Burnt to memory

Dr Benjamin Jones, Research Co-ordinator at the Experimental Techniques Centre, Brunel University, turns the spotlight on to data extraction from damaged mobile phones…

Mobile phones are essential tools for work and leisure in modern society. This ubiquity of use in the general public can be an asset in crime scene investigations, as many criminals and victims of crime will be carrying mobile phones, each with a unique Subscriber Identity Module (SIM) card. Many phones turn up at crime scenes and accident sites. Whether a phone is found with a body, or has been used to detonate a bomb, forensic analysis may be able to help identify victims or perpetrators, last active location, or calls made and received – which could provide vital assistance to investigators of these incidents.

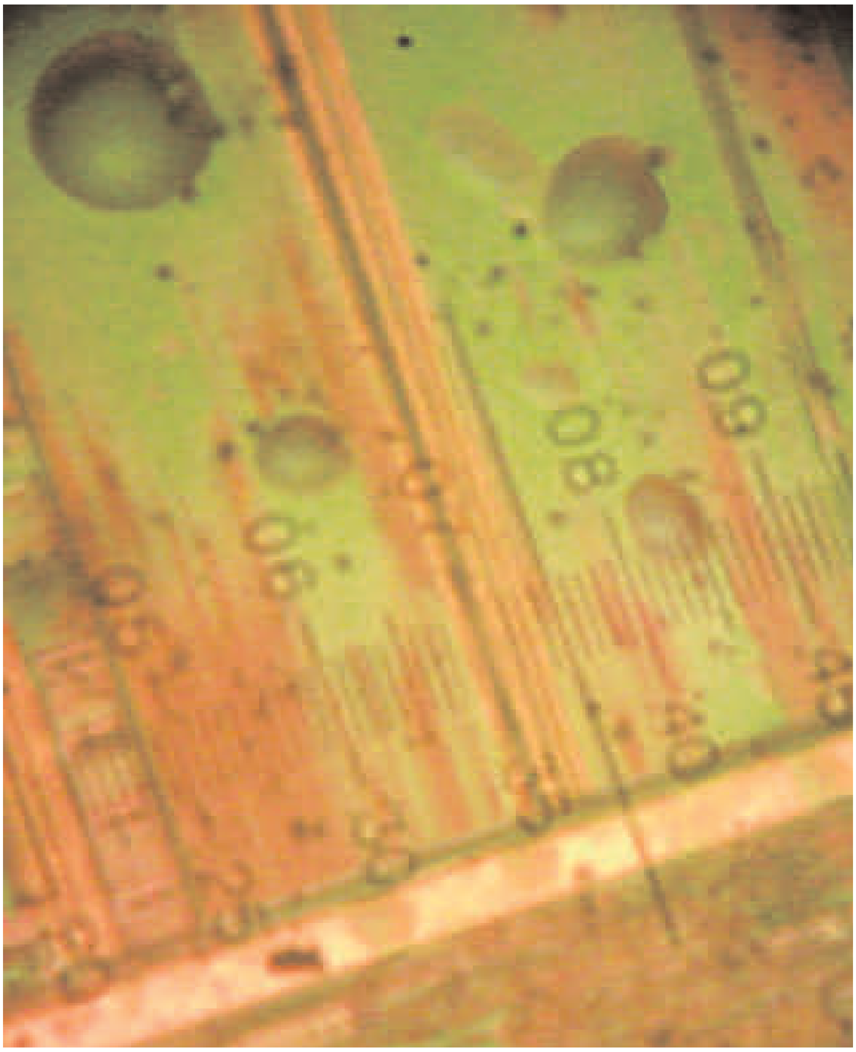
Unfortunately, in some cases such as road traffic accidents, bomb sites and building fires, mobile phones may be significantly damaged, either mechanically or by high temperatures. In many cases data from damaged phones can not be read in the usual manner; however, the actual data may be retained in even highly damaged phones, but is inaccessible by conventional techniques.

EPSRC funded researchers at ETCbrunel and UCL Electronic Engineering, in association with The Forensic Science Service, have been working to determine the level of retained data within a heat damaged SIM card or smart card, and to develop novel data extraction methods to glean information from burnt or damaged SIM cards for use in forensic investigations.

SIM card recovered from fire

In this respect, the most valuable part of a SIM card is the non-volatile re-writable memory, usually in the form of flash memory. This is part of the chip that is integrated into the familiar SIM card package and allows easy reading of the data via electrical contact to the interface. In some instances where the SIM card package has been damaged, electrical contacts can be made on the surface of the chip itself. However, this practice is becoming more difficult for a number of reasons, including the need for specific hardware access control circuits for each different type of chip, and, in particular, because of the high likelihood of the chip being damaged during criminal activities, by fire, or during extraction.

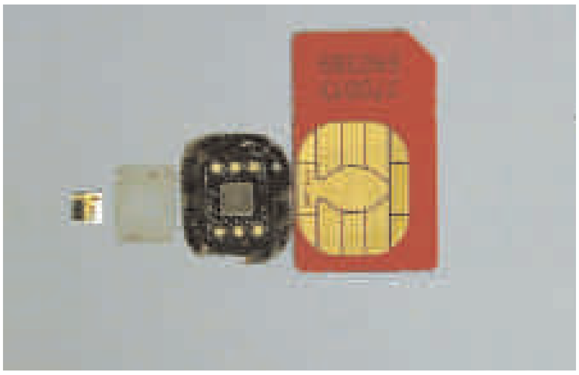
In a typical memory device, data are held in individual bit cells, in the form of charge stored on a floating gate, electrically isolated top and bottom by a very thin oxide layer. Each memory bit (making up 1/8th of a byte) is either a 0 or 1 and consists of the presence or absence of charge that is introduced or removed from the floating gate by applying a voltage to various control points – writing or erasing the data. Once in the floating gate, charge is held there due to the surrounding oxide. Modern flash memories are capable of holding charge for several decades. Each bit cell is less than a thousandth of a millimetre in size,



Magnified optical image of moderate heat-induced damage to surface of SIM card chip

and thousands of these are connected via multiple layers of micro-circuitry to the microprocessor unit, interface and the outside world.

Damage by heat or fracture may have broken some of these connections, or damaged the upper circuitry, thus causing a SIM card to become unreadable via the interface or through direct probing of electrical contacts. However, the stored data – charge retained in the floating gate – will not necessarily have been compromised; only the conventional access route is removed.



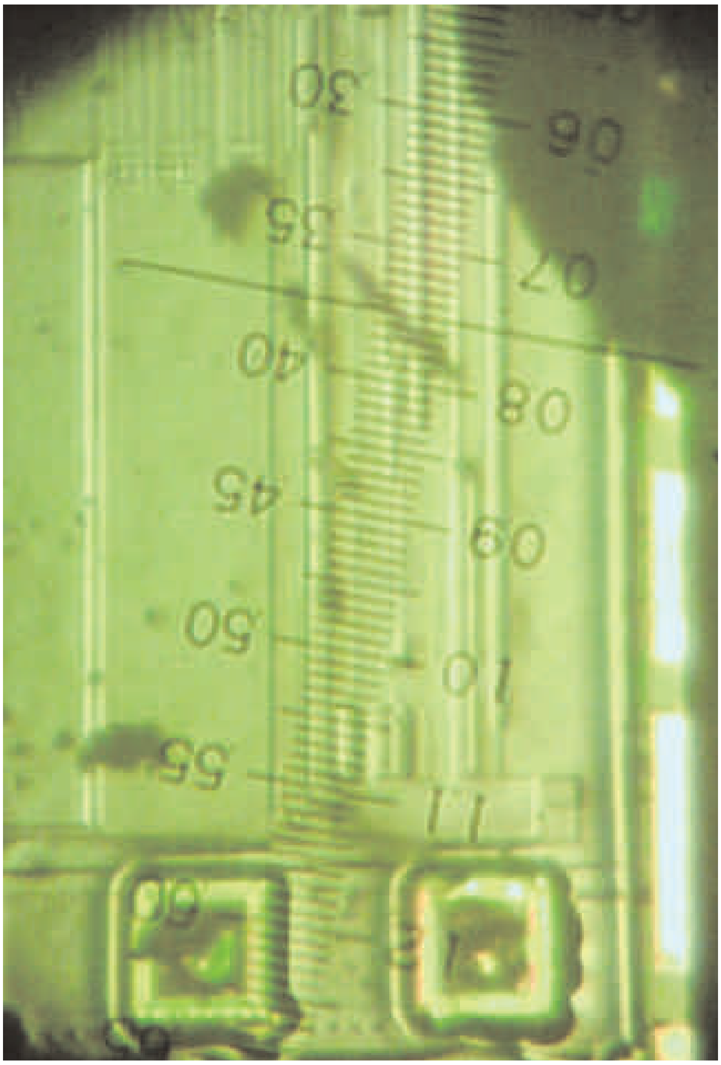
Sections salvaged from SIM card suffering minor heat damage, including, far left, the microchip; with undamaged SIM card for comparison

Samples of SIM cards representing a range of manufacturers, networks and ages were collected from networks, distributors and members of the public in Ireland, Sweden and the UK. Researchers processed the SIM cards and created a deliberately artificial experimental arrangement, an idealised situation where mechanical damage to the chip is minimised.

SIM card chips were heated in idealised conditions to a range of temperatures up to 650°C, then reassembled and connected to an interface for reading via conventional means. At the highest temperatures, the heating caused damage that rendered reading by reconnection impossible. However, all mechanically undamaged chips heated to temperatures of around 180°C could be read with this method, and uncorrupted data was also obtained from a device heated to approximately 450°C.

These experimental results are supported by data published by manufacturers. Most memory device manufacturers provide nominal data retention times for operation at room temperature. In some cases, this can be extrapolated to operation times at different temperatures, using a variety of models. Information for one memory type suggests data can be retained at 450°C for approximately an hour, while at 700°C this has reduced to a few minutes.

The relevance of these temperatures can be seen from experiments conducted by researchers in the National Institute of Standards and Technology in America. In their experiment on a full-scale house fire, fuelled by household furniture and accelerated with petrol and oil, the temperature experienced varies with location within the house, and increases significantly with height. Although the maximum temperature reached was 738°C, this is only obtained briefly, close to the ceiling. The maximum temperature in the floor area is 166°C and temperatures here are in fact only maintained above 100°C for 90 seconds, indicating that phones in these locations will not suffer data loss due to heating effects. At approximately desk height, the temperature is sustained at an average of 450°C; data retention will only become an issue for phones that experience this temperature for an hour or longer.



It is worth noting that these temperatures are maximums and the house fire temperature is considerably reduced away from the source of ignition and highly combustible furnishings. The temperatures reached in an adjacent room comfortably allow sustained data retention.

From these experiments we can see that data are likely to be retained in phones that experience temperatures similar to those of a house fire. However, for many SIM cards heated outside idealised laboratory conditions, access to the data through conventional electrical contacts is impossible due to the additional damage caused to the chip.

A key question is the feasibility of reading this data from chips that have been exposed to elevated temperatures or have suffered mechanical damage. A range of techniques exists to access protected data or programs in embedded microprocessors during program execution – what might commonly be called hacking. Such techniques can be non-invasive: side channel attacks monitor unintended outcomes of processor operation. For example, it is possible to measure charge movement within processors using magnetic probes. Highly invasive techniques can also be used, such as deliberately introducing a fault in the chip and observing the response. Fraud countermeasures, advanced cryptography and physical protection systems are put in place by manufacturers to curtail the effectiveness of such attacks.

Many of these techniques are unsuitable for reading memory from burnt phones as they require either an operating chip, knowledge of the specific electronic architecture, or they may result in degradation or erasure of the stored memory.

An alternative is to use a highly controllable, ultra-fine, electrically sensitive probe to directly read the charge in individual floating gates, each corresponding to one bit. This has the advantages of not requiring the upper circuitry to remain intact, and is operable even if only fragments of the chip are available. This may, therefore, be a useful technique to detect the data that is retained even in damaged chips. However, there are considerable drawbacks in such techniques, including the very slow read speed, the delicate and lengthy preparation process which may destroy cells or compromise the integrity of any data retained – and, lastly, the descrambling of the binary contents of the memory array into meaningful data.

In summary, data is retained in SIM card devices that are subjected to temperatures which exceed those likely to be experienced in house fires. In some cases the data is retrievable by rebuilding severed connections; however, in the majority of instances, chips will suffer additional damage to the top surface or circuitry, or experience some mechanical damage. In these cases, although the data is retained in the memory, it cannot be read by conventional methods, and an alternative technique, such as direct probing of the stored charge, needs to be employed to access the retained data. Investigations into the development of data reading techniques are continuing, as part of ETCbrunel's broader interest in forensics, which extends into fingerprinting, ballistics and failure analysis.

Dr Benjamin Jones
Research Co-ordinator

Experimental Techniques Centre
Brunel University
Uxbridge
Middlesex UB8 3PH

b.j.jones@physics.org
www.ETCbrunel.co.uk