International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12– No.18, January 2019 – www.ijais.org

Security Vulnerabilities of Skype Application Artifacts: A Digital Forensic Approach

S. Idowu
Lecturer, Computer Science Department
Babcock University

Ehiwe D. Dominic
PG Student, Computer Science Department
Babcock University

S. O. Okolie
Lecturer, Computer Science Department
Babcock University

N. Goga
Lecturer, Computer Science Department
Babcock University

ABSTRACT
Social network platforms and apps have gained popularity partly because of the ease by which users are able to sign up on the platform. This is in addition to the open source nature of majority of these software applications. By making use of these social network platforms and applications, users consent to the disclosure of information that may be used to recreate their profile, to reconstruct events that have taken place, and provide most times geo-location information that can be used to track or trace participants. In this study, presentation of the potential security vulnerabilities that can be associated with the digital artifacts harvested from Skype, a social network app in use by millions of subscribers worldwide is made. The study methodology involved set up of a forensic workstation for the acquisition and examination of the digital artifacts obtained from Skype application installed on a test Infinix HotNote Smartphone running Android OS version 5.5 that was utilized for this study. Following the National Institute of Science & Technology (NIST) guideline, the chain-of-custody of the performed activities was documentation. A key finding of this study indicates the acquired and examined stored user data and other metadata information are stored in plain and clear text formats. The security implication for this is significant as the ease or potential for a cyber-criminal activity becomes heightened. Therefore, the implementation of a robust and secure data encryption standard for protecting stored user records is recommended. While there are different types of encryption algorithms that may be utilized for achieving user security and privacy requirements, the decision to enforce any of the known standards can be taken following global application security standards for implementing security of software applications.

Keywords
Security vulnerabilities, Digital artifacts, Encryption, Metadata, Algorithms

1. INTRODUCTION
Networking socially has in recent years become the latest trend of online communication by which people come together from far and near. This trend now accounts for billions of people connected from all over the world with physical barriers no longer a hindrance. Joining these services make real-time conversations possible with audio and video media shared by participants. Social networking has indeed created a form of social economy and shattered myths and barriers that were once thought impregnable. Participants are able to socialize and interact, share ideas and disseminate information, provide updates and make comments, participate in activities and online events, share audio and video files and photos, carry on extended real-time conversations and instant messaging all over the world. Social network platforms and apps have gained popularity partly because of the ease by which users are able to sign up on the platform. This is in addition to the open source nature of majority of these software applications. While a few applications may be proprietary in nature or restricted to use by only members of a group, the majority of applications are available publicly for anyone to download, install, sign-up and communicate freely with others. Examples of the most popular social networking applications are Facebook, WhatsApp, Instagram, Twitter, Viber, Skype etcetera. At the end of 2017, an estimated 2.46 billion users worldwide were reported to be on social network platforms. This figure is expected to grow up to 2.77 billion by 2019 (International Telecommunications Union, 2018). In addition to this statistic, it is reported that about 71% of users on the internet have social network profiles and users are concentrated across the different continents of the world. By making use of these social network platforms and applications, users consent to the disclosure of information that may be used to recreate their profile, to reconstruct events that have taken place, and provide most times geo-location information that can be used to track or trace participants. While networking socially enforces the concept of communal living, it however provides avenue for cyber related criminal activities taking place. Interestingly, the events that take place among social network participants are logged on the internal storage mechanism or hard disk of the devices from which users connect and share information. These digital artifacts are available for anyone that knows how and also possess the means to access these information. To both the good and the bad guys this trove of information can be leveraged for achieving other objectives often unintended by the data owner. From the perspective of digital crime occurrence and the forensic investigation of these crimes, the availability of this large amount and variety of information has two major implications. Firstly, social network platforms and applications can be leveraged by malicious individuals. Cyber criminals are able to utilize the harvested information for creating fake user profiles, create untraceable accounts to stalk, blackmail others, and carry out phishing and spamming attacks etcetera. Secondly, the availability of this information enables skilled digital forensic investigators track the perpetrators of these cyber related criminal activities. By aggregating and correlating the artifacts identified, collected, examined and processed, investigators are able to determine where, when, why and how these criminal activities may have taken place.

In this study, the potential security vulnerabilities that can be associated with the digital artifacts harvested from Skype, a social network app in use by millions of subscribers worldwide is presented. The rest of the paper is organized as follows: section II provides details of related works in the area of social networks and applications forensics by other

researchers. Section III describes the methodology and setup of the experimental test environment for acquiring the digital artifacts of Skype social networking application. This section also presents the security vulnerabilities that are associated with these acquired digital artifacts. Finally, in section IV, the research conclusion and relevant recommendations of interest to forensic investigators and researchers is presented.

2. RELATED WORKS

Researchers such as [1] performed forensic analysis of Facebook application artifacts that run on different browser types on the Microsoft Windows XP operating system. Their research found differences in the sessions of chat events performed on the different browsers. According to the study findings, more traces were left on Internet Explorer browser compared to the traces found on Google Chrome and Mozilla Firefox. Their research also found out about the complicated process of performing key search operations during forensic analysis of the digital artifacts where the chat data is in Arabic language. This is due to the chat messages being saved after conversion to Unicode characters. Furthermore in 2012, [1] carried out the forensic analysis of other social networking applications performed on mobile devices. Forensic investigation of Viber application was performed by [5]. The retrieval of the application artifacts stored in Random Access Memory (RAM) of devices running the Android operating system was carried out. The research found out that Viber application artifacts are still present on a device even after it must have been reset or formatted. In consequence, this indicates the application artifact persists in RAM of user devices. Extracting the file system artifacts on smartphones through forensic data acquisition techniques, [2] carried out the forensic analysis of both Viber and WhatsApp applications on Android devices. Findings from the experimental study showed traces of users shared contents, list of contacts and chronological listing of communication history for both applications. A study that was focused on what the researchers referred to as "volatile instant messaging" applications operated via web interfaces was conducted by [6] 2008 and 2010. From the findings of the study, the researchers concluded that cyber criminals are capable of taking advantage of the popularity of instant messaging applications to violate the privacy rights of participants. Kiley et al analyzed, within a Windows desktop operating environment, three popular instant messaging applications that are web-based. They found forensic artifacts of these applications stored both in the cache files of the browser and the page files on Windows. Their experimental study retrieved timeline artifacts of participant communication, the account profiled usernames on the application, the registered contact names saved by users on their devices in addition to snippets of shared conversations. However, one interesting finding of their research was that retrieving the complete shared conversation artifacts end-to-end was not a possibility. The authors presented a framework for addressing the volatility of instant messaging applications from a forensic investigation viewpoint; this includes artifact recognition, artifact formulation and searching.

3. METHODOLOGY

3.1 Test Environment Set Up

A forensic workstation was set up for the acquisition and examination of the digital artifacts obtained from Skype application installed on a test Infinix HotNote Smartphone running Android OS version 5.5 that was utilized for this study. Table 1 below lists the hardware and software utilities that were used to acquire the application artifacts for a profiled user.

Table 1. List of Forensic Tools for Application Data Acquisition & Examination

Application/ Tool	Classification	Make / Version	Summary of Functionality
VM workstation on Windows PC	Hardware	Intel Core i5 with Windows 8.1 operating system	Forensic Lab Workstation
DB Browser for SQLite Autopsy Forensic	Software Software	V3.10.1 V4.4.0	SQLite Database File Browser Application. Forensic Image Analysis
Android Debug Bridge Tool	Hardware	V1.0.32	Android OS Debug Tool.
Infinix HotNote 4	Hardware	Android OS V 5.5	User Smartphone Device
HashCalc	Software	SlavaSoft V2.4.0	Hash Algorithm Application for Data Integrity Check.

3.1.1 Skype Application Data Acquisition Procedure

Forensic investigative studies begin with identification of data of interest. As defined by the National Institute of Standards and Technology (NIST), the four phases of a forensic investigation include the following:

- Identification
- Acquisition
- Examination
- Reporting

For this study, the data acquisition procedure involved performing the below documented chain-of-custody activities for obtaining the artifacts from Skype:

i. INFINIX HotNote smartphone was placed in a rooted mode to allow root user access to the entire file system and partitions on the device;

ii. Applications were downloaded and installed from Google Play Store;

iii. Sign-up and sign-in to the applications on the rooted device;

iv. Application files acquisition and hashing using MD5 and SHA-1 hash algorithms;

v. Creation of image copy of application files for forensic examination and analysis;

vi. Hashing of duplicate image copies to verify data integrity.

3.2 Research Finding and Discussion of Associated Security Vulnerabilities

Figures 1 & 2 below show the contact information of a Skype application user and the associated application artifact metadata information.

Application Metadata Artifact (User Contact)

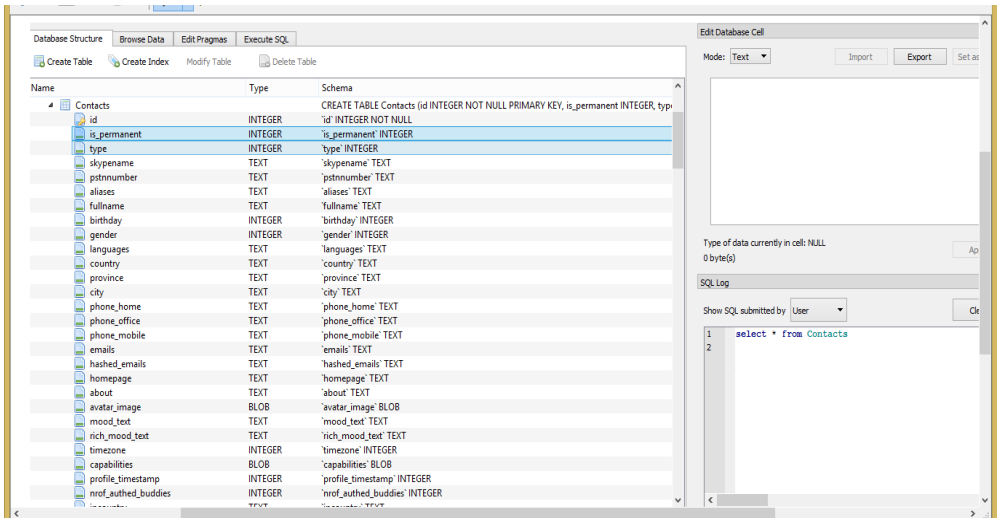

Fig 1: Application Database Table Structure – Contacts Table

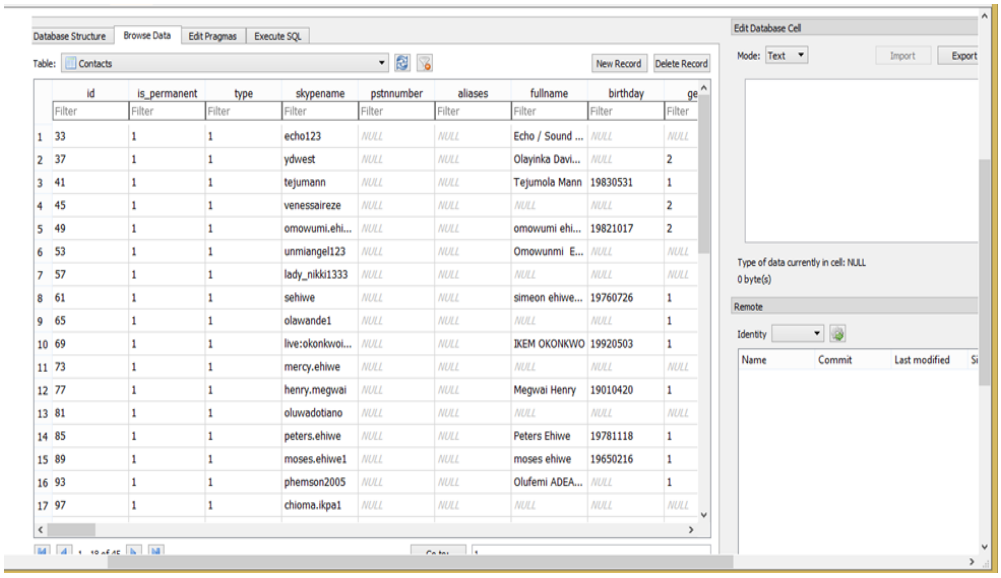

Fig 2: Digital Artifact from User Contacts List

- Security Vulnerability Associated With Contacts Details Metadata Information

Figure 2 above shows filtered records for the application user's contact. This table contains records of other users which the Skype account owner have connection or communicate with. As shown, some of the fields have sensitive data content displayed in plain-text. The security vulnerability of plain-text display of user profile account details makes the application user a potential target for "Profile Cloning Attacks". Profile Cloning Attacks is a growing type of cyber-criminal attack which focuses on faking user profiles on social network applications for malicious purposes.

Application Metadata Artifact (Messages)

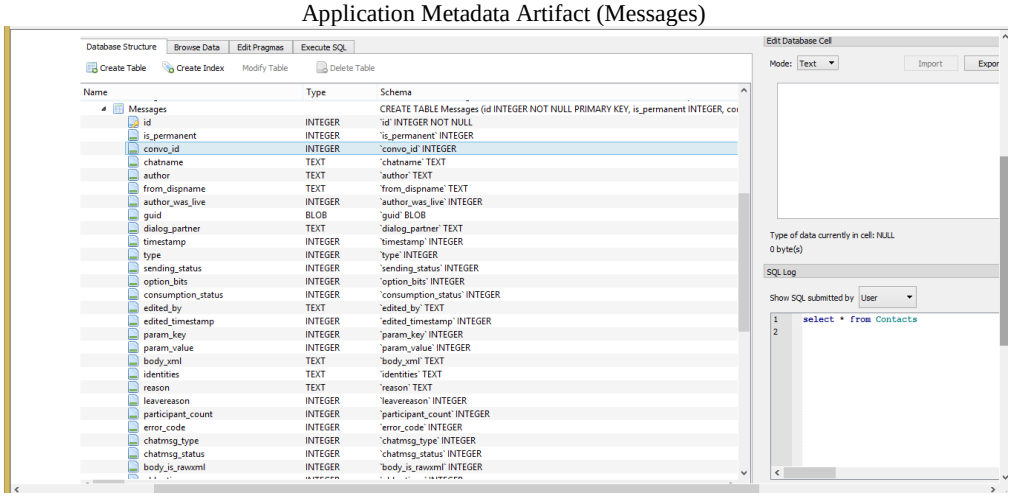

Fig 3: Application Database Table Structure – Messages Table

Figure 4 below is a snapshot of the messages table that has been filtered by the columns in the SQL query statement retrieved from Skype.

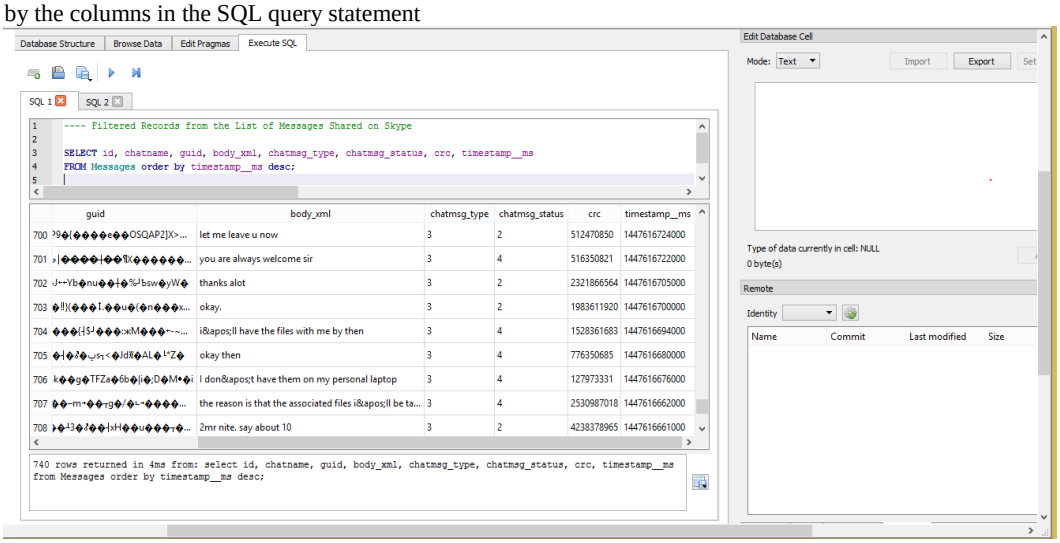

Fig 4: Digital Artifacts from Shared Messages

- Security Vulnerability Associated With Messages Metadata Information

Majority of social network applications do not implement encryption of user communication. As messages are logged and transmitted in plain-text, this represents a key security and privacy risk for users. In addition, user preferences and behavioral profiling can be determined by mining the content of shared messages. This kind of information can be utilized by parties such as marketing companies that target users with adverts tailored to their interests, government security agencies and also cyber criminals who seek to commit fraud.

- Application Metadata Artifact (Shared Files)

Users of social network applications take advantage of the file sharing features available on the applications for transmitting documents, pictures, audio and video files. While this feature enables interconnection of people and serves as means of communication, it also presents opportunity for information security or user privacy breach.

Though the sharing of pictures, videos and other types of multi-media artifacts through social network applications might be harmless, cyber-criminals are taking advantage of this to share illicit images online, transfer malicious codes and other types of virus applications. This potential for crime continues to be a source of concern for information and cyber security professionals.

These possible cyber-criminal activities that can be carried out through the use of media sharing features on these applications include the following:

- Data hiding in image files;
- Malicious payload transfers via audio and video file header details;
- RansomeWare attacks carried out through data encryption in exchange for decryption keys.

On Skype social network application, records of shared files by default are stored on the HD of the computing device and the path to this shown below:

Root\Users\%userprofile%\AppData\Roaming\Skype\My Skype Received Files

Figures 2 to 4 show details of multi-media artifacts that a Skype user has shared with others. The metadata information available from these artifacts can be seen from the logged records.

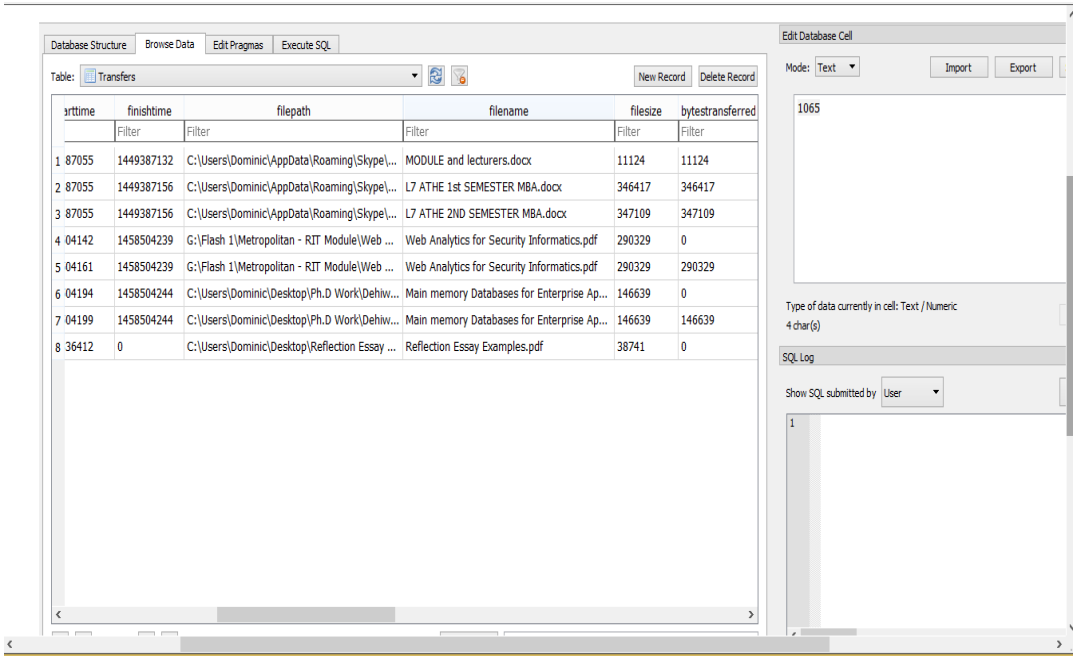

Fig 5: Shared Multi-Media File Records 1

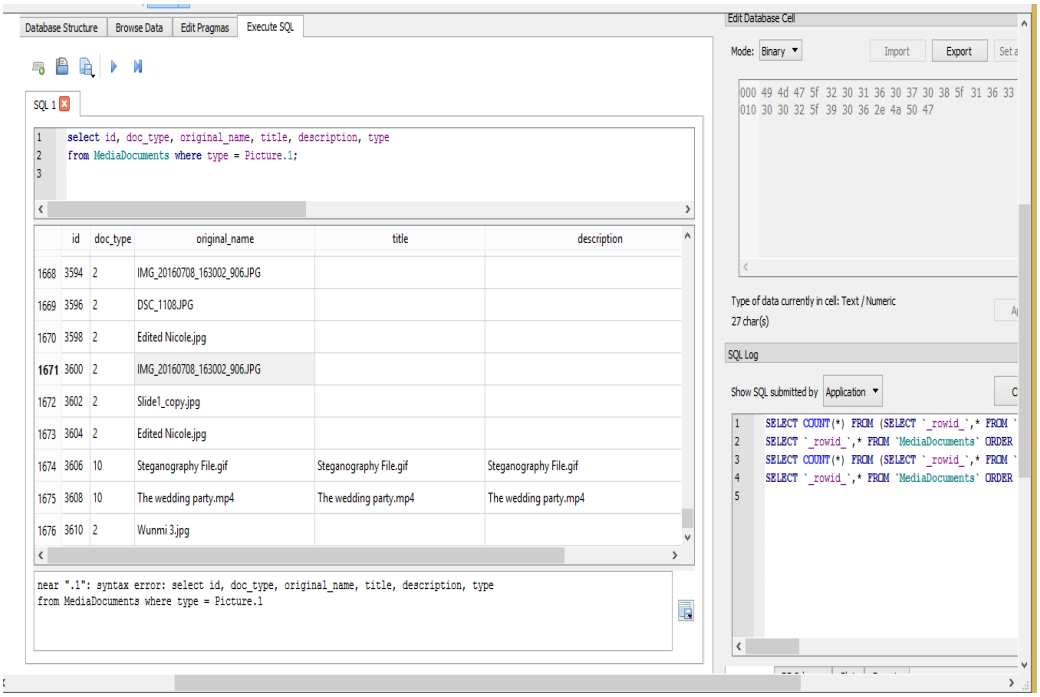

Fig 6: Shared Multi-Media File Records 2

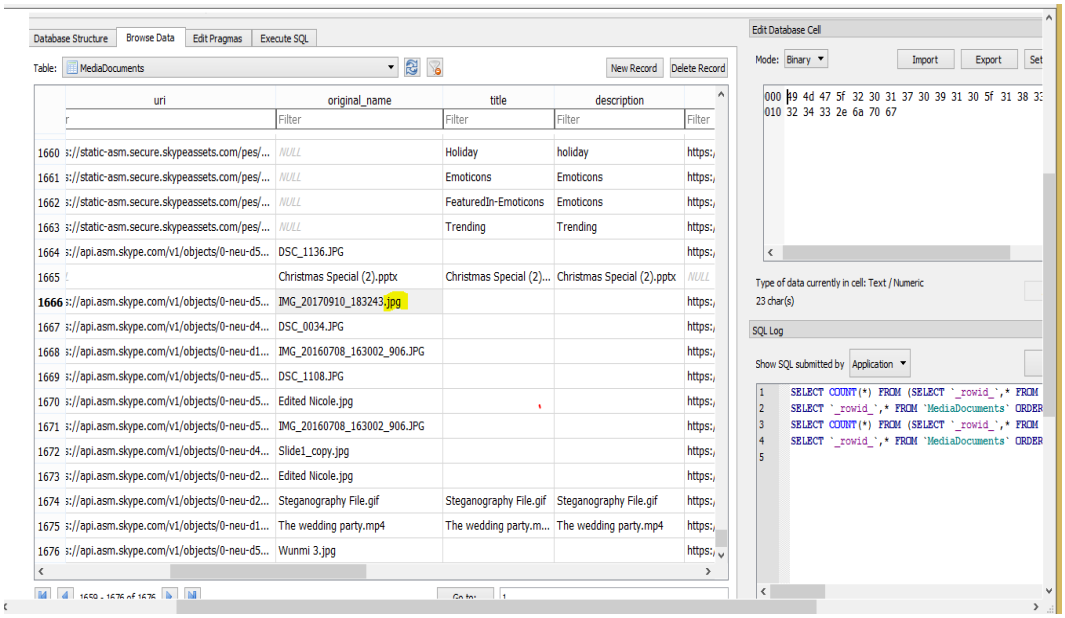

Fig 7: Shared Multi-Media File Records 3

4. CONCLUSION AND RECOMMENDATION

In view of the information security vulnerabilities generally attributable to social networking platforms and applications, in this study, the digital artifacts that are associated with the Skype application have been identified. As described in section III, a number of potential cyber-criminal activities can be` perpetuated using the data anyone can harvest from the records of Skype users stored within the internal storage of the computing device. One key finding of the acquired and examined records indicates that user data and other metadata information are stored in plain and clear text format. The security implication for this is significant as the ease or potential for a cyber-criminal activity becomes heightened.Therefore, the implementation of a robust and secure data encryption standard for protecting stored user records is recommended. While there are different types of encryption algorithms that may be utilized for achieving user security and privacy requirements, the decision to enforce any of the known standards can be taken following global application security standards for implementing security of software applications.

5. REFERENCES

[1] Al Muttawa, 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.

[2] A. Mahajan, M. Dahiya, and H. Sanghvi, “Forensic Analysis of Instant Messenger Applications on Android Devices,” International Journal of Computer Applications, vol. 68, no. 8, pp. 38–44, 2013

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

[4] C. Carpene, “Looking to iPhone backup files for evidence extraction,” in Proceedings of the 9th Australian Digital Forensics Conference, 2011, pp. 16–32.

[5] H. Chu, S. Yang, S. Wang, and J. Park, “The Partial Digital Evidence Disclosure in Respect to the Instant Messaging Embedded in Viber Application Regarding an Android Smart Phone,” in Proceedings of the 4th FTRA International Conference on Information Technology Convergence and Services (ITCS-12), 2012, pp. 171–178.

[6] M. Kiley, S. Dankner, and M. Rogers, “Forensic Analysis of Volatile Instant Messaging,” in in Advances in Digital Forensics IV, vol. 285, 2008, pp. 129–138.

[7] The Register, “Italian crooks use Skype to frustrate wiretaps,” 2009.

[8] Europol, “Threat Assessment - Italian organised crime,” 2013.