Forensic Analysis of Instagram on Android

Carolin Alisabeth, Yogha Restu Pramadi*
Cyber Security Engineering, Department of Cyber Security, Politeknik Siber dan Sandi Negara
carolin.alisabeth@student.poltekssn.ac.id, *yogha.restu@poltekssn.ac.id

Abstract. The use of social media has become a new lifestyle trend in today's society. Social media provides a variety of benefits, ranging from building connections, delivering news, and sharing daily activities. On the other hand, social media is often misused to commit crimes, such as cyberbullying, child grooming, buying and selling drugs, spreading hoaxes, etc. Information uploaded on social media can be made into consideration for investigations in finding evidence of crimes. Therefore, efforts in supporting the verification of crimes in social media need to be done using the right forensic techniques. Topic of this research is an analysis of artifacts produced by the Instagram application on Android. This research provides benefits for analysts and practitioners to help in finding digital evidence of Instagram on Android. The results of this study successfully identified artifacts of Instagram application on Android, such as user account information, message exchange documentation, and user-uploaded activity traces.

1. Introduction
At present, the development of social media is very rapid. Social media has become part of people's lifestyles today. There are many popular social media, such as Facebook, Instagram, Twitter, Snapchat, and LinkedIn [1]. Generally, social media is used to build relationships with other people, share information, and share ideas, photos, videos, and activities which the user carried out. In addition to the benefits it has, social media can be used as a tool in committing crimes, especially cybercrime [2]. Instagram is a popular social media, therefore Instagram is also often misused for cybercrime, such as buying and selling drugs, cyberbullying, hoax, child grooming.

Lately, social media has become a new domain in digital forensics [3]. Information uploaded on social media can become investigations material by investigators in investigating a crime [4]. Forensic investigations on social media might be required to gather evidence of the crime [4] [5]. Social media usually is used on smartphone, such as Android, iOS, and Windows. Smartphone can store data on social media regarding activities which the user carried out [6]. The focus of this research is to look for artifacts of Instagram on Android that can be used to help practitioners locating and mapping digital evidence. Forensic analysis methodology used within this research is the methodology of Angalano et al. The methodology was chosen because it focuses on finding the location of artifacts and able to interpretations and correlations of the artifacts [7].
2. Methods and Materials

2.1. Research Method
The goal of this research is to find artifacts produced by Instagram on Android. Stages of analysis in this study are using the methodology of Anglano et al. The methodology focuses on the exploration of artifacts produced by Android-based applications [7]. The following are the stages of artifact exploration of Instagram on Android based on the methodology of Anglano et al [7].

- Performs analysis functionalities of Instagram;
- Create experimental designs from the results of the Instagram functionality analysis;
- Execute the design of the experiments one by one. Extract each result of the experimental design stages that have been run then compare it with the previous conditions, especially file system;
- After the design of the experiment has been carried out entirely, explore the results of the artifacts produced, then interpret and correlate the artifacts.

2.2. Analysis environment
This research was conducted in the environment of a virtual android device, GenyMotion. The GenyMotion application can simulate an Android operating system within a virtual mobile device that looks and behave like the original. In addition, the virtual mobile device can be adapted to the characteristics of the hardware and the desired Android version. In this study, the Google Nexus 5x virtual device with the version 7.1 (API 25) Android is being used. Table 1 describes the tools used to conduct an analyst.

| Tool Name                     | Version | Description                                                                 |
|-------------------------------|---------|-----------------------------------------------------------------------------|
| Epoch Converter               | Online  | Epoch time converter                                                        |
| DB Browser for SQLite         | 3.11.2  | A tool to show the contents of SQLite Database File                         |
| Android Studio – Device File Explorer | 3.5.3  | A tool to show the file directory structure for an android device and logs  |
| Sqliteparser GUI by Mari Degrazia | 1.3    | A tool to recover deleted SQLite records                                    |

3. Result and Discussion

3.1. Analysis Functionalities of Instagram
Analysis functionalities is carried out to identify Instagram functionalities that is relevant to the investigative point of view. The following is a mapping of Instagram features that are of value relevant to the investigative point of view.

| NO | FEATURES | FUNCTION |
|----|----------|----------|
| 1. | Posting  | Share photos or videos.  
This feature can provide information related to the user's lifestyle or as evidence of a possible crime. |
### 2. Analysis functionalities of Instagram (continued).

|   |   |
|---|---|
| 2. | Stories | Share user’s daily stories. This feature only lasts 24 hours after being uploaded.  
This feature can provide information related to the presence or absence of deviant acts committed and can be used as evidence of traces of possible crimes. |
| 3. | Direct Message | Send messages, such as texts, photos, videos, and voice notes, privately to other user accounts. In addition, users can make video / voice calls.  
This feature can provide information about the communication documentation by the user. It also give an insight about user's mindset that can be used as evidence of traces of possible crimes. |
| 4. | IGTV | Share videos that are longer than one minute.  
This feature provides the same information as the posting feature. |
| 5. | Search & Explore | Find accounts and content that you might like from accounts that have not yet been followed.  
This feature is useful for finding evidence of impersonation and theft of account identity and provides information related to user activity. |

### 3.2. Design Experiments

The experimental design describes all user activities based on Instagram features. The following are the design of the experiments carried out:
- Log-in to the Instagram application according to the user's credentials;
- The user follows two other accounts;
- The user adds one of the follower accounts to become closefriends;
- The user exchange messages personally and in groups through the Direct Messages feature. The message consists of text, photos, videos, sound recordings, and video/voice calls;
- The user upload photos, videos, and IG stories;
- The user give comments and likes on another account;
- The user delete all messages that have been sent on Direct Message.

### 3.3. Dealing with deletions

File of deleted messages, such as photos, video, and voice notes, are still stored in the device's local storage. On the other hand, record messages in the database deleted, except video/voice call. Even though it has been deleted, SQLite generally keeps records of deleted data in two areas, namely unallocated blocks and free blocks [8]. Furthermore, effort to recover the deleted record is using sqliteparse GUI by Mari Degrazia [9]. The results show that not all deleted data records can be recovered. Records that can be recovered are
only pieces of data from the records. This can happen because some deleted records vacuumed or defragmented by the SQLite database [10].

3.4. Result

Table 3. List of artifacts of Instagram on Android.

| No | Artifacts            | Directory   | Path                                                                 | Content                                                                 |
|----|----------------------|-------------|----------------------------------------------------------------------|-------------------------------------------------------------------------|
| 1  | User account information | shared_prefs | /data/data/com.instagram.android/shared_prefs/com.instagram.android_preferences.xml | User ID, account type, user name, user full name, biography, user account access time, profile photo URL |
| 2  | Contact list | following | shared_prefs | /data/data/com.instagram.android/shared_prefs/com.instagram.android_preferences.xml | the number of followers, following, and closefriends |
|    |                      | followers  | shared_prefs  | /data/data/com.instagram.android/shared_prefs/<ID account>_usersBootstraprapService.xml | information of the user on the 'finding friend' tab |
| 3  | Posting Photos      | media      | /data/media/0/Pictures/Instagram | Photos uploaded |
|    |                      | Videos     | /data/media/0/Movies/Instagram | Videos uploaded |
|    |                      | IG Stories | files | /data/data/com.instagram.android/files/pending_media_images | IG stories photos uploaded |
|    |                      |            |      | /data/data/com.instagram.android/files/rendered_videos | IG Stories videos uploaded |
| 4  | Activity Comments Likes | -        | - | - | Not stored on the local storage system of an Android mobile device |
| 5  | Direct Message Photos | databases   | /data/data/com.instagram.android/databases/direct.db | Record messages on Direct Message |
|    |                      | sent       | cache | /data/data/com.instagram.android/cache/origin al_images | Photos message sent |
Table 3. List of artifacts of Instagram on Android. (continued)

|         | action  | location                                   | status                        |
|---------|---------|--------------------------------------------|-------------------------------|
| Videos  | sent    | /data/data/com.instagram.android/files/rendered_videos | Videos message sent           |
|         | received| /data/data/com.instagram.android/databases/direct.db | Using URL information in the message column |
|         | sent    | /data/data/com.instagram.android/databases/direct.db | Voice notes sent              |
|         |         | /data/data/com.instagram.android/cache/ExoP layerCacheDir |                               |
|         |         | /data/data/com.instagram.android/files/music |                               |
|         | received| /data/data/com.instagram.android/databases/direct.db | Using URL information in the message column |
| Voice   | notes   | databases                                   |                               |
| Video/voice call | databases | /data/data/com.instagram.android/databases/direct.db | Status of starting and ending calls |

4. Conclusion
This research succeeded in identifying artifacts produced by Android-based Instagram applications. These artifacts includes user configurations that contain information related to user accounts, number of following, followers, and close friends accounts. Furthermore, the traces of exchanging user account messages both personally and in groups can be reconstructed based on the chronology and type of the message, such as photos, videos, and sound recordings. The location of media messages sent by user can be identified in local storage on the device. Finally, video uploads, photos, and IG stories can be located on the device storage. As for things that were obtained during the research process that media messages received by user through the direct message feature are not stored in the device's local storage system. However, efforts to find out the media message received can only be seen through the URL link information in the message column of the direct.db database. Unfortunately, the URL link information has an expiry period. Finally, traces of data related to comments and likes are not stored on the device's local storage system.

References

[1] K. Kellogg, "The 7 Biggest Social Media Sites in 2020," 3 February 2020. [Online]. Available: https://www.searchenginejournal.com/social-media/biggest-social-media-sites/.
[2] P. Patel, K. Kannoorpatti, B. Shanmugam, S. Azam and K. C. Yeo, "A Theoretical Review of Social Media Usage by Cyber-Criminals," in International Conference on Computer Communication and Informatics, Coimbatore, 2017.
[3] H. Arshad, A. Jantan and E. Omolara, "Evidence collection and forensics on social networks: Research challenges and directions," Digital Investigation, vol. 28, pp. 126-138, 2019.
[4] D. M. Taylor, D. J. Haggerty, D. Gresty, P. Almond and D. T. Berry, "Forensic Investigation of Social Networking Applications," Network Security, vol. 2014, 2014.
[5] M. S. Chang, "Evidence Gathering of Instagram on Windows 10," *International Journal of Innovative Science, Engineering & Technology*, vol. 3, no. 10, 10 October 2016.

[6] N. A. Mutawa, I. Baggili and A. Marrington, "Forensic Analysis of Social Networking Applications on Mobile Devices," *Digital Investigation*, vol. 9, pp. S24-S33, 2012.

[7] C. Anglano, M. Canonico and M. Guazzone, "Forensic Analysis of Telegram Messenger on Android Smartphones," *Digital Investigation*, vol. 23, pp. 31-49, 2017.

[8] S. Jeon, J. Bang and K. Byun, "A Recovery Method of Deleted Record for SQLite Database," *Personal and Ubiquitous Computing*, vol. 16, pp. 707-715, 2011.

[9] M. DeGrazia, "Python Parser to Recover Deleted SQLite Database Data," 2 September 2014. [Online]. Available: http://az4n6.blogspot.com/2013/11/python-parser-to-recover-deleted-sqlite.html. [Accessed 12 Juli 2020].

[10] Tamma Rohit and D. Tindall, Learning Android forensics: a hands-on guide to Android forensics, from setting up the forensic workstation to analyzing key forensic artifacts, Birmingham: Packt Publ, 2015.