Effectiveness of Mobile Wiping Applications

Kevin Jochims, Andres Bello, and Kim-Kwang Raymond Choo(✉)

Department of Information Systems and Cyber Security,
University of Texas San Antonio, San Antonio, TX 78249, USA
{kevin.jochims,ren574}@my.utsa.edu,
raymond.choo@fulbrightmail.org

Abstract. Given the considerable amount of data (including sensitive and personal information) collected, stored, disseminated by mobile devices, there is a need to ensure that such devices can be securely wiped when they are misplaced, stolen or disposed. Hence, in this paper we evaluate the effectiveness of three categories of wiping applications: Factory Reset, Remote Reset, Data Wiping Applications (apps). Specifically, we study two popular wiping apps (i.e., Shreddit – Data Eraser by PalmTronix, and Secure Wipe by Pinellas CodeWorks) and install both apps on three test devices, namely: Samsung S5 (Android 6.0.1), Samsung S5 Active (OS version 6.0.1), and an iPhone 6S (iOS 13.2.2). We then study the extent of data that can be recovered, from the three categories of wiping, using two popular commercial mobile forensic software, namely: Mobile Phone Examiner Plus (MPE+) from Accessdata, and MOBILedit from Compelson labs.

Keywords: Remote wiping · NAND memory · Mobile forensics · Secure data deletion · Android forensics · iOS forensics

1 Introduction

Advances in mobile device technologies (e.g. processing speeds, and memory capacity) have partly contributed to significant growth in the sales of mobile devices, particularly smartphones [1–5]. Contemporary mobile devices are capable of collecting, accessing, storing and disseminating a broad range of information (e.g. user physiological data, user credentials, and other personal identifiable information – PII) [6–8]. However, leakage or unauthorized access to such information can be (ab)used to facilitate criminal activities such as identity theft [9, 10]. For example, there has been a growing trend of individuals taking compromising or nude photos with their mobile devices, as evidenced by a number of studies [7], such as the Pew Internet study. The latter study found that an increasing number of young adults are now using their smartphones to exchange sexual pictures and sexual conversations (also referred to as sexting) [7]. In 2011, sexting was identified as one of the top 10 major health concerns for youth [7]. As of 2019, over 27% of adolescences (aged between 13 and 15) have either sent or received nude pictures from sexting [11], and according to a Cosmopolitan Magazine poll [12], up to 90% of the Millennial women admitted to taking nude photos of themselves. Milne's [13] study

D. Perakovic and L. Knapcikova (Eds.): FABULOUS 2021, LNICST 382, pp. 3–24, 2021.
https://doi.org/10.1007/978-3-030-78459-1_1

shows the effects and trauma from loss of sensitive and personal information can resulted in monetary, social, physical, and psychological harms or damages. Associated consequences also include loss of self-esteem or sense of worth, and in some cases fatality. The fast pace of users replacing their mobile devices (estimated to be approximately every two years) reinforce the importance of ensuring users are able to securely wipe data from such devices, particularly sensitive information.

Newer Android and iOS devices, for example, have built in encryption and factory reset features. The latter feature is used to wipe a device of user data and return it to a sanitized state. This feature only works if the individual has direct access to the device, but with theft and loss, users need the ability to perform a remote initiated wipe of user data from the device. There are times where a user wishes to only wipe recently deleted data that can be carried out using third-party mobile apps.

However, there are a number of questions associated with the utility of these third-party mobile apps. For example, how effective are such third-party apps, have factory resets improved enough to prevent data recovery, and are remote initiated wipes as good as a factory reset? This is the focus of this paper. Specifically, in this paper we study two popular wiping apps namely: Shreddit – Data Eraser by PalmTronix, and Secure Wipe by Pinellas CodeWorks. Data, programs (apps). We attempt data recovery following a factory reset, using two popular commercial mobile forensic software, namely: Mobile Phone Examiner Plus (MPE+) from Accessdata, and MOBILedit from Compelson labs.

In the next section, we will briefly introduce data deletion and the extant literature.

2 Background and Related Work

2.1 Data Deletion

There are two main categories for deleting files on a digital device: namely: deletion and secure data deletion [3, 5, 14–17]. For most operating systems, when a user "deletes" a file, just the metadata for that file (e.g. in the Master File Table (MFT) for a NT file system (NTFS)), is changed, and the drive space the old data bits occupy is marked as unallocated. Using forensic tools can potentially allow a user to recover the deleted data [3, 5, 15–17]. A secure data deletion, on the other hand, is designed to compound the challenge of recovering deleted data.

There are three ways to accomplish a secure data deletion of a smartphone with no physical impact to the device; providing the device is available to the user. The first option is to use a third-party software (e.g. app) that focuses on wiping just the unallocated areas/space on the device. The next option is to perform a factory reset of the device. The last option is to encrypt the data on the phone (and deleting the decryption key) [15–32].

Smartphones read and write data slightly different than other computer systems, and generally store data in three partitions, namely: system data, internal flash data storage, and external data storage (e.g. SD card) [19]. The internal data is a form of flash media called NAND. It is designed with multiple blocks filled with tiny memory cells [15, 16, 20]. When the device wants to write new data, bits are stored in the empty cells of a block and a logical address pointer is created and mapped to the file. When a delete command is made for a file, the logical address pointer for that file is redirected to an empty space

in a block, making the data available for erasure. With no moving parts NAND memory is very fast and allows for higher storage capacity [3, 15, 16, 20].

There is one limitation associated with NAND; whereas disk drives can be re-written on the fly, the data marked for deletion must be erased prior to writing new data in that cell, [3, 16–20] with NAND the erasure is done on the block level, not bit by bit [15, 20]. The erasing function in NAND memory is hard on the cells creating a limit to how many times data can be erased and written to it. Yang et al. [15] express that failure is typically after 104 to 105 cycles, and the block use is balanced through wear levelling.

Prior to transferring ownership of a phone, additional steps should be taken to ensure all PII is removed. For use with third-party wiping apps, manually locate and delete data, with PII, and delete any installed apps that may contain PII. Third-party software only wipes the data blocks that are marked as unallocated; not active data locations. Since deletion is performed at the block level, fragments of old data may still be present in un-erased blocks, although these data fragments may not be visible without the use of appropriate forensic tools. A factory reset is designed to return the phone to a generic initial state, with all user apps and user data removed. Both iOS and Android devices have the ability to perform a factory reset.

Prior literature on factory resets has shown that Apple iOS has performed well since version 4.0, with very minimal or no data recovered. In Android devices running versions 2.3 to 7.0, varying amounts of deleted data could be recovered after factory reset [12, 15, 16, 19, 25–27, 30]. For example, Khramova [12] tested 68 Android phones from nine different manufacturers, running versions from 2.3 to 7.0, and was able to recover data from these phones after a factory reset.

2.2 Remote Wiping Apps

When a device is misplaced or stolen, the user will not be able to physically activate the factory reset option. In circumstances like this, a remote wiping app could be used. Such an app can be downloaded from the manufacture's website (Samsung, Apple, Google, HTC, etc.), the official OS site (Google for Android, Apple for iPhones, etc.), or a third-party app store. The first two options usually come by default as the phone is activated and the user sets up their accounts with the OS or manufacture's website [33].

A number of major anti-malware companies have also put out remote wipe apps like Norton's Mobile Security, Avast's Anti-theft, or Bitdefender's Anti-Theft. These apps do require a purchase, but there are free apps available. Such free apps require some software installed on the phone prior to use. Research has shown there is extensive data on factory resets of smartphones running OS versions prior to 2014, but limited data is available on the effectiveness of remote wiping applications [33].

In the next section, we will briefly explain how remote wiping apps work.

3 Remote Wiping Apps and Their Effectiveness

3.1 How Remote Wiping Apps Work

Remote wiping capabilities are commonly available from the mobile device manufacturer or through third-party apps that can be enabled by the device's user or managed

services with access to the device. The objective of remote wiping is to securely delete user data stored in the mobile device whether it is stored in the manufacturer's delivered applications or third-party apps installed and enabled by the device user.

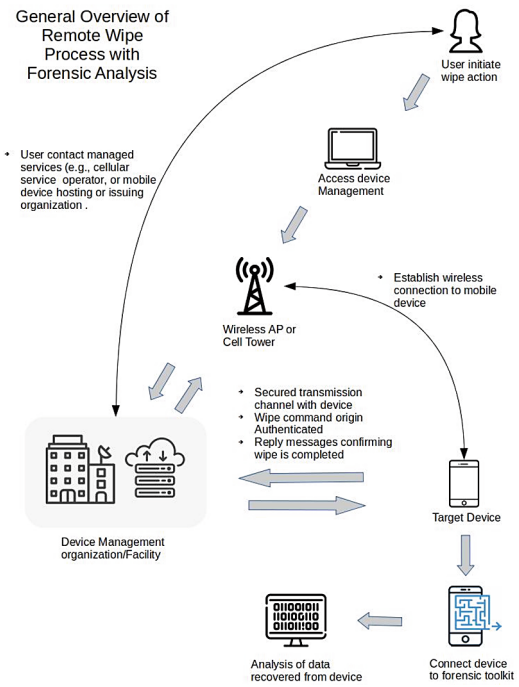

Fig. 1. Remote wiping process initiated by user (adapted from [34]).

Figure 1 illustrates the general request process for remote wiping of mobile devices. The user can access management utilities (typically provided by the organization managing the cellular service, or hosting the device such as the case of organizations that issue mobile devices to employees, or third-party apps) through another device. The user could select predefined options for the wiping functions such as low-level formatting, factory reset, data deletion, removal of header only or full clearing of dedicated storage areas in the device including unallocated areas. Alternatively, the user can contact the device management organization/facility directly to initiate the wiping process. Once a secured connection is established between the device and the management organization or facility the wipe commands are authenticated between the device and the device management organization/facility [27, 34]. Reply messages confirming the completion of phases of the wiping process or summary message indicating the full completion of the process are transmitted to the device management organization/facility. These messages would be sent back to the user in case (s)he is the origination point and logged-in at the device management organization.

An example of a manufacturer wiping process is the patented process of Apple [35], which starts with accessing the remote management account facility. In the process, it

is assumed that the commands can be initiated from devices connected to a network, for example a web service. The web service accessing the remote account functions is able to generate and transmit command messages. Additionally, it is able to receive transmitted messages from the remote devices to acknowledge the completion or failure of the original command transmitted. The centralized device management system will display the mobile devices available to the user for the wiping functions. Once a device selection is made, the user can select the commands that will execute a specific wiping command. A remote command message is generated that will instruct the remote device to execute the wiping function. It should be noted that the remote command is generated and transfer to a server that will publish it thru the available network and reach the device selected. Once the wiping command is executed in the remote device, a message is generated and transmitted back to the management account facility via the available network and routing server to the web service that originated the initial command. The message will carry the completion status of the wiping process (success or failure). Once complete, the user is able to select other remote commands for the same device or select a different device and start the same process again.

In addition to manufacturer's wiping applications, mobile users can install third party applications in their mobile devices to execute wiping commands [28]. For example, the process patented by Air Watch LLC [36] establishes connection with the mobile device and start a two-command process: backup data from the mobile device and issue a wipe command. Through a centralized management facility, that can be accessed by a web service, the user can select to back up the data from the remote device and wipe it, back up the data from the remote device, or just wipe the data without backing it up. Once the user has made a command selection, based on the network availability, the command is issued and routed to a server for publishing. If the user selects the backup and wiping functions, a separate message is generated for each command. In this scenario, the backup command is executed first to ensure that the data is transmitted from the remote device and backed up by the centralized management facility. Once the backup confirmation is received; then, the second command to wipe the data is generated and transmitted to the remote device. Finally, once the data has been wiped out, the remote device generate and transmit a message confirming that the data wiping has been completed [27].

3.2 Effectiveness of Remote Wiping Apps

In the last two patented processes reviewed, on remote data wipe of devices, the user relies on messages generated and transmitted by the remote device to verify that data wiping took place [37]. b However, detailed information on the deletion method is not readily available from the messages transmitted from the remote device. It is not specified whether the wiping process performed a physical or logical deletion of the user data, and whether traces of user data are left behind. Therefore, to verify the wiping process was effective and to identify user data that might have been left behind on the device, forensic toolkits are required to perform in depth analysis. Previous research conducted have determined that in addition to user data, residual network and cloud storage application data can still be found and in devices that were remotely wiped. Furthermore, there could be significant differences among devices and whether the remote wipe was executed using a manufacture's wiping process or a third-party application [26]. Other

considerations in the effectiveness of remote wiping include security of the transmission of command messages generated to wipe information in remote devices, and the receiving messages confirming completion of the wiping command. Additionally, the handling of interrupted messages and capabilities to regenerate, re-transmit command messages in case of network disruptions or power failures from the mobile device. Similarly, capabilities from the mobile device to report on incomplete wiping command executed [34].

Evaluating the effectiveness remote wiping by using forensic toolkits can help law enforcement resources manage time used in research when investigating a crime involving mobile devices. For example, knowing that manufacturer's-based wiping from a particular device might have different results from third party applications and what traces of user data is left behind could help law enforcement identify important forensic evidence based on device, wiping process or forensic toolkit utilized.

Research on the effectiveness of data recovery after wiping commands are executed on remote devices is limited. Current research has relied on the availability of forensic toolkits with limited functionality or non-commercial licenses, and older device releases used for research. Forensic tools functionality relies on software, hardware tools, or a combined software/hardware approaches. We observe that most research has been conducted using the software approach only. Available research shows a similar methodology with the following steps when evaluating results from different remote wiping processes utilized: Identify forensic toolkit to be utilized; backup user application data from the devices to be used for testing; identify the categories of data available on the device and the number of files associated with each category; identify the wiping process to be utilized (manufacturer or third party); select and execute wiping commands; record and evaluate results; using forensic toolkit to recover, identify and categorize user data left behind after wiping process; and compare the number of files before and after executing remote wiping for each category identified [7, 10, 23].

4 Proposed Evaluation and Methodology

Remote wiping capabilities are commonly available from the mobile device manufacturer or through third-party apps that can be enabled by the device's user or managed services with access to the device. The objective of remote wiping is to securely delete user data stored in the mobile device whether it is stored in the manufacturer's delivered applications or third-party apps installed and enabled by the device user.

Forensic data recovery/retrieval starts with two main focal points, namely: the "Specialized Tool(s)" used for data recovery, and the "Deletion Process" used to delete or wipe the data.

Additional points to consider for the effectiveness of data recovery relies on an understanding of the following: (1) What type of data can be recovered?; (2) Where the data is stored (e.g. location the data is stored on a device, or if not on the local device where is the physical location of the data, such as network or cloud based)?; (3) What is the format of the data stored as (e.g., text, media, standard data exchanging formats such as Extensible Markup Language (XML), Data Base (DB), and JavaScript Object Notation (JSON))?; and (4) Whether files are encrypted?.

Our proposed research focuses on data that can be recovered after a remote delete/wipe process has completed on a mobile device. The scenario for all mobile devices used in our research require the following: (1) Smartphone(s) for testing data recovery; (2) Data objects to attempt recovery of on the smartphone(s): email, images, different application data, calendar objects, and text messages; (3) Network availability: Wi-Fi or Cellular; (4) A network-based account to allow for backing up the smartphone(s); (5) Network-based ability to initiate/execute the remote delete/wipe; (6) Forensic tool(s) to recover data; and (7) Forensic reports to allow for data analysis.

The equipment used include three smartphones, without sim cards or external SD cards: Android – Samsung S5, Model # SAMSUNG-SM-G900A, running OS version 6.0.1 (hereafter referred to as Samsung G900 or as G900), Android – Samsung S5 Active, Model # SAMSUNG-SM-G870A, running OS version 6.0.1 (hereafter referred to as Samsung G870 or as G870), and Apple- iPhone 6S, Model # MN1K2, running iOS version 13.2.2 (hereafter referred to as iPhone 6S). All three smartphones had a Wi-Fi access account added to allow for network/Internet access. For both G900 and G870, a Google account was created and added to allow for backup and remote wipe ability. For the iPhone 6S, an Apple ID and iTunes account was created to allow for backup and remote wipe capability.

Data installed included multiple instances of the following: Four (4) contacts, two (2) emails, three (3) SMS texts, four (4) pictures, four (4) documents, 506 calendar events, three (3) audio files, one (1) video, four (4) random web pages were opened and two (2) pictures from those web pages were downloaded. We also installed the following applications: Shreddit – Data Eraser by PalmTronix, and Secure Wipe by Pinellas CodeWorks.

We also used Mobile Phone Examiner Plus (MPE+) from Accessdata, and MOBILedit from Compelson labs, on computers running Windows 10 OS. The evaluation methodology will follow the forensics investigation model of [34], which is also described below.

Preservation: Smartphones will be selected for research, data baseline will be established, and a data backup will be performed. Baselining will consist of sanitizing/removing any personally identifiable information (PII) currently on the phone and then installing, or adding, selected data and apps to each phone. Backup will be performed using a manufacturer online account to store a device-initiated backup. There will also be a logical copy of the baseline imaged device, stored on a laptop; this is only a failsafe in case the online backup fails.

Acquisition: Forensic tool(s) will be selected that allow for mobile phone examination. The tool will be used to extract the data from the smartphones at different acquisition points. Data acquisition reports, if not provided by the forensic tools, will be created after each of the different analysis tests. There are four proposed different data acquisition points: After initial baseline of the device; After a factory reset is performed; After a restore of the device to baseline; After a remote delete/wipe is performed. Prior to performing the factory reset, a locally installed data wiping app will be used to remove any prior residual deleted data or data fragments remaining after baselining the device. Data acquisition tests will be used to validate the effectiveness of the app. This is to ensure the tests focus on residual data of freshly deleted items.

Examination Analysis: All of the acquisition reports will be created in the same manner as to allow for data comparison on two levels. The first comparison will of the all data recovery reports for each individual device to see how what data could be recovered. The second comparison will be to look for differences in the data recovery ability of the three different devices.

Reporting: Explanation and summary of forensic reports findings are included and written in this paper with a conclusion of our findings and identified areas for further research.

5 Case Study

5.1 Data Installation and Preservation

The smartphones, selected for this research, were found to still contain the previous user's data; not wiped/reset. Each phone was examined and PII that was discovered was deleted. This included all deleting previous accounts, deleting internet history, and browser form filling data. Online accounts were created for the phones to allow for backup, restore, and remote delete/wipe ability. The reason for using new accounts were to avoid possible data spillage or cross deletion with our personal phones. Both Android phones, G870 and G900, were able to use a single Google account. An Apple account was created for the iPhone 6S.

The selection of Apple for the iPhone and Google for the Androids was to create a condition that the majority of users would find themselves in if needing to remotely wipe their devices. Third-party apps were available but would require additional steps such as downloading, installing, and configuring an account. The majority of third-party apps that allow remote wiping required a cost. The additional data selected was copied onto the device. The online accounts were used to update all installed apps and to download the two third-party local data erasing apps: Shreddit-Data Eraser and Secure Wipe. These were selected due to high recommendations in different electronic review sites and high ratings on the Google Play Store.

The two wiping apps will be used prior to performing the factory reset test. Their purpose is to remove any of the previously deleted data, or residual data fragments, remaining after baselining the device. The old deleted data would not be backed up to the online account or copied to a folder on the laptop being used, unless a physical image could be obtained. These unallocated data fragments may cause variances in the expected data acquisitions. A logical copy of the files and folders on the phone were copied to folder on a laptop as an emergency backup in the event of a crash.

These steps were to ensure and establish repeatable baseline images allowing for initial data consistency prior to the different analysis tests, or recovery in the event of data corruption due interrupted forensic scans or device malfunctions. Once all data and apps were installed and updated, an online backup was initiated through the phones setting options. Once completed, the Wi-Fi was disabled to prevent the data from changing. The phone was now ready for the acquisition phase.

5.2 Data Acquisition

This section will describe how the data acquisitions were performed. The first step after baselining the device, was to create a baseline data acquisition report with the use the forensic tools. Several varying steps were required based on the type of phone analysed, Android vs. Apple, and different issues occurred while using the different forensic tools. Both of the selected forensic tools were full versions and required a paid licence for use. They were installed in UTSA's computer lab.

After preparing the phones for examination, the forensic software tool will be started and the smartphone plugged into the computer or laptop running the software. If the software tool or operating system (OS) does not recognize the phone, a set of phone drivers or speciality software may need to be downloaded and installed. It could also mean additional steps with the phone is needed to be recognized.

Documentation from both tools showed that Android phones need to be placed in the debugging mode for them to work. Debug mode is not turned on by default due to security issues. MPE+ recommends using a third-party tool to root the phone if unable to turn on debugging mode. MOBILedit does have some options available to access a locked phone if access to the phone's system menu was not available. The software documentation discussed that using these options will or may overwrite the internal software; based on the method used to access the phone. To prevent damage to the phones, and since we had access to the phones interface, we selected the manual way of putting the phones in to debug mode. For this reason, the phones examined were not rooted, and the screens were unlocked, during the whole data acquisition process.

To place the phones in debug mode, the hidden Developer Option button must be unlocked. First, locate the Build Number in Settings, most likely in the About options. Tap on the Build Number multiple times, most phones take seven times, then go back into Settings to find the Developer Option button visible. In there, select debug mode, select stay awake while charging, and deselect verify apps via USB.

The first data recovery tool attempted was MPE+. Due to licensing, the software could only be installed on select computers in the computer lab and had to be run with administrator privileges. Multiple attempts were made to use this tool but none were successful. None of the phones were identified by the software, manual selection of the phones still did not allow the software to recognize the phones. Going through the different screen pages displayed, it was obvious that the Androids were being seen but only as a device in Media Transfer Protocol (MTP) mode. The phone was recognized in Windows. MTP mode does not allow for data recovery or viewing of all the internal files. The iPhone was not recognized by MPE+ at all. Due to the multiple issues only the MOBILedit software was used for data extraction in this research.

Compelson Labs had issued our forensic class a limited number of MOBILedit full access licences, that would expire after 60 days. This allowed MOBILedit to be loaded on two personal laptops, eliminating the administrative mode issues. MOBILedit is a specialized forensic tool for smartphones. The installation was straight forward with an easy to use interface. The iPhone was recognized right away by the software as an iPhone, and displayed a menu to allow the user to select which version the iPhone was; we used the 6S version for all tests. The Android devices did require that the debug mode be enabled for the software to effectively work. MOBILedit has additional options to

connect to the phones by Bluetooth or Wi-Fi; these connection methods were not used during this research. The software allows for different data recovery configurations (such as full, deleted only, user specified and others) and it has the ability to create different reports or data backups based on the selections made.

There are four (4) different data acquisition points required for the test data to be relevant. The first is after the initial baseline of the device is created. This data acquisition test is needed to create a data acquisition baseline. The results can be used to validate if the backup restore process worked, and helps identify how much data is restored from the backup; 100% or less. The second acquisition point is after a factory reset is performed. This data acquisition test is needed to identify if any previous data or user PII can be recovered, and establishes a data acquisition reset baseline. The test results allow for a comparison of the factory reset option vs. a remote reset option. The third acquisition point is after the device is restored from the back up to the baseline. The fourth acquisition point is after the remote delete/wipe is performed.

There were six additional tests with the Android phones, and four additional tests with the iPhone. All proposed tests are as follows: (1) Full content - Baseline (without debug mode enabled) (Android only); (2) Full content – Baseline; (3) Deleted data only – Baseline; (4) Deleted data only – After running Shreddit with default settings; (5) Deleted data only – After running Secure Wipe with default settings; (6) Full content – After Factory Reset (without debug mode enabled and without a user account); (7) Full content – After Factory Reset (without a user account); (8) Deleted data only – After Factory Reset (without a user account) (Android Only); (9) Full content – After phone restored from backup; and (10) Full content – After Remote Delete/Wipe (without a user account) (with debug mode enabled).

Android Devices

The Samsung G870 was selected as the first device for data acquisition. The following is the data, steps, and findings for the Samsung G870 only. The Samsung G900 results were very similar and the differences will be explained at the end of this section.

Since the Android devices required the extra step of turning on the debug mode, the first data acquisition test with MOBILedit was performed with the phone in the same configuration as a normal user; without the debug mode option. The phone was recognized but only as an MTP device, and little data was discovered during the test; only 314 files. The debug mode was enabled and the phone was properly recognized. MOBILedit did request an extra step to allow it to install its software on the phone. As it installed, it requested access to five areas: device location, contacts, calendar, photos/media/files, and SMS messages. A full content data acquisition of the baseline with the debug enabled was conducted. Comparing this report against the no-debug report of baseline showed a significant increase in data recovered; 3,687 files/data. See Table 1 for a comparison of the data from the summary reports.

The next three data acquisitions were for deleted data only. Once the baseline data acquisition was recorded, the next step was to try and wipe the deleted items found using Shreddit. This application is used directly on the phone to delete unallocated data on smartphones. It has the ability to perform multiple passes, but was run with the default setting selected. Once started, Shreddit required access to the smartphones' photos, media, and files. After it finished, the Android device was restarted and a data

acquisition test was performed. MOBILedit found the same deleted items as were found in the full report. There was no change, it was as if Shreddit was ever run.

This same process was performed using the Secure Wipe app. Once again, the same previously identified deleted data was discovered. It was only after a factory reset was performed that the deleted data was no longer found. The failure to delete the unallocated data may be due to the way NAND memory cells work. Deletion only happens when all data in the cell is marked for deletion and deletion is done on the cell level, not the file or bit level. If any data is still relevant in a cell, the unallocated data in that cell will not be wiped. All three deleted data only acquisitions are found to be redundant since the deleted data is already displayed in the full report. Table 2 shows an extract of deleted data found during five consecutive data acquisitions.

Table 1. Comparison of the data from the MOBILedit summary reports

FileSystems	No Debug	Baseline	Factory Reset
Internal Filesystem	314 files	17 files	17 files
External Filesystem		419 files	17 files
Application System		2645 files	1447 files
Extra Filesystem		275 files	222 files
Misc Filesystem	0 file	1 file	0 file
System Logs		91 files	90 files
Bluetooth Pairings		0	0
Contact Analysis		0	0
Cookies		169	0
Loactions			
GPS Locations	0	0	1
Notifications		2	4
Passwords			
Password from Chrome (Saved Passwords)		1	
Passwords SAMSUNG-SM-G870A (Wi-Fi)		1	
Screen Unlocking History		3	7
User Dictionary		0	0
Wi-Fi-Networks		2	1
Web			
Web Browsing History		56	0
Web Search History		5	0
Bookmarks		0	0

Table 2. Extract of deleted data found during five consecutive data acquisitions

Download Manager	Baseline-Full	Delete Only	Shreddit	Secure Wipe	Factory Reset
Downloaded Files	10 (8 deleted)	(8 deleted)	(8 deleted)	(8 deleted)	
Account Kaa80@gmail.com					
Contacts	68 (67 deleted)	(67 deleted)	(67 deleted)	(67 deleted)	
Circles	27 (25 deleted)	(25 deleted)	(25 deleted)	(25 deleted)	

The factory reset was carried out natively within the phone setting options, with the option to erase all the data on the phone selected. After the factory reset was complete a data acquisition test was performed. Two data acquisition were performed without any user account being entered: one data acquisition with no-debug, another with debug enabled. The Google account was installed and a backup sync was requested from the phone's settings. All apps were updated and the two data delete/wipe apps were installed. When complete the wireless connection was turned off and full content data acquisition was performed. This was done to validate the restore function worked, and to allow comparison with the baseline on how much data does not get restored. The last step was to perform a remote deletion of the phone. The wireless connect function of the phone was turned back on. Using the laptop, the user Google account was accessed. The phones for this account were found in the managing your account section, in the security option. By selecting the G870 phone, and then the find my phone option, a window will appear which allows the user different options to include remotely erasing the phone's data called "Consider erasing your device".

If the Android device was not connected to a Wi-Fi or cellular network at the time the remote wipe was requested, the reset request will wait and the next time the device is connected the process will be carried out. After the phone finishes restarting, a data acquisition test was performed. This data acquisition was performed without any user account being entered, and with debug enabled. The Samsung G900 was then selected and put through the same steps and tests that the G870 was put through. There were a few minor differences in how some of the apps were handled in the report, and how much data was retrieved after the resets. The most significant finding was that the Google account for this phone, did not provide an option to remotely delete the data on the phone. The process to find the phone on the web page was the same but the final popup window displayed different options.

In order to facilitate a remote delete/wipe of the phone, a Samsung account had to be created. Through the Samsung website the remote delete option was available. It performed similar to the Google account remote wipe. Figure 2 depicts the process flow used for the Android smartphones, to prepare the devices, data acquisitions, factory reset, and remote wiping.

Apple Device

The iPhone 6S was recognized right away by MOBIL edit as an iPhone as it was plugged in. The difference in how MOBILedit recognized the phone. With the Androids,

MOBILedit recognized the make and version right away, with the iPhone the version of iPhone had to be selected from a provided list. The same action and steps taken with the Androids, were performed with the iPhone except: debug enabling was not required and the two downloaded delete/wipe apps were not used. A similar delete/wipe app was not found in the iTunes store. This reduced the number of data acquisitions from ten (10) to four (4).

The final step of remote delete/wipe was performed slightly different than the Androids. With the iPhone 6S this task was performed through the iCloud website. Once the website was accessed, using the Apple account, the proper iPhone was selected. The website will attempt to locate the iPhone and the option to erase all content and settings in the iPhone data accessible. Once the phone finishes resetting a full data acquisition is performed. Figure 3 depicts the process flow followed with the iPhone to prepare the device and the scanning actions followed by executing the remote wiping functions.

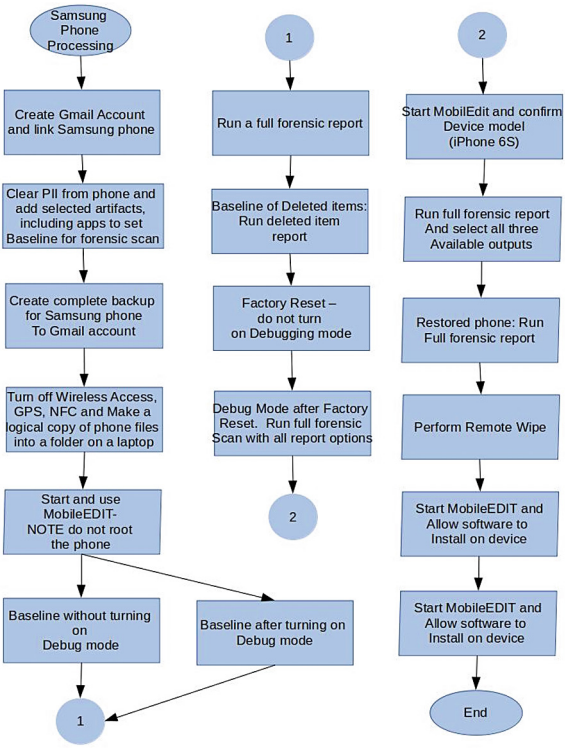

Fig. 2. Samsung devices – Processing and forensic scan process flow

6 Discussion

Data collected, during the data acquisitions tasks, were performed requesting all three report formats and all four exports available, from the MOBILedit forensic software

package used. The purpose was to have more options with how to analyse the collected data. The easiest report format to collect the data from was the pdf reports. Copies of the first three sections of each report (Screenshots of Report Settings, Summary, and Deleted Data) were extracted. The final section, Data Extraction Log, was also extracted.

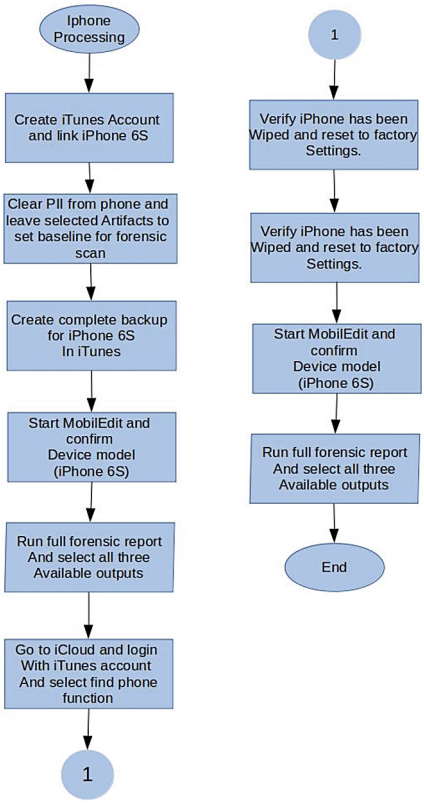

Fig. 3. iPhone – Processing and forensic scan process flow

The extracted data presented in each of the baseline's data report Summary section, was used to create an Excel spreadsheet for that specific phone. The data displayed in the Summary section from each of the 10 Android tests, 4 Apple tests, was transferred to a corresponding line in that phone's spreadsheet. The data from each of the Data Extraction Log sections of the reports, was similarly transferred to a spreadsheet for that phone.

Each column of the spreadsheets represented the data from one of the 10 acquisition tests, discussed earlier in this report. From here it was easily seen that the four deleted data only reports were not needed. The data displayed in the "deleted data only" reports is already listed in the full content reports and the downloaded wiping apps were unsuccessful; these four columns were hidden. The next redundant report found was comparing the two data acquisitions where the debug mode was not enabled. Since

these two reports were identical, the no debug report after the factory reset column was hidden. The remaining columns, five (5) for the Android phones and four (4) for the Apple phone, were used for evaluating the data acquired. The extra column for the Android phones is the data from first acquisition test (no-debug), since this shows a valid contrast to the other reports. Similarly, the Data Extraction Log section spreadsheets were adjusted to match the four identical column identifiers for both phones; the no-debug report was not used when analysing the data from this section.

The bulk of the MOBILedit data acquisition report is detailed breakouts for each application and the system files. Most have a link to open the corresponding data/file for a more detailed inspection. These detailed data sections were reviewed to examine if any relevant, or PII, data remained and was captured in the data acquisition but hidden from easy visibility.

The baseline amount of data for each phone was recorded as: G870 = 4,207 (Table 3); G900 = 3,338 (Table 4); and the iPhone 6S = 6,188 (Table 5). It is understandable why the iPhone differed from the Androids, but both Androids should have been closer. This information shows that even a slight change to the phone (a regular S5 to a S5 Active) can create a significant data change. This was further demonstrated with examination of how much data extraction change there was, after each acquisition event, against the baseline data for each of the phones.

The percent of data change against the baseline was examined next. Comparing of the baseline data numbers to the amount of data recovered following the factory reset showed 41–84% reduction of data. Comparison of baseline data to the amount of data found after a restore action showed a 10–30% reduction in data. Comparison of the amount of data found after the factory reset to the amount of data found after the remote wipe showed less than a .2% data reduction change for each phone: G870 = .1% loss, or 2 data objects; G900 = .2%, or 4 data objects; iPhone 6S 0% with no data reduction (See Table 6).

The G870 showed the highest reduction in recoverable SQL, XML, and JSON data following the remote wipe, with 74% reduction of SQL data, 36% reduction of XML data, and 100% reduction of JSON data. The iPhone showed the lowest reduction percentage for these three data types with 64% reduction of SQL data, 19% reduction of XML data, and 94% reduction of JSON data.

The iPhone also had the highest data restore percentage rate with only 10% loss of all data after the restore operation, −1% loss for SQL, 1% loss for XML, and 0% loss of JSON. Unsure why there was a slight SQL increase; this should be examined further in a later research project. The lower part of the Summery section of the G870 data reports, show similar reduction percentages with the recovered filesystems data (See Table 7).

The data acquired after both the factory reset and the remote reset, showed all previously deleted data was sanitized and no longer recoverable with the software. Additionally, examination of the detailed section and the two summaries (Summary and Data Extraction sections) for these two acquisition tasks, did not reveal any of the users PII or any of the user relevant data that was installed on the phones to achieve a baseline.

Table 3. Data extraction numbers for G870

G870	Base	Factory Reset	Restored	Remote Delete
Phone Books	4	1	4	1
Messages	1	1	2	1
Events	506	0	297	0
Phone call	0	0	0	0
Archive Files	15	1	6	1
Documents	13	3	3	3
Certificates	1	1	1	1
Audio	3	1		1
Image	500	402	407	402
JSON	90	XXX	13	XXX
Sqlite	122	33	89	32
Video	1	0	0	0
XML	683	439	603	437
Other Files	1	1	1	1
All Other files	1937	822	1175	823
Applications	330	321	326	321
Totals	4207	2026	2927	2024

The downloaded third-party apps, for wiping the unallocated data space were, ineffective on the phones. They were chosen as highly recommended by review sites and had a high user feedback rating. They were used with the default settings, which only completes one wipe pass, but this should have at least reduced the number of recoverable deleted items.

The failure of the third-party wiping apps, might be discovered examining the amount of time they spent performing their tasks. The deletion down time with the two third-party apps was just about 10 s each. The deletion down time for the factory reset and remote reset was 2–5 min each. Based on the results it appears the two events (factory reset and remote reset) performed a wipe similar in results to a low-level format of a hard drive. Justification for this line of thinking is that the previously identified deleted data was no longer seen in the acquisition reports after these two tasks.

It is unsure what the two third-party wiping apps did. There are two possibilities for their failure, the structure of the NAND cells prevents completing a secure wipe of all unallocated data in an active cell. The other possibility could be that the algorithms in MOBILedit allows for greater data recoverability.

Table 4. Data extraction numbers for G900

G900	Base	Factory Reset	Restored	Remote Delete
Phone Books	4	1	4	1
Messages	0	0	0	0
Events	506	0	298	0
Phone call	0	0	0	0
Archive Files	7	1	11	1
Documents	4	3	3	3
Certificates	1	1	1	0
Audio	3	1	3	1
Image	405	397	407	397
JSON	85	XXX	67	XXX
Sqlite	92	28	78	27
Video	0	0	0	0
XML	596	425	546	423
Other Files	1	1	1	1
All Other files	1312	792	1228	792
Applications	322	316	326	316
Totals	3338	1966	2973	1962

Table 5. Data extraction numbers for iPhone 6S

iPhone 6S	Base	Factory Reset	Restored	Remote Delete
Archive Files	2	XXX	1	XXX
Documents	7	1	7	1
Image Files	XXX	104	XXX	104
Auddio	404	0	404	0
Extracted	2491	267	2098	267
JSON	49	3	49	3
plist	967	382	1023	382
sqlite	156	56	158	56
Realm databases	2	1	2	1
Video	186	0	88	0
XML	118	96	117	96
Binary coockies	33	XXX	33	XXX
Other files	1656	0	1469	0
Applications	117	96	116	96
Totals	6188	1006	5565	1006

Table 6. Percentage of data change to the baseline, for each phone

Baseline Total Change	G870	G900	iPhone S6
% Change after FR	52%	41%	84%
% Change after restore	30%	11%	10%
% Change after remote	52%	41%	84%
% Difference between base and restore events	41%	41%	N/A
% Difference between base and restore SQL	27%	15%	-1%
% Difference between base and restore XML	12%	8%	1%
% Difference between base and restore JSON	86%	21%	0%
% Difference between base and remote SQL	74%	71%	64%
% Difference between base and remote XML	36%	29%	19%
% Difference between base and remote JSON	N/A	N/A	94%
Count difference between base and restore	1280	365	623
Count difference between FR and remote	2	4	0

Table 7. G870 spreadsheet data

Filesystems	No-Debug	Baseline	Factory Reset	Recovery	Remote Delete
Internal Filesytem	314 files	17 files	17 files	17 files	17 files
External Filesystem		419 files	17 files		17 files
Applications Filesystem		2645 files	1447 files	2010 files	1445 files
Extra Filesystem		275 files	222 files	271 files	222 files
Misc Filesystem	0 file	1 file	0 file	1 file	0 file
System Logs		91 files	90 files	91 files	90 files

7 Conclusion

Previous studies on recovering data from smartphones, mostly focused on extracting PII and relevant user data after executing wiping commands from the devices themselves by using OS available functions or third-party apps. There were multiple studies conducted using Android phones, but almost all of them were version 5.0 or earlier; very few studies were found using iPhones and those found used iOS 4.0 and earlier. There were a few studies found that addressed data recovery after a factory reset, but they were also conducted with the early version of smartphones just addressed. Their tests also showed that some of the smartphones, Apple iOS prior to version 4.0 and Android OS prior to version 7.0, had faulty factory reset ability, allowing varying amounts of data to be recovered; the amount of data varied with different models. Research showed that Android OS version 5.0 and Apple iOS version 4.0 allowed for encrypting the device's data, but encryption was not turned on by default until 2014. The smartphones displayed great factory reset ability, although this does not address the problem of deleting data in the event of a lost or stolen phone. It is acknowledged that encrypted data is not useful without the key, so in this instance the data is considered sanitized.

The focus of this study was to see the effectiveness of a remote delete/wipe, and if any relevant or PII data remains on a smartphone after the wipe. Based on the results found, from the different data acquisition attempts, it appears that the remote wipe and factory resets on these smartphone devices are effective in sanitizing PII data and other user data. However, the findings could also be due to the fact that the data acquisition methods chosen had limited visibility into the devices used. Hence, future research should include the use of other mobile forensic software. It was also noticed that data backup/sync functions do not completely restore a phone to its previous state, and may be a good basis for another research project in the future as to why.

Continued research should be performed using a larger variety of devices from different manufacturers and running different operating systems, to test if the effectiveness of the remote wiping commands might vary. Additional research should be done to examine the contents of the XML, SQL, and JSON files. The data size suggests minimal data is present; many are listed less than 1kb. Due to time and tool restraints, this was not performed during this research project.

Encryption on by default allows for a quick recovery following a factory or remote reset since only the encryption token needs to be wiped. Additional research should be conducted on trying to recover the deleted encryption tokens. This will allow law

enforcement access to encrypted data. Future tests should review the ability to access locked phones of newer makes and models without firmware, software, or hardware damage to the phones.

Acknowledgement. We would like to express our gratitude to Compelson Labs for the support and making MobilEdit available to our research. We would also like to acknowledge the contributions of Andrew Mendoza in the research of background and related work, and testing.

References

1. Jones, B.H., Chin, A.: On the efficacy of smartphone security: a critical analysis of modifications in business students' practices over time. Int. J. Inf. Manag. **35**(5), 561–571 (2015). https://doi.org/10.1016/j.ijinfomgt.2015.06.003. Accessed 17 Oct 2019
2. Allam, S., Flowerday, S., Flowerday, E.: Smartphone information security awareness: a victim of operational pressures. Comput. Secur. **42**, 56–65 (2014). https://doi.org/10.1016/j.cose.2014.01.005. Accessed 17 Oct 2019
3. Cardwell, G.: Residual Network Data Structures in Android Devices, Masters, Naval Postgraduate School (2011)
4. Yao, M., Chuang, M., Hsu, C.: The kano model analysis of features for mobile security applications. Comput. Secur. **78**, 336–346 (2018). https://doi.org/10.1016/j.cose.2018.07.008. Accessed 17 Oct 2019
5. Blancco Technology Group: Analysis of Data Remanence After Factory Reset, and Sophisticated Attacks on Memory Chips. Blancco Technology Group (2019)
6. Bransfield-Garth, S.: Mobile phone calls as a business risk. Network Secur. **2010**(9), 4–11 (2010). https://doi.org/10.1016/s1353-4858(10)70114-8. Accessed 17 Oct 2019
7. Korenis, P., Billick, S.: Forensic Implications: adolescent sexting and cyberbullying. Psychiatric Quart. **85**(1), 97–101 (2013). https://doi.org/10.1007/s11126-013-9277-z. Accessed 17 Oct 2019
8. Ehatisham-ul-Haq, M., Azam, M., Naeem, U., Rèhman, S., Khalid, A.: Identifying smartphone users based on their activity patterns via mobile sensing. Procedia Comput. Sci. **113**, 202–209 (2017). https://doi.org/10.1016/j.procs.2017.08.349. Accessed 17 Oct 2019
9. Narayanan, S.V.: Myths and fallacies of "Personally Identifiable Information". Commun. ACM **53**(6), 24 (2010). https://doi.org/10.1145/1743546.1743558. Accessed 17 Oct 2019
10. Wilbanks, L.: The impact of personally identifiable information. IT Professional **9**(4), 62–64 (2007). https://doi.org/10.1109/mitp.2007.77. Accessed 17 Oct 2019
11. Gámez-Guadix, M., Mateos-Pérez, E.: Longitudinal and reciprocal relationships between sexting, online sexual solicitations, and cyberbullying among minors. Comput. Hum. Behav. **94**, 70–76 (2019). https://doi.org/10.1016/j.chb.2019.01.004.. Accessed 17 Oct 2019
12. Barker, Cosmo Survey: 9 out of 10 Millennial Women Take Naked Photos. Cosmopolitan (2014). https://www.cosmopolitan.com/sex-love/advice/a30675/ninety-percent-millennial-women-take-nude-photos-cosmo-survey/. Accessed 17 Oct 2019
13. Milne, G., Pettinico, G., Hajjat, F., Markos, E.: Information sensitivity typology: mapping the degree and type of risk consumers perceive in personal data sharing. J. Consumer Affairs **51**(1), 133–161 (2016). https://doi.org/10.1111/joca.12111. Accessed 17 Oct 2019
14. Tankard, C.: The security issues of the Internet of Things. Comput. Fraud Secur. **201**(9), 11–14 (2015) https://doi.org/10.1016/s1361-3723(15)30084-1. Accessed 17 Oct 2019
15. Yang, L., Wei, T., Zhang, F., Ma, J.: SADUS: secure data deletion in user space for mobile devices. Comput. Secur. **77**, 612–626 (2018). https://doi.org/10.1016/j.cose.2018.05.013.Accessed 17 Oct 2019

16. Reardon, J., Basin, D., Capkun, S.: SoK: secure data deletion. In: 2013 IEEE Symposium on Security and Privacy (2013). https://doi.org/10.1109/sp.2013.28. Accessed 17 Oct 2019
17. Di Leom, M.: Remote Wiping in Android. University of South Australia, Masters (2015)
18. Kissel, R., Regenscheid, A., Scholl, M., Stine, K.: Guidelines for Media Sanitization (2014). https://doi.org/10.6028/nist.sp.800-88r1. Accessed 17 Oct 2019
19. Simon, L., Anderson, R.: Security Analysis of Android Factory Resets. University of Cambridge (2015)
20. Patel, N.: Utilisation of Flash Storage Memory, no. 2018 (2018). https://doi.org/10.13140/RG.2.2.35672.34565.. Accessed 17 Oct 2019
21. Brown, Almost ALL iPhones Are Encrypted, Almost ALL Android Smartphones Are NOT, Express.co.uk (2019). https://www.express.co.uk/life-style/science-technology/653099/iPhone-iOS-Encryption-Android-OS-Google-Smartphone. Accessed 17 Oct 2019
22. Miller, J.: Google and Apple to Introduce Default Encryption, BBC News (2014). https://www.bbc.com/news/technology-29276955. Accessed 17 Oct 2019
23. Gómez-Miralles, L., Arnedo-Moreno, J.: Hardening iOS devices against remote forensic investigation. Security and Resilience in Intelligent Data-Centric Systems and Communication Networks, pp. 261–283 (2018). https://doi.org/10.1016/b978-0-12-811373-8.00012-4. Accessed 17 Oct 2019
24. Kingsley-Hughes, Here's How to Securely Wipe Your Android Smartphone for Resale, ZDNet (2019). https://www.zdnet.com/article/heres-how-to-securely-wipe-your-android-smartphone-for-resale/. Accessed 17 Oct 2019
25. Altuwaijri, H., Ghouzali, S.: Android data storage security: a review. J. King Saud University – Comput. Inf. Sci. (2018). https://doi.org/10.1016/j.jksuci.2018.07.004. Accessed 17 Oct 2019
26. Meckley, T.: An Empirical Comparison of Smartphone Factory-Resets to Remote Deletion Applications. University of South Alabama, Masters (2019)
27. UZ, The Effectiveness of Remote Wipe as a Valid Defense for Enterprises Implementing a BYOD Policy, Masters, University of Ottawa (2019)
28. Pollitt, M., Shenoi, S. (eds.): DigitalForensics 2005. ITIFIP, vol. 194. Springer, Boston (2005). https://doi.org/10.1007/0-387-31163-7
29. Barmpatsalou, K., Cruz, T., Monteiro, E., Simoes, P.: Current and future trends in mobile device forensics. ACM Comput. Surv. **51**(3), 1–31 (2018). https://doi.org/10.1145/3177847. Accessed 17 Oct 2019
30. Thomas, D.: How to delete files on android so they can't ever be recovered. Gadget Hacks (2016). https://android.gadgethacks.com/how-to/delete-files-android-so-they-cant-ever-be-recovered-0169550/. Accessed 17 Oct 2019
31. Bilić, D.: How to delete your smartphone data securely before selling your device. WeLiveSecurity (2016). https://www.welivesecurity.com/2016/06/03/how-do-you-delete-your-data-securely-before-selling-your-cell-phone/. Accessed 17 Oct 2019
32. Glisson, W., Storer, T., Blyth, A., Grispos, G., Campbell, M.: In-the-wild residual data research and privacy. J. Digital Forens. Secur. Law **11**(1) (2016). https://doi.org/10.15394/jdfsl.2016.1371
33. Yu, X., Wang, Z., Sun, K., Zhu, W., Gao, N., Jing, J.: Remotely wiping sensitive data on stolen smartphones. In: Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security - ASIA CCS 2014, no. 2014, pp. 537–542 (2014). https://doi.org/10.1145/2590296.2590318.. Accessed 17 Oct 2019
34. Di Leom, M., Choo, K., Hunt, R.: Remote wiping and secure deletion on mobile devices: a review. J. Foren. Sci. **61**(6), 1473–1492 (2016). https://doi.org/10.1111/1556-4029.13203. Accessed 17 Oct 2019
35. Apple Inc. Remotely Locating and Commanding a Mobile Device, US 2018/0337974 A1 (2018)

36. AirWatch LLC, Device Back and Wipe, US 2019 / 0073271 A1 (2019)
37. Hoffman, Why Deleted Files Can Be Recovered, and How You Can Prevent It. How-To Geek (2019). https://www.howtogeek.com/125521/htg-explains-why-deleted-files-can-be-recovered-and-how-you-can-prevent-it/. Accessed 17 Oct 2019