- Overview -

- Techniques -

- Worked Examples -

Introduction

The ubiquity of mobile phone use in the general public can be an asset in crime scene investigations. Many criminals and victims of crime will be carrying mobile phones, each with a unique Subscriber Identity Module (SIM) card. However, in some cases such as road traffic accidents and building fires, mobile phones may be significantly damaged. The criminal fraternity is becoming wise to the significance of data held within the SIM card and will often attempt to damage or destroy a SIM rather than let it fall into the hands of an investigator. In addition, mobile phones have been used recently in a number of terrorist bomb attacks, both as detonators and for communication.

Data may be retained in even highly damaged phones and an ability to read this data could help identify the owner, place of purchase, last active location, or calls made and received, which could provide vital assistance to investigators of these incidents. Reading data from the memory of damaged SIM cards, and similar devices such as credit cards and some types of ID cards, will therefore assist in the identification of both victims of incidents and perpetrators of crimes. Similar techniques can be employed to connect to devices recovered from within mobile phones, memory cards USB memory sticks and other such products that may hold personal or incriminating data.

During forensic investigations, the most valuable data is likely to be the user related data such as Abbreviated Dial Number memory and Short Message memory. There are a number of forensically sound techniques extract and examine this information – notably SIMIS (SIM Interrogation System) In cases where the chip package has been damaged, and making contact via the smart card interface un viable, alternative methods need to be utilized to make contact to the surface of the chip itself and by pass the damaged electrical circuits.

Other barriers exist to prevent recovery of data such as the likelihood of the chip being “locked” by a personal identification number (PIN) or the silicon chip being physically damaged to the point that it is in operable.

However, damage by heat, corrosion, bending, breaking etc may cause a SIM card or similar device to become unreadable via the standard interface but with the correct techniques or through direct probing of the silicon surface valuable data can still be recovered where the damage has not compromised the stored data.

Damage to SIM cards can occur by mechanical means or when the cards are heated (such as in house fire or explosion) and further damage can be caused by the processing of the device prior to probing for data, such as the removal of epoxy and other packaging materials. Decapsulation of SIM card chip, via any

method, can cause mechanical damage to the chip, or reveal or exacerbate existing damage. Even a low level of damage can render the chip unreadable via connection to a SIM card reader or simple probe station. It is therefore important that tried and tested techniques are used on evidential material or where intelligence is being gathered, however it is equally important to continue to improve techniques and processes to improve reliability and remove unsound practices.
When faced with a particularly difficult job, an important point to note is that, although desirable, it is not always necessary to read ALL of the data held on a SIM card. In many cases, only a very small fraction of the data is necessary – for example, the IMSI can yield valuable information linking the card and phone to a specific person and a particular location. With a co-operative mobile system provider, even an ICCID from a badly burned SIM could be used to tie the SIM to a person or mobile. Extracting nothing more than the ICCID could lead to success.

Forensic SIM Card Data Recovery

Subscriber **I**dentity **M**odule **I**nterrogation **S**ystem **"SIMIS"** is a system that facilitates the retrieval of information from SIM and USIM cards used in the mobile communications industry. SIMIS has been developed under the guidance of leading UK forensic and police technical support units. SIMIS supports best practices in the preservation, recovery, analysis and court-ready reporting of SIM and USIM digital evidence. SIMIS adheres to the technical specifications laid down in the ETSI document GSM11.11 and other supporting documents from 3GPP and British standards. These documents identify the interface between the Subscriber Identity Module (SIM) and the Mobile Equipment(ME). SIMIS uses these defined standards to correctly recover raw data from the SIM and USIM and correctly interpret the data presenting it in both raw and human readable form for presentation in the evidential bundle.

A prerequisite for the use of SIMIS, is that the SIM or USIM card must be functional. A physically damaged, broken or dirty SIM may not function correctly, resulting in the recovery of corrupted data, or no data at all. In the forensic data recovery environment, SIM and USIM's will be presented in a variety of different conditions, ranging from good, but lightly soiled, through blood soaked to physically broken. Lightly soiled and blood soaked SIM's may be cleaned using appropriate methods, ensuring that the SIM is not further damaged taking care to preserve surface printing where possible. However, physically damaged or broken SIM's require more specialised processing to produce a viable SIM for data recovery purposes.

De-contamination

Before any device is handled certain precautions should be taken to avoid loss of biological evidence and or contamination of the investigating personnel with any hazardous material that may be present on the SIM / USIM to be examined. Through out the examination Heath and Safety is of paramount importance. The following section, therefore, discusses the nature of biological agents and the measures you should use to decontaminate the SIM / USIM before further processing to recover data.

The chief objective of biological agents is mass infection that results in the incapacitation or death of large numbers of individuals. In the case of the SIM or USIM the examiner is most likely to face blood bourn or body fluid contamination, however with the increasing use of mobile technology in terrorist activity, enquiries should be made as to the likely hood of other biological agents being present on the card.

In case of a biological contamination there are certain instructions that should be carried out for decontamination of the device contaminated by biological agents. Good hygienic practices are the best defence against many aspects of biological warfare.

De-contamination Methods

Protective clothing should be worn as a matter of course, the breathing of contaminated dust or debris should be prevented with appropriate dust excluding masks, disposable over garments and suitable gloves should be worn at all times.
The device may be washed and gently cleansed in calcium hypochlorite (bleach) solution for general biological decontamination. For Hepatitus or HIV contamination or blood urine and body fluid decontamination a wash in 10% Virkon solution should be used before attempting any cleaning. If specific biological or warfare contamination is suspected, best practice methods should apply.
The silicon chip in the SIM / USIM is normally protected by an epoxy encapsulant, the silicon chip will not be affected by normal biological decontamination processes. Even exposed silicon will not be affected in the short term by exposure to biological cleaning agents if used as a precautionary wash. Decontamination is unlikely to do any harm and will not erase data!
Generally all plastics will age under the influence of light, heat and oxygen. Virtually every plastic material is affected by reactions with oxygen. Oxidation breaks the long chains of the plastic molecules which causes a loss in plastic qualities, because these molecules are responsible for the plastic's properties.

It is important to remember that most bleaches are oxidising agents and in strong concentration will damage the SIM module carrier and printing. Be sure to use solutions of oxidising bleaches between 1-5%.

If the SIM has been manufactured to the full GSM specification, it will be carried in ABS, though many SIM modules are carried in cheaper PVC card bodies., it is unusual to find other materials used, though PET has been tried for some very low cost products.

Reformation of deformed SIM

If the SIM is deformed , bent, twisted etc it may be possible to reform the package without exerting excessive force. Reforming of the SIM module is desirable because it will allow the ICCID and any other marking to be easily read and photographed, the SIM can be accessed and data extracted using the "Bed of Nails" card interface and the SIM will be easier to work with if front or rear probing has to be employed. Our reforming technique relies on the so-called memory effect of plastics - plastic wants to return to its original shape. All thermo plastics exhibit some degree of memory effect and the SIM card body is particularly "memorable", thus severely deformed parts can be returned ,close to, their original shape and dimensions by exploiting this property.

Visual Inspection

An initial visual inspection of the device should be undertaken. It is important to record all aspects of the examination, a standard record sheet should be drawn up to allow the recording of information and the taking of notes.
Attention should be paid to:

i) general condition of the device
ii) photograph of the front, rear and from an angle that best shows any damage or interesting features. Pay special attention to any cracks in the card body or evidence of flexing. *See examples*
iii) note the number printed on the sim module this will be the ICCID. It may be abbreviated to show only the last few significant digits.
iv) Note the pattern of the contacts, this information should be entered in your data base to help identify SIM's of unknown origin.

If the SIM has been damaged by mechanical stress, bending or tearing, a microscopic inspection should be carried out with a polarised light source. Viewing into cracks and tears will allow an assessment of the level of damage to bond wires and may even reveal cracked or damaged Silicon.

If bond wires can bee seen to be broken, this gives a good basis on which to base further investigation. It is sometimes possible to probe through cracks or tears to attach directly to the exposed bond wire and thus connect to the internal silicon without excessive work on the SIM packaging or stripping down the protective layers.

Remember: The less we work on the SIM module the better !

> Decapsulation of SIM card chip, via any method, can cause mechanical damage to the chip, or exacerbate existing damage. Even a low level of damage can render the chip unreadable via connection to a SIM card reader or simple probe station.

Electrical inspection

Electrical inspection should be carried to determine if the device is electrically functional. This will help determine if the device can be accessed without stripping the packaging and protective layers. The visual inspection database should be extended to include observed electrical properties of the SIM. By building a database of the properties observed we can more easily decide if the damaged SIM harbours broken bond wires, without employing further resources such as X-Ray Inspection. Electrical tests should be performed to determine both forward and reverse impedance across all combinations of the active contacts.

The electrical inspection database will be useful when probing the silicon device, it is an important resource that will pay dividends in the long run.

Data Extraction

Data extraction requires reliable low impedance connection to the silicon dia. This is best achieved by connection to the smart card contact in a traditional smart card reader. Where the sim module is deformed or damaged, traditional methods cannot be used. Alternatives may be employed with varying levels of complexity.

- **Bed of nails:** Where the SIM module is deformed but electrically sound, the bed of nails may be employed to effect a good electrical connection to the original contacts surfaces even though they may be uneven or out of alignment.
- **Front face external probe:** Where the sim module is damaged by corrosion, for example, when recovered from a decomposed body, or buried in soil, the sim module maybe physically intact, except for severely corroded and unusable contact faces. In this case removal of

the contacts and probe of the underlying micro vias is the preferred approach.

- **External Wire Bond Probe:** Where the SIM module is cracked or torn and electrical connection is possible on some or most contacts, visual inspection may show the internal wire bonds to be exposed along the crack or tear. In this case it is preferable to utilise the bed of nails to connect to the viable electrical contacts and micro probe into the crack or tear to attach to the broken bond wires. A proprietary solvent blend may be used to excavate some of the encapsulant material to provide better access. This approach requires minimal work on the SIM module and therefore enhances the likely hood of reliable data recovery.
- **Back Side Wire Bond Probe:** Where the sim module is damaged such that several wire bonds are broken, good results may be achieved by removing the module from its plastic carrier and excavating the encapsulant surrounding the bond wire. This technique does not require complete de-capsulation of the silicon die but does give access to allow probes to be attached to the die vie the residual wire bonds. Once again this technique minimises the work on the SIM .
- **Decap**: Decapsulation exposes the integrated circuit for the purpose of direct probe connection to the silicon die. Various techniques have been developed to achieve this, suitable methods should be should be employed to be compatible with the particular packaging configuration in order to minimize complications from introduction of foreign matter or damage to the silicon device. Some de-capsulation techniques are as basic as breaking a package open or heating to melt the encapsulant, these are NOT recommended. Chemical removal of polymeric encapsulating material with acid, or mixtures of acids and solvents, is a very common method that gives good results if carried out correctly. However the acids involved are used in a concentrated form and significant health and safety issues are associated with this methodology. We favour the use of a proprietary mix of organic solvents, formulated to breakdown the molecular bonds within the encapsulant without damage to the die or bond wires, resulting in a very clean die, with reduced health and safety issues and a non aggressive action on the evidential material.

Once the die is electrically accessible via any of the aforementioned methods, micro positioners are utilised to attach probes to the bond wires or bond pads to provide a low impedance connection to the silicon chip. During setup proprietary software is used along with specially designed interfaces to give an indication of valid connection. Once electrical connection has been established, the ICCID of the device can be read to verify that the device is functional and ready to be accessed via SIMIS for the data extraction.

End of overview. The next section in this document will describe the above methods and specialist techniques and equipment in detail. Followed by worked examples with stage by stage images and descriptions.