Bulletin of Environment, Pharmacology and Life Sciences
Bull. Env. Pharmacol. Life Sci., Spl Issue [5] 2022 : 62-69
©2022 Academy for Environment and Life Sciences, India
Online ISSN 2277-1808
Journal's URL:http://www.bepls.com
CODEN: BEPLAD
REVIEW ARTICLE **OPEN ACCESS**

Future, Resources, and Obstacles of Mobile Phone Forensics

Bhoopesh Kumar Sharma[1], Rajiv Vatsa[2], Nishith Kumar Mishra[3], Yogesh Sharma[4],M. T Ahmad Beig[5]
[1]Professor, Faculty of Science, SGT University Gurugram, Haryana – 122505
[2]Research Scholar, Faculty of Science, SGT University Gurugram, Haryana – 122505
[3]Associate Professor, Faculty of Commerce and Management, SGT University Gurugram, Haryana - 122505
[4-5]Assistant Professor, Faculty of Science, SGT University Gurugram, Haryana - 122505
Corresponding Author: Dr. Bhoopesh Kumar Sharma (bhoopesh_fosc@gmail.com)

ABSTRACT

Numerous illegal actions have an effect on the lives of hundreds of millions of people who rely on their smartphones to get them through the day. As the popularity of smartphones continues to rise, so does the possibility that they may be exploited for criminal purposes. There is a wealth of applications, cutting-edge hardware, and operating systems built into today's smartphones. Thanks to improvements in semiconductor technology and an increase in processing power, mobile phones have become more effective while still being tiny enough to fit in a pocket. As a result, Forensic investigators faces difficulties when trying to investigate a mobile phone to analyse evidence. The data stored on mobile devices has become a crucial piece of evidence in forensic investigations. Knowledge of forensic instruments and their capabilities is essential for gathering meaningful information from the digital devices. In this study, we analyse the features of certain cutting-edge data formats that might be presented as mobile device evidence for Forensic investigations. Some of the newest technology for mobile phone evidence collection is also discussed, along with their efficacy. This review examines the features of mobile devices, the procedures of mobile forensic investigations, the different mobile forensic technologies, and their present and future uses.

Keywords: *Digital Evidences, Criminal Activities, Emerging Technology, Mobile Phone Forensics, Forensic Investigation*

Received 22.10.2022 Revised 23.11.2022 Accepted 20.12.2022

INTRODUCTION

Hundreds of millions of people's regular phone use is disrupted by various illicit activities. The proliferation of smart phones has coincided with a rise in the possibility that they would be employed in criminal acts [1]. There is a wealth of applications, cutting-edge hardware, and operating systems built into today's smartphones. Since the first "bag and brick" models appeared in the middle of the 1990s, mobile phones have become an integral part of our everyday lives [1, 2]. Thanks to improvements in semiconductor technology and an increase in processing power, mobile phones have become more effective while still being tiny enough to fit in a pocket. With the advent of smartphones and the growth of 5G networks, there are now more than 5.31 billion people throughout the world who use their phones regularly [3]. The proliferation of smartphones is in large part attributable to the success of free social messaging applications like WhatsApp, Telegram, Instagram, and Facebook. More than half a million people join the Internet every day, which amounts to a yearly growth rate of over four percent [3, 4]. Security risks posed by mobile apps have skyrocketed as their use has grown. Since the number of mobile transactions has doubled in the past few years, hackers are increasingly focusing on mobile consumers as a primary target for online and internet fraud. [4].

Security experts warn that employees' rising reliance on BYOD and mobile devices to access sensitive company information raises the likelihood of breaches. Fake applications distributed via the Google Play Store are a common vector for cybercriminal attacks. A wide variety of free smartphone apps have been utilised for forensic reasons, such as digitally inspecting the crime scene and other evidence [5].

However, this freeware once again may have a huge security impact when received from open sources or without authentication. Users that are tricked into installing them have their data stolen. McAfee claims that many of these malicious programmes mimic popular mobile software. There are several phoney apps pretending to be different versions of popular games like Fortnite, which has over 200 million users worldwide and over 60 million downloads. [6].

New methods of dissemination for cybercrime are also being developed. All sorts of methods, from SMS phishing to legitimate apps that circumvent app store security, can be used to spread malware. As mobile banking becomes more ubiquitous, cybercriminals have responded by enhancing the sophistication of their malicious software. They are able to evade security measures and steal more than just credit card data. Accessing data is made simple with the help of smartphones.

The most readily available data from a mobile device are text messages, call logs, and phone records [6]. Cyber security companies have started working with mobile device makers to improve user safety. Examples of bolstered partnerships are those between McAfee and Samsung and Türk Telekom [7]. Customers will be safer from online dangers thanks to Samsung and McAfee's partnership, which includes pre-installed McAfee Virus Scan anti-malware software. Symantec claims that mobile phones are the most effective spying weapon ever made in their Internet Security Threat Report. The firm claims that users may learn much more about their surroundings using a smartphone that has a camera, microphone, and GPS tracker. The efficacy of the cell phone forensic tool is determined by comparing the data collected from the mobile device to the baseline. The Subscriber Identity Module (SIM card) is now the most widely used identity module [8]. It is used to keep private information separate from the phone or tablet, to enable phone ubiquity, and to retain contact information, names, and communications networks. Finding the sources of evidence that will be useful for an investigation is one of the most pressing practical issues faced by digital investigators. It may be difficult to identify which sources of evidence are crucial to an inquiry, even if the evidence is found.

2. Comparing Digital Forensics and Mobile Forensics

Digital forensics refers to the practises involved in investigating and analysing digital evidence [9]. With the goal of presenting this data as evidence in a legal proceeding. When a crime is committed in the digital environment, digital forensics is triggered. Also, as can be shown in Figure 1, there are several subfields within the field of digital forensics.

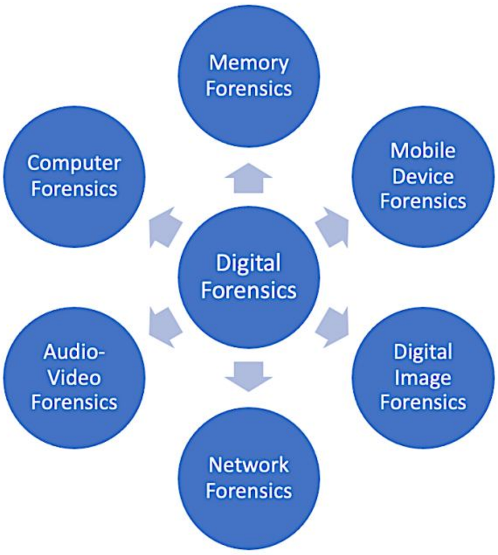


Fig 1: Components of Digital Forensics

As the number of people who own and regularly use smartphones rises, so does the significance of mobile device forensics. Smartphones are commonly discovered at crime scenes, therefore this is a brilliant idea. Mobile phone forensics is "the art and science of obtaining digital evidence from a smart phone using recognised forensic procedures," as defined by the National Institute of Standards and Technology [9, 10]. Meeting this need is complicated by factors such as the rapid pace at which new mobile phone models are introduced, the wide diversity of available operating systems, and the wide range of available hardware. Forensics is employed in many ways during an internal audit inquiry, much like it is during a criminal investigation. The world is better because forensics helps put an end to crime and wrongdoing. As shown in Figure 2, the primary objective of mobile device forensics—a subfield of digital forensics—is to collect evidence and information from mobile devices such as smartphones.

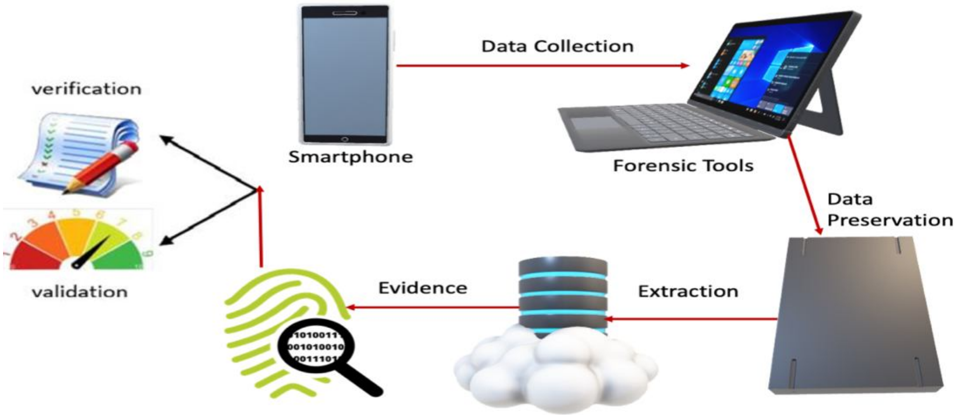
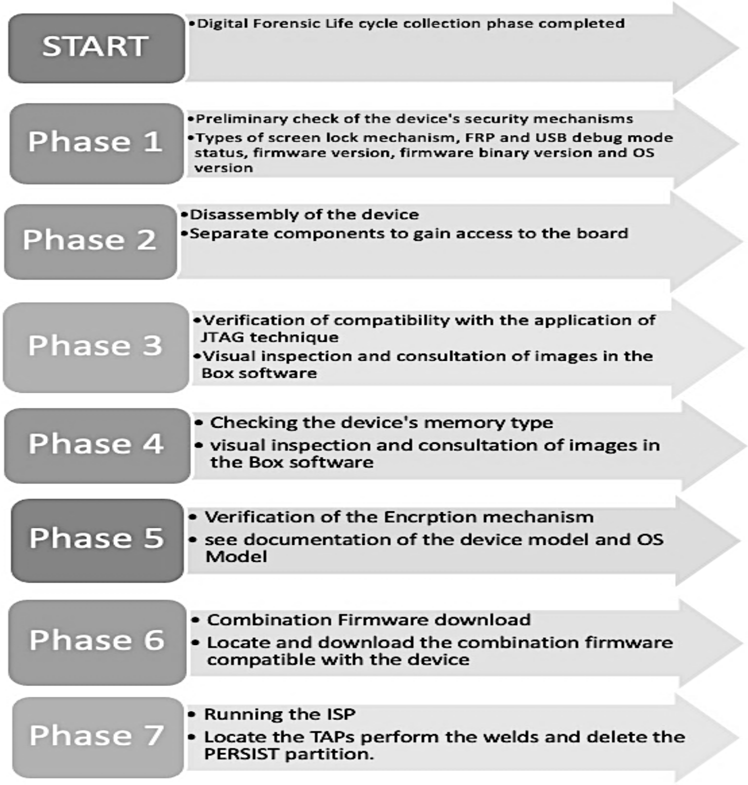


Fig 2: Process of Digital Evidence Analysis



START
- Digital Forensic Life cycle collection phase completed

Phase 1
- Preliminary check of the device's security mechanisms
- Types of screen lock mechanism, FRP and USB debug mode status, firmware version, firmware binary version and OS version

Phase 2
- Disassembly of the device
- Separate components to gain access to the board

Phase 3
- Verification of compatibility with the application of JTAG technique
- Visual inspection and consultation of images in the Box software

Phase 4
- Checking the device's memory type
- visual inspection and consultation of images in the Box software

Phase 5
- Verification of the Encrption mechanism
- see documentation of the device model and OS Model

Phase 6
- Combination Firmware download
- Locate and download the combination firmware compatible with the device

Phase 7
- Running the ISP
- Locate the TAPs perform the welds and delete the PERSIST partition.

Figure 3: A typical digital forensic investigation's phases and steps

When looking into a case involving mobile device-based communication, forensics may be used to provide light on a number of questions [11]. Mobile device forensics differs significantly from digital forensics in that it necessitates dealing with a wide range of hardware and software standards, making the development of a globally accepted standard instrument difficult [12]. The many steps involved in digital forensics are shown in Figure 3. Due to the lack of uniform and built-in techniques for data retrieval, Mobile device software is more specialised than PC software, therefore there are more alternatives to choose from. The proliferation of new phone models and the emergence of companies with their own proprietary software have made it more difficult to address the problem of mobile devices being used in criminal activity. Forensic tools for smartphones are designed to be non-destructive, allowing investigators to collect as much information as possible from the device in question. Important updates should be sent via the tool quickly in order to keep up with the rapid changes in mobile phone operating systems [12, 13]. Forensic and non-forensic tools each have their own advantages and disadvantages. Some of the features of a modern smartphone that might prove useful in a forensic investigation are: geolocation, ringtones, pre-programmed replies, live video, still image files, email alerts, and geolocation.

Computer and mobile phone forensics include collecting and analysing data from a device in great detail. Windows, Mac OS, and Linux are the most often encountered OSs in the field of computer forensics. Goal-wise, things are very much the same, but the obstacles are all over the place. Due to the frequent OS updates in mobile forensics, constant monitoring is required to guarantee the most up-to-date results. Because they are meant to be carried along, mobile gadgets are constantly online [14]. Therefore, preventing data tampering requires rapid evidence processing. It is conceivable, for instance, to direct a mobile phone to erase all of its data in response to a remote command. Mobile device detectives risk losing all their work if the phone is not properly isolated from wireless transmissions. Different data extraction depths and their advantages and disadvantages are compared in Table 1.

LEVEL	ADVANTAGES	DISADVANTAGES
Manual Extraction	lacking a specialist tool and has little technical complexity	Large data volumes take a lot of time, there's a chance that data will be accidentally modified, lost data can't be recovered, and it's probably impossible with damaged equipment
Logical Extraction	High data abstraction level; simple technical requirements	Limited access to data; possibility of unintentional data change (remnants)
Hex dumping/Joint Test Action Group (JTAG)	Attainable using common communication interfaces; treats damaged devices; provides access to data leftovers	Data decoding and parsing can be challenging; JTAG requires substantial expertise; there is no guarantee of access to all memory sectors.
Chip-off	Gives a full binary image that is appropriate for standard analysis.	Physical harm possibility; significant training necessary
Micro read	Viable last-resort option	Technically challenging and incredibly resource-intensive

Solid-state non-volatile memory is used in mobile devices instead of traditional hard drives due to its many advantages over traditional memory technologies, including lower power consumption, greater reliability, lower weight, and greater durability. There are no platters or other moving elements in a solid-state drive. While analysis of solid-state drives can follow the same basic procedure and strategy as that of hard disc drives, there are certain key differences that may aid or hinder an investigator [15]. Solid-state drives don't need magnetic charges to store data on a device. In its place, they employ a network of gates to temporarily store the energy of a single electron, with each gate standing in for a different binary digit. Since the gate mechanism limits the drive's write capability, the Flash Transition Layer controls where data is recorded to and how gates are used. The benefit goes to the investigator since the drive can prevent further writing to the deleted data, hence extending the gate's useful life. It is also possible for the contents of the volatile memory to be copied to the non-volatile memory before powering down the device. Nonetheless, solid-state may be a challenge for detectives to work with due to the fact that data that has been successfully erased cannot be recovered [3, 15].

3. Digital dangers linked to smartphones

Cybercrime and other crimes committed utilising digital technology are on the increase along with the proliferation of electronic gadgets. Each of these innovations—from the iPhone to the flip phone—has had and will continue to have a major impact on modern culture [5, 15]. While most individuals have become accustomed to having their every need met, con artists persist. The sophisticated cyberthreats that have emerged throughout time to fool nave people include phishing, fake networks, malicious software, and grayware.

3.1. Cell Phone Acquisitions:

Smartphones may store a lot of information and function as minicomputers on the go. Because there is so variety in mobile phone design, certain acquisitions will generate greater returns than others. Mobile devices may be able to collect the following types of information: Information such as location, call logs, pictures, videos, and text messages, as well as audio files such as voicemails, music, and more. Data from your calendar, documents, browser history, notes, emails, and applications (social media, user behaviour, etc.). Since it is hard to keep up with the steady influx of new phones and the technical improvements that go along with them, there is no universal technique for accessing mobile phone data [16]. There are four main types of cell phone purchases:

- Screen captures: Images of what is displayed on the phone's screen are captured using a camera. Using a mobile phone is usually the only way to keep data private.
- Logical analysis (LA): The process of obtaining data from your mobile phone that you can see and access is known as logical analysis, or LA. Today, this tactic is the most often employed.

- Physical analysis enables information to be extracted from both the internal and external memory of the device.
- Chip level analysis: the procedure of removing the storage chips from the phone and doing an information search on them in order to conduct an analysis.

Obtaining both a system and the associated software is usually a good forensic method. The examiner can access the examinee's phone logs, texts, and emails using the logical image. The detective can use the actual photograph in an effort to reconstruct the deleted data. The discipline of mobile phone forensics is rapidly growing, and chip-level analysis is a relatively new but rising competence. However, it may be difficult to remove the chip from a mobile phone and retrieve data from a forensic digital device.

3.2 Smishing

- Scammers send fake text messages purportedly from well-known businesses in an attempt to trick their targets into divulging personal information. Since the fraud relies on phishing emails that "fish" for a response, it exposes you to a number of threats. You're more inclined to believe the scam since the frightening message was sent to your phone via short message service (SMS). Scammers' attacks can have far-reaching consequences, from compromising your personal information to allowing them to steal money from your bank accounts. While SMS text messages are the most typical vector for smishing attacks, these scams may appear on any messaging service [16]. This would be the first sign of violence to a victim. When a user visits a fraudulent website and is requested to log in, the fraudster behind the site will steal their credentials. The second form of attack is an effort to trick a user into downloading or running malicious software while they are using a web browser [16, 17]. You can avoid being caught off guard if you know what safety measures to take and what red flags to keep an eye out for. Certain factors, such as:
- Don't reply: To identify the current cellphone number, even instructions on how to respond, such as texting "STOP" to terminate a subscription, might be utilised. Attackers prey on your interest in the issue or your dread of it, yet you could be hesitant to cooperate.
- If the message is urgent, pay close attention to it: Red flags for smuggling include time-sensitive account upgrades and limited incentives. Be cautious and sceptical as you go on.
- If you have any concerns, speak with your bank or retailer immediately soon.
- Reputable institutions do not send text messages asking for login information or account updates. Any urgent alerts can also be confirmed by calling an authorised phone support or accessing your online accounts.
- Double-check the phone number. Email-to-text service providers are recognised by their unusual four-digit numbers. This is only one of several methods a scam artist may employ to conceal their actual phone number.
- Avoid texting credit card numbers if at all feasible.
- Never storing financial information in a digital wallet in the first place is the greatest approach to guard against it being stolen. The use of two-factor authentication is highly recommended (MFA). A stolen password may still be ineffective to a smishing attacker if the compromised account requires a second "key" for verification. The most popular MFA solution is two-factor authentication (2FA), which frequently uses a text message verification code. A better substitute is to use a different verification app (such as Google Authenticator).
- Never text someone your password or account recovery code. Passwords and recovery codes for two-factor authentication (2FA) supplied by text message both run the risk of making your account vulnerable to unauthorised usage. Never share this information with anyone; it should only be used on official websites.
- Anti-malware software needs to be set up.
- Using tools like Kaspersky Internet Security for Android, you can guard yourself from phishing URLs and dangerous SMS programmes.
- Report any attempted SMS phishing to the appropriate authorities.

3.3 Public WiFi Problems

- Public Wi-Fi is widely available nowadays, and in some cities it extends across the entire municipality. Hackers might potentially use security flaws in the Wi-Fi network to steal messages, login credentials, and other sensitive information if users' mobile devices were linked to it. Some con artists go to great lengths to take advantage of loopholes, creating false connections with aliases to deceive naive customers into plugging in their gear. These types of networks are sometimes referred to as "evil-twin" networks. A survey conducted by Kaspersky Security Network found that 25% of all public Wi-Fi connections globally do not employ any encryption at all [17]. At any one time, the vast majority of a coffee shop's tables will be occupied by people typing away on laptops. Many professionals, students, and startup founders use these spaces as their secondary workplaces. The vast majority of people who connect to public Wi-Fi networks do so because they need to obtain information that may be lethal in the wrong hands. The millions of individuals who use public Wi-Fi, however, are probably oblivious to the risks they face. If you want to stay safe when utilising public Wi-Fi, you need to know what you're getting into beforehand [17, 18]. There are seven main groups that these dangers fall into:

- Theft of personally identifiable information is a major and growing concern. Access credentials, personal information, and photographs are the most sensitive types of personal data.
- Businesses are vulnerable to cyberattacks because their employees use public Wi-Fi to access company accounts, download files, browse client records, and do a variety of other network-dependent operations. Even though most businesses have security protocols in place to minimise the risk of connecting through Wi-Fi, there are still worries if one of your workers has to use a security tool to access the internal network.
- Man-in-the-middle attacks: These occur when an attacker poses as the owner of a public Wi-Fi network in an effort to trick you into joining to their fake network. Let's pretend for a moment that you've booked a room at "Wonder's" hotel. Since the hotel provides free Wi-Fi, the guest fires up their laptop, activates Wi-Fi, and looks for the network named "Wondars." The misspelling is easy to notice if you aren't paying great attention. A individual in a room down the hall has set up their own hotspot network under the guise of the "Wondars" network in order to entice naive visitors.
- Data sent and received through an encrypted connection is protected by a secret key. The information would look like gibberish to anyone who intercepted it if they didn't have the key. However, not all online services provide secure connections. The presence of the HTTP prefix before the domain name is informative. HTTPS indicates an encrypted connection to the website. The web address is not encrypted if it consists of just "HTTP."
- Anyone on the same Wi-Fi network as you can eavesdrop on your communications by employing a packet analyzer, also known as a packet sniffer.
- If your Wi-Fi isn't secured, these programmes will show you everything being sent and received. Obviously, not every single one of these devices is risky. Much like any other instrument, they may be used to either positive or negative usage.
- Spyware can help network administrators detect and troubleshoot Wi-Fi connectivity and transmission difficulties (good). However, this opens the door for hackers to obtain sensitive information from other users (bad).
- Using public Wi-Fi also exposes you to the risk of malware infection. Malware comes in numerous forms, some of which are: Threats include, but are not limited to, viruses, worms, Trojan horses, ransomware, and adware. Inadequately protecting your PC might leave you vulnerable to malware attacks when using public Wi-Fi. When you connect to an unsecure Wi-Fi hotspot, your computer is at risk of being infected with malware that takes advantage of one of these flaws.
- Security issues with public Wi-Fi networks also include: • Account Hijacking. In this scenario, an adversary obtains knowledge of the services and websites to which your system connects. If the attacker learns enough about your system, he might potentially impersonate it and seize control of the connection.

3.4 Malicious Apps:

Taking over a user's account is another security risk associated with public Wi-Fi networks. In this scenario, an adversary obtains knowledge of the services and websites to which your system connects. If the attacker learns enough about your system, he might potentially impersonate it and seize control of the connection.

4. Mobile forensics challenges

Although they can be used for that purpose, non-forensic methods were not created to expose data from mobile devices. Forensic tools are software programmes created for the express purpose of retrieving information from mobile devices. There are two ways to address this issue [5, 18]: either decrease the period between a phone's release and the release of Mobile Device forensic software for that phone, or establish a baseline against which the effectiveness of a tool may be measured.

The potential for information to be available, maintained, and synchronised across numerous devices is one of the most critical forensic challenges pertaining to the mobile platform. Data is more difficult to keep safe since it is volatile and may be altered or deleted remotely with little to no effort. Compared to computer forensics, mobile forensics adds new complications for investigators [19]. Digital evidence from mobile devices is notoriously difficult to obtain for forensic and law enforcement investigators. Some of the reasons why are as follows:

There are a wide variety of mobile phone models available on the market today, each with its own unique set of features and hardware specifications. There is a wide variety of mobile phones that forensic

investigators may meet. These phones might vary in screen size, processing power, storage capacity, and other hardware and software specifications. The rapid pace of product development also means that new versions are released often. Examiners need to be flexible enough to overcome new challenges and up-to-date enough on mobile device forensics to do their jobs effectively as the mobile environment evolves.
According to Network Careers Differ, the first step in any mobile phone inquiry is to identify the phone in question. Because there are so many different network providers, not even the most seasoned detectives can identify who owns a phone simply by looking at it. Some hardware manufacturers market only a subset of its features to carriers.
According to Network Careers Differ, the first step with every mobile phone enquiry is to identify the phone. Because there are so many different carriers, not even the most seasoned detectives can tell a phone apart just by looking at it. It's conceivable for many service providers to offer identical functionality using hardware from the same manufacturer.
In order to keep any relevant information from being overwritten or lost during a smartphone investigation, it is essential to disable the device's ability to receive any new data or voice transmissions. As SMS messages are stored utilising the "First In, First Out" principle, newer messages may overwrite older ones. If your device isn't safeguarded, you risk losing all of your data and the call records will be wiped if you receive an incoming call. Thus, after the first purchase, these handsets need to be stored in a wireless storage container. There are a few different ways to do this, and their success rates vary.

- There is a lack of funds: As the number of mobile devices proliferates, the demand for forensic analysis tools is expected to increase. Forensic acquisition equipment, such as power cables, chargers, and adapters for various cell devices, must be maintained in order to acquire such devices.
- Data masking, obfuscation, falsification, and secure deletion are only some of the anti-forensic tactics that make it more difficult to investigate digital material.
- Energy and Auxiliary Ports: Keeping their phones charged is another issue that detectives have to deal with. Disconnecting a phone for an extended period of time may drain the battery. Many mobile devices use ramdisk to store data, therefore a complete blackout might result in the loss of data and, by extension, critical evidence. Therefore, it is recommended to always have a fully charged phone. There isn't currently a consensus on how much juice mobile phones should have.
- Inconsistency of the evidence: It is easy to alter digital evidence, either intentionally or unintentionally. It's possible, for instance, that the information included in a mobile app might be altered if its user browsed it.
- Moving programme data, renaming files, changing the device's operating system, and switching the manufacturer's OS are all viable options when it comes to updating a mobile device's software. It's crucial in this case to take into account the suspect's level of education and experience.
- Resources are easily accessible, and there are several mobile device configurations from which to choose. There is a need for a variety of tools rather than just one since it is unlikely that a single tool would be able to handle all devices or complete all relevant activities. It might be difficult to choose which accessory is best for a certain mobile device.
- Because of Legal Repercussions: Transnational crimes can be committed with the use of mobile devices used by criminals. The forensic examiner's knowledge of both the nature of the crime and local legislation is necessary for resolving these important issues for law enforcement.

CONCLUSION

Wireless technology is increasingly relied upon. The need for testing standards for smart phones and other smart devices is rising in tandem with the number of such devices that need to be evaluated. Each time we use one of these convenient tools, we record a small chunk of our day. This data is invaluable to businesses and law enforcement organisations in reconstructing our movements and activities over time. Your smartphone may record your location in addition to your phone logs, contacts, text messages, songs, pre-written messages, videos, photos, and Google Calendar entries. Researchers need to treat and interpret this data with extreme caution.
This issue is exacerbated by the fact that the network is operational and has a wide variety of different parts. Power outages may be problematic since they might restart the activation of security protocols. The remote erasure of data is another area of worry. Investigators face training and time constraints as they try to piece together what happened on a smartphone or other networked device. Unfortunately, there is not yet a standardised method for gathering data from these devices that may be relevant to scientists.This complexity is due to a number of interrelated factors, such as the sheer number of networks and devices, the difficulty of maintaining a charged phone while simultaneously blocking incoming messages, the wide variety of operating systems and communication protocols in use, the providers of relevant data storage, and the hundreds of electrical and data connectors in use. Although

the particulars of the inspection will differ from device to device, the examiner can assure that all data acquired from each smartphone is accurately documented and that the results are repeatable and defendable in court [18, 19]. This article's goal is to help scientists and multimedia researchers develop approaches that are unique to their areas of study and research strategies [20].
Potential Future Applications: Mobile forensics techniques will eventually be used to look at the various file systems available in cell phones. This might completely alter the way that crimes are investigated and evidence is gathered.

ACKNOWLEDGEMENTS

Authors would like to express their gratitude towards the management of Shree Guru Gobind Singh Tricentenary University, for providing ample support throughout the study.

REFERENCES

1. E. Casey, (ed.) (2010). Handbook of Digital Forensics and Investigation, Academic Press.
2. Larson S. (2014). The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Journal of Digital Forensics, Security and Law. doi:10.15394/jdfsl.2014.1165
3. J. Bates, (1998). Fundamentals of computer forensics, Information Security Technical Report, Elsevier.
4. Kessler G. (2012). Advancing the Science of Digital Forensics. Computer (Long Beach Calif). 45(12):25-27. doi:10.1109/mc.2012.399
5. S. Conder and L. Darcey. (2009). Android Wireless Application Development, Addison Wesley.
6. N. Al Mutawa, I. Baggili, A. Marrington,(2012). ”Forensic analysis of social networking applications on mobile devices”, Digital Investigation, Volume 9, Pages S24-S33.
7. Kumar M. (2021). Mobile Phone Forensics. *International Journal of Electronic Security and Digital Forensics*. ;13(1):1. doi:10.1504/ijesdf.2021.10029656
8. Singh P, Bhargava B, Paprzycki M, Kaushal N, Hong W. (2012). *Handbook Of Wireless Sensor Networks: Issues And Challenges In Current Scenario's*.
9. Kallil M. (2020). The Potential Problems of Admissibility and Relevancy of Digital Forensics Evidence in Syariah Courts. *International Journal of Psychosocial Rehabilitation*. 2020;24(5):1027-1032. doi: 10.37200/ ijpr/v24i5/pr201776
10. Ayers, R., Jansen, W., Cilleros, N., Daniellou, R. (2006). An Overview of Cell Phone Forensic Tools. Retrieved on Sept. 10, 2007 from http://www.techsec.com/TF-2006- PDF/TF-2006-RickAyers-MobileForensics-TechnoForensics.pdf
11. J. Park, H. Chung, S. Lee,(2012). Forensic analysis techniques for fragmented flash memory pages in Smartphone”, Digital Investigation, Volume 9, Issue 2, Pages 109-118.
12. Ayers, R. P. Jansen, W. A. (2006). Forensic Software Tools for Cell Phone Subscriber Identity Modules. Association of Digital Forensics, Security and Law , April 20-21.
13. Forensic analysis of mobile phone internal memory Svein Y. (21012). Willassen Norwegian University of Science and Technology .pp90.
14. Chetry A, Sarkar M. (2020). Mobile Forensics and Its Challenges. Digital Forensics (4n6) Journal. doi:10.46293/4n6/2020.02.03.07
15. Hylton, H. (2007). What Your Cell Phone Knows About You. Time. Retrieved on September 1, 2007 from http://www.time.com/time/health/article/0,8599,1653267,0 0.html
16. Scientific Working Group on Digital Evidence. (2007). Special Considerations When Dealing With Cellular Telephones. Retrieved September 12, 2007 from http://68.156.151.124/documents/swgde2007/SpecialConsiderationsWhenDealingwithCellularTelephones-040507.pdf
17. Zareen, & S. Baig,. (2010). Mobile Phone Forensics Challenges, Analysis and Tools Classification”. Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE.2010), pp. 47 – 55.
18. S. Raghav, & A. K. Saxena,(2009).” Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition”. IEEE student Conference on Research and Development, pp. 5-8, 2009.
19. B. Sharma, M. Hachem,V.P. Mishra, M.J. Kaur. (2020). Internet of Things in Forensics Investigation in Comparison to Digital Forensics. In: Singh P., Bhargava B., Paprzycki M., Kaushal N., Hong WC. (eds) Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's. Advances in Intelligent Systems and Computing, vol 1132. Springer, Cham
20. B. K. Sharma, M. A. Joseph, B. Jacob and B. Miranda, (2019). "Emerging trends in Digital Forensic and Cyber security- An Overview," 2019 Sixth HCT Information Technology Trends (ITT), Ras Al Khaimah, United Arab Emirates. pp. 309-313, doi: 10.1109/ITT48889.2019.9075101.

CITATION OF THIS ARTICLE

Bhoopesh Kumar Sharma, Rajiv Vatsa, Nishith Kumar Mishra, Yogesh Sharma, M. T Ahmad Beig : Future, Resources, and Obstacles of Mobile Phone Forensics. Bull. Env.Pharmacol. Life Sci., Spl Issue [4]: 2022: 62-69