SAN DIEGO POLICE DEPARTMENT

CRIME LABORATORY

Forensic Technology

Unit Manual

Issuing Authority: Lisa Merzwski, January 26, 2021

1. UNIT DESCRIPTION

Office hours are based on an alternative work schedule and generally run from 0600 to 1630 hours. Staffing consists of two full time analysts and a technical lead, 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 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 ASSIGNMENT AND RECEIVING EVIDENCE

2.1 The supervisor will review work requests prior to assigning. Legal authority (search warrant, consent form signed by the possessor of the device, etc.) must be provided with the actual work request before commencing with any forensic examination. Legal authority for 4th waivers needs to be attached unless the phone belongs to a person on parole or Post-Release Community Supervision (PRCS). The 4th waiver must specify electronic devices or similar wording are allowed to be searched as part of the 4th waiver condition.

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

1. An examiner checks out impounded evidence from the Property Room.
2. An examiner transfers evidence to themselves that has been retained in the Forensic Technology Unit, using FileOnQ.
3. If evidence is designated with a barcode, the evidence may be transferred to the Forensic Technology Unit. The evidence will be transferred to **"RETAINED IN FTU – FORENSIC TECH. UNIT"**. When an examiner has been assigned, they can receive the evidence via procedure #2 (above). The releasing party will authorize the transfer via signature. This transfer will ensure that Property Unit staff are not searching for a missing item.
4. If evidence is not designated with a barcode or if FileOnQ is not accessible, the evidence will be transferred to an examiner using an Internal Chain of Custody form.

3. LEGAL ISSUES

3.1 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 extractions or analysis. The legal authority is verified by the unit supervisor, an independent analyst, or the examiner.

A copy of the legal authority documentation will be uploaded to LabLynx.

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.

3.2 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 DA Liaison, assigned prosecutor and/or submitting investigator for guidance as to how to proceed.

3.3 EVIDENCE OF OTHER CRIMES

If an examiner discovers evidence that is outside the scope of the submitted legal authority, the examiner will notify the assigned prosecutor and/or submitting investigator of the discovery and nature of the evidence.

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

3.4 DESTRUCTION OF EVIDENCE

If examination of a mobile device has the potential to cause the destruction of that device or the loss of information stored on the device, permission to proceed will be obtained from the DDA assigned to the case. If no DDA is assigned, permission must be obtained from the case Detective. Documentation of permission to proceed will be maintained in the case record.

4. GENERAL ANALYTICAL PROCEDURES

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 are available in order to analyze these devices. Tools shall be updated as software updates or new protocols are released.

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.

Case notes must document each analytical 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 user-confidential password protection.

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

The device identification is located in the extraction report. If there is no extraction report or the identification is missing, the examiner will record the manufacturer, model, and identifiers (e.g. IMEI, MEID) of the submitted equipment, as well as its condition.

4.5 ISOLATING THE PHONE

Stop the reception and transmission of data by powering down the device, removing the SIM card, using a transmission blocking barrier, or activating Airplane Mode, as applicable.

4.6 EXAMINATION PROCEDURE

For device-specific instructions, see OEM manuals for examination equipment and software.

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

Devices containing biological materials that pose a biohazard related risk can be cleaned as part of the examination procedure if a request for DNA analysis is not

pending.

Attempt to prohibit the transmission/reception of data as described in Section 4.5 as soon as practical.

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.

As part of the repair process, the mobile device may be disassembled and inspected. If corrosion is evident on critical components, it may 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.

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

Perform examination of the mobile device as soon as possible.

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.

Whenever possible a quality check is performed by comparing data visible on the device to extracted data.

4.6.1 iOS-SPECIFIC PROCEDURES

iOS devices that are passcode protected can only be unlocked with the Grayshift GrayKey device.

iOS devices will be extracted with the Grayshift GrayKey device, followed by analysis of the extracted data.

iOS devices awaiting unlock via the GrayKey Agent will be held in the FTU for a maximum of 3 months, with an allowable variation for work schedules. The 3-month time limit may be extended with supervisor approval. If approved, an email will be sent to the investigator, copied to the unit supervisor, to offer an extension of analysis. At the conclusion of each iPhone examination, the Agent will be removed from the device, and the device will be released according to FTU/Lab policy.

If an extension is granted, an email will be sent to the investigator, copied to the unit supervisor.

Wording of the email will be similar to the following:

"We have reached the 3-month mark in our attempt to determine the phone's passcode. At your request, we are going to continue working on the device in an attempt to recover any data that has not already been released to you.

Please let us know if circumstances change and we can discontinue our efforts."

GrayKey procedures are stored at G:\Laboratory\Forensic Technology Unit\Manuals\Grayshift GrayKey.

4.7 DATA ANALYSIS

The examiner will review the work request and accompanying documents to ascertain what information is needed from the device, and if possible, become familiar with the details of the incident, the parties involved, and potential evidence that might be found. Conducting

the examination in a partnership with the investigator is advised. The investigator provides insight into what investigative information is being sought, while the analyst provides the means to find relevant information that might be on the system. Keywords provided by the investigator/analyst may be used to search the data set.

5. CASE FILE DOCUMENTATION

5.1 GENERAL

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

Details of findings, such as:

Specific data related to the request

Other data that support the findings

Search results

Indicators of ownership

Description of relevant apps on the examined items

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

As appropriate, the following (or similar) wording will be included in each report:

Note: Dates and times associated with files stored on the device(s), such as images and videos, may not reflect the actual dates and times the files were recorded.

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.

In the event that data is analyzed from a locked phone and the information obtained cannot be verified, a disclaimer will be added to the report: *The interpretation of this extracted data could not be verified against the device due to the lack of a password. It may change if additional information is received.*

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

5.2 EXTRACTED DATA MANAGEMENT

Two sets of extracted data will be placed on an appropriate medium (CD/DVD/Blu-ray/flash drive/harddrive/department network drive). One set will be designated as the master disk(s) and will have all of the extracted data files, as well as the data released to the investigator. This set of data can be stored in the department network drive by "Case/Incident# Master Data" or will be assigned a barcode number using FileOnQ, and impounded in the property room. The data on the master disk(s) may also be maintained on workstation hard drives.

The other set of extracted data will be released to the investigator as a working copy for their final review. The copy created for release will have only the readable data file(s). A copy of the master disk(s) will be provided to the DDA as part of any discovery request.

When an analyst determines that workstation data storage space is running low, data may be transferred to the unit's Network Attached Storage (NAS).

Data will be stored on the NAS according to the Laboratory's data storage policies.

6. EQUIPMENT

Extraction Tools

Cellebrite UFED Touch

Cellebrite UFED Physical Analyzer

MSAB XRY Complete

Magnet Forensics Axiom

Grayshift GrayKey

Data Release

Rimage Evidence Disk System 5410N Professional (for burning and copying disks), flash drives, department network drive, and hard drives

Data Transfer Verification

Hashing software (ensures data has been copied correctly)

Data copy software with hash algorithm verification

UFED 4PC 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 analysts will report any anomalous performance of the equipment immediately to the technical lead and unit supervisor.

7.2 VALIDATION

Any new method must be validated per laboratory Quality Manual.

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

The Forensic Technology Unit's (FTU) mobile device reference collection consists of mobile devices that may be used for testing, training, or parts. The collection is composed of mobile devices that were marked for disposal/destruction pursuant to Property Room protocol.

Procedure

1. A member of the FTU (or designee) obtains custody of all devices collected by the Property Room for the Mobile Device Reference Collection. The transfer of custody is documented in the San Diego Police Department's (SDPD) evidence tracking system.

2. The mobile devices are catalogued with, at a minimum, their original SDPD barcode number, a description of the device (e.g. make/model), and a unique FTU reference collection number. An electronic log containing all information regarding the reference device collection is maintained and is only accessible by a member of the FTU (or designee). All access is tracked by the SDPD.

3. The devices are physically stored in a locked room within the 5th floor laboratory storage room. The room is only accessible by a member of the FTU (or designee) via keycard. All access is tracked by the SDPD.

4. All data on devices are confidential and handled according to SDPD policy.

5. Devices are not authorized to be released to detectives or other members of the department. Devices that are determined to be unsuitable for retention are to be returned to the Property Room for destruction pursuant to department policy.

7.5 SOFTWARE AND 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 to the affected tools/devices in use in the laboratory as quickly as work schedules will allow. The newly updated tool(s) will then be performance checked (see below). 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.

Updates will be documented in a log file maintained in the FTU directory on the SDPD LAN.

7.6 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 performance checked prior to its first use on casework. This is for new tools being used with an established method.

Performance checks ensure that the known populated data on the control device(s) are correctly retrieved/parsed in the extracted data set(s).

An entry will be made in the maintenance log for the updated equipment with the date of the performance check (if the equipment is in the laboratory) or date of version upgrade (if the equipment is deployed outside of the laboratory).

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.

7.7 PERFORMANCE CHECKING WRITE/SIGNAL BLOCKERS

The following applies to all performance checks of write/signal blockers:

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

Note: If the write/signal 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/signal 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/signal blocker will be removed from service until the failure is resolved.

7.18 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.

7.9 PERFORMANCE CHECKING BATTERIES AND CHARGING CABLES

Battery and charging cables will be checked to ensure functionality before being used in casework.

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 PROFICIENCY TESTING

Analysts will be proficiency tested on an annual basis in either Android or iOS device analysis. Passing is determined through comparison to CTS summary data for all test submissions. Answering 90% of manufacturer's questions with the consensus of other participants must be obtained.

8. TRAINING

At the completion of training, analysts will be expected to adequately perform all duties described in Section 1 of this manual.

MINIMUM TRAINING REQUIREMENTS

An analyst 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
  - NIST guideline documents
- Cellebrite Certified Physical Analyst (CCPA) manual
- Shadowing:
  - Case file review (minimum 10)
  - Forensic analysis (minimum 2)

- 5 co-signed reports
- Past CTS practice analysis exercise
- Competency test:
  - Written exam
  - Any available CTS analysis + report

Moot court (desirable before first court testimony)

Note: Any unexplained variations from expected responses will require additional training and re-testing.

Appendix A – Acronyms and Abbreviations

ADB – Android Debug Bridge

AFU – After First Unlock

API – Application Programming Interface

BD – Blu-ray Disk

BD-DL – Dual-layer Blu-ray Disk

BD-TL – Triple-layer Blu-ray Disk

BD-QL – Quad-layer Blu-ray Disk

BFU – Before First Unlock

CD – Compact Disk

CDMA – Code Division Multiple Access

CD-R – Recordable Compact Disk

CD-RW – Rewritable Compact Disk

Config – Configuration

Cont – Continued

CW – Clockwise

DB / db – Database

DDA – Deputy District Attorney

DFU – Device Firmware Update

DVD – Digital Versatile Disk

DVD-DL – Dual-layer Digital Versatile Disk

EDL Mode – Emergency Download Mode

EDT – Eastern Daylight Time

eMMC-embedded MultiMediaCard

ESN – Electronic Serial Number

EST – Eastern Standard Time

EXT Data – Extended Data

GK - GrayKey

GSM – Global Systems for Mobile Communications

ICCID – Integrated Circuit Card Identifier

iDEN – Integrated Digitally Enhanced Network

IEF – Internet Evidence Finder

IMEI – International Mobile Equipment Identity

IMG – Image

IMSI – International Mobile Subscriber Identity

JPEG / .jpeg / jpg – 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

OEM – Original Equipment Manufacturer

PIN – Personal Identification Number

PR – Property Room

PUK – Personal Unlock Key

QA – Quality Assurance

RAM – Random Access Memory

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 / tif – Tagged Image File Format / Graphics File Format

TMSI – Temporary Mobile Subscriber Identity

UAL – UFED Advance Logical

UDUL – UFED Disable User Lock

UFS – UFED File SystemUICC – Universal Integrated Circuit Card

UL – UFED Logical

UP – UFED PhysicalUSIM – Universal Subscriber Identity Module

UTC – Coordinated Universal Time

XL - XRY Logical (No Files)

XLFR - XRY Logical (Full Read)