

Forensic Analysis of Modern E-Business Applications

Muhammad Asim¹, Ammar Rafiq¹, Muhammad Asgher Nadeem², Omer Usman³, Danial Niazi⁴, Sadaqat Ali Ramay⁵, Kalsoom Safdar⁶, and Muhammad Usman Younus^{6*}

¹Department of Computer Sciences, NFC-Institute of Engineering and Fertilizers Research Faisalabad, Faisalabad, Pakistan.

²Department of Computer Science and IT, Thal University Bhakhar, Bhakhar, Pakistan.

³Senior Project Manager, ARC, Saudia Arabia.

⁴Group Marketing Manager, AFI-Rentals, UAE.

⁵Department of Computer Science TIMES Institute, Multan, Pakistan.

⁶Department of Computer Science and IT, University of Jhang, Jhang, Pakistan.

*Corresponding Author: Muhammad Usman Younus. Email: usman1644@gmail.com

Received: November 21, 2023 Accepted: January 26, 2024 Published: March 01, 2024

Abstract: In this paper, a plugin is developed for our automated digital forensics framework to extract and preserve the evidence from the IOS-based mobile phone application, Olx. This plugin extracts personal details from Olx users, e.g, user name, mobile number, User Location, Country name, State name, City name, Last check-in attempt, Ad Images between different Olx users. While developing the plugin, we identified resources available in IOS-based devices holding key forensics artifacts. We highlighted the poor privacy scheme employed by Olx. This work has shown how the sensitive data posted in the Olx 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 Olx user without any critical credential verification. We also employed the anti-forensics method on the Olx IOS 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 Olx mobile application directories on IOS-based mobile phones.

Keywords: Digital forensics; Olx; Mobile application forensics; Antiforensics; 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 Olx, (primarily used via its mobile application) which has over a billion registered users [2]. It is a social networking application that lets users to buy, sell, or find anything in their community. Users of Olx, register themselves with a unique user ID and password. This visual sharing platform has become more popular nowadays because for buying and selling services and goods such as electronics, fashion items, furniture, household goods, cars, bikes etc. The "story" functions as a secondary newsfeed, situated atop the main personal newsfeed of every Instagram user. Through such activities, the platforms help people from across the globe, to connect and form new relationships, in a very interactive manner. However, unbeknownst to its users, applications such as Olx

provide personal information of its users to other users, which can be potentially dangerous [3]. In today's technologically advanced era, people are using platforms such as Olx for the purchasing and selling of items. Buyer and Seller connect with each other freely on Olx, without comprehending the potential danger they are exposed to [4]. Over the years, OLX has become a common place for fraud, especially sellers who post fake advertisements to dupe buyers upon receiving advance payment, and fraudulent buyers who engage in UPI scam, phishing, and sending fake SMS and emails of payment confirmation [5]. Cases of online theft, copyright infringement, extortion, kidnapping 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 [6].

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 [7]. 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 [8]. 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 [9]. So many applications and so many technologies are being created and continuously updated, that forensic investigators cannot keep up [10]. "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 [11]. In this paper, we have studied the forensic artifacts of the Olx application on IOS phones. We implemented code to automatically extract these forensics artifacts using our forensic framework environment, which is capable of extracting evidence from 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).

In this paper, we developed a plugin for our automated digital forensics framework to extract and preserve the evidence from the IOS-based mobile phone application, Olx. This plugin extracts details Olx users, e.g., name, user name, mobile number, ID, direct text and picture messages exchanged between different Olx users(seller,buyer). While developing the plugin, we identified resources available in IOS-based devices holding key forensics artifacts. We highlighted the poor privacy scheme employed by Olx. This work, has shown how the sensitive data posted in the Olx mobile application can easily be reconstructed, and how the traces, as well as the URL links of pictures, can be used to access the privacy of any Olx user without any critical credential verification.

2. Associated Research

During the 1980s and 1990s, the growth of computer crime prompted law enforcement agencies to form specialist groups, generally at the national level, to handle the technical aspects of investigations [12]. The phrase "computer forensics" was used in academic literature in 1992 (although it had been in use informally previous to that); a research by Collier and Spaul sought to legitimize this new field to the forensic science community [13].

Because of the rapid pace of growth, there was a lack of standards and training. K. Rosenblatt said in his 1995 book "High-Technology Crime: Investigating Cases Involving Computers" that "the greatest forensic problem faced by law enforcement sectors is seizing, preserving, and evaluating evidence stored on a computer." Despite the fact that most forensic procedures, such as fingerprinting and DNA testing, are done by professionally trained professionals, gathering and interpreting computer data is frequently delegated to patrol officers and detectives [14].

Recent research has targeted variety of mobile phones, which involved different strategies for acquiring analyzing the local storage of the mobile phone and the information by extracting data from these devices [15]. Findings revealed that valuable traces of data could be extracted using both physical method or a logical method. The physical technique necessitates jailbreaking the system, which results in a little data alteration. However, Zdziarski's most recent approach obtains a physical-logical picture of an iPhone

without jailbreaking it [16]. It is considered the best forensic method for acquiring iPhone and has been evaluated by the National Institute of Standard and Technology [17].

Forensic investigation of smart phone crimes used a variety of acquisition approaches. Al-Mutawa demonstrated a method for doing forensic analysis on three popular mobile applications: Myspace, Facebook, and Twitter, on three distinct smart phones: Android, iPhone, and Blackberry [18].

Every gadget was subjected to its own set of tests. Every application on the smart phones was used to complete a sequence of tasks. After that, he made a computer file of each application and saved it in the device's internal memory [19]. The backup files were forensically acquired and analyzed, revealing a range of database files and plist files related to mobile applications. Using the SQLite dB browser to see each database file and examining the data returned gave significant trails of evidence [20]. Forensic analysis on various android phone applications which belonged to the categories like bank and network carrier was performed [21].

Analysis aimed to discover sensitive data associated with the user of the cell phone. The two major methodologies that were used for forensic analysis included disk analysis code analysis. Findings discovered the failure of incorporating privacy and security to protect user's sensitive information on these mobile apps despite taking critical measures. Lwin and Htar examined the digital forensics of Android phone mobile banking and mobile pay apps used in Myanmar [22].

Due to the sensitivity of users' sensitive data, digital forensic on banking apps was developed. Three distinct mobile banking apps and five mobile cash apps were picked as the most popular in Myanmar. For the extraction of valuable information, different extraction and analysis technologies were employed from free sources. According to the findings, some applications did not save information, while others encrypted the user's credentials and stored them on the user's Android phone. The methodologies for standard investigation that are supported manually, don't seem to be expandable for wider range of mobile phone apps. While performing analysis dynamically, it is difficult to operate as there is lot of burden for generating runtime environment that can provide convenience to operating system variations and possible paths for different programs. Fordroid is a complete automated platform that was proposed by Xiaodong Lin and can be used for performing forensic analysis on android applications [23].

Statically inter component analysis on APKs of android was conducted using Fordroid. Moreover, it identified location of information stored in internal memory of android phone. Messenger mobile applications like WhatsApp and Viber were investigated by Neha S.Thakur on android phones using a Universal Forensic Extraction Device (UFED) [24]. Personal chats, encoded timestamps, and files transmitted and received were among the digital artefacts retrieved from the WhatsApp program, however the place where these items were kept on internal storage was not discovered.

Rusydi Umar and Imam Riadi examined and assessed Belka soft Evidence and WhatsApp key extractor, which are often utilized for extracting digital artefacts of the newest WhatsApp version (with.crypt12 encryption) on android phones [25]. For searching out artifacts for creating evidence that can be useful in investigation of crime an identification was created. Once the artifacts were successfully analyzed, they proceeded to the information retrieval method. A tool was required that can decrypt and extract information because WhatsApp is provided with encryption feature. Android phone Samsung galaxy (version:5.0.1) WhatsApp (version: 2.17.147) were used for analysis. Experimental results showed that WhatsApp text message artifacts were not found but document, video images artifacts were successfully extracted.

Skype provides a very secure and localized method of efficient communication that leaves very little trace on static media, making digital forensics less effective. Matthew Simon demonstrated a set of generic target artefacts that detailed information that may be targeted for data extraction [26]. For retrieving evidence physical memory was explored. Skype was used under controlled analysis and memory was collected from targeted machine. Forensic analysis concluded that the recovery of targeted information can be recovered.

Muchamad Kukuh Tri Haryanto conducted forensic analysis of IMO application for android phones [27]. For this experiment, two distinct Android phones were utilized. The first stage was to install the IMO program on each android phone, followed by numerous user actions on the IMO application and the creation of a logical picture of each android phone. The main objective of forensic analyst was to find multiple ways to evaluate the folders structure of IMO mobile application. Discovered results un-concealed

different folders of IMO application that were obtained by forensic acquisition process were stored on mobile phone internal storage. Facebook app stores tremendous information which may facilitate in reconstructing the sequence of crime. Agrawal performed an in-depth analysis of the Facebook application on the latest android version of a virtual phone [28].

The concept of virtual android device using genymotion emulator was used to discover various artifacts stored by Facebook application which may be presented as crucial evidence within the Court of Law. Examiners can use WhatsApp artefacts like contacts, messages, and attachments to retrieve evidence during an investigation. Auqib Lone assessed and presented a method for obtaining artefacts from Whatsapp and Viber (mobile apps) [29]. During the forensic examination of the WhatsApp application, SQLite db files were discovered. The msgstore.db file folder contained the details of the talks between the user and their contacts. The wa.db file folder included a complete list of the user's contacts. The database files found comprised a full list of WhatsApp contacts, including phone numbers, display names, and timestamps.

a) If the decision tree predicts a yes result, a warning is sent to the farmer.

b) If the technique predicts the result as no, a warning is sent to the farmer.

This is a similar study in which authors improved the performance of the DT model in relation to irrigation management, a hybrid approach involving the integration of DT and genetic techniques (GA) was proposed to provide the optimal decision tree model for predicting irrigation schedules was Implemented [7-1]. The irrigation schedule event takes the form of a binary classification problem leading to a decision to irrigate or not [20-1].

A KNN model that will calculate the characteristics and contains reveal the crop which is perfect for the system drawing. The bitmap that a definite region instantly [1]. Environmental parameters like soil type, rain, humidity, etc. are collected and crop prediction is completed around with all the accuracy for your crops done utilizing the KNN [21-1].

The focus is on proposing IoT-based smart farming systems that help farmers get recommendations based on various factors such as humidity, temperature, pH, humidity, and rainfall [4-1]. The system also focuses on suggesting fertilizers to farmers based on factors such as nitrogen, phosphorus, and potassium levels in the soil [9-1]. Various machine learning techniques such as Decision Trees, Naive Bayes, Support Vector Machines, Logistic Regression, Random Forest, and XGBoost were applied to the training data set and compared based on model accuracy. XGBoost was used for the prediction model as it showed the highest accuracy [11-1].

In a study by Chen et al, he used an ensemble learning model to predict the watering of crops based on an agricultural IoT system [19-1]. About four models, including linear SVR, Adaboost DT, and RF, which support linear regression, were trained to evaluate the performance of the intelligent irrigation system[15-1]. An IoT framework was implemented along with a platform and mobile application to enable the model to be used for real-time irrigation planning [5-1]. Another framework provides an ensemble learning irrigation model based on agricultural IoT systems [20-1].

They mixed regression and classification techniques and applied them to stack and boost different procedures. The proposed model achieves an accuracy of 94.27 [30].

In the section above, it has been discussed in the study that they mixed regression and classification techniques and then reservations to different techniques for better results in irrigation prediction [31]. In our research, we've decided to experiment with ensemble learning techniques on classification procedures & techniques [8-1].

3. Test Environment and Requirements

This framework was developed in Visual Studio with C# editor/Interpreter tools installed. Below is a complete list of all the hardware and software tools used to perform the forensics analysis of IOS based mobile application (OLX):

- IOS device (iPhone 5s, v.12.4.9)
- USB Data Cable • Micro SD card
- Olx Mobile Application (v. 11.52.1)
- Local Backup Application (iTunes v12.11.4.15)
- Microsoft Visual Studio 2019
- SQLite Database Browser (v 3.12.2)

- Windows 10 Operating System
- Web Browser (Internet Explorer)
- Forensic Workstation (min 4GB RAM)
- iMazing App 2.14.2
- Plist editor (2.5)

4. Forensics Analysis of IOS-Based OLX Application

4.1 Retrieval of the OLX Directory Structure

We chose a mobile application based on popularity in Pakistan because this framework is designed for the use of Pakistan law enforcement agencies and public security organizations to help solve cases more easily, and hence provide a more safe and secure social life within Pakistan cities. A picture of the front end for our framework can be seen in [Fig. 1].

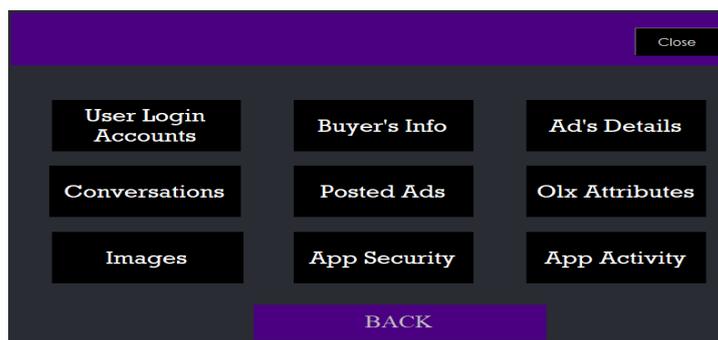


Figure 1. Forensics framework front end

We performed forensics analysis of the OLX application on Apple IOS device. For this activity, we first installed the OLX application on an IOS device. In this specific experiment, we used an IOS device (iPhone 5s, with IOS version 12.4.9).

4.2 Android Devices Data Extraction

The second stage was to extract data using iTunes which helped us extract the contents of “AppDomain-asia.olx.pk” 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 IOS Olx App

After acquiring the directories from an IOS 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 Olx app so that data is generated and stored into the Olx directory structure. We created a user name on Olx to generate the forensics artifacts in the Olx 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 Olx on IOS (AppDomain-asia.olx.pk): C:\Users\DEll\AppData\Roaming\AppleComputer\MobileSync\Backup\831c5d6e283be97807887feda53502095d7c1e05-20210617-134514 to store all the directories and files. Directories of AppDomain-asia.olx.pk are shown in Fig. 3.

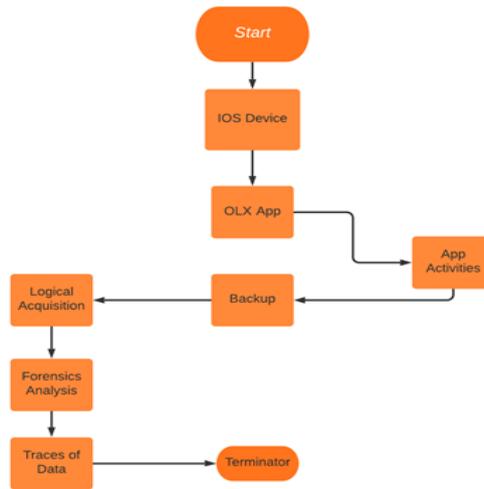


Figure 2. Flow diagram of the analysis process

The “Documents” directory and “Library” directory hold important forensics artifacts for digital forensics analysis of Olx. “Preferences” directory inside Library folder contains Plist files that hold ‘location’, ‘userPhoneNumber’, ‘Mobileversion’, current country, and other important information about the user of the application. The Documents directory contains the direct messages exchanged between the user and other Olx users.

Table 1. Activities performed

Mobile & Application	Activity
<ol style="list-style-type: none"> 1. IOS iPhone 5s 2. AppDomain-asia-olx.pk 	<ol style="list-style-type: none"> 1. Creating Olx account using phone number 2. Managing profile 3. Posting different Ads in Olx application 4. Observing different sale items 5. Conversations with the buyers or costumers

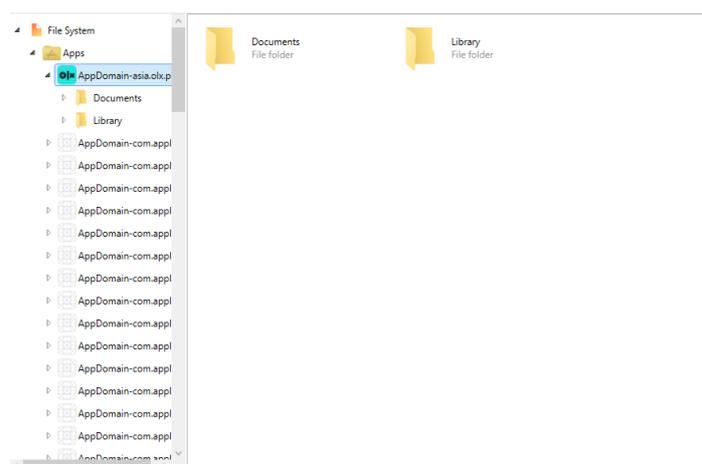


Figure 3. Directory structure of AppDomain-asia.olx.pk package extracted from IOS device

In the following section, we will describe the anatomy of the “C:\Users\rasoo\Desktop\fyp\Library\Preferences\ panamera.olx.pk” file. Snapshot of this file is presented in Fig. 4, and we have listed important forensics artifacts in Tab. 2

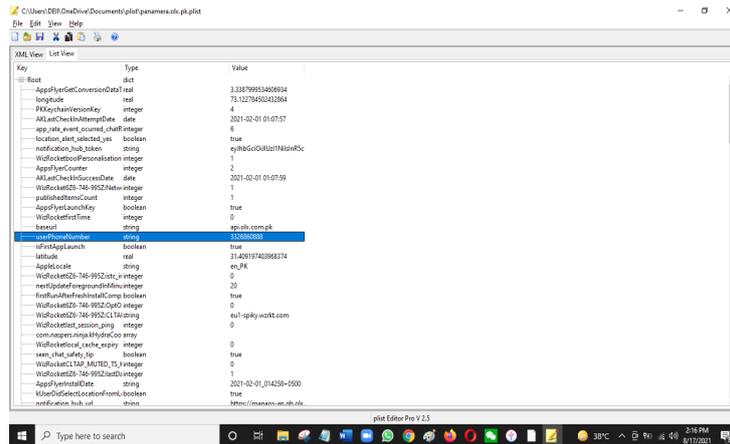


Figure 4. Contents of panamera.olx.pk

This Plist 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 Plist files and directories contain user bootstrap services information, cookies, etc. The next directory of our interest is the Documents directory, which contains direct messages (in the file named 'ChatDataModel.db') exchanged between the registered user of the mobile application, and other Olx users. Fig. 5 shows the relations and tables in the Chat-DataModel.sqlite file of Olx; 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 panamera.olx.pk

Forensic Information	Key	Value
User Location	longitude	73.12287
User Location	latitude	31.04569
User phone number	userPhoneNumber	3326860888
User country location	country	en_PK
user mobile version	version number	11.52.1
user last login method	last login mode	Phone
language of App	currentLanguage	en
User login email	userEmail	93326860888@olxpk.com

It can also be observed that the ZBODY and ZFROM are the current user's id to identify the user of the current Olx mobile application. As Olx 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, while ZTIMESTAMP is the time for when the message was received.

6. Forensics Analysis of IOS-Based OLX 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 & Baggili [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.

Name	Type	Schema
Z_PK	INTEGER	"Z_PK" INTEGER
Z_ENT	INTEGER	"Z_ENT" INTEGER
Z_OPT	INTEGER	"Z_OPT" INTEGER
ZINTERVENTIONACTIONID	INTEGER	"ZINTERVENTIONACTIONID" INTEGER
ZINTERVENTIONID	INTEGER	"ZINTERVENTIONID" INTEGER
ZISAUTOREPLY	INTEGER	"ZISAUTOREPLY" INTEGER
ZISREPLIED	INTEGER	"ZISREPLIED" INTEGER
ZCONVERSATIONDATA	INTEGER	"ZCONVERSATIONDATA" INTEGER
ZQUESTIONID	INTEGER	"ZQUESTIONID" INTEGER
ZAUDIODURATION	INTEGER	"ZAUDIODURATION" INTEGER
ZMESSAGEDATA	INTEGER	"ZMESSAGEDATA" INTEGER
ZTIMESTAMP	TIMESTAMP	"ZTIMESTAMP" TIMESTAMP
ZBODY	VARCHAR	"ZBODY" VARCHAR
ZDATESTRING	VARCHAR	"ZDATESTRING" VARCHAR
ZFROM	VARCHAR	"ZFROM" VARCHAR
ZMESSAGEID	VARCHAR	"ZMESSAGEID" VARCHAR
ZREPLYTO	VARCHAR	"ZREPLYTO" VARCHAR
ZSTATUS	VARCHAR	"ZSTATUS" VARCHAR
ZSUGGESTIONS	VARCHAR	"ZSUGGESTIONS" VARCHAR

Figure 5. Table relation in ChatDataModel.sqlite

7. Key Forensics Artifacts Identification of OLX in IOS-based Device

Logical acquisition of an IOS device using the backup facility, provides a wealth of information for forensic analysis. After being installed on the IOS device, the OLX application creates the following directory structure as shown in Fig. 6 In the "AppDomain-asia.olx.pk" directory of the iPhone, a directory with "ChatDataModel.sqlite" name is created to store the data of OLX 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 "Apps\ AppDomain-asia.olx.pk \Documents\ ChatDataModel.sqlite" file.

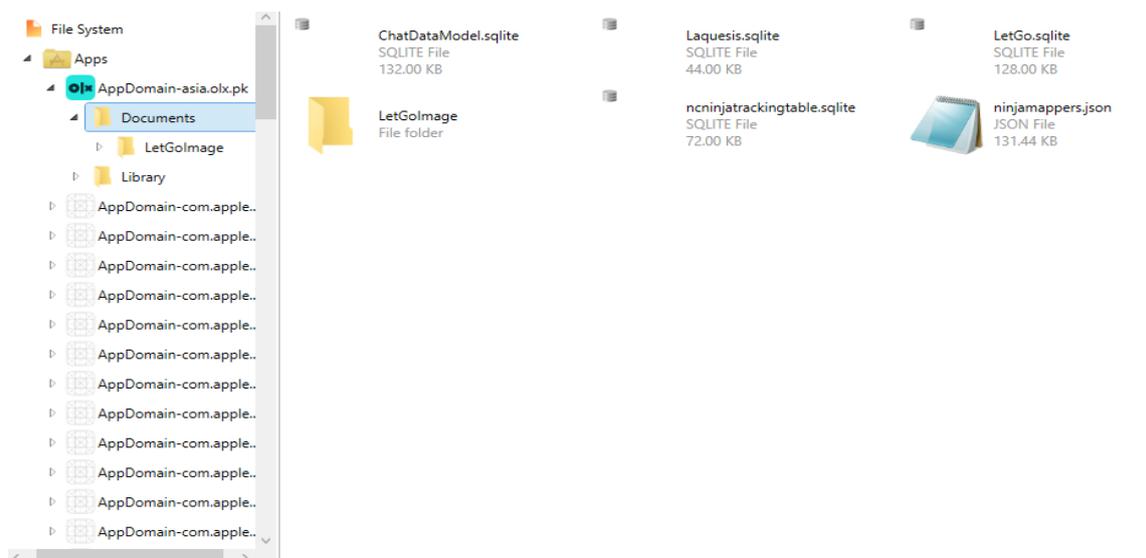


Figure 6. Asia OLX directory of the iPhone

The second important file that contains significant digital artifacts related to the OLX user in IOS devices is the "panamera.olx.pk.plist," which is located in the "Apps\ AppDomain-asia.olx.pk \Library\ Preferences." directory.

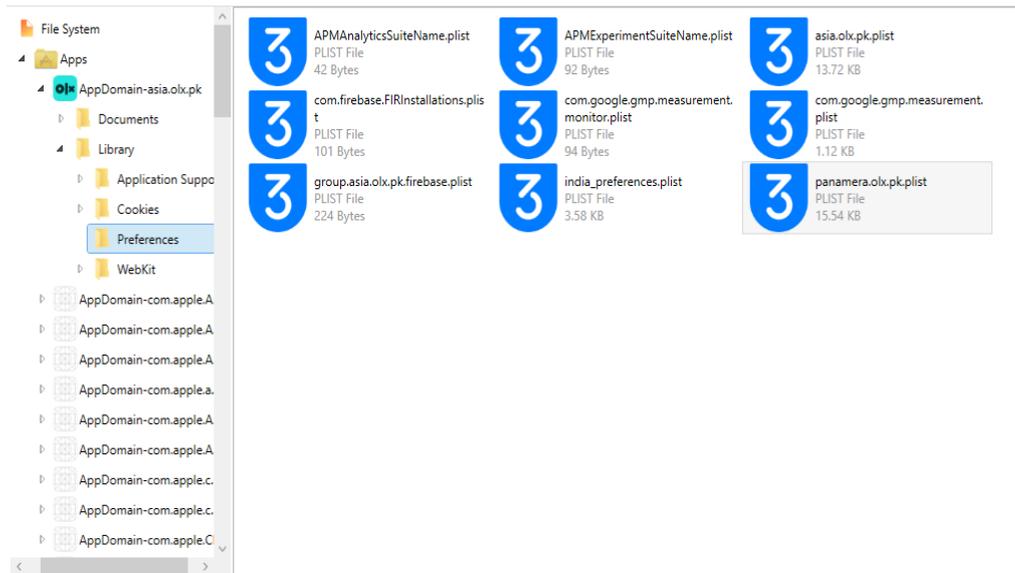


Figure 7. OLX app location

Fig. 8 reveals all the information stored within the “panamera.olx.pk.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).

```

plist Editor - panamera.olx.pk.plist
Save Export Refresh
<key>notification_nub_token</key>
<string>eyJhbGciOiJIUzI1NiIsInR5cCI6IkpzVCJ9.eyJpYXQiOiJlMjMTxMjYyNTYsImJyYW5kIjoib2x4IiwiaWF0IjoiY291bnRyeUNvZGU
iOiJwayIsInVzZXJZCmTEOMDY3MjklfQ.sqzVRoSfYfu-svlwL4RuGjry-Fe7Qg8bRJGhE9v86CqQ</string>
<key>WizRocketboolPersonalisationEnabled</key>
<integer>1</integer>
<key>AppsFlyerCounter</key>
<integer>2</integer>
<key>AKLastCheckInSuccessDate</key>
<date>2021-01-31T20:07:59Z</date>
<key>WizRocket6Z6-746-995Z:NetworkInfo</key>
<integer>1</integer>
<key>publishedItemsCount</key>
<integer>1</integer>
<key>AppsFlyerLaunchKey</key>
<true/>
<key>WizRocketfirstTime</key>
<integer>0</integer>
<key>baseurl</key>
<string>api.olx.com.pk</string>
<key>userPhoneNumber</key>
<string>3326860888</string>
<key>isFirstAppLaunch</key>
<true/>
<key>latitude</key>
<real>31.409197403968374</real>
<key>AppleLocale</key>
<string>en_PK</string>
<key>WizRocket6Z6-746-995Z:istc_inapp:-v035b490ae42a4fcab282b5aaea9fe01f</key>
<integer>0</integer>
<key>nextUpdateForegroundInMinutes</key>
<integer>20</integer>

```

Figure 8. Information stored in panamera.olx.pk.plist

Also we find a directory which hold the images of posted Ads. Path of directory is “Apps\AppDomain-asia.olx.pk \Documents\LetGoImage”.

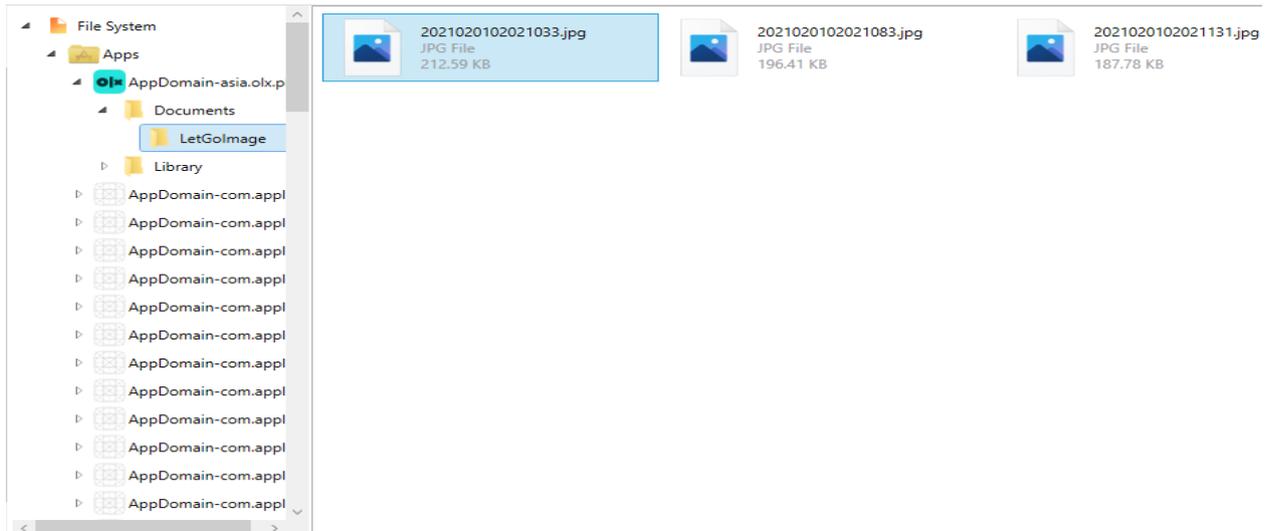


Figure 9. Images of posted Ads

This directory contains all posted ad images. That can be also used as potential evidence.

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 OLX mobile application as shown in figure 10.

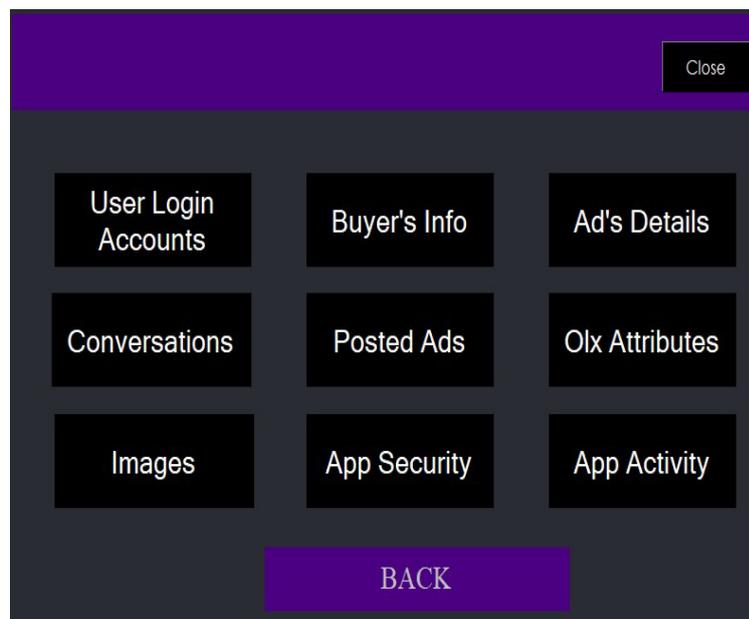


Figure 10. App Interface

8.1 Login Details

By clicking on "user login accounts" button, the forensic examiner can get the necessary information details about user's login and location as shown in figure 11.



Buyer Name	Message ID	Sender Type	Text
Muhammad Ahmad	2106a90b-b2b8-49b3-b93d-0a51b75e2122	buyer	Is it available?
Muhammad Ahmad	a30a81ca-9288-419d-b849-fb4eccf1993e	buyer	Hello
Muhammad Ahmad	CF21665E-6997-4D65-9E21-0E1BB04EE884	seller	Yes, it's still available. Are you interested?
Muhammad Ahmad	53c557b2-d3b3-4ba2-a335-5668f1960ac8	buyer	What's your location?
Muhammad Ahmad	4FD68164-269C-4765-B227-D7858F308AE1	seller	Yes
Muhammad Ahmad	ad587991-0a36-491b-8b1a-9fe2d5bb86ae	buyer	Ok I'll call you tomorrow
Muhammad Ahmad	8e8264c5-0c20-464d-a334-789e51968695	buyer	I would like to buy this for Rs 1,900
Muhammad Ahmad	4B66C634-974C-4EE1-9C5B-2F3138AA1AA	seller	I accept your offer, let's close this deal fast.
Muhammad Ahmad	1a076995-df79-4a5f-884f-6bb8a80a724	buyer	[This is a system message] Safety tip: Stay on the safer OLX chat and don't share your personal/whatsa

Figure 13. Conversation summary

9. Privacy Issues of Instagram

During the forensics investigation of IOS version of the Olx Application, we have found a serious privacy issue regarding user's multimedia content stored on the server-side. As we have seen that pictures shared by Olx sellers are not stored in the local directory structure of the application, instead, the Ad 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 seller images directly, using any web browser, and without having to verify or input any critical credentials (username or passwords).

To test this, we upload a picture of birthday gift, after sometime we remove the picture from Olx than we observed that the picture is actually removes from the app but the URL to that picture is not remove from the Ad table in the database. It remains there as it was. That is a concern, it should be removed with the deletion of a picture from the App.

The outcome of this project 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 Olx mobile application directories on IOS-based mobile phones.

10. Conclusion

Only a few studies have addressed the forensic analysis and recovery of activities performed through E-commerce applications on an iOS phone, so dissecting the Olx application was a good learning experience as the research revealed the behavior of the e-commerce applications data, which was extracted from backup files of each application stored on the IOS device internal storage. It is a novel approach and methodology was very effective in retrieving digital artifacts. Application contained a huge repository of information and we successfully extracted the digital evidence that will be helpful in crime investigation. Moreover, it is the open-source software for performing digital forensics on e-commerce applications. The amount, importance, and placement of e-commerce apps data that could be identified and retrieved from an IOS device backup file were established using forensic analysis. User login and location details, chats with customers, purchaser's information (Name and mobile phone number), and posted Ad details are among the digital artefacts acquired from the Olx application backup files.

References

1. Kävrestad, J. (2020). *Fundamentals of Digital Forensics*. Springer International Publishing.
2. Casey, E. (2009). *Handbook of digital forensics and investigation*. Academic Press.
3. Kruse II, W. G., & Heiser, J. G. (2001). *Computer forensics: incident response essentials*. Pearson Education.
4. Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *digital investigation*, 7, S64-S73.
5. Nance, K., & Ryan, D. J. (2011, January). Legal aspects of digital forensics: a research agenda. In 2011 44th hawaii international conference on system sciences (pp. 1-6). IEEE.
6. PECA : Prevention of electronic crimes act, 2015. <https://pcsw.punjab.gov.pk/PreventionofElectronicCrimesAct2C2016>
7. Mocas, S. (2004). Building theoretical underpinnings for digital forensics research. *Digital Investigation*, 1(1), 61-68.
8. Mohay, G. M. (2003). *Computer and intrusion forensics*. Artech House.
9. Reedy, P., Police, A. F., & Holohan, M. Digital Analysis. In 16th International Forensic Science Symposium Interpol–Lyon 5 th-8 th October 2010 Review Papers (Vol. 609, p. 397).
10. Narwal, B., & Goel, N. (2020). A Walkthrough of Digital Forensics and its Tools.
11. Sift Workstation : Forensic tool, 2020. <https://digitalforensics.sans.org/community/downloads>
12. Wilding, E. (1997). Computer evidence: a forensic investigations handbook. *Computer Fraud & Security*, 1(1997), 17-18.
13. Brunty, J. (2011). Validation of forensic tools and software: a quick guide for the digital forensic examiner. *Forensic Mag*.
14. Rosenblatt, K. S. (1995). *High-Technology Crime: Investigating Cases Involving Computers*. San Jose, CA: KSK Publications.
15. Zdziarski, J. (2008). *iPhone forensics: recovering evidence, personal data, and corporate assets*. " O'Reilly Media, Inc."
16. NIST (National Institute of Standards and Technology) : General test methodology for computer forensic toolsl, 2018. <http://www.cftt.nist.gov/documents.htm;2001>.
17. Kim, D., & Lee, S. (2020). Study of identifying and managing the potential evidence for effective Android forensics. *Forensic Science International: Digital Investigation*, 33, 200897.
18. Al Mutawa, N., Baggili, I., & Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. *Digital investigation*, 9, S24-S33.
19. Lessard, J., & Kessler, G. (2010). *Android forensics: Simplifying cell phone examinations*.
20. Vidas, T., Zhang, C., & Christin, N. (2011). Toward a general collection methodology for Android devices. *digital investigation*, 8, S14-S24.
21. Kitsaki, T. I., Angelogianni, A., Ntantogian, C., & Xenakis, C. (2018, November). A forensic investigation of Android mobile applications. In *Proceedings of the 22nd Pan-Hellenic Conference on Informatics* (pp. 58-63).
22. Lwin, H. H., & Aung, W. P. (2020). *Forensics Analysis of Mobile Financial Applications used in Myanmar* (Doctoral dissertation, MERAL Portal).
23. Lin, X., Chen, T., Zhu, T., Yang, K., & Wei, F. (2018). Automated forensic analysis of mobile applications on Android devices. *Digital Investigation*, 26, S59-S66.
24. Thakur, N. S. (2013). *Forensic analysis of WhatsApp on Android smartphones*.
25. Umar, R., Riadi, I., & Zamroni, G. M. (2018). Mobile forensic tools evaluation for digital crime investigation. *Int. J. Adv. Sci. Eng. Inf. Technol*, 8(3), 949-955.
26. Simon, M., & Slay, J. (2010, February). Recovery of skype application activity data from physical memory. In 2010 International Conference on Availability, Reliability and Security (pp. 283-288). IEEE.
27. Tri, M. K., Riadi, I., & Prayudi, Y. (2018). Forensics acquisition and analysis method of imo messenger. *International Journal of Computer Applications*, 179(47), 9-14.
28. Agrawal, A. K., Sharma, A., & Khatri, P. (2019, March). Digital forensic analysis of Facebook app in virtual environment. In 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 660-664). IEEE.
29. Lone, A. H., Badroo, F. A., Chudhary, K. R., & Khaliq, A. (2015). Implementation of forensic analysis procedures for WhatsApp and Viber android applications. *International Journal of Computer Applications*, 128(12), 26-33.
30. Saha, A. K., Saha, J., Ray, R., Sircar, S., Dutta, S., Chattopadhyay, S. P., & Saha, H. N. (2018, January). IOT-based drone for improvement of crop quality in agricultural field. In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 612-615). IEEE.
31. Maduranga, M. W. P., & Abeysekera, R. (2020). Machine learning applications in IoT based agriculture and smart farming: A review. *Int. J. Eng. Appl. Sci. Technol*, 4(12), 24-27.