

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	4
Case Background.....	4
Examination Summary	4
Relevant Findings.....	5
File system examination	5
Pictures of Interest	7
Database of Interest	9
Videos of Interest	9
Emails of Interest	10
Temporal Analysis.....	12
Relational Analysis.....	13
Additional Subsections	14
Attacker Methodology.....	14
User Application.....	14
Conclusions	14
Glossary	15
Files of interests	15
Pictures of interests	16
Appendices	18
Evidence	18
Examination	20
Drive information.....	21
Notable files.....	22
Skype Content.....	24
Image content	28
Glossary	29

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...  fÈ ã°i °x          □C          command
keyscan_d
ump  . ã°i  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  ÈySî°i  x          -A          output?Dumping
capt
ured keystrokes...  g Qî°i  x          □@          command
keyscan_dump  ]ÚPî°i
Úw          -?          outputcScreenshot saved to:
C:/metasploit/grMyydzw.jpeg
ò 'Ä°i  Øw          □>          command screenshot  g!ªÄ°i  Ôw
==          output;Unknown command: screenshit.  rLrÄ°i  fw          -
<
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

00000008000000030bfd.dat

True Path	Alicia Simon\Alicia\Users\Alicia\AppData\Local\Comms\Unistore\data\3\i\00000008000000030bfd.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

Metasploit Community License Key

Your

 [\[https://system.netsuite.com/core/media/media.nl?id=18768&...\]](https://system.netsuite.com/core/media/media.nl?id=18768&...) [\[http://www.rapid7.com/\]](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
[\[http://www.rapid7.com/products/metasploit/metasploit-communi...\]](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

Boston, MA 02110

100 Summer Street, 13th Floor,

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

Copyright © 2016 Rapid7® All

Rights Reserved.

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 computer 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

SQLLite Forensic Explorer

File: ea8be807ceb512dd

Tables: Deleted Records

Places

moz_places

moz_places_history

Table Properties

Table Name: moz_places

Table Schema: CREATE TABLE moz_places (url LONGVARCHAR, title LONGVARCHAR, visit_count INTEGER, hidden INTEGER, favicon_id INTEGER, frequency INTEGER, last_visit_date INTEGER)

Table Data

url	title	rev_host	visit_count	hidden	favicon_id	last_visit_date	
http://maplelea.com/	<Null>	moz.ae...	1	1	<Null>	11489513369614000	
https://passport.asiasoftsea.com/	Asiasoft Passport	moz.ae...	2	0	<Null>	21489465839888000	
https://passport.asiasoftsea.com/summary.aspx	Summary	moz.ae...	3	0	<Null>	31489553072168000	
https://passport.asiasoftsea.com/payment/apaymentTOKEN.aspx	<Null>	moz.ae...	4	1	<Null>	21489552963891000	
https://member.playpark.net/apayment/py_payment.aspx	<Null>	tenkra...	1	1	<Null>	11489465832202000	
https://member.playpark.net/apayment/py_payment.aspx	Asiasoft @Payment	tenkra...	3	0	<Null>	21489552964043000	
https://member.playpark.net/apayment/py_payment.aspx	<Null>	tenkra...	1	1	<Null>	11489465836960000	
https://www.google.com/search?q=metasploit+framework&ie=utf-8&oe=utf-8	<Null>	moz.ae...	1	1	<Null>	21489466773739000	
https://www.google.com/search?q=metasploit+framework&ie=utf-8&oe=utf-8	metasploit framework - Google Search	gs.moc...	1	0	7	21489466737513000	
https://www.metasploit.com/	Penetration Testing Software Metasploit	moz.ae...	1	0	10	11489466742901000	
https://www.rapid7.com/products/metasploit/download.jsp	<Null>	moz.ae...	1	1	0	<Null>	11489466753510000
https://www.rapid7.com/products/metasploit/download/	Metasploit Download: Most Used Pen Testing Tool Rapid7	moz.ae...	1	0	11	11489466754476000	
https://www.rapid7.com/products/metasploit/download/pro/	Metasploit Pro Download: Free Pen Testing Tool Rapid7	moz.ae...	1	0	11	11489466761783000	
https://www.rapid7.com/products/metasploit/download/community/	Metasploit Community Download: Pen Testing Tool Rapid7	moz.ae...	1	0	11	1148946683665000	
https://www.rapid7.com/products/metasploit/download/community/thank-you.jsp	<Null>	moz.ae...	1	1	0	<Null>	1148946683994000
https://www.rapid7.com/products/metasploit/download/community/thank-you.jsp	<Null>	moz.ae...	1	0	<Null>	11489466874513000	
https://www.rapid7.com/products/metasploit/download/community/thank-you.jsp	Metasploit Community Download: Thank You Rapid7	moz.ae...	1	0	11	21489466875342000	
https://www.google.com/search?q=shoulder-surfing&ie=utf-8&oe=utf-8&clie=utf-8	<Null>	moz.ae...	1	1	<Null>	2148946688887000	
https://www.google.com/search?q=shoulder-surfing&ie=utf-8&oe=utf-8&clie=utf-8	Shoulder surfing - Google Search	gs.moc...	1	0	7	21489466899012000	
https://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security)	Shoulder surfing (computer security) - Wikipedia	gro.aie...	1	0	12	1148946690259000	
https://www.google.com/search?q=metasploit+framework+keylogging&ie=utf-8&oe=utf-8	<Null>	moz.ae...	1	1	<Null>	21489466914143000	
https://www.google.com/search?q=metasploit+framework+keylogging&ie=utf-8&oe=utf-8	metasploit framework keylogging - Google Search	gs.moc...	1	0	7	21489466914316000	
https://www.hacking-tutorial.com/hacking-tutorial/5-step-using-metasploit-meterpreter-keylogger(keylogging)...	5 Step Using Metasploit Meterpreter Keylogger(Keylogging)...	moz.ae...	1	0	<Null>	1148946692068000	

Hex

00000000 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F ...

85 Bytes Ln 1 Col 1

Main.db

SQLLite Forensic Explorer

File: main

Tables: Deleted

Messages

Messages_history

Table Properties

Table Name: Messages

Table Schema: CREATE TABLE Messages (id INTEGER, is_permanent INTEGER, convo_id INTEGER, chatname VARCHAR, author VARCHAR, from_displayname VARCHAR, author_was VARCHAR, li_guid VARCHAR, dialog_partne VARCHAR, timestamp INTEGER, type INTEGER, sending_status INTEGER, option_bits INTEGER, consumption INTEGER, edited INTEGER)

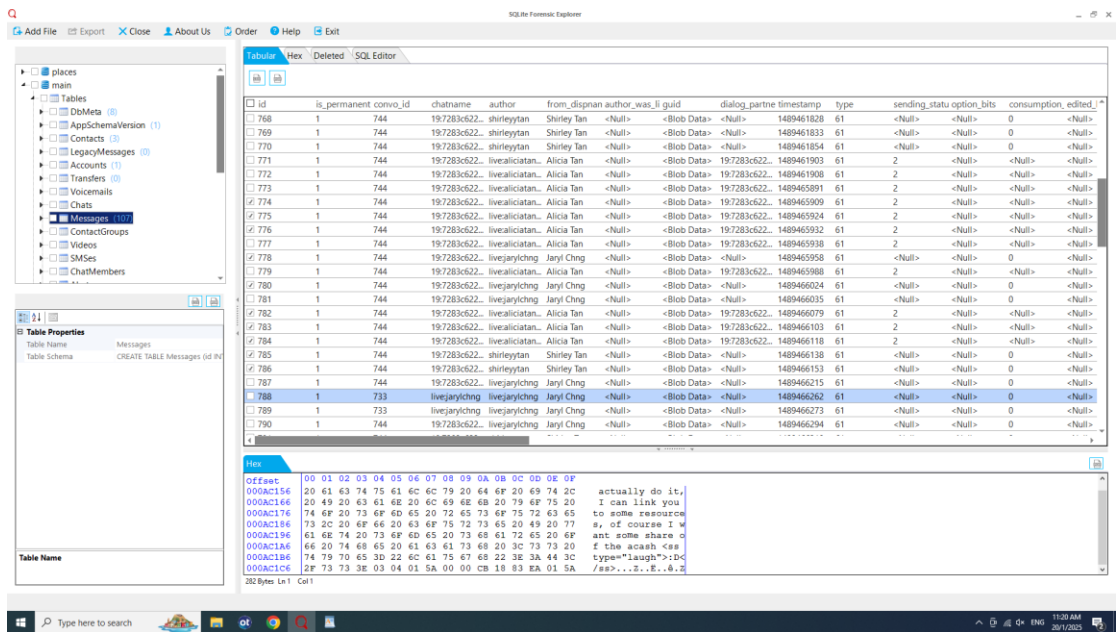
Table Data

id	is_permanent	convo_id	chatname	author	from_displayname	author_was	li_guid	dialog_partne	timestamp	type	sending_status	option_bits	consumption	edited
832	1	744	197283622...	livejarychng	Jaryl Chng	<Null>	<Blob Data>	<Null>	1489553674	61	<Null>	<Null>	0	<Null>
833	1	733	livejarychng	livejarychng	Jaryl Chng	<Null>	<Blob Data>	<Null>	1489553690	61	<Null>	<Null>	0	<Null>
834	1	733	livejarychng	livejarychng	Jaryl Chng	<Null>	<Blob Data>	<Null>	1489553699	61	<Null>	<Null>	0	<Null>
835	1	744	197283622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	<Null>	197283622...	61	2	<Null>	<Null>	<Null>
836	1	744	197283622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	<Null>	197283622...	61	2	<Null>	<Null>	<Null>
837	1	733	#livealiciatan	livealiciatan	Alicia Tan	<Null>	<Blob Data>	livejarychng	1489553744	61	2	<Null>	0	<Null>
838	1	733	#livealiciatan	livealiciatan	Alicia Tan	<Null>	<Blob Data>	livejarychng	1489553748	61	2	<Null>	0	<Null>
839	1	733	#livealiciatan	livealiciatan	Alicia Tan	<Null>	<Blob Data>	livejarychng	1489553754	61	2	<Null>	0	<Null>
840	1	733	livejarychng	livejarychng	Jaryl Chng	<Null>	<Blob Data>	<Null>	1489553770	61	<Null>	<Null>	0	<Null>
841	1	744	197283622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	<Null>	1489553775	61	<Null>	<Null>	0	<Null>
842	1	744	197283622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	<Null>	197283622...	61	2	<Null>	<Null>	<Null>
843	1	744	197283622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	<Null>	197283622...	61	2	<Null>	<Null>	<Null>
844	1	744	197283622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	<Null>	197283622...	61	2	<Null>	<Null>	<Null>
845	1	744	197283622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	<Null>	197283622...	61	2	<Null>	<Null>	<Null>
846	1	744	197283622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	<Null>	1489563917	61	<Null>	<Null>	0	<Null>
847	1	744	197283622...	shirleytan	Shirley Tan	<Null>	<Blob Data>	<Null>	1489563951	61	<Null>	<Null>	0	<Null>
848	1	744	197283622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	<Null>	197283622...	61	2	<Null>	<Null>	<Null>
855	1	744	197283622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	<Null>	1489628568	61	<Null>	<Null>	0	<Null>
856	1	744	197283622...	shirleytan	Shirley Tan	<Null>	<Blob Data>	<Null>	1489628578	61	<Null>	<Null>	0	<Null>
857	1	744	197283622...	livejarychng	Jaryl Chng	<Null>	<Blob Data>	<Null>	1489628587	61	<Null>	<Null>	0	<Null>
858	1	744	197283622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	<Null>	197283622...	61	2	<Null>	<Null>	<Null>
859	1	744	197283622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	<Null>	197283622...	61	2	<Null>	<Null>	<Null>
860	1	744	197283622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	<Null>	1489631416	61	2	<Null>	<Null>	<Null>

Hex

00000000 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F ...

283 Bytes Ln 1 Col 1

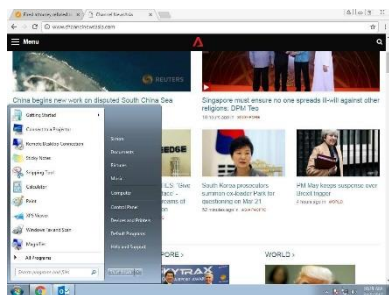


Pictures of interests

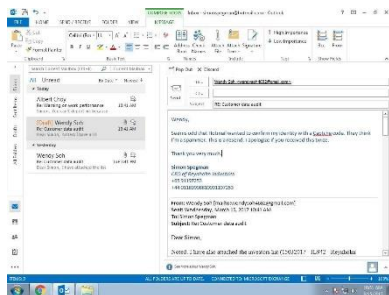
i1^cimgpsh_orig.png



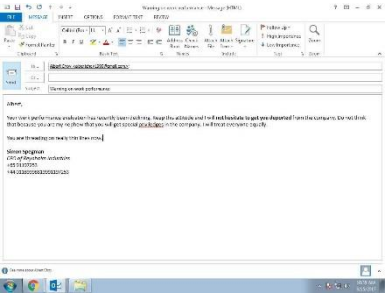
ABXzidWS.jpeg



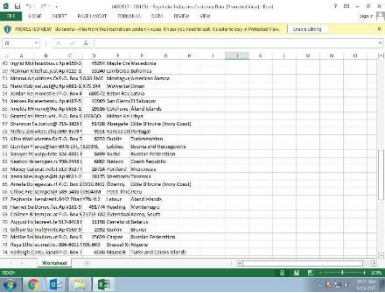
grMyydzw.jpeg



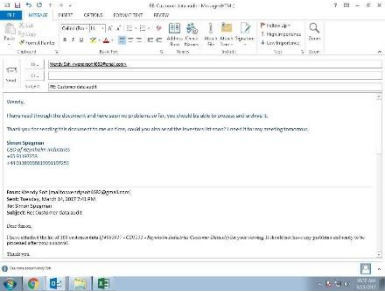
NglbWxjz.jpeg



TakHuvGO.jpeg



zrpffDcf.jpeg



Appendices



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	64
Granularity	
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

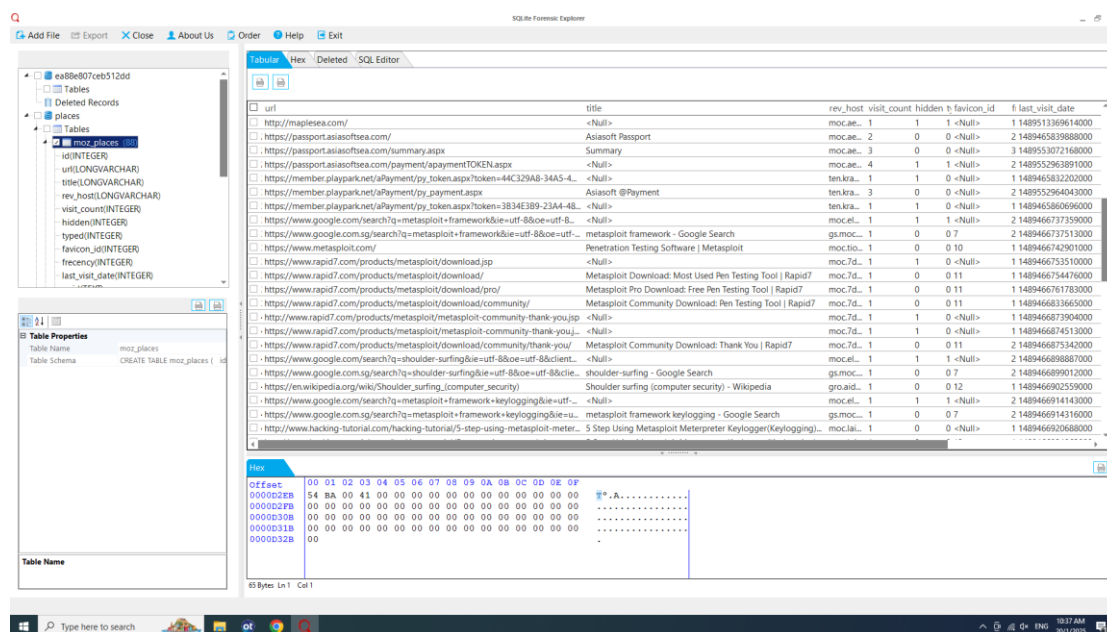
Notable files

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



Add File **Export** **X Close** **About Us** **Order** **Help** **Edit** **Delete** **SQL Editor**

Tables **Hex** **Deleted** **SQL Editor**

- ea8be07ceb512dd
 - Tables
 - Deleted Records
 - places
 - Tables
 - moz_places
 - id(INTEGER)
 - url(LONGVARCHAR)
 - title(LONGVARCHAR)
 - rev_host(LONGVARCHAR)
 - visit_count(INTEGER)
 - hidden(INTEGER)
 - types(INTEGER)
 - favicon_id(INTEGER)
 - frequency(INTEGER)
 - last_visit_date(INTEGER)

url	title	rev_host	visit_count	hidden	favicon_id	f_last_visit_date
https://www.hacking-tutorial.com/hacking-mozilla-firefox-3-5-to-3-6-range-vulnerability	Hacking Mozilla Firefox 3.5 to 3.6 range Vulnerability	moc.lac..	1	0	13	14895476569000
https://localhost:3790/login	Metasploit	tsloh.ac..	1	0	15	2489543206360000
https://localhost:3790/workspaces/1	Metasploit - Overview	tsloh.ac..	1	0	15	1489545758650000
https://localhost:3790/workspaces/1/sessions	Metasploit - Sessions	tsloh.ac..	1	0	15	1489545761334000
https://localhost:3790/workspaces/1/sessions/2	Metasploit - Session 2	tsloh.ac..	2	0	15	1489546038578000
https://localhost:3790/host/1	Metasploit - 172.20.39.128 - SIMON-PC	tsloh.ac..	1	0	15	148954547720730000
https://localhost:3790/workspaces/1/session/history/1	Metasploit - Session history for 1	tsloh.ac..	1	0	15	1489545759470000
https://youtube.com/	YouTube	moc.cb..	1	1	<Null>	1489547955396000
https://www.youtube.com/results?search_query=maple+mmv	maple mmv - YouTube	moc.cb..	1	0	16	2489547195410000
https://www.youtube.com/watch?v=DnJZMN5ySjI	MMV : Tong Hua (童話) Fairytale - YouTube	moc.cb..	1	0	16	1489547199780000
https://www.youtube.com/results?search_query=maple+legends+1	Maple legends 1 - YouTube	moc.cb..	1	0	16	1489547204318000
https://www.youtube.com/watch?v=_0dUXVTX9w	Maple Legends Episode 1 - YouTube	moc.cb..	1	0	16	1489547513610000
https://www.youtube.com/watch?v=OEP_cot6lBAg	Maple Legends Episode 2 - YouTube	moc.cb..	1	0	16	1489547960200000
https://passport.asiafirefly.com/login.aspx?ReturnUrl=/%2tpayment/%2tpaymen..	AsiaSoft Passport	moc.ca..	1	0	<Null>	2489552393748000
https://member.playpark.net/apiPayment/vr_token.aspx?token=CASF9E1C-36B1A..	<Null>	ten.kra..	1	1	<Null>	1489552604005000
https://member.playpark.net/apiPayment/payment/vr_paypal.aspx?action=purchase	<Null>	ten.kra..	1	1	<Null>	1489552994198000
https://www.paypal.com/cgi-bin/webscr?cmd=_express-checkout&token=EC-1YS..	PayPal	moc.la..	1	0	17	1489552996260000
https://www.paypal.com/cgi-bin/webscr?cmd=_express-checkout&token=EC-1YS..	PayPal	moc.la..	1	0	17	1489552998444000
https://www.paypal.com/cgi-bin/webscr?cmd=_express-checkout&token=EC-1YS..	PayPal Checkout - Log In	moc.la..	1	0	<Null>	1489552998587000
https://passport.asiafirefly.com/AccountModule/ACashHistory.aspx	AsiaSoft Passport	moc.ca..	1	0	<Null>	1489553077881000
http://go.microsoft.com/fwlink/?LinkId=691046	<Null>	moc.cf..	1	0	<Null>	14896612178120000
https://support.office.com/article/982cb2b3c-b9ad-48bc-ac53-c6b136e4405b	<Null>	moc.ec..	1	1	<Null>	1489663127505000

Table Properties

Table Name: moz_places
CREATE TABLE moz_places (id

```

id INTEGER NOT NULL PRIMARY KEY,
url LONG VARCHAR(255),
title LONG VARCHAR(255),
rev_host LONG VARCHAR(255),
visit_count INTEGER(4),
hidden INTEGER(1),
types INTEGER(1),
favicon_id INTEGER(10),
frequency INTEGER(1),
last_visit_date INTEGER(10)
);
    
```

Table Name

85 Bytes | Len 1 | Col 1

Date of Report: 20/01/25

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

The screenshot displays the SQL Explorer interface with a table of chat messages. The table has columns: id, is_permanent, convo_id, chatname, author, from_dispan, author_was, li_guid, dialog_partne, timestamp, type, sending_status, option_bits, consumption, and edited. The data rows show messages from jaryl chng, shirley tan, and alicia tan. The hex view at the bottom shows the raw data for the selected row.

id	is_permanent	convo_id	chatname	author	from_dispan	author_was	li_guid	dialog_partne	timestamp	type	sending_status	option_bits	consumption	edited
832	1	744	197283c622...	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	197283c622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	<Null>	197283c622...	61	2	<Null>	<Null>	<Null>
836	1	744	197283c622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	<Null>	197283c622...	61	2	<Null>	<Null>	<Null>
837	1	733	#livealiciatan	livealiciatan	Alicia Tan	<Null>	<Blob Data>	livejarylchng	1489553744	61	2	<Null>	0	<Null>
838	1	733	#livealiciatan	livealiciatan	Alicia Tan	<Null>	<Blob Data>	livejarylchng	1489553748	61	2	<Null>	0	<Null>
839	1	733	#livealiciatan	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	197283c622...	livejarylchng	Jaryl Chng	<Null>	<Blob Data>	<Null>	1489553775	61	<Null>	<Null>	0	<Null>
842	1	744	197283c622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	197283c622...	1489563865	61	2	<Null>	<Null>	<Null>
843	1	744	197283c622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	197283c622...	1489563868	61	2	<Null>	<Null>	<Null>
844	1	744	197283c622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	197283c622...	1489563885	61	2	<Null>	<Null>	<Null>
845	1	744	197283c622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	197283c622...	1489563892	61	2	<Null>	<Null>	<Null>
846	1	744	197283c622...	livejarylchng	Jaryl Chng	<Null>	<Blob Data>	<Null>	1489563917	61	<Null>	<Null>	0	<Null>
847	1	744	197283c622...	shirleytan	Shirley Tan	<Null>	<Blob Data>	<Null>	1489563951	61	<Null>	<Null>	0	<Null>
854	1	744	197283c622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	197283c622...	1489628505	61	2	<Null>	<Null>	<Null>
855	1	744	197283c622...	livejarylchng	Jaryl Chng	<Null>	<Blob Data>	<Null>	1489628568	61	<Null>	<Null>	0	<Null>
856	1	744	197283c622...	shirleytan	Shirley Tan	<Null>	<Blob Data>	<Null>	1489628578	61	<Null>	<Null>	0	<Null>
857	1	744	197283c622...	livejarylchng	Jaryl Chng	<Null>	<Blob Data>	<Null>	1489628587	61	<Null>	<Null>	0	<Null>
858	1	744	197283c622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	197283c622...	1489631404	61	2	<Null>	<Null>	<Null>
859	1	744	197283c622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	197283c622...	1489631408	61	2	<Null>	<Null>	<Null>
860	1	744	197283c622...	livealiciatan	Alicia Tan	<Null>	<Blob Data>	197283c622...	1489631416	61	2	<Null>	<Null>	<Null>

SQLite Forensic Explorer

File Edit View Options Help

Table Properties

Table Name: Messages

Table Schema: CREATE TABLE Messages (id INT, is_permanent BOOLEAN, convo_id INT, chatname TEXT, author TEXT, from_display_name TEXT, author_was_li BOOLEAN, guid TEXT, dialog_partner TEXT, timestamp INT, type TEXT, sending_status TEXT, option_bits TEXT, consumption TEXT, edited TEXT)

Table Name

id	is_permanent	convo_id	chatname	author	from_display_name	author_was_li	guid	dialog_partner	timestamp	type	sending_status	option_bits	consumption	edited
832	1	744	197283c622..livejanychnq	Jaryl Chng	<Null>	<Null>	<Null>	<Null>	148953674	61	<Null>	<Null>	0	<Null>
833	1	744	197283c622..livejanychnq	Jaryl Chng	<Null>	<Null>	<Null>	<Null>	148953690	61	<Null>	<Null>	0	<Null>
834	1	744	197283c622..livejanychnq	Jaryl Chng	<Null>	<Null>	<Null>	<Null>	148953699	61	<Null>	<Null>	0	<Null>
835	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	148953710	61	2	<Null>	<Null>	<Null>
836	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	148953714	61	2	<Null>	<Null>	<Null>
837	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	148953744	61	2	<Null>	<Null>	<Null>
838	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	148953748	61	2	<Null>	<Null>	<Null>
839	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	148953754	61	2	<Null>	<Null>	<Null>
840	1	744	197283c622..livejanychnq	Jaryl Chng	<Null>	<Null>	<Null>	<Null>	148953770	61	<Null>	<Null>	0	<Null>
841	1	744	197283c622..livejanychnq	Jaryl Chng	<Null>	<Null>	<Null>	<Null>	148953775	61	<Null>	<Null>	0	<Null>
842	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	148953865	61	2	<Null>	<Null>	<Null>
843	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	148953868	61	2	<Null>	<Null>	<Null>
844	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	148953885	61	2	<Null>	<Null>	<Null>
845	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	148953892	61	2	<Null>	<Null>	<Null>
846	1	744	197283c622..livejanychnq	Jaryl Chng	<Null>	<Null>	<Null>	<Null>	148953917	61	<Null>	<Null>	0	<Null>
847	1	744	197283c622..livejanychnq	Shirley Tan	<Null>	<Null>	<Null>	<Null>	148953951	61	<Null>	<Null>	0	<Null>
848	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	148962805	61	2	<Null>	<Null>	<Null>
854	1	744	197283c622..livejanychnq	Jaryl Chng	<Null>	<Null>	<Null>	<Null>	148962858	61	<Null>	<Null>	0	<Null>
856	1	744	197283c622..livejanychnq	Shirley Tan	<Null>	<Null>	<Null>	<Null>	148962858	61	<Null>	<Null>	0	<Null>
857	1	744	197283c622..livejanychnq	Jaryl Chng	<Null>	<Null>	<Null>	<Null>	148962887	61	<Null>	<Null>	0	<Null>
858	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	148963104	61	2	<Null>	<Null>	<Null>
859	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	148963108	61	2	<Null>	<Null>	<Null>
860	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	148963146	61	2	<Null>	<Null>	<Null>

Hex

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 19 72 83 c6 22 05 50 40 00 00 B1 9A 37 37 61 62 34 30 34 66 31 34 32 31 39 64 36 62 77 ab 40 4f 142 19 d6 b cc28 thread skyp eX e, = lme to bu y some Garba tle kets and cubea l... .00e... .20M% 20M% .20M%

38 Bytes Len 1 Col 1

SQLite Forensic Explorer

File Edit View Options Help

Table Properties

Table Name: Messages

Table Schema: CREATE TABLE Messages (id INT, is_permanent BOOLEAN, convo_id INT, chatname TEXT, author TEXT, from_display_name TEXT, author_was_li BOOLEAN, guid TEXT, dialog_partner TEXT, timestamp INT, type TEXT, sending_status TEXT, option_bits TEXT, consumption TEXT, edited TEXT)

Table Name

id	is_permanent	convo_id	chatname	author	from_display_name	author_was_li	guid	dialog_partner	timestamp	type	sending_status	option_bits	consumption	edited
762	1	744	197283c622..livejanychnq	Shirley Tan	<Null>	<Null>	<Null>	<Null>	1489461704	61	<Null>	<Null>	0	<Null>
763	1	744	197283c622..livejanychnq	Shirley Tan	<Null>	<Null>	<Null>	<Null>	1489461749	61	<Null>	<Null>	0	<Null>
764	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	1489461767	61	2	<Null>	<Null>	<Null>
765	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	1489461779	61	2	<Null>	<Null>	<Null>
766	1	744	197283c622..livejanychnq	Jaryl Chng	<Null>	<Null>	<Null>	<Null>	1489461802	61	<Null>	<Null>	0	<Null>
767	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	1489461821	61	2	<Null>	<Null>	<Null>
768	1	744	197283c622..livejanychnq	Shirley Tan	<Null>	<Null>	<Null>	<Null>	1489461828	61	<Null>	<Null>	0	<Null>
769	1	744	197283c622..livejanychnq	Shirley Tan	<Null>	<Null>	<Null>	<Null>	1489461833	61	<Null>	<Null>	0	<Null>
770	1	744	197283c622..livejanychnq	Shirley Tan	<Null>	<Null>	<Null>	<Null>	1489461854	61	<Null>	<Null>	0	<Null>
771	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	1489461903	61	2	<Null>	<Null>	<Null>
772	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	1489461908	61	<Null>	<Null>	<Null>	<Null>
773	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	1489465891	61	2	<Null>	<Null>	<Null>
774	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	1489465909	61	2	<Null>	<Null>	<Null>
775	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	1489465924	61	2	<Null>	<Null>	<Null>
776	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	1489465932	61	2	<Null>	<Null>	<Null>
777	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	1489465938	61	2	<Null>	<Null>	<Null>
778	1	744	197283c622..livejanychnq	Jaryl Chng	<Null>	<Null>	<Null>	<Null>	1489465958	61	<Null>	<Null>	0	<Null>
779	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	1489465988	61	2	<Null>	<Null>	<Null>
780	1	744	197283c622..livejanychnq	Jaryl Chng	<Null>	<Null>	<Null>	<Null>	1489466024	61	<Null>	<Null>	0	<Null>
781	1	744	197283c622..livejanychnq	Jaryl Chng	<Null>	<Null>	<Null>	<Null>	1489466035	61	<Null>	<Null>	0	<Null>
782	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	1489466079	61	2	<Null>	<Null>	<Null>
783	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	1489466103	61	2	<Null>	<Null>	<Null>
784	1	744	197283c622..livejanychnq	Alicia Tan	<Null>	<Null>	<Null>	<Null>	1489466118	61	2	<Null>	<Null>	<Null>

Hex

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 72 6F 6D 20 74 68 61 74 20 43 45 4F 20 74 68 61 74 20 79 6F 75 20 6D 65 6E 74 69 6F 6E 65 64 20 69 6E 20 67 61 6D 65 20 74 68 61 74 20 6C 69 76 65 73 20 77 69 74 68 20 79 6F 75 2F 20 49 26 61 70 6F 73 3B 6D 20 73 75 72 65 20 68 65 20 77 6F 6E 26 61 70 6F 73 3B 74 20 6E 6F 74 69 63 65 20 3C 73 73 20 74 79 65 30 22 74 6F 6E 67 75 65 6F 75 74 22 3E 5A 50 3C 2F 73 73 3E 03 04 01 5A rom that CEO tha t you mentioned in game that liv es with you? 144 posy sure he wd nnapost notice ces type"longue out"> PC/aa...>

38 Bytes Len 1 Col 1

Add File Export Close About Us Order Help Exit

SQL Editor

places

main

Tables

DoMeta (8)

AppSchemaVersion (1)

Contacts (3)

LegacyMessages (0)

Accounts (1)

Transfers (0)

Voicemails

Chats

Messages (16)

ContactGroups

Videos

SMSes

ChatMembers

Tabular Hex Deleted SQL Editor

id	is_persistent	conv_id	chatname	author	from_dispan	author_was_li_id	dialog_partne	timestamp	type	sending_status	option_bits	consumption	edited
768	1	744	197283c22...	shirleytan	Shirley Tan	<Null>	<Blob Data>	1489461828	61	<Null>	<Null>	0	<Null>
769	1	744	197283c22...	shirleytan	Shirley Tan	<Null>	<Blob Data>	1489461833	61	<Null>	<Null>	0	<Null>
770	1	744	197283c22...	shirleytan	Shirley Tan	<Null>	<Blob Data>	1489461854	61	<Null>	<Null>	0	<Null>
771	1	744	197283c22...	liveicalicatan	Alicia Tan	<Null>	<Blob Data>	197283c622...	61	2	<Null>	<Null>	<Null>
772	1	744	197283c22...	liveicalicatan	Alicia Tan	<Null>	<Blob Data>	1489461908	61	2	<Null>	<Null>	<Null>
773	1	744	197283c22...	liveicalicatan	Alicia Tan	<Null>	<Blob Data>	197283c622...	61	2	<Null>	<Null>	<Null>
774	1	744	197283c22...	liveicalicatan	Alicia Tan	<Null>	<Blob Data>	197283c622...	61	2	<Null>	<Null>	<Null>
775	1	744	197283c22...	liveicalicatan	Alicia Tan	<Null>	<Blob Data>	197283c622...	61	2	<Null>	<Null>	<Null>
776	1	744	197283c22...	liveicalicatan	Alicia Tan	<Null>	<Blob Data>	197283c622...	61	2	<Null>	<Null>	<Null>
777	1	744	197283c22...	liveicalicatan	Alicia Tan	<Null>	<Blob Data>	197283c622...	61	2	<Null>	<Null>	<Null>
778	1	744	197283c22...	liveicalicatan	Jaryl Chng	<Null>	<Blob Data>	1489465958	61	<Null>	<Null>	0	<Null>
779	1	744	197283c22...	liveicalicatan	Alicia Tan	<Null>	<Blob Data>	197283c622...	61	2	<Null>	<Null>	<Null>
780	1	744	197283c22...	liveicalicatan	Jaryl Chng	<Null>	<Blob Data>	1489466024	61	<Null>	<Null>	0	<Null>
781	1	744	197283c22...	liveicalicatan	Jaryl Chng	<Null>	<Blob Data>	1489466035	61	<Null>	<Null>	0	<Null>
782	1	744	197283c22...	liveicalicatan	Alicia Tan	<Null>	<Blob Data>	197283c622...	61	2	<Null>	<Null>	<Null>
783	1	744	197283c22...	liveicalicatan	Alicia Tan	<Null>	<Blob Data>	197283c622...	61	2	<Null>	<Null>	<Null>
784	1	744	197283c22...	liveicalicatan	Alicia Tan	<Null>	<Blob Data>	197283c622...	61	2	<Null>	<Null>	<Null>
785	1	744	197283c22...	shirleytan	Shirley Tan	<Null>	<Blob Data>	1489466138	61	<Null>	<Null>	0	<Null>
786	1	744	197283c22...	shirleytan	Shirley Tan	<Null>	<Blob Data>	1489466153	61	<Null>	<Null>	0	<Null>
787	1	744	197283c22...	liveicalicatan	Jaryl Chng	<Null>	<Blob Data>	1489466215	61	<Null>	<Null>	0	<Null>
788	1	733	liveicalicatan	liveicalicatan	Jaryl Chng	<Null>	<Blob Data>	1489466262	61	<Null>	<Null>	0	<Null>
789	1	733	liveicalicatan	liveicalicatan	Jaryl Chng	<Null>	<Blob Data>	1489466273	61	<Null>	<Null>	0	<Null>
790	1	744	197283c22...	liveicalicatan	Jaryl Chng	<Null>	<Blob Data>	1489466294	61	<Null>	<Null>	0	<Null>

16

Messages

Table Schema

CREATE TABLE Messages (id NV

Tabular Hex Deleted SQL Editor

id	is_persistent	conv_id	chatname	author	from_dispan	author_was_li_id	dialog_partne	timestamp	type	sending_status	option_bits	consumption	edited
768	1	744	197283c22...	shirleytan	Shirley Tan	<Null>	<Blob Data>	1489461828	61	<Null>	<Null>	0	<Null>
769	1	744	197283c22...	shirleytan	Shirley Tan	<Null>	<Blob Data>	1489461833</					

Add File Export Close About Us Order Help Exit

SQLD Forensic Explorers

places
main

Tables
 # Meta (0)
 AppSchemaVersion (1)
 Contacts (3)
 LegatoMessages (0)
 Accounts (0)
 Transfers (0)
 Voicemails
 Chats
 Messages (10)
 ContactGroups
 Videos
 SMSes
 ChatMembers

Tabular Hex Deleted SQL Editor

id	is_permanent	conv_id	chatname	author	from_dispan	author_was_li	id	dialog_partne	timestamp	type	sending_status	option_bits	consumption	edited...
780	1	744	197283622...	liveyarching	Jaryl Cng	<Null>	<Blob Data>	<Null>	1949466024	61	<Null>	<Null>	0	<Null>
781	1	744	197283622...	liveyarching	Jaryl Cng	<Null>	<Blob Data>	<Null>	1949466035	61	<Null>	<Null>	0	<Null>
782	1	744	197283622...	liveyarching	Alicia Tan	<Null>	<Blob Data>	197283622...	1949466079	61	2	<Null>	<Null>	<Null>
783	1	744	197283622...	liveyarching	Alicia Tan	<Null>	<Blob Data>	197283622...	1949466103	61	2	<Null>	<Null>	<Null>
784	1	744	197283622...	liveyarching	Alicia Tan	<Null>	<Blob Data>	197283622...	1949466118	61	2	<Null>	<Null>	<Null>
785	1	744	197283622...	shirleytan	Shirley Tan	<Null>	<Blob Data>	<Null>	1949466138	61	<Null>	<Null>	0	<Null>
786	1	744	197283622...	shirleytan	Shirley Tan	<Null>	<Blob Data>	<Null>	1949466153	61	<Null>	<Null>	0	<Null>
787	1	744	197283622...	liveyarching	Jaryl Cng	<Null>	<Blob Data>	<Null>	1949466215	61	<Null>	<Null>	0	<Null>
788	1	733	liveyarching	liveyarching	Jaryl Cng	<Null>	<Blob Data>	<Null>	1949466262	61	<Null>	<Null>	0	<Null>
789	1	733	liveyarching	liveyarching	Jaryl Cng	<Null>	<Blob Data>	<Null>	1949466273	61	<Null>	<Null>	0	<Null>
790	1	744	197283622...	liveyarching	Jaryl Cng	<Null>	<Blob Data>	<Null>	1949466294	61	<Null>	<Null>	0	<Null>
791	1	744	197283622...	shirleytan	Shirley Tan	<Null>	<Blob Data>	<Null>	1949466310	61	<Null>	<Null>	0	<Null>
792	1	744	197283622...	liveyarching	Alicia Tan	<Null>	<Blob Data>	197283622...	1949466315	61	2	<Null>	<Null>	<Null>
793	1	733	#livearcat...	liveyarching	Alicia Tan	<Null>	<Blob Data>	liveyarching	1949466362	61	2	<Null>	<Null>	<Null>
794	1	733	#livearcat...	liveyarching	Alicia Tan	<Null>	<Blob Data>	liveyarching	1949466371	61	2	<Null>	<Null>	<Null>
795	1	744	197283622...	liveyarching	Jaryl Cng	<Null>	<Blob Data>	<Null>	1949466404	61	<Null>	<Null>	0	<Null>
796	1	744	197283622...	shirleytan	Shirley Tan	<Null>	<Blob Data>	<Null>	1949466431	61	<Null>	<Null>	0	<Null>
797	1	733	liveyarching	liveyarching	Jaryl Cng	<Null>	<Blob Data>	<Null>	1949466476	61	<Null>	<Null>	0	<Null>
798	1	733	liveyarching	liveyarching	Jaryl Cng	<Null>	<Blob Data>	<Null>	1949466533	61	<Null>	<Null>	0	<Null>
799	1	733	liveyarching	liveyarching	Jaryl Cng	<Null>	<Blob Data>	<Null>	1949466541	61	<Null>	<Null>	0	<Null>
800	1	733	liveyarching	liveyarching	Jaryl Cng	<Null>	<Blob Data>	<Null>	1949466556	61	<Null>	<Null>	0	<Null>
801	1	733	liveyarching	liveyarching	Jaryl Cng	<Null>	<Blob Data>	<Null>	1949466581	61	<Null>	<Null>	0	<Null>
802	1	733	liveyarching	liveyarching	Jaryl Cng	<Null>	<Blob Data>	<Null>	1949466612	61	<Null>	<Null>	0	<Null>

Hex


```

Offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000B5516 44 83 71 C3 57 68 82 86 58 C7 74 D5 3D 5A 68 C1
000B5526 70 74 77 61 79 2C 20 77 65 60 68 65 20 68 65 20 6C
000B5536 69 67 73 20 69 6E 20 74 69 20 68 69 73 20 49 63
000B5546 42 43 20 61 63 63 6F 75 6E 74 2C 20 79 6F 75 20
000B5556 63 61 62 60 63 61 70 74 75 72 65 20 68 69 73 20
000B5566 75 75 65 72 6E 60 65 20 61 6E
```

Date of Report: 20/01/25

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

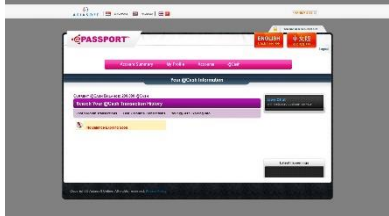
File Created 15/03/17 12:50:00 PM

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.

