Mobile Technology: Mobile Incident Response and Investigations

[Name of the Student:]

[Name of the Institution:]

Mobile Technology: Mobile Incident Response and Investigations

# Mobile Technology Overview

Mobile technology is the technology that is used to carry out cellular communication. This implies that mobile technology is used for enabling efficient communication between mobile devices through a network. Mobile technology makes use of radio communication to connect with other devices over the network. The most commonly used method of radio communication is CDMA that stands for Code-Division Multiple Access. However, this method of mobile communication has evolved greatly over the past two decades.

Mobile devices are electronic devices that work as connecting points in a cellular network. The cellular network consists of cell sites that are specialized base stations for emitting and receiving the data signals (Ooi & Tan, 2016). These cell sites control the communication in a cellular network in the sense that they provide the basis for connections in transferring the data to the destined mobile devices as well as receiving data from those devices to float through the network. A cell phone offers the opportunity of transferring connection from one cell site to another. This is called full-duplex communication. It implies that the cell phone automatically switches between frequencies when the mobile phone user shifts from the range of a cell site to another cell site area. This allows the user to carry mobile phone from one place to another as the mobile phone adjusts and connects to the nearest cell site automatically that offers stronger signals.

Mobile devices have evolved considerably over time, and these devices are not meant only for voice communication in the modern world. Mobile devices have become capable of sending and receiving text messages, voice messages, multimedia messages, and other data. Mobile devices are used for calling video, as well as for having conferences online. These devices offer the facility of using email-enabled with full access to receiving and sending messages as well as the attached files. Further mobile devices can be utilized for sharing information of many types such as text files, audio or video files, images, podcasts, etc. There are many options for choosing among the available software and applications for sharing information through mobile devices (Heflin, Shewmaker, & Nguyen, 2017). Some mostly used sharing facilities in mobile devices include Bluetooth, Share-it, and similar other options. Moreover, mobile devices offer multimedia players, video players, audio players, radio, and mp3 players. These applications have reduced the use of other devices by consumers. People prefer to interact with multimedia through their mobile devices. Today, viewers of sports, TV programs, movies, animated films, documentaries, and others confine their usage to mobile devices only for this purpose.

Mobile devices have the packet switching capacity that enables them to connect to the Internet when required. When connected to the Internet, mobile devices can access all the world's information and let the user avail it. The mobile devices are now extensively been used by consumers for banking purposes. Mobile or Internet banking has enabled customers to make most of the needed transactions through mobile devices. Nowadays, consumers make use of mobile devices to send or receive money, pay utility bills, purchase goods, and services online, and many other purposes. There are many other features that enabled these days in mobile devices that have made the life of consumers very easy. Mobile devices are used for navigation purposes and show the user direction of routes to guide him/her in the right way. The user can browse through the websites for collecting necessary information as well as for making transactions. Many users spend plenty of time playing games on their mobile devices. Finally, mobile devices can store data and keep track of transactions, activities, and contacts that the user has made in previous days.

Mobile networks are also referred to as cellular networks. The cell sites, as discussed above, occupy certain areas of land where cell towers have been installed. The cell towers use various radio frequencies and connect to transfer packets of signals. The cell sites are usually hexagonal, and the cell towers connect to other cell towers as well as the telephone exchanges. The mobile devices connect through these cell towers. To conclude, it can be said that mobile networks constitute a complex network of different devices, towers, and exchanges to provide unrivaled communication experience to consumers of this modern age. In this era, mobile networks have become the focal point of connecting consumers and sharing information with the advent of cellular phones, tablets, and other similar devices.

Mobile networks allow consumers to operate their cell devices over various frequencies in different areas. However, the point is to be noted that the cellular devices and networks adjust the frequencies to use for communicating the data. They make use of the low power transmitters so that they can offer their services with the minimum interference. Mobile networks have evolved with time and grown from simpler to more sophisticated and efficient series of generations. This has been made possible through improvements in mobile technology. The earlier two mobile networks used analog voice for transmitting data, referred by 1G. Later introduced was the digital voice, that is, 2G for communication purposes. Then emerged the 3G technology that introduced the data connections, and this technology proliferated the smartphones in the market. This was combined with access to the Internet on the mobile phone. This invention revolutionized the market of communications. Finally, with the rise of 4G technology, it became possible to use broadband technology over mobile devices. Broadband increased the pace of Internet browsing substantially. The latest version of these technologies has appeared, though. That is a 5G revolution in the mobile service. This technology offers the greatest speeds to consumers' Internet usage. The 5G technology also reduces interference with wireless devices that exist nearby. The latest 5G technology uses signals with shorter wavelength signals and very high frequencies in transmitting data over the network. This technology offers increased bandwidths, and the signals have little chances of distortion. That implies the signals remain more directional, ultimately reducing interference.

# Trends in Mobile Technology

A trend is a way in some practice or industry that is becoming increasingly and widely accepted by the people involved. Trends in mobile technology refer to the gradual advancements in the technical aspects, increased usage preferences or inclinations of consumers, and the shaping of interacting behaviors of consumers with mobile networks and devices. Mobile technology has shown certain trends in new developments and productions. Mobile devices and mobile networks exhibit specific directions of advancements that are being observed in these days and will be speculated in the future more effectively (Fu & Hwang, 2018). Trends in modern technology have been noticed by the researchers, and these trends indicate a hopeful future of technology.

The mobile apps are more heavily incorporated with artificial intelligence capabilities. This is to make mobile apps more intelligent. The term smartphone also indicates the fact that mobile devices are increasingly being equipped with artificial intelligence features. The use of banking services, shopping features, and browsing options demonstrate the trend exquisitely. Many apps have increased the capabilities of mobile phones. Google Assistant, Google Maps, Alexa, and many others are examples of the AI integrations to the mobile devices. Further, mobile technologies are being integrated with location tracking facilities, as well. Every time people use download feature installed in their devices, their location is accessed by the device. This is a common phenomenon. Mobile devices track their location to get permission for downloads from related websites. These location accesses enable various organizations to interact with the user for different purposes. For instance, the businesses can send their targeted customers ads featuring their exceptional features or ads directed toward specific customers. The government agencies can also trace the individuals based on their mobile phone devices’ locations.

Mobile phones have reshaped the lives of consumers to a great extent. People have shifted most of their communication over mobile devices. They are relatively in less contact with each other, especially families who strived to get together in the past; these days, members of a family are not more physically closer. Yet they are more connected mentally and feel more satisfied this way rather than the traditional direct way of communication all day long. This has given people more freedom and privacy. The children are also more connected with their parents. The parents can ask about their wellbeing and progress now and then. The parents feel an enhanced sense of supervising their children and being informed of their activities. The members of a family or a group of friends can share pictures instantly at any occasion or event. The concept of social linkage and living together in a community have got strengthened due to existence of mobile devices.

Mobile technology is focusing on the speed of the processes involved. The programmers in mobile companies are working hard to develop mobiles that take little processing time. For instance, developers are striving to empower mobiles with fast browsing capabilities. Mobile commerce experience for the customers has to be improved by enabling certain features on the device that allow customers to make transactions with ease and credibility. To offer customers an opportunity to carry out payments with convenience and reliability is deemed to win customer loyalty and trust. Many new apps have been legalized and verified for providing reliable transactions to customers, and these apps allow the users to make financial transactions directly through the mobile and without intervention of banks or target companies. The mobile device manufacturers are required to create personalized experiences for customers. They have to interact with them on a priority basis and address their problems with focus and responsibility. People can choose to interact on any platform with the company. The mobile devices are the future of communication devices. The current trends indicate that future success will be for those companies that stay competent in this age (Lai, 2019). Further, a new trend in mobile technology has emerged to be the pairing of wearable items with mobile devices. "Smartwatches, glasses, bracelets, healthcare monitoring devices, etc." are in great demand. People want every accessory they use to be smart and powerful. The mobile devices paired with them create a mutual link, and these accessories exhibit intelligence and communication depending upon their capacities.

Mobile technologies are advancing toward achieving great features for mobile devices. The companies have started making efforts to enable mobile devices to control the outside objects nearby. The hope exists about digital devices to control houses of people and allow them more comfort in life. For this purpose, the houses will also be intelligent a little bit. The mobile technology is advancing to optimize the customer experience with innovation, quality, and performance.

Among the latest trends in mobile technology is to enhance data protection and security. These efforts are being made to win the customer's loyalty. Improved protection and security means reduced risks of data loss. Further, mobile technology has turned to address the needs of investigating cases of mobile incidents and provide useful clues to solve those issues. This practice is associated with the implementation of certain scientific techniques and procedures to detect crimes. It is referred to as device forensics. The device forensics uses embedded systems for finding evidence that can prove helpful in the court. The embedded systems used in mobile or other electronic devices are GPS tracking systems, personal data assistants, and multimedia players. The evidence generated as an outcome of the forensics research is digital and reliable. The mobile devices are prevalent these days, and people are involved in many activities using these mobiles. Therefore, a lot of important personal data is associated with these mobile devices.

Threats posed to the extensive and universal usage of mobile devices entail cyber-crimes, social crimes, and crimes committed against individuals, organizations, or states. The information saved in or via mobile devices is the only way to solve the issue in most cases. The email history, previous calls are done by the user or received calls, messages exchanged, or the embedded apps used – all can be sources of evidence. The apps installed on mobile devices are becoming more proactive. The artificial intelligence has a great contribution toward enabling the mobile manufacturing companies to incorporate the intelligent systems in the devices. It provides certain algorithms, programs, and applications that will empower the electronic or mobile devices to meet the needs of the future and provide security to the user as well as the society on the whole.

# Laws, Regulations, and the Forensic Handling of Mobile Devices

People in the modern world have become involved in countless activities that make use of the Internet and electronic devices such as mobiles, computers, tablets, etc. These activities are linked to different issues related to security and privacy. For instance, individuals can receive threats by a party on mobile devices via the Internet. Hackers can plan attacks against a computer network and can cause serious damages to the identity, assets, or confidential data of the entities involved. Another considerable threat that is prone to harm the vulnerable networks is the viruses that are generated artificially as well as they can emerge automatically due to system flaws. The viruses can cause defects in operating systems and other computer applications, leading to disturbance in work and potential loss of data. The electronic devices are used for storing data, which can contain information regarding the incidents.

Given the above-mentioned situation, it becomes necessary to address the issues of insecurity, crimes, and social evils related. To this end, the government has to step in and make the regulatory framework for the use of mobile and other electronic devices. The government authorities establish regulations to control online traffic, data, and assets security and protect identities of individuals and organizations. The laws and regulations that govern digital evidence in investigations of crimes are primarily sourced by the Fourth Amendment made to the United States Constitution or the statutory laws ensuring privacy. While considering various situations that emerge as a result of cyber-crimes, it can be noted that these situations mostly fall under either the Fourth Amendment or any one of the three statutory laws. The two primary sources of law sometimes overlap in regulating the use of electronic devices for communicating over a network. Therefore, these laws and their implications are usually discussed together to serve the purpose.

The laws restrict the authorities to search and seize digital evidence without a legal warrant. This is to ensure transparency, unbiasedness, and efficacy in the implementation of concerning laws (Losavio, Chow, Koltay, & James, 2018). This is to ensure the security and dignity of people, organizations, and records so that no violations occur of the basic as well as civil rights of the entities involved. The law states that the search and seizure of property can be permitted only in case of some serious or meaningful interference with the possessions of an entity. The court will not accept any evidence that has been collected in violence of the “Fourth Amendment Protection Act." The laws have interfered and governed many situations that involve examination of the devices used by terrorist suspects (Wayne, 2018). To this end, sometimes, the authorities have to acquire the services of a third party to solve the cases. The third party's role is usually to decode sensitive information or investigate records of possible suspects.

Certain aspects of evidence collection by law enforcement are not restricted by the Fourth Amendment. Information that has been shared on a drive with others, or the private searches made individually and already found by other workers are not covered by the amendment as well. In a Supreme Court’s jurisdiction, it has been ordained that intrusion with the use of technology should be considered to be a search of evidence, and the protection given in the Fourth Amendment was extended to even those areas for which an individual has a reasonable expectation of privacy. The US court ruled out for complicated issues that no files would be given privacy in case a specific portion of a memory drive is under inspection, and the argument that those files are separate in their use will hold no value.

Digital forensics is the study of principles, techniques, and procedures applied in recovery and investigation of susceptible data recorded in or via the digital devices to provide evidence in criminal cases (Sunde & Dror, 2019). All digital devices that can be used in digital or cyber-crimes lie within the scope of digital forensics. Mobile phones, tablets, personal computers, laptops, SIM cards, memory chips, memory cards, portable hard drives, email records, calling details, messages history, and many similar sources come in direct observation in case an incident occurs that needs to be responded by the investigating team.

Several institutions today define and exercise notable practices in forensics research and analysis. The “Scientific Working Group on Digital Evidence” emphasizes the best methods to collect, analyze, and report forensic evidence for use by a court. Another example is the "National Institute of justice," which lays a basis of principles and standards for conducting forensic research effectively. The “American Bar Association” is prominent in this respect, and it has issued a detailed guide on carrying out digital forensics efficiently.

The forensic research principles and guidelines say that the evidence must not be lost in research and investigation procedures. That is why the situations require to be handled gently that makes sure the devices involved are intact, or not damaged more in case they are already damaged. Whether the device involved is physical or digital, the evidence should be acquired with care and protocol. The handling of mobile or other electronic devices should be assigned to experienced and skillful persons because many times, certain situations arise that demand professional knowledge. For instance, a situation may arise where the digital device is programmed to destroy data actively through the disk formatting feature; it may be necessary to turn off the device immediately so that the crucial data needed for evidence can be saved from being destroyed. It can be considered alternatively, however, that the device should not be turned off at once to allow the investigating forensics research team to check the temporary run-time memory of the device.

Digital evidence has many similar issues, like those of the physical evidence. For instance, digital evidence can get contaminated by external factors. Therefore, it is recommended in forensics research practice that all digital evidence should be saved by creating digital backups, replicas, or captures. Images are usually created to save digital evidence or susceptible data. The images are very useful in this respect and provide accurate recovery of the data in case of evidence lost. Further, images are the most dependable source of data in most of the cases provided that the images indicate the required incident. The forensic information can be produced by several other useful sources such as susceptible encrypted files, deleted files, or metadata.

# Analysis and Presentation of Forensic Information

It should be noted that in cases of digital crimes, most of the digital evidence is likely to be found within the file system. However, the most challenging job of a forensics research professional is to understand the file systems of digital devices. The professionals should demonstrate the ability to explore, find, and evaluate the relevant information from within the file systems existing in the electronic devices. The file system analysis entails several activities to be completed depending upon the case requirements. The researcher has to identify the crucial information on the storage device, probably a disk drive. An ability to read source data is an essential skill. The researcher has to indulge in analyzing several partitions on the hard drive employing various techniques. Further, the researcher needs to analyze the contents of disk drives. Finding relevant evidence is the outcome of all effort, and it can be accomplished by finding metadata, recovering deleted files, and identifying locations used for data handling.

Mobile devices investigation usually involves forensic tools that may be commercial or open-source. Forensic tools are used to search for data from within the internal memory of mobile devices. The content of internal memory is not changed in forensic examination. The integrity hashes also have to be calculated for the information collected. All forensic tools must adhere to the protocol and standards that have been developed for regulating communications with digital devices (Cameron, 2018).

When investing in digital crimes, forensic researchers should pay enough attention to locating the information storage location accurately. The investigators are confronted with immense trouble in dealing with mobile devices during forensics research. This is because mobile phone users are used to installing several applications in their devices, which are not provided by the mobile company. These applications are referred to as third-party applications. These applications include IMO, tango, KM player, and many others. The problem arises in finding out the exact location of information storage. For instance, a third-party app usually doesn't allow the user to record the file history somewhere in the mobile device; instead, the files are located in the server of the third-party app's server. When the forensic researcher tries to locate the relevant information in mobile device storage, the files are not found, and the researcher is prone to be misled.

Forensic research involves data carving that is applied in case no metadata is available. It entails fetching the data files from raw data fragments of the memory drive and reassembling them. Data carving is performed by the researcher to find out the lost or deleted data. It is carried out, for instance, when a memory drive is encountered with failure of an action. The inherent concept in this activity is that the file systems in storage devices do not delete the data in absolute terms. Certain means of extracting the deleted data do exist like the data carving technique to assist in providing evidence in digital forensics. There are four steps involved in the data carving process. A data set is needed to perform the task for testing the data carving tools and the outcomes. Producing a valid data file is also necessary for the fragmented files. The use of languages invalidating the data files often referred to as semantic validation, is essential in doing digital forensic research. The final step in data carving is to leverage the process of carving validation so that it may be enabled to identify the injected codes or potential data evidence.

A compound file is a file containing data or information, and it consists of other files or data. The ZIP compressed file is a vivid example of what a compound file can be. It is required in forensics research to expand the compound files in the early stages of a forensic research project so that the forensic researcher could explore the contents fully. Further, it is suggested that forensic research requires to perform compound file expansion before the index search is conducted.

Digital forensics research needs to be presented in a written form formally once it has been completed in every respect. These reports are probable to be reviewed by organizations, individuals, forensic researchers, lawyers, judges, and many others. Therefore, the report should comply with all the established standards for report presentation. A formal digital forensic analysis report consists of an executive summary, research findings, appendices, and a conclusion.

The introduction describes an account of the case under discussion, informing the reader about the issue of cyber-crime and outlining the steps briefly to be taken in the research. The introduction also gives details about initialization of the project, and the need for evidence to be extracted through this study. The next step is to coming in contact with the digital evidence sources and preserving digital devices with care. This section details the careful handling of digital devices. The techniques and tools to be used in the digital forensic investigation are discussed and justified in this section. The details of forensic investigation and their analysis are presented in the third section. The tools and techniques used in the research are elaborated. The analytical methods employed need to be described with a complete explanation so that the reader finds the report credible enough for referencing in several places. The findings will be presented after analysis. The findings should be based on objective judgments, and digital forensic knowledge has to be employed in deducing inferences from the analysis data. Finally, a conclusion is given based on the analysis and findings. To present report findings after giving detailed analysis is more than an art. The way these findings are inferred makes the audience persuaded.

# Biggest Threat & the most promising Technology in Mobile Devices

Social engineering is likely to be the greatest threat among the cybersecurity issues in the future. It refers to the use of deceptive tactics to misuse individuals so that they leak out their personal information or confidential information related to an organization, eventually leading to identity or property damages. Social engineering can be executed through computers, mobiles, and other electronic devices. With mobile devices, social engineering can cause serious threats to users' identity or assets. Fake messages can be received by users, and they could be persuaded to share their personal information. The users may also be urged to register with some malicious application or connect with a malicious link. Further, the hacker might send spam emails or messages that can harm if opened carelessly. Sometimes, certain web links are suggested by anonymous service providers, which can harm the device potentially. Social engineering, when performed to attack corporates, can damage them considerably. To intrude an organization, social engineering geniuses find someone in the organization to get confidential information. They manipulate employees in many ways and make them divulge secret information. The hackers use this information to plan cyber-crimes.

The best solution to confront the challenge of social engineering threat is to be pro-active and think and prepare for it is one step ahead of the hackers. To this end, individuals must be educated to have the necessary cyber-awareness. In the context of a corporate, they should implement strict identification policies, security systems, and authentication procedures. Appropriate privileges must be granted to employees for accessing their relevant information within the premises of the organization. The latest software should be installed to protect any cyber-attacks. This software should comprise antivirus as well as anti-phishing. The organizations should classify their information and take protective measures by granting controlled access to all employees. In an individual context, it is important to beware of unknown identities. Android scanners need to be used and updated regularly. Any unknown or suspicious email, message, or call should be avoided. It is most dangerous to do as advised in a fake message. The connections on social media should be monitored and verified.

Works Cited

Cameron, L. (2018). *The future of digital forensics faces six security challenges in fighting borderless cybercrime and dark web tools*. Retrieved from Computer. org: https://publications. computer. org/security ….

Fu, Q.-K., & Hwang, G.-J. (2018). Trends in mobile technology-supported collaborative learning: A systematic review of journal publications from 2007 to 2016. *Computers & Education*, *119*, 129–143.

Heflin, H., Shewmaker, J., & Nguyen, J. (2017). Impact of mobile technology on student attitudes, engagement, and learning. *Computers & Education*, *107*, 91–99.

Lai, C.-L. (2019). Trends of mobile learning: A review of the top 100 highly cited papers. *British Journal of Educational Technology*.

Losavio, M. M., Chow, K. P., Koltay, A., & James, J. (2018). The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. *Security and privacy*, *1*(3), e23.

Ooi, K.-B., & Tan, G. W.-H. (2016). Mobile technology acceptance model: An investigation using mobile users to explore smartphone credit card. *Expert Systems with Applications*, *59*, 33–46.

Sunde, N., & Dror, I. E. (2019). Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. *Digital Investigation*, *29*, 101–108.

Wayne, J. (2018). *Cybercrime and Digital Forensics*. Clanrye International.