ISSN No: 2309-4893
International Journal of Advanced Engineering and Global Technology
Vol-03, Issue-07, July 2015

Analysis of Open Source and Proprietary Source Digital Forensic Tools

Neelam Maurya
Department of MS-Cyber Law & Information Security
Indian Institute of Information Technology
Allahabad, India
neelamcs0046@gmail.com

Jyoti Awasthi
Department of MS-Cyber Law & Information Security
Indian Institute of Information Technology
Allahabad, India
jyotiawasthi91@gmail.com

Raghvendra Pratap Singh
Department of MS-Cyber Law & Information Security
Indian Institute of Information Technology
Allahabad, India
er.rps16@gmail.com

Dr. Abhishek Vaish
Assistant Professor
Department of MS-Cyber Law & Information Security
Allahabad, India
abhishek.infosec@gmail.com

***Abstract*- The dispute between the virtues of open source and proprietary source forensic software has always prevailed in the society based on critical issues such as security and reliability. To prove the goodness of either of them it is necessary to do a comparative analysis of proprietary source and open source tools to provide sufficient confidence to the open source tools that their results as an alternate to the closed source can be accepted in the court of law. This paper in the light of Daubert's guidelines tries to check various features and functions of the forensic tools to show that open source tool may more clearly meet the guidelines and may give similar results to closed source forensic tools. This paper is based on a comparative study between open source and proprietary source tools for five forensic tools. It also includes a brief description of the tools which are used for the comparative study and the details of the parameters which would be used for the comparison.**

***Keywords*- Chain of Custody, Daubert's Guidelines, Digital Forensics, Open Source Tools, Proprietary Source Tools**

I. INTRODUCTION

Today we advance and prosper in a world of information and technology where we rely mainly on computer system and resources for everyday work. However, as a result of our over-reliance on computers we have begun to witness a hike in computer crimes. A computer crime may be defined as a crime committed using a computer or computer resource, or any crime in which computer is the victim. To solve such crimes a new branch of knowledge for study has been adopted which is commonly known as digital forensics. Digital forensics is basically focused with the investigation of any suspected crime or behaviour that may be indicated by digital evidence. The evidence is present in various forms and at places from digital devices or computer system that can simply be used as repository of evidence that documents the activity or it may consist of information residing on the electronic devices or computers that have been used originally to facilitate such activity or that have been targeted. Digital forensics is an important tool dedicated to the computer crime, where a computer was used either as an agent or a target for the crime. In order to present digital evidence in court, one must keep in mind and prove that a series of legal standards were met when the said evidence was collected or generated.

This paper is divided into four parts. The first part of the paper presents a brief overview of the classical forensic investigation process and also includes a brief description of the tools which are used for the comparative study. The second part of the paper comprise of the details of the parameters which would be used for the comparison. In the third section of this paper, a comparison matrix is provided which gives us results, which can be further used for analyzing the digital forensic tools. Also, we have tried to map the parameters with the four phases of digital forensics investigation process for better understanding of the parameters used. Finally, the fourth section gives the conclusion based on the comparative analysis.

The digital evidences must follow the four Daubert's guidelines to be accepted in the court of law, which are:

1. Testing-

All the tools taken for identifying, generating and verifying the digital evidence must be scientifically tested and proved to be efficient and reliable so that to be accepted in the court of law. This guideline establishes if a process can be tested in a way to ensure the accuracy of the results it provides.

2. Error Rate-

The guideline identifies if there is a known error of the process. Error rate for any tool can be calculated on the basis of number and severity of bugs that is produces.

3. Publication-

The tools used during the investigation process must be those which are not uncommon in the society. There should be experts who are able to work on those tools. The publication guideline ensures that the procedure has been documented and has undergone several peer reviews for assuring quality and work.

2. Acceptable-

The tools and the results generated using it should be such so that to be accepted by the digital forensics community. Published procedures are required for this guideline to be true.

II. BACKGROUND STUDY

Many papers are published in this domain showing the use of digital forensic tools either proprietary or open source, proving their goodness and efficiency in solving crimes done through computer or computer resources. *Dan Manson, Anna Carlin, Steve Ramos, Alain Gyger, Matthew Kaufman, Jeremy Treichelt* presented a paper *'Is the Open Way a Better Way? Digital Forensics using Open Source Tools'* [3] in which they provided a detailed analysis of three computer forensic software that is Encase, FTK and Autopsy and compared them on the basis of certain functionalities. Their end results show that Open Source tools are as good as proprietary tools in identifying the evidences. Another paper titled '*OSForensics Comparison*' [2] by *Colby Lahaie, Kyle Porto, and David Leberfinger* compares the time taken by two forensics tools OSForensics and Encase v7 for different processes such as acquisition, hashing, internet history, recovery of deleted files and keyword searching. The comparison proves that OSForensics is a powerful forensic acquisition and analysis tool because it is more user-friendly and much easier to navigate than Encase v7. In another paper '*Analysis and Comparison of Open Source and Proprietary Digital Forensic Tools*' [1] by *Atul Raj, Irman Ali and Praveen Kumar*, they have focused on comparison of open source data recovery tools having similar objective with proprietary tools. They have taken two proprietary source tools EnCase and FTK and some Linux based data recovery forensic tools and compared them.

A. Digital Forensic Investigation

Digital forensic investigation is a step wise process in which the digital devices such as computer, computer resources, electronic devices, mobile phones etc. are investigated for identifying, generating, analysing, verifying and presenting digital evidences in the court of law using standard tools and by following certain policies, guidelines, standards, laws which are acceptable to the jurisdiction process for getting hold of the criminal and giving justice to the victim. It generally comprises of four major processes:

1. Acquisition-

In this first phase of investigation, the digital devices are identified for presence of digital evidences, if any and then collected in such a way that the original state or content of the evidences remains the same and no tampering or modification of the evidence, such as deletion or addition, is done in any manner.

2. Preservation-

The evidences collected from the targeted or suspicious machines should be preserved to maintain and guarantee the Chain of Custody. To prove the chain of custody, service providers are needed who can ensure that the evidence offered in court is the same as that was collected and there was no tampering with the evidence while it was in the custody, and ultimately show that the evidence has remained intact.

3. Analysis-

Analysis phase plays an important role because the result or output obtained after the analysis of the evidences using different digital forensic tools should be such that to help the investigators in identifying the cause of the incident and provide him with results which he could be assure of to be effective and sufficient to be submitted in the court for justice. This phase includes recovery of deleted content and examining the system content. Scientific methods are used in this phase to draw conclusions based on the evidence that was found.

4. Presentation-

This phase presents the conclusions and the evidences obtained from the forensic investigation. This is a phase where acquired data is processed to achieve relevant information as per the need and is based entirely on policy and law.

B. Comparison between Open Source and Proprietary Source Digital Forensic Tools

OPEN SOURCE: They are freely available to be used and also provide the original source code to the user. These can be installed in any computer system free of cost.

PROPRIETARY SOURCE: They are not freely available to the users. The company that develops the software owns it and no one may duplicate it or use it without the developers consent. Users need to pay for using this software and must have a license before installing it.

C. Forensic Tools Overview

There are many digital forensic tools, open source as well as proprietary source. Some of the tools that we are using for our research purpose are as follows:

1. FTK 3.0-

Forensic Toolkit is proprietary source forensic software developed by Access Data for investigation of digital evidences so that it can be produced in the court. The toolkit includes tools such as FTK Imager which is used to create forensic image of any type of media. Language Selector utility provides an option for selecting the language in which we want to see the case. Mobile Phone Examiner used for examining data from cell phones and data card. Registry Viewer provides the function of viewing the contents of Windows operating system registry files and registry's protected storage. Distributed Network Attack and Password Recovery Toolkit are used for analyzing the file signatures and recovery of password. This toolkit helps in filtering, analysing, investigating and reporting on acquired evidence.

2. EnCase 4.20-

It is proprietary source forensic software developed by Guidance to conduct effective digital investigations. It is used

for acquisition, analysis and reporting process. This tool has scripting functionality named EnScript for interacting with evidences using various API's. It provides integrated keyword searching, integrated registry viewer.

3. Autopsy 3.1.2-

It is a GUI based open source forensic software. It is used by law enforcement agencies, military and security professionals for investigation of evidences in hard drives and smart phones. It helps in indexing, keyword searching, registry analysis, web artefacts analysis, email analysis and reporting.

4. OSForensics 3.1-

It is open source forensic software that is used for imaging, extracting, analysing and reporting of digital evidences from digital media in an efficient manner. It able to see the recent activities, downloaded files and connected USB devices in the system. It provide indexing, keyword searching, email viewer, registry viewer, raw disk viewer, search and recover deleted files efficiently.

5. SIFT 3.0-

Sans Investigation Forensic Toolkit 3.0 is open source forensic software which support Linux platform. It is a VMware image that has forensic tools pre-installed. It provides guidelines for securing the integrity of evidences. This toolkit includes different tools such as: The Sleuth Kit which is used for Files system Analysis, log2timeline used for Timeline view, ssdeep&md5deep are the two Hashing Tools, WireShark used for Network Forensics, Pasco for Internet Explorer Web History examination, Rifiuti for Recycle Bin examination, Volatility Framework used for Memory Analysis, etc.

III. PROPOSED WORK

In this paper, we have tried to bring out the virtues and goodness of open source tools when compared to the proprietary source digital forensic tools. For this purpose we have used different functionalities and features of the forensic tools as parameters for the comparison. Then we have used these predefined parameters for the comparative analysis of the tools.

A. The parameters are as follows:

(i) MD5 Hashing-
It is used for assuring integrity of the evidence. MD5 hash creates a signature of 128 bits.

(ii) SHA-1 Hashing-
It is also used for integrity purpose and creates signature of 160 bit.

(iii) Platform Support for Windows OS-
Whether the tool is working efficiently on windows platform?

(iv) Platform Support for Linux OS-
Whether the tool is working efficiently on Linux platform?

(v) User Friendly–
Feature of any tool to be easily understandable and feasible to work on.

(vi) Timeline Analysis-
Is the tool able to provide a line graph for the activities happened recently in the system?

(vii) Cost–
How much money has to be paid to buy the tool?

(viii) License–
Does the tool require any license before installation and working?

(ix) Repeatability-
Feature of any tool to provide similar results every time for the same data set and same working environment.

(x) Reliability-
It tells about the trustworthiness of any tool with reference to the results it provides.

(xi) Documentation and reporting-
Whether the tool provides a report of overall investigation and results obtained?

(xii) Use of GUI vs. Command line-
Whether the tool is operated through command line or graphical user interface?

(xiii) Supported File Format-
Different type of file formats that the tool supports?

(xiv) Supported Image Format-
The image formats which can be used as an input to the tool for analysis.

(xv) Time taken for Keyword Search-
Quantum of time taken by a tool to search and provide result based on the given keyword.

(xvi) Time taken for verification-
Time taken for verifying if the imported image is the same as that of the image acquired originally.

(xvii) Identify deleted files-
Whether the tool is able to identify the files which are deleted from the drive or the system?

(xviii) Recover deleted filed-
Is the tool able of recovering the files which were permanently deleted?

(xix) Mismatch extension-
Is the tool able to identify the mismatching of extensions or not?

(xx) Identify slack spaces-
Is there any feature which can be used to identify slack spaces in the give image?

(xxi) Ability to browse internet history-
Is the tool able to browse the internet history, i.e. the searching, surfing, downloading, visiting of various websites?

(xxii) Ability to browse cookies-
Is there any feature in the tool for browsing cookies?

(xxiii) Log of investigation activity-
Is the tool creating and maintaining the case logs?

(xxiv) Show file created time-
Does the tool show the created time for any file?

(xxv) Show file modified time-
Does the tool show the modified time of any file?

(xxvi) Show file accessed time-
Is the tool able to show the last accessed time for any file?

(xxvii) Identify registry file-
Is the tool able to identify and analyse the registry files for getting system information?

(xxviii) Search and recover recycle bin-
Does the tool provide any feature of searching and recovering the recycle bin data?

(xxix) File Carving-
If the tool is able to search the file based on the content rather than the Meta data?

(xxx) Search Unallocated Space-
Whether the tool is able locate the unallocated space?

(xxxi) Most recently used-
Can the tool give information about the tools and software which were run on the system recently?

B. Comparison based on the Predefined Functional Parameters

TABLE 1
COMPARISON TABLE

TOOLS → / PARAMETERS ↓	FTK 3.0	ENCASE 4.20	AUTOPSY 3.1.2	OSFORENSICS 3.1	SIFT 3.0
MD5 HASHING	YES	YES	YES	YES	YES
SHA-1 HASHING	YES	NO	YES	YES	YES
PLATFORM SUPPORT FOR WINDOWS OS	YES	YES	YES	YES	NO
PLATFORM SUPPORT FOR LINUX OS	NO	NO	NO	NO	YES
USER FRIENDLINESS	YES	YES	YES	YES	NO
COST	COSTLY	COSTLY	FREE	FREE	FREE
LISCENSE	REQUIRED	REQUIRED	NOT REQUIRED	NOT REQUIRED	NOT REQUIRED
TIMELINE VIEW	NO	YES	YES	YES	YES

REPEATABILITY	YES	YES	YES	YES	YES
RELIABILITY	YES	YES	YES	YES	YES
DOCUMENTATION & REPORTING	YES	YES	YES	YES	YES
USE OF GUI vs. COMMAND LINE	GUI	GUI	GUI	GUI	COMMAND LINE
SUPPORTED FILE FORMAT	FAT 12, FAT 16, FAT 32, NTFS, EXT2, EXT 3	FAT 12, FAT 16, FAT 32, NTFS, EXT2, EXT3, REISER , UFS, JFS, OPENBSD, NETBSD, PALM, HFS, HFS+, CDFS, ISO 9660, UDF, DVD, TIVO1, TIVO 2	NTFS, FAT, UFS 1 UFS 2, EXT2, EXT 3	NTFS, FAT 16, FAT 32, EXT 2, EXT 3, EXT 4, HFS+, HFSX	NTFS, ISO9660, HFS+, RAW , SWAP, FAT 12, FAT 16, FAT 32, EXT2, EXT3, EXT4, UFS1, UFS2, VMDK
SUPPORTED IMAGE FORMAT	E01, SNAPBACK,SAFEBACK 2.0, DD, ICS, Ghost, SMART, CD, DVD, MDS, CCD, ISO, ISOBUSTER, CUE, NRG, PGI, PXI, CIF, VC4	EX01, .E01, LX01, L01, SAFEBACK (001), VMWARE (VMDK), VIRUAL PC(VH)	IMG, DD, 001, AA, RAW, E01	IMG, DD, 00N, AFF, AFM, AFD, VMDK, E01, S01, VHD	RAW, DD, AFF, AFD, AFM, AFFLIB, EWF, SPLIT RAW, SPLIT EWF , P, PY, EWFMOUNT
TIME TAKEN FOR KEYWORD SEARCH (in seconds)	2	114	5.6	2	30
TIME TAKEN FOR VERIFICATION (in seconds)	33	36.2	24	2	42
IDENTIFY DELETED FILES	YES	YES	YES	YES	YES
RECOVER DELETED FILES	YES	YES	NO	YES	YES
MISMATCH EXTENSION	YES	YES	YES	YES	YES
IDENTIFY SLACK SPACE	YES	YES	NO	YES	YES
ABILITY TO BROWSE INTERNET HISTORY	YES	YES	YES	YES	YES
ABILITY TO BROWSE COOKIES	YES	YES	YES	YES	YES
LOG OF INVESTIGATION ACTIVITY	YES	NO	YES	NO	NO
SHOW FILE CREATED TIME	YES	YES	YES	YES	YES
SHOW FILE MODIFIED TIME	YES	YES	YES	YES	YES
SHOW FILE ACCESSED TIME	YES	YES	YES	YES	YES
IDENTIFY REGISTRY FILES	YES	YES	YES	YES	YES

SEARCH AND RECOVER RECYCLE BIN	YES	YES	YES	YES	YES
MOST RECENTLY USED	YES	YES	NO	YES	YES
FILE CARVING	YES	YES	YES	YES	YES
SEARCH UNALLOCATED SPACE	YES	YES	YES	YES	YES

We have analyzed five digital forensic tools, FTK 3.0, EnCase 4.20, Autopsy 3.1.2, OSForensics 3.1 and SIFT 3.0 on the basis of several functional parameters and made a comparison matrix, i.e., Table-1, which shows that open source tools are as good as the proprietary tools and thus, can be used in the legal proceedings. Table-2 shows the mapping of different parameters with the four phases of digital forensic investigation process (acquisition, preservation, analysis and reporting).

C. Mapping the parameters with the four phases of investigation

TABLE 2
PARAMETERS MAPPING

INVESTIGATION PHASE	PARAMETERS
Acquisition	1. Supported image format
Preservation	*Hashing*- By calculating the hash of the image and verifying it with the stored hash we can prove the integrity of the image which will mean that the evidence from the time of acquisition to the time analysis was not tampered in any way. 2. MD5 hash 3. SHA-1 hash
Analysis	4. Timeline Analysis 5. Repeatability 6. Reliability 7. Use of GUI vs. Command Line 8. Time taken for Keyword search 9. Time taken for verification 10. Identify deleted files 11. Recover deleted files 12. Supported File format 13. Supported Image format 14. Identify slack space 15. Browse internet history 16. Browse cookies 17. Log of investigation process 18. Show file created time 19. Show file modified time 20. Show file accessed time 21. Identify registry files 22. Search and recover recycle bin 23. Most Recently used 24. File carving 25. Search unallocated space
Presentation	26. Documentation 27. Reporting

IV. Conclusion

After the analysis of open source and proprietary source tools we obtained a comparison matrix which provides the overview of each tool based on the functionalities. After studying the table, we can conclude that many of the features that are present in closed source tools are also there in open source tools. There are certain other features which an open source tool provides but proprietary tool does not. Such as SHA-1 hashing is not there in EnCase but is available in the open source tools. Open source tools are easy to buy due to no or negligible cost. Other benefits of open source tool is that it takes less time to search keywords and for verifying the integrity of evidence which means that its processing time is less as compared to closed source tools, which is a the most required feature of any tool. This research is very helpful in proving the goodness of the open source tools with comparison to the proprietary tool and also in concluding its usefulness for fast and cheap solution to the society moving towards the imminent danger of epidemic of cyber-crime.

V. Future Scope

In the future, few other tools can also be used to give a more detailed result regarding the effectiveness of the open source tools. Many features of SIFT has not been studied, these may be used to give a better view of this tool; also several other features may also be included for comparison.

VI. References

[1] Atul Raj, Irman Ali, Praveen Kumar "Analysis and Comparison of Open Source and Proprietary Digital Forensic Tools" "in press spanda14"

[2] Colby Lahaie, Kyle Porto, and David Leberfinger "OSForensics Comparison"- Senator Patrick Leahy Center for Digital Investigation (LCDI)

[3] Dan Manson, Anna Carlin, Steve Ramos, Alain Gyger, Matthew Kaufman, Jeremy Treichelt "Is the Open Way a Better Way? Digital Forensics using Open Source Tools, Proceedings of the 40th Hawaii International Conference on System Sciences - 2007

[4] Palmer, Gary, "A Road Map for Digital Forensic Research," Technical report DTR-T001-0, Digital Forensics Workshop, Utica, New York, 2001.

[5] http://en.wikipedia.org/wiki/Forensic_Toolkit

[6] http://en.wikipedia.org/wiki/EnCase

[7] www.sleuthkit.org/autopsy/

[8] www.osforensics.com

[9] digitalforensics.sans.org/community/downloads/overview