

Moto Madness
Lee Reiber
Mobile Forensics, Inc
October 2008

Again I come to you talking about cellular devices. This time the Motorola flavor.

Hopefully these papers have made it safely to your inbox, outbox or spam box. I have been sending out these documents a little at a time but they are really just “excerpts” from an upcoming publication that I have been generating the last few years. Most of these papers I have sent out early because I see the need will benefit the examiners NOW more than later as they await a long winded publication! Again, thanks for reading on.

Motorola’s have long been around, starting with Martin Cooper and the sweet DynaTAC 8000, or the “Brick” as it was aptly named because of it’s enormous size and weight. I always poke fun in my lectures about “Sonny Crocket and Rico Tubbs” walking the beaches of Miami on those sweet phones without cables. Not to mention the sweet threads they were wearing! I better get off the 80’s references quick. Back to the phones.

Since examiners have started extracting data from these Motorola handsets they have really never ran into much trouble in both the GSM and CDMA world. I still talk to my instructors and tell them to grab a Motorola handset when conducting a LIVE demo because they are pretty well supported by most software and you can extract pretty much all logical data. So, grabbing logical data was and is a snap as has obtaining physical data in the recent years.

In MFI training blocks instructors speak of obtaining the handset PIN lock for both GSM /iDEN and CDMA handsets (Not PDA devices) and instruct the students about the locations for these little artifacts. You as the examiner should know that if a handset is locked, chances are when using a logical tool you will not be able to extract any data. So, in order to utilize these logical tools the examiner must unlock the handset PIN and then proceed to conduct the examination with the logical tool of choice. Like I mentioned earlier in the paragraph, MFI instructs students on the location and harvesting of these artifacts and also shows students how easily these can be obtained using programs like Bitpim (for CDMA) and Hardware Service Tools. Have you tried to grab the security code of a CDMA Motorola when it is locked? What if it is PIN locked and set to mass storage mode!! Now we have two problems, the handset is PIN locked and also set to mass storage mode. Lets talk first about the second issue, mass storage mode.

When a handset is set to mass storage mode it is “seen” by the computer as just what I mentioned, a storage device. When a handset is set to this mode the phone user or examiner can access the portion of the handset that stores media files and also the area allotted to the removable media card. This area should not be thought of as “the internals of the phone” with the ability to obtain a bit by bit copy of the phone’s internal memory, but storage space for the phone’s media files. The problem arises when the phone is set to mass storage mode. Logical programs cannot access the device to extract logical data to include contacts, sms, call history etc because it is set to mass storage mode. The logical software needs to communicate with the device via communication channels, i.e., modems or other serial interfaces, etc. The examiner has to switch the phone to be

recognized as a modem for this type of examination to occur. This is normally done by navigating the phone's menu and switching the device to be seen as a modem or PC syncing device for some devices. What if the phone is set to mass storage mode and locked? That can spell double trouble. This document will only discuss the steps for solving this problem with a Motorola CDMA handset.

If you come into contact with a CDMA Motorola that is PIN locked and stuck in **mass storage** mode follow these steps.

- Turn the handset OFF
- Press the * the # and the RED OFF button
- The phone will then show on the LCD that it is in BOOT LOADER or FLASH mode

You are now ready to move to the next step, getting the lock code!

In obtaining the lock code you will need a couple of easily accessible FREE programs. There are of course many programs that can make this happen for the examiner but only a couple are mentioned to demonstrate the technique. You can obtain both of these programs from <http://www.mfi-training.com/MotoMadness/SEEMS.zip>. Also, the most current Motorola USB drivers are needed which are located on the Motorola site or MFI forum.

The first program we will talk about is the Motorola Software Update application. This software is used to UPDATE the software on the Motorola GSM device, but we are only using it for one thing. Placing our Motorola in P2K Mode. What the? P2 WHO?

P2K mode is a proprietary mode for Motorola handsets that allows the user to communicate using additional protocols. Do you recall seeing several different drivers installing when you use Paraben's Device Seizure and select the Motorola physical plugin? It is in essence setting the Motorola to MODE=8. We discuss these modes and protocols in the MFI 202 course, "*Additional Techniques and Methodologies.*"

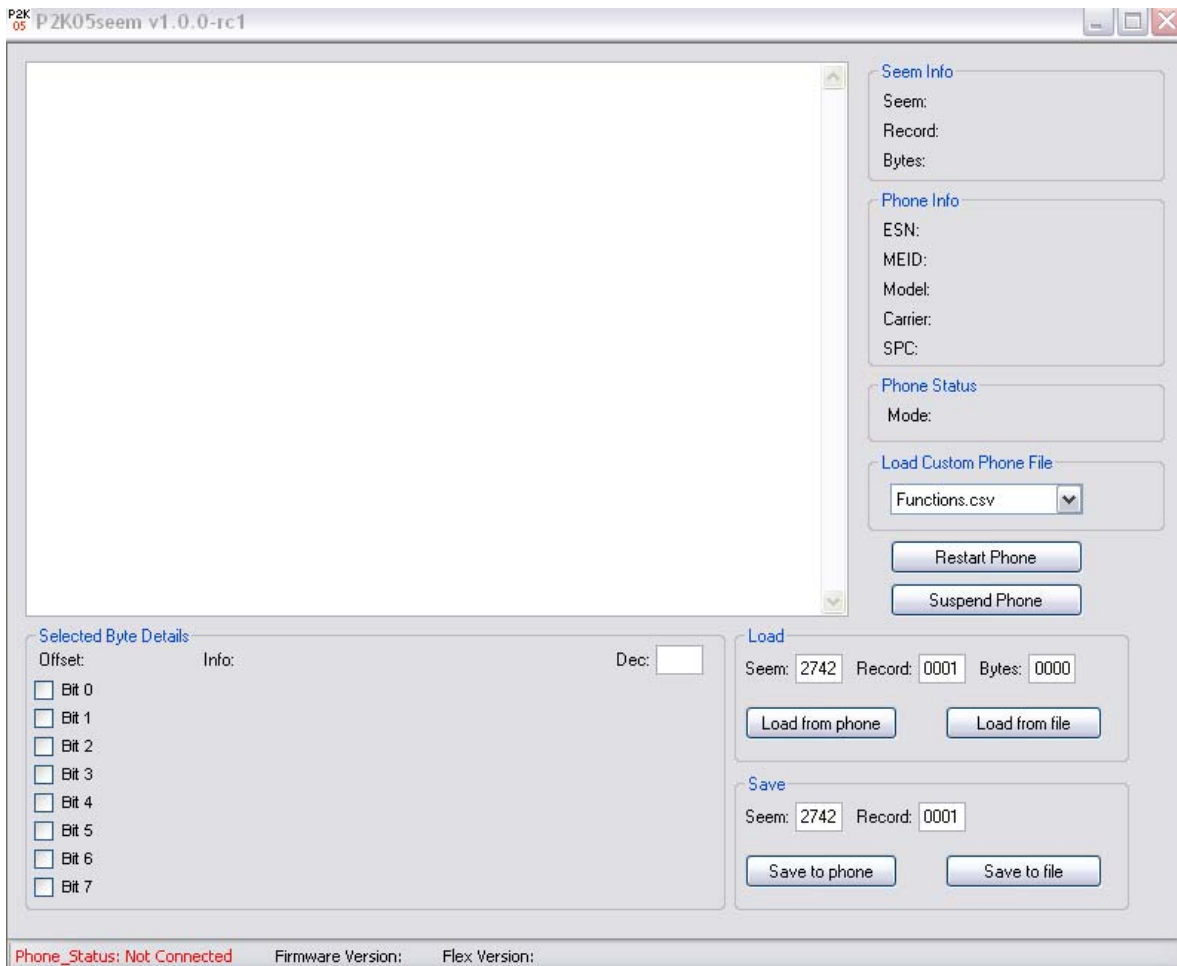
The second piece of software is a SEEM editor. That is S-E-E-M, but is pronounced seam like what expands during the holidays. The SEEM of the Motorola device is simply a piece of the storage area, specific file areas or locations in the handset's memory. Think of SEEMs as memory locations represented in hexadecimals. Pretty much PEEK and POKE if you remember back to your hacking days of old (oh the great times). So with SEEMs we need to know the memory offset, but also we will want to know the record number and the size of the data in bytes. Manipulating or changing SEEMs on a phone can allow the user to re-brand logos, change the dim on the LCD, make other things display on the handset then original programming, change the 1 key press to a 2 key press (fun to really freak your friends with that one!), and more. But what we are going to do is go to a memory location and GRAB the security code of the handset and have it display for us using a SEEM editor. Yes, the second word is editor, meaning you can edit SEEMs, fry phones, and make evidence into a paper weight. This of course is

why this paper has been written. It is to be used as a GUIDE to ONLY grab the handset PIN code and sub lock keys if needed. When I say by grabbing I mean READING. Lets find out how! First, connect your Motorola CDMA handset to your computer. Make sure it is OFF THE NETWORK!

If you have already loaded the Motorola driver set from the Motorola site or the Mobile Forensics Inc site you can then run the Motorola update software and wait. We are waiting for the additional Motorola Drivers to load, ie MCU logger, Test Command, Diagnostic Port etc. We use the Motorola Update Software to place the handset into P2K mode period. There are other methods to complete this process and sometimes the handset jumps into P2K mode with the start of the SEEM software, but this method will get everyone to a happy place, P2K mode. Back to the software. Once these drivers load you will see the ESN number display in the Motorola Update Software. Leave the software running. Now startup the SEEM editor that was in the download package from the MFI site.

If you encounter a Motorola E815 and some V series CDMA motos use Advanced P2KSEEM in the P2KSeem4V710 folder. Otherwise use p2k05seem 1.0-rc1.exe in the p2k05seem 1.0-rc1 folder. Lets start up p2k05Seem 1.0-rc1.

*** p2k05seem 1.0 will place your handset into P2K mode without the Motorola updater and Advanced P2KSEEM will not, but of course it does not hurt to already have the handset in P2K mode using the MUS.*



You will notice in the bottom left corner the status bar indicating that the phone is not connected. If will see this it is because of one of these issues:

1. Motorola Updater Software did not place the phone into P2K mode
2. You did not run Motorola Update Software
3. Your phone is not connected and on.

Satisfy all of the errors and hopefully you will now see in green CONNECTED.

Lets now learn how to enter the SEEM information. Look on the interface for the area that says **LOAD**. It is located in the lower right quadrant of the interface as seen below.

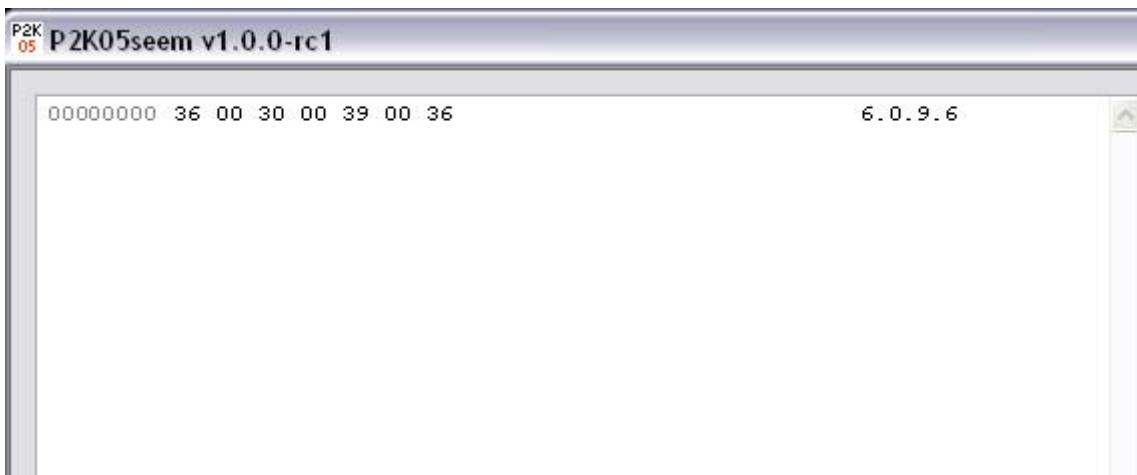
Load

Seem: Record: Bytes:

We are going to now learn what to enter in the various text boxes depending on what we want to extract from the phone's memory.

Lets just work on the security code and the SPC or subsidy lock code.

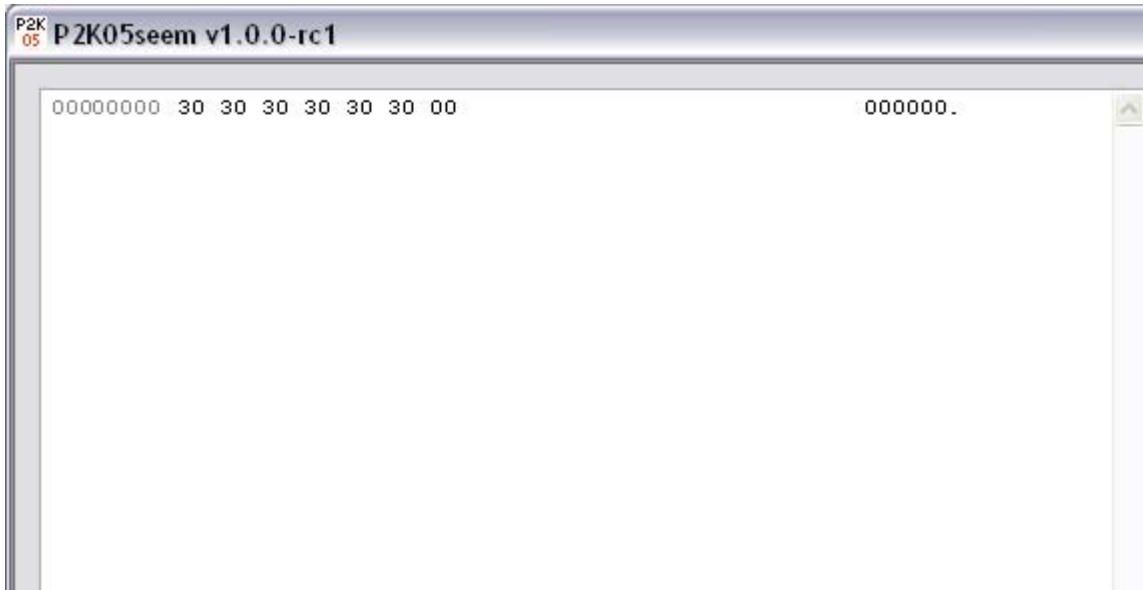
Place **2784** into SEEM, **0001** into Record and **0007** into bytes. This identifies the SEEM, 2784, the record 1 and the amount of data to extract from that location, 7 bytes. Then PRESS the Load from phone button. Shazzam! Look what is displayed in the large output box. The 4 digit LOCK code of the handset!



The SPC (Subsidy Lock) will be SEEM **0055**, **0001** and also **0007** bytes.

Load

Seem: Record: Bytes:



Obviously a Verizon phone, due to the 000000 SPC.

Mobile Forensic Inc is currently developing a tool that will do all of this with the click of a button without the knowledge of the SEEM. The user will just have to only know what model of Motorola you are looking to obtain the security code from.

Using the method I have just outlined the examiner can now do two things when processing the Motorola device:

- Get around the mass storage mode problem and data extraction when the handset is locked.
- And process a locked Motorola CDMA handset when the lock code is not available utilizing other methods (i.e. Bitpim)

LEE REIBER is the lead instructor and President of Mobile Forensics Inc. (MFI), a training and consulting company located in Boise Idaho, USA. 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 Mobile Forensics Certified Examiner course, the **ONLY** non vendor certification process that certifies the examiner **NOT** the tool. Several candidates currently in the program are due to complete the process in the upcoming months. For more information please visit www.mfci.us.

Many thanks to Karl Sonnenberg who kindly edited, ripped apart and made this sound better than the rambling mess it originally was.