**Mobile Device forensic**

Student name

Institutional affiliation

Course number and name

Instructor’s name

**Mobile Device Forensics**

**Introduction**

A Digital Forensics Investigation’s primary goal is to follow the proof and settle on the crime or the offense. Envision a security penetrate occurs at an organization, bringing about taken information (Iqbal & Alharbi, 2020). In the present circumstance, a PC scientific expert would decide how aggressors accessed the organization, where they crossed the organization, and what they did on the organization, regardless of whether they took data or planted malware. Under those conditions, a computerized legal agent's job is to recuperate information like records, photographs, and messages from PC hard drives and different information stockpiling gadgets, like zipping and glimmer drives, erased, harmed, or in any case-controlled (Iqbal & Alharbi, 2020).

Digital forensics is a key aspect of internal investigations that contain a hidden audit trail that provides crucial evidence about a crime. A forensic image preserves all data within a computer when it is taken; hence, the time it takes to image a digital device, the opportunity to capture the data required by an investigator to piece together the evidence increases (Iqbal & Alharbi, 2020). Digital forensics is implemented into a proactive risk management policy that states the legislation visible for a company and can act as a significant deterrent to those considering unauthorized activity. Completing and efficiently implementing the provisions can satisfy a number of compliance requirements within standards and accreditations (Iqbal & Alharbi, 2020). During computerized criminology and incident reaction, IT experts may be entrusted with malware examination. Programming experts can figure out malware to become familiar with how it works, how it was created, and who made it. Digital forensic investigators help identify threats/ vulnerabilities, and the experts implement risk mitigation methodologies. The risk mitigation techniques confront the risks and help resume the operations that were stopped due to natural calamities or any disasters. The information acting as evidence in a case of such a crime is retrievable from electronic devices like mobile phones, iPods, personal computers, and even network interfaces (Iqbal & Alharbi, 2020). In this research paper, the primary goal is to find technologies, software, and devices that can be used to retrieve and analyze digital forensic information.

**Mobile forensic**

Phone memories preserve information such as the call log, messages, location, emails, and other essential information that might be effective in digital forensic investigation. Mobile forensic is specific forensic conducted from the personal or any mobile device memory (Alatawi et al., 2020). Mobile forensics include call logs, location, web search history, plus other large variety of information that the phone stores. The information collected in the form of forensic from phone memories is applicable in intelligent planning and operations focused on managing crime and criminal activities like terrorism and cyberattacks (Alatawi et al., 2020). Mobile forensic is also applicable in an organization as a strategy to manage and mitigate risks specifically associated with information handling and data management. For example, suppose an employee stills data from the organization using a personal phone or computer. In that case, it is easy to trace by scanning the computer memory or any other electronic device that the employee might use in sharing data.

Mobile forensic is significant in handling cases involving crimes, identity theft, homicides, computer crime, cyberbullying, and terrorism, and terrorism in court. This is possible through the extraction of digital information from mobile devices like personal phones, disk drives, laptops, or desktops using advanced software tools (Alatawi et al., 2020). Using the advanced technologies designed for data forensic data retrieval and analysis, the investigators use information trends used as evidence to justify criminal activities. For effective retrieval and analysis of forensic data in mobile forensics, accepted practices and policies must be met. The forensically accepted standards are defined as the procedures necessary for acquiring electronic information in a manner that does not distort the information but ensures information recovered is reliable and effective for admission as evidence in any cases involving the owner of the mobile device.

Mobile forensic, like any other risk management procedure and method, has got various challenges that impact the investigation either positively or negatively. Data from the devices might play a crucial role in instigating the challenges. Some of the negative challenges investigators experience in a mobile forensic investigation include;

Data deletion. Mobile forensic entirely depends on data stored within the mobile devices, and in case this information is deleted or erased completely from the device memory, it becomes complex retrieving the data. Accessing already deleted data from a mobile phone is not an easy task for investigators to retrieve existing information.

Another challenge is the use of passwords and locks. In this era, passwords and locks are not numbers and patterns like before. Password locks now include biometric features like eye lenses, fingerprints, facial recognition, and even sound recognition. These security modes are capable of protecting even against prying or eavesdropping on personal communications and information. Breaking into these security layers to access the phone memories is a hard nut to crack. It will require special software, more time, and increased investment to retrieve and analyze information from locked mobile devices effectively.

Another challenge mobile forensic investigators experience is true mobility. True mobility involves various advanced technologies necessary for data sharing, retrieval, and storage. For example, a cybercriminal can use a virtualized mobile device to conduct an attack and simply mirrors the device across a network, so it is untraceable and inaccessible by mobile forensic investigators. Under true mobility, documents can be shared over a cloud or internet storage facilities then the information shared gets deleted. This results in inefficient data utilization and complex access by the investigators into the device.

Mobile devices exist in different operating systems, for example, Android and iOS. These operating systems contain different security levels and data policies. Retrieving and analyzing data from the various operating systems might be different since they require different tools. However, this complexity is defined by the frameworks in which the operating system is built. Comparing Android and iOS or Blackberry, Android has different hardware meaning access, and analysis is also different. An operating system or device that uses iOS technology requires a tool like Elcomsoft iOS forensic toolkit specifically for cracking, retrieving, and analyzing information stored in the iOS devices. Despite having different frameworks tools for analysis, mobile devices, regardless of the operating system, contain the same type of information as evidence in mobile forensic. Therefore, analysis for pieces of evidence is the same.

Mobile devices are advancing with data being stored in the cloud, device virtualization, and advanced security, investigators, also require advanced technology to retrieve and analyze information for the mobile devices. An effective tool for mobile forensic in this age must be able to prioritize, collect and decrypt information from various devices to maintain integrity and mining useful data formats for forensic investigation. The tools also focus on investigating, retrieving, analyzing, and preserving forensic information as evidence and handling data with care.

Some of the forensic tools necessary for investigating, collecting, and analyzing forensic data, according to Agrawal et al. (2018), include; Elcomsoft iOS forensic toolkit that deals with iOS devices only. The tool can access highly sensitive data like location: email, social networking accounts, Wi-Fi username, and call logs. Application varies from military intelligence, law enforcement agencies, and the government. Another tool, UFED Ultimate, makes information retrieving, deleting, examining, and gathering evidence easy. Performs complete information acquisition and logical extraction through bypassing the security of the encrypted mobile devices for easy information extraction and processing. The next mobile forensic tool is the E3:DS software which is an advanced mobile forensic solution for data extraction and forensic analysis. The tool automates searching and processing of evidence, support extraction, bypassing, chip dump, and cloud information retrieval, as well as automated reporting. Another more advanced tool used by several organizations and internet companies is the Oxygen Forensic Detective. It allows for data analysis, decoding, and extraction from almost every electronic device existing like android phones, iPhone, and drones. The companies that use this forensic tool are majorly services providers like Email, Facebook, Google, WhatsApp, Microsoft, Twitter, Instagram, and iCloud. The last tool for this study AccessData's forensic toolkit FTK which combines power, technology, speed, stability, and fast searching with standalone and advanced software for effective mobile forensic services. It is effective for complete extraction and recovery since it utilizes hardware resources to extract forensic evidence quickly.

**Conclusion**

Research has shown that several mobile devices are exposed to several security risks as well as being used to carry out attacks. Digital forensic is effective in discovering and deciphering electronic information with the primary goal of providing safety and managing risks associated with criminal activities conducted using electronic gadgets (Iqbal & Alharbi, 2020). Mobile forensic is a branch or a sector of the general digital forensic. The primary goal of digital forensic is recovering digital evidence from a mobile device in a way in which information can be preserved as forensic evidence. Forensic data is extracted from a mobile device procedurally, including seizing, identifying and extracting, examining, and analyzing data to find forensic evidence.

**References**

Alatawi, H., Alenazi, K., Alshehri, S., Alshamakhi, S., Mustafa, M., & Aljaedi, A. (2020, September). Mobile Forensics: A Review. In *2020 International Conference on Computing and Information Technology (ICCIT-1441)* (pp. 1-6). IEEE.

Agrawal, A. K., Khatri, P., & Sinha, S. R. (2018). Comparative study of mobile forensic tools. In *Advances in Data and Information Sciences* (pp. 39-47). Springer, Singapore.

Chernyshev, M., Zeadally, S., Baig, Z., & Woodward, A. (2017). Mobile forensics: Advances, challenges, and research opportunities. *IEEE Security & Privacy*, *15*(6), 42-51.

Lei, Z., Nan, Y., Fratantonio, Y., & Bianchi, A. (2021, February). On the insecurity of SMS one-time password messages against local attackers in modern mobile devices. In *Proceedings of the 2021 Network and Distributed System Security (NDSS) Symposium*.

Shakir, A., Hammad, M., & Kamran, M. (2021). Comparative Analysis & Study of Android/iOS Mobile Forensics Tools.