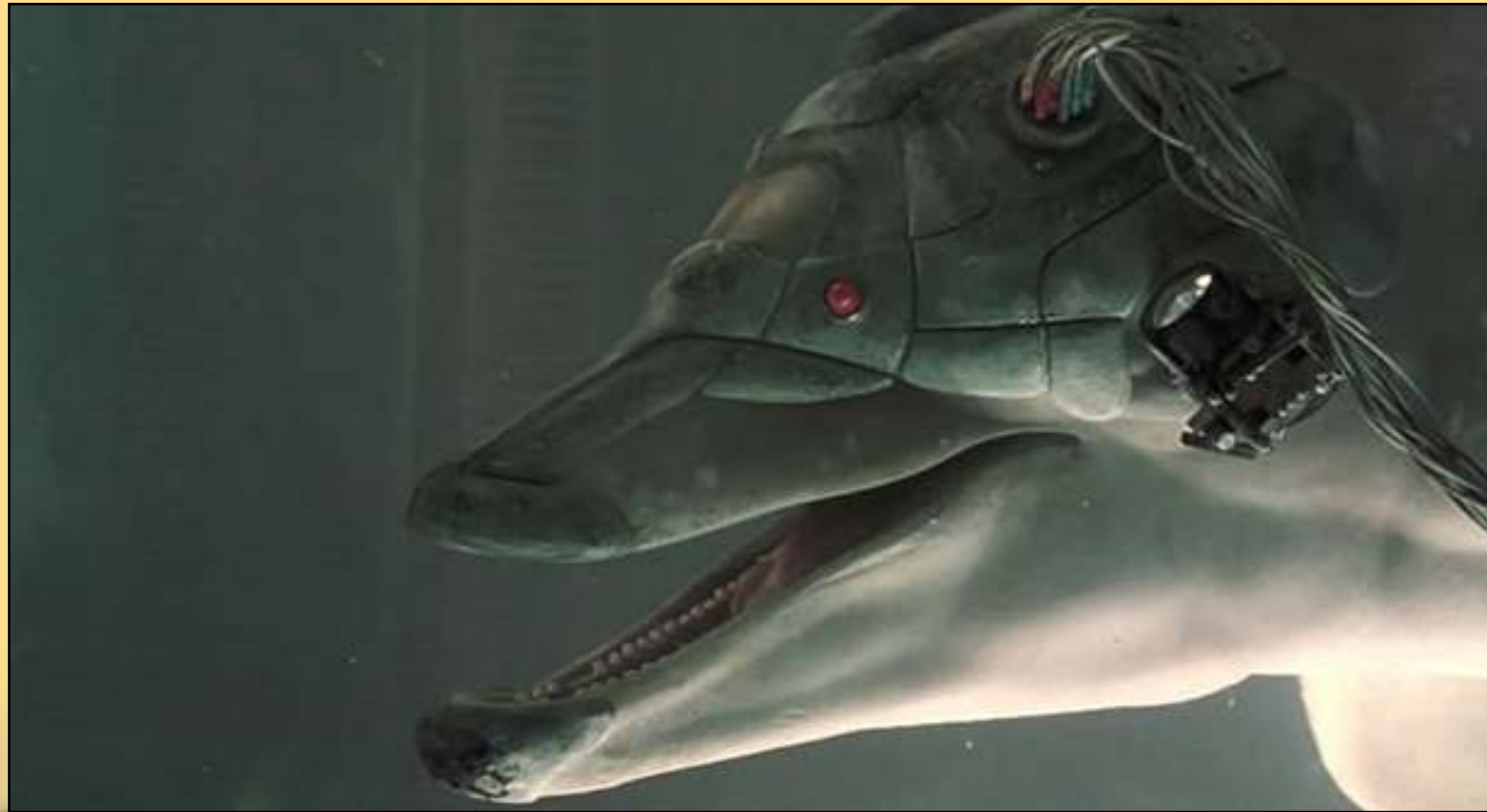


The Flipper Zero presentation for VanLUG community



by Levko Kravchuk ©

This cyberdolphin is from the Johnny Mnemonic movie

About me

Levko Kravchuk

I started my career back in 2008. I was involved in creating fiber optic networks and providing internet access. I administered Windows servers and client operating systems, as well as Linux, routers, and firewalls. I worked with networks of varying levels of security. I have a strong interest in cybersecurity and continuously develop my skills in this area.



The flipper in VanLUG conference

The Disclaimer

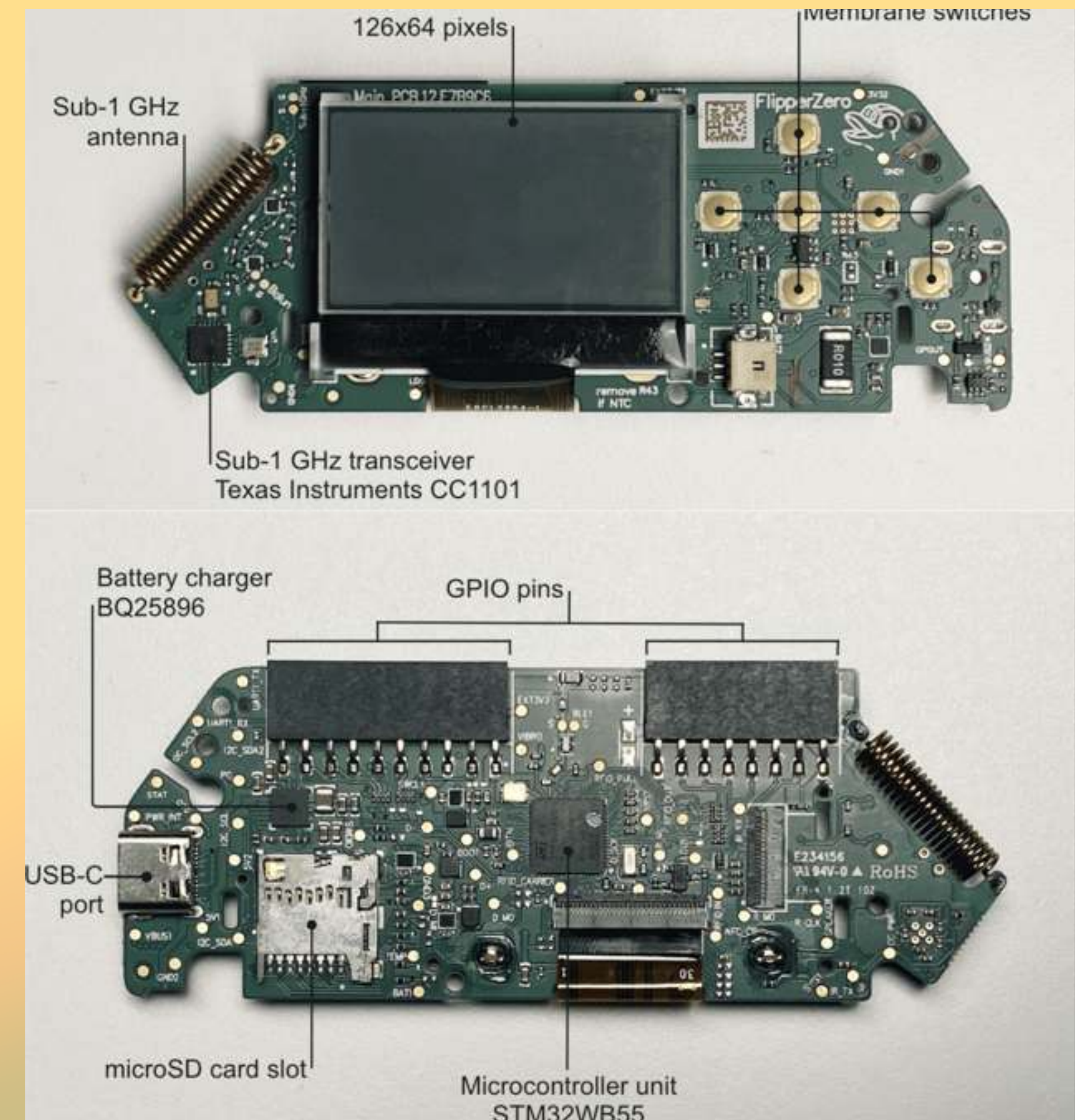
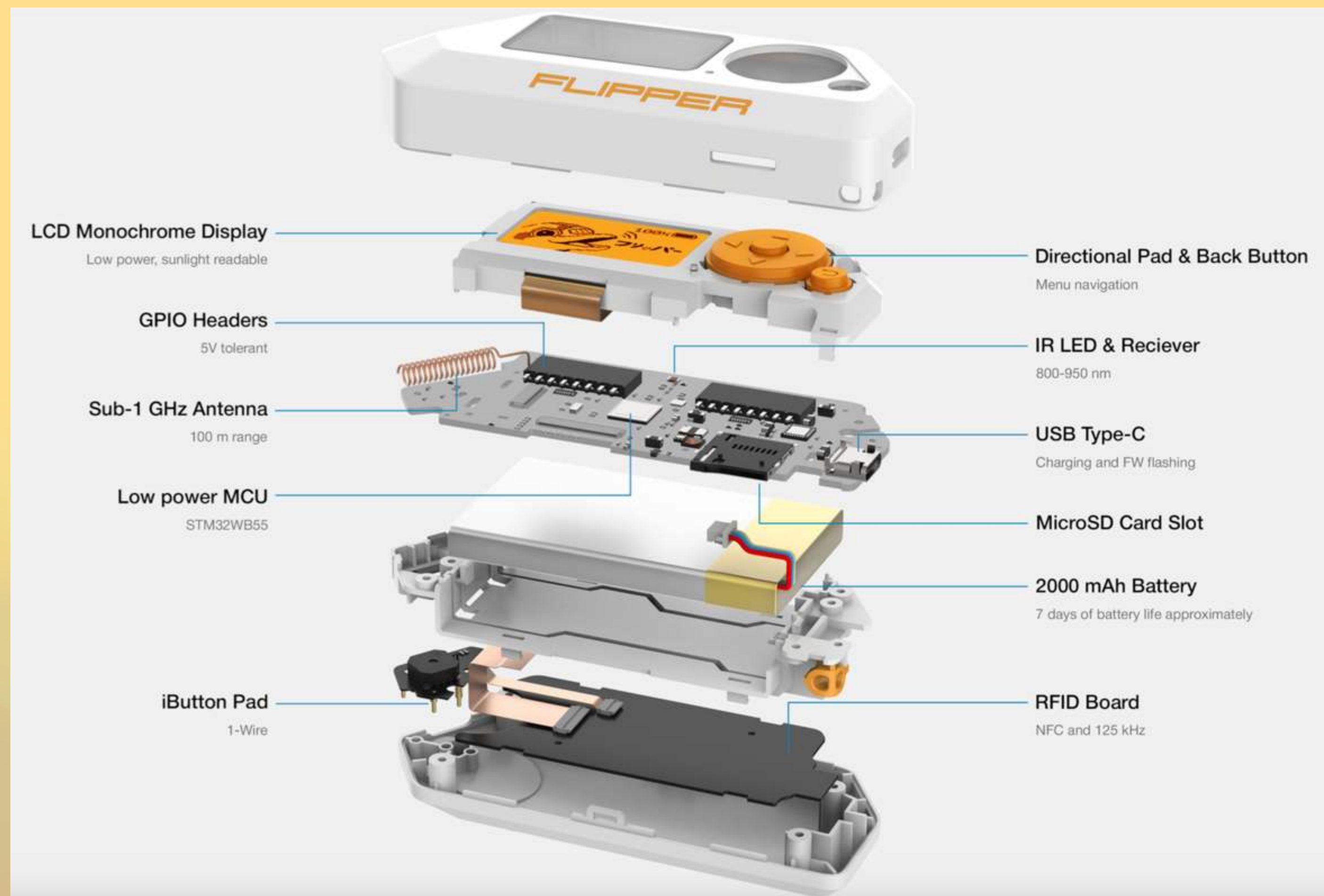
- Due to the prohibition of the flipper in Canada, I will solely showcase content that is already available on the internet and YouTube. I provide this information solely for *educational purposes* **only**, aiming to understand the potential dangers of this device and how to protect oneself. I do not assume any responsibility if anyone engages in any illegal activities, explicitly or implicitly, using the flipper or other devices and knowledge gained from this conference. My goal is to inform Canadians or guests about this device and its potential hazards, and how to be more safety.

About flipper

- Hardware ARM CPU.
- The Flipper is project are open sourced under the GNU License.
- Flipper OS: FreeRTOS (stewardship is Amazon)
- Ref. <https://en.wikipedia.org/wiki/FreeRTOS>
- Mosts applications are public in GitHub.

The Flipper Hardware

What's inside ?



Most popular Flipper firmwares

- Types of Flipper firmwares: RogueMaster, Unleashed, and Xtreme.
- <https://flipper-xtre.me/>
- <https://rogue-master.net/>
- <https://github.com/DarkFlippers/unleashed-firmware>

The Flipper's FWs compare list

Feature	RogueMaster	Unleashed	Xtreme
Stable Updates	✗	✓	✓
Rolling Code Support	✓	✓	✓
BLE Spam	⚠ Noproto hackamith API	✓	✓
Bad Keyboard (BT & USB)	⚠ Only as two separate apps	⚠ Only as two separate apps	✓
Subdriving (Saving coordinates for subghz)	✗	✗	✓
Full Customization (Layouts, Menus, Shortcuts, etc.)	✗	✗	✓
Management App (For easy configuration)	⚠ Partial functionality	✗	✓
Enhanced RGB Backlight modes (Full customization & Rainbow mode)	✓	✗	✓
Easy spoofing (Name, Mac, Serial)	✗	✓	✓
Advanced Security measures (Lock on Boot, reset on false pins, etc.)	✗	✗	✓
Asset Packs	✗	✗	✓
Advanced Level System	✓	✗	✓
File Search	✗	✗	✓
Improved Error Messages (Showing actual root)	✗	✗	✓
External Apps (Last checked: 07.2023)	✓ 204	⚠ Only with [e] pack (102)	✓ 122

Main app and Flipper CLI

[illegible]

The Flipper zero Article

- <https://infosecwriteups.com/the-ultimate-guide-cheatsheet-to-flipper-zero-d4c42d79d32c>



Wi-Fi Marauder hardware

- ESP32 controller - powerful Wifi controller developed for internet of things.
- Can be used for WiFi, Bluetooth, attack.
- 2.4 GHz ONLY!
- ESP32-S2-SOLO - Is my controller



The Flipper Marauder companion firmware

WIFI Marodeur firmware list



- https://lab.flipper.net/apps/esp32_wifi_marauder

- <https://github.com/SkeletonMan03/FZEasyMarauderFlash>

- <https://github.com/justcallmekoko/ESP32Marauder?tab=readme-ov-file>

- <https://github.com/chris-bc/esp32-gravity>



The Flipper Marauder companion & Gravity SW

- The gravity SW performs powerful attacks on Bluetooth, BLE, WiFi, and Zigbee.
- My ESP32-S2-SOLO is not supported by that FW :(

Supported Targets	ESP32	ESP32-C6	ESP32S2	ESP32S3
Wireless (802.11)	Yes	Yes	Yes	No(t Yet)
Bluetooth	Yes	Not Yet	No	No(t Yet)
BTLE	Yes	Maybe?	No	No(t Yet)
ZigBee/Thread	No	Yes	No	No(t Yet)
(802.15.4)				

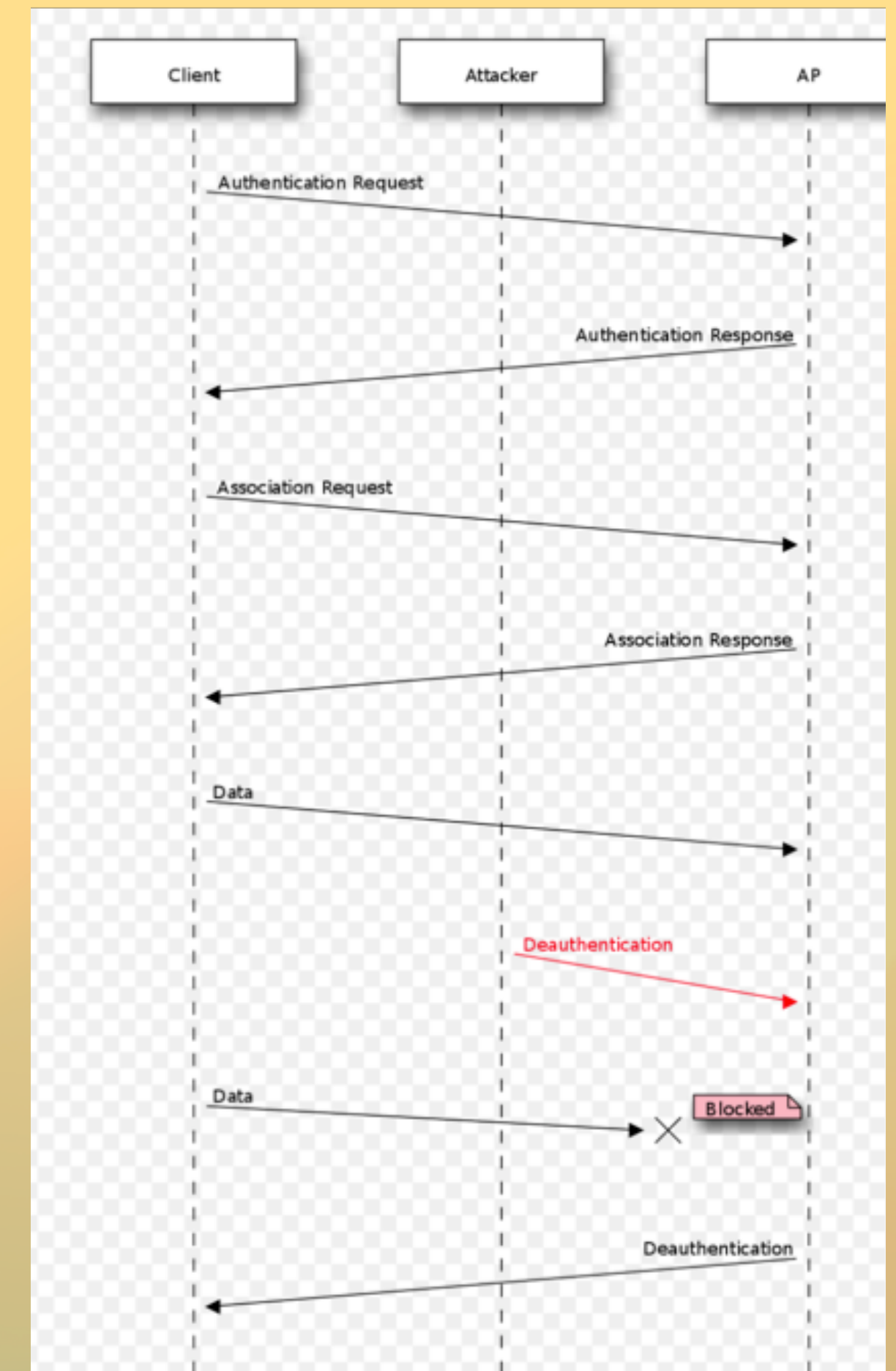
- <https://github.com/chris-bc/esp32-gravity>

What kind of Wi-Fi attacks Flipper (Marauder) support ?

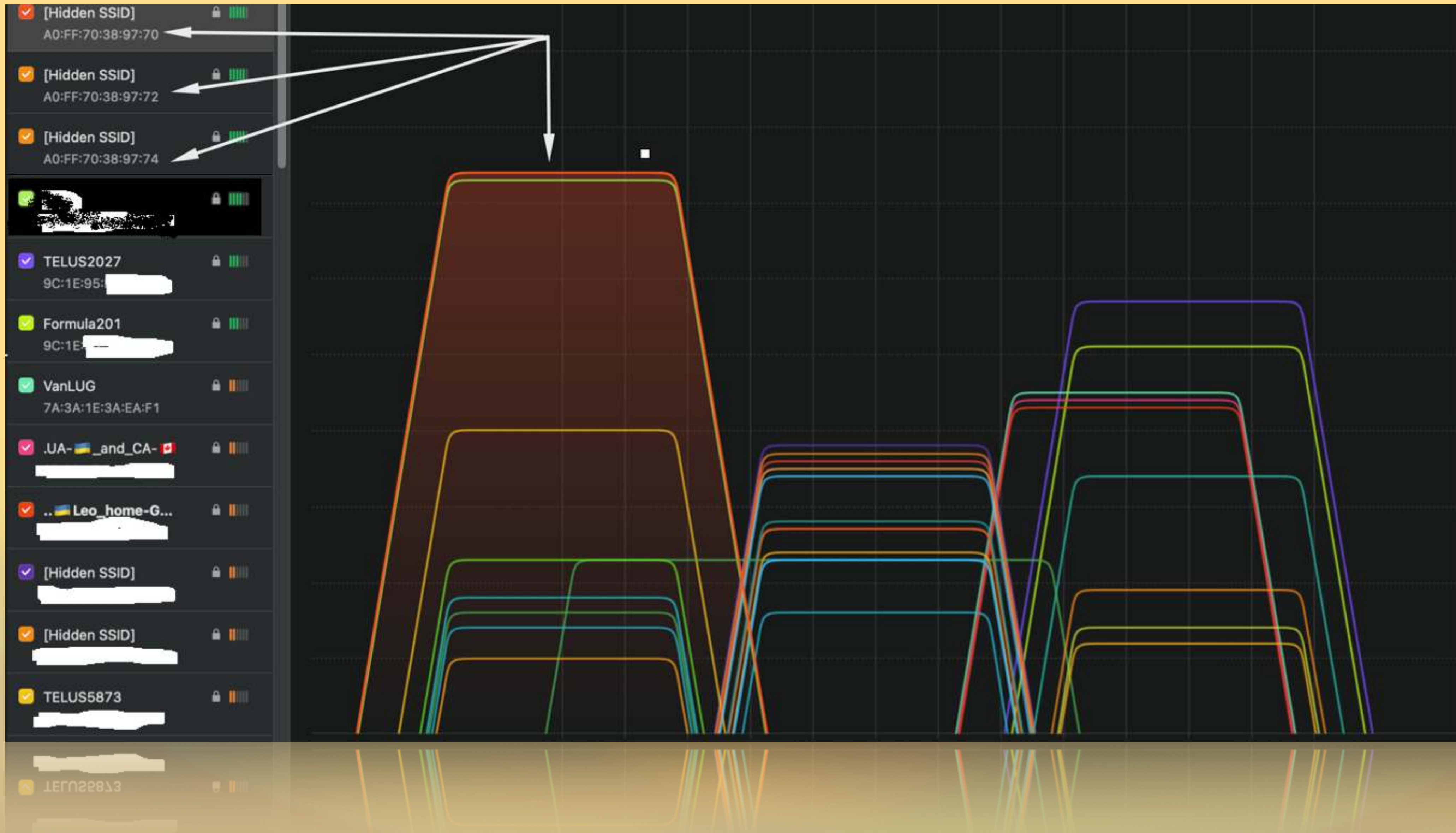
- Deauthentication attack
- Probe attack
- Rickroll attack
- Sour Apple
- Swiftpair spam
- Samsung spam
- Google spam
- Bt spam all

Wi-Fi “deauthentication” attack explanation

- This attack can be performed on WPA, WPA2, (WPA3 not tested by me)
- It is used to perform Evil twin access point(s), and Password attacks, or just wireless duos.
- How to protect? - MFP/802.11w



Wi-Fi “deauthentication” attack detection



Wi-Fi “deauthentication” attack detection

Wireshark investigation

701	2.789685	3b:39:68:e0:6c:9b	64:ce:98:46:5a:bd	802.11	172	Disassociate, SN=476, FN=12, Flags=opm..MFT[Malformed Packet]
1503	5.138657			802.11	154	Disassociate[Malformed Packet]
1505	5.139768	ad:c0:f0:9b:31:c8	c5:a5:7e:44:36:2d	802.11	172	Disassociate, SN=3237, FN=1, Flags=o.m.R.FT[Malformed Packet]
2944	8.401539	7c:70:92:c7:0a:34	4d:f1:d1:a3:83:65	802.11	172	Fragmented IEEE 802.11 frame
6460	14.622990	54:09:1a:c7:02:aa	ad:6b:c7:9d:e7:e0	802.11	172	Disassociate, SN=417, FN=5, Flags=.p..RMFT
131...	19.368618	94:be:5d:ad:60:14	a1:20:3b:31:1e:6c	802.11	172	Disassociate, SN=1152, FN=6, Flags=..m.R.FT[Malformed Packet]
132...	19.572994	2e:68:a0:86:f7:91	33:21:c2:f0:93:7a	802.11	168	Fragmented IEEE 802.11 frame
158...	24.848034	c3:98:e1:5f:af:54	40:8f:b3:18:f0:6a	802.11	172	Disassociate, SN=1254, FN=2, Flags=.pmP.MFT
171...	27.931085	d6:5a:da:ea:cf:70	30:12:92:4d:42:e0	802.11	172	Fragmented IEEE 802.11 frame
178...	30.256615	b7:f9:ba:0c:b2:6d	7c:6b:d8:97:e7:fc	802.11	172	Disassociate, SN=1710, FN=6, Flags=op...M.T[Malformed Packet]
181...	31.383565		85:eb:82:d4:f9:4d (85:eb:82:d4:f9:...	802.11	172	Control Wrapper, Flags=op.P.M..
189...	33.286186	b0:e9:4c:e4:ec:b6	97:51:2e:be:5a:17	802.11	172	Disassociate, SN=3061, FN=8, Flags=.pmP.M.T
207...	35.450592	d2:40:51:c4:50:cd	8b:b8:70:25:94:fa	802.11	172	Fragmented IEEE 802.11 frame
216...	36.863520	32:51:84:66:d8:3d	bb:d2:e0:79:f0:12	802.11	172	Disassociate, SN=3129, FN=5, Flags=op..RM.T[Malformed Packet]
222...	37.722475	0b:3d:20:24:4e:22	5a:26:9b:df:2c:67	802.11	172	Disassociate, SN=3779, FN=11, Flags=o.mP...T[Malformed Packet]
226...	38.142853		6e:3a:1e:3a:ea:f1	802.11	183	Disassociate, SN=1964, FN=0, Flags=.....
226...	38.143055		6e:3a:1e:3a:ea:f1	802.11	183	Disassociate, SN=1964, FN=0, Flags=.....
270...	40.492662	94:d5:3c:c5:d9:08	17:b3:85:98:5e:05	802.11	172	Disassociate, SN=1481, FN=13, Flags=.p..RM.T
276...	42.080027	f1:ff:22:97:9a:6a	ff:2d:7a:80:b2:6a	802.11	172	Disassociate, SN=3207, FN=1, Flags=.....T[Malformed Packet]
334...	52.986075	7b:0f:bf:75:c9:f8	7f:16:4c:75:cb:8e	802.11	172	Disassociate, SN=1952, FN=12, Flags=.pmP..FT
338...	53.780275			802.11	154	Disassociate[Malformed Packet]
342...	54.511576	b5:ba:9a:2d:00:99	c5:ac:50:18:17:2f	802.11	172	Disassociate, SN=1468, FN=7, Flags=op..R..T[Malformed Packet]

345... 24.211210 p2:p9:09:59:00:00 c2:9c:20:18:11:54 802.11 115 DT29220C19f6' 2M=1408' FN=1' F19d2=ob...B...T[Malformed Packet]
338... 23.180512 802.11 124 DT29220C19f6[Malformed Packet]
345... 24.211210 p2:p9:09:59:00:00 c2:9c:20:18:11:54 802.11 115 DT29220C19f6' 2M=1408' FN=1' F19d2=ob...B...T[Malformed Packet]
338... 23.180512 802.11 124 DT29220C19f6[Malformed Packet]

Wireshark filter command: wlan.fc.type_subtype == 0x0c

Rickroll Attack & Live Demo

The list of SSIDs of words form the Rickroll song

02	Never gonna let you down	4A:A4:69:37:97:B9		8	2.4	Open	4A:A4:69	b/g		-29	-29	-29	-29	-99	3s ago
07	Never gonna tell a lie	9E:FC:6E:07:4A:F2		5	2.4	Open	9E:FC:6E	b/g		-29	-29	-29	-29	-99	3s ago
02	Never gonna let you down	86:8E:04:EA:44:23		9	2.4	Open	86:8E:04	b/g		-29	-29	-29	-29	-99	3s ago
04	and desert you	60:11:25:9B:09:0E		5	2.4	Open	60:11:25	b/g		-30	-30	-30	-30	-99	3s ago
08	and hurt you	CC:57:E0:F8:62:CC		8	2.4	Open	CC:57:E0	b/g		-30	-30	-30	-30	-99	3s ago
06	Never gonna say goodbye	0A:20:F8:71:3B:3B		8	2.4	Open	0A:20:F8	b/g		-30	-30	-30	-30	-99	3s ago
05	Never gonna make you cry	D6:6E:9B:ED:DF:E8		9	2.4	Open	D6:6E:9B	b/g		-30	-30	-30	-30	-99	3s ago
06	Never gonna say goodbye	16:A1:B1:56:D7:28		5	2.4	Open	16:A1:B1	b/g		-31	-31	-31	-31	-99	3s ago
03	Never gonna run around	AE:3A:58:62:D0:13		9	2.4	Open	AE:3A:58			-31	-31	-31	-31	-99	3s ago
05	Never gonna make you cry	52:CA:37:3C:4D:38		9	2.4	Open	52:CA:37	b/g		-31	-31	-31	-31	-99	3s ago
01	Never gonna give you up	36:0D:89:44:8A:75		7	2.4	Open	36:0D:89	b/g		-31	-31	-31	-31	-99	3s ago
05	Never gonna make you cry	C0:C1:97:10:B0:41		7	2.4	Open	C0:C1:97	b/g		-31	-31	-31	-31	-99	3s ago
07	Never gonna tell a lie	6A:DE:20:91:21:1B		7	2.4	Open	6A:DE:20	b/g		-31	-31	-31	-31	-99	3s ago
07	Never gonna tell a lie	AA:A3:FD:CD:57:79		2	2.4	Open	AA:A3:FD	b/g		-32	-32	-32	-32	-99	3s ago
02	Never gonna let you down	1C:F6:C8:75:F1:74		5	2.4	Open	1C:F6:C8	b/g		-32	-32	-32	-32	-99	3s ago
04	and desert you	0C:FD:7E:03:48:46		8	2.4	Open	0C:FD:7E	b/g		-33	-33	-33	-33	-99	3s ago
03	Never gonna run around	AC:D4:FD:10:96:6C		1	2.4	Open	AC:D4:FD			-34	-34	-34	-34	-99	3s ago
02	Never gonna let you down	D0:B1:3B:D8:B4:A9		1	2.4	Open	D0:B1:3B	b/g		-34	-34	-34	-34	-99	3s ago
06	Never gonna say goodbye	CA:2B:38:B1:EE:F1		5	2.4	Open	CA:2B:38	b/g		-34	-34	-34	-34	-99	3s ago
03	Never gonna run around	08:BF:6F:95:C4:4B		2	2.4	Open	08:BF:6F			-34	-34	-34	-34	-99	3s ago
03	Never gonna run around	40:96:2F:5D:2B:2F		10	2.4	Open	40:96:2F			-35	-35	-35	-35	-99	3s ago
08	and hurt you	FA:DD:CC:81:F5:F1		2	2.4	Open	FA:DD:CC	b/g		-35	-35	-35	-35	-99	3s ago
08	and hurt you	FA:DD:CC:81:F5:F1		5	2.4	Open	FA:DD:CC	p/g		-32	-32	-32	-32	-99	3s ago
03	Never gonna run around	40:96:2F:5D:2B:2F		10	2.4	Open	40:96:2F			-32	-32	-32	-32	-99	3s ago
03	Never gonna run around	08:BF:6F:95:C4:4B		5	2.4	Open	08:BF:6F			-34	-34	-34	-34	-99	3s ago

The Wi-Fi Probe attack

Cisco's Meraki logs

- It is Probe spam (flood attack). It's DDOS tool

- ```
20:44:26.951190 unknown 802.11 ctrl frame subtype (5)
20:44:26.951537 unknown 802.11 ctrl frame subtype (5)
20:44:26.951940 unknown 802.11 ctrl frame subtype (5)
20:44:26.952240 unknown 802.11 ctrl frame subtype (5)
```

- ```
20:44:26.792254 unknown 802.11 frame type (3)
```

- ```
21:01:46.110238 Probe Request (VanLUG) [6.0* 9.0 12.0 18.0 24.0 36.0 48.0 54.0 Mbit]
21:01:46.110239 Probe Request (VanLUG) [6.0* 9.0 12.0 18.0 24.0 36.0 48.0 54.0 Mbit]
```

# The Wi-Fi Probe attack

Pay attention on Malformed packets

Apply a display filter ... <3%>

| No. | Time      | Source               | Destination          | Protocol | Length | Info                                                                           |
|-----|-----------|----------------------|----------------------|----------|--------|--------------------------------------------------------------------------------|
| 1   | 0.000000  | 7a:3a:1e:3a:ea:f1    | 7a:3a:1e:3a:ea:f1    | 802.11   | 197    | DMS Request[Malformed Packet]                                                  |
| 2   | 0.000001  | 7a:3a:1e:3a:ea:f1    | 7a:3a:1e:3a:ea:f1    | 802.11   | 197    | DMS Request[Malformed Packet]                                                  |
| 3   | 2.895547  | Broadcast            | Broadcast            | 802.11   | 312    | Probe Request, SN=3404, FN=0, Flags=....., SSID="VanLUG"                       |
| 4   | 2.895548  | Broadcast            | Broadcast            | 802.11   | 312    | Probe Request, SN=3404, FN=0, Flags=....., SSID="VanLUG"                       |
| 5   | 2.915811  | Broadcast            | Broadcast            | 802.11   | 312    | Probe Request, SN=3405, FN=0, Flags=....., SSID="VanLUG"                       |
| 6   | 2.915813  | Broadcast            | Broadcast            | 802.11   | 312    | Probe Request, SN=3405, FN=0, Flags=....., SSID="VanLUG"                       |
| 7   | 6.323070  | CiscoMeraki_3a:ea... | CiscoMeraki_3a:ea... | LLC      | 204    | I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Management Group, SSAP NULL LSAP Command |
| 8   | 6.510453  | CiscoMeraki_3a:ea... | CiscoMeraki_3a:ea... | LLC      | 254    | I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Management Group, SSAP NULL LSAP Command |
| 9   | 6.510464  | CiscoMeraki_3a:ea... | CiscoMeraki_3a:ea... | LLC      | 249    | I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Management Group, SSAP NULL LSAP Command |
| 10  | 6.510471  | CiscoMeraki_3a:ea... | CiscoMeraki_3a:ea... | LLC      | 251    | I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Management Group, SSAP NULL LSAP Command |
| 11  | 6.510479  | CiscoMeraki_3a:ea... | CiscoMeraki_3a:ea... | LLC      | 250    | I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Management Group, SSAP NULL LSAP Command |
| 12  | 11.386924 | CiscoMeraki_3a:ea... | CiscoMeraki_3a:ea... | LLC      | 248    | I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Management Group, SSAP NULL LSAP Command |
| 13  | 12.396268 | CiscoMeraki_3a:ea... | CiscoMeraki_3a:ea... | LLC      | 248    | I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Management Group, SSAP NULL LSAP Command |
| 14  | 13.405621 | CiscoMeraki_3a:ea... | CiscoMeraki_3a:ea... | LLC      | 248    | I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Management Group, SSAP NULL LSAP Command |
| 15  | 17.691253 | CiscoMeraki_3a:ea... | CiscoMeraki_3a:ea... | LLC      | 204    | I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Management Group, SSAP NULL LSAP Command |
| 16  | 29.994475 | CiscoMeraki_3a:ea... | CiscoMeraki_3a:ea... | LLC      | 204    | I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Management Group, SSAP NULL LSAP Command |
| 17  | 40.831124 | CiscoMeraki_3a:ea... | CiscoMeraki_3a:ea... | LLC      | 204    | I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Management Group, SSAP NULL LSAP Command |
| 18  | 51.480264 | CiscoMeraki_3a:ea... | CiscoMeraki_3a:ea... | LLC      | 204    | I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Management Group, SSAP NULL LSAP Command |

> Frame 2: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits)  
> Prism capture header  
> 802.11 radio information  
> IEEE 802.11 Action, Flags: .....  
IEEE 802.11 Wireless Management  
Fixed parameters  
Tagged parameters (27 bytes)  
Tag: Diagnostic Report  
Tag Number: Diagnostic Report (81)  
Tag length: 99  
[Expert Info (Error/Malformed): Tag Length is longer than remaining payload]  
[Tag Length is longer than remaining payload]  
[Severity level: Error]  
[Group: Malformed]  
[Malformed Packet: IEEE 802.11]  
[Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]  
[Malformed Packet (Exception occurred)]  
[Severity level: Error]  
[Group: Malformed]

0000 44 00 00 00 90 00 00 00 00 00 00 00 00 00 00 00 D.....  
0010 00 00 00 00 00 00 00 00 00 00 44 00 01 00 00 00 04 00 .....D..  
0020 00 00 00 00 44 00 02 00 00 00 04 00 00 00 00 00 00 .....D..  
0030 44 00 03 00 00 00 04 00 0a 00 00 00 44 00 04 00 D.....  
0040 00 00 04 00 16 00 00 00 00 00 00 00 00 00 00 00 .....  
0050 00 00 00 00 44 00 06 00 00 00 04 00 16 00 00 00 .....D..  
0060 00 00 00 00 00 00 00 00 00 00 00 00 44 00 08 00 .....  
0070 00 00 04 00 02 00 00 00 44 00 09 00 00 00 04 00 .....  
0080 00 00 00 00 44 00 0a 00 00 00 04 00 35 00 00 00 .....D..  
0090 d0 00 3a 01 7a 3a 1e 3a ea f1 76 02 27 8a b6 d0 :.:z:..  
00a0 7a 3a 1e 3a ea f1 f0 58 0a 17 51 63 18 00 16 00 z:~:..  
00b0 0e 13 00 04 55 04 00 00 00 00 c0 00 00 fb 00 00 .....U..  
00c0 00 09 00 11 00 .....  
00d0 .....

Levkos\_home\_MX-Levko's Home router\_IF-Wireless (5).pcap  
Levkos\_home\_MX-Levko's Home router\_IF-Wireless (2).pcap

Packets: 18 - Displayed: 18 (100.0%)  
Packets: 18 - Displayed: 18 (100.0%)

Profile: Defau  
Profile: Defau

# The Wi-Fi Probe Attack

| No.    | Time      | Source                | Destination | Protocol | Length | Info                                                                              |
|--------|-----------|-----------------------|-------------|----------|--------|-----------------------------------------------------------------------------------|
| 780... | 54.299360 | 1d:ed:58:16:1a:30     | Broadcast   | 802.11   | 216    | Probe Request, SN=0, FN=1, Flags=....., SSID=VanLUG                               |
| 781... | 54.506158 | 5e:09:8f:59:86:32     | Broadcast   | 802.11   | 216    | Probe Request, SN=0, FN=1, Flags=....., SSID="VanLUG"                             |
| 781... | 54.545826 | 9a:42:28:e1:5a:fd     | Broadcast   | 802.11   | 216    | Probe Request, SN=0, FN=1, Flags=....., SSID="VanLUG"                             |
| 781... | 54.545828 | 9a:42:28:e1:5a:fd     | Broadcast   | 802.11   | 216    | Probe Request, SN=0, FN=1, Flags=....., SSID="VanLUG"                             |
| 782... | 54.721412 | 44:24:a6:59:e5:ab     | Broadcast   | 802.11   | 216    | Probe Request, SN=0, FN=1, Flags=....., SSID="VanLUG"                             |
| 782... | 54.721414 | 44:24:a6:59:e5:ab     | Broadcast   | 802.11   | 216    | Probe Request, SN=0, FN=1, Flags=....., SSID="VanLUG"                             |
| 782... | 54.899408 | dc:8f:e6:ce:26:15     | Broadcast   | 802.11   | 216    | Probe Request, SN=0, FN=1, Flags=....., SSID="VanLUG"                             |
| 783... | 55.002528 | 55:8f:cd:e0:37:3e     | Broadcast   | 802.11   | 216    | Probe Request, SN=0, FN=1, Flags=....., SSID="VanLUG"                             |
| 783... | 55.106635 | 8b:81:0a:48:06:9a     | Broadcast   | 802.11   | 216    | Probe Request, SN=0, FN=1, Flags=....., SSID="VanLUG"                             |
| 783... | 55.106636 | 8b:81:0a:48:06:9a     | Broadcast   | 802.11   | 216    | Probe Request, SN=0, FN=1, Flags=....., SSID="VanLUG"                             |
| 784... | 55.408784 | 8a:b7:6c:7e:60:12     | Broadcast   | 802.11   | 216    | Probe Request, SN=0, FN=1, Flags=....., SSID="VanLUG"                             |
| 786... | 55.500433 | 4f:19:9c:2e:4a:d2     | Broadcast   | 802.11   | 216    | Probe Request, SN=0, FN=1, Flags=....., SSID="VanLUG"                             |
| 786... | 55.500439 | 4f:19:9c:2e:4a:d2     | Broadcast   | 802.11   | 216    | Probe Request, SN=0, FN=1, Flags=....., SSID="VanLUG"                             |
| 786... | 55.500446 | b3:1b:86:4f:73:23     | Broadcast   | 802.11   | 216    | Probe Request, SN=0, FN=3, Flags=....., SSID=acc2dc989ace330002101825 [Malformed] |
| 787... | 55.570052 | 09:0a:1e:99:0f:8f     | Broadcast   | 802.11   | 216    | Probe Request, SN=0, FN=1, Flags=....., SSID="VanLUG"                             |
| 787... | 55.570054 | 09:0a:1e:99:0f:8f     | Broadcast   | 802.11   | 216    | Probe Request, SN=0, FN=1, Flags=....., SSID="VanLUG"                             |
| 787... | 55.611942 | TexasInstrum_7f:86:40 | Broadcast   | 802.11   | 238    | Probe Request, SN=1126, FN=0, Flags=....., SSID="4KQCyrN6HS0k"                    |
| 787... | 55.611943 | TexasInstrum_7f:86:40 | Broadcast   | 802.11   | 238    | Probe Request, SN=1126, FN=0, Flags=....., SSID="4KQCyrN6HS0k"                    |
| 787... | 55.618022 | TexasInstrum_7f:86:40 | Broadcast   | 802.11   | 238    | Probe Request, SN=1127, FN=0, Flags=....., SSID="4KQCyrN6HS0k"                    |
| 787... | 55.618023 | TexasInstrum_7f:86:40 | Broadcast   | 802.11   | 238    | Probe Request, SN=1127, FN=0, Flags=....., SSID="4KQCyrN6HS0k"                    |
| 787... | 55.684512 | 81:f8:75:8a:27:90     | Broadcast   | 802.11   | 216    | Probe Request, SN=0, FN=1, Flags=....., SSID="VanLUG"                             |
| 787... | 55.693533 | TexasInstrum_7f:88:88 | Broadcast   | 802.11   | 238    | Probe Request, SN=1113, FN=0, Flags=....., SSID="4KQCyrN6HS0k"                    |
| 787... | 55.693535 | TexasInstrum_7f:88:88 | Broadcast   | 802.11   | 238    | Probe Request, SN=1113, FN=0, Flags=....., SSID="4KQCyrN6HS0k"                    |
| 788... | 55.818250 | 02:5e:df:07:f8:07     | Broadcast   | 802.11   | 216    | Probe Request, SN=0, FN=1, Flags=....., SSID="VanLUG"                             |

> Frame 78602: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits)

> Prism capture header

> 802.11 radio information

> IEEE 802.11 Probe Request, Flags: .....

> IEEE 802.11 Wireless Management

< [Malformed Packet: IEEE 802.11]

- [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
- [Malformed Packet (Exception occurred)]
- [Severity level: Error]
- [Group: Malformed]

```

0000 44 00 00 00 90 00 00 00 00 00 00 00 00 00 00 00 D...
0010 00 00 00 00 00 00 00 00 44 00 01 00 00 00 04 00
0020 00 00 00 00 44 00 02 00 00 00 04 00 00 00 00 00
0030 44 00 03 00 00 00 04 00 0a 00 00 00 44 00 04 00 D...
0040 00 00 04 00 1a 00 00 00 00 00 00 00 00 00 00 00
0050 00 00 00 00 44 00 06 00 00 00 04 00 1a 00 00 00D
0060 00 00 00 00 00 00 00 00 00 00 00 00 44 00 08 00
0070 00 00 04 00 02 00 00 00 44 00 09 00 00 00 04 00
0080 00 00 00 00 44 00 0a 00 00 00 04 00 48 00 00 00D
0090 40 00 00 00 ff ff ff ff ff ff b3 1b 86 4f 73 23 @....
00a0 fe ff ff ff ff ff 03 00 00 0c ac c2 dc 98 9a ce
00b0 33 00 02 10 18 25 30 48 00 a6 01 6c 21 79 3d 58 3...
00c0 4f 3f 23 0b 57 e8 b8 f6 ff 8e 81 11 b1 69 18 a8 0?#·W
00d0 fd c4 db 89 ca a4 76 c3

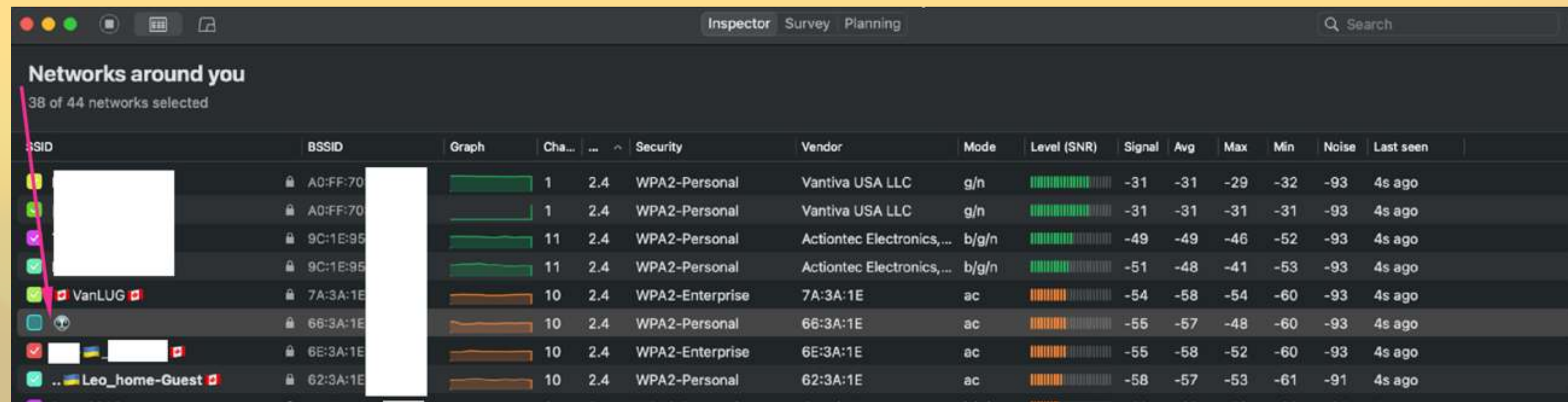
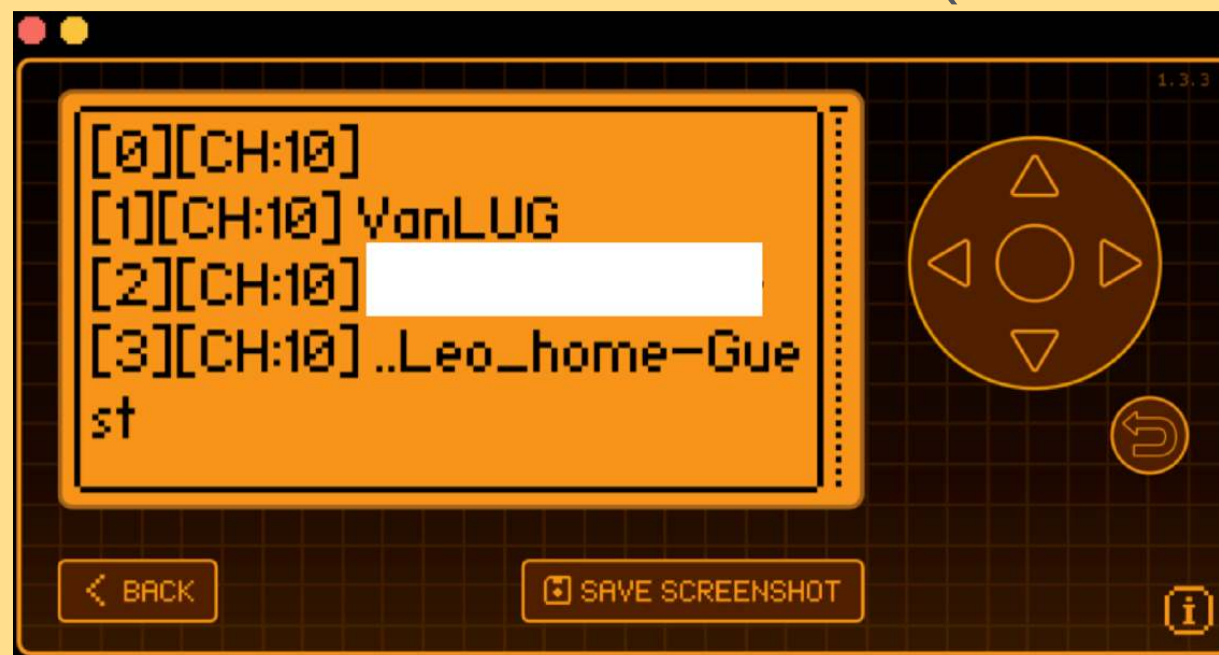
```

- The Wireshark filter: wlan.fc.type\_subtype == 0x04

# Wi-Fi SSID and Unicode name(s)

Flipper can't visualise unicodes

- But it can attack (deauthentication) that network(s) by ID :)



| SSID             | BSSID        | Graph      | Cha... | ... | Security        | Vendor                    | Mode  | Level (SNR) | Signal | Avg | Max | Min | Noise | Last seen |
|------------------|--------------|------------|--------|-----|-----------------|---------------------------|-------|-------------|--------|-----|-----|-----|-------|-----------|
| [REDACTED]       | A0:FF:70:... | [REDACTED] | 1      | 2.4 | WPA2-Personal   | Vantiva USA LLC           | g/n   | [REDACTED]  | -31    | -31 | -29 | -32 | -93   | 4s ago    |
| [REDACTED]       | A0:FF:70:... | [REDACTED] | 1      | 2.4 | WPA2-Personal   | Vantiva USA LLC           | g/n   | [REDACTED]  | -31    | -31 | -31 | -31 | -93   | 4s ago    |
| [REDACTED]       | 9C:1E:95:... | [REDACTED] | 11     | 2.4 | WPA2-Personal   | Actiontec Electronics,... | b/g/n | [REDACTED]  | -49    | -49 | -46 | -52 | -93   | 4s ago    |
| [REDACTED]       | 9C:1E:95:... | [REDACTED] | 11     | 2.4 | WPA2-Personal   | Actiontec Electronics,... | b/g/n | [REDACTED]  | -51    | -48 | -41 | -53 | -93   | 4s ago    |
| VanLUG           | 7A:3A:1E:... | [REDACTED] | 10     | 2.4 | WPA2-Enterprise | 7A:3A:1E                  | ac    | [REDACTED]  | -54    | -58 | -54 | -60 | -93   | 4s ago    |
| [REDACTED]       | 66:3A:1E:... | [REDACTED] | 10     | 2.4 | WPA2-Personal   | 66:3A:1E                  | ac    | [REDACTED]  | -55    | -57 | -48 | -60 | -93   | 4s ago    |
| [REDACTED]       | 6E:3A:1E:... | [REDACTED] | 10     | 2.4 | WPA2-Enterprise | 6E:3A:1E                  | ac    | [REDACTED]  | -55    | -58 | -52 | -60 | -93   | 4s ago    |
| ..Leo_home-Guest | 62:3A:1E:... | [REDACTED] | 10     | 2.4 | WPA2-Personal   | 62:3A:1E                  | ac    | [REDACTED]  | -58    | -57 | -53 | -61 | -91   | 4s ago    |

Here is my article about Wi-Fi and unicodes:

<https://leo2008k.medium.com/and-other-pictures-based-on-unicode-in-your-wireless-network-name-via-wifi-ssid-at-mikrotik-425a72a9ce34>

# WPA/WPA 2 and the Flipper zero

RAW data sniffed

- Manually Convert network dump file with handshakes: PMKID&EAPOL, PMKID, EAPOL-hccapx, EAPOL-hccap, WPAPSK-john to hashcat.22000 file  
<https://github.com/ZerBea/hcxttools>
- To Automatically convert that .pcap we can use that hashcat web site:  
<https://hashcat.net/cap2hashcat/>
- Then execute this command:  
`hashcat -m 22000 -a 3 VanLUG_PMKID.hc22000 '123QWEasdZX?u'`



# Wi-Fi and flipper zero

WPA/WPA 2 Hacking topic

- Live DEMO

# WiFi and flipper zero

We can Automate that process by this web resource:

<https://www.onlinehashcrack.com/tasks>

[HOME](#) [PASSWORD RECOVERY](#) [HOW TO?](#) [FREE TOOLS](#) [ALGORITHMS](#) [ABOUT](#)

Hashes / WPA / Office

Tutorials About Security

For Passwords

And Cryptography

Our Services

MY TASKS: 2 / 10

⚠ We highly recommend setting up a password for your account to ensure its protection. This can be easily done on the [Settings](#) page.

🎉 Success!

✓ ESSID\_Leo\_home-Guest : successfully added.

📧 We will use [redacted] to notify you if recovered or not (watch your spam folder!)

✓ Private link to follow the task process: [www.OnlineHashCrack.com/s7exj6qnd1](https://www.OnlineHashCrack.com/s7exj6qnd1)

SHOW 25 ENTRIES

SEARCH:

| Task                                                                                           | Algorithm | Priority            | Wordlist                                                | Bruteforce             | Status                      | Size | Password  |
|------------------------------------------------------------------------------------------------|-----------|---------------------|---------------------------------------------------------|------------------------|-----------------------------|------|-----------|
|  Leo_62.3e1 | WPA(2)    | Normal<br>Speed up! | <a href="#">Free wordlist</a><br><a href="#">SELECT</a> | <a href="#">SELECT</a> | <a href="#">IN PROGRESS</a> | -    | -         |
|  Leo_62.3e1 | WPA(2)    | Normal              | <a href="#">Free wordlist</a>                           |                        | <a href="#">FOUND</a>       | 9    | 123QWEasd |

Showing 1 to 2 of 2 entries

[Export all tasks as](#)

[Previous](#)



# WPA 2 Enterprise

I found EAP Identity value - its means Wi-Fi reconnaissance attack can be performed

The image shows a Wireshark packet capture of an EAP Identity exchange. The top pane displays a list of packets, with packet 453 selected. The bottom pane shows the detailed view of packet 453, which is an IEEE 802.11 QoS Data frame. The frame contains a Logical-Link Control (LLC) subframe, which in turn contains an 802.1X Authentication subframe. The 802.1X Authentication subframe is an Extensible Authentication Protocol (EAP) packet, specifically an EAP Identity packet. The packet details show the following structure:

- IEEE 802.11 QoS Data, Flags: .....T
- Logical-Link Control
- 802.1X Authentication
  - Version: 802.1X-2001 (1)
  - Type: EAP Packet (0)
  - Length: 22
  - Extensible Authentication Protocol
    - Code: Response (2)
    - Id: 211
    - Length: 22
    - Type: Identity (1)
    - Identity: blkbnk3c@duck.com

The packet details pane also shows the raw data of the packet, which is a hexadecimal string: 88 01 3a 01 7a 3a 1e 3a ea f1 10 8e e0 1a 1a c4 7a 3a 1e 3a ea f1 00 00 06 00 aa aa 03 00 00 00 88 8e 01 00 00 16 02 d3 00 16 01 62 6c 6b 62 6d 6b 33 63 40 64 75 63 6b 2e 63 6f 6d 78 56 ad ba. The packet list pane shows the following information for packet 453:

| No. | Time      | Source       | Destination  | Protocol | Length | Info               |
|-----|-----------|--------------|--------------|----------|--------|--------------------|
| 453 | 12.152121 | SamsungElect | 7a:3a:1e:3a: | EAP      | 64     | Response, Identity |
| 524 | 14.233203 | Apple        | 6e:3a:       | EAP      | 65     | Response, Identity |

# Evil Twin Attack

FAKE Access Point. Please don't connect!

- Live DEMO

# Evil Twin Attack

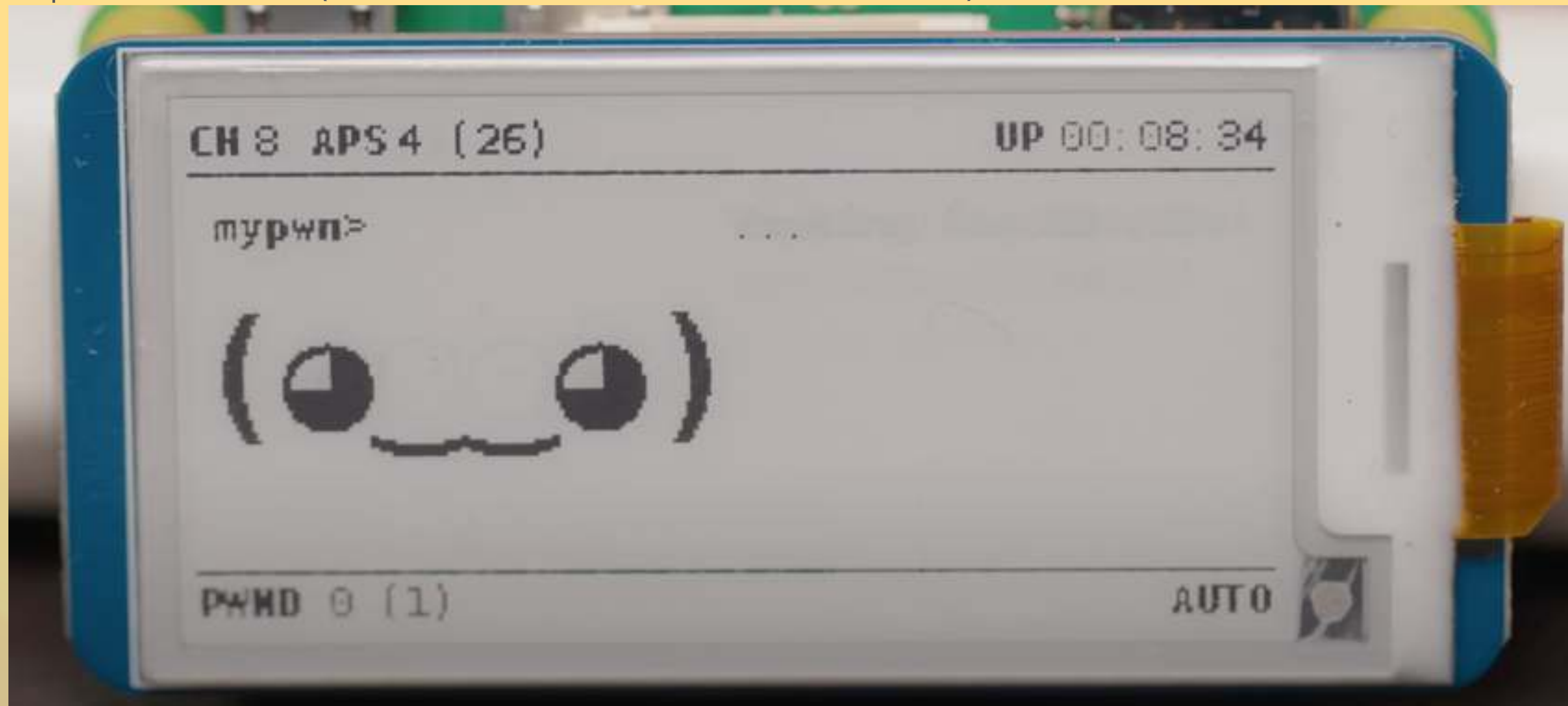
FAKE Access Point. Please don't connect!

- How to protect?
- Use VPN in public Wi-Fi
- Check SSL/TLS

# Flipper Fi-Wi hacking alternative(s)

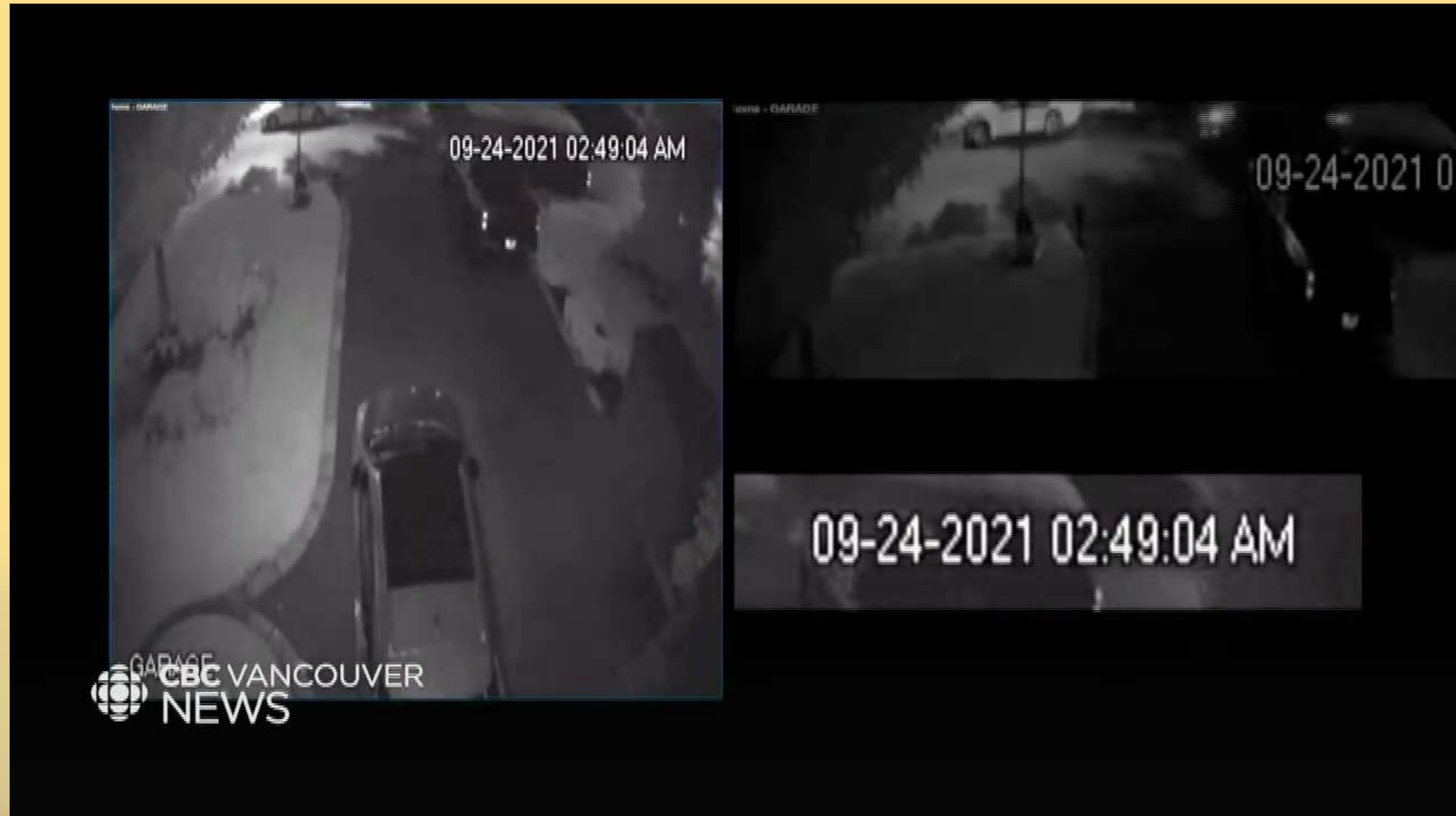
PWNAGOTCHI

- Open source (Based on Arduino and Linux)



# Car theft

Let's review that video



As far as you can see, professionals use different devices than Flipper.

# Bluetooth, BLE, spam/flood attack

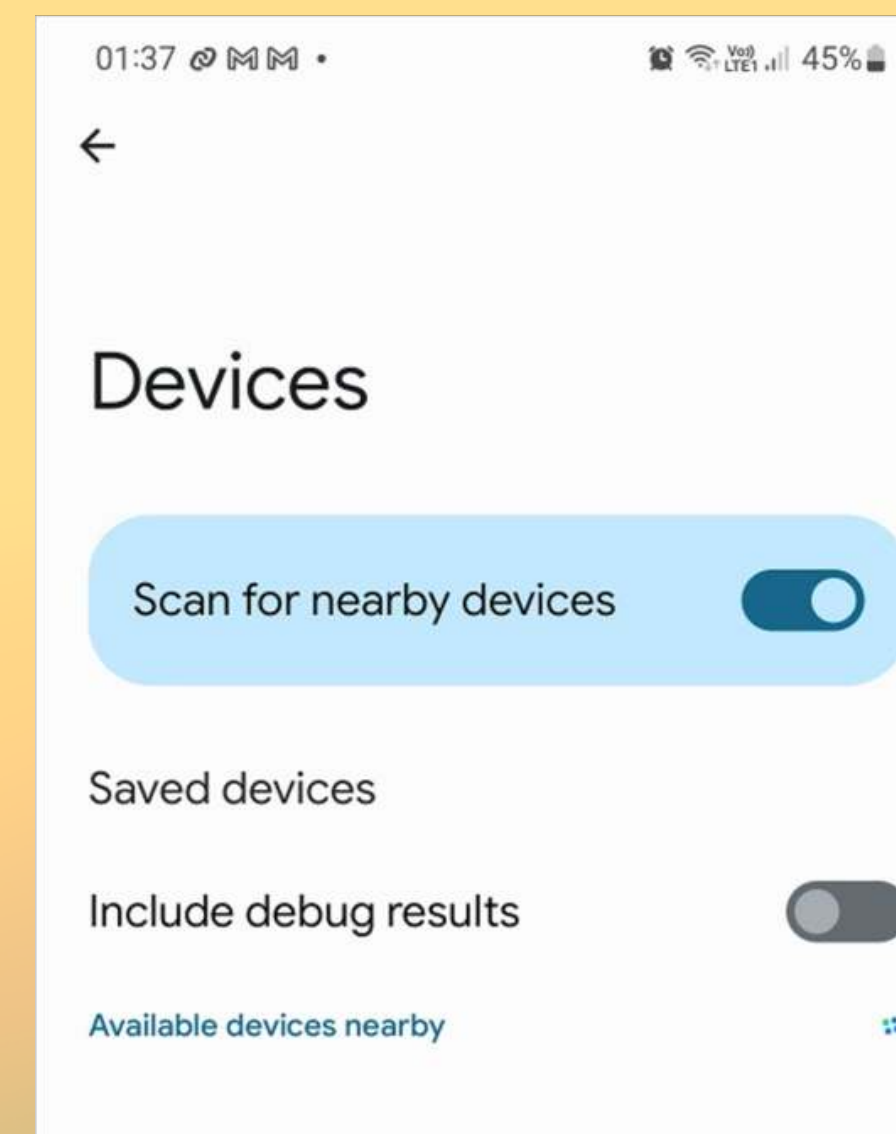
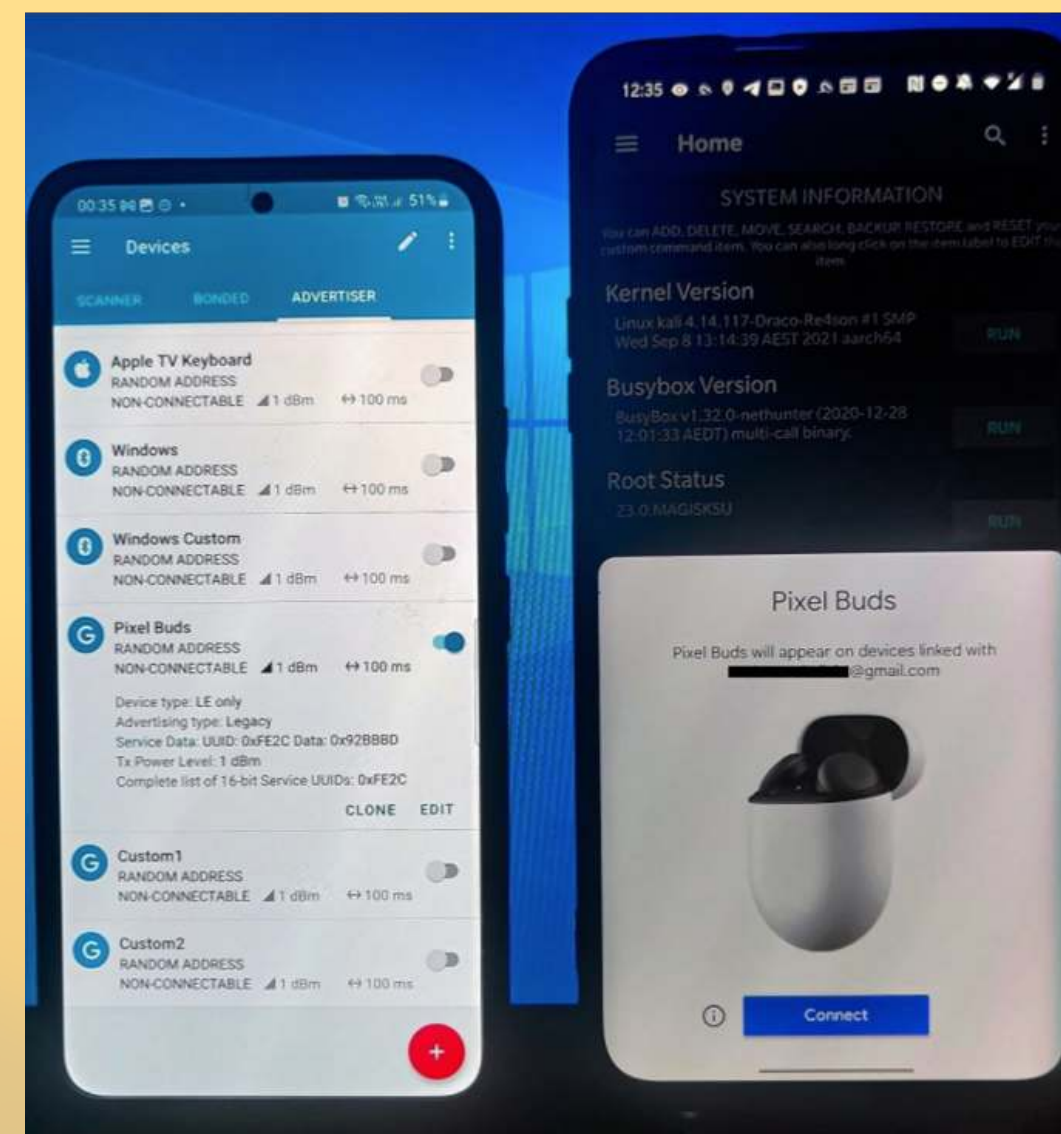
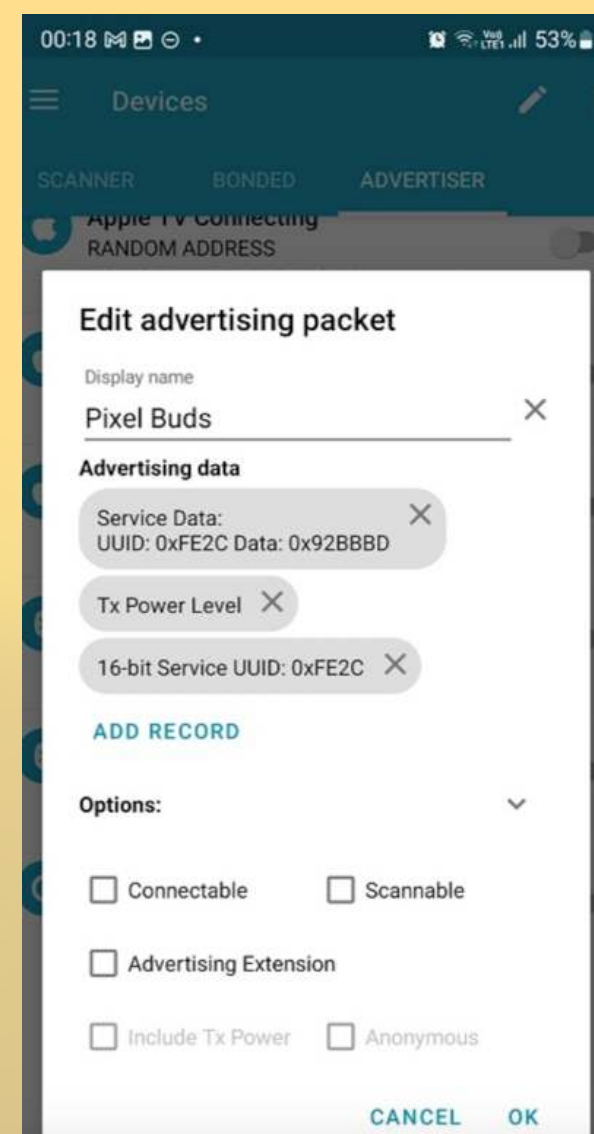
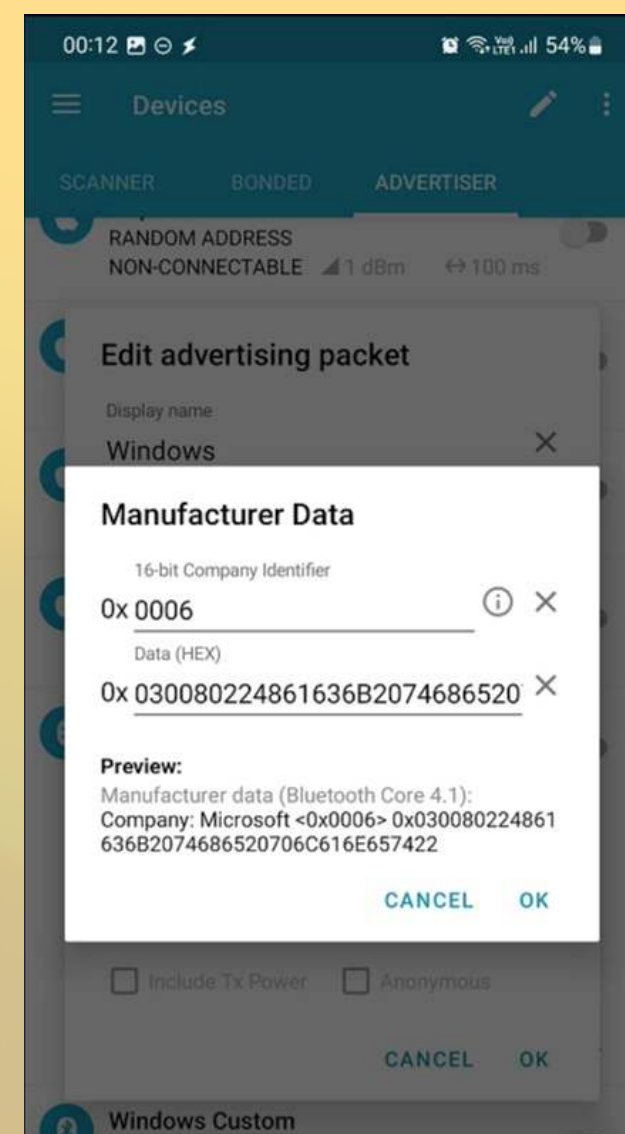
Live demo

- Source <https://github.com/ECTO-1A/AppleJuice>
- Additional option “Mac randomisation”

# Bluetooth, BLE, flood alternative

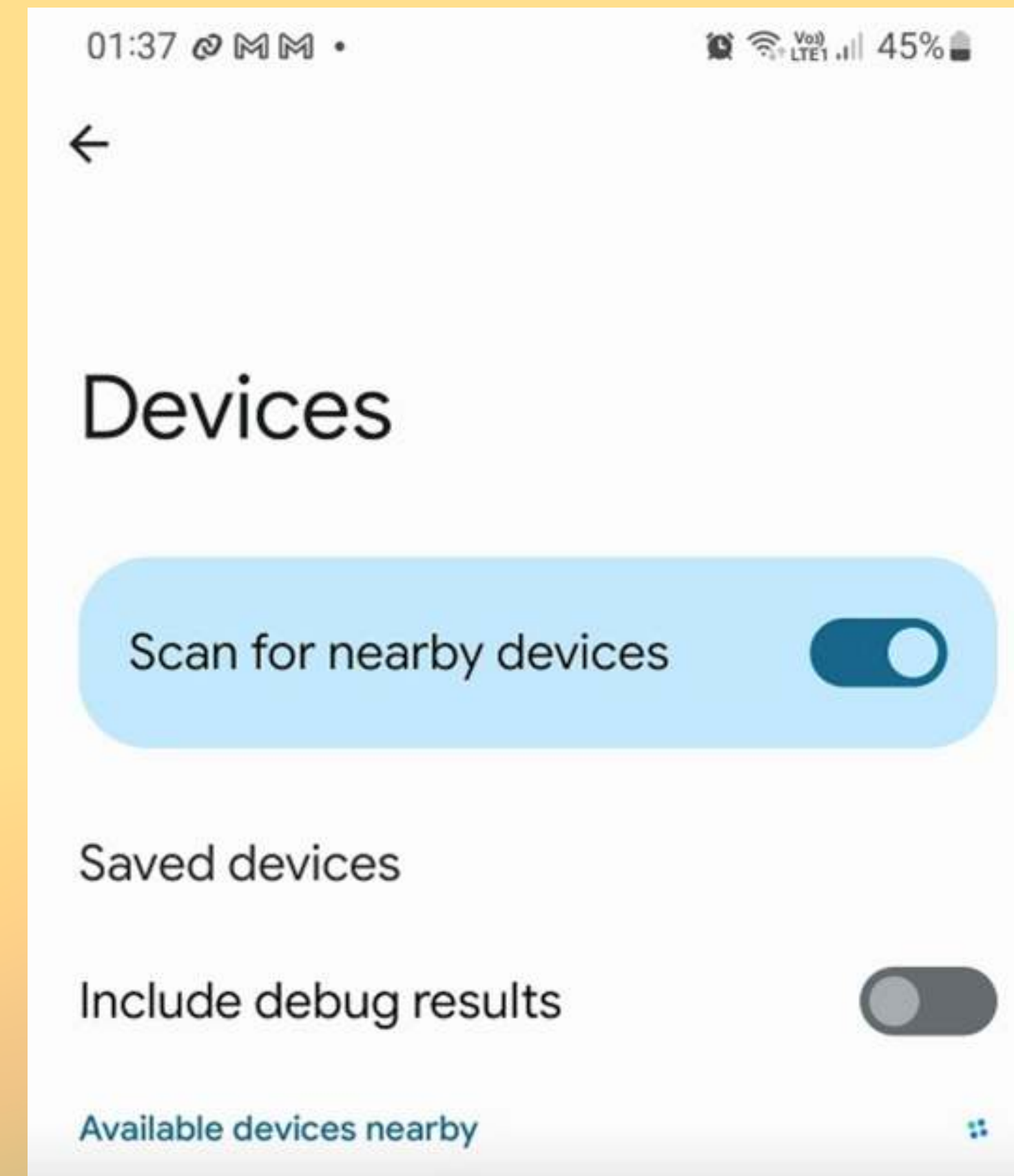
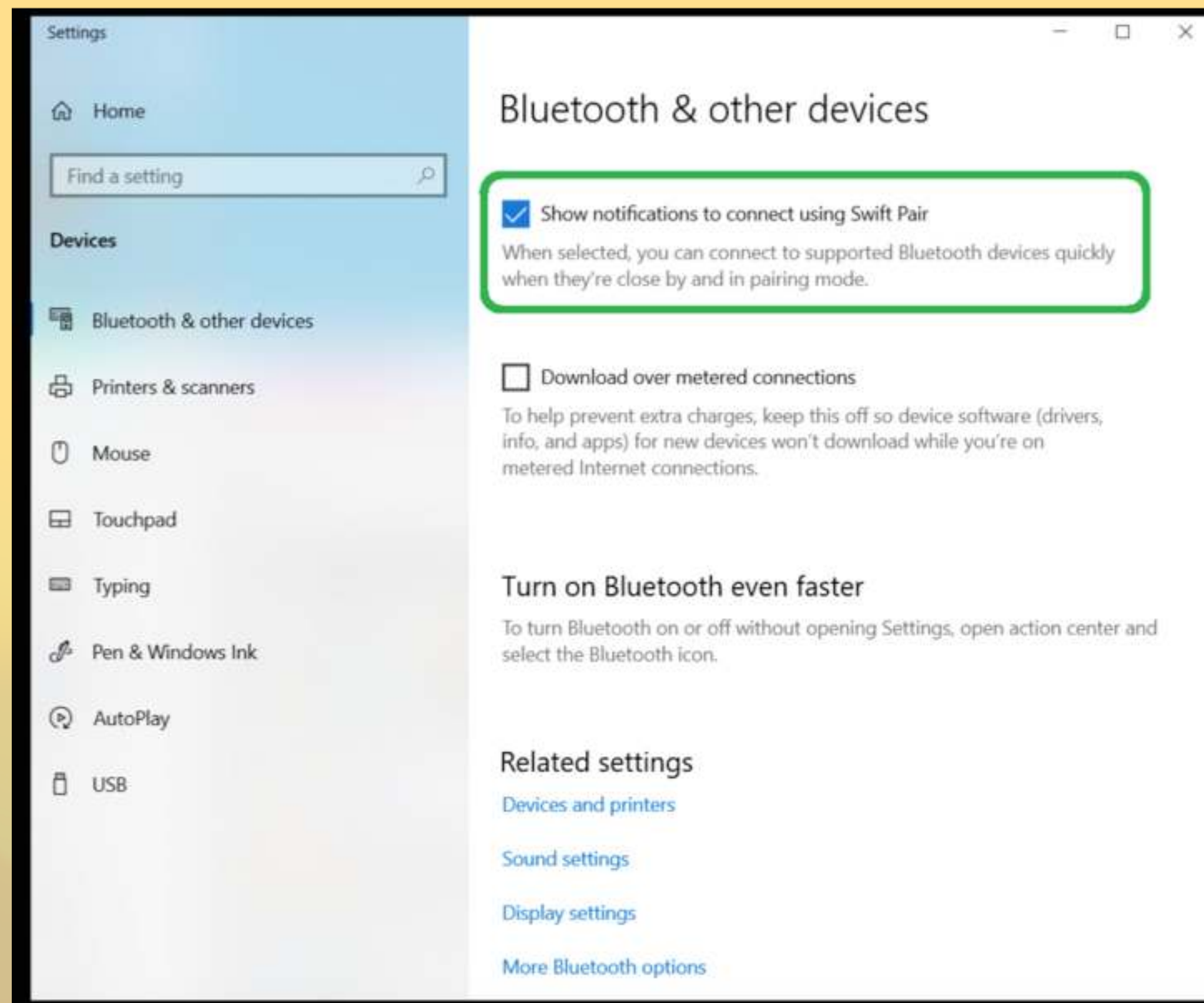
As variant it can perform via Android phone

- Alternative tool is mobile phones i.e. Android
- Source: <https://www.mobile-hacker.com/2023/10/17/spam-ios-android-and-windows-with-bluetooth-pairing-messages-using-flipper-zero-or-android-smartphone/>



Bluetooth (BLE) spam protection, or better yet, mitigation of attacks.

How to protect? Solution: Disable Notifications or Bluetooth



# Bad USB

- The Flipper support the “Rubber Ducky Script Language”
- Ref. <https://web.archive.org/web/20220816200129/http://github.com/hak5darren/USB-Rubber-Ducky/wiki/Duckyscript>
- Ref. [https://github.com/UNC0V3R3D/Flipper\\_Zero-BadUsb/tree/main/BadUsb-Collection/Windows\\_Badusb/Execution](https://github.com/UNC0V3R3D/Flipper_Zero-BadUsb/tree/main/BadUsb-Collection/Windows_Badusb/Execution)
- Ref. <https://github.com/topics/badusb>
- Why it can be dangerous?



# Bad USB

- Live demo

# The NFC clone alternatives

- Proxmark3
- NFC Research group on GitHub
- Live demo

## NFC Research



iceman1001



RFID Research Group

## Proxmark3 Easy



# Infrared port, Sub Ghz, iButton, 125 Khz RFID, RFID

- The Flipper owner can enable/disable TVs, Air conditioners, control remote devices, etc.



# The flipper's alternatives

- 1. Raspberry Pi
- 2. Crazy Radio 2
- 3. Cactus WHID (Keylogger)
- 4. Dstike Wi-Fi Deauther
- 5. USB Rubber Ducky
- 6. LAN Turtle
- 7. Magspoof
- 8. Piña Wi-Fi
- 9. Ubertooth One
- 10. Smartphone(s)
- 11. The Wi-Fi Pineapple
- 12. ChameleonMini (NFC emulator)
- 13. USB Rubber Ducky (perform BAD USB attack)



Levko Kravchuk

