Journal of Positive School Psychology http://journalppw.com
2022, Vol.6, No.4, 4463-4474

# Challenges, Tools, and Future of Mobile Phone Forensics

**Bhoopesh Kumar Sharma[1*],Vipin Yadav[2], Mandeep Kaur Purba[3*],Yogesh Sharma[4],Vikhyaat Kumar[5], Ishant[6], Pulkit Mehta[7]**

*[1]Professor, Department of Forensic Science, Shree Guru Gobind Singh Tricentenary University, Gurugram -122505 (India)*
*[2]Research Scholar, Department of Forensic Science, Shree Guru Gobind Singh Tricentenary University, Gurugram -122505 (India)*
*[3,4] Assistant Professor, Faculty of Science, Shree Guru Gobind Singh Tricentenary University, Gurugram -122505 (India)*
*[4,5,]M.Sc. Forensic Science, Department of Forensic Science, Shree Guru Gobind Singh Tricentenary University, Gurugram -122505 (India)*
*[6]M.Sc. Physics, Indian Institute of Technology (IIT), Hyderabad, Telangana – 502285 (India)*

**Abstract:**

Daily, hundreds of millions of people use their phones in their everyday lives, and many of them become victims of a variety of illicit activities.With the ongoing expansion of the smart phone market, the likelihood of their usage in illegal acts has also increased. Nowadays, mobile phones come with a diverse set of software applications, new technologies, and operating systems. Advances in mobile phone semiconductor technology, as well as an increase in computational power, have allowed mobile phones to become more efficient while remaining tiny enough to fit in a pocket. As a result, examining evidence via a mobile phone becomes difficult for a forensic investigator. The capture of information from mobile devices is routinely used as persuasive proof, and it's become an important part of forensic investigations.To obtain meaningful data, a thorough understanding of forensic tools and their characteristics is essential. The nature of some of the newest types of information that can become possible evidence on mobile phones is examined in this paper. It also covers several newer technologies and their effectiveness in collecting phone-based evidences.This study also assesses mobile device characteristics, mobile forensic investigation steps, and distinct mobile forensic technologies along with their limitations and future scope.

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

## 1. Introduction:

Daily, hundreds of millions of people use their phones in their everyday lives, and many of them become victims of a variety of illicit activities. With the ongoing expansion of the smart phone market, the likelihood of their usage in illegal acts has also increased [1]. Nowadays, mobile phones come with a diverse set of software applications, new technologies, and operating systems.Mobile phones have been a part of our daily lives since with the launch of "bag and brick" cell phones in mid-1990s [1, 2]. Advances in mobile phone semiconductor technology, as well as an increase in computational power, have allowed mobile phones to become more efficient while remaining tiny enough to fit in a pocket.With the launch of smart-phones and growing up to fifth generation networks, currently there are over 5.31 billion unique mobile phone users who access their mobile devices daily [3]. Also, along with the calling facility, an increase in the free social messaging applications like WhatsApp, Telegram, Instagram, Facebook etc., is one of the significant elementthat have contributed to the mobile phone's widespread use.Internet users are rising exponentially at the rate of 4.0 percent each year, equal to more than half a million new users per day [3, 4]. As the increase in the number of use of mobile applications,the related security threats have

also increased at an exponential rate. In the last few years, the amount of mobile transactions has increased fourfold, and cyber criminals are now targeting mobile users to steal data and money through online and internet fraud methods [4].

According to analysts, the culture of taking personal gadgets to work and accessing corporate data on mobile devices has increased the danger of security breaches.Fake apps on the Google Play Store are one of the most common ways for cyber thieves to attack online.There are instances of using several free mobile applications for forensic purposes as well for measuring the crime scene and other evidences digitally [5]. However, these freeware again may pose a great security impact when downloaded from open sources or un authentically.Users that are duped into installing these have their information stolen.According to McAfee, many of these fraudulent programmes are based on famous smartphone apps. For example, the game Fortnite has over 200 million players worldwide and has received over 60 million downloads, and a slew of fraudulent apps posing as alternative versions of Fortnite have sprung up [6].Cybercriminals are also continuing to develop new distribution channels, ranging from phishing SMS messages to applications with real-world functionality that allow malicious payloads to avoid app store security checks.As banking becomes more integrated into mobile device usage, attackers have begun to incorporate more complex features into their mobile banking malware. They take more than just credit card data and get around security procedures by staying under the radar.Information can be found in abundance on mobile phones. The most apparent sorts of data which may be accessed from a cell phone are phone records, call logs, and SMS [6, 7].

Cyber security firms have even begun collaborating with mobile device manufacturers in order to protect consumers' security. McAfee, for example, has strengthened its ties with Samsung and Türk Telekom [7]. The collaboration with Samsung will help protect users from cybersecurity, which come pre-installed with McAfee VirusScan anti-malware protection.In its Internet Security Threat Report, another cyber security firm, Symantec, notes that cell phones may be the biggest espionage instrument ever devised. According to the business, a smartphone with a camera, a listening device, and a GPS tracker collects more data from the user's location.The data received from the Mobile Device by the forensic tool is evaluated to the baseline to assess the efficacy of the cell Phone forensic tool. Subscriber Identity Module, sometimes known as a SIM card, is the most widely used identity module today [8].

It's utilised to maintain personal data distinct from the real phone or tablet, as well as to save contact information, names, and communications networks, and to enable phone ubiquity. One of the major practical issues confronting digital investigators is that it is often difficult to determine which evidence source will be relevant to an investigation at the outset of an investigation. Even though the evidence is found, determining which source of evidence is important to an inquiry is typically challenging.

## 2. Digital Forensics Vs Mobile Phone Forensics

Digital forensics refers to procedures that can be used to identify and detect evidence from digitally committed crimes [9]. This information is gathered in order to present it in a court of law. In layman's terms, Digital Forensics is called into action whenever a digital crime or a crime involving computers occurs. Furthermore, digital forensic is divided into several categories as discussed in figure 1.

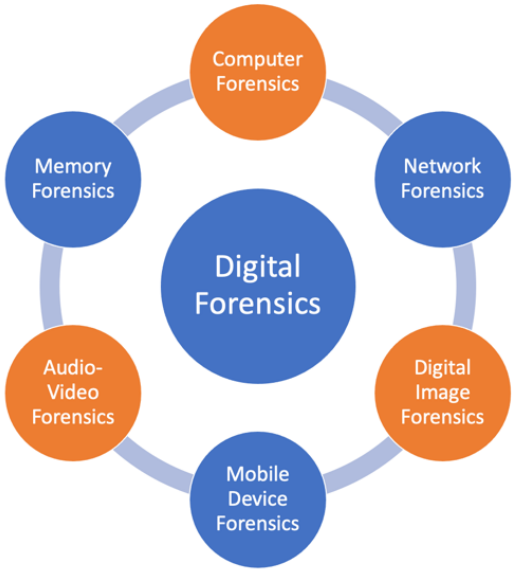


Fig 1: Components of Digital Forensics

Mobile Device forensics is becoming increasingly relevant as the usage of mobile devices becomes more popular, because mobile systems are commonly identified at scene of the crime, this is a good idea. " "The art and science of obtaining digital evidence from a smart phone utilising established procedures in forensically" is considered as Mobile Phone Forensics, says the National Institute of Standards and Technology [9, 10]. This is a difficult condition to meet because mobile phone model release cycles are short, and operating systems and hardware come in a wide range of variations and kinds. Similarly, in a company internal audit investigation, to a criminal investigation case that is widely observed in law enforcement, forensics is employed in a variety of contexts. Many crimes and other wrongdoings make forensics vital to making the world a better place.As part of digital forensics, mobile device forensics tries to retrieve or acquire data and evidence from smart phones and other comparable devices used in daily life as shown in figure 2.

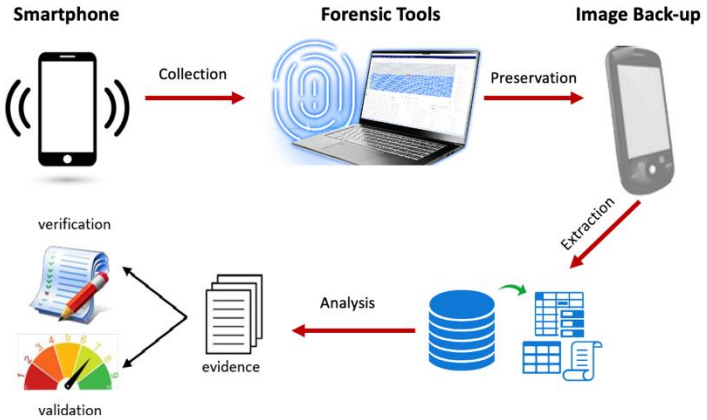


Fig 2: Process of digital evidence analysis

Investigators can use Mobile Device Forensics to answer questions about a given issue connected to Mobile Device-based communication [11].The key contrast between digital forensics and smart phone forensics is that mobile device forensics requires dealing with a variety of different hardware and software standards, making the creation of a universal standard instrument nearly impossible [12].Figure 3, discusses about the various steps followed during the digital forensic life cycle. Because embedded

software in mobile devices is more specialised than PCs, data retrieval methods are non-standardized, necessitating a large number of alternatives. With new generation phones hitting the market at an increasing rate, and also new firms entering the market with their own proprietary software, tackling the issue where a mobile device is implicated in crime has become even more challenging. The goal of a smart phone forensic tool is to retrieve device information without causing it any harm. Important updates should be provided via the tool in a timely manner to keep up with the fast changes in Mobile Phone operating systems [12, 13]. There are forensic and non-forensic tools, each with its own set of difficulties and solutions. Ring tones, programmed replies, streaming video, still pictures files, email alerts, miscellaneous documents and file systems, and geolocation are all capabilities of a contemporary phone that might be relevant in a forensic investigation.

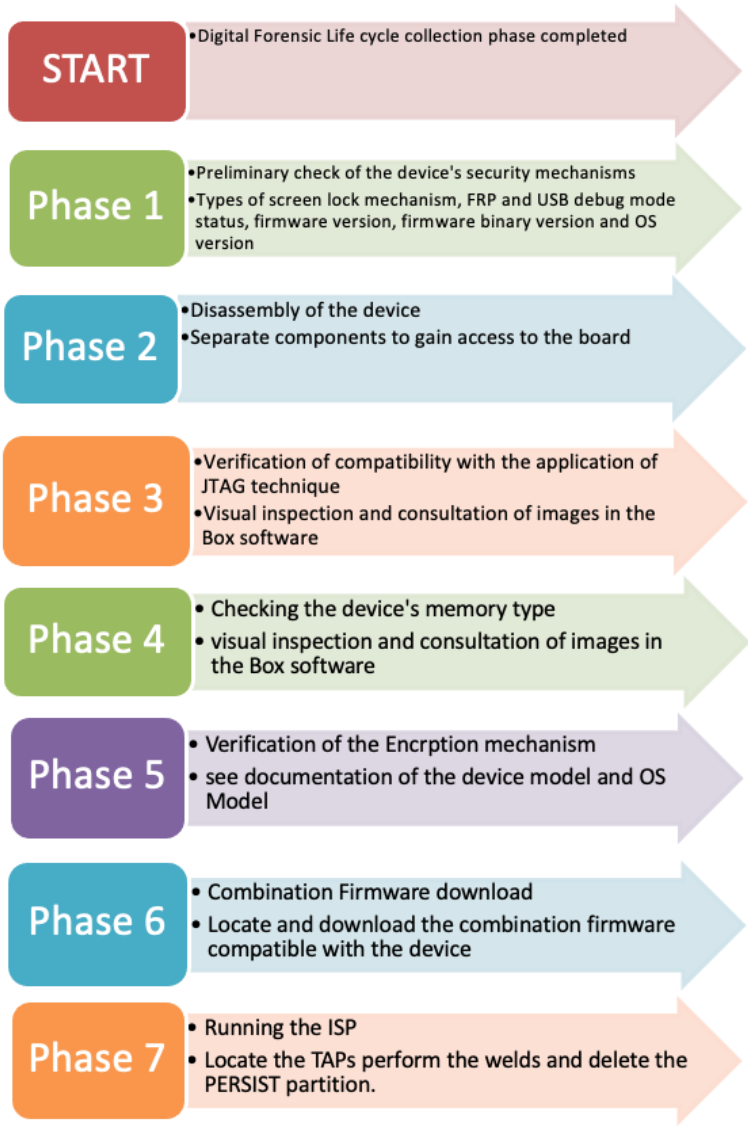


Figure 3: Steps and phases during a typical Digital Forensic Investigation

Computer forensics and smart phone forensics both attempt to correctly collect and analyse data from a device. While the purpose is the same, the challenges are dramatically different.

In computer forensics, the most common operating systems (OSs) are Windows, Mac OS, and Linux. In mobile forensics, operating systems are frequently upgraded, necessitating constant monitoring to keep updated. Because mobile devices are built to travel, they are always in contact with

the outside world [14]. As a result, effective evidence processing is critical to avoid data contamination. Cell phones, for example, may be remotely directed to erase all of the data stored on them. Mobile device investigators could lose everything if the phone is not properly isolated from wireless transmissions.Different levels of data extraction and their advantages and disadvantages have been discussed in Table 1.

Table 1: Different levels of data extraction and their advantages and disadvantages

| S.No. | LEVEL | ADVANTAGES | DISADVANTAGES |
|---|---|---|---|
| 1. | Manual Extraction | Doesn't require a specialized tool; minimal technical complexity | Time-consuming for large volumes of data; risk of inadvertent data modification; doesn't recover deleted data; likely infeasible with damaged devices |
| 2. | Logical Extraction | High level of data abstraction; low technical complexity | Risk of inadvertent data modification; limited access to data (remnants) |
| 3. | Hex dumping/Joint Test Action Group (JTAG) | Achievable though standard connectivity interfaces; handles devices with minor damage; allow access to data remnants | Data parsing and decoding can be difficult; no guaranteed access to all memory sections; invasive device access (JTAG); requires extensive training |
| 4. | Chip-off | Provides a complete binary image suitable for more traditional analysis | Risk of causing physical damage; requires extensive training |
| 5. | Micro read | Viable last-resort option | Very resource intensive and technically challenging |

Solid-state non-volatile memory is utilised in cell phones as it consumes less energy, is lighter than a hard disc with the same data storage, and is less sensitive to breakage from shaking (Regan, 2009).There are no platters or moving components in solid-state drives. While the main procedure and methodology for analysing a hard disc drive also apply to solid state drives, there are a few differences that might aid or hinder an investigator [15]. Magnetic charges are not written to a device by solid-state SSDs. They instead store one electron's energy in a series of gates that represent ones and zeros.Because the drive's writing capabilities is limited by the gate mechanism, the Flash Transition Layer selects where data is recorded to and regulates the use of gates.This feature favours the investigator since data can remain much longer because the drive can resist writing back to the deleted material to extend the gate's life. Furthermore, when the device is switched off, the volatile memory's live contents may be copied to the non-volatile memory for storage.Solid-state, on the other hand, may provide a dilemma for investigators since properly deleted data cannot be recovered[3, 15].

### 3. Cyber Threats Associated With Smart Phones

The number of persons who conduct cybercrime or crimes employing digital technology is increasing as the number of electronic gadgets increases. These innovations, whether it's an iPhone or a flip phone, have had and will continue to have a significant influence on society [5, 15].

While most people have become accustomed to having practically whatever they desire at

their fingertips, fraudsters are hard at work establishing their fraud operations. Smishing, phoney networks, rogue programs, and grayware are just a handful of the sneaky cyberthreats that have evolved over time to trick vulnerable users - some of which consumers may not even be aware of.

***3.1. Cell Phone Acquisitions:***

Smartphones are essentially portable computers that hold a wealth of data. Some acquisitions will yield more than others due to variances in cell phone designs.Mobile devices may be able to collect the following data types:Contact information, Call logs,Images and videos, as well as sms messages,Voice (voicemail, songs, and so on), Geolocation position, and so on. Mail, Memorandums (notes), Planner, Files, Browser History, and Apps (social media, user behaviour, etc.). Due to the difficulties of keeping up with the steady flood of new phones and the advancement of technologies that comes with them, there is no one-size-fits-all strategy for obtaining mobile phone data [16].There are four primary types of cell phone purchases:

- Screen captures: The contents of the phone's screen are photographed using a camera.Cell phone data is often the only way to keep it private.
- Logical analysis is the process of extracting the data on your mobile phone that you can see and access.This is the most used method nowadays.
- Physical analysis: Information is retrieved from the device's primary storage and external memory via this mechanism.
- Chip level analysis: The procedure of removing the phone's storage chips and probing them for data in order to analyse them.

Attempting to obtain both a system and software acquisition is a reasonable forensic technique in most circumstances. Using the logical image, the examiner may access phone records, text messages, and email.

The investigator can utilise the physical picture to try to recover data that has been destroyed.Chip level analysis is a relatively new discipline that is gaining traction in the cell phone forensics world. Techniques for removing cell phone chips and recovering data from a forensic digital device, on the other hand, are incredibly difficult to master.

***3.2 Smishing***

Smishing is a deceitful tactic that involves sending text messages that look to come from reputable firms in order to trick users into divulging personal information such as passwords or credit card details. The fraud is based on phishing emails that "fish" for a response, leaving you open to numerous hazards. However, the threatening message is delivered to your phone via SMS, making you more likely to fall for the hoax.Smishing attacks can have serious and varied consequences, such as someone acquiring access to your financial accounts or taking control of your social media accounts. Smishing attacks are usually accomplished via SMS text message, but they can also appear on any messaging network, including WhatsApp and Instagram [16].

The first type of attack one will encounter is a link to a dubious website, which might be a spoof of a well-known corporation website or social networking network. The victim will be asked to enter username and password, but instead of checking in to the legitimate site, the person who put up the false site will capture your information and use it for evil purposes.The second type of attack will try to persuade to download or execute a malicious software through the web browser [16, 17].However, if you are aware of the warning signals to look for and the precautions to take, you can avoid being caught off guard.There are certain parameters, which can be taken care of for avoiding such attacks viz:

- Do not respond:Even response suggestions, such texting "STOP" to unsubscribe, may be used to locate current mobile number. Attackers prey on your interest or dread of the scenario, but you may refuse to deal.
- Take it carefully if a message is urgent:Smishing red flags include urgent account upgrades and restricted offers. Continue with caution and scepticism.

- Ask your bank or merchant right away if you have any worries.
- Account modifications or login details are not requested via text texts by reputable institutions. Any urgent alerts can also be verified via your online accounts or by calling an authorised phone support.
- In your message, don't include any links or contact information.When giving links or contact information in emails that make you feel anxious, be cautious. If at all feasible, use formal communication methods.
- Please double-check the phone number.Strange numbers, like 4-digit ones, are used to identify email-to-text providers. This is only one of the numerous methods a con artist might conceal their true phone number.

- If at all possible, avoid texting credit card numbers.The best way to prevent financial information from being stolen from a digital wallet is to never store it there in the first place.
- It's a good idea to utilise two-factor authentication (MFA). A disclosed password may still be worthless 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 typically uses a text message verification code.Using a separate verification app is a better alternative (such as Google Authenticator).
- It's never a good idea to text a password or account recovery code.Both passwords and text message two-factor authentication (2FA) recovery codes might put your account in jeopardy if they fall into the wrong hands. This information should only be used on official websites and should never be shared with anybody.
- Anti-malware software should be installed.Products like Kaspersky Internet Security for Android can protect you against malicious applications as well as SMS phishing links.
- All attempted SMS phishing should be reported to the proper authorities.

### *3.3 Public Wi-Fi Woes*

Nowadays, public, and free Wi-Fi is available practically everywhere, and some towns even provide city-wide Wi-Fi. However, the Wi-Fi network to which users connect their mobile device may not be the safest, since hackers may use network flaws to steal messages, login passwords, and other personal data. In addition to exploiting flaws, some con artists go so far as to construct phoney connections with pseudonyms in order to trick unwary consumers into joining their devices. These types of networks are referred to as "evil-twin" networks.As per a survey conducted by the Kaspersky Security Network, about a 25% of all public Wi - fi connectivity across the world utilize no encryption at all [17]. Anytime, most of the tables in any coffee shop will have patrons tapping away on laptops. Many entrepreneurs, students, and businesspeople use these places as a second office.Most individuals who use public Wi - fi networks have a lot of important and possibly privileged data on their gadgets, some of which may be disastrous if a hacker had access to it. However, the millions of individuals who use public Wi-Fi are probably ignorant of the risks they are putting themselves in. If one wants to be secure while using public Wi-Fi, he must first understand the hazards [17, 18]. These hazards are mainly divided into seven main categories:

- Personal data Theft: One of the most serious and prevalent hazards is the theft of personal information. Personal information can come in a variety of formats: The most susceptible are login passwords, financial information, personal data, and photographs.
- Businesses are vulnerable to cyber attacks because they use public Wi - fi networks to check their accounts, receive files, examine client data, and do a variety of other network-dependent functions. Even while most organizations have security procedures in place to limit the risk of connecting through Wi-Fi, there are still concerns about using a public connection if one

of your workers must use a security tool to get access to the internal network.

- Man-in-the-Middle Attacks: A man-in-the-middle attack occurs if someone pretends to be a legal public Wi-Fi network provider in order to trick you into joining. Let's pretend you're spending the night in a “Wonder’s” hotel. The hotel provides free Wi-Finetwork to its guests, so the guest turns on his/her laptop, switch on Wi-Fi, and look for the network "Wondars." You can overlook the small misspelling if you aren't paying close enough attention. In actuality, the “Wondars” network is a person in a room down the hall who has built up their own hotspot network to entice unsuspecting visitors.
- Connections that are not encrypted: The data you send and receive is encrypted using a secure key while you connect to a website that uses encryption. Without the key, someone intercepting the data would be unable to understand it since it would appear to be unintelligible computer code. Not all websites, however, provide encryption. This is indicated by the HTTP prefix, which appears before the domain name. The site is encrypted if the URL starts with HTTPS. It is not encrypted if the web address only contains HTTP.

- Spyware / Eavesdropping: Anyone connected to the same Wi-Fi network as you can use a packet analyzer, often known as a packet sniffer, to watch what you send and receive.
- If your Wi-Fi network isn't encrypted, these tools allow you to see anything that is transferred over it. These devices aren't always hazardous. Like any other tool, you may use them for good or for bad.
- Network managers can employ spyware to diagnose connection difficulties and other technical problems with their Wi-Fi communication (good). On the other side, they allow hackers to get access to other users' information and steal anything valuable (bad).
- Malware Distribution: Another risk of using public Wi-Fi is that your device will become infected with malware.Malware comes in a wide range of forms and sizes, including: To mention a few, viruses, worms, Trojan horses, ransomware, and adware. If you're on a public Wi-Fi network with someone with nefarious intent, they could be able to install malware on your computer if it's not well-protected. By exploiting the hotspot, itself, an unscrupulous Wi-Fi provider may infect your PC with one or more of these vulnerabilities.
- Account Hijacking: Another problem with public Wi-Fi network security is the hijacking of accounts. An attacker hijacks data about your system's connection to websites or other services in this situation. Once the attacker gets that information, he may impersonate your machine and seize control of the connection.

***3.4 Malicious Apps:***

For both Android and iPhone users, fake apps have become a serious problem.This is mostly due to fraudulent programmes that hide in plain sight on well-known sites like Google Play and Apple's App Store. Cybercriminals install malware on consumers' mobile devices in the background after they download malicious software, making it hard for them to notice anything is amiss. While people believe they've merely installed a new software, spyware is busily gathering personal data.

**4. Challenges in Mobile Forensics**

Non-forensic tools aren't meant to expose information from mobile devices, although they can be used to do so. Forensic tools are tools created particularly to extract data from mobile devices. To address this scenario, two different techniques have been used: either reducing the time between the release of the phone and the availability of Mobile Device forensic software for that phone, or creating a baseline to determine the usefulness of a tool on a certain device [5, 18].

The fact that information may be accessible, saved, and synced throughout several devices is one of the most important forensic challenges with regard to the mobile platform. Because the data is volatile and may be readily manipulated or withdrawn from afar, it necessitates extra work to keep it secure. Mobile forensics differs from computer forensics in that it offers forensic examiners with new obstacles [19].Digital evidence from mobile devices is typically difficult to gather for law enforcement and forensic investigators.Some of the causes are as follows:

- Hardware Disparities: There are a plethora of mobile phone models available on the market from a variety of manufacturers. Depending on the size, hardware, features, and operating system of the phone, forensic examiners may face a variety of mobile phones. Furthermore, due to the short product development cycle, new models arrive often.Examiners must be able to adapt to new challenges and keep current on mobile device forensic techniques as the mobile environment grows.

- Network Careers Differ: The first step in any mobile phone enquiry is to identify the phone.Due to the different network providers, even skilled detectives find it impossible to identify a phone by look alone.A subset of features from a specific hardware vendor might be offered under many carrier names.

- Mobile Platform Security: Security systems are in place on modern mobile platforms to protect user data and privacy.During forensic collection and examination, these features function as a stumbling block. Modern mobile devices, for example, include built-in encryption methods from the hardware to the software layers. To retrieve data from the devices, the examiner may need to break through various encryption techniques.

- Data Preservation: It's critical to restrict the device from receiving any more data or voice communication during a smartphone investigation.Because sms messages are kept in a "First In, First Out" fashion, fresh messages may overwrite previous ones. Incoming calls can also wipe all call history logs, and if a device isn't safeguarded from incoming communications, it can be remotely erased of all data. As a result, these phones will need to be stored in a wireless storage container when they are first acquired. This may be done in a number of ways, each with various degrees of success. Three layers of conventional aluminium foil, a nickel, silver, and copper tri-weave mesh material shield, and an anodized aluminium shielded enclosure designed to protect wireless devices from radio waves are among the instruments available.

- Inadequate Resources: As previously stated, as the number of mobile devices increases, so will the number of forensic examiner tools required.Forensic acquisition gear including as Power cords, chargers, and adapters for various cell devices must be maintained on hand in order to acquire such devices.

- Data concealment, obfuscation, falsification, and secure deletion are anti-forensic tactics that make digital media investigations more difficult.

- Power and Connectors: Keeping the phone charged up is another challenge that investigators face. A phone's battery will eventually die if it is kept unplugged for an extended length of time. Because many cell devices store data in ramdisk, a complete loss of power might result in the loss of data and, as a result, vital evidence. As a result, it is preferable to maintain a phone charged. Regrettably, there is currently no standard for mobile phone power requirements.

- Data Formats: Like the other components that make up a

contemporary mobile phone, most of the information sought by an investigator does not have a standard format or location.Data files can be kept in a number of places. As previously indicated, certain SIM card can be used to store data in the phone's memory.RAM can be classified as either volatile (needs an electrical charge to maintain information) or non-volatile (does not require an electrical charge to maintain information). in mobile phone hardware (retains information without an electrical charge). All of these forms of memory may include information, which investigators and forensic software developers must be aware of.

- Inconsistency of Evidences: Digital evidence may be readily manipulated with, whether intentionally or unwittingly. Browsing an app on a phone, for example, might cause that app's data to be altered.

- Changing the Operating System of a Mobile Device: Moving programme data, renaming files, and changing the device's operating system, as well as changing the manufacturer's operating system, are all possibilities.The suspect's expertise and experience should be taken into account in this case.

- Availability of Tools: There are a plethora of smart phones to choose from. A variety of tools must be used since a single tool may not be able to support all devices or perform all of the essential activities. It might be tough to select the appropriate tool for a certain phone.

- Legal Issues: Mobile devices can be used by criminals to conduct crimes that cross national borders. The forensic examiner must be knowledgeable with both the seriousness of the offence and local legislation in order to deal with these appropriate law enforcement concerns.

**Conclusion:**

Our lives are becoming increasingly reliant on wireless technology. A need for method guidelines for the evaluation of smart phones and other smart devices has evolved as a result of the rising demand for testing of these devices. These devices record a bit of our day every time we use them for convenience.Companies and law enforcement are increasingly using this data to establish a timeline of our locations and behaviours that would otherwise be lost.Smart phones store call records, contact information, sms, music, prepared replies, streaming video, still picture files, google calendar, records and data files, and location data. Investigators must be cautious in their use of this data and in their interpretation of it. If you don't, what you believed would lead to digital paradise may instead lead to digital prison.

The mix of diverse devices and systems, as well as the fact that it is connected to a live network, causes additional problems. One issue is power outages, which might result in security protocols reactivating. Another problem is the remote destruction of critical information. When attempting to probe a smart telephone or gadget on a network system, investigators have hurdles with both training and time constraints [18]. On the other hand, investigators do not have a standardised process for obtaining evidence from these devices to help in investigations.The sheer quantity of networks and device manufacturers;the challenge of keeping a phone powered while preventing it from receiving incoming messages; the hundreds of electrical and data connectors currently in use; the many operating systems and communication protocols currently in use; by vendors for storing relevant information.While the specifics of each device's inspection may differ, the examiner may guarantee that data collected from each smart phone is adequately recorded and by applying same examination procedures, the outcomes are reproducible and defensible in court [18, 19].

The purpose of this article is to assist scientific investigators and multimedia investigators in designing techniques that are adapted to their individual demands [20].

Future Scope: Future applications of mobile phone forensic techniques include analysing multiple file systems used in smart phones,

such as Android, Windows Mobile, and iOS, among others. This might be incredibly useful in detecting crimes and gathering evidence.

**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.) Handbook of Digital Forensics and Investigation, Academic Press, 2010.
2. Larson S. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Journal of Digital Forensics, Security and Law. 2014. doi:10.15394/jdfsl.2014.1165
3. J. Bates, Fundamentals of computer forensics, Information Security Technical Report, Elsevier, 1998.
4. Kessler G. Advancing the Science of Digital Forensics. Computer (Long Beach Calif). 2012;45(12):25-27. doi:10.1109/mc.2012.399
5. S. Conder and L. Darcey. Android Wireless Application Development, Addison Wesley, 2009.
6. N. Al Mutawa, I. Baggili, A. Marrington,"Forensic analysis of social networking applications on mobile devices", Digital Investigation, Volume 9, Pages S24-S33, August 2012.
7. Kumar M. Mobile Phone Forensics. *International Journal of Electronic Security and Digital Forensics*. 2021;13(1):1. doi:10.1504/ijesdf.2021.10029656
8. Singh P, Bhargava B, Paprzycki M, Kaushal N, Hong W. *Handbook Of Wireless Sensor Networks: Issues And Challenges In Current Scenario's*.
9. Kallil M. 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," Forensic analysis techniques for fragmented flash memory pages in Smartphone", Digital Investigation, Volume 9, Issue 2, Pages 109-118, November 2012.
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, 2006 , Las Vegas, NV.
13. Forensic analysis of mobile phone internal memory Svein Y. Willassen Norwegian University of Science and Technology
14. Chetry A, Sarkar M. Mobile Forensics And Its Challenges. Digital Forensics (4n6) Journal. 2020. 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,." Mobile Phone Forensics Challenges, Analysis and Tools Classification". Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE.2010), (pp. 47 – 55),2010.
18. S. Raghav, & A. K. Saxena," Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition". IEEE student Conference on Research and Development, (pp. 5-8), Malaysia, 2009.
19. B. Sharma, M. Hachem,V.P. Mishra, M.J. Kaur. 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, 2020, vol 1132. Springer, Cham

20. B. K. Sharma, M. A. Joseph, B. Jacob and B. Miranda, "Emerging trends in Digital Forensic and Cyber security-An Overview," 2019 Sixth HCT Information Technology Trends (ITT), Ras Al Khaimah, United Arab Emirates, 2019, pp. 309-313, doi: 10.1109/ITT48889.2019.9075101.