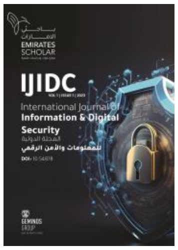


International Journal of Information & Digital Security
Vol 2 Issue 1 (2024)
Pages (17–28)

Available at www.emiratesscholar.com

Forensic Analysis of Health and Fitness Applications on Android

Nasser Jarallah Al-Ghamdi[1], Dr. Mousa Al-Akhras[2], Dr. Fuad Alhosban[3]
nr.ghamdi@me.com[1], mousa.akhras@ju.edu.jo[2], falhosban@hct.ac.ae[3]
SAUDI ELECTRONIC UNIVERSITY, College of Computing & Informatics[1]
Cybersecurity Services, IBM Consulting, Riyadh[1]
The University of Jordan, CIS[2]
Higher Colleges of Technology, CIS[3]

ARTICLE INFO

Published on 30th of December 2024
Doi: 10.54878/6e0nbs05

KEYWORDS

Android Forensics, Health and Fitness Applications, Mobile Forensics, Privacy and Security, Data Extraction

HOW TO CITE

Forensic Analysis of Health and Fitness Applications on Android. (2024). *International Journal of Information & Digital Security*, *2*(1), 17-28.

ABSTRACT

The field of computer forensics focuses on retrieving, analyzing, and presenting computer-based data to be used as evidence in legal proceedings. With the proliferation of digital evidence in civil litigation, legal systems worldwide have adapted to accommodate these new forms of evidence. This research delves into the forensic analysis of health and fitness applications on Android devices, which are now critical targets for forensic investigations due to the sensitive data they store, such as contacts, messages, images, and location information. Given the widespread use of over 250,000 health and fitness applications, there is an urgent need to evaluate their security and privacy measures. The objective of this study is to identify the potential forensic artifacts available within these applications and assess their implications for user privacy and security. By employing rigorous forensic methodologies, we analyze various popular health and fitness apps to understand how securely they store user data and how this data can be extracted and utilized in forensic investigations. Our findings highlight the importance of choosing secure applications that protect user privacy, a crucial consideration for users and developers alike.

1. Introduction

Computers and networks have grown so pervasive in our culture and ingrained in our daily lives that any inquiry or legal issue will almost certainly entail some digital evidence. Computers use in child exploitation, fraud, drug trafficking, terrorism, and homicide. Electronic discovery has grown so prevalent in civil litigation that countries have updated their legal frameworks to include provisions for digital evidence. Investigations into intrusions into business and government information technology systems rely significantly on digital evidence and become increasingly difficult as criminals improve their ability to conceal their tracks (Popescu & Farid, 2004).

According to the website Computer Forensics World, computer forensics is generally defined as applying analytical and investigative procedures to identify, collect, inspect, and preserve evidence/information that is magnetically stored or encoded.

Computer forensics' purpose is to recover, analyze, and present computer-based data in a manner that enables it to use as evidence in a court of law. As with any other forensic science discipline, the emphasis must be on the integrity and protection of evidence in computer forensics. A forensic specialist must follow strict criteria and abstain from shortcuts.

Computer forensics can be applied to any device capable of storing data. This covers network servers, personal PCs, and laptops.

It should emphasize that computer forensics has grown in popularity. Cell phone forensics, router forensics, global positioning system (GPS) device forensics, tablet forensics, and forensics of various other devices are increasingly included in the topic. Digital forensics is a broader phrase that encompasses all of these gadgets. Whichever word is used, the objective is the same: to apply sound scientific procedures to a gadget to obtain evidence for use in a court process.

While the subject of computer forensics and the tools and techniques used are fundamentally different from traditional forensics—such as DNA analysis and bullet examination—the objective is to acquire evidence that can use in a court case. Computer forensics applies to all domains of a typical information technology architecture, ranging from the User Domain and Remote Access Domain to the Wide Area Network (WAN) Domain and Internet Domain (Easttom, 2019).

Digital forensics is the science of gathering, conserving, inspecting, analyzing, and presenting pertinent digital evidence for use in court processes, according to Pollit and Whitledge.

Digital evidence is defined as "any constitution or pertinent digital data sufficient to show a crime in computer and network storage media, including patterns with text, picture, audio, and image." Computer evidence or digital evidence, which is stored on computer and network storage media with electromagnetic means and has the properties of an undifferentiated copy, original authors who are difficult to authenticate, and data verification, is also known as computer evidence or digital evidence. To put it another way, computer storage medium or electromagnetic storage on a network can be utilized as evidence in a criminal investigation (Jasmin & Miroslav, 2010).

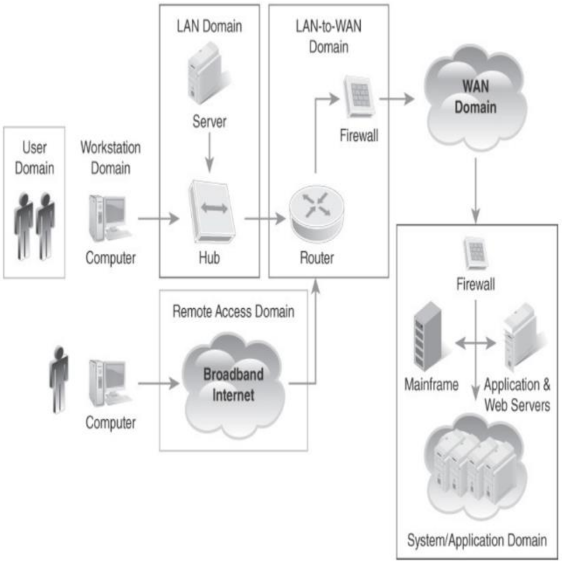


Figure 1: The seven domains of a typical IT infrastructure (Easttom, 2019).

1.1 Mobile Forensics

The term "mobile devices" does not include thumb drives, USB flash drives, memory sticks, or portable externally enclosed hard drives. Cellular (or mobile) phones, Portable Digital/Data Assistants (PDA's), and Smart Phones are all examples of mobile devices. Bear in mind that some earlier PDA models, such as the original Palm and BlackBerry series devices, lack radio (cellular) functionality and are primarily used to store personal information (contacts, calendars, memos, to-do lists) (Hussain et al., 2008).

Representation of Mobile Devices:

- Mobile Phones

- PDAs (Portable Digital/Data Assistants)

- Smart Phones - a mix of the first two, but with radio functionality.

Mobile devices are capable of storing and processing data in various ways. Mobile forensics, also known as device examination, is a challenging area for the legal process to navigate because it encompasses devices such as many brand-model mobile phones, smartphones, and tablets. These devices are available in various models, hardware configurations, memory structures, and operating systems. When each device is reviewed under the light of digital forensics, these structures are deleted from the standard. However, similar to digital forensics, mobile forensics follows the same basic processes as digital forensics, as illustrated in Figure

2.

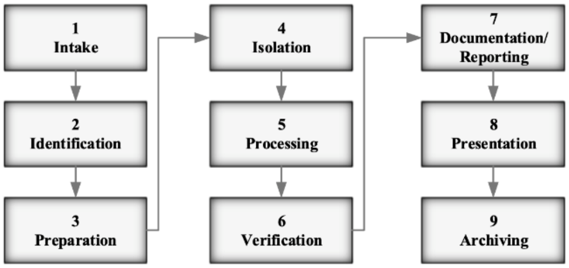


Figure 2: The processes involved in the examination of a mobile phone (Dogan & Akbal, 2017).

A cell phone or tablet might contain a wealth of forensic data is one area of digital forensics that is clearly beyond the boundaries of computer crimes. The evidence discovered on mobile devices can be relevant to any crime. The following items should attempt to recover from a mobile device: The history of calls, emails, texts, and/or other forms of communication Images and video, Contact information, and GPS (global positioning system) data Information about the network (Easttom, 2019).

1.2 Research Gap

Mobile applications are tools that may assist us in making educated health choices. Hundreds of health and wellness applications are accessible in online app stores, and many of us have tried one of them. There are over 250000 health and fitness apps available presently (Tzanou, 2020) ,but how safe are these apps, mainly because they collect sensitive data like the location. Health and fitness apps are becoming more popular due to the added convenience. Smartphones store a vast quantity of sensitive user data, such as contacts, messages, photos, and notes, and are thus regarded as critical targets for investigation. Although there has been much study on safeguarding messenger data, there is not much technical literature on analyzing health and fitness apps.

From the standpoint of digital forensics, there is a need to investigate health and fitness apps, including how secure they are, how to store user-generated information, and how they might assist investigators in using the data in these apps.

2. Literature Review

The presence of an Android forensic framework that covers all phases of the forensic investigation process is necessitated by the continued rapid increase of the Android smartphone market share. Smartphones are becoming comparable to portable PCs. They hold a wide range of information, from personal to professional. Smartphones can give a plethora of evidence to establish or deny incident facts in the event of an occurrence. Evidence must, however, be gathered in such a way that it cannot be contested in a court of law. Mobile forensics is the process of acquiring digital evidence from a mobile phone under forensically sound settings and using well-accepted procedures (Akarawita et al., 2016). Also, more pervasive in our daily lives. Smartphones, on the other hand, have been seen to be increasingly employed in criminal activity (Wu et al., 2018). The judiciary has also recognized this issue. It is becoming increasingly vital to correctly extract information from mobile phones when obtaining evidence. Mobile electronic devices with Android operating systems are valuable sources of data for forensic investigations in the legal process (Guo et al., 2017).

2.1 Process of Digital Forensic Investigation

In the field of digital forensics, there are presently no formal process models that courts may use to establish the credibility of a digital investigation's method. Existing models are frequently built by digital forensic practitioners based on their own experience and an ad-hoc basis, with little regard for the formation of industry standardization. As a result, the establishment of the formal processes that are sorely needed has been hampered. Furthermore, because digital forensic investigators work in various industries such as law enforcement, commerce, and incident response, existing models tend to focus on a single field and fail to account for all possible scenarios (Montasari et al., 2019).

There are four primary phases in this process. The first step in preservation is identifying, recording, and seizing the mobile device. The acquisition of raw data from a mobile device is known as data gathering. The analysis phase is when scientific approaches extract significant digital evidence relevant to the case from raw data. The inspected and analyzed evidence from the previous stage is presented relevantly (Akarawita et al., 2016).

The National Institute of Standards and Technology (NIST) has established a high-level digital forensics procedure that includes the following steps in Figure 4 (Dimitriadis et al., 2020).

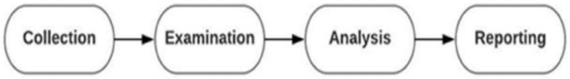


Figure 4: Digital Forensics Process proposed by NIST. (Dimitriadis et al., 2020)

The INTERPOL Innovation Center (IC), on the other hand, has published the Guidelines for Digital Forensics First Responders, which are based on international standards. The Guidelines are based on the Council of Europe's Electronic Evidence Guide, the National Center of Excellence in Cybersecurity in Spain's (INCIBE) Digital Evidence Collection Certificate Manual, and other law enforcement agencies' best practice guides for the seizure and treatment of electronic evidence. The INTERPOL Innovation Centre Digital Forensics Laboratory (ICDFL) also solicited comments from digital forensic professionals from across the world to reach an agreement on some of the hotly discussed or complex issues that digital forensic first responders face (Best Practices for Search and Seizure of Electronic and Digital Evidence GUIDELINES FOR DIGITAL FORENSICS FIRST RESPONDERS, 2021).

They are as follows:

First: The stage of search and seizure preparation phase, including:

(Planning and preparation of equipment), Second: search and seizure execution phase including: (Secure the scene, Assessment, Document the scene, Collection and the handling of digital evidence, Seizure Phase), Third: technical considerations including (The forensic copy, Alternatives to the forensic copy, HASH function), Fourthly: specific procedure including all the details.

2.2 Digital Evidence Integrity

Evidence integrity is an important aspect of forensics since it refers to the requirement that evidence remains intact and not tampered with throughout gathering and processing. The integrity of the data is checked using a hash value checksum. While computer forensics determines the hash value of evidence throughout the acquisition process, mobile forensics does not (Akarawita et al., 2016). For data to be acceptable in a court of law, a forensic expert must be able to demonstrate that it is forensically sound, meaning that it has not been tampered with during the inquiry (Anobah et al., 2014).

2.3 The methods for Data Extraction

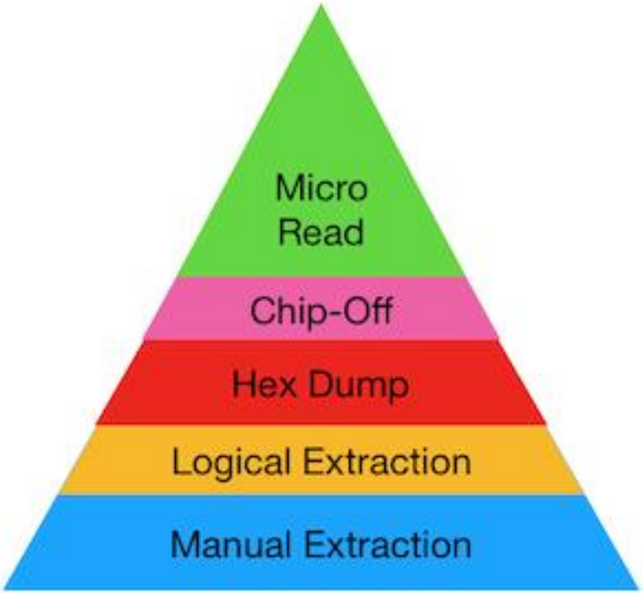


Figure 5: Mobile Device Tool Classification

• Manual Extraction: Viewing the data material saved on a mobile device is a manual extraction approach. To access the contents of the mobile device shown on the LCD screen, human manipulation of the buttons, keyboard, or touchscreen is required. An external digital camera can be used to record the information found. It is difficult to restore erased data at this level. Some technologies have been created to aid forensic examiners in documenting and categorizing the information collected more rapidly. However, if a considerable quantity of data needs to be gathered, a manual extraction might take a long time, and the data on the device may be accidentally changed, erased, or overwritten as a result of the analysis. When dealing with a broken/missing LCD screen or a damaged/missing keyboard interface, manual extractions become progressively difficult, if not impossible. Additional difficulties arise when the gadget is set to show a language that the investigator is unfamiliar with; this might make menu navigating difficult(Ayers et al., 2014).

• Logical Extraction: By accessing the file system, a bit-by-bit copy of specified logical storage is created, and the data stored on the device is extracted. A logical acquisition can reveal the majority of the device's important data, such as SMS, call history, application data, system logs, and media (Boueiz, 2020).

• Hex Dumping: The forensic examiner now has more direct access to the raw data contained in flash memory thanks to extraction technologies (Ayers et al., 2014).

• Chip-off: Chip-off is the process of heating the circuit board of a device until the solder that holds the components to the board melts, then removing the flash memory chip. Commercial instruments can then read the memory chip, yielding a complete physical picture (Skulkin et al., 2018).

• Micro Read: entails using an electron microscope to record the physical observation of the gates on a NAND or NOR device (Ayers et al., 2014).

2.4 Tools and Techniques Used in Mobile Digital Forensics

The availability of forensic software solutions for mobile devices differs significantly from that for PCs. Although personal computers and mobile devices differ in terms of hardware and software, their operation is becoming increasingly comparable (Ayers et al., 2014). To execute a job or task in any profession, the appropriate tools are required. The program is one of the most valuable tools in mobile digital forensics. The program is needed to examine the device and retrieve the information that digital forensic investigators seek (Wilson & Chi, 2018). The software tools are tested on several levels, including basic, sophisticated, and the capacity to deal with unforeseen situations. The differences in behavior between different tools for the scenarios we're testing help us figure out how effective and useful they are (Padmanabhan et al., 2017).

2.5 Challenges of Android Forensics

Mobile device security has been a concern for device makers for some years and will continue to be so as personal privacy becomes more essential to their consumers. Consequently, techniques for safeguarding and/or encrypting data differ significantly from device to device and operating system to operating system. The job of extracting data from unlocked devices is simple. Accessing locked devices, on the other hand, might be difficult. Manufacturers are working on password and encryption systems that will make it very hard for law enforcement to access the information. The difficulties that forensic investigators encounter is growing by the day. Privacy activists are putting increasing pressure on Google to make the Android platform safer by encrypting device data using end-to-end encryption and better encryption methods. Criminals are taking use of these features to securely connect across networks and encrypt their devices. Criminals are becoming more tech-savvy, and they are employing a variety of applications that allow encryption and safe communication. WhatsApp, Facebook Messenger, iMessage, Telegram, Skype, Line, and other mobile messaging apps are quickly becoming the primary form of communication throughout the globe. Instant messaging's (IM) share of worldwide message traffic is expected to rise from 50% to 63 percent in the next several years due to increasing demand. Several websites and services have adopted end-to-end encryption lately as shown in figure 7, rendering them unavailable to law enforcement authorities (Lewis et al., 2017).

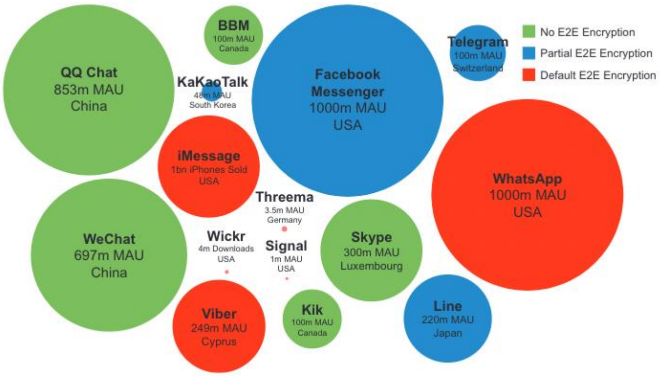


Figure 6: Mobile Messaging Apps Usage (Lewis et al., 2017).

So, the challenge in obtaining this digital evidence has become more necessary and urgent to find ways to help extract evidence in these applications. and the encryption methods utilized by such apps make unlawful activity traces almost untraceable. Despite the difficulties, it is critical to learn what information is saved on the devices that might be harmful if used against people or valuable for criminal investigations (Shortall & Azhar, 2016).

2.6 Forensic Analysis of the Apps on the Android Operating System

Android offers five options for saving data on a device to developers. Data can be found in at least four of the five formats by forensic investigators. As a result, it's critical to comprehend each in depth. Persistent data is saved to the NAND flash memory, the SD card, or the network (Hoog & McCash, 2011). The five approaches are as follows:

1. Shared preferences.
2. Internal storage.
3. External storage.
4. SQLite.
5. Network.

Random Access Memory (RAM) and NAND flash memory are the two primary forms of memory found in Android handsets. To be modified, operations and data must pass via RAM. The RAM is volatile, meaning it will lose its state if it is turned off. It may, however, store sensitive data such as encryption keys, usernames, passwords, and application data. NAND flash memory, on the other hand, is nonvolatile. This implies that the data in the NAND flash is retained even if the device is turned off or restarted. Both system and user data are stored in NAND flash memory. NAND flash is a popular storage media because of its small size, rapid speed, and low power consumption (Al-Saleh & Forihat, 2013).

3. Methodology

Recently, the automation of our daily tasks has increased significantly, even those related to exercise, fitness and health, and with the goals of the Quality of Life Program, one of the programs of the Kingdom's Vision 2030, which are: Promoting sports activities in the community, and with a target to raise the percentage of people practicing sports and physical activities weekly to 40% (Quality of Life - Vision 2030, n.d.). Which makes choosing a secure application that maintains user privacy is one of the essentials at this time.

Our research process is shown in Figure 9. There are four stages in this process. We begin by examining the apps' fundamental technical data, which allows us to categorize them into categories based on their software requirements. The data is then extracted from the application. Then we do a forensic study of the data to see how we may use or profit from it.

Finally, how can this data be recovered if it has been erased or destroyed. Wall these trials and tests will be done on Android (12), for three types of devices (Google Pixel). Try to extract data with and without root and compare the differences between that

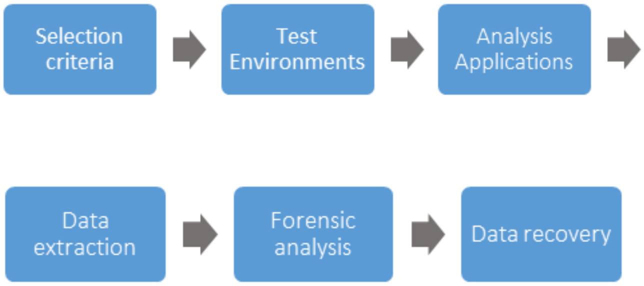


Figure 8: Workflow of the analysis methodology.

3.1 Selection Criteria

We picked Android applications downloaded over 10 million times from the Health & Fitness category on Google Play Store; the apps were chosen based on Google Play results and received a rating of at least 4 out of 5 stars as shown in table 3. In addition, paid applications are not included.

Table 2: Android applications.

Application Name	Ratings	Installs	Version	Offered By
Strava tracker: Record running, cycling & swimming	4.4 745,990 total	50,000,000+	246.11	Strava Inc.
Runkeeper-Distance Run Tracker	4.7 587,902 total	10,000,000+	12.5.2	ASICS Digital, Inc.
Adidas Running - Run tracker	4.5 1,236,451 total	50,000,000+	12.15	Adidas Runtastic
8fit Workouts & Meal Planner	4.4 149,211 total	10,000,000+	22.03.0	Urbanite Inc
Nike Run Club - Running Coach	4.4 1,030,138 total	10,000,000+	4.13.0	Nike, Inc.
MyFitnessPal: Calorie Counter	4.3 2,489,374 total	50,000,000+	22.4.0	MyFitnessPal, Inc.

3.2 Test Environments

Table 3 shows the smartphone model and App versions, whereas Table 4 shows the software that was utilized in the trial.

The applications were downloaded from the google play with the version shown in Table 2 and were not activated with any monthly fees to imitate the general user base

.

Table 3: Hardware for Smartphones and Computers.

Smartphone	Xiaomi Redmi Note 10S Android Device
Android OS version	Android 11 MIUI 12.5
Model Number	M2101K7BG
Phone Storage	64 GB
Access Level	Root
Build Number	SQ1A.220105.002
Kernel Version	14.243-g9e033a27a412-ab7943174
Forensic Computer	kali-linux-2022.2-virtualbox (amd64.ova)
Network Adapter	Atheros Chipset (AR9271)

Table 4: Software Instruments.

Software	Version
Androlyze	v3.2.0.
Android Debug Bridge (ADB)	33.0.1
Root Checker Basic	6.5.0
Wireshark	3.6.3
StegoMagic	1.0
Dex2jar	2.1
JD-GUI	1.6.6
IrfanView 64-bit	4.60

3.3 Analysis Applications

Analyze the health application and discuss results in this field through several methods, namely:

3.3.1 Reverse Engineering

Androguard is a Python-based open-source tool for reverse engineering Android apps. Android application package files (.apk) are sent into Androguard, which separates them for examination. Androguard requires Python version 3.4 or above to be installed on Windows, Linux, and OSX. The Ubuntu Linux distribution was used in this paper

3.3.2 Metadata Analysis

For steganography analysis, StegoMagic and Steghide are used. Images of Stego have been utilized in health applications that enable this data to be shared while ensuring the metadata and content of the data once it has been transferred and uploaded on it.

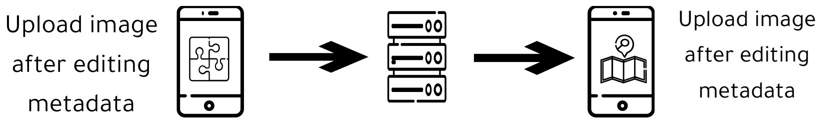

Upload image after editing metadata
Upload image after editing metadata

Figure 9: transferred and uploaded.

3.3.3 Network Traffic Analysis

Using Wireshark to examine all (. pcap) files guarantees that passwords and data are encrypted, preventing data from being readily sniffed across the network.

3.4 Data Extraction

The custom recovery image data extraction technique will be utilized in this section to concentrate on the recovery partition and recovery mode of Android devices. This approach is described by Vidas et al. for getting logical and physical pictures of the device storage. This procedure necessitates the alteration of the recovery partition. However, since most of the relevant data is stored on the "userdata" partition, changing the recovery partition will have no effect.

Upload image after editing metadata

Here's a rundown of how this method of acquisition works.

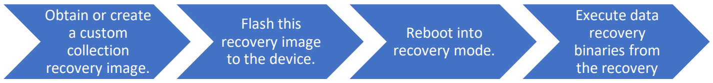
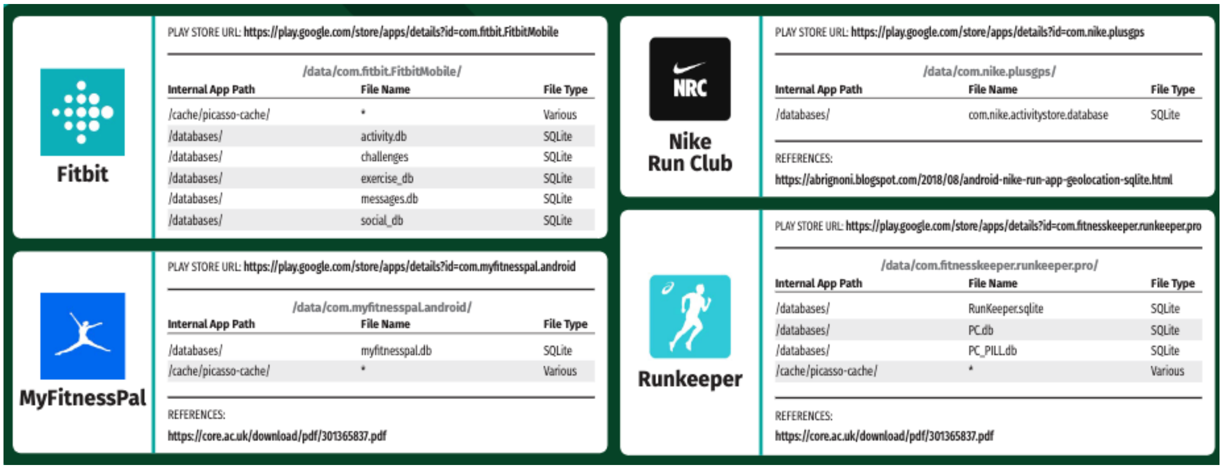

Obtain or create a custom collection recovery image.
Flash this recovery image to the device.
Reboot into recovery mode.
Execute data recovery binaries from the recovery

Figure 10: method of acquisition.

3.5 Forensic Analysis

Based on SANS, a list of the most interesting files and folders has been compiled in the "Data" folder of the third-party apps most frequently used in the health and fitness industry. Which can be reviewed and searched for what it contains in each application.



Fitbit

PLAY STORE URL: https://play.google.com/store/apps/details?id=com.fitbit.FitbitMobile

/data/com.fitbit.FitbitMobile/

Internal App Path	File Name	File Type
/cache/picasso-cache/	*	Various
/databases/	activity.db	SQLite
/databases/	challenges	SQLite
/databases/	exercise_db	SQLite
/databases/	messages.db	SQLite
/databases/	social_db	SQLite

MyFitnessPal

PLAY STORE URL: https://play.google.com/store/apps/details?id=com.myfitnesspal.android

/data/com.myfitnesspal.android/

Internal App Path	File Name	File Type
/databases/	myfitnesspal.db	SQLite
/cache/picasso-cache/	*	Various

REFERENCES:
https://core.ac.uk/download/pdf/301365837.pdf

Nike Run Club

PLAY STORE URL: https://play.google.com/store/apps/details?id=com.nike.plusgps

/data/com.nike.plusgps/

Internal App Path	File Name	File Type
/databases/	com.nike.activitystore.database	SQLite

REFERENCES:
https://abrignoni.blogspot.com/2018/08/android-nike-run-app-geolocation-sqlite.html

Runkeeper

PLAY STORE URL: https://play.google.com/store/apps/details?id=com.fitnesskeeper.runkeeper.pro

/data/com.fitnesskeeper.runkeeper.pro/

Internal App Path	File Name	File Type
/databases/	RunKeeper.sqlite	SQLite
/databases/	PC.db	SQLite
/databases/	PC_PILL.db	SQLite
/cache/picasso-cache/	*	Various

REFERENCES:
https://core.ac.uk/download/pdf/301365837.pdf

Figure 11: Interesting files and folders in health and fitness Apps.

3.6 Data Recovery

Using different forensic tools, such as Access Data FTK and Backtrack dd, in obtaining the physical image of the device and analyzing the utility of each different forensic tool to recover data files from restored Android mobile applications (Ogazi-Onyemaechi et al., 2017).

4 Conclusions

This study reveals significant security vulnerabilities in several popular health and fitness applications on Android devices. Direct communication through shared links is possible on MyFitnessPal, where Stego-embedded images can be posted and shared across various social media platforms. Similarly, Runkeeper allows the uploading of embedded files without any security mechanisms to detect hidden metadata, enabling these files to be shared as links across multiple platforms. The 8fit application, however, does not support the transmission of messages through Stego-embedded images.

The Nike Run Club application lacks a security feature to detect photos with hidden metadata, allowing multiple images to be posted on its feed. Strava also uploads hidden messages within the feed, facilitating the sharing of these embedded images across various social media platforms. Adidas Running permits the uploading of multiple photos in post-exercise activities without a security filter to check for modified metadata, and these posts can be shared across other Strava applications.

Our investigation highlights that once a recipient receives an embedded photo, tools like Steatite can extract the hidden data using a password key. Stegosuite can be used to communicate explicit text messages covertly, demonstrating how easily malicious users can exploit these applications for hidden communication.

In summary, most health and fitness applications analyzed allow photo posting on their feeds, posing a significant risk as malicious users can embed hidden messages within these photos. The current security features in these applications are insufficient to prevent such activities. Future investigations will involve extracting system data from the Redmi Note 10s device with pre-installed Android applications using OSForensic tools to identify questionable content within the application's data folders.

Table 13: Summary Table

Apps name	advantages	disadvantages	Note
Strava tracker: Record running, cycling & swimming	Multiple embedded photos can be shared in the post and across numerous social media platforms.	Dangerous, especially when photos with embedded data are shared	No security feature to filter embedded photos
Runkeeper-Distance Run Tracker	Photo feeds can be shared as links.	Dangerous, especially when photos with embedded data are shared	No security feature to filter embedded photos
Adidas Running - Run tracker	Photos can be uploaded to running activities and d shared across other platforms.	Dangerous, especially when photos with embedded data are shared	No security feature to filter embedded photos
8fit Workouts & Meal Planner	Photos cannot be shared on the app	Feeds cannot be posted	No meals can be posted
Nike Run Club - Running Coach	Photos can be shared on the feed.	Dangerous, especially when photos with embedded data are shared	No security feature to filter embedded photos
MyFitnessPal: Calorie Counter	Photos can be posted either on the feed or shared as a direct message	Dangerous, especially when pictures with embedded data are shared	No security feature to filter embedded photos

5. References

Akarawita, I. U., Perera, A. B., & Atukorale, A. (2016). ANDROPHSY - Forensic framework for Android. 15th International Conference on Advances in ICT for Emerging Regions, ICTer 2015 - Conference Proceedings, 250–258. https://doi.org/10.1109/ICTER.2015.7377696

Al-Saleh, M. I., & Forihat, Y. A. (2013). Skype Forensics in Android Devices. International Journal of Computer Applications, 78(7), 975–8887. www.android.com

Alyahya, T., & Kausar, F. (2017). Snapchat Analysis to Discover Digital Forensic Artifacts on Android Smartphone. Procedia Computer Science, 109, 1035–1040. https://doi.org/10.1016/J.PROCS.2017.05.421

Anobah, M., Saleem, S., & Popov, O. (2014). Testing Framework for Mobile Device Forensics Tools. Journal of Digital Forensics, Security and Law, 9(2), 18. https://doi.org/https://doi.org/10.15394/jdfsl.2014.1183

Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on mobile device forensics. National Institute of Standards and Technology . https://doi.org/10.6028/NIST.SP.800-101R1

Best practices for search and seizure of electronic and digital evidence GUIDELINES FOR DIGITAL FORENSICS FIRST RESPONDERS. (2021).

Boueiz, M. R. (2020). Importance of rooting in an Android data acquisition. 8th International Symposium on Digital Forensics and Security, ISDFS 2020. https://doi.org/10.1109/ISDFS49300.2020.9116445

Chang, M. S., & Yen, C. P. (2019). Forensic Analysis of Social Networks Based on Instagram. International Journal of Network Security, 21(5), 850. https://doi.org/10.6633/IJNS.201909

Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I-Digital forensics framework for reviewing and investigating cyber attacks. https://doi.org/10.1016/j.array.2019.100015

Dogan, S., & Akbal, E. (2017). Analysis of mobile phones in digital forensics. 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2017 - Proceedings, 1241–1244. https://doi.org/10.23919/MIPRO.2017.7973613

Easttom, C. (2019). System Forensics, Investigation, and Response.

Gilbert, A., Seigfried-Spellar, K. C., & Seigfried-Spellar, K. (2022). Forensic Discoverability of iOS Vault Applications. Journal of Digital Forensics, Security and Law, 17(1), 1. https://doi.org/https://doi.org/10.15394/jdfsl.2022.1773

Guo, W., Wu, S., & Wang, D. (2017). A forensics method for android devices based on the technique of temporary root. ICCSE 2017 - 12th International Conference on Computer Science and Education, 502–505. https://doi.org/10.1109/ICCSE.2017.8085543

Hussain, W., Punja, S. G., & Mislan, R. P. (2008). Mobile Device Analysis. SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL, 2(1). http://www.numberingplans.com/?page=analysis

Jasmin Cosic ; Miroslav Baca. (2010, June). Do we have full control over integrity in digital evidence life cycle? | IEEE Conference Publication | IEEE Xplore. Proceedings of the ITI 2010, 32nd International Conference on Information Technology Interfaces. http://0y10egqdk.y.https.ieeexplore.ieee.org.seu.proxy.deepknowledge.io/document/5546413/citations?tabFilter=papers#citations

Lewis, J. A., Zheng, D. E., & Carter, W. A. (2017). The Effect of Encryption on Lawful Access to Communications and Data. www.rowman.com

Montasari, R., Hill, R., Carpenter, V., & Hosseinian-Far, A. (2019). The standardised digital forensic investigation process model (SDFIPM). Advanced Sciences and Technologies for Security Applications, 169–209. https://doi.org/10.1007/978-3-030-11289-9_8

Ogazi-Onyemaechi, B. C., Dehghantanha, A., & Choo, K. K. R. (2017). Performance of Android Forensics Data Recovery Tools. Contemporary Digital Forensic Investigations of Cloud and Mobile Applications, 91–110. https://doi.org/10.1016/B978-0-12-805303-4.00007-1

Padmanabhan, R., Lobo, K., Ghelani, M., Sujan, D., & Shirole, M. (2017). Comparative analysis of commercial and open source mobile device forensic tools. 2016 9th International Conference on Contemporary Computing, IC3 2016. https://doi.org/10.1109/IC3.2016.7880238

Popescu, A. C., & Farid, H. (2004). Statistical Tools for Digital Forensics. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 3200, 128–147. https://doi.org/10.1007/978-3-540-30114-1_10

Quality of Life - Vision 2030. (n.d.). Retrieved March 23, 2022, from https://www.vision2030.gov.sa/v2030/vrps/qol/

Shortall, A., & Azhar, M. A. H. bin. (2016). Forensic Acquisitions of WhatsApp Data on Popular Mobile Platforms. Proceedings - 2015 6th International Conference on Emerging Security Technologies, EST 2015, 13–17. https://doi.org/10.1109/EST.2015.16

Skulkin, Oleg., Tindall, Donnie., & Tamma, Rohit. (2018). Learning Android Forensics Analyze Android Devices with the Latest Forensic Tools and Techniques, 2nd Edition. https://learning.oreilly.com/library/view/learning-android-forensics/9781789131017/

Son, N., Lee, Y., Kim, D., James, J. I., Lee, S., & Lee, K. (2013). A study of user data integrity during acquisition of Android devices. Digital Investigation, 10, S3–S11. https://doi.org/10.1016/J.DIIN.2013.06.001

statcounter. (2022). Mobile Operating System Market Share Worldwide | Statcounter Global Stats. https://gs.statcounter.com/os-market-share/mobile/worldwide

Tzanou, M. (2020). Health data privacy under the GDPR : big data challenges and regulatory responses. https://www.routledge.com/Health-Data-Privacy-under-the-GDPR-Big-Data-Challenges-and-Regulatory-Responses/Tzanou/p/book/9780367077143

Wilson, R., & Chi, H. (2018). A Framework for Validating Aimed Mobile Digital Forensics Evidences. https://doi.org/10.1145/3190645.3190695