Computer Systems Science & Engineering
DOI:10.32604/csse.2021.014472
Article

Tech Science Press

Instagram Mobile Application Digital Forensics

Muhammad Asim Mubarik[1], Zhijian Wang[1], Yunyoung Nam[2,*], Seifedine Kadry[3] and Muhammad Azam waqar[4]

[1]College of Information and Computer Science, Hohai University, Nanjing, 210098, China
[2]Department of Computer Science and Engineering, Soonchunhyang University, Asan, 336811, Korea
[3]Department of Mathematics and Computer Science, Beirut Arab University, Beirut, 000000, Lebanon
[4]School of Business Management, NFC Institute of Engineering & Fertilizer Research, Faisalabad, 38800, Pakistan
[*]Corresponding Author: Yunyoung Nam. Email: ynam@sch.ac.kr
Received: 22 September 2020; Accepted: 27 November 2020

Abstract: In this research, we developed a plugin for our automated digital forensics framework to extract and preserve the evidence from the Android and the IOS-based mobile phone application, Instagram. This plugin extracts personal details from Instagram users, e.g., name, user name, mobile number, ID, direct text or audio, video, and picture messages exchanged between different Instagram users. While developing the plugin, we identified resources available in both Android and IOS-based devices holding key forensics artifacts. We highlighted the poor privacy scheme employed by Instagram. This work, has shown how the sensitive data posted in the Instagram mobile application can easily be reconstructed, and how the traces, as well as the URL links of visual messages, can be used to access the privacy of any Instagram user without any critical credential verification. We also employed the anti-forensics method on the Instagram Android's application and were able to restore the application from the altered or corrupted database file, which any criminal mind can use to set up or trap someone else. The outcome of this research is a plugin for our digital forensics ready framework software which could be used by law enforcement and regulatory agencies to reconstruct the digital evidence available in the Instagram mobile application directories on both Android and IOS-based mobile phones.

Keywords: Digital forensics; Instagram; mobile application forensics; anti-forensics; forensics framework plugin

1 Introduction

Since the introduction of Facebook, online social networks have evolved (over the last decade) and a countless number of applications, that provide different features, have surfaced on the Internet [1]. These applications vary from generic social network services, to image-sharing, and video sharing, social networking services. Their primary purpose is help people from different continents to stay connected with one another.

Among the most popular social networking sites is Instagram, (primarily used via its mobile application) [2] which has over a billion registered users [3]. It is a social networking application that lets users capture and share photos and videos within their social circles. Users of Instagram, register themselves with a unique user ID and password. They also have the option of connecting their Instagram accounts with their Facebook accounts, which help users share their photos and videos with their audience (social circles) more effectively. Similar to Facebook's functionality, every Instagram user has their own personal newsfeed, which functions as a personal notice board, displaying content shared by individuals or pages that the user has subscribed to ("follows"). This visual sharing platform has become more popular nowadays because Instagram provides users with additional features including video editing and photo editing tools (enabling users to add filters, animals, and shapes, to their photos and videos). The "story" feature of Instagram allows users to attract more audience, which consequently helps them increase interaction on their regular posts. This results in users accumulating more highly desired "likes" on their posts. The "story" functions as a secondary newsfeed, situated atop the main personal newsfeed of every Instagram user. Through such activities, the platforms helps people from across the globe, to connect and form new relationships, in a very interactive manner. However, unbeknownst to its users, applications such as Instagram provide personal information of its users to other users, which can be potentially dangerous. In today's technologically advanced era, people are using platforms such as Instagram to find their future spouses online. Couples connect with each other freely on Instagram, without comprehending the potential danger they are exposed to. Cases of online theft, copyright infringement, extortion, kidnapping [4] and even rape, have been reported, which occurred because the victim had trusted a friend from their social network friend list, and shared personal information online.

In recent times, more and more cases are being reported to investigation agencies, which involve criminal activity caused by the misuse of social media platforms. These investigation agencies employ various digital forensics tools to extract key evidence from the mobile devices of culprits, to help get them convicted in the court of law. The problem here is that there are so many different devices and applications generating such large amounts of data, that its difficult for digital forensics experts keep themselves updated on latest digital forensics tools [5]. Keeping in mind the significance of social networking applications and digital forensics, national governments are now updating their standards and training their staff to detect drug-related crimes and stop drug trafficking operations [6].

"So many applications and so many technologies are being created and continuously updated, that forensic investigators cannot keep up" [7].

"Our Digital Forensics research group here at Shanghai Forensic Research Center keeps adding automated forensics plugins for every new app that is popular among the masses so that our law enforcement officers can extract evidence from all the apps available on mobile phones whether it's an Android phone or an IOS phone."

In this paper, we have studied the forensic artifacts of the Instagram application on both Android and IOS phones. We implemented code to automatically extract these forensics artifacts using our forensic framework environment, which is capable of extracting evidence from more than seventy different Android and IOS applications. At the end of this paper, we have discussed an anti-forensics experiment conducted on the Android Instagram application, to gauge its effectiveness. We have also presented a few privacy issues that we found in both versions of the Instagram application (Android and IOS).

2 Related Work

Forensics analysis of the Instagram mobile application is not a very popular topic. Several researchers have done the forensics analysis of Instagram, but none of them have helped digital forensics investigators to reconstruct the data from forensic artifacts available in mobile devices. Instagram has always been a

successful and popular application. Within only two months of its inception, it had 2 million users registered worldwide. The popularity of the Instagram application coupled with the abundant forensics artifacts it leaves behind is why forensics experts find the application so interesting. Consequently, standalone applications like Instagram that run on mobile phones can provide add-on forensic information to help identify criminal suspects. A suspect's geolocation near a crime scene and their digital signature available on their installed Instagram application, can help resolve many cases. Such applications nowadays also provide a very convenient one-tap login facility, which allows you to set your mobile phone as your default device.

Reema Al Mushcab et al. performed forensics analysis of the iPhone 5s Instagram application [8]. Their focus was primarily on "write-blockers" rather than the forensics artifacts of the Instagram application. A problem that we identified in this research is that they could not locate the direct messages database in the Instagram directory "com.instagram.android" of the IOS application, where the main evidence usually resides. This is the main focus of our research. We want to extract evidence (messages exchanged between the victim and the accused directly using this application) of a criminal nature, which will prove the involvement of suspects in kidnapping, murdering, bombing, raping, or financial corruption cases.

In 2015, Ming [9] employed evidence-gathering techniques on Instagram using the Windows 10 Operating System. The focus of Ming Sang Chang's research matches our own research objectives which is to capture extensive evidence from social networking services that can be used to help deter people from committing crimes such as spreading slander, cyberstalking, cyberbullying, hacking, copyright infringement, rape, murder, and financial corruption. Chang's research involved capturing evidence from Internet Explorer and Google Chrome, using the SQLite database and WinHex to find data remnants of user's account IDs and passwords. The researchers created a scenario in which, after performing a criminal activity, the user tried to remove the digital evidence using Eraser Portable v5.8.8.1 and CCleaner V5.19.5633. The researchers subsequently performed digital forensics analysis of the user's hard drive to uncover any evidence. Unlike Mr. Chang's research, our own research focuses mainly on forensics analysis of the Android and IOS mobile applications.

Wong et al. (security researcher at Valkyrie-X Security Research Group) [10] conducted a detailed digital forensics study of Facebook's web application and mobile application. This research was conducted on the iPhone 3GS IOS version 4.3 which is why it's very old and outdated. The research is also limited only to IOS forensics, neglecting the large majority of Android device users.

Yusoff et al. [11], conducted a forensic investigation of social media and instant messaging services on Firefox OS, including Instagram, in 2017. This research involved using Forensics Toolkit (FTK) version 3.1.2 and HxD Hex Editor 1.7.7.0 to capture and analyze memory images on a phone called Peak (Geeksphone, 2013) running Mozilla FxOS. The limitation in this research is that volatile memory cannot hold data for long periods and forensic artifacts can only be found on the phone while Mozilla FxOS is running. If forensics analysis is performed after the phone has restarted, all the digital forensics evidence will have evaporated out of the phone's volatile memory. More importantly, every social networking service has now launched their own customized application, and registered users prefer accessing this application, rather than browsing the social media site it is affiliated with, on the mobile browser. The main reason for this is that users no longer need to re-login every time to use their desired social networking site, instead they can use the application's one-tap login feature. The mobile applications enable this feature by saving the registered user's account credentials on the mobile device. Mobile apps such as Instagram have their directory structures saved onto the users mobile device's physical storage. Such mobile applications store crucial information on persistent storage of the device aswell. In this research (of ours) we will show that the complete SQL lite database file can be found in different directories in both Android and IOS devices.

In 2015, Daniel Walnysky et al. [12], published their research on direct messaging mobile applications and established how evidentiary traces allow reconstruction of data, and permit reconstruction of activities performed by users and applications. Their work mainly focuses on only Android applications. In their research, they have also suggested that the automated reconstruction of data is also possible, mentioning it as the basis of their future work. This automated reconstruction of data is the main outcome of our own research. In our research's analysis and results section we will discuss how our framework reconstructs the forensic remnants available inside the mobile phone and the concerned application directories for both Android and Apple devices. Walnysky et al. [12], also performed similar work on Facebook forensics analysis [13,14]. Our own research group has also conducted similar extensive research on Mobile application's digital forensics. Until now, our group has performed digital forensics analysis on more than seventy popular mobile applications used by the masses in China and elsewhere. The fruits of our labor will enable law enforcement personnel to use our digital forensics-ready workstation to perform necessary forensics analysis in ongoing cases, and present the evidence in a court of law.

This paper discusses our research and development of a forensics plugin for the Instagram mobile application.

3 Test Environment and Requirements

This framework was developed in Visual Studio with devexpress tools installed. Below is a complete list of all the hardware and software tools used to perform the forensics analysis of both Android and IOS based mobile applications:

- iPhone 7Plus (v. 12.0.1)
- Meizu Note 6
- Instagram (v. 69.0)
- Apple iTunes application (v. 12.1)
- Android Debug Bridge (ADB)
- Microsoft Visual Studio Professional 2012 (v. 11.0.50727.1 RTMREL)
- DEVEXPRESS
- SQLite Expert Professional (v. 3.5.21.2440)
- DATABASE Browser for SQL open-source (Version 3.10.1)
- Plist Editor Pro (v. 2.0)
- Win Hex/X-Ways Forensics software
- Apple's iPhone 7Plus USB data cable
- Windows Photo Viewer
- VLC Media player (v. 2.1.3)

4 Forensics Analysis of Android-Based Instagram Application

4.1 Retrieval of the Instagram Directory Structure

We selected the Instagram application because our research group had already performed digital forensics for almost all the popular social media networking applications including Facebook, WhatsApp, Line, Weibo, and so many others. A picture of the front end for our framework can be seen in Fig. 1.

We chose a mobile application based on popularity in China because this framework is designed for the use of Chinese law enforcement agencies and public security organizations to help solve cases more easily, and hence provide a more safe and secure social life within Chinese cities. We performed forensics analysis

of the Instagram application for both Android and Apple IOS versions. For this activity, we first installed the Instagram application on an Android device as well as an Apple IOS device. In this specific experiment, we used an Android-based Meizu Note 5 phone and an Apple IOS 7 plus mobile device with IOS version 12.1.1.

Figure 1: Forensics framework front end

4.2 Android Devices Data Extraction

The second stage was to utilize the "pull" command of Android Debug Bridge (ADB), which helped us extract the contents of "com.instagram.android." We did this so that we could perform manual analysis of the changes in the contents of the package upon performing different activities (creating user, sending a message, and sharing pictures) via the mobile application. Fig. 2 shows the flow diagram of our experiment analysis process that we followed.

5 Key Forensics Artifacts Identification of Android Instagram App

After acquiring the directories from an Android device, we performed a manual analysis of the application and attempted to locate the files of interest. Tab. 1 elaborates the information cum evidence that we wanted to locate from these devices; for this purpose, we performed an activities in the Instagram app so that data is generated and stored into the Instagram directory structure. We created two user names on Instagram to generate the forensics artifacts in the Instagram mobile application database. Tab. 1 elaborates on the activities performed in the mobile application to generate the data that would be extracted as evidence later on by our forensics framework.

Examination of Instagram on Android (com.instagram.android): Instagram creates com.instagram.android in data/app/ to store all the directories and files. Directories of com.instagram.android are shown in Fig. 3.

The "databases" directory and "shared_prefs" directory hold important forensics artifacts for digital forensics analysis of Instagram. "shared_prefs" directory contains XML files that hold 'full name', 'user

name', 'id', location, and other important information about the user of the application. The databases directory contains the direct messages exchanged between the user and other Instagram users.

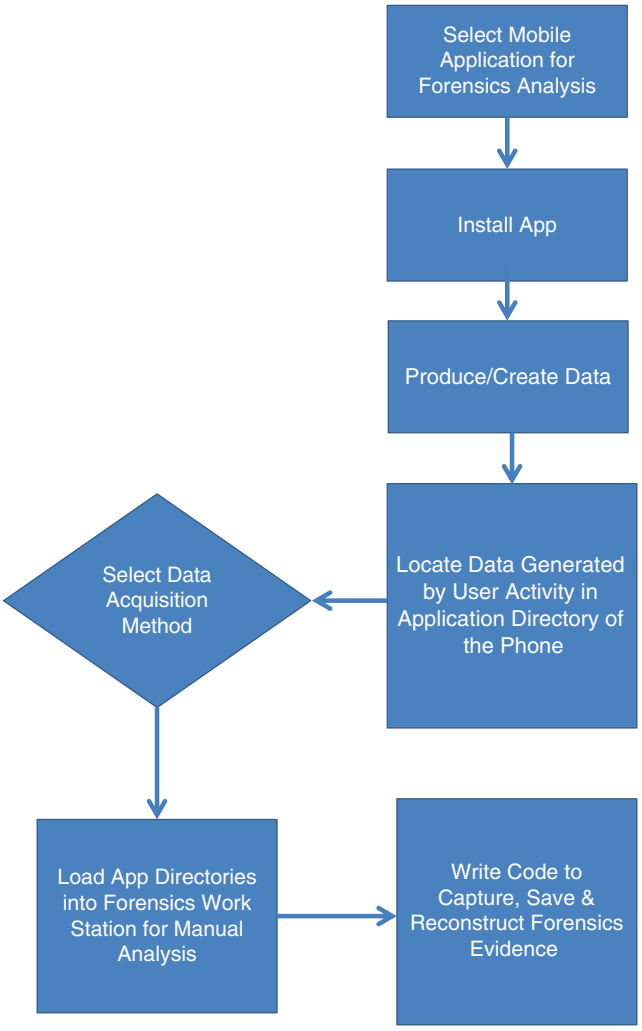
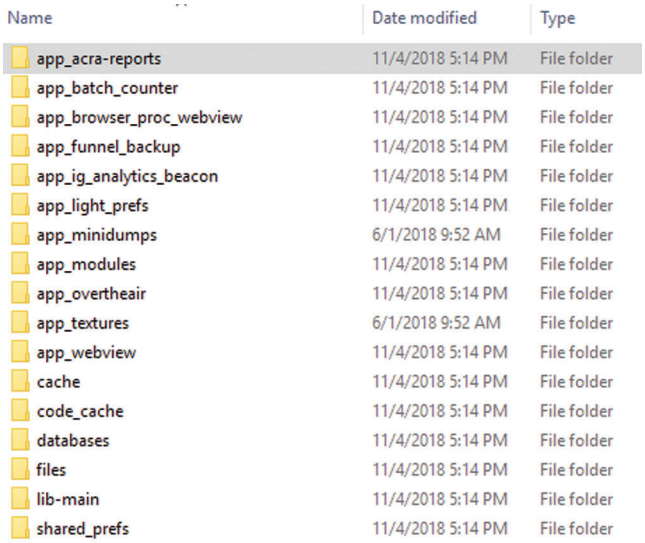


Figure 2: Flow diagram of the analysis process

Table 1: Activities performed

Mobile & Application	Activity
1. Meizu Android Instagram.apk 2. IOS iPhone 7plus Instagram	1. New user registration 2. Following another Instagram user 3. Send text message 4. Send picture message 5. Send audio message 6. Send video clip



Name	Date modified	Type
app_acra-reports	11/4/2018 5:14 PM	File folder
app_batch_counter	11/4/2018 5:14 PM	File folder
app_browser_proc_webview	11/4/2018 5:14 PM	File folder
app_funnel_backup	11/4/2018 5:14 PM	File folder
app_ig_analytics_beacon	11/4/2018 5:14 PM	File folder
app_light_prefs	11/4/2018 5:14 PM	File folder
app_minidumps	6/1/2018 9:52 AM	File folder
app_modules	11/4/2018 5:14 PM	File folder
app_overtheair	11/4/2018 5:14 PM	File folder
app_textures	6/1/2018 9:52 AM	File folder
app_webview	11/4/2018 5:14 PM	File folder
cache	11/4/2018 5:14 PM	File folder
code_cache	11/4/2018 5:14 PM	File folder
databases	11/4/2018 5:14 PM	File folder
files	11/4/2018 5:14 PM	File folder
lib-main	11/4/2018 5:14 PM	File folder
shared_prefs	11/4/2018 5:14 PM	File folder

Figure 3: Directory structure of com.instagram.android package extracted from Android Phone

In the following section, we will describe the anatomy of the "com.instagram.android_preferences.xml" file. Snapshot of this file is presented in Fig. 4, and we have listed important forensics artifacts in Tab. 2.

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <map>
    <string name="App Restrictions">AAAAAA== </string>
    <int name="carousel_nux_impressions" value="25"/>
    <string name="google_ad_id">abf68bb6-70af-4438-a72b-822e83f188f0</string>
    <string name="user_access_map">[{"user_info":
      {"id":"7526247127","blocking":false,"blocking_reel":false,"follower_count":13,"following_count":null,"follow_status":"Fo
      sit4-1.cdninstagram.com/vp/b38273e465e0bb2777b6845dea25cbd2/5BB665AE/t51.2885-
      19/s150x150/30078315_212007865488308_1563912706187067392_n.jpg","profile_pic_id":"1759213689388687079_7
      followers","coeff_weight":0.0,"can_see_organic_insights":false,"aggregate_promote_engagement":false,"can_boost_post
      {"mode":0,"gradient":2,"emoji":"😎","selfie_sticker":0,"selfie_url":null}},"time_accessed":1527749843766}]</string>
    <string name="preference_hardware_id">862806035351425</string>
    <long name="push_reg_dateandroid_mqtt" value="1527749587114"/>
    <string name="one_tap_login_user_map">{"user_info_list":
      [{"upsell_seen_before":false,"allow_non_fb_sso":true,"rejected_sso_upsell":false,"one_tap_upsell_after_login_count":0,
      sit4-1.cdninstagram.com/vp/be544683a2099264ae250fdc1e6fff7a/5BC4F2EC/t51.2885-
      19/s150x150/30591478_1604198099628650_1119136862359781376_n.jpg"}]}</string>
    <string name="cm_last_bandwidth">ConnectionManagerHistoricalData:mData=54.34873103962058,
      mTimestamp=1527753149029</string>
    <int name="number_of_carousels_swiped" value="1"/>
    <long name="b_LAST_REQUEST" value="1527749698"/>
    <boolean name="show_tos" value="false"/>
    <boolean name="used_double_tap" value="true"/>
    <string name="fb_attribution_id">a3ea46e6-dc0b-4da0-949b-6b49d64db586</string>
    <string name="cm_last_latency">ConnectionManagerHistoricalData:mData=250.30865273515246,
      mTimestamp=1527753149029</string>
    <string name="current">
      {"id":"7526247127","blocking":false,"blocking_reel":false,"follower_count":13,"following_count":null,"follow_status":"Fo
      sit4-1.cdninstagram.com/vp/b38273e465e0bb2777b6845dea25cbd2/5BB665AE/t51.2885-
      19/s150x150/30078315_212007865488308_1563912706187067392_n.jpg","profile_pic_id":"1759213689388687079_7
      followers","coeff_weight":0.0,"can_see_organic_insights":false,"aggregate_promote_engagement":false,"can_boost_post
      {"mode":0,"gradient":2,"emoji":"😎","selfie_sticker":0,"selfie_url":null}}</string>
    <boolean name="google_ad_id_logged" value="true"/>
    <boolean name="opt_out_ads" value="false"/>
    <boolean name="written_cache_dummy_file" value="true"/>
    <int name="used_double_tap_hint_impressions" value="3"/>
    <boolean name="com.facebook.sdk.appInstallEvent" value="true"/>
```

Figure 4: Contents of com.instagram.android.xml

This XML file contains two important tags that store information regarding the user of the application; the information is stored in a key-value pairs format, which can be easily extracted using any programming technique. In our experiment, as we mentioned above, we utilized Visual Studio with devexpress tool, to program the extraction of these forensics artifacts. The rest of the XML files and directories contain user bootstrap services information, cookies, etc. The next directory of our interest is the databases directory, which contains direct messages (in the file named 'direct.db') exchanged between the registered user of the mobile application, and other Instagram users. Fig. 5 shows the relations and tables in the direct.db file of Instagram; In these tables, the messages table, contains the direct messages exchanged between different users and has great significance as digital forensics information.

Table 2: Important forensics artifacts available within User Access Map tag com.instagram.android.xml

Forensic Information	Key	Value
Unique ID by Instagram	Id	7526247127
Total number of people following this ID	follower_count	13
Count of IDs this user is following	following_count	Null
Full name of user	full_name	DarkTest
URL of user profile picture	profile_pic_url	https://scontent-sit4-1.cdnInstagram.com/vp/b38273e465e0bb2777b6845dea25cbd2/5BB665AE/t51.2885-19/s150x150/30078315_2120078654888308_1563912706187067392_n.jpg
Unique ID by Instagram for this profile picture	profile_pic_id	1759213689388687079_7526247127
User name registered on Instagram	Username	dark2539
Selfie picture URL	selfie_url	Null
Last online time	time_accessed	1527749843766

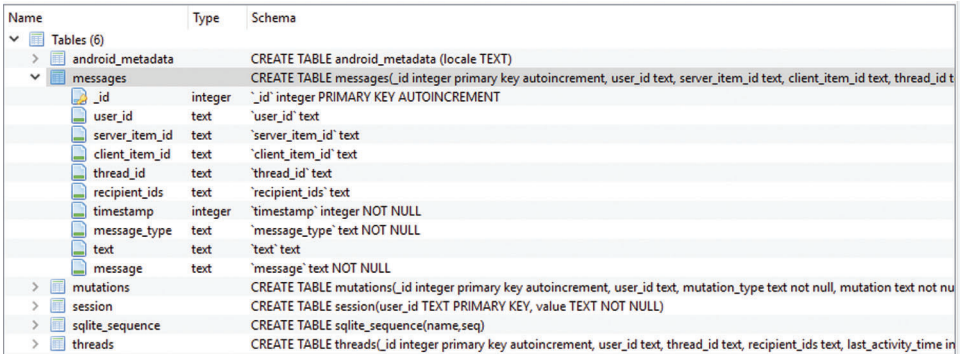


Figure 5: Table relation in Direct.db

Here, we can observe that the message-id and user-id are the current user's id to identify the user of the current Instagram mobile application. As Instagram stores a copy of the contents on the server side, so every message is assigned a server_item_id whereas contents that reside in mobile application directories are assigned client_item_id, while recipient_id timestamp is for when the message was received.

Message_type distinguishes whether the message is a text message or an audio-video message. In case it is a text message, the text is stored in the 'text' field of this table. However, if the message is a picture or video message, then the link of the multimedia message is stored in the message field while the 'text' field is kept empty and has no value stored in it; this has been shown in Fig. 5 and Fig. 6b by highlighting the message field data in these pictures. The Message field is an important element of this table and stores the most valuable forensics information for all kinds of messages, whether it is a text, video, or audio message.

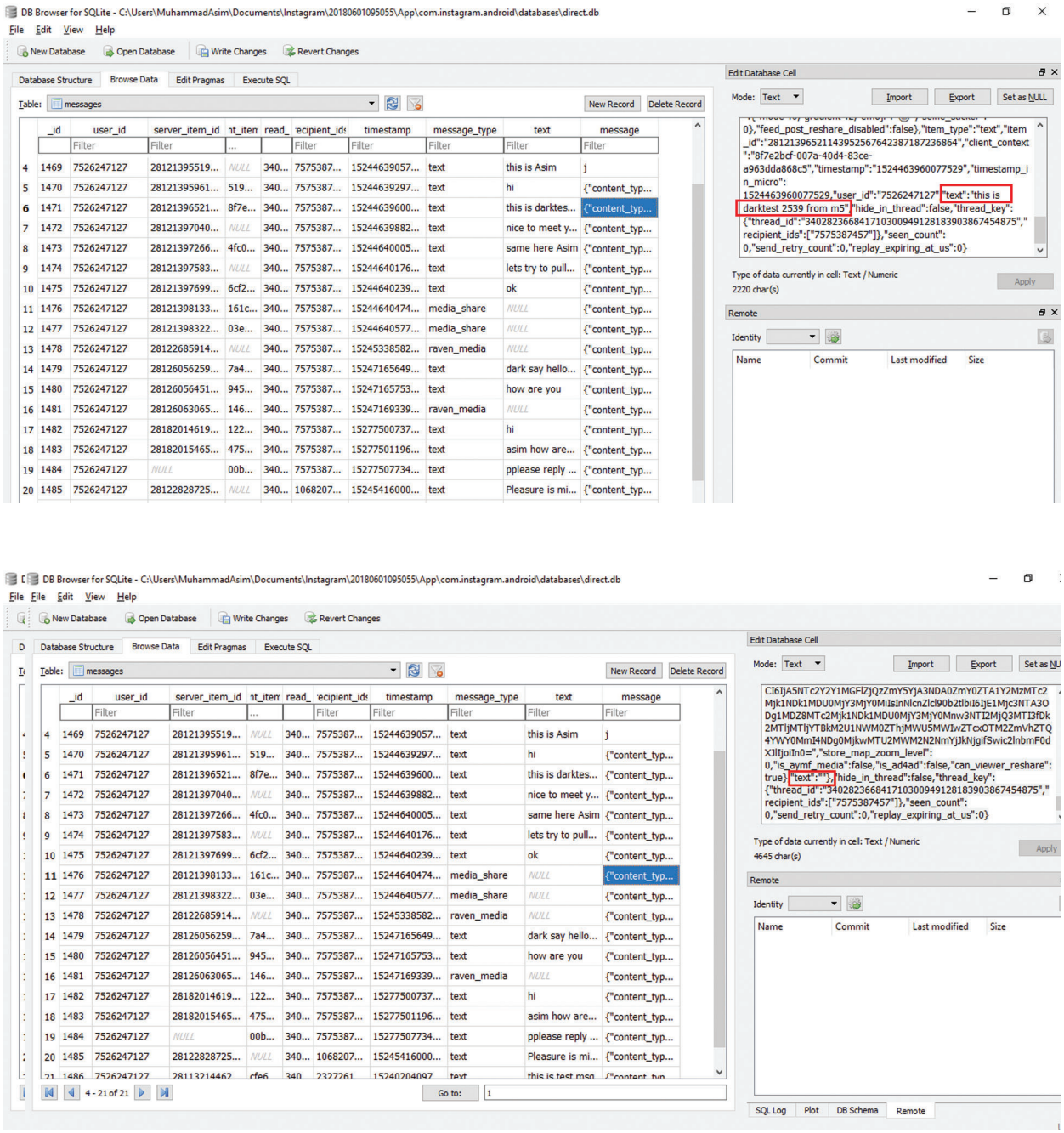


Figure 6: Messages table of Direct.db (b) Contents of message field messages table of Direct.db

This information is stored in JSON format. Contents of the message field for text message and visual (image or video) messages are listed in Fig. 7.

Once we had identified the information available in the different files and directories, we extracted this information in our digital forensics ready framework software. For this purpose, we created our local databases to store the forensics artifacts in. In the results section, we have shown how we extracted valuable information from different files to be stored permanently in our forensics workstation evidence database.

{"content_type":"TEXT","status":"UPLOADED","user":{"username":"dark2539","full_name":"DarkTest","profile_pic_url":"https://scontent-sit4-1.cdninstagram.com/vp/b38273e46
"profile_pic_id":"1759213689388687079_7526247127","hd_profile_pic_url_info":{"url":"https://scontent-sit4-1.cdninstagram.com/vp/8ff5fbeb9abde2f5d483404c30eaba04/5BBCE9D
"width":1080,"height":1080,"type":0},"has_anonymous_profile_picture":false,"id":"7526247127","is_favorite":false,"is_profile_action_needed":false,"usertag_review_enable
"external_lynx_url":"","external_url":"","follower_count":14,"following_count":18,"besties_count":0,"recently_bestied_by_count":0,"media_count":3,"is_private":false,"al
"has_chaining":false,"auto_expand_chaining":false,"coeff_weight":0.0,"is_needy":true,"is_new":false,"is_unpublished":false,"social_context":"Following","aggregate_promc
"can_convert_to_business":true,"can_see_organic_insights":false,"is_business":false,"unseen_count":0,"show_insights_terms":false,"allow_contacts_sync":true,"show_busine
"can_link_entities_in_bio":true,"reel_auto_archive":"unset","nametag":{"mode":0,"gradient":2,"emoji":"😎","selfie_sticker":0},"feed_post_reshare_disabled":false},"item_t
"timestamp":"1524463960077529","timestamp_in_micro":1524463960077529,"user_id":"7526247127","text":"this is darktest 2539 from m5","hide_in_thread":false,"thread_key":{

Figure 7: JSON Contents of the message field

Table 3: Important forensics artifacts available within in User Access Map tag

Forensic Information	Key	Value
User information	User	"username":"dark2539", "full_name":"DarkTest", "profile_pic_url":"https://scontent-sit4-1.cdnInstagram.com/vp/b38273e465e0bb2777b6845dea25cbd2/5BB665AE/t51.2885-19/s150x150/30078315_2120078654888308_1563912706187067392_n.jpg, "profile_pic_id": "1759213689388687079_7526247127", "hd_profile_pic_url_info": {"url":"https://scontent-sit4-1.cdnInstagram.com/vp/8ff5fbeb9abde2f5d483404c30eaba04/5BBCE9D6/t51.2885-19/30078315_2120078654888308_1563912706187067392_n.jpg"
Instagram ID	Id	7526247127
Follower count	follower_count	14
	following_count	18
	besties_count	0
	Timestamp	1524463960077529
	Timestamp	1524463960077529
	Text	this is darktest 2539 from m5

6 Forensics Analysis of IOS-Based Instagram Application

For the logical acquisition of the iPhone image from Apple devices, iTunes is the best authentic software available. Many research articles suggest and recommend the use of iTunes for the logical acquisition of Apple device contents; in their research, Bader et al. [15] described in detail how the logical acquisition of a device image using iTunes, with auto synchronization disabled, ensures that the acquired logical image of the device is forensically sound. Once the whole directory structure containing the data for forensics analysis was extracted into our forensics workstation, we started analyzing the contents of the directories and files manually to find the evidence we needed so we could code our framework. The purpose of this framework would be to extract similar forensics artifacts automatically later by just the click of a button.

7 Key Forensics Artifacts Identification of Instagram in IOS-based Device

Logical acquisition of an IOS device using the backup facility, provides a wealth of information for forensic analysis [16]. After being installed on the IOS device, the Instagram application creates the following directory structure as shown in Fig. 8. In the AppDomain directory of the iPhone, a directory with "com.burbn.Instagram" name is created to store the data of Instagram on the IOS device. We extracted

the entire directory structure from the IOS device using the iTunes backup facility [17]. After manual analysis of this directory structure, we noted that the database file containing direct messages exchanged between users of Instagram, was stored in the "AppDomain\com.burbn.Instagram\Library\Application Support \DirectSQLiteDatabase\7463799528.db" file. Another important fact we noted was that the direct messages file was named differently from that of the Android database file name counterpart. This number 7463799528 is the unique identifier for each Instagram user. As seen in the "com.instagram. android_preferences.xml" file of the Android Instagram version, this kind of unique identifier is being used to identify users of Instagram as well. Similarly in the IOS, the database file name is also assigned a congruent identifier to distinguish between the messages and databases of different users. We will now explain how we extracted the messages exchanged between users from this "7463799528.db" file.

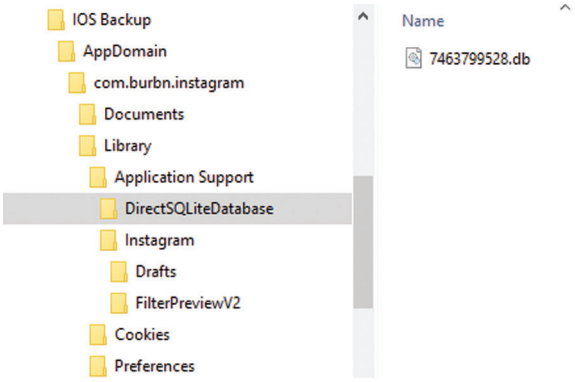


Figure 8: Directory structure of com.burbn.Instagram package extracted from Apple iPhone

The second important file that contains significant digital artifacts related to the Instagram user in IOS devices is the "com.burbn.Instagram.plist," which is located in the "AppDomain\com.burbn.Instagram \Library\Preferences" directory.

Fig. 9 reveals all the information stored within the "com.burbn.Instagram.plist" file. In this file we are only interested in the key data which can serve as evidence and give away the personal details of the mobile application's user (name, user name, phone number, email address).

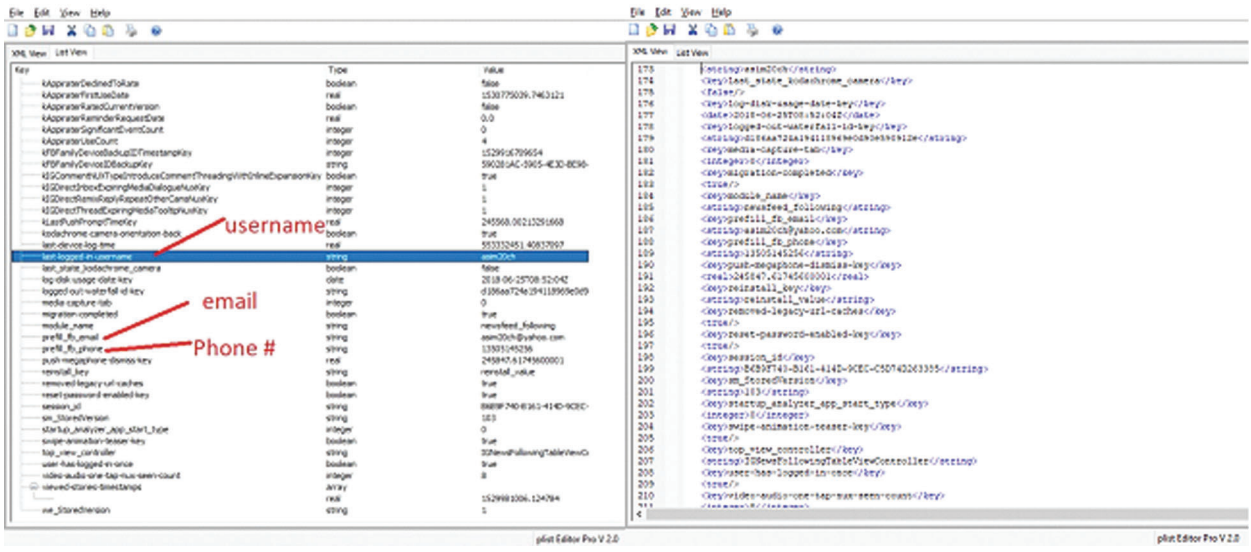


Figure 9: Key forensics artifacts stored in com.burbn.Instagram.plist

After we had identified the personal information associated with the user, we wanted to extract the personal messages exchanged through this device using the Instagram application. This information is available in the "7463799528.db" file. Analysis of this file showed that the archive column of the messages table contains important information stored in the Binary Large Object (BLOB) format.

In Fig. 10 you can see the contents of the database file and the contents of its corresponding messages table and "archive" column. It is important to note that pictures and video messages are not stored locally on the device, instead, if the user shared any visual message, only its URL would be stored in this local database file.

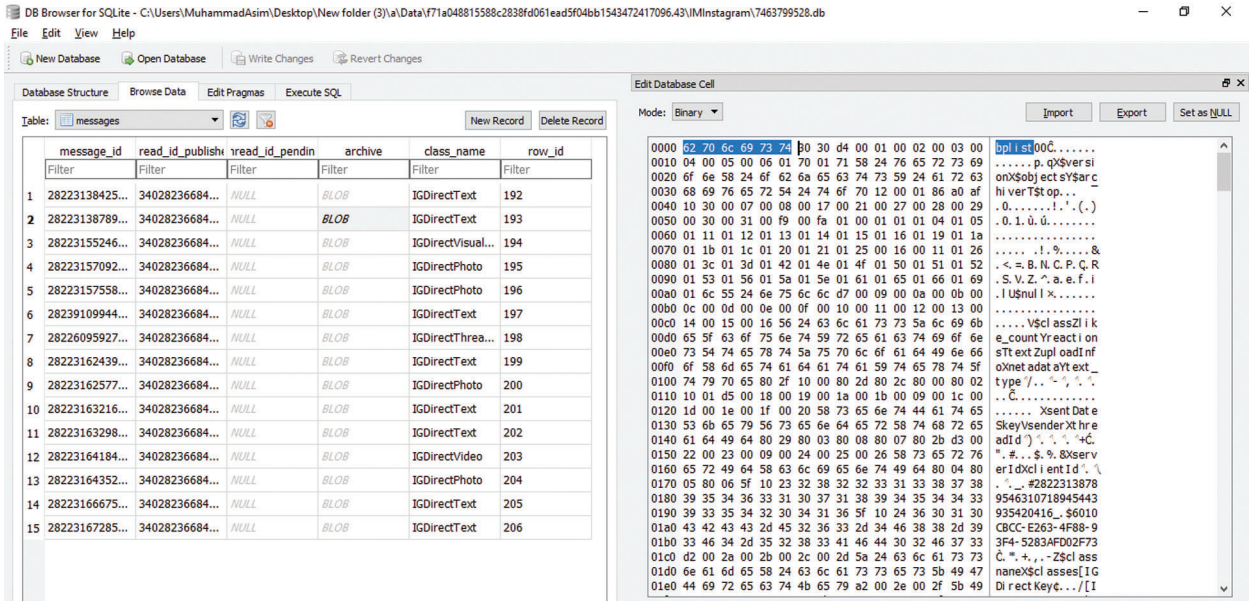


Figure 10: Table relation in 7463799528.db

Upon analyzing the archive column's BLOB object, and contents of the binary data, it was found that this BLOB contains data in the bplist format as shown in Fig. 11. The first 6 offsets of every BLOB object is 62 72 6c 69 73 74 which corresponds to a bplist format of data.

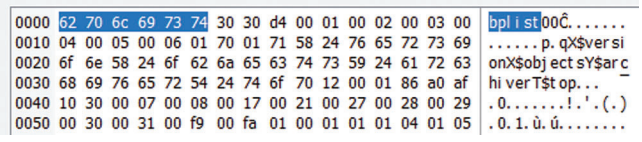


Figure 11: Pblist Hexadecimal Header in BLOB object

In the next step, we exported the binary data into the bplist file. After this, we opened the bplist file with WinHex/X-Ways Forensics software, and were able to view the contents of a text message in hex file as shown in Fig. 12.

Further analysis of this binary data revealed the contents of text messages, which were found at offsets 11B3 to 11F7. For visual messages, the URL of the contents are also stored in a BLOB. This bplist file contains a directory named "root" which has four keys stored in its directory, namely: $archiver, $objects, $top, and $version (as shown in Fig. 13).

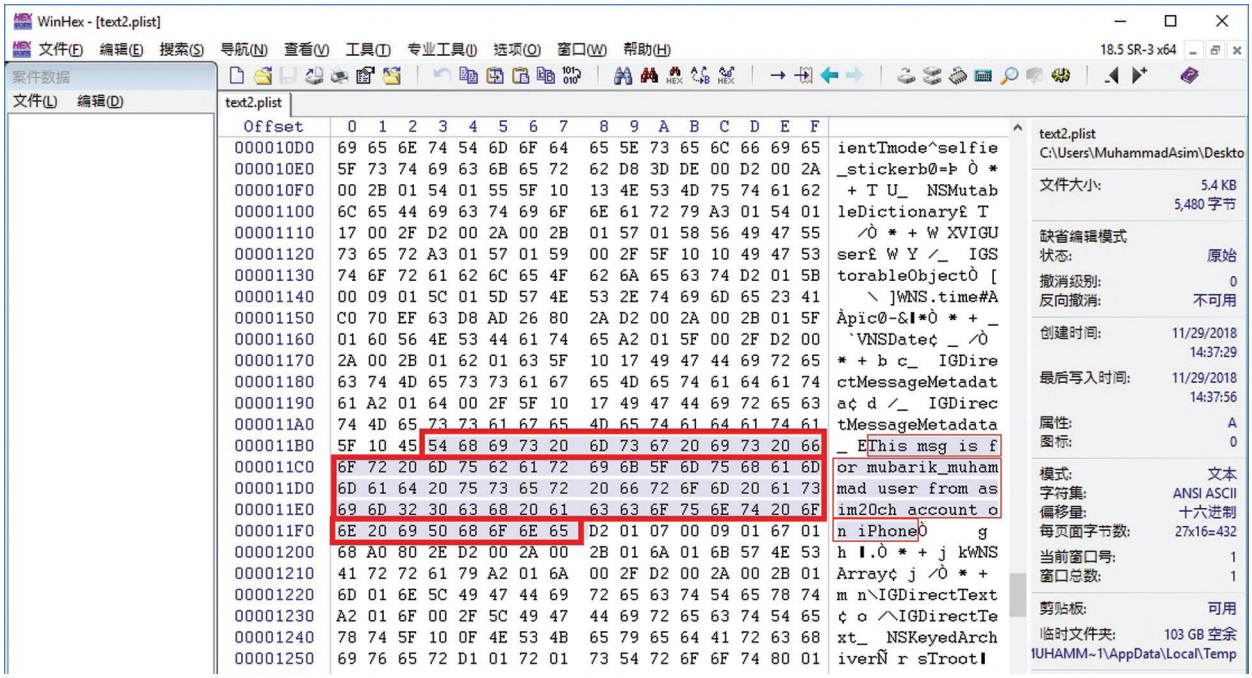


Figure 12: The text message is visible along with related metadata in the BLOB object of the archive column (in the messages table)

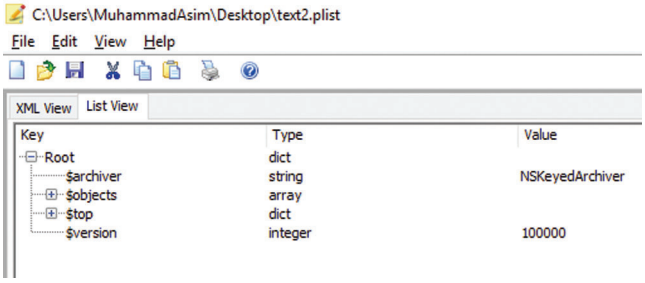


Figure 13: Bplist list view

$Objects has sub directories which store the text messages exchanged within them, or the URL of picture messages exchanged between different users. Fig. 14 shows the hierarchy of directories in this bplist, $Objects are stored as BLOB objects in the archive column, of the messages table, in the user direct messages database file. In the next section, we will discuss the forensics results and data reconstructed from these files.

8 Evidence Retrieval, Plugin Implementation, and Results

As elaborated in previous sections, we successfully identified and located the valuable information which could serve as potential evidence. In this section, we will now present the extracted evidence from the Instagram mobile application. Instagram forensics was implemented in our forensics-ready framework as a dynamic link library. A unique identifier was created, and in this folder, forensics data of each application was saved into a separate folder (named according to the corresponding mobile application). In case of Instagram, the IMINSTAGRAM directory stored a copy of original files extracted from the

Instagram app. Briefly explaining how the forensics software operated; it first extracted, and made a copy of the files containing digital forensics artifacts ("com.instagram.android," "direct.db" and "burbn.Instagram.plist," "7463799528.db") for both the IOS and Android devices respectively, into the IMInstagram directory, as shown in Fig. 15. Then, the software created a results folder, in which it stored a database file, containing the reports of all relevant information and direct messages exchanged between the current user and other Instagram users. Figs. 16 and 17 exhibit the extraction of the currently logged in user's information, and messages exchanged between this user and different users within this application.

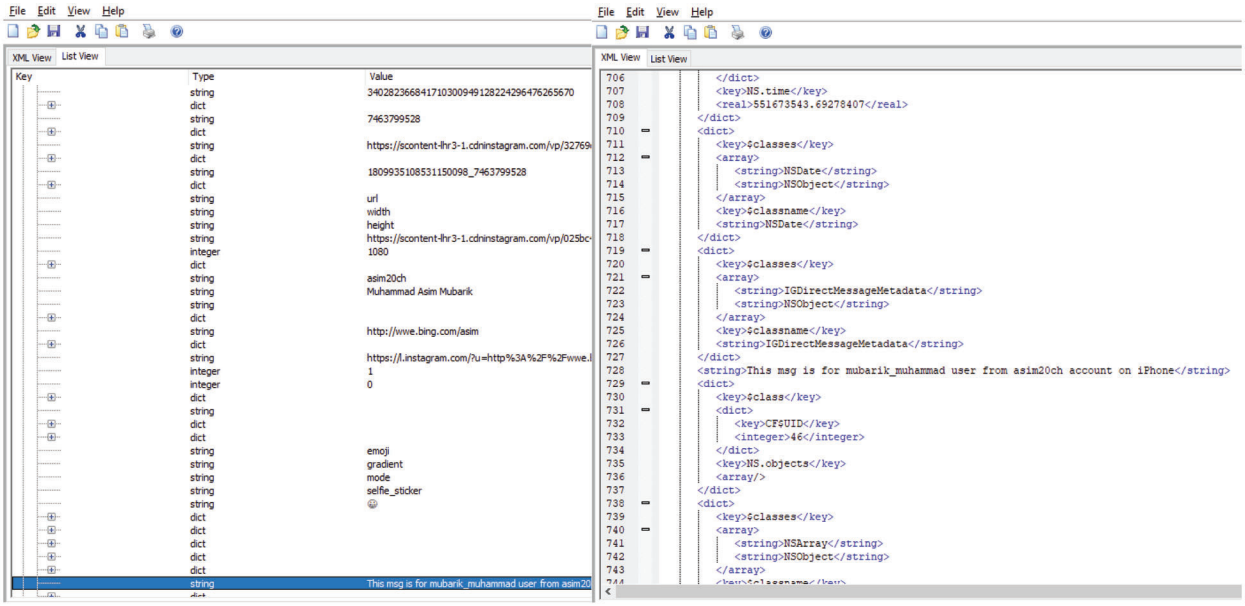


Figure 14: List view & XML view of the bplist extracted from the BLOB object of the archive column in the messages table

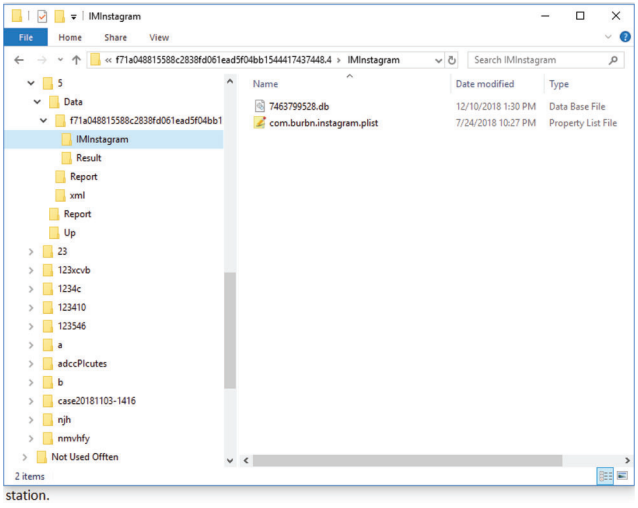


Figure 15: Forensics workstation evidence files local copy

Figure 16: Direct messages reconstructed from Android application

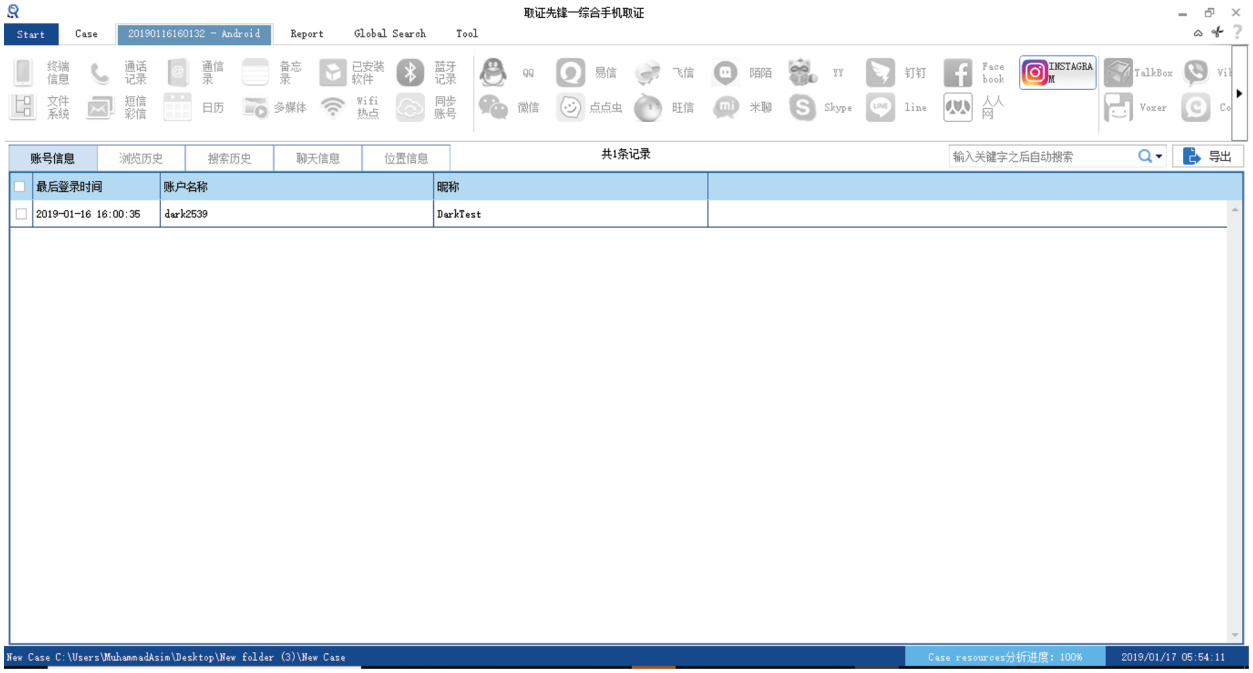


Figure 17: User information retrieved from Meizu Android-based application

9 Instagram Anti-Forensics on Android

In IOS-based devices, it is not possible to perform any anti-forensics techniques. However, for Android-based devices, if suspected culprits are aware of currently employed digital forensics techniques that could get them convicted, the culprits can potentially get away with their criminal activities by simply corrupting

the evidence in the application directory. This can be done easily by simply extracting the database file located in the "\com.instagram.android \databases\direct.db" path of Instagram, and alter its contents, then subsequently save them back into the directory.

To confirm the presented hypothesis, we simulated this scenario, and attempted to change the contents of the text messages placed in "direct.db," and save this direct.db file onto the following path "\com.instagram.android\databases\direct.db."

Here are the details of this experiment.

We sent a message from the Android-based Meizu phone hosting "Dark2539" user to "Mubarik_Muhammad" Instagram user on the iPhone7 device.

Message: "I am DarkTest from mezu"

This message is located in "\com.instagram.android\databases\direct.db" file.

We extracted the "direct.db" file, opened it in the database software, and changed the contents of the message to

"I am wangle from Meizu"

In the next step, we restored this altered 'direct.db' file into the phone.

The file was successfully restored on the Android phone.

Next, we connected the device to the internet, went online, and opened the Instagram Application, to check if our altered text is visible in the application as well.

As expected Instagram displayed the original text, "I am DarkTest from Meizu."

This shows that Instagram maintains a copy of chat on their own servers, and updates the data when users appear online.

We concluded that a criminal may be smart enough to leave his/her phone offline. However another reason that invalidates this anti-forensics technique, the "direct.db" file also displays the date it was modified alongside it, so if the data is changed, it will be quite evident to a forensics analyst.

10 Privacy Issues of Instagram

During the forensics investigation of both the Android and IOS versions of the Instagram Application, we have found a serious privacy issue regarding user's multimedia content stored on the server-side. As in the previous sections, we have explained that pictures and videos shared by Instagram users are not stored in the local directory structure of the application, instead, the messages table of the database file stores only the URL link of the multimedia messages. A person with very little knowledge of digital forensics can extract this URL of multimedia messages and have access to a user's images and videos directly, using any web browser, and without having to verify or input any critical credentials (username or passwords). To test this, we experimented. The user Dark2539 shared a few pictures with the Mubarik_Muhammad account and we extracted the URL of these pictures from the messages table of the database file. All the URLs were available, so we accessed the URL in the Chrome web browser and successfully retrieved all the pictures.

This depicts that the invalidity of user privacy on Instagram; anyone can have access to your personal multimedia information if they has access to these URLs. When Dark2539 shared a picture of the Shanghai River with the Mubarik_Muhammad account, we extracted the URL from the messages table of the database and accessed the image in the Chrome browser. We successfully retrieved the image without inputting any user verification information. However (over time), as we were developing this plugin and writing this article, Instagram updated their application and the URLs extracted from the messages database table do

not work anymore. We noticed a visible change in both URLs saved in an older version and a newer version of Instagram.

URL of Pictures shared in the old version.

https://scontent-sit4-1.cdnInstagram.com/vp/8e2ae39215d58a78971a0fa373565e5d/5BB77629/t51.2885-19/s150x150/35509004_417214398762526_2675262676875083776_n.jpg

URL of Pictures shared in New Version.

https://scontent-lhr3-1.cdnInstagram.com/vp/32769d90c55fe39e08da1cd97c5deb98/5BDF0329/t51.2885-19/s150x150/35509004_417214398762526_2675262676875083776_n.jpg?efg=eyJ1cmxnZW4iOiJ1cmxnZW5fZnJvbV9pZyJ9

Old URLs were un-signed but now Instagram is using signed URLs for their pictures in the new version. URL signing is a way to control time-limited access to HTTP resources which are the pictures in our experiment. In the new URLs, Instagram has added a URL parameter 'efg' which has an encrypted value; this acts as a URL signature. When we open the image URL, the Instagram server decrypts the signatures, and decides whether it is expired or not, based on the timestamp used while creating the URLs originally. Once the URL has expired, the Instagram app receives a new URL with updated signatures while the app is authenticated (logged in). If we try to run an expired URL in the Chrome browser (outside Instagram app scope), the Instagram server will not send us a new URL because we're not logged in. This resolves the privacy issues we found in the old version of Instagram.

11 Conclusion

This was a great learning experience on how Instagram organizes their application on both Android and IOS based devices. As technology keeps enhancing, Instagram also has updated its application over time. We intend to add versioning in our Instagram forensics plugin, so it keeps track of changes and keeps extracting data from all the versions of the Instagram application. In conclusion, I would like to extend my gratitude to "Chen Star Electronic Data Forensic Research Center" Ministry of Public Security Beijing China for their help and guidance in conducting this research.

Acknowledgement: This research article is part of my Ph.D. work by the Chinese scholarship council (CSC) 'www.csc.edu.cn' conducted under the collaboration between "College of Information and Computer Science Hohai University Nanjing China" And "Chen Star Electronic Data Forensic Research Center" Ministry of Public Security Beijing China.

Funding Statement: This research was supported by the Korea Institute for Advancement of Technology (KIAT) Grant Funded by the Korea Government (MOTIE) (P0012724, The Competency Development Program for Industry Specialist) and the Soonchunhyang University Research Fund.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] W. McIver, W. Birdsall and M. Rasmussen, "The Internet and the right to communicate," *First Monday*, vol. 8, no. 12, 2003. [Online]. Available: https://www.firstmonday.org/article/view/1102/1022/.

[2] P. Kallas, "Top 15 most Popular Social Networking Sites and Apps," DreamGrow, 2018. [Online]. Available: https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/.

[3] Anonymous, "Instagram active users," Statista, 2018. [Online]. Available: https://www.statista.com/statistics/253577/number-of-monthly-active-instagram-users/.

[4] J. M. Olsen, "Norwegian billionaire's wife kidnapped, ransom demanded: police," HuffPost, 2019. [Online]. Available: https://www.huffingtonpost.com/entry/norway-businessman-s-wife-abducted-ransom-demanded_us_5c3629bde4b00c33ab5f12d9.

[5] S. G. Punja and R. P. Mislan, "Mobile device analysis," *Small Scale Digit Device Forensics Journal*, 2008. [Online]. Available: https://pdfs.semanticscholar.org/279c/06abd3861704ed20883fbd49b7666b00113b.pdf.

[6] Y. Fedotov, "The drug problem and organized crime, illicit financial flows, corruption, and terrorism 5 world drug report," 2017. [Online]. Available: https://www.unodc.org/wdr2017/field/Booklet_5_NEXUS.pdf.

[7] I. Baggili, "Cyber forensics team launches digital forensics database," University of New Haven, 2019. [Online]. Available: http://www.newhaven.edu/news/releases/2017/cyber-forensics-team-launches-digital-forensics-database.php.

[8] R. Al Mushcab and P. Gladyshev, "Forensic analysis of Instagram and path on an iPhone 5s mobile device," in *IEEE Symposium Computers and Communication ISCC*, pp. 146–151, 2015.

[9] S. C. Ming, "Chang Evidence Gathering of Instagram on Windows 10," *International Journal of Innovative Science, Engineering & Technology*, vol. 3, no. 10, pp. 2348–7968, 2016.

[10] K. Wong, A. C. T. Lai, J. C. K. Yeung, W. L. Lee and P. H. Chan, "Facebook forensics," 5, Valkyrie-X Secur. Res. Group, 2011. [Online]. Available: https://www.fbiic.gov/public/2011/jul/Facebook_Forensics-Finalized.pdf.

[11] M. N. Yusoff, A. Dehghantanha and R. Mahmod, "Forensic investigation of social media and instant messaging services in Firefox OS: Facebook, Twitter, Google+, Telegram, OpenWapp, and Line as case studies," *Contemporary Digital Forensic Investigations Of Cloud And Mobile Applications Elsevier*, pp. 41–62, 2017.

[12] D. Walnycky, I. Baggili, A. Marrington, J. Moore and F. Breitinger, "Network and device forensic analysis of android social-messaging applications," *Digital Investigation*, vol. 14, pp. S77–S84, 2015.

[13] N. Al Mutawa, I. Baggili and A. Marrington, "Forensic analysis of social networking applications on mobile devices," *Digital Investigation*, vol. 9, pp. S24–S33, 2012.

[14] N. Al Mutawa, I. Al Awadhi, I. Baggili and A. Marrington, "Forensic artifacts of Facebook's instant messaging service," in *Int. Conf. for Internet Technology and Secured Transactions*, pp. 771–776, 2011.

[15] M. Bader and I. Baggili, "iPhone 3GS forensics: Logical analysis using apple iTunes backup utility," *Small Scale Digital Device Forensics Journal*, vol. 4, no. 1, pp. 1–15, 2010.

[16] C. Carpene, "Looking to iPhone backup files for evidence extraction," in *Proc. of the 9th Australian Digital Forensics Conf.*, 2011.

[17] Anonymous, "Locate backups of your iPhone, iPad, and iPod touch—Apple Support," 2019. [Online]. Available: https://support.apple.com/en-us/HT204215.