Mobile Forensics Solution for Cloud Permission Challenges: Xiaomi Smartphones Case Study

Ammar Yasser Dawabsheh
Arab American University
Faculty of Artificial Intelligence and Data Science
Ramallah, West Bank, Palestine
ammar.nasr@aaup.edu

Majdi Owda
Arab American University
Faculty of Artificial Intelligence and Data Science
UNESCO Chair in Data Science for Sustainable Development
Ramallah, West Bank, Palestine
majdi.owda@aaup.edu

Amani Yousef Owda*
Arab American University
Faculty of Graduate Studies
Department of Natural, Engineering and Technology Sciences
Ramallah, West Bank, Palestine
amani.owda@aaup.edu

Raed Amayra
Security Forces Judicial Commission (SFJC)
raedamayra4@gmail.com

Hasan HajHamad
Palestine Technical University
Tulkarm, Palestine
h.hamad@ptuk.edu.ps

***Abstract*—With the tremendous and rapid advancements in mobile device forensics, traditional forensic methods and tools often become ineffective due to the evolving diversity of devices and their constant internet connectivity. This study addresses the challenge of obtaining application permissions during the acquisition phase, particularly the difficulties in accessing the full contents and databases of applications due to permission restrictions. We highlight several critical aspects, including the challenges faced by law enforcement in using forensic tools on Android systems, and the phases of seizure, acquisition, and data extraction. Additionally, we examine vulnerabilities in current forensic tools when handling Android devices, especially in the context of Xiaomi Cloud. This research presents methods for bypassing application permissions using third-party tools. As a result, we successfully bypassed security settings on Android devices, allowing the acquisition software (XRY) to downgrade applications despite initial restrictions. This demonstrates a practical approach to overcoming forensic limitations.**

***Keywords*—Mobile forensics, Digital forensics tools and Applications, Permission, Cloud forensics, Synchronization.**

I. Introduction

Smartphones offer a wide range of features that traditional phones lack. They enable us to send emails, engage in video calls, use the Global Positioning System (GPS) navigation, and stay connected to the world anywhere, anytime. In criminal investigations, these devices are important sources of evidence[1]. Criminals frequently use their phones to send encrypted communications and are increasingly adept at erasing all traces of their actions. Even if the phones are seized, law enforcement officials will have great difficulty extracting data from them[2]. The challenges that investigating agencies encounter are identified in this experiment, and we will focus on Xiaomi cloud and Android third-party applications for acquisition and permissions for forensics tools[3]. We will concentrate on Android smartphones because they are more popular nowadays. Statista [4] reports that the Android market share is 87%, and IOS with 13% of the global smartphone market. So, there is a good chance that a seized device will be an Android smartphone[5]. According to any forensics tool, it needs to downgrade third-party apps to be able to extract the data from these apps[6]. This study contributes to this field by presenting a practical method for extracting data from some instant messaging applications on the Android operating system platform, despite the need for an Internet connection in some cases and maintaining the digital evidence. The research aims to achieve the following objectives: -

1. Create the application: Install the WhatsApp application on the Xiaomi Note 4 phone to send and receive messages.
2. Prepare the phone for acquisition: Make sure to enable developer mode, prevent the application from accessing the Internet from the settings, and not run in the background.
3. Enable the USB download feature
4. Take over the device: Perform physical acquisition of the mobile phone, to capture a comprehensive snapshot of the device storage, including user-generated content.

978-9950-8599-0-6

5. Recover data from the application: Investigate the feasibility and effectiveness of preventing permissions and not logging out of the application, even if the user has already intentionally logged out remotely.

The rest of the paper is organized as follows: Section 2 describes the results of current relevant studies and background. Section 3 describes the methodology and development for conducting forensic analysis. Section 4 draws the general conclusions of the paper.

II. Background and Related Works

In this section, we talk about an introduction to cloud forensics, a description of mobile forensics, and a summary of the methods and difficulties digital forensic investigators use to obtain data from mobile devices[7].

Digital forensic tools are getting better all the time, and they've even adopted Artificial intelligence (AI) [8][9]. Automation, analysis, and reporting are all common elements of forensic software [10] [11]. Around the world, mobile traffic continues to rise [12]. According to a 2017 research, Americans utilized 15.7 trillion gigabytes (GBs) of smartphone data in 2017, nearly quadrupling since 2014 and roughly 40 times the traffic volume in 2010 [13].

Krishnan et al. [14] highlight the legal problems in getting this data and the cloud provider's involvement, given the multiple apps on a smartphone that each link to the cloud for data storage. With the cost of cloud storage falling, evaluating vast amounts of data from a smartphone requires automation and machine learning. The difficulties in forensic automation are highlighted by James and Gladyshev [15]. North Americans were more concerned with mobile forensics, whereas Europeans were most concerned with cloud forensics, according to a poll conducted by Harichandran et al.[16] in 2016. This might be owing to new privacy rules adopted in 2016, such as the General Data Protection Regulation (GDPR), which are more stringent than those in the United States.

Meanwhile, Irons et al. [17] looked at how to teach competent digital investigators, noting that each sector needs improvement to ensure proficiency. Although forensics toolkits exist for forensic investigators, Umale et al. [18] argued that the majority of them do not provide full capabilities for numerous devices. The National Institute of Standards and Technology (NIST) and the Scientific Group on Digital Evidence (SWGDE) take a deep dive into the mobile forensics process, describing the benefits and problems that these devices provide to law enforcement [19]. The Digital Forensics process consists of four fundamental steps illustrated in Figure 1 [20] [21].

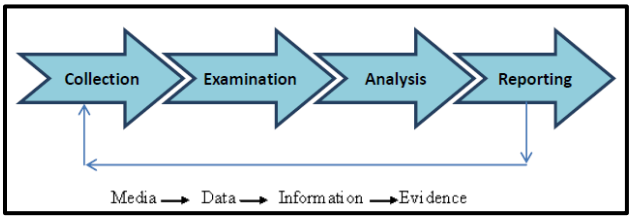

Figure 1: Digital Forensics Process

III. Methodology

In this paper, we will present a special model in order to bypass the installation via USB option with an Internet connection and preserve all data and sessions of applications without making any data traffic to the applications. The main problem with Android phones is that when trying to acquire the phone, the option to install via USB should be enabled, and many phones refuse to activate this option unless the phone is connected to Xiaomi Cloud and connected to the Internet. Here lies the main danger, as when connecting the phone to the Internet, we may lose many application databases, and some applications may even lose current sessions and log out. The explanatory report of the Cybercrime Convention indicated that law enforcement agencies are allowed to obtain and preserve any electronic evidence[22], [24], [25].

In this section, we will deal with a Xiaomi phone to explain the Case Study to deal with files related to the cloud and how acquisition works for these files. XRY software will be used to complete the extraction, clarify the challenges we encountered in this experiment, and suggest solutions to successfully bypass these challenges.

Standard acquisition steps can apply to all Android smartphones, especially Xiaomi phones[24], [25]. Figure 1 shows the proposed flow chart that we will work with. We will deal with an unlocked Xiaomi phone. Figure 2 shows the general proposed model road map used for Android mobile devices that we used in our experiment in two stages. The first one is without enabling developer mode, and the second one is with developer mode enabled.

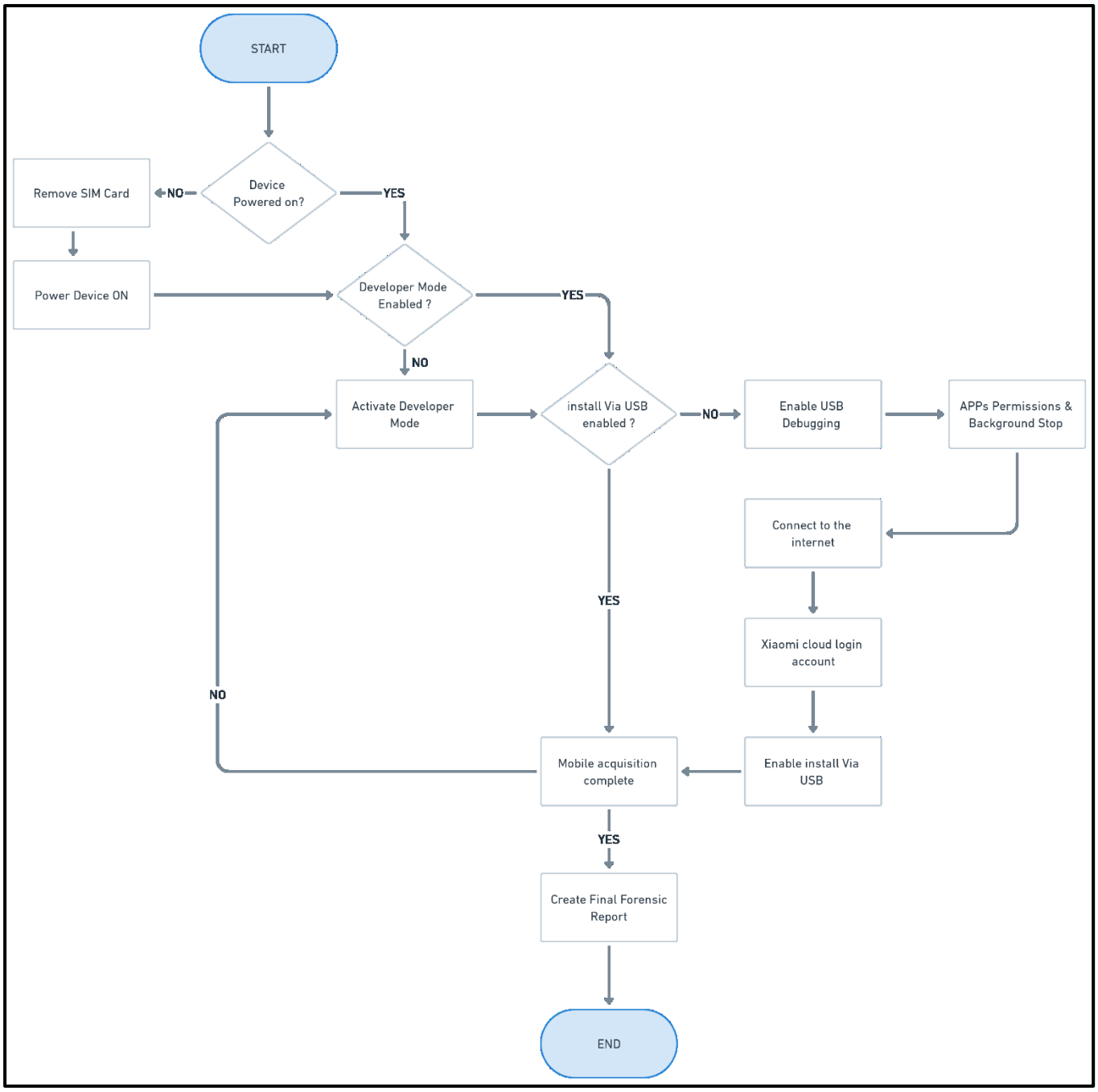

Figure 2: Mobile acquisition proposed model flow chart

Downgrade applications will be selected for a downgrade stage to extract data and media, such as Facebook and WhatsApp Apps. The next step will be illustrated in Figure 3:

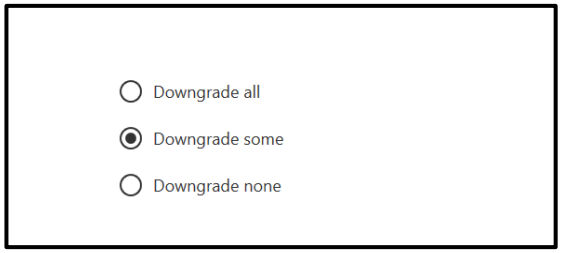

Figure 3: Downgrade some Applications

Through this option in XRY software, we can choose some applications to make the tool extract their contents and all related to these applications. We can, for example, choose the information and data related to the WhatsApp application and not extract and downgrade for the rest of the applications. At this stage, we will choose some applications and try to downgrade them and note the performance and the results after making this choice. And what data will be extracted from the tool in the normal procedure without making the proposed flow chart and without changing the cloud and the application permission settings.

Index	Module	Status	Time	Message
129	ANDROID	Unsuccess	4/24/2021 15:06	An error occurred while trying to downgrade application Facebook Messenger (com.facebook.orca)
130	ANDROID	Success	4/24/2021 15:06	Installing older version of application Snapchat (com.snapchat.android)
131	ANDROID	Unsuccess	4/24/2021 15:06	ADB install response: Failure [INSTALL_FAILED_USER_RESTRICTED: Install canceled by user]
132	ANDROID	Unsuccess	4/24/2021 15:06	An error occurred while trying to downgrade application Snapchat (com.snapchat.android)
133	ANDROID	Success	4/24/2021 15:06	Installing older version of application WhatsApp (com.whatsapp)
134	ANDROID	Unsuccess	4/24/2021 15:06	ADB install response: Failure [INSTALL_FAILED_USER_RESTRICTED: Install canceled by user]
135	ANDROID	Unsuccess	4/24/2021 15:06	An error occurred while trying to downgrade application WhatsApp (com.whatsapp)
136	ANDROID	Success	4/24/2021 15:06	Installing older version of application TikTok - Make Your Day (com.zhiliaoapp.musically)
137	ANDROID	Unsuccess	4/24/2021 15:06	ADB install response: Failure [INSTALL_FAILED_USER_RESTRICTED: Install canceled by user]

Figure 4: failed downgrade log

Although the USB debugging in developer options has been enabled for the phone, as shown in Figure 5, the XRY software was unable to downgrade the applications, and the attempt to downgrade these applications failed. Although the developer options have been enabled, as shown in the Figure. 4. The logs for the software show that an error occurred while trying to downgrade applications linked with the date, time, and status for the message.

The main challenge with this experiment is that the install via USB option is disabled, and this option must be enabled so that any software can downgrade applications and extract data and information related to these applications. The investigators can only activate this option by connecting the devices to the Internet. This step has great risk for the investigators and the acceptance of evidence in the courts[26]. Some evidence may be lost from the device if it is connected to the Internet because the suspect may have logged out of all applications remotely[26].

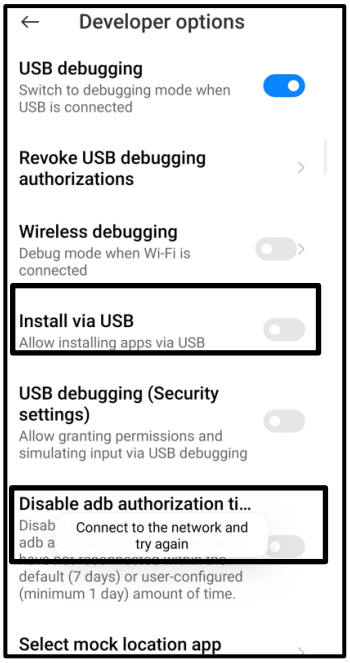

Figure 5: Install via USB error

IV. Implementation, Results, and Discussion:

As we mentioned earlier, we cannot activate the installation via the USB option until the device is connected to the Internet and as shown in Figure 4. We will now apply our proposed model, and this will be done through these steps:

1- Enabling install via USB option:
Before enabling this option, we need to stop any traffic between the device applications and the Internet. By manually editing the permissions for all applications on the device. For example, we find a lot of permissions for WhatsApp, and one of these permissions is the network connection, WIFI connection, and disconnect from WIFI. So, we need to stop all these permissions, as shown in Figure 5.

2- Disabling all permissions:
Figure 6 shows how the permission settings should be, with disabling all permissions, especially WIFI connections and the application background running. We can repeat this step for all applications that have online sessions.

3- Cloud synchronization:
After turning off all these permissions, we must also make sure that the sync through Google and Xiaomi accounts is turned off.

4- Xiaomi account:
It is necessary for the success of this proposed model. The Xiaomi account should link to the device. Even if we need to create a new account and link it to the phone temporarily. This is an important step to enabling installation via the USB option, as shown in Figure 7.

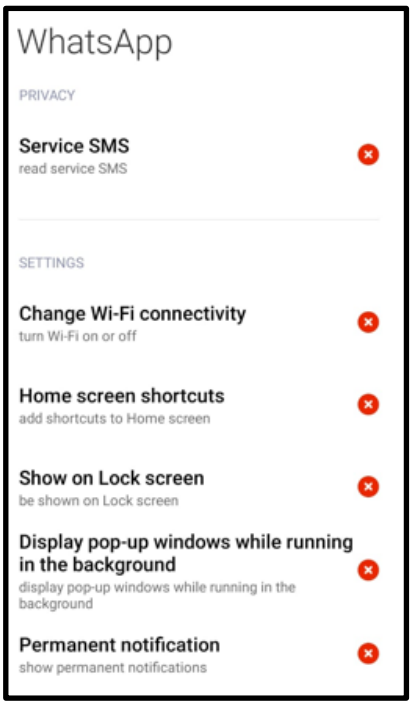

Figure 6: modified permission settings

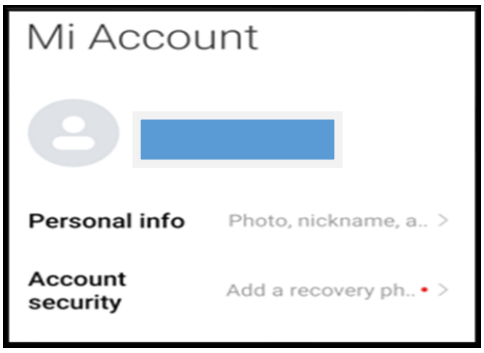

Figure 7: Mi account

5- Install via USB, enabling:

Finally, after making all the previous steps and repeating them for all applications in the phone that use the Internet and prevent them from working in the background, we can now connect the phone to the Internet and activate the option to **install via USB** and try to make a new acquisition of the phone again.

The acquisition was completed successfully at all levels, after making the previous steps also succeeded in maintaining the downgrade of the applications, as shown in the event logs for the program in Figure 8:

Success	Downgrading application Facebook (com.facebook.katana)
Success	Uninstalling current version of application Facebook (com.facebook.katana)
Success	Downgrading application Facebook Messenger (com.facebook.orca)
Success	Uninstalling current version of application Facebook Messenger (com.facebook.orca)
Success	Downgrading application Snapchat (com.snapchat.android)
Success	Uninstalling current version of application Snapchat (com.snapchat.android)
Success	Downgrading application TikTok - Make Your Day (com.zhiliaoapp.musically)
Success	Uninstalling current version of application TikTok - Make Your Day (com.zhiliaoapp.musically)
Success	Downgrading application WhatsApp (com.whatsapp)
Success	Uninstalling current version of application WhatsApp (com.whatsapp)
Success	Restarting device.
Success	Successfully reconnected to device.
Success	Installing older version of application Facebook (com.facebook.katana)
Success	Application Facebook (com.facebook.katana) downgraded successfully!
Success	Installing older version of application WhatsApp (com.whatsapp)
Success	Application WhatsApp (com.whatsapp) downgraded successfully!
Success	Installing older version of application Facebook Messenger (com.facebook.orca)
Success	Application Facebook Messenger (com.facebook.orca) downgraded successfully!
Success	Installing older version of application Snapchat (com.snapchat.android)
Success	Application Snapchat (com.snapchat.android) downgraded successfully!
Success	Installing older version of application TikTok - Make Your Day (com.zhiliaoapp.musically)
Success	Application TikTok - Make Your Day (com.zhiliaoapp.musically) downgraded successfully!
Success	Backup: All apps
Success	Backup: Include key/value backup apps

Figure 8: Success downgrade logs

V. Conclusion and Future Work

Through this research, we successfully achieved the desired objective of bypassing security settings on Android phones. We enabled the acquisition software (XRY) to downgrade applications on these devices, while the security settings prevented us from performing this step. In future work, we aim to explore alternative methods for bypassing security settings without connecting the phone to the internet by Dumping the full image of an Android phone.

References

[1] S. Alqahtany, N. Clarke, S. Furnell, and C. Reich, "Cloud Forensics: A Review of Challenges, Solutions and Open Problems," in *2015 International Conference on Cloud Computing, ICCC 2015*, Institute of Electrical and Electronics Engineers Inc., Jul. 2015. doi: 10.1109/CLOUDCOMP.2015.7149635.

[2] P. Gladyshev, A. Marrington, and I. Baggili, Eds., *Digital Forensics and Cyber Crime*, vol. 132. in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 132. Cham: Springer International Publishing, 2014. doi: 10.1007/978-3-319-14289-0.

[3] S. Sachdeva, B. L. Raina, and A. Sharma, "Analysis of Digital Forensic Tools," *J Comput Theor Nanosci*, vol. 17, no. 6, pp. 2459–2467, Sep. 2020, doi: 10.1166/jctn.2020.8916.

[4] statista, “Share of global smartphone shipments by operating system,” 2019. Accessed: Apr. 28, 2022. [Online]. Available: https://www.statista.com/statistics/272307/market-share-forecast-for-smartphone-operating-systems/#:~:text=Smartphones running the Android operating,percent share of the market.

[5] A. A. Sheikh, P. T. Ganai, N. A. Malik, and K. A. Dar, “Smartphone: Android Vs IOS,” *The SIJ Transactions on Computer Science Engineering & its Applications (CSEA)*, vol. 01, no. 04, pp. 31–38, Oct. 2013, doi: 10.9756/sijcsea/v1i4/0104600401.

[6] C. Anglano, “Forensic analysis of whats app messenger on Android smartphones,” *Digit Investig*, vol. 11, no. 3, pp. 201–213, Sep. 2014, doi: 10.1016/j.diin.2014.04.003.

[7] K. Hoover, “Digital Forensics,” in *Global Crime: An Encyclopedia of Cyber Theft, Weapons Sales, and Other Illegal Activities: Volume 1: AL: Volume 2: MZ*, vol. 1–2, Bloomsbury Publishing Plc., 2019, pp. 164–167. doi: 10.4018/ijoci.2020040103.

[8] K. Salih and N. Dabagh, “Digital Forensic Tools: A Literature Review,” *Journal of Education and Science*, vol. 32, no. 1, pp. 109–124, Mar. 2023, doi: 10.33899/edusj.2023.137420.1304.

[9] D. Dunsin, “The Use of Artificial Intelligence in Digital Forensics and Incident Response (DFIR) in a Constrained Environment,” 2022. [Online]. Available: https://www.researchgate.net/publication/361241108

[10] K. Ghazinour, D. M. Vakharia, K. C. Kannaji, and R. Satyakumar, “A study on digital forensic tools,” in *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, ICPCSI 2017*, Institute of Electrical and Electronics Engineers Inc., Jun. 2018, pp. 3136–3142. doi: 10.1109/ICPCSI.2017.8392304.

[11] Q. Do, B. Martini, and K. K. R. Choo, “A forensically sound adversary model for mobile devices,” *PLoS One*, vol. 10, no. 9, Sep. 2015, doi: 10.1371/journal.pone.0138449.

[12] M. Amine Chelihi, A. Elutilo, I. Ahmed, and C. Papadopoulos, “An Android Cloud Storage Apps Forensic Taxonomy.”

[13] T. Ctia, “Background on CTIA ’ s Semi-Annual Wireless Industry Survey ANNUALIZED WIRELESS INDUSTRY SURVEY RESULTS,” no. January 1985, 2004.

[14] C. L. Krishnan S., *Legal Concerns and Challenges in Cloud Computing*. 2014. doi: 10.48550/arXiv.1905.10868.

[15] S. Miura and N. Yamamoto, “Figitumumab,” *Biotherapy*, vol. 25, no. 2, pp. 649–656, 2011, doi: 10.32388/jdexl5.

[16] V. S. Harichandran, F. Breitinger, I. Baggili, and A. Marrington, “A cyber forensics needs analysis survey: Revisiting the domain’s needs a decade later,” *Comput Secur*, vol. 57, no. March, pp. 1–13, 2016, doi: 10.1016/j.cose.2015.10.007.

[17] A. D. Irons, P. Stephens, and R. I. Ferguson, “Digital Investigation as a distinct discipline: A pedagogic perspective,” *Digit Investig*, vol. 6, no. 1–2, pp. 82–90, 2009, doi: 10.1016/j.diin.2009.05.002.

[18] T. M. D. Umale M., Deshmukh A. B., *Mobile phone forensics challenges and tools classification: A review”*. 2014.

[19] R. Ayers, W. Jansen, and S. Brothers, “Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1),” *NIST Special Publication*, vol. 1, no. 1, p. 85, 2014.

[20] P. Sharma, D. Arora, and T. Sakthivel, “Mobile cloud forensic readiness process model for cloud-based mobile applications,” *International Journal of Digital Crime and Forensics*, vol. 12, no. 3, pp. 58–76, Jul. 2020, doi: 10.4018/IJDCF.2020070105.

[21] K. Kent, S. Chevalier, T. Grance, and H. Dang, “Guide to Integrating Forensic Techniques into Incident Response,” *The National Institute of Standards and Technology*, 2006.

[22] N. F. Hassan and H. M. Jaber, “Offline vs. Online Digital Forensics of Cloud-based Services,” *Journal of Al-Nahrain University of Science*, vol. 20, no. 4, pp. 117–124, Dec. 2017, doi: 10.22401/JNUS.20.4.18.

[23] H. M. Al-Khateeb and P. Cobley, “How you can preserve digital evidence and why it is important?” 2015.

[24] F. M. Granja and G. D. R. Rafael, “The preservation of digital evidence and its admissibility in the court,” *International Journal of Electronic Security and Digital Forensics*, vol. 9, no. 1, pp. 1–18, 2017, doi: 10.1504/IJESDF.2017.081749.

[25] A. E. Franț, “Forensic challenges regarding the Internet of Things,” *SHS Web of Conferences*, vol. 177, p. 03002, 2023, doi: 10.1051/shsconf/202317703002.