Investigation of Concealed Data Applications on Android Smartphones: A Forensic Perspective

Sunil Kumar Yadav[1], Saniya Ahamad Patel[2], Preet Kumar[3], Rajeev Kumar[4], Deepika Bhandari[5*]

[1]Department of Forensic Science, Galgotias University, Uttar Pradesh, 203201

[2]Department of Forensic Science, Galgotias University, Uttar Pradesh, 203201

[4] Head, Department of Forensic Science, Galgotias University, Uttar Pradesh, 203201

[3]Department of Forensic Chemistry and Toxicology, Institute of Forensic Science, Mumbai-400032

[5]Head, Department of Forensic Science, Institute of Forensic Science, Mumbai-400032

***Corresponding Author**- Dr. Deepika Bhandari, Head, Department of Forensic Science, Institute of Forensic Science, Mumbai-400032

ABSTRACT

In the realm of cybercrime, mobile devices often harbor crucial information, yet their data recovery poses significant challenges when they are locked or employ specialized concealment applications. The adoption of techniques to identify these tools or apps for uncovering and extracting concealed data can significantly enhance the efficacy of mobile forensic applications. This paper provides a concise summary of recent research endeavors in this domain, offering a critical review of these studies while exploring the methodologies employed for the retrieval of covert data on Android smartphones.

Keywords- Android Forensics, Data Recovery, Mobile Forensics, Hidden Data, Cybercrime

INTRODUCTION

Mobile forensics constitutes a specialized branch of digital forensics, focused on the retrieval of digital evidence from mobile devices, adhering to forensically sound procedures. The evolution in technology has reshaped the landscape of crime, as well as its resolution methods. The widespread adoption of smartphones, the internet, and smart gadgets in daily life has transformed them into vital repositories of information. Globally, the demand for smartphones reached a staggering 432 million units in the final quarter of the year, as reported by Gartner. Highly interconnected smartphones have become commonplace, often facilitated by a plethora of applications that users can readily access from app stores. However, this ubiquity of smartphone applications has raised significant concerns regarding security and privacy. Smartphones, in essence, serve as essential communication hubs, housing an extensive repository of personal data. In many instances, mobile devices contain more revealing information per unit of storage than traditional computers [1]. To address this, a technique for concealing information on smartphones has been developed, enabling detection applications to encrypt and embed sensitive data or identification codes within other data streams on a mobile device. Information hiding techniques encompass a range of methodologies utilized to securely embed data within a host media, such as images, with minimal degradation to the host, and providing means for subsequent extraction of the concealed data [2]. Notably, mobile vault applications support the secure storage of personal data, mitigating the risk of data leakage in the event of device loss or theft. When users input the correct password or passphrase, hidden data becomes accessible. Various vault applications are readily available on platforms like the Google Play Store, with some having amassed over a hundred million downloads [2]. In the context of legal investigations involving seized smartphones, standard forensic analysis tools and techniques suffice for data examination. However, complications arise when data, including video and audio files, images, documents, or applications, are secured with data protection measures such as passwords. These security applications, designed to safeguard files and documents within mobile devices, are commonly referred to as Data Security or Hiding Applications. When files are locked or password-protected, they remain concealed during visual inspections of the smartphone. Information hiding techniques encompass a range of methodologies utilized to securely embed data within a host media, such as images, with minimal degradation to the host, and providing means for subsequent extraction of the concealed data [2,3]. One notable security technique in this domain is steganography, where confidential data is covertly embedded within a cover medium. Phrases like distortion-free, reversible, lossless, or erasable watermarking are often used interchangeably with reversible watermarking in this context.

Bridging the Gap and Current Scenario

It's fair to say that a significant proportion of contemporary crimes involve the direct or indirect use of smartphones. Regardless of the nature of the offense, these devices have become pivotal sources of information due to their role in storing and transmitting data. In the early days of mobile phones, call detail records (CDRs) were the primary information considered in crime-solving [3]. However, in today's landscape, smartphones contain a wealth of data, including internet browsing history, location data, social media activity, emails, documents, multimedia files, and more. Smartphones play a direct role in both digital and conventional crimes, often serving as crucial pieces of evidence. Moreover, they can indirectly provide insights into a person's activities, whereabouts, contacts, interests, and even psychological profiles based on their app usage and internet content access [4]. Although these fragments of information may not directly prove criminality, they can offer valuable context about an individual, whether they are a victim or a suspect.

During the third quarter of 2019, RSA recorded a global total of 55,484 fraudulent activities. Among these, phishing attacks accounted for 23,800 cases, constituting 43 per cent of all identified fraud attacks and marking a 6 per cent rise from the previous quarter. Additionally, social media saw a surge in fraud and brand abuse attacks, comprising 17 per cent of all fraud incidents during Q3. This represents a substantial 75 per cent increase compared to the same period in the previous year [5]. This underscores the growing targeting of mobile phones for criminal activities, indicating a likely increase in such crimes soon.

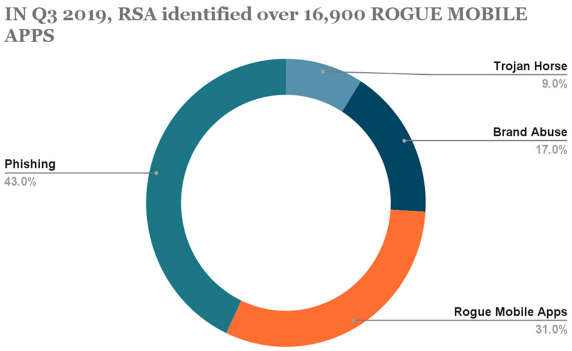

Fig. 1: Mobile Apps Contribution in Fraud as per the RSA Quarterly Fraud Report Volume 2, Issue 3, Q3 2019

Privacy and anti-forensic measures have become increasingly important as crimes evolve and investigative techniques become more sophisticated. Criminals and regular users alike employ techniques to maintain anonymity and remove traces of their activities, such as clearing logs and history. While these methods are used in anti-forensic activities, everyday users also employ them to safeguard their privacy. For instance, many users utilize incognito or private browsing modes to prevent tracking, even though their intentions are not malicious. Erasing browsing history after web access is also a common practice among end-users, often motivated by a desire for privacy. The ethical and legal implications of such tools and techniques are often debated, exemplified by cases like Apple vs. FBI, where smartphone encryption posed challenges for law enforcement. Encryption is just one facet of privacy-related tools and technologies; others can similarly be employed to protect privacy but may also be exploited by criminals to conceal their identities [6].

One common scenario involves a forensic investigator acquiring a smartphone from a crime scene only to find it equipped with a document locker app, restricting access to media files and selecting social networking apps. In such cases, investigators must devise strategies to overcome these obstacles and extract as much information as possible from the device. As Android currently dominates nearly 85% of the smartphone market, the following section delves into critical characteristics of these content-hiding Android applications, aiming to aid forensic investigators in understanding how these applications operate and ensure user privacy [7].

Various Methodologies for the Investigation of Concealed Data Applications on Android Smartphones are provided in Table 1 below.

Table 1: Various Software and Methods adopted by different researchers and experts to recover the forensically valuable data on various devices

Researcher And Year	**Mobile Phones Used**	**Data Security Applications**	**Software/Tools Used**	**Data Types**	
				Before Recovery	**After Recovery**
Sai *et al.* (2015)		Image Steganography, Text Steganography, Video Steganography, Audio	Embedding Algorithm, Extraction Algorithm	1 –Image, 2 – Audio 3 – Video 4 – Text 5 - Network	1 –Image, 2 –Audio 3 – Video 4 – Text 5 - Network

		Steganography, Network Steganography			
Sgaras *et al.* (2015)		WhatsApp, Skype,Viber, Tango	Cellebrite UFED Physical Analyzer (targeted data)	1 -Image, 2 – Audio 3 – Video 4 – Doc File 5 – Im Chats , 6- Sms,	1 - Sms, 2- Emails, 3 - Im Chats
			2 - Logical extraction (targeted data)	1 -Image, 2 – Audio 3 – Video 4 – Doc File 5 – Im Chats , 6- Sms,	1-Image, 2-Audio 3-Video Files
Manjula *et al.* (2015)		1-Image Steganography, 2-Information security, 3-LSB 4-Spatial domain	1-Algorithm of Encoding. 2-Algorithm of Decoding Algorithm HASH BASED	1-Image	1-Image
Hu *et al.* (2015)		1-Prediction-error expansion, 2-reversible data hiding, 3-minimum rate prediction, optimized 4- Histogram modification. 5-PEE based reversible data hiding	1-OHM-Single 2-OHM-Stitched 3-PEE algorithms 4-OHM extracting	1-Images, 2- Text File	1-Images, 2- Text File

Qian *et al.* (2015)		1-Reversible data hiding, 2-image encryption	1-embedding key 2-Comparison with VRAE Method	1-Images , 2- Audios	1-Images, 2- Audios
Riaz (2016)	1 – Qmobile Noir A9 Korean based, 2 - Samsung S II HD LTE SHV-E120L , 3- Google Nexus, 4 Samsung Galaxy Ace HTC Wildfire	1.App Lock 2.App Lock bolo 3. Safe Gallery 4.Gallery Lock	1.Access Data FTK Imager 2.Quick Hash V1.5.5 3.Access Data FTK 4.0.2.2 4.Cellebrite UFED Touch 5.Cellebrite UFED Classic 6.MSAB XRY Forensics	1.Images 2.Audios 3.Videos 4.Zip Files 5.Doc Files	1.Images 2.Audios 3.Videos 4.Zip Files 5.Doc Files
Kapre *et al.* (2016)	1-Windows Phone, 2 Android, 3- iPhone 4-Blackberry, 5-Symbian, 6-Chinese		1-Manual extraction,	1- Image, 2 – Audio 3 – Video 4 – Doc file 5 – Chats , 6- Hidden file 7 – Hide password , 8 – Zip file	Not found any data in manual extraction

	phones , 7-CDMA phones				
			2 – Logical extraction	1 -Image, 2– Audio 3 – Video 4 – Doc File 5 – Chats , 6- Hidden file 7 – Hide password 8 – Zip file	1-Image, 2- Audio 3 – Video 4 – Doc File 5 – Chats
			3 - Physical Analysis	1 -Image, 2– Audio, 3 – Video, 4 – Doc file, 5 – Chats , 6- Hidden file, 7 – Hide password , 8 – Zip file	1 -Image, 2 Audio 3 – Video 4 – Doc File 5 – Chats , 6- Hidden File 7– Hide Password ,
			4- Chip off (Damage device)	1 -Image, 2 – Audio 3– Video 4– Doc File 5– Chats , 6- Hidden File 7– Hide Password , 8– Zip File	1 -Image, 2– Audio 3 – Video 4 – Doc File 5 – Chats , 6- Hidden File 7– Hide Password , 8 – Zip File

	Android v4.4,5.0 Android v5.0.1 Android v4.4.2, Froyover 2.2, GingerBread v2.3.x, IceCream Sandwich v4.0.x	1.Instagram, 2. LINE, 3. Whisper, 4. WeChat, and 5. Wickr	Tools based approach namely, 1.Magnet 2.AXIOM, 3.XRY, and 4.Autopsy	Images Videos Artifacts Messages Contacts Documents	Android images and videos not fully detected, No artifacts Found

DISCUSSION

Mobile forensic investigations may encounter the risk of evidence data contamination, either during data collection or when storing and transporting the evidence. Mobile forensic investigators mu be vigilant about potential sources of evidence of data contamination, such as active connections to the Internet and telecommunications networks, the presence of Android malware, and electromagnetic interference from nearby devices in possession of the mobile device containing the evidence data [18].

Forensic analysts must adhere to specific procedures when taking possession of a smartphone to preserve the data stored on the seized device. Consequently, they need to determine whether the phone is powered on. If the device is turned off, it becomes important to assess the possibility of extracting data from its memory card [19]. Notably, some Android smartphones feature an internal memory card that cannot be accessed using a standard USB card reader for file copying. However, if it is feasible to remove and duplicate the memory card for safety reasons, this should be executed using an analyst's memory card, similar to the approach employed with pen drives. Subsequently, to prevent any potential data alterations or leaks, the mobile device should be placed in flight mode, thereby disconnecting it from Internet and Telecommunication networks [19, 20, 21].

A substantial portion of the evidence related to mobile devices resides in volatile memory. Gathering transient data poses a significant challenge due to the ever-changing state of the system and memory content. If the mobile device faces a low battery situation, it is at risk of losing valuable details [22]. In such circumstances, it becomes imperative to maintain sufficient power, either by using a power adapter or replacing the batteries as needed [22]. If adequate power cannot be ensured, it is advisable to power off the mobile device to conserve battery life and safeguard memory contents. This phase also warrants a thorough check for the presence of any user-installed malicious software [23].

To guarantee the preservation and integrity of electronically collected evidence, it is essential to adhere to and meticulously document correct protocols [24]. When shipping, it is critical to accurately identify and label all potential sources of evidence. Utilizing standard plastic bags can generate static electricity, underscoring the significance of employing anti-static evidence packaging [25,26,27]. Furthermore, the evidence must be securely stored in an area that shields it from electromagnetic radiation, dust, excessive heat, and humidity. Access to the storage area should be strictly restricted to authorized personnel.

CONCLUSION

The comprehensive examination of recent research in the field of mobile forensics underscores the substantial need for further investigation into the extraction of concealed data on smartphones. The review proposes various methodologies for retrieving such data, including brute force attacks, dictionary attacks, swap attacks, rainbow attacks, and the endorsement of specific software tools by various researchers. These software tools include Cellebrite UFED 4 PC, Cellebrite UFED Physical Analyzer, Access Data FTK Imager, MSAB XRY Forensics, Cellebrite UFED Touch, among others. However, it is noted that the methods described may not be entirely effective for the latest versions of Android smartphones. Notably, MSAB XRY is considered the most effective tool for hidden data recovery but has limited functionality in comparison to open access tools.

REFERENCES

1. D. M. Sai, N. R. G. K. Prasad, & S. Dekka, "The forensic process analysis of mobile devices," *Int. J. Comput. Sci. Inf. Technol.*, vol. 6, no. 5, pp. 4847-4850, 2015.
2. H. Gawali, & R. C. Samant, "Review of Reversible Data Hiding Techniques," *International Research Journal of Engineering and Technology*, 2015.
3. H. Riaz, "Recovering data from password protected data security applications in android based smartphones," *Sciences*, vol. 1658, pp. 6794, 2016.
4. X. Zhang, I. Baggili, & F. Breitinger, "Breaking into the vault: Privacy, security and forensic analysis of Android vault applications," *Computers & Security*, vol. 70, pp. 516-531, 2017.
5. N. A. Azeez, B. B. Salaudeen, S. Misra, R. Damaševičius, & R. Maskeliūnas, "Identifying phishing attacks in communication networks using URL consistency features," *International Journal of Electronic Security and Digital Forensics*, vol. 12, no. 2, pp. 200-213, 2020.

6. P. Rughani, "Forensic analysis of content hiding android applications," *Int. J. Adv. Res. Comput. Sci. Software Eng.*, vol. 7, 2017.
7. Statista Research Department, "Market share of mobile operating systems worldwide 2009-2023," *Statista*, 31-Aug-2023. [Online]. Available: https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/
8. J. Kaur, & E. V. Kaur, "A Review on reversible Data hiding Technique," *International Journal of Computer Science and Mobile Computing*, vol. 4, no. 7, pp. 334-340, 2015.
9. H. Alatawi, K. Alenazi, S. Alshehri, S. Alshamakhi, M. Mustafa, & A. Aljaedi, "Mobile forensics: A review," in *2020 International Conference on Computing and Information Technology (ICCIT-1441)*, IEEE, 2020, pp. 1-6.
10. C. Tassone, B. Martini, K. K. R. Choo, & J. Slay, "Mobile device forensics: A snapshot," *Trends and Issues in Crime and Criminal Justice*, no. 460, pp. 1-7, 2013.
11. J. Lessard, & G. Kessler, "Android forensics: Simplifying cell phone examinations," 2010.
12. Y. T. Chang, K. C. Teng, Y. C. Tso, & S. J. Wang, "Jailbroken iPhone forensics for the investigations and controversy to digital evidence," *Journal of Computers*, vol. 26, no. 2, pp. 19-33, 2015.
13. Y. Chen et al., "Demystifying hidden privacy settings in mobile apps," in *2019 IEEE Symposium on Security and Privacy (SP)*, IEEE, 2019, pp. 570-586.
14. X. Pan, X. Wang, Y. Duan, X. Wang, & H. Yin, "Dark Hazard: Learning-based, Large-Scale Discovery of Hidden Sensitive Operations in Android Apps," in *NDSS*, Feb. 2017.

15. E. W. Ngai, Y. Hu, Y. H. Wong, Y. Chen, & X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," *Decision Support Systems*, vol. 50, no. 3, pp. 559-569, 2011.
16. X. Sun et al., "Demystifying hidden sensitive operations in android apps," *ACM Transactions on Software Engineering and Methodology*, vol. 32, no. 2, pp. 1-30, 2023.
17. K. Deshpande, & N. Kamble, "Application of Data Hiding in Audio-Video Using Advance Algorithm," 2016.
18. N. P. Yadav, & R. C. Shivamurthy, "Faamac: Forensic Analysis of Android Mobile Applications using Cloud Computing," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 2, no. 5, pp. 1069-1073, 2013.
19. X. Hu, W. Zhang, X. Li, & N. Yu, "Minimum rate prediction and optimized histograms modification for reversible data hiding," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 653-664, 2015.
20. L. Xue, X. Luo, L. Yu, S. Wang, & D. Wu, "Adaptive Unpacking of Android Apps," in *2017 IEEE/ACM 39th International Conference on Software Engineering (ICSE)*, Buenos Aires, Argentina, 2017, pp. 358-369, doi: 10.1109/ICSE.2017.40.
21. X. Zhang, I. Baggili, & F. Breitinger, "Breaking into the vault: Privacy, security and forensic analysis of Android vault applications," *Computers & Security*, vol. 70, pp. 516-531, 2017.
22. C. Sgaras, M. T. Kechadi, & N. A. Le-Khac, "Forensics acquisition and analysis of instant messaging and VoIP applications," in *Computational Forensics: 5th International Workshop, IWCF 2012, Tsukuba, Japan, November 11, 2012 and 6th International*

Workshop, IWCF 2014, Stockholm, Sweden, August 24, 2014, Revised Selected Papers, Springer International Publishing, pp. 188-199, 2015.

23. J. Grover, "Android forensics: Automated data collection and reporting from a mobile device," *Digital Investigation*, vol. 10, pp. S12-S20, 2013.
24. N. Al Barghouthy, A. Marrington, & I. Baggili, "The forensic investigation of android private browsing sessions using orweb," in *2013 5th International Conference on Computer Science and Information Technology*, IEEE, 2013, pp. 33-37.
25. R. Sinha, V. Sihag, G. Choudhary, M. Vardhan, & P. Singh, "Forensic analysis of fitness applications on android," in *International Symposium on Mobile Internet Security*, Singapore: Springer Nature Singapore, 2021, pp. 222-235.
26. N. Amer, & Y. S. Al-Halabi, "Android forensics tools and security mechanism: survey paper," in *Proceedings of the Fourth International Conference on Engineering & MIS 2018*, June 2018, pp. 1-6.
27. H. A. Ghannam, "Forensic Analysis of Artifacts of Giant Instant Messaging “WhatsApp” in Android Smartphone," *Journal of Applied Information, Communication and Technology*, vol. 5, no. 2, pp. 63-72, 2018.