Elements of Mobile Forensic Process Cheat Sheet

by [deleted] via cheatography.com/2754/cs/11896/

Introduction

Digital forensics is the process of uncovering electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital evidence for the purpose of reconstructing past events. The context is most often for usage of data in a court of law, though digital forensics can be used in other instances.

Credit: https://digital-forensics.sans.org/media/DFIR-Smartphone--Forensics-Poster.pdf

Elements of Mobile Forensic Process

Intake

□ Receive device as evidence

□ Receive request for examination

Identification

Identify device specifications & capabilities

□ Identify goals of examination

□ Identify legal authority for examination

Preparation

Prepare methods and tools to be used

□ Prepare media and forensic workstation for exam

□ Prepare tools to most recent version

Isolation

□ Protect the evidence

□ Prevent remote data destruction

□ Isolate from the cellular network, bluetooth, & wifi

Processing

{fa-square-o}}Conduct forensic acquisition

□ Perform forensic analysis

□ Scan for malware

Verification

□ Validate your acquisition

□ Validate your forensic findings

Documenting/Reporting

□ Keep notes about your findings and process

Elements of Mobile Forensic Process (cont)

□ Draft and finalize your forensic reports

Presentation

□ Prepare exhibits

□ Present findings

Archiving

□ Keep a gold copy of data in a safe place

□ Keep data in common formats for future

Forensic Artifacts

Forensic artifacts varies from operating system to operating system as the architecture differs from device to device. To collect the digital evidence from a smart phone below are the commonly used types of extraction techniques used by major forensic tools.

1. Physical Collection
2. Logical Collection
3. File System Extraction

Physical Collection

Physical extraction extracts the information from the device by accessing its flash memory. It creates a bit-by-bit copy of the device. Physical collection supports deleted file extraction.

Types of Physical Acquisitions:

Most devices doesn’t support physical extraction unless the user has the root privileges, to overcome such challenges extraction is performed by using two techniques:

JTAG - Joint Test Action Group

JTAG involves using advanced data acquisition methods at the hardware level, which is done by connecting to specific ports on the device and transfer the data. Analyst must have proper training and experience prior to attempting JTAG as the device may be damaged if handled improperly.

Chip-off

Chip-off, is another type of physical acquisition where in the flash chips would be removed from the device to extract the data. This type of acquisition usually damages the device.

Logical Data Collection

The preferred method is physical extraction, however due to the wide range of devices the second preferred method is logical extraction. Logical extraction extracts the data which is accessible and not from the unallocated space. It extracts data without root access however having root access on a device can allow examiner to acquire more data. The data is extracted based on the application programming interface.

Types of Logical Extraction:

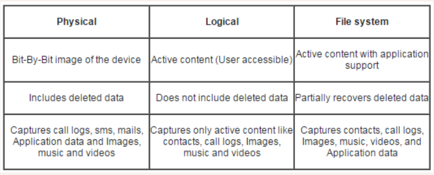
i. Agent Based Extraction

In this extraction an agent will be pushed in to the device and extracts the data then uninstall the agent and its traces. The extraction method from device to device and operating system to operating system differs as the architecture is different.

ii. Data Extraction using ADB commands

ADB (Android Debug Bridge) is a command line tool which is used to communicate with the device to retrieve the information, it can extract the data which is on device having root access to the device provides you more information than as a normal user. ADB shell uses USB debugging mode. If the device is locked and USB debugging is not enabled ADB commands will not able to fetch the results. In most of the cases Application data is stored as a SQLite database. In any type of extraction these dBs are parsed altogether and report is generated..

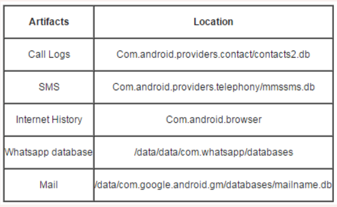
File System Extraction



Physical	Logical	File system
Bit-By-Bit image of the device	Active content (User accessible)	Active content with application support
Includes deleted data	Does not include deleted data	Partially recovers deleted data
Captures call logs, sms, mails, Application data and Images, music and videos	Captures only active content like contacts, call logs, Images, music and videos	Captures contacts, call logs, Images, music, videos, and Application data

It is used to acquire the data stored in the allocated space, unlike physical extraction it only captures the application specific entries in the database to recover the deleted items.

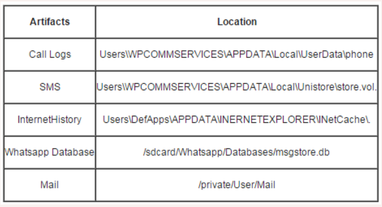
Mobile Android Artifacts



Artifacts	Location
Call Logs	Com.android.providers.contact/contacts2.db
SMS	Com.android.providers.telephony/mmssms.db
Internet History	Com.android.browser
Whatsapp database	/data/data/com.whatsapp/databases
Mail	/data/com.google.android.gm/databases/mailname.db

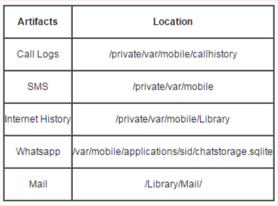
Every operating system has their own architecture to store the artifacts below is the details of different artifacts these artifacts locations varies from device to device and version of the Operating System to Operating System.

Windows File Artifacts



Artifacts	Location
Call Logs	Users\WPCOMMSERVICES\APPDATA\Local\UserData\phone
SMS	Users\WPCOMMSERVICES\APPDATA\Local\Unistore\store.vol.
InternetHistory	Users\DefApps\APPDATA\INERNETEXPLORER\INetCache\.
Whatsapp Database	/sdcard/Whatsapp/Databases/msgstore.db
Mail	/private/User/Mail

IOS File Artifacts



Artifacts	Location
Call Logs	/private/var/mobile/callhistory
SMS	/private/var/mobile
Internet History	/private/var/mobile/Library
Whatsapp	/var/mobile/applications/sid/chatstorage.sqlite
Mail	/Library/Mail/