CERIAS
The Center for Education and Research in Information Assurance and Security

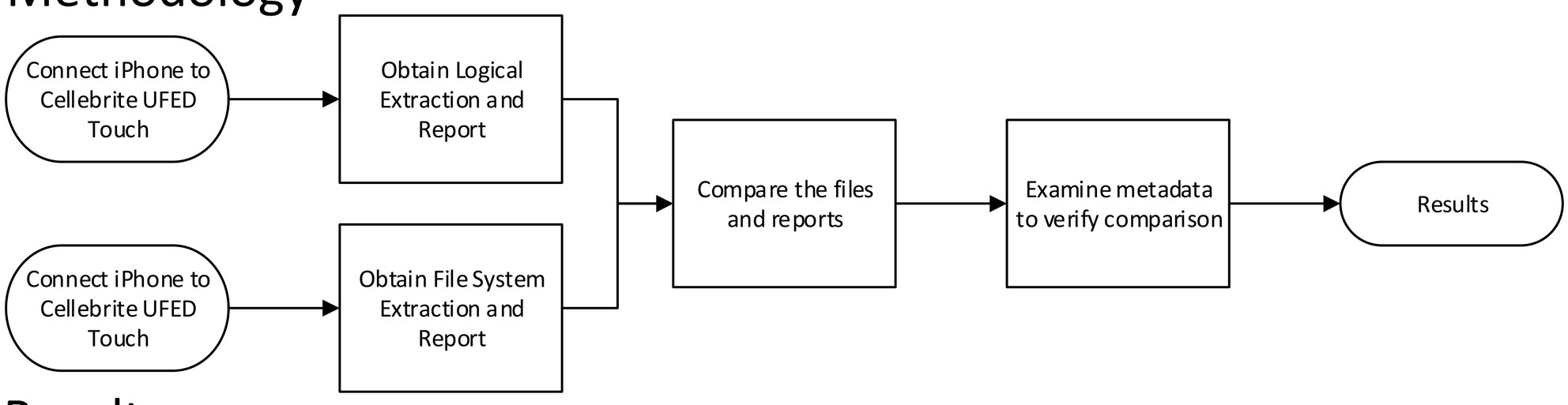
Exploring the Cellebrite Universal Forensic Evidence Device (UFED) File System Extraction Process

Kaitlyn Gurule, Marcus Thompson

Abstract

Extracting data from a mobile device from Cellebrite's UFED can be done using three different methods: physical, file system, and logical. The physical and logical extraction methods are commonly used among law enforcement digital forensic examiners. The terminology of file system extraction was created by Cellebrite. It is not as understood as the other methods. To better understand this method, a logical and file system extraction were obtained from a user populated, jailbroken iPhone 5s with iOS 8.4, and the reports from the two extractions were compared. Upon analyzing the reports, it was determined the file system extraction obtained more data than the logical extraction. It also obtained some of the deleted data Cellebrite stated only the physical extraction could obtain. This may be an effect of the device being jailbroken.

Methodology



Results

Table 1: Device Summary

Item Name	Logical Information Retrieved	File System Information Retrieved
Detected Model	ME345	-
Device Name	iPhone	iPhone 5S
Revision	8.4 (12H143)	8.4
ESN	##########	-
Serial Number	##########	-
MDN	(###) ###-####	##########
ICCID	##########	##########
IMSI	##########	-
Bluetooth Address	ADDRESS	Six shown in Bluetooth Devices
Wi-Fi Address	ADDRESS	Four shown in Wireless Networks
Unique Device ID	##########	-
Extraction start date/time	10/05/2015 04:19:29 PM	10/5/2015 2:33:05 PM
Extraction end date/time	10/06/2015 08:51:54 AM	10/5/2015 4:09:00 PM
Apple ID	-	APPLE ID EMAIL
Is Encrypted	-	False
Is Jailbroken	-	True
Location Services Enabled	-	True
Synced with	-	Computer: NAME \User: USER NAME

Table 2: Logical Extracted Data

Item Type	Number of Items Retrieved
Contacts	310
SMS - Text Messages	3646
Calendar/Notes/Tasks	2296
Call Logs	2825
MMS - Multimedia Messages	276
Instant Messages	1954
Browser Bookmarks	3
Browser History	291
Images	12433
Ringtones	300
Audio	128
Video	35

Table 3: File System Extracted Data

Item Type	Total Number of Items Retrieved	Number of Deleted Items
Bluetooth Devices	6	-
Calendar	2908	620
Call Log	3114	134
Carved Strings	19	19
Chats	244	208
Contacts	505	1
Installed Applications	189	-
Locations	614	-
MMS Messages	276	-
Notes	15	7
Searched Items	3	-
SMS Messages	3545	-
Timeline	12484	746
User Accounts	4	-
Voicemail	49	-
Web Bookmarks	3	-
Web History	428	-
Wireless Networks	4	-
Data Files	17201	-
Activity Analytics	706	-
Analytics Phones	443	-

Conclusions

This study was performed in order to determine what differences exist between the logical and file system extraction methods. In completing this research, many differences were found. The file system extraction retrieved more data including deleted data from the iPhone than the logical extraction. The Bluetooth devices, user accounts, voicemail messages, applications, data files are some of the additional data that the file system extraction obtained.

This study shows in the interest of completeness of evidence it would be better to obtain the file system extraction over the logical extraction. This provides more data and can possibly recover some of the data the user deleted. Retrieving this information is imperative in locating evidence to support the mobile phone investigation. The logical extraction should also be conducted to support verification of the results. Further research should be conducted to compare the output of the file system extraction method of jailbroken and non-jailbroken devices.