BREAKING ALL THE THINGS — A SYSTEMATIC SURVEY OF FIRMWARE EXTRACTION TECHNIQUES FOR IOT DEVICES

SEBASTIAN VASILE, DAVID OSWALD, TOM CHOTHIA

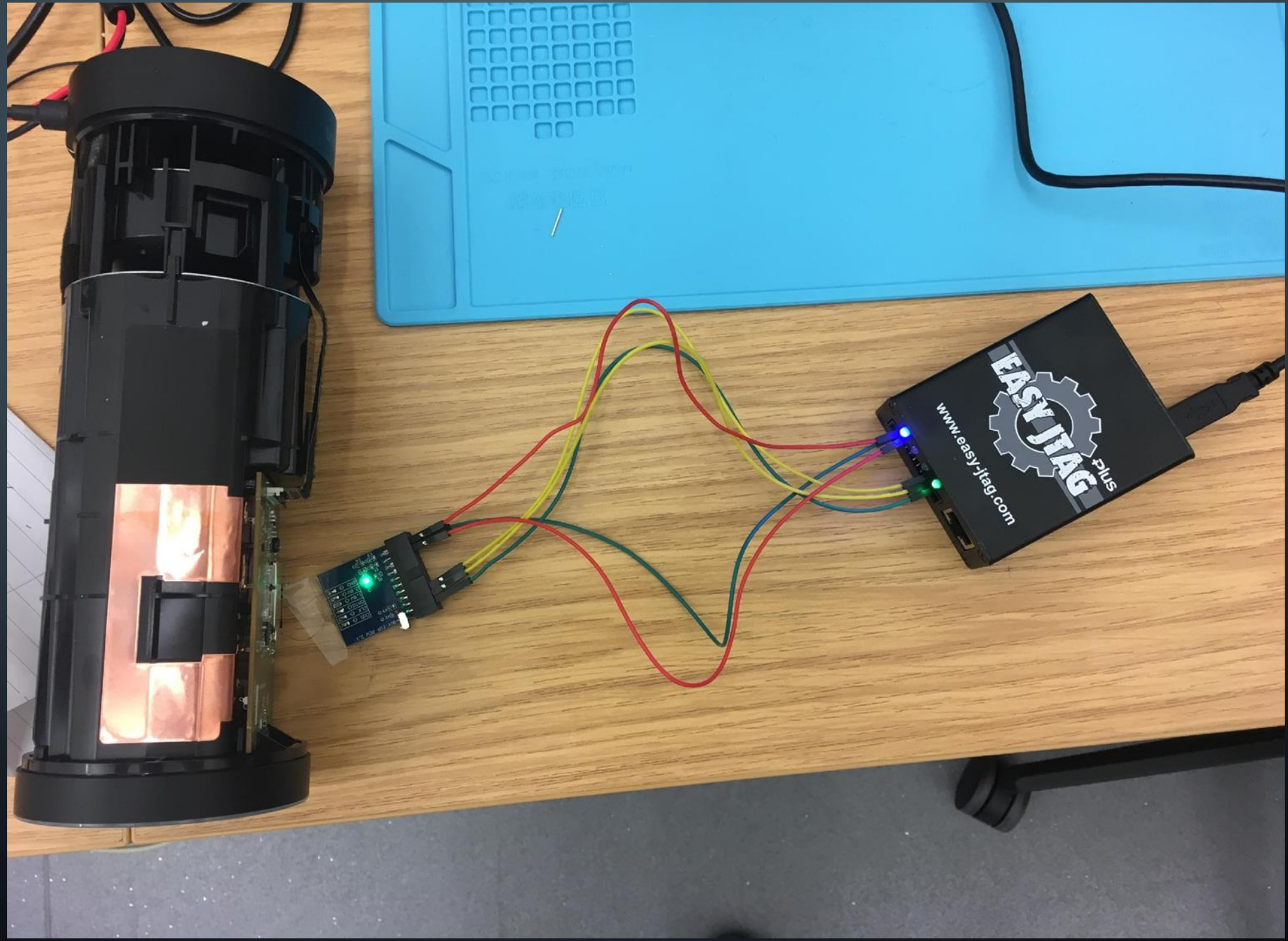
UNIVERSITY OF BIRMINGHAM

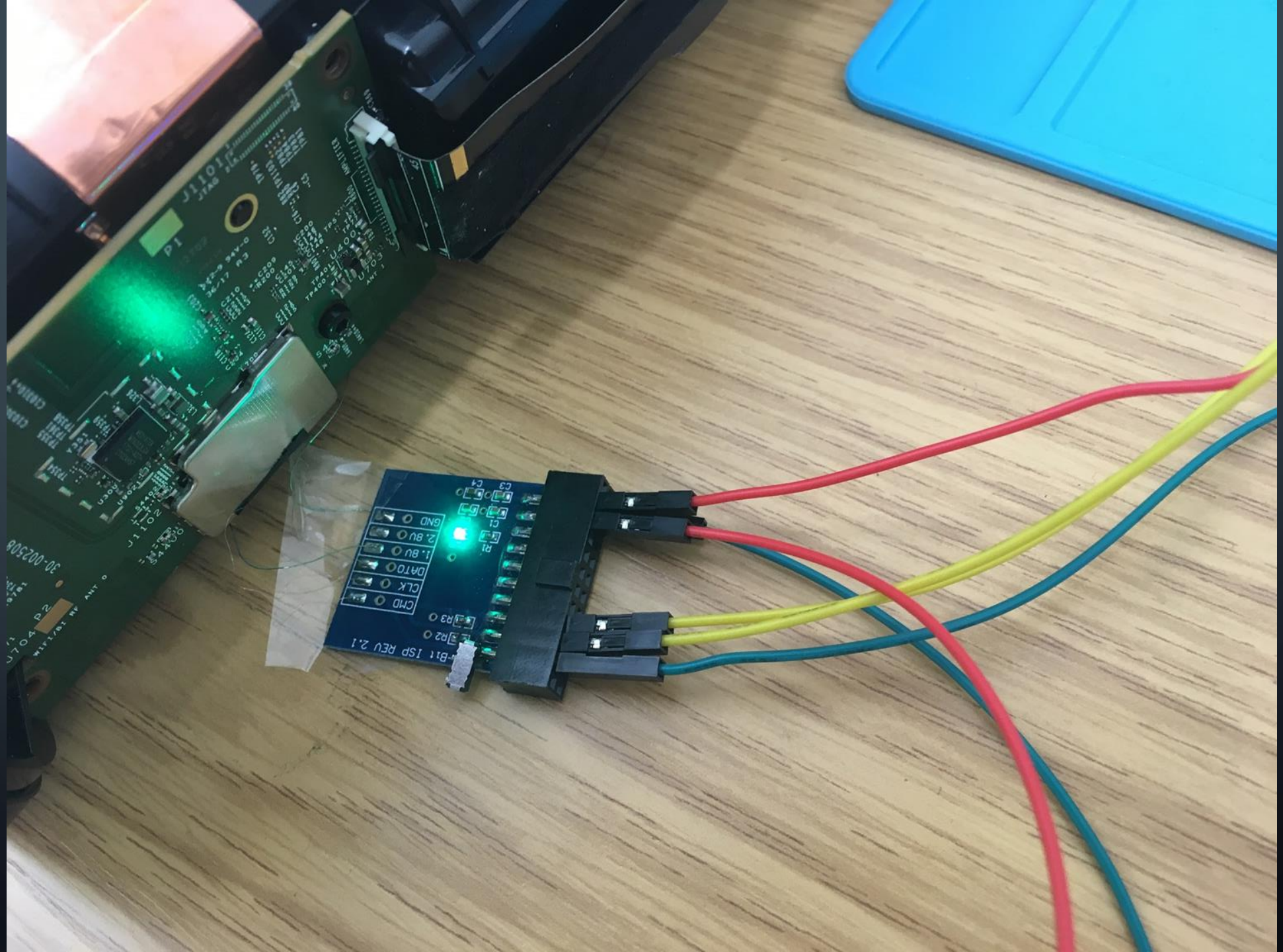
QUICK BREAKDOWN

- Purpose of firmware extraction
- Firmware extraction methods
- Survey results
- Countermeasures

WHY DOES IT MATTER?

- Analyze device functionality
- Find vulnerabilities
- Steal IP
- Supply chain attack


EASY JTAG
plus
www.easy-jtag.com


GND
2.8V
1.8V
DAT0
CLK
CMD
R3
R2
R1
C3
C4
C1

FIRMWARE EXTRACTION METHODS

- Software
- Hardware

FIRMWARE EXTRACTION METHODS

- Software
  - Check manufacturer's website
- Hardware

Setup Video | FAQ | Firmware | Apps | GPL Code

Emulators

Firmware

A firmware update can resolve issues that the previous firmware version may have and improve its current performance.

To Upgrade

IMPORTANT: To prevent upgrade failures, please read the following before proceeding with the upgrade process

- Please upgrade firmware from the local TP-Link official website of the purchase location for your TP-Link device, otherwise it will be against the warranty. Please click here to change site if necessary.
- Please verify the hardware version of your device for the firmware version. Wrong firmware upgrade may damage your device and void the warranty. （Normally V1.x=V1）
  How to find the hardware version on a TP-Link device?
- Do NOT turn off the power during the upgrade process, as it may cause permanent damage to the product.
- Do NOT upgrade the firmware through wireless connection unless there is no LAN/Ethernet port on the TP-link device. For LTE-MiFi, it is recommended to upgrade via USB port.
- It's recommended that users stop all Internet applications on the computer, or simply disconnect Internet line from the device before the upgrade.
- Use decompression software such as WinZIP or WinRAR to extract the file you download before the upgrade.

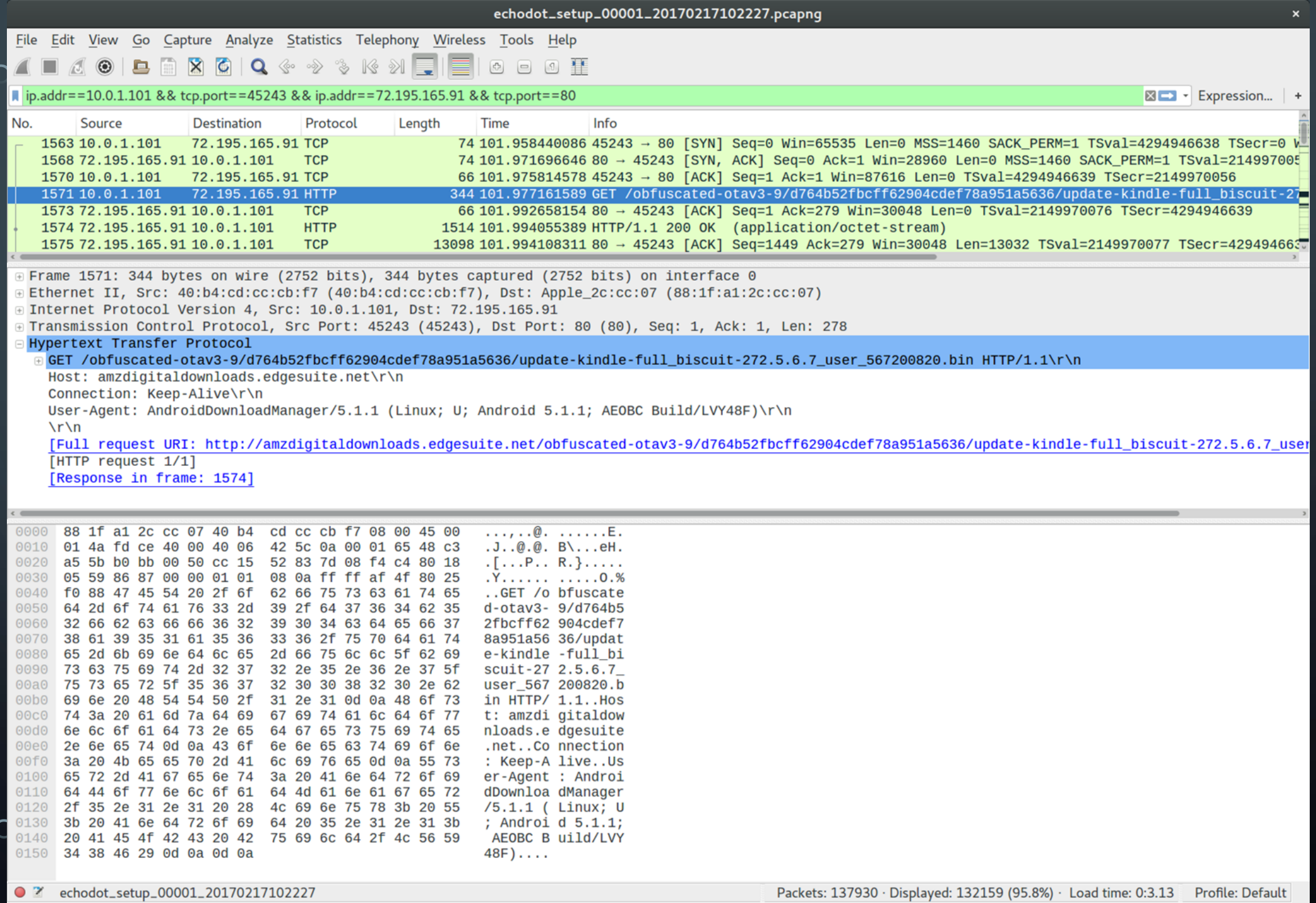
TL-WR841N(EU)_V13_180119		
Published Date: 2018-02-24	Language: English	File Size: 4.73 MB

Modification and Bug Fixes:

1. Fixed WPA2 (KRACKs) vulnerability.
2. Fixed the bug that router cannot forward some specific DNS requests.
3. Shorten the interval time to reconnect to PPPoE server after disconnection.
4. Improved the stability of Quick Setup.

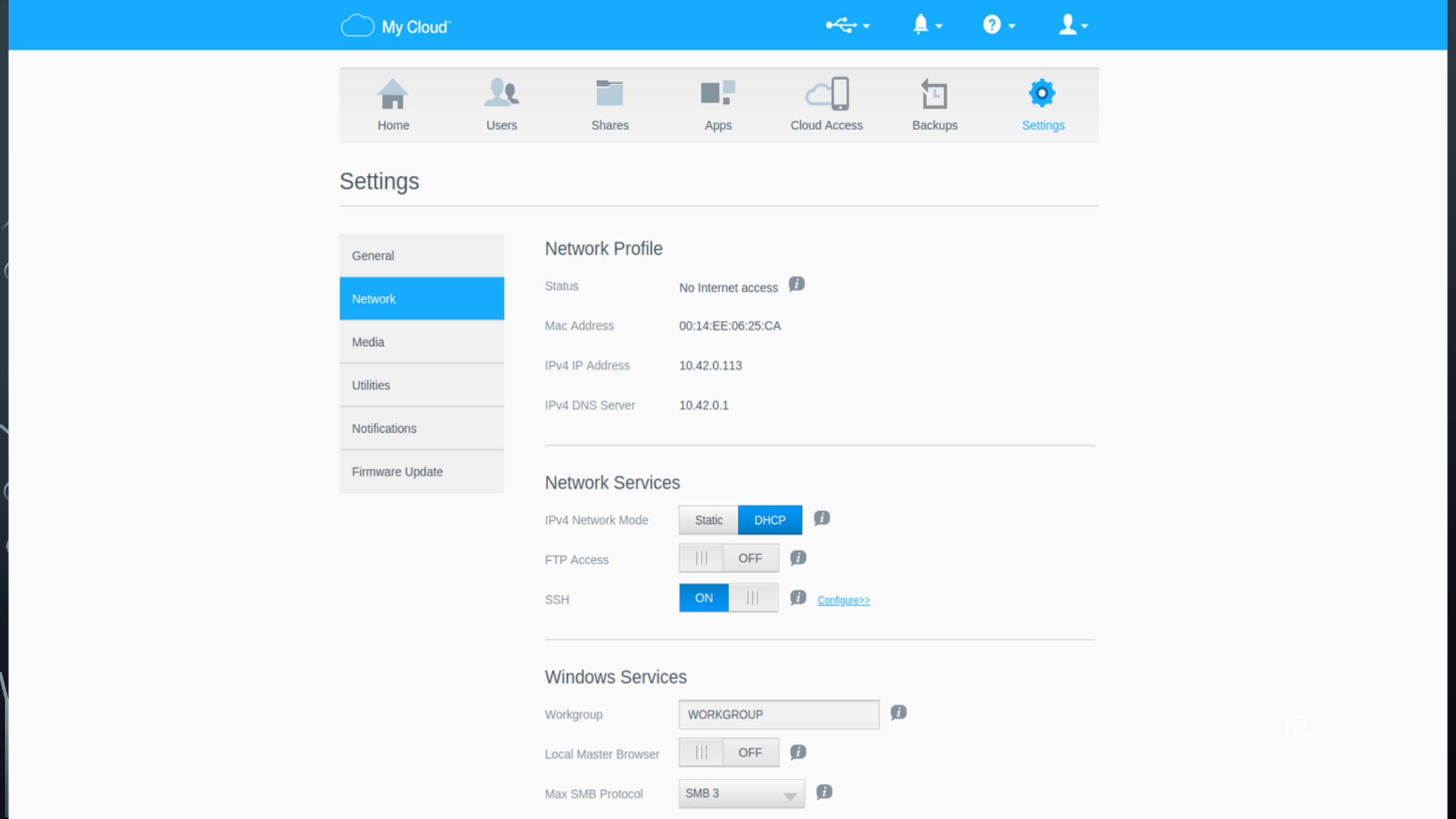
FIRMWARE EXTRACTION METHODS

- Software
  - Check manufacturer’s website
  - Intercept firmware updates
- Hardware


echodot_setup_00001_20170217102227.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==10.0.1.101 && tcp.port==45243 && ip.addr==72.195.165.91 && tcp.port==80
Expression...
No. Source Destination Protocol Length Time Info
1563 10.0.1.101 72.195.165.91 TCP 74 101.958440086 45243 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=4294946638 TSecr=0
1568 72.195.165.91 10.0.1.101 TCP 74 101.971696646 80 → 45243 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=214997005
1570 10.0.1.101 72.195.165.91 TCP 66 101.975814578 45243 → 80 [ACK] Seq=1 Ack=1 Win=87616 Len=0 TSval=4294946639 TSecr=2149970056
1571 10.0.1.101 72.195.165.91 HTTP 344 101.977161589 GET /obfuscated-otav3-9/d764b52fbcff62904cdef78a951a5636/update-kindle-full_biscuit-27
1573 72.195.165.91 10.0.1.101 TCP 66 101.992658154 80 → 45243 [ACK] Seq=1 Ack=279 Win=30048 Len=0 TSval=2149970076 TSecr=4294946639
1574 72.195.165.91 10.0.1.101 HTTP 1514 101.994055389 HTTP/1.1 200 OK (application/octet-stream)
1575 72.195.165.91 10.0.1.101 TCP 13098 101.994108311 80 → 45243 [ACK] Seq=1449 Ack=279 Win=30048 Len=13032 TSval=2149970077 TSecr=42949466
Frame 1571: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface 0
Ethernet II, Src: 40:b4:cd:cc:cb:f7 (40:b4:cd:cc:cb:f7), Dst: Apple_2c:cc:07 (88:1f:a1:2c:cc:07)
Internet Protocol Version 4, Src: 10.0.1.101, Dst: 72.195.165.91
Transmission Control Protocol, Src Port: 45243 (45243), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 278
Hypertext Transfer Protocol
GET /obfuscated-otav3-9/d764b52fbcff62904cdef78a951a5636/update-kindle-full_biscuit-272.5.6.7_user_567200820.bin HTTP/1.1\r\n
Host: amzdigitaldownloads.edgesuite.net\r\n
Connection: Keep-Alive\r\n
User-Agent: AndroidDownloadManager/5.1.1 (Linux; U; Android 5.1.1; AEOBC Build/LVY48F)\r\n
\r\n
[Full request URI: http://amzdigitaldownloads.edgesuite.net/obfuscated-otav3-9/d764b52fbcff62904cdef78a951a5636/update-kindle-full_biscuit-272.5.6.7_user
[HTTP request 1/1]
[Response in frame: 1574]
0000 88 1f a1 2c cc 07 40 b4 cd cc cb f7 08 00 45 00 ...,..@. ......E.
0010 01 4a fd ce 40 00 40 06 42 5c 0a 00 01 65 48 c3 .J..@.@. B\...eH.
0020 a5 5b b0 bb 00 50 cc 15 52 83 7d 08 f4 c4 80 18 .[...P.. R.}.....
0030 05 59 86 87 00 00 01 01 08 0a ff ff af 4f 80 25 .Y...... .....O.%
0040 f0 88 47 45 54 20 2f 6f 62 66 75 73 63 61 74 65 ..GET /o bfuscate
0050 64 2d 6f 74 61 76 33 2d 39 2f 64 37 36 34 62 35 d-otav3- 9/d764b5
0060 32 66 62 63 66 66 36 32 39 30 34 63 64 65 66 37 2fbcff62 904cdef7
0070 38 61 39 35 31 61 35 36 33 36 2f 75 70 64 61 74 8a951a56 36/updat
0080 65 2d 6b 69 6e 64 6c 65 2d 66 75 6c 6c 5f 62 69 e-kindle -full_bi
0090 73 63 75 69 74 2d 32 37 32 2e 35 2e 36 2e 37 5f scuit-27 2.5.6.7_
00a0 75 73 65 72 5f 35 36 37 32 30 30 38 32 30 2e 62 user_567 200820.b
00b0 69 6e 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 in HTTP/ 1.1..Hos
00c0 74 3a 20 61 6d 7a 64 69 67 69 74 61 6c 64 6f 77 t: amzdi gitaldow
00d0 6e 6c 6f 61 64 73 2e 65 64 67 65 73 75 69 74 65 nloads.e dgesuite
00e0 2e 6e 65 74 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e .net..Co nnection
00f0 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 55 73 : Keep-A live..Us
0100 65 72 2d 41 67 65 6e 74 3a 20 41 6e 64 72 6f 69 er-Agent : Androi
0110 64 44 6f 77 6e 6c 6f 61 64 4d 61 6e 61 67 65 72 dDownloa dManager
0120 2f 35 2e 31 2e 31 20 28 4c 69 6e 75 78 3b 20 55 /5.1.1 (Linux; U
0130 3b 20 41 6e 64 72 6f 69 64 20 35 2e 31 2e 31 3b ; Androi d 5.1.1;
0140 20 41 45 4f 42 43 20 42 75 69 6c 64 2f 4c 56 59 AEOBC B uild/LVY
0150 34 38 46 29 0d 0a 0d 0a 48F)....
echodot_setup_00001_20170217102227
Packets: 137930 · Displayed: 132159 (95.8%) · Load time: 0:3.13
Profile: Default

FIRMWARE EXTRACTION METHODS

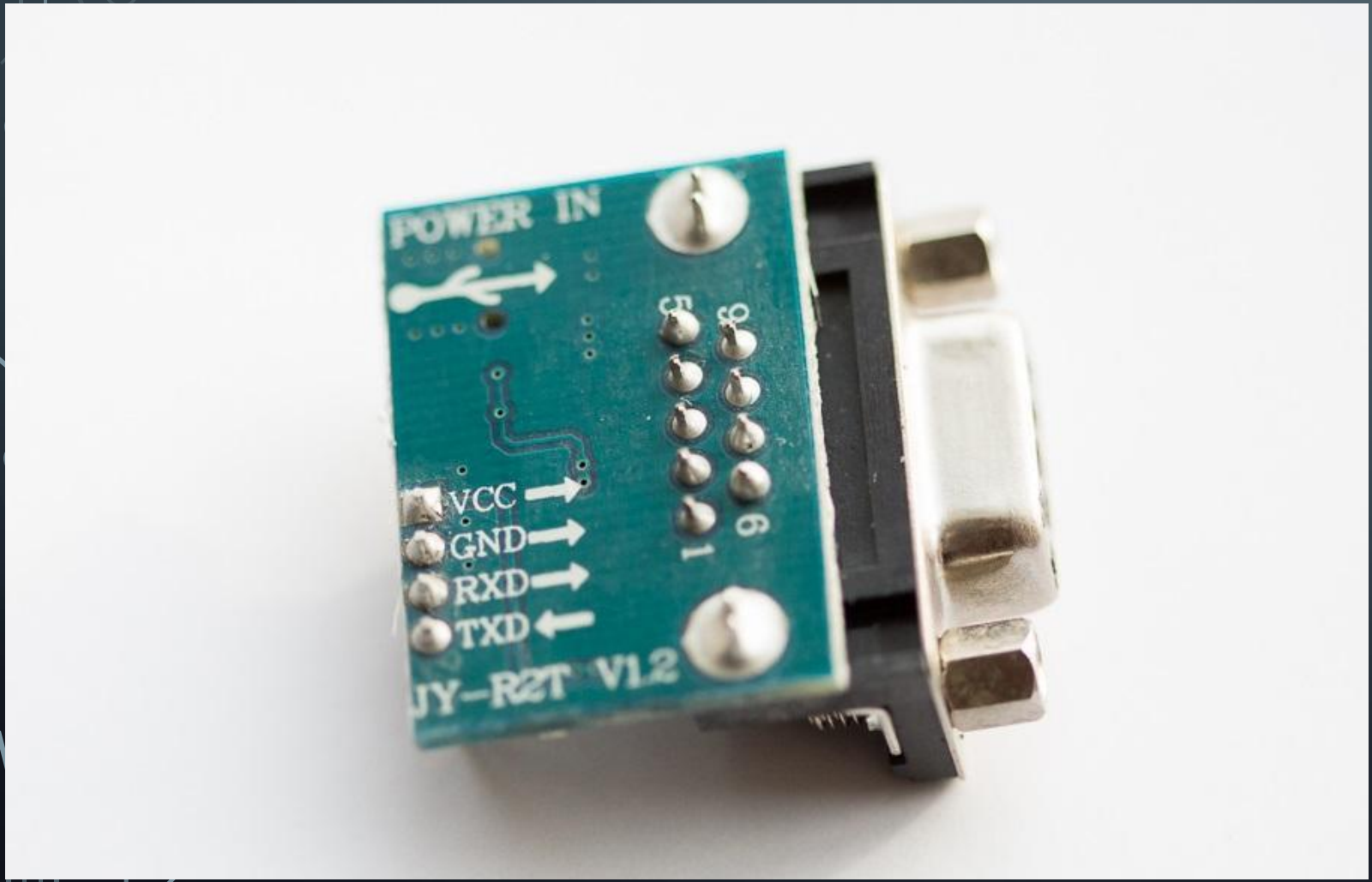
- Software
  - Check manufacturer's website
  - Intercept firmware updates
  - Leverage/exploit running services (Telnet, SSH, FTP, etc.)
- Hardware


My Cloud
Home
Users
Shares
Apps
Cloud Access
Backups
Settings
Settings
General
Network
Media
Utilities
Notifications
Firmware Update
Network Profile
Status
No Internet access
Mac Address
00:14:EE:06:25:CA
IPv4 IP Address
10.42.0.113
IPv4 DNS Server
10.42.0.1
Network Services
IPv4 Network Mode
Static
DHCP
FTP Access
OFF
SSH
ON
Configure>>
Windows Services
Workgroup
WORKGROUP
Local Master Browser
OFF
Max SMB Protocol
SMB 3

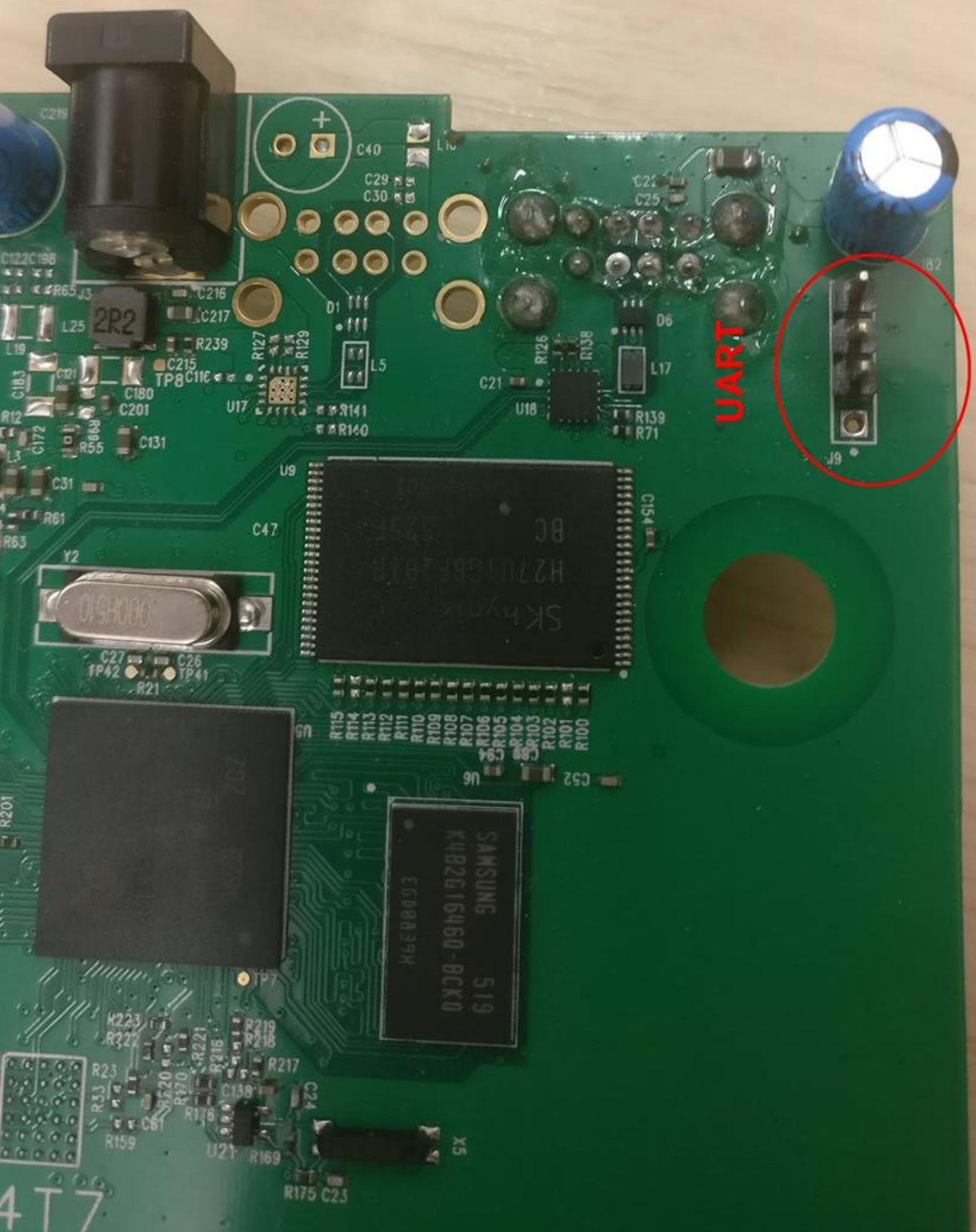
FIRMWARE EXTRACTION METHODS

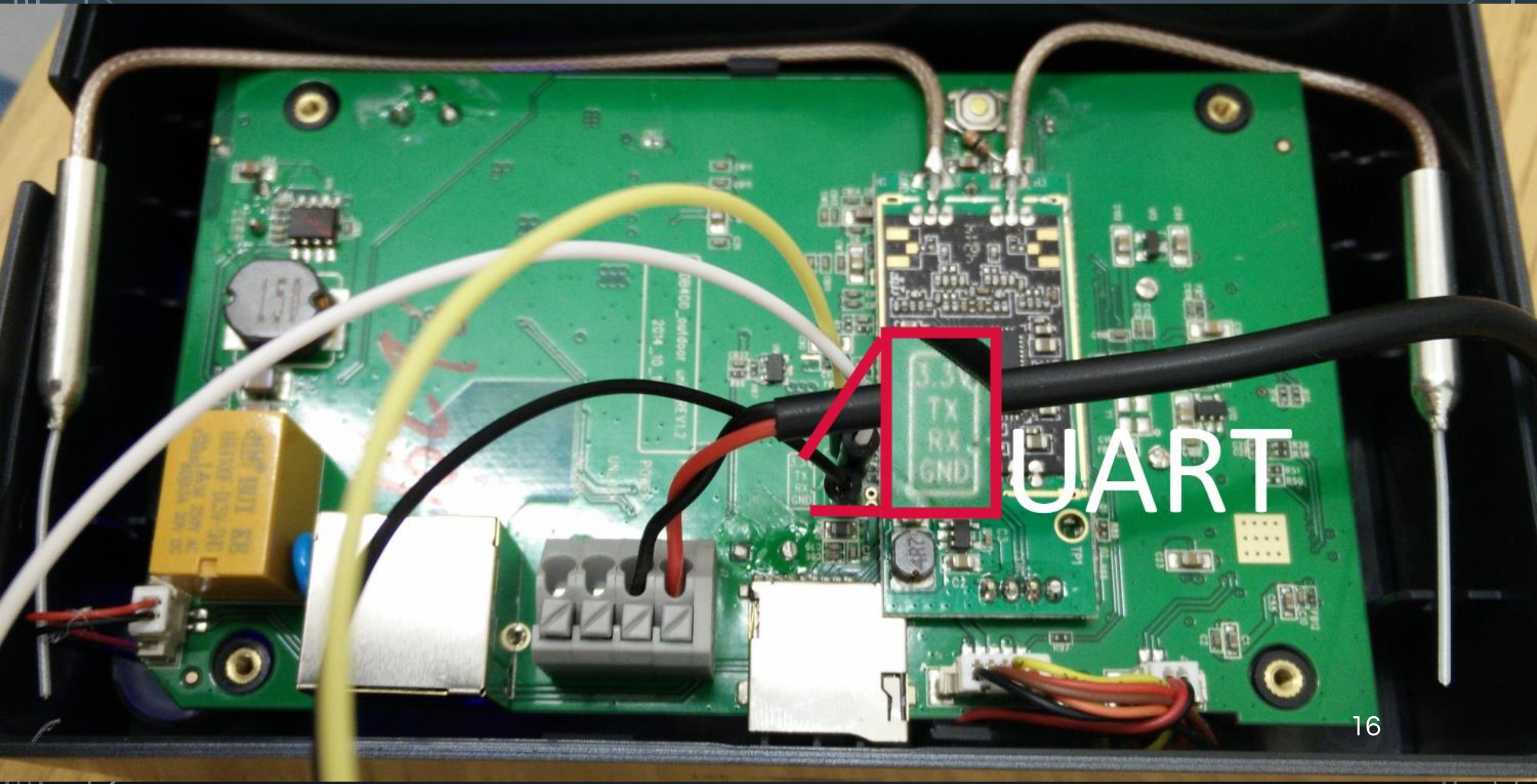
- Software
- Hardware
  - UART

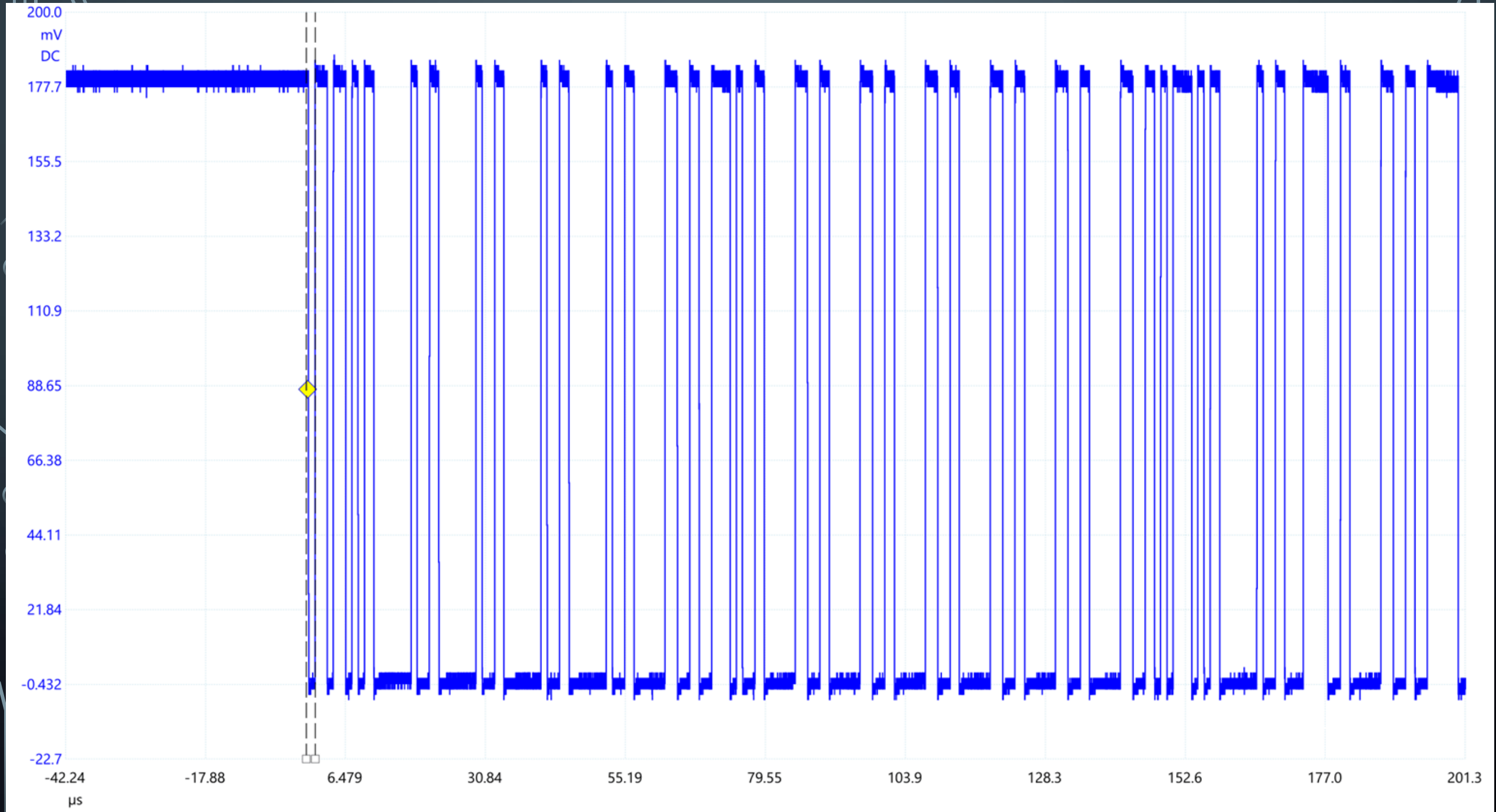
UART



- Serial comms interface
- Used for debugging
- 3 pins: GND, RX, TX + VCC


UART
J9
C40
C29
C30
C22
C25
D1
L5
D6
L17
C21
U18
U17
U9
C47
Y2
C27
C26
TP42
TP41
R21
TP7
SAMSUNG
K4B2G1646Q-BCK0
2R2
L25
C216
C217
R239
C215
TP8
C180
C201
C131
C31
R61
R63
R55
R127
R129
R141
R140
R126
R138
R139
R71
R115
R114
R113
R112
R111
R110
R109
R108
R107
R106
R105
R104
R103
R102
R101
R100
C52
R223
R222
R221
R216
R219
R218
R217
R23
R33
R159
R176
R169
R175
C23
X5
U21


3.3V
TX
RX
GND
UART


200.0
mV
DC
177.7
155.5
133.2
110.9
88.65
66.38
44.11
21.84
-0.432
-22.7
-42.24
-17.88
6.479
30.84
55.19
79.55
103.9
128.3
152.6
177.0
201.3
µs

```
[   14.170000] PPP generic driver version 2.4.2
[   14.180000] NET: Registered protocol family 24
[   14.250000] cfg80211: Calling CRDA for country: US
[   14.250000] cfg80211: Regulatory domain changed to country: US
[   14.260000] cfg80211:  DFS Master region: FCC
[   14.270000] cfg80211:   (start_freq - end_freq @ bandwidth), (max_antenna_gain, max_eirp), (dfs_cac
[   14.280000] cfg80211:   (2402000 KHz - 2472000 KHz @ 40000 KHz), (N/A, 3000 mBm), (N/A)
[   14.280000] cfg80211:   (5170000 KHz - 5250000 KHz @ 80000 KHz, 160000 KHz AUTO), (N/A, 1700 mBm),
[   14.290000] cfg80211:   (5250000 KHz - 5330000 KHz @ 80000 KHz, 160000 KHz AUTO), (N/A, 2400 mBm),
[   14.300000] cfg80211:   (5490000 KHz - 5730000 KHz @ 160000 KHz), (N/A, 2400 mBm), (0 s)
[   14.310000] cfg80211:   (5735000 KHz - 5835000 KHz @ 80000 KHz), (N/A, 3000 mBm), (N/A)
[   14.320000] cfg80211:   (57240000 KHz - 63720000 KHz @ 2160000 KHz), (N/A, 4000 mBm), (N/A)
[   14.330000] ieee80211 phy0: Atheros AR9531 Rev:2 mem=0xb8100000, irq=47

Philips-hue login: root
Password:


BusyBox v1.19.4 (2015-12-16 12:35:48 CET) built-in shell (ash)
Enter 'help' for a list of built-in commands.

 _    _ _    _ _______  ____          _    _                 ___   ___
| |  | | |  | |  ____| |  _ \        (_)  | |               |__ \ / _ \
| |__| | |  | | |__    | |_) |_ __ _  __| | __ _  ___        ) || | | |[   23.220000] random: nonblocking
|  __  | |  | |  __|   |  _ <| '__| |/ _` |/ _` |/ _ \      / / | | | |
| |  | | |__| | |____  | |_) | |  | | (_| | (_| |  __/     / /_ | |_| |
|_|  |_|\____/|______| |____/|_|  |_|\__,_|\__, |\___|    |____(_)___/
|||| //                                      __/ |                    ||   |
```

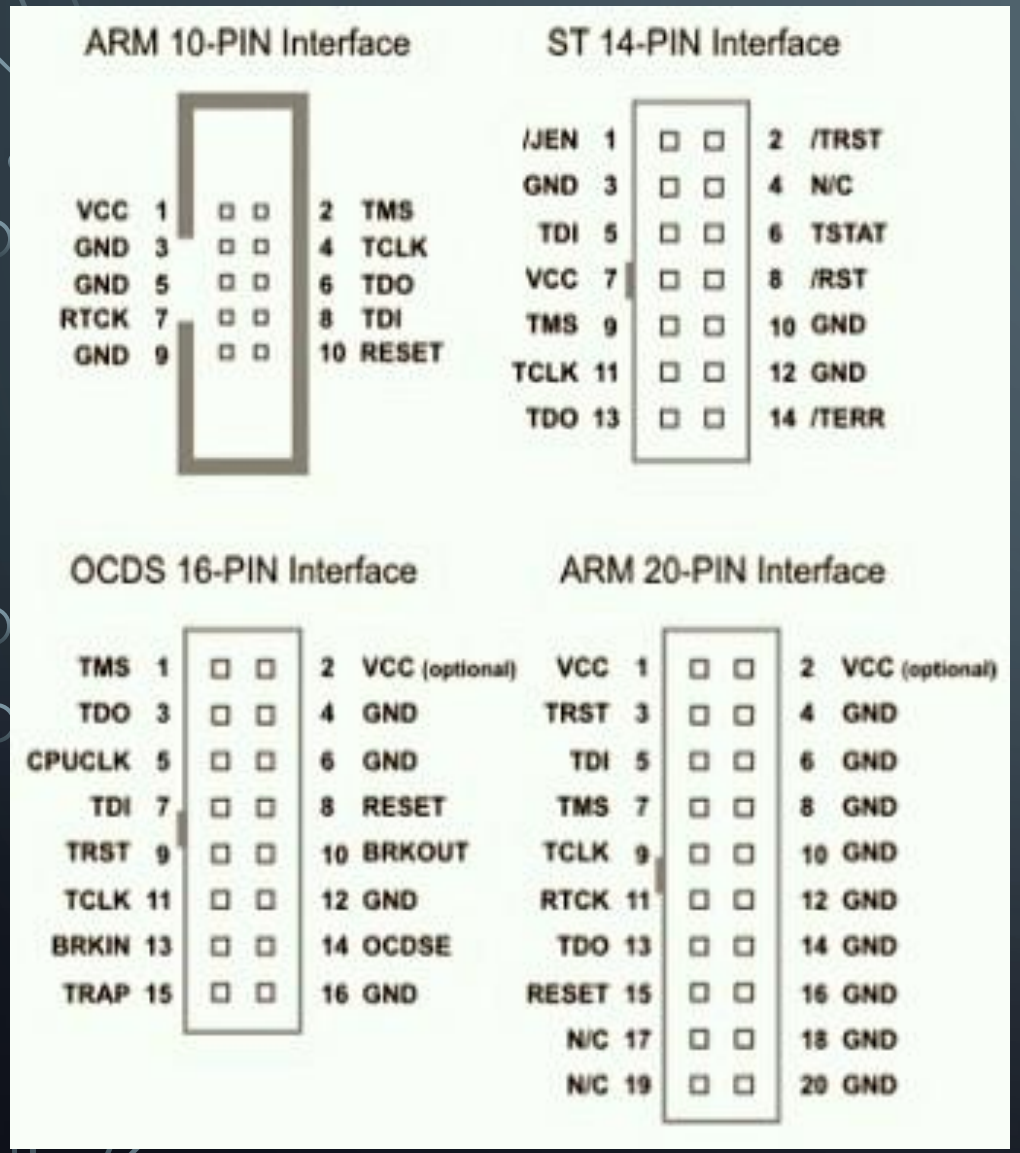
UART

- Most embedded devices run some form of busybox
- What if netcat is not available?
- All you really need is a shell and printf/echo
- Transfer missing binaries by printing binary data to file
- https://github.com/c0mpute/serial-transfer

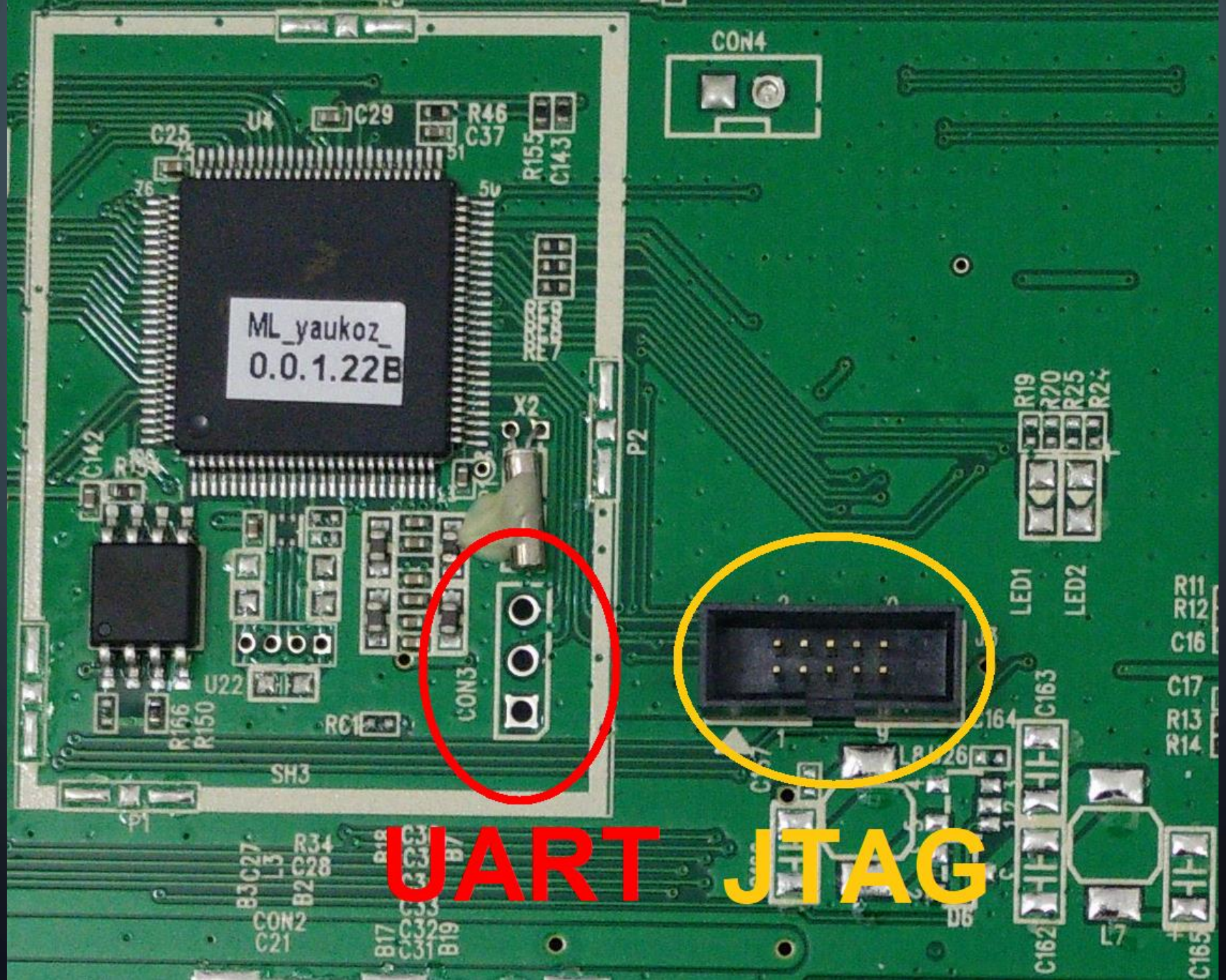
FIRMWARE EXTRACTION METHODS

- Software
- Hardware
  - UART
  - JTAG

JTAG



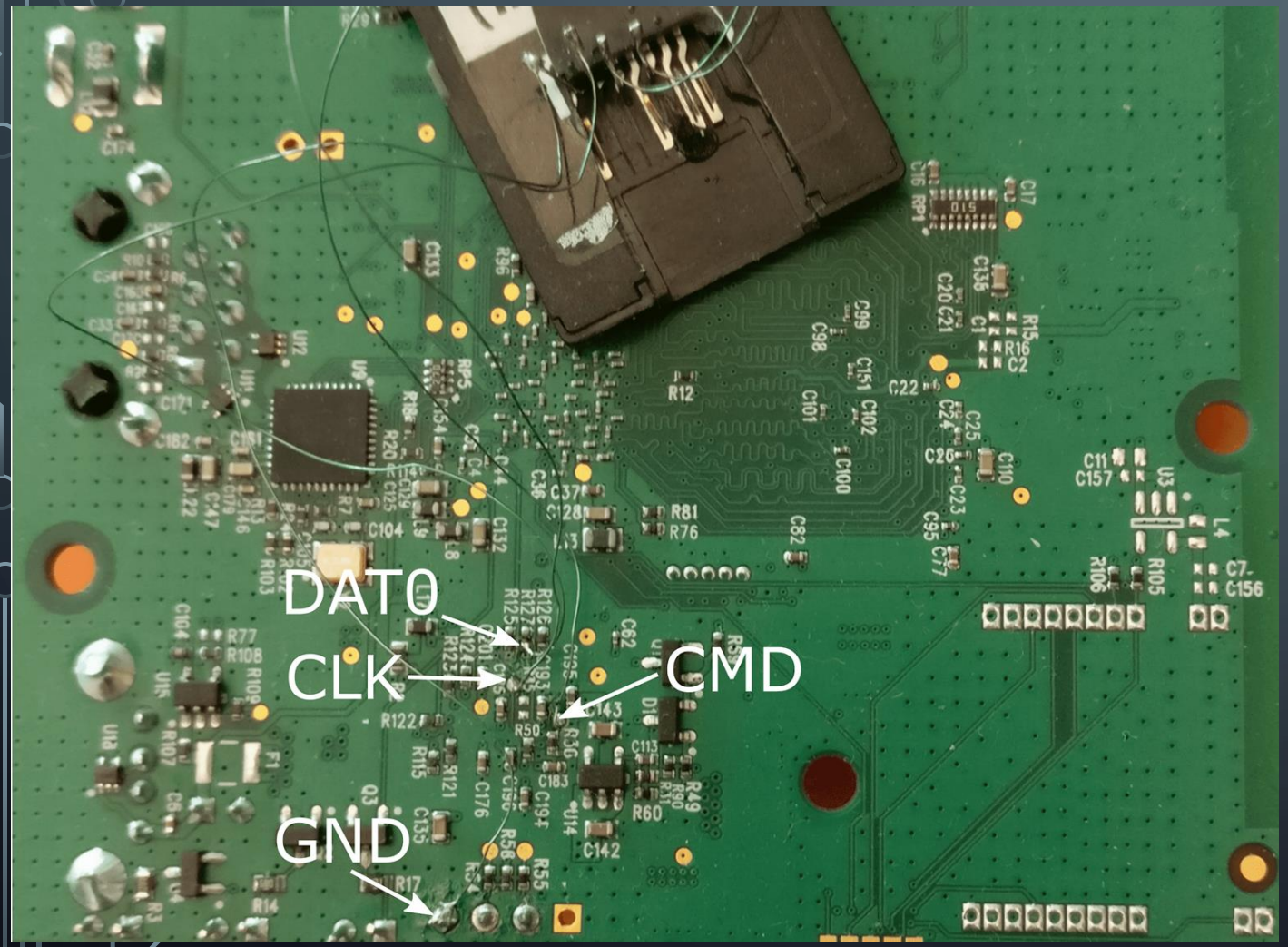
- Debugging and programming interface
- Many different pinout variations
- Official standard - 4 pins + 1 optional
- TCK, TMS, TDI, TDO + TRST


ML_yaukoz_
0.0.1.22B
CON4
CON3
UART
JTAG

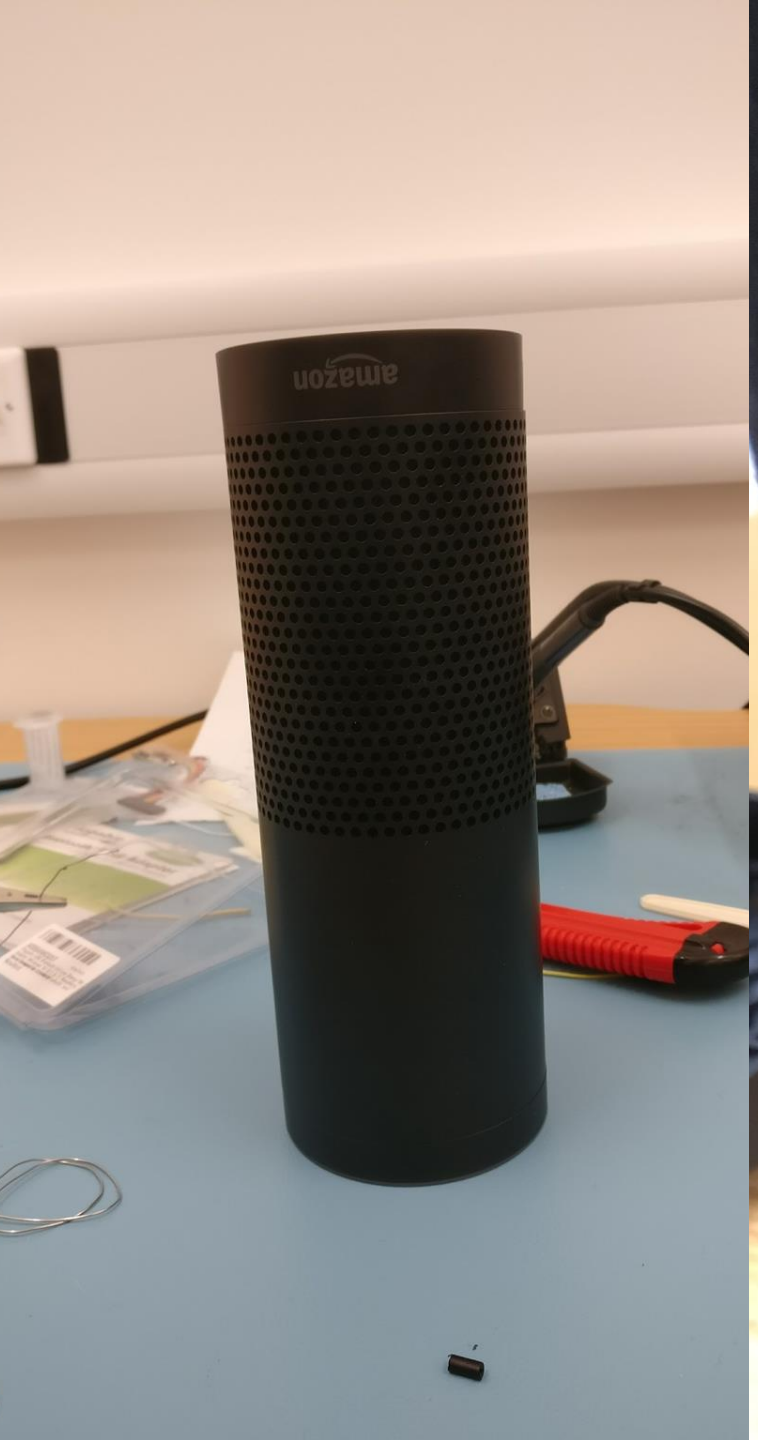
FIRMWARE EXTRACTION METHODS

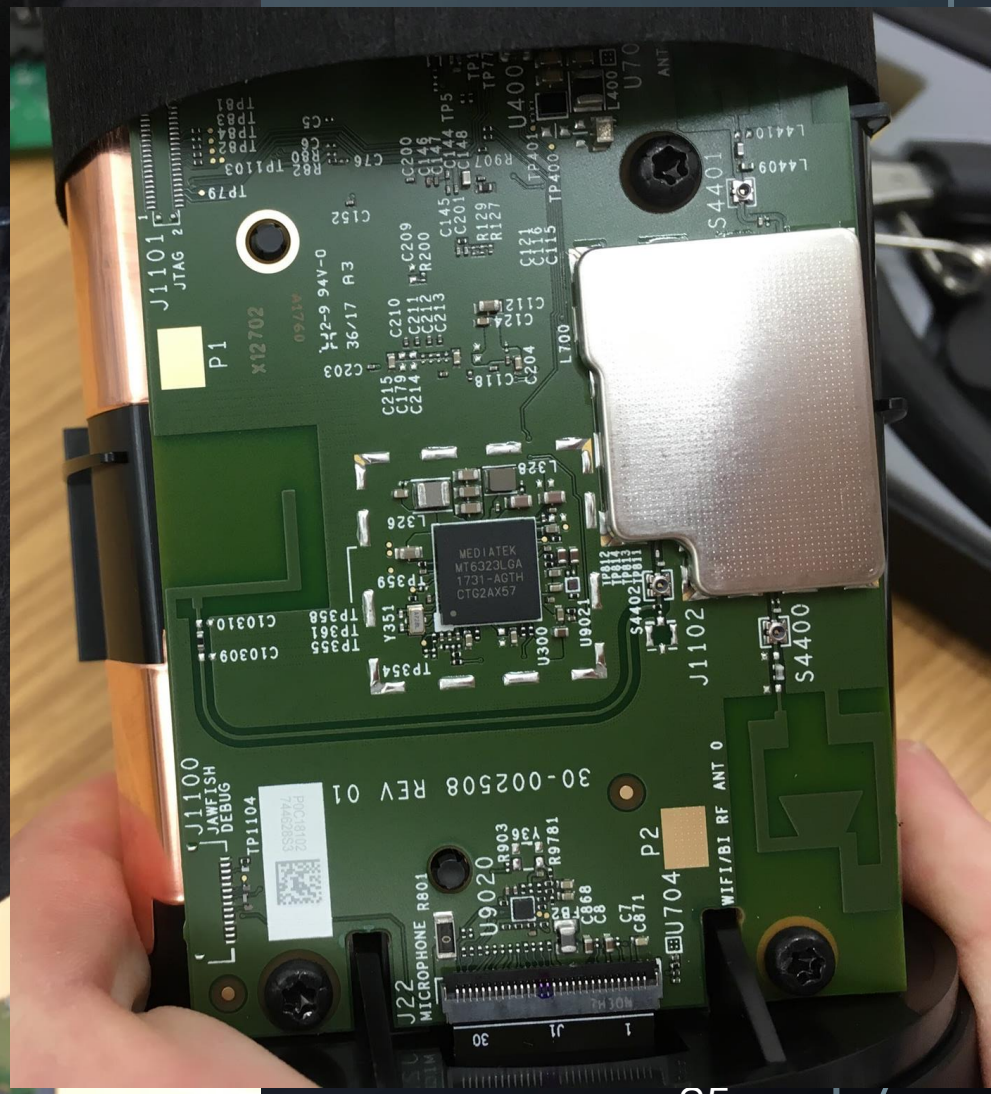
- Software
- Hardware
  - UART
  - JTAG
  - Direct flash chip memory dump (eMMC)

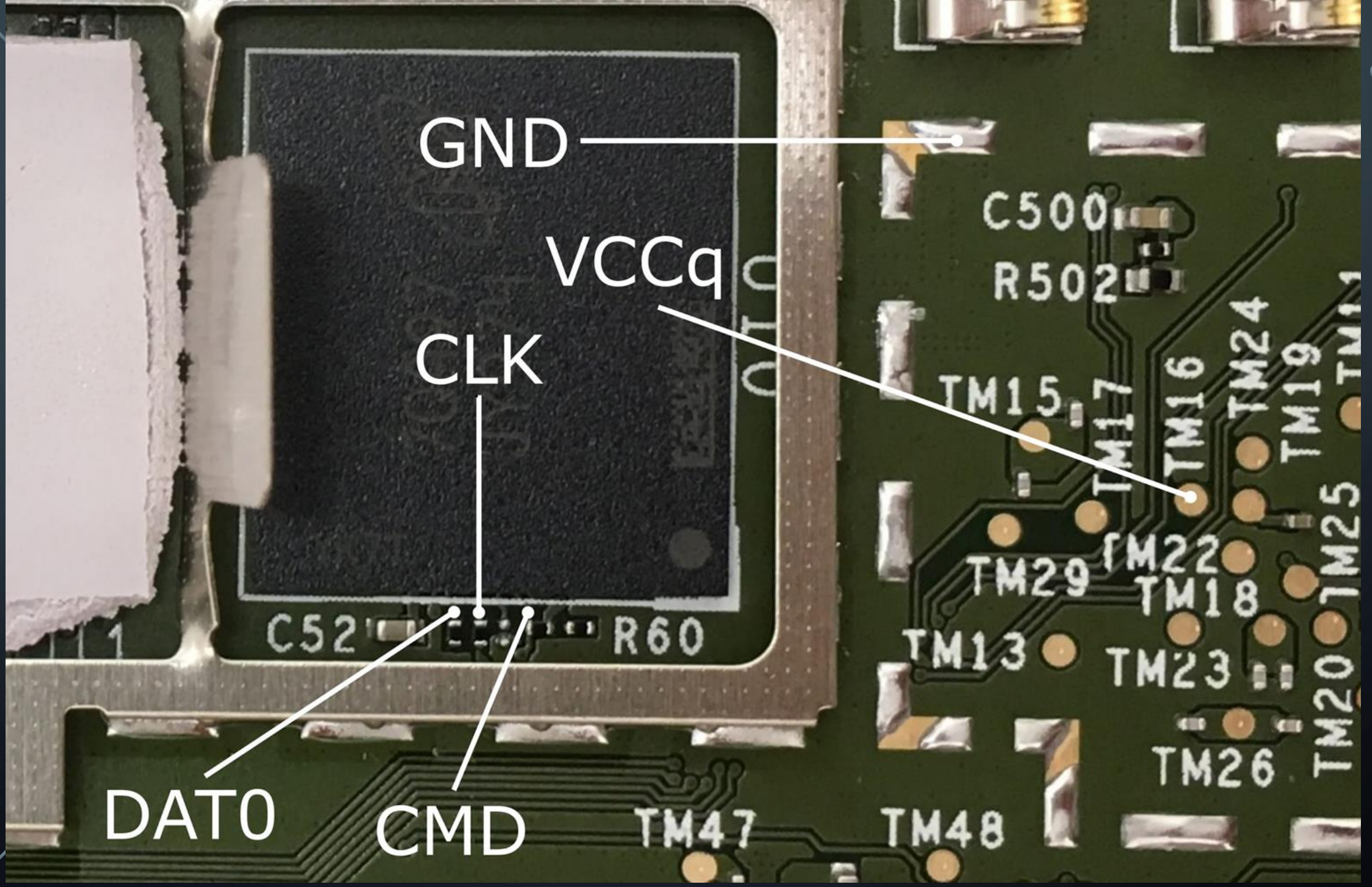
eMMC

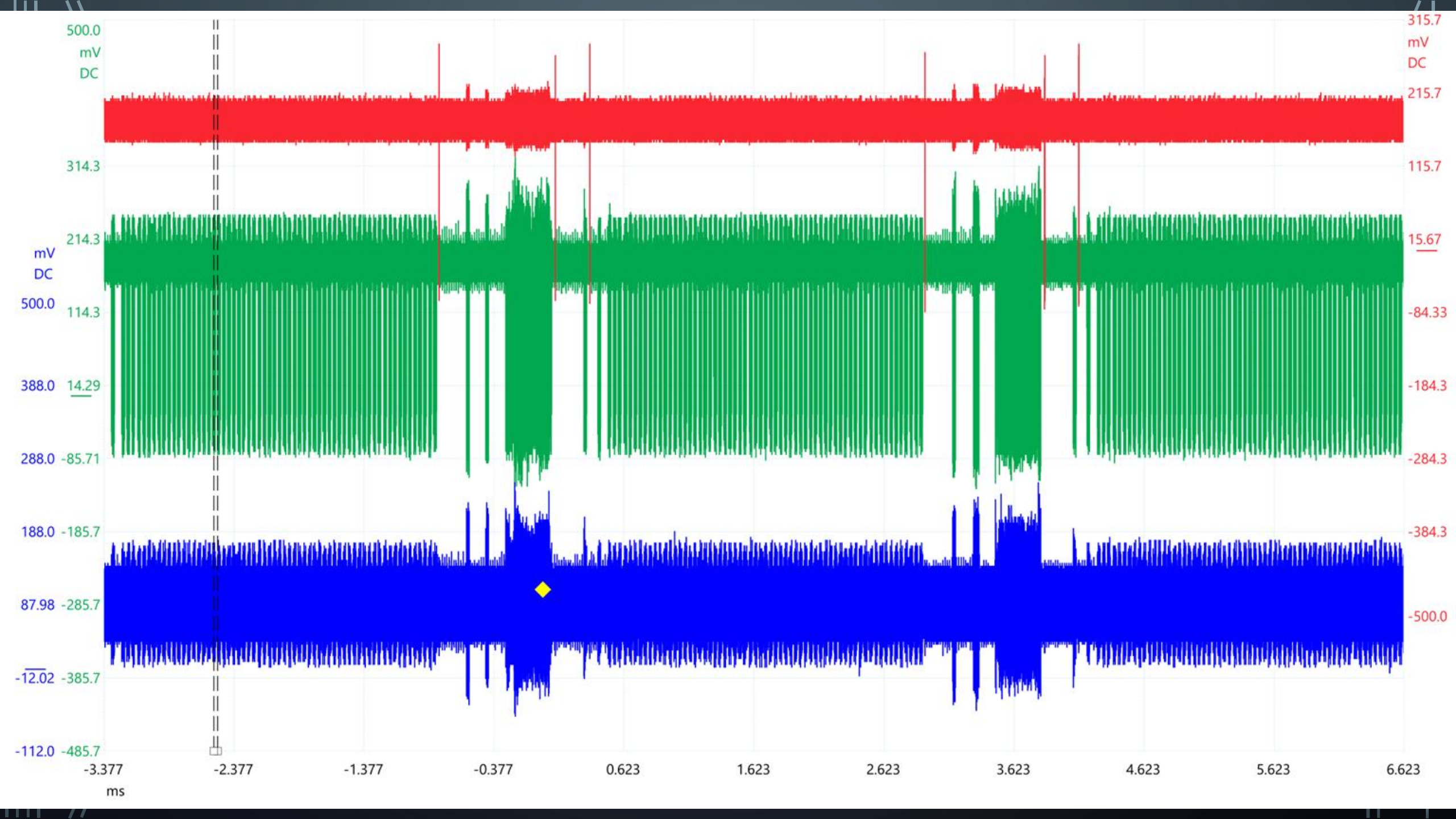


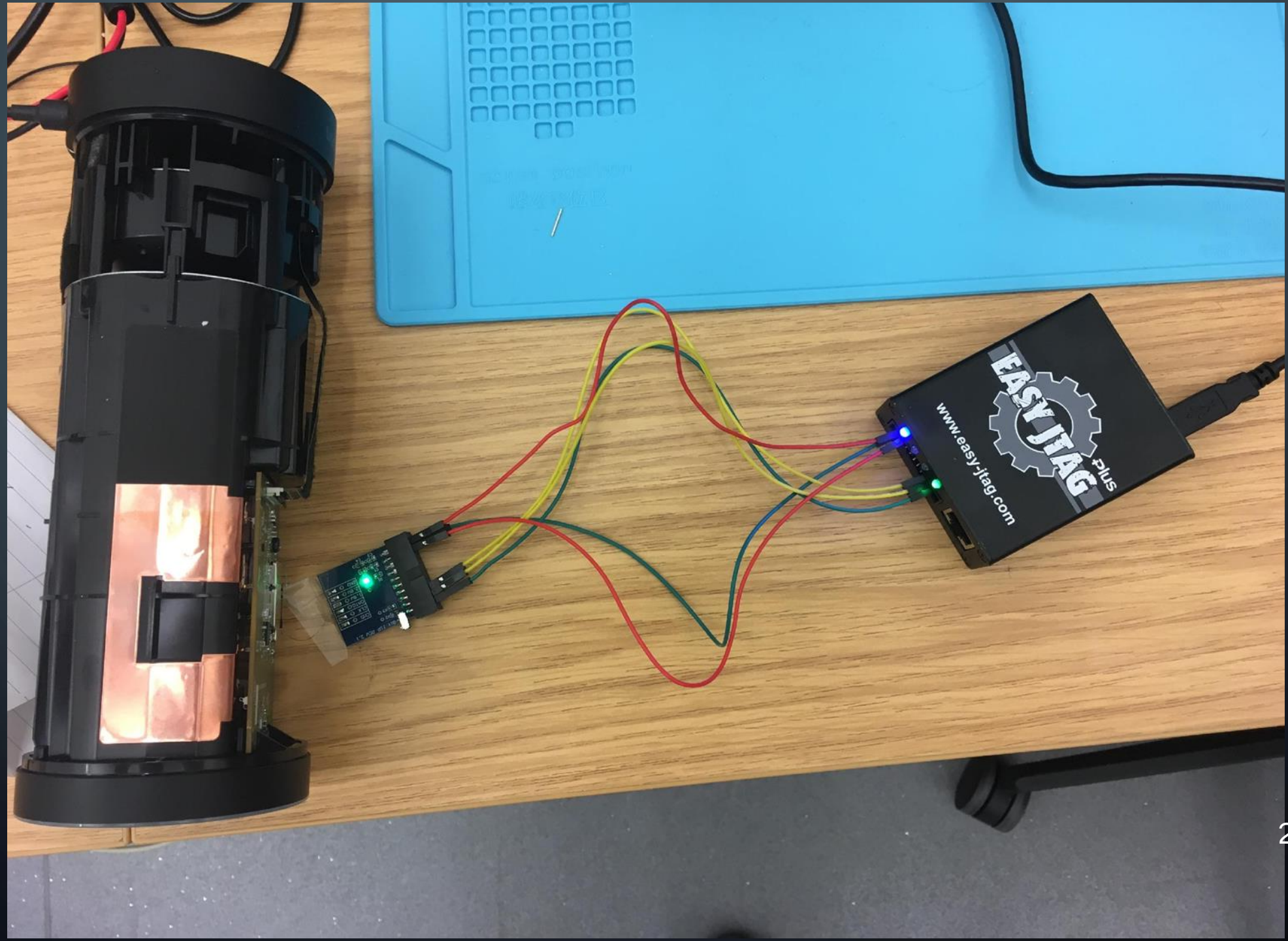
- 3 pins: DAT0, CLK, CMD + GND
- Standard package - BGA
- In-Circuit vs External dump
- In-Circuit - Identify pins with oscilloscope
- External - Look up flash chip number and datasheet


amazon


MEDIATEK
MT6323LGA
1731-AGTH
CTG2AX57
30-002508 REV 01
J1101
JTAG 2
J1102
J1100
JAWFISH
DEBUG
J22
MICROPHONE
U9020
U704
P1
P2
S4400
WIFI/BI RF ANT 0


GND
VCCq
CLK
DAT0
CMD
C500
R502
C52
R60
TM15
TM17
TM16
TM24
TM19
TM29
TM22
TM18
TM13
TM23
TM26
TM20
TM25
TM47
TM48


500.0
mV
DC
315.7
mV
DC
215.7
314.3
115.7
214.3
mV
DC
15.67
500.0
114.3
-84.33
388.0
14.29
-184.3
288.0
-85.71
-284.3
188.0
-185.7
-384.3
87.98
-285.7
-500.0
-12.02
-385.7
-112.0
-485.7
-3.377
-2.377
-1.377
-0.377
0.623
1.623
2.623
3.623
4.623
5.623
6.623
ms


EASY JTAG
plus
www.easy-jtag.com

Survey results

Software Methods (20.83%)

JTAG (12.5%)

Other (12.5%)

UART (45.83%)

eMMC Dump (29.16%)

Root

- Got root on 75% of devices
- Some devices were not tested (monolithic OS, Windows CE, etc.)
- Only case of root failure - Amazon Echo Plus (but see related Defcon talk by Huiyu/Wenxiang)
- Best defense against root seen in this survey - Verified Boot, SELinux (Android) on Amazon Echo Plus

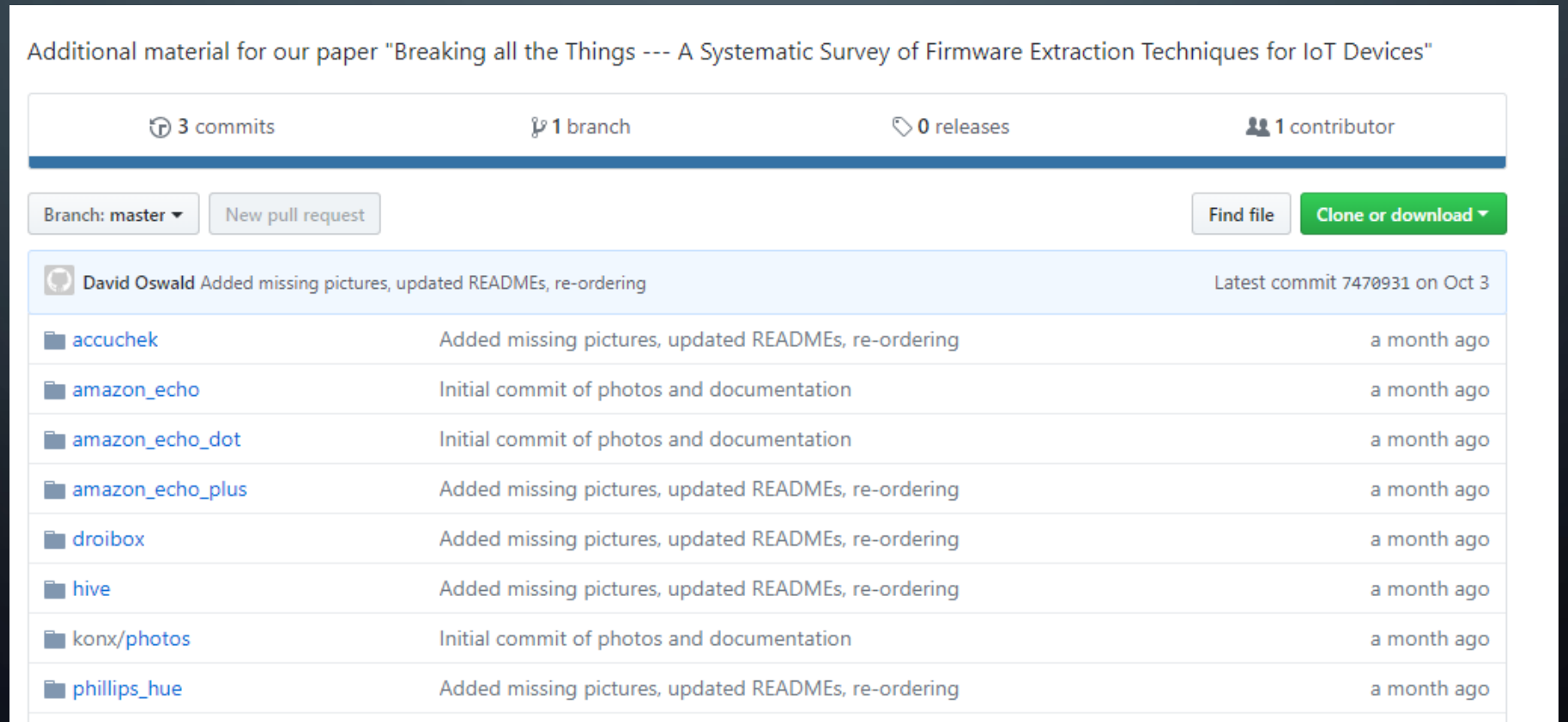
Countermeasures

- Software Methods
  - No telnet / SSH - Very widespread
  - Encrypt firmware updates & TLS - Very widespread
  - Unique device passwords - Uncommon
- UART/JTAG
  - Disable or protect UART/JTAG - Uncommon
  - Anti-tamper measures - Very uncommon
- eMMC Dump
  - Flash storage encryption - Very uncommon
  - Route flash connections on PCB inner layers - Very uncommon
  - Cover PCB with epoxy - Very uncommon

Questions?

https://github.com/david-oswald/iot-fw-extraction

sxv512@cs.bham.ac.uk



Additional material for our paper "Breaking all the Things --- A Systematic Survey of Firmware Extraction Techniques for IoT Devices"

3 commits | 1 branch | 0 releases | 1 contributor

Branch: master | New pull request | Find file | Clone or download

David Oswald Added missing pictures, updated READMEs, re-ordering — Latest commit 7470931 on Oct 3

accuchek	Added missing pictures, updated READMEs, re-ordering	a month ago
amazon_echo	Initial commit of photos and documentation	a month ago
amazon_echo_dot	Initial commit of photos and documentation	a month ago
amazon_echo_plus	Added missing pictures, updated READMEs, re-ordering	a month ago
droibox	Added missing pictures, updated READMEs, re-ordering	a month ago
hive	Added missing pictures, updated READMEs, re-ordering	a month ago
konx/photos	Initial commit of photos and documentation	a month ago
phillips_hue	Added missing pictures, updated READMEs, re-ordering	a month ago