Hacking toys ... and other things

Tobias Schrödel

Budapest // March 2nd, 2017

BSIDES BUDAPEST


MINI TANK
Wi Fi

Für größere Ansicht Maus über das Bild ziehen

GoolRC Neue Wifi Mini i-Spy RC Tank Car RC Ferngesteuerte Kamera Autos Happy Cow 777-270 mit 30W Pixel Camera Support iPhone iPad iPod Controller

von GoolRC

3 Kundenrezensionen | 11 beant

Hinweis: Dieser Artikel ist nur bei Drittanbietern erhält

Erhältlich bei diesen Anbietern.

1 neu ab EUR 47,99

Farbe: **grau**

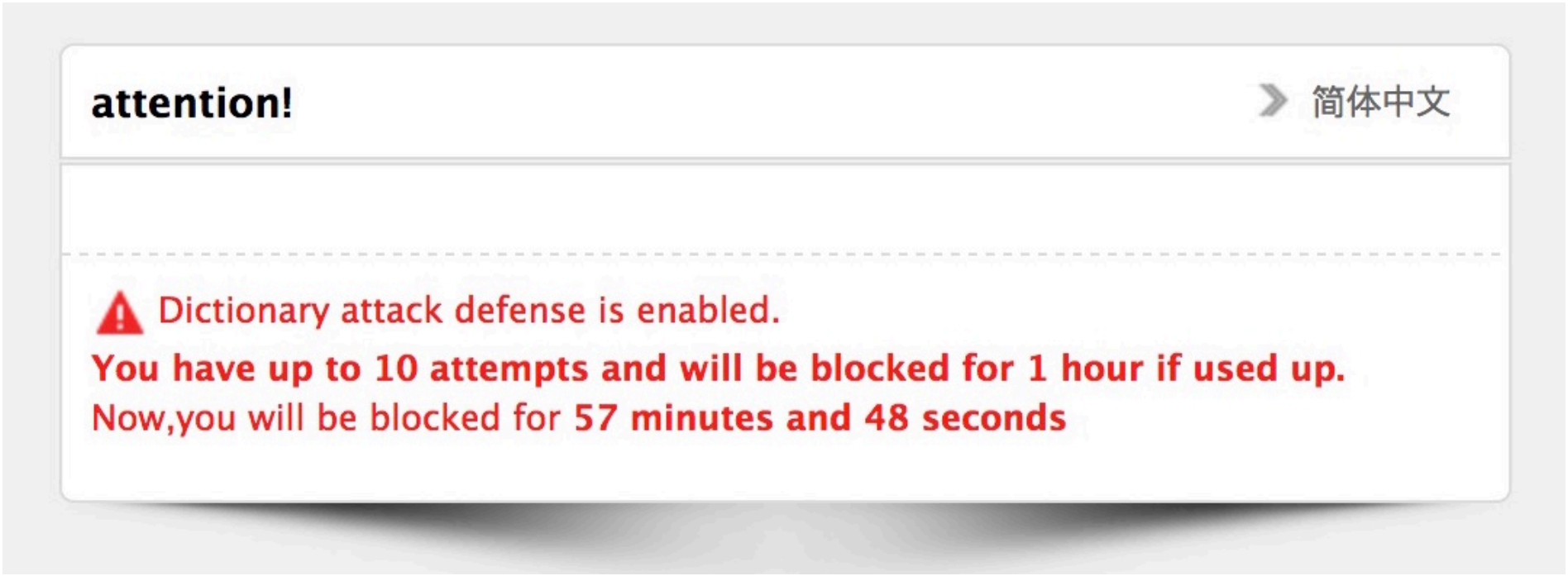
ab EUR 47,99 | ab EUR 47,99

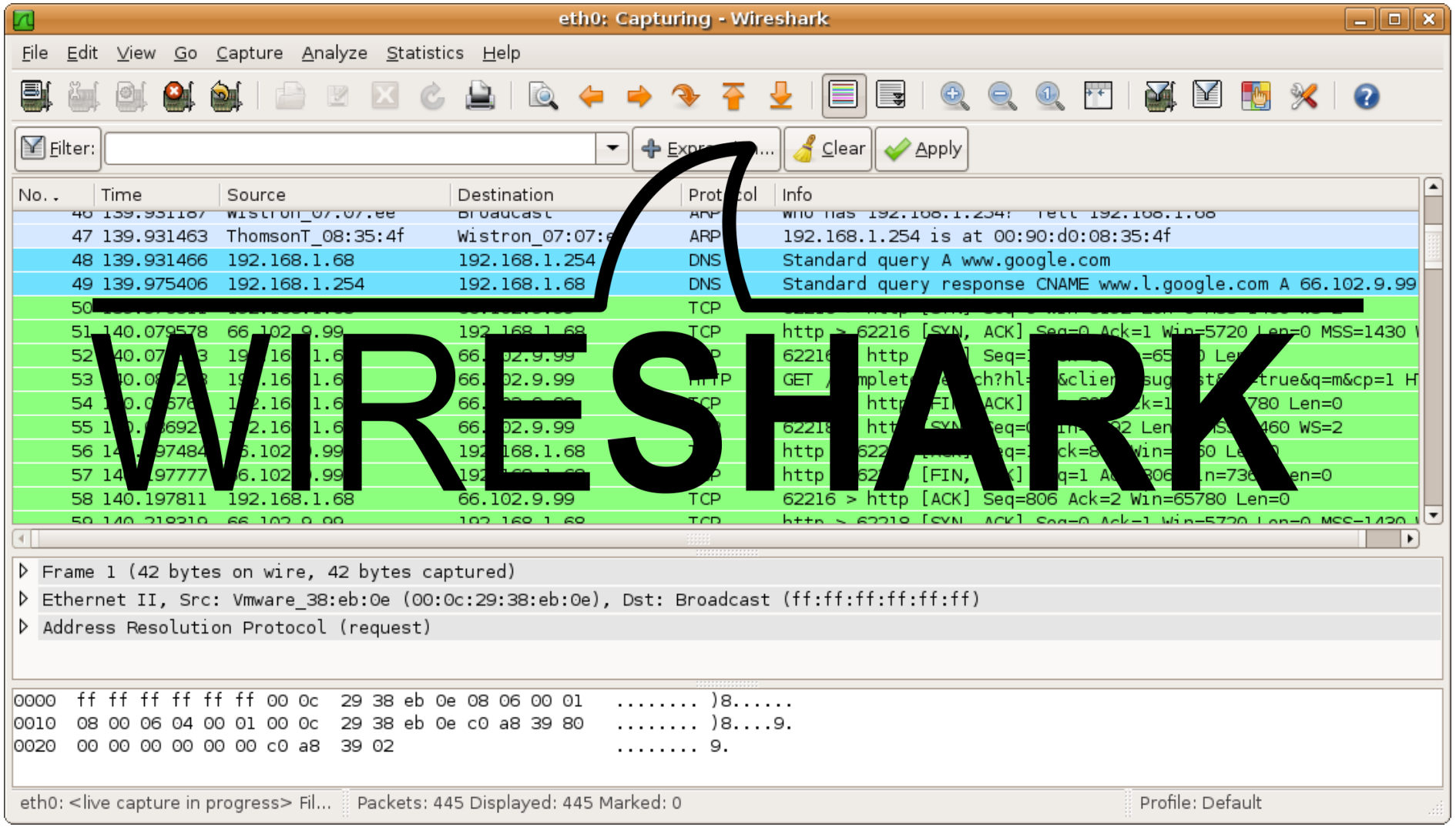
- kompaktes und leichtes Design.
- qualitativ hochwertige und langlebige Leistung.
- Happy Cow 777-270 Wifi RC Auto mit 0.3MP Kame
- Langdistanz-Fernbedienung & flexible Bewegung ko
- Kontrolle durch Wi-Fi, können 18-Meter lange Strecl

Möchten Sie Ihr Elektro- und Elektronik-Gerät kostenlos recyce

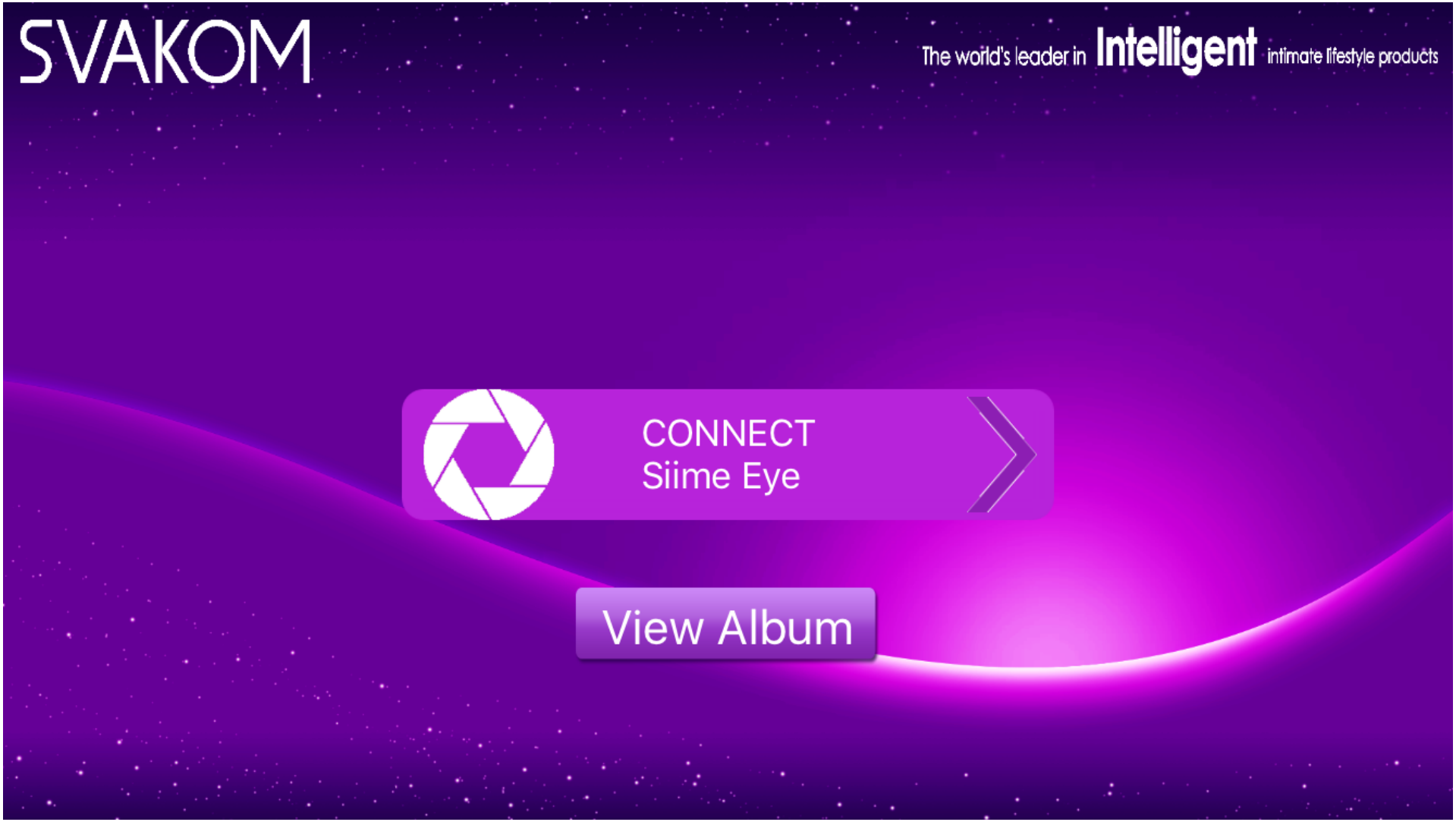

MINI TANK
WiFi
Wi Fi

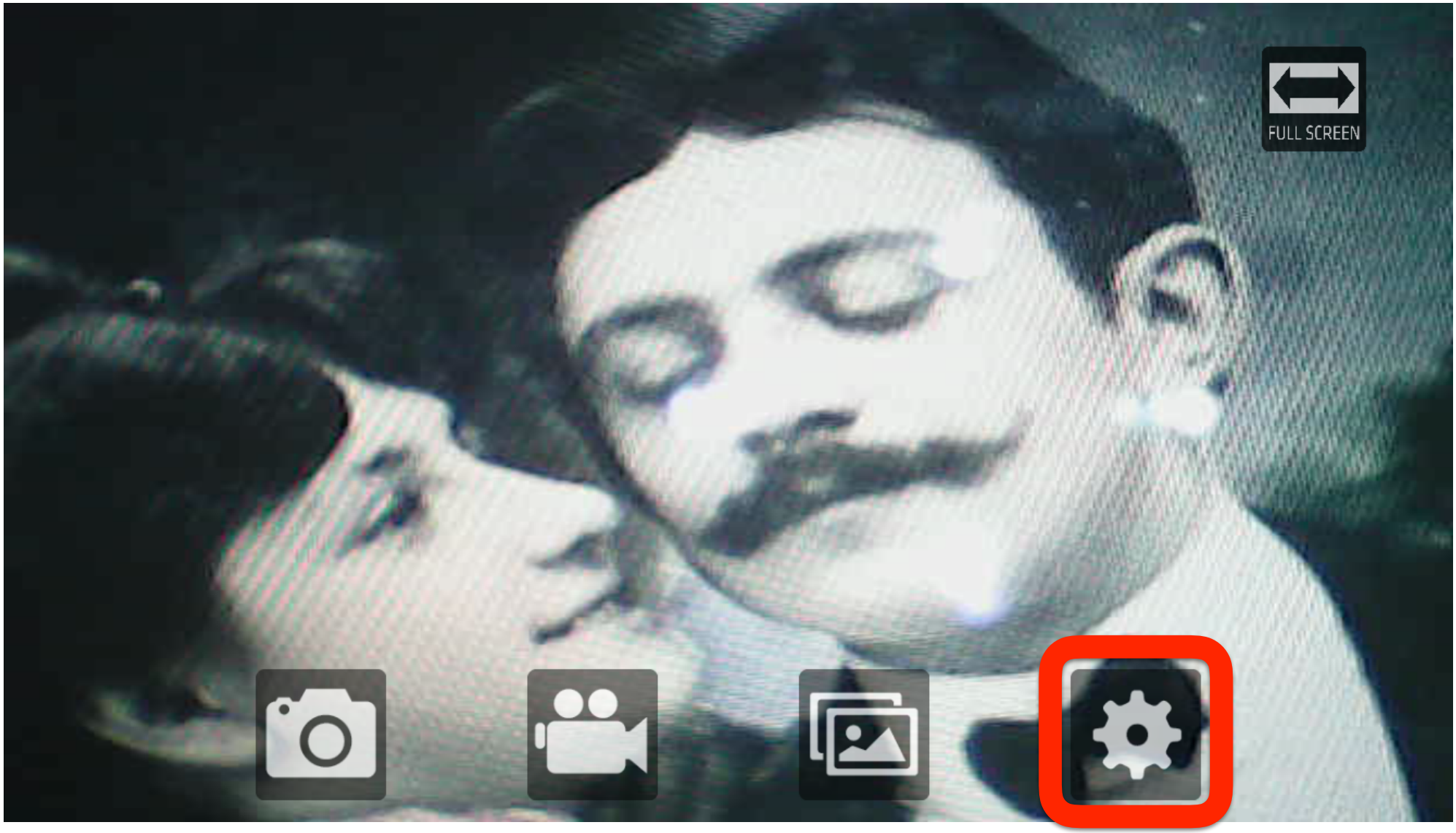
DEMO

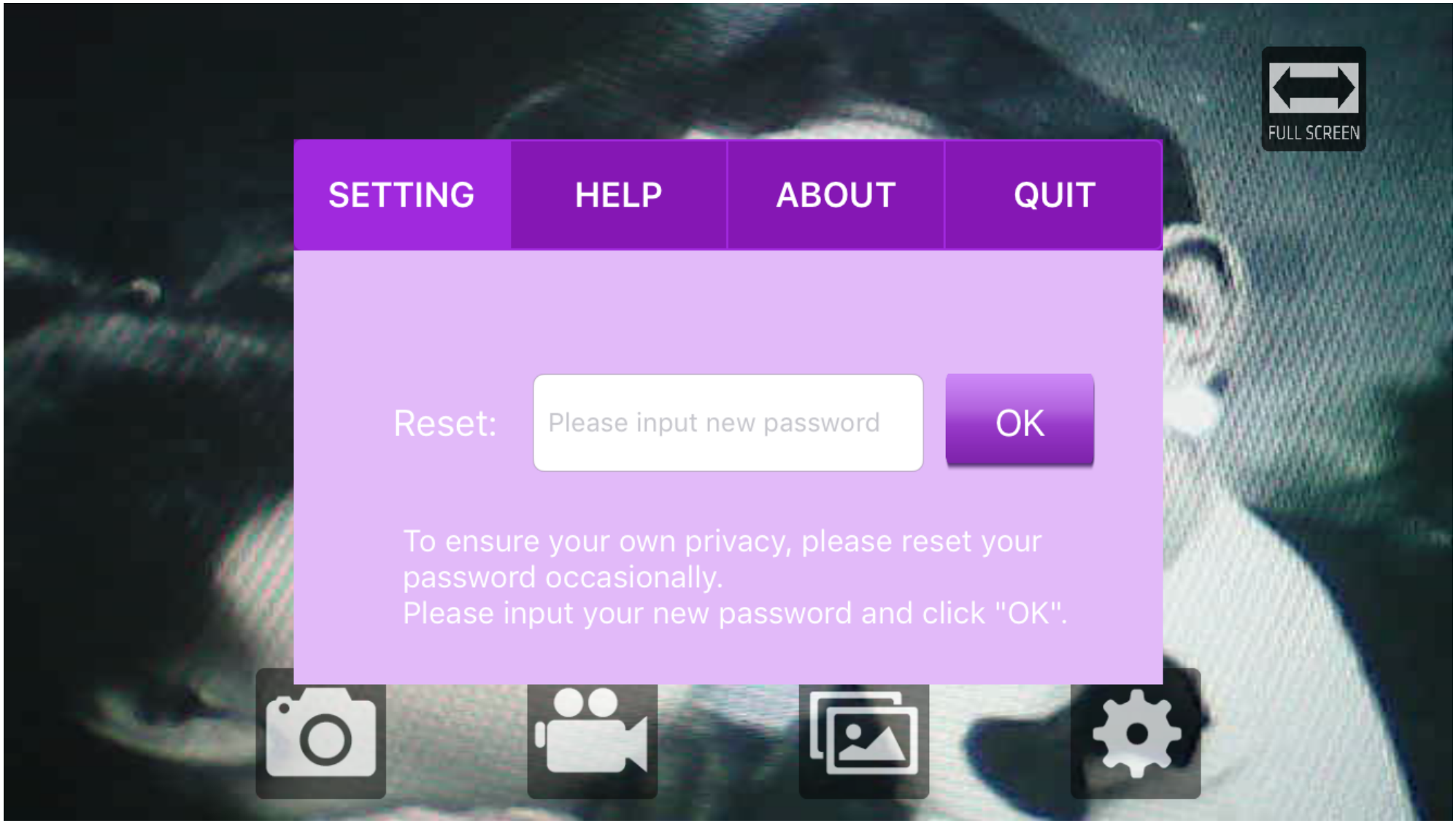

attention!
简体中文
Dictionary attack defense is enabled.
You have up to 10 attempts and will be blocked for 1 hour if used up.
Now,you will be blocked for 57 minutes and 48 seconds


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Clear
Apply
No. Time Source Destination Protocol Info
47 139.931463 ThomsonT_08:35:4f Wistron_07:07:e ARP 192.168.1.254 is at 00:90:d0:08:35:4f
48 139.931466 192.168.1.68 192.168.1.254 DNS Standard query A www.google.com
49 139.975406 192.168.1.254 192.168.1.68 DNS Standard query response CNAME www.l.google.com A 66.102.9.99
58 140.197811 192.168.1.68 66.102.9.99 TCP 62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
Frame 1 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 0c 29 38 eb 0e 08 06 00 01 ....)8......
0010 08 00 06 04 00 01 00 0c 29 38 eb 0e c0 a8 39 80 ....)8....9.
0020 00 00 00 00 00 00 c0 a8 39 02 .... 9.
eth0: <live capture in progress> Fil... Packets: 445 Displayed: 445 Marked: 0 Profile: Default

WIRESHARK


SVAKOM
The world's leader in Intelligent intimate lifestyle products
CONNECT
Siime Eye
View Album


FULL SCREEN


FULL SCREEN
SETTING
HELP
ABOUT
QUIT
Reset:
Please input new password
OK
To ensure your own privacy, please reset your password occasionally.
Please input your new password and click "OK".

http://192.168.1.1/set_params.cgi?user=admin&pwd=&json=1&ssid=88888888&save=1&reboot=1

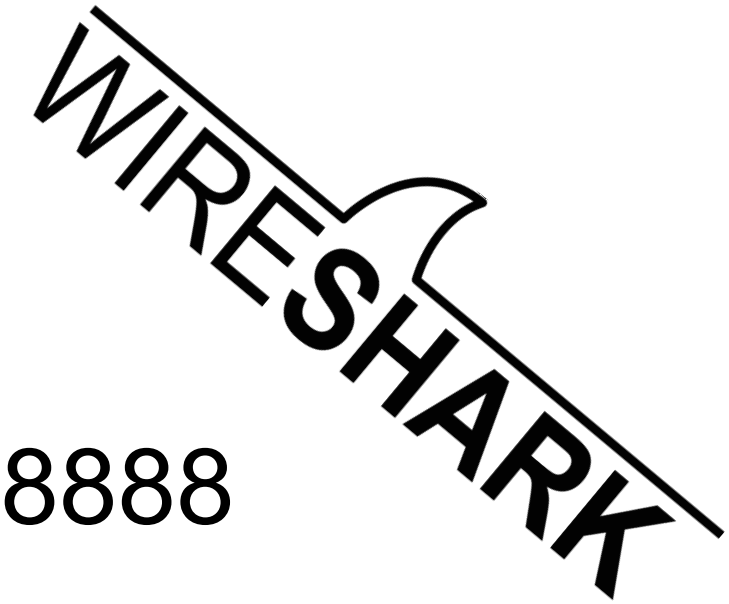
set_params.cgi

user=admin&pwd=

ssid=88888888

save=1

reboot=1



TRIAL AND ERROR

set ERROR counter to zero

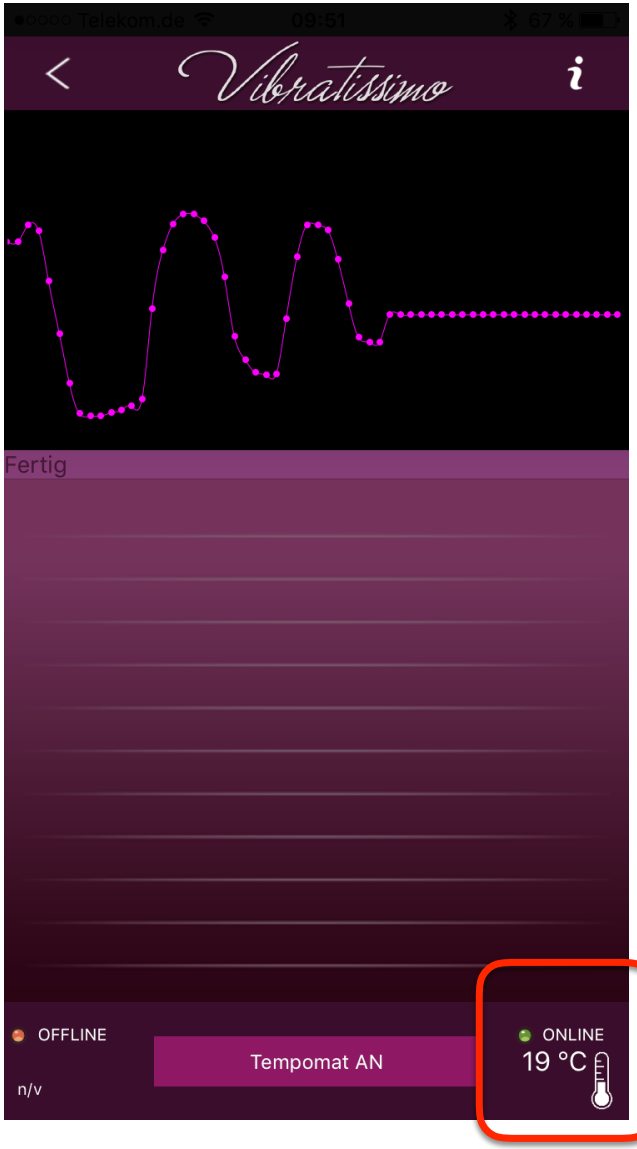
192.168.1.1/
set_params.cgi?user=admin&pwd=&json=1
&error_times=0&save=1

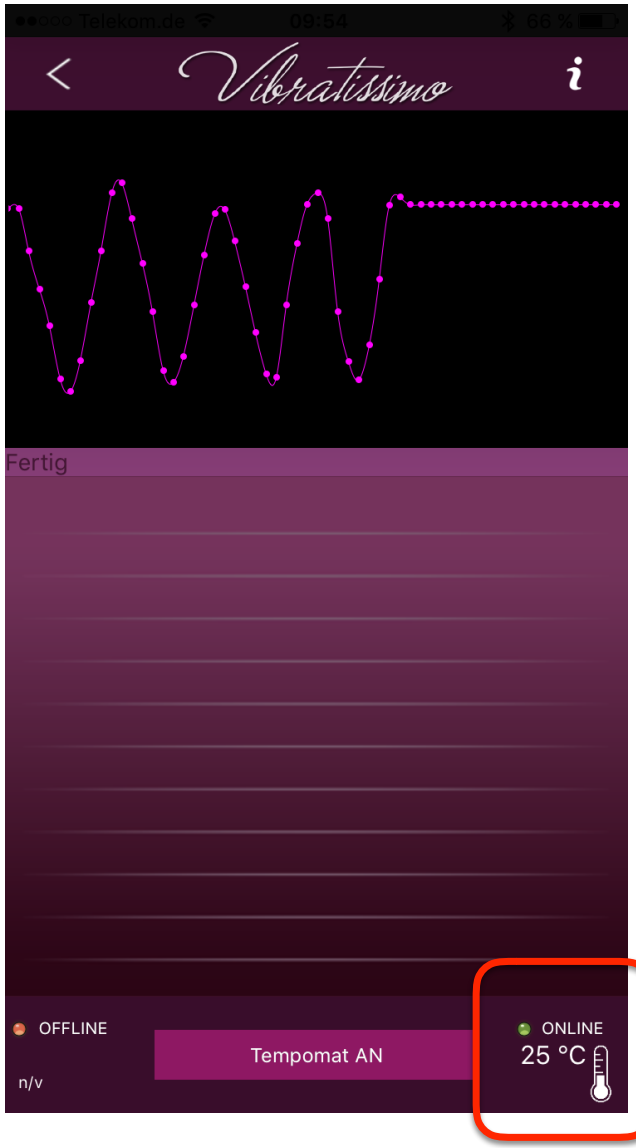
read STATUS

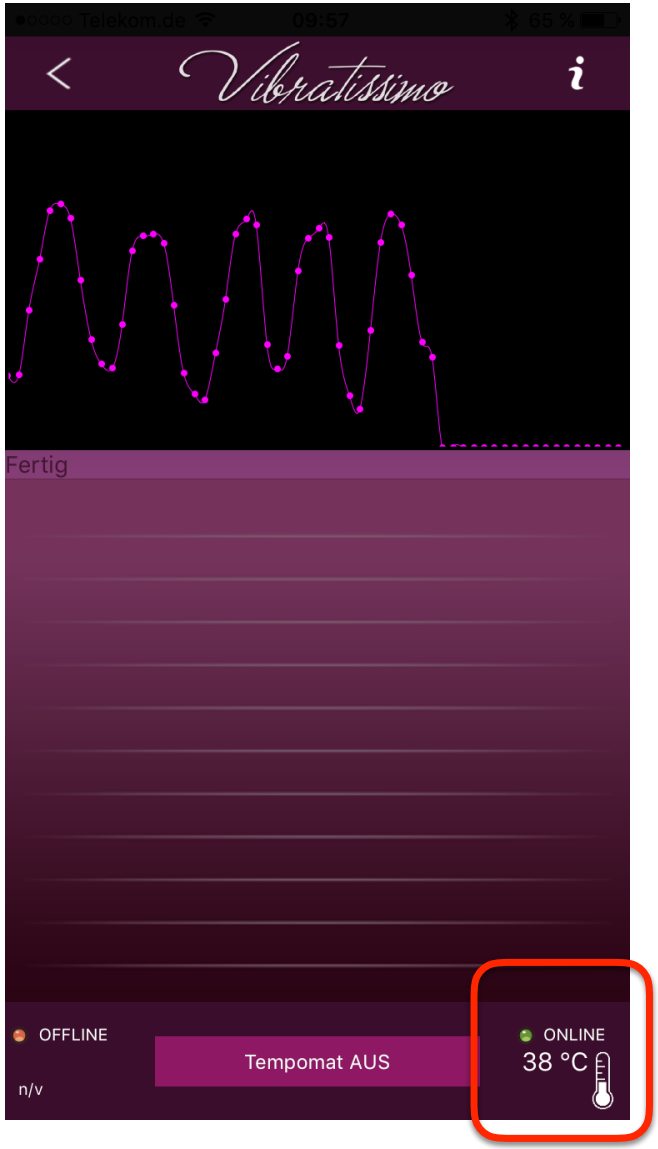
http://192.168.1.1/get_badauth.cgi

DEMO


Anmelden
Meine Toys
Toy-Steuerung
Vibratissimo
Meine Vibes
OFFLINE


Vibratissimo
Fertig
OFFLINE
n/v
Tempomat AN
ONLINE
19 °C


Vibratissimo
Fertig
OFFLINE
n/v
Tempomat AN
ONLINE
25 °C


Vibratissimo
Fertig
OFFLINE
n/v
Tempomat AUS
ONLINE
38 °C

DEMO

WIN A RASPBERRY PI 2 (1GB)

Be the first to control the dildo.

a) download app Vibratissimo
b) connect to dildo via bluetooth
c) vibrate the dildo
d) you are a winner!

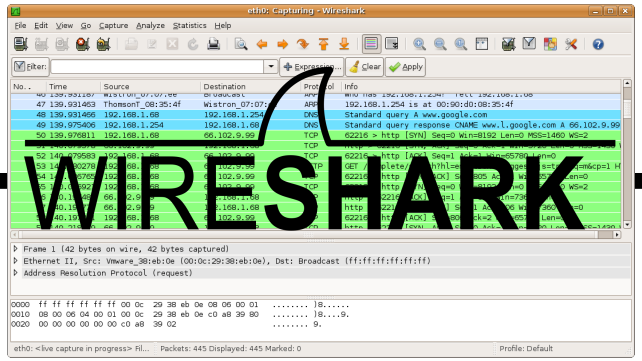
There will be light

CREDITS to Marco di Filippo

eth

mghz

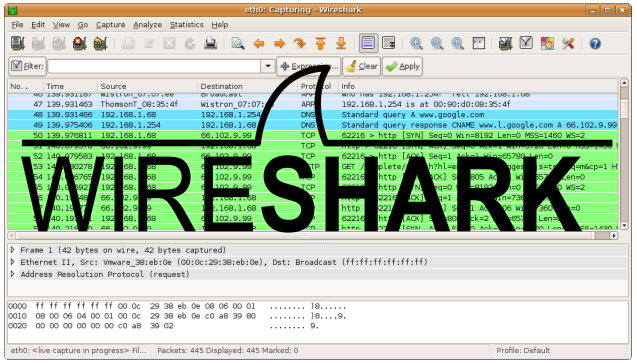
wifi



WIRESHARK

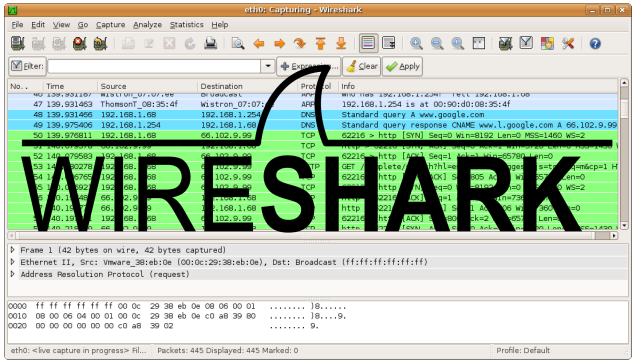
mghz

wifi



PUT request

http://192.168.2.2/api/H42VLZyIzAM3atNKhIgVigZsrNokZWfMqqYpyYCH/lights/3/state

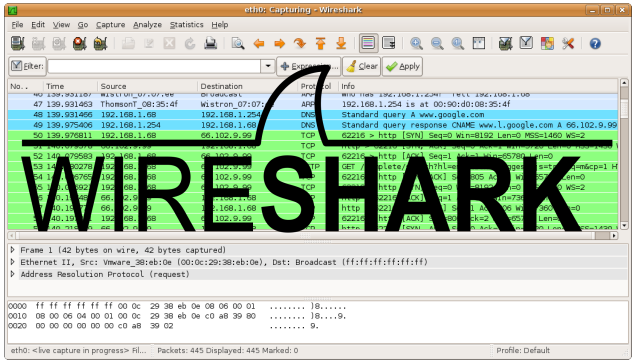


How to get the API key?

H42VLZyIzAM3atNKhlgVigZsrNokZWfMqqYpyYCH

- Brute Force with CURL: 25 API keys / second
(too slow, ineffective)

- CURL status while button pressed

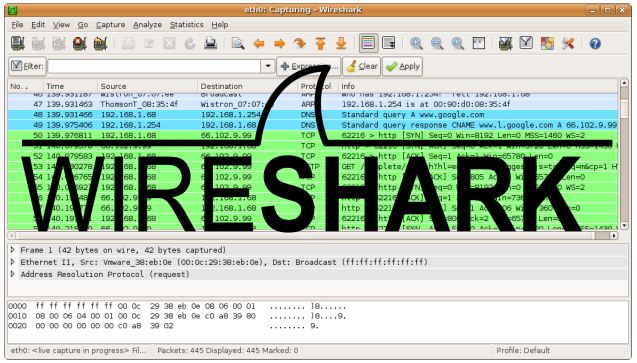


PUT request

http://192.168.2.2/api/H42VLZyIzAM3atNKhIgVigZsrNokZWfMqqYpyYCH/lights/3/state

PUT parameters

hue = 0-65535 (the lamp)
sat (saturation) 0-255
bri (brightness) 0-255
ct (colortemp) 153-500
alert = none, select, lselect (=one or endless flash)
effect = none, colorloop
transitiontime n (x100ms e.g. 4=400ms)



PUT request

http://192.168.2.2/api/H42VLZylzAM3atNKhlgVigZsrNokZWfMqqYpyYCH/lights/3/state
Parameters: ct=300

CURL PUT request

curl -X PUT -d '{"ct":300}' http://192.168.2.2/api/H42VLZylz(...)ZWfMqqYpyYCH/lights/3/state;

* allows programming in PHP, Perl, etc *

DEMO

IoT security today …

… must be cheap
… must be first on market
… manufacturer is good in what he does
… but has no idea about IT security

IoT security tomorrow …

… must be tested from 3rd parties
… must be secured by design
… updates must be available
    at least for the planned lifetime of the device

How? By law!

Hacking toys ...
and other stuff

Twitter
@comedyhacker

Tobias Schrödel