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

Kelsey Wilkinson, B.S.[1]; Corporal Robert J. Boggs[2]; Joshua Brunty, M.S.[1]; Terry Fenger, Ph.D.[1]

[1] *Marshall University Forensic Science Center, 1401 Forensic Science Drive, Huntington, WV 25701*

[2] *West Virginia State Police Digital Forensics Unit, 1401 Forensic Science Drive, Huntington, WV 25701*

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, may not support every tool, and have proprietary code. Open source tools are free and available to everyone; there is no need for licensing fees each year, which can cost a lab thousands of dollars. A simple device was developed for under $300, utilizing both a 3D printed case and a small pelican case design. A ROBO 3D™ printer was used for the 3D printed version. The Raspberry Pi 2 Model B board was used for the processing unit. The Debian-based operating system Raspbian was loaded onto the micro SD card, and several open source tools with easy-to-use graphic user interfaces (GUI's) were tested for use with the device. Open Source Android Forensics Toolkit (OSAF-TK) was cross-compiled and run on the Raspberry Pi. This open source tool was then compared to commercial tools for Android operating systems. OSAF-TK and the portable devices developed for about $300 named MOBIUS were comparable to other commercial tools. 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' toolkits in the near future.

Introduction

Mobile devices have been growing in popularity and thus becoming increasingly common as evidence. Commercial tools such as UFED, XRY, MPE+, Tarantula, and Oxygen Forensic Suite are used to extract and analyze the information on mobile devices. However, these devices are expensive and have many disadvantages. Open source tools are free tools that provide the source code with the program, which can allow examiner's to troubleshoot and optimize their own tools. The source code could also be provided in court testimony.

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, single board 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.

Materials & Methods

Hardware was purchased from stores that would be easy for individuals to access, such as Amazon or Wal-Mart. The devices were designed and assembled using a Raspberry Pi 2 Model B, hardware, and either a Pelican case or a 3D printed case. Autodesk 123D software was used to design the 3D printed case, and a ROBO 3D printer was used to print the case. The design of the printed case was uploaded to https://www.thingiverse.com/thing:1190996.

Open source tools were researched and Open Source Android Forensics Toolkit (OSAF-TK) was chosen for use with the device. OSAF-TK allows for logical mobile phone acquisition of Android phones. This tool was cross-compiled from x86 to ARM for the Raspberry Pi processor and loaded onto the micro SD card along with the operating system Raspbian. The complete devices along with software and hardware were named MOBIUS.

A comparison study was performed to compare MOBIUS, AFLogical, Cellebrite, and XRY. The artifacts used for this study were SMS, MMS, call logs, contacts, email, browser history/favorites, calendar events, audio files, images, and videos. Two phones with Android operating systems version 4.4.2 were used for the study, a Motorola Droid Razor M (XT907) and an LG Lucky (L16C). Once all data was loaded onto each phone, they were placed into airplane mode to preserve the information. Each phone was extracted using the acquisition tools and the reports and results were analyzed.

Results

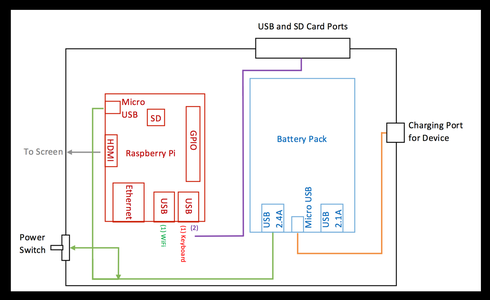

Figure 1. Pelican case device hardware diagram

Figure 2. Final Pelican case device

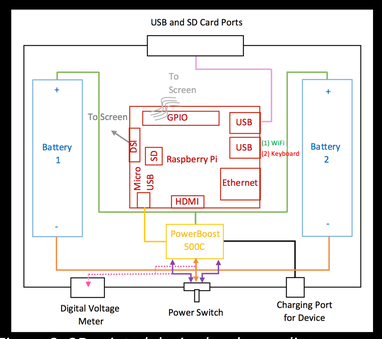

Figure 3. 3D printed device hardware diagram

Figure 4. Final 3D printed device

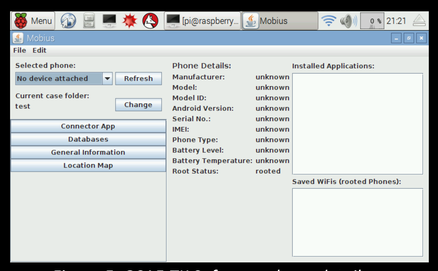

Figure 5. OSAF-TK Software phone details

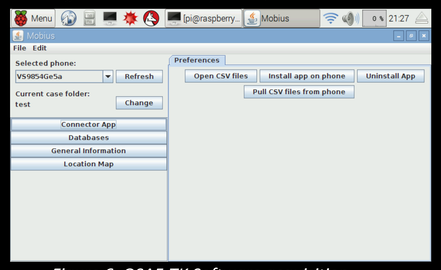

Figure 6. OSAF-TK Software acquisition

Table 1. The results from the comparison study

											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 came with phone originally.*

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 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 in the future as the Digital Forensics field continues to grow and develop.

References

Adafruit. Raspberry Pi 2 Model B - ARMv7 with 1G RAM. <http://www.adafruit.com/products/2358?gclid=CjwKEAjw8NaxBRDhiafRuvkpywSJAAxcl6fwPOCIFQ6gBnkBA2Jstw4IF_wgy1sCpcRMISta8A2VhoCvsPw_wcB>

Altheide C, Carvey H. Digital Forensics with Open Source Tools. Massachusetts: Elsevier Science, 2011.

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.

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.

Carrier B. Open Source Digital Forensics Tools: The Legal Argument. Stake, Inc; 2002 Oct. Research Report.

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>

Daubert v. Merrell Dow Pharmaceuticals (92-102), 509 U.S. 579 (1993). <https://www.law.cornell.edu/supct/html/92-102.ZS.html>.

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.

Harris, G. Southampton engineers a Raspberry Pi Supercomputer. 11 Sept 2012. <http://www.southampton.ac.uk/~sjc/raspberrypi/Raspberry_Pi_supercomputer_11Sept2012.pdf>

Hi-tech News. 12 Oct 2013. <http://raqwe.blogspot.com/2013/10/iphone-6-will-receive-magnetic-slot-for.html>.

Mahalik H. Open Source Mobile Device Forensics. Proceedings of the NIST Mobile Forensics Workshop and Webcast; 2014 May 7; Gaithersburg, MD.

Open Source Initiative. The Open Source Definition. <http://opensource.org/osd>.

Palmer, G. A Road Map for Digital Forensic Research. First Digital Forensics Research Workshop; 2001 Nov 6. DFRWS Technical Report No.: DTR – T001-01.

Pew Research Center. Mobile Technology Fact Sheet. <http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/>.

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>

Singh TR, Kumar SB, Patil MS. Gsm Based Real Time Multiface Tracking System With Visual Surveillance Camera. IJEEC 2014 Oct;6(20):411-5.

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/>.

The Raspberry Pi Foundation. <https://www.raspberrypi.org/>.

Vijayan V. Android Forensic Capability and Evaluation of Extraction Tools [dissertation]. Edinburgh (UK): Edinburgh Napier University, 2012.

Acknowledgements

Special thanks to Nick Zimniski for advice 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 advice. 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.