C19 A Comparison of Computer Forensic Tools: An Open-Source Evaluation

Adam Cervellone, BS, 611 22nd Street, Apt 323, Huntington, WV 25703; Robert Price, MS, North Carolina State Crime Laboratory, 121 E Tryon Road, Raleigh, NC 27601; 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 better understand the capabilities of EnCase® Forensic 6, FTK® 5.6, and the SANS Investigative Forensic Toolkit (SIFT) Workstation 3.0, as well as learning if the SIFT Workstation 3.0 could be used as a viable forensic tool in a laboratory setting.

This presentation will impact the forensic science community by providing a clear and concise breakdown of the capabilities of the leading industry standard tools as well as a popular open-source tool. Very little documented research has been conducted comparing an open-source forensic tool with the industry standard tools; as such, this presentation will add to the research and hopefully encourage other studies.

The world of digital forensics is an ever-evolving field with multiple tools for analysis from which to choose. Many of these tools have very focused functions such as Mac® and iOS® device analysis registry examination, steganography analysis, mobile device examination, password recovery and countless others. Other tools are full-featured suites capable of analyzing a large case with multiple items.[1] The major problem with many of these tools is cost.[2] While they may be robust, they may not be affordable for a smaller laboratory that wants to engage in digital forensics.[3] This research focuses on industry standard forensic software such as: Guidance Software EnCase® Forensic 6, AccessData FTK® 5 as well as SANS' SIFT Workstation 3.0.[4-6] The SIFT Workstation is a freely available open-source processing environment that contains multiple tools with similar functionality to EnCase® and FTK®.[6] This study evaluates the processing and analysis capabilities of each tool. In addition to processing functionality, two other studies were conducted. The first is a virtualization study focusing on the ability of the software to create or help create a virtual machine from an E01 evidence file. The advent of cloud computing would make this an advantageous procedure in digital forensics.[3] The second is a simple cost analysis study. This portion of the research displayed how much a laboratory may have to spend to get a single examiner fully on-line with each tool. While comparison studies between commercially available software have been conducted and published, research comparing industry standard tools with an open-source tool is not well documented.[1]

For this study, mock test cases were created using North Carolina State Crime Laboratory (NCSCL) Mac® Minis and Dell® Latitude D810 laptops. The hard drives contained in these devices were hashed and imaged via EnCase® Forensic 6.19 and fully processed according to NCSCL guidelines in EnCase® Forensic 6.19, FTK® 5.6.3, and the SIFT Workstation 3.0. In addition to evaluating analysis, the tools were also evaluated based on their ability to create a virtual machine from the evidence file as well as on overall cost for a single examiner.[7-9]

This research has shown that the SIFT workstation is a viable option to use as a forensic tool, from a financial and functionality perspective. Its capabilities are vast and are similar to those of FTK® and EnCase® Forensic; however, due to its open-source nature and heavy reliance on the Linux® Terminal and command line, it is advised that only examiners highly skilled in Linux® use the SIFT Workstation for casework in order to maintain its viability.

*Presenting Author

Reference(s):

1. Kröger K., Creutzburg R. A practical overview and comparison of certain commercial forensic software tools for processing large-scale digital investigations. *Proceedings SPIE* Volume 8755, Mobile Multimedia/Image Processing, Security, and Applications May 2013; 875519.
2. Garfinkel S.L. Digital forensics research: The next 10 years. *Digital Investigation* 2010; 7:64-73.
3. Hawthorne E.K., Shumba R.K. Teaching Digital Forensics and Cyber Investigations Online: Our Experiences. *European Scientific Journal* Sept 2014; Special (2): 255-261.
4. https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx?cmpid=nav.
5. http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk.
6. http://digital-forensics.sans.org/community/downloads.
7. http://forensicswiki.org/wiki/Virtual_machine.
8. Lesson 14-EnCase® Physical Disk Emulator (PDE) Module. In: *Guidance Software*. EnCase® Computer Forensics II. Pasadena: 2014; 173-185.
9. http://www.securityisfun.net/2014/06/booting-up-evidence-e01-image-using.html.

EnCase® Forensic, FTK®, SIFT Workstation