Xournals

Academic Journal of Forensic Sciences

ISSN: 2581-4273 | Volume 05 | Issue 02 | October-2022

Forensic Investigation of the Basic Digital Evidences in Mobile Devices

Gladwel Kubwalo[1], Tejasvi Bhatia[1]

Available online at: www.xournals.com

Received 06th September 2021 | Revised 20th January 2022 | Accepted 12th September 2022

Abstract:

Crimes have been taking place since time in memorial. These crimes are committed differently and that is the reason why they have different names with respect to the factors that determine the offence. It is the core duty of investigators in law enforcement agencies as well as other relevant stake holders to crack down and identify the perpetrators of crimes. It is empirical to mention that the identification of perpetrators of crime is based on the piece of evidence that has been collected. Evidence most of the times is collected at the scene of crime in physical form or from eye witnesses who are people that are present when an offence is being committed. Sometimes evidence is circumstantial depending on how the events surrounding the criminal act occurred. In the modern world, mobile devices are playing a very significant part in our day to day life. These days, mobile devices are being used by individuals of all classes as opposed to a distant past whereby usage of mobile devices was limited only to high class people. The wide usage of mobile phones provides vast availability of evidence. Potential piece of evidence is collected from electronic devices such as mobile phone in digital form. It is advisable that all sorts of evidence that has been scientifically collected and analysed must be treated bearing in mind the set out legal standards so that they can be accepted in court. Forensic investigators are mandated to make sure that they follow proper legal standards when handling forensic evidence. This paper will highlight some forensic evidences and the methodologies on how to collect them from mobile devices. It will also highlight some of the tools that are employed in order to recover data or forensic evidences found in mobile devices.

Keywords: *Forensic Evidence, Mobile devices, Forensics, Drone Forensics, Data Acquisition, potential evidences, electronic devices, forensic investigator*

Authors:

1. *Lovely Professional University, Phagwara, Punjab, INDIA*

Introduction

Forensic evidence found in mobile devices is studied under the field of digital forensics. Mobile devices in this case shall mean electronic equipment like mobile phones, Personal Digital Assistant (PDA) devices, Global Positioning System (GPS) devices and tablet computers **(Bennett, 2012).** Digital forensics is generally a branch of forensic science that deals with the investigation and recovery of evidence in mobile devices normally that are connected to computer crimes **(Daware *et al*, 2012).** This definition collaborates to the explanation that digital forensics also comes under the field of forensic science but its main objective is to see to it that potential evidence which can be traced in digital devices as a result of a computer crime is thoroughly collected, examined and stored according to the set legal standards **(Anghel, 2019).**

Digital forensics has been defined as a sub-set of forensic science that constitutes the elements of law and computer science to retrieve and examine data that can be acquired from digital devices, different types of networks and storage devices based on the set legal standards and procedures to guarantee admissibility of the evidence in the criminal justice system **(Pernik *et al*, 2016).** Mobile forensics on the other hand is a field under digital forensics whose goal is the recovery of potential evidence from mobile devices **(Casey, 2009).** This branch of mobile forensics has as of late gained much recognition as a result of the increase in the number of people that are in need of the services which are available in mobile devices **(Kylämies, 2019).** This increase in the number of people in need of mobile device services has created the availability of mobile devices throughout the whole world. Since mobile devices demand connectivity, this has resulted in the fast-growing Internet of Things (IoT) technology to supplement the availability of the desired services **(Al-Dhaqm *et al.*, 2020)**. The onus to select a specific forensic methodology when examining evidence is based on the quality and quantity of the evidence in question.

The major aim for a sound forensic examination of digital evidence in question is that the original evidence must not be modified at all costs **((Kylämies, 2019).** It is therefore the responsibility of forensic investigators to present evidences to the courts without any modifications. Any modification or alteration made to forensic evidence renders it invalid and therefore not accepted in court **(Jain and Chhabra, 2014).** This situation has negative repercussions to the justice system as the genuine case may end up being thrown out of court simply because the evidence was mishandled at a certain point in course of the investigations. Mobile devices are defined as portable electronic equipment that has the capability to connect to the internet **(Sathiyanarayanan, 2016).** Mobile devices are used to commit various types of crimes by ill-minded people. Some examples of nefarious activities that are done using mobile gadgets are defamation, forgery, terrorism, cyber harassment, cyberstalking among others **(Yeboah-Boateng and Amanor, 2014).**

It is the responsibility of forensic investigators to identify the potential evidences in these devices. It is only through the process of the investigation of such evidence that they can connect the crime under investigation to the perpetrators. In an effort to deal with these nefarious activities, digital forensics is taken into account to combat computer-related crimes and to pinpoint the device-assisted crime and the authors of it **(Sathiyanarayanan, 2016).** This entails that without evidence then it will be a tall order to bring to light the author of the crime. There are so many ways in which mobile devices can be used **(Muzyleva *et al*., 2015).** They are sometimes used to communicate with families and friends through voice calls. Sometimes mobile devices are used to send messages. Some individuals use mobile devices to chat with their loved ones through various social network platforms like WhatsApp, Facebook, Instagram and Twitter. Mobile devices have the potential to perform video calls and sometimes send videos and photos. Mobile devices have the ability to compose videos and record audio. Mobile devices can send and receive emails and give the location of an individual **(Song *et al*., 2013).** These services that individuals access through interaction with mobile devices are the very same services that are employed to commit crimes. As a result, these very same services if employed in criminal activity then they are sources of potential evidence. It is therefore the responsibility of investigators to investigate mobile devices that were involved when committing the crime and find the evidence from such devices.

Forensic Evidence

Evidence can be defined that when an offence has taken place and an allegation has been made against someone, investigators will try to find anything which is accepted by the court of competent jurisdiction to prove or disprove the allegation made **(Pandey, 2020).** The type or form of evidence used in the criminal justice system is called forensic evidence. Relevance and reliability are the only two conditions that have to be satisfied for evidence to be accepted in court **(Prakasam, 2004).** Investigators are mandated to acquire the necessary skills and knowledge to identify any potential evidence at a crime scene. After

identification of any potential evidence at the scene of the crime, investigators must classify each type of evidence accordingly so that they build a strong case **(Pandey, 2020).**

Evidence Identification

It is the responsibility of crime scene investigators to visit the crime scene and possibly identify and collect all potential evidences necessary for analysis in a forensic laboratory. Potential evidences are identified at a crime scene because of their uniqueness **(Kennedy, 1996).** For instance, if a serial number of a particular mobile device has been identified that its device was used to originate a cyber-stalking message then, the owner of that mobile will be regarded as one of the suspects. The forensic evidence should also lower the likelihood of an event having happened by chance **(Aitken and Taroni., 1995).** . This means that if the mobile device contains biometric data like fingerprints then the owner of those prints is considered as the suspect in the offence in question. If there is a physical match between a stolen item and the item that one is possessing then that should be identified as potential evidence. This implies that if one is found with mobile equipment that was stolen at a homicide scene of crime then that particular device should be treated as evidence **(Pandey, 2020).**

Types of Evidence

Some of the main types of evidence with respect to the Indian Evidence Act under section 65B are;

a) Oral Evidence is a type of evidence given by an eyewitness.
b) Documentary Evidence is a form of evidence presented in written form in form of documents.
c) Real Evidence is basically physical objects which are held that forms part of the crime like a mobile phone used in a criminal act **(Schachter, 2009).**
d) Hearsay Evidence is a form of evidence given by a witness from what was heard from another person.
e) Circumstantial Evidence is a type of evidence given by a witness that does not directly prove a fact but depends on how the events occurred.
f) E-evidence is a kind of evidence that is obtained from electronic equipment like file footage of a CCTV camera **(Taylor, 2019).**

Evidence Collection

Evidence found in mobile devices is collected in several ways based on the nature of such evidence. It is clear that tools used to analyse evidences will differ according to the form of the evidence **(Ahmed *et al.*, 2008).** For example, the procedure to collect deleted data is different to the procedure of collecting data from simple plain text. The procedure to collect evidence will also differ based on the condition of the mobile device to be examined. The United Kingdom Association of Chief Police Officers (ACPO) came up with some guidelines that highlighted that mobile phone, for example, will need a Faraday bag or to remove the sim cards to avoid it from communicating with other mobile devices remotely thereby barring it from receiving and sending any data (**Biggs and Vidalis, 2009)**. Similarly, a laptop is switched off mode will be treated differently to that in switched on mode.

Forensic Evidence Collection Tools

Several forensic software is used to collect evidence from mobile devices depending on what type of evidence is to be collected. There are so many forensic tools that have already been discovered that are used to extract data from mobile devices **(Garfinkel, 2010).** Some of the well-known and most used tools because of their accuracy in data recovery are:

a) Wondershare Dr. Fone toolkit is used to recover deleted data, unlock iPhone apple identity and locked screen etc.
b) MOBILedit Forensic Express was initially designed for use by law enforcement officials but now it is available for use by the general public to retrieve deleted data.
c) FonePaw has the capability to recover deleted data from android phones **(Chernyshev t *et al.*, 2017).**
d) eMailTrackerPro detects the IP address of the device used to send the email.
e) EmailTracer has been developed in India to trace the origin of emails.
f) AccessData FTK is used for computer forensic analysis, decryption and password cracking.
g) EnCase Forensic Tool is used to produce an image of the storage drive in the data recovery process.
h) Paraben Network E-mail Examiner is used for comprehensive email analysis **(Carvey, 2018).**

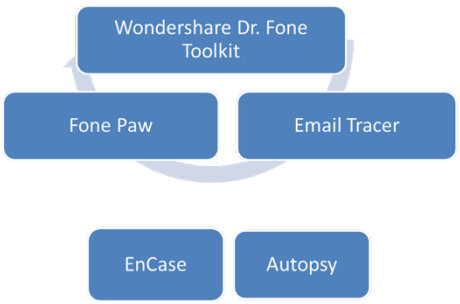

Figure No. 1: Examples of some Forensic tools

Evidence Acquisition

Data acquisition from mobile devices is a process of obtaining and organising information from them and their peripheral devices **(Al-Hadadi and AlShidhani, 2013).** Peripheral devices are those kinds of equipment that work together with other devices through a wired or wireless connection. For example, a computer keyboard can provide potential evidence in the form of biometric data if it is connected to a crime. Other examples include image scanners, digital cameras, computer mice etc. Forensic investigators should ensure that proper legal standards are followed and adhered to during the entire process of data acquisition, analysis, transportation and storage. There are three basic methods of data acquisition which have been briefly discussed below **(Garfinkel, 2010).**

Data Acquisition Methods

The manual acquisition is a process done when the forensic investigator makes use of the user interface to find out what is contained in the memory of the mobile device **(Tajuddin and Manaf, 2015).** In the case of a mobile phone, the forensic investigator will either use the keypad or the touch screen according to the type of the phone to navigate through and acquire the targeted data. This stage of data acquisition does not need complicated technical skills because the mobile phone is used normally and sometimes in the presence of the owner of the phone. The investigator is encouraged at all costs to take note of passwords wherever applicable. Any event at any point during the acquisition process must be documented to maintain the chain of custody. The investigator is also encouraged to take pictures throughout the entire process **(Bommisetty *et al.*, 2014).** This process of data acquisition is advantageous because the application software gives chance to investigators to navigate through the phone without using complicated tools to change raw data into human-readable information **(Al Mutawa *et al.*, 2012).** One of the drawbacks is that data recovered is only the kind of data that is available to the operating system. Secondly, the kind of data that is recovered is only in form of photographs. This process of data acquisition is also time-consuming **(Bommisetty *et al.*, 2014).**

The logical acquisition involves a piece by piece copy of logical storage data like directories and files that are stored in the mobile device. This method of data acquisition can afford to recover data that is stored in the logical partition of the memory of the mobile device. The logical acquisition method does not have the capacity to recover data that is available in other storage locations apart from the logical partitions like the unallocated space. In the case of mobile phone, the phone from which the data is copied is connected to another device that will store the copy and the forensic investigator uses prescribed commands in order to extract the data using tools like Oxygen phone manager or Paraben cell seizure **(Alghafli *et al.*, 2012).**

This method of data acquisition has a limitation in that it cannot recover deleted evidence or information **(Daware *et al.*, 2012).** This means that if the mobile device is damaged then there is no way a bit by bit copy of its data could be made **(Fukami and Nishimura, 2019).** This method, therefore, does not possess the capacity to bypass the security system of the mobile phone from which the data is recovered.
Physical acquisition implies that the whole substantial storage of the mobile phone is copied gradually **(Daware *et al.*, 2012).** This method of data acquisition works in the same way as if someone is doing a clinical analysis of a personal computer. This method gives an opportunity to forensic investigators to recover deleted data **(Beebe *et al.*, 2005).** This means that data from physically damaged phones can be recovered using this method. This method gives chance to forensic investigators to recover information from a mobile device whose sim card has been lost or removed **(Kubi *et al.*, 2011).**

However, there are certain technicalities that must be investigated to recover the deleted data due to security features that are installed by the equipment manufacturers to avoid the arbitrary reading of the device memory **(Daware *et al.*, 2012).** This shows that this method should not be used unless all other methods have proved futile because it has the limitation that it can alter the evidence. This method is complicated and requires specialised technical personnel to carry out the analysis **(Srivastava and Tapaswi, 2015).** As a result, there is more time taken for the examination and analysis of data using this method. The figure below shows the data acquisition methods. As you go up the pyramid, there is an increase both in time and technical expertise needed during the data acquisition process.

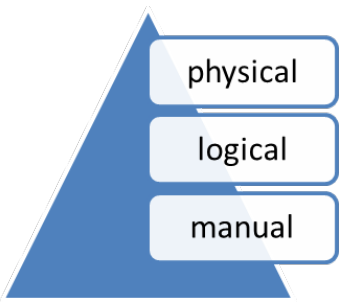

Figure No. 2: Data Acquisition Methods

Figure No. 3: Some Examples of Mobile Devices

a) Smartwatches are a source of call logs, messages, pictures, videos and locations used to track where a person is.
b) Digital/Video cameras are used to record or capture and store videos and pictures.
c) Cell phones are sources of call logs, SMS, MMS, social media accounts like WhatsApp, Facebook, etc.
d) Laptop computers are a source of internet search history, social media accounts and email accounts among others.
e) Storage devices like hard drives, pen drives and optical media are sources of stored data that can be retrieved whenever necessary.
f) Drones also termed unmanned aerial vehicles are flying objects that are sources of potential forensic evidence in form of videos and pictures taken from places that it was designated**.** Drones are mobile devices that are studied in the field of drone forensics. Drone forensics falls under the study of digital forensics which focuses much on digital data recovery from drones **(Chávez and Swed, 2020).** Drones have proven to be valuable sources of forensic evidence if used in both civil and nefarious activities.

There are so many nefarious activities that are done using the drones like smuggling of contraband goods into restricted areas **(Schmersahl, 2018).** They can be used by drug dealers to transport several pounds of illicit goods from one area to the other because drones have the capacity they can be operated remotely a couple of miles away from their base. Drones are also used to spy on people in their bedrooms or bathrooms because they have the capacity to take pictures and record videos. A drone that was used to spy on a couple in their bedroom was caught and upon its examination, it was discovered to contain illicit images in its memory card. Forensic investigators used those images against the perpetrators of that crime who were charged with an offence referred to as voyeurism **(Chávez and Swed, 2020).**

Drones are supposed to be registered for easy monitoring when flown into the air space. There are certified organisations that control movements of air traffic in controlled airspace like the Federal Aviation Administration (FAA) in a number of states across the globe including the United States of America whose rules apply to the entire National Space System **(Bouafif *et al*., 2020).**

However, criminals do possess homemade drones which are then used for criminal activities. These drones are difficult to monitor because they are not registered and therefore difficult to catch. It is based on this fact that criminals use unregistered drones to commit crimes and consequently evade trial. However, efforts are being made to fight this malpractice **(Bouafif *et al*., 2018).**

Table No. 1: Some examples of mobile devices and the data stored

Name of Device	**Data Stored**
Smartwatch	Call logs, pictures, audios and videos
Digital Camera	Pictures, videos
Cell phone	Call logs, messages, videos, audios
Laptop Emails	Emails, audios, videos, photos
Drones	Illicit goods, videos, audio, photos.

Examples of Evidence Found In Mobile Devices

Serial number. This is a peculiar number that mobile phone manufacturers allocate to specific equipment. It is a number that is allocated specifically to a mobile phone **(Kumar and Kaur, 2015).** This implies that no two mobile phones can bear the same serial number even from different phone manufacturers. This number is referred to as the International Mobile Equipment Identity (IMEI). This number has fifteen digits and is used to track mobile phones that may have been stolen or used to commit a crime. This specific number is mostly found printed inside the battery compartment of most mobile phones. The number can be accessed on the screen of the mobile phone dialled *#06#. All those phones that accommodate double sim cards are allocated two serial numbers. An example of a serial number can be 860913041314934.

Simcard. The term SIM is an abbreviation that stands for Subscriber Identity Module (SIM). It is an integrated circuit that is specifically made to securely store the sim card number. This number is technically referred to as the International Mobile Subscriber Identity (IMSI) number **(Casadei *et al*., 2006).** When a call is made, this number is the one that gets dialled and the caller number gets displayed on the receivers screen. This number is also unique and assigned to one individual at a time by the service provider to which one is affiliated. These numbers are assigned by network providers to the particular sim card. This number holds the details of the owner of that number which is then used for identification **(Strobel, 2007).** IMSI number can identify the IMEI of the mobile phone in question. When an offence has occurred, the investigator will use this number to identify the author of the crime or to identify the owner of the phone that was lost. This card is used also to store phone contact numbers. Sim cards are not only used in mobile phones but also in smartwatches and some cameras. The sim card contains the Personal Identification Number (PIN) and the Personal Unblocking Key (PUK) for security reasons **(Clarke *et al*., 2005).**

Call logs. This is the kind of information that is created when a call is made. This is the basic information that is readily available in each mobile phone unless deleted **(Zhang and Dantu, 2010).** Call logs are found in almost every mobile phone because mobile phones are procured mostly for voice calls. This kind of data is available from internet service providers and can be accessed only by law enforcement agencies like the police. Therefore, once a crime has been perpetrated using a particular mobile phone, it is the duty of the forensic investigators to find out the call partners by analysing the call logs. Call logs contain data like origin and destination of the call, the time when a call began and finished which shows the length of the call and the specific network that was used during the call among others. Both the call history and mobile device location are used in several ways to solve criminal cases. An example of one of the cases that were solved through the use of call logs and GPS data is the attempted bombing of Times Square in New York in 2010 **(Kylämies, 2019).** Below is an example of a call log made in January 2021.

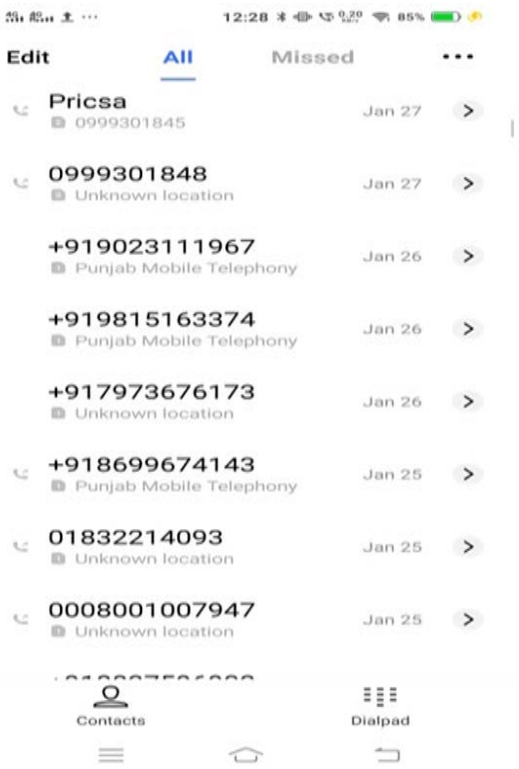

Figure No. 4: Example of the call log

Call logs in essence imply that people communicated by talking to each other. Forensic investigators should acquire the necessary skills to make a voice analysis or audio analysis from mobile calls. This is possible if the voice recorder is turned on during the conversation.

Biometric Data. This is the kind of information that is available in the mobile phone that contains features and characteristics of the user of the mobile phone **(Kylämies, 2019).** In an effort to improve the security features of modern phones like smartphones, the manufacturers introduced the biometric system used to

lock and unlock mobiles. Since innovations are still going on to improve the workability of mobile phones, human features are now being used to secure phones in addition to the usual pin codes or passwords. Smartphones have the capability to identify human features like face, voice and fingerprints **(Bali *et al*., 2019).** Biometric data is therefore used as evidence to track down the author of crime by simply examining the biodata found on the mobile phone used to commit the offence. Biometric data is also used to generate digital identity using an eye or fingerprint scan which is then used to identify specific individuals. Mobile devices are good sources of biological evidence if used in criminal activity. Biological evidence must be collected before examination of the mobile device to avoid contamination unless the collection method will affect negatively the mobile device **(Kylämies, 2019).** It is therefore advisable for forensic examiners to put on protective gear and follow the necessary legal standards required when handling any forensic evidence.

Web Site. This is a form of a web page where data and some pieces of information about a particular subject can be accessed. Mostly, individuals have different preferences about the kind of information that they look for on the internet. Such browsing history can help to figure out the kind of character or behaviour a particular person has. For example, some criminals have a browsing history on the ways how to destroy evidence. This means that there will be multiple web pages all of which will be looking for ways how to destroy evidence. Forensic investigators are therefore supposed to be skilled enough to analyse web browsing history critically. From the past decade, the world has seen a tremendous increase as far as internet usage is concerned. This trend has given an opportunity to a lot of business individuals and organizations to create websites where they could advertise and consequently sell their products and services to all people around the world **(Brügger, 2009).** A lot of fake websites are also created for criminal activities. Internet users should have the capability to differentiate a fake from a legit website by among others authenticating the Uniform Resource Locator (URL). Forensic investigators should be able to identify such websites, identify the owner of those websites and bring them before the law.

Text Messages. It has been discovered that one of the popular ways how written electronic communication is done is by using text messages. Text messaging is done through the normal mode or done through other social media accounts like WhatsApp, messenger etc. more commonly using the mobile phone **(Cain and Gradisar, 2010)**. There are several brands of smartphones nowadays with high performance and huge storage like the Samsung Galaxy series, Apple iPhone and BlackBerry whose functionality can be like that of computers. These types of smartphones can store huge amounts of data in form of text messages. Texting is just one of the simple communication tasks that a mobile device is used for not only in the social setting but also for academic purposes. Most recent mobile phones have the functionality of being user friendly to the extent that even an average person can send and receive texts through them **(Kylämies, 2019).** This is the reason why text messages apart from being cheap and easy to compose can be found and accessed easily on mobile devices. Text messages have proven to be a substantial source of evidence because they can be stored or retrieved and answered at a time that is convenient to the receiver **(Riadi and Firdonsyah, 2018).** This mobile phone service is available to a larger population compared to normal calls since it is accessible to people with vision but who have a hearing impairment.

Emails. This word simply means electronic mail. This is one of the methods that individuals use to exchange digital messages by using electronic devices like computers and mobile phones. Emails are studied under Email forensics which is a sub-branch of digital forensics **(Guo *et al*., 2013).** E-mail forensics refers to the process of identifying and analysing the origin and content of an e-mail used as evidence that might be used to identify the actual sender and recipient of the email. It also deals with the identification of the date and time when the communication was done **(Banday, 2011).**

If an electronic device was used to originate an email containing a ransom note and then deleted, the forensic investigator will be required to use forensic tools like EmailTracer or Encase to recover the deleted data. Emails contain addresses that are used to identify the origin of the mail or the email account. This means that if an email account was involved in criminal activity, then the source of the email will definitely be known because of the email addresses. The email addresses are used to either send or receive email messages over the internet. Email messages are a good source of forensic evidence because they contain information about the sender and the receiver.

Below is an example of an email message:

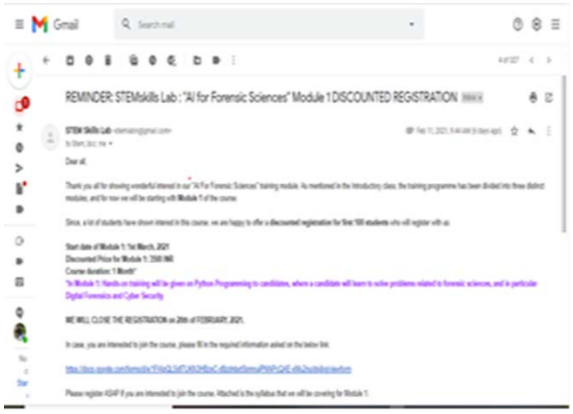

Figure No. 5: Example of a Received Email

Figure No. 6: Examples of forensic digital evidences found in mobile devices

NOTE: The figure above does not in any way highlight the level of importance nor does it highlight the frequency of the most used or found piece of evidence nor the direction for example that serial numbers as evidence come after biometric data. This flow chart is nondirectional which implies that each piece of evidence might be used or accessed at any time depending on the circumstances.

Services Available in Mobile Devices

There are several services that one can access from electronic devices that can be bought from the market today. The diversity in brands, types and models of mobile devices brings the difference in their functionality as well. There are smartphones on the market today like the Research in Motion's (RIM) BlackBerry which is an example of a multimedia phone that allow users to download videos and access several services like television programs. These types of smartphones have the computing capabilities like those that are used to take pictures and shoot and compose videos **(Kroski, 2008).**

Figure No. 7: Services offered by Smartphones

Police and Forensic Scientists in Malawi

The Malawi Police Service is an independent arm of government whose motto is creating a safe and secure Malawi. It is basically one of the law enforcement agencies in Malawi. It is basically mandated to enforce the laws of the land **(Patel and Tostensen, 2006).** It is now divided into six regions which are Northern, Central West, Central East, South West, South East and the Eastern Region. It is further divided into several branches one of which is the Criminal Investigations Department (CID) which was established to deal with all serious crimes **(Makabira and Waiganjo, 2014).** Investigators in this branch are equipped with the necessary skills and knowledge required for them to handle criminal cases. It is their duty to investigate criminal cases through evidence collection and analysis.

The authors of a specific crime are identified if the evidence is procedurally and legally collected and analysed. However, some pieces of evidence are referred to by technical experts for forensic analysis to ensure objectivity in the investigations. For example, dead bodies that need post-mortem examination are referred to government medical doctors who carry out the exercise and offer expert opinions on the possible reason that might lead to loss of life. There is also a Central Government Laboratory located within the

capital city (Lilongwe) where biological evidences are sent for examination. This is done to avoid subjectivity when analysing the evidences because all evidences that are handled without following proper legal standards are rendered inadmissible in court **(Maguire and Epstein, 1927).**

This implies that though the police are able to identify pieces of evidence found at the crime scene they depend upon the forensic experts to examine that piece of evidence and give back the results of the forensic analysis. This shows that there is interdependence between the police and the forensic experts. The Malawi Police Service, though being an independent arm of the government and with a variety of skilled personnel, it cannot work in isolation. It usually depends upon other equally independent arms of the government and even some stakeholders for it to function effectively and efficiently when handling evidence.

When a crime has been committed and officially reported, the police will rely on some members of the general public to furnish it with relevant information about the crime in question. There should be a good working relationship, cooperation and trust between the police and the members of the general public **(Tyler and Huo 2002).** It is through such cordial relationships that the members of the general public are now free to open up and offer nonbogus tips about a crime to the police. Otherwise, it becomes a very difficult task for the police to achieve breakthroughs of some criminal cases if they work in the community without the help of the community members.

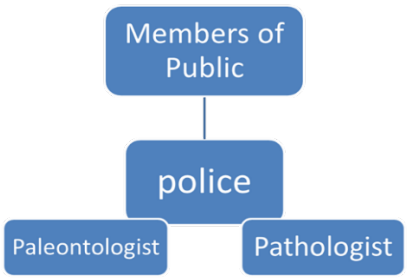

Figure No. 8: Some stakeholders that work collaboratively with the Police

Case Study of Forensic Evidence Found In Mobiles

There are three basic areas where data used as potential evidence is stored in mobile devices like smartphones. A case study titled Smartphone Forensics Analysis found out that data in smartphones is stored in different locations. One of such storage locations available on the smartphone is in sim cards which primarily contains contact information and texts messages. The other storage location is the device memory which stores data voluntarily created by the user of the phone, phone operating system and the settings. The device memory also stores the portable application software like WhatsApp and the appropriate logs that emanates from such social media accounts. There are also portable memory storage devices like Micro SD cards, pen drives etc. that store large amounts of data. The case study discovered that smartphones manufacturers have increased the storage capacity of mobile phones because there is an overreliance on mobile devices nowadays by the general populous **(Al-Hadadi and AlShidhani, 2013).** This means that a lot of data that could be stored in computers is now being stored in mobile phones due to the huge memory and its portability.

Conclusion

We are living in a dynamic world and surrounded by a variety of features and facilities. As it is now, the world over is experiencing the diverse effects of the variance of the coronavirus. A lot of measures have been put in place to help control the spread of this virus. Avoidance of overcrowding has paved the way for individuals to work from home. This has culminated in the extensive use of mobile devices not only to the working class but also to the general populous including criminals. There is over-reliance on the use of electronic devices by both the general public and the criminals. As the use of mobile devices by criminals increases, the possibility of finding substantial evidence in them also increases.

Mobile devices are constantly being used in criminal activities. Some examples of mobile devices are laptop computers, smartphones, PDA, smartwatches, drones and digital cameras. A few examples of criminal activities done using mobile devices are cyberstalking, phishing, spoofing, cyber harassment and child pornography among others. There are several types of evidences but the most common is the direct evidence that comes from an eyewitness, the real evidence which is the object directly connected to the offence i.e. an object used to commit an offence, documentary evidence and circumstantial evidence.

Mobile devices used to commit an offence or several offences are potential sources of substantial evidence like call logs, SMS, Emails and social media accounts. It is the core duty of forensic investigators to see to it that proper legal standards are followed during identification, collection, analysis, storage and presentation of evidence otherwise it becomes inadmissible in court.

References:

Ahmed, Rizwan, et al. "Mobile Forensics: The Study of Collecting Digital Evidence from Mobile Devices." *International Conference on Computer Networks and Security (ICCNS 2008)*, 2008, pp. 246–53.

Aitken, Colin, and Franco Taroni. *Statistics and the Evaluation of Evidence for Forensic Scientists*. Wiley, 1995.

Al-Dhaqm, Arafat, et al. "A Review of Mobile Forensic Investigation Process Models." *IEEE Access*, vol. 8, 2020, pp. 173359–75. *Crossref*, doi:10.1109/access.2020.3014615.

Alghafli, Khawla Abdulla, et al. "Forensics Data Acquisition Methods for Mobile Phones." *2012 7th International Conference for Internet Technology and Secured Transactions (ICITST)*, IEEE, 2012, pp. 265–69.

Al-Hadadi, Mubarak, and Ali AlShidhani. "Smartphone Forensics Analysis: A Case Study." *International Journal of Computer and Electrical Engineering*, 2013, pp. 576–80. *Crossref*, doi:10.7763/ijcee.2013.v5.776.

Al Mutawa, Noora, et al. "Forensic Analysis of Social Networking Applications on Mobile Devices." *Digital Investigation*, vol. 9, 2012, pp. S24–33. *Crossref*, doi:10.1016/j.diin.2012.05.007.

Anghel, Cătălin. "Digital Forensics – A Literature Review." *The Annals of "Dunarea de Jos" University of Galati. Fascicle III, Electrotechnics, Electronics, Automatic Control and Informatics*, vol. 42, no. 1, 2019, pp. 23–27. *Crossref*, doi:10.35219/eeaci.2019.1.05.

Bali, Akanksha, et al. "Biometrics Security in Mobile Application Development & Its Applications." *International Journal of Scientific and Technical Advancements*, vol. 5, no. 1, 2019, pp. 51–60.

Banday, M. Tariq. "Techniques and Tools for Forensic Investigation of E-Mail." *International Journal of Network Security & Its Applications*, vol. 3, no. 6, 2011, pp. 227–41. *Crossref*, doi:10.5121/ijnsa.2011.3617.

Beebe, Nicole Lang, and Jan Guynes Clark. "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process." *Digital Investigation*, vol. 2, no. 2, 2005, pp. 147–67. *Crossref*, doi:10.1016/j.diin.2005.04.002.

Bennett, David. "The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations." *Information Security Journal: A Global Perspective*, vol. 21, no. 3, 2012, pp. 159–68. *Crossref*, doi:10.1080/19393555.2011.654317.

References:

Biggs, Stephen, and Stilianos Vidalis. "Cloud computing: The impact on digital forensic investigations." *2009 International Conference for Internet Technology and Secured Transactions, (ICITST)*. IEEE, 2009.

Bommisetty, Satish, et al. *Practical Mobile Forensics*. Packt Publishing, 2014.

Bouafif, Hana, et al. "Drone Forensics: Challenges and New Insights." *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2018. *Crossref*, doi:10.1109/ntms.2018.8328747.

Bouafif, Hana, et al. "Towards a Better Understanding of Drone Forensics: A case study of parrot AR drone 2.0." *International Journal of Digital Crime and Forensics*, vol. 12, no. 1, 2020, pp. 35–57. *Crossref*, doi:10.4018/ijdcf.2020010103.

Brügger, Niels. "Website History and the Website as an Object of Study." *New Media & Society*, vol. 11, no. 1–2, 2009, pp. 115–32. *Crossref*, doi:10.1177/1461444808099574.

Cain, Neralie, and Michael Gradisar. "Electronic Media Use and Sleep in School-Aged Children and Adolescents: A Review." *Sleep Medicine*, vol. 11, no. 8, 2010, pp. 735–42. *Crossref*, doi:10.1016/j.sleep.2010.02.006.

Carvey, Harlan. *Windows Forensic Analysis DVD Toolkit*. Maarssen, Netherlands, Elsevier Gezondheidszorg, 2018.

Casadei, Fabio, et al. "Forensics and SIM Cards: An Overview." *International Journal of Digital Evidence*, vol. 5, no. 1, 2006.

Casey, Eoghan. *Handbook of Digital Forensics and Investigation*. 1st ed., Academic Press, 2009.

Chávez, Kerry, and Dr. Ori Swed. "Off the Shelf: The Violent Nonstate Actor Drone Threat." *Air and Space Power Journal*, 2020.

Chernyshev, Maxim, et al. "Mobile Forensics: Advances, Challenges, and Research Opportunities." *IEEE Security & Privacy*, vol. 15, no. 6, 2017, pp. 42–51. *Crossref*, doi:10.1109/msp.2017.4251107.

Clarke, Nathan L., and Steven M. Furnell. "Authentication of Users on Mobile Telephones – a Survey of Attitudes and Practices." *Computers & Security*, vol. 24, no. 7, 2005, pp. 519–27. *Crossref*, doi:10.1016/j.cose.2005.08.003.

Daware, Shubhangi, wt al. "Mobile forensics: Overview of digital forensic, computer forensics vs. mobile forensics and tools." *Int. J. Comput. Appl* 2012, 2012, pp. 7-8.

Fukami, Aya, and Kazuhiro Nishimura. "Forensic Analysis of Water Damaged Mobile Devices." *Digital Investigation*, vol. 29, 2019, pp. S71–79. *Crossref*, doi:10.1016/j.diin.2019.04.009.

Garfinkel, Simson L. "Digital Forensics Research: The Next 10 Years." *Digital Investigation*, vol. 7, 2010, pp. S64–73. *Crossref*, doi:10.1016/j.diin.2010.05.009.

References:

Guo, Hong, et al. “Analysis of Email Header for Forensics Purpose.” *2013 International Conference on Communication Systems and Network Technologies*, 2013. *Crossref*, doi:10.1109/csnt.2013.78.

Jain, Anu, and Gurpal Singh Chhabra. “Anti-Forensics Techniques: An Analytical Review.” *2014 Seventh International Conference on Contemporary Computing (IC3)*, 2014. *Crossref*, doi:10.1109/ic3.2014.6897209.

Kennedy, Robert B. “Uniqueness of Bare Feet and Its Use as a Possible Means of Identification.” *Forensic Science International*, vol. 82, no. 1, 1996, pp. 81–87. *Crossref*, doi:10.1016/0379-0738(96)01969-x.

Kroski, Ellyssa. *On the Move with the Mobile Web: Libraries and Mobile Technologies (Library Technology Reports)*. Amer Library Assn, 2008.

Kubi, Appiah Kwame, et al. “Evaluation of Some Tools for Extracting E-Evidence from Mobile Devices.” *2011 5th International Conference on Application of Information and Communication Technologies (AICT)*, 2011. *Crossref*, doi:10.1109/icaict.2011.6110999.

Kumar, Krishan, and Prabhpreet Kaur. “Vulnerability Detection of International MobileEquipment Identity Number of Smartphone AndAutomated Reporting of Changed IMEI Number.” *International Journal of Computer Science and Mobile Computing*, vol. 4, no. 5, 2015, pp. 527–33.

Kylämies, Ville. “Mobiiliforensiikan Nykytilakartoitus.” *Theses and Publications of Polytechnics*, 2019. *Thesis*.

Maguire, John MacArthur, and Charles S. S. Epstein. “Preliminary Questions of Fact in Determining the Admissibility of Evidence.” *Harvard Law Review*, vol. 40, no. 3, 1927, p. 392. *Crossref*, doi:10.2307/1330995.

Makabira, D. K., and Dr. Ester Waiganjo. “Role of Procurement Practices on the Performance of Corporate Organizations in Kenya: A Case Study of Kenya National Police Service.” *International Journal of Academic Research in Business and Social Sciences*, vol. 4, no. 10, 2014. *Crossref*, doi:10.6007/ijarbss/v4-i10/1233.

Muzyleva, Inna, et al. “Practical Aspects of Creating a Teacher’s Information Space.” *2020 V International Conference on Information Technologies in Engineering Education (Inforino)*, 2020. *Crossref*, doi:10.1109/inforino48376.2020.9111850.

Pandey, Pushkal Kumar. *The Law of Evidence: Commentary on Evidence Act, 1872*. OrangeBooks Publication, 2020.

Patel, Nandini, and Arne Tostensen. *Parliamentary-Executive Relations in Malawi 1994–2004*. Chr. Michelsen Institute, 2006.

Pernik, Piret, et al. "National cyber security organisation: United States." *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia*, 2016.

Prakasam, V. "The Indian Evidence Act 1872: a lexicogrammatical study." *J. Gibbons et al.*, 2004.

References:

Riadi, Imam, and Arizona Firdonsyah. "Forensic Analysis of Android-Based Instant Messaging Application." *2018 12th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*, 2018. *Crossref*, doi:10.1109/tssa.2018.8708798.

Sathiyanarayanan, Mithileysh. "Introduction to Digital Forensics." *Academia*, 2016, www.academia.edu/37613861/Introduction_to_Digital_Forensics.

Schachter, Ron. "Mobile Devices in the Classroom." *District Administration*, vol. 45, no. 10, 2009.

Schmersahl, Aaron R. *Fifty Feet above the Wall: Drug Cartel Drones in the U.S. - Mexico Border Zone Airspace, and What to Do About Them*. Naval Postgraduate School, Monterey, United States, 2018.

Song, Helena S. Y., et al. "Mobile devices for learning in Malaysia: Then and Now." *ASCILITE-Australian Society for Computers in Learning in Tertiary Education Annual Conference*. Australasian Society for Computers in Learning in Tertiary Education, 2013.

Srivastava, Himanshu, and Shashikala Tapaswi. "Logical Acquisition and Analysis of Data from Android Mobile Devices." *Information & Computer Security*, vol. 23, no. 5, 2015, pp. 450–75. *Crossref*, doi:10.1108/ics-02-2014-0013.

Strobel, Daehyun. "IMSI catcher." *Chair for Communication Security, Ruhr-Universität Bochum* 14, 2007.

Tajuddin, Taniza Binti, and Azizah Abd Manaf. "Forensic Investigation and Analysis on Digital Evidence Discovery through Physical Acquisition on Smartphone." *2015 World Congress on Internet Security (WorldCIS)*, 2015. *Crossref*, doi:10.1109/worldcis.2015.7359429.

Taylor, Brooke. "Teaching Introductory Forensic Chemistry Using Open Educational and Digital Resources." *Teaching Chemistry with Forensic Science (ACS SYMPOSIUM SERIES)*, American Chemical Society, 2019, pp. 79–91.

Tyler, Tom, and Yuen Huo. *Trust in the Law: Encouraging Public Cooperation with the Police and Courts (Russell Sage Foundation Series on Trust)*. Illustrated, Russell Sage Foundation, 2002.

Yeboah-Boateng, Ezer Osei, and Priscilla Mateko Amanor. "Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices." *Journal of Emerging Trends in Computing and Information Sciences*, vol. 5, no. 4, 2014, pp. 297–307.

Zhang, Huiqi, and Ram Dantu. "Predicting Social Ties in Mobile Phone Networks." *2010 IEEE International Conference on Intelligence and Security Informatics*, 2010. *Crossref*, doi:10.1109/isi.2010.5484780.