|  |  |
| --- | --- |
| **Digital Forensics**  Diploma in CSF/IT  Year 2/3 (2022/23) Semester 4/6 | Week 12 |
| Tutorial 8 |
| **Examiner Report (Optional)** | |

**OBJECTIVES**

After completing this tutorial, you should be able to

1. Construct a proper Examiner report base on the evidence recovered.

Case Write-up:

Raylen Morgan, 32 has been detained by police officers on suspicion of using stolen bank account information to defraud a bank of more than $1 million. He was found loitering near an ATM machine at New York City when the police officers approached him.

Raylen denied the accusation and claimed that he was innocent. You are the forensic investigator assigned for this case. You are to perform first incident respond and to conduct a full investigation of the case. During the search at his house, you found and seized a laptop.

Base on the case write-up above and the sample RTF report given in the appendix, write *ONE* short paragraph for each of the sections of an examiners report. Make use of the extracted evidence in Appendix.

Note: You may choose to write just *ONE* point for each section.

* 1. Case Summary

This section will vary in length. You will include any relevant information regarding what led to you as the forensic examiner/analyst becoming involved with the digital evidence.

You may be just receiving the forensic image and someone else conducted the forensic acquisition and this is a good place to document that as this will correlate with your chain of custody information that you immediately started once you came into contact with the digital evidence.

Graphical user interface, text, application

Description automatically generated

Text

Description automatically generated

* 1. Forensic Acquisition (Imaging)

This section is very important, as you must detail your interaction with the digital evidence and the steps taken to preserve and forensically acquire the evidence.

Any additional steps that you take (e.g. forensically wiping storage/examination media, etc.) should be notated in this section of your report.

Thoroughly documenting what you have done is very important to the integrity of the digital evidence and your chain of custody.

You should have a digital camera in your forensic toolkit. Take a picture of the evidence and document each step of the forensic acquisition and preparation process. Regardless, if you include the picture in your report or as an exhibit, this picture is a perfect field note for you as the examiner to reference when completing your report.

You will need to briefly describe the process you used when making a working copy from the forensic image of the original evidence, such as tools used.

You will also need to include that you verified your forensic image and notate the hash values (e.g., MD5, SHA-1).

* 1. Details of Findings (Forensic Analysis)

This is the most detailed section of your investigation. You should include all artefacts that you find during your analysis relating to the case.

It may include:

* + Specific files related to the request.
  + Other files, including deleted files that support the findings.
  + String searches, keyword searches, etc.
  + Internet-related evidence, such as chat logs, cache files, e-mail, etc.
  + Graphic image analysis.
  + Indicators of ownership, which could include program registration data.
  + Data analysis.
  + Techniques used to hide or mask data, such as encryption, steganography, hidden attributes, hidden partitions, and file name anomalies.
  1. Conclusion

In this section, you are basing your conclusion off the forensic evidence.

The goal of the forensic examination is to report the facts, regardless if the evidence is inculpatory or exculpatory in nature.

**Appendix**

Administrative Information

| Serial Number | 3AE2-E112 |
| --- | --- |
| Full Serial Number | E43AE3123AE2E112 |
| Driver Information | NTFS 3.1 |

**Volume**

| File System | NTFS |
| --- | --- |
| Sectors per cluster | 8 |
| Bytes per sector | 512 |
| Total Sectors | 42,602,495 |
| Total Capacity | 21,812,473,856 Bytes (20.3GB) |
| Total Clusters | 5,325,311 |
| Unallocated | 6,111,301,632 Bytes (5.7GB) |
| Free Clusters | 1,492,017 |
| Allocated | 15,701,172,224 Bytes (14.6GB) |
| Volume Offset | 0 |
| Id | S-1-5-21-305837926-1768984753-988666380 |
| Drive Type | Fixed |

| Name | Raylen's Laptop |
| --- | --- |
| Actual Date | 09/20/12 05:25:35AM |
| Target Date | 09/20/12 05:25:35AM |
| File Path | C:\Program Files\270603\Raylen\Raylen's Laptop.E01 |
| Case Number | ATM Skimming\_Raylen |
| Evidence Number | 001 |
| Examiner Name | Tan Siok Ching |
| Notes | Laptop seized from Raylen's home |
| Drive Type | Fixed |
| File Integrity | Completely Verified, 0 Errors |
| Acquisition MD5 | e3fe9202c1ee60e3bec1aae183401ea4 |
| Verification MD5 | e3fe9202c1ee60e3bec1aae183401ea4 |
| GUID | c042d1dfd2d18c4986a3bc5f5d50b879 |
| EnCase Version | 6.16.2 |
| System Version | Windows 7 |
| Raid Stripe Size | 0 |
| Error Granularity | 64 |
| Process ID | 0 |
| Index File | C:\P07\Cases\Raylen\Index\Raylen's Laptop-c042d1dfd2d18c4986a3bc5f5d50b879.Index |
| Read Errors | 1 |
| Missing Sectors | 0 |
| CRC Errors | 0 |
| Compression | Good |
| Total Size | 21,812,477,440 Bytes (20.3GB) |
| Total Sectors | 42,602,495 |
| Disk Signature | 00000000 |
| Partitions | Valid |

Drive Information

1) Raylen\Raylen's Laptop\$Boot

**File Record**

| Type | Name | Status | Start | Stop | Relative | Size |
| --- | --- | --- | --- | --- | --- | --- |
| 4f | Unknown | 0d | 335:10:2 | 327:84:13 | 1936269394 | 1836016416 |
| 73 | Unknown | 70 | 371:114:37 | 256:101:36 | 1917848077 | 544437093 |
| 2b | Unknown | 43 | 364:116:50 | 372:65:44 | 1818575915 | 544175136 |
| 61 | Speedstor | 72 | 372:101:51 | 269:114:52 | 2844524554 | 54974 |

Email Content

2) Raylen\Raylen's Laptop\Users\Encase\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\QKCKJES2\wbk130.tmp

Ok, count me in.   Ivan

On Fri, Sep 14, 2012 at 1:33 AM, Raylen Morgan <raylen\_morgan12@hotmail.com [mailto:raylen\_morgan12@hotmail.com] > wrote:

I know this is illegal, but you know, if we can get their bank account information, we will be rich! After getting all the money, we will be able to live a good life. Not to worry, I will destroy all the evidences when this whole thing is over and we will take a flight to leave here immediately.

3) Raylen\Raylen's Laptop\Users\Encase\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\QKCKJES2\wbk130.tmp

  Raylen   **From:** Ivan Meni **Sent:** Wednesday, September 12, 2012 7:26 PM **To:** Raylen Morgan **Subject:** Re: Are you interested?   Wow! It's a great idea. But that is an illegal act, we might get caught.   Ivan

On Fri, Sep 14, 2012 at 1:27 AM, Raylen Morgan <raylen\_morgan12@hotmail.com [mailto:raylen\_morgan12@hotmail.com] > wrote:

Hi Ivan, Hey buddy! I think that you might be interested. Recently I have figured out an idea on how to earn money easily. We could earn big bucks by skimming the ATM, getting their account information’s and so we can withdraw all their money. Isn’t it a good chance?!

4) Raylen\Raylen's Laptop\Users\Encase\AppData\Local\Microsoft\Windows Live Mail\Hotmail (ra a1f\Inbox\546D36AD-00000004.eml

On Fri, Sep 14, 2012 at 1:52 AM, Raylen Morgan <raylen\_morgan12@hotmail.com [mailto:raylen\_morgan12@hotmail.com] > wrote:

Here=92s an attachment on the complete account access you will need to= encode these into the gift cards so we can use that to withdraw funds from= the compromised accounts. =A0 Raylen

5) Raylen\Raylen's Laptop\Users\Encase\AppData\Local\Microsoft\Windows Live Mail\Hotmail (ra a1f\Inbox\546D36AD-00000004.eml

On Fri, Sep 14, 2012 at 1:52 AM, Raylen Morgan wrote: Here=92s an attachment on the complete account access you will need to encode these into the gift cards so we can use that to withdraw funds fro= m the compromised accounts. Raylen --bcaec51b150d17b9dd04c98c5c27 Content-Type: text/html; charset=windows-1252 Content-Transfer-Encoding: quoted-printable Alright, meet you at the usual ATM later. =A0 Ivan

6) Raylen\Raylen's Laptop\Users\Encase\AppData\Local\Microsoft\Windows Live Mail\Hotmail (ra a1f\Inbox\546D36AD-00000004.eml

Date: Thu, 13 Sep 2012 10:49:44 +0800 Message-ID: Subject: Re: Accounts From: Ivan Meni To: Raylen Morgan Content-Type: multipart/alternative; boundary=bcaec51b150d17b9dd04c98c5c27 Return-Path: ivanmeni77@gmail.com X-OriginalArrivalTime: 13 Sep 2012 02:49:44.0885 (UTC) FILETIME=[6E659E50:01CD915A] --bcaec51b150d17b9dd04c98c5c27 Content-Type: text/plain; charset=windows-1252 Content-Transfer-Encoding: quoted-printable Alright, meet you at the usual ATM later. Ivan

Favourites Folder

Suspect's favourite site saved.

7) Raylen\Raylen's Laptop\Users\Encase\Favorites\Personal\ATM SKIMMER FRAUD HOW IT WORKS STEP BY STEP - YouTube.url

8) Raylen\Raylen's Laptop\Users\Encase\Favorites\GOOD AND FRESH CREDITCARD NUMBERS, FULL BANK ACCOUNT LOGINS CREDIT CARD SKIMMERS FOR SALE.url

9) Raylen\Raylen's Laptop\Users\Encase\Favorites\Skimming Device-Skimming Device Manufacturers, Suppliers and Exporters on Alibaba.com.url·favicon



10) Raylen\Raylen's Laptop\Users\Encase\Favorites\GOOD AND FRESH CREDITCARD NUMBERS, FULL BANK ACCOUNT LOGINS CREDIT CARD SKIMMERS FOR SALE.url·favicon



11) Raylen\Raylen's Laptop\Users\Encase\Favorites\Skimming Device-Skimming Device Manufacturers, Suppliers and Exporters on Alibaba.com.url

12) Raylen\Raylen's Laptop\Users\Encase\Favorites\Personal\Air France - flights schedules.url

13) Raylen\Raylen's Laptop\Users\Encase\Favorites\Personal\Itinerary.url

14) Raylen\Raylen's Laptop\Users\Encase\Favorites\Personal\Itinerary.url·favicon



15) Raylen\Raylen's Laptop\Users\Encase\Favorites\Personal\Air France - flights schedules.url·favicon



Notable Files

16) Raylen\Raylen's Laptop\Program Files\EnCase6\Config\Keywords.ini

17) Raylen\Raylen's Laptop\Users\Encase\AppData\Local\IconCache.db

18) Raylen\Raylen's Laptop\Personal\Accounts.jpg

19) Raylen\Raylen's Laptop\$Recycle.Bin\S-1-5-21-305837926-1768984753-988666380-1000\My Family Photo.jpg

Video of Interest

Name ATM Skimming Video.wmv

Last Accessed 09/20/12 02:26:04AM

File Created 09/20/12 02:26:04AM

Last Written 09/07/12 01:35:10PM

Entry Modified 09/20/12 02:26:05AM

Logical Size 14,086,241

Hash Value fe4d99bb73cba8cee1c1d05681b28472

Name My Work.txt

Last Accessed 09/14/12 12:50:31AM

File Created 09/14/12 12:50:31AM

Last Written 09/07/12 01:35:10PM

Entry Modified 09/20/12 02:25:54AM

Logical Size 14,086,241

Hash Value fe4d99bb73cba8cee1c1d05681b28472

**Search Summary**

| Hits | First Searched | Last Searched | Search Text |
| --- | --- | --- | --- |
| 410 | 01/25/13 01:23:07PM | 01/25/13 01:26:00PM | Raylen Morgan |
| 19,450 | 01/25/13 01:26:00PM | 01/25/13 01:26:00PM | ATM |
| 129 | 01/25/13 01:26:00PM | 01/25/13 01:26:00PM | Credit Card |
| 3 | 01/25/13 01:26:00PM | 01/25/13 01:26:00PM | Debit Card |
| 44,329 | 01/25/13 01:26:00PM | 01/25/13 01:26:00PM | Account |
| 48,332 | 01/25/13 01:26:00PM | 01/25/13 01:26:00PM | Scheme |
| 0 | 01/25/13 01:26:00PM | 01/25/13 01:26:00PM | Scheming |
| 0 | 01/25/13 01:26:00PM | 01/25/13 01:26:00PM | Defraud |
| 1,178 | 01/25/13 01:26:00PM | 01/25/13 01:26:00PM | Bank |
| 2,523 | 01/25/13 02:50:40PM | 01/25/13 02:50:40PM | \xFF\xD8\xFF[\xE0\xEE] |
| 20,050 | 01/25/13 02:50:40PM | 01/25/13 02:50:40PM | \xFF\xD8\xFF[^\xFE\xE1\xE0\xDB\xEE] |
| 1,956 | 01/25/13 02:50:40PM | 01/25/13 02:50:40PM | GIF8[79]a |
| 449 | 01/25/13 03:02:45PM | 01/25/13 03:02:45PM | Skimming |

**Case Time Settings**

| Account for seasonal Daylight Saving Time | Yes |
| --- | --- |
| Convert all dates to correspond to one time zone | No |

Searching

Status: Completed

Start: 01/25/13 01:23:07PM

Stop: 01/25/13 01:34:17PM

Time: 0:11:10

Files: 81,471

Records: 0

Files scanned: 80,768

Signature mismatches: 2,289

Hash values: 81,070

Search Hits: 435

Added Search Hits: 410

Searching

Status: Completed

Images of Interest

Name ProjectTemplate.docx

Last Accessed 09/14/12 12:48:07AM

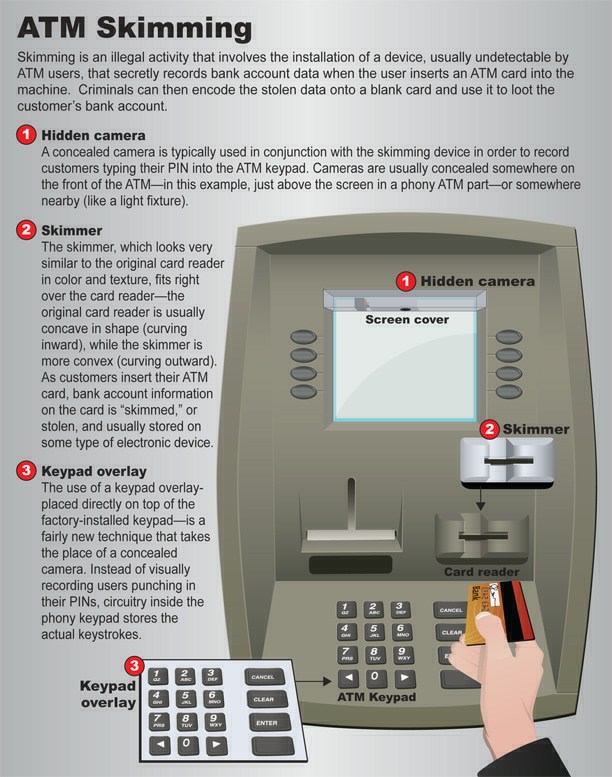
File Created 09/14/12 12:48:07AM

Last Written 09/04/12 11:54:04PM

Entry Modified 09/14/12 04:26:28AM

Logical Size 325,279

Hash Value 9f98dd1e1935a04dda9170a08ccb8781



Name ATM location.jpg

Last Accessed 09/20/12 02:26:32AM

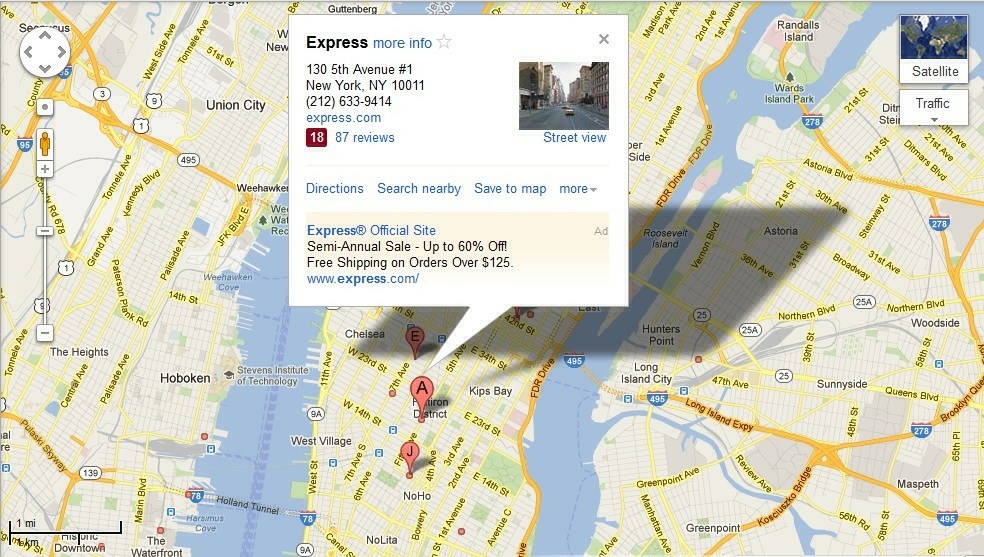
File Created 09/20/12 02:26:32AM

Last Written 09/20/12 01:52:56AM

Entry Modified 09/20/12 02:26:32AM

Logical Size 272,423

Hash Value 658d664a6ee0a3cdcc7c00952ee6d7f1



Name atm skimmer 1.jpg

Last Accessed 09/20/12 02:31:00AM

File Created 09/20/12 02:31:00AM

Last Written 09/20/12 02:05:46AM

Entry Modified 09/20/12 02:32:20AM

Logical Size 110,504

Hash Value 0896033ce384ccab1392f40278dce063



Name atm\_render.jpg

Last Accessed 09/14/12 12:45:17AM

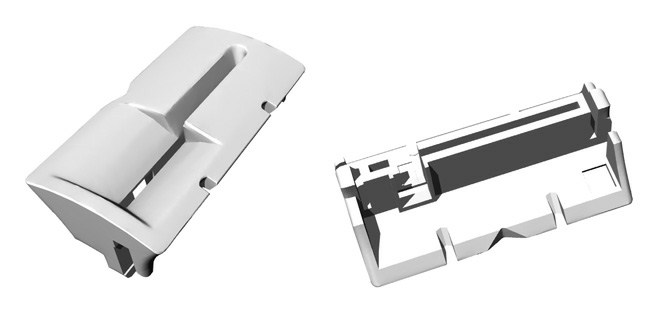
File Created 09/14/12 12:45:17AM

Last Written 09/08/12 03:17:30AM

Entry Modified 09/14/12 12:45:32AM

Logical Size 26,400

Hash Value 42d3a9cbff13be80c9ca94859be7e303



Name blank\_card.jpg

Last Accessed 09/14/12 12:45:17AM

File Created 09/14/12 12:45:17AM

Last Written 09/05/12 01:34:38AM

Entry Modified 09/14/12 12:45:32AM

Logical Size 14,215

Hash Value 8919c66abc424f35350ac0544bb8787d



Name fix atm skimmer.jpg

Last Accessed 09/20/12 02:31:00AM

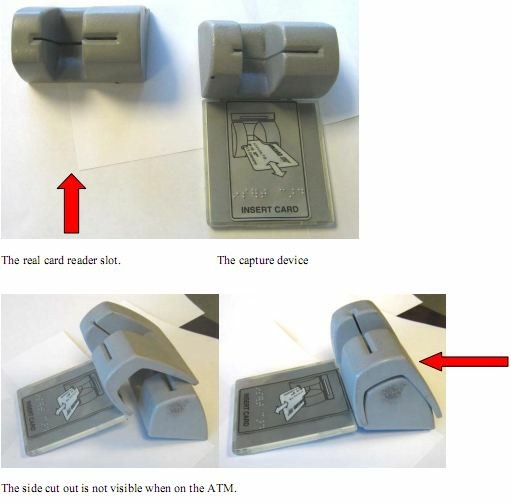
File Created 09/20/12 02:31:00AM

Last Written 09/20/12 02:06:30AM

Entry Modified 09/20/12 02:32:20AM

Logical Size 36,128

Hash Value 1f12d4b71ada328e8cbb9be6ae3656f0



Name spycam.jpg

Last Accessed 09/14/12 12:45:17AM

File Created 09/14/12 12:45:17AM

Last Written 09/08/12 01:20:10AM

Entry Modified 09/14/12 12:45:32AM

Logical Size 27,180

Hash Value c595d4ffd5de09d1e05bcb6305e156e1



Name Eiffel Tower Paris.jpg

Last Accessed 09/14/12 12:44:32AM

File Created 09/14/12 12:44:32AM

Last Written 09/13/12 01:04:00AM

Entry Modified 09/14/12 12:44:32AM

Logical Size 89,608

Hash Value b9126a74e099609d37ab6b8aef5fdd91



Name map.jpg

Last Accessed 09/14/12 12:44:32AM

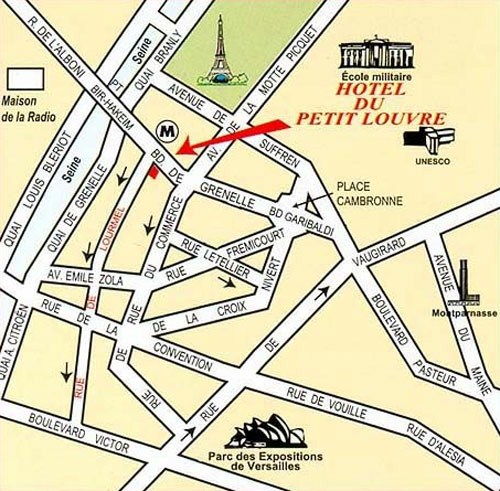
File Created 09/14/12 12:44:32AM

Last Written 09/14/12 12:06:40AM

Entry Modified 09/14/12 12:44:32AM

Logical Size 85,115

Hash Value 2a7bc5555844d1f7fd34c482b6c5e799



Name air france plane.jpg

Last Accessed 09/20/12 02:31:00AM

File Created 09/20/12 02:31:00AM

Last Written 09/20/12 02:13:38AM

Entry Modified 09/20/12 02:32:20AM

Logical Size 210,168

Hash Value feb9b78c2fd40d4a2de125dcbeaf268a



Name Paris Eiffel Panorama.jpg

Last Accessed 09/20/12 02:31:00AM

File Created 09/20/12 02:31:00AM

Last Written 09/20/12 02:11:32AM

Entry Modified 09/20/12 02:32:20AM

Logical Size 7,722,771

Hash Value 6a880004a9b068d36fa8564eac62458c