

## **An Analysis of Smartphones Using Open Source Tools versus the Proprietary Tool Cellebrite UFED Touch®**

Marcie Bachler, B.S., Graduate Student, Marshall University Forensic Science Center, 1401 Forensic Science Drive, Huntington, WV 25701

Agency Supervisor: Detective Dave Lindman, Digital Forensic Investigator, Edina Police Department 4801 W 50th St, Edina, MN 55424

Agency Supervisor and Reviewer: Sergeant Kevin Rofidal, Investigations, Edina Police Department 4801 W 50th St, Edina, MN 55424

Technical Reviewer: Ian Levstein, M.S., Computer Operations Manager, Marshall University Forensic Science Center, 1401 Forensic Science Drive, Huntington, WV 25701

MU Faculty Advisor and Reviewer: Dr. Terry Fenger, Ph.D., Program & Center Director, Marshall University Forensic Science Center, 1401 Forensic Science Drive, Huntington, WV 25701

<i>Table of Contents</i>	<i>Page</i>
<b>Abstract</b> .....	4
<b>Section 1: Introduction</b> .....	5
<b>Section 2: Materials &amp; Methods</b> .....	9
2.1: Materials .....	9
2.2: Phone Obtainment .....	9
2.3: Cellebrite UFED Touch® .....	9
2.4: Initial Phone Extraction .....	10
2.5: Initial Factory Reset .....	11
2.6: Data Creation .....	11
2.7: Phone Extraction(s) with Data .....	14
2.7.1: Cellebrite UFED Touch® .....	14
2.7.2: Paladin® and Autopsy® .....	14
2.7.3: Andriller® .....	15
2.7.4: BitPim® and Other Programs .....	16
2.8: Final Factory Reset .....	16
2.9: Final Phone Extraction .....	16
<b>Section 3: Results</b> .....	17
3.1: Initial Phone Extraction .....	17
3.2: Initial Factory Reset .....	17
3.3: Phone Extraction(s) with Data .....	18
3.3.1: Cellebrite UFED Touch® .....	19
3.3.2: Paladin® and Autopsy® .....	19
3.3.3: Andriller® .....	23
3.4: Final Phone Extraction .....	24

---

3.5: Leftover Artifacts from a Factory Reset Comparisons .....	24
<b>Section 4: Discussion .....</b>	<b>28</b>
4.1: Initial Phone Extraction .....	28
4.2: Initial Factory Reset .....	29
4.3: Data Creation .....	29
4.4: Phone Extraction(s) with Data .....	30
4.4.1: Cellebrite UFED Touch® .....	30
4.4.2: Paladin® and Autopsy® .....	31
4.4.3: Andriller® .....	34
4.4.4: BitPim® and Other Programs .....	34
4.5: Final Phone Extraction .....	35
4.6: Leftover Artifacts from a Factory Reset .....	35
4.7: Future Studies .....	36
<b>Acknowledgements .....</b>	<b>38</b>
<b>References .....</b>	<b>38</b>
<b>Appendices .....</b>	<b>40</b>

## Abstract

Law enforcement agencies do not have a limitless budget, so they need to cut costs when it's doable. One way they could save money is by switching from highly expensive proprietary digital forensic tools, to low-cost or free open source tools. Proprietary tools have been the gold standard for digital forensics, however, that is changing with the increase use of open source tools. In the age of script kiddies, open source tools allow the code to be seen by all and changed publicly when it needs to be updated. This is unlike the proprietary tools that keep the inner workings of the tools secret, which can be a downfall when trying to explain the tool set used in the investigation in a court room. Open source tools have been gaining attractiveness as they compile themselves into huge forensic suites with all sort of tools in just one download. This is key since a digital examiner is always taught to use more than one tool to validate her/his findings.

This experiment deals with the amount of data open source tools can get from smartphones, and whether it is comparable to that of a proprietary tool like Cellebrite®. In short, Cellebrite® is more user friendly than the open source tools, and still extracts more data. Perhaps a different combination of open source tools could reach the same level of extraction as the Cellebrite®, but that was not the case here.

In addition, the experiment also looked at what user-generated artifacts could be recovered on a smartphone, using the Cellebrite®, after a factory reset. Three of the phones in particular left artifacts from two prior factory resets. The artifacts included mainly pictures and videos. This suggests that factory resets do not always delete personal user data like it states.

## Section 1: Introduction

With the digital age upon us, everyone has smartphones from 80 year old grandmas to 6 year old kids. Smartphones have infiltrated every part of our daily lives from getting directions, sending pictures, or emailing work. A majority of people use their smartphones for the former activities listed, but there is a population that use their smartphones for nefarious activities. Sadly, they aren't all hardened criminals, but they're the teenage drug dealers, stalkers, fraudsters, and those who like child pornography. With these types of people in the world, law enforcement agencies need ways to get access to not just their phones, but the data locked within them. The abundance of smartphones makes it challenging not only for forensic tool developers, but for law enforcement agencies as well.

“Digital forensic tools are used to fire employees, convict criminals, and demonstrate innocence.”<sup>1</sup> Keeping this statement in mind, an investigator must think about what tools she/he is using when analyzing digital evidence. There are a wide variety of tools ranging from closed source, proprietary tools that cost thousands of dollars to open source, freeware tools that cost little to nothing at all. The aspects of these tools should be weighed and measured when a police department, or any agency, decides what tools will be used to analyze forensic data. Open source tools allow their code to be seen online, viewed by anyone, and be fixed when a bug is found and noted. On the other hand, proprietary tools keep their code a secret and the bugs are handled behind closed doors. Yes, people can manipulate the open source tools and their codes, but those same people could also find holes in proprietary tools. The big difference between the readily available code and the secret code, is an average user will be notified about the gaps in open source tools with a new or updated release version.<sup>1</sup>

Another aspect that open source tools have over proprietary ones is they are more cost effective. Being free or less expensive than thousands of dollars for a yearly license fee, open source can help smaller agencies, like local police departments, analyze digital evidence instead of contracting it out. This way the evidence stays with the police investigating the case, instead of going to someone else who does not know the specifics of the case. Also, contracting out the evidence is another cost that can be avoided with free, open source tools. With a lower budget for digital forensic tools, a department can focus its money on other things like bulletproof vests, helmets, or body cameras.

Smartphone forensics is covered under the general term mobile forensics, which is defined as mining data from mobile digital devices using techniques closely related to those for digital forensic investigations.<sup>3</sup> This experiment deals with extracting data from smartphones using open source tools and the proprietary Cellebrite® tool. The Cellebrite® is able to perform three different types of extractions: physical, file system, and logical. The physical extraction mines all the data it can get, including data from the unallocated/deleted space. The file system extraction is like the physical extraction, but it does not probe unallocated/deleted space even though it extracts hidden files. The logical extraction is basically what the user sees when they use the phone, so no hidden or deleted files.<sup>2</sup> All open source tools used had to meet the requirements of the Open Source Initiative guidelines as follows:

1. **Free Redistribution:** There must be no restrictions by the license on use, distribution, or selling of a program that uses the code as a component.
2. **Source Code:** The source code must be made easily available to the user.
3. **Derived Works:** Any derived or modified works must be allowed distribution under the same licensing as the original software.

- 4. Integrity of The Author's Source Code:** If the license restricts modified versions of the source code from being distributed, it may only do so if and only if the license allows “patch files” to be distributed with the source code. Individuals must be allowed to use these “patch files” upon building their program and allow distribution of this built program. A requirement of a different name or version number can be established.
- 5. No Discrimination Against Persons or Groups:** No persons or groups can be discriminated against by the license.
- 6. No Discrimination Against Fields of Endeavor:** No fields can be restricted for use by the license.
- 7. Distribution of License:** Redistribution under the same rights must be possible without the need for an additional license
- 8. License Must Not Be Specific to a Product:** The license and rights of the program cannot be limited to a specific product.
- 9. License Must Not Restrict Other Software:** The license must not restrict other software being used with the original program in any way.
- 10. License Must Be Technology-Neutral:** No individual technology or style of interface can be specifically stated for use by the license<sup>4</sup>.

The open source tools also had to permit law enforcement agencies to use them, which can be found only in the fine print of license agreements.

The experiment will start with an initial physical extraction of data by the UFED Touch® on all the phones to see how much data the phone had on it prior to this research. The phone will then be reset to factory defaults. Some of the phones will be powered on, while the

remainder will be powered off. The phones will then have new identities created specifically for each phone. Artifacts from 13 different areas of phone use will be created in equal amounts on the phone when available. The phones will then have another physical extraction taken by the UFED Touch® as well as a logical extraction. Since not every open source tool is able to do a physical extraction, a logical one from the UFED Touch® will be used as a control.

Three open source tools will be used to analyze the created data: Paladin Forensic Suite®; Autopsy®; and Andriller®. It should be noted that Andriller® is not free. The version of Andriller® used was a trial, but overall Andriller® is less expensive than a proprietary tool. Once each of these tools has extracted and examined the data from each phone, the amount of data extracted will be noted and compared to each tool used. After that, the phones will once again be factory reset. A physical extraction of the phones will occur again.

The last two steps of factory resetting the phones and another physical extraction are to see if there are any personal artifacts that can be left on the phones and if so, what types of artifacts are left. There has been research done about the amount of “user-generated content” that can still be recovered after a factory reset. This research in particular found that some phones left user data like “photographs, audio files, text files, login information and geolocation data” on the phones proving the “unreliable nature of a factory reset.”<sup>5</sup> This is relevant because criminals who steal phones and re-sell them, or those who try to hide behind a reset can still leave potential evidence on their phone unknowingly.

There are two hypotheses: 1.) Can open source tools extract the same amount of evidence as the proprietary Cellebrite UFED Touch®; and 2.) What user-generated artifacts can be recovered after a factory reset. Both hypotheses are quintessential in helping law enforcement



agencies. With this experiment, digital forensic tools could be used more cost effectively, and the possibility of recovering lost data could catch a criminal.

## **Section 2: Materials & Methods**

### **2.1: Materials**

A variety of tools were used. The Cellebrite UFED Touch® was for phone extractions and examined with the physical analyzer software it came with. There was a computer used to not only analyze data, but to download open source tools. The open source tools used were Paladin Forensic Suite® with Autopsy®, Andriller®, and BitPim®. An external hard drive was used to store extracted data and screenshot images. The phones used were: Kyocera C5170 Hydro, ZTE GSM Z830, Nokia GSM Lumia 635, LG CDMA LS-720, and a HTC Vivid.

### **2.2: Phone Obtainment**

The phones that were used were given to the researcher from a Lost & Found at a local mall. There were roughly 40 phones, but only 20 smartphones and iPods®. The non-smartphones were immediately excluded, as well as the iPods®. The remaining 17 phones were all turned on to check for phone locks/pins. All five of the iPhones were locked as well as three android phones. Since they were locked, these phones were excluded. That left nine android phones to be examined for the possibility of being included in the experiment. The phones were put into airplane mode, not connected to the Wi-Fi, the display was put onto the longest time possible, and developer options were made available (when applicable) and stay awake and USB debugging were turned on.

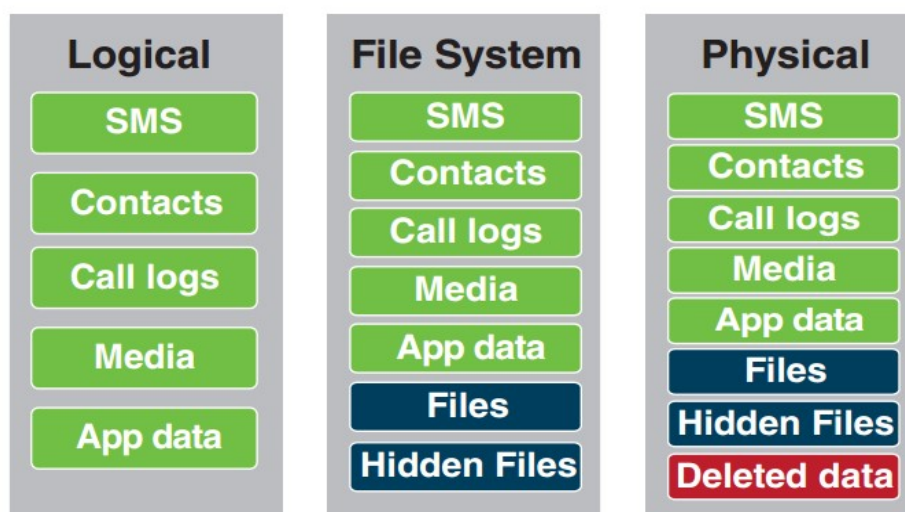
### **2.3: Cellebrite UFED Touch®**

A Cellebrite UFED Touch® was used in this experiment, because it is one of the top forensic mobile phone tools. The UFED Touch® is a portable version of Cellebrite® that can be

taken on any investigation. It has an easy to use Graphic User Interface (GUI) that tells a person how to specifically run it properly. It explains what write-blocking cord has to be used on a specific phone and where to put it, along with where to connect a receiving location device. There are three types of extractions that can be performed: physical, file system, and logical. The UFED Touch® can also capture images and screenshots of the phone. Each phone is different and therefore has different extractions and artifacts that can be imaged from it. Once the phone is recognized, or manually searched for on the UFED Touch®, a list of what actions can be performed is shown. From then on, directions are given to aid in the imaging process.

#### 2.4: Initial Phone Extraction

Putting the phone in airplane mode and stay awake with USB debugging were done in order for the UFED Touch® to make forensic images from the phones. The UFED Touch® was used to do a physical extraction of the data on each phone. If a physical extraction was unavailable for a phone, then a file system and/or logical extraction was performed. Physical extractions were preferred because they get the most data from a phone compared to a file system or logical extraction.



**Figure 1.** Cellebrite's® types of extractions and the artifacts each one supports.

The extractions were saved to an external hard drive, to be analyzed later. Two phones only had a logical extraction because the physical and file system ones were not available. These two phones were then excluded because they were unable to provide hidden or deleted files. That left a total of seven phones.

## 2.5: Initial Factory Reset

All seven phones had a factory reset performed on them. Three of them had the reset performed while the phone was turned on; the rest had the phones turned off (see Table 6 in Results).

## 2.6: Data Creation

After the phones were reset, data had to be created for the controlled experiment. Each phone was given an identity and a Google Mail© (Gmail) account to set up the rest of the phone and install applications (see Table 1).

**Table 1.** A list of each phone's identity and the data used to create it.

Phone Account Info						
Phone Type	Name	Birth day	Gmail© Accounts	Passw ords	Phone Number	Microsoft Outlook Account
Kyocera C5170 Hydro	Elizabeth Bennet	4-Mar-93	Lizzy.Bennet7	Pride*	612-474-2573	N/A
ZTE GSM Z830	Anne Elliot	4-Feb-94	Anne.Elliot83	Persua sion	612-474-7683	N/A
Nokia GSM Lumia 635	Marianne Dashwood	5-Jun-98	<a href="#">Marianne.Dashwood2468</a>	Sensib ility	612-474-2468	Same as Gmail©, just Outlook
LG CDMA LS-720	Emma Woodhouse	22-Nov-91	<a href="#">Emma.Woodhouse1316</a>	Knigh tley	612-474-1316	N/A
Samsung GSM SGH-T499 Dart	Fanny Price	11-Nov-92	Fanny.Price81	Mansf ield	612-474-5839	N/A
ZTE GSM V768 Concord	Jane Bennet	22-Jun-01	<a href="#">Jane.Bennet952</a>	Prejud ice	612-474-1952	N/A
HTC Vivid	Catherine Morland	25-Nov-95	<a href="#">Catherine.Morland406</a>	Abbey *	612-474-6406	N/A

\*The identities were changed for copyright reasons.

After the identities on each phone was created, artifacts were produced on each phone, when available.

**Table 2.** *A list of artifacts created on each phone.*

Artifacts Created for the Experiment	
Fake Text *	Taken Videos
Fake Call Log*	Deleted Videos
Emails	Contacts
Taken Pictures	Web History
Deleted Pictures	Web Favorites/Bookmarks
Downloaded Pictures	Favorite Locations
Calendar Events	

*\*Fake Text and Fake Call Log applications were not available for every phone.*

Each phone had roughly the same amount of artifacts created in each section; this was done to normalize the results as much as possible. Most of the time the number of artifacts per section was five total, though some had more due to accidental addition like fake calls, or deleted pictures. The contacts had all seven of the identities added to them. The calendar reminders also had the seven birthdays along with Halloween, Christmas, and New Year's. The fake call log and fake text messages were from downloaded applications from the Google Play Store®, specifically, Fake Call Logs from Mobitop® and Fake Text Messages from NeruoDigital®. The pictures and videos were of numbered sticky notes from 1-5. There was a total of ten pictures taken, so five of them could be deleted. This was the same process for the videos. The downloaded pictures came from Wikipedia®. The emails were sent through the Gmail® accounts of the five phones that were included in the experiment. Each phone had the same five favorite locations saved to them (see Table 3).

**Table 3.** *All the created artifacts in each section for each phone.*

Phone ID#	Fake Calls	Fake Text Threads	Text Message Total	Emails	Pictures	Deleted Pictures	Downloaded Pictures	Videos	Deleted Videos	Contacts*	Web History*	Web Favorites/Bookmarks	Favorite Locations	Calendar Reminders	Notes
1	6	5	12	6	5	6	5	5	5	11		20	5	10	
2	6	5	16	6	5	7	5	5	7	10		9	5	10	*Includes Email addresses from 4 contacts
3	-	-	-	7*	5	7	7*	5	6	14		11	5	10	Could not send emails, but could receive them. 7 downloaded pictures, but deleted 2. Out of the 14 contacts 6 of them were added.
4	6	5	12	6	5	5	5	5	5	11		14	5	10	*Includes Email addresses from 4 contacts, and a self-made contact
5															Could not take pictures because there was no SD card. Could use Internet and create contacts, decided against its use.
6															Had no SD card could not download applications or take pictures; decided not to use the phone.
7	-	-	-	7	5	5	5	5	5	7		11	5	10	Had no preformed contacts (emergencies/phone company)

Web History was grayed out, because although there was history made, the number of Web sites visited was not noted. The differences in the web favorites/bookmarks is detailed in Appendix A. Phones 5 and 6, were not only unable to install the fake text and fake call log applications, but could not take pictures because they had no SD cards in them. These two phones were excluded for lack of artifacts created. Phones 3 and 7, stayed in the experiment even though the fake text and fake call logs were not installed.

## 2.7: Phone Extraction(s) with Data

After the data was created, and each phone had not only an identity, but also artifacts from the 13 sections, they were imaged and analyzed by various tools.

### **2.7.1: Cellebrite UFED Touch®**

Like the previous extraction using the UFED Touch®, a physical extraction was taken when available. A logical extraction was also taken, when offered. As a fall back to either one of the other extractions not working, a file system extraction was taken. Some of the phones could not do just one extraction at a time, but instead became multi-step extraction. This meant a physical extraction and file system extraction, or a logical extraction and file system extraction occurred at the same time. These images were saved on an external hard drive for later analysis.

### **2.7.2: Paladin® and Autopsy®**

Paladin® is an open source forensic suite of tools and applications. For Paladin® to work there is no need for a write-blocker because it mounts devices only as “Read-Only” when initially plugged into the computer. After that, you can change a device to “Read/Write,” which was only done for the external hard drive in order to save screenshots of the activities being performed. Each phone was connected to the computer through a USB port and showed up on the Paladin® device list. However, only phones 1 and 7 were recognized as external drives to be imaged through Paladin®. The other three phones existed, but were never mounted as drives. However, all of the phones were able to list what percentage of them was being used and for what purpose. Since only phones 1 and 7 were imaged, they were the only ones examined using Paladin®. When they were being imaged, a box for verification of hash values was checked in order to make sure nothing was added or removed from the phone.

Autopsy® is another well know forensic open source tool. Though Autopsy® phones 1 and 7 were analyzed with their images taken from Paladin®. With this image, Autopsy® was able to create timelines for all the activities performed on each phone. The timelines could then be examined as a whole, separate events, or days, etc.

### 2.7.3: Andriller®

Andriller® is also an open source tool. It is specifically designed for android phones; phone 3 with the Windows© operating system, was not recognized, and could not be examined with this tool. The other four phones were plugged into the computer via a USB port, and had data extracted via Android Backup method.

# This report was generated using Andriller # (This field is editable in Preferences)

# This report was generated using Andriller version 2.6.0.1 on 2016-07-20 15:22:20 Central Daylight Time #

#### [Andriller Report] HTC HTC Holiday | IMEI:356298045216132

Type	Data
ADB serial:	FA27VVJ03551
Shell permissions:	shell
Manufacturer:	HTC
Model:	HTC Holiday
IMEI:	356298045216132
Android version:	4.0.3
Build name:	IML74K
Wifi MAC:	a0:f4:50:77:f0:3e
Local time:	2016-07-20 15:22:20 Central Daylight Time
Android time:	2016-07-20 15:22:07 CDT
Accounts:	com.htc.sync.provider.weather: Wea***r com.htc.newsreader: News com.htc.stock: Sto**s com.google: tia*****m
System:	<a href="#">Wi-Fi Passwords (2)</a>
Web browser:	<a href="#">Android Web Browser History (44)</a>
System:	<a href="#">Android Download History (5)</a>
Communications data:	<a href="#">Contacts (11)</a>

**Figure 2.** A screenshot of an Andriller® report and what can be extracted from a phone.

To examine the Andriller® report make sure to check the box that says “Open REPORT .html in browser.” Once the browser opens up with the report, like the one

shown above, the rest of the examination happens by clicking on the blue hyperlinks, to open a section and examine it further.

#### **2.7.4: BitPim® and Other Programs**

BitPim® can be considered one of the best open source forensic mobile phone tools.<sup>10</sup> However, when any of the phones were attached via a USB port, none of them were recognized by BitPim®. Even when the program was directed to a similar phone to the one plugged in, it would not recognize the actual phone. With the inability to recognize any phone, BitPim® was unable to examine the phones.

There were several open source tools looked at for this experiment, yet most of them had some defect, or inability to be used in this experiment. For a list of the tools and the reasons for their exclusion from this experiment, please refer to Appendix B.

#### **2.8: Final Factory Reset**

To finish the experiment, the phones were factory reset again, to delete any the data that was created. Once again, those phones that were left on for the first factory reset, were left powered on again. Those that were powered off for the first factory reset, were again powered off.

#### **2.9: Final Phone Extraction**

After the final factory reset, the phones had extractions taken from them with the UFED Touch®. The physical extractions were preferred, but again file system and logical extractions were taken when the physical extraction was not offered. Using all the existing extractions from the UFED Touch®, a comparison of the artifacts that were present (from the previous owner) and those that were created for this experiment will be analyzed to determine what can be left on a phone after a factory reset.



## Section 3: Results

### 3.1: Initial Phone Extraction

Table 4 shows the types of extractions that were taken using the UFED Touch®, for the first time. These nine phones were unlocked and able to be imaged.

**Table 4.** *All the phones that had the first UFED Touch® extractions taken.*

Phones from the Initial Dump	Extraction Performed	Notes
Kyocera C5170 Hydro	Physical	Logical and file system extraction also performed. Date and time were correct.
ZTE GSM Z830	Physical	Date and time not correct
Nokia GSM Lumia 635	File system and Logical	No physical extraction occurred. Very quick to extract. Not a lot on the phone.
LG CDMA LS-720	Physical	-
Samsung GSM SGH-T499 Dart	Physical	-
ZTE GSM V768 Concord	Physical	Date and time not correct
LG GSM P659 Optimus F3	Logical	No physical or file system extraction offered.
HTC-HD7	Logical	No physical or file system extraction offered. Date and time not correct.
HTC Vivid	Physical	-

Most of these phones were able to have a physical extraction performed. If the physical extraction was not performed a logical extraction was, and only one file system extraction was executed.

### 3.2: Initial Factory Reset

Phones that only had logical extractions done by the UFED Touch®, LG GSEM P659 Optimus F3, and HTC-HD7, were excluded from the experiment. The exclusion of those two phone, resulted in seven phones moving forward to factory reset. The reset was split into phones that were powered on or powered off when the factory reset was performed.

**Table 5.** *How the phone was factory reset.*

Phone ID #	Phone	Power On/Off	Factory Reset	Wipe Cache Partition	Notes
1	Kyocera C5170 Hydro	Off	Yes	Yes	Pictures and videos still on the phone.
2	ZTE GSM Z380	On	Yes	N/A	Could not do a hard rest without the phone being off, just got a FTM message.
3	Nokia GSM Lumia 635	Off	Yes		It auto resets itself, leaving no options to user
4	LG CDMA LS-720	Off	Yes		
5	Samsung GSM SGH-T499 Dart	Off	Yes	Yes	Says online to do the "wipe cache partition" for a hard reset.
6	ZTE GSM V768 Concord	On	Yes	N/A	Didn't work when powered off. No SD card so couldn't erase it.
7	HTC Vivid	On	Yes	N/A	Decided to do with the power on to do half and half.

Not every user data action or artifact was deleted from every phone. Most notably, phone 1 and its pictures and videos. For the total number of pictures and videos left over on phone 1 see Appendix C.

### 3.3: Phone Extraction(s) with Data

### 3.3.1: Cellebrite UFED Touch®

**Table 6.** *Types of extractions performed on the phones after the experiment artifacts were added.*

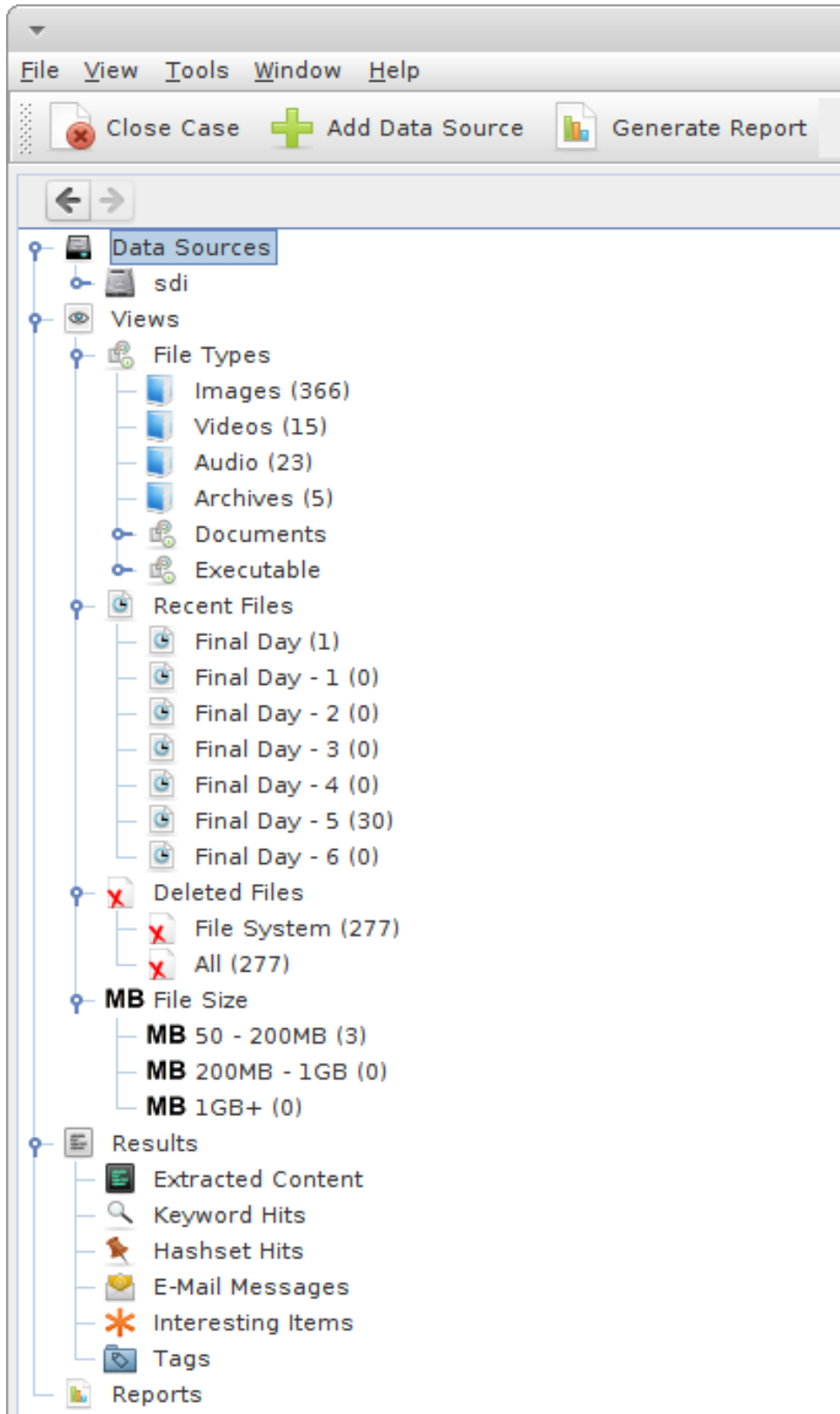
Phones from the Data Dump	Extractions Performed	Notes
Kyocera C5170 Hydro	Physical, Logical	N/A
ZTE GSM Z830	File System/Physical	Just a physical extraction was unable to occur since the phone wasn't rooted, so the extraction is considered a multi-step doing a physical and file system extraction at the same time.
Nokia GSM Lumia 635	File system/Logical	No physical extraction could be performed. A multi-step where a file system and logical extraction occurred at the same time.
LG CDMA LS-720	Physical, Logical	N/A
HTC Vivid	Physical, Logical	A physical extraction with "Bypassing Lock" was also performed, but there were fewer bytes than the original physical extraction.

### 3.3.2: Paladin® and Autopsy®

Paladin® was able to image only phones 1 and 7, therefore Figures 3, 4, and 5 are those of phone 1. The screenshots in Paladin® and Autopsy® of phone 7 can be found in Appendix D.

Folder	Usage	Size	Contents
9016-4EF8	100.0 %	871.5 MB	10686 items
DCIM	73.9 %	444.9 MB	179 items
Camera	73.9 %	329.3 MB	168 items
.thumbnails	25.7 %	113.5 MB	4 items
browser-photos	0.4 %	2.0 MB	5 items
100ANDRO	0.0 %	32.8 kB	1 item
Android	19.4 %	383.3 MB	10288 items
data	100.0 %	383.3 MB	10287 items
telenav	2.3 %	15.2 MB	106 items
.android_secure	2.1 %	12.8 MB	2 items
Pictures	0.8 %	5.5 MB	46 items
cache	87.6 %	4.3 MB	12 items
com.google.android.googlephotos	99.2 %	4.2 MB	11 items
download-cache	40.5 %	1.7 MB	4 items
picasa_covers	0.8 %	32.8 kB	1 item
Messenger	8.8 %	983.0 kB	29 items
NAVER_LINE	1.5 %	98.3 kB	2 items
Screenshots	1.4 %	98.3 kB	2 items
Music	0.6 %	3.3 MB	4 items
LINEcamera	0.5 %	3.0 MB	6 items
Download	0.2 %	1.0 MB	6 items
Ringtones	0.1 %	524.3 kB	4 items
Editadas	0.1 %	458.8 kB	5 items
Notifications	0.1 %	426.0 kB	3 items
Facebook Messenger	0.0 %	262.1 kB	8 items
postitital	0.0 %	294.9 kB	9 items
lwmedia	0.0 %	131.1 kB	6 items
LOST.DIR	0.0 %	65.5 kB	2 items
smvvm	0.0 %	65.5 kB	4 items
pers	0.0 %	65.5 kB	2 items
LINE_Backup	0.0 %	32.8 kB	1 item
Movies	0.0 %	32.8 kB	1 item
Alarms	0.0 %	32.8 kB	1 item
Podcasts	0.0 %	32.8 kB	1 item
.mmsyscache	0.0 %	32.8 kB	1 item

**Figure 3.** The Disk Usage Analyzer is featured above, showing how much space is being used and for what.



**Figure 4.** This shows what Autopsy® was able to extract from the Kyocera Hydro phone.



**Figure 5.** The Autopsy® tool was used to make a timeline of activities and artifacts on the Kyocera Hydro.

Databases were not installed on the program or computer which limited Autopsy® as an analyzer tool.

The Paladin® suite toolbox was unable to be used, so there was no further examination than what is shown.

### 3.3.3: Andriller®

The only type of extraction Andriller® used in this experiment was via the Android Backup method. No other information was pulled from the phones, besides that shown above in Figure 2.

**Table 7.** *The results of each phone's report for the four categories extracted.*

Andriller® Reports				
Phones	Wi-Fi Passwords	Android Web Browser History	Android Download History	Contacts
1	1	1	38	8
2	2	27	12	-
3				
4	1	30	13	-
7	2	44	5	11

Phone 3 was not recognized by Andriller®. The four other phones consistently got Wi-Fi passwords, web browser history, and download history. However, only phones 1 and 7 got any contacts, see table 7.

### 3.4: Final Phone Extraction

**Table 8.** A description of the extractions performed on the phones for the last time after the second factory reset.

Phones from the Final Reset Dump	Extractions Performed	Notes
Kyocera C5170 Hydro	Physical	N/A
ZTE GSM Z830	Physical	Had to become a developer again
Nokia GSM Lumia 635	Logical	A file system extraction could not be performed because there were no pictures on the phone
LG CDMA LS-720	Physical	N/A
HTC Vivid	Physical	A physical extraction with "Bypassing Lock" was also performed, but there was less bytes than the original physical extraction.

All of the phones, except for phone 3, had a physical extraction. Phone 3 was unable to have a file system extraction, leaving a logical extraction the only option.

### 3.5: Left Over Artifacts from a Factory Reset Comparisons

There were three different times the UFED Touch® was used for extractions. The three extractions happened before the phones were factory reset, after they were reset and the experimental data was created, and after another factory reset. The results are specified in the tables below.

**Table 9.** Number of calls extracted from each UFED Touch® extraction.

Call Log				
Phone ID#	Initial Dump	Data Dump	Final Dump	Notes
1	831	6, 12*	-	The data dump had conflicting numbers between the physical (6) and the logical (12) extractions.
2	1	0*	-	Fake calls from the application were not observed.
3	-	-	-	No phone calls were made, not even with a fake application.
4	231	7, 12*	-	The data dump had conflicting numbers between the physical (7) and the logical (12) extractions.
7	505	-	-	A fake call application was not used.



**Table 10.** Number of SMS/text messages extracted from each UFED Touch® extraction.

SMS (text messages)				
Phone ID#	Initial Dump	Data Dump	Final Dump	Notes
1	1950	6	0	
2	3	0*	0	Fake text application was installed and used on the phone.
3	*	N/A	N/A	Know there were text messages that came in when the phone was turned on. There was no fake text application installed on phone.
4	179	13, 24*	0	The data dump had conflicting numbers between the physical (13) and the logical (24) extractions.
7	2338	N/A	N/A	There was no fake text application installed on phone.

**Table 11.** Number of emails extracted from each UFED Touch® extraction.

Emails				
Phone ID#	Initial Dump	Data Dump	Final Dump	Notes
1	149	27, 26*	0	The data dump had conflicting numbers between the physical (27) and the logical (26) extractions.
2	2	0*	0	Emails were sent and received during the data creation stage.
3	0	0*	0	Only could receive emails, could not send them.
4	0	25	0	
7	321	26, 25*	0	The data dump had conflicting numbers between the physical (26) and the logical (25) extractions.

**Table 12.** Number of pictures extracted from each UFED Touch® extraction.

Pictures				
Phone ID#	Initial Dump	Data Dump	Final Dump	Notes
1	16494 (15388 non-system)	11695 (11347 non-system), 806 (647 non-system)*	11406 (11110 non-system)	The data dump had conflicting numbers between the physical (11695) and the logical (806) extractions.
2	759 (302 non-system)	168 (95 non-system)	582 (140 non-system)	
3	16 (8 non-system)	20 (10 non-system)	0	
4	1948 (1546 non-system)	1014 (669 non-system), 82 (64 non-system)*	702 (427 non-system)	The data dump had conflicting numbers between the physical (1014) and the logical (82) extractions.
7	4186 (3263 non-system)	578 (522 non-system), 47 (40 non-system)*	389 (346 non-system)	The data dump had conflicting numbers between the physical (578) and the logical (47) extractions.

**Table 13.** *Number of photos carved from each UFED Touch® extraction.*

Photo Carving				
Phone ID#	Initial Dump	Data Dump	Final Dump	Notes
1	322	493	463	
2	4		*	In the final dump, the program said it was carving photos but there appeared to be none
3				Because a physical extraction could not be performed, no carving could be done.
4	23*	26	2	There are two different screenshots and one says there are 23 photos while another says there are only 22.
7	467	114	81	

**Table 14.** *Number of videos extracted from each UFED Touch® extraction.*

Videos				
Phone ID#	Initial Dump	Data Dump	Final Dump	Notes
1	25	21, 15*	21	The data dump had conflicting numbers between the physical (21) and the logical (15) extractions.
2	0	5	0	
3	12	10	0	
4	15	20, 5 *	15	The data dump had conflicting numbers between the physical (20) and the logical (5) extractions.
7	24	23, 0*	18	The data dump had conflicting numbers between the physical (23) and the logical (0) extractions.

**Table 15.** *Number of contacts extracted from each UFED Touch® extraction.*

Contacts				
Phone ID#	Initial Dump	Data Dump	Final Dump	Notes
1	363	10, 20*	4	The data dump had conflicting numbers between the physical (10) and the logical (20) extractions.
2	14	12	12	
3	0	0*	0	Contacts were added.
4	1	21, 31*	0	The data dump had conflicting numbers between the physical (21) and the logical (31) extractions.
7	193	11, 22*	0	The data dump had conflicting numbers between the physical (11) and the logical (22) extractions.

**Table 16.** Number of web addresses extracted from each UFED Touch® extraction.

Web History				
Phone ID#	Initial Dump	Data Dump	Final Dump	Notes
1	256	44	0	
2	20	31	0	
3	0	0*	0	The web was search to make web favorites.
4	203	47	0	
7	261	45	0	

**Table 17.** Number of web favorites/bookmarks extracted from each UFED Touch® extraction.

Web Favorites/Bookmarks				
Phone ID#	Initial Dump	Data Dump	Final Dump	Notes
1	15	20	0	
2	4	9	4	
3	0	0*	0	Web favorites were saved, and there were ones preinstalled.
4	9	14	9	
7	7	12	6	

**Table 18.** Number of locations extracted from each UFED Touch® extraction.

Locations				
Phone ID#	Initial Dump	Data Dump	Final Dump	Notes
1	269	18, 22*	0	The data dump had conflicting numbers between the physical (18) and the logical (22) extractions.
2	3	0*	3	Phone locations from google maps were saved.
3	8	0*	0	Phone locations from google maps were saved.
4	0	7	0	
7	388	17	0	

**Table 19.** Number of calendar reminders extracted from each UFED Touch® extraction.

Calendar Reminders				
Phone ID#	Initial Dump	Data Dump	Final Dump	Notes
1	0	12, 25*	0	The data dump had conflicting numbers between the physical (12) and the logical (25) extractions.
2	0	10	0	
3	0	0*	0	Calendar reminders were made and saved.
4	1	10, 20*	0	The data dump had conflicting numbers between the physical (10) and the logical (20) extractions.
7	42	10, 20*	0	The data dump had conflicting numbers between the physical (10) and the logical (20) extractions.

The tables above show each created artifact section. A few phones had differing numbers when it came to physical extractions versus logical extractions. These occurrences happened in all but three of the data sections: photos carved, web history, and web favorites/bookmarks (see Tables 13, 16, and 17). The other eight sections had at least one conflicting incident noted (see Tables 9, 10, 11, 12, 14, 15, 18, and 19). Some phones did not extract data when they should have, namely phone 3 and sometimes phone 2 (see Tables 9, 10, 11, 15, 16, 17, 18, and 19).

## **Section 4: Discussion & Conclusions**

### **4.1: Initial Phone Extraction**

The initial phone extraction went smoothly, although some phones were locked. The locked phones were not able to have extraction done by the UFED Touch®. These phones were quickly rejected from the experiment, as there was no time to crack the codes, or potentially harm the data within them. The unlocked iPod Touch© did have a file system and a logical extraction took place. However, since there were no other Apple products being used, it was excluded in order to normalize the results. The LG GSM p659 Optimus F3 and the HTC-HD7, were the two phones that allowed only for a logical extraction. Since logical extractions are just showing what a person would see on a phone, instead of the hidden or deleted files that an investigation would want to look at, these phones were excluded from the rest of the experiment. The Nokia GSM Lumia 635, phone 3, was allowed to stay in the experiment because a file system extraction was able to occur. The file system extraction extracts not only everything that can be seen on the phone, but also the files and hidden files within it. These hidden files could be essential in an investigation, especially one dealing with the criminal use of digital devices.

## 4.2: Initial Factory Reset

The initial factory reset was used to wipe any personal artifacts or activities performed by the previous owners. This reset was done with some phones powered on and extracted via the settings menu. The phones chosen for this method would not factory reset without the phones being on. The other phones were reset when the phones were turned off. Two of these phones required not only a factory reset, but also a wipe of the cache partition. The LG CDMA LS-720 (phone 4) had only the factory reset available, while the Nokia GSM Lumia 635 (phone 3) automatically reset itself with no user options.

## 4.3: Data Creation

The original identities created for the phones were copyrighted, and therefore were changed to public domain names of Jane Austen characters. The different artifact sections were chosen because Cellebrite® claims that with a physical extraction it can get artifacts such as: SMS, contacts, call logs, media, app data, files, hidden files, and deleted data (see Figure 1). With those specific sections, the limits of the physical extraction were widened to see if email, web history, and web favorites were included. The locations and calendar reminders were already included in the app data. As previously stated, the Samsung GSM SGH-t499 Dart (phone 5) and the ZTE GSM V768 Concord (phone 6), were unable to take pictures because they had no SD card. In an investigation, by law enforcement, pictures are key to helping discover the various aspects of a case. The Nokia GSM Lumia 635 did not have the same applications market, therefore it did not have the same fake text and call log apps. The HTC Vivid had an application market, but it crashed before it could be used. Therefore, these two phones did not get the Fake Text Messages and the Fake Call Logs applications, hence no SMS or phone artifacts created.

An interesting occurrence, was that the Nokia GSM Lumia 635 could receive emails, but could not send emails. So the data created for the emails on this phone was from using Gmail© on a computer to send emails back, but opening the received emails on the phone.

#### **4.4: Phone Extraction(s) with Data**

##### **4.4.1: Cellebrite UFED Touch®**

Physical extractions were performed on all of the phones that allowed it. Oddly, phones changed what extraction types they would allow. The only two phones that stayed with the same extraction options were the Kyocera Hydro (phone 1) and the LG CDMA LS-720, which allowed for all three types of extractions.

The ZTE GSM Z830 (phone 2) originally allowed a “physical extraction (rooted),” but it did not allow that option after the phone was reset. Instead, the ZTE would only do a file system and physical extraction at the same time. A logical extraction was not offered.

The Nokia GSM Lumia 635 never offered a physical extraction, yet it initially did separate logical and file system extractions. However, once the phone was reset and data was added, it again created a multi-step file system and logical extraction.

The HTC Vivid was able to do physical and logical extractions, as it could initially. The difference this time, was a new physical extraction option that was a “Bypassing Lock” and was “Recommended.” So both the regular physical extraction and the physical extraction bypassing lock were performed on this phone. While the data from both extractions seemed to match up, the byte size of the overall images was different. The regular physical extraction was bigger in bytes, so it was used for the collected data. There was no explanation for this incidence. During an investigation, an

image with more bytes will almost always be used, because the lesser one may have missed some minuscule data that could be crucial. Although, both should be looked at extensively.

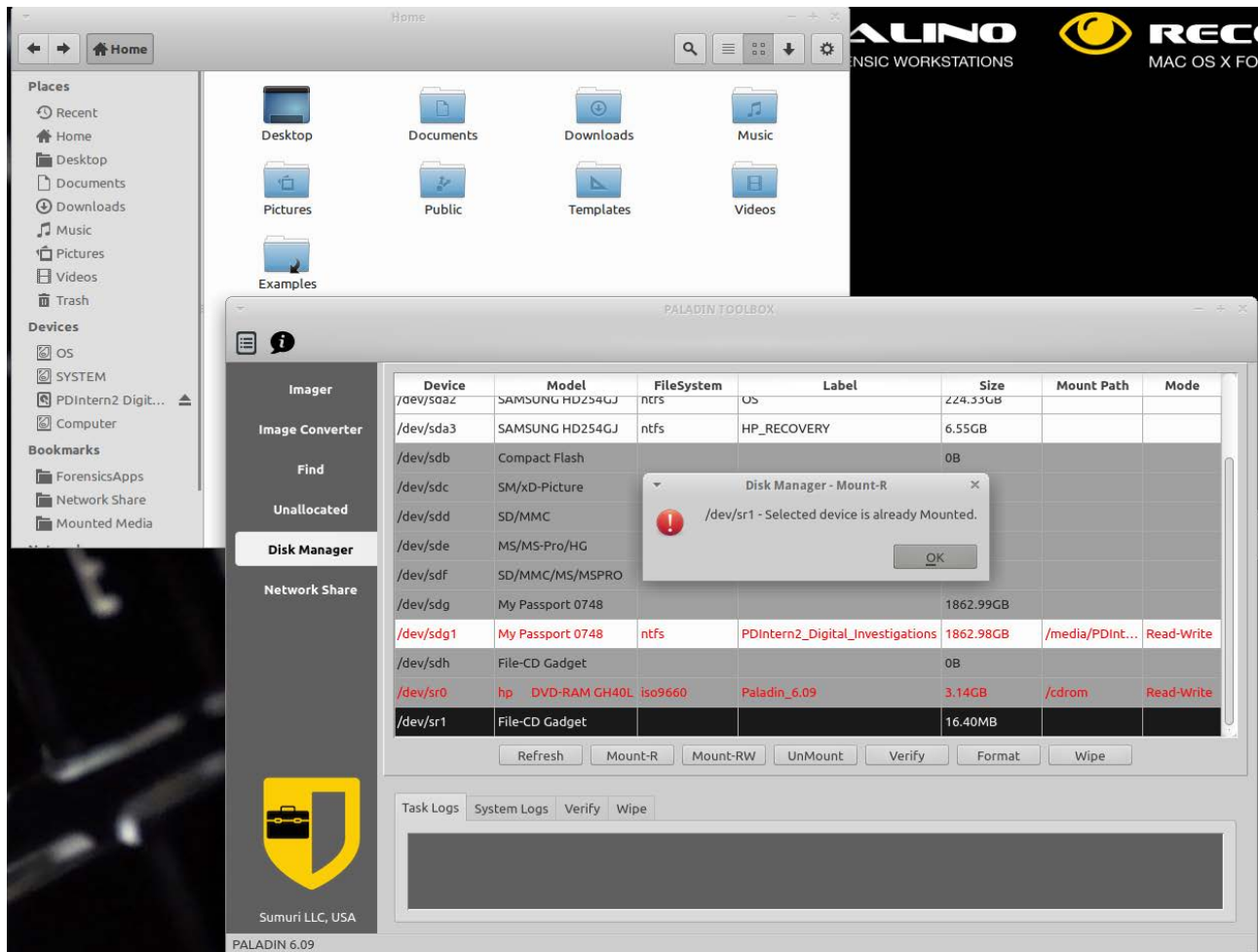
Another odd event was the different amounts of data extracted between the physical and logical extractions (see Tables 9, 10, 11, 12, 14, 15, 18, and 19). Some of the discrepancies can be explained by the duplication of artifacts on the logical extraction because they are not only on the phone, but are synchronized through the Gmail<sup>®</sup> accounts. This can be seen with call logs, contacts and calendar reminders (see Tables 9, 15, and 19). As for the other idiosyncrasies, there seems to be no confirmed explanation. These peculiarities should be noted and watched for, especially when investigating a case. One should either do all physical or all logical extractions to keep them from becoming confusing, unless there is a confirmed explanation as to why there are differing numbers.

#### **4.4.2: Paladin<sup>®</sup> and Autopsy<sup>®</sup>**

The Paladin Forensic Suite<sup>®</sup> was the first open source tool downloaded, because of its variety of tools, including Autopsy<sup>®</sup>. The manual was read and notes were taken on how to use the suite. When the phones were plugged into the USB port on the computer they would show up on the Disk Usage Analyzer, showing how much space was being used and for what. Nevertheless, only the Kyocera Hydro and the HTC Vivid were recognized as drives that could be imaged. The other three phones were just shown as a “USB Driver” or “Internal Storage” device (see Appendix E for an example). In Disk Manager, the three unrecognized phones would either not show up, or appear but would not be mounted. When they appeared but not as mounted, trying to mount them would

bring up an error message saying it was already mounted or could not be mounted (see Figure 6).

**Figure 6.** A screenshot from Paladin® showing the ZTE Z830 being mounted but at the same



*time not being recognized.*

For the two phones that were recognized, the Kyocera Hydro and the HTC Vivid had different USB connection options other than MTP (Media Transfer Protocol) mode or charging only. The Kyocera Hydro was connected via the Mass Storage Mode, while the HTC Vivid was on the Disk Drive Connection. It's likely that these modes make the



phones into USBs instead of media devices. There is no explanation as to why the other three phones could not be mounted.

The two images that were taken of the phones had hash value verification for each one (See Appendix D). The unallocated and find applications of Paladin® were used on the Kyocera Hydro, but turned up nothing substantial (See Appendix F). Therefore, no unallocated or find application was used on the HTC Vivid image. Autopsy® then used the Paladin® images to create new cases for each phone. The only screenshots taken in Autopsy® were those of the list of extracted artifacts, and a timeline created of all the activities performed on the phones (See figures 4 and 5 for the Kyocera Hydro and Appendix D for the HTC Vivid). Both timelines showed events happening in random years like 1992, when these smartphones were not even made yet. At closer look these activity dates are for calendar events, and some pictures including the ones created for this experiment. The author suggests that the dates represent the earliest date the phone can go back to and that's where backups of artifacts are kept. Also, the calendar events like birthdays and holidays are set to recur every year, and begins in the earliest date possible. Another thing to note on the timelines are orphan files. These files are of pictures and artifacts left over after the factory reset. This seems reasonable because the factory reset likely deleted part of the headers, but not enough data was deleted to permanently delete the artifacts. There were no databases on the computer or the Paladin® program itself, to run any further examination in Autopsy®.

The rest of the forensic suite tools offered in the Paladin Toolbox® did not work. Specific commands were entered according to the instruction, but to no avail. No further examination was done using Paladin®.

#### **4.4.3: Andriller®**

There was only one type of Andriller® extraction performed. That was the Android Backup method because no other information was extracted using the other types of extraction since the phones were not rooted (See Appendix G). The Nokia GSM Lumia 635 was not recognized with this tool because it does not use an Android based operating system. Every phone report had Wi-Fi passwords, web history, and web downloaded history. The only difference on the report was that the Kyocera Hydro and the HTC Vivid had contacts extracted likely because the contacts were synchronized through the Gmail© accounts, while the other phones just had the contacts on the phone. As for other information that was not extracted from these phones using Andriller® were certain applications and vendors are not supported for this tool. Also, other apps where data could be extracted were not used or made for this experiment. Though this tool was not used to the fullest extent, it would be a quick way for examiners to get the basics of an Android phone.

#### **4.4.4: BitPim® and Other Programs**

BitPim® has not been updated since 2010, and therefore a lot of phones are not recognized by this tool. Unfortunately, none of the phones in this experiment were recognized (See Appendix H for an example).

Other open source tools were examined for this experiment through trial and error, but some tools were proprietary or you had to pay for them, so they were not used. Other tools forbid law enforcement agencies from using them and were excluded from

this experiment. For a complete list of the tools looked at for this experiment, and the reasons for being excluded, please refer to Appendix B.

#### **4.5: Final Phone Extraction**

Most of the phones had physical extractions taken by the UFED Touch®. Oddly, the multiprojects that occurred in the data extractions (second extractions), were not offered, and reverted back to the original extractions. The only extraction that changed from the first time extraction was the Nokia GSM Lumia 635, where a file system extraction could not take place. This was because no photos were left on the phone after the second reset. Hence, only a logical extraction for the Nokia GSM Lumia 635 was performed. The HTC Vivid had a physical extraction and physical extraction bypassing lock executed. The bypassing lock extraction was fewer bytes than the regular physical extraction.

#### **4.6: Leftover Artifacts from a Factory Reset**

When a factory reset is applied to a phone, it is supposed to delete all personal artifacts from it. However, after two factory resets the Kyocera Hydro, LG CDMA LS-720, and the HTC Vivid had more artifacts than created for this experiment. None of these created artifacts should be showing up after a reset. On top of that, since there were more artifacts than the created ones, the previous owners' artifacts were also extracted from the phone. This meant that even after two factory resets, a person's artifacts on these phones can still be examined and analyzed. It is helpful to know that even with a factory reset a phone can still hold onto created artifacts. This can be used in cases where someone is stealing phones and re-selling them, and/or for other cases where people try to cover up their tracks. One explanation for these phones holding onto their artifacts could be the synchronized Gmail© accounts. The Nokia GSM Lumia 635 may

have contained more artifacts if there were more artifacts on the phone originally. Also, the phone did not have a physical extraction done on it, so no deleted files could be examined thus rendering it useless for artifacts after a reset.

#### **4.7: Future Studies**

There are many things that could improve upon this study. To start, a physical extraction with the UFED Touch® should be performed after the first reset, to see how many artifacts are left over, instead of an estimate of what artifacts were created for the experiment versus the artifacts left from the previous owner. There could also be more data created on the phones to see if that would increase the number of artifacts left over after a factory reset. It would also be interesting to see if there are any differences between the factory resets performed while the phone was powered on versus powered off.

It would be beneficial to have access to more open source tools. It would help to have someone who knows how to code, or use different computer languages to help analyze the phones. Also, a few other proprietary tools should be used; no examiner uses just one tool and there can always be more artifacts on a phone. They just need to be looked at from a different angle.

Other phones, specifically iPhones© should be added to this experiment. It would also be nice to have at least two of each phone to see if there are any differences between the artifacts collected. This would improve reproducibility. Also, more applications should be used, specifically social media ones where people give their information freely, and/or the account is synchronized to the phone.

Other future directions of this study would be to do an extraction on an iPhone©, and then lock it and force the iPhone© to delete all its information with the misuse of passwords.

After the iPhone© has deleted all its information, a secondary extraction should be conducted to see if there is anything left over. This could help cut the time wasted by a law enforcement agency if the study shows that the information isn't fully deleted. Another future study could look into how many times a factory reset has to happen to fully delete any certain artifact. This study could also look into the different operating systems to determine if that affects the factory reset at all. Also interesting, would be looking into different phone carriers to see if there is a difference of what can be extracted from a phone.

## Acknowledgements

I acknowledge the Edina Police Department for letting me conduct my research there. I specifically thank Detective Dave Lindman for teaching me how to use the Cellebrite UFED Touch® and other digital equipment. I thank Sergeant Kevin Rofidal for supporting and supervising me for this internship. Then a big thank you to Ian Levstein who is not only a reviewer for this internship, but a guiding hand that kept me going when times got tough. Also, a thank you to Dr. Terry Fenger for teaching me about digital forensics and being one of my reviewers. Also, a huge thank you to Kelsey Wilkinson, for giving me ideas and a direction for open source tools.

## References

1. Carrier, Brian, Open Source Digital Forensic Tools: The Legal Argument, @stake Research Report, 2002 <[http://www.digital-evidence.org/papers/opensrc\\_legal.pdf](http://www.digital-evidence.org/papers/opensrc_legal.pdf)>
2. Cellebrite. What Happens When You Press that Button? Explaining Cellebrite UFED Data Extraction Processes <<http://smarterforensics.com/wp-content/uploads/2014/06/Explaining-Cellebrite-UFED-Data-Extraction-Processes-final.pdf>> 17.
3. Mumba, E. R., & Venter, H., Mobile Forensics using the Harmonised Digital Forensic Investigation Process. 2014  
<[http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6950491&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs\\_all.jsp%3Farnumber%3D6950491](http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6950491&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D6950491)>
4. Open Source Initiative. The Open Source Definition. <<http://opensource.org/osd>>.
5. Sumuri LLC. Paladin Forensic Suite, 2016 <<https://sumuri.com/software/paladin/>>

6. DenCo Forensics. Home - Andriller - Android Forensic Tools, 2016, July 6  
<<http://www.andriller.com/>>
7. R. Schwamm, "Effectiveness of the factory reset on a mobile device", 2014  
<[www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA607911](http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA607911)>
8. Wikipedia. List of Disney Princesses - Disney Princess Wiki – Wikia, 2016, June 25,  
<[http://disneyprincess.wikia.com/wiki/List\\_of\\_Disney\\_Princesses](http://disneyprincess.wikia.com/wiki/List_of_Disney_Princesses)>
9. Pham, J. (n.d.). Welcome to *BitPim*. Retrieved from <http://www.bitpim.org/>
10. Concise AC. Our Recommended Six Mobile Forensics Tools - Concise Courses, 2013  
<<https://www.concise-courses.com/security/mobile-forensics-tools/>>
11. Wilkinson, K. Development of a Portable Mobile Phone Forensic Acquisition and Analysis Toolkit Utilizing Open Source Tools, 2015  
<[http://www.marshall.edu/forensics/files/Wilkinson\\_Final-Paper.pdf](http://www.marshall.edu/forensics/files/Wilkinson_Final-Paper.pdf)>
12. Cellebrite UFED Touch®, Parsippany, NJ.
13. Paladin Forensic Suite®, by Sumuri, Wyoming, Delaware
14. Autopsy®, by Basis Technology, Cambridge, Massachusetts
15. Andriller®, by DenCo Forensics
16. BitPim®, by Joe Pham





## Appendix B

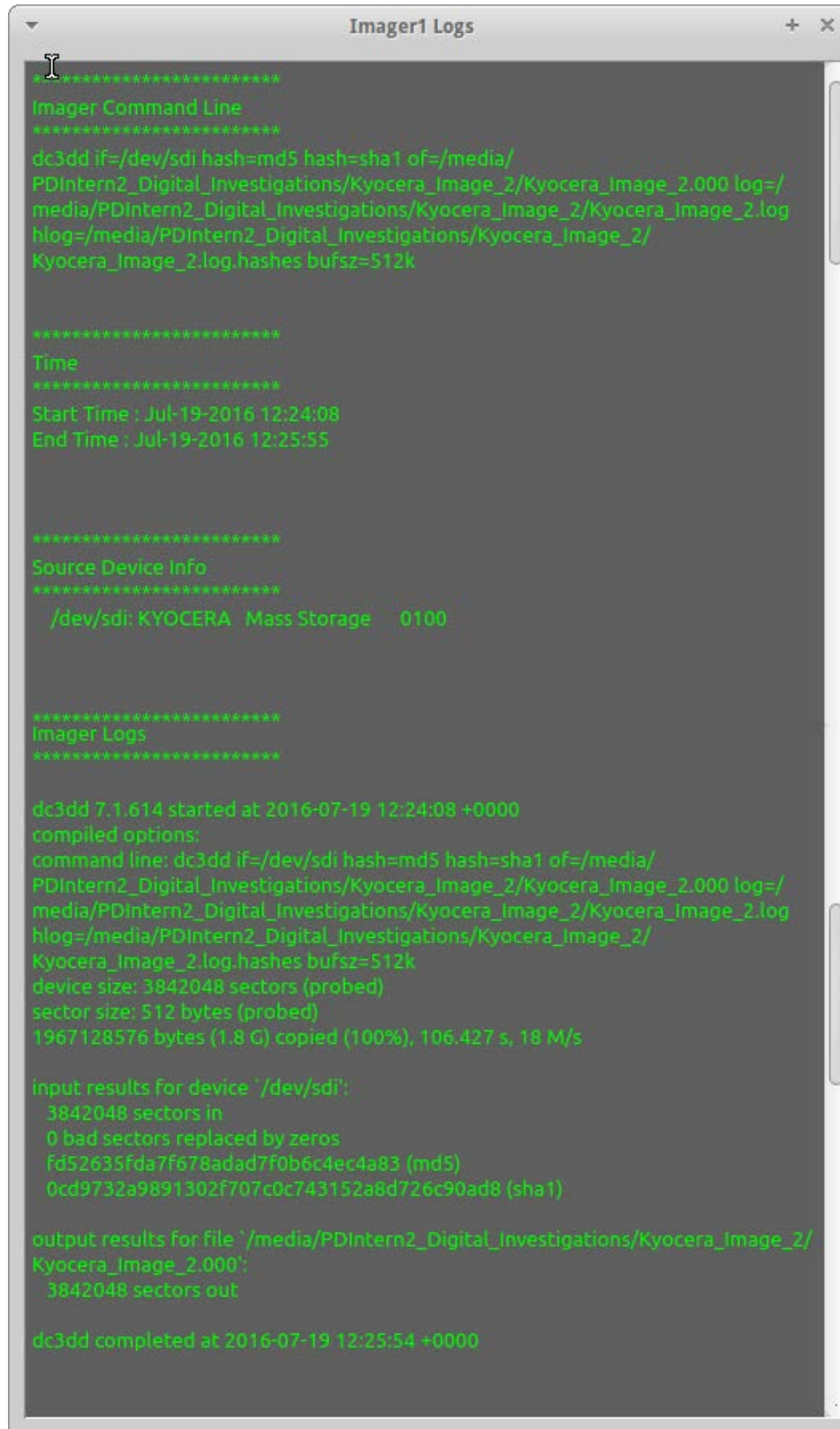
**Table 21.** *A list of tools that were not used in the experiment and the reasons as to why.*

Unused Tools	
iPhone Analyzer	No iPhone© examined
Oxygen Forensic Suite	No longer open source
Bulk Extractor	Was on Paladin®, but did not work
OSAF-TK	Had not been updated and could not get it to work
SAFT	Does not exist
Rubus	No Blackberries© examined
SIFT(Sans)	Ubuntu platform like Paladin®
Mobile Phone Examiner (MPE +)	Must use FTK to analyze
freeiphonedatarecovery.com	Just a trial, and no iPhones© examined
easeus.com/android	Just a trial, and only for deleted data
Deft Linux	Like Paladin, did not understand how to work it
TULP2G	Old, did not know if it was working
MIAT	Phones with Symbian or Windows OS only, and SourceForge did not have
Katana Forensics	Have to buy, and only on Mac Computers©
viaForensics	Vmware did not work
Foremost	Could not image by itself
Digital Forensic Framework	Never got a return email with download pass
Fieldsearch (NIJ)	Only for Criminal Justice agencies, could not get with intern privileges
AF Logical	No law enforcement can use
Android Data Forensics Tool	Requires phone to be rooted, which would've wrote on a phone

**Appendix C****Table 22.** *A table of the graphic data left on phone 1 after factory reset.*

Pictures on Phone 1	
Folders	8*
Total Photos Left	196
Total Videos Left	9
Notes	1 folder added for downloaded folders

## Appendix D



```
Imager1 Logs
*****
Imager Command Line
*****
dc3dd if=/dev/sdi hash=md5 hash=sha1 of=/media/
PDIntern2_Digital_Investigations/Kyocera_Image_2/Kyocera_Image_2.000 log=/
media/PDIntern2_Digital_Investigations/Kyocera_Image_2/Kyocera_Image_2.log
hlog=/media/PDIntern2_Digital_Investigations/Kyocera_Image_2/
Kyocera_Image_2.log.hashes bufisz=512k

*****

Time
*****
Start Time : Jul-19-2016 12:24:08
End Time : Jul-19-2016 12:25:55

*****

Source Device Info
*****
 /dev/sdi: KYOCERA  Mass Storage  0100

*****

Imager Logs
*****

dc3dd 7.1.614 started at 2016-07-19 12:24:08 +0000
compiled options:
command line: dc3dd if=/dev/sdi hash=md5 hash=sha1 of=/media/
PDIntern2_Digital_Investigations/Kyocera_Image_2/Kyocera_Image_2.000 log=/
media/PDIntern2_Digital_Investigations/Kyocera_Image_2/Kyocera_Image_2.log
hlog=/media/PDIntern2_Digital_Investigations/Kyocera_Image_2/
Kyocera_Image_2.log.hashes bufisz=512k
device size: 3842048 sectors (probed)
sector size: 512 bytes (probed)
1967128576 bytes (1.8 G) copied (100%), 106.427 s, 18 M/s

input results for device '/dev/sdi':
 3842048 sectors in
 0 bad sectors replaced by zeros
Fd52635Fda7F678adad7F0b6c4ec4a83 (md5)
0cd9732a9891302f707c0c743152a8d726c90ad8 (sha1)

output results for file '/media/PDIntern2_Digital_Investigations/Kyocera_Image_2/
Kyocera_Image_2.000':
 3842048 sectors out

dc3dd completed at 2016-07-19 12:25:54 +0000
```



```
Imager1 Logs
+ x

*****
Hashes
*****

dc3dd 7.1.614 started at 2016-07-19 12:24:08 +0000
compiled options:
command line: dc3dd if=/dev/sdi hash=md5 hash=sha1 of=/media/
PDIntern2_Digital_Investigations/Kyocera_Image_2/Kyocera_Image_2.000 log=/
media/PDIntern2_Digital_Investigations/Kyocera_Image_2/Kyocera_Image_2.log
hlog=/media/PDIntern2_Digital_Investigations/Kyocera_Image_2/
Kyocera_Image_2.log.hashes bufisz=512k

input results for device '/dev/sdi':
  fd52635fda7f678adad7f0b6c4ec4a83 (md5)
  0cd9732a9891302f707c0c743152a8d726c90ad8 (sha1)

output results for file '/media/PDIntern2_Digital_Investigations/Kyocera_Image_2/
Kyocera_Image_2.000':

dc3dd completed at 2016-07-19 12:25:54 +0000

*****
Verification
*****

dc3dd 7.1.614 started at 2016-07-19 12:25:55 +0000
compiled options:
command line: dc3dd of=/dev/null hash=md5 hash=sha1 ifs=/media/
PDIntern2_Digital_Investigations/Kyocera_Image_2/Kyocera_Image_2.000 hlog=/
media/PDIntern2_Digital_Investigations/Kyocera_Image_2/
Kyocera_Image_2.verify.log

input results for files '/media/PDIntern2_Digital_Investigations/Kyocera_Image_2/
Kyocera_Image_2.000':
  fd52635fda7f678adad7f0b6c4ec4a83 (md5)
  0cd9732a9891302f707c0c743152a8d726c90ad8 (sha1)

output results for file '/dev/null':

dc3dd completed at 2016-07-19 12:26:00 +0000
```

**Figure 7.** Screenshots from the Kyocera Hydro image and hash value verification in Paladin®.

```
Imager1 Logs
*****
Imager Command Line
*****
dc3dd if=/dev/sdh hash=md5 hash=sha1 of=/media/
PDIntern2_Digital_Investigations/
HTC_image_on_disk_drive_connection_read_only_/
HTC_image_on_disk_drive_connection_read_only_.000 log=/media/
PDIntern2_Digital_Investigations/
HTC_image_on_disk_drive_connection_read_only_/
HTC_image_on_disk_drive_connection_read_only_.log hlog=/media/
PDIntern2_Digital_Investigations/
HTC_image_on_disk_drive_connection_read_only_/
HTC_image_on_disk_drive_connection_read_only_.log.hashes bufosz=512k

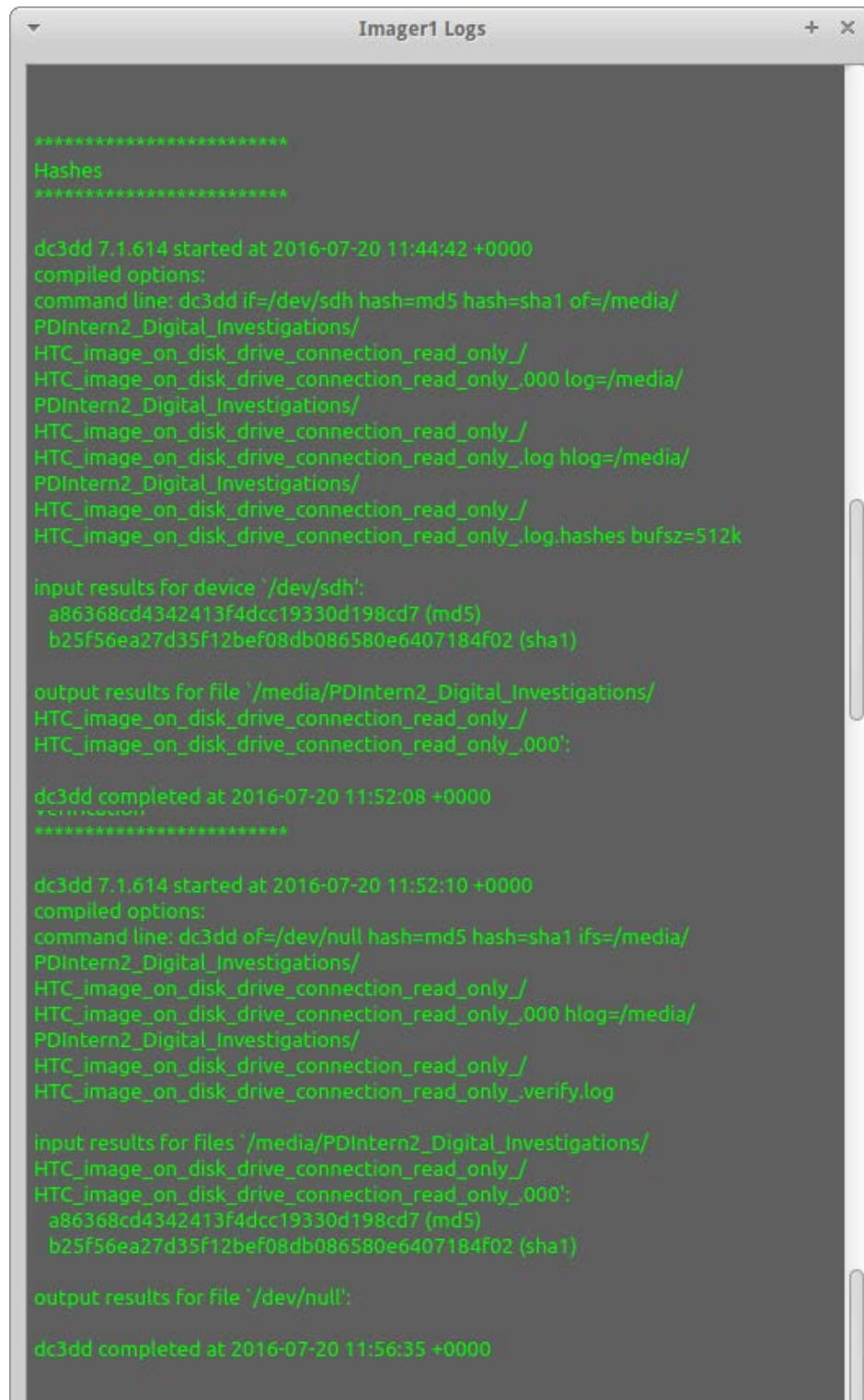
*****
Time
*****
Start Time : Jul-20-2016 11:44:41|
End Time : Jul-20-2016 11:52:08

*****
Source Device Info
*****
/dev/sdh: HTC Android Phone 0000
*****
Imager Logs
*****
dc3dd 7.1.614 started at 2016-07-20 11:44:42 +0000
compiled options:
command line: dc3dd if=/dev/sdh hash=md5 hash=sha1 of=/media/
PDIntern2_Digital_Investigations/
HTC_image_on_disk_drive_connection_read_only_/
HTC_image_on_disk_drive_connection_read_only_.000 log=/media/
PDIntern2_Digital_Investigations/
HTC_image_on_disk_drive_connection_read_only_/
HTC_image_on_disk_drive_connection_read_only_.log hlog=/media/
PDIntern2_Digital_Investigations/
HTC_image_on_disk_drive_connection_read_only_/
HTC_image_on_disk_drive_connection_read_only_.log.hashes bufosz=512k
device size: 18538496 sectors (probed)
sector size: 512 bytes (probed)
9491709952 bytes (8.8 G) copied (100%), 445.646 s, 20 M/s

input results for device `/dev/sdh':
18538496 sectors in
0 bad sectors replaced by zeros
a86368cd4342413f4dcc19330d198cd7 (md5)
b25f56ea27d35f12bef08db086580e6407184f02 (sha1)

output results for file `/media/PDIntern2_Digital_Investigations/
HTC_image_on_disk_drive_connection_read_only_/
HTC_image_on_disk_drive_connection_read_only_.000':
18538496 sectors out

dc3dd completed at 2016-07-20 11:52:08 +0000
```



```
Imager1 Logs
+ x

*****
Hashes
*****

dc3dd 7.1.614 started at 2016-07-20 11:44:42 +0000
compiled options:
command line: dc3dd if=/dev/sdh hash=md5 hash=sha1 of=/media/
PDIntern2_Digital_Investigations/
HTC_image_on_disk_drive_connection_read_only_/
HTC_image_on_disk_drive_connection_read_only_000 log=/media/
PDIntern2_Digital_Investigations/
HTC_image_on_disk_drive_connection_read_only_/
HTC_image_on_disk_drive_connection_read_only_log hlog=/media/
PDIntern2_Digital_Investigations/
HTC_image_on_disk_drive_connection_read_only_/
HTC_image_on_disk_drive_connection_read_only_log.hashes bufosz=512k

input results For device '/dev/sdh':
  a86368cd4342413f4dcc19330d198cd7 (md5)
  b25f56ea27d35f12bef08db086580e6407184f02 (sha1)

output results For file '/media/PDIntern2_Digital_Investigations/
HTC_image_on_disk_drive_connection_read_only_/
HTC_image_on_disk_drive_connection_read_only_000':

dc3dd completed at 2016-07-20 11:52:08 +0000
*****

dc3dd 7.1.614 started at 2016-07-20 11:52:10 +0000
compiled options:
command line: dc3dd of=/dev/null hash=md5 hash=sha1 ifs=/media/
PDIntern2_Digital_Investigations/
HTC_image_on_disk_drive_connection_read_only_/
HTC_image_on_disk_drive_connection_read_only_000 hlog=/media/
PDIntern2_Digital_Investigations/
HTC_image_on_disk_drive_connection_read_only_/
HTC_image_on_disk_drive_connection_read_only_verify.log

input results for Files '/media/PDIntern2_Digital_Investigations/
HTC_image_on_disk_drive_connection_read_only_/
HTC_image_on_disk_drive_connection_read_only_000':
  a86368cd4342413f4dcc19330d198cd7 (md5)
  b25f56ea27d35f12bef08db086580e6407184f02 (sha1)

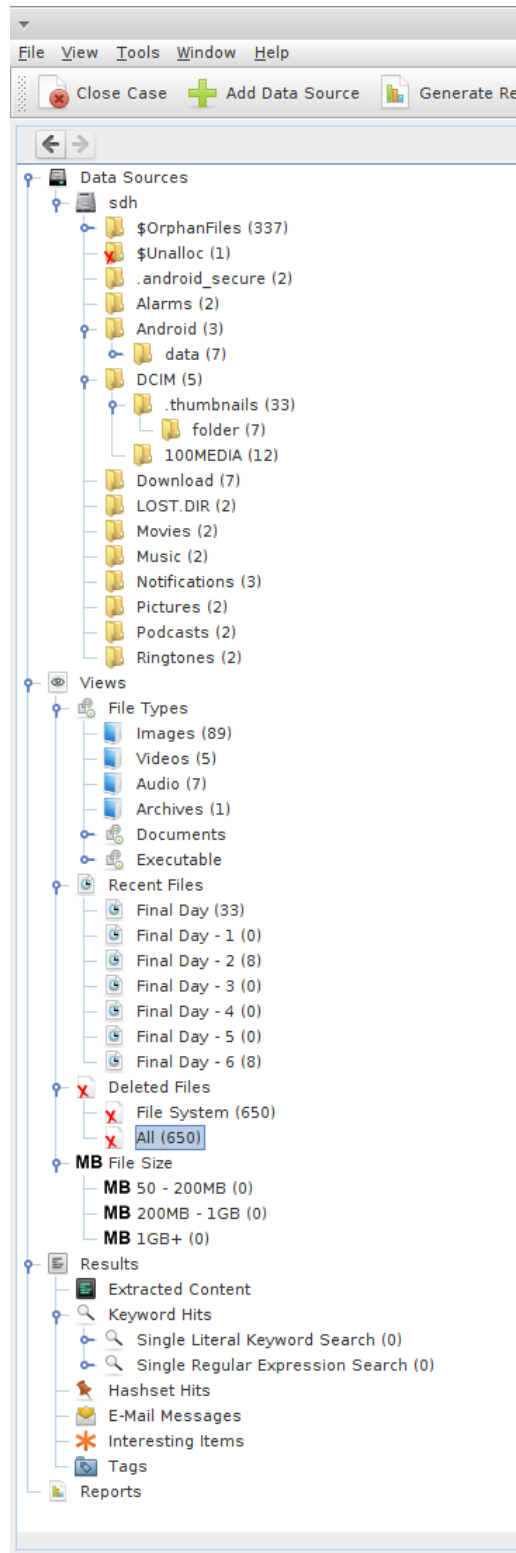
output results For file '/dev/null':

dc3dd completed at 2016-07-20 11:56:35 +0000
```

**Figure 8.** Screenshots from the HTC Vivid image and hash value verification in Paladin®.

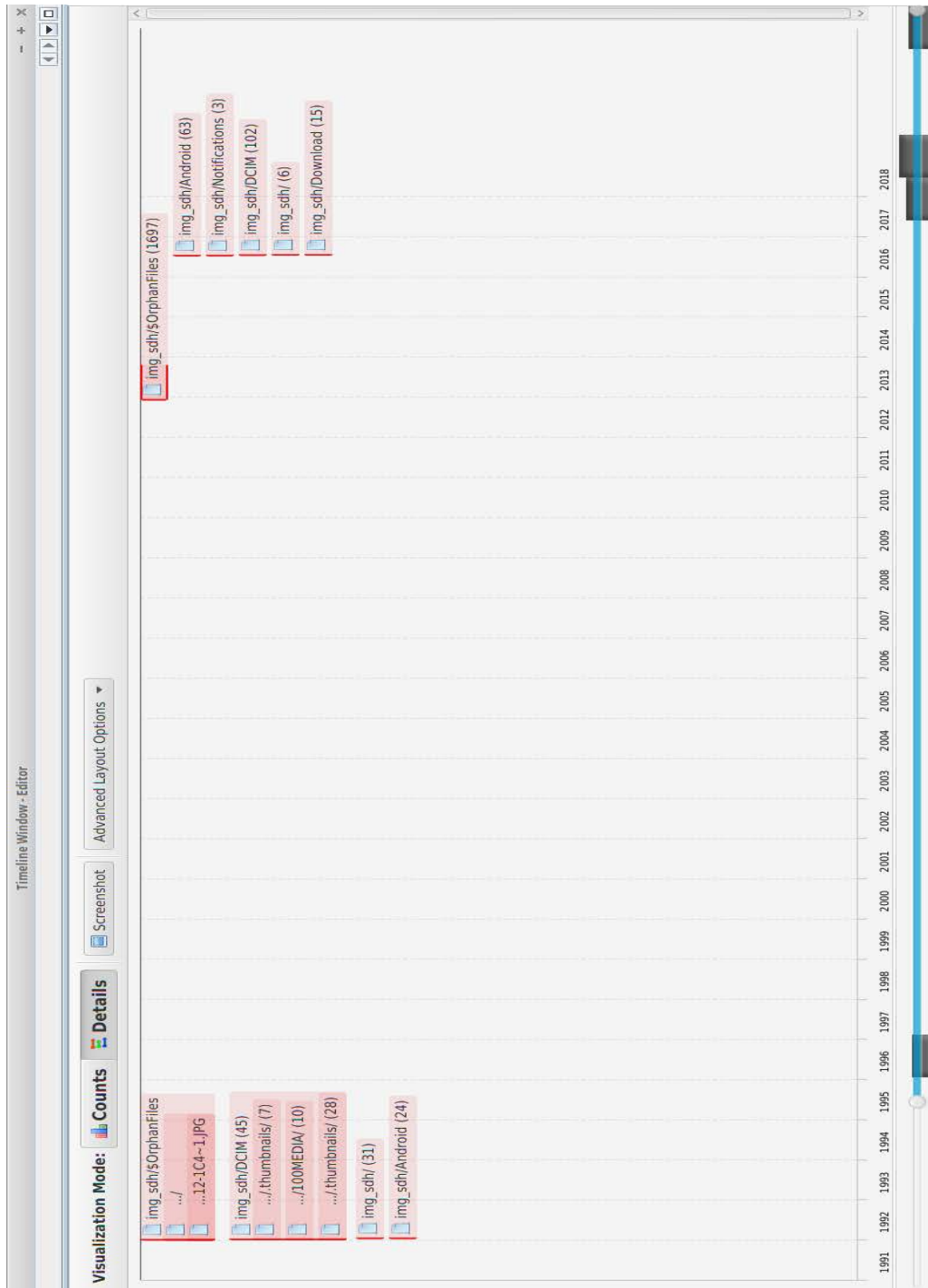
Folder	Usage	Size	Contents
HTC_STORAGE	100.0 %	47.6 MB	93 items
DCIM	66.2 %	31.7 MB	47 items
100MEDIA	97.1 %	30.0 MB	11 items
.thumbnails	2.8 %	1.6 MB	35 items
folder	6.4 %	196.6 kB	6 items
Android	29.7 %	13.9 MB	29 items
data	99.8 %	13.9 MB	28 items
com.google.android.apps.maps	98.3 %	13.6 MB	19 items
com.google.android.videos	0.7 %	98.3 kB	3 items
com.htc.mediacheprovider	0.5 %	65.5 kB	2 items
com.google.android.apps.genie.geniewidget.news-content-cache	0.2 %	32.8 kB	2 items
Download	3.4 %	1.7 MB	6 items
Notifications	0.1 %	65.5 kB	2 items
.android_secure	0.1 %	32.8 kB	1 item
LOST.DIR	0.1 %	32.8 kB	1 item
Music	0.1 %	32.8 kB	1 item
Podcasts	0.1 %	32.8 kB	1 item
Ringtones	0.1 %	32.8 kB	1 item
Alarms	0.1 %	32.8 kB	1 item
Pictures	0.1 %	32.8 kB	1 item
Movies	0.1 %	32.8 kB	1 item

**Figure 9.** The disk usage manager screenshot of the HTC Vivid phone on Paladin® is pictured above.



**Figure 10.** Shows what Autopsy® was able to extract from the HTC Vivid.





**Figure 11.** The Autopsy® tool was used to make a timeline of activities and artifacts on the HTC Vivid, shown above.

## Appendix E

The screenshot shows the Paladin forensic workstation interface. The main window displays the disk manager view for the LG-LS720 device. The device is identified as an internal storage device rather than a drive. The interface includes a sidebar with navigation options, a main table of disk partitions, and a task log at the bottom.

Device	Model	FileSystem	Label	Size	Mount Path	Mode
/dev/sda	SAMSUNG HD254GJ			232.89GB		
/dev/sda1	SAMSUNG HD254GJ	ntfs	SYSTEM	2.00GB		
/dev/sda2	SAMSUNG HD254GJ	ntfs	OS	224.33GB		
/dev/sda3	SAMSUNG HD254GJ	ntfs	HP_RECOVERY	6.55GB		
/dev/sdb	Compact Flash			0B		
/dev/sdc	SM/xD-Picture			0B		
/dev/sdd	SD/MMC			0B		
/dev/sde	MS/MS-Pro/HG			0B		
/dev/sdf	SD/MMC/MS/MSPRO			0B		
/dev/sdg	My Passport 0748			1862.99GB		
/dev/sdg1	My Passport 0748	ntfs	PDIntern2_Digital_Investigations	1862.98GB	/media/PDInt...	Read-Write
/dev/sr0	hp DVD-RAM GH40L iso9660		Paladin_6.09	3.14GB	/cdrom	Read-Write

Task Logs

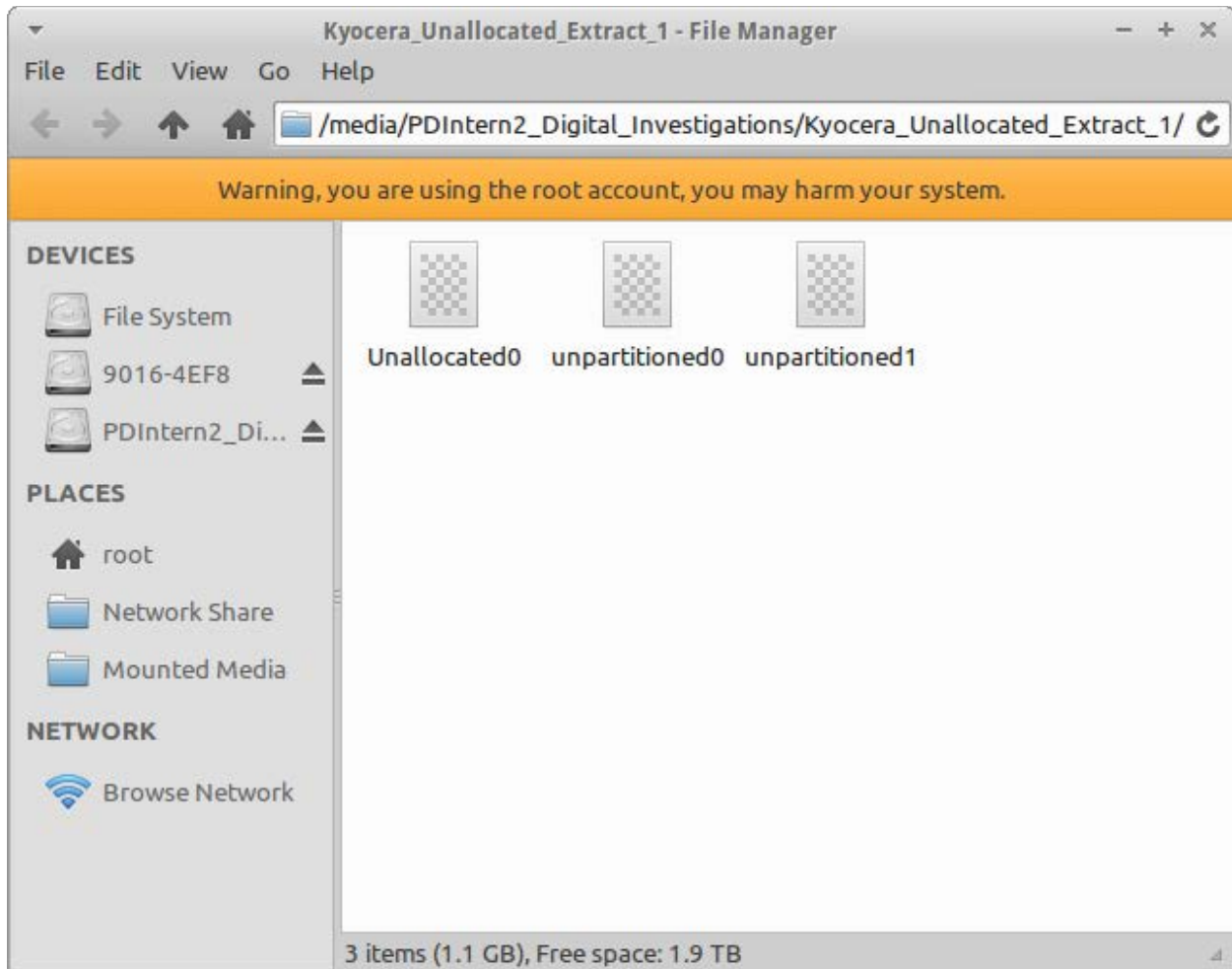
```

Jul-20-2016 11:42:59 /dev/sdb (Model: Android Phone, Serial No.: FA27VVJ03551, Size: 8.84GB) has been unmounted
Jul-20-2016 11:43:06 /dev/sdb (Model: Android Phone, Serial No.: FA27VVJ03551, Size: 8.84GB) mounted as readonly
Jul-20-2016 11:44:41 Task started: dc3dd if=/dev/sdb hash=md5 hash=sha1 of=/media/PDIntern2_Digital_Investigations/
HTC_image_on_disk_drive_connection_read_only /HTC_image_on_disk_drive_connection_read_only_000 log=/media/
PDIntern2_Digital_Investigations/HTC_image_on_disk_drive_connection_read_only /
HTC_image_on_disk_drive_connection_read_only_log log=/media/PDIntern2_Digital_Investigations/
HTC_image_on_disk_drive_connection_read_only /HTC_image_on_disk_drive_connection_read_only_log hashes.bufsz=512k
Jul-20-2016 11:52:08 Imager1 completed successfully
Jul-20-2016 11:52:08 Verification started for Imager1
Jul-20-2016 11:56:35 Imager1 verification completed successfully

```

**Figure 12.** Screenshot on Paladin® of the LG CDMA LS-720 was not recognized as a drive, but an internal storage device, shown above.

## Appendix F



**Figure 13.** *The results from the unallocated search on Paladin® on the Kyocera Hydro image.*

## Appendix G

Data type	Android ver 2.x (unrooted)	Android ver 4-5.x (unrooted, via AB extraction)	Android ver 2-5.x (rooted, adb or su)	Android ver 2-5.x (via CWM recovery)
Android device make and model	+	+	+	?
IMEI, build version, OS version	+	+	+	?
WiFi mac address	+	+	+	-
Time and date check	+	+	+	-
SIM card details (for a some Galaxy Sx devices only)	+	+	+	?
Synchronised accounts	+	+	+	-
Lockscreen Gesture patter decoding	-	-	+	+
Lockscreen PIN cracking up to 4 digits	-	-	+	+
Bluetooth mac address and name	-	-	+	+
Wi-Fi passwords (WPA-PSK/WEP)	-	+	+	+
Phonebook contacts	-	-	+	+
Call logs register	-	?	+	+
SMS messages	-	?	+	+
Call logs (Samsung) register	-	+	+	+
SMS (Samsung) snippets	-	+	+	+
Android browser saved passwords	-	?	+	+
Android browser browsing history	-	?	+	+
Google Chrome saved passwords	-	?	+	+
Google Chrome browsing history	-	?	+	+
Dolphin web browsing history	-	+	+	+
Skype Calls	-	+	-	-
Skype Messages	-	+	-	-
ChatOn messages	-	+	+	+
Facebook chat messages	-	?	+	+
Facebook user viewed photographs	-	?	+	+
Facebook user notifications	-	?	+	+
WhatsApp contacts list	-	?	+	+
WhatsApp calls	-	?	+	+
WhatsApp chat messages	-	?	+	+
Kik Messenger chat messages	-	+	+	+
BBM (Blackberry Messenger) chat messages	-	?	+	+
Viber calls register	-	+	+	+
Viber chat messages	-	+	+	+
Tinder matches	-	+	+	+
Tinder chat messages	-	+	+	+
MeowChat messages	-	+	+	+

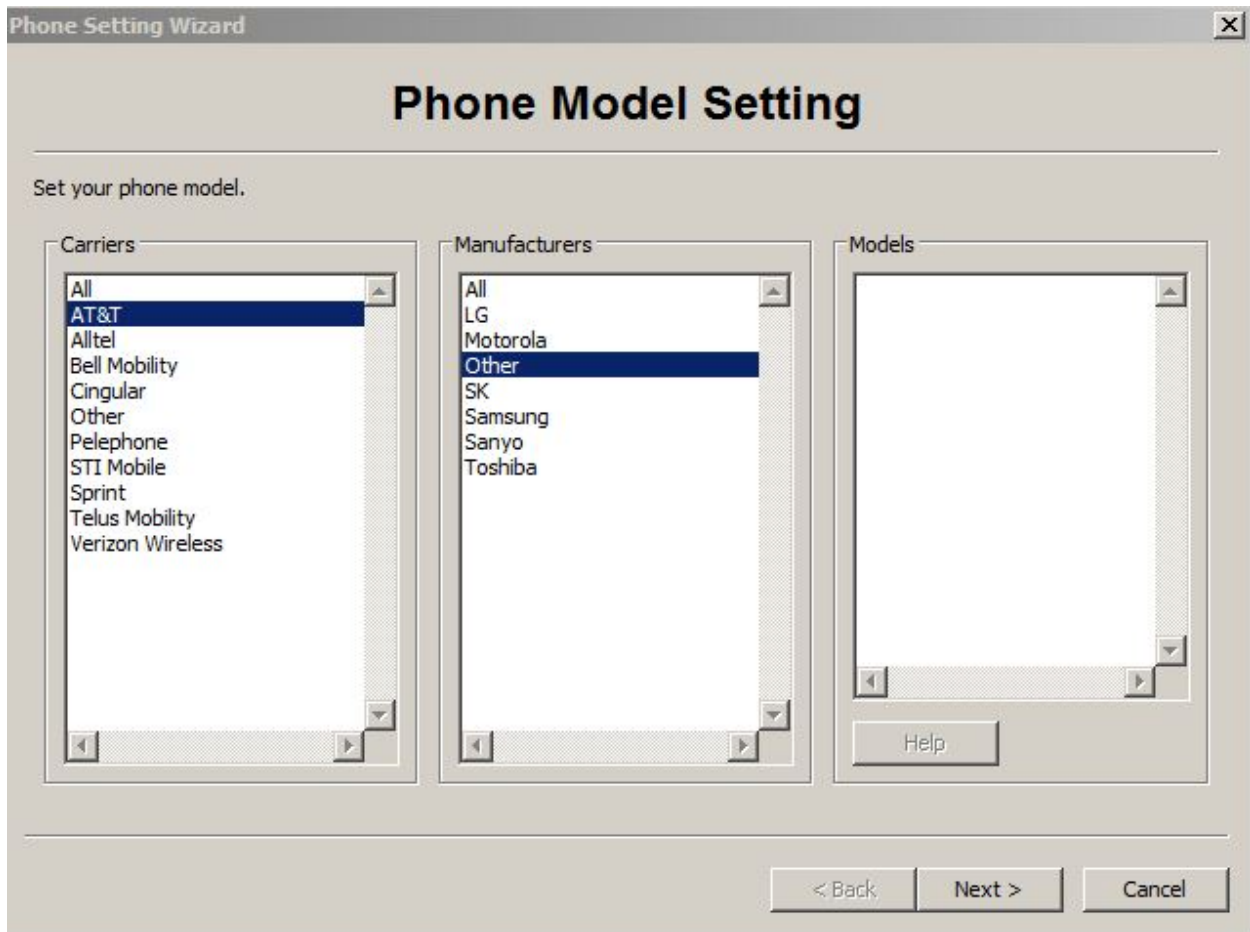
"+" Supported for the extraction method

"?" May be supported for extraction method (Android version, App version or vendor dependant)

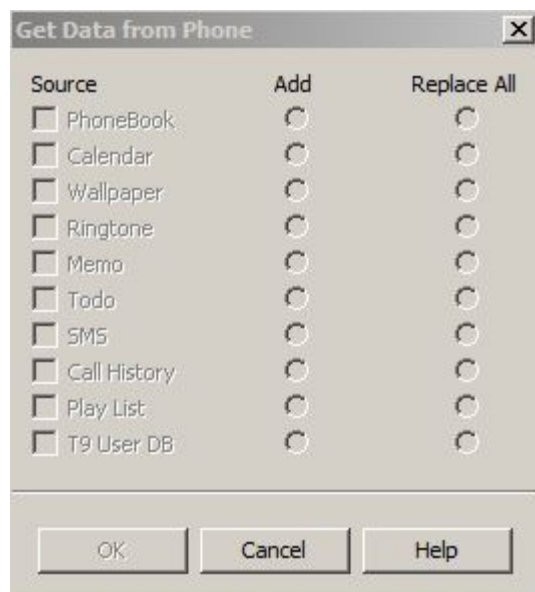
"-" Not supported for the extraction method

**Figure 14.** The list shows what can be mined from certain extractions using Andriller®.

## Appendix H



**Figure 15.** The selection of phones that BitPim® is able to recognize.



**Figure 16.** The artifacts that cannot be extracted by BitPim®.

