2007

Introduction to Mobile Phone Flasher Devices and Considerations for their Use in Mobile Phone Forensics

Marwan Al-Zarouni
Edith Cowan University

DOI: 10.4225/75/57ad5edd7ff34
Originally published in the Proceedings of the 5th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2007.

Introduction to Mobile Phone Flasher Devices and Considerations for their Use in Mobile Phone Forensics

Marwan Al-Zarouni
School of Computer and Information Science
Edith Cowan University
forensics@marwan.com

Abstract

The paper gives an overview of mobile phone flasher devices and their use for servicing mobile phones, their illegitimate uses and their use in mobile phone forensics. It discusses the different varieties of flasher devices and the differences between them. It also discusses the shortcomings of conventional mobile forensics software and highlights the need for the use of flasher devices in mobile forensics to compensate for the shortcomings. The paper then discusses the issues with the use of flasher devices in mobile forensics and precautions and considerations of their use. The paper goes further to suggest means of testing the flasher devices and suggest some tools that can be used to analyse raw data gathered from mobile phones that have been subjected to flasher devices.

Keywords

Mobile Forensics, Cell Phone Forensics, Flasher Box, Hex Dumping, UFS-3 Tornado.

INTRODUCTION

The need to address issues with mobile phone forensics is ever important. The number of mobile phone users nowadays surpasses 2.5 billion people across 218 countries and territories (Smith and Pringle 2007). Mobile phone abuse and problems caused by the use of camera devices within mobile phones are also increasing (Tarica 2007). Yet, conventional mobile phone forensic solutions do not seem to keep up with advances in mobile phone technologies. Furthermore, the development cost for supporting less popular mobile phones by such forensic solutions contributes to driving the prices of such forensic solutions higher (Espiner 2007). This is in addition to expensive updates and yearly subscriptions or service agreements that are sometimes needed to get support for the latest mobile phone devices.

New types of devices called "flasher boxes", also know as "flashers", are relatively cheap and are now becoming significant additions to mobile forensic investigators' arsenal of forensic tools. These devices are being used by forensic investigators in Europe and the United States of America to acquire forensic images directly from mobile phone devices (Breeuwsma et al. 2007, Purdue 2007).

ABOUT FLASHERS AND THEIR MOBILE SERVICE USES

Flasher boxes are also known as flashers or clips and they are mobile phone service devices used by mobile phone service providers and shops. They are mainly used to recover user data from dead or faulty mobile phones that otherwise will not provide access to data stored on their internal memory. They can also be used to update or replace software that is stored in the mobile phone's Read Only Memory (ROM). This software is commonly referred to as "firmware" and is usually pre-installed on phones by either the manufacturer of the phone such as Nokia and Sony-Ericsson or phone service providers such as Three Mobile or Telstra.

Flashers are also used to add language support and set regional settings for mobile phones. Changing regional settings can enable a user that bought a mobile phone device from Australia with Telstra-based firmware for example and did not have Arabic language support by default in the firmware to re-flash it with an Arabic-supported firmware supplied by Nokia in the Middle East. Therefore, he or she will have a mobile phone that now supports the Arabic language and will therefore be able to send and receive Arabic Short Message Service (SMS) messages.

Other uses for flasher boxes include removing or changing carrier settings and unlocking SIM restrictions or carrier based locks or call restrictions. Even though Subscriber Identity Module (SIM) unlocking is legal in some countries such as Australia, it can be illegal in some other countries.

IMEI AND THE ILLEGAL USE OF FLASHERS

International Mobile Equipment Identity (IMEI) is a unique 15 digit international serial number used to identify a mobile phone handset to a mobile phone network. This number can used to identify illegal mobile phone handsets. Each time a mobile phone is switched on or a call is made on it, the network provider checks the IMEI number of the handset, then it cross references it with a blacklist register such as the Central Equipment Identity Register (CIER) used in the United Kingdom. If it is on the blacklist then the network will either refuse to send a signal to the phone or will supply a signal but will not allow any outgoing or incoming calls (UnlockMe 2007).

Flashers can be illegally used to change the IMEI number of some mobile phone devices. This in effect enables criminals to illegally re-enable stolen or lost mobile phones that won't be otherwise usable on a certain mobile phone network.

Figure 1 below is a screen shot of the flasher software for UFS3 by SarasSoft that shows the option to change (rebuild) the IMEI number of the mobile device under the Aux features box within the DCTL group of devices options for the Nokia mobile phone brand flashing. It is worth noting that for Nokia, only DCT3 and DCTL group of devices allow for IMEI modification. Newer Nokia mobile phone devices embed the IMEI number in a non-re-writable chip and therefore are not subject to IMEI rebuilding.

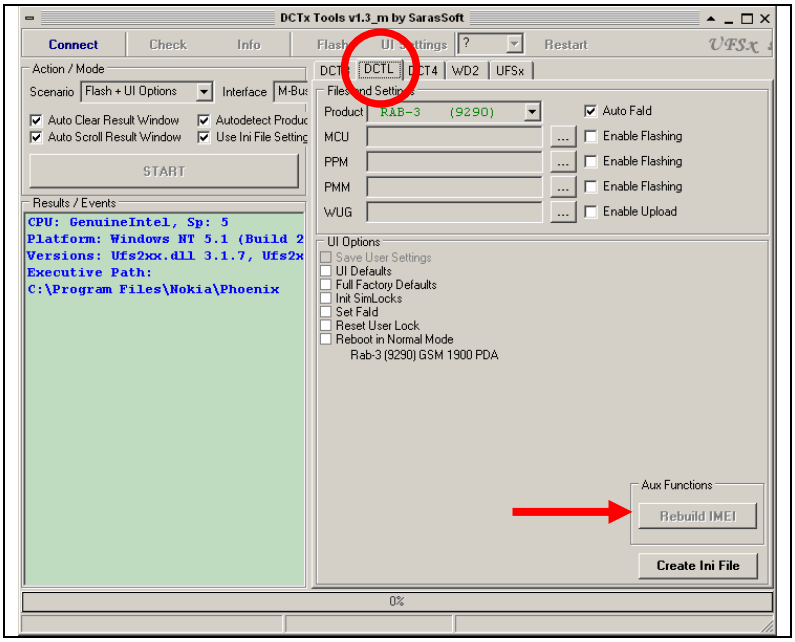

Figure1: Rebuild IMEI option for DCTL range of Nokia mobile phones

FLASHER BOX COMPONENTS AND VARIETIES

Flashers are a combination of software, hardware and drivers. There are many varieties of flasher boxes covering a wide variety of mobile phones. Therefore, choosing the correct box for a type of mobile phone device or phone model or mobile phone manufacturer can be a daunting task. There are two main categories of flasher boxes:

- Branded Boxes. The features of which include:
    - They are more expensive than their proprietary counterparts.
    - They have well known names and model numbers.
    - They have unique serial numbers.
    - Some boxes need activation. Software, updates and support is provided for these boxes. The level of support varies depending on manufacturer of box.
    - They are widely used by service technicians.
    - They are sold by recognized suppliers and an "approved supplier list" is often found on the manufacturer's website.
    - Easier to get support for them in forums and on other support websites.

    - Some boxes come with a large amount of cables and can cover both GSM and CDMA phones.
    - They do not usually require an external power supply to function. They rely on the USB interface as a power source.
- Unbranded (Proprietary) Boxes:
    - Much cheaper than branded boxes
    - Sometimes match the original flasher boxes in components and functionality.
    - Sometimes combine the functionality and phone support of more than one branded flasher box.
    - Sometimes support the addition of a smartcard from branded flasher boxes.
    - Do not usually come with any software and/or drivers and put the onus on the buyer to come up with the software from other Internet sources.
    - Some boxes come with phone flashing/servicing cables while others do not.
    - Some require an external power supply that is not usually provided with the purchase (IPMart 2007).

Figure 2: I-Pmart 2 In 1 Flasher Box With Smart Card Holder (IPMart 2007)

It is worth mentioning that none of the flasher boxes, branded or unbranded, are supported or indorsed by the manufacturers of mobile phones such as Nokia, Sony-Ericsson and others. The top selling branded boxes for the Nokia brand of mobile phone devices include:

- Universal box (UniversalBox 2007).
- JAF box (Odeon 2007).
- MT-Box for Nokia. There is a separate MT-Box for Sony-Ericsson. Even though both boxes are exactly the same and come with a 10 uses trial for the opposite brand (MT-Box 2007).
- UFS 3 tornado: The original flasher box and most widely recommended and used (UFSxSupport 2007).

Figure 3: UFS 3 Tornado Flasher Box

Widely used flasher boxes with support for multiple brands of mobile phones include:

- Smart Clip: Motorola, Sendo and others (Smart-Clip 2007).
- GTS Box: Nokia, Motorola, Samsung, Sharp, LG, Sony Ericsson and Siemens (GTS 2007).
- Vygis: LG, Sharp, Sanyo, NEC, BenQ, Alcatel, and Toshiba (Vygis 2007).

There are paid service sites and free phone repair communities that provide the following:

- Video tutorials on setup and use of boxes (FoneFunShop 2007).
- Constantly updated raw ROM images and language packs to flash mobile phone memory with.
- Service manuals and updates for software to cover a wide variety of mobile phones and flasher boxes.

USB flasher dongles that can be used for mobile phone servicing often offer less functionality than USB flasher boxes but may offer other added services such as:

- Remote unlocking and de-branding of phones.
- Credit points that can be used to do things such as IMEI change or unlocking of devices from a service provider.

An example of a product that needs pre-paid credit to unlock and de-brand mobile phones is the JAF device for Windows Mobile Phones (GSMServer 2007). It should be noted however that the JAF device will not work with all phone models running Windows Mobile software. While it supports some phones made by the Taiwanese HTC manufacturer, the do not support devices made by Palm which run Windows Mobile software.

Figure 5: JAF WM software and USB Dongle (PolPhone 2006)

ISSUES WITH COMMAND BASED FORENSICS SOFTWARE TOOLS

There are a wide range of software applications and mobile forensic toolkits that claim to acquire data from mobile phones in a forensically sound manner without altering any content in the mobile phone's memory. Such claims however cannot be verified. The basic flaw in these forensic software tools is in the way they gain access to data in the phone's memory. They use command and response protocols that provide indirect access to memory (McCarthy 2005).

Command and response protocols such as AT Commands (AT is short for attention) are commands that were originally developed to control modems to do things like dial, hang up, switch modes, and other modem commands. These commands are utilized by current command based forensic software to communicate with the mobile phone and query it about certain data held in the phone's memory. This means that the forensic software does not have direct access or low level access to data within the phone's memory and in effect treats every mobile phone as a black box. This also means that the software is dependant on the phone's operating system based command to retrieve data in the phone's memory. This could also mean that by querying the operating system, the device could be creating changes to the memory of the device. Because of this dependency on the operating system, such forensic toolkits cannot recover data from dead or faulty mobile phones.

Another flaw with these forensic software applications is that they cannot recover deleted data. This is because they access data at a high level or logical level which means that when a file is deleted, the pointer to that file within the operating system is erased which means that the file is no longer accessible by the operating system or visible to the phone's software. In addition, some mobile phone devices do not respond to AT commands making acquiring them with command based tools impossible (Purdue 2007).

Some command based mobile forensics software were not originally developed for forensic purposes and therefore they could unexpectedly write to the mobile phone device's memory (Horenbeeck 2007). Some forensic software suits such as MOBILedit Forensic 2.2 sometimes require the investigator to install additional software on the target mobile device (MOBILedit 2007). This is in direct violation of the principles of electronic evidence as published by the United Kingdom's Association of Chief Police Officers (ACPO) Good Practice Guide for Computer based Electronic Evidence (ACPO 2003). The guide states the following:

"No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court."

It is also in violation of the Guidelines for Best Practice in the Forensic Examination of Digital Technology published by the European Network of Forensic Science Institutes (ENFSI) which states (ENFSI 2006):

"Upon seizing digital evidence, actions taken should not change that evidence." and "Wherever possible no actions taken during the seizing of any evidential material should cause that material to be changed and this is of particular importance when dealing with digital evidence which could be seen as prone to accidental 'tampering'. Where actions have been taken that change the data, this should be fully documented."

Therefore, new ways to gain direct access to data held on mobile phones without resorting to the operating system software or hardware command and response protocols must be utilized in mobile phone forensics. Flasher boxes can provide this direct low level access and therefore they can be considered as a future pathway on the quest for a more optimal acquisition of mobile phones.

FLASHER BOXES AND MOBILE PHONE FORENSICS

The forensic use of flashers is already being taught to future digital forensic examiners in Purdue's College of Technology in the United States of America (Purdue 2007). It is also being used by European investigators in mobile forensic cases (Purdue 2007, Gratzer and Naccache 2007).

Flasher boxes offer access to the phone memory unmatched by command based methods. They also do not require the investigator to install any software on the target mobile phone and therefore do not disrupt the evidence in that way. This in turn means that they follow rules of evidence more closely than command based forensic software tools. But because they are not usually documented, there are no easy methods of determining if they do actually preserve evidence in the phones memory and there is no guarantee that the flashers will work in a consistent manner (Gratzer and Naccache 2007).

Moreover, these devices not approved or tested by the mobile phones manufacturers to work properly on their mobile phone headsets. Furthermore, they are not forensically proven nor tested for forensic soundness. Because of that, investigators should be careful when attempting to use such devices in mobile phone forensics cases.

Flasher software and hardware were designed for mobile phone servicing needs which means that they are capable of writing to the memory of the phone as well as reading from it. By design, the flasher software does

not offer write blocking as with made-for-purpose forensic software. So, the flasher software could be writing to the phone while reading data from it, it effect altering evidence on the phone.

One of the limitations of flasher reading capabilities is dependant on the mobile phone device and/or range of mobile phone devices and the design of the software itself. With some mobile phone devices, full access to memory is blocked and only partial access is possible through the use of flasher software. Some flasher software skip some spare areas in the memory space and do not perform a full copy of the devices memory (Breeuwsma et al. 2007).

Moreover, flasher software present the user with both the memory reading and writing buttons on the same screen which can lead to accidental pressing or the wrong button on the flasher software which could lead to the total loss of evidence from the phone's memory. Figure 6 below shows some of the dangerous buttons that should be avoided by forensic investigators:

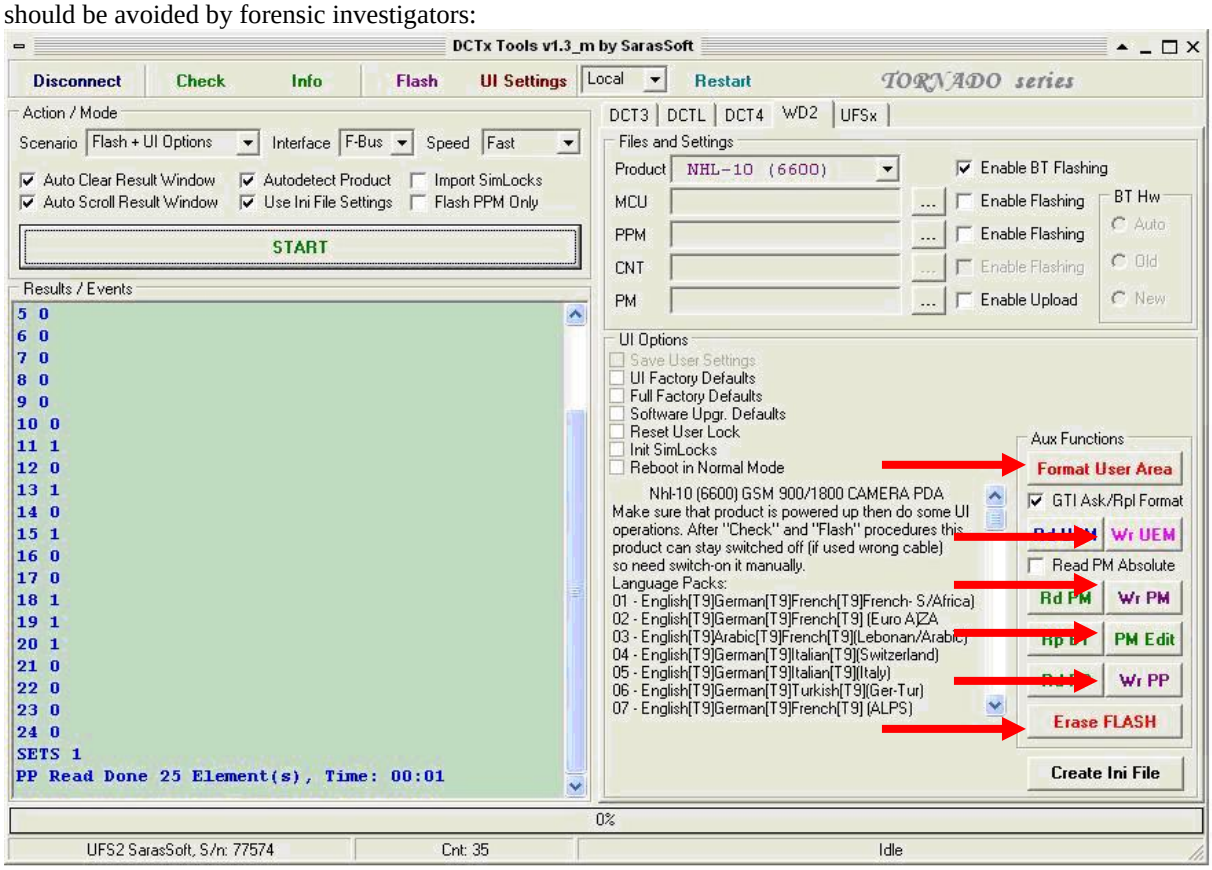

Figure 6: Some of the buttons that should be avoided.

Pressing the wrong write button could also damage the phone's memory in a way that could render the device useless turning the device into a "brick" (Harrington 2007).

FLASHER CABLES AND INTERFACES

The flasher box typically connects to the mobile device via a special cable made for that phone model. One side of the cable is the RJ-45 standard Ethernet networking cable interface. The other side usually contains a number of pins that contact the mobile phone's service ports through the Joint Test Action Group (JTAG) connection or the Mbus/Fbus connections (Harrington 2007). Figure 7 below shows a Nokia 6600 cable for the UFS3 Tornado Box.

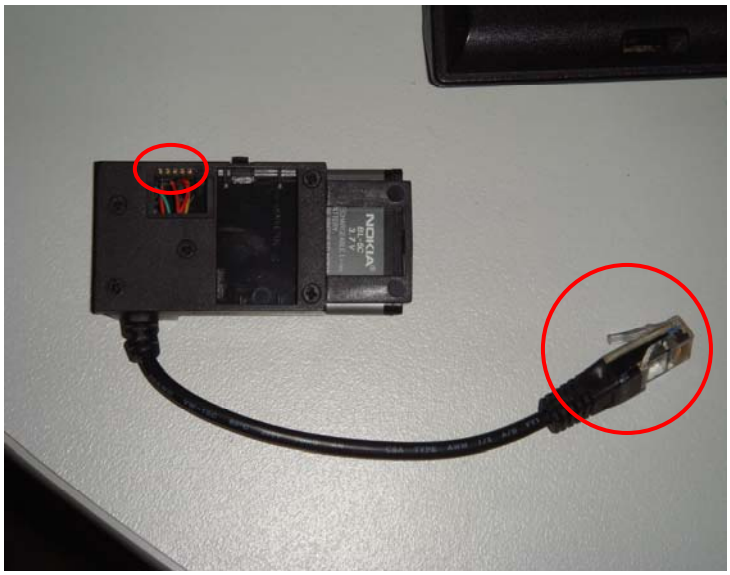

Figure 7: Connectors on the UFS3 cable for Nokia 6600

Software Installation Precautions

The appropriate software for each type of flasher box is usually made available through the official support site for the flasher box manufacturer. A username and password are given to each customer once they purchase a flasher box. Each flasher box is has a unique serial number that is displayed in the software's dialog box after it's installed.

Choosing the right driver for the type of mobile device can be confusing at times. This is because the support sites usually update the drivers frequently. Sometimes an older version of a USB driver and software bundle will run perfectly with some mobile phone models while a newer USB driver and software bundle will not work with the same device. Information about the best version of driver for each type of device or device range can be found in phone service forums as well as the support site itself.

USB drivers for the flasher box hardware in addition to the phone servicing software should always be installed BEFORE connecting the USB cable to the flasher box. If a certain version of software does not work properly with a mobile phone model or phone range then both the flasher servicing software and the USB drivers associated with it should be completely uninstalled. After restarting the machine after the un-installation the investigator can try another USB driver and software bundle until the appropriate driver and software combination is found. The following section of the paper describes some further considerations when using flasher boxes.

CONSIDERATIONS WHEN USING FLASHER BOXES

Some phones are accessible through service ports located on the bottom of the phone as with some Nokia models such as the 3220 shown below:

Figure 8: Nokia 3220 Fbus connections (Harrington 2007).

Some phones such as the Nokia N95 require an external 9V battery to be connected to the cable to power the phone while operating it with the flasher box. The investigators must always make sure that the battery is fully charged to insure consistent operation and results.

One of the biggest concerns when it comes to acquisitions through the use of flashers is the loss of volatile data. This is because, in the some cases, the phone needs to be turned off and the battery for the phone needs to be removed to allow for access to the phone's service ports which are pin contact points on the back of the phone that enable the acquisition of the mobile phone device. These points can be located under the battery of the phone, underneath the SIM card or just below the phone itself without the need to remove the battery of the phone. The location of the service ports is highly dependent on the model of the mobile phone.

Investigators should be careful when they deal with mobile phones with service ports under the SIM card. This is because when SIM cards are removed, some phones tend to loose information associated with them and this information might not be recoverable again. The pictures below show a connection cable with contact pins, a mobile phone with the pin contact points under the battery but not under the SIM card, and another mobile phone where the contact points are located beneath the SIM card (Nokia 6600).

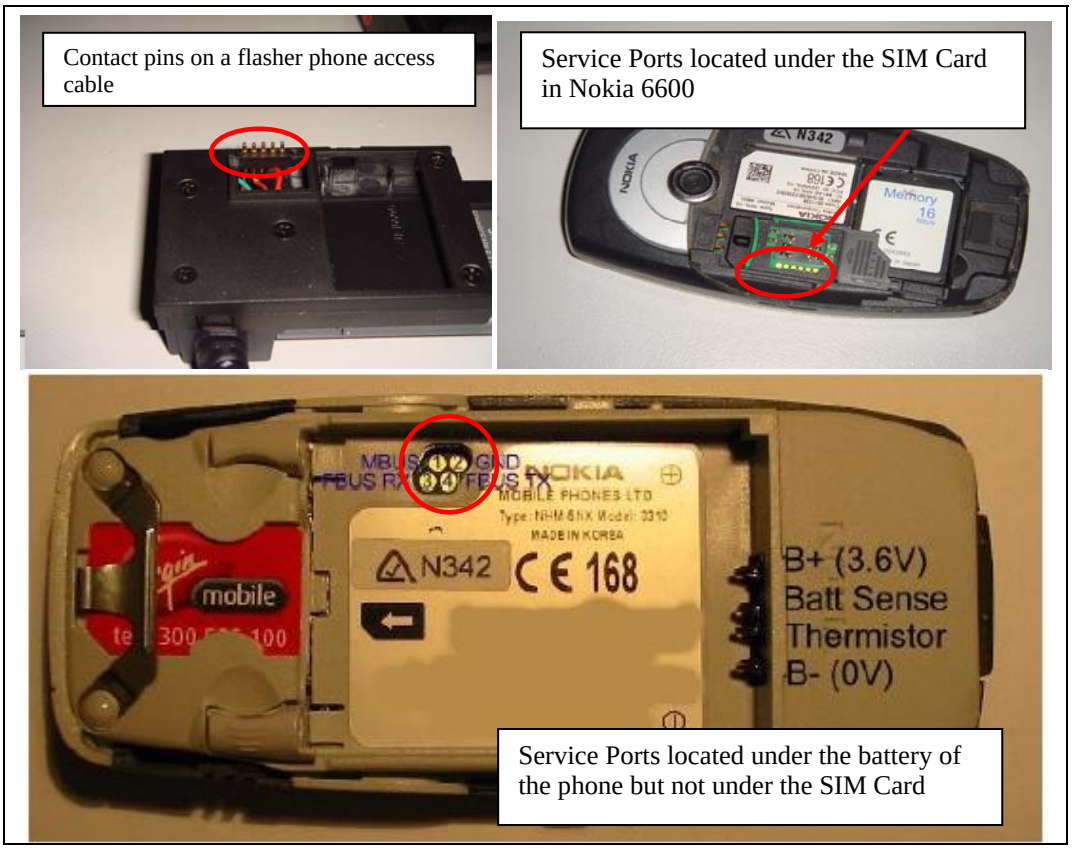

Figure 9: Contact pins that the cable from the flasher device connects to can be either under the SIM card or not depending on the device model(EmbedTronics 2005).

On the other hand, if a phone to be investigated has no SIM card inserted in its SIM card slot, it is recommended that a flasher box is used before any other command based tools. This is because if another SIM card is inserted in the phone, or if the phone is powered up normally without a SIM card inserted, it might lose important information about the SIM card previously inserted into it.

Some mobile phones require a SIM card to be inserted into them before allowing access to the phone, this means that command based software will not be able to acquire the phone without a SIM card present. Therefore, through testing of flasher boxes with each phone model is essential before using them for the forensic acquisition of mobile phones. Scenarios such as the ones described above, with and without SIM cards with AT commands first then flashers and vice versa should also be tested. Additional in depth testing considerations and suggestions are listed hereafter.

TESTING AND VERIFYING FLASHER ACQUISITIONS

One of the ways to verify the functionality of flasher boxes it to disassemble the flasher's code and track its behaviour with a logical analyser to understand its effect on the handset. This is not always easy to do and sometimes not possible at all and depends on the competence of the investigators and their knowledge in the practical use of logical analysers (Gratzer and Naccache 2007).

Another way to verify the use of the flasher device is to test it with a large number of mobile phone devices of the same model investigated in a particular case. One study into the use of flashers in mobile forensics suggests that some of these devices be used to develop an experimental protocol or acquisition procedure (Breeuwsma et al. 2007). The protocol is then fine tuned and made more stable and the procedures modified until they produce desired results. The device investigated is then examined using the tested procedure.

Another study takes this further and suggests that the finalized protocol should not be applied to the investigated device after testing the protocols or procedures but rather it should be tested on another set of mobile phones and the occurrences of the following six possible outcomes are then calculated: {information extracted, information not extracted} X {device unaltered, device altered, device destroyed}. This is then carefully documented and all the results are presented to the investigating judge to make a decision on whether to allow the use of flashers in the investigation (Gratzer and Naccache 2007).

PHYSICAL IMAGE ANALYSIS TOOLS

There are many tools that have surfaced in the last couple of years that address the need for the analysis of physical memory dumps from mobile phone devices. The tools range from easy to use tools to tools that require extensive forensics and hex editing and decoding expertise. The following is a rundown some of the tools and their features.

- FTS Hex: The first forensic tool that was developed for the purpose of low level examination of hex dumps from mobile phone memory. It is very basic and mainly sold to law enforcement officers (Knijff 2007, FTS 2007).
- BK forensics' Cell Phone Analyzer: The tool is a simple to use Windows based program that can analyse physical dumps from the following phone manufacturer devices: Sony-Ericsson, Nokia, Blackberry, Motorola and Samsung. The tool does not give the investigator great flexibility to examine the raw data in the dumped image but rather attempts to decode and display phone records, SMS data, pictures and other forms of data to the examiner. An evaluation copy is available to investigators for evaluation purposes from the developer's website (BKForensics 2007).
- Pandora's Box: A new tool developed by Mike Harrington. It recently passed beta testing and is now available in a full retail version. This tool is a very affordable alternative to BK Forensics' Cell Phone Analyser and offers the investigator with more control over the hex decoding process. It can retrieve data such as power down time and date on Series 30 Nokia phones (MFC 2007).
- Neutrino: A mobile phone acquisition device by Guidance Software to be used with Encase version 6. Extracted mobile device data is stored in an EnCase® Logical Evidence File (LEF) format and can be examined via EnCase v6 only (GuidanceSoftware 2007).

Conventional hex editors, decoder software and file comparison tools can also be used to examine the physical dump image and provide the investigator with more flexibility in examining the hex dump but require good knowledge in hex editing, some decoding skills and an eye for recognizing patterns and oddities.

CASE HISTORIES

The first case involves a witness who declared that he recorded a confession with the video camera in his mobile phone. The XRY forensic toolkit was used in his mobile phone to try to recover this piece of evidence but it did not find any videos files on the mobile phone device. Copying raw data from the phone memory did result in the recovery of a plethora or information about videos recorded in the memory and meta-data related to the videos in addition to the recovery of some thumbnails of some videos. The examination also resulted in the discovery of fragments of files in .3gp format that are used for video as well. No evidence was found though to back up the witness's claims (Breeuwsma et al. 2007).

The second case involves the discovery of two yet to be detonated improvised explosive device which used a mobile phone as detonator. The examination of the physical image of the non-volatile memory from the mobile device resulted in the recovery of the history of the of three to four International Mobile Subscriber Identity (IMSI) of the SIM cards used within those two devices and helped in linking the suspects to the mobile phones and to each other (Knijff 2007). This evidence would have not been recoverable by using command based mobile phone forensic toolkits that rely on logical acquisition of mobile phone devices.

CONCLUSION

As with all digital forensic investigations, it is essential to recover potential evidence from a device in a well documented manner and in a scientifically reliable manner with affecting the data on the device as little as

possible. All examinations must be conducted within the law of the country or state in which the investigation is taking place. The usage of flasher boxes requires a high degree of knowledge and competency from the investigator and a great deal of preparation, carefulness and a large amount of research and testing before the examination of a mobile device. Therefore, ample time should be allowed for the examination of such devices.

The future of mobile phones seems to be heading towards convergence with other digital devices such as the MP3 player, GPS navigational devices, laptop computers, camcorders, Personal Digital Assistants (PDA) and digital cameras. This means that more data will be held on such devices and the need for direct access to this data held in flash memory in a forensically sound manner will dramatically increase because of the complexity and the sheer amount of data stored on mobile devices. Therefore, it is very important for law enforcement personnel to familiarize themselves with the use of flasher devices and other means of acquisition and analysis of data held on flash memory.

REFERENCES

ACPO (2003) Good Practice Guide for Computer Based Electronic Evidence, URL http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf, Accessed 1 October 2007

BKForensics (2007) Cell Phone Analyzer, URL http://www.bkforensics.com/CPA.html, Accessed 8 October 2007

Breeuwsma, M., Jongh, M. d., Klaver, C., Knijff, R. v. d. & Roeloffs, M. (2007) Forensic Data Recovery from Flash Memory. *Small Scale Digital Device Forensics Journal*, 1.

EmbedTronics (2005) Welcome to Embedtronics, URL http://www.embedtronics.com/, Accessed 6 October 2007

ENFSI (2006) Guidelines for Best Practice in the Forensic Examination of Digital Technology v, URL http://www.enfsi.org/ewg/fitwg/documents/ENFSI_Forensic_IT_Best_Practice_GUIDE_5.0.pdf, Accessed 1 October 2007

Espiner, T. (2007) Mobile phone forensics 'hole' reported, URL http://news.zdnet.co.uk/hardware/0,1000000091,39277347,00.htm?r=6, Accessed 29 September 2007

FoneFunShop (2007) JAF WM : Flashing Windows Mobile Smart Phones Video Turorials, URL http://www.fonefunshop.co.uk/helpzone/jafwm.htm, Accessed 29 September 2007

FTS (2007) Forensic Telecommunication Services Ltd, URL http://www.forensicts.co.uk/phone-forensics.asp, Accessed 8 October 2007

Gratzer, V. & Naccache, D. (2007) Cryptography, Law Enforcement, and Mobile Communications, URL http://info.computer.org/portal/site/security/menuitem.6f7b2414551cb84651286b108bcd45f3/index.jsp?&pName=security_level1_article&TheCat=1001&path=security/2006/v4n6&file=crypto.xml, Accessed 27 September 2007

GSMServer (2007) JAF WM - Windows Mobile based phones solution. Debranding, software update, language change functions implemented, URL http://gsmserver.com/software/JAF-WM.php, Accessed 29 September 2007

GTS (2007) GTS-Box.org, URL http://www.gts-box.org/, Accessed 5 October 2007

GuidanceSoftware (2007) Neutrino, URL http://www.guidancesoftware.com/products/neutrino.aspx, Accessed 8 October 2007

Harrington, M. (2007) Hex Dumping Primer Part 1, URL http://www.mobileforensicscentral.com/mfc/include/Hex_Primer_Pt_1.pdf, Accessed 6 October 2007

Horenbeeck, M. V. (2007) Key constraints in forensic mobile device acquisition, URL http://www.daemon.be/maarten/mobforensics.html, Accessed 2 October 2007

IPMart (2007) I-Pmart 2 In 1 Box With Smart Card Holder, URL http://www.ipmart.com/main/product/IPmart,2,In,1,Box,With,Smart,Card,Holder,,Packaged,with,187,pcs,GSM,,CDMA,Cables,16927.php?cat=10&prod=16927&prod=16927, Accessed 29 September 2007

Knijff, R. v. d. (2007) Ten Good Reasons Why You Should Shift Focus to Small Scale Digital Device Forensics, URL http://www.dfrws.org/2007/proceedings/vanderknijff_pres.pdf, Accessed 6 September 2007

McCarthy, P. (2005) Forensic Analysis of Mobile Phones, URL http://esm.cis.unisa.edu.au/new_esml/resources/publications/forensic%20analysis%20of%20mobile%20phones.pdf, Accessed 31 September 2007

MFC (2007) Mobile Forensics Central, URL http://www.mobileforensicscentral.com/mfc/products/pandora.asp?pg=d&prid=346, Accessed 8 October 2007

MOBILedit (2007) MOBILedit! Forensic Application Overview, URL http://www.mobiledit.com/forensic/default.asp, Accessed 1 September 2007

MT-Box (2007) MT-Box Nokia, URL http://www.mt-box.org/products.php, Accessed 29 September 2007

Odeon (2007) JAF by Odeon, URL http://www.odeon.cn/, Accessed 29 September 2007

PolPhone (2006) JAF WM, URL http://polphone.pl/img/resources/1150455234JAF_WM.jpg, Accessed 6 October 2007

Purdue (2007) Expert: 'Flasher' technology digs deeper for digital evidence, URL http://www.physorg.com/news95611284.html, Accessed 27 September 2007

Smart-Clip (2007) Smart-Clip is a professional device for unlocking cell phones. Overview, URL http://www.smart-clip.com/, Accessed 5 October 2007

Smith, M. & Pringle, D. (2007) Global Mobile Communication is 20 years old, URL http://www.gsmworld.com/index.shtml, Accessed 28 September 2007

Tarica, E. (2007) Trouble in Cyberia, URL http://www.theage.com.au/news/education-news/trouble-in-cyberia/2007/10/19/1192301048347.html?page=fullpage#contentSwap3, Accessed 28 September 2007

UFSxSupport (2007) UFS 3 Universal Flasher Software, URL http://www.ufsxsupport.com/, Accessed 29 September 2007

UniversalBox (2007) Universal Box, URL http://www.universalbox.com/, Accessed 29 September 2007

UnlockMe (2007) Is your Mobile phone barred or blacklisted?, URL http://www.unlockme.co.uk/blacklist.html, Accessed 29 September 2007

Vygis (2007) VygisToolbox - Oficial website, URL http://www.vygistoolbox.com/, Accessed 5 September 2007

COPYRIGHT