C9 Development of a Portable Mobile Phone Forensic Acquisition and Analysis Toolkit Utilizing Open Source Tools

Kelsey L. Wilkinson, BS, 1024 8th Street, Apt 5, Huntington, WV 25701; Robert J. Boggs, West Virginia State Police Digital Forensics Unit, 1401 Forensic Science Drive, Huntington, WV 25701; Joshua L. Brunty, MS*, Marshall University, 1 John Marshall Drive, Huntington, WV 25755; and Terry Fenger, PhD, 1401 Forensic Science Drive, Huntington, WV 25701*

After attending this presentation, attendees will understand the usefulness of a Raspberry Pi™ and open source tools for mobile phone acquisition and how to assemble a portable device using these tools.

This presentation will impact the forensic science community by demonstrating the possibility and effectiveness of analyzing mobile phones in a simple and affordable way. Using open source tools and a Raspberry Pi™ allows individuals to modify the device for their specific needs.

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-sized 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.[1] Many forensics applications of this device have developed over the years as well, including penetration testing, surveillance, and network forensics.[2,3] 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 laboratories.

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, 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. With open source tools, the source code can be presented during trial.[4,5] A noted disadvantage of many open source tools is the use of the command prompt; however, some open source tools have added user-friendly Graphical User Interfaces (GUIs), such as Autopsy® (for Sleuth Kit®) or Development Environment For Tutorials (DEFT).

A simple device was developed for less than 300 dollars, utilizing both a 3D printed case and a small pelican case design. A ROBO 3D™ printer was utilized for the 3D printed version. An ARM7™-compatible operating system was loaded onto the Secure Digital (SD) card, and several open source tools with easy-to-use GUIs were tested for use with the device. Chosen open source tools were then compared to commercial tools for both Android™ and iOS® operating systems. The design, items, and development of the operating system used to create this device will be discussed in this presentation, as well as the results found during comparison studies. With further research and continued development of mobile phone forensic tools and GUIs, open source tools may prove to be a useful addition to digital forensic examiners' toolkits in the near future.

Reference(s):

1. The Raspberry Pi Foundation. <https://www.raspberrypi.org/>.
2. 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.
3. Singh T.R., Kumar S.B., Patil M.S. GSM based real time multiface tracking system with visual surveillance camera. *IJEEC* 2014 Oct;201(6):411-15.
4. Altheide C., Carvey H. *Digital Forensics with Open Source Tools*. Amsterdam: Syngress, 2011.
5. 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.

Open Source, Mobile Device Forensics, Raspberry Pi™

*Presenting Author