Development of a Portable Mobile Phone Forensic Acquisition and Analysis Toolkit Utilizing Open Source Tools

Kelsey Wilkinson, B.S.

Marshall University Forensic Science Department

Summer 2015

Reviewers: Robert J. Boggs; Joshua L. Brunty, M.S.; Terry Fenger, Ph.D.

Abstract

Commercial tools have dominated mobile phone analysis in digital laboratories for years. Commercial tools are expensive and are not perfect – they can still miss data. In addition, some mobile devices are not supported by commercial tools. Open source tools are free and available to everyone; there is no need for licensing fees each year, which can cost a laboratory thousands of dollars. Since the programming script is open source, any bugs or issues with the tool can be found and fixed quickly by users. Also, the open source feature allows examiners to modify and customize their forensic tools to their specific needs. The proprietary nature of commercial tools has made it difficult to explain and demonstrate the process of acquisition in court, while open source tools allow source code to be presented in court. Open source tools have also started adding user-friendly GUI's, such as Autopsy (for Sleuth Kit) or DEFT.

The Raspberry Pi was developed by The Raspberry Pi Foundation, a non-profit organization dedicated to educational charity. Since its release in 2012, the Raspberry Pi's use in the digital community has grown steadily. This small, credit card size computer allows people to develop and create their own projects and uses for the device beyond its intended concept of learning programming in the classroom. Many forensics applications of this device have developed over the years as well, including penetration testing, surveillance, and network forensics. The use of the Raspberry Pi 2 Model B to construct a small device with a touchscreen for mobile phone acquisition was researched. Using a Raspberry Pi and open source tools for acquisition could increase efficiency, while greatly lowering the cost for digital forensic labs.

A simple device was developed for around about $300, utilizing both a 3D printed case and a small pelican case design. A ROBO 3D™ printer was used for the 3D printed version. Raspbian, a Debian-based operating system was loaded onto the SD card, and several open

source tools with easy-to-use GUI's were tested for use with the device. The Open Source Android Forensics Toolkit (OSAF-TK) tool was chosen and then compared to commercial tools for Android operating systems. The compiled OSAF-TK tool labeled MOBIUS was able to perform a logical extraction comparable to commercial tools. The design and open source tool used to create this device will be discussed, as well as the specific results found during comparison studies. With further research and continued development of mobile phone forensic tools and GUI's, open source tools may prove to be a useful addition to digital forensic examiners' toolkit in the near future.

Introduction

At the first Digital Forensics Research Workshop (DFRWS) in 2001, digital forensics was defined as:

> The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.[1]

A large number of digital sources can be analyzed, including but not limited to: removable media, hard drives, and mobile devices. In the field of digital forensics, the number of mobile devices being analyzed has steadily grown. According to the Pew Research Center, as of October 2014 at least 90% of Americans own a cell phone and 64% have a Smartphone[2]. With increasing numbers of Americans who own cell phones, mobile devices associated with or seized from criminal activities is on the rise as well. Videos, texts, pictures, browser history, and much more

can be obtained from these devices and can lend to investigation in numerous ways. Not only are mobile devices personal computers, they are also used as cameras and video devices during events as well. A great example of an event in which this type of evidence was useful is when investigators used mobile devices and videos of the Boston bombings in order to determine the time and origin of the bombs[3].

Mobile Devices

Mobile devices come with a variety of features and sizes, ranging from a simple telephone to a personal computer. However, their basic concept is still the same. Each are small, portable devices that are mainly used for communication purposes. Their hardware can consist of the following: a microprocessor, liquid crystal display (LCD), radio frequency (RF) module, digital signal processor, microphone, speaker, secure digital (SD) card, subscriber identity module (SIM) card, read only memory (ROM), and random access memory (RAM). Operating systems (OS) can also vary between mobile devices, including a personal or an open source OS. The main types of OS are Android, iOS, Symbian, BlackBerry OS, WebOS and Windows Phone. Although the operating systems can differ, the information stored on each device is similar[4].

Mobile devices use various configurations of non-volatile NAND and NOR flash memory in combination with RAM. Figure 1 shows the configurations of flash memory for each generation according to the National Institute for Standards and Technology (NIST). NAND flash memory has a higher capacity for storage, however it is more susceptible to bad blocks making it less reliable. NOR flash memory is much more reliable and allows random access to its memory, while NAND must be accessed sequentially. The RAM is volatile memory, which

means that as a device is shut off and no electricity flows to the capacitors, the memory from RAM will be lost. Volatile memory is used by the device to increase efficiency in processing; the memory stored in RAM is application or OS information that is needed at the time for processing, which gives the microprocessor faster access to the information needed currently[4].

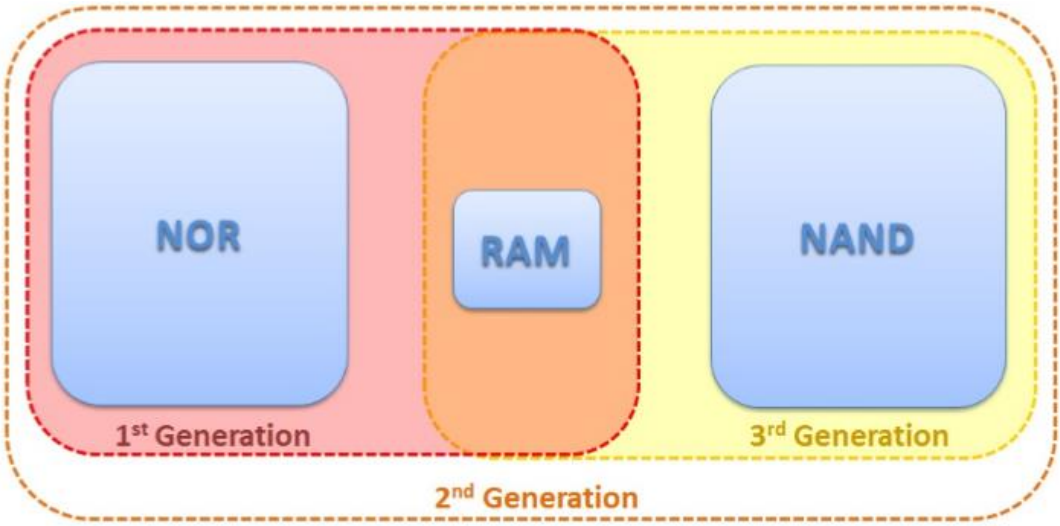

Figure 1. *NIST's representation of first, second, and third generation flash memory configurations in mobile devices*[4].

The data and information that is found in each section of memory can be useful to a forensic examiner. NOR flash memory will usually store information such as the operating system, OS kernel, booting information for the OS and applications, and device drivers. In contrast, NAND memory will generally contain user information or files, such as videos, graphics, application cache, or settings. Flash memory can only be written over a certain number of times before a block will fail. Wear-leveling is a feature that optimizes movement and organization of information in order to increase the life of each block. This management of data affects the deletion of information. Once deleted, data will remain in a block until garbage

collection is initiated and sanitizes this block. Because of the movement and deletion processes, data may be found twice and deleted data may still be found in unallocated space[4].

SIM cards or identity modules (also known as Universal Integrated Circuit Card or UICC) are found in GSM or newer CDMA mobile devices. GSM mobile devices cannot function without the SIM card present, while newer CDMA models use a CDMA Subscriber Identity Module (CSIM) application running on a UICC for 4G/LTE. SIM cards are usually found underneath the battery or back of the device, while SIM cards in Apple devices or newer Android phones can be accessed from the side of the phone using a paper clip or other small, thin tool. Figure 2 shows examples of each SIM card position. There are three sizes of SIM cards used in mobile devices, which can be found in Figure 3. Nano SIM cards are found in newer devices. SIM cards can consist of a processor, RAM, ROM, electronically erasable programmable read only memory (EEPROM), and a file system. This file system can have probative information for an analyst, such as user and service information, passwords, contact lists, text messages, and last numbers dialed (LND). A four to eight digit Personal Identification Number (PIN) may be required to read or update this information. If the PIN is incorrectly entered 10 times it will lock the user out, which will then require a PIN Unblocking Key (PUK) to reset the PIN[4].

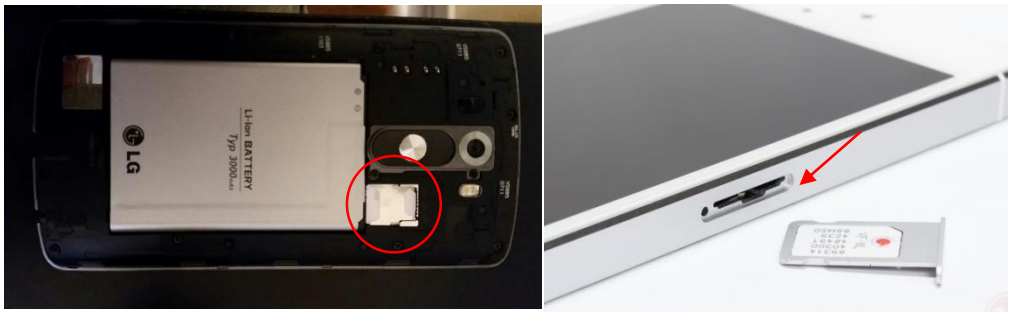

Figure 2. *The SIM card location in an Android (left) and Apple (right) device is shown above*[5].

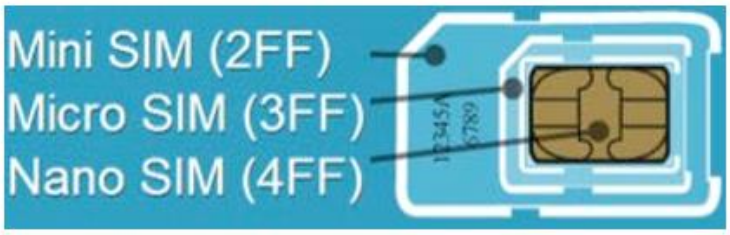

Figure 3. *The three sizes of SIM cards used in mobile devices are shown above*[4].

In addition to a SIM card, some mobile devices may also have a secure digital (SD) media card located in the same locations a SIM card can be found. These cards can be used for optional extra storage on a mobile device for graphics, videos, or applications. Analysis of the SD media card is beneficial for the analyst, because of the large amount of data that can be stored on them. SD cards can be imaged separately from the mobile device with imaging software such as FTK Imager[4].

Mobile Device Acquisition and Analysis

Acquisition is the process of extracting the data from a mobile device and producing an image from which to parse and analyze data. The data and information stored on mobile devices can be obtained several ways. NIST describes five mobile acquisition levels, which are shown in Figure 4. As the levels increase, the difficulty of acquisition increases as well. Levels 4 and 5 require a highly trained analyst. The first level is manual extraction, which is manually photographing the probative evidence on the screen of the device. This is usually only done when the device is not supported by another tool, since it is time consuming and does not allow for unallocated space to be analyzed. Level 2 consists of logical extractions, which provides an

image only consisting of the file system and data in the allocated space. While this type of extraction provides easier parsing and analysis, it does not allow examination of unallocated space. Hex Dumping and JTAG acquisition are Level 3 acquisitions. These provide a complete bit by bit image of the memory in the device, including both allocated and unallocated space. However, these are much more difficult to obtain. For hex dumping, a forensic software tool is usually used to root the device or install a bootloader. The fourth level is the chip-off method, which produces a binary image of the memory. As the name suggests, it involves physically removing the memory chip in order to dump the information. Level 5 is a micro read or the use an electron microscope to read the gates of the NAND or NOR memory chip. This is the most difficult level of acquisition and is only used in high profile cases such as national security.

Figure 4. *The five levels of mobile acquisition as defined by NIST are shown above*[4].

Commercial tools, such as UFED, XRY, MPE+, Tarantula, and Oxygen Forensic Suite, are used most often in order to extract data from mobile devices. Tools such as these vary in acquisition levels and support of different models and operating systems of mobile devices. SIM cards can be extracted separate from the device using UFED, SIMIS, or other similar tool using a

SIM card reader. There are a few advantages of using commercial tools, including the general acceptance and use by the forensic community. Also, classes or certificates are often offered by the companies and manufacturers of commercial tools for a price. Licensing fees can include customer service or IT help if a problem arises with the tool.

Although commercial tools have their advantages, there are many disadvantages to using them as well. Commercial tools can be expensive for digital laboratories with a high initial cost and an annual license fee worth thousands of dollars. Each tool offers a different list of supported devices. While using more than one commercial tool can cover a large number of mobile devices, it can be expensive to purchase and maintain two or more tools. In addition, although a tool claims to support a specific mobile device, it still may not work. There is such a large number of configurations of mobile devices including models, versions, and service providers that many of the commercial tools cannot keep up with every device. Although they are expensive, commercial tools still miss information[6]. Lastly, due to the proprietary nature of the source code for commercial tools, it is difficult to know exactly how the extraction is occurring, what bugs may be present in the tool, and how to give full disclosure of analysis in court testimony.

Open Source Tools

Open source tools are mobile acquisition tools that allow the distribution and use of the source code to everyone and are usually free. The Open Source Initiative gives guidelines that must be followed in order for a program or software to be considered open source[7]. These guidelines are 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[7].

The two most common forms of open source licensing are the GNU Public License (GPL) and the Berkeley Software Distribution License (BSD). The GPL license requires the original source code to remain available, while the BSD license only requires a statement referencing that the original code came from a BSD licensed program. In 2011, the Open Source Initiative recognized 58 licenses as open source[8].

A few open source mobile forensic tools are The Sleuth Kit, iPhone Analyzer, Androphsy, and Open Source Android Forensics Toolkit (OSAF-TK). An important disadvantage for many examiners is that open source tools are not always user-friendly. The majority of open source tools include a command line interface that requires commands to be typed in for every step of the process. This can be confusing and difficult to learn for many analysts who do not have any Linux experience. However, many tools are now developing better graphic user interfaces (GUI's), such as DEFT or Autopsy (GUI for Sleuth Kit).

There are other advantages to using open source tools. With the source code available to the user, a student or examiner can learn how a tool operates and where the information comes from. In addition, these tools can be downloaded on most computers or remote systems and are easily portable. Another advantage is that these tools are almost always free of cost. This means that there are no licensing fees or large initial costs for the original equipment. Perhaps the most important advantage is that the source code is available to the examiner. There is no mystery to how this tool works, what information it is extracting, and where it is looking for information. All bugs or issues with the program are being publicly reviewed. Once an issue arises, a patch or fix to the problem occurs more rapidly than commercial tools since all users can work on it together. This source code can also be taken to court in order to show methodology if necessary[8]. Lastly, testing and errors may be easier to address for court hearings[9].

In the case Daubert v. Merrell Dow Pharmaceuticals, Inc., a new standard for forensic evidence was set. This precedence stated that forensic evidence did not only have to be generally accepted by the forensic community as determined by Frye v. United States, but it also had to be testable, have a known error rate, and have published and peer-reviewed papers[10]. Under these rules, digital forensics has come under scrutiny recently by the court system. NIST has been working on tool testing and standards for the digital forensic community, but no standards have been set as of yet. Open source tools may apply to these guidelines easier than commercial tools[9].

When examiners have access to the source code, testing and addressing bugs is much easier. There is no direct way to test commercial tools – they must be compared to another similar tool. In addition, open source means that all bugs can be identified and are publically available, making error rate determination easier. All procedures are disclosed publicly through source code and available to the entire community for review. These codes and procedures could be easily published in peer-reviewed papers. There is little published information about commercial tools besides the features offered. Acceptance of open source tools can be easily determined by the community as it is available to everyone. As open source tools gain more acceptance in the community, they could prove to be useful in each examiner's toolkit[9].

Raspberry Pi

In 2012, the Raspberry Pi Foundation released the Raspberry Pi, a small, single board computer no larger than a credit card and extremely affordable at under $40 each. The most recent model, the Raspberry Pi 2 Model B, has many useful features including: 900MHz quad-core ARM Cortex-A7 central processing unit (CPU), 1GB RAM, 4 USB ports, 40 general

purpose input output (GPIO) pins, full HDMI port, ethernet port, combined 3.5mm audio jack and composite video, camera interface (CSI), display interface (DSI), micro SD card slot, and videoCore IV 3D graphics core. Figure 5 shows the Raspberry Pi 2 Model B[11].

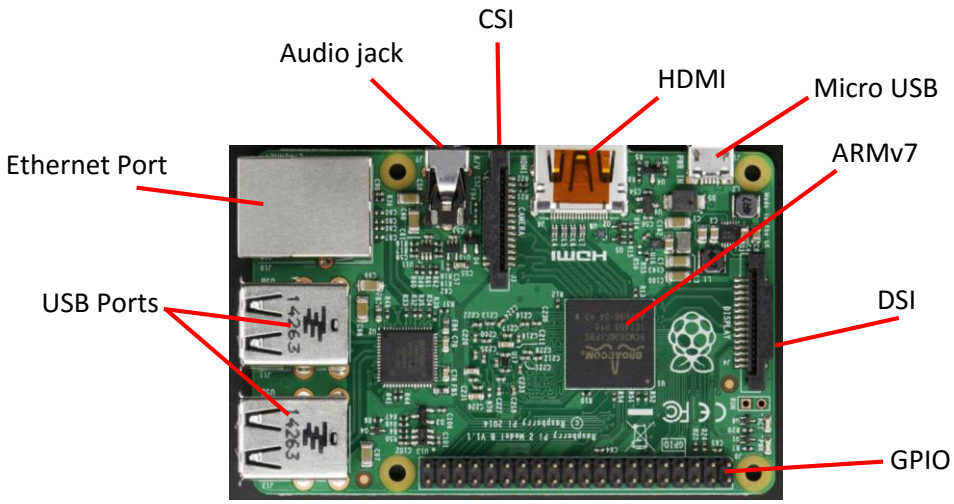

Figure 5. *The Raspberry Pi 2 Model B is shown above*[12].

The USB ports allow for a mouse, keyboard, or Wi-Fi dongle to be used. The HDMI, GPIO, and DSI gives the user options for connecting the Raspberry Pi to a display or monitor. The GPIO can be used for many other inputs or outputs in projects as well. The micro SD card slot is located on the back of the Raspberry Pi 2 Model B. This micro SD card is used for the operating system. The processor sits on top of the memory chip in order to save space. In addition, the ARM 7 processor in the newest model allows for a range of ARM Linux distributions to be used as well as an ARM version of Windows 10. The Raspberry Pi Foundation also provides a Debian-based operating system specifically for the Raspberry Pi called Raspbian[11].

The Raspberry Pi Foundation created the Raspberry Pi in hopes that it would inspire students to learn and practice programming once again[11]. Although educational programs have recognized its use in the classroom, other fields have started using them as well. Several studies have shown the usefulness of the Raspberry Pi in the field of digital forensics. In 2014, Dan Blackman reviewed the substitution of a cluster of Raspberry Pi's for a large server in Network Intrusion Detection Systems (NIDS). This study concluded that while the Raspberry Pi's processing was slower and updates had to be done individually there were many benefits to using them including substantial power savings[13]. Another study by Singh *et al.*, demonstrated two Raspberry Pi's being used for a GSM real time multiface tracking system hooked to a video surveillance camera. The system was able to give an accurate estimation of people or vehicles in a specific time frame[14]. The University of Southampton in the UK was able to create a super computer out of 64 Raspberry Pi boards and Legos[15]. It is clear that the Raspberry Pi can be used to create inexpensive devices, while still remaining efficient. The Raspberry Pi 2 Model B was chosen for this project due to its versatility, number of compatible accessories available, and large amount of online support.

Material & Methods

For this research, a Raspberry Pi Model B was used with other hardware to create an inexpensive mobile device for mobile forensic acquisition. A 3D printed model and a Pelican case model were both designed and created to show two possibilities for creating this device. Open source tools with user-friendly GUI's were examined and then modified to work with an ARM processor and the operating system Raspbian. After the device was assembled and the

software was optimized, comparison studies were performed against commercial tools to determine its usefulness to digital forensics examiners.

Hardware

Hardware for this project was purchased from easy to find sites and at affordable prices. Table 1 displays the hardware name, amount purchased, where it was purchased, and the price of each for the Pelican case models. The total price of hardware for this design was $340.71. The hardware in the Pelican Case model was assembled using plastic stand-offs, white foam board, wood, and hot glue. This provided a sturdy support for the hardware, so that it was not moving inside of the case. The hardware was connected as shown in the circuit diagram Pelican case model in Figure 6. The screen and Raspberry Pi was attached via HDMI ports. Two 270 degree HDMI adapters and one straight HDMI male to male adapter was used in order to conserve space (Figure 7). Plastic standoffs were attached to the four holes in the corners of the screen. The Raspberry Pi was placed between the battery and the board using the HDMI adapters to hold it up and foam board and cables to support it (Figure 8). All cables were organized using Velcro cord straps – however, twist-ties or glue could be used instead. The battery was glued to the board and foam board was cut and glued strategically to provide support for the screen (Figure 9). Figure 10 demonstrates using the foam board as support for the outside ports. The SD card reader extension, SD/USB port, on/off Switch, and micro USB (from battery) were all made available for use. The student desk pad was cut to the pelican case dimensions and holes were made for each outside port (Figure 11). Foam board was cut to these measurements as well and glued to the back of the pad to keep it from bending. All ports were glued in place, and after it

was allowed to dry, the whole apparatus was placed into the pelican case. The final Pelican Case model is shown in Figure 12.

Table 1. *The hardware used, where each was purchased, and price for the Pelican case model is shown below.*

Hardware	Amount	Purchased From	Price (each)
Raspberry Pi 2 Model B Project Board	1	Amazon	$39.95
SainSmart 7 inch TFT LCD 800*480 Touch Screen Display for Raspberry Pi 2 B+ B	1	Amazon	$64.99
RAVPower Portable Charger 15,000mAh External Battery Pack Power Bank	1	Amazon	$39.99
SanDisk Ultra 32GB Micro SD media card	1	Amazon	$13.99
Manufacture SD - micro SD Card Reader Extension Cable	1	Amazon	$15.97
USB 2.0 Extension Adapter Cable A to A - M/F	1	Amazon	$2.99
YCS Basics 6 inch USB Micro male to female OTG Extension Cable	1	Amazon	$5.39
Juiced Systems Microsoft Surface Pro 3 (4 in 1 Adapter) USB 3.0, SD/SDHC/MMC4.0, Micro SD/SDHC	1	Amazon	$29.99
Kootek Raspberry Pi Wifi Dongle Adapter - 150Mbps Fully Compatible USB Wifi For Raspberry Pi/Windows /Linux/Mac OS	1	Amazon	$7.99
SKmoon™ Raspberry Pi Micro USB Cable with On/Off Switch	1	Amazon	$5.99
Komingo HDMI Cable Adapters KIT HDMI 270 Degree Male to Female Angle Adapters 4 Pcs Pack	1	Amazon	$6.99
HDMI Male To Male Adapter Gold Plated	1	Amazon	$7.99
Rii Mini Wireless Keyboard with Mouse Touchpad	1	Amazon	$14.72
Slim HDMI with Ethernet Cable, 1m	1	Walmart	$16.72
Hot Glue	1	Michaels	$5.49
Wood Rectangle 6 x 5”	1	Michaels	$1.39
White Foam Board 20 x 30”	1	Office Depot	$4.39
Black Student Desk Pad	1	Office Depot	$9.99
M3 Nylon Male-female Hex Spacers Screw Nut Stand-off Plastic Assortment Kit 180 Pcs Black	1	Amazon	$7.99
Pelican 1150 Case with Foam for Camera	1	Amazon	$37.80

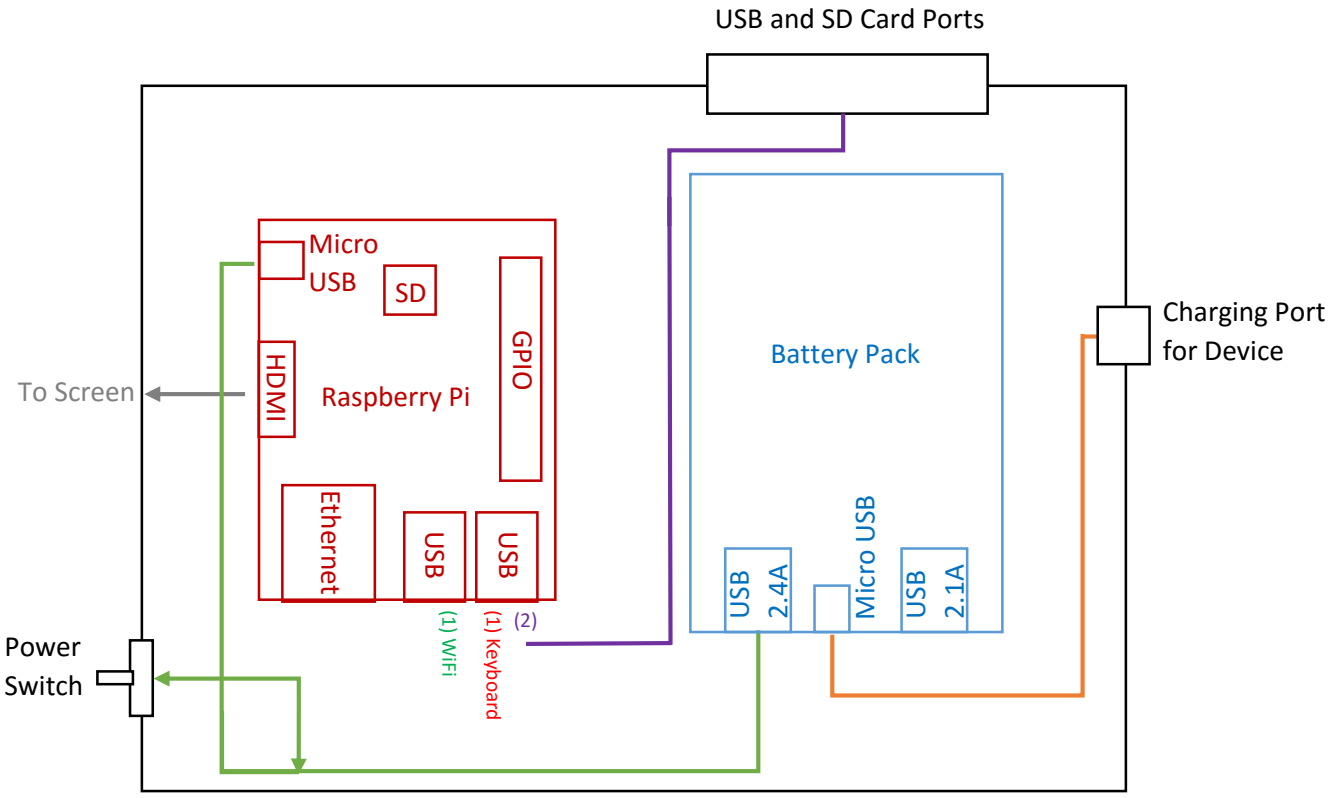

Figure 6. *The basic layout of the Pelican Case device is shown above.*

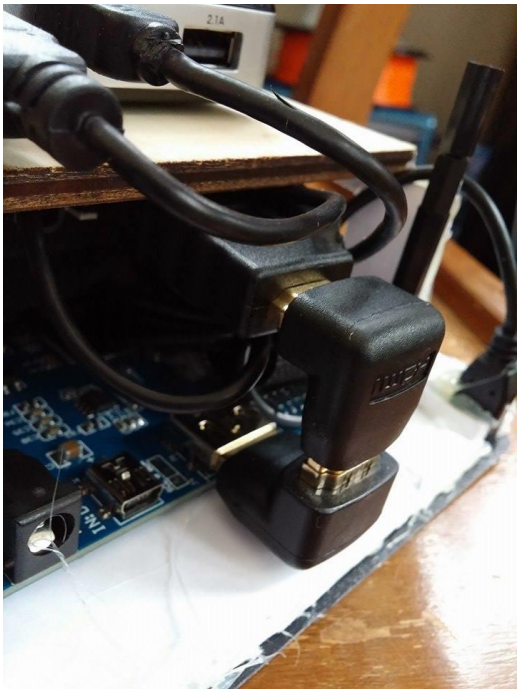

Figure 7. *The above figure demonstrates the HDMI adapters used for the screen and Raspberry Pi connection.*

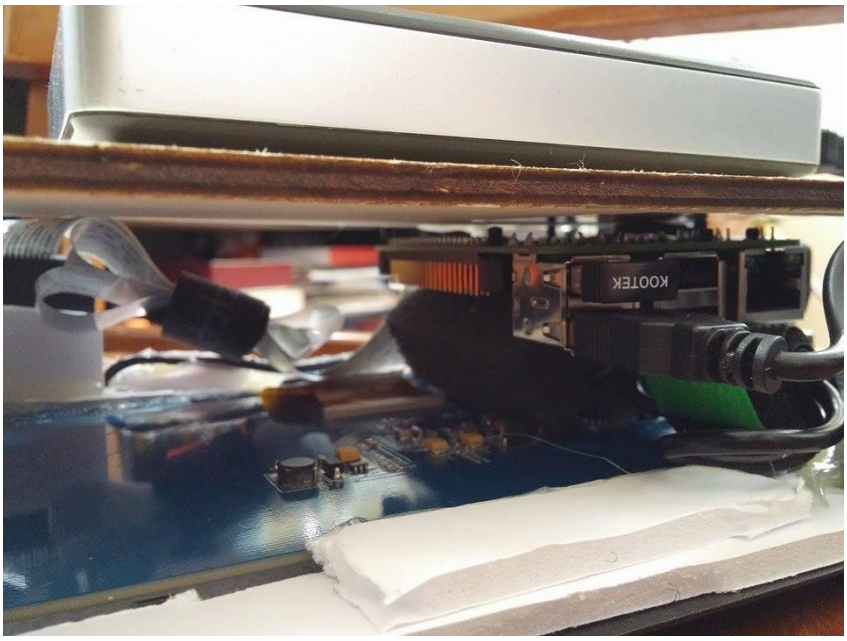

Figure 8. *The Raspberry Pi was attached to the board as shown above.*

Figure 9. *The battery was glued to the board as shown above.*

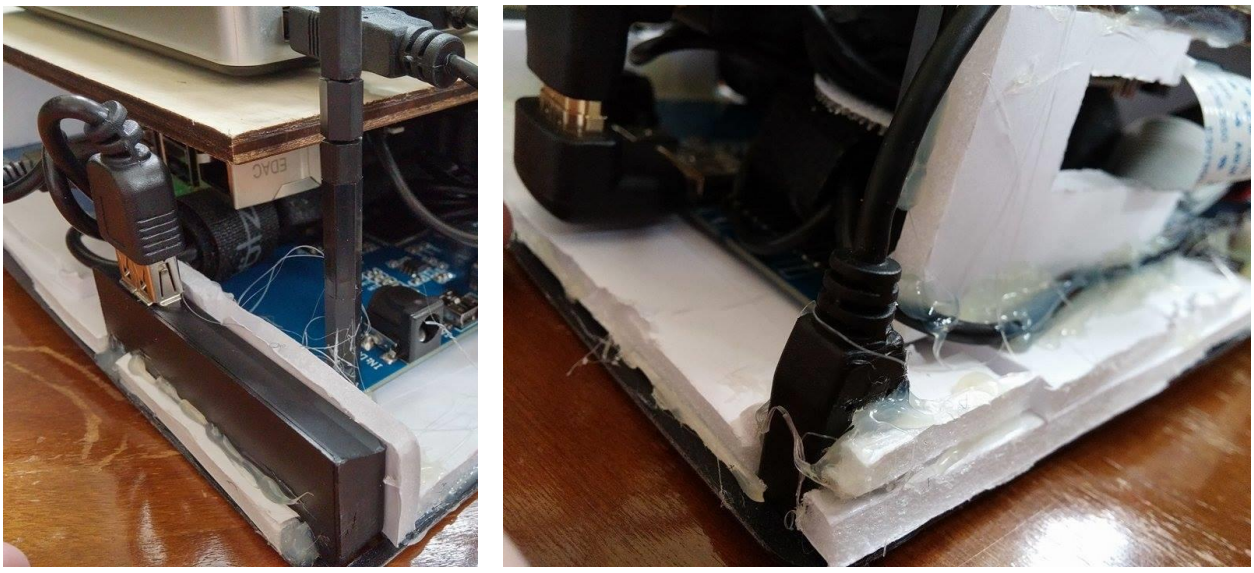

Figure 10. *The above figure shows foam board being used for support of the outside ports.*

Figure 11. *The outside ports were glued into the plastic desk pad as shown above.*

Figure 12. *The final Pelican Case model.*

The hardware, amount purchased, where it was purchased, and the price of each piece for the 3D printed case design is shown in Table 2. The total price of the hardware for this design was $267.42. AutoDesk123D was used for design of the 3D printed case. This design has been posted to http://www.thingiverse.com/thing:1190996. There are two parts to the design – one for each of the two Lithium Ion batteries, and one for the outside case. The basic circuit diagram can be found in Figure 13. Two Lithium Ion batteries were used in parallel to power the device. The batteries were placed into the 3D printed holders. Silicone cover stranded-core wire was soldered to each battery and fully insulated disconnects were used to connect the positive ends of the batteries to each other, as well as the negative ends (Figure 14). The battery wires were connected in parallel between the three-pole switch and the Powerboost 500 Charger using female disconnects. An enable wire and two jumper wires for the digital voltage meter were also connected in parallel to the three-pole switch. The enable wire, positive wire, and negative wire were then soldered to the enable (EN), battery (BAT), and ground (GND) pinouts on the Powerboost 500 Charger, respectively.

Table 2. *The hardware used, where each was purchased, and price for the 3D printed model is shown below.*

Hardware	Amount	Purchased From	Price (each)
Raspberry Pi 2 Model B Project Board	1	Amazon	$39.95
7” Pi Touchscreen LCD Display	1	MCM Electronics	$60.00
18650 3400 mAh Rechargeable Lithium Ion Battery (2 Piece)	1	Amazon	$9.99
SanDisk Ultra 32GB Micro SD media card	1	Amazon	$13.99
USB 2.0 Extension Adapter Cable A to A - M/F	1	Amazon	$2.99
YCS Basics 6 inch USB Micro male to female OTG extension cable	1	Amazon	$5.39
Juiced Systems Microsoft Surface Pro 3 (4 in 1 Adapter) USB 3.0, SD/SDHC/MMC4.0, Micro SD/SDHC	1	Amazon	$29.99
Kootek Raspberry Pi Wifi Dongle Adapter - 150Mbps Fully Compatible USB Wifi For Raspberry Pi/Windows /Linux/Mac OS	1	Amazon	$7.99
Rii Mini Wireless Keyboard with Mouse Touchpad	1	Amazon	$14.72
240 Pcs M2 M3 Brass Spacer Standoff Screw Nut Assortment Kit	1	Amazon	$20.99
Neewer Durable 2.8V-25.2V Indicator for 2S-6S LiPo Battery in RC Model	1	Amazon	$7.66
Silicone Cover Stranded-Core Wire - 2m 26AWG Green	1	Adafruit	$0.95
Silicone Cover Stranded-Core Wire - 2m 26AWG White	1	Adafruit	$0.95
Premium Female/Female Jumper Wires - 40 x 6"	1	Adafruit	$3.95
Powerboost 500 Charger	1	Adafruit	$14.95
3 Pole Marine Switch	1	AutoZone	$5.99
Fully Insulated Disconnects 0.250” (22-18G)	1	AutoZone	$5.99
¼” Female Disconnects (16-14G)	1	AutoZone	$5.99
Gorilla Glue Epoxy	1	Hobby Lobby	$5.99
PLA 3D Printed Case	1	Print Service*	$9.00

**This is a not a specified printing service. This number is based on local printing services.*

In addition, the USB was soldered to the Powerboost board in its specified location. This is shown in Figure 15. Finally, the jumper wires were attached to the digital voltmeter and battery wires were attached using insulated disconnectors. All connections are shown in Figure 16. All solder points were covered using epoxy glue, so that the stress of movement while placing the hardware in the case would not disturb the connections.

Standoffs were used to attach the Raspberry Pi to the back of the screen with the inside four holes (Figure 17). The display was connected by plugging the ribbon cable into the DSI and using jumper wires. The pinouts for the jumper wire connections are shown in Figure 18. The enclosed batteries were screwed onto the back of the case with standoffs in the outside four holes. Figure 19 shows the Raspberry Pi and batteries attached to the back of the screen. All cables and ports were connected to the Raspberry Pi as shown earlier in Figure 13. The ports were secured into the designated holes as shown in Figure 20 and the Powerboost 500 C was placed inside the designated center holder. Figure 21 shows the entire device prior to fitting the screen into place. Finally, the entire apparatus was placed into the outside case and the screen was snapped into place along the edge. Four screws were screwed through the back of the case and into the standoffs inside, which is shown in Figure 22. The final 3D printed design can be found in Figure 23.

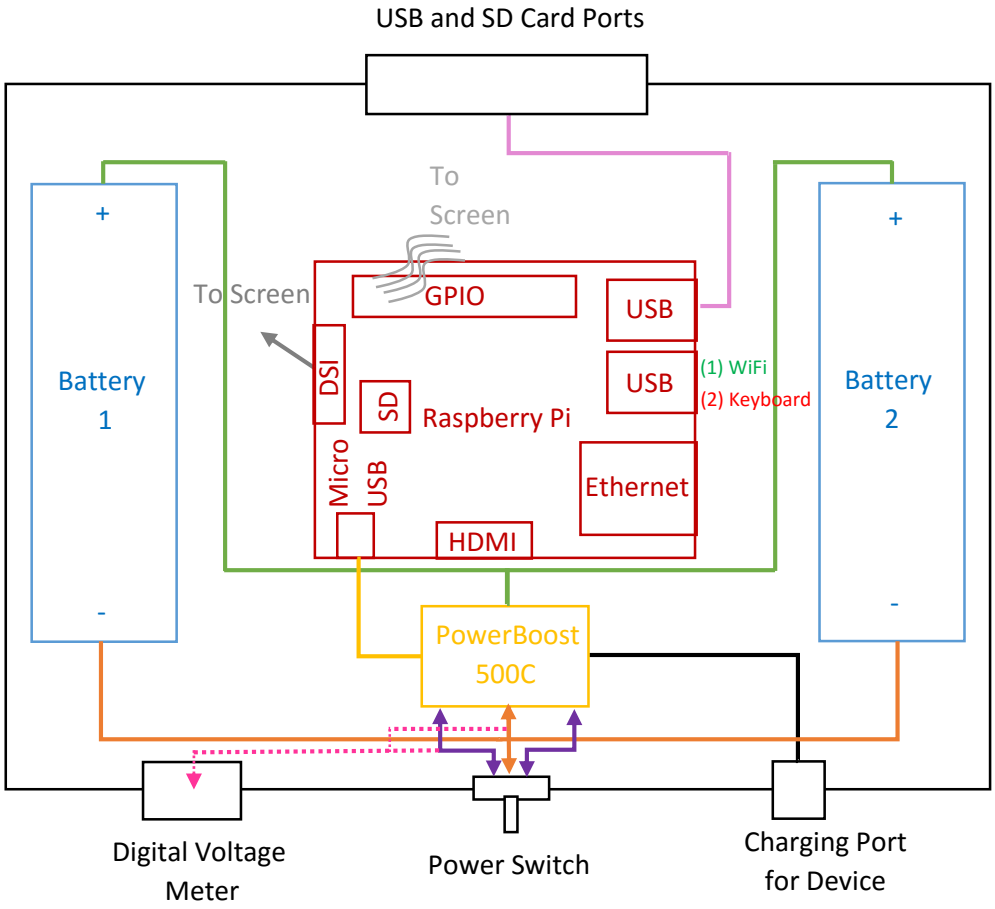

Figure 13. *The basic layout of the 3D Printed device is shown above.*

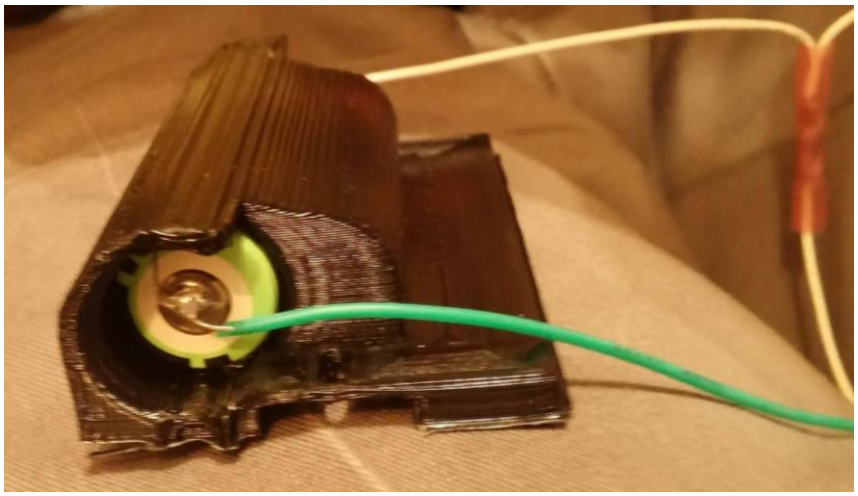

Figure 14. *Silicone cover stranded-core wires were soldered to the batteries and the positive ends of each battery were attached using insulated disconnects, as well as the negative ends.*

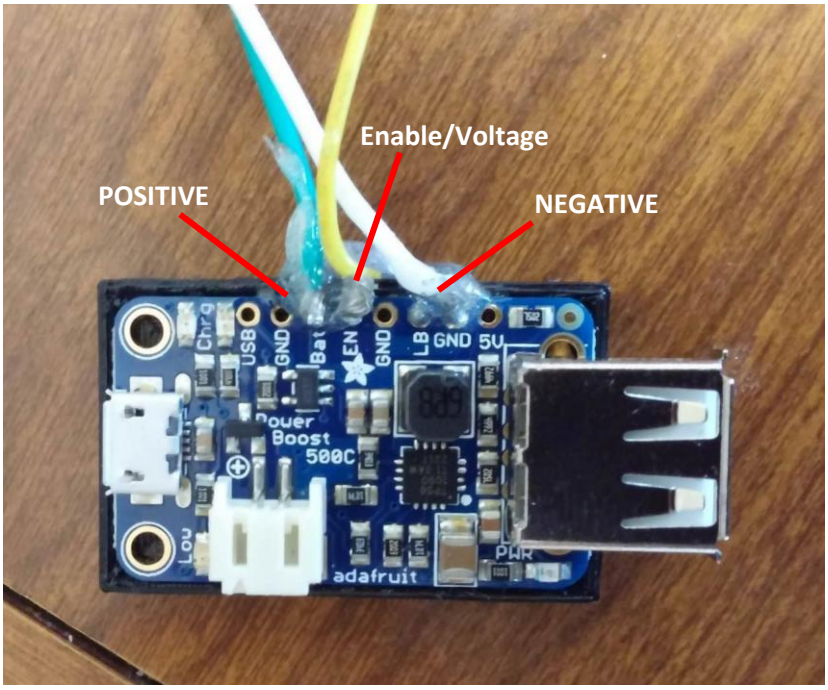

Figure 15. *The Powerboost 500 Charger pinout is shown above.*

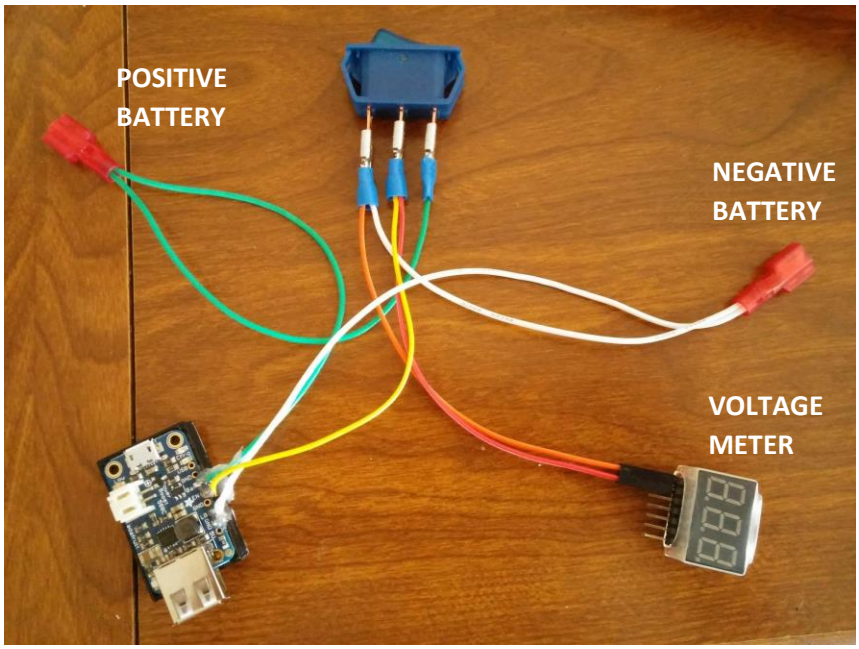

Figure 16. *The connections for power and voltage monitoring are shown above.*

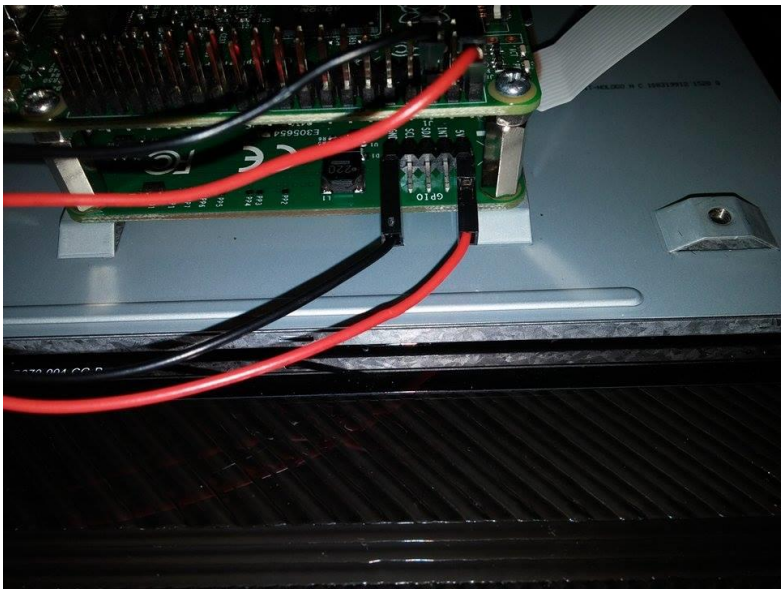

Figure 17. *Standoffs were used to connect the Raspberry Pi to the Screen.*

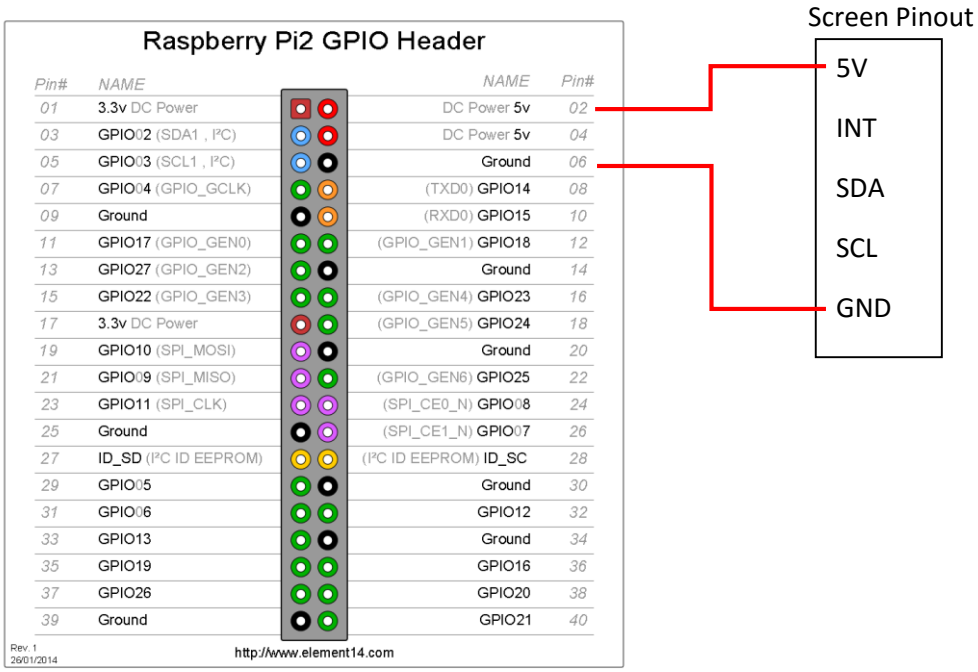

Figure 18. *The jumper wire pinout for the Raspberry Pi and screen connection.*

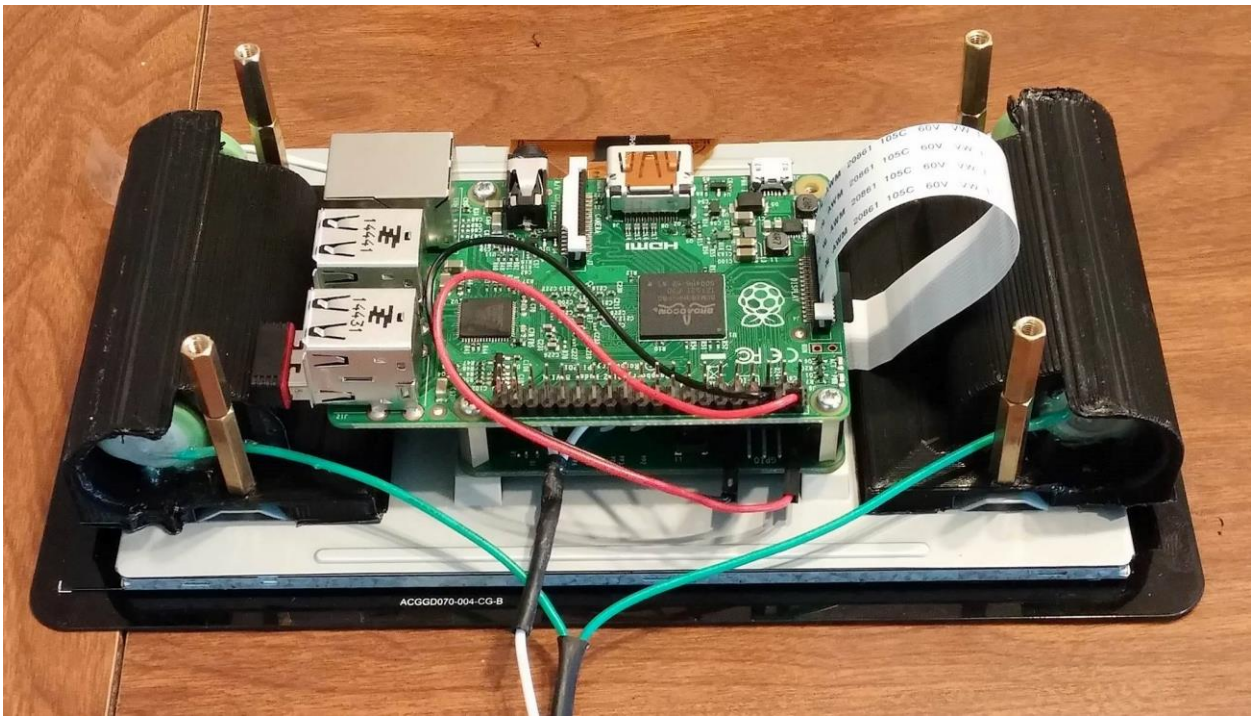

Figure 19. *The Raspberry Pi 2 and batteries were attached to the screen using standoffs as shown above.*

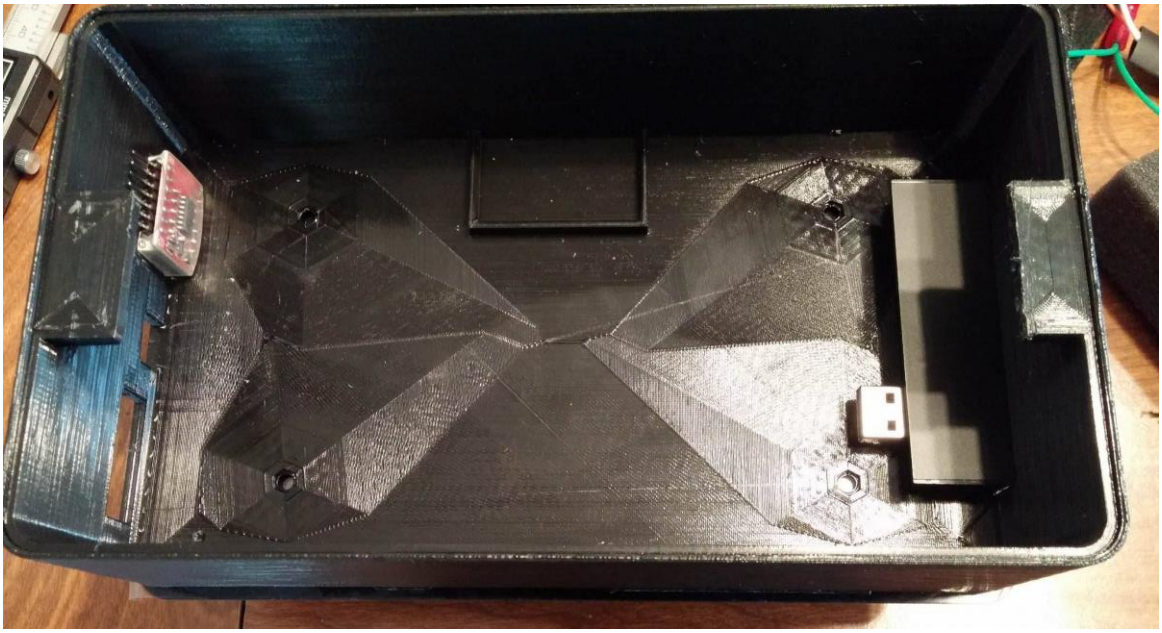

Figure 20. *The USB, SD Card, micro USB, and digital voltage meter ports were fit into the designated holes of the 3D printed case.*

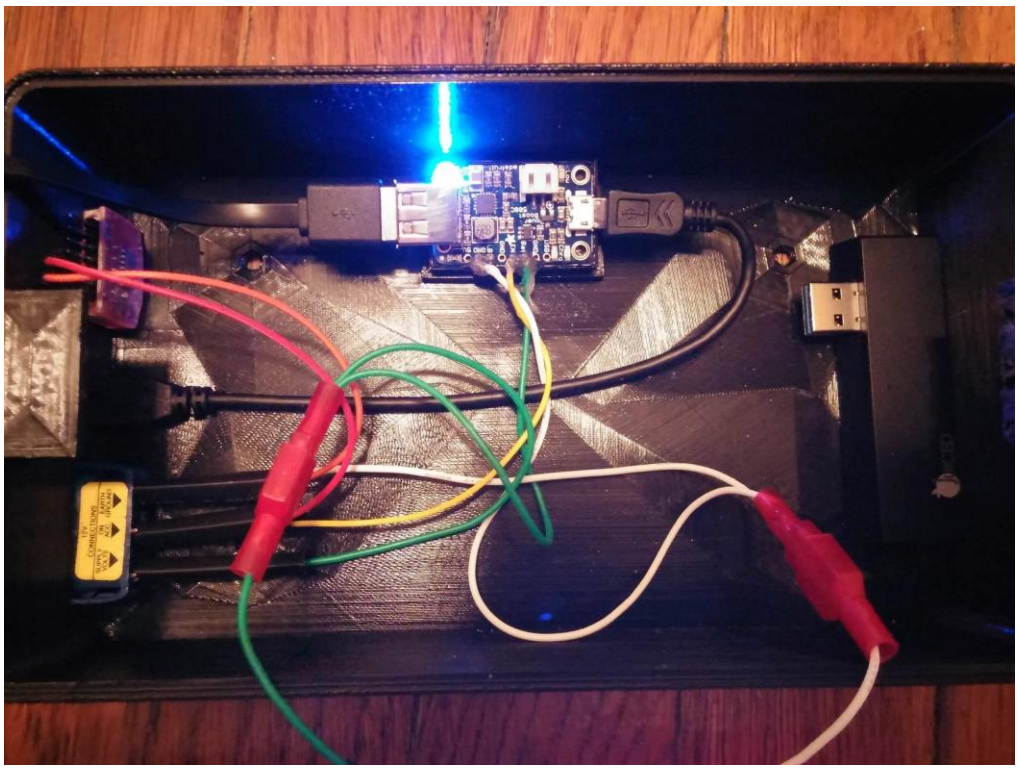

Figure 21. *The above figure shows the device and hardware prior to fitting the screen into the case.*

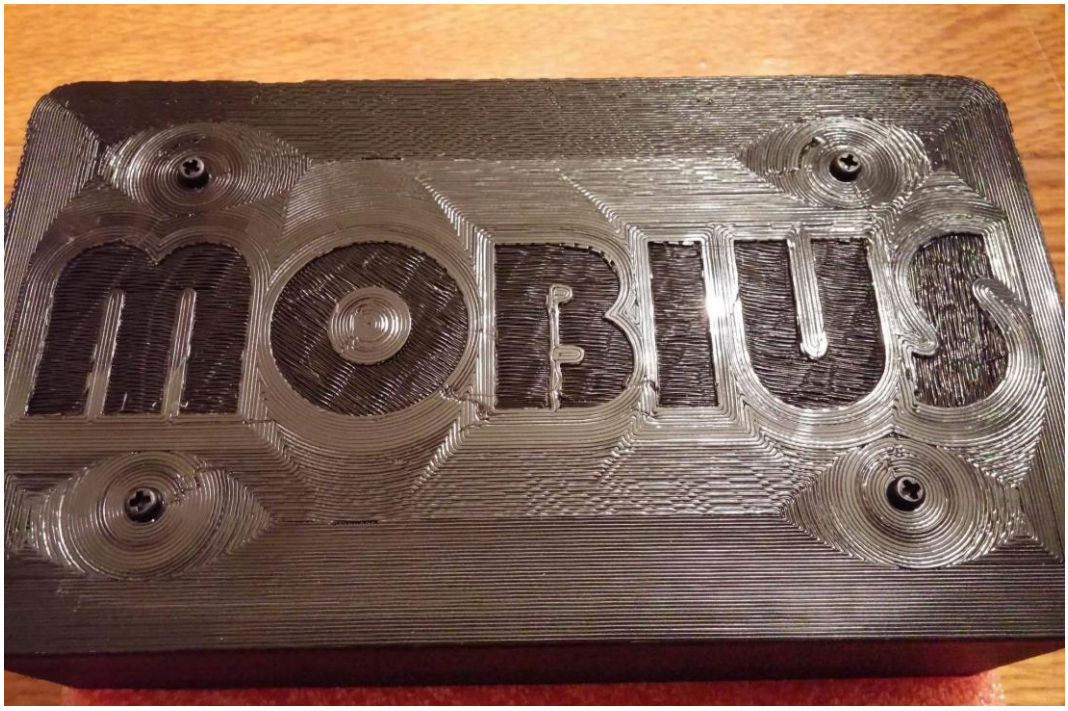

Figure 22. *Four screws were placed into the standoffs through the back of the case in order to secure the device.*

Figure 23. *The final 3D printed case design is shown above.*

Software

Several open source tools were examined and researched for use on the Raspberry Pi 2 Model B. Some tools, such as AFLogical or NowSecure Forensics had open source versions that were not available to Law Enforcement. Other open source tools, such as Oxygen Forensic Suite, have now become commercial after improvements to their product. After careful review, the two tools selected for examination were Androphsy and Open Source Android Forensics Toolkit (OSAF-TK). Androphsy had bugs in the code and could not be fixed in the time available, which left OSAF-TK for the remainder of the study. OSAF-TK, written in Java, was cross-compiled from x86 to ARM using the program Eclipse. This was completed in Ubuntu 12.04.5 LTS 64 bit desktop. The steps and commands used for this task can be found below. The original OSAF-TK source code can be found on Github.com at https://github.com/j-koenig/osaft.

Download Ubuntu 12.04.5 LTS Desktop 64 bit at:
www.ubuntu.com/download/alternative-downloads

Burn to DVD and install Ubuntu to computer OR use in VMware with large amount of memory (at least 20GB)

Update Ubuntu Tools

$ sudo apt-get update

Download and install Android SDK at: developer.android.com/sdk/index.html

Download and install Eclipse at eclipse.org

Add Android adt plugin repository in Eclipse at:
http://dl-ssl.google.com/android/eclipse

Run Android SDK manager in Eclipse

Install Eclipse c/c++ tools

$ sudo apt-get install eclipse eclipse-cdt g++ gcc

Install toolchain for arm cross compile

$ sudo apt-get install gcc-arm-linux-gnueabi

$ sudo apt-get install g++-arm-linux-gnueabi

Import project from Github

Compile using the ant build tool

Save to USB and transfer to Raspberry Pi

Comparison Studies

The ability to obtain a logical extraction was compared for the mobile forensic tools AFLogical, MOBIUS, Cellebrite, and XRY. AFLogical was chosen, because it a closed source, commercial tool with command line and Linux-based features. Although it is not available for law enforcement use, the free version of AFLogical was used for this project due to cost. Cellebrite and XRY were also chosen, because they were the commercial tools available during the time of this study.

Two Android phones were used for this comparison and the information regarding these phones can be found in Table 3. Phone 2 was purchased new from a store prior to this study. However, Phone 1 was a used phone. Before the study was performed, the SIM card was removed from Phone 1 and then the phone was factory reset. Since a logical extraction was being used for comparison, there was no concern if the factory reset only removed directory information rather than overwriting all data.

Table 3. *The hardware and software information of the two phones used in the comparison study are shown below.*

	Phone 1	**Phone 2**
Manufacturer	Motorola	LG
Series	Droid Razor M	Lucky
Model	XT907	L16C
Platform	Android	Android
OS version	4.4.2	4.4.2

The artifacts chosen for analysis were based on what Cellebrite claims a logical extraction will support, which can be seen in Figure 24. Five of each artifact chosen were deposited on both phones; this list of items is given in Table 4. Since there was no service provider for the phones and only Wi-Fi was available, two apps were used to assist with SMS and Call sending/receiving. For SMS messages, the app Fake Text Message was used; the Fake Call Logs app was used for sent, received, and missed calls. Both of these apps allow the call or SMS message to appear on the phone as if it has been sent. The only difference noticed between the app created message or call and an original one, is that they are not actually sent to another individual. For the contacts, fake numbers with area code 555 were used. Three fake Gmail accounts were set up for this study, so there was no personal information being extracted. The audio files artifacts were the ringtones already on each device, and the images were taken with the camera on the device and left on the camera roll. These precautions allowed all artifacts on both phones to be known, maintained, and controlled for the comparison study and extraction process.

The artifacts found by each tool were recorded. If all five artifacts in one category were found, the artifact category was considered as found and extracted by the tool. If however, it only found a partial number of the artifacts in one category, the artifact category was considered found but not successfully extracted. When the tool did not find any artifacts in one category, it was labeled not supported or extracted by the tool.

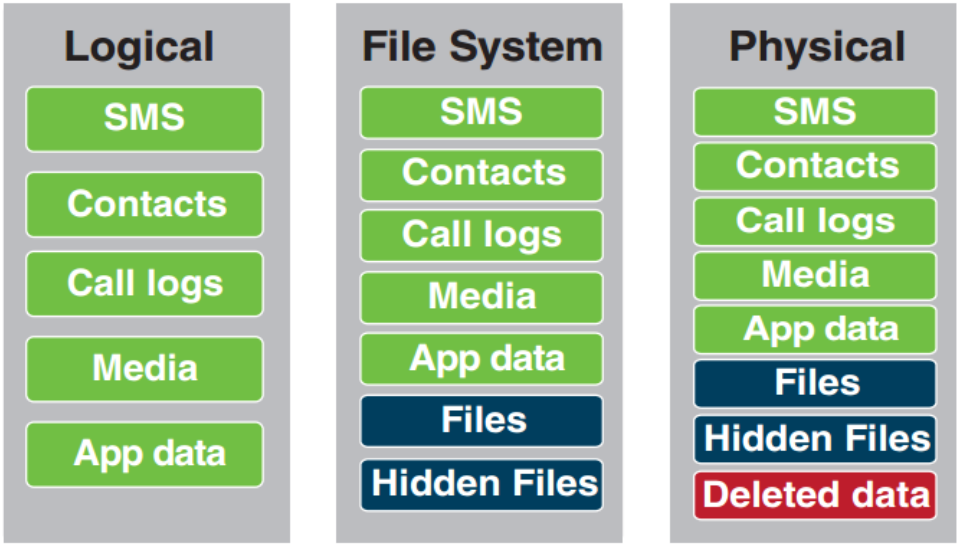

Figure 24. *Cellebrite's list of artifacts supported by each type of extraction is found above*[15].

Table 4. *Below is a list of artifact categories used for the comparison study.*

Artifacts Used for Study	
Contacts	Browser History
SMS Sent	Browser Favorites
SMS Received	Calendar Events/Appointments
Emails Sent	Audio
Emails Received	Video
Calls To	Images
Calls From	
Calls Missed	

Results

The results from the comparison study are shown in Table 5. There were no partial extractions by any tool. If a tool found and extracted an artifact, it was mark with an "X." Otherwise, the box was left blank. Cellebrite did not support the specific LG Lucky Tracphone, so a Generic Android extraction was used for the LG L16C (Phone 2) with Cellebrite. None of the mobile forensic tools extracted emails or Opera browser history/favorites. AFLogical did not obtain any media or browser history as well. XRY extracted only the media, browser history, and calendar events. MOBIUS obtained browser history when Cellebrite did not. However, it was not able to extract media, while Cellebrite found images and videos for the Motorola XT907. It is worth noting that the MOBIUS device was able to extract the same artifacts for both phones. Figure 25 shows the user-friendly GUI of the MOBIUS device.

Table 5. *The results from the comparison study are shown below.*

										History			Favorites						
Tool	Phone	Contacts	SMS Sent	SMS Rcvd	Email Sent	Email Rcvd	Calls To	Calls From	Calls Missed	Chrome	Firefox	Opera	Chrome	Firefox	Opera	Calendar	Audio	Video	Images
MOBIUS	XT907	X	X	X			X	X	X	X			X			X			
	LG L16C	X	X	X			X	X	X	*			*			X			
AFLogical	XT907		X	X			X	X	X										
	LG L16C		X	X			X	X	X										
Cellebrite	XT907	X	X	X			X	X	X							X		X	X
	LG L16C	X	X	X			X	X	X							X			
XRY	XT907													X		X	X	X	X
	LG L16C									*	X		*	X		X	X	X	X

**For the LG L16C, the history and bookmarks found were from the browser that originally came with the phone.*

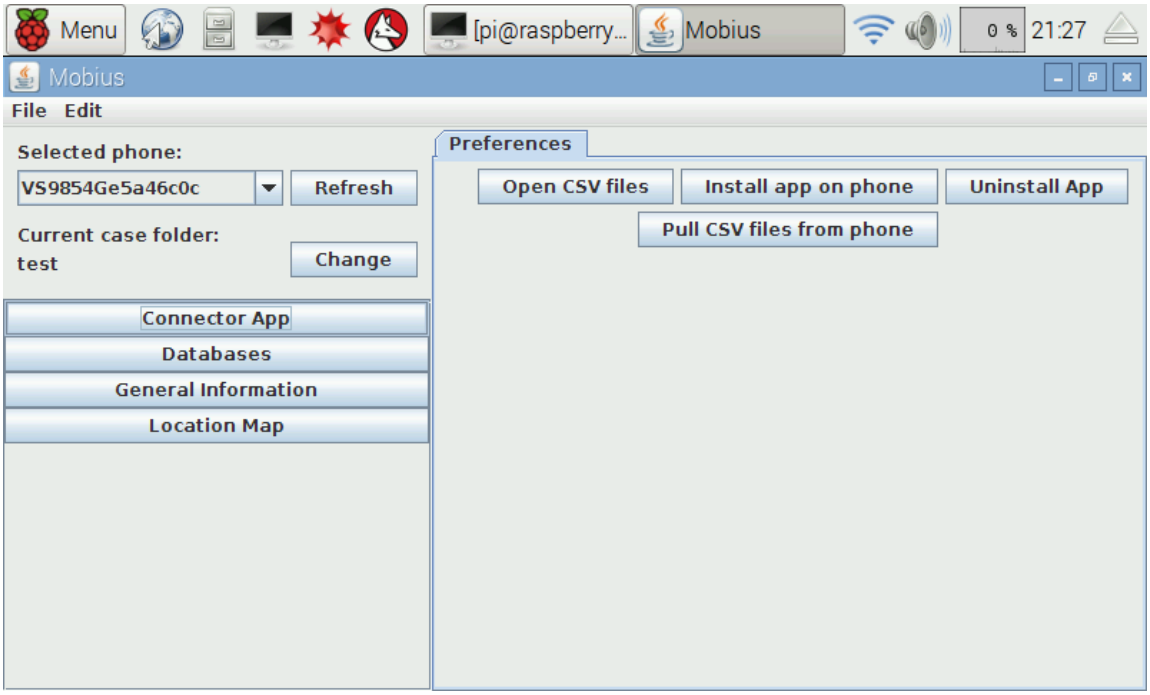

Figure 25. *The user-friendly GUI on the MOBIUS device is shown above.*

Conclusions

This research examined if a portable, inexpensive device could be created for use with open source tools and if a user-friendly open source tool could be cross-compiled to work on a Raspberry Pi for logical extractions. Two simple, inexpensive devices were created for use with a Raspberry Pi. Both of these devices were portable and produced for about $300. In addition, OSAF-TK was successfully cross-compiled to ARM using Eclipse. This tool provided an easy-to-use GUI with simple steps to follow. During the comparison study, the logical extraction produced by MOBIUS was comparable to those of commercial tools. In comparison to Cellebrite, MOBIUS was able to extract default browser information, but could not extract the media on either device. MOBIUS was also able to extract the same artifacts for both the Motorola XT907 and LG L16C phones. The general extraction used by this tool allows it to be reliable for numerous phones and operating system versions.

For future studies, the mobile forensic tool compiled could be improved to find media and emails. In addition, open source tools that support iOS extraction should be considered for use with the MOBIUS device. It would also be beneficial to expand the comparison study to other mobile phones and Android operating system versions. Although there is much to improve on, the use of open source tools for mobile phone forensic acquisition is becoming a possibility. With the benefit of having access to the source code, it may be advantageous for forensic examiners to use open source tools rather than proprietary commercial tools. The source code allows examiners to know exactly what is occurring and how, as well as present the program and source code in court during testimony. According to Daubert, the tools used by examiners must be tested, and open source tools allow this to occur[10]. With further research and continued

development of mobile phone forensic tools and GUI's, open source tools may prove to be a useful addition to digital forensic examiners' toolkit in the near future.

Acknowledgements

Special thanks to Nick Zimniski for advisement on 3D modeling and printing with the ROBO 3D™ printer, as well as assistance with cross compiling of open source tools. The author thanks the Marshall University Forensic Science Graduate Program and its entire faculty, including Dr. Pamela Staton, Dr. Terry Fenger, Ian Levstein, and Joshua Brunty for their review and advisement. Additionally, the author thanks Corporal Boggs and Dale Mosley from the West Virginia State Police Digital Forensics Unit for their expertise and support of this project.

References

1. Palmer, G. A Road Map for Digital Forensic Research. First Digital Forensics Research Workshop; 2001 Nov 6. DFRWS Technical Report No.: DTR – T001-01.
2. Pew Research Center. Mobile Technology Fact Sheet. <http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/>.
3. Stroud M. In Boston Bombing, Flood of Digital Evidence is a Blessing and a Curse. CNN 2013 Apr 18. < http://www.cnn.com/2013/04/17/tech/mobile/boston-bombing-evidence-search-verge/>.
4. Ayers R, Brothers S, Jansen W. Guidelines on Mobile Device Forensics. National Institute of Standards and Technology, U.S. Department of Commerce; 2014 May. NIST Special Publication 800-101 Revision 1.
5. Hi-tech News. 12 Oct 2013. <http://raqwe.blogspot.com/2013/10/iphone-6-will-receive-magnetic-slot-for.html>.
6. Mahalik H. Open Source Mobile Device Forensics. Proceedings of the NIST Mobile Forensics Workshop and Webcast; 2014 May 7; Gaithersburg, MD.
7. Open Source Initiative. The Open Source Definition. <http://opensource.org/osd>.
8. Altheide C, Carvey H. Digital Forensics with Open Source Tools. Massachusetts: Elsevier Science, 2011.
9. Carrier B. Open Source Digital Forensics Tools: The Legal Argument. Stake, Inc; 2002 Oct. Research Report.
10. Daubert v. Merrell Dow Pharmaceuticals (92-102), 509 U.S. 579 (1993). <https://www.law.cornell.edu/supct/html/92-102.ZS.html>.
11. The Raspberry Pi Foundation. <https://www.raspberrypi.org/>.

12. Adafruit. Raspberry Pi 2 Model B - ARMv7 with 1G RAM. <http://www.adafruit.com/products/2358?gclid=CjwKEAjw8NaxBRDhiafRuvkpywSJAAxcl6fwPOCIFQ6gBnkBA2Jstw4IF_wgy1sCpcR MISta8A2VhoCvsPw_wcB>
13. Blackman, D. Rapid forensic crime scene analysis using inexpensive sensors. Proceedings of the Twelfth Australian Digital Forensics Conference. 2014 Dec 1-3; Perth, Western Australia: Edith Cowan University, Joondalup Campus.
14. Singh TR, Kumar SB, Patil MS. GSM Based Real Time Multiface Tracking System With Visual Surveillance Camera. IJEEC 2014 Oct;6(20):411-5.
15. Harris, G. Southampton engineers a Raspberry Pi Supercomputer. 11 Sept 2012. <http://www.southampton.ac.uk/~sjc/raspberrypi/Raspberry_Pi_supercomputer_11Sept2012.pdf>
16. 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. Vijayan V. Android Forensic Capability and Evaluation of Extraction Tools [dissertation]. Edinburgh (UK): Edinburgh Napier University, 2012.
18. Grispos G, Storer T, Glisson WB. A comparison of forensic evidence recovery techniques for a windows mobile smart phone. Digital Investigation 2011;8:23-36.
19. Segall B. Cell phone warning: Deleted personal information often left behind. WTHR 2014 Mar 11 <http://www.wthr.com/story/21419450/cell-phone-warning-deleted-personal-information-often-left-behind>