2014-03

Effectiveness of the factory reset on a mobile device

Schwamm, Riqui

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EFFECTIVENESS OF THE FACTORY RESET ON A MOBILE DEVICE

by

Riqui Schwamm

March 2014

Thesis Advisor:	Neil Rowe
Second Reader:	Simson Garfinkel

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE EFFECTIVENESS OF THE FACTORY RESET ON A MOBILE DEVICE		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Riqui Schwamm			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

All mobile phones use internal flash memory to store information. The flash memory contains personal user data that can be extracted with the use of forensics tools. This information could be used to profile a user's daily activity. However, all smartphones provide a tool to erase (factory reset) the information from the flash memory. Twenty-one smartphones were used to evaluate the effectiveness of the factory-reset feature. A set of forensics tools from Cellebrite was used for the extraction and analysis process. The factory-reset feature was found to leave significant amounts of user-generated content after operation. The amount of user-generated content varied by vendor and model number. Extracted data are presented as evidence to show the ineffectiveness of the reset. User data such as photographs, audio files, text files, login information and geolocation data were left on the phone. The data analysis uncovered the unreliable nature of a factory reset and how the user is not properly protected.

14. SUBJECT TERMS Android Operating System, Apple iOS, Mobile Forensics, smartphone, personal user data			**15. NUMBER OF PAGES** 67
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

EFFECTIVENESS OF THE FACTORY RESET ON A MOBILE DEVICE

Riqui Schwamm
Civilian, Department of the Navy
B.S., California State University, Monterey Bay, 2011

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
March 2014

Author: Riqui Schwamm

Approved by: Neil Rowe
Thesis Advisor

Simson Garfinkel
Second Reader

Peter J. Denning
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

All mobile phones use internal flash memory to store information. The flash memory contains personal user data that can be extracted with the use of forensics tools. This information could be used to profile a user's daily activity. However, all smartphones provide a tool to erase (factory reset) the information from the flash memory. Twenty-one smartphones were used to evaluate the effectiveness of the factory-reset feature. A set of forensics tools from Cellebrite was used for the extraction and analysis process. The factory-reset feature was found to leave significant amounts of user-generated content after operation. The amount of user-generated content varied by vendor and model number. Extracted data are presented as evidence to show the ineffectiveness of the reset. User data such as photographs, audio files, text files, login information and geolocation data were left on the phone. The data analysis uncovered the unreliable nature of a factory reset and how the user is not properly protected.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ADB	Android Debug Bridge
CDMA	code division multiple access
DoD	Department of Defense
GPS	Global Positioning System
GSM	Global System for Mobile
IEEE	Institute of Electrical and Electronics Engineers
iOS	iPhone Operating System
MMS	Multimedia Messaging Service
MTP	Media Transfer Protocol
NFC	Near field communication
NPS	Naval Postgraduate School
OS	operating system
SD	Secure Digital
SIM	subscriber identity modules
SMS	Short Message Service
URL	Uniform Resource Locator
USB	Universal Serial Bus
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This research project would not have been possible without the guidance and support of Dr. Neil Rowe and Dr. Simson Garfinkel. I would especially like to recognize Dr. Rowe for his patience and encouragement when it was most required.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. MOBILE DEVICES, APPLICATIONS, AND USER DATA

There has been significant growth in personal smartphone devices. In June 2013, the Google Android smartphone held 51.8% of the market, the highest share in the U.S. Table 1 [1]. Apple iOS maintained the second largest share at 40.6%, followed by BlackBerry at 3.4% and Microsoft at 3.1% [1]. Symbian still holds a 0.2% market share but has been discontinued by Nokia. The last Symbian smartphone was shipped in mid-2012, according to the company's 2012 Interim Report [2].

Top Smartphone Platforms **3 Month Avg. Ending Dec. 2013 vs. 3 Month Avg. Ending Sep. 2013** **Total U.S. Smartphone Subscribers Age 13+** **Source: comScore MobiLens**			
	Share (%) of Smartphone Subscribers		
	Sep-13	**Dec-13**	**Point Change**
Android	51.8%	51.5%	-0.3
Apple	40.6%	41.8%	1.2
BlackBerry	3.8%	3.4%	-0.4
Microsoft	3.3%	3.1%	-0.2
Symbian	0.3%	0.2%	-0.1
Total Smartphone Subscribers	**100.0%**	**100.0%**	

Table 1. Top Smartphone Platforms (from [1]).

Mobile phones use flash-memory [3] to store the base mobile operating system (OS), applications (apps), and user data. First-party applications are software created by the operating-system provider. For example, the Android smartphone includes a phonebook, a calendar and text-messaging applications created by Google's own software-development team. Third-party applications are created by developers other than the provider of the mobile operating system.

The internal flash memory of a mobile device contains several types of user-generated information such as phone numbers, addresses, Short Message Service (SMS)

text messages, and cell data. These data can be extracted with the use of digital forensics tools and used to profile a user's activity. Digital forensics is a branch of forensic science that investigates digital information stored in various electronic media. It can help investigate cybercrime, computer-based terrorism, and computer hacking involving digital environments.

All smartphones provide a way to erase (reset) personal information from flash memory. The main focus of this thesis will be to evaluate the effectiveness of "factory data reset" feature on smartphones. A detailed and comprehensive survey can benefit not only the forensic community, but also anyone who uses a smartphone. The end result will help illustrate the limits of privacy protection offered by factory-reset features. It can also contribute to improved smartphone security and privacy policies if venders use this research to improve their products.

B. RESEARCH QUESTIONS

This thesis attempts to answer one primary question:

- How much user-generated data is left on a smartphone after using the mobile phone's factory reset/wipe function?

Two secondary questions also need to be addressed:

- How much private/personal information can be extracted after the wipe?
- Can recovered data be used to identify or profile a user?

C. THESIS STRUCTURE

The remainder of the thesis is organized as follows. Chapter II will discuss prior work in mobile forensics and similar research work done under this topic. Chapter III will cover the process of forensics research all hardware, software and computer environments used in these experiments. Chapter IV will cover experiments with some sample memory images. Chapter V will end with conclusions and propose future research work.

II. BACKGROUND AND RELATED WORK

A. GROWTH OF SMARTPHONES AND MOBILE COMPUTERING

Mobile phones have become a significant consumer product in recent years. A telephone survey by Google Inc. of 2,000 adults in five countries [4] found that consumers own mobile phones more than any other mobile devices As Table 3 depicts, the survey found that Japan has highest adoption rate of mobile phones (96%), followed by the United Kingdom (87%).

	United States	United Kingdom	France	Germany	Japan
Feature phone/Smartphone	78%	87%	74%	76%	96%
Media player with web access	24%	17%	23%	12%	30%
Tablet PC Slate/Pad	9%	4%	3%	3%	5%
Handheld gaming device	15%	17%	14%	7%	42%
eReader	9%	3%	1%	1%	2%

Table 2. Mobile Internet & Smartphone Adoption: October 2011 (from [4]).

A smartphone contains much of the functionality of a desktop PC, but it also includes radio communications capabilities that desktop PCs typically lack. Communication functionalities include GSM/CDMA radio, Near Field Communications, GPS, Wi-Fi and Bluetooth communication. The high mobility of these devices can be the most important factor in the shift from desktop/laptop computer to smartphones. Unlike laptops or desktop computers, a smartphone can easily fit in a pocket. It is a computer that is easy to use and small enough to be used almost anywhere. A user can browse the Internet, check email, use GPS navigation, and make online payments from personal bank accounts. Hence, a device this capable is also likely to contain personal user data.

There are various ways a user can protect his or her personal information on smartphones. Android and iOS phones can be set up require a login password. Some phones include a data encryption method to protect sensitive data. Also, third-party

developers' market mobile protection/encryption software [5] can be installed on both Android and iOS phones. The iPhone has hardware encryption enabled by default for all data stored in memory. There is also a Data Protection API provided by Apple that can be used to implement application-level encryption.

In addition, common smartphones on the market today include some kind of "factory reset" feature. A factory reset is similar to formatting a hard disk drive on a computer system, but the details differ. Formatting deletes all pre-existing partitions and data on the hard drive and creates a new file system. The factory reset is intended to remove everything except pre-installed software, deleting user data in particular.

The following is a list of data that should be erased by the factory reset [6], [7].

- User account information (including email address)
- User settings for the operating system and applications
- Downloaded third-party applications
- Downloaded music (.mp3s, .flac, and .aac)
- Downloaded images and photos taken by the camera (.jpg, .png)
- Other user data (address book/phone book/calendar data)

The data that should be left behind after a factory reset is:

- The operating system installed with the smartphone
- First-party software (the operating system and associated software of the main vendor) and software (by other vendors authorized by the main vendor) bundled with the operating system
- SD card files, as contrasted with files on the main flash memory on the phone

B. PRIOR WORK

Very little academic research has been conducted regarding the correctness of the factory reset feature on smartphones. However, there have been numerous articles on technology websites discussing potential risks [8], [9], [10]. The following are examples of the kinds of data left behind after a factor reset, from the *GottaBeMobile: Mobile News & Reviews* website:

- Porn
- Court records
- Social Security Numbers
- Resumes
- College applications
- Cookies
- Child support documents
- Employee records
- Bank statements
- Credit card statements
- Tax returns
- Emails
- Contact lists
- Photos

The authors tested secondhand phones purchased through Craigslist, which they then reset using the factory feature. The article concluded that the factory-reset feature did not work as expected.

Another publication studied the effectiveness of the factory reset for network data structures left on an Android device [11]. The primary question was "Do sufficient residual artifacts exist on mobile devices to extract enough data to identify the device's previous network access points?" The research used controlled data transfers between Android smartphones and multiple network access points (cellular, wireless, and Bluetooth). Residual data left on test devices included "userdata" partitions containing Service Set Identifiers (SSID), wireless-router Subscriber Identity Modules (SIM), DHCP ACKs from wireless routers, and base-station metadata that included the Mobile Network Code (MNC), Mobile Country Code (MCC), Local Area Code (LAC) and Cell Identification (CID), wireless router Media Access control (MAC) addresses, and Bluetooth MAC address of devices paired with the phone. It concluded that the factory-reset feature was not sufficient in deleting user-generated network data.

This thesis expands the research scope by analyzing all user-generated content. It analyzes all types of residual artifacts left behind after a factory reset.

THIS PAGE INTENTIONALLY LEFT BLANK

III. DIGITAL FORENSICS TOOLS

A. COMPUTER FORENSICS

Computer forensic investigations follow a similar process to other forensic investigations [12]. The process involves acquisition, analysis and reporting of potential evidence involving criminal activity. The evidence can be collected from any type of storage media. Examples of storage media are:

- A hard disk drive from computer system
- A CD/DVD/Blu-ray optical disk
- A MO magnetic disk
- A CF/SM/MMC memory card
- A mobile SIM card
- A USB flash memory

Forensic tools can be used to acquire data from storage media by physical or logical acquisition. Physical acquisition is a bit-by-bit copy of an entire physical store of data. Logical acquisition is a bit-by-bit copy of the logical storage object such as directories and files.

The National Institute of Standards and Technology provides guidelines for forensic data acquisition and specifications for forensic tools [13]. NIST's Computer Forensics Tool Testing (CFTT) program establishes the methodology for testing computer forensic software. CFTT is part of the Software Diagnostics and Conformance Testing Division which is supported by The Office of Law Enforcement Standards. The project provides a means to help understand the capability, limitations, and validity of computer forensics tools. The tools to be tested are broken up into several categories: disk imaging, forensic media preparation; write-blocking software, write-blocking hardware, and mobile devices.

Disk imaging is the process of making a secure forensically sound copy of digital media that can retain the data for an extended period. "Disk Imaging takes sector-by-

sector copy usually for forensic purposes and as such it will contain some mechanism to prove that the copy is exact and has not been altered." [14].

Forensic media preparation is the practice of wiping the target media before storing forensics data onto the forensics examiner's computer. A hard disk drive is usually used as a target media to store collected data. A wiping process prevents collected data on the target media from being "contaminated" by previously collected evidential data. A wipe should completely delete the existing data by overwriting all writable parts of the media. The Unix "dd" command is a common utility used to wipe storage media [15], and it can also be used to wipe data from internal flash memory in mobile phones. Write blockers are write-protection utilities used in the acquisition of digital forensic data. These utilities enable examiners to create images of media devices without the risk of accidentally writing to the subject media and thereby altering the contents [16].

Several forensic techniques have been developed to help investigations such as string search, memory forensics, file extraction, feature extraction, and cross-drive analysis [17], [18], [19], [20]. These techniques increase the utility of captured data in forensics analysis. Memory forensics analyzes information stored on volatile memory, internal memory inside a computer or mobile device that requires power to maintain. The data stored in the memory changes frequently while the computer or mobile device is operational, which makes it hard to verify the data collected from memory. This can lead to problems if the examiner wants to run the acquisition process more than once [21].

String searching is a process of locating specific ASCII or Unicode strings from text files and directories. These strings can be names, phone numbers, email addresses, country codes, IP addresses, or software installed on a system. The examiner can look for any type of key terms or single words, but it can also help spot patterns in a system. Regular expressions can be used to describe patterns in a string. An example regular expression is "/^[a-z0-9_-]/ " which will look for any string that begins (^) with a lower case letter (a-z) followed by any number (0-9) then an underscore and a hyphen.

B. MOBILE FORENSICS

Mobile forensics has its own set of acquisition tools [22], [23], [24]. Imaging, forensic extraction, memory forensics, and string searching can all be applied to mobile forensics investigations. However, there are some differences. Hard disk drives can easily be removed from a computer system for data acquisition and analysis, and during this process the hard disk drives can be protected using a write blocker utility. A mobile device cannot be processed the same way because the internal flash memory is usually soldered onto the circuit board, and removing the flash memory may damage it. Most mobile forensics tools do not require for the flash memory to be removed, but connect the phone directly into a forensics hardware tool, or plug the phone into a computer system running the forensics software [25]. The mobile phone architecture is also different from a standard desktop computer. The mobile hardware supports various radio communications like GSM/CDMA, GPS, Wi-Fi, NFC and Bluetooth. This radio communication capability will generate additional user data on the smartphone. The GSM/CDMA and GPS radios store geolocation data. Wi-Fi, NFC and Bluetooth may store user account login information and passwords. User data are locally stored on the smartphone's flash memory.

C. MOBILE FORENSIC TOOL CELLEBRITE UFED

A commercial forensics tool from Cellebrite was used for the data extraction process in our experiments. The Cellebrite UME-36 Pro is a standalone phone-memory transfer and backup solution that is capable of extracting data from a wide variety of mobile devices [26]. There are three key components for this forensics tool:

- Cellebrite UME-36 Pro – Universal Memory Exchanger 1.2.2.3
- Cellebrite UFED Physical Analyzer 3.7.2.0
- Cellebrite Phone Detective 1.2

The UME-36 Pro enables logical, password, SIM, file-system, and physical extractions of data from mobile devices. It is a hardware solution for data extraction. The extracted data can be viewed and analyzed with the UFED Physical Analyzer software. UME-36 Pro claims to extract the following data from a smartphone [27]:

- Call logs
- Contacts
- Email
- Pattern locks
- Bookmarks
- Cookies
- Text strings from Short Message Service (SMS) / Multimedia Messaging Service (MMS)
- Chat messages
- Location data including cell tower locations and usage
- Web browser history including records of visited websites
- Digital photography, digital videos, and audio files
- Text files
- Deleted data
- Wi-Fi including connection times, base service set identifications (BSSId), service set identifiers (SSID), and Security Modes
- GPS information added to media files (geotags)

The UFED Physical Analyzer is software for physical extraction. This extraction creates a single binary extraction file for each embedded flash memory chip, or at least by the address range used by the mobile device. Unlike logical extraction, physical extraction can bypass the device's operating system and extract data directly from the mobile device's internal flash memory. The UFED-extracted data from the device is saved into a hexadecimal file that is later read and decoded using the UFED Physical Analyzer application. The images created from the physical extraction process include files deleted by the operating system or user. The images are saved with an .ufd extension. It provides an overview of the mobile-device data with decoding, analysis, and report generation [28].

The Cellebrite Phone Detective application helps investigators identify a mobile phone by its physical attributes, eliminating the need to start the device and risk device lock or possible data loss. It asks eight key questions regarding the phones' physical appearance. It provides the user with a detailed extraction capability per device,

connectivity details and device characteristics [29]. The eight visual elements used to identify device are:

- Phone type (candy bar, clamshell, slider, tablet)
- Body (connection port, cable, charging socket)
- Power button (power, volume, camera, keypad)
- Miscellaneous (battery cover type, memory card slot)
- Basic (Brand logo: Apple, HTC, Acer, LG / network technology: GSM, CDMA)
- Camera (type, location, flash)
- Display type (touch, non-touch, stylus)

D. MOBILE FORENSIC TOOL BULK EXTRACTOR

The forensics software Bulk Extractor (bulk_extractor-1.4.1-windowsinstaller.exe) [30] was also used for analysis of recovered files. Bulk Extractor is a carving and feature extraction tool that can be used on all kinds of digital media. It can scan disk images (raw, split-raw, EnCase E01, AFF), files and directories to extract useful information without parsing the file system or file system structures. The program can extract phone numbers, email addresses, credit card numbers and URLs from inspection of file contents of any file or file fragments. It can also collect data from compressed files with ZIP and gzip algorithms. The extractor is run on a file system and creates a report directory with feature files. Each feature file contains the location the feature found, the feature itself, and the feature surrounded by its local context (e.g., email.txt, url.txt). The tool is generally used for file identification and cross-drive analysis [31].

E. OTHER MOBILE FORENSICS TOOLS TESTED

Several other forensics tools were tested for this research project before we selected Cellebrite. Some that offer similar features to the Cellebrite UFED tools were as follows.

viaExtract: This is a mobile forensics tool developed and distributed by viaForensics [32]. It is designed for extracting and analyzing data from Android smartphones. It is distributed as a standalone virtual appliance that runs on a VMware

workstation. The pre-installed extraction tools could not properly analyze several Android phones. It would often return an error during the extraction process on our test phones.

Key features:

- Temporarily or permanently remove a password/pattern/PIN lock on an Android device running OS 2.2 or higher.
- Allow the examiner to forensically image external (SD) and internal (EMMC) storage cards directly from the device.
- Allow examiners an additional bypass option on gesture key locked devices.

Oxygen Forensic Suite 2013: This forensics suite is developed and distributed by Oxygen Software [33]. The company specializes in forensic data examination tools for smartphones and mobile devices. The program performed fairly well and could recovery a large number of files (images, video, system files, logs).

Key features:

- Displays complete technical information about the mobile device.
- Extracts user contact information with all its data: name, occupation, phone numbers, addresses, emails, notes.
- Extracts event log data, phonebook, messages (SMS, MMS, Emails, iMessages).
- File browser analyzes user phones, videos, documents and device databases.

Recuva: This is a free program developed and distributed by Priform [34]. It is a disk recovery tool that is capable of extracting files deleted or damaged on media devices. The program can recover a large number of files from the internal flash memory of a smartphone. However, the program does not provide an analysis tool for the recovered data. This makes the file analysis very difficult. Several files could not be opened or viewed with the program.

Key features:

- Undelete files.
- Recover damaged or formatted disks.

- Recover deleted emails.
- Recover deleted iPod music.
- Restore unsaved documents.
- Perform deep scan.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. EXPERIMENTS

A. CONTROLLED EXPERIMENT WITH TWO SMARTPHONES

Two smartphones were used for a controlled experiment: an Apple iPhone 4S and a Samsung Galaxy SIII. The following protocol was used to artificially generate data under a controlled environment.

- Log into the Android phone with the account forensic.nps@gmail.com, and the iPhone with the account rschwamm@nps.edu.
- Connect to NPS wireless network (NGSTV224) and visit 4 websites using default browser
  1. Nps.edu
  2. Fark.com
  3. Yahoo.com
  4. Npr.org
- Take six pictures with built in camera: 6 pictures of the numbers 1, 2, 3, 4, 5, 6. First 3 image files are left unaltered. Second 3 image files manually renamed:
  - testschwamm_pic_4
  - testschwamm_pic_5
  - testschwamm_pic_6
- Access files and links from the following website:

  http://faculty.nps.edu/ncrowe/testschwamm0114__doc_sample.docx
  http://faculty.nps.edu/ncrowe/testschwamm0114__pdf_sample.pdf
  http://faculty.nps.edu/ncrowe/testschwamm0114__ppt_sample.pptx
  http://faculty.nps.edu/ncrowe/testschwamm0114__wav_sample.wav

  http://faculty.nps.edu/ncrowe/testschwamm_0114_link.html
  http://faculty.nps.edu/ncrowe/testschwamm_0114_pics.html
  http://faculty.nps.edu/ncrowe/testschwamm_0114_video.html
  http://faculty.nps.edu/ncrowe/testschwamm0114_feat.html

- Install the following list of software for Android phones:

  "Reddit is fun"
  https://play.google.com/store/apps/details?id=com.andrewshu.android.reddit&hl=en
  Visit 3 postings on www.reddit.com

- "ELI5: The Amanda Knox Appeal" http://www.reddit.com/r/explainlikeimfive/comments/1wlin9/eli5_the_amanda_knox_appeal/
- "Why are the wheels of NASA's Mars rover, Curiosity, wearing out?" http://www.reddit.com/r/askscience/comments/1wnb8s/why_are_the_wheels_of_nasas_mars_rover_curiosity/
- "Hey, I am Nikki Sixx from Motley Crue, AMA" http://www.reddit.com/r/IAmA/comments/1wnsxv/hey_i_am_nikki_sixx_from_m%C3%B6tley_cr%C3%BCe_ama/

"Facebook"
https://play.google.com/store/apps/details?id=com.facebook.katana&hl=en
Login and browse.

"Google Drive"
https://play.google.com/store/apps/details?id=com.google.android.apps.docs&hl=en
Login/sync and open 3 files
- testschwamm_ppt1.pptx
- testschwamm_ppt2.pptx
- testschwamm_ppt3.pptx

"DropBox"
https://play.google.com/store/apps/details?id=com.dropbox.android&hl=en
Login/sync and open 3 files
- testschwamm_doc1.docx
- testschwamm_doc2.docx
- testschwamm_doc3.docx

"Youtube"
https://play.google.com/store/apps/details?id=com.google.android.youtube&hl=en
Login and watch 3 videos
- 'PSY-GANGNAM STYLE' http://www.youtube.com/watch?v=9bZkp7q19f0
- 'GIFs, now with sound!' http://www.youtube.com/watch?v=CgVpR4KdLRA
- 'BEST DUBSTEP CAT!' http://www.youtube.com/watch?v=i4SSoWEw5CI

"Audible"
https://play.google.com/store/apps/details?id=com.audible.application&hl=en
Login and download/listen to 3 excerpts
- Bossypants (Excerpt)
- The Hunger Games (Excerpt)
- Matterhorn (Excerpt)

"Kindle"
https://play.google.com/store/apps/details?id=com.amazon.kindle&hl=en
Login and open 3 PDF files
- testschwamm_article1.pdf
- testschwamm_article2.pdf
- testschwamm_article3.pdf

- Upload a text document 'testschwamm_password.txt' to root directory of each phone.
- Upload zip file containing above text named 'testschwamm_userdata.zip' to root directory of each phone
- Use the following list of pre-installed software on iPhone:

"Youtube"
Login and watch 3 videos
- 'PSY-GANGNAM STYLE'
  http://www.youtube.com/watch?v=9bZkp7q19f0
- 'GIFs, now with sound!'
  http://www.youtube.com/watch?v=CgVpR4KdLRA
- 'BEST DUBSTEP CAT!'
  http://www.youtube.com/watch?v=i4SSoWEw5CI

"Notes"
Create 3 note entries
- DVD Movie List
- Shopping List
- Test date and homework due date

"Remind Me"
Create 3 reminders different dates
- 'Reminder 1' '02/01/2014 5:00PM'
- 'Reminder 2' '03/03/20145 7:00AM'
- 'Reminder 3' '04/05/2014 11:00AM'

The phones were not password protected by the user and no data intentionally encoded or encrypted by the phone. Following use, a factory reset was performed through

the phone's setup menu under "Privacy" or "Backup & Reset". The reset menu lists all data that will be erased in the process (User account, system and application data and settings, downloaded applications, music, pictures and other user data). The user did not have any selectable options for the reset on any of the phones. The process takes a few minutes after which the phone restarts and resumes normal operation.

Following factory reset, the phones were images with the UME-36 Pro and UFED Physical Analyzer. All images were saved in the tools proprietary format (.ufd).

A total of 61,276 files were recovered from the pre-wipe for the iPhone and 43,165 from the post-wipe. 42,728 files matched path and contents from both pre-wipe and post-wipe. Partial matches were deleted which produced 17,914 pre-reset files and 115 post-reset files that did not match. 36,292 files had a zero size from the pre-wipe and 36,319 files had zero size from the post-wipe. Executable ".app" files found pre-wipe were 24,862, and 8,062 post-wipe. Files relating to the operating system were 29,812 pre-wipe and 27,621 post-wipe.

Overall, the reset did a good job of removing third-party software. All the picture images and text documents were deleted by the reset with the exception of some cache and settings information (YouTube, Facebook).

The Bulk Extractor was used for string search. A number of preference and configuration files were recovered after the reset but none containing the keywords. "Preferences" can include private user information [35], but none were seen in the ".plist" preference files. Table 3 lists some sample files remaining after the reset that could be interesting for forensic investigations. The indirect information can be collected and used to profile a user. A forensic investigator could determine where and how the device was used.

File	Description
System/InnsbruckTaos11B554a.N90OS/System/Library/PrivateFrameworks/Preferences.framework/SupplementalLocaleData.plist	Location and language settings
System/InnsbruckTaos11B554a.N90OS/usr/share/mecabra/ja /rerank.dat	Resource rankings?
Data/Data/Keychains/keychain-2.db	Keys
Data/Data/logs/lockdownd.log	Security event log
Data/Data/mobile/Applications/B8AD4B05-2518-4570-8447-7BE2BFDA8F9F/Library /Preferences/com.apple.mobilesafari.plist	Browser preferences
Data/Data/mobile/Library /BulletinBoard/SectionInfo.plist	Bulletin board index
Data/Data/mobile/Library /Caches/com.apple.springboard /Cache.db-wal	Screen cache for user "wal"
Data/Data/mobile/Library /Cookies/com.apple.itunesstored.2.sqlitedb	Cookies for iTunes
Data/Data/mobile/Library/Mail /Content Index	Mail keywords
Data/Data/mobile/Library/Maps /Bookmarks.plist	Map bookmarks
Data/Data/mobile/Library /Preferences/com.apple.identityservicesd.plist	Account information
Data/Data/mobile/Media /PhotoData/changes-shm	Incremental photo data
Data/Data/root/Library/Caches /locationd/consolidated.db	Location data
Data/Data/tmp/MediaCache /diskcacherepository.plist	Disk cache information

Table 3. Sample files from post-wipe iPhone

A total of 5,141 files were recovered from the pre-wipe for the Android phone and 3,578 from the post-wipe. 3,292 files matched path and content from both pre-wipe and post-wipe. Partial matches were deleted which produced 968 pre-wipe and 65 post-wipe that did not match. 227 files had a zero size from the pre-wipe and 278 files had zero size form the post-wipe. Executable ".apk" files found pre-wipe were 396, and 277 post-wipe. Other executable files such as ".dex" files went from 140 pre-wipe to 121 post-wipe. ".so" files from 302 to 254. The reset did not delete any picture images taken with the camera. None of the created text files (.txt, .doc, .pdf, .ppt) was removed. Cache and deleted copies of these file and image components were also not erased. Third-party applications were deleted. However, following the wipe we could recover files from the Kindle and DropBox applications that belonged to the user. These files should have been deleted along with the application. The fact that files from deleted applications were

found post-wipe implies that the wipe process explicitly deleted files, a topic that we will return to in Chapter V.

The Bulk Extractor was used again for additional string search. Website links were all deleted in the reset. However, the links for the four visited websites were found in various files pre-wipe. A total of 116 links were found pre-wipe. It is unclear why there were so many duplicate links saved on the phone. The wipe left most of the operation system files intact just like the iPhone reset. Table 4 lists some sample files remaining after the reset that could be interesting for forensic investigations.

File	**Description**
CACHE/Root/recovery /last_log	Recovery log
SYSTEM/Root /addon.d /blacklist	Four MD5 hash values
SYSTEM/Root/etc/apns-conf.xml	Phone carrier IP address
SYSTEM/Root/etc /audio_policy.conf	Attached audio devices listing
SYSTEM/Root/etc/gps.xml	GPS settings
USERDATA/Root/backup /pending/journal2114683955.tmp	Data backup
USERDATA/Root/data/com.android.providers.calendar/databases/calendar.db	Calendar data
USERDATA/Root/data/com.android.deskclock/databases/alarms.db	Alarm data
USERDATA/Root/media/0 /amazonmp3/temp/log.txt	Log file of Amazon Cloud Player
USERDATA/Root/media/0/Android/data/com.andrew.apollo/cache/ImageCache/3910b1e0ccab19bc46fd9db27cca49c9.0	Image cache data
USERDATA/Root/media/0/iPhone3G.2013-11-07.16-39-30/Email/108/478/1256.sql	Database script of ours, unclear how it got here
USERDATA/Root/misc /wifi/softap.conf	Access point data
USERDATA/Root/system/users/userlist.xml	User ID information
USERDATA/Root/drm /fwdlock/kek.dat	Lock data
USERDATA/Root/media/0/And-roid/data/com.dropbox.android /files/scratch/09thesis_regan.pdf	Document of previous phone user

Table 4. Sample files from post-wipe Android phone

Some smartphones provide several variations for reset. A “hard reset” can be performed by using the hardware keys (by a procedure specific to each device). Newer iPhones provide the additional reset options “Reset All Settings,” “Reset Network

Settings," "Reset Keyboard and Dictionary," "Reset Home Screen Layout,, and "Reset Location and Memory". All of these options were used and a new post-wipe image was generated. These options deleted an additional 222 files from the phone but did not delete any files listed in Table 3. The additional reset options did not produce any significant further deletions.

The hard reset on the Android phone gave an additional option for a "cache reset". This option was used and a new post-wipe image was generated just like the iPhone. It did not delete any text and media files put on the device; it only deleted the sixth file of the files in Table 4. Four files with the "db" extension were deleted. The reset added an additional six files (two Bluetooth cache, four "telephony"), but did not do much beyond the regular reset.

B. EXPERIMENT AND DATA EXTRACTION

Two sets of smartphones were used for the main experiment. The first set of Apple iPhone images was created by the UME-36 Pro and UFED Physical Analyzer. These images were taken from the Real Data Corpus [36], a large-scale forensic corpus. All images were generated from legally obtained smartphones used by real people. The second set was of various smartphones (iPhone, Android, Blackberry) that had been used for other research projects at our school. These phones did not have a SIM card installed on them. SIM cards contain a unique identification number associated with the user's mobile account and contain the phone number, security data and billing information; phone calls cannot be made without a SIM card, but otherwise the phone will function normally. A few of the phones came with a custom Android operating system (CyanogenMod 10.1), a custom aftermarket firmware based on the Android Open Source Project [37] [38]. The same protocol was used to generate data but no accounts were associated with the Blackberry phones. A Python script was written to convert the Cellebrite proprietary XML report format to the forensic metadata standard DFXML [39]. A taxonomy created [40] was used to classify files by extension and directory path. The full list of smartphones and the status is listed in Table 5.

#	Smartphone	OS Version	Readiness
I1	Apple iPhone 4	iOS 5.1.1	OK
I2	Apple iPhone 4	iOS 5.1.1	OK
I3	Apple iPhone 2	iOS 3.1.3	OK
I4	Apple iPhone 2	iOS 3.1.3	OK
I5	Apple iPhone 2	iOS 3.1.3	OK
I6	Apple iPhone 2	iOS 3.1.3	OK
I7	Apple iPhone 2	iOS 3.1.3	OK
I8	Apple iPhone 2	iOS 3.0	OK
I9	Samsung Galaxy SIII	CyanogenMod 10.1	Hard reset
A10	Samsung Nexus	CyanogenMod 10.1	OK
A11	Samsung Galaxy Anycall	Android 1.5	OK
A12	Motorola Atrix 4G	Android 2.2	OK
A13	HTC Droid Eris	Android 2.1	OK
A14	HTC Magic	Android 1.6	Hard reset
A15	HTC Flyer (tablet)	Android 3.2	OK
A16	HTC One	Android 4.1	OK
B17	BlackBerry 8900 Curve	BlackBerry OS 4	Unusable after reset
I18	Apple iPhone 4S	iOS 5.1.1	OK
I19	Apple iPhone 2G	iOS 3.13	Unusable without SIM card
B20	BlackBerry 8100 Pearl	BlackBerry OS 4.5.0.174	OK
B21	BlackBerry 8300 Curve	BlackBerry OS 4.5.0.162	OK
A22	Motorola FIRE	Android 2.3.4	Unrecognized by Cellebrite
A23	Huawei U8500	Android 2.1	OK
A24	Huawei U8150 IDEOS Comet	Android 2.2	Unusable after reset
A25	Dell XCD35	Android 2.2	OK
I26	Apple iPhone 2	iOS 3.1.3	Unusable after reset
A27	Motorola Charm	Android 2.1	Totally dead
p28	LG-500GHL	Unknown	Unrecognized by Cellebrite

Table 5. Full list of smartphone and status (from [41], [42]).

Table 6 list the total counts of pre-wipe and post-wipe files. A large number of files were not affected by the reset. There were four types of partial matches between pre-wipe and post-wipe files (File name and hash, Hash only, File path only, Path ignoring digits). Several unmatched files were found post-wipe which appear to be new records created by the operating systems activity and reset feature. The factory reset does not completely wipe a device. Several files are removed during the reset but others are just renamed and additional new files are added after the reset.

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-wipe and post-wipe	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

Table 6. Summary data from 21 smartphones

The file taxonomy was used to further investigate what types of files are being removed in the reset. The full results are listed in Table 7. Each file path is classified by file extension (E) and directory name of the file (D). 8,346 extensions and 6,445 directory names have a classification. The rest are labeled as "miscellaneous". Extensions that are longer than 10 characters are ignored.

The reset appears to focus on video and picture images, text documents, copies and temporary files, disk images, log files, XML documents and gaming applications. There is a smaller emphasis on database files, compressed data, audio, source code and data directories. The reset seem to target applications, picture images and temporary files, but not as focused on long-term user data. The reset does not remove explicitly deleted and zero-size files (which have no content but do have filename and dates). Zero-size files may not be useful for the applications, but could provide partial user information. An empty log file could indicate the user is not using a particular category or parameter in an application.

A clear time pattern could not be created because the phones were used in various time periods. The Physical Analyzer software also created some issues while analyzing the recovered data. Different versions of the Physical Analyzer would produce different results from the same image. The file access and creation time would be reported differently depending on the Physical Analyzer version, and the root directory name would change between two different Physical Analyzer versions.

Type of file extension (E) or directory (D)	Pre-wipe	Post-wipe
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: Database	5627	2377
E: Spreadsheets	425	356
E: Compressed	601	278
E: Audio	16427	8313
E: Video	303	90
E: Source code	1791	736
E: Executable	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
E: Miscellaneous	7307	3536
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
D: Miscellaneous	2046	1126
".DELETED." in path(*)	20087	4181
Zero-size files	120112	128026

Table 7. File type counts before and after the factory reset.

(*) Paths containing the word ".DELETED" were found on the phone.

The data collected from the Physical Analyzer are listed in Table 8 and 9. The Physical Analyzer categorizes each data type and groups.

Phone Data:

- **Application Usage:** Applications name, number of launches, activations, active time, and date
- **Call Log:** Caller phone number, time stamp, duration, and type (incoming/outgoing/missed).
- **Contacts Cookies:** Contacts name, organizations, phone number, emails, other entries, notes, and addresses.
- **Installed Applications**: Application name, version, identifier, App 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, folder (drafts, inbox, sent), phone number, text string, and status (unsent, sent, or read).
- **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

Data Files:

- Picture Images (png, jpg), Audio (wav, mp3), Text (html, txt, xml), Databases (db, sqlite3, itdb), Configuration (plist), or Application (jar, apk, ipa).
- Name, path, size, metadata, created, modified, accessed, and bookmark note.

	I1	I2	I3	I4	I5	I6	I7	I8
Phone Type	I	I	I	I	I	I	I	I
Application 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 Applications	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
Configurations	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 8. The number represents user data and system data on smartphones part 1. (post-wipe/pre-wipe) I=iPhone, A=Android, B=BlackBerry

	A9	A10	A11	A12	A13	A14	A15	A16	I18	B20	B21	A25
Phone Type	A	A	A	A	A	A	A	A	I	B	B	A
Application Usage	0/0	1/139	0/0	0/102	0/0	0/0	0/0	0/0	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	0/1	0/100	0/11	0/61
Contacts	0/0	0/5	0/0	0/48	0/0	0/2	0/0	0/65	0/0	0/477	0/0	5/252
Cookies	0/0	0/3	0/0	0/0	0/0	0/5	0/0	0/0	0/17	0/0	0/0	0/16
Installed Applications	30/30	48/102	25/43	23/32	26/70	20/24	12/44	0/0	34/34	0/0	0/0	0/1
IP Connections	0/0	0/2	0/0	0/3	0/0	0/1	0/0	0/0	1/6	0/0	0/0	0/0
Locations	0/0	0/0	0/5	0/0	0/10	0/0	0/0	0/0	0/0	0/0	0/0	0/9
Maps	0/15	0/5	0/8	0/0	0/0	0/0	0/0	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	5/9	0/0	0/0	0/1
SMS Messages	0/80	0/5	0/0	0/121	0/0	0/2	0/0	0/66	0/0	0/4	0/0	0/76
User Accounts	1/1	1/1	0/0	0/0	0/1	0/1	0/0	0/1	1/1	0/0	0/0	0/2
User Dictionary	0/132	0/50	0/0	0/84	0/40	0/1	0/0	0/0	0/6	0/0	0/0	0/2
Wireless Networks	0/1	0/1	0/0	0/1	0/0	0/0	0/1	0/0	3/7	0/0	0/0	0/1
Images	150/150	764/764	11/11	1815/1815	42/42	15/15	9/9	616/616	3716/3743	0/7	0/3	71/159
Audio	1/1	1/1	1/1	1/1	0/0	2/2	2/2	82/82	1/1	0/1	0/0	1/1
Text	130/130	48/48	0/0	132/132	1/1	0/0	4/4	1/1	243/263	0/0	0/0	440/3031
Databases	5/65	12/45	0/0	25/41	0/0	10/24	0/0	16/36	37/58	0/0	0/0	24/55
Configurations	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	2850/2953	0/0	0/0	0/0
Applications	0/0	313/313	0/0	7/7	3/3	1/1	24/24	0/3	6/6	0/0	0/0	388/390

Table 9. The number represents user data and system data on smartphone part 2 (post-wipe/pre-wipe) I=iPhone, A=Android, B=BlackBerry

C. ISSUES WITH THE SMARTPHONES

The factory reset was performed without any problems on most of the smartphones. However, on the HTC Magic (A14) and Samsung Galaxy SIII (A9) the smartphones locked up after the reset. The HTC Magic was running a standard Android 1.6 operating system and the Samsung Galaxy SIII was running a custom CyanogenMod 10.1 operating system. A hard reset on the HTC Magic and a custom reset had to be performed on the Samsung Galaxy SIII running CyanogenMod 10.1 to recover normal operations. Holding down the volume up button and the power button at the same time performs a hard reset, but does not remove any applications or user data from the smartphone. After the hard reset the factory reset did not cause any further problems. The cause of the lockup could not be determined.

The factory-reset on the BlackBerry 8900 Curve (B17), Huawei U8150 Comet (A24) and Apple iPhone 2 (I26) made the devices unusable after the restart. The device could not be properly restarted or became unstable. The Motorola Charm (A27) could not be charged or booted and appeared to be unusable.

The HTC Eris (A13) could not be properly processed without a micro SD card and installed on the phone. The Apple iPhone 2G (I19) could not be used without a SIM card. Both the UME36-Pro and UFED Physical analyzer returned an error when there was no micro SD or SIM card in the phone. A compatible micro SD/SIM card was not available at the time of the experiment. These two phones were the only ones that produced this error. The cause of the error could not be determined.

The Motorola FIRE (A22) and LG-500GHL (p28) was not recognized by Cellebrite. The Motorola FIRE is running the Android OS 2.3.4 and is officially supported by UFED Touch Ultimate. The LG-500GHL is a prepaid phone with a proprietary operating system by LG. None of the forensics tools tested was able to identify or extract data from these phones. This could be due to the proprietary operating system installed on the LG phone.

The HTC One returned the same results for most of the tools tested. There is an important difference between the HTC One and the other smartphones used in this project. When a smartphone is connected (via USB) to a computer system it is mounted as a USB mass storage device. The HTC One and several newer Android phones (4.0 and up) are connected using a different protocol developed by Microsoft called the Media Transfer Protocol (MTP) [43]. The computer sees the attached smartphone as a media player while connected with MTP. The different mounting protocols created conflict with the forensics tools used for this project. However, during this research project we were able to gain access to a newer Cellebrite hardware solution, the Cellebrite UFED Touch Ultimate [44], an updated version of the UME-36 Pro. It provides a touchscreen interface with Windows XP running as the base operating system. It provides the same functionality with a wider range of supported mobile devices. The UFED Touch Ultimate is capable of extracting data from MTP devices and was used for the HTC One (A16).

D. DATA ANALYSIS WITH THE PHYSICAL ANALYZER

A list of extracted data was created and viewed in the Physical Analyzer application. All phones listed in Table 8 and 9 were used (Android, IPhone, BlackBerry). Phone data (traditional telephone usage information) in both sets was almost completely removed after a factory reset, including:

- Call log
- Contacts
- Cookies
- IP connections
- SMS
- Maps
- Password
- User directory

Application Usage data were limited to system applications and did not contain any user information. System applications are indicated by the identifier com.apple.XX for iOS and com.google.XX for Android. A list is generated by the Physical Analyzer.

Installed Applications data left on the phones were default first-party applications such as maps, YouTube, mobile mail, calculator, weather, preferences, and mobile notes. The same system application identifiers were used to verify first-party applications. There were no third-party applications left on the phones after a factory reset. However, the number of installed applications on post-wipe phones varied. The Physical Analyzer could not identify any user-installed applications on the I7 and I8 iPhones after the factory reset. The system applications and first-party applications are not supposed to be removed after a factory reset. The Physical Analyzer showed zero entries after the wipe. This means the UME-36 Pro could not properly identify the applications. The reasons are unknown as to why the UME-36 Pro failed to identify the installed applications.

Location data were only left on the I6: Apple iPhone 2. The data contained latitude and longitude (18.47717, 73.87550 – Pune, India) information for a cell tower and a time stamp (3/24/2011 7:44:24AM). This can be considering sensitive user information since it reveals the time, date, and location of where the user has been.

User Accounts and Wireless Networks data was recovered from a number of phones but it did not contain any identifiable information. Entries were listed in the Physical Analyzer but it did not contain any data (user name, email, BSSId, SSId, password). It identified a previously existing account, but could not recover any additional user or network data. The account information could have been encrypted or encoded after the reset.

JPEG and PNG image files were not removed from any of the Android phones by the factory reset. All picture images (downloaded, camera, and browser thumbnails) are supposed to be removed after a reset. All picture images were left on those phones untouched and were still viewable within the smartphone. The 6 images added before the reset was also left untouched and viewable in the smartphone. The iPhones did a better job at wiping the images and none of the image files including thumbnails were viewable after the factory reset. However, the metadata (name, file path, size, created, modified, accessed) for the images were still viewable in the Physical Analyzer.

Audio data was not removed from any of the Android set, including .wav audio files from applications and user-downloaded files (.mp3). The iPhone set deleted most of

the audio files, but some .wav files were still recoverable. The files recovered from the iPhones included system audio files (e.g. ring tones) and notification sound clips that had been installed by third-party software. All recovered audio files could be played back on a media player.

Text data were not removed from any of the Android set. The file types that were recognized as data were files with .txt and .xml extensions. The iPhones did delete some text files, but the same types of files were recovered. Recovered .xml files contained readable string data such as domain names and IP addresses associated with user activities. Text files contained various notes or memos created by the user.

Database data (.db, sqlite, .sql) recovered from both sets contained no data. The results were similar to the user accounts data and wireless network data. The metadata (name, file path, size, creation time, modification time, and access time) was viewable after the factory reset but no data was stored in the files.

Configuration data recovered from the iPhones only contained system-file access data. The access information appears to be the same data as the Applications files. Data was not recoverable from any of the Android set, but this could be due to the fact that the same information is already in the Applications files. The recovered data did not contain any user information.

Applications data only contained information from first-party software installed on the phone. The data contained various framework, library, and plug-in information for system software. No user data was stored in the applications files. The application data on the A16 Android phone contained user account information before the wipe. The Physical Analyzer labeled it as installed applications. This was the only data that was mislabeled. The data was cleared after a reset and did not contain any user account information. It is unclear why the Physical Analyzer mislabeled this information.

Each file that contained user-generated data was counted and summarized in Table 10 and Table 11. The numbers indicate the total number of files found with user data.

	I1	I2	I3	I4	I5	I6	I7	I8
Data Files:								
Images	0	0	0	0	0	0	0	0
Audio	0	0	1	0	0	0	0	0
Text	1	2	5	7	1	1	1	1
Databases	0	0	0	0	0	0	0	0
Configurations	0	0	0	0	0	0	0	0
Applications	0	0	0	0	0	0	0	0

Table 10. User data files found in the smartphones part 1

	A9	A10	A11	A12	A13	A14	A15	A16	I18	A20	B21	A25
Data Files:												
Images	5	61	10	1698	42	15	5	616	0	0	0	6
Audio	0	0	0	0	0	2	0	15	0	0	0	0
Text	1	4	1	7	0	0	1	0	1	0	0	4
Databases	0	0	0	0	0	0	0	0	0	0	0	0
Configurations	0	0	0	0	0	0	0	0	0	0	0	0
Applications	0	0	0	0	0	0	0	0	0	0	0	0

Table 11. User data files found in the smartphones part 2

E. STRING SEARCHING WITH LINUX GREP COMMAND

- String searching was used for additional analysis of recovered files. During the analysis process with the Physical Analyzer, we searched for some keywords of interest in data files:
- password
- root certificate
- hash
- cert
- SHA1
- MD5
- SSL

The standard Linux grep [45] command was used to search for the keywords.

The A10 Android phone was the only one that returned a value with the "password" keyword, and this should have been deleted by the factory reset. This is one of the phones with a custom CyanogenMod 10.1 installed. An .xml file under the Cyanogen system directory contained several entries with website URLs and user names with passwords stored in clear text that should have been deleted. The other phones did not contain any password information. All phones returned at least one file that contained the "root certificate" phrase. The files contained characters varying in length between 115-144. It is unclear if this is the default trusted certificate installed with the operating system or if it is part of third-party software that used certificates. In the latter case the data should have been deleted. The information included in the files could not be identified as user data. Searches for the strings "hash", "cert", "SHA1", "MD5", and "SSL" did not return any significant results. These keywords only occurred in configuration files, which did not contain any user data.

Searching for the "hash" keyword did not return anything significant, but searching for "HASH" returned some interesting results. The "HASH" keyword still occurred in configuration files for iPhones but the files were always associated with an application called Rocky Racoon on the iPhones I3, I4, I5, I6, I7, and I8. This application is used exclusively with jailbroken iPhones [46]. Jailbreaking is the process of using a hardware or software exploit to break the restrictions on the iPhones file system [47]. A jailbroken iPhone grants the user root access to the iOS operating system. Once the iPhone is jailbroken it can be freely modified. The user can install unauthorized third-party applications, plugins and themes on the iPhone. It also allows the user to switch mobile carriers without any restrictions. Jailbreaking a phone also exposes the user to various security risks. Unauthorized software runs the risk of damaging or disabling the iPhone. This may have affected the data on the iPhones. It is not clear if these iPhones have been jailbroken. However, there is a high chance they were since the Rocky Racoon software is only used with jailbroken iPhones.

F. DATA ANALYSIS WITH BULK EXTRACTOR

The Bulk Extractor tool (Ver. 1.4.1: Windows installer with GUI) was used to verify some of the user data generated from the experiment procedures. The smartphone images created from the physical extraction process (.ufd) were not compatible with Bulk Extractor and needed to be converted. A full dump of the file system was created from the .ufd images using the Physical Analyzer. Each .ufd image generated a directory of files, which was run on the Bulk Extractor.

The 'url_histogram.txt' generated by the extractor showed that all website (youtube.com, facebook.com, reddit.com, faculty.nps.edu) links were deleted in the reset. Duplicate links for the four visited websites (nps.edu, fark.com, yahoo.com, npr.org) were found in various files on pre-wipe iPhones. It is unclear why there were duplicate links saved on iPhones. None of the other phones contained multiple copies of the same links.

Preference and configuration files (.plist) were recovered from most of the phones except for the BlackBerry phones (B20, B21) after the reset. None of the files contained user information. Setting information was checked in the 'json.txt' file generated by the extractor.

The zip file uploaded to the root directory 'testschwamm_userdata.zip' was not deleted from any of the Android phones and the text file 'testschwamm_password.txt' can be viewed in the 'zip.txt' generated by the extractor.

During the keyword search several files containing the word 'DELETED' appeared in the 'Feature File' results window. The Bulk Extractor displayed some text files (.txt) that included the word 'DELETED' as part of the file name. None of these files contained any readable data and were all located at the top-level directory. The Physical Analyzer could not find any of these tagged files. It became clear that further investigation was needed to determine if any more user-generated data were not properly identified by the Physical Analyzer. The following common file extensions [48] were

used for a string search against the full file system dump. The same grep command was used to search for these common file extensions.

- Text files (doc, docx, log, msg, odt, pages, rtf, tex, txt, wpd, wps)
- Data files (csv, dat, gbr, ged, ibooks, key, keychain, pps, ppt, pptx, sdf, tar,
- tax2012, vcf, xml)
- Audio files (aif, iff, m3u, m4a, mid, mp3, mpa, ra, wav, wma)
- Video files (3g2, 3gp, asf, asx, avi, flv, m4v, mov, mp4, mpg, rm, srt, swf, vob
- , wmv)
- 3D image files (3dm, 3ds, max, obj)
- Raster image files (bmp, dds, gif, jpg, png, psd, pspimage, tga, thm, tif, tiff, yuv)
- Vector image files (ai, eps, ps, svg)
- Page layout files (indd, pct, pdf)
- Spreadsheet files (xlr, xls, xlsx)
- Database files (accdb, db, dbf, mdb, pdb, sql)
- Executable files (apk, app, bat, cgi, com, exe, gadget, jar, pif, vb, wsf)
- Game files (dem, gam, nes, rom, sav)
- CAD files (dwg, dxf)
- GIS files (gpx, kml, kmz)
- Web files (asp, aspx, cer, cfm, csr, css, htm, html, js, jsp, php, rss, xhtml)
- Plugin files (crx, plugin)
- Font files (fnt, fon, otf, ttf)
- System files (cab, cpl, cur, deskthemepack, dll, dmp, drv, icns, ico, lnk, sys)
- Settings files (cfg, ini, prf)
- Encoded files (hqx, mim, uue)
- Compressed files (7z, cbr, deb, gz, pkg, rar, rpm, sitx, tar.gz, zip, zipx)
- Disk image files (bin, cue, dmg, iso, mdf, toast, vcd)
- Developer files (c, class, cpp, cs, dtd, fla, h, java, lua, m, pl, py, sh, sln
- , vcxproj, xcodeproj)

- Backup files (bak, tmp)
- Miscellaneous files (crdownload, ics, msi, part, torrent)

Each extension was used as a search term against both sets of smartphones. All files that matched the keywords were checked for user data. The numbers include both user data and system data (Table 12 & 13).

	I1	**I2**	**I3**	**I4**	**I5**	**I6**	**I7**	**I8**
Text Files	54/55	54/55	8/252	20/53	12/148	8/40	8/11	15/50
Data Files	406/406	403/406	73/355	115/91	73/1501	73/107	73/73	73/147
Audio Files	2007/2007	2007/2007	20/2673	20/63	20/1298	20/1162	20/20	20/1190
Video Files	0/0	0/0	0/9	0/0	0/9	0/95	0/0	0/9
3D Image Files	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
Raster Image Files	71/71	71/71	3/54	2/4	2/2	2/2	2/2	2/4
Vector Image Files	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
Page Layout Files	18/18	18/18	7/28	14/14	7/7	7/26	7/7	7/13
Spreadsheet Files	0/0	0/0	0/0	0/0	0/1	0/1	0/0	0/0
Database Files	79/80	80/87	15/52	60/60	15/47	14/51	15/16	15/58
Executable Files	3/3	3/3	2/10	2/6	2/5	2/4	2/2	2/6
Game Files	2/2	2/2	2/5	2/2	2/4	2/2	2/2	2/2
CAD Files	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
GIS Files	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
Web Files	211/211	212/212	13/13	14/14	12/13	12/12	12/12	12/12
Plugin Files	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
Font Files	66/66	66/66	56/56	47/47	56/56	56/56	56/56	56/56
System Files	5/5	6/6	2/2	2/2	2/2	2/2	2/2	2/2
Settings Files	0/0	0/0	0/2	0/0	0/4	0/38	0/0	0/1
Encoded Files	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
Compressed Files	2/2	2/2	7/7	0/1	0/5	0/1	0/1	0/1
Disk Image Files	87/87	87/87	8/339	14/14	8/119	8/35	8/8	8/59
Developer Files	18/18	19/19	1/10	1/9	1/17	1/1	1/7	1/11
Backup Files	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
Misc Files	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0

Table 12. Search result (post-wipe/pre-wipe) part 1

	A9	A10	A11	A12	A13	A14	A15	A16	I18	A20	A21	A25
Text Files	1/1	14/14	1/1	141/142	0/0	0/0	1/1	0/0	54/55	0/0	0/0	66/552
Data Files	0	50/50	0/0	66/66	1/1	0/0	0/0	0/0	406/406	0/0	0/0	374/2479
Audio Files	0/0	1/1	1/1	68/68	0/0	2/2	0/0	0/0	2007/2007	0/0	0/0	1/1
Video Files	0/0	5/5	0/0	6/6	10/10	5/5	0/0	0/0	0/0	0/0	0/0	0/0
3D Image Files	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
Raster Image Files	5/5	716/716	11/11	1938/1938	42/42	15/15	5/5	616/616	71/71	0/7	0/3	70/88
Vector Image Files	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
Page Layout Files	0/0	0/0	0/0	39/39	0/0	0/0	0/0	0/0	18/18	0/0	0/0	0/0
Spreadsheet Files	0/0	0/0	0/0	0/1	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
Database Files	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	80/87	0/0	0/0	0/0
Executable Files	0/0	95/95	0/0	7/7	3/3	1/1	0/0	0/0	3/3	0/0	0/0	75/77
Game Files	0/0	1/1	0/0	0/0	0/0	0/0	0/0	0/0	2/2	0/0	0/0	0/0
CAD Files	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
GIS Files	0/0	0/0	0/0	69/69	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
Web Files	0/0	4/4	0/0	0/0	0/0	0/0	0/0	0/0	212/212	0/0	0/0	0/0
Plugin Files	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
Font Files	0/0	39/39	0/0	1/1	0/0	0/0	0/0	0/0	66/66	0/0	0/0	0/0
System Files	0/0	3/3	0/0	0/0	0/0	0/0	0/0	0/0	6/6	0/0	0/0	0/0
Settings Files	0/0	1/1	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
Encoded Files	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
Compressed Files	0/0	22/22	0/0	20/20	6/6	0/0	0/0	0/0	2/2	0/0	0/0	3/3
Disk Image Files	0/0	15/15	0/0	0/0	0/0	0/0	0/0	0/0	87/87	0/0	0/0	0/0
Developer Files	0/0	10/15	0/0	22/22	0/0	0/0	0/0	0/0	19/19	0/0	0/0	12/12
Backup Files	0/0	13/13	0/0	24/25	0/0	0/0	0/0	0/0	0/0	0/0	0/0	177/1018
Misc Files	0/0	0/0	0/0	0/1	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0

Table 13. Search result (post-wipe/pre-wipe) part 2

No files with the keyword “DELETED” were found in any of the iPhones, only on the Android smartphones. Most of the tagged files were text files, but some were zip archives, Adobe PDF, MP4 video, and Microsoft Office files. All files containing the keyword “DELETED” were unreadable and did not include any user data.

User-generated Word and Excel files were found as email attachments on the pre-wipe iPhones (I4, I5, I8) but these files were properly deleted post-wipe. A significant amount of user-generated files were recovered from two of the post-wipe Android smartphones (A10, A12). Both included Adobe PDF files, Microsoft Word files, Microsoft Excel files, MP4 Video files and zip archives. All of these files were user-generated and contained sensitive information (user name, phone number, email address, and personal-video footage). Some of these personal files were located at the top-level directory just like the tagged files. However, most of them were found in the directory ‘\data\com.dropbox.android\file\scratch’. The A10 Android phone contained several documents under this directory. Dropbox is third-party software that is installed by the user and is used as a file hosting service for various platforms. The software client creates a local folder that can be synchronized across multiple platforms. Files that are placed in the folder are synced over the network through Dropbox servers [49]. None of the user data appears to have been deleted from the Dropbox folder. The same number of files was found in this directory pre-wipe.

G. DISCUSSION

The reset did a good job of removing user-account and Wi-Fi information associated with the phones. However, it did not fully remove photo images, audio files, text files, website login information, and geolocation data.

The UME-36 Pro and Physical Analyzer was able to collect a large variety of data after the factory reset. The tool was able to recover several files containing user data or user generated text files. There were 20 files recovered from the iPhones and 2483 files recovered from the Android phones. These are the total number of files that Cellebrite was able to identify. Text and audio files were recovered from several iPhones. Other

kinds of user data were left behind on some of the Android phones, including audio, text, and picture files. Many remaining pictures were still viewable, and some remaining audio files could still be played back.

The string search using the grep command found one xml file on an Android phone. The xml file contained user login and password information. The Cellebrite tools did not identify this xml file. No additional files were found from the iPhone set using this method.

The Bulk Extractor helped uncover several text files that were not identified by Cellebrite or the string search. An additional 157 user files were recovered from the Android phones. Some files were left behind by third-party applications such as Dropbox. The reset removed the applications but some user data was left behind in the installed directory. These files were Microsoft Office files (Word, Excel), Adobe PDF's and MP4 video files. Bulk Extractor did a better job of finding email addresses, fax numbers and phone numbers within files. However, the additional information was almost always found in manuals, acknowledgements, service agreements, and support information for system software. It was not personal user information but developer contacts (@tech, @helpdesk) and tech support (1-800 numbers). Several text files could be viewed with a standard text viewer. Some files contained IP addresses and domain names. Geolocation data was found along with timestamps, enabling a view of the locations the phone has been used. No additional files were discovered on the iPhones.

Cellebrite identified that 59% of the files were removed from iPhones and 47% of the files were removed from Android phones after a reset. The percentage is calculated from the total number of files pre-wipe and post-wipe. It is based off of the total number of files identified and listed by the forensics tools. All files identified by both tools were manually analyzed and counted.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND FUTURE WORK

A. CONCLUSION

The main goal of this thesis was to analyze residual user data on smartphones after a factory reset. A total of 21 smartphones were used to test the effectiveness of the reset. The experiment was successful in extracting residual user data from the smartphones. The data showed that factory resets do not remove all user information. A factory reset is not a complete wipe of the device. It appears to only remove files that the operating system deems as user generated. If this is the case the reset feature does not properly categorize user information. Anybody who has access to commercial forensics tools could collect user data from smartphones. This can be a major problem for some organizations. The military and the active duty members use smartphones on a daily basis and deal with sensitive information. This can become a serious security issue and needs to be addressed. There are also many challenges for digital forensics investigations. There is a large variability in the number and types of files that are recoverable from smartphones. An investigator may not be able to find the specific file or evidence needed for the case even when much personal information remains. A large data set can be recovered from a phone, but these data files might be files that already existed on the device. At the same time, not finding files does not mean evidence is not present on the device. The files could be unrecoverable by a single forensic tool and a single experiment may not be enough to recover all the evidence. Multiple experiments and forensics tools should be used to distinguish a wide range of files and evidence.

B. RECOMMENDED PROCEDURES

We conclude that a "factory reset" as currently implemented is insufficient for removing personal data on today's smartphones. The user wanting to remove all such data should take the following steps.

Delete cache files, browser history files, and browser cookies. Usually this can be done through the smartphone settings menu.

Manually uninstall all third-party software and review its directories for residual user data since a "factory reset" does not generally affect it. Be especially careful with off-site backup software such as Dropbox which often store a considerable amount of personal data of a user.

Perform a "factory reset" for the smartphone.

Check possible locations of remaining copies of personal files, and delete any such files that are found, since generally a user file that has been manually copied or moved to a top-level or user-created directory will not be erased during a reset.

Search for remaining personal user files by their common extensions (such as "doc", "txt", and "mp3") and delete them. A file explorer application can be used to find these files.

Overwrite deleted data and possibly unused drive storage with specialized software. Zeroing out will overwrite free space where deleted files are stored. This will prevent deleted files from being recovered.

In addition, the criticality of these steps can be reduced if the smartphone is password-protected and uses OS-level encryption on files. Encryption will eliminate the sensitivity of the data to which it is applied, and passwords will make it harder to access data of other users. The Apple iPhone and Google Android phone provide both of these with their smartphones.

C. FUTURE WORK

Possible additional work can be done:

- A larger and more diverse set of smartphones (including Blackberry, Windows Phone, Firefox OS, and Ubuntu Edge) could help provide a better overview of the strength and weaknesses of a factory reset. The new Cellebrite UFED Touch hardware supports a larger range of smartphones and is compatible with MTP.
- Several forensics tools were tested but not used for this project. Testing other tools against Cellebrite and creating a cross reference between different tools may produce more reliable data.

- This thesis did not explore password protection or encrypted data types. Additional research can be conducted on the effectiveness of various encryption types. These data types may require additional tools or special techniques to decipher. It can create a unique challenge for forensics research.
- Other security techniques can be tested for user-data protections. Several software programs (iErase [50], SHREDroid [51]) claim to completely erase the internal flash memory of a smartphone. The effectiveness of these can be tested and compared against the finding from this paper.
- A targeted analysis can be done on third-party software solutions. Backup software solutions can be further investigated. The research should focus on residual data left by third-party software after a factory reset.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] comScore. (2014, Feb. 3). "Reports December 2013 U.S. smartphone subscriber market share." [Online]. Available: http://www.comscore.com/Insights/Press_Releases/2014/2/comScore_Reports_December_2013_US_Smartphone_Subscriber_Market_Share

[2] Nokia Corporation. (2013, Jan. 24). "Q4 and full year 2012 interim report" [Online]. Available: http://www.results.nokia.com/results/Nokia_results2012Q4e.pdf

[3] Micron Technology, Inc. (2013, Apr.). "Micron technical note, NAND Flash 101; an introduction to NAND Flash and how to design it in to your next product," TN-29-19: NAND Flash 101 pp.1-2 [Online]. Available: https://www.micron.com/~/media/Documents/Products/Technical%20Note/NAND%20Flash/tn2919_nand_101.pdf

[4] Google Inc. (2013, Jan.) "Mobile internet & smartphone adoption, Google, January 2011" [Online]. Available: http://services.google.com/fh/files/blogs/Google_Ipsos_Mobile_Internet_Smartphone_Adoption_Insights_2011.pdf

[5] TechMedia Network. (2013). "TopTenReviews: 2013 Best Mobile Encryption Software Reviews and Comparisons" [Online]. Available: http://mobile-encryption-software-review.toptenreviews.com/

[6] Apple. (2013, July. 8). "iOS: Understanding 'Erase all content and settings" [Online]. Available: http://support.apple.com/kb/ht2110s

[7] Google. (2013). "Manage my devices"[Online]. Available: https://support.google.com/a/users/answer/1235372?hl=en

[8] M. Honan. (2013, Apr. 1). Break out a hammer: You'll never believe the data 'wiped' smartphones store. *Wired* [Online]. Available: http://www.wired.com/gadgetlab/2013/04/smartphone-data-trail/all/

[9] J. Smith. (2012, Sept. 13). "Security guru: don't sell your Android phone until turning it into Swiss cheese." *GottaBeMOBILE: Mobile News & Reviews* [Online]. Available: http://www.gottabemobile.com/2012/02/27/security-guru-dont-sell-your-android-phone-until-turning-it-into-swiss-cheese/

[10] *The Guardian*. (2013). "Recycled mobile phones retain previous owner data," [Online]. Available: http://www.theguardian.com/media-network/partner-zone-infosecurity/mobile-phones-previous-owner-data

[11] G. S. Cardwell. "Residual network data structures in Android devices", M.S. thesis, Comp. Science Dept., Naval Postgraduate School, California, 2011. [Online]. Available: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA552175

[12] J. Lyle. (2010, Feb. 25). "Computer Forensics Tool Testing (CFTT)," The National Institute of Standard and Technology, Gaithersburg, MD. [Online]. Available: http://www.nist.gov/itl/ssd/cs/forensics-tool-testing.cfm

[13] *Computer Forensics Tool Testing Handbook*, Computer Forensics Tool Testing Program, Office of Law Enforcement Standard, National Institute of Standard and Technology. Gaithersburg, MD. Feb. 1, 2012. [Online]. Available: http://www.cftt.nist.gov/CFTT-Booklet-Revised-02012012.pdf

[14] M. M. Saudi. "An Overview of Disk Imaging Tool in Computer Forensics," SANS Institute, Bethesda, MD, 2001. [Online]. Available: http://www.sans.org/reading-room/whitepapers/incident/overview-disk-imaging-tool-computer-forensics-643

[15] *GNU Operating System, Coreutils - GNU core utilities.* Free Software Foundation. Feb. 14, 2013. [Online]. Available: http://www.gnu.org/software/coreutils/manual/html_node/dd-invocation.html

[16] B. Carrier. "Hard disk data acquisition" in *File System Forensic Analysis*. Pearson Education, Upper Saddle River, NJ, pp. 53–55. 2005.

[17] S. Garfinkel. "Forensic feature extraction and cross-drive analysis" in Proc. the Sixth Annual DFRWS Conference, 2006, pp. 71-81 [Online]. Available: http://www.dfrws.org/2006/proceedings/10-Garfinkel.pdf

[18] N. L. Beebe, and J. G. Clark. "Digital forensic text string searching: Improving information retrieval effectiveness by thematically clustering search results*" in Proc. of the Seventh Annual DFRWS Conference*, 2007, pp 49–54. [Online]. Available: http://www.dfrws.org/2007/proceedings/p49-beebe.pdf

[19] K. Amari. (2009, Mar. 26). *Techniques and tools for recovering and analyzing data from volatile memory*, SANS Institute, Bethesda, MD. [Online]. Available: http://computer-forensics.sans.org/community/papers/gcfa/techniques-tools-recovering-analyzing-data-volatile-memory_3609

[20] A. Pal, and N. Memon. (2009, Mar.). The evolution of file carving: The benefits and problems of forensics recovery. *IEEE Signal Processing Magazine* [Online]. Available: http://digital-assembly.com/technology/research/pubs/ieee-spm-2009.pdf

[21] T. Vidas, C. Zhang and N. Christin. "Toward a general collection methodology for Android devices" in Proc. of the Eleventh Annual DFRWS Conference, Aug. 2011 [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1742287611000272

[22] P. Owen, P. Thomas, and D. McPhee. "An analysis of digital forensic examination of mobile phones" in Proc. 4th Intl. Conf. on Next Generation Mobile Applications Services and Technologies, July 2010. [Online]. Available: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5558244&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5558244

[23] F. Marturana, G. Me, R. Berte, and S. Tacconi. "A quantitative approach to triaging in mobile forensics" in Proc. 2011 International Joint Conference of IEEE TrustCom- in Changsha, China, 2011. [Online]. Available: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6120868&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6120868

[24] S. Omeleze, and H. Venter. "Testing the harmonized digital forensic investigation process mode using an Android mobile phone" in Proc. on Information Security for South Africa. 2013, Aug. [Online]. Available: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6641063&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel7%2F6621627%2F6641027%2F06641063.pdf%3Farnumber%3D6641063

[25] O. Afonin, and Y. Gubanov. (2013, May). Catching the ghost: how to discover ephemeral evidence with Live RAM analysis, *DFI Magazine* [Online]. Available: http://forensic.belkasoft.com/en/live-ram-forensics

[26] *UME-36Pro User Manual - Universal Memory Exchanger for Mobile Phones*. Cellebrite Mobile Synchronization Ltd, Parsippany, NJ, 2007. [Online]. Available: http://www.cellebrite.com/images/stories/support%20files/UME36_Manual.pdf

[27] *UFED User Manual Version 1.1.9.7*. Cellebrite Mobile Synchronization Ltd. , Parsippany, NJ, Mar. 2012 [Online]. Available: http://www.ume-update.com/UFED/UFED%20User%20Guide_June.pdf

[28] *UFED Physical Analyzer Manual*. Cellebrite Mobile Synchronization Ltd., Parsippany, NJ, Nov. 2012 [Online]. Available: https://www.cellebrite.com/images/stories/support%20files/UFED_PA_Manual.pdf

[29] Cellebrite Mobile Synchronization Ltd. (2013). UFED Phone Detective [Online]. Available: http://www.cellebrite.com/mobile-forensic-products/ufed-applications/ufed-phone-detective.html

[30] Digital Corpora. (2013). Bulk Extractor [Online]. Available: http://digitalcorpora.org/downloads/bulk_extractor/

[31] S. Garfinkel. (2013, Feb.) "Digital media triage with bulk data analysis and bulk_extractor" in *Computer & Security* 32. [Online]. Available: http://simson.net/clips/academic/2013.COSE.bulk_extractor.pdf

[32] ViaForensics. (2013). ViaExtract [Online]. Available: https://viaforensics.com/products/viaextract/

[33] Oxygen Forensics, Inc. (2013). Oxygen Forensic Suite 2013 [Online]. Available: http://www.oxygen-forensic.com/en/

[34] Piriform. (2013). Recuva [Online]. Available: http://www.piriform.com/recuva

[35] H. Zhu, E. Chen, H. Xiong, K. Yu, H. Cao, and J. Tian. "Mining mobile user preferences for personalized content recommendation," *ACM Transactions on Intelligent Systems and Technology*, 2014.

[36] S. Garfinkel. P. Farrell. V. Roussev, and G. Dinolt. "Bringing science to digital forensics with standardized forensic corpora" in Proc. of the Ninth Annual DFRWS Conference. 2009. [Online]. Available: http://www.dfrws.org/2009/proceedings/p2-farfinkel.pdf

[37] CyanogenMod, LLC. (2013). CyanogenMod 10.1 [Online]. Available: http://www.cyanogenmod.org/

[38] Google Inc. (2013). Android open source project [Online]. Available: http://source.android.com/

[39] S. Garfinkel. (2011, Sept. 3). Digital Forensics XML and the DFXML Toolset [Online]. Available: http://simson.net/ref/2011/dfxml.pdf

[40] N. Rowe. (2012, Aug.). "Testing the National Software Reference Library" in *Digital Investigation*, 9, pp. S131–S138. [Online]. Available: http://www.dfrws.org/2012/proceedings/DFRWS2012-14.pdf

[41] Everyi.iPhone Specs. (2013, Sep. 16). Every iPhone: iPhone specs, answers, comparison & more [Online]. Available: http://www.everymac.com/systems/apple/iphone/index-iphone-specs.html

[42] Arena Com Ltd. (2013). GSM arena [Online]. Available: http://www.gsmarena.com/

[43] B. Manders, and D. Mathieu. (2005). Media transfer protocol implementation details [Online]. Available: http://download.microsoft.com/download/9/8/f/98f3fe47-dfc3-4e74-92a3-088782200fe7/TWMD05003_WinHEC05.ppt

[44] Cellebrite Mobile Synchronization Ltd. (2013). UFED touch ultimate: All-inclusive mobile forensics solution [Online]. Available: http://www.cellebrite.com/mobile-forensics/products/standalone/ufed-touch-ultimate

[45] *The Open Group Base Specifications Issue 7* in IEEE Standard 1003.1, 2013 Edition. 2013. [Online]. Available: http://pubs.opengroup.org/onlinepubs/9699919799/utilities/grep.html

[46] F. Truta. (2012, May. 29). "Revised iOS 5.1.1 Jailbroken with Rocky Racoon 1.0-2." Softpedia [Online]. Available: http://news.softpedia.com/news/Revised-iOS-5-1-1-Jailbroken-with-Rocky-Racoon-1-0-2-272368.shtml

[47] C. Miller, D. Blazakis, D. D. Zovi, S. Esser, V. Iozzo R. P Weinmann. "Jailbreaking" in *iOS Hacker's Handbook*. John Wiley & Sons, Inc. pp.297-325. 2012, May. 8.

[48] Common File Types. (2013). The Central File Extensions Registry. FileInfo.com [Online]. Available: http://www.fileinfo.com/filetypes/common

[49] Dropbox, Inc. (2013). "How does the Dropbox service work?" [Online]. Available: https://www.dropbox.com/help/1968/en

[50] Jonathan Zdziarski's Domain. (2009). iErase [Online]. Available: http://www.zdziarski.com/blog/?page_id=407

[51] infsyssec. (2011). SHREDroid [Online]. Available: https://play.google.com/store/apps/details?id=ch.ethz.infsyssec.sddroid&hl=en

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California