Many criminal cases can be greatly assisted by mobile telephone evidence. Our casework includes all kinds of crime, from minor harassment to high-profile, complex murder cases.

Mobile handset examination

A mobile handset can contain a wealth of unseen evidence. Large amounts of data are captured in its memory, to provide useful evidence to corroborate statements and to track the behaviour, lifestyle and interactions of suspects, victims and witnesses.

Today's mobile handsets are powerful, multi-functional devices for taking pictures, browsing the web, texting, diary management and voice recording, as well as making phone calls. All this information, including deleted items, can be forensically investigated for evidence.

A typical Sony Ericsson device, for example, can potentially store sent, received, forwarded, delivered and saved dates for text messages. Some data on a handset that eludes forensic software can still be recovered by manually interrogating it.

When LGC Forensics examines a handset, we use a combination of software, intellect and experience to extract and analyse any digital data recorded on it, taking comprehensive notes – our version of the policeman's notebook – to detail every step of the examination process and act as an aide memoir when we present our evidence in court.

Mobile phone examinations yield a wide variety of information including call logs, contacts, messages, video and photographic evidence, sound recordings and handset/SIM identification data. Our investigators have retrieved and analysed stored data in several different languages and even recovered information from damaged devices.

Examinations are carried out by experts and data is presented in full colour, graphical reports, with any recovered media recorded on CDROM or DVDROM. We will prepare a witness statement and, if required, personally present this in court.

Our procedures follow the ACPO (Association of Chief Police Officers) guidelines and PACE (Police and Criminal Evidence Act) codes of practice to ensure the integrity and continuity of exhibits and the overall accuracy and quality of the evidence that we report and present. High standards have earned UKAS accreditation for our laboratory.

Evidence to track every move

The telephone team is part of our digital and document forensics department and serves a broad client base. Our main customers are UK police forces, the Department for Work and Pensions and private defence solicitors. We work impartially to assist the Crown Prosecution Service and produce a full evidential package, appearing in court when required.

The team is UKAS 17025 accredited and proficient in examining a wide variety of digital devices and media. As well as mobile phones, SIM cards and memory cards, we have experience of examining satellite navigation tools, fax machines, pagers, dictation machines, PDAs, MP3 devices and USB data drives.

Many criminal cases and other investigations can be greatly assisted by mobile telephone evidence. Our casework includes all kinds of crime, from minor harassment to high-profile, complex murder cases.

Today, every facet of our lives can be digitally documented. Social networking sites such as Facebook, Bebo, Twitter and Flickr can be accessed and edited from modern handsets, leaving a trail of digital evidence which is recoverable using forensic software.

For forensic analysis, three components are relevant: the SIM (Subscriber Identity Module) card memory, handset memory and a removable memory card. Each is examined separately using a variety of forensic techniques.

LGC Forensics

What can we learn from a handset?

Many types of digital data can be recovered from a SIM card, handset or memory card, including:

- Phonebook and contacts list
- Call logs
- Text, multimedia and email messages, including push text messages
- Picture, video and audio files
- Organiser information, such as calendar, notes and tasks lists
- Geo tagging photo information
- GPS data
- Symbian-handsets cell ID's
- Documents downloaded from the internet or transferred from another device
- Internet and web browsing history, including bookmarks
- Bluetooth details, including devices paired by and information received from Bluetooth connections
- Deleted data – deleted information can sometimes be recovered from digital storage, such as SIM cards.

The secrets of the SIM

We use a range of tools to examine SIM cards. These tools are used to forensically recover live and deleted data from SIM cards, presented in a clear and formatted report.

If a SIM card is PIN locked, we will ask you to ask the network provider to supply the PUK (Personal Unblocking Key).

The data we can recover includes:

- The phone number of the SIM card (known as the MSISDN – Mobile Station Integrated Services Digital Network)
- Contacts/phonebook entries: a list of all contacts stored on the SIM card, often stored in the order in which they were entered onto the memory
- Text messages, and deleted text messages that can be recovered if they have not been overwritten
- The SIM stores messages in a consecutive order, and once deleted by the user of the handset these messages remain on the SIM card until further messages arrive and are saved over the deleted message
- The SIM card also stores out-going and in-coming information
- The last ten dialled calls, stored in most cases without a date/time but this data can occasionally be obtained and is produced in the forensic examination report if it is there
- Email addresses (3 Network)
- Information acquired from a SIM card examination can help identify the make and model of the last few handsets the SIM card may have been used in
- Network information – compatible and forbidden mobile networks which the SIM card may or may not be able to use when roaming, i.e. when the user is abroad and wishes to connect to the networks in use in a particular country.

A memory card can record vital documentary evidence

Memory cards may contain a vast amount of data. Any kind of file may be stored on a memory card, from standard photographs taken by the handset camera to Microsoft Excel© spreadsheets containing detailed financial information, and more.

The memory card is removed before the handset is activated to prevent any further data being written to it when the handset is investigated. Using the forensic application EnCase, we take a complete image of the card and verify it using an MD5 hash, a mathematical equation that highlights any difference between the created image of the card and the data stored on the card itself.

The card is searched for all relevant data types, which are logged in the analyst's notes and can be made available in court at any time.

Exploring the mobile landscape

With so many products able to store electronic data in so many ways, it is becoming harder for investigators to access, retrieve and make sense of information buried in and spread across a multitude of devices.

The distinction between mobile phones, smart phones, PDAs and even computers is becoming blurred. As new devices have emerged, our team must constantly evolve new ways of recovering forensic data from them.

Our investigators are able to analyse a wide variety of devices from leading manufacturers such as Nokia, Sony Ericsson, LG, Motorola, Samsung, Siemens, Sharp, NEC, Alcatel, Windows Pocket PC, Palm, Blackberry, Apple iPhone and HTC. When combined with cell site analysis, these devices can tell us a great deal about a person's day-to-day movements and interactions.

All things forensic

Mobile handset examination is one of a number of key services provided by the digital and document forensics team, and complements and integrates seamlessly with other LGC Forensics services. We offer the fullest range of high-quality, forensic services, providing powerful assistance and expert evidence to support crime investigations, and civil or private disputes.

Highly qualified experts are available to discuss your specific casework problems and advise potential, integrated solutions to provide the greatest certainty of a satisfactory outcome.

For further information in confidence, please contact:
LGC Forensics Tel: +44 (0)844 264 1999 • Email: d&df@lgcforensics.com
Web: www.digital.lgcforensics.com

LGC Forensics

2396/OR/0210