Test DFI Case #1

Digital Forensic Report

Prepared by:

Naif Hussain (naif.hussain0@gmail.com)

Abdullah Alhakami (aalhakami.26@gmail.com)

Mohammad Alattas (mohammed.Alattas@outlook.sa)

Jawad Fakiha (jawadfageha@gmail.com)

Specialist field:

Digital Forensics

Table of Contents

Digital Forensic Report

1 | Introduction

The purpose of this report is to provide a comprehensive analysis on a SD card that was contained in a Skimming Device connected to an ATM to steal CC information. The facts within this report are those within the prepares own area of expertise and knowledge and do not extend to matters and knowledge outside such expertise.

Image Name:	skimmer_microSD_Physical.e01
SHA-256:	1c5ad394daa49573f4088a31fb7f6a3f537dbcd092fdfd5abc8b572ebedbc262
Bytes per Sector / Sector Count	512 / 33,554,432
Image Type	E01
Notes	Internal description: microSD found in skimmer device at EPFL Postomat.|16GB Size.|
Acquired on OS	Win 10, Build 19042 (64 bit)
Acquired Using	XWF 20.0
Acquired Date	4/9/2021 8:05:21 PM
Unique Description	skimmer_microSD_Physical

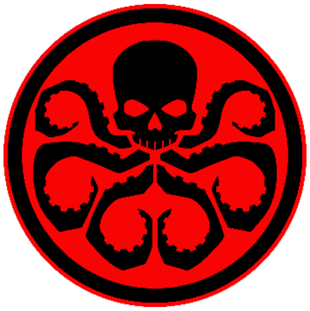
1.1 Summary of Case

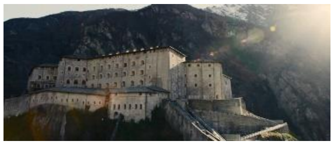
Skimming Device contains an SD card connected to ATM to steal CC information. The event was happened on April 9th, 2021, at 16:25.

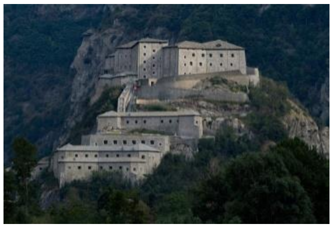
1.2 Software Application

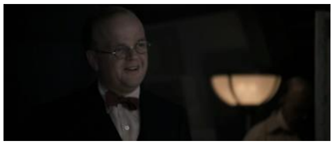
- Autopsy 4.19.3
- AccessData FTK Imager 4.2.0.13
- Audacity
- MagstripeDecoder
- Exiftool

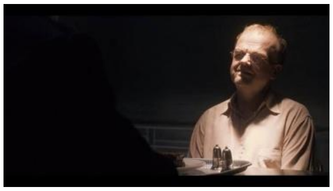
2 | Content Relating to Offence

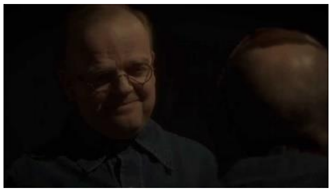
	Filename	f1776330.png
	Location	/img_skimmer_microSD_Physical.e01//$CarvedFiles/f1776330.png
	MIME Type	image/png
	Size	52971
	Modified	-
	Accessed	-
	Created	-
	MD5 Hash	1daefb3706215bf450bd1c3ae2ce873d
	Analysis	Hydra logo

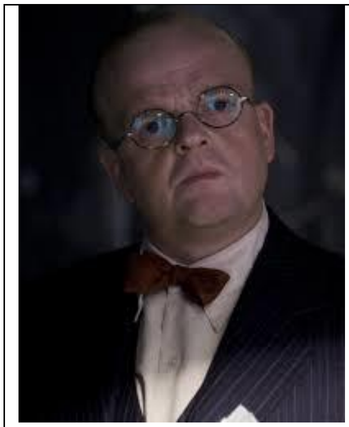
	Filename	f1974175.jpg
	Location	/img_skimmer_microSD_Physical.e01//$CarvedFiles/f1974175.jpg
	MIME Type	image/jpeg
	Size	56776
	Modified	-
	Accessed	-
	Created	-
	MD5 Hash	9f96afd95f63ce272c68c1f83d2748c8
	Analysis	Hydra Research Base

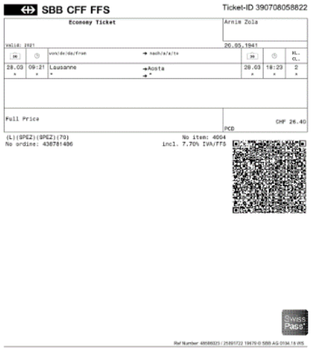
	Filename	f0906533.jpg
	Location	/img_skimmer_microSD_Physical.e01//$CarvedFiles/f0906533.jpg
	MIME Type	image/jpeg
	Size	68185
	Modified	-
	Accessed	-
	Created	-
	MD5 Hash	adcd973854bbe10d17f4b35ce8ec8905
	Analysis	Hydra Research Base

	Filename	f1459779.png
	Location	/img_skimmer_microSD_Physical.e01//$CarvedFiles/f1459779.png
	MIME Type	image/png
	Size	65015
	Modified	-
	Accessed	-
	Created	-
	MD5 Hash	4a442f111021aea457c8baaca0e991e9
	Analysis	Doctor Arnim Zola, a Swiss-born scientist who worked for HYDRA, during, and after World War II.

	Filename	f1459906.jpg
	Location	/img_skimmer_microSD_Physical.e01//$CarvedFiles/f1459906.jpg
	MIME Type	image/jpeg
	Size	29703
	Modified	-
	Accessed	-
	Created	-
	MD5 Hash	4a913e0006786d5372bfebb3a4b7db78
	Analysis	Doctor Arnim Zola, a Swiss-born scientist who worked for HYDRA, during, and after World War II.

	Filename	f0906675.jpg
	Location	/img_skimmer_microSD_Physical.e01//$CarvedFiles/f0906675.jpg
	MIME Type	image/jpeg
	Size	15914
	Modified	-
	Accessed	-
	Created	-
	MD5 Hash	777695e55f10dd2507d9a6005278678d
	Analysis	Doctor Arnim Zola, a Swiss-born scientist who worked for HYDRA, during, and after World War II.

<table>
<tr><td rowspan="9"></td><td>Filename</td><td>f0906667.jpg</td></tr>
<tr><td>Location</td><td>/img_skimmer_microSD_Physical.e01//$CarvedFiles/f0906667.jpg</td></tr>
<tr><td>MIME Type</td><td>image/jpeg</td></tr>
<tr><td>Size</td><td>3946</td></tr>
<tr><td>Modified</td><td>-</td></tr>
<tr><td>Accessed</td><td>-</td></tr>
<tr><td>Created</td><td>-</td></tr>
<tr><td>MD5 Hash</td><td>9ffc15e326ef989db6d0b08276af103e</td></tr>
<tr><td>Analysis</td><td>Doctor Arnim Zola, a Swiss-born scientist who worked for HYDRA, during, and after World War II.</td></tr>
</table>

<table>
<tr><td rowspan="11">
SBB CFF FFS Ticket-ID 390708058822
Economy Ticket
Arnim Zola
Valid: 2021
20.05.1941
von/de/da/from → nach/a/a/to Kl. Cl.
28.03 09:21 Lausanne →Aosta 28.03 18:23 2
Full Price
CHF 26.40
PCD
(L)(SPEZ)(SPEZ)(70)
No ordine: 438781486
No item: 4004
incl. 7.70% IVA/FFS
Swiss Pass
Ref Number: 48608023 / 25891722 19679 © SBB AG 0104.18 WS</td><td>Filename</td><td colspan="2">f0905815_ticket_pdf.pdf</td></tr>
<tr><td>Location</td><td colspan="2">/img_skimmer_microSD_Physical.e01//$CarvedFiles/f0905815_ticket_pdf.pdf</td></tr>
<tr><td>MIME Type</td><td colspan="2">application/pdf</td></tr>
<tr><td>Size</td><td colspan="2">124864</td></tr>
<tr><td>Author</td><td colspan="2">ArnimZola</td></tr>
<tr><td>Modified (Metadata)</td><td colspan="2">2021-03-27 14:37:08 AST</td></tr>
<tr><td>Accessed</td><td colspan="2">-</td></tr>
<tr><td>Created (Metadata)</td><td colspan="2">2021-03-27 14:37:08 AST</td></tr>
<tr><td>MD5 Hash</td><td colspan="2">0df93f0eae98a8669aed40c138710e83</td></tr>
<tr><td rowspan="2">Analysis</td><td colspan="2">An economy ticket from Swiss Federal Railways (SBB CFF FFS) that was booked for Arnim Zola.
The trip time = 8 hours and 2 minutes.
Ticket Price : 26.40 CHF (Swiss franc currency of Switzerland).</td></tr>
<tr><td>From Lausanne (Capital of the canton Vaud on Switzerland).
Take off : 28/03/2021 - 9:21 AM</td><td>To Aosta (Capital of the Valle d'Aosta region, in northwestern Italy).
Lands : 28/03/2021 – 18:23 (6:23 PM)</td></tr>
</table>

🔊	Filename	recording.mp3
	Location	/img_skimmer_microSD_Physical.e01/recording.mp3
	MIME Type	audio/mpeg
	Size	4335015
	Modified	2021-04-09 23:24:56 AST
	Accessed	2021-04-09 00:00:00 AST
	Created	2021-04-09 23:20:01 AST
	MD5 Hash	b52421a7547369a770b892026d1b25d0
	Analysis	Magnetic stripes for credit cards information as an audio format (will be explained in Intention phase).

🔊	Filename	2021_04_09T1621.mp3
	Location	/img_skimmer_microSD_Physical.e01/2021_04_09T1621.mp3
	MIME Type	audio/mpeg
	Size	1301392
	Modified	2021-04-09 23:21:28 AST
	Accessed	2021-04-09 00:00:00 AST
	Created	2021-04-09 23:21:25 AST
	MD5 Hash	066c187f3010f62a56c82298116ec3f8
	Analysis	A part of recording.mp3, which contains magnetic stripes for credit cards information as an audio format (will be explained in Intention phase).

3 | Identification

Statements and evidence collected identified Hydra Organization is behind the incident and agent Arnim Zola as a suspect of the skimming crime.

- Hydra logo and Arnim Zola photos were deleted from the SD card which indicates a removing footprints intention.
- Two photos for Hydra Research Base in Sokovia was found in the SD card which indicates the involvement of Hydra in the crime.
- A railway ticket for Arnim Zola was found which indicates that Arnim played an important role in the crime.

4 | Intent

First we should know how does the skimming device works?

When a card is slid past the magnetic reader, the MP3 player sniffs the data stored on the card’s magnetic stripe and records it as an audio file to the SD card. “Some of the earliest skimming devices observed in Sweden were COTS MSR hardware based skimmers, encapsulated in fake slot-in readers and attached onto ATMs. The more advanced contained recordable MP3 players embedded in homemade ATM panels. Each time a magstripe card was put into the slot, the MP3 player recorded the analogue data on the magnetic stripe – typically track 2. In the most likely scenario, after the skimmer was removed, the audio file was decoded in the same way as for regular magnetic stripe card readers.”[1]

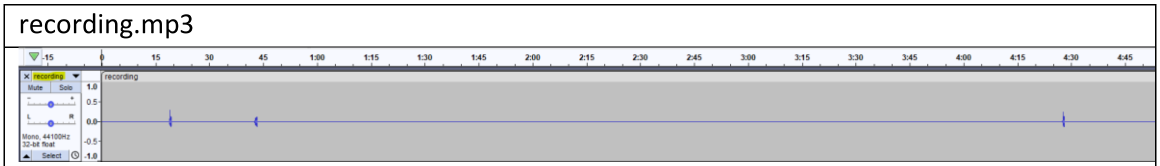
How does the regular magnetic stripe card reader works?

The magnetic stripe reader reads the information by detecting the changes in the magnetic field caused by the flux reversals on the badge's magnetic stripe.

How to extract the data (CC information) from the magstripe from the audio?

Using Magnetic-StripeDecoder program written in C#, we can extract the stolen credit cards information. For more information on how it works and how that data is stored.[2]

recording.mp3

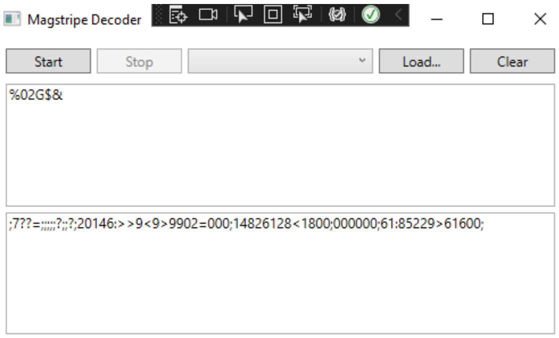


Analysis

Playing the audio file the only thing we can hear is a confusion.

Firstly we convert the audio file to wav (file uncompressed) because mp3 audio files are compressed and may affect the magnetic stripes because they are sensitive. From our understanding we know that this is a magnetic stripe because skimming devices uses this technique to store credit cards information.[3]

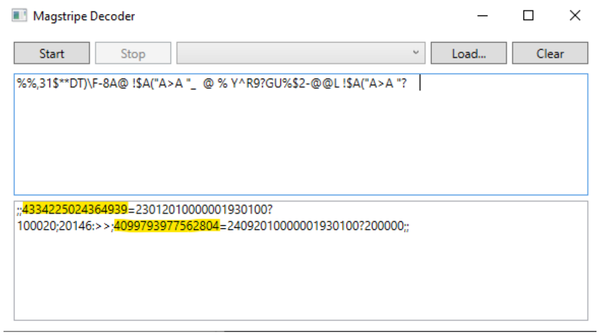
Therefore we tried to decode it using Magnetic-StripeDecoder, but there was nothing but weird numbers on both track 1 and track 2.



```
%02G$&
```

```
;7??=;;;;;?;;?;20146:>>9<9>9902=000;14826128<1800;000000;61:85229>61600;
```

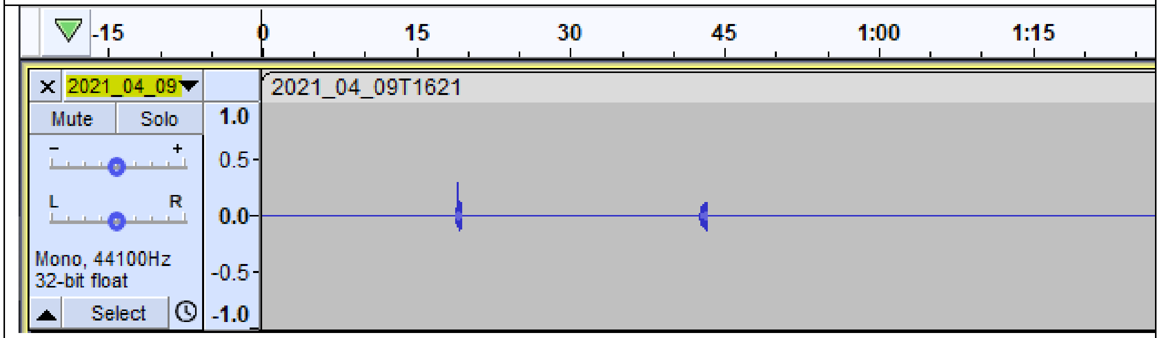
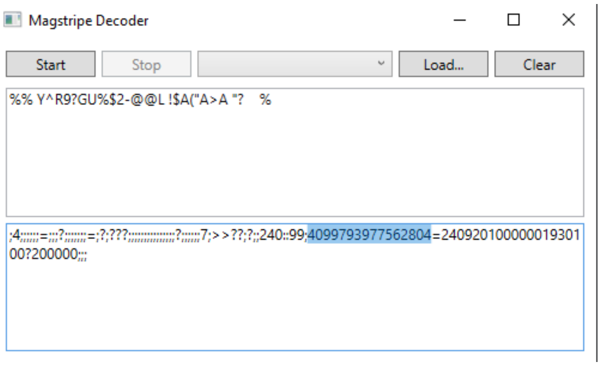
After that we tried to do some Steganography analysis, we reversed the audio file track and tried to decode it again, then we got credit cards information on track 2 for two cards.



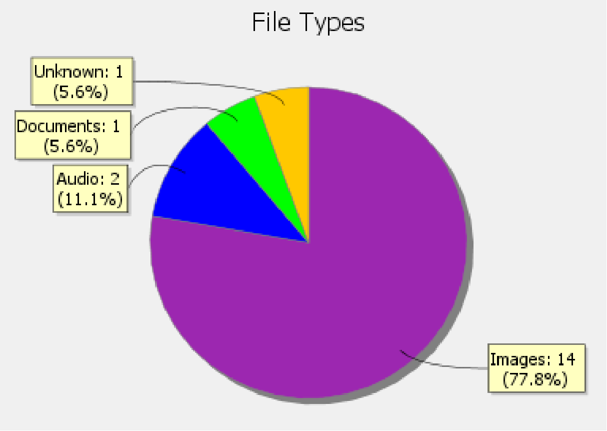
```
%%,31$**DT)\F-8A@ !$A("A>A "_  @ % Y^R9?GU%$2-@@L !$A("A>A "?
```

```
;;4334225024364939=23012010000001930100?
100020;20146:>>;4099793977562804=24092010000001930100?200000;;
```

As shown track 2 contains information about these cards:
CC Number : 4334 2250 2436 4939 (Visa card)
CC Number : 4099 7939 7756 2804 (Visa card)

2021_04_09T1621.mp3	
 -15 0 15 30 45 1:00 1:15 2021_04_09 Mute Solo L R Mono, 44100Hz 32-bit float Select 1.0 0.5 0.0 -0.5 -1.0 2021_04_09T1621	
Analysis	Playing the audio file the only thing we can hear is a confusion. Firstly we convert the audio file to wav (file uncompressed) because mp3 audio files are compressed and may affect the magnetic stripes because they are sensitive. While analyzing this audio file we compared it to the first audio file (recording.mp3) and we discovered that this audio file is just a part of the first audio file, therefore it followed the same steganography technique. It contains a part of the magnetic stripe that we already decoded before, as a result when we decoded it we discovered that the magnetic stripe is related to this card :  %% Y^R9?GU%$2-@@L !$A("A>A "? % ;4;;;;;;=;;;?;;;;;;=;?;???;;;;;;;;;;;;;;?;;;;;7;>>??;?;;240::99;4099793977562804=24092010000001930100?200000;;; Track 2 contains information about these cards: CC Number : 4099 7939 7756 2804 (Visa card)

5 | Quantity of Files



File Type	Quantity
JPEG	12
PNG	2
MP3	2
PDF	1

6 | Timeline of Events

List of events or activities that took place in the accident.

Date / Time	Description	Event Type	Analysis
2021-04-09 23:20:01 AST	recording.mp3 was created.	File creation	The recording.mp3 was created from the magnetic stripe of two cards.
2021-04-09 23:21:25 AST	2021_04_09T1621.mp3 was created.	File creation	The 2021_04_09T1621.mp3 is basically a part of recording.mp3, and it has only a one magnetic stripe of one card.

7 | References

List of References:

[1]. Paper: DIVING INTOMAGNETIC STRIPECARD SKIMMINGDEVICES by Johnny Bengtsson

https://journals.sas.ac.uk/deeslr/article/view/1866/1803

[2]. How magnetic stripe cards work By Jacobo Tarrío

http://jacobo.tarrio.org/know/how-magnetic-stripe-cards-work

[3]. How to read Magstripes and a detailed analysis on the data

https://www.youtube.com/watch?v=fLWA0bG5XyQ&ab_channel=Th3Y34r3000