iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VI **Month of publication:** June 2020

DOI: http://doi.org/10.22214/ijraset.2020.6347

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 8 Issue VI June 2020- Available at www.ijraset.com

A Study on Cyber Forensics

Muthuramalingam B[1], Illayaraja P[2]
[1, 2]*Assistant Professor, Department of Computer Applications, Sir MVIT, Karnataka, Bangalore*

Abstract: ***In the recent years, the use of internet and information technology across the globe has been increased tremendously. The opportunity to use the internet is huge and unconditional. Therefore, the criminal activities in the cyber world is increased in greater scale. Cyber forensics is an emerging research area that applies cyber crime investigation and analysis techniques to detect these crimes and prove the same with digital evidence in court. In this paper we have used the terms cyber, computer and digital forensics interchangeably and how cyber forensics play a key role in investigating a cybercrime.***
Keywords: Cyber Forensics, Cyber Crime, Digital Evidence, Computer Forensics

I. INTRODUCTION

The application of computer for investigating computer-based crime has led to develop a new field called computer/cyber Forensics. This is still comparatively new discipline in the domain of cyber security. Computer forensics is a systematic Identification, acquisition, preservation and analysis of digital evidence. The goal of digital forensics is to determine the Evidential value of crime scene and related evidence. In this article, we briefly discuss about need for cyber forensics, Evidences, forensics analysis of e-mail, digital forensics life cycle, chain of custody, challenges in computer forensics.

II. NEED FOR CYBER FORENSICS

The blend of information and communication technology provides many advantages to end users. In the internet world. There is no restriction for accessing the information. This is opened the gate for ever increasing cybercrimes. The users, Enterprises world wide have to live with constant threat from crackers who use different techniques and tools to break the System, steal the confidential information, eavesdrops and cause havoc. The ubiquity of computers and technologies result in Increasing crime rate. If the cyber crime attack is filed as a complaint, then it has to be investigated and proved in the court with Digital evidence. In the legal world, evidence is the core entity, hence cyber forensics will play a pivotal role in proving the Cybercrime.

III. EVIDENCES

According to Indian Evidence Act 1872, there are various types of evidences such as oral evidence, documentary evidence.
Digital evidence is a new entity introduced in Information Technology era.

1) *Oral Evidence:* Statements which is required to prove the crime by the witness during inquiry is called Oral Evidence
2) *Documentary Evidence:* Written documents produced in the court for examination is called Documentary Evidence
3) *Digital Evidence:* Digital Evidence is logical and developed using tools based on paper evidence. The process must be Understandable to the members of the court. The law specifies what can be seized, under what conditions, from whom and from Where The digital evidence could be a word document, an executable file, an audio or video. Digital Evidence will be identified
4) *As Follows:* Physical context which deals with media, Logical context which contains data and Legal context gives information and in turn provides evidence.

IV. FORENSIC ANALYSIS OF E-MAIL

Forensic analysis of email is one of the important aspects of Cyber forensics analysis. Email is the common mode of Communication worldwide. Therefore, criminals can create fake emails using various tools to launch an attack. In the Global business environment, any organization will do their transaction via electronic mail. There are two primary components in email servers and email gateways.

1) *E-Mail Servers:* Computers that forward, collect, store and deliver mail to their clients
2) *E-Mail Gateways:* Connections between E-Mail servers
3) *Forensic View:* The header of the email plays a vital role in analyzing the authenticity of an email. Header provides entire path Of email's journey from its origin to its destination. Header of a legitimate email will be following bottom-up approach. Header Of a fake email will not be in any proper approach. By viewing the header one can understand the difference between original Email and fake email.

V. DIGITAL FORENSICS LIFE CYCLE

1) *Identifying the Evidence:* This process consists of recognizing the incident, tools and techniques used, search warrants and Authorization.
2) *Search and Seizure:* This involves recognizing and collection of evidences
3) *Preservation:* This refers to securing and protecting the integrity of evidence
4) *Examination:* Examination is the process of ensuring the uniqueness and recovering the data.
5) *Analysis:* Analysis determine the significance of evidence, reconstructing the fragments of data and drawing conclusions.
6) *Reporting:* Reporting involves summarizing, translating and explaining conclusions to concern authorities.

VI. CHAIN OF CUSTODY

Chain of custody is the heart of cyber forensics investigation. This is a chronological written record of those individuals who Have had custody of evidence from its initial acquisition until its final disposition. Accountability is crucial because if the Evidences are not properly maintained in the order; it will not be accepted in the court.

VII. CHALLENCES IN CYBER FORENSICS

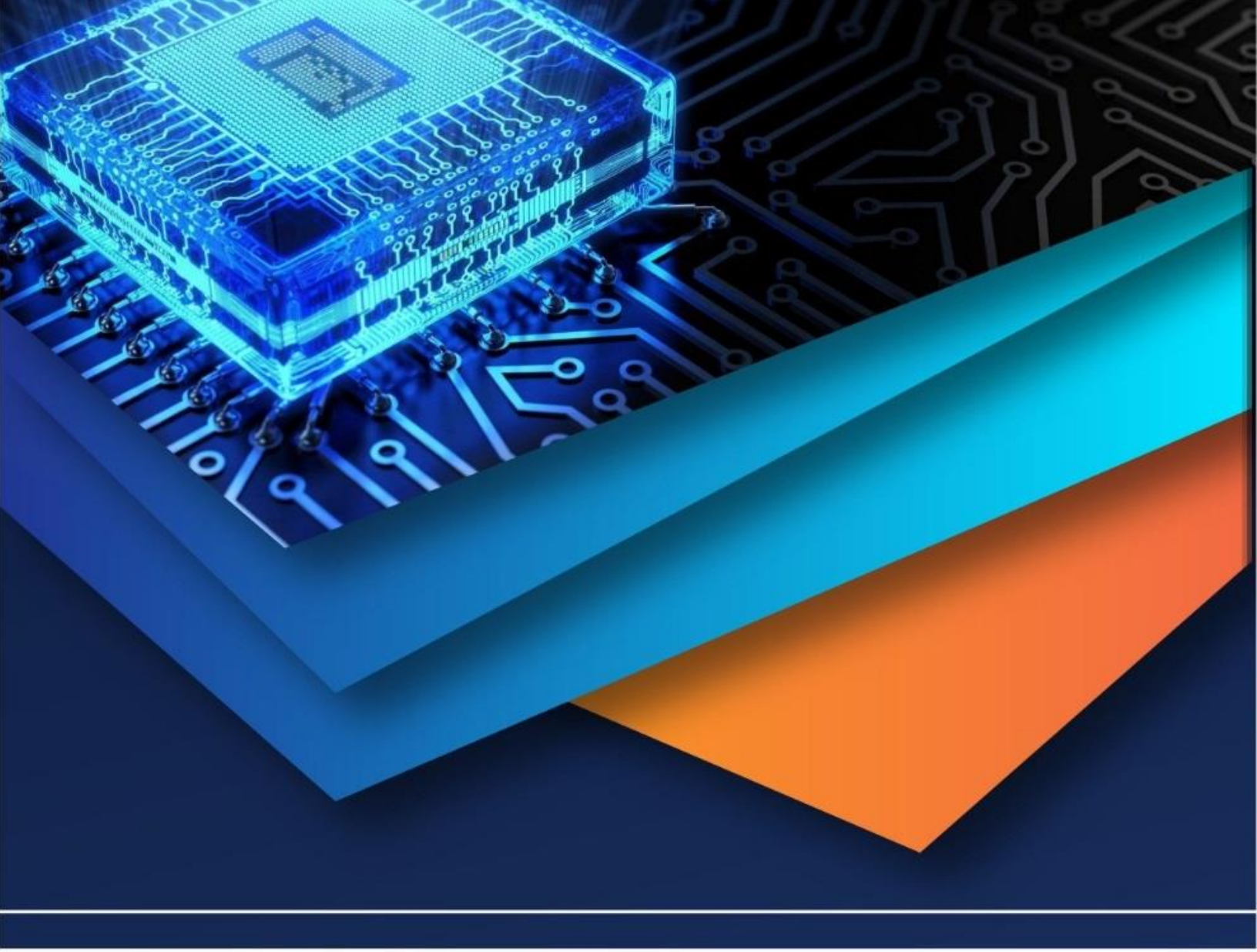
In every country, billions of messages, emails, websites are exchanged and visited every day. Cybercrime investigators Are challenged by how to collect the specific case related information from very large group of files. Technical challenges Like understanding the raw data and its structure. Legal challenges and data privacy issues such as identifying relevant electronic Evidence without violating specific laws, maintaining chain of custody and investigation process.

VIII. CONCLUSION

The field of Cyber Forensics has grown rapidly in the 21st century. The emergence of information forensics comes from the Incidence of criminal, illegal and inappropriate behaviors. The chain of custody and proving the evidence accurately is very Important in Cyber Forensics investigation. In this paper, the fundamentals of Cyber Forensics and its associated aspects are Briefly discussed.

REFERENCE

[1] http:// en.wikipedia.org/wiki/computer_online_forensic_evidence_extractor (6 November 2009)
[2] http:// www.digital-evidence.org/papers/opensrc_legal.pdf (December 2009)
[3] understanding cyber crimes, computer forensics and legal perspective by Nina Godbole, Sunit Belapure
[4] http:// www.accessdata.com/forensictoolkit.html
[5] http://www.digitalintelligence.com/softwareguidances/encase
[6] http://www.ghacks.net
[7] http://en.wikipedia.org/wiki/wirelessforensics
[8] http://net-forensis.blogspot.com



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY