISSP, CISA, CISM, CHFI, CEH, is Director Digital Evidence at AFENTIS Forensics – an independent firm specialising in the provision of Technical Expert Witness services to the investigative and legal community.

**AFENTIS FORENSICS**[www.afentis.com](http://www.afentis.com)

FREEPHONE 0800 180 4545  
24x7 Confidential Enquiry Hotline

Computer Analysis / Mobile Telephone Forensics / Data Recovery CCTV  
Drives / Covert Surveillance / Obscene Images & Media  
Investigations Training / Expert Witness

1. Evolution of Malicious Code, British Computer Society (Feb '07)  
Ref: [www.bcs.org.uk](http://www.bcs.org.uk)
2. Soham Trial - BBC Report.  
Ref: [http://news.bbc.co.uk/1/hi/in\\_depth/uk/2003/soham\\_trial/](http://news.bbc.co.uk/1/hi/in_depth/uk/2003/soham_trial/)
3. RAM, ROM and Flash Memory.  
Ref: <http://www.storagesearch.com/flash.html>
4. Evolution of Mobile Telephones.  
Ref: [http://en.wikipedia.org/wiki/History\\_of\\_mobile\\_phones](http://en.wikipedia.org/wiki/History_of_mobile_phones)
5. SIM Card Forensics, 5 Minute Forensics Series, CrimeLine 2006  
Note: There are provisions in Part III of the Regulation of Investigatory Power Act 2000 that empower authorities to force disclosure of passwords and encryption keys by making refusal (even through loss of memory or inability) an offence.
6. CDRs provide overview information in terms of when and roughly where the device was used. Text messages, phone calls and the actual traffic between individuals is not recorded.
7. A list of manufacturer codes that can be used to display network and special system information is available online at [www.afentis.com/mobile/netcode](http://www.afentis.com/mobile/netcode)