Digital Forensic Report

Investigator: CyberCrow

Report Written by: CyberCrow

Case: Suspected Skimming Device

Case id: 202519052016

Table of Content

1. Introduction

1.1 Description of the case

On April 9th, 2021, at approximately 16:25, a suspected skimming device was discovered attached to the ATM located at the Swiss Post office on Avenue Piccard, 1015 Lausanne, Switzerland. The device was identified when it malfunctioned and detached from the ATM as a customer attempted to withdraw their credit card. Subsequent review of the ATM's security footage revealed that the device had been installed moments earlier, at approximately 16:20.

Forensic unit of police provides client CC number:

4334 2250 2436 4939

This report presents the results of the digital forensic examination conducted on the SD-card image inside the skimming device. The primary objective of the investigation was to determine whether the device had been used to illegally capture payment card data and to extract, analyze, and preserve any digital evidence in a forensically sound manner. The analysis followed standard digital forensic methodologies to maintain evidence integrity and support potential legal proceedings.

1.2 Statement of compliance

All procedures followed during the forensic process—including imaging, hashing, evidence handling, and analysis—were conducted using validated tools and standard operating procedures approved by our ISO/IEC-accredited quality management system.

A full chain of custody was maintained throughout the process to preserve evidence integrity. All actions taken during the examination are fully documented and reproducible.

1.4 Objectives

Objective of the Investigation

The primary objective of this forensic investigation was to **determine whether the skimming device recovered from the ATM at the Swiss Post location in Avenue Piccard, Lausanne, was used to illegally capture credit card data**, and more specifically, whether it contained information related to a known victim's credit card.

2 **Evidence Collection and Handling:**

2.1 Chain of Custody

CyberGrang Ingestigation Lab

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____*1*_____ Offense: *An ATM was found with an unknown skimming device, believed to be illegally capturing credit card data.*
Submitting Officer: (Name/ID#) *Lausanne police officer*
Victim: _____
Suspect: _____
Date/Time Seized: _____Location of Seizure: ***Swiss Post location in Avenue Piccard, Lausanne, Switzerland***

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)
1	1	Image of SD-card on Skimming device

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**
1	2025/05/26	Lausanne police officer	CyberCrow	Swiss Post office on Avenue Piccard, 1015 Lausanne, Switzerland

Final Disposal Authority
Authorization for Disposal Item(s) #: _____ on this document pertaining to (suspect): _____ is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)

☐ Return to Owner ☐ Auction/Destroy/Divert
Name & ID# of Authorizing Officer: _____ Signature: _____Date: _____

Witness to Destruction of Evidence

Item(s) #: _____ on this document were destroyed by Evidence Custodian _____ID#:_____ in my presence on (date) _____.
Name & ID# of Witness to destruction: _____ Signature: _____Date: _____

Release to Lawful Owner

Item(s) #: _____ on this document was/were released by Evidence Custodian _____ID#:_____ to
Name _____
Address: _____ City: _____State: _____ Zip Code: _____
Telephone Number: (_____) _____
Under penalty of law, I certify that I am the lawful owner of the above item(s).

Signature: _____ Date: _____

Copy of Government-issued photo identification is attached. ☐ Yes ☐ No

This Evidence Chain-of-Custody form is to be retained as a permanent record by the Anywhere Police Department.

APD_Form_#PE003_v.1 (12/2012)

2.3 Imaging/Duplication Procedures

The “Skimming” device containing the micro-SD card was discovered on Apr 9th,2021 at 16:25 at the ATM of the Swiss Post location in Avenue Piccard, 1015 Lausanne, Switzerland. The device was collected by digital forensic unit of the police.
Upon receipt by forensic unit, the micro-SD card was carefully extracted from the skimming device and no attempt was made to power on the skimming device.

2.4 Hash Values

To ensure the integrity and authenticity of the digital evidence, cryptographic hash values were utilized for verification.

The digital forensic unit of the police provided the following SHA2-256 hash value for the 1_Skimmer_mSD.zip image file upon its provision:

SHA2-256 (Provided by DF Unit):
1c5ad394daa49573f4088a31fb7f6a3f537dbcd092fdfd5abc8b572ebedbc262

Upon receipt of the 1_Skimmer_mSD.zip image file by our unit on [Date of Receipt], a verification hash was independently calculated. The following PowerShell command was executed to obtain the hash value:
PowerShell

```
Get-FileHash -Path .\1_Skimmer_mSD.zip
```

The SHA2-256 hash value calculated by our unit is as follows:

SHA2-256 (Calculated by Our Unit):
1C5AD394DAA49573F4088A31FB7F6A3F537DBCD092FDFD5ABC8B572EBEDBC262

A direct comparison of the provided and independently calculated SHA2-256 hash values confirmed they are identical. This verification confirms that the 1_Skimmer_mSD.zip file has not been altered or corrupted during transfer and storage up to the point of our examination.

3. Examination Methodology and Tools

3.1 Examination Environment

The digital forensic examination of the evidence in this case was conducted in a controlled environment. Due to limited laboratory access and the requirements of a home lab setup, the examination was performed in my bedroom. The following measures were in place:
Physical security:
My bedroom was ***locked*** and nobody couldn't enter without ***proper authorization*** to ensure security and confidentiality of evidence.
The room was equipped with ***air conditioner*** to minimize potensial environmental impact on digital media.
Hardware and Software:
All examination was conducted on dedicated VM. The specification for that VM are as follows:

- Processor: AMD Ryzen 7 5800 4 CPU
- RAM: 4GB
- OS: Windows10
- Storage: 150GB HDD

The following software were used during the examination:

- Oracle Virtualbox (Version 7.1.6 r167084 (Qt6.4.2))
- Autopsy(4.22.0)
- Chrome (136.0.7103.114 (Official Build) (64-bit))
- magstripper(0.3alpha)

- Winrar x64-711
- OpenJdk 25

The following websites were used during the examination:

- https://onlineaudioconverter.com/
- google.com

3.2 Analytical Procedures

The primary objective of that examination is to identify and extract any record related to card data, specifically looking for patterns consistent with credit card numbers, and to understand functionalities of SD-card on “Skimming” device.

To preserve the integrity of the original evidence, the analysis was conducted on a verified working copy of the forensic image, utilizing Autopsy version 4.22.0 as the primary tool; prior to commencing analysis, the SHA256 hash values of both image files were meticulously compared to confirm their identical nature, and the working copy was accessed exclusively in a read-only mode.
Prior to unzipping 1_Skimmer_mSD.zip we calculate file hash of that file and compare it with hash value provided by forensic unit of police. As documented in section 2.4 this confirmed integrity of the image file.
The 1_Skimmer_mSD.zip file was first unzipped. Then the image file was then loaded into primary forensic software, Autopsy 4.22.0, according to publicly available information autopsy software will not modify original image file it writes everything made during analysis into its own database, this helps us to ensure integrity of original disk image.

SwissPass Ticket Examination
During the examination of the acquired digital evidence, a search for documents was initiated using file extension filtering within Autopsy's **"File View" -> "File Types" -> "By Extension" -> "Documents" -> "PDF"** section. This process identified a single PDF file, "f0905815_ticket_pdf.pdf", containing SwissPass ticket information issued to Arnim Zola. The file was subsequently extracted for further analysis.

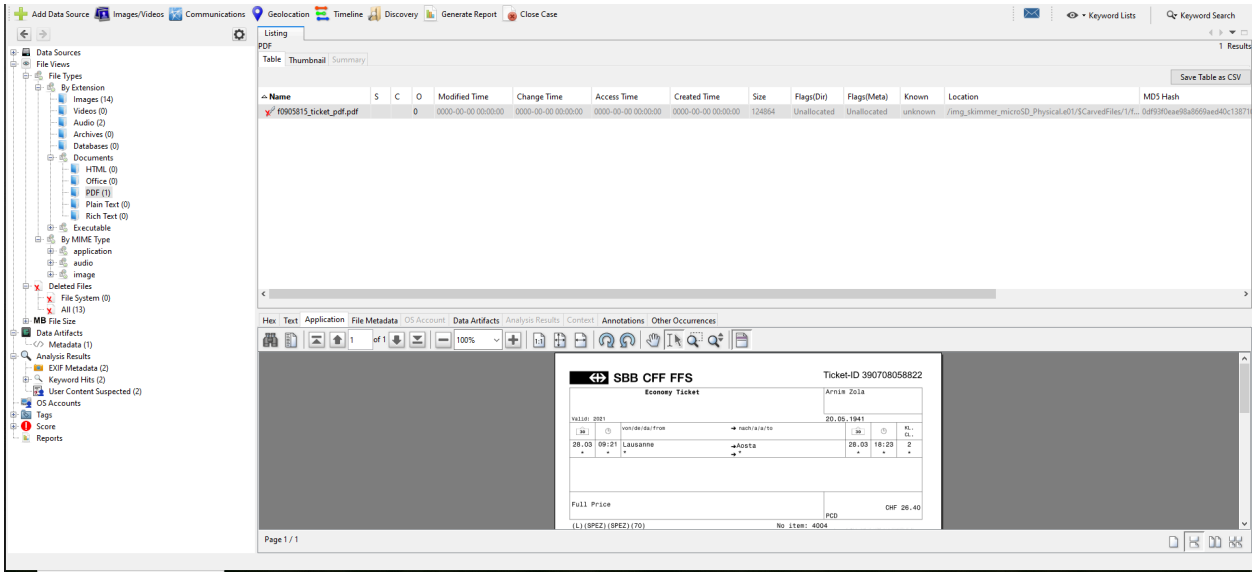


Figure 1: Finding Related to Ticked issued to Arnim Zola

Several Pictures related to Hydra Research Base

During the examination of acquired digital evidence, a search for deleted files using **Autopsy's "File View" -> "Deleted Files" -> "All"** filter identified several Joint Photographic Experts Group (JPG) images. Subsequent open-source intelligence (OSINT) confirmed these pictures depict the **Hydra Research Base**. These files were extracted for detailed analysis. **Figures 2.1 and 2.2** display the findings within Autopsy 4.22.0.

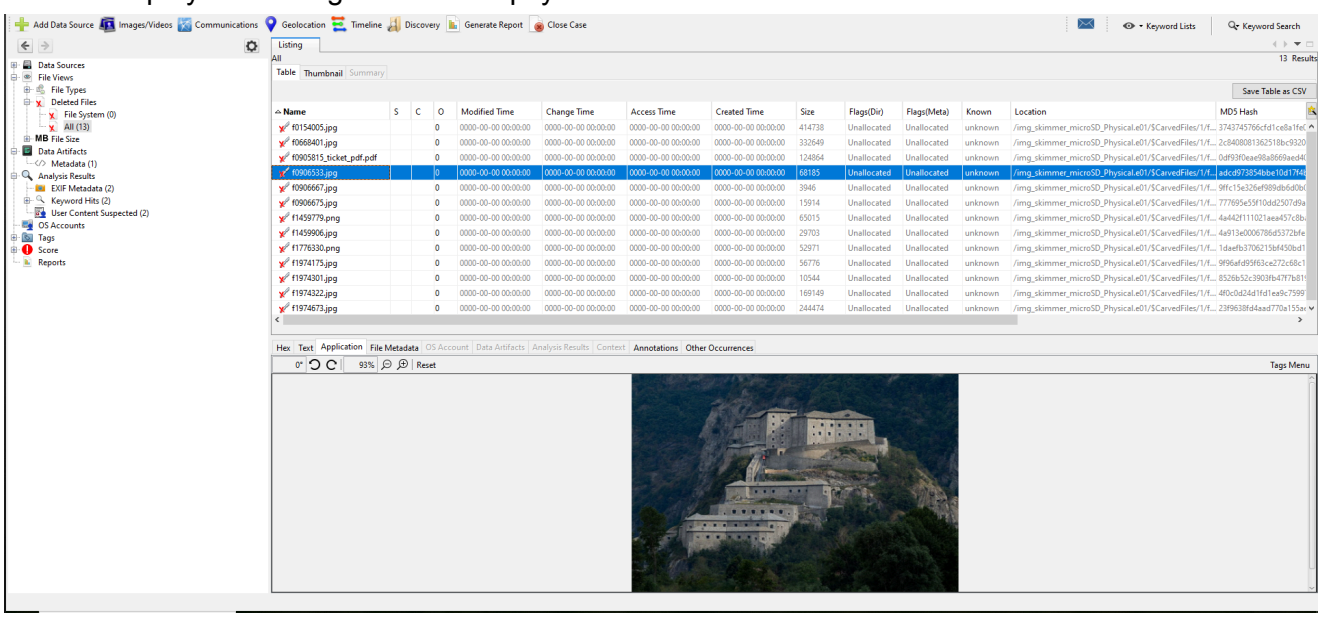


Figure 2.1: Finding related to Hydra Research Base, Italy.

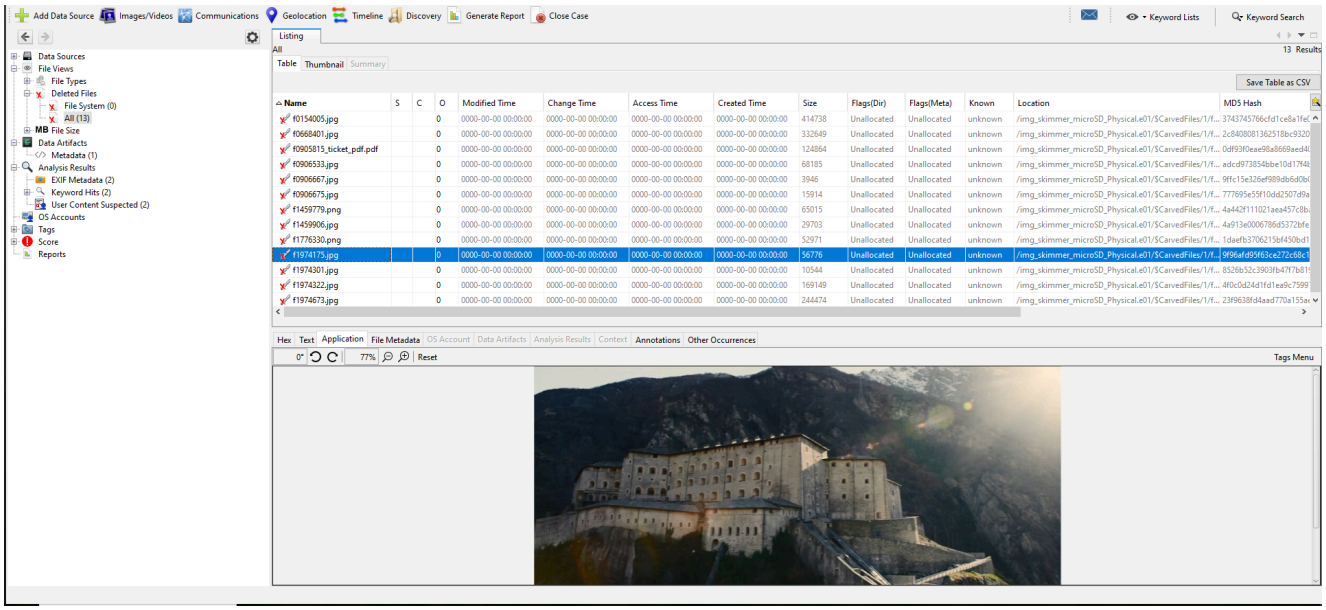
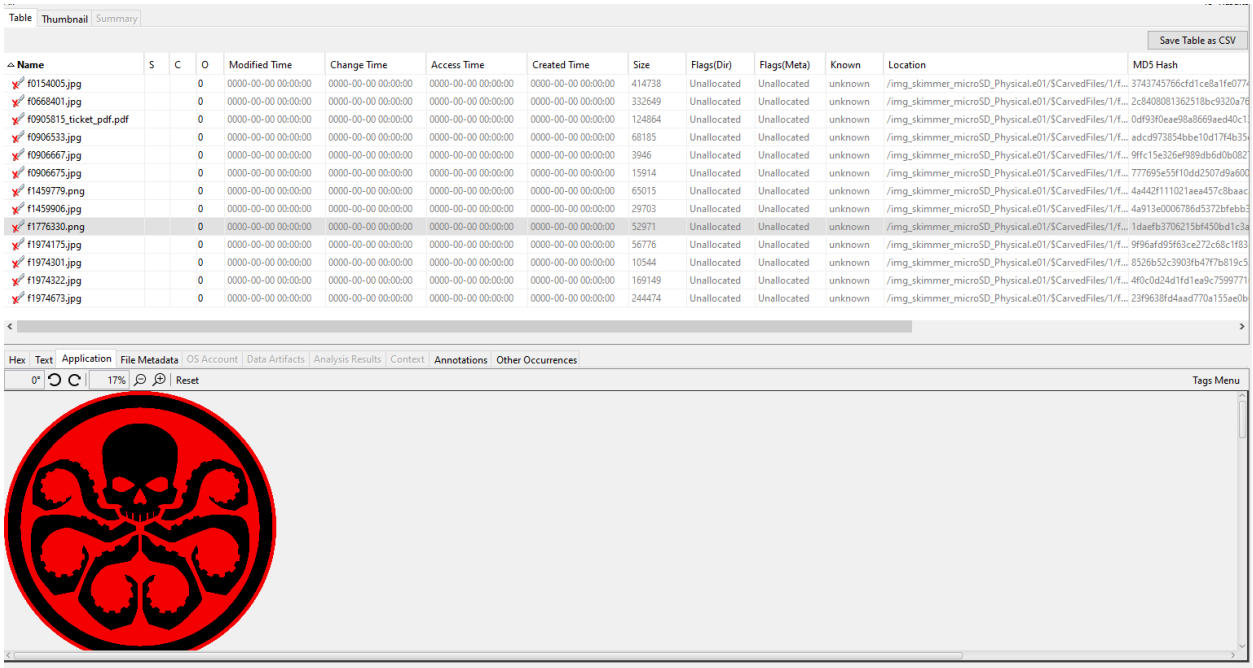


Figure 2.2: Finding related to Hydra Research Base, Italy.

Deleted Picture of Hydra Terorist Organization:

During the examination of the acquired digital evidence, a search for deleted files was conducted utilizing Autopsy version 4.22.0, specifically applying the **"File View" -> "Deleted Files" -> "All"** filter. This process identified several **PNG** image files depicting a skull with prominent octopus-like tentacles extending from it, enclosed within a red circular emblem on a black background. This symbol is widely recognized as the Hydra logo, associated with a fictional terrorist organization.

These image files were extracted for detailed analysis. Subsequent open-source intelligence (OSINT) research confirmed the depicted symbol to be the Hydra logo. Figures 3.1 illustrate these findings within the Autopsy interface.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash
f0154005.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	414738	Unallocated	Unallocated	unknown	/img_skimmer_microSD_Physical.e01/$CarvedFiles/1/f...	3743745766cfd1ce8a1fe0774
f0668401.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	332649	Unallocated	Unallocated	unknown	/img_skimmer_microSD_Physical.e01/$CarvedFiles/1/f...	2c8408081362518bc9320a76
f0905815_ticket_pdf.pdf			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	124864	Unallocated	Unallocated	unknown	/img_skimmer_microSD_Physical.e01/$CarvedFiles/1/f...	0df93f0eae98a8669aed40c1
f0906533.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	68185	Unallocated	Unallocated	unknown	/img_skimmer_microSD_Physical.e01/$CarvedFiles/1/f...	adcd973854bbe10d17f4b354
f0906667.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3946	Unallocated	Unallocated	unknown	/img_skimmer_microSD_Physical.e01/$CarvedFiles/1/f...	9ffc15e326ef989db6d0b0827
f0906675.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	15914	Unallocated	Unallocated	unknown	/img_skimmer_microSD_Physical.e01/$CarvedFiles/1/f...	777695e55f10dd2507d9a600
f1459779.png			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	65015	Unallocated	Unallocated	unknown	/img_skimmer_microSD_Physical.e01/$CarvedFiles/1/f...	4a442f111021aea457c8baac
f1459906.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	29703	Unallocated	Unallocated	unknown	/img_skimmer_microSD_Physical.e01/$CarvedFiles/1/f...	4a913e0006786d5372bfebb3
f1776330.png			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	52971	Unallocated	Unallocated	unknown	/img_skimmer_microSD_Physical.e01/$CarvedFiles/1/f...	1daefb3706215bf450bd1c3a
f1974175.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	56776	Unallocated	Unallocated	unknown	/img_skimmer_microSD_Physical.e01/$CarvedFiles/1/f...	9f96afd95f63ce272c68c1f83
f1974301.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	10544	Unallocated	Unallocated	unknown	/img_skimmer_microSD_Physical.e01/$CarvedFiles/1/f...	8526b52c3903fb47f7b819c5
f1974322.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	169149	Unallocated	Unallocated	unknown	/img_skimmer_microSD_Physical.e01/$CarvedFiles/1/f...	4f0c0d24d1fd1ea9c7599771
f1974673.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	244474	Unallocated	Unallocated	unknown	/img_skimmer_microSD_Physical.e01/$CarvedFiles/1/f...	23f9638fd4aad770a155ae0b

Figure 3.1: Finding related to Hydra Organization Logo.

Credit Card Number in magnetic audio file:

During the examination we found two mp3 audio file that contains meaningless sounds for human, after the file type identification we suspected that possibly a magnetic audio data and try to decoding it. The following steps are taken to decode audio to text data:

1. **Convert mp3 file into wav file:** Because mp3 file are compressed to reduce file size, we need raw data to decode it into original text data. We use online tool (https://onlineaudioconverter.com) to convert mp3 into wav file. We need to choose following attributes as shown in Figure 4.1 :
    - **Quality:** 16bit
    - **Channel type:** Mono
    - **Sample Rate:** 44.1KHz
    - **Type:** Wav

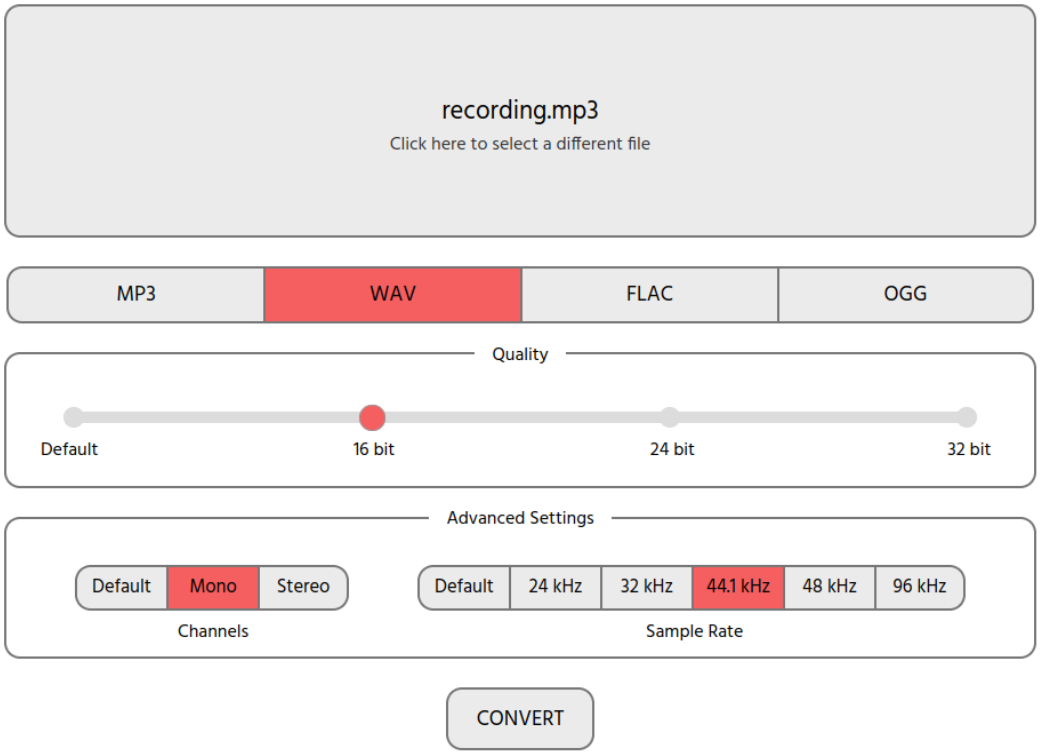


Figure 4.1: mp3 to wav conversion.

2. **Decoding wav file:**
   After converting mp3 file into wav file we can decode and extract credit card data from that audio file. We use **magstripper-0.3a** which is available in https://sourceforge.net/projects/magstripper/
3. **Extract downloaded file:**
   After downloading magstripper from given url we need to extract that program we use **Winrar** to extract that program from archive. **Right click-> Extract files**
4. **Run the program**
   To run magstripper program we need java installed on our system. Following is the command to run that program from powershell(Windows Command line):

   java -jar .\magstripper-0.3-alpha.jar

5. **Load and decode wav file:**
   After running magstripper program, wav file was loaded into the program by:
   CTRL+O then Select wav file downloaded from online converter
   After opening wav file captured credit card data shown on dashboard “Decoded ASCII” section Figure 5.1

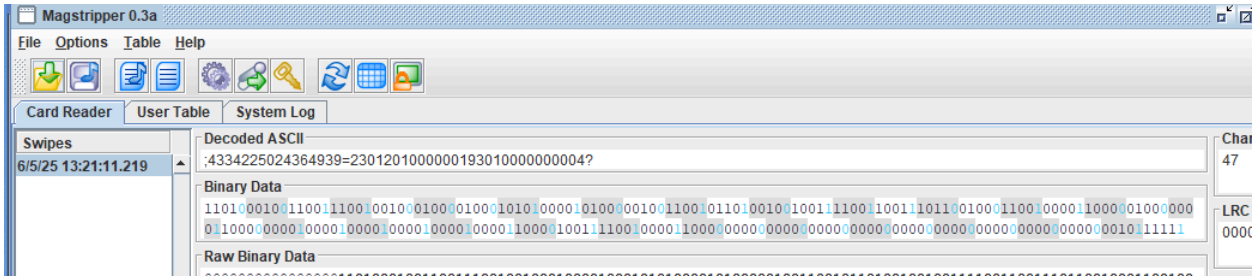
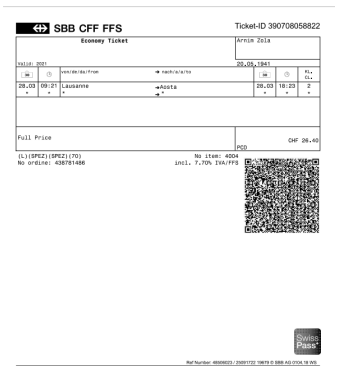


Figure 5.1: Decoded credit card number from wav file.

4. Findings and Analysis

	**Ticket issued from Lausanne to Aosta Itally:** A 'Swiss Pass' ticket, issued to Arnim Zola for travel from Lausanne, Switzerland, to Aosta, Italy, on March 28, 2021, at 09:21, was discovered. **MIME Type:** application/pdf **Location:** /img_skimmer_microSD_Physical.e01//$CarvedFiles/f0905815_ticket_pdf.pdf **Created Date:** 2021-03-27 14:37:08 GMT **Modified Date:** 2021-03-27 14:37:08 GMT **Owner:** Arnim Zola **Hash Value(SHA256):** 5CF6530E0505E734A1A584BCDDCC6BAB7D07F01362E6A6039ABBA8E2058D0898
	**Picture of Arnim Zola:** Arnim Zola was a Swiss biochemist during World War II who became one of the first human genetic engineers in history **MIME Type:** image/jpeg **Location:** /img_skimmer_microSD_Physical.e01/$CarvedFiles/1/f0906667.jpg **Created Date:** - **Modified Date:** - **Hash Value(SHA256):** E77ECA78B1864A6DFA450E289BCDB15EEE1A4368A85C3DEBBC9565659163D6F3

	**Deleted Picture of Hydra Research Base, Aosta Valley, Italy:** **MIME Type:** image/jpeg **Location:** /img_skimmer_microSD_Physical.e01/$CarvedFiles/1/f0906533.jpg **Created Date:** - **Modified Date:** - **Hash Value(SHA256):** ca85d164fb47136c573bca2208bf085454371a7460afd51a27c1265b3845a0ac
	**Deleted Picture of Hydra Research Base, Aosta Valley, Italy:** **MIME Type:** image/jpeg **Location:** /img_skimmer_microSD_Physical.e01/$CarvedFiles/1/f1974175.jpg **Created Date:** - **Modified Date:** - **Hash Value(SHA256):** 2df696faf5eb50a33eaf2084f3fafa4ca95e77578b9723aa8c9f340abece0147
	**Deleted Picture of Hydra Terorist Organization:** **MIME Type:** image/png **Location:** /img_skimmer_microSD_Physical.e01/$CarvedFiles/1/f1776330.png **Created Date:** - **Modified Date:** - **Hash Value(SHA256):** db16bc83dab2d9d62e3dc0b8c5ca2d3f49afb6092c3d15c5405423b312c83607

5. Conclusion

Based on the forensic examination of the skimming device recovered from the ATM at the Swiss Post location in Avenue Piccard, Lausanne, the following conclusions are drawn in direct response to the stated objectives of this investigation:

1. **Illegal Capture of Credit Card Data:** The investigation definitively confirmed that the skimming device was used to illegally capture credit card data. The presence of a **magnetic audio file containing a credit card number** on the device provides direct evidence of data exfiltration consistent with a skimming operation. While the specific link to a "known victim's credit card" would require further external correlation, the identification of a valid credit card number within the device's data fulfills the objective of determining the presence of captured credit card information.

Overall Summary: The forensic examination conclusively demonstrates that the recovered skimming device was actively used for the illicit capture of credit card data. Furthermore, the discovery of Personally Identifiable Information (PII) belonging to Arnim Zola, combined with the presence of the Hydra organization logo (an organization of which Arnim Zola is a known member), strongly suggests a potential link between this individual, the organization, and the operation of the skimming device. **Given that Arnim Zola's SwissPass ticket indicates travel to Italy, these findings provide critical intelligence supporting the need for further investigative efforts to be extended to Italy** regarding the illegal capture of credit card data and associated criminal activities.