iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VIII **Month of publication:** August 2021

DOI: https://doi.org/10.22214/ijraset.2021.37684

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VIII Aug 2021- Available at www.ijraset.com

Review Paper on Introduction to Cyber Forensics

Miss. Priya R. Yadav[1], Dr. Sunil R. Gupta[2]
[1] *PG Scholar,* [2] *Professor, Computer Science & Engineering, Prof. Ram Meghe Institute of Technology & Research, Badnera, Maharashtra, INDIA*

Abstract: ***Cyber Forensics is termed as scientific methods or applications in association with the judiciary or court of laws. The aim behind these methods is to unveil the digital evidence to be utilized in court for solving crime cases. This sort of technology wasn't practiced before therefore most criminals tend to urge away with their criminal acts without valid proof to incriminate or prosecute them. During that time the oaths, confessions, testimonies from witnesses were the sole determining factors of evidence***

Crimes committed within electronic or digital domains, particularly within cyberspace, have become common. Criminals are using technology to commit their offenses and make new challenges for law enforcement agents, attorneys, judges, military, and security professionals. Digital forensics has become a vital instrument in identifying and solving computer-based and computer-assisted crime. This paper provides a quick introduction to cyber forensics.

During this paper we present a typical model for both Incident Response and Computer Forensics processes which mixes their advantages in an exceedingly flexible way: It allows for a management oriented approach in digital investigations while retaining the chance of a rigorous forensics investigation.

Keywords: cyber forensics, digital forensic science, computer forensics, evidence, judicial system.

I. INTRODUCTION

Cyber forensics within the simplest words means investigating, gathering, and analysing information from a computer device which may then be transformed into hardware proof to be presented within the court regarding the crime in question [1]. An awful important aspect of the investigation is making a digital copy of the storage cell of the computer and further analysing it so that the device itself doesn't get violated accidentally during the whole process. The aim is to only find malware within the software a part of the device and leave the particular component of it on one side. While studying the entry and exit points of the device's storage, one can easily and efficiently study about the individuals who accessed the device and also the circumstances under which the logs were made which successively gives a crystal-clear picture of what happened and at what date and time. Cyber forensics is an unavoidable force that's extremely significant in today's ever-changing, evolving, and technologically transforming world.

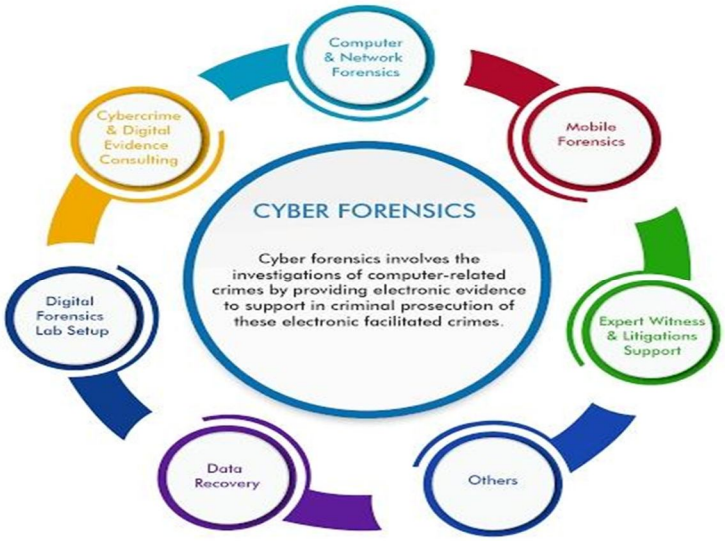


Fig.1 Application of Cyber Forensics

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VIII Aug 2021- Available at www.ijraset.com

Digital devices like cell phones, tablets, gaming consoles, laptop and desktop computers have become indispensable a part of the trendy society. Digital forensics is employed to assist investigate cybercrime or identify evidence of a computer-assisted crime. The concept of digital forensics dates back to late 1990s and early 2000s when it absolutely was considered as computer forensics [2].
Computer Forensics may be a discipline which is anxious with the collection, analysis and interpretation of digital data connected to a computer security incident; it's some-times also called digital forensics.
Computer Forensics, or Digital Forensics, may be a forensic science that deals with obtaining, analysing and presenting digital evidence, which may be defined as "any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense like intent" By employing accepted and proven techniques and principles, which also are applied in other forensic sciences, admissibility during a court of law and credibility of the evidence is achieved.
It's all about provision of digital evidence usually retrieved from digital devices like hard disks, cameras. Set of analysis techniques are accustomed achieve this by gathering data to be used as evidence. Each process done must be documented until final report is produced. This ranging from the onset which is crime scene until last stage, And the powerful ability behind computer forensics is that even damaged, deleted or lost data from devices can still be recover.

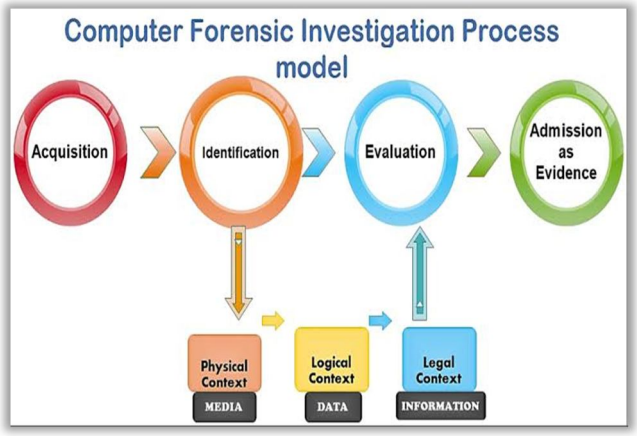


Fig 2. Computer Forensic Investigation Process model

II. INVESTIGATION STEPS IN FORENSICS:

It consist of four main steps which are as follows,

A. Acquiring of Evidence

This is the very first step in gathering information for evidence purposes. Is it done immediately after the occurrence of an incident? There are tools (sniffer and monitor) used for collecting such evidence and bend preserved until court case. A duplication or copy is formed since during court case original copy isn't used [3].

B. Identification

Here comes the second step after acquisition step. Collected information from crime scene is then going to be analysed for it to be ready to be used as evidence. It also entails the employment of methodologies and procedures that are even capable of retrieving the damaged/destroyed or deleted data from a device. The results here may be presented in either hardware or a soft copy format.

C. Evaluation

Third step after identification, a collective o parties (Team) from forensics investigator, examiners now working together to see whether identification information is that valid and valuable to be used. This might even involve the conductions of DNA investigations if necessary.

D. Presentation

The Last stage of forensic investigation, this is often where a final report (document) from previous stages is now taken to relevant officials to see if it admissible to be utilized in court. It's actually a summary of all findings in each stage from different parties involved in an investigation.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VIII Aug 2021- Available at www.ijraset.com

III. TYPES OF COMPUTER FORENSICS

There are various varieties of computer forensic examinations. Each deals with a particular aspect of information technology. A number of the most types include the following:

1) *Database Forensics:* The examination of data contained in databases, both data and related metadata.
2) *Email Forensics:* The recovery and analysis of emails and other information contained in email platforms, like schedules and contacts.
3) *Malware Forensics:* Sifting through code to spot possible malicious programs and analysing their payload. Such programs may include Trojan horses, ransomware or various viruses.
4) *Memory Forensics:* Collecting information stored access exceedingly computers random access memory (RAM) and cache.
5) *Mobile Forensics:* The examination of mobile devices to retrieve and analyse the information they contain, including contacts, incoming and outgoing text messages, pictures and video files.
6) *Network Forensics:* Searching for evidence by monitoring network traffic, using tools like a firewall or intrusion detection-system.

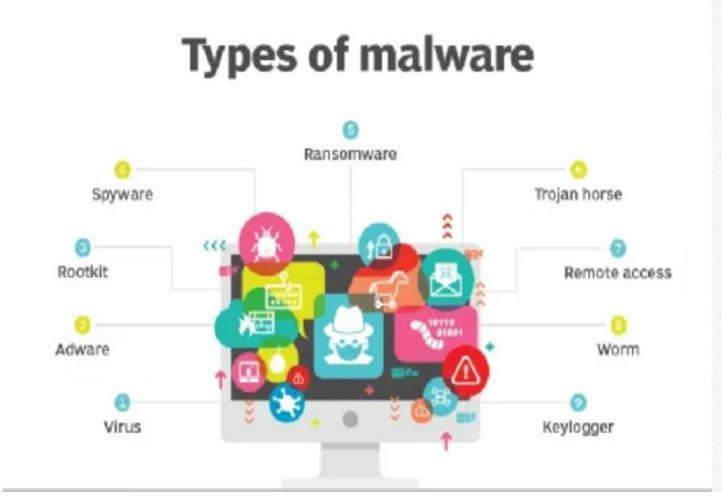


Fig 3. Types of Malware

IV. NEED FOR CYBER FORENSICS

The necessity for cyber forensics is easy yet of utmost importance. Cyber Forensics is required for the investigation of crime and law enforcement. There are cases like hacking and denial of service (DOS) attacks where the personal computer system is that the crime scene. The proof of the crime is present within the automatic data processing system [5]. The proofs will be browsing history, emails, documents, etc. These proofs on the computer system alone are often used as evidence within the court of law to map out allegations or to shield the innocent people from charges.

V. LITERATURE REVIEW

In “A Study on Cyber and Network Forensic in Computer Security Management” paper, they highlight basics related to computer and network security. Also an information beneficial to prosecutors, as Law enforcement on the rules and procedures for creating use of digital evidence similarly as obtaining it. Both authors state computer security as about confidentiality and protection of data from exposure to unauthorized entities. One author mentioned it as associate with the protection of data from damage to both hardware and software as along with services disruption, whilst another author defined it using 3 triangular security trends being CIA Confidentiality, Integrity and Availability as further as authentication.[1] In “Digital Forensic” paper, they provides a brief introduction of digital forensics. Digital forensics could be a multi-disciplinary and inter-disciplinary field encompassing diverse disciplines like criminology, law, ethics, computer engineering, and information and communication technology (ICT), computer science, and forensic science. Uncovering and interpreting electronic data so on to preserve any evidence in its most original form. [2] The AI based forensics also helps to get generate IT blocks within the cyber world which will easily identify the centre for cyber and virtual attacks and to search out a responsive solution to them. AI could be a field of computer science that is capable of constructing the software smart and tamed and making them act and perform like humans. [3]

VI. CHARACTERISTICS OF CYBER FORENSICS

A. Computer forensics is typically related to the detection and prevention of cybercrime.
B. It is said to digital security in this both are focused on digital incidents.
C. While digital security focuses on preventative measures, Cyber forensics focuses on reactive measures.
D. Digital forensics can be split up into five branches.
E. Computer forensics, network forensics, mobile device forensic, memory forensics, emails forensics.

VII. CONCLUSION

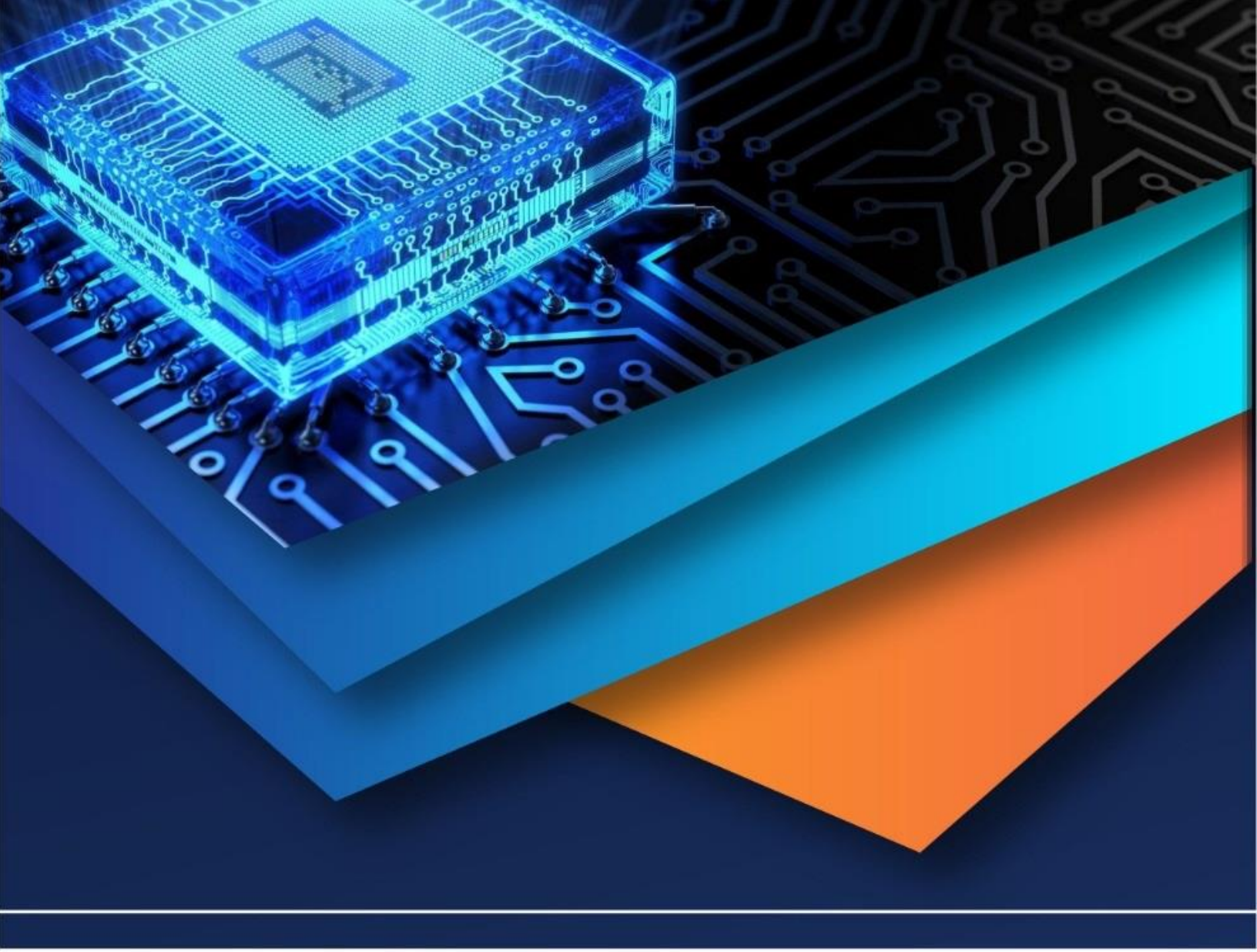
In this paper we included different aspect and method of cyber forensics. Lastly understanding forensics world from both cyber and network perspective would actually help individuals, private companies, businesses, organizations to be able to understand how to safeguard their data more especially in a digital way. All sorts of communication from storage mediums to online charts (via network) moreover as cloud storage, email systems should be kept as secure as possible. The most goal of computer forensics is to identify, collect, preserve, and analyse data in a way that preserves the integrity of the evidence collected so it may be used effectively in a legal case.

VIII. ACKNOWLEDGEMENT

First and foremost, I would like to express my sincere gratitude to my guide Dr. Sunil R. Gupta who has in the literal sense, guided and supervised me. I am indebted with a deep sense of gratitude for the constant inspiration and valuable guidance throughout the work.

REFERENCES

[1] Baboloki Janet Phuthologo, "A Study on Cyber and Network Forensic in Computer Security Management," 1. 2017 International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE) Volume 1, Issue 2, August.
[2] Matthew N. O. Sadiku:-Roy G. Perry, "Digital Forensics," 2017 International Journal of Advanced Research in Computer Science and Software Engineering .
[3] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," International Journal of Digital Evidence, vol. 1, no. 3, Fall 2002.
[4] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. San Diego, CA: Academic Press, 3rd edition, 2011, chapter 1.
[5] O. M. Adedayo, "Big data and digital forensics: Rethinking digital forensics," Proceedings of IEEE International Conference on Cybercrime and Computer Forensic, June 2016.
[6] N. M. Karie and H. S. Venter, "Taxonomy of challenges for digital forensics," Journal of Forensic Sciences, vol. 60, no. 4, July 2015, pp. 885-893.
[7] M. Losavio, K. C. Seigfried-Spellar, and J. J. Sloan III, "Why digital forensics is not a profession and how it can become one," Criminal Justice Studies, vol. 29, no. 2, 2016, pp.143-162.
[8] S. L. Garfinkel, "Digital forensics research: The next 10 years," Digital Investigation, vol. 7, 2 0 1 0, pp. S 6 4-S 7 3
[9] S. A. Asadollah, R. Inam, and H. Hansson. "A Survey on Testing for Cyber Physical System." in IFIP4141 International Federation for Information Processing,, 2015, pp. 194–207
[10] M. Anand, E. Cronin, M. Sherr. "Security challenges in next generation cyber-physical systems", technical report, University of Pennsylvania, 2007
[11] R. Chaâri, F. Ellouze, A. Koubâa, B. Qureshi,, N. Pereira, H. Youssef, E. Tovar. "Cyber-physical systems clouds: A survey". Computer Networks, 108, 2016, pp.260-278.
[12] J. Bloem, M. van Doorn, S. Duivestein, D. Excoffier, R. Maas, E. van Ommeren. "The Fourth Industrial Revolution Things to Tighten the Link Between IT and OT". Sogeti VINT 2014.
[13] R. R. Rajkumar, I. Lee, L. Sha, J. Stankovic. "Cyber-physical systems: the next computing revolution". in Proceedings of the 47th Design Automation Conference, June 2010, pp. 731-736.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY