

**Digital Forensics**

Year 2/3 (2022/23), Semester 4/6

**SCHOOL OF INFOCOMM TECHNOLOGY**

Diploma in Information Technology

Diploma in Cybersecurity & Digital Forensics

**Examiner Report (Assignment)**

**Duration:** Weeks 3 - 17

**Individual/Team/Both:** Team

**Deadline: 12 Feb 2023, 23:59hrs (Sunday)**

(For each day past the deadline, 10% of the total possible marks will be deducted up to a maximum of 7 calendar days, after which a zero mark is given.)

|  |  |
| --- | --- |
| **Student ID** | **S10223468, S10223426** |
| **Name** | **Leroi June Yen Hao, Lor Jing Xiang Eugene** |
| **Module Group** | **T02** |
| **Grade** |  |

Table of Contents

[1.0 Purpose and Organization of this Report 2](#_Toc127127591)

[2.0 Executive Summary 3](#_Toc127127592)

[3.0 Forensic Examination on External Storage Devices 4](#_Toc127127593)

[3.1.1 Observation 1 4](#_Toc127127594)

[3.1.2 Observation 2 5](#_Toc127127595)

[3.1.3 Analysis and Opinion 1 5](#_Toc127127596)

[3.2.1 Observation 3 6](#_Toc127127597)

[3.2.2 Observation 4 6](#_Toc127127598)

[3.2.3 Observation 5 6](#_Toc127127599)

[3.2.4 Analysis and Opinion 2 6](#_Toc127127600)

[3.3.1 Observation 6 7](#_Toc127127601)

[3.3.2 Analysis and Opinion 3 7](#_Toc127127602)

[Examiner Notes 8](#_Toc127127603)

[Appendix A 9](#_Toc127127604)

[Appendix B 9](#_Toc127127605)

[Appendix C 14](#_Toc127127606)

[Appendix D 16](#_Toc127127607)

[Appendix E 17](#_Toc127127608)

[Appendix F 18](#_Toc127127609)

[RTF Report 20](#_Toc127127610)

# Purpose and Organization of this Report

* 1. This computer forensics report states the key observations, analysis and opinions from the work performed by Leroi June Yen Hao and Lor Jing Xiang Eugene. The work involves the review of the forensics image of the hard disk drive of the exhibit 20170316-001-E02HD1 belonging to the individual Alicia Tan Hui Jing.
  2. Observations and discovery are made on data on the forensics image of the hard disk drive 20170316-001-E02HD1. Our observations, analysis and opinions are organized into different sections and sub-titles for the ease of reading.
  3. Section 2 contains the executive summary on our opinions from the forensics review. The subsequent sections describe the observations and analysis of relevant data discovered during the review.
  4. The sub-titles in the sections are:
     1. Observation: describes the data noted during the reviews; and
     2. Analysis and Opinion describes our analysis and opinions on a specific set of data.
  5. Appendices referred to in this report are enclosed at the last section of this report.

# 2.0 Executive Summary

On 30 January 2022, we were informed to handle case number 20170316-001. Simon Spegman reported an unauthorised bank transfer of SGD $2000 in his OCBC bank account history and the recipient of the transaction was traced to the tenant of his apartment, Alicia Tan Hui Jing. After police interrogation Alicia denied any wrongdoing and insists that Simon has transferred the money on his own accord. When looking through the bank’s online banking logs, it has been verified that the transaction was made from Simon’s apartment’s public IP address. Hence, both Simon and Alicia’s personal computers in the apartment has been seized for investigation.

We were instructed to do an analysis on the laptop to determine the following:

To establish if Alicia was the one responsible for the unauthorised bank transfer of SGD $2000 from Simon’s Bank; and

Whether sexual harassment has been committed by Simon.

Back in the lab, both computers we acquired and forensic images of the computer have been created by him for further investigation. He examined Simon’s image file (Simon.Ex01) and sent me Alicia’s image file (Alicia.Ex01) to examine and help solve the case.

A forensics analysis was done on the image of the laptop for evidence to support claims in court. The analysis was done on an extracted bit copy image of the hard drive from the computer with serial number Alicia.Ex01 and a verified hash of 132a9f27dc3a02f90d64f50b12b797c16f74089b.

Based on the data reviewed and analysed on exhibit 20170316-001-E02HD1, which is outlined in section 3, it is highly probable that Alicia has broken the laws of unauthorised access to computer material and access with intent to commit or facilitate commission of offence. All observations and opinions will be backed up by evidence within the appendix of this document.

# 3.0 Forensic Examination on External Storage Devices

### 3.1.1 Observation 1

We have analysed the contents within the recycle bin of exhibit 20170316-001-E02HD.

We noted that there was an image file with the subject title “20170315\_100927.jpg” that was created 15/03/17 10:57:44 AM. This file was in the directory of “Alicia\$RECYCLE.BIN\S-1-5-21-4134190322-1791598225-2319710166-1002”. Upon further analysis, the file header was mismatched. It was determined that the file was a renamed mp4 file. When renaming and viewing the contents of “20170315\_100927.mp4”, a video is shown of someone recording the log in process of another. A screenshot of this photo can be found in [Appendix A](#_Appendix_A_1)

### 3.1.2 Observation 2

In the file directory of “Alicia\Users\Alicia\AppData\Roaming\Skype\live#3aaliciatanhuijing\main”, we were able to recover the main.db database. When viewing the contents of the database, we are able to see a conversation between Alicia and an individual named Jaryl with the username “live:jarylchng”. The contents of these messages include topics of hacking and methods of doing so. One of the methods mentioned was shoulder-surfing. The user also had told Alicia about a tool called Metasploit and how it could be a way to capture Simon’s OCBC username and pin number. The full contents of the extracted Skype chat logs from main.db can be found in [Appendix B.](#_Firefox_Thumbnails)

## 3.1.3 Analysis and Opinion 1

Based on observation 1 and 2, we have probable evidence that Jaryl had conspired with Alicia and gave her the idea of performing shoulder surfing in order to obtain the computer password of Simon’s personal computer. It is also likely that the Alicia had attempted to hide and obfuscate the video of Simon entering in his password as the file extension of the video had been renamed from MP4 to JPG, a hidden file attribute had been set and the file was located in the recycling bin folder, indicating that it had been deleted.

### 3.2.1 Observation 3

We noted that in the file directory of “Alicia\Users\Alicia\AppData\Local\Mozilla\Firefox\Profiles\lx5oaqu6.default\thumbnails”, there were multiple pictures of Metasploit, an exploitation tool and ways of using Metasploit for key logging. The screenshots show the Metasploit login page, a search about the Metasploit framework, and the main page of Metasploit, There was also two photos relating to shoulder-surfing. These images can be found in [Appendix C](#_Firefox_Cache).

### 3.2.2 Observation 4

In the file directory of “Alicia\Users\Alicia\AppData\Local\Mozilla\Firefox\Profiles\lx5oaqu6.default\cache2\entries”, there was a recording of the phrase “Dumping captured keystrokes...ocbc.com.sg” and “Dumping captured keystrokes...7566721999811”. The file was created on 15/03/17 10:42:45 AM. This can be found in [Appendix D](#_Appendix_C).

### 3.2.3 Observation 5

In the file directory of “Alicia\$RECYCLE.BIN\S-1-5-21-4134190322-1791598225-2319710166-1002\”, a txt file was recovered with the Simon’s OCBC bank number along with a 6 digit pin which is likely the pin number of the bank account. We are also able to see the phrase “abc12345”. The file was created on 15/03/17 10:54:38 AM. This text file can be found in [Appendix E](#_Appendix_D).

## 3.2.4 Analysis and Opinion 2

Based on the observation 3, 4 and 5, it is extremely likely that Alicia has used Metasploit on her personal computer to gain access of Simon’s bank account. Using a combination of Metasploit and shoulder surfing, Alicia would be able to gain unauthorised access to Simon’s credentials to both his personal computer and bank account. We can also identify a timeline from the creation date of the files. In observation 4, the keystroke captured was dated on 15/03/17 10:42:45 AM.. In observation 5, which talks about the recording of credentials into a text file, the creation of the file is 10:54:38 A.M. of the same day. This is likely Alicia first getting information of Simon’s bank credentials and recording it into the text file.

### 3.3.1 Observation 6

We noted that in the file directory “Alicia\Users\Alicia\Pictures”, there was a picture of a transaction in @Cash, a currency in maple story. The picture was created on 15/03/17 12:46:08 PM. This date is after the creation of the text file in observation 5. This picture can be found in [Appendix F](#_Appendix_F).

## 3.3.2 Analysis and Opinion 3

Based on observation 6 and 5, it is highly likely that Alicia has gained unathorised access to the credentials of Simon’s bank account details and have made a transfer of funds to her own account to buy @Cash, the currency in maple story. The creation of the files supports these claims, with the credentials gained before the purchase of @Cash was performed.

# Examiner Notes

Data Extraction was done on following directories:

* Alicia\metasploit\postgresql\data\base (Metasploit postgresql database)
* Alicia\Users\Alicia\Appdata\Local\Mozilla\Firefox\Profiles\lx5oaqu6.default\cache2\entries (Firefox cache)
* Alicia\Users\Alicia\Appdate\Local\Mozilla\Firefox\Profiles\lx5oaqu6.default\thumbnails (Firefox thumbnails)
* Alicia\$RECYCLE.BIN\ (Alicia recycle bin)

The following files were extracted to analyse using Sqlite:

* Alicia\Users\Alicia\Appdata\Roaming\Mozilla\Firefox\Profiles\lx5oaqu6.default\places.sqlite (Firefox places.sqlite)
* Alicia\Users\Alicia\Appdata\Roaming\Mozilla\Firefox\Profiles\lx5oaqu6.default\cookies.sqlite (Firefox cookies)
* Alicia\Users\Alicia\AppData\Roaming\Skype\live#3aaliciatanhuijing\main.db (Skype artifacts)

Keyword Searching was performed using the following keywords:

* aliciatanhuijing (Alicia’s Email and Skype address)
* aliciathj (Alicia’s Maplestory and Metasploit username)
* simonspegman (Simon’s Email address)
* 7566721 (Simon’s bank account number)

# Appendix A

2) 20170315\_100927.jpg

Item Path Alicia\$RECYCLE.BIN\S-1-5-21-4134190322-1791598225-2319710166-1002\20170315\_100927.jpg

File Created 15/03/17 10:57:44 AM

Last Written 15/03/17 10:09:35 AM

Last Accessed 15/03/17 10:57:44 AM

MD5 b11c1849c085dac85cd1365dbbe9a1bf

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.

A person using a computer

Description automatically generated with medium confidence

# Appendix B

11) 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

Start Sector 1,251,303

Sector offset 176

File Offset 704,176

Length 3,880

Comment Skype Conversation about hacking

%ôº ZÐR õ ZÐR õ ZÐR ô‚7†E, {7! L) G Ý#live:aliciatanhuij

ing/$live:jarylchng;8e75cb82b2111ff4live:aliciatanhuijingAlicia Tan 0 é¤ Ó,Â[‘} õÈó• ¬ïœP<

Ø Ë¼  Ž‚live:jarylchngXÈÉP= Haha, yeah, I definitely didn&apos;t resort to hacking to get

it. It&apos;s too risky for me.

%ô¹ ‚ÛNF

%ô¹ ZÐR ZÐR ZÐR

' í

ä ’ -

í o 5 ï Ì ê à Æ '  † + ))! L %

Ýlive:jarylchnglive:jarylchngJaryl Chng ÊUk,Ð M —Ü bU¹ 8 ¾E=ƒò¡0ýXÇs¡=Let me kn

ow. Z Ë ªp ZË P1 ZË P; ‚ † , ))! L ‚

Ýlive:jarylchnglive:jarylchngJaryl ChngüÌD ¥Ê< <G+÷¼ñpRktÀ¿«îvâ¹ :a±aéXÇs–=Hey, if y

ou want to actually do it, I can link you to some resources, of course I want some share o

f the acash <ss type="laugh">:D</ss> Z Ë ƒê ZË )û ZË )ö‚ † , m)! L 7

è19:7283c6220550477ab404f14219d6bcc2@thread.skypelive:jarylchngJaryl Chng3ÄxÊt»éíyäé~

¦P™nÁÚNºeŽ.¤PAo–øZ XÇsg=Yeah, it&apos;s just a joke, don&apos;t take it so seriously <ss

type="laugh">:D</ss> Z Ë Çy ZË m ZË m{^† + m## L m

è19:7283c6220550477ab404f14219d6bcc2@thread.skypeshirleyytanShirley Tan·üxÇó7°ë= ‡õE

ÎÆÿ$

Ý Â7è1—u`k0XÇs)=It looks like you are actually considering it D: Z Ë Û– ZË k ZË n‚ †

, m## L m

è19:7283c6220550477ab404f14219d6bcc2@thread.skypeshirleyytanShirley Tan[¦b%µ‚›A@Àã– #

æ‰H~8– fF\*O è!9 Ì\*XÇs =Hey Alicia, Jaryl is just joking, please don&apos;t take this serio

usly, if you get caught it won&apos;t be good Z Ë žL ZË D ZË Cø‚B† , m7! Lm

7 è19:7283c6220550477ab404f14219d6bcc2@thread.skypelive:aliciatanh

uijingAlicia Tan

ü ·KùR

@Ýó+’ÕÌð¹p©‚ µÍ—½Kárä19:7283c6220550477ab404f14219d6bcc2@thread.skypeXÇs = He did add me a

s a transfer recipient to return me some money before though... Hmm... iýçb ZË õ“ ZË õ“

ZË õu‚6† , m7! Lm  è19:7283c6220550477ab404f14219d6bcc

2@thread.skypelive:aliciatanhuijingAlicia Tan† Á¸SV9Û!PsžHøÞ‡:/© ?; –å ëšc19:7283c62205

50477ab404f14219d6bcc2@thread.skypeXÇr÷= But I doubt I can get my hands on his OCBC userna

me and pin number anyway 2 ·Ö ZË ¼Ð ZË ¼Ð ZË ¼Ñ‚z† , m7! Lm ‚'

è19:7283c6220550477ab404f14219d6bcc2@thread.skypelive:aliciatanhuijingAlicia TanI

Ô q&–N (5Ð x¯A†<üŠê ñþ—J$ÆYœä19:7283c6220550477ab404f14219d6bcc2@thread.skypeXÇrß= I thi

nk he keeps his iBanking token hidden in one of his drawers, I&apos;ve seen him put it the

re before. He checks his OCBC account everyday 3Ôwg ZË \ ZË \ ZË \‚ †

, m)! L I

è19:7283c6220550477ab404f14219d6bcc2@thread.skypelive:jarylchngJaryl Chngè9ŒUÚÏz$½'=

x í

ZùpFOb\_õS¿ä`ùUý XÇr³=But hey, it&apos;s just a joke, don&apos;t take it too seriously <ss

type="tongueout">:P</ss>. Z Ë · ZË ±¸ ZË ±±‚)† , m)! L }

è19:7283c6220550477ab404f14219d6bcc2@thread.skypelive:jarylchngJaryl Chng ›% "%­Ec5k

LSÔ ¼zÈl¶»–GÃ ‡KTÆ¶XÇr¨=Well, if you had access to his pin number and iBanking token, I t

hink it&apos;s possible to transfer money via e-banking Z Ë â ZË ˆG ZË ˆO‚a† , m7! L

m q è19:7283c6220550477ab404f14219d6bcc2@thread.skypelive:

aliciatanhuijingAlicia Tan­[ðx[p‚a‚Ð ’Hc›¦É³ÓvMñÅ Å'¹goÈ¯19:7283c6220550477ab404f14219d6b

cc2@thread.skypeXÇr„= No way! He doesn&apos;t keep cash around the house anyway... He most

ly uses his bank and credit to purchase items. ö¶¥ ZË ý\ ZË ý\ ZË ýL‚N†

, m)! L ‚G

è19:7283c6220550477ab404f14219d6bcc2@thread.skypelive:jarylchngJaryl Chngž 3Åžû–` = ß

›1ÚíÞ\EµK[€éMþüv€êXÇrf=Why not &quot;borrow&quot; some from that CEO that you mentioned

in game that lives with you? I&apos;m sure he won&apos;t notice <ss type="tongueout">:P</s

s> Z Ë ß

12) 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

Start Sector 1,251,336

Sector offset 178

File Offset 721,074

Length 2,442

Comment Conversation about Metasploit

Ýlive:jarylchnglive:jarylchngJaryl Chng©

(€ È9Dx— ÏAyû5z|‘I†ÖºÉQöï ñÊÏXÇu\*=Good luck! Z Ë ®¤ ZË!S ZË!S¡)†%+ ))! L C

Ýlive:jarylchnglive:jarylchngJaryl Chngt~‚:×ì4îb

Ñ tÞ×ÐÒ'ðb ˜‹»±f ZÚtXÇu&=It&apos;s quite fool proof. Z Ë ŸO ZË!E% ZË!E\*o†$, ))! L

M

Ýlive:jarylchnglive:jarylchngJaryl Chng#Â¨^tó–`ÇX@[& €…Q·û<z

Ýq ÃKÖ 4%XÇu =Just take your phone camera and go behind him when he types his password to

log in his computer. Z Ë w$ ZË! ZË! j†#+ {7! L) /

Ý#live:aliciatanhuijing/$live:jarylchng;8e75cb82b2111ff4live:aliciatanhuijingAlicia Tan\_iË

¬N ñÝ :‹ÌÆ“ˆÈynCéQè”Ë ÈÅ˜ ž´live:jarylchngXÇt÷= What&apos;s that?

%ô¶ â’·å

%ô¶ ZË Œ ZË Œ ZË Œ q†", ))! L Q

Ýlive:jarylchnglive:jarylchngJaryl Chngð`=&U×'ó}ví;– wæ¾\*“†âëxv@Sg<&—BXÇtô=But you m

ay have to have his computer password first though. Maybe you could try shoulder-surfing?

Z Ë Ö ZË |3 ZË {ýc†!, ))! L 5

Ýlive:jarylchnglive:jarylchngJaryl Chng ÿÙ®Êàƒ\* yfù í@#®Ÿ^Ÿ DƒqÃWh²†XÇtÕ=That way,

when he logs in to his OCBC account, you can capture his username and pin. Z Ë `f ZË

G ZË O^† , ))! L +

Ýlive:jarylchnglive:jarylchngJaryl Chng 1f§Bd—cýý ‘Ý¢l4í#Ö „'ÚyV­ŠÓËûRXÇt¼=Like you

login with psexec and you can run a keylogger on your victims computer Z Ë å ZË §¼ ZË

§Ã1† + ))! L S

Ýlive:jarylchnglive:jarylchngJaryl ChngL£¾ ˜¨nŽ1h—0IJ$’ ÷“ßCþ;+-/ µk ûbXÇt­=It has a

remote keylogger and stuff Z Ë ÁQ ZË g( ZË g [† , ))! L %

Ýlive:jarylchnglive:jarylchngJaryl ChngªI‰­÷ð™õ<+ Añ`Ê¹ÑS÷ Ÿ;…L»£ 06c“ÈXÇt¥=I&apos;ve

learnt that in my course that it&apos;s a very simple tool to use. Z Ë ¨ ZË Mó ZË Më

C† + ))! L w

Ýlive:jarylchnglive:jarylchngJaryl Chng¡¶Äñ¼?¤ˆ ã#h—[v`Üw×tmÀ^&Åe:}º #XÇtl=Well, you

can try to research on Metasploit Framework Z Ë Ã

ZË há ZË hé g† + m## L 

è19:7283c6220550477ab404f14219d6bcc2@thread.skypeshirleyytanShirley Tan© …¥ÿfR. }® ï

9¦Ç zš!ÃuÙ4sÃu –®—XÇt?=Ehh, alright then, i&apos;ll go do some solo quests first Z Ë ô

ZË ½é ZË ½à ‚ † , m)! L \_

è19:7283c6220550477ab404f14219d6bcc2@thread.skypelive:jarylchngJaryl ChngËrô]ŽµAÑØb

13) 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

Start Sector 1,251,341

Sector offset 436

File Offset 723,892

Length 730

Comment Conversation about hacking simon's account

%ôµ ZË Ñ¥ ZË Ñ¥ ZË Ñ¢‚j† , {7! L) ‚- Ý#live:aliciatanhuij

ing/$live:jarylchng;8e75cb82b2111ff4live:aliciatanhuijingAlicia TanUhk0ÛFÛÛç ÝŽœ¤~cÓ£W k?«

þ/vS. 'X²live:jarylchngXÇsú= The temptation is too strong, it can help my mic purchase too

. I think Simon has a lot of money in his bank. He definitely wouldn&apos;t notice.

%ô´ ·løA

%ô´ ZË ­T ZË ­T ZË ­B‚(† , m7! Lm  è19:7283c6220550477a

b404f14219d6bcc2@thread.skypelive:aliciatanhuijingAlicia TanÆJª8ÜoPÉ«ÔÈ”6Z ¿Ô¥œ8§øðRÀs±ßßå

âé19:7283c6220550477ab404f14219d6bcc2@thread.skypeXÇsË= Actually, I have things that cropp

ed up, you guys go ahead? 2ô ñ ZË ú\ ZË ú\ ZË ú\K† + m## L G

14) 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

Start Sector 1,251,369

Sector offset 320

File Offset 738,112

Length 1,434

Comment Alicia claimed Simon gave her $2000

è19:7283c6220550477ab404f14219d6bcc2@thread.skypelive:aliciatanhuijingAlicia TanïIÈ©Â)Ì P

ƒôvZVÔ>WC ØÒ 3™“‘’)®19:7283c6220550477ab404f14219d6bcc2@thread.skypeXÈÇò= Look what was

my first purchase! `£è 6 ZÐL®} ZÐL®} ZÐL®oƒ-†5, m7! Lm ƒ

è19:7283c6220550477ab404f14219d6bcc2@thread.skypelive:aliciatanhui

jingAlicia TaniÓ¶A,…N/Êà12 Ç‡— +ü MDA8³y ÄÏ ¿19:7283c6220550477ab404f14219d6bcc2@thread.s

kypeXÈÇè= Hey guys! Simon just recently won first prize in the recent 4D drawings and trea

ted me to $2000 as part of his generosity! I didn&apos;t have to do anything in the end <s

s type="laugh">:D</ss> l

¨ 5 ZÐLˆµ ZÐLˆµ ZÐLˆ·6†4+ m## L

è19:7283c6220550477ab404f14219d6bcc2@thread.skypeshirleyytanShirley Tan 5JgŠ% £y Çø2

³AÐ,iÓ  .¸Ÿ » ôÐƒXÈ¥²=Alrights Z ÏÄ:Œ ZÏÆç ZÏÆæö‚ †3+ m7! Lm G

è19:7283c6220550477ab404f14219d6bcc2@thread.skypelive:aliciatanhuijingAlicia Ta

nŠ "€ÑÖ BñèK¡%Ø<ÿR²KÛ¿À Ù ¤‘RH!ð19:7283c6220550477ab404f14219d6bcc2@thread.skypeXÈ¤Œ= May

be later in the afternoon? ™ Ï± 3 ZÏÂgà ZÏÂgà ZÏÂgÓ‚ †2+ m7! Lm U

è19:7283c6220550477ab404f14219d6bcc2@thread.skypelive:aliciatanhuijingAlicia T

an°Dñü ž›‚X —× h=å#’ôa`ZÉìÉeé£¿ &Í19:7283c6220550477ab404f14219d6bcc2@thread.skypeXÈ¤‡= Oh

sorry, I&apos;m a little busy now &$®1 2 ZÏÂZT ZÏÂZT ZÏÂZG:†1+ m## L %

15) 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

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."

Graphical user interface, text, application, email

Description automatically generated

Timeline

Description automatically generated with medium confidence

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

# Appendix C

6) 6c890fe1c3b4379ff283d50f9ec3e5be.png

Item Path Alicia\Users\Alicia\AppData\Local\Mozilla\Firefox\Profiles\lx5oaqu6.default\thumbnails\6c890fe1c3b4379ff283d50f9ec3e5be.png

File Created 14/03/17 12:45:46 PM

Last Written 14/03/17 12:45:46 PM

Last Accessed 14/03/17 12:45:46 PM

MD5

Comment Metasploit Download on Alice PC

Graphical user interface, website

Description automatically generated

7) a0f41b24a6ab2d48f5586c609f7054fb.png

Item Path Alicia\Users\Alicia\AppData\Local\Mozilla\Firefox\Profiles\lx5oaqu6.default\thumbnails\a0f41b24a6ab2d48f5586c609f7054fb.png

File Created 14/03/17 12:48:49 PM

Last Written 14/03/17 12:48:49 PM

Last Accessed 14/03/17 12:48:49 PM

MD5

Comment Guide on How to Use Keylogger on Alice PC

Graphical user interface, text, email, website

Description automatically generated

8) cf86cc03d5956612fb30964eccd98bd8.png

Item Path Alicia\Users\Alicia\AppData\Local\Mozilla\Firefox\Profiles\lx5oaqu6.default\thumbnails\cf86cc03d5956612fb30964eccd98bd8.png

File Created 14/03/17 12:49:00 PM

Last Written 14/03/17 12:49:00 PM

Last Accessed 14/03/17 12:49:00 PM

MD5

Comment Alice Researching on Computer Security Methods

Graphical user interface, text, application, email

Description automatically generated

9) ce3158c8bdf4c7310c2238c2995cd7fe.png

Item Path Alicia\Users\Alicia\AppData\Local\Mozilla\Firefox\Profiles\lx5oaqu6.default\thumbnails\ce3158c8bdf4c7310c2238c2995cd7fe.png

File Created 14/03/17 01:01:19 PM

Last Written 14/03/17 01:01:19 PM

Last Accessed 14/03/17 01:01:19 PM

MD5

Comment Metasploit on Alice PC

Graphical user interface, application, email

Description automatically generated

10) e14b61d4d03a7283206b9b61b1c71b77.png

Item Path Alicia\Users\Alicia\AppData\Local\Mozilla\Firefox\Profiles\lx5oaqu6.default\thumbnails\e14b61d4d03a7283206b9b61b1c71b77.png

File Created 14/03/17 12:49:14 PM

Last Written 14/03/17 12:49:14 PM

Last Accessed 14/03/17 12:49:14 PM

MD5

Comment Metasploit Framework Search

Graphical user interface, text, application, email

Description automatically generated

# Appendix D

16) 79881C3C06818DD50F2DF9C1D35A4390039C729C

Item Path Alicia\Users\Alicia\AppData\Local\Mozilla\Firefox\Profiles\lx5oaqu6.default\cache2\entries\79881C3C06818DD50F2DF9C1D35A4390039C729C

File Created 15/03/17 10:42:45 AM

Last Written 15/03/17 10:51:50 AM

Last Accessed 15/03/17 10:51:45 AM

MD5

Start Sector 41,248,286

Sector offset 408

File Offset 32,152

Length 1,861

Comment Firefox cache containing Simon OCBC Bank Account Number

<pre class="output">Dumping captured keystrokes...ocbc.com.sg &lt;Return&gt; &lt;N7

&gt; &lt;N5&gt; &lt;N6&gt; &lt;N6&gt; &lt;N7&gt; &lt;N2&gt; &lt;N1&gt; &lt;N9&gt;

&lt;N9&gt; &lt;N9&gt; &lt;N8&gt; &lt;N1&gt; &lt;N1&gt; UMQGQN</pre>

</td>

</tr>

<tr class=odd>

<td class="timestamp" valign="top" width="80">

2017-03-15 10:44:12 +0800

</td>

<td valign="top" width="120">

<b>command</b>

</td>

<td>

<pre class="command">keyscan\_dump</pre>

</td>

</tr>

<tr class=even>

<td class="timestamp" valign="top" width="80">

2017-03-15 10:44:12 +0800

</td>

<td valign="top" width="120">

<b>output</b>

</td>

<td>

<pre class="output">Dumping captured keystrokes...7566721999811GAQHKH &lt;Return&gt;

</pre>

</td>

</tr>

<tr class=odd>

<td class="timestamp" valign="top" width="80">

2017-03-15 10:46:46 +0800

</td>

<td valign="top" width="120">

<b>command</b>

</td>

<td>

<pre class="command">keyscan\_dump</pre>

</td>

</tr>

<tr class=even>

<td class="timestamp" valign="top" width="80">

2017-03-15 10:46:46 +0800

</td>

<td valign="top" width="120">

<b>output</b>

</td>

<td>

<pre class="output">Dumping captured keystrokes...Wendy, &lt;Return&gt; &lt;Return&

gt; Thank you very much. &lt;Return&gt; &lt;Return&gt; &lt;Back&gt; &lt;Back&gt; &lt;B

ack&gt; Suit yourself alb &lt;Back&gt; &lt;Back&gt; &lt;Back&gt; Albert. &lt;Return&gt;

&lt;Return&gt; Take nte &lt;Back&gt; &lt;Back&gt; ote that your parents will be notified

of this outrageous act. You should feel ashamed. &lt;Return&gt; &lt;Return&gt; Good luck

y &lt;Back&gt; out there. &lt;Return&gt; &lt;Return&gt; &lt;Back&gt; &lt;Back&gt; &lt

;Back&gt; Unknown command: screenshit.</pre>

</td>

</tr>

# Appendix E

The below bookmarks represent documents that are potentially relevant to this case.

1) note.txt

Item Path Alicia\$RECYCLE.BIN\S-1-5-21-4134190322-1791598225-2319710166-1002\note.txt

File Created 15/03/17 10:54:38 AM

Last Written 15/03/17 10:57:15 AM

Last Accessed 15/03/17 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

# Appendix F

Pictures

|  | Name | Logical Size | Item Type | Signature Analysis | File Type |
| --- | --- | --- | --- | --- | --- |
| 1 | acash.png | 164,629 | Entry | Match | Portable Network Graphic |

The below bookmarks represent pictures that are potentially relevant to this case.

5) acash.png

Item Path Alicia\Users\Alicia\Pictures\acash.png

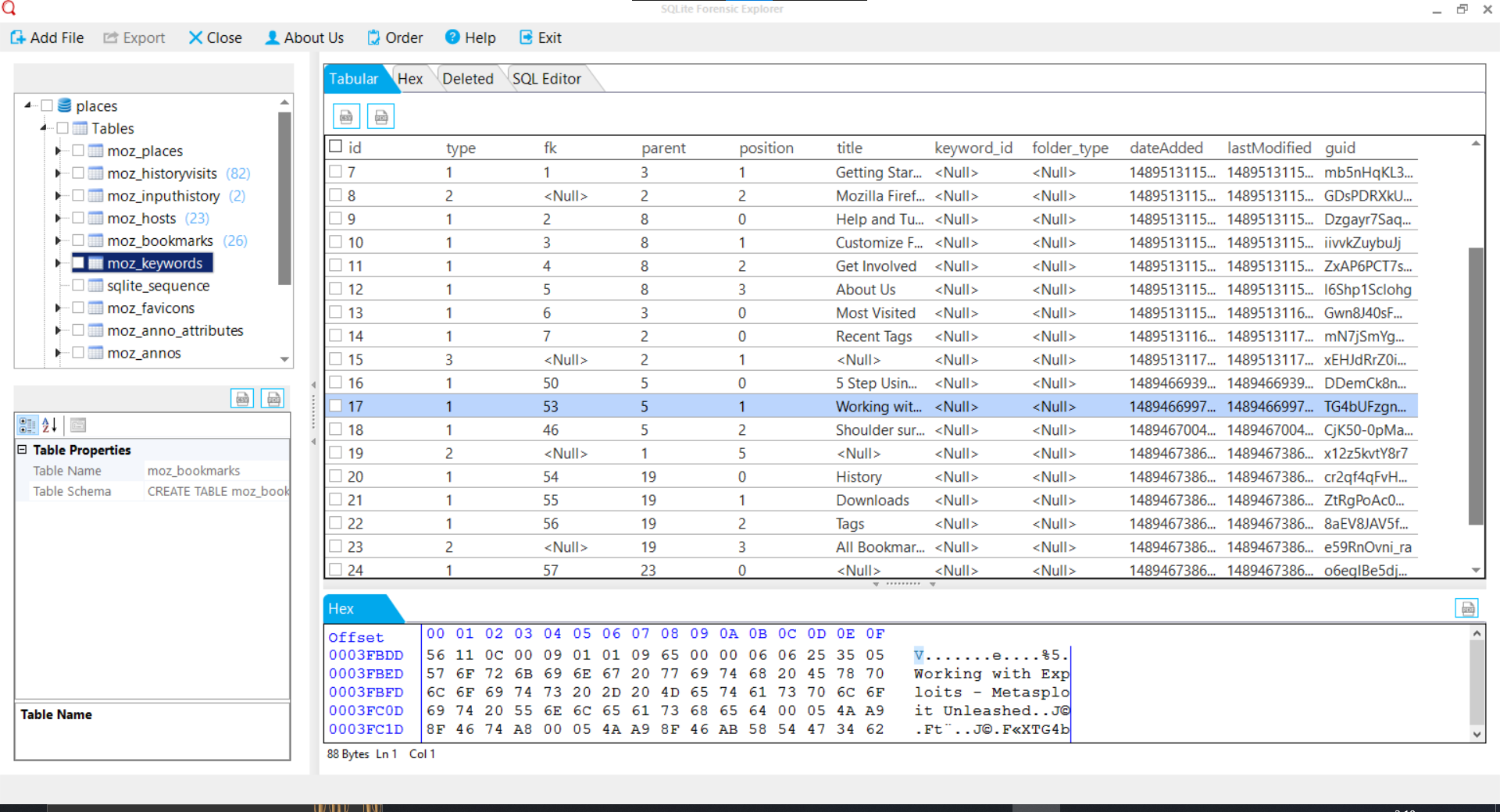
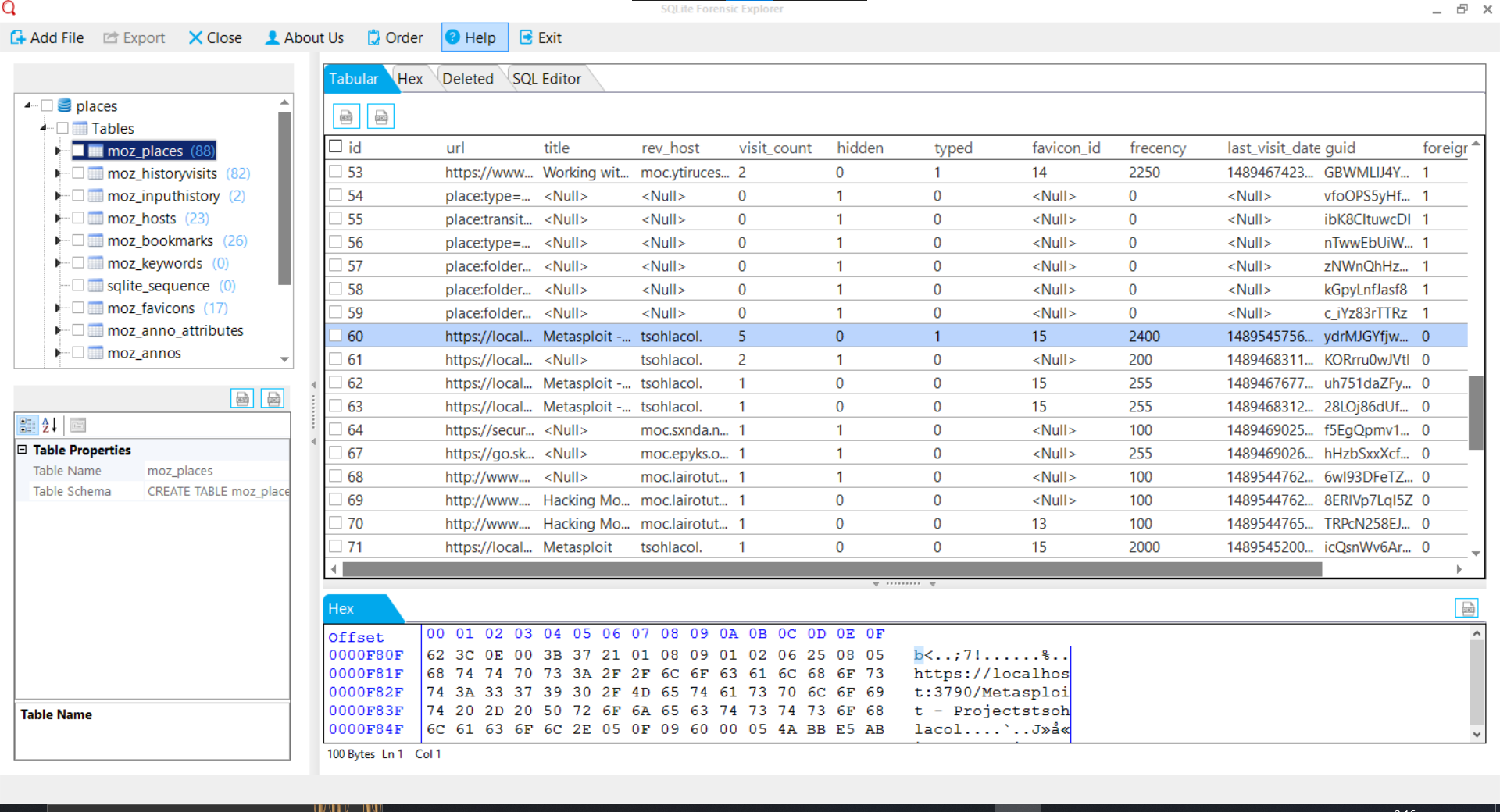
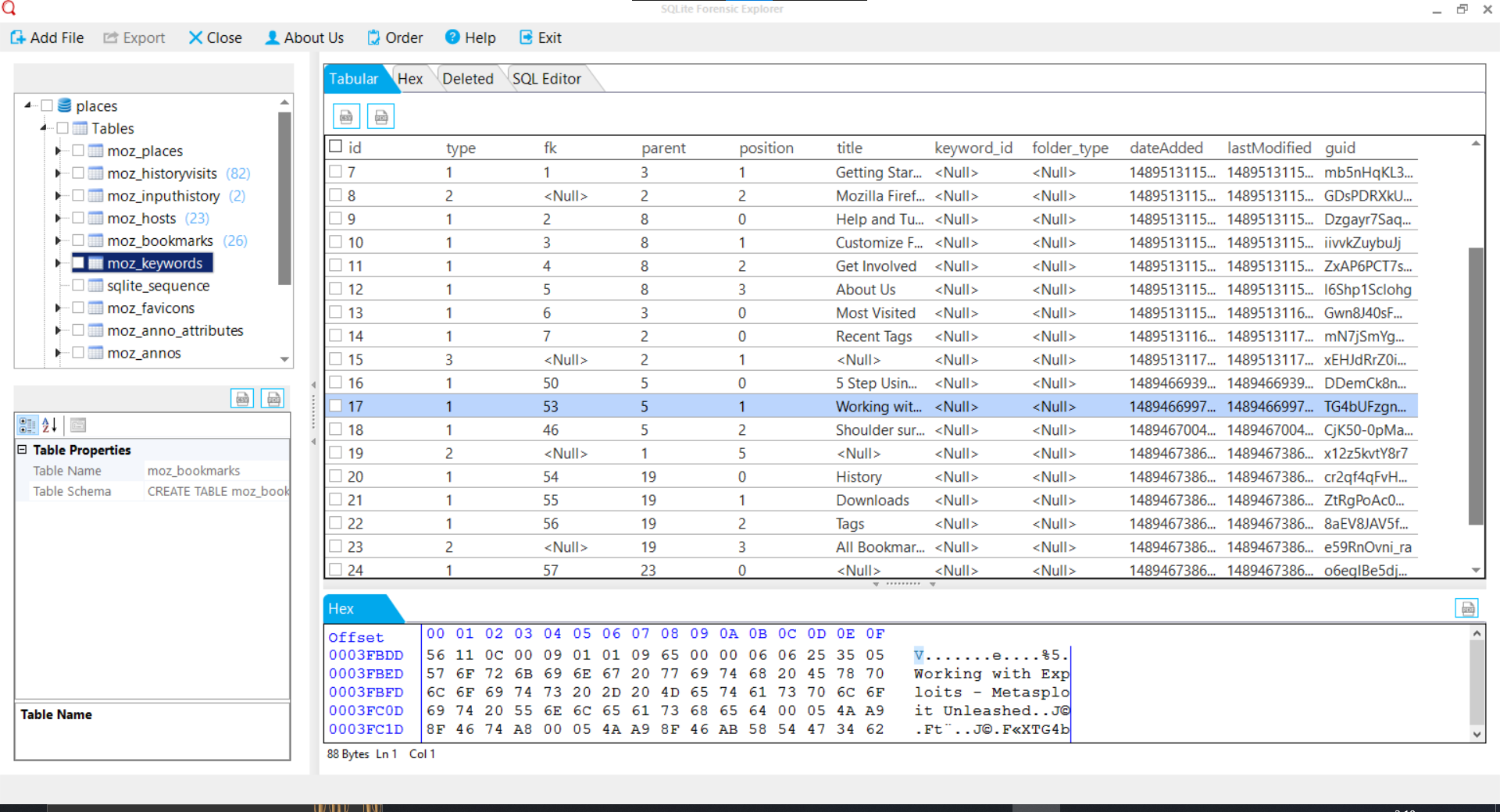
File Created 15/03/17 12:46:08 PM

Last Written 15/03/17 12:46:08 PM

Last Accessed 15/03/17 12:46:08 PM

MD5 28c9f69a77c74847434c57228eb2f76d

Comment Located on Alicia's computer:



A screenshot showing a recent transaction of @Cash, a currency in MapleStory bought using real world money. It is likely that it was bought using the $2000 transferred to her from Simon's account.

Text

Description automatically generated

# RTF Report

