# Forensic Analysis of three Social Media Apps in Windows 10

Asma Majeed, Haleemah Zia, Rabeea Imran and Shahzad Saleem
School of Electrical Engineering and Computer Science, NUST
Islamabad, Pakistan
Email: {asma.majeed,14msishzia,14msisrimran,shahzad.saleem}@seecs.edu.pk

***Abstract*—Social media facilitates communication and provides easy way of reaching out to people. However, it also poses a risk of disclosure of personal details which, if exploited, can lead to privacy issues and also crimes such as blackmailing, identity theft etc. In this regard, it is essential to study social media from a forensics point of view. In this paper we have explored the remnants of Facebook, Viber and Skype. All work is carried out for Windows 10 technical preview. The potential locations are explored and examined to find artifact locations and their details. An effort has also been made to recover the items from unallocated space, which also includes those that were permanently deleted from Windows.**

***Index Terms*—Digital forensics, Windows forensics, Social media forensics, Skype artifacts, Viber artifacts, Facebook artifacts, Deleted artifacts, FTK Imager**

## I. Introduction

In the recent years, social media apps have gained popularity in general public due to their ease of use. Faster access and informal way of signing up for the app are positive aspects which make them a preferred choice over traditional browser access . Few of the popular social media apps are Facebook, Twitter, Viber, WhatsApp etc. By using these apps, users voluntarily disclose large amounts of information ranging from their likes, dislikes to personal activities. In many cases, the privacy settings of these apps may allow this information to be easily retrieved by any individual, regardless of his relationship to the user. This has two major implications for a forensics investigator. Firstly, it may help him gather information about a suspect by acquiring public information on his social media profiles. Secondly, social media apps can be leveraged by malicious users to create fake and untraceable accounts through which they may perform illicit activities such as stalking, blackmailing, spamming or identity theft etc. This necessitates the investigators need for acquiring knowledge and skills required for collecting artifacts discharged by these apps.

There are a number of criminal cases where the case history is deeply rooted in the usage of social media. In an incident [8], a trainee nurse was killed by a person with whom she connected via social media. Investigation revealed that she was lured by the social media user to meet him at a certain place. Many other cases of murder, identity impersonation and blackmailing have also surfaced in the news recently [9].

Facebook is the most popular social networking application. Statistics of the first quarter of 2015 show that it has 1.44 billion active users followed by Twitter with 236 million users [6]. Viber is another application that supports calls and instant messaging services. According to the report [7], 573 million users have joined Viber since June 2011 to April 2015. Viber on any device needs to be registered with a SIM Card number and the app is synchronized with the user's contact book . Skype has gained popularity as a voice communication service. Statistics [19] of March 2015 show that it has 500 million active users.

Interestingly, many of the activities are logged on the hard disk of the device from which access is made. The artifacts may reveal details about private connections and the on-going user activities. Features of these apps may include Geo-location that can be used to identify the places from where the criminal accessed the service.

Investigating Windows behavior has become imperative for forensic investigators due to increased usage of Windows OS on desktop, laptop and even on cellphones. Focus of our research is to explore potential location of the remnants for Facebook, Viber and Skype running over Windows 10 only because (to the best of our knowledge) no published work exists for it.

The rest of the paper is organized as follows: we have mentioned related work in section II, followed by the test environment setup in section III, the methodology and experiment results overview is in section IV. Finally in section V, we conclude our findings and discuss the direction for the future work.

## II. Related Work

Social Networking apps, because of their increased popularity, have received attention from forensics researchers for quite some time now. In 2011, N.Muttawa et al tested artifact recovery of Facebook messaging service [11]. They performed their test on Facebook running in three different browsers on Windows XP. They found that chat sessions carried out on Internet Explorer left more traces compared to Mozilla Firefox and Google Chrome. They also found that chat conducted in Arabic language was saved after being converted to Unicode characters, hence complicating the key search process for any forensic examiner. In their research in 2012, N.Muttawa et al analyzed forensic artifacts of several Social Media apps on various mobile platforms [12]. Their main focus had been mobile device forensics. In this regards they identified and

978-1-4673-9268-6/15/$31.00 ©2015 IEEE

TABLE I: Tools and Software used for experiment

| Device | Purpose | Model/Version |
|---|---|---|
| Laptop | OS and other software installation for experimental procedure | DELL n7010 |
| OS | Platform for performing experiments | Window 10 Technical Preview |
| FTK imager | Taking image of the drive and exploring MFT records | 3.2.0 |
| Dcode | Verification of the MFT timestamps | 4.02a |
| Process Monitor | Tracing the artifact locations for all three apps | Sysintarnals Suite |
| Sqlite DB Browser | Exploring the details of the databases found | 3.7.0 |
| EaseUs | Recovering the data from unallocated space | Trial version |

analyzed artifacts of MySpace, Twitter and Facebook each on Blackberry phone, iPhone (iOS) and Android.

A research based on the analysis of Facebook artifacts in internet activity was carried out by M.Baca et al in 2013 [13]. They conducted their experiments on Windows XP in virtual machine and were able to find significant evidence traces related to Facebook activity. Release of Window 8 in 2012 brought a rapid transition from the traditional Windows OS. Josh Brunty [17] and Nikhalesh Singh Bhadoria [18] provide useful details on the artifacts exclusive to Windows 8.

In 2013, Mahajan et al studied Whats-app and Viber artifacts on Android phone [14]. They were able to recover WhatsApp contacts list and plain text chat messages along with their timestamps. For Viber, they identified two database files (in contrast to one for WhatsApp) from where useful information could be extracted .

A Masters' thesis was carried out in 2013 regarding WhatsApp forensics on android [15]. Research findings showed that android devices reveal all WhatsApp information in plain text format when analyzed as a rooted image. When analyzed otherwise, they reveal only partial information and in encrypted state. A more recent research [22] correlates WhatsApp artifact from different locations to help the investigator better construct the crime scene.

Saleh et al's research in 2013 focused on Skype artifacts analysis [16]. They found out that records of Skype call and chat sessions are saved in RAM and NAND flash memories. They also claimed that the data persists in memory for quite a long duration of time even after deletion from parent directories. Walnycky et al. [20] have carried out network and device forensic analysis of twenty android social messaging apps to explore digital evidence. Their results can be of great value to forensic examiners but their work is strictly limited to the messaging service only . Narayan et al [10] also found very interesting and important artifacts by analyzing smartphones .

## III. Setting up the Test Environment

Before beginning experimentation, there was a need to setup a Windows 10 system with the required forensic tools installed over it. Also, social media apps needed to be installed and some activity be performed using each of these. Details of this preliminary setup are given below .

In order to perform our experiments, we installed Window 10 technical preview as the host system on DELL n7010 Laptop. Hardware specifications of this system were; Intel i5 processor, 2.4 GHz and 4 GB RAM. A space of 25 GB was allocated to the Windows OS. This much space was large enough for our research process and small enough to speed up the imaging process. Further details of the tools and the software used during the test are listed in Table I.

Following windows installation, Facebook, Skype and Viber were installed on the system via Window's App store. This was followed by some activities on all three apps in order to generate some significant evidentiary artifacts. The activities performed on each app are listed in Table II. The listings are in chronological order. For experiment purpose dummy accounts were created and an interaction was made with authors personal accounts .

TABLE II: Activities performed on three apps

| App name | Activity Performed |
|---|---|
| Facebook | Y sent a friend request to X<br>Y posted in X's timeline<br>Z made a comment on this post<br>X opened the notification<br>X liked the comment<br>X made a comment to the same post |
| Viber | A sent text message to B<br>A sent stickers in message to B<br>A sent photo in message to B<br>B sent text message to A<br>B sent stickers in message to A<br>B sent photo in message to A<br>A called B, B accepted and the call lasted for 20 seconds<br>B called A. A rejected twice and accepted on the third time. |
| Skype | created account for A<br>A attempted to search for B's account<br>A added B in their contact's list<br>A called B<br>B accepted; A and B conversed for few min |

| | id | thread_id | body | sender | timestamp |
|---|---|---|---|---|---|
| | Filter | Filter | Filter | Filter | Filter |
| 1 | m_mid.1434780... | t_mid.14347806... | hello | {"user_id":"1000... | 1434780608827 |
| 2 | m_mid.1434780... | t_mid.14347806... | Hi | {"user_id":"1000... | 1434780651491 |
| 3 | m_mid.1434780... | t_mid.14347806... | check logss in db | {"user_id":"1000... | 1434780662715 |
| 4 | m_mid.1434780... | t_mid.14347806... | ok sure | {"user_id":"1000... | 1434780668574 |

Fig. 1: Screenshot of messages.db for Facebook

## IV. Methodology

NIST defines any digital forensics case to consist of four main stages [1, 21], namely identification, collection, organization and presentation. The identification phase refers to the identification of incident or the evidence. In the collection

phase, evidentiary data is acquired and then carved which is followed by reducing the amount of data by discarding off any redundancies. In the organization phase, carved data is examined and correlated with the crime scene in order to reach solid conclusions. Finally, the presentation phase deals with bringing the data in a format that can be understood by the jury.

Presentation phase was out of the scope of this research as the focus here was to locate and explore remnants left by social media apps, rather than building a case that could be presented in-front of jury. Rest of the three phases are entailed below.

### A. Identification

In digital forensic investigation, identification of evidence could mean a walkthrough of the crime scene and identifying any hardware or software worthy of collection. In this research however, it was pre-established that Facebook, Skype and Viber app artifacts were to be studied. Hence, an image of the hard disk (specifically the drive bearing windows 10 installation) was identified for collection.

### B. Collection

We refer to our process of acquiring the disk image as the collection phase. We used FTK Imager for acquisition purpose (as well as for examination as discussed later on in this paper).. The choice was made owing to the fact that FTK Imager is considered the fastest and most reliable imaging tool [4]. The disk size, as mentioned in section 3 was intentionally kept to 25 GB. A raw (dd) bit by bit (physical) image was acquired and saved onto another partition drive on the same system.

The identification of artifacts and their examination was easily carried out over the live system. However we chose to execute the entire examination process on storage medias image so as to reflect a real world scenario whereby integrity preservation is of considerable significance. To further preserve the integrity, we used digital hashes of the collected evidence.

Initially process monitoring was done in order to get to the artifact locations . Collection of only specific folders identified by Process Monitor could be made, however we chose to image the entire disk space instead as our intention was to study the unallocated space for deleted artifacts as well.

### C. Examination(Organization)

The image was explored for Facebook, Skype and Viber artifacts in this phase. The artifacts were examined and correlated in order to analyse their usefulness in any real world case. Findings for each app are discussed below.

*1) Facebook Artifacts:* Most of the Facebook artifacts were found from the same location as in window 8.1 [2]. Number of SQLite database files including Friends, Stories, Friend Requests, Messages, Stickers were found at the location \AppData\Local\Packages\Facebook.Facebook_8xx8rvfyw5nnt\LocalState*FacebookID\DB. Most of these files were easily readable through the DB Browser for SQLite.

| | Number | ClientName | MessagesCount | CallsTotalDuration |
|---|---|---|---|---|
| | Filter | Filter | Filter | Filter |
| 1 | 923455... | Haleema MSIS | 8 | 89 |
| 2 | 923157... | Safoora | 0 | 0 |
| 3 | 923365... | Adnan | 0 | 0 |
| 4 | 925144... | IUIC | 0 | 0 |

Fig. 2: Screenshot of originnumberinfo table in viber.db

| from_dispname | body_xml | timestamp |
|---|---|---|
| anonymous xyz | Hello Haleemah Zia, I'd like to add you as a contact. | 1434788107 |
| Haleemah Zia | NULL | 1434788133 |
| anonymous xyz | <partlist alt=""> <part identity="haleemah42"> | 1434788228 |
| anonymous xyz | <partlist alt=""> <part identity="live:anonymous_investigator"> | 1434788244 |

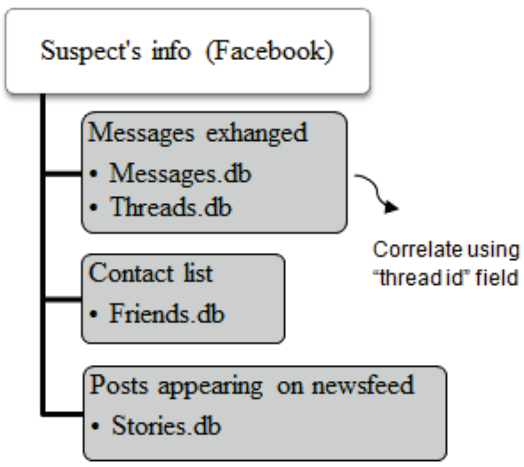
Fig. 3: Screenshot for messages table of main.db for Skype

Most interestingly message body was displayed in plain text (Fig. 1) and fields for timestamps and any attachments were also present among others. Although only sender was displayed in the messaging database, but as discussed in [3], recipient's identification could easily be done by using threads.db in corroboration. Another interesting fact is that the location coordinates of the sender were also visible in messages.db. Stories.db showed the Facebook newsfeed visible on user's time line and also the permissions to the people in the list e.g. whether they were allowed to send friend requests or not.

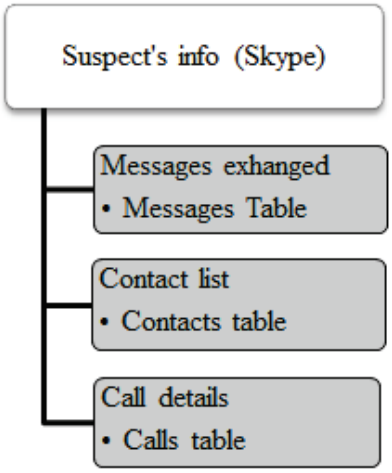
To analyze the above mentioned files in MFT, we used the freeware FTK Imager. MFT Record of friends.sqlite was identified using MFT Record number and then calculating its offset accordingly. Time stamps in Standard Information Attribute and File Name Attributes were decoded using the DCode application. Both time stamps correlated and matched with the system timings set when the activities were carried out.

*2) Viber Artifacts:* Viber artifacts were found at the location *\AppData\Local\Packages\2414FC7A.Viber-FreePhoneCallsText_p61zvh252yqyr\LocalState\viber. They were present as separate files within the folder and also in a database by the name of viber.db.

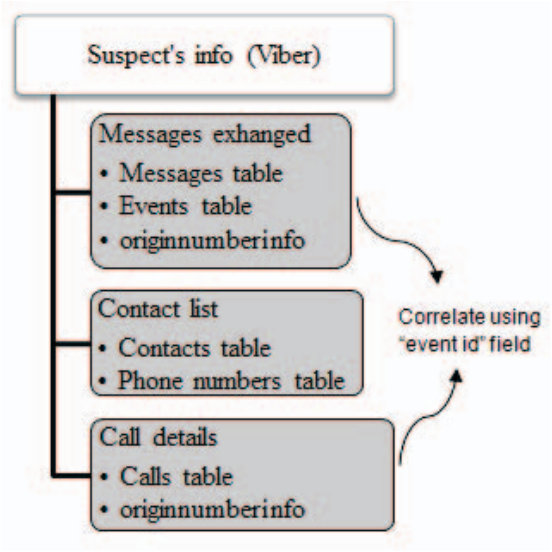
When we explored the folders within the parent directory containing Viber artifacts, messages were found in "/shared/transferred" folder but were stored encrypted and hence not human-readable. For us, they were easily identifiable to be text messages as they correlated with the timings at which we carried out our text-messaging activity. Moreover, stickers and photos exchanged during the conversation were present unencrypted in separate folders within the same directory. An interesting fact was that the profile pictures of all contacts of A were automatically saved in a separate folder




(a) Facebook




(b) Skype




(c) Viber

Fig. 4: Summary of artifact locations of the three apps

even though we did not use As account to view any of these pictures. Upon exploring viber.db, we found the same data along with its meta data. The database contained several tables among which the "messages table displayed clear text message, event id, any pictures shared along with the path for thumbnails stored for these pictures. Unlike Facebook's "messages table", it did not contain timestamps. However the event ids, when correlated with the event ids in the "events" table revealed timestamps as well as sender's number (with which Viber had been registered) for incoming messages. Recipient's number for outgoing messages was not displayed; however this information could also be deduced by correlating the "originnumberinfo" table (Fig. 2) which showed total calls duration and total number of messages exchanged with each contact.

Contact names and IDs were present in the "contacts" table and information about whether they use viber, whether they had recently joined viber etc was present in the "phonenumbers" tables.

The "calls" table showed call durations and event ids which could be correlated again with the "events" table and "originnumberinfo" to reveal extra information regarding sender and receiver .

*3) Skype Artifacts:* The location *\AppData\Local\Packages\Microsoft.SkypeApp_kzf8qxf38zg5c\LocalState contained a database with the name main.db that revealed evidence for these activities. The account creation, call duration, name and Skype ID of participants amongst whom the conversation took place and specific timestamps were all recovered.

The database contained multiple tables such as Videos, Calls, Messages, Accounts, Participants etc. The "calls" table revealed information about the calls made. It showed the time stamps, Skype id of both participants, whether video was enabled or not, sound level, whether it was an incoming call or not etc. The "contacts table showed information about friend searches. When searched for the name "Haleema" many Skype users with this user name were listed in the table. The

"messages" table (Fig. 3) showed timestamps and participants' IDs. The default Skype message that gets sent to the recipient was also visible in this table. Unlike viber.db, the event ID in Skype's database was unique and hence could not be correlated with the tables to extract any subtle information.

A visual representation of information retrievable from Facebook, Skype and Viber is shown in Fig 4a, 4b and 4c respectively. The figures display the suspect's information that an investigator would try to recover while building a crime story. For Facebook, information is contained within different databases while for Viber and Skype, it is found in different tables of the same database. Facebook is distinguished for its newsfeed stories while Viber and Skype for their call features.

*4) Analysis of Unallocated Space for Deleted Artifacts:* In order to check the deleted artifacts related to these social media apps, we purposefully deleted some images (Viber profile pictures) and SQLite files (Facebook artifacts). We then used trial version of EaseUs Software [5] for analysis of unallocated space. This choice of EaseUs was made for its user friendly GUI and the ability to recover many file types while presenting them in a segregated view according to file types. Searching for our specific files was made relatively easier by the file type specification and file sizes (we had recorded the file sizes of the files that we deleted). Nevertheless, it still required deep searching within the folder as unallocated space contained huge amounts of redundant data. However, once the deleted artifacts were successfully identified within the unallocated space, we were able to preview the deleted images. No further images could be gathered from the trial version. Recovering the file to its original location required the use of commercial version of EaseUs.

This work is limited in its scope, in a real investigation scenario, the investigator will not be having knowledge about file sizes beforehand. Therefore, some other pointers or tags that can help him identify relevant deleted artifacts need be studied too.

## V. Conclusion and Future Work

So far we have analyzed Windows 10 technical preview for location of storage of Facebook, Skype and Viber artifacts. The parent directory for most of the artifacts was the same. Within that parent directory, separate folders for all three applications were present. We were able to find very interesting artifacts for all three applications in plain text. These can prove to be sources of significant leads in various cases involving usage of social media in any form.

In future, we intend to investigate others apps as well, such as Twitter, Reddit and LinkedIn. Our further research will be carried out on the full version of window 10 and a comparison will be made between artifact locations in window 8.1 and window 10. Since the trial version of EaseUS did not fulfill our requirements completely so we will explore ProDiscover and some other tools for the same purpose. Furthermore, we plan to explore live system processes and threads of the social media apps in window 10 for further in-depth forensic analysis of the apps behavior. Finally, the limitation mentioned regarding deleted artifacts discovery in unallocated space would be catered for.

## References


[1] Radack, S. "Forensic techniques: helping organizations improve their responses to information security incidents" 2009. Retrieved September 18, 2015, from http://www.itl.nist.gov/lab/bulletns/bltnsep06.htm

[2] Parsons, A. "Windows 10 Forensics: Conclusion" - Computer & Digital Forensics Blog, 2015, April 30. Retrieved June 22, 2015, from http://computerforensicsblog.champlain.edu/2015/04/30/windows-10-forensics-conclusion/

[3] Parsons, A. "Windows 10 Forensics Part 2: Facebook Forensics", - Computer & Digital Forensics Blog, 2015, April 1. Retrieved June 21, 2015, from http://computerforensicsblog.champlain.edu/2015/04/01/windows-10-facebook-forensics/

[4] Shavers, B." Virtual Forensics (A Discussion of Virtual Machine Related to Forensic Analysis)", 2008. Retrieved August, 15, 2010.

[5] EaseUS. Retrieved June 21, 2015, from http://www.easeus.com/

[6] Facebook: Monthly active users 2015 — Statistic. (n.d.). Retrieved June 21, 2015, from http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[7] Viber: Number of registered users 2015 — Statistic. (n.d.). Retrieved June 21, 2015, from http://www.statista.com/statistics/316414/viber-messenger-registered-users/

[8] Doyle, J." A Facebook crime every 40 minutes: From killings to grooming as 12,300 cases are linked to the site", 2012, June 5. Retrieved June 21, 2015, from http://www.dailymail.co.uk/news/article-2154624/A-Facebook-crime-40-minutes-12-300-cases-linked-site.html

[9] Poh, M. (n.d.). "10 Most Bizarre Crimes Linked to Facebook". Retrieved June 21, 2015, from http://www.hongkiat.com/blog/bizarre-facebook-crimes/

[10] Vibhuti Narayan Singh, Shalini and G.Khan, "Forensic Analysis of Messaging App Artifacts from Smartphones for Law Enforcement Perspectives",Published in AjMS, Volume 3, Issue 2, Feb 2015, Impact Factor 0.92

[11] Al Mutawa, N., Al Awadhi, I., Baggili, I., & Marrington, A. " Forensic artifacts of Facebook's instant messaging service", Internet Technology and Secured Transactions (ICITST), 2011 International Conference for (pp. 771-776). IEEE.

[12] Al Mutawa, N., Baggili, I., & Marrington, A. " Forensic analysis of social networking applications on mobile devices", 2012, Digital Investigation, 9, S24-S33.

[13] Baca, M., Cosic, J., & Cosic, Z. "Forensic analysis of social networks (case study"), Information Technology Interfaces (ITI), Proceedings of the ITI 2013 35th International Conference on (pp. 219-223). IEEE.

[14] Mahajan, A., Dahiya, M. S., & Sanghvi, H. P. "Forensic analysis of instant messenger applications on android devices", 2013, arXiv preprint arXiv:1304.4915.

[15] Thakur, N. S. "Forensic analysis of WhatsApp on Android smartphones", University of New Orleans Theses and Dissertations

[16] Al-Saleh, Mohammed I., and Yahya A. Forihat."Skype forensics in android devices", International Journal of Computer Applications 78.7 (2013): 38-44.

[17] Josh Brunty, " Microsoft Windows 8: A Forensic First Look". (n.d.). Retrieved June 22, 2015, from http://www.forensicmag.com/articles/2012/09/microsoft-windows-8-forensic-first-look

[18] Nikhalesh Singh Bhadoria, "Windows 8 Forensics Analysis Database" [Tutorial]. (n.d.). Retrieved June 22, 2015, from http://blog.hackersonlineclub.com/2014/01/windows-8-forensics-analysis-database.html

[19] Most popular global mobile messenger apps 2015 Statistic. (n.d.). Retrieved June 22, 2015, from http://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/

[20] Daniel Walnycky, Ibrahim Baggili, Andrew Marrington, Jason Moore, & Frank Breitinger, "Network and device forensic analysis of Android social-messaging applications". Published in DIGITAL INVESTIGATION Impact Factor: 0.99 DOI: 10.1016/j.diin.2015.05.009

[21] NIST, S. 800-86. "Guide to Integrating Forensic Techniques into Incident Response", 2006, 800-86.

[22] Anglano, C." Forensic analysis of WhatsApp Messenger on Android smartphones". Digital Investigation, 2014, 11(3), 201-213.