A Review on: the Rise in Cyber Forensics & Innovations

Gyana Ranjana Panigrahi, Nalin Kanta Barpanda and Sambit Mishra

May 21, 2021

A review on:
The Rise in Cyber Forensics & Innovations

Gyana Ranjana Panigrahi
Department of Electronics
SUIIT
*(Sambalpur University)*Burla, India
0000-0003-2173-2545

Dr Nalin Kanta Barpanda
Department of Electronics
SUIIT
(Sambalpur University)
Burla, India
nkbarpanda@suniv.ac.in

Sambit Mishra
Department of Cybersecurity & Digital Forensics
CUTM
Bhubaneswar, India
192105290001@cutm.ac.in

***Abstract*— The extensive relevance of forensics in today's data-driven environment has been brought into focus in this article. Both freeware and profitable software are contentious fields, with opposing concerns about accessibility and security. This article has a primary goal of using pre-defined criteria and a platform-oriented approach and using it to examine profitable and freeware mobile forensic alternatives. Test conditions are put in place to ensure that the tools provide an inclusive approach to respond to digital problems and scenarios. Oxygen Forensic Suite and Prodiscover are considered profitable tools, whereas The Magnet Forensics and Sleuth Kit are considered freeware tools. The study concludes with a comparison matrix that may aid in determining the best-fit option for the investigation's requirements. This might suggest how freeware ones may replace many proprietary applications: Can proprietary software replace freeware tools? This might maybe be implemented.**

Keywords*— Digital Forensics, Oxygen Forensic Suite, Prodiscover, Digital Investigations, Cybercrimes.

I. INTRODUCTION

Smartphone forensics is an emerging discipline for digital forensics, dated from the early 2000s [1]. Digital evidence or data from a mobile device is analyzed and stored forensically. The cybercrime activities in mobile telephones have expanded exponentially, presumably as they are being utilized in many daily tasks, such as personal and business data storage and transfer, as well as in Internet-based communications [1][13].

Increasing at the rate of over three times faster than other threats has caused the mobile device to turn into one of the most prevalent weaknesses, with an alarming 188% increase in Windows Phone vulnerabilities and a 262 percent increase in iOS vulnerabilities 2011[2].

Several evidence and technological levels are an especially hard forensic investigation of mobile devices. Serious mistakes can arise with the forensic examination without the required knowledge, and key data might be removed and lawsuit results endangered. The document is broken down into six sections.

The first section provides an overview of digital developments and the purpose of this article. The following is a summary of the whole field research carried out. Section 3 covers the various tools utilized in this work in forensic mobile open source and commercial devices.

The above part covers the various phases of a forensic study and the key factors for evaluating the effectiveness and the feasibility of the instrument classes. The study environment is then outlined, consisting of several desktops and mobile devices. The major result of this study is the matrix for comparison and the conclusions derived from this study.

II. RELATED WORK

Numerous publications in cyber forensics demonstrate commercial or open-source digital forensic equipment and show the importance and effectiveness of solving crime.

The study "Mobile Forensics: an overview, tools, trending in the future and challenges in law enforcement" by Ahmed et al. (2008) emphasized the necessity for developments and weaknesses in mobile law-enforced research.

Williamson et al. (2006) released “Forensic analysis of Nokia handsets” When a series of software programs were selected for the examination, four were chosen: Oxygen Forensic Suite, Prodiscover, sleuth kit, and Magnet forensic.

This is done in work by Maurya et al. (2015), “An Analysis of Open Source and Proprietary Digital Forensic Tools,” in which a brief introduction of such forensic examination is presented, followed by a similar evaluation of FTK, Autopsy, SIFT, and OS Forensics is conducted, is provided."

Compared to those features, the cost, the MD5 hashing algorithm, general user-friendliness, and platform support "Survey on Mobile Forensic Phraseology: this study was written by Lohiya et al. (2015) mobile forensic tools, the procedure was defined in step-by-by-by-step process pictures. These cover the following: collection, exploration, data processing, and preservation.

III. Digital Forensic Suite Overview

The tools may be recovered from smartphones and produced reports, relying on excellent forensics procedures. These reports contain all data connected to the cash activities of the person and trip activities. Even a basic, extraordinary and sophisticated degree of expertise in addressing new difficulties is analyzed in the software tools. Software comparisons for certain tasks assist us in understanding its strengths and drawbacks. We discussed two free source tools and two commercial solutions.

A. Oxygen Forensic Suite

Oxygen Forensic Suite is the first smartphone forensics software that enables investigators to review all critical data in a centralized location. The Passwords section contains logins and passwords taken from the system's default safe storage, such as the keychain database. Additionally, application files may include this vital data.

B. ProDiscover Forensic

ProDiscover Forensic is an all-in-one digital forensics solution that enables analysts to extract crucial evidence from computing devices. ProDiscover is equipped to manage all facets of an in-depth forensic investigation, including collecting, preserving, filtering, and analyzing evidence.

C. The Magnet Forensics

Magnet encrypted disk detector is a wide, integrated platform for digital forensics. The only platform for PC, smartphone, and cloud in a single scenario gathers and processes data.

D. The Autopsy (Sleuth Kit)

It is a digital forensic software platform and gateway to other technologies. Computer forensics is widely employed by federal, local, state, and military forces and computer investigators in the business world. It is also possible to retrieve pictures from the memory card or camera. The best-in-class digital forensics platform is Autopsy. Built on the ground of Basis Forensic Technology, the customer's demands, Autopsy is a rapid, comprehensive, and competent computer forensic solution that stays ahead of the curve.

IV. The Investigative Proceedings

a) Stages of Forensic Examination

The authors developed relevant criteria for the comparison of the tools through a series of brainstorming processes. The measures so developed would assess the tool's potential as an integrative one that could be used to investigate any scale.

A typical forensic tool analyses the information gathered in order to generate the final evidence in the analysis process:

1) First Stage - Data sources and integration of existing data:

The initial stage is to physically / logically acquire data stored in various forms across several mobile devices. In this case, it may be required to unlock a smartphone and get info for encrypted information. It is essential to check the level of use of compatible devices. The computer then adds all the crumpled information to a report which may be used as evidence.

2) Second Stage – Information Execution:

This step analyses the retrieved data by executing several ingest modules. Speed and precision are obvious concerns for determining the tool's efficiency. However, uncontrolled occurrences (Power Failure, System Crash) may diverge from the regular procedure. Additionally, malicious harm to the gadgets being studied may be caused on occasion in order to block information execution.

3) Third Stage - Integrity authentication:

This type of testing may be used to determine whether a person is doing anything illegal and may then be employed to detect the corruptness (Criminal investigation is studied by gathering and analyzing data from real-world instances and then looking for common mistakes). First, fingerprints are generated and are compared to verify obtained data. The total amount of data should be consistent if the software is applied to the same number of items and/retrospect's of devices. This is a complete system to test the findings to see if the results are repeatable and whether they can be accepted as proof.

4) Fourth Stage - Exhibition:

Each reporting tool comes with several modules to aid in generating reports inside itself. The tools can link with external applications to enhance the reporting. The extent to which such partnership may be achieved can nonetheless vary. In the end, the dependability of its supplier depends on an essential consideration for selecting a tool. Therefore, adequate criteria are designed to monitor the effectiveness of these phases. The settings have been selected such that they are not too basic or too sophisticated. In the selecting procedure, there were no biases.

b) Criteria Description

The research parameter and assessment criteria for each of those metrics are mentioned below.

1) A Single Tool Data Integrations using Multiple Smart Devices/Sources:

Examining the tool's source coverage, Data formats may be held together using Data Support, allowing the organization to derive coherent and standardized results from several sources with varying degrees of validity and integrity [7].

2) The capability of Outpacing Cryptography & Account Logins:

It will be possible to overcome user-enabled credentials and their level locks, analyze the detectability of concealed files, detect and extract data using file-level encryption and obfuscation techniques.

3) Data accuracy and data extraction accuracy:

Average data acquisition rate measurement and data analysis stages, Accuracy assessment [8] of the data collected, Provisions for sorting and filtering [9].

4) Identification of data manipulation:

Could the application identify manipulation of digital photos, audio, and video files (Resized, Transformed, and Obscured)?

5) Governance of User Authentication:

More secure means that the integrity of the data can be verified in all of the integrity after files have been moved, the program verifies the multiple file level of file integrity, and if there are any difficulties, it looks for differences in file extensions [9].

6) Data Extraction Confidentiality with Extraction Methods:

It would help if you decided whether the user's identity may be exposed by applying logic, but also usefulness, in which case you may include a recovery feature to ensure that no form of the device or files are lost [10, 11].

7) Forensics Tolerance for error Tools:

The proportion of data gathered before and after the crash in the extraction or analysis phases occurs when crashes occur: Efficiency calculation (if any) of the backup [12].

7) Forensic Tool Alliance Characteristics:

Evaluation of the internal collaboration capacity of the forensic instrument, as measured by the amount and functionality of plug-ins, as well as its ability to collaborate with external applications.

8) Seller details (Updates, Security Data Storage, Integrity, Evidence Admissible):

The frequency and usefulness of the vendors' updates should be estimated. Obtaining an in-expand capability to detect security and multi-user functionality of the data storage systems determine factors involved in assessing vendor dependability concerning the number of reliable users. Verification by a court of law is accepted by both admissible evidence and acceptable evidence.

c) Plotting Attributes

Table-1 explains how to link the specified characteristics to the digital forensic research procedure phases

TABLE I. PLOTTING ATTRIBUTES

Integration of Source Information	1) Data integration with a single tool from several mobile devices/sources. 2) Capability to Bypass User authentication. 3) Extracted data privacy and extraction methods.
Data Interpretation	1) Data extraction speed and data accuracy 2) Forensic instrument fault tolerance
Error detection and correction, Authentication	1) Detection of data handling 2) Management of data integration
Exhibition	1) Forensic Instrument Integration Functionality
Additional Factors	1) Seller details (Updates, Security Data Storage, Integrity, Evidence Admissible)

V. TRAINING DATASET

The extent of support for the selected forensic instruments was checked during different computer and mobile devices in the implementation phase. The same calculation gadgets or smartphones do not have to be used in the future when dealing with identical systems.

A. Personal Computer Environment

Sleuth kits all need a computer to analyze data, examine findings, and prepare reports. All four forensic tools - Oxygen, Prodiscover - were commercial tools, while the Magnet forensics and Sleuth Kit, which was based on system investigation, and detection were utilized for processing and discoveries, as were the freeware. Sleuth Kit can only be used for Linux; thus, you will have to employ the Sleuth GUI version if your Linux machine can only be used in CLI, i.e., command line. The Oxygen Forensic and Prodiscover products, both of which could be utilized with Windows 10 workstations, were installed on the workstations.

B. Listing of Modern Smartphones

Modern PDAs used here in research are the Apple 11 Pro Max / 11 Pro. iPhone XR, iPhone 12 Pro Max, Galaxy A12, Galaxy A72, Samsung Galaxy A31, BlackBerry Evolve X, and BlackBerry Key2. To guarantee that the research's findings were genuine and similar to real-world practice as feasible, the phones used for this research were widely utilized by actual users before being employed in this research.

The tests were conducted not just on several operating systems but also on various operating system versions. As a consequence, only newer models of phones were selected. This is a purposeful attempt to compare the previous versions of the analytic tools.

B. Conduit-based Connecting Mechanisms:

A SCSI-based micro-type USB cable was necessary for the Android, the BlackBerry, and the Windows Phone, but the iOS phones required a Sync type 8-pin din USB cable.

Radiocommunication: The mobile device might be linked through Wi-Fi or near-frequency communication for various products such as oxygen or forensics.

VI. DIFFERENCE MEASURE

According to the authors' in-head study, a difference measure appears in Table II after a careful investigation of the freeware vs. profitable tools. This table depicts the different landscapes of each tool according to its role.

TABLE II. COMPARISON MATRIX

Norms	**Freeware Application**		**Profitable Application**	
	Magnet Forensics	***Sleuth Kit (Autopsy)***	***ProDiscover***	***Oxygen Forensic Suite***
Correctness	Less accurate	More accurate	Less accurate	More accurate
Support for Graphics and Videos	Existing	Existing	Existing	Existing
Availability of community assistance	Massive	Massive	Limited	Limited
Are the findings stable in several imaging?	Regularly	Constantly	Regularly	Constantly
Accessibility & readiness	Certainly	Certainly	Certainly	Certainly
Software's	accessible	accessible	accessible	accessible
Cloud Forensics	Partial Support	No	Yes	Yes
Geolocation Capability	No	Yes	No	Yes
Recovery rate in %	65	78	68	82
Password Breeching ability	File, User Level	Application, User & File Level	Application, User & File Level	Application, User & File Level
Owner tracing back capability	It can	No	It can	It can
Unallocated Data Carving Support	Yes	No	No	Yes
Multilingual Capabilities for Full-Text Search	Contemporary	Contemporary	Contemporary	Contemporary
Extensive Automation and Scripting	Not So Thorough	Very Thorough	Comprehensive	Comprehensive
Price	No	No	Costlier	Very Costlier
Integrated AI/ML Tools for Image and Video Analytics	Not Integrated	Not Integrated	Integrated	Integrated
Add on Plug-in Support	Not Support	Partial Support	Yes Support	Yes Support
Dead case efficacy	79%	81%	97%	100%
Explicit Smartphone Compatibility	No	Yes	Yes	Yes
Failure Resistance	Fewer	More	Fewer	Very Less
Hybrid Filtering ability	Better	Best	Excellent	Excellent
Social Media Artifacts	Plug-in to installed	NA	Integrated	Integrated
Hashing Mechanisms	MD-4, 5, SHA-1, 256	MD5, SHA – 1/256/512, MD-2, CRC32	MD 4,5, SHA – 1/256/384/512, MD-2, CRC32	MD 4,5, SHA – 1/256/384/512, MD-2, CRC32, RIPEMD 160
Core Competencies	Satisfactory	Sufficient	Outstanding	Outstanding
Automatic Report Generation	Manual	Manual	Automatic	Automatic
Is it an official?	Yes	Yes	Yes	Yes
can transcripts be customized?	No	Yes	No	NO

Norms	**Freeware Application**		**Profitable Application**	
	Magnet Forensics	***Sleuth Kit (Autopsy)***	***ProDiscover***	***Oxygen Forensic Suite***
Is the evidence acceptable in judiciary?	Absolutely	Absolutely	Absolutely	Absolutely
License required	No	No	Yes	Yes
Multiuser Support	Exist	Exist	No	No
CDR Analysis	Not possible	Not possible	Not possible	Possible
Weekly downloads	3890	5291	788	1267
Update Patches	Presented	Seldom	Presented	Presented
Acquisition ability Status	Encountered & acquired	Encountered only	Encountered & acquired	Encountered & acquired
CLI Console Support	Yes	Yes	No	No
GNOME Support	Yes	Yes	No	Yes
Protection Capability	Stable and highly matured	Stable and highly matured	Stable and highly matured	Stable and highly matured
Cataloguing ability	No	No	Exist	Exist
Scanning Speed	Moderate	High	Higher	Highest
Graph & Timeline Analysis	Yes	Yes	Yes	Yes
Location Visualization	Exist	No	No	Exist
SQLite Viewer	Exist	No	No	Exist
Merchant Support	Upright	Upright	Better	Best
Web activity detection	Exist	Exist	Exist	Exist

VII. CONCLUSION

For the choosing of forensic instruments, the 'one-size-fits-all method cannot be employed. Special attention is also necessary to identify some subjective aspects, such as resource availability, researchers' skills, the likely requirement for instrument-interoperability, and their application.

A series of significant freeware Tools components include a multi-user setting, CLI/GUI-based command/graphical interface, logging capacity, and better failure tolerance. Its popularity is due to the convenience of purchasing and the great support of the community.

However, good tools lead over their freeware equivalents by increasing their precision and agility throughout data mining and analysis, which define basic principles for examining forensic cases.

This is the most important attribute of the authors. Profitable tools may also aid by slicing file data, recovering deleted data, breaking user-level encryption by physical removal, efficient both dead and live analysis, and disclosing a person's identity. If adjustments are taken into consideration, we can witness a significant trend towards future use of more freeware technologies.

VIII. The FUTURE ENHANCEMENTS

Several other freeware and profitable tools are now accessible on the market for a wider range of criteria, which the authors have developed to extend and generalize the findings achieved in this research.

As updated versions and entirely new forensic instruments are introduced in the research, your answers may be verified for the simultaneous evolution and development achieved in mobile telephone technology. As cyber-crime continues to increase tremendously, the world might face modern and extremely developed bots in the future. The metrics that focus on these threats and concern them may thus be developed to indicate if the forensic instruments can battle these risks.

ACKNOWLEDGMENT

This study was performed for the author's thesis. The authors are grateful for their prompt advice, support, and direction from Project Supervisor Prof. Nalin Kanta Barpanda. Prodiscover and Oxygen Forensic Suite would also want us to access their newest commercial mobile forensic product for a 30-day free trial.

REFERENCES

1. Miller, C. (2013). The value of mobile data in criminal investigations. Accessed on, 12.
2. State of Mobile Security and What to Expect in 2015 | FireEye Inc
3. Ahmed, R., & Dharaskar, R. V. (2008, December). Mobile forensics: an overview, tools, future trends and challenges from law enforcement perspective. In 6th international conference on e-governance, iceg, emerging technologies in e-government, m-government (pp. 312-23).
4. Williamson, B., Apeldoorn, P., Cheam, B., & Mcdonald, M. (2006, April). Forensic analysis of the contents of Nokia mobile phones. In Australian digital forensics conference (p. 36).

5. Maurya, N., Awasthi, J., Singh, R. P., & Vaish, A. (2015). Analysis of open source and proprietary source digital forensic tools. International Journal of Advanced Engineering and Global Technology I, 3.

6. Lohiya, R., John, P., & Shah, P. (2015). Survey on mobile forensics. International Journal of Computer Applications, 118(16).

7. Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. NIST Special Publication, 10(14), 800-86.

8. Saleem, S., Popov, O., & Appiah-Kubi, O. K. (2012, October). Evaluating and comparing tools for mobile device forensics using quantitative analysis. In International Conference on Digital Forensics and Cyber Crime (pp. 264-282). Springer, Berlin, Heidelberg.

9. Pulver, A., & Medina, R. M. (2018). A review of security and privacy concerns in digital intelligence collection. Intelligence and National Security, 33(2), 241-256.

10. Croft, N. J., & Olivier, M. S. (2010). Sequenced release of privacy-accurate information in a forensic investigation. Digital Investigation, 7(1-2), 95-101.

11. Reddy, K., & Venter, H. (2009, January). A forensic framework for handling information privacy incidents. In IFIP International Conference on Digital Forensics (pp. 143-155). Springer, Berlin, Heidelberg.

12. “Data recovery.” Available from https://www.wikipedia.org.

13. Radhika Padmanabhan, Karen Lobo, Mrunali Ghelani, Dhanika Sujan, Mahesh Shirole. "Comparative analysis of commercial and open-source mobile device forensic tools," 2016 Ninth International Conference on Contemporary Computing (IC3), 2016