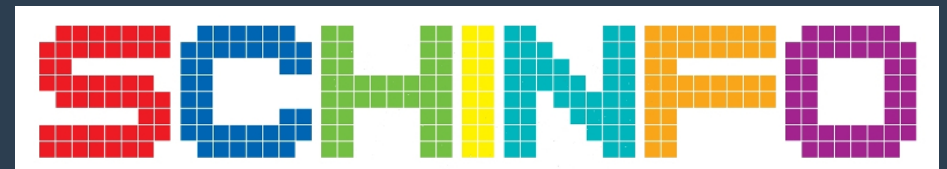




2.4 GHz WLAN

- ganz sicher unsicher !

- Helmut Stult
- IT-Professional seit 1983
- <https://www.schinfo.de>



SCHINFO

Linux Mint Sponsor #61

Wer bin ich / wer sind wir ?

- Internationale Gruppe aus D, ES, GB, GR, H

Projekte:

- **Deauther**
- **hackOx**
- **MalDuino**
- **KickThemOut**
- **LanGost**
- **u.v.m. ...**



Der Aha-Moment

- **Nehmen Sie Ihr Smartphone, Tablett oder Notebook zur Hand**
- **Verbinden Sie sich mit dem WLAN „schinfo-test“ (PW: 12345678)**
- **Jeder verbunden ?**
- **Immer noch ?**



SCHINFO is coming ... WiFi is going!

Das Problem

- **IEEE 802.11 hat einen Design-Fehler**
- **akzeptiert**
„unprotected Management Frames“
- **ist damit unsicher und angreifbar**
- **Fix mit 802.11w-2009 vorhanden,**
aber kaum benutzt bzw. bekannt
- **bisher Lösen durch „Totschweigen“**
und Ignorieren

Die Folgen

- **keine WLAN-Verbindung mehr !!!**

Beispiele:

- kein WiFi-VoIP-Telefon, Amzon EchoSpot, ...
- keine Kommissionier-Scanner
- materielle Folgeschäden in nicht absehbarer Höhe (z.B. >1000 € pro Sekunde in meinem Umfeld)

Wir haben KEIN Problem !

- **AVM - Fritz!Box** (es geht um 802.11w):
Wer möchte, kann das Feature schon jetzt ausprobieren über die FRITZ!Labor https://avm.de/fritz-labor/?pk_campaign=labor&pk_kwd=left, derzeit verfügbar für die FRITZ!Box 7490 und FRITZ!Box 7590.

Dieses Feature wird zeitnah, so die bisherige Planung, auch in FRITZ!OS-Versionen für andere aktuelle FRITZ!Box Modelle veröffentlicht werden.

- **c't - Redakteur:**
Solange die WLAN-Nutzer aber die insbesondere in öffentlichen Hotspots üblichen Vorsichtsmaßnahmen walten lassen (nur TLS-geschützte Dienste verwenden, Zertifikatswarnungen ernst nehmen, idealerweise ein VPN verwenden), fallen der Deauther und verwandte Tools für mich eher unter die Kategorie WLAN-Vandalismus statt Angriffswerkzeug.

Technischer Hintergrund

- **IEEE 802.11 ist der Protokoll-Standard für WiFi-Verbindungen**
- **Management-Frames dienen dem Auf- und Abbau einer Verbindung**
- **sie werden unverschlüsselt akzeptiert**
- **damit ist dies ein weit offenes Tor für Angriffe bzw. Sabotage**

Das Funktions-Prinzip von Deauth

- **WLAN-Adapter im Monitoring-Modus**
- **Scannen nach APs und Clients**
- **Erfassen von MAC-Adresse, SSID und Kanal (auch hidden SSID)**
- **Bilden des Deauth-Strings**
- **Senden des Deauth-Paketes**
- **ständige Wiederholung**

Was ist mit 5 GHz WLAN ?

- **Aircrack-NG nur für 2.4 GHz**
- **Kaum geeignete WLAN-Adapter (Monitoring Modus)**
- **bisher keine IoT-Hardware (ESP)**

Gründe:

- **geringere Reichweite**
- **noch wenig Verbreitung**

Alternative Hard- / Software

Hardware:

- **z.B. Google Nexus 5 (gerootet)**
- **Raspberry Pi (nexmon)**

Software:

- **Kali-Linux (NetHunter für Android)**
- **Aircrack-NG (v1.2-rc3 vom 14.02.2016)**
- **Hijacker / Nexmon (Apps für Android)**

Erkennungsmöglichkeiten

- **WiFi-Sniffer (z.B. Wireshark, Airodump)**
- **WiFi-Scanner (z.B. Acrylic Wi-Fi)**

Unsere Projekte:

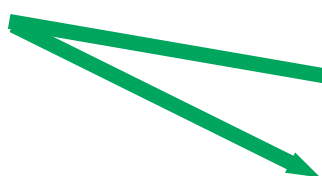
- **DeauthDetector (Spacehuhn)**
- **PacketMonitor32 (Spacehuhn)**
- **Deauth Locator (schinfo)**

Beispiel: Aircrack-NG

AP erkannt



deauth



„Vodafone Problem“

SSID immer gleich!

```
CH 3 ][ Elapsed: 3 mins ][ 2017-04-18 12:32 ][ WPA handshake: C8:0E:14:...
```

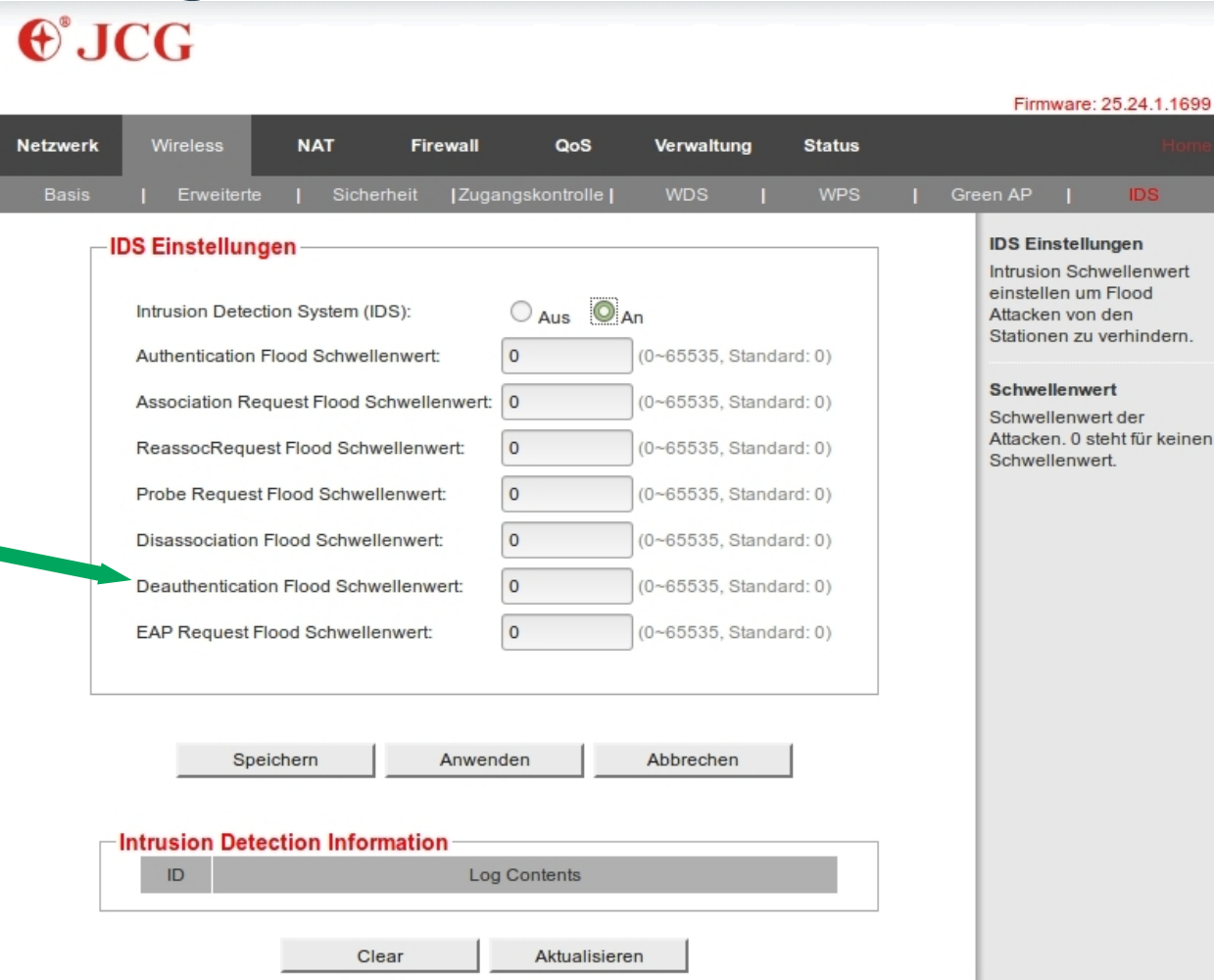
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
C8:0E:14:...	-20	1723	12115 26	1	54e.	WPA2	CCMP	PSK	schinfo
F4:F2:6D:...	-48	1	0 0	6	54e.	WPA2	CCMP	PSK	schinfoT
BC:14:01:...	-61	6	0 0	11	54e	WPA2	CCMP	PSK	HITRON-AC50
BC:14:01:...	-62	6	0 0	11	54e	OPN			Vodafone Hotspot
70:5A:0F:...	-63	0	0 0	-1	-1				<length: 0>
E0:28:6D:...	-63	0	0 0	-1	-1				<length: 0>
BC:14:01:...	-63	5	0 0	11	54e	OPN			Vodafone Homespot
4A:0E:14:...	-63	0	0 0	-1	-1				<length: 0>
50:7E:5D:...	-64	0	0 0	-1	-1				<length: 0>
54:67:51:...	-64	0	0 0	-1	-1				<length: 0>
3A:0E:14:...	-64	0	0 0	-1	-1				<length: 0>
BC:05:43:...	-64	0	0 0	-1	-1				<length: 0>
C0:25:06:...	-64	0	0 0	-1	-1				<length: 0>
08:96:D7:...	-64	0	0 0	-1	-1				<length: 0>
84:94:8C:...	-64	0	0 0	-1	-1				<length: 0>
BC:14:01:...	-64	1	0 0	1	54e	WPA2	CCMP	PSK	HITRON
84:94:8C:...	-64	0	0 0	-1	-1				<length: 0>
24:65:11:...	-64	0	0 0	-1	-1				<length: 0>
BC:05:43:...	-65	0	0 0	-1	-1				<length: 0>
04:35:3B:...	-65	0	0 0	-1	-1				<length: 0>
DC:53:7C:...	-65	0	0 0	-1	-1				<length: 0>
84:94:8C:...	-65	0	0 0	-1	-1				<length: 0>
C8:0E:14:...	-65	0	0 0	-1	-1				<length: 0>
BC:14:01:...	-65	58	0 0	1	54e	OPN			Vodafone Hotspot
46:67:51:...	-72	0	0 0	-1	-1				<length: 0>
54:67:51:...	-73	0	0 0	-1	-1				<length: 0>
C8:0E:14:...	-78	0	0 0	13	54e.	WPA2	CCMP	PSK	FRITZ!Box 6490 Cable
3A:0E:14:...	-78	3	0 0	13	54e.	OPN			Vodafone Hotspot
4A:0E:14:...	-80	0	0 0	13	54e.	OPN			Vodafone Homespot
BC:14:01:...	-81	59	0 0	1	54e	OPN			Vodafone Homespot
BC:14:01:...	-85	84	1 0	1	54e	WPA2	CCMP	PSK	HITRON
00:1E:2A:...	-88	2	0 0	13	54e	WPA2	CCMP	PSK	NETGEAR
5C:DC:96:...	-89	87	0 0	1	54e	WPA2	CCMP	PSK	WLAN

Deauth-Angriffe wie verhindern?

- **Einsatz von IEEE 802.11w-2009**
- **Deauth-Frames ignorieren (nur AP)**
- **bisher leider kaum vorhanden bzw. genutzt !!!**
- **Verbieten hilft nicht !!!**

Beispiel: JCG

- Einstellmöglichkeit in der Firmware



The screenshot displays the JCG router's web-based configuration interface. At the top, the JCG logo is visible on the left, and the firmware version 'Firmware: 25.24.1.1699' is on the right. A navigation bar contains tabs for 'Netzwerk', 'Wireless', 'NAT', 'Firewall', 'QoS', 'Verwaltung', and 'Status'. Below this, a secondary bar shows sub-menus: 'Basis', 'Erweiterte', 'Sicherheit', 'Zugangskontrolle', 'WDS', 'WPS', 'Green AP', and 'IDS' (which is highlighted in red). The main content area is titled 'IDS Einstellungen' in red. It features a section for 'Intrusion Detection System (IDS):' with radio buttons for 'Aus' and 'An' (the 'An' option is selected). Below this are seven rows, each with a label and a numeric input field set to '0': 'Authentication Flood Schwellenwert', 'Association Request Flood Schwellenwert', 'ReassocRequest Flood Schwellenwert', 'Probe Request Flood Schwellenwert', 'Disassociation Flood Schwellenwert', 'Deauthentication Flood Schwellenwert' (highlighted by a green arrow), and 'EAP Request Flood Schwellenwert'. Each input field has a range '(0~65535, Standard: 0)' to its right. At the bottom of this section are three buttons: 'Speichern', 'Anwenden', and 'Abbrechen'. Below the main settings is a section titled 'Intrusion Detection Information' containing a table with two columns: 'ID' and 'Log Contents'. At the very bottom are 'Clear' and 'Aktualisieren' buttons. On the right side of the interface, a sidebar provides additional information under the heading 'IDS Einstellungen', explaining that the 'Intrusion Schwellenwert' is used to prevent flood attacks and that '0' represents no threshold.

IDS Einstellungen

Intrusion Detection System (IDS): ☐ Aus ☒ An

Authentication Flood Schwellenwert: (0~65535, Standard: 0)

Association Request Flood Schwellenwert: (0~65535, Standard: 0)

ReassocRequest Flood Schwellenwert: (0~65535, Standard: 0)

Probe Request Flood Schwellenwert: (0~65535, Standard: 0)

Disassociation Flood Schwellenwert: (0~65535, Standard: 0)

Deauthentication Flood Schwellenwert: (0~65535, Standard: 0)

EAP Request Flood Schwellenwert: (0~65535, Standard: 0)

Speichern Anwenden Abbrechen

Intrusion Detection Information

ID	Log Contents
----	--------------

Clear Aktualisieren

IDS Einstellungen

Intrusion Schwellenwert einstellen um Flood Attacken von den Stationen zu verhindern.

Schwellenwert

Schwellenwert der Attacken. 0 steht für keinen Schwellenwert.

Beispiel: Windows

• Einsatz von PMF (802.11w)

Logische WLAN-Netzwerke (SSIDs) - Neuer Eintrag

☒ Logisches WLAN-Netzwerk aktiviert

Name:

Vererbung
Erbt Werte von Eintrag:

Netzwerk-Name (SSID):

SSID verbinden mit:

VLAN-Betriebsart:

VLAN-ID:

Verschlüsselung:

Schlüssel 1/Passphrase: ☐ Anzeigen

RADIUS-Profil:

Zulässige Freq.-Bänder:

Autarker Weiterbetrieb: Minuten

802.11u-Netzwerk-Profil:

☐ OKC (Opportunistic Key Caching) aktiviert

☐ MAC-Prüfung aktiviert

SSID-Broad. unterdrücken:

☐ RADIUS-Accounting aktiviert

☒ Datenverkehr zulassen zwischen Stationen dieser SSID

WPA-Version:

WPA1 Sitzungsschl.-Typ:

WPA2 Sitzungsschl.-Typ:

WPA2 Key Management:

Basis-Geschwindigkeit:

Client-Bridge-Unterst.:

Maximalzahl der Clients:

Min. Client-Signal-Stärke: %

☐ Lange Präambel bei 802.11b verwenden

☐ (U-)APSD / WMM-Powersave aktiviert

Mgmt.-Frames verschlüsseln: 

802.11n

Max. Spatial-Streams:

☒ Kurzes Guard-Intervall zulassen

☒ Frame-Aggregation verwenden

☒ STBC (Space Time Block Coding) aktiviert

☒ LDPC (Low Density Parity Check) aktiviert

LANmonitor

Datei Gerät Ansicht Extras ?

QuickFinder...

WAN-Verbindungen: Keine

Wireless LAN

WLAN - 1

WLAN - 2

Netzwerk 1 (SSID): PMF-Test; 802.11g/b/n (gemischt)

Client: 24:77:03:09:b4:03 (Intel Corporate)

IP-Adresse: 192.168.1.97

Senderate: 130 MBit/s

Empfangsrate: 217 MBit/s

Signalstärke: 100 %

Durchsatz: 2,9 KByte/s

Kanalbandbreiten: 20 MHz

WPA-Version: 2

Schlüsseltyp: AES-CCM

Protected-Management-Frames: Ja 

IPv6-Firewall: 04/27/2014 13:37:59 DENY-ALL (inbound) - Paket zurückgewiesen

IPv4-Firewall: Aktiv

Lokale Netzwerke

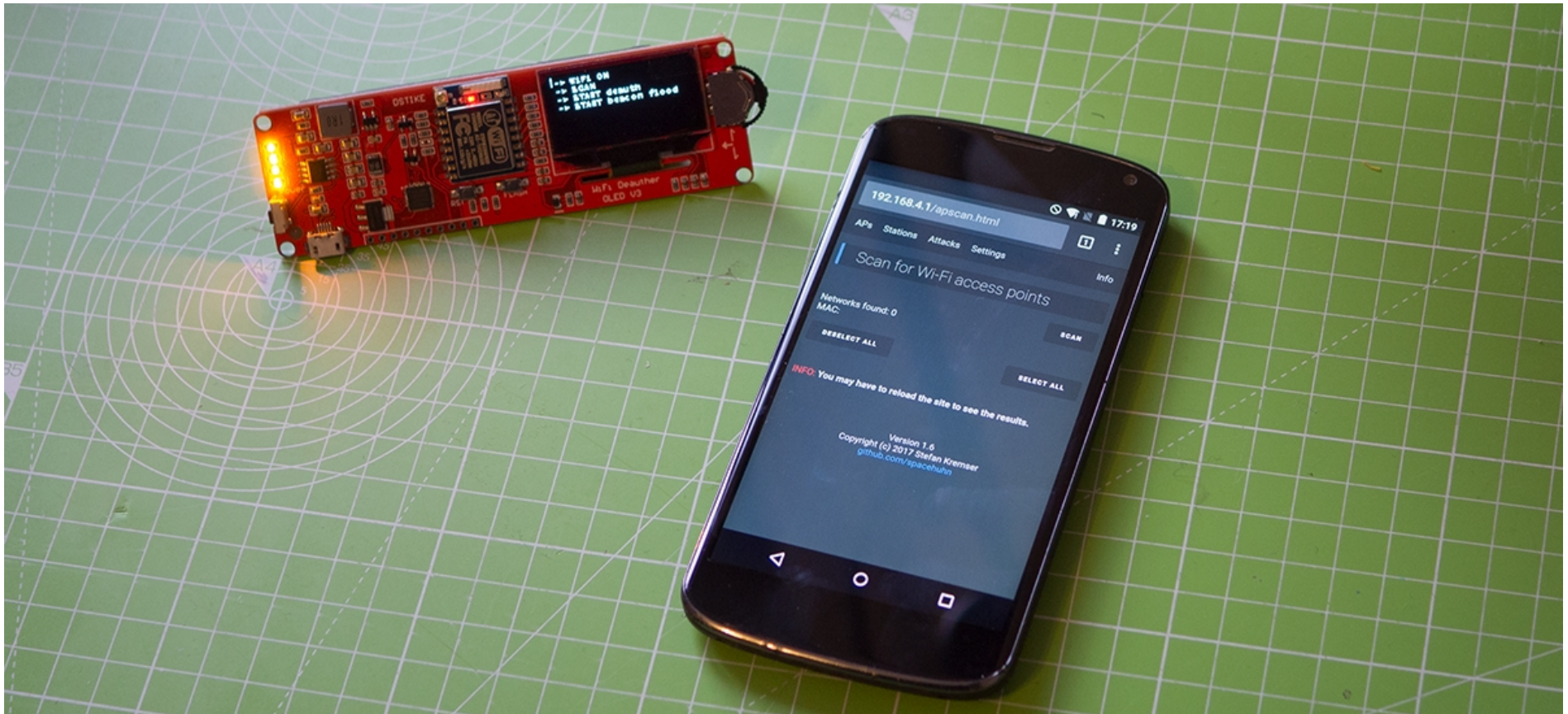
DHCP-Server: Inaktiv

Budget

System-Informationen

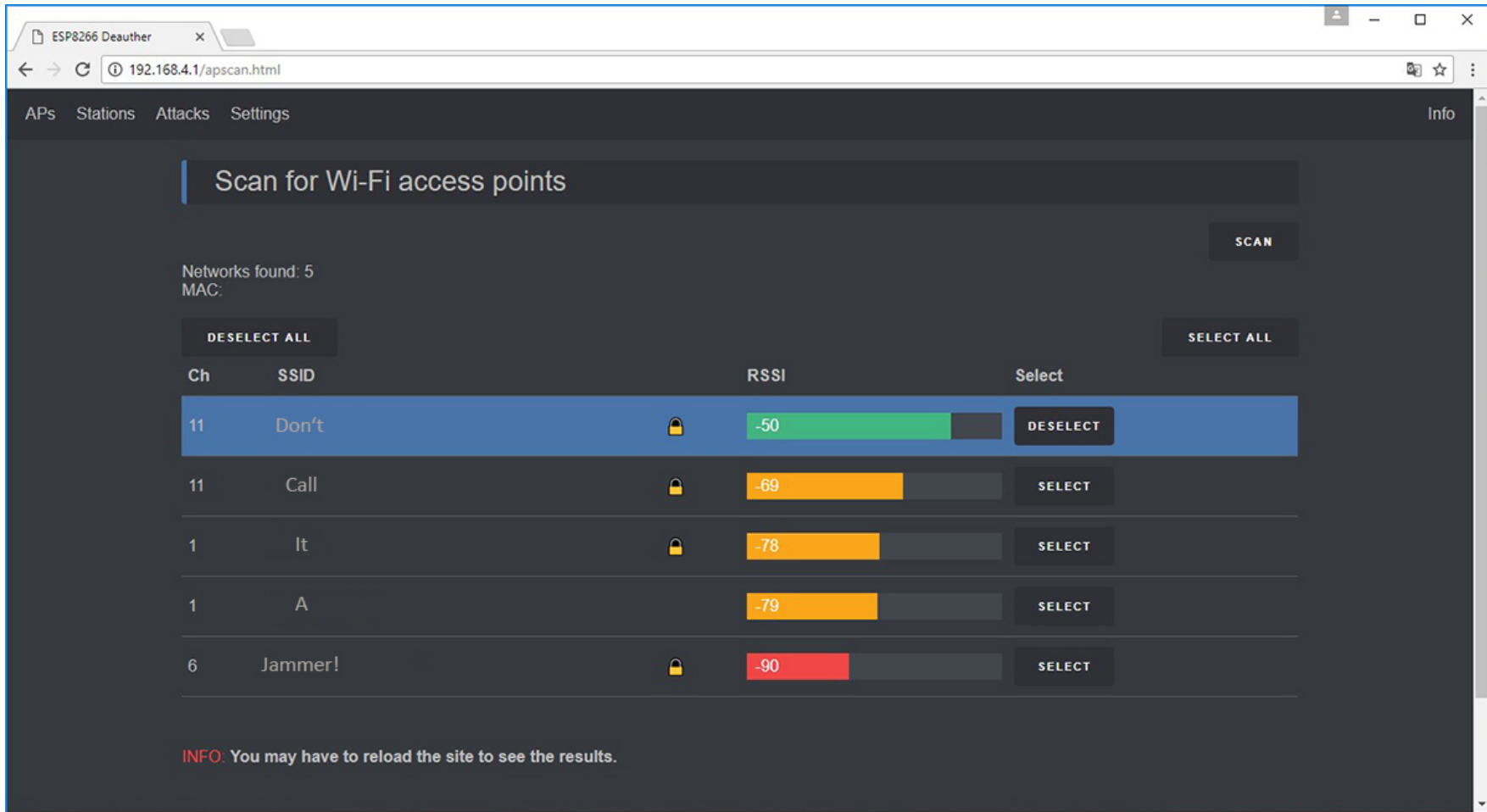
ESP8266 Deauther

- von Stefan Kremser (Spacehuhn)



ESP8266 Deauther - WEB-Interface

- Scan-Mode für Access-Points



ESP8266 Deauther

192.168.4.1/apscan.html

APs Stations Attacks Settings Info

Scan for Wi-Fi access points

SCAN

Networks found: 5
MAC:

DESELECT ALL SELECT ALL

Ch	SSID		RSSI	Select
11	Don't		-50	DESELECT
11	Call		-69	SELECT
1	It		-78	SELECT
1	A		-79	SELECT
6	Jammer!		-90	SELECT

INFO: You may have to reload the site to see the results.

ESP8266 Deauther - WEB-Interface

- Scan-Mode für Clients

ESP8266 Deauther

192.168.4.1/stations.html

APs Stations Attacks Settings Info

Scan for Wi-Fi Stations

Scan time: 15 s **START**

The access point will be unavailable while scanning and you may have to reconnect!

Stations found: 4

DESELECT ALL **SELECT ALL**

Pkts	Name	MAC	AP	Select
12	set	MurataMa:00:00:00	der-link	SELECT
11	set	Tp-LinkT:00:00:00	der-link	SELECT
6	Phone	Htc:00:00:00	der-link	DESELECT
0	set	LgElectr:00:00:00	?	SELECT

Saved stations: 1/50

ESP8266 Deauther - WEB-Interface

- **Attack-Mode**

The screenshot shows the web interface of an ESP8266 Deauther in Attack-Mode. The browser address bar shows the URL `192.168.4.1/attack.html`. The interface has a dark theme with a navigation bar at the top containing links for **APs**, **Stations**, **Attacks** (which is active), and **Settings**. An **Info** link is also present in the top right corner.

Under the **Attacks** section, there is a **Selected AP(s):** field with a **CLONE** button next to it. Below this, a warning message says "• Just please don't ok?". The **Selected Station(s):** field shows a list of stations, including `n0:j4:mm:3r Htc - Phone`.

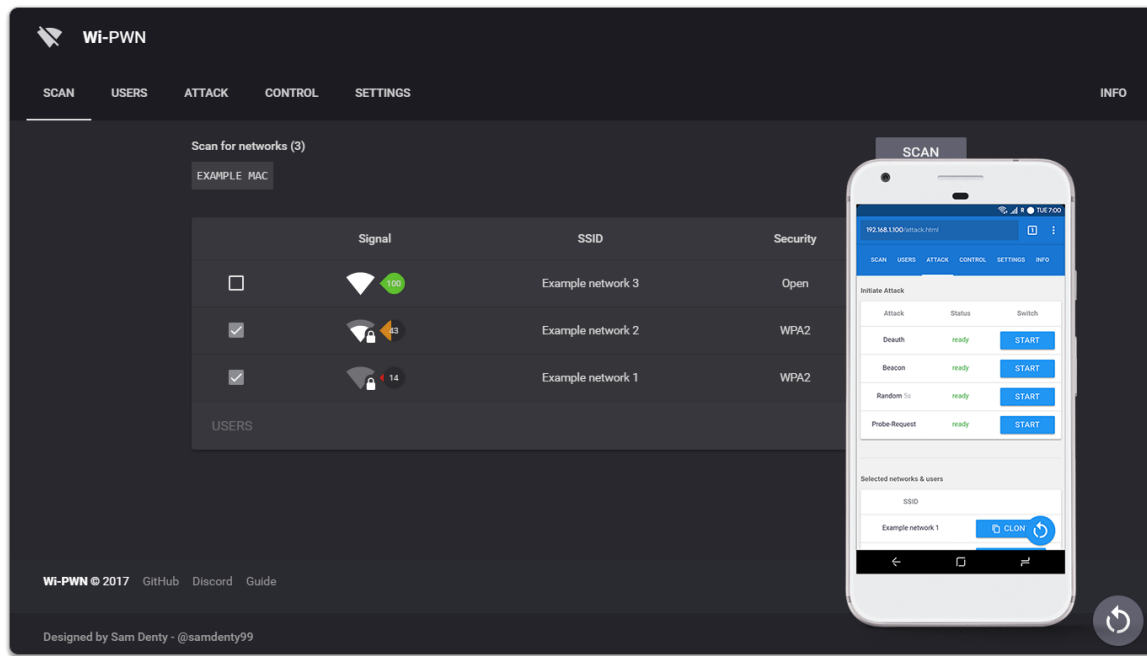
A table displays the available attack types:

Attack	Status	Start/Stop
Deauth	ready	START
Beacon	ready	START
Probe-Request	ready	START

At the bottom of the interface, there is a timer set to **5** seconds and an **ENABLE RANDOM** button.

ESP8266 Deauther - WEB-Interface

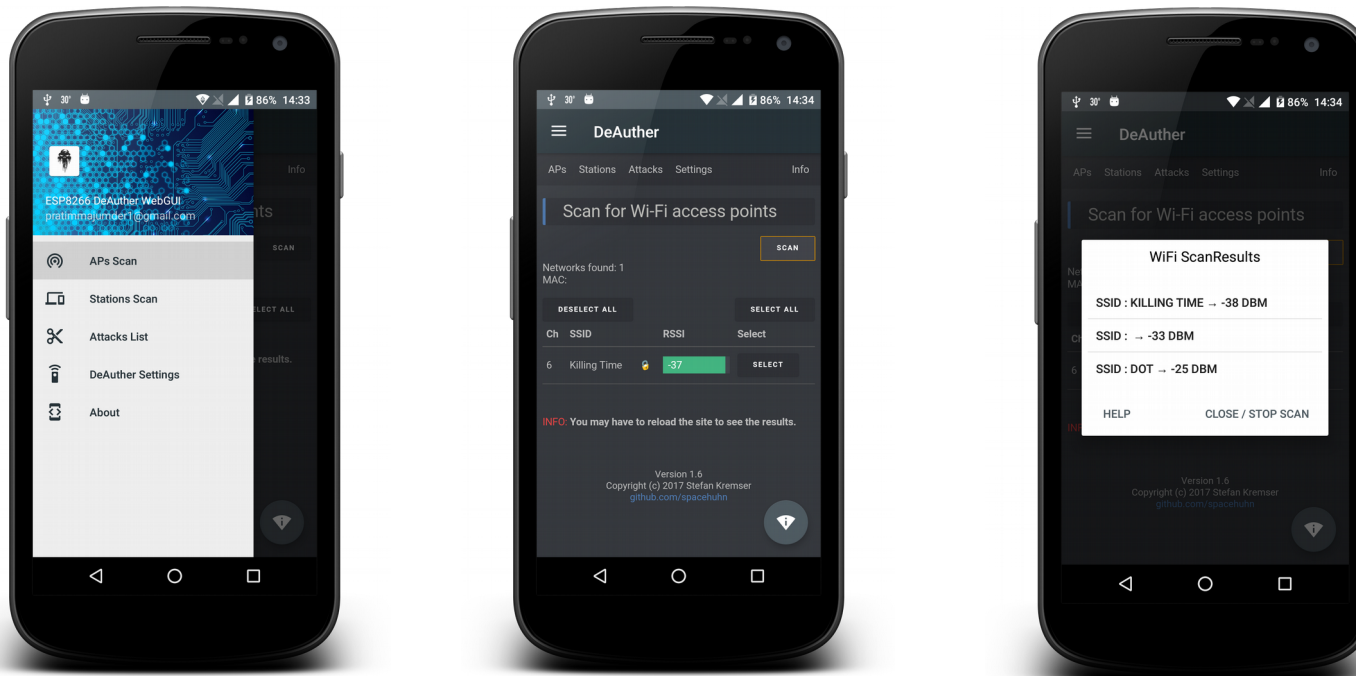
- Alternativen:



- **Wi-PWN - @samdenty99**
- **<https://github.com/samdenty99/Wi-PWN>**
- **<https://play.google.com/store/apps/details?id=samdd.wipwn>**

ESP8266 Deauther - WEB-Interface

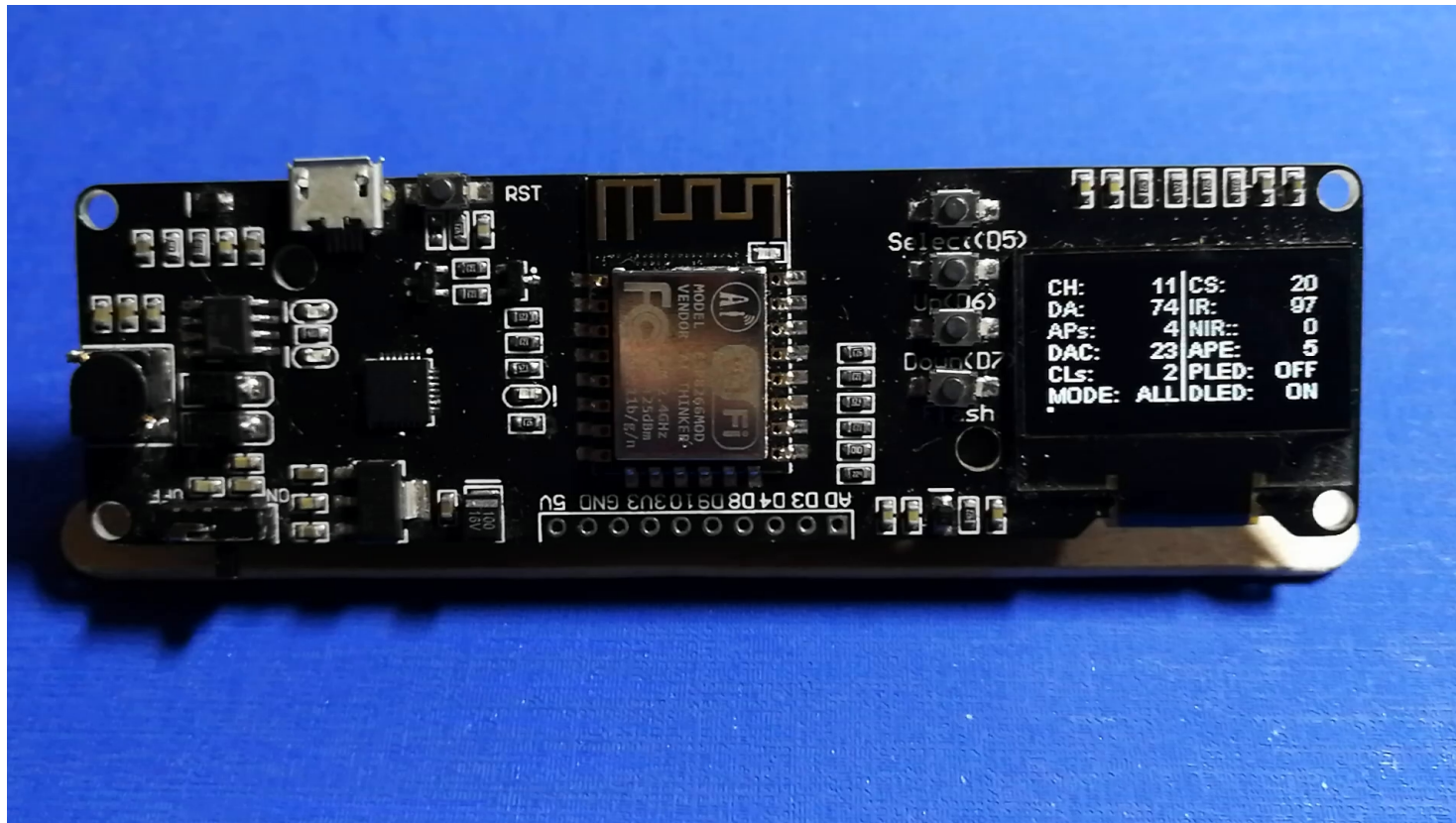
- **Alternativen:**



- **DeAutherDroid Android APP - @ExploitR**
- **<https://github.com/ExploitR/DeAutherDroid>**

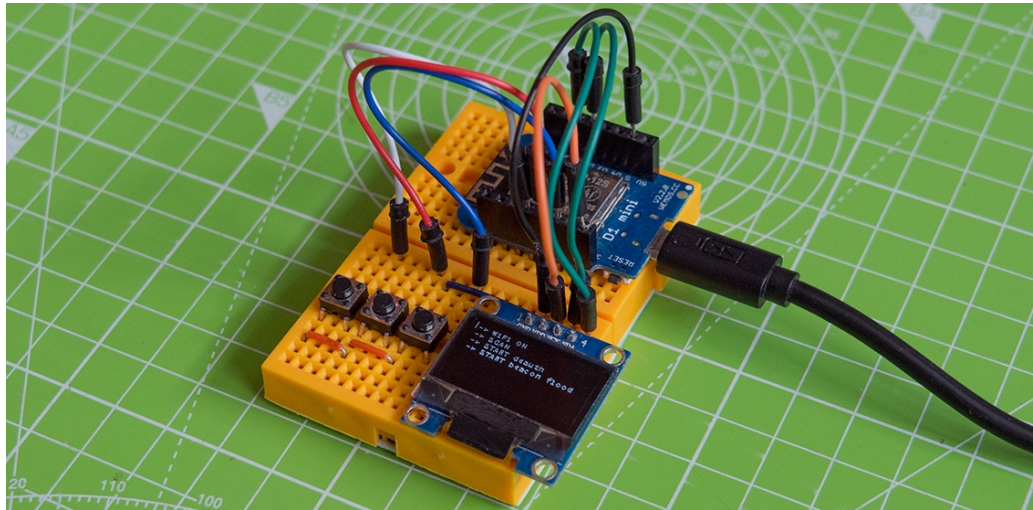
DeAuth-All-OLED

- **NICHT frei verfügbar !!!**
- **Alle 14 Kanäle in 1 Sekunde !!!**



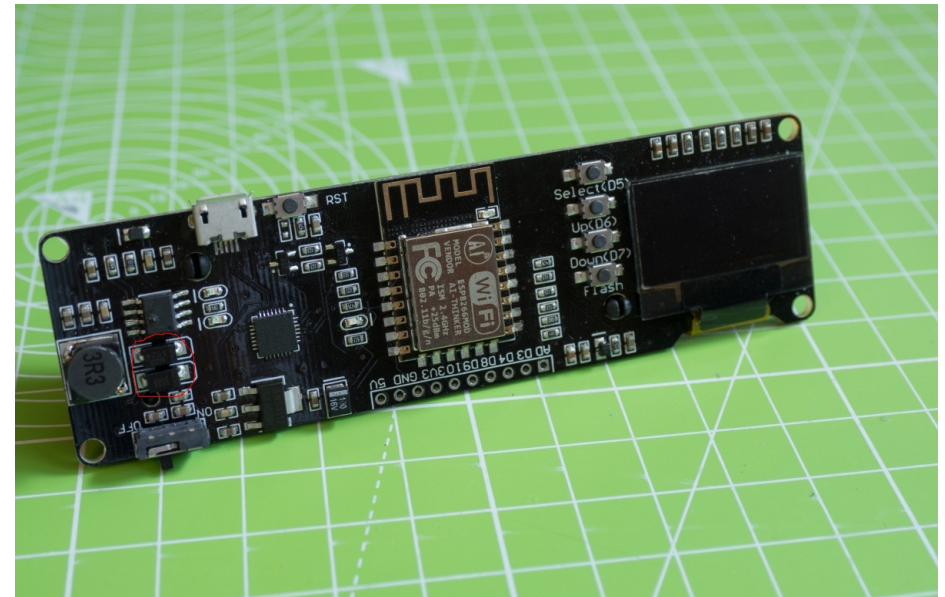
Hardware Entwicklung

- **Erste Versuche und Versionen**



Versuchsaufbau mit OLED

WiFi deauther OLED v1.0 und 1.5
(waren wirklich „heiße“ Teile 😊)



ESP8266 - Module

ESP-01
512KB/1MB



ESP-07
1MB

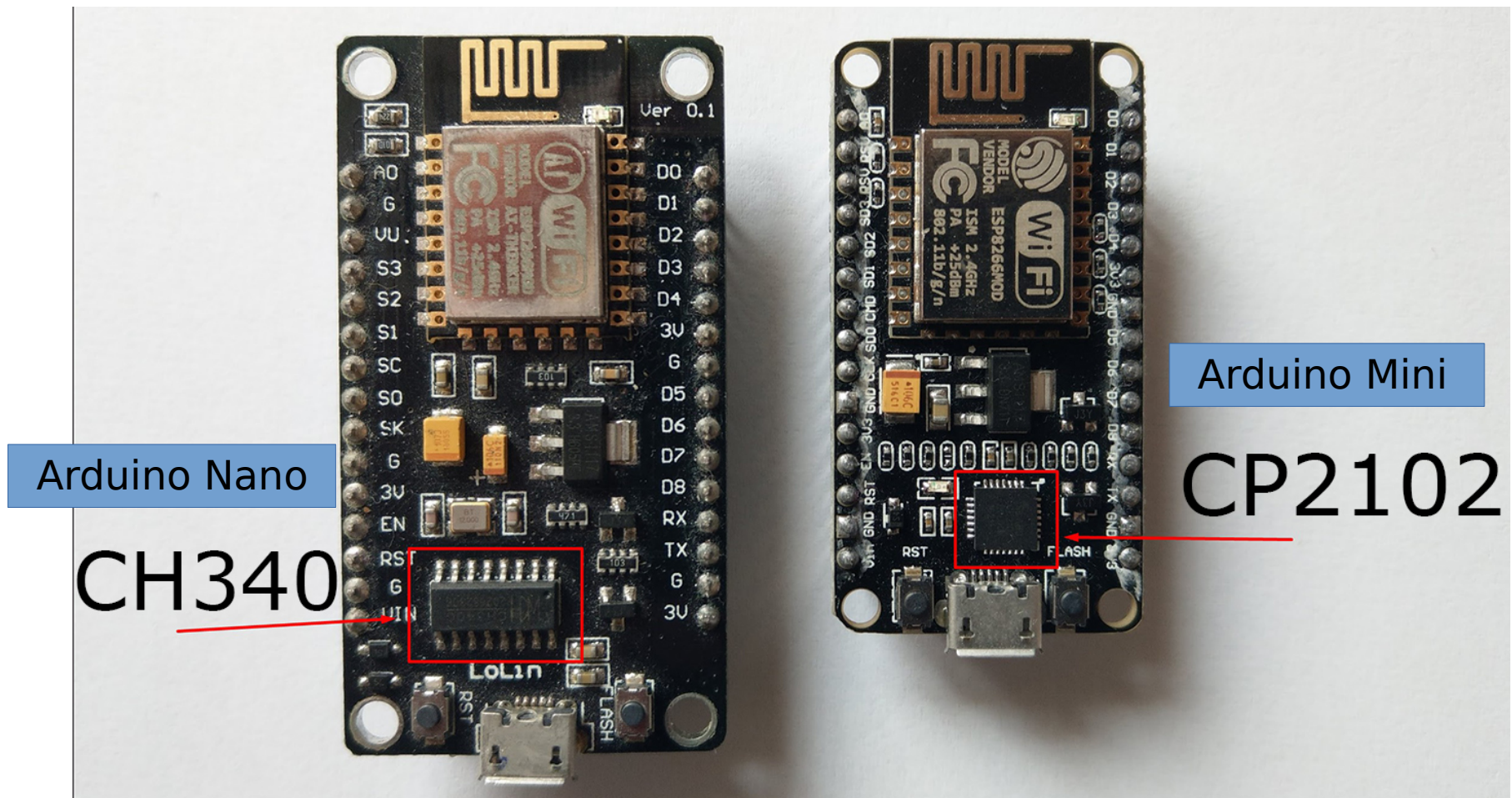


ESP-12
4MB



ESP8266 - NodeMCU

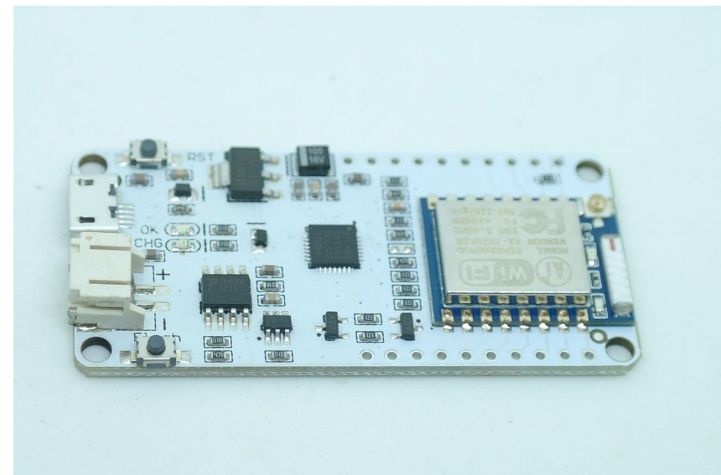
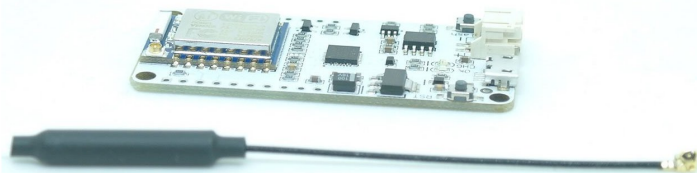
- **Achtung - Unterschiede**



NodeMCU-07

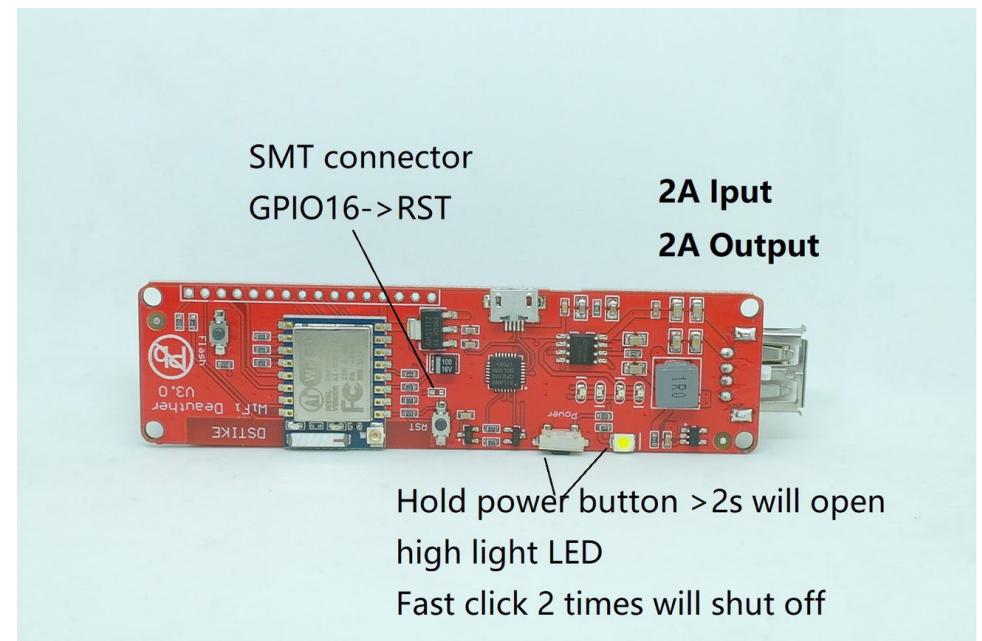
- **ESP-07**
(On-Board Keramikantenne und U.FL „Pigtail“ Anschluss für eine externe Antenne.)
- **WiFi deauther Pre-flashed**
- **Bedienung über WEB-Interface**
- **Akku-Anschluss mit Lader + Anzeige**

Product list:
NodeMCU-07 x1
Antenna x1



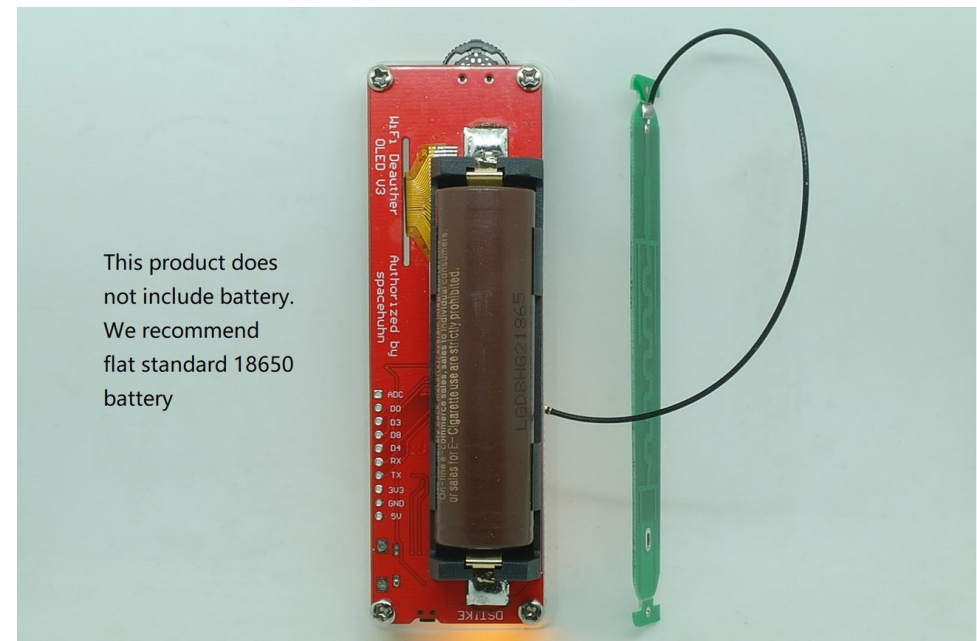
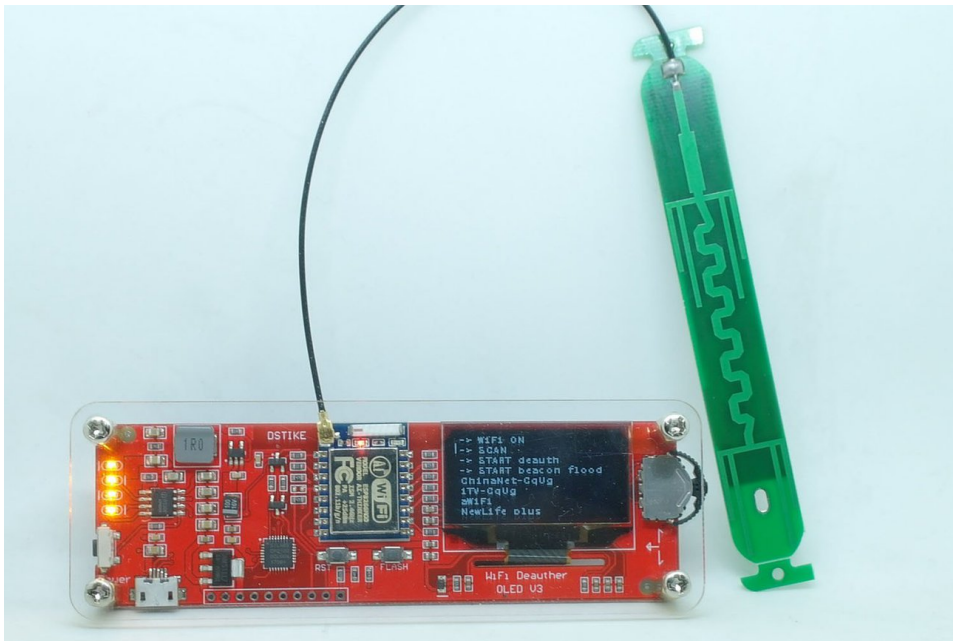
WiFi deauther V3

- **Pre-flashed**
- **2 dBi Antenne**
- **Bedienung über WEB-Interface**



WiFi deauther OLED V3

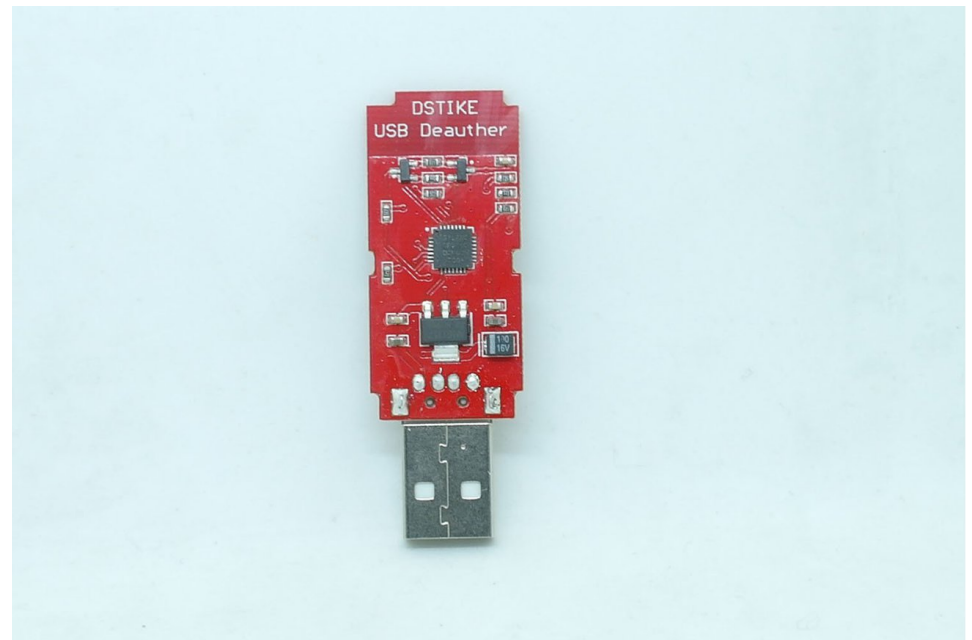
- **Pre-flashed**
- **Plexiglas-Case und 8 dBi Antenne**
- **Bedienung über OLED oder WEB-Interface**



This product does not include battery. We recommend flat standard 18650 battery

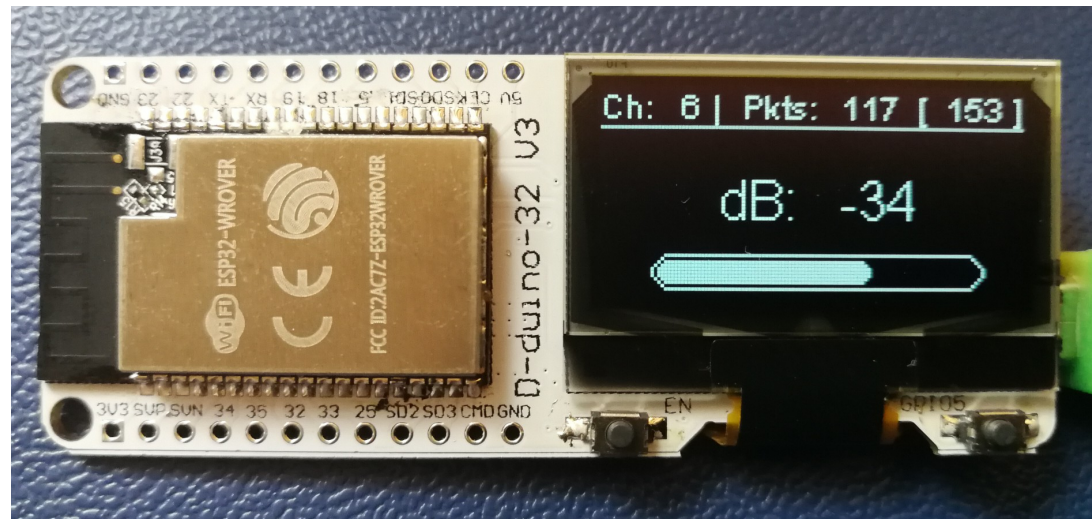
Deauth Detector

- **Pre-flashed**
- **zeigt WiFi-Deauth-Angriffe mit LED an**



Deauth Locator - der blitz

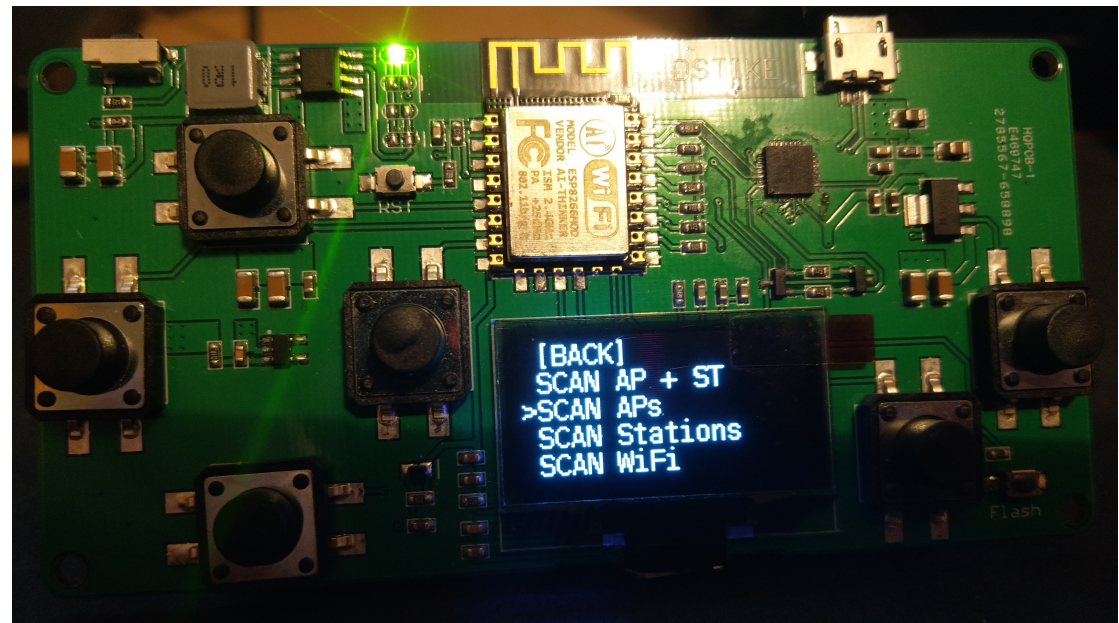
- momentan noch in der Entwicklung
- Lokalisierung mit Richtantenne
- geplante Verfügbarkeit von v1.0 in II/2018
- mit ESP32
- basiert auf PacketMonitor32
- v2.0 eventuell mit neuer Hardware



Ganz neu – bald erhältlich

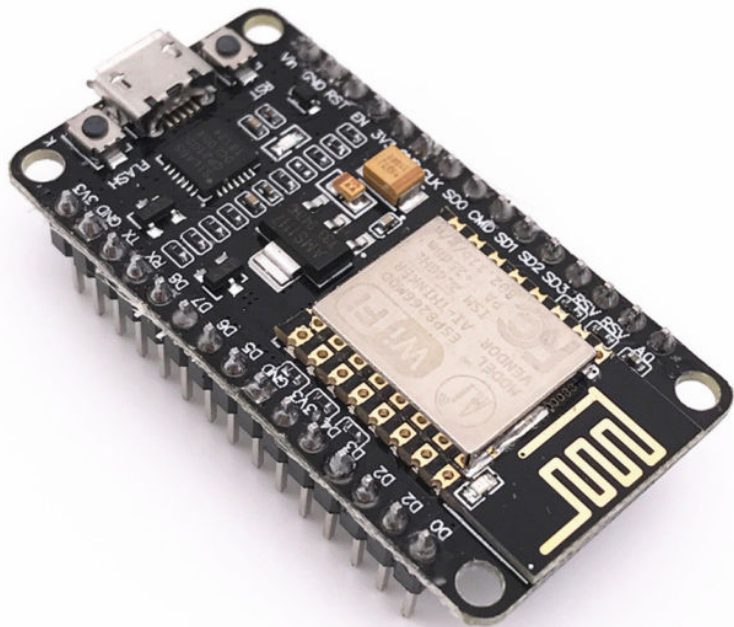
deauther2.0

- mit ausführlicher Anleitung (Wiki)
- All in One
- Scripts möglich
- höhere Paket-Rate
- eigene Hardware
- Befehle über COM
- individuell Settings
- geplant für Anfang II/2018



Das ist KEIN Jammer !!!

NodeMCU Deauther



DAS ist ein Jammer



Vorsicht! - Trittbrettfahrer

 Stöbern in Kategorien

Was suchen Sie?

Alle Kategorien

Finden

Erweiterte Suche

[Zurück zu den Suchergebnissen](#) | Kategorie: [Business & Industrie](#) > [Elektronik & Messtechnik](#) > [Elektronische Bauelemente](#) > [Halbleiter & Aktive Elemente](#) > [Platinen & Entwicklungskits](#)



Klicken, um das Bild zu vergrößern

Deauther Plug & Play WIFI WLAN Jammer NodeMCU Lua ESP8266 ESP-12E CH340G

🔥 1 Mal pro Stunde aufgerufen ★★★★★ Schreiben Sie die erste Rezension.

Artikelzustand: **Neu**

Stückzahl: 4 verfügbar
150 verkauft / Bewertung anzeigen

EUR 12,90
(inkl. MwSt.)

EUR 10,84
(exkl. MwSt.)

Sofort-Kaufen

In den Warenkorb

[Auf die Beobachtungsliste](#)

[Zur Kollektion hinzufügen](#)

100% Käuferzufriedenheit 150 verkauft Über 96% verkauft

Abholung: Lieferung an Abholstation möglich

Versand: **KOSTENLOS** Sparversand | [Weitere Details](#)
Artikelstandort:  Deutschland
Versand nach: Deutschland [Ausschlussliste anzeigen](#)

Lieferung: Zwischen **Do, 1. Mrz. und Sa, 3. Mrz.** bei heutigem Zahlungseingang

Zahlungen: **PayPal**, Lastschrift, Kreditkarte | [Weitere Zahlungsmethoden](#)

Rücknahmen: Verbraucher können den Artikel zu den unten angegebenen Bedingungen zurückgeben | [Weitere Details](#)

Sicherheit: **ebay KÄUFERSCHUTZ** | [Weitere Details](#)

 Auf die Beobachtungsliste

eBay-Garantie

- 1 Monat Widerrufsrecht
- Geld zurück – falls Artikel nicht erhalten oder nicht wie beschrieben (Käuferschutz)
- eBay-geprüfter Händler

Ein Service-Versprechen von eBay. Gesetzliche Rechte des Verbrauchers bleiben unberührt.
[Garantiebedingungen.](#)

Angaben zum Verkäufer

 (9972 ★)

100% Positive Bewertungen

Angemeldet als gewerblicher Verkäufer

[Diesen Verkäufer speichern](#)

[Andere Artikel aufrufen](#)

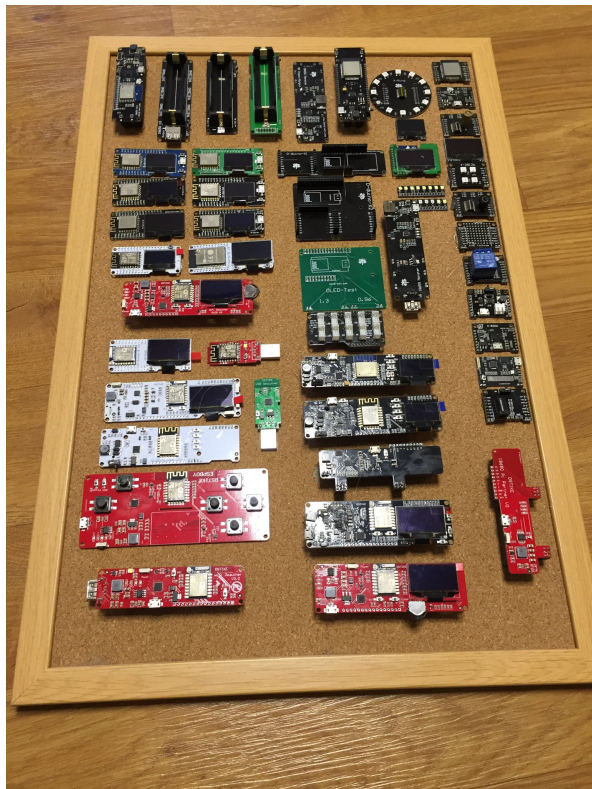
[Verkäufer kontaktieren](#)

Shop besuchen: 

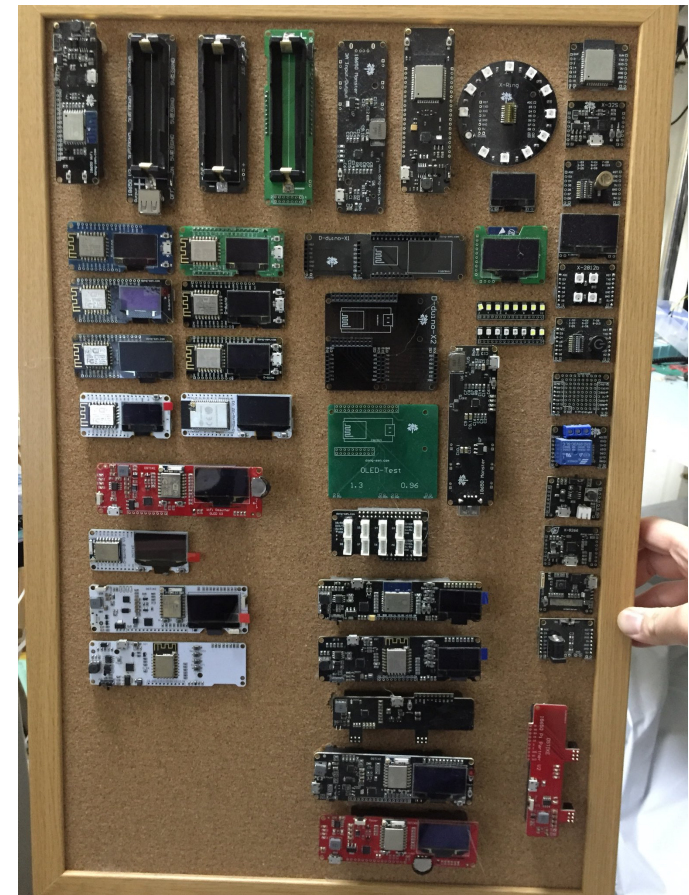
Das Original – nur von Travis Lin

Unser Hardware-Entwickler

- <https://twitter.com/dongsentech>



DSTIKE



Weiterführende Links

- <https://www.schinfo.de>
- <https://github.com/schinfo>
- <https://twitter.com/schinfo>

- <https://spacehuhn.com>
- <https://github.com/spacehuhn>
- <https://twitter.com/spacehuhn>
- <https://www.youtube.com/channel/UCFmjA6dnjv-phqrFACyl8tw>

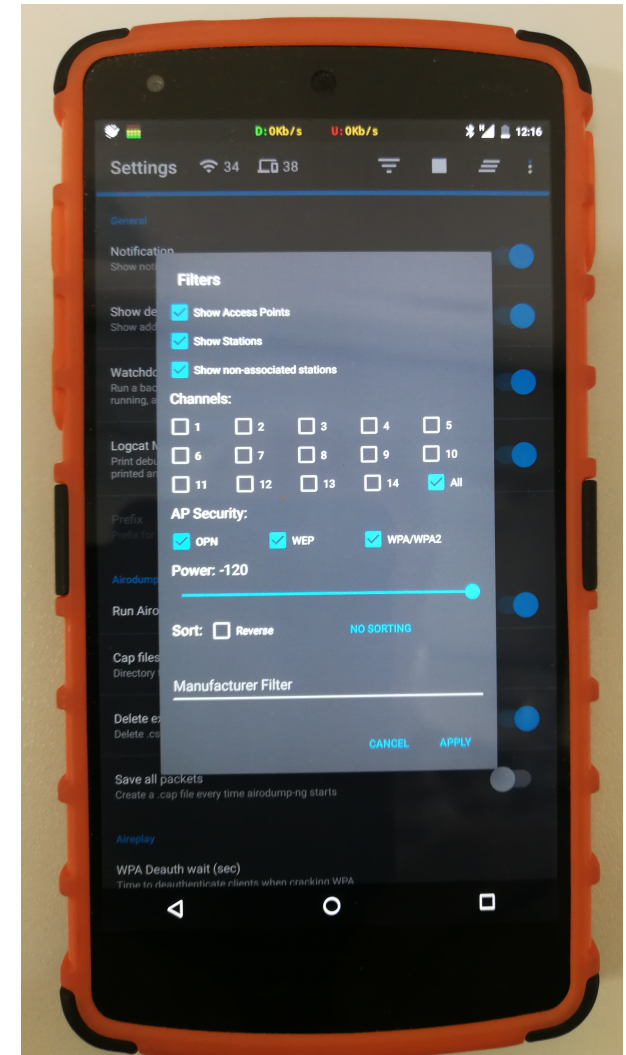
Hardware (Original) NUR erhältlich über:

DSTIKE (Travis Lin)

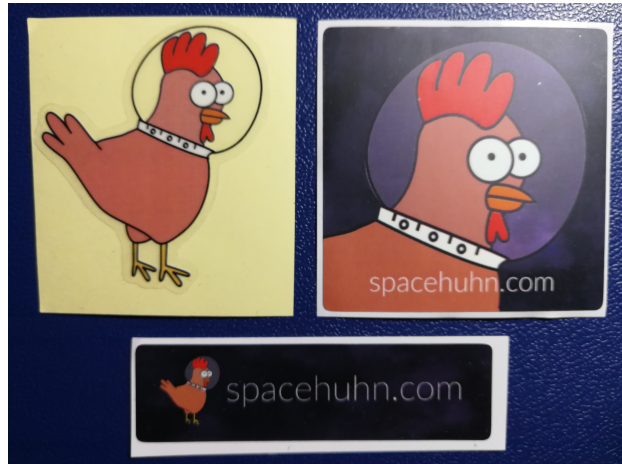
<https://www.tindie.com/stores/lspoplove>

Hijacker auf dem Google Nexus 5

- **DAS Tool für die Hosentasche**
- **Hijacker**
 - Airodump-NG
 - installiert Nexmon und Tools automatisch
- **Nexus 5 kann als einziges Gerät Monitoring-Mode + Packet Injektion**
- **leider nur noch gebraucht erhältlich**
- **nicht mit Nexus 5X verwechseln !!!**
- **<https://github.com/chrisk44/Hijacker>**



Infos und Sticker zum Mitnehmen



@schinfo

An "older than the internet" IT-Professional who is still looking for new and finds it too.
</schinfo.de>

DeauthChecker, ESP8266-DeAuth-All



@xdavidhu

Security researcher, hacker and coder.
</xdavidhu.me>

mitmAP, probeSniffer, KickThemOut, postSpider, lanGhost



@seytonic

I make tech related youtube videos specifically focused on DIY electronics and hacking.
</seytonic.com>

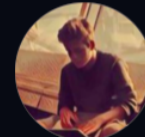
Malduino



@spacehuhn

Computer Science student that loves to experiment with WiFi to do fun stuff.
</spacehuhn.de>

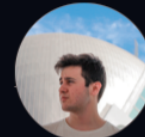
ESP8266 Deauther, PacketMonitor, WiFi Ducky, Arduino ARP Spoof, WiFi Keylogger, Deauth Detector



@nikolaskama

High-school student by day. Aspiring hacker by night.
</nikolaskama.me>

ONIOFF, KickThemOut, Terminals Are Sexy, Movies For Hackers



@deantonious

Computer Engineering student, software developer, gamer, maker and security researcher.
</deantonious.es>

hackOx, Requester, MrGather, MrFiler, Wifi Deauther Interface

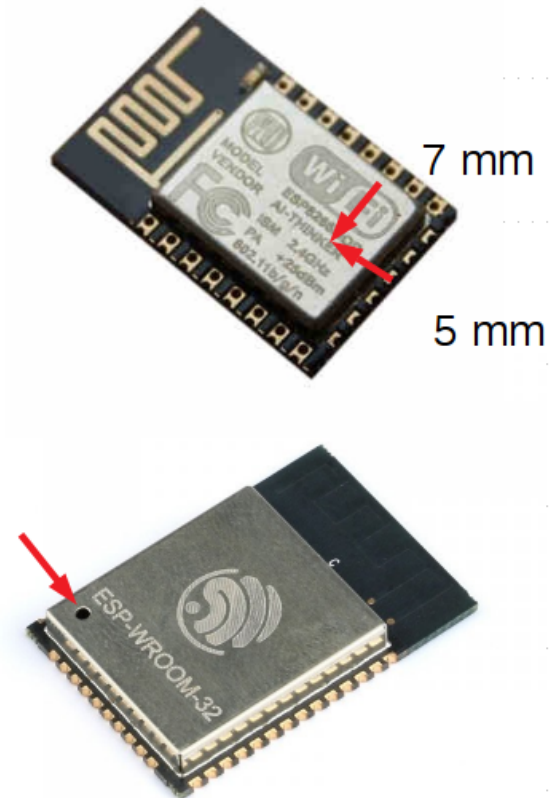
**Vielen Dank für Ihre
Aufmerksamkeit!**

Noch Fragen ?

... ah - Einen hab ich noch !

How to build a 3G/4G Deauther with ESP8266 / ESP32

- 1) You need a 1.5 mm drill
- 2) Drill a hole at the exact position:
for ESP8266
5 mm left from the upper right corner and 7 mm down
for ESP32
hole in the case already exist
- 3) You have to drill through the case (for ESP8266)
and the board,
you have only to drill through the board (for ESP32)
- 4) This opens the hidden shorting bridge that prevents
the 3G / 4G Deauth mode



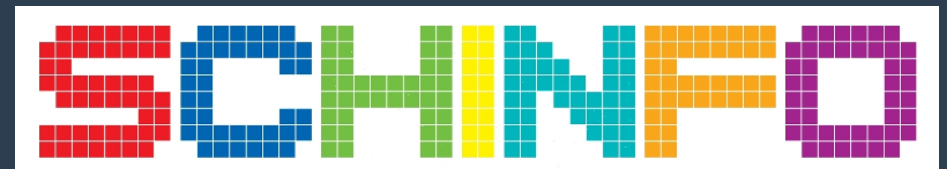
Now you have a full working 3G/4G Deauther !!!



2.4 GHz WLAN

- ganz sicher unsicher !

- Helmut Stult
- IT-Professional seit 1983
- <https://www.schinfo.de>



SCHINFO

Linux Mint Sponsor #61