2014

Effects of the Factory Reset on Mobile Devices

Schwamm, Riqui

ADFSL

Schwamm, Riqui, and Neil C. Rowe. "Effects of the factory reset on mobile devices." Journal of Digital Forensics, Security and Law 9.2 (2014): 205-220.
http://hdl.handle.net/10945/49294

EFFECTS OF THE FACTORY RESET ON MOBILE DEVICES

Riqui Schwamm and Neil C. Rowe
U.S. Naval Postgraduate School
Computer Science Department
Monterey, CA 93943 USA
{rschwamm, ncrowe}@nps.edu

ABSTRACT

Mobile devices usually provide a "factory-reset" tool to erase user-specific data from the main secondary storage. 9 Apple iPhones, 10 Android devices, and 2 BlackBerry devices were tested in the first systematic evaluation of the effectiveness of factory resets. Tests used the Cellebrite UME-36 Pro with the UFED Physical Analyzer, the Bulk Extractor open-source tool, and our own programs for extracting metadata, classifying file paths, and comparing them between images. Two phones were subjected to more detailed analysis. Results showed that many kinds of data were removed by the resets, but much user-specific configuration data was left. Android devices did poorly at removing user documents and media, and occasional surprising user data was left on all devices including photo images, audio, documents, phone numbers, email addresses, geolocation data, configuration data, and keys. A conclusion is that reset devices can still provide some useful information to a forensic investigation.

Keywords: mobile device, forensics, factory reset, file types, Cellebrite, privacy

1. INTRODUCTION

An increasing amount of criminal activity uses mobile devices (McMillan, Glisson, and Bromby, 2013). Devices do provide ways to erase user information from secondary storage and criminals will likely use them. However, these methods are not entirely effective and information of forensic value can be left after these attempts to erase it. In addition, with frequent device upgrades by manufacturers, discarded older devices are common. This paper attempts to determine how much and what kind of residual user data are left after a "factory reset" or "wipe" intended to remove user data. This analysis will aid forensic examiners that encounter reset drives.

Recently a number of researchers have developed methodologies for forensic investigation of mobile devices (Marturana, et al., 2011; Omeleze and Venter, 2013; Owen, Thomas, and McPhee, 2010). Systematic analysis of mobile devices differs somewhat from that of desktop and laptop computers because of the difficulty of accessing the main secondary storage, which is usually a flash storage soldered to the device board. Cutting out and removing the storage (Alghafli, Jones, and Martin, 2012) usually destroys the device functionality. Hence most mobile forensic tools attempt to access the storage through the operating system. Several issues particular to mobile devices arise such as finding where data are stored and dealing with data aggregation. For instance, on most smartphones the call records are stored in a single file. In addition, the operating system may not permit access to all files.

The term "factory reset" is used by manufacturers to mean restoring an electronic device to the state when it left the factory, deleting all user data and third-party

applications in the process (Rouse, 2013). It should be done when discarding a device or transferring it to a new owner. The concept is clear when referring to music players and other simple devices, but its meaning is less clear for complex mobile devices where some user data may be necessary to configure it adequately, and some user data are stored within operating-system files.

No systematic testing appears to have been done of the factory reset on mobile devices, although technology websites report gripes (The Guardian, 2013). For example, (Smith, 2012) tested secondhand phones purchased through Craigslist where a factory rest had been performed on the devices. Data that they found included court records, social security numbers, resumes, college applications, child support documents, employee records, bank statements, credit-card statements, tax returns, email, contact lists, and photos. One investigation (Cardwell, 2013) studied the effects of a factory reset on network data left on an Android phone. Data was transferred between Android phones and multiple network access points (cellular, wireless, and Bluetooth). Residual data in secondary storage on test phones after the reset included "userdata" partitions containing Service Set Identifiers, wireless-router Subscriber Identity Modules, DHCP ACKs from wireless routers, and base-station metadata that included the Mobile Network Code, Mobile Country Code, Local Area Code and Cell Identification, wireless router Media Access control addresses, and Bluetooth addresses of devices paired with the phone.

These reports suggests that useful forensics on reset devices is indeed possible. They also raise worrisome questions about the privacy of information stored on mobile devices. Privacy of personal information is currently subject of much attention (Payton and Claypoole, 2014). If private data are left on devices after users have reset them, users may be able to sue manufacturers, and this needs to be factored into business decisions (Kauffman, Lee, and Sougstad, 2009). Matters are even worse if the data left on devices are unpredictable as it appears to be from the anecdotal reports.

2. EXPERIMENTAL SETUP

Tools from Cellebrite (www.cellebrite.com/mobile-forensics) were used to extract data from the main storage of test devices. The Cellebrite UME-36 Pro Universal Memory Exchanger 1.2.2.3 hardware accessed the devices, and the Cellebrite UFED Physical Analyzer 3.7.2.0 software analyzed the images. Other products claiming similar functionality include the Forensic Toolkit (www.accessdata.com), Oxygen Forensic Suite (www.oxygen-forensic.com), EnCase Neutrino (www.guideancesoftware.com), Recuva (www.piriform.com), and ViaExtract (viaforensics.com). The Oxygen Forensic suite was tested on some of our phones and it appeared to work well. ViaExtract showed compatibility issues with some Android phones (the Samsung Galaxy SIII and the Motorola Atrix 4G). Recuva is primarily for hard drive recovery; it could extract small data sets but did not provide useful analysis.

A full ufd-format dump of the file system on each device was made by the Cellebrite Physical Analyzer. A program was written to calculate DFXML metadata (www.nsrl.nist.gov/DFXML /fileobject.xsd) on the dumps, including calculation of hash values on files. Another program discussed in section 4.2 was written to compare the pre-reset and post-reset DFXML metadata. A taxonomy from (Rowe, 2013) was used to classify files by extension and directory. The Bulk Extractor tool from digitalcorpora.org (Garfinkel, 2013) was used to extract strings. We did not exclude operating-system files from analysis because our previous work (Rowe, 2013) found some user data in them.

Except for two unresponsive phones and also in section 3.4, resets were performed through software using each device's setup menu under "Privacy" or "Backup & Reset".

The reset takes a few minutes after which the device restarts.

2.1 Other Storage for Devices

This work focused on the main nonvolatile storage. A separate removable memory card on some phones ("SIM" or "subscriber identity module") contains the user's identity, account information, and keys, and is necessary to make phone calls. It may also contain text messages and contacts depending on the phone. SIM cards were not available for most of our phones. SIM cards are unaffected by a factory reset and contain information of definite forensic interest, so they should be analyzed if available.

Besides SIM cards, many devices have additional removable storage in the form of SD or MMC cards that is not subject to the factory reset. No such cards were available for the devices tested in section 4, but 76 cards comprising 54,279 files were acquired from smartphone images from an international corpus. Classifying its files by extension using our taxonomy, 31.7% were camera pictures, 15.0% were audio, 11.8% were video, 5.6% were documents, and 5.6% had no extension. Hence these cards had rich materials for forensic investigation compared with 4.3% camera images, 4.8% audio, and 0.1% video on the mobile-device main-storage corpus to be described. That suggests that the cards should be checked first when available in a forensic investigation.

3. EXPERIMENTS WITH TWO PHONES

To get a more detailed view of what a reset accomplishes, experiments were done with an Apple iPhone 4S phone (p18 in Table 3) and an Android Samsung Galaxy SIII phone (p9), after making copies of the original pre-reset and post-reset images to use later. These experiments placed specific files on the phones that we thought should be deleted by a reset.

3.1 Experimental Protocol

The phones were "factory-reset"; a protocol was followed to put applications and data onto the phones; images were taken of the phone with the Cellebrite Physical Analyzer; the phones were reset again; and images were taken again. The furnished data included distinctive keywords to make it easier to recognize forensically. The phones were not connected to a cellular account, so messaging services could not be tested. The protocol was:

1. Reset the device.
2. Visit four specified websites: nps.edu, fark.com, yahoo.com, and npr.org.
3. Take six pictures with the built-in camera and rename three distinctively.
4. Click on eight specified links to Web pages and documents (4 html, 1 docx, 1 pdf, 1 pptx, and 1 wav file).
5. Download to the root directory of the phone a specified text document and zip file.
6. For the Android: (a) download and install the Facebook app, login, and browse specified pages; (b) download and install the Google Drive app, login/sync, and open three specified files; (c) download and install the DropBox (www.dropbox.com) app, login/sync, and open three specified files; (d) download and install the YouTube app, login, and watch three specified videos; (e) download and install the Audible app, login, and download three specified excerpts; (f) download and install the Kindle app, login, and open three specified PDF files; and (g) download and install the "Reddit Is Fun" app, and visit three specified postings.
   For the iPhone: (a) view three YouTube videos with the installed software;
   (b) create three specified note entries with the installed software; and (c) create three specified reminders with the installed software. (The iPhone

does not allow download of arbitrary software and files.)

3.2 Analysis of the Android Test Phone

On the Android, 5,141 files were recovered pre-reset and 3,578 post-reset, of which 3,292 matched exactly in both path and contents. After deleting partial matches or analogous files (defined as being on filename and hash, hash only, path only, or path ignoring digits), there were 968 pre-reset and 65 post-reset files that did not match in both path and contents between pre-reset and post-reset images. We conclude that 968 files were deleted and 65 were added by the reset. 278 of the post-reset files had zero size of which 227 also had zero size before the reset. The number of executable ".apk" files went from 396 to 277, ".dex" files from 140 to 121, and ".so" files from 302 to 254, so executables were not filtered much by the reset. The "copies and backup" category went from 512 to 33 files, but otherwise the Android reset did not seem to target any particular extensions or directories.

The reset of the Android was not effective at deleting emplaced files as it did not delete any images taken with the camera, nor the created txt, doc, pdf, and ppt files, nor some cache and deleted copies of these files and their image components. (The other Androids similarly did not delete these files, so the operating-system version did not affect this.) The reset did delete most third-party applications, but it had trouble with the Kindle and DropBox applications and left documents of the previous owner of the phone. Using BulkExtractor, 116 links to three visited Web sites were found pre-reset in various files, but all were deleted post-reset.

The reset left intact many operating-system files; 1,971 files with modification times older than one week before the reset were present before the reset and exactly the same number after. Our previous research showed that user data may be contained in operating-system files of settings and logs. Table 1 lists some example files remaining after the reset that could be interesting for forensic purposes. None of the Android phones still had a SD card and directories used to store SD-card data were not specifically searched. However, data was found under 'USERDATA/Root/media/0', which should have been erased during a reset. Again, there is a variety of indirect information about usage in addition to the direct information of the undeleted user files.

Table 1 Some Forensically Interesting Files on the Test Android after Reset

File	Description
CACHE/Root/recovery/last_log	Ascii recovery log
SYSTEM/Root/addon.d \/blacklist	Four hexadecimal MD5 hash values
SYSTEM/Root/etc/apns-conf.xml	Ascii phone carrier IP address
SYSTEM/Root/etc/audio_policy.conf	Ascii audio devices listing
SYSTEM/Root/etc/gps.xml	Ascii GPS settings
USERDATA/Root/backup/pending/journal2114683955.tmp	Data backup
USERDATA/Root/data/com.android.providers.calendar /databases/calendar.db	Ascii calendar data
USERDATA/Root/data/com.android.deskclock/databases /alarms.db	Ascii alarm data
USERDATA/Root/media/0/amazonmp3/temp/log.txt	Ascii log file of Amazon Cloud Player
USERDATA/Root/media/0/Android/data/com.andrew.apollo /cache/ImageCache/3910b1e0ccab19bc46fd9db27cca49c9.0	Binary image cache data

USERDATA/Root/media/0/iPhone3G.2013-11-07.16-39-30 /Email/108/478/1256.sql	Text database script of ours, unclear how it got here
USERDATA/Root/misc/wifi/softap.conf	Ascii access-point data
USERDATA/Root/system/users/userlist.xml	Ascii User ID information
USERDATA/Root/drm/fwdlock/kek.dat	Lock data
USERDATA/Root/media/0/Android/data/com.dropbox.androi d /files/scratch/09thesis_regan.pdf	PDF document of previous phone user

3.3 Analysis of the iPhone Test Phone

On the iPhone, 61,276 files were recovered pre-reset and 43,165 post-reset, of which 42,728 matched exactly in both path and contents; iPhones had more files than Androids. After deleting partial matches (defined as in section 3.2), there were 17,914 pre-reset files and 115 post-reset that did not match, so we conclude 17,914 files were deleted and 115 added by the reset. 36,319 of the post-reset files had zero size of which 36,292 were also had zero size before reset; that indicates that zero-size files after the reset convey some forensic information since they are almost certainly present before the reset. The number of executable ".app" files went from 24,862 pre-reset to 8,062 post-reset, but the number of files of all kinds in recognizable operating-system directories went from 29,812 to 27,621, so the operating-system files were generally preserved.

The reset on the iPhone did well in deleting most files put on it by user activity, due to Apple's tighter control on what can be put on the phone. All the images and documents were deleted by the reset except for some cache and settings information from YouTube, and all third-party software except for Facebook. Table 2, however, lists example files remaining after

Table 2 Some Forensically Interesting Files on the Test iPhone after Reset

File	Description
System/InnsbruckTaos11B554a.N90OS/System/Library/ PrivateFrameworks/Preferences.framework/ SupplementalLocaleData.plist	Binary location and language settings
System/InnsbruckTaos11B554a.N90OS/usr/share/ mecabra/ja /rerank.dat	Binary resource rankings
Data/Data/Keychains/keychain-2.db	Ascii keys
Data/Data/logs/lockdownd.log	Ascii security event log
Data/Data/mobile/Applications/B8AD4B05-2518-4570-8447-7BE2BFDA8F9F/Library/Preferences/ com.apple.mobilesafari.plist	Ascii browser preferences
Data/Data/mobile/Library /BulletinBoard/SectionInfo.plist	Ascii bulletin board index
Data/Data/mobile/Library/Caches /com.apple.springboard /Cache.db-wal	Ascii screen cache for user "wal"
Data/Data/mobile/Library /Cookies/com.apple.itunesstored.2.sqlitedb	Ascii cookies for iTunes
Data/Data/mobile/Library/Mail/Content Index	Nonrandom encoded mail keywords
Data/Data/mobile/Library/Maps/Bookmarks.plist	Ascii map bookmarks
Data/Data/mobile/Library /Preferences/com.apple.identityservicesd.plist	Ascii account information
Data/Data/mobile/Media/PhotoData/changes-shm	Incremental photo data

File	Description
Data/Data/root/Library/Caches/locationd /consolidated.db	Ascii location data
Data/Data/tmp/MediaCache /diskcacherepository.plist	Ascii disk cache information

the reset that could be interesting for forensic purposes by providing indirect information about what the user was doing. Despite Apple's claims (Apple, 2014) of using AES-256 hardware encryption to protect user data and deleting the key during a factory reset, we did find unencrypted data in the form of Ascii files in cache, log, and preference files though its precise purpose was unclear. 115 new post-reset files did include files of forensic value in directories UserSettings, EffectiveUserSettings, com.apple.mobilemail/Cache, fsCachedData, photostream, and bulletinboard, apparently from the reset and subsequent rebooting, and Table 2 includes some examples.

"Preferences" can include private user information (Zhu et al., 2014) though we saw none here. However just using the data we found using BulkExtractor, an investigator could determine where the user was, when and how they used the device, their deleted applications, network configuration, cache data, keywords, and even some plaintext keys.

Timeline analysis showed the reset reduced the number of files with modification times within the last month from 18,000 before the reset to 500 after the reset. On the other hand, of the files with modification times earlier than one week before the reset, there were 43,984 before the reset and 42,468 after. It appears that older files are rarely deleted in a reset, but it is unclear whether this is due to their timestamps, location, or contents.

3.4 Effects of Alternative Resets

Most devices provide an alternative "hardware reset" using the hardware keys (with many different device-specific procedures described on factory-reset.com), and this is usually coupled to rebooting. On the test Android, the hardware reset gave a new menu which enforced a "cache reset" as well (an option for the software reset). An image after this kind of reset was taken on our test Android after the regular reset, and 3391 files out of 3578 remained identical. It did not delete any of the files and media put on the device, and deleted only the sixth interesting file in Table 1. Only four files all with extension "db" were deleted, two for Bluetooth and two for "optables". Six new files were added, two Bluetooth cache files and four "telephony" files. Thus it appears that the cache reset does not do much beyond the regular reset, though it apparently does not execute identical code.

The iPhone hardware reset just sends the user to the regular reset "Erase All Content and Settings" used in section 3.2. But newer iPhones provide six additional software reset options that can confuse users: "Reset All Settings", "Reset Network Settings", "Reset Keyboard and Dictionary", "Reset Home Screen Layout", and "Reset Location and Memory". In our experiments, all of these were selected, an image taken, and the results were compared to that of just doing the first option. 222 additional files were deleted and 144 were added to the 43,165 files, so it did delete additional files, but nothing in Table 2. No obvious patterns were discerned in the deletions. Thus it appears that the additional reset options do not affect very much though they do not execute identical code as the regular reset.

We also employed a "firmware reset" to restore the test Android back to the standard Android operating system after a regular reset. We then took an image, did a regular software reset, took an image, did another software reset, and took a final image. The second regular reset deleted 161 files and added 259, and the third regular reset deleted

98 and added 88. This shows that effects of the firmware reset were inconsistent even on a previously reset device, which suggests opportunities for investigators.

4. EXPERIMENTS WITH A SET OF DEVICES

4.1 The Mobile Corpus Used

To see how general this analysis was, pre-reset and post-reset images of 21 previously owned devices were analyzed (Table 3). Some were from the Real Data Corpus (Garfinkel et al, 2009) of drives purchased as used equipment and were unmodifiable. Others were smartphones that have been used for other research projects at our school and were modifiable. Additional files were created and downloaded for the modifiable devices similarly to the experiments in section 3. None of the phones were password-protected and no data were explicitly encoded or encrypted. Unlike in section 3, the devices were not reset before taking pre-reset images (and the two phones of section 3 were imaged before the tests reported there) to test persistence of a wider range of files.

Table 3 Devices Tested in Our Mobile Corpus

#	**Device**	**OS Version**	**Status**
p1	Apple iPhone 4	5.1.1	OK
p2	Apple iPhone 4	5.1.1	OK
p3	Apple iPhone 2	3.1.3	OK
p4	Apple iPhone 2	3.1.3	OK
p5	Apple iPhone 2	3.1.3	OK
p6	Apple iPhone 2	3.1.3	OK
p7	Apple iPhone 2	3.1.3	OK
p8	Apple iPhone 2	3.0	OK
p9	Samsung Galaxy SIII	CM 10.1	Hard reset only
p10	Samsung Nexus	CM 10.1	OK
p11	Samsung Galaxy Anycall	1.5	OK
p12	Motorola Atrix 4G	2.2	OK
p13	HTC Droid Eris	2.1	OK
p14	HTC Magic	1.6	Hard reset only
p15	HTC Flyer (tablet)	3.2	OK
p16	HTC One	4.1.2	OK
p17	BlackBerry 8900 Curve	4	Unusable after reset
p18	Apple iPhone 4S	5.1.1	OK
p19	Apple iPhone 2G	3.13	Unusable without SIM card
p20	BlackBerry 8100 Pearl	4.5.0.174	OK
p21	BlackBerry 8300 Curve	4.5.0.162	OK
p22	Motorola FIRE	2.3.4	Unrecognized by Cellebrite
p23	Huawei U8500	2.1	OK
p24	Huawei U8150 IDEOS Comet	2.2	Unusable after reset
p25	Dell XCD35	2.2	OK
p26	Apple iPhone 2	3.1.3	Unusable after reset
p27	Motorola Charm	2.1	Totally dead
p28	LG-500GHL	Unknown	Unrecognized by Cellebrite

The table lists the devices tested, with a variety of manufacturers and operating-system versions to provide breadth to experiments. Very few files were found on the BlackBerry images and no software, so Cellebrite appears to have had trouble imaging them. Those not identified as Apple or BlackBerry were Google Android devices, and two had a custom operating system CyanogenMod 10.1. The table indicates several problems in using the devices, resetting them, and analyzing them. Some devices (p22 and p28) could not be handled at all by Cellebrite. Some devices (p27) were apparently faulty. Some (p19) had special requirements that could not be accomplished. Some (p9 and p14) had special requirements for reset. Some (p17, p24, and p26) had a too-efficient reset that made the devices subsequently unable to restart. Also, four phones needed to be processed more than once due to Cellebrite crashes. It appears that forensic investigators will need to accept a significant failure rate in attempts to analyze devices they acquire.

4.2 Effects of Resets on File Counts

Many files were unchanged by the reset. Table 4 gives a summary of pre-reset and post-reset file counts. As before, there were four types of partial matches between pre-reset and post-reset: filename and hash (typically, when a file is moved), hash only (when a file is copied), path only (when a file is modified), and path ignoring digits (for temporary files). The "unmatched" files post-reset are interesting as they represent new records created by the reset itself and routine operating-systems activity. As we saw in section 3, resets do not simply erase devices; they delete many files, but rename others and add some new ones.

Table 4 Summary Data on the 21 Usable Devices

File count type	**Pre-reset**	**Post-reset**
Total files	349,915	200,987
iPhone files	299,058	176,907
Android files	50,846	24,058
Exact matches pre-reset and post-reset	140,320	140,320
Subsequent matches on filename and hash value but not all directories	34,228	36,540
Subsequent matches on hash value alone	9,269	12,911
Subsequent matches on full path alone	2,849	2,836
Subsequent matches on full path ignoring digits alone	6,448	256
Remaining unmatched	156,801	8,124

To get a better understanding of what kinds of files are being removed, files were classified by type of file extension (E) and type of the immediate directory (D) (Table 5). Our current taxonomy classifies 8,346 extensions and 6,445 directory names, labeling the rest as "miscellaneous". Proposed extensions longer than 10 characters were ignored, and the file path above the bottom-level directory was searched until a directory was found which could be classified.

Overall, it appears that resets preponderantly target files with extensions of pictures, video, documents, copies and temporaries, disk images, logs, XML and games. They had little effect on extensions of operating-system files, configuration files, and executable files. Results were similar with classifying files by immediate directories. The resets primarily targeted files in directories mentioning pictures, video, documents, temporaries, Web pages, applications, and games. They had little effect on directories of

the operating system, security, and the root. Thus resets appear to predominantly target third-party software and some (but not all) categories of likely user files, but ignore user data in the operating system and other configuration data. We observed that the number and types of files deleted did not differ significantly on the more-recent operating systems (p10, p15, p16, and p18).

Table 5 File Type Counts Before and After Reset

Type of file	Count before reset	Count after reset
E: No extension	36561	21078
E: Operating system	106168	104406
E: Graphics	98618	27522
E: Camera pictures	15443	3967
E: Temporaries	733	159
E: Web pages	1418	680
E: Documents	3089	1233
E: Spreadsheets	425	356
E: Compressed	601	278
E: Audio	16427	8313
E: Video	303	90
E: Source code	1791	736
E: Executables	3432	2856
E: Disk image	13828	1932
E: Log	599	73
E: Copies and backup	7347	905
E: XML	5193	1045
E: Configuration	20788	18379
E: Games	3741	1048
D: Root	1012	966
D: Operating system	122625	117701
D: Hardware	1128	319
D: Temporaries	12141	2928
D: Pictures	17950	4328
D: Audio	10812	7814
D: Video	2570	0
D: Web	2714	277
D: Data	18300	9771
D: Programs	3616	2876
D: Documents	6211	1036
D: Sharing	7500	2368
D: Security	2953	2749
D: Games	53722	0
D: Applications	84593	46696

Zero-size files increased (120,112 before and 128,026 after) but files whose path contained the word "DELETED" decreased (20,087 before and 4,181 after). Files are designated for deletion for a good reason and it would seem reasonable to delete them in a reset. Zero-size files are useless to software, but may provide information about the user just in their zero size, as for instance empty log files that say the user has not done anything in the category of the log. Investigators should be aware that the Cellebrite software reported different fronts of the paths, and also different creation and access times, on the same image with different releases of their software.

4.3 Cellebrite Analysis of Files

The devices were previously used for a variety of purposes. Specific kinds of information within files were searched for using the Cellebrite Physical Analyzer (Tables 6, 7, and 8). The rows correspond to Cellebrite categories and the type codes are I=iPhone, A=Android, and B=BlackBerry. Cellebrite describes its categories as:

- Application usage: application name, number of launches, activations, active time, and date
- Call log: caller phone number, time stamp, duration, and type (incoming, outgoing, or missed)
- Contacts: contacts name, organizations, phone number, emails, other entries, notes, and addresses
- Cookies
- Installed applications: application name, version, identifier, application ID, purchase date, and delete date
- IP connections: timestamp, domain, router address MAC address, Cellular WAN, Device IP, DNS address, and service name
- Locations: timestamp, position, and name
- Maps: source, zoom level, and tiles
- Passwords
- SMS messages: timestamp, type of folder, phone number, text string, and sending status
- User accounts: name, user name, password, and service type
- User dictionary: word, locale, and bookmark note
- Wireless networks: last connected, BSSId, SSId, and security mode
- Content file types: picture images, audio, text, databases, configuration, application
- Directory information: name, path, size, metadata, created, modified, accessed, bookmark note

One lesson of these tables is that effects of resets differ between devices. To confirm the results, the extracted data were viewed in the Physical Analyzer. Nearly all the connection data in both sets was removed after a reset, including call logs, contacts, cookies, IP connection data, SMS data, maps, passwords, and user directories. But location data were left on p6 (an IPhone) of latitude and longitude for a cell tower and a corresponding time stamp. This is sensitive user information since it reveals the when and where a user has been. Null account data were found on several devices indicating that a user account had existed at some point. Null wireless network data also occurred indicating a previous wireless connection.

Applications data generally only contained information from first-party software installed on the phone, indicated by the identifier com.appl for iPhones and com.google for Android phones. The data was contained various framework, library, and plug-in information for system software including maps, video, mobile mail, calculators, weather, preferences, and mobile notes which could be considered user data. The application data on p16 contained user-account information before the reset, but the Physical Analyzer mislabeled it as installed applications. It also could not identify any installed applications on the p7 and p8 iPhones after the factory reset but there must have been some or the phone would not have functioned.

Table 6 Data Counts (Post-Reset/Pre-Reset) on Test Devices, Part 1

Phone	**p1**	**p2**	**p3**	**p4**	**p5**	**p6**	**p7**	**p8**
Type	I	I	I	I	I	I	I	I
App. Usage	0/0	0/0	1/199	0/0	1/125	1/56	9/23	0/23
Call Log	0/0	0/2	0/103	0/0	0/107	0/104	0/13	0/105
Contacts	0/0	0/0	0/209	0/0	0/1461	0/2366	0/0	0/284
Cookies	0/0	0/0	0/5	0/0	0/0	0/43	0/0	0/6
Installed Apps.	34/34	34/34	23/127	28/34	23/142	23/56	0/24	0/79
IP Connections	0/2	0/2	0/2	0/1	0/0	0/1	0/0	0/7
Locations	0/0	0/0	0/1	0/0	0/0	5/10	0/0	0/72
Maps	0/0	0/0	0/12	0/0	0/0	0/2	0/0	0/19
Passwords	0/6	0/5	0/0	0/1	0/0	0/0	0/0	0/0
SMS Messages	0/0	0/2	0/30	0/0	0/1152	0/50	0/0	0/672
User Accounts	0/0	1/1	1/1	1/1	1/1	1/6	1/1	1/3
User Dictionary	0/0	0/1	0/161	0/0	0/30	0/312	0/0	0/819
Wireless Networks	0/0	1/1	0/1	0/0	0/0	0/0	0/0	0/0
Images	3714/ 3716	3715/ 3716	2488/ 16541	2631/ 2716	2488/ 25106	5888/ 14477	2491/ 2611	2488/ 13705
Audio	1/1	1/1	2/2512	1/1	2/1202	2/1125	2/2	2/1120
Text	159/161	159/164	11/392	20/34	11/1689	12/67	12/21	12/135
Databases	31/38	32/43	13/60	21/50	23/54	12/63	13/24	23/55
Configuration	2797/ 2969	2831/ 2959	1349/ 4798	1976/ 2969	1352/ 6978	1345/ 2237	1348/ 1382	1349/ 10930
Applications	6/ 6	6/ 10	164/ 489	227/ 304	164/ 458	164/ 200	164/ 310	164/ 670

Table 7 Data Counts (Post-Reset/Pre-Reset) on Test Devices, Part 2

Phone	**p9**	**p10**	**p11**	**p12**	**p13**	**p14**	**p15**	**p16**
Type	A	A	A	A	A	A	A	A
App. Usage	0/0	1/139	0/0	0/102	0/0	0/0	0/0	0/0
Call Log	0/0	0/0	0/0	0/52	0/5	0/6	0/0	7/192
Contacts	0/0	0/5	0/0	0/48	0/0	0/2	0/0	0/65
Cookies	0/0	0/3	0/0	0/0	0/0	0/5	0/0	0/0
Installed Apps.	30/30	48/102	25/43	23/32	26/70	20/24	12/44	0/0
IP Connections	0/0	0/2	0/0	0/3	0/0	0/1	0/0	0/0
Locations	0/0	0/0	0/5	0/0	0/10	0/0	0/0	0/0
Maps	0/15	0/5	0/8	0/0	0/0	0/0	0/0	0/0
Passwords	0/0	0/0	0/0	0/1	0/0	0/1	0/1	0/0
SMS Messages	0/80	0/5	0/0	0/121	0/0	0/2	0/0	0/66
User Accounts	1/1	1/1	0/0	0/0	0/1	0/1	0/0	0/1
User Dictionary	0/132	0/50	0/0	0/84	0/40	0/1	0/0	0/0
Wireless Networks	0/1	0/1	0/0	0/1	0/0	0/0	0/1	0/0
Images	150/ 150	764/ 764	11 /11	1815/ 1815	42/ 42	15/ 15	9/ 9	616/ 616
Audio	1/1	1/1	1/1	1/1	0/0	4/4	1/1	243/26 3
Text	130/13 0	48/48	0/0	132/13 2	1/1	0/0	4/4	1/1
Databases	5/65	12/45	0/0	25/41	0/0	10/24	0/0	16/36
Configuration	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
Applications	0/0	313/31 3	0/0	7/7	3/3	1/1	24/24	0/3

Table 8 Data Counts (Pre-Reset/Post-Reset) on Test Devices, Part 3

Phone	**p18**	**p20**	**p21**	**p25**
Type	A	I	B	B
App. Usage	0/0	0/0	0/0	0/0
Call Log	0/1	0/100	0/11	0/61
Contacts	0/0	0/477	0/0	5/252
Cookies	0/17	0/0	0/0	0/16
Installed Apps.	34/34	0/0	0/0	0/1
IP Connections	1/6	0/0	0/0	0/0
Locations	0/0	0/0	0/0	0/9
Maps	0/0	0/0	0/0	0/0
Passwords	5/9	0/0	0/0	• 0/1
SMS Messages	0/0	0/4	0/0	0/76
User Accounts	1/1	0/0	0/0	0/2
User Dictionary	0/6	0/0	0/0	0/2
Wireless Networks	3/7	0/0	0/0	0/1
Images	3716/3743	0/ 7	0/3	71/159
Audio	1/1	0/1	0/0	1/1
Text	243/263	0/0	0/0	440/3031
Databases	37/58	0/0	0/0	24/55
Configuration	2850/2953	0/0	0/0	0/0
Applications	6/6	0/0	0/0	388/390

The Androids did not delete any user pictures. The iPhones did a better job and no pictures including thumbnails were viewable after the factory reset. However, metadata (name, file path, size, created, modified, accessed) for the images was still viewable in the Physical Analyzer and this could violate privacy. Audio data were not removed from any of the Android set, including wav audio files from applications and user-downloaded mp3 files. The iPhone set deleted most of the audio files, but some WAV files were still recoverable from the operating system and third-party software, and could be played on a media player. Database data (db, sqlite, and sql) were recovered from both sets but did not include any user data. What Cellebrite called configuration data was recovered from the iPhones but only contained system-file access data.

4.4 String Searches in Post-Reset Files

String searching was also done with Bulk Extractor for specialized kinds of strings, including those within encoded files such as compressed files, and with the Unix "grep" for Ascii strings in text files. We chose a sample of keywords indicating possible user-related security information including "password", "root certificate", "hash", "cert", "SHA1", "MD4", and "SSL". The p10 Android phone with Cyanogen was the only one that returned a value with the "password" keyword after reset, in an XML file under the Cyanogen system directory that contained website URLs and user names with passwords stored in clear text. All phones returned at least one file that contained the "root certificate" phrase and had a length between 115 and 144. Searches for the strings "hash", "cert", "SHA1", "MD5", and "SSL" matched some configuration files, but they did not appear to contain any user data. "Hash" occurred in post-reset configuration files for iPhones on which we found the application "Rocky Racoon" (p3, p4, p5, p6, p7, and p8), an application on "jailbroken" iPhones that try to circumvent the operating system. Such unauthorized software can damage a phone and may have affected the data.

Bulk Extractor also found email addresses, fax numbers, and phone numbers within files. However, most findings were in manuals, acknowledgements, service agreements, and support information for system software, recognizable by such strings as "@tech" and "@helpdesk" and 1-800 information phone numbers. The reset did appear to remove user-account and Wi-Fi information. However, Bulk Extractor found several text files with IP addresses and domain names. Geolocation data were found along with timestamps on p18, enabling a view of the locations at which the phone had been used.

Bulk Extractor claimed to uncover text files that were not found by Cellebrite, for an additional 157 user files on the Android phones. Some of these were left behind by third-party applications such as DropBox where the reset removed the software but not all the data. These included Microsoft Office files (Word, Excel), Adobe PDFs, and MP4 video files.

5. CONCLUSION

Files and data on 21 devices were analyzed before and after a "factory reset" and a variety of residual user information was found. Android devices did not delete most emplaced user files in the reset, and both Android and iPhones did not delete a variety of indirect data from and about users. On average 42% of the files on a device were deleted by the reset, with pictures, documents, copies, temporaries, logs, drive images, and games singled out for predominant removal, though some examples of each of these were spared. Modified files were also found after the reset, and even some new files, which reflected routine system operations. The year of the operating-system release did not affect results much. 7 of our original 28 devices could not be imaged either post-reset or pre-reset, so there was a significant failure rate which will probably be similar for other investigations of mobile devices.

These results show that much can be understood about resets without having to reverse-engineer operating-systems code. The results were dependent on Cellebrite software, and it appeared to miss 157 files on the Androids. However, it is the major vendor of mobile-device forensic software and has had years of successful use, so the data it provided is likely highly accurate.

These results have implications both for forensic investigations and for user privacy. Users are confronted with confusing choices for resets on both the iPhone (six options) and the Android (three options), so they may not reset what they want, and this provides a forensic opportunity. Even with a proper reset, Androids do not delete much of forensic interest, and both Androids and iPhones left plenty of clues to the device usage in the remaining files, although it becomes harder to extract them once a device has been reset. Software applications were major targets of the resets, but they are only occasionally interesting forensically. The number and kinds of files that were recoverable after the reset varied between devices and operating-system versions, consistent with the experiments of (Kubi, Saleem, and Popov, 2011) with extracting other kinds of data from mobile devices, so there are few guarantees about what gets deleted.

As for implications for user privacy, further measures need to be taken by users. Users can encrypt their data, though it imposes an additional burden on them and it was not seen on our devices. For now, a user wishing to discard or give away the device, should (1) do a software or "factory" reset; (2) manually delete any remaining user files that have been moved to unconventional locations (like a compressed file in the root directory); (3) manually delete remaining user data from software directories; (4) delete remaining cache files, browser history files, cookies, and settings files; (5) delete zero-size files; (6) overwrite deleted data with zeros; (7) remove the SIM card and any other removable storage. Commercial software such as data erasing tools will be generally necessary for steps 2, 3, and 6.

ACKNOWLEDGEMENTS

This opinions expressed are those of the authors and do not represent the U.S.

Government. Simson Garfinkel provided the corpus and contributed ideas, and Gavin Sonne assisted with the research.

REFERENCES

Alghafli, K., Jones, A, and Martin, T. (2012). Forensics data acquisition methods for mobile phones. Proceedings of 7th International Conference for Internet Technology and Secured Transactions, 265-269, December 2012.

Apple Inc. (2014). iOS: Understanding 'Erase All Content and Settings. Retrieved on May 1 from support.apple.com/ kb/ht2110.

Cardwell, S. (2011). Residual Network Data Structures in Android Devices. M.S. thesis, Naval Postgraduate School. Retrieved on September 13, 2013 from www.dtic.mil/cgi-bin/GetTRDoc ?Location=U2 & doc=GetTRDoc.pdf &AD=ADA552175.

Garfinkel, S. (2013). Digital media triage with bulk data analysis and bulk_extractor. *Computer & Security 32,* 56-72.

Garfinkel, S., Farrell, P., Roussev, V., and Dinolt, G. (2009). Bringing Science to Digital Forensics with Standardized Forensic Corpora. *Digital Investigation 6,* S2-S11.

The Guardian. (2013). Recycled Mobile Phones Retain Previous Owner Data. *Infosecurity Magazine*, retrieved September 13 from www.theguardian.com/media-network/partner-zone-infosecurity/ mobile-phones-previous-owner_data.

Kauffman, R., Lee, Y., and Sougstad, R. (2009). Cost-effective investments in customer information privacy. Proceeding of the 42nd Hawaii Intl. Conf. on Systems Sciences, 1-10.

Kubi, A, Saleem, S., and Popov, O. (2011). Evaluation of Some Tools for Extracting E-evidence from Mobile Devices. 5th Conference on Application of Information and Communication Technologies, Baku, Azerbijan, October, 1-6.

Marturana, F., Me, G., Berte, R., and Tacconi, S. (2011). A Quantitative Approach to Triaging in Mobile Forensics. Prof. IEEE TrustCom, 582-588.

McMillan, J., Glisson, W., and Bromby, M. (2013). Investigating the increase in mobile phone evidence in criminal activities. 46th Hawaii International Conference on System Sciences, 4900-4909.

Omeleze, S., and Venter, H. (2013). Testing the harmonized digital forensic investigation process model–Using an Android mobile phone. Proceedings of the Conference on Information Security for South Africa, August, 1-8.

Owen, P., Thomas, P., and McPhee, D. (2010). An Analysis of Digital Forensic Examination of Mobile Phones. Proc. 4th International Conference on Next Generation Mobile Applications, Services, and Technologies, Amman, Jordan, July.

Payton, T., and Claypoole, T. (2014). *Privacy in the Age of Big Data*. Lanham, MD, US: Rowman and Littlefield.

Rouse, M. (2014). Hard Reset. Retrieved on February 7 from whatis.techtarget.com/ definition/hard-reset-factory-reset-master-reset.

Rowe, N. (2013). Identifying forensically uninteresting files using a large corpus. 5th International Conference on Digital Forensics and Computer Crime, Moscow, Russia, September.

Smith, J. (2012). Security guru: Don't sell your Android Phone until turning it into Swiss cheese. *GottaBeMOBILE: Mobile News & Reviews*, February 27.

Zhu, H., Chen, E., Xiong, H., Yu, K., Cao, H., and Tian, J. (2014). Mining mobile user preferences for personalized content recommendation. *ACM Transactions on Intelligent Systems and Technology*, to appear.

