

## Mobile Telephone Handsets

### The Essentials

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.

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 capacity of the phone.

Many specialists argue that the mobile phone has become the new fingerprint – a case in point being Ian Huntley's conviction for the Soham murders<sup>1</sup> 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.

### Digital Evidence

Mobile phones employ what is known as 'flash memory'<sup>2</sup> 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.

As mobile communication devices continue to evolve<sup>3</sup>, 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<sup>4</sup> and within the handset memory. Therefore it is recommended that comprehensive evaluations of both are

---

<sup>1</sup> 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/)

<sup>2</sup> RAM, ROM and Flash Memory. Reference: <http://www.storagesearch.com/flash.html>

<sup>3</sup> Evolution of Mobile Telephones. Reference: [http://en.wikipedia.org/wiki/History\\_of\\_mobile\\_phones](http://en.wikipedia.org/wiki/History_of_mobile_phones)

<sup>4</sup> SIM Card Forensics, 5 Minute Forensics Series, CrimeLine 2006

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.

*Can obscene images/material be stored on a handset?*

The prevalence of high resolution cameras on most mobile telephones has led to an increase in the number of offences being committed in relation to creation, or attempted creation, of obscene images. Assuming a standard handset with 32MB of memory, close to 500 still images could be taken and stored.

*Data deleted six months ago – can it be recovered?*

Dependent upon a number of factors, such as whether the information has since been over-written, it is possible to retrieve even the oldest materials committed to the phone – including material that were never saved by the user. In most cases a surprising amount of information can be retrieved, often going back several years.

*Does locking the handset keep information private?*

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<sup>5</sup>. 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 Data Records' (CDRs)<sup>6</sup> can be retrieved from the network provider, providing near post-code location information as to where and when the device was used.

*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 be retrieved during a forensic examination, a quick way to force the handset to display onscreen the code is to enter \*#06# on the keypad<sup>7</sup>. Caution: this approach to identifying the IMEI may affect valuable evidence in storage.

## 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 therefore often stored in this archive – a potentially valuable source of intelligence for investigators.

## Find out more...

- [Digital Evidence from Mobile Devices](#) – MS PowerPoint presentation
- [GSM Security Algorithms](#) – GSM World
- [Understanding Cellular Telephone Security](#) – Simson 2003
- [Central Equipment Identity Register](#) (CEIR)

---

<sup>5</sup> Note: There are provisions in the *Regulation of Investigatory Power Act 2000* that empower authorities to force disclosure of passwords and encryption keys.

<sup>6</sup> 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.

<sup>7</sup> 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)