Bitlis Eren University Journal of Science
BİTLİS EREN ÜNİVERSİTESİ FEN BİLİMLERİ DERGİSİ
ISSN: 2147-3129/e-ISSN: 2147-3188
VOLUME: 11 NO: 1 PAGE: 278-293 YEAR: 2022
DOI: 10.17798/bitlisfen.1019621

Digital Forensic Analysis of Wallapop Application on Android Operating System

Elifnur İPEK[1], Erhan AKBAL[1*]

[1]Department of Digital Forensics Engineering, Technology Faculty, Firat University, Elazig, Turkey
(ORCID: 0000-0002-1912-9088) (ORCID: 0000-0002-5257-7560)

Keywords: Application analysis, forensic artifact, wallapop forensic, android OS.

Abstract
The use of second-hand shopping applications is increasing day by day. Applications can be used for product search, product sale / purchase, product search / search, specific filtering for the searched product, product selection by category, saving searched products, product listing and messaging with people. There may be situations that may create legal problems between users in shopping applications. Defamation, fraud, fraudulent products, sale of prohibited substances are carried to judicial authorities. Wallapop app is a second-hand sales app with more than 10 million downloads on google play store. Application were examined by XRY, Praben, Oxygen, Axiom, Ufed and Autopsy Forensic examination programs and no characteristic information about the application could be obtained. In the study, manual forensic analysis of Wallapop application on mobile devices with Android operating system was performed and an examination method was proposed. In the study, manual forensic analysis of Wallapop application on mobile devices with Android operating system is performed and a methodology about the artifacts produced by Wallapop application, their analysis and the relations with each other is presented. The contents of the database files, location information, session information and other data that may be considered as evidence are shown.

1. Introduction

Today, shopping applications where second-hand products are marketed are one of the most preferred applications by mobile / computer users worldwide. One of the most important reasons for this is that the products are cheaper than the store prices in the location on the internet and the product variety is more than the varieties available in the location stores. Together with these applications, it is possible to find the desired product easily by filtering according to the desired features over the internet, to be able to return or exchange the purchased product easily [1]. The necessity of allocating a separate time to visit the stores for shopping and the elimination of the time limit problem for shopping are among the conveniences provided by these applications. In addition, the shopping application is marketed for second-hand products and the lower prices make these applications more attractive. Shopping applications provide users with a lot of flexibility. However, due to its widespread use and the possibilities it provides, it can be realized in negative uses with the application. Fraud, message hiding, selling counterfeit items and insulting people and so on. It is possible to perform such behaviors. In the event of such a situation, the case must be resolved, the offense has to be found and the identity of the perpetrator. Therefore, the analysis of shopping applications has become important for the mobile forensic field [2].

In this study, the method of obtaining remnants left by andorid device memory of Wallapop application is given. The Wallapop application was created by the founders of Miguel Vicente, Agustín Gómez and Gerard Olivé, who are members of Wallapop, founded in 2013. With more than 10,000,000 downloads in the Google Play

[*]Corresponding author: *erhanakbal@firat.edu.tr*

Received: 05.11.2021, Accepted: 06.01.2022

Store, the Wallapop application was named the highest-income startup company in Spain in 2015 with a $ 1 billion transactions [3].

The Wallapop app has features such as selling / buying second hand products, sending / receiving products, searching products, performing specific filtering for the searched product, selecting products by category, registering searched products, product listing, messaging [4]. Despite the possibility of having conversations that may constitute a criminal element in the field of messaging with these features, deception in product sending / receiving, fraud, it has created an important field of study for forensic IT researchers. The data obtained with this study for the Wallapop application have an important role in most studies, such as data from other shopping applications where second-hand products are marketed.

Forensic analysis tools can characteristically examine specific applications [5, 6]. However, it cannot characteristically examine many applications used. For this reason, there are many scientific studies that show how to examine applications that are widely used but cannot be examined by commercial software. Saxena et al. have shown how the Amazon kindle application should be examined on android devices [7]. Kim et al. Have shown what remains of the Android applications left in the cache and how they should be analyzed [8]. Karakoca et al. have conducted benchmarking tests of android messenger applications in terms of digital forensics [9]. Their success in the examination phase was measured. Idowu et al. Recommended some security precautions and method of digital examination of Skype application [10]. Heap memory analysis of Android applications is shown [11]. There are many studies on Android messaging applications. These are BIP Messenger, telegram, Wechat, Kik Messenger, Google Allo Messenger, Skype, Spy, respectively [10, 12-19]. There are also general recommended approaches and studies for instant messaging applications. The main purpose of the study is to present an investigation method when an unknown instant messaging application is encountered [9, 20-23]. In their studies related to Android-based applications that can be made voice calls, methods of obtaining user data left in the application are presented [24, 25]. There are studies that present the methodology of investigating bank applications for mobile devices [26]. The structure of mobile examination tools and their use in digital forensics has been shown [27, 28]. There are studies made for games. Since messaging can be done within the game, content that can be used as digital evidence can be accessed. Sablatura et al. have shown the remains of the PokemonGo application on Android devices [29]. Shariati et al. reviewed the SugarSync application for analysis of file backup applications. The artifact of the application on the device has been shown [30]. Azfar et al. presented a model for the analysis of social media applications working on android [31]. Andrew et al. demonstrated the forensic analysis of the zoom video conferencing application [6].

The main objectives of the proposed analysis methodology in this study,

-Display all the data that may be needed on an android device with Wallapop application.

-Fully reconstruct all user activity by revealing this data and explaining how it can be resolved.

-It is aimed to evaluate the independent data separately and show the correlation between the data which cannot normally be obtained but which may be important for the examiner.

The main contributions of the study are as follows;

-Methodology of forensic analysis of the application running on android operating system is presented.

-With the presented methodology, the completeness and accuracy of the data that can be obtained from Wallapop application was checked. Thus, all the remains on the mobile device have been revealed.

-Wallapop application's communication style, data storage formats and database relations are introduced.

Thus, it will be understood how to re-create user data and to interpret message contents and user behaviors with the data taken from smart mobile device with android operating system using Wallapop application.

2. Analysis Methodology and Tools

In order to find out which data the Wallapop application holds, the wallapop application was installed on the android mobile device, products were searched through the application, profiles of product marketers were examined, users were contacted from the chat area for the products and conversations were made. After these procedures are applied, the data generated on the wallapop application is taken from the mobile device and the analysis procedures are started. For the analysis of the data in the Wallapop application, it was examined what kind of information it would use by using Magnet 3.0, Oxygen Forensic, XRY and Paraben commercial forensic software. However, it has been observed that commercial software does not recognize the data generated by wallapop application. To eliminate this problem, the analysis of the application was performed manually without using commercial software. The steps of the said analysis method are as follows. (1) Android mobile device is root. (2) Files created by wallapop application on the device are extracted with es file manager. (3) The extracted application data is copied to the computer. (4) Application databases (SQLite) are examined with db browser SQLite. (5) The results are reported.

In the application analysis wallapop version 1.86.2 was used. The device is a 4-core, 16 Gb internal storage, 1 GB Ram memory and Android 4.4.2 (kitkat) operating system with a General Mobile brand Discovery model Android device was used. DB Browser SQLite version used in database analysis is 3.11.2, Qt Version is 5.11.3 and SQLite version is 3.27.2. The mobile device is rooted by flashing supers from the boot screen. The ES file manager (version 4.2.0.2.1) application is used to access, view, and extract files that the application holds to the root directory on the mobile device.

2.1. Proposed Methodology

The Wallapop app is a shopping app that markets popular second-hand products around the world. Commercial forensic software and wallapop applications cannot be examined. Therefore, the inability to analyze this application with forensic software has created a problem. As a solution to this problem, a manual examination of the application has been developed. In the first review of the manual wallapop application was installed on the android device. Then, if the device is not rooted, the root operation is performed because the data cannot be obtained. After the root operation, Es File Manager was installed on the device and the application files were accessed. With this access, database files belonging to the application were found and the process of copying these database files to the computer was completed. The wallapop database files copied on the computer were examined and analyzed with DB Browser SQLite. Afterwards, files belonging to the application other than databases were examined and reported. The block diagram of the described methodology is given in Figure 1.

If necessary, subheadings can be added under the main heading [5].

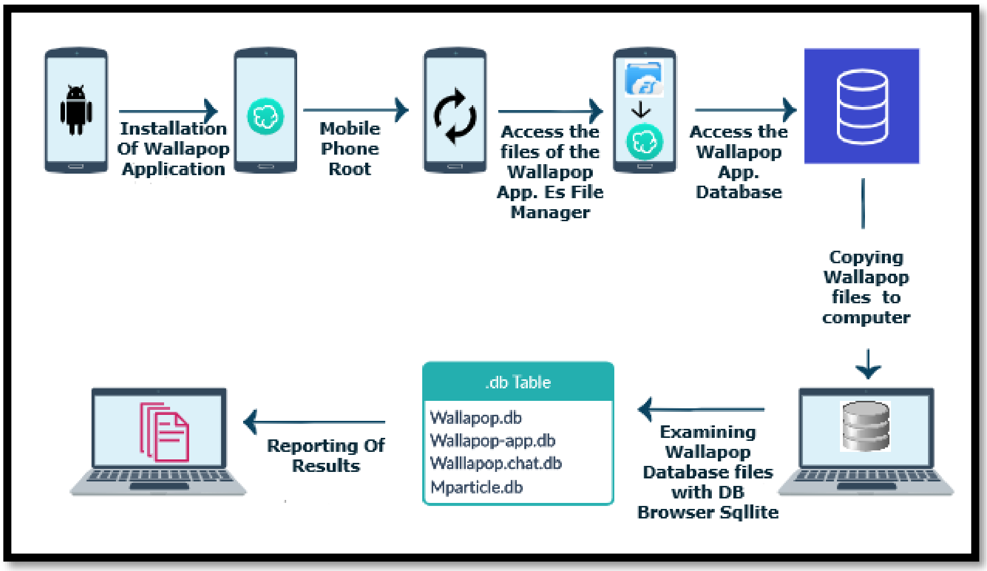
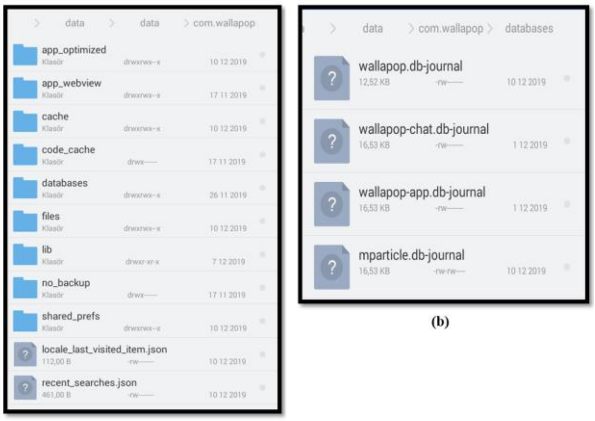

Installation Of Wallapop Application
Mobile Phone Root
Access the files of the Wallapop App. Es File Manager
Access the Wallapop App. Database
Copying Wallapop files to computer
Examining Wallapop Database files with DB Browser Sqllite
.db Table
Wallapop.db
Wallapop-app.db
Walllapop.chat.db
Mparticle.db
Reporting Of Results

Figure 1. Proposed analysis method block diagram

2.2. Wallapop File / Directory Structure and Content

During the forensic analysis of the Wallapop application, information was obtained from the file directory structure of the application, how the wallapop application stores the application data, in which files and directories the stored data is stored, what data the held files contain, and where the application stores the data. The information about the data was obtained by examining the file directory structure and the files held by the application, and the file directory path of the data examined in the forensic analysis is given hierarchically with the titles in Figure 3.

It was found with the Es file manager program that application data is located in the path data / data / com.wallapop. The files and folders in the data / data / com.wallapop path are given in Figure 2. (a). In addition, Figure 2. (b) shows the databases in the database folder located in data / data / com.wallapop path.



> data > data > com.wallapop
app_optimized
Klasör drwxrwx--x 10 12 2019
app_webview
Klasör drwxrwx--x 17 11 2019
cache
Klasör drwxrwx--x 10 12 2019
code_cache
Klasör drwx------ 17 11 2019
databases
Klasör drwxrwx--x 26 11 2019
files
Klasör drwxrwx--x 10 12 2019
lib
Klasör drwxr-xr-x 7 12 2019
no_backup
Klasör drwx------ 17 11 2019
shared_prefs
Klasör drwxrwx--x 10 12 2019
locale_last_visited_item.json
112,00 B -rw------- 10 12 2019
recent_searches.json
461,00 B -rw------- 10 12 2019

(a)

> data > com.wallapop > databases
wallapop.db-journal
12,52 KB -rw------- 10 12 2019
wallapop-chat.db-journal
16,53 KB -rw------- 1 12 2019
wallapop-app.db-journal
16,53 KB -rw------- 1 12 2019
mparticle.db-journal
16,53 KB -rw-rw---- 10 12 2019

(b)

Figure 1. a) Application directory structure **b)** Database directory

2.3. Wallapop Communication Protocols

Wallapop app is a second-hand shopping application available for both iOS and android devices. Chat area has been created on the application for the user to contact the product vendor for the product he wants to purchase. When a message is sent in the buyer / seller communication via chat, the message is stored on the wallapop servers used by the wallapop application. The server sends the sent message repeatedly until the receiving device accepts the message. When the message is accepted by the recipient, the server transfers the stored message to the recipient. The Wallapop application uses the Xmmp protocol, a set of open xml protocols and technologies that allow the two ends of the Internet to transfer any structural information between each other and almost simultaneously. The communication mechanism in Wallapop application is given in Figure 4.

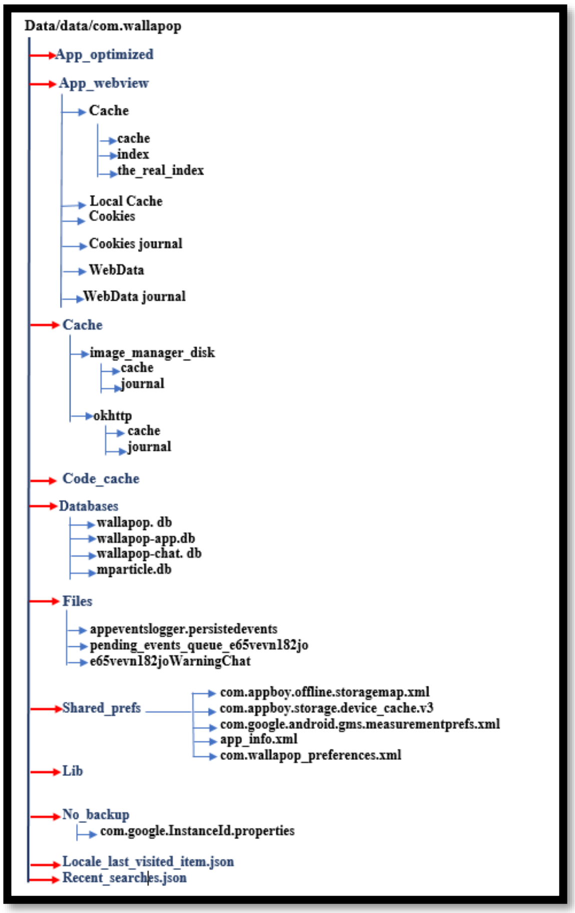


Figure 3. Wallapop application file directory structure

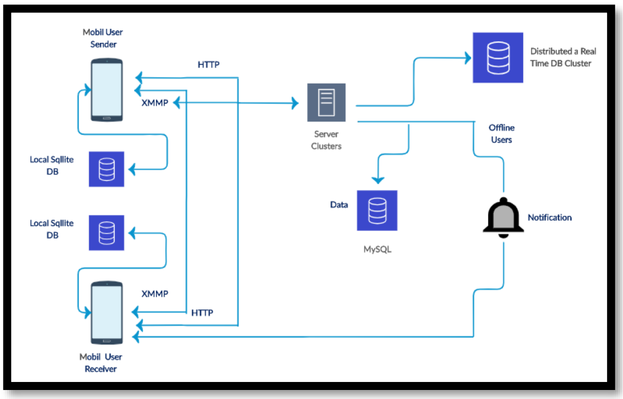


Figure 4. Wallapop application messaging and communication structure

The structure of the mentioned operation is as follows.

1-The message sender decides to send the message from the chat area to the seller of the product of interest on the application.

2-The sender targets the product vendor as the recipient in order to send the message.

3-Sender, to send the message contents to the destination, requests the device information of the recipient from the wallapop server with TCP protocol.

4-The Wallapop server verifies the message request. It then attaches the user information of the message sender to the information of the recipient and forwards the message to the recipient.

5-The message sent by the sender to the recipient is temporarily stored in the wallapop-chat-journal database under the data / data /com.wallapop directory on the sender's phone. It is then saved permanently in the database wallapop-chat.db under the data / data / com.wallapop directory. The main purpose of temporary storage is to prevent possible losses.

6-If the recipient's internet connection is not active, the message continues to be sent repeatedly until the message is forwarded to the recipient.

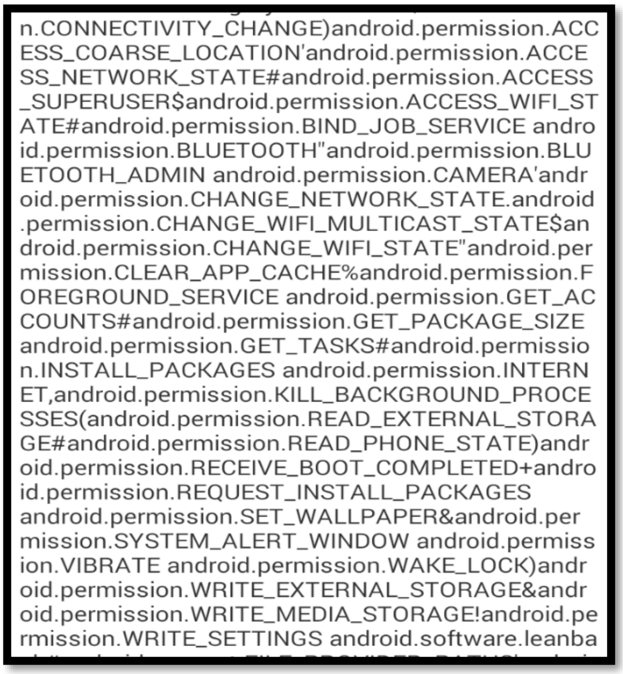
7-When the receiver opens the internet, the message sent by the sender is forwarded to the recipient with notification feature.

8-When the transmission is performed, the server sends information to the message sender that the message has been delivered.

2.4. Device Permissions in AndroidManifest.XML

Androidmanifest.xml files are files that contain the basic information of an application. Wallapop application's AndroidManifest file is found in the apk content of the application. For information about the application, refer to the AndroidManifest file. Figure 5 shows the contents of the AndroidManifest.Xml file that contains permissions for the Wallapop application.

When the AndroidManifest.xml file is examined, it is seen that many permissions are requested for the application. Requested permissions access to full location, access to network information, access to wi-fi networks, change the status of network connections, access to wi-fi multicast mode, access to phone status, camera, access to accounts, internet, read / write access to external storage, bluetooth, cache cleaning, screen darkening, packet installation, system settings read / write permissions were given.



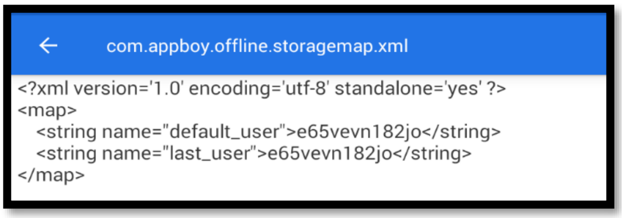
```
n.CONNECTIVITY_CHANGE)android.permission.ACC
ESS_COARSE_LOCATION'android.permission.ACCE
SS_NETWORK_STATE#android.permission.ACCESS
_SUPERUSER$android.permission.ACCESS_WIFI_ST
ATE#android.permission.BIND_JOB_SERVICE andro
id.permission.BLUETOOTH"android.permission.BLU
ETOOTH_ADMIN android.permission.CAMERA'andr
oid.permission.CHANGE_NETWORK_STATE.android
.permission.CHANGE_WIFI_MULTICAST_STATE$an
droid.permission.CHANGE_WIFI_STATE"android.per
mission.CLEAR_APP_CACHE%android.permission.F
OREGROUND_SERVICE android.permission.GET_AC
COUNTS#android.permission.GET_PACKAGE_SIZE
android.permission.GET_TASKS#android.permissio
n.INSTALL_PACKAGES android.permission.INTERN
ET,android.permission.KILL_BACKGROUND_PROCE
SSES(android.permission.READ_EXTERNAL_STORA
GE#android.permission.READ_PHONE_STATE)andr
oid.permission.RECEIVE_BOOT_COMPLETED+andro
id.permission.REQUEST_INSTALL_PACKAGES
android.permission.SET_WALLPAPER&android.per
mission.SYSTEM_ALERT_WINDOW android.permiss
ion.VIBRATE android.permission.WAKE_LOCK)andr
oid.permission.WRITE_EXTERNAL_STORAGE&andr
oid.permission.WRITE_MEDIA_STORAGE!android.pe
rmission.WRITE_SETTINGS android.software.leanba
```

Figure 5. AndroidManifest.xml file content

3. Wallapop Forensic Analysis

3.1. Default Last User Information

From the file in data / data / com.wallapop / shared_prefs/com.appboy.offline.storagemap.xml, last user information has been reached with “last_user”, and default user information has been reached with “default_user”. It is shown in Figure 6 that both users are the same person and the user's name in the application is e65vevn182jo.



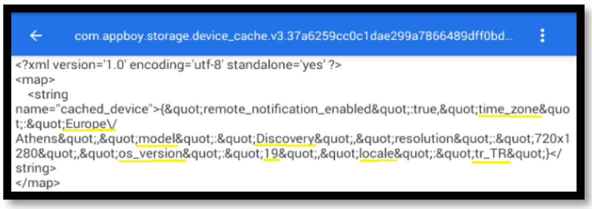
```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="default_user">e65vevn182jo</string>
  <string name="last_user">e65vevn182jo</string>
</map>
```

Figure 6. com.Appboy.Offline.Storagemap.xml file content

In terms of digital forensic, the name of the registered user and the last user information are important in an application. In an event occurring on the application, in the forensic analysis step of the application, the information of who is the registered user of the application on the device and which user was last logged in the application can be accessed. In this respect, it is a digital evidence.

3.2. Device Information

In the file in data / data / com.wallapop / shared_prefs/com.appboy.storage.device_cache.v3, timezone information, model, os_version, and location information of the device on which the application was installed were obtained and these information are given in Figure 7.



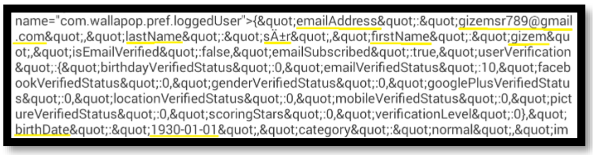
```
com.appboy.storage.device_cache.v3.37a6259cc0c1dae299a7866489dff0bd...
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
   <string
name="cached_device">{&quot;remote_notification_enabled&quot;:true,&quot;time_zone&quo
t;:&quot;Europe\/
Athens&quot;,&quot;model&quot;:&quot;Discovery&quot;,&quot;resolution&quot;:&quot;720x1
280&quot;,&quot;os_version&quot;:&quot;19&quot;,&quot;locale&quot;:&quot;tr_TR&quot;}</
string>
</map>
```

Figure 7. com.Appboy.Storage.Device_Cache.V3 file content

Timezone, location, operating system version information, which can be accessed with device information, may be some of the supporting evidence in digital forensic investigations. For example, if we assume that an event has occurred on the application on the device, we can access the timezone and location of the event and also the brand / model operating system version of the device on which the event took place.

3.3. Time Information

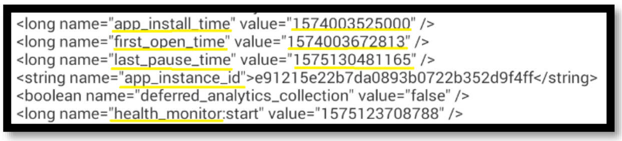
A number of application time information was found in the file path data / data / com.wallapop /shared_prefs/com.google.android.gms.measurementprefs.xml. app_install_time shows when the application was installed on device, first_open_time shows the first boot time, last_pause_time shows the last stop time, app_instance_id shows the application id. health_monitor shows battery power and battery health information. The content of the findings is shown in Figure 8.



```
name="com.wallapop.pref.loggedUser">{&quot;emailAddress&quot;:&quot;gizemsr789@gmail
.com&quot;,&quot;lastName&quot;:&quot;sÄ±r&quot;,&quot;firstName&quot;:&quot;gizem&qu
ot;,&quot;isEmailVerified&quot;:false,&quot;emailSubscribed&quot;:true,&quot;userVerification
&quot;:{&quot;birthdayVerifiedStatus&quot;:0,&quot;emailVerifiedStatus&quot;:10,&quot;faceb
ookVerifiedStatus&quot;:0,&quot;genderVerifiedStatus&quot;:0,&quot;googlePlusVerifiedStatu
s&quot;:0,&quot;locationVerifiedStatus&quot;:0,&quot;mobileVerifiedStatus&quot;:0,&quot;pict
ureVerifiedStatus&quot;:0,&quot;scoringStars&quot;:0,&quot;verificationLevel&quot;:0},&quot;
birthDate&quot;:&quot;1930-01-01&quot;,&quot;category&quot;:&quot;normal&quot;,&quot;im
```

Figure 8. com.wallapop_preferences.xml file content

The date of the application, the first opening time, the last stop time, the unique id number of the user using the application are digital evidence and are important information. Date / time stamps are an essential part of a forensic investigation. Because each operation of the user takes place over time and this recorded time information can provide important information about the event. These timestamps, which were mentioned in the forensic computer review of Wallapop application, were reached and the timestamps that were reached were learned with the timestamp converters in which day, month, year, and hours, minutes, seconds. Time-related data is stored in com.google.android.gms. measurementprefs.xml. The content of the file is shown in Figure 9.

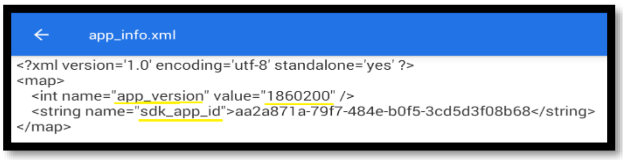


```
<long name="app_install_time" value="1574003525000" />
<long name="first_open_time" value="1574003672813" />
<long name="last_pause_time" value="1575130481165" />
<string name="app_instance_id">e91215e22b7da0893b0722b352d9f4ff</string>
<boolean name="deferred_analytics_collection" value="false" />
<long name="health_monitor:start" value="1575123708788" />
```

Figure 9. com. google. android. gms. measurementprefs.xml file content

3.4. SDK Information

The application version and sdk application id information were found in the path of data / data / com.wallapop / shared_prefs / app_info.xml. App_version shows the version information, sdk_app_id sdk shows the application id information. The content of the file is given in Figure 10.



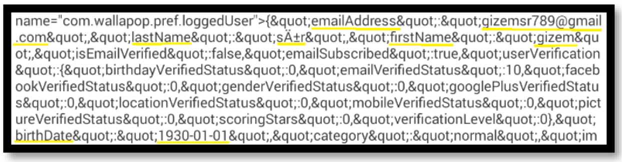
```
app_info.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
   <int name="app_version" value="1860200" />
   <string name="sdk_app_id">aa2a871a-79f7-484e-b0f5-3cd5d3f08b68</string>
</map>
```

Figure 10. App_info.xml file content

In the forensic review of the Wallapop application, some information about the application was found in the app_info.xml file, and the version information and id information in this field are important for forensic information.

3.5. User Information

Data/data/com.wallapop/shared_prefs/com.wallapop_preferences.xml file path has been found to be used by the user when logging in. User's e-mail address, user name and date of birth has been reached from this file. Content of this file is shown in Figure 11. In forensic investigations, if there is an event on an application, the information about who is using the application is extremely important. By obtaining this information, the information of the suspicious user in case of an event on Wallapop application can be learned as described.



```
name="com.wallapop.pref.loggedUser">{&quot;emailAddress&quot;:&quot;gizemsr789@gmail
.com&quot;,&quot;lastName&quot;:&quot;sÄ±r&quot;,&quot;firstName&quot;:&quot;gizem&qu
ot;,&quot;isEmailVerified&quot;:false,&quot;emailSubscribed&quot;:true,&quot;userVerification
&quot;:{&quot;birthdayVerifiedStatus&quot;:0,&quot;emailVerifiedStatus&quot;:10,&quot;faceb
ookVerifiedStatus&quot;:0,&quot;genderVerifiedStatus&quot;:0,&quot;googlePlusVerifiedStatu
s&quot;:0,&quot;locationVerifiedStatus&quot;:0,&quot;mobileVerifiedStatus&quot;:0,&quot;pict
ureVerifiedStatus&quot;:0,&quot;scoringStars&quot;:0,&quot;verificationLevel&quot;:0},&quot;
birthDate&quot;:&quot;1930-01-01&quot;,&quot;category&quot;:&quot;normal&quot;,&quot;im
```

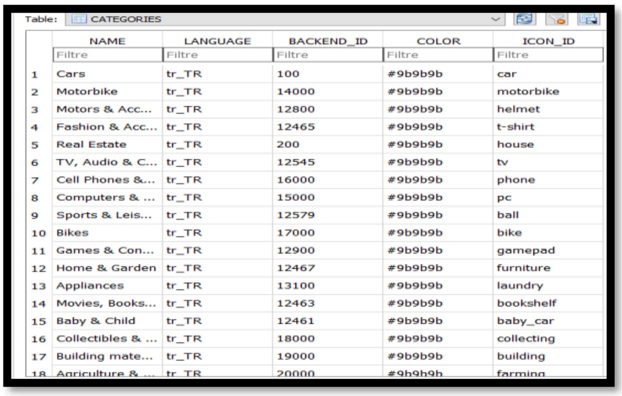
Figure 11.shared_prefs/com.wallapop_preferences.xml file content

4. Analysis of Application Database Files

The Wallapop application has four database files. These; Wallapop.db, Wallapop-chat.db, Wallapop-app.db, Mparticle.db. Application database files are located in the data / data / com.wallapop / databases file path. The database files are transferred to the computer in order to find out which files the databases consist of, and what kind of information these files contain, what the table names are, and the rows and columns of the tables. After that, the contents of the databases were obtained with DB Browser. Databases store the behaviors that users perform on the application. Therefore, forensic analysis of an application can provide clues about a number of topics, such as information about other users with which the user has contacted, message content if contacted, session information, id information, location information. Since the information obtained is important in digital forensic, the data obtained can be considered as digital evidence. In addition, since databases store information in many areas of the application, data from the databases is of great benefit in resolving a forensic event.

When the Categories table is examined, there are a total of 5 columns that hold the names, grammar, product ID number, color code and icon id of the products on the application. The content of these columns is shown in Table 1.

In the Currency table, it is found out which currencies are used on the application. Figure 13 shows the contents of the currency table.

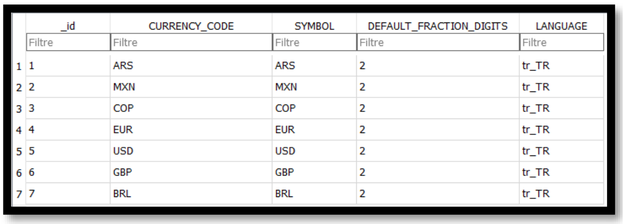


	NAME	LANGUAGE	BACKEND_ID	COLOR	ICON_ID
	Filtre	Filtre	Filtre	Filtre	Filtre
1	Cars	tr_TR	100	#9b9b9b	car
2	Motorbike	tr_TR	14000	#9b9b9b	motorbike
3	Motors & Acc...	tr_TR	12800	#9b9b9b	helmet
4	Fashion & Acc...	tr_TR	12465	#9b9b9b	t-shirt
5	Real Estate	tr_TR	200	#9b9b9b	house
6	TV, Audio & C...	tr_TR	12545	#9b9b9b	tv
7	Cell Phones &...	tr_TR	16000	#9b9b9b	phone
8	Computers & ...	tr_TR	15000	#9b9b9b	pc
9	Sports & Leis...	tr_TR	12579	#9b9b9b	ball
10	Bikes	tr_TR	17000	#9b9b9b	bike
11	Games & Con...	tr_TR	12900	#9b9b9b	gamepad
12	Home & Garden	tr_TR	12467	#9b9b9b	furniture
13	Appliances	tr_TR	13100	#9b9b9b	laundry
14	Movies, Books...	tr_TR	12463	#9b9b9b	bookshelf
15	Baby & Child	tr_TR	12461	#9b9b9b	baby_car
16	Collectibles & ...	tr_TR	18000	#9b9b9b	collecting
17	Building mate...	tr_TR	19000	#9b9b9b	building
18	Agriculture & ...	tr_TR	20000	#9b9b9b	farming

Figure 12. data /data /com.wallapop /databases /Wallapop.db categories table content

Table 1. Categories table data structure

Column name	Content
Name	Knowledge of categorical names of products
Language	Language
Backend_Id	Unique number to which categories correspond
Color	Product color code
Icon_Id	Object name information corresponding to each product



	_id	CURRENCY_CODE	SYMBOL	DEFAULT_FRACTION_DIGITS	LANGUAGE
	Filtre	Filtre	Filtre	Filtre	Filtre
1	1	ARS	ARS	2	tr_TR
2	2	MXN	MXN	2	tr_TR
3	3	COP	COP	2	tr_TR
4	4	EUR	EUR	2	tr_TR
5	5	USD	USD	2	tr_TR
6	6	GBP	GBP	2	tr_TR
7	7	BRL	BRL	2	tr_TR

Figure 2. Currency content

There are 5 columns in the Currency table: id, currency code, currency symbol, default fraction number and language. Table 2 provides the information contained in these columns.

Table 2. Currency table data structure

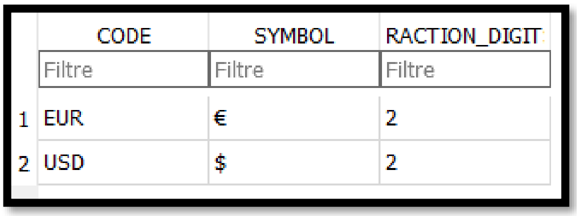
Column Name	Content
Id	Unique number
Currency_Mode	Currency spelling
Symbol	Currency spelling
Defaulth_Fraction_Digit	Default fraction number information
Language	Language

4.2. Wallapop-App.Db

There are 7 tables in the Wallapop-app.db database named currency, image, item, item categories, item images, location, user. This database contains information about the products and users on the application. In the forensic examination, the user information and product information obtained on the application are related to each other and are important as they are digital evidence.

4.2.1. Currency Table

In the Currency table in Wallapop-app.db, the currency of the products the user has examined, the symbols of these currencies and the fraction numbers of the currencies are obtained. Figure 14 shows the visual representation of the Currency table.



	CODE	SYMBOL	RACTION_DIGIT
	Filtre	Filtre	Filtre
1	EUR	€	2
2	USD	$	2

Figure 3 .Currency table view in Wallapop-app.db

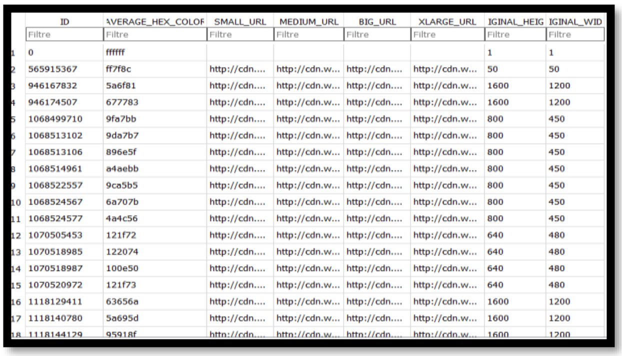
This table consists of 3 columns: code, symbol, fraction_digit. Table 3 contains the information contained in the columns.

Table 3. Currency table data structure in Wallapop-app.db

Column Name	Content
Code	Currency code information
Symbol	Symbolic representation of currency
Fraction_Digit	Currency fraction fraction information

4.2.2. Image Table

In the Image table in Wallapop-app.db, photos of the products the user has examined in the application have been found. The table content view is shown in Figure 15.



	ID	AVERAGE_HEX_COLOF	SMALL_URL	MEDIUM_URL	BIG_URL	XLARGE_URL	IGINAL_HEIG	IGINAL_WID
	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre
1	0	ffffff					1	1
2	565915367	ff7f8c	http://cdn....	http://cdn.w...	http://cdn....	http://cdn.w...	50	50
3	946167832	5a6f81	http://cdn....	http://cdn.w...	http://cdn....	http://cdn.w...	1600	1200
4	946174507	677783	http://cdn....	http://cdn.w...	http://cdn....	http://cdn.w...	1600	1200
5	1068499710	9fa7bb	http://cdn....	http://cdn.w...	http://cdn....	http://cdn.w...	800	450
6	1068513102	9da7b7	http://cdn....	http://cdn.w...	http://cdn....	http://cdn.w...	800	450
7	1068513106	896e5f	http://cdn....	http://cdn.w...	http://cdn....	http://cdn.w...	800	450
8	1068514961	a4aebb	http://cdn....	http://cdn.w...	http://cdn....	http://cdn.w...	800	450
9	1068522557	9ca5b5	http://cdn....	http://cdn.w...	http://cdn....	http://cdn.w...	800	450
10	1068524567	6a707b	http://cdn....	http://cdn.w...	http://cdn....	http://cdn.w...	800	450
11	1068524577	4a4c56	http://cdn....	http://cdn.w...	http://cdn....	http://cdn.w...	800	450
12	1070505453	121f72	http://cdn....	http://cdn.w...	http://cdn....	http://cdn.w...	640	480
13	1070518985	122074	http://cdn....	http://cdn.w...	http://cdn....	http://cdn.w...	640	480
14	1070518987	100e50	http://cdn....	http://cdn.w...	http://cdn....	http://cdn.w...	640	480
15	1070520972	121f73	http://cdn....	http://cdn.w...	http://cdn....	http://cdn.w...	640	480
16	1118129411	63656a	http://cdn....	http://cdn.w...	http://cdn....	http://cdn.w...	1600	1200
17	1118140780	5a695d	http://cdn....	http://cdn.w...	http://cdn....	http://cdn.w...	1600	1200
18	1118144129	95918f	http://cdn....	http://cdn.w...	http://cdn....	http://cdn.w...	1600	1200

Figure 15. Image table content in Wallapop-app.db

This table consists of 8 columns: image id, average_hex_color, small_URL, medium_URL, big_URL, Xlarge_URL, Original height, Original Width. Table 4 shows what these areas are. With the data obtained from the Image table, we can access the photo of the product that the user has looked at on the application with the address given in the table and we can know what the product is. In addition to this, we can reach the actual dimensions of the product photo and the id number that is defined to the product.

Table 4. Image table data structure in Wallapop-app.db

Column Name	Content
Image Id	photo's unique number
Average_Hex_Color	average hex color information
Small_URL	small Url address information
Medium_URL	medium URL address information
Big_URL	large Url address information
Xlarge_URL	longest URL address information
Original Height	Original width info
Original Width	original size information

The small_Url address in line 3 in Figure 15 (A http://cdn.wallapop.com/images/10420/6d/tp/__/c10420p386018089/i946167832.jpg?picturSize = W320) Figure 16 shows the result.

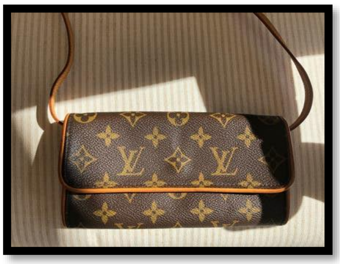
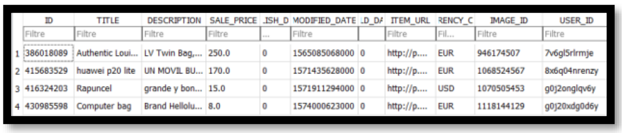


Figure 16. Image from the 3rd row of the Image table

4.2.3. Item Table

In the Item table in Wallapop-app.db, there are informations about items that the user was viewed. Item table consists of 11 columns: id, title, description, sale_price, publish_date, modified_date, sold_date, item_URL, currency_code, image_id, user-id. The table content is shown in Figure 17.



	ID	TITLE	DESCRIPTION	SALE_PRICE	.ISH_D	MODIFIED_DATE	.D_DA	ITEM_URL	RENCY_C	IMAGE_ID	USER_ID
	Filtre	Filtre	Filtre	Filtre	...	Filtre		Filtre	Fil...	Filtre	Filtre
1	386018089	Authentic Loui...	LV Twin Bag,...	250.0	0	1565085068000	0	http://p....	EUR	946174507	7v6gl5rlrmje
2	415683529	huawei p20 lite	UN MOVIL BU...	170.0	0	1571435628000	0	http://p....	EUR	1068524567	8x6q04nrenzy
3	416324203	Rapuncel	grande y bon...	15.0	0	1571911294000	0	http://p....	USD	1070505453	g0j2onglqv6y
4	430985598	Computer bag	Brand Hellolu...	8.0	0	1574000623000	0	http://p....	EUR	1118144129	g0j20xdg0d6y

Figure 17. Wallapop-app.db Item Table content

Table 5. Wallapop-app.db Item Table data structure

Column Name	Content
Id	unique number information of the product (Item_id)
Title	Information of the product (categorical name of the product)

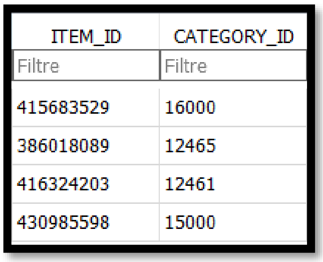
Description	Product description of the product vendor
Sale_Price	Specified price information of the product in question
Publish_Date	Product release date information
Modifies_Date	Information about when a change has been made to the product
Sold_Date	Date of sale
İtem_URL	URL of product sales page
Currency_Code	The currency in which the product is sold
İmage Id	Photo URL address of product
User_Id	Vendor user id information in the application

The information contained in the columns in the table is shown in Table 5. In the Item table, we can find a lot of information about the products the user is interested in. With this data we can obtain important information about the products the user is interested in and the products of interest. For example, the user has looked at a product with the title Rapuncel, and the ID of the vendor of that product has also been reached. When the given table and figure are examined, it can be said that informations gathered from this table have a digital quality for digital investigations.

When we look at line 1 in the table given in Figure 16, we can find out which category the product belongs to from id number. In the title field, we can see the product was found to be entitled “Authentic Louis Vuitton Twin Bag. Here, the product can be obtained with the brand. With sale_price, you can get price information for the product. Modified date is 1565085068000 in table. When we convert this timestamp information, we can see that the posting was last modified on Tuesday, August 6, 2019 09:51:08. Item_URL includes http://p.wallapop.com/i/386018089?_pid=wi&_uid=279296196. When we use this url, we get the sales page of the mentioned bag. The User Id indicates that the bag vendors user id is 7v6gl5rlrmje. (By default, 0 is placed in the Publish / Sold Date columns.)

4.2.4. Item Categories Table

The Item categories table contains the id numbers of the products the user looks at and corresponds with, and which category the product numbers correspond to. This table consists of the Item_id and Category_id columns. Figure 18 shows the Item categories table.



ITEM_ID	CATEGORY_ID
Filtre	Filtre
415683529	16000
386018089	12465
416324203	12461
430985598	15000

Figure 18. Wallapop-app.db Item Categories table view

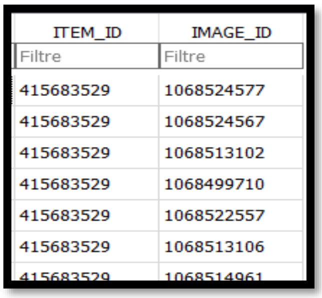
The information contained in the columns is given in Table 6. Referring to the table given in Figure 17, the product ID of the product involved in a forensic event on the application can be categorically identified which ID number corresponds to. In the case of a forensic examination, if there is not enough information in the category information of the product, more content can be found in the product table by using the product_id number. Or, if there is not enough information in the product table in reverse, the item categories table can be used to obtain the product categorical id number and additional information can be found in the category table.

Figure 17 shows that item_id number is 415683529 in the first line. This id is shown to be 16000 in the category_id number. When looking at the Categories table, it was found that the product is in the Cell phones & Accesories category.

Table 6. Wallapop-app.db Item Categories table data structure

Column Name	Content
Item_Id	Unique number of product the user has looked at on the application
Category_Id	Unique categorical number of the product the user has looked at on the application

4.2.5. Item_Images Table



ITEM_ID	IMAGE_ID
Filtre	Filtre
415683529	1068524577
415683529	1068524567
415683529	1068513102
415683529	1068499710
415683529	1068522557
415683529	1068513106
415683529	1068514961

Figure 19. Item_Images table view

The Item_Images table contains the id numbers of the products the user is looking at, corresponding with, and which photo id number of those product numbers. Item_images table consists of 2 columns, item_id and image_id. This table view is shown in Figure 19.

By looking at the table, the product id number of the product photo can be obtained from the product id number of the product involved in a forensic event, and then we can obtain more information from the forensic examination based on the photo links with other tables. Or vice versa, the product id number can be easily seen from the item_images table and the product id number corresponds to the product id number, and more digital evidence is obtained by looking at the other information in the product table.

4.2.6. Location Table

The Location table contains information about the locations of the products the user corresponded with on the application. Location table consists of 8 columns: id, approximate_latitude, approximated_longitude, Km_error, City, Zip, instance_from_you, currency code. The information contained in the columns is shown in Table 7.

By looking at the “Location” table, we can access location information about the product or vendor involved in a forensic event on the application. In addition, we can reach the seller's city information, latitude and longitude values, and distance from us in kilometers. Thus, with the obtained address information, many digital data can be used.

Table 7. Location table data structure

Column Name	Content
Id	Unique id for location
Approximated_latitude	The latitude position of the advertised product
Approximated_longitude	The longitude position of the advertised product
Km_error	Error rate in Km
City	In which city the advertised product is located
Zip	City postal code / area code
Instance_from_you	How far the product is from the user viewing the product
Currency_code	Currency used by cities

4.2.7. User Table

The User table is a table that contains information about the user. The User table contains information about the person using the application, as well as the contacts the user communicates with. The table contains User_Id, Legacy-Id, Micro-Name, Birth_Date, Image-Id, Location_Id, Sold_Count, Selling_Count, Receiwed_Reviews_Count, _Verified_Status, Scoring_Stars, Verification_Level, Gender, Banned, Online, Favorites_Count, Purchased_Count, and Notification_Read_Pending_Count_Count columns. Table contents are shown in Table 8.

User table is a table where critical forensic data about the user can be obtained. The user's birth date, mail account and many detailed information showing the user's activity in the application can be accessed through this table.

4.3. Wallapop-Chat.Db

Wallapop-Chat.db contains messages on the application and information about messaging. It is the most important database file in terms of digital forensics. Instead of communicating through the instant messaging application, users can use these applications for private messaging. Therefore, the application that appears innocent can be used as a tool for criminals. In the examination made with commercial software, no message content related to chat processes could be reached. Wallapop-Chat.db basically consists of 2 tables, Chat-message and Conversation.

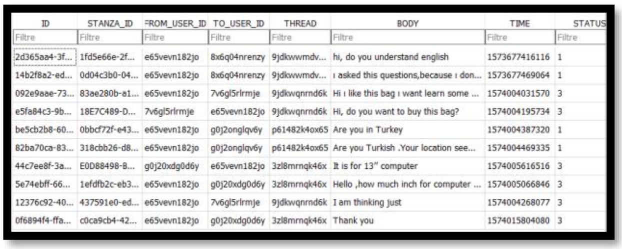
Table 8. User table data structure

Column Name	Content
Id	Unique user id
Legacy_Id	If available, the old id number
Micro_Name	User name
Birth_Date	Birthday of the user
Image_Id	Profile photo id
Location_Id	Location information
Sold_Count	Number of products he/she sold
Selling_Count	Number of products on sale
Receiwed_Reviews _Count	Number of comments received
E-Mail_Verified_Status	E-mail verification status (1 or 0)
Scoring_Stars	Number of stars users receive on the application
Gender	User's gender (1 or 0)
Banned	Users' ban status
Online	Online status of users (online 1, offline 0)

Favorites_Count	Favorite users number
Purchased_Count	Number of products purchased
Notification_Read_ Pending_Count	Number of pending notifications to read
Verification_Level	Verification levels of users

4.3.1. Chat-message Table

The chat-message table contains information about the messages on the application. This table consists of 8 columns: id, stanza_id, from_user_id, to_user_id, thread, body, time, status. The chat-message table is shown in Figure 20.



ID	STANZA_ID	FROM_USER_ID	TO_USER_ID	THREAD	BODY	TIME	STATUS
Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre
2d365aa4-3f...	1fd5e66e-2f...	e65vevn182jo	8x6q04nrenzy	9jdkwwmdv...	hi, do you understand english	1573677416116	1
14b2f8a2-ed...	0d04c3b0-04...	e65vevn182jo	8x6q04nrenzy	9jdkwwmdv...	ı asked this questions,because ı don...	1573677469064	1
092e9aae-73...	83ae280b-a1...	e65vevn182jo	7v6gl5rlrmje	9jdkwqnrnd6k	Hi ı like this bag ı want learn some ...	1574004031570	3
e5fa84c3-9b...	18E7C489-D...	7v6gl5rlrmje	e65vevn182jo	9jdkwqnrnd6k	Hi, do you want to buy this bag?	1574004195734	3
be5cb2b8-60...	0bbcf72f-e43...	e65vevn182jo	g0j2onglqv6y	p61482k4ox65	Are you in Turkey	1574004387320	1
82ba70ca-83...	318cbb26-d8...	e65vevn182jo	g0j2onglqv6y	p61482k4ox65	Are you Turkish .Your location see...	1574004469335	1
44c7ee8f-3a...	E0D88498-B...	g0j20xdg0d6y	e65vevn182jo	3zl8mrnqk46x	It is for 13" computer	1574005616516	3
5e74ebff-66...	1efdfb2c-eb3...	e65vevn182jo	g0j20xdg0d6y	3zl8mrnqk46x	Hello ,how much inch for computer ...	1574005066846	3
12376c92-40...	437591e0-ed...	e65vevn182jo	7v6gl5rlrmje	9jdkwqnrnd6k	I am thinking just	1574004268077	3
0f6894f4-ffa...	c0ca9cb4-42...	e65vevn182jo	g0j20xdg0d6y	3zl8mrnqk46x	Thank you	1574015804080	3

Figure 20. Chat-Message table in Wallapop-chat.db

Table 9. Chat-Message table data structure

Column Name	Content
Id	The numerical structure that increases with every new registry (set by SQLite)
From_User_Id	Message sender id
To_User_Id	Message reciever id
Thread	The number of the message header
Body	Message body
Time	Information when the message was created, when it was sent
Status	Number of messages in the messaging area / page

The information contained in the columns is shown in Table 9. If there is messages only written by user, the status column set to 1.

4.3.2. Conversation Table

The Conversation table holds information about which product the conversations / messages are about, the date of creation of the last message, the format of the message. This table consists of 7 columns: id, legacy_id, user_id, item_id, message_read_pending_count, last_message_create_date, message_media_type. The information contained in these columns is given in Table 10.

Table 10. Conversation table data structure

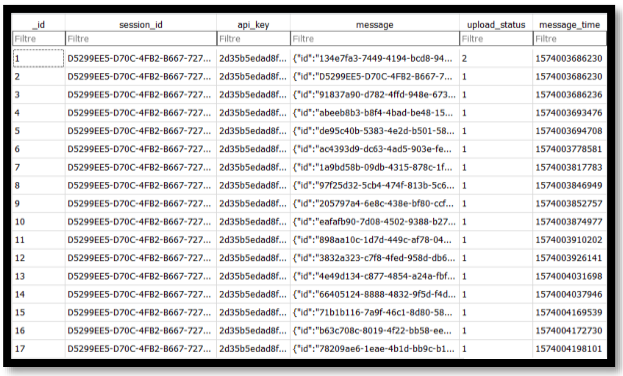
Column Name	Content
Id	Conversation_id
Legacy_Id	Legacy id of message
User_Id	The user number of the messaging users on the application
Item_id	Product id information indicating which product the messaging is for
Message_Read_ Pending_Count	Number of messages waiting to be read
Last_Message_ Create_Date	Date when the message was last created
Message_Media_Type	Data type of message

4.4. Analysis of Session Information

Mparticle.db stores data about sessions opened on the application. Mparticle.db consists of 3 tables: messages, session and sqllite sequence. By means of these tables, content that can be considered as forensic evidence such as the user's activity on the application, when he / she logs off, and the duration of the session can be obtained. For this purpose, the tables in the database file should be examined in detail.

4.4.1. Messages Table

Message table consists of 6 columns: id, session_id, api_key, message, upload_status, message_time. This table generally includes information such as session time, session content, session id. The visual representation of the Messages table is shown in Figure 21.



_id	session_id	api_key	message	upload_status	message_time
Filtre	Filtre	Filtre	Filtre	Filtre	Filtre
1	D5299EE5-D70C-4FB2-B667-727...	2d35b5edad8f...	{"id":"134e7fa3-7449-4194-bcd8-94...	2	1574003686230
2	D5299EE5-D70C-4FB2-B667-727...	2d35b5edad8f...	{"id":"D5299EE5-D70C-4FB2-B667-7...	1	1574003686230
3	D5299EE5-D70C-4FB2-B667-727...	2d35b5edad8f...	{"id":"91837a90-d782-4ffd-948e-673...	1	1574003686236
4	D5299EE5-D70C-4FB2-B667-727...	2d35b5edad8f...	{"id":"abeeb8b3-b8f4-4bad-be48-15...	1	1574003693476
5	D5299EE5-D70C-4FB2-B667-727...	2d35b5edad8f...	{"id":"de95c40b-5383-4e2d-b501-58...	1	1574003694708
6	D5299EE5-D70C-4FB2-B667-727...	2d35b5edad8f...	{"id":"ac4393d9-dc63-4ad5-903e-fe...	1	1574003778581
7	D5299EE5-D70C-4FB2-B667-727...	2d35b5edad8f...	{"id":"1a9bd58b-09db-4315-878c-1f...	1	1574003817783
8	D5299EE5-D70C-4FB2-B667-727...	2d35b5edad8f...	{"id":"97f25d32-5cb4-474f-813b-5c6...	1	1574003846949
9	D5299EE5-D70C-4FB2-B667-727...	2d35b5edad8f...	{"id":"205797a4-6e8c-438e-bf80-ccf...	1	1574003852757
10	D5299EE5-D70C-4FB2-B667-727...	2d35b5edad8f...	{"id":"eafafb90-7d08-4502-9388-b27...	1	1574003874977
11	D5299EE5-D70C-4FB2-B667-727...	2d35b5edad8f...	{"id":"898aa10c-1d7d-449c-af78-04...	1	1574003910202
12	D5299EE5-D70C-4FB2-B667-727...	2d35b5edad8f...	{"id":"3832a323-c7f8-4fed-958d-db6...	1	1574003926141
13	D5299EE5-D70C-4FB2-B667-727...	2d35b5edad8f...	{"id":"4e49d134-c877-4854-a24a-fbf...	1	1574004031698
14	D5299EE5-D70C-4FB2-B667-727...	2d35b5edad8f...	{"id":"66405124-8888-4832-9f5d-f4d...	1	1574004037946
15	D5299EE5-D70C-4FB2-B667-727...	2d35b5edad8f...	{"id":"71b1b116-7a9f-46c1-8d80-58...	1	1574004169539
16	D5299EE5-D70C-4FB2-B667-727...	2d35b5edad8f...	{"id":"b63c708c-8019-4f22-bb58-ee...	1	1574004172730
17	D5299EE5-D70C-4FB2-B667-727...	2d35b5edad8f...	{"id":"78209ae6-1eae-4b1d-bb9c-b1...	1	1574004198101

Figure 21. Messages table in Mparticle.db

It is seen in Figure 21 that there are user data in the table. The Messages column contains the id of the session information, the product category, the item id, the title of the product being viewed. This information is variable for each row.

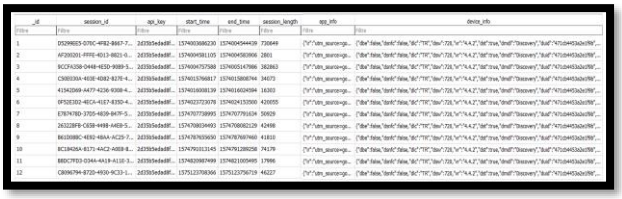
Because each session has different activities. The data structure of the data held in the columns is given in Table 11.

Table 11. Messages table data structure

Column Name	Content
Id	Row ids
Session_Id	Unique number for sessions
Api-Key	Api_key of the application
Message	Contains information about the content of the sessions.
Upload_Status	Upload state information (number)
Message_Time	Time of sessions

4.4.2. Sessions Table

The Sessions table contains the start and end times of sessions, id numbers, application and device information from which the session was opened. Id, session_id, api_key, start_time, end_time, session_length, app_info, device_info are the columns. Table content is shown in Figure 22.



_id	session_id	api_key	start_time	end_time	session_length	app_info	device_info
Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre
1	D5299EE5-070C-4F82-8667-7...	2d35b5edad8f...	1574003686230	1574004544439	730649	{"ir":"utm_source=go...	{"dbe":false,"dsnfc":false,"dlc":"TR","dosv":728,"vr":"4.4.2","dst":true,"dmdl":"Discovery","duid":"471cb4453a2e1f98",...
2	AF200201-FFFE-4D13-8821-0...	2d35b5edad8f...	1574004581105	1574004583906	2801	{"ir":"utm_source=go...	{"dbe":false,"dsnfc":false,"dlc":"TR","dosv":728,"vr":"4.4.2","dst":true,"dmdl":"Discovery","duid":"471cb4453a2e1f98",...
3	9CCFA358-0448-4E5D-9089-5...	2d35b5edad8f...	1574004757588	1574005147986	382863	{"ir":"utm_source=go...	{"dbe":false,"dsnfc":false,"dlc":"TR","dosv":728,"vr":"4.4.2","dst":true,"dmdl":"Discovery","duid":"471cb4453a2e1f98",...
4	C50E030A-403E-4D82-827E-4...	2d35b5edad8f...	1574015766817	1574015808744	34073	{"ir":"utm_source=go...	{"dbe":false,"dsnfc":false,"dlc":"TR","dosv":728,"vr":"4.4.2","dst":true,"dmdl":"Discovery","duid":"471cb4453a2e1f98",...
5	41542D69-A477-4236-9308-4...	2d35b5edad8f...	1574016008139	1574016024594	16303	{"ir":"utm_source=go...	{"dbe":false,"dsnfc":false,"dlc":"TR","dosv":728,"vr":"4.4.2","dst":true,"dmdl":"Discovery","duid":"471cb4453a2e1f98",...
6	0F52E3D2-4ECA-41E7-835D-4...	2d35b5edad8f...	1574023723078	1574024153500	420655	{"ir":"utm_source=go...	{"dbe":false,"dsnfc":false,"dlc":"TR","dosv":728,"vr":"4.4.2","dst":true,"dmdl":"Discovery","duid":"471cb4453a2e1f98",...
7	E787478D-3705-4839-847F-5...	2d35b5edad8f...	1574707738995	1574707791634	50929	{"ir":"utm_source=go...	{"dbe":false,"dsnfc":false,"dlc":"TR","dosv":728,"vr":"4.4.2","dst":true,"dmdl":"Discovery","duid":"471cb4453a2e1f98",...
8	263228FB-C658-4498-A4E8-5...	2d35b5edad8f...	1574708034493	1574708082129	42498	{"ir":"utm_source=go...	{"dbe":false,"dsnfc":false,"dlc":"TR","dosv":728,"vr":"4.4.2","dst":true,"dmdl":"Discovery","duid":"471cb4453a2e1f98",...
9	B61D088C-4E92-48AA-AC25-7...	2d35b5edad8f...	1574787655650	1574787697460	41810	{"ir":"utm_source=go...	{"dbe":false,"dsnfc":false,"dlc":"TR","dosv":728,"vr":"4.4.2","dst":true,"dmdl":"Discovery","duid":"471cb4453a2e1f98",...
10	8C18426A-8171-4AC2-A0E8-8...	2d35b5edad8f...	1574791013145	1574791289258	74179	{"ir":"utm_source=go...	{"dbe":false,"dsnfc":false,"dlc":"TR","dosv":728,"vr":"4.4.2","dst":true,"dmdl":"Discovery","duid":"471cb4453a2e1f98",...
11	88DC7FD3-D34A-4A19-A11E-3...	2d35b5edad8f...	1574820987499	1574821005495	17996	{"ir":"utm_source=go...	{"dbe":false,"dsnfc":false,"dlc":"TR","dosv":728,"vr":"4.4.2","dst":true,"dmdl":"Discovery","duid":"471cb4453a2e1f98",...
12	C8096794-8720-4930-9C33-1...	2d35b5edad8f...	1575123708366	1575123756719	46227	{"ir":"utm_source=go...	{"dbe":false,"dsnfc":false,"dlc":"TR","dosv":728,"vr":"4.4.2","dst":true,"dmdl":"Discovery","duid":"471cb4453a2e1f98",...

Figure 22. Session table in Mparticle.db file

There are many fields of user data in the table. Information may be obtained from these fields as evidence. Specifically, the usage period of the application and the start and end times of the application session are evidence. Content information is given in Table 12.

Table 12. Sessions Table data structure

Column Name	Content
Id	Row ids
Session_Id	Unique number for sessions
Api_key	Api_key of the application
Start_Time	Session start time
End_Time	Session end time
Session_Length	Total time of the session
App_Info	Information about the application
Device_Info	Information about the device

Device_info provides information about the device on which the application is installed.

4.4.3. SQLite Sequence Table

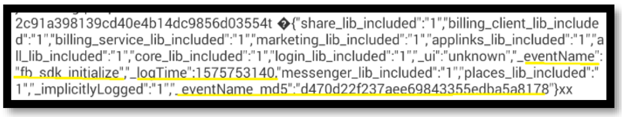
The "SQLite sequence" table holds the number of rows in the sessions and messages tables. The table consists of 2 columns: "Name" and seq. The Name column holds the names of the Messages and sessions tables. The Seq column contains the number of lines that the Messages and sessions tables have.

5. Log and Cache Analysis

The accuracy of the data in the application is confirmed by log examinations. There are important files related to log and cache in the "data / data / com.wallapop / files" directory in the device storage of the Wallapop application. AppEventsLogger, pending_events_queue files contain data that can be considered as evidence. Cache information of the application was reached in the Cache folder. Cache records the operations performed on the application, viewed product photos and content about the internet. Even if the user deletes some contents from the device, the contents have been reached by cache analysis.

5.1. AppEventsLogger

"data / data / com.wallapop / files / appeventslogger.persistedevents" file has been observed to have records of an ongoing event on the application. From these records, the name of the event and the time information were obtained. In addition, it was found that the event name was encrypted with md5 encryption method. The information found is shown in Figure 23.



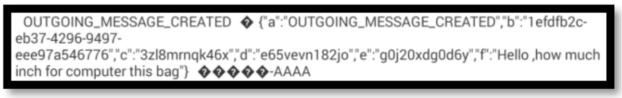
```
2c91a398139cd40e4b14dc9856d03554t �{"share_lib_included":"1","billing_client_lib_include
d":"1","billing_service_lib_included":"1","marketing_lib_included":"1","applinks_lib_included":"1","a
ll_lib_included":"1","core_lib_included":"1","login_lib_included":"1","_ui":"unknown","_eventName":
"fb_sdk_initialize","_logTime":1575753140,"messenger_lib_included":"1","places_lib_included":"
1","_implicitlyLogged":"1","_eventName_md5":"d470d22f237aee69843355edba5a8178"}xx
```

Figure 23. AppEventesLogger file

In the figure, when the value held by eventName_md5 is converted with md5 converter, this event name was found to be fb_sdk_initialize. The time stamp information that logTime holds is translated with timestamp converter and it is reached that the real time is 08/12/2019 00:12:20.

5.2. Pending Event Records

In the file "data/data/com.wallapop/files/ pending_events_queue_e65vevn182jo", the user's recorded information about pending events has been reached (e65vevn182jo is user id). This file contains information about the message sent. The available data are shown in Figure 24.



```
OUTGOING_MESSAGE_CREATED � {"a":"OUTGOING_MESSAGE_CREATED","b":"1efdfb2c-
eb37-4296-9497-
eee97a546776","c":"3zl8mrnqk46x","d":"e65vevn182jo","e":"g0j20xdg0d6y","f":"Hello ,how much
inch for computer this bag"} �����-AAAA
```

Figure 24. pending_events_queue file

Figure 24 provides information about an outgoing message. Here, "a" is pending event information, "b" is stanza_id, "c" is conversation_id (thread), "d" is sender id, "e" is message id and "f is message text.

5.3. Photo Caches

The cache information is located in the file path "data/data/com.wallapop/cache/image_manager_disk_cache". The photos of the products viewed on the application were recorded with different names. In addition to the saved photo files, a journal file has been created for these photo files. An example of a cached photo is shown in Figure 25.

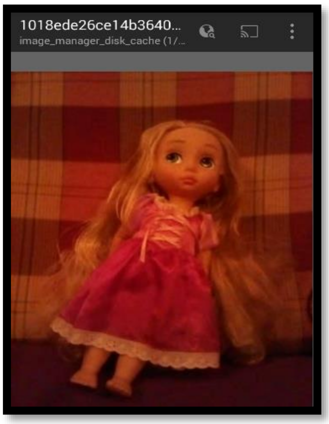
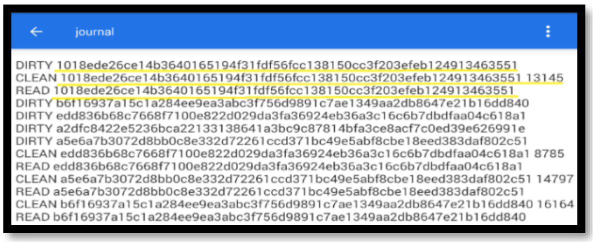


Figure 25. photo obtained from cache

The photograph shown in the Figure 25 is a product that the user has looked at on the application. In addition, the user has contacted the product vendor for this product. More information about the product can be found in the message, item and categories tables.



```
DIRTY 1018ede26ce14b3640165194f31fdf56fcc138150cc3f203efeb124913463551
CLEAN 1018ede26ce14b3640165194f31fdf56fcc138150cc3f203efeb124913463551 13145
READ 1018ede26ce14b3640165194f31fdf56fcc138150cc3f203efeb124913463551
DIRTY b6f16937a15c1a284ee9ea3abc3f756d9891c7ae1349aa2db8647e21b16dd840
DIRTY edd836b68c7668f7100e822d029da3fa36924eb36a3c16c6b7dbdfaa04c618a1
DIRTY a2dfc8422e5236bca22133138641a3bc9c87814bfa3ce8acf7c0ed39e626991e
DIRTY a5e6a7b3072d8bb0c8e332d72261ccd371bc49e5abf8cbe18eed383daf802c51
CLEAN edd836b68c7668f7100e822d029da3fa36924eb36a3c16c6b7dbdfaa04c618a1 8785
READ edd836b68c7668f7100e822d029da3fa36924eb36a3c16c6b7dbdfaa04c618a1
CLEAN a5e6a7b3072d8bb0c8e332d72261ccd371bc49e5abf8cbe18eed383daf802c51 14797
READ a5e6a7b3072d8bb0c8e332d72261ccd371bc49e5abf8cbe18eed383daf802c51
CLEAN b6f16937a15c1a284ee9ea3abc3f756d9891c7ae1349aa2db8647e21b16dd840 16164
READ b6f16937a15c1a284ee9ea3abc3f756d9891c7ae1349aa2db8647e21b16dd840
```

Figure 26. Content of image _manager _disk_ cache/ journal

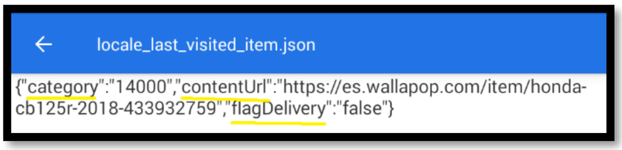
Figure 26 shows some of the contents of the log for photograph caches. it is understood from the name of the file that the first 3 lines are recorded for the photograph shown in Figure 26. It is observed that "dirty", "clean" and "read" commands are used. "DIRTY" indicates that a new entry has been made to the log file, "CLEAN" indicates that an entry has been successfully added and accessible in the log file, and "READ" indicates that the added entry is readable.

5.4. Okhttp Caches

Okhttp is used to send and receive http requests to the web server. The okhttp file saved in the application contains the cache data related to okhttp. A separate file is saved in this folder for each okhttp information. In addition to the files saved in the folder, there is also a journal file.

5.5 Last Visited Product Information

In the file "data/data/com.wallapop/ locale_last_visited_item.json" the category number, url content information and flag information of the last viewed product are given in the application. Figure 27 shows the contents of this file.



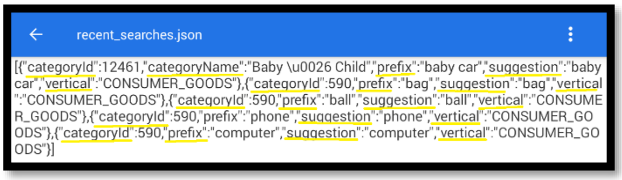
```
{"category":"14000","contentUrl":"https://es.wallapop.com/item/honda-
cb125r-2018-433932759","flagDelivery":"false"}
```

Figure 27. Information of last reviewed product

The latest product in the application is a Honda cb125r 2018 model motorcycle. It is observed that the product category is 14000 aka motorbike.

5.6 Recently Searched Product Information in Searches Area

In the "data/data/com.wallapop/ recent_searches.json" file, information about what the searched products are, what category they are in, how they were written when searching, and what the spelling suggestion is, if it is misspelled, were found. Figure 28 shows the contents of the file for the product being searched.



```
[{"categoryId":12461,"categoryName":"Baby \u0026 Child","prefix":"baby car","suggestion":"baby
car","vertical":"CONSUMER_GOODS"},{"categoryId":590,"prefix":"bag","suggestion":"bag","vertical
":"CONSUMER_GOODS"},{"categoryId":590,"prefix":"ball","suggestion":"ball","vertical":"CONSUME
R_GOODS"},{"categoryId":590,"prefix":"phone","suggestion":"phone","vertical":"CONSUMER_GO
ODS"},{"categoryId":590,"prefix":"computer","suggestion":"computer","vertical":"CONSUMER_GO
ODS"}]
```

Figure 28. Contents of recent_seraches.json file

Table 13 shows what the marked fields in the content of "recent_searches.json" mean.

Table 13. Information and descriptions kept in the "recent_searches.json" file

Parameter	Data information
Category_Id	ID of the searched product
Category_Name	Name of the searched product
Prefix	Prefix of the searched product
Suggestion	Suggestion of the searched product
Vertical	By default, customer property is written

6. CONCLUSION

Forensic investigations are concerned with obtaining the data of users from digital evidences by appropriate methods and reporting them to be submitted to the legal process. The first stage of forensic investigations is the process of acquiring data from digital material. It aims to investigate and reveal the contents of the offender's material that may constitute a criminal element. Therefore, all system, application and user contents on their devices are examined. In this study, user data left on mobile device of Wallapop application used for second hand trading on android operating system was analyzed. Since application data cannot be detected by commercial review software, it has been shown that manual review is required. The findings have an important function in judicial processes. Communication architecture of the application, user permissions, user data stored in database files, log and cache memory traces are explained. Wallapop.db, Wallapop-chat.db, Wallapop-app.db and Mparticle.db files hold important data. Wallpop.db provides access to the categorical classification of products and information on the currency of the products. The Wallapop-chat.db file has been shown to hold data specifically related to in-app communication. With this file, it has been shown that important contents are obtained in offenses such as insults, illegal correspondence and concealment of communication. With the Wallapop-app.db file, information about the products and users on the application was reached. The Mparticle.db file contains data about the session information and location information on the application. Important information for forensic investigations, such as when the application was opened / closed and how long it was used was obtained. In addition to database files, important information belonging to the user has been reached in cache and log files. In particular, data such as last searched, examined product, picture of the examined product are shown. The results presented by the study provide an important reference in the analysis and interpretation of the Wallapop application on android mobile devices. It is planned to examine how the evidence left by the application can be analyzed in IOS devices in future studies.

Contributions of the authors

All authors contributed equally to the study.

Conflict of Interest Statement

There is no conflict of interest between the authors.

Statement of Research and Publication Ethics

The study is complied with research and publication ethics

References

[1] B. Deebak and H. Zahmatkesh, "Forensic analysis in social networking applications", in *Security in IoT Social Networks*, Elsevier, 2021, pp. 133-147.

[2] X. Zhang, F. Breitinger, E. Luechinger, and S. O'Shaughnessy, "Android application forensics: A survey of obfuscation, obfuscation detection and deobfuscation techniques and their impact on investigations," *Forensic Science International: Digital Investigation*, vol. 39, p. 301285, 2021.

[3] P. C. Rubio and J. L. Micó, "Communications strategies in the new economy: the case studies of wallapop, westing and fotocasa/La planificacion estrategica de la comunicacion en la era digital. Los casos de studio de Wallapop, Westing y Fotocasa/ Planificacao estrategica da comunicacao na era digital. os casos dos estudos de wallapop, westwing e fotocasa," Vivat Academia, no. 147, pp. 125-139, 2019.

[4] E. Hernández Padilla, "Análisis de wallapop y su competencia," 2019.

[5] G. C. Schipper, R. Seelt, and N.-A. Le-Khac, "Forensic analysis of Matrix protocol and Riot. im application," *Forensic Science International: Digital Investigation*, vol. 36, p. 301118, 2021.

[6] A. Mahr, M. Cichon, S. Mateo, C. Grajeda, and I. Baggili, "Zooming into the pandemic! A forensic analysis of the Zoom Application," *Forensic Science International: Digital Investigation*, vol. 36, p. 301107, 2021.

[7] A. Saxena, J. Walker, and V. Kulkarni, "Forensic Analysis on Kindle and Android," in *Digital Forensic Education*, Springer, 2020, pp. 155-174.

[8] H. Kim, D. Kim, W. Jo, and T. Shon, "Digital Forensic Analysis using Android Application Cache Data," in *2019 International Conference on Platform Technology and Service (PlatCon)*, 2019, pp. 1-4.

[9] A. Karahoca, D. Karahoca, and S. K. Bağirici, "Forensic benchmarking for android messenger applications", *Technology*, vol. 10, no. 01, pp. 926-934, 2019.

[10] S. Idowu, E. D. Dominic, S. Okolie, and N. Goga, "*Security Vulnerabilities of Skype Application Artifacts: A Digital Forensic Approach*," 2019.

[11] J. Zhang, E. Chengyuan, and A. Hu, "A Method of Android Application Forensics Based on Heap Memory Analysis", in *Proceedings of the 2nd International Conference on Computer Science and Application Engineering*, 2018: ACM, p. 186.

[12] L. Zhang, F. Yu, and Q. Ji, "The forensic analysis of WeChat message," *in 2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC)*, 2016, pp. 500-503.

[13] K. Pettersson, "*Android Messaging Investigator: Forensic text analysis tool for SMS, Kik and Hangouts conversations*", 2018.

[14] V. Agrawal and S. Tapaswi, "Forensic analysis of Google Allo messenger on Android platform", *Information & Computer Security*, vol. 27, no. 1, pp. 62-80, 2019.

[15] E. Akbal, I. Baloglu, T. Tuncer, and S. Dogan, "Forensic analysis of BiP Messenger on android smartphones", *Australian Journal of Forensic Sciences*, pp. 1-20, 2019.

[16] D. Hintea, A. Sangins, and R. Bird, "Forensic Analysis of the Telegram Instant Messenger Application on Android Devices", *in European Conference on Cyber Warfare and Security*, 2018: Academic Conferences International Limited, pp. 217-XII.

[17] T. Y. Yang, A. Dehghantanha, K.-K. R. Choo, and Z. Muda, "Windows instant messaging app forensics: Facebook and Skype as case studies," *PloS one*, vol. 11, no. 3, p. e0150300, 2016.

[18] S. Hutchinson and U. Karabiyik, "Forensic Analysis of Spy Applications in Android Devices", 2019.

[19] S. Wu, Y. Zhang, X. Wang, X. Xiong, and L. Du, "Forensic analysis of WeChat on Android smartphones", *Digital investigation*, vol. 21, pp. 3-10, 2017.

[20] H. Zhang, L. Chen, and Q. Liu, "Digital Forensic Analysis of Instant Messaging Applications on Android Smartphones", *in 2018 International Conference on Computing, Networking and Communications (ICNC)*, 2018, pp. 647-651.

[21] 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", *in Contemporary Digital Forensic Investigations Of Cloud And Mobile Applications*, Elsevier, 2017, pp. 41-62.

[22] T. Y. Yang, A. Dehghantanha, K.-K. Choo, and Z. Muda, "Investigating America Online instant messaging application: data remnants on Windows 8.1 client machine", *in Contemporary Digital Forensic Investigations Of Cloud And Mobile Applications,* Elsevier, 2017, pp. 21-39.

[23] C. Anglano, M. Canonico, and M. Guazzone, "Forensic analysis of the chatsecure instant messaging application on android smartphones", *Digital investigation*, vol. 19, pp. 44-59, 2016.

[24] C. Sgaras, M. Kechadi, and N.-A. Le-Khac, "Forensics Acquisition and Analysis of instant messaging and VoIP applications", *arXiv preprint arXiv:1612.00204,* 2016.

[25] T. Dargahi, A. Dehghantanha, and M. Conti, "Forensics Analysis of Android Mobile VoIP Apps", *in Contemporary Digital Forensic Investigations Of Cloud And Mobile Applications,* Elsevier, 2017, pp. 7-20.

[26] A. P. Kuncoro, I. Riadi, and A. Luthfi, "Mobile Forensics Development of Mobile Banking Application using Static Forensic", *International Journal of Computer Applications*, vol. 975, p. 8887, 2017.

[27] R. Umar, I. Riadi, and G. M. Zamroni, “Mobile forensic tools evaluation for digital crime investigation”, *International Journal on Advanced Science, Engineering and Information Technology*, vol. 8, no. 3, pp. 949-955, 2018.

[28] T.-I. Kitsaki, A. Angelogianni, C. Ntantogian, and C. Xenakis, “A forensic investigation of Android mobile applications”, *in Proceedings of the 22nd Pan-Hellenic Conference on Informatics*, 2018, ACM, pp. 58-63.

[29] J. Sablatura and U. Karabiyik, “Pokémon go forensics: An android application analysis”, *Information,* vol. 8, no. 3, p. 71, 2017.

[30] M. Shariati, A. Dehghantanha, and K.-K. R. Choo, “SugarSync forensic analysis”, *Australian Journal of Forensic Sciences*, vol. 48, no. 1, pp. 95-117, 2016.

[31] A. Azfar, K.-K. R. Choo, and L. Liu, “An android social app forensics adversary model”, *in 2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2016, pp. 5597-5606.