IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Analysis Of Whatsapp Messenger Data Through Digital Forensic Techniques.

[1]Meghna R

[1]LLB Student, Symbiosis Law School, Pune, India.

Abstract: Rise of technology in this digital era has paved way not only to the increase in means of networking and communication, but also several digital scams. Apart from scams several acts of crime happen in a virtually manifested environment. WhatsApp is one of the most predominantly used IMS, where such offences might take place, along with the great many advantages it provides. Under the sect of Digital Forensics, the procurement and analysis of such material device, can be carefully extracted and produced as evidence. The extent of its admissibility and the many procedures for such report to be produced without any tampering is explained in this paper. The observation with the current trend of rise in crimes in digital devices can be noted. The paper in furtherance focuses on WhatsApp Messenger data and the several ways it is used to deceive people and to usher an offence. It also makes a comparative study on Digital Forensic report in India with respect to its global counterparts.

Index Terms: WhatsApp Messenger, Digital Forensic, Evidence, Criminal Report.

I. INTRODUCTION

Every individual in this digital era possesses an Android phone, and use these android mobiles in their day-to-day life so much so that a day doesn't pass without its usage and application. Communication and building network around the world are the prime purpose of these mobile phones. Apart from phone calls, messaging systems have far developed and surpassed its expectations and within a blink of an eye, messages are transmitted.[1] Any number of messages can be relayed in seconds and the information including many personal data is being exchanged at a higher rate. This gives opportunity to people of malignant motives to commit offences through the easiest and fastest way as well. In today's world there is no need for people to meet physically to form a coupe and commit crime. This is made possible by several instant messaging services. One can organize, plan and commit crime in this environment, without any immediate external interference

[1] Kennedy, Dennis. "TECHNOLOGY: GET THE (INSTANT) MESSAGE, DUDE! By Phone or PC, Messaging Offers Several Advantages." ABA Journal, vol. 94, no. 11, 2008, pp. 40–41. JSTOR, http://www.jstor.org/stable/27846842.

through their mobile devices.[2] One such frequently used Instant messaging service is WhatsApp. WhatsApp provides encrypted services and is a cross platform application that is made available to all with any smart mobile devices. Many activities can take place in different mechanisms either via personal chats, broadcasting messages or formation of groups. In case a crime is being committed and a group chat is being opened to discuss and organize a crime and plan the course of action, the conviction of these members remains and is open to several interpretations and defence arguments. The extraction of these messages should be done by collecting the mobile device on one them and the examination of the device, is done and submitted as an electronic record in the court. While seizure is done by the investigation officer, the identification, extraction, analyses and presentation are done by the Digital forensic team.[3] A normal investigation procedure cannot be done by any crime that is been executed or organized in a virtual environment. The importance of the Digital forensic techniques is pivotal.[4]

II. Issue at Hand

There are numerous challenges faced from the time of recovery of data till the time of it being displayed in the court. The issue arises when there is no set environment to make proper evaluation of the recovered digital device.

2.1 Research Objective

The objective of the paper is to make a detailed study on the ways in which Digital forensic science is being used to extract the data in question, to produce it as evidence. To study regarding its admissibility in the court of law. To analyse the procedure followed in India alongside its global counterparts.

2.2 Research Question

The research question comprises as follows: *How do Digital forensic experts process the data from WhatsApp messenger to produce it as evidence? To what extent is this data being appreciated in the Court as Evidence? What are the ways in which these WhatsApp chats and recordings are used to be produced as Evidence without duping with the help of Forensic Science? How well is Indian Legislation functions at par with its global counterparts?*

III. Research

3.1 Components in Digital Forensic

Digital Forensic is also known as “cyber forensics” or “computer forensic”, as the name suggests it deals with making forensic investigation on electronic devices which have been wither found in the scene of crime or allegedly involved in the commencement. The investigation done, can be used in variety of places in proving

[2] KSHETRI, NIR. “Diffusion and Effects of Cyber-Crime in Developing Economies.” *Third World Quarterly*, vol. 31, no. 7, 2010, pp. 1057–79. *JSTOR*, http://www.jstor.org/stable/27896600.
[3] Tanvi, Gupta, Suruchi, Parashar, Aju D, “A Study of Cybercrimes in India using Digital Forensic” iJraset,Vol.8, No. X, Oct 2020, https://doi.org/10.22214/ijraset.2020.31865.
[4] CBI v. Arif Azim, 2013

the accused guilty or even innocent, as our lives are so entwined with the electronic devices around us. This makes us dependent on those devices, thus the information contained in such devices are enormous and thus when some evidences are deleted, some can be retrieved or any other modes even google searches can be linked to the crime committed to establish motives of the accused person, and vice-versa.[5]

There are different ways of Forensic examinations as follows[6]:

- Database Forensic: It comprises of a study done on databases and metadata (data about data)
- Disk Forensic: It deals with study of extracting data from storage media.
- Email Forensic: It is an investigation made to analysis the source and content of an email, also identify, inspect, scan and conduct keyword searches, relating to emails.
- Malware Forensic: It is an investigation made to locate a hacker, examine aspects of malware to identify a perpetrator and cause of attack.
- Memory Forensic: It is a study made to extract volatile data from the memory dump, it is used to investigate and detect any breach or malicious activities.
- Mobile Forensic: It is an investigation made in the mobile devices, by accessing the internal memory and extracting various information about the owner.
- Network Forensic: It is used to investigate upon more volatile and dynamic data, as the network traffic can be lost and a study makes a proactive inquiry. It also comprises of a division of Wireless Forensics

The steps to make a digital forensic investigation are as follows[7]:

- Identification: This is the first step taken to identify the source and the purpose of the investigation.
- Preservation: The step 2 after identification is followed by preservation of the data in question by isolation and securing the given information.
- Analysis: After preservation, the data is being extracted to interpret the data, here certain tools and techniques are used to process the data.
- Documentation: After analysing the data, a record of all the visible data should be made, which helps recreate the crime scene.
- Presentation: The final step is to make a layout so as to the data that has been documented can be presented with the required expertise vouching for the data to make a presentation in the court of law.

A few techniques used by Digital forensic experts are listed below:

- Reverse Steganography: To identify data encrypted and to extract them from relevant files into readable format.

[5] Garfinkel, Simson L. "Digital Forensics." American Scientist, vol. 101, no. 5, 2013, pp. 370–77. JSTOR, http://www.jstor.org/stable/43707091.
[6] Shreeya, Panjala, Vinihsa, Kaveti, "Digital Forensics In India- An Overview", Feb 2022, https://lawtimesjournal.in/digital-forensics-in-india-an-overview/#_ftn8.
[7] Alissa, K., Almubairik, N.A., Alsaleem, L. et al. A comparative study of WhatsApp forensics tools. SN Appl. Sci. 1, 1320 (2019). https://doi.org/10.1007/s42452-019-1312-8.

- Stochastic Forensic: Analysing theft and reconstructing digital activity to give rise to the property that has been stolen with the help of the stochastic nature of modern computer.
- Cross drive and live analysis: To help make a study of the data from disks and also a using tool to extract information of computers.

3.2 MODERN-DAY EVIDENCE: USAGE OF DIGITAL FORENSIC IN WHATSAPP CHATS AND RECORDINGS

WhatsApp is a cross platform application that can be accommodated in any mobile devices with any operating system making it an application with universal application. WhatsApp Messenger is not phone dependent or operating system dependent, that is, WhatsApp doesn't support only a particular type of phone or its operating system.[8] The versatile use of WhatsApp messenger not only favours the innocent users, but also hackers and offenders the same. The below image explains the level of vulnerability that WhatsApp holds though its uses supersede our risks.

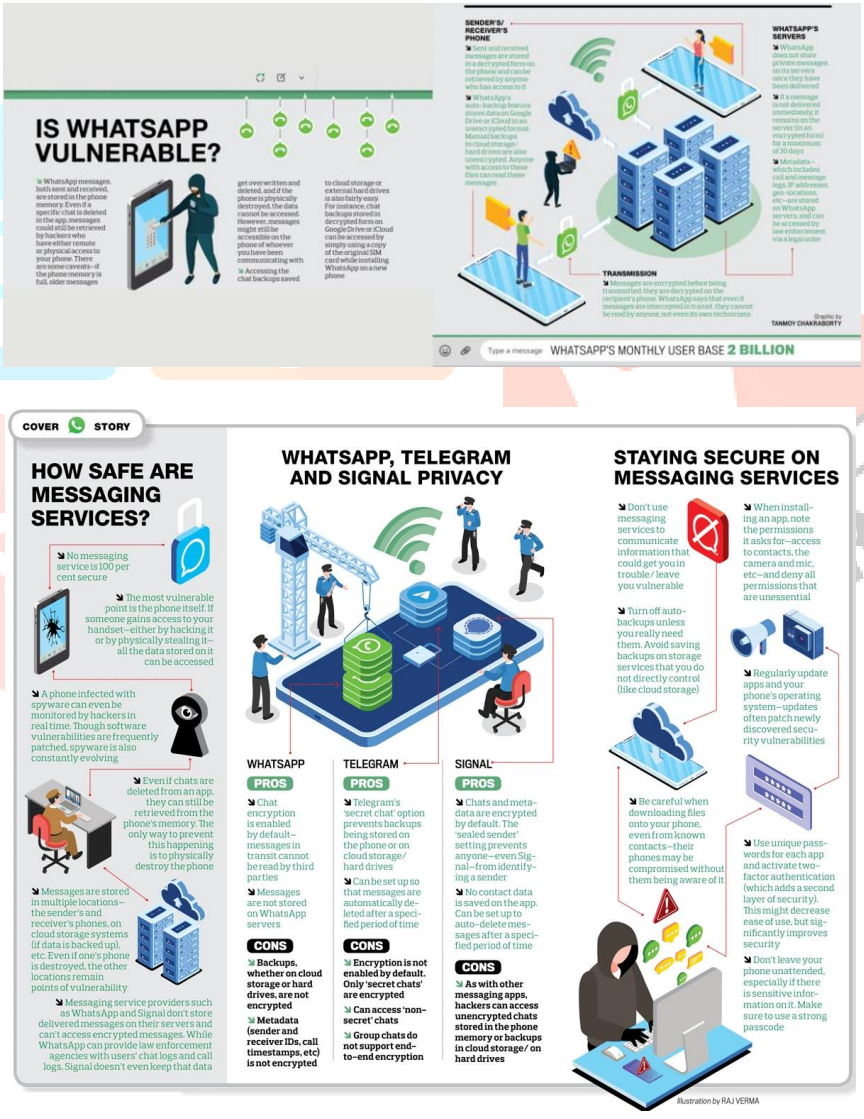


Image explaining the question of if WhatsApp is vulnerable?[9]

[8] Thakur, Neha S., "Forensic Analysis of WhatsApp on Android Smartphones" (2013). University of New Orleans Theses and Dissertations. 1706., https://scholarworks.uno.edu/td/1706.

[9] Deka, Kaushik, "How private are your WhatsApp chats?", Oct 2020, https://www.indiatoday.in/magazine/cover-story/story/20201012-how-private-are-your-whatsapp-chats-1727605-2020-10-03.

Various tools have been developed to extract information from the WhatsApp Messenger, and cane be broadly discussed as follows:

- Physical Extraction, it comprises of copying the devices's storage and is used in older devices.
- Logical Extraction, used often through the OS of the devices and application interface.
- Cloud Extraction, it is made by backing up the device to a cloud service network like the Google drive or iCloud, once the investigator get access of the backups.

There are majorly two forms of acquisition of data from WhatsApp:

- Hardware Acquisition and
- Software Acquisition.

Hardware Acquisition techniques involve the physical analysis with the mobile devices and analyses is made by looking into different database files of WhatsApp in the phone's internal memory. Consideration of extraction of deleted messages will be stored in RAM. Database extraction is proceeded with UFED Physical analyser and to obtain an unencrypted version one needs to root the phone.[10] Information took from the hardware acquisition of data comprises of chat message artifacts, Timestamps and names of different files sent and received from the media storage location in our phones.

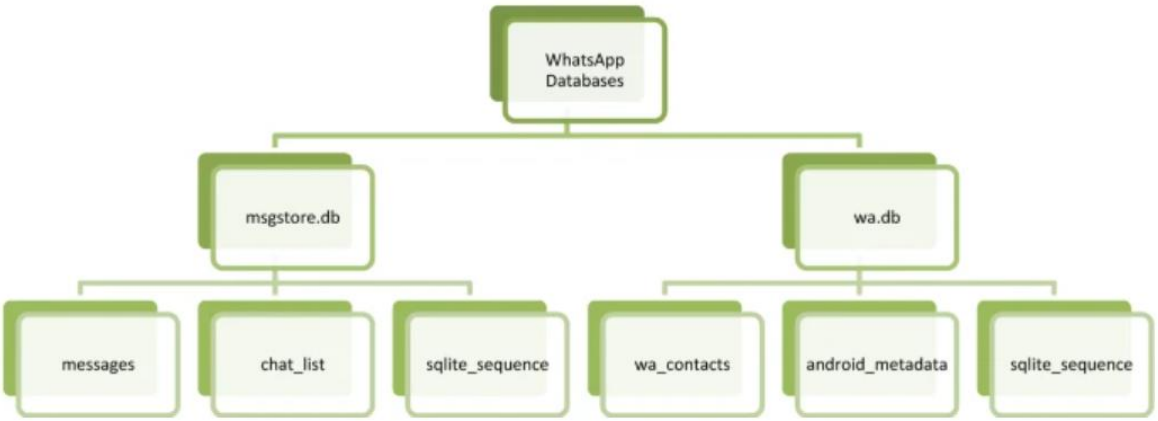
Row #	Content	Directory	File
1	contacts database	/data/data/ com.whatsapp/databases	wa.db (SQLite v.3)
2	chat database	/data/data/ com.whatsapp/databases	msgstore.db (SQLite v.3)
3	backups of the chat database	/mnt/sdcard/ Whatsapp/Databases	msgstore.db.crypt msgstore-<date>.crypt
4	avatars of contacts	/data/data/ com.whatsapp/files/ Avatars	UID.j, where UID is the identifier of the contact
5	copies of contacts avatars	/mnt/sdcard/ What-sApp/ProfilePictures	UID.j, where UID is the identifier of the contact
6	log files	/data/data/ com.whatsapp/files/ Logs	whatsapp.log, whatsapp-<date>.log
7	received files	/mnt/sdcard/ Whatsapp/Media	various files
8	sent files	/mnt/sdcard/ Whatsapp/Media/Sent	various files
9	user settings and preferences	/data/data/ comm.whatsapp/files	various files

Image of WhatsApp Messenger Artifacts[11]

[10] Mahajan, Aditya, M., S. Dahiya, and H. P. Sanghvi. Forensic Analysis of Instant Messenger Applications on Android Devices.", (2013) [3]

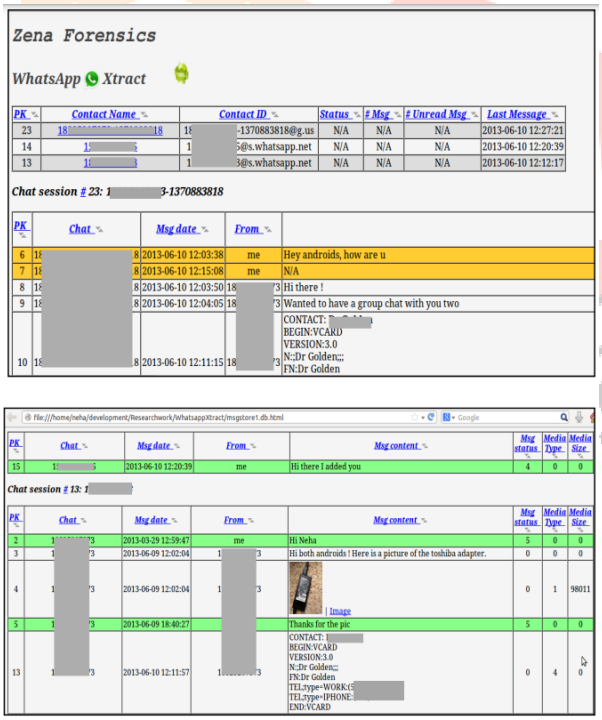
[11] Cosmo Anglao,"Forensic Analysis of WhatsApp Messenger on Android Smartphones", Digital Investigation Journal, Vol. 11, No. 3, pp. 201–213, September 2014, doi:10.1016/j.diin.2014.04.003

The database of the WhatsApp is as shown in the image:



Flowchart of the WhatsApp databases.[12]

Software Acquisition, the first tool was built to decrypt and organize SQLite data base files in an organised HTML form.[13] This tool can work with both the encrypted and decrypted database files. Through the SQLite browser such as the Zenforce being one of the many examples, the tool can represent static data , the timestamps from this tool are not entirely straightforward but the main advantage stands that media need not be accessed through separate files they simply display over the HTML Page itself.



Snapshot of Zenforce being executed[14]

WhatsApp database Extraction has several steps and can be used by many technique on such is extraction based on Oxygen Forensics, with Andriller.[15] Retrieval of deleted messages is also possible by going through several files that have stored data and cannot be removed as they are stored only destruction of the phone

[12] Alissa, K., Almubairik, N.A., Alsaleem, L. et al. A comparative study of WhatsApp forensics tools. SN Appl. Sci. 1, 1320 (2019). https://doi.org/10.1007/s42452-019-1312-8

[13] Aqeel Khalique, "Implementation of Forensic Analysis Procedures for WhatsApp and Viber Android Applications", International Journal of Computer Applications, Vol., 128 , No.12, October 2015.

[14] Thakur, Neha S., "Forensic Analysis of WhatsApp on Android Smartphones" (2013). University of New Orleans Theses and Dissertations. 1706.

[15] Yuliani, Vindy & Riadi, Imam. (2019). Forensic Analysis WhatsApp Mobile Application On Android-Based Smartphones Using National Institute of Standard and Technology (NIST) Framework. International Journal of Cyber-Security and Digital Forensics. 8. 223-231. 10.17781/P002615.

would lead to deletion of messages. There are several forensic tools to extract and explore, decrypt information from the electronic devices to read the data, SalvationDATA WhatsApp Forensics, Elcomosft WhatsApp Explorer, Guasap and WhatsApp Key/DB Extractor. The following are the functionalities of the tools[16]:

- To check if the devices is rooted.
- The device is rooted to the authority in control.
- To extract WhatsApp Multimedia
- To extract encrypted database
- To extract WhatsApp logs.

3.3 ADMISSIBILITY OF WHATSAPP DATA

Admissibility of WhatsApp is the court of law has been questioned time in and out as the chance of tapering, mishandling and mismanagement of the data at hand. Apart from these reasons, the admissibility of such data is questioned due to no proper authorization by the holder of the electronic devices.

3.4 LEGAL PROVISION:

The legal provision that enforces on appreciability and admissibility of electronic evidence such as WhatsApp chats and recordings that might hold information be challenged as evidence by the alleged accused or even the victim.

- Sec 2(1)(t)[17] of IT Act, 2000, that defines an electronic record, as a any records that are in an electronic form and stored in computer generated system.
- Sec 3[18] of Indian Evidence Act, that defines "electronic record" as evidence under the definition of "Documentary evidence".
- Section 65A[19] of Evidence Act, provides special provision to produce any evidence as electronic evidence.
- Section 65B[20] of Evidence Act, that illustrates how the electronic records need to produced in order for it to be admissible in the court.
- Section 79A[21] of IT Act, provides that the Central Government to provide notification to the examiners for the electronic evidence to get and expert opinion on matters dealt in court.

The admissibility in the court of law depends upon the originality of the document for it to be considered either of it being a primary evidence or secondary evidence according to the sections 64 and 65 of Evidence Act[22]. A 3-judge bench of the Apex court, held that, WhatsApp chats is admissible when there is authentic

[16] Alissa, K., Almubairik, N.A., Alsaleem, L. et al. A comparative study of WhatsApp forensics tools. SN Appl. Sci. 1, 1320 (2019). https://doi.org/10.1007/s42452-019-1312-8
[17] Information Technology Act, 2000 § 2 , No. 21, Acts of Parliament, 2000(India).
[18] Indian Evidence Act, 1872, Act No. 1 of 1872, Acts of Parliament, 1872 (India).
[19] Indian Evidence Act, 1872, Act No. 1 of 1872, Acts of Parliament, 1872 (India).
[20] Ibid
[21] Information Technology Act, 2000 § 79A, No. 21, Acts of Parliament, 2000(India).
[22] Indian Evidence Act, 1872, Act No. 1 of 1872, Acts of Parliament, 1872 (India).

certification of the particular electronic record.[23] It is then accepted that WhatsApp chats are to understood in a cumulative manner and not deciphered separately.[24]

IV. ANALYSIS

4.1 DESCRIPTIVE ANALYSIS

The Digital Forensic department has evolved since with evolution of technology to better be able to identify the source and present it before the court. Apart from criminal usage digital forensic is used in civil cases as well, in case to prove that the WhatsApp messenger chats where even the WhatsApp blue ticks as proof for service summons[25]. WhatsApp chats are thus being used in several area to prove as electronic record evidence. The consent of the holder of the electronic device is of importance as the illegally handling and production of evidence is again held invalid. It was argued that in recent Aryan Khan's case the WhatsApp chats should be held inadmissible as there was no proper certification and authentication given to handle such material devices.

4.2 STATISTICAL ANALYSIS

The below image provides statistical data regarding the amount of users of WhatsApp Messenger.[26]

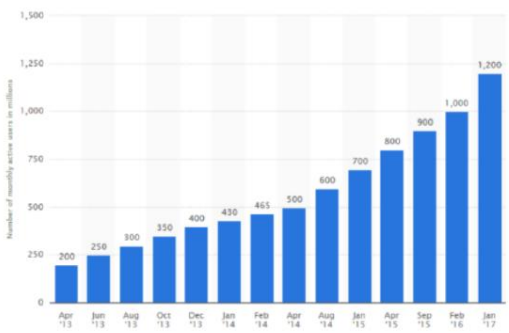


Figure 1. The statistics of whatsapp user

Figure 2. The statistics of whatsapp messages

4.3 ANALYSIS WITH CASE LAWS

- In Ambalal Sarabhai Enterprise Ltd. v. KS Infraspace LLP Limited and Another[27], it was held that WhatsApp messages should not be considered and read separately but in a cumulative manner.

[23] Arjun Pandit Rao v. Kailash Kushanrao,(2020) 7 SCC 1.
[24] Sanjay Rawat, "Are WhatsApp Chats Admissible in Court?", Nov 2021, https://sociallawstoday.com/national-green-tribunal/#_ftn9.
[25] Viswajith Anand, "Whatsapp Summons : Positive Trends Of Courts Embracing Technology", Feb 2019, https://www.livelaw.in/columns/whatsapp-summons-positive-trends-of-courts-embracing-technology-142608?infinitescroll=1
[26] Yuliani, Vindy & Riadi, Imam. (2019). Forensic Analysis WhatsApp Mobile Application On Android-Based Smartphones Using National Institute of Standard and Technology (NIST) Framework. International Journal of Cyber-Security and Digital Forensics. 8. 223-231. 10.17781/P002615.
[27] Ambalal Sarabhai Enterprise Ltd. v. KS Infraspace LLP Limited and Another,(2020) 5 SCC 410.

- In Rakesh Kumar Singla vs Union Of India[28], had granted liberty to the NCB that upon compliance with Section 65(b) of the Evidence Act, to rely on the WhatsApp messages.
- In National Lawyers Campaign for Judicial Transparency and Reforms v Union of India[29], it was held that Forwarded messages cannot be held as 'Documents'.

4.4 Comparative Analysis

India has lack of technical expertise when compared to its global counterparts who have technology and experts to provide with greater amount of efficiency. The evolution in the US technology in field and policy changes have been farfetched.[30] The United States has the Computer Fraud and Abuse Act (CFAA) and the Federal Rules of Evidence, which govern digital evidence. The European nations are governed by the General Data Protection Regulation (GDPR), which has implications for digital evidence handling. While the backlogs or the pending cases in the departments are similar everywhere as the digitization expands the need for the law enforcement to grow along with it grows. The issues of documentation, that is, the authentication and the chain of custody is the same all around.[31]

4.5 Critical Analysis

The evidence and data collected to incriminate a person shall not in any way disturb the right to privacy of the people surrounding. If a larger amount of spyware technology and ability is given for the government in accessing private information, this data might as well be used for enforcing their political agenda. The sensitive data in case, later turn into making the general public more vulnerable and influenced to the motives of the one who handles these data. In name of precaution and public safety exploitation of public might occur. Hence the data should be left as encrypted and inaccessible to anyone, only in matters of crime can the data be accessed to provide justice with proper certification being produced. WhatsApp messages being accessed without proper certification may lead to self-incrimination of the alleged accused though it may seem appealing way to expose the truth, the question of whether fair trial is being followed in face of self-incrimination is food for thought.

V. Suggestions and Conclusion

India is Digitizing at a faster rate and the legislation though taking a little setback to be passed and resolved, but while it comes to form of implementation it is rather later than the speed at which the technology is being developed. India is still facing a growing problem in having number of experts in the digital sector, in departments of digital forensic to establish timely justice. The need in the current era of digital experts is seen with the number of setbacks and pending cases which are yet to resolved. Awareness needs to be provided to

[28] Rakesh Kumar Singla vs Union Of India , (2020) Gujrat High Court 1834
[29] National Lawyers Campaign for Judicial Transparency and Reforms v Union of India, 2019 SC 191
[30] Third Way. 2020 Thematic Brief: US Cybersecurity Efforts. Third Way, 2020. JSTOR, http://www.jstor.org/stable/resrep26169.
[31] Goodison, Sean E., et al. "Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence." Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, RAND Corporation, 2015, pp. 1–32. JSTOR, http://www.jstor.org/stable/10.7249/j.ctt15sk8v3.1.

the general public regarding various fraudulent practises that are taking place along with their duty not to exploit people. The privacy laws in India have to be made more stringent in face of personal data being accessible and stolen by malignant users. The conclusion can be made with highlighting the increased importance of Digital Forensics in India.