SAN DIEGO POLICE DEPARTMENT
FORENSIC SCIENCE SECTION

Forensic Technology Unit Manual

1. UNIT DESCRIPTION

Office hours are based on an alternative work schedule and generally run from 0600 to 1630 hours. Staffing consists of three full time and 1 part-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. Ensuring 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 or unit supervisor 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 for 4th waivers need not be attached.

2.2 CASE ASSIGNMENT

Incoming cases are generally prioritized with the highest priority on cases involving a threat, then cases with a court date, homicides, and finally by the date of receipt. The supervisor may adjust priority levels at any time based on the circumstances of the case.

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. Multiple cases may be worked simultaneously; it is the responsibility of the examiner to maintain proper management of the evidence and documentation.

2.3 CASE TRACKING

All requests are logged into the laboratory computer database either by the Clerical Unit or the unit supervisor. 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 data such as, but not limited to, 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.

Currently there is no available method that will capture or parse all electronically stored information from all mobile devices. Manual preservation (photography, video recording and/or transcription) may be necessary to document the information observed on the mobile device's display.

An audit trail must be accurately document each investigative step in order to allow replication of the results by an independent third-party. In order to prevent unauthorized access to unit computer systems and networks, computer systems will employ unit-confidential password protection.

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 investigator 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 will notify the submitting investigator 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 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

4.4 DEVICE IDENTIFICATION

When possible, record the manufacturer, model, and identifiers (e.g. IMEI, MEID) of the submitted equipment, and also its condition.

4.5 ISOLATING THE PHONE

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

4.6 EXAMINATION PROCEDURE

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

Attempt to prohibit the transmission/reception of data as soon as practical (e.g. Faraday fabric, metal “Arson evidence” container, placing device 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.

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 it 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.

Check for passwords and consider disabling it if possible.

If it is not possible to prohibit the transmission/reception of data to the device, turn the device off.

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 the 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.

Perform examination of the mobile device as soon as possible.

Note: Some devices may require constant power from the battery to maintain volatile memory.

In most cases, if SIM or SD cards are in the device when it is received, the device will be processed as received. At the discretion of the examiner, the SD or SIM cards may be extracted separately from the device.

A write blocker must be used when extracting data from removable storage media independent of the mobile device.

In most instances, the examiner will perform the highest level extraction available for a device and supplement it with a Logical Extraction. As each case is different, extractions performed will depend on the type of device and the specifics of the case.

Mobile devices submitted to the laboratory for latent print processing or DNA analysis will be first routed to the Forensic Technology Unit, where an attempt will be made to extract data identifying the user of the device. FTU examiners will take precautions to ensure that the evidence is not contaminated. If extracted, the device user's name/email address/telephone number will be released to the requesting investigator and a Master Disk of extracted data will be impounded in the Property Room.

4.7 DATA ANALYSIS

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 analyst provides the means to find relevant information that might be on the system. A word list or keywords provided by the investigator / analyst may be used to search the data set.

5. CASE FILE DOCUMENTATION

5.1 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.

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

Details of findings:

> Specific data related to the request
>
> Other data that support the findings
>
> String searches, keyword searches, and text string searches
>
> Indicators of ownership, which could include program registration data
>
> 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, the following (or similar) wording will be included in each report:

> 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.

> Pursuant to the California Electronic Communications Privacy Act (ECPA) under Penal Code Section 1546.1(d), it is the investigating officer's responsibility to seal any portion of that data set which is found to be unrelated to the objective of the warrant, such that it is not subject to further review, use, or disclosure without a court order.

A selection of commonly used acronyms and abbreviations are defined within Appendix A of this document.

5.2 EXTRACTED DATA MANAGEMENT

The extracted data will be placed on an appropriate medium (CD/DVD/Blu-ray/flash drive/hard drive). One set will be kept as the master and impounded in the Property Room with its own barcode. Unless otherwise requested, one set will be released to the investigator for their final review.

The master disk will have all of the extracted data files, including any partial or empty folders accumulated during the extraction process, as well as the data released to the investigator. The copies created for release will have only the readable data file(s). A copy of the master disk will be provided to the DDA as part of any discovery request.

The data on the master disk may also be maintained on unit hard drives.

6. EQUIPMENT

Extraction Tools

Cellebrite UFED Touch

Cellebrite UFED Physical Analyzer

MSAB XRY Complete

Data Release

Rimage Evidence Disc System 5410N Professional (for burning and copying disks)

Data Transfer Verification

Hashing software (ensures data has been copied correctly)

Data copy software with hash algorithm verification

UFED Touch and XRY devices are distributed in various units of the department. The only ones included in the laboratory program are the ones listed in the FTU spreadsheet showing instrument tracking or control numbers and locations.

7. QUALITY ASSURANCE

7.1 GENERAL

The reliability and performance of the equipment used in the examination of digital evidence is checked to ensure the equipment is operating properly.

It is expected that the examiners will report any anomalous performance of the equipment immediately to the Unit Supervisor.

7.2 VALIDATION

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

Licensed software is generally regarded as reliable by merit of the testing and validation conducted by the developer, as well as by the widespread use in the digital forensic community, however, additional internal verification may be required.

7.3 PERFORMANCE CHECK (CONTROL) DEVICES

Performance Check Devices are devices (e.g., a phone or an SD card) which have been examined prior to use with casework, the contents of which are known. These devices are used when doing performance checks of new or updated software and hardware.

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

7.4 REFERENCE DEVICES

Reference Devices are devices (e.g., phones, tablets, etc.) which are used for testing, training, or parts.

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.

7.5 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.

Updates will be applied first to the tools/devices in use in the laboratory. The newly updated tools will then be performance checked. If the performance checks prove successful, the updates will be rolled out to the other laboratory-controlled devices distributed throughout the department. No performance checks will be required on department equipment outside the laboratory unless maintenance has to be performed or the equipment is replaced with a new device.

7.6 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.

7.7 PERFORMANCE CHECK AFTER AN UPDATE OR MAINTENANCE

A performance check of equipment using the control devices will be conducted after the installation of an update or if any maintenance is performed.

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

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. Acquired data files will be compared to the control device data files.

An entry will be made in the maintenance log for the updated equipment with the details of the update or maintenance, along with the date of the performance check and the initials of the operator/analyst who performed the check.

If a performance check fails, a previous version of the tool may continue to be used until a compatible version upgrade is available. The supervisor and staff will be immediately notified.

7.8 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 recorded in the notes for the current case.

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 log.

7.9 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 log for the tool. Once corrected, another performance check on the tool will be conducted to verify that it is performing as expected.

7.10 INTEGRITY OF TRANSFERRED DATA

Transfer of data from one medium to another (e.g., flash drive to hard drive or flash drive to flash drive) will be verified through a hashing algorithm.

7.11 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.

7.12 UNCERTAINTY OF MEASUREMENT

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

8. TRAINING

Examiners in the FTU are designated as either Operators or Analysts.

Analysis of extracted data relates to any type of search for specific words, phrases, or anything else that an investigator might request. Limiting data by date range is not considered analysis.

Operators are able to perform data extractions on mobile devices, but are not allowed to analyze the extracted data. Analysts are able to extract data from mobile devices and search through the extracted files using criteria supplied by the detective.

OPERATOR MINIMUM TRAINING REQUIREMENTS

An operator must complete the following items before they are allowed to extract data from mobile device evidence:

Practice phone extractions (minimum 20)

5 practice reports on any phone

Structured training classes with testing

Literature review:

SWGDE/IT Guidelines

Cellebrite & XRY user manuals

U.S. Supreme Court Riley decision

Developing Process for Mobile Device Forensics

FTU policy/procedure manuals

Shadowing:

Case file review (minimum 5)

Forensic examiner (minimum 2)

Operator level final competency tests:

Written or oral and Practical, to include report

ANALYST MINIMUM TRAINING REQUIREMENTS

An analyst must complete the following additional items before they are allowed to analyze extracted data from mobile device evidence:

- Readings:
  - NIST guideline documents
  - Cellebrite Certified Physical Analyst (CCPA) manual
- 5 co-signed reports at analysis level
- Case shadowing:
  - Case file review (minimum 5)
- Past CTS practice analysis exercise
- Analyst level final competency test:
  - Written exam
  - Any available CTS analysis report
  - Moot court (desirable before first court testimony)

Appendix A – Acronyms and Abbreviations

ADB – Android Debug Bridge

API – Application Programming Interface

BD – Blu–ray Disc

BD-DL – Dual-layer Blu-ray Disc

BD-QL – Quad-layer Blu-ray Disc

CD – Compact Disc

CDMA – Code Division Multiple Access

CD-R – Recordable Compact Disc

CD-RW – Rewritable Compact Disc

Config – Configuration

Cont – Continued

CW – Clockwise

DB / db - Database

DFU – Device Firmware Update

DVD – Digital Versatile Disc

DVD-DL – Dual-layer Digital Versatile Disc

EDT – Eastern Daylight Time

eMMC-embedded MultiMediaCard

ESN – Electronic Serial Number

EST – Eastern Standard Time EXT Data – Extended Data

GSM – Global Systems for Mobile Communications

ICCID – Integrated Circuit Card Identifier

iDEN – Integrated Digitally Enhanced Network

IMEI – International Mobile Equipment Identity

IMG – Image

IMSI – International Mobile Subscriber Identity

JPEG / .jpeg – Joint Photographic Experts Group

MDN – Mobile Directory Number

MEID – Mobile Equipment Identifier

MIN – Mobile Identification Number

MMS – Multimedia Messaging Service

MSISDN – Mobile Subscriber Integrated Services Digital Network

PIN – Personal Identification Number

PUK – Personal Unlock Key

QA – Quality Assurance

SD – Secure Digital

SDN – Service Dialed Number

SIM – Subscriber Identity Module

SMS – Short Message Service

SMSC – Short Message Service Center

S/N – Serial Number

TDMA – Time Division Multiple Access

TIFF / .tiff – Tagged Image File Format / Graphics File Format

TMSI – Temporary Mobile Subscriber Identity

UICC – Universal Integrated Circuit Card

USIM – Universal Subscriber Identity Module

UTC – Coordinated Universal Time