CUSTOMS AND BORDER PROTECTION
LABORATORIES AND SCIENTIFIC SERVICES

Portable Digital Media Examination and Analysis

ORIGINATED BY THE QUALITY MANAGEMENT BOARD

APPROVED BY: (b)(6) (b)(7)(C) [redacted]

SIGNATURE: DATE:

Laboratories and Scientific Services quality documents (manual, procedures, work instructions, etc.) contain law enforcement sensitive information and shall not be released to anyone other than Laboratories and Scientific Services personnel without the written approval of the Executive Director, Laboratories and Scientific Services.

1 PURPOSE

This procedure defines requirements for managing the flow of Portable Media evidence through Laboratories and Scientific Services (LSS) and ensures proper receipt, inventory, analysis and reporting of examination results. Digital forensics evidence includes data from, but not limited to, the following devices:

1.1 Cellular Phones (e.g., Motorola Flip or HTC Evo)
1.2 Global Positioning System (GPS) Devices (e.g., Garmin Nuvi or Furuno Mariner)
1.3 Personal Digital Assistant (PDA) Devices (e.g., Palm Zire or HP iPAQ)
1.4 Tablets (e.g., Samsung Galaxy S or Apple iPad) and Media/MP3 Players (e.g., Microsoft Zune or Apple iPod Shuffle)

2 SCOPE

Procedures described in this document apply to all portable media forensic samples submitted to LSS for imaging and analysis.

3 RESPONSIBILITY

3.1 In addition to responsibilities already delineated in (b) (7)(E) the Laboratory Director (LD) is also responsible for providing (b) (7)(E) for each examiner.
3.2 The Assistant Laboratory Director (ALD) and the Quality Manager retain their responsibilities as specified in (b) (7)(E)
3.3 The (b) (7)(E) or other designated employee, is responsible for entering the sample information into the (b) (7)(E)
3.4 The Portable Media Analyst (PMA) is responsible for the following:

3.4.1 (b) (7)(E)
3.4.2 (b) (7)(E)
3.4.3 (b) (7)(E)

3.5 The Portable Media Imager (PMI) is responsible for the following:

3.5.1 (b) (7)(E)
3.5.2 (b) (7)(E)
(b) (7)(E)
3.5.3 (b) (7)(E)
3.5.4 (b) (7)(E)
3.5.5 (b) (7)(E)
3.5.6 (b) (7)(E)
(b) (7)(E)
3.5.7 (b) (7)(E)

4 REFERENCES

4.1 (b) (7)(E) Quality Manual
4.2 (b) (7)(E) Management of Samples
4.3 (b) (7)(E)
4.4 (b) (7)(E) Data Management and Reporting
4.5 NIST 800-88,NIST Guidelines for Media Sanitization Publication Rev. 1

5 ACRONYMS AND DEFINITIONS

5.1 Analysis Report – A detailed summary generated by the analyst of what was discovered and analyzed from the (b) (7)(E) of the digital evidence.
5.2 ATS – Administratively Transferred Sample
5.3 CD-R – Compact Disc-Recordable
5.4 COC– Chain of Custody
5.5 DFA – Digital Forensics Analyst
5.6 DFI – Digital Forensics Imager
5.7 DFT – Digital Forensics Team located at the (b) (7)(E)
5.8 Digital Forensics - Presents the digital (b) (7)(E) (b) (7)(E)
5.9 Flash Media – Data stored in NAND or NOR type memory Arrays (e.g., Solid State Hard Drives, USB Flash Drives)
5.10 GPS – Global Positioning System
5.11 (b) (7)(E)
5.12 (b) (7)(E)
5.13 LSS – Laboratories and Scientific Services
5.14 Magnetic Media – Any device that stores data using magnetic polarization to store data. (e.g., IDE Hard Disk, SCSI Hard Disk)
5.15 NIST – National Institute of Standards and Technology
5.16 Optical Media – Any CD/DVD recordable media (e.g., CDROM or DVD-R).
5.17 PDA – Personal Digital Assistant
5.18 PIN – Personal Identification Number
5.19 PMA – Portable Media Analyst: Individual qualified to (b) (7)(E) (b) (7)(E) (b) (7)(E)
5.20 PMI – Portable Media Imager: Individual qualified to (b) (7)(E) (b) (7)(E)
5.21 Portable Media – These devices can include but are not limited to: Cellular Phones, GPS Devices, PDA's, Tablets and Media/MP3 Players.
5.22 Portable Media Analysis – (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E)
5.23 Portable Media Imaging – A process where all storage areas of portable media are either (b) (7)(E) or by (b) (7)(E) to target media creating a forensic image.
5.24 Portable Media Triage – (b) (7)(E) of portable media for the presence of specific (b) (7)(E) or information.

5.25 PUK – Personal Unblocking Key
5.26 Raw Data - Unrefined data (b) (7)(E)
5.27 Raw Data Report – A report that is generated (b) (7)(E)
5.28 RIC – Radio Isolation Card
5.29 SIM – Subscriber Identity Module
5.30 USIM – Universal Subscriber Identity Module

6 QUALIFICATIONS

Digital forensics analysis shall not be completed by anyone other than qualified staff as outlined below:

6.1 Not Responsive

6.2 Portable Media Imager (PMI) Qualifications

6.2.1 LSS PMI minimum skills, knowledge and training requirements:

6.2.1.1 Successful completion of the appropriate DFA training program portable media modules.
6.2.1.2 It is recommended that a PMI be a DFI, however it is not mandatory.

7 SAMPLE INSPECTIONS, INVENTORY AND RECEIPT

7.1 Sample Inspection

7.1.1 At the discretion of the analyst evidence intake may be witnessed by a second person and documented on (b) (7)(E)
7.1.2 Open outside container to determine number of packages and the condition of the evidence packaging. Compare with information provided on submitted COC form(s).
7.1.3 Evidence bags, boxes, envelopes, etc., contained within exterior packaging shall be photographed.
7.1.4 Condition of seals, packaging and evidence shall be documented on (b) (7)(E) (b) (7)(E)

7.2 Inventory

7.2.1 Remove and carefully inspect all components.

7.2.2 Media discovered and identified for imaging shall be documented on (b) (7)(E) [redacted] The following information shall be documented for each item:

7.2.2.1 Make (e.g., Nokia)

7.2.2.2 Model (e.g., 6610)

7.2.2.3 (b) (7)(E) [redacted]

7.2.3 Each line item received as listed on COC shall be documented in detail on (b) (7)(E) [redacted]

7.2.4 If evidence inventory does not coincide with what is documented on the COC, submitter shall be notified to reconcile any discrepancies. This communication shall be:

7.2.4.1 Entered into the (b) (7)(E) [redacted] section of the (b) (7)(E) [redacted]

7.2.4.2 Recorded on the (b) (7)(E) [redacted]

7.3 Receipt of evidence

7.3.1 Mail Delivered

7.3.1.1 Upon satisfactory completion of inventory for the submitted evidence, the receiving analyst shall officially receive samples via his/her signature on the COC.

7.3.1.2 Delivery method and package tracking number shall be recorded at the top of (b) (7)(E) [redacted]

7.3.2 Hand Delivered/On-Site

7.3.2.1 Upon satisfactory completion of inventory for evidence that is retained, the receiving analyst shall officially receive samples via his/her signature on the COC.

7.3.2.2 Items not retained but examined on-site do not require the completion of a COC.

7.3.2.3 Delivery method and name of POC shall be recorded at the top of (b) (7)(E) [redacted]

7.3.3 A digital camera shall be used to take photographs of any unusual conditions regarding items of evidence submitted, such as damaged devices or broken evidence seals.

7.3.4 Photographs taken shall document the following for each device:

7.3.4.1 Make (e.g., Nokia)

7.3.4.2 Model (e.g., 6610)
7.3.4.3 (b) (7)(E)

7.3.5 Each photograph shall be documented on (b) (7)(E) For example:

EVIDENCE PHOTOGRAPHY LOG

PHOTOGRAPHER	CAMERA (MAKE/ MODEL)
Joe Photographer	Nikon CoolPix SD7600

COC #	LINE ITEM #	IMAGE #	DESCRIPTION
123456	1	1	1TB Western Digital Model T1000 (Front)
123456	1	2	1TB Western Digital Model T1000 (Back)

7.4 Sample Entry and Administration

7.4.1 Sample entry and administration shall be done in accordance with sections (b) (7)(E) of (b) (7)(E)

7.4.2 Upon issuance of a (b) (7)(E) the analyst shall label all evidence containers with the (b) (7)(E)

8 PORTABLE DIGITAL MEDIA PROCESS DESCRIPTION

8.1 Portable Media Triage

This section only addresses when (b) (7)(E) are performed (b) (7)(E)

8.1.1 The (b) (7)(E) may use approved portable media tools for the (b) (7)(E) of data provided the (b) (7)(E) has received the appropriate training. The (b) (7)(E) (b) (7)(E) may be provided to the submitter.

8.1.2 If the submitter requests additional information beyond what is provided from the (b) (7)(E) the device should be submitted to the (b) (7)(E) (b) (7)(E)

8.1.3 If (b) (7)(E) the device shall then be processed (b) (7)(E)

8.1.4 (b) (7)(E) of the portable media shall be (b) (7)(E) (b) (7)(E)

8.1.5 The originating lab may complete and publish a report after transferring the sample via (b) (7)(E) The narrative should include a final sentence stating: (b) (7)(E)

8.1.6 The results of the analysis by the (b) (7)(E) shall be sent directly to the submitter.

8.2 General Forensic Process

8.2.1 Not Responsive shall only be conducted by qualified and appropriately trained personnel that have successfully completed the Not Responsive

8.2.2 A tool may be used in the laboratory or on-site upon successful completion of the training requirements for that tool.

8.2.3 Not Responsive shall only be done on Not Responsive Not Responsive

8.2.4 Access to the (b) (7)(E) shall be (b) (7)(E)

8.2.5 At all times physical access to the evidence shall be restricted to authorized personnel only.

8.2.6 Examinations shall be conducted using approved laboratory hardware and software. Refer to (b) (7)(E)

8.2.7 For use of other tools refer to (b) (7)(E) (b) (7)(E) (b) (7)(E) may be used at the discretion of the analyst.

8.2.8 (b) (7)(E) shall be conducted on Cell phone and GPS forensic tools using (b) (7)(E) and shall be documented in the (b) (7)(E)

8.2.9 If Not Responsive is being conducted pursuant to a search warrant, then prior to commencing Not Responsive the Not Responsive should request a copy of the warrant (if not submitted) authorizing the search. Questions regarding the scope of the warrant's applicability shall be directed to the CBP Associate/Assistant Chief Counsel.

8.2.10 If evidence of a crime outside the scope of search authorized by the warrant is suspected, then the examiner shall immediately notify the submitter of the discovery and request guidance on how to proceed

8.2.11 (b) (7)(E) forms shall be reviewed and when necessary, the submitter shall be contacted to ascertain the scope of the investigation and its requirements.

8.2.12 (b) (7)(E) shall be completed for each (b) (7)(E) that includes any type of portable media as listed in Section 1.

8.3 Cell Phone/Smart Phone Handsets

8.3.1 (b) (7)(E) (b) (7)(E) prior to and during the entire portable media examination process.

8.3.2 Handsets shall be (b) (7)(E) (b) (7)(E)

8.3.3 Tools utilized shall be documented on (b) (7)(E)

8.3.4 If a (b) (7)(E) is unavailable or (b) (7)(E), then (b) (7)(E) may be used. The connection type used shall be documented (b) (7)(E)

8.3.5 When using multiple tools on a single device, Not Responsive Not Responsive

8.3.6 If requested information cannot be extracted from the handset and requires further analysis, the original evidence shall be (b) (7)(E) (b) (7)(E)

8.3.7 If data extraction is unsuccessful, the evidence may be (b) (7)(E) (b) (7)(E)

8.4 (U)SIM Cards

8.4.1 Tools utilized shall be documented on (b) (7)(E)
8.4.2 (b) (7)(E) (b) (7)(E)
8.4.3 (b) (7)(E) (b) (7)(E)
8.4.4 Attempts at (b) (7)(E) shall be documented on the Notes line of (b) (7)(E)
8.4.5 (b) (7)(E)

8.5 Media Cards within Portable Media

8.5.1 For (b) (7)(E) ortable media triage, (b) (7)(E) (b) (7)(E) However, it is recommended that these media cards be handled (b) (7)(E)
8.5.2 In the laboratory, (b) (7)(E) (b) (7)(E)

8.6 GPS Devices

8.6.1 (b) (7)(E) prior to and during the entire portable media examination process.
8.6.2 The make, model and (b) (7)(E) of the GPS shall be documented on (b) (7)(E) (b) (7)(E)
8.6.3 Any (b) (7)(E) on the GPS shall be documented (e.g., color and condition of the device) on (b) (7)(E)
8.6.4 Steps taken to acquire data from the device shall be documented on (b) (7)(E) (b) (7)(E)
8.6.5 (b) (7)(E) (b) (7)(E)
8.6.6 (b) (7)(E) must be performed for each device.
8.6.7 (b) (7)(E)

8.6.8 Data shall not be transferred to the GPS device. Any unintentional transfer shall be documented on (b) (7)(E)

9 (b) (7)(E)

When (b) (7)(E) shall send the created copies of the original evidence media for analysis. (b) (7)(E) (b) (7)(E)

9.1 Documentation Required for (b) (7)(E)

When (b) (7)(E) the following shall be included:

9.1.1 COC with enough detail to uniquely identify the items sent. (e.g., (1) Motorola V3r (b) (7)(E)

9.1.2 The device, removable media and/or SIM card along with any cables or accessories (if applicable).

9.1.3 Any (b) (7)(E) of the digital media that were captured.

9.1.4 Attach the following items in the (b) (7)(E)

9.1.4.1 Search warrant/consent to search (if submitted).

9.1.4.2 (b) (7)(E)

9.1.4.3 Request for (b) (7)(E)

9.1.4.4 Request for (b) (7)(E)

9.1.5 (b) (7)(E)

9.1.5.1 No documentation shall be placed in (b) (7)(E)

9.1.5.2 Evidence shall be packaged in (b) (7)(E) and labeled with the (b) (7)(E) and shall be (b) (7)(E) in a manner to preserve evidence during transit.

9.1.5.3 Items shall be placed in (b) (7)(E) labeled with (b) (7)(E) COC number, and description. (e.g., (b) (7)(E) COC#123456 (1) Motorola V3r (b) (7)(E)

9.1.5.3.1 Copies of (b) (7)(E) recorded to optical media shall be labeled with (b) (7)(E) date created and sequential numbers identifying order. (e.g., (b) (7)(E) 12/1/2009 1 of 12) and placed in plastic jewel cases.

9.1.5.4 (b) (7)(E) (b) (7)(E)

9.1.6 After (b) (7)(E) the (b) (7)(E) will:

9.1.6.1 Update the contact field of the (b) (7)(E) with the case agent's information.

9.1.6.2 Record the investigative case number (if available) in the ID field of the (b) (7)(E)

10 REPORTING OF EXAMINATIONS AND FINDINGS

Documentation to support conclusions shall be such that in the absence of the analyst, another competent analyst should be able to arrive at the same conclusion.

10.1 The following data points shall be included with each laboratory report as applicable to the examination (Triage or Analysis) conducted:

10.1.1 (b) (7)(E)
10.1.2 Agency name and case number
10.1.3 Date
10.1.4 Case Brief
10.1.5 Objective
10.1.6 Analysts Name
10.1.7 Examination Location
10.1.8 COC number, Line Item number and description
10.1.9 Tools Utilized
10.1.10 Summary of Findings

10.2 Refer to attachment (b) (7)(E) for guidance. See (b) (7)(E) (b) (7)(E)

10.3 Raw data reports shall not be attached in (b) (7)(E)

11 EVIDENCE RETENTION AND RETURN

11.1 Original evidence shall be returned to the submitter.

11.2 Raw data reports shall be (b) (7)(E) , (b) (7)(E) shall be stored in a secure manner and (b) (7)(E)

11.3 Analysis and Raw data reports mailed to the submitter shall use the following criteria:

11.3.1 (b) (7)(E)
11.3.2 (b) (7)(E)
11.3.3 (b) (7)(E)

11.4 If (b) (7)(E) to the submitter, a (b) (7)(E) shall be sent containing the (b) (7)(E) (b) (7)(E)

11.5 If (b) (7)(E) to the submitter, an (b) (7)(E) shall be sent to the submitter containing the (b) (7)(E)

11.6 Evidence containers shall include the following information:

11.6.1 Initials of the individual sealing the evidence
11.6.2 Date of sealing
11.6.3 (b) (7)(E)

11.7 No data shall be retained by the laboratory to include raw data reports.

11.8 Once the original evidence and published report have been confirmed as received by the submitter, (b) (7)(E)

12 RECORD KEEPING

12.1 Sample Laboratory Cards (b) (7)(E)

Evidence related to a single case should be kept in a single (b) (7)(E) Multiple (b) (7)(E) (b) (7)(E) may need to be created if more than one analyst is required to perform analysis on different evidence items in the case.

If additional items of evidence associated with a previously completed (b) (7)(E) are submitted to the laboratory, a (b) (7)(E) shall be generated.

12.2 (b) (7)(E) - The following data fields shall be completed as delineated:

12.2.1 (b) (7)(E)
12.2.2 (b) (7)(E)
12.2.3 (b) (7)(E)
12.2.4 (b) (7)(E)
(b) (7)(E)
12.2.5 (b) (7)(E)
12.2.6 (b) (7)(E)
12.2.7 (b) (7)(E)
12.2.8 (b) (7)(E)

12.3 Narrative

12.3.1 The narrative shall include (b) (7)(E) (b) (7)(E) sections, or similar language.

12.3.2 Language such as (b) (7)(E) shall be included along with a statement regarding the disposition of evidence.

Sample (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

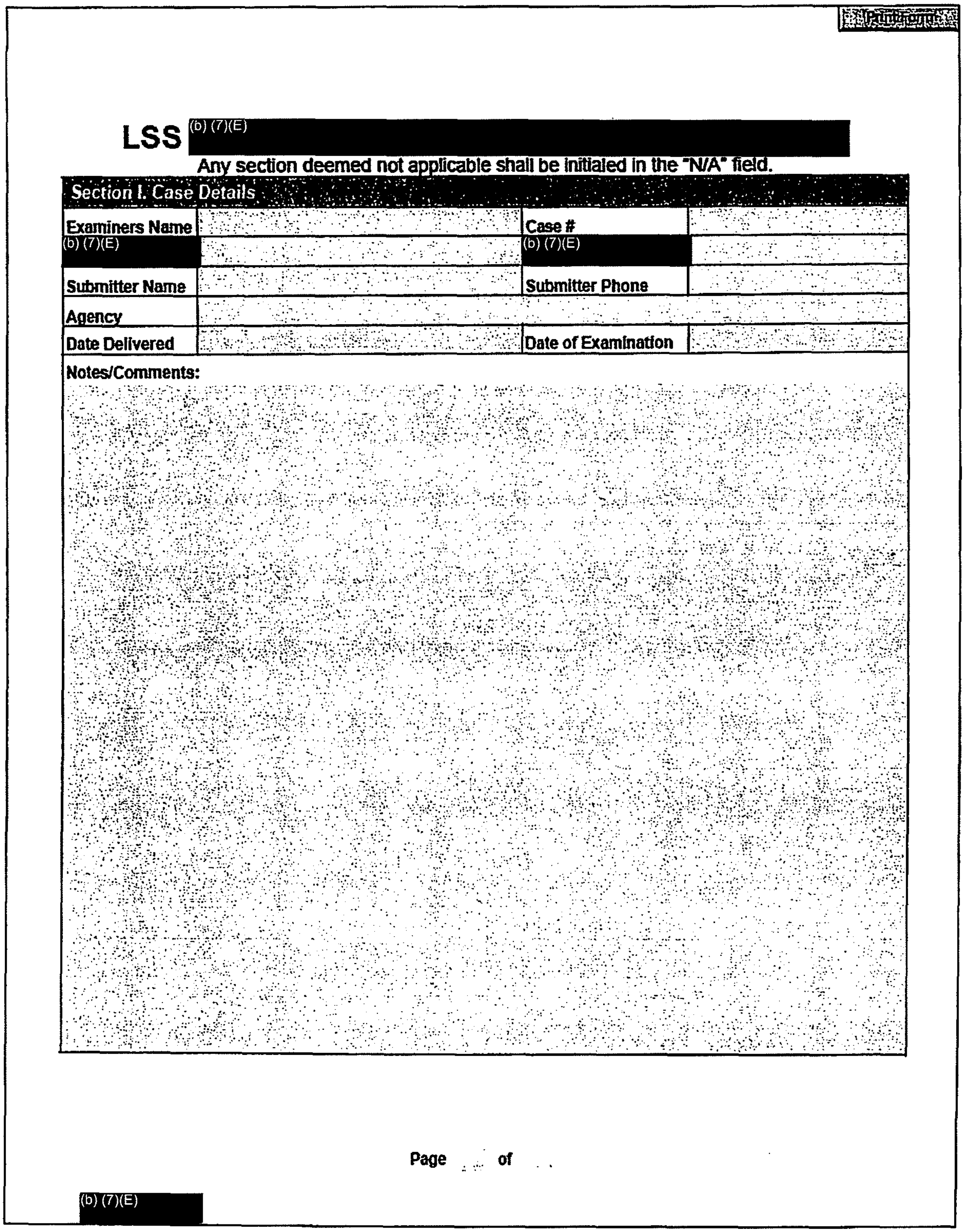
12.4 Attachments

When uploading attachments i(b) (7)(E)hey shall be (b) (7)(E)
The following shall be filed, if applicable, with the (b) (7)(E)

12.4.1 Analysis Report
12.4.2 Attachment 1: Signed COC, Custody Receipt Seize Property/Evidence Property;
12.4.3 Attachment 2: (b) (7)(E)
12.4.4 Attachment 3: (b) (7)(E)
12.4.5 Attachment 4: (b) (7)(E)
12.4.6 Attachment 5: Pictures of Evidence;
12.4.7 Attachment 6: (b) (7)(E) for each of the original evidence items.

13 FORMS

13.1 (b) (7)(E)



LSS (b) (7)(E) [redacted]

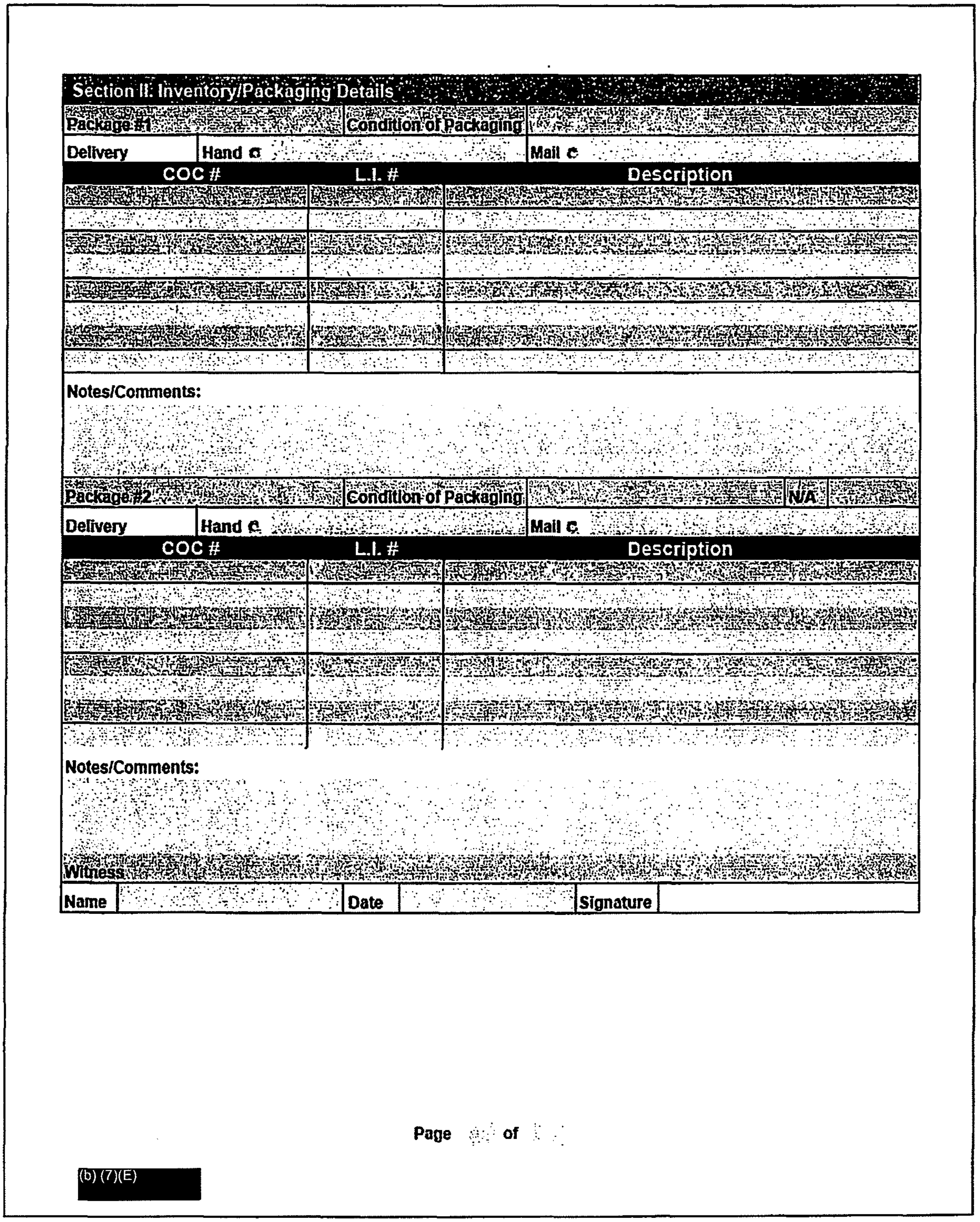
Any section deemed not applicable shall be initialed in the "N/A" field.

Section I. Case Details			
Examiners Name		Case #	
(b) (7)(E) [redacted]		(b) (7)(E) [redacted]	
Submitter Name		Submitter Phone	
Agency			
Date Delivered		Date of Examination	

Notes/Comments:

Page of

(b) (7)(E) [redacted]



Section II: Inventory/Packaging Details

Package #1		Condition of Packaging		
Delivery	Hand ○		Mail ○	

COC #	L.I. #	Description

Notes/Comments:

Package #2		Condition of Packaging		N/A
Delivery	Hand ○		Mail ○	

COC #	L.I. #	Description

Notes/Comments:

Witness

Name		Date		Signature	

Page of

(b) (7)(E)

Section III. Photography Log Details

EVIDENCE PHOTOGRAPHY LOG

PHOTOGRAPHER	CAMERA (MAKE/MODEL)

COC #	LINE ITEM #	IMAGE #	DESCRIPTION

Page _ of _

(b) (7)(E)

Initial here if entire page is not applicable ->

Section IV. (b) (7)(E) [redacted] Initial in N/A column if not applicable

Cell Phone # Details			
Make		**Model**	
(b) (7)(E) [redacted]		**Condition**	
SIM Card	Yes ○ No ○	(b) (7)(E) [redacted]	
Memory Card	Yes ○ No ○	**Start Date**	
Tool/Version		(b) (7)(E) [redacted]	
Tool/Version		(b) (7)(E) [redacted]	

Notes:

Cell Phone # Details			**N/A**
Make		**Model**	
(b) (7)(E) [redacted]		**Condition**	
SIM Card	Yes ○ No ○	(b) (7)(E) [redacted]	
Memory Card	Yes ○ No ○	**Start Date**	
Tool/Version		(b) (7)(E) [redacted]	
Tool/Version		(b) (7)(E) [redacted]	

Notes:

Initial here if entire page is not applicable ->

Section IV. (b) (7)(E) Initial in N/A column if not applicable

Cell Phone # _ Details

Make		**Model**	
(b) (7)(E)		**Condition**	
SIM Card	Yes ○ No ○	(b) (7)(E)	
Memory Card	Yes ○ No ○	**Start Date**	
Tool/Version		(b) (7)(E)	
Tool/Version		(b) (7)(E)	

Notes:

Cell Phone # _ Details N/A

Make		**Model**	
(b) (7)(E)		**Condition**	
SIM Card	Yes ○ No ○	(b) (7)(E)	
Memory Card	Yes ○ No ○	**Start Date**	
Tool/Version		(b) (7)(E)	
Tool/Version		(b) (7)(E)	

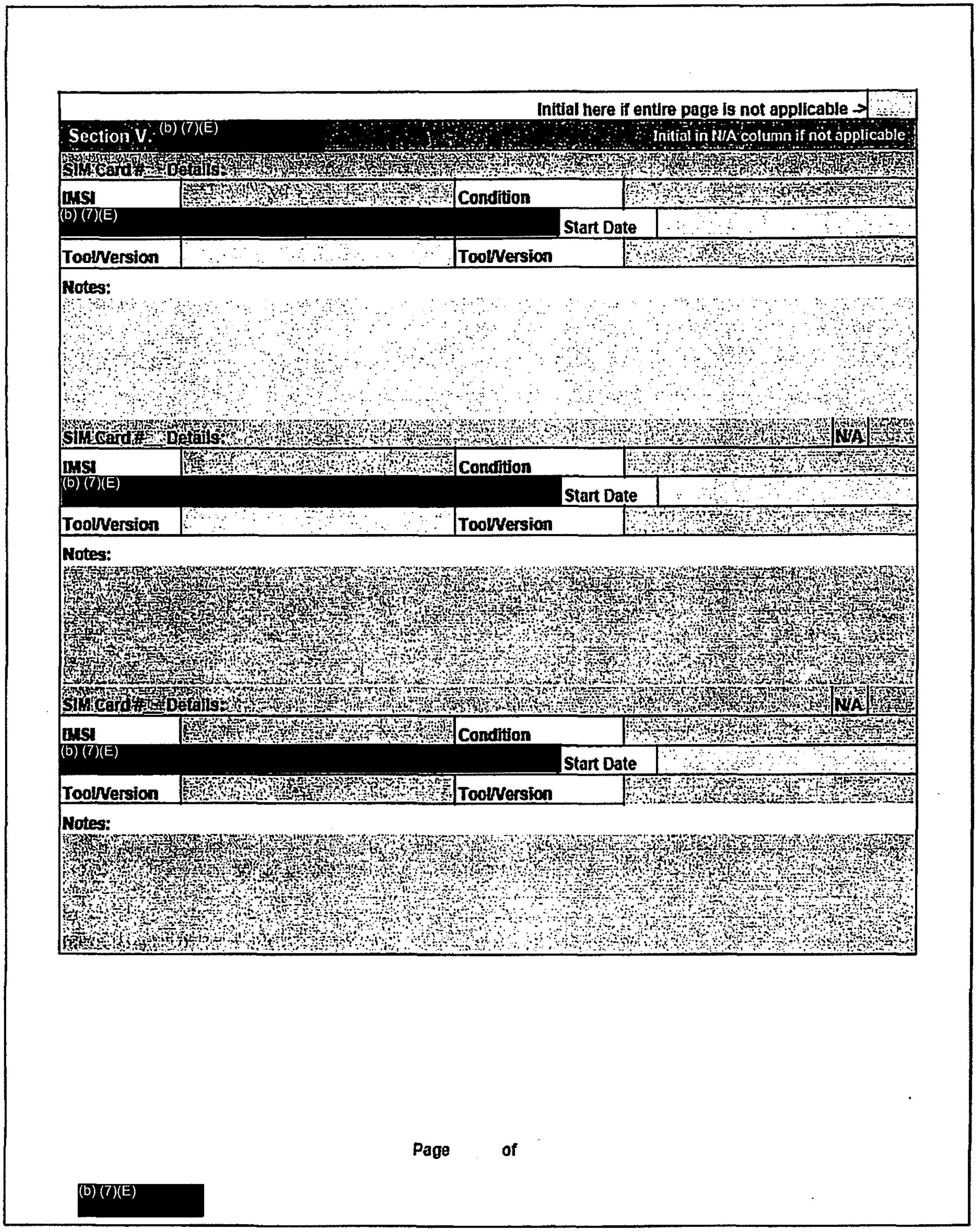
Notes:

Initial here if entire page is not applicable ->

Section V. (b) (7)(E)		Initial in N/A column if not applicable		
SIM Card #__ Details:				
IMSI		Condition		
(b) (7)(E)		Start Date		
Tool/Version		Tool/Version		
Notes:				
SIM Card #__ Details:			N/A	
IMSI		Condition		
(b) (7)(E)		Start Date		
Tool/Version		Tool/Version		
Notes:				
SIM Card #__ Details:			N/A	
IMSI		Condition		
(b) (7)(E)		Start Date		
Tool/Version		Tool/Version		
Notes:				

Page of

(b) (7)(E)



Initial here if entire page is not applicable →

Section V. (b) (7)(E) Initial in N/A column if not applicable

SIM Card # Details:

IMSI		**Condition**	
(b) (7)(E)		**Start Date**	
Tool/Version		**Tool/Version**	

Notes:

SIM Card # Details: **N/A**

IMSI		**Condition**	
(b) (7)(E)		**Start Date**	
Tool/Version		**Tool/Version**	

Notes:

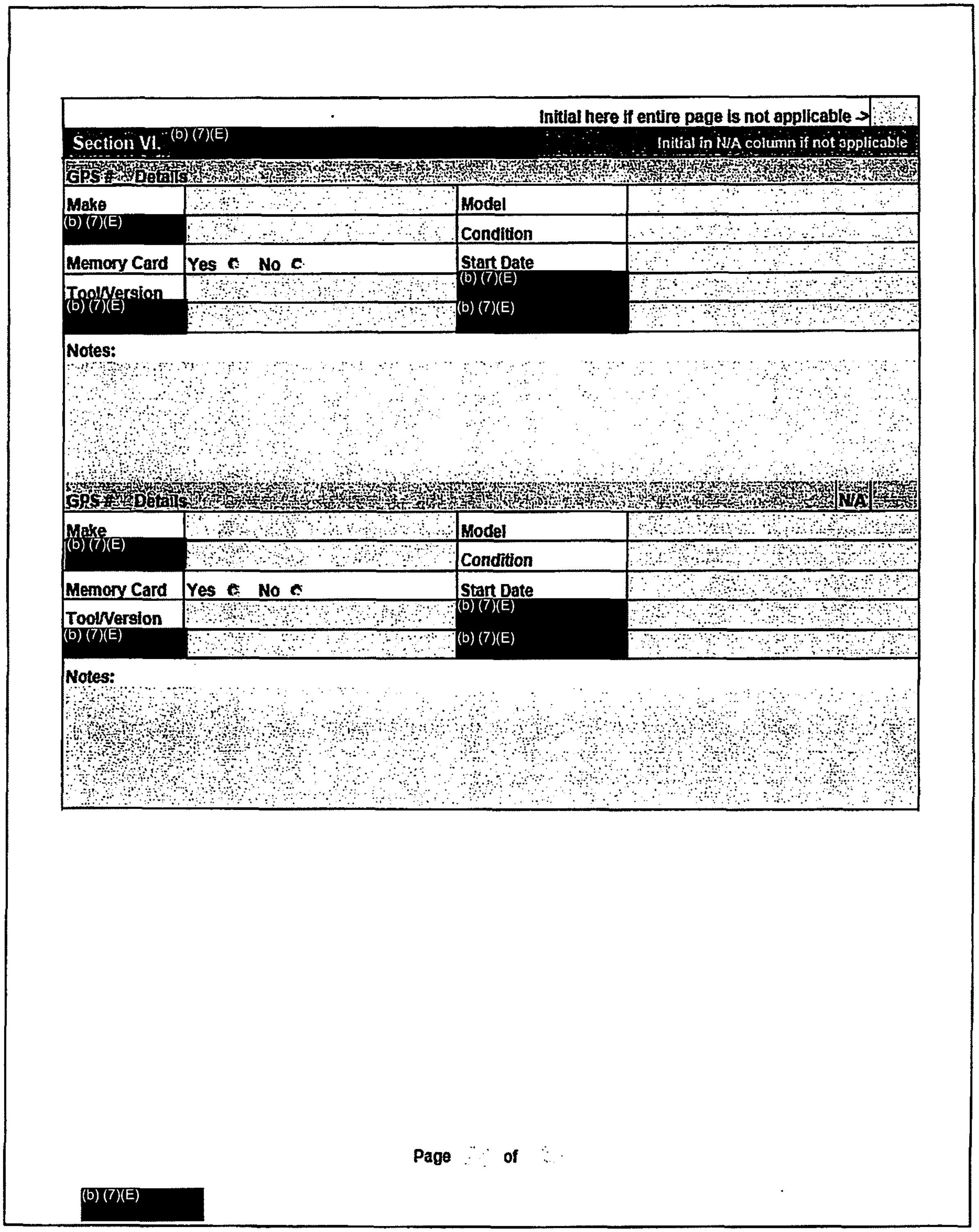
SIM Card # Details: **N/A**

IMSI		**Condition**	
(b) (7)(E)		**Start Date**	
Tool/Version		**Tool/Version**	

Notes:

Page of

(b) (7)(E)



Initial here if entire page is not applicable ->

Section VI. (b) (7)(E) Initial in N/A column if not applicable

GPS # Details

Make		**Model**	
(b) (7)(E)		**Condition**	
Memory Card	**Yes** ○ **No** ○	**Start Date**	
Tool/Version		(b) (7)(E)	
(b) (7)(E)		(b) (7)(E)	

Notes:

GPS # Details **N/A**

Make		**Model**	
(b) (7)(E)		**Condition**	
Memory Card	**Yes** ○ **No** ○	**Start Date**	
Tool/Version		(b) (7)(E)	
(b) (7)(E)		(b) (7)(E)	

Notes:

Page of

(b) (7)(E)

Initial here if entire page is not applicable ->

Section VI. (b) (7)(E) Initial in N/A column if not applicable

GPS # Details

Make		Model	
(b) (7)(E)		Condition	
Memory Card	Yes ○ No ○	Start Date	
Tool/Version		(b) (7)(E)	
(b) (7)(E)		(b) (7)(E)	

Notes:

GPS # Details N/A

Make		Model	
(b) (7)(E)		Condition	
Memory Card	Yes ○ No ○	Start Date	
Tool/Version		(b) (7)(E)	
(b) (7)(E)		(b) (7)(E)	

Notes:

Calendar Year 2005-July 23, 2011

Tool	# of usages	Frequency of Use for Each Tool	Frequency of Use per Evidence Item Analyzed
(b) (7)(E) [redacted]	75	14.73%	15.50%
[redacted]	1	0.20%	0.21%
[redacted]	1	0.20%	0.21%
[redacted]	3	0.59%	0.62%
[redacted]	285	55.99%	58.88%
[redacted]	34	6.68%	7.02%
[redacted]	28	5.50%	5.79%
[redacted]	36	7.07%	7.44%
[redacted]	21	4.13%	4.34%
[redacted]	17	3.34%	3.51%
[redacted]	2	0.39%	0.41%
[redacted]	2	0.39%	0.41%
[redacted]	4	0.79%	0.83%
Total:	**509**		

LIN: Labs(b)(6) (b)(7)(C) [redacted]72511

Items Tested: 484

LIN: Labs (b)(6) (b)(7)(C) 72511

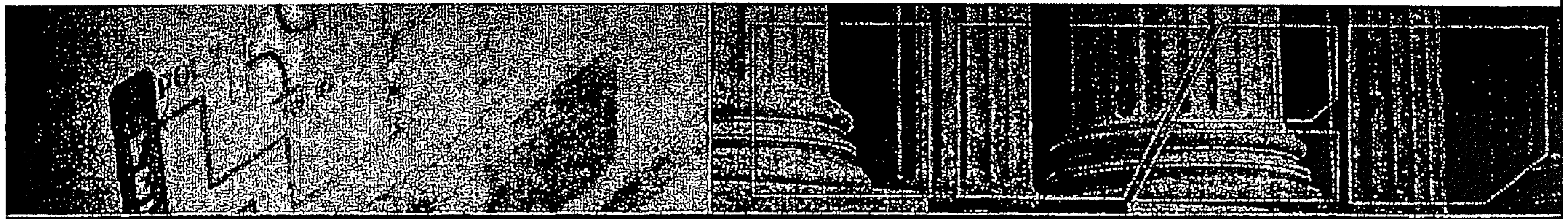
Calendar Year 2005-July 23, 2011

Cellebrite UFED
(Ruggedized Version)

(b)(6) (b)(7)(C) [redacted]

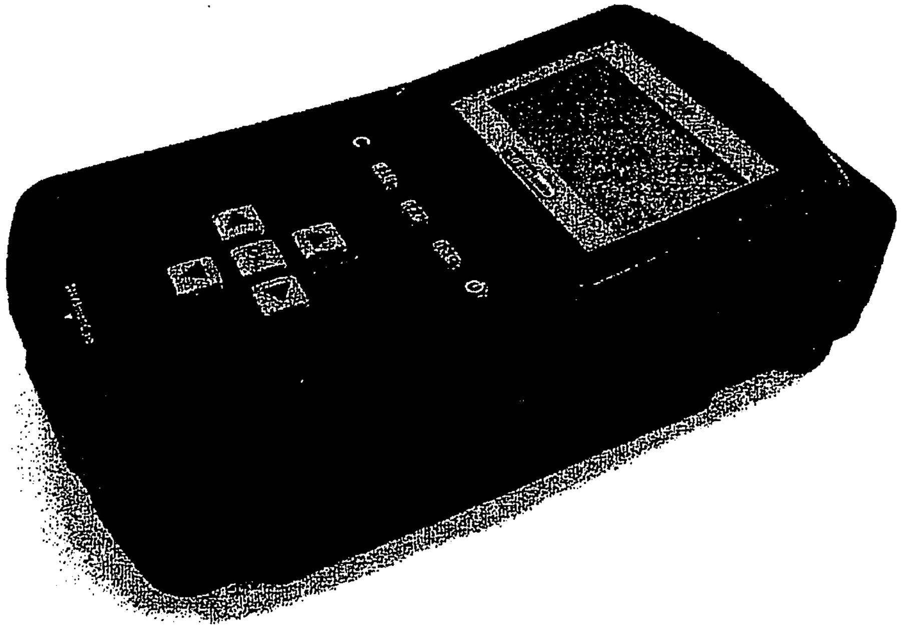
Digital Forensics Expert

Changing the Retrieved Folder

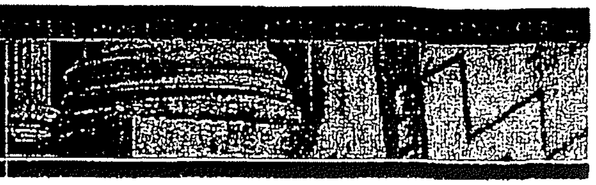


U.S. Customs and
Border Protection

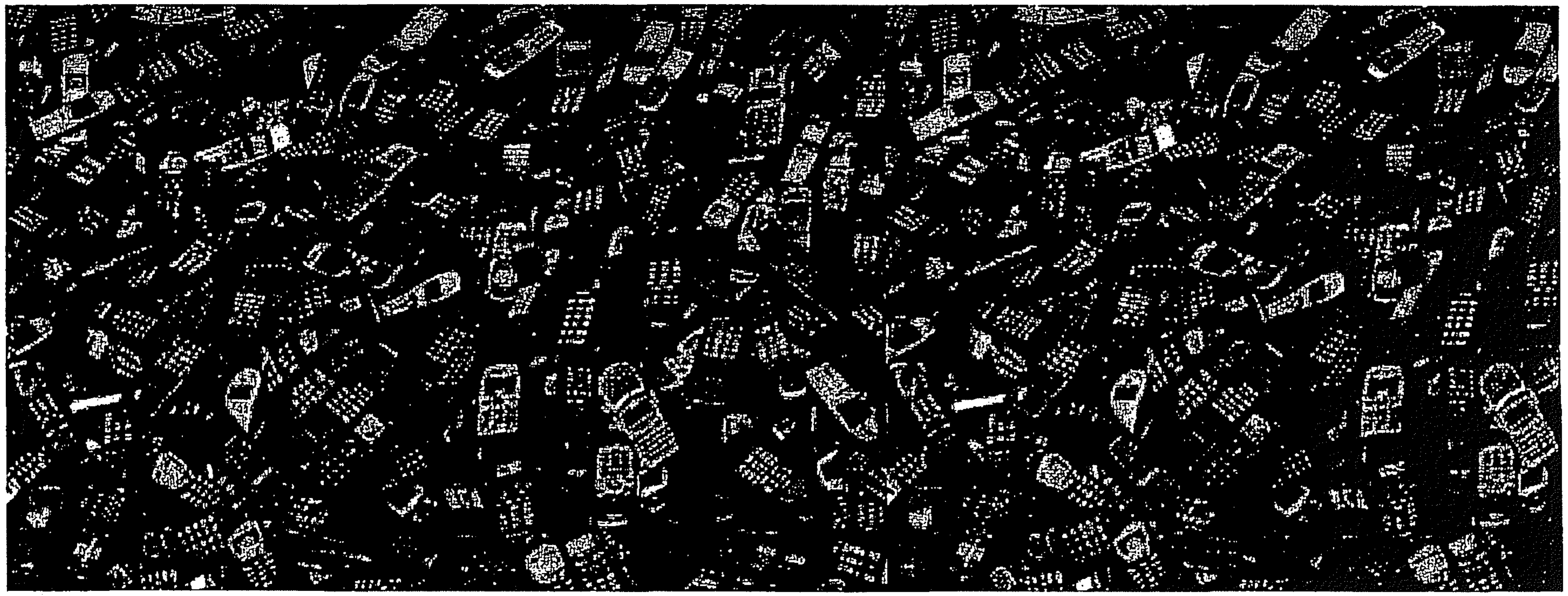
▶ Universal Forensic Extraction Device (UFED) Ruggedized

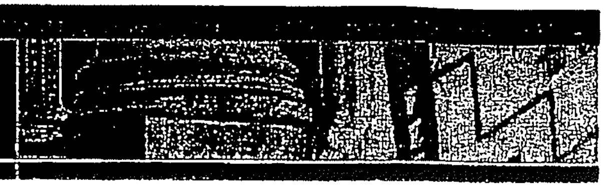


CelleBrite
Universal Forensic Products



- **Cell Phone Coverage -** Acquires data from over 2000 North American and European handset models.
- **Supported Phone List -** The full list of phones that are supported by the UFED system is regularly updated and available at: http://www.cellebrite.com/UFED-Supported-Phones.html





- **Field extraction of data -** Insures that a suspect's phone can be examined before the individual has a chance to destroy or erase data.
- **Work exclusively with most major carriers worldwide –**
  - **Verizon Wireless**
  - **AT&T**
  - **Sprint/ Nextel**
  - **T-Mobile**
  - **Orange France**
  - **Telstra Australia**
  - **50 other carriers in the US**

verizonwireless

at&t

T··Mobile·

Sprint

TRACFONE

Sprint

metroPCS

US Cellular

boostmobile

Virgin mobile

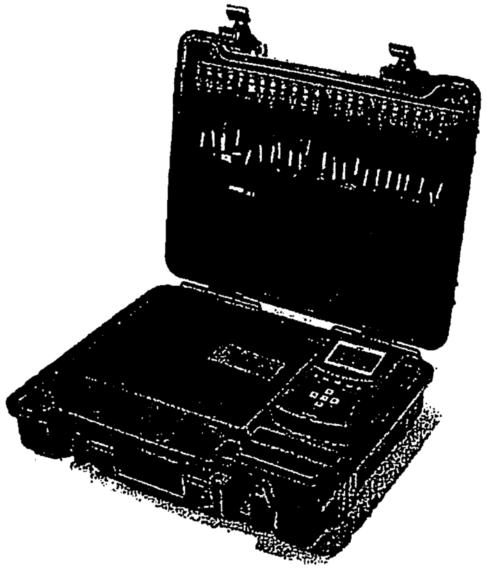
cricket

alltel

SouthernLINC Wireless

- **Support of new phones -** Cellebrite ensures that future devices are supported prior to their being distributed in the market.
- **Supported smart phones include:**
  - Symbian
  - Palm
  - RIM
  - Windows Mobile
  - Apple
  - Android

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



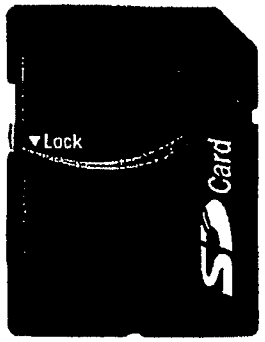
- **Different Data Transfer Means:** Cellebrite acquires cell phone data via USB, Bluetooth, IrDA, SD Card, and SIM card reader.

USB

UNIVERSAL SERIAL BUS

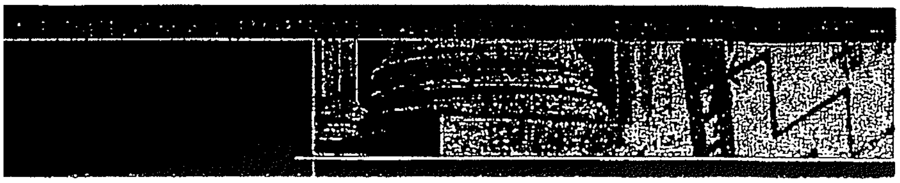
Bluetooth™

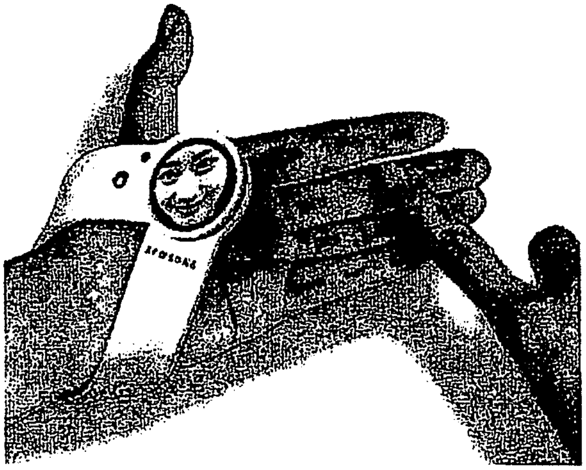
Infrared

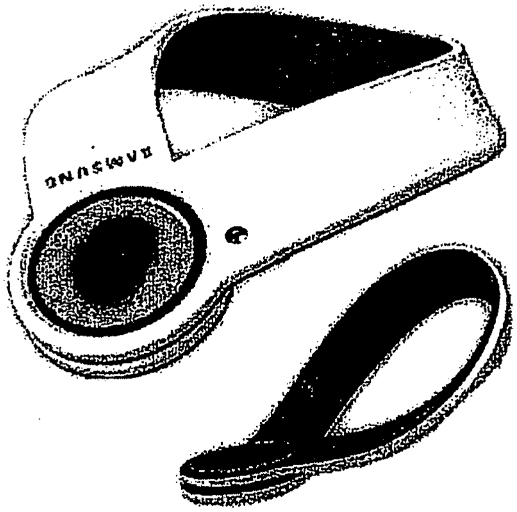


- **Standalone device that can be used in the field and in the forensic lab.**
- **No computer required for extraction.**
- **Generation of complete, MD5 verified evidence reports.**
- **UFED extracts vital data such as:**
  - Phonebook
  - Camera pictures
  - Videos
  - Audio
  - Text messages (SMS)
  - Call logs
  - ESN
  - IMEI
  - ICCID
  - IMSI
Phonebook

- CDMA - No SIM card
- GSM – SIM Card
- IDEN/TDMA – SIM Card

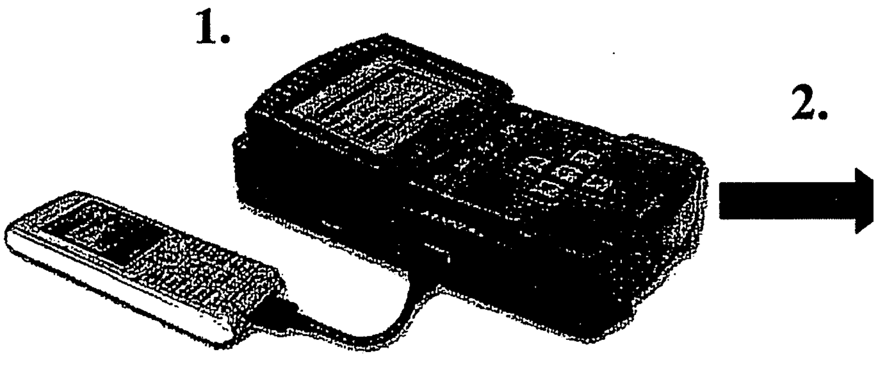



SAMSUNG


SAMSUNG

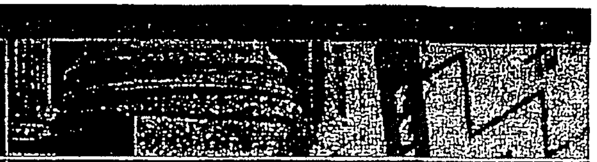
[redacted]

1. Connect Phone/SIM Card
2. Transfer data to (b) (7)(E) [redacted]
3. (b) (7)(E) [redacted]
4. (b) (7)([redacted]

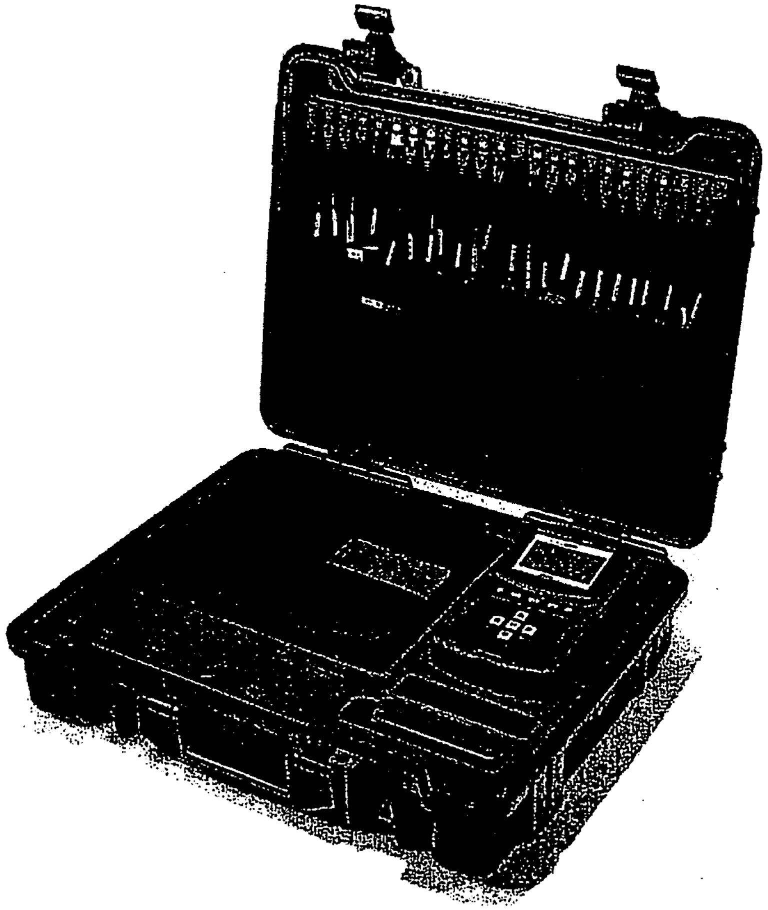


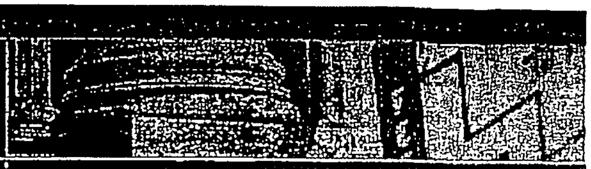
(b) (7)(E)

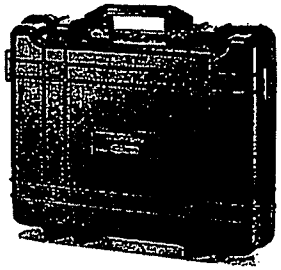
[redacted]

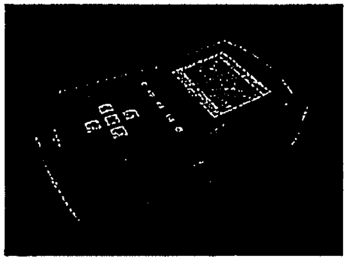


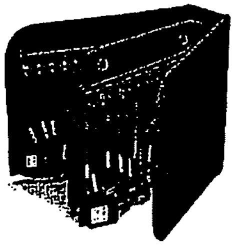
1. Hard-side plastic casing with secure latches
2. UFED Device with Rubber casing
3. Cable Organizer
4. Full Set of Data Cables
5. Small Cable Pouch
6. Bluetooth Dongle
7. USB Flash Drive
8. AC Power Supply
9. UFED Battery Pack
10. 12V In-vehicle (Cigarette Lighter) Power adapter
11. SIM ID Cloning Cards
12. Card Reader
13. Mobile Phone Battery Charger set
14. Faraday Bag
15. UFED Manager- Report Viewing and Printing Software
16. Phone Connection Cleansing Brush
17. User Manual and Support CD

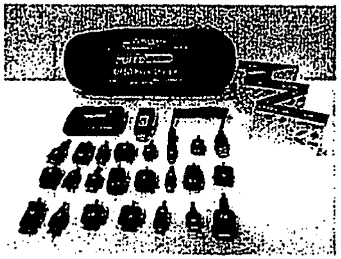


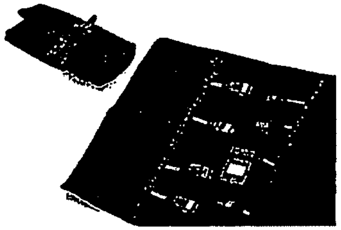


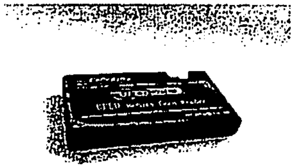


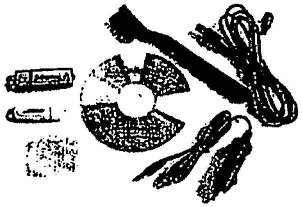


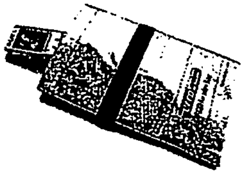


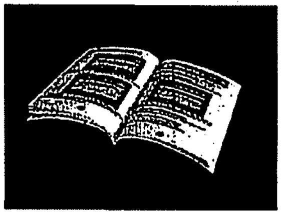


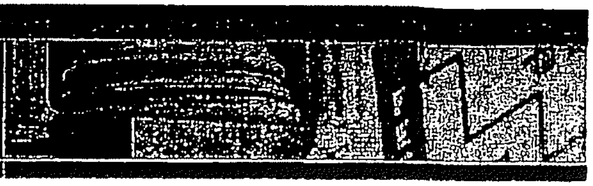


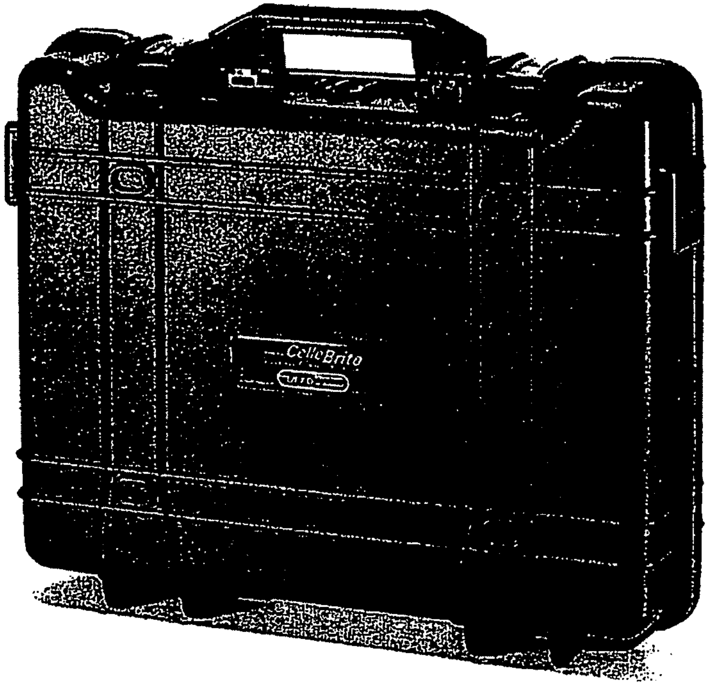




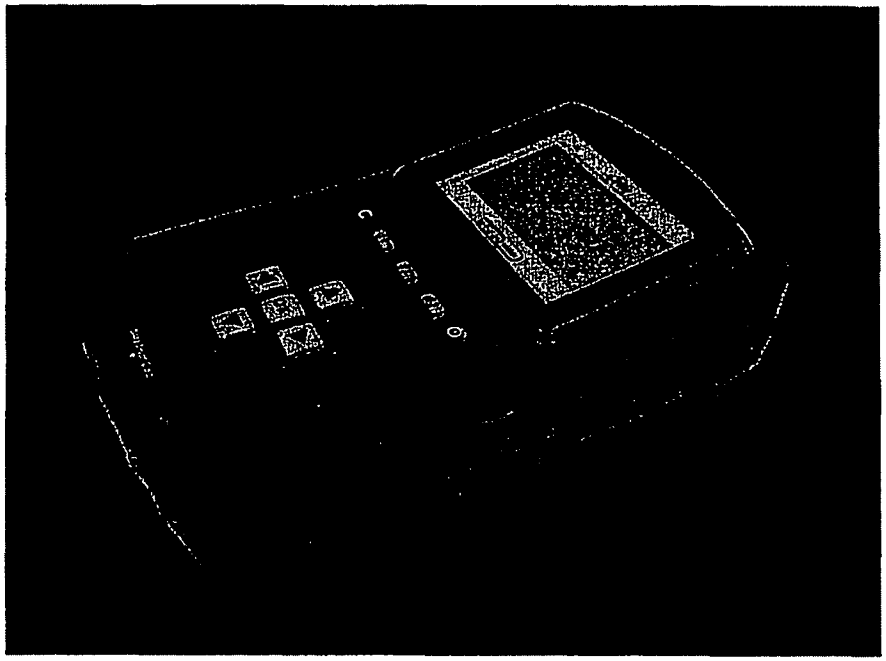




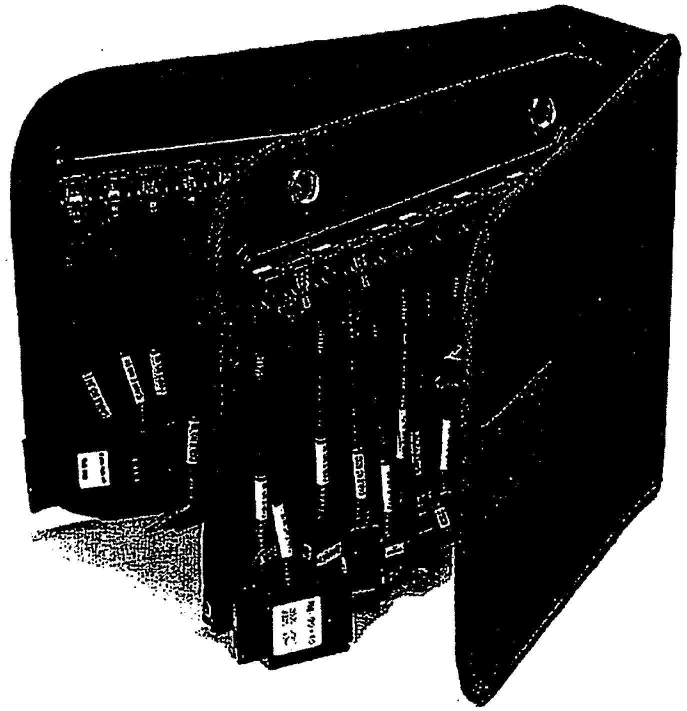




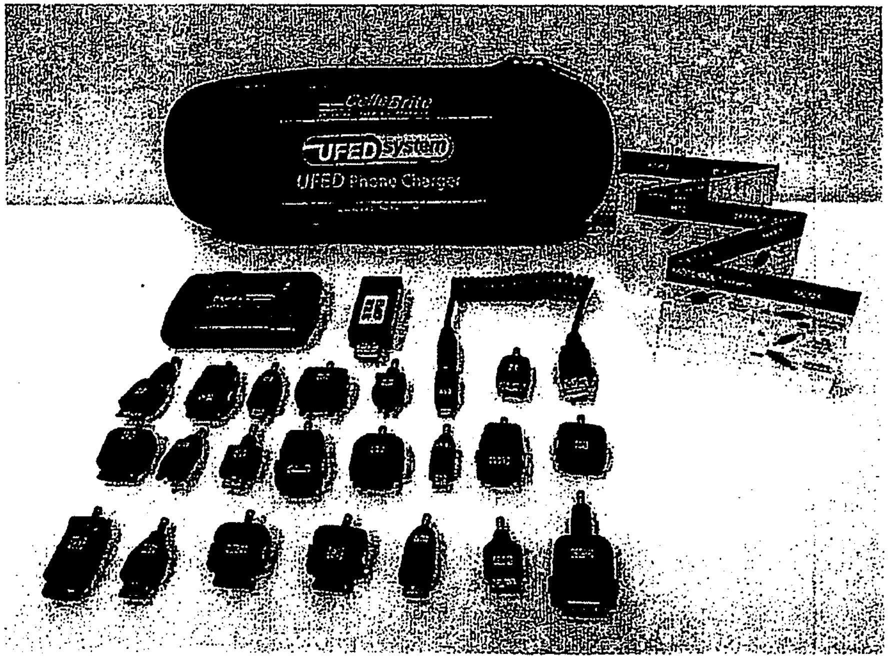
Unit Case



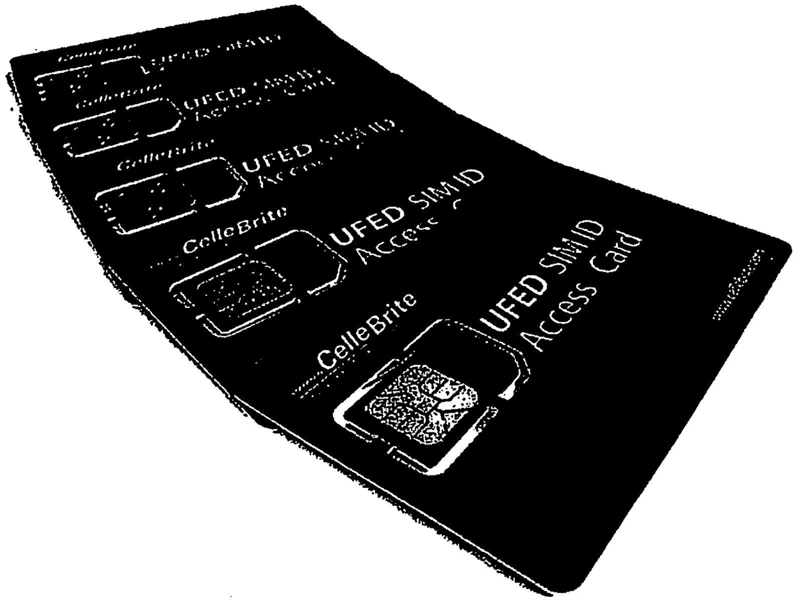
UFED Device



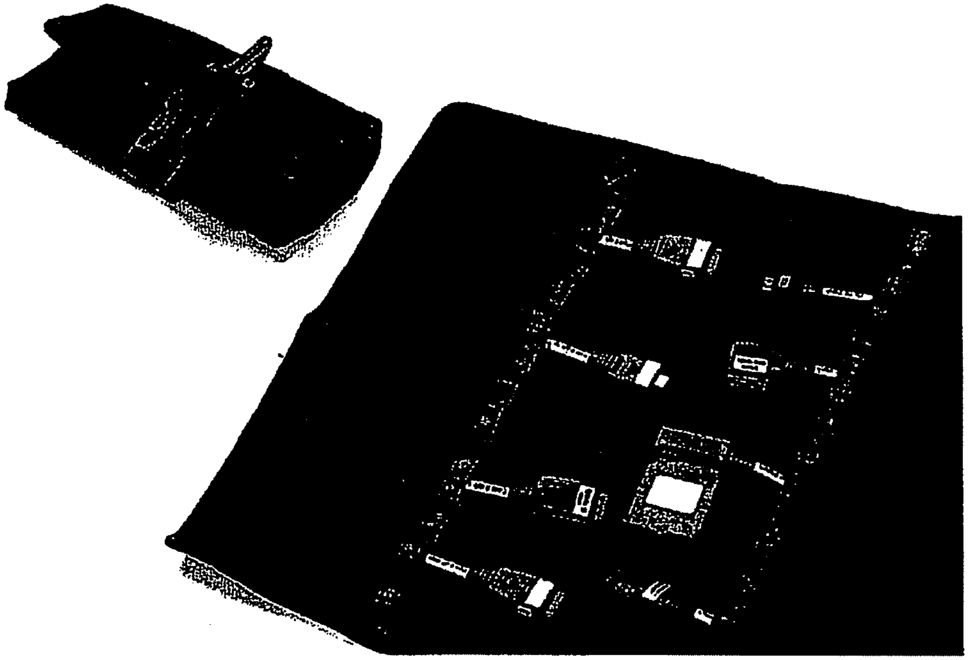
Cable Organizer (75+ Cables)



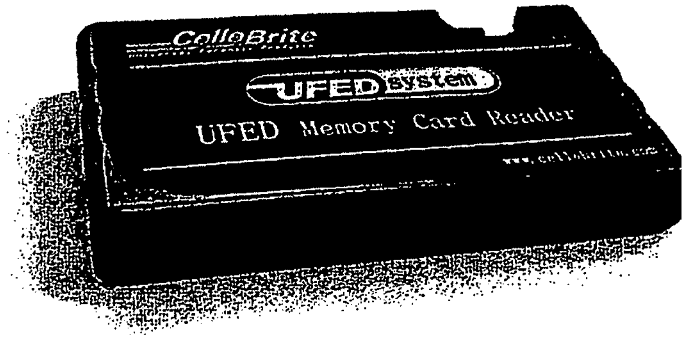
Phone Charger Set



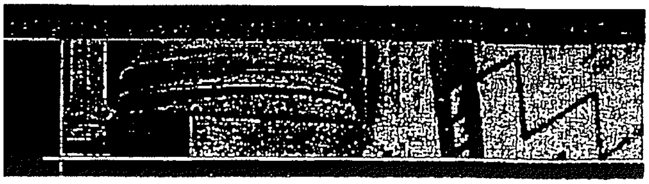
SIM ID access Card

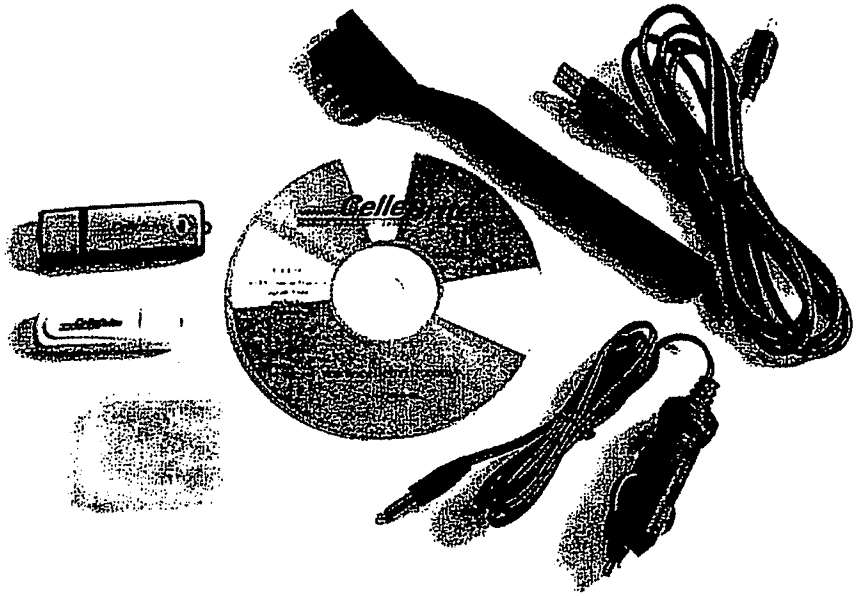


Cable Carrying Pouch

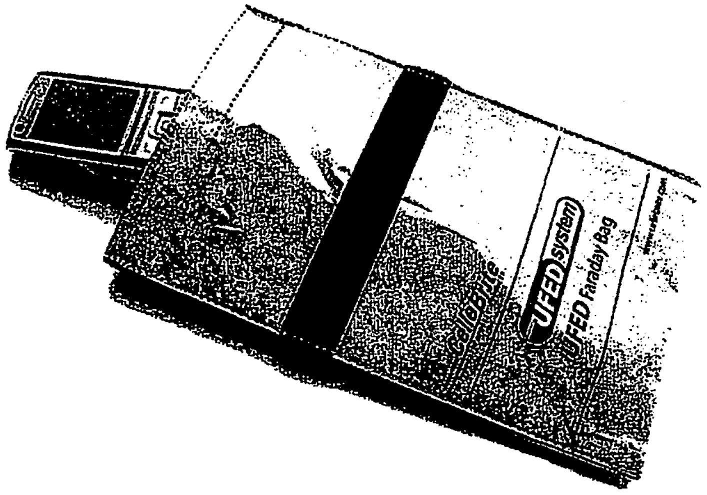

CelloBrite
UFED System
UFED Memory Card Reader
www.cellebrite.com

Card Reader

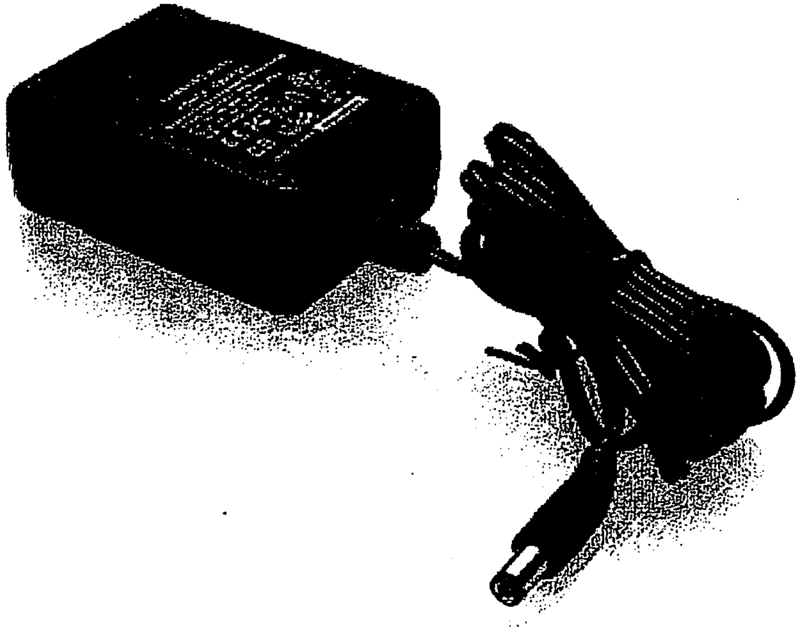




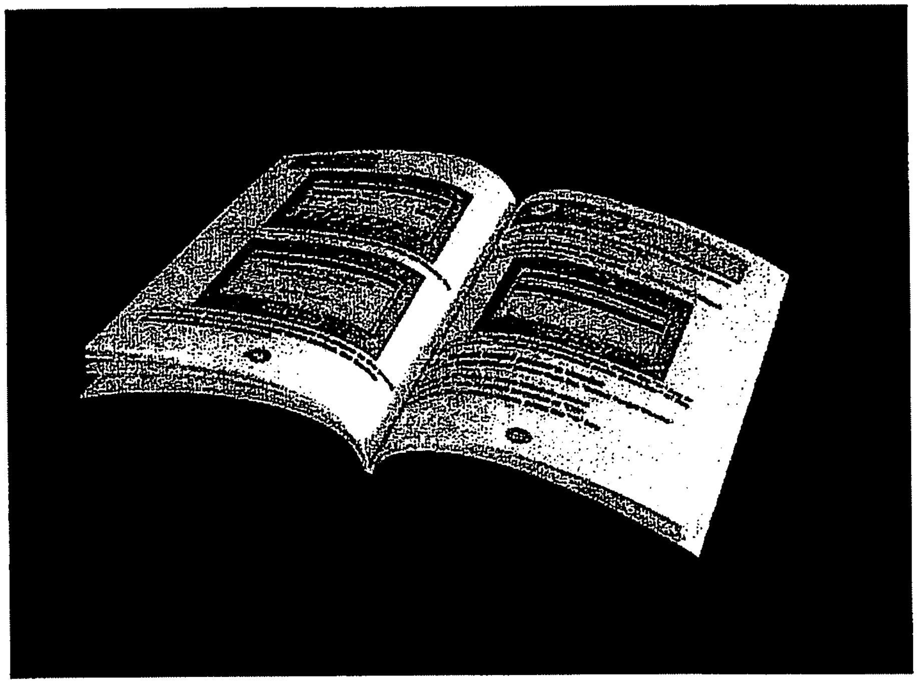
Accessories



Faraday Pouch



Power Cable



User Manual

[redacted]

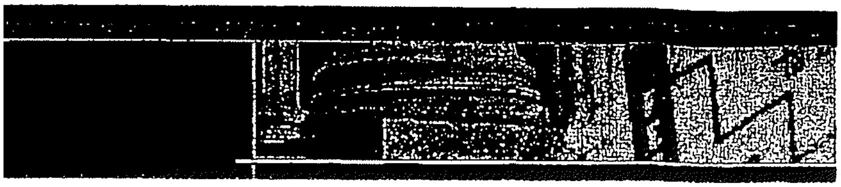
1. **Cancel Button**
2. **Source-side Connectors**

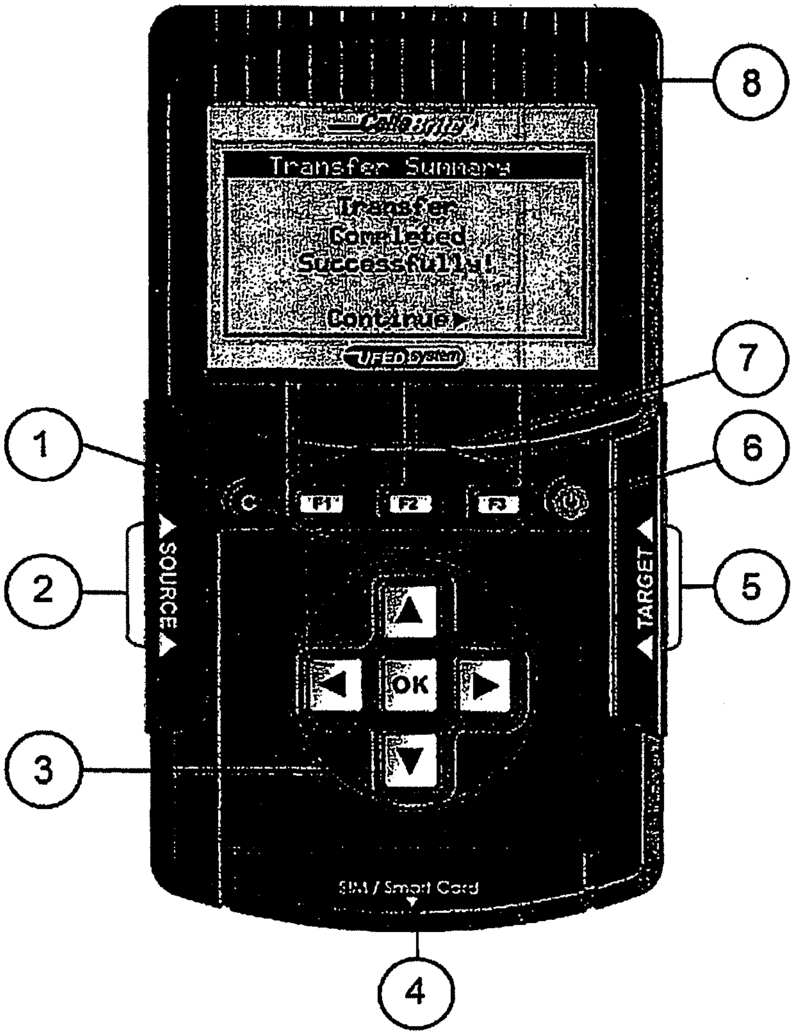
   (b) (7)(E) [redacted]
3. **Navigation Keys**

   (For navigating the UFED menu)
4. **SIM Card Slot**
5. **Target-side Connectors**

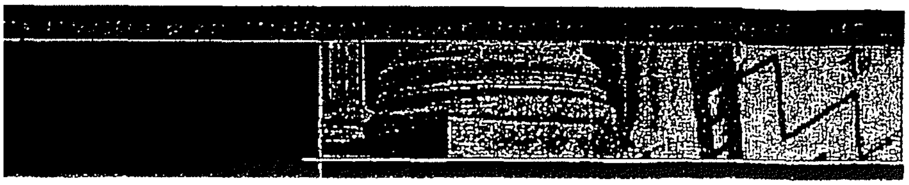
   (For extraction to USB disk drive)
6. **Power Button**
7. **Function Keys**

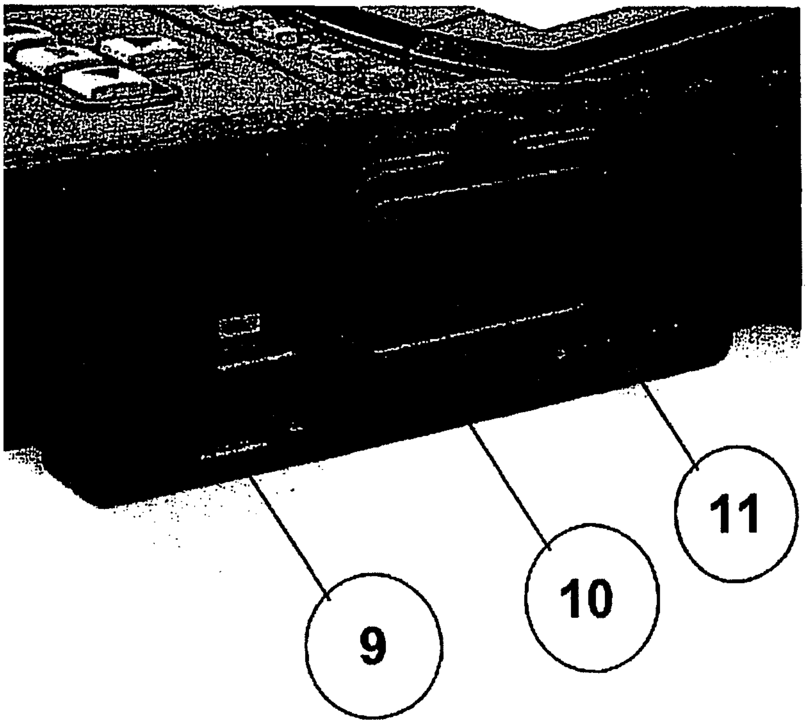
   (F1 for help. F2 for select/deselect all)
8. **Power Connector**

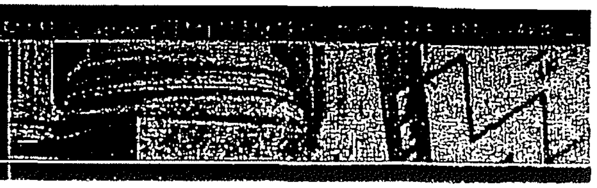



Cellebrite
Transfer Summary
Transfer
Completed
Successfully!
Continue▶
UFED system
C
F1
F2
F3
▲SOURCE▲
▲TARGET▲
OK
SIM / Smart Card
1
2
3
4
5
6
7
8

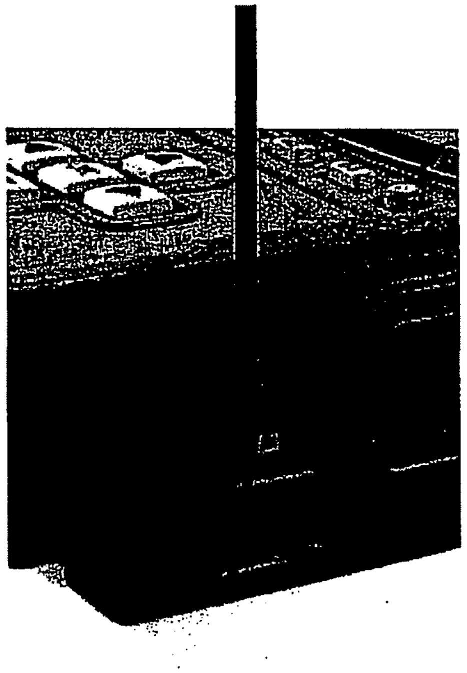
9. Charging switch.
10. Battery kit and battery housing protective covering
11. Battery's state-of-charge LED indicators.



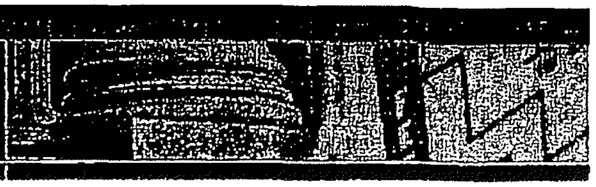

9
10
11



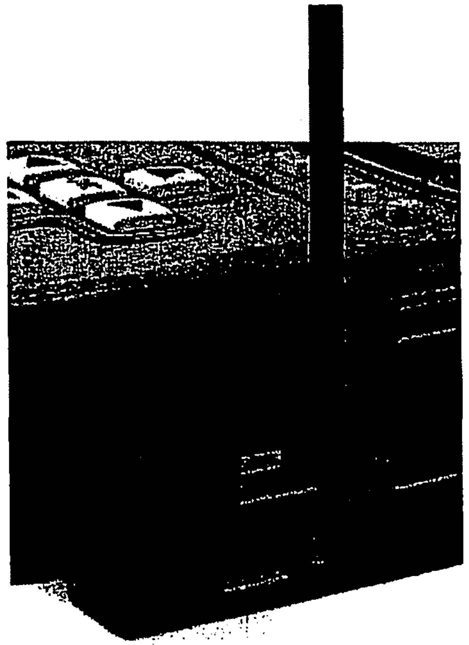
- The UFED device can be powered by:
  1. **AC power supply**
  2. **Car power supply**
  3. **Battery power**



- **Battery Power**
  - To run the UFED on battery power, flip the power switch to the right ("BAT") position. Battery power will take over.
- **Charging the Battery**
  - To re-charge the battery, connect the device to an AC adapter (supplied with the kit), and then flip the power switch to the left ("CHG") position.

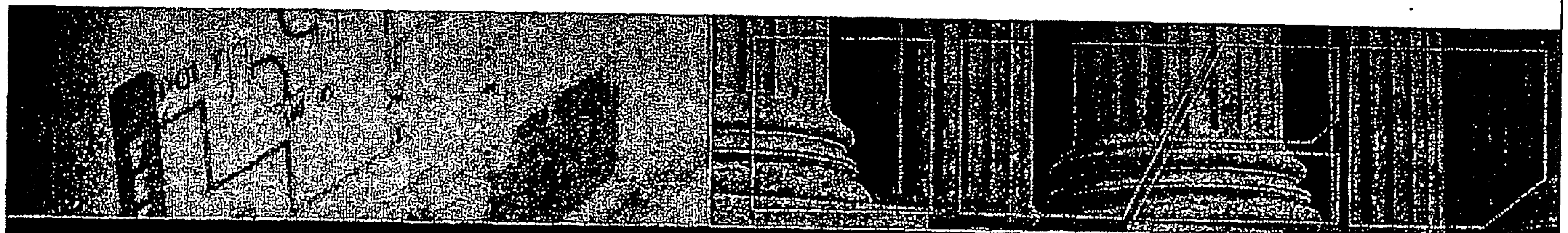


LED Status		Indication
Red	●	Battery charge in process
Green	◍	Battery fully charged
No light	○	Sleep mode (no input power source) OR No battery connected OR Charge suspended (timer fault or thermal shutdown) OR Over-voltage fault
Flashing Red	◐	Indicates a problem with the battery. Verify that the battery is connected properly



Cellebrite UFED

Getting Started



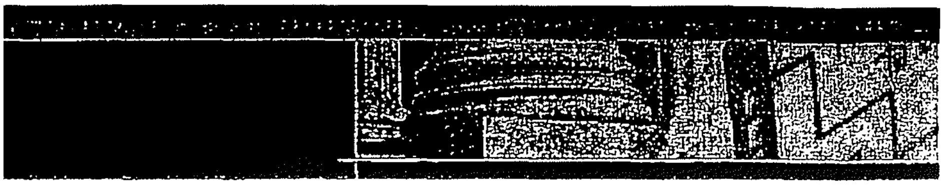
U.S. Customs and
Border Protection

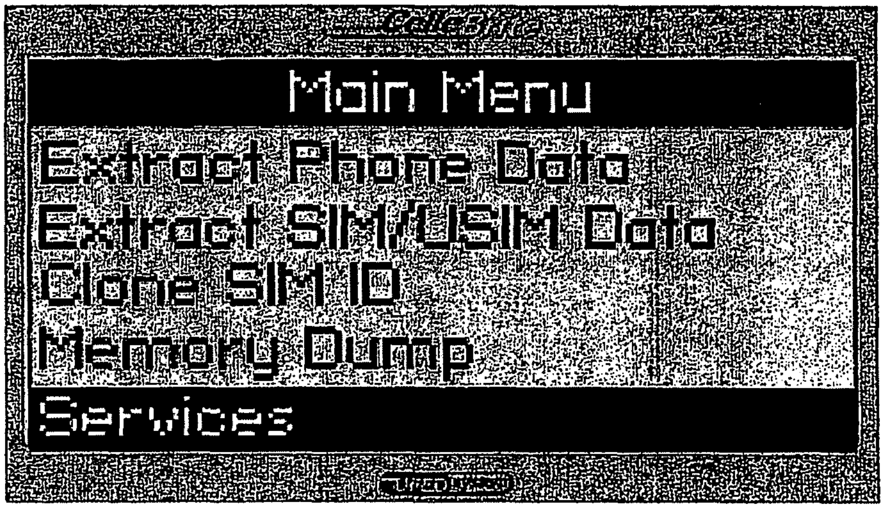
[redacted]

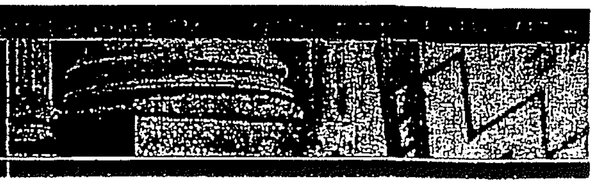
- ▶ Connect the power supply adapter to the UFED. “Please Wait” appears briefly on the screen.

- ▶ Version numbers will appear.

- ▶ The UFED is ready to be used, when the following Main Menu is displayed:



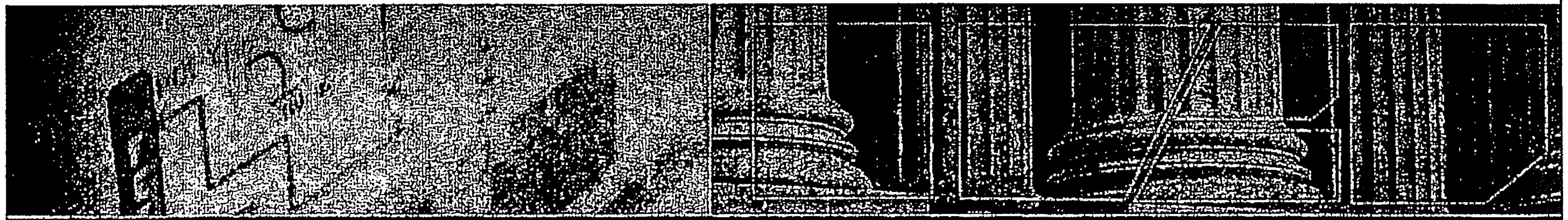

Cellebrite
Main Menu
Extract Phone Data
Extract SIM/USIM Data
Clone SIM ID
Memory Dump
Services



- **The UFED shows menu options on the display.**
- **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

Cellebrite UFED

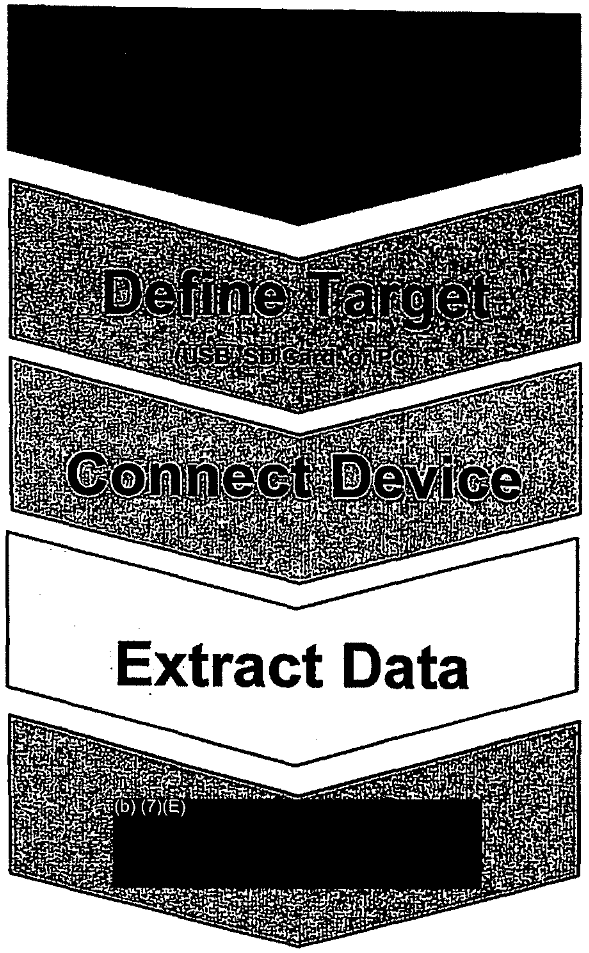
Extracting Phone Data



U.S. Customs and
Border Protection

[redacted]

- When working with the UFED, the process flows as described in the following flowchart.
- The process is the same for SIM cards as it is for phones.



[redacted]

Define Target

(USB, SD Card, or PC)

Connect Device

Extract Data

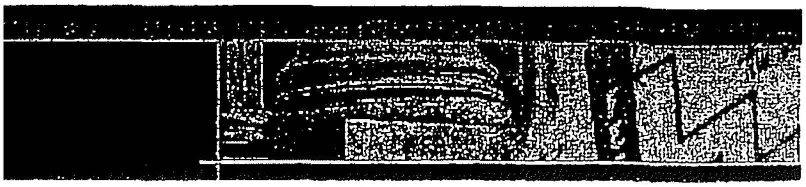
(b) (7)(E)

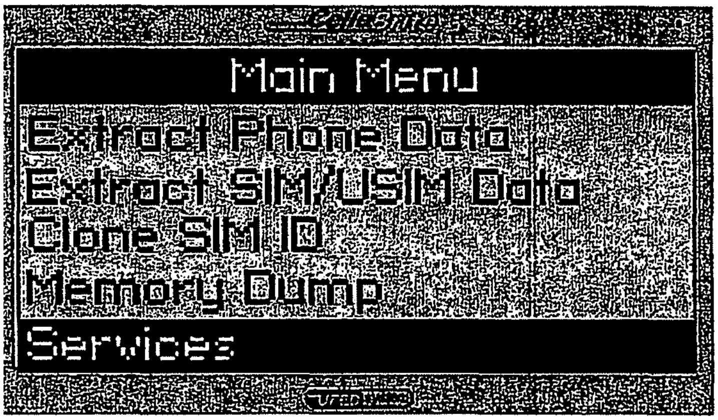
[redacted]

- Select **Extract Phone Data** from the **Main Menu** in order to copy data from a phone (the source) (b) (7)(E) (b) (7)(E) (the target).

- This function can extract:
  - Phonebook
  - SMS text messages
  - Pictures, etc.
  - From mobile phone memory (b) (7)(E) (b) (7)(E)

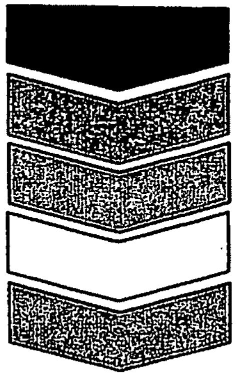
- The UFED guides you each step of the way during this process.



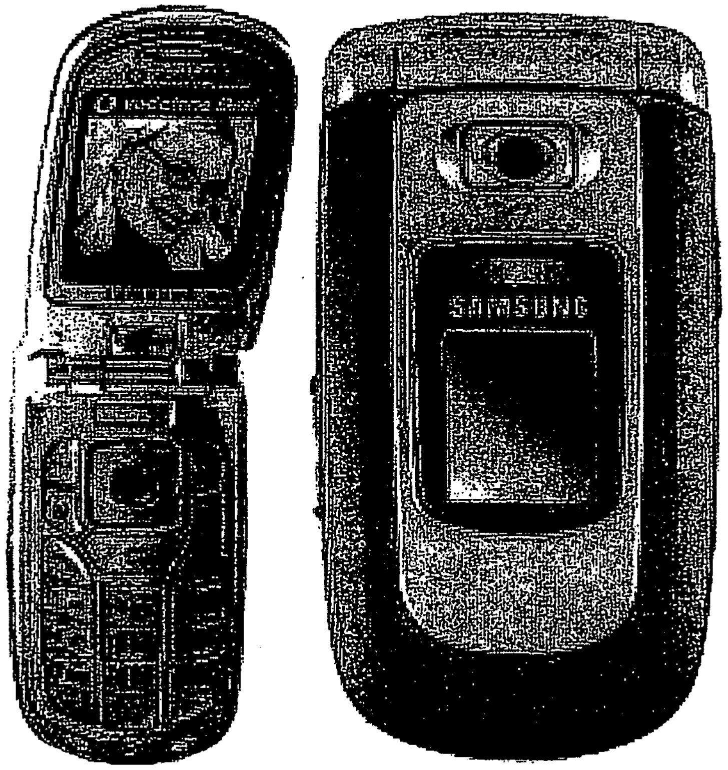

CelleBrite
Main Menu
Extract Phone Data
Extract SIM/USIM Data
Clone SIM ID
Memory Dump
Services

- **The overall flow when performing a phone data extraction is as follows:**

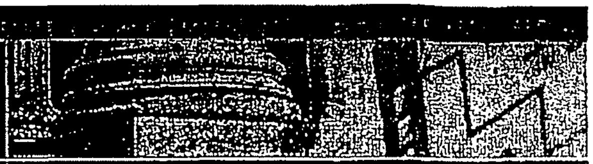
  1. **Define the source phone:**
     - Phone vendor
     - Phone model
     - Place you will copy **from** (Cell Phone or SIM card)
     - Method of connectivity with the phone
       - (b) (7)(E) [redacted]
     - Content you wish to extract from the phone (Call log, phonebook, images etc.)
  2. **Define the target for the data extraction**: USB drive - (b) (7)(E) [redacted]
  3. (b) (7)(E) [redacted]
  4. **Extract data.**
  5. (b) (7)(E) [redacted]

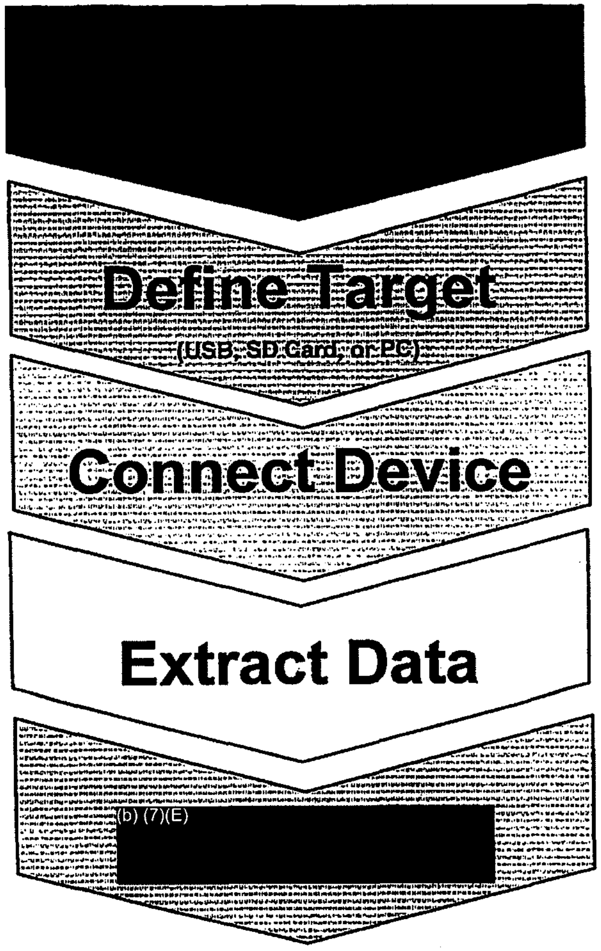


▶ Samsung Model: ZV-30



[redacted]





[redacted]

Define Target

(USB, SD Card, or PC)

Connect Device

Extract Data

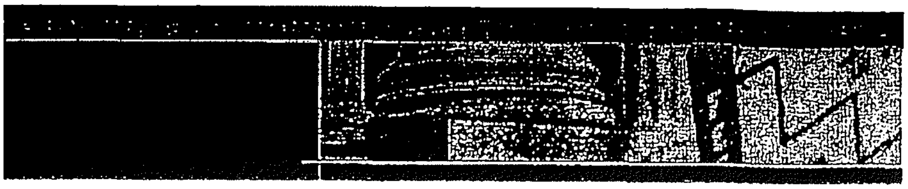
(b) (7)(E)

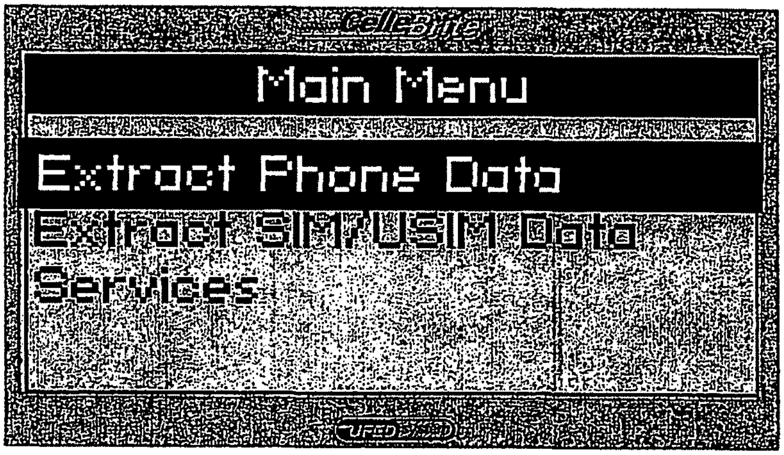
[redacted]

1. Define Your Source:

A. Main Menu

- ➢ Select Extract Phone Data from the main menu.
- ➢ Use the ▲▼ keys to move between options. Press OK or ► to continue.

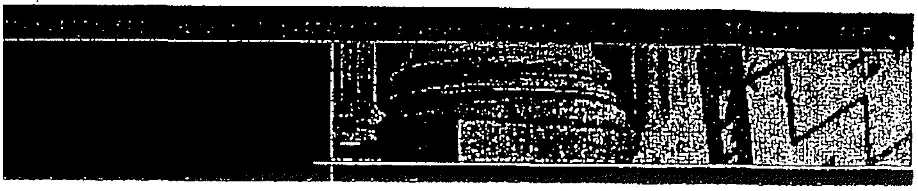


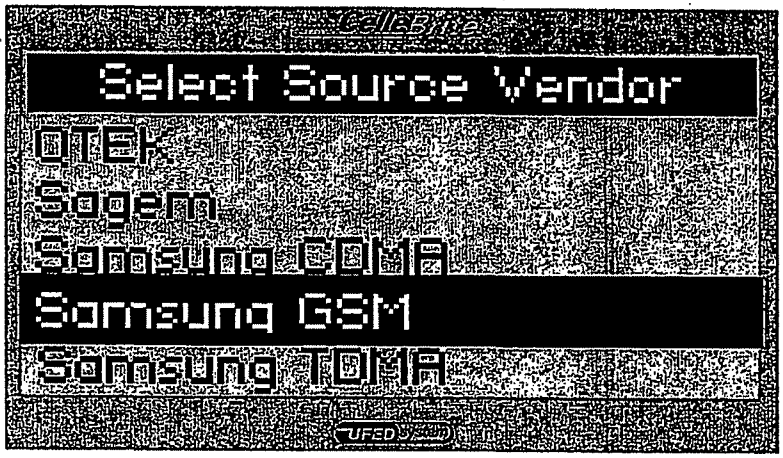


Cellebrite
Main Menu
Extract Phone Data
Extract SIM/USIM Data
Services
UFED

B. Select Source Vendor

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





Select Source Vendor

QTEK

Sagem

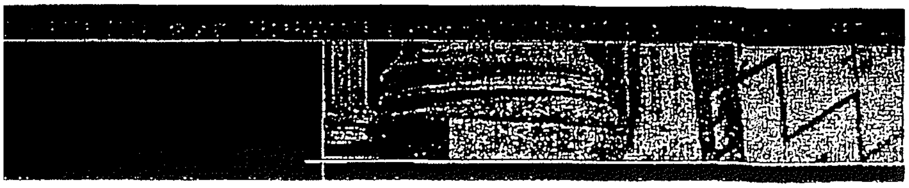
Samsung CDMA

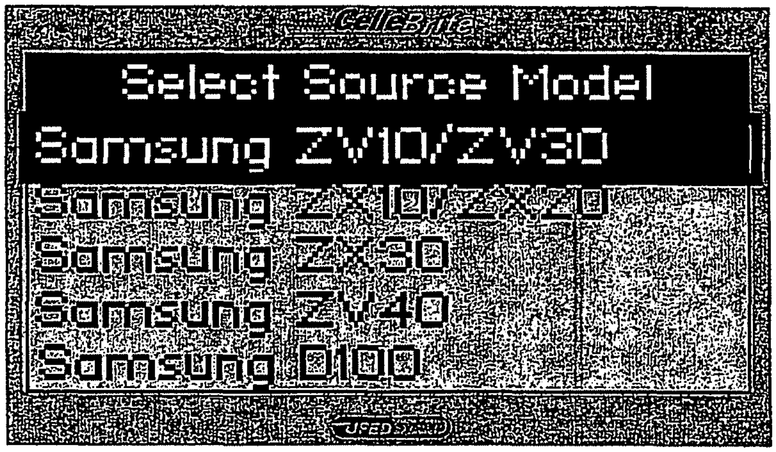
Samsung GSM

Samsung TDMA

C. Select Source Model

- Select the **source phone model.**
- **NOTE:** *If you do not know the model, you can often find the phone model on a sticker beneath the battery.*
- Use the ▲▼ keys to move between options. Press OK or ► to continue.
- To return to the previous menu, press ◄ .

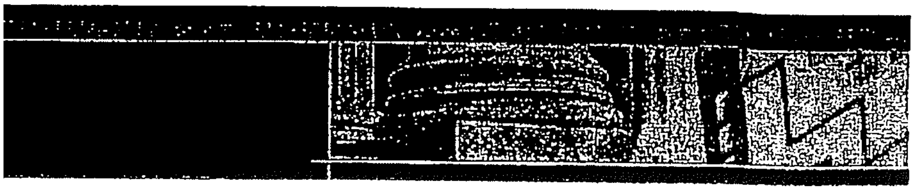


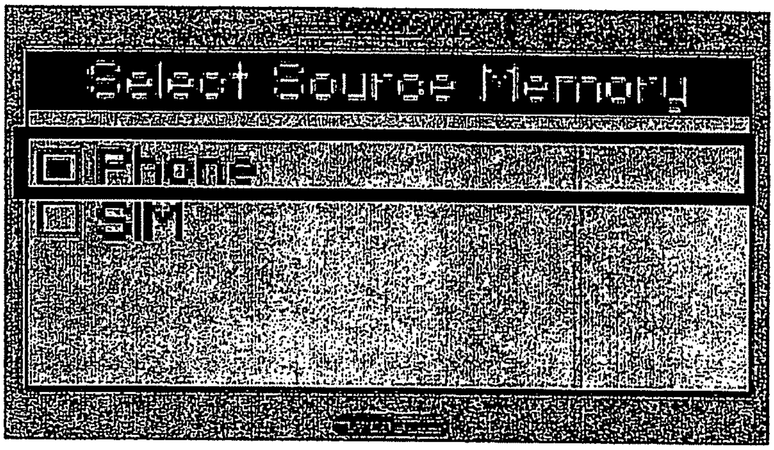


CelleBrite
Select Source Model
Samsung ZV10/ZV30
Samsung ZX10/ZX20
Samsung ZX30
Samsung ZV40
Samsung D100
UFED

D. Select Source Memory

- 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.*





Select Source Memory

□ Phone

□ SIM

[redacted]

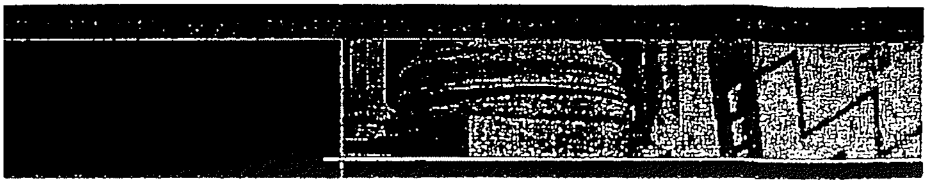
E. Select Source Link

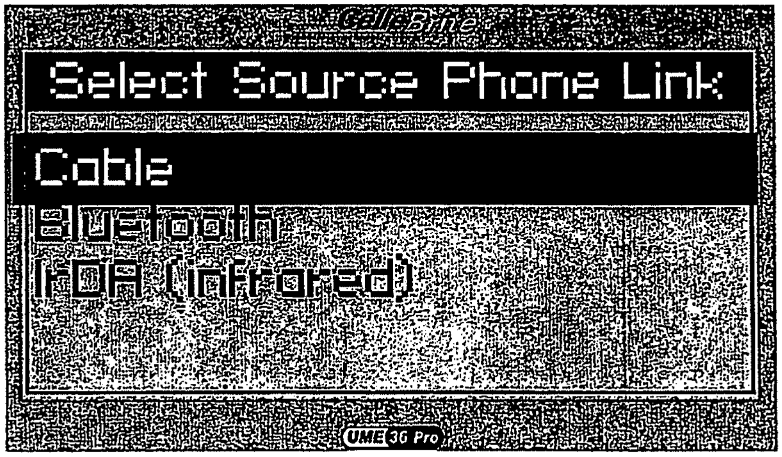
- This step determines how the phone will connect to the UFED. **This message appears only if the phone supports more than one connection method:**

(b) (7)(E)

  - [redacted]
  -

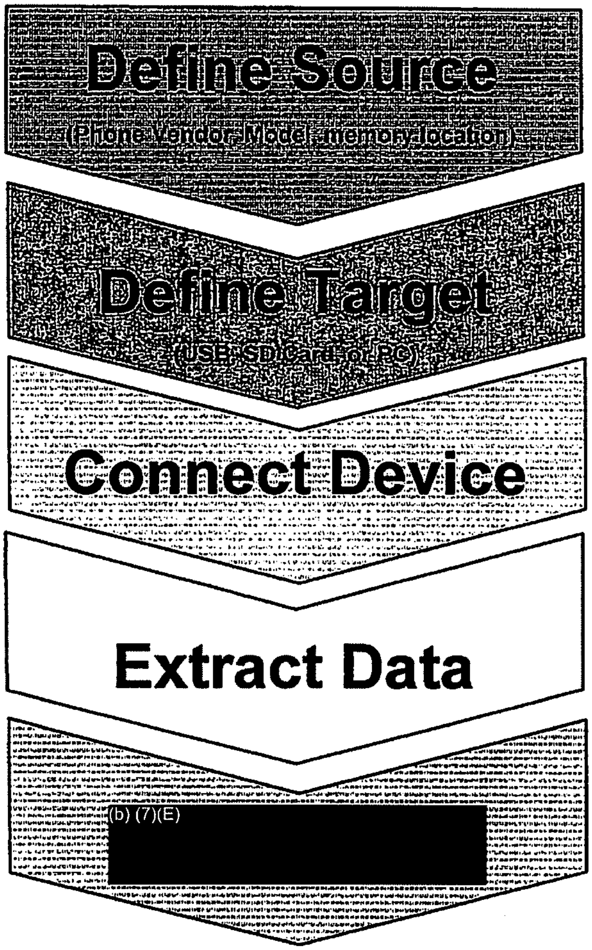
- Use the ▲▼ keys to move between options. Press OK or ► to continue.





Select Source Phone Link

[redacted]



Define Source

(Phone Vendor, Model, memory location)

Define Target

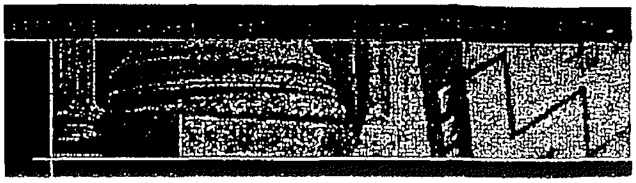
(USB, SD Card, or PC)

Connect Device

Extract Data

(b) (7)(E)

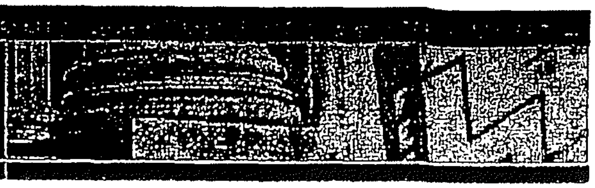
[redacted]



[redacted]

2. Target Selection

- Select (b) (7)(E) [redacted] (b) (7)(E) [redacted] where the content will be copied to.
- **NOTE:** When (b) (7)(E) [redacted] (b) (7)(E) [redacted] the content is stored (b) (7)(E) [redacted] (b) (7)(E) [redacted]
- Use the ▲▼ keys to move between options. Press OK or ► to continue.

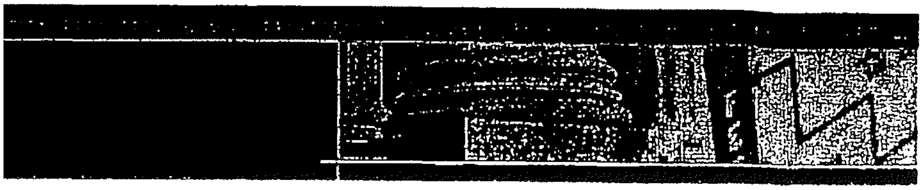


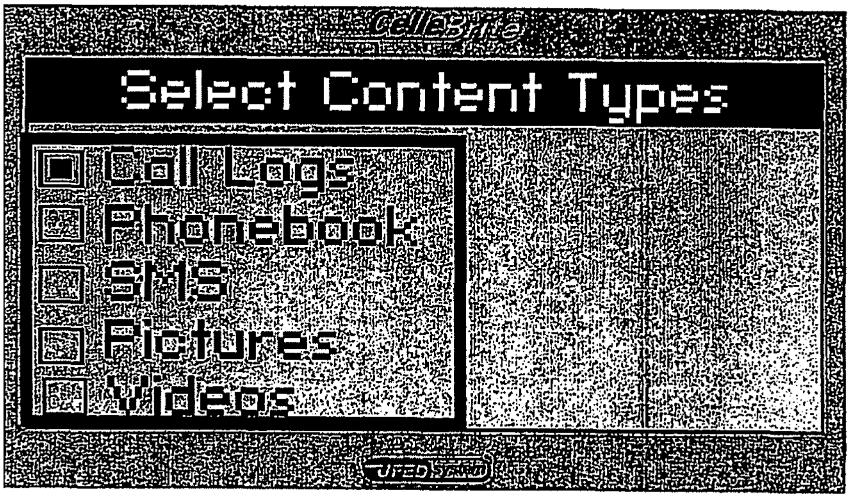
(b) (7)(E)

[redacted]

2. 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).*
- Use the ▲▼ keys to move between options. Press OK to select an option. **Pressing on F2 will select/deselect all options.**
- Press ► to continue.





Select Content Types

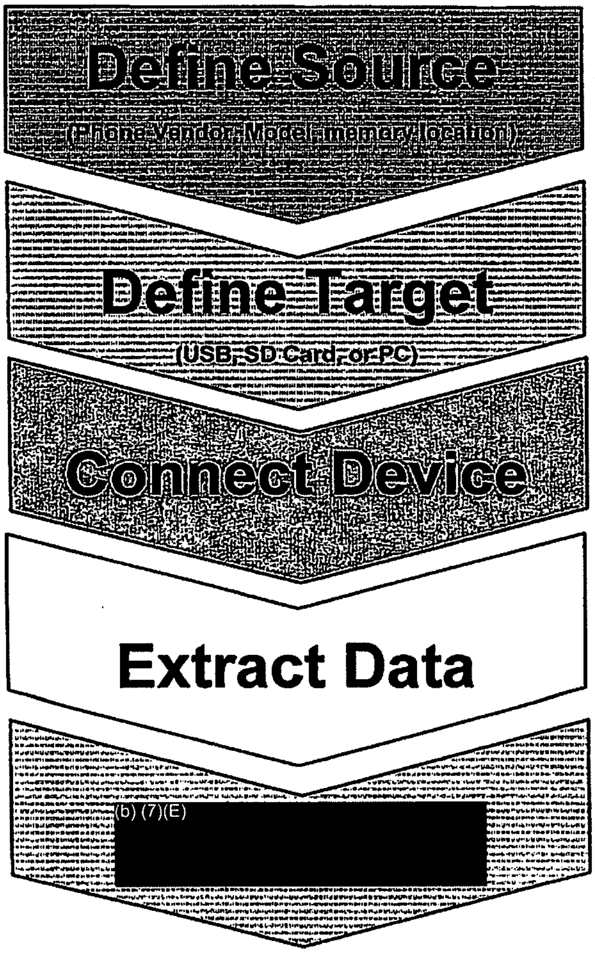
■ Call Logs

□ Phonebook

□ SMS

□ Pictures

□ Videos



Define Source

(Phone Vendor, Model, memory location)

Define Target

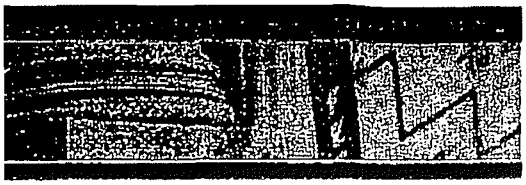
(USB, SD Card, or PC)

Connect Device

Extract Data

(b) (7)(E)

[redacted]



3. Transfer Instructions: Connection

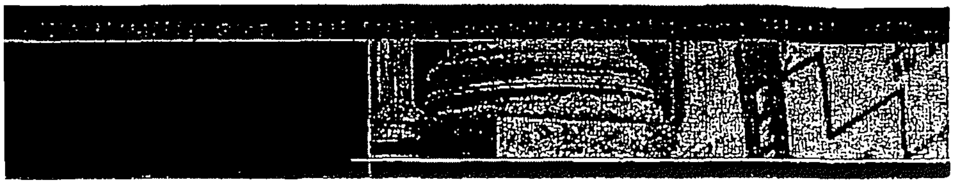
The UFED now displays the connectivity instructions.

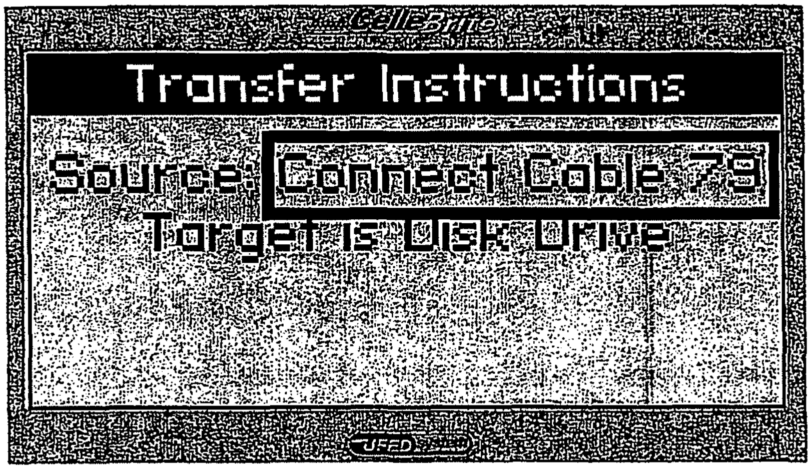
A. **Make sure that the phone is powered on, and the data connector is clean.**

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

B. Press ► to Start extraction.

C. UFED will connect to the phone and the phone entries will be read.





Transfer Instructions

Source: Connect Cable 79

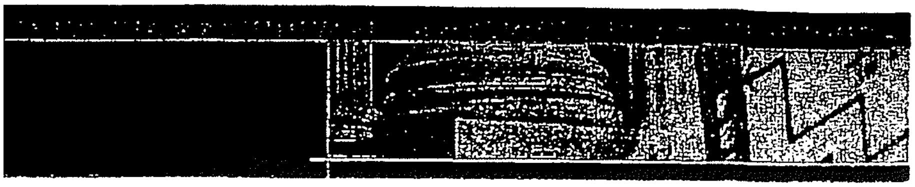
Target is Disk Drive

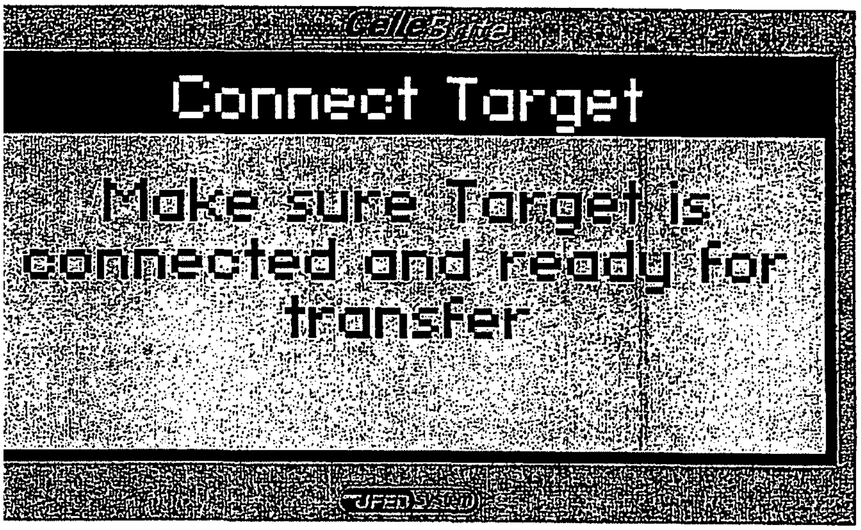
(b) (7)(E)

[redacted]

3. Connect Target Device

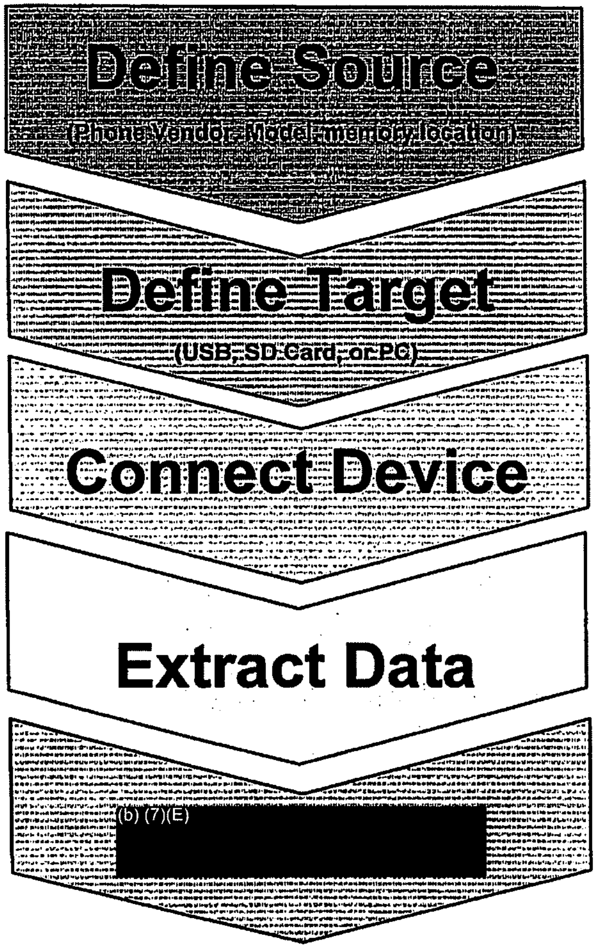
- (b) (7)(E)
- The UFED is ready to copy the data (b) (7)(E)
- **Press ► to continue.**
- WARNING: **Do not disconnect the phone or the power adaptor during the process! Once started, the process should not be interrupted.**





Connect Target

Make sure Target is connected and ready for transfer



Define Source

(Phone Vendor, Model, memory location)

Define Target

(USB, SD Card, or PC)

Connect Device

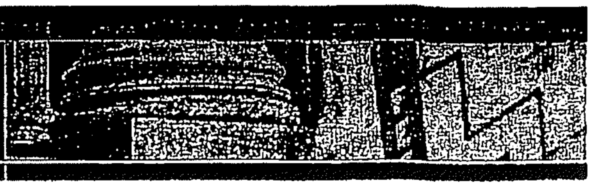
Extract Data

(b) (7)(E) [redacted]

[redacted]

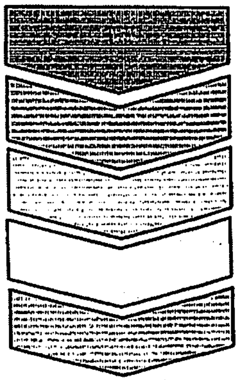
4. (b) (7)(E) [redacted]

   - (b) (7)(E) [redacted]
   - Follow the instructions on the screen for your specific model.
   - Press ▶ to continue.



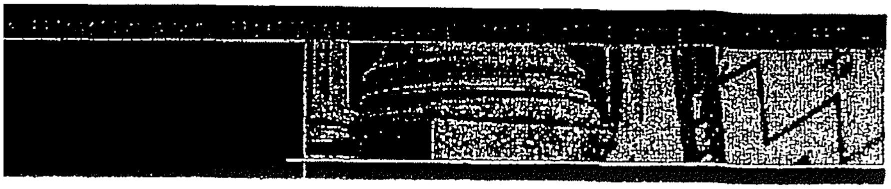
(b) (7)(E)

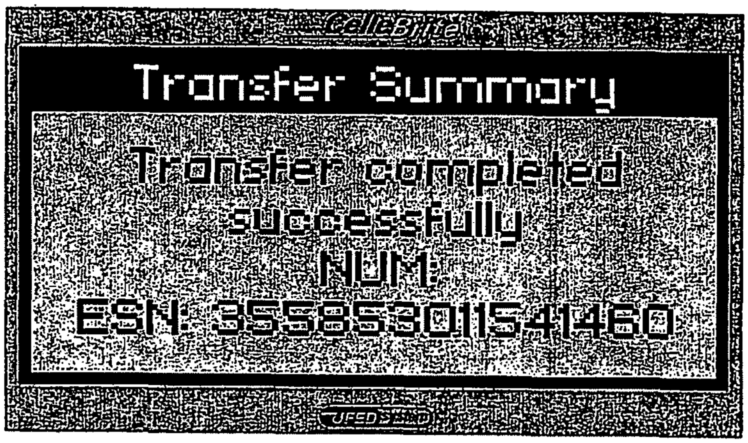
[redacted]



4. Completion

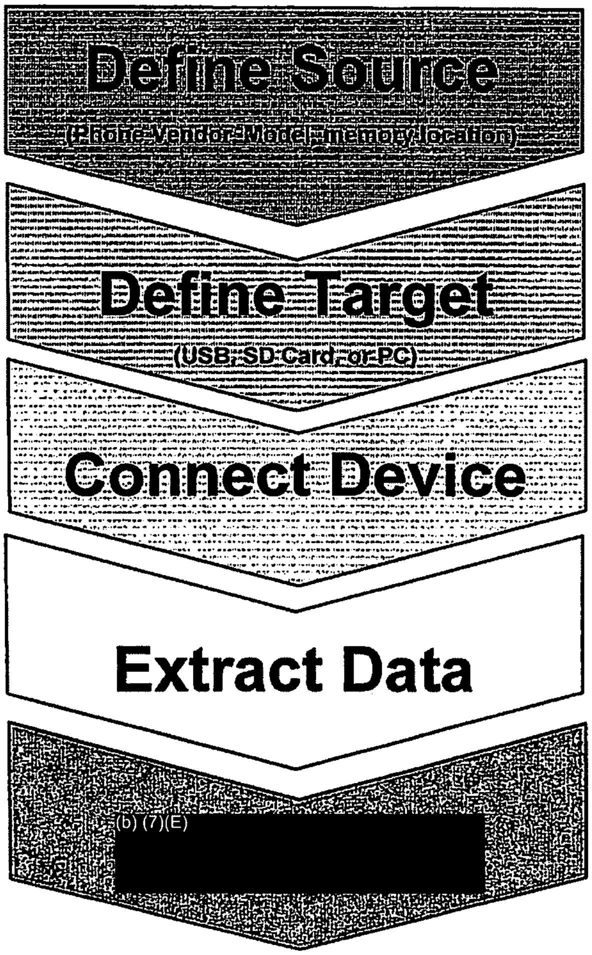
- Upon the completion of the process the UFED- displays a message.
- The message on the screen includes the status of the transfer, the phone's ESN (for GSM) OR IMEI (for CDMA) number.





Transfer Summary

Transfer completed successfully
NUM:
ESN: 355853011541460



Define Source

(Phone Vendor-Model, memory location)

Define Target

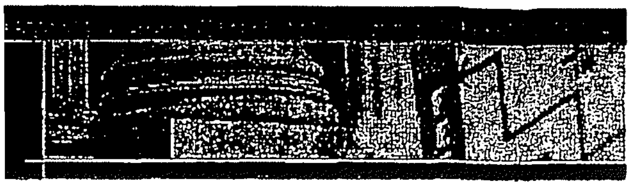
(USB, SD Card, or PC)

Connect Device

Extract Data

(b) (7)(E)

[redacted]



[redacted]

5. (b) (7)(E) [redacted]

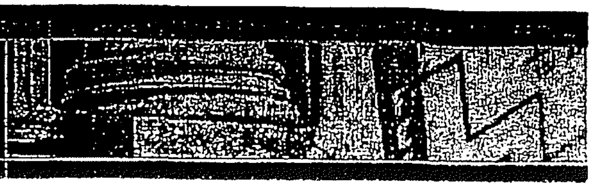
A. (b) (7)(E) [redacted]

- ✓ We just need to (b) (7)(E) [redacted]

A. (b) (7)(E) [redacted] (b) (7)(E) [redacted] and can be opened on any PC.

B. The transfer process is complete and you may now disconnect the phone and the PC from the UFED device.

[redacted]

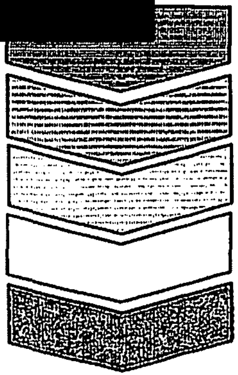


(b) (7)(E)

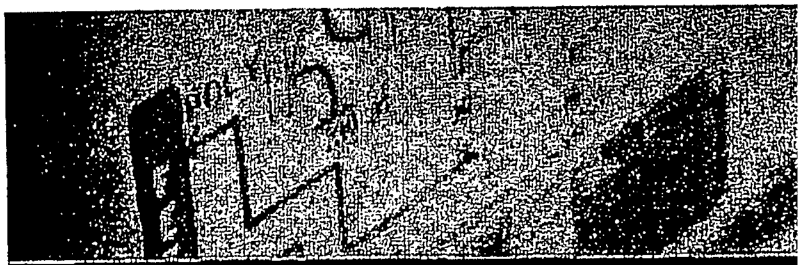
[redacted]

(b) (7)(E)

[redacted]

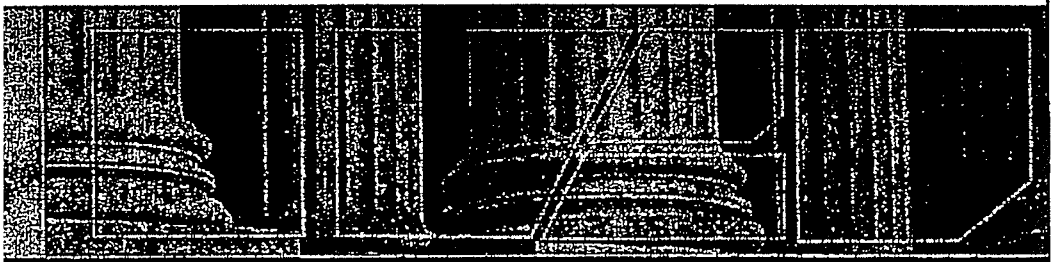


U.S. DEPARTMENT OF HOMELAND SECURITY



Cellebrite UFED

Extracting SIM/USIM Data

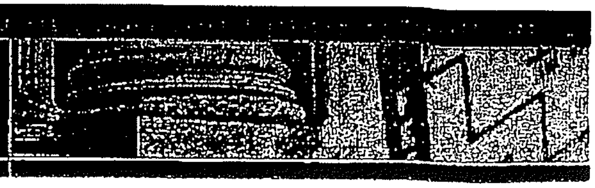


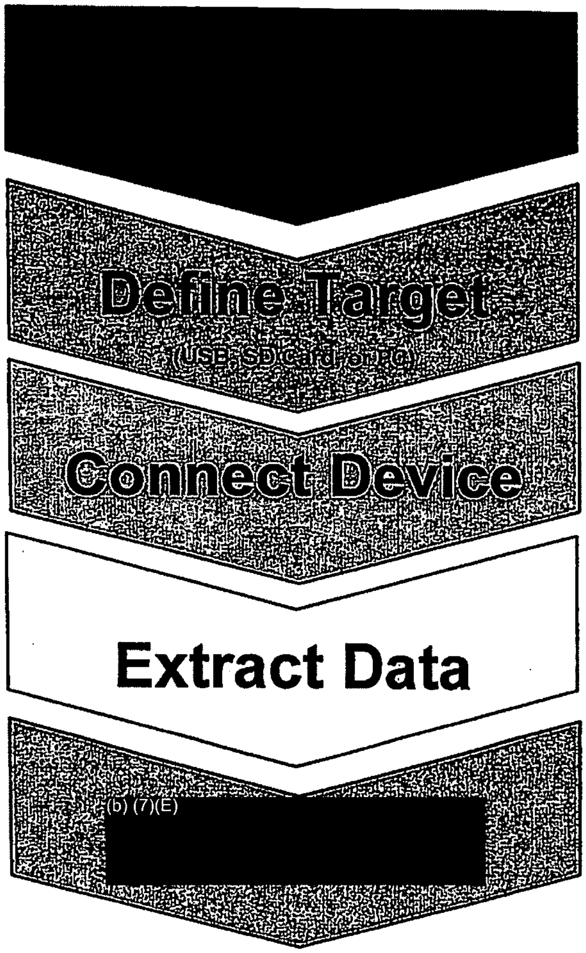
U.S. Customs and
Border Protection

[redacted]

- When working with the UFED, the process flows as described in the following flowchart:

[redacted]





[redacted]

Define Target

(USB, SD card, etc.)

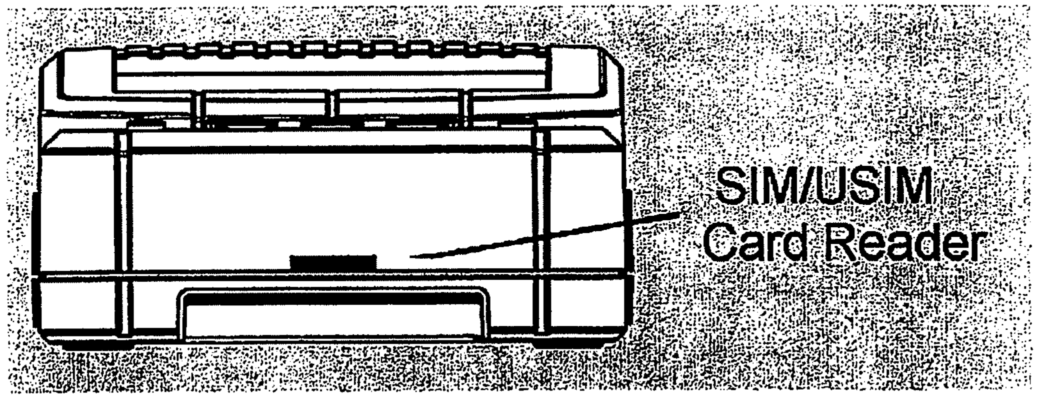
Connect Device

Extract Data

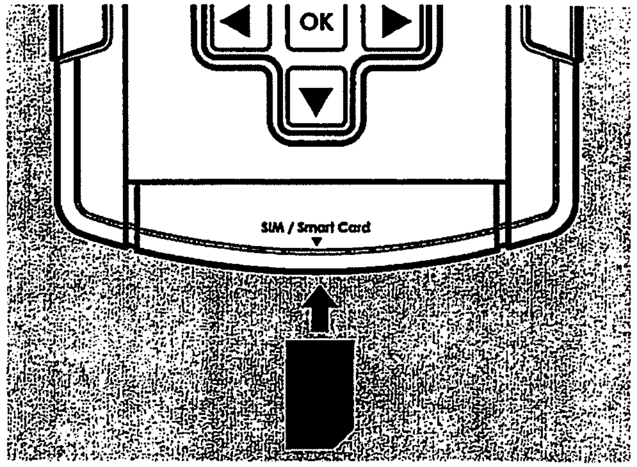
(b) (7)(E)

[redacted]

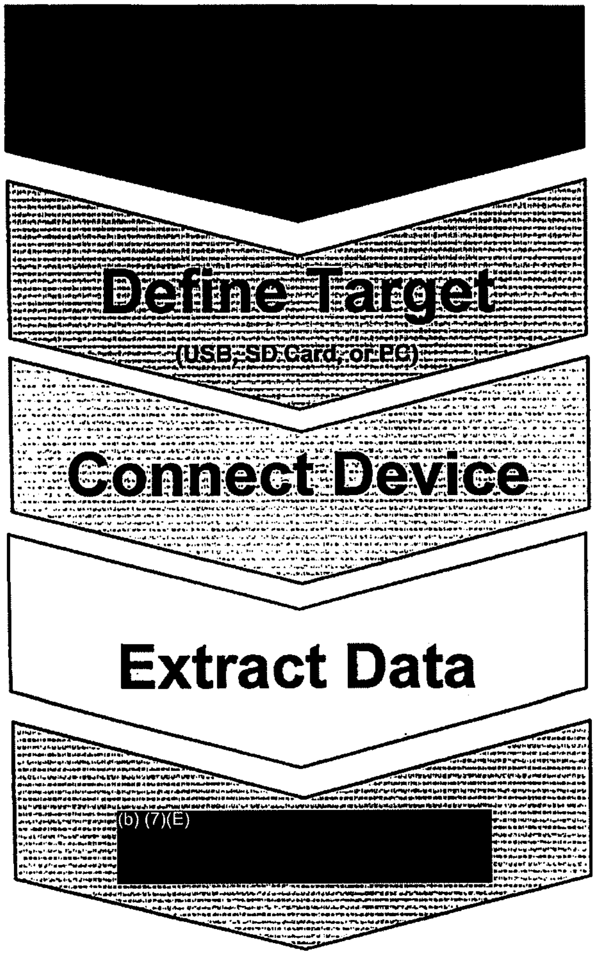
- UFED is equipped with an integrated SIM/USIM card reader.
- It is located at the bottom of the UFED.
- Use this SIM reader to extract data directly from the SIM card instead of via the phone.



- In other words, in a SIM extraction, the UFED reads the SIM data bit by-bit, which will also read deleted messages.
- In a phone extraction, the UFED requests SIM data from the phone, and the phone does the actual SIM reading.
- As a result, the SIM data that comes when performing a phone extraction is dependant on the phone.
- When using the SIM Card Reader, insert the SIM as shown in the picture below. Be sure that the angled side is on the outer side. The actual SIM contacts should be facing down.



[redacted]



[redacted]

Define Target

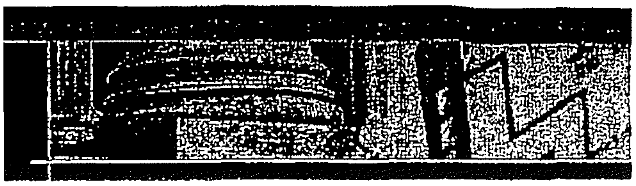
(USB, SD Card, or PC)

Connect Device

Extract Data

(b) (7)(E)

[redacted]



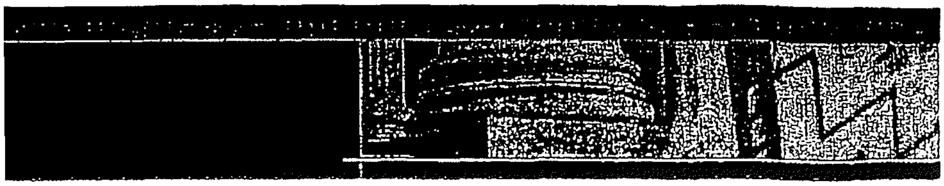
[redacted]

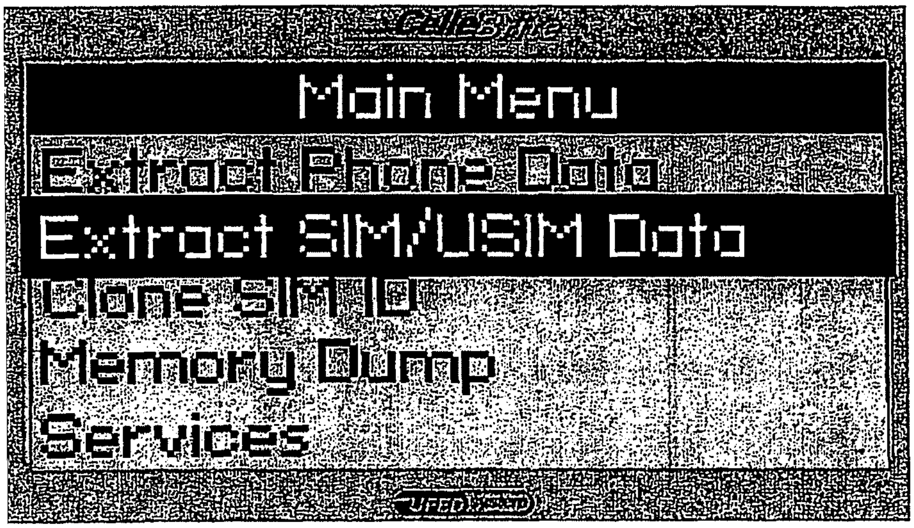
1. Extract SIM/USIM Data

- **Select** Extract SIM/USIM **Data from the main menu.**
- **NOTE:** If the SIM is protected with a PIN, you will need to enter the PIN during the transfer process.

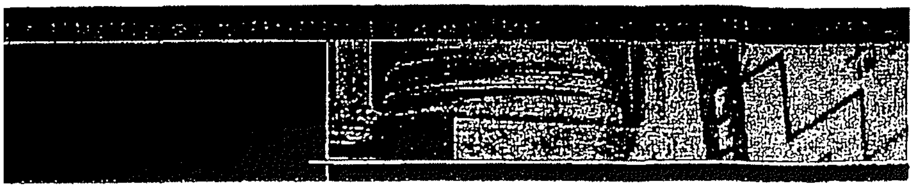
(b) (7)(E)
[redacted]

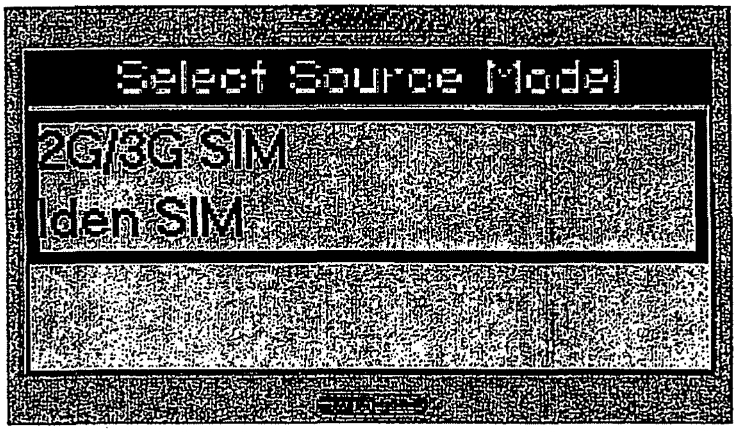
- To enter the PIN code, use the ▲▼ keys to move the cursor to the required digit, and press OK to select that digit.
- Repeat this for each digit of the PIN. To delete a digit, press the © key. When complete, press F3.




Cellebrite
Main Menu
Extract Phone Data
Extract SIM/USIM Data
Clone SIM ID
Memory Dump
Services
UFED

- **Extract SIM/USIM Data**
  - **Select Source Model**
    - 2G/3G SIM
    - Iden SIM



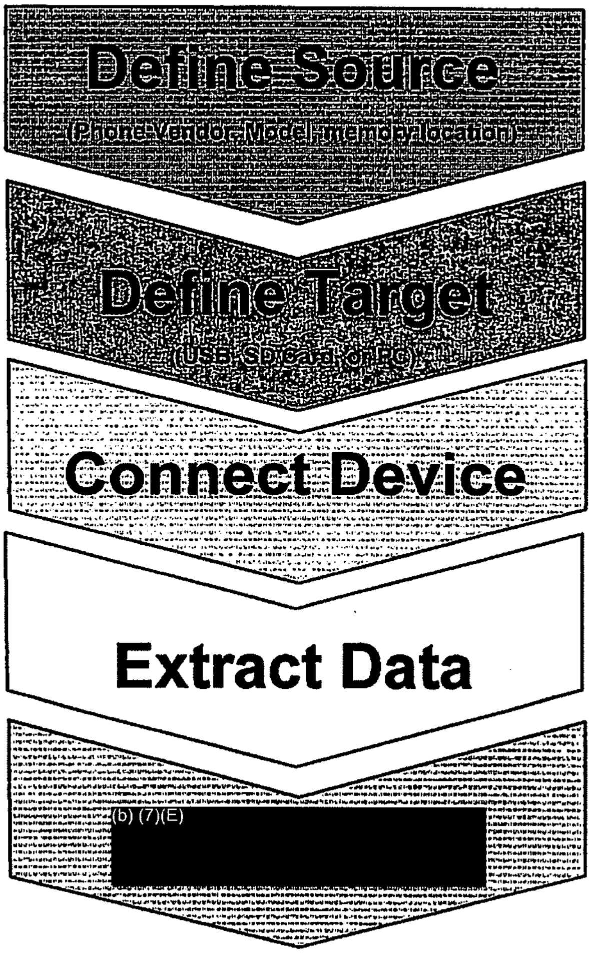


Select Source Model

2G/3G SIM

Iden SIM

[redacted]



Define Source

(Phone Vendor, Model, memory location)

Define Target

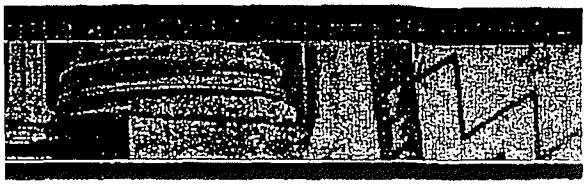
(USB, SD Card, or PC)

Connect Device

Extract Data

(b) (7)(E)

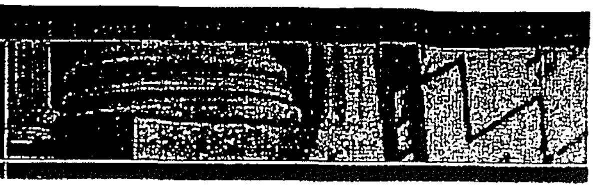
[redacted]



2. Target Selection

- (b) (7)(E) [redacted] (b) (7)(E) [redacted] where the content will be copied to.
- Use the ▲▼ keys to move between options. Press OK or ▶ to continue.

[redacted]



(b) (7)(E)

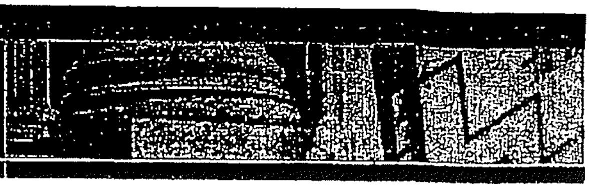
[redacted]

[redacted]

2. Content Types

- (b) (7)(E) [redacted]
- Use the ▲▼ keys to move between options. Press OK to select an option. Pressing on **F2** will select/deselect all options. Press ► to continue.

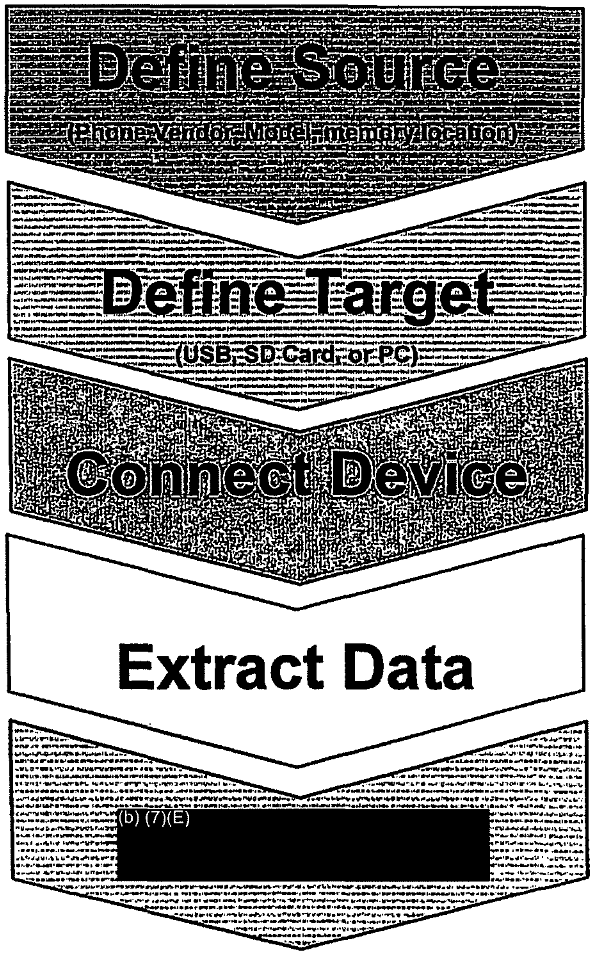
[redacted]



(b) (7)(E)

[redacted]

[redacted]



Define Source

(Phone Vendor, Model, memory location)

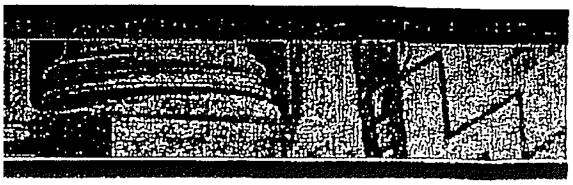
Define Target

(USB, SD Card, or PC)

Connect Device

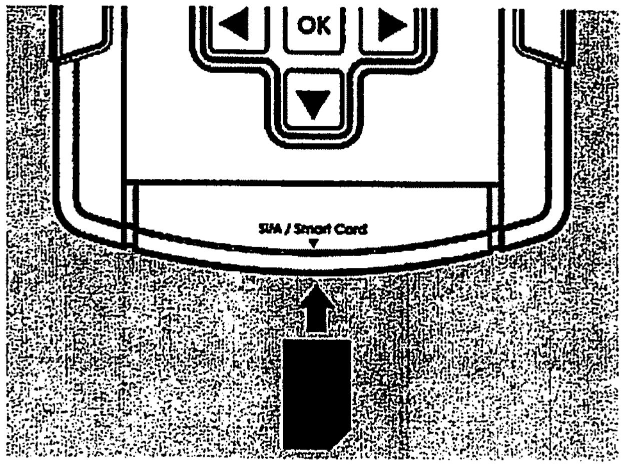
Extract Data

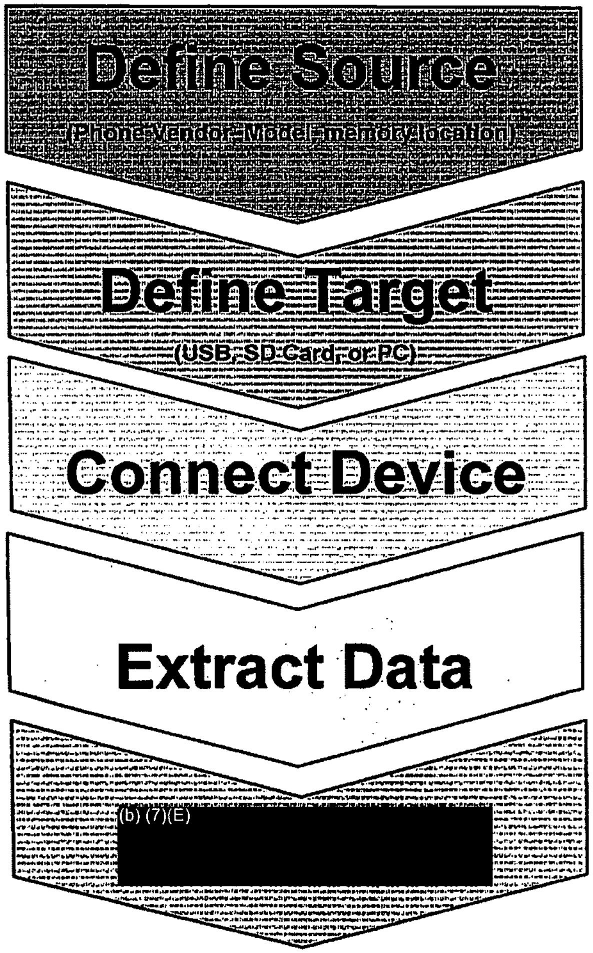
(b) (7)(E) [redacted]



3. Connect Target Device

- (b) (7)(E)
- **Message on UFED:**
  - **Sim reader:** Insert SIM card into the UFED with the SIM card's contacts facing down and the sliced corner pointing toward you.
- Press OK or ► to continue.
- The UFED will connect and read the SIM info.





Define Source

(Phone vendor, Model, memory location)

Define Target

(USB, SD Card, or PC)

Connect Device

Extract Data

(b) (7)(E)

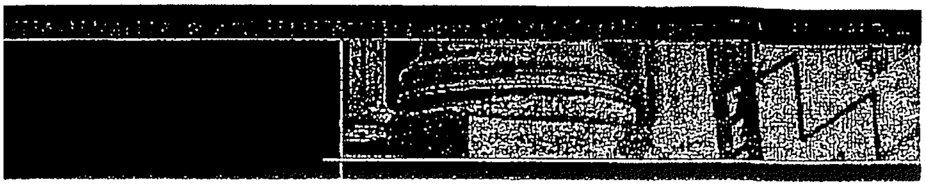
[redacted]

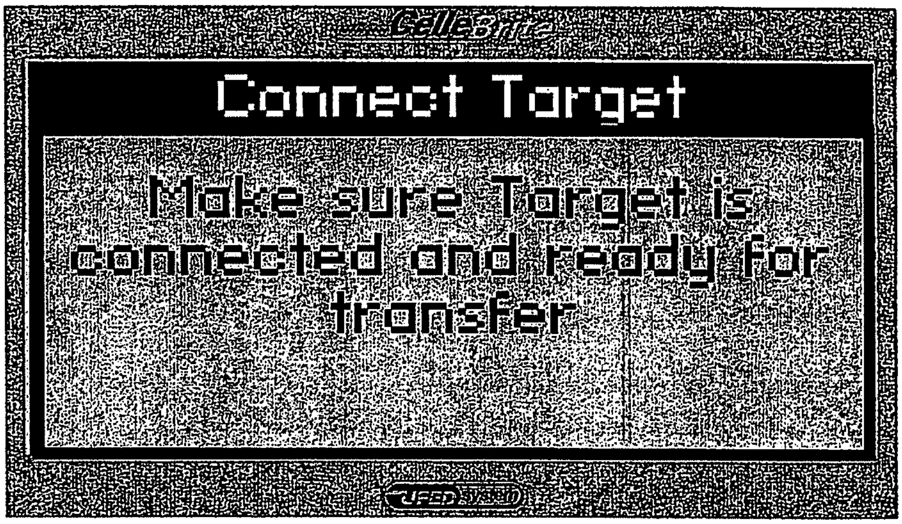
[redacted]

4. Connect Target Device

- The UFED is ready to copy the data (b) (7)(E) [redacted]

- Press ► to Continue.
- Transfer completed successfully NUM: and ESN will be displayed.
- Press ► to continue.

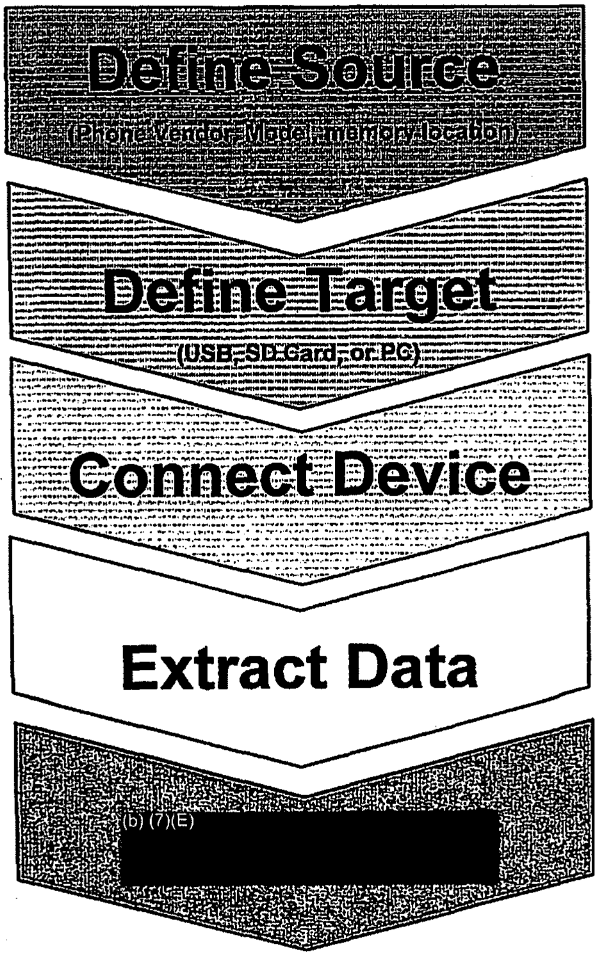




Connect Target

Make sure Target is connected and ready for transfer

[redacted]



Define Source

(Phone Vendor, Model, memory location)

Define Target

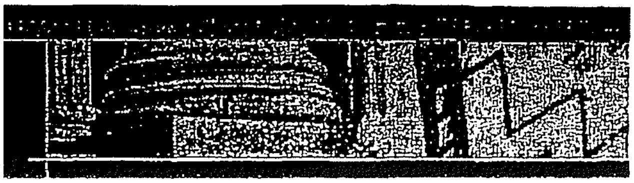
(USB, SD Card, or PC)

Connect Device

Extract Data

(b) (7)(E)

[redacted]



[redacted]

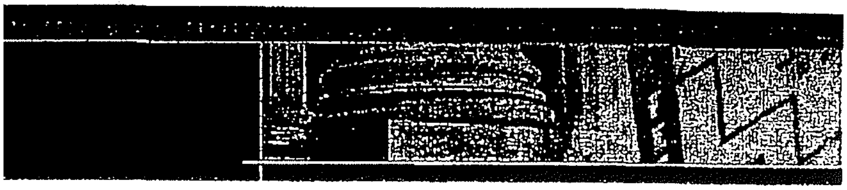
5. (b) (7)(E)

A. (b) (7)(E)

✓ We just need to (b) (7)(E)

A. (b) (7)(E) (b) (7)(E) and can be opened on any PC.

B. The transfer process is complete and you may now disconnect the phone and the PC from the UFED device.



(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]