IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12642

A Study on Digital Forensic Tools

SOURABH SHIVAJI KATKAR[1], DR. RAMA BANSODE[2]

P.G. Student, Department of Computer Application, P.E.S. Modern College of Engineering, Pune, Maharashtra, India[1]

Assist. Professor, P.E.S. Modern College of Engineering, Pune, Maharashtra, India[2]

Abstract: The risk of data misuse is growing in tandem with the exponential growth in data storage and utilisation in the modern world. As a result of this, data kept on controllers, mobile devices, or computers, whether it was acquired by humans or machines, is susceptible to numerous cyber-attacks. There are several digital forensic tools available nowadays that assist with conducting investigations by gathering evidence using various techniques. The numerous digital forensic tools that businesses, governments, and individuals employ to gather, extract, and present the information gathered are thoroughly examined in this paper. In this work, we also assess the forensic tools using several parameters so that customers may quickly choose the tool that best suits their requirements .We also briefly talk about some of the challenges people face in using digital forensic tools.

Keywords – Digital Forensics; Tools; Software Development; Forensic phases; Benchmark.

I. INTRODUCTION:

The creation of software application tools and computer forensics tools is the most exciting technical advancement in digital forensics. Controllers on industrial machines, autonomous devices, personal computers, mobile devices, computer networks, cloud based systems, and servers are a few examples of the platforms on which the data are kept. The preservation of the original file or data once the data is recovered from these devices is one of the main features of the various types of digital forensics tools that are readily available on the market. To ensure that the extracted data was not corrupted or altered, they can be compared with the original data. A digital forensic tool's main goal is to prevent identity theft, money laundering, and invasions of privacy, blackmail, and unauthorized access. Unauthorized access to confidential information, preventing Sexual harassment, Corruption and many such cybercrimes where digital data and sensitive information are involved. Hacking was a term that was gaining spotlight in the 1960s. With this, several researchers began their study of hacking and were successful in compromising a system's security. Crime by Computer, on the other hand, was published in 1976 by Donn Parker. A straightforward framework was given to the US Department of Defense so that they could check the access logs on the data that was being kept. While using digital forensic tools, there are a few fundamental concepts to keep in mind. Data shouldn't be changed once it has been obtained. People who use digital forensic tools ought to keep records of everything they do. And the fundamental tenet is that, in order to prevent any tampering with or changing of the evidence, access to the original document should be restricted.

II. LITERATURE REVIEW:

Depending on who you ask, the term "computer forensics" can indicate a variety of things in the field of forensic science. Although it is best described as "the application of scientifically derived and proven methods to the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of criminal events, or assisting in the anticipation of unauthorized activities shown to be disruptive to planned operations" Computer forensics, mobile device forensics, network forensics, and database forensics are all subfields of digital forensics. That examine various tools, media, or data. With the development of digital forensics and its applications in business, new tools focused on various forensic-related issues started to appear on the market. Why because storage space is growing exponentially larger, scanning the device and making a disc image of the device will take longer. • There will be a problem creating the device's image as implanted flash drives become more and more common and the hardware interface streamlines. Another area of concern is the growing usage of encryption methods. The lost encrypted data may be retrieved, however there may be an issue when attempting to decode that data. • Cloud storage is becoming more popular. Finding the segments during analysis can be challenging due to the data being stored across numerous cloud segments that are dispersed over the network. The procedure and flow of a digital forensic inquiry are described by Vishal R. Ambhire and Dr. B.B. Meshram in their study, Digital Forensic Tools. Once an incident is reported or a crime is discovered, the process begins. Following that, it continues in the flow seen in Fig.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12642

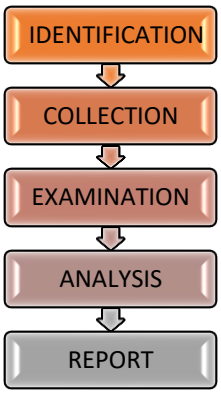

Fig. The investigational method of digital forensics

III. DIGITAL FORENSIC TOOLS:

Cybercrime is a term used to describe any crime that involves the virtual world. Digital forensics is the name of the procedure used to find this crime. Digital forensics often comprise data preservation, extraction, identification, analysis, and report generation. The following are the tools that we examine.

A. Encase

Encase was made by Guidance Software. One of the most frequently utilised forensic tools worldwide. Encase is actually used by 90% of consumer goods corporations worldwide, 93% of banks, 100% of federal organisations, 75% of power providers, and 80% of American universities. The investigation lifecycle is essentially the same as what is being presented, with the investigation coming first, followed by data collection, analysis, and report generation.
The following are the features of the Encase Forensic:

- Able to collect data from a wide range of sources, including networks, clouds, and mobile devices
- When conducting research on a targeted device or collection, it makes advantage of metadata, keywords, and hash values while maintaining the integrity of the evidence.
- Can do disc imaging and memory acquisition

B. Forensic Toolkit (FTK)

The creators of FTK are Access Data Group. They are the main source for forensics tool certification and training. Law firms and over 130,000 governing bodies use FTK globally. It is capable of doing analysis on mobile devices, network connections, personal PCs, and laptops. Searching and filtering are performed more quickly than with any other tool. The characteristics of FTK are as follows: It has the ability to gather data from 3,500 mobile devices and store it throughout the network.

- It is able to quickly identify missing data, vindictive behaviors, and data leaking.
- It can easily identify if any data has been transferred from the system or mobile device.
- It can even gather information during static analysis.
- One can run FTK from a USB drive.
- It has the option of expert review, where reviewing will be done and compared with the witness on the final analysis of the evidence
- Recovery of passwords
- It can analyse emails.

C. Digital Forensic Framework (DFF)

An open source forensics platform called the Digital Forensics Framework was created using a unique application programming interface. Mostly employed by commercial businesses, educational institutions, and police enforcement agencies worldwide. DFF, which is free, DFF Pro, which costs €1,000 for a year of support, and DFF Live, which costs €1,300 for a year of assistance, are the three alternatives offered. When compared to DFF Pro and DFF Live, DFF Free does not offer any professional support, report editor, automation engine, user activities reporting, hash scanner, or Skype analysis. The characteristics of DFF are as follows: It contains the following capabilities: Computation of cryptographic hashes, extraction of EXIF meta-data, importation of all Microsoft Outlook mailboxes, analysis of memory dumps, scripting and batching capabilities, intuitive reporting of important data, and online browsing. Data may be automatically extracted, and research can be done both during live and static analysis.

DOI: 10.17148/IJARCCE.2023.12642

D. SANS Investigative Forensic Toolkit (SIFT)

An international group of professionals created SIFT. One of the most popular open source forensic tools is this one. It was found to be an incident response workstation and subsequently made accessible to everyone. SIFT has the following characteristics:

- Is capable of live analysis
- It has several useful features
- Quick Report and Analysis
- Malware Detection
- Disc Imaging
- Recall Framework

IV. ATTRIBUTES:

Platform:

A platform is nothing more than a hardware and operating system combination that enables the execution of all applications. In the past, programmes that are written for one platform could not be used with another. However, programmers are developing new frameworks that enable the programmes to run on several systems. Similar to this, all digital forensic tools require a platform in order to do analysis. The tools are created using a variety of operating systems, including Windows, Linux, Mac, and DOS Machine

License:

There are two divisions: open source and proprietary. The software that can be downloaded for free is open source, whereas the proprietary software costs money to download. There will be alternatives like monthly or yearly subscriptions in this situation, where the user will also need to pay for services. Many tools have free or limited service versions called "basic" that were made available by the developers.

Disk Imaging:

The reproduction will be the whole image of the disc or drive. On the CD, copies are made of all the data and software places. The forensic experts dissect the disc imaging segment by segment for investigative purposes. The copying process does not change the original disc in any way. Selecting the appropriate tool is an important step in disc imaging.

Data Recovery:

Data that has been erased can be recovered. A forensic investigator can restore data using a variety of recovery techniques from hidden data, corrupted devices, and other sources in order to gather evidence.

Password Recovery:

The developers' main obstacle is swiftly recovering the password. Numerous tools use various setups and methodologies for password recovery. Live mail passwords, Wi-Fi passwords, and even product keys are recoverable. Table 1 displays the analysis of several digital forensic tools using a few characteristics typically needed or used by the customer. The client can save time by using this table to decide which tool will be most beneficial for their problem

Email Analysis:

The forensic officer can analyse client emails with the use of some instruments. This functionality makes it possible to recover deleted emails and determine where they originated.

V. ANALYSIS:

The reference has discussed the potential crisis for the developer. Therefore, we have contrasted the difficulties with the current state of the instruments at our disposal and proposed which framework is useful in fixing the issue. The tool's time-consuming process for analysing the gadget was the first issue they talked about. En Case, DFF, Pro-Discover, FTK, Bulk Extractor, X-ways Forensics, The Sleuth Kit, and Windows SCOPE are the tools that have overcome the time barrier.

The operating system was the second obstacle listed in. En Case, for example, can function on Windows, Linux, Dos, and MAC. Similar to this, there are other tools that support different stages, such as DFF, Pro-Discover, Xways Forensics, FTK, The Sleuth Kit, and Bulk Extractor.

If the files are not stored on the same machines, it presents the third issue outlined in. There should be some sort of forensic tools that can extract the information from these networks, for instance, if a file is saved on computer A and a related file is maybe stored on computer B. Encase, Quest Change Auditor, Window SCOPE, X-ways Forensic, and FTK are the tools that are used to extract these files from various machines.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12642

What if the data is kept in the cloud? Is the fourth problem raised by the writers in . Encase, Quest Change Auditor, Windows SCOPE, and Bulk_ Extractor are the tools used to tackle this situation.

VI. CONCLUSION:

We have examined numerous digital forensic tools and created a benchmark by contrasting them against one another in terms of key characteristics. Encase and FTK are the commercial products that are used the most frequently, and the bulk of them work with Windows operating systems, followed by UNIX/Linux, Macintosh, and others. We have also talked about the difficulties that developer's encounter and the problems that still need to be resolved. Based on the specifics of the inquiry, our findings could be utilised to choose the best instrument for a certain circumstance.

It can also be used by the tool's creators to create more versatile tools with the capacity to target several domains. The researchers can compare their tools to others using our findings as a guide, which might lead to better features for their tools.

VII. REFERENCES

[1] Vishal R. Ambhire and Dr. B.B. Meshram, "Digital Forensic Tools", IOSR Journal of Engineering, Mar, 2012, Vol. 2(3) pp.392-398

[2] Varsha Karbhari Sanap, Vanita Mane "Comparative Study and Simulation of Digital Forensic Tools", International Conference on Advances in Science and Technology 2015 (ICAST 2015)

[3] Charles W. Adams, "Legal Issues Pertaining to the Development of Digital Forensic Tools", Third International Workshop on Systematic Approaches to Digital Forensic Engineering, pp.123-132.

[4] 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, Jan. 29, 2007.

[5] George Grispos, Tim Storer, William Bradley Glisson, "A comparison of forensic evidence recovery techniques for a windows mobile smartphone", Digital Investigation, Volume 8, Issue 1, July 2011, pp. 23– 36.