Investigation of Cloud-Based Mobile Applications Within the Scope of Online Data Acquisition Method

Mustafa GÜNGÖR

Turkish Gendarmerie Forensic Department

Türkiye Gendarmerie Forensic Department

The Digital Forensics Research Conference (DFRWS EU 2024) 19-22 March 2024 Zaragoza / SPAIN

Abstract

Cloud computing has an important place in modern technology solutions but the issues such as security, privacy, performance, cost management and lack of resources raise some concerns about cloud computing. While cloud computing brings great convenience to our business and private lives with its dynamic structure, it is seen that the same dynamic structure reflects negatively on the field of digital forensic and brings along some difficulties. The problem is that traditional forensic methods cannot be implemented in the cloud. In this context, the aim of the research is to review the effectiveness of new methods and tools used in the cloud and to determine to what extent the data in the cloud can be accessed by using forensic tools. In this context, images of mobile phones with iOS and Android operating systems were acquired in different situations. Various reviews were made on the social media applications Instagram and Facebook. By using Oxygen Forensic Detective software, it was tested whether it is possible to access user credentials and data in the cloud and whether the obtained data complies with forensic standards. It was concluded that both offline and online data acquisition tools should be used together in order to obtain the best results enabling access to more concrete digital data in mobile cloud forensics.

Introduction

We use cloud computing systems widely in all areas of our lives. The widespread use of cloud computing technologies and usage areas has made the cloud environment suitable for cybercrime and conventional crimes. It is important to quickly collect the necessary data from the relevant cloud system in order to detect criminal elements and forensic analysis of cloud-based mobile applications. It is still unclear how to obtain data from social media applications and cloud storage environments that contain very valuable data about users. Data access requests from international service providers are managed through mutual legal assistance processes. However, this process is often an obstacle to the investigation in terms of cost and time. Cloud-based forensic tools are relatively new compared to traditional forensic tools and continue to evolve day by day. Since cloud computing technologies have begun to be used extensively by criminals and criminal organizations, there is a need for studies on cloud computing in terms of digital forensics.

Research Aim and Objectives

The main objective of the research is to examine the effect of cloud computing on digital forensic investigations. Sub-objective of the research is to review the effectiveness of new methods and tools used in the cloud environment.

- Do authentication tokens and access to usernames and passwords differ on mobile devices based on copying methods?
- To what extent can the data in the cloud be accessed using forensic tools?
- Is data integrity ensured?

Methodology

The model used in the research is a one-group post-test design model from quasi-experimental research designs. In order to access the data in the cloud, authentication tokens and user names and passwords obtained as a result of image acquisition are used.

The mobile phones used in the research were first upgraded to the latest software version they supported and returned to factory settings, the social media applications examined within the research were installed, a data set was created to be used in the applications, and the analysis phase was started by applying user behaviors step by step (Table 1-3).

Table 1. Versions of devices and software used

Device / Application / Forensic Software Name	Version Used in Research
iPhone	iPhone SE A2296 (iOS 16.3.1)
iPhone	iPhone 6s Plus A1687 (iOS 15.7.3)
Samsung	Samsung Galaxy S7 SM-G930F (Android 8.0.0)
Huawei	Huawei P40 ANA-NX9 (Android 10.0.0)
Instagram	275.1 (iPhone 6s Plus ve iPhone SE) 275.0.0.27.98 (Samsung Galaxy S7 ve Huawei P40)
Facebook	407.1 (iPhone 6s Plus ve iPhone SE) 407.0.0.30.97 (Samsung Galaxy S7 ve Huawei P40)
Oxygen Forensic® Detective	15.3.1.145
Cellebrite UFED 4PC	7.57.0.13
HashMyFiles	v2.31

Table 2. Details of the transactions performed

Application	Application Behaviors	User Behaviors
Instagram / Facebook	Account creation	Creating an account in the application.
	Sign in	Login to account.
	Profiling	Adding profile photo and biography.
	Adding a contact	Adding a following/follower.
	Photo and video sharing	Sharing photos and videos, liking, commenting and tagging.
	Creating a story	Creating a story with photos and videos.
	Reels video sharing	Shooting and sharing reels video.
	Live broadcast	Broadcasting live through the application.
	Chat	Send/receive text messages, photos and videos.

Table 3. Copy types

Mobile Phone	Copy Type	Software
Apple iPhone SE A2296	iTunes backup	Oxygen Forensic® Detective
iPhone 6s Plus A1687	iOS checkm8	Oxygen Forensic® Detective
Samsung Galaxy S7 SM-G930F	Decrypted Boot Loader	Cellebrite UFED 4PC
Huawei P40 ANA-NX9	Kirin Live	Cellebrite UFED 4PC

Results

In this context, it has been observed that Instagram data can be accessed in cases where the password is saved on iPhone SE A2296 and iPhone 6s Plus A1687. On the Samsung Galaxy S7 SM-G930F and Huawei P40 ANA-NX9, the authentication token / username and password that will allow access to the application data could not be detected (Table 4).

Regarding the Facebook; it has been observed that application data can be accessed on iPhone SE A2296 and iPhone 6s Plus A1687 when the password is saved. In addition, access was also achieved when the password was not saved but the user logged in. On the Samsung Galaxy S7 SM-G930F and Huawei P40 ANA-NX9, the authentication token / username and password could not be detected (Table 5).

As a result of the hash comparison, it was seen that *the hash values of the data uploaded from Instagram and Facebook* <u>*changed*</u> compared to the original data.

Table 4. Data acquired from Instagram

		iPhone SE A2296 (iOS 16.3.1)				iPhone 6s Plus A1687 (iOS 15.7.3)				Samsung Galaxy S7 SM-G930F (Android 8.0.0)		Huawei P40 ANA-NX9 (Android 10.0.0)	
		Password are saved		Password are not saved		Password are saved		Password are not saved					
		Logged in	Logged out	Logged in	Logged out	Logged in	Logged out	Logged in	Logged out	Logged in	Logged out	Logged in	Logged out
Instagram	Account info	✓	✓	X	X	✓	✓	X	X	X	X	X	X
	Profile photo	✓	✓	X	X	✓	✓	X	X	X	X	X	X
	Biography	✓	✓	X	X	✓	✓	X	X	X	X	X	X
	Following / Followers	✓	✓	X	X	✓	✓	X	X	X	X	X	X
	Sharing	✓	✓	X	X	✓	✓	X	X	X	X	X	X
	Likes, Comments and Tagging	✓	✓	X	X	✓	✓	X	X	X	X	X	X
	Story	✓	✓	X	X	✓	✓	X	X	X	X	X	X
	Reels video sharing	✓	✓	X	X	✓	✓	X	X	X	X	X	X
	Live broadcast	✓	✓	X	X	✓	✓	X	X	X	X	X	X
	Chats	✓	✓	X	X	✓	✓	X	X	X	X	X	X

Table 5. Data acquired from Facebook

		iPhone SE A2296 (iOS 16.3.1)				iPhone 6s Plus A1687 (iOS 15.7.3)				Samsung Galaxy S7 SM-G930F (Android 8.0.0)		Huawei P40 ANA-NX9 (Android 10.0.0)	
		Password are saved		Password are not saved		Password are saved		Password are not saved					
		Logged in	Logged out	Logged in	Logged out	Logged in	Logged out	Logged in	Logged out	Logged in	Logged out	Logged in	Logged out
Facebook	Account info	✓	✓	✓	X	✓	✓	✓	X	X	X	X	X
	Profile photo	✓	✓	✓	X	✓	✓	✓	X	X	X	X	X
	Biography	✓	✓	✓	X	✓	✓	✓	X	X	X	X	X
	Following / Followers	✓	✓	✓	X	✓	✓	✓	X	X	X	X	X
	Sharing	✓	✓	✓	X	✓	✓	✓	X	X	X	X	X
	Likes, Comments and Tagging	✓	✓	✓	X	✓	✓	✓	X	X	X	X	X
	Story	✓	✓	✓	X	✓	✓	✓	X	X	X	X	X
	Reels video sharing	✓	✓	✓	X	✓	✓	✓	X	X	X	X	X
	Live broadcast	✓	✓	✓	X	✓	✓	✓	X	X	X	X	X
	Chats	✓	✓	✓	X	✓	✓	✓	X	X	X	X	X

Conclusion

- Acquiring the data in the cloud with forensic tools seems to be the most practical way.
- Cloud-based forensics extract and then import all tokens found on a device rather than just a single account. This provides new research opportunities for the examiner.
- Using tokens often bypasses the multi-factor authentication security measure.
- On devices using cloud storage applications, it should first be investigated whether there are applications related to cloud service providers.
- Before any search, it should be evaluated how much data is required or how far back into a user's history is required.
- Using offline and online data acquisition together will allow access to the maximum data of the user.
- It will be beneficial to make an action plan for emergencies.
- The accountability mechanism will eliminate the discussion of unlawful evidence.

Reference List

- Ali, S. A., Memon, S. and Sahito, F. (2018). Challenges and solutions in cloud forensics. *In Proceedings of the 2018 2nd International Conference on Cloud and Big Data Computing (ICCBDC'18), Association for Computing Machinery*, New York, NY, USA, 6–10.
- Freet, D., Agrawal, R., John, S. and Walker, J.J. (2015). Cloud forensics challenges from a service model standpoint: IaaS, PaaS and SaaS. *MEDES '15: Proceedings of the 7th International Conference on Management of computational and collective intElligence in Digital EcoSystems*, 148-155.
- Manral, B., Somani, G., Choo, K.K.R., Conti, M. and Gaur, M.S. (2020). A systematic survey on cloud forensics challenges, solutions, and future directions. *ACM Computing Surveys*, 52(6), 1-38.
- NIST (2014). NIST cloud computing forensic science challenges (Draft NISTIR 8006), EUA.