# A Comparative Study of Analysis and Investigation using Digital Forensics

Nikunj Pansari*1, Dr. Ajay Agarwal2

[1]*Software Engineer, Newgen Softwares, Noida, India*

[2]*Professor, IT Department, KIET Group of Institutions*

***Abstract*** — Data Analysis and Investigation using Digital forensics from Digital Storage Devices, is a defined way towards effective data backup strategies, as well as a key aspect in Data Privacy and Confidentiality. Digital storage Devices like Hard Drives (internal or external), USB Drives, floppy disks, etc. provide a good medium for better utilisation and storage of data and information. So, the main task is to retrieve the stolen or lost data from these devices. Digital forensics provides the exact concept for this data extraction, in a systematic and effective manner. Now, there can be various conditions of a damaged digital storage device like it may be burnt, wet or physically damaged parts, all these conditions play a significant role in Data Extraction. Since, Data is the most important asset for any organisation, so compromising with its Security and Confidentiality, may be wrong or devastating option, for future. Just spending thousands and millions of dollars in finding the vulnerability (large-scale or small-scale), is not a solution for being secure. There has to be proper and effective choice of ways and tools for it.

***Keywords*** — *Data Extraction; Digital Forensics; Confidentiality; Security; Tools*

## 1. Introduction

It is of paramount importance for a Cyber Security professional to undergo a thorough process of identifying, preserving, analysing and presenting digital evidence in a methodical manner. This process is known as Digital Forensics, which began in the 1970s. Collection of various types of electronic data stored and preserved for defining it, in a court of law, forms the basis of Digital Forensics [6][7]. Data is a major concern for any organization or individual. It is also the main module of the architecture and working of IT industries. Therefore, it is repercussions can't be ignored. The security of the Enterprise may include spending a huge Sum of money, but its byproduct would have saved them from, Data theft or loss. In evaluating large scale vulnerabilities, Data protection can be quite useful. Numerous tools are available for achieving this, namely WireShark or Network Miner, which will be further evaluated using Case Studies.We look at the various technologies used in the building of these tools like Virtual Machines, Embedded Systems, flash memory, flash translation layer, forensic acquisition and its analysis. Digital Forensics can be implemented using open-source and licensed tools. Few open-source tools like Wireshark and Network Miner are very much popular and are primarily used for most of the cases [7][8].

Wireshark is a Packet Analyser tool quite useful across different platforms. The main purpose of Wireshark is to monitor the network traffic, much like what firewall does in case of a Windows Operating System. It is used to thoroughly investigate, all the network related issues existing in that environment. For packet capturing, it can be operated on Windows, Linux or Unix, using widget toolkit and pcap files. Malicious and Suspicious content can be quite easily controlled using this tool [1][4][3][6]. Now, primarily for Windows, Network Miner Tool is used. Forensic Network Analyzer tool used for detecting open ports, sessions, host name and OS, using either packet sniffing or .pcap files. Also, it is quite useful for performing Advanced Network Traffic Analysis (NTA), by providing extracted artifacts in an interactive user interface [1][4][3][6].

Other Open-source Digital Forensic tools like Autopsy, which is efficiently used for Investigation of Data from Hard-drives and Smart Phones. It works by searching the index files and summarizing reports based upon its activities. Security Auditing tool like NMAP, primarily defined for monitoring of Network by service, operation system detection and host discovery. Latency and Congestion during scan are few Network Conditions, which can be easily adapted using this tool. For Encryption and Decryption, HashMyFiles are used and for Analyzing and Extracting browser based information and artifacts, Dumpzilla is used [1][4][3][6]. As an example, a tool like Wireshark can easily investigate network related issues and can access data in a clear and logical way. Similarly, a tool like Network Miner saves time for the forensic investigator and easily performs Network Traffic Analysis (NTA), unlike any other tool, which is extremely handy, when time is not in the hands of the investigators. It performs these tasks by providing extracted artifacts in an intuitive user interface. [1][4][3][6].

## 2. Investigation of Digital Forensic Framework

Cyber Criminals or Computer Criminals are the ones, who are the major reason behind the Cyber Crime, and are prosecuted by an essential framework called Computer

DOI: **10.30726/ijlca/v7.i2.2020.72004**

Forensics. There are strategies to effectively implement forensic Investigation, which are briefed using no of steps. These Steps form the basis of Evidence Collection and Acquisition, permissible in the court of law. Some defined and existing forensic models are analysed and adapted to form the basis of Entry point forensics or specific application framework [2][6][8]. There are following stages for Forensic Evidence to be admissible, for Investigation.

- *Preparation* - All the details regarding the Forensic analysis should be collected and strategies should be made for investigation scenario and Evidence Collection [2][6][8].
- *Investigation* – Investigation of the evidence should be effectively conducted, with the maximum chances of Data Retrieval, without actually tampering the Evidence, also[2][6][8].
- *Presentation* – A detailed report should be prepared for Evidence Analysis and summarised in the form, suitable for sustained Inference from the Evidence [2][6][8].

These steps would enable to conclude on a reasonable framework, which will be a path for proper Evidence Acquisition. They actually comply to the set standard of Forensics, and define the meaning of forensics. Now, if these processes or steps are not inculcated properly for Evidence Analysis, then there would be quite a lot redundancy and inaccuracy in the definition of a sustainable Forensic Investigation [2][6][8].

## 3. Analysis of Forensic Tools

Security researchers have defined proper mechanism for Investigation and Analysis of Digital Forensics tools. There are mainly 4 basic stages of Digital Forensics Investigation, to be followed to carry out most sustainable Forensic Analysis namely, Acquisition, Preservation, Analysis and Presentation [1][4][2][6].

Now, the tools used for Examination using Digital Forensics are FTK 3.0, EnCase 4.20, Autopsy 3.1.2, OS Forensics 3.1, SIFT 3.0, etc. This is considerable that the Open source tools would have less features and functioning as compared to Proprietary Tools, but this shortcoming can let open source tool of its downfall. So, different functionalities and parameters for effective comparative analysis of the tools namely, MD5 Hashing, SHA-1 Hashing, Platform Support for Windows OS, Platform Support for Linux OS, User-friendly, Time Analysis, Cost, License, Repeatability, Reliability, Documenting and Reporting, Use of GUIs vs Command Line, Supported Image and File Format, Time Taken for Verification and Keyword search, Identify and Recover deleted files, Mismatch Extension and Identify slack spaces, etc. [1][4][2][6].

The Investigation phase and its parameters play a key role in implementation of effective Digital Forensics Framework. Different tools differ in their functioning from each other as it may signify performing different operations, in certain Forensic circumstances. The epidemic of Cyber-Crime can be easily avoided by using proper and defined protocols for Forensic examinations [1][4][2][6].

## 4. Overview of Cloud Forensics

Forensic Analysis using Cloud Computing, paves the way for Cloud Forensics. Now, Cloud Computing is a generalised framework for defining network access dynamically to a shared set of computing resources easily configurable such as servers, applications, services and networks. Shifting the Organisational data to cloud can easily result in benefiting the organisation, for preserving confidential data. Various organisations provide these services like Amazon Web Services (AWS), Microsoft Azure Services, Google, etc. [4].

Cloud Forensics can be defined as the application aspect of Cloud Computing framework. It is defined cross-discipline between Digital Forensics and Cloud Computing. Now, various tools are defined for Cloud forensics namely, FROST, UFED Cloud Analyzer, EnCase SSS, Xplico, Bulk Extractor, TcpDump, Wireshark, X-Ray Forensics, etc. Various Challenges to Cloud Forensics make it slightly vulnerable for defining an absolutely secure framework, thereby which results in remains and requirement of Progressive dialog [4].

## 5. Case Study

In Network Forensic Analysis, in the ideal perfect case scenario, we can get our hands on perfect fidelity evidence, and we create a zero impact on the environment, also preserving the evidence along the way. But practically speaking, this is not possible. It is impossible to achieve an investigation with zero footprints. [1][4][7][9]. In the following case study, we will dive deep into the working of Forensic Analysis Investigators, real-life practical scenario-based implementation of the use of these tools. We will learn about various cases, and we will basically be dealing with open-source multi-platform tools like Wireshark and Network Miner [1][4][7][9].

### *5.1 Level 1: Secret agent- Rachel Greene*

Automobile leader in the industry, Impetus Inc. concluded that one of their chief engineers in the Research & Development Department, Rachel Greene, is suspected to be a turncoat and has switched sides to work for another

DOI: **10.30726/ijlca/v7.i2.2020.72004**

Chinese Automobile Company, Sungyong. Rachel, working in the R&D Department, has full control over the company's confidential details regarding the development to the company's prize asset, the magic ratio of the length, breadth and height of the cylinder piston which makes it far ahead of its competitors by delivering best- in-the industry performance. The apprehension of the Security Department of the company is that Rachel Greene, might misuse her power and sell the calculations to foreign company. [1][4][7][9].

The Department has been monitoring Rachel's whereabouts and her work and have finally discovered the entry of an unexpected Computer System in the Company premises. The Wireless Security of the company had been compromised for a brief time and it was found out that indeed there was an entry of a foreign computer system in the premises, which was found out later, to be used in the Canteen & Refreshments area. Also discovered was the fact that Rachel's IP address, (192.168.1.158) was used to transmit messages to this foreign computer IP. That was all that happened, and the foreign computer as gone from the radar in no time. [1][4][7][9].

*Following questions arises as:*
1. Rachel's Instant Message partner has
what name?
Sec558user1

2. Captured Instant Message conversation consists of what message?
Here's the secret ratio... I just downloaded it from the file server. Just copy to a pen drive
and you're good to go &gt; :-)
Page 13 of 19

3. Which file was being transferred by
Racheal?
ratio.docx

4. What is the secret ratio?
Ratio:
Dimensions:
4 length pistons up
2 breadths cylinders' down

To extract information from PCAP file, different tools like tcpdump, Wireshark, Tshark, etc are used. 'pcapcat' script in Perl (PCAP cat) which reads the content of a PCAP file and provides an overview for dumping content of a TCP stream into a file [1][4][7][9].

### 5.2 Level 2: Rachel on the Move

Further we can move forward with the study by building all possible scenarios where Rachel would try to escape legal actions from her Company, being the employee of the same. One
possible scenario could be something along these lines. Rachel had a pretty good lawyer to begin with and she took full advantage of that fact and got released on the bail. The investigators were not ready to give up either upon it. The good thing for them was that luckily, they were tracking down her network activities all throughout. We can figure out the following queries for the investigation to produce further in depth of this chain of events. [1][4][7][9]

1.What is Rachel's email
address?
sneakyg33k@aol.com

2. What is Rachel's email
password?
558r00lz

3.What is Rachel's partner's email address?
mistersecretx@aol.com
The smtp tool used, findsmtpinfo.py creates report of all the smtp information and stores
Information in message format and stores compressed attachments from emails in decompressed formats as well [1][4][7][9].

### 5.3 Level 3: Going Further Deep

Rachel and her partner have now decided to purchase a Smart TV. The investigators are waiting for Rachel and her partner's extradition paper work, while covertly monitoring her activity as well. What is of prime importance is that her Smart TV is being configured by a static IP address 192.168.1.10. Luckily for investigators, they managed to get a packet capture of their latest activity using Wireshark tool and saved it in evidence03.pcap file [1][4][7][9].

*The following questions can be answered about Rachel using the information provided to us:*
1. Rachel's Smart TV has what MAC address assigned?
00:25:00: fe:07:c4

2. In HTTP requests, Rachel's Smart TV used which User-Agent?
AppleTV/2.4

3. What were Rachel's first four search terms on the Smart TV?
h
ha
hac
hack

4. Rachel clicked a movie, titled what?
Hacker

We built up a simple tool with the help of Python which could parse a pcap and creates a report for each potential Smart TV client, also creating an overview report for each client.

## 6. Comparative Study of Tools

Table 6.1 shows the Comparative Study of Open Source Digital Forensic Tools and their effective implementation in different scenarios. It also depicts the various characteristics, functionalities and uses of these tools. It enables to define the appropriate tool for each situation like network forensics, computer forensics or finding the vulnerabilities in a website [1][4][7][9].

**Table 1: Comparative Study of Open Source Digital Forensic Tools**

| S.No. | Tool Name | Platform Supported | Version (Latest) | Description | Uses |
|---|---|---|---|---|---|
| (1) | Wireshark | Cross-Platform(Packet Analyser) | No version (as such) | It is a network capture and analyzer tool used to monitor the network. It is used to investigate network related issues. | Investigate network related issues. Can access Data(network packets) clearly and logically, to enable know it's working. |
| (2) | Autopsy | Open-source digital forensic tool and GUI. (Sleuth Kit) | 4.5 | It is used for the analysis of Hard Drives and Smart Phones, easily and efficiently. Used to investigate Data Theft from the System | Used for searching for index files and summarising a report(HTML/PDF) based on its activities. |
| (3) | Encrypted Disk Detector | Command-line tool | V2.2.0 | It is used for further investigation to define live acquisition, made to secure and preserve the evidence, that might be lost. | Used for Investigating Encrypted physical drives.(Supported formats:TrueCrypt, PGP, Bitlocker, Safeboot encrypted volumes). |
| (4) | NMAP | Cross-platform | v7.70 | Nmap(Network Mapper):monitoring of the networks and security auditing tool. | Used for probing computer networks, including host discovery, service and operating system detection. Network conditions such as latency and congestion during the scan can be adapted by this tool. |
| (5) | Network Miner | Forensic Analysis tool for Windows (but can also work for other platforms) | v2.3 | Network forensic analyzer used to detect hostname,OS,open ports and sessions by either .pcap files or packet sniffing. | Saves time for the forensic investigator and easy to perform advanced Network Traffic Analysis (NTA) by providing extracted artifacts in an intuitive user interface. |
| (6) | Magnetic RAM Capture | Windows XP, Vista, 7, 8, 10, 2003, 2008, 2012 (32 and 64-bit support) | No version specifically. | It is used for capturing and analyzing the physical artifacts in memory of a computer. Some Evidence acquisition activities can be registry hives, malware intrusion, decrypted files and keys,etc. | Primarily used for evidence acquisition and volatile storage of RAM for analysis and investigation. |
| (7) | USB Write Blocker | Supports any hardware and software. | Forensic tool (No version) | Viewing the USB drive contents and changes to timestamp and metadata. It uses the Windows registry to write-block USB devices. | It facilitates the analysis and acquisition of data on a drive without actually tampering the shreds of evidence or the data. |
| (8) | NFI Defraser | All platforms | v1.2.7 | A forensic analysis application that can be used to find (and restore) complete or partial video files in datastreams (for instance, unallocated diskspace). | Used for analysis and detection of partial and full multimedia files in the data streams. |
| (9) | Dumpzilla | Mozilla browser forensic tool (Unix and Windows 32/64 bits' systems) | No specific version | It is used for extracting and analyzing the browser-based artifacts and information. | It will show SHA256 hash of each file to extract the information and finally a summary with totals |

DOI: **10.30726/ijlca/v7.i2.2020.72004**

| | | | | | |
|---|---|---|---|---|---|
| (10) | HashMyFiles | All latest Windows OS. (Windows 2000/XP/2003/Vista/Windows 7/Windows 8/Windows 10) | v2.31 | Used for calculation of MD5 and SHA1 hashes. | Used in encryption and decryption purposes. |
| (11) | FAW (Forensic Acquisition of Websites) | All platforms | Professional and law enforcement | It captures the entire or partial page, HTML source code, different types of images and can easily be integrated with Wireshark. | Used for acquiring web pages for Analysis and Forensic Investigation |

## 7. Conclusion

The forensic analysis provides a domain for defining the repercussions of data loss or data theft. Now, it can be a vital breakthrough if people are made aware of all the advantages and disadvantages of digital forensics and especially when it comes to the data security domain. Secondly, hard drives, USB drives, and other digital storage devices provide a path for data accessing and retrieval but can also prove to be a disaster when it comes to the loss of most important part of any system or workspace. Defining tools for implementing digital forensics at an organization, criminal investigation or on an individual level are developed, where some are the proprietor and some GPL. Various branches of digital forensics also defined as a solution for maintaining integrity at different levels of software development. Different stages of digital forensics also define a relationship and inter-dependence of data retrieval or extraction scenario through its effective and secure implementation. All the services provided by Digital forensic are evaluated and helpful enough to access the various domains of data or individual property loss related to data and cyber-crimes, which includes forensic analysis. In this study, one can figure out, with practice, implementation and skill, as to which tool, can be used for what particular purpose, be it Mobile Forensics, Network Forensics, Computer Forensics, Network Forensics or Database Forensics. This is because different tools have different pros and cons and all of them work differently, and are used for different purposes.

## Acknowledgements

I would like to express my heartiest gratitude to all the highly experienced preceding paper authors. These papers and references have defined me a path towards effective models and strategies in Digital forensics. It would have been quite difficult for me without the kind support and help of many individuals. Analysing these papers and articles has helped me in defining this comparative study of tools. Big thanks to Prof. Ajay Agarwal, the mentor for this research and Prof. Adesh Kumar Pandey for guiding me proactively to pursue this research work. They have always been a keen supporter and motivated me as a researcher in this field, trying to figure new ways of research strategies.

## References

[1] Analysis of Open Source and Proprietary Source Digital Forensic Tools by Neelam Maurya , Jyoti Awasthi , Raghvendra Pratap Singh , Dr. Abhishek Vaish. International Journal of Advanced Engineering and Global Technology I Vol-03, Issue-07, July 2015 [ISSN No: 2309-4893].
[2] Framework for a Digital Forensic Investigation,Michael Kohn, JHP Eloff and MS Olivier, Information and Computer Security Architectures Research Group (ICSA),Department of Computer Science,University of Pretoria
[3] A Review and Comparative Study of Digital Forensic Investigation Models, Kwaku Kyei , Pavol Zavarsky , Dale Lindskog, Ron Ruhl, Information Systems Security Department, Concordia University ,College of Alberta, Edmonton T5B 4E4, Canada.
[4] Comparative Analysis and Study of Forensic Investigation Tools: A View, Ms. Neha N. Agrawal, Dr. R. N. Jugele, International Journal of Computer Technology & Applications,Vol 9(3),75-79 [ISSN: 2229-6093].
[5] A Comparative Study based Digital Forensic Tool:Complete Automated Tool by Nilakshi Jain1, Dr. Dhananjay R Kalbande, The International Journal of FORENSIC COMPUTER SCIENCE, IJoFCS (2014) 1, 22-29.
[6] https://www.digital4n6journal.com/
[7] https://www.guidancesoftware.com/blog/digital-forensics/
[8] https://www.intaforensics.com/digital-forensics/
[9] https://en.wikipedia.org/wiki/List_of_digital_forensics_tools

DOI: **10.30726/ijlca/v7.i2.2020.72004**