How to Challenge Law Enforcement Examinations of Mobile Devices

Overview of Discussion Topics

- Types of Digital Data Stored on Mobile Devices
- Types of Mobile Device Extractions
- Tools Used to Conduct Extractions
- Law Enforcement Only Tools Sold by Vendors
- Challenging the Documentation Process
- Challenging the Type of Examination Conducted
- Requesting Access to the LE Only Tools for Defense Use
- Recent Case Examples
- How to Protect Your Mobile Data and the Data of Your Clients

Types of Data

Extraction Summary

+ Add extraction | Add external file | Project settings | Generate report

Extractions: 1

File System
Apple iPhone 7 (A1780)
File System

Extraction start date/time
1/28/2020 8:48:46 AM(UTC-5)
Extraction end date/time
1/28/2020 10:21:03 AM(UTC-5)
F:\Iphone 7 test\UFED checkmat8 Apple i...

Device Content

10 data sources can be extracted using UFED Cloud Analyzer

Phone Data

Activities 94916	Application Usage 17	Applications Usage... 12776	Bluetooth Devices 1127 (99)	Calendar 507 (5)	Call Log 259	Chats 2576 (124)
Contacts 5449 (318)	Cookies 13846 (15)	Device Events 11688	Device Locations 6344 (681)	Device Notifications 1	Emails 15773	Installed Applications 783
Instant Messages 40	IP Connections 68	Log Entries 3331	MMS Messages 1056	Mobile Cards 9	Notes 36 (11)	Passwords 1734
Recordings 3	Searched Items 1534 (434)	SMS Messages 7213	User Accounts 35 (2)	User Dictionary 8058	Voicemails 61	Web Bookmarks 8
Web History 2333 (1978)	Wireless Networks 353					

Data Files

Applications 278	Archives 473	Audio 9903	Configurations 246643	Databases 3451	Documents 629	Exchange 11408
Images 127197	Text 5305	Uncategorized 155995	Videos 3966			

Types of Mobile Device Extractions

- There are three types of extractions that may be performed on a mobile device: logical, filesystem, and physical. The feasibility of these three types of extractions depends upon the make, model and operating system of the mobile device.

What is a Logical Extraction

- The quickest and most supported extraction method, but also the most limited.
- The typical data available via a logical extraction are call logs, SMS (commonly known as text messages), MMS (Multimedia Messaging Service, which are generally text messages with attachments or group text messages), images, videos, audio files, contacts, calendars and limited application data.
- All the data exported in these categories will be live data and will not have the possibility of containing any deleted data.

What is a Filesystem Extraction?

- The primary differentiator between logical extractions and filesystem extractions is the ability for the forensic tools to access the files on the mobile device's internal memory directly instead of having to communicate through API's for each type of data. This direct access allows the forensic tools to extract all files present in the internal memory including database files, system files and logs. Filesystem extractions are useful for examining the file structure, web browsing history and app usage history of a mobile device.
- The most important part of a filesystem extraction is the full access to the database files on a mobile device. Numerous applications, such as iMessage, SMS, MMS, Calendar and others, store their information in database files. When a user deletes data that is part of a database, such as SMS, the entry within this database is marked as deleted and is no longer visible to the user. This deleted data remains intact within the database and is recoverable until the database performs routine maintenance and is cleaned up.

What is a Physical Extraction

- The most extensive but least supported extraction method is the physical extraction. Physical extraction is least supported because getting full access to the internal memory of a mobile device is completely dependent upon the operating system and security measures employed by the manufacturer like Apple and Samsung. A physical extraction performs a bit-by-bit copy of the entire contents of the flash memory of a mobile device. This extraction allows for the collection of all live data and also data that has been deleted or is hidden.
- Most Physical Extraction capabilities for newer devices are held closely by the developers and they restrict the sale/use of them to Government and Law Enforcement only. This is creating a situation in which the Vendors are dictating what evidence can be obtained for trial.

Tools Used to Conduct Phone Examinations

- Cellebrite UFED4PC
- Magnet Axiom
- Oxygen Forensics
- Belkasoft Evidence Center
- MSAB XRY
- All of these tools are vendor based tools available to purchase and license by the digital forensic community. These tools create push-button reports that are commonly provided by Law Enforcement without any in-depth analysis being conducted. THIS IS A PROBLEM!!

LE Only Tools

- Cellebrite Premium Services (advanced level extraction / unlocking Android & Apple)
- Grayshift Graykey (advanced level extraction / unlocking Applde devices, Hidden UI to capture passcodes, other advanced features like remote monitoring)
- These tools come with NDA's to the agencies using them from the vendor. They are provided as in house tools for LE use. These tools are not what you will find listed in your reports from LE. They don't discuss their use or even mention this is how they obtained the data. Instead they provide you filtered data using one of the previously discussed tools.

Challenging the Documentation Process

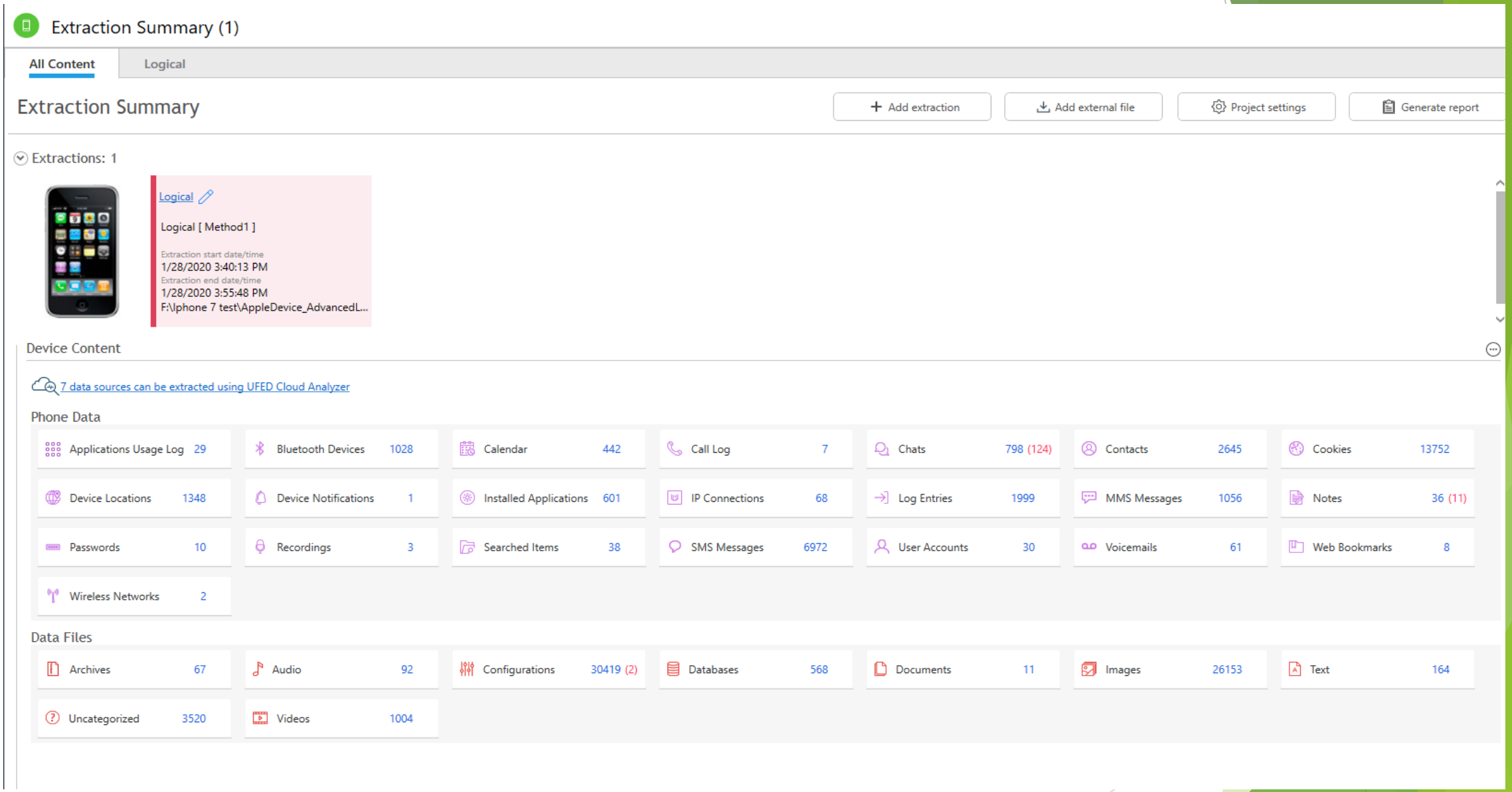
- LE doesn't provide reports / notes which detail the steps they used to gain access to your clients data. They only provide reports which detail the results of what they found or in some cases of the program generated reports without any documentation of their actions at all pertaining to the evidence.
- It is at this point you can question them about their process such as:
- Did you review all available data?
- What tools did you utilize in this process?
- Why didn't you document the use of A or B? (LE only Tools)
- Has that tool been tested and accepted by the forensic community?
- Did the tool make any changes to the data? Is this Raw Data or Filtered Data?

Challenging the Type of Examination Conducted

- Was it a push button exam?
- Did you manually review the databases for partially deleted files?
- Did you use a SQLITE Browser to review the application data?
- Was it a logical, filesystem or Physical extraction? Why did you choose this level of extraction? Did it provide the most data available from the device?
- Did you provide all of the extracted data?
- How many tools did you use to examine the device? Are they all documented?
- Did any of the tools provide different results? Why?

Requesting Access to the LE Only Tools for Defense Use

- The LE only tools provided by Vendors are not tested outside of the LE community. Each time an issue has been found with one of these tools including them not disclosing the use, I advise Defense Counsel to request access to the full results (RAW DATA), Access to the Actual Evidence (Client's Phone) and the use of their LE only tool at their Facility to make our own extraction for comparison.
- This strategy drives Prosecutors crazy! This has even resulted in cases being dropped because if this motion is won they still refuse to allow access to the LE only tools.
- When access to these tools are provided the results are remarkable in the difference in data retrieved as seen on the next slide.



Extraction Summary

+ Add extraction | Add external file | Project settings | Generate report

Extractions: 1

File System

Apple iPhone 7 (A1780)
File System

Extraction start date/time
1/28/2020 8:48:46 AM(UTC-5)
Extraction end date/time
1/28/2020 10:21:03 AM(UTC-5)
F:\Iphone 7 test\UFED checkmat8 Apple i...

Device Content

10 data sources can be extracted using UFED Cloud Analyzer

Phone Data

Activities 94916	Application Usage 17	Applications Usage... 12776	Bluetooth Devices 1127 (99)	Calendar 507 (5)	Call Log 259	Chats 2576 (124)
Contacts 5449 (318)	Cookies 13846 (15)	Device Events 11688	Device Locations 6344 (681)	Device Notifications 1	Emails 15773	Installed Applications 783
Instant Messages 40	IP Connections 68	Log Entries 3331	MMS Messages 1056	Mobile Cards 9	Notes 36 (11)	Passwords 1734
Recordings 3	Searched Items 1534 (434)	SMS Messages 7213	User Accounts 35 (2)	User Dictionary 8058	Voicemails 61	Web Bookmarks 8
Web History 2333 (1978)	Wireless Networks 353					

Data Files

Applications 278	Archives 473	Audio 9903	Configurations 246643	Databases 3451	Documents 629	Exchange 11408
Images 127197	Text 5305	Uncategorized 155995	Videos 3966			

Recent Case Examples

- Detective XXX of County XXX provided me with a copy of a Virginia State Police Results of Forensic Examination Report. This report detailed items submitted for examination and identified Item XXX as “laptop hard drive used by Client” however in the details it describes 924-1 as an Apple iPhone 8. It also states the phone extract and report was provided to Detective XXX on 1 May 2019 and no further reporting shall be done with this device. No further explanation was provided in this report about the forensic extraction, examination, tagging of files, reviews of databases or findings during the examination pertaining to the Apple iPhone. However, the report did provide detailed information about the laptop hard drive used by Client which was also mislabeled as the wrong item. The details stated after reviewing 234,573 media artifacts which would include all picture files no evidence of child pornography was located. This report was signed by VSP Examiner XXX.

- Between 19-20 May 2020, I conducted a review of the full data extracted from the Apple iPhone in this case at the Virginia State Police Lab, I was provided a hard disk drive containing the GrayKey extractions (ordered by Judge) for review by VSP Examiner XXX. I asked Examiner XXX if I could review the case notes and reports pertaining to the forensic examination conducted of the apple iPhone. Examiner XXX stated the notes are part of a working file and would not be disclosed for review. Examiner XXX also told me there was no written report of what was done however as referenced previously there was a report provided by Examiner XXX about the examination to Detective XXX. Further discussion with Examiner XXX revealed they only loaded 1 of the 3 files produced by GrayKey into the forensic tool Axiom to review the data. The file containing the memory and keychain data were not loaded as part of the examination. The manufacturer of the tool Axiom recommends to load all 3 files to obtain the most complete data extraction.

Recent Case Examples

- Between 11 May 2020 – 10 June 2020, I conducted a review of the full data extracted from the Apple iPhone in this case. No notes or reports were provided to show how the Forensic tools were utilized by VSP during the examination of the data. The Kingston DataTraveler 100 G3, 64GB, Flash Drive contained 5 files. One of the files was “XXX.pdf” which was the GrayKey Progress report which revealed the data extraction took place on 2 March 2020.
- I then questioned why this extraction occurred months after the was charged. On 29 May 2020, I was then provided a 2nd Kingston DataTraveler 100 G3, 64GB, Flash Drive, which was provided by VSP and it contained only 2 files (neither of which were originally provided under the order). One of the files was also a .pdf with the filename of “XXX” which was the GrayKey Progress report which revealed the data extraction took place on 22 November 2019.

Recent Case Examples

- A comparison of the 2 extractions that were provided revealed one was larger than the other. The first extraction conducted was 30GB in size and the second extraction was 46.2GB in size.
- This device was in LE control the entire time.
- The second extraction had no reason to be conducted.
- Every time you turn a phone on or off it changes!!!!

Recent Case Examples

- On 6/9/2020, I conducted a review of the case file located at the Prosecutor's office. During this review it was discovered in incident report Detective XXX stated:
- On 11/26/2019 DET XXX spoke with Special Agent XXX, with the VA State Police concerning the download of several thousand images and videos. Special Agent XXX told me they saw in excess of 100,000 images and approximately 14,000 videos of child pornography on Client's iphone and in his icloud.
- I have not received a report from Special XXX which states this information. The only report I have received from Special Agent XXX doesn't report any findings as stated above. Furthermore, my examination of the data doesn't show 14,000 videos of child pornography. A search for all the video files from the extracted data using multiple forensic tools doesn't reveal 14,000 total videos on the device.
- It also mentions iCloud data which was not provided as part of discovery and no search warrant was located in the case file for iCloud data. The search warrant authorized the search of the devices not cloud storage data. iCloud data is stored on servers which are controlled by Apple. A search of that data would require a search warrant for the iCloud data to be granted and served to Apple. I found no documentation in the case file which shows this action was conducted.

How to Protect Your Mobile Data and the Data of Your Clients

- Use 8 – 10 digit or character password on your devices
- If the device is to be collected by Law Enforcement, ensure it is powered off!!
- Get the data extracted by your own examiner prior to the collection by LE if possible
- Hire a skilled Digital Forensic Firm to dig into all details of the evidence handling, examination, tools used, reporting, etc.
- Know what data your phone is collecting and how it is stored.
- Don’t let your clients give up their passcode!!
- STOP THE PUSH-BUTTON PLEA DEAL!!!!

QUESTIONS???

Patrick A. Eller
CEO
Metadata Forensics, LLC
1108 E. Main St, Suite 503
Richmond, VA 23219
Office: 866-382-3282
Email: patrick@metadataforensics.com
Website: https://metadataforensics.com

METADATA
FORENSICS