UFED Physical Analyzer 2.0

USER MANUAL

mosira

cellebrite
mobile data secured

UFED system

LEGAL NOTICES

This manual is delivered subject to the following conditions and restrictions:

- This document contains proprietary information belonging to Cellebrite Ltd. Such information is supplied solely for the purpose of explicitly assisting authorized users of the Universal Forensic Extraction Device (UFED) System, and its associated components.
- No part of the content of this document may be used for any other purpose, disclosed to any person, or firm, reproduced by any means, electronic or mechanical, without the express prior written permission of Cellebrite Ltd.
- The text and graphics are for the purpose of illustration and reference only. The specifications and documented procedures on which they are based are subject to change without notice.
- Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.

CAUTION: To avoid damage to the UFED, it should be used only with the dedicated AC/DC adapter supplied with this device.

CAUTION: To avoid damage to the UFED, USB, Ethernet and target and source connectors should be connected only to CE approved devices (according to IEC/EN 60065 standard).

WARNING: To avoid possible harm, make sure that all external connections to other devices (excluding the power adapter) are only indoor and SELV (safety extra low voltage, not exceeding 42.4 V peak or 60 VDC).

Contents

Chapter 1: Introduction......................................1

1.1 Overview...1

1.2 Physical Memory Extraction..1

1.3 Data Analysis 2

Chapter 2: Installation and Activation.............4

2.1 Introduction..4

2.2 Activating the UFED Physical Extraction Module.....4

2.2.1 Renewing the UFED Physical Extraction Module License....................................5

2.2.2 UFED Software Upgrade..9

2.3 Installing the UFED Physical Analyzer Application ..9

2.3.1 System Requirements...9

2.3.2 Software Installation...10

2.4 Activating the Physical Analyzer application 12

2.4.1 Using an Activation Code 12

2.4.2 Using a Hardware License Key..........................16

2.5 Deactivating a UFED Physical Analyzer License 17

Chapter 3: Performing Data Extraction.........19

3.1 Performing a Physical Dump..19

3.1.1 Using Removable Media......................................20

3.1.2 Extracting Data Directly to Your PC................21

3.2 Extracting the File System...23

3.3 Extracting Passwords...23

Chapter 4: Overview of UFED Physical Analyzer Application 25

4.1 Introduction..25

4.2 Launching UFED Physical Analyzer Application.....25

4.3 Application Structure Overview......................................26

4.3.1 Application Menu 27

4.3.2 Application Toolbar...30

4.3.3 Project Tree Area 31

4.3.4 Data Display Area 42

Chapter 5: Physical Analyzer - Basic Use 48

5.1 Opening File for Analysis 48

5.2 Searching for Information in the Project....50

5.2.1 The Quick Results List 50

5.2.2 The Results Tab 51

5.3 Browsing the Hex Dump 52

5.4 Browsing the File System....53

5.5 Browsing the Analyzed Data 55

5.5.1 Analyzed Data 55

5.5.2 Data Files....55

5.6 Generating Reports....57

Chapter 6: Physical Analyzer - Advanced Use....61

6.1 Using the Advanced Opening Feature 61

6.1.1 Advanced Opening of a UFED Extraction File 62

6.1.2 Advanced Opening of a non-UFED Extraction File 67

6.1.3 Saving a UFD File....69

6.2 Hash Verification....70

6.3 Searching for Information in the Hex Dump and Parsed Data....71

6.3.1 Search Modes 71

6.3.2 Search Results....72

6.3.3 Strings Search 73

6.3.4 Bytes Search....74

6.3.5 Dates Search....75

6.3.6 SIM ICCID Numbers Search 76

6.3.7 SMS Numbers Search 77

6.3.8 Regular Expression (GREP) Search 78

6.3.9 SMS Text Search....79

6.3.10 Pattern Search 80

6.3.11 Code Search....81

6.4 Working with Data Files....82

6.4.1 Accessing Data Files 82

6.4.2 Data File Pointers....82

6.4.3 Data Display Modes 83
6.4.4 Redirecting the Offset 86
6.4.5 Bookmarks 87
6.4.6 Values tab 89
6.4.7 Highlights tab 90
6.4.8 Information Frame 90
6.5 Chains 91
6.5.1 Managing Chains 91
6.6 Plug-ins 97
6.6.1 Managing Plug-ins 97
6.6.2 Running a Specific Plug-in 98
6.6.3 Getting Plug-ins 98
6.7 Using the Python Shell 100
6.8 Exporting the File System 100

Chapter 7: General settings 101
7.1 General Settings 101
7.2 Data Files Settings 102
7.2.1 Data Files Filtering Methods 103
7.2.2 Managing Data Files Settings 104
7.3 Hex Viewer Settings 106
7.4 Models Settings 107
7.5 Report Settings 108
7.5.1 Additional Report Fields 108
7.5.2 Report Defaults 110

Appendix A: Using Python in the Physical Analyzer 112
1.1 Accessing the data store 112
1.2 File Systems, Files and Directories 112
1.2.1 Listing the current file systems 112
1.2.2 Get a specific file system by name 113
1.2.3 Go over all files in a file system (recursively) 113
1.2.4 Get a specific file by path 114
1.2.5 Print some information about the file 114
1.2.6 List all files in a directory 115
1.2.7 Searching for files with a regular expression 115
1.2.8 Find out if a node is a file or a directory 116

1.2.9 Reading data from a file 116
1.2.10 Viewing data in a textual hex dump 117
1.2.11 Creating a new file (without data) 118
1.2.12 Creating a new file from chunks 119
1.3 Memory Ranges 120
1.3.1 Accessing the project's Memory Ranges 120
1.3.2 Reading data from a Memory Range 121
1.3.3 Creating a new MemoryRange and adding to the project 121
1.4 Models 123
1.4.1 Accessing the Model Store 123
1.4.2 Counting the amount of SMSes 123
1.4.3 Print some details about an SMS 123
1.4.4 Print the SMS "Message" Field for all SMSes 124
1.4.5 Create a new SMS message 125
1.4.6 Using AddRange to add models quickly. 126
1.4.7 Create a new Call 126
1.4.8 Create a new Contact 127
1.4.9 Create a new Email 128
1.4.10 Create a new MMS Message 129
1.4.11 Add an Attachment to an Email (or MMS) 129
1.4.12 Create a new Location 130
1.4.13 Create a new Journey 131
1.4.14 Create a new Instant Message 131
1.4.15 Create a new Chat 132
1.4.16 Create a new Calendar Entry 133
1.4.17 Create a new Note 133
1.4.18 Create a new Bluetooth Device 134

Chapter 1: **Introduction**

1.1 Overview

The UFED Physical Pro is comprised of two components:

- The UFED hardware with Physical Extraction module, used to create Physical and/or Logical dumps from mobile devices, which can then be saved to a USB disk drive, SD memory card, or directly to your PC.
- The UFED Physical Analyzer (PA) PC application, which provides an in-depth physical memory analysis of the extracted mobile phone data (phonebook contents, SMS messages, call logs, image files, video files, audio files, and more) The Physical Analyzer also serves to generate comprehensive and verified evidence reports of relevant data extracted and analyzed from the mobile device.

The UFED PA work flow consists of two steps:

- Physical memory extraction via UFED hardware
- Data analysis via PC Physical Analyzer

1.2 Physical Memory Extraction

The UFED's physical memory extraction function provides the most comprehensive access to mobile device data, including deleted and hidden information, as well as access to phone passwords. Unlike the logical extraction process, the physical extraction bypasses the phone's operating system, acquiring the data directly as an image, from the phone's internal flash memory.

The phone memory is captured into hex dump file (or files, depending on the memory structure of the specific phone) which can later be analyzed and decoded using the UFED Physical Analyzer (PA) application.

1.3 Data Analysis

The UFED Physical Analyzer software allows the investigator to perform in-depth analysis of the extracted data and generate reports.

The UFED PA application provides the following key features:

- Analysis of the hex dump with a layered view of memory content
  - Provides a detailed view of the hex dump
  - Reconstructs the phone file system
  - Decodes contact lists, SMS messages, call logs, phone information (IMSI, ICCID, user codes) and more
  - Provides a view of data files – images, videos, etc.
  - Provides access to both current and deleted data
  - Retrieves phone passwords
- Simple viewing and user friendly browsing of information
- Powerful search tools
  - Instantly search for project content
  - Search the hex dump or file system

  - Search by various parameters such as strings, bytes, numbers, dates
  - Use GREP search (regular expressions) to look for specific data strings
  - Bookmarking memory locations for indexing of key areas for later review
- Ability to use Python shell commands for data analysis
- Plug-ins
  - Manage installed plug-ins
  - Write your own plug-ins using Python scripting language
  - Get additional plug-ins from the community website
- Generation of customized reports

Chapter 2: **Installation and Activation**

2.1 Introduction

This chapter describes the activation process of the UFED Physical Extraction module on the UFED hardware itself, as well as the installation and activation process of the UFED Physical Analyzer (PA) software on your PC.

2.2 Activating the UFED Physical Extraction Module

Important: This section applies to users upgrading their current UFED to the Physical Module. It is not required for new UFED Physical Pro systems with the Physical Module already enabled.

The UFED has two types of licenses:

- Logical license - Standard license for logical data extraction functionality.
- Physical license - Advanced license enabling physical extraction and analysis.

To enable physical data extraction and analysis capabilities, the UFED Physical license must be activated.

NOTE: Activation of the UFED Physical Extraction Module must be performed on the UFED hardware prior to installing the UFED Physical Analyzer software on your PC.

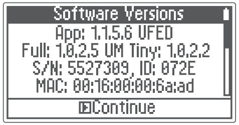
The installation of the UFED firmware on the UFED device is a two-step process and involves:

- Upgrading the UFED software to a version that supports physical extraction.
- Activation of the UFED Physical Extraction Module.

2.2.1 **Renewing the UFED Physical Extraction Module License**

To activate the UFED Physical Extraction Module, perform the following steps:

1. Power on the UFED.
2. Locate the UFED device serial number and ID information by selecting Services > Software Versions from the main menu. Make a note of the 7 digit serial number marked "S/N" and ID information.

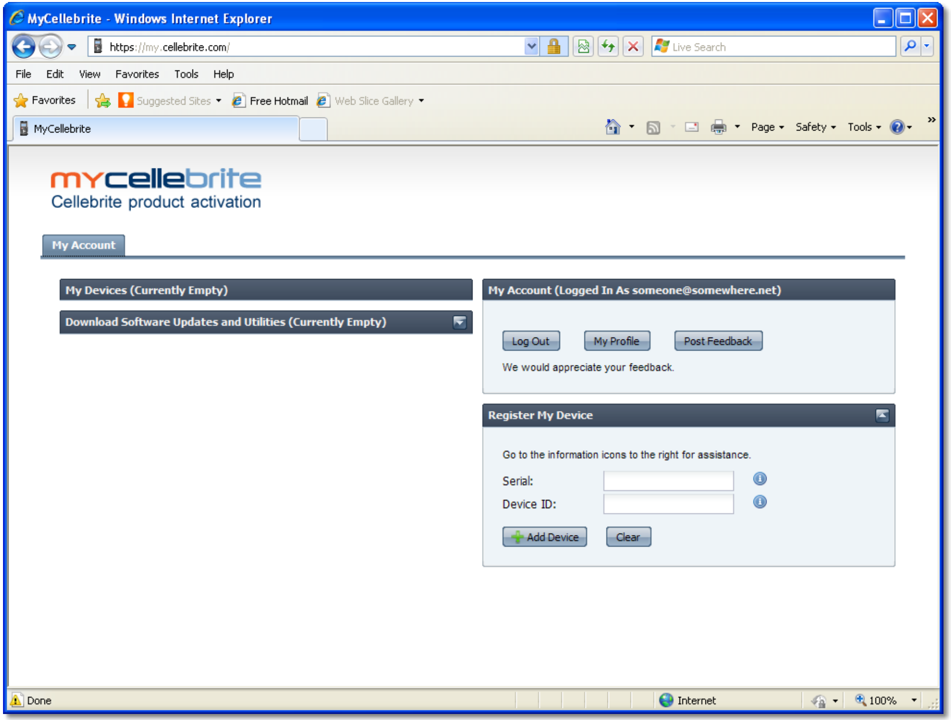


Software Versions

App: 1.1.5.6 UFED
Full: 1.0.2.5 UM Tiny: 1.0.2.2
S/N: 5527309, ID: 072E
MAC: 00:16:00:00:6a:ad

Figure 1: The UFED Software Versions screen

3. On a PC with a web access, launch your web browser and go to **my.cellebrite.com**. You will be asked to enter your user name and password to login into your MyCellebrite web page.



MyCellebrite - Windows Internet Explorer

https://my.cellebrite.com/

mycellebrite

Cellebrite product activation

My Devices (Currently Empty)

Download Software Updates and Utilities (Currently Empty)

My Account (Logged In As someone@somewhere.net)

We would appreciate your feedback.

Register My Device

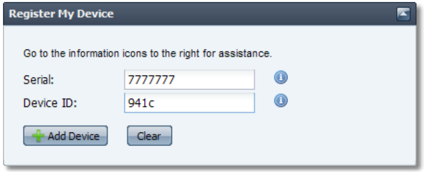
Go to the information icons to the right for assistance.

Serial:

Device ID:

Figure 2: The Cellebrite UFED Activation screen

4. In the **Add a Device to My Devices** section, enter the **Serial** number and **Device ID** of your UFED, which were obtained from the Software Versions screen, then click **Add Device**.



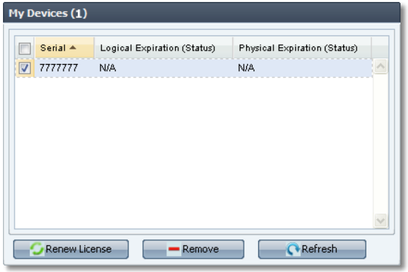
Go to the information icons to the right for assistance.

Serial: 7777777

Device ID: 941c

Figure 3: Adding a new device

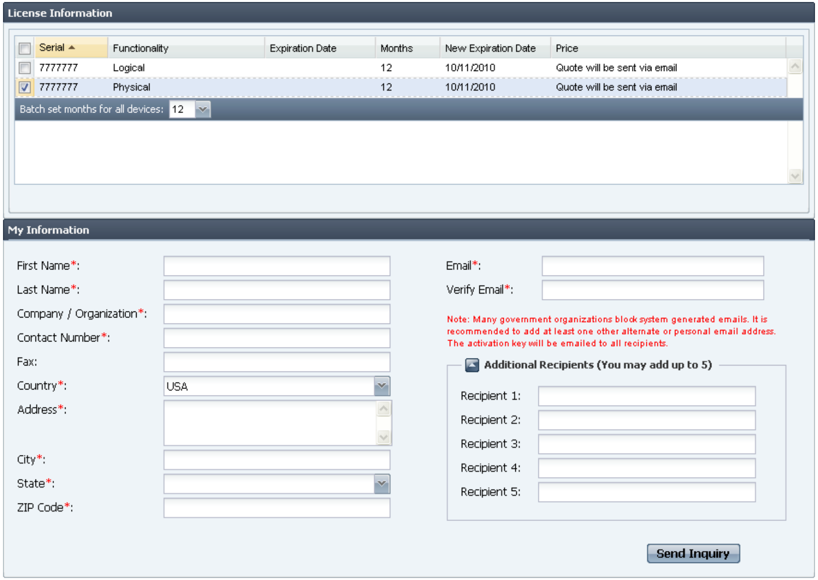
5. The device will be added to the **My Devices** list. Click the checkbox beside this device, and then click on the **Renew License** button.



□	Serial ▲	Logical Expiration (Status)	Physical Expiration (Status)
☑	7777777	N/A	N/A

Figure 4: My Devices list.

6. On the **Renewal Process** page, fill in the required fields, including email address, then click the **Send Inquiry** button. A quote for the required license will be sent to you via the specified email address.



License Information

□	Serial ▲	Functionality	Expiration Date	Months	New Expiration Date	Price
□	7777777	Logical		12	10/11/2010	Quote will be sent via email
☑	7777777	Physical		12	10/11/2010	Quote will be sent via email

Batch set months for all devices: 12

My Information

First Name*:	
Last Name*:	
Company / Organization*:	
Contact Number*:	
Fax:	
Country*:	USA
Address*:	
City*:	
State*:	
ZIP Code*:	

Email*:	
Verify Email*:	

Note: Many government organizations block system generated emails. It is recommended to add at least one other alternate or personal email address. The activation key will be emailed to all recipients.

Additional Recipients (You may add up to 5)

Recipient 1:	
Recipient 2:	
Recipient 3:	
Recipient 4:	
Recipient 5:	

Figure 5: The Renewal Process screen

7. After the license purchasing process is concluded, you will receive an email message containing the activation key. To enter your key, power on your UFED System, select: **Services > Upgrade > UFED License > Activate License, and enter the key string**.

2.2.2 UFED Software Upgrade

Once activated, the UFED Physical Extraction module is ready for use. To verify that you have the latest version of the device firmware, you should upgrade the software version.

To upgrade the software version, select Services > Upgrade > Upgrade Application Now. For further instructions, please refer to the UFED User Manual (chapter 11).

NOTE: If the menu options of the UFED Physical Analyzer do not appear, contact Cellebrite support to verify that your UFED and UFED Physical Analyzer licenses are registered correctly.

2.3 Installing the UFED Physical Analyzer Application

2.3.1 System Requirements

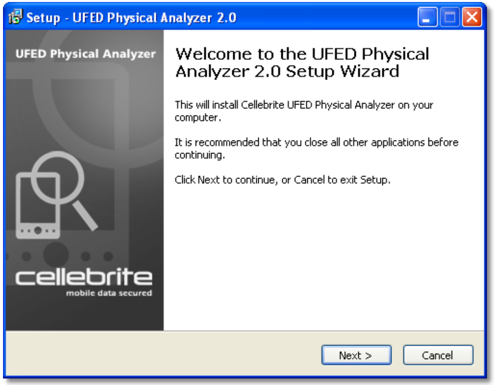
PC	Windows compatible PC with a Pentium® IV or compatible processor running at 1.6 GHz or higher
Operating System	Microsoft® Windows® XP with SP1 or later Microsoft® Windows Vista™ or Windows 7
Memory	2 GB RAM
Space Requirements	500 MB of free disk space for installation
Additional Requirements	Microsoft® .Net version 3.5 Service Pack 1

2.3.2 Software Installation

Insert the UFED Physical Analyzer CD into your computer's optical drive and browse the contents.

2.3.2.1 Installing the UFED Physical Analyzer

1. Double click on the setup program to install the UFED Physical Analyzer application.
2. Select the setup language, then click **OK** to continue.



Setup - UFED Physical Analyzer 2.0

Welcome to the UFED Physical Analyzer 2.0 Setup Wizard

This will install Cellebrite UFED Physical Analyzer on your computer.

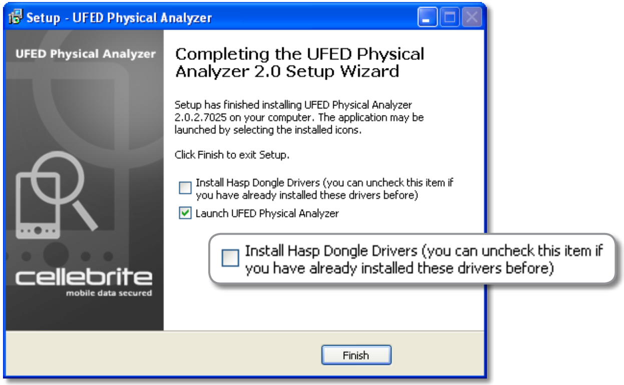
It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Figure 6: The UFED Physical Analyzer setup wizard

3. Follow the installation setup wizard prompts.

4. At the end of the installation process you will be prompted to install the HASP USB Kay drivers. If you intend to activate the application using a hardware license key (dongle) provided by Cellebrite, check the **Install Hasp Dongle Drivers** option, then click the **Finish** button.



Completing the UFED Physical Analyzer 2.0 Setup Wizard

Setup has finished installing UFED Physical Analyzer 2.0.2.7025 on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

□ Install Hasp Dongle Drivers (you can uncheck this item if you have already installed these drivers before)

☑ Launch UFED Physical Analyzer

□ Install Hasp Dongle Drivers (you can uncheck this item if you have already installed these drivers before)

Figure 7: HASP Dongle Drivers installation option

5. When finished, if the **Launch UFED Physical Analyzer** option was checked at the end of the installation process, the application will launch automatically. Otherwise, run the application by selecting **Start > Programs > Cellebrite Mobile Synchronization > UFED Physical Analyzer**, or by double clicking the **UFED Physical Analyzer** shortcut added to your desktop (if you selected to add it during the installation process).

2.4 Activating the Physical Analyzer application

Activating the UFED Physical Analyzer can be done by:

- Using an activation code
- Using a hardware license key

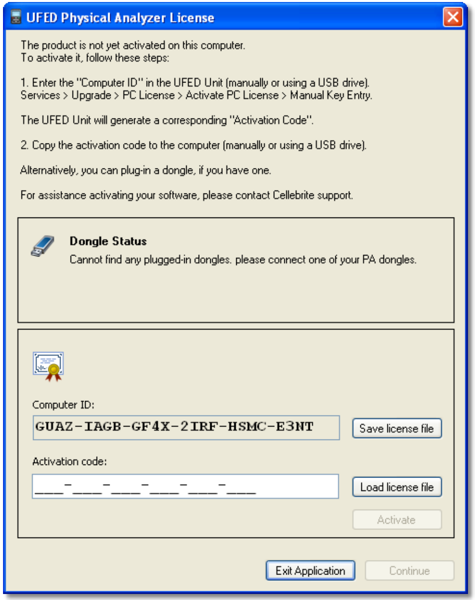
To activate the application:

1. Launch the **UFED Physical Analyzer** application.
2. When launching for the first time, or when using a hardware license key, a license window appears.

2.4.1 Using an Activation Code

A license is required to activate the UFED Physical Analyzer. The UFED Physical Extraction module, which was previously activated, can generate these licenses.

NOTE: The number of simultaneous activated copies of the UFED Physical Analyzer application (one license per PC) is restricted according to the purchased UFED Physical Extraction module license.



The product is not yet activated on this computer.
To activate it, follow these steps:

1. Enter the "Computer ID" in the UFED Unit (manually or using a USB drive).
Services > Upgrade > PC License > Activate PC License > Manual Key Entry.

The UFED Unit will generate a corresponding "Activation Code".

2. Copy the activation code to the computer (manually or using a USB drive).

Alternatively, you can plug-in a dongle, if you have one.

For assistance activating your software, please contact Cellebrite support.

Dongle Status
Cannot find any plugged-in dongles. please connect one of your PA dongles.

Computer ID: GUAZ-IAGB-GF4X-2IRF-HSMC-E3NT

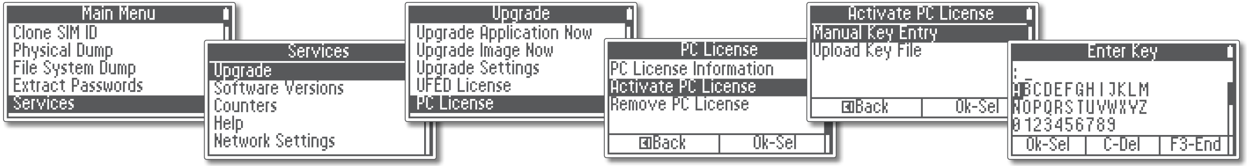
Activation code: ___-___-___-___-___-___

Figure 8: The UFED Physical Analyzer License window

2.4.1.1 **Manual Activation Process**

To manually enter the Activation Code:

1. Note the Computer ID displayed in the **UFED Physical Analyzer License** window on your PC.
2. On the UFED unit, select **Services** > **Upgrade** > **PC License** > **Activate PC License** > **Manual Key Entry** from the main menu.



3. Using the directional keypad, enter the Computer ID that was displayed in the **UFED Physical Analyzer License** window. Select **F3** to confirm.
4. The UFED unit will display the PC Activation Code.
5. On the **Physical Analyzer License** window, enter the Activation Code as it is displayed on your UFED unit.
6. Click **Activate**.

Your UFED device and Physical Analyzer application are now both ready for use.

2.4.1.2 **File Based Activation Process**

Manual Key entry can be avoided by saving the key file to a USB drive. Doing so shortens the activation process and can save a lot of time when installing multiple instances of the UFED Physical Analyzer.

On your PC:

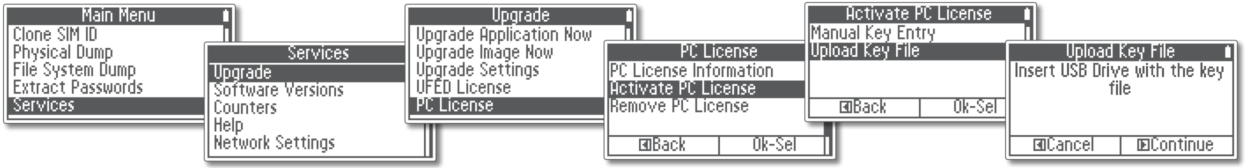
1. Connect a USB disk drive to your PC.
2. Click the **Write to USB** button next to the Computer ID field to generate a Computer ID file which will be written to your USB disk drive.
3. On the **Browse for Folder** window, select the USB disk drive or target folder to which the Computer ID file will be saved, and click **OK**.

   NOTE: The Computer ID file can either be saved directly to a USB disk drive (if connected), or to any location on your hard drive, in case you need to send it to a remote location for Activation Code generation.

4. Save the Computer ID file to the root directory of the USB disk drive.
5. Safely disconnect the USB disk drive from the PC.

On your UFED unit:

1. Connect the USB disk drive containing the saved ID file to any of the USB ports on the UFED unit.
2. From the Main Menu on your UFED unit, select **Services** > **Upgrade** > **PC License** > **Activate PC License** > **Upload Key File** to read the Computer ID from the USB disk drive.



Insert USB Drive with the key file

3. The UFED unit will display the generated PC Activation Code. Choose **Save to USB** to save the Activation Code file to the connected USB disk drive.

4. On the **Physical Analyzer License** window, click the **Read from USB** button next to the Activation Code field.

5. On the **Browse for Folder** window, select the USB disk drive or target folder to which the Activation Code file was saved, and click **OK**. The Activation Code will load into the field.

6. Click **Activate**.

Your UFED device and Physical Analyzer application are now both ready for use.

2.4.2 **Using a Hardware License Key**

You can also use a HASP hardware license key (dongle), provided by Cellebrite as part of your UFED system, to activate the locally installed copy of UFED Physical Analyzer.

NOTE: Using a hardware license key provides you with a “mobile license”, enabling you to take your license on the road and use it to activate a copy of the UFED Physical Analyzer application wherever you are.

To activate the UFED Physical Analyzer application using a hardware license key:

1. Connect the hardware license key to a USB port on your computer.

   NOTE: The HASP dongle drivers must be installed in order to use a hardware license key. If the drivers were not installed during the software installation process, you can run the installation process again (see “Installing the UFED Physical Analyzer” on page 10) and select the Install Hasp Dongle Drivers option at the end of the process.

2. After the key was recognized by the operating system, the application will be able to read the license and allow you to continue.

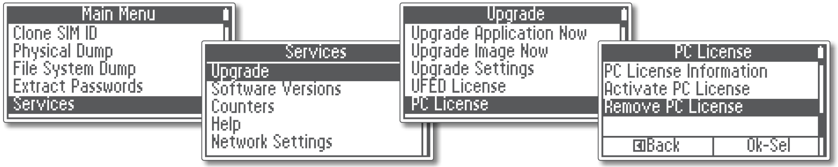
Your UFED Physical Analyzer application is now ready for use.

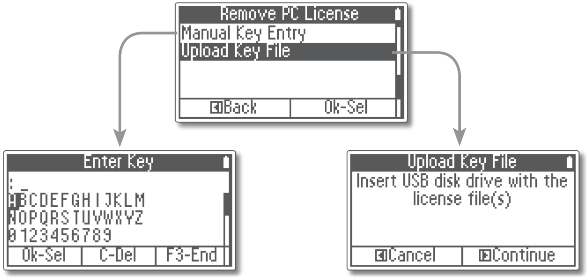
2.5 Deactivating a UFED Physical Analyzer License

In cases where a UFED Physical Analyzer installation, activated by an Activation Code, needs to be moved to another PC, or cleanly installed on the same PC, you must first deactivate (remove the license) from the computer. The license should be reloaded in your UFED device for re-use on a different PC or a clean install on the same PC.

To deactivate the PC license, perform the following steps:

1. Launch the **UFED Physical Analyzer** application.
2. From the UFED Physical Analyzer menu, select **Help** > **License** > **Deactivate**.
3. Click the **Deactivate** button to deactivate the PC license.
4. A **Browse for Folder** window will appear. Select the target folder to save the deactivation key, then click the **OK** button.
5. The system will open a new window showing the deactivation key.
6. On the UFED unit, select **Services** > **Upgrade** > **PC License** > **Remove PC License** from the main menu.





Insert USB disk drive with the license file(s)

7. Select either **Manual Key Entry** to enter the license manually, or **Upload Key File** to upload it from USB disk drive.
8. If **Manual Key Entry** was selected, enter the deactivation key using the directional keypad and select **F3**.
9. If **Upload Key File** was selected, connect the USB disk drive to any of the UFED USB ports, then press the ▶ key to continue.
10. The deactivated license of the UFED Physical Analyzer application is now re-added to your UFED unit, ready for use to activate another UFED Physical Analyzer installation.

Chapter 3: **Performing Data Extraction**

The information provided in this chapter is based on the assumption that the user is familiar with the basic operations of the UFED device. Please refer to the *UFED User Manual*, Chapter 4 to familiarize yourself with UFED before continuing. This chapter describes advanced features specific to the UFED Physical module only.

NOTE: Use the ▼▲ keys to move between options in the **Main Menu**. Use the ◀ key to return to a previous menu.

3.1 **Performing a Physical Dump**

When performing a physical dump operation, the UFED Physical Pro uses advanced extraction methods to create a single hex dump file for each flash memory chip, or address range utilized by the mobile device. Unlike conventional logical extraction processes, the physical extraction method bypasses the phone's operating system, acquiring the data directly from the phone's internal flash memory. The phone memory is captured into hex dump file(s) that will later be read and analyzed using the UFED Physical Analyzer application.

The physical dump created includes memory space unallocated by the phone's OS which may contain deleted data such as SMS, Call logs, Phonebook entries, Pictures, Video and user passwords.

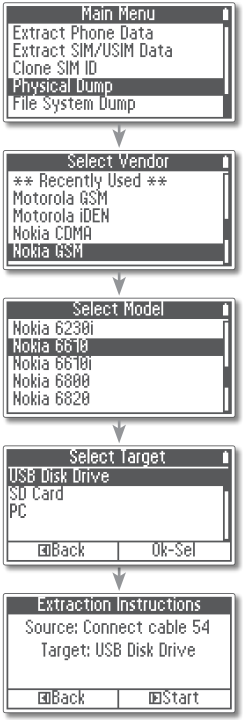
3.1.1 **Using Removable Media**

1. Select **Physical Dump** from the **Main Menu**. Press **OK** or ▶ to continue.
2. Select the manufacturer of the phone from the **Select Vendor** menu. Press **OK** or ▶ to continue.
3. Select the model of the phone. Press **OK** or ▶ to continue.
4. Select the target storage media (USB disk drive or SD Card) from the **Select Target** menu. Press **OK** or ▶ to continue.
5. You will be instructed to connect the source phone, using the appropriate cable to the left USB port of the UFED, and then connect the target storage media to the appropriate port right side of the UFED.

   NOTE: USB disk drive storage media should be connected to right side **Target** port. SD card storage media should be inserted in the SD card slot on the left side of the UFED unit.

   Make sure both are connected, and then press ▶ to start the dump process.

   NOTE: When connecting the phone to the UFED unit, some phone models will prompt you to select the connection mode on the phone’s display screen. Choose Data Mode, PC, or PC Sync mode. Actual selection choice will vary depending on the phone model.

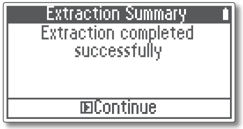


Source: Connect cable 54
Target: USB Disk Drive

CAUTION: To prevent possible loss of data, do not disconnect the phone or storage media (USB disk drive or SD card) during the extraction process.

6. Upon the completion of the dump process, the UFED unit will display "Extraction completed successfully".

   It is now safe to disconnect the phone and remove the target storage media for analysis using the UFED Physical Analyzer PC tool.



Extraction Summary

Extraction completed successfully

▶Continue

7. A folder named according to the phone model, current date, and a counter (for example, "Physical Nokia GSM Generic 2009_05_15 (001)" is created on the target storage drive. This folder contains the extracted binary files (one for each extracted memory module), and the UFD file, used by the UFED Physical Analyzer application to access the extracted data.

   Multiple dumps from different phones can be saved to the same USB drive or SD card. A new folder will automatically be created for each device dump.

3.1.2 Extracting Data Directly to Your PC

1. Connect your UFED device to your PC using a USB to mini-USB cable, utilizing the port marked "PC" located on the top of your UFED unit. Your PC may prompt you to install drivers (refer to chapter 9 in the UFED User Manual).

On the UFED unit:

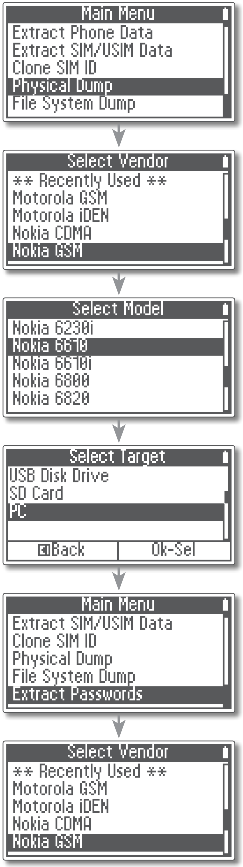
1. Select Physical Dump from the Main Menu. Press OK or ▶ to continue.
2. Select the manufacturer of the phone from the Select Vendor menu. Press OK or ▶ to continue.

3. Select the model of the phone. Press **OK** or ▶ to continue.
4. Select **PC** as the target. Press **OK** or ▶ to continue.

On your PC:

5. Launch the UFED Physical Analyzer application.
6. In the application toolbar, click on the **Read Data from UFED** button.
7. In the displayed UFED Downloader window, specify the download path to which the dump should be saved, then click the **Start** button.
8. The UFED unit will create the dump under the specified folder.
9. At the end of the extraction process, you will be prompted to open the extracted dump.

NOTE: Clicking the Open Target Folder button to display the content of the selected target folder.

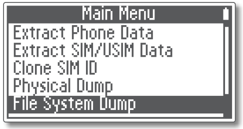


3.2 Extracting the File System

The File System Dump option extracts all the accessible files on the mobile phone using a logical process.

Extracting the file system is an alternative way to get data from phones, including phone models that are not currently supported with physical dump. UFED Physical Pro provides access, and extracts hidden files and databases inaccessible by other file system acquisition tools.

From the extracted file system you can get many different types of application files that can be decoded and then searched for information, such as the Contacts or SMS database files.



The process for extracting a File System Dump is almost identical to performing a Physical Dump, as described in "Performing a Physical Dump" on page 19.

Start by selecting **File System Dump** from the **Main Menu**, as in step 1 of "Performing a Physical Dump" on page 19, and continue with same steps afterwards.

The resulting folder will include a ZIP archive of the phone's file system, instead of the Hex file(s) of the memory dump files, and a .ufd info file that enables the file system archive to be read by the Physical Analyzer application.

3.3 Extracting Passwords

The Extract Passwords feature provides quick access to the phone's user passwords without the need to analyze a dump using the UFED Physical Analyzer application.

1. Select **Extract Passwords** from the **Main Menu**. Press **OK** or ▶ to continue.
2. Select the phone's manufacturer from the **Select Vendor** menu. Press **OK** or ▶ to continue.

3. Select the phone's model from the **Select Model** menu. Press **OK** or ▶ to continue.

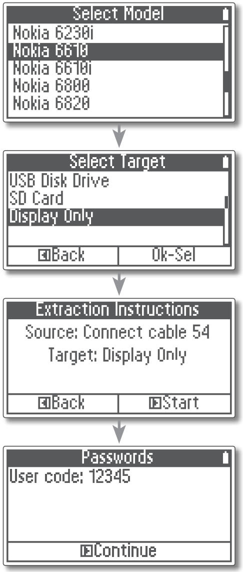
4. From the **Select Target** options, select **USB Disk Drive** or **SD Card** to store the extracted data on the selected storage media, or select **Display Only** to display the extracted password data on the UFED unit, without storing it.

5. You will be instructed to connect the source phone, using the appropriate cable, to the left USB port of the UFED unit marked "source". Connect removable media if extracting to file.

   NOTE: USB disk drive storage media should be connected to right side "Target" port. SD card storage media should be inserted in the SD card slot on the left side of the UFED unit.

   Make sure both are connected, and then press ▶ to start the extraction.

   NOTE: When connecting the phone to the UFED unit, some phone models will prompt you to select the connection mode on the phone's display screen. Choose Data Mode, PC, or PC Sync mode. Actual selection choice will vary depending on the phone model.



Select Model

Nokia 6230i
Nokia 6610
Nokia 6610i
Nokia 6800
Nokia 6820

Select Target

USB Disk Drive
SD Card
Display Only

◧Back | Ok-Sel

Extraction Instructions

Source: Connect cable 54
Target: Display Only

◧Back | ◨Start

Passwords

User code: 12345

◨Continue

6. When the extraction process is completed, the password information will be displayed on the screen. When the phone has more than one password, multiple passwords will be shown.

Chapter 4: **Overview of UFED Physical Analyzer Application**

4.1 Introduction

The UFED Physical Analyzer application provides powerful analysis tools for the extracted phone data, and simplifies the task of navigating through the phone's data structures. Using the UFED Physical Analyzer application will assist you in the complex tasks of intelligence gathering, investigative research, and providing legal evidence in the form of reports.

The application is designed to utilize the memory extracted by the UFED unit and presents the phone's hex dump, file system and analyzed data in a clear and concise way, allowing investigator to use powerful search tools to parse and decode relevant information.

As a completing step, the application will allow you to generate reports of your findings and export them in various file formats, such as HTML, PDF, Excel (*.xlsx), and XML.

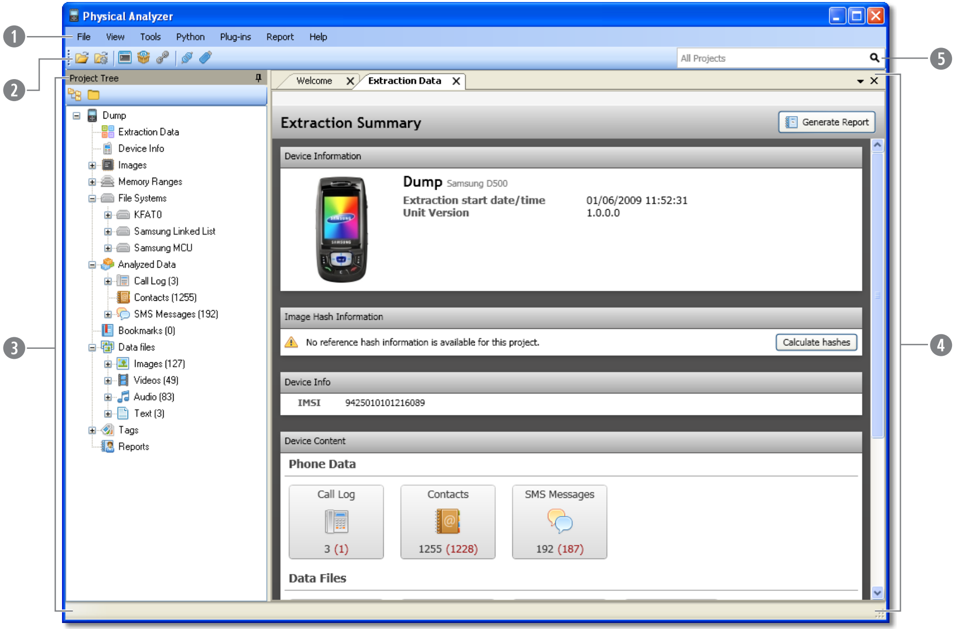
4.2 Launching UFED Physical Analyzer Application

To launch the UFED Physical Analyzer application, double click on the **UFED Physical Analyzer** desktop shortcut icon, or select **Start** > **Programs** > **Cellebrite Mobile Synchronization** > **UFED Physical Analyzer**.

4.3 Application Structure Overview

The UFED Physical Analyzer application structure is comprised of the following components:

1. Application Menu
2. Application Toolbar
3. Project Tree Area
4. Data Display Area
5. Search Field



Extraction Summary

Device Information

Dump Samsung D500

Extraction start date/time 01/06/2009 11:52:31

Unit Version 1.0.0.0

Image Hash Information

No reference hash information is available for this project.

Device Info

IMSI 9425010101216089

Device Content

Phone Data

Call Log 3 (1)

Contacts 1255 (1228)

SMS Messages 192 (187)

Data Files

Figure 9: Application structure overview

4.3.1 Application Menu

The application menu provides access to the following menus and commands and functions:

- **File** menu:
  - **Open:** Select and open a file for analysis using the standard analysis process.
  - **Open (Advanced):** Select and open a file for analysis using the advanced analysis process. See "Using the Advanced Opening Feature" on page 61.
  - **Recent:** Displays a list of the recent projects.
  - **Close:** Closes the currently active project.
  - **Exit:** Closes the application and all active projects.
- **View** menu:
  - **Show Welcome Screen:** Displays the **Welcome** screen. See "The Welcome tab" on page 42.
  - **Trace Window:** Show/hide the trace panel at the bottom of the data display area.
- **Tools** menu:
  - **Dump File System:** Exports and saves the parsed file system to actual files and folders in a directory structure. See "Exporting the File System" on page 100.
  - **Read Data from UFED:** Extract phone data directly to the computer.
  - **Dump GPS / Mass Storage Device:** Reads and saves data from GPS and mass storage devices connected to the workstation via USB connection.

    - **Settings:** Access to the application settings window. See "General settings" on page 101.
- **Python** menu:
    - **Python Shell:** Opens the Python Shell window for user customized analysis using Python commands. See "Using the Python Shell" on page 100.
    - **Run Script:** Runs a pre-written Python script (*.py file).
    - **Run Script (Debug enabled):** Enables you to run a pre-written Python script (*.py file) in debug mode.
- **Plug-ins** menu:
    - **Add/Remove Plug-ins:** Displays the list of installed plug-ins to enable management of the currently installed plug-ins. See "Managing Plug-ins" on page 97.
    - **Run Plug-in:** Allows the user to select a specific plug-in and run it. See "Running a Specific Plug-in" on page 98.
    - **Chain Manager:** Displays the Chain Manager window to enable management and creation of device processing chains. See "Managing Chains" on page 91.
- **Report** menu:
    - **Generate Report:** Generates a report summary of all information found by the analysis process. See "Generating Reports" on page 57.
- **Help** menu:
    - **Manual:** Launches Adobe Reader (aka Acrobat Reader) and displays the user manual (in PDF format).
    - **License** sub-menu:

  - **Enter New License:** Enables you to enter a new Activation Code.
  - **Show License Details:** Displays the current license code validation period, and the current Computer ID and Activation Code.
  - **Show Dongle Details:** When using a hardware license key, displays the details of the currently used dongle.
  - **Deactivate:** Deactivates the license used to activate the application on the current workstation. See "Deactivating a UFED Physical Analyzer License" on page 17.
- **About:** Provides information about the installed UFED Physical Analyzer application version and its components.

4.3.2 Application Toolbar

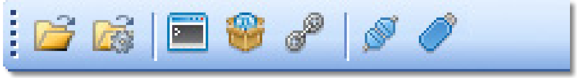


Figure 10: The Application Toolbar

The application toolbar provides shortcuts to quickly access commonly used functions:

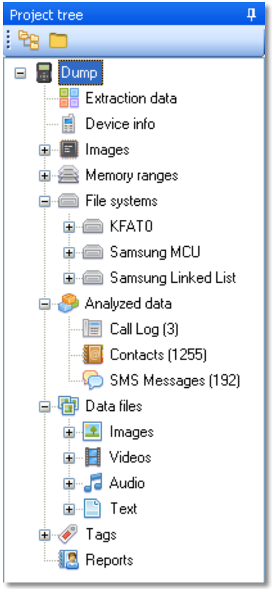
	Open	Click to open a file for analysis (**File** > **Open...**).
	Open (Advanced)	Click to use the advanced options to open a file for analysis (**File** > **Open (Advanced)...**).
	Python Shell	Click to display the Python Shell window (**Python** > **Python Shell...**)
	Add/Remove Plug-ins	Click to display the Add/Remove Plugins window (**Plug-ins** > **Add/Remove Plug-ins...**)
	Chain Manager	Click to display the Chain Manager window (**Plug-ins** > **Chain Manager...**)
	Read Data from UFED	Initiates an extraction process of phone data from a UFED unit connected directly to the PC via USB cable (**Tools** > **Read Data from UFED...**).
	Dump GPS / Mass Storage Device	Initiates an extraction process of GPS or mass storage device data connected directly to the PC via USB cable (**Tools** > **Dump GPS / Mass Storage Device...**).

4.3.3 Project Tree Area

The Project Tree area displays the following extracted information structure of each file opened for analysis:

- Extraction data
- Device info
- Images (one for each extracted memory module or extracted memory range)
- Memory ranges
- File systems
- Analyzed data (where supported)
- Data files
- Tags
- Reports

By opening the **Analyzed data** or **Data files** sub-trees, you can drill down into the tree structure to search for specific information. Double clicking on any of the lower-level nodes, will display the relevant information viewer in the **Data Display** area.



Project tree

- Dump
  - Extraction data
  - Device info
  - Images
  - Memory ranges
  - File systems
    - KFAT0
    - Samsung MCU
    - Samsung Linked List
  - Analyzed data
    - Call Log (3)
    - Contacts (1255)
    - SMS Messages (192)
  - Data files
    - Images
    - Videos
    - Audio
    - Text
  - Tags
  - Reports

Figure 11: Project Tree Overview

Each extraction file you open will add a project at the bottom of the Project Tree.

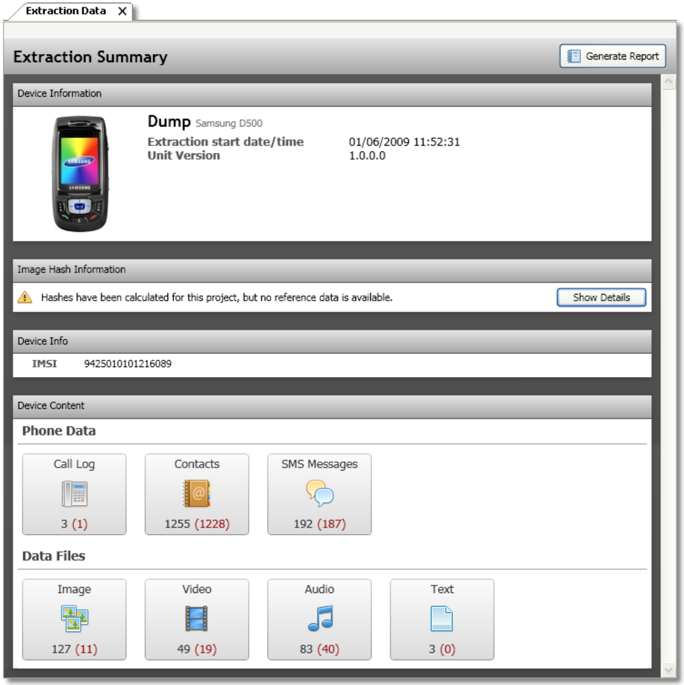
Every branch in the **Project Tree** can be expanded or collapsed by clicking the ⊞ or ⊟ icons. In addition, the entire tree can be fully expanded or collapsed by clicking the 🗂 or 📁 buttons at the top the tree section.

4.3.3.1 **Extraction Data**

Double clicking the **Extraction data** item will display its tab in the Data Display area.

The **Extraction data** tab displays the following information:

- Device Information - Information related to the device extraction.
- Image Hash Information - Verification of the logged hash values of the extracted memory dump with the hash values of the parsed images. See “Hash Verification” on page 70.
- Device Info - A Summary of th specific device info pulled from the extracted data. See “Device Info” on page 34.
- Device Content - Analyzed content, separted to:
    - Phone Data - The types of analyzed phone data found in the extracted memory dump, such as Call Log, Contacts, SMS Messages, and others. For the complete list of Phone Data types, see “Analyzed Data” on page 38.



Extraction Summary

Device Information

Dump Samsung D500

Extraction start date/time	01/06/2009 11:52:31
Unit Version	1.0.0.0

Image Hash Information

⚠ Hashes have been calculated for this project, but no reference data is available.

Device Info

IMSI	9425010101216089

Device Content

Phone Data

Call Log	Contacts	SMS Messages
3 (1)	1255 (1228)	192 (187)

Data Files

Image	Video	Audio	Text
127 (11)	49 (19)	83 (40)	3 (0)

Figure 12: The Extraction Data tab

- **Data Files** - The types of standard data files found in the extracted memory dump, such as Images, Video, Audio, and Text files.

NOTE: The **Extraction data** tab will be displayed automatically whenever you open a new file for analysis.

Clicking on any of the Device Content categories will display the relevant information viewer tab in the in the data display area, listing all the items logged in this category. See "Analyzed Data" on page 38 and "Data Files" on page 40.

Clicking the Generate Report button at the top right of the tab will prompt you to generate a report for the current project. See "Generating Reports" on page 57.

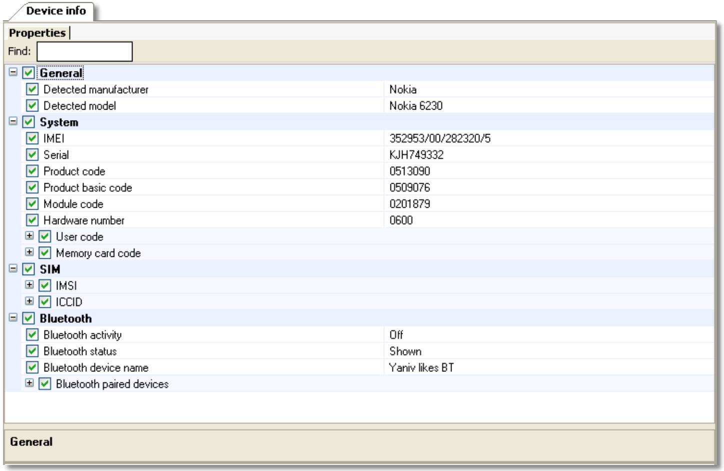
4.3.3.2 **Device Info**

Double clicking the **Device info** item will display its tab in the data display area.

The **Device info** tab provides extensive amount of existing and deleted information, as well as important identifiers of the phone such as, SIM card and user lock codes, where supported.

The **Properties** list is divided to display the different Device Info categories.

NOTE: The number of categories and amount of displayed information may vary, depending on the device model and manufacturer.



Device info

Properties |

Find:

⊟ ☑ **General**	
☑ Detected manufacturer	Nokia
☑ Detected model	Nokia 6230
⊟ ☑ **System**	
☑ IMEI	352953/00/282320/5
☑ Serial	KJH749332
☑ Product code	0513090
☑ Product basic code	0509076
☑ Module code	0201879
☑ Hardware number	0600
⊞ ☑ User code	
⊞ ☑ Memory card code	
⊟ ☑ **SIM**	
⊞ ☑ IMSI	
⊞ ☑ ICCID	
⊟ ☑ **Bluetooth**	
☑ Bluetooth activity	Off
☑ Bluetooth status	Shown
☑ Bluetooth device name	Yaniv likes BT
⊞ ☑ Bluetooth paired devices	

General

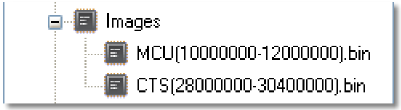
Figure 13: Device Info

A checkbox next to each of the categories and properties indicate whether this item will be included (checked) or excluded (unchecked) in the report.

A **Find** field, at the top of the properties list allows you to filter the displayed items (Categories, Subjects, and data) to display items containing the entered text string.

4.3.3.3 Images

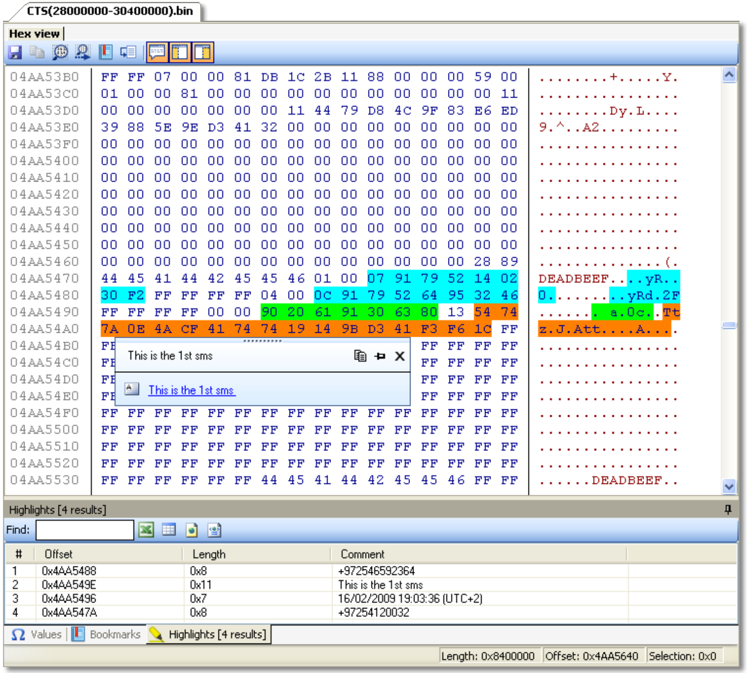
The **Images** item of the project tree lists all the dump files generated by the data extraction from the memory modules of the device.



Images
MCU(10000000-12000000).bin
CTS(28000000-30400000).bin

Figure 14: Memory dump images

Double clicking on any image item will display it in a new Hex View tab for it in the data display area.



CTS(28000000-30400000).bin

Hex view

```
04AA53B0  FF FF 07 00 00 81 DB 1C 2B 11 88 00 00 00 59 00  ........+.....Y.
04AA53C0  01 00 00 81 00 00 00 00 00 00 00 00 00 00 00 11  ................
04AA53D0  00 00 00 00 00 00 00 11 44 79 D8 4C 9F 83 E6 ED  ........Dy.L....
04AA53E0  39 88 5E 9E D3 41 32 00 00 00 00 00 00 00 00 00  9.^..A2.........
04AA53F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
04AA5400  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
04AA5410  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
04AA5420  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
04AA5430  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
04AA5440  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
04AA5450  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
04AA5460  00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 89  ..............(.
04AA5470  44 45 41 44 42 45 45 46 01 00 07 91 79 52 14 02  DEADBEEF....yR..
04AA5480  30 F2 FF FF FF FF 04 00 0C 91 79 52 64 95 32 46  0.........yRd.2F
04AA5490  FF FF FF FF 00 00 90 20 61 91 30 63 80 13 54 74  ....... a.0c..Tt
04AA54A0  7A 0E 4A CF 41 74 74 19 14 9B D3 41 F3 F6 1C FF  z.J.Att....A....
04AA54B0  FF                                  FF FF FF FF  ................
04AA54C0  FF                                  FF FF FF FF  ................
04AA54D0  FF                                  FF FF FF FF  ................
04AA54E0  FF                                  FF FF FF FF  ................
04AA54F0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
04AA5500  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
04AA5510  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
04AA5520  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
04AA5530  FF FF FF FF FF FF 44 45 41 44 42 45 45 46 FF FF  ......DEADBEEF..
```

This is the 1st sms

This is the 1st sms

Highlights [4 results]

Find:

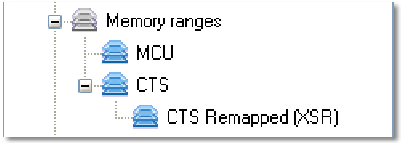
#	Offset	Length	Comment
1	0x4AA5488	0x8	+972546592364
2	0x4AA549E	0x11	This is the 1st sms
3	0x4AA5496	0x7	16/02/2009 19:03:36 (UTC+2)
4	0x4AA547A	0x8	+97254120032

Length: 0x8400000 Offset: 0x4AA5640 Selection: 0x0

Figure 15: Hex View tab

4.3.3.4 **Memory Ranges**

The **Memory ranges** item of the project tree lists the analyzed memory ranges for each of the memory module dumps of the device (listed under Images).

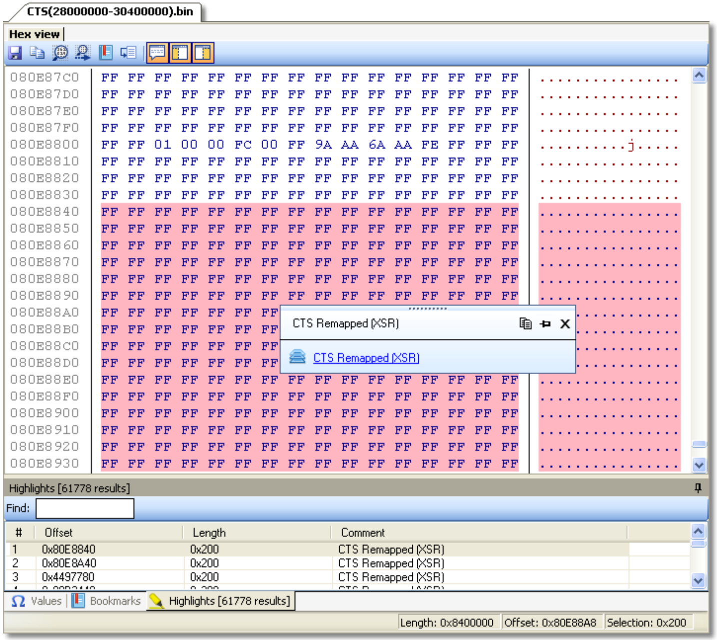


Memory ranges
MCU
CTS
CTS Remapped (XSR)

Figure 16: Memory ranges

Selecting a memory range will automatically add it to the highlights list of the displayed binary image it belongs to (located at the bottom of the Hex view tab), and will highlight the memory range portion in the displayed data.

Double clicking on any memory range item will display its content in a new Hex View tab in the data display area.



```
080E87C0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
080E87D0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
080E87E0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
080E87F0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
080E8800  FF FF 01 00 00 FC 00 FF 9A AA 6A AA FE FF FF FF  ..........j.....
080E8810  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
080E8820  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
080E8830  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
080E8840  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
080E8850  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
080E8860  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
080E8870  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
080E8880  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
080E8890  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
080E88A0  FF FF FF FF FF FF FF                                  ............
080E88B0  FF FF FF FF FF FF FF                                  ............
080E88C0  FF FF FF FF FF FF FF                                  ............
080E88D0  FF FF FF FF FF FF FF                                  ............
080E88E0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
080E88F0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
080E8900  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
080E8910  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
080E8920  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
080E8930  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
```

CTS Remapped (XSR)

CTS Remapped (XSR)

Highlights [61778 results]

Find:

#	Offset	Length	Comment
1	0x80E8840	0x200	CTS Remapped (XSR)
2	0x80E8A40	0x200	CTS Remapped (XSR)
3	0x4497780	0x200	CTS Remapped (XSR)

Length: 0x8400000 Offset: 0x80E88A8 Selection: 0x200

Figure 17: Highlighted memory range in the image Hex view tab

4.3.3.5 **File Systems**

The **File systems** item of the project tree lists all the file systems found and reconstructed out of the analyzed binary data.

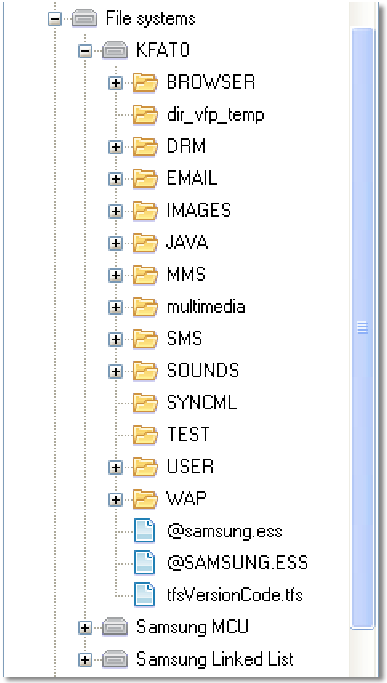
Each file system found will appear as a hard drive icon 🖴.

You can browse the file system to display folders and files by clicking the ⊞ or ⊟ icons.

NOTE: Deleted items appear as ❎.

Double clicking on any file item in the file system tree will display its content in a new Hex View tab in the data display area.

Selecting a file system item will automatically add it to the highlights list of the displayed binary image and/or memory range it belongs to (located at the bottom of the Hex view tab), and will highlight its data range portion in the displayed data.



- ⊟ File systems
  - ⊟ KFAT0
    - ⊞ BROWSER
    - dir_vfp_temp
    - ⊞ DRM
    - ⊞ EMAIL
    - ⊞ IMAGES
    - ⊞ JAVA
    - ⊞ MMS
    - ⊞ multimedia
    - ⊞ SMS
    - ⊞ SOUNDS
    - SYNCML
    - TEST
    - ⊞ USER
    - ⊞ WAP
    - @samsung.ess
    - @SAMSUNG.ESS
    - tfsVersionCode.tfs
  - ⊞ Samsung MCU
  - ⊞ Samsung Linked List

Figure 18: File systems

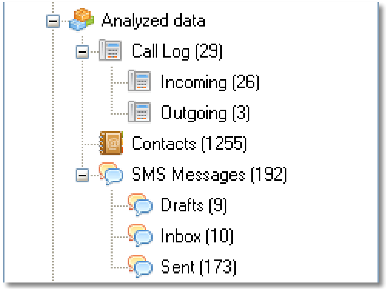
4.3.3.6 **Analyzed Data**

This **Analyzed data** item of the project tree displays phone data item groups that were found in the extracted data.

The listed of items will include:

- **Personal information**, such as calendar, contacts, notes, call log
- **Messaging items**, such as SMS, MMS, email, instant message, chat
- **Web browser items**, such as bookmarks, history, cookies
- **GPS information**, such as locations, journeys, fixes
- **Device information**, such as bluetooth pairings, SIM data

NOTE: Additional types of Analyzed Data groups may be available according to the device features and the application version.



- Analyzed data
  - Call Log (29)
    - Incoming (26)
    - Outgoing (3)
  - Contacts (1255)
  - SMS Messages (192)
    - Drafts (9)
    - Inbox (10)
    - Sent (173)

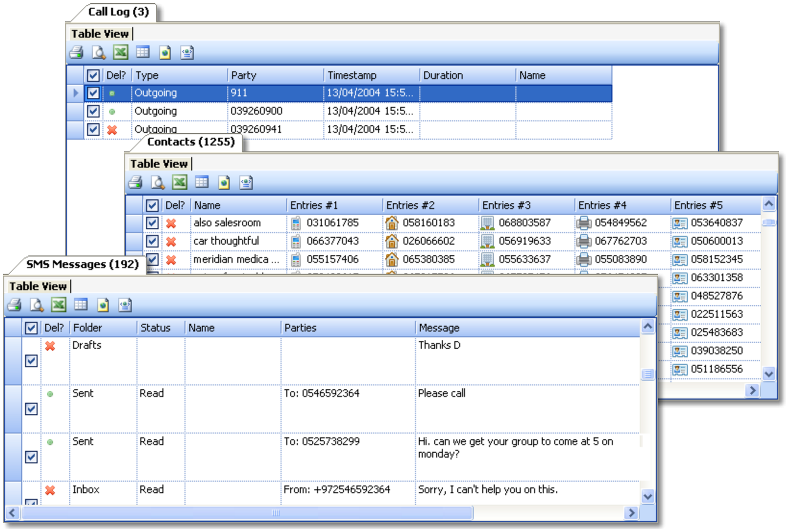
Figure 19: Analyzed Data section

A number, in parenthesis, next to each item type, shows the number of items of this type that were found in the extracted data (excluding duplicates).

Expanding any of the Analyzed Data item groups by clicking the ⊞ icon next to it, will reveal a 2nd level sorting of the logged items according to type or folder. Clicking ⊟ icon will collapse the 2nd level sorting. For example, SMS Messages will be sorted according to the sorting folders used by the messaging feature of the phone, such as: Drafts, Inbox, Outbox, Sent, etc.

Double clicking on each of the item type groups or 2nd level sorting group, will display a detailed table of all its items in the data display area. The structure and information displayed by the table will vary according to the selected item type.

Selecting any analyzed data category will automatically add it to the highlights list of the displayed binary image and/or memory range it belongs to (located at the bottom of the Hex view tab), and will highlight its data range portions in the displayed data.



Call Log (3)

Table View

☑	Del?	Type	Party	Timestamp	Duration	Name
☑	●	Outgoing	911	13/04/2004 15:5...		
☑	●	Outgoing	039260900	13/04/2004 15:5...		
☑	✖	Outgoing	039260941	13/04/2004 15:5...		

Contacts (1255)

Table View

☑	Del?	Name	Entries #1	Entries #2	Entries #3	Entries #4	Entries #5
☑	✖	also salesroom	031061785	058160183	068803587	054849562	053640837
☑	✖	car thoughtful	066377043	026066602	056919633	067762703	050600013
☑	✖	meridian medica ...	055157406	065380385	055633637	055083890	058152345
							063301358
							048527876
							022511563
							025483683
							039038250
							051186556

SMS Messages (192)

Table View

☑	Del?	Folder	Status	Name	Parties	Message
☑	✖	Drafts				Thanks D
☑	●	Sent	Read		To: 0546592364	Please call
☑	●	Sent	Read		To: 0525738299	Hi. can we get your group to come at 5 on monday?
	✖	Inbox	Read		From: +972546592364	Sorry, I can't help you on this.

Figure 20: Analyzed Data display tables

4.3.3.7 Data Files

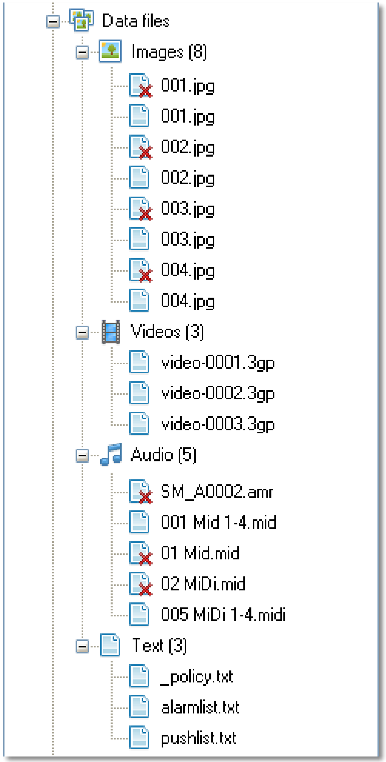
This **Data files** item of the project tree provides access to the files that were found in the extracted data, filtered according to the following file types:

- **Images** - Files that were recognized as image file formats
- **Videos** - Files that were recognized as video file formats
- **Audio** - Files that were recognized as audio file formats
- **Text** - Files that were recognized as text file formats

NOTE: Deleted items appear as ☒.

Note: New Data File groups for other common file types, can be created according to the Data Files setting. See “Data Files Settings” on page 102.

Double clicking on each of the filtering groups will display a list of the parsed items in the data display area. In addition, the tree view can be expanded to allow access to individual files. See “Working with Data Files” on page 82.



- Data files
  - Images (8)
    - ☒ 001.jpg
    - 001.jpg
    - ☒ 002.jpg
    - 002.jpg
    - ☒ 003.jpg
    - 003.jpg
    - ☒ 004.jpg
    - 004.jpg
  - Videos (3)
    - video-0001.3gp
    - video-0002.3gp
    - video-0003.3gp
  - Audio (5)
    - ☒ SM_A0002.amr
    - 001 Mid 1-4.mid
    - ☒ 01 Mid.mid
    - ☒ 02 MiDi.mid
    - 005 MiDi 1-4.midi
  - Text (3)
    - _policy.txt
    - alarmlist.txt
    - pushlist.txt

Figure 21: Data Files section

4.3.3.8 **Tags**

When the extracted data is processed, certain file types are identified and are tagged accordingly.

NOTE: The four default tags are Image, Text, Audio, and Video, and files that were identified and tagged by each of them will also show up under the **Data files** section.

You can use plug-ins or the Python shell to look for additional data segments and tag them with one of the existing tags, or log them under a new branch in the **Tags** section by applying a custom tag to them.

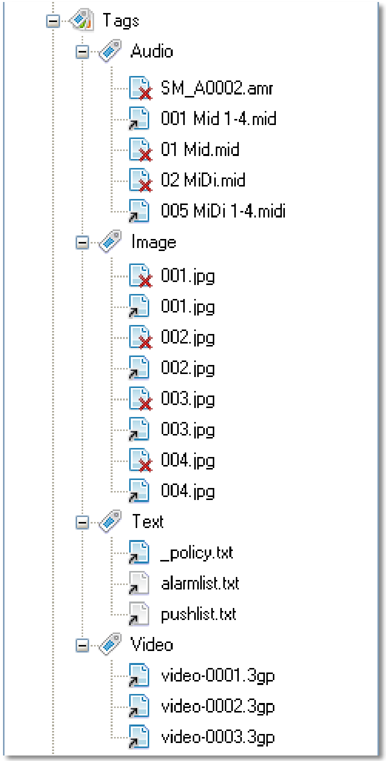
NOTE: Deleted items appear as ☒.

Double clicking a tagged item will take you to its file item under the **File systems** item.

4.3.3.9 **Reports**

Double clicking a report item listed under **Reports** will display the report file generated for the project using the application associated with the report format (ie. Internet Explorer for HTML report).

If a report has not yet been generated for this project, the **Generate Report** dialog will be displayed prompting you to generate one.



- Tags
  - Audio
    - SM_A0002.amr
    - 001 Mid 1-4.mid
    - 01 Mid.mid
    - 02 MiDi.mid
    - 005 MiDi 1-4.midi
  - Image
    - 001.jpg
    - 001.jpg
    - 002.jpg
    - 002.jpg
    - 003.jpg
    - 003.jpg
    - 004.jpg
    - 004.jpg
  - Text
    - _policy.txt
    - alarmlist.txt
    - pushlist.txt
  - Video
    - video-0001.3gp
    - video-0002.3gp
    - video-0003.3gp

Figure 22: Tags section

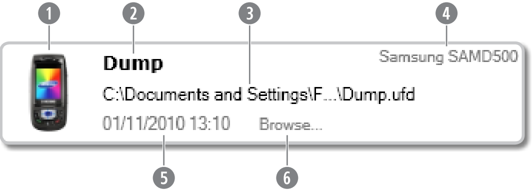
4.3.4 **Data Display Area**

Displays the content of the currently selected project tree item. A new data display panel is opened for each selected item (ex. Hex memory, list of contacts, file content, etc.). Tabs are utilized to navigate between the views.

4.3.4.1 **The Welcome tab**

The Welcome tab is automatically displayed in the data display area when the application is launched, and displays a list of the recently opened files.

Each recently opened file item in the list is displayed as a framed information group that contains the following items:



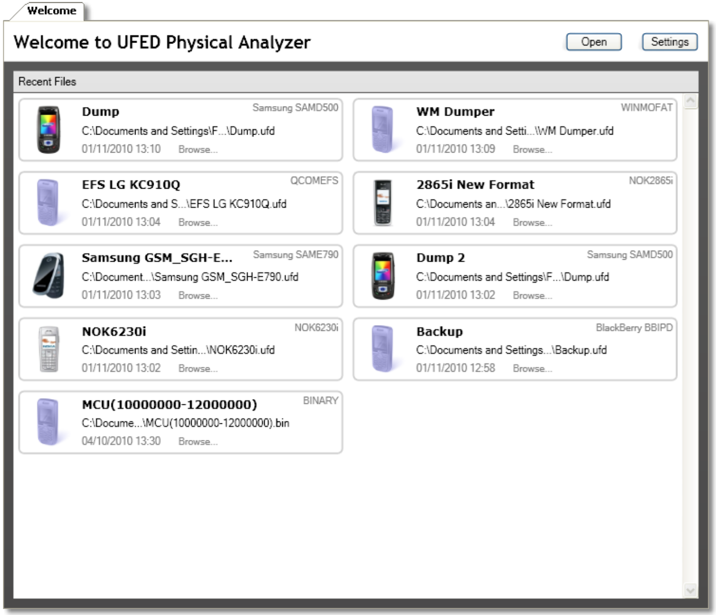
Dump

Samsung SAMD500

C:\Documents and Settings\F...\Dump.ufd

01/11/2010 13:10 Browse...

1 **Device icon** - A thumbnail image of the device from the application resources, if available. When not available a general placeholder image is used.



Welcome to UFED Physical Analyzer

Recent Files

Dump — Samsung SAMD500 — C:\Documents and Settings\F...\Dump.ufd — 01/11/2010 13:10 Browse...

WM Dumper — WINMOFAT — C:\Documents and Setti...\WM Dumper.ufd — 01/11/2010 13:09 Browse...

EFS LG KC910Q — QCOMEFS — C:\Documents and S...\EFS LG KC910Q.ufd — 01/11/2010 13:04 Browse...

2865i New Format — NOK2865i — C:\Documents an...\2865i New Format.ufd — 01/11/2010 13:04 Browse...

Samsung GSM_SGH-E... — Samsung SAME790 — C:\Document...\Samsung GSM_SGH-E790.ufd — 01/11/2010 13:03 Browse...

Dump 2 — Samsung SAMD500 — C:\Documents and Settings\F...\Dump.ufd — 01/11/2010 13:02 Browse...

NOK6230i — NOK6230i — C:\Documents and Settin...\NOK6230i.ufd — 01/11/2010 13:02 Browse...

Backup — BlackBerry BBIPD — C:\Documents and Settings...\Backup.ufd — 01/11/2010 12:58 Browse...

MCU(10000000-12000000) — BINARY — C:\Docume...\MCU(10000000-12000000).bin — 04/10/2010 13:30 Browse...

Figure 23: Welcome screen

➋ **File Name** - The name of the opened file, without the file extension.

➌ **File Path** - The file system path to the file location.

➍ **Device Model** - The identified device manufacturer and model, or BINARY in case the opened file was a binary dump.

➎ **Date and time** - The date and time stamp in which the file was opened.

➏ **Browse link** - A direct link to the file in file system.

Click on a framed item to open the recently opened files for analysis.

Click on the **Browse...** link of a recent file item to go directly to the file associated with it in the file system.

NOTE: Whenever the Welcome tab is not displayed, you can display it by selecting **View > Show Welcome Screen**.

4.3.4.2 **Hex View tab**

A new Hex View tab (screen) will appear for each binary item you open from the project tree.

The Hex View tab is comprised of the following sections:

❶ Hex data display pane

❷ Hex View toolbar

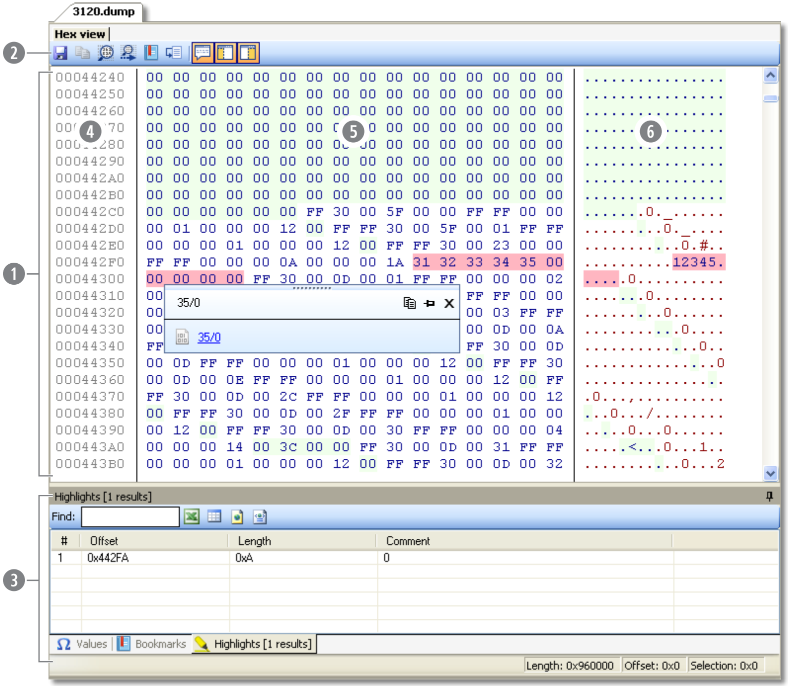
❸ Analysis Information tabs

4.3.4.2.1 **Hex Data Display Pane**

The Hex data display pane is divided into 3 sections:

❹ **Address Column** - The number information column in Hex or Decimal value, displaying the start address of each row in the Hex and ASCII representation data sections.

❺ **Hex data view column** - The Hex data of the selected item.



```
00044240  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00044250  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00044260  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00044270  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00044280  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00044290  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000442A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000442B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000442C0  00 00 00 00 00 00 FF 30 00 5F 00 00 FF FF 00 00  .......0._......
000442D0  00 01 00 00 00 12 00 FF FF 30 00 5F 00 01 FF FF  .........0._....
000442E0  00 00 00 01 00 00 00 12 00 FF FF 30 00 23 00 00  ...........0.#..
000442F0  FF FF 00 00 00 0A 00 00 00 1A 31 32 33 34 35 00  ..........12345.
00044300  00 00 00 00 FF 30 00 0D 00 01 FF FF 00 00 00 02  .....0..........
00044310  00                                  FF FF 00 00  .......0........
00044320  00                                  00 03 FF FF  .........0......
00044330  00                                  00 0D 00 0A  ...........0....
00044340  FF                                  FF 30 00 0D  .............0..
00044350  00 0D FF FF 00 00 00 01 00 00 00 12 00 FF FF 30  ...............0
00044360  00 0D 00 0E FF FF 00 00 00 01 00 00 00 12 00 FF  ................
00044370  FF 30 00 0D 00 2C FF FF 00 00 00 01 00 00 00 12  .0...,..........
00044380  00 FF FF 30 00 0D 00 2F FF FF 00 00 00 01 00 00  ...0.../........
00044390  00 12 00 FF FF 30 00 0D 00 30 FF FF 00 00 00 04  .....0...0......
000443A0  00 00 00 14 00 3C 00 00 FF 30 00 0D 00 31 FF FF  .....<...0...1..
000443B0  00 00 00 01 00 00 00 12 00 FF FF 30 00 0D 00 32  ...........0...2
```

#	Offset	Length	Comment
1	0x442FA	0xA	0

Length: 0x960000 | Offset: 0x0 | Selection: 0x0

Figure 24: Hex View tab (screen)

❻ **ASCII representation view column** - The ASCII representation of the Hex data.

4.3.4.2.2 **Hex Data Toolbar**

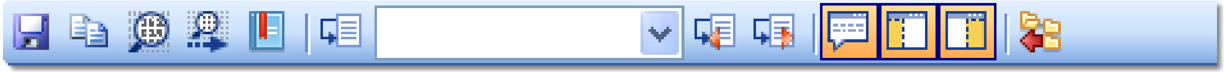


Figure 25: The Hex View toolbar

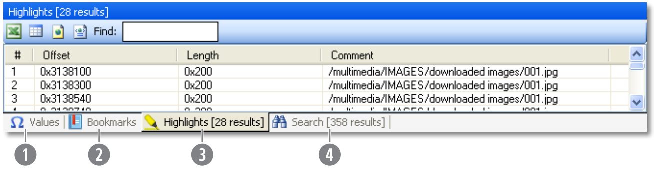
Located at the top of the Hex data display pane, the Hex data toolbar provides access to the following functions related to the data displayed.

	Save	Click to save the entire memory dump to a local folder.
	Copy Selection	Copy the currently selected content of the Hex View tab to the clipboard.
	Find	Displays the **Find** dialog to search for all occurrences of specified information in the displayed Hex display pane.
	Find Next	Displays the **Find** dialog with the search parameters used in the latest search.
	Add Bookmark	Bookmark the currently selected content of the Hex display pane.
	Go To	Redirect the offset to specific address in the content of the Hex display pane. See "Redirecting the Offset" on page 86.
	Enable Info Frame	Toggles on/off the display of floating information frame at the cursor location.
	Show Address	Toggles on/off the left address column display.

	Show ASCII view	Toggles on/off the right ASCII representation column display.
	Locate File in Tree	Selects the displayed file in the File Systems section of the Project Tree.

4.3.4.2.3 **Analysis Information Tabs**

Located under the Hex Data display pane by default, the **Analysis Information** tabs displays the following types of information related directly to the displayed Hex data:



#	Offset	Length	Comment
1	0x3138100	0x200	/multimedia/IMAGES/downloaded images/001.jpg
2	0x3138300	0x200	/multimedia/IMAGES/downloaded images/001.jpg
3	0x3138540	0x200	/multimedia/IMAGES/downloaded images/001.jpg

Figure 26: Analysis Information tabs

1. **Values** - A wide array of value interpretations, such as 8, 16, 32 and 64 bit, various String encoding, Date & Time formats, and more, calculated on the fly for the currently selected data in the Hex view.
2. **Bookmarks** - A list of bookmarks added in the displayed Hex data.
3. **Highlights** - A list of content segments markups highlighted in the displayed Hex data. The number of highlight results is shown in brackets next to the tab name.
4. **Search** - Displays results of a search in the displayed Hex data. A new search results tab will open for each search query performed. The number of results for each search is shown in brackets next to the tab name.

4.3.4.2.4 **Rearranging the Analysis Information Tabs**

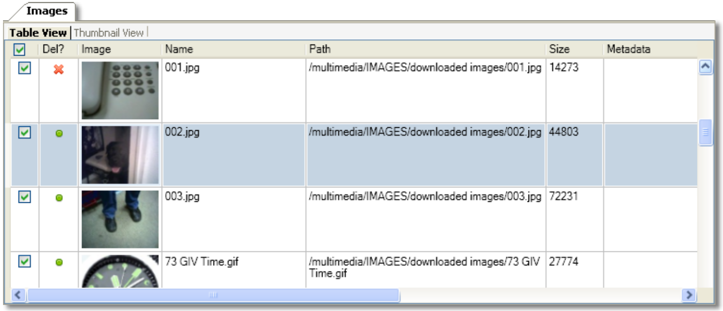
You can rearrange the display of the Analysis Information to suit your preference:

- Double click the header strip of the section to display the entire section as a floating panel. Double click the floating panel header strip to dock it back to the default location (at the bottom of the Hex View tab).
- Double click the name label of any tab to display it as a floating panel. Double click the floating panel header strip to dock it back to the original location.
- Drag the name label or floating panel over any of the docking labels that appear to dock it at that location in the Hex View tab.

4.3.4.3 **Data Items View tab**

A Data Item View tab will be added to the data display area whenever you double click on a data item group located under the **Analyzed Data** or **Data Files** sections of the project tree.

The Data Item View tab displays a list of all the files of a specific type (images, videos, audio, or text) that where found during the data analysis process.



☑	Del?	Image	Name	Path	Size	Metadata
☑	✖		001.jpg	/multimedia/IMAGES/downloaded images/001.jpg	14273	
☑	●		002.jpg	/multimedia/IMAGES/downloaded images/002.jpg	44803	
☑	●		003.jpg	/multimedia/IMAGES/downloaded images/003.jpg	72231	
☑	●		73 GIV Time.gif	/multimedia/IMAGES/downloaded images/73 GIV Time.gif	27774	

Figure 27: Files View tab

NOTE: Image files can be displayed either in **Table view** or **Thumbnail view**, using the two display option tabs at the top of the files list display pane.

Chapter 5: **Physical Analyzer - Basic Use**

5.1 Opening File for Analysis

1. If the phone data was extracted to a removable media, connect the USB disk drive or SD card containing the extracted data to a PC with an activated running copy of UFED Physical Analyzer application.

   NOTE: For faster processing, copy the extracted data folder from the removable media to the PC, and open directly from the PC.

2. From the application menu, select **File** > **Open**, or click the **Open** button on the application toolbar.
3. Navigate to the location of the extracted phone data folder, and open it.
4. In the displayed **Open** dialog, select the data extraction file.

   By default, the **Open** dialog is set to display UFED Dump files (*.ufd) which is the information mapping file of the extracted phone data.

   Additional formats available for selection from the **Files of Type** list of the Open dialog include:

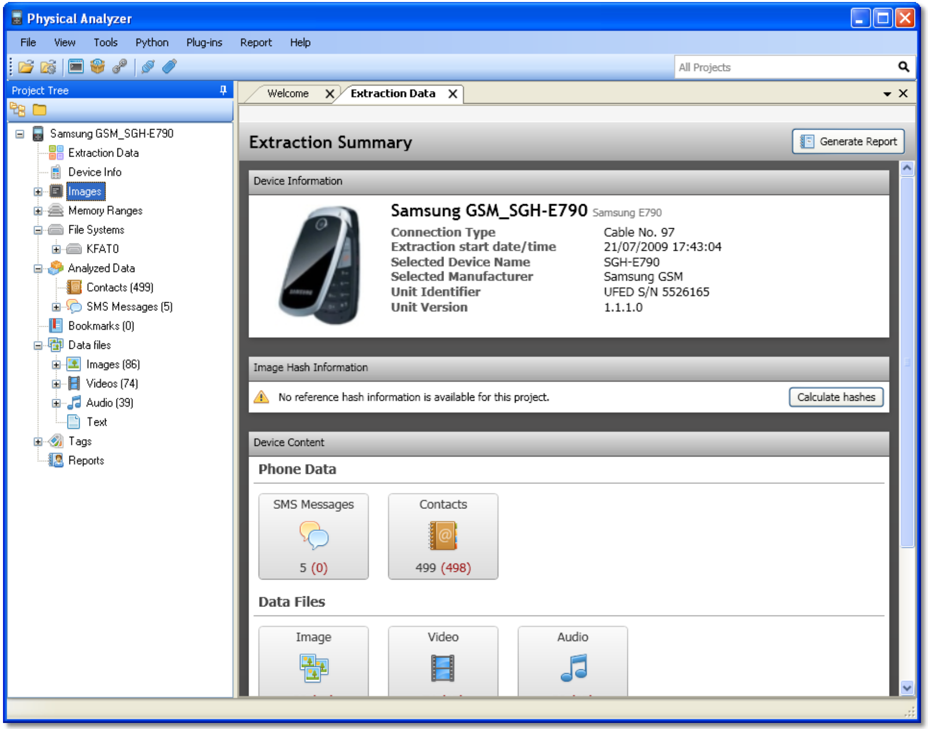
   - UFED report (*.xml). Logical reports generated by the UFED unit.
   - Binary files (*.bin). Raw binary files or any hex dump generated by another application.

   NOTE: Opening a binary file will only allow hex dump view, with no file system or data analysis. However, you will still be able to perform your own searches and analysis using the provided tools.

- Proprietary phone data. File formats such as the Nokia PM (*.pm) and the BlackBerry backup file (*.ipd), which are proprietary file formats of specific phones/vendors file systems.

5. Click **Open**.

   The data analysis process will begin and run for several seconds. At the end of the process, a new project will be added in the Project Tree area, and the Extraction Summary screen will display in the Data Display area.



Extraction Summary

Device Information

Samsung GSM_SGH-E790 Samsung E790

Connection Type: Cable No. 97
Extraction start date/time: 21/07/2009 17:43:04
Selected Device Name: SGH-E790
Selected Manufacturer: Samsung GSM
Unit Identifier: UFED S/N 5526165
Unit Version: 1.1.1.0

Image Hash Information

No reference hash information is available for this project.

Device Content

Phone Data

SMS Messages: 5 (0)
Contacts: 499 (498)

Data Files

Figure 28: New opened project

5.2 Searching for Information in the Project

The search field at the top right of the application window allows you to search for information in the entire project or projects that are currently open in the application.

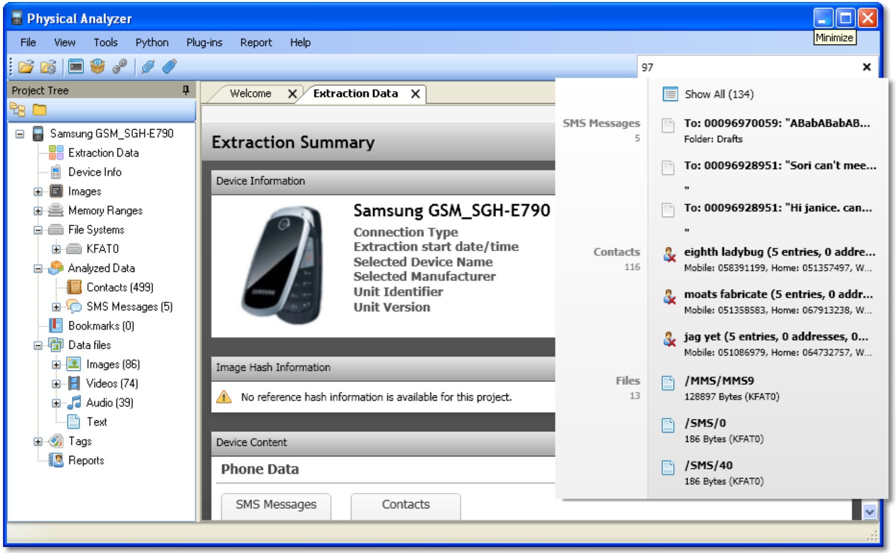
To search for contents, type the search string in the field.

5.2.1 The Quick Results List

A quick list of matching results will appear under the search field.

Sorting categories along the left edge of the quick results list, sort the results according to their type (such as SMS Messages, Contacts, Files, etc.), and display the number of matching results found in each type category.

Selecting a result from the list will display it in the Data Display area using the appropriate information display tab.



No reference hash information is available for this project.

To: 00096970059: "ABabABabAB...
Folder: Drafts

To: 00096928951: "Sori can't mee...
"

To: 00096928951: "Hi janice. can...
"

eighth ladybug (5 entries, 0 addre...
Mobile: 058391199, Home: 051357497, W...

moats fabricate (5 entries, 0 addr...
Mobile: 051358583, Home: 067913238, W...

jag yet (5 entries, 0 addresses, 0...
Mobile: 051086979, Home: 064732757, W...

/MMS/MMS9
128897 Bytes (KFAT0)

/SMS/0
186 Bytes (KFAT0)

/SMS/40
186 Bytes (KFAT0)

Figure 29: The contents search quick results list

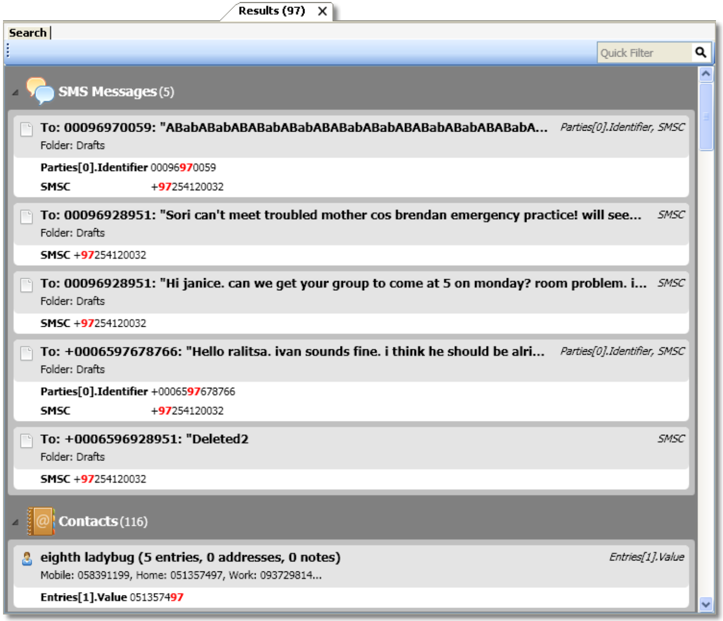
5.2.2 The Results Tab

Selecting **Show All** from the top of the quick results list will display a **Results** tab in the Data Display area, listing all the matching search results. The matching string in each found item will be colored in red.

As in the quick results list, the **Results** tab list will display the found items sorted according to type categories.

To make it easier to scroll through the results:

- Click on the small triangle at the left of each sorting category header to collapse or expand the items list of the category, thus shortening the list and limiting the displayed items to the required types.
- Use the **Quick Filter** field at the top right of the **Results** tab to filter the found items by entering a quick filtering string.



SMS Messages (5)

To: 00096970059: "ABabABabABABabABabABABabABabABABabABabABABabA... *Parties[0].Identifier, SMSC*
Folder: Drafts
Parties[0].Identifier 00096970059
SMSC +97254120032

To: 00096928951: "Sori can't meet troubled mother cos brendan emergency practice! will see... *SMSC*
Folder: Drafts
SMSC +97254120032

To: 00096928951: "Hi janice. can we get your group to come at 5 on monday? room problem. i... *SMSC*
Folder: Drafts
SMSC +97254120032

To: +0006597678766: "Hello ralitsa. ivan sounds fine. i think he should be alri... *Parties[0].Identifier, SMSC*
Folder: Drafts
Parties[0].Identifier +0006597678766
SMSC +97254120032

To: +0006596928951: "Deleted2 *SMSC*
Folder: Drafts
SMSC +97254120032

Contacts (116)

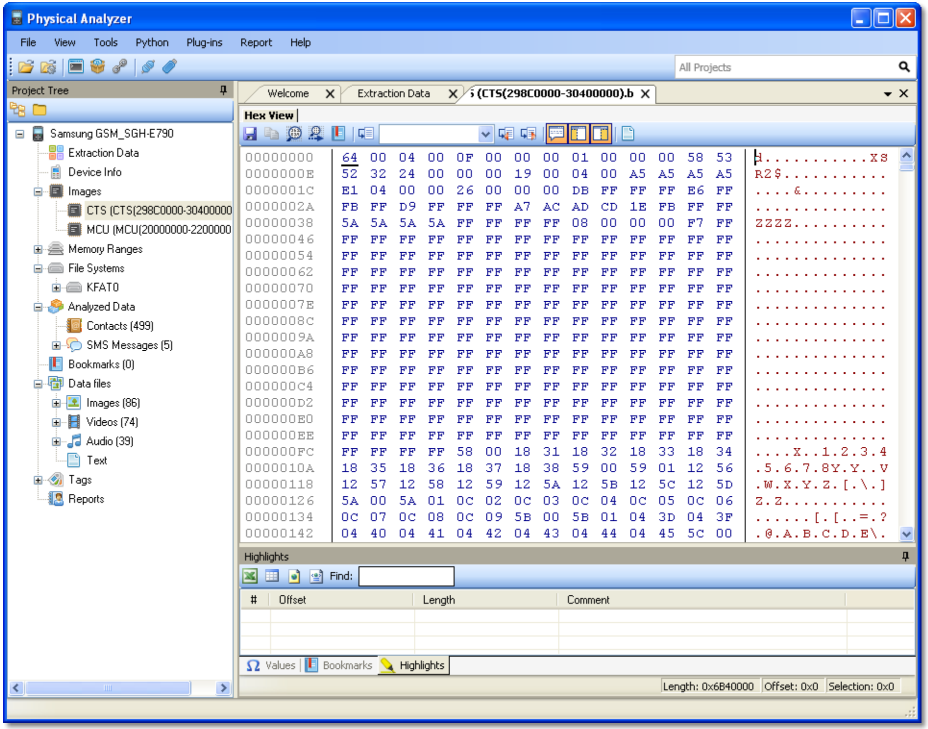
eighth ladybug (5 entries, 0 addresses, 0 notes) *Entries[1].Value*
Mobile: 058391199, Home: 051357497, Work: 093729814...
Entries[1].Value 051357497

Figure 30: The contents search Results tab

5.3 Browsing the Hex Dump

Double clicking on a binary hex dump in the **Project Tree** will display its content in a **Hex View** tab within the data display area.

You can display the extracted Hex dump by clicking on the image links displayed in the Extraction Log area at the bottom of the Extraction Summary tab.



Samsung GSM_SGH-E790
- Extraction Data
- Device Info
- Images
  - CTS (CTS(298C0000-30400000
  - MCU (MCU(20000000-2200000
- Memory Ranges
- File Systems
  - KFAT0
- Analyzed Data
  - Contacts (499)
  - SMS Messages (5)
- Bookmarks (0)
- Data files
  - Images (86)
  - Videos (74)
  - Audio (39)
  - Text
- Tags
- Reports

```
00000000  64 00 04 00 0F 00 00 00 01 00 00 00 58 53  d...........XS
0000000E  52 32 24 00 00 00 19 00 04 00 A5 A5 A5 A5  R2$...........
0000001C  E1 04 00 00 26 00 00 00 DB FF FF FF E6 FF  ....&.........
0000002A  FB FF D9 FF FF FF A7 AC AD CD 1E FB FF FF  ..............
00000038  5A 5A 5A 5A FF FF FF FF 08 00 00 00 F7 FF  ZZZZ..........
00000046  FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ..............
00000054  FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ..............
00000062  FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ..............
00000070  FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ..............
0000007E  FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ..............
0000008C  FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ..............
0000009A  FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ..............
000000A8  FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ..............
000000B6  FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ..............
000000C4  FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ..............
000000D2  FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ..............
000000E0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ..............
000000EE  FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ..............
000000FC  FF FF FF FF 58 00 18 31 18 32 18 33 18 34  ....X..1.2.3.4
0000010A  18 35 18 36 18 37 18 38 59 00 59 01 12 56  .5.6.7.8Y.Y..V
00000118  12 57 12 58 12 59 12 5A 12 5B 12 5C 12 5D  .W.X.Y.Z.[.\.]
00000126  5A 00 5A 01 0C 02 0C 03 0C 04 0C 05 0C 06  Z.Z...........
00000134  0C 07 0C 08 0C 09 5B 00 5B 01 04 3D 04 3F  ......[.[..=.?
00000142  04 40 04 41 04 42 04 43 04 44 04 45 5C 00  .@.A.B.C.D.E\.
```

#	Offset	Length	Comment

Length: 0x6B40000 Offset: 0x0 Selection: 0x0

Figure 31: Browsing the Hex dump

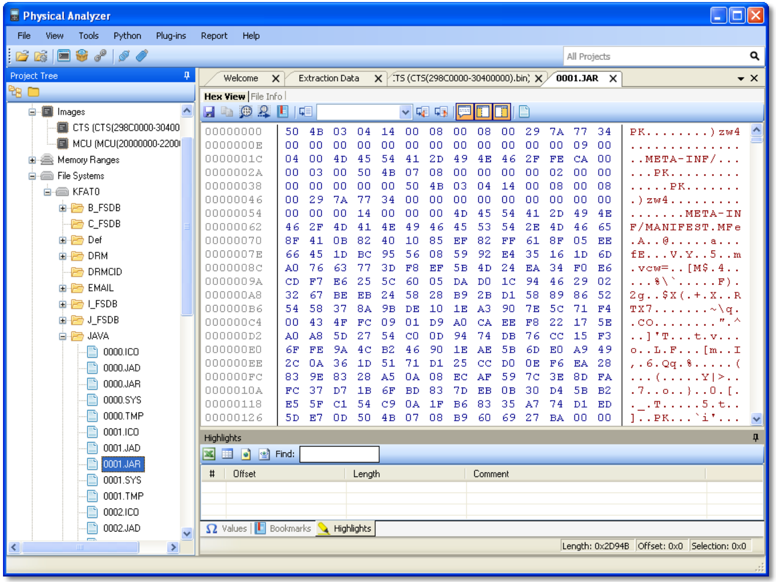
5.4 Browsing the File System

The UFED Physical Analyzer has the ability to reconstruct and display the phone file system as a tree structure of folders and files.

To browse the file system:

1. Click the ⊞ icon at every node to expand the tree display under it.
2. Continue drilling down in the file system tree to explore its content.
3. When you reach a file:
4. Double click on it to display its information in the data display area.

   The number information tabs displayed for the file will change according to the file type. For example, an unknown file may display only the **Hex View** and **File info** tabs, while a jpeg image may display additional **Image view** and **Meta data** tabs. The default view is the **Hex view**.

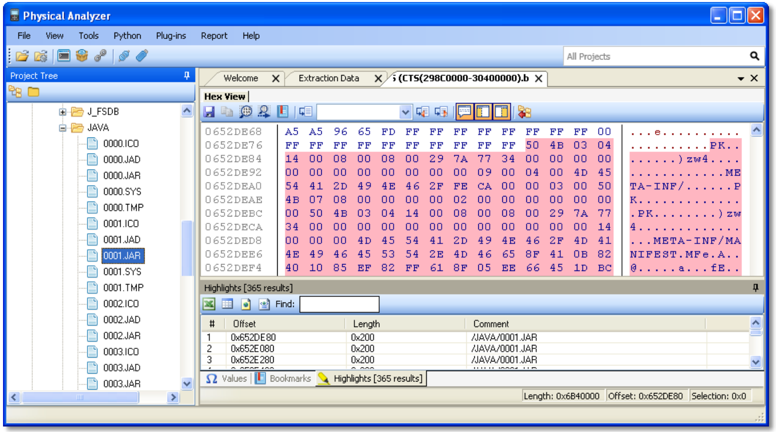


```
00000000  50 4B 03 04 14 00 08 00 08 00 29 7A 77 34  PK........)zw4
0000000E  00 00 00 00 00 00 00 00 00 00 00 00 09 00  ..............
0000001C  04 00 4D 45 54 41 2D 49 4E 46 2F FE CA 00  ..META-INF/...
0000002A  00 03 00 50 4B 07 08 00 00 00 00 02 00 00  ...PK.........
00000038  00 00 00 00 00 50 4B 03 04 14 00 08 00 08  .....PK.......
00000046  00 29 7A 77 34 00 00 00 00 00 00 00 00 00  .)zw4.........
00000054  00 00 00 14 00 00 00 4D 45 54 41 2D 49 4E  .......META-IN
00000062  46 2F 4D 41 4E 49 46 45 53 54 2E 4D 46 65  F/MANIFEST.MFe
00000070  8F 41 0B 82 40 10 85 EF 82 FF 61 8F 05 EE  .A..@.....a...
0000007E  66 45 1D BC 95 56 08 59 92 E4 35 16 1D 6D  fE...V.Y..5..m
0000008C  A0 76 63 77 3D F8 EF 5B 4D 24 EA 34 F0 E6  .vcw=..[M$.4..
0000009A  CD F7 E6 25 5C 60 05 DA D0 1C 94 46 29 02  ...%\`.....F).
000000A8  32 67 BE EB 24 58 28 B9 2B D1 58 89 86 52  2g..$X(.+.X..R
000000B6  54 58 37 8A 9B DE 10 1E A3 90 7E 5C 71 F4  TX7.......~\q.
000000C4  00 43 4F FC 09 01 D9 A0 CA EE F8 22 17 5E  .CO........".^
000000D2  A0 A8 5D 27 54 C0 0D 94 74 DB 76 CC 15 F3  ..]'T...t.v...
000000E0  6F FE 9A 4C B2 46 90 1E AE 5B 6D E0 A9 49  o..L.F...[m..I
000000EE  2C 0A 36 1D 51 71 D1 25 CC D0 0E F6 EA 28  ,.6.Qq.%.....(
000000FC  83 9E 83 28 A5 0A 08 EC AF 59 7C 3E 8D FA  ...(.....Y|>..
0000010A  FC 37 D7 1B 6F BD 83 7D EB 0B 30 D4 5B B2  .7..o..}..0.[.
00000118  E5 5F C1 54 C9 0A 1F B6 83 35 A7 74 D1 ED  ._.T.....5.t..
00000126  5D E7 0D 50 4B 07 08 B9 60 69 27 BA 00 00  ]..PK...`i'...
```

Length: 0x2D94B | Offset: 0x0 | Selection: 0x0

Figure 32: File Hex dump display (after double clicking on the file)

While the Hex dump of an image is displayed in the Data Display area, selecting a file under the file system tree will highlight the data portion of this file in the Hex dump data. The **Highlights** list, under the Hex viewer, will display the data chunks in the Hex dump from which this file is comprised.



```
0652DE68  A5 A5 96 65 FD FF FF FF FF FF FF FF FF 00  ...e..........
0652DE76  FF FF FF FF FF FF FF FF FF FF 50 4B 03 04  ..........PK..
0652DE84  14 00 08 00 08 00 29 7A 77 34 00 00 00 00  ......)zw4....
0652DE92  00 00 00 00 00 00 00 00 09 00 04 00 4D 45  ............ME
0652DEA0  54 41 2D 49 4E 46 2F FE CA 00 00 03 00 50  TA-INF/......P
0652DEAE  4B 07 08 00 00 00 00 02 00 00 00 00 00 00  K.............
0652DEBC  00 50 4B 03 04 14 00 08 00 08 00 29 7A 77  .PK........)zw
0652DECA  34 00 00 00 00 00 00 00 00 00 00 00 00 14  4.............
0652DED8  00 00 00 4D 45 54 41 2D 49 4E 46 2F 4D 41  ...META-INF/MA
0652DEE6  4E 49 46 45 53 54 2E 4D 46 65 8F 41 0B 82  NIFEST.MFe.A..
0652DEF4  40 10 85 EF 82 FF 61 8F 05 EE 66 45 1D BC  @.....a...fE..
```

#	Offset	Length	Comment
1	0x652DE80	0x200	/JAVA/0001.JAR
2	0x652E080	0x200	/JAVA/0001.JAR
3	0x652E280	0x200	/JAVA/0001.JAR

Length: 0x6B40000 Offset: 0x652DE80 Selection: 0x0

Figure 33: File data display in the extracted Hex dump

Files in the reconstructed file system will display one of the following icons:

📄	Existing file found in the file system
📄✗	Deleted file data found in the file system

5.5 Browsing the Analyzed Data

The **Analyzed Data** and **Data Files** sections of the project tree display data items that were found in the extracted device data during the analysis process.

The difference between item types grouped under **Analyzed Data** to those grouped under **Data Files** is that **Analyzed Data** item types are related to phone specific features such as Contacts, SMS Messages, Call Logs, and other, while **Data Files** item types are data and media files in common or known file formats, used by devices and computers, such as image, video, audio, or text files.

5.5.1 Analyzed Data

Double clicking on an Analyzed Data group, will add a data list tab to the Data Display area, listing all items of this type found in the extracted data.

The structure and content displayed by the list table will vary according to the selected item type:

For the complete list of Analyzed Data item types, see "Analyzed Data" on page 38.

5.5.2 Data Files

Data files are image, video, audio or text files. Additional data files groups will display according to the Data Files settings. See "Data Files Settings" on page 102.

Double clicking on any data files group will display the list of the data file items (images, videos, etc.) that were found in the extracted data.

For each of the data file types, the table list includes the following fields:

Checkbox	Indicates whether to include (checked) or exclude (unchecked) the item in the report generated.
Del?	An icon indicating if the data file was deleted (red "x" ✖), not deleted (green dot ●), or has an unknown status (gray dot ●).
Image	A thumbnail of the image or an icon of the file type.
Name	The file name.
Path	The root path of the data file.
Size	The size of file.
Metadata	Additional metadata of the data file.
Created	The creation time stamp of the data file.
Modified	The modification time stamp of the data file.
Accessed	The last access time stamp of the data file.

NOTE: Image files can be displayed either in **Table view** or **Thumbnail view**, using the two display option tabs at the top of the files list display pane.

Double clicking on an item record (table row) will add a Hex Viewer tab with the Hex data of the selected file to the Data Display area.

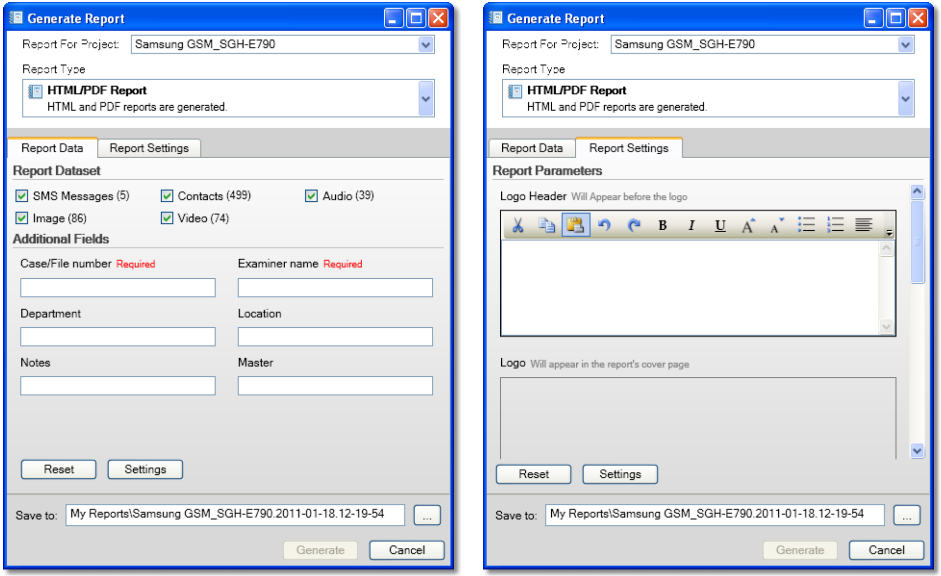
5.6 Generating Reports

You can generate a summary report of all information found in the physical dump by:

- Selecting **Report > Generate Report** from the application menu.
- Clicking the **Generate Report** button in the top right corner of the Welcome tab.
- If a report was not previously generated, double clicking on **Reports** section in the **Project Tree**.

Using any of these methods will display the **Generate Report** dialog, where you are prompted to provide the following information:

- **Report For Project** - A list of the currently opened projects. Select the project for which the report will be generated.



Generate Report

Report For Project: Samsung GSM_SGH-E790

Report Type

HTML/PDF Report
HTML and PDF reports are generated.

Report Data | Report Settings

Report Dataset

☑ SMS Messages (5) ☑ Contacts (499) ☑ Audio (39)
☑ Image (86) ☑ Video (74)

Additional Fields

Case/File number Required
Examiner name Required
Department
Location
Notes
Master

Reset Settings

Save to: My Reports\Samsung GSM_SGH-E790.2011-01-18.12-19-54 ...

Generate Cancel

Generate Report

Report For Project: Samsung GSM_SGH-E790

Report Type

HTML/PDF Report
HTML and PDF reports are generated.

Report Data | Report Settings

Report Parameters

Logo Header Will Appear before the logo

Logo Will appear in the report's cover page

Reset Settings

Save to: My Reports\Samsung GSM_SGH-E790.2011-01-18.12-19-54 ...

Generate Cancel

Figure 34: The Generate Report dialog

- **Report Type** - The file format of the generated report. Select from: HTML, MS Excel spreadsheet (.xlsx), or XML.
- **Report Data:**
  - **Report Dataset** - The **Analyzed Data** and **Data Files** section that will be included in the report. Only checked data types will be included in the generated report.
  - **Additional Fields** - Additional useful information fields added by the user in the **Additional Report Fields** settings. See "Additional Report Fields" on page 108.

    Case/File number, Examiner name, Department, Location, and Notes, are 5 additional default fields, from which, the Case/File number and Examiner name are set as required fields. You can edit these fields and change their attributes in the report settings. See "Additional Report Fields" on page 108.

    Click on the **Settings** button to jump directly into the **Additional Report Fields** settings to edit existing fields or add more fields. The changes and new fields will be automatically applied to the open **Generate Report** dialog when you click **Apply** or click **OK** and return to the **Generate Report** dialog.

    Use the **Reset** button to clear all the information entered in the fields, and set them back to their default values.
- **Report Settings** - The logo header, Image, and footer, sections page breaks, PDF generation, and item totals display settings of the report.

  The default contents and options of these settings are set by the **Report Defaults** setting of the application. See "Report Defaults" on page 110.

Click on the **Settings** button to jump directly into the **Report Defaults** settings to edit the contents and options. The changes will be automatically applied to the open **Generate Report** dialog when you click **Apply** or click **OK** and return to the **Generate Report** dialog.

Use the **Reset** button to clear all changes made, and set the contents and options back to their default values.

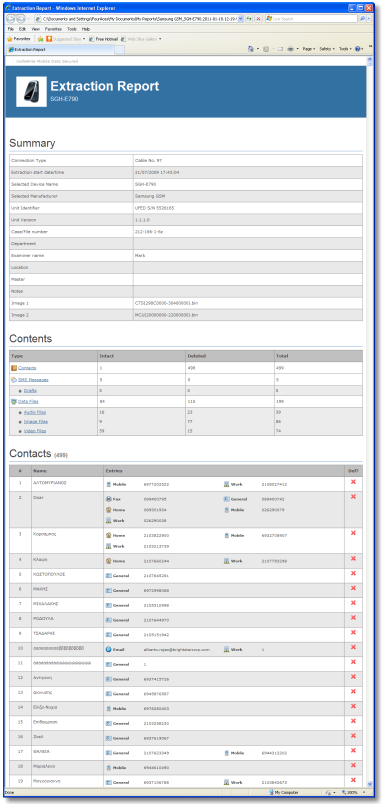
- **Save to** - The path and folder name to which the generated report file will be saved. Click the ... button to set a different path. The default target folder name will be constructed from the project name and the date and time it was generated (for example, Samsung GSM_SGH-E790.2011-01-18.12-19-84).

Click **Generate** to generate the new report.

Note: The **Generate** button will not be enabled until all the required fields are filled.

When the report generation ends successfully, you will be prompted to open the generated report file. The file will be opened using the associated application to the file format installed in the workstation.

Once a report has been generated for the project, it can be accessed from the **Reports** section in the project tree. Double clicking on any of the generated reports will open it in the associated application installed in the workstation. Right clicking any of the generated reports will allow you to open the report file or select **Open containing folder** to browse the files and folders of the report.


Extraction Report - Windows Internet Explorer
C:\Documents and Settings\FourAces\My Documents\My Reports\Samsung GSM_SGH-E790.2011-01-18.12-19-
Live Search
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Free Hotmail
Web Slice Gallery
Extraction Report
Page
Safety
Tools
Done
My Computer
100%

CelleBrite Mobile Data Secured

Extraction Report
SGH-E790

Summary

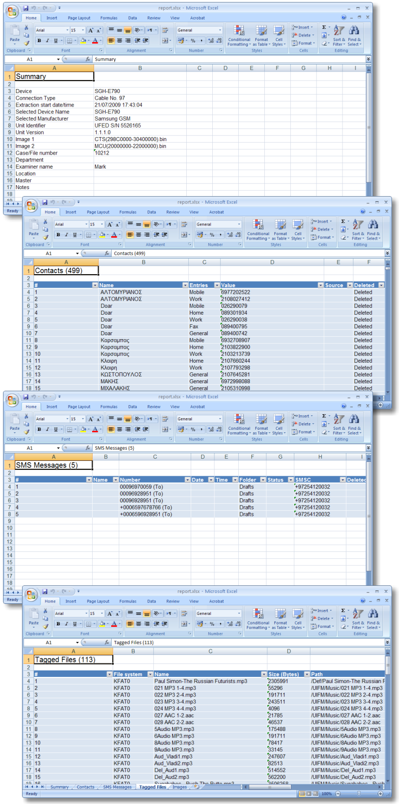
Connection Type	Cable No. 97
Extraction start date/time	21/07/2009 17:43:04
Selected Device Name	SGH-E790
Selected Manufacturer	Samsung GSM
Unit Identifier	UFED S/N 5526165
Unit Version	1.1.1.0
Case/File number	212-166-1-6z
Department	
Examiner name	Mark
Location	
Master	
Notes	
Image 1	CTS(298C0000-30400000).bin
Image 2	MCU(20000000-22000000).bin

Contents

Type	Intact	Deleted	Total
Contacts	1	498	499
SMS Messages	5	0	5
● Drafts	5	0	5
Data Files	84	115	199
● Audio Files	16	23	39
● Image Files	9	77	86
● Video Files	59	15	74

Contacts (499)

#	Name	Entries				Del?
1	ΑΛΤΟΜΥΡΙΑΝΟΣ	Mobile	6977202522	Work	2108027412	✗
2	Doar	Fax Home Work	089400795 089301934 026290038	General Mobile	089400742 026290079	✗
3	Καρσαμπας	Home Work	2103822900 2103213739	Mobile	6932708907	✗
4	Κλαιρη	Home	2107660244	Work	2107793298	✗
5	ΚΩΣΤΟΠΟΥΛΟΣ	General	2107645281			✗
6	ΜΑΚΗΣ	General	6972998088			✗
7	ΜΙΧΑΛΑΚΗΣ	General	2105310998			✗
8	ΡΟΔΟΥΛΑ	General	2107644970			✗
9	ΤΣΑΔΑΡΗΣ	General	2105151942			✗
10	ααααααααααββββββββββ	Email	alberto.rojas@brightstarcorp.com	Work	1	✗
11	άάάάάάάάάάώώώώώώώώώώ	General	1			✗
12	Αντιγονη	General	6937415726			✗
13	Διονυσης	General	6945876587			✗
14	Ελιζα-Νυχια	Mobile	6978280403			✗
15	Επιθεωρηση	General	2103258230			✗
16	Ζοελ	General	6937619067			✗
17	ΘΑΛΕΙΑ	General	2107623349	Mobile	6944312202	✗
18	Μαριαλενα	Mobile	6944610490			✗
19	Μογγογιαννη	General	6937106788	Work	2103842673	✗



Summary

	A	B
1	Summary	
2		
3	Device	SGH-E790
4	Connection Type	Cable No. 97
5	Extraction start date/time	21/07/2009 17:43:04
6	Selected Device Name	SGH-E790
7	Selected Manufacturer	Samsung GSM
8	Unit Identifier	UFED S/N 5526165
9	Unit Version	1.1.1.0
10	Image 1	CTS(298C0000-30400000).bin
11	Image 2	MCU(20000000-22000000).bin
12	Case/File number	10212
13	Department	
14	Examiner name	Mark
15	Location	
16	Master	
17	Notes	

Contacts (499)

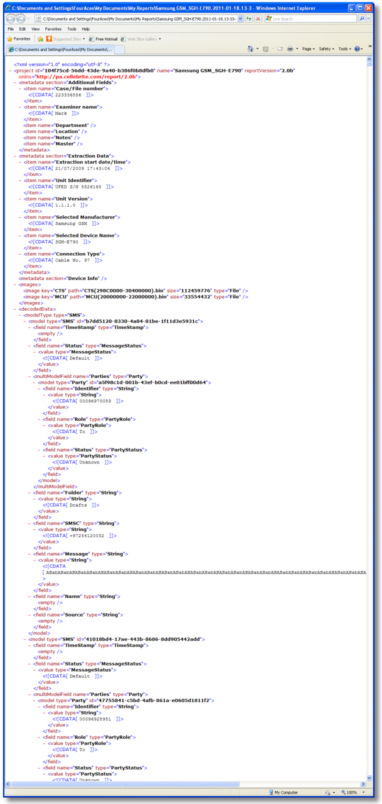
#	Name	Entries	Value	Source	Deleted
1	ΑΛΤΟΜΥΡΙΑΝΟΣ	Mobile	6977202522		Deleted
2	ΑΛΤΟΜΥΡΙΑΝΟΣ	Work	2108027412		Deleted
3	Doar	Mobile	026290079		Deleted
4	Doar	Home	089301934		Deleted
5	Doar	Work	026290038		Deleted
6	Doar	Fax	089400795		Deleted
7	Doar	General	089400742		Deleted
8	Καρσαμπας	Mobile	6932708907		Deleted
9	Καρσαμπας	Home	2103822900		Deleted
10	Καρσαμπας	Work	2103213739		Deleted
11	Κλαιρη	Home	2107660244		Deleted
12	Κλαιρη	Work	2107793298		Deleted
13	ΚΩΣΤΟΠΟΥΛΟΣ	General	2107645281		Deleted
14	ΜΑΚΗΣ	General	6972998088		Deleted
15	ΜΙΧΑΛΑΚΗΣ	General	2105310998		Deleted

SMS Messages (5)

#	Name	Number	Date	Time	Folder	Status	SMSC	Deleted
1		00096970059 (To)			Drafts		+97254120032	
2		00096928951 (To)			Drafts		+97254120032	
3		00096928951 (To)			Drafts		+97254120032	
4		+0006597678766 (To)			Drafts		+97254120032	
5		+0006596928951 (To)			Drafts		+97254120032	

Tagged Files (113)

#	File system	Name	Size (Bytes)	Path
1	KFAT0	Paul Simon-The Russian Futurists.mp3	2305991	/Def/Paul Simon-The Russian F
2	KFAT0	021 MP3 1-4.mp3	55296	/UIFM/Music/021 MP3 1-4.mp3
3	KFAT0	022 MP3 2-4.mp3	191711	/UIFM/Music/022 MP3 2-4.mp3
4	KFAT0	023 MP3 3-4.mp3	243511	/UIFM/Music/023 MP3 3-4.mp3
5	KFAT0	024 MP3 4-4.mp3	4096	/UIFM/Music/024 MP3 4-4.mp3
6	KFAT0	027 AAC 1-2.aac	21785	/UIFM/Music/027 AAC 1-2.aac
7	KFAT0	028 AAC 2-2.aac	46537	/UIFM/Music/028 AAC 2-2.aac
8	KFAT0	5Audio MP3.mp3	175488	/UIFM/Music/5Audio MP3.mp3
9	KFAT0	6Audio MP3.mp3	191711	/UIFM/Music/6Audio MP3.mp3
10	KFAT0	8Audio MP3.mp3	78417	/UIFM/Music/8Audio MP3.mp3
11	KFAT0	9Audio MP3.mp3	33145	/UIFM/Music/9Audio MP3.mp3
12	KFAT0	Aud_Vladi1.mp3	247607	/UIFM/Music/Aud_Vladi1.mp3
13	KFAT0	Aud_Vladi2.mp3	82513	/UIFM/Music/Aud_Vladi2.mp3
14	KFAT0	Del_Aud1.mp3	514552	/UIFM/Music/Del_Aud1.mp3
15	KFAT0	Del_Aud2.mp3	562200	/UIFM/Music/Del_Aud2.mp3


C:\Documents and Settings\FourAces\My Documents\My Reports\Samsung GSM_SGH-E790.2011-01-18.13-3 - Windows Internet Explorer
C:\Documents and Settings\FourAces\My Documents\My Reports\Samsung GSM_SGH-E790.2011-01-18.13-33-
Live Search
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Free Hotmail
Web Slice Gallery
C:\Documents and Settings\FourAces\My Documents\...
Page
Safety
Tools
My Computer
100%

```
  <?xml version="1.0" encoding="utf-8" ?>
- <project id="104f75cd-56dd-43de-9a40-b386f0b8dfb0" name="Samsung GSM_SGH-E790" reportVersion="2.0b"
   xmlns="http://pa.cellebrite.com/report/2.0b">
  - <metadata section="Additional Fields">
    - <item name="Case/File number">
        <![CDATA[ 223336556 ]]>
      </item>
    - <item name="Examiner name">
        <![CDATA[ Mark ]]>
      </item>
      <item name="Department" />
      <item name="Location" />
      <item name="Notes" />
      <item name="Master" />
    </metadata>
  - <metadata section="Extraction Data">
    - <item name="Extraction start date/time">
        <![CDATA[ 21/07/2009 17:43:04 ]]>
      </item>
    - <item name="Unit Identifier">
        <![CDATA[ UFED S/N 5526165 ]]>
      </item>
    - <item name="Unit Version">
        <![CDATA[ 1.1.1.0 ]]>
      </item>
    - <item name="Selected Manufacturer">
        <![CDATA[ Samsung GSM ]]>
      </item>
    - <item name="Selected Device Name">
        <![CDATA[ SGH-E790 ]]>
      </item>
    - <item name="Connection Type">
        <![CDATA[ Cable No. 97 ]]>
      </item>
    </metadata>
    <metadata section="Device Info" />
  - <images>
      <image key="CTS" path="CTS(298C0000-30400000).bin" size="112459776" type="File" />
      <image key="MCU" path="MCU(20000000-22000000).bin" size="33554432" type="File" />
    </images>
  - <decodedData>
    - <modelType type="SMS">
      - <model type="SMS" id="b7dd5120-8330-4a84-81be-1f11d3e5931c">
        - <field name="TimeStamp" type="TimeStamp">
            <empty />
          </field>
        - <field name="Status" type="MessageStatus">
          - <value type="MessageStatus">
              <![CDATA[ Default ]]>
            </value>
          </field>
        - <multiModelField name="Parties" type="Party">
          - <model type="Party" id="a5f98c1d-001b-43ef-b0cd-ee01bff00d64">
            - <field name="Identifier" type="String">
              - <value type="String">
                  <![CDATA[ 00096970059 ]]>
                </value>
              </field>
            - <field name="Role" type="PartyRole">
              - <value type="PartyRole">
                  <![CDATA[ To ]]>
                </value>
              </field>
            - <field name="Status" type="PartyStatus">
              - <value type="PartyStatus">
                  <![CDATA[ Unknown ]]>
                </value>
              </field>
            </model>
          </multiModelField>
        - <field name="Folder" type="String">
          - <value type="String">
              <![CDATA[ Drafts ]]>
            </value>
          </field>
        - <field name="SMSC" type="String">
          - <value type="String">
              <![CDATA[ +97254120032 ]]>
            </value>
          </field>
        - <field name="Message" type="String">
          - <value type="String">
              <![CDATA
              [ ABabABabABABabABabABABabABabABABabABabABABabABabABABabABabABABabABabABABabABabABABabABabABABabABabABABabABabABA
              >
            </value>
          </field>
        - <field name="Name" type="String">
            <empty />
          </field>
        - <field name="Source" type="String">
            <empty />
          </field>
        </model>
      - <model type="SMS" id="41018bd4-17ae-443b-8686-8dd905442add">
        - <field name="TimeStamp" type="TimeStamp">
            <empty />
          </field>
        - <field name="Status" type="MessageStatus">
          - <value type="MessageStatus">
              <![CDATA[ Default ]]>
            </value>
          </field>
        - <multiModelField name="Parties" type="Party">
          - <model type="Party" id="47755841-c5bd-4afb-861a-e0605d1811f2">
            - <field name="Identifier" type="String">
              - <value type="String">
                  <![CDATA[ 00096928951 ]]>
                </value>
              </field>
            - <field name="Role" type="PartyRole">
              - <value type="PartyRole">
                  <![CDATA[ To ]]>
                </value>
              </field>
            - <field name="Status" type="PartyStatus">
              - <value type="PartyStatus">
                  <![CDATA[ Unknown ]]>
```

Figure 35: Typical HTML, Excel, and XML reports

Chapter 6: **Physical Analyzer - Advanced Use**

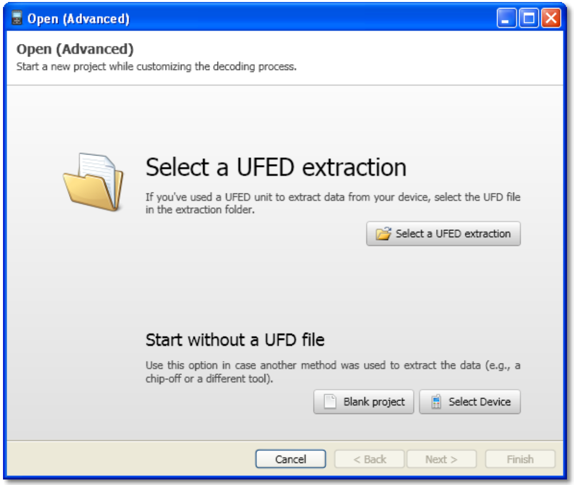
6.1 Using the Advanced Opening Feature

The Open (Advanced) feature enables you to open projects in advanced mode, where you can specify the system dumps and parsing options.

Selecting **File** > **Open (Advanced)** or clicking the button in the application toolbar displays the Open (Advanced) dialog, enabling you to set the process of parsing the extracted data for your new project.

The **Open (Advanced)** dialog enables you to select from two main project opening methods:

- **Select a UFED extraction** - Enables you to specify how to parse the extracted or specified data of a UFED extraction file (*.ufd).
- **Start without a UFD file** - Enables you to start a new project from extracted data or a file system dump that where not generated by a UFED unit.



Open (Advanced)

Start a new project while customizing the decoding process.

Select a UFED extraction

If you've used a UFED unit to extract data from your device, select the UFD file in the extraction folder.

Start without a UFD file

Use this option in case another method was used to extract the data (e.g., a chip-off or a different tool).

Figure 36: The Open (Advanced) dialog

6.1.1 Advanced Opening of a UFED Extraction File

The standard **Open** process uses a parsing process set according to the device and manufacturer information logged in the *.ufd file, or known file formats (*.bin, *.pm, *.ipd, etc.), to parse the data and create a new project.

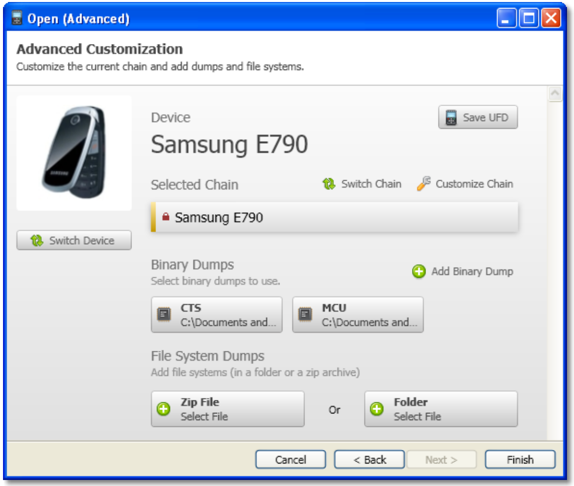
Using the **Select a UFED extraction** method enables you to skip the standard **Open** process, and specify a custom parsing process, or specify how to parse unknown devices.

To create a new project from UFED extracted data using **Open (Advanced)**:

1. Click the **Select a UFED extraction** button.
2. In the displayed file selection dialog, select the *.ufd file that will be processed and click **OK**.

   The dialog contents changes to **Advanced Customization** and displays the following settings:

   - **Device** - The manufacturer name and model of the device.
   - **Selected Chain** - The standard device parsing chain automatically assigned to the device.
   - **Binary Dumps** - The binary dumps images referenced by the UFD file.
3. Customize the file open options as described in sections 6.1.1.1 to 6.1.1.4.
4. Click **Finish**.


Open (Advanced)

Advanced Customization

Customize the current chain and add dumps and file systems.

Device: Samsung E790

Selected Chain: Samsung E790

Binary Dumps

Select binary dumps to use.

CTS C:\Documents and...

MCU C:\Documents and...

File System Dumps

Add file systems (in a folder or a zip archive)

Figure 37: Advanced opening of a UFED extraction

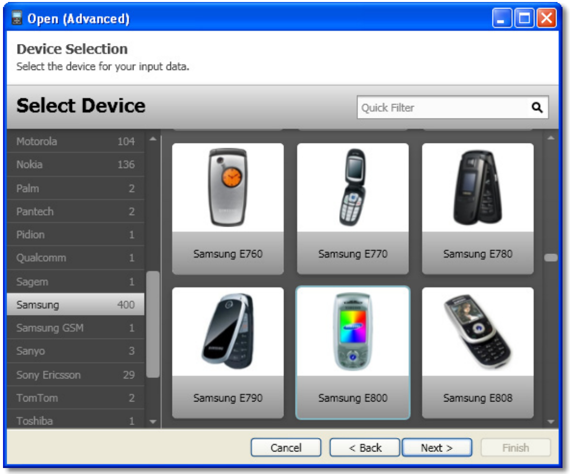
6.1.1.1 Specifying a Different Device

You can specify an entirely different parsing process of the extracted data by replacing the selected device.

To select a different device:

1. Click on the **Switch Device** button.
2. From the **Select Device** list, select the desired device.

   Use the list of manufacturers on the left to filter the displayed devices by manufacturer, and the **Quick Filter** field to filter the displayed devices.
3. Click **Next** to return to the **Advanced Customization** panel.



Select the device for your input data.

Motorola	104
Nokia	136
Palm	2
Pantech	2
Pidion	1
Qualcomm	1
Sagem	1
Samsung	400
Samsung GSM	1
Sanyo	3
Sony Ericsson	29
TomTom	2
Toshiba	1

Figure 38: Selecting a different device

6.1.1.2 Changing the Parsing Chain

A chain is a set of plug-ins grouped together in a certain order, which is used to process the extracted data. Each device in the supported devices list of the application has a predefined parsing chain assigned to it.

NOTE: Beside plug-ins, a chain can also include other chains as part of it, which is a simpler way to use a predefined set of plug-ins within another chain.

For more information about parsing chains and plug-ins, see "Chains" on page 91 and "Plug-ins" on page 97.

6.1.1.2.1 **Selecting a Different Chain**

To select a different chain:

1. Click on **Switch Chain**.

   The **Switch Chain** dialog opens and displays the default chain assigned to the device.

   NOTE: A device can have several assigned chains, but only one of them can be set as the default chain.

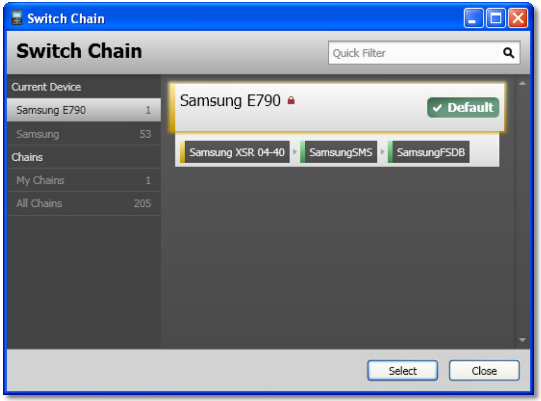


Figure 39: Selecting a different chain

2. From the chains list, select the desired chain.

   Select the manufacturer name under the **Current Device** section at the top of the list to display the chains assigned to devices of the same manufacturer.

   Under the **Chains** section of the list:

   - Select **My Chains** to select from the list of custom chins you constructed.
   - Select **All Chains** to select from the list of all predefined device chains.

   Use the list of manufacturers on the left to filter the displayed devices by manufacturer.

   Use the **Quick Filter** field to filter the displayed list items.

3. Click **Select** to return to the **Advanced Customization** panel.

   The default chain will be replaced by the selected chain.

6.1.1.2.2 **Editing the Current Chain**

You can open the current chain and edit it to suit your needs.

To edit the current chain:

1. Click on **Customize Chain**.

   The chain structure dialog of the current chain opens and displays the chain.

2. To add a component to the chain:

   A. Click **Add Chain/Plugin**.

   B. From the **Component Library**, select a components category - Chains, Plugins, or Devices.

   - **Device**: The entire chain of a specific plug-in.
   - **Chain:** A specific predefined chain.
   - **Plugin:** A specific plug-ins.

   NOTE: Both **Device** and **Chain** are added to the chain as a Chain component.

   C. Click on the **+** at the right of the component line to add it.

3. To remove a component from the chain list, click on the **×** at the right of the component item, then click **Yes** to approve.

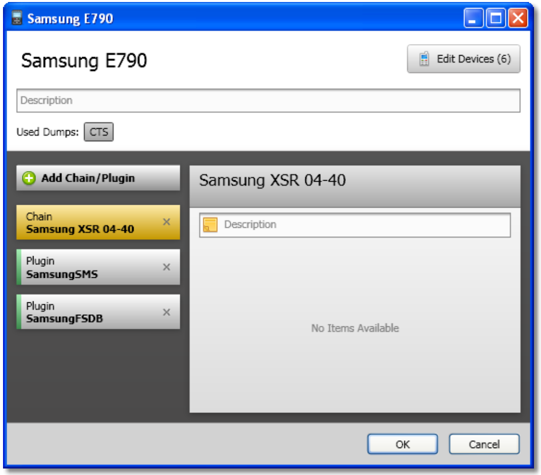


Figure 40: Editing the current chain

4. Click **OK** to return to the **Advanced Customization** panel.

   The current chain will be replaced by the customized chain.

6.1.1.2.3 Saving a Customized Chain

After you customize a chain, you can save the changes made to the chain for future use using the **Save As** or **Save** buttons added under the **Selected Chain** section.

> **NOTE:** the **Save** button is enabled only for customization done for unlocked user defined chains saved in **My Chains**. For more information about user defined chains, see "Managing Chains" on page 91.

To save a customized chain:

1. Click **Save** (if enabled) to replace the user defined chain with the current one or **Save As** to save the current chain as a new chain.
2. If you click **Save As**, enter a name for the new chain and click **Save**.

   The new chain will be added to the **My Chains** list of customized chains of the application, and the saved chain will appear as the **Selected Chain**.

6.1.1.3 Add a Binary Dump

You can add more binary dump files received from a different source or generated separately to the project.

To add a binary dump, click on **Add Binary Bump** and select the binary dump file you wish to add. Each binary dump you add will show up as a separate binary dump component in the **Binary Dumps** section of the dialog.

To remove a binary dump, click on the ☒ icon that appears at its top right corner when rolling over it.

6.1.1.4 **Add a File System Dump**

You can add a file system dump to the project received either as a ZIP archive or as a folder containing the file system dump files.

To add a file system dump, click on either the **Zip File** or **Folder** buttons and select the ZIP archive or folder you wish to add.

> **NOTE:** You can add one file system dump. Trying to add more than one will remove the previously added file system dump, regardless if it's a zip archive or folder.

To remove a file system dump, click on the ☒ icon that appears at its top right corner when rolling over it.

6.1.2 **Advanced Opening of a non-UFED Extraction File**

When you receive binary and file system dumps that were not generated by a UFED unit, or you don't have the *.ufd file that accompanies them, you can use the **Open (Advanced)** feature to define how to parse them for the new project.

The **Start without a UFD file** option provides you with two starting points for your new project:

- **Select Device** - Enables you to select the specific device definition that will be used to parse the extracted or specified data. This option is useful when the device manufacturer and model are known to you.
- **Blank Project** - Provides you with an empty **Advanced Customization** panel to set your process parameters and data. This option is useful when you have no information about the device and/or manufacturer, and would like to construct a custom parsing process.

6.1.2.1 Starting with Device Selection

To create a new project for an extracted data, based on a known device:

1. Click the **Select Device** button.
2. From the **Select Device** list, select the desired device.

   Use the list of manufacturers on the left to filter the displayed devices by manufacturer, and the **Quick Filter** field to filter the displayed devices.
3. Click **Next**.

   The **Advanced Customization** panel will display with the name and default parsing chain of the selected device.
4. To select a different device, see "Specifying a Different Device" on page 63.
5. To select a different parsing chain, see "Selecting a Different Chain" on page 64.
6. To customize the parsing chain, see "Editing the Current Chain" on page 65.
7. To add binary dumps, see "Add a Binary Dump" on page 66.
8. To add a file system dump, see "Add a File System Dump" on page 67.
9. Click **Finish**.

6.1.2.2 Starting from a Blank Project

1. Click the **Blank Project** button.
2. To select a device, see "Specifying a Different Device" on page 63.

3. To select a different parsing chain, see "Selecting a Different Chain" on page 64.
4. To customize the parsing chain, see "Editing the Current Chain" on page 65.
5. To add binary dumps, see "Add a Binary Dump" on page 66.
6. To add a file system dump, see "Add a File System Dump" on page 67.
7. Click **Finish**.

6.1.3 Saving a UFD File

At any point of setting the **Open (Advanced)** parameters you can click the **Save UFD** button at the top right corner of the dialog to save a *.ufd file that logs the selected binary dumps and device information, for future use.

The next time you need to parse that file you can use the saved UFD file to open it with **Open** or **Open (Advanced)**.

6.2 Hash Verification

A hash value is a unique and compact representation of a piece of data, which can be used for integrity protection due to the fact that it is computationally improbable to find two distinct inputs that hash to the same value.

Comparing a reference hash value that was generated during the extraction process for each binary dump against their calculated hash values enables you to verify the integrity of the binary dumps you received.

To verify the hash values:

1. Click the **Calculate hashes** button in the **Extracted Data** tab of the project.
2. After the hash values were calculated for the project, click the **Show Details** button.

   The **Image Hash Details** dialog will display the comparison result of the reference and calculated hash values of each image. A ✓ Verified label indicates matching values. A ❗ Bad Verification label indicates the images do not match.

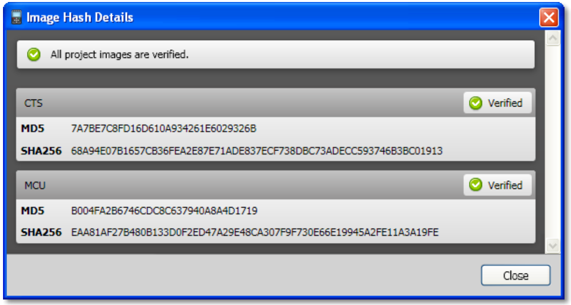


Image Hash Details

✓ All project images are verified.

CTS ✓ Verified

MD5 7A7BE7C8FD16D610A934261E6029326B

SHA256 68A94E07B1657CB36FEA2E87E71ADE837ECF738DBC73ADECC593746B3BC01913

MCU ✓ Verified

MD5 B004FA2B6746CDC8C637940A8A4D1719

SHA256 EAA81AF27B480B133D0F2ED47A29E48CA307F9F730E66E19945A2FE11A3A19FE

Figure 41: The Image Hash Details dialog

Projects without reference hash values will display a **No reference hash information is available for this project** alert in the **Image Hash Information** section of the **Welcome** tab.

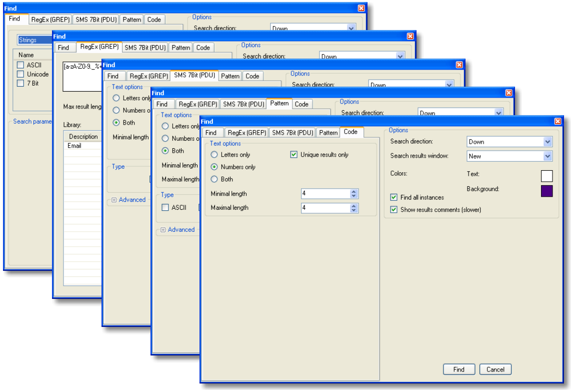
You can calculate hash values for a project without hash reference values. A **Hashes have been calculated for this project, but no reference data is available** message will be displayed in the **Image Hash Information** section of the **Extracted Data** tab.

6.3 Searching for Information in the Hex Dump and Parsed Data

6.3.1 Search Modes

The following search modes enable you to search for information within the Hex dump:

- **Find** - Enables searching for specific parameters such as strings, bytes, dates and more.
- **RegEx (GREP)** - Enables searching for strings using Regular Expressions.
- **SMS 7Bit (PDU)** - Enables searching after SMS text strings.
- **Pattern** - Enables searching for text patterns, in cases in which the pattern of the text is understood but not the text itself (mainly used for 7 bit search to locate SMS messages).
- **Code** - Specialized search tool used to find user codes and passwords.



Text options
○ Letters only
● Numbers only
○ Both
☑ Unique results only
Minimal length 4
Maximal length 4

Options
Search direction: Down
Search results window: New
Colors: Text: □ Background: ■
☑ Find all instances
☑ Show results comments (slower)

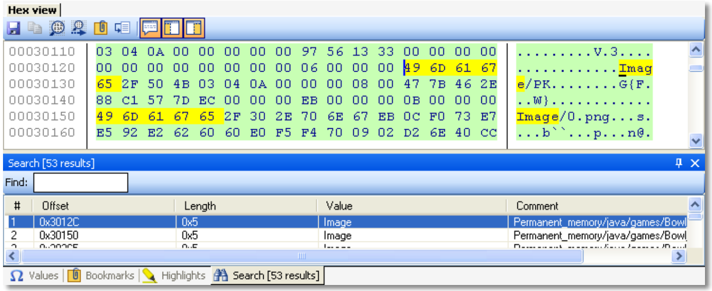
Figure 42: Find dialog modes

NOTE: The Find modes were built using the Plug-ins architecture. The following find options can be enhanced and extended by adding new search plug-ins developed either by Cellebrite or by the user.

6.3.2 Search Results

If the **Find All Instances** option was selected for the search, the results will appear in the **Search** results tab at the analysis information section (under the Hex view pane).

To make it easier to distinguish between the given results of each search performed, different Text and Background colors can be set for each search you run.



```
00030110  03 04 0A 00 00 00 00 00 97 56 13 33 00 00 00 00  .........V.3....
00030120  00 00 00 00 00 00 00 00 06 00 00 00 49 6D 61 67  ............Imag
00030130  65 2F 50 4B 03 04 0A 00 00 00 08 00 47 7B 46 2E  e/PK........G{F.
00030140  88 C1 57 7D EC 00 00 00 EB 00 00 00 0B 00 00 00  ..W}............
00030150  49 6D 61 67 65 2F 30 2E 70 6E 67 EB 0C F0 73 E7  Image/0.png...s.
00030160  E5 92 E2 62 60 60 E0 F5 F4 70 09 02 D2 6E 40 CC  ...b``...p...n@.
```

Find:

#	Offset	Length	Value	Comment
1	0x3012C	0x5	Image	Permanent_memory/java/games/Bowl
2	0x30150	0x5	Image	Permanent_memory/java/games/Bowl

Figure 43: Typical String search results

Search results include the following fields:

#	The number of results.
Offset	The address offset of the data file in the HEX dump.
Length	The string length in bytes.
Value	The string itself.
Comment	The file name/number and the location of the result in the Hex dump. When empty, the found data is in the un-allocated area.

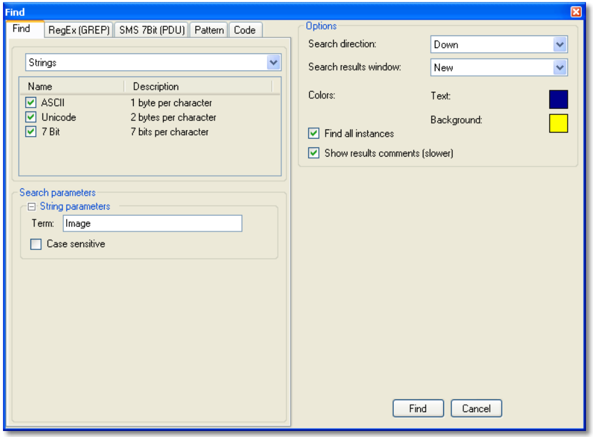
Clicking on any of the search results will display the item in the Hex view.

The Find field above the results list filters the search results by searching for specific data within the **Find** results.

6.3.3 Strings Search

Searching for strings enables you to locate different types of data in the Hex dump, e.g. text message, phone numbers, names or any other type of string data.

1. While viewing a Hex dump, click on the **Find** button in the Hex view toolbar.
2. Select **String** from the list at the top of the dialog.
3. Check the type of text encoding to search for the given string:
   - ASCII.
   - UNICODE (mainly for non-Latin characters).
   - 7 bits (mainly for SMS text).
4. Enter the search string in the **Term** field.
5. Select the **Case sensitive** option, if necessary.
6. Set the **Search direction**, **Search result window**, and **search colors** options.
7. Select **Find all instance** to display all search results at the end of the process, or deselect to move through the found items one-by-one during the search (can also be done by pressing F3).
8. Click **Find**.



Strings

Name	Description
☑ ASCII	1 byte per character
☑ Unicode	2 bytes per character
☑ 7 Bit	7 bits per character

Search parameters

⊟ String parameters

Term: Image

☐ Case sensitive

Options

Search direction: Down

Search results window: New

Colors: Text: 🟦 Background: 🟨

☑ Find all instances

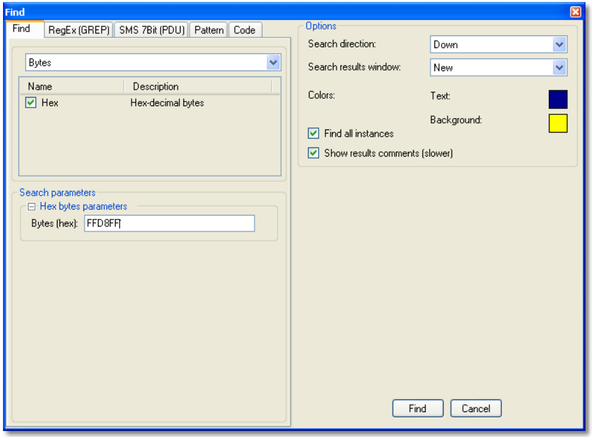
☑ Show results comments (slower)

Figure 44: String search

6.3.4 Bytes Search

Searching for bytes enables you to look for specific bytes occurrences in the Hex dump. This is especially useful when the identifying header of a file type or information you are looking for is known.

For example, the starting Hex bytes of a JPG image are FF D8 FF. Therefore, the result of searching for FF D8 FF will provide us with the locations of all possible JPG image headers in the Hex dump.



Bytes

Name	Description
☑ Hex	Hex-decimal bytes

Search parameters

⊟ Hex bytes parameters

Bytes (hex): FFD8FF

Options

Search direction: Down

Search results window: New

Colors: Text: ■ Background: ■

☑ Find all instances

☑ Show results comments (slower)

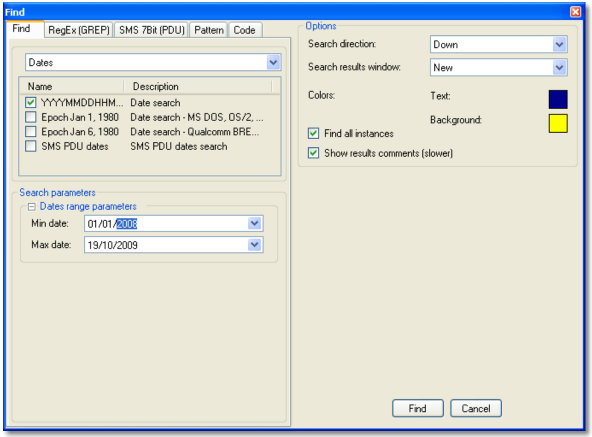
Figure 45: Bytes search

1. While viewing a Hex dump, click on the **Find** button in the Hex view toolbar.
2. Select **Bytes** from the list at the top of the dialog.
3. Select the **Hex** option.
4. In the **Bytes (hex)** field enter the Hex value, e.g. FFD8FF.
5. Set the **Search direction**, **Search result window**, and **search colors** options.
6. Select **Find all instance** to display all search results at the end of the process, or deselect to move through the found items one-by-one during the search (can also be done by pressing F3).
7. Click **Find**.

6.3.5 Dates Search

This search method finds a range of dates in the Hex dump.

1. While viewing a Hex dump, click on the **Find** button in the Hex view toolbar.
2. Select **Dates** from the list at the top of the dialog.
3. Select the desired date format to be used in the current search (more than one date format can be selected).
4. In the **Min Date** and **Max Date** fields enter the required date range.
5. Set the **Search direction**, **Search result window**, and **search colors** options.



Dates

Name	Description
☑ YYYYMMDDHHM...	Date search
□ Epoch Jan 1, 1980	Date search - MS DOS, OS/2, ...
□ Epoch Jan 6, 1980	Date search - Qualcomm BRE...
□ SMS PDU dates	SMS PDU dates search

Search parameters

⊟ Dates range parameters

Min date: 01/01/2008

Max date: 19/10/2009

Options

Search direction: Down

Search results window: New

Colors: Text: ■ Background: 🟨

☑ Find all instances

☑ Show results comments (slower)

Figure 46: Dates search

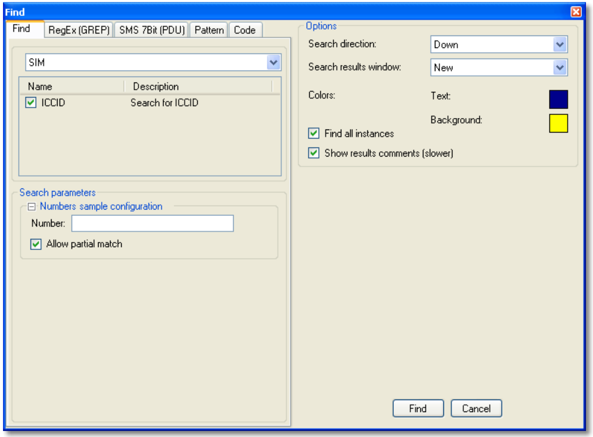
6. Select **Find all instance** to display all search results at the end of the process, or deselect to move through the found items one-by-one during the search (can also be done by pressing F3).
7. Click **Find**.

NOTE: To reduce the number of given results it is advised to set the date range using the Min Date and Max Date fields.

6.3.6 SIM ICCID Numbers Search

This search method enables you to search for SIM ICCID numbers in the Hex dump.

1. While viewing a Hex dump, click on the **Find** button in the Hex view toolbar.
2. Select **SIM** from the list at the top of the dialog.
3. Select the **ICCID Search** option.
4. Enter the ICCID number.
5. If only part of the number is known, select the **Allow Partial Match** option. For example, entering the number 89972 and selecting this option, will search for ICCID numbers provided by an Israeli service provider.



SIM

Name	Description
☑ ICCID	Search for ICCID

Search parameters

⊟ Numbers sample configuration

Number:

☑ Allow partial match

Options

Search direction: Down

Search results window: New

Colors: Text: ■ Background: ■

☑ Find all instances

☑ Show results comments (slower)

Figure 47: SIM ICCID search

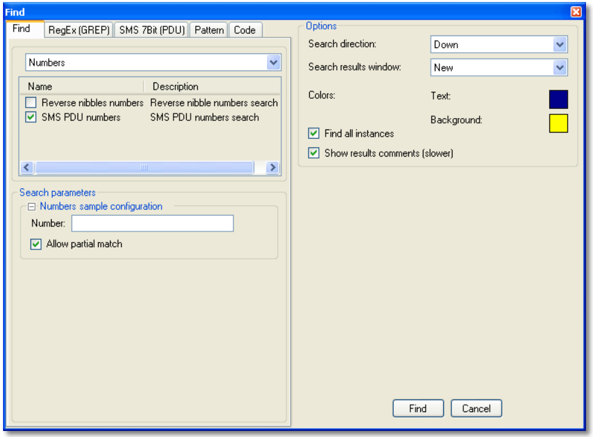
6. Set the **Search direction**, **Search result window**, and **search colors** options.
7. Select **Find all instance** to display all search results at the end of the process, or deselect to move through the found items one-by-one during the search (can also be done by pressing F3).
8. Click **Find**.

NOTE: If the Number field is left empty, the search result will include all the numbers that match the ICCID format.

6.3.7 SMS Numbers Search

This search method enables you to search for SMS numbers in the Hex dump.

1. While viewing a Hex dump, click on the **Find** button in the Hex view toolbar.
2. Select **Numbers** from the list at the top of the dialog.
3. Select the **SMS PDU numbers** option.
4. In the **Number** field, enter the search number.
5. If only part of the number is known, select the **Allow Partial Match** option.
6. Set the **Search direction**, **Search result window**, and **search colors** options.



Numbers

Name	Description
☐ Reverse nibbles numbers	Reverse nibble numbers search
☑ SMS PDU numbers	SMS PDU numbers search

Search parameters

⊟ Numbers sample configuration

Number:

☑ Allow partial match

Options

Search direction: Down

Search results window: New

Colors: Text: 🟦 Background: 🟨

☑ Find all instances

☑ Show results comments (slower)

Figure 48: SMS Numbers search

7. Select **Find all instance** to display all search results at the end of the process, or deselect to move through the found items one-by-one during the search (can also be done by pressing F3).
8. Click **Find**.

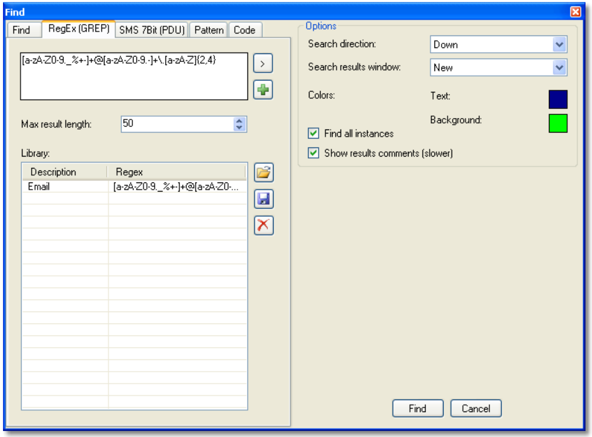
NOTE: If the Number field is left empty, the search result will include all the numbers that match the SMS Number format.

6.3.8 Regular Expression (GREP) Search

This search method enables you to invoke the power of regular expressions (RegEx) in order to look for a specific string structure within the data.

For example, the regular expression "`[a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[A-Za-z]{2,4}`", will search your data for all the email addresses that match the structure *<string>@<string>.<2 to 4 letters>*.

1. While viewing a Hex dump, click on the **Find** button in the Hex view toolbar.
2. Select **RegEx (GREP)** tab.
3. In the expression field enter the search expression.
4. Set the **Max result length** value to filter only results that are up to the specified length.
5. Set the **Search direction**, **Search result window**, and **search colors** options.
6. Select **Find all instance** to display all search results at the end of the process, or deselect to move through the found items one-by-one during the search (can also be done by pressing F3).
7. Click **Find**.



[a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,4}

Max result length: 50

Library:

Description	Regex
Email	[a-zA-Z0-9._%+-]+@[a-zA-Z0-...

Search direction: Down

Search results window: New

Colors: Text: ■ Background: 🟩

☑ Find all instances

☑ Show results comments (slower)

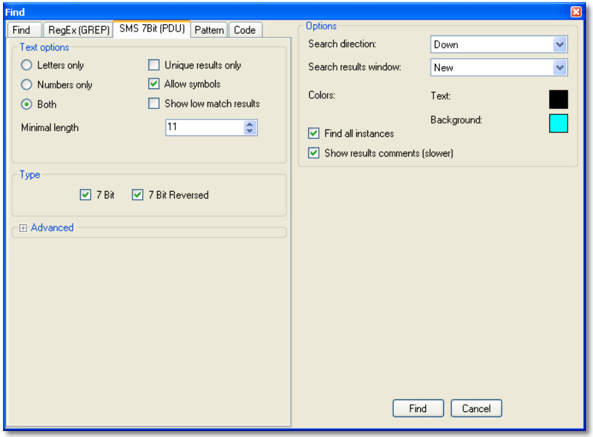
Figure 49: GREP search

NOTE: The Library list enables you to save the entered regular expression for future use. To save the current expression, click on the click the **Save** button .

6.3.9 SMS Text Search

This search method enables you to search for SMS text strings (7bit PDU) in the Hex dump

1. While viewing a Hex dump, click on the **Find** button in the Hex view toolbar.
2. Select the **SMS 7Bit (PDU)** tab.
3. In the **Text Options** section, set the search options of the text string.
4. Set the search results **Text** and **Background** colors.
5. Click **Find**.



Text options

○ Letters only
○ Numbers only
● Both
□ Unique results only
☑ Allow symbols
□ Show low match results

Minimal length: 11

Type

☑ 7 Bit
☑ 7 Bit Reversed

Options

Search direction: Down

Search results window: New

Colors: Text: ■ Background: 🟦

☑ Find all instances

☑ Show results comments (slower)

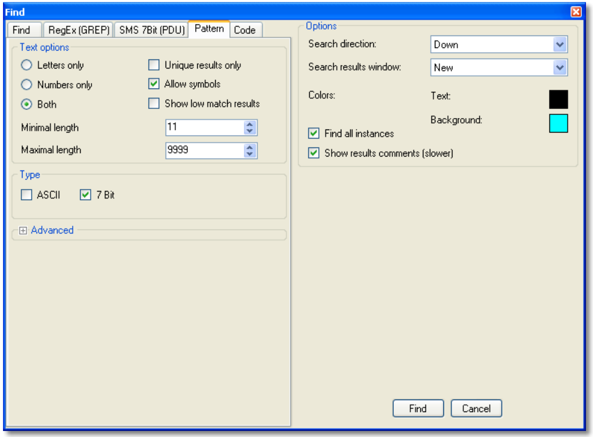
Figure 50: SMS Text search

6.3.10 **Pattern Search**

When navigating within a large memory structure, the **Find Pattern** tool locates any content that is textual in nature. A user has broad control over what to include within the search criteria.

1. While viewing a Hex dump, click on the **Find** button in the Hex view toolbar.
2. Select the **Pattern** tab.
3. In the **Minimal length** and **Maximal length** fields, set the pattern length range.

   This option enables filtering the results according to the searched patterns.
4. Select the type of the patterns (ASCII and/or 7 Bit).
5. Set the search results **Text** and **Background** colors.
6. Click **Find**.



○ Letters only
○ Numbers only
● Both
□ Unique results only
☑ Allow symbols
□ Show low match results
Minimal length: 11
Maximal length: 9999
□ ASCII
☑ 7 Bit
Search direction: Down
Search results window: New
Colors: Text: ■ Background: 🟦
☑ Find all instances
☑ Show results comments (slower)

Figure 51: Pattern search

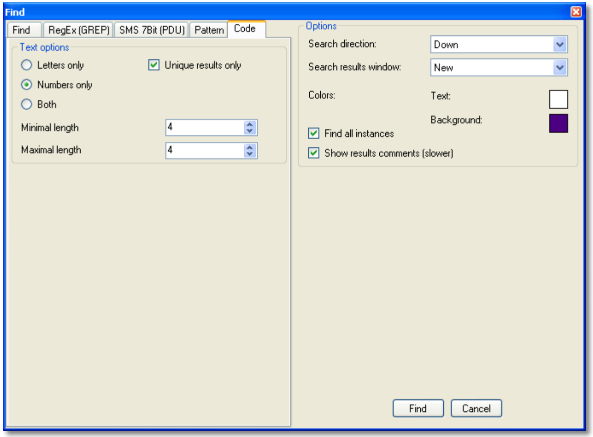
NOTE: Pattern search can be used to locate all possible 7 bit SMS text results. To minimize the number of false positive results set the Minimal Length value to a higher number.

6.3.11 **Code Search**

When navigating within a large memory structure, the **Find Code** search method can locates user codes and passwords.

1. While viewing a Hex dump, click on the **Find** button 🔍 in the Hex view toolbar.
2. Select the **Code** tab.
3. In the **Minimal length** and **Maximal length** fields, set the pattern length range.

   This option enables filtering the results according to the searched patterns.
4. Set the search results **Text** and **Background** colors.
5. Click **Find**.



Text options

○ Letters only

● Numbers only

○ Both

☑ Unique results only

Minimal length: 4

Maximal length: 4

Options

Search direction: Down

Search results window: New

Colors: Text: □ Background: ■

☑ Find all instances

☑ Show results comments (slower)

Figure 52: Code search

6.4 Working with Data Files

6.4.1 Accessing Data Files

To access one of the Data Files:

1. In the Project Tree, double click on any of the item type groups under Data files. A list view is presented in the data display area.

NOTE: For images, the data files can be displayed in **Table View** or **Thumbnail View**.

2. To display a specific data file, perform one of the following:
   - Double click on the file icon in the data display area.
   - Double click on the data file name in the Project Tree.
   - Right click on the data file name in the Project Tree and select **Open**.

6.4.2 Data File Pointers

All data files contain pointers to the file system location, so they can be located easily.

To display the pointers, click the (+) sign next to the file name in the Project Tree.

Double clicking the pointer will redirect you to the relevant file in the file system section of the Hex dump.

6.4.3 **Data Display Modes**

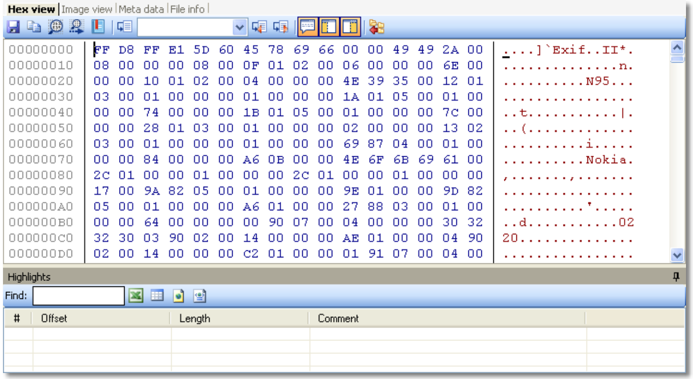
Each type of data file has several data display modes:

Image files	**Hex view**, **Image view**, and **File Info**
Video files	**Hex view** and **File Info**
Audio files	**Hex view** and **File Info**
Text files	**Hex view** and **File Info**

6.4.3.1 **Hex View**

To display the data file Hex dump, click the **Hex view** tab.

For more information about the **Hex view** tab, see "Hex View tab" on page 44.



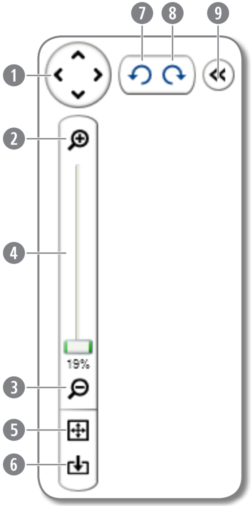
```
00000000  FF D8 FF E1 5D 60 45 78 69 66 00 00 49 49 2A 00  ....]`Exif..II*.
00000010  08 00 00 00 08 00 0F 01 02 00 06 00 00 00 6E 00  ..............n.
00000020  00 00 10 01 02 00 04 00 00 00 4E 39 35 00 12 01  ..........N95...
00000030  03 00 01 00 00 00 01 00 00 00 1A 01 05 00 01 00  ................
00000040  00 00 74 00 00 00 1B 01 05 00 01 00 00 00 7C 00  ..t...........|.
00000050  00 00 28 01 03 00 01 00 00 00 02 00 00 00 13 02  ..(.............
00000060  03 00 01 00 00 00 01 00 00 00 69 87 04 00 01 00  ..........i.....
00000070  00 00 84 00 00 00 A6 0B 00 00 4E 6F 6B 69 61 00  ..........Nokia.
00000080  2C 01 00 00 01 00 00 00 2C 01 00 00 01 00 00 00  ,.......,.......
00000090  17 00 9A 82 05 00 01 00 00 00 9E 01 00 00 9D 82  ................
000000A0  05 00 01 00 00 00 A6 01 00 00 27 88 03 00 01 00  ..........'.....
000000B0  00 00 64 00 00 00 00 90 07 00 04 00 00 00 30 32  ..d...........02
000000C0  32 30 03 90 02 00 14 00 00 00 AE 01 00 00 04 90  20..............
000000D0  02 00 14 00 00 00 C2 01 00 00 01 91 07 00 04 00  ................
```

Figure 53: Hex view

6.4.3.2 **Image View**

To display the image, select the **Image view** tab.

The **Image view** controllers on the left provides the following functions:



1 Navigation
2 Zoom In
3 Zoom Out
4 Zoom Slider
5 Zoom to Fit
6 Reset View
7 Rotate Left
8 Rotate Right
9 Show/Hide Controller

Figure 55: The Image view controllers

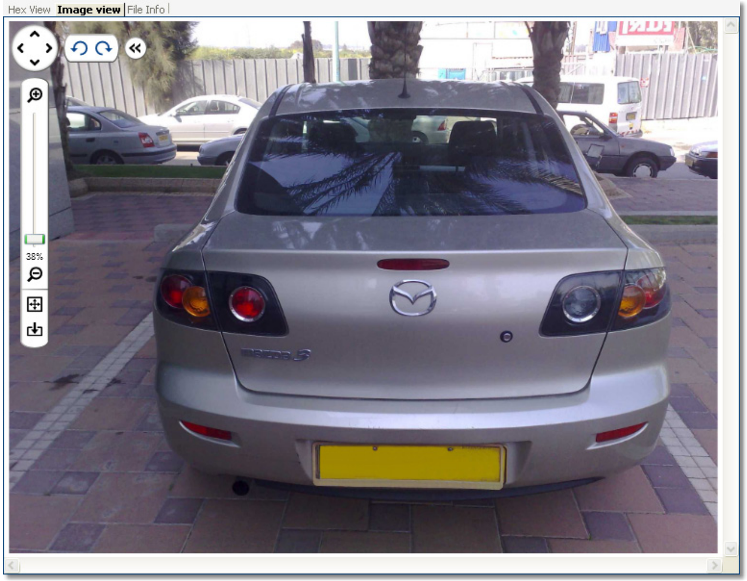


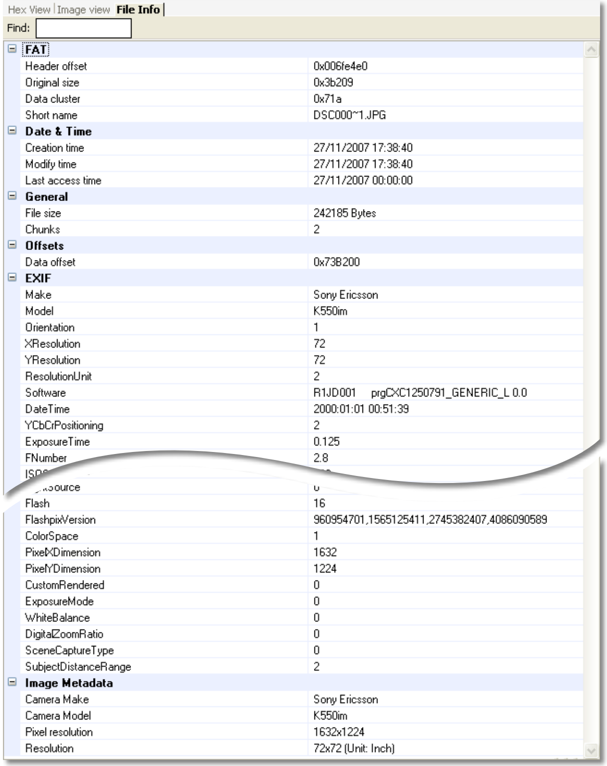
Figure 54: Image view

6.4.3.3 **File Info**

Click the **File Info** tab to display information about the data file.

The File Info list includes the following information sections:

- **FAT** - The file system information of the file.
- **Date & Time** - Created, Modified, and Last Access time stamps of the data file.
- **General** - The file Size in bytes and the number of file system Chunks of which the data file is comprised.
- **Offsets** - The offset addresses of the data file in the HEX dump.
- **EXIF** - The embedded EXIF information logged by the camera (if it exists).
- **Image Metadata** - The general information of the image (resolution, size and color depth).



FAT	
Header offset	0x006fe4e0
Original size	0x3b209
Data cluster	0x71a
Short name	DSC000~1.JPG
Date & Time	
Creation time	27/11/2007 17:38:40
Modify time	27/11/2007 17:38:40
Last access time	27/11/2007 00:00:00
General	
File size	242185 Bytes
Chunks	2
Offsets	
Data offset	0x73B200
EXIF	
Make	Sony Ericsson
Model	K550im
Orientation	1
XResolution	72
YResolution	72
ResolutionUnit	2
Software	R1JD001 prgCXC1250791_GENERIC_L 0.0
DateTime	2000:01:01 00:51:39
YCbCrPositioning	2
ExposureTime	0.125
FNumber	2.8
ISO	[illegible]
Source	0
Flash	16
FlashpixVersion	960954701,1565125411,2745382407,4086090589
ColorSpace	1
PixelXDimension	1632
PixelYDimension	1224
CustomRendered	0
ExposureMode	0
WhiteBalance	0
DigitalZoomRatio	0
SceneCaptureType	0
SubjectDistanceRange	2
Image Metadata	
Camera Make	Sony Ericsson
Camera Model	K550im
Pixel resolution	1632x1224
Resolution	72x72 (Unit: Inch)

Figure 56: Image File Info

6.4.4 **Redirecting the Offset**

When viewing the Hex data of a file or image you can use the offset redirection section in the Hex View toolbar to move to a specific address in the displayed data.

The offset redirection section includes the following components:

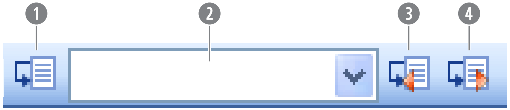
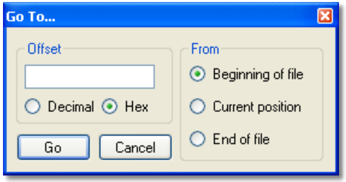


Figure 57: The offset redirection section



Go To...

Offset

○ Decimal ● Hex

Go Cancel

From

● Beginning of file

○ Current position

○ End of file

Figure 58: The Go To dialog

❶ **Go To button** - Click this button to display the **Go To...** dialog, where you can set the offset value (in Decimal or Hex) and set the reference point from where this offset is set (Beginning of file, Current position, or End of file).

❷ **Offset value field** - Enables you to enter the offset value you wish to go to, or select one of the previously entered values from the list. You can enter the value in decimal format (20) or Hex value format (0x20). Adding a "+" or "-" before the value indicated the offset should be calculated from the current position.

❸ **Jump Back button** - Uses the value entered/selected in the offset value field to jump to the set offset. For an offset from current position value (with "+" or "-"), redirects the offset backward (or forward for "-") from the current offset. For an offset address value (decimal or Hex) redirects the offset to that address.

❹ **Jump Forward button** - Uses the value entered/selected in the offset value field to jump to the set offset. For an offset from current position value (with "+" or "-"), redirects the offset forward (or backward for "-") from the current offset. For an offset address value (decimal or Hex) redirects the offset to that address.

6.4.5 Bookmarks

The **Bookmarks** feature is used to define and save specific locations in the hex dump. Bookmarks provide easy access to locate data segments in the future.

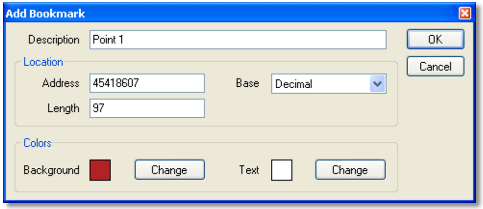
To bookmark a data segment:

1. In the Hex view, click and drag to highlight the data segment.
2. Click on the **Add Bookmark** button in the Hex view toolbar.

   The **Add Bookmark** dialog is displayed.
3. In the displayed **Add Bookmark** dialog:
   - Enter a name for the bookmark In the **Description** field.
   - Set the **Background** and **Text** colors of the bookmark in the **Colors** section.
4. Click the **OK** button.

   The new bookmark will be saved and displayed in the **Bookmarks** tab at the bottom of the Hex view.

   The marked segment is highlighted in the chosen colors. Details about the bookmark appear in the results window.


Add Bookmark

Description: Point 1

Location

Address: 45418607

Base: Decimal

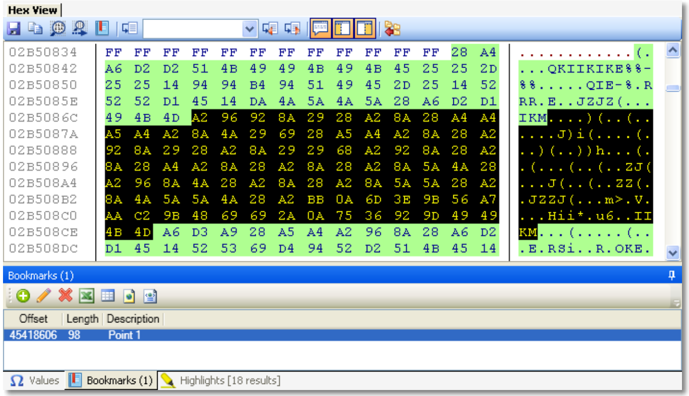
Length: 97

Colors

Background: 🟥

Text: □

Figure 59: The Add Bookmark dialog


Hex View

```
02B50834  FF FF FF FF FF FF FF FF FF FF FF FF 28 A4  ............(.
02B50842  A6 D2 D2 51 4B 49 49 4B 49 4B 45 25 25 2D  ...QKIIKIKE%%-
02B50850  25 25 14 94 94 B4 94 51 49 45 2D 25 14 52  %%.....QIE-%.R
02B5085E  52 52 D1 45 14 DA 4A 5A 4A 5A 28 A6 D2 D1  RR.E..JZJZ(...
02B5086C  49 4B 4D A2 96 92 8A 29 28 A2 8A 28 A4 A4  IKM....)(..(..
02B5087A  A5 A4 A2 8A 4A 29 69 28 A5 A4 A2 8A 28 A2  ....J)i(....(.
02B50888  92 8A 29 28 A2 8A 29 29 68 A2 92 8A 28 A2  ..)(..))h...(.
02B50896  8A 28 A4 A2 8A 28 A2 8A 28 A2 8A 5A 4A 28  .(...(..(..ZJ(
02B508A4  A2 96 8A 4A 28 A2 8A 28 A2 8A 5A 5A 28 A2  ...J(..(..ZZ(.
02B508B2  8A 4A 5A 5A 4A 28 A2 BB 0A 6D 3E 9B 56 A7  .JZZJ(...m>.V.
02B508C0  AA C2 9B 48 69 69 2A 0A 75 36 92 9D 49 49  ...Hii*.u6..II
02B508CE  4B 4D A6 D3 A9 28 A5 A4 A2 96 8A 28 A6 D2  KM...(.....(..
02B508DC  D1 45 14 52 53 69 D4 94 52 D2 51 4B 45 14  .E.RSi..R.OKE.
```

Bookmarks (1)

Offset	Length	Description
45418606	98	Point 1

Figure 60: Bookmarked data segment

Clicking on any bookmark item in the Bookmarks list will automatically display it in the Hex view

A toolbar at the top of the Bookmarks section provides the following functions:

⊕	Add Bookmark	Bookmark the selected data segment
✏	Edit Bookmark	Edit the selected bookmark parameters
✖	Remove Bookmark	Delete the selected bookmark
	Export to Excel	Export the bookmarks list to a Microsoft Excel spreadsheet (*.xlsx)
▦	Export to CSV	Export the bookmarks list to a CSV file
	Export to HTML	Export the bookmarks list to HTML file
	Export to XML	Export the bookmarks list to XML flie

Each bookmark displays the following information:

- **Offset** - The address offset of the bookmark paragraph in the HEX dump
- **Length** - The bookmarked data segment length
- **Description** - The bookmark name

6.4.6 **Values tab**

A user can decode the raw data to a variety of encoding types, which can be expanded in the **Values** list. This enables the user to decode the result of the selected data segment on the fly, in real time.

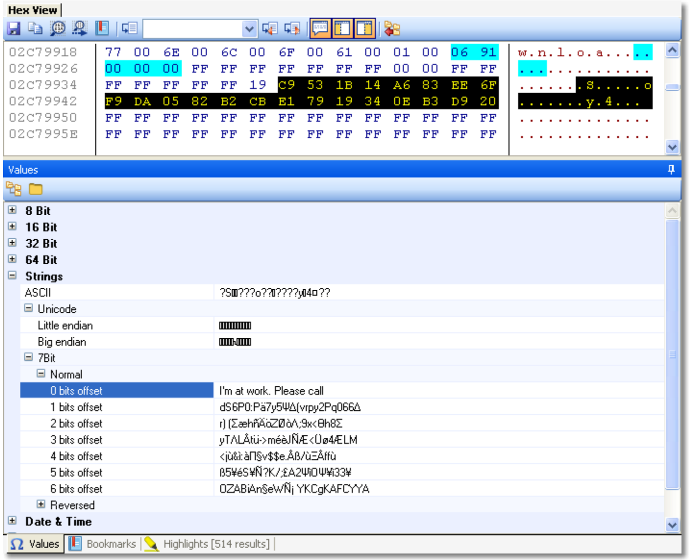
1. To access the **Values** tab, click on **Values** tab at the bottom section of the Hex view.

2. Select a data segment in the Hex view.

3. To display the decoded data, scroll to the desired encoding, then click on the ⊞ icon next to it to expand the display.

   Some encoding options, like 16 Bit, have sub-encoding types.

NOTE: You can fully expand or collapse all the encoding types by clicking the 🗂 or 📁 buttons.



```
02C79918  77 00 6E 00 6C 00 6F 00 61 00 01 00 06 91  w.n.l.o.a.....
02C79926  00 00 00 FF FF FF FF FF FF FF 00 00 FF FF  ..............
02C79934  FF FF FF FF FF 19 C9 53 1B 14 A6 83 EE 6F  .......S.....o
02C79942  F9 DA 05 82 B2 CB E1 79 19 34 0E B3 D9 20  .......y.4....
02C79950  FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ..............
02C7995E  FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ..............
```

⊞ **8 Bit**	
⊞ **16 Bit**	
⊞ **32 Bit**	
⊞ **64 Bit**	
⊟ **Strings**	
ASCII	?S▯???o??▯????y▯4¤??
⊟ Unicode	
Little endian	▯▯▯▯▯▯▯▯▯▯
Big endian	▯▯▯▯√▯▯▯▯
⊟ 7Bit	
⊟ Normal	
0 bits offset	I'm at work. Please call
1 bits offset	dS6P0:Pä7y5ΨΔ(vrpy2Pq066Δ
2 bits offset	r) (ΣæhñÄöZØòΛ;9x<Θh8Σ
3 bits offset	yTΛLÅtü->méèJÑÆ<Üø4ÆLM
4 bits offset	<jù&ì:àΠ§v$$e.Åß/ùΞÅffù
5 bits offset	ß5¥éS¥Ñ?K/;£A2ΨìOΨ¥ì33¥
6 bits offset	OZABiAn§eWÑ¡ YKCgKAFCYYA
⊞ Reversed	
⊞ **Date & Time**	

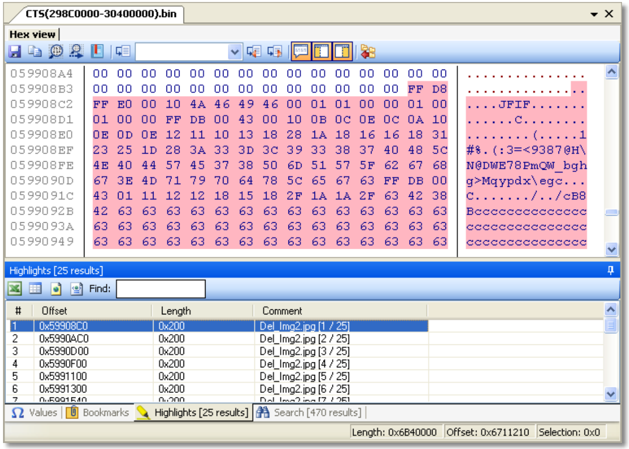
Figure 61: Decoded data segment

6.4.7 Highlights tab

The **Highlights** function presents analyzed data locations within the HEX dump. It allows the user find the exact location(s) of a particular type of analyzed data in HEX dump.

1. Click Highlight in the Hex window tab bar to access the Highlights window.
2. Upon selecting one of the analyzed data folders (e.g. contacts), the location of the selected contacts is listed in the Highlights window.

When a file is selected, the **Highlights** tab displays the list of chunks that this file is comprised of.



```
059908A4  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...............
059908B3  00 00 00 00 00 00 00 00 00 00 00 00 00 FF D8  ...............
059908C2  FF E0 00 10 4A 46 49 46 00 01 01 00 00 01 00  ....JFIF.......
059908D1  01 00 00 FF DB 00 43 00 10 0B 0C 0E 0C 0A 10  ......C........
059908E0  0E 0D 0E 12 11 10 13 18 28 1A 18 16 16 18 31  ........(.....1
059908EF  23 25 1D 28 3A 33 3D 3C 39 33 38 37 40 48 5C  #%.(:3=<9387@H\
059908FE  4E 40 44 57 45 37 38 50 6D 51 57 5F 62 67 68  N@DWE78PmQW_bgh
0599090D  67 3E 4D 71 79 70 64 78 5C 65 67 63 FF DB 00  g>Mqypdx\egc...
0599091C  43 01 11 12 12 18 15 18 2F 1A 1A 2F 63 42 38  C......./../cB8
0599092B  42 63 63 63 63 63 63 63 63 63 63 63 63 63 63  Bcccccccccccccc
0599093A  63 63 63 63 63 63 63 63 63 63 63 63 63 63 63  ccccccccccccccc
05990949  63 63 63 63 63 63 63 63 63 63 63 63 63 63 63  ccccccccccccccc
```

#	Offset	Length	Comment
1	0x59908C0	0x200	Del_Img2.jpg [1 / 25]
2	0x5990AC0	0x200	Del_Img2.jpg [2 / 25]
3	0x5990D00	0x200	Del_Img2.jpg [3 / 25]
4	0x5990F00	0x200	Del_Img2.jpg [4 / 25]
5	0x5991100	0x200	Del_Img2.jpg [5 / 25]
6	0x5991300	0x200	Del_Img2.jpg [6 / 25]
7	0x5991540	0x200	Del_Img2.jpg [7 / 25]

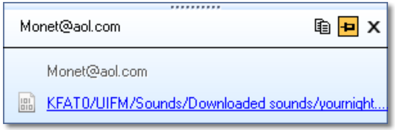
Figure 62: Highlighted data chunks

6.4.8 Information Frame

The **Information Frame** automatically appears whenever the mouse cursor is positioned over the displayed information in the Hex view.

The floating information frame displays:

- Links (pointers) to analyzed data items such as files and folders in the Project Tree.
- Search results associated with the pointed data.


Monet@aol.com

Monet@aol.com

KFAT0/UIFM/Sounds/Downloaded sounds/yournight...

Figure 63: Info Frame

6.5 Chains

A chain is a set of plug-ins grouped together, which is used to process the extracted data of a device. Each device in the supported devices list of the application has a predefined parsing chain assigned to it.

As part of its building blocks, a chain can also include other predefined chains.

6.5.1 Managing Chains

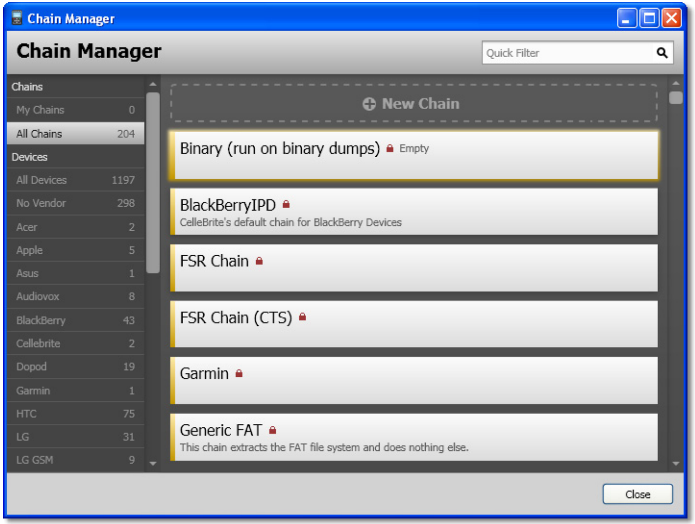
The **Chain Manager** enables you to:

- Manage and edit existing chains.
- Create new chains.
- Assign chains to devices.

To manage the application chains, select **Plug-ins > Chain Manager** or click the **Chain Manager** button in the application toolbar.

The **Chains** section of list on the left enables you to filter the displayed chains list. Select **My Chains** to display only custom chains you constructed, or **All Chains** to display a list of all the predefined chains.

Use the **Quick Filter** field at the top left of the window to filter the displayed list of chains.



Chains	
My Chains	0
All Chains	204
Devices	
All Devices	1197
No Vendor	298
Acer	2
Apple	5
Asus	1
Audiovox	8
BlackBerry	43
Cellebrite	2
Dopod	19
Garmin	1
HTC	75
LG	31
LG GSM	9

Binary (run on binary dumps) Empty

BlackBerryIPD
CelleBrite's default chain for BlackBerry Devices

FSR Chain

FSR Chain (CTS)

Garmin

Generic FAT
This chain extracts the FAT file system and does nothing else.

Figure 64: The Chain Manager window

To display the chains assigned to a specific device:

1. From the **Devices** section of the list, select:

   - **All Devices** to display a list of all the predefined devices.
   - A manufacturer name to display a list of the predefined devices of the selected manufacturer.

   Use the **Quick Filter** field at the top right of the window to filter the displayed devices.

2. Double click on a device to display its chains window.

   The chains window of the device will display at least one chain that was assigned to it.

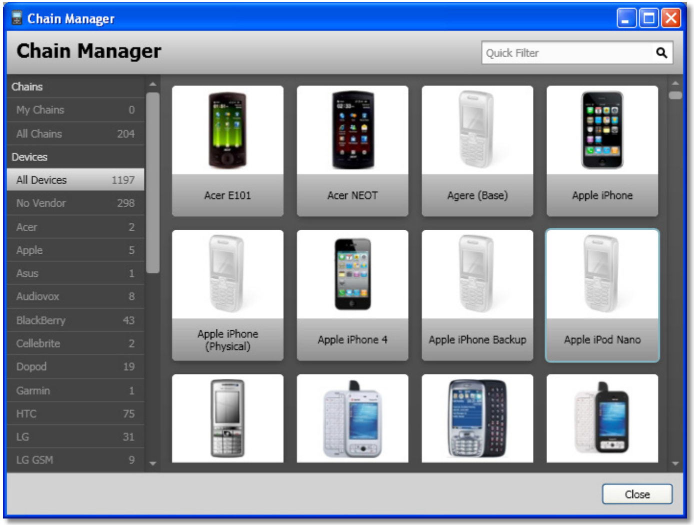


Figure 65: Selecting a device chain

6.5.1.1 **Constructing a New Chain**

To construct a new chain:

1. In the **Chain Manager** window or the chains list of a specific device, click the **New Chain** area at the top of the chains list.

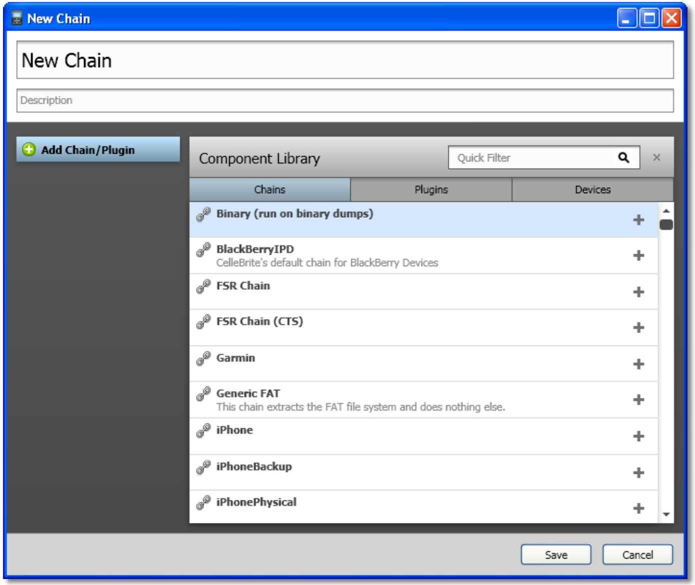
   The **New Chain** window appears.

2. In the **Name** field, enter a name for the new chain.

3. In the **Description** field, enter a short description for the chain (optional).

4. From the **Component Library**, select a components category - Chains, Plugins, or Devices.

   - **Device**: The entire chain of a specific plug-in.
   - **Chain:** A specific predefined chain.
   - **Plugin:** A specific plug-ins.



New Chain

Description

Binary (run on binary dumps)

BlackBerryIPD
CelleBrite's default chain for BlackBerry Devices

FSR Chain

FSR Chain (CTS)

Garmin

Generic FAT
This chain extracts the FAT file system and does nothing else.

iPhone

iPhoneBackup

iPhonePhysical

Figure 66: The New Chain window

NOTE: Both **Device** and **Chain** are added to the chain as a Chain component.

5. Click on the **+** at the right of the component line to add it.

6. To remove a component from the chain list, click on the **×** at the right of the component item, then click **Yes** to approve.

7. To edit the parameters of a plug-in or chain, select it from the chain components list (on the left) and set the options displayed.

   NOTE: To return to the Component Library display and continue adding more plug-ins and chains, click on **Add Chain/Plugin**.

8. When finished, click **Save**.

   The new chain will be add to your **My Chains** list.

6.5.1.2 Editing an Existing Chain

A chain can be opened and edited to suit your needs.

To edit a existing chain:

1. Double click on the chain you wish to edit.

2. Click on **Add Chain/Plugin** to display the **Component Library**.

3. To make the necessary changes, follow steps 4 through 7 of "Constructing a New Chain" on page 93.

4. When finished, click **Save** to save the changes or **Save As** to save the edited chain as a new chain.

   If you selected **Save As**, enter a name for the new chain and click **Save**.

NOTE: Changes made to factory predefined locked chains can only be saved as a new chain.

6.5.1.3 **Managing Device Chains**

6.5.1.3.1 **Attaching devices to a chain**

To attach devices to a chain:

1. Double click on the chain to which you would like to attach a device.
2. Click on the **Edit Devices** button at the top right of the chain window.
3. In the Devices For Chain window, click on the **Attach Device** button.
4. In The **Select Device** window, select the device you would like to attach to the chain.

   Use the **Devices** list to display only the devices of a specific manufacturer.

   Use the **Quick Filter** field to filter the displayed devices.
5. Click **Select**.
6. Repeat steps 4 and 5 to add more devices.
7. When you have finished attaching the devices, click **Close**.
8. Click **Cancel** to close the chain window.

6.5.1.3.2 **Setting the Default Device Chain**

To set the default chain of a device:

1. In the **Chain Manager** window, use the **Devices** list to locate the device you wish to modify.
2. Double click on the device to display its chains window.

3. If the chains list of the device contains more than one chain, click the ✔ at the right edge of a chain to set it as the default chain of the device.
4. Click **Close** to close the device chains window.

6.5.1.3.3 Detaching Devices from a Chain

To detach a device from a chain:

1. Double click on the chain from which you wish to detach a device.
2. Click on the **Edit Devices** button at the top right of the chain window.
3. Click on the ✕ at the right of every device you wish to detach from the chain.
4. Click **Close**.
5. Click **Cancel** to close the chain window.

6.5.1.4 Removing a Chain

NOTE: Only chains in the My Chains list can be removed.

To remove a chain from **My Chains**:

1. In the **Chain Manager** window, select **My Chains**.
2. If necessary, use the **Quick Filter** field to filter the chains list.
3. Click on the ✕ at the right of the chain.

6.6 Plug-ins

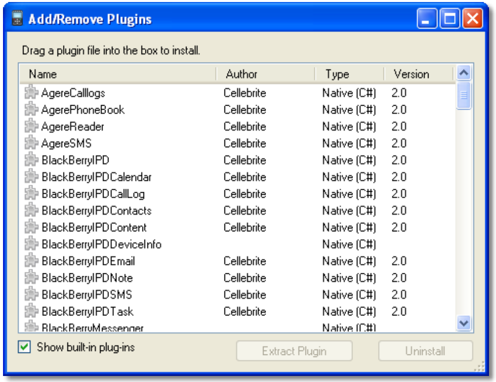
The **Plug-ins** mechanism is an API that allows users to expand the abilities of the application by adding plug-ins provided by Cellebrite, or custom tailored plug-ins written using Python.

6.6.1 Managing Plug-ins

The **Add/Remove Plugins** window enables you to manage the installed plug-ins.

To open the **Add/Remove Plugins** window, select **Plug-ins > Add/Remove Plugins**, or click the **Add/Remove Plug-ins** button in the application toolbar.

NOTE: To display all the installed plug-ins, including the built-in plug-ins that cannot be removed, select the Show built-in plug-ins option at the bottom left of the window.



Drag a plugin file into the box to install.

Name	Author	Type	Version
AgereCalllogs	Cellebrite	Native (C#)	2.0
AgerePhoneBook	Cellebrite	Native (C#)	2.0
AgereReader	Cellebrite	Native (C#)	2.0
AgereSMS	Cellebrite	Native (C#)	2.0
BlackBerryIPD	Cellebrite	Native (C#)	2.0
BlackBerryIPDCalendar	Cellebrite	Native (C#)	2.0
BlackBerryIPDCallLog	Cellebrite	Native (C#)	2.0
BlackBerryIPDContacts	Cellebrite	Native (C#)	2.0
BlackBerryIPDContent	Cellebrite	Native (C#)	2.0
BlackBerryIPDDeviceInfo		Native (C#)	
BlackBerryIPDEmail	Cellebrite	Native (C#)	2.0
BlackBerryIPDNote	Cellebrite	Native (C#)	2.0
BlackBerryIPDSMS	Cellebrite	Native (C#)	2.0
BlackBerryIPDTask	Cellebrite	Native (C#)	2.0
BlackBerryMessenger		Native (C#)	

☑ Show built-in plug-ins

Figure 67: The Plug-in Manager window

The **Add/Remove Plugins** window enables you to perform the following management tasks:

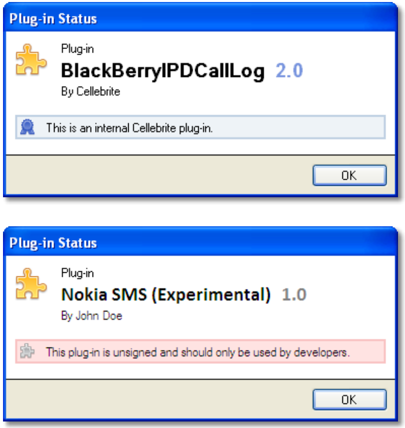
- To Install additional plug-ins, drag and drop them into the **Add/Remove Plugins** window.
- To extract a copy of an installed plug-in, select the plug-in and click the **Extract Plugin** button.
- To remove an installed plug-in, select the plug-in and click the **Uninstall** button.

NOTE: You cannot extract or uninstall a built-in plug-in of the application.

- To display the plug-in status, double click on the plug-in.

  The **Plug-in Status** dialog will display the status of the plug-in which can be either signed or unsigned.

  A signed plug-in is a plug-in that was approved and signed by Cellebrite.



Plug-in Status

Plug-in

BlackBerryIPDCallLog 2.0

By Cellebrite

This is an internal Cellebrite plug-in.

Plug-in Status

Plug-in

Nokia SMS (Experimental) 1.0

By John Doe

This plug-in is unsigned and should only be used by developers.

Figure 68: The Plug-in Status dialog of a signed and an unsigned plug-ins

6.6.2 Running a Specific Plug-in

The **Run Plug-in** window enables you to individually run an installed plug-in on your project.

To open the **Run Plug-in** window, select **Plug-ins > Run Plug-in...**.

To run a specific plug-in, select it from the list of plug-ins and click **Run**.

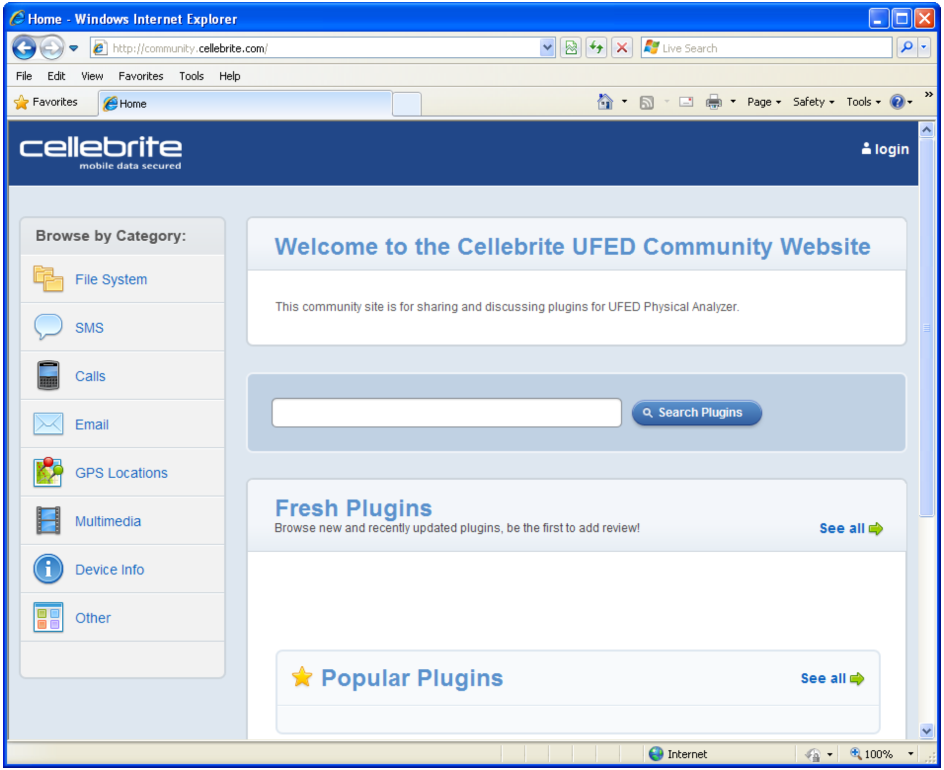
6.6.3 Getting Plug-ins

To get additional plug-ins:

1. Using your Cellbrite user name and password, login to the Cellebrite Community website at **community.cellebrite.com**.

   NOTE: You must first have a registered UFED unit and license (see "Activating the UFED Physical Extraction Module" on page 4).

2. Get new or updated plug-ins.



Welcome to the Cellebrite UFED Community Website

This community site is for sharing and discussing plugins for UFED Physical Analyzer.

Fresh Plugins

Browse new and recently updated plugins, be the first to add review!

Popular Plugins

Figure 69: The Cellebrite community website

6.7 Using the Python Shell

The built-in **Python Shell** enables you to run customized analysis using Python commands.

To open the **Python Shell** window, select **Python** > **Python Shell...**, or click the **Python Shell** button in the application toolbar.

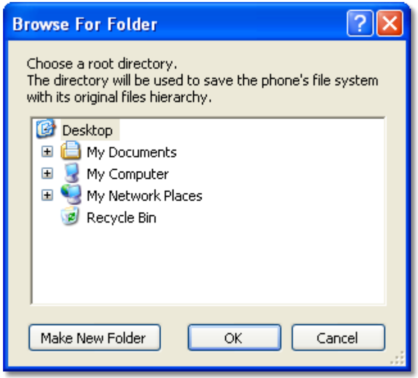
For detailed examples of how to use Python Shell commands for custom analysis, See "Appendix A: Using Python in the Physical Analyzer" on page 112.

6.8 Exporting the File System

Exporting the extracted file system saves the entire file system to the selected location on your computer. Exporting the File System provides physical files and folders structure saved in the same hierarchy as the original file system.

To export the extracted file system:

1. From the application menu, select **Tools** > **Dump file system**, or click the **Dump file system** button in the application toolbar.
2. In the **Browse For Folder** dialog, select the target location to which the extracted file system will be saved. Use the **Make New Folder** button to create a new folder in the target location.
3. Click **OK** to export the file system.



Choose a root directory.
The directory will be used to save the phone's file system with its original files hierarchy.

Figure 70: Exporting the file system

Chapter 7: **General settings**

The Settings window provides access to a set of functional and behavioral setup options used to fine-tune and control the functionality and usability of the UFED Physical Analyzer application.

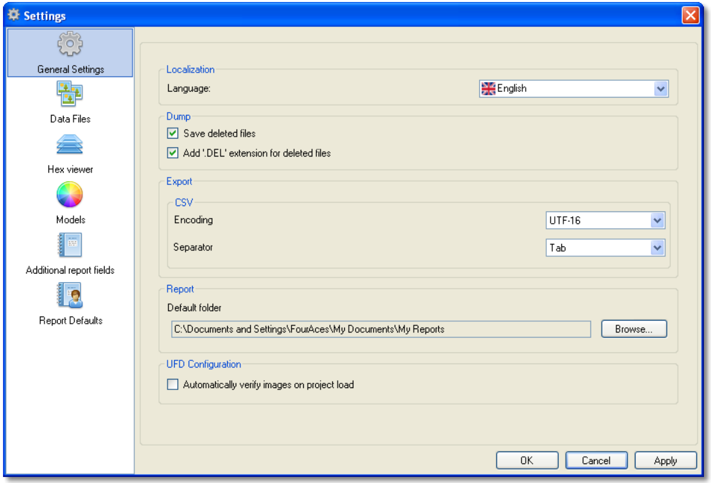
To access the **Settings** window, select **Tools** > **Settings** or click the **Settings** shortcut button at the top right of the Welcome screen.

The main settings categories appear in the column at the left of the window. Click on a category to access and change its options.

7.1 General Settings

These settings determine the following general application properties:

- **Localization** - Sets the interface language of the application.
- **Dump** - Sets how deleted files are dealt by the **Tools** > **Dump GPS/Mass Storage Device** feature.
- **Export** - Sets the encoding and separator of exported CSV files.



Settings

Localization

Language: English

Dump

☑ Save deleted files

☑ Add '.DEL' extension for deleted files

Export

CSV

Encoding UTF-16

Separator Tab

Report

Default folder

C:\Documents and Settings\FourAces\My Documents\My Reports

UFD Configuration

☐ Automatically verify images on project load

Figure 71: General settings

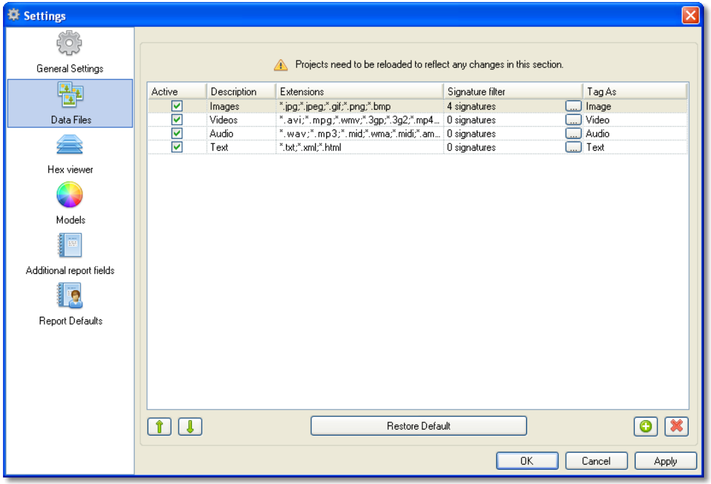
- **Report** - Sets the default path to the folder where reports you generate are saved.
- **UFD Configuration** - Settings used for loading *.ufd files.

7.2 Data Files Settings

The Data Files settings determine the different file and tagging groups under the **Data Files** and **Tags** sections of the project tree, and the types of files filtered to each group.

Every data file record in the list consists of the following fields:

- **Active** - Indicates whether to display (checked) or hide (unchecked) this group of data files in the project tree.
- **Description** - A descriptive name for the type of data files that will be used as the group name under the **Data files** section in the project tree.



⚠ Projects need to be reloaded to reflect any changes in this section.

Active	Description	Extensions	Signature filter	Tag As
☑	Images	*.jpg;*.jpeg;*.gif;*.png;*.bmp	4 signatures ...	Image
☑	Videos	*.avi;*.mpg;*.wmv;*.3gp;*.3g2;*.mp4...	0 signatures ...	Video
☑	Audio	*.wav;*.mp3;*.mid;*.wma;*.midi;*.am...	0 signatures ...	Audio
☑	Text	*.txt;*.xml;*.html	0 signatures ...	Text

Figure 72: Data Files settings

- **Extensions** - The file extensions that will be used to filter the data files of this group.
- **Signature filter** - The header and/or footer signatures that will be used to filter the data files of this group.
- **Tag As** - The tag name that will be applied to the data file and will be used to list the files under the **Tags** section of the project tree.

7.2.1 **Data Files Filtering Methods**

The group filtering can be achieved by using one or more of the following methods:

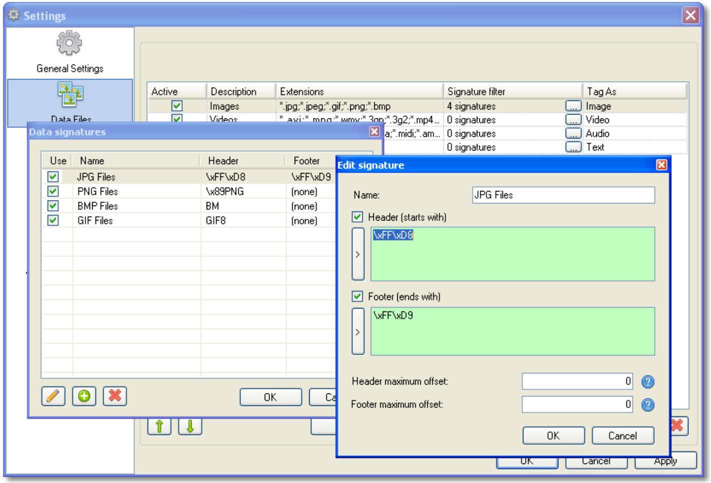
- Signature filter
- Extension filter

7.2.1.1 **Signature Filter**

A Signature is a definition of the file header and/or footer that will be searched, in order to detect a file type and associate it with a specific Date File group.

The header and/or footer can be configured to be in a defined range from the beginning and end of the file respectively by using the offset parameter (see in figure 56).

For example, a JPEG image starts with the header **`FF D8 FF`** and ends with the footer **`FF D9`**. Entering this information in the Header and Footer fields of the signature (see in figure 56) will create a signature that identifies JPEG images.



Active	Description	Extensions	Signature filter	Tag As
☑	Images	*.jpg;*.jpeg;*.gif;*.png;*.bmp	4 signatures	Image
☑	Videos	*.avi;*.mpg;*.wmv;*.3gp;*.3g2;*.mp4...	0 signatures	Video
		a;*.midi;*.am...	0 signatures	Audio
			0 signatures	Text

Use	Name	Header	Footer
☑	JPG Files	\xFF\xD8	\xFF\xD9
☑	PNG Files	\x89PNG	(none)
☑	BMP Files	BM	(none)
☑	GIF Files	GIF8	(none)

Name: JPG Files

☑ Header (starts with)

\xFF\xD8

☑ Footer (ends with)

\xFF\xD9

Header maximum offset: 0

Footer maximum offset: 0

Figure 73: JPEG Signature

7.2.1.2 **Extension filter**

A list of common file extensions that are associated with file formats that belong to the specific data file group.

For example, the different image file formats can be filtered by the file extensions *.jpg, *.jpeg, *.gif, *.png or *.bmp.

7.2.2 **Managing Data Files Settings**

You can add new types of data files, or edit and delete data files of an existing type.

Using the following buttons at the bottom of the list you can:

⇧ ⇩	Move Up/Down	Change the order of data file types by moving the selected type row up or down.
⊕	Add	Add a new data file type or signature filter.
✖	Delete	Delete the selected data file type or signature filter.
Restore Default	Restore Default	Restore the default settings.
✎	Edit	Edit the signature filter.

To add a new data file record:

1. In the Data Files settings, click on ⊕ to add a new data file record.
2. Check the Active checkbox to display the added data type in the Data Type section of the project tree.

3. In the **Description** field, enter file type description.
4. If applicable:
   - In the **Extensions** field, enter the file extensions commonly used by your data file type in the format *.xxx, separated by ";".
   - In the **Signature filter** field, click on the … button to add a filtering signatures that identify your data file type.
5. In the **Tag As** field, select a tag name from the list.

To delete an exiting data file record:

1. Select the Data File row In the Data Files settings.
2. Click on ✖ to delete the selected data file row.

To edit a existing data file record:

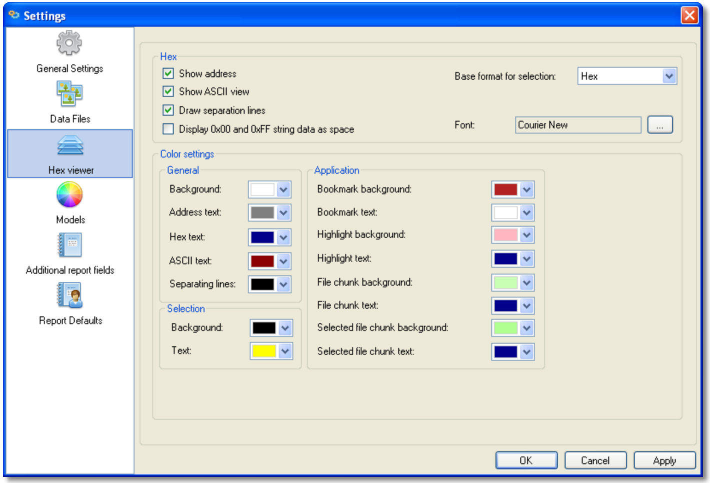
1. Select the Data File row in the Data Files settings.
2. Go through the different fields and make the necessary changes.

7.3 Hex Viewer Settings

The **Hex Viewer** setting enables you to control the display options of Hex dumps to suit personal preference and enhance readability.

The following setting are available:

- **Show address -** Show/Hide the line numbers column of the Hex Viewer.
- **Show ASCII view -** Show/Hide the ASCII view column of the Hex Viewer.
- **Draw separation lines -** Show/Hide the separation lines between the address, Hex data, and ASCII view columns
- **Display 0x00 and 0xFF string data as space -** Set the string data to display both 0x00 and 0xFF characters as space instead of a "".



Hex

☑ Show address

☑ Show ASCII view

☑ Draw separation lines

☐ Display 0x00 and 0xFF string data as space

Base format for selection: Hex

Font: Courier New

Color settings

General: Background:, Address text:, Hex text:, ASCII text:, Separating lines:

Selection: Background:, Text:

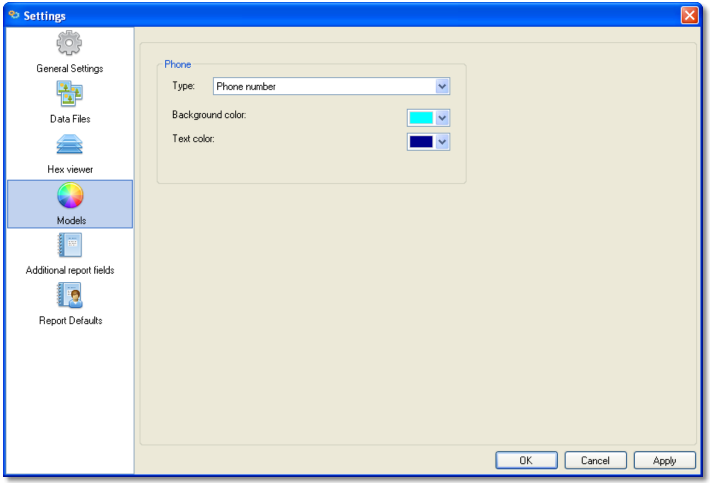
Application: Bookmark background:, Bookmark text:, Highlight background:, Highlight text:, File chunk background:, File chunk text:, Selected file chunk background:, Selected file chunk text:

Figure 74: Hex Viewer settings

- **Base format for selction -** The line numbers format (Decimal, Hex, or Both).
- **Font -** The font used to display the information.
- **Color settings -** Set the colors applied to different features of the Hex viewer.

7.4 Models Settings

The **Models** setting enables you to set the **Background** and **Text** color schemes applied to various types of phone data.



Phone

Type: Phone number

Background color:

Text color:

Figure 75: Models settings

7.5 Report Settings

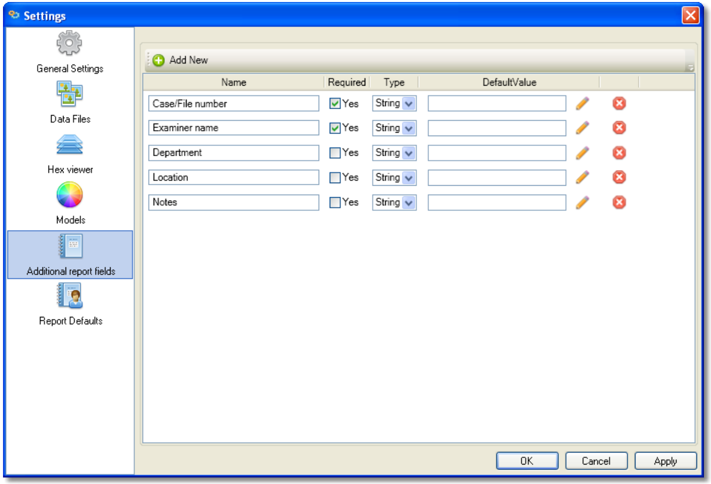
The Report settings enable you to customize several aspects of the generated report.

7.5.1 Additional Report Fields

Optional information is user-defined information presented at the beginning of the report. It usually includes information about the case, investigator and the organization details.

Every Optional information record consists of the following fields:

Name	The name of the report field.
Required	Indicates if the field must be filled in order to generate the report
Type	The types of entry - String or List.
Default value	The default content that will appear in the field.



Name	Required	Type	DefaultValue
Case/File number	☑ Yes	String	
Examiner name	☑ Yes	String	
Department	□ Yes	String	
Location	□ Yes	String	
Notes	□ Yes	String	

Figure 76: Reports - Optional Information settings

7.5.1.1 **Adding a New Report Field**

To add a new report field:

1. Click on the ⊕ above the fields list to add a new report field entry.
2. In the **Name** field, enter the field label that will be displayed.
3. Check the **Required** checkbox if this field must be filled to generate the report.
4. Use the **Type** list to specify the type of the new field:
   - **String** for a text entry field where you should type your information
   - **List** for a specified list of options to choose from.
5. Set the default content of the field:
   - For a **String** type field, enter the default string in the Default Value field. For a multiline string, click on ✎ and enter the default string in the **Option Editor**, then click **Save**.
   - For a **List** type field, click on ✎ and enter the list items, each item as a separate line, in the **Option Editor**, then click **Save**.

7.5.1.2 **Deleting a Report Field**

To delete an exiting data file record, click on ⊗ at the right edge of the field entry to delete report field.

7.5.1.3 **Editing a Report Field**

To edit an existing report field, go through steps 2 to 5 of Adding a New Report Field and change it to suit your needs.

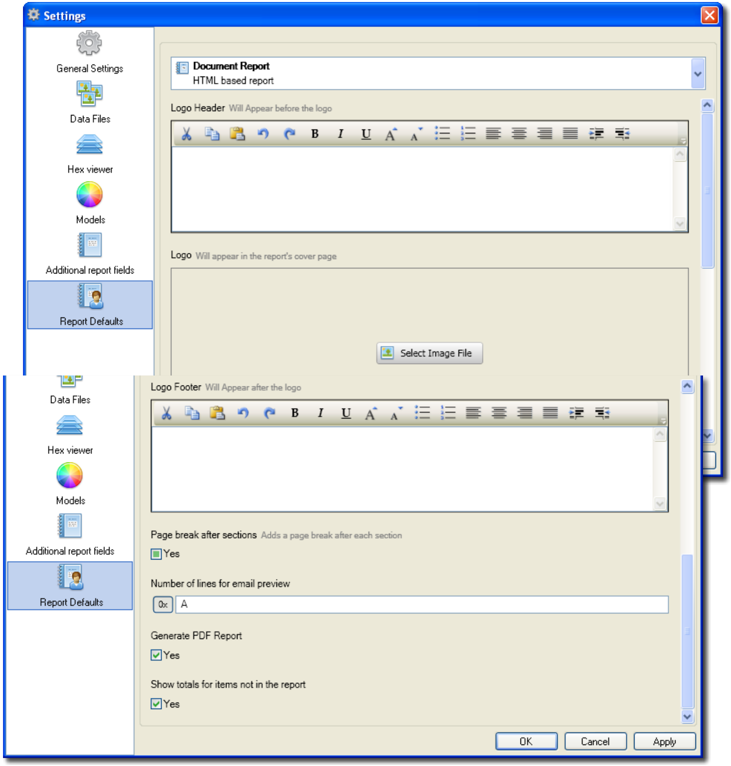
7.5.2 **Report Defaults**

The **Report Defaults** settings enables you to specify the following report options:

- **Report type** - Select the type of report to display its relevant report option.

7.5.2.1 **HTML/PDF Report Settings**

- **Logo Header** - Text area where you can enter and format custum text that will appear in the report header before the logo image.
- **Logo** - Click on the **Select Image File** button to add the logo image that will be added to the report header. Available file formats are: BMP, JPG, GIF, and PNG.
- **Logo Footer** - Text area where you can enter and format custum text that will appear in the report header after the logo image.
- **Page break after sections** - Selecting this option will set each section of the report to start on a new page.



Document Report
HTML based report

Logo Header Will Appear before the logo

Logo Will appear in the report's cover page

Logo Footer Will Appear after the logo

Page break after sections Adds a page break after each section
■ Yes

Number of lines for email preview
0x A

Generate PDF Report
☑ Yes

Show totals for items not in the report
☑ Yes

Figure 77: Reports - Report Defaults settings

- **Number of lines for email preview** - Sets the maximum number of lines from each email message that will appear in the report.
- **Generate PDF Report** - Generates a PDF version of the report in addition to the report file in the selected report format.
- **Show totals for items not in the report** - Adds a Total column to the report displaying the total number of items that were excluded from the report.

7.5.2.2 Excel Report Settings

- **Unprintable characters placeholder** - Set the placeholder character that will replace the unprintable characters.
- **Email body size limit** - Sets the maximum number of lines from each email message that will appear in the report.

Appendix A: **Using Python in the Physical Analyzer**

1.1 Accessing the data store

```
>>> ds
DataStore for device SAMD500 (3 file systems (3506 nodes), 1398 models)
```

1.2 File Systems, Files and Directories

1.2.1 Listing the current file systems

```
>>> for fs in ds.FileSystems:
    print fs.Name

KFAT0
Samsung MCU
Samsung Linked List
```

1.2.2 Get a specific file system by name

```
>>> fs = ds.FileSystems["KFAT0"]
>>> fs
FileSystem 'KFAT0' (712 nodes) [DRM, IMAGES, WAP, dir_vfp_temp, multimedia, @
samsung.ess, SMS, JAVA, SYNCML, @SAMSUNG.ESS, BROWSER, SOUNDS, EMAIL, TEST, USER,
MMS, tfsVersionCode.tfs]
```

1.2.3 Go over all files in a file system (recursively)

```
>>> fs = ds.FileSystems["KFAT0"]
>>> for f in fs.GetAllNodes():
    print f.AbsolutePath

/DRM
/DRM/RIGHTS
/DRM/RIGHTS/macrainit.bin
/DRM/RIGHTS/ssc.dat
/DRM/TEMP
/IMAGES
/IMAGES/charging_ani_01.icn
...
```

1.2.4 Get a specific file by path

```
>>>  f = ds.FileSystems["KFAT0"]["/SMS/sms.dat"]
>>>  f
File '/SMS/sms.dat' (39600b)
```

1.2.5 Print some information about the file

```
>>>  f = ds.FileSystems["KFAT0"]["/SMS/sms.dat"]
>>>  f.Name
'sms.dat'
>>>  f.Size
39600L
>>>  f.AbsolutePath
'/SMS/sms.dat'
>>>  f.Deleted
Data.Files.DeletedState.Intact
>>>  f.Parent
Directory '/SMS' (7 children) [sms.dat, aniheader, ANI, imageheader, MELODY,
animation, IMAGE]
```

1.2.6 List all files in a directory

```
>>> for f in ds.FileSystems["KFAT0"]["/SMS"]:
        print f.Name


sms.dat
aniheader
ANI
imageheader
MELODY
animation
IMAGE
```

1.2.7 Searching for files with a regular expression

```
for i in f.Search("/multimedia/.*jpg$"):
        print i.AbsolutePath


/multimedia/IMAGES/downloaded images/62 New - Samsung D500 128x96 1-6.jpg
/multimedia/IMAGES/downloaded images/6 LG U8330 94x144 1-5.jpg
/multimedia/IMAGES/downloaded images/Vladi_Img3.jpg
/multimedia/IMAGES/downloaded images/55 New - SAMSUNG S410i 176x148 2-5.jpg
...
```

1.2.8 Find out if a node is a file or a directory

```
>>>  f = ds.FileSystems["KFAT0"]["/SMS/sms.dat"]
>>>  if (f.Type == NodeType.File):
     print "This is a file"
elif (f.Type == NodeType.Directory):
     print "This is a directory"

This is a file
```

1.2.9 Reading data from a file

```
>>>  f = ds.FileSystems["KFAT0"]["/SMS/sms.dat"]
>>>  f.seek(0) # go to the beginning of the file
>>>  f.read(50)
u'\x07\x00\x00\x81\x00\x00\x00\x00$\x18\x96\x18\x00\x00\x01\xff\x0b\x81\x00\x90\x96\
x07P\xf9\xff\xff\xff\xff\x00\x00\xff\xff\xff\xff\xff\xff\xff\xa0AaX\x1c\x14\x86\
xc5AaP\x18\x16'
```

1.2.10 Viewing data in a textual hex dump

```
>>> data = f.read(300)
>>> hexdump(data)
00000000:  0785 6171 5018 1486 c541 6158 1c14 0685 | ..aqP....AaX....
00000010:  6171 5018 1607 8541 6158 1c14 86c5 4161 | aqP....AaX....Aa
00000020:  5018 1607 8561 7150 1814 86c5 4161 581c | P....aqP....AaX.
00000030:  1406 8561 7150 1816 0785 4161 581c 1486 | ...aqP....AaX...
00000040:  c541 6150 1816 0785 6171 5018 1486 c541 | .AaP....aqP....A
00000050:  6158 1c14 0685 6171 5018 1607 8541 6158 | aX....aqP....AaX
00000060:  1c14 86c5 4161 5018 1607 8561 7150 1814 | ....AaP....aqP..
00000070:  86c5 4161 581c 1406 8561 7150 1816 0785 | ..AaX....aqP....
00000080:  0000 0000 0000 0000 0000 dcad 4445 4144 | ............DEAD
00000090:  4245 4546 0700 0081 0000 0000 2418 9618 | BEEF........$...
000000a0:  0000 0100 0b81 0090 9682 59f1 ffff ffff | ..........Y.....
000000b0:  0000 ffff ffff ffff ff5b d3b7 3c0d 1a87 | .........[..<...
000000c0:  dd27 3aa8 5d2e d341 74f9 bb2e 6697 c9a0 | .':.]..At...f...
000000d0:  f69b 8e2e cb41 e3f7 1c24 9697 dde4 b01b | .....A...$......
000000e0:  546e 97e5 e7b2 7b9c 07c1 e5e1 313d 3d2e | Tn....{.....1==.
000000f0:  8740 f734 9b0d 9a97 cb20 7459 0e62 87e9 | .@.4..... tY.b..
00000100:  65b9 0b44 47af e72e 8502 ffff ffff ffff | e..DG...........
00000110:  ffff ffff ffff ffff ffff ffff ffff ffff | ................
00000120:  ffff ffff ffff ffff ffff ffff           | ............
```

1.2.11 **Creating a new file (without data)**

```
>>>  new_file = Node("new_file.dat", NodeType.File)
>>>  new_file.Deleted = DeletedState.Deleted # mark this file as deleted
>>>  fs["/SMS"].Children.Add(new_file)       # add to a directory
>>>
>>>  # list the files to see if it’s there
>>>  for i in fs["/SMS"]:
     print i.Name

sms.dat
aniheader
ANI
imageheader
MELODY
animation
IMAGE
new_file.dat          ‹ new file exists in the directory
```

1.2.12 **Creating a new file from chunks**

(Read more about chunks in the architecture section)

```
>>>  # get the sms.dat file out
>>>  sms_dat = ds.FileSystems["KFAT0"]["/sms/sms.dat"]
>>>  # first let’s create the MemoryRange with chunks from the sms.dat file
>>>  chunks = []
>>>  chunks.append(Chunk(sms_dat.Data, 0, 1024)) # take the first KB
>>>  chunks.append(Chunk(sms_dat.Data, 5000, 1024)) # take 1KB from offset 5000
>>>  chunks.append(EmptyChunk(1000)) # add 1000 zero bytes
>>>
>>>  new_file.Data = MemoryRange(chunks) # set the file’s data
```

1.3 Memory Ranges

1.3.1 Accessing the project's Memory Ranges

```
>>>  ds.MemoryRanges
MemoryRangeCollection (3 items) ['MCU', 'CTS', 'CTS Remapped (XSR)']
>>>  for m in ds.MemoryRanges.All:
     print m.Name
MCU
CTS
CTS Remapped (XSR)
>>>  cts = ds.MemoryRanges['CTS']
>>>  cts
MemoryNode 'CTS' (69206016b in 1 chunks), 1 child
>>>  cts.Length
69206016L
>>>  cts.LengthMB # length in megabytes
66.0
```

1.3.2 Reading data from a Memory Range

This is done the same way as reading data from a file. **`file.Data`** is a **`MemoryRange`** object.

```
>>> mr = ds.MemoryRanges["CTS"]
>>> mr.seek(0) # go to the beginning of the data
>>> mr.read(50)
u'd\x00\x00\x00\x0f\x00\x00\x00\x01\x00\x00\x00XSR1\x00\x00\x00\x00\x00\x00\x00\x00\
xa5\xa5\xa5\xa5\x08\x08\x00\x00\x01\x00\x00\x00\xff\xff\xff\xff\xff\xff\xff\xff\xfe\
xff\xff\xff\xa7\xac'
```

1.3.3 Creating a new MemoryRange and adding to the project

A **`MemoryNode`** is a **`MemoryRange`** with a name and children. It can therefore exist in the Memory Ranges section of the project. To add a **`MemoryRange`** to a project, you must first create a **`MemoryNode`** from it.

```
>>> mr = MemoryRange(chunks)
>>> mn = MemoryNode("MyNode", mr)
>>> ds.MemoryRanges.Add(mn)
```

You can also create a **`MemoryNode`** directly with a name and a list of chunks:

```
>>> mn = MemoryNode("MyNode", chunks)
>>> ds.MemoryRanges.Add(mn)
```

Creating file data from **MemoryNodes** or **MemoryRanges** works the same as creating file data from other files.

```
>>>  # get our memoryrange out
>>>  cts = ds.MemoryRanges["CTS"]
>>>  chunks = []
>>>  chunks.append(Chunk(cts, 1048576, 65536)) # take 64k from offset 1MB
>>>  chunks.append(Chunk(cts, 0x18E0000, 32)) # take 32 bytes from 0x18E0000
>>>
>>>  new_file.Data = MemoryRange(chunks) # set the file’s data
```

A shorthand for getting just part of a **MemoryRange** into a new **MemoryRange** is **GetSubRange()**:

```
>>>  second_kb = original.GetSubRange(1024, 1024) # (offset, length)
```

1.4 Models

The Physical Analyzer application introduces the concept of Models. SMS messages, Calls, Contacts and the like are all models. All the models are based on the same logic, so what works for SMS messages works also for Contacts and Calls. Also, in the future it will be possible to add new user-defined models.

1.4.1 Accessing the Model Store

```
>>>  ds.Models
ModelStore {Call: <3 items>, Contact: <1285 items>, SMS: <192 items>}
```

1.4.2 Counting the amount of SMSes

```
>>>  ds.Models[SMS].Count
192
```

1.4.3 Print some details about an SMS

```
>>>  s = ds.Models[SMS][0]
>>>  s
SMS {Status: Field(Default), To: Field(00096970059), Folder: Field(Drafts), Message:
Field(This is a text message)}
```

1.4.4 Print the SMS “Message” Field for all SMSes

```
>>>  for i in ds.Models[SMS]:
     print i.Message.Value

I'm at home. Please call
I'm at work. Please call
I'm in a meeting, call me later at
Meeting is canceled.
I am late. I will be there at
See you in
See you at
Sorry, I can't help you on this.
I will be arriving at
...
```

1.4.5 Create a new SMS message

```
>>>  s = SMS()
>>>  s.Parties.Add(Party("341414141", PartyRole.From)) # add a “from” party
>>>
>>>  # multiple parties are possible, so we use Add
>>>  s.Parties.Add(Party("234646335", PartyRole.To)) # add a “to” party
>>>
>>>  # When we aren’t sure about from/to, we add a “general” party
>>>  s.Parties.Add(Party("353753536"))
>>>
>>>  s.Body.Value = "Example text"
>>>  s.SMSC.Value = "238423842"
>>>
>>>  s.Deleted = DeletedState.Deleted # set this SMS as deleted
>>>  ds.Models.Add(s)
```

Creating a new Call or a new Contact is similar, but the fields (marked in pink) are different.

1.4.6 Using AddRange to add models quickly

When adding a large amount of models to a project, it is much more efficient to use the **AddRange** method.

```
>>>  smses = create_many_smses()
>>>  len(smses)
1356
>>>  # Now we’ll add all the SMSes at once
>>>  ds.Models.AddRange(smses)
```

1.4.7 Create a new Call

```
>>>  c = Call()
>>>  c.Party.Value = "03453552234"
>>>  c.Type.Value = CallType.Outgoing
>>>  # There’s also TimeStamp and Duration
>>>
>>>  ds.Models.Add(c)
```

1.4.8 Create a new Contact

```
>>>  n = Contact()
>>>  n.Name.Value = "Jack Johanson"
>>>  n.Entries.Add(PhoneNumber("123123", "Home")) # Home is the category
>>>  n.Entries.Add(EmailAddress("jack@example.com", "Office"))
>>>  # Mark as deleted
>>>  n.Deleted = DeletedState.Deleted
>>>
>>>  ds.Models.Add(n)
```

1.4.9 Create a new Email

```
>>>  e = Email() # MMS messages have the same fields, just create an MMS object
>>>  e.From.Value = "Alfred Vogel <alfred@vogel.com>"
>>>  e.To.Add("jim@jimmers.com") # Multiple To, Cc and Bcc are possible
>>>  e.To.Add("jamest@abc.com")
>>>  e.Cc.Add("thomasr@abc.com")
>>>  e.Bcc.Add("contact@more.com")
>>>
>>>  e.Subject.Value = "An Important Email from Alfred"
>>>  e.Body.Value = "You’re invited to Alfred’s party! ..."
>>>
>>>  e.Priority.Value = MailPriority.High
>>>
>>>  # set the timestamp to Feb 1, 2009 at 10:50:30 AM
>>>  e.TimeStamp.Value = TimeStamp(DateTime(2009, 2, 1, 10, 50, 30))
>>>
>>>  ds.Models.Add(e)
```

1.4.10 Create a new MMS Message

MMS messages are very similar to e-mails. Therefore, to make things easier, e-mails and MMS behave the same way in the PA world. Just create an **`MMS()`** object instead of an **`Email()`** object, and fill in the fields in the same way.

1.4.11 Add an Attachment to an Email (or MMS)

```
>>>  a = Attachment()
>>>  a.Filename.Value = "coolimage.jpg"
>>>  a.ContentType.Value = "image/jpg"
>>>  a.Data.Source = MemoryRange(...)
>>>  # you can also use a file’s data by using this syntax:
>>>  a.Data.Source = your_file.Data
>>>  # another trick is using GetSubRange() to quickly get only part of a file
>>>  a.Data.Source = your_file.Data.GetSubRange(your_offset, your_length)
>>>
>>>  your_email_or_mms.Attachments.Add(a) # add the attachment
```

1.4.12 **Create a new Location**

A Location is a GPS coordinate with added information such as the street address, timestamp and others.

```
>>>  loc = Location()
>>>  loc.Position.Value = Coordinate(34.556, 20.450534) # lat, long
>>>  loc.RoadPosition.Value = Coordinate(34.558, 20.451)
>>>  addr = StreetAddress()
>>>  addr.City.Value = "Paris"
>>>  addr.Country.Value = "France"
...
>>>  loc.Address.Value = addr
>>>  loc.Name.Value = "My House"
>>>  loc.Description.Value = "In the middle of the street"
>>>
>>>  ds.Models.Add(loc)
```

1.4.13 Create a new Journey

A Journey is a name for a list of Locations, with some added information about the entire trip. This model is useful for trip logs or track logs as they are saved in some GPS devices.

```
>>>  j = Journey()
>>>  j.WayPoints.Add(loc) # loc is a Location object
>>>  j.WayPoints.Add(loc2)
>>>  j.WayPoints.Add(loc3)
>>>  j.WayPoints.Add(loc4)
>>>  j.Name.Value = "Trip #47"
>>>
>>>  ds.Models.Add(j)
```

1.4.14 Create a new Instant Message

```
>>>  m = InstantMessage()
>>>  m.From.Value = "PersonA"
>>>  m.To.Add("PersonB")
>>>  m.To.Add("PersonC")
>>>  m.Body.Value = "Hi B and C! What’s up?"
>>>
>>>  ds.Models.Add(m)
```

1.4.15 **Create a new Chat**

Chats, much like Journeys for Locations, are an aggregation of instant messages, with some added metadata about the conversation itself. Chats are an effective way of storing a list of messages belonging to the same conversation.

```
>>>  c = Chat()
>>>  c.Messages.Add(msg) # msg is an InstantMessage object
>>>  c.Messages.Add(msg2)
>>>  c.StartTime.Value = TimeStamp(DateTime(2009, 10, 3, 10, 45, 12))
>>>  c.LastActivity.Value = TimeStamp(DateTime(2009, 10, 3, 11, 15, 32))
>>>  c.Participants.Value = "PersonA, PersonB, PersonC"
>>>
>>>  ds.Models.Add(c)
```

1.4.16 **Create a new Calendar Entry**

CalendarEntry models have many fields. Therefore, only a partial example is given below.

```
>>>  c = CalendarEntry()
>>>  c.Details.Value = "Important meeting!"
>>>  # More fields like Details are Category, Subject and Location
>>>  c.StartDate.Value = TimeStamp(DateTime(2010, 9, 10, 15, 40, 0))
>>>  # More date fields are EndDate and Reminder
>>>
>>>  ds.Models.Add(c)
```

1.4.17 **Create a new Note**

```
>>>  n = Note()
>>>  n.Title.Value = "Note to self"
>>>  n.Body.Value = "I’m awesome!"
>>>  n.Summary.Value = "Summarily, I’m awesome!"
>>>  n.Creation.Value = TimeStamp(DateTime(2010, 9, 10, 15, 40, 0))
>>>  n.Modification.Value = TimeStamp(DateTime(2010, 9, 10, 15, 40, 0))
>>>
>>>  ds.Models.Add(n)
```

1.4.18 Create a new Bluetooth Device

```
>>>  d = BluetoothDevice()
>>>  d.Name.Value = "Gilad’s iPhone"
>>>  d.MACAddress.Value = "00:01:34:55:66:77"
>>>  d.Info.Value = "An awesome iPhone"
>>>
>>>  ds.Models.Add(d)
```

mcsira

cellebrite

UFED system

www.McSira.com

info@McSira.com