© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 13 Issue: 03 | NCASIT- 2022 | April 18th 2022
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Peer Reviewed

Digital Forensics

Elevating the Cyberspace

Shantanu Jangale, Om Vispute, Aryan Dadhe, Arya Babhulkar, Rushi Wagh

Students, St. Vincent Pallotti College of Engineering & Technology, Nagpur.

Introduction:-

The World is now on the verge of moving to a fully digitalized ecosystem. The present digital system has evolved a lot over the period of time which eventually has led to more and more dependency of humans on machines. This dependency has naturally many pros but with pros come the cons. The entire data and privacy of an individual or an organization are on the reality of the machines. Every day malicious tools, methods, software, and techniques are developed and designed to create harm to public and personal networks and simultaneously exploit data hubs for valuable information. This change has developed in the emergence of security breaches, cybercrimes, internet frauds, and cyber espionage which has eventually resulted in the use of digital forensics in fighting cybercrimes which has been an important development in the world of cybersecurity. Digital Forensics is a division of Forensic Science majorly based on its five pillars which are identification, preservation, analysis, documentation, and the most important presentation. It has been traditionally associated with criminal law. It requires accurate ideology to stand up to cross-examination in court. The prime aim of digital forensics is to extract data from the evidence and convert it into actionable intelligence and present the findings in front of the court. All the techniques used to extract the findings must ensure that they are admissible in the court.

[4] **Locard's Exchange Principle: 'Every contact by a criminal leaves behind a trace.'**

Without leaving a trace, a criminal cannot commit a crime. A criminal infallibly leaves evidence. Various attacks, thefts, and computer crimes that we consider are part of cybercrimes, we believe that evidence will exist and the suspect will leave a testimony for the incident responders.

The initial responders have the preparatory approach to the cases for a basic computer event; the things are administered by an individual who was at the outset at that very moment.

[2]Some Digital forensics approaches are bothered about securing cybernetic evidence from digital devices. Nevertheless, with the ample number of media subscribers and users, data availability on other public databases should be used in a digital forensic investigation case for tracking down the information or data and it is legalized and available.

What is “Digital Forensics?”

The use of scientifically derived and proven methods for the preservation, collection, validation, identification, analysis, interpretation, and documentation is what we called digital forensics in technical terms.

[2] Digital Forensics with Open Source Tools derived from digital sources for the purpose of maintaining the reorganization of criminal events, or helping to predict the unauthorized actions shown to be a disturbance to disciplined operations.

Types of Digital Forensics:-

Some of the digital forensics include:

- **Disc Forensics:** It deals with collecting the evidence from storage media such as USB devices, DVDs, CDs, etc.
- **Network Forensics:** It deals with monitoring and detecting network traffic to extract crucial data for all legal evidence to present at the court.
- **Wireless Forensics:** It falls under the type of network forensics that aims at gathering evidence from networking wireless traffic.
- **Audio & Video Forensic:** Audio and video refer to digital evidence that can be found at the scene of the crime. These are some of the most crucial pieces of evidence that can be found on any crime scene and hence are of utmost importance in digital forensics.
- **Database Forensics:** This type of digital forensic deals with forensic study and collection of databases and their relevant metadata.

Related Work:-

The argument we can make here is that nothing demonstrates the hypothesis of evidence dynamics better than Interweb elements. On an end-user computer system, the immensity of the user’s interaction with the system will likely be related to Internet communication & socializing of some sort. Every hyperlink, cookie, and query can leave indicative & evidential traces (digital footprints) on the user’s system. The related work examines web-specific elements created by Web browsers and then moves to delve into the analysis of the contents forming the local formats.

[3] The predominating and an asset to digital forensics can be articulated that digital forensics with open source tools have successfully covered a growth towards defending the cyber-crimes. Digital forensics in Cyber security covers the vast majority of cybernated things which netizens, organizations and normal users are dealing with based on many irregularities.

The cyber-crimes we often discuss are majorly initiated by the client-side which can be better said as human error. The world is witnessing digital cyber-crimes in various formats.

Recently, a report based on increasing social media crimes majorly pronounced

the utter reality of data theft by activists related to cybercrime. A survey was done on the e-crime and data theft reflected that the activists or crackers who are the prime attractors have selected a series of things and planned format of attacks if discussed on social media, websites, or browser forensics encompassing various types of drive-by-download, Phishing, vishing, virus writing, ransomware attacks. The immensity of digital crimes resulted in the generation of various tools and technologies to counter them. The open-source networks have a commanding position to contact the trace, the things which were measured, constructed, and done using the specific Linux environment are now achievable with the use of open generation tools practicable on the internet. 'Internet has its colossal secrets'.

Web browsers moreover can contain information entered into shapes: look questions, logins, and passwords for email accounts, social systems, other web locations, and money-related data. Favourites and looks can grant the analyst a think of the gadget owner's interface.

Website and server security have become a complex issue with the growing number of crackers and attacks, precaution to that we can have a secured clone server that will work as a trap and cage for attackers and criminals. We can hide our main database server inside the clone server, if in case the attacker tries to do some unusual activities around the server related to data theft, we will hide temporary data set inside the clone server which will be a look-alike of the main server, here we will trick an attacker that he has successfully penetrated the server and he is taking the information but that will be the temporary information while doing it he will obviously leave the digital footprints of his works and from where we can track him down and the organizations' data will be unharmed and criminal will be tricked at the same time when an attacker will penetrate into the clone server which is considered to be a real server organization will be alarmed for security and by that time organization can infallibly secure their system with network surveillance.

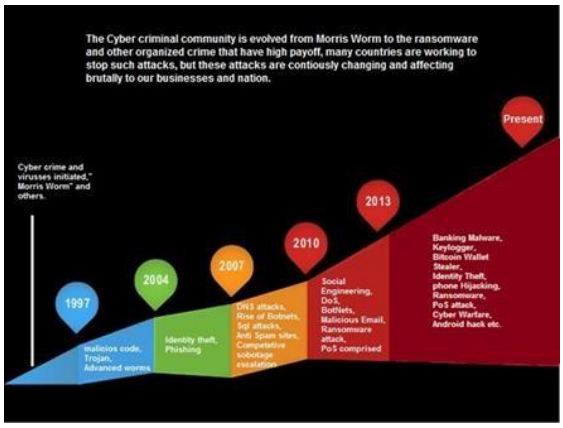

Fig – 1 Evolution of Cyber Crime

The various internet-mentioned case studies revealed that Law enforcement agencies are motivated to train officers to collect digital evidence and keep up with emerging generations. Analyzing evidence stored on a digital computer is the forensic challenge facing law agencies.[1] Laws may restrict the abilities of responders and officers to undertake investigations since protocols can abruptly determine how much data can be seized.

Methodology:

The forensic analysis highlights the traces that solve the computer crime. It requires using efficient tools.

Digital Forensics follows the **CHAIN OF CUSTODY** with respect to every case

better known as the Digital Forensics Investigation process it deals with step-by-step analysis right from identification of evidence from a crime scene to presenting it in front of a Court of law.

- **Identification:** It is done of the evidence, after a particular crime occurred, a forensic analyst or incident responder has to identify the data that has been compromised and the tools and systems used for initiating a particular crime.

- **Preservation:** It is the following step after identification that primarily deals with securing evidence proper security of evidence is of utmost importance as evidence must not hamper. Securing the evidence has some parameters
  - ➔ Warrant
  - ➔ Seizure of evidence
  - ➔ Transportation of evidence

- **Extraction:** Extraction follows the process of creating a copy and acquiring the evidence from the data, information, and suspected system collected from the scene. Bit-by-bit copy is generated, and encryption techniques are countered in the support of the evidence.

- **Interpretation:** It is the fourth step towards the chain of custody which accords with the analysis of evidence that is extracted.

- **Documentation:** Documenting the analysis of evidence, documentation plays a crucial role in this process. It encompasses the written format of photos, videos, and physical & digital evidence.

- **Presentation:** Presenting the evidence with the clean processes of case handling in front of the court of law is of vital importance, clean and clear presentation is helpful as no surpassing of proven comments is done by other authorities.

The authorities follow probe with such methodologies in digital forensics.

[1] Anti-forensic techniques are becoming an alarming barrier for the digital forensic community. They are designed to obstruct or evade the forensic process. They are any attempts to compromise the availability or usefulness of evidence to the forensics analysis. People use anti-forensics to baffle investigations, forensic tools, and investigators.

Conclusion:-

The Society of digital forensics has an extensive past of relying on closed-source tools but presently the scenario changed with ease that open source networks have paved an enormous growth for it. It is going through the change from uncertain methods and techniques to a well-organized scientific stream that needs to be continuously connected to top standards. The domain of digital forensics is still growing and has drawn a lot of attention from many in this expanding field.

The aforementioned investigation process has constructed the defense of e-crime with a good and constructive impact it is the process of grasping electronic data so as to sustain any evidence in its most original form. [1] Although the field of digital forensics is still budding, increased awareness of digital forensics and cybercrimes is appreciable. It is going through a transition from a relatively uncertain position to a scientific stream that needs to be continuously held to achievable dogma.

References:-

[1] - Research Paper Digital Forensics/ Volume 7, Issue 4, April 2017 ISSN: 2277 128X / Matthew N. O. Sadiku, Mahamadou Tembely, and Sarhan M. Musa / Roy G. Perry College of Engineering, United States.

[2] - Digital Forensics: Crimes and Challenges in Online Social Networks Forensics by Bandr Fakiha / Umm Al Qura University, Al Qunfudah, Saudi Arabia.

[3] - Digital Forensics with Open Source Tools by Cory Altheide Harlan Carvey © 2011 Elsevier, Inc. All rights reserved.

[4] - /SI110/Cyber Operations/Computer Forensics / https://www.usna.edu/Users/cs/wcbrown/courses/si110AY13S/lec/l30