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

Adam Cervellone, B.S.[1]; Robert Price, M.S.[2]; Josh Brunty, M.S.[1]; Terry Fenger, Ph.D.[1]

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

[2]North Carolina State Crime Laboratory, 121 E. Tryon Road, Raleigh, NC 27603

## Abstract

The realm of digital forensics is full of vetted industry standard tools such as Guidance Software® EnCase® and AccessData® Forensic Toolkit®(FTK®). While these tools are great at what they do, open source tools are becoming more commonplace in the field and need to be evaluated. The research describes an evaluation of the capabilities of EnCase® Forensic 6.19 and FTK® 5.6.3 and compares them to the SANS Investigative Forensic Toolkit (SIFT) Workstation 3.0. The SIFT Workstation is a Linux based forensic operating system (OS) with the ability to process a case in a fashion similar to the industry standard tools. The research found that the SIFT Workstation is a viable tool for a digital forensics environment both in terms of cost and functionality. This viability does come with a learning curve.

## Introduction

The world of computer or digital forensics has many capable tools that can analyze evidence. These tools, mostly proprietary, range from single function tools such as AccessData® Registry Viewer all the way to full featured case processing software suites such as Guidance Software® EnCase® Forensic or AccessData® Forensic Toolkit® (FTK). These tools and others like them have become industry standards. They have been vetted and are now trusted to handle evidence in a forensically sound manner.

As stated above, these industry standard tools are mostly proprietary and as such can be costly and fixed in overall functionality. As the nature of evidence changes, the abilities and needs of examiner changes and budgets for labs become limiting, so tools of the open source variety need to be vetted. These tools are often freely available, modular and are far more customizable than the industry standard tools . They are also often “lightweight” compared to the industry standard tools.

The project described serves as a comparison between EnCase® Forensic 6.19, FTK® 5.6.3 and the SANS Investigative Forensic Toolkit (SIFT) Workstation 3.0.

## Research Questions

- Can the SIFT Workstation hash and image an evidence item in a forensically sound manner?
- How does the SIFT Workstation compare as a case processor to industry standard tools?
- Is SIFT a viable option as a forensic tool in terms of cost and functionality when compared to industry standard tools?

## Materials

- Forensic Computers™ Forensic Tower II
- Forensic Computers™ Forensic Tower III
- Guidance Software® EnCase® Forensic 6.19.7.2
- AccessData® FTK® 5.6.3
- SIFT™ Workstation 3.0
- Apple® Mac® Mini A1283
- Dell® Latitude® D810
- 1TB SATA Hard drive
- FireWire cable
- VMware Player 7 Free
- Oracle VirtualBox 5.0

## Methods

- Verification hashing and imaging
- Evidence hashing and imaging
- Case processing
- Virtualization
- Cost Analysis

## Processing Results

EnCase® Forensic 6.19

- Test Case 1 and 2
  - Successfully verified the hash value of a known flash drive
  - Successfully hashed both evidence drives from both cases
  - Created E01 image for all evidence
  - Able to handle pictures but not cached pictures
  - Handles desktop mail but not webmail
  - HTML reports

FTK® 5.6.3

- Test Case 1 and 2
  - Successfully verified the hash value of a known flash drive
  - Verified the hash value computed for evidence drives images
  - Handles cached pictures in addition to all expected pictures
  - Handles desktop mail but not webmail
  - HTML and PDF reports

SIFT 3.0 – Libewf tools and Autopsy 2.24

- Test Case 1 and 2
  - Libewf tools successfully imaged and verified the hash value of a known flash drive (Figure 1)
  - EWFverify successfully verified the hash value of a mock evidence drive (Figure 2)
  - Autopsy acted as an effective case processor (Figure 3)

## Processing Results

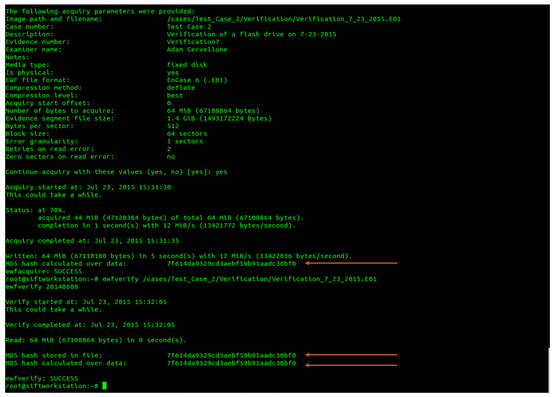


Figure 1: Libewf tools acquisition and verification of reference drive

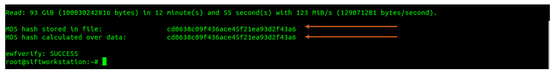


Figure 2: EWFverify successfully verified the hash value of a mock evidence item

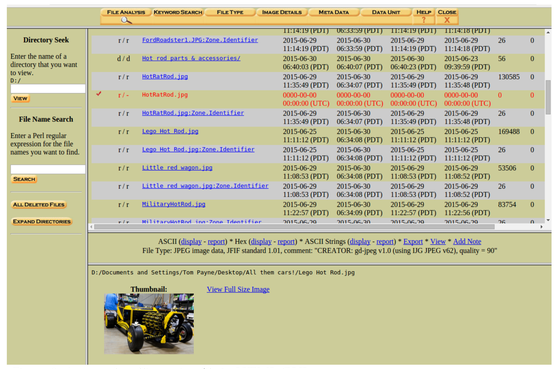


Figure 3: Autopsy handling a .jpg file in HTML GUI

## Virtualization Results

EnCase® Forensic 6.19 using Physical Disk Emulator (PDE) and LiveView .07b

- Failure due to network restrictions on forensic towers

EnCase® Forensic 6.19 using PDE and Virtual Box 5.0

- Failure, likely due to incompatibility between PDE and Virtual Box

FTK® 5.6.3 using Virtual Box 5.0

- Test Case 1 – OS X 10.5: Failure to boot due to lack of support for OS X 10.5 in Virtual Box
- Test Case 2 – Windows XP: Successful Boot, failure to activate Windows XP

SIFT Workstation 3.0

- Failure to use QEMU created vmdk file in Virtual Box

## Cost Analysis Results

| Software Tool | Single license cost (USD) | Support & Maintenance (USD) | Certification Available | Certification Cost (USD) | Training Cost (USD) | Total Cost for single examiner |
|---|---|---|---|---|---|---|
| EnCase® Forensic 6.19 | $2,995 | $599/year | EnCE® | $300 | $2,195 for EnCase 1 & 2 online | $8,284 |
| | | | | | $2,750 per course at training center | $9,394 |
| FTK® 5.6.3 | $3,995 | $1,119/year | ACE® | $0 | $2,495 for 3 day boot camp | $7,609 |
| | | | | | $4,990 for boot camp and ACE prep | $10,104 |
| | | | | | $7,000 for 1 year unlimited training pass | $12,114 |
| SIFT 3.0 | $0 | $0 | GCFE from GIAC | $629 | $5,350 for FOR508 + shipping and handling | $5,979 + shipping and handling |

## Conclusion

The research has shown that the SIFT Workstation 3.0 is a viable tool in a forensic environment. While the Linux environment presents its own challenges that some examiners may not be used to, these can be overcome by encouraging examiners to learn the command line interface and a different operating system.

In order to use SIFT in a forensic environment, an examiner competent in Linux should write a Best Practices or Standard Operating Procedure (SOP) that is comparable to similar documents used in EnCase, FTK or any other commercial forensic tool.

## References

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

## Acknowledgements

I thank Robert Price, Josh Brunty, and Dr. Terry Fenger for acting as reviewers on this project. In addition, I thank Jim Trevillian, Ben Trotter, Katie Williams, Karen Morrow, and Ben Smith, members of the NCSCL Digital/Latent Evidence section who lent knowledge, expertise and aid during my time at the lab.