Hardware Hacking Quickstart

Besides Tirana 2024

Roland Sako / WINSLOW.IO

Intro

Smart devices?

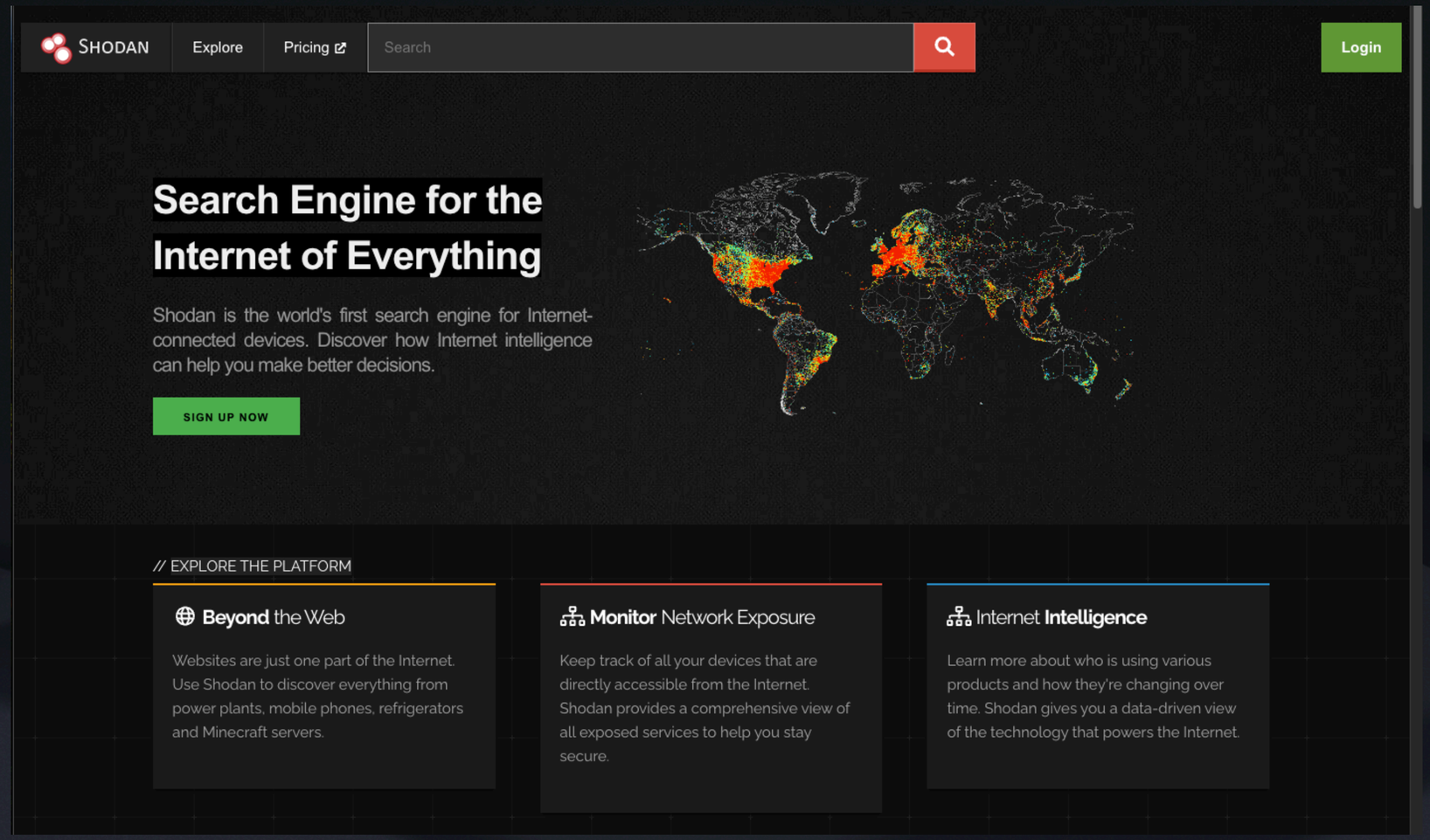
Smart devices?

Smart devices?

Smart devices?

```
Host is up (0.095s latency).
Not shown: 954 filtered ports, 32 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
2222/tcp open  EtherNetIP-1
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 25.60 seconds
```

Smart devices?



Vuln Research Process

Firmware

Firmware

Antennas

Smart Home > Home Security

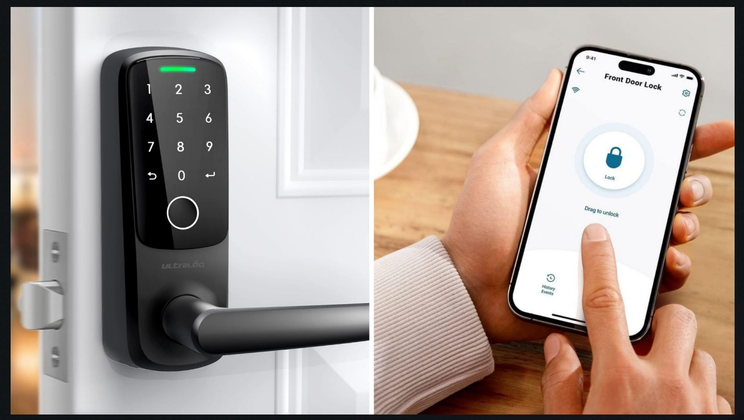
Tapo C425 KIT	Tapo C425	Tapo C420	Tapo C420S1	Tapo C420S2
Tapo C420S4	Tapo C410 KIT	Tapo C410	Tapo C402 KIT	Tapo C402
TC85 KIT	TC82 KIT	TC85	TC82	TCB82
Tapo C720	Tapo C520WS	Tapo C51A	Tapo C510W	Tapo C500
Tapo C325WB	Tapo C320WS	Tapo C310P2	Tapo C310	TC65
TC55	TC53	TC40	TC41	Tapo C222
Tapo C220	Tapo C225	Tapo C210	Tapo C201	TC70P2
Tapo C101	Tapo C200P2	Tapo C200C	Tapo C202	TC72
Tapo C210P2	Tapo C110P4	Tapo C211	Tapo C111	Tapo C120
Tapo C212	Tapo D130	TC71	EC71	Tapo C125
Tapo D230S1	TC70	EC60	Tapo C200	Tapo A100
Tapo A200	Tapo C110	TC60	Tapo C100	KC300S2
KC310S2	KC410S	KC105	KC200	NC450
NC260	NC200	TL-SC3430	TL-SC3430N	TL-SC4171G
Tapo A201	KC120			

tp-link.com/en/support/download

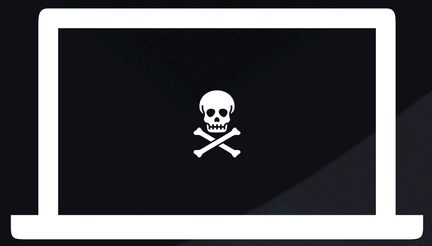
Firmware

Paris Games Equestrian
GOOGLE
tl-wr841n firmwar
tl-wr841n firmware

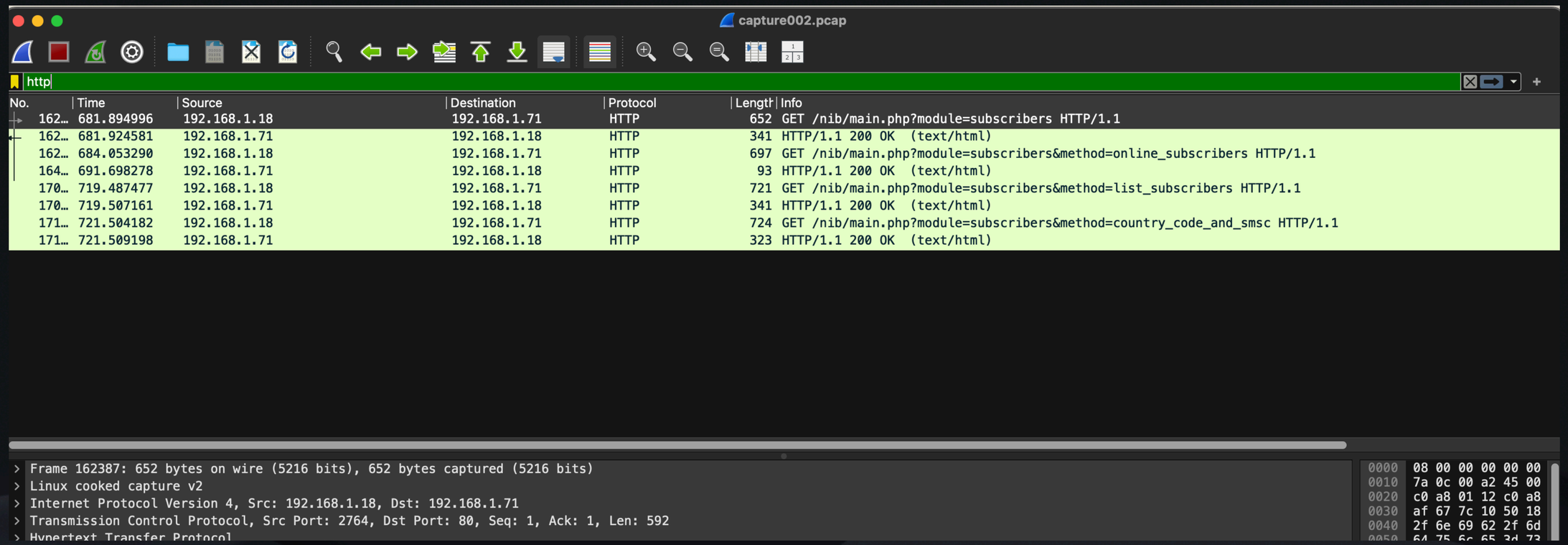
Firmware


Front Door Lock
Lock
Drag to unlock

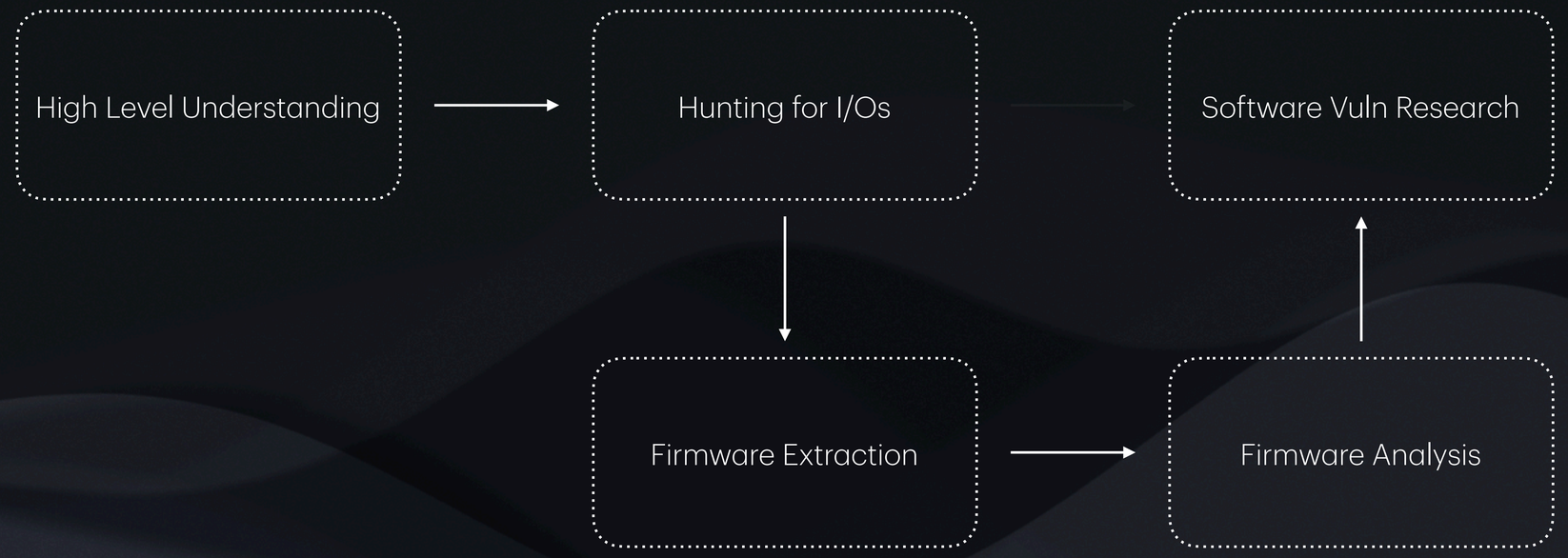
0111011011011001101010 01
0100110001101001001010
1101011011010101101001 01
1001101001010110101000 1
1001010100101001001001
1001010010101010010101 1
1110010100001110011010 0
0111011011011001101010 01



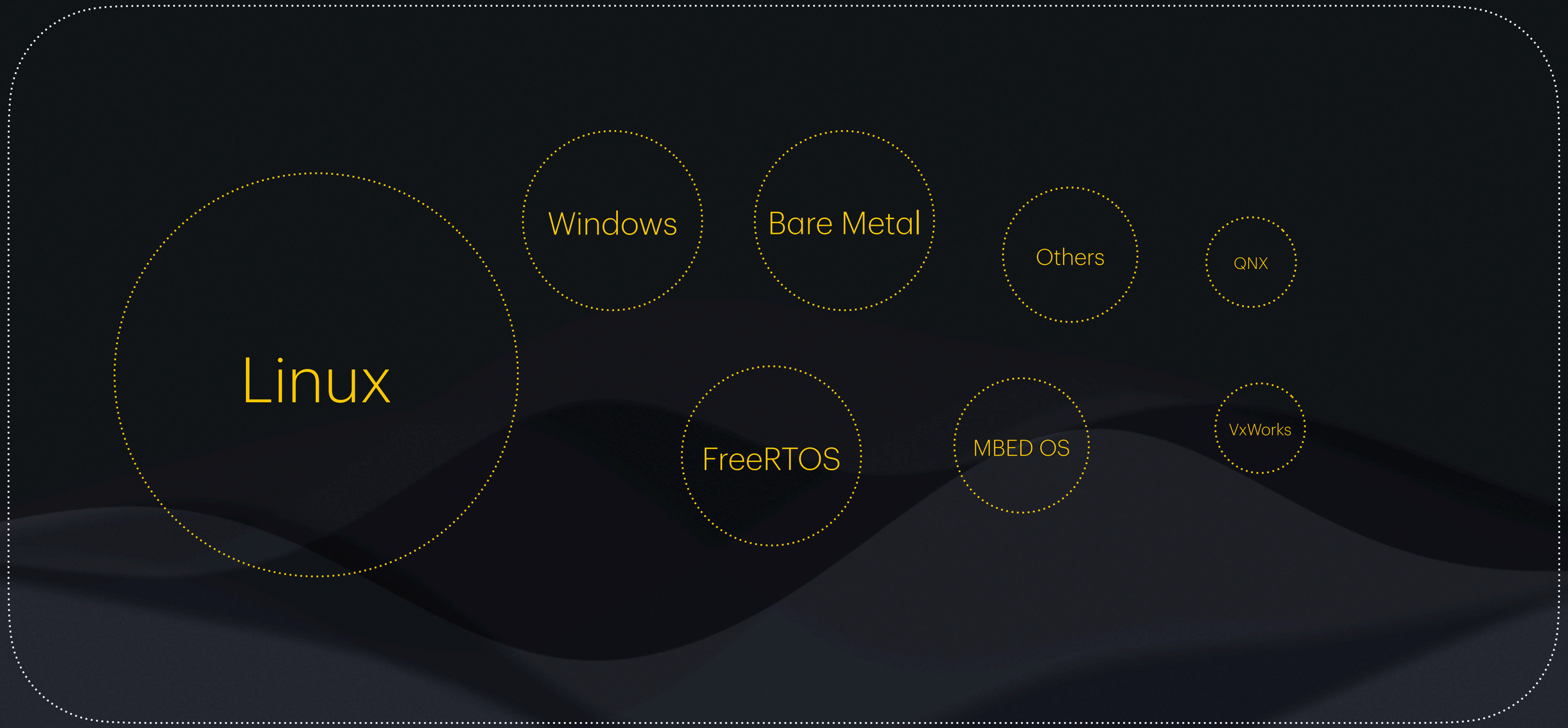
Firmware


capture002.pcap
http
No. Time Source Destination Protocol Length Info
162… 681.894996 192.168.1.18 192.168.1.71 HTTP 652 GET /nib/main.php?module=subscribers HTTP/1.1
162… 681.924581 192.168.1.71 192.168.1.18 HTTP 341 HTTP/1.1 200 OK (text/html)
162… 684.053290 192.168.1.18 192.168.1.71 HTTP 697 GET /nib/main.php?module=subscribers&method=online_subscribers HTTP/1.1
164… 691.698278 192.168.1.71 192.168.1.18 HTTP 93 HTTP/1.1 200 OK (text/html)
170… 719.487477 192.168.1.18 192.168.1.71 HTTP 721 GET /nib/main.php?module=subscribers&method=list_subscribers HTTP/1.1
170… 719.507161 192.168.1.71 192.168.1.18 HTTP 341 HTTP/1.1 200 OK (text/html)
171… 721.504182 192.168.1.18 192.168.1.71 HTTP 724 GET /nib/main.php?module=subscribers&method=country_code_and_smsc HTTP/1.1
171… 721.509198 192.168.1.71 192.168.1.18 HTTP 323 HTTP/1.1 200 OK (text/html)
Frame 162387: 652 bytes on wire (5216 bits), 652 bytes captured (5216 bits)
Linux cooked capture v2
Internet Protocol Version 4, Src: 192.168.1.18, Dst: 192.168.1.71
Transmission Control Protocol, Src Port: 2764, Dst Port: 80, Seq: 1, Ack: 1, Len: 592
Hypertext Transfer Protocol
0000 08 00 00 00 00 00
0010 7a 0c 00 a2 45 00
0020 c0 a8 01 12 c0 a8
0030 af 67 7c 10 50 18
0040 2f 6e 69 62 2f 6d

Vuln Research Process

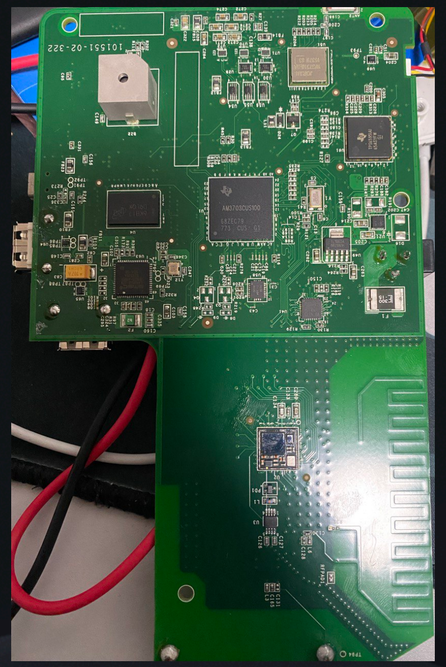


IoT OS Market Share (2021)

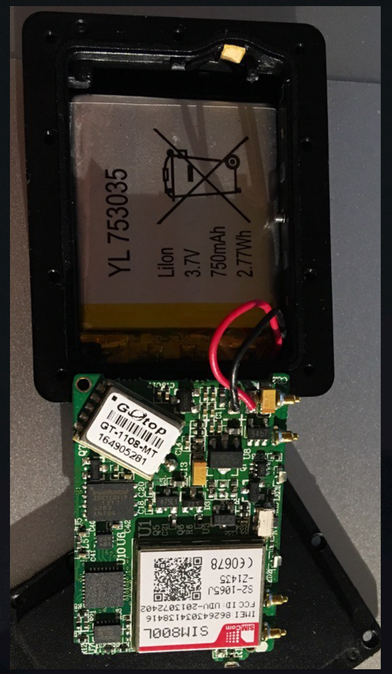


Hardware

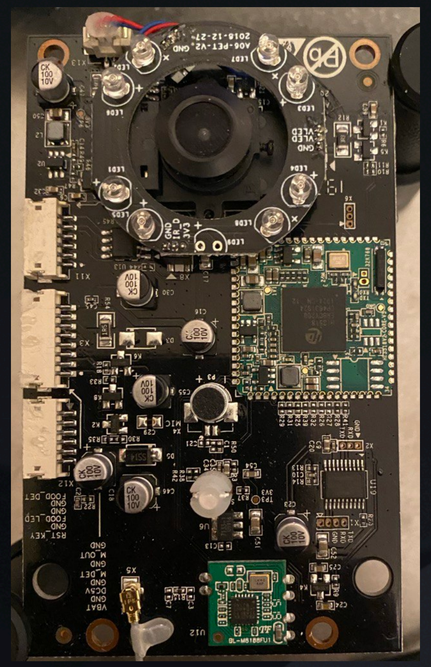
!(Hard)ware - OSINT



Medical Device



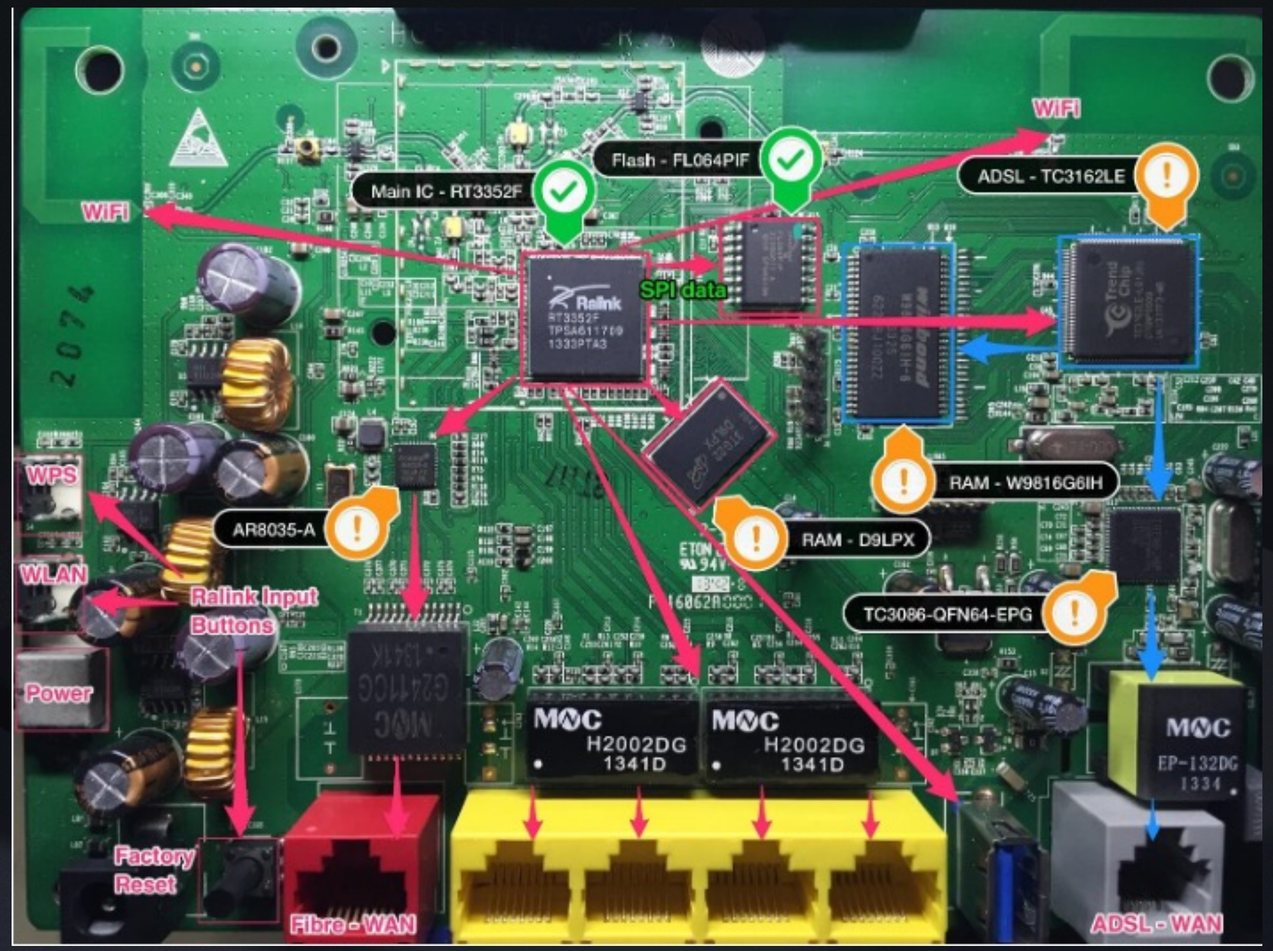
Pet Tracker



Smart Camera

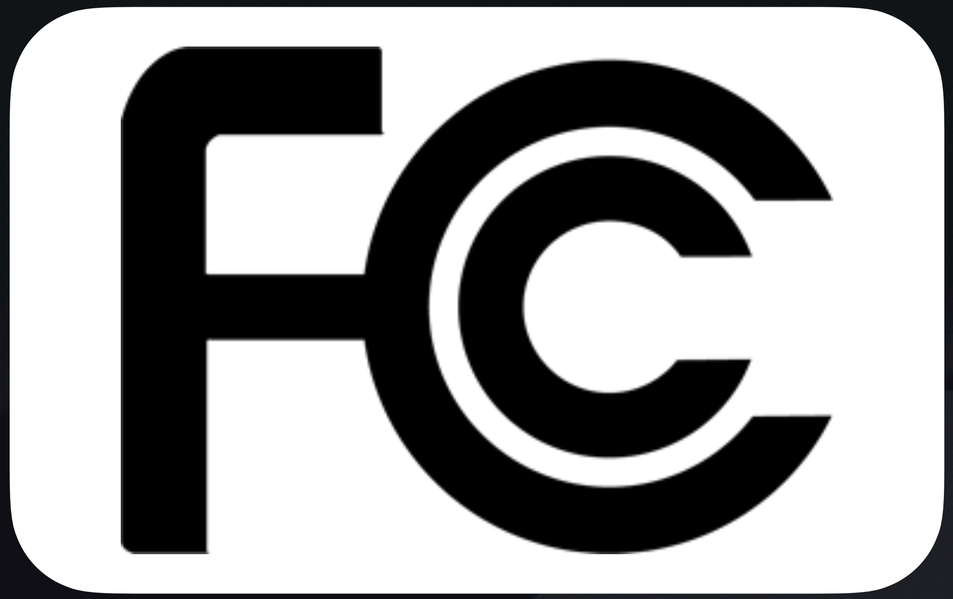
Car Infotainment

!(Hard)ware - OSINT



!(Hard)ware - OSINT

Looks familiar?



!(Hard)ware - OSINT

!(Hard)ware - OSINT

There are 483+ device authorizations with frequency operating ranges overlapping with the specified frequeny range.

FCC ID	Lower Frequency GHz	Upper Frequency GHz
2AA22CR56 High Resolution Car Recorder (Sanjet Technology Corp.)	2.412	2.462
2AA22CR58 Wicorder (Sanjet Technology Corp.)	2.412	2.462
2AA22SR10 SPORTS CAM (Sanjet Technology Corp.)	2.412	2.462
2AA28ADAPTER BLUETOOTH ADAPTER (Benway Electronics Co., Ltd)	2.402	2.48
2AA28BB BassBoomz (Benway Electronics Co., Ltd)	2.402	2.48
2AA28SPEAKER Bluetooth Speaker (Benway Electronics Co., Ltd)	2.402	2.48

!(Hard)ware - OSINT

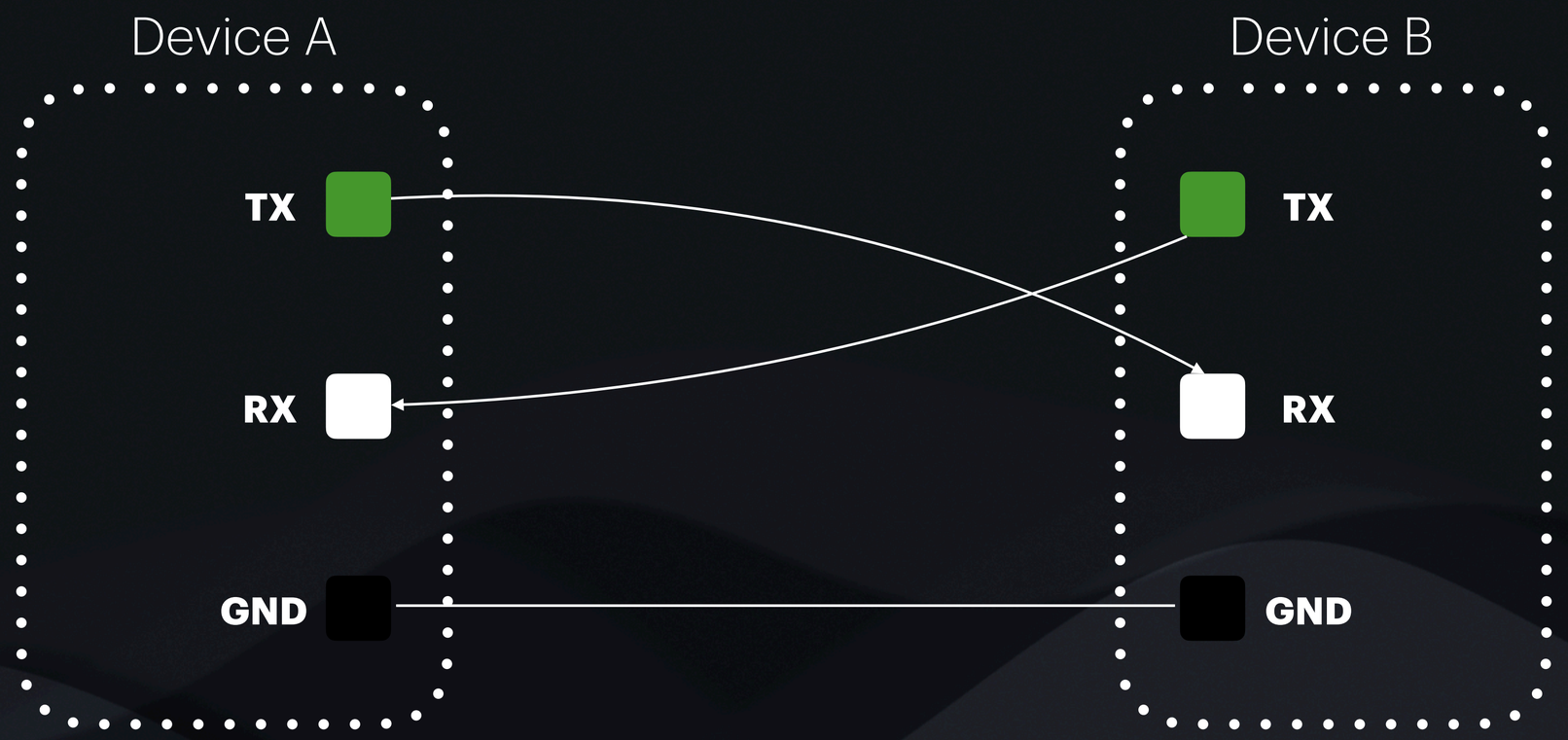
3	User Manual	Users Manual Adobe Acrobat PDF (358 kB)	2014-09-18 2015-03-18
3	Test Setup Photos	Test Setup Photos Adobe Acrobat PDF (410 kB)	2014-09-18 2015-03-18
3	Test Report	Test Report Adobe Acrobat PDF (798 kB)	2014-09-18 2014-09-19
3	MPE Calculation	RF Exposure Info Adobe Acrobat PDF (350 kB)	2014-09-18 2014-09-19
3	Label Location	ID Label/Location Info Adobe Acrobat PDF (97 kB)	2014-09-18 2014-09-19
3	Internal Photos	Internal Photos Adobe Acrobat PDF (2343 kB)	2014-09-18 2015-03-18
3	External Photos	External Photos Adobe Acrobat PDF (1463 kB)	2014-09-18 2015-03-18
3	WLAN 5GHz Declaration	Attestation Statements Adobe Acrobat PDF (315 kB)	2014-09-18 2014-09-19
3	WLAN 2.4GHz Declaration	Attestation Statements Adobe Acrobat PDF (318 kB)	2014-09-18 2014-09-19
3	Agent Authorization	Cover Letter(s) Adobe Acrobat PDF (36 kB)	2014-09-18 2014-09-19
3	Request for Confidentiality	Cover Letter(s) Adobe Acrobat PDF (93 kB)	2014-09-18 2014-09-19
3	Cover Letter	Cover Letter(s) Adobe Acrobat PDF (34 kB)	2014-09-18 2014-09-19
1	ConfidReq	Cover Letter(s) Adobe Acrobat PDF (67 kB)	2011-09-14 2011-09-20
2	ConfidReq	Cover Letter(s) Adobe Acrobat PDF (67 kB)	2011-09-14 2011-09-20

!(Hard)ware - UART

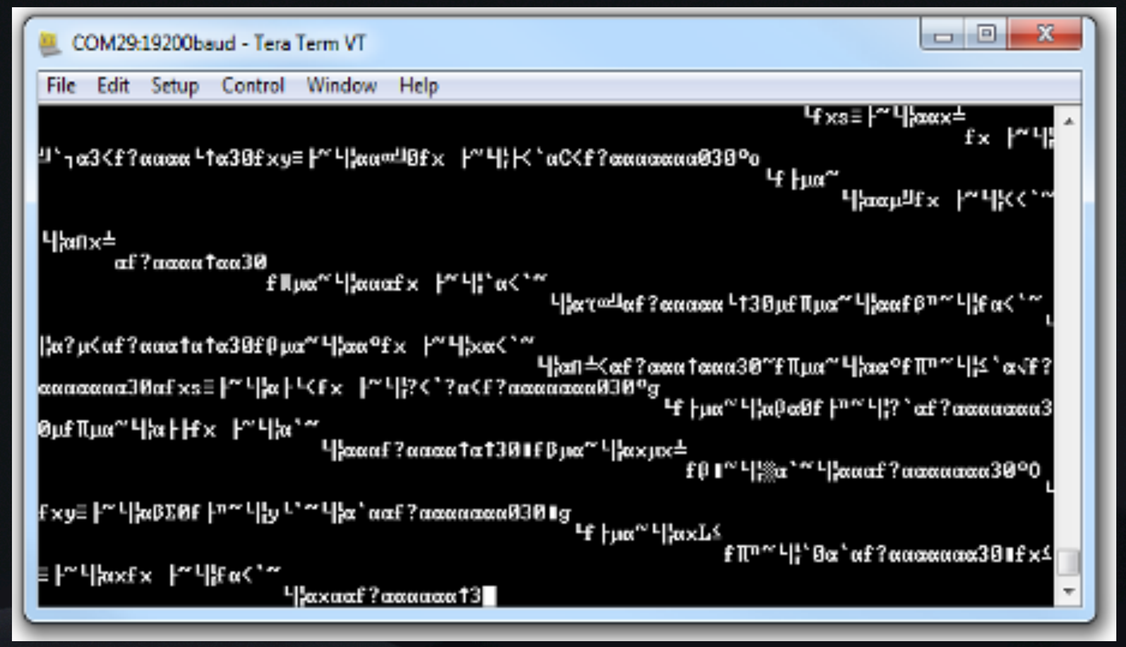
Universal Asynchronous

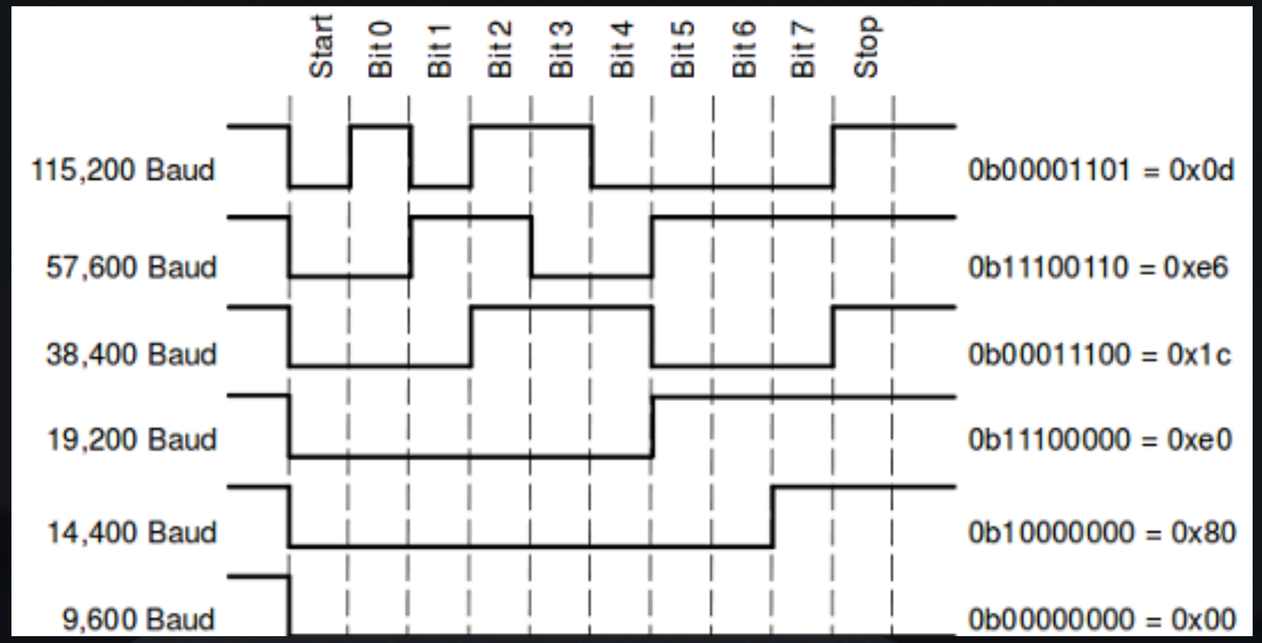
Receiver-Transmitter

!(Hard)ware - UART

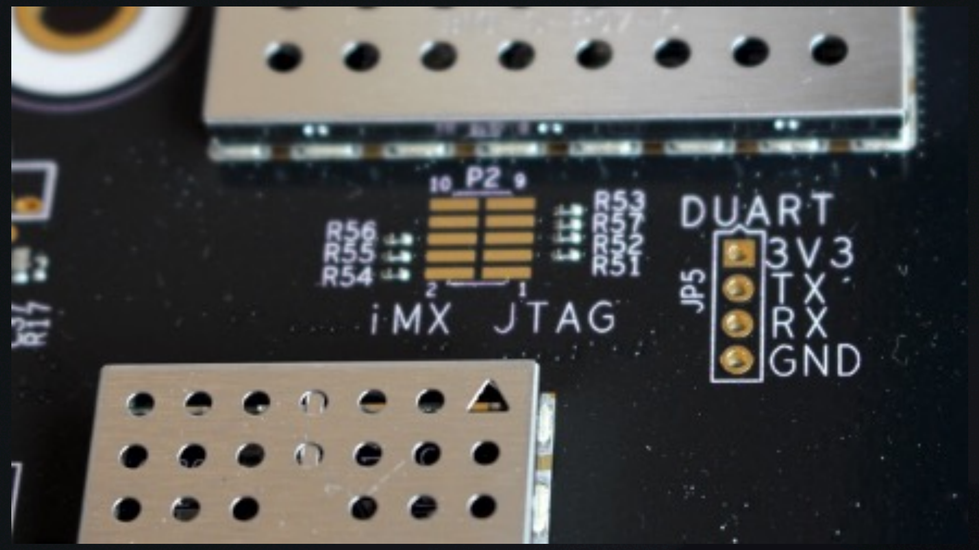


!(Hard)ware - UART



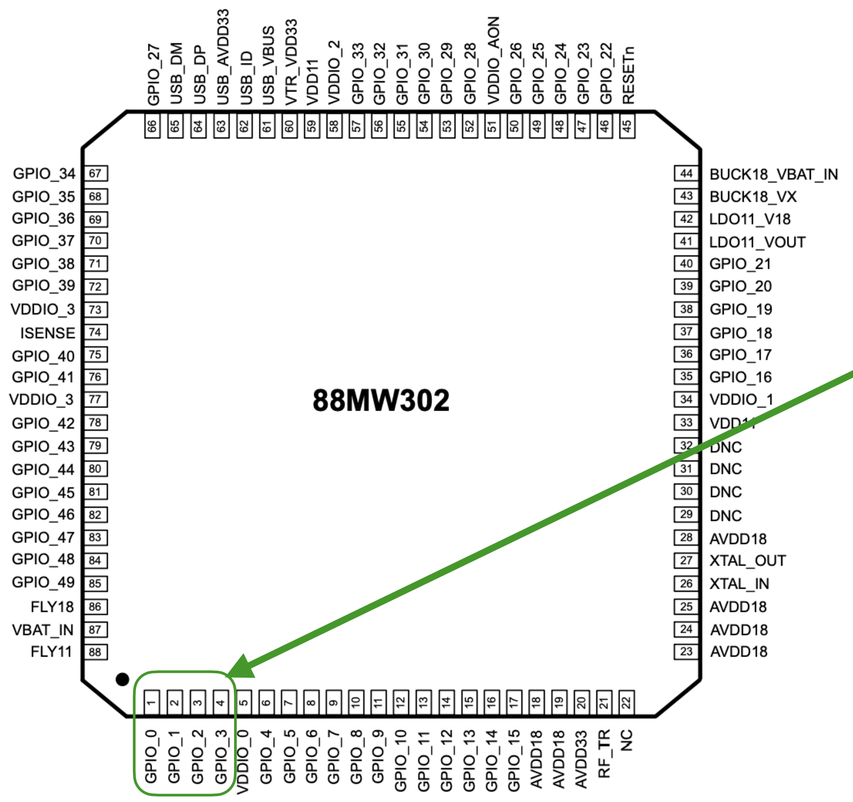


!(Hard)ware - UART



!(Hard)ware - UART

Figure 4: Pinout—88-Pin QFN[1]



1. Connect pin 22 to ground.

Wireless Microcontroller

Table 6: UART Interface[1]

88-Pin	68-Pin	Signal Name	Type	Supply	Description
GPIO_0		UART0_CTSn	I	VDDIO_0	UART 0 CTSn (active low)
GPIO_1		UART0_RTSn	O	VDDIO_0	UART 0 RTSn (active low)
GPIO_2		UART0_TXD	O	VDDIO_0	UART 0 TXD
GPIO_3		UART0_RXD	I	VDDIO_0	UART 0 RXD
GPIO_23		UART0_CTSn	I	VDDIO_AON	UART 0 CTSn (active low)
GPIO_24		UART0_RXD	I	VDDIO_AON	UART 0 RXD
GPIO_30		UART0_CTSn	I	VDDIO_2	UART 0 CTSn (active low)
GPIO_31		UART0_RTSn	O	VDDIO_2	UART 0 RTSn (active low)
GPIO_32		UART0_TXD	O	VDDIO_2	UART 0 TXD
GPIO_33		UART0_RXD	I	VDDIO_2	UART 0 RXD
GPIO_37	--	UART0_RTSn	O	VDDIO_3	UART 0 RTSn (active low)
GPIO_27		UART0_TXD	O	VDDIO_3	UART 0 TXD
GPIO_11	--	UART1_CTSn	I	VDDIO_0	UART 1 CTSn (active low)
GPIO_12	--	UART1_RTSn	O	VDDIO_0	UART 1 RTSn (active low)
GPIO_13	--	UART1_TXD	O	VDDIO_0	UART 1 TXD
GPIO_14	--	UART1_RXD	I	VDDIO_0	UART 1 RXD
GPIO_35	--	UART1_CTSn	I	VDDIO_3	UART 1 CTSn (active low)
GPIO_36	--	UART1_RTSn	O	VDDIO_3	UART 1 RTSn (active low)

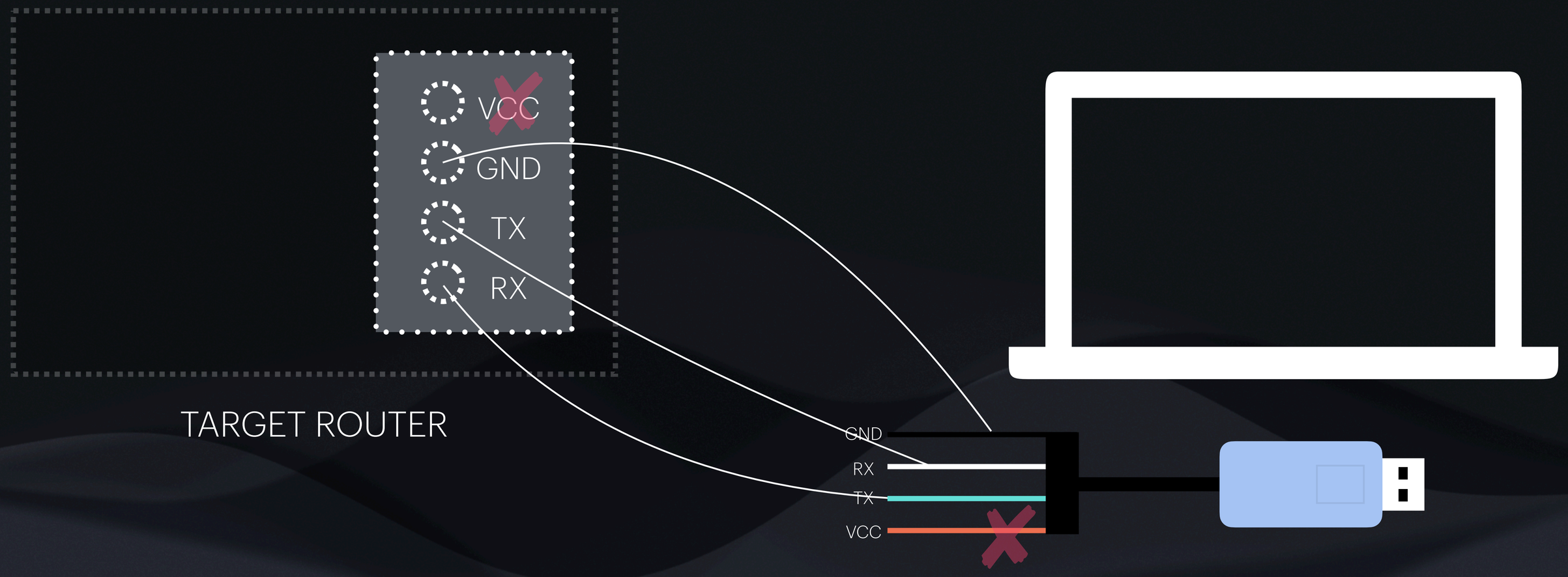
!(Hard)ware - UART

TARGET ROUTER

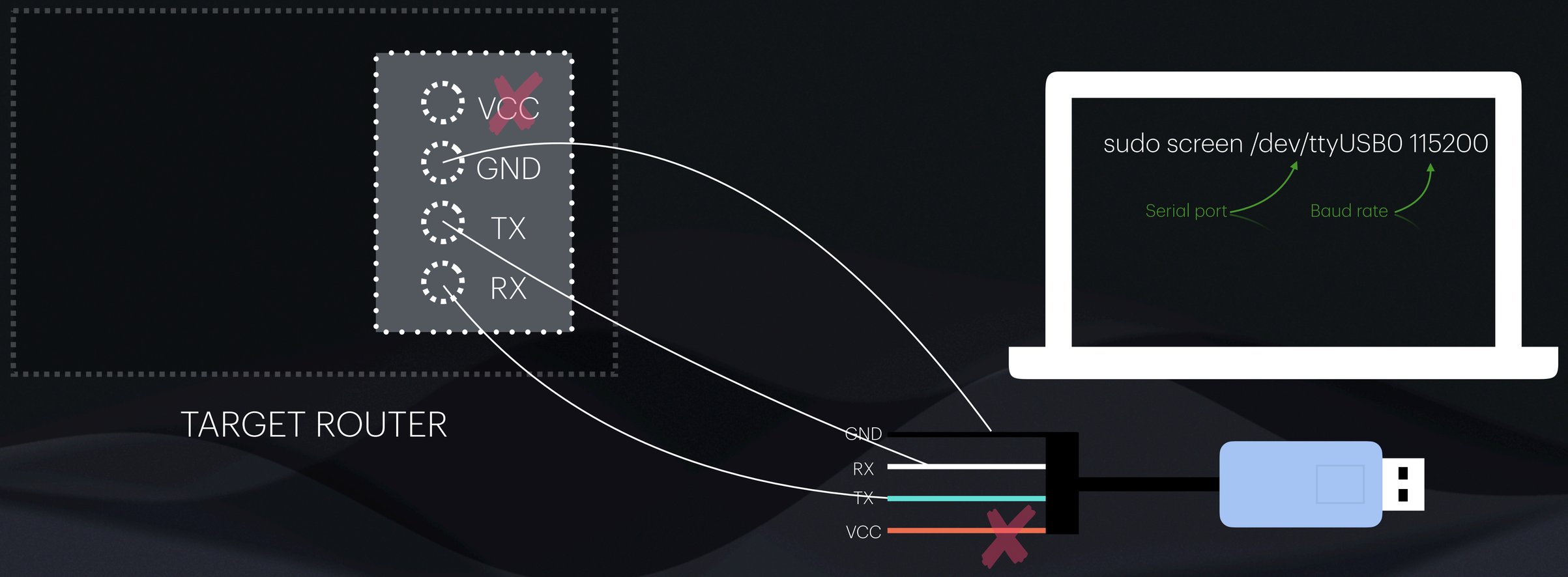
!(Hard)ware - UART

!(Hard)ware - UART

!(Hard)ware - UART



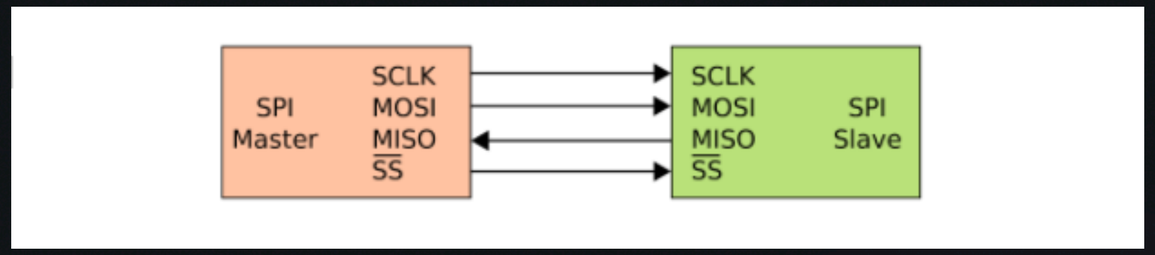
!(Hard)ware - UART

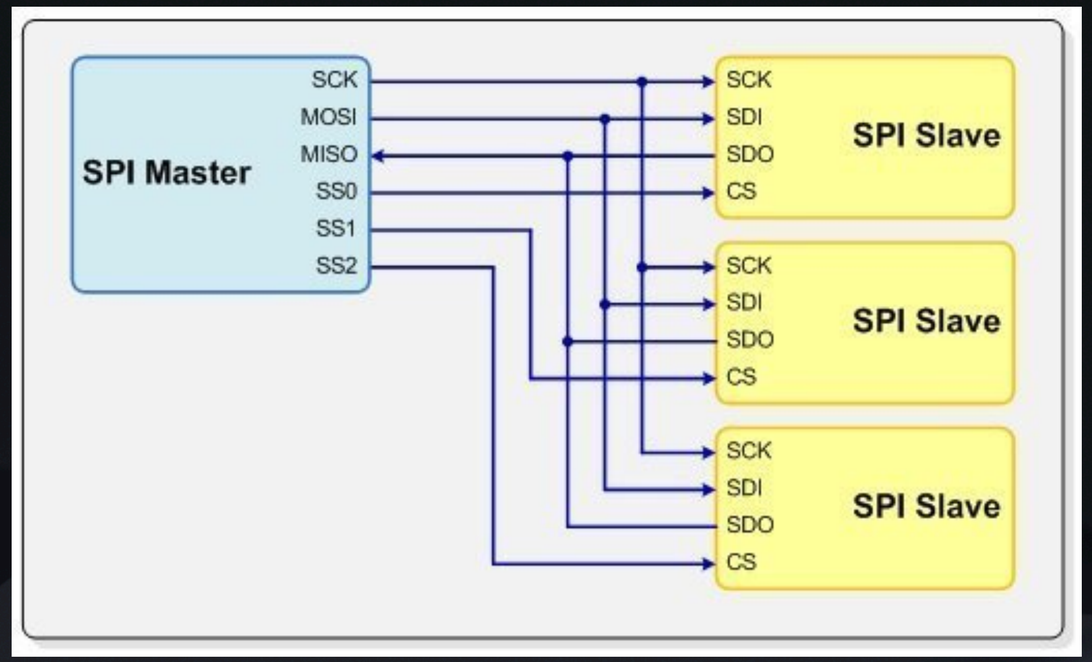


!(Hard)ware - SPI

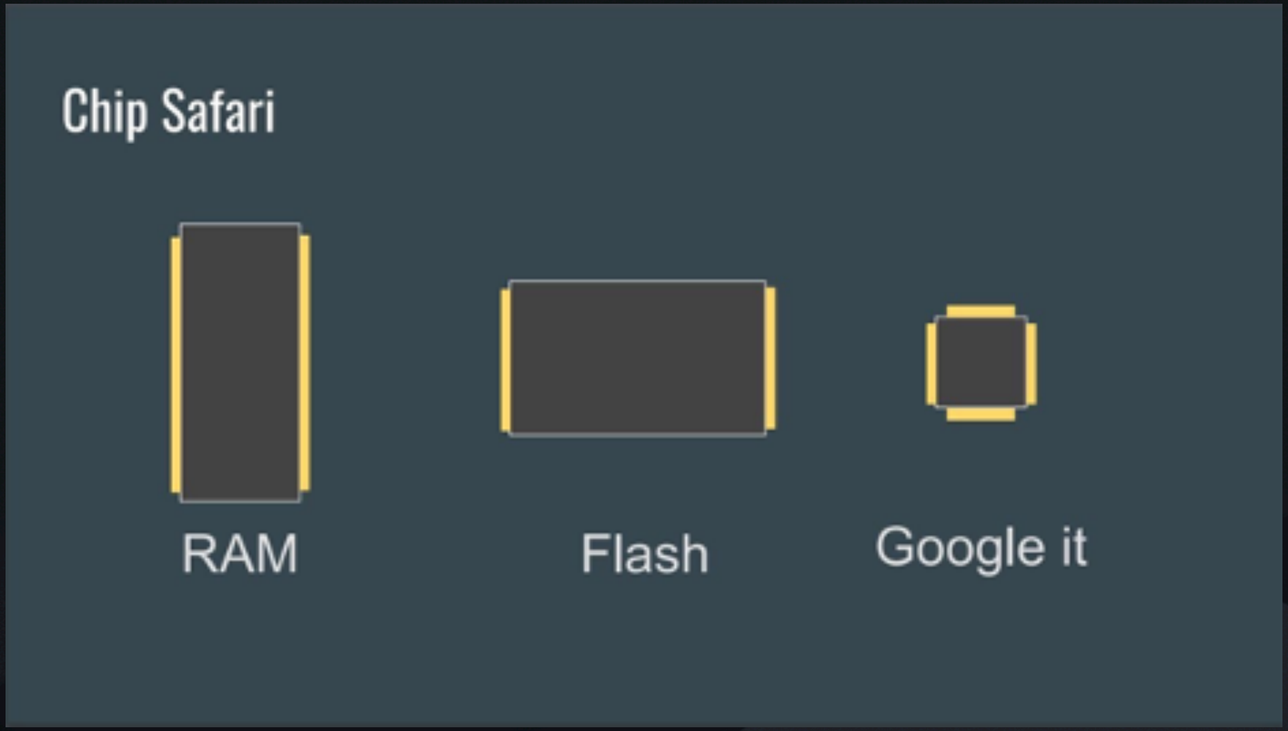
Serial Peripheral Interface

!(Hard)ware - SPI

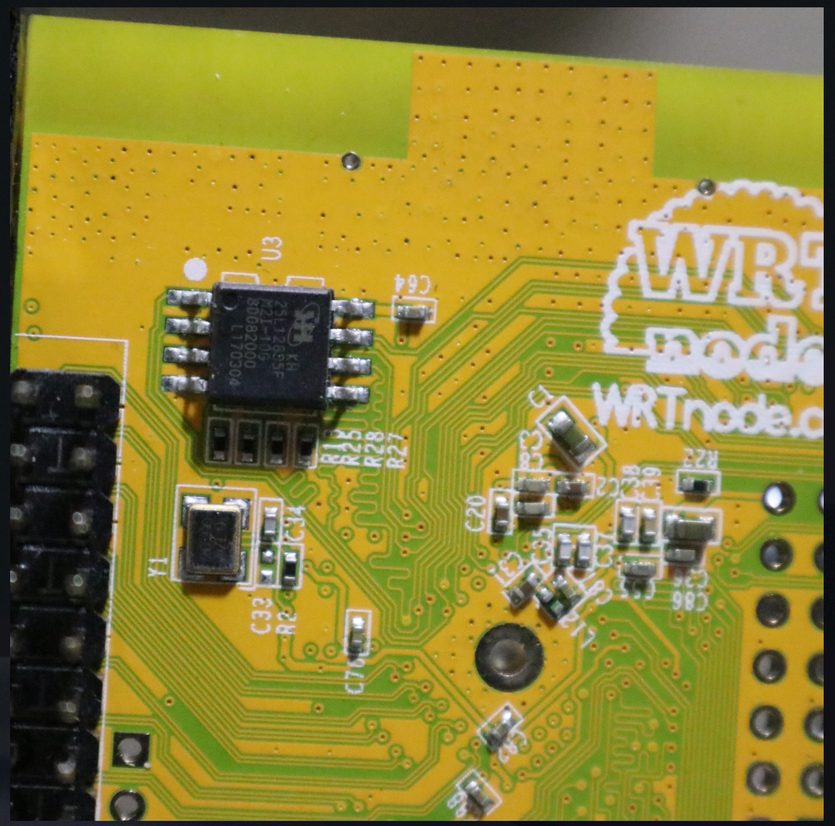


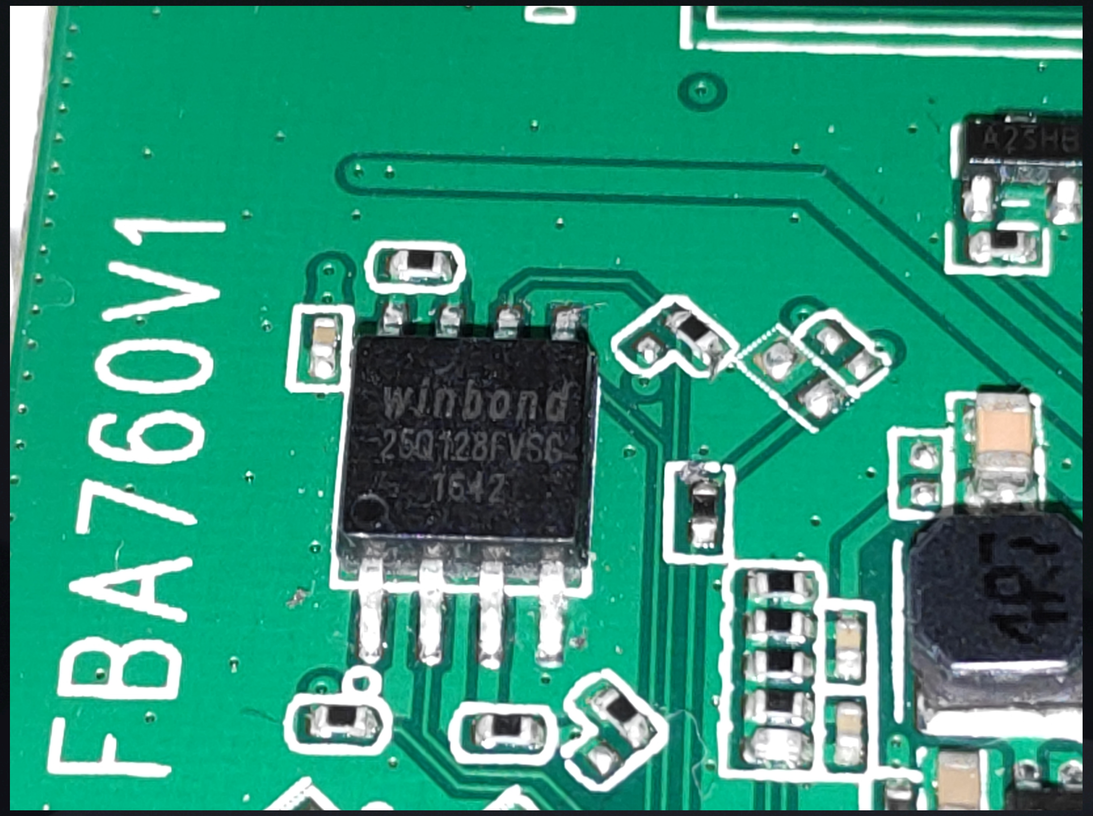


!(Hard)ware - SPI

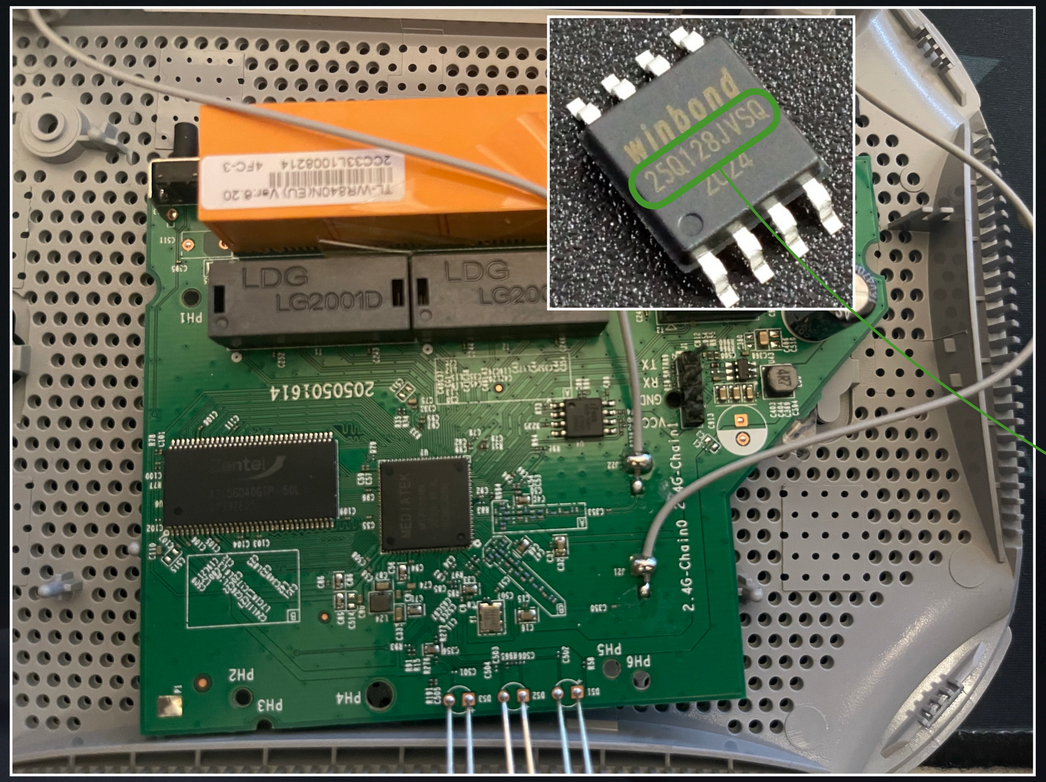


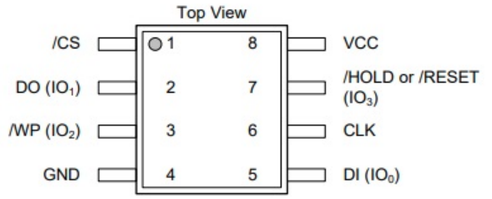
!(Hard)ware - SPI





!(Hard)ware - SPI

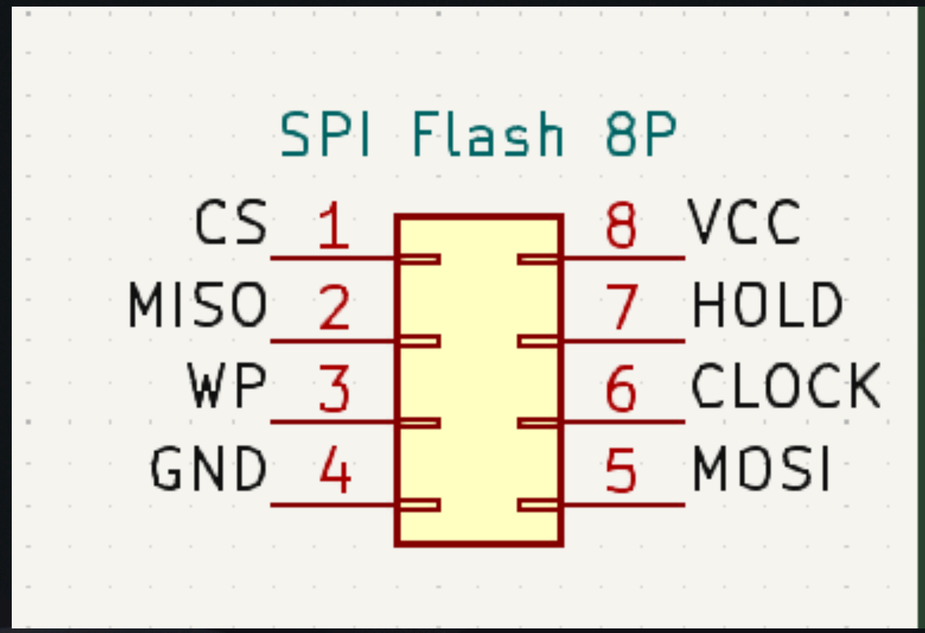


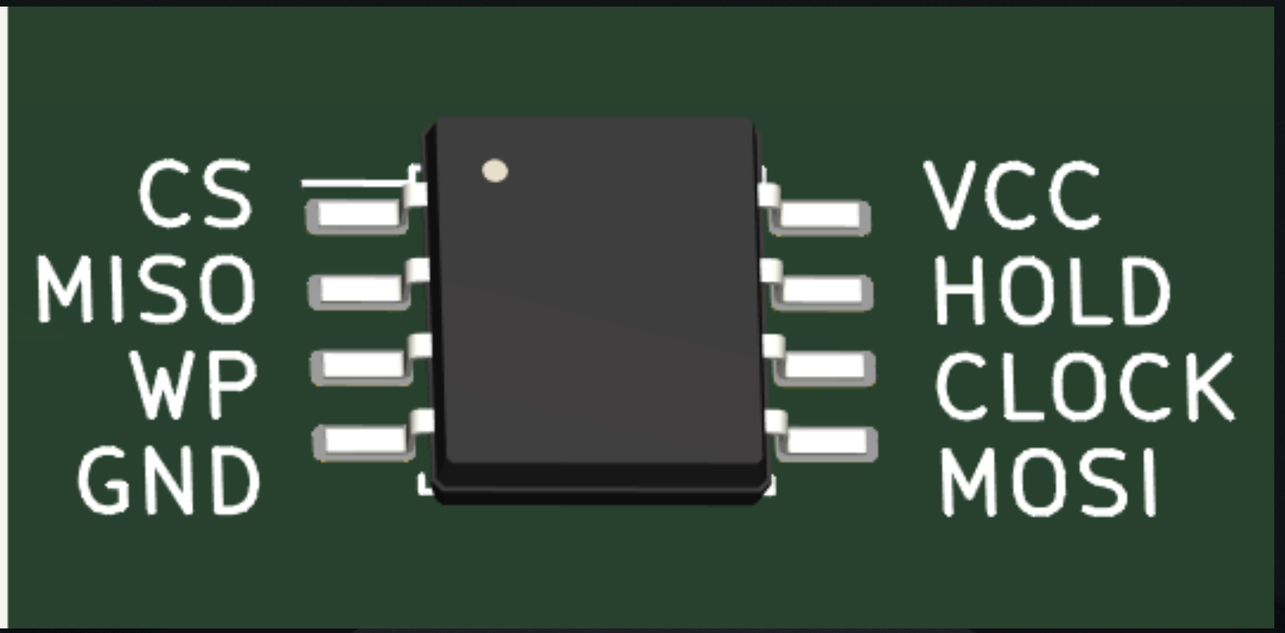


PAD NO.	PAD NAME	I/O	FUNCTION
1	/CS	I	Chip Select Input
2	DO (IO1)	I/O	Data Output (Data Input Output 1)(1)
3	/WP (IO2)	I/O	Write Protect Input (Data Input Output 2)(2)
4	GND		Ground
5	DI (IO0)	I/O	Data Input (Data Input Output 0)(1)
6	CLK	I	Serial Clock Input
7	/HOLD or /RESET (IO3)	I/O	Hold or Reset Input (Data Input Output 3)(2)
8	VCC		Power Supply

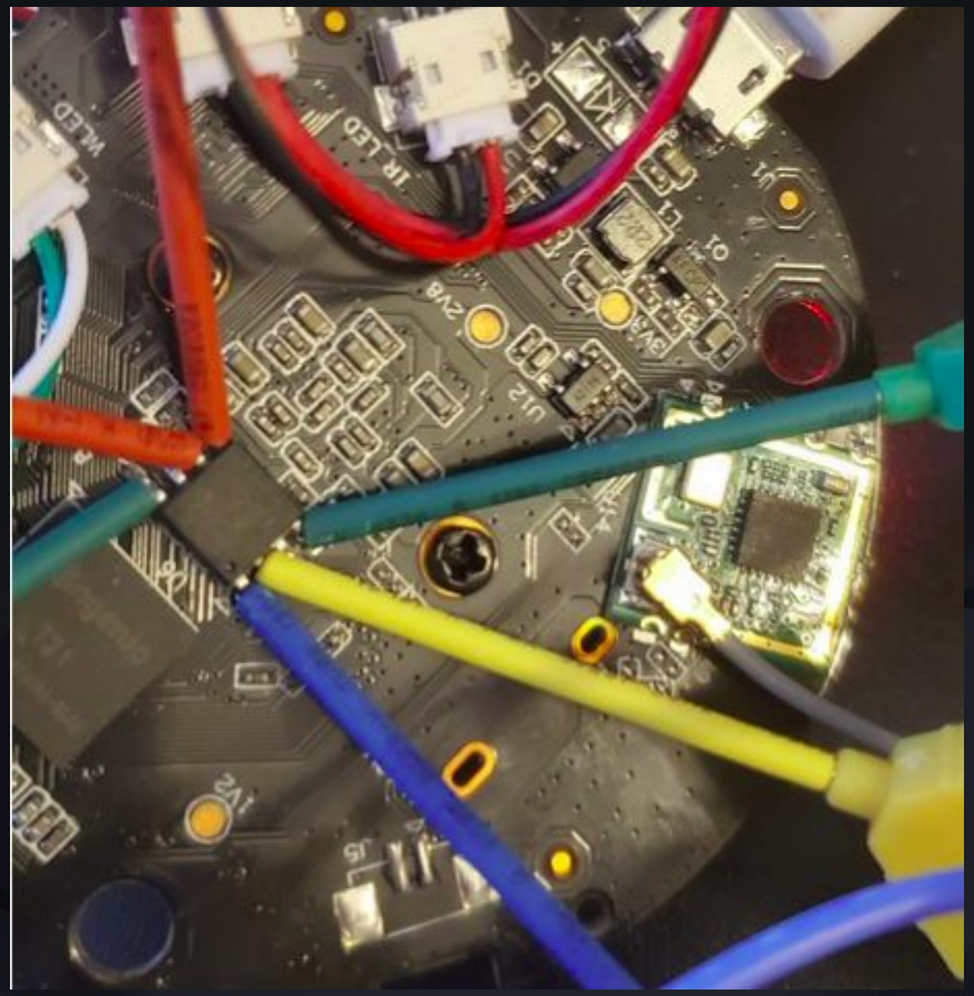
W25Q128JV Pinout

!(Hard)ware - SPI





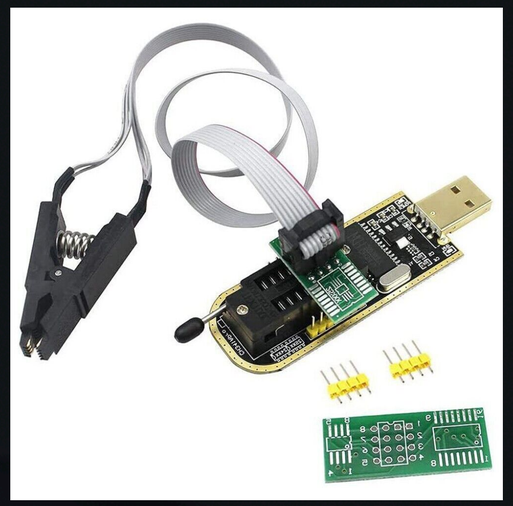
!(Hard)ware - SPI



!(Hard)ware - SPI

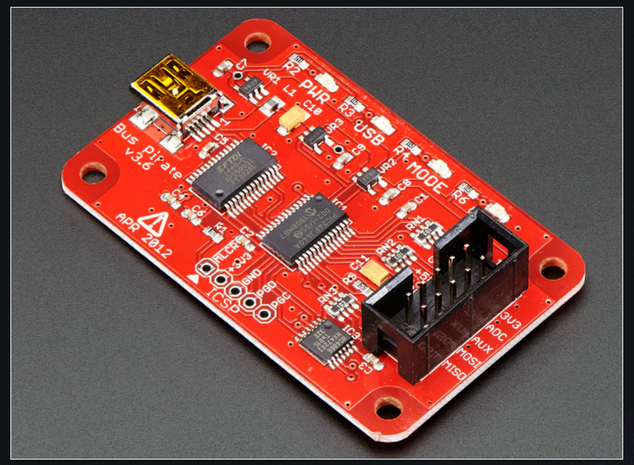
Xeltek SuperPro

Elnec BeeProg

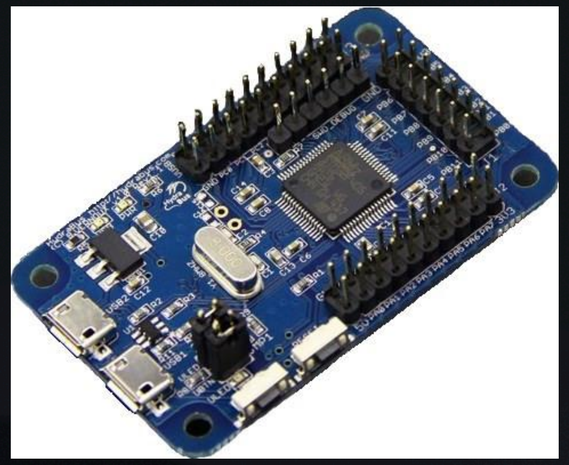


CH341A-based Programmer

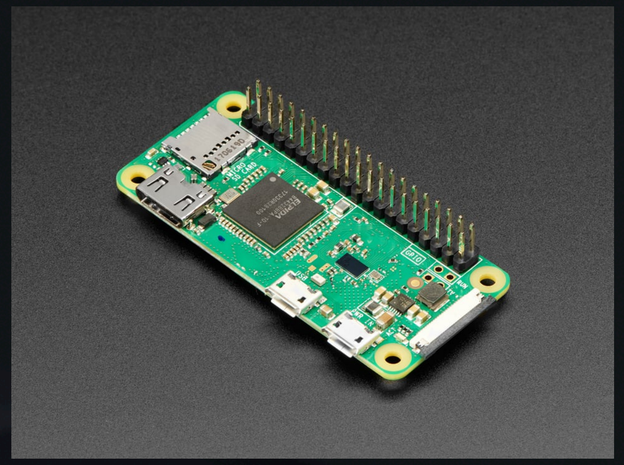
!(Hard)ware - SPI



Bus Pirate



HydraBus



Raspberry Pi Zero

!(Hard)ware - SPI

Means "reading"

```
sudo flashrom --programmer ch341a_spi -r firmware.bin
```

Just because we have to

The output file

The chip used by our programmer

!(Hard)ware - SPI

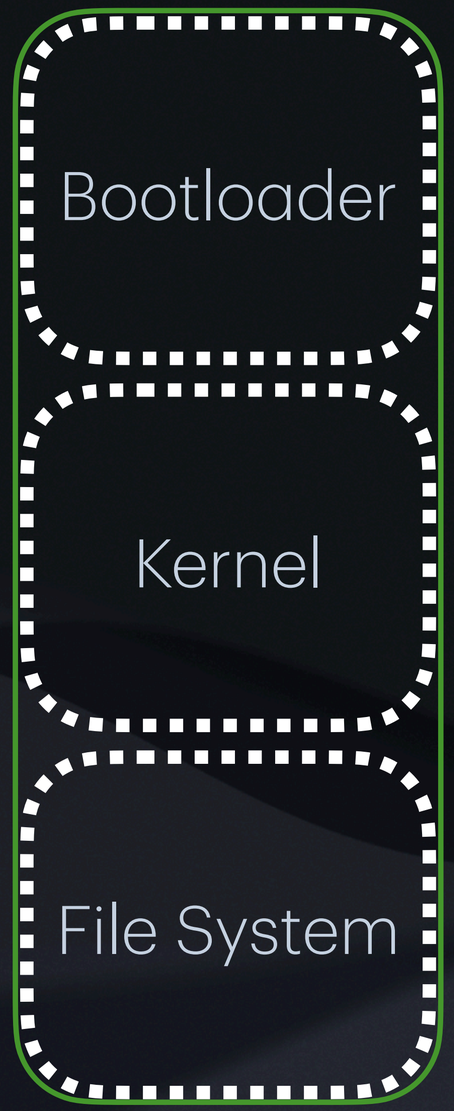
```
flashrom v1.2 on Linux 5.4.0-53-generic (x86_64)
flashrom is free software, get the source code at https://flashrom.org

Using clock_gettime for delay loops (clk_id: 1, resolution: 1ns).
Bus Pirate firmware 6.1 and older does not support SPI speeds above 2 MHz. Limiting speed to 2 MHz.
It is recommended to upgrade to firmware 6.2 or newer.
Found Winbond flash chip "W25Q16.V" (2048 kB, SPI) on buspirate_spi.
Reading flash... done.
```

Firmware analysis

Firmware analysis

Embedded Linux

This is what we're after!



Firmware analysis

SquashFS

CramFS

RomFS

Firmware analysis

ReFirmLabs/
binwalk

Firmware Analysis Tool

69 Contributors | 2k Used by | 11k Stars | 2k Forks

Firmware analysis

```
binwalk -Mre firmware.bin
```

Firmware analysis

```
binwalk -Mre firmware.bin
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
54096         0xD350          U-Boot version string, "U-Boot 1.1.3 (Jan 20 2022
- 15:15:35)"
66560         0x10400         LZMA compressed data, properties: 0x5D,
dictionary size: 8388608 bytes, uncompressed size: 2986732 bytes
1049088       0x100200        Squashfs filesystem, little endian, version 4.0,
compression:xz, size: 2873020 bytes, 552 inodes, blocksize: 524288 bytes,
created: 2022-01-20 07:26:57
```

Firmware analysis

```
cd _firmware.bin.extracted/squashfs-root/
ls
bin  dev  etc  lib  linuxrc  mnt  proc  sbin  sys  usr  var  web
```

Firmware analysis

```
cd _firmware.bin.extracted/squashfs-root/
ls
bin  dev  etc  lib  linuxrc  mnt  proc  sbin  sys  usr  var  web
```

Secret keys

Hardcoded credentials

Config files

Web interfaces

Vulnerable libraries

Firmware analysis

```
grep -r "BEGIN RSA PRIVATE KEY" [fw_path]

grep -r -E "([0-9]{1,3}\.){3}[0-9]{1,3}" [fw_path]

grep -r -i "backdoor" [fw_path]
```

Yeah why not!?

Firmware analysis

D-Link

Security **Announcement**

Announcement > SAP10001

DI-524/524UP/604+/604UP/624S, DIR-100/120, and TM-G524G authenticate administrative access using specific User-Agent string resulting in a stack-overflow vulnerability

Overview

Various D-Link routers allow administrative web actions if the HTTP request contains a specific User-Agent string. This backdoor allows an attacker to bypass password authentication and access the router's administrative web interface. Exlploiting these vulnerability may cause the device to become unstable and unreliable. Planex and Alpha Networks devices may also be affected, please contact these vendors directly at their regional websites.

Overview

Various D-Link routers allow administrative web actions if the HTTP request contains a specific User-Agent string. This backdoor allows an attacker to bypass password authentication and access the router's administrative web interface. Exlploiting these vulnerability may cause the device to become unstable and unreliable. Planex and Alpha Networks devices may also be affected, please contact these vendors directly at their regional websites.

D-Link Security Incident Reponse Policy

All public communication on this issue will be offered at http://securityadvisories.dlink.com/security/
Our security response team can be contacted for incident information or to report incidents at security@dlink.com
Any non-critical security issue, help in updating firmware, or configuration regarding this issue please contact your D-Link Customer care channel.

Reference

Patch diffing

CVE-2013-2645

CVSS 9.3

CWE-352 (CSRF)

http://192.168.1.1/userRpm/LanDhcpServerRpm.htm?
dhcpserver=1&ip1=192.168.1.100&ip2=192.168.1.199&Lease=120&gateway=0.0.0.0&domain=&dnsserver=8.8.4.4
&dnsserver2=8.8.8.8&Save=%B1%A3+%B4%E6

Exploit!

Patch diffing

Extract both firmware blobs

Open them up with kdiff3

Check the vulnerable page(s) for changes

Figure out where the issue is

There you have it!

Lab 1 / Patch diffing

https://github.com/winsl0w-io/BSidesTirana2024/patch_diffing

Hardcoded credentials

Use grep to find references to telnet

Inspect files that actually do reference it

Check for credentials

Figure out where the issue is

There you have it!

Lab 2 / Hardcoded credentials

https://github.com/winsl0w-io/BSidesTirana2024/dlink_backdoor

That's a wrap!

Questions ?

trainings@winsl0w.io

Oh yeah, that's a **zero**