Forensic Acquisition and Analysis of Tango VoIP

Nhien-An Le-Khac*, Christos Sgaras, and M-Tahar Kechadi

School of Computer Science and Informatics, University College Dublin, Belfield, Dublin 4, Ireland.

Abstract

The advent of the Internet has significantly transformed the daily activities of millions of people, with one of them being the way people communicate where Instant Messaging (IM) and Voice over IP (VoIP) communications have become prevalent. Although IM applications are ubiquitous communication tools nowadays, it was observed that the relevant research on the topic of evidence collection from IM services was limited. The reason is an IM can serve as a very useful yet very dangerous platform for the victim and the suspect to communicate. Indeed, the increased use of Instant Messengers on smart phones has turned to be the goldmine for mobile and computer forensic experts. Traces and Evidence left by applications can be held on smart phones and retrieving those potential evidences with right forensic technique is strongly required. Recently, most research on IM forensics focus on applications such as WhatsApp, Viber and Skype. However, in the literature, there is no forensic analysis related to Tango, an IM on both iOS and Android platforms, even though the total users of this application already exceeded 100 million. Therefore, in this paper we present forensic acquisition and analysis of Tango VoIP for both iOS and Android platforms. We try to answer on how evidence can be collected when IM communications are used. We also define taxonomy of target artefacts in order to guide and structure the subsequent forensic analysis. Additionally to the forensic analysis, alternative sources of evidence were examined such as the possibility to clone an IM session and perform communication interception. Finally, a review of the information that can become available via the IM vendor was conducted. The achieved results of this research provided elaborative answers on the types of artefacts that can be identified by this IM application. We compare moreover the forensics analysis of Tango with two other popular IM: WhatApp and Viber.

Keywords: Type your keywords here, separated by semicolons ;

1. Introduction

One of the daily activities that has seen significant changes due to service introduced via the Internet is the social networking and communication amongst people [4]. Various Internet based communication services have been introduced that offer diverse methods of communication such as instant messaging, audio, video, file exchange and image sharing. The term “Instant Messaging application” or “IM applications” will be used throughout this text in order to refer to this category of Internet based communication services.

However, it was not only the legitimate activities that shifted to Internet based services. Eventually, criminal activities started being facilitated or taking place over the Internet [5] and criminals started using IM applications to communicate, either with potential victims [6] or amongst themselves to avoid interception [7]. It becomes obvious that, due to their popularity, IM applications have the potential of being a rich source of evidential value in criminal investigations. Moreover, for most of these applications, the type of information that can be collected in the context of an investigation can span beyond text messages. Europol has identified the threat of misused IM communications by criminals to facilitate their illegal activities due to the fact that it is harder to monitor or regulate these services [8].

Despite the wide prevalence of IM applications, there has been limited published research towards the assessment of their evidential value in criminal investigations. Moreover, the existing published research has not addressed all the popular OS platforms and IM applications, either due to the fact that they did not all exist at the time the research was
conducted or the specific IM application was not that prevalent at that point to attract the attention of deep investigations.

As a result, this acted as the main motivation in proceeding with this specific problem since any solution to it would address the gap in the existing published research and contribute to its further progress. In this paper, we present forensic acquisition and analysis of Tango VoIP for both iOS and Android platforms. Tango is a popular IM app as its total users already exceeded 100 million [x]. Indeed, to the best of our knowledge, there is no published research regarding forensic artefacts of Tango. Besides, most of the published research has been focusing on Android devices whereas iOS based devices have not been extensively examined. In this paper we aim to answer how evidence can be collected when Tango’s communications are used. In order to provide answers to this problem, the idea is to select a number of Tango IM services and operating systems based on current popularity and conduct test communications for further analysis. Furthermore, a taxonomy of target artefacts was defined in order to guide and structure subsequent forensic analysis. Additionally to the forensic analysis, alternative sources of evidence were examined such as the possibility to clone a Tango IM session and perform communication interception. Finally, a review of the information that can become available via the vendor was conducted. Based on this approach, experimental tests were also conducted in order to identify potential forensic artefacts for Tango IM application.

The rest of this paper is structured as follows: Section 2 looks at the literature survey and relevant work that has been conducted in the field. Section 3 describes the acquisition techniques in order to address the problem as identified in this section. Section 4 presents the evaluation and discussion of the outcomes of applying the adopted approach to solve the problem. Finally, Section 5 summarises some concluding remarks and discusses some future work.

2. Related work

Although IM and VoIP applications were not very widespread in 2006, Simon & Slay [9] had already identified that the use of VoIP communications poses new challenges to law enforcement authorities. Specifically, they pointed out that new methods for collecting evidence were needed due to the fact the VoIP communications are based on a decentralised data network and can be easily encrypted. In the same paper, the authors described the challenges of performing call interception due to VoIP architecture of non-carrier solutions with a special reference to Skype, which was one of the few VoIP applications at that time. They present a potential real life scenario where criminals could avoid the traditional PSTN network and communicate via Skype in order to avoid interceptions and achieve the necessary obscurity required to remain undetected [10]. Moreover, they referred to the immaturity of legislation regarding the regulation of non-carrier VoIP and the complexity of introducing relevant legislation at an international level. Finally, they proposed memory forensics as a potential direction in retrieving volatile evidence related to running VoIP software, although they do not present a concrete methodology since their research was still incomplete at that point.

Kiley et al [11] conducted some research on IM forensic artefacts and they also pointed out that IM is being exploited by criminals due to its popularity and privacy features. However, their research focused on, what they named, volatile instant messaging which described the IM services operating via a web interface, without requiring a fat client. They analysed four popular web-based IM services on Windows desktop environments and concluded that it is possible to retrieve forensic artefacts via the browser cache files and the Windows page files. The identified forensic artefacts included communication timelines, usernames, contact names and snippets of conversation. However, the entire conversation was never possible to be retrieved. The authors concluded their paper by presenting an investigative framework for addressing volatile messaging, which consists of three phases: recognition, formulation and search.

Simon & Slay [12] continued their work on investigative techniques for VoIP technologies by conducting experiments in order to identify traces left by Skype in the physical memory. They drew their inspiration from similar research on the operating system recovery level information from the physical memory and expanded the approach to application level information. To better structure the objectives of their proposed investigative approach, the authors defined a number of data type categories that could be identified in the context of an investigation: Communication Content, Contacts, Communication History, Passwords and Encryption Keys. In order to capture the memory of the system under investigation, they leveraged virtualisation and the inherent functionalities of memory extraction. They concluded
that it is possible to retrieve useful information about the use of Skype via the physical memory and specifically: information about the existence of the Skype process, the password and the contact list of the Skype account that was used. However, it was not possible to retrieve any encryption keys although it is known that Skype uses encryption.

Vidas et al [13] conducted work towards the definition of a general methodology for collecting data on Android devices. Although not directly relevant to the IM investigation issue, their work provides useful information that assisted in developing our approach. More precisely, the authors have provided a comprehensive overview of an Android device and proposed specific data collection objectives and processes that were taken into account in our experiments, which are described in Section 4.

Alghafli et al [14] gave guidelines on the digital forensic capabilities in smartphones where they considered Skype as a source of evidence. They also referred to VoIP applications being used to communicate without leaving logs in the traditional phone functions of the smartphones.

Carpene [15] and Tso et al [16] approached the evidence extraction for iOS based devices from a different perspective, which does not require the actual seizure of the device. Their approach was to leverage the backup files created via the iTunes application, the PC companion software for managing iOS devices. In [15] the author took a more generic approach in an attempt to create taxonomy for all potential evidence that can be extracted from the iTunes backup file. Skype is one of the applications that were included in this taxonomy and the potential evidence identified is limited call history and limited contact data. The same approach was followed in [16] to investigate the iTunes backup files. Nevertheless, their research focused in identified forensic artefacts of five popular IM devices: Facebook, Skype, Viber, Windows Live Messenger, and WhatsApp Messenger. They concluded that it is possible to retrieve the content of IM communications via the backup files. Since three of these IM applications are included in analysis, their outcome will be taken into consideration.

Schrittwieser et al [17] conducted a security assessment of nine popular IM and VoIP applications, including Viber, WhatsApp and Tango. Although their approach is stemming from a vulnerability assessment perspective, the outcome could also be valuable in a law enforcement investigation context. For instance, their results about weak authentication mechanisms could be used in order to perform session hijacking or session cloning and intercept the communication, wherever the applicable legislation allows for such activities by law enforcement authorities.

Chu et al [18] examined the possibility of retrieving Viber communication content via the Random Access Memory (RAM) in Android devices. They concluded that it is possible to retrieve partial evidence via the RAM and, furthermore, that the evidence is present even after resetting the device.

Mahajan et al [19] conducted forensic analysis for both Viber and WhatsApp on Android devices, using forensic acquisition equipment to perform the file system extraction of the smartphones. Their research concluded that for both IM applications it is possible to retrieve useful information about the user’s activities such as communication content, communication history and the contact list.

We also want to validate what has been concluded in [19] and go beyond by expanding it to issues that they have not been addressed such as the recovery of deleted messages or factory reset phones. Moreover, we will expand further to more platforms and more IM applications. As presented above, IM and VoIP applications are in the rise within the last few years and most likely will remain popular in the future. The shift from traditional communications (i.e. over PSTN or GSM networks) to IM and VoIP services calls requires new ways of collecting evidence.

The existing literature has identified the issue of identifying and monitoring VoIP traffic [9][10][20] and some research has been conducted towards the retrieval of evidence from IM and VoIP services [12][15][16][19][21]. Nevertheless, there are gaps in the existing research and developments on this field, which have yet to be addressed. For instance, the investigating forensic artefacts of Tango, which is popular amongst Android users or the desktop version of Viber which was only released in May 2013 is highly required. Moreover, very little is known about alternative investigation techniques such as IM session cloning, which is often used by law enforcement for Skype investigations. Finally, most of the published research has been focusing on Android devices whereas iOS based devices have not been extensively examined.

These open issues formulate the problem statement of this work, which can be summarised in the following questions:
What types of forensic artefacts can be found in the most popular IM services?

How and where can evidence be collected from the most popular IM services?

What alternative sources exist in order to capture evidence from IM services?

What information can the IM vendors provide to law enforcement?

In order to address these questions we follow the approach that is described in the following Section.

3. Acquisition Techniques

The first step is to set-up an investigation environment for various mobile devices in with Tango IM is installed. Following the environment setup and the definition of the list of target artefacts, the next steps are dedicated to the whole investigation itself; from the data collection to the extraction of evidence (artefacts in this case). The overall approach has two main phases. In the first phase we use session cloning technique and in the second phase we perform the forensic analysis on the data:

- **Session cloning:** This technique is an alternative proposal for intercepting communication of IM applications, since it might be technically not possible to perform communication interception of IM traffic via the IM vendor or the Internet Service Provider.

- **Forensic analysis:** This approach implies that a device has been seized and therefore we can conduct a forensic analysis on it in order to extract evidence in a post mortem fashion.

Both the approaches are further described in the following sections.

3.1. Taxonomy of target artefacts

<table>
<thead>
<tr>
<th>Target Artefacts</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Data</td>
<td>Data related to the installation of an IM client on a specific device. It can be very useful in the initial phase of an investigation, as it can lead to further queries related to IM data.</td>
</tr>
<tr>
<td>Traffic data</td>
<td>According to the European Data Protection Supervisor [29], traffic data are data processed for the purpose of conveying a communication on an electronic communications network.</td>
</tr>
</tbody>
</table>

3.2. Forensics Analysis

The objective of this analysis is to identify the artefacts stored by each IM application in the file system of every seized device. The following questions are usually expected to be answered during this analysis:

- What data is generated and stored on the device for each of the used IM functionality?
- Where is this data stored on the file system?
- In what format is the data stored?
- How can the data be retrieved, accessed and analysed?

For the data extraction and analysis from the devices, we use specialised mobile forensic tools:

- Cellebrite UFED Touch Ultimate - data extraction / acquisition – with the following extraction modes:

According to the means of communication used, the data needed to convey the communication will vary, but may typically include contact details, time and location data. Therefore it is crucial for forensic analysis.

- **Content data**: The actual content of a communication, which can be text, audio, video, or any other format of the data. In the context of this study, we do not categorise attachments or exchanged files as content data but we establish category for them.
- **User profile data**: Information related to the profile of the IM user such as name, surname, birthdate, gender, picture, address, phone number and email.
- **User authentication data**: Data that is used to authenticate the user to a service or an application such as a password, session key, etc.
- **Contact database**: The list of contacts associated to the IM user.
- **Attachments/Files exchanged**: Data files that were exchanged via a file transfer functionality.
- **Location Data**: According to the UK Information Commission Officer [30], location data means any data processed in an electronic communications network or by an electronic communications service that indicates the geographical position of the terminal equipment of a user of a public.
3.3. Session Cloning

The objective of session cloning is to investigate whether it is possible to concurrently login on another instance of the IM application, beyond the control environment of the potential target of an investigation. This can be a very effective way of conducting communication interception without having to perform live interception on the communication channel. Alternatively, the proposition of cloning a session is to attempt taking advantage of the fact that IM applications usually allow multiple concurrent sessions of the same user to be opened. To that end, our examination is focused on the following:

- Is it possible to clone a session of the IM application on a different device?
- Is there a limitation on the concurrent sessions that can be running simultaneously on different devices?
- What is the behaviour of the clone when the IM application receives text, files, audio or video calls?
- Is it possible to know whether there is a concurrent open session?
- Is it otherwise possible to detect a running clone session? and under which circumstances?
- What happens if an IM client is installed after the same account has been used in another instance? Are there any cached messages forwarded to the newly installed client?

In order to answer the aforementioned questions, the technical specifications of Tango were studied to identify its potential and restrictions. Moreover, it was attempted to create clone session for Tango on different devices, either mobile phones or desktop computers, and observe the behaviour of both the original and the clone session.

3.4. Review of information available via the IM vendor

The objective here is to identify what information could the IM vendor provide, which might be stored centrally in their infrastructure. To this end, the privacy policies of the IM vendors were reviewed in order to identify relevant provisions and practices towards sharing information in the context of criminal investigations. The focus of the review was on information regarding:

- The procedure according to which request can be submitted to the vendor by law enforcement authorities.
- The type of information that is centrally available to the vendor and can be provided to law enforcement authorities (e.g. communication content, communication history, etc.).
- The retention period of data stored by the vendor.
- The prerequisites under which the vendor supplies this information to law enforcement authorities.

3.5. Discussion

The approach adopted in order to conduct this study is influenced by Simon & Slay [12] with regards to the definition of data categories of expected evidence. Moreover, the adopted approach for the data acquisition from the mobile devices is based on the same technique used in [19]. Nevertheless, the adopted approach differs from these previous studies in the following:

- It covers both iOS and Android platforms. Previous work mainly focused either on Android devices [19] or the backup files of iOS devices [15][16], but not both at the same time.
- It covers the four most popular IM applications; in total more than 830 million users, on the two most popular mobile platforms, covering 63% of the market share as described earlier. Overall, the scope of the examined IM and mobile OS platforms should cover the vast majority of IM based communications via mobile devices.
- With the exception to the study presented in [19], none of the previous work was based on the file system forensic analysis of data images acquired by mobile devices.
- Although mostly focusing on the mobile file system forensic analysis, it addresses the IM communications from multiple perspectives: 1)
file system forensic analysis, 2) session cloning and 3) information retrieval from the IM vendors. However, previous work was focused only on the technical forensic analysis of the file system [19], backup files [15][16] or the physical memory [12][18].

4. Description of results and Analysis

In this section, we describe the experimental results on the forensic analysis of Tango IM.

4.1. Test environment

In order to examine the Tango IM applications and answer the questions posed in the problem statement, a testing environment is setup, based on two different mobile devices with all the four IM applications installed (see Figure 1). The communications between the two devices was conducted for a week using all features of Tango.

![Fig.1. Test environment setup](image)

We used the iOS version 6.1.3 and the Android version 2.3.5 (Gingerbread) during the testing. Although the Android operating system is characterised by considerable fragmentation in terms of versions, it can be assumed that the results of the tests can be extended to all current versions of Android as it was also concluded in [19].

It must be noted that both devices were neither jailbroken nor rooted. In the case of a jailbroken or rooted device, the test would result in at least the same amount of evidence, if not more due to the more uncontrolled environment in a jailbroken or rooted device.

Moreover, the devices used were not locked with a passcode, although the equipment we used was able to retrieve almost the same data when the devices were locked. Nevertheless, the passcode recovery or cracking of the devices is out of the scope of this study.

4.2. iOS Forensic Analysis

**Logical Extraction Analysis:** The Logical Extraction of information from the iPhone did not produce any IM related results. As shown in Figure 2, the data from UFED Physical Analyser do not include any explicit information related to the four IM applications under investigation.

![Fig.2. iOS data after Logical Extraction](image)

**File System Extraction Analysis:** Unlike the information retrieved via the File System Extraction analysis for Skype [x] and Viber [y], there is not much information for Tango, as shown in the following Table.

<table>
<thead>
<tr>
<th>Identified Artefacts</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Data</td>
<td>Tango appears in the Installed Application List.</td>
</tr>
<tr>
<td>Content data</td>
<td>IM related images can be filtered out when searching by the application name: e.g., searching for Tango will return the pictures related to Tango.</td>
</tr>
<tr>
<td>User profile data</td>
<td>The Tango user account information appears in the “User Accounts” section.</td>
</tr>
</tbody>
</table>

**Manual File System Extraction Analysis:** Tango was the only application in the scope of this study that had never been included in any of the publications, according to the related work. Therefore, we conducted the manual file system analysis without any previous reference.
The first remark that was made the investigation of the Tango application in the iOS device was the fact that the application is registered with the name ‘sgiggle’ instead of tango in the file system (see Figure 3).

Secondly, it has to be noted that Tango’s application folder ‘sgiggle’ was the only one of the IM applications that is hidden in the file system.

While analysing the files included in Tango’s application folder, it was initially noted that the majority of them are part of the SQLite database “.db files” and this the same across the Tango applications. However, when attempting to parse the database files, it was noticed that the content of the databases are not in clear text; they are all encrypted. For instance, the database file “tc.db” appears to be the one storing the communication content in Tango (see Figure 4).

Further examination of the Table ‘messages’, its structure shown in Figure 5, we finally understood its format. The field ‘conv_id’ is presumably storing the id of the conversation and the field ‘payload’ is storing the content of the exchanged message. A deep examination of the data of the table ‘messages’, the content of the fields ‘conv_id’ and ‘payload’ appear to be unintelligible which leads to the conclusion that they are stored in an encrypted form.

The same kind of encryption was encountered with all other database files in the Tango application folder, which made the further analysis of the data not feasible in the context of this study, as it would require extensive cryptanalysis attacks.

However, there was data in clear text, which could be retrieved and this was found in the TangoCache.db database file included in the appData folder. The content of this database file is a list of URLs pointing at the media files (images and videos) exchanged via Tango and is stored and available in Tango’s file servers. Moreover, for each of the media files, there is also a local URL pointing to a local folder named ‘TCSStorageManagerMediaCache’, which is supposed to be the files stored locally. However that specific folder does not exist in the iOS analysis and no copies of the exchanged media files were found locally on the device.

Fig. 3. Tango folder structure in iOS

Fig.4. Tango tc.db database structure.
Nevertheless, this proved to be valuable information in the context of an investigation at an initial analysis phase.

4.3. Android Forensic Analysis

Logical Extraction Analysis: During the analysis of the Logical Extraction image by the UFED Physical Analyser, the only related information to Tango was a record in the ‘User Accounts’ section of an account entitled “Sync Tango friends”.

File System Extraction Analysis: In addition to the information retrieved by the Logical Extraction Analysis, the File System Extraction Analysis revealed an entry of the Tango application in the ‘Installed Applications’ section of the UFED Physical Analyser, which contains highly relevant insights.

Manual File System Analysis: The manual analysis file system in the Android file system resulted in identical conclusions as the one described in the iOS section. All the Tango database files were encrypted and TangoCache.db was the only file, which is not encrypted and it is pointing to exchange media files. The only difference with the version of the file found in the iOS device is the fact that the folder TCStorageManagerMediaCache and the contained media files were in fact available locally.

4.4. Session Cloning

Following the application specifications review and after conducting relevant tests the questions posed regarding the session cloning possibilities in the adopted approach are answered in the following:

- **The possibility of cloning a session of the IM application:** Yes it is possible, but only when using the desktop application. Is not possible to have two simultaneous sessions on mobile devices. Once a second mobile device is registered, the original instance is automatically unregistered.

- **Prerequisites for creating a clone session:** We need to know the activation code, which is sent via Tango message or SMS to the original session and an installed instance of Tango in a desktop environment.

- **Limitation on the number of sessions that can be running simultaneously:** As long as the additional sessions are created on the desktop version, there is no limitation on the number of concurrent sessions.

- **The behaviour of the clone when the IM application receives text, files, audio or video calls:** The desktop version of Tango supports only audio and video calls. Audio and video calls cannot be handled by the clone session, as this would cut the call from the original user, which would in most cases not be beneficial for an investigation.

- **Visibility of a concurrent open session:** There is no clear indication that there is another session running concurrently for the user of the original session.

- **Detection of a running clone session from the user of the original session:** Unless the clone session actively participates in the...
communication; for instance initiates a call, there
is no way to detect that another session is running.
• **The case of an installed IM client after the
  same account has been used in another
instance:** The list of recent calls is fully refreshed
in the clone session and can be retrieved, so one
can conduct a real-time investigation if this is
needed.
• **Information that can be retrieved from the
  clone session:** we can retrieve Traffic Data, User
profile data, and Contact database.

4.5. Information available via the Tango IM vendor

Type of data collected: Tango’s Privacy Policy
contains the following information about categories of
collected data: private identifiable information about
users (optional, during the download process for the
Service). For registration through Tango, the mobile
phone number and/or the email address of the user are
also collected. This depends on the device that is used
for the service. In addition, when the user installs the
service on their device and registers with Tango, s/he
will be asked to allow the vendor to access their
address book (names, numbers, emails, and Facebook
ID, but not notes or other personal information in
users’ address book). The vendor stores this
information on their servers.

Indeed, Tango may also collect and gather non-
personal identifiable information, such as certain
profile information including country of residence and
preferences. Tango may collect and store information
about the service usage from all users and interaction
with the service and user websites, including calls,
numbers of calls made by members, call durations,
text messages, information relating to games played
through the service (such as game scores and how
often the game was played, etc.), usage by locations,
device and connection information, IP address, device
capability, bandwidth, statistics on page views,
network type and traffic to and from our websites.

Tango allows the user to share text messages,
photos, videos and other communications (such as
greeting cards or interactions during games) with other
users, and all this data will be stored on our servers.

Tango seems to classify mobile phone numbers, e-
mail addresses and IP addresses as non-personal, so it
is collected and stored remotely. As a consequence,
Tango collects personal data, non-personal data (such
as country of residence and number of calls, etc.) and
the content of the communications. The location
information is not explicitly mentioned.

**Retention period of stored data:** Tango’s Privacy
Policy does not contain information about the
Retention period of stored data.

**Providing data to the authorities:** According to
Tango’s Privacy Policy, data may be provided to the
authorities when Tango has “a good faith belief that
the law, any legal process, law enforcement, national
security or issue of public importance requires
disclosure”. This broad definition would allow Tango
to provide data to the authorities for the purpose of a
criminal investigation. Moreover, there is no mention
of specific procedures to be followed; the term ‘good
faith belief’ makes Tango’s cooperation largely subject
to their own assessment. Specific procedures for the
disclosure of information are not mentioned.

**Comments on the Privacy Policy:** Tango collects
several categories of data: personal data, non-personal
data and the communication content. The Privacy
Policy does not contain provisions about retention
periods. Tango has made information disclosure
dependent on the ‘good faith belief’ clause, which
offers a large degree of flexibility to cooperate with
criminal investigations – even in the absence of a
formalised legal obligation to do so. Tango’s Privacy
Policy does not mention specific procedures for the
disclosure of information to the authorities. This
should be challenged and changed to make sure that
what is understood as private from the users is
reflected in the terms and conditions of the IM use.

4.6. Compare Tango with other IMs

**WhatsApp:** WhatsApp is a popular IM for both
Android and iOS platforms. The number of it users is
over 250 million [23]. In this paper, we only focus on
its iOS version. Table 3 shows WhatsApp artefacts in
iOS via an analysis of the data extracted from the file
system.

Table 3. WhatsApp artefacts in iOS

<table>
<thead>
<tr>
<th>Identified Artefacts</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Data</td>
<td>WhatsApp appears in the Installed Application List.</td>
</tr>
<tr>
<td>Content data</td>
<td>WhatsApp chat content. IM related images could be filtered out when searching by the application name.</td>
</tr>
<tr>
<td>Traffic data</td>
<td>WhatsApp chat history.</td>
</tr>
</tbody>
</table>
By comparing Table 3 with Table 2, we notice that Tango does not have the Traffic data. WhatsApp has moreover the chat content in Content data. Tango however has user profile data that stores user account information. Besides, as expected, the manual file system analysis revealed that the WhatsApp application files reside in an iOS folder; /var/mobile/Applications/ directory. The application files are stored in two subfolders; ‘Documents’ and ‘Library’, with the first one storing all the database and iOS plist settings files while the second contains media files such as images and videos. The subfolder Library/Media contains the following subfolders:

• `<contact_number>@s.whatsapp.net`: Containing all the media files exchanged in conversations with the specific contact.

• `Profile`: Containing thumbnail images of the profile pictures of all contacts.

Nevertheless, the database files storing the activity and contact information for WhatsApp reside in the Documents folder. The communication activity is stored in the database called ChatStorage.sqlite and the WhatsApp contact information is stored in the Contacts.sqlite database file.

Viber: Viber is also a popular IM for both Android and iOS platforms. It also has a desktop version for both Windows and Mac OS X. The number of its users is over 200 million [24]. Again, we only focus on its iOS version. Table 4 shows Viber artefacts in iOS via an analysis of the file system.

Table 4. Viber artefacts in iOS

<table>
<thead>
<tr>
<th>Identified Artefacts</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Data</td>
<td>Viber appears in the Installed Application List.</td>
</tr>
<tr>
<td>Content data</td>
<td>Viber chat content. Viber related images could be filtered out when searching by the application name, e.g. searching for Viber will return the pictures related to Viber.</td>
</tr>
<tr>
<td>Traffic data</td>
<td>Viber call history. Viber chat history.</td>
</tr>
</tbody>
</table>

By comparing Table 4 with Table 2, we notice that Tango does not have the Traffic data. Viber has moreover the chat content in Content data. Tango however has user profile data that stores user account information. By analysing Viber’s file system manually, some important information are:

• `AttachmentsPreview` contains thumbnail size images of pictures and videos sent or received.
• `CustomLocationImage` stores images that are defined with a different location at the moment of sending the message.
• `Stickers` folder contains sticker images that are used in Viber messages.
• `ViberIcons` includes the profile pictures of all Viber contacts including the users one.
• `ackTasks` contains iOS setting files.
• `Contacts.data` that is the main SQLite database contains all the activity data of application.

5. Conclusion and Future Work.

Tango was the only IM application that has not been examined so far. Therefore, the research results presented in this dissertation are considered as the initial effort to the forensic investigation possibilities. It is worth emphasising that Tango was the only IM application that stores the communication data in an encrypted format, which presents a challenge for the forensic investigators. Developing tools that can deal with the encrypted data is very challenging and we will look at this issue in our future work.

References


26. Digital Trends, “Messaging app Tango steps into social network status with new photo filters and 100M users.”


29. “EDPS Glossary - Traffic Data.”

