Universal Forensic Extraction Device (UFED)

Agenda

- Understanding how cell phones work
- Introduction to the Universal Forensic Extraction Device (UFED)
  - Safety/Environment
  - Overview
  - Power options/indicator
  - Report Manager Software
- Extract Phone Data
- Practical Exercise

Understanding how cell phones work

General Cellular Network Map

Mobile Telephone Switching Office

Public Switched Telephone Network

Mobile Switching Center

Broadcasting System Identification Code (SID)

HLR

SMS

MMS

EMAIL

Base Transceiver Station (BTS)

Off-site Data Storage Facility (Advanced/Smart Phones)

Cell Phone Access Technologies

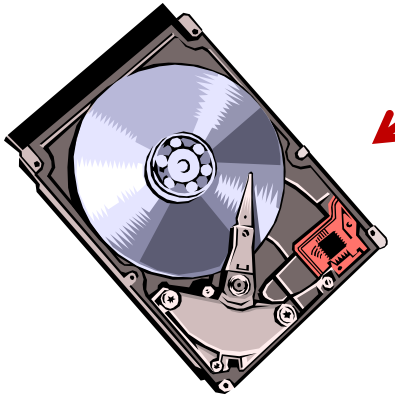
- **Frequency Division Multiple Access (FDMA)**
  Places each caller on a separate frequency
- **Time Division Multiple Access (TDMA)**
  Assigns each caller a portion of time on designated frequency
- **Code Division Multiple Access (CDMA)**
  Provides unique code to callers and spreads it over available frequencies
- **Global System for Mobile (GSM)**
  Uses TDMA with encryption to secure separate channels

GSM/PCS Format

- Truly digital, third generation system
- Uses TDMA overlay of FDMA system, with Data and Voice Channels
- Allows use of Subscriber Identity Modules (SIM)
- Data based subscriber information to reduce fraud, enhance usage

Memory Considerations

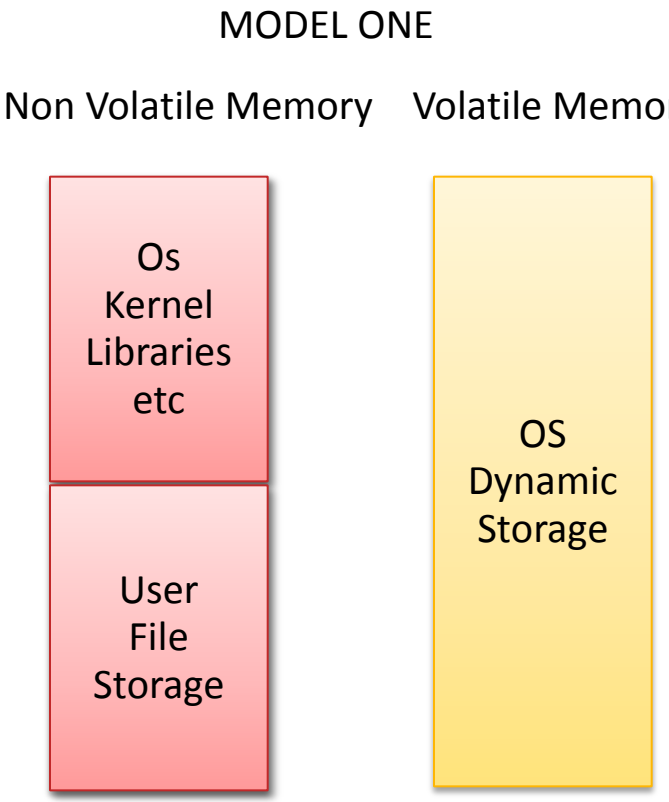
Traditional Forensics Complete Analysis of the Volume

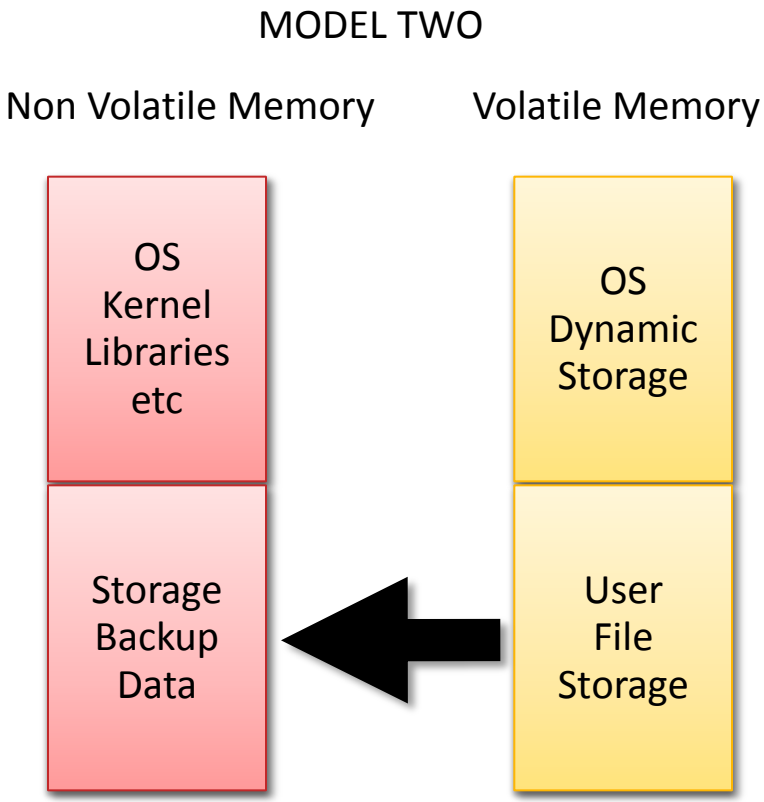


Hard Drive for Example

- The Cell Phone works differently, data is stored in container storage or slotted storage.
- A command must be issued to the phone to acquire the Cell Phone

Memory Considerations





Memory - Smart Phones

- Any phone that has an OS is connected to by the OS itself
- Third party applications are not always required to connect to the memory container of the phone
- Phones like the IPHONE require the use of ITUNES, an Apple specific application
- Phones that come with Android allow for full connectivity to the storage containers.

Cloud Network

Must have an Analytics Tool

Actionable Intelligence/Evidence location

- The Subscriber Identity Module (SIM)
  - Customer Identification (IMSI)
  - List of telephone numbers stored by the user
  - List of telephone numbers dialed by the user
  - Text Messages – including deleted messages
  - Location information from the position of last usage
- Phone Internal Memory
  - Phone identity
  - Stored audio recordings
  - Images from camera or multimedia messages
  - Stored computer files
- Flash/SD (micro/mini) Memory Cards

Introduction to the Universal Forensic Extraction Device (UFED)

UFED Overview

- The Cellebrite UFED Forensics system enables you to capture critical forensic evidence and intelligence from mobile phones, Smart phones and PDAs.

UFED Overview

- Extracts vital data such as phonebook, camera pictures, videos, audio, text messages (SMS), call logs, ESN IMEI, ICCID and IMSI information from over 1,600 handset models, including Symbian, Microsoft Mobile, Blackberry and Palm OS devices.

- Enables SIM ID cloning, allowing you to extract phone data while preventing the cellular device from connecting to the network.

UFED Overview

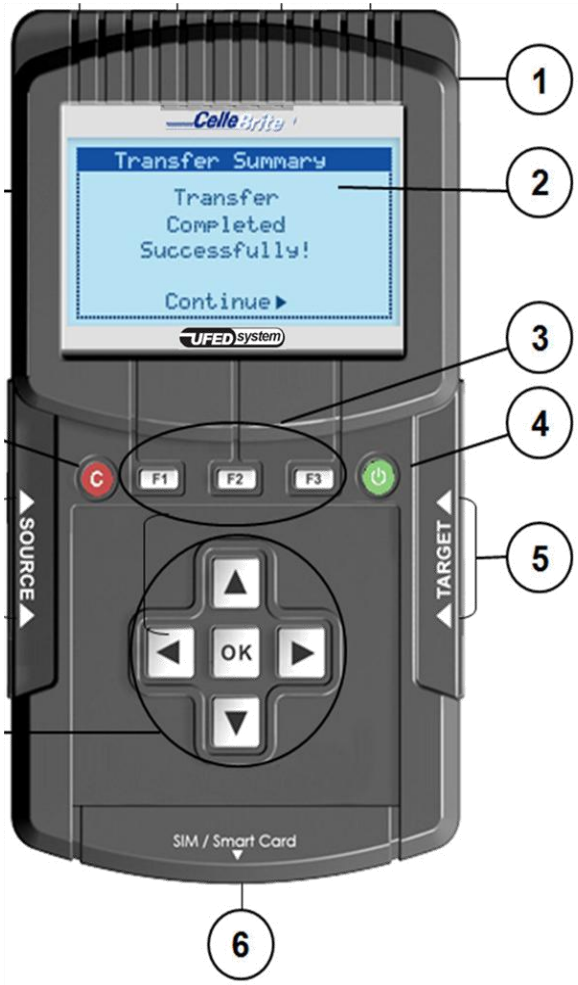
- The UFED can extract data from a phone, or directly from the SIM card.
  - When extracting from phone, the UFED connects to the phone via cable, Bluetooth or infrared, and the data is read logically from the phone.
  - It also performs a physical extraction from SIM cards, allowing extraction of additional data such as deleted SMS, ICCID, IMSI, location information and more.

UFED Overview

- Data is copied to any standard USB flash drive or SD card and is then organized into clear and concise reports.
  - The UFED Report Manager software on a PC creates detailed reports of the extracted data that can be used as evidence.
  - Reports include full extraction details as well as MD5/SHA256 hash information that proves that the data is original and untouched.

UFED Device Overview

1. Power Supply (Connect to power adapter)
2. LCD Display
3. Function Keys (F1 for help. F2 for select/deselect all)
4. ON/OFF Power Button
5. Target-side Connectors (For extraction to USB disk drive)
6. SIM / Smart Card Slots (Slot for reading SIM cards and smart cards)



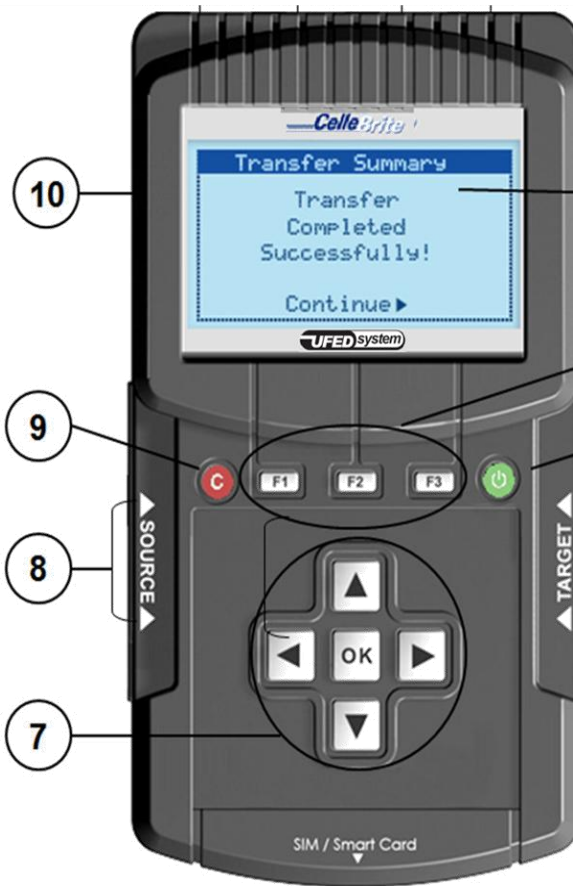
UFED Device Overview

7. Navigation Keys (For navigating the UFED menu)

8. Source-side Connectors (Connect phone via USB, serial or IR)

9. Cancel Button

10. SD Card Slot (For extraction to SD card)



UFED Device Overview

11. USB Port Extension (For Bluetooth dongle or other external devices i.e. keyboard)

12. Serial connection (not in use)

13. Ethernet port (for network connection for automatic updates and uploading data to a network)

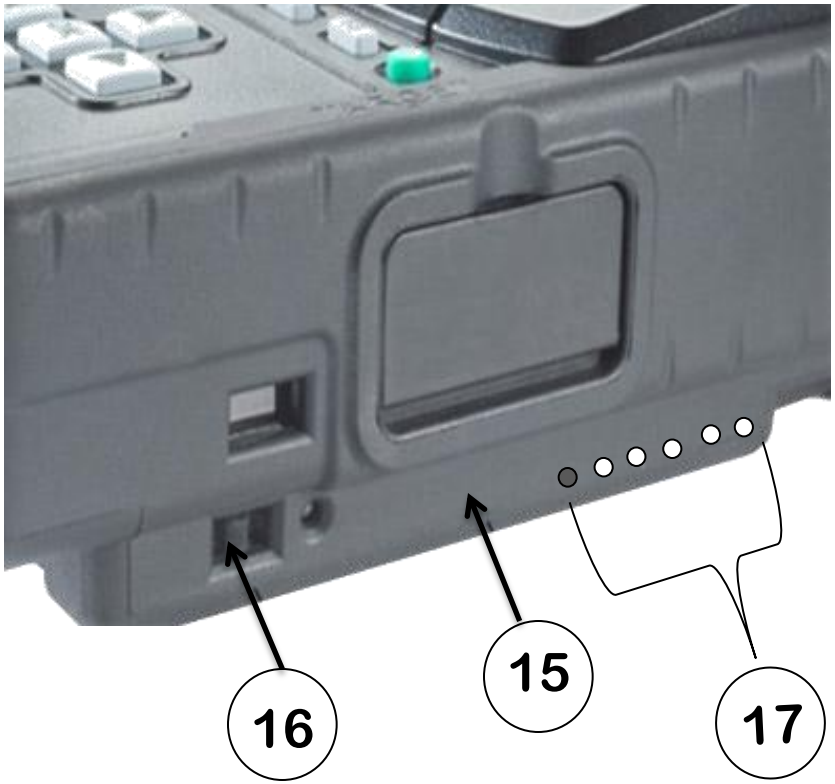
14. Mini-USB Port (connect to a PC via mini-USB cable, for extraction to PC)

UFED Device Overview

15. Battery kit and battery housing protective covering

16. Charging Switch

17. Battery state-of-charge-test and LED's



UFED Power Options

- The UFED device can be powered by an AC power supply, a car power supply, or by battery power.
  - To run the UFED on battery power, flip the charging switch to the right (“BAT”) position.
  - To re-charge the battery, connect the device to an AC adapter (supplied with the kit), and then flip the charging switch to the left (“CHG”) position.

Charging Switch

LED Power Indicator

- The LED indicator provides input regarding the state of the UFED power
  - **Red:** Battery charge in process
  - **Green:** Battery fully charged
  - **No light:** Sleep mode (no input power source) OR no battery connected OR charge suspended (timer fault or thermal shutdown) OR over-voltage fault
  - **Flashing Red:** Indicates a problem with the battery. Verify that the battery is connected properly.

Carrying Case

- The UFED Ruggedized carrying case is designed specifically for field use conditions.

- To open the case, flip the two latches open.

Initial Setup

Initial Setup

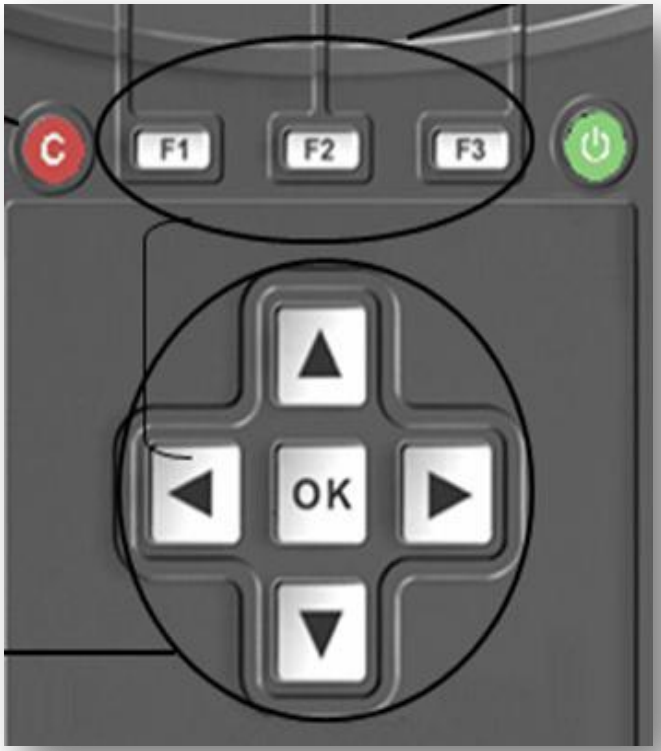
- Remove the UFED device from the case.
- Connect the power supply adapter to the UFED. “Please Wait” appears briefly on the screen, followed by a screen showing the version numbers.
- When starting the UFED for the first time, you need to set the date, time and GMT.
- The UFED is ready to be used, and the Main Menu is displayed.

Main Menu

- **Extract Phone Data** - This option is for extracting data from a mobile phone.
- **Extract SIM/USIM Data** – This option is physical extraction directly from a SIM card.
- **Clone SIM ID** – This option copies a SIM card, enabling you to analyze the phone without it being open for incoming calls.
- **Services** - Allows you to upgrade your UFED with updated phone support. You can also use Services to perform various administrative tasks.

UFED Menu Navigation

- Use the ▲ ▼ keys to move between options.
- To select an option, press ▶ or the **OK** key.
- To return to the previous menu, press ◀
- When additional help is available, a help icon will appear in the upper left of the screen. Press F1 to view this help.

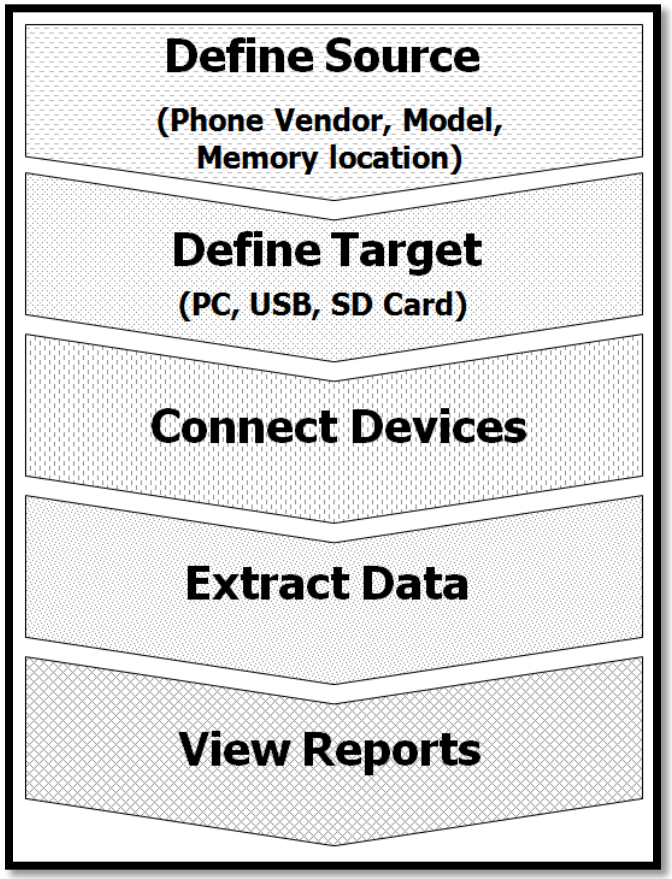


Extract Cell Phone Data

Extract Cell Phone Data

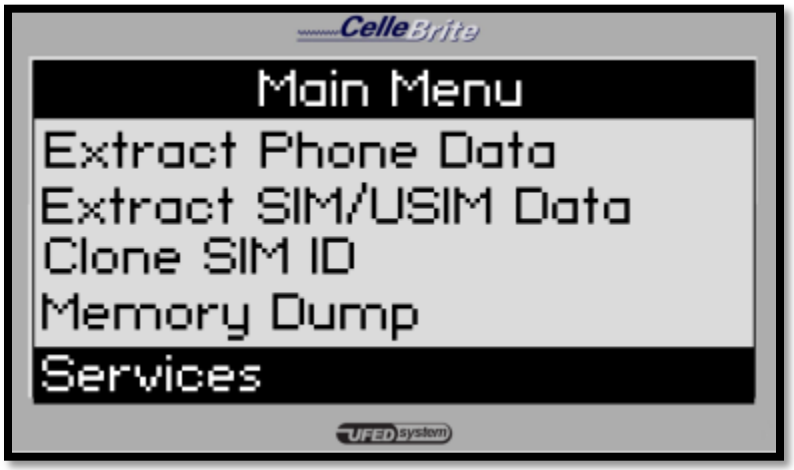
- Overview
  - Select “Extract Phone Data” from the main menu in order to copy data from a phone (the source) to a PC, USB or SD card (the target)
  - Use this function to extract phonebook, SMS text messages, pictures, etc. from mobile phone memory to a USB disk drive, SD card or directly to a PC.

The UFED guides you through each step of the process



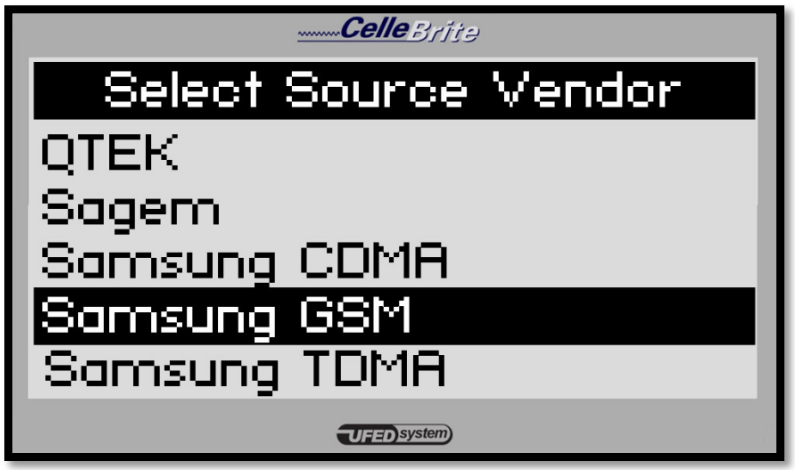
Extract Cell Phone Data to USB Disk Drive or SD Card

- Main Menu
  - Use the ▲ ▼ keys to move between options.
  - Select “Extract Phone Data” from the main menu.
  - Press “OK” or ▶ to continue.



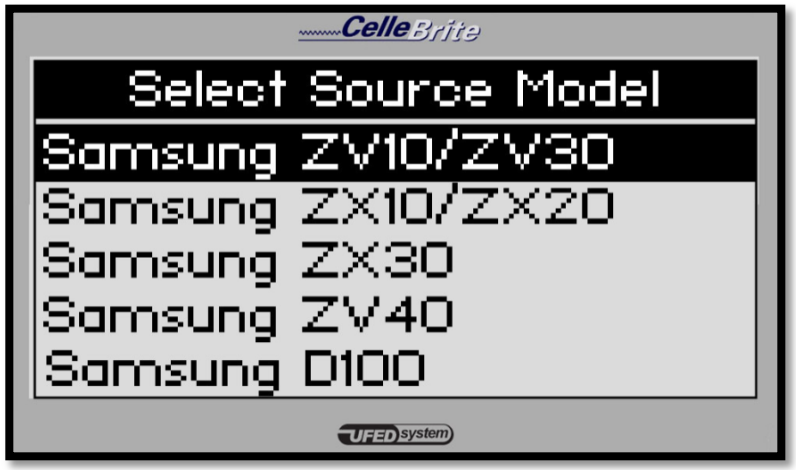
Extract Cell Phone Data to USB Disk Drive or SD Card

- Select the vendor (manufacturer) of the source phone.
- Use the ▲▼ keys to move between options.
- Press “OK” or ▶ to continue.



Extract Cell Phone Data to USB Disk Drive or SD Card

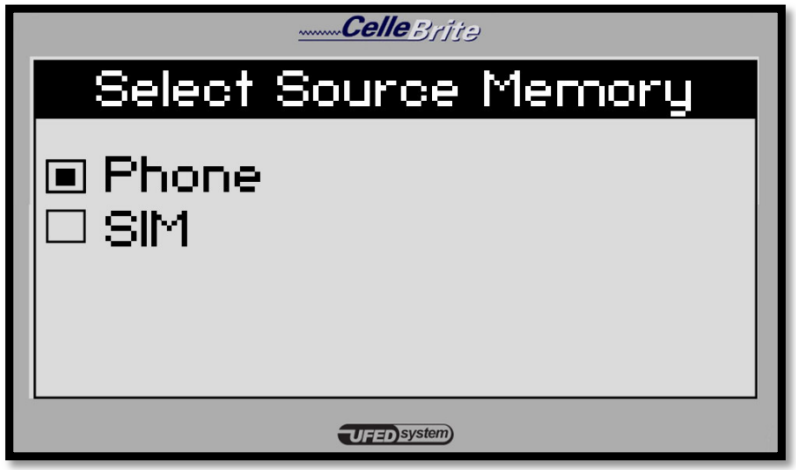
- Select the source phone model.
- Use the ▲▼ keys to move between options.
- Press “OK” or ▶ to continue. Press ◀ to go back



NOTE: If you do not know the model, you can often find the phone model on a sticker beneath the battery.

Extract Cell Phone Data to USB Disk Drive or SD Card

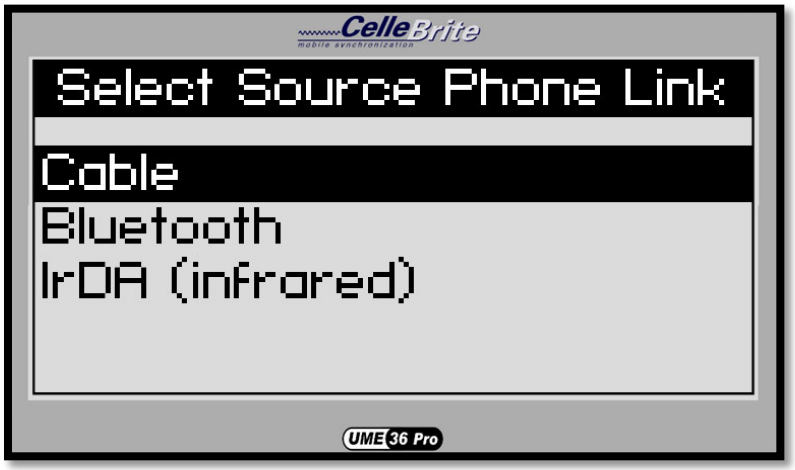
- Select the source memory location you wish to extract.
- Use the ▲▼ keys to move between options.
- Press “OK” to select the currently highlighted option, or press “F2” to select all.
- Press ▶ to continue.



NOTE: Some phones do not allow access to the SIM card data via the data cable. In these cases, you will be prompted during the process to remove the SIM card and insert it into the SIM Card Slot.

Extract Cell Phone Data to USB Disk Drive or SD Card

- Source Link
  - This step determines how the phone will connect to the UFED.
  - This message appears only if the phone supports more than one connection method (Cable, Bluetooth or IrDA-Infrared).
- Operate arrow and “OK” keys as before



NOTE: For best speed and reliability, use a cable whenever possible.

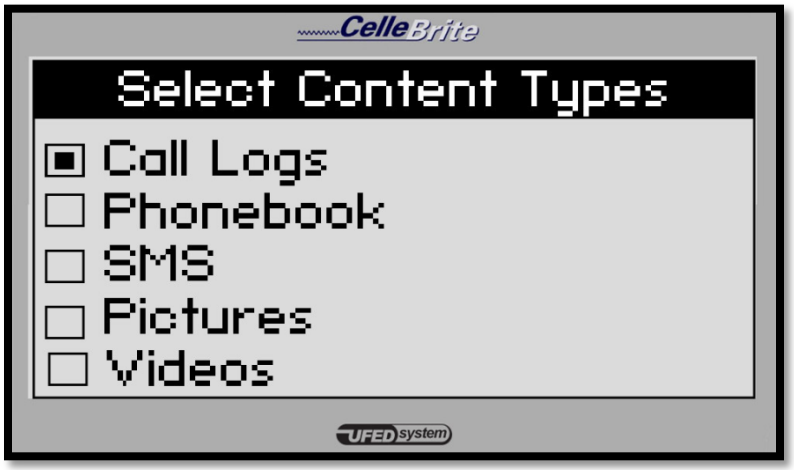
Extract Cell Phone Data to USB Disk Drive or SD Card

- Target Selection
  - Select “USB” or “SD card” as the target location where the content will be copied to.
- Operate arrow and “OK” keys as before

NOTE: If you extract to PC, the content goes directly into the UFED Report Manager software. If you extract to USB or SD, the content is stored in a separate directory on the storage device.

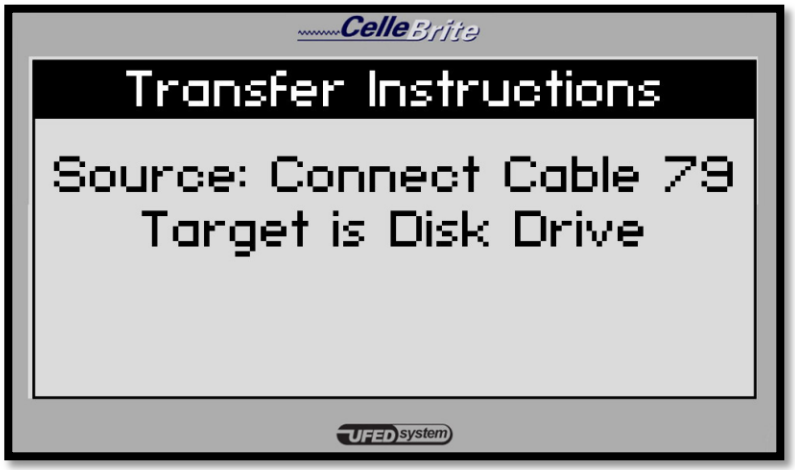
Extract Cell Phone Data to USB Disk Drive or SD Card

- Content Types
  - Select “Content Types” to be extracted.
  - The UFED displays the options according to the capabilities available in the phone. (ex. If the phone does not support video, the “Videos” option will not appear).
- Operate arrow and “OK” keys as before. “F2” selects or deselects all.



Extract Cell Phone Data to USB Disk Drive or SD Card

- The UFED now displays the connectivity instructions.
  - If connecting via cable, the cable number is displayed.
  - Make sure that the phone is powered on, and the data connector is clean.
  - Press ▶ to continue.



NOTE: When connected to the UFED, some phones will prompt you to choose an operating mode, such as “PC Suite” or “Phone Mode”.

Extract Cell Phone Data to USB Disk Drive or SD Card

- If you have not yet plugged the USB drive or SD card into the UFED, do it now.
- The UFED is ready to copy the data to the storage device.
- Press ▶ to continue.

WARNING: Do not disconnect the phone or the power adaptor during the process! Once started, the process should not be interrupted.

Extract Cell Phone Data to USB Disk Drive or SD Card

- If the phone is a Smart Phone or PDA, you may need to install a client application on the phone.

- Press ▶ to continue.

Extract Cell Phone Data to USB Disk Drive or SD Card

- Upon the completion of the process the UFED-displays a message.

- The message on the screen includes the phone's ESN (for CDMA/TDMA) OR IMEI (for GSM) number.

Extract Cell Phone Data to USB Disk Drive or SD Card

- Besides the standard user phone data, the UFED also provides metadata about the phone.
  - Among this data is the ESN (for CDMA/TDMA phones) or IMEI (for GSM phones).
  - The ESN or IMEA is a unique identifier or serial number uniquely associated with each single handset device.
- The transfer process is complete and you can disconnect the source and target devices from the UFED.

Extract Cell Phone Data to USB Disk Drive or SD Card

- The data is stored on the USB drive.
  - It can be opened in the UFED Report Manager PC software to analyze data and generate reports.
  - It is also stored in HTML format, and can be opened on any PC .

Smart Phones/PDA Support

- When extracting data from Smart Phones or PDA's, you will be asked to upload a client application from the UFED to the phone.
- This application enables access to the phone memory.
- Application upload is not necessary for Blackberry and Symbian 3rd edition phones.

Smart Phones/PDA Support

- Client Upload
  - When necessary, the UFED will inform you to upload the client application.

Smart Phones/PDA Support

- Install Client Prompt
  - The UFED now instructs you to run the installation on the phone.

Smart Phones/PDA Support

- Install and Run the client
  - If the phone prompts you to install, follow the installation steps. Then run the application. You can identify it by the icon. 
  - Pressing F1 on the UFED will inform you of the exact location where the program can be found on the phone.
- NOTE: After completing the entire extraction process, you need to uninstall the client from the phone.

Using Bluetooth Connectivity

- Phone Settings
  - On the mobile phone, you must enable the phone to connect via Bluetooth, by turning Bluetooth capabilities on.
- The UFED kit comes with a Bluetooth USB adapter
  - Insert the Bluetooth adapter in either of the two USB ports at the top of the UFED, as shown.
- Press the right arrow to continue.

UFED Bluetooth Adapter

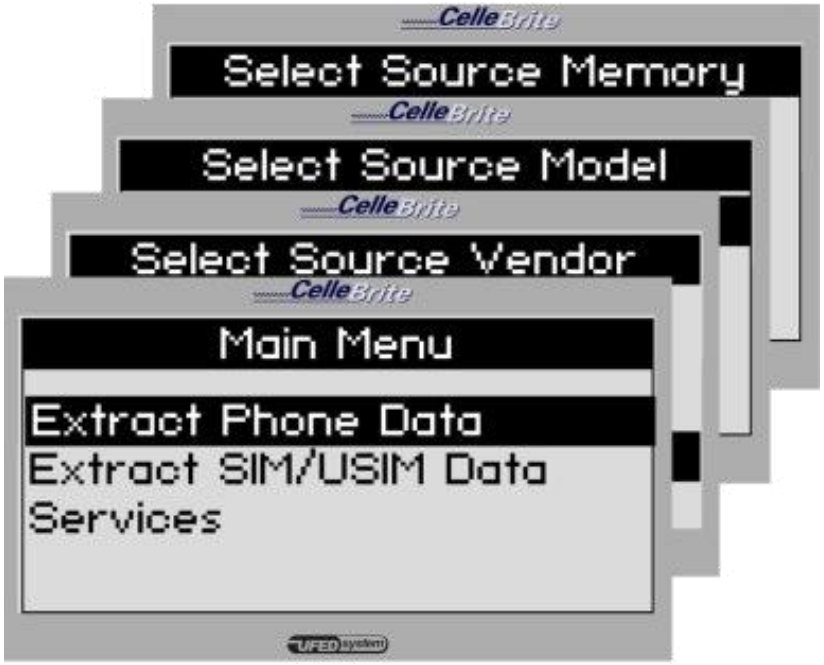
Bluetooth Dongle USB Ports

Using Bluetooth Connectivity

- Identifying the Phone via Bluetooth
  - The UFED searches for visible Bluetooth devices within its proximity, and provides a list of all devices that it finds.
  - Use the up and down keys to move between devices. Select the appropriate device from this list.
  - The UFED then instructs you to enter "0000" in the phone to complete the paring between the devices.
  - Press the right arrow to start the extraction process.

Extract Cell Phone Data to a PC

- Main Menu and Phone Definitions
  - This part of the process is identical to the previously USB or SD card extraction process.

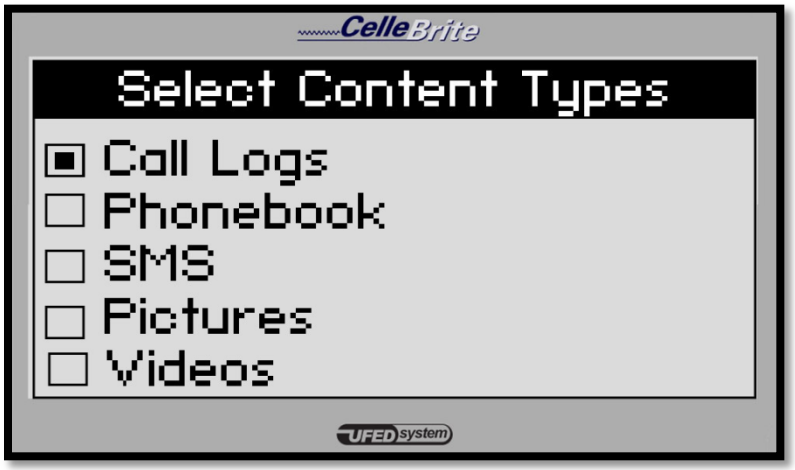


Extract Cell Phone Data to a PC

- Select PC from the target menu.
- Use the arrow keys to move between options. Press “OK” or ▶ to continue.

Extract Cell Phone Data to a PC

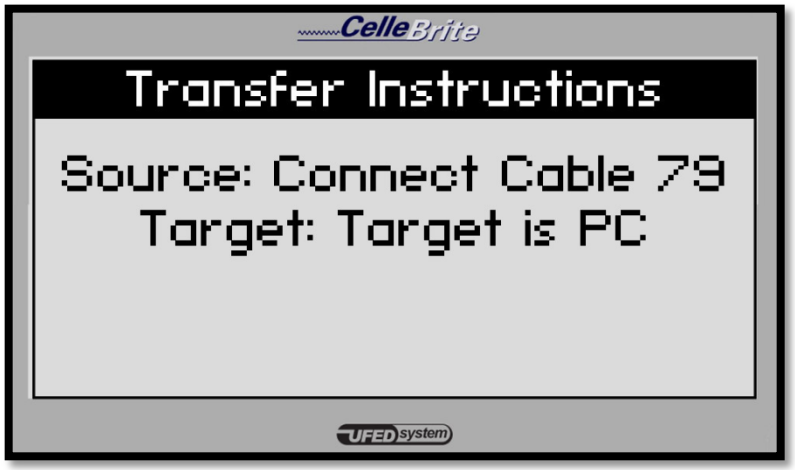
- Content Types
  - The UFED displays the options according to the capabilities available in the source phone.



NOTE: Transfer time varies according to the data types selected. Selecting all options will increase the transfer time.

Extract Cell Phone Data to a PC

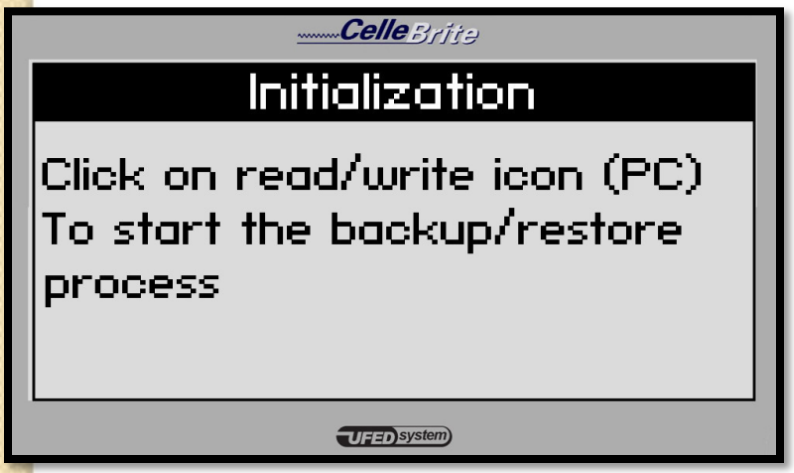
- Make sure that the UFED is connected to the PC using the mini-USB cable.
- The UFED displays the cable number to be used to connect the phone.



NOTE: When connected to the UFED, some phones will prompt you to choose an operating mode, such as “PC Suite” or “Phone Mode”.

Extract Cell Phone Data to a PC

- The UFED now extracts the selected data to its internal memory, the message below will appear at the end of the extraction.



Extract Cell Phone Data to a PC

- Read Data from Phone
  - Click the Read phone icon.

  - If connecting the phone via cable, the UFED informs you which cable number to use.
  - Find the cable in the cable organizer, according to the numbers indicated on the cable.

UFED Report Manager Software

UFED Report Manager Software

- Overview
  - The UFED System includes UFED Report Manager Software, which you can use to view and analyze the extracted data on your PC.
  - The UFED Report Manager enables you to:
    1. View and analyze the data extracted.
    2. Print a detailed report of the extracted content.
    3. Save extracted data.

UFED Report Manager Software

- Overview
  - Throughout the report, data is shown with its full MD5 hash information.
  - When extracting pictures, audio and video files, the UFED system calculates an MD5 hash of each file.
  - The MD5 hash provides a tamperproof signature of the source file.
  - Any modifications to the file will cause the MD5 hash to change. In this way, the MD5 hash proves the authenticity of each file.

UFED Report Manager Software

- Run the UFED Report Manager
  - Run the UFED Report Manager software on your PC by choosing Start/Programs/Cellebrite Mobile Synchronization/UFED Report Manager.

Summary

- Understanding how cell phones work
- Introduction to the Universal Forensic Extraction Device (UFED)
  - Safety/Environment
  - Overview
  - Power options/indicator
  - Report Manager Software
- Extract Phone Data
- Practical Exercise

QUESTIONS?