iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52201

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Harvesting Cloud Credentials in iOS and Android Devices: An Investigative Resource

Ashmit Sharma[1], Rajat Choudhary[2]
[1]*Lead Forensic Analyst, Sardar Vallabhbhai Patel National Police Academy, Ministry of Home Affairs, Govt. Of India*
[2]*Scientist B, Documents, Central Forensic Science Laboratory, Bhopal*

Abstract: ***The innovative advancement in digital data storage has facilitated the storage of important files and documents on cloud storage, where the digital data is stored in logical pools. The widespread use of mobile and cloud technologies in our daily lives has led to a significant increase in the amount of sensitive data stored on these platforms, owing to their user-friendliness and secure storage capabilities. The flexibility of cloud storage for accessing any files anywhere and with the limited storage capacity of mobile devices, users are increasingly relying on cloud storage to store their data. Therefore, data extraction from mobile devices and cloud storage has become a critical area of research in the field of digital forensics. This study presents, step-by-step guide that helps Digital Forensic Investigators (DFIs) to acquire saved cloud credentials on iOS and Android mobile phones. Such credentials lead to successful cloud data extraction of relevant digital evidence in an ethical and forensically sound manner. The study emphasizing the need for continuous research in the field of mobile and cloud forensics to tackle the latest threats and vulnerabilities in these domains.***

Keywords: Credentials, Cloud, Extraction, Investigator, Cloud Forensics, Cloud Data Analysis

I. INTRODUCTION

The fields of cloud forensics and mobile forensics are closely interconnected within the realm of digital forensics. With the wide-ranging adoption of mobile and cloud technologies, individuals frequently utilize their mobile devices to access and store sensitive information on cloud platforms. Hence, examining cloud data may be crucial in the forensic investigation of a mobile device, and vice versa [4]. Mobile forensics involves the preservation, analysis, and retrieval of digital evidence from mobile devices, such as smartphones and tablets. On the other hand, cloud forensics deals with the examination of data stored on cloud platforms, such as Google Drive, Dropbox, and iCloud. The relationship between these two areas of digital forensics emerges from the common use of cloud storage by individuals to save and share files, including photos, videos, and other sensitive data. In many instances, the mobile device is utilized to manage and access cloud data, rendering it a crucial piece of evidence in an investigation. Mobile forensics presents challenges such as device encryption, data fragmentation, and third-party applications storing data on the cloud. Traditional methods, such as physical extractions, may not be effective in recovering data, and cloud forensics techniques may be necessary to access and analyze cloud data. Various cloud forensics tools [2], such as [10] UFED Cloud Analyzer, Magnet AXIOM Cloud, and Elcomsoft Cloud eXplorer, have been developed to overcome the challenges of cloud technologies, but proper protocols and procedures must be followed to ensure the admissibility and legality of collected evidence [9].

II. CLOUD CREDENTIALS ON IOS DEVICES

The iOS is a mobile operating system created by Apple Inc. for its mobile devices like the iPhone, iPad, and iPod Touch. It was first released in 2007 and has since undergone several updates, with iOS 16 serving as the most recent iteration as of 2022. By restricting access to underlying hardware and software and enabling automatic encryption of stored data, iOS' closed system architecture is intended to create a safe and reliable environment. [6] Digital forensics investigators always struggle to retrieve digital evidence, particularly from iOS devices, which necessitates keeping up with the most recent tools and methods. The study presents a unique iOS device vulnerability that, if the pin or password is known, may be used to get access to a sizable number of credentials that have been saved locally. The study offers two approaches for gaining access to credentials and passwords kept on an iOS device.

1) *Method 1:* Navigate to the "Settings" app on the iOS device and select the "Passwords" option. This can be done by tapping on the "Settings" icon on the home screen and then scrolling down to find the "Passwords" option. Once selected, the device will prompt for the device's passcode, and after providing it, the user can view all the saved passwords and credentials associated with the device. (Figure-I)

©IJRASET: All Rights are Reserved

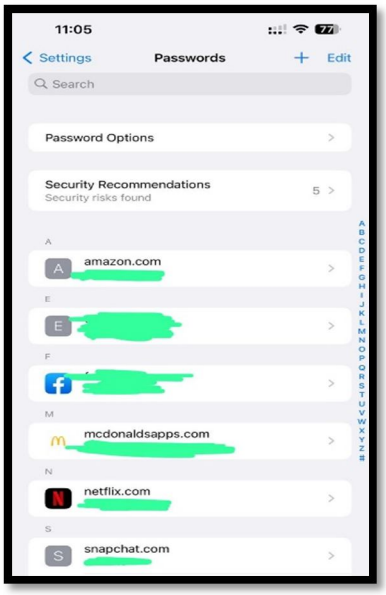


Figure-I

2) *Method 2:* Access saved passwords through Google Chrome if it has been installed on the iOS device. If the user has saved their passwords in Chrome, they can be accessed by navigating to the "Settings" option within Chrome and selecting "Password Manager". Once prompted for authentication, the user can view all the saved passwords and credentials associated with the Chrome browser. (Figure-II)

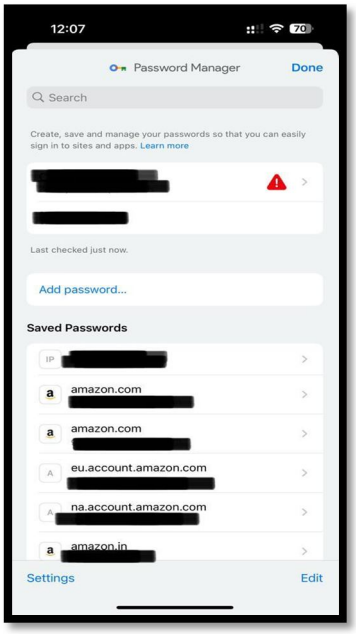


Figure- II

DFIs who need to extract data from iOS devices may encounter difficulties due to the closed system architecture of iOS. Apple's security features make it difficult to perform a physical extraction of the device, and logical extraction may also be limited by encryption and other protections. DFIs employ specialized tools and methods to retrieve data from iOS devices in order to overcome these difficulties. These programs are made to go over Apple's security measures and get the most info out of the gadget. Jailbreaking the device to access the file system and utilizing specialized software to extract data from backup files kept on the device or in the cloud are common methods utilized.

©IJRASET: All Rights are Reserved

A. The Case Study

DFIs examined a challenging case where a deleted photo on an Apple iPhone 13 Pro Max (A4284) could not be recovered using traditional methods [1]. The phone had File Base Encryption, which made physical extraction impossible, and the extracted logical dump did not recover the image [7]. The examiner found Google credentials on the mobile phone, leading to the use of Cellebrite UFED Cloud Analyzer, which enabled access to the Google Photos data stored in the cloud, resulting in the recovery of the required photo for forensic analysis. This case emphasizes the importance of exploring alternative methods and tools to extract critical evidence, especially when traditional methods fail. It also highlights the significance [3] of continuous research and development to keep pace with evolving technologies in digital forensics. As the use of mobile devices and cloud technologies continues to grow, new challenges and opportunities will arise for digital forensic investigators.[5]

III. CLOUD CREDENTIALS ON ANDROID

Android is an open-source operating system used in various mobile devices, including smartphones and tablets, and has dominated the mobile operating system market with over 80% share worldwide. Developed by Google in 2008, it has undergone numerous updates and enhancements, [1] with the latest version being Android 13 released in 2022. Unlike iOS devices, Android devices offer greater flexibility and customization options, enabling users to modify system settings and install third-party apps. The study explores a specific vulnerability in Android devices, which involves accessing saved passwords and credentials if the Pin/Password is known, without internet connection, during forensic investigations. The method for accessing saved passwords is through the Google Chrome browser if it has been installed on the Android device. If the user has saved their passwords in Chrome, they can be accessed by opening the Chrome app, selecting the "More" option (usually represented by three dots in the upper-right corner), and selecting "Settings." Within the settings, the user can select "Password Manager" to view all of the saved passwords and credentials associated with the Chrome browser. (Figure-III)

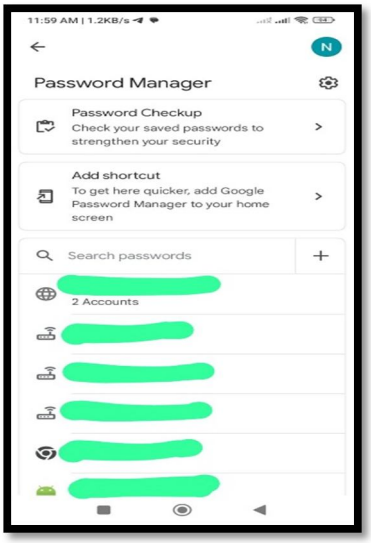


Figure-III

To maintain the admissibility of the data in court, it is crucial to ensure that forensic examiners access saved passwords and credentials on an Android device using specialized tools and techniques in a forensically sound manner. This involves documenting the entire process to ensure its validity. [8]

IV. CONCLUSION AND DISCUSSIONS

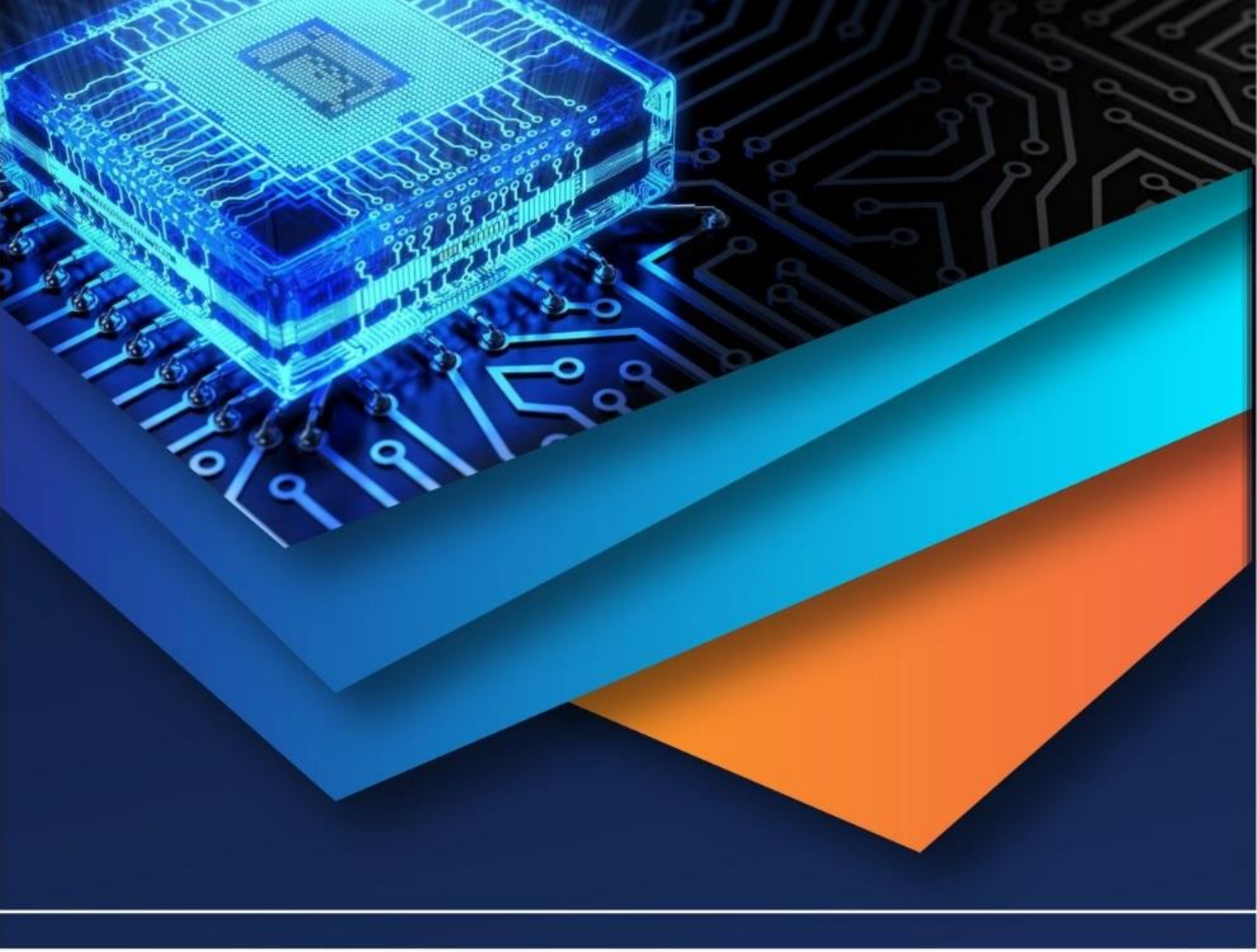
The study underscores the significance of exploring alternative methods and tools to retrieve crucial evidence when conventional techniques fail. It presents a case where a researcher faced challenges in recovering deleted photos from an encrypted iPhone 13 Pro Max. Despite unsuccessful attempts to recover the photos through conventional methods, the researcher discovered Google credentials stored on the device, which led to the utilization of a cloud forensics tool resulting in the recovery of the photo. DFIs face new challenges and opportunities with the widespread use of mobile devices and cloud technologies.

Mobile forensics has become critical due to the increasing amount of sensitive data stored on mobile platforms, while cloud forensics is necessary because of the popularity of cloud technologies for data storage and accessibility. Even with various encryption methods, modern iOS and Android devices still have vulnerabilities that allow access to critical cloud credentials. Therefore, cloud forensics is essential for extracting valuable data from cloud services that may not be available through traditional mobile device forensics. As a result, mobile and cloud forensics are becoming increasingly important in the digital age and can help provide essential insights into criminal activities and bring perpetrators to justice.

REFERENCES

[1] Almutairi, A., & Pattinson, C. (2021). A review of mobile device forensic acquisition tools. Journal of Forensic Sciences, 66(1), 247-259.
[2] Alazab, M., Venkatraman, S., & Alashoor, T. (2019). Digital forensics in the cloud: Review and research directions. Journal of Network and Computer Applications, 133, 67-84.
[3] Alshammari, R., & Pattinson, C. (2019). The challenges and implications of cloud forensics. Digital Investigation, 28, 1-10.
[4] Akinyemi, B., Abade, T. O., & Sanyaolu, A. (2020). A review of mobile device forensics tools and techniques. International Journal of Advanced Trends in Computer Science and Engineering, 9(1), 350-357.
[5] Alharbi, A., & Pattinson, C. (2020). Mobile device forensic tools: A comparative analysis. Digital Investigation, 32, 101-114.
[6] Gouglidis, A., & Parkin, S. (2018). Cloud forensics: A survey and research challenges. ACM Computing Surveys, 51(5), 92.
[7] Alazab, M., Venkatraman, S., & Alashoor, T. (2019). Digital forensics in the cloud: Review and research directions. Journal of Network and Computer Applications, 133, 67-84.
[8] Zhang, Q., Huang, S., & Li, J. (2019). A survey on mobile device forensics: Challenges and future research directions. IEEE Access, 7, 40186-40196.
[9] Patil, P. G., & Singh, A. K. (2020). Cloud forensics: Current trends and future directions. International Journal of Computer Science and Mobile Computing, 9(8), 46-55.
[10] Anandarajan, M., & Bodorik, P. (2019). Mobile forensics: A review. Journal of Organizational and End User Computing (JOEUC), 31(2), 60-78.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)