JOURNAL OF FORENSIC SCIENCES

J Forensic Sci, March 2017, Vol. 62, No. 2
doi: 10.1111/1556-4029.13267
Available online at: onlinelibrary.wiley.com

TECHNICAL NOTE

DIGITAL & MULTIMEDIA SCIENCES

Abdullah Azfar,[1] *M.Sc.; Kim-Kwang Raymond Choo*,[2,1] *Ph.D.; and Lin Liu*,[3] *Ph.D.*

Forensic Taxonomy of Android Social Apps

ABSTRACT: An Android social app taxonomy incorporating artifacts that are of forensic interest will enable users and forensic investigators to identify the personally identifiable information (PII) stored by the apps. In this study, 30 popular Android social apps were examined. Artifacts of forensic interest (e.g., contacts lists, chronology of messages, and timestamp of an added contact) were recovered. In addition, images were located, and Facebook token strings used to tie account identities and gain access to information entered into Facebook by a user were identified. Based on the findings, a two-dimensional taxonomy of the forensic artifacts of the social apps is proposed. A comparative summary of existing forensic taxonomies of different categories of Android apps, designed to facilitate timely collection and analysis of evidentiary materials from Android devices, is presented.

KEYWORDS: forensic science, digital forensics, forensic taxonomy, mobile app forensics, mobile forensics, social app taxonomy

Smart phones (e.g., Android and iOS devices) are widely used, and this usage appears to be influenced by users' experiences using mobile apps. For example, these apps are used in social activities such as day-to-day communications with friends, family, and colleagues; video streaming; financial transactions including mobile banking and money transfer; location searches; and an extensive list of other services and activities. One of the most popular app categories is social apps, of which Facebook and Twitter are examples. The key factors that have influenced the use of social apps include social identity, ease of use, altruism, telepresence, usefulness, and encouragement (1). Social app usage increased by 103% in 2014 and consumers were reported to spend 30% of their mobile device usage time on social apps, which was more than any other app category (2,3).

Smart phones are able to access and store a rich set of personally identifiable and sensitive information, such as geospatial information from the use of maps and navigation apps, and other metadata from the use of photograph apps, communication apps, social apps, and other categories of apps. End-users are unlikely to be aware of the information stored in their smart phones, especially user locations (4). It is therefore unsurprising that mobile devices and apps are targeted by cybercriminals. In the investigation of cybercriminal activities, for example, compromise of corporate or user data due to mobile malware or malicious apps, a forensic investigator would need an up-to-date understanding of the types of artifacts that could potentially be recovered. Timely recovery and analysis of these artifacts are critical in ensuring that key evidence is not erased or lost (5,6).

[1]Information Assurance Research Group, University of South Australia, Adelaide SA 5095, Australia.
[2]Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX, 78249-0631, USA.
[3]School of Information Technology and Mathematical Sciences, University of South Australia, Adelaide SA 5095, Australia.

Received 20 Dec. 2015; and in revised form 14 May 2016; accepted 22 May 2016.

Mobile device forensics, represented as a subcategory of the small-scale device forensics domain in the ontological representation for digital forensic disciplines by Karie and Venter (7), is challenging due to the wide range of mobile operating systems and constant evolution of mobile software and hardware. Although mobile forensics is an emerging area, it is understudied compared to other forensic science disciplines. However, recent reviews of the mobile forensics literature identified that interests in this area are increasing, albeit slowly (8–10).

Although there is a wide range of mobile platforms available in the market, recent statistics have suggested that Android is the dominant platform, and since its release in 2008, the Android operating system has undergone several iterations and is still updated regularly. At the time of this research investigation, Android devices reportedly have a 78% market share (11); therefore, we focus on Android in the development of our social app forensic taxonomy.

A taxonomy is designed to provide an informative categorization of data remnants in the forensic investigation of mobile apps. In our recent research, for example, we presented the first taxonomy incorporating the artifacts of forensic interest from 40 mobile health (mHealth) Android apps (12), and then, we presented another taxonomy incorporating the artifacts of forensic interest from 30 communication Android apps (13). Immanuel et al. (14) also noted the lack of research on forensic taxonomy. They presented an Android Cache Forensic Process, designed to forensically classify, extract, and analyze Android caches. To the best of our knowledge, there has been no published forensic taxonomy for Android social apps. This is, thus, the main contribution of this study.

In this study, the social apps are broadly categorized into three categories based on the services provided, and the forensic artifacts are classified based on our study of these social apps. Then, a two-dimensional taxonomy of the social apps is provided. In our previously published forensic taxonomy papers, mHealth apps (12) and communication apps (13) were considered, and it is likely that forensic artifacts in social apps will

differ from those in mHealth and communication apps. Therefore, a comparative summary is provided.

The contributions of this study are threefold:

1 Identification and analysis of data remnants of forensic interest to an investigator from the Android social apps.
2 Providing a two-dimensional taxonomy for Android social apps with the social app categories in one dimension and the forensic artifacts in the other dimension.
3 Providing a comparison of the findings with the existing forensic taxonomies of different Android app categories.

The rest of the article is organized as follows. Review of existing work is outlined in the next section. The forensic analysis and experiment results are presented in the "Case study: 30 Social Apps" section, prior to the presentation of the two-dimensional taxonomy in the "Proposed Forensic Taxonomy for Social Apps" section. A comparison of the findings with the existing forensic taxonomies of different categories of Android apps is presented in the "A Comparative Summary" section. The last section concludes the article.

Related Work

Plachkinova et al. (15) proposed a security and privacy taxonomy for mobile health apps, without considering the forensic artifacts and any other category of apps in their taxonomy. Alliano et al. (16) reviewed 21 Augmentative and Alternative Communication (AAC) apps for iPads and identified how individuals with complex communication needs could use them for a variety of communication purposes and to target a variety of treatment goals. However, forensics is not the focus of their work.

Al Mutawa et al. (17) conducted a forensic analysis of Facebook, Twitter, and MySpace apps installed on BlackBerry, iPhone, and Android phones. The authors conducted common user activities using the apps, acquired forensically sound logical images of the devices, and manually performed forensic analysis on each logical image. They were only able to forensically recover the information, such as user and friend data including contact details and profile in Facebook, from iPhones and Android phones.

Jang and Kwak (18) proposed a forensic investigation procedure for social networking services. The procedure describes real-time data investigation, data collection, and data analysis methodologies for these services, based on their case study using a desktop computer and an Android smart phone.

Chu et al. (19) examined the Facebook app and recovered locations of the users and the email ids of the last five users who logged in to their accounts using the same smart phone.

In a forensic examination, user-generated data, for example, due to app usage, such as in cloud and dating apps, could potentially be recovered in plaintext format from the device's user data partition (20–27). In the forensic analysis of nine popular dating apps, Farnden et al. (20) determined that artifacts, such as chat messages and user details, could be recovered from user devices. The authors also discussed the privacy implications of such recovered data.

Levinson et al. (28) undertook a forensic analysis of iOS social apps and demonstrated that third-party social apps could provide sufficient data as key evidence of time and location detection. They also found that information provided to the device by the user through their interactions with the apps was typically stored in plaintext format and could be extracted from the device's user data partition. Similarly, in the forensic examinations of the Android WhatsApp Messenger by Anglano (29) and Thakur (30), various artifacts and data were recovered.

Dezfouli et al. (31) investigated the Facebook, Twitter, LinkedIn, and Google+ apps, on Android and iOS platforms to locate the forensic remnants of forensic interest. The authors were able to recover various artifacts from the apps, including username, user id, last login time, user friend list, user email address, user phone number, profile picture, messages, posts, and comments.

In another independent investigation (32), Tinder app was found to be sharing user locations. The users could be located to within 100 feet of their present location. This is the second reported breach of privacy in the Tinder app, the first producing the exact latitude and longitude coordinates of users as well as their date of birth and Facebook IDs (33). These security flaws were uncovered by the community members who chose to responsibly disclose the breaches and have since been fixed.

To the best of our knowledge, there is no concerted effort to provide a taxonomy that provides a useful summary or categorization of forensic remnants of mobile social app investigations. This is the gap that this study seeks to address.

Case Study: 30 Social Apps

In this section, the findings of five apps (Facebook (version 36.0.0.45.19), LinkedIn (version 3.4.9), MeetMe (version 10.1.1), Path (version 4.3.3), and Whisper (version 4.6.5.223)) are discussed, and the interested reader is deferred to Tables 17 and 22 for the summary of findings of all the 30 apps and the forensic taxonomy, respectively. Facebook is one of the most widely used social networks internationally, centered on sharing photographs, links, and other user-generated contents. At the time of this research (i.e., June 2015), around 81% of adult Internet users (outside China) are reportedly members of Facebook (34). Similarly, LinkedIn is one of the most widely used professional social media sites, which allows users to network professionally, get in touch with vendors, recruit new employees, and keep up with the latest business or industry news and trends. LinkedIn has reportedly more than 300 million members and its revenue is estimated to be between $2.93 billion and $2.95 billion in 2015 (35). MeetMe is a social networking dating app with over 40 million users and over 1.1 million mobile daily active users (36). Path is a social network that allows capturing and sharing important moments such as photographs, videos, thoughts, places, music, television shows, movies, books, workouts, and sleep. The app was reported to have more than 4 million daily users (37). Whisper app allows users to share and discuss anonymous confessions. The app is popular with young people (users are primarily 18–24 years old and 70% users are female) and gets 3.5 billion page views per month (38).

In the case study, 30 popular free Android social apps available on Google Play Store (39) were examined. The 30 apps examined in this study were among the 100 most popular communication apps. Similar to the approach we took in our previous studies (12,13), the apps were installed and registered on two Google Nexus 4 phones (Android version 5.1). WiFi-to-WiFi communication channel was used for the experiments. Both phones had WiFi enabled and were connected to the same WiFi network. MicroSystemation XRY (version 6.10.1), a popular commercial forensic tool, was used to extract a logical forensic image (see the manual (40) for a step-by-step guide in conducting a logical acquisition using XRY). The use of XRY was based on the authors' access, and no personal recommendations or endorsement should be presumed from the tool selected.

TABLE 1—*Facebook artifacts.*

File/Table of Forensic Interest	Contents (of File/Table)	Location (of File/Table)
contacts contacts_indexed_data	Friend list and groups	/data/data/com.facebook.katana/databases/contacts_db2
bookmark_name	Groups followed	/data/data/com.facebook.katana/databases/bookmarks_db2
analytics_db_properties	User details	/data/data/com.facebook.katana/databases/analytics_db2
traffic_stats	Data usage	/data/data/com.facebook.katana/databases/data_usage_db
home_stories	Newsfeed	/data/data/com.facebook.katana/files/Newsfeed,/data/data/com.facebook.katana/databases/newsfeed_db
entities	Searches	/data/data/com.facebook.katana/databases/search_bootstrap_db
messages	Text messages	/data/data/com.facebook.katana/databases/threads_db2

A Windows 7 desktop machine was used to analyze the artifacts. Individual sets of experiments were conducted, one set for each app. After one set of experiments was concluded, the phone was wiped prior to installing the next app. We refer the interested reader to (13) for a detailed outline of the steps we undertook in forensic wiping.

Findings: Facebook

Files and data generated by the Facebook app were stored on the internal device memory, which is normally inaccessible by users. For example, the generated data stored in the databases of Facebook could be located in the `/data/data/com.facebook.katana/databases` directory. There are 34 databases in the Facebook app. In Table 1, we list the database tables/files containing the artifacts of forensic interest.

Friend List and Groups—The `contacts` table in the `contacts_db2` database stores the list of Facebook friends of a user. Each friend is identified by a unique `internal_id` and a unique Facebook id (`fbid`). The `first_name`, `last_name`, and `display_name` fields identify the names of the friends. The `communication_rank` field carries useful information for the forensic investigators regarding the frequency of communications between the device user and a contact. A higher value in the `communication_rank` field indicates a contact with more frequent communications. The `is_messenger_user` field identifies whether the friend uses Messenger for text communications. The `added_time_ms` field identifies the time in Unix millisecond epoch when the device user added the friend. The structure of the `contacts` table is given in Table 2.

TABLE 2—*Structure of the contacts table of the contacts_db database.*

Field Name	Meaning
`fbid`	Unique Facebook id of the contact
`first_name`	First name of contact as registered in Facebook
`last_name`	Last name of contact as registered in Facebook
`display_name`	Display name of contact in Facebook
`communication_rank`	A numerical value indicating the frequency of communications with a contact
`is_messenger_user`	Indicates whether the contact uses Facebook Messenger
`added_time_ms`	Time in Unix millisecond epoch when the contact was added

The `contacts_indexed_data` table in the `contacts_db2` database stores more information about the friends, among which the phone numbers of the friends are the most significant ones for forensic investigators. The phone numbers are stored in relation to the `contact_internal_id` field which corresponds to the `internal_id` field of the `contacts` table.

Facebook app stores the pages and groups followed by a user in the `bookmarks` table of the `bookmarks_db2` database. The `bookmark_name` field identifies the name of the page or group.

User Analysis—The `analytics_db_properties` table in the `analytics_db2` database of the Facebook app stores various information about the user. The table stores the id of the user who used the app in the last session, the id of the session, the last time when any data were sent, and the last time of an occurrence of an event.

Data Usage—The `traffic_stats` table (see Table 3) in the `data_usage_db` database stores the data usage of the device for using Facebook. The `date_col` field stores the dates when Facebook app was used from the device. The `data_received` and `data_sent` fields store the amounts of received and sent data in bytes on a specific day, respectively.

Newsfeeds—Facebook app stores the top stories from the newsfeed of a user in the `newsfeed_db` database as well as in different files in the `/data/data/com.facebook.katana/files/Newsfeed` directory. The files are named as `top_storiesTIMESTAMPS`, where TIMESTAMPS represents the Unix epoch time of creating the file. The `home_stories` table in the `newsfeed_db` database stores the cache file path of these files containing the newsfeeds (see Table 4). The files are partially encoded as the user status and names are in plaintext, whereas the URLs and images are encoded.

Facebook Searches—The `entities` table in the `search_bootstrap_db` database stores the searches

TABLE 3—*Structure of the traffic_stats table of the data_usage_db database.*

Field Name	Meaning
`date_col`	Date of using Facebook app
`data_received`	Amount of data received in bytes
`data_sent`	Amount of data sent in bytes

TABLE 4—*Structure of the home_stories table of the newsfeed_db database.*

Field Name	Meaning
feed_type	Type of newsfeed (top story/ most recent)
fetched_at	Time when newsfeed was fetched
cache_file_path	Name and location of the file where the newsfeed is stored
cache_file_offset	Offset position (in bytes) in the file where the newsfeed is stored
cache_file_data_length	Size of the cached file in bytes

performed by the user. The table stores the name of the page/person, fbid of the searched page/person, whether the searched page/person is connected (i.e., a friend) with the user, and whether the page/person has a verified Facebook profile.

Text Messages—The one-to-one and group messages are stored in the messages table of the threads_db2 database (see Table 5). The thread_key field identifies whether the chat is a one-to-one or group chat. In the event of a one-to-one chat, the fbid of the participants is specified. In the event of a group chat, a group id is assigned instead of the individual fbids of the participants. The text field stores the messages in plaintext. The sender field stores the Facebook email id of the sender, Facebook id of the sender, and the full name of the sender. The timestamp field stores the timestamp of the message in Unix millisecond epoch. The attachments field identifies the type of attachment (if any) with the attached file name. The coordinates field indicates the longitude and latitude of the user from where the message was sent. The source field identifies whether Facebook Messenger or web browser was used to send the message.

Findings: LinkedIn—Files and data generated by the LinkedIn app were stored in the internal device memory, which is normally inaccessible by users. For example, the generated data stored in the databases of LinkedIn are located in the /data/data/com.linkedin.android/databases directory. There are two databases in the LinkedIn app, namely linkedin.db and linkedin_search.db. In Table 6, we list the artifacts of forensic interest found in the LinkedIn app.

TABLE 5—*Structure of the messages table of the threads_db2 database.*

Field Name	Meaning
msg_id	A unique id of the message
thread_key	An identifier indicating one-to-one or group messages with participants' fbid
text	Plaintext messages
sender	Sender Facebook email with fbid and full name
timestamp_ms	Time of sending the message in Unix millisecond epoch
attachments	Filename and type of attachment
coordinates	User location with latitude and longitude
source	Indicating whether Facebook Messenger or web browser is used for the chat

Friend Lists and Connections—The connections table in the linkedin.db database stores the information of the friends/connections of a user (see Table 7). The display_name field stores the full name of the connection; first_name and last_name fields store the first and last name of the connection, respectively. The headline field stores the affiliation of the connection, and the picture_url field stores the globally accessible URL of the profile picture of the connection. The member_id field stores the unique LinkedIn id of the connection.

Friend Invitations—LinkedIn allows the sending and receiving of invitations to expand the social connection. The invitations received by the user are stored in the invitations table of the linkedin.db database. The table stores the display name, first name, last name, affiliation, URL of the profile picture, and LinkedIn id of the person who sent the invitation. The table also stores the timestamp when the invitation was sent and the message sent with the invitation in plaintext. The structure of the invitations table is given in Table 8.

Messages—The private messages exchanged between two users are stored in the messages table of the linkedin.db database. The structure of this table is similar to that of the invitations table (Table 8). The body field contains the plaintext messages. The folder field specifies the location of the message. The is_seen and is_read fields identify whether the message has been seen and read, respectively. The message_id is a unique id for the message. The subject field contains the subject of the message in plaintext, and the timestamp field stores the time when the message was received. The to_members field identifies the LinkedIn id of the member(s) to whom the message was sent. The table also stores the display name, firs name, last name, affiliation, URL of the profile picture, and LinkedIn id of the person who sent the message.

User Profile Picture—The profile picture of the user is stored in the /data/data/com.linkedin.android/files/sso directory of the LinkedIn app.

TABLE 7—*Structure of connections table of linkedin.db database.*

Field Name	Meaning
display_name	Full name of the friend / connection
first_name	First name of the friend / connection
last_name	Last name of the friend / connection
headline	Affiliation of the friend / connection
picture_url	Globally accessible URL of the profile picture of a friend / connection
member_id	Unique LinkedIn id of a friend / connection

TABLE 6—*LinkedIn artifacts.*

File/Table of Forensic Interest	Contents (of File/Table)	Location (of File/Table)
connections	Friend list	/data/data/ com.linkedin.android/databases/linkedin.db
invitations	Invitations	/data/data/ com.linkedin.android/databases/linkedin.db
messages	Text messages	/data/data/ com.linkedin.android/databases/linkedin.db
profile_pic.png	User profile picture	/data/data/com.linkedin.android/files/sso

TABLE 8—*Structure of invitations and messages tables of linkedin.db database.*

Field Name	Meaning
body	Body of the invitation / message in plaintext
folder	Location of the invitation / message in LinkedIn account
is_read	0 if unread, 1 if read
is_seen	0 if unseen, 1 if seen
message_id	Unique id of the invitation / message
message_type	Type of message
subject	Subject of the invitation message in plaintext
timestamp	Timestamp of receiving the invitation
to_members	LinkedIn ids of member(s) to whom the invitation / message has been sent
from_display_name	Display name of the user who sent the invitation / message
from_first_name	First name of the user who sent the invitation / message
from_last_name	Last name of the user who sent the invitation / message
from_headline	Affiliation of the user who sent the invitation / message
from_picture_url	Globally accessible URL of the profile picture of the sender
from_member_id	Unique LinkedIn id of the sender

Findings: MeetMe—Our analysis indicates that the files and databases generated by MeetMe are stored in the internal device memory, which is normally inaccessible by users. For example, the databases of MeetMe are stored in the /data/data/com.myyear book.m/databases directory. The names, locations, and contents of the artifacts of forensic interest generated by the app are listed in Table 9.

Exchanged Text Messages—The conversations table in the chats.db database stores the last message of each conversation thread. The near_member_id field stores the MeetMe member id of the device user, and far_member_id stores the other user participating in the conversation. The thread_id field contains a unique id for each thread. The last_updated_at field stores the timestamp of last message sent/received in the thread, and the last_activity_preview field stores the last message of the thread in plaintext.

The complete conversations are stored in the messages table of the chats.db database. The thread_id field identifies the unique thread id similar to the conversations table. The sent_by field contains the MeetMe id of the sender, sent_at field stores the timestamp when the message was sent, seen_at stores the timestamp of when the message was seen (read) by the recipient, type field contains the type of the message (e.g., text, photograph), and the body field stores the plaintext messages.

The structure of the conversations and messages tables is given in Table 10.

Friend Lists—The members table in the chats.db database stores the list of MeetMe friends of a user. Each friend is identified by a unique member_id. The first_name and last_name fields identify the name of the friend. The age, gender, state_abbreviation, and country_id fields identify the age, gender, name of the state, and country id of the friend, respectively. The structure of the members table is given in Table 11.

User Location and Device Information—The sessions table in the /data/data/com.my yearbook.m/databases/com.localytics. android.3d6dfb80bc77408754a1da607d17 408b5b3a7289736558adb87ceafeaf599cd6. sqlite database stores information about user location and device information. The table identifies the mobile operator being used by the device. The mobile operator can be identified even if WiFi connection is used. We could also identify the app version, device model, android version, and device manufacturer based on information from the table. The name of the sqlite database that stores the sessions table is randomly generated (i.e., the name may vary with each installation of the app on different devices). However, the location of the database remains the same.

Stored Images and Facebook Tokens—MeetMe app stores the profile images of the visited accounts in /data/data/com.myyearbook.m/cache/Picasso-cache directory. The user profile pictures are stored in the //data/data/com.myyearbook.m/cache/doodle-photos directory.

In the directory /data/data/com.myyear book.m/shared_prefs, we located the following files of interest:

- com.facebook.sdk.attributionTracking.xml
- com.facebook.SharedPreferencesTokenCachingStrategy.DEFAULT_KEY.xml

TABLE 9—*MeetMe artifacts.*

File/Table of Forensic Interest	Contents (of File/Table)	Location (of File/Table)
conversations	last message of each conversation thread	/data/data/com.myyearbook.m/databases/chats.db
messages	Text messages	/data/data/com.myyearbook.m/databases/chats.db
members	Friend list	/data/data/com.myyearbook.m/databases/chats.db
sessions	User location and device information	/data/data/com.myyearbook.m/databases/com.localytics.android.3d6dfb80bc77408754a1da607d17408b5b3a7289736558adb87ceafeaf599cd6.sqlite
Files in different directories	Images	/data/data/com.myyearbook.m/cache
com.facebook.sdk.attributionTracking.xml, com.facebook.SharedPreferencesTokenCachingStrategy.DEFAULT_KEY.xml	Facebook token	/data/data/com.myyearbook.m/shared-prefs

TABLE 10—*Structure of conversations and messages tables of chat.db database.*

Field Name	Table	Meaning
near_member_id	conversations	MeetMe id of the device user
thread_id	conversations, messages	Unique thread id
far_member_id	conversations,	MeetMe id of the participant in the conversation
last_updated_at	conversations	Date and time when last message was sent in the conversation
last_activity_preview	conversations	The plaintext last message in the thread
last_sent_by	conversations	MeetMe id of the user who sent the last message in the thread
last_seen_on_server	conversations	Date and time when the user was last seen on MeetMe
sent_by	messages	MeetMe id of the message sender
sent_at	messages	Date and time when the message was sent
type	messages	Type of the message (e.g., text, photograph)
seen_at	messages	Date and time when the message was received and seen
body	messages	The plaintext message

TABLE 11—*Structure of members table of chat.db database.*

Field Name	Meaning
member_id	Unique MeetMe id of the contact
first_name	First name of contact as registered in Facebook
last_name	Last name of contact as registered in Facebook
photo_url	URL of the profile picture of the user
age	Age of the user
gender	Gender of the user
state_ abbreviation	Abbreviated form of the state location of the user
country_id	A numeric value identifier for the country of the user

Both files contain the Facebook authentication token string for the app. Facebook tokens can be used to tie account identities together and gain access to user contributed information on Facebook.

Findings: Path

The main database of path is the path_4.3.3_503_en_US.db database, which is stored in the /data/data/com.path/databases directory. The names, locations, and contents of the artifacts of forensic interest generated by the app are listed in Table 12.

Friend Lists and Profile Images—The FRIEND_LIST table in the path_4.3.3_ 503_en_US.db database stores the Path ids of the friends of the device user. The USER table stores the detailed information of the device user and the friends of the device user. The _id field in the USER table stores the unique path id of the users. The USERNAME field stores the user names. The FIRST_NAME and LAST_NAME fields store the first and last names of the users, respectively. The FACEBOOK_ID and EMAIL fields are empty fields even though a user logs in using Facebook id and/or provides email id during registration. The IS_FRIEND field indicates whether the listed person is the device user, or a friend of the device user. A value of 1 in the IS_FRIEND field indicates the listed person is a friend of the device user, whereas a value of 0 indicates the listed person is the device user. The SMALL_URL, MEDIUM_URL, and ORIGINAL_URL fields store the URL of the profile images of the users. There are two fields in the table associated with timestamp. One is the CREATED_AT field which stores the timestamp when the user account was created, and the other is the INCOMING_REQUEST_CREATED field which stores the timestamp when the friend request was sent. The structure of the USER table is given in Table 13.

User Activities, Comments, and Notifications—The MOMENT table (Table 14) stores all the activities performed in Path by the device user and the friends of the device user. The _id field is used to identify an activity. The USER_ID field is used to identify the user who initiated the activity. The HEADLINE field contains the activity in plaintext. The activities may include the joining of a new user, locating a user, changing profile picture, watching a movie, hearing a song, and so on. The SUBHEADLINE field stores additional information about the activities (e.g., time and date). The CREATED_IN_SECONDS, CREATED_ON_

TABLE 12—*Path artifacts.*

File/Table of Forensic Interest	Contents (of File/Table)	Location (of File/Table)
FRIEND_LIST, USER	Friend list and profile images	/data/data/com.path/databases/path_4.3.3_ 503_en_US.db
MOMENT	User activities	/data/data/com.path/databases/path_4.3.3_ 503_en_US.db
COMMENT	Comments	/data/data/com.path/databases/path_4.3.3_ 503_en_US.db
ACTIVITY	Notifications	/data/data/com.path/databases/path_4.3.3_ 503_en_US.db
CITY	User location	/data/data/com.path/databases/path_4.3.3_ 503_en_US.db
application.xml	User email id	/data/data/com.path/shared_prefs
com.facebook.internal. preferences.APP_SETTINGS.xml	Facebook token	/data/data/com.path/shared_prefs

TABLE 13—*Structure of USER table of Path database.*

Field Name	Meaning
_id	Unique Path id of the contact
USER_NAME	User name or login id of the user
FIRST_NAME	First name of contact as registered in Path
LAST_NAME	Last name of contact as registered in Path
FACEBOOK_ID	Empty field
EMAIL	Empty field
IS_FRIEND	0 if device user himself, 1 if a friend of the device user
SMALL_URL	URL of the profile picture of the user
MEDIUM_URL	
ORIGINAL_URL	
CREATED_AT	Time when the user account was created
INCOMING_ REQUEST_CREATED	Time when friend request was sent

TABLE 14—*Structure of MOMENT table of Path database.*

Field Name	Meaning
_id	Unique id of the activity
USER_ID	Unique Path id of the user
HEADLINE	User activity or post in plaintext
SUBHEADLINE	Additional information about user activity
CREATED_IN_SECONDS	Timestamps of the activities
CREATED_ON_SERVER_ IN_SCONDS	
CREATE_DATE_MILLIS	
CREATED_ON_SERVER_ DATE_MILLIS	

SERVER_IN_SCONDS, CREATE_DATE_MILLIS, and CREATED_ON_SERVER_DATE_MILLIS fields store the timestamps of the activities.

The COMMENT table stores the comments posted in an activity by the device user or a friend of the device user. The USER_ID identifies the user who posted the comment. The MOMENT_ID identifies the id of the activity corresponding to the _id field of the MOMENT table. The BODY field stores the plaintext comment, and the CREATED field stores the timestamp in Unix millisecond epoch.

The ACTIVITY table stores the notifications received by the device user. The ACTOR_ID field stores the Path id of the user who sent the notification. The ACTIVITY_ DESCRIPTION and ACTIVITY_CALLOUT fields store the plaintext notification. The CREATED_AT field stores the timestamp of the notification.

User Location, Email id, and Facebook Token—The CITY table in the /data/data/com.path/ databases/path_4.3.3_503_en_US.db database stores the name of the city, province, and country of the device user in plaintext. The email id of the device user is stored in the application.xml file in the /data/ data/ com.path/shared_prefs directory.

TABLE 16—*Structure of m table of c.db database.*

Field Name	Meaning
c_id	A numeric value to identify each message thread
mid	A unique id of the messages
ts	Timestamp in Unix millisecond epoch
sid	Sender Whisper id
text	Plaintext message
mine	0 if message received; 1 if message sent

The com.facebook.internal.preferences.APP_SETTINGS.xml file located in the /data/ data/com.path/shared_prefs directory contains the Facebook authentication token string for the app. Facebook tokens can be used to tie account identities together and gain access to information entered into Facebook by the user.

Findings: Whisper

Similar to the other apps investigated in this study, files and data generated by the Whisper app were stored on the internal device memory. For example, the generated data stored in the databases of Whisper could be located in the /data/data/sh.whisper/databases directory. There are three databases in the Whisper app. In Table 15, we list the artifacts of forensic interest found in the Whisper app.

Text Messages—The exchanged text messages are stored in the m table (see Table 16) of the c.db database. The mid field identifies the unique message id, and the sid field identifies the Whisper id of the sender. The ts field stores the timestamp of sending/receiving the messages in Unix millisecond epoch. A value of 0 in the mine field indicates the message is received by the device user, and a value of 1 in the mine field indicates the message has been sent by the user. The plaintext message is stored in the text field. The c_id field uses numeric values for each message thread. A message thread can be reconstructed by combining the messages with the same c_ids together. As Whisper does not maintain any user profile, it was not possible to reveal the identities of the users involved in text message exchanging.

User Locations—Whisper claims to be a social networking platform, which does not require an identity for the user to use the services. Users do not need to register individually to get connected using Whisper. However, our analysis found that the device user location was stored in the sh.whisper_preferences.xml file of the app. The file is stored in the location /data/data/sh.whisper/shared_prefs. The coordinates of the longitude and latitude of the user are stored in this file. A snapshot of the user longitude and latitude in the sh.whisper_preferences.xml file is given in Fig. 1.

Individual Whisper user locations are stored in the w table of the w.db database. A user can choose not to declare his/her

TABLE 15—*Whisper artifacts.*

File/Table of Forensic Interest	Contents (of File/Table)	Location (of File/Table)
m	Text messages	/data/data/sh.whisper/databases/c.db
sh.whisper_preferences.xml	Location of the user	/data/data/sh.whisper/shared_prefs
w	Location of others	/data/data/sh.whisper/databases/w.db
sh.whisper_preferences.xml	User passcode	/data/data/sh.whisper/shared_prefs

location while logging into Whisper, and in this context, their location will have a "somewhere" value in the location field of the w table. A snapshot of the individual user locations from the w table of the w.db database is given in Fig. 2.

User Passcode—The Whisper app allows a user to use a 4-digit passcode to access their account in the mobile device. Our analysis found the passcode stored in plaintext in the sh.whisper_preferences.xml file (Fig. 3).

Proposed Forensic Taxonomy for Social Apps

Due to the increasing number of social apps, it is important to have a forensic taxonomy for existing popular social apps. Therefore, based on the case study of 30 apps (see Table 17 for a summary of findings), a forensic taxonomy is proposed.

The social apps are broadly categorized into three categories (according to their purposes), namely Friends and Family apps, Dating apps, and Professional Networking apps:

Friends and Family apps are used to connect and maintain social relationships with friends and relatives. These social apps are commonly used for socializing with people, sharing thoughts, posting images and videos, and posting day-to-day activities, but are not generally used for real-time text communications.

Dating apps provide a platform facilitating the sharing of private information that one may not share on other social apps. These could include information like sexual preferences or fetishes. These apps provide a networking opportunity to find suitable dates or partners.

Professional Networking apps are the social apps that provide a professional relationship among users. These apps allow users to create and share resumes and other professional interests, and connect with other users having similar professional backgrounds.

From the artifacts determined from the forensic analysis of the 30 most popular Android social apps, the artifacts are broadly categorized into four groups, namely User and contact information, Exchanged messages, Timestamps, and User location and other artifacts. To maintain consistency in the forensic taxonomy for the different app categories, the naming convention used in this article is similar to that used in the previously published taxonomies (12,13).

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <float name="longitude_prefs_key" value="138.61969" />
    <float name="lattitude_prefs_key" value="-34.810112" />
    <int name="wgcm_appVersion" value="181" />
    <string name="app_launch_tab">popular</string>
```

FIG. 1—*Longitude and latitude of user location in Whisper app.*

_id	puid	user	ts	url	location
Filter	Filter	Filter	Filter	Filter	Filter
Individual	051921ced9a12...	[redacted]	1435036833000	http://cdn-clie...	Flint
051921b123e32...	051921b123e32...	[redacted]	1435033005000	http://cdn-clie...	Wheat Ridge
051921e027ab7...	051921e027ab7...	[redacted]	1435036683000	http://cdn-clie...	Somerset
050f00e5bfd2f9...	050f00e5bfd2f9...	[redacted]	1423871495709	http://cdn-clie...	Venice
0519273460380...	0519273460380...	[redacted]	1435031165322	http://cdn-clie...	Adelaide, South Australia, AU
0518e2b3e07cfe...	0518e2b3e07cfe...	[redacted]	1434736843102	http://cdn-clie...	Somewhere
0518bc9b54eec...	0518bc9b54eec...	[redacted]	1434573222536	http://cdn-clie...	Somewhere

FIG. 2—*Individual user locations in Whisper.*

```
<boolean name="pin_exists" value="true" />
<int name="sessions" value="3" />
<int name="creates" value="5" />
<string name="pin">2525</string>
<string name="puid">c01f1e30-b9da-4ac6-a7ac-2909f476ebf1
```

FIG. 3—*Plaintext passcode stored in Whisper.*

TABLE 17—*Summary of findings.*

						Artifact Category																							
						User and Contact Information								Exchanged Messages					Timestamps						User Location and Other Artifacts				
App ID	App Name	Version	App Categories			Find phone number from Contact ID	Find date of Birth of the User	Recover Email id of the user	Recover user name	Find user pro fi LIG MISSING le image	Recover user passcode	View friend list of the user	View imported address book	View chat history	Determine types of exchanged messages (text, audio, video)	View received noti fi LIG MISSING cations	View unencrypted exchanged text messages	View unencrypted exchanged images	Determine when add request was sent to/from a contact	Determine when add request was accepted by a contact	Determine when text/multimedia message was sent	Determine when text multimedia message was received/delivered	Determine when notification was received	Determine when status was posted	Identify latitude and longitude of user location	Identify name and place of user location	Extract databases	Identify Facebook tokens	View status posts
App1	Facebook	36.0.0.45.19	F*	N†	N	F	N	N	F	N	N	F	F	F	F	N	F	N	N	F	F	N	F	N	N	N	F	N	N
App2	LinkedIn	3.4.9	N	N	F	N	N	N	F	F	N	F	N	F	F	F	F	N	F	N	F	F	F	N	N	N	F	N	N
App3	MeetMe	10.1.1	N	F	N	N	N	N	F	F	N	N	N	F	F	N	F	N	N	N	F	F	N	N	N	F	F	F	N
App4	Path	4.3.3	F	N	N	N	N	F	F	F	N	F	N	F	N	N	F	N	F	N	F	F	N	F	N	F	F	F	F
App5	Whisper	4.6.5.223	F	N	N	N	N	N	F	N	F	N	N	F	N	N	F	N	N	N	F	N	N	N	F	F	F	N	N
App6	9Chat	2.7.2	F	N	N	N	N	N	F	F	N	N	N	F	F	N	F	N	N	N	F	N	N	N	N	N	F	F	N
App7	Ask.fm	2.1	F	N	N	N	N	N	F	F	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	F	F	N
App8	Badoo	4.6.4	N	F	N	N	N	N	N	F	N	N	N	F	F	N	F	N	N	N	F	N	N	N	N	N	F	F	N
App9	Fling	1.0.60	F	N	N	N	F	F	F	N	N	N	N	F	F	N	F	F	N	N	N	N	N	N	F	F	F	N	N
App10	Indiegogo	1.2.6	F	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	F	N	N
App11	Kiwi	1.3.11	F	N	N	N	N	N	N	F	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	F	F	N
App12	Meetup	2.7.6	F	N	N	N	N	N	N	F	N	N	N	F	F	N	F	N	N	N	F	F	N	N	N	F	F	F	N
App13	MeowChat	2.21.3	F	N	N	N	N	N	F	F	N	N	N	F	F	N	F	N	N	N	F	N	N	N	N	N	F	F	N
App14	Minds	1.0.12	F	N	N	N	N	N	N	F	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
App15	MocoSpace	2.6.57	N	F	N	N	N	N	F	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	F	F	F	N
App16	Oasis	2.0.326	N	F	N	N	N	N	F	F	N	N	N	N	N	F	N	N	N	N	N	N	F	N	N	N	F	F	N
App17	OkCupid	4.4.1	N	F	N	N	N	N	N	F	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
App18	ooVoo	2.5.2	F	N	N	N	N	F	F	N	N	F	N	F	F	N	F	N	N	N	F	F	N	N	N	N	F	F	N
App19	Pinterest	4.8.2	F	N	N	N	N	N	F	F	N	N	N	F	N	F	N	F	N	N	N	N	F	N	N	N	F	N	N
App20	POF Dating	3.15.0.1415972	N	F	N	N	N	N	F	F	N	N	N	N	N	F	N	F	N	N	N	N	F	N	N	N	F	F	N
App21	SinglesAroundMe	1.2.0	N	F	N	N	F	F	F	F	N	N	N	F	F	N	F	N	N	N	F	F	N	N	F	F	F	F	N
App22	Skout	4.12.8	N	F	N	N	N	N	F	N	N	F	N	F	F	N	F	N	N	N	F	N	N	N	F	N	F	F	N
App23	Snapchat	9.8.0.0	F	N	N	N	N	N	N	F	N	F	F	F	N	N	F	N	N	N	N	N	N	N	N	N	F	N	N
App24	Tagged	6.0.1	F	N	N	N	F	N	F	F	N	F	N	F	F	N	F	N	N	N	F	N	N	N	N	F	F	F	N
App25	Tapatalk	4.15.5	F	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	F	F	N
App26	Tumblr	3.8.7.16	F	N	N	N	N	F	F	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	F	N	N
App27	Twitter	5.57.0	F	N	N	N	N	N	F	F	N	N	N	N	N	N	N	F	N	N	N	N	N	N	N	F	F	N	F
App28	Vk	3.12	F	N	N	N	N	N	F	F	N	F	F	F	F	N	F	N	N	N	F	F	N	N	N	N	F	F	N
App29	We Heart It	4.3	F	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	F	F	N
App30	Wishbone	2.0	F	N	N	N	N	N	N	F	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	F	N	N

*"F"–detailed information was recovered.
†"N"—unsupported category.

User and contact information: This group of artifacts contains the following data remnants related to the user identity and list of contacts:

1 *Find phone number from a contact ID*: It is not always possible to determine the phone number of the user from his/her contact ID. However, some apps store the phone number with the user ID.
2 *Find date of birth of the user*: Apps may require users to provide their date of birth during registration. The date of birth artifact can be useful for identifying a user.
3 *Recover email id of the user*: Apps may also require users to provide their email id during registration. The email id artifact can be useful for identifying a user.
4 *Recover user name:* Communication apps generally require a user to create a personal user name, which could be forensically recovered in a number of apps.
5 *Find user profile image*: The user profile image is an important artifact to visually identify a user.
6 *Recover user passcode*: User passcode to access the user account is, perhaps, one of the most important artifacts for a forensic investigator. For example, it is known that users tend to use the same passcode/username and password for different accounts, and recovery of the passcode may allow the investigators to gain access to other social networking or Internet accounts.
7 *View friend list of the user*: This group of artifacts contains data remnants relating to the user's contacts.
8 *View imported address book*: Many apps import the stored contact list from the phone address book. This group of artifacts helps to identify all the contacts of a user.

Exchanged messages: This group of artifacts contains the information of the text, multimedia, and group message communications:

1 *View chat history*: This allows an investigator to determine whether there was a prior conversation between the users.
2 *Determine the types of exchanged messages (text, audio, video)*: This allows an investigator to determine the message type.
3 *View received notifications*: Notifications are frequently received by the users about their posts and any other activities. This artifact allows tracking of the notifications received by the user.
4 *View unencrypted exchanged text messages*: The unencrypted exchanged messages stored in the app database.
5 *View unencrypted exchanged images*: Most apps store the sent or received images in their database, and in some cases, unencrypted.

Timestamps: This group of artifacts contains the information of the timestamp of a communication.

1 *Determine when add request was sent to/from a contact*: This is the timestamp when a friend request was sent to or received from another user on the device.
2 *Determine when add request was accepted by a contact*: This is the timestamp when a friend request was accepted by a contact using the device.
3 *Determine when text/multimedia message was sent*: The timestamp of the sent text or multimedia (e.g., image) message.
4 *Determine when text/multimedia message was received/delivered*: The timestamp when the text or multimedia (e.g., image) message was received or delivered.
5 *Determine when notification was received*: The timestamp when a notification was received by the user.
6 *Determine when status was posted*: The timestamp when a status was posted by the user.

User location and other artifacts: The user location and remaining artifacts are considered under this category.

1 *Identify latitude and longitude of user location*: This allows an investigator to determine the exact coordinates of the location of the user.
2 *Identify name and place of user location*: This allows an investigator to determine the name and place of user location.
3 *Extract databases*: Android apps typically generate their own databases in the internal device memory, where the latter is normally inaccessible by users. Information from these databases could be used to locate useful user information.
4 *Identify Facebook tokens*: Many apps allow a user to login using Facebook authentication string. This artifact allows an investigator to locate the Facebook authentication strings of a user.
5 *View status posts*: This group of artifacts contains the data remnants related to the posted statuses by a user.

The findings are summarized using the above-proposed categorization of the artifacts (see Table 17). Based on the categorizations, we propose a two-dimensional taxonomy of social apps (Fig. 4). In the taxonomy, the social app categories are represented in one dimension, and the forensic artifact categories are represented in the other dimension. The locations of the artifacts of the 30 apps are listed in Tables 18–21. Each of the four tables contains the locations of the artifacts of the 30 social apps for a specific artifact category (e.g., Table 18 contains the locations of the artifacts relating to user and contact information of the 30 social apps).

Due to the nature of mobile apps and mobile app forensics, it is not possible to have a single generic model for different app categories. For example, a key difference between the forensic taxonomy for the mHealth apps in our earlier research (12) and this work is in the number of forensic artifacts. In the forensic taxonomy for the mHealth apps, only seven forensic artifacts were identified, whereas for the social apps, 24 different types of forensic artifacts were identified, which were categorized under four broad groups. An application of this proposed forensic taxonomy is given in Table 22. The social apps are identified with the app IDs specified in Table 17.

A Comparative Summary

Similar to the forensic taxonomy presented in this article, our previous forensic taxonomies for Android mHealth apps (12) and Android communication apps (13) had two dimensions where the apps were divided into categories in one dimension based on their purposes, and the forensic findings were represented in the other dimension. However, due to the different services provided by the different apps, the categories are different for mHealth, communication, and social apps. More specifically, Android mHealth apps, communication apps, and social apps were divided into four categories (12), three categories (13), and three categories (i.e., Friends and Family apps, Dating apps, and Professional Networking apps), respectively. The artifacts found in communication apps and social apps were broadly divided into four categories, whereas

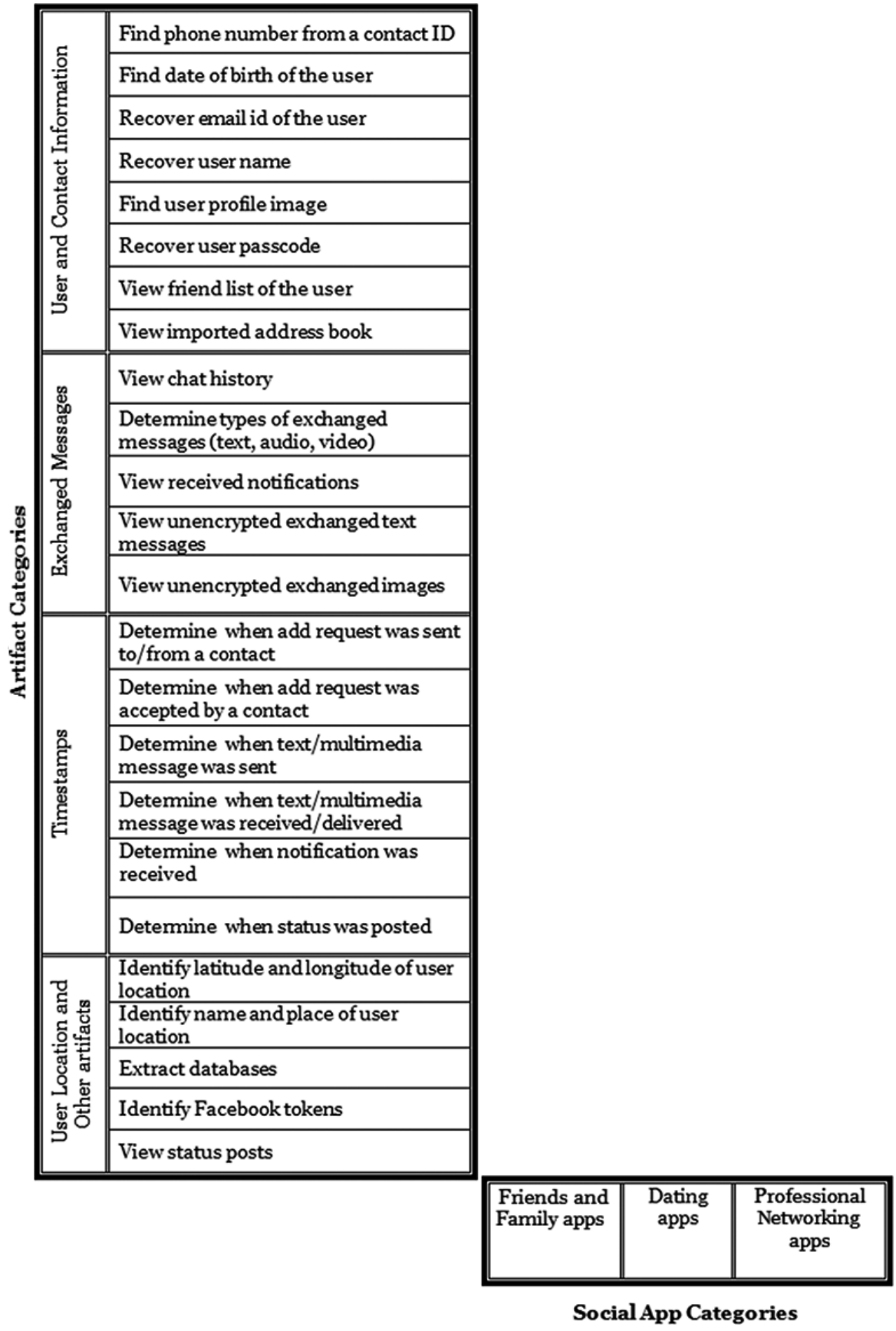

FIG. 4—*A two-dimensional social app forensic taxonomy.*

TABLE 18—*Location of the artifacts containing user and contact information.*

			Location of User and Contact Information Related Artifacts (Database/Table/File)							
App ID	App Name	Parent Directory	Find Phone Number from Contact ID	find Date of Birth of the User	Recover Email id of the User	Recover User Name	Find user Profile Image	Recover User Passcode	View Friend List of the User	View Imported Address Book
App1	Facebook	/data/data/com.facebook.katana	/databases/Contact_db2/contacts	N/A	N/A	/databases /Contact_db2/contacts	/databases /Contact_db2/contacts	N/A	/databases Contact_db2/contacts	N/A
App2	LinkedIn	/data/data/com.linkedin.android	N/A	N/A	N/A	/LinkedInPrefs/shared_prefs	/files/sso	N/A	/databases/linkedin.db/connections	N/A
App3	MeetMe	/data/data/com.myyearbook.m/	N/A	N/A	N/A	/databases /chats.db/members	/cache/picasso-cache	N/A	N/A	N/A
App4	Path	/data/data/com.path	N/A	N/A	/shared_prefs/application	/databases /path_4.3.3_503_en_US.db/USER	/databases /path_4.3.3_503_en_US.db/FRIEND_LIST	N/A	/databases/path_4.3.3_503_en_US.db/FRIEND_LIST	N/A
App5	Whisper	/data/data/sh.whisper/databases	N/A	N/A	N/A	/shared_prefs/sh.whisper_preferences	N/A	/shared_prefs/sh.whisper_preferences.xml	N/A	N/A
App6	9Chat	/data/data/com.ninechat.android.chat	N/A	N/A	N/A	/databases/core/PROFILE	/databases /cache/picasso-cache	N/A	N/A	N/A
App7	Ask.fm	/data/data/com.askfm	N/A	N/A	N/A	/shared_prefs/AskFm Preferences	/cache/Image RsponseCache	N/A	N/A	N/A
App8	Badoo	/data/data/com.badoo.mobile	N/A	N/A	N/A	N/A	/cache/decorator	N/A	N/A	N/A
App9	Fling	/data/data/com.unii.fling	N/A	/shared_prefs/fling_prefs.xml	/shared_prefs/fling_prefs.xml	/shared_prefs/ fling_prefs.xml	N/A	N/A	N/A	N/A
App10	Indiegogo	/data/data/com.indiegogo.android	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
App11	Kiwi	/data/data /com.chatous.pointblank	N/A	N/A	N/A	N/A	/cache/picasso-cache	N/A	N/A	N/A
App12	Meetup	/data/data /com.meetup	N/A	N/A	N/A	N/A	/databases/com.meetup.db/members	N/A	N/A	N/A
App13	MeowChat	/data/data /com.minus.android	N/A	N/A	N/A	/databases /com.minus.android/MinusMessage	/cache/image_manager_disk_cache	N/A	N/A	N/A
App14	Minds	/data/data /com.minds.mobile	N/A	N/A	N/A	N/A	/cache	N/A	N/A	N/A
App15	MocoSpace	/data/data /com.jnj.mocospace.android	N/A	N/A	N/A	/shared_prefs/SerializedUser	N/A	N/A	N/A	N/A
App16	Oasis	/data/data /com.oasis.wrapper	N/A	N/A	N/A	/databases/Alert/ALERT	/databases/Alert/ALERT	N/A	N/A	N/A
App17	OkCupid	/data/data /com.okcupid.okcupid	N/A	N/A	N/A	N/A	/cache/org.chromium.android_webview	N/A	N/A	N/A

TABLE 18—*Continued.*

			Location of User and Contact Information Related Artifacts (Database/Table/File)							
App ID	App Name	Parent Directory	Find Phone Number from Contact ID	find Date of Birth of the User	Recover Email id of the User	Recover User Name	Find user Profile Image	Recover User Passcode	View Friend List of the User	View Imported Address Book
App18	ooVoo	/data/data /com.oovoo	N/A	N/A	/databases/ Core.db/ groups	/databases/Core.db/ appConfig	N/A	N/A	/databases/Core. db/groups	N/A
App19	Pinterest	/data/data /com.pinterest	N/A	N/A	N/A	/databases/ pinterest-db14320 90229690/USER	/data/data/com.pinterest/ cache/picasso_cache	N/A	N/A	N/A
App20	POF Dating	/data/data /com.pof. android	N/A	N/A	N/A	/databases/NOTIFICATION_ CENTER/nc_user	/sdcard/Android/data/ com.pof.android/cache/ images	N/A	N/A	N/A
App21	Singles AroundMe	/data/data /com.singles aroundme.android	N/A	/databases / samdb/ profiles	/databases/ samdb/profiles	/databases /samdb/profiles	/databases /samdb/list_ new_peeps	N/A	N/A	N/A
App22	Skout	/data/data /com.skout. android	N/A	N/A	N/A	/databases /com,skout. android/ skoutUsersTable	N/A	N/A	/databases/ com,skout. android/ skoutUsers Table	N/A
App23	Snapchat	/data/data /com.snapchat. android	N/A	N/A	N/A	N/A	/cache/profile/image/	N/A	/databases/ tcspahn.db/ Friends	/databases/ tcspahn.db/ Contacts NotOn Snapchat Table
App24	Tagged	/data/data /com.taggedapp	N/A	/databases / tagged_ 6029676964/ users	N/A	/databases /tagged_ 6029676964/ luv_users_view	/databases /tagged_ 6029676964/luv_ users_view	N/A	/databases/ tagged_ 6029676964/ friends	N/A
App25	Tapatalk	/data/data /com.quoord. tapatalkpro.activity	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
App26	Tumblr	/data/data /com.tumblr	N/A	N/A	/shared_prefs/ tumblr	/shared_prefs/tumblr	N/A	N/A	N/A	N/A
App27	Twitter	/data/data /com.twitter. android	N/A	N/A	N/A	/databases/966083424- 23.db/tokens_ user_view	/sdcard/Android/data/ com.twitter.android/ cache/users	N/A	N/A	N/A
App28	Vk	/data/data /com.vkontakte. android	N/A	N/A	N/A	/shared_prefs/null	/databases/vk.db/users	N/A	/databases/ vk.db/ users	/databases/ vk.db/ imported_ contacts
App29	We Heart It	/data/data /com.weheartit	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
App30	Wishbone	/data/data /com.science. wishboneapp	N/A	N/A	N/A	N/A	/cache/org.chromium. android_webview	N/A	N/A	N/A

TABLE 19—*Location of the artifacts containing exchanged messages.*

			Location of Exchanged Messages Related Artifacts (Database/Table/File)				
App ID	App Name	Parent Directory	View Chat History	Determine Types of Exchanged Messages (Text, audio, Video)	View Received Notifications	View Unencrypted Exchanged Text Messages	View Unencrypted Exchanged Images
App1	Facebook	/data/data/com.facebook.katana	/databases/threads_db2/messages	/databases /threads_db2/messages	N/A	/databases /threads_db2/messages	N/A
App2	LinkedIn	/data/data/com.linkedin.android	/databases /linkedin.db/messages	/databases /linkedin.db/messages	/databases/linkedin.db/notification_center	/databases /linkedin.db/messages	N/A
App3	MeetMe	/data/data/com.myyearbook.m/	/databases /chats.db/messages	/databases /chats.db/messages	N/A	/databases /chats.db/conversations	N/A
App4	Path	/data/data/com.path	/databases/ path_4.3.3_503_en_US/COMMENT	N/A	N/A	/databases/ path_4.3.3_503_en_US/COMMENT	N/A
App5	Whisper	/data/data/sh.whisper/databases	/databases /databases/c.db/c	N/A	N/A	/databases /databases/c.db/c	N/A
App6	9Chat	/data/data/com.ninechat.android.chat	/databases/core/CHAT_MESSAGE	/databases/core/CHAT_MESSAGE	N/A	/databases/core/CHAT_MESSAGE	N/A
App7	Ask.fm	/data/data/com.askfm	N/A	N/A	N/A	N/A	N/A
App8	Badoo	/data/data/com.badoo.mobile	/databases/badoo.db/Message	/databases/badoo.db/Message	N/A	/databases/badoo.db/Message	N/A
App9	Fling	/data/data/com.unii.fling	/database/fling.db/CHAT_MESSAGE_DB_MODEL	/database/fling.db/CHAT_MESSAGE_DB_MODEL	N/A	/database/fling.db/CHAT_MESSAGE_DB_MODEL	sdcard/com.unii.fling
App10	Indiegogo	/data/data/com.indiegogo.android	N/A	N/A	N/A	N/A	N/A
App11	Kiwi	/data/data /com.chatous.pointblank	N/A	N/A	N/A	N/A	N/A
App12	Meetup	/data/data /com.meetup	/databases/com.meetup.db/conversations	/databases/com.meetup.db/conversations	N/A	/databases/com.meetup.db/conversations	N/A
App13	MeowChat	/data/data /com.minus.android	/databases/com.minus.android/MinusMessage	/databases/com.minus.android/MinusMessage	N/A	/databases/com.minus.android/MinusMessageList	N/A
App14	Minds	/data/data /com.minds.mobile	N/A	N/A	N/A	N/A	N/A
App15	MocoSpace	/data/data /com.jnj.mocospace.android	N/A	N/A	N/A	N/A	N/A
App16	Oasis	/data/data /com.oasis.wrapper	N/A	N/A	/databases/Alert/ALERT	N/A	N/A
App17	OkCupid	/data/data /com.okcupid.okcupid	N/A	N/A	N/A	N/A	N/A
App18	ooVoo	/data/data /com.oovoo	/databases/Core.db/moment	/databases/Core.db/moment	N/A	/databases/Core.db/moment	N/A
App19	Pinterest	/data/data /com.pinterest	/databases/pinterest-db1433732876003/NOTIFICATION	N/A	/databases/pinterest-db1433732876003/NOTIFICATION	N/A	/cache/picasso-cache

TABLE 19—*Continued.*

App ID	App Name	Parent Directory	Location of Exchanged Messages Related Artifacts (Database/Table/File)				
			View Chat History	Determine Types of Exchanged Messages (Text, audio, Video)	View Received Notifications	View Unencrypted Exchanged Text Messages	View Unencrypted Exchanged Images
App20	POF Dating	/data/data /com.pof.android	N/A	N/A	/databases/NOTIFICATION_CENTER/nc_notification	N/A	/sdcard/com.pof.android/cache/images
App21	Singles AroundMe	/data/data /com.singlesaroundme.android	/databases/samdb/messages_threaded	/databases/samdb/messages_conversation	N/A	/databases/samdb/messages_conversation	N/A
App22	Skout	/data/data /com.skout.android	/databases/skoutDatabase/skputMessagesTable	/databases/skoutDatabase/skputMessagesTable	N/A	/databases/skoutDatabase/skputMessagesTable	N/A
App23	Snapchat	/data/data /com.snapchat.android	/databases/tcspahn.db/Chat	N/A	N/A	/databases/tcspahn.db/Conversation	N/A
App24	Tagged	/data/data /com.taggedapp	/databases/tagged_6029676964/conversations	/databases/tagged_6029676964/conversations	N/A	/databases/tagged_6029676964/messages	N/A
App25	Tapatalk	/data/data /com.quoord.tapatalkpro.activity	N/A	N/A	N/A	N/A	N/A
App26	Tumblr	/data/data /com.tumblr	N/A	N/A	N/A	N/A	N/A
App27	Twitter	/data/data /com.twitter.android	N/A	N/A	N/A	N/A	/sdcard/com.twitter.android/cache/photos
App28	Vk	/data/data /com.vkontakte.android	/databases/vk.db/messages	/databases/vk.db/dialogs	N/A	/databases/vk.db/messages	N/A
App29	We Heart It	/data/data /com.weheartit	N/A	N/A	N/A	N/A	N/A
App30	Wishbone	/data/data /com.science.wishboneapp	N/A	N/A	N/A	N/A	N/A

TABLE 20—*Location of the artifacts containing timestamps.*

App ID	App Name	Parent Directory	Location of Timestamps Related Artifacts (Database/Table/File)					
			Determine When Add Request was Sent to/from a Contact	Determine When Add Request was Accepted by a Contact	Determine When Text/ Multimedia Message was Sent	Determine When Text/Multimedia Message was Received/ Delivered	Determine When Notification was Received	Determine When Status was Posted
App1	Facebook	/data/data/com.facebook.katana	N/A	/databases/ contacts_db2/ contacts	/databases/threads_db2/ messages	N/A	/databases/notifications_ db/gql_notifications	N/A
App2	LinkedIn	/data/data/com.linkedin.android	/databases/ linkedin.db/ invitations	N/A	/databases /linkedin.db/ messages	/databases /linkedin.db/ messages	/databases /linkedin.db/ notification_center	N/A
App3	MeetMe	/data/data/com.myyearbook.m/	N/A	N/A	/databases /chats.db/ messages	/databases /chats.db/ messages	N/A	N/A
App4	Path	/data/data/com.path	/databases/ path_4.3.3_ 503_en_US/ MOMENT	N/A	/databases/ path_4.3.3_503_ en_US/COMMENT	/databases/ path_4.3.3_503_ en_US/COMMENT	N/A	/databases/ path_4.3.3_ 503_en_US/COMMENT
App5	Whisper	/data/data/sh.whisper/databases	N/A	N/A	/databases /databases/c.db/c	N/A	N/A	N/A
App6	9Chat	/data/data/com.ninechat.android. chat	N/A	N/A	/databases/core/CHAT_ MESSAGE	N/A	N/A	N/A
App7	Ask.fm	/data/data/com.askfm	N/A	N/A	N/A	N/A	N/A	N/A
App8	Badoo	/data/data/com.badoo.mobile	N/A	N/A	/databases/badoo.db/Message	N/A	N/A	N/A
App9	Fling	/data/data/com.unii.fling	N/A	N/A	N/A	N/A	N/A	N/A
App10	Indiegogo	/data/data/com.indiegogo.android	N/A	N/A	N/A	N/A	N/A	N/A
App11	Kiwi	/data/data /com.chatous.pointblank	N/A	N/A	N/A	N/A	N/A	N/A
App12	Meetup	/data/data /com.meetup	N/A	N/A	/databases/com.meetup.db/ conversations	/databases/com.meetup.db/ conversations	N/A	N/A
App13	MeowChat	/data/data /com.minus.android	N/A	N/A	/databases/com.minus.android/ MinusMessage	N/A	N/A	N/A
App14	Minds	/data/data /com.minds.mobile	N/A	N/A	N/A	N/A	N/A	N/A
App15	MocoSpace	/data/data /com.jnj.mocospace. android	N/A	N/A	N/A	N/A	N/A	N/A
App16	Oasis	/data/data /com.oasis.wrapper	N/A	N/A	N/A	N/A	/databases/Alert/ALERT	N/A
App17	OkCupid	/data/data /com.okcupid.okcupid	N/A	N/A	N/A	N/A	N/A	N/A
App18	ooVoo	/data/data /com.oovoo	N/A	N/A	/databases/Core.db/moment	/databases/Core.db/moment	N/A	N/A
App19	Pinterest	/data/data /com.pinterest	N/A	N/A	N/A	N/A	/databases/pinterest- db1433732876003/ NOTIFICATION	N/A

TABLE 20—*Continued.*

App ID	App Name	Parent Directory	Location of Timestamps Related Artifacts (Database/Table/File)					
			Determine When Add Request was Sent to/from a Contact	Determine When Add Request was Accepted by a Contact	Determine When Text/ Multimedia Message was Sent	Determine When Text/Multimedia Message was Received/ Delivered	Determine When Notification was Received	Determine When Status was Posted
App20	POF Dating	/data/data /com.pof.android	N/A	N/A	N/A	N/A	/databases/ NOTIFICATION_ CENTER/nc_ notification	N/A
App21	Singles AroundMe	/data/data /com.singlesaroundme. android	N/A	N/A	/databases/samdb/messages_ threaded	/databases/samdb/messages_ threaded	N/A	N/A
App22	Skout	/data/data /com.skout.android	N/A	N/A	/databases/skoutDatabase/ skputMessagesTable	N/A	N/A	N/A
App23	Snapchat	/data/data /com.snapchat.android	N/A	N/A	N/A	N/A	N/A	N/A
App24	Tagged	/data/data /com.taggedapp	N/A	N/A	/databases/tagged_6029676964/ conversations	N/A	N/A	N/A
App25	Tapatalk	/data/data /com.quoord. tapatalkpro.activity	N/A	N/A	N/A	N/A	N/A	N/A
App26	Tumblr	/data/data /com.tumblr	N/A	N/A	N/A	N/A	N/A	N/A
App27	Twitter	/data/data /com.twitter.android	N/A	N/A	N/A	N/A	N/A	N/A
App28	Vk	/data/data /com.vkontakte.android	N/A	N/A	/databases/vk.db/messages	/databases/vk.db/messages	N/A	N/A
App29	We Heart It	/data/data /com.weheartit	N/A	N/A	N/A	N/A	N/A	N/A
App30	Wishbone	/data/data /com.science. wishboneapp	N/A	N/A	N/A	N/A	N/A	N/A

TABLE 21—*Location of the artifacts containing user location and other information.*

			Location of User Location and Other Artifacts (Database/Table/File)				
App ID	App Name	Parent Directory	Identify Latitude and Longitude of User Location	Identify Name and Place of User Location	Extract Databases	Identify Facebook Tokens	View Status Posts
App1	Facebook	/data/data/com.facebook.katana	N/A	N/A	/com.facebook.katana/ databases	N/A	/files/Newsfeed
App2	LinkedIn	/data/data/com.linkedin.android	N/A	N/A	/com.linkedin.android/ databases	N/A	N/A
App3	MeetMe	/data/data/com.myyearbook.m/	N/A	/databases/com.localytics. android.3d6dfb80bc 77408754a1da607d1 7408b5b3a7289736558 adb87ceafeaf599cd6. sqlite/sessions	/com.myyearbook.m/ databases	/shared_prefs/ com.facebook. SharedPreferencesToken CachingStrategy.DEFAULT_ KEY.xml	N/A
App4	Path	/data/data/com.path	N/A	/databases/path_4.3.3_503_ en_US.db/CITY	/com.path/databases	/shared_prefs/ com.facebook. internal.preferences.APP_ SETTINGS.xml	/path_4.3.3_503_ en_US.db/ ACTIVITY
App5	Whisper	/data/data/sh.whisper/databases	/shared_prefs/ sh.whisper_ preferences.xml	/databases /databases/w.db/w	/sh.whisper/databases	N/A	N/A
App6	9Chat	/data/data/com.ninechat.android. chat	N/A	N/A	/com.ninechat.android. chat/databases	/shared_prefs/com.facebook. AccessTokenManager. SharedPreferences	N/A
App7	Ask.fm	/data/data/com.askfm	N/A	N/A	/com.askfm/databases	/shared_prefs/com.facebook. SharedPreferencesToken CachingStrategy.DEFAULT_ KEY	N/A
App8	Badoo	/data/data/com.badoo.mobile	N/A	N/A	/com.badoo.mobile/ databases	/shared_prefs/com.facebook. SharedPreferencesToken CachingStrategy.DEFAULT_ KEY	N/A
App9	Fling	/data/data/com.unii.fling	/shared_prefs/ fling_prefs.xml	/shared_prefs/ fling_prefs.xml	/com.unii.fling/ databases	N/A	N/A
App10	Indiegogo	/data/data/com.indiegogo.android	N/A	N/A	/com.indiegogo. android/databases	N/A	N/A
App11	Kiwi	/data/data /com.chatous.pointblank	N/A	N/A	/com.chatous. pointblank/databases	/shared_prefs/com.facebook. AccessTokenManager. SharedPreferences	N/A
App12	Meetup	/data/data /com.meetup	N/A	/databases/com.meetup.db/ members	/com.meetup/databases	/shared_prefs/com.facebook. SharedPreferencesToken CachingStrategy.DEFAULT_ KEY	N/A
App13	MeowChat	/data/data /com.minus.android	N/A	N/A	/com.minus.android/ databases	/shared_prefs/com.facebook. SharedPreferencesToken CachingStrategy.DEFAULT_ KEY	N/A
App14	Minds	/data/data /com.minds.mobile	N/A	N/A	N/A	N/A	N/A
App15	MocoSpace	/data/data /com.jnj.mocospace. android	N/A	/shared_prefs/SerializedUser	/com.jnj.mocospace. android/databases	/shared_prefs/com.facebook. AccessTokenManager. SharedPreferences	N/A

TABLE 21—*Continued.*

App ID	App Name	Parent Directory	Location of User Location and Other Artifacts (Database/Table/File)				
			Identify Latitude and Longitude of User Location	Identify Name and Place of User Location	Extract Databases	Identify Facebook Tokens	View Status Posts
App16	Oasis	/data/data /com.oasis.wrapper	N/A	N/A	/com.oasis.wrapper/ databases	/shared_prefs/com.facebook. SharedPreferencesToken CachingStrategy.DEFAULT_ KEY	N/A
App17	OkCupid	/data/data /com.okcupid.okcupid	N/A	N/A	/com.okcupid.okcupid/ databases	N/A	N/A
App18	ooVoo	/data/data /com.oovoo	N/A	N/A	/com.oovoo/databases	/shared_prefs/com.facebook. SharedPreferencesToken CachingStrategy.DEFAULT_ KEY	N/A
App19	Pinterest	/data/data /com.pinterest	N/A	N/A	/com.pinterest/ databases	N/A	N/A
App20	POF Dating	/data/data /com.pof.android	N/A	N/A	/com.pof.android/ databases	/shared_prefs/ com.facebook. internal.preferences.APP_ SETTINGS.xml	N/A
App21	Singles AroundMe	/data/data /com.singlesaroundme. android	/databases/samdb/ geolocpoint	/databases/samdb/ geolocpoint	/com.singlesaroundme. android/databases	/shared_prefs/com.facebook. SharedPreferencesToken CachingStrategy.DEFAULT_ KEY	N/A
App22	Skout	/data/data /com.skout.android	/shared_prefs/ LOCATION_ PREFS	N/A	/com,skout.android/ databases	/shared_prefs/com.facebook. SharedPreferencesToken CachingStrategy.DEFAULT_ KEY	N/A
App23	Snapchat	/data/data /com.snapchat.android	N/A	N/A	/com.snapchat.android/ databases	N/A	N/A
App24	Tagged	/data/data /com.taggedapp	N/A	N/A	/com.taggedapp/ databases	/shared_prefs/com.facebook. SharedPreferencesToken CachingStrategy.DEFAULT_ KEY	N/A
App25	Tapatalk	/data/data /com.quoord. tapatalkpro.activity	N/A	N/A	/com.quoord.tapatalkpro. activity/databases	/shared_prefs/com.facebook. SharedPreferencesToken CachingStrategy.DEFAULT_ KEY	N/A
App26	Tumblr	/data/data /com.tumblr	N/A	N/A	/com.tumblr/databases	N/A	N/A
App27	Twitter	/data/data /com.twitter.android	N/A	/databases/ 966083424-23.db/ users	/com.twitter.android/ databases	N/A	/databases/ 966083424-23.db/ statuses
App28	Vk	/data/data /com.vkontakte.android	N/A	N/A	/com.vkontakte.android/ databases	/shared_prefs/com.facebook. SharedPreferencesToken CachingStrategy.DEFAULT_ KEY	N/A
App29	We Heart It	/data/data /com.weheartit	N/A	N/A	/com.weheartit/databases	/shared_prefs/com.facebook. SharedPreferencesToken CachingStrategy.DEFAULT_ KEY	N/A
App30	Wishbone	/data/data /com.science. wishboneapp	N/A	N/A	/com.science.wishboneapp/ databases	N/A	N/A

TABLE 22—*An application of the proposed forensic taxonomy of social apps.*

App Category/Artifact Category		Friends and Family Apps	Dating Apps	Professional Networking Apps
User and contact information	Find phone number from a contact ID	App1		
	Find date of birth of the user	App9, App24	App21	
	Recover email id of the user	App4, App9, App18, App21, App26		
	Recover user name	App1, App4, App5, App6, App7, App13, App18, App19, App24, App26, App27, App28	App3, App8, App15, App16, App20, App21, App22	App2
	Find user profile image	App4, App6, App7, App11, App12, App13, App14, App19, App23, App24, App27, App28, App30	App3, App8, App16, App17, App20, App21	App2
	Recover user passcode	App5		
	View friend list of the user	App1, App4, App18, App23, App24, App28	App22	App2
	View imported address book	App23, App28		
Exchanged messages	View chat history	App1, App4, App5, App6, App9, App12, App13, App18, App19, App23, App24, App28	App3, App8, App21, App22	App2
	Determine types of exchanged messages (text, audio, video)	App1, App6, App9, App12, App13, App18, App24, App28	App3, App8, App21, App22	App2
	View received notifications	App19	App16, App20	App2
	View unencrypted exchanged text messages	App1, App4, App5, App6, App9, App12, App13, App18, App23, App24, App28	App3, App8, App21, App22	App2
	View unencrypted exchanged images	App9, App19, App27	App20	
Timestamps	Determine when add request was sent to/from a contact	App4		App2
	Determine when add request was accepted by a contact	App1		
	Determine when text/multimedia message was sent	App1, App4, App5, App6, App12, App13, App18, App24, App28	App3, App8, App21, App22	App2
	Determine when text/multimedia message was received/delivered	App4, App12, App18, App28	App3, App21	App2
	Determine when notification was received	App1, App19	App16, App20	App2
	Determine when status was posted	App4		
User location and other artifacts	Identify latitude and longitude of user location	App5, App9	App21, App22	
	Identify name and place of user location	App4, App5, App9, App12, App24, App27	App3, App15, App21	
	Extract databases	App1, App4, App5, App6, App9, App10, App11, App12, App13, App18, App19, App23, App24, App25, App26, App27, App28, App29, App30	App3, App8, App15, App16, App20, App21, App22	App2
	Identify Facebook tokens	App4, App6, App7, App11, App12, App13, App18, App24, App25, App28, App29	App3, App8, App15, App16, App20, App21, App22	
	View status posts	App1, App4, App27		

the mHealth app artifacts were divided into seven categories. Each of the four categories of artifacts found from communication and social apps was further divided into a number of subcategories.

Table 23 shows the comparison of the forensic artifacts recovered from the social apps, communication apps, and mHealth apps. Many of the user and contact information, such as user name, could be forensically recovered from all apps. However, the hidden/blocked/deleted contacts could only be recovered from some of the communication apps.

Android mHealth apps did not provide any text messaging functionality; thus, no artifact related to exchanged messages could be recovered from the apps. Exchanged text messages and images between two users were recovered from most social apps and communication apps. The time when an add request was sent and accepted, and when a text or multimedia message was sent and delivered could also be recovered from both social apps and communication apps. However, only the timestamp of a user activity could be recovered from the mHealth apps. The location information about the users was recovered from some of the social apps and mHealth apps.

Chat history, timestamp of a received notification, status posts and the timestamp, and Facebook tokens were the artifacts that could only be recovered only from the social apps.

Concluding Remarks

In this study, a forensic analysis of 30 popular Android social apps has been conducted, and based on the findings, a forensic artifact taxonomy has been constructed. The proposed taxonomy provides a means of capturing relevant forensic artifacts in a

TABLE 23—*Comparison of forensic artifacts recovered from different categories of Android apps.*

Artifact Categories		Social Apps	Communication Apps (13)	mHealth Apps (12)
User and Contact Information	Find phone number from a contact ID	✓	✓	
	Find date of birth of the user	✓		✓*
	Recover email id of the user	✓		✓*
	Recover user name	✓	✓†	✓*
	Find user profile image	✓		✓
	Recover user passcode	✓	✓	✓
	View friend list of the user	✓		✓
	View imported address book	✓	✓	
	View contact status message		✓	
	View blocked/hidden contacts		✓	
	View deleted contacts		✓	
	User activities			✓
Exchanged Messages	View chat history	✓		
	Determine types of exchanged messages (text, audio, video)	✓	✓	
	View received notifications	✓		
	View unencrypted exchanged text messages	✓	✓	
	View unencrypted exchanged images	✓	✓	
	View unencrypted contents of a group chat		✓	
	View hidden chats		✓	
Timestamps	Determine when add request was sent to/from a contact	✓	✓	
	Determine when add request was accepted by a contact	✓	✓	
	Determine when text/multimedia message was sent	✓	✓	
	Determine when text/multimedia message was received/delivered	✓	✓	
	Determine when notification was received	✓		
	Determine when status was posted	✓		
	Identify time when voice call was made		✓	
	Activity timestamp			✓
User Location and Other artifacts	Identify latitude and longitude of user location	✓		✓
	Identify name and place of user location	✓		
	Extract databases	✓	✓	✓
	Identify Facebook tokens	✓		
	View status posts	✓		
	Identify the members of a group chat		✓	
	Identify the duration of voice calls		✓	

*Artifact category named as "Personal details of users".
†Artifact category named as "View contact ID".

social app investigation. More specifically, the taxonomy has documented our recovered forensic artifacts and their potential locations; thus, benefiting the digital forensic community by providing them an up-to-date understanding of the types of data that can be recovered. A typical example might include a list of contacts, when a contact was added, locating of Facebook tokens, and reconstructing of the chronology of exchanged text and multimedia messages.

There are several practical implications of this research. First, this research highlights the need for an open source or standard way of preserving data that would facilitate a timely and effective forensic investigation. It emphasizes the need for forensic readiness to be incorporated in the design of mobile apps, so that forensic investigators will know where and what to collect. Second, a publicly available and up-to-date taxonomy would inform app users of the privacy implications of using a specific app. It outlines what data could potentially be recovered by someone using a commercial or open source forensic tool, should their devices be lost or stolen. If a user is not willing to disclose his/her location, the user should consider installing apps that do not disclose the user location. Third, app developers should consider the types of sensitive data they are collecting and storing on mobile devices that may be subject to unauthorized access and how these data can be better protected. For example, the developers could create a layer of abstraction while storing the data on the devices. This can be done by minimizing the data stored in the database and encrypting the files that store sensitive information. Findings from our study can help developers to have an in-depth understanding of the types of data that do not need to be stored or need to be secured on the database.

With new releases of the social apps, artifacts that can be forensically recovered may vary. Therefore, future work would include examining other and new releases of the social apps and potentially include additional artifact categories to the proposed taxonomy.

References

1. Choi C-R, Jeong H-Y, Park J, Jeong Y-S. Relative weight evaluation of the factors inducing social media service use. Multimed Tools Appl 2015;74(14):5041–54.
2. Perez S. App usage grew 76% in 2014, with shopping apps leading the way, 2015; http://techcrunch.com/2015/01/06/app-usage-grew-76-in-2014-with-shopping-apps-leading-the-way/ (accessed June 19, 2015).
3. Nielsen. Social media report 2012: social media comes of age, 2015; http://www.nielsen.com/us/en/insights/news/2012/social-media-report-2012-social-media-comes-of-age.html (accessed June 19, 2015).

4. Furini M, Tamanini V. Location privacy and public metadata in social media platforms: attitudes, behaviors and opinions. Multimed Tools Appl 2015;74(21):9795–825.
5. Casey E, Ferraro M, Nguyen L. Investigation delayed is justice denied: proposals for expediting forensic examinations of digital evidence. J Forensic Sci 2009;54(6):1353–64.
6. Song C-W, Chung K-Y, Lee J-H. Catching up faster data in digital crime using mobile devices. Multimed Tools Appl 2015;74(20):9007–16.
7. Karie NM, Venter HS. Toward a general ontology for digital forensic disciplines. J Forensic Sci 2014;59(5):1231–41.
8. Keith MJ, Babb J, Lowry PB. A longitudinal study of information privacy on mobile devices. Proceedings of the 47th Hawaii International Conference on Systems Sciences (HICSS 2014); 2014 Jan 6-9; Waikoloa, HI. Piscataway, NJ: Institute of Electrical and Electronics Engineers, 2014;3149–58.
9. Barmpatsalou K, Damopoulos D, Kambourakis G, Katos V. A critical review of 7 years of mobile device forensics. Digit Invest 2013;10(4):323–49.
10. La Polla M, Martinelli F, Sgandurra D. A survey on security for mobile devices. IEEE Commun Surv Tutorials 2013;15(1):446–71.
11. IDC. Smartphone OS market share, Q1 2015, 2015; http://www.idc.com/prodserv/smartphone-os-market-share.jsp (accessed July 7, 2015).
12. Azfar A, Choo K-KR, Liu L. Forensic taxonomy of popular Android mHealth apps. Proceedings of the 21st Americas Conference on Information Systems (AMCIS 2015), 2015 Aug 13-15; Fajardo, Puerto Rico. Atlanta, GA: Association for Information Systems; 2015.
13. Azfar A, Choo K-KR, Liu L. An Android communication app forensic taxonomy. J Forensic Sci 2016;61(5):1337–50.
14. Immanuel F, Martini B, Choo KKR. Android cache taxonomy and forensic process. Proceedings of 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2015); 2015 Aug 20–22; Helsinki, Finland. Los Alamitos, CA: IEEE Computer Society Press, 2015;1094–101.
15. Plachkinova M, Andrés S, Chatterjee S. A Taxonomy of mHealth apps–security and privacy concerns. Proceedings of the 48th Hawaii International Conference on System Sciences (HICSS 2015); 2015 Jan 5–8; Kauai, HI. Piscataway, NJ: Institute of Electrical and Electronics Engineers, 2015;3187–96.
16. Alliano A, Herriger K, Koutsoftas AD, Bartolotta TE. A review of 21 iPad applications for augmentative and alternative communication purposes. Perspect Augment Alter Commun 2012;21(2):60–71.
17. Al Mutawa N, Baggili I, Marrington A. Forensic analysis of social networking applications on mobile devices. Digit Invest 2012;9(Suppl):S24–S33.
18. Jang Y-J, Kwak J. Digital forensics investigation methodology applicable for social network services. Multimed Tools Appl 2015;74(14):5029–40.
19. Chu H-C, Yang S-W, Hsu C-H, Park J. Digital evidence discovery of networked multimedia smart devices based on social networking activities. Multimed Tools Appl 2014;71(1):219–34.
20. Farnden J, Martini B, Choo K-KR. Privacy risks in mobile dating apps. Proceedings of the 21st Americas Conference on Information Systems (AMCIS 2015), 2015 Aug 13–15; Fajardo, Puerto Rico. Atlanta, GA: Association for Information Systems, 2015.
21. Martini B, Choo K-KR. Cloud storage forensics: ownCloud as a case study. Digit Invest 2013;10(4):287–99.
22. Martini B, Do Q, Choo K-KR. Mobile cloud forensics: an analysis of seven popular Android apps. In: Ko R, Choo K-KR, editors. Cloud security ecosystem. Waltham, MA: Syngress an Imprint of Elsevier; 2015;309–45.
23. Quick D, Choo K-KR. Dropbox analysis: data remnants on user machines. Digit Invest 2013;10(1):3–18.
24. Quick D, Choo K-KR. Google drive: forensic analysis of data remnants. J Netw Comput Appl 2014;40:179–93.
25. Quick D, Martini B, Choo K-KR. Cloud storage forensics. In: Shavers B, editor. Waltham, MA: Syngress an Imprint of Elsevier, 2013;8.
26. Shariati M, Dehghantanha A, Martini B, K-KR C. Ubuntu One investigation: detecting evidences on client machines. In: Ko R, Choo K-KR, editors. Cloud security ecosystem. Waltham, MA: Syngress an Imprint of Elsevier, 2015;429–46.
27. Shariati M, Dehghantanha A, Choo K-KR. SugarSync forensic analysis. Aust J Forensic Sci 2016;48(1):95–117.
28. Levinson A, Stackpole B, Johnson D. Third party application forensics on Apple mobile devices. Proceedings of the 44th Hawaii International Conference on System Sciences (HICSS 2014); 2011 Jan 4–7; Kauai, HI. Piscataway, NJ: Institute of Electrical and Electronics Engineers, 2011;1–9.
29. Anglano C. Forensic analysis of WhatsApp messenger on Android smartphones. Digit Invest 2014;11(3):201–13.
30. Thakur NS. Forensic analysis of WhatsApp on Android smartphones [Master's thesis]. New Orleans, LA: University of New Orleans, 2013.
31. Dezfouli FN, Dehghantanha A, Eterovic-Soric B, Choo K-KR. Investigating social networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms. Aust J Forensic Sci 2016;48(4):469–88.
32. Dredge S. Tinder dating app was sharing more of users' location data than they realised, 2014; http://www.theguardian.com/technology/2014/feb/20/tinder-app-dating-data-location-sharing (accessed July 7, 2015).
33. Seward ZM. Tinder's privacy breach lasted much longer than the company claimed, 2013; http://qz.com/107739/tinders-privacy-breach-lasted-much-longer-than-the-company-claimed/ (accessed July 7, 2015).
34. Olson P. Facebook was the one network people used less In 2014. Forbes, 2015; http://www.forbes.com/sites/parmyolson/2015/01/27/facebook-active-users-decline/ (accessed June 30, 2015).
35. Sharf S. LinkedIn stock pops on 44% sales growth, 2015; http://www.forbes.com/sites/samanthasharf/2015/02/05/linkedin-stock-pops-on-44-sales-growth/ (accessed June 30, 2015).
36. Davis CF. MeetMe: translating user growth to profits, 2015; http://seekingalpha.com/article/3160566-meetme-translating-user-growth-to-profits (accessed June 30, 2015).
37. Hamburger E. Path is back with a new messaging app that can talk to people and places, 2015; http://www.theverge.com/2014/6/20/5827452/path-is-back-path-talk-messaging-app-acquires-talkto-unlimited-friends-list-dave-morin (accessed June 30, 2015).
38. Fiegerman S. Report: secret-sharing app Whisper now valued at $200 million, 2014; http://mashable.com/2014/03/11/whisper-funding/ (accessed June 30, 2015).
39. Google. Google Play, 2015; https://play.google.com/store/apps (accessed February 2, 2015).
40. Retrieving data from Android OS devices using XRY. Patrick Leahy Center for Digital Investigation (LCDI); www.champlain.edu/Documents/LCDI/Android_OS_Tutorial_Final_PDF.pdf (accessed September 4, 2015).

Additional information and reprint requests:
Kim-Kwang Raymond Choo, Ph.D.
Department of Information Systems and Cyber Security
University of Texas at San Antonio
One UTSA Circle
San Antonio, TX 78249-0631
E-mail: Raymond.choo@fulbrightmail.org