Examiner Report

### Overview

On January 25, 2022, Simon reported an unauthorised 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. Alicia denied any wrongdoings and claimed that Simon had 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.

### Objectives

This report is a summary of forensic investigators, Edward Neo and Jeremy Sng, findings regarding the authenticity of the unuathorised bank transfer based on the analysis of the media retrieved. This report is not intended to detail each and every aspect of the forensic investigators’ work in this engagement.

### Evidence Analysed

Pursuant to the court order, True Identity Pte Ltd. collected digital media that was found at the crime scene. The forensic investigators inspected the data on the following media for analysis according to the terms of the Court-ordered Protocol:

A 20170316-001-E01 desktop computer with Windows 7 operating system

A 20170316-001-E02 desktop computer with Windows 10 operating system

A 200 Gigabyte Seagate internal hard drive [image file: Simon.Ex01]

A 500 Gigabyte Seagate internal hard drive [image file: Alicia.Ex01]

Using widely accepted digital forensic techniques and procedures, True Identity Pte Ltd. verified the forensic image of the 200 Gigabyte Seagate Hard Drive and the 500 Gigabyte Seagate in Alicia’s PC. The digital forensic copying process captured the entire contents of each piece of media, including the active user-accessible files, the deleted files, and the unallocated space, which may contain deleted content. Because the forensic images created are a forensic image file, True Identity Pte Ltd. used a forensically-sound copy method to copy the forensic image files on that drive to preservation media.

### Investigation Steps

True Identity Pte Ltd. conducted its analysis of the Alicia media pursuant to the protocol issued by the court. True Identity searched and analyzed the Alicia media to “Recover as much relevant evidence as possible from the image file” by “perform[ing] extraction and analysis on the image file, Alicia.Ex01”.

During this analysis, True Identity Pte Ltd. employed a methodology tailored to the particular facts of this case. True Identity Pte Ltd.’s methodology included: (1) conducting keyword and other searches of the digital forensic copies of the Alica Media and other data, including webmail accounts such as ‘Skype’, to identify responsive documents or fragments of documents; (2) manually reviewing the documents containing keyword hits, certain unsearchable file types, such as image files with no text, and other documents to determine whether they were relevant to the authenticity of the bank transfer; and (3) reviewing the digital forensic copies of the Alicia Media for digital forensic artifacts relevant to the authenticity of the bank transaction.

### Findings

Alicia recently joined a MapleStory guild called “PQRaiderz” and joined their Skype group chat. In the group chat, she spoke about how she spent the money Simon gave her from him winning the lottery on “Gachapon Tickets”.

Alicia spoke about how she was tempted to steal Simon’s money as she believed he was rich and would not notice a small amount missing. Alicia said in the group chat she would google for a solution which led True Identity Pte Ltd. to believe her “guild mates” might have recommended ideas to her.

Through findings, True Identity Pte Ltd. knows Alicia browsed Firefox for guides on Metasploit’s Keylogger and have found proof of her registering and activating a Metasploit account. There is also evidence to show that she downloaded Metasploit on her computer. Furthermore, there was also a search in Firefox for Shoulder Surfing guides.

In Alicia’s Recycling Bin, True Identity Pte Ltd. found a text document that contained 3 items. There was also a suspicious “.png” file that could not be viewed. After further investigation, True Identity Pte Ltd. found that the “.png” file was supposedly an “.mp4” file that had been tampered with. The contents of the “.mp4” file revealed Simon entering his password to login to his computer, which revealed Alicia’s intent of shoulder surfing.

From the video, True Identity Pte Ltd. learned that Simon’s computer password was “abc12345” and coincidentally, one of the items listed in the deleted text file was Simon’s login credentials.

Upon further inspection of Alice’s hard drive, True Identity Pte Ltd. found evidence of Alicia making a remote connection to Simon’s PC. From there, True Identity Pte Ltd. knew that Alicia was able to login to Simon’s PC and had installed a keylogger on Simon’s PC as seen from the evidence.

After viewing the keylogger dumps from Alice’s Hard Drive, True Identity Pte Ltd. found that Metasploit was able to steal a credential from Simon. Upon further inspection, True Identity Pte Ltd. found that the Keylogger took down Simon’s Bank Account details. From the dump, True Identity Pte Ltd. can see that Simon’s bank account number is “7566721” and “999811” is his password. These numbers are an exact match to the last two items in the deleted text document found in Alicia’s Recycling Bin.

By viewing the artifacts, True Identity Pte Ltd. found evidence of a remote connection being made using Alicia’s computer. Through further investigation, True Identity Pte Ltd. found that the session name of the remote login was ‘Simon-PC\Simon @ SIMON-PC’.

Lastly, there was a transaction photo found in Alicia's pictures that shows a transaction of in-game currency for Maplestory that when converted to S$SGD, equates to S$200.00.

### Conclusion

True Identity Pte Ltd. found direct and compelling digital forensic evidence that Alicia is the one that is responsible for making the transaction of SGD S$2000.00 through unauthrorised access of Simon’s bank account. As previously mentioned in the findings, True Identity found incriminating evidence through searching chat and browsing histories as well as deleted media that has been modified with intent of concealing the evidence.

True Identity Pte Ltd. found a deleted video that was disguised as an image to avoid detection and suspicion. Through analysis of the recovered video, True Identity Pte Ltd. found evidence of Alicia performing ‘shoulder surfing’ and thus obtaining Simon’s credentials for his PC, which falls under the Computer Misuse Act Cap.50 section 8b - “Obtaining, etc., items for use in certain offences.”.

Additionally, True Identity Pte Ltd. found evidence of Alicia installing a keylogger on Simon’s Computer through Metasploit. After his bank credentials were logged, Alica used Metasploit to establish a remote connection and used the stolen credentials to access Simon’s bank account to transfer herself the S$2000.00

As a result, True Identity Pte Ltd. can conclude that Alicia had framed Simon and had used his bank account to transfer herself money to spend on in-game currency for “MapleStory”. This is further supported as True Identity Pte Ltd. know from interviews that Alicia is an avid gamer. Hence, True Identity Pte Ltd. can draw the conclusion that is backed up from the previous findings that she had made unauthorized bank transfers from Simon’s account. The digital forensic evidence strongly indicates that Alicia fabricated her story and was responsible for the unauthorised transactions of Simon’s bank account, making Alicia guilty.

### Appendices



Examiner Report

Case Information

| Case Number | 20170316-001 |
| --- | --- |
| Examiner Name | Edward Neo, Jeremy Sng |
| Description | Alica’s Image File (Alicia.Ex01) |

# Evidence

| Name | Acquisition SHA1 | Verification SHA1 | Model | Examiner Name | Evidence Number | Serial Number |
| --- | --- | --- | --- | --- | --- | --- |
| Alicia | 132a9f27dc3a02f90d64f50b12b797c16f74089b | 132a9f27dc3a02f90d64f50b12b797c16f74089b | ST500DM002-1BD142 | Edward Neo, Jeremy Sng | E02HD1 | Z3TNNKM4\_206848 |

## Video Recording – Recycling Bin

11) 20170315\_100927.jpg

Name 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

We noticed that the size of the jpg was big and was unable to open the picture for viewing. Normally, photos are not this large, hence we suspected that the file format was tampered with.

We decided to export the file and change the file extension to a mp4. A video was found of Simon logging into his computer



## Email Conversation - Mail

16) 00000005000000030bfd.dat

Name 00000005000000030bfd.dat

File Created 15/03/17 02:03:20 AM

Last Written 15/03/17 02:03:20 AM

Last Accessed 15/03/17 02:03:20 AM

# 

This screenshot shows that Alicia was in contact with Jaryl Chng and joined a Maplestory guild

## Intent of Alicia - Skype

1) main.db

Name 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

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.

We found this text sent out by Alicia to her Maplestory Skype group chat indicating malicious intent.

## Simon Keyword - Skype

2) main.db

Name 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

3) main.db

Name 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

## Alicia Keyword - Skype

4) main.db

Name 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

Hey Alicia! Welcome to the chat <ss type="smile">:)</ss> Z ÊŽN( ZÊó

ZÊó T…o+ m)! L G è19:7283c6220550477ab404f14219d6bcc2

@thread.skypelive:jarylchngJaryl Chng×°\* ë)WjÀà h¸ ƒÁŠc X]¥ê± ¤¥Š-•WXÈ0ñ <MapleSEA PQRai

derz Skype Chat ™\*Û¾ Z ÊÆ ZÊÆ ZÊÆÁ >…n+ m)! L

Proof of Alicia’s joining the guild’s skype group chat.

## Firefox Browsing History

5) places.sqlite

Name 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

http://www.hacking-tutorial.com/hacking-tutorial/5-step-using-metasploit-meterpreter-keylo

gger-keylogging/#sthash.qNLoiub7.dpbs5 Step Using Metasploit Meterpreter Keylogger(Keylogg

ing) | Ethical Hacking Tutorials, Tips and Tricksmoc.lairotut-gnikcah.www.

¯ J©Šö

0et9M9srioCr-r&æ^i\*‚ 1 aY? % http://www.hacking-tutorial.com/hacking-tutorial/5-s

tep-using-metasploit-meterpreter-keylogger-keylogging/5 Step Using Metasploit Meterpreter

Keylogger(Keylogging) | Ethical Hacking Tutorials, Tips and Tricksmoc.lairotut-gnikcah.www

.d

Alicia’s Firefox browsing history showed malicious intent of learning how to use Metasploit’s Keylogger.

6) places.sqlite

Name 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

https://www.google.com.sg/search?q=shoulder-surfing&ie=utf-8&oe=utf-8&client=firefox-b-ab&

gfe\_rd=cr&ei=-3XHWPGwCuHH8gf-2YewBQshoulder-surfing - Google Searchgs.moc.elgoog.www. Ð

J©‰k™ uUfNApNIV1gb+ ¿Ø)\* , 9 + % https://www.google.com/search?q=shoulder-surfing

&ie=utf-8&oe=utf-8&client=firefox-b-abmoc.elgoog.www. Ð J©‰i±XKmqnddY\_vacr+ ›)b

Alicia’s Firefox browser history showed malicious intent of learning how to commit shoulder surfing.

7) places.sqlite

Name 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

https://www.rapid7.com/products/metasploit/download/community/Metasploit Community Downloa

d: Pen Testing Tool | Rapid7moc.7dipar.www. d J©…†{èXJvXMQfMpA\_f+ …gÛ(& }{+ % ht

tps://www.rapid7.com/products/metasploit/download/pro/Metasploit Pro Download: Free Pen Te

sting Tool | Rapid7moc.7dipar.www. d J©=¦Øpp9Nt6IaXOAA+ ²swQ%% u}+ % https://www

.rapid7.com/products/metasploit/download/Metasploit Download: Most Used Pen Testing Tool |

Rapid7moc.7dipar.www. d J©€Î'à4Z-qYfvl9VP8+ }eJ  # C\_3 % https://www.metasploit.

com/Penetration Testing Software | Metasploitmoc.tiolpsatem.www.

d J©€ ‰ ZKeS2OSzNk2e+ ýÈc" ‚ U1 % https://www.google.com.sg/search?q=metasploit

+framework&ie=utf-8&oe=utf-8&client=firefox-b-ab&gfe\_rd=cr&ei=WXXHWJ7zJuHH8gf-2YewBQmetasp

loit framework - Google Searchgs.moc.elgoog.www. Ð J©ËR(AifObO0vpI6S+ å˜‹ï

Proof of downloading Metasploit on Alicia’s Computer

## Commands Used on Simon’s PC.

8) 79881C3C06818DD50F2DF9C1D35A4390039C729C

Name 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

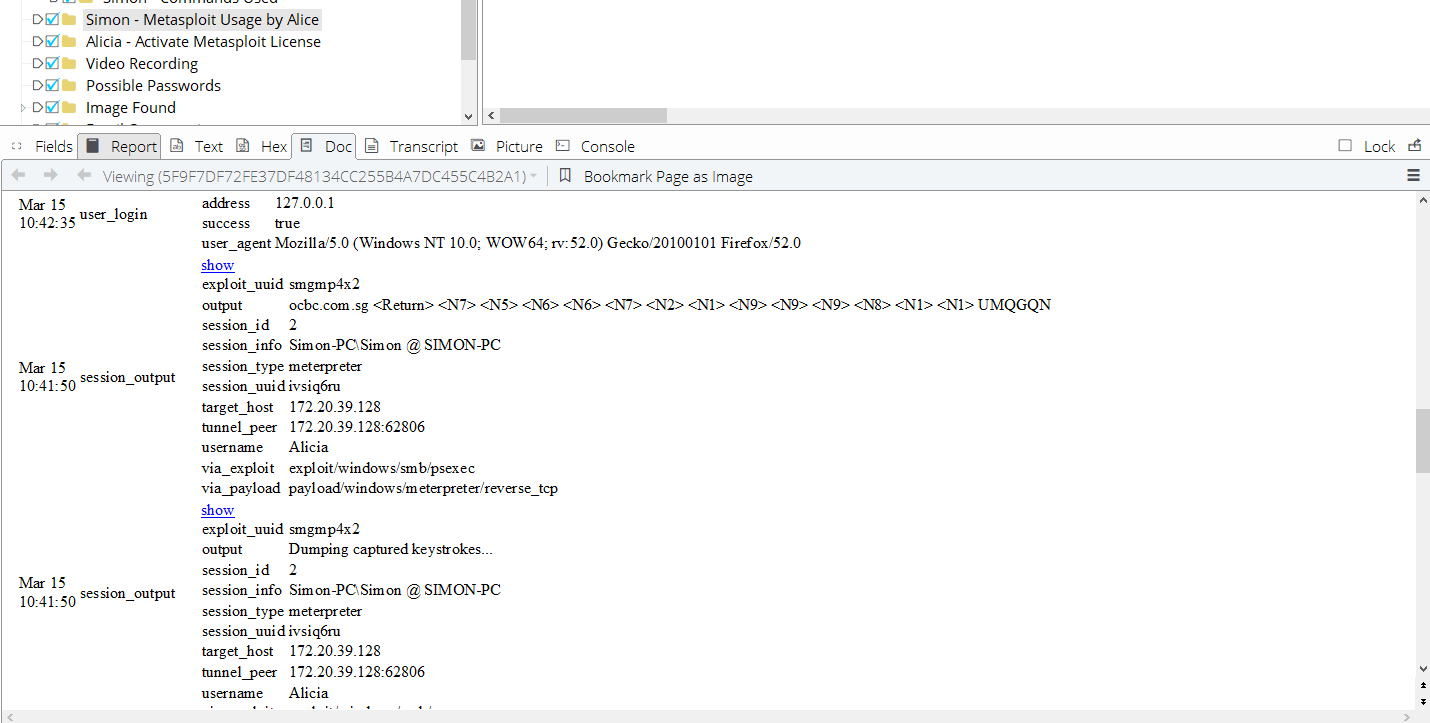
9) 5F9F7DF72FE37DF48134CC255B4A7DC455C4B2A1

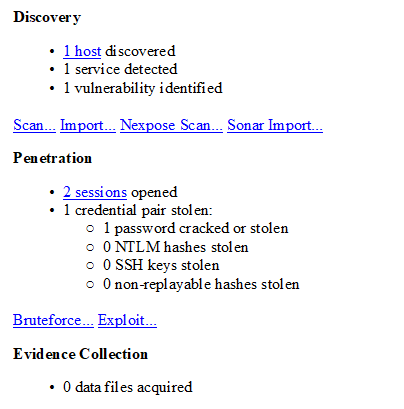
Name 5F9F7DF72FE37DF48134CC255B4A7DC455C4B2A1

File Created 15/03/17 10:42:38 AM

Last Written 15/03/17 10:42:40 AM

Last Accessed 15/03/17 10:42:38 AM





## Alicia - Activate Metasploit License

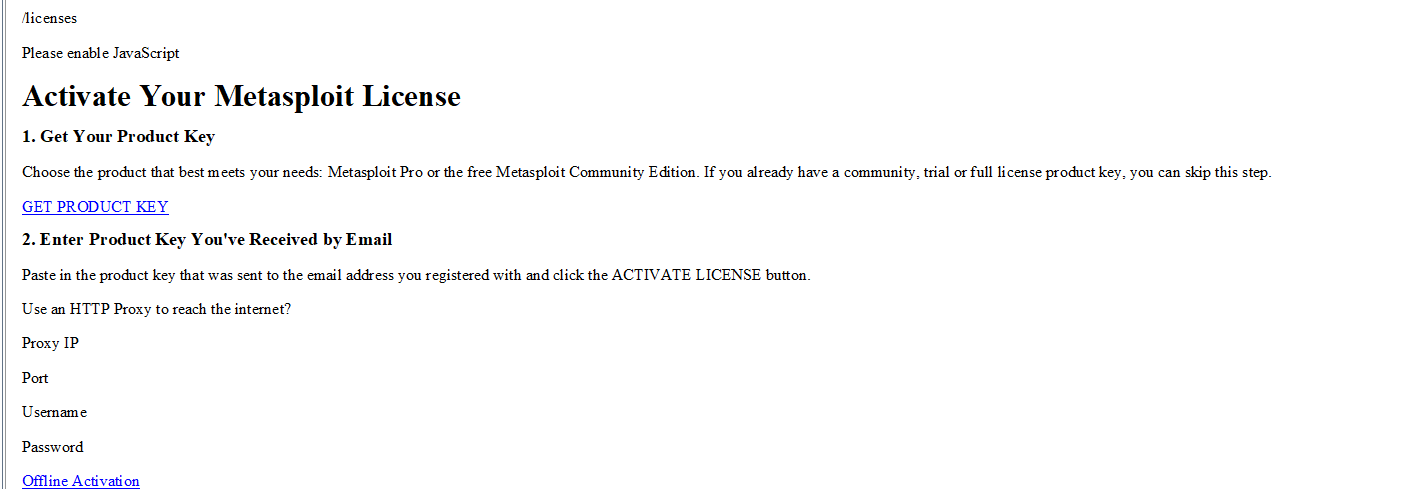
10) 58CE13540C1F6C3499CD0CF4AFCB1D4F06D99074

Name 58CE13540C1F6C3499CD0CF4AFCB1D4F06D99074

File Created 14/03/17 01:11:52 PM

Last Written 14/03/17 01:12:13 PM

Last Accessed 14/03/17 01:11:52 PM



## Possible Passwords

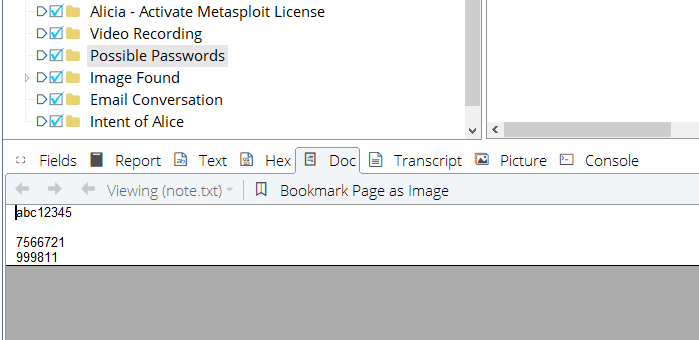
11) note.txt

Name 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



According to the videos found in section 1, we realised that “abc12345” is the password to Simon’s computer and contains Simon’s bank account number. There is 1 more item that yet to be known.

## Image Found

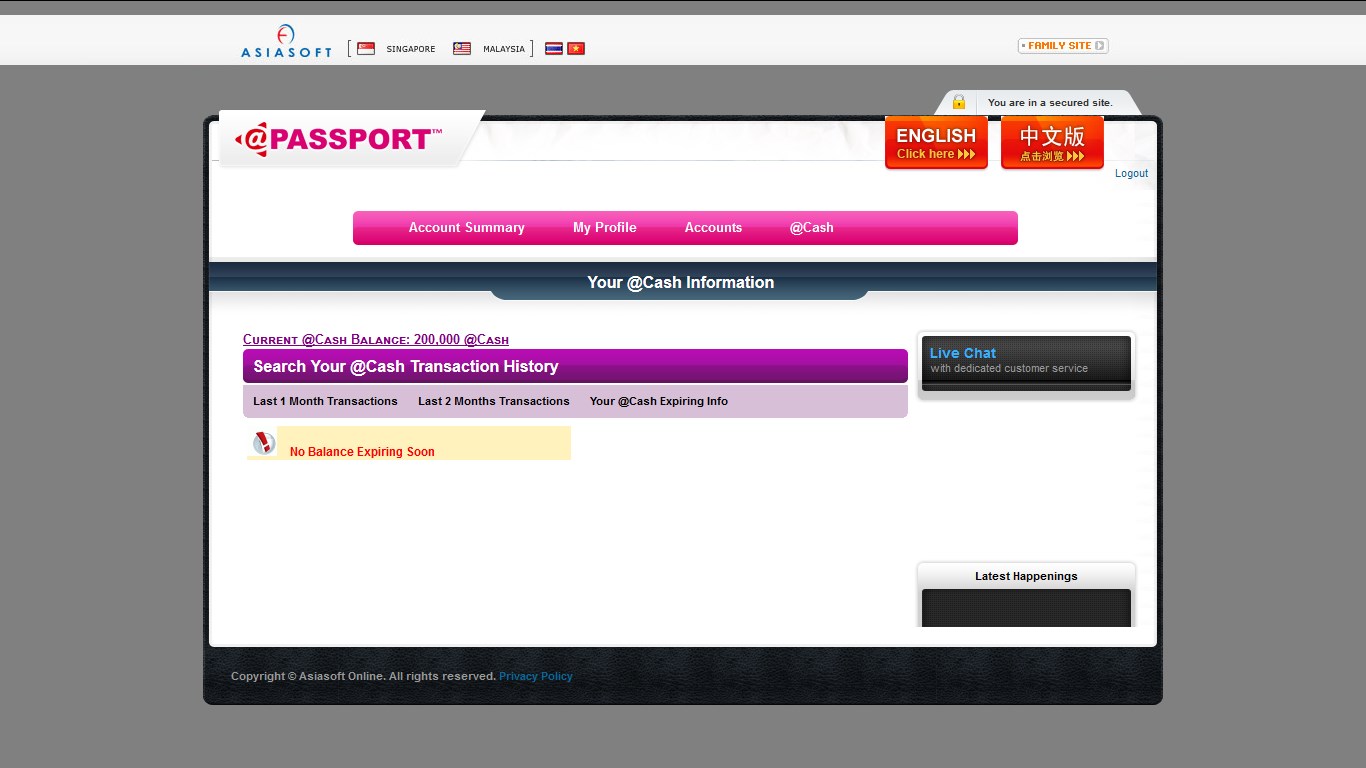
12) acash.png

Name 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



This image illustrates a balance of 200,000 @Cash which is the currency used for Alicia’s games.

## Account Information through Keylogger

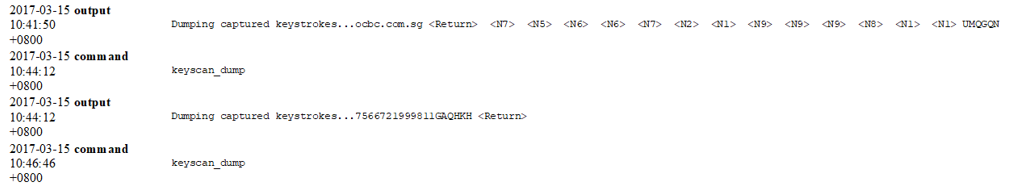
13) 79881C3C06818DD50F2DF9C1D35A4390039C729C

Name 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



This image proves that Alicia used a keylogger on Simon’s computer. We found the use behind the final item in the deleted text document. It was the pin number for Simon’s Bank account.

## Metasploit Community License Key

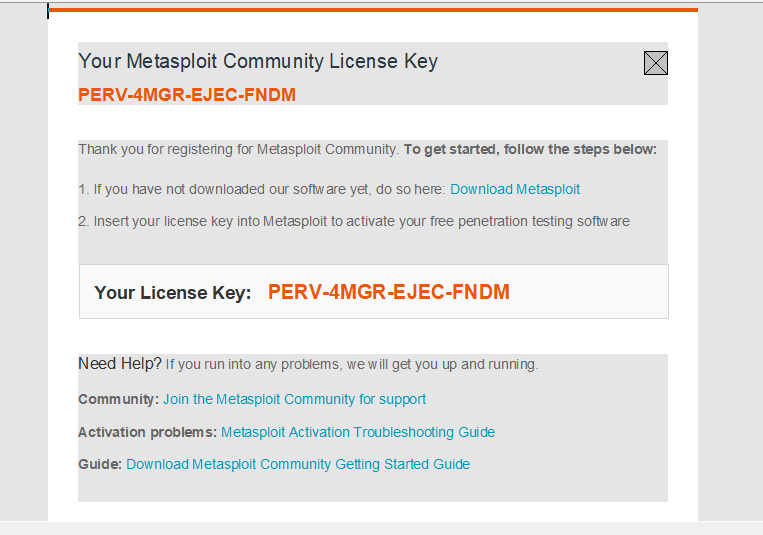
14) 00000008000000030bfd.dat

Name 00000008000000030bfd.dat

File Created 14/03/17 12:48:27 PM

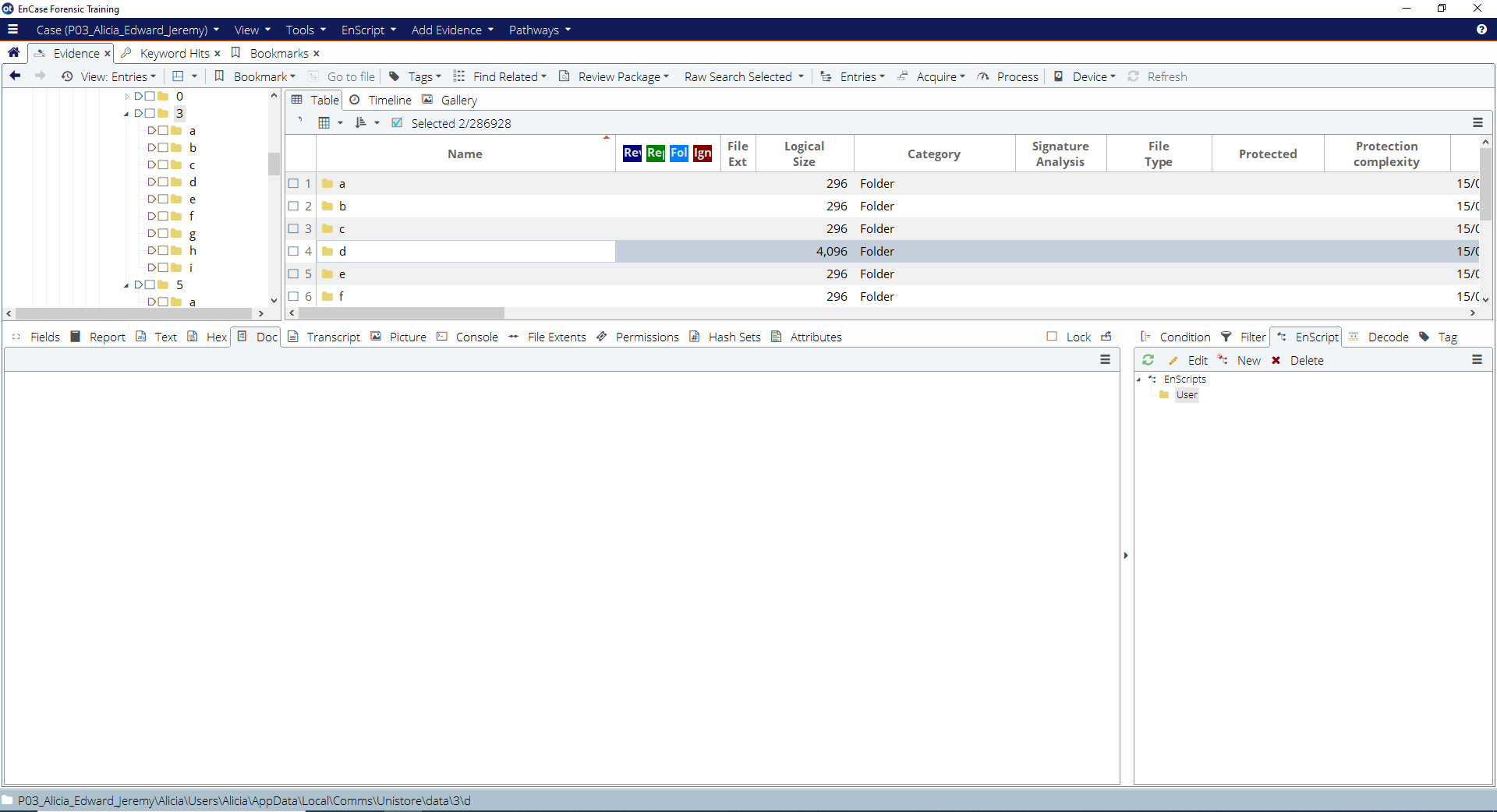
Last Written 14/03/17 12:48:27 PM

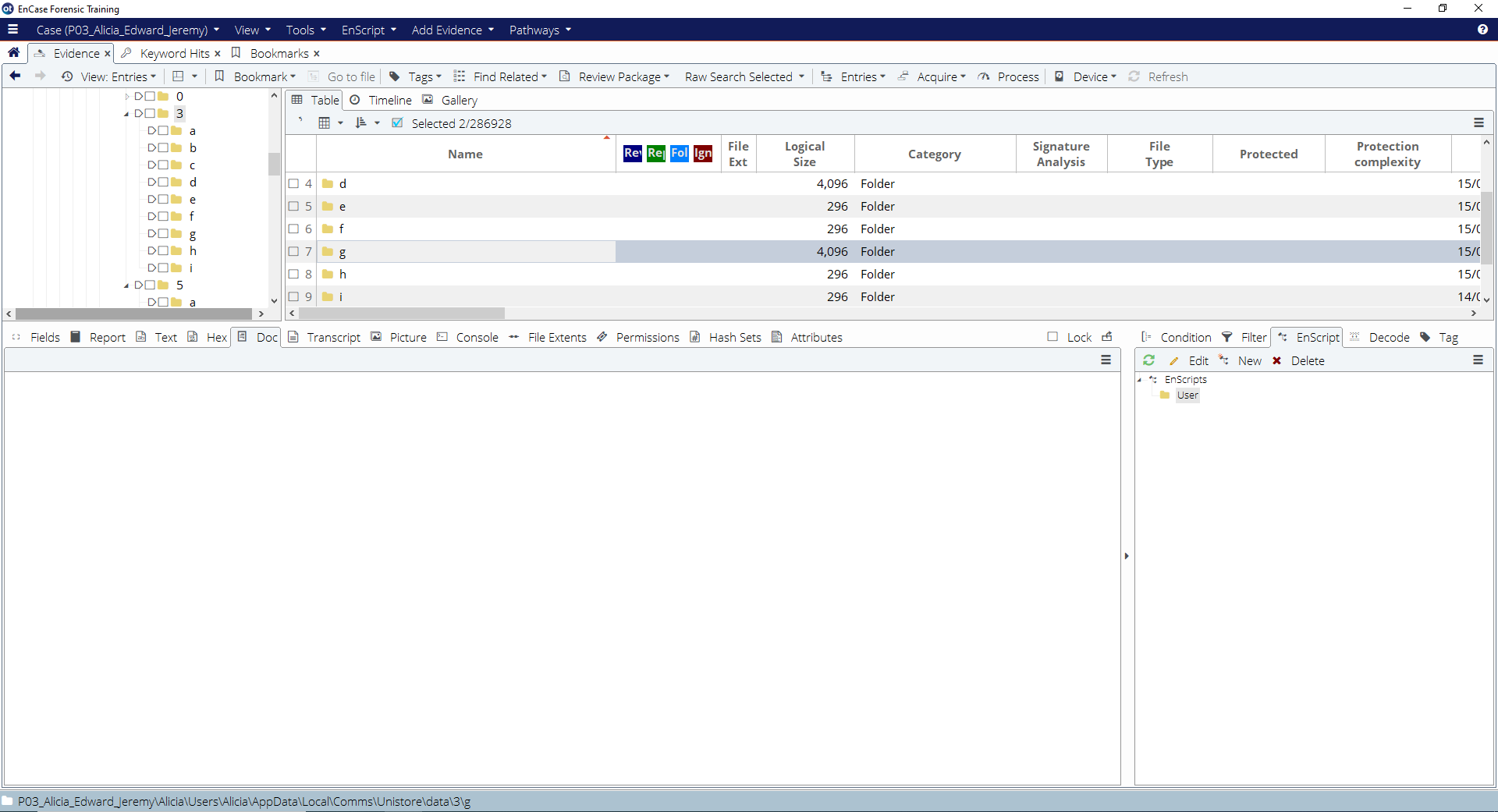
Last Accessed 14/03/17 12:48:27 PM



This is proof that Alicia has downloaded Metasploit

**Hidden Files**





We found 2 files in Alicia’s Mail that had a large logical size compared to other files. When attempting to access the file, the content in the file could not be seen. This means that Alicia had tempered with the files to make the content hidden.