NUST Journal of Engineering Sciences, Vol. 10, No. 1, 2017, pp. 37-45

Forensic Analysis of Social Media Apps in Windows 10

Asma Majeed[1*], Shahzad Saleem[1]
[1]School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Sector H-12, Islamabad, Pakistan
[*]asma.majeed@seecs.edu.pk
Received: 12 September 2016 Accepted: 01 December 2016

Abstract

The rapid revolution in technology has made the interaction among people easier through social media Apps and has given the business people novel ways to promote their business products and services. Therefore, now social media usage is not limited to only personal matters or fun but is also used for business advertising and selling purposes. The increased usage and need of social media has raised the risks associated with it which if exploited contribute to major losses. On the other hand, the increase in storage space with advancement in technology has made the digital forensic investigation a time consuming and difficult task. Therefore, it is necessary to have knowledge of the artifact locations of different frequently used applications so that the pre-hand information may be helpful in resolving any criminal cases faster. In this paper we have examined the behavior of Facebook, Skype and Twitter in Window 10 and has also highlighted some of the differences found with windows' previous versions i.e. Window 8.1. In our research we have put effort to find remnants of above mentioned social media Apps' usage in both the relevant databases and the registry entries.

Keywords: Digital Forensics, Investigation, Window Registry, Process Monitoring, Social Media Apps, Facebook, Skype, Twitter, Artifacts.

Abbreviations

OS	Operating System
DF	Digital Forensics
OC	Out of Court
IC	In Court
FB	Facebook
Edu.	education

Introduction

In recent years, social media has become important communication channel primarily due to its ease of access. In addition, free availability and interesting features of social media Apps keep the people of all ages attracted towards them. People can not only keep in touch with their friends through social media Apps but can also perform important tasks using them, for example Facebook groups can be used for group studying and sharing reading materials with in a class, Facebook pages can be created and shared for promotional purposes, similarly Skype can be used for online teaching.

Facebook is the most popular social media App, according to July 2016 statistics [4] and [5] Facebook has 1.712 billion active users. If we compare the stats with last year [3] we can clearly see an increase of roughly 300 million users. Facebook services include but are not limited to instant messaging, sharing pictures, statuses, news, promotional ads and entertainment. Twitter is also very popular App with around 286 million active users. According to the statistics in [6] number of expected twitter users till 2020 is approximately 370 million. The App is famous for sharing tweets and following trends. Tweets can be used to spread news or other word of mouth quickly and trends are the occasional topics. Skype is another frequently used social media App both for professionals and amateur. It supports instant messaging, video/audio calls both on mobile numbers or skype to skype.

People cannot resist using social media Apps because of their popularity and frequency of use in daily life, on the other hand, its diverse and anonymous nature has made it important platform to conduct cybercrimes, according to [7] roughly 5.5% of the Facebook accounts are fake. Moreover, many criminal cases have been reported in the recent years that are deeply rooted to the usage of one or the other social media Apps. Statistics in [8] shows that social media based crimes has risen by 15% percent in the last year.

According to the news [9] a man was held for uploading a girl's intimate video on Facebook in India. Recently German police launched nationwide raids targeting social media users [10] who posted racial hatred on Facebook and other online networks. It was first-ever such mass raids targeting online hate crime. Another cybercrime termed as the biggest cyber frauds involving an individual in this year [11] was reported by a senior citizen residing in India who was duped of nearly IRs. 1.97 crore. Many other criminal cases can be found at news sites [8] and [30].

Fortunately, the device from which the access to different social media Apps is made keeps many user details, traces and logs saved inside. This exposure of information is very significant from the perspective of an investigator. The arrangements and depth of the information vary from one operating system to another. Therefore, studying OS behavior is very imperative for any forensic investigator. Microsoft windows according to the latest statistics of [13] 89.79% market share of the operating systems on desktops is taken by Microsoft's Windows OS as shown in **Error! Reference source not found.** out of which Window 7 usage is 47% Window 8 and 8.1 usage is around 10% and Window 10 is 21.13%. One important thing to be noted here is that Window 10 is replacing window 7 as its usage is continuously increasing day by day see **Error! Reference source not found.** for detail. Furthermore, window 10 is also available in mobile versions for mobile users.

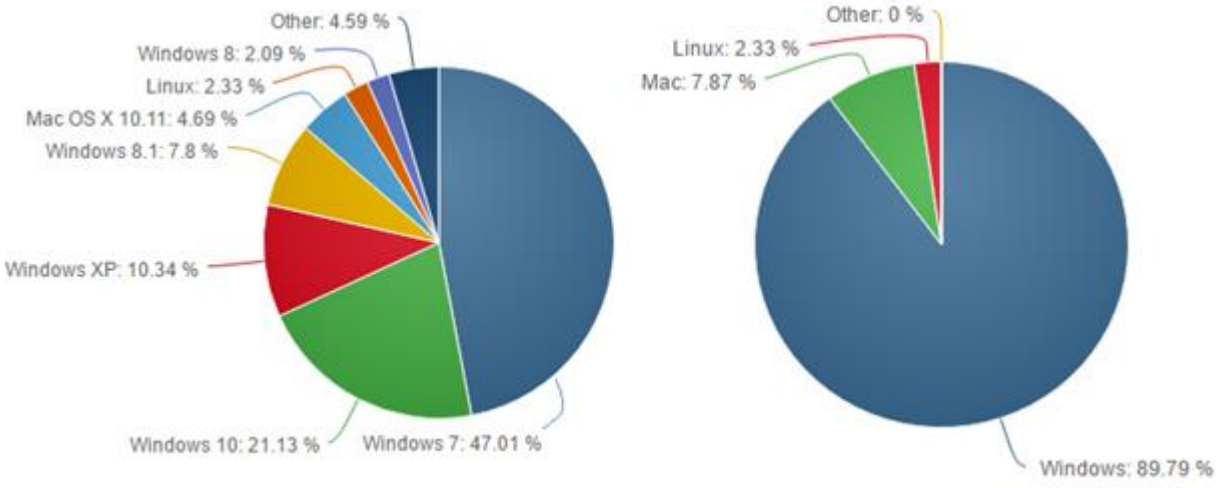

Fig. 1: Operating System usage Statistics

Due to considerable usage of window 10 on different type of devices including desktops, laptops, tablets and smart phones it is highly required that one explores the operating system in order to identify/locate maximum potential evidentiary locations and also reveal the relevant information available on these places.

We in our research are focused on social media apps usage on windows platform, selected social media apps are Facebook, Twitter and Skype. The paper explores potential locations of interest for Facebook, Twitter, and Skype remnants in both the operating systems i.e. Window 10 and Window 8.1 that might prove helpful to any forensic investigator.

Rest of the paper is organized as follows: we have discussed the literature review in section 2, followed by a brief overview of digital forensic investigation model in section 3. Section 4 comprises of the setup of test environment details. The complete methodology followed and experimentation details along with analysis results are discussed in section 5. Finally, we conclude our work and discuss the direction for the future work in section 6.

Literature Review

The technology evolution in computer science field has impacted our lives in different ways, where on one side people have utilized the advanced technology for improvements and better life style, the illegal activities have also got reshaped, the corrupt/mean people exploit the same technology augmentation for their nasty motives as discussed in “Introduction” section. This leads to the need of training the digital forensic investigators to be proficient in their area since they are now needed in every other case.

Many researchers have sensed the importance of this area and has worked in different ways to help the investigators by their research. Their main focus has been the reduction of time taken in investigation and the authenticity of the evidence collection process. In order to find gaps and room for further research we initially conducted a detailed literature review.

In [2] authors have put an effort to find traces of Facebook on Window XP using three different browsers and concluded that chat sessions run on Internet Explorer left more traces than on Mozilla Firefox and google chrome. They also observed that the chat sessions carried in Arabic language were difficult to reconstruct since they were first converted to Unicode before being saved. In [1] authors did forensic analysis of Window 7 registry. In their research, they have tried to analyze Window-7 registry with many aspects including System, application, Network, history and attached device analysis. They also developed a tool which may be helpful in their work but their work in application analysis was limited to skype and windows live messenger related artifacts only. In another research [12] authors traced the illegal activity using key logger and virtual network computing on Window 7. Researchers in [14] has also explored Window 7 registry and found the configuration related artifacts. Window registry may provide proof of an application installation by a suspect in an evident system [15]. In another paper [16] window registry is explored for system configuration and time zone details they were focused on two main digital forensics investigation steps i.e. examination and analysis in window XP (an old version of Microsoft windows).

A lot of similar work has also been done on other operating systems and devices such as android OS and mobile devices since the Apps usage in mobile devices started quite some time ago when the smart phones were initially launched. For instance, in paper [17] authors have focused on the following Apps on different mobile platforms including Blackberry phone, iPhone and android.

- Myspace
- Twitter
- Facebook

They analyzed the internal memory of the devices for identifying and analyzing artifacts residing there. They successfully found much more traces of social media Apps usage on android and iPhone as compared to the Blackberry results. Another extensive research particularly focused on messaging services of different social media Apps on android was carried out in 2015 [18], this research was focused on both the data left in the device memory as well as on the fly (network), their experiments revealed that there is a huge

privacy risk in using different messaging Apps since the messages could easily be sniffed over the network as well as

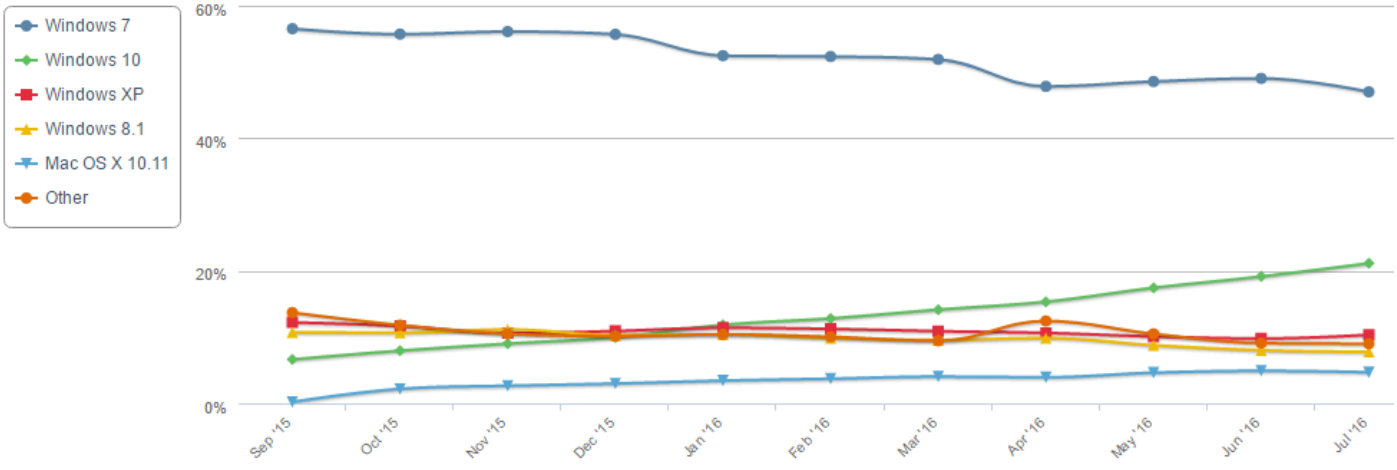

Fig. 2: Operating Systems Trend of last one year

left traces in the used device. Similarly, [19] WhatsApp forensic analysis on android platform were carried out and found all plain related information in plain text. In an another research [20] WhatsApp and Viber artifacts were examined and authors successfully found very useful databases, contact lists and plain text messages. In paper [21] Skype related artifacts were explored again on the same android platform but in the RAM and NAND flash memories.

In order to perform such forensic analysis in a way that they are useful and trustworthy there is a need to develop user friendly tools and analyze those tools in reliable manner so that these tools can be utilized effectively in this area. Many researchers have also worked for this purpose for example this paper [22] evaluates XRY 5.0 and UFED 1.1.3.8 mobile forensic tools using validation approach their results are of great interest to an examiner when choosing a better suitable tool for the case. In another research [23] authors have discussed two tools XRY (Alt1) dominates UFED (Alt2) through a case study for their performances, this can help the investigator for choosing the correct tool in the second phase of digital forensics investigation discussed in next section.

Fig. 3: DF investigation steps

Coming back to discuss the forensic investigation related research work another paper [3] discusses the artifact locations of three social media apps i.e. Facebook, Viber and Skype in Window 10 technical preview are identified. At that time, the scope was limited to the folder locations and deleted artifacts recovery. Many useful databases were successfully retrieved in this regard and permanently deleted items were also recovered using different forensic tools. Interestingly the updated Window 10 (version 10240) gives a different picture of the artifact locations hence it is very necessary to discover the new locations and data available now which we have done in this research. In addition, we have also explored the social media activity traces in window registry hives and successfully revealed some significant artifact locations. Our work shall contribute towards making the digital forensics investigation faster.

According to a thesis author [24] Window 8 registry is more or less similar to Window 7 registry however while exploring Window 8 registry he successfully found some new aspects such as the typed URLs along with IE typed URLs, he also found the remnants of Microsoft word office installation. In another research [25] authors have put effort in creating a tool "Window Forensic Analyzer" to automatically collect event logs and window registry and volatile data.

In [26] a comprehensive report is written by LCDI employees to look into the artifact locations of Window 10 and Window

So far we have been able to figure out that many researchers are working in this area still there are loopholes and gaps and according to our knowledge no published research fully focused on social media apps in window 10 (10240 version) is present. Previously independent Apps were limited for mobile phones that is why a lot of work on social media Apps is done for

android OS and mobile devices however Microsoft has changed this trend by offering Apps facility on Windows environment including Window 8, 8.1 and 10. These operating systems are widely used on desktops, laptops, tablets and other mobile devices hence social media Apps usage through these operating systems on laptops, tablets and desktops is rising hence with our research we have tried to fill the gap and provide helpful material for forensic investigators. In this regard we have analyzed the artifact locations of social media Apps in both the window registry and other folder locations, further more comparison of Window 8.1 and Window 10 behavior with these applications has also been conducted in our research.

Table 1: Activities Performed on the three Apps

Activity Code	Experiments Performed
Facebook	chat using fb messenger posting on friend's timeline Commenting on the post view notification like the comment friend commenting on same post
Skype	Account Creation search for some one's account add some one in the contact's list call a friend conversation for few min exchange text messages e
Twitter	share some one's tweet create and share new tweet follow someone add/ remove friends follow trends

Digital Forensics Investigation

In digital forensics (DF), while solving any case, the investigator should use any of the defined investigation models. In our research we have used the extended abstract digital forensics process model discussed in [27], accordingly we divided our research work into eleven phases/sub processes that are shown in the **Error! Reference source not found.**.

The identification phase refers to the identification of incident or the evidence, followed by preparation and approach strategy which involves the planning for further proceeding e.g. choosing the appropriate tools to be used during the investigation process. Preservation is also a very important and critical phase since the soundness of the arguments depends on it. In the collection phase, the investigator actually acquires the material anticipating it to be of evidentiary significance followed by the examination and analysis process of the collected data through various means, in this phase attempts to extract/carve useful artifacts are made in order to get certain leads about the case and conclude the findings. These phases are all part of OC (out of court stage). Finally, in the In-Court stage the reporting and presentation phases are steered that deals with bringing the data in a format that can be understood by the jury after which the evidence collected/ kept under observation for investigation may be archived and then returned. One important step along with all the steps is proper and safe documentation of each investigation phase.

The focus of our research is locating and exploring artifacts of social media applications in latest and relatively less explored operating systems and the scenario is not directly related to solving a particular case in jury therefore we are discussing OC stage of the investigation model in this paper. However, our outcomes are intended to speed up the future case investigations. we are locating and exploring artifacts of social media applications on disk drive both in the folders as well as window registry.

Table 2: Tools and Software List

Device/ Software	Purpose	Model/version
Laptop/ Tablet	OS and other software installation for experimental procedure	Haier Y11B core m
Desktop	OS and other software installation for experimental procedure	hp core i5
OS	Platform for performing experiments	Window 10 Edu. edition version 10240
OS	Platform for performing experiments	Window 8.1 pro
FTK imager	Taking image of the drive and exploring MFT records	3.3.0
Dcode	Verification of the MFT timestamps	4.02a
Regshot	Registry Analysis and Comparison	1.9.0
Reg decoder	Registry Data decoding	R96
Registry editor	Window Registry exploration	Version 5
Process Monitor	Tracing the artifact locations for all three apps	Sysinternals suit
Sqlite DB browser	Exploring the details of the databases found	3.7.0
Ultraedit	decoding hex/bin data	Trial version

Test Environment Setup

In order to conduct experiments, we had to setup an environment and generate artifacts, as it was not a real case where evidences are just identified and the remnants are previously generated as discussed in Section \ref{sec:m1}. We installed window 8.1 and window 10 on two different systems i.e. Laptop/tablet Haier core m y11b with 4 GB ram, 1 GB processor and Desktop HP core i5 with 4 GB ram, 2.7 GB processor. Table I provides a brief list of tools and equipment used for the purpose. We could have used a single system's multiple disk drives to install OS however we intentionally used both type of devices to cover maximum type of users and real world scenarios in our research since now days along with desktops laptops and tablets are being widely used. Furthermore, the disk drives used for window installation was intentionally

kept 30 GB so that we would easily install all the required software's and at the same time imaging the drive would not become too space and time consuming. Following window installation, Facebook, Skype, and Twitter were installed on the systems via Window's App store.

Once done, we purposely performed some activities on all three apps so as to generate some significant and interesting artifacts. The activities performed on each App are listed in Table II. For the purpose dummy accounts were created and interaction was made with our own accounts.

Methodology

As mentioned in "Digital Forensic Investigation" section we have followed the digital forensics investigation model proposed in [27] throughout our research. the steps are detailed in this section along with the discussion on our results.

Identification, Preparation and Approach Strategy

In any case where digital forensic (DF) investigation is involved, identification of evidence could mean a walkthrough of the crime scene and identifying any hardware or software worthy of collection. In our research however, in order to study social media Apps artifacts, we have decided to do our experiments on two different hardware's i.e. desktop and laptop/tablet with Window 10 OS and Window 8.1 OS as the platform for the conduct of experiments. Moreover, we have chosen Facebook, Skype, and Twitter applications to monitor and study the artifacts due to their significant market share that directly represents their popularity and frequency of use. The statistical figures of OS and Apps are already discussed in "Introduction" section as the major influencing factor. Set of reliable tools to be used were also chosen as part of preparation and strategy phases. Initially process monitoring was done using Sysintenal's 'Process Monitor' in order to get to the artifact locations. Images of the hard disk drives (specifically the drives bearing windows installation) were also identified for collection. Moreover, for window registry analysis different tools were chosen including regshot, regedit and RegdecoderR96. Windows registry was shot and saved at different stages of evidence generation in order to analyze the registry behavior of both the operating systems.

Preservation and Collection of the Evidence

We refer to our process of acquiring the disk and registry images as the collection phase. We use FTK Imager for acquisition of disks as well as for examination. The choice is made due to the fact that FTK Imager is considered the fastest and most reliable imaging tool according to [28]. The disk size as mentioned in "Test Environment Setup" section, was intentionally kept 30 to 50 GB. A raw (dd) bit by bit (logical) image was acquired and saved onto other partition drives on the same systems. Further we used regshot 1.9.0 for registry snap shots. These shots were captured at different times of experiments and were preserved for evaluation.

The identification of artifacts and their examination could easily be done over the live system. However, we chose to execute the entire examination process on images so as to reflect a real world scenario whereby integrity preservation is of considerable significance. We also used digital hashes of the collected digital evidence in order to preserve the integrity.

Examination and Analysis

The examination phase, as already mentioned dealt with exploring the image for all the selected applications i.e. Facebook, Skype and Twitter artifacts. It further required studying for any useful information that could be acquired from these artifacts. We have discussed our findings for each app separately below.

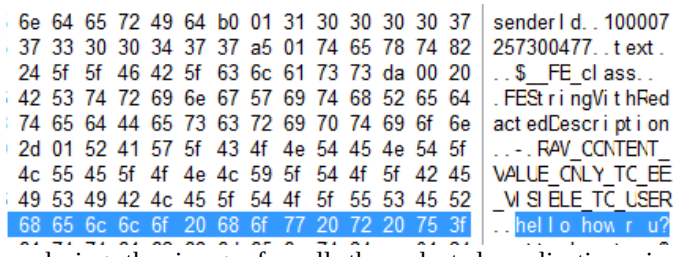

Fig. 4: Facebook conversation revealed

Fig. 5: Facebook Contact Detail

1) Facebook Analysis

Facebook App and messenger were used to generate artifacts, the activity performed is shown in Table II. Interestingly Window 8.1 gives a similar picture of artifact locations as observed in Window 10 technical preview in a previous research [3]. the location C:\Users\userA\AppData\Local\Packages\Facebook.Facebook_8xx8rvfyw5nnt\LocalState\100001833006007\DB provides several SQLITE databases with very useful information about the suspect. These databases are rich with the data from suspect FB credentials, friends' details to even plain text chat messages along with the time stamps including notifications and other posts information. Though, the Window 10 version (10240) gives a completely different picture of the scenario. In the new Window 10, instead of having most FB information in the same folder's databases the information is scattered among different folders and databases. The main reason behind this change is that now Microsoft is using osmeta instead of Islandwood as appeared in the news [29], although technically there is no difference for the Facebook App if it uses osmeta or islandwood but it makes significant difference with a forensic investigators point of view. For instance in Window 8.1 plain text messages can be found in a database "messages.sqlite" present however in Window 10 the messages are located in a different location i.e. ...\Packages\Facebook.317180B0BB486_8xx8rvfyw5nnt\L

	person_id	display_name	username	is_friend	has_messenger
1	1368464423	Saima Majeed	saimajeed	1	1
2	100012846273536	Shiza Zaheer	NULL	1	0
3	1549530756	Asma Majeed	asma.majeed	1	1
4	100001833006007	Kashi ZKashif	zaheer.kashif.7	1	1
5	100002959003117	Ambreen Khan	ambreen.khan.79	1	1
6	100008425578466	Zaryab Touseef	NULL	1	0
7	624958911	Haleemah Zia	haleemahzia	1	0
8	100007257300477	Shafaq Zaheer	shafaq.zaheer.3	0	0

ocalState\AppData\Local\osmeta_store_A645671E-DB60-47B6-9B6D-0B55EC54EFEB\messenger_messages_v1 and are in binary format not in plain text as shown in **Error! Reference source not found.**. Furthermore we have also been able to find the list of users' contact lists from the new location …\Packages\Facebook.Facebook_8xx8rvfyw5nnt\LocalState\AppData\Local\osmeta_store_87DC014B-DE1D-

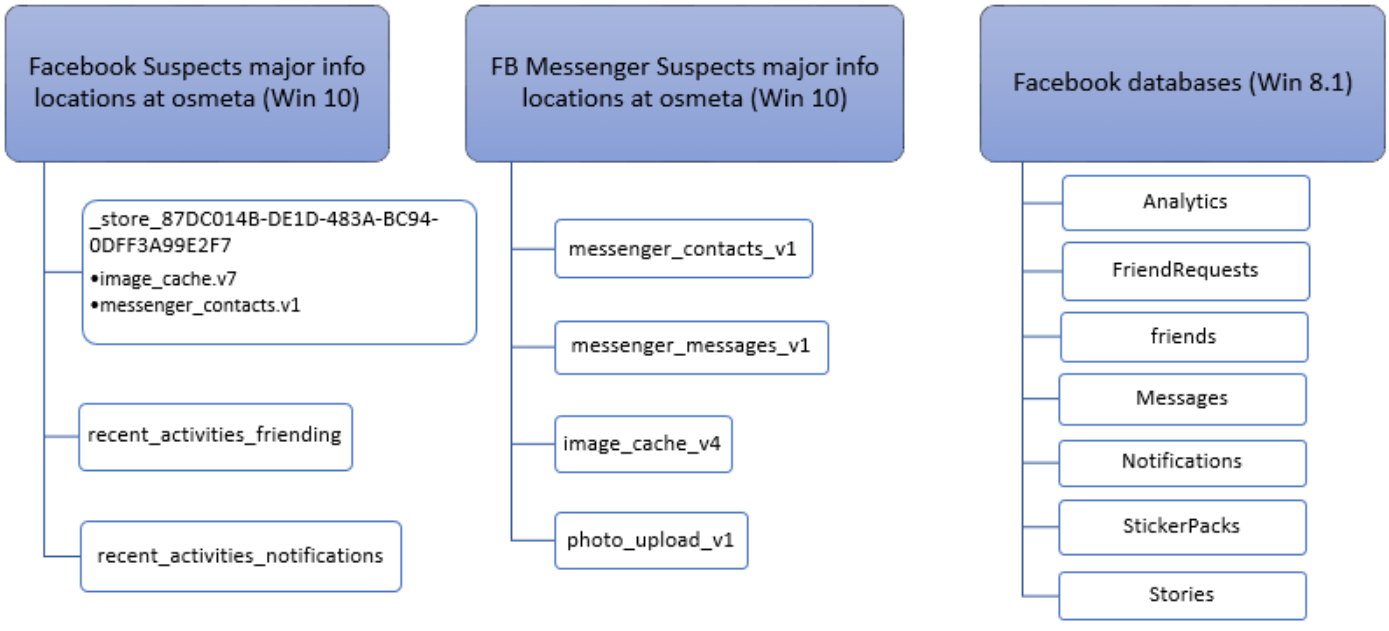

Fig. 6: Facebook Artifacts Summery

	content	sender_screen_name	reciepient_screen_name
1	Hi. Thanks for following! Welcome to the exciting wo...	TalibUzZaman	saimajeed
2	Hi Thanks for the welcome message, I follow and ad...	saimajeed	TalibUzZaman
3	hi Nadia - How r u?	saimajeed	NadiaQureshi05
4	Thank you Saima	TalibUzZaman	saimajeed
5	Hai	NadiaQureshi05	saimajeed
6	Thank you for the follow! We run summer camps for ...	summer_camps_	saimajeed

Fig. 7: Twitter plain text messages revealed

483A-BC94-0DFF3A99E2F7\messenger_contacts.v1 **Error! Reference source not found.** shows not only the peoples' usernames but also tells their statuses i.e. if they are using messenger or not.

Information about user's other activities like visiting pages, joining groups, adding removing friends along with their timestamps were also disclosed in our research. A folder at ...\Packages\Facebook.Facebook_8xx8rvfyw5nnt\LocalState\AppData\Local\osmeta_store_87DC014B-DE1D-483A-BC94-0DFF3A99E2F7\image_cache.v7 shows all the pictures seen/downloaded via Facebook along with their timestamps. The timestamps of all the activities were also verified in FTK imager images using Dcode. **Error! Reference source not found.** summarizes the overall artifact locations related to Facebook in both Windows platforms.

2) Twitter Analysis

Twitter analysis revealed very informative evidentiary data within a database at location C:\Users\username\AppData\Local\Packages\9E2F88E3.Twitter_wgeqdkkx372wm\LocalState\500897384 i.e. "twitter.sqlite". This database contains a lot of evidentiary data including plain text messages and other user activity details such as remnants of retweets, statuses, friends, followers and visited/followed trends with their timestamps. **Error! Reference source not found.** provides a snapshot of list of trends we searched for and followed as a user during artifacts generation phase. Table "messages" provide plain text messages exchanged between users along with information of the sender and receiver as shown in **Error! Reference source not found.**. Other interesting tables are "statuses", "activities2" and "users". "Users" table shows users being followed by the suspect, their total number of statuses tweets/retweets and the current status i.e. whether they are following the user or not is

available in this table. “Statuses” table provides current and previous statuses associated with the user on the device along with the information about the tweet origin. “Activities2” table keeps information about all other activities of the user including mention, retweet, favorite, reply and following a person or tweet.

3) Skype Analysis

The updated Skype App for windows also provide a lot of information about the user which may be helpful in reconstructing a crime scene. Both the operating systems has shown similar remnant locations. Skype maintains each user’s separate profile folder at location C:\Users\userA\AppData\Roaming\Skype\username.folder this folder contains several databases containing meta data and other relevant information, among those, two databases “statistics” and “main” are of more interest as they keep records related to the user activity. “Statistics” database contain different statistics including message stats, chat error stats and login stats with timestamps and user id details. On the other hand “main” database is even more revealing and interesting for an investigator since it contains plain text messages (see **Error! Reference source not found.**) along with the timestamps and

Table: search_queries

	query_id	query
	Filter	Filter
1	1	#NeverForget
2	2	#عيد_اضحى_مبارك

user credentials., user and friend details, call details including call duration (**Error! Reference source not found.**), and video calls. The tables in this database reveal information about all the members involved in the call/chat and also tells whether the call was received or initiated from the user side.

Fig. 8: Twitter Trends

Fig. 9: Skype Calls Table

Window registry was analyzed to locate social media Apps related information that are of potential evidential value and may help in digital forensic analysis process.

host_identity	current_video_audience	duration	is_incoming
saima.majeed	asma.zaheerk	75	0
saima.majeed	NULL	NULL	0
saima.majeed	NULL	NULL	0
saima.majeed	NULL	NULL	1
saima.majeed	NULL	NULL	1
saima.majeed	NULL	NULL	1
saima.majeed	asma.zaheerk	39	1
saima.majeed	asma.zaheerk	68	0

There are five root keys of window registry as shown in **Error! Reference source not found.** out of which the two highlighted root keys are the non-volatile (saved on hard disk) registry keys and the other three root keys are volatile and are the subset of the two non-volatile root keys [1].

4) Window Registry Analysis

Our analysis revealed several registry locations which

from_dispname	chatname	body_xml	timestamp
saima.majeed	majidshabbir04	AOA Sir	1472104887
saima.majeed	um.e.musab	aoa	1472627241
saima.majeed	um.e.musab	uzma how ar...	1472627244
saima.majeed	um.e.musab	how are your...	1472627251
saima.majeed	majid.shb	AOA Sir	1472104897
saima.majeed	19:6523769de...	NULL	1472106656
saima.majeed	19:c4bf9e466f...	NULL	1472106650
saima.majeed	asma.zaheerk	hello	1471775591

maintains Apps related information. Some of the useful locations are listed below

- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Skype*
- HKEY_CURRENT_USER\SOFTWARE\Classes\videocall-skype-com
- HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Families\Microsoft.SkypeApp_kzf8qxf38zg5c
- HKEY_CURRENT_USER\SOFTWARE\IDM Computer Solutions\UltraCompare Pro\ShellParams
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Facebook.Facebook_2016.817.2010.0_neutral_~_8xx8rvfyw5nntHKEY_USERS\S-1-5-21-1497239072-2030282736-2386478908-1001\SOFTWARE\Classes\ActivatableClasses\Package

Fig. 10: Skype plain text Messages Table

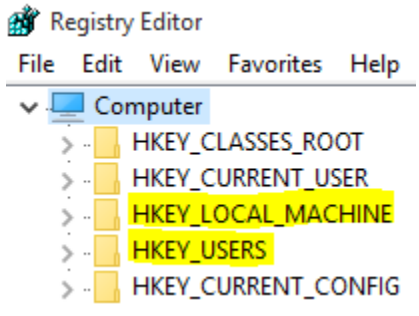

Fig. 11: Window Registry Root Keys

Conclusion

In this research we have put effort in finding social media Apps related evidentiary data that may help in recreating the crime scene fast. We successfully found locations of significant user information including plain text messages exchanged along with the sender/receiver names and timestamps. We were also able to find other user activities performed. Noteworthy differences in data location with operating systems perspective were also revealed in our research. In addition, we also found configuration and Apps installation related valuable data including timestamps.

Due to quick technology developments, there is room for extending our work in terms of more social media Apps, more detailed and in-depth study of threads and processes may also reveal more worthy evidential locations.

REFERENCES

1. Khawla A and Alghafli and Andrew Jones and Thomas Anthony Martini,"Forensic Analysis of the Windows 7 Registry ",Proceedings of the 8th Australian Digital Forensics Conference, Edith Cowan University , Perth Western Australia, November 2010
2. Al Mutawa, N., Al Awadhi, I., Baggili, I., and Marrington, A. (2011, December). Forensic artifacts of Facebook's instant messaging service. In Internet Technology and Secured Transactions (ICITST), 2011 International Conference for (pp. 771-776). IEEE.
3. Asma Majeed, Haleema Zia, Rabeea Imran, Shahzad Saleem, "Forensic Analysis of three social media Apps in window 10", HONET IEEE December 2015
4. Facebook Statistics July 2016, Retrieved 8th Aug 2016 from http://www.statista.com/statistics/264810/ number-of-monthly-active-facebook-users-worldwide/
5. Top 20 Valuable Facebook Statistics, Retrieved 14th Sep 2016 from https://zephoria.com/top-15-valuable-facebook-statistics/
6. Twitter Usage Statistics, Retreived 10th Aug 2016 from http://www. statista.com/statistics/303681/twitter-users-worldwide/
7. Facebook Statistics Retrieved 20th Aug 2016 from http://thenextweb. com/facebook/2014/02/03/facebook-estimates-5-5-11-2-accounts-fake/ \#gref
8. NDTV news June 2016, Retrieved 20th June 2016 from http://www. ndtv.com
9. Man held for uploading a video, Retrieved 20 Aug 2016 from http://www.ndtv.com/india-news/ man-held-for-uploading-girlfriends-intimate-video-1430997
10. Mass Raids Over Online Hate Speech, Retrieved 20th Aug 2016 from HTTP://GADGETS.NDTV.COM/SOCIAL-NETWORKING/NEWS/ GERMAN-POLICE-LAUNCH-MASS-RAIDS-OVER-ONLINE-HATE-SPEECH-860667
11. Fraud case june 2016, Retrieved 20th Aug 2016 from http://www.ndtv.com/mumbai-news/ mumbai-lured-by-us-soldier-on-facebook-72-yearold-conned-of-rs-2-crore-1417086
12. Raihana Md Saidi and Siti Arpah Ahmad and Noorhayati Mohamed Noor and Rozita Yunos, "Wndow Registry Analysis for Forensic Investigation",2013 IEEE, isbn 978-4673-5613-8.
13. Operating System Market Shares, Retrieved 5th Aug 2016 from https://www.netmarketshare.com/operating-system-market-share.aspx? qprid=10\&qpcustomd=0
14. Shuhui Zhang and Lianhai Wang and Lei Zhang, "Extracting windows registry information from physical memory" , 2011 IEEE.
15. Milind G. Meshram and Prof. Deepak Kapgate, "A review on forensic Investigation Using Window Registry and Event Log files ", IJCSMC, volume 4 June 2015, pages 620 to 624
16. Kisik Chang and Gibum Kim and Kwonyoup Kim and Woosuk Kim, "Initial Case analysis using window registry in computer forensics" 2005.
17. Al Mutawa, N., Baggili, I., & Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. Digital Investigation, 9, S24-S33.
18. Daniel Walnycky, Ibrahim Baggili, Andrew Marrington, Jason Moore, & Frank Breitinger, (2015, August). 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
19. Thakur, N. S. (2013). Forensic analysis of WhatsApp on Android smartphones.
20. Mahajan, A., Dahiya, M. S., & Sanghvi, H. P. (2013). "Forensic analysis of instant messenger applications on android devices". arXiv preprint arXiv:1304.4915.
21. Al-Saleh, Mohammed I., and Yahya A. Forihat. "Skype forensics in android devices." International Journal of Computer Applications 78.7 (2013): 38-44.
22. Appiah Kwame Kubi , Shahzad Saleem, Oliver Popov, "Evaluation of some tools for extracting e-evidence from mobile devices ", Application of Information and Communication Technologies (AICT), 2011 5th International Conference 2011 IEEE, ISBN 978-1-61284-832-7
23. Shahzad Saleem, Oliver Popov, Ibrahim Baggili, "A method and a case study for the selection of the best available tool for mobile device forensics using decision analysis", Mar 2016, Digital Investigation Volume 16
24. Jeremy M. Stormo, "Analysis of Windows 8 Registry Artifacts", University of New Orleans Theses and Dissertations Dec 2013.
25. Kaveesh Dashora and Deepak Singh Tomar and J.L. Rana, "A practical Approachforevidencegatheringinwindowsenvironment",I nternational Journal od Computer Applications 2010, Volume 5.
26. LCDI, "Window 10 Forensics", Leahy Center for Digital Investigation 2010
27. Shahzad Saleem and Ibrahim Baggili and Oliver Popov, "Quantifying relevance of mobile digital evidence

as they relate to case types: A survey and a guide for best practice", JDFSLVolume 9 2014.
28. Shavers, B., "Virtual Forensics (A Discussion of Virtual Machine Related to Forensic Analysis)", 2008.
29. Facebook For Windows 10, Retrieved 10th Aug 2016 from http://www.technewstoday.com/ 27755-facebook-beta-app-for-windows-10-uses-osmeta-instead-of-islandwood/
30. Pakistan Criminal Record Retrieved 10th Aug 2016 from http:// pakistancriminalrecords.com/tag/cyber-crime/