INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

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

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

 ISSN: 2582-6433

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.

 ISSN: 2582-6433

DIGITAL FORENSICS IN INDIA: CHALLENGES AND OPPORTUNITIES

AUTHORED BY - KRATIKA SHARMA

A few decades back, the threat whose concept didn't even exist has now overtaken the world, the concept of Cybercrimes. Cybercrimes have made sure we don't take the advanced world for granted. Every progress comes with a regress, Cyber Crimes are such regressed variable that has come as a by-product of digitalization. From finding measures to physically defend us to now finding measures to defend us digitally, we have come a long way. So much emphasis is put on safeguarding, taking precautionary measures, and preventing a cyber-crime that we often forget to pay attention to its aftermath. What happens when the crime actually happens? In today's world of digital hassle, where every move of an individual can be easily traced, tracked, and tampered with by anyone sitting in any part of the world without even having physical access to your device, it speaks volumes of the threats that loom over us.

To deal with the aftermath, digital forensics comes into the picture. Digital Forensics is a branch of forensics science that deals with the observation, collection, and preservation of digital evidence post-incident. Mitigating ways to trace down the offender while collecting untampered evidence that can be presented in a courtroom and ensuring justice is served is the need of the hour. Despite its vital importance, Digital Forensics has not received the aid and ammunition it deserves. It is high time we focus on the importance of digital forensics and realize how digital forensics is the 'new black'. This article is an attempt to understand India's new legal landscape by exploring the field of Digital Forensics in India, the challenges it faces, and the future opportunities it holds, while understanding the magnificent role it plays in tackling digital crimes in the digital world.

Keywords: Cyber Crimes, Cyber Security, Digital Forensics, Challenges, Opportunities.

 ISSN: 2582-6433

INTRODUCTION

In a world where everything is running toward the digital world, there is a sort of race among everything to get 'digitalized', from shopping to booking tickets, every field has been digitalized, where even crimes did not fall behind. In fact, they are acing the modern online era. Crimes have occupied an extremely crucial place in the digital world, where digital crimes have emerged as the star villain of the entire generation. To deal with digital crimes, we need digital investigation. This is where digital forensics comes into the picture. Digital Forensics is a newly evolved branch of science that deals with the aftermath of a crime scene. It includes collecting, analyzing digital databases, and preserving data in a manner that can be presented as evidence in a courtroom. It plays a key role in investigating various crimes such as financial fraud, hacking, online harassment, identity theft, etc.

The field of digital forensics has grown at par with digitalization. With advancements in technologies, the field of digital forensics is advancing alongside. It is one of the few areas that is empowered by technology rather than being threatened by it. In a rapidly developing country like India, digitalization has become the backbone of the nation's economy. With the major involvement of Internet services, digital banking, e-commerce, etc., there has been a steep spike in cybercrime cases. Such instances speak out for the threat to be taken seriously, for fields like digital forensics to be taken seriously. There is a need for a strong digital forensics framework to be implemented for the sake of national security, individual privacy, safeguarding businesses, etc.

Although digital forensics is of vital importance in India, it still faces many challenges. The country lacks advanced forensic infrastructure, faces a shortage of specialized digital forensic experts, issues related to encryption and cross-border cybercrimes, dynamic nature of cybercrimes makes it difficult for cyber experts to be at par with efficiency. But just as night comes with the promise of another day, so do the challenges. Every challenge holds a characteristic to be overcome and turn into a futuristic opportunity. We have now arrived at a time where people can buy land on the metaverse, and are investing in Artificial Intelligence. So, being backward in fields like Digital forensics is out of the question. The need to develop with time comes with the need to have developed laws that are at par with the current environment, which in our case is digital laws to efficiently provide justice in the digital world in digital ways. Sadly, the instrument to provide justice and tackle our sufferings is suffering itself. It's time we acknowledge the fact that Digital Forensics 'is the new black'.

 ISSN: 2582-6433

UNDERSTANDING DIGITAL FORENSICS

What is Digital Forensic?

Digital Forensics is a branch of Forensic Science that involves extracting, collecting, and preserving digital data as evidence without compromising procedural integrity, making it legally admissible in the courtroom. Digital Forensics has overcome the traditional ways of collecting evidence in forensics and follows modern ways supported by advanced technologies in collecting data from various digital sources such as mobile phones, computers, cloud storage, etc.

Digital Forensics comes into the picture much later in the crime process but makes sure to provide a just end to it. It majorly deals in the investigation of fraud, data breaches, cybercrimes, and various other digital offenses. It investigates crime from its grassroots by analyzing and drawing conclusions from data stored in various digital devices such as personal computers, servers, smart gadgets like smartphones, smart watches, etc.

Key branches of Digital Forensics

The field of Digital Forensics encompasses a broad horizon and has branches in sub-branches. It contains various specialized fields that deal with different types of digital investigation. A few key specializations in Digital Forensics are as follows:

1. **Mobile Forensics** - As the name suggests, the branch of Mobile Forensics deals with the extraction of data from mobile devices such as smartphones, smart watches, tablets, etc. It involves accessing call logs, text messages, social media activities, GPS location, etc. However, the process of processing data collected through mobile devices often faces complexities due to various digital restrictions such as password protection, encryption features, etc.
2. **Computer Forensics** – It deals with the extraction of data from various digital storage devices such as personal computers, hard disks, external storage devices, etc. It follows the technique of reviving deleted files, disc imagining, tracing malware's path to lead to the source, etc. It majorly deals with the investigation of cybercrimes such as hacking, stalking, cyber stalking, etc.
3. **Network Forensics** - Network forensics involves monitoring and analyzing network traffic to detect and investigate cyber incidents. It plays a crucial role in identifying data breaches, denial-of-service (DoS) attacks, and unauthorized access attempts. Tools like

 ISSN: 2582-6433

Wireshark and Snort assist in capturing and analyzing network packets to uncover potential security threats.

4. **Cloud Forensics** - Cloud forensics is dedicated to investigating cybercrimes that occur within cloud computing environments. Key challenges include handling data stored across multiple jurisdictions, restricted access due to third-party service providers, and strong encryption measures. Cooperation with cloud service providers (CSPs) is essential to access logs, metadata, and other critical evidence.
5. **IoT Forensics** - IoT forensics focuses on collecting and analyzing data from Internet of Things (IoT) devices, including smart home gadgets, wearable technology, and industrial sensors. It is instrumental in investigating cyber-physical threats, smart home intrusions, and security breaches in connected vehicles. Challenges in this field include proprietary hardware designs, limited device storage, and vulnerabilities in IoT security frameworks.

Digital Forensics tools and techniques

Unlike traditional forensics which uses scissors, gloves, and magnifying glass, this branch of forensics uses various digital tools and techniques such as autopsy, Oxygen forensics suits, Wireshark, etc. to extract, collect, analyze, and preserve data. Some of the tools and techniques are given below:

1. **Forensic Imaging and Data Recovery** – This method involves the creation of an exact digital replica (forensic image) of storage devices that allows investigators to examine data without tampering with the original files. This method also helps in recovering deleted data. A few vital tools used for this method are Autopsy, FTK Imager, and EnCase.
2. **Memory and Mobile Device Forensics** – This method involves the extraction of volatile data from a system's RAM and retrieving deleted files, including messages, call history, and app data from mobile devices. This is crucial for investigating cybercrimes involving smartphones and other portable gadgets. A few vital tools used for this method are Oxygen Forensic Suite, Cellebrite, and Magnet AXIOM.
3. **Network and Cloud Forensics** – This method involves monitoring and analyzing network traffic to detect security breaches, unauthorized access, and malicious activities. In cloud environments, it helps track cyber incidents and retrieve evidence from remote servers. A few vital tools used for this method are Wireshark, Splunk, and XRY Cloud.

 ISSN: 2582-6433

These digital forensic tools and techniques play a crucial role in cyber investigations, by assisting law enforcement agencies, cybersecurity professionals, and corporate security teams in uncovering digital crimes.

THE CURRENT STATE OF DIGITAL FORENSICS IN INDIA

Rapid Growth of Digital/ Cybercrimes in India

In the past few decades, cybercrimes have emerged as a pioneering crime in the field of crimes. According to the Federal Bureau of Investigation, Cybercrime cases witnessed an increase of 22% between 2022 and 2023 in the United States of America. On the other hand, according to the National Crime Records Bureau (NCRB), cybercrime cases in India grew by over 63% between 2019 and 2021. With the growth in technology, cyber-crimes have multiplied as well, acquiring various forms and shapes. From Ransomware to spyware, from financial fraud to identity theft, cybercrimes occur anywhere, happening in any part of the world, by anyone. The definition of cybercrimes in the world's largest democracies has a new notional dimension: it can occur in any part 'of' the world, 'By' anyone in the world, and 'From' any device in the world. Some major incidents that have taken place in the past few years, like the Prime Minister of India's Twitter account being hacked in 2020, have raised severe concerns regarding Cybersecurity in India and have forced India to take cybercrimes as a national threat.

Role of Government Agencies

Recent incidents have nudged the Indian government to strengthen cybersecurity and digital forensics for national security, and the government has introduced several initiatives. Various agencies have been equipped with the task of tackling cyber threats and improving cyber security. Some of the key agencies working on the tedious task are as follows:

1. **Indian Computer Emergency Response Team (CERT-In):** CERT-In serves as the country's primary cyber security agency, CERT-In deals with the task of detection, prevention, and response to cyber incidents. It issues security advisories, conducts awareness programs, and collaborates with organizations to enhance cyber resilience.
2. **National Cyber Crime Reporting Portal**: It's an online portal that the Ministry of Home Affairs manages, it enables individuals to report cybercrimes, particularly cases of financial fraud, identity theft, online harassment, and social media-related offenses. It helps streamline the reporting and resolution process.
3. **Cyber Crime Coordination Centers (I4C):** it was established to improve coordination between central and state authorities, I4C focuses on investigating

 ISSN: 2582-6433

cybercrimes, providing training to law enforcement agencies, and strengthening overall cyber capabilities. These centers work towards a more robust digital security framework in India.

These agencies collectively contribute to building a more secure digital environment, ensuring effective cybercrime investigation, prevention, and response mechanisms.

Existing forensic capabilities in India's law enforcement agencies

Any change doesn't happen overnight, similarly, a problem does not get eliminated overnight. India is dealing with the gigantic issue of cybercrimes at a steady pace to the best of its abilities. Dedicated Cyber Forensics labs are established in major cities in India such as New Delhi, Hyderabad, etc. Various agencies like the Central Bureau of Investigation (CBI), the Defence Cyber Agency (DCA), and State Police Cyber Cells have been provided with forensics tools to retrieve data, malware analysis, and mobile forensics. For example, The Department of Telecommunications has launched various new initiatives to combat cybercrimes like asking all telecom operators to play cybercrime awareness caller tune on cell phones nationwide, establishing Cyber Swachhta Kendra, etc. However, we still have a long way ahead as these facilities are very urban centralized at present and have not successfully reached the rural and remote parts of India.

KEY CHALLENGES IN DIGITAL FORENSICS IN INDIA

As simplified and subtle as the concept of Digital Forensics seems theoretical, it is full of hurdles practically. India despite being one of the fastest digital-growing economies in the world, lacks the technological advancement that is the need of the hour. With cybercrimes advancing daily, it becomes difficult for currently available tools to be at the same pace. Some of the major challenges that Digital Forensics play in today's world are:

1. **Infrastructure and resource constraints –** There is a shortage of modern forensic labs and tools to tackle the modern versions of cybercrimes. The higher cost of efficient software makes them a scarce commodity. This caused a delay in forensic analysis due to a heavy backlog hence slowing down the entire system.
2. **Lack of Awareness and Expertise** – There is a shortage of trained forensic analysts and cyber security experts. There's a need for the establishment of institutions dedicated to specialized professional courses in the area.

 ISSN: 2582-6433

3. **Legal and Regulatory hurdle** – There are many gaps in IT Laws which makes the procedure of admissibility of evidence in court, complex. There is a lack of Standard Operating Procedure (SOP).
4. **Technical Challenges** – There are various challenges with end-to-end encryption in cloud storage and digital mobile apps. Quick advancement in cyber threats like malware, identity theft, etc. possesses severe obstacles.
5. **Cross-Border Cybercrimes** – There are often challenges in tracking international cyber criminals as there's often difficulty faced in seeking international cooperation for cyber investigations.
6. **Delayed Investigation Processes** – There are various bureaucratic and procedural delays in forensic analysis.

The above challenges are a few of the many challenges that India faces today. But just as every dusk is overcome by dawn, time is slowly advancing with which the field of digital forensics advances too. The day is not far when we overcome all these challenges and successfully establish ourselves as warriors in the digital realm to eliminate digital injustices.

There are many opportunities that the field of digital forensics possesses which are discussed below.

OPPORTUNITIES IN DIGITAL FORENSICS IN INDIA

Many people believe that Artificial Intelligence (AI) will take over the world in the future, completely eradicating humans in job sectors. In such a threatening environment as well, Digital Forensics is one of the sectors that will flourish through advancements in AI. It possesses severe opportunities in the near future to efficiently fulfill the needs of the hour. A few of the possible opportunities that Digital Forensics possesses are as follows:

1. **Rising Demand for Digital Forensic Professionals** - With cybercrimes on the rise, there is a growing need for skilled digital forensic experts who can investigate cyber threats, recover lost data, and ensure digital security. Both the government and private sectors are actively looking for professionals who can tackle cybersecurity challenges, making this field one of the most promising career paths today.
2. **Technological Advancements Transforming Digital Forensics** - Innovations in technology are reshaping digital forensic investigations. Artificial Intelligence (AI) and Machine Learning (ML) are making it easier to detect patterns in cybercrimes and automate complex investigative processes. Meanwhile, blockchain technology is

 ISSN: 2582-6433

emerging as a powerful tool for securing digital evidence, ensuring it remains tamper-proof and legally valid. Automation is also streamlining forensic procedures, helping experts analyze data faster and more efficiently.

3. **Strengthening Legal Frameworks for Cybercrime Investigation** - To keep pace with evolving cyber threats, India is working on enhancing its legal structure. Amendments to the Information Technology (IT) Act and the Indian Penal Code (IPC) aim to address cyber-specific offenses more effectively. Additionally, there is an increasing focus on developing standardized guidelines for courts to handle digital evidence, ensuring fair and transparent legal proceedings.
4. **Enhancing Law Enforcement Capabilities** - Building a robust digital forensic ecosystem requires equipping law enforcement agencies with the right tools and expertise. The government is investing in setting up advanced forensic labs to handle complex cyber investigations. Additionally, specialized training programs are being introduced to educate police officers and judicial authorities on handling digital evidence correctly and efficiently.
5. **Global Partnerships and Industry Collaboration** - Since cybercrimes often cross national borders, international cooperation is essential. India is strengthening its ties with global agencies like INTERPOL and the United Nations Office on Drugs and Crime (UNODC) to enhance cybercrime investigation efforts. At the same time, partnerships with private cybersecurity firms are playing a crucial role in improving forensic capabilities and providing access to cutting-edge tools and expertise.
6. **Advancing Education and Research in Digital Forensics** - To bridge the skill gap in digital forensics, universities across India are introducing specialized courses in cybersecurity and forensic science. The government is also encouraging research and development in this field, funding projects that explore new forensic techniques and technologies. These initiatives aim to build a strong foundation for future experts and strengthen India's cyber resilience.

To overcome Cybercrime in the world of digitalization, we need to opt for the same route of digitalization to grant cyber justice. The above-mentioned opportunities are not merely pointers but a vast set of possibilities that the field of Digital Forensics will possess soon. The time has come for Digital Forensics to come out of the shadows and help this modern world of digitalization.

 ISSN: 2582-6433

FUTURE OF DIGITAL FORENSICS IN INDIA

Digital Forensics got its origin from digitalization, and hence, until digitalization advances, so will Digital Forensics. The increasing digitization of India has elevated the significance of digital forensics in national security. Cyber threats such as espionage, data breaches, and ransomware attacks present risks to government agencies, defense organizations, and critical infrastructure. Technological advancements ought to influence the future of digital forensics in India.

In a world where AI is considered a threat by individuals, it is a robust element in the field of digital forensics. The incorporation of Artificial Intelligence (AI), Big Data analytics, and the Internet of Things (IoT) into forensic methodologies can improve the efficiency and accuracy of cybercrime investigations.

Professionals in digital forensics need to be trained in emerging technologies, and law enforcement agencies require updated legal frameworks to manage cybercrimes effectively. Strengthening forensic infrastructure and standardizing investigative procedures can further enhance the effectiveness of digital forensic practices. By advancing technological capabilities and forensic expertise, the country can immensely improve cybersecurity measures and establish itself as a key player in global cybercrime investigations.

CONCLUSION

The field of Digital Forensics might have just a few decades-old footprints, but will have the deepest fingerprints in the future. Digitalization has introduced us to a new world, a world of vast opportunities. Those opportunities have been limited by the new forms of crimes that have originated from digitalization, the cybercrimes. The world understood the threats cybercrime possesses and hence, the emphasis on its awareness soon became a trending topic in the world. But after a rapid hike in the number of cybercrime cases, it has finally been realized that cybercrimes are no longer just imaginary threats that can be tackled by spreading awareness but are a national threat, and the role of Digital Forensics swoops into the picture.

This article attempted to unravel the newer dimensions of cybersecurity by exploring the field of Digital Forensics, the challenges it faces, and the opportunities it possesses in fast-growing digital economies like India. Digital Forensics originated from digitalization, and hence, until

 ISSN: 2582-6433

digitalization advances, so will Digital Forensics. It is bound to advance with advancing technologies. While many perceive AI as a threat, it plays a crucial role in digital forensics. Integrating Artificial Intelligence (AI), Big Data analytics, and the Internet of Things (IoT) into forensic techniques enhances the accuracy and efficiency of cybercrime investigations.

For the successful growth of Digital Forensics, there is a need for all sectors, like the government, private sector, and various sections of society, to come together and work collaboratively towards eradicating a common threat. There is also a need for aid and ammunition to be deployed in the field of research for further advancements and continued investment in digital literacy initiatives to bridge the digital divide in rural India. It is time for us to realize the importance of the role of Digital Forensics in providing digital justice in the new world of digitalization.