Artifact Integrity in Forensic Acquisitions of iPhones using Jailbreak Preprocessing

Ian Hamilton and Marcus Thompson
Computer & Information Technology
Purdue University

PROBLEM

The increasing security present on iPhones and iOS devices prevents some types of forensic acquisitions, making it more difficult to get data from the phone [1]. While jailbreaking a phone may allow a forensic examiner to bypass these restrictions, jailbreaking a phone for a forensic acquisition is believed to corrupt the integrity of the evidence leaving anything found afterwards as inadmissible in a court of law [2][3]. There is a lack of research demonstrating this claim. One study claims jailbreaking is acceptable and does change evidence [4]. Their method compares the name, date, size, and, number of files before and after jailbreaking – an invalid forensic method. There was no indication of hashing used to show file integrity. This study attempts to empirically determine if the jailbreaking process is or is not forensically sound.

METHODOLOGY

The methodology performed in this study was divided into three steps. For each acquisition, a Filesystem and Logical extraction was performed using UFED Physical Analyzer. In the first step, a baseline image was created and hash values were calculated for the selected files shown in the results. In the second step, the device was jailbroken using the evasi0n jailbreak application. The device was then acquired once again and the files were hashed a second time. The third step was to perform an iTunes Restore and Sync to Encrypted Backup procedure to determine if the jailbreak was reversible. This process required a clean restore and sync in order to completely reverse the jailbreak. After the jailbreak was reversed, the device was acquired and the files were hashed for the third and final time. There was an error in the initial backup process that caused the restore process to restore considerably less data than if the options to backup the data been selected.

RESULTS

The final comparison of the hash results for each file can be seen in the table to the right. Two comparisons were done for each file acquired. The first comparison performed was between the two copies of the file acquired by the filesystem acquisition. The second comparison performed was between the two copies of the file acquired by the logical acquisition. The hash values of four files were different after the jailbreak process for both the filesystem and logical acquisition, and the hash of one other file was the same for the filesystem acquisition and different for the logical acquisition. Throughout the entire methodology the only file to retain the same hash value was the AddressBookImages database. It is difficult to determine what changes introduced during the restore process were caused by the errors in the initial encrypted backup process. These errors may not be related to changes during the jailbreak process, but are important in the determination of its reversibility.

CONCLUSION

The purpose of this research was to determine if the jailbreaking process altered, updated, or deleted user information that would invalidate the forensic integrity of all data collected afterwards. The initial conclusion to this question, based on the research performed in this study, is yes. The results of the study determined files containing important user information changed after the jailbreak process, so the null hypothesis was rejected.

This study is important, but its significance is limited. There are multiple jailbreaking applications, multiple iPhones with different hardware, and multiple versions of the iOS operating system. Future research should be conducted using this methodology taking these differences into account. This research will create a better understanding of these differences and determine what impact these differences have upon the validity of jailbreaking as a mobile forensic preprocessing technique.

Overall, the jailbreak process is an invasive process that causes an unknown number of changes to the information stored on the device. Jailbreaking as a preprocessing technique may be acceptable as a last resort for some organizations, but currently, it cannot be considered forensically sound given the research in this study and the lack of research using other devices, operating systems, and jailbreak applications.

RESEARCH QUESTION

Does jailbreaking an iOS device alter, update, or delete any user information that would invalidate the forensic integrity of evidence retrieved afterward?

H_0: Jailbreaking an iOS device does not alter, update, or delete user information that would invalidate the forensic integrity of evidence retrieved afterward.
H_a: Jailbreaking an iOS device alters, updates, and or deletes user information that would invalidate the forensic integrity of evidence retrieved afterward.

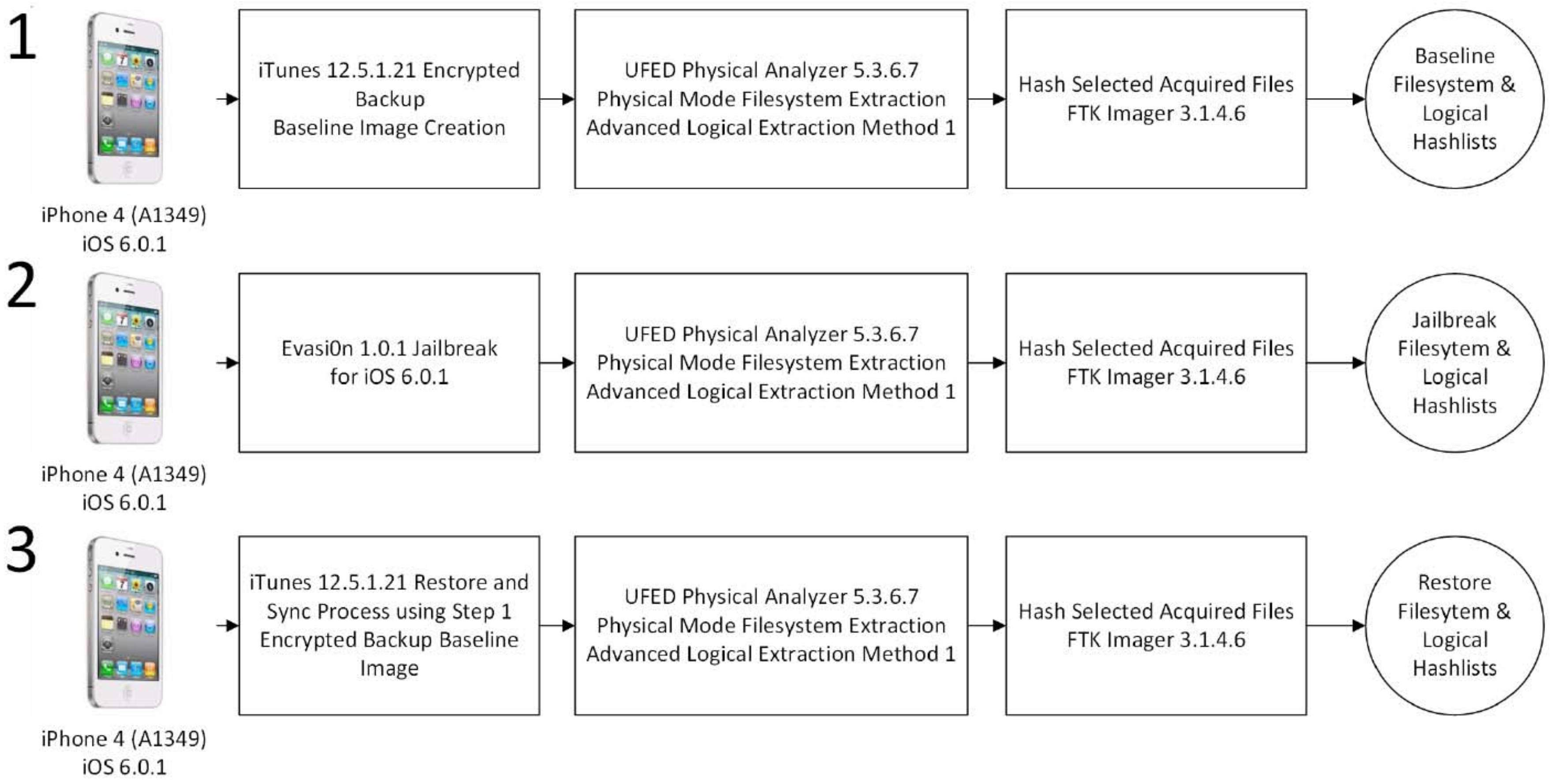
1
iPhone 4 (A1349)
iOS 6.0.1
iTunes 12.5.1.21 Encrypted Backup
Baseline Image Creation
UFED Physical Analyzer 5.3.6.7
Physical Mode Filesystem Extraction
Advanced Logical Extraction Method 1
Hash Selected Acquired Files
FTK Imager 3.1.4.6
Baseline Filesystem & Logical Hashlists
2
iPhone 4 (A1349)
iOS 6.0.1
Evasi0n 1.0.1 Jailbreak for iOS 6.0.1
UFED Physical Analyzer 5.3.6.7
Physical Mode Filesystem Extraction
Advanced Logical Extraction Method 1
Hash Selected Acquired Files
FTK Imager 3.1.4.6
Jailbreak Filesytem & Logical Hashlists
3
iPhone 4 (A1349)
iOS 6.0.1
iTunes 12.5.1.21 Restore and Sync Process using Step 1 Encrypted Backup Baseline Image
UFED Physical Analyzer 5.3.6.7
Physical Mode Filesystem Extraction
Advanced Logical Extraction Method 1
Hash Selected Acquired Files
FTK Imager 3.1.4.6
Restore Filesystem & Logical Hashlists

Table of File Hash Comparisons

File	Baseline vs Jailbreak	Jailbreak vs Restore	Restore vs Baseline
AddressBook.sqlitedb	FS & Logical Match	FS & Logical Mismatch	FS & Logical Mismatch
AddressBookImages.sqlitedb	FS & Logical Match	FS & Logical Match	FS & Logical Match
Bookmarks.db	FS Match & Logical Mismatch	FS & Logical Mismatch	FS & Logical Mismatch
Calendar.sqlitedb	FS & Logical Mismatch	FS & Logical Mismatch	FS & Logical Mismatch
Extras.db	FS & Logical Match	FS & Logical Mismatch	FS & Logical Mismatch
call_history.db	FS & Logical Match	FS & Logical Mismatch	FS & Logical Mismatch
cache_encryptedA.db	FS Mismatch	FS & Logical Mismatch	FS & Logical Mismatch
consolidated.db	FS & Logical Match	FS & Logical Mismatch	FS & Logical Mismatch
Cache.db	FS Match	Not Recovered in Restore	Not Recovered in Restore
notes.idx	FS & Logical Match	FS & Logical Mismatch	FS & Logical Mismatch
notes.sqlite	FS & Logical Match	FS & Logical Mismatch	FS & Logical Mismatch
Photos.sqlite	FS & Logical Match	FS & Logical Mismatch	FS & Logical Mismatch
sms.db	FS & Logical Mismatch	FS & Logical Mismatch	FS & Logical Mismatch
voicemail.db	FS & Logical Mismatch	FS & Logical Mismatch	FS Match & Logical Mismatch

FS = Filesystem acquisition; Logical = Logical acquisition

REFERENCES

[1] Mahalik, H., Tamma, R., & Bommisetty, S. (2016). Practical mobile forensics: A hands-on guide to mastering mobile forensics for the iOS, Android, and the Windows Phone platforms.

[2] Ahmed, M. J., Khalid, U., & Aslam, B. (2014, December). iDevice forensics - Data integrity. 17th IEEE International Multi Topic Conference 2014, 260-265. doi:10.1109/inmic.2014.7097348

[3] Iqbal, B., Iqbal, A., & Obaidli, H. A. (2012, March). A novel method of iDevice (iPhone, iPad, iPod) forensics without jailbreaking. 2012 International Conference on Innovations in Information Technology (IIT), 238-243. doi:10.1109/innovations.2012.6207740

[4] Chang, Y.-T., Teng, K.-C., Tso, Y.-C., & Wang, S.-J. (2015). Jailbroken iPhone Forensics for the Investigations and Controversy to Digital Evidence.