



SAN DIEGO POLICE DEPARTMENT
FORENSIC SCIENCE SECTION



Forensic Technology Unit Manual

ARCHIVED

1. UNIT DESCRIPTION

Office hours are based on an alternative work schedule and generally run from 0600 to 1530 hours. Staffing consists of three full time examiners, trained to provide laboratory analyses of mobile devices and related materials. All positions within this unit are currently filled by civilians.

The unit is responsible for extracting and/or examining digital evidence stored in mobile devices for the purpose of providing investigators with evidence that may assist in their investigation.

Job duties include, but are not limited to:

1. Extraction of data from mobile devices
2. Analysis of extracted data
3. Preparing reports on mobile device examinations
4. Court testimony
5. Training investigators in evidence collection pursuant to mobile device examinations
6. Maintaining equipment
7. Assuring quality control elements of the program are implemented throughout the process
8. Projecting, planning, and reviewing new technologies as they become available.

2. CASE MANAGEMENT

2.1 WORK REQUESTS

The Forensic Technology Unit work request form can be submitted to the laboratory receptionist, the Forensic Technology Unit, the crime laboratory manager, or Forensic Technology Unit supervisor. A request may be submitted on other laboratory forms.

The request will be processed through the Clerical Unit for entry into the laboratory's work request database. The supervisor will review for appropriateness prior to assigning.

Legal authority (search warrant, consent form, etc.) must be provided with the actual work request before commencing with any forensic examination. Legal authority is not required for 4th graders.

2.2 CASE ASSIGNMENT

Incoming cases are prioritized with the highest priority on cases involving a threat, then cases with a court date, and finally by the date of receipt.

The Unit Supervisor will maintain requests for cases to be worked. When an examiner is ready for a new case, the examiner will inform the supervisor who will then assign the highest priority case to the examiner. If an examiner is already at work on a case when a higher priority case is submitted, the lower priority case will be repackaged and put away until the higher priority case is completed.

2.3 CASE TRACKING

All requests are logged into the laboratory computer database by the Clerical Unit. Case assignment and completion are tracked by the unit supervisor with the dates being entered into the laboratory case tracking database.

Unit statistics (completed cases, backlogged cases, etc.) are available upon request.

3. RECEIVING EVIDENCE

Evidence may reach the Forensic Technology Unit by the following routes:

1. The evidence can be impounded in the Property Room and received by the examiner.
2. A requesting officer can submit evidence directly to the examiner during walk-in examinations. The requesting officer will maintain chain of custody throughout the examination.
3. Direct transfers other than walk-ins. A Chain of Custody form will be created in these instances.

Due to the importance of chain-of-custody, evidence submitted through inter-office mail will not be accepted. It will be routed back to the detective.

Impounded evidence is not to remain in the unit for more than one month if it is not being analyzed. The examiner must return the evidence and pick it up again later when the case is ready to be worked. The supervisor may approve longer stays depending on the case circumstances.

4. GENERAL ANALYTICAL REQUIREMENTS

4.1 INTRODUCTION

Mobile devices may contain, but are not limited to, data such as text messages, phone numbers, audio files, and graphic files.

Due in large part to the various protocols used on mobile devices by the various manufacturers, a variety of tools and techniques should be available in order to analyze these devices. Tools shall be constantly updated as new devices with new protocols are released, or as research determines that more data may be extracted for certain models.

An audit trail or other record of applied processes, suitable for replication of the results by an independent third party, must be created and preserved, accurately documenting each investigative step.

4.2 LEGAL AUTHORITY TO CONDUCT EXAMINATIONS

It is the responsibility of the examiner to have documentation of the legal authority (i.e. search warrant, consent form, etc.) to perform an examination prior to commencing any search examinations. The scope of the legal authority must also be reviewed by the examiner.

A copy, when possible, of the legal authority documentation will be placed in the case record.

The examiner may need to specifically inquire about potential confidential or privileged information per the Privacy Protection Act that may be encountered while processing the submitted evidence.

Privileged Data

In the event that an examiner encounters documents or data files which the Examiner believes may be legally privileged, the examiner will immediately stop the analysis and contact the submitting agency and/or the prosecuting attorney handling the case for guidance as to how to proceed.

Evidence of Other Crimes

If an examiner discovers evidence of another crime(s) that is outside the scope of the submitted legal authority, the examiner must stop all analysis and contact the submitting agency and/or prosecuting attorney handling the case for guidance as to how to proceed. The examiner will inform the Digital Evidence Unit supervisor, or designee, of the discovery and nature of any evidence of other crime(s) outside the scope of the original search warrant.

NOTE: Analysis per the original legal authority can be continued, but only to include the original search criteria.

4.3 PRELIMINARY CONSIDERATIONS

When examining a device, the examiner should proceed cautiously. Incorrect procedures or improper handling of a mobile phone can cause loss of digital evidence. Moreover, traditional forensic measures, such as fingerprints or DNA testing, may need to be applied to establish a link between a mobile phone and its owner or user, or for other reasons. If the device is not handled properly, physical evidence can be easily contaminated and rendered useless.

Alertness to device characteristics and issues (e.g., memory volatility) and familiarity with associated accessories (e.g., media, cables, cradles, and power adapters) are essential. For cell phones, sources of evidence include the device, (U)SIM, and media. Associated peripherals, cables, cradles, power adapters, and other accessories are also of interest.

Mobile phones and associated media may be found in a damaged state. Devices or media with visible external damage do not necessarily prevent the extraction of data from them. Repairing damaged components on a mobile phone and restoring the device to working order for examination and analysis may be possible. Undamaged memory components may also be removed from a damaged device and their contents recovered independently. It should be understood, though, that in any given case, data may not be entirely extracted or could possibly be deleted.

It should be noted that, due to constant changes in mobile device technology, there may be data on any given device that is irretrievable.

Since dynamic functions of a mobile device (i.e. the internal clock, activity counters, etc.) continue changing beyond the point of seizure, preserving the mobile device in exactly the same state as when seized may not be possible.

4.4 EQUIPMENT

Approved forensic hardware/software to include necessary cables

Device to block the transmission and reception of data for mobile devices

Cell phone repair tools and parts

4.5 DEVICE IDENTIFICATION

Record the manufacturer and model of the seized equipment, and also its condition. This information allows examiners to select the appropriate tools for acquisition.

Individuals may attempt to thwart specialists by altering the device to conceal its true identity. Device alteration could range from removing manufacturer labels to filing off logos. In addition, the operating system and applications may be modified or in rare situations completely replaced, and appear differently as well as behave differently than expected. For example, removing or replacing splash screens is a widely discussed modification in phone forums.

If the phone is powered on, the information appearing on the display can sometimes help identify the type of phone. For example, the manufacturer's or service provider's name may appear on the display, or the screen layout may indicate the family of operating system used. Information such as the manufacturer's label may be found in the battery cavity (e.g., Make, Model, IMEI, and ESN). Removing the battery from the cavity of a phone, even when powered off, can affect its state, particularly the contents of volatile memory. Most phones keep user data in non-volatile memory, however, with the exception of certain smart phones. If the phone is powered on, battery removal will power it off, possibly causing an authentication mechanism to trigger when again powered on.

Other clues that allow identification of a device include such things as manufacturer logos, serial numbers, the cradle, and power adapter. Overall, knowing the make and model helps to limit the potential service providers, by differentiating the type of network the device operates over (i.e., GSM, non-GSM), and vice versa. Synchronization software discovered on an associated computer also helps to differentiate among operating system families. Further means of identification include the following areas:

Device Characteristics – The make and manufacturer of a phone can sometimes be identified by its observable characteristics (e.g., weight, dimensions, and form factor), particularly if unique design elements exist. Various Web sites contain databases of phones that can be queried based on

selected attributes to identify a particular device and obtain its specifications and features. Coverage is considerable, but not extensive or complete, and may require consulting more than one repository before making a match.

Device Interface – The power connector is often specific to a manufacturer and a reliable aid to identification. With familiarization and experience, the manufacturers of certain devices can be readily identified. Similarly, the size, number of contacts, and shape of the data cable interface of a phone used to create a connection to a host computer are often specific to a particular manufacturer and may prove helpful in identification. Unfortunately, the available databases for these interfaces lack the broad coverage to be of assistance.

Device Label – For phones powered-off, information obtained from within the battery cavity can be revealing, particularly when coupled with an appropriate database. The manufacturer's label often lists the make and model number of the phone and also unique identifiers, such as the Federal Communications Commission Identification Number (FCC ID) and an equipment identifier (IMEI or ESN). The FCC and equipment identifiers can be found on cell phones sold in the U.S. domestic market. For GSM or other (U)SIM bearing phones, the (U)SIM is usually located under the battery and is typically imprinted with a unique identifier called the Integrated Circuit Card Identification (ICCID). For powered-on GSM and UMTS phones, the International Mobile Equipment Identifier (IMEI) can be obtained by keying in *#06#. Similar codes exist for obtaining the Electronic Serial Number (ESN) from powered-on CDMA phones. Various sites on the Internet offer databases for querying the identifier and providing information about the device.

The IMEI is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The initial 8-digit portion of the IMEI, known as the Type Allocation Code (TAC), gives the model and origin. The remainder of the IMEI is manufacturer specific, with a check digit at the end [GSM04]. A database lookup service is available from the GSM numbering plan Web site.

The ESN is a unique 32-bit identifier recorded on a secure chip in a mobile phone by the manufacturer. The first 8-14 bits identify the manufacturer and the remaining bits the assigned serial number. Many phones have codes that can be input into the handset to display the ESN. Hidden menus can also be activated on certain phones by placing them in "test mode" through the input of a code. Besides the ESN, other useful information such as the phone number of the device can be obtained. Manufacturer codes can be checked on-line at the Telecommunications Industry Association Web site.

The ICCID of the (U)SIM can be up to 20 digits long. It consists of an industry identifier prefix (89 for telecommunications), followed by a country code, an issuer identifier number, and an individual account identification number. The country and network operator name can be determined by the ICCID. If the ICCID does not appear on the (U)SIM, it can always be obtained with a (U)SIM acquisition tool. The GSM numbering plan Web site supports ICCID queries for this information.

The first 3 characters of the FCC ID are the company code; the next 14 are the product code. The FCC provides a database lookup service that can be used to identify a device manufacturer and retrieve information about the phone, including photos, user manual, and radio frequency test results.

Reverse Lookup – If the telephone number of the phone is known, a reverse lookup can be used to identify the network operator (e.g., Cingular) and the originating city and state (e.g., Washington D.C.). For example, FoneFinder (<http://fonefinder.net/>) is a service to obtain such information by inputting the user's area code, three-digit prefix, and the seventh digit of the phone number. The network operator's Web site typically contains lists of supported phones that can be used to narrow down and possibly identify the phone in question. Because phone numbers can be ported among service providers, in many situations more up-to-date information is needed. The Number Portability Administration Center (NPAC) provides an automated phone system for law enforcement agencies to determine the current service provider assigned to a number and obtain contact information.

Other websites that allow identification of a device's provider include: <http://www.numberingplans.com/>, <http://www.searchlog.com/peoplefinder/landline-or-cellphone.aspx>, and www.nationalnanpa.com

4.6 ISOLATING THE PHONE

Stop the reception and transmission of data by powering down the device, use of a transmission blocking barrier, or device setting (e.g. Airplane Mode), if applicable.

When determining which method of isolating the device is appropriate, keep in mind the following considerations:

Turning off the phone may activate authentication codes (e.g., SIM PIN and/or handset security codes) when it is turned on again, which are then required to gain access to the device, complicating acquisition and delaying examination.

Keeping the phone on, but radio isolated, hastens battery depletion due to increased power consumption as it tries unsuccessfully to connect to a network, raising its signal strength to the maximum. After some period,

failure to connect to the network may cause certain phones to reset or clear network data that otherwise would be useful if recovered. Containers (e.g., Faraday bag) attenuate the radio signal, but may not eliminate it completely, allowing the possibility of communications being established with a cell tower if in its immediate vicinity. The risk of improperly sealing the radio isolation container, thereby allowing access to the cell network cannot be ignored.

Enabling “Airplane Mode” requires interaction with the phone via the keypad, which poses some risk – less so, if the technician is familiar with the device in question and documents the actions taken (e.g., on paper or on video).

Caution should be exercised when handling a phone suspected of being modified, especially if the modifications are presumed to be done by a security-minded individual or organization. Certain modifications to the software applications and operating system of the device might require special care in the way it is handled.

Following is a list of examples of some classes of modifications to consider:

Security Enhancements – Organizations and individuals may enhance their handheld devices with add-on security mechanisms. A variety of visual login, biometric, and token-based authentication mechanisms are available for smart phones to use as replacement or supplements to password mechanisms. Improper interaction with a mechanism could cause the device to lock down and even destroy its contents. This is particularly a concern with mechanisms that use security tokens whose presence is constantly monitored and whose disconnection from a card slot or other device interface is immediately acted upon.

Malicious Programs – A phone may contain a virus or other malicious software. Such malware may attempt to spread to other devices over wired or wireless interfaces, including cross platform jumps to completely different platforms. Common utilities or functions may also be intentionally replaced with versions that contain software designed to alter or damage data present on a phone. Such Trojan-bearing programs could conditionally be activated or suppressed based on conditions such as input parameters or hardware key interrupts. Watchdog applications could also be written to listen for specific events (e.g., over-the-air messages) and carry out actions such as wiping the device clean.

Key Remapping – Hardware keys may be remapped to perform a different function than the default. A key press or combination of key presses intended for one purpose could launch an arbitrary program (e.g., “Global Thermonuclear War”).

4.7 MOBILE DEVICE DATA ACQUISITION—GENERAL INFORMATION

Data acquisition is the process of imaging or otherwise obtaining information from a digital device and its peripheral equipment and media. Performing acquisition at the scene has the advantage that loss of information due to battery depletion, damage, etc. during transportation and storage is avoided.

However, finding a controlled setting in which to work, having the appropriate equipment, and satisfying other prerequisites may not be possible at the scene, but readily achievable within a laboratory setting. The crime laboratory is the preferred setting for data acquisition.

Mobile devices are often submitted for laboratory processing with only specific items requested for recovery, such as phone call logs or images. If any doubt or concerns exist about the requested data, contacting the person who initiated the examination for clarification is recommended. Though it is not always necessary to recover all available data, a complete acquisition avoids having to redo the process later if other data is needed, and the possibility that technical problems may arise on a later attempt.

To acquire data from a phone, a connection must be established to the device from the forensic workstation. Before performing an acquisition, the version of the tool being used should be documented, along with any applicable patches or errata from the manufacturer applied to the tool. Caution should be taken to avoid altering the state of a mobile phone when handling it, for example, by pressing keys that could potentially corrupt or erase evidence. Once the connection has been established, the forensic software suite can proceed to acquire data from the device. Steps involved in an acquisition include selecting a connection, identifying the device to be acquired, identifying the data to be recovered, and viewing the recovered data.

Acquiring a device's contents requires the device to be switched on. This effectively means that the evidentiary principle "actions taken should not modify data contained on the device" cannot be complied with, strictly speaking. Therefore, the goal during acquisition is to affect memory contents as little as possible and then only with the knowledge of what is occurring internally, relying more on adherence to evidentiary principles that emphasize high competence of the specialist and the capture of a detailed audit trail of the actions taken.

The contents of a phone are typically dynamic and continually changing. Two back-to-back acquisitions of a device using the same tool may produce different results overall (e.g., if memory compaction occurs), though the majority of information remains unchanged.

Forensic tools that acquire the contents of a resident memory card normally perform a logical acquisition. To recover deleted data that might reside on the memory card, a direct acquisition can be performed on it after the contents of the mobile phone have been successfully acquired. With either type of acquisition, the forensic tool may or may not have the capability to decode recovered phone data stored on the card, requiring additional manual steps to be taken.

After an acquisition is finished, the examiner should always confirm that the contents of a device were captured correctly. On occasion, a tool may fail its task without any error notification and require the specialist to reattempt acquisition with the same tool or another tool. Similarly, some tools do not work as well with certain devices as others do and may fail with an error notification. Thus, where possible, it is advisable to have multiple tools available and be prepared to switch to another if difficulties occur with the initial tool.

Invariably, not all relevant data viewable on a phone using the available menus can be captured through a logical acquisition. For example, draft and archived messages are sometimes not recovered by forensic tools. Manually scrutinizing the contents via the phone interface menus while video recording the process not only allows such items to be captured and reported, but also confirms that the contents reported by the tool are consistent with observable data. Manual acquisition must always be done with care, preserving the integrity of the device in case further, more elaborate acquisitions need to be conducted.

The contents of a phone's memory often contain information, such as deleted data, that is not recoverable through either a logical acquisition or a manual examination. Lacking a software tool able to perform a physical acquisition, it may be necessary to turn to a hardware-based technique.

4.8 EXAMINATION PROCEDURE

The following steps should be taken into consideration when examining a cellular device.

Step 1

If the device is off, do not turn it on until ready for examination.

If the device is on, continue to Step 2.

If the device is damaged or cannot be determined that it is turned off, continue to Step 2.

Step 2

Check for passwords and consider disabling it if possible.

Attempt to prohibit the transmission/reception of data as soon as practical (e.g. Faraday fabric, metal "non evidence" container, placing phone in airplane mode, etc.).

Document what measures were taken to prohibit the transmission/reception of data and any alterations made to the mobile device.

Note: A Faraday device may not block all radio frequency transmissions for some mobile devices. Document any observed transmission activity.

Step 3

As soon as possible, attempt to power the cellular device by an external power source or ensure it has enough power reserves to prevent it from turning off prior to examination. Charge battery prior to examination if the device cannot be powered during examination.

Note: When a radio frequency blocking device is utilized, the cellular phone may boost its wireless signal strength in an attempt to connect with the cellular network. The power consumption will increase during this activity and drain the battery. The power cable may act as an antenna, so the cable must also be shielded to prevent the transmission/reception of radio frequencies.

Step 4

Perform examination of the mobile device as soon as possible.

Note: Some devices may require constant power from the battery to maintain volatile memory. If the device is discovered in a liquid, the device's battery or power supply should be removed and kept separate from the device. The device should be collected in and left in the sample of the discovered liquid to prevent oxidation of the metallic components prior to examination.

Note: Blood and corrosive liquids may continue damaging the metallic components, and the device may need to be stored in a different liquid (i.e. water) to limit the damage, pending examination.

When possible, a forensic image should be created from removable storage media independent of the mobile device prior to conducting any examinations on the mobile device.

Descriptive information of the removable storage media must include, at minimum, the following:

Make

Model (if displayed)

Serial Number (if displayed) Capacity

A write blocker must be used when extracting data from removable storage media independent of the mobile device. Some devices require the flash memory card to be present for the device to work normally, so the card may be returned to the mobile device for additional examinations.

SIM Card Examination

When possible, the SIM / Micro SIM card should be examined independent of the mobile device prior to conducting any examinations on the mobile device. Each partition that is present on the SIM card should be selected for extraction and analyzed.

If the mobile phone is active, a joint acquisition of the handset and (U)SIM contents should be carried out before the (U)SIM is acquired directly.

External descriptive information of the SIM / Micro SIM card must include the following if present:

Network

ICCID

Some devices require the SIM / Micro SIM card to be present for the device to work normally, so the SIM / Micro SIM card (or a clone made from it) may be returned to the mobile device for additional examinations.

Repair – If the mobile device is not functioning it may be repaired by an analyst trained in mobile device repair techniques. These repairs may include removing and replacing internal parts, or cleaning corrosion caused by water damage or age.

The mobile device shall be carefully disassembled and inspected. If corrosion is evident on critical components shall be cleaned as appropriate. If the corrosion is widespread, the entire circuit board may be cleaned using cleaning solution and an ultrasonic cleaner.

If a critical component is physically damaged it may be repaired or replaced by an analyst trained in such repairs. Replacement parts may be found from online distributors or in the laboratory's mobile device collection. Photographic documentation of the repair will be kept in the case notes. If the replacement part is easily removable (i.e. not soldered to the circuit board) it may be removed from the mobile device prior to returning the device.

GSM Phone Consideration

If the mobile phone is active, a joint acquisition of the handset and (U)SIM contents should be carried out before the (U)SIM is acquired directly. A direct acquisition recovers deleted messages present on a (U)SIM, while an indirect acquisition via the handset does not. The SIM must be removed from the phone and inserted into an appropriate reader for direct acquisition. One reason for this sequence is that removal of the (U)SIM, which is typically located beneath the battery, can result in the loss of non-volatile memory due to the power disruption.

A well-known forensic issue that arises when following this sequence is that the reported status of unread SMS text messages is inconsistent between each (U)SIM acquisition – the first one declaring it to be unread, while the second one read. Reading an unread SMS message from a (U)SIM indirectly through the handset

causes the operating system of the phone to change the status accordingly. Had the (U)SIM been read directly by a tool, no change in status would occur. One way to avoid the inconsistency is to omit selecting the recovery of (U)SIM-resident SMS text messages when performing the joint acquisition, if the tool allows such an option.

If the mobile phone is inactive, the contents of the (U)SIM may be acquired independently before that of the handset. The (U)SIM acquisition should be done directly through a (U)SIM reader. The handset acquisition should be attempted without the (U)SIM present. Many phones permit an acquisition under such conditions, allowing PIN entry for the (U)SIM to be bypassed, if it were enabled. If the acquisition attempt is unsuccessful, the (U)SIM can be reinserted and a second attempt made. Performing separate independent acquisitions (i.e., acquiring the (U)SIM before acquiring the contents of the handset) avoids any operating system-related forensic issues associated with an indirect read of (U)SIM data. However, removing the SIM can reportedly cause data to be deleted on some phones.

In addition, if removing the battery is required to gain access to the SIM, a loss of the date and time values can occur on certain phones. Similarly, when the battery is removed from certain smart phones the user data present in volatile memory can be lost if a second backup battery is not built-in to support battery replacement or cannot maintain volatile memory for a sufficient time.

In situations where lost data can occur, the acquisition sequence described at the beginning of this section for active phones should be followed.

(U)SIMS

Similar to a mobile phone, acquiring data from a (U)SIM requires that a connection be established from the forensic workstation to the device, using a reader. As before, the version of the tool being used should be documented, along with any applicable patches or errata from the manufacturer applied to the tool. Once the connection has been established, the forensic software tool can proceed to acquire data from the device.

Capturing a direct image of the (U)SIM data is not possible because of the protection mechanisms built into the module. Instead, forensic tools send command directives called Application Protocol Data Units (APDUs) to the (U)SIM to extract

data logically, without modification, from each elementary data file of the file system. The APDU protocol is a simple command-response exchange. Each element of the file system defined in the GSM standards has a unique numeric identifier assigned, which can be used to walk through the file system and recover data by referencing an element and performing an operation, such as reading its contents.

Because (U)SIMs are highly standardized devices, few issues exist with regard to a logical acquisition. The main consideration is selecting a tool that reports the status of any PINs and recovers the data of interest. Vast differences exist in the data recovered by (U)SIM tools, with some recovering only the data thought to have the highest relevance in a typical investigation, and others performing a complete recovery of all data, even though much of it is network related with little investigative value.

Substitute (U)SIMs

Substitute (U)SIMs, sometimes referred to as access cards, can be useful in a number of situations:

If the (U)SIM for a phone is missing or damaged and needed for acquisition with a forensic tool, a substitute (U)SIM allows phone data to be recovered.

If the (U)SIM for a phone is present, but requires a PUK code, a substitute (U)SIM allows acquisition to proceed immediately without having to contact the service provider for the PUK.

If radio isolation is needed to prohibit communications to acquire evidence from a phone, avoiding incoming calls or messages from altering or modifying evidence, a substitute (U)SIM can be used in lieu of a Faraday room or enclosure.

If the forensic tool used to examine a handset accesses the resident (U)SIM indirectly, using a substitute (U)SIM in the handset eliminates the possibility of the original being altered during examination.

The values by which the phone remembers the previously inserted (U)SIMs are the ICCID and the IMSI. Often only one of these values is used. Both identifiers are unique and used to authenticate the user to the network. If these values are known for a specific phone (e.g., either indirectly through the service provider records or

directly by reading memory from the phone), it may be possible to prepare a substitute (U)SIM with the correct values needed to trick the phone to accepting it. While the minimum data needed to create a (U)SIM may be simply one of these two values, some phones may require additional data to be populated on the (U)SIM to be correctly recognized. The possibility exists that data, other than user data, may change on the handset as the result of inserting a substitute (U)SIM.

Obstructed Devices

The phrase “obstructed devices” typically refers to devices that require successful authentication using a password or some other means to gain access. Common obstructed devices include mobile phones with missing identity modules, PIN-enabled identity modules, or an enabled phone lock setting. Password-locked memory cards are beginning to emerge as the capability to set such locks appears in more phones. Content encryption capabilities are currently not offered as a standard feature in most cell phones, but may be available through an add-on application.

A number of ways exist to recover data from obstructed devices. They fall into three classes: investigative, software-based, and hardware-based. Experimenting with a seized device to bypass or overcome its security mechanisms should be avoided and instead done with a test device of the same make, model, and version of software.

Seemingly simple actions can cause the device to lock permanently or lose data, making evidence recovery more difficult or impossible. PIN and password-protected devices may require the expertise of a specially trained forensic specialist to gain access to the device contents in a forensically sound manner, once conventional techniques have been exhausted. Preserving the contents of the device when conventional techniques are applied is vital to allow more sophisticated techniques to succeed.

Software and hardware-based methods are often directed at a particular device or narrow class of device, as are some investigative methods. In developing a method, the following actions should be considered for determining possible approaches:

 Contacting the device manufacturer and service provider for information on known backdoors and vulnerabilities that might be exploited.

Reviewing manufacturer specifications and other documentation when formulating plausible approaches.

Contacting commercial evidence recovery professionals that specialize in handheld devices.

Searching Internet sites for exploit information.

Contacting device maintenance and repair companies, as well as commercial organizations that provide architecture information on handheld devices.

4.9 DATA ANALYSIS

Because of the prevalence of proprietary case file formats, the forensic toolkit used for acquisition will typically be the one used for examination and analysis.

Interoperability among the acquisition and examination facilities of different tools is also unlikely for this reason, with the exception of certain Palm OS devices and perhaps other devices with a PDA lineage.

The examiner should have studied the case, if possible, and become familiar with the parameters of the wrongdoing, the parties involved, and potential evidence that might be found. Conducting the examination in a partnership with the investigator guiding the case construction is advisable for the examiner. The investigator provides insight into the types of things sought, while the examiner provides the means to find relevant information that might be on the system.

Prepared with the background of the incident, the forensic examiner can proceed toward accomplishing the following objectives:

Gather information about the individual(s) involved {who}.

Determine the exact nature of the events that occurred {what}.

Construct a timeline of events {when}.

Uncover information that explains the motivation for the offense {why}.

Discover what tools or exploits were used {how}.

The table below provides a cross reference of evidence sources commonly found on mobile phones and their likely contribution toward satisfying the above objectives.

	Who	What	Where	When	Why	How
Subscriber/Device Identifiers	X					
Call Logs	X			X		
Phonebook	X					
Calendar	X	X	X	X	X	X
Messages	X	X	X	X	X	X
Location			X	X		
Web URLs/Content	X	X	X	X	X	X
Images/Video	X	X	X	X		X
Other File Content	X	X	X	X	X	X

4.10 APPLYING TOOLS

To uncover evidence, specialists should gain a background of the suspect and offense and determine a set of terms for the examination. Search expressions can be developed in a systematic fashion, such as using contact names that may be relevant. By proceeding systematically, the specialist creates a profile for potential leads that may unveil valuable findings.

Analysis of extracted data may include:

Determination of ownership and possession – Identify the individuals who created, modified, or accessed a file, and the ownership and possession of questioned data by placing the subject with the device at a particular time and date, locating files of interest in non-default locations, recovering passwords that indicate possession or ownership, and identifying contents of files that are specific to a user.

Times and Locations - GPS locations and /or Cell Tower hits may indicate where the phone was at a given time.

Application and file analysis – Identify information relevant to the investigation by examining file content, correlating files to installed applications, identifying relationships between files (e.g., e-mail files to e-mail attachments), determining the significance of unknown file types, examining system configuration settings, and examining file metadata (e.g., documents containing authorship identification).

Timeframe analysis – Determine when events occurred on the system to associate usage with an individual by reviewing any logs present and the date/time stamps in the file system, such as the last modified time. Besides call logs, the date/time and content of messages and e-mail can prove useful.

Data hiding analysis – Detect and recover hidden data that may indicate knowledge, ownership, or intent by correlating file headers to file extensions to show intentional obfuscation; gaining access to password-protected, encrypted, and compressed files; gaining access to steganographic information detected in images; and gaining access to reserved areas of data storage outside the normal file system.

5. TOOL-SPECIFIC PROCEDURES

5.1 TOOL SELECTION

Once the make and model of the phone are known, available manuals can be retrieved and studied. Additional information regarding the phone's model can be retrieved through the manufacture's web site.

An Internet search of the model number can also reveal a significant amount of information about the device. The device being acquired largely dictates the choice of forensic tools. The following criteria should be considered when a choice of tools is available.

Usability – the ability to present data in a form that is useful to an investigator

Comprehensiveness – the ability to present all data to an investigator so that both inculpatory and exculpatory evidence can be identified

Reliability – the ability for the tool to produce the same output when given the same set of instructions and input data

Verifiability – the ability to ensure accuracy of the output

Quality – technical support, reliability, and upgrade version path

Capability – supported feature set, performance, and richness of features with regard to flexibility and customization

Affordability – cost versus benefits in productivity

5.1.1 Depth of Examination

If the case being examined is a Crime Against Person (homicide, assault, threat, etc.), all available levels of examination will be performed (Physical, Logical (Full Read), Logical (No Files), etc.).

Other case types (burglary, narcotics, etc.) will be examined by using only the highest-level examination for each tool (Logical being the lowest-level and Physical being the highest-level).

5.2 XRY

Before Starting an Extraction

If possible, turn on Airplane Mode (to isolate the phone from the Network) and turn off the passcode/password/PIN (this will allow for subsequent extraction). Also, for Android devices, turn on USB Debugging.

Starting XRY

Ensure the USB key is plugged in as you will not be able to perform an extraction without a valid license.

Double-click on the blue XRY icon.



In the upper left corner of the XRY window, select the **Extract Data** option to open the wizard.

From the XRY Extraction Wizard screen, click the Device Finder Icon.



In Device Finder, click on the boxes for Device Type, Manufacturer, Form Factor, and OS and select the item appropriate for the device you're extracting. Only select items that you're sure of. For example, if you know the phone manufacturer is Motorola, select Manufacturer, then select Motorola. If you aren't sure of the Operating System, do not select the OS box.

Once you have made your selections, look at the images of the devices presented and attempt to find the one you're attempting to extract. If you find it, click on it and continue with the extraction. If your device is not listed, but a similar one is, click on that device and attempt the extraction.

Once you've selected a device, XRY will present a page with information about the device, (including which cable should be used to connect it to the computer), as well as specific instructions about what should be done prior to beginning the extraction

ARCHIVED

SIM Card Extraction

Insert the SIM card into a SIM card/USB adapter. Insert the adapter into an available USB port.

Click "Find Devices and Apps" in the XRY Main Screen.

In the Search Box, type "SIM Card".

Select "SIM Card" from the device list.

Click "Continue"

Select "Logical (Full Read)" or "Logical (No Files)".

Select the appropriate device connection.

Select where to save the file along with the filename.

Click "OK".

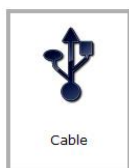
When the extraction is finished, click "Continue".

Logical Extraction

Begin a logical extraction by connecting the device to the computer, using the recommended cable. Connect the device to the computer using the recommended cable. If the device does not turn on automatically, turn it on manually. Then click on **Logical (No Files)**, **Logical (Full Read)**, or **Physical**.



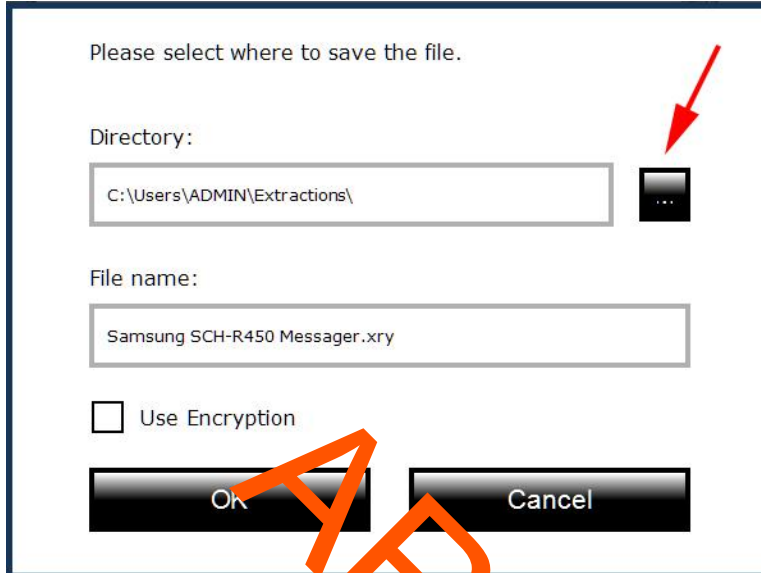
Click on **Cable**.



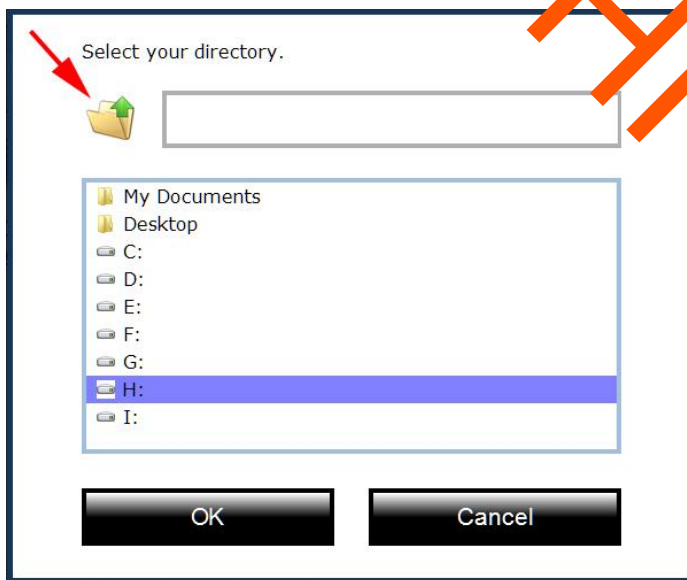
Click on the device you wish to examine.

Select the connection method that most closely matches your device.

The Save File screen will appear. Click the black box with three dots.



Click the folder icon until you see the drive indicating your flash drive.



Select the flash drive as the location you want the extraction to be saved. Then click **OK**.

You can accept the filename recommended by XRY or change it. Either way, remember or write down the file name. Then click **OK**.

XRY will then begin **Processing** the device and querying it for information.

When the **Device Extraction** has finished, click **Continue**.

Select **Finish**.

Select **Close Wizard**.

Eject the flash drive and remove it from the computer.

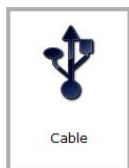
Physical Extraction

Begin a physical extraction by clicking on **Physical**.



If any special instructions are given, follow them and click on OK.

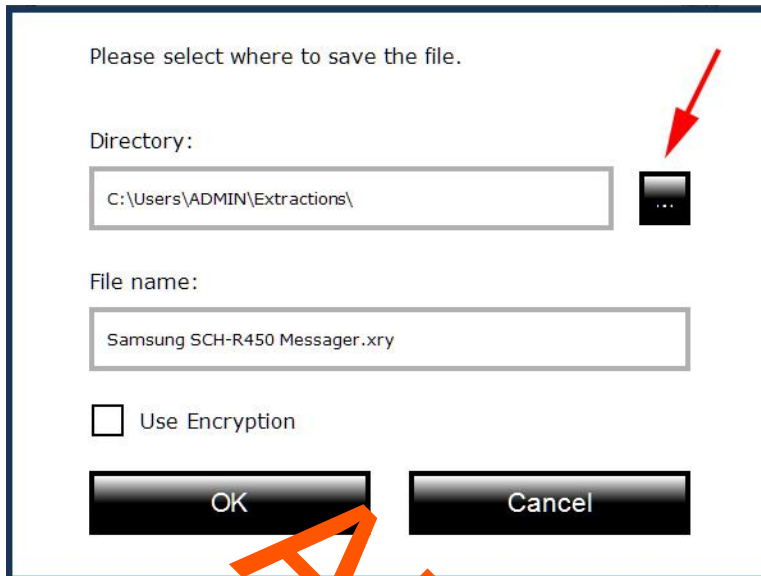
If given the option, click on Cable.



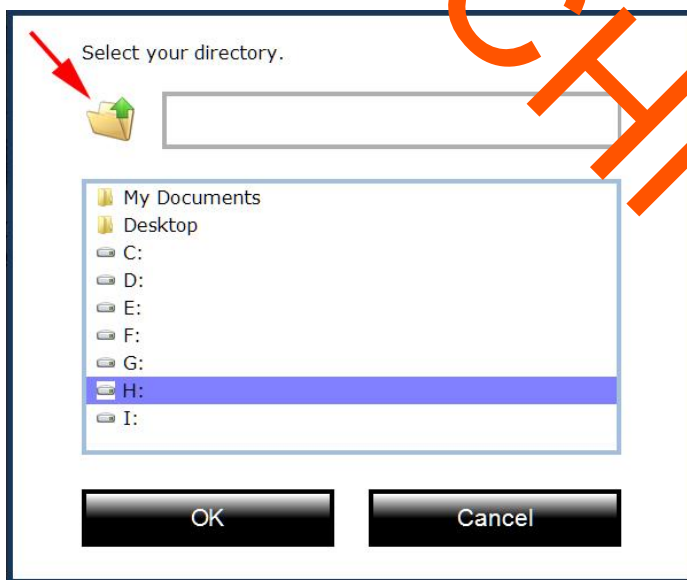
Click on the device you wish to examine.

If given the option, select the connection method that most closely matches your device.

The Save File screen will appear. Click the black box with three dots.



Click the folder icon until you see the drive indicating the flash drive.



Select the flash drive as the location you want the extraction to be saved. Then click **OK**.

You can accept the filename recommended by XRY or change it. Either way, remember or write down the file name. Then click **OK**.

XRY will then begin **Processing** the device and querying it for information.

When the **Device Extraction** has finished, click **Continue**.

Select **Finish**.

Select **Close Wizard**.

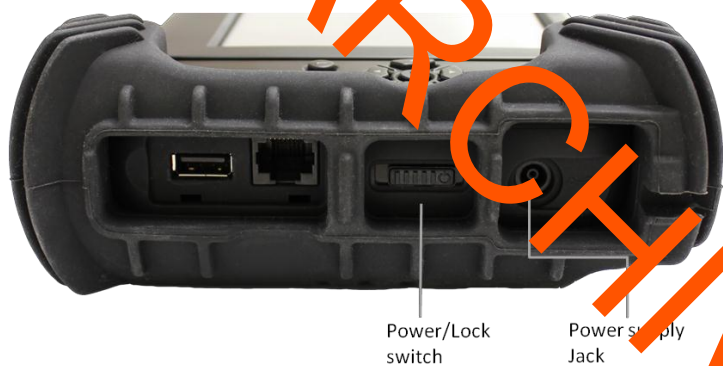
Eject the flash drive and remove it from the computer.

ARCHIVED

5.3 Cellebrite UFED Touch

Turning the UFED Touch Unit On or Off

The On/Off switch of the UFED Touch unit is located in the right (Target) panel.



Device Right Panel – On/Off Switch

To turn the UFED Touch on:

Push the power switch right to the On position.

The LED Power indicator will light up and the startup sequence will initiate.



Power Indicator

To turn UFED Touch off:

NOTE: Turning UFED Touch off is just like the standard procedure of turning a Windows based computer off.

Close the UFED Touch application

In Desktop, Select Start > Turn Off Computer > Turn Off

To perform an immediate shut down, pull the Power switch all the way to the left and hold it until the device shuts down

Starting the UFED Touch Application

Application Startup

After turning the UFED Touch unit on, the UFED Touch application will launch automatically. If the application doesn't launch automatically or if you quit the application, use one of the following methods to launch it:



Tap the UFED Touch application shortcut icon located in the UFED shortcut panel at the right of the screen.



Double tap the UFED Touch application icon on the Desktop.

Welcome Screen

Please select your method of extraction:



SIM Card Extraction

Insert the SIM card into the SIM card adapter, and Insert the adapter into the slot in the front of the UFED Touch.

Click "Extract from SIM card" on the UFED Touch Main Screen.

Select the appropriate SIM card type from the list.

Select the appropriate type of extraction.

Select the extraction location.

Select the content you wish to extract

Click "Next".

Click "Continue".

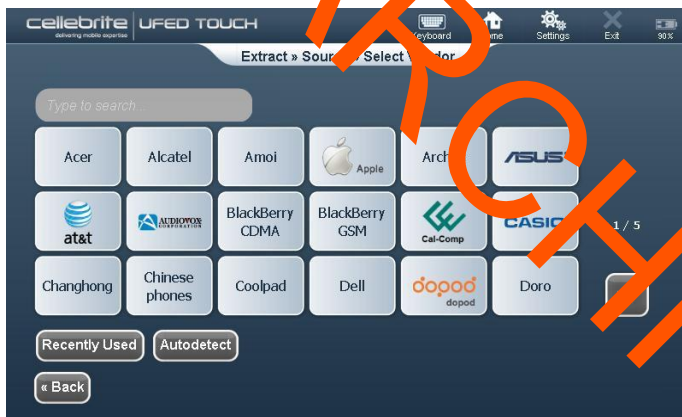
When the extraction has completed, click "Finished".

Logical or File System Extraction

Note: Before beginning an extraction, be sure you have either an empty flash drive on which to save the data or a cable to attach the UFED Touch to a computer.

Select Vendor and Model

There are multiple ways in which the vendor and device model can be selected. This guide will describe how to select a device using the Search Function (see next page) and the Vendor List (see pg 44).



Select Vendor Screen

Search Function

To search for the source mobile device:

In the "Select Vendor" screen, activate the device keyboard by tapping the *keyboard* icon in the Application Taskbar



Start typing the vendor's name. The list of vendors will be narrowed down to meet your criteria.

The typed letters will appear in the Search field




Select Vendor Search Results Screen

The relevant vendors will appear on the screen. In this example "Sa" was the typed search criteria and the Vendors that matched the criteria were displayed accordingly.

Select the vendor, and the "Select Model" screen will open



Select Model Screen

In the "Select Model" screen, activate the device keyboard by tapping the *keyboard*  icon in the top toolbar

Type the letters of the model in the keyboard. These letters will appear in the search field. The various options will appear on the screen


Choose the device model from the list.

The "Select Phone Memory" screen will open (see next page).

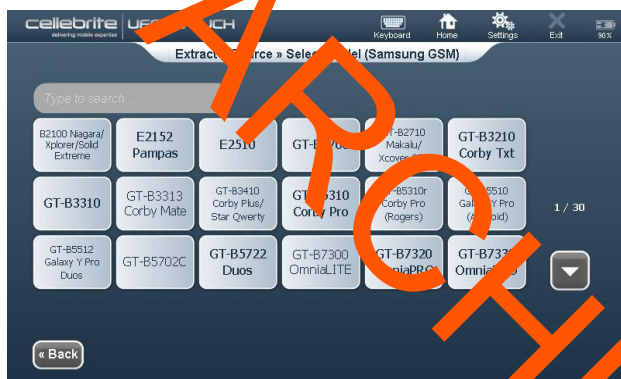
Select the Source Device from the Vendor List

To select the mobile device's model:

Choose the vendor from one of the vendor icons displayed in the "Select Vendor List" screen


Use the *Down* arrow  to view additional vendors. If the vendor type is known, it is recommended to use the Search function.

The "Select Model" screen will open. In this example a Samsung GSM vendor has been selected.



Select Model Screen

Choose the device's model type from the list.

Use the *Down* arrow  to view additional models. If you know which type of mobile device you are looking for, it is recommended you use the Search function.

The "*Select Phone Memory*" screen will open.

Select Phone Memory

Note: Where only a single memory is available the "Select Phone Memory" screen will not be displayed.

Information can be extracted from a mobile device's memory, memory cards and SIM memory. All memories can be selected or only one. The types of memories can vary between devices.

To select the mobile device's memory:



Select Phone Memory Screen

The Phone memory selection box is selected by default. It can be deselected

Select the other memories if required

Tap *Next* to continue. The "*Connect Mobile Device*" screen opens.

Connect Mobile Device

NOTE: Where only a single connection option is available, the Connect Mobile Device screen will not be displayed.

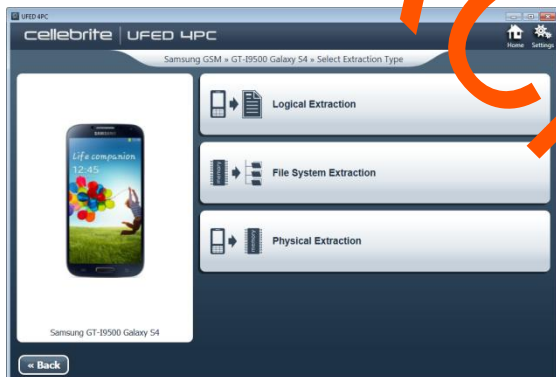
To connect the mobile device:



Connect Mobile Device Screen

Select "USB Cable" from the options shown.

The Select Extraction Type screen will appear.



Select the type of extraction you wish to perform.

The Select Extraction Location screen will appear.

Select Extraction Location



Device Extract Location Screen

In the "Select Extract Location" screen, choose *Removable Drive* to extract the device data to a USB drive connected to the UFED Touch TARGET USB port (on the right panel).

At the end of the data extraction process, the extracted data will be saved in the location you select.

The extracted data folder will be named "UFED" with the selected device name, the IMEI/MEID info. and the extraction date. For example, "UFED Nokia GSM 3720 fol_356935030349119 2011_06_11 (001)"

The extracted data folder contains:

- Multimedia files folders named Audio, Images, Ringtones, and Video folders, containing each of the respective type of media files.

- Phone extraction report files in HTML and XML formats.

- UFED Manager files of the extracted calls log (*.clog), phonebook (*.pbb), SMS messages (*.sms), calendar (*.cal), Email (*.Email), MMS(*.MMS), and IM(*.IM) data.

- HTML contents files for the phonebook and SMS messages data.


- UFD file.


NOTE: UFED Manager files will be generated only for data types that contain items.

The Select Content Types screen will appear.

Select Content Types

If you are performing a Logical extraction, the Select Content Types screen will appear. Multiple content types are listed. The types are displayed in three different ways:

Types selected by default – shown with a check mark 

Types available for selection – shown with no check marks 

Types not available – shown with a cross 



Select Content Types Screen

To select content types:

Select the additional content types required to be included in the information extracted from this device.

You can tap Select All to select all the available types.

Tap Next to continue. The "Waiting for Device" screen will open (see next page).

NOTE: The Target window differs depending on the option selected in the "Select Extraction Location" screen

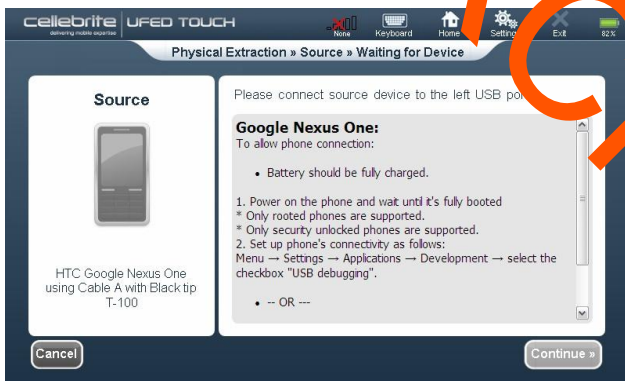
Waiting for Device

The application requires that the device is connected in order to continue. Connect the device to the UFED Touch using the recommended cable. If the device does not turn on automatically, turn it on manually. The "Waiting for Removable Drive" screen will open.

This screen is divided into 2 sections:

Left source side bar - The cable required to connect the device to the source port is listed here


Mobile device settings – Instructions on how to change the settings in the mobile device.



Waiting for Device Screen

Locate the correct cable and tip for the mobile device in your tips and cables kit, based on the information written in the "Source" section of the screen

Change the device settings according to the instructions on the screen

Connect the mobile device to UFED Touch. A red source arrow  will continue flashing on the left of the screen until the device is connected.

If relevant, follow the displayed instructions to enable USB connection to the source device

Tap Continue. The "Waiting for Removable Drive" screen will open.

Waiting for Removable Drive



This screen is divided into 2 sections:

A left side bar – Instructions on where to connect the removable drive

Target – an alert to insert removable drive



Waiting for Removable Drive Screen

Connect the removable storage device to the UFED Touch. A red target arrow  will continue flashing on the right of the screen and a red SD card arrow  will continue flashing at the top of the screen until the removable storage device is connected.

In the event that the removable storage device is full, damaged or write protected an error message will appear.



Error message

If an error occurs:

Replace the removable storage

Tap Continue. The "Extraction in Progress" screen will appear.

Extraction in Progress



Extraction in Progress Screen

If the Multimedia Selection screen opens, make sure there is a check mark next to the types of media you wish to extract, remembering that the more media to be downloaded, the longer the extraction will take.

When the extraction is complete and if required, the "Source Instructions" screen will appear.



Source Instructions Screen

Follow the instructions to return the mobile device settings to the correct settings, and then tap Continue.

When the "Phone Extraction Summary" screen opens, tap OK to complete the extraction.

Eject your flash drive and remove it from the computer.

Physical Extraction

Performing a Physical Extraction

Note: Before beginning an extraction, be sure you have an empty flash drive on which to save the data.

Select Vendor and Model

There are multiple ways in which the vendor and device model can be selected. This guide will describe how to select a device using the Search Function and the Vendor List (see pg 55).



Select Vendor Screen

Search Function

To search for the source mobile device:

In the "Select Vendor" screen, activate the device keyboard by tapping the *keyboard* icon in the Application Taskbar



Start typing the vendor's name. The list of vendors will be narrowed down to meet your criteria.

The typed letters will appear in the Search field




Select Vendor Search Results Screen

The relevant options will appear on the screen. In this example "Sa" was the typed search criteria and the Vendors that matched the criteria were displayed accordingly.

Select the vendor and the "Select Model" screen will open



Select Model Screen

In the "Select Model" screen, activate the device keyboard by tapping the *keyboard*  icon in the top toolbar

Type the letters of the model in the keyboard. These letters will appear in the search field. The various options will appear on the screen


Choose the device model from the list.

The "Select Phone Memory" screen will open (see next page).

Select the Source Device from the Vendor List

To select the mobile device's model:

Choose the vendor from one of the vendor icons displayed in the "Select Vendor List" screen


Use the *Down* arrow  to view additional vendors. If the vendor type is known, it is recommended to use the Search function.

The "Select Model" screen will open. In this example a Samsung GSM vendor has been selected.



Select Model Screen

Choose the device's model type from the list.

Use the *Down* arrow  to view additional models. If you know which type of mobile device you are looking for, it is recommended you use the Search function.

The "Select Phone Memory" screen will open.

Select Phone Memory

Note: Where only a single memory is available the "Select Phone Memory" screen will not be displayed.

Information can be extracted from a mobile device's memory, memory cards and SIM memory. All memories can be selected or only one. The types of memories can vary between devices.

To select the mobile device's memory:



Select Phone Memory Screen

The Phone memory selection box is selected by default. It can be deselected

Select the other memories if required

Tap *Next* to continue. The "*Connect Mobile Device*" screen opens.

Connect Mobile Device

NOTE: Where only a single connection option is available, the Connect Mobile Device screen will not be displayed.

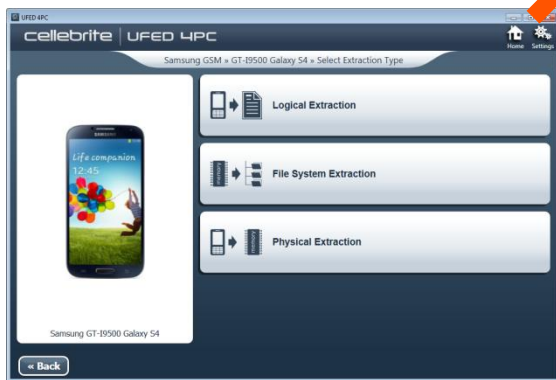
To connect the mobile device:



Connect Mobile Device Screen

Select "USB Cable" from the options shown.

The Select Extraction Type screen will appear.



Select the type of extraction you wish to perform.

The Select Extraction Location screen will appear.

Select Extraction Location



Device Extract Location Screen

In the "Select Extract Location" screen, choose *Removable Drive* to extract the device data to a USB drive connected to the UFED Touch TARGET USB port (on the right panel) or SD card inserted to the SD card reader (on the back panel)

At the end of the data extraction process, the extracted data will be saved in the location you selected previously.

The extracted data folder will be named "UFED" with the selected device name, the IMEI/MEID info. and the extraction date. For example, "UFED Nokia GSM 3710 and 3569? 03 0349119 2011_06_11 (001)"

The extracted data folder contains:

- Multimedia files folders named Audio, Images, Ringtones, and Video folders, containing each of the respective type of media files.

- Phone extraction report files in HTML and XML formats.

- UFED Manager files of the extracted calls log (*.clog), phonebook (*.pbb), SMS messages (*.sms), calendar (*.cal), Email (*.Email), MMS(*.MMS), and IM(*.IM) data.

- HTML contents files for the phonebook and SMS messages data.


- UFD file.


NOTE: UFED Manager files will be generated only for data types that contain items.

The Select Content Types screen will appear.

Select Content Types

If you are performing a Logical extraction, the Select Content Types screen will appear. Multiple content types are listed. The types are displayed in three different ways:

Types selected by default – shown with a check mark 

Types available for selection – shown with no check marks 

Types not available – shown with a cross 



Select Content Types Screen

To select content types:

Select the additional content types required to be included in the information extracted from this device.

You can tap Select All to select all the available types.

Tap Next to continue. The "Waiting for Device" screen will open (see next page).

NOTE: The Target window differs depending on the option selected in the "Select Extraction Location" screen

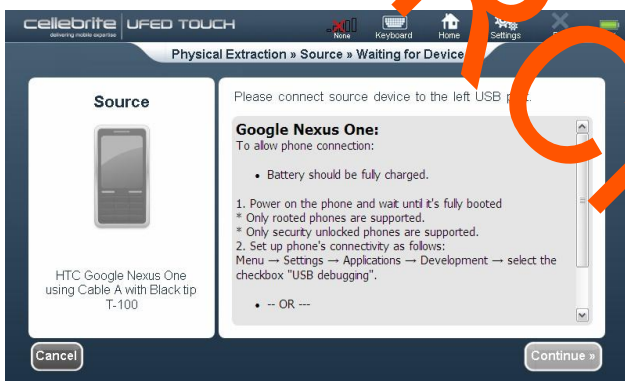
Waiting for Device

The application requires that the device is connected in order to continue. In the event that the device was connected at the start of the process the "Waiting for Removable Drive" screen will open.

This screen is divided into 2 sections:

Left source side bar - The cable required to connect the device to the source port is listed here


Mobile device settings - instructions on how to change the settings in the mobile device.



Waiting for Device Screen

Locate the correct cable and tip for the mobile device in your tips and cables kit based on the information written in the "Source" section of the screen

Change the device settings according to the instructions on the screen

Connect the mobile device to UFED Touch. A red source arrow  will continue flashing on the left of the screen until the device is connected.

If relevant, follow the displayed instructions to enable USB connection to the source device

Tap Continue. The "Waiting for Removable Drive" screen will open.

Waiting for Removable Drive

This screen is divided into 2 sections:

A left side bar – Instructions on where to connect the removable drive

Target – an alert to insert removable drive



Waiting for Removable Drive Screen

Connect the removable storage device to the UFED Touch. A red target arrow will continue flashing on the right of the screen and a red SD card arrow will continue flashing at the top of the screen until the removable storage device is connected.

In the event that the removable storage device is full, damaged or write protected an error message will appear.



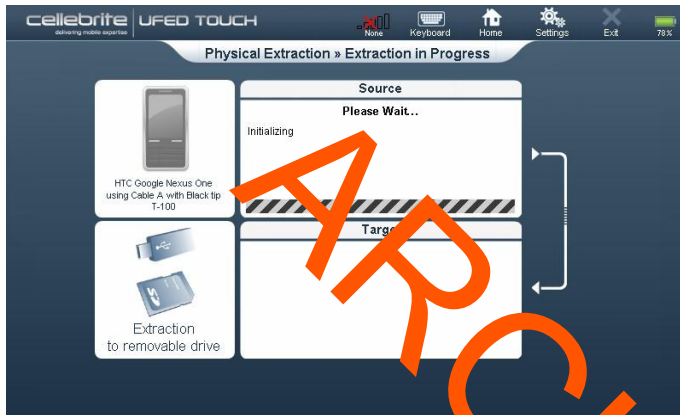
Error message

If an error occurs:

Replace the removable storage

Tap Continue. The "Extraction in Progress" screen will appear.

Extraction in Progress



Extraction in Progress Screen

Note that the extraction may take anywhere from a few minutes to a few hours. Once the extraction has begun, it cannot be aborted.

If the Multimedia Selection screen opens, make sure there is a checkmark next to the types of media you wish to extract, remembering that the more media to be downloaded, the longer the extraction will take.

When the extraction is complete and if required, the "Source Instructions" screen appears (depending on the device's model)



Source Instructions Screen

Follow the instructions to return the mobile device settings to the correct settings, and then tap Continue.

When the "Phone Extraction Summary" screen opens, tap OK to complete the extraction, then remove your flash drive from the UFED Touch.

Cloning a (U)SIM card

Cloning a SIM card consists of copying the IMSI and ICCID from an evidence phone's SIM card to a blank SIM card.

Cloning a SIM card may be done for any of three reasons:

The need to isolate a phone from the network

If your evidence phone is missing a SIM card

If your evidence phone has a PIN-locked SIM

Warning – apps exist that will lock a phone when a new SIM is detected.

The following procedure can be used to extract data from a phone while it is isolated from the network:

Note: a write-blocking device should be used, if available.

Read the SIM card with XRY

Clone the SIM card

Insert cloned SIM card into evidence phone

Power on phone and extract data with XRY

ARCHIVED

5.4 Katana Lantern

Note: Katana Lantern is currently only authorized for extraction of Apple devices. Android devices are not to be extracted using the Lantern software.

Open the Lantern program.

Name the project in the Save As box.

Select the location to save the project.

Fill out identifying information, as appropriate.

Click "Save".

Performing an Extraction

Attach a device to the computer, using the appropriate cable.

Click the "Acquire" button.

Select the appropriate "Source".

Select "iOS".

Click "Acquire"

When the extraction is complete, the extracted data will be saved to the location previously specified.

6. CASE FILE DOCUMENTATION

6.1 GENERAL

Follow the note-taking policy and general report format as detailed in the laboratory's quality assurance policies.

In addition to lab-wide reporting requirements, a mobile device examination report will include the following information, as appropriate:

The equipment and set up used in the examination

Brief description of steps taken during examination, such as string searches, graphics image searches, and recovering erased files.

Supporting materials such as printouts of particular items of evidence, digital copies of evidence, and chain of custody documentation

Details of findings:

Specific files related to the request

Other files, including deleted files, that support the findings

String searches, keyword searches, and text string searches

Internet-related evidence, such as Web site traffic analysis, chat logs, cache files, e-mail, and news group activity

Graphic image analysis

Indicators of ownership, which could include program registration data

Data analysis

Description of relevant programs on the examined items

Techniques used to hide or mask data, such as encryption, steganography, hidden attributes, hidden partitions, and file name anomalies

Requests to the investigator for information pursuant to a search warrant such as decryption of data that is not recoverable with current tools employed by the unit.

As appropriate, a note will be included in each report which reads as follows:

NOTE: Where possible, all evidence mobile devices are disconnected from the network when returned. Enabling network connection on these devices may result in loss of all currently stored data.

6.2 EXTRACTED DATA MANAGEMENT

The extracted data will be placed on an appropriate medium (cd/dvd/blue-ray/flash drive/hard drive). One copy will be kept as the master and impounded in Property with its own barcode. This copy will be labeled, "SDPD Crime Lab – Master Copy" and will include the case number. Two copies will normally be prepared for release to the investigator. These copies will be labeled, "SDPD Crime Lab – Release Copy" and will include the case number. One copy is intended to be sent to the DDA on the case.

The master copy will have all extracted data files and any partial or empty folders accumulated during the extraction process. The copies created for release will have only the readable datafile(s). The master copy will be provided to the DDA as part of any discovery request.

The data on the master copy will also be maintained on unit hard drives.

7. QUALITY ASSURANCE

7.1 GENERAL

Quality control measures will be applied when first choosing a forensic data extraction tool to ensure its acceptability, reapplied either on a regular basis or when updates or new versions of the tool become available to uphold consistency, or when equipment repairs become necessary.

Examiners will have received adequate up-to-date training in the tools and procedures to employ, and have been successfully competency tested as a quality measure.

A collection of reference devices will be maintained to assist with validations, performance checks, and to evaluate specific device functions. Ideally, the collection should contain a representative example of devices the lab may encounter in casework.

7.2 VALIDATION

Any new method must be validated per Quality Assurance policy 2.1.

7.3 REFERENCE DEVICE

A reference device is a device (i.e. a cellular phone, a floppy disk, hard drive, a SD card, etc.) which has been examined prior to use with casework, and its contents are known.

When held within the laboratory, the reference device must be powered off when in storage and labeled with a unique reference number.

If any changes are made to reference devices, a notation will be put in the maintenance binders wherein reference device information is documented.

Reference Device Log

A log will be maintained of the reference device collection which will, at a minimum, document the following:

Type of device

A unique reference number.

Manufacturer, model, serial number and/or unique manufacturer numbers.

7.4 EQUIPMENT UPDATES

Software and equipment manufacturers update their products periodically. In order to maintain the most current updates and upgrades, annual or bi-annual renewal of service fees may be required by manufacturers.

Without the most current update product probative data may not be found on some devices at time of processing.

Retention of Updates and Upgrades

The current software version of the equipment and firmware, when possible, must be archived.

Old versions of the software are maintained in the laboratory in order to reproduce an extraction which was previously conducted using the same capabilities as when originally examined.

Performance Check after an Update or Maintenance

A performance check of equipment using reference devices will be conducted after any maintenance is performed.

A new tool that is being installed to replace a defective tool will be performance checked prior to its first use on casework. This is for new tools being used with an established method.

An entry will be made in the maintenance log with the date of the performance check and the initials of the examiner who performed the check.

Performance checks will be conducted on laboratory equipment once an update is installed. If the update is proven to be operational, it will be rolled out to the field units without a performance check. If a problem is encountered during an update installation, a performance check may be required.

Performance Check Using Designated Control Device

Performance checks using a control device (a specific reference device with installed known data to be used in performance checks) will involve an acquisition in which the equipment or technique can retrieve data which has been placed on the device specifically for validation/performance check purposes. Generated data files will be compared to the reference data files.

Performance Checking Write Blockers

The following applies to all performance checks of write blockers:

A write blocker will be performance checked each day it is going to be used.

Note: If the write blocker is attached and continually extracting data into the next day, it does not require a performance check for the new day.

The results of the performance check will be maintained in a write blocker log. The log will document, at minimum, the following:

Date

Write blocker used

Adapter used (if any)

Reference device used

Status of performance check

Laboratory case number

Examiner initials.

If a write blocker fails to block the transmission of data it may not be used for case

work. The supervisor and staff will be immediately notified. The write blocker will be removed from service until the failure is resolved. Documentation of repairs or removal from service will be maintained in the maintenance binder.

Failed Performance Check

If any tool fails a performance check, no analytical work will be conducted with that tool until the source of the problem has been determined and corrected.

The tool will be marked as “Out of Service.”

The unit supervisor and staff will be notified of the failed performance check as soon as possible.

All documentation will be retained in the maintenance binder for the tool. Once corrected, another performance check on the tool will be conducted to verify that it is performing as expected.

Documentation

All performance checks and any relevant comments will be logged in the spreadsheet created for tracking purposes.

7.5 REUSE OF DIGITAL MEDIA

Whenever media is to be reused (e.g., a USB drive for an extraction with the UFED Touch), steps must be taken to insure that there is no pre-existing data on the media. Previously used media will be reformatted before use.

7.6 MEDIA RECEIVED FROM AN OUTSIDE PARTY

If an outside party provides media that is intended to be used to store data and will be returned to an outside party (e.g. discovery request, business records request, etc.), that media will be reformatted before use.

7.7 POWER ON SELF TEST (POST) FOR CASEWORK DEDICATED COMPUTER

A successful Power-On-Self-Test (POST) followed by a successful boot sequence of the currently installed computer operating system will be considered as proper calibration of a casework-dedicated computer. Any casework dedicated computer that fails this sequence will be repaired prior to its use in any examination.

The assigned examiner will indicate the following in their case notes: the identifying name or number of the examination computer and operating system that was used, along with the results of this test

Note: This information should be recorded for each boot sequence executed during the processing of a case

7.8 UNCERTAINTY OF MEASUREMENT

Digital evidence examination is a qualitative method and measurements noted are descriptive in nature; therefore, uncertainty of measurement does not apply.