ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

Forensic Examination On Windows And Android Devices To Acquire Skype Artefacts

Anjana.R
M.Tech in Computer Science with Specialization in Cyber Forensics and Information Security
ER&DCIIT, Trivandrum, Kerala, India anjanar1992@gmail.com

Abstract -- **Skype is one of the most popular VoIP application that specializes in providing video chat and voice calls from computers, tablets, and mobile devices via the Internet to other devices or telephones/smartphones. The method by which Skype transmits data over the internet and between clients has been frequently examined, to discover any potential data leaks. An area that has not received much attention is that of the local data stored on systems by Skype. This paper describes a forensic examination on Windows and Android devices and the acquisition of Skype related artecfacts. The study aims to recover information from user account, calls, messages, contacts, group chats, file transfers, voice mail, SMS etc.**

1. INTRODUCTION

Skype is a telecommunications application software product that specializes in providing video chat and voice calls from computers, tablets, and mobile devices via the Internet to other devices or telephones/smartphones. Users can also send instant messages, exchange files and images, send video messages, and create conference calls. Questions regarding the security of data sent and received between Skype clients are not uncommon, with a number of investigations being carried out to see what sort of data can be intercepted whilst it is being sent over a network. Although this is quite a popular area of investigation, much less research has been done into data stored locally on systems running the Skype client. Owing to the secrecy surrounding the network protocols used by Skype, and due to the encryption methods used both whilst transmitting data over a network and storing it on local systems, it is very difficult to intercept and utilise Skype data whilst it is being transmitted, or to even read some data stored locally on Skype-enabled computer systems.

There are multiple reasons why this investigation is being conducted, the first of which is purely down to curiosity as to what sort of information Skype records, stores and uses. If we then consider the information that Skype is privy to – such as the information required to create an account, which includes our email address, forename, surname and date of birth – it can be quite concerning to think that this personal information could be stored in an insecure manner. Although this is likely to be stored on Skype's secure servers, it is also possible that some of this data may be used by the Skype local client, which may mean that the data is stored locally on the user's computer, in a directory created by Skype. Although this may not seem like an issue to the majority of people, it is likely to be much easier for an unscrupulous individual to gain access to someone's personal computer and take this information from there, rather than accessing Skype's servers, especially if the locally stored information is stored in plaintext and not encrypted or hidden in any way.

The results of this investigation may be used for three key reasons. Firstly, the information found will be used to assist in the development of a software tool that will automatically gather any useful artefacts left behind by Skype on local systems. This could then be used to aid in the investigation of hard drives that may have been seized by authorities, from someone accused of committing some form of illegal activity.

2. RELATED WORKS

Mohammed I. Al-Saleh in his paper "Skype Forensics in Android Devices"[1], investigates the artefacts of Skype calls and chats in the Android devices. This paper inspects both the RAM and NAND flash memories in different scenarios and time durations. Even though Skype provides secure communications over the Internet, this paper shows that Skype call and chat evidences can be truly found in the devices. It aim at showing that Skype artefacts in the Android

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

systems can be utilized in digital forensics. It shows the searching of the dumps of both of the RAM and NAND flash memories for the artefacts of Skype calls and chats.

Igor Mikhaylov in the article, "Extracting Evidence from Destroyed Skype Logs and Cleared SQLite Databases", describes common approaches used for the recovery of cleared Skype histories and deleted chat logs, and discusses methods and techniques for recovering evidence from cleared and damaged SQLite databases. This article represents methods and techniques used by forensic specialists to handle evidence contained in cleared Skype histories and deleted SQLite databases, particularly those located on formatted or repartitioned hard drives or discovered in the computer's volatile memory.

Dodge addresses the topic of locally stored Skype data in his paper "Skype Fingerprint" but, although the findings are detailed, this investigation was carried out before Microsoft acquired Skype in 2011[7].

Microsoft's acquisition of Skype brought along a myriad of changes to the Skype client, including the method by which Skype stores data locally on computer systems. Much like this paper, Dodge's paper focuses on; "an analysis of the information that can be gleaned from a Skype installation and use on a client system." (Dodge, 2008). All in all, Dodge's paper does a good job of detailing the discoveries he made and the processes by which he made these discoveries. Despite the fact that some of the results in this paper are relatively irrelevant in the current version of Skype (such as files that no longer exist), the locations in which a lot of his results appeared are still the same today, so these locations may still be a useful source of information. The only issue to be raised, is the method by which Dodge manufactures the Skype clients he examines.

3. EXAMINATION ON WINDOWS DEVICES

With Windows being the most popular operating system in use today, the primary operating system examined within this investigation will be a recent version of Windows. Also, Microsoft owning Skype added to the appeal of using Windows as the primary operating system for this investigation.

The first step of the examination on Windows was to search through the most common areas in which Windows stores application data. Firstly, the Program Files and Program Files (x86) folders were examined in an attempt to locate the Skype install files. Once located, within C:\Program Files (x86)\Skype, these files were examined for any potentially useful data[7]. Although a large number of programs store the majority of their application data within their Program Files folders, in the case of Skype, the files contained within this directory were used purely for the execution of the Skype application. The only files within this location were ―desktop.ini‖, which points to the icon file that should be used by the desktop shortcut, and a simple text file entitled ―third-party_attributions which provides copyright information for certain elements within Skype.

The files contained within the subdirectories were the executable file for the Skype update program and the Skype application itself, along with an archive entitled ―login, which contains data such as emoticon images and different languages that can be used by the application. As the data stored within "*Program Files*" did not prove useful, the next location to be examined was the "AppData" folder, stored within Windows user directories. In this particular case, the full folder path was "*C:\Users\Daniel\AppData*". Once in the AppData folder, the subdirectories of "*Local*", "*LocalLow*" and "*Roaming*" were to be examined for any Skype data. There was a Skype directory found within "*Local*" and "*Roaming*". The directory within "*Local*" simply contains a subdirectory entitled "*Apps*". Within this directory, is another, entitled "*login*", along with an .md5 file, also entitled "*login*". The "*login*" directory seems to contain the data extracted from the "*login*" archive found previously. The .md5 file simply contains the md5 hash value (or the ―fingerprint) for the original archive. The Skype data stored within the "*Roaming*" directory is by far the most important. Within this directory there are a number of subdirectories, along with three individual files. The majority of the subdirectories, along with the individual files, do not seem to hold much in the way of useful information. The one useful directory here is the one that uses a Skype username as the title.

Within the Skype user directory, there are a myriad of subdirectories and individual files. The first directory of interest was the "*chatsync*" folder. Within this folder, there appears a varying number of folders, each with a two character long name, that seems to be a mix of letters and numbers. Although some of these directories contain no data, the ones that do contain information are extremely useful. By opening the .dat files found within these folders in Notepad++ we can see encoded data. But while properly analysing these files we can see plaintext in places between the encoded data. This plaintext data seems to consist of the conversation history between

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

any users that were part of a Skype call or instant messaging session at that particular time.

Browsing through the remaining directories within the Skype user folder does not present any useful data as the majority of the directories were either empty, or the files that were found tended to be encoded.

The "*config.xml*" file also contains a list of all video input devices connected to the system, along with any audio input/output devices connected. This list not only shows that there are devices present, but also gives the make and model of each device, provided that that information is available to the system itself. The devices listed here do not always have to be physical. The final file found that contains useful information is by far the most useful. The "*main.db*" file, found within the Skype user folder, is a SQLite database file and thus must be opened within a SQLite database editor to be viewed[3]. In this investigation, the tool used was ―SQLite Browser. Within this database file, an extensive amount of data is stored. Although a number of sections of the database do not hold much useful data, others hold plenty.

The first section containing detailed information is the "*Videos*" table. Within this table, there is a record of each time a video stream was initiated. Not only does this file identify when a video stream was initiated, it also identifies a device ID for the device used, and if the video session was a video conversation or a screen sharing session. In the cases where it was a screen sharing session, the dimensions of the screen shared is also recorded, although this is only the case when the user being examined has broadcast their screen, rather than viewing another user's screen. The next useful table is that of the "*CallMembers*" table. Within this table, a record is kept of each of the calls the user has been a part of, along with the username and display name of the users with whom the call was initiated. Skype also keeps a record of the duration of the call, but the timeframe used is not specified. The logical assumption for the timeframe would be that of seconds, but this cannot be guaranteed. Finally, the "*CallMembers*" table also keeps a record of the IP address of the other participants of the recorded conversations. The *"Conversations"* table contains similar information to that already seen in previous tables, but it also has the added record of the username and display name of anyone that the current user has been in conversations with, even if they are not on one another's contact lists. The "*VideoMessages*" table is only populated if a video message is recorded and sent to someone using the built in Skype function. If a video has been sent from the account being examined, there is no record of the user to whom it was sent, just a confirmation that it was sent from the user account in question. If a video has been received, the username for the user that sent the video is displayed. Within this table, there are two sections that are most important, the first of which is "*vod_path*". Within this column, a URL is stored that, when copied into a web browser, displays an online version of the video sent or received. Although this is useful, testing showed that this link is only valid for around 24 hours, after which it is no longer available. The other useful column is "*local_path*" which, as the name suggests, provides the local path for any video messages sent from the computer being examined. The "*Contacts*" table presents a list of all the contacts within the current user's address book. The table presents both the display name and Skype username for each user. The majority of the rest of the information displayed here is dependent on the information that each user has entered into their Skype account details. If it has been entered, the data recorded in here includes each user's birth date, gender, spoken language, country, province, city, home telephone number, mobile telephone number and a link to any associated websites. Although the majority of this information is viewable on the user in question's profile, it is only viewable by people that have been approved by the user. If an unscrupulous individual were able to gain access to all of the above information, the potential consequences could be disastrous for the target individual. The "*Calls*" table displays a history of calls that the current user has been involved in. The list keeps a record of the identity of the user hosting the call, as well as other users involved with that particular call. Another potentially useful table is the "*Transfers*" table. As the name suggests, this table keeps a record of every file transfer made between users, including a record of who the sending/receiving party was, the local file path for where the document was sent from or saved to, and the name of the file that was sent or received. Finally, the "*Messages*" table contains a record of the majority of messages sent and received via the Skype instant messaging function, along with the users who were involved with each message. Although the messages are stored individually rather than in conversations, the majority of them are easy to read and to follow on from.

4. EXAMINATION OF ANDROID DEVICES

The first Android device to be examined was the Samsung Galaxy S3, with full "root" permissions. The first stage of this examination was to simply use a file explorer application freely available on the Google Play Store. In this case, the application used was "ES File Explorer". Upon opening the application navigating to

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

the root directory, or "/", shows the directory structure used by Android. By simply browsing through the first few directories, a number of files are encountered that are key for the functioning of Android, empty folders and configuration files.

Upon entering the "data" directory, a number of directories are located with the word "app" in the title, hinting that these folders may contain application data. This suspicion is confirmed by entering the very first folder, simply entitled "app". Within this folder, are the .apk files (installation files) for all user-installed applications on the device, including the installation package for Skype, entitled com.skype.raider-1.apk (the full application package name). At this point, the device was connected to a Windows computer system so that the Skype installation package could be extracted for investigation. Using the Android Debug

Bridge application, the "adb pull" command was utilised to make an exact copy of the Skype application package file. The full command used was; adb pull /data/app/com.skype.raider-1.apk[4]. Once the file had been copied, the aim was to examine the files contained within the package to identify something that defined where the Skype data would be stored. By utilising the program 7zip's ―extract archive feature, access was gained to a number of different files from within the original .apk file[8]. A lot of these files were image files of emoticons and other images that users can send whilst using Skype. The file that was most intriguing was the "AndroidManifest.xml" file stored in the root area of the file, as the name of the file gave the impression that this would be where a large number of the core settings would be declared, for use by the Android operating system. Upon opening this file in Notepad++, a relatively large amount of text is displayed, but the majority of it appears to be either encrypted or corrupt making the majority of the data available relatively useless as the majority of it is unreadable.

Utilising APKTool, the *com.skype.raider-1.apk* file was fully decompiled. Although this seemed to produce less files than when they were extracted using 7zip, the missing files did not seem to have much relevance, as they appear to be files generated at compilation of the .apk file. Once decompiled, the AndroidManifest.xml file was once again opened in Notepad++. This time round, all of the data was in plaintext and organised correctly. By searching through the multitude of folders for the Skype package (*com.skype.raider*, as defined by the title of the .apk file located earlier), data stored and utilised by the Skype application can be found. At first glance, the directory structure for the Skype application files on Android looks different to that of the directory structure found during the Windows examination. This impression is given by the first set of directories presented when accessing the *com.skype.raider* directory. The directories displayed are "*app_webview"*, *"cache"*, *"files"*, *"lib"* and "*shared_prefs"*. Although the majority of these folders store encoded data, the "*files*" directory brings up a set of files and directories similar to that found on a Windows system running Skype. Although not all the directories found on the Windows version of Skype can be found on the Android version, the one that contained the most useful artefacts was still present.

5. CONCLUSION

Owing to the secrecy surrounding the network protocols used by Skype, and due to the encryption methods used both whilst transmitting data over a network and storing it on local systems, it is very difficult to intercept and utilise Skype data whilst it is being transmitted, or to even read some data stored
locally on Skype-enabled computer systems. The main aim of this paper is to demonstrate the examination of Windows and Android Devices for Skype related artefacts. The system is examined to recover information from user account, calls, messages, contacts, group chats, file transfers, voice mail, SMS etc.

6. REFERENCES

1. Mohammed I. Al-Saleh, "Skype Forensics in Android Devices",2013
2. Anderson, B. (2013). Android News for Costa Rica, *Understanding the Android File Hierarchy* - http://www.all-things-android.com/content/understandingandroid-file-hierarchy
3. Creutzburg, R. Kröger, K. Meißner, T. (2013). *Client-side Skype Forensics – An Overview.*
4. Android. (Unknown A). Android Developers, *Android Debug Bridge*.-http://developer.android.com/tools/help/adb.html
5. Anon. (2010). Skype IT Administrators Guide, *Skype for Windows version 4.2*. [Online]. Available at: http://download.skype.com/share/business/g uides/skype-it-administratorsguide.pdf
6. Matthew Simon and Jill Slay, "What are you looking for: Identification of Remnant Communication Artefacts in Physical
Memory", 2010
7. Dodge, R C. (2008). *Skype Fingerprint*, 1

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

(1) pp. 1-6 IEEE Xplore [Online]. Available at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?

8. Tumbleson, C. (Unknown). Android-APKTool, *Project Home*. Available at: https://code.google.com/p/android-apktool/