

SIMs and Salsa

Lee Reiber
Mobile Forensics, Inc.
September 2008

Introduction:

This document has been created for examiners to assist them in the search for the most forensically sound processing methods in cellular data extraction. Also, I have been asked many times about the creation, duplication, isolation and make up of Subscriber Identity Module (SIM) cards and decided that a document covering these items would be of benefit to everyone.

SIM Cards

A SIM card's main function for all intents and purposes is the key for a GSM (Global System for Mobile Communications) and iDEN (Integrated Digital Enhanced Network) networks. This small plastic smart chip is needed for communication on the cellular network, without it the cellular handset is just a digital storage device, not a cellular phone. In short the SIM card is needed to make up the Mobile Station (MS) and allows the Mobile Equipment (ME) to be told by the network, "OK, you belong on the system", or "you are denied from operating on the system".

In cellular phone forensics we want, or better yet strive for "DENIED" or "INACTIVE SMART CARD (chip) to be displayed on a GSM/iDEN device. Why? Simply, we have fulfilled the most important rule of cellular phone processing, NETWORK ISOLATION.

Why is network isolation so important or moreover the most important step to take in processing ANY cellular device? The answer is easy. If we successfully inhibit the communication between the Mobile System and the network by isolating the device we have established a quasi "write protection". The cellular network cannot change, alter, or delete data in the handset because it cannot "see" or "touch" the device over the air (OTA). This now puts the pressure on the examiner to effectively process the device in a safe manner because the excuse that the network information that arrived onto the handset overwrote the data will be non existent. The responsibility now shifts to the steps that are taken by the examiner to process the device in a forensic manner using a tested procedure. The PROCESS and PROCEDURE of the examiner is the focus of the Mobile Forensic Certified Examiner (MFCE) course of study and a cornerstone to the training courses of Mobile Forensics, Inc. This process is not the focus of this document and will not be discussed further.

The focus of course are SIM cards and eliminating the need for Faraday boxes, bags or any other device or contraption that focuses on "shielding" a device from radio signals physically.

SIM cards are composed of a plastic shell and a computer chip. The exact characteristics of these smart cards can be located in the GSM Standards ETSI TS 102 221. We will not be discussing these in this document. In the interior or file system, if you will, there are

many files that hold data that also follow GSM standards and are documented in GSM standards under ETSI TS 131 102.

The two files we will focus on in this document are the ICCID (Integrated Circuit Card Identifier) and the IMSI (International Mobile Subscriber Identity). We will be focusing on these two important files because these files are needed to complete a **Forensic SIM Clone™** and effectively isolate the device from the cellular network. To further elaborate, some handsets only need the IMSI, while some need only the ICCID and in some cases the device needs both the ICCID and IMSI.

Mobile Forensics Inc coined the term **Forensic SIM Clone™** because the completion of this method should not be considered in anyway a “clone” in the sense that the card is a duplicate of the original SIM. If that were the case then we have not effectively isolated the clone from the network because if it is a duplicate of the evidence all the network information still resides on the handset. If this network information still resides on the cloned card we know that the cellular network can add, delete or change data on the handset. Hence “Forensic” was added because all the network information is non existent. More on this later.

*** There are some trainers, companies and institutions that have instructed students that the Ki is also needed for a successful clone of a card. Well, this would be a true statement if we were actually attempting to “steal” service from a GSM subscriber because the Ki is used in the Authentication process with the network. This was a technique used to actually USE someone’s service and has no bearing on correctly creating a **Forensic SIM Clone™** .*

Some say, “Hey, why not just place an inactive SIM into the evidentiary phone?” The answer to this is “sure, that would effectively remove the handset from the cellular network”, but because the handset “sees” the SIM card as foreign, data will be deleted from the device. Sometimes images, videos, text messages and contacts are removed by doing this. The call history is usually always eliminated if a foreign SIM is inserted into the evidentiary device.

Foreign, why would a handset “see” another card as foreign? The handset “looks” for a known file or files on a device. If the device “recognizes” the file or files it continues the cycle up of the device without error. If the device does not recognize the file or files and exception occurs and the device errors usually deleting user data. This damage has been seen in all makes and models tested.

So the idea behind compiling a **Forensic SIM Clone™** is to only duplicate the ICCID and IMSI of the original evidentiary SIM card. In duplicating these files the handset in essence is “tricked” into believing that the right SIM card is inserted and because the card contains no other network information, the handset cannot communicate with the network.

We will not go into the steps to compile a **Forensic SIM Clone™** manually for obvious reasons, one of which was the long process of research and development to make this technique a reality and the other is that other developers, companies and researchers may forgo their own research. The manual steps are covered in the Mobile Forensics Inc. 202 course where the goal is to teach the examiner this important information on their way to becoming an expert in the field of mobile forensics. In the interim, Mobile Forensics Inc. has developed an application that automates the process of creating a **Forensic SIM Clone™** in a matter of seconds. The examiner can read the evidentiary SIM in the application and then write the necessary files to the **Forensic SIM Clone™ Card**. The examiner can now be certain that the device has been isolated from the network and data HAS NOT been deleted.

What if the original SIM card is PIN locked? SIM card is gone? Damaged?

For starters, if the SIM is PIN locked you are limited by the inability of most logical software to process the device. Again, I say logical, we will discuss physical software shortly. We know if the SIM PIN is locked, the ICCID is still readable. This is due to the fact the ICCID does not need a security condition to be satisfied to be read. Reading the ICCID is easy, but how about the IMSI ? Well, the opposite is true for the IMSI. The IMSI does have a security condition, the PIN. Unfortunately if we do not have the PIN we cannot satisfy the condition to read the IMSI. Without the IMSI we cannot in confidence create a **Forensic SIM Clone™** that the device will not think is foreign.

So how do we obtain the IMSI?

There are three methods that can help with this dilemma.

- Send court order to cellular carrier
- Obtain the IMSI from physical memory
- Or create the IMSI yourself

I am sure you are aware of the first solution. By sending a valid court order to the carrier they can supply the last IMSI utilized by the device and matches the ICCID you have supplied. The second way mentioned above involves using specialized hardware/software to obtain RAW data from the device and then parse the data, recovering the last IMSI or last IMSI's of the SIM. The examiner can then manually type this information into the MFI Forensic SIM Cloner application and create a **Forensic SIM Clone™**. I am sure you are wondering about the third situation, creating the IMSI yourself.

For some US cellular providers, particularly T-Mobile, AT&T and Cingular, have made it easy for us! A little background first.

The ICCID is made up of five parts: The System code , MCC (Mobile Country Code), MNC (Mobile Network Code), the Subscriber number and Check digit.

For example the number 89310170105113168601 broken down would identify:

89310170105113168601 – System Code (89 for GSM)

89310170105113168601 – United States - MCC

89310170105113168601 – Cingular - MNC

89310170105113168601- Subscriber number

89310170105113168601- Check digit

*some network carriers use digits after the MNC to identify Home Register.

The IMSI is made up of three parts: The MCC (Mobile Country Code), MNC (Mobile Network Code) and the Subscriber number.

For example the number 310260123456789 broken down would identify:

310260123456789– United States - MCC

310260123456789 – T-Mobile - MNC

310260123456789 – Mobile Subscriber Identification Number

For T-Mobile, Cingular and AT&T the Subscriber number for the IMSI is deposited in the ICCID. What this means to the examiner is this:

Should a phone come into the lab with the SIM PIN locked, or without the SIM or a damaged SIM and the ICCID can be accessed we can create our own IMSI to produce the **Forensic SIM Clone™** without contacting the network provider! The examiner can take the raw ICCID and IMSI and enter this text into the MFI Forensic SIM Cloner and click write. The RAW text will be converted and written to the SIM card in the correct formatting! Of course it is suggested that the carrier be contacted if the SIM is locked to obtain the PUK to process as evidence at a later date, but because you have compiled the IMSI using the existing ICCID you can start processing the handset logically immediately! Below are some examples for T-Mobile, Cingular and AT&T.

I did examine SIM cards from both Mexico and Canada and was unable to duplicate the findings to indicate the IMSI is stored within the ICCID. Because I was unable to get my hands on many SIMs from outside of the United States I could not research and examine further, but I challenge those examiners in other parts of the world to look into the ICCID and identify the common thread between the numbers. You might be surprised.

How to take the ICCID of a T-Mobile Card to produce an IMSI

- Scan original SIM in SIM reader software of choice.
 - The ICCID will display
- Take the ICCID and move from the right to the left.

- We know that we are dealing with Cingular or AT&T and country code for US from information contained in the ICCID.
 - Please refer to the breakdown in this paper for more information
 - If you are not sure take the ICCID on numberplans.com and analyze. It will identify the Country and Network.
- So we will add MCC (310) and MNC (170) to Subscriber Number
 - 310170123456789
- We have created the IMSI from the ICCID.
 - We can now take that RAW IMSI and enter it into the MFI Forensic SIM Cloner along with the ICCID and create our **Forensic SIM Clone™**

89310170101234567891 *ICCID*



Subscriber Number



310170123456789 *IMSI*

Using these methods of:

- Network Isolation
- Compilation of **Forensic SIM Clone™**
 - By generating own from ICCID
 - Reading of Original SIM
 - Location in Physical Memory

It is my hope as an examiner that we will continue to move forward in the methods and processes being used UNIVERSALLY. Hopefully we will see the PROCESS of the examiners and the examination process being standardized through proper training and education. It is my hope that this method will be of use to the examiners around the globe.

LEE REIBER is the lead instructor and President Mobile Forensics Inc. (MFI), a training and consulting company who happens to think salsa should be placed on everything, even SIM cards. MFI is one of the leading training companies in the United States, training law enforcement, security and corporate professionals in cellular data extraction.

Lee Reiber and MFI have also developed the FIRST and ONLY PortScrubber application and has recently added the Forensic SIM Cloner application to their arsenal of forensic products.

MFI has recently joined CellPhoneDetectives.com and now offers a cellular handset processing service. Reiber is also a computer and cellphone forensic examiner for the Boise (Idaho) Police Department.

All materials contained in this document are protected by United States copyright law . You may not alter or remove any trademark, copyright or other notice from copies of the content.