International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Digital Forensics Tools

Vedanta Kapoor, Sanya Taneja, Kakelli Anil Kumar

Abstract*: *In this paper we will we reviewing the basic fundamentals of digital forensics and all go through the various types of forensics investigation teams available to us. We will also discuss about the different types of digital crimes that take place and the various tools present in order to counteract the crimes that are being committed. There will also be a comparative review among all the tools present based on various factors present giving the reader an abstract view about which tool to use for the best type of results.

***Keywords*: *Cyber-crime, Digital, Forensics,* Tools**

I. INTRODUCTION

Digital forensics is a branch of computer science which is used mainly for the identification, recovery, investigation, validation and complication of the information gathered by the research work done to gather the evidences for the crime committed. It would be wise to say that digital forensics is a sub -branch of Forensics Science. Digital Forensics was born due to the revolution of Computer Sciences which meant that as the Computer Science field progressed to greater Heights of innovation the need to protect enormous data emerging was a must, therefore in order to submerge and reduce the amount of crime that could take place on a computer the Branch of Forensics Sciences was introduced.

A digital forensics investigation goes through a lot of phases for the final report to be generated. Once the crime has been committed and a forensics team is asked to report on the site of the crime. The digital forensics team sends in their agents commonly known as the First Respondent. The Job of the First Respondent is to analyze the situation and seize and all the available resources present of the site of the crime it can be anything ranging from the hard-disk of a computer to the entire computer, PDAs, Personal Cell phones anything that could have been used to commit the crime. The second step taken by the First Respondent is to assign the case to the team that would handle the situation most aptly.

There are a lot of different branches of Digital Forensics similarly a lot of different branch of people to handle all the different crimes that are being committed under these respective branches.

The various branches of Digital forensics are:

- Email Forensics
- OS Forensics
- Cyber Forensics
- Cloud Forensics

All the mentioned branches play a very important role when it comes to managing the security of a firm or a given individual, therefore it is vital for a digital forensics investigator to be thorough with all the branches mentioned above.

i. EMAIL FORENSICS

These days due to the rise in e-commerce and the digitalization of the society its very important for us to protect ourselves against fraudulent e-mails. Most of the communications takes via emails and has become one of the primary means of communications among two individuals, companies, banks. Hence it is very important to have email forensics.

The different types of crimes that are committed using emails can be as follows

- Phishing
- Pharming
- Spoofing

Phishing- As the name suggests Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication. It's one of the most common method used for the commitment of email crime. Emails usually contain text which redirects the user to a website in order to steal his/her details

Pharming- Pharming is commonly known as the method to redirect the traffic of a website to another website that that has malicious intents of stealing the users information. Similarly, Pharming is done using fraudulent emails which redirects the user to an unknown website have might have potential threat to the user and might have malicious intents of stealing his/her sensitive information.

Spoofing- It's of the methods where in the user receives a mail thinking it's from the trusted sender or a known individual whereas it is from a unknow person with wrong intentions using a forged sender address. Its very easy to carry out spoofing because the core email protocols do not contain any mechanism for the authentication against forged email addresses.

A few examples of Email Crimes are

- Narcotic Trafficking
- Child Abduction
- Pornography
- Terrorism

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
Vedanta Kapoor*, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India. Email: vedantkapoor98@gmail.com
Sanya Taneja, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India. Email: sanyataneja32@gmail.com
Kakelli Anil Kumar, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India. Email: anilsekumar@gmail.com

In case of an Email Fraudulent the first respondent assigns an email, forensics investigator who has to go through a series of step to find out the main source of crime.
The few methodologies and step taken by them to trace the root cause is as follows
1. Exploring the role of client and server in E-mail
The client could have been any sort of tool for the exchange of emails like outlook, evolution, lotus and all these applications/tools have different strategies when it comes to extracting information from them.
2. Examining E-mail Message
It might include getting the copy of the email for the further investigation, and in case of a deleted or missing email the forensics investigator might even have to recover the deleted email.
3. Viewing E-mail Header
It is important to have a copy of the email header before the investigation starts. Every email service provider has a unique method which needs to be followed in order to get the header required for the investigation. A Email Forensics Investigator should be thorough will the all the method present.
4. Tracing an Email Message
Tracing means finding the origin of the message. It is done by using a registry site like for e.g. www.arin.net to find the point of contact.
5. Using the Network email logs
6. Using various Email Forensics tools like

- DataNumen for Outlook and Outlook Express
- FINALeMAIL for Outlook Express and Eudora
- Sawmill for Novell GroupWise
- DBXtract for Outlook Express
- Fookes Aid4Mail and MailBag Assistant
- Paraben E-Mail Examiner

ii. OS FORENSICS

An operating system is a software or a program that link and controls the hardware and other software on a computer. An OS is present on all computers and computer like devices be it a smart watch, smart phone, smart fridge etc. Since the presence of an operating system is like basically everywhere, it is very important to have forensics system that governs the wellbeing and monitors our actions and the processes that goes on in our computer to avoid any sort of data loss or malicious acts that might happen in our system.
Like any other forensics operation OS forensics also deals with monitoring and examining the actions of a person. Whenever a person carries out an operation it leads to an action or event being created in a operating system, what OS forensics basically does is understands how system changes results due to the action done by a person in the real world.
For Eg:
If we have suspect who we believe is smuggling weapons or arsenal online illegally. We can use OS forensics to investigate his system in order to find proof to solidify our assumptions.
To perform OS forensics, it's important for an Investigator to know the following:
1. NTFS- NT File system. Windows XP used NTFS it is a set of important files that store information like the last log in date and time stamps which can be a very important asset when it comes to investigating criminal cases.
2. Window Registry- Registry of an Operating System is its heart and soul. One could extract a bundle of very important information of the registry of a computer.

Window Registry Contains Information like:

- System configuration
- Devices on the system
- User names
- Personal settings and browser preferences
- Web browsing activity
- Files opened
- Programs executed
- Passwords

All the mentioned information is very essential and helpful when it comes to doing an Operating System Investigation.
3. Window Events Log: It contains a log of all the vents that take place inside a system of the user. It records and logs all the details like log in log out time. The files that are being accessed etc.

iii. CYBER FORENSICS

Commonly also known as computer forensics it one of the main branches of digital forensics. Crime committed using computer and internet which has a hidden and foreseen motive of stealing someone's personal information. Cybercrime which is committed has various branches like:

- Against Person
- Against Property
- Against Government

To counteract all these crimes and to prevent them from occurring again and again digital forensics created a branch called cyber forensics which deals will the above-mentioned crimes.
There are various cyber laws that a forensics investigator should be known with in order to make process a little easier and classify the and flag the crime committed under the given section and thereby carrying out the required procedure.

iv. CLOUD FORENSICS

In today's world where everyone is switching to cloud for storing data it is very important that we have a governing body protect us from stealing the sensitive information. From individuals to big MNCs all are shifting to cloud for the storage of data.
Cloud forensics is basically a mix of cloud computing and digital forensics. Cloud Forensics is a branch/application of digital forensics that handles the crime committed over the cloud and investigates it. When it comes to cloud forensics there are three main subparts that need to be understood in order to manipulate and handle the investigations namely.

- Technical
- Organizational
- Legal

II. LITERATURE SURVEY

Nowadays, computers have become an integral part of our day-to-day lives, and it is very likely that [1] digital evidence will be required in case of any cyber-crime like phishing, illegal downloads, industrial espionage, fraud, terrorism among a few. With the increase in the number of crimes, corporate IT systems need to incorporate more features in order to be able to re-trace the steps of offenders. Whether it is a personal mobile phone or a group of computers linked in a corporate work environment, adequate security measures need to be put in place to avoid any sort of attack. All this leads to the rise of digital forensics tools which help in collection of digital evidence and eventually lead to a conclusion.

[2] Autopsy is one of the software tools used for this purpose. It is a platform for digital forensics which is used by military, law firms and examiners to look for evidence regarding the attack occurred. It also provides a graphical user interface to The Sleuth Kit, which is a Unix and Windows based library used for forensics analysis. After the forensics search is carried out, the results are displayed on the GUI making it effortless for the examiners to mark important parts. This tool follows four basic guidelines- Extensibility, Centralization, Ease of Use, Access by Multiple Users. Customization is also a feature which helps enable the user to add open-source modules for ingesting files, viewing and reporting results. It is highly recommended to use Autopsy when examiners are working with multiple file systems and machines so that a central location can be made which allows to store the marked data. Further, the use of SQL Lite or PostgreSQL databases enables more easy access to the stored information. It also maintains the evidence integrity by performing file and directory level hashing. Being available free of cost with an easy and fast interface, it is used widely.

Another tool used by digital forensic experts is ProDiscover, an ARC Group's next-generation solution to crime against computers. It is used by law agencies and investigators to diagnose data on hard disk and protect the evidence. This evidence is further used to create reports to be presented in law proceedings. These reports are automatically generated for quality reference. It is used by Windows, MAC and Linux file systems. [3] It is available at a low cost and combines speed with easy and flexible usage. It has the industry's best capabilities and makes sure none of the file data is altered while the file is being viewed. To further ensure the integrity of files, MD5 hash of each file is taken. In addition, the search capability enables fast search for any word or sentence, available anywhere on the disk. It supports features of recovering the deleted files, and dynamic previewing data. As the data cannot be hidden from this software, it is considered as one of the top digital forensic tools. Complexity of networks is rising day-by-day and new attacks are getting launched to steal information and hijack machines.[4] This causes a severe problem for not only the users but digital forensic experts who need to find the source of attack. In order to find the origin point, packets travelling across networks need to be captured. This is where Wireshark (formerly known as 'ethereal') comes into place, it is a software tool used to capture, analyze and filter packets, such that attacks can be detected. It is also used to inspect network traffic and displays everything in real-time. It plays a major role in network forensics industry, for example, in finding and displaying emails which can be used for evidence against attackers. Also, IP or MAC address can be identified to use it as a network monitoring tool. It is a robust software which has the capability to read live data and capture raw traffic as well. TShark is the GUI of Wireshark to view and edit the captured packets. Additional features sch as color coding and filters greatly help in detecting the packets. Thus, Wireshark has uses not only in network detection but also in defense and protection.

There are times when investigators aren't able to locate relevant data for an investigation which may be hidden or buried. Finding this data becomes easy with the help of EnCase Forensic which is a powerful platform for finding data, performing analysis, preparing reports and finally preserving them in such a way that it can be used in court directly. It is mainly used to recover digital evidence from enclosed hard disks by in-depth analysis. It is a multipurpose tool with six phase investigation life cycle- Forensic triage, Collect, Decrypt, Process, Investigate, Report. [5] EnCase is a technology and also offers training and certification courses including products such as EnCase Forensic, EnCase Endpoint Investigator, EnCase eDiscovery. Around 100000 people have trained under the certification provided by EnCase. Expert Witness File Format is supported which is used to analyze the media by creating forensic images. These images have. ex01 extension. It is the only tool which also supports mobile analysis. Furthermore, it has the capability to acquire data from any source be it disk, image, e-mail or even servers. In order to verify the data, it uses Forensically Sound Acquisition which generates a duplicate of the original media and then hashes it (MD5) to check if it is the same or has been tampered with. It is one of the most trusted software because of its easy to use interface and flexible reporting options. However, it is costly and the latest versions are not usually compatible with other software.

Another multipurpose tool is Forensic Toolkit i.e. FTK, which is the only software that uses multi-core CPUs to parallelize actions. This leads to performance boost and reduces the time of investigation. Documentation reports 400% less investigation time as compared to other tools. It is made by AccessData. It is completely database supported with one shared case database, i.e., all data is available to use for all at one single place. [6] Not only does this save the organization's resources in creating multiple datasets but also increases the efficiency of the work. Speed and Performance are the main goals of FTK; thus, it focuses on indexing the file before-hand, which greatly reduces speeds. It can work in-hand with eDiscovery and mobile. This all-in-one investigation solution has built-in support for email analysis, file decryption, data carving, data visualization, web viewer, Cerberus and OCR. In addition, it has FTK Imager which is used to store images of drive in a document and view it later by computing MD5 hash of it. Yet, it does not have a progression bar and hence there is no way to see much time is remaining for the task to finish. Easy to use GUI and advanced filtering search options make it the go to software for digital forensics.

III. COMPARATIVE STUDY

Results are in minutes: seconds or hours: minutes: seconds for searching terms

Table 1. Encase vs FTK

Program	8 terms	34 terms	Resource usage	Time to verify test image (ERZ)
EnCase 8	2:36	3:31	~45% CPU and ~4300 MB memory	1:50
FTK 6	1:05:27	3:56:03	95%CPU and ~500 MB memory, then down to 25% after first third of processing time	0:51

Table 1. shows that search time for relevant/hidden terms is a lot higher for FTK than Encase. This is because FTK has stability issue and it crashes while processing and indexing of data. This makes FTK really slow as we can observe in the results.

Table 2. Autopsy vs EnCase

Program	Cost	Speed	Memory usage
Autopsy	Free	Very fast	813 MB with case open, indexing not applicable
EnCase 8	Very Expensive	Slow	5800 MB with case open, 15,900 MB during indexing

Autopsy is used for finding digital evidence while EnCase is used to process the evidence. Results show Autopsy is faster than EnCase and takes less memory however it does not support advanced features like EnCase.

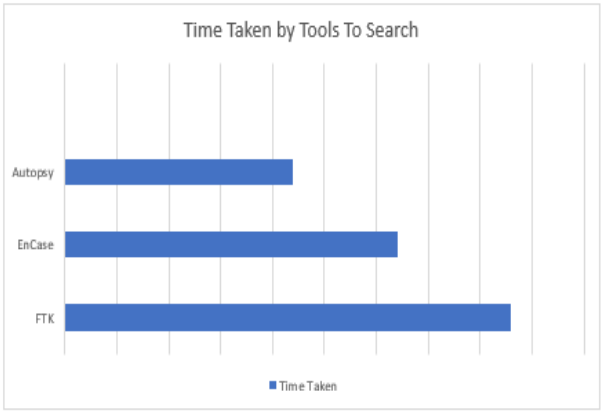

Fig. 1. Time Taken by Tools

From Table 1 and Table 2, we observe that Autopsy takes the least time followed by EnCase and finally FTK. Autopsy is easily available with an easy interface however for additional features, EnCase should be used.

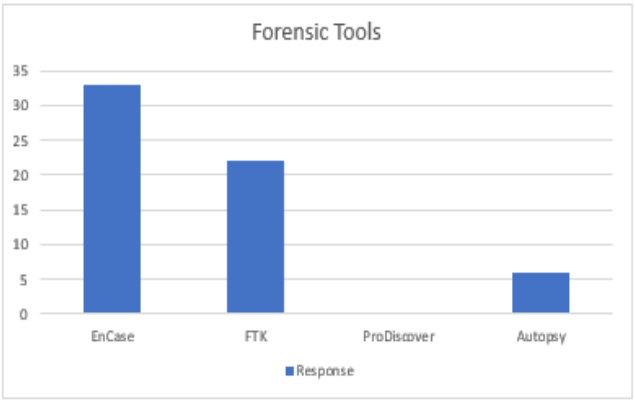

Fig. 2. Comparison Chart

Fig. 2. shows the Digital Forensics and Incident Response (DFIR), which is used to look for data breach, threats, virus and more. EnCase is highest with 33 responses, followed by FTK and Autopsy, while ProDiscover doesn't support DFIR.

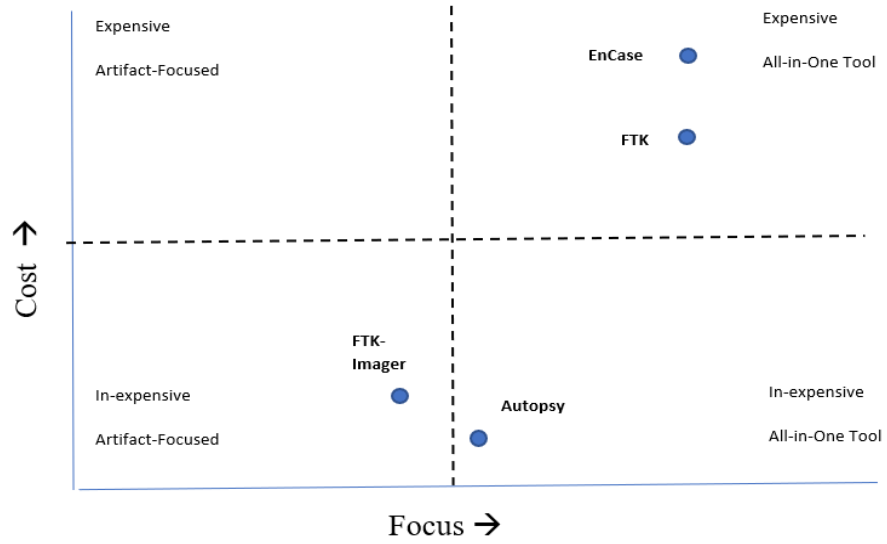

Fig. 3. Cost vs Focus

Fig. 3. Gives a cost vs focus analysis of various tools. If we want to work on a particular artifact without spending too much, we can use the FTK-Imager, or if we want a single tool for all functions, Autopsy can be used. However, if we need a tool with advanced features, we can use EnCase or FTK which are considered expensive.

IV. CONCLUSION

As we all know that in this world of emerging internet wherein internet is a vital part of each and every item in our day to day life having a branch that automates and regulates proper functioning of all the process on the internet is a must. The government is finally realizing the importance of such branches and readily spending on them in order to have security and reliability. In the past few years cybercrime has significantly reduced due to the presence of digital forensics experts. Based on the tools surveyed in this research paper we have finally concluded that Autopsy one the most strongest tool present which can offer a complete thorough report about all the information present on the computer of the person who has committed some cybercrime, moreover it is an opensource software and easy to learn and can be used by anyone to conduct an exclusive investigation. Autopsy is also the fastest among all the tools that we have surveyed. These a days with the rise in technology advancement digital forensics tool are getting available even on mobile interface, with that said we should always try and use these tool on for ethical purposes and for the good of the community because each of these tools have a very powerful impact and is always under surveillance of the governing body.

REFERENCES

1. Handbook of Digital Forensics and Investigation, By Eoghan Casey
2. Autopsy Wikipedia
3. Comparative Study and Simulation of Digital Forensic Tools, Varsha Karbhari Sanap, Vanita Mane, Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, International Journal of Computer Applications (0975 – 8887) International Conference on Advances in Science and Technology 2015 (ICAST 2015)
4. Network forensics analysis using Wireshark. International Journal of Security and Networks
5. https://www.secureindia.in/?page_id=1105
6. https://resources.infosecinstitute.com/category/computerforensics/introduction/commercial-computer-forensics-tools/ftk-forensic-toolkit-overview/#gref
7. https://www.researchgate.net/publication/258332973_A_practical_overview_and_comparison_of_certain_commercial_forensic_software_tools_for_processing_large-scale_digital_investigations
8. https://www.champlain.edu/Documents/LCDI/Tool_Comparison_(1).pdf
9. https://binaryforay.blogspot.com/2016/09/let-benchmarks-hit-floor-autopsy-vs.html
10. https://www.marshall.edu/forensics/files/CERVELLONEADAM_FinalResearchPaper-8-7-2015_-1.pdf
11. Pick a Tool, the Right Tool: Developing a Practical Typology for Selecting Digital Forensics Tools, STI Graduate Student Research by J. Richard “Rick” Kiper, Ph.D. , March 2018

AUTHORS PROFILE

Vedanta Kapoor is currently pursuing his B.Tech Degree in Computer Science from VIT Vellore. He has worked on various project like automated home, sentiment analysis, and AI chat bots. He has done various technical internships. He is good at android coding and competitive coding and has a good knowledge of database management. He is enthusiastic about data science and financial engineering.

Sanya Taneja is currently pursuing B.Tech in Computer Science from Vellore Institute of Technology, Vellore. She has worked on projects like Spot-A-Spot- Efficient car parking system, Vocabulary Enhancer which published in Springer journal. She has done various technical internships and worked on projects involving latest technologies like deep learning, natural language processing, blockchain.

Dr. Kakelli Anil Kumar, working as Associate Professor at the School of Computer Science and Engineering (SCOPE), Vellore Institute of Technology, Vellore, Tamil Nadu, India. His research interests are secure protocol design in IOT and wireless sensor networks, secure cloud computing services, blockchain and cryptocurrency and digital forensics. He has published over 25 research articles in reputed international journals and conferences.