NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume –3, Issue – 1, June 2024
E – ISSN – 2583-7559

ANALYSIS OF DIGITAL FORENSIC PRACTICES IN INDIA

Ayush Sood

Amity School of Business Studies,
Amity University Punjab, Mohali, India
Ayushsood137uk@gmail.com

Shubhani Aggarwal

Amity School of Engineering and Technology,
Amity University Punjab, Mohali, India
saggarwal@pb.amity.edu

Shobhita Singh

Amity School of Engineering and Technology,
Amity University Punjab, Mohali, India
shobhitasingh2805@gmail.com

***Abstract*— With the growing global recognition and the increase in number of digital crimes, it is paramount to prevent public from such wrongdoings in a timely manner. Law enforcers are seldom equipped with the relevant legal and technological resources to address such threats. This study focuses on the impact and usefulness of current laws and practices related to digital forensics in India. With significant technological advancements, Digital Forensics has emerged to be one of the most crucial processes in modern day criminal investigations. This study recommends relevant improvements based on the experiences of professionals who deal with such cases in India, on a regular basis. This study analyses and recommends changes related to law, policies, infrastructure, and training that may significantly improve DF in India.**

***Keywords*— Digital forensic, India, investigation, legislation, education & training**

I. INTRODUCTION

Digital Forensics (DF) as a discipline investigates crimes of digital nature. To that extent, it is heavily reliant on Information Technology (IT) infrastructure. Since the development of computers in the late 20th century, IT has developed leaps and bounds. Initially, internet and IT infrastructure were a rare commodity, but the constant development and evolution of technology resulted in their explosive accessibility, resulting in 21st century to be referred to as the digital era. Like any development, IT is both a boon and a bane. Technical novelties have paved a way for criminals to upgrade their traditional practices into a digital nightmare, advancing the incursion of forensics into the digital domain. McAfee reported that in 2020, cyber incidents costed world around $1 trillion, roughly 1% of the global GDP [1], [2], [3]. To counter such scenarios, fields such as cybersecurity and DF have been developed. DF is a highly specialised field which aims to identify and prevent the perpetrators of a digital crime by establishing a trail of events by gathering evidence. DF being evidence centric and closely related to crimes signifies that it provides a formal approach in dealing with investigations and evidence with special consideration to legal aspects assisting courts to prosecute both crimes and electronic-crimes (e-crimes) [4]. The World Economic Forum (WEF) have considered cybersecurity to be the largest global risk, tackling it by launching a "Global Centre for Cyber Security" in 2018 [5], [6]. This goes to highlight the importance of DF and the beneficial impact of legal domain in its development. It is important to note that DF in India is currently in its infancy and needs to be scrutinised to further develop the field to satisfy all the parties impacted by it. Currently, sub-fields such as "Audio and Video" forensics fall under physics department in Indian forensic laboratories, rather than DF as a sperate department, as is done globally. Despite being a nascent scientific field, DF has garnered much attention over the past few years. This is credited to the high volumes of data generated by the modern computer systems that lay the foundation for digital evidence (DE) [7]. In the case *Dharam Dev Yadav v/s State of Uttar Pradesh (2014)*, the Supreme court of India highlighted the importance of forensic evidence. Upon closely observing DF system, lapses pertaining to DF processes have been identified worldwide. In the United Kingdom (UK), 900 cases were dropped due to issues related to disclosure in 2016, up from 732 the previous year and 537 in 2014 [8]. Initially India had seven Central Forensic Science Laboratories (CFSLs) that reported on various forensic disciplines, assisting the law enforcement agencies. Following recommendations from the Ministry of Electronic and Information (2013), DF capabilities have been evolved to such an extent that each Indian state has a dedicated state forensic laboratory (SFSLs). Unfortunately, these laboratories lack a standard procedure, hindering the evolution and uniformity of DF in India [9]. Like any other field, there are several challenges associated with DF globally. Compared to countries like United States of America (USA) and UK where statistics are employed to conclude the reliability and validity of forensic results, in India, such practices are seldom employed. However, in India this is countered by the fact that forensic reports only depict the probability and are categorised as corroborative evidence rather than conclusive evidence for adjudicating a criminal case in the court of law [11].

Implementation and application of technologies and processes mould the way in which such techniques are used.

Interestingly, India was the first country to be collecting forensic data globally, but it was not used for forensic purposes until much later. In the late 20th century, in India, fingerprints were used in lieu of signatures due to the then illiterate population of the country. The first Central Fingerprint Bureau of India was established in Kolkata in 1897, which was also the first of its kind in the world. India was the first country in the world to use fingerprints as the sole basis for personal identification [12]. Since then, forensic infrastructure has developed significantly. Traditionally, these facilities dealt with evidence related to serology, chemistry, documentation, footprints, forgery amongst others while lacking in the digital front. Mumbai terror attacks of 2008 was a wake-up call for India. It demonstrated the lack of digital and forensic infrastructure in India [5], [13] and stressed the eminent need for such structures. Another, outline nearly every crime having a digital footprint associated resulting in a 50% rise in start-ups in technology-based companies related to DF investigations since 2011 [14]. Although, there is a progression in terms of establishing guidelines for DF investigation, they vary in terms of procedures to its UK and USA counterparts. Simply put, everyone is trying globally, but are not there yet! Similarly, India needs to update its digital laws to streamline and improve digital investigations. There needs to be strict consequences for the crimes, provision for private companies to assist investigative agencies, and laws relating to digital storage for Indian citizens. Furthermore, the need to explore the applicability of current judicial statutes, police/law enforcement structure and academic structures [13]. Therefore, this study will focus on these key points.

With the growing global recognition regarding the importance of outlawing malicious digital practices, law enforcement agencies are seldom equipped with the legal and technical resources required to address such threats. As a counter, DF has emerged to be the most crucial process. It is to be noted that DF defines the boundaries of law and law in turn frames DF. This outlines DF's dynamic nature, rendering it challenging for the law to define its parameters. To counter this conundrum, it is paramount to engage with existing laws to identify and analyse the gaps. Ultimately, this study analyses the impact and usefulness of Indian laws, current practices and implications related to DF in India.

It is hypothesised that the current Indian laws relating to DF lack clarity, resulting in acquittals and neglection of major digital evidence (DE). It is hypothesized that the current process is hindered by lack of common legal framework, manpower, infrastructure, and standardisation. This not only fails to prevent incidents relating to digital/cybercrime but also acts as a hindrance during the legal process. To that end, this study examines whether current laws, policies and infrastructure set-up in India for DF are fit for purpose?

This study aims to investigate and identify the reliability of DF process in India. The reliability will be analysed from (a) legal, (b) policy, (c) manpower, (d) infrastructure, and (e) training standpoint, stressing the need for a proper legislation and the relevant judicial structure. DF is being heavily scrutinised and developed world over. There is a constant and imminent need to improve and develop current practices and laws. Law being an integral part of DF, there is an imperative need to analyse its application and impact while suggesting recommendations to improve the current standard practices of DF in India.

This study aims to seek:

- The understanding of Indian laws that corelate to and are applicable to DF cases while identify gaps and making recommendations to improve them.
- Existing policy pertaining to DF processes with hopes of identifying current gaps to recommend new and improved policies.
- Capabilities of existing infrastructure and explore the need for further investment to set up laboratories, sort out software and hardware capabilities, or any other needs of the practitioners.
- Manpower capabilities for policing and scientific examination.

II. LITERATURE REVIEW

This section presents the literature survey related to the analysis of digital forensic practices. Beek *et.al* highlights the ubiquitous application of technology in society, providing real time access to various resources [13]. Although aimed at providing ease of accessibility, unwillingly attracts nefarious inclinations to commit crime via digital means [16]. To prevent such scenarios, there is a real need for DF. It was concluded that an open and extensible platform is a must to enable efficient and effective corporation and knowledge sharing.

This is where forensic readiness comes in to play. There have been several efforts to prepare for digital investigations. To that end, several researchers have tested and prepared their own methodologies for conducing digital investigations [17]. However, such practices have resulted in excess information, multiple methodologies, and cluttering of information. Although, the option of multiple procedures provides the opportunity to test out various hypothesis and substantiate existing and new practices, they also run the risk of bringing about chaos to the whole process. To mitigate such scenarios, there have been efforts to refine existing methodologies into a well-established digital model that offer standardisation to the current practices [18], [19]. One such study by Dhaqm, stressed the importance of scientifically proven DF technique to corroborate any incident. They outlined that traditional DF techniques which initially focused on desktop and servers were limited due to the rapid development of technology [20]. They proposed a high-level abstract metamodel that combines common investigative processes, techniques, activities, and tasks for sub-domains of DF. It was done to organise the available processes effectively and efficiently.

Reliance of DF on digital tools and software have paved way for a novel industry to flourish. In the absence of such tools, the analysis of digital devices and the evidence is hampered. Despite heavy "reliance, the techniques for validating DF software are sparse and the research is limited in both volume and depth" [21]. As investigators aim to produce robust

evidence, they are expected to ensure both the accuracy and the quality of their tools. While tool error is a hindrance, recognising a tool's limitations further raises investigatory challenges. For any forensic testing, the results for subsequent testing must be reliable and reproducible. They need to allow addition of new findings during the investigation or at a later stage to enable the criminal justice system (CJS) to determine the innocence/guilt of the perpetrator. This may further result in potential user error, ultimately raising questions on the accountability. Horsman, noted that universally, there is a lack of procedures in DF which is a huge concern. Moreover, to date, not a single DF tool is available to practitioners guaranteeing 100% accurate results, with documented proof [22].

Bhat *et.al* investigated computer forensic tools (CFT) to establish the credibility of the digital evidence from digital crime scenes in the presence of file system anti-forensic (AF) attacks. Four leading CFTs were tested for their potential against eleven different file system AF attacks. Surprisingly, CFTs were only able to identify a few AF attacks whilst the remainder went undiscovered. This study illustrated that the evidence collected by CFTs during digital investigations potentially lack credibility in the presence of AF attacks[23]. Sunde and Dror highlighted the importance of DF and the increasing number of human errors highlighted both in UK and US. They described the impact of cognitive bias and potential countermeasures within various forensic disciplines and how DF has yet to identify and counter these issues [24]. Through this study they identified these issues offered relevant countermeasures. They also experimented to examine the impact of information contextualisation and consistency of DF observations, interpretations, and conclusions. They found DF examiners' observations were commonly affected by the biasing contextual information [25].

Belonging to a rapidly evolving domain, cybercrime is quite elusive when it comes to law. Steps are being undertaken continuously by governments world-over to counter this conundrum and categorised the factors impacting the success of digital investigation in Sweden [26]. In another study, highlighted the ambiguity pertaining to successful investigation and prosecution of DF perpetrators by Indiana law enforcement agencies. These studies assessed the training level, needs, and perceptions of abilities of law enforcement agencies along with the prosecuting attorneys [27]. Ultimately, recommendations suggested a comprehensive resource guide, formation of standard operating procedures (SOPs) and awareness regarding available training/educational materials. There have been various studies world over that identify how legal community is failing to keep up with DF due to lack of understanding and application [28]. Moreover, the existence of policies in governmental institutions resulting in slow progress of DF processes and that the scattered and cumbersome existing legislations needing further amendments to counter such issues [29].

It was observed that the term "computer" is relatively undefined in legislations of countries such as Australia, Canada and UK compared to US and India who defined the term in a quite exhaustive manner. It continues to contrast subtle differences in how the laws in these countries define "access offences and data impairment". Lastly, discussing the provisions in laws relating to misuse of computer and other digital devices with criminal intentions [16]. Although trivial individually, these differences form a ripple effect in a large scale of things, unintentionally preventing the uniformity of laws in different countries. This indirectly effects individual country in a large scale in today's global society. This may be in the form of international agreements, treaties, or other such factors.

Zahadat, explored and discussed the need for standardisation and credentials required in DF [30]. It was seen that although training sessions are conducted for professionals, these sessions rarely add required information to the existing knowledge and hence the imminent need for credentialing such courses. A bold allegation was made to not consider DF as a profession yet rather a series of attempts to justify claims on various grounds [31]. This paper recognises a profession to have specialised knowledge, training, highly valuable work, self-regulation, established code of ethics amongst other significant elements. Although, credentialing and certification ensure code of ethics, autonomy of practice, and evidence of specialised training, this paper argues a severe lack of these components within DF. Furthermore, there were various credentialing bodies available but most of the were privately owned and focused on profits [32].

This study draws our attention over the imminent need to review DF worldwide. However, there needs to be a starting point for such feat. Therefore, this study focuses on India. There have been efforts made by Indian scholars to address similar issues, but nothing of significance could be discovered. [33] discuss India's capacity and capability of cybersecurity in the nuclear domain, whereas [34], discusses cybersecurity in India from technical and legal perspective respectively.

Computer forensics or DF aims to uncover and preserve encrypted/lost data whereas cybersecurity focuses on preventing data loss or cybercrimes [35]. However, more than often, these terms are used interchangeably. This study aims to review the current DF process in India by investigating the ground reality and establishing how matters such as laws, policies, infrastructure, and manpower affect the process of DF.

III. METHODOLOGY

Due to lack of literature and confidentiality/unavailability of information regarding the process of DF and the investigations conducted, it was decided not to include case studies as a part of methodology. Unavailability of the said data made it challenging to comment on the investigation process, hindering the qualitative analysis of DF in India. To counter this and to review the ground reality and the current state of DF practices in India, interviews were conducted from DF practitioners. These practitioners included police officers, scientific officers from FSLs and lawyers. A

minimum of three interviews were conducted from each profession. A questionnaire was prepared to conduct interview, see Appendix 1. Aim of this questionnaire was to identify and establish (a) relevant experience of participant, (b) types of cases encountered, (c) relevancy of current system and practices, and (d) recommendations.

Due to privacy concerns and the sensitive nature of the work undertaken by the participants, it was decided to conduct interviews anonymously and confidentially. Participants were contacted and informed regarding the ethics and ensured anonymity of their participation. Interviews were conducted over the phone, while some were conducted in-person, depending upon the accessibility of the interviewee. Some participants allowed recording while others insisted on noting down of responses. It was done according to participant's wish and transcripts were compiled later, see Appendix 2. Initial replies and recordings were later destroyed to ensure privacy of the participants, as promised. These responses are discussed and analysed in detail in section 5 and recommendations were made accordingly.

It was quiet challenging to get government officials (both police and scientific officers) to agree to the interview. Many people agreed but stopped reverting to calls and messages while the others kept on delaying the interview for months and never participated. Personal and professional contacts were used heavily for this process, but the entire process was very hectic and yielded very limited results contrary to what was initially anticipated. Responses from government employees may result in socio-political issues. To that end, certain amount of bias in their replies were anticipated. While most participants replied completely to the questionnaire, a certain amount of bias could possibly have been introduced in their replies.

To further substantiate or dispute claims of the participants, a Right to Information (RTI) application was applied to MHA requesting information regarding DF in India. This application sought data regarding (a) number of cases received per forensic discipline in CFSLs, (b) statistics regarding (i) average reporting time for DF cases, (ii) Number of DF cases that were reported and tried in court, (iii) Categorising subdivisions of DF according in their laboratories, (iv) number of DF cases received for year 2020-2022, and lastly (v) number of cases reported and solved by CFSLs. Reply to this application is attached in Appendix 3. This entire process allowed a quantitative analysis of DF practices in India. It was decided to establish the quality of the process prior to delving into the quantity. Moreover, limited amount of information also factored into the hinderance of further quantitative process.

IV. ANALYSIS & DISCUSSION

This study highlights a rapid increase in the number of cybercrime cases throughout the world. A similar trend was reported in India, see table 2. It is to be noted, that the crime rate is calculated as a crime incidence per one lakh (one hundred thousand) of population. This trend reiterates the dire need for reforms and the urgency for the review of DF practices in India, see section 5.1. All participants having a minimum of seven years' experience along with working on more than 200 cases, rendered them experts in their respective fields.

Financial fraud, money laundering and murders were amongst the most common crimes that are dealt with regularly relating to DF in India, see Appendix 2. As discussed in section 3.1.2, this goes to show the deep roots of digitalisation into traditional crimes. This poses a unique challenge to law enforcers to update their standard practices to incorporate DE into their investigations, evidence collection, analysis, reporting and ultimately defending it all in the court of law. With the novelty of the digital crimes and lack of awareness and knowledge pertaining to digital crimes it has emerged out to be a huge concern that requires immediate attention. Unfortunately, there are no set standard procedures laid out for investigation and analysis. These processes are generally carried out by person-in-charge based on their experience or lack of it. There is a dire need to set out standard practices to streamline the processes all over the country, see Appendix 2. Furthermore, lawyers feel the that the lack of digital knowledge of the judiciary makes them to neglect cases related to DF and regularly postpone them to escape the unwanted hassle, refer to interview 3.

Table 1: Cybercrime state wise in India (2018-2020) [36]

SL	State/UT	2018	2019	2020	Mid-year Projected Population (in Lakhs)	Rate of Total Cyber Crimes (2020)	Chargesheeting Rate (2020)
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
	STATES:						
1	Andhra Pradesh	1207	1886	1899	526.0	3.6	40.1
2	Arunachal Pradesh	7	8	30	15.2	2.0	33.3
3	Assam	2022	2231	3530	347.9	1.0	87.4
4	Bihar	374	1050	1512	1219.0	1.2	65.0
5	Chhattisgarh	139	175	297	292.4	1.0	87.4
6	Goa	29	15	40	15.5	2.6	50.0
7	Gujarat	702	784	1283	691.7	1.9	47.1
8	Haryana	418	564	656	292.1	2.2	49.6
9	Himachal Pradesh	69	76	98	73.6	1.3	41.9
10	Jharkhand	930	1095	1204	381.2	3.2	53.0
11	Karnataka	5839	12020	10741	665.0	16.2	72.9
12	Kerala	340	307	426	353.7	1.2	70.6
13	Madhya Pradesh	740	602	699	837.6	0.8	85.6
14	Maharashtra	3511	4967	5496	1236.8	4.4	27.1
15	Manipur	29	4	79	31.4	2.5	0.0
16	Meghalaya	74	89	142	32.6	4.4	1.4
17	Mizoram	6	8	13	12.1	1.1	57.1
18	Nagaland	2	2	8	21.8	0.4	-
19	Odisha	843	1485	1931	454.7	4.2	33.5
20	Punjab	239	243	378	301.8	1.3	62.4
21	Rajasthan	1104	1762	1354	786.1	1.7	26.8
22	Sikkim	1	2	0	6.7	0.0	-
23	Tamil Nadu	295	385	782	761.7	1.0	53.1
24	Telangana	1205	2691	5024	375.4	13.4	42.5
25	Tripura	20	20	34	40.4	0.8	26.3
26	Uttar Pradesh	6280	11416	11097	2289.3	4.8	49.9
27	Uttarakhand	171	100	243	113.1	2.1	63.0
28	West Bengal	335	524	712	977.2	0.7	45.9
	TOTALSTATE(S)	26931	44511	49708	13152.0	3.8	47.5
	UNION TERRITORIES						
29	A&N. Islands	7	2	5	4.0	1.3	62.5
30	Chandigarh	30	23	17	12.0	1.4	30.0
31	Daman and Diu	0	3	3	10.4	0.3	100.0
32	Delhi	189	115	168	203.2	0.8	66.3
33	Jammu & Kashmir*	73	73	120	133.4	0.9	42.4
34	Ladakh	-	-	1	3.0	0.3	-
35	Lakshadweep	4	4	3	0.7	4.4	-
36	Pondicherry	14	4	10	15.5	0.6	100.0
	Total UT(s)	317	224	327	382.1	0.9	59.7
	Total All India	27248	44735	50035	1353.9	3.7	47.5

Frauds, hacking, data theft, murders, forgery, and financial frauds are commonly investigated relating to DF on a regular basis. It was observed that the cases relating to child pornography and sextortion offered a unique and novel challenge compared to the regular DF cases, see Appendix 2. As mentioned in section 3.4, most Indians lack means and awareness to secure themselves online. To counter crimes,

public is reliant on the police. To put things into perspective, police constables are generally 10th or 12th pass who lack formal training and knowledge regarding most technical information that may be used in an investigation [37], [38]. Inadequacy and inefficacy of law enforcers play a deep role in lapses pertaining to securities regarding digital crime and prevention. Although, investigation in charge is an officer with a better education, it cannot be neglected that more than often these officers are assisted by constables and the impact they might have on a case, see Interview (1), (2), (3), (5), and (8). Moreover, it has been observed, due to lack of understanding and appreciation of DE, it is more than often neglected or underappreciated. Several instances have been observed, where crucial DE had been submitted to the court, but the lack of knowledge and understanding resulted in no discussion of the crucial evidence throughout the proceedings see Interview (1), (2), and (8).

These lapses can further be traced into the Indian judicial system. For example, in cases of child sexual abuse, a child is victimised at the time of the video shoot but is victimised time and time again whenever the video is replayed. In such cases, "video", the main evidence is never presented in the court. This is a huge conundrum where digital evidence cannot be properly utilised. Moreover, there are other instances where DE is not admitted or presented to the court, see interview 2. In cases, where evidence do make it to the court room, it is often not accepted due to lacking procedure, chain of custody or other similar reasons. These cases have raised a huge concern regarding the dire need to collect and manage evidence in a forensic manner.

4.1. Strength of India's current approach to DF investigation (DFI)

India adopted quite rapidly to the digital domain and its approach towards tackling e-crimes is a pragmatic one. Its laws are a hybrid that enable the provision for both digital and traditional crimes. Such laws offer flexibility to accommodate almost all crimes imaginable. In recent years, GOI invested heavily in the infrastructure to monitor and prevent crimes, see Appendix 4. Forensic laboratories have been established and upgraded in all states throughout India. Several states have installed high-definition CCTV cameras to monitor and prevent dubious activities. This not only enabled speedier investigations but also reduced the crime rates in several cities [39], [40]. Whilst the installation of CCTV cannot be attributed to result in lower crime rates, as seen in the national capital, Delhi [41], but these results were indeed seen in other states such as Karnataka, Baddi and Chandigarh, see interview (5) and (6). Police officers, lawyers, judges, and forensic scientists attended training sessions to update their knowledge and skillset while dealing with new technologies and associated crimes. GOI regularly provide funding to the states using schemes such as Cyber Crime Prevention Against Women and Children (CCPWC), Prevention of Children from Sexual Offences (POSCO) Act, Nirbhaya fund amongst others, see interview, see interview (4) and (7).

Government makes laws, police enforce them, and the courts adjudicate while defining parameters of such laws. Similarly, there had been several instances in the past decades where several cases were affected due to poor understanding of section 65 (B) of IEA, but this has been well settled by *Pandit Rao case of 2020*. Since then, from legal perspective, all concerns regarding the existing digital laws are well settled.

India has developed its infrastructure to tackle digital crimes within the last decade. CCPWC scheme ensured that forensic laboratories were established in each state throughout India, ensuring a baseline infrastructure to investigate crimes, see Appendix 4. But there have been lapses in terms of standardising operating procedures (SOPS), see interview (1), (2), (3), and (10). Due to lack of SOPs, each state has their own policy and procedures, which when looked upon from a broader/nationwide preview leaves us with more than 36 varying SOPs bringing about confusion and chaos when reviewing DF practices in India. Lack of knowledge and training, mishandling of evidence, lack of communication between various government agencies involved in investigation, and lack of infrastructure and software is a huge concern for DFI in India.

4.2. Obstacles

Evidence collection, management, and preservation is majorly affected by the lack of knowledge and trained staff. Volatile data is not collected by the investigators on a regular basis, see interview (2) and (8). Today data security and privacy are quite common. People safeguard their digital data using password protection and encryptions. Owners are not obliged to share passwords which further complicate the investigations, see interview (1), (4), (5), (6), (7), (8) and (9). Lack of available tools and high-end encryptions often results in delay/unsuccessful investigations. Digital domain is quite dynamic. With the introduction of new technology every day, criminals continuously seek loopholes to evade law and justice. Novel technologies in the form of IoT, Artificial Intelligence (AI), Augmented Reality (AR), Virtual Reality (VR), cloud forensics, and drones; have further complicated digital forensic investigations, see interview (7). With the emergence of these novel software and hardware, there has been an imminent need of specialists to investigate these sub-fields under DF. Lack of knowledge, technology, and forensic tools is a huge concern. Lack of understanding and appreciation of DE by the judiciary is another obstacle, frequently faced in India. This further resulted in lower courts delaying cases related to DF to avoid unnecessary complications. Moreover, there are instances where DE is not even mentioned/discussed in courts rather only submitted as a piece of evidence, see interview (2) and (3). Cases related to cloud storage further complicates matter. Most of the data centres are situated overseas and lack of international treaties and company's security and privacy policies complicates the procedure to retrieve data for DFI.

All challenges discussed limits the development of DF in India. There are three ways of mitigating them, namely:

Technical: Indigenous development of tools and technology, focus on research and development (R&D), offer incentives

to researchers. This can be achieved with the combination of government, private companies, and academia. Despite of GOI's effort to promote R&D by scientist appointed by the FSLs, either no significant research is conducted or is being conducted at a much slower pace. Need for trained operators and nationalised SOPs is a must. This will guide the investigator to follow accredited and established methodologies.

Legal: There needs to be a dynamic law to meet the requirements and fill the gaps formed by the current technologies. Indian laws are quite old and needs to be updated. Cooperation and partnerships with international agencies also play a crucial role. Ultimately, there is a need establish data centres in India for Indian users. This not only ensures easier access but also ensures privacy of Indian citizens and their data protection.

In *State of Punjab v. Amritsar Beverages Ltd.*, the Supreme Court expressed that there are a lot of difficulties faced by investigating officers due to lack of scientific expertise and insight into digital evidence techniques. The court also noted that IT Act does not deal with all types of problems and hence the agencies are seriously handicapped in some respects.

Capacity Building: This recommendation also paves way for entrepreneurship and start-ups to assist government with their dilemma. There is a need for public-private partnership, where IT industry lends its technology and understanding, and the law enforcement can share the knowledge of law to build up a symbiotic relationship.

4.3. Applicability of current laws and the challenges it poses

IT Act was never supposed to regulate cybercrimes. Its preamble focused on providing legal recognition to electronic transits. However, it was amended to compensate and accommodate laws of IPC, IEA, and CrPC into digital domain [5]. As discussed previously, IT Act made amendments to plethora of existing laws to accommodate e-crimes. Although majority of crimes are covered by these laws, but the technology is rapidly evolving the digital hemisphere, resulting in an increased demand for new laws to accommodate them. Moreover, India's current laws are quite old and as such the penalties associated with the crimes are quite lenient compared to the damage caused by them. It is a shared feeling that there needs to be stringent repercussions associated with all crimes, especially digital crimes, see interview (3) and (4).

Recently, e-crime cases have also raised concerns regarding amendments in other laws. For example, video recorded statements are accepted in courts without the need for a written transcript contrary to CrPC which distinctively states that any/all evidence must be submitted in writing which renders video statements inadmissible in courts. This clause negatively affects video evidence collected form CCTV cameras or other sources, rendering them as mere corroborative evidence, see interview (3).

State of Delhi Vs. Mohd. Afzal & Others, set the precedent for electronic records to be admissible as evidence in Indian courts. If a person disputes the accuracy of a computer evidence or electronic record based on system misuse, operating failure, or interpolation, then the person challenging it must establish evidence beyond reasonable doubt. The court observed that mere theoretical and general apprehensions cannot make clear evidence defective and inadmissible. This case has well demonstrated the admissibility of electronic evidence in various forms in Indian courts.

IT Act was last amended in 2008 and is in a dire need to be amended to accommodate crimes relating to the latest technologies and trends. There needs to be a committee to ensure and enable periodic amendments. Current laws are severely lacking to deal with issues relating to cryptocurrency, digital signatures, and transfer of digital assets such as e-commerce businesses or accounts of influencers, see interview (3). Data protection is a huge concern of the 21st century. Indian constitution does not grant the fundamental right to privacy. However, in the landmark case of *Justice K S Puttaswamy & Anr. Vs Union of India and Ors.*, the Supreme Court held right to privacy as a fundamental right with certain restrictions. Presently, India lacks express legislations governing data protection and privacy [42].

4.4. Improvements in Practices

Post discussion, these improvements can be broken down into four categories, namely

4.4.1. LAW

1. There is a need for regulatory and supervisory authority in India for forensic science like UK.
2. Annual amendments in IT Act to accommodate the dynamic technology.
3. Standardisation is a must to ensure quality of services and investigations. There is a need for a uniform standardisation of practices throughout India.
4. International treaties and agreements enabling access to information from data centres situated overseas and encouraging/directing companies to establish and move Indian data centres to India.
5. Laws for companies allowing backdoor access to forensic practitioners.
6. Allowing private companies to conduct DFI under supervisory authorities.

4.4.2. POLICY

1. Government establishments need to ensure that the laws passed by the government are followed. GOI previously published a guideline directing all government institutions to create and maintain updated records of activities and practices on their websites. However, this is not followed by many institutions including CFSLs.
2. Time bound reporting must be encouraged. Today, case log has resulted in reporting time exceedingly more than 6 months.
3. Accreditation of laboratories.
4. Vigilance over social media to prevent and identify crimes in a timely manner.
5. Budget for new and advanced tools.

NFSU – Journal of Cyber Security and Digital Forensics
Volume –3, Issue – 1, June 2024
E – ISSN – 2583-7559

6. Collaboration between academia, law enforcement agencies and private companies.

4.4.3. INFRASTRUCTURE

1. Better infrastructure and more regional laboratories with bare minimum competency.
2. Infrastructure development in district and high courts enabling them to review DE.
3. Trained technicians and manpower. Currently, FSLs throughout India lack scientist occupancy despite them having vacancies. These vacancies are not advertised and hence remain vacant for years.

4.4.4. TRAINING

1. Regular training and learning courses for existing and new practitioners.
2. R&D.
3. Specific trainings for niche DF sub-fields.

4.5. Role of private companies

Current laws do not accommodate/allow private companies to conduct forensic examinations or investigations. Under IT Act, central government may notify any government agency as the investigators. Only they may conduct instigations, legal. However, private companies often assist government agencies with DFI anonymously. These companies are better equipped in terms of technology, knowledge, and trained staff and as such they must be allowed to assist in official capacity. Not only they provide a fresh perspective but also allow handling of huge workload.

4.6. Differences of practices between states

All the police officers and forensic scientists interviewed belonged to state departments and lacked experience to comment on this. However, lawyers felt a strong need for standardisation. Just to put things into prospective, to file a case on a particular issue in high courts of different states, different procedure and documentations are used. To date, not all states in India offer to file a case in high court online [43]. Adding multiple SOPs from various laboratories with limited knowledge and understanding of digital domain, judiciary is often rendered confused in matters of DF. As mentioned in section 3.4.2, states promote regional languages and state FSLs write reports in regional languages. This acts as a barrier for intra-state collaboration and standardisation of practices throughout India. India is a nation with the largest number of English speakers, if Hindi cannot be adopted as a standardised language due to political issues, English must be considered as an alternative. However, it Is to be noted, in India, not everyone can communicate using English. Different states have different sizes, population, and tax collection. Therefore, resource allocation varies majorly between various state. This not only impacts the quality of infrastructure but also the investigation capacity.

V. CONCLUSION

Contrary to participant's claims of excessive workload, see interview (1), (2), (4), (6), (7), (8), and (9) it was observed that the number of cases relating to DF were not as high as anticipated, see Figure 10, Appendix 3. Out of all seven CFSLs, only three had an established DF department. Moreover, only Hyderabad CFSL had a huge workload going up to 400 cases a year compared to others where cases rarely exceeded the 200 marks. Furthermore, the very first entry in the said figure did not add up further raising the questions on the authenticity and the quality of records shared by the department. This information is further found to be contradicting in figure 11 and 12, Appendix 3, where the total number of cases solved by CFSL Pune in the year 2022 do not match either. Upon inquiring about the average reporting time for DF cases, it was told that the same cannot be measured and was unrealistic which raises further questions on the quality of records and the laboratory. Lastly, it is to be noted that the said data was requested from all seven CFSLs but only one laboratory ended up reverting back. This further limited the qualitative analysis of the data shared by the participants as discussed in this section.

India's approach to DF is a strong one. Like many other western nations who are struggling to keep up with digital crimes, the same trend is being visualised in India. Lapses in factors such as laws, policies, infrastructure, and knowledgeable/trained officials and technicians is bringing cracks in the current system. All these factors form the foundation of DF practices in a country, playing a crucial role in shaping and sustaining the quality of DF. There is an urgency to review these factors to cement the gaps and cracks appearing into the current system.

All conclusions recommended are to answer the questions raised by the study which was also reiterated by the participants and reconfirmed at the time of analysis and discussions. Challenges addressed and the recommendations made can be broken down into (a) law, (b) policy, (c) infrastructure, and (d) training/capacity building.

In terms of laws, it was recommended to have a regulatory and supervisory authority, regular amendments in the IT law, standardisation of practices, international treaties for access to data centres containing data of Indian users and providing legal recognition to private companies for conducting DFI.

For policy, it was recommended to ensure that the directives of the government are followed appropriately, enforcing time-bound reporting, properly accrediting laboratories, vigilance, increased funding, and a dire need for collaboration between academia, law enforcement and private companies.

For infrastructure and capacity building it is imperative to ensure forensic laboratories are made available to the states at a regional level, infrastructure development and training of the judiciary, trained technicians for conducting quality analysis, regular training, and R&D.

It is to be noted that that these factors do not form the sole basis of improvements into the current system. There is a need for further analysis into DF practices in India. A sever

lack of research, non-availability of inner workings, and hesitation of officials to discuss matters in large is a serious concern and a need for internal review committee to further investigate the matters is a must. Ultimately, the research conducted, and data gathered confirms my hypothesis that "that the current process of DF in India is hindered by lack of common legal framework, manpower, infrastructure, and standardisation".

REFERENCES

[1] S. D. Jayasekara and I. Abeysekara, 'Digital forensics and evolving cyber law: case of BIMSTEC countries', *Journal of Money Laundering Control*, vol. 22, no. 4, pp. 744–752, Oct. 2019, doi: 10.1108/JMLC-02-2019-0019.

[2] The Hindu, 'The year that lost 1% of global GDP to cybercrime - The Hindu'. Accessed: Mar. 23, 2022. [Online]. Available: https://www.thehindu.com/sci-tech/technology/the-year-that-lost-1-of-global-gdp-to-cybercrime/article33430555.ece

[3] Bloomberg, 'Watch Cybercrime Costs Global Economy Over $1T, McAfee Says - Bloomberg'. Accessed: Mar. 23, 2022. [Online]. Available: https://www.bloomberg.com/news/videos/2020-12-07/cybercrime-costs-global-economy-over-1t-mcafee-says-video?sref=WRZ1CKod

[4] E. Conrad, S. Misenar, and J. Feldman, 'Domain 7: Security Operations (e.g., Foundational Concepts, Investigations, Incident Management, Disaster Recovery)', in *CISSP Study Guide*, Elsevier, 2016, pp. 347–428. doi: 10.1016/B978-0-12-802437-9.00008-4.

[5] M. I. Ali and S. Kaur, 'The Impact of India's Cyber Security Law and Cyber Forensic on Building Techno-Centric Smartcity IoT Environment', in *Proceedings - IEEE 2021 International Conference on Computing, Communication, and Intelligent Systems, ICCCIS 2021*, Institute of Electrical and Electronics Engineers Inc., Feb. 2021, pp. 751–759. doi: 10.1109/ICCCIS51004.2021.9397243.

[6] G. Schmitt, 'To Prevent a Digital Dark Age: World Economic Forum Launches Global Centre for Cybersecurity > Press releases | World Economic Forum', World Economic Forum. Accessed: Mar. 23, 2022. [Online]. Available: https://www.weforum.org/press/2018/01/to-prevent-a-digital-dark-age-world-economic-forum-launches-global-centre-for-cybersecurity/

[7] K. Conlan, I. Baggili, and F. Breitinger, 'Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy', *Digit Investig*, vol. 18, pp. S66–S75, Aug. 2016, doi: 10.1016/J.DIIN.2016.04.006.

[8] M. Mansfield, '"The need for active vigilance is now more important than ever" – The Justice Gap', The Justice Gap. Accessed: Jul. 22, 2021. [Online]. Available: https://www.thejusticegap.com/the-need-for-active-vigilance-is-now-more-important-than-ever/

[9] G. Misra and C. Damodaran, 'Perspective Plan for Indian Forensics', New Delhi, Jul. 2010. Accessed: Mar. 23, 2022. [Online]. Available: http://dfs.nic.in/pdfs/IFS(2010)-FinalRpt_0.pdf

[10] Ministry of Electronic and Information, 'National Cyber Security Policy', 2013. Accessed: Mar. 23, 2022. [Online]. Available: https://www.meity.gov.in/writereaddata/files/National_cyber_security_policy-2013_0.pdf

[11] P. Kathane, A. Singh, J. R. Gaur, and K. Krishan, 'The development, status and future of forensics in India', *Forensic Science International: Reports*, vol. 3, p. 100215, Jul. 2021, doi: 10.1016/J.FSIR.2021.100215.

[12] National Crime Records Bureau, 'Central Finger Print Bureau | National Crime Records Bureau', National Crime Records Bureau. Accessed: Mar. 23, 2022. [Online]. Available: https://ncrb.gov.in/en/central-finger-print-bureau

[13] H. S. Lallie, 'An overview of the digital forensic investigation infrastructure of India', *Digit Investig*, vol. 9, no. 1, pp. 3–7, Jun. 2012, doi: 10.1016/J.DIIN.2012.02.002.

[14] S. D. Jayasekara and I. Abeysekara, 'Digital forensics and evolving cyber law: case of BIMSTEC countries', *Journal of Money Laundering Control*, vol. 22, no. 4, pp. 744–752, Oct. 2019, doi: 10.1108/JMLC-02-2019-0019.

[15] H. M. A. van Beek, J. van den Bos, A. Boztas, E. J. van Eijk, R. Schramp, and M. Ugen, 'Digital forensics as a service: Stepping up the game', *Forensic Science International: Digital Investigation*, vol. 35. Elsevier Ltd, Dec. 01, 2020. doi: 10.1016/j.fsidi.2020.301021.

[16] K. R. R. Bhatele, D. D. Mishra, H. Bhatt, and K. Das, 'The Fundamentals of Digital Forensics and Cyber Law', *Cyber Warfare and Terrorism*, pp. 64–81, Mar. 2020, doi: 10.4018/978-1-7998-2466-4.CH005.

[17] L. Englbrecht, S. Meier, and G. Pernul, 'Towards a capability maturity model for digital forensic readiness', *Wireless Networks*, vol. 26, no. 7, pp. 4895–4907, Oct. 2020, doi: 10.1007/S11276-018-01920-5.

[18] M. D. Kohn, M. M. Eloff, and J. H. P. Eloff, 'Integrated digital forensic process model', *Comput Secur*, vol. 38, pp. 103–115, 2013, doi: 10.1016/J.COSE.2013.05.001.

[19] Agarwal A, Gupta M, Gupta S, and Gupta S, 'Systematic digital forensic inves... preview & related info | Mendeley', International Journal of Computer Science and Security. Accessed: May 09, 2022. [Online]. Available: https://www.mendeley.com/catalogue/f902584e-e6c0-3a21-9ca7-b4f5acb9b636/

[20] A. Al-Dhaqm *et al.*, 'Digital Forensics Subdomains: The State of the Art and Future Directions', *IEEE Access*, vol. 9, pp. 152476–152502, 2021, doi: 10.1109/ACCESS.2021.3124262.

[21] G. Horsman, '"I couldn't find it your honour, it mustn't be there!" – Tool errors, tool limitations and user error in digital forensics', *Science & Justice*, vol. 58, no. 6, pp. 433–440, Nov. 2018, doi: 10.1016/J.SCIJUS.2018.04.001.

[22] G. Horsman, 'Tool testing and reliability issues in the field of digital forensics', *Digit Investig*, vol. 28, pp. 163–175, Mar. 2019, doi: 10.1016/J.DIIN.2019.01.009.

[23] W. A. Bhat, A. AlZahrani, and M. A. Wani, 'Can computer forensic tools be trusted in digital investigations?', *Science & Justice*, vol. 61, no. 2, pp. 198–203, Mar. 2021, doi: 10.1016/J.SCIJUS.2020.10.002.

[24] N. Sunde and I. E. Dror, 'Cognitive and human factors in digital forensics: Problems, challenges, and the way forward', *Digit Investig*, vol. 29, pp. 101–108, Jun. 2019, doi: 10.1016/J.DIIN.2019.03.011/COGNITIVE_AND_HUMAN_FACTORS_IN_DIGITAL_FORENSICS_PROBLEMS_CHALLENGES_AND_THE_WAY_FORWARD.PDF.

[25] N. Sunde and I. E. Dror, 'A hierarchy of expert performance (HEP) applied to digital forensics: Reliability and biasability in digital forensics decision making', *Forensic Science International: Digital Investigation*, vol. 37, p. 301175, Jun. 2021, doi: 10.1016/J.FSIDI.2021.301175.

[26] Cervantes Mori M, Kävrestad J, and Nohlberg M, 'Success factors and challenges in... preview & related info | Mendeley', 2021. Accessed: May 08, 2022. [Online]. Available: https://www.mendeley.com/catalogue/41542552-4924-30cb-b51c-ce792698f457/

[27] T. Flory, 'Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies', *Journal of Digital Forensics, Security and Law*, 2016, doi: 10.15394/JDFSL.2016.1374.

[28] Garris J, 'Tackling the Unique Digital Foren... preview & related info | Mendeley', 2017. Accessed: May 08, 2022. [Online]. Available: https://www.mendeley.com/catalogue/41a2f9e5-1439-3f8b-98bc-ba29c74b9f29/

[29] R. Apau and F. N. Koranteng, 'An overview of the digital forensic investigation infrastructure of Ghana', *Forensic Sci Int*, vol. 2, pp. 299–309, Jan. 2020, doi: 10.1016/J.FSISYN.2020.10.002.

[30] N. Zahadat, 'Number 1 Article 3 3-31-2019 Part of the Computer Law Commons, and the Information Security Commons Recommended Citation Recommended Citation Zahadat', *Journal of Digital Forensics, Security and Law*, vol. 14, no. 1, 2019, doi: 10.15394/jdfsl.2019.1560.

[31] M. Losavio, K. C. Seigfried-Spellar, and J. J. Sloan, 'Why digital forensics is not a profession and how it can become one', *https://doi.org/10.1080/1478601X.2016.1170281*, vol. 29, no. 2, pp. 143–162, Apr. 2016, doi: 10.1080/1478601X.2016.1170281.

[32] N. Zahadat, 'Digital Forensics, A Need for Credentials and Standards', *The Journal of Digital Forensics, Security and Law*, 2019, doi: 10.15394/JDFSL.2019.1560.

[33] P. Mohan, 'Can India Address the Growing Cybersecurity Challenges in the Nuclear Domain? | ORF', Observer Research Foundation. Accessed: May 16, 2022. [Online]. Available: https://www.orfonline.org/research/can-india-address-the-growing-cybersecurity-challenges-in-the-nuclear-domain/

[34] S. D. Parmar, 'Cybersecurity in India: An Evolving Concern for National Security', *International Journal of Cyber Security*.

[35] DeVry University, 'Computer Forensics vs. Cyber Security', DeVry University. Accessed: May 16, 2022. [Online]. Available: https://www.devry.edu/online-programs/area-of-study/cyber-security/computer-forensics-vs-cybersecurity.html

[36] National Crime Records Bureau, 'Cyber Crimes (State/UT-wise) - 2018-2020', National Crime Records Bureau. Accessed: Apr. 14, 2022. [Online]. Available: https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/TABLE%209A.1.pdf

[37] A. Tibbi, 'UP Police Constable Recruitment 2022: Vacancy, Notification PDF, Apply Online'. Accessed: Apr. 16, 2022. [Online]. Available: https://www.sainikschooladmission.in/up-police-constable-recruitment-notification-form-apply/

[38] Ministry of Home Affairs, 'SCHEME FOR COMMON RECRUITMENT OF CONSTABLES IN CENTRAL POLICE FORCES TO BE CONDUCTED BY STAFF SELECTION COMMISSION', *Ministry of Home Affairs*. 2011.

[39] M. G. Naik, 'Crime rate comes down in Malpe after CCTV camera installation | Deccan Herald', *Deccan Herald*, Jul. 2016. Accessed: Apr. 24, 2022. [Online]. Available: https://www.deccanherald.com/content/556777/crime-rate-comes-down-malpe.html

[40] R. Malpani and M. Chablani, 'Impact of CCTV surveillance on Crime'.

[41] A. ul Haque, '"More camera surveillance does not equate to lower crime rate" -', *Patriot*, 2021. Accessed: Apr. 24, 2022. [Online]. Available: https://thepatriot.in/2021/10/26/more-camera-surveillance-does-not-equate-to-lower-crime-rate/

[42] P. DALMIA, 'DATA PROTECTION LAWS IN INDIA - EVERYTHING YOU MUST KNOW - PRIVACY - INDIA', *MONDAQ*, 2017, ACCESSED: APR. 24, 2022. [ONLINE]. AVAILABLE: HTTPS://WWW.MONDAQ.COM/INDIA/DATA-PROTECTION/655034/DATA-PROTECTION-LAWS-IN-INDIA--EVERYTHING-YOU-MUST-KNOW

[43] Indian Courts, 'High Courts - eCourt India Services'. Accessed: May 03, 2022. [Online]. Available: https://services.ecourts.gov.in/ecourtindia_v6/static/highcourts.php