Facebook Forensics for Windows 10

Pankaj Choudhary, Upasna Singh, Nitesh K Bharadwaj, Bhopendra Singh
Department of Computer Engineering, Defence Institute of Advanced Technology (DI), Pune
{pankaj_pcse13, upasnaspringh, nitesh_pcse14, bhopendra_pcse14}@diat.ac.in

Abstract—The launch of Windows 10 has attracted various forensic communities worldwide, as many new features are incorporated in it. The Universal App Platform (UAP) of new version of Windows enables the same app to run on different Windows devices. Facebook App on Windows platform is the most popular social networking app, which also attracts various criminal activities. In the past, Facebook artefacts have acknowledged as evidence in various criminal trials and may be admissible in court of law. Windows Facebook App has changed the way of forensics, as it temporarily generates SQLite databases for storing the private data of user, such as user’s friend list, chat messages, events, notifications, news feed and their public location information. The records maintained by these databases have the potential to provide the forensic investigator a rich source of evidences about a user’s social networking activity. In this paper, forensic artefacts of Windows 10 Facebook App are extracted from SQLite databases and their importance are discussed.

Index Terms—Windows Forensics, Windows 10, Facebook Forensics, Facebook App, Universal App Platform (UAP), SQLite Database.

I. INTRODUCTION

Microsoft launched Windows 10, on 29th July, 2015, In 190 countries. Within the 24 hours of the launch, Windows 10 was installed more than 14 million devices [7]. According to Windows Central [8], more than 67 million devices are running Windows 10 now. Microsoft introduced many new feature in its new launch, including Windows 10 Apps, Edge Browser, Cortana, Notification Center, OneDrive, Universal App Platform (UAP), Quick Access, Continuum, Windows Hello etc [7].

As a digital forensic viewpoint, these features will have capability to reveal many new forensic artefacts than ever. These potential forensic artefacts can be found in event logs, internet browsers, LNK files, recycle bin, thumbnails, page-file.sys, lsyberfil.sys, OneDrive, prefetch files and Windows apps like Facebook, Twitter, Skype etc [7].

The Universal App Platform in Windows 10, enables one application to run on every Windows devices like, desktop, laptop, mobile, XBox, IoT device etc. One of the most popular social networking application is Facebook. In 2013, the official Facebook App was first appeared for Windows 8.1 and is also available for Windows 10. Almost all features are included in this app as in Facebook website.

Before the Facebook App released, only web browser traces were used as the source of Facebook related artefacts [7] [7]. Facebook App forensics of Windows 8 mobile has been research in forensics community [7] [7]. However, Facebook App forensics on PC running Windows 10 has changed the way of forensics, as it temporarily generates SQLite databases for storing the private data of user, such as user’s friend list, chat messages, events, notifications, news feed and their public location information.

The paper focuses on, where these databases are located on the disk, what potential forensic artefacts can be extracted from these databases and how they can contribute in an investigation. Section 2 focuses on Windows 10 Facebook App features and location of SQLite databases. Section 3 describes about the potential artefacts extracted from these databases and their importance from forensics viewpoint. The next section, concludes the paper with research challenges for further research.

II. WINDOWS 10 FACEBOOK APP

Windows Facebook App is accessible from Windows App Store for Windows 10. After installing, when a user first logs in the app with Facebook credentials, the application creates various SQLite database files for storing users private data. In Windows 10 these databases can be found on this location: C:\Users\UserName\AppData\Local\Packages\Facebook.facebook_8xx8rvfsw5nn\LocalState\FacebookUserID\DB [7]. In the given file path, following seven SQLite database files are generated as shown in Figure 1: Analytics.sqlite, FriendRequests.sqlite, Friends.sqlite, Messages.sqlite, Notifications.sqlite, StickerPacks.sqlite and Stories.sqlite.

III. EXTRACTING ARTEFACTS FROM FACEBOOK APP DATABASES

As discussed in the previous section, each SQLite database contains a wealth of information regarding the user’s activities on the Facebook App. Our focus is to explore each database with its tables and fields and to highlight the type of information within it. This information may be very important in the case of user’s social networking activities are of forensics investigator’s interest. For examining these SQLite databases, DB Browser for SQLite [7] is used. SQLite database of Windows 10 Facebook app is shown in Table 1. In the following subsection, each database with its tables and type of information in it, is discussed in detail.

1) Analytics.sqlite: Analytics.sqlite database comprises various statistics of user activity on the app, which is used by Facebook as an application feedback. It includes information such as user’s chatting activity with time of last chat. Statistics of user activity in Analytics.sqlite Database is shown in Figure 2.
TABLE I

Windows 10 Facebook App Databases

<table>
<thead>
<tr>
<th>SQLite Database</th>
<th>Tables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analytics.sqlite</td>
<td>analytics_log</td>
<td>Contains users analytical information, used by Facebook to get app feedback</td>
</tr>
<tr>
<td>FriendRequests.sqlite</td>
<td>friend_requests</td>
<td>Contains all the pending friend requests sent to user with timestamps</td>
</tr>
<tr>
<td>Friends.sqlite</td>
<td>friends</td>
<td>Information about users Facebook friends such as, name, e-mail, phone number, communication rank, birthday etc.</td>
</tr>
<tr>
<td>Messages.sqlite</td>
<td>folder counts</td>
<td>Contains information about cached chats messages on the device such as chat text sender and recipient detail, timestamps, attachments, geolocation coordinates etc</td>
</tr>
<tr>
<td></td>
<td>messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>thread_to_user</td>
<td></td>
</tr>
<tr>
<td></td>
<td>thread</td>
<td></td>
</tr>
<tr>
<td></td>
<td>users</td>
<td></td>
</tr>
<tr>
<td>Notifications.sqlite</td>
<td>notifications</td>
<td>Contains information of users Facebook notification such as likes, comments, events, birthdays etc.</td>
</tr>
<tr>
<td>StickerPacks.sqlite</td>
<td>recent_stickers</td>
<td>Contains information of stickers used in the chat messages by the user with timestamps</td>
</tr>
<tr>
<td></td>
<td>sticker_packs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>stickers</td>
<td></td>
</tr>
<tr>
<td>Stories.sqlite</td>
<td>actors</td>
<td>Stores information about users news feed and stories available on user timeline with content of stories and timestamps</td>
</tr>
<tr>
<td></td>
<td>attachments</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cursors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>feed_media</td>
<td></td>
</tr>
<tr>
<td></td>
<td>feed_sections</td>
<td></td>
</tr>
<tr>
<td></td>
<td>feedback</td>
<td></td>
</tr>
<tr>
<td></td>
<td>places</td>
<td></td>
</tr>
<tr>
<td></td>
<td>profiles</td>
<td></td>
</tr>
</tbody>
</table>

This database contains following tables:

(i) analytics_log: It stores following information:
- *id*: unique identifier for users app related activity.
- *time*: time of user activity or client_event (in unix/epoch time format)
- *log_type*: type of user/client action or event
- *name*: name of user action such as page navigation, selecting bookmark
- *extra*: detailed description of users app activity such as selecting news feed, page, notification, users activity time on the app etc.

(ii) sqlite_sequence_table: Stores the value of last recorded ID of analytics_log table, for keeping track of last session

2) FriendRequests.sqlite: This database contains the detail of all pending friend requests sent to user with timestamps of these friend requests. Pending friend requests in FriendRequests.sqlite database are shown in Figure 3. It contains friend_requests with following fields:
- *uid_from*: Facebook user ID from which friend request is sent
- *time*: time when friend request is sent (in regular time format)
- *unread*: whether the friend request is seen or not (value 0 or 1)
- *name*: first and last name of Facebook user, who sent the friend request.
- *affiliations_name*: affiliation details about the user

3) Friends.sqlite: This database keeps track of user’s Facebook friends and related details. In most of the cases it stores information of all the friends of user. Freind-list information in Friends.sqlite database is shown in Figure 4. It contains friends table with following fields:
- *uid*: Facebook user ID of user’s Facebook friends
- *name*: Full name of user’s Facebook friends
contact_email: Email addresses of user’s Facebook friends

phones: Detail of phone number of user’s Facebook friends with country code and type of phone such as cell phones

is_pushable: Information about whether or not the user can receive push notifications (value 0 or 1)

has_messenger: whether or not the user is using Facebook messenger app (value 0 or 1)

communication_rank: Ranking or rating of Facebook users based on the recent interactions. It represents, how often the user communicates with particular Facebook friend.

birthday_date: birthday date of user’s friend (if shared publicly)

4) Messages.sqlite : This database contains information about cached chat messages on the device such as, chat text, sender and recipient detail, timestamps, attachments, geolocation coordinates etc. It stores all the messages which are currently loaded in the Facebook App. The database contains following table:

(i) folder_count: This table contains following fields:

folder: type of folder for storing message such as Inbox

unread_count: total number of unread messages in the chat inbox

unseen_count: total number of unseen messages in the
chat inbox
- `last_action_id`: identifier composed of timestamp (in unix/epoch time) of last inbox activity
- `last_seen_time`: timestamp (in unix/epoch time) of users last seen chat message

Chat messages information in `folder_count` table of Messages.sqlite database is shown in Figure 5.

(ii) messages: This table contains following informations:
- `id`: unique identifier for each message instance in inbox. These IDs follow different structures as Facebook updates its message ID structure time to time. For example, m_mid.<timestamp>:<hex hash value>is the new message ID structure and m_id. <numeric value>is old message ID structure.
- `thread_id`: identifier for the message thread. It can be used to identify the message thread or conversation of user with friends and groups. It contains a timestamp (in unix/epoch time) of message thread generation, in other words, it is the time of users first chat message with particular friend.
- `body`: It contains the original chat message between Facebook users or group in text.
- `sender`: It stores the details of sender of the particular chat message. It contains Facebook user ID, name and email of the sender.
- `tags`: It contains information related to message storage location, messaging app used, status of message sent or received etc.
- `timestamp`: It stores the server timestamp (in unix/epoch time) value of the message
- `action_id`: Identifier, composed of a timestamp (in unix/epoch time) value of last messaging related action.
- `coordinates`: It stores the geolocation coordinates of the message sender/receiver, in case of GPS sensor is used.
- `attachments`: It contains details of attachments, if attached with chat message. It includes attached file name, unique ID if attached image, thumbnail and image url of attached image etc.
- `shares`: It contains detail of, if any link or url is shared in the chat message.
- `type`: Type of chat message such as personal or group message.
- `server_timestamp`: Timestamp (in unix/epoch time) of particular message_id on the message server.

Chat messages information in `messages` table of Messages.sqlite database is shown in Figure 6.

(iii) thread_to_user: This table stores the detail of individual chat message thread of user. It stores following informations:
- `t_id`: Message thread ID of, unique for particular chat message thread.
- `u_id`: Facebook user ID of all Facebook users involved in particular message thread.
- `is_participant`: Whether or not user participated in the particular message thread.
- `read_recipient_timestamp`: Timestamp (in unix/epoch time) to acknowledge, when recipient of the message reads it.

Individual chat message thread of user in `thread_to_user` table of Messages.sqlite database is shown in Figure 7.

(iv) thread: This table keeps track of each Facebook message thread such as timestamps, sender and receiver details, number of messages in the thread etc. It stores following information:
- `thread_id`: Unique identifier for all message threads
- `timestamp`: Timestamp (in unix/epoch time) of last message instance within the particular message thread.
- `action_id`: Unique identifier consisting of a timestamp (in unix/epoch time) value of last action related to message thread.
- `name`: Name of message thread, if any
- `folder`: folder within the app, where particular thread is stored, e.g. inbox
- `snippet`: Text of last chat message in the particular message thread.
- `snippet_sender_id`: Facebook user ID of user for last sent message with respect to particular thread.
- `senders`: Facebook user ID of all the participants in the personal or group conversation for particular message thread.
- `num_messages`: Total number of messages in the particular message thread.
- `single_recipient`: Facebook user ID of the recipient of the message.
- `can_reply`: whether or not the user can reply in the particular message thread (value 0 or 1)
- `is_subscribed`: whether or not the user is subscribed to get notifications for particular message thread (value 0 or 1)
- `draft`: Whether message is stored in the draft, in case of not sent.

Message thread information in `thread` table of Messages.sqlite database is shown in Figure 8.

(v) users: This table stores the detail of all participants involved in Facebook chat with user. It contains following information:
- `id`: Facebook user ID of all participants involved in Facebook chat with user.
- `type`: Type of user such as Facebook user, page or group.
- `email`: Facebook user email ID
- `name`: full name of all Facebook users involved in chat with user.
- `last_active_timestamp`: Last activity timestamp (in unix/epoch time) of Facebook users involved in conversation with user.

Chat participants in `users` table of Messages.sqlite database are shown in Figure 9.
5) Notifications.sqlite: This database contains information of user’s last received Facebook notification such as likes, comments, events, birthdays, page and group posts etc. It contains notifications table storing following information about user’s notifications:

- notification_id: Unique identifier, consisting of a timestamp (in unix/epoch time) value of particular user notification of Facebook App.
- object_id: unique identifier for objects involved in the notification.
- object_type: type of objects in the notification such as photos, page, group, birthday reminder, event, stream etc.
- sender_id: Facebook user ID of the sender of current notification.
- title_text: Text content of the notification.
- href: reference of the page, user, group or event for which notification is generated.
- unread: Whether or not the notification is read (value 0 or 1)
- updated_time: last updated time of the notification in the app.
- created_time: time when notification is first created.

Last received notifications in Notifications.sqlite database are shown in Figure 10.

6) StickerPacks.sqlite: This database contains information of stickers used in the chat messages by the user with various timestamp values. These timestamp values are very essential when stickers are used in chat messages. It contains following tables:

(i) recent_stickers: It stores following information:
- uid: unique identifier of individual sticker.
- added_datetime: Time when sticker is added with particular chat message.

(ii) sticker_packs: This table contains information about particular sticker pack such as unique id, name of sticker pack, artist, date and time of adding sticker pack etc.

(iii) stickers: This table contains the detail of cached stickers in the chat messaging window.
7) **Stories.sqlite**: This database stores information about users' news feed and stories available on user timeline. It is very important database as it stores the content and timestamp of the users' news feed and the current activity of user can be captured from this. It stores following tables:

(i) actors: this table keeps track of Facebook users, pages and groups involved in the particular news feed or story.

Facebook users involved in news feed in actors table of Stories.sqlite database are shown Figure 11.

(ii) attachments: It keeps track of all the attachments used in particular news feed or story such as story id, author of the story, details of like, comments and shares for particular story, post creation time, text of post, url of shared images, videos and files, target with respect to story.

Attachments used in news feed in attachments table of Stories.sqlite database are shown in Figure 12.

(iii) feed_media: This table contains the information images, videos and other media items shared in the news feed. It may help in finding media details such as url, created and modified time of media etc.

(iv) feedback: It keep track of various information for particular posts such as: likes, comments, shares etc. it contains following fields:

- **id**: unique identifier with respect to particular Facebook post.
- **can_viewer_comment**: Whether or not the Facebook
user can comment on the particular post (value 0 or 1)
- **can_viewer_like:** Whether or not the Facebook user can like on the particular post (value 0 or 1)
- **does_viewer_like:** Whether user liked the particular post (value 0 or 1)
- **legacy_api_post_id:** Facebook id to identify and visit particular post.
- **comments:** Total number of comments for particular Facebook post.
- **likes:** Total number of likes for particular Facebook post.
- **reshares:** How many times a particular Facebook post is reshared.

Feedback information in feedback table of Stories.sqlite database is shown in Figure 13.

(v) **places:** This table keeps track of location and places shared in the news feed. It may be helpful for tracking person based on shared places. It stores following information:
- **id:** Facebook id of shared place, location page in the post
- **facebook_sub_type:** type of place such as page, free form place, location etc.
- **address:** address of the shared location (if available)
- **category_names:** category of location or place such as shopping mall, city, restaurant, historic or tourist place, home etc.
- **contextual_name:** name of shared place such as Mumbai, waterfall, school, peoples mall etc.
- **description:** description of the place
- **location:** coordinates and time zone details of shared place.
- **url:** Facebook url of the shared place.

Shared places and locations in news feed in places table of Stories.sqlite database are shown in Figure 14.

(vi) **profiles:** It contains the detail of user profiles, pages and groups involved in the news feed. It may help in identifying users, pages, groups, events for particular post. It stores following information:
- **id:** Facebook ID of user, page, group or events.
- **facebook_sub_type:** whether user, page, group or event.
- **name:** name of Facebook user, page, group or event.
- **url:** url of Facebook user, page, group or event.
- **friend_request_status:** Whether or not the user is friend with particular Facebook user.
- **is_owned:** Whether user liked or subscribed to particular page or group.
- **mutual_friends:** number of mutual friends between user and other users.

User profiles, pages and groups in profiles table of Stories.sqlite database are shown in Figure 15.

(vii) **stories:** This table keeps track of all stories and news feed of users cached in the Facebook App. It may be helpful for tracking user’s last Facebook activity. It stores following information:
<table>
<thead>
<tr>
<th>id</th>
<th>can_viewer_comment</th>
<th>can_viewer_like</th>
<th>does_viewer_like</th>
<th>legacy_api_post_id</th>
<th>comments</th>
<th>likers</th>
<th>reshares</th>
<th>top_level_comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ZmVlZGlhY2s6MTAuNTI...</td>
<td>1</td>
<td>1</td>
<td>10153198610757675</td>
<td>60</td>
<td>282</td>
<td>0</td>
<td>60</td>
</tr>
<tr>
<td>2</td>
<td>ZmVlZGlhY2s6OTExNjA...</td>
<td>1</td>
<td>1</td>
<td>9116078218789</td>
<td>4</td>
<td>51</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>ZmVlZGlhY2s6MTk4MDE...</td>
<td>1</td>
<td>1</td>
<td>1610845203173761</td>
<td>7</td>
<td>18</td>
<td>0</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>ZmVlZGlhY2s6ODYyODM...</td>
<td>1</td>
<td>1</td>
<td>864873110270055</td>
<td>4</td>
<td>50</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>ZmVlZGlhY2s6MTAuNTI...</td>
<td>1</td>
<td>0</td>
<td>10132989772713456</td>
<td>1</td>
<td>112</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

**Fig. 13. Feedback Information in feedback Table of Stories.sqlite Database**

<table>
<thead>
<tr>
<th>id</th>
<th>facebook_sub_type</th>
<th>address</th>
<th>category_names</th>
<th>contextual_name</th>
<th>location</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Freedom Place</td>
<td>NULL</td>
<td><img src="image1.png" alt="Image" /></td>
<td>Mumbai</td>
<td>NULL</td>
</tr>
<tr>
<td>2</td>
<td>Page</td>
<td>NULL</td>
<td><img src="image2.png" alt="Image" /></td>
<td>People's Mall</td>
<td>NULL</td>
</tr>
<tr>
<td>3</td>
<td>Page</td>
<td>NULL</td>
<td><img src="image3.png" alt="Image" /></td>
<td>Karimna Dhaba</td>
<td>NULL</td>
</tr>
<tr>
<td>4</td>
<td>Page</td>
<td>NULL</td>
<td><img src="image4.png" alt="Image" /></td>
<td>Bhavanidhi</td>
<td>NULL</td>
</tr>
<tr>
<td>5</td>
<td>Page</td>
<td>NULL</td>
<td><img src="image5.png" alt="Image" /></td>
<td>Singhbad Fort</td>
<td>NULL</td>
</tr>
</tbody>
</table>

**Fig. 14. Shared Places in News Feed in places Table of Stories.sqlite Database**

<table>
<thead>
<tr>
<th>id</th>
<th>facebook_sub_type</th>
<th>name</th>
<th>username</th>
<th>url</th>
<th>friend/request_status</th>
<th>mutual_friends</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Page</td>
<td>Four Fountains De-Str...</td>
<td>TheFourFountain...</td>
<td>NULL</td>
<td>NULL</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>User</td>
<td>Varsha Sarawagi</td>
<td>varsha.sarawagi</td>
<td>NULL</td>
<td>AreFriends</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>User</td>
<td>Raghuvan Singh</td>
<td>neeleshaterred...</td>
<td>NULL</td>
<td>AreFriends</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>Page</td>
<td>Computer Tricks</td>
<td>Tricktronics</td>
<td>NULL</td>
<td>NULL</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>Page</td>
<td>Vaishnav Khirakar</td>
<td>NULL</td>
<td><a href="https://www.facebook.com/vaishh">https://www.facebook.com/vaishh</a>...</td>
<td>AreFriends</td>
<td>0</td>
</tr>
</tbody>
</table>

**Fig. 15. User Profiles, Pages and Groups in profiles Table of Stories.sqlite Database**

- **id**: Facebook ID of particular news feed or story.
- **hidden**: Whether or not post is hidden (value 0 or 1)
- **can_viewer_delete**: Whether or not user has permission to delete the particular post.
- **can_viewer_edit**: Whether or not user has permission to edit the particular post.
- **creation_time**: Timestamp (in unix/epoch time) of creation of the post
- **url**: Facebook url of the post
- **to**: To which page or group the post is shared.
- **message**: Original text of the post.
- **explicit_place_id**: Facebook Id of the exact place such as airport, station or Mall shared in the post.
- **implicit_place_id**: Facebook id of the place where explicit place is located.
- **privacy_scope**: privacy scope of the post such as public, private or custom.
- **edit_history**: Number of times the particular post has been edited.

All stories in stories table of Stories.sqlite database are shown in Figure 16.

**IV. CONCLUSION AND FUTURE RESEARCH**

Windows 10 was released with lot of new features such as Edge Browser, Cortana, Notification Center, OneDrive, Universal App Platform (UAP), Windows 10 Apps (Facebook, Twitter, mail), Quick Access, Continuum, new Start menu etc. These features discover treasure new forensic artefacts, useful in forensic investigation of devices running Windows 10. As a source of digital evidence against various digital crimes,
Facebook artefacts are being used by various law enforcement agencies and administrations. Windows version of Facebook App was first appeared for Windows 8.1 and is also available for Windows 10, involving same features as in Facebook website. The Universal App Platform in Windows 10, enables this app to run on all Windows devices like desktop, laptop, mobile, XBox, IoT device etc. Windows Facebook App has transformed the direction of forensics, as it's SQLite database structure for storing the private data of user. However, as of now, limited research has been done in this domain.

In this paper, we discussed about the location of seven databases generated by Facebook App in Windows 10, potential social networking artefacts extracted from these databases, and their importance in forensics investigation. As a forensics point of view, information extracted from these databases, such as users friend list, chat messages, events, notifications, news feed and their public location information, are important and may assist in an investigation. The paper does not cover the recovery of deleted SQLite database, however, the carving of deleted data from SQLite database is a current forensics challenge. Further research may be focused on this issue.

REFERENCES


