Project 1:
Tools of Mobile Forensics

4055-841 12/16/08

A brief analysis by:

Conzetti Finocchiaro
Eric Goldman
Abhiney Natarajan
Maegan Stanek

For:

Professor Yin Pan

Contents

Cellebrite's UFED

About

The UFED (Universal Forensics Extraction Device) is a handheld device that can be used to extract information from mobile devices, specifically mobile phones and PDAs. The UFED can be connected to mobile devices in a variety of ways, making it versatile for numerous form factors and technologies. Cellebrite boasts that the UFED can connect and interpret data from 95% of the available phones on the market; this is done without affecting the data on the phone at all.

After phone data is analyzed and copied, the UFED possesses the capability to create detailed reports in HTML format, which can later be printed or emailed (or potentially used in a court case).

Usage/Merit

Without the need for an additional computer, the UFED can gather and save phonebook, picture, video, text message, call log, ESN and IMEI data from mobile devices. It can also be used to perform 'system dumps' on mobile devices utilizing the QCP file format. Such system dumps can be analyzed to restore data that was recently in memory, and potentially recently deleted items.

What makes Cellebrite's UFED so versatile, is its ease of use anywhere and its extensive list of supported mobile phones. The base UFED system comes with 65 connector cables, for interfacing with the majority of mobile phones available.

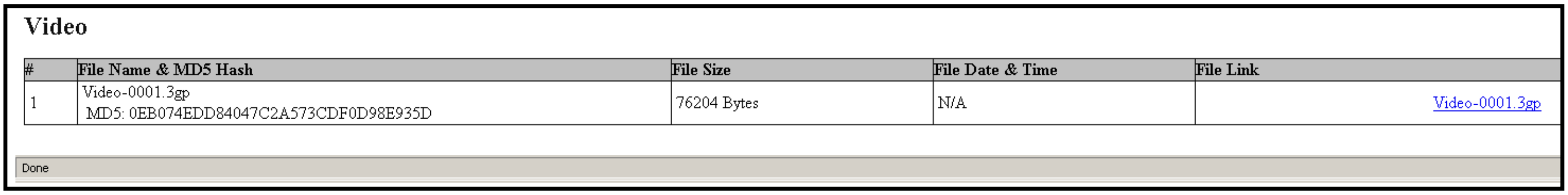
The UFED interfaces to mobile devices or mobile storage with the following connection types:

- Bluetooth
- USB
- IrDA
- Mini DIN to PC COM Port
- Mini-USB extension
- SIM / USIM reader
- SD Card reader

Local storage, in the form of USB storage or SD cards, can be used to house data from multiple mobile devices. This, paired with the portability of the UFED, makes the tool extremely useful in situations requiring immediate data backup.

Screenshots

The Cellebrite UFED, to provide an idea on the aesthetics of the device



Video

#	File Name & MD5 Hash	File Size	File Date & Time	File Link
1	Video-0001.3gp MD5: 0EB074EDD84047C2A573CDF0D98E935D	76204 Bytes	N/A	Video-0001.3gp

Wireless phone video data, gathered with the UFED. One of the many sections included in the HTML reports generated from the device. This was provided in a sample report, generated by Cellebrite, upon request.

Drawbacks/Liabilities

This tool is proprietary; non-free. The UFED could also become useful to a malicious user, if stolen. Additionally, it does not provide an authentication mechanism for the user of the device.

Methods of circumvention

The methods of circumvention would be specific to the device. Encryption could protect certain information, given the phone is robust enough to support such capabilities. Other circumventions are unknown.

Development Language

Unknown

OS targeted / limitations

As this is a standalone device, it does not possess the typical OS limitations. However, it is specific to the phones that are currently supported by the manufacturer. Cellebrite claims that they provide updates to their customers; however, to continuously add support for phones as they become available.

Also, as previously stated, system dumps are only available for a specific sect of devices.

Paraben's Device Seizure

About

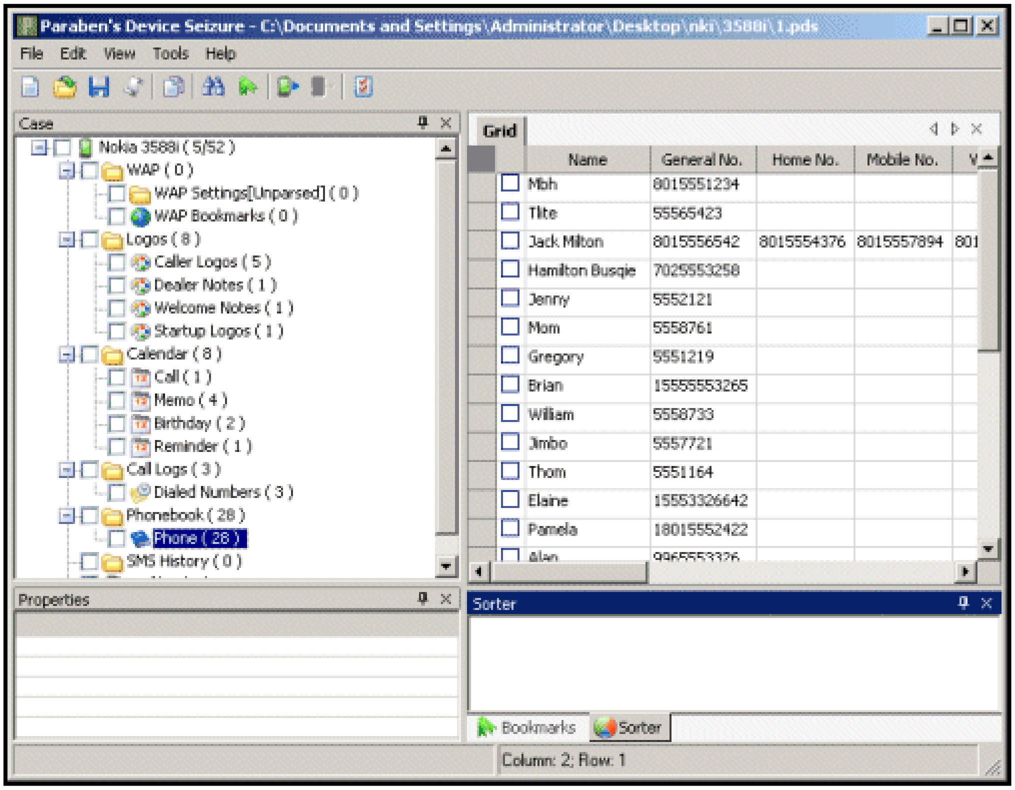
The Paraben Corporation established itself as a leader in specialized computer forensics software with its release of PDA Seizure in early 2002. Soon after, Paraben then released Cell Seizure, the first commercial tool for performing cell phone forensics. With the combination of these two tools, Device Seizure v2.2 was developed. Device Seizure acquires and analyzes data from over 1,950 mobile devices, PDAs, and GPS devices including the popular iPhones. Unlike much of the other commercial and free software devices, Device Seizure does not allow data to be modified on a device. If devices are designed to not only view data but to upload data as well, this poses an unsafe operation in the performance of a forensic examination.

Usage/Merit

Device Seizure can acquire the following data:

- SMS History (Text Messages)
- Deleted SMS
- Phonebook (Both stored in the memory of the phone and on the SIM card)
- Call History – received calls, dialed numbers, missed calls, and call dates and durations
- Datebook
- Scheduler
- Calendar
- To-Do List
- File system (physical memory dumps):
    - System files
    - Multimedia files (images, videos, etc.)
    - Java files
    - Deleted data
    - Quicknotes and more
- GPS waypoints, tracks, routes, etc.
- RAM/ROM
- PDA Databases
- E-mail
- Registry (Windows Mobile Devices)

Screenshots


Paraben's Device Seizure - C:\Documents and Settings\Administrator\Desktop\nki\3588i\1.pds
File
Edit
View
Tools
Help
Case
Grid
Properties
Sorter
Bookmarks
Sorter
Column: 2; Row: 1

- □ Nokia 3588i (5/52)
  - □ WAP (0)
    - □ WAP Settings[Unparsed] (0)
    - □ WAP Bookmarks (0)
  - □ Logos (8)
    - □ Caller Logos (5)
    - □ Dealer Notes (1)
    - □ Welcome Notes (1)
    - □ Startup Logos (1)
  - □ Calendar (8)
    - □ Call (1)
    - □ Memo (4)
    - □ Birthday (2)
    - □ Reminder (1)
  - □ Call Logs (3)
    - □ Dialed Numbers (3)
  - □ Phonebook (28)
    - □ Phone (28)
  - □ SMS History (0)

	Name	General No.	Home No.	Mobile No.	V
□	Mbh	8015551234			
□	Tlite	55565423			
□	Jack Milton	8015556542	8015554376	8015557894	801
□	Hamilton Busqie	7025553258			
□	Jenny	5552121			
□	Mom	5558761			
□	Gregory	5551219			
□	Brian	15555553265			
□	William	5558733			
□	Jimbo	5557721			
□	Thom	5551164			
□	Elaine	15553326642			
□	Pamela	18015552422			
□	Alan	9965553326			

Device Seizure, showing an exploded view of the available gatherable data from a Nokia 3588i

Drawbacks/Liabilities

Device Seizure does not support many common phone types. As a result, the drivers need to be installed for further examination. In addition, if a device has no data connection, been flashed with a firmware update, been unlocked to work on different networks, been dropped and damaged, has had internal firmware failures, or requires a different driver set, etc., Device Seizure may not be able to acquire any data even if the device has been tested by Paraben. Furthermore, Device Seizure alone, with disregard to the Training Bundle, Field Kit, or Command Kit, starts at a price of $1,095.00. This is a significant disadvantage of the product because it is not very affordable. Lastly, with the price rate of this product, you would assume that if a given device is password protected, it could be recovered as well by Device Seizure. However, an additional password recovery software tool is required. Of course, Paraben recommends their Decryption Collection which runs for $495.00.

Methods of circumvention

If a user's device has no data connection, been flashed with a firmware update, been unlocked to work on different networks, been dropped and damaged, has had internal firmware failures, or requires a different driver set, etc., Device Seizure is perhaps unable to perform a forensic examination on a given device. Thus, a knowledgeable user may be aware of the simplicity in modifying certain system settings.

Development Language

Unknown

OS targeted / limitations

Paraben’s Device Seizure initially supports the following cell phone manufacturers: LG, Motorola (including IDEN), Nokia, Siemens, Samsung, Sony-Ericsson, and, as previously mentioned, the iPohne. Although, Paraben can also add support for unsupported cell phone models from supported manufacturers with simple log files and simply a bit of time. GSM SIM cards with the use of a SIM card reader are additionally supported by Device Seizure as well. Subsequently, Device Seizure includes Palm DD Command Line Acquisition (PDD) and supports PDAs with the following Operating Systems: Palm through 5.4, Windows CE/Pocket PC/Mobile 6.x and earlier, BlackBerry 4.x and earlier, Symbian 6.0, 6.1, 7.X, 8.X, and 9.X, and EPOC 16/32 (Psion devices). Lastly, Device Seizure supports the Garmin type of GPS Devices with more manufacturers to follow.

SIMIS 2

About

SIMIS is one of the world's most comprehensive SIM card analysis solutions. It was engineered in accordance with ACPO guidelines to ensure that no data on the SIM is modified during the read process. SIMIS reports are digitally signed with both MD5 and SHA 256 hashes to ensure integrity.

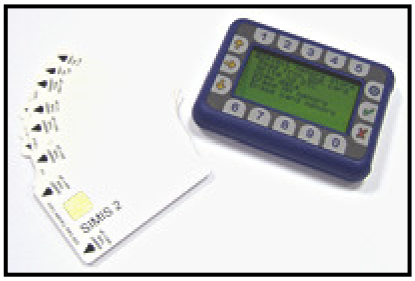
SIMIS works well with non-GSM based SIM cards, especially Nextel phonebooks. Satellite SIM cards from Inmarsat, Irridium, and Thuraya are also supported. SIMIS automates the process of forensic SIM data recovery. By interrogating the SIM card, SIMIS provides a detailed report in an easy viewable HTML format and user-definable printed format for every SIM interrogated.

The SIMIS software is used to collect data from multiple SIM cards. The compact easy-to-operate mobile unit is battery powered and comes with Data Transfer Cards for easy storage and transportation. Data stored on SIM cards is as integral to a thorough and complete investigation as the information is pulled from the phone. SIMIS brings a legacy of success, independent testing and the widest support of SIMs from around the world to examiners looking to ensure they get the most data from the SIM

Usage/Merit:

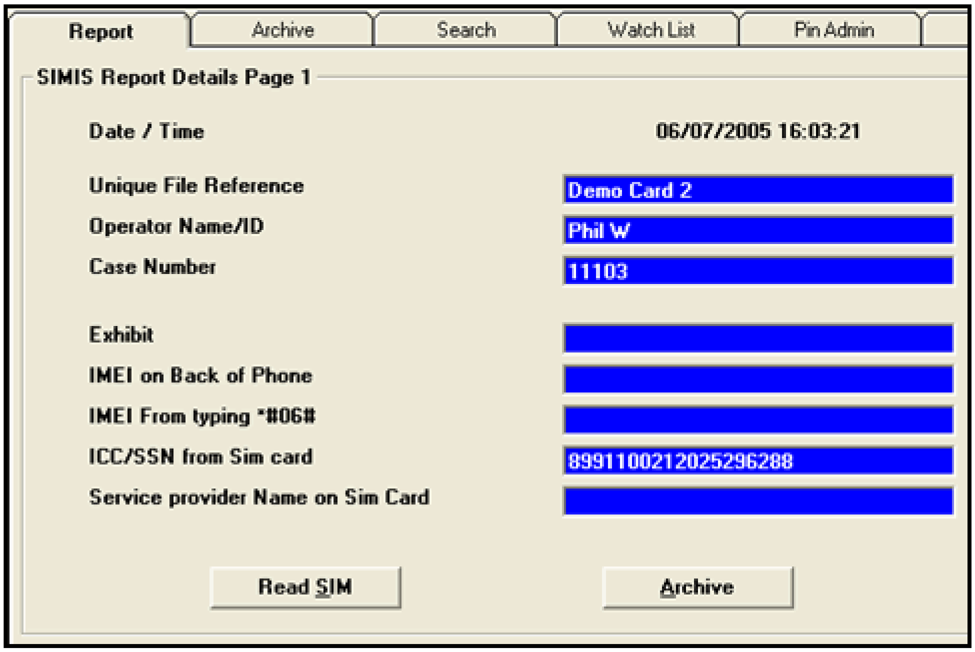
- Retrieve data from SIM cards
- Survey Cell coverage independently of Operators
- Recover data from damaged SIM cards
- Detect mobile phone usage
- Detect illegal mobile phone blockers
- Exchange encrypted SMS messages in covert operations

Screenshots:



SIMIS Handheld Card Reader

SIMIS Package



SIMIS Report Details Page 1

Date / Time 06/07/2005 16:03:21

Unique File Reference: Demo Card 2

Operator Name/ID: Phil W

Case Number: 11103

Exhibit:

IMEI on Back of Phone:

IMEI From typing *#06#:

ICC/SSN from Sim card: 8991100212025296288

Service provider Name on Sim Card:

SIMIS data gathering

Drawbacks/Liabilities

- It requires 2 AAA cells for the Reader and SIMIS does not work well with a wide range of mobile devices. However, there is a separate SIMIS 3G for 3G mobile phones.
- This tool is proprietary; non-free.

Methods of circumvention:

The methods of circumvention would be specific to the device. EmoSec, a secure text messaging system never stores the message on the phone. However, the phone should support the very feature. Other circumventions are unknown.

Development Language:

Unknown

OS targeted / limitations:

The limitations are set on the mobile phones. SIMIS II works well with a good range of mobile devices. Also, it can be used with third- party SIM reading software packages.

MOBILedit! Forensic

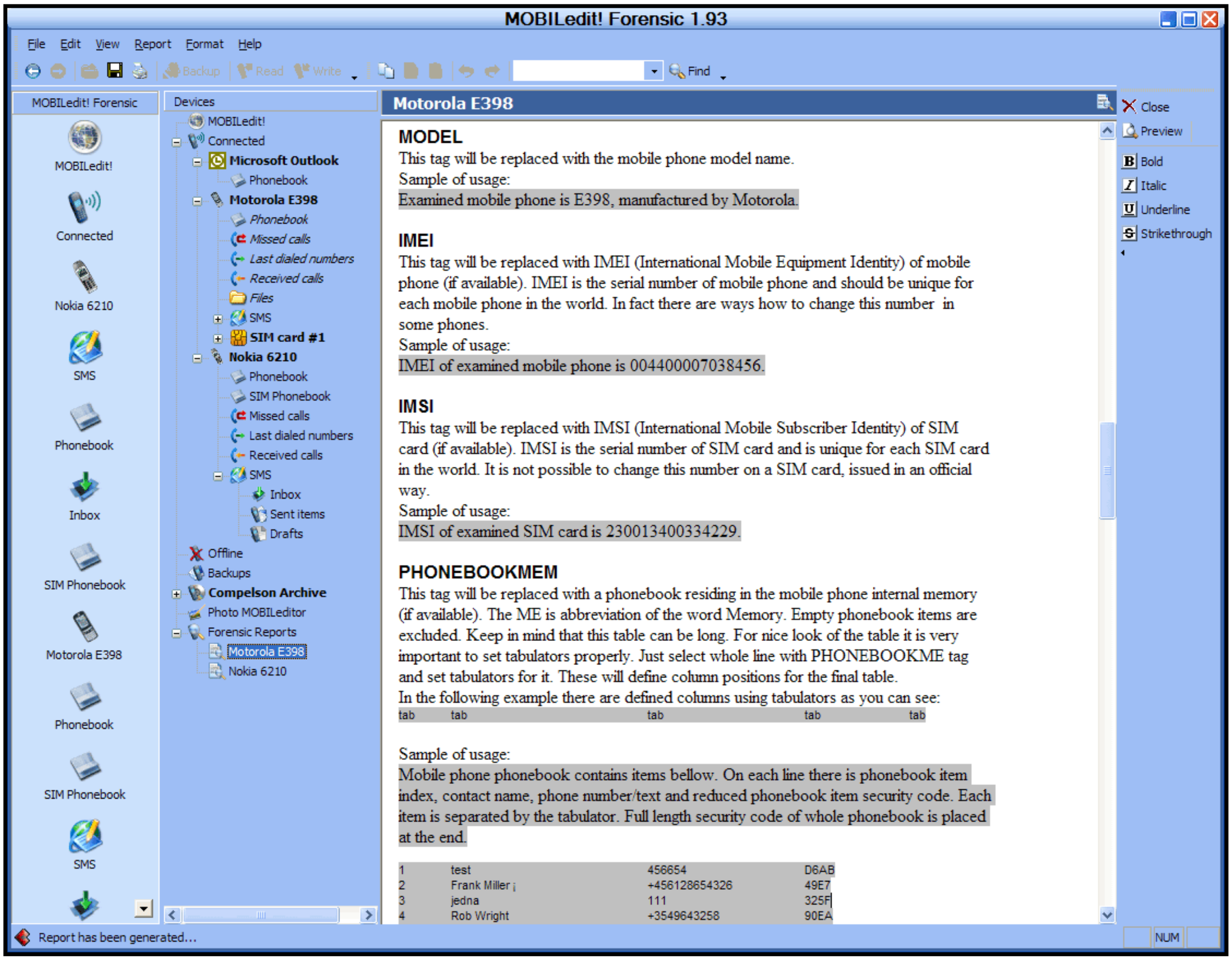
About

MOBILedit! Forensic is developed and sold commercially by COMPELSON Laboratories. The software is based upon MOBILedit!, which is designed for end users to manage their phones. The Forensics version retrieves more system and subscriber information and is designed to pull data without modifying the original contents of the phone. The program provides an intuitive GUI interface to easily generate forensics reports in a similar manner to Nessus or other GUI scanning tools. The phone can pull basic information such as call-logs, contacts, text messages, and pictures. This information is very useful for investigations for establishing relationships and timing of events. It can also obtain information direct from SIM cards. The tool is used globally by various agencies and provides built in reporting features.

Usage/Merit

MOBILedit! has a built in reporting tool, that can be customized with templates, which allows for easy formatting of information in a way that is admissible and useful in court. The reports can also be multilingual which is useful for international or cross-jurisdictional cases. Furthermore, reports can be exported into many formats. The XML export could be particularly useful to integrate with other programs or to populate databases. The program is GUI based and recent versions have an improved processing wizard. There is support for a large number of current phones, including the iPhone. From the changelog, it seems they have fairly regular updates (http://www.mobiledit.com/forensic/whatisnew.asp). The application also seems well received and they have many government and law enforcement clients. Another interesting factor is that they sell accompanying hardware, which includes the many different types of cables you might need to connect the phone to the forensics machine. The high quality support is also continued in the documentation, which was very user friendly. It seems the developers are keen to develop a very usable tool. They also provide an SDK for integration and building out the application (http://www.mobiledit.com/downloads.asp?show=me_developers).

Screenshots



MODEL
This tag will be replaced with the mobile phone model name.
Sample of usage:
Examined mobile phone is E398, manufactured by Motorola.

IMEI
This tag will be replaced with IMEI (International Mobile Equipment Identity) of mobile phone (if available). IMEI is the serial number of mobile phone and should be unique for each mobile phone in the world. In fact there are ways how to change this number in some phones.
Sample of usage:
IMEI of examined mobile phone is 004400007038456.

IMSI
This tag will be replaced with IMSI (International Mobile Subscriber Identity) of SIM card (if available). IMSI is the serial number of SIM card and is unique for each SIM card in the world. It is not possible to change this number on a SIM card, issued in an official way.
Sample of usage:
IMSI of examined SIM card is 230013400334229.

PHONEBOOKMEM
This tag will be replaced with a phonebook residing in the mobile phone internal memory (if available). The ME is abbreviation of the word Memory. Empty phonebook items are excluded. Keep in mind that this table can be long. For nice look of the table it is very important to set tabulators properly. Just select whole line with PHONEBOOKME tag and set tabulators for it. These will define column positions for the final table.
In the following example there are defined columns using tabulators as you can see:

```
tab     tab                          tab                      tab              tab
```

Sample of usage:
Mobile phone phonebook contains items bellow. On each line there is phonebook item index, contact name, phone number/text and reduced phonebook item security code. Each item is separated by the tabulator. Full length security code of whole phonebook is placed at the end.

```
1       test                         456654                   D6AB
2       Frank Miller ¡               +456128654326            49E7
3       jedna                        111                      325F
4       Rob Wright                   +3549643258              90EA
```

(More at: http://www.mobiledit.com/forensic/screenshots.asp)

Drawbacks/Liabilities

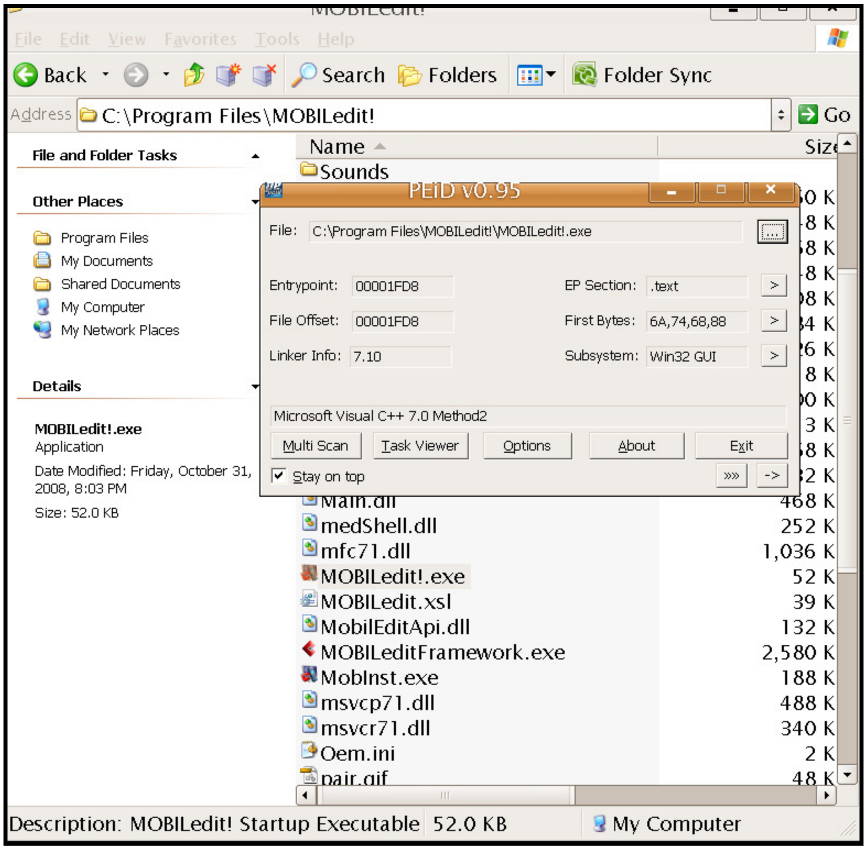
This is commercial ($600) software that does not provide the source code (though, an integration SDK is available). Because cell phone forensics deal with many vendors in an industry with no standardization, support for individual phones or phone families must manually be added, and new phone profiles are only added in major releases, not as they are debuted. Proprietary or vendor specific tools may still be required in addition to this tool. The tool also only seems to deal with available information, and does not seem to be able to recover deleted information nor does it create full images of RAM, ROM, or storage.

Methods of circumvention

An experienced user may know how to modify certain system settings that do not affect connectivity to the cell network, but that would not make sense as evidence. A smart user could delete logs and not keep a contact list; it is not clear if these logs are still stored on all devices after a user delete them.

Development Language

Using PEiD I was able to determine that it was written in Visual C++ 7.0



Address C:\Program Files\MOBILedit!

MOBILedit!.exe
Application
Date Modified: Friday, October 31, 2008, 8:03 PM
Size: 52.0 KB

File: C:\Program Files\MOBILedit!\MOBILedit!.exe

Entrypoint: 00001FD8 EP Section: .text

File Offset: 00001FD8 First Bytes: 6A,74,68,88

Linker Info: 7.10 Subsystem: Win32 GUI

Microsoft Visual C++ 7.0 Method2

☑ Stay on top

Name	Size
Sounds	
Main.dll	468 K
medShell.dll	252 K
mfc71.dll	1,036 K
MOBILedit!.exe	52 K
MOBILedit.xsl	39 K
MobilEditApi.dll	132 K
MOBILeditFramework.exe	2,580 K
MobInst.exe	188 K
msvcp71.dll	488 K
msvcr71.dll	340 K
Oem.ini	2 K
pair.gif	48 K

Description: MOBILedit! Startup Executable 52.0 KB My Computer

PEiD, displaying some interpreted details of `MOBILedit!.exe`

OS targeted / limitations

- Currently supports over 500 phone models; specific model support and drivers seem to be only through official releases.
- Support GSM/CDMA/PCS technologies.
- Symbian OS, Windows Mobilbe 2003/5.0/6.0, iPhone
- Tool runs on 32 bit windows operating systems only.

pdd

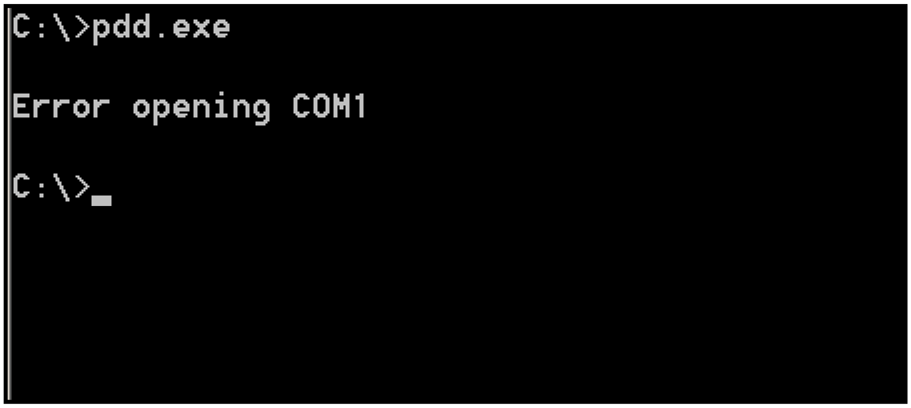
About

While pdd is not the most current tool, it is one of the few Palm OS specific tools. The application is a command line only tool that interfaces with the PDA running Palm OS using console mode (as opposed to hot-syncing). As the name implies, it is very similar to the Linux tool dd which does bit for bit copying, which guarantees that the recorded image is exactly the same as the physical evidence.

Usage/Merit

pdd may be a simple tool, but it does its job. It can copy all the memory in a very simple matter. While it has no extra built-in functionality, it is useful because the image can then be loaded into a program like EnCase or a Hex Editor. The tool is no longer maintained, but it is distributed under an open source license. The binary and source code can easily be found on the Internet. The source code could be very useful for developing new tools.

Screenshots



```
C:\>pdd.exe

Error opening COM1

C:\>_
```

(Command Line program only, no device to test upon)

Drawbacks/Liabilities

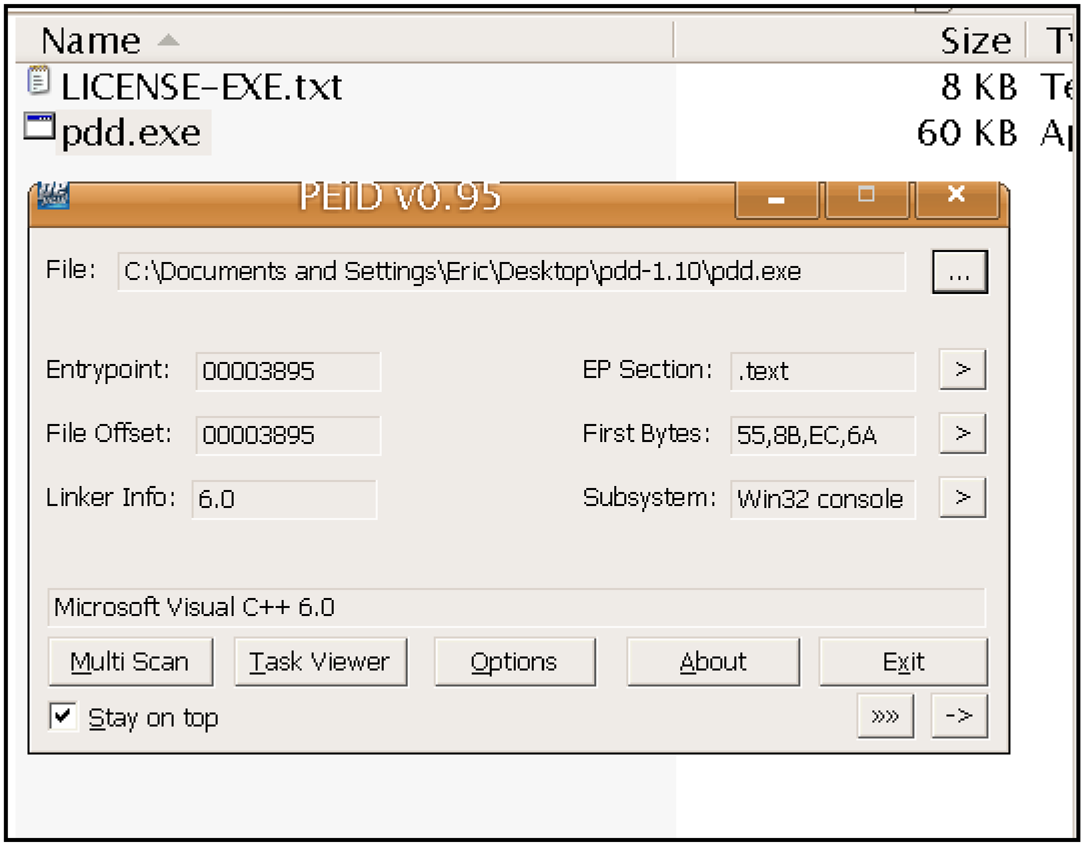
The software is open source, but is no longer maintained. The author's website redirects to Symantec, so the code may actually be used in newer product. It does not prepare reports or facilitate any of the investigation, forcing a forensic analyst to use other tools as well.

Methods of circumvention

As it is a bit-for-bit copy and the program that runs in console mode, it would be very hard to circumvent this method of obtaining an image. If it used a hot sync approach, it is possible that those binaries and libraries could be modified by a hacker and the data integrity would not be as definite.

Development Language

Using PEiD, I was able to determine that it was written in Visual C++ 6.0.



Name	Size	T
LICENSE-EXE.txt	8 KB	Te
pdd.exe	60 KB	A

PEiD v0.95

File: C:\Documents and Settings\Eric\Desktop\pdd-1.10\pdd.exe

Entrypoint: 00003895

EP Section: .text

File Offset: 00003895

First Bytes: 55,8B,EC,6A

Linker Info: 6.0

Subsystem: Win32 console

Microsoft Visual C++ 6.0

☑ Stay on top

PEiD, displaying some interpreted details of `pdd.exe`

OS targeted / limitations

- Palm OS
- Motorola DragonBall Processor

Sources

1. http://www.cellebrite.com/UFED-Standard-Kit.html
2. http://www.crownhillmobile.com/sample-report/index.html
3. http://www.crownhillmobile.com/simismobile.htm
4. http://www.mobiledit.com
5. http://www.paraben-forensics.com/catalog/product_info.php?products_id=405
6. http://www.paraben-forensics.com/cell_models.html
7. http://www.paraben-forensics.com/device-seizure.html
8. http://www.teeltech.com/tt2/simis.asp
9. http://www.waylog.it/prodotti.aspx?cat1=20