

Data Recovery from Smart Cards for Forensic Applications

B.J. Jones¹ and A.J. Kenyon²

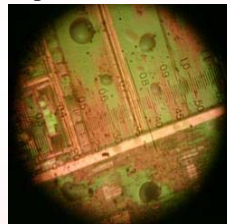
1. ETCbrunel, Brunel University, Uxbridge 2. UCL Electronic Engineering, London

Mobile Phones & Crime

Mobile phones have been used recently in a number of bomb attacks, either as detonators or for communication. Data may be retained in even highly damaged phones and an ability to read this data could help identify the owner, last active location or call records, which could provide vital assistance to incident investigators. In addition, many victims of crime will be carrying mobile phones, each with a unique Subscriber Identity Module (SIM) card. Reading data from damaged SIM cards can therefore assist in the identification of victims of events such as car accidents and building fires, as well as terrorist incidents.



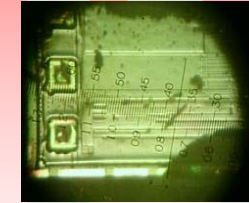
Top: Mobile phone detonator from Madrid bombings. **Below:** SIM card subjected to 450°C, average desk height temperature in a house fire.



Memory Access

There are a number of available routes to accessing memory chips, both non-invasive and highly invasive techniques, such as side channel attacks and fault induction. There are significant drawbacks, however:

- Intact and operational chip not available
- Little knowledge of chip architecture
- Damage means that making electrical contacts is impracticable
- Cryptographic and physical countermeasures in place to protect memory from unauthorised access



Fire!

The optical micrograph shows damage to a SIM card from exposure to a temperature of ~650°C.

This is below the maximum temperature in a house fire, and shows that the electrical contact pads have been destroyed, the chip surface melted and part-covered in burnt residue, and sections of the chip are missing. However, the charge, and thus the data, may still be intact. This is a good example of the type of device from which data is to be read, following development of methods outlined.



Forensic Investigations

During forensic investigations, the most valuable part of a system such as a smartcard or a mobile phone SIM card is the memory: in particular the non-volatile re-writable memory, usually an erasable electrically programmable read-only memory (EEPROM). Conventionally, data from the EEPROM are read using an interface provided for the purpose or, in cases where the chip package has been damaged, by making electrical contacts on the surface of the chip itself. However, this practice is becoming more difficult because of the high likelihood of the chip being extensively damaged during criminal activities.



"I can guarantee no one can read it now..."

New Techniques

We have identified a possible method based on a variant of scanning probe microscopy (SPM), for direct reading of data from SIM cards that have been mechanically damaged or subjected to extreme temperatures. This technique has been shown to successfully operate on a small section of a memory chip and requires little prior knowledge of chip-architecture. The measurement has a resolution that exceeds current requirements and does not destroy, damage or corrupt either the data or the sample structure. The method also has an in-built quality assurance mechanism. This technique and associated preparation methods are being jointly developed by ETCbrunel and UCL Electronic Engineering, in collaboration with The Forensic Science Service®.

Acknowledgements:



Christophe De Nardi, CNRS
Andy Beard, Birkbeck
Lucy Ataby, Virgin Mobile