

ODCUDZENIE BANKOVÝCH ÚDAJOV

AUTOR : ROMAN FEDOR

Link na prezentáciu: <https://bcstudent.fpvucm.sk/~fedorroman/dfa/prezentacia.pdf>

POPIS PRÍPADU:

Na polícií bol nahlásen prípad podozrivého pohybu osoby v blízkosti bankomatu. Podozrivý sa údajne snažil manipulovať s bankomatom. Polícia po príchode v bankomate zaistili skimovacie zariadenie. Toto zariadenie sa používa na čítanie kreditných kariet. V zariadení bola objavená micro-SD karta, ktorá bola poslaná na analýzu. Po prvotnej analýze polícia zistila možnú polohu páchatela ako aj ukradnuté kreditné karty vo forme nahrávky. Na adrese bola budova, v ktorej bola objavená 3-d tlačiareň napojená na Raspberry Pi, s ktorého bola odpojená micro-SD karta. Podozrivá osoba sa ale v budove nenachádzala. Tieto údaje boli poslané do banky, ktorá potvrdila že bol zaznamenaný podozrivý pohyb na účte – kúpa letenky zo Genevy. Podľa tejto letenky bol zadržaný na letisku podozrivý. Po zatknutí bola vytvorená digitálna kópia mobilu podozrivého. Všetky kópie boli uložené na USB kľúč, ktorý bol zaslaný na ďalšiu analýzu.

PREDMET VYŠETROVANIA:

Dataset (cvičenia 1-3) dostupný na:

<https://dfrws.org/dfrws-2021-challenge/>

Filename: 1_Skimmer_mSD.zip

SHA2-256: 1c5ad394daa49573f4088a31fb7f6a3f537dbcd092dfd5abc8b572ebedbc262

Filename : 2_Raspberry_Pi_mSD.zip

SHA2-256 : aabec0c1305e785d1ba5b4ba01c5dacd27cc128fdd32078758be826e75449953

Filename: 3_Samsung GSM_SM-G973F_DS Galaxy S10.zip

SHA2-256: 54877505f1b4eb26c4cb6b43fd6338424660c207e678b773044a4a79d6e374b7

Hľadané súbory:

.mp4, .stl súbory, sms komunikácia, vymazané súbory (.jpg, .png), metadáta

Veľkosť datasetu:

38,5 GB (37 374 súborov dokopy)

5WH ANALÝZA:

WHO?

Zatknutí podozrivý, ktorý pravdepodobne manipuloval z bankomatom. Momentálne nie je známe, či operoval sám alebo v rámci organizovanej skupiny.

WHAT?

Kreditné karty osôb a overiť, či už bolo manipulované z prostriedkami na nich.

WHEN?

9. 4. 2021, 16:25

Vyšetovanie začalo, keď bolo nájdenie skimovacie zariadenie v bankomate.

21. 4. 2021

Zatknutie podozrivej osoby na letisku v Geneve.

WHERE?

Zariadenia boli nájdenie na:

- Lausanne - miesto činu (skimovacie zariadenia – micro SD karta)
- Aosta - v budove páchatela (mobil, micro SD karta 3-d tlačiarne)
- Geneva - pri zadržaní na letisku (mobil).

WHY?

Potrebujem dokázať, že podozrivý súvisí s prípadom, overiť či sa na skimovacom zariadení nachádza nahrávka s kreditnými kartami. Overiť či sa 3D tlačiareň použila pri výrobe zariadenia. Preskúmať telefón či sa tam nenachádzajú relevantné dôkazy.

HOW?

Vyšetovanie sa vykoná pomocou forenzných metód, ako sú analýza metadát, kontrola systémových logov a obnovenie vymazaných súborov.

HYPOTÉZY:

1. Podozrivý pracoval ako jednotlivec.
2. Podozrivý je súčasťou organizovanej skupiny, informácie zbieral a posielal danej skupine.
3. Podozrivý je nevinný, bol len v nesprávnom čase na nesprávnom mieste.
4. Na skimovacom zariadení sa nachádzajú ukradnuté údaje kariet (4334 2250 2436 4939 – číslo karty svedka, ktorý použil nedávno konkrétny bankomat).
5. 3D tlačiareň bola použitá na výrobu skimovacieho zariadenia.
6. Podozrivý použil ukradnuté údaje karty.

CIEĽ VYŠETROVANIA:

Cieľom vyšetrovania je zistiť, či sa na skimovacom zariadení nachádzajú ukradnuté kreditné karty, dokázať že sa 3D tlačiareň použila na výrobu tohto zariadenia a overiť či sa už z kariet nevyberali peniaze. Taktiež máme jedného zadržaného podozrivého, u ktorého treba overiť či je nejako spojený s prípadom. K tomuto nám pomôže vytvorená digitálna kópia jeho osobného mobilu.

INFORMÁCIE, KTORÉ HĽADÁME:

Video súbory alebo zvukové nahrávky na SD karte skimovacieho zariadenia, ktoré obsahujú citlivé informácie. Overiť systémové logy a metadáta na SD karte ktorá bola pripojená na Raspberry_Pi, aby sme dokázali že bola pripojená k 3D tlačiarňi a overiť či sa tam nenachádzajú .stl súbory alebo zvyšky kódu použitého na vyrobenie skimovacieho zariadenia alebo softvéru do neho. V telefóne podozrivého treba overiť sms komunikáciu, geolokáciu (či sa nachádzal v blízkosti bankomatu kde bolo zariadenie). Vo všetkých zariadeniach sa taktiež obnovia vymazané dáta, ak sa v nich náhodou nachádzajú ďalšie dôkazy.

OČAKÁVANÝ VÝSLEDOK:

- Overiť stanovené hypotézy
- Zistiť aké karty boli odcudzené a či už boli použité.
- Overiť či podozrivý súvisí s prípadom a či je napojení na nejakú skupinu
- Overia sa už zistené dôkazy z popisu prípadu.

POUŽITÉ NÁSTROJE:

- FTK Imager – softvér na tvorbu forenzných obrazov USB zariadenia.
- Autopsy – forenzný nástroj na prehliadanie a analýzu obrazov USB diskov.
- HxD Hex Editor – nástroj na analýzu pamäte a USB na úrovni hexadecimálnych hodnôt
- Audacity – práca zo zvukovými súbormi

ZARIADENIE S DATASETOM:

KINGSTON DTKN/128GB



Kapacita

128 GB

Rozhranie

USB 3.2 Gen 1

Rýchlosť čítania

do 200 MB / s

Rýchlosť zápisu do

60 MB / s

Rozmery

39 mm x 12,6 mm x 4,9 mm

Hmotnosť

4 g

Prevádzková teplota

0 ° C ~ 60 ° C

Skladovacia teplota

-20 ° C ~ 85 ° C

Kompatibilita

Windows® 10, 8.1, 8, Mac OS (v.10.10.x +), Linux (v. 2.6.x +), Chrome OS™

ANALYZOVANÉ ZARIADENIA:

MICRO SD KARTA ZO SKIMOVACIEHO ZARIADENIA

Kingston MicroSDHC 16 GB Industrial



Kapacita

Kapacita disku 16 GB

Kapacita úložiska (celková) 16 GB

Typ

Typ pamäťovej karty microSDHC

Rýchlosť čítania a zápisu

Rýchlosť čítania 100 MB/s

Rýchlostná kategória

Speed Class Class 10

UHS Class U3, UHS-I

Video Class V30

Application Performance Class A1

MICRO SD KARTA Z 3-D TLAČIARNE

Kingston Canvas Select Plus micro SDXC 128GB Class 10 UHS-I



Kapacita

Kapacita disku 128 GB

Kapacita úložiska (celková) 128 GB

Typ

Typ pamäťovej karty micro SDXC

Rýchlosť čítania a zápisu

Rýchlosť čítania 100 MB/s

Rýchlostná kategória

Speed Class Class 10

UHS Class U1, UHS-I

Video Class V10

Application Performance Class A1

DIGITÁLNA KÓPIA MOBILU SAMSUNG GALAXY S10



Základné parametre (SM-G973):

OS: Android 9 Pie

chipset: Exynos 9820, 8 nm

procesor: osemjadrový (max. 2,7 GHz + 2,3 GHz + 1,9 GHz)

grafický procesor: Mali-G76 MP12

frekvencie: GSM 850 / 900 / 1800 / 1900 MHz, UMTS 900 / 2100 MHz, LTE 800 / 1800 / 2100 / 2600 MHz
(frekvencie LTE v Európe), CAT 20

rozмеры: 150 x 70 x 7,8 (8,5) mm

hmotnosť: 157 gramov (overené)

displej: 6,1" (155 mm), Dynamic AMOLED, 1440 x 3040 b., 550 ppi, pomer 19:9, Gorilla Glass 6, HDR10+, 67 x

140 mm

hlavný fotoaparát (26 mm): 12 Mpix (4:3) / 9 Mpix (16:9), clona f/1.5, f/2.4, video 4K (60 fps), super
stabilized Full HD, HDR10+ video, super slo-mo HD (960 fps až 0,8 s), AF, OIS, 77° uhol

teleobjektív (52 mm): 12 Mpix (4:3) / 9 Mpix (16:9), f/2.4, AF, OIS, 45° uhol záberu

širokouhlý fotoaparát (13 mm): 16 Mpix (4:3) / 12 Mpix (16:9), clona f/2.2, FF, 123° uhol záberu

predný fotoaparát: 10 Mpix (4:3) / 9 Mpix (16:9), clona f/1.9, video 4K, 80° uhol záberu

pamäť: 128 / 512 GB + 8 GB RAM + microSD do 512 GB (hybridný slot)

globálny prenos dát: 2G, 3G, 4G / LTE

lokálny prenos dát: Bluetooth 5.0, Wi-Fi, NFC, ANT+, USB-C, USB OTG

ostatné: GPS, Galileo, Glonass, BeiDou, ultrazvuková čítačka odtlačkov v displeji, senzor tepu, stereo
repro, zvýšená odolnosť voči vode (IP68), audio jack

dual-SIM: 2 x nanoSIM (hybridný slot)

batéria: 3400 mAh

BITOVÉ KÓPIE:

- Prvá bitová kópia (BK1):

Umiestnenie: Uložená na laptop s Windows 10, ktorý slúži ako pracovné prostredie na forenznú analýzu.

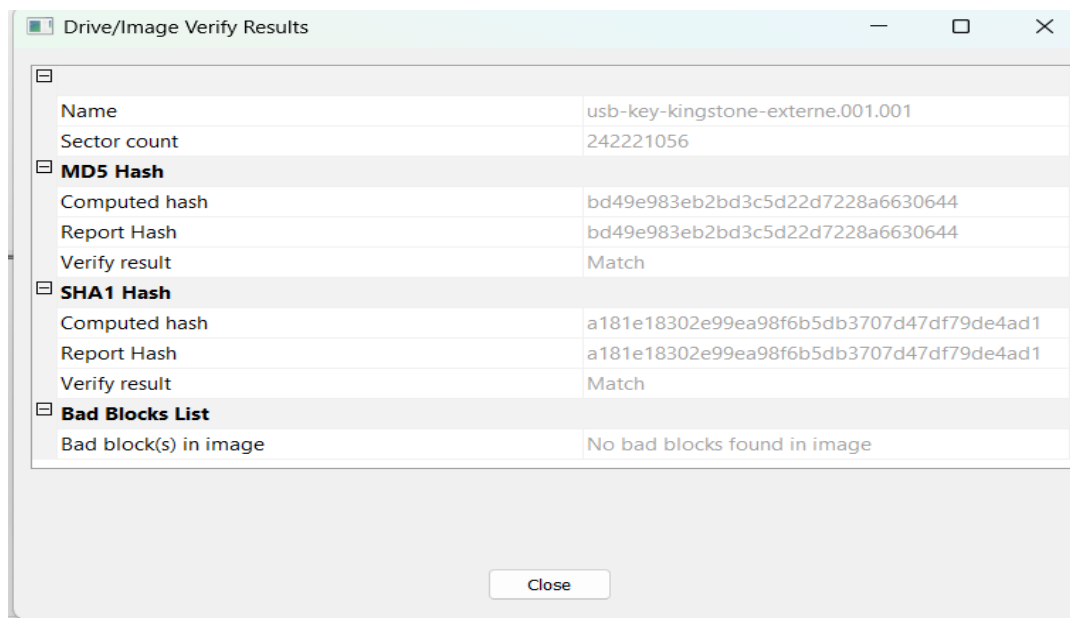
Použitie: Notebook je v mojom vlastníctve a využíva sa na prácu s digitálnymi dôkazmi a analýzu dát z USB kľúča.

- Druhá bitová kópia (BK2):

Umiestnenie: Uložená na externom HDD vo forenznom laboratóriu.

Použitie: HDD je zabezpečené a uzamknuté v laboratóriu, ktoré slúži ako špecializované pracovné prostredie na digitálnu forenznú analýzu.

VÝSLEDOK OVERENIA OBRAZU:



INFORMÁCIE Z FTK IMAGER

Created By Exterro® FTK® Imager 4.7.3.81

Case Information:

Acquired using: ADI4.7.3.81

Case Number: 01

Evidence Number: 01

Unique description: Kingstone USB

Examiner: Roman Fedor

Notes: 128 GB moj prípad

Information for C:\Users\fedko\Downloads\ram-capturer\RamCapturer\x64\usb-key-kingstone-externe.001:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 15 077

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 242 221 056

[Physical Drive Information]

Drive Model: Kingston DataTraveler 3.0 USB Device

Drive Serial Number: 0E479C212969

Drive Interface Type: USB

Removable drive: True

Source data size: 118272 MB

Sector count: 242221056

[Computed Hashes]

MD5 checksum: bd49e983eb2bd3c5d22d7228a6630644

SHA1 checksum: a181e18302e99ea98f6b5db3707d47df79de4ad1

Image Information:

Acquisition started: Mon Mar 24 15:28:05 2025

Acquisition finished: Mon Mar 24 15:46:57 2025

Segment list:

C:\Users\fedko\Downloads\ram-capturer\RamCapturer\x64\usb-key-kingstone-externe.001.001

COMPUTED HASH : bd49e983eb2bd3c5d22d7228a6630644

COMPUTED HASH : a181e18302e99ea98f6b5db3707d47df79de4ad1

Image Verification Results:

Verification started: Mon Mar 24 15:46:57 2025

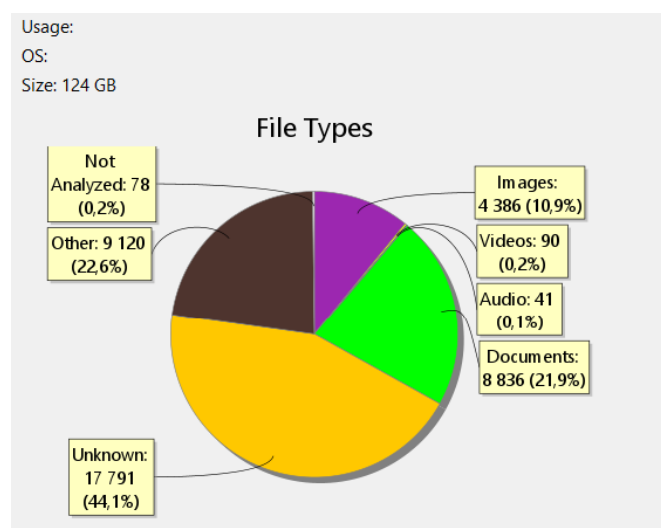
Verification finished: Mon Mar 24 15:52:02 2025

MD5 checksum: bd49e983eb2bd3c5d22d7228a6630644 : verified

SHA1 checksum: a181e18302e99ea98f6b5db3707d47df79de4ad1 : verified

VÝSLEDKY ANALÝZY:

SÚBOROVÉ INFORMÁCIE



MICRO SD KARTA ZO SKIMOVACIEHO ZARIADENIA

Súborový systém:

Save Table as CSV										
△ Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
 \$FAT1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8388608	Allocated	Allocated
 \$FAT2				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8388608	Allocated	Allocated
 \$MBR				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	512	Allocated	Allocated

Nájdene dôkazy:

Filename	2021_04_09T1621.mp3
Location	/img_skimmer_microSD_Physical.e01/2021_04_09T1621.mp3
MIME Type	audio/mpeg
Size	1301392
Modified	2021-04-10 00:21:28 SELČ
Accessed	2021-04-09 01:00:00 SELČ
Created	2021-04-10 00:21:25 SELČ
MD5 Hash	066c187f3010f62a56c82298116ec3f8
Analýza	Časť nahrávky s recording.mp3, obsahuje informácie o 2 kreditných kartách.

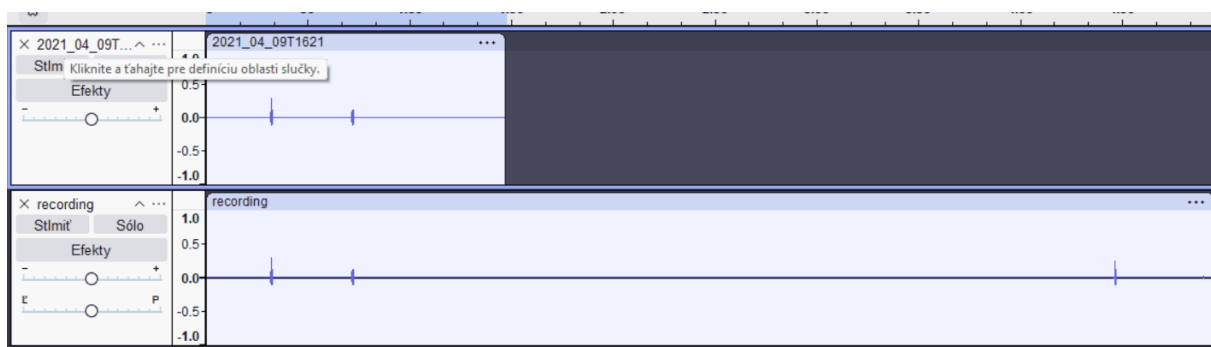
Filename	recording.mp3
Location	/img_skimmer_microSD_Physical.e01/recording.mp3
MIME Type	audio/mpeg
Size	4335015
Modified	2021-04-10 00:24:56 SELČ
Accessed	2021-04-09 01:00:00 SELČ
Created	2021-04-10 00:20:01 SELČ
MD5 Hash	b52421a7547369a770b892026d1b25d0
Analýza	Magnetická páska kariet, nahratá vo forme audio súboru.



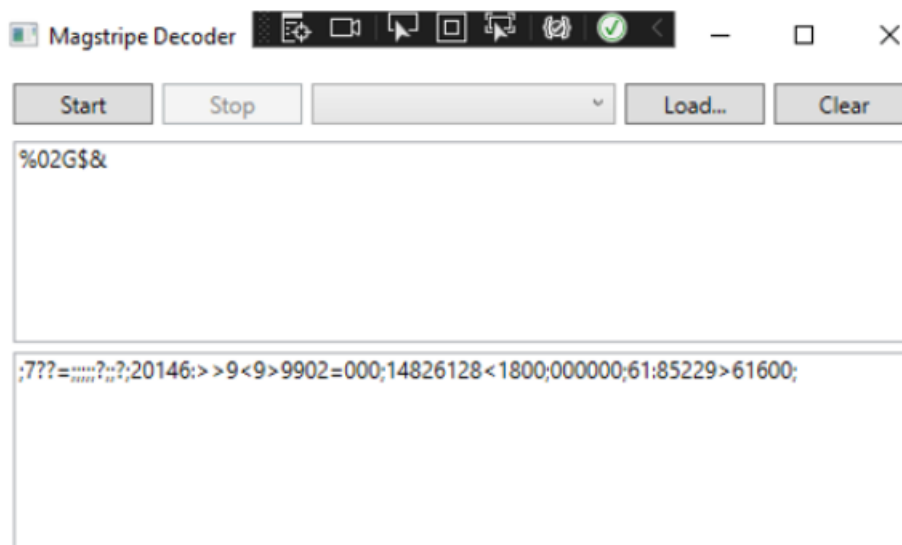
Filename	003BC60A.png
Location	/img_skimmer_microSD_Physical.e01//\$CarvedFiles/ 003BC60A.png
MIME Type	image /png
Size	101296640
Modified	-
Accessed	-
Created	-
MD5 Hash	1daefb3706215bf450bd1c3ae2ce873d
Analýza	Logo – pravdepodobne patrí skupine pod ktorú patrí obvinený.

Filename	004E7D97.pdf
Location	/img_skimmer_microSD_Physical.e01//\$CarvedFiles/ 004E7D97.pdf
MIME Type	Documents/pdf
Size	124864
Modified	2021-03-27 14:37:08 AST
Accessed	-
Created	2021-03-27 14:37:08 AST
MD5 Hash	0df93f0eae98a8669aed40c138710e83
Analýza	Lístok na vlak – z Lausanne do Aosta

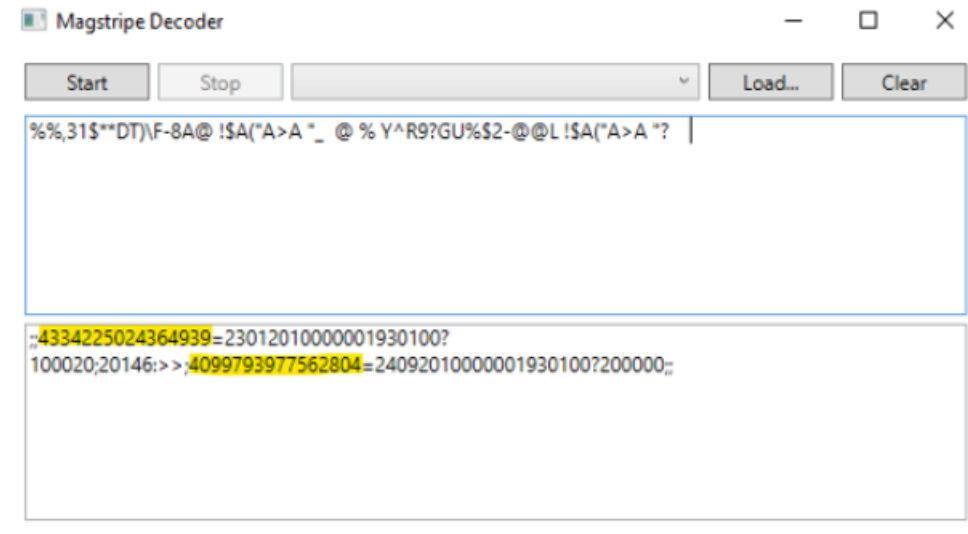
Na karte boli nájdené 2 nahrávky - recording.mp3 a 2021_04_09T1621.mp3. Dolu sú zobrazené zvukové stopy v audacity:



Pri porovnaní sa zistilo, že prvá nahrávka (2021_04_09T1621.mp3) je zostrih spravený z druhej (recording.mp3). Ak chceme zistiť, či sa tam nachádzajú údaje z kariet, budeme potrebovať program, ktorý nám danú stopu preloží, a to tak že sa najskôr detegujú pulzy, čas medzi pulzami, extraktujú sa bity a preložia sa na symboly v ASCII. Výsledok z programu Magstripe Decoder:



Bohužiaľ nám vyšli len nezmyselné čísla takže zvuková stopa je pravdepodobne ešte pred uložením upravená. Pri steganografickej analýze sa zistilo že stopa mohla byť len obrátená, keďže sa tam nachádza pravidelná frekvencia, typická pri čítaní magnetického pásika. Stopa sa teda len obrátila a výsledok bol nasledovný:



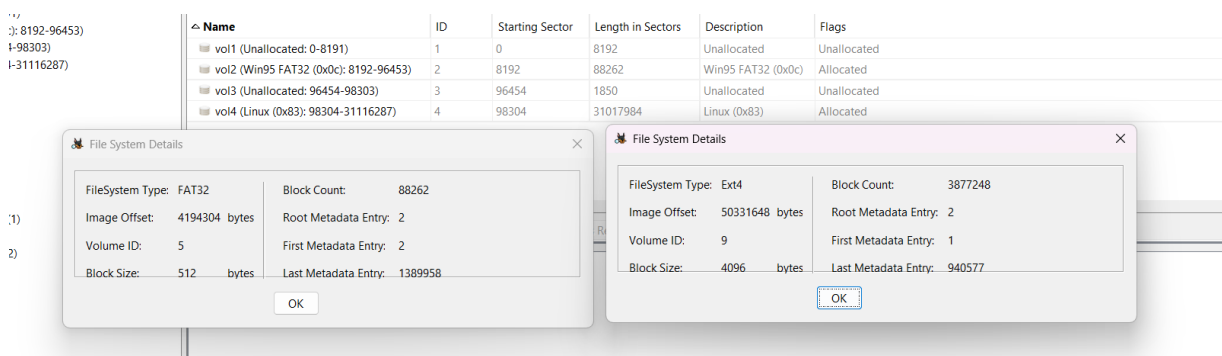
Našli sme 2 čísla kariet : 4334 2250 2436 4939 a 4099 793977562804. Sú to Visa karty a prvé a číslo bolo už nahlásené pre podozrivý pohyb peňazí. Týmto sme potvrdili hypotézu 4.

Na SD karte sa nachádzal aj lístok na vlak z miesta činu do mesta Aosta. Po preskúmaní tejto oblasti bola objavená budova, v ktorej bola objavená 3D tlačiareň napojená na Raspberry P. S Raspberry P bola vytiahnutá ďalšia SD karta.

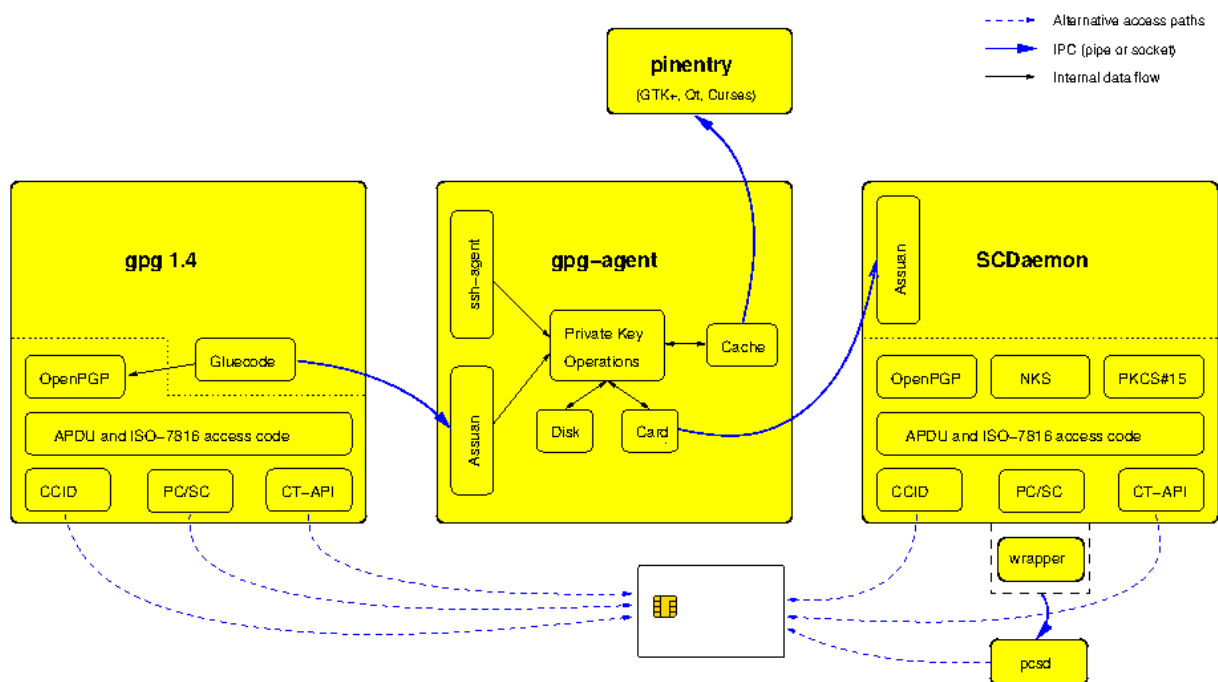
Bol nájdený aj podozrivý obrázok loga, ktorý by mohol súvisieť s nejakou organizovanou skupinou ale zatiaľ nemôžeme obvineného spojiť so skupinou, keďže nemáme priame dôkazy.

MICRO SD KARTA Z 3-D TLAČIARNE

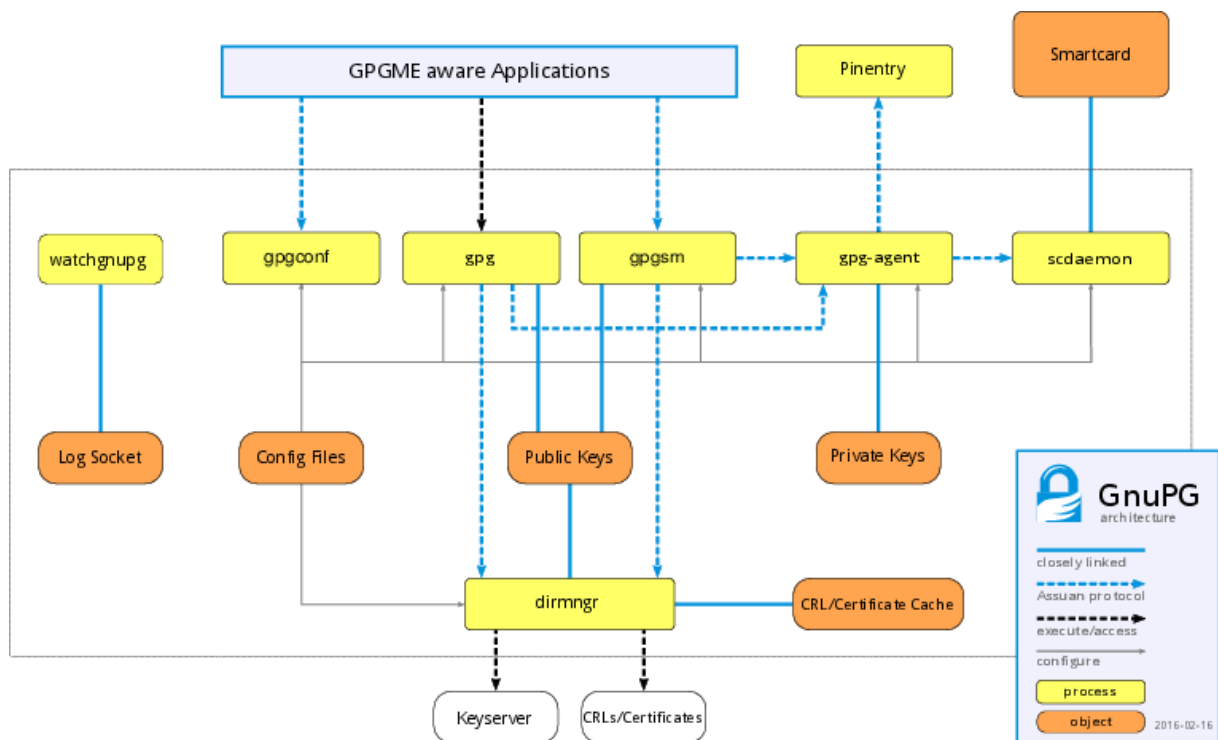
Súborový systém:



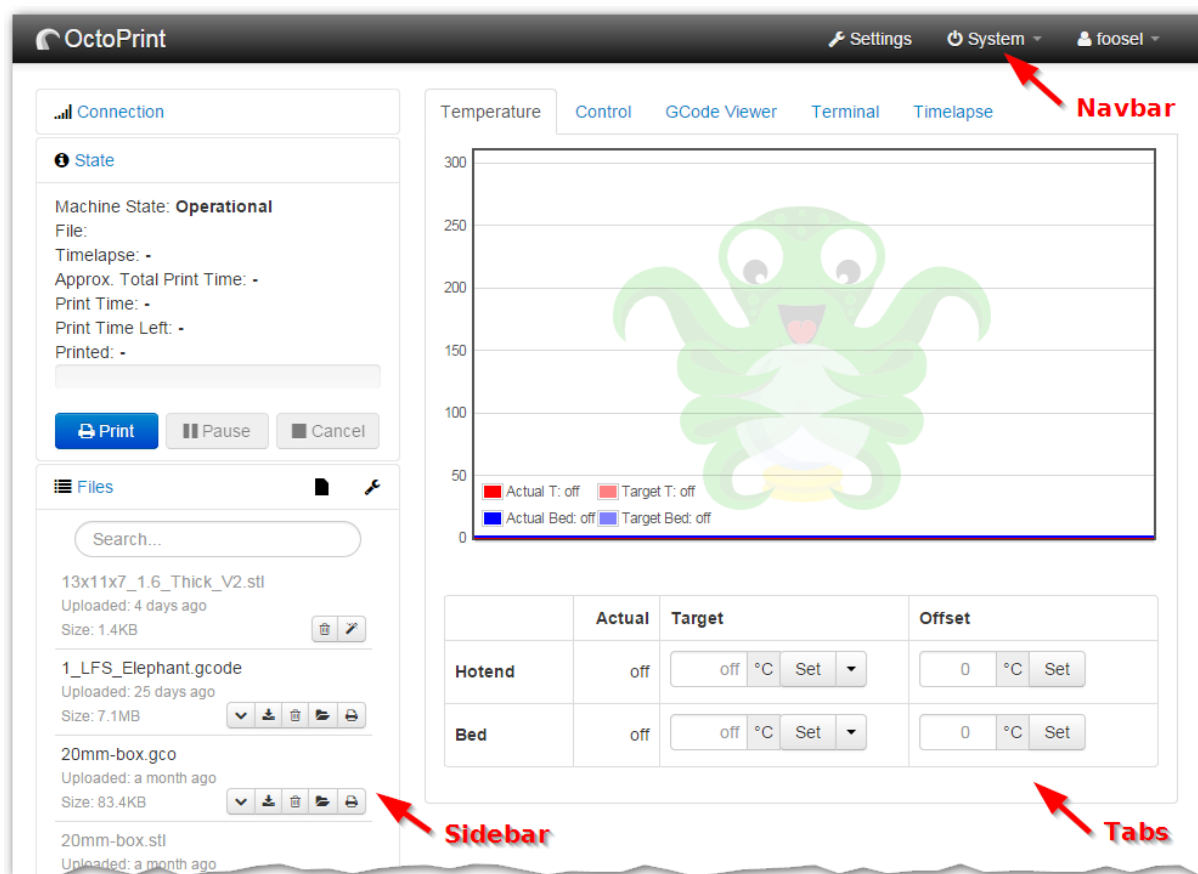
Nájdené dôkazy:



Filename	000B14F8.png
Location	/img_skimmer_microSD_Physical.e01//\$CarvedFiles/000B14F8.png
MIME Type	Image/png
Size	16384
Modified	-
Accessed	-
Created	-
MD5 Hash	
Analýza	Schéma skimovacieho zariadenia 1



Filename	000B1518.png
Location	/img_skimmer_microSD_Physical.e01//\$CarvedFiles/000B1518.png
MIME Type	
Size	40960
Modified	-
Accessed	-
Created	-
MD5 Hash	
Analýza	Schéma skimovacieho zariadenia 2

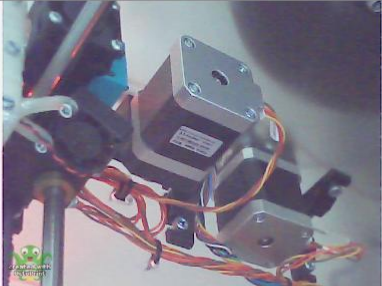


Filename	001EC420.png
Location	/img_skimmer_microSD_Physical.e01//\$CarvedFiles/001EC420.png
MIME Type	image/png
Size	180224
Modified	-
Accessed	-
Created	-
MD5 Hash	
Analýza	UI Octoprint – aplikácia používaná s 3D tlačiarňou

Na tejto karte sme našli fotky schémy skimovacieho zariadenia, ako aj súbor Octoprint, ktorý sa pravdepodobne používal s 3D tlačiarňou. Našli sa taktiež fotky a jedno video zo samotného tlačenia komponentov pre zariadenie.

gif.mp4		2	2020-07-03 14:23:33 SELČ	2020-07-03 14:23:33 SELČ	2020-07-03 14:23:29 SELČ	2020-07-03 14:23:29 SE
VK_trigger_20210413151731.mp4		2	2021-04-13 17:34:05 SELČ	2021-04-13 17:34:05 SELČ	2021-04-13 17:32:25 SELČ	2021-04-13 17:32:25 SE
VK_trigger_20210413151043-fail.mp4		2	2021-04-13 17:14:32 SELČ	2021-04-13 17:14:32 SELČ	2021-04-13 17:14:10 SELČ	2021-04-13 17:14:10 SE
VK_frame(no_sn)_20210414062616.mp4		2	2021-04-14 17:21:32 SELČ	2021-04-14 17:21:32 SELČ	2021-04-14 16:28:30 SELČ	2021-04-14 16:28:30 SE
VK_bottom_cover_20210413154828.mp4		2	2021-04-13 18:03:16 SELČ	2021-04-13 18:03:17 SELČ	2021-04-13 18:01:45 SELČ	2021-04-13 18:01:45 SE

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences



00:00:00/00:00:07

Volume 

Speed 1x

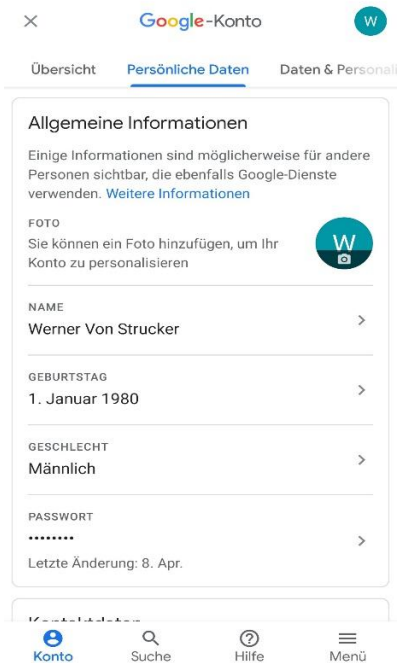
Ďalej sme objavili stránky pre samotný Octoprint a nástroj na kodovanie/dekodovanie zvukových stôp, čo nám dokazuje obvinený mal prístup k nástrojom, potrebným na prácu zo zvukom, akú sme videli v skimovacom zariadení. Týmto sme podvrdili hypotézu číslo 5.

My webcams (0010F370)...	File	6.21 KB
OctoPrint (0005CAC0).html	File	11.83 KB
OctoPrint (00064940).html	File	10.73 KB
OctoPrint (0018A300).html	File	10.73 KB
OctoPrint Login (0005D5F...	File	3.86 KB
OctoPrint Recovery (000...	File	9.29 KB
OctoPrint is still starting (...)	File	10.87 KB
OpenSSH FAQ (000B123...	File	44.92 KB
OpenSSH FAQ (0014E34...	File	44.92 KB
OpenSSH FAQ (0018EAC...	File	44.92 KB

VMCS-X OpenMAX IL Com...	File	12.45 KB
VMCS-X OpenMAX IL Com...	File	12.43 KB
audio_capture (000B5BC...	File	5.12 KB
audio_capture (001541D...	File	5.12 KB
audio_capture (0018A77...	File	5.09 KB
audio_decode (000B5BD0...	File	6.86 KB
audio_decode (001541E8...	File	6.86 KB
audio_decode (0018A780...	File	6.83 KB
audio_encode (000B5BE0...	File	5.64 KB
audio_encode (001541F8...	File	5.64 KB
audio_encode (0018A790...	File	5.61 KB
audio_lowpower (000B5B...	File	3.04 KB
audio_lowpower (001542...	File	3.04 KB
audio_lowpower (0018A7...	File	3.01 KB
audio_mixer (000B5BF8)...	File	6.92 KB
audio_mixer (00154210)...	File	6.92 KB

DIGITÁLNA KÓPIA MOBILU SAMSUNG GALAXY S10

Nájdeneé dôkazy:



Filename	141.jpg
Location	/img_usb-key-kingstone-externe.001.001/vol_vol2/3_Samsung GSM_SM-G973F_DS Galaxy S10/Dump/data/system_ce/0/snapshots/141.jpg
MIME Type	Image/jpeg
Size	232 822
Modified	2021-04-18 15:41:54 SELČ
Accessed	-
Created	2025-03-21 22:07:47 SEČ
MD5 Hash	dc1971dfdce33a138ce2a6622fa91774
Analýza	Prihlasovacie údaje do Google účtu podozrivého



Last Message Received

Btw
Lay low, it seems your little fuckup with the Postomat
had big consequences.

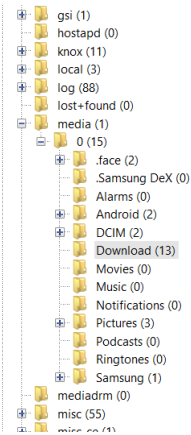
Send Message

SEND

Dst # (Reserviert für RS)

will do. and again my apologies, will
never happen again, i've installed the
others much more carefully.

Filename	164.jpg
Location	/img_usb-key-kingstone-externe.001.001/vol_vol2/3_Samsung GSM_SM-G973F_DS Galaxy S10/Dump/data/system_ce/0/snapshots/164.jpg
MIME Type	Image/jpeg
Size	150 941
Modified	2021-04-18 17:07:08 SELČ
Accessed	-
Created	2025-03-21 22:07:49 SEČ
MD5 Hash	e8a5582f3f17a75e1b80c43e38be83e2
Analýza	Jedna zo šifrovaných správ – podozrivý si bol vedomý že ho hľadajú policajti, komunikácia s organizovanou skupinou



7624f08c-d26d-4ccd-92b1-d552bd54fb43.jpeg

2021_04_09T1621.mp3

3

2

4

2021-04-08 18:32:02 SELČ

2021-04-09 16:22:42 SELČ

0000-00-00 00:00:00

0000-00-00 00:00:00

2025-03-21 22:03:06 SEČ

2025-03-21 22:03:07 SEČ

2025-03-21 22:03:06 SEČ

2025-03-21 22:03:07 SEČ

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Metadata

Name: /img_usb-key-kingstone-externe.001.001/vol_vol2/3_Samsung GSM_SM-G973F_DS Galaxy S10/Dump/data/media/0/Download/2021_04_09T1621.mp3

Type: File System

MIME Type: audio/mpeg

Size: 1301392

File Name Allocation: Allocated

Metadata Allocation: Allocated

Modified: 2021-04-09 16:22:42 SELČ

Accessed: 2025-03-21 22:03:06 SEČ

Created: 2025-03-21 22:03:07 SEČ

Changed: 0000-00-00 00:00:00

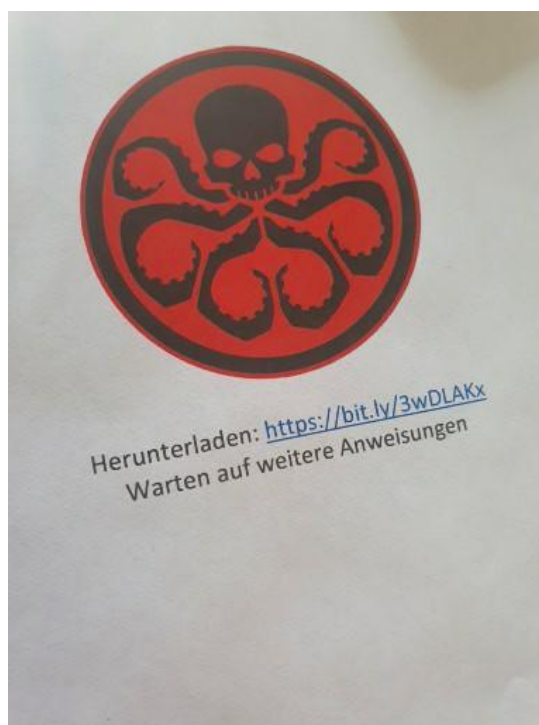
MD5: 066c187f3010f62a56c82298116ec3f8

SHA-256: 2bbe2b7bab41502bdbc696f9df0ecd21c93344cb2001627eb19d4442597eb1

Hash Lookup Results: UNKNOWN

Internal ID: 54129

Filename	2021_04_09T1621.mp3
Location	/img_usb-key-kingstone-externe.001.001/vol_vol2/3_Samsung GSM_SM-G973F_DS Galaxy S10/Dump/data/media/0/Download/2021_04_09T1621.mp3
MIME Type	audio/mpeg
Size	1301392
Modified	2021-04-09 16:22:42 SELČ
Accessed	2021-04-09 16:22:42 SELČ
Created	2021-04-09 16:22:42 SELČ
MD5 Hash	066c187f3010f62a56c82298116ec3f8
Analýza	Nahrávka zo skimovacieho zariadenia, zhoda MD5 hash

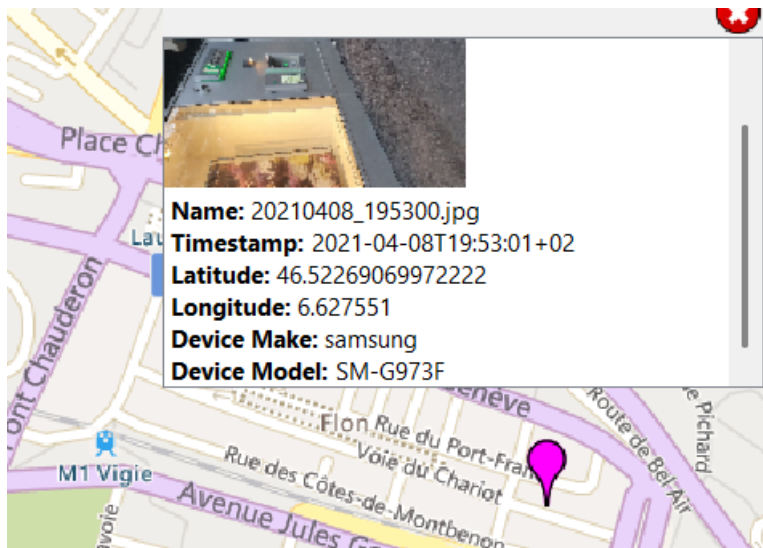


Filename	22.jpg
Location	/img_usb-key-kingstone-externe.001.001/vol_vol2/3_Samsung GSM_SM-G973F_DS Galaxy S10/Dump/data/media/0/Pictures/.thumbnails/22.jpg
MIME Type	image/jpeg
Size	34 954
Modified	2021-04-11 14:56:06 SELČ
Accessed	-
Created	2025-03-21 22:03:14 SEČ
MD5 Hash	cd2f34b97b7e25188b05499817fdef68
Analýza	Link na OmniNotes – šifrovací notepad, konkrétne pre sms komunikáciu

Na telefóne podozrivého sme našli fotku s tým istým logom, aké sme našli aj na SD karte skimovacieho zariadenia, čiže môžeme konštatovať že podozrivý () je napojený na organizovanú skupinu Hydra, pre ktorú

zbieral kreditné karty, s ktorých pravdepodobne kradli peniaze. Týmto sme potvrdili hypotézu 2 a zároveň vyvrátili hypotézy 1 a 3. Vo fotkách bola nájdená aj časť komunikácie medzi podozrivým a Hydrou.

Taktiež bola nájdená v telefóne aj nahrávka so skimovacieho zariadenia, čiže môžeme podozrivého prepojiť aj s týmto zaradením.



S geolokácie sme zistili že sa nachádzal aj na mieste kde bolo skimovacie zariadenie nájdené, čiže podozrivý ho tam aj nainštaloval. Toto bolo aj dokázané pomocou sms komunikácie. Táto je ale šifrovaná.

Showing Messages for Thread: HHYgSQ2GGQd5ZEvKdOk5qRrWfoEH0baqjRkTwacpwgxp02qqrNOueQ0z31. [Threads](#)

Type	From	To	Date	Subject	Attachments
Message	+41786909109	04e6495a-ae5...			0
Message	04e6495a-ae5...				0
Message	+41786909109	04e6495a-ae5...			0
Message	04e6495a-ae5...				0
Message	+41786909109	04e6495a-ae5...			0
Message	04e6495a-ae5...				0
Message	+41786909109	04e6495a-ae5...			0
Message	04e6495a-ae5...				0
Message	+41786909109	04e6495a-ae5...			0
Message	04e6495a-ae5...				0

From: 04e6495a-ae5-4ab7-87eb-a8d3435fea8e 2021-04-08 19:11:08 SELČ
To: +41786909109 Outgoing
CC:
Subject:

Headers Text HTML RTF Attachments (0) Accounts

Original Text

HHYU1+uAKNdKlJ0YsLDmmJw3M2bFrl0/R5oPXCCfJYqUwZ6z+usTidJxqnRJuWEeiw8po5Hi1Gf6AaNdxUeqGBq+g==

Na fotke s logom bol uvedený aj link na aplikáciu OmniNotes. Po dekompilácii bola zistená funkcia, pomocou ktorej bola šifrovaná sms komunikácia.

```
private String open_msg(byte[] bArr) throws NoSuchPaddingException, NoSuchAlgorithmException,
    SecretKeySpec secretKeySpec = new SecretKeySpec(get_data().getBytes(), "AES");
    Cipher instance = Cipher.getInstance("AES/ECB/PKCS5Padding");
    instance.init(2, secretKeySpec);
    return new String(instance.doFinal(bArr), "UTF-8");
}
```

S funkcie môžeme vyčítať že bola použitá AES šifra v ECB móde a bol použitý padding PKCS5.

```
private String open_msg(byte[] bArr) throws NoSuchPaddingException, NoSuchAlgorithmException, InvalidParameterSpecException, InvalidAlgorithmParameterException, InvalidKeyException, BadPaddingException
    SecretKeySpec secretKeySpec = new SecretKeySpec(get_data().getBytes(), "AES");
    Cipher instance = Cipher.getInstance("AES/ECB/PKCS5Padding");
    instance.init(2, secretKeySpec);
    return new String(instance.doFinal(bArr), "UTF-8");
}

78 public String put(String str) {
79     try {
80         return "HHY" + Base64.encodeToString(save_msg(str), 2);
81     } catch (IOException | InvalidKeyException | NoSuchAlgorithmException | InvalidParameterSpecException | BadPaddingException | IllegalBlockSizeException | NoSuchPaddingException | JSONException u
82     ) {
83         return BuildConfig.FLAVOR;
84     }
85 }
```

Taktiež sa ku každému stringu pridáva „HHY“.

```
private String get_data() throws IOException, JSONException {
    String decomp = ZipHelper.decomp("J2xMyUkVdAIBNATZStBkHkH5wSHUk17FrNyNk30TmghpB9Z4jztYDpM45w3rrcunA5rQDMHIV");
    HttpURLConnection httpsURLConnection = (HttpURLConnection) new URL(decomp + ZipHelper.decomp("eJwFwIEI4AAAAACCO/ai0AEAAQAm=") + ZipHelper.decomp(this.resources.getString(
    try {
        BufferedReader bufferedReader = new BufferedReader(new InputStreamReader(httpsURLConnection.getInputStream()));
        StringBuffer stringBuffer = new StringBuffer();
        while (true) {
            String readLine = bufferedReader.readLine();
            if (readLine != null) {
                stringBuffer.append(readLine);
            } else {
                String string = new JSONObject(stringBuffer.toString()).getString("key");
                String format = new SimpleDateFormat(ZipHelper.decomp("eJvNwIEAAAMHECULJdi0u0eyBfWSAGE="), Locale.getDefault()).format(new Date());
                return string + format;
            }
        }
    } finally {
        httpsURLConnection.disconnect();
    }
}
```

Ešte nám chýba kľúč, vyzerá že je vytvorený pomocou iného kľúča + dátumu, kedy bola správa poslaná. Poslednú časť získame dekodovaním vyznačeného stringu s ktorého dostaneme adresu(Base64 + Zlib): <https://hy1.blob.core.windows.net/hy-ws-1/key.json>.

Kde nájdeme kľúč: rb5CuefkDLyb9T

Takže môžeme dekodovať sms komunikáciu podľa postupu:

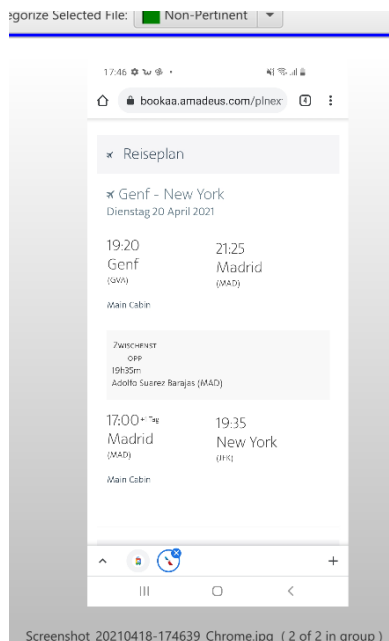
1. Odstránime zo stringu „HHY“
2. Nastavenie dešifrovania:
 - a. AES šifrovanie
 - b. Input type – text, Input Encoding – Base64
 - c. Output – UTF-8
 - d. Mode – ECB
 - e. Key size – 192bits
 - f. Padding – PKCS7
 - g. Key Type – Custom(UTF-8)
 - h. Key - rb5CuefkDLyb9T+dátum odoslania správy (yyyy-mm-dd)

Výsledky:

Správa	Dátum poslania	Výsledok dešifrovania
HHY6cKEMFINU3NPs/bxhxPKQRyDXU rQK7a8tHtX5xBXdYQ=	2021-04-08	Heil Hydra 🦋!
HHYZEuQn5pA1hKmulAHVx55cA==	2021-04-08	Heil Hydra!
HHYU1+uAKNdKlj0YsLDmmJw3M2bFr l0/R5oPXCCfJYqUwZ6z+usTidJxqnRJu WEeiw8po5Hi1Gf6AaNdxUeqGBq+g= =	2021-04-08	Apologies for the email. Will never happen again.
HHYKvEbze+wdEalheouf7A2m98++su Lv5Dv4GHZKFM4lpw=	2021-04-08	Sure hope so for you.
HHYsskk9VxsMQLIQ5jsWVGKu0cikDE ZYDdgJOW//zKch62LATxcR5WGFF6Mt RtDWHJhLYMHxZ2TgngAqvsZrSsJKcH mTmlYAVR3P/U0uneLDbBbZkGDKzMj kfb9349ydCAT	2021-04-08	Identify the best places for the items we sent you. Install them ASAP. I want Zola to proceed.
HHYbRTTaGxxLatLwNLMF7ptPDTjpMn xkyp53B6M6sPV9khvr0kKZpEK0zmG 7uAJa79	2021-04-08	Will do. I've already some ideas. Hail Hydra!
HHYCIUGa/i7pLYjRGwzXrvpVg==	2021-04-09	Hail Hydra!
HHYCIUGa/i7pLYjRGwzXrvpVg==	2021-04-09	Hail Hydra!
HHYBNsxyjLdeJ2KD5cKwnO1A81zVE6 Xad+i+X0wojD9jsFUumW48isXBeodD 7cPCEAJ1r8fSw2D3FzsmCD5u2Tavch 2MC8acODGbE20imqxTGhoeZC8UrJg 5AThVC4McgpSfzlaRiuC77a6k2A81IY d7A==	2021-04-09	Installed second device today but something went wrong. Lots of policemen on place 15min after. I'm worried.
HHYod/v/R9xC1A8TqJ/UWcf/pdR9nO 4f85nxcgE3GKZBwJspL7YqyD5PtqGT8 pTXlhlcJHuQXln4Gro+BYU2FxiI5ingKE y6BHoYedEMSGWdj0=	2021-04-09	Proceed as planned, Ward will take care of that if it escalates.
HHY2NToA10DeweA+V3mutF9QA==	2021-04-15	Hail Hydra!
HHY2NToA10DeweA+V3mutF9QA==	2021-04-15	Hail Hydra!
HHYHiiOyvP7s0llu5N2ta9y/Qsk5FeloF JOXZvQpzDR7p9XBQHyYuhfdel6g3OU S4cj	2021-04-15	What's the status on the devices?
HHYOeHfDhFU8plFmx7J5qXltG1XGw pcbrBtUjNSeROwGZ95dNIEMUGQFJd O7n3U3m6PaSjcUUKMY9yQZkdmulu V6UhxQ+j33/Vyjvc+z2+hAVo=	2021-04-15	Installed two more in the scouted locations. still have a couple available.
HHYiNf68BXbaolSBtAav5yYU7WHDH aADyWmtazUbSOTFTukKKj2wv4zRTpjf +l9n3sb/YUXpRbOjQmos4+Ql8Np1Q= =	2021-04-15	Good... everything is still calm despite Friday incident.
HHYbm0jyH9MsbIM1DsylvNU9iDm63 RQa9/1FxfRs/A75m3wAM04VwDGphJ4 m9lUTjPQ//3qbJmQkxQQueu50WmK0z LHj93BiByuFEHsvHwzcfHsl=	2021-04-15	We need to meet you. Get to geneva asap, further instructions will follow.
HHYS6+p9lajgCnkXIIm0touuBzw/c5dS k4ZVzCEeA7BZmnR7+J5ybgmhLeXCyx	2021-04-15	understood, was headed to geneva anyway, already on a train.

pwovM8yFaK1NQtfAJXHKwHnMGlXg= =		
HHYcdZD5nSpEbiNiPHaMn/eJR3qfnG 1bBjxHLgN2Q91Jjx+DaAtq15BuatyPqS SH0ZOqLPbis211525r4RikumQSF1p8 xjb7tbOHZWN250Sqmh9v+9kcE6ln WMOcYHo4ub	2021-04-15	Good. Meet us at our base. Below the Turkish consulate. Delete this message once read!
HHY9frkML1o7eM6Ri32ERhNUEnmlb Dg1syRQ+CP5zcYWYQ=	2021-04-15	wilco hail hydra!
HHY2NToA10DeweA+V3mutF9QA==	2021-04-15	Hail Hydra!
HHY2NToA10DeweA+V3mutF9QA==	2021-04-15	Hail Hydra!
HHY6JGyTGtI0lJl8PgtU2T/w5YPNCw1P hZ/Lagr4MhnCQHx+q36vX3TeUBZ6r/o dTJU	2021-04-15	Installed device at airport as discussed
HHYj6DtE+EQdYzoKjUoVP8DQw==	2021-04-18	Hail Hydra!
HHYj6DtE+EQdYzoKjUoVP8DQw==	2021-04-18	Hail Hydra!
HHYqDAJ2HSbMahjfWcjFcL8H41ALc W17JkzdXUV02H4eHGTt+6mU+twizvA svdMU6FkIUHhrPcLzbiBsCV99j/skyID 1A6fR7cocoqjOb61DM8=	2021-04-18	We sent you the payment to the address you provided us. confirm reception.
HHYRvZdXk+/U616OwdSp1fk350Qysr JXGGJ9XkQkDIgFl0sMmxZm8fbD0SYK 5ON8zcc	2021-04-18	Understood, Payment received successfully.
HHY97NA5dDGdqomydjZt0GGycKgRS 2T2vltP40yuOAo9azlfHzaNR3r2Fw78G XBuVC4YlifClzf+VKxxK13O2MgHwKDe GxIGva+uFj7wL+YnpKhdeGdwLiZ2/ws zZN9dKlx	2021-04-18	Btw Lay low, it seems your little fuckup with the Postomat had big consequences.
HHYgSQ2GGQd5ZEvdOk5qRrWfoEH 0baqjRkTwacpwgxp02qqrNOueQ0z31 KEiL65EZCnHrjYy+7qbqFiVcCJCbnXn QdMC1MI64+dyXkuK6e/9I/ebQM3ZaA hqNLbIHNPokTv35Hz1VseDqLE1YpO PI4YQ==	2021-04-18	will do. and again my apologies, will never happen again, i've installed the others much more carefully.

Tieto správy nám už len potvrdili predošlé hypotézy a máme aj úplnú časovú líniu ako boli zariadenia nainštalované.



Nakoniec sme našli aj letenku podľa, ktorej bol zatknutí podozrivý Werner von Strucker. Letenka bola kúpená na meno Adolfo Suarez Barajas, ktorého karta bola nahratá pomocou skimvaciaho zariadenia. Werner túto kartu použil aby si kúpil túto letenku. Týmto sme potvrdili hypotézu 6.

OBRAZ RAM PAMÄTE:

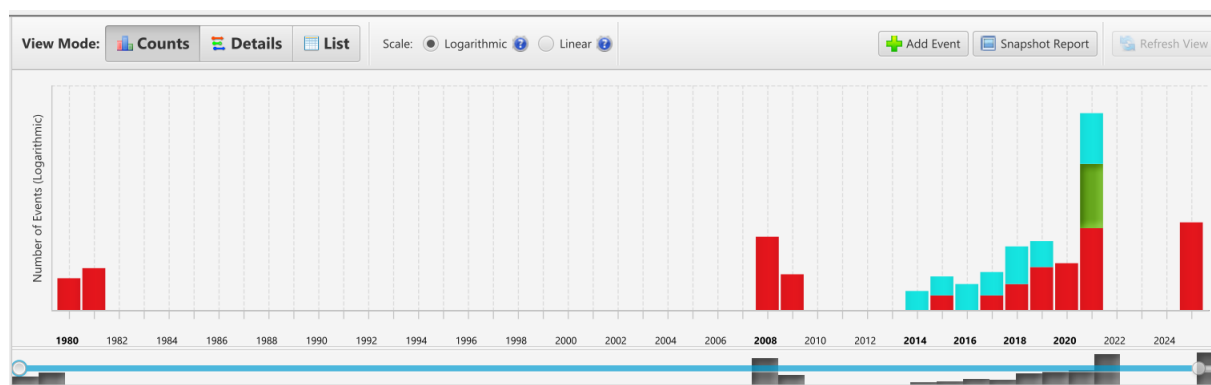
V pamäti boli taktiež nájdenie podozrivé stránky, čo len potvrdzuje, že si obvinený hľadal informácie, aby lepšie vedel kradnúť bankové karty:

```

81B079A20 30 2A F5 8B FE 7F 00 00 00 00 00 00 01 00 00 00 0*6<t.....
81B079A30 61 62 6F 75 74 3A 62 6C 61 6E 6B 2E 66 62 69 2E about:blank.fbi.
81B079A40 67 6F 76 2F 68 6F 77 2D 77 65 2D 63 61 6E 2D 68 gov/how-we-can-h
81B079A50 65 6C 70 2D 79 6F 75 2F 73 63 61 6D 73 2D 61 6E elp-you/scams-an
81B079A60 64 2D 73 61 66 65 74 79 2F 63 6F 6D 6D 6F 6E 2D d-safety/common-
81B079A70 66 72 61 75 64 73 2D 61 6E 64 2D 73 63 61 6D 73 frauds-and-scams
81B079A80 2F 73 6B 69 6D 6D 69 6E 67 00 00 00 00 00 00 00 /skimming.....
81B079A90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

TIMELINE



REŤAZEC STAROSTLIVOSTI:

KINGSTON DTKN/128GB

Číslo:	01	Typ súboru:	raw	Obnovený súbor:	Nie	Veľkosť:	38, 5 GB
Popis prípadu:		Odcudzenie bankových údajov					
Názov súboru:		usb-key-kingstone-externe.001					
Miesto získania digitálnej stopy:		Forenzné laboratórium					
Poznámky:		Určené pre DFA					
Časové pečiatky							
Access:	23.03.2025 10:40:16		Modify:	23.03.2025 10:50:16		Change:	-
Digitálny odtlačok (heš)	MD5	bd49e983eb2bd3c5d22d7228a6630644					
	SHA1	a181e18302e99ea98f6b5db3707d47df79de4ad1					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
23.03.2025 15:40:16		Otvorenie obrazu USB					
23.03.2025 15:42:26		Následná extrakcia obsahu a práca s forenznými artefaktami					
23.03.2025 16:35:56		Zatvorenie obrazu USB					

--	--

MICRO SD KARTA ZO SKIMOVACIEHO ZARIADENIA

Číslo:	02	Typ súboru:	raw	Obnovený súbor:	nie	Veľkosť:	102,5 MB
Popis prípadu:		Odcudzenie bankových údajov					
Názov súboru:		1_Skimmer_mSD.001					
Miesto získania digitálnej stopy:		Skimovacie zariadenie, nájdené v bankomate					
Poznámky:		Obraz bol vytvorený cez FTK Imager 4.7.1.2					
Časové pečiatky							
Access:	23.03.2025 15:40:16		Modify:	23.03.2025 15:42:16		Change:	-
Digitálny odtlačok (heš)	MD5	-					
	SHA1	1c5ad394daa49573f4088a31fb7f6a3f537dbcd092fd5abc8b572ebdbcb262					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
23.03.2025 15:41:06		Extrakcia dát s pamäťovej kópie					

MICRO SD KARTA Z 3-D TLAČIARNE

Číslo:	03	Typ súboru:	raw	Obnovený súbor:	nie	Veľkosť:	3,76 GB
Popis prípadu:		Odcudzenie bankových údajov					
Názov súboru:		2_Raspberry_Pi_mSD.001					
Miesto získania digitálnej stopy:		Raspberry_Pi pripojené k 3D tlačiarňi v dome podozrivého					
Poznámky:		Obraz bol vytvorený cez FTK Imager 4.7.1.2					
Časové pečiatky							
Access:	23.03.2025 15:42:16		Modify:	23.03.2025 15:44:18		Change:	-
Digitálny odtlačok (heš)	MD5	-					
	SHA1	aabec0c1305e785d1ba5b4ba01c5dacd27cc128fdd32078758be826e75449953					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
23.03.2025 10:43:50		Extrakcia dát s pamäťovej kópie					

--	--

DIGITÁLNA KÓPIA MOBILU SAMSUNG GALAXY S10

Číslo:	04	Typ súboru:	raw	Obnovený súbor:	nie	Veľkosť:	14,19 GB
Popis prípadu:		Odcudzenie bankových údajov					
Názov súboru:		3_Samsung GSM_SM-G973F_DS Galaxy S10.001					
Miesto získania digitálnej stopy:		Kópia mobilného zariadenia podozrivého					
Poznámky:		Obraz bol vytvorený cez FTK Imager 4.7.1.2					
Časové pečiatky							
Access:	23.03.2025 15:46:18		Modify:	23.03.2025 15:49:34		Change:	-
Digitálny odtlačok (heš)	MD5	-					
	SHA1	54877505f1b4eb26c4cb6b43fd6338424660c207e678b773044a4a79d6e374b7					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
23.03.2025 15:47:28		Extrakcia dát s kópie					

BEZPEČNOSTNÉ OPATRENIA:

1. Fyzická ochrana

- Zariadenie bolo uložené do antistatického obalu a bezpečnostného puzdra.
- Chránené pred teplotou, vlhkosťou a magnetickými poľami.

2. Digitálna ochrana

- USB kľúč nebol pripájaný k bežnému počítaču, aby sa predišlo zmene dát.
- Bol použitý write-blocker na ochranu pred zápisom.
- Čo najskôr vytvorený forenzný obraz (pomocou FTK Imager).

3. Dokumentácia a skladovanie

- Bol evidovaný dátum, čas, miesto nálezu a manipulácia.
- USB kľúč bol uchovávaný v trezore a analyzovaný v izolovanom prostredí.

ZÁVER:

POTVRDENÉ HYPOTÉZY:

Hypotéza 2.

S sms komunikácie sme zistili že zariadenia boli poskytnuté od skupiny Hydra, pre ktorú podozrivý Werner von Strucker inštaloval skimovacie zariadenia do bankomatov a kradol informácie s kreditných kariet.

Hypotéza 4.

Karta bola nájdená šifrovaná v nahrávke v SD karte skimovacieho zariadenia.

Hypotéza 5.

Našli sme videá a fotky na ktorých je viditeľná výroba zariadenia, taktiež sme našli ich schémy.

Hypotéza 6.

Letenka bola zakúpená pomocou ukradnutej karty.

VYVRÁTENÉ HYPOTÉZY:

Hypotéza 1. a 3.

Máme jasné dôkazy, že podozrivý Werner von Strucker pracoval s organizovanou skupinou – Hydra.

ZHRNUTIE:

Werner von Strucker bol kontaktovaný organizovanou skupinou Hydra aby pre nich zbieral kreditné karty pomocou skimovacích zariadení. Tieto boli nainštalované na rôznych miestach v Geneve a Lausanne. V Lausanne bol Werner spozorovaný svedkom ako jedno takéto zariadenie inštaluje. So zariadenia bola vybratá SD karta, na ktorej po analýze boli objavené nahrávky, ktoré obsahovali kreditné karty a bol objavený aj lístok na vlak do Aosty. Tu bola objavená budova v ktorej sa samotné zariadenia vyrábali. Vyplynulo nám to s dôkazov zo videí a fotiek, ktoré boli nájdené na SD karte v 3D tlačni v tejto budove a s sms komunikácie vo Wernerovom mobile. Nakoniec bol Werner zadržaný na letisku v Geneve, kde sa

snažil nastúpiť na lietadlo do New Yorku. Letenka bola zakúpená pomocou ukradnutej karty, ktorá bola odcudzená pomocou skimvacieho zariadenia v Lausanne. Telefón obsahoval tú istú nahrávku(overené pomocou MD5 odtlačku).

LITERATÚRA A PRÍPADOVÉ ŠTÚDIE:

Jacobo Tarrío – How magnetic stripe cards work

Popis: Článok popisuje spôsob ako funguje magnetická páska na karte, ako nahráť pásku pomocou čítačky a ako pracovať z nahratou zvukovou stopou. Taktiež popisuje program, ktorý dokáže preložiť bity na ASCII znaky.

Dostupné na: <https://jacobo.tarrio.org/2014/how-magnetic-stripe-cards-work.html>

Muhammad Furqan Ul Haq - APK Decompilation: A Beginner's Guide for Reverse Engineers

Popis: Článok popisuje ako správne dekompilovať aplikáciu pomocou JADX, Apktool a Bytecode Viewer.

Dostupné na: <https://hackernoon.com/apk-decompilation-a-beginners-guide-for-reverse-engineers>

Elizabeth Schweinsberg - DFRWS 2021 Challenge

Popis: Článok, z ktorého bol použitý dataset a príbeh. V kapitolách sú popísané jednotlivé zariadenia, ako aj odkaz na stiahnutie jednotlivých digitálnych kópií a ich odtlačky.

Dostupné na: <https://dfrws.org/dfrws-2021-challenge/>