Small scale digital device forensics journal, vol. 3, no. 1, june 2009 issn# 1941...

Technology, Mobile Phone

SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL, VOL. 3, NO. 1, JUNE 2009 ISSN# 1941-6164 1 The Fraternal Clone Method for CDMA Cell Phones Det. Cynthia A. Murphy Abstract - There are times during the examination of CDMA cell phones where the available phone forensics tools do not allow the forensic examiner/analyst to extract the data they need from the device. At other times, the available tools may allow the forensic examiner/analyst to extract the full file system of a CDMA phone, but data contained in the file system is encoded in a proprietary manner and cannot be decoded using forensic tools such as EnCase or FTK. Additionally, there are a number of situations that might preclude a forensic examiner/analyst from using a camera to document the data on a phone, such as when the phone's LCD screen is broken, the phone itself is broken, or the forensic examiner/analyst wishes to avoid physical manipulation of the phone to the extent possible during the examination. The CDMA Fraternal Clone method will allow the forensic examiner/analyst to transfer all user-created files and current settings from one CDMA phone into another phone, so that the target phone (CDMA Fraternal Clone) can be examined. The CDMA Fraternal Clone is used as a means to view the user created data and settings from the original phone in their native format allowing the forensic examiner/analyst to view and work with the extracted data in a way that emulates the original phone. Index Terms - CDMA Cell Phone, CDMA Clone, Mobile Phone, BitPim, broken cell phone, broken mobile phone, Mobile Phone Forensics, Cell Phone Forensics, Cell Phone Forensics Techniques, CDMA, ESN, MIN, CDMA Protected Files The CDMA Fraternal Clone method will allow the forensic examiner/analyst to transfer all user-created files and current settings from

one CDMA phone into another, so that the target phone (CDMA Fraternal Clone) can be examined. The CDMA Fraternal Clone is used as a vehicle to view the user created data and settings from the original phone in their native format. The CDMA Fraternal Clone process allows the forensic examiner/analyst to view and work with the extracted data in a way that emulates the original phone. I. INTRODUCTION T HERE are times during the examination of CDMA cell phones where the available phone forensics tools do not allow the forensic examiner/analyst to extract the specific data they need from the device. At other times, the available tools may allow the forensic examiner/analyst to extract the full file system of a CDMA phone, but data contained in the file system is still encoded in a proprietary manner and cannot be decoded using forensic tools such as EnCase or FTK. When these situations arise, a common fall back method is to document the contents of the phone screen by screen, using a camera system such as Project-A-Phone or ZRT. There are a number of situations that might preclude an forensic examiner/analyst from using a camera to document the data on a cell phone using screenshots, such as when the phone’s LCD screen is broken, the phone itself is broken, or the forensic examiner/analyst wishes to avoid physical manipulation of the phone to the extent possible during the examination. With GSM cell phones, a common solution used during the examination of the phone is to clone the SIM card from the evidentiary phone and to insert the cloned SIM card into another GSM phone to complete the examination. This method is not an option for CDMA phones because the data exists on internal storage chips within the phone and not on a SIM card. Figure 1: Using the CDMA Fraternal Clone method, it is

possible to transfer user data and settings from a broken CDMA phone to an intact one in order to view data from the original phone in its native format. II. USES AND LIMITATIONS OF THE CDMA FRATERNAL CLONE METHOD The CDMA Fraternal Clone method may be helpful to the forensic examiner/analyst under the following circumstances: 1. A CDMA cell phone is damaged or broken in a way that does not allow the forensic examiner/analyst to view the data displayed on the LCD screen, 2. The forensic examiner/analyst would like to work with the data extracted from a CDMA phone with minimal physical manipulation of the original evidence, 3. Available software tools don’t report all of the pertinent data from the broken phone such as the duration of the last call or other data of importance to the investigation, 4. Available software tools report conflicting information regarding data on the broken phone. Limitations: In order for the CDMA Fraternal Clone method to be successful, the phone must not be so damaged that the data on the phone isn’t accessible electronically and the data port must be functional. This method may not be successful on all CDMA based smart phones, but does work with some such phones. If the forensic examiner/analyst is unable to access SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL, VOL. 3, NO. 1, JUNE 2009 ISSN# 1941-6164 2 and create a copy of the file structure of the phone, this method will not be effective. III. CREATING A CDMA CELL PHONE FRATERNAL CLONE The goal of creating a CDMA Fraternal Clone is to transfer all of the user settings and user created data from the evidentiary phone into a second phone that is identical in make, model and firmware version. The resulting “ Fraternal Clone" is so named because although the user data in the fraternal clone will

be identical to that in the original phone, some system files will differ from phone to phone. This is an expected result: phone manufactures and service providers protect certain system files such as the Electronic Serial Number (ESN) as a method of preventing CDMA cloning fraud [1]. CDMA devices are protected by Electronic Serial Numbers (ESN), which acts as the authentication facility between the devices and the network [2]. 1 IV. HARDWARE AND SOFTWARE REQUIREMENTS In order to successfully complete the CDMA Fraternal Clone process, the following hardware and software is necessary: - Forensic computer - Correct USB Cable and drivers for the CDMA phone - A CDMA phone of same make, model, and firmware version of original phone 2 - Cell phone software/equipment capable of extracting or creating an image of the file system of the CDMA phone such as BitPim, 3 Paraben’s Device Seizure, or Cellebrite V. THE CDMA FRATERNAL CLONE PROCESS The process of creating a CDMA Fraternal Clone phone consists of four phases: (1) preparation of the forensic machine and the target phone; (2) creation of a full copy of the file structure of the evidentiary phone; (3) transfer of the data extracted from the evidentiary phone to the target phone to create the CDMA Fraternal Clone, and (4) verification of the integrity of the data transferred from the evidence phone to the CDMA Fraternal Clone. Phase 1 - Prepare the forensic machine and target phone: - Ensure that all necessary software and drivers are installed on the forensic computer: 1 - Applicable cell phone and cable drivers Chosen software for extracting the logical file system of from the evidentiary cell phone (Instructions for using BitPim are included here.) Clear the data from the target phone: o Ensure that the target phone (the eventual CDMA Fraternal

Clone) is reset to factory default settings. 4 o Physically check the target phone to ensure that it contains no remaining user data. If there are extra files and folders on the target phone from previous user installed application installations that are not removed by the factory reset process, the forensic examiner/analyst may wish to delete these files and folders using BitPim prior to beginning the Fraternal Clone Process. o The target phone will maintain its original ESN and other manufacture and/or carrier protected files. o o Phase2 - Create a full copy of the file structure of the evidentiary phone: - Using BitPim, set up a read-only session for the original evidence phone. Follow the instructions described in “ Setting Up BitPim to Extract &Document Cell Phone Data" in Appendix A. Following this process carefully will prevent co-mingling of data between cases and between phones. - Attach the evidentiary phone to the forensic computer and ensure that the phone is recognized in BitPim. If the phone isn’t recognized automatically in BitPim, try clicking the “ Find Phone" icon. Figure 2: BitPim Find Phone “ A CDMA device is protected by an Electronic Serial Number (ESN), which acts as the authentication facility between the devices and the network. So in the CDMA world, instead of approaching fraud from the ESN side, criminals are more likely to try to obtain handsets or network access fraudulently and build their attacks from there. " 2 It is easier than may be expected to find phones of the same make, model, and firmware. Good sources of target phones are cell phone recycling companies, and cell phone donation programs, and ebay. com. 3 Instructions for using BitPim to extract the file structure from CDMA cell phones are described in this document. - BitPim will notify you when the phone has been detected, and will inform you of the

phone’s status on the bottom panel of the BitPim screen. 4 Instructions for resetting CDMA phones to factory default can be found in the user manual for the phone, or at phone recycling sites such as: http://www. recellular. com/recycling/ data_eraser/default SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL, VOL. 3, NO. 1, JUNE 2009 ISSN# 1941-6164 3 Figure 3: BitPim Phone Recognized TROUBLESHOOTING HINTS: If the phone isn’t recognized automatically in BitPim, go to Edit > Settings and either choose the correct make/model of phone or choose Other CDMA Phone. Then choose Edit> Detect Phone. You may have to manually set the correct port for the phone in BitPim. To set the port manually, choose Edit> Settings> Browse and find the correct port setting. - Once the phone is detected by BitPim, choose View > View Filesystem. , (Even if BitPim reports that it doesn’t detect the phone, this may still work.) Figure 5: BitPim View Filesystem - expanded o Once the file system of the phone is displayed in BitPim, right-click on the root of the file system and choose “ Backup entire tree". Figure 4: BitPim View Filesystem Figure 6: Bit Pim - Backup Entire Tree - Next, click on the file system icon on the left side of the window. Once you see the folder in the middle pane of BitPim, click on the plus sign, and BitPim will begin to read and display the file system of the phone. o BitPim will then allow you to save the file system of the phone to a . zip file on your forensic machine. Save the . zip file in the proper directory on your forensic computer, and make sure to give it an identifiable file name. SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL, VOL. 3, NO. 1, JUNE 2009 ISSN# 1941-6164 4 Figure 7: BitPim — Backup Entire Tree — Save to . zip file TROUBLESHOOTING HINT: You may need to copy out each folder individually from the file structure of the phone,

depending on the make and model of the phone you are working with. To do so, right click on each folder and save it out to your forensic machine. o Once you have successfully obtained a copy of the logical file structure from the phone, secure your original evidentiary phone. Figure 8: BitPim — Restore from Backup TROUBLESHOOTING HINT: If the BitPim restore function does not work, each folder or file may need to be added manually. To manually restore the file system of the phone, unzip the archive you created earlier from the evidence phone and drag and drop the folders and files individually. o Once you have successfully restored the files from the original phone to the target phone, your CDMA Fraternal Clone is complete. Phase 3 - Transfer the data back into the target phone to create the CDMA Fraternal Clone: o Set up a BitPim session for the target phone. Follow the instructions described in “ Setting Up BitPim to Extract &Document Cell Phone Data: " in Appendix A. Following this process carefully will prevent co-mingling of data between cases and between phones. o Select Edit > Settings and then uncheck the box titled “ block writing data to the phone". This will allow you to write the data extracted back to the target phone. o Attach the Target phone to the forensic computer using the correct USB Cable. o Choose View > View Filesystem and view the file system of target phone in BitPim. 5 o Right click on the root of the directory (/) and select Restore… Locate the backup of the evidentiary . zip created earlier and click open. Phase 4 - Verify the data transferred from the evidence phone to the CDMA Fraternal Clone: 1. To ensure that the user data and settings transferred from the evidence phone to the CDMA Fraternal Clone are identical, create a logical image of the file structure of the fraternal clone phone with BitPim, using the

“ back up entire tree" option described earlier. 2. Using EnCase, FTK, or another tool that has the ability to analyze hash values, compare the hash values of the files from within the archive files of the evidence phone and the CDMA Fraternal Clone phone. 6 o You should find that the hash values related to the user-created data on the evidence phone and the CDMA Fraternal Clone are identical. 3. Those files that are system generated and/or protected will not have identical hash values. After completion of the above processes, the CDMA Fraternal Clone Phone will contain all of the data from the evidence phone, and the CDMA Fraternal Clone Phone can be used to view the files extracted from the evidence phone in their native format. 5 Caution: Because you have disabled the function to block writing data to the phone, this will allow you to not only view, but also to manipulate the file system of target phone directly. 6 Note that the archive files from the original phone and the cloned phone will not be identical because they contain the protected system files from the originating phones. SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL, VOL. 3, NO. 1, JUNE 2009 ISSN# 1941-6164 5 REFERENCES VI. ABOUT BITPIM BitPim is an open source tool designed to allow the user to view and manipulate data on cell phones (www. bitpim. org). BitPim runs on Windows, Linux and Mac. The latest version of BitPim can be found at www. bitpim. org. (As of the writing of this document, the current version of BitPim is: 1. 0. 7) VII. VALIDATION OF THE CDMA FRATERNAL CLONE METHOD The CDMA Fraternal Clone method was tested and results successfully replicated at the Champlain College Center for Digital Investigation, and by the Cyber Forensics Program, College of Technology at Purdue University. VIII. SUMMARY Under circumstances where

cell phone forensic tools do not allow the forensic examiner/analyst to extract or view the data they need from a device; available tools allow the extraction of the file system of a CDMA phone, but data contained in the file system is encoded and unreadable; or when the phone’s LCD screen is broken, the phone itself is broken, the CDMA Fraternal Clone method will allow the forensic examiner/analyst to transfer all user-created files and current settings from one CDMA phone into another, so that the CDMA Fraternal Clone phone can be examined. The CDMA Fraternal Clone is used to view user created data and settings from the original phone in their native format. The CDMA Fraternal Clone process allows the forensic examiner/analyst to view and work with the extracted data in a way that emulates the original phone. ACKNOWLEDGEMENT The CDMA Fraternal Clone method was developed during the course of an ongoing homicide investigation to address limitations of current phone forensics tools in reporting data extracted from a severely broken phone. The author would like to express her gratitude to Richard Mislan, Richard Ayers and Gary Kessler for making themselves available for consultation and advice during the homicide investigation. The author recognized that external testing and validation of the method would be necessary in the event of a trial. The author would like to thank Jeff Lessard and Gary Kessler at Champlain College Center for Digital Investigation, and Matt Levendowski and Richard Mislan in the Cyber Forensics Program, College of Technology at Purdue University for their assistance in the testing and validation of the CDMA Fraternal Clone Method. The author would also like to acknowledge the contributions of Garilyn Truttschel, Sam Brothers, and Gary Kessler who

reviewed and commented on this document. [1] Federal Communications Commission. (November , 2008). FCC consumer advisory: cell phone fraud. Retreived from htttp://www. fcc. gov/cgb/consumerfacts/ cellphonefraud. html [2] Henegouwen, E. B. (Winter, 2008). Protecting mobile networks from fraudulent attack. Retreived from www. cita. org/advocacy/index. cfm/ AID/11210 Cynthia A. Murphy is a Detective with the City of Madison, Wisconsin Police Department and has been a law enforcement officer since 1985. She is a certified computer forensic examiner and has directly participated in the forensic examination hundreds of digital devices pursuant to criminal investigations of various types of crimes including homicides, missing persons, computer intrusions, sexual assaults, child pornography, financial crimes, and other investigations. She has successfully utilized her skills in the investigation and prosecution of numerous criminal cases involving digital evidence and has testified as an expert in both state and federal court. Det. Murphy is also a part time Digital Forensics instructor at Madison Area Technical College. SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL, VOL. 3, NO. 1, JUNE 2009 ISSN# 1941-6164 6 APPENDIX A Setting Up BitPim to Extract &Document Cell Phone Data: BitPim software can be set up to store data from multiple phones in separate storage areas, preventing the co-mingling of data between cases and between phones. 1. Install BitPim Software — www. sourceforge. net/ projects/bitpim 2. Create a Master Copy of BitPim. The BitPim Master will be the starting point for each phone you process: a. Create a Folder on your desktop (or elsewhere if you want) named “ BitPim Master" b. Open BitPim. Set up BitPim to Block Writing Data to the Phone: From the upper right menu bar, choose > Edit > Settings 5.

Next, choose, Data > Create New Storage in the upper right menu bar of BitPim. 6. In the “ Storage Name" box, type “ BitPim Master" 3. 7. In the “ Select New Storage Dir" box, browse to the BitPim Master folder you created earlier. 4. The Settings screen will appear. Click the box “ Block writing anything to the phone. " Set Phone type to “ Other CDMA Phone" and Com Port to “ Auto" SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL, VOL. 3, NO. 1, JUNE 2009 ISSN# 1941-6164 7 8. In the “ Select Options" box, select “ Use Current Settings" 9. You will now see a box called “ Selection Summary. " Check your settings to be sure they are correct and then click “ Finish". If so, you have successfully configured the master copy of BitPim. 12. Create a unique name for the new instance of BitPim. Choose a name that will allow you to specifically identify the phone you are working on (case number, make, model, property tag or other unique ID.) 10. Once you are finished with the above process, EXIT OUT OF BITPIM. 11. For each phone that you process, you will create a new storage area for the individual phone. a. Start by opening the BitPim Master that you created above. b. From the BitPim Master, create a new instance of BitPim. In the upper right menu bar, choose > Data > Create New Storage 13. Create a unique folder for each cell phone you process. Again, choose a unique name for the folder (case number, make, model, property tag or other unique ID.) Browse to that storage location in BitPim, and then choose Next. SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL, VOL. 3, NO. 1, JUNE 2009 ISSN# 1941-6164 8 14. In the Select Options dialog box, select “ Use Current Settings" and then choose Next. 15. A summary dialog box will appear showing your selections. If you want to change anything, hit the back button and change the settings

accordingly. 16. Close out of the BitPim Master, and open up the new BitPim storage area you created for the phone you are working on. Use this instance of BitPim to process the phone. While it may seem that this is a lengthy process to go through for each phone, once you get a couple of repetitions in, it will become second nature. This process will ensure that the data you extract from each individual phone is not co-mingled in BitPim.