Skype Analyzer

By: Matt Anderson, Wesly Delva, & Stacey Francoeur

Forensics Tool Project

May 3, 2013

Table of Contents

Executive Summary

Skype Analyzer is a useful forensics tool when it comes to analyzing Skype account information. It is an open source, easy-to-use Perl script that queries the database where Skype keeps its data for the plaintext information an investigator may want. This information can include a list of contacts of the Skype user and all the messages they have sent and received as well as the timestamps. As this tool is open source, the forensics community is welcome to modify the source code in order to add functionality and improve the tool.

Current Condition Overview

Many people currently use the program Skype to message their friends, video chat with them, or even transfer files. Skype also requires a username (or “skypename”) and password to log in and use. If an investigator images a suspect machine and finds that Skype was installed while analyzing that image, then they may want to view the chat messages between the suspect and his/her contacts because these messages may be used as evidence against or in favor of the suspect.

Since Skype is password protected, the investigator may not be able to get in without the cooperation of the suspect who may not be very accommodating. A simple Google search will tell the investigator that the Skype history is kept in a database called “main.db” located in the Skype directory for that user. Unfortunately, this file contains a lot of gibberish when viewing it in plaintext. This is where the need arises for tools to analyze the history. There are a few downloadable tools that already exist but we didn’t like the way they functioned.

Tool Selection

Currently, the forensics community contains a few tools that can be used to analyze Skype history on a system. However, these tools are all graphical user interfaces (GUIs) and one of them even installed malware-esque things (such as browser toolbar & changed homepage) on one of our systems. These tools are also typically made to run solely on Windows machines. We wanted to make a tool that would function similarly but while using a command-line interface and being able to run on multiple platforms.

Tool Development

We decided to make a Perl script to read and analyze the information contained in the database. In order to use it, only a couple things need to be installed on the system: Perl and the Perl module Database Interface Module (DBI). Currently, the script is set to run on Windows 7 or higher but we plan to make it work on Apple and Linux platforms as well.

Interesting Issues

The biggest issue we ran into while creating this script was we had to figure out the structure of the database, main.db. We needed to figure out what variables are stored where and how it was set up in order to create the correct queries. We were able to do this by using SQLite version 3 which can allow you to create, write, and access SQLite databases. Another issue we had was that not all of us were familiar with SQLite syntax so we had to allot time in order to become familiar enough to use it with our script.

Conclusion

Skype Analyzer has basic functionality as of right now. We plan on adding more functionality to it over time and as I've stated before, we plan to alter it in order to make it run on multi platforms. The three of us enjoyed working on this tool and learned more than we knew when starting it. If you're looking for a good, command-line tool to analyze your Skype history, Skype Analyzer is the right choice. Skype Analyzer can be found at http://code.google.com/p/skype-analyzer/.

References

SQLite. “SQLite.” Web. 1 May 2013.
<http://www.sqlite.org/index.html>.

ZetCode. “SQLite Perl Tutorial.” 1 May 2013.
<http://zetcode.com/db/sqliteperltutorial/>.

Pants.org. “SQLite Commands and General Usage.” 1 May 2013.
<http://www.pantz.org/software/sqlite/sqlite_commands_and_general_usage.html>.

NirSoft. “Skype Logs Reader/Viewer.” 14 April 2013.
<http://www.nirsoft.net/utils/skype_log_view.html>.

Google Code. “Skype Log Viewer.” 14 April 2013.
<http://code.google.com/p/skype-log-viewer/>.