Examination Report

Case Information

Case Number	**01**
Examiner Name	**Ivan Ng** **Jun Hang**
Description	**In-class forensic investigation**

Name	Acquisition SHA1	Verification SHA1	Evidence Number	Examiner Name
Alicia	132a9f27dc3a02f90d64f50b12b797c16f74089b	132a9f27dc3a02f90d64f50b12b797c16f74089b	E02HD1	Thomas Chee

Name	Alicia
GUID	1e11d3d1dca5f4c6a9f08c902e24886c
Index File	C:\Users\DF Student P04\Cases\prac2\EvidenceCache\1E11D3D1DCA5F4C6A9F08C902E24886C\DeviceIndex.L01
Actual Date	16/03/17 10:50:29 AM
Target Date	16/03/17 10:50:30 AM
File Integrity	Completely Verified, 0 Errors
Acquisition SHA1	132a9f27dc3a02f90d64f50b12b797c16f74089b
Verification SHA1	132a9f27dc3a02f90d64f50b12b797c16f74089b
EnCase Version	7.10
Error Granularity	64
Read Errors	1
Missing Sectors	0
CRC Errors	0
Compression	Best
Examiner Name	Thomas Chee
Notes	Acquired from Alicia Tan Hui Jing's computer at Simon Spegman's apartment
Serial Number	Z3TNNKM4_206848
Model	ST500DM002-1BD142
Drive Type	Fixed
System Version	Windows 8.1
Total Sectors	83,886,079

Contents

Abstract

This report presents the forensic examination procedures, findings, and recommendations concerning a simulated financial dispute involving Alicia and Simon. Included in the report are the digital forensic standards, principles, methods, and legal issues that may impact the court's decision.

This report follows digital forensic best practices and methodologies to ensure the integrity, confidentiality, and admissibility of evidence. It provides an unbiased technical evaluation of the digital artifacts recovered from Alicia's system, assessing whether any evidence supports or refutes the claims made by either party. Additionally, it considers the potential legal implications and evidentiary value of the findings. The conclusions drawn from this examination will assist in determining the credibility of the allegations and contribute to the resolution of this case.

Case Background

Simon recently reported an unauthorized bank transfer of SGD $2000 in his OCBC bank account history and reported it to the police. The recipient of the transaction was traced to the tenant of his apartment, Alicia.

When interrogating Alicia, she consistently denied any wrongdoings and claimed that Simon has transferred the money on his own accord. She mentioned that Simon had been sexually harassing her in the apartment, and the money was transferred as hush money to keep her quiet. She gave a possibility that Simon might be trying to frame her to get his money back and avoid any criminal indications if she reported the sexual harassment to the police. According to the bank's online banking logs, the transaction was made from Simon's apartment's public IP address. Hence, both Simon and Alicia's personal computers in the apartment have since been seized for investigation.

Examination Summary

The tools used for the examination includes Autopsy (v7.10), a digital open source platform for forensic investigations and SQLite, a software library that allows storage of structured data, such as text or numbers, in a database file on the computer's hard drive. The tools highlighted are used due to their standards and acceptance within the forensic community.

Autopsy was used in this examination to extract and recover information such as emails, images, videos, message logs and suspicious strings. Additionally, Autopsy was used to uncover system information and registry files including CHS information and CRC errors. SQLite on the other hand was used to process .db files of user message logs within the system.

Important data presented within the system such as message logs and emails sent and received were extracted from the suspect's devices. Renamed files with changed extensions were checked for the possibility of hidden information. Data that was deleted was also inspected.

Unimportant data such as program files used by operating systems were ignored in the process of this forensic investigation.

Any relevant information regarding findings may be referenced in the glossary below.

Relevant Findings

This section of Relevant Findings gives a summary of evidence found of probative Value.

File system examination

This section covers all files and directories within the forensic image that may be of interest

history

Item Path	Alicia\Users\Alicia\.msf4\history
File Created	15/03/17 10:22:25 AM
Last Written	15/03/17 11:00:06 AM
Last Accessed	15/03/17 10:22:25 AM
MD5	6d16ebabb1b553c8fe6e7235e149865e
Comment	Metasploit command used to initiate attack

When observing under the item path of Alicia's history \Users\Alicia\msf4\history, we identified and extracted traces of commands issues by Alice using Metasploit to issue a keylogger on Simon's device.

places.sqlite

Item Path	Alicia\Users\Alicia\AppData\Roaming\Mozilla\Firefox\Profiles\lx5oaqu6.default\places.sqlite
File Created	15/03/17 01:38:34 AM
Last Written	16/03/17 10:28:13 AM
Last Accessed	15/03/17 01:38:34 AM
MD5	fd851a27740402563da60fba7900191b
Comment	Firefox browser history timeline

Browsing through the folders of Mozilla Firefox lead us to a database file called places.sqlite. Outputting this file in SQLite produces a comprehensive view of the search history of Alicia's browser. Search strings such as "Metasploit free download" and "Metasploit framework keylogging" can be observed. The file additionally includes search strings such as "localhost", suggesting the usage of the Metasploit GUI portal.

note.txt

Item Path	Alicia\$RECYCLE.BIN\S-1-5-21-4134190322-1791598225-2319710166-1002\note.txt
File Created	03/15/17 10:54:38 AM
Last Written	03/15/17 10:57:15 AM
Last Accessed	03/15/17 10:54:38 AM
MD5	
Start Sector	83,228
Sector offset	336
File Offset	0
Length	27
Comment	Located on Alicia's computer:

A text file containing Simon's computer password and OCBC account credentials, attempts to hide it includes setting hidden file attribute and deleting the file.

```
abc12345

7566721
999811
```

The deletion of this note containing Simon's sensitive login details represents potential evidence of unauthorized access or intent. The deletion and concealment of information such as this further suggest knowledge of wrongdoing. However, additional forensic analysis is required to establish whether these credentials were actively used in the unauthorized bank transfer.

main.db

Item Path	Alicia\Users\Alicia\AppData\Roaming\Skype\live#3aaliciatanhuijing\main.db
File Created	03/15/17 01:43:23 AM
Last Written	03/16/17 10:32:01 AM
Last Accessed	03/15/17 01:43:23 AM
MD5	
Comment	Located on Alicia's computer:

SQLite3 database that shows recent communications with a group called "MapleSEA PQRaiderz Skype Chat" and directly with a person with the username "live:jarylchng".

In the group chat, an important conversation can be seen here:
Alicia: "Browsing the cash shop recently really makes me want to buy some so much..."
live:aliciatanhuijing: "Need save up for mic also"
live:jarylchng: ":P">Why not "borrow" some from that CEO that you mentioned in game that lives with you? I'm sure he won't notice :P"
live:aliciatanhuijing: "No way! He doesn't keep cash around the house anyway... He mostly uses his bank and credit to purchase items."
live:jarylchng: "Well, if you had access to his pin number and iBanking token, I think it's possible to transfer money via e-banking"
live:aliciatanhuijing: "I think he keeps his iBanking token hidden in one of his drawers, I've seen him put it there before. He checks his OCBC account everyday"
live:aliciatanhuijing: "But I doubt I can get my hands on his OCBC username and pin number anyway"
live:aliciatanhuijing: "He did add me as a transfer recipient to return me some money before though... Hmm..."
This suggests that Alicia wanted money to purchase @Cash and a mic, but needed to save up. "live:jarylchng" then proceeded to tempt her to steal from Simon. She also mentioned that she was able to do so with access to Simon's account credentials as she knew where his iBanking security token was kept.

Communications with "live:jarylchng" shows that he was the one who taught Alicia about hacking and is worth investigating. Some of the messages by him include:
"Well, you can try to research on Metasploit Framework"
"I've learnt that in my course that it's a very simple tool to use."
"It has a remote keylogger and stuff"
"Like you login with psexec and you can run a keylogger on your victims computer"
"That way, when he logs in to his OCBC account, you can capture his username and pin."

"But you may have to have his computer password first though. Maybe you could try shoulder-surfing?"
"Just take your phone camera and go behind him when he types his password to log in his computer."

conversations detailing hacking techniques and financial fraud strategies within main.db provide critical evidence linking Alicia to the unauthorized bank transfer. Additionally, the involvement of "live:jarylchng" in guiding her through potential cybercrime methods suggests a broader conspiracy

Pictures of Interest

Images are referenced in glossary

i1^cimgpsh_orig.png

Item Path	Alicia\Users\Alicia\AppData\Roaming\Skype\live#3aaliciatanhuijing\media_messaging\media_cache_v3\i1^cimgpsh_orig.png
File Created	15/03/17 12:50:00 PM
Last Written	15/03/17 12:50:00 PM
Last Accessed	15/03/17 12:50:00 PM
MD5	28c9f69a77c74847434c57228eb2f76d
Comment	Cash transaction history image

A transaction history image was extracted from the media_cache folder under Skype, the transaction was made through Asiasoft and displays a bank transfer of $200 in exchange for a currency in MapleStory.

ABXzidWS.jpeg

Item Path	Alicia\Metasploit\ABXzidWS.jpeg
File Created	03/15/17 10:28:27 AM
Last Written	03/15/17 10:28:27 AM
Last Accessed	03/15/17 10:28:27 AM
MD5	
Comment	Located on Alicia's computer: Remote screenshot of Simons computer, browsing news websites.

The image strongly indicates that she gained unauthorized remote access to Simon’s computer. The existence of a screenshot further supports the theory that she monitored Simon’s activities, potentially as part of a plan to obtain his financial credentials.

grMyydzw.jpeg

Item Path	Alicia\Metasploit\grMyydzw.jpeg
File Created	03/15/17 10:49:56 AM
Last Written	03/15/17 10:49:56 AM
Last Accessed	03/15/17 10:49:56 AM
MD5	
Comment	Located on Alicia's computer: Remote screenshot of Simon's computer, writing an e-mail to Wendy Soh

The jpeg image being in Alicia's Metasploit directory \Alicia\Metasploit\grMyydzw.jpeg serves as very compelling evidence that she has maintained remote access and is monitoring Simon's computer and email communications, suggesting that she has been collecting information on Simon's activities and other sensitive company information.

NgIbWxjz.jpeg

Item Path	Alicia\Metasploit\NgIbWxjz.jpeg
File Created	03/15/17 10:37:17 AM
Last Written	03/15/17 10:37:17 AM
Last Accessed	03/15/17 10:37:17 AM
MD5	
Comment	Located on Alicia's computer:

Remote screenshot of Simons computer, writing an e-mail to Albert Choy.

The timestamp on the device being 10:38AM 3/15/2017 suggests that Alice is still maintaining persistence on the device, monitoring and even capturing sensitive information such as the investors list. Considering that the image was located on Alicia's device further justifies the theory that Alicia was collecting information on Simon's activities.

TAkHuvGO.jpeg

Item Path	Alicia\metasploit\TAkHuvGO.jpeg
File Created	03/15/17 10:30:10 AM
Last Written	03/15/17 10:30:10 AM
Last Accessed	03/15/17 10:30:10 AM
MD5	
Comment	Located on Alicia's computer:

Remote screenshot of Simons computer, browsing through Customer Data sent by Wendy Soh to him

This screenshot of Simon's customer data further implies that Alicia was going through sensitive company data through remote desktop access.

zrpffDcf.jpeg

Item Path	Alicia\metasploit\zrpffDcf.jpeg
File Created	03/15/17 10:31:15 AM
Last Written	03/15/17 10:31:15 AM
Last Accessed	03/15/17 10:31:15 AM
MD5	
Comment	Located on Alicia's computer:

Remote screenshot of Simons computer, sending an e-mail to Wendy Soh and a bank transfer

The image extracted from this evidence image proves that Simon's statement of Alicia making an illegal fund transfer to her account is proven. The timestamp of the image is 10:31AM 2/15/2017 suggesting that this event took place after Alicia had access to Simon's desktop.

Database of Interest

16764

Item Path	Alicia\metasploit\postgresql\data\base\16385\16764
File Created	03/14/17 12:57:05 PM
Last Written	03/15/17 11:02:48 AM
Last Accessed	03/14/17 12:57:05 PM
MD5	
Start Sector	41,080,469
Sector offset	248
File Offset	23,288
Length	1,277
Comment	Located on Alicia's computer:

PostgreSQL database containing remote keylogging logs of Simon's computer, seems to contain Simon's e-mail credentials along with other activities

```
Dumping captured keystrokes...  £È ã°í  °x                    □C        command
keyscan_d
ump   . ã°í   x                    —B        output 0   simonspegman@hotmail.com
<Return
> i<3rainbowsPY <N5> WP <Return>  <Delete>  <Up>  <Delete>  <Return>   <Back>  <Back>
<Ba
ck>  <Return>  <Return>  <Up> Seems odd that hotmail wanted toc <Back>  confirm my
identit
y with a captcha code. They think I'm a spam  <Back> mer. This is a resend, I
apologize if
 you received this twice.C    ÈySÌ°í   x                    —A        output?Dumping
capt
ured keystrokes...  g QÌ°í   x                    □@        command
keyscan_dump   ]ÚPÌ°í
  Úw                    —?        outputcScreenshot saved to:
C:/metasploit/grMyydzw.jpeg
ò ´Ä°í  Øw                    □>        command screenshot     g!¤Ä°í  Ôw
     —=        output;Unknown command: screenshit.    rLrÄ°í  ƒw                    —
<
     output ¸   Wendy, <Return>  <Return> Thank you very much. <Return>  <Return>
<Back>
 <Back>  <Back> Suit yourself alb <Back>  <Back>  <Back> Albert. <Return>  <Return>
Take n
te <Back>  <Back> ote that your parents will be notified of this outrageous act. You
shoul
d feel ashamed. <Return>  <Return> Good luck y <Back> out there. <Return>  <Return>
<Back
>  <Back>  <Back>
```

16764 serves as strong evidence of unauthorized keylogging activity on Simon's computer, capturing his email credentials and other sensitive information. This evidence when considering the context of Metasploit-related screenshots and unauthorized screenshots of chat logs, strongly suggests Alicia's direct involvement in monitoring and potentially misusing Simon's accounts

Videos of Interest

20170315_100927.jpg

Item Path	Alicia\$RECYCLE.BIN\S-1-5-21-4134190322-1791598225-2319710166-1002\20170315_100927.jpg
File Created	03/15/17 10:57:44 AM
Last Written	03/15/17 10:09:35 AM
Last Accessed	03/15/17 10:57:44 AM
MD5	
Comment	Located on Alicia's computer:

Video of a shoulder-surfing shot of Simon typing his computer password "abc12345", attempts to hide it includes renaming file extension from MP4 to JPG, setting hidden file attribute and deleting the file

Considering how the file was not only extracted from the recycle bin and renamed to a jpg extension, but also containing restricted information such as Simon's personal device's password details. This piece of evidence heavily implies that Alicia was demonstrating conscious efforts in hiding her actions and concealing her involvement in malicious activities, reinforcing her potential involvement in unauthorized access and fraudulent activity.

Emails of Interest

0000000800000030bfd.dat

True Path	Alicia Simon\Alicia\Users\Alicia\AppData\Local\Comms\Unistore\data\3\i\0000000800000030bfd.dat
File Created	03/14/17 12:48:27 PM
Last Written	03/14/17 12:48:27 PM
Last Accessed	03/14/17 12:48:27 PM
MD5	
Start Sector	13,444,624
Sector offset	0
File Offset	0
Length	8,192
Comment	Located on Alicia's computer:

An e-mail showing that Alicia signed up on Rapid7 for a free license key to Metasploit Framework, a hacking tool which was used to remote keylog and screenshot Simon's computer.

Rapid7

Your Metasploit Community License Key

IMG [https://system.netsuite.com/core/media/media.nl?id=18768&amp...] [http://www.rapid7.com/]

PERV-4MGR-EJEC-FNDM

Thank you for registering for Metasploit Community. To get started, follow the steps below:

1. If you have not downloaded our software yet, do so here: Download Metasploit [http://www.rapid7.com/products/metasploit/metasploit-communi...]

2. Insert your license key into Metasploit to activate your free penetration testing software

Your License Key: PERV-4MGR-EJEC-FNDM

Need Help? If you run into any problems, we will get you up and running.

Community: Join the Metasploit Community for support [https://community.rapid7.com/community/metasploit]

Activation problems: Metasploit Activation Troubleshooting Guide

Guide: Download Metasploit Community Getting Started Guide [https://community.rapid7.com/docs/DOC-1565]

We hope you enjoy Metasploit.

Best regards,

The Rapid7 Team

100 Summer Street, 13th Floor, Boston, MA 02110

Contact Us [http://www.rapid7.com/contact/]

This email is a crucial component in confirming Alicia's intent in executing a keylogger. The internet history files and extracted chat logs have mentioned the usage of Metasploit to execute a keylogger on Simon's device which accurately aligns with the email presented above.

Temporal Analysis

This section aims to establish a timeline of this digital forensic investigation. The goal is to reconstruct the order in which the actions have taken place, aiding in understanding the events that took place, prompting this investigation.

Chronological list of relevant events:

1. The incident begins on **March 14, 2017 12:48 PM** – Alicia registers for a free Metasploit Community license on the Rapid7 website and receives the activation key via email.
2. At **12:57 PM** – PostgreSQL database containing remote keylogging logs is created.
3. On **March 15, 2017 01:43:23 AM,** Alicia was communicating with a group called "MapleSEA PQRaiderz Skype Chat" and directly with a person with the username "live:jarylchng". We can observe based on information derived from main.db that Alicia was interested in the purchase of in game currency and a new microphone. Following that message, jarylchng responded by tempting Alicia to steal from Simon. She also mentioned that she was able to do so with access to Simon's account credentials as she knew where his iBanking security token was kept. Further communications with "live:jarylchng" shows that she was the one who taught Alicia about hacking and is worth investigating. The log concludes with Jarylchng providing further detailed steps in executing the plan.
4. From **01:38:34 AM**, Alicia was searching information regarding keyloggers. Websites such as "5 Step Using Metasploit Meterpreter Keylogger(Keylogging) | Ethical Hacking Tutorials, Tips and Tricks", "Working with Exploits - Metasploit Unleashed" and "Shoulder surfing (computer security) - Wikipedia" were seen being browsed and bookmarked. Alice could be searching this up due to the influence of her chat earlier.
5. At **03/15/17 10:09:35 AM,** Alicia recorded a video of Simon keying in details regarding his computer password, suggesting that she has the intent of carrying out the plan to steal Simon's funds
6. At **10:22:25 AM,** Alicia issues Metasploit commands, establishing a remote desktop connection with Simon's desktop. This log was extracted from the \.msf4\history folder.

7. At **10:28:27 AM,** Alicia can be seen monitoring Simon browsing news websites, this may be the first time she has established the remote connection to Simon's device.
8. At **10:30:10 AM**, Alicia monitors and screenshots sensitive information, consisting of customer data.
9. At **10:31:15 AM**, Alicia uses Simon's account to transfer funds over to her account.
10. At **10:32:15AM**, Alicia screenshots the email Simon sends to Wendy Soh
11. At **10:54:38 AM**, Alicia conceals information regarding Simon's computor password, OCBC credentials and attempts to mask it using a hidden file attribute and deleting the file in an attempt to conceal her tracks.
12. The recording of Simon keying in his computer password was renamed and hidden at **10:57:44 AM** on the same day. Further attempting to cover traces of her actions.

Relational Analysis

This relational analysis examines the digital evidence obtained from Alicia's computer to establish the connection between Alicia, Simon, and the unauthorized bank transfer of SGD $2000. By correlating forensic artifacts such as chat logs, keylogging records, and file system metadata, we can determine Alicia's intent, method, and possible influence from external parties.

- Alicia and Simon shared the same apartment, making physical access to Simon's computer possible, this is further supported by the video recording of Simon keying in his password.
- Simon's password was clearly identified and recorded in a txt file located on Alicia's device under note.txt
- The Skype chat logs retrieved from Alicia's main.db file show that she was tempted and encouraged by the user "live:jarylchng" to access Simon's financial accounts, indicating that there might be another user at play in this case study.
- Alicia carried out the attack using metasploit as suggested by Jarylchng, this is mainly how she executed remote desktop access on Simon's device.
- Simon's activity was captured on Alicia's device, indicating that Alicia had monitoring access to Simon's computer

Additional Subsections

Attacker Methodology

This section outlines the techniques and strategies employed by the attacker to compromise the victim's system, providing a detailed breakdown of how unauthorized access was gained, what tools or methods were used, and how the attacker attempted to remain undetected.

- Alicia records Simon logging into his computer to obtain his password credentials
- Alicia leveraged the use of Metasploit's keylogger tool and uploads it onto Simon's device using her knowledge of Simon's login credentials
- Alicia was able to establish remote desktop access as proven by screenshots of Simon's activity being present on her desktop.
- Alicia transfers funds of $2000 to her bank account and removes traces of such activity by renaming file extensions and deleting logs.

User Application

This section examines the software and applications installed or executed on the suspect's device. It helps determine if any suspicious programs, unauthorized tools, or hacking-related applications were used in the attack.

- Alicia uses Skype as a platform for communicating with Jarylchng, a user responsible for influencing Alicia's actions
- Alicia uses Mozilla Firefox for information regarding the usage and implementation of keyloggers
- Alicia uses Metasploit to execute the keylogger

Conclusions

The forensic findings establish a clear pattern of Alicia's intent and actions leading up to the unauthorized bank transfer. The evidence obtained demonstrates deliberate reconnaissance, password harvesting, and the use of hacking tools to compromise Simon's online security. Furthermore, the investigation highlights Alicia's attempts to erase or conceal incriminating files.

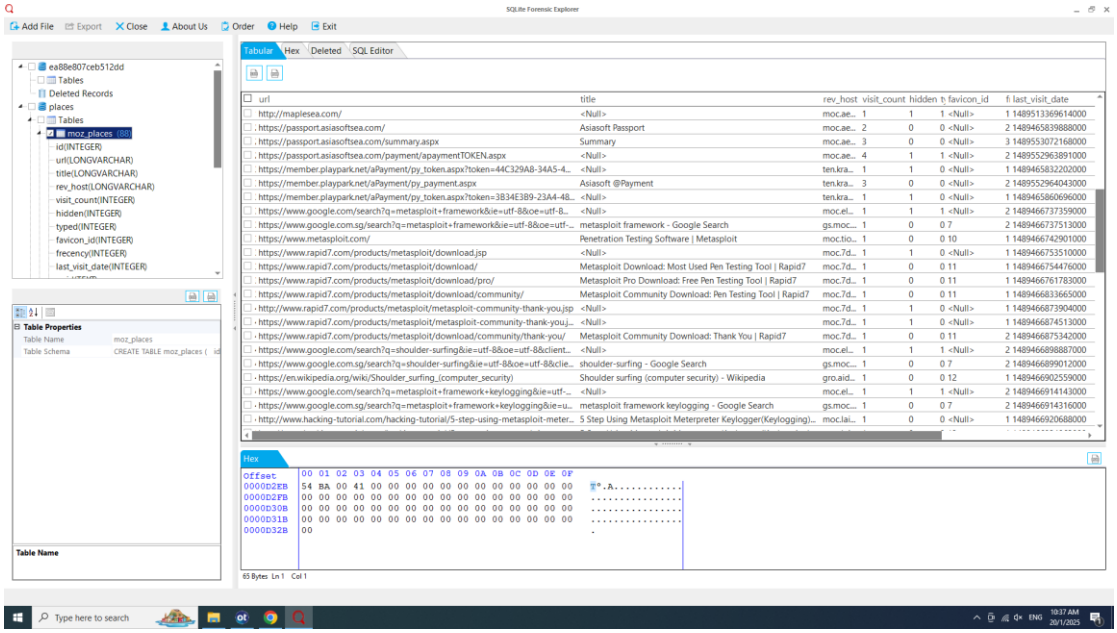
Based on these findings, it is strongly recommended for further investigation and conductions regarding "live:jarylchng," who was actively guiding and influencing Alicia through the process.

Glossary

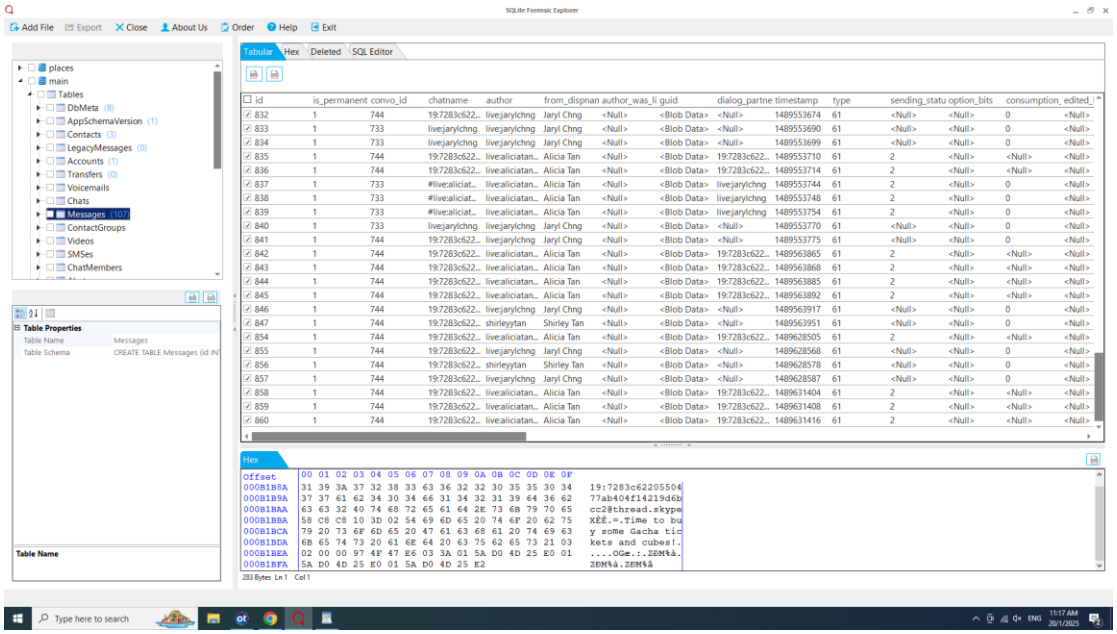
Images go here

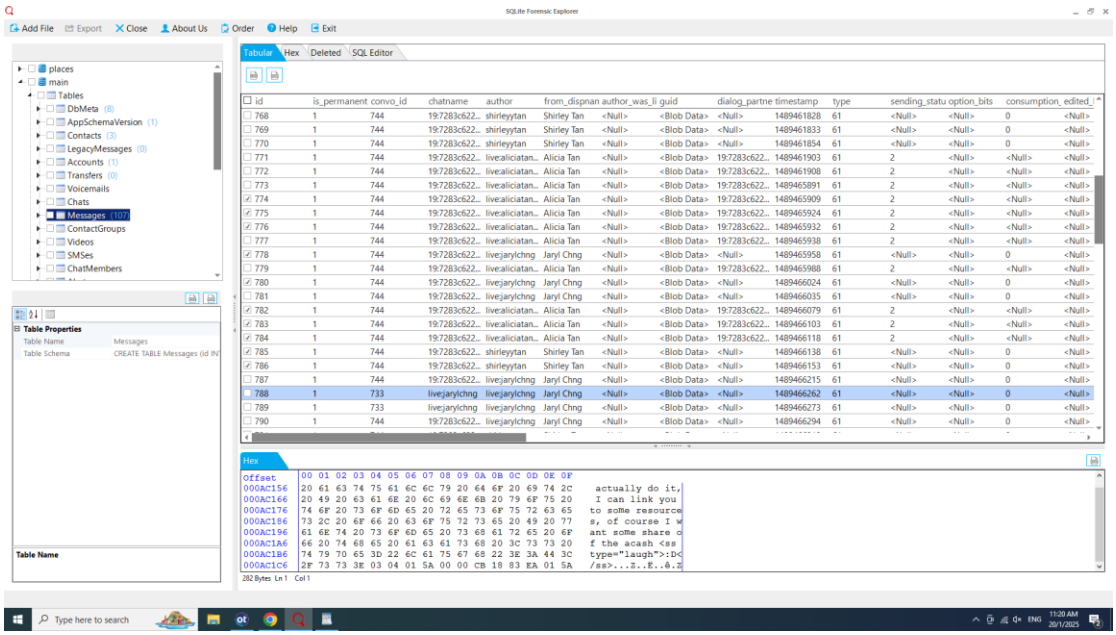
Files of interests

Places.sqlite



Main.db

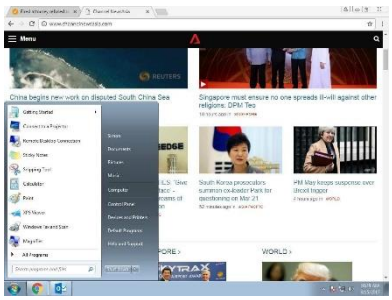




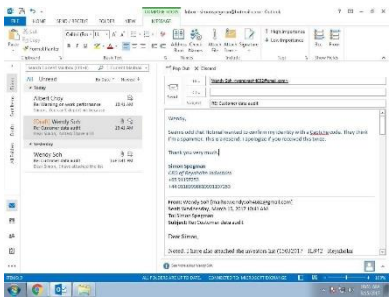
Pictures of interests

i1^cimgpsh_orig.png

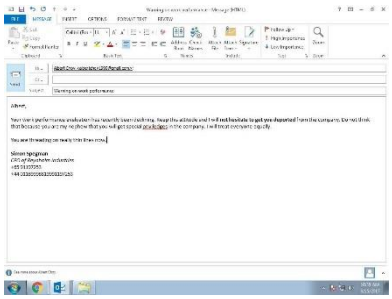
ABXzidWS.jpeg



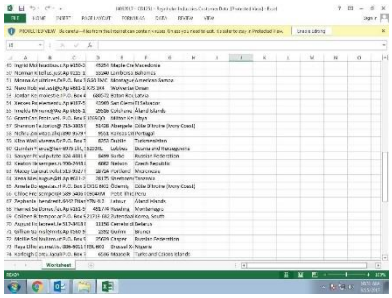
grMyydzw.jpeg



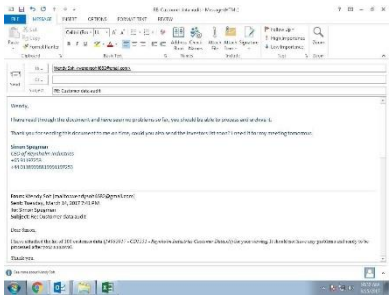
NgIbWxjz.jpeg



TAkHuvGO.jpeg



zrpffDcf.jpeg



Appendices

opentext™

Examiner Report

Case Information

Case Number	01
Examiner Name	Ivan, Jun Hang
Description	In-class forensic investigation

Evidence

Name	Acquisition MD5	Verification MD5	Evidence Number	Examiner Name
Alicia			E02HD1	Thomas Chee

Name	Alicia
GUID	1e11d3d1dca5f4c6a9f08c902e24886c
Index File	C:\Users\DF Student P04\Cases\prac2\EvidenceCache\1E11D3D1DCA5F4C6A9F08C902E24886C\DeviceIndex.L01
Actual Date	16/03/17 10:50:29 AM
Target Date	16/03/17 10:50:30 AM
File Integrity	Completely Verified, 0 Errors
Acquisition SHA1	132a9f27dc3a02f90d64f50b12b797c16f74089b
Verification SHA1	132a9f27dc3a02f90d64f50b12b797c16f74089b
EnCase Version	7.10
Error Granularity	64
Read Errors	1
Missing Sectors	0
CRC Errors	0
Compression	Best
Examiner Name	Thomas Chee
Notes	Acquired from Alicia Tan Hui Jing's computer at Simon Spegman's apartment
Serial Number	Z3TNNKM4_206848
Model	ST500DM002-1BD142
Drive Type	Fixed
System Version	Windows 8.1
Total Sectors	83,886,079

Examination

Drive information

1) $Extend

Item Path	Alicia\$Extend
File Created	14/02/17 11:48:45 PM
Last Written	14/02/17 11:48:45 PM
Last Accessed	14/02/17 11:48:45 PM
MD5	
Comment	Drive information

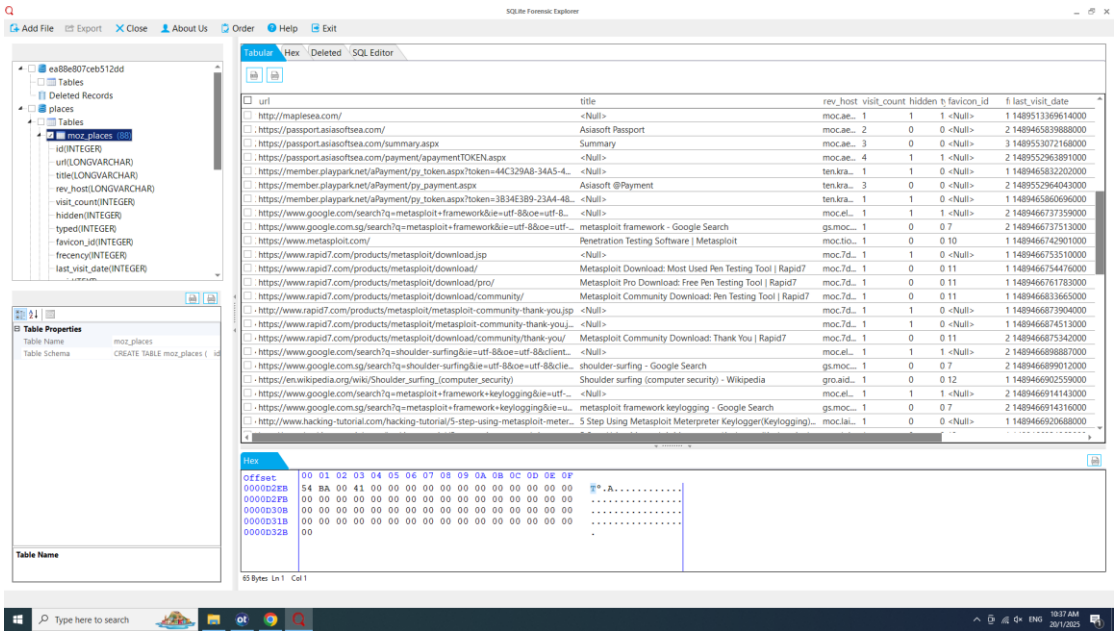
Notable files

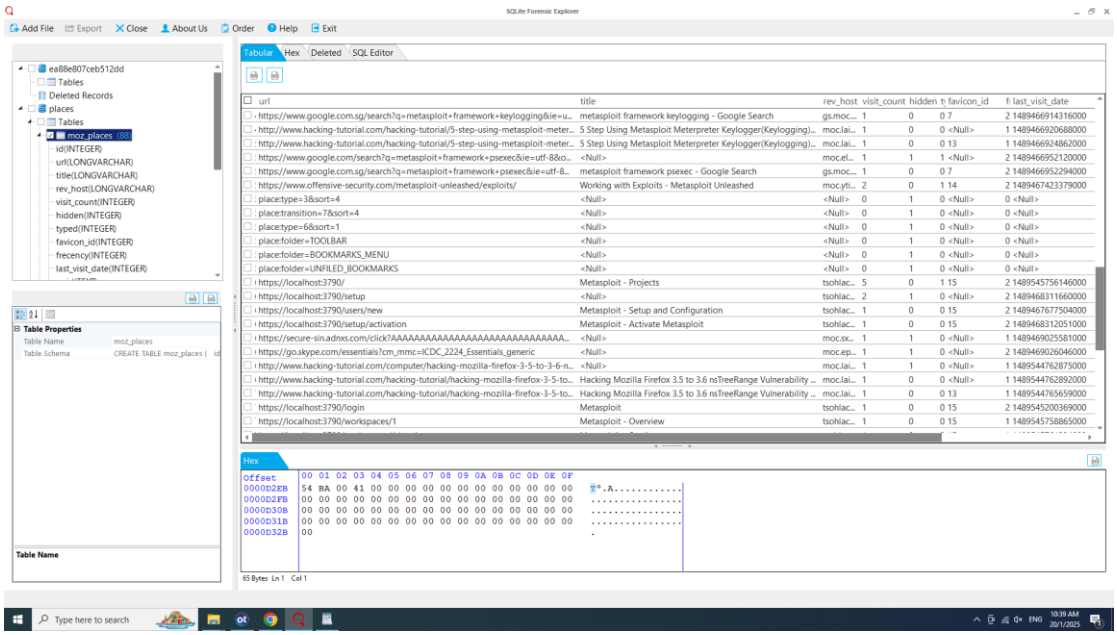
2) history

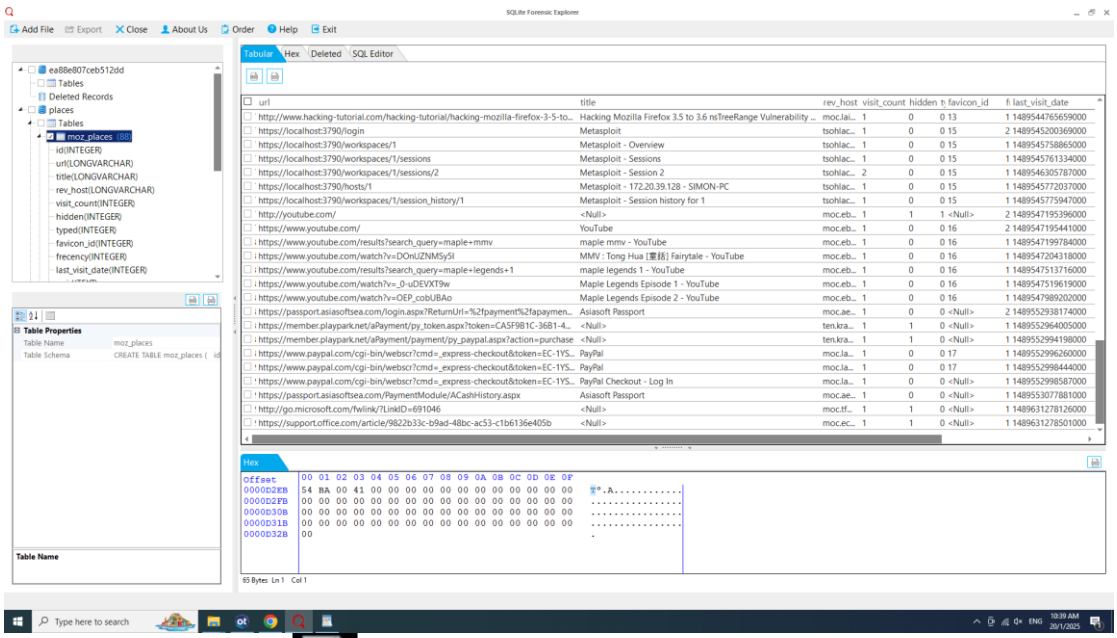
Item Path	Alicia\Users\Alicia\.msf4\history
File Created	15/03/17 10:22:25 AM
Last Written	15/03/17 11:00:06 AM
Last Accessed	15/03/17 10:22:25 AM
MD5	6d16ebabb1b553c8fe6e7235e149865e
Comment	Metasploit command used to initiate attack

3) places.sqlite

Item Path	Alicia\Users\Alicia\AppData\Roaming\Mozilla\Firefox\Profiles\lx5oaqu6.default\places.sqlite
File Created	15/03/17 01:38:34 AM
Last Written	16/03/17 10:28:13 AM
Last Accessed	15/03/17 01:38:34 AM
MD5	fd851a27740402563da60fba7900191b
Comment	Firefox browser history timeline







places.sqlite

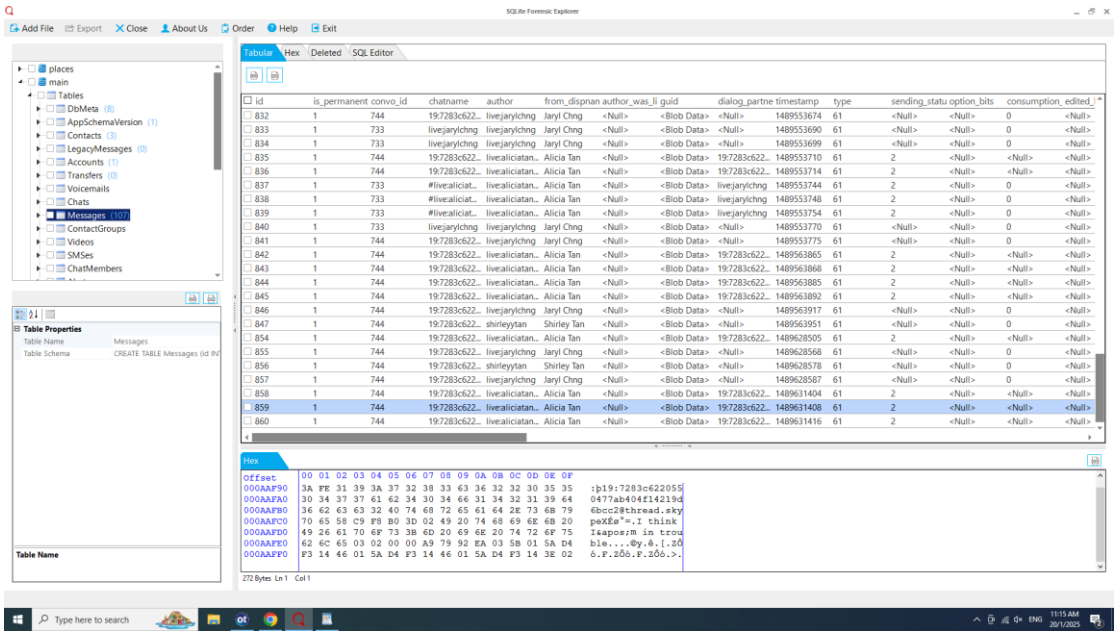
Skype Content

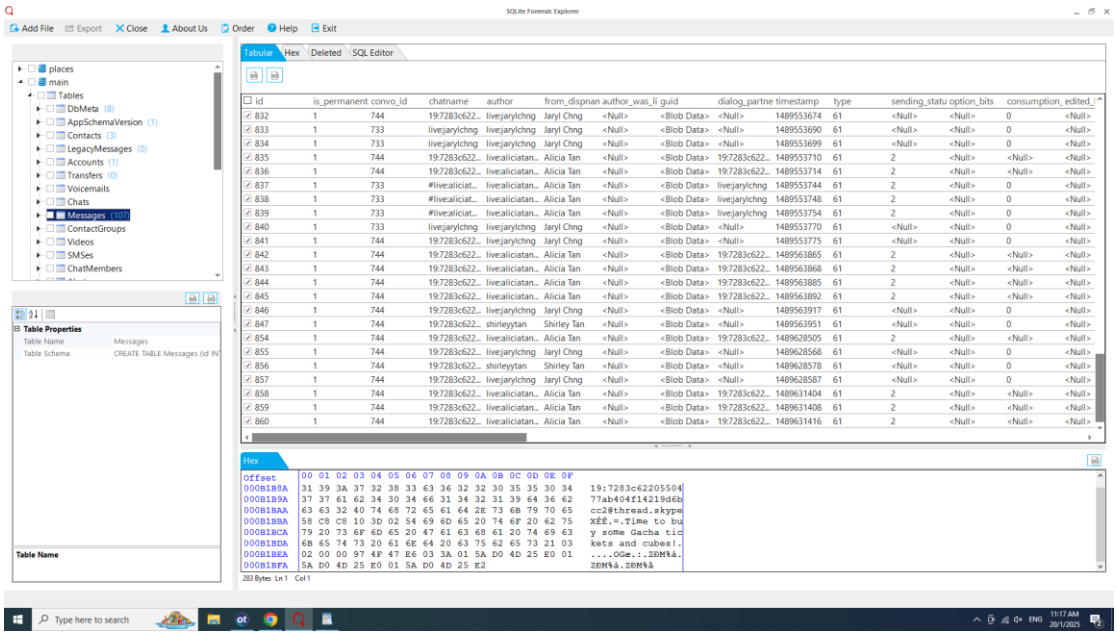
4) main.db

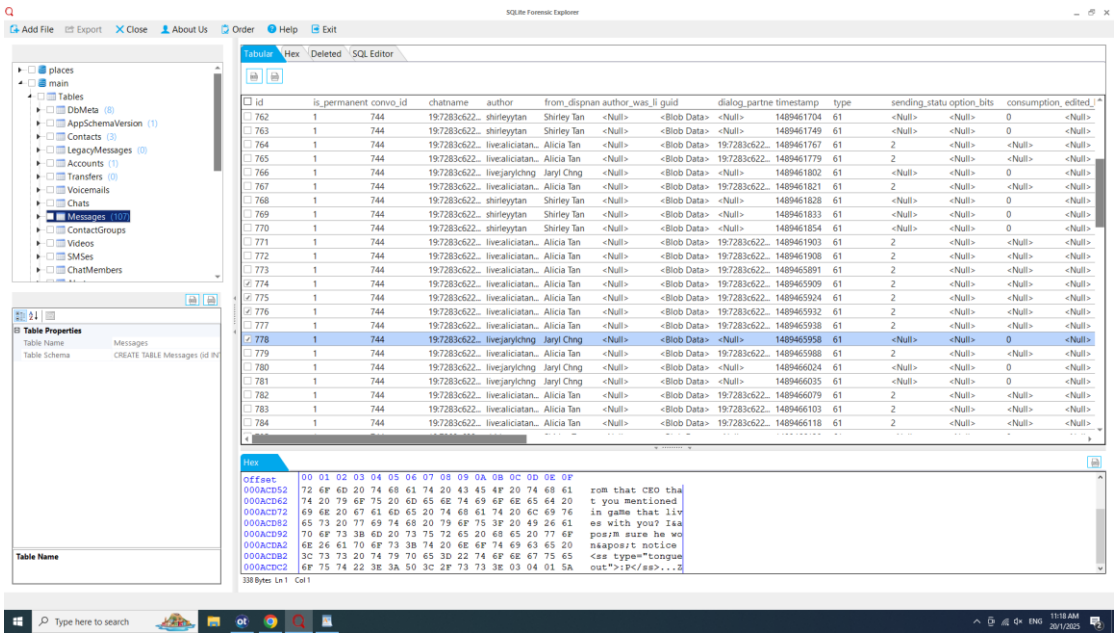
Item Path	Alicia\Users\Alicia\AppData\Roaming\Skype\live#3aaliciatanhuijing\main.db
File Created	15/03/17 01:43:23 AM
Last Written	16/03/17 10:32:01 AM
Last Accessed	15/03/17 01:43:23 AM
MD5	8067e9ef5ead2f5560f55b564a7f0b7d
Comment	Main chat log for alicia skype, throw into sqlite for more info

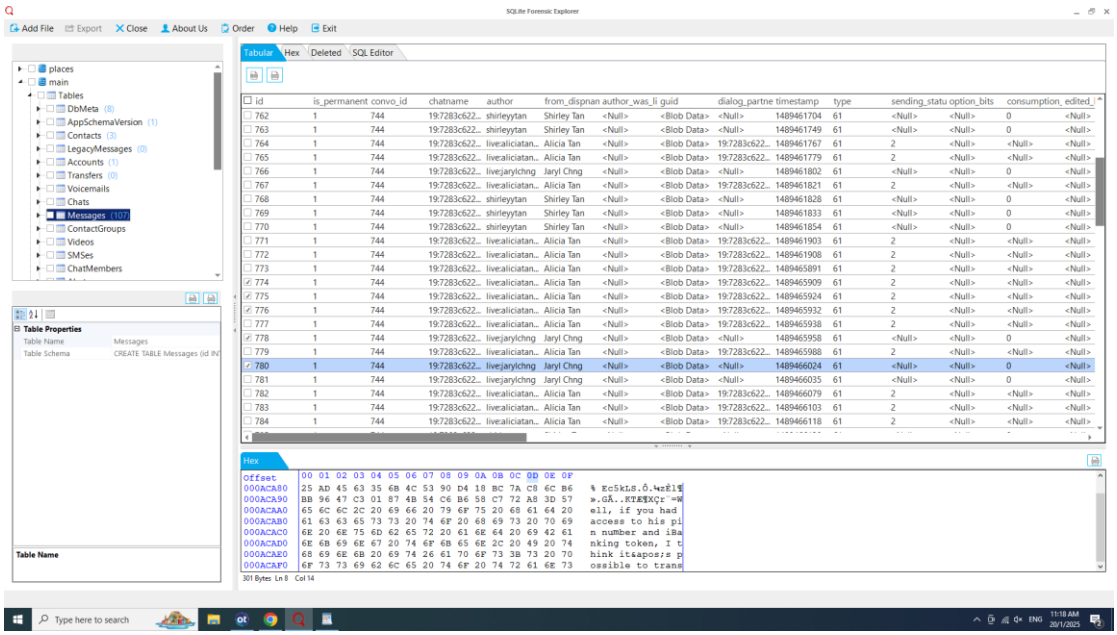
5) ea88e807ceb512dd.dat

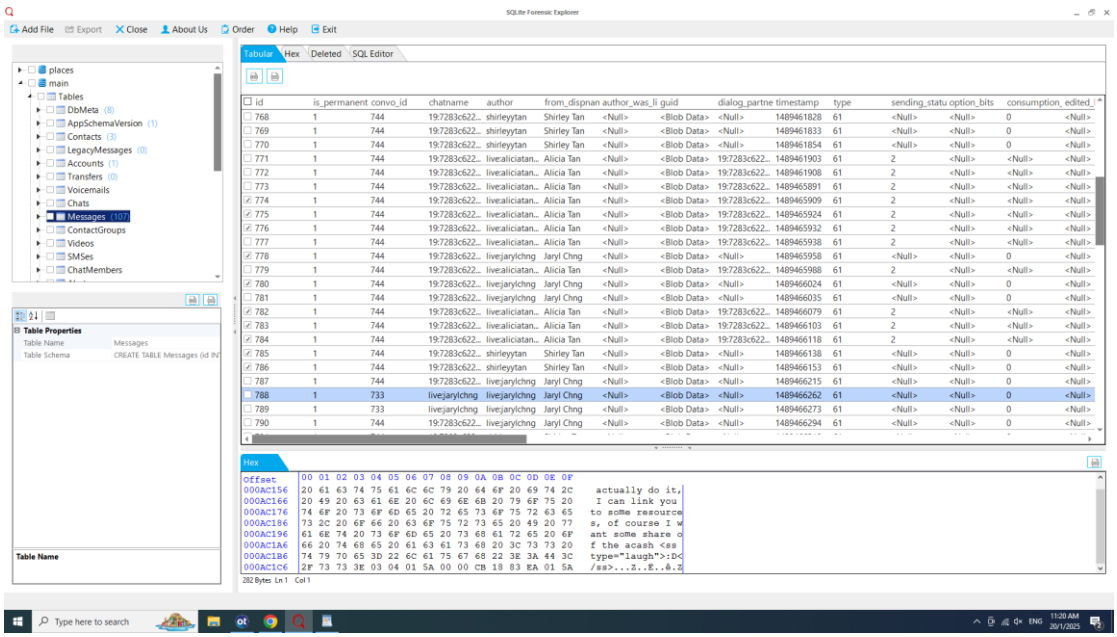
Item Path	Alicia\Users\Alicia\AppData\Roaming\Skype\live#3aaliciatanhuijing\chatsync\ea\ea88e807ceb512dd.dat
File Created	15/03/17 02:04:17 AM
Last Written	15/03/17 01:07:09 PM
Last Accessed	15/03/17 02:04:17 AM
MD5	f639ac0faa5326c2175f04981a742872
Comment	Chat log (jaryl chng, shirley tan, alicia tan) indicating intent or desperation for cash

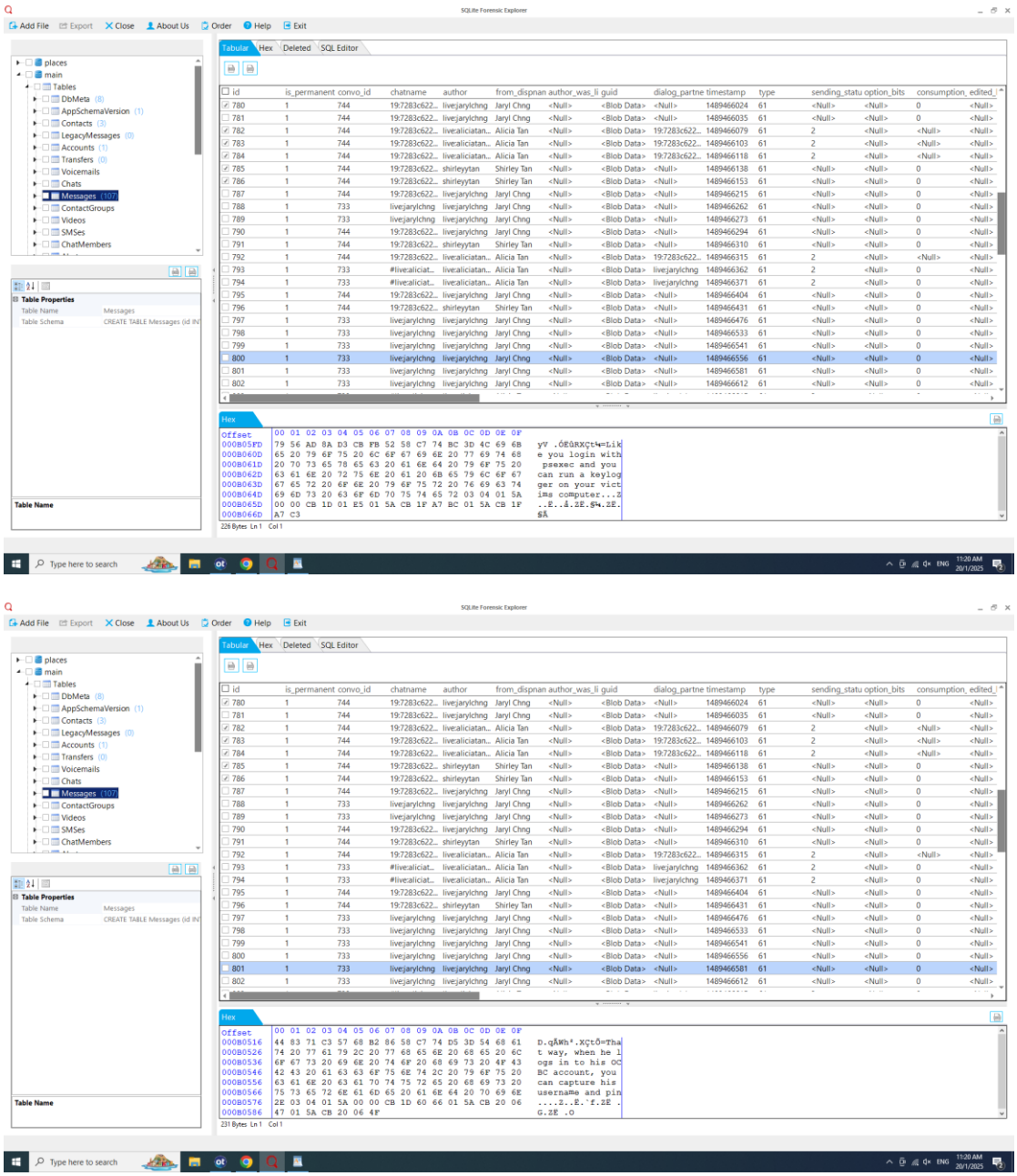



SQLite Forensic Explorer
Add File
Export
Close
About Us
Order
Help
Exit
places
main
Tables
DbMeta (8)
AppSchemaVersion (1)
Contacts (3)
LegacyMessages (0)
Accounts (1)
Transfers (0)
Voicemails
Chats
Messages (107)
ContactGroups
Videos
SMSes
ChatMembers
Table Properties
Table Name
Messages
Table Schema
CREATE TABLE Messages (id IN
Tabular
Hex
Deleted
SQL Editor
id is_permanent convo_id chatname author from_dispnan author_was_li guid dialog_partne timestamp type sending_statu option_bits consumption_edited_
832 1 744 19:7283c622... livejarylchng Jaryl Chng <Null> <Blob Data> <Null> 1489553674 61 <Null> <Null> 0 <Null>
833 1 733 livejarylchng livejarylchng Jaryl Chng <Null> <Blob Data> <Null> 1489553690 61 <Null> <Null> 0 <Null>
834 1 733 livejarylchng livejarylchng Jaryl Chng <Null> <Blob Data> <Null> 1489553699 61 <Null> <Null> 0 <Null>
835 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489553710 61 2 <Null> <Null> <Null>
836 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489553714 61 2 <Null> <Null> <Null>
837 1 733 #livealiciat... livealiciatan... Alicia Tan <Null> <Blob Data> livejarylchng 1489553744 61 2 <Null> 0 <Null>
838 1 733 #livealiciat... livealiciatan... Alicia Tan <Null> <Blob Data> livejarylchng 1489553748 61 2 <Null> 0 <Null>
839 1 733 #livealiciat... livealiciatan... Alicia Tan <Null> <Blob Data> livejarylchng 1489553754 61 2 <Null> 0 <Null>
840 1 733 livejarylchng livejarylchng Jaryl Chng <Null> <Blob Data> <Null> 1489553770 61 <Null> <Null> 0 <Null>
841 1 744 19:7283c622... livejarylchng Jaryl Chng <Null> <Blob Data> <Null> 1489553775 61 <Null> <Null> 0 <Null>
842 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489563865 61 2 <Null> <Null> <Null>
843 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489563868 61 2 <Null> <Null> <Null>
844 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489563885 61 2 <Null> <Null> <Null>
845 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489563892 61 2 <Null> <Null> <Null>
846 1 744 19:7283c622... livejarylchng Jaryl Chng <Null> <Blob Data> <Null> 1489563917 61 <Null> <Null> 0 <Null>
847 1 744 19:7283c622... shirleyytan Shirley Tan <Null> <Blob Data> <Null> 1489563951 61 <Null> <Null> 0 <Null>
854 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489628505 61 2 <Null> <Null> <Null>
855 1 744 19:7283c622... livejarylchng Jaryl Chng <Null> <Blob Data> <Null> 1489628568 61 <Null> <Null> 0 <Null>
856 1 744 19:7283c622... shirleyytan Shirley Tan <Null> <Blob Data> <Null> 1489628578 61 <Null> <Null> 0 <Null>
857 1 744 19:7283c622... livejarylchng Jaryl Chng <Null> <Blob Data> <Null> 1489628587 61 <Null> <Null> 0 <Null>
858 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489631404 61 2 <Null> <Null> <Null>
859 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489631408 61 2 <Null> <Null> <Null>
860 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489631416 61 2 <Null> <Null> <Null>
Hex
Offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000B1B8A 31 39 3A 37 32 38 33 63 36 32 32 30 35 35 30 34 19:7283c62205504
000B1B9A 37 37 61 62 34 30 34 66 31 34 32 31 39 64 36 62 77ab404f14219d6b
000B1BAA 63 63 32 40 74 68 72 65 61 64 2E 73 6B 79 70 65 cc2@thread.skype
000B1BBA 58 C8 C8 10 3D 02 54 69 6D 65 20 74 6F 20 62 75 XÈÈ.=.Time to bu
000B1BCA 79 20 73 6F 6D 65 20 47 61 63 68 61 20 74 69 63 y some Gacha tic
000B1BDA 6B 65 74 73 20 61 6E 64 20 63 75 62 65 73 21 03 kets and cubes!.
000B1BEA 02 00 00 97 4F 47 E6 03 3A 01 5A D0 4D 25 E0 01 ....OGæ.:.ZÐM%à.
000B1BFA 5A D0 4D 25 E0 01 5A D0 4D 25 E2 ZÐM%à.ZÐM%â
283 Bytes Ln 1 Col 1
Type here to search
ENG
11:17 AM
20/1/2025


SQLite Forensic Explorer
Add File
Export
Close
About Us
Order
Help
Exit
places
main
Tables
DbMeta (8)
AppSchemaVersion (1)
Contacts (3)
LegacyMessages (0)
Accounts (1)
Transfers (0)
Voicemails
Chats
Messages (107)
ContactGroups
Videos
SMSes
ChatMembers
Table Properties
Table Name
Messages
Table Schema
CREATE TABLE Messages (id IN
Tabular
Hex
Deleted
SQL Editor
id is_permanent convo_id chatname author from_dispnan author_was_li guid dialog_partne timestamp type sending_statu option_bits consumption_edited_
762 1 744 19:7283c622... shirleyytan Shirley Tan <Null> <Blob Data> <Null> 1489461704 61 <Null> <Null> 0 <Null>
763 1 744 19:7283c622... shirleyytan Shirley Tan <Null> <Blob Data> <Null> 1489461749 61 <Null> <Null> 0 <Null>
764 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489461767 61 2 <Null> <Null> <Null>
765 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489461779 61 2 <Null> <Null> <Null>
766 1 744 19:7283c622... livejarylchng Jaryl Chng <Null> <Blob Data> <Null> 1489461802 61 <Null> <Null> 0 <Null>
767 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489461821 61 2 <Null> <Null> <Null>
768 1 744 19:7283c622... shirleyytan Shirley Tan <Null> <Blob Data> <Null> 1489461828 61 <Null> <Null> 0 <Null>
769 1 744 19:7283c622... shirleyytan Shirley Tan <Null> <Blob Data> <Null> 1489461833 61 <Null> <Null> 0 <Null>
770 1 744 19:7283c622... shirleyytan Shirley Tan <Null> <Blob Data> <Null> 1489461854 61 <Null> <Null> 0 <Null>
771 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489461903 61 2 <Null> <Null> <Null>
772 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489461908 61 2 <Null> <Null> <Null>
773 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489465891 61 2 <Null> <Null> <Null>
774 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489465909 61 2 <Null> <Null> <Null>
775 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489465924 61 2 <Null> <Null> <Null>
776 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489465932 61 2 <Null> <Null> <Null>
777 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489465938 61 2 <Null> <Null> <Null>
778 1 744 19:7283c622... livejarylchng Jaryl Chng <Null> <Blob Data> <Null> 1489465958 61 <Null> <Null> 0 <Null>
779 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489465988 61 2 <Null> <Null> <Null>
780 1 744 19:7283c622... livejarylchng Jaryl Chng <Null> <Blob Data> <Null> 1489466024 61 <Null> <Null> 0 <Null>
781 1 744 19:7283c622... livejarylchng Jaryl Chng <Null> <Blob Data> <Null> 1489466035 61 <Null> <Null> 0 <Null>
782 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489466079 61 2 <Null> <Null> <Null>
783 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489466103 61 2 <Null> <Null> <Null>
784 1 744 19:7283c622... livealiciatan... Alicia Tan <Null> <Blob Data> 19:7283c622... 1489466118 61 2 <Null> <Null> <Null>
Hex
Offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000ACD52 72 6F 6D 20 74 68 61 74 20 43 45 4F 20 74 68 61 rom that CEO tha
000ACD62 74 20 79 6F 75 20 6D 65 6E 74 69 6F 6E 65 64 20 t you mentioned
000ACD72 69 6E 20 67 61 6D 65 20 74 68 61 74 20 6C 69 76 in game that liv
000ACD82 65 73 20 77 69 74 68 20 79 6F 75 3F 20 49 26 61 es with you? I&a
000ACD92 70 6F 73 3B 6D 20 73 75 72 65 20 68 65 20 77 6F pos;m sure he wo
000ACDA2 6E 26 61 70 6F 73 3B 74 20 6E 6F 74 69 63 65 20 n't notice
000ACDB2 3C 73 73 20 74 79 70 65 3D 22 74 6F 6E 67 75 65 <ss type="tongue
000ACDC2 6F 75 74 22 3E 3A 50 3C 2F 73 73 3E 03 04 01 5A out">:P</ss>...Z
338 Bytes Ln 1 Col 1
Type here to search
ENG
11:18 AM
20/1/2025





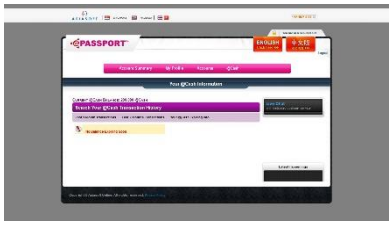


Alicia chat log

Image content

6) i1^cimgpsh_orig.png

Item Path	Alicia\Users\Alicia\AppData\Roaming\Skype\live#3aaliciatanhuijing\media_messaging\media_cache_v3\i1^cimgpsh_orig.png
File Created	15/03/17 12:50:00 PM
Last Written	15/03/17 12:50:00 PM
Last Accessed	15/03/17 12:50:00 PM
MD5	28c9f69a77c74847434c57228eb2f76d
Comment	Cash transaction history image



Glossary

The following terms and definitions may be used throughout the report.