INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | Jan 2024

ISSN: 2582-6433

SIGNIFICANCE OF CYBER FORENSICS

AUTHORED BY - SANSKRITI NIGAM

ABSTRACT

The increasing use of electronic devices has given rise to concerns about digital security, which has led to an enormous rise in cybercrimes. In order to gather evidence related to digital crimes, digital forensics is required, for which appropriate use of forensic tools and technical expertise is necessary. These tools and technique play pivotal role in the administration of justice.

In the age of rapidly growing industry of technology advancement, Digital Forensics is essential because without adequate evidence, even its difficult for Judiciary to deliver justice. Embedded endurance strategy requires both macro-level (organizational) andmicro-level (people, network, and systems) thinking. Credit card scams and account hacking are becoming more common due to the increased use of social media and reliance on electronic payment methods.

Hackers have been able to bypass security measures and gain access to protected systems belonging to banks, organizations, and many more. There aren't many harsh penalties foundin information technology laws; most of them are relatively mild. Although a significant step forward, the Information Technology Act of 2000 stillneeds work.

In order to find digital evidence, it is extremely important that laws and techniques be updated. Digital forensics can play a crucial role in the emergence of new crimes such as credit card scams, WhatsApp scams, UPI frauds, Remote Access Screen sharing frauds, scams utilizing QR codes, and so forth. This paper will discuss digital forensics' significance in the digital era.

KEYWORDS

Cybercrime, Cyber Forensics, Digital evidences, Electronic devices, Digital Data

ISSN: 2582-6433

INTRODUCTION

Cyber forensics is popularly known as digital forensics or computer forensics, is one of the important subfield of forensic sciences, related to recovery or extraction of data from electronic devices. Before that one need to know what is cybercrime and forensics? Cybercrime is basically criminal activities which executed with help of digital medium. forensics is the practices of using scientific methods to collect evidences related to crime similarly cyber forensics is scientific method to collect, examine and store digital evidences. Initially it was used for crimes related to computer only but now it is extended toall devices which have capacity to hold anydigital data. The growth of this area of forensicsis directly related to increasing use of digital devices like computer, laptop, tabs, mobile, hard-disk, etc. So, cyber forensics, is a field of technology that uses investigation techniques to help identify, collect, and store evidence from an electronic device[1].

The concept of digital evidence emerged from legal system, digital evidences play's important role in all crimes and cyber forensics support is important for law enforcement toinvestigate these digital crimes. Different types of sources like computer, cell phone, smartphone, unmanned aerial system and shipment provide digital footprint. The most important purpose of cyber forensics is to collect data and dig only those which can be used as evidences in court so, to assist judicial system to deliver justice

PROCESS

To identify the right source of cybercrime, the very first thing is to specifically identify each device present in the location of cybercrime, with help of this process one can identify real source or device of cybercrime. There are five steps which is to be followed, the first step is to identify, which includes determining the purposeof the research and the necessaryresources. experts need to analyse what data is stored and how it is stored.

the second step is data protection which includes preventing unauthorized access to a digital device in order to maintain its integrity.

The third step is to analysis, in which experts determine the tools and techniques needed to process the data and interpret the results. This step may involve several iterations to supporta specific crime theory. The fourth step is crime scene documentation, which means creating a

ISSN: 2582-6433

record of all visible information. This documentation assists in the creation and review of a crime scene and includes sketches, crime scene mapping, and the creation of photographs and diagrams.

The final step is to organize and present the collected digital evidence. However, it is very important to ensure that the evidence is presented in a written form that meets the appropriate documentation standards.

DIFFERENT TYPES OF CYBER FORENSICS [2]

- Disk forensics – In this the data is restored by searching active, modified or deleted file
- Network forensics – It includes monitoring and analyzing computer network traffic togather evidences andimportant information
- Wireless forensics -This is a branch of network forensics. The main purpose of wireless forensics is to providetools to collect and analyze wireless network traffic data.
- Database Forensics - It is a branch of digital forensics that deals with the study andinvestigation of databasesand their associated metadata.
- Malware Forensics - This branch deals with the detection of malicious code, their payloads, viruses, worms,etc.
- Email Forensics - Deals with email recovery and analysis, including deleted emails, calendars and contacts.
- Memory crime - It involves collecting data from system memory (system registers, cache,RAM) in raw formand then extracting data from raw garbage.
- Mobile Phone Forensics - It mainly focuses on the investigation and analysis of mobile devices. It helps to retrieve phone and SIM contacts, call logs, incoming and outgoing SMS/MMS messages, voice, videos, etc.

TECHNIQUES USED IN CYBER FORENSICS [3]

cybercrime forensics plays a critical role in the investigation and resolution of many cybercrime cases, from traditional digital investigations to more sophisticated cyber threatsand attacks. The field is constantly evolving at the pace of technological advances and the changing cyber threat landscape.

File carving – File carving is like solving a puzzle with scattered pieces. It digs deep into the system to find and analyze data even when the file structure is damaged or deleted.

ISSN: 2582-6433

Chain of Custody - As a careful registrar, the chain of custody oversees the use and preservation of evidence. This ensures the integrity of the evidence, making it reliable and trustworthy in court.

Data Recovery - When important data seems lost, data recovery techniques come to the rescue. These methodsextract essential information that allows it to be analyzed.

Hash count - Think of a hash count as a digital fingerprint of a file. This ensures data integrity - every small change changes the hash, revealing possible tampering or alteration.

Timeline Analysis - Timeline Analysis creates a chronological order of events, like ordering events on a timeline. This helps scientists reconstruct functions and changes and gives a clear picture of the sequence.

Detecting Steganography - Steganography is like hiding secrets in files. Special techniques are needed to detect it. Revealing hidden information using these techniques can reveal hidden information or secrets.

TOOLS USED IN CYBER FORENSICS[4]

SIFT (SANS Investigative Forensic Toolkit) - A tool for many cyber forensics experts, SIFT provides a set offunctions for investigating digital system

Pro Discover Forensic - It is a forensic tool with excellent disk imaging and analysis, which can turn raw datainto useful information.

Volatility Framework - This tool will make memory analysis easy, allowing you to understand what's goingon in the system RAM.

Sleuth Kit (+dissection) - To analyze the file system, this tool can allow an expert tobrowse and look at itsstructure.

SPF Pro - A mobile forensic tool developed by Salvation Data that can be used for data acquisition, recovery,analysis and report export from mobile devices.

ISSN: 2582-6433

VIP 2.0 - This advanced video collector from Salvation data integrates deleted orfragmented video recovery,search, recovery, analysis and reporting

Xplico - The Xplico Network Forensics domain allows you to trace network traffic and understand what'sgoing on in it.

X-Ways Forensics - XWays Forensics is a comprehensive set of tools that can clone, viewand analyze thedisk.

SIGNIFICANCE OF CYBER FORENSICS

- Criminal investigation – digital forensics is a strong counter against crime like frauds, terror activities by unfolding their digital footprint by converting the data into reliable evidences admissible in court of law
- Corporate World – cyber forensics protect important information of business world. This ensures the safety of corporate secrets, whether they are protecting intellectual property rights or safeguarding financial data.
- Data Recovery - There can be a catastrophe if you lose your data unexpectedly. With reliable methods of recovery, retrieval of lost information and savings in both time and resources, cyber forensics is a savior.
- Ensure proper compliance of law - It is a complex task to ensure that laws and regulations are complied with. Cyber forensics is helping organizations to comply with the legal requirements in order to maintain integrity and transparency.
- Educational and Awareness - cyber forensics is not just a field of study but an area for awareness. It supports responsible use of the Internet, through education to society on Digital Safety.
- Disaster management - Cyber forensics will act quickly in case of a cyber disaster, whetherit's a hack or failure. In order to mitigate the damage, its tools and techniques are used to restore systems and recover data.
- Consumer protection - There is a huge incidence of fraud and identity theft on the Internet. Cyber forensics enables law enforcement to identify the perpetrators, so as to protect consumers and restore trust in Internet commerce.
- Enhancing cooperation: Cyber forensics increases collaboration between different agenciesand leads to more efficient solutions, as it bridge the gap between conventional

ISSN: 2582-6433

methods of investigation and internet technologies.

- International - Criminal activity transcends borders in the globalized world. In order to combat international crime, cyber forensics operates beyond geographical boundaries and engages in cross border collaboration.
- Innovation and research - Innovation solutions arise from continuous developments in this area. The research and development of cyber forensics ensures that it keeps pace with the curve, responding to new challenges through cutting edge methods.
- Personal Security: Beyond corporations and governments, cyber forensics ensures personaldigital safety. It protects individual privacy and makes digital space more secure for users.

DRAW BACK OF CYBER FORENSICS

- Digital evidences which presented in court of law is only admissible when proved that thereis no tampering
- Its is very expensive to preserve and store digital records
- Law professional must have technical / computer based knowledge
- We need to produce evidence that is authentic and persuasive.
- During investigation the privacy of individual is hampered

LAND MARK CASE LAW AND TYPES OF CASES SOLVED

The application of digital forensics in solving crimes is vast and comprehensive. Specialists use digital forensics tools to investigate a wide range of crimes, from violent crimes to financial espionage. Below are five real-life examples that highlight the importance of cybercrime technology in today's crime solving

- BTK Serial Killer Case[5]

Cybercrime technology did not play a significant role in the BTK case because the crimes occurred between 1974 and 1991, well before the widespread use of digital technology. Thecase was mostly solved using traditional investigative methods, with success when Dennis Rader reappeared in 2004 and sent police a diskette that later led to his identification and arrest.

Although the BTK case dates back to the digital age, it is important to understand that forensic techniques, including digital forensics, have evolved significantly since then. In modern cases,

ISSN: 2582-6433

cybercrime technology plays a vital role in analyzing digital evidence such as electronic communications, computer files and networkactivity.

- Silk Road Dark Web Marketplace Case[6]

Silk Road was an online black market that facilitated illegal transactions primarily involving drugs and other illegal goods. It operated on the dark web, providing anonymity to its users and administrators. Founder RossUlbricht was arrested in 2013.

Cyberforensics played a key role in this case by analyzing digital evidence related to Silk Road activities. Researchers have used techniques such as blockchain analysis to track Bitcoin transactions and identify money flows associated with illegal activity. In addition, digital forensics experts are examining servers, logs and other electronic evidence to builda case against Ulbricht.

- Colonial Pipeline Ransomware Attack Case[7]

In May 2021, a major US fuel pipeline, Colonial Pipeline, fell victim to a ransomware attack. The attackers, believed to be part of the Dark Side ransom group, demanded a ransom.Cyberforensics played a crucial role in the investigation of the ransomware attack. Forensic experts analyze malware samples, network logs and other digital artifacts to understand the attack vector, the extent of the compromise and the identity of the perpetrators. This information was critical for law enforcement agencies to respond effectively and for organizations to strengthen their cyber security measures.

- Internet Financial Crimes

Internet financial crimes cover a wide range of illegal activities, including identity theft, credit card fraud, phishing and various Internet fraud.Cyber Forensics plays a key role in the investigation of financial crimes committed on the Internet. Forensic experts analyze digital evidence such as email communications, financial transactions and logs to identify the origin of the fraud. Digital forensics tools and techniques help law enforcement agencies identify and apprehend cybercriminals who commit financial fraud.

- Cyber espionage

Cyber espionage involves the theft of sensitive information, often from state-sponsored actors or criminal organizations for political, economic or military purposes.CyberForensics is essential

ISSN: 2582-6433

in the investigation and attribution of cyber espionage cases. Forensic experts analyze malware, network traffic and communication patterns to identify tactics, techniques and procedures (TTP) used by attackers. This information helpsto understand intelligence motives, target attacks against specific threat actors, and developstrategies to mitigatefuture incidents.

INDIAN CASE LAW

- NASSCOM v. Ajay Sood & Ors [8]
- FACTS
- The defendants used a placement agency and pretended to be the respectable National Association of Software and Service Companies (NASSCOM) in order to carry out phishing activities.
- Under the pretense of NASSCOM, the defendants sent phony emails to third parties, requesting personalinformation for recruitment. They also created fake email addresses.
- The defendants took advantage of India's lack of phishing-specific laws by adopting a number of falseidentities in order to evade detection and prosecution.
- A permanent injunction was requested by NASSCOM in a lawsuit it filed to stop the defendants fromdisseminating phony emails bearing the NASSCOM trademark.

ISSUES

- Is it true that the defendants' actions amounted to phishing, which is a fraudulent misrepresentation made in the course of business that causes confusion regarding the originand source of emails?
- Does the absence of phishing-specific legislation in India impact NASSCOM's legal options?
- Was it appropriate for NASSCOM to request a permanent injunction to defend its trademark from phonyemails?
- Would the court be able to compensate and provide relief in the absence of laws that specifically addressphishing?

JUDGEMENT

The court determined that phishing is an unlawful act and that it involves a deceptive act thatcauses confusion, as defined by Indian law. Although the court recognized that there was noexplicit

ISSN: 2582-6433

legislation regarding phishing, it nevertheless interpreted the laws that were in place and declared phishing to be unlawful.In order to safeguard NASSCOM's intellectual property rights and prevent the defendants from using the NASSCOM trademark in fraudulent emails, the court issued a permanent injunction.

By accepting a settlement wherein the defendants acknowledged their unlawful actions, consented to pay damages, and turned over evidence that had been taken from their computers, the court enabled relief. The court's ruling established a standard for handling technical aspects of cyber scams and emphasized the necessity of enacting laws to combat them.

- Pune Citibank Mphasis Call Center Fraud

FACTS

A fraudulent account was used to receive an unauthorized transfer of US$3,50,000 from four US customers'

Citibank accounts online in 2005. Call center workers at MphasiS took advantage of customers' trust by pretending to be helpful assistants in order to obtain PINs. They found weaknesses in the MphasiS system rather than cracking encrypted software.

JUDGEMENT

The accused were identified by the court as former employees of the MphasiS call center. The court emphasized the strict monitoring of employees' entries and exits, highlightingthe possibility that account details were memorized. The crime falls under the category of cybercrimes because the unauthorized access involved the use of SWIFT (Society for Worldwide Interbank Financial Telecommunication) for fund transfers. Section 43(a) of theIT Act, 2000, which deals with unauthorized access in transactions, was applied by the court. In addition to sections 420 (cheating), 465, 467, and 471 of the Indian Penal Code, 1860, the accused was charged under section 66 of the IT Act, 2000. The court emphasizedthe flexibility of the IPC by stating that offenses involving electronic documents are equivalent to crimes involving written documents.

- AVINASH BAJAJ vs. STATE (NCT) OF DELHIFACTS

Avinash Bajaj was CEO of the Bazee company was arrested under section 67 of IT Act for broadcasting of pornographic content in their websites. someone else have sold CD containing pornographic material throughtheir website

ISSN: 2582-6433

JUDGEMENT

The court held that Mr. Bajaj was not included in the broadcasting of pornographic materialin their websites also the material was not on their website but they received commission from the sales and revenue for advertisement on the web page , further the bench observed that the evidence collected indicated that the offence of pornographic cannot be attributed with the website , instead to other person. So the bench granted Mr. Bajaj bail on security of Rs 1 lakh each.

CONCLUSION

The primary priorities are the simplification of current legislation, the application ofcurrent policies, and the legal and technological prerequisites for the acceptance of evidence. It is important to follow standard operating procedures that are logical and guarantee harmony between attorneys, judges, forensic specialists, law enforcement agencies, businesses, individuals, and the court. Second, as cybercrime investigations sometimes span many legal jurisdictions, it is imperative that digital forensics and cybercrime investigative procedures be harmonized internationally. Significant funding must also be allocated to strengthen the capabilities of the pertinent organizations involved in the collection and prosecution of digital evidence.

REFERENCE

1. What is Computer Forensics?, by Coursera Staff
2. Computer forensics, by Ben Lutkevich
3. What is Cyber Forensics? Tools, Technologies and Platform, by Sangfor
4. What is Cyber Forensics? Tools, Technologies and Platform, by Sangfor
5. Office of justice program, bind torture kill case
6. United states vs. Ulbricht,858 F.3d71
7. Srinivasan, Suraj, and Li-Kuan Ni. "Ransomware Attack at Colonial Pipeline Company." Harvard Business School Teaching Note123-070, March 2023.
8. NASSCOM v. Ajay Sood And Ors,119 (2005) DLT 596.
9. Pune Citibank Mphasis call center fraud, Legalserviceindian.com
10. Avnish Bajaj vs State (N.C.T.) Of Delhi on 21 December, 2004 (2005) 3 CompLJ 364 Del, 116 (2005) DLT 427