# Is the Open Way a Better Way? Digital Forensics using Open Source Tools

Dan Manson, Anna Carlin,
Steve Ramos, Alain Gyger, Matthew Kaufman, Jeremy Treichelt

*California State Polytechnic University*
*Computer Information Systems Department*
*Pomona, California 91768 USA*
*Email: {dmanson, acarlin, saramos, acgyger, mdkaufman, jdtreichelt}@csupomona.edu*

## Abstract

*The subject of digital forensics can be quite challenging. Digital forensics is in its infancy and teaching digital forensics includes the techniques as well as the tools that assist in the process. This article discusses the tools used in computer forensics, compares an open source tool to two commercial tools, and the advantages and disadvantages of all three tools in an academic environment.*

*A team of four senior students sponsored by two faculty members established the project scope and requirements, presented three prototypes, and detailed the considerations of using open source tools. The same image was used to measure the performance of each software tool. The team found that the three tools provided the same results with different degrees of difficulty. The end results indicate that Open Source tools are a very good verification of evidence found using other products and should be included in the academic environment.*

## 1. Introduction

Brian Carrier, a well known expert in the open source forensics field, states that few published comparisons of open source and commercial forensic software exist [1]. Carrier cites a September 2000 review in SC Magazine [2], and a 2001 National Institute of Standards and Technology (NIST) Computer Forensic Tool Testing (CFTT) study on forensics tools [3, 4]. A recent publication by NIST provides updated test assertions and a test methodology for testing conformance of digital data acquisition tools [5]. However, NIST has not developed a test methodology for analysis tools.

A senior project team was formed to evaluate an open source alternative such as Sleuth Kit with the Autopsy browser to two commercial software products currently used such as EnCase and FTK. The team evaluated all three tools in terms of ease of use, robust functionality, and reliable and verifiable results.

The team conducted three prototypes using the same image to measure the relative performance of each software tool. The forensic image was acquired using FTK Imager and the results compared amongst the three tools. Operating system registry files and image file viewing were also analyzed. Each prototype is discussed in detail later with the lessons learned and implementation issues.

The image created contained password protected worksheets and entire workbooks. Images were inserted into the root directory, Program Files folder, and Documents and Settings folder. Executable files were renamed with a text file extension to trigger a file name mismatch. A suspicious program such as Tracks Eraser Pro was installed and several files were shredded. Once the files were shredded, the Recycle Bin was emptied. Two email accounts were created and logged onto to save the logon passwords.

The results indicated that the tools identified the same information that has evidentiary value with varying degrees of intricacy. For example, Autopsy would extract SAM information to then import into RegViewer to view registry information such as cookies and URLs.

The acquired image was imported into the three products. Sleuth Kit and EnCase imported the image in a relatively reasonable timeframe. FTK, on the other hand, could have a lengthy import process depending on the options selected. All three products provide MD5 hashing but

Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07)
0-7695-2755-8/07 $20.00 © 2007 IEEE
1530-1605/07 $20.00 © 2007 IEEE

SHA1 is only provided by Sleuth Kit and FTK. Sleuth Kit and FTK log all investigator actions when analyzing the image while EnCase does not.

The senior project team stated that FTK has an intuitive GUI for efficient analysis while EnCase would require a greater amount of training time. For Sleuth Kit, the Autopsy browser is necessary for those students familiar only with Windows.

Searching through the volume of data must be done quickly and efficiently. Searching features in EnCase were the most powerful compared to the other two products but would require training to use its full capabilities. EnCase has extensive search customization using string conditions, EnScript commands, and GREP.

The senior project team concluded that all three products should be used in the academic environment.

## 2. Methodology

The Cal Poly Pomona Computer Information Systems (CIS) Department requires students to take a capstone senior project course where teams of four to six students work as a "consulting group" for a real customer. The senior project course offered every quarter is a part of the polytechnic heritage and campus tradition of "learn by doing". Senior project examples include programming, website creation, database development, software evaluation, and similar projects.

A National Science Foundation grant enabled the CIS Department to purchase commercial computer forensics tools such as Guidance Software's EnCase® Enterprise and AccessData's Ultimate Toolkit™ (UTK) for use in the computer forensics class. The UTK includes the Forensic Toolkit, Registry Viewer, Password Recovery Toolkit, Distributed Network Attack, and FTK Imager.

Both of the tools mentioned above have demonstration versions that students can download, however, the functionality is very restricted. To obtain the full functionality requires purchased dongles and/or software keys to activate the full product. Dongles and software keys become problematic when access to the lab where the software is installed is not available. Working outside of the lab is very limited since students cannot afford to purchase these products for home use.

Open source tools such as Autopsy and Sleuth Kit have marginal costs compared to EnCase and FTK. Acquisition costs are restricted to time and bandwidth spent downloading the software and burning CDs. Students using open source tools can perform their acquisition and analysis anywhere at a very low cost. However, the support for open source alternatives is minimal at best. A public community support for troubleshooting exists but thus far no professional support.

As an instructor, using commercial software such as EnCase and FTK does not only include the software but also user manuals, online tutorials, frequently asked questions, white papers, and technical support. Students can access the online tutorials to complement the demonstrations provided by the instructor in class. Technical support can be contacted with any questions regarding results reported by their product. Both companies offer training classes year-round worldwide. Instructors should attend the training to learn the software quickly but also to network with other users for examples and future help.

Open source tools are not so easy to learn in a short time unless one has previous experience with Linux and would definitely be harder for a person who has only worked in Windows. Instructors would need to create their own tutorials and instructional guides for students. Instructors also become the "technical support" which could affect the amount of coverage that can be provided in a 10 week class. Students are required to use one primary software suite of their choosing and one secondary software suite for verification purposes. The key here is to ensure that all results are verified by a second tool.

It is important to note differences in approach between the senior project discussed in this paper and more detailed CFTT requirements. CFTT requirements are "developed by a focus group of individuals who have been trained and are experienced in the use of hardware write blocking tools and have performed investigations that have depended on the results of these tools"[5]. Senior project requirements are communicated to the team from the client, and documented in a matrix outlining priorities, project goals, and completion of individual requirements. The limited input and time (4 unit class – 10 week quarter) provided to a senior project limits requirements compared to the CFTT project.

Procedures and categories also differed between the authors' project and CFTT goals in several ways. The goal of this project was to

evaluate Open Source alternatives to software currently in use within the program, namely EnCase and FTK. Analysis was performed by using all available software for analyzing the same image and measuring the relative performance of all choices. Conversely, the goal of the CFTT project is to ensure that forensic tools consistently produce accurate, repeatable and objective test results.

An abbreviated comparison of the 12 senior project requirements and 26 CFTT requirements are shown below.

| **Senior Project Requirements Traceability Matrix (abbreviated)** | **CFTT Traceability Matrices – Tool Requirements (abbreviated)** |
|---|---|
| 1. Software package capabilities compared | 1. Acquire digital source using tool |
| 2. Client understands software capabilities | 2. Tool creates clone of digital source |
| 3. Client understand software analysis capabilities | 3. Tool operates in execution environment |
| 4. Client understands password protection tools | 4. The acquires all visible data sectors |
| 5. Client understands registry viewing for software | 5. The tool acquires all hidden data sectors |
| 6. Client understands image viewing capabilities | 6. Data sectors accurately acquired |
| 7. Client understands reporting capabilities | 7. Tool identifies unresolved errors |
| 8. Client provided with Open Source pros and cons | 8. Tool shall use a benign fill in destination object |
| 9. Implementation and support costs provided | 9. Image file created in the selected format |
| 10. Client understands corporate and legal use | 10. Image file errors identified |
| 11. Client understands user requirements | 11. Insufficient space issues identified |
| 12. Reliability and functionality limits identified | 12. Multi-file image creation capabilities identified |
| | 13. Image file integrity checking is performed |
| | 14. Tool offers conversion of an image file |
| | 15. Tool offers destination device switching |
| | 16. Tool offers clone creation during an acquisition |
| | 17. Tool offers clone creation from an image file |
| | 18. Tool offers creation of a partial clone |
| | 19. Tool offers unaligned clone creation |
| | 20. Tool offers cylinder-aligned clone creation |
| | 21. Tool controls excess sectors on clone destination |
| | 22. Insufficient space on clone creation is addressed |
| | 23. Write errors creating the clone are addressed |
| | 24. Tool shall log correct hashes for blocks |
| | 25. Tool offers log file creation details |
| | 26. Unprotected source not modified in acquisition |

**Figure 1. Senior Project and CFTT requirements comparison [5]**

## 3. Forensics Software Tools

**3.1 EnCase** Since its founding in 1997, Guidance Software has grown to be a leading providing of computer forensic software and services with over 20,000 worldwide clients and 285 employees [6].

Guidance Software states that their suite of EnCase® solutions enables corporations, government and law enforcement agencies to conduct effective digital investigations, respond promptly to eDiscovery requests and other large-scale data collection needs, and take decisive action in response to external attacks. [6].

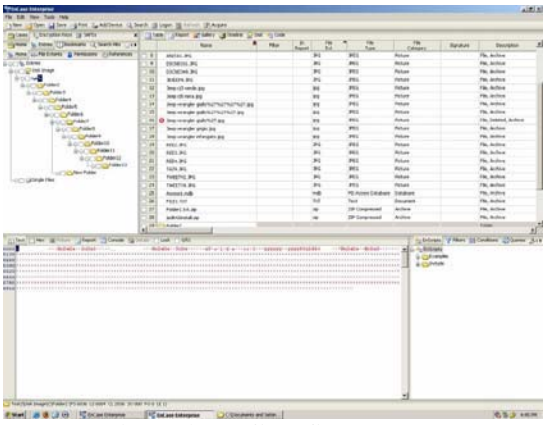

**Figure 2. EnCase Screenshot**

An Initial Project Scope Analysis of EnCase included the following product features:

1. Can read multiple file system formats such as FAT, NTFS, ext2, ext3, ReiserFS, UFS, and JFS.
2. Can read multiple disk image formats such as Raw (dd), VMware, EnCase (.E01), and Safeback
3. Can remotely acquire disk images from networked computers running an EnCase acquisition agent
4. Integrated keyword searching
5. EnScript programming language automates almost any functionality with complete control over the details
6. Disk browsing, searching, and EnScript are primary ways to view evidence
7. Integrated viewer allows viewing of many popular file formats, such as image files
8. Indexes zip files for analysis of compressed files/folders
9. Can create hash values for any file in the case
10. Integrated registry viewer

**3.2 FTK** Since its inception in 1987, AccessData has provided investigators with digital forensic tools that seamlessly integrate for the reading, acquisition, decryption, analysis and reporting of digital evidence. The AccessData Forensic Toolkit® (FTK™) offers law enforcement and corporate security professionals the ability to perform complete and thorough computer forensic examinations. [7].

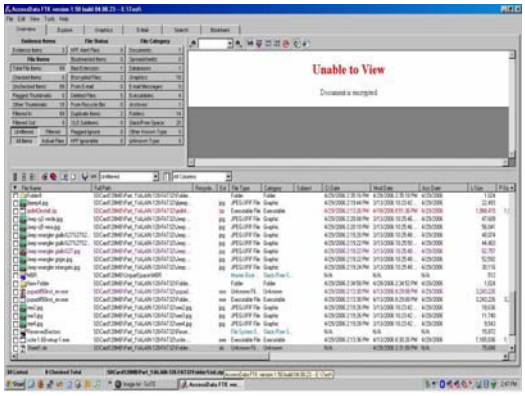


**Figure 3. FTK Screenshot**

An Initial Project Scope Analysis of FTK included the following product features:

1. Can read multiple file system formats such as FAT, ext2, ext3, and NTFS
2. Can read multiple disk image formats such as Raw (dd), SMART, EnCase (.E01), Snapback, and Safeback
3. Supports most modern email clients for email analysis
4. Indexes zip files for analysis of compressed files/folders
5. Known File Filter (KFF) feature aids the investigator in focusing on items of interest
6. Interface is filter-based, with multiple different pre-programmed filters for evidence viewing
7. Internal viewer allows investigator to view Word, PowerPoint, and Excel documents, and various image files
9. Internal email viewer allows investigator to navigate email from various email store formats without having the email client used to generate the store
10. Search feature using keywords
11. Expanded functionality, such as registry viewing and password recovery, comes in the form of program integration with other company products
12. Creates hash values for any file

**3.3 Autopsy and Sleuth Kit** Sleuth Kit is a freeware tool designed to perform analysis on imaged and live systems. One can examine file systems in a non-intrusive manner because the tools do not rely on the operating system to process the file systems, allowing deleted and hidden content to be shown. When performing a complete analysis of a system, Autopsy was used which has a graphical user interface to Sleuth Kit. Autopsy provides case management, image integrity, keyword searching, and other automated operations [8].

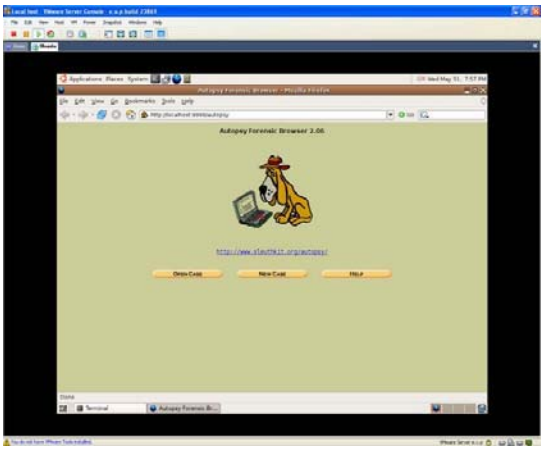

**Figure 4. Sleuth Kit Screenshot**

Since the package is open source it inherits the security principles which all open source projects benefit from, namely that anybody can

look at the code and discover any malicious intent on the part of the programmers. An argument against this might be that many people do not really care about the code, but there is still the potential for more people to look at open source code than there is for a few programmers of a closed source application to look at their peer's code.

One advantage for a classroom style analysis operation is the fact that since Autopsy is running on a TCP port; several students can connect to the server and work on a case simultaneously. Each investigator must enter their name when starting a case so that separate log files are created, thus allowing each investigator to work on their own evidence chains while maintaining separate accounts of their actions.[16]

When looking at just the Sleuth Kit portion of the package it contains more than 21 very powerful Linux based tools which are divided into 9 distinct categories: File System Layer, File Name Layer, Meta Data Layer, Data Unit Layer, File System Journal, Media Management, Image File, Disk, and Other Tool [14].

An Initial Project Scope Analysis of Autopsy and Sleuth Kit included the following product features:

1. Tools can be run on a live UNIX system showing files that have been "hidden" by rootkits while not modifying the accessed time of files viewed
2. Can read multiple file system formats such as NTFS, FAT, ext2fs, ext3fs,UFS 1, UFS 2, and ISO 9660
3. Can read multiple disk image formats such as Raw (dd), EnCase (.E01), AFF file system and disk images

## 4. Categories for Comparison

Performance categories were chosen for evaluation reflecting capabilities expected to be used during the acquisition and analysis stages of forensic investigations. The following categories were covered during the project:

- Calculates MD5 and SHA1 image hashes
- Provides hash value for individual files
- Verifies image integrity
- Finds deleted and encrypted files
- Identifies deleted and encrypted files clearly
- Recovers deleted files
- Identifies file extension mismatches
- Searches for strings (ASCII and Unicode)
- Includes HEX level viewer
- Organizes files into predetermined categories
- Provides an image gallery
- Shows file modified, accessed, and creation dates and times
- Logs investigator activity
- Identifies and analyzes slack/free space
- Finds and identifies overwritten files
- Finds cookies and URLs in registry
- Image import speed
- Initial import data

## 5. Prototypes

The primary focus of the work was to evaluate Open Source alternatives to the commercial software currently used. Three prototypes were conducted by the team and the results communicated to the faculty sponsors.

The same image was used to measure the relative performance of each software tool. In doing so, the following forensic steps were performed:

- Acquisition of the forensic image using FTK Imager
- Compared the results from each tool
- Formulated recommendations for the use of open source tools in the academic environment.

**5.1 First Prototype** The first prototype acquired an image from a Treo 650 phone Secure Digital (SD) card. The image was acquired in a Raw dd (disk-to-disk) format using FTK Imager for use across all forensics suites. A Raw disk image is a direct copy of a disk drive. Windows delete and a shredder program called Tracks Eraser were used to delete files; files and file extensions were renamed; and, documents were password protected.

The following was accomplished:

- FTK Imager 2.1a was used to generate the forensics image for use across all software suites.
- Comparative categories were identified and detailed.
- Analysis was performed on the basis of whether or not the software could identify and/or perform in those categories.

- Testing methodology for the tools was established.

Changes were identified for integration into the next prototype. A larger hard drive device should be used in order to analyze operating system files such as registry entries and Internet cookies. Additional categories for comparative analysis should be identified.

**5.2 Second Prototype** A 15GB hard drive was used for the second prototype with various files installed in addition to Windows XP, Service Pack 2. The image was acquired using FTK Imager. Autopsy and Sleuth Kit were tested using a VMware virtualization environment. VMware allows one physical machine to run numerous operating systems simultaneously.

The image became corrupted when transferring the files due to the VMware environment. Hashes were verified to check image integrity; however, the image had to be reacquired. Due to the numerous starts and missteps coupled with a lengthy imaging of a larger drive, limited testing was performed.

The virtualization environment needed adjustments for the forensics software. Physical drives must be mounted to the virtual environment in addition to virtual drives. Also spaces in the file path created file navigation problems in a Linux environment and permission restrictions necessitated running a user as root in the environment.

**For the next prototype, the original evidence drive was** reduced to one large enough to install an operating system on. Windows XP takes just over 2 GB of space. Limiting the size will also limit the time spent imaging the drive. Changes to the virtualization setup were researched to accommodate the forensics software. Recommendations for the curriculum were to avoid Linux issues such as naming files without spaces, placing files in root directories of drives, and giving users root permissions.

**5.3 Third Prototype** A 4 GB image was created and acquired into Raw dd format using FTK Imager for use across all forensics suites. The forensics suite included FTK 1.61a, EnCase 5.05C, Autopsy 2.06, Sleuth Kit 2.03, and VMware EXP build 23869. Autopsy and Sleuth Kit were tested using the VMware virtualization environment.

The hard drive had various files installed in addition to Windows XP SP2. The steps taken in adding files for analysis and creating the image used for comparative analysis across FTK, EnCase, and Autopsy were as follows:

1. Created workbook1.xls with text and image inserted
2. Sheet protected with password: 1dFa466Cis
3. Workbook protected with password: 123qwe456RTY
4. Added workbook1.xls to hard drive
5. Added 41463750_gal_map.jpg, 20051130-0361_RPH_large.jpg to hard drive under Program Files folder
6. Added dawn7a.jpg, georg-profile.png, IMG_3492.jpg in root directory of hard drive
7. Added lake.louise.1.gif, newyork.jpg, vwboard.jpg to Documents and Settings folder of hard drive
8. Added fileshred.exe to hard drive root directory
9. Renamed fileshred.exe to fileshred.txt
10. Deleted newyork.jpg and dawn7a.jpg from hard drive
11. Installed Tracks Eraser Pro 5.7
12. Shredded/overwrote georg-profile.png 2X with Tracks Eraser Pro 5.7
13. Shredded/overwrote _41463750_gal_map.jpg 2X with Tracks Eraser Pro 5.7
14. Emptied Recycle Bin
15. Got onto the Internet with MS Internet Explorer 6.0.2900.xpsp_sp2_rtm.040803-2158
16. Created account on thinkgeek.com with username: swingtime_45@hotmail.com and password: forensics
17. Created account on slashdot.org with username: forensics and password: forensics
18. Logged onto both accounts with MS Internet Explorer and saved passwords.

## 6. Results

**6.1 Robust functionality** The following was determined regarding the functionality of all three tools:

1. EnCase is identified with certain characteristics:
   - Requires a greater amount of time in training before a user can be effective in analysis
   - Searching can be confusing
   - No log file is available to investigators of their actions performed in a session

- Extensive search customization afforded through string conditions, EnScript language commands, GREP, and filters.
- Convenient analysis afforded by importing the image and hashing files in the background after importing

2. FTK is identified by certain characteristics:
   - Requires substantially less time commitment to training to use the program
   - Intuitive GUI design for speedy analysis
   - Lengthy importing process restricts time for analysis of contents of the image
   - Least customizable of all three software choices
3. Autopsy and Sleuthkit are identified by certain characteristics:
   - Does not easily identify encrypted files
   - Many functions require a "Sort by File Type"
   - Vague identification of overwritten files
   - Extreme amount of customization afforded by PERL scripting and utilization of the Linux environment
   - Works well in tandem with other Linux tools

**6.2 Reliable and verifiable results** Figure 5 provides a detailed comparative analysis.

| | Category | EnCase | FTK | Autopsy |
|---|---|---|---|---|
| 1 | Uses MD5 Hash | Run a search first then yes | Yes | Yes |
| 2 | Uses SHA1 Hash | No | Yes | Yes |
| 3 | Shows hash for individual file | Run a search first then yes | Yes | Yes |
| 4 | Can verify image integrity | Yes | Yes | Yes |
| 5 | Find deleted files | Yes | Yes | Yes |
| 6 | Identify deleted files clearly | Yes | Yes | Yes |
| 7 | Recover deleted files | If not overwritten, yes | If not overwritten, yes | If not overwritten, yes |
| 8 | Find encrypted files | Yes | Yes | Yes |
| 9 | Identify encrypted files clearly | No | Yes | No |
| 10 | Identify file extension mismatches | Yes, after search or selection of "Conditions - Renamed extensions" | Yes | Run a "Sort By File Type" then yes |
| 11 | Can search for strings (ASCII and Unicode) | Yes | Yes | Yes |
| 12 | Includes HEX level viewer | Yes | Yes | Yes |
| 13 | Organizes files into predetermined categories | Yes - "Filters" / "Conditions" | Yes | Run "Sort By File Type" then yes |
| 14 | Shows image gallery | Yes | Yes | Run "Sort By File Type" then yes |
| 15 | Shows file modified/accessed/created times | Yes | Yes | Yes |
| 16 | Provides a log file of investigator activity | No | Yes | Yes |
| 17 | Identifies and analyzes slack/free space | Yes | Yes | Yes |
| 18 | Find overwritten files | Yes | Yes | Yes |
| 19 | Identify overwritten files | Yes | Yes | Only by file name |

| | | | | |
|---|---|---|---|---|
| 20 | Find cookies | Yes | Yes | Use Autopsy to Extract SAM and Regviewer to see Cookies |
| 21 | Find URLs in registry | No | Not by itself; a separate program must be used | Use Autopsy to Extract SAM and Regviewer to see URLs |
| 22 | Image import speed | Fastest (Standard Options - None) | Slowest (Standard Options - Hash, Index, Sort) | Middle (Standard Options - MD5 Hash image) |
| 23 | Initial import data | Gives the smallest amount of data right after an image import | Gives the largest amount of data right after an image import | Gives hash right after image import |

**Figure 5. Comparative Analysis**

**6.3 Ease of use** The usability of the individual programs varies due to the user's computer knowledge. For instance, Sleuthkit/Autopsy is easier to use for a person with Linux experience but it would be harder for a person who has only worked in Windows. FTK is easy for most people to use if they have basic knowledge of forensic theory and a background in computers. EnCase is difficult for almost anybody to use because of its feature set, EnScript, incomplete help files and general user interface.

For these reasons it would be very difficult to measure program usability and any measurements that might be obtained would almost always be incorrect when applied to another person.

**6.4 Support Issues** Support for commercial products like EnCase and FTK are provided as part of the purchase price. Both companies have a technical support group available and messages groups/forums to resolve issues in a timely manner. Both companies offer user manuals documenting the features of their product and additional hands-on training in one of their facilities.

Support for Open Source alternatives is sketchy at best. Public community support exists for troubleshooting the software but thus far no professional support has been located. As the popularity of the Sleuth Kit/Autopsy package has increased and has been able to prove itself, the lack of documentation problem is being overcome. One of the reasons there is a lack of documentation is because those using these tools are already Linux users and have a tendency to memorize many commands for their operating system. However, this can be very daunting to a Windows user because of their dependence on graphical interfaces. The Autopsy client is graphical but it is still just controlling a command line input, therefore it has some rough edges and is not as user friendly as its Windows counterparts.

## 7. Further Research Recommendations

In order to provide investigators with sufficient confidence to use open source computer forensics tools within an investigation, research and comparative analysis of open source vs. closed source tools must take place.

This research must be performed by trusted organizations or authorities. Examples of such include Government agencies such as the National Institute of Standards and Technology (NIST) [3], Department of Defense (DoD) [10] and Department of Justice (DOJ) [11]. Other trusted organizations and institutions can include international government organizations research institutes, accredited schools, trade associations and professional organizations.

Validation performed by a trusted entity will provide open source tools with the weight needed to stand up in court. When it comes to challenging the credibility of an expert witness on the basis of usage of free tools, this validation will be able to provide considerable assistance if validated by a well-recognized, trusted source.

Research has been performed by the NIST Computer Forensics Tool Testing project, however the number of tools analyzed thus far is limited. The only tool related to open source

computer forensics that has been tested is dd for image acquisition. It has been tested twice, on two separate platforms [3].

It would be useful to build test suites that, in essence, "calibrate" forensics software. A test suite that consists of the latest program installations of Sleuthkit/Autopsy, FTK and EnCase plus a standardized image would be needed to adequately calibrate each software package. This forensics image would need to be carefully built and imaged in compliance with law enforcement standards.

Future research could compare how software programs compare technically, in terms of usability and stability. However, usability of the individual programs varies greatly and is very dependent on a broad spectrum of knowledge. The basic theory to be able to effectively analyze an image using any of these programs should include hard drive and partition setup, file manipulation processes, encryption, and other areas. Without this basic knowledge, analysis of a hard drive is a very slow and error prone mix of uncoordinated actions, which no program will be able to work with.

The stability of each program greatly depends on hardware, operating systems, user experience, environmental conditions, image quality, image cleanliness (e.g. virus infestations, malware, spyware, adware, etc), and other factors. Without being able to isolate all of these variables it is very difficult to measure stability. One operating system can not be used to run all of these programs, two are Windows based and one is Linux based. A Windows based program will have issues with an image containing Windows viruses which will affect the stability of the entire environment. Linux based systems do not have the support of all the hardware manufacturers that Windows does thereby introducing firmware and hardware incompatibilities.

It is possible to perform tests like this but they will be influenced by many factors, which can not be controlled, thus skewing the test each time it is performed. This makes for a very unclean test environment and produces inconsistent results. For these reasons the senior project described in this paper did not attempt to perform these tests, but someone with more time might be able to produce some type of useful metric.

Additional software that enrich the quality of the tools recommended and evaluated in this report include Linux tools such as Air, a GUI for DD and/or DCFLDD [12], and RegViewer for windows registry files [13]. Future testing should also look into running multiple users on one Autopsy server, and provide a detailed look at reporting functions of all software packages.

## 8. Conclusion

The senior project compared Sleuth Kit to EnCase and FTK to determine whether evidentiary data was identified by all three products. The team evaluated Sleuth Kit in terms of ease of use, robust functionality, and reliable and verifiable results. The use of open source tools in the classroom environment was also evaluated.

The same forensic image was used to measure the relative performance of each software tool using predetermined criteria. Three prototypes were conducted by the team and the results communicated to the faculty sponsors.

The results indicated that the tools provided the same results with varying degrees of intricacy. An example would be that EnCase and FTK automatically present an image gallery, where as, Autopsy needs to sort by file type before images are displayed. The acquired image was imported into the three products. Sleuth Kit and EnCase imported the image in a relatively reasonable timeframe. FTK, on the other hand, could have a lengthy import process depending on the options selected which could restrict the time spent on analysis. All three products provide MD5 hashing but SHA1 is only provided by Sleuth Kit and FTK. Sleuth Kit and FTK log all investigator actions when analyzing the image while EnCase does not.

The graphical user interface was always a hot topic of discussion among students when using EnCase and FTK. The senior project team confirmed that FTK has an intuitive GUI for efficient analysis while EnCase would require a greater amount of training time. For Sleuth Kit, the Autopsy browser is necessary for those students familiar only with Windows.

Searching for evidence is sometimes like looking for a needle in a haystack. Sifting through the volume of data must be done quickly and efficiently. Searching features in EnCase were the most powerful compared to the other two products but would require training to use its full capabilities. EnCase has extensive search customization using string conditions, EnScript commands, and GREP.

The senior project team concluded that all three products should be used in the academic

environment. Each tool has its strengths and weaknesses that require consideration when deciding when implementing them in an academic environment.

Senior project deliverables included a virtualization environment with Linux on DVD, including Ubuntu Linux, VMware, and user instructions. The authors can provide a copy of this DVD on request. In addition, the authors would like to partner with other institutions on future evaluation and comparisons of open source and commercial forensic software and hardware.

The authors agree with Carrier's conclusion that confidence in forensic tools will increase through publication, review, and formal testing [1]. Open source software continues to be one of the most widely used tools in computer forensics [15]. The senior project evaluation discussed here is a step in that direction.

While one tool like Sleuthkit/Autopsy is very good at performing certain tasks it is of vital importance to be able to duplicate the steps taken with it in obtaining an evidence file with another forensic program because credibility can not be built by one program alone. Since the aim of performing computer forensics is not to have a duel between two competing technologies but to prosecute a person for the crimes they have been accused of. Therefore it is important that both open and closed source programs work together to validate each others results so that justice can be done to those who deserve it. This means that closed source users must have an open mind and must try other tools, preferably open source tools, to validate their results. If an open source tool creates the same evidence as a closed source tool, the open source tool's code can be analyzed and proved to be working correctly. Therefore the closed source tool's source code can be assumed to also be working correctly without inspection because of the identical outcome [16].

## 9. References

[1] Carrier, Brian, Open Source Digital Forensic Tools: The Legal Argument, @stake Research Report, October 2002.

[2] James Holley. Computer Forensics Market Survey. SC Magazine September 2000. Available at: http://www.scmagazine.com/scmagazine/2000_09/survey/survey.html

[3] NIST. Computer Forensics Tool Testing. Available at http://www.cftt.nist.gov/

[4] NIST CFTT. Disk Imaging Tool Specification, 3.1.6 Edition, Available at: http://www.cftt.nist.gov/DI-spec-3-1-6.doc.

[5] Digital Data Acquisition Tool Test Assertions and Test Plan, November 10, 2005. Available at http://www.cftt.nist.gov/DA-ATP-pc-01.pdf.

[6] Guidance Software, maker of EnCase, provides Incident Response and Computer Forensics Solution, Expert Forensic Services and Computer Forensic Training. Available at http://www.guidancesoftware.com/.

[7] Welcome to Access Data! Available at http://www.accessdata.com/.

[8] The Sleuth Kit & Autopsy: Digital Investigation Tools for Linux and other Unixes. Available at http://www.sleuthkit.org/.

[9] E-mail response from Gregory Carlton, 5/26/2006.

[10] DoD Cyber Crime Center. Available at http://www.dc3.mil/.

[11] National Institute of Justice – Electronic Crime Available at http://www.ojp.gov/nij/topics/ecrime/welcome.html.

[12] Air: Automated Image and Restore. Available at http://air-imager.sourceforge.net/.

[13] SourceForge.net: regviewer. Available at http://sourceforge.net/projects/regviewer/.

[14] Carrier, Brian. The Sleuth Kit: Tool Details. Sleuthkit.org. 13 Feb. 2006 http://www.sleuthkit.org/sleuthkit/tools.php

[15] Byfield, Bruce. The two-edged sword: Legal computer forensics and open source. 11 April. 2005. News Forge. 13 Feb. 2006 http://software.newsforge.com/software/05/04/05/2052235.shtml

[16] Gyger, Alain. Sleuthkit/Autopsy: An Open Source Forensic Package. February 15, 2006.