FORENSIC ANALYSIS OF SOCIAL NETWORKS *FACEBOOK / INSTAGRAM*

Pinal Arvindbhai Amrutiya

Student

M.tech in Cyber Security

Rashtriya Raksha University, Gandhinagar, Gujarat, India

pinalamrutiya18198@gmail.com

Dr.Ravi sheth

Assistant Professor

School of Information Technology, Artificial Intelligence and Cyber Security

Rashtriya Raksha University, Gandhinagar, Gujarat, India

ravi.sheth@rru.ac.in

Mr. Priyank parmar

Assistant Professor

School of Information Technology, Artificial Intelligence and Cyber Security

Rashtriya Raksha University, Gandhinagar, Gujarat, India

priyank.parmar@rsu.ac.in

Abstract : Two of today's most popular networks are Instagram and Facebook. With the rising use of apps for social networking on smartphones, they are a gold mine for forensic scientists. Potentials may be stored and derived using appropriate research techniques and procedures. This article focuses on a forensic analysis on apps widely used on smartphones such as Facebook and Instagram in social networking. The forensic exam is to determine whether these programming' operations are stored in the inner memory of the computer. The analyzers will reconstruct the contact list and the timeline of messages shared by users using the findings described in this article.

Keywords : Facebook Artifacts, Instagram Artifacts, Mobile Forensics Tools, Digital Forensics, Social Media Forensics,

I. Introduction

In recent years, a new online contact called social networking has grown rapidly. By joining these administrations, clients can associate and mingle, trade data and considerations, post Feedback and cautions, participate in occasions and projects, transfer documents and pictures, partake progressively communications and prompt informing. These advances draw a huge number of clients from across the globe.

The pattern in interpersonal organizations is changing people's ways of life. Since both cell phones and PCs are associated with similar instruments, recently created applications should serve the two closures to fulfill the clients. Albeit the previous flourishing interpersonal organizations like Facebook, Instagram, Whatsapp, Snapchat, LinkedIn, among other informal communication locales, actually have huge quantities of clients, their development rates have bit by bit decreased. It has been supplanted by arising long range informal communication locales like Instagram or Facebook, so examples of cybercrime have likewise changed by user's exercises. To distinguish wrong doings, it is essentially important to utilize suitable measurable procedures to recuperate these follows and the proof This examination thinks about informal communities in Facebook and Instagram as a point for re-research. Investigate the excess antiques on the Facebook/Instagram application and show proof of assortment like stories, posting photographs, labeling others, and profile data on the Android stage, individually.

Instagram is also exploited for cybercrime, including drug buying and trading, e-blasts, hoaxing, child-support, and mainstream media are Facebook and Instagram. The police investigating a criminal offence will share inquiry content on the social media. Forensic social media surveys can also be used to gather data on the case. Like Android, smartphones usually use social media.

The population of social media in 2019 was about 2.77 billion. And we should expect that these figures will rise much higher with smartphones and the Internet connection being cheaper and easier access. By 2021, social media will be used by more than 3 billion people. In Social media Facebook & Instagram popularity high level.

Social networking has since become a significant influence in modern culture. This has also, however, contributed

to endless illegal activity on social networks, including cyberbullying, social engineering, and identity fraud. The identification of cybercrimes on social networks is distinct from other cybercrimes depending on the following characteristics. Therefore, research into these emerging technology is required to assist the investigators in enhancing their quality of crime resolution.

- **Anonymity :** Because they deal with a fictional account, people are often unsure of the actual identity of their counterpart on a social network. Therefore, it is impossible to obtain information from the suspect and to take arrests promptly in the event of a social network cybercrime.
- **Diffuseness :** Any news released by the social network, which causes the diffusion effect, will be sent or exchanged automatically. There are therefore substantial damages to the victim if the crime in the social network cannot be reached immediately.
- **Cross-Regional feature :** Because of the existence of the internet, cyber crime's origin is not always the location of the perpetrators. Owing to the difficulties of identifying suspects, a backlog is created during the criminal investigation.
- **The Vulnerability of Evidence :** The evidence obtained in the form of digital data on social networks. In addition to the highly volatile nature of digital evidence from collection to storage in the processing program, digital evidence can be changed, deleted, lost, or contaminated due to the anti forensic operation of the investigators' suspects or neglect.

Our work focuses on exploring the potential location of the Facebook and Instagram remains of the documents: we have mentioned the literature survey for Mobile Device Forensics, Social Networking Forensic Artifacts, Analysis of Social Application, Analysis Funcationality of Facebook & Instagram Section II, also include in comparision tools table for mobile forensics analysis. Finally, we conclude in Section III and Section IV Reference.

1.1 Case Scenario Process :

A simulated case of pornographic crime was conducted in the research. The simulation is necessary to enable the researcher to determine how the case of pornographic crimes occurs, whereas the scenario is seen in the figure.

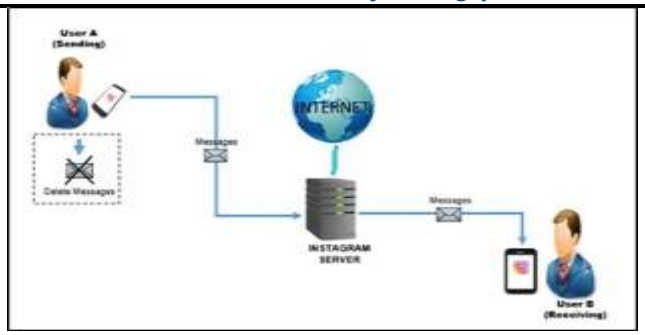

Figure : Chronology of communication and Client B using an Instagram messenger smartphone.

In view of the above case reenactment, two clients will utilize the Instagram application to convey, that is, client one, and Customer B. (Message beneficiary). Customer A has a cell phone with the GT-S5282 Samsung World Star, while customer B has a Samsung Universe GT-S7580. The two clients have a cell phone. Both of them are connected to Instagram's social media account and are used for communications by the client's own account, that is by sending chat and photos via Instagram, the client sends user B pornographic chat and photos after sending a chat and photos and the user deletes everything to delete the evidence. Instagram also has a chat and photos function. User B reports directly to the authorities the incident he has experienced. Client reports B are answered directly by the authorities. In the following procedure, the authorities give the customer a search letter to protect the mobile that acts as the means of Instagram access for interacting with Client B. For visual documentation in the form of a conversation and pictures taken from your mobile by client B to be found and returned. The following measures can then be extended to a system NIST, namely compilation, revision, review, report, by a case suggesting porn crime, Based on the simulation of the timeline of cases indicated by porn crimes mentioned above.

II. Literature Survey

2.1 Mobile Device Forensics

Beginning work zeroed in on buy procedures and general scientific investigation of brilliant gadgets. In his work, we discussed the measurable audit of old Android forms and the equipment and programming for procurement. We likewise depicted diverse examination techniques, including the utilization of hex editors and emulators. Later exploration gave essential ideas to the new ages of cell phones for scientific investigation (for example Android and iPhone). The innovations utilized, the taking care of techniques and the

regular stockpiling settings have been depicted for every gadget. For every gadget, stockpiling settings were portrayed. Call logs, SMS, MMS, email messages, Pages bookmarks, photographs, recordings and schedules were the information that can be removed from the inner stockpiling of these gadgets. Recent science has focused on different smartphone types and methods for collecting and analyzing device internal memory and data from each device. The physical method requires a system breakdown, resulting in a minor modification of the system data. It is regarded as the best method of forensics to take the iPhone and the NIST assessed. Android-based smartphones can be purchased physically or logically, similar to iPhones. The physical technique requires root access to the device, to get add image of the phone memory. Discuss an acquisition procedure using special forensic acquisition software to overwrite the "Recovery" partition on the Android device card.

Commonly recoverable information contains:

- Text Messages (SMS – Short Message Service)
- Photo/Multimedia Messages
- Pictures and Images
- Video and Audio Recordings
- Call History Logs Phonebook and Contacts
- Calendar and Task List Entries
- Emails stored on The handset
- Internet Browsing History
- Social Networking Artifacts(Facebook etc…)

2.2 Social Networking Forensic Artifacts

As social applications for smartphones are growing, they provide forensic investigators with the largest archive of data. Were you aware that over 90% of social media consumers access social media sites on mobile devices? Besides, with the appropriate inspection procedures and equipment, this data can provide vital leads in a case. In this sense, they store an array of possible knowledge that medium forensic experts may obtain from the correct instruments.

Our project has also included research on computer systems and methods that lead to the retrieval of those objects left behind by social networking sites. Additional studies explored how Facebook and Instagram chat objects can be retrieved and rebuilt from the hard drive of a computer. The database saves data on any friend in the list, including names, ID and telephone numbers.

The use of cyber forensics and data retrieval tools in social media forensics includes:

* extract information from websites like social media Instagram, Youtube, Email, LinkedIn, etc.

* Saving, Storing,

* Research and analysis

* Retaining the information about the location of the origins of electronic proof in the Court of Justice. The unimpeded selection is followed by reverence for all laws.

2.3 Analysis of Social Applications

A digital criminal case, describing it as having four principal phases: recognition, compilation, organization, and introduction, is a National Institute of Standards and Technology (NIST). The stage of identification implies the identification of an occurrence or evidence. It generates and then sculptures inferential data and subsequently, it decreases the sum of the data by removing redundancies. To draw firm conclusions, the gravitated evidence is analyzed and related to the crime scene. Finally, the presentation process coherently covers the interpretation of evidence by the jury.

1. Identification of evidence

This move requires a detailed analysis of the malfunctioning scene to identify hardware or software worth gathering. It also includes a rudimentary search for user-friendly networking accounts on this subject. A definitive hunt in the Gregarious media for both relatives, colleagues, and acquaintances.

2. Collection

Forensic analysts use many techniques to obtain electronic data. The approaches to gathering facts in easy-to-use media are as follows.

- Manual documentation
- Screen scraping / Screen capture
- Open source tools (HTTrack)
- Commercial tool (X1)
- Web hosting (page freezer)
- Medico-legal establishment
- Assigning content

Furthermore, different social media toolkits for collecting facts on the smartphone are accessible in a rational way. The logical acquisition requires a logical photograph of all the data of the smartphone's internal memory. The files are then reviewed to check the different operations.

3. Examination (Organization)

During the logical acquisition, the files received require special decoding tools and content visualization. They have a

wide variety of user data until decoded, such as call history, sending and receiving SMS, calendar events, and address book entries. They have an immense bank with social media signatures for forensic investigators. These objects are then analyzed and compared to the case itself.

Facebook Analysis Artifacts : profile information, places visited, locations Activity logs, Facebook archives and geographic locations, groups, Memories, Your time in Facebook, interests, Stories, text and links, friends and family, pages, all activity timestamps, details of busy friends in active chat sessions with the subject and much more.

Instagram Analysis Artifacts : Profile information, Friends Followers & Following, posts, Archive, Stories, Locations Activity logs, pages, Groups, Text & Links, Story Highlight, Reels, Saved items.

2.4 Analysis Functionalities of Facebook & Instagram

Functions for analysis are performed to recognize the features of Instagram that are important to research. This is a map of Instagram's characteristics that are of investigative importance

No.	Features	Function
1	**Posting**	Share photos or videos. This feature can provide information related to the user's lifestyle or as evidence of a possible crime.
2	**Stories**	Share user's daily stories. This feature only lasts 24 hours after being uploaded. This feature can provide information related to the presence or absence of deviant acts committed and can be used as evidence of traces of possible crimes.
3	**Direct Message**	Send messages, such as texts, photos, videos, and voice notes, privately to other user accounts. Besides, users can make video/voice calls. This feature can provide information about the communication documentation by the user. It also gives an insight into the user's mindset that can be used as evidence of traces of possible crimes.
4	**Search & Explore**	Find accounts and content that you might like from accounts that have not yet been followed. This feature is useful for finding evidence of impersonation & theft of account identity and provides information related to user activity.

Table 1. Analysis Functionality of Facebook & Instagram

2.5 Comparision Tools For Mobile Forensic

	Andriller	ANDROPHSY	Celebrite UFED	Oxygen Forensics Suite	Paraben Mobile Forensic Tools	MSAB	Lime	Autopsy	MOBILedit Forensic	Belkasoft
Open Source	☑	☑	☒	☒	☒	☒	☑	☑	☒	☑
Root required	☑	☑	☒	☒	☒	☑	☑	☑	☒	☑
Call Logs	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
SMS/MMS	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Contacts	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Browser History	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Photos	☑	☒	☑	☑	☑	☑	☑	☑	☑	☑
Facebook Messages	☒	☒	☑	☑	☑	☑	☑	☒	☑	☑
Instagram Messages	☒	☒	☑	☑	☑	☑	☑	☒	☑	☑
Deleted Data	☑	☒	☑	☑	☑	☑	☑	☒	☑	☒
Recovery of Data	☑	☒	☑	☑	☑	☑	☑	☒	☒	☒
Presentation	☑	☒	☑	☑	☑	☑	☒	☒	☒	☒

Table 3. Comparision tools for Mobile Forensic Analysis

III. Conclusion

Social media is an important part of our daily lives. This is one of the most essential ways in which we interact. For, This research has identified artifacts produced by Instagram and Facebook applications based on Mobile Operating System. These artifacts include user setups that contain user accounts information, number of users, followers, and accounts of close friends. In this Document, we analyze the functionality of Facebook and Instagram. It is also analyzed many free and commercial mobile devices Specifically forensics tools that focus on the operating system. We have also analyzed mobile forensics tools that restrict forensics collected data such as open-source, root required, call logs, contacts, etc. Therefore, the specifications for all data are forensically retrieved into the Instagram & Facebook Application using a Mobile operating system

IV. References

[1] P. Patel, K. Kannoorpatti, B. Shanmugam, S. Azam and K. C. Yeo, \"A Hypothetical Survey of Online Media Utilization by Digital Criminals,\" in Worldwide Gathering on PC Correspondence, and Informatics, Coimbatore, 2017.

[2] H. Arshad, A. Jantan and E. Omolara, \"Evidence assortment and criminology on informal organizations: Exploration challenges and directions,\" Computerized Examination, vol. 28, pp. 126-138, 2019.

[3] D. M. Taylor, D. J. Haggerty, D. Gresty, P. Almond and D. T. Berry,"Forensic Examination of Informal communication Applications," Organization Security, 2014.

[4] M. S. Chang, \"Evidence Get-together of Instagram on Windows 10,\" Global Diary of Imaginative Science, Designing and Innovation, vol. 3, no. 10, 2016.

[5] G. Satrya, P. Daely and S. Shin, \"Android crime scene investigation examination: Private talk on social messenger\", Pervasive and Future Organizations (ICUFN) 2016 Eighth Worldwide Meeting on, pp. 430-435, 2016.