NLECTC NIJ

Criminal Justice
Electronic Crime Technology
Center of Excellence

Cellebrite UFED

Version 1.1.7.6

EVALUATION REPORT

July 2012

NIJ Electronic Crime Technology Center of Excellence
550 Marshall St., Suite B
Phillipsburg, NJ 08865
www.ECTCoE.org

NIJ ECTCOE TESTING AND EVALUATION PROJECT STAFF

Robert J. O'Leary, CFCE; DFCP
Russell Yawn, CFCE
Chester Hosmer
Mark Davis, Ph.D.
Michael Terminelli, ACE
Randy Becker, CFCE
Jacob Fonseca
Victor Fay-Wolfe, Ph.D.
Kristen McCooey, CCE; ACE
Laurie Ann O'Leary

Table of Contents

This report is current at the time of writing. Please be sure to check the vendor website for the latest version and updates.

Introduction

The National Institute of Justice (NIJ) Electronic Crime Technology Center of Excellence (ECTCoE) has been assigned the responsibility of conducting electronic crime and digital evidence tool, technology and training testing and evaluations in support of the NIJ Research, Development, Testing and Evaluation (RDT&E) process.

The National Institute of Justice RDT&E process helps ensure that NIJ's research portfolios are aligned to best address the technology needs of the criminal justice community. The rigorous process has five phases:

- **Phase I: Determine technology needs principally in partnership with the Law Enforcement and Corrections Technology Advisory Council (LECTAC) and the appropriate Technology Working Group (TWG).** NIJ identifies criminal justice practitioners' functional requirements for new tools and technologies. (For more information on LECTAC and the TWGs, visit http://www.justnet.org.)
- **Phase II: Develop technology program plans to address those needs.** NIJ creates a multiyear research program to address the needs identified in Phase I. One of the first steps is to determine whether products that meet those needs currently exist or whether they must be developed. If a solution is already available, Phases II and III are not necessary, and NIJ moves directly to demonstration, testing and evaluation in Phase IV. If solutions do not currently exist, they are solicited through annual, competitively awarded science and technology solicitations and TWG members help review the applications.
- **Phase III: Develop solutions**. Appropriate solicitations are developed and grantees are selected through an open, competitive, peer-reviewed process. After grants are awarded, the grantee and the NIJ program manager then work collaboratively to develop the solutions.
- **Phase IV: Demonstrate, test, evaluate and adopt potential solutions into practice.** A potential solution is tested to determine how well it addresses the intended functional requirement. NIJ then works with first-adopting agencies to facilitate the introduction of the solution into practice. After adoption, the solution's impact on practice is evaluated. During the testing and evaluation process, performance standards and guides are developed (as appropriate) to ensure safety and effectiveness; not all new solutions will require the publication of new standards or guides.
- **Phase V: Build capacity and conduct outreach to ensure that the new tool or technology benefits practitioners.** NIJ publishes guides and standards and provides technology assistance to second adopters.[1]

The High Priority Criminal Justice Technology Needs are organized into five functional areas:

- Protecting the Public.
- Ensuring Officer Safety.
- Confirming the Guilty and Protecting the Innocent.
- Improving the Efficiency of Justice.
- Enabling Informed Decision-Making.

The NIJ ECTCoE tool, technology and training evaluation and testing reports support the NIJ RDT&E process, which addresses high priority needs for criminal justice technology.

[1] *National Institute of Justice High-Priority Criminal Justice Technology Needs,* March 2009 NCJ 225375.

Overview

With the world becoming more mobile every day, law enforcement encounters more cellphones and mobile devices in their investigations. Many tools exist on the market to process these mobile devices, but every tool does not support every device.

Cellebrite's Universal Forensics Extraction Device (UFED) is a hardware-based platform that supports extraction of data from more than 4,000 phones and devices. The hardware is available in both standard and ruggedized versions. The ruggedized version is designed for field use by military, law enforcement and government agencies, and the standard version for office and lab use. Along with the standard hardware, Cellebrite offers an upgrade package called Physical Pro, which is designed to perform physical memory dumps and file system extractions from supported devices.

Product Information

The following information is from Cellebrite's website:

> The Cellebrite UFED forensics system is the ultimate standalone mobile forensic device, ready for use out in the field or in the lab.
>
> The UFED system extracts vital information from 95 percent of all cellular phones on the market today, including smartphones and PDA devices (Palm OS, Microsoft, Blackberry, Symbian, iPhone and Google Android). Simple to use even in the field, with no PC required, the UFED can easily store hundreds of phonebooks and content items onto an SD card or USB flash drive.
>
> Cellebrite UFED supports all known cellular device interfaces, including serial, USB, infrared and Bluetooth. Extractions can then be brought back to the forensic lab for review and verification using the reporting/analysis tool. Cellebrite works exclusively with most major carriers worldwide, including Verizon Wireless, AT&T, Sprint/Nextel, T-Mobile, Rogers Wireless-Canada, Orange France and Telstra Australia, as well as 140 others. This ensures that future devices are supported prior to retail launch.

Product Description

The following information is from the UFED manual:

> The Cellebrite UFED forensics system empowers law enforcement, antiterror and security organizations to capture critical forensic evidence from mobile phones, smartphones and PDAs.
>
> UFED extracts vital data such as phonebook, camera pictures, videos, audio, text messages (SMS), call logs, ESN IMEI, ICCID and IMSI information from over 1,600 handset models, including Symbian, Microsoft Mobile, Blackberry and Palm OS devices.
>
> Cellebrite UFED enables SIM ID cloning, allowing you to extract phone data while preventing the cellular device from connecting to the network.
>
> The UFED can extract data from a phone, or directly from the SIM card. When extracting from a phone, the UFED connects to the phone via cable, Bluetooth or infrared, and the data is read logically from the phone. It also performs a physical extraction from SIM cards, allowing extraction of additional data such as deleted SMS, ICCID, IMSI, location information and more.
>
> Data is copied to any standard USB flash drive or SD card and is then organized into clear and concise reports.

Data can also be copied directly to a computer via the UFED Physical Analyzer interface, as is indicated in the Test Bed Configuration section on page 5.

Cellebrite's industry expertise provides reliability and ease-of-use, and ensures the broadest support for handset varieties, including updates for newly released models even before they are available in the market.

Portable and easy to operate, the UFED can be used in the forensic lab as well as in the field. The UFED is a handheld device, without the need for a PC in the field. The ruggedized version comes with a hard-sided case and battery power for even greater mobility and flexibility, and is fully loaded with all needed accessories.

The UFED Report Manager software on your PC creates detailed reports of the extracted data that can be used as evidence. Reports include full extraction details, as well as MD5 hash information that proves that the data is original and untouched.

Special Features

The following features are from Cellebrite's website:

- The UFED allows you to extract a wide variety of data types, including:
  - Contacts.
  - SMS text messages.
  - Deleted text messages (SIM/USIM).
  - Call history (Received, Dialed, Missed).
  - Audio.
  - Video.
  - Pictures and images.
  - Ringtones.
  - Phone details (IMEI / ESN, phone number).
- The Cellebrite UFED system comes complete with a user-friendly PC reporting and analysis software application. Easy-to-analyze report logs can be generated in HTML, XLS, CSV and XML formats, providing organized printouts for use as a reference and in the courtroom.

Target Customers

The target customers for the UFED are state and local law enforcement organizations that have an interest in the forensic examination of cellphones. The UFED is a forensic acquisition tool that provides reports in an easy-to-read format.

Law Enforcement Applications

Cellebrite's UFED is designed to assist state and local law enforcement with the acquisition of, and reporting on, both logical and physical examinations of mobile devices such as cellphones, PDAs and GPS device.

Test Bed Configuration

The UFED is a hardware device that can be used standalone (without a computer) to perform data extraction. However, in order to view any HTML reports, a target device (thumb drive, SD card, etc.) must be connected to a computer. Software applications developed by Cellebrite allow capturing the acquisition directly to a computer; this is the method used in this testing.

The test machine is a Dell OptiPlex 760 with a clean Windows 7 x64 installation, 4GB of RAM, and a 2.66 GHz Intel Core 2 Duo processor. Installed on this machine were Cellebrite's UFED Report Manager (v 1.8.3.171110) and UFED Physical Analyzer (v 2.2.0.8966). Report Manager is used to perform logical acquisitions and Physical Analyzer is used for physical acquisitions.

Configuration of UFED

The software installers were downloaded for UFED Report Manager and UFED Physical Analyzer from Cellebrite's website. Once downloaded, the setup files were executed and the installer prompts were stepped through.

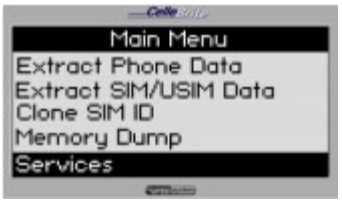
In order to connect the UFED to a workstation, the UFED Physical Analyzer software needs to register the device to the PC. The software supports two methods of activation: a hardware license key or an activation code provided by the UFED. The configuration of the UFED was performed using the following steps:

1. Opened Physical Analyzer. Since this was the first time the software was run, an activation window loaded automatically.
2. Performed activation according to the user manual using the activation code provided by the UFED device.

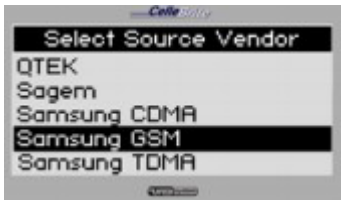
Evaluation and Testing of Cellebrite UFED

The UFED interface is three separate parts; a hardware device and two software programs. The UFED hardware device initiates a connection to a mobile device to extract information. For each of the tests below, the following general steps were followed for data extraction:

1. When starting the device, a screen is presented to select the type of extraction.



2. Once an extraction type is selected, a mobile device vendor and model selection screen is displayed.



3. A memory source selection screen is displayed.

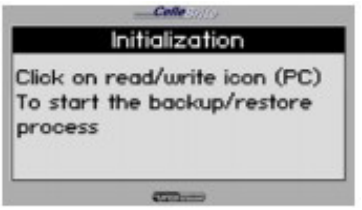
4. The UFED will ask for the connection method to be used for the extraction.

5. Next, the target for the extraction results will be selected. Extraction to the USB device or SD card will create a report in HTML and PDF formats on the target media. Extraction to the PC will export the results to either software, UFED Report Manager or Physical Analyzer.

6. The next screen allows for the selection of content type to be extracted.

7. The UFED will provide instructions depending on the connection type selected. Instructions for connecting the UFED to a PC are shown in the screenshot.

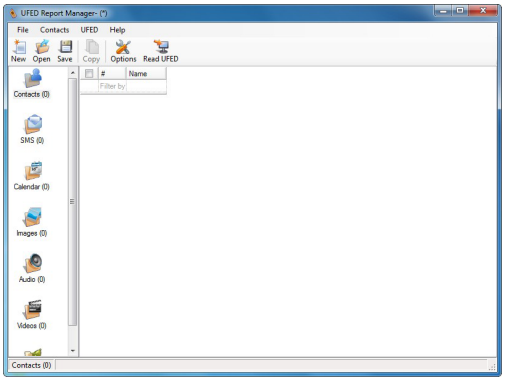
8. At this point, if exporting to USB or SD devices, the UFED will request that the target drive is connected. If using a PC connection, the UFED will request that the read icon in the PC application is clicked. A progress window is displayed.



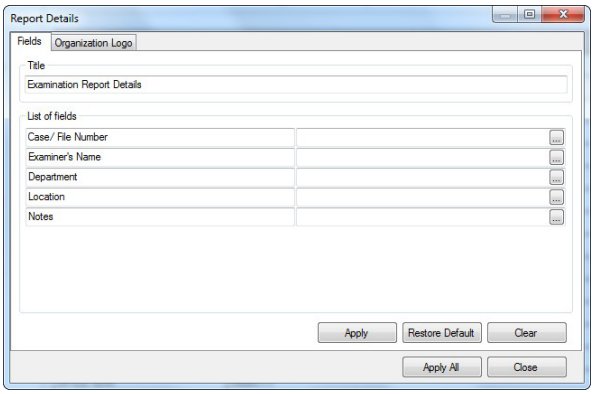
9. Upon completion, the UFED displayed a confirmation screen.

If an SD card or USB drive was used to store the results of the acquisition, the reports can be viewed by connecting the external media to a PC. If the target of the acquisition was a PC, the acquisition can be further analyzed by using one of the two pieces of software. Analysis of logical extractions can be performed using UFED's Report Manager. File system or physical memory extractions can be analyzed with UFED's Physical Analyzer.

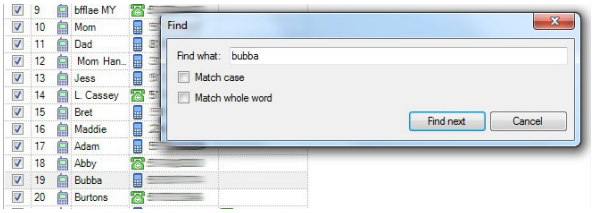
Report Manager's user interface consists of three panes. The left pane allows the user to select which information will be displayed in the right pane. The final pane of the interface is the top icon bar that provides quick access to common features of the tool.



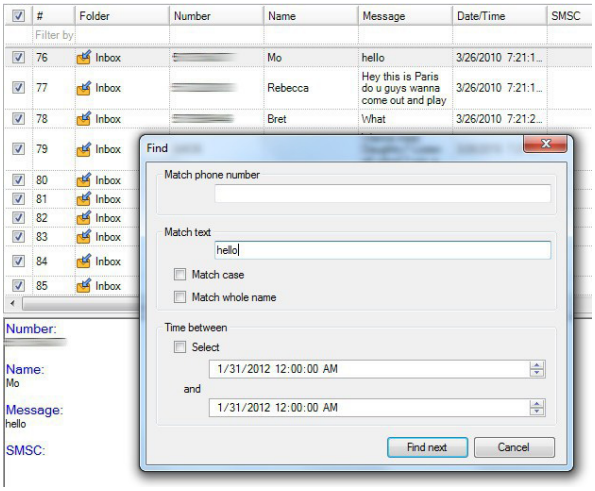
Following the extraction of a device with a target destination of PC, the interface displays the Report tab to the user. The report can also be exported from Report Manager in several different formats. Useful information can be added to the report through the Report Details menu, which is accessed with the top icon bar or through the application's menu items.



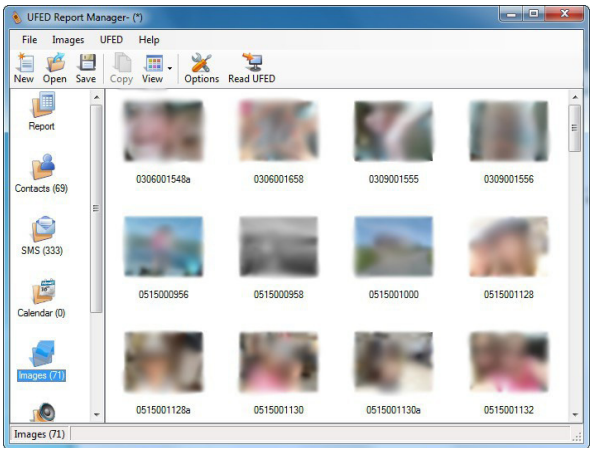
The application allows the user to search through contacts, SMS and calendar events. Name or phone number with a simple search dialog can search contacts.



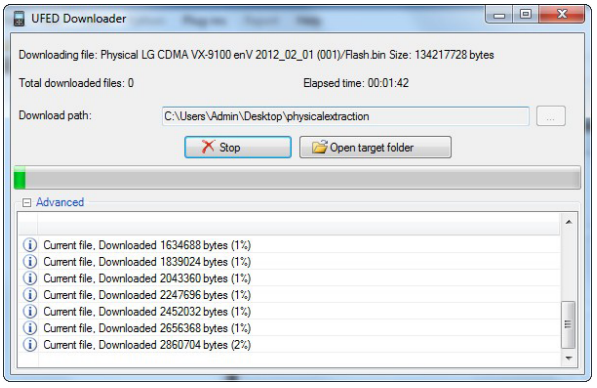
SMS messages can be searched using phone number, text matching or a particular timeframe.



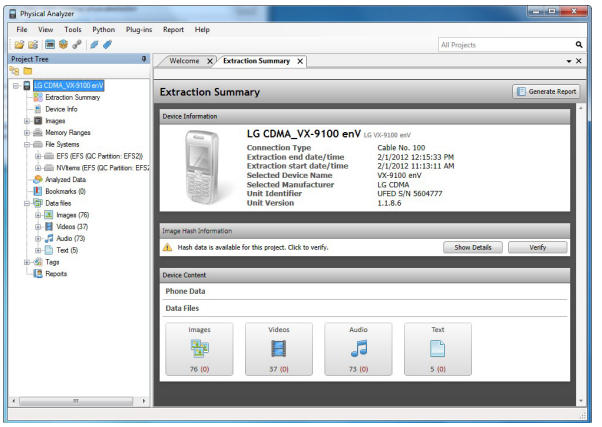
Images discovered on the device can be displayed and exported by selecting 'Images' from the left pane.



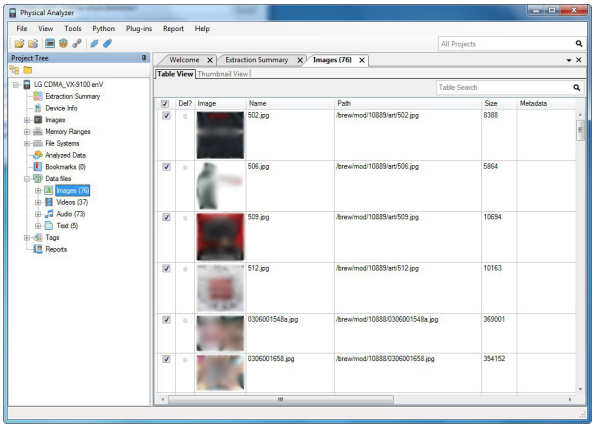
The second piece of software supporting the UFED is the Physical Analyzer. Physical Analyzer takes the input from the UFED device of a physical or file system dump. The interface is the same for both types of extractions, but the amount of information will vary. During extraction, the interface displays a progress window with statistics on the files that are being transferred from the UFED to the PC.



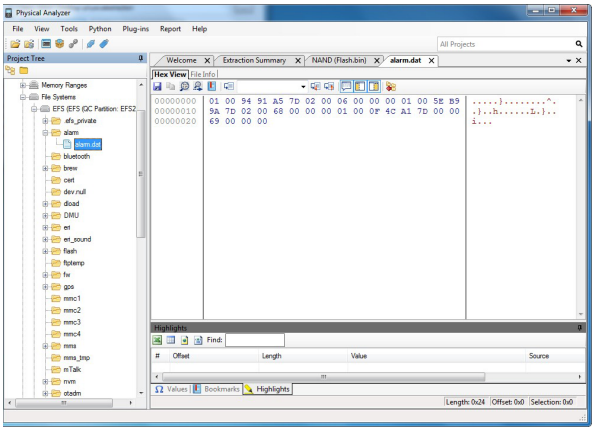
When the extraction is complete, a summary of the extraction is displayed.



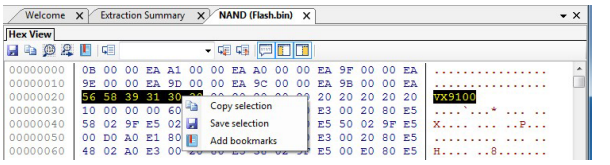
Much like the Report Manager, Physical Analyzer has the capability to display data files such as images, videos, audio and text. These are also related to the file system where possible.



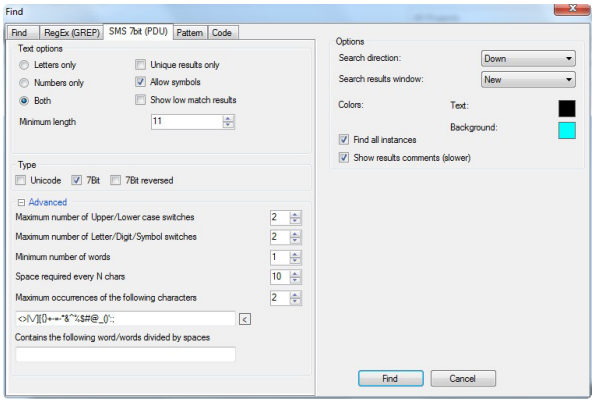
Physical Analyzer allows the user to traverse the file system and view with a familiar tree structure.



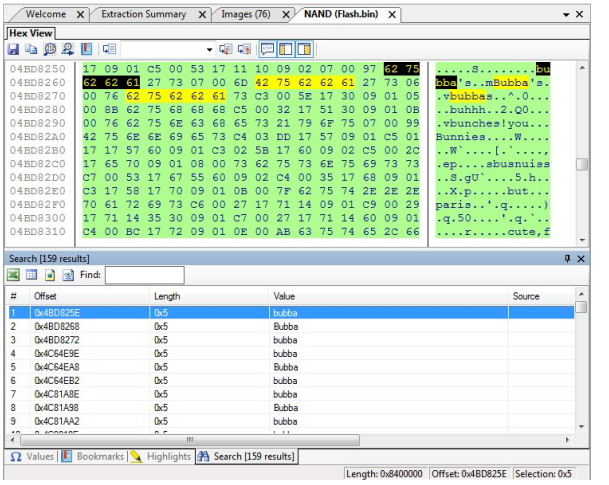
Information can be highlighted, bookmarked or copied to the clipboard.



Bookmarked data is highlighted in red by default. The bookmarks tab displays a list and provides the capability to organize the bookmarks. Bookmarks can be rearranged or deleted. Data cannot be browsed within the bookmarks tab. The search tool can be used to find particular information.



The results of the search are presented in a list and highlighted.



Once all of the information has been processed and reviewed, a report can be generated in several formats. Reports can be customized using the application's settings to edit field names or add new fields to the report. These reports can also be customized with formatted text header and a logo.

Test 1: LG VX-9900

This test was performed to determine how well the UFED acquires data from an LG VX-9900.

Prior to starting the test, the phone's battery was fully charged and the phone was powered on.

Logical Extraction

The following steps were performed to extract logical data:

1. Powered on the UFED device and selected Extract Data from the menu.
2. Selected LG CDMA from the Source Vendor menu and pressed OK.
3. Selected VX-9900 enV from the Source Model menu and pressed OK.
4. Checked Phone (Phonebook) and Phone (Content) from the Source Memory menu and pressed the right arrow to continue. Memory Card (Content) was not checked because there was no memory card present.
5. Selected PC as the Target.
6. Checked all options, including Call Logs, Phonebook, SMS, Pictures, Videos and Audio/Music from the Content Types menu and hit the right arrow to continue.
7. Connected the phone to the UFED with cable 93/113 as instructed by the UFED and pressed the right arrow to Start.
8. When the extraction was completed, the UFED Report Manager application was opened and the Read UFED button was clicked to download the report to the computer.

Results of Logical Extraction

The UFED found three phonebook contacts, 90 incoming calls, 90 outgoing calls, 90 missed calls, zero SMS messages, 43 images, eight videos and zero audio files. The results match the data found when manually examining the phone.

File System

The following steps were performed to dump the file system:

1. Selected File System Dump from the UFED main menu and pressed OK.
2. Selected LG CDMA from the Source Vendor menu and pressed OK.
3. Selected VX-9900 enV from the Source Model menu and pressed OK.
4. Selected Normal EFS as the mode and pressed OK.
5. Selected PC as the Target.
6. Connected the phone to the UFED with cable 93/113 as instructed by the UFED and pressed the right arrow to Start.
7. Opened the Physical Analyzer application, clicked the Read Data from UFED button, selected the download path, and pressed start to begin the file system extraction.

Results of File System Dump

The file system dump was successful and can be examined within Physical Analyzer.

Physical Dump

The following steps were performed to obtain a physical dump:

1. Selected Physical Dump from the UFED main menu and pressed OK.
2. Selected LG CDMA from the Source Vendor menu and pressed OK.
3. Selected VX-9900 enV from the Source Model menu and pressed OK.

4. Selected PC as the Target.
5. Connected the phone to the UFED with cable 93/113 as instructed by the UFED and pressed the right arrow to Start.
6. Opened the Physical Analyzer application, clicked the Read Data from UFED button, selected the download path, and pressed start to begin the physical dump.

Results of Physical Dump

The physical dump was completed successfully and an image of the phone's flash memory was created.

Extract Passwords

The following steps were performed to extract passwords:

1. Selected Extract Passwords from the UFED main menu and pressed OK.
2. Selected LG CDMA from the Source Vendor menu and pressed OK.
3. Selected VX-9900 enV from the Source Model menu and pressed OK.
4. Selected Display Only as the target.
5. Connected the phone to the UFED with cable 93/113 as instructed by the UFED and pressed the right arrow to Start.

Results of Password Extraction

The user code, ESN/MEID, phone number and MIN were extracted successfully.

Test 2: Motorola V3M

This test was performed to determine how well the UFED acquires data from a Motorola V3M.

Prior to starting the test, the phone's battery was fully charged and the phone was powered on.

Logical Data

The following steps were performed to extract logical data:

1. Powered on UFED device and selected Extract Phone Data from the main menu.
2. Selected Motorola CDMA from the Source Vendor menu and pressed OK.
3. Selected V3m RAZR from the Source Model menu and pressed OK.
4. Checked Phone (Phonebook) and Phone (Content) from the Source Memory menu and pressed the right arrow to continue. Note: Memory Card (Content) was not checked since a memory card was not present.
5. Selected PC as the Target.
6. Checked off all options including Call Logs, Phonebook, SMS, Pictures and Video from the Content Types menu and hit the right arrow to continue.
7. Connected the phone to the UFED with cable 80 as instructed by the UFED and pressed the right arrow to Start.
8. When the extraction was completed, the UFED Report Manager application was opened and the Read UFED button was clicked to download the report to the computer.

Results of Logical Extraction

The UFED found one contact, one sent SMS, four outgoing calls, 31 images and one video. The results match the data found when manually examining the phone.

File System

The following steps were performed to dump the file system:

1. Selected File System Dump from the UFED main menu and pressed OK.

2. Selected Motorola CDMA from the Source Vendor menu and pressed OK.
3. Selected V3m RAZR from the Source Model menu and pressed OK.
4. Selected PC as the Target.
5. Connected the phone to the UFED with cable 80 as instructed by the UFED and pressed the right arrow to Start.
6. Opened the Physical Analyzer application, clicked the Read Data from UFED button, selected the download path, and pressed start to begin the file system extraction.

Results of File System Dump

The file system dump completed successfully, although Physical Analyzer could not decode the extracted data.

Extract Passwords

The following steps were performed to extract passwords:

1. Selected Extract Passwords from the UFED main menu and pressed OK.
2. Selected Motorola CDMA from the Source Vendor menu and pressed OK.
3. Selected V3m RAZR from the Source Model menu and pressed OK.
4. Selected Display Only as the target.
5. Connected the phone to the UFED with cable 80 as instructed by the UFED and pressed the right arrow to Start.

Results of Password Extraction

The user code and the security code were extracted successfully.

Test 3: Nokia 2610

This test was performed to determine how well the UFED acquires data from a Nokia 2610.

Prior to starting the test, the phone's battery was fully charged and the phone was powered on.

Logical Data

The following steps were performed to extract logical data:

1. Powered on UFED device and selected Extract Phone Data from the UFED main menu and pressed OK.
2. Selected Nokia GSM from the Source Vendor menu and pressed OK.
3. Selected 2610/2626 from the Source Model menu and pressed OK.
4. Checked Phone from the Source Memory menu and hit Next. SIM was not checked because the phone did not contain a SIM card.
5. Selected PC as the Target.
6. Checked all options including Call Logs, Phonebook, SMS, Calendar, Ringtones and Audio/Music from the Content Types menu and hit the right arrow to continue.
7. Connected the phone to the UFED with cable 53 as instructed by the UFED and pressed the right arrow to Start.
8. When the extraction was completed, the UFED Report Manager application was opened and the Read UFED button was clicked to download the report to the computer.

Results of Logical Extraction

The UFED found one phonebook contact, 12 received SMS messages, one calendar event, one outgoing call, eight audio files and 11 ringtones. The results match the data found when manually examining the

phone. The phonebook could not be verified because it could not be accessed without a SIM card in the phone. A cloned SIM card could alleviate some of these issues.

File System

The following steps were performed to dump the file system:

1. Selected File System Dump from the UFED main menu and pressed OK.
2. Selected Nokia GSM from the Source Vendor menu and pressed OK.
3. Selected 2610 from the Source Model menu and pressed OK.
4. Selected PC as the Target.
5. Connected the phone to the UFED with cable 53 as instructed by the UFED and pressed the right arrow to Start.
6. Opened the Physical Analyzer application, clicked the Read Data from UFED button, selected the download path, and pressed start to begin the file system extraction.

Results of File System Dump

The file system dump was successful and can be examined within Physical Analyzer.

Test 4: Motorola V3xx

This test was performed to determine how well the UFED acquires data from a Motorola V3xx.

Prior to starting the test, the phone's battery was fully charged and the phone was powered on.

Logical Data

The following steps were performed to extract logical data:

1. Powered on UFED device and selected Extract Phone Data from the UFED main menu and pressed OK.
2. Selected Motorola GSM from the Source Vendor menu and pressed OK.
3. Selected V3xx from the Source Model menu and pressed OK.
4. Checked Phone (Phonebook), Phone (Content) and Memory Card (Content). Note: There was a 4 GB SanDisk micro SD card included with the phone.
5. Selected PC as the Target.
6. Checked all options, including Call Logs, Phonebook, SMS, Calendar, Pictures, Videos, Ringtones and Audio/Music from the Content Types menu and hit the right arrow to continue.
7. Connected the phone to the UFED with cable 80 as instructed by the UFED and pressed the right arrow to Start.
8. Instructions for changing the phone's connectivity settings appeared on the UFED, but the phone's menu could not be accessed because there was no SIM card.
9. The phone book read failed. After retrying it several times without success, the F3 button was pressed to skip that step.
10. The calendar read failed. After retrying it several times without success, the F3 button was pressed to skip that step.
11. When the extraction was completed, the UFED Report Manager application was opened and the Read UFED button was clicked to download the report to the computer.

Results of Logical Extraction

The UFED found zero SMS messages, 230 images, zero videos, zero ringtones, and two audio files. The results could not be verified because the phone menus

could not be accessed without a SIM card. The UFED failed to read the phonebook and calendar. This is likely because the phone did not have a SIM card.

File System

The following steps were performed to dump the file system:

1. Selected File System Dump from the UFED main menu and pressed OK.
2. Selected Motorola GSM from the Source Vendor menu and pressed OK.
3 Selected V3xx from the Source Model menu and pressed OK.
4. Selected PC as the Target.
5. Connected the phone to the UFED with cable 80 as instructed by the UFED and pressed the right arrow to Start.
6. Opened the Physical Analyzer application, clicked the Read Data from UFED button, selected the download path, and pressed start to begin the file system extraction.

Results of File System Dump

The file system dump was successful and can be examined within Physical Analyzer.

Physical Dump

The following steps were performed to obtain a physical dump:

1. Selected File System Dump from the UFED main menu and pressed OK.
2. Selected Motorola GSM from the Source Vendor menu and pressed OK.
3. Selected V3xx from the Source Model menu and pressed OK.
4. Selected PC as the Target.
5. Connected the phone to the UFED with cable 80 as instructed by the UFED and pressed the right arrow to Start.
6. Instructions for changing the phone's connectivity settings appeared on the UFED, but the phone's menu could not be accessed because there was no SIM card.
7. Opened the Physical Analyzer application, clicked the Read Data from UFED button, selected the download path, and pressed start to begin the file system extraction.
8. Received error that said that a connection could not be made to the phone. Attempted to retry several times without success and eventually pressed the left arrow to abort the process.

Results of Physical Dump

A connection could not be established to perform a physical dump. It is likely the connection could not be made because the phone was lacking a SIM card. It is likely that these shortcomings could be alleviated with the use of a cloned 'dummy' SIM card.

Test 5: LG C729 Double Play

This test was performed to determine how well the UFED acquires data from an LG C729. The device is running the Android Operating System, version 2.3.4.

Prior to starting the test, the phone's battery was fully charged and the phone was powered on.

The following steps were performed to extract logical data:

1. Powered on UFED device and selected Extract Phone Data from the UFED main menu and pressed OK.
2. Selected LG GSM from the Source Vendor menu and pressed OK.
3. Selected C729 Double Play (Android) from the Source Model menu and pressed OK.

4. Checked off Phone and Memory Card from the Source Memory menu and hit Next.
5. Selected PC as the Target.
6. Checked off all options including Call Logs, Phonebook, SMS, Calendar, MMS, Pictures, Videos, Ringtones and Audio/Music from the Content Types menu and hit the right arrow to continue.
7. Connected the phone to the UFED with cable 100 as instructed by the UFED and pressed the right arrow to Start.
8. When the extraction was completed, the UFED Report Manager application was opened and the Read UFED button was clicked to download the report to the computer.

Result of Logical Extraction

The UFED found 87 phonebook contacts, 44 calendar events and 78 entries in the call log, including 26 outgoing, 36 incoming and 16 missed calls. In addition, one ringtone, 193 pictures and 20 audio files were extracted. The results match the data found when manually examining the phone, with the exception of SMS extraction causing an error. No SMS messages were able to be written to the PC after reading them from the device.

File System

The following steps were performed to extract the file system:

1. Selected File System Extraction from the UFED main menu and pressed OK.
2. Selected LG GSM from the Source Vendor menu and pressed OK.
3. Selected C729 Double Play (Android) from the Source Model menu and pressed OK.
4. Selected PC as the Target.
5. Connected the phone to the UFED with cable 100 as instructed by the UFED and pressed the right arrow to Start.
6. Opened the Physical Analyzer application, clicked the Read Data from UFED button, selected the download path, and pressed start to begin the file system extraction.

Result of File System Extraction

The file system extraction was successful and can be examined within Physical Analyzer.

Physical Memory

The following steps were performed to extract the physical memory:

1. Selected Physical Extraction from the UFED main menu and pressed OK.
2. Selected LG GSM from the Source Vendor menu and pressed OK.
3. Selected C729 Double Play (Android) from the Source Model menu and pressed OK.
4. Selected PC as the Target.
5. Connected the phone to the UFED with cable 100 as instructed by the UFED and pressed the right arrow to Start.
6. Opened the Physical Analyzer application, clicked the Read Data from UFED button, selected the download path, and pressed start to begin the extraction.

Result of the Physical Extraction

The physical extraction was successful and can be examined within Physical Analyzer.

Test 6: Apple iPhone 4S

This test was performed to determine how well the UFED acquires data from an iPhone 4S.

Prior to starting the test, the phone's battery was fully charged and the phone was powered on.

The following steps were performed to extract logical data:

1. Powered on UFED device and select Extract Phone Data from the UFED main menu and pressed OK.
2. Selected Apple from the Source Vendor menu and pressed OK.
3. Selected iPhone 4/4S GSM from the Source Model menu and pressed OK.
4. Checked off Phone from the Source Memory menu and hit Next. The SIM card was not extracted in this test.
5. Selected PC as the Target.
6. Checked off all options, including Call Logs, Phonebook, SMS, MMS, Ringtones, Videos and Audio/Music from the Content Types menu and hit the right arrow to continue.
7. Connected the phone to the UFED with cable 110 as instructed by the UFED and pressed the right arrow to Start.
8. When the extraction was completed, the UFED Report Manager application was opened and the Read UFED button was clicked to download the report to the computer.

Result of Logical Extraction

The UFED found 107 phonebook contacts, 2,717 SMS messages and 100 entries in the call log, including 60 outgoing, 26 incoming and 14 missed calls. In addition, 41 ringtones, 242 pictures and 16 videos were extracted. The results match the data found when manually examining the phone, with the exception of audio file extraction causing an error. There were 41 songs listed in the phone according to manual examination.

File System

The following steps were performed to extract the file system:

1. Selected File System Extraction from the UFED main menu and pressed OK.
2. Selected Apple from the Source Vendor menu and pressed OK.
3. Selected iPhone 4S from the Source Model menu and pressed OK.
4. Selected PC as the Target.
5. Connected the phone to the UFED with cable 110 as instructed by the UFED and pressed the right arrow to start.
6. Opened the Physical Analyzer application, clicked the Read Data from UFED button, selected the download path, and pressed start to begin the file system extraction.

Results

The file system extraction was successful and can be examined within Physical Analyzer.

Test 7: Apple iPhone 3GS

This test was performed to determine how well the UFED acquires data from an iPhone 3GS. Prior to starting the test, the phone's battery was fully charged and the phone was powered on.

The following steps were performed to extract logical data:

1. Powered on UFED device and selected Extract Phone Data from the UFED main menu and pressed OK.
2. Selected Apple from the Source Vendor menu and pressed OK.
3. Selected iPhone 4/4S GSM from the Source Model menu and pressed OK.
4. Checked off Phone from the Source Memory menu and hit Next. SIM card was not extracted in this test.
5. Selected PC as the Target.

6. Checked off all options including Call Logs, Phonebook, SMS, MMS, Ringtones, Videos and Audio/ Music from the Content Types menu and hit the right arrow to continue.
7. Connected the phone to the UFED with cable 110 as instructed by the UFED and pressed the right arrow to Start.
8. When the extraction was completed, the UFED Report Manager application was opened and the Read UFED button was clicked to download the report to the computer.

Result of Logical Extraction

The UFED found 85 phonebook contacts, 1,606 SMS messages and 107 entries in the call log, including 32 outgoing, 53 incoming and 22 missed calls. In addition, 775 pictures and three videos were extracted and four voicemails. There were 2,259 songs listed in the phone, according to manual examination.

The results match the data found when manually examining the phone.

File System Extraction

The following steps were performed to extract the file system:

1. Selected File System Extraction from the UFED main menu and pressed OK.
2. Selected Apple from the Source Vendor menu and pressed OK.
3. Selected iPhone 4S from the Source Model menu and pressed OK.
4. Selected PC as the Target.
5. Connected the phone to the UFED with cable 110 as instructed by the UFED and pressed the right arrow to start.
6. Opened the Physical Analyzer application, clicked the Read Data from UFED button, selected the download path, and pressed start to begin the file system extraction.

Results of File System Extraction

The file system extraction was successful and the resultant data was examined within Physical Analyzer. The results were the same as the logical extraction.

Conclusion

Cellebrite's UFED performed consistently well during the testing. Connectivity issues between the UFED and phones tested were rare. In these tests, the UFED only had difficulty connecting to certain GSM phones that did not contain a SIM card, and these issues most likely could be remedied by creating a cloned SIM card.

The UFED's physical interface is simple to use and it is easy to select certain information to extract from a phone. The user interface of the software is presented well, allowing quick discovery of desired information. Searching is implemented well in both software tools, providing the ability to search for information relevant to an investigation. Cellebrite's Report Manager customizes the search dialog box for the appropriate fields based within the current view. However, the Report Manager does not provide the capability to search the entire extraction for a particular string. The Physical Analyzer provides additional search capabilities not found in the Report Manager.

The physical device and the two software applications do an excellent job of extracting and interpreting the data. In order to maintain maximum operational capability, users will have to keep both software packages and the UFED up to date. The combination of a physical device and software applications have proven to work together to successfully complete investigations.