

Cell Phone Forensics

By Marty Musters, CISSP, CFE, BMath

Forensic examiners are called upon to preserve the evidence by ensuring that the acquired media is not changed or altered in any way, thus enabling courts to accept the evidence from them. These examinations have typically been done on hard drives, (whether those hard drives come from desktop computers, notebooks or servers). The most useful pieces of information are typically e-mail, Web site visits or electronic files such as documents or pictures that are part of a crime.

That is, until now. What is becoming increasingly useful is the information stored on cell phones. As you'd expect, this includes information like phone numbers dialed, incoming calls received, phone directories, appointment reminders and calendars. But there is more. Cell phones also allow you to text message, browse the internet and take pictures. You can even set up your cell phone with a free e-mail address. With over a billion subscribers worldwide, cell phones are a realm that is for the most part an untapped resource of valuable information when it comes to forensic examinations of digital media.

Nothing comes without its challenges of course. Cell phone data storage is proprietary, based on the manufacturer, model and system. Each device is unique and caution should be used as each phone has unique considerations. Never the less there are now software vendors out there to help. The challenge of course is to acquire the information in a forensically sound manner. Not an easy task given that a new message or call can come in *after* the cell phone was seized which would mean that the evidence was altered.

The most popular system for cell phones today is the Global System for Mobile communications (GSM), now implemented at a global scale on all continents. GSM is a fully digital system allowing both speech and data services and allows roaming across networks and countries. There are several points of interest to us as forensic examiners. The first of course is the phone itself and the Subscriber Identity Module (SIM) card located inside the phone. The name of the network provider is usually visible on the SIM card along with a unique identification number that can be used to get information from the provider, such as name, address and phone number associated with the SIM card. A PIN code (Personal Identification Number) is usually required to access the SIM. If a user fails to enter a valid PIN through three attempts the card becomes blocked and then an 8 digit code called the PUK (Personal Unlock Number) must be entered. You now have 10 attempts to get the PUK correct before the SIM is permanently disabled. The good news is that the user cannot change the PUK which is provided by the network operator, who almost always keeps track of the PUK. An investigator can then almost always gain access to the SIM by contacting the network operator for the PUK.

The SIM card is simply a smart card containing a processor and non-volatile memory. In cell phones, the SIM card is used as a storage device for subscriber related data. The processor is used to implement the access mechanisms to the network and the security features. The SIM card can therefore be accessed by mounting it in a standard smartcard reader. The on-board processor will challenge the examiner for either the PIN or PUK code after which the binary contents of the card are made available. Best practices would dictate that a forensic bit stream image is made of the SIM card and a hash of the contents computed. Subsequent analysis would be done on the image. Care must be taken at all times to ensure that the contents of the SIM card are not altered in any way. Following are useful pieces of information for the forensic examiner

- Location Area Identifier – This is an identifier of where the mobile phone is currently located. This value is retained by the SIM card when then the phone is turned off. This is useful for determining in which location area the mobile was last used when it was operating. The network operator will usually have to assist in determining the physical location area. It should be noted that a location area can contains hundreds of cells. Unfortunately the cell within the location area is not stored.
- Serial number – This number can be retrieved without providing the PIN and will therefore identify the SIM itself
- Customer number – Referred to as the IMSI it is the customer identification number which will allow you, with the aid of the network provider to identify the customer who owns the phone
- Cell phone number – Referred to as the MSISDN
- Text Messages – Normally there is space on the SIM which will show the last 12 text messages that were sent. In addition cell phones also store messages in memory. A typical cell phone configuration will store all incoming messages by default and outgoing messages are only stored at the users request. Most cell phones use the SIM memory first before using internal memory.
- Deleted Messages – Similar to deleting a file on a typical hard drive; the first byte is set to zero. This means that deleted messages can be retrieved except for the first byte as long as a new message has not overwritten the old message.
- Dial Numbers – Most phones have the ability to store about 100 dial numbers with an associated name.
- Last Dial Number – Most cards only store about the last 5 phone numbers dialed on the SIM card. Most phones however store many more last dialed numbers on the phones internal memory.

Now as forensic examiners we need to be aware that phones can be altered or cloned. If one has direct access to a phone a “flasher” can be used to freely modify the contents of the phone. This is typically done to remove the access constraints of a phone which locks a certain phone to a certain Service Provider. These “locked” phones are often sold as part of a package tying that customer to the service provider. Another change one would want to do is to change the actual phone number of the cell phone which is stored on the

SIM card. This is necessary to use a stolen phone as the original number would be “blacklisted” once it was reported as stolen. It would be important for a forensic examiner to determine if the internal phone number of the phone had been changed. Normally the “original” phone number is printed under the battery so a comparison of the phone number of the SIM card against the externally printed number is a good practice. In fact, 80% of all phones used in criminal activity are phones that have been stolen and the phone number modified.

It is also possible to do a “man in the middle” attack to steal the phone credentials thus allowing the attacker to program a phone to look and pretend to be someone else’s phone. In the Saturday Dec 15, 2005 newspaper of the *Toronto Globe and Mail*, Cindy Hopper, a Manger in Rogers Wireless security department, said that terrorists groups had targeted senior Rogers executives for cell phone cloning since the company was loath to shut off the cell phone of their busy executives and of course the public-relations debacle that would take place if word ever got out.

In summary, the challenges never cease for the forensic investigator. With proprietary phones and operating systems and the ability for end users to change the SIM data, we still are faced with the same questions. “Who committed the crime?” And the answer, a resounding, “It wasn’t me!”

Marty Musters graduated with a Bachelor of Mathematics and Computer Science from the University of Waterloo. He is a CISSP and a CFE (Certified Fraud Examiner) and a member of the High Tech Crime Investigation Association (HTCIA).