

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-toend 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 Da	ata
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;
- Sign-up and sign-in to the applications on the rooted device;
- 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)

abase Structure Browse Data Edit Prag	mas Execute SQL		Eart Database Cell
Create Table 🛛 🗞 Create Index Modify	Table 🔛 Delete Ta	ble	Mode: Text Import Export S
ne	Туре	Schema ^	
4 Contacts		CREATE TABLE Contacts (id INTEGER NOT NULL PRIMARY KEY, is_permanent INTEGER, type	
💫 id	INTEGER	"id' INTEGER NOT NULL	
is_permanent	INTEGER	ïs_permanent' INTEGER	
L type	INTEGER	'type' INTEGER	
skypename	TEXT	'skypename' TEXT	
pstnnumber	TEXT	'pstnnumber' TEXT	
aliases	TEXT	'aliases' TEXT	
fullname	TEXT	'fullname' TEXT	
birthday	INTEGER	'birthday' INTEGER	
gender	INTEGER	'gender' INTEGER	
Ianguages	TEXT	'languages' TEXT	Type of data currently in cell: NULL
country	TEXT	`country` TEXT	0 byte(s)
province	TEXT	'province' TEXT	601 Jan
city	TEXT	'city' TEXT	SQL LOG
phone_home	TEXT	'phone_home' TEXT	Show SQL submitted by Liser
phone_office	TEXT	'phone_office' TEXT	
phone_mobile	TEXT	phone_mobile`TEXT	1 select * from Contacts
emails	TEXT	'emails' TEXT	2
hashed_emails	TEXT	'hashed_emails' TEXT	
homepage	TEXT	'homepage' TEXT	
📄 about	TEXT	'about' TEXT	
avatar_image	BLOB	`avatar_image` BLOB	
mood_text	TEXT	'mood_text' TEXT	
📄 rich_mood_text	TEXT	'rich_mood_text' TEXT	
timezone	INTEGER	'timezone' INTEGER	
capabilities	BLOB	`capabilities` BLOB	
profile_timestamp	INTEGER	'profile_timestamp' INTEGER	
nrof authed buddies	INTEGER	'prof. authed. buddies' INTEGER	

Fig 1: Application Database Table Structure – Contacts Table

ata	base Structure	Browse Data Edit	Pragmas Exe	cute SQL						Edit Database Ce			
sle	: Contacts				- 💈 😼]		New Record	Delete Record	Mode: Text	•	Import	Ex
	id	is_permanent	type	skypename	pstnnumber	aliases	fullname	birthday	ge ^				
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter				
	33	1	1	echo123	NULL	NULL	Echo / Sound	NULL	NULL				
	37	1	1	ydwest	NULL	NULL	Olayinka Davi	NULL	2				
	41	1	1	tejumann	NULL	NULL	Tejumola Mann	19830531	1				
	45	1	1	venessaireze	NULL	NULL	NULL	NULL	2				
	49	1	1	omowumi.ehi	NULL	NULL	omowumi ehi	19821017	2				
	53	1	1	unmiangel123	NULL	NULL	Omowunmi E	NULL	NULL	Toron of data and	and the set of the set		
	57	1	1	lady_nikki1333	NULL	NULL	NULL	NULL	NULL	0 byte(s)	rently in cell: NULL		
	61	1	1	sehiwe	NULL	NULL	simeon ehiwe	19760726	1	Pamota			
	65	1	1	olawande1	NULL	NULL	NULL	NULL	1	recinote.	-1.02		
	69	1	1	live:okonkwoi	NULL	NULL	IKEM OKONKWO	19920503	1	Identity	•		
	73	1	1	mercy.ehiwe	NULL	NULL	NULL	NULL	NULL	Name	Commit	Last modifi	ied
	77	1	1	henry.megwai	NULL	NULL	Megwai Henry	19010420	1				
	81	1	1	oluwadotiano	NULL	NULL	NULL	NULL	NULL				
	85	1	1	peters.ehiwe	NULL	NULL	Peters Ehiwe	19781118	1				
	89	1	1	moses.ehiwe1	NULL	NULL	moses ehiwe	19650216	1				
	93	1	1	phemson2005	NULL	NULL	Olufemi ADEA	NULL	1				
	97	1	1	chioma.ikpa1	NULL	NULL	NULL	NULL	NULL				
									>				

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)

Database Structure Bro	vse Data Edit Pragmas	Execute SQL		Edit Database Cell
🐻 Create Table 🛛 💊 Cre	ate Index Modify Table	Delete Ta	ble	Mode: Text Import
Name		Туре	Schema ^	
4 🔠 Messages			CREATE TABLE Messages (id INTEGER NOT NULL PRIMARY KEY, is_permanent INTEGER, col	
💫 id		INTEGER	'id' INTEGER NOT NULL	
📄 is_permane	nt	INTEGER	'is_permanent' INTEGER	
convo_id		INTEGER	`convo_id` INTEGER	
📄 chatname		TEXT	'chatname' TEXT	
author		TEXT	'author' TEXT	
📄 from_dispn	ame	TEXT	'from_dispname' TEXT	
author_was	live	INTEGER	'author_was_live' INTEGER	
📄 guid		BLOB	"guid" BLOB	
📄 dialog_part	ner	TEXT	'dialog_partner' TEXT	Tupo of data ourseath, is call, NUL
📄 timestamp		INTEGER	'timestamp' INTEGER	Type of data currently in cell. Note
type		INTEGER	'type' INTEGER	0 byte(s)
sending_sta	itus	INTEGER	`sending_status` INTEGER	SOL Log
option_bits		INTEGER	'option_bits' INTEGER	
📄 consumptio	on_status	INTEGER	`consumption_status` INTEGER	Show SQL submitted by User
edited_by		TEXT	`edited_by` TEXT	
edited_time	stamp	INTEGER	'edited_timestamp' INTEGER	1 select * from Contacts
📄 param_key		INTEGER	'param_key' INTEGER	2
📄 param_valu	e	INTEGER	'param_value' INTEGER	
body_xml		TEXT	'body_xml' TEXT	
identities		TEXT	"identities" TEXT	
📄 reason		TEXT	'reason' TEXT	
leavereasor		INTEGER	'leavereason' INTEGER	
participant,	count	INTEGER	`participant_count` INTEGER	
error_code		INTEGER	'error_code' INTEGER	
lend the chatmsg_ty	pe	INTEGER	`chatmsg_type` INTEGER	
📄 chatmsg_st	atus	INTEGER	`chatmsg_status` INTEGER	
body_is_rav	vxml	INTEGER	'body_is_rawxml' INTEGER	1

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.
-----------	------	--------

Filtered Records fr SELECT id, chatname, gui FROM Messages order by t	<pre>com the List of Messages Shared on Skype .d, body_xml, chatmsg_type, chatmsg_status imestamp_ms desc;</pre>	, crc, timest	tampms			^				
					2					
guid	body_xml	chatmsg_type	chatmsg_status	crc	timestamp_ms	^				
00 ⁹ 9 0{000000 2]X>	let me leave u now	3	2	512470850	1447616724000		Type of data currently in c	al- NUL		
01 > &&&& && ¶X &&&& \$	you are always welcome sir	3	4	516350821	1447616722000		0 byte(s)	EI: NULL		
l2 J++Yb ⊕ nu ⊕⊕∔⊕ %J5sw ⊕ yW ⊕	thanks alot	3	2	2321866564	1447616705000		Remote			
3 0 !!}{ 0001.000	okay.	3	2	1983611920	1447616700000		Identity 🔻			
04	i'Il have the files with me by then	3	4	1528361683	1447616694000		Name Con	∝. nmit	Last modified	Size
os ♦ ♦ ¢ ¢ و s₁ < ♦ Jdx ♦ L♦ ^L *Z♦	okay then	3	4	776350685	1447616680000					
06 k��g�TFZa�6b� i�;D�M•�i	l don't have them on my personal laptop	3	4	127973331	1447616676000					
07 00-m*00 ⊤g 0/0-*0000	the reason is that the associated files i'II be ta	3	4	2530987018	1447616662000					
08 ••+3•**	2mr nite. say about 10	3	2	4238378965	1447616661000	~				
40 rows returned in 4ms from rom Messages order by timest	: select id, chatname, guid, body_xml, cha amp_ms desc;	atmsg_type, c	hatmsg_status,	crc, tim	stamp_ms					

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.



ble: 🔲 Ti	ransfers		- 🔁 🔀	New Reco	rd Delete Record	induct fext
arttime	finishtime	filepath	filename	filesize	bytestransferred	1065
	Filter	Filter	Filter	Filter	Filter	
87055	1449387132	C:\Users\Dominic\AppData\Roaming\Skype\	MODULE and lecturers.docx	11124	11124	
87055	1449387156	C:\Users\Dominic\AppData\Roaming\Skype\	L7 ATHE 1st SEMESTER MBA.docx	346417	346417	
87055	1449387156	C:\Users\Dominic\AppData\Roaming\Skype\	L7 ATHE 2ND SEMESTER MBA.docx	347109	347109	
04142	1458504239	G:\Flash 1\Metropolitan - RIT Module\Web	Web Analytics for Security Informatics.pdf	290329	0	
04161	1458504239	G:\Flash 1\Metropolitan - RIT Module\Web	Web Analytics for Security Informatics.pdf	290329	290329	
04194	1458504244	C:\Users\Dominic\Desktop\Ph.D Work\Dehiw	Main memory Databases for Enterprise Ap	146639	0	
04199	1458504244	C:\Users\Dominic\Desktop\Ph.D Work\Dehiw	Main memory Databases for Enterprise Ap	146639	146639	l ype of data currently in cell: Text / Numeric 4 char(s)
36412	0	C:\Users\Dominic\Desktop\Reflection Essay	Reflection Essay Examples.pdf	38741	0	
						Show SQL submitted by User I

Fig 5: Shared Multi-Media File Records 1

tahase	Structu	re Brou	wse Data Edit Pragmas Execute SC	1		Edit Database Cell	
SQL 1 1 2 3	sele from	ct id, d	N oc_type, original_name, title comments where type = Picture.	, description, type		Mode: Binary ▼ Import Export 000 49 47 5f 32 30 31 36 30 37 30 38 5f 31 36 30 37 30 38 5f 31 30 30 32 5f 39 30 36 2e 4a 50 47	Set a
۲	14	de e terre	a first serve	cu.	description	<u> </u>	
1000	10	aoc_type		title	description		
1008	3,594	2	DEC 1100 DC			Type of data currently in cell: Text / Numeric	
1009	2200	2	DSC_1106JPG			27 char(s)	A
16/0	3098	2	Edited Nicole.jpg			SQLLog	
1671	3600	2	IMG_20160708_163002_906.JPG			Show SOI submitted by	0
1672	3602	2	Slide1_copy.jpg			1 SELECT OFFICE (SELECT ' you'd ' * F	
1673	3604	2	Edited Nicole.jpg			2 SELECT `_rowid_`,* FROM `MediaDocuments` O	RDER
1674	3606	10	Steganography File.gif	Steganography File.gif	Steganography File.gif	3 SELECT COUNT(*) FROM (SELECT `_rowid_`,* F 4 SELECT ` rowid `,* FROM `MediaDocuments` O	RDER
1675	3608	10	The wedding party.mp4	The wedding party.mp4	The wedding party.mp4	5	
1676	3610	2	Wunmi 3.jpg			v	
< near from	".1": Media	: syntax aDocument	error: select id, doc_type, o ts where type = Picture.1	briginal_name, title, descripti	on, type		

Fig 6: Shared Multi-Media File Records 2



able:	MediaDocuments	- 🕄 🏹		New Record D	elete Record	Mode: Binary Import Export
	uri	original_name	title	description	^	000 #9 4d 47 5f 32 30 31 37 30 39 31 30 5f 31 3
	r	Filter	Filter	Filter	Filter	010 32 34 33 2e 6a 70 67
660	s://static-asm.secure.skypeassets.com/pes/	NULL	Holiday	holiday	https:/	
661	s://static-asm.secure.skypeassets.com/pes/	NULL	Emoticons	Emoticons	https:/	
662	s://static-asm.secure.skypeassets.com/pes/	NULL	FeaturedIn-Emoticons	Emoticons	https:/	
663	s://static-asm.secure.skypeassets.com/pes/	NULL	Trending	Trending	https:/	
664	s://api.asm.skype.com/v1/objects/0-neu-d5	DSC_1136.JPG			https:/	<
665	-	Christmas Special (2).pptx	Christmas Special (2)	Christmas Special (2).pptx	NULL	Type of data currently in cell: Text / Numeric
666	s://api.asm.skype.com/v1/objects/0-neu-d5	IMG_20170910_183243 <mark>.jpg</mark>			https:/	23 char(s)
667	s://api.asm.skype.com/v1/objects/0-neu-d4	DSC_0034.JPG			https:/	SQL Log
668	:://api.asm.skype.com/v1/objects/0-neu-d1	IMG_20160708_163002_906.JPG			https:/	Show SOL submitted by Application 💌
669	s://api.asm.skype.com/v1/objects/0-neu-d5	DSC_1108.JPG			https:/	1 SPLECT COUNT(\$) FORM (SPLECT) resid) \$
670	s://api.asm.skype.com/v1/objects/0-neu-d5	Edited Nicole.jpg			https:/	2 SELECT '_rowid_',* FROM 'MediaDocuments'
671	:://api.asm.skype.com/v1/objects/0-neu-d5	IMG_20160708_163002_906.JPG			https:/	3 SELECT COUNT(*) FROM (SELECT `_rowid_`,* 4 SELECT `_rowid_` * FROM `MediaDocumenta`
672	:://api.asm.skype.com/v1/objects/0-neu-d4	Slide1_copy.jpg			https:/	5
673	3://api.asm.skype.com/v1/objects/0-neu-d2	Edited Nicole.jpg			https:/	
674	s://api.asm.skype.com/v1/objects/0-neu-d2	Steganography File.gif	Steganography File.gif	Steganography File.gif	https:/	
675	s://api.asm.skype.com/v1/objects/0-neu-d1	The wedding party.mp4	The wedding party.m	The wedding party.mp4	https:/	
676	s://api.asm.skype.com/v1/objects/0-neu-d5	Wunmi 3.jpg			https:/v	

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

 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.