Forensic Analysis of Social Media Apps

B. Manjula Josephine, K. V. Raja Shekar, G. Meghana, K.V.S.N Rama Rao, Ch. Rajesh

Abstract: ***Social networks in any form, specifically online social networks (OSNs), are becoming a part of our everyday life in this new kind of millennium especially with the advanced and simple communication technologies through easily accessible devices such as smartphones and laptops and desktops. The data generated through the use of these technologies need to be analyzed for forensic purposes when criminal and terrorist activities are involved. And is useful to analyze and come to an understanding about their further intentions. In order to deal with the forensic implications of social networks, current research on both digital forensics and social networks need to be incorporated and understood. In this paper we are conducting forensic analysis on different networking sites such as Twitter, Skype, and WhatsApp on famous search engine called Firefox.***

Keywords**: *Artifacts, Decryption, Encryption, Skype, Twitter, WhatsApp.***

I. INTRODUCTION

In last few years we have seen rapid evolution of a new form of online communication known as social networking. In these websites users can interact and socialize, share information and ideas, post comments and updates, participate in events, upload files, photos and engage in instant messaging and conversation they attract billons of people form all over the world number of unique users using social media is approximately 830 million .

Online social networks have become more essential like electricity, water, gas. People are using/misusing them. Forensic Science is often referred to as examining and gathering of an event or crime. With the increase use of technology and social media users the forensic science has evolved to great extent. Number of crimes are increasing day by day out of them mostly they are related to social media. Social media involve people making threats, bullying, harassing and stalking others, hacking and fraud, buying illegal things, posting videos of criminal activity, vacation robberies.

Despite of using this for communication with friends many people are using this for cybercrimes, phishers, fraudsters, child predators and othercyber criminals they all will register with fake identities. These social networks encourage to share personal data like whereabouts and schedules for cybercriminals this is a goldmine they manipulate this information and use them to commit crimes.

This paper focuses on conducting forensic analysis on widely used social networking applications like Facebook, WhatsApp, Twitter, Skype on browsers and performing forensics on the data.

II. RELATED WORK

Social networking apps because of their increased use and attention have become primary source of evidence for digital investigators now-a-days.

Asma Majeed et al. [1] performed social media forensics on Facebook, Viber, and Skype. With a series of actions such as creating accounts, sending friend requests, posting on others time line commenting on posts and also sending and receiving messages. Tools used for this process were FTK imager, SQLite DB browser, EaseUS trail version. The parent directory for all the three artifacts is same and within the parent directory separate folders are present for each application is present. And can 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 2011, N.Muttawaetal.[2] tested artifacts recovery of Facebook messaging service . They conducted this experiment on three different browsers like Firefox, Chrome and Internet Explorer. They came to know that chat retrieved on Internet Explorer left more traces when compared to Mozilla Firefox and Google Chrome.In their research in 2012, N.Muttawaanalyzed forensic artifacts of several Social Media apps on various mobile platforms. The tools with which they worked on are SQLite database browser, DCode and EnCase. Their main focus had been mobile device forensics. In this regards they identified and analysed artifacts of MySpace, Twitter and Facebook each on Blackberry phone, iPhone (iOS) and Android.

In 2015 Fazeel Ali Awanetal.[3] conducted forensic analysis on three social networking sites namely, Facebook, Twitterand LinkedIn over different smart phone devices such as Apple iphone, Samsung galaxy, Windows phone as well as Blackberry. With using tools like SQLite DB browser, EnCase, andMyBackup Pro. Performing some of the common activities such as logging in, status updates, picture uploads, commenting, messaging as the results obtained are interestingly no artifacts have been found on blackberry phone.

In 2018 Taylor Cloydet al.[4] performed forensic process on Facebook exclusively on three of the browsers like Firefox, Chrome and Internet Explorer analysis of the data gathered from the Mozilla Firefox, Google Chrome, and Internet Explorer browsers using FTK supports the idea that different browsers retain varyingamounts of information about social media interactions. Findings from this study suggested that chat messages can be challenging to locate, while login information was consistently available across all three browsers. In this experiment,

Revised Manuscript Received on November 05, 2019.

***** Correspondence Author

B.Manjula Josephine, Assitant Professor**,** Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.. Email:manjulajosephine@gmail.com.

K.V.RajaShekar, Student in the Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India... Email: rajakollimarla98@gmail.com.

G. Meghana, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India. Email:meghanagudapati98@gmail.com.

K.V.S.N Rama Rao Professor**,** Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, ,Aziz Nagar, Hyderabad, India.

Ch. Rajesh Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.. Email: chrajesh984@gmail.com

Google Chrome retained the most information while Mozilla Firefox saved the least amount of residual data.

In 2015,Ibrahim Baggiliet al.[5]and his team conducted forensic analysis on android social messaging applications over upto 20 applications namely Facebook, Viber, WhatsApp, Instagram ... by connecting devices with virtual Wireless Access Point and performing some notable actions such as sending and receiving message, images etc.... The tools used for this process were Laptop, HTC mobile, Apple ipad, Network miner, Wireshark, SQLite DB browser. They are able to extract the messages in plain text format.

In 2016, Urjashee Shaw et al[6] conducted forensic analysis on windows 10 over Facebook, MySpace and LinkedIn with using tools such as IDS, Wireshark to detect network traffic and look for all kind of possible evidences that used to provide in court of law.

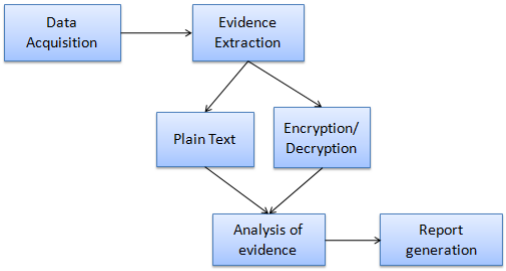
Norouzizadeh Dezfouli et al[7] performed social networking forensic analysis on applications such as Facebook, Twitter, LinkedIn and Google+ and managed to get artifacts related to them over android and IOS platforms with different actions such as usernames, passwords, login information, posts uploaded, messages that had been exchanged on each device with every application such that they help to facilitate the further criminal investigation.

Dr. Taylor, M et al[8] in his article stated that online social networking sites were acting as major barriers in current day online terror activities where suspects/criminals interact with each other on different platforms and plan their further terror activities without knowing that theirwere been watched. In his works he used different tools to work on namely Twitter investigator, Facebook forensics and also some of the most predominant tools like FTK imager, SQLite DB browser.

Umair, A et al[9] In his paper discussed how cautious the Facebook users were been in this digital era of life. He has conducted a survey on different users about how extent they were sharing their personnel information on online. He also calculated relationship strength between two persons with number of likes given by first person to second one divided by total number of likes given by first person. Thus helps in estimating the relationship strength between two people.

Thakur, N. S et al[10] has conducted his forensic analysis on WhatsApp where he tried to extract information on two kinds of WhatsApp data i.e WhatsApp data on volatile memory and WhatsApp data on non-volatile memory where he used SQLite DB browser to examine the artifacts that such as msgstore.db and wa.db. He managed to extract different kinds of tables such as message list, media, location etc.. which was used for further examination process.

III. METHODOLOGY



A. Data Acquisition:

This step of the process includes looking for all kind of physical evidences that can be retrieved in location. As we are assuming that laptop is obtained in the location. The Acquisition phase generally consists of creating the image of the system in order not to allow the system to get connected to network where there can be possibility of integrity problem. So we disclose the evidence into a faraday bags which doesn't allow signals get through it. There is no need of FTK imager in this experiment as we are performing analysis on browser artifacts.

B. Evidence Extraction:

In this step of process, we deal with existing database files, as it is unreadable format we use SQLite DB browser to look for all the evidences. DB browser for SQLite is an open source tool which is used to create, search for records in system.

The DB file for twitter is present in followingpath:*\AppData\Roaming\Mozilla\Firefox\Profiles \hsicf0xs.default-1536057033091 , on examining the above db file we are able to retrieve some information such as twitter login details, messages and tweets made.

In case of WhatsAppwe are using another tool exclusively for it called Smart phone Forensic Tool. Here in WhatsApp we work on an encrypted file which will be backed up during backup process that takes places regularly. This file is saved in the format of msgstore.db.crypt12 which is in of encrypted file. This file then need to be decrypted and then a db file is obtained which is further subjected to evaluation in order to retrieve messages that have been exchanged along with shared photos and even location details.

C. Analysis:

The results of the examination should be analyzed, in order to construct the scenario and build up the case. Analysis step consists of detailly examining each obtained result in predicting their further intentions that going to be occur. In this paper we examined all the obtained results which specify the interaction between two persons and how they were going to perform some more actions in future.

D. Report Generation:

The results of the analysis should be reported. Items to be reported may include: a description of the actions employed; an explanation of how tools and procedures were selected; a determination of any other actions that should be performed, such as forensic examination of additional data sources, securing identified vulnerabilities, and improving existing security controls; and recommendations for improvements to policies, guidelines, procedures, tools, and other aspects of the forensic process.

What if the criminals act really smart by exchanging messages and posts in encoded format? Here we also used encryption and decryption technique called Playfair cipher and performed some actions on encoded text too.

IV. ENCRYPTION & DECRYPTION

We have observed in many research papers showing that the evidence extracted is in plain text format. We are trying to encrypt the plain text and send the encrypted text to receiver and are trying to get plain text from encrypted text once received at other end.In this Project we tried to implement encryption and decryption techniques through Playfair

cipher technique which is one of the widely used encryption techniquefor exchanging encoded messages. This technique may not result in 100% successful results but showing results to some extent. The Playfair cipher starts with creating a key table. The key table is a 5*5 matrix of letters which is used to encrypt the plaintext. In this experiment thekeyweused is "Freedom". Theencryption process is explained in detail in below algorithm.

Algorithm:

Step 1: Firstly, we take input message which is user defined.

Step 2: If any space or punctuations or special symbols are present in text, then it should be automatically removed from the input message.

Step 3: If any letter is occurring two timesthen add "X" automatically in between these two characters such that specifying as they are two as this technique encrypts on pair of letters if overall count is summed up as odd number then a "X" is added at the end making it even.

Step 4: After removing the unwanted space and special characters along with balancing it we get a modified message which is called the digraph message.

Step 5: Next we encrypt this digraph message with the Keyword "Freedom" which taken as "Fredom".

Step 6: During encryption process if any two character occurs same row or same column and any one of the character occurs at the last column(for same row character) or at the last row(for same column character) then in the encrypted message they becomes first column character(for same row character) or first row character(for same column character).

Step 7: During decryption process if any two character occurs same row or same column and any one of the character occurs at the first column(for same row character) or at the first row(for same column character) then in the encrypted message they becomes last column character(for same row character) or last row character(for same column character).

Step 8: This message then may include several capital "X". Some of them may be unnecessary because they are inserted between two same occurrence character or may be inserted at the end of the message to make the message alphabet count even. Some of which may be with the original message. So we have to take only the necessary capital "X" and to discard the unnecessary capital "X". This process some times results in uneven results.After removing the unnecessary capital "X" we get our original message.

V. RESULTS AND DISCUSSION

Through this whole process we are successfully able to retrieve all the possible evidences in Twitter and Skype as well. In each of the above database files we are able to find every action that being performed on twitter. Interestingly all the user data in skype database file is shown in plain text format without hiding any data or encoding it. In case of WhatsApp the messages that has been exchanged between two parties is able to retrieved using msgstore.db file along with deleted messages also showing in the results. The messages that were encoded are able to decode using decryption algorithm specified above. Thus proving that these apps provide less security and need to be more concentrated on security measures.In the below fig.1 the screen shot clearly shows a tweet made on twitter saying the other recipient to use Playfair cipher as encryption technique

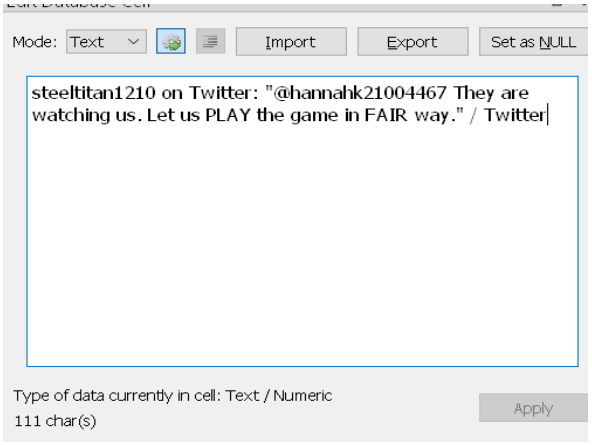


Fig. 1. Twitter image showing PLAYFAIR as encryption technique.

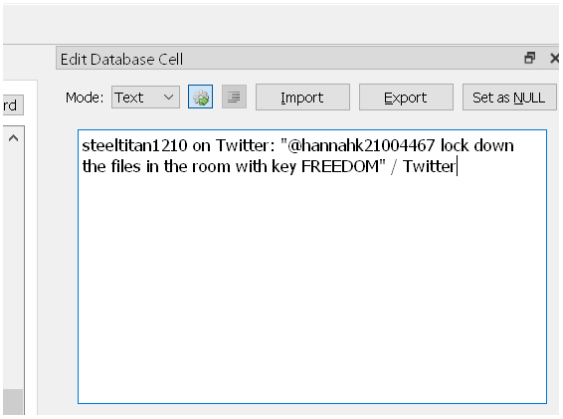
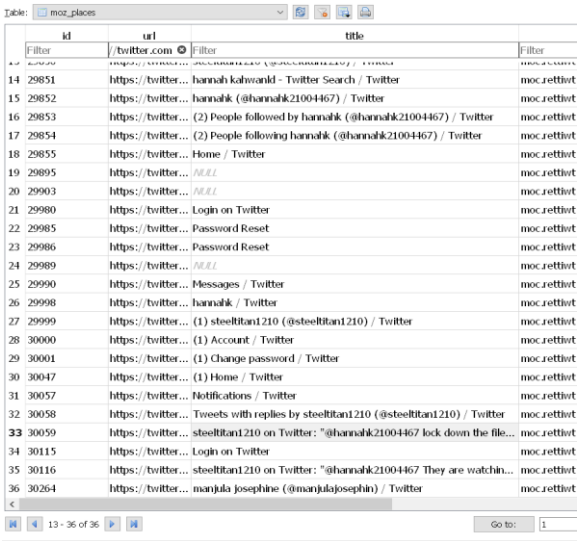


Fig. 2. Twitter image showing FREEDOM to use key for making matrix..

In the above image(fig.2) the screenshot says to use freedom as a keyword in order to make matrix which is very important for play fair cipher technique.

Table – I: Showing all actions performed on different chosen Online Social Networking Applications

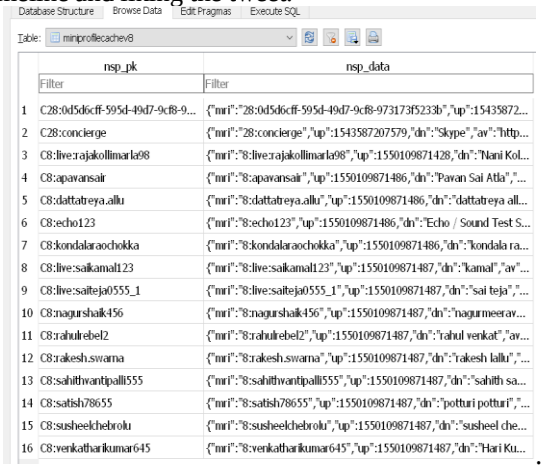
App Name	Activity Performed
Twitter	Creating account Logging in Searching for user Following User Tweeting on Timeline Sending/Receiving messages Liking the tweets
Skype	Creating account Saving contact details Looking for contact details
WhatsApp	Sending / Receiving messages Sending/Receiving images Sending/Receiving audio messages Sending/Receiving location details Sharing contacts
Facebook	Creating account Logging in Sending friend request Posting on Timeline Liking the post Commenting on the post



	id	url	title
	Filter	/twitter.com	Filter
14	29851	https://twitter...	hannah kahwanld - Twitter Search / Twitter
15	29852	https://twitter...	hannahk (@hannahk21004467) / Twitter
16	29853	https://twitter...	(2) People followed by hannahk (@hannahk21004467) / Twitter
17	29854	https://twitter...	(2) People following hannahk (@hannahk21004467) / Twitter
18	29855	https://twitter...	Home / Twitter
19	29895	https://twitter...	NULL
20	29903	https://twitter...	NULL
21	29980	https://twitter...	Login on Twitter
22	29985	https://twitter...	Password Reset
23	29986	https://twitter...	Password Reset
24	29989	https://twitter...	NULL
25	29990	https://twitter...	Messages / Twitter
26	29998	https://twitter...	hannahk / Twitter
27	29999	https://twitter...	(1) steeltitan1210 (@steeltitan1210) / Twitter
28	30000	https://twitter...	(1) Account / Twitter
29	30001	https://twitter...	(1) Change password / Twitter
30	30047	https://twitter...	(1) Home / Twitter
31	30057	https://twitter...	Notifications / Twitter
32	30058	https://twitter...	Tweets with replies by steeltitan1210 (@steeltitan1210) / Twitter
33	30059	https://twitter...	steeltitan1210 on Twitter: "@hannahk21004467 lock down the file...
34	30115	https://twitter...	Login on Twitter
35	30116	https://twitter...	steeltitan1210 on Twitter: "@hannahk21004467 They are watchin...
36	30264	https://twitter...	manjula josephine (@manjulajosephin) / Twitter

Fig. 3. Screenshot showing all the actions performed on twitter

The above figure gives all the details of every action that has been performed on twitter like logging in, searching for user, following users, messaging to particular user posting tweet on timeline and liking the tweet.



	nsp_pk	nsp_data
	Filter	Filter
1	C28:0d5d6cff-595d-49d7-9cf8-9...	{"mri":"28:0d5d6cff-595d-49d7-9cf8-973173f5233b","up":15435872...
2	C28:concierge	{"mri":"28:concierge","up":1543587207579,"dn":"Skype","av":"http...
3	C8:live:rajakollimarla98	{"mri":"8:live:rajakollimarla98","up":1550109871428,"dn":"Nani Kol...
4	C8:apavansair	{"mri":"8:apavansair","up":1550109871486,"dn":"Pavan Sai Atla","...
5	C8:dattatreya.allu	{"mri":"8:dattatreya.allu","up":1550109871486,"dn":"dattatreya all...
6	C8:echo123	{"mri":"8:echo123","up":1550109871486,"dn":"Echo / Sound Test S...
7	C8:kondalaraocholka	{"mri":"8:kondalaraocholka","up":1550109871486,"dn":"kondala ra...
8	C8:live:saikamal123	{"mri":"8:live:saikamal123","up":1550109871487,"dn":"kamal","av"...
9	C8:live:saiteja0555_1	{"mri":"8:live:saiteja0555_1","up":1550109871487,"dn":"sai teja","...
10	C8:nagurshaik456	{"mri":"8:nagurshaik456","up":1550109871487,"dn":"nagurmeerav...
11	C8:rahulrebel2	{"mri":"8:rahulrebel2","up":1550109871487,"dn":"rahul venkat","av...
12	C8:rakesh.swarna	{"mri":"8:rakesh.swarna","up":1550109871487,"dn":"rakesh lallu","...
13	C8:sahithwantipalli555	{"mri":"8:sahithwantipalli555","up":1550109871487,"dn":"sahith sa...
14	C8:satish78655	{"mri":"8:satish78655","up":1550109871487,"dn":"potturi potturi","...
15	C8:susheelchebrolu	{"mri":"8:susheelchebrolu","up":1550109871487,"dn":"susheel che...
16	C8:venkatharikumar645	{"mri":"8:venkatharikumar645","up":1550109871487,"dn":"Hari Ku...

Fig 4. Screenshot showing Skype contacts details

The above figure (fig .4) shows the contact details of each skype contact along with their name specifying their name and also usernames with which they were registered.

VI. CONCLUSION AND FUTUREWORK

Thus in this paper we are able to perform forensic analysis on twitter and skype and WhatsApp as well with getting exceptional results. Recording all the actions performed like logging in, following people, tweeting and liking the tweets. Sending/ Receiving messages, images, location details, sharing contacts, deleting messages in WhatsApp. Making calls with Skype contacts etc... In future we are looking to perform this forensic process on almost every social networking applications that are currently in trending.

REFERENCES

1. Majeed, A., Zia, H., Imran, R., & Saleem, S. (2015, December). Forensic analysis of three social media apps in windows 10. In *2015 12th International Conference on High-capacity Optical Networks and Enabling/Emerging Technologies (HONET)* (pp. 1-5). IEEE.
2. Al Mutawa, N., Baggili, I., &Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. *Digital Investigation*, *9*, S24-S33.
3. Awan, F. A. (2015, December). Forensic examination of social networking applications on smartphones. In *2015 conference on information assurance and cyber security (ciacs)* (pp. 36-43). IEEE.
4. Cloyd, T., Osborn, T., Ellingboe, B., Glisson, W. B., & Choo, K. K. R. (2018, August). Browser Analysis of Residual Facebook Data. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 1440-1445). IEEE.
5. Walnycky, D., Baggili, I., Marrington, A., Moore, J., &Breitinger, F. (2015). Network and device forensic analysis of android social-messaging applications. *Digital Investigation*, *14*, S77-S84.
6. Shaw, Urjashee, Dolly Das, and Smriti Priya Medhi. "Social Network Forensics: Survey and Challenges." *International Journal of Computer Science and Information Security* 14.11 (2016): 310.
7. NorouzizadehDezfouli, F., Dehghantanha, A., Eterovic-Soric, B., & Choo, K. K. R. (2016). Investigating Social Networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms. *Australian journal of forensic sciences*, *48*(4), 469-488.
8. Taylor, M., Haggerty, J., Gresty, D., Almond, P., & Berry, T. (2014). Forensic investigation of social networking applications. *Network Security*, *2014*(11), 9-16.
9. Umair, A., Nanda, P., & He, X. (2017, August). Online social network information forensics: A survey on use of various tools and determining how cautious facebook users are?. In *2017 IEEE Trustcom/BigDataSE/ICESS* (pp. 1139-1144). IEEE.
10. Thakur, N. S. (2013). Forensic analysis of WhatsApp on Android smartphones.
11. Rao, K. R., & Josephine, B. M. (2018, October). Exploring the Impact of Optimal Clusters on Cluster Purity. In 2018 3rd International Conference on Communication and Electronics Systems (ICCES) (pp. 754-757). IEEE.
12. " **Integrity based Video Watermarking using Gaussian Based DWT Embedding and Extraction process."** had published in International Journal of Applied Engineering Research (**IJAER**), Volume 11, Number 5**(2016)** ,pp. 3235-3240, ISSN :0973-4562 , Research India Publications.

AUTHORS PROFILE

Ms. B.Manjula Josephine working as an Assistant Professor, in the Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram. Andhra Pradesh. Had 2 years of teaching experience. Her main areas of research interest are Machine Learning and Computer Forensics

K. V. Raja Shekar is a student at the Department of Computer Science and Engineering at Koneru Lakshmaiah Education Foundation Vaddeswaram, Andhra Pradesh. His interested area of research is Networking

G. Meghana is a student at the Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation Vaddeswaram ,Andhra Pradesh..

Dr. K.V.S.N.Ramarao Professor, in the department of computer science and engineering at Koneru Lakshmaiah Education Foundation. Deemed to be University, Aziz Nagar, Hyderabad.. Had 20+ years of experience in academics and industry. International experience at Australian University. His research intrests include cyber security, machine learning and bioacoustics.

Ch.Rajesh, is a student at the department of Computer Science and Engineering at Koneru Lakshmaiah Educational Foundation, Deemed to be University, Vaddeswaram, Andhra Pradesh.

.