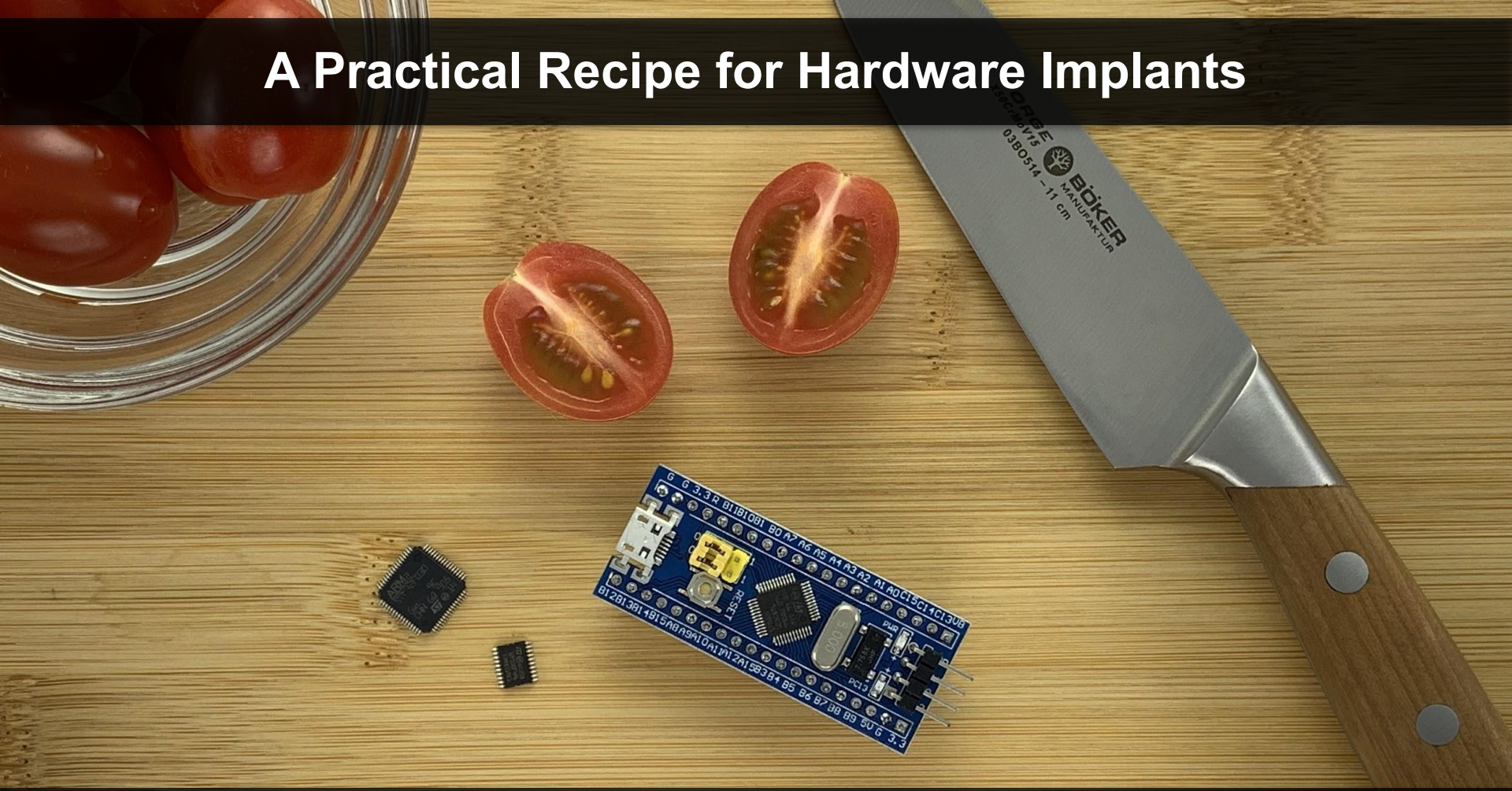
A Practical Recipe for Hardware Implants



Andrés Blanco

Lautaro Fain

Lautaro Fain

Andrés Blanco

Prior Work

The Tao
of Hardware
&
The Te of Implants

Prior Work

Modchips of the State

Trammell Hudson

9597

Prior Work

@KimZetter, @joegrand, @securelyfitz, @_MG_
@r00tkillah, @HackingThings, @_jmeltzer

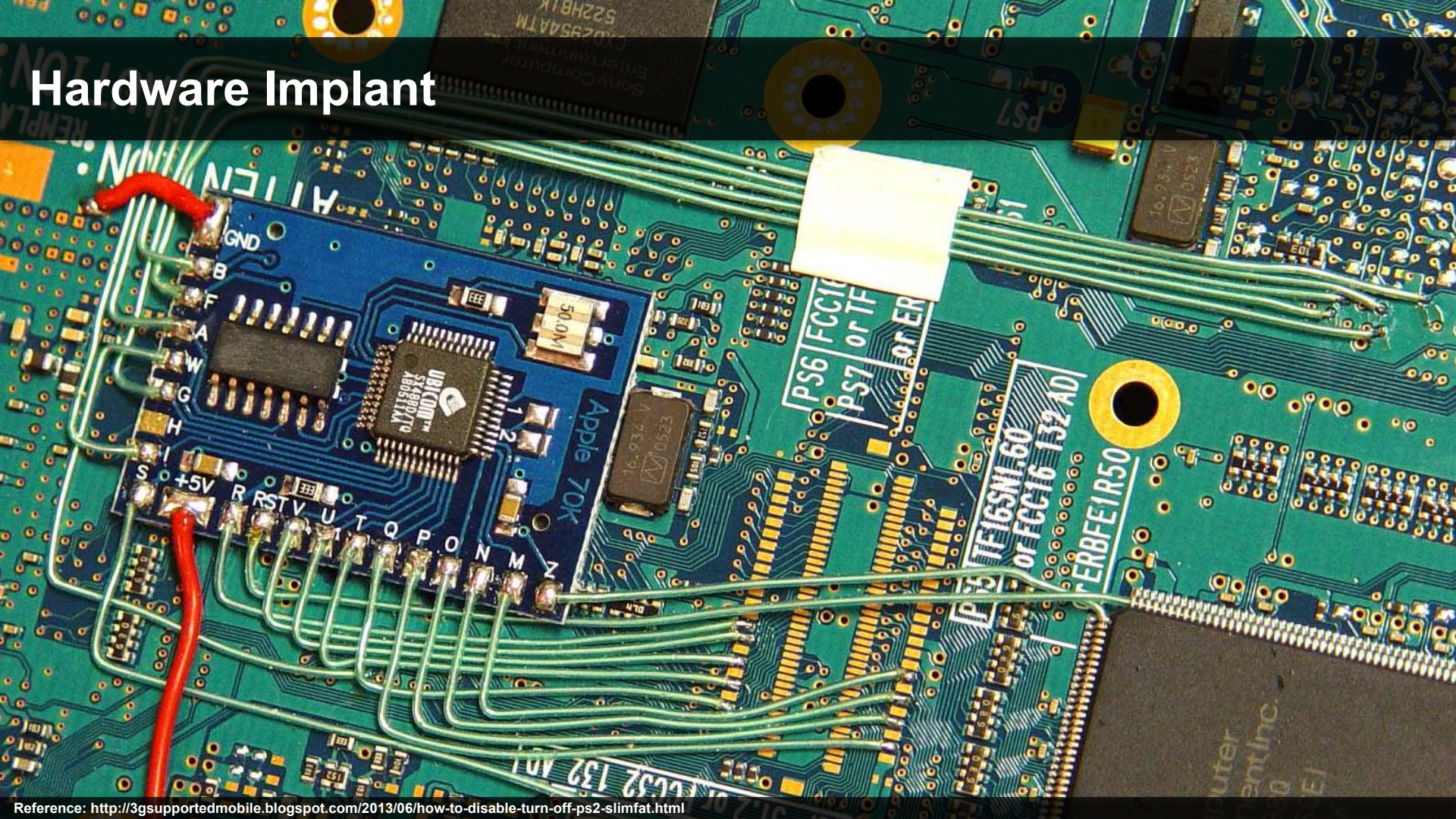
Based on the interesting news in the past few weeks, we rounded up the top technical experts with experience designing, detecting, and building hardware imlpants to discuss both what's technically possible as well as what's realistically probable with implants.

In addition, we're honored to have veteran infosec and national security journalist and author Kim Zetter moderate this panel.

Rootkit

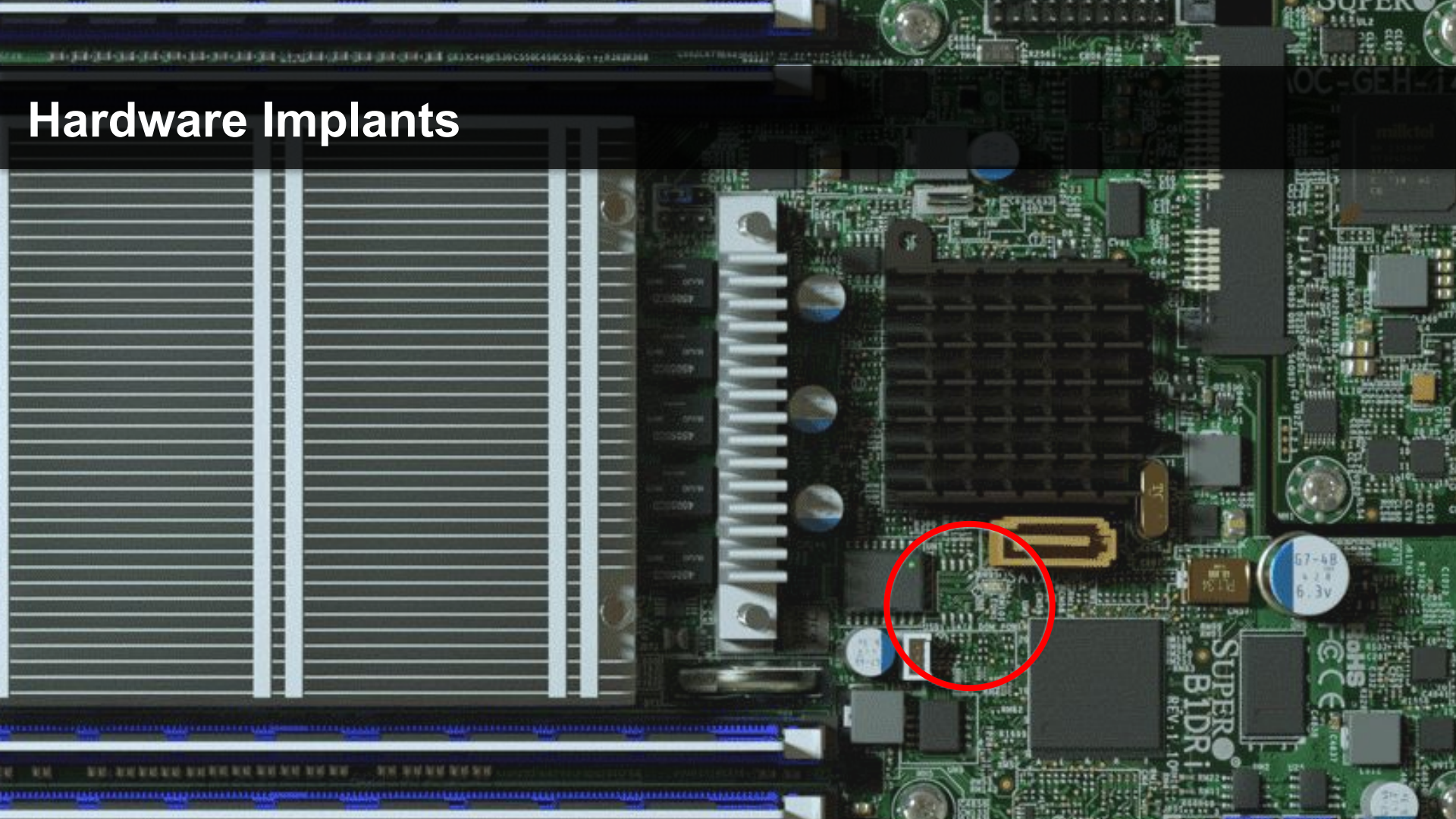

MY LOVE
Essential Collection
SONY BMG
MUSIC ENTERTAINMENT
COLUMBIA
1 MY HEART WILL GO ON (LOVE THEME FROM "TITANIC") 2 THINK TWICE 3 IT'S ALL COMING
BACK TO ME NOW 4 A NEW DAY HAS COME (RADIO REMIX) 5 MY LOVE (LIVE VERSION)

Hardware Implant



Reference: http://3gsupportedmobile.blogspot.com/2013/06/how-to-disable-turn-off-ps2-slimfat.html

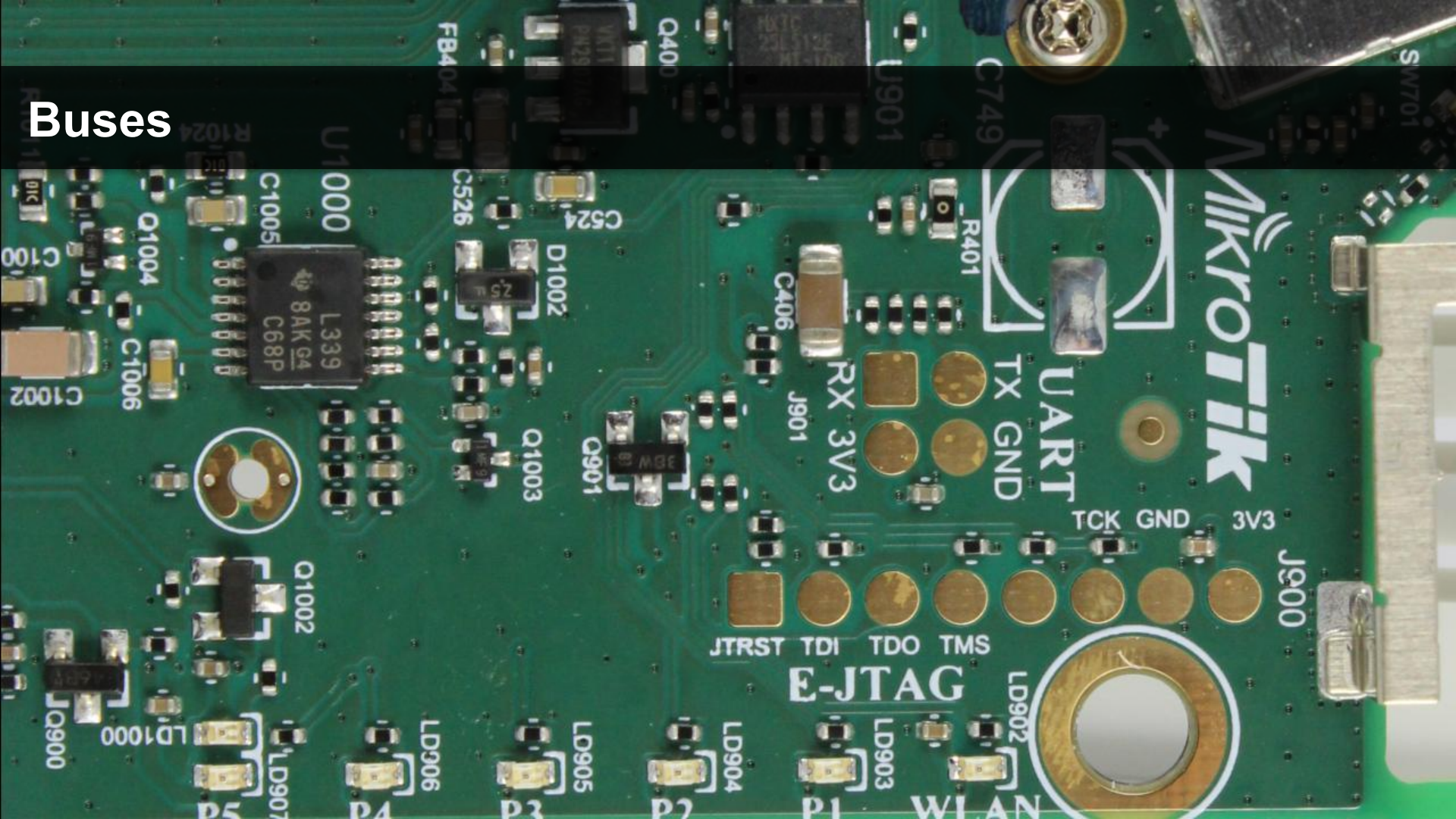
Hardware Implants



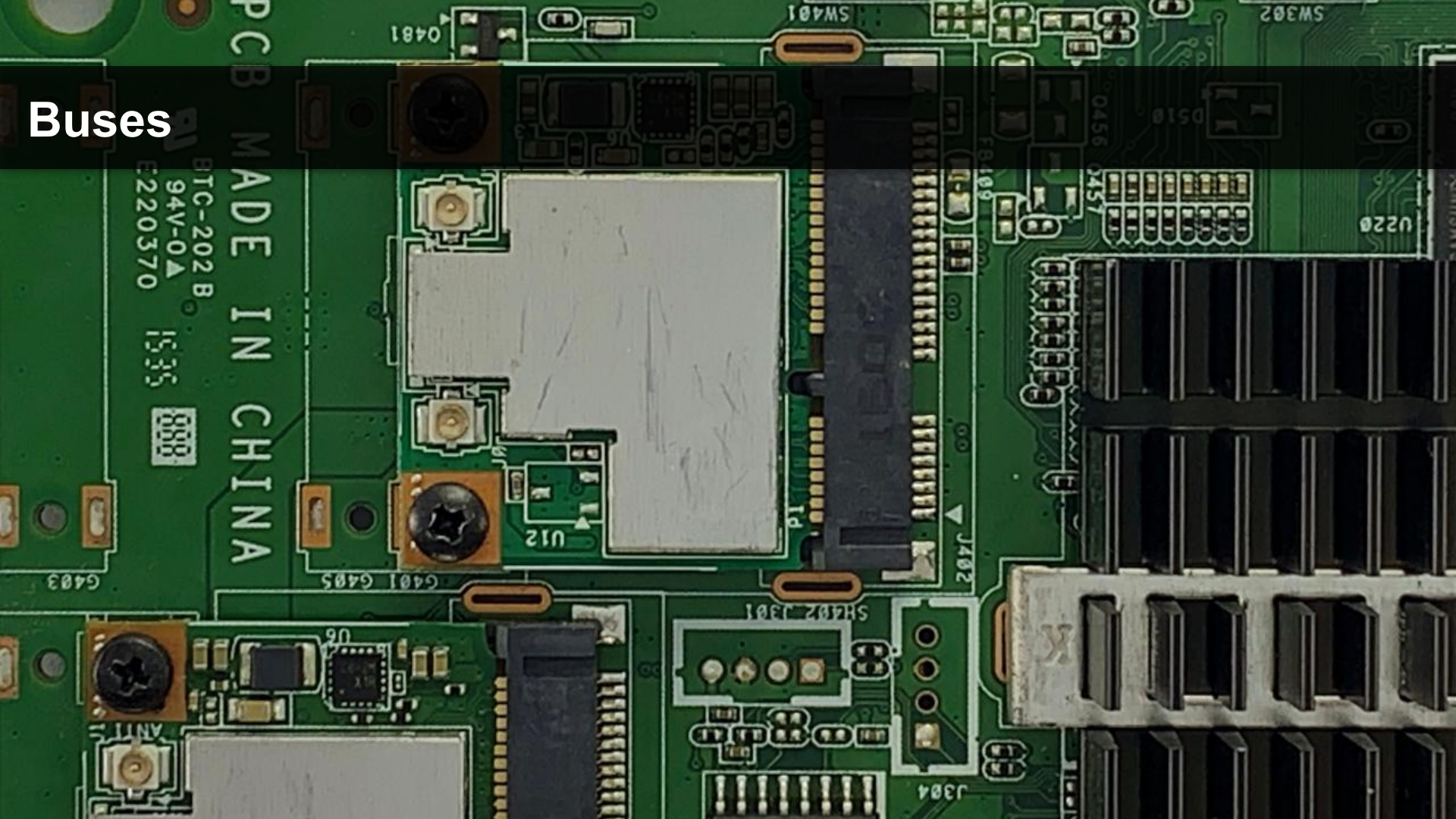
Microcontroller

Buses

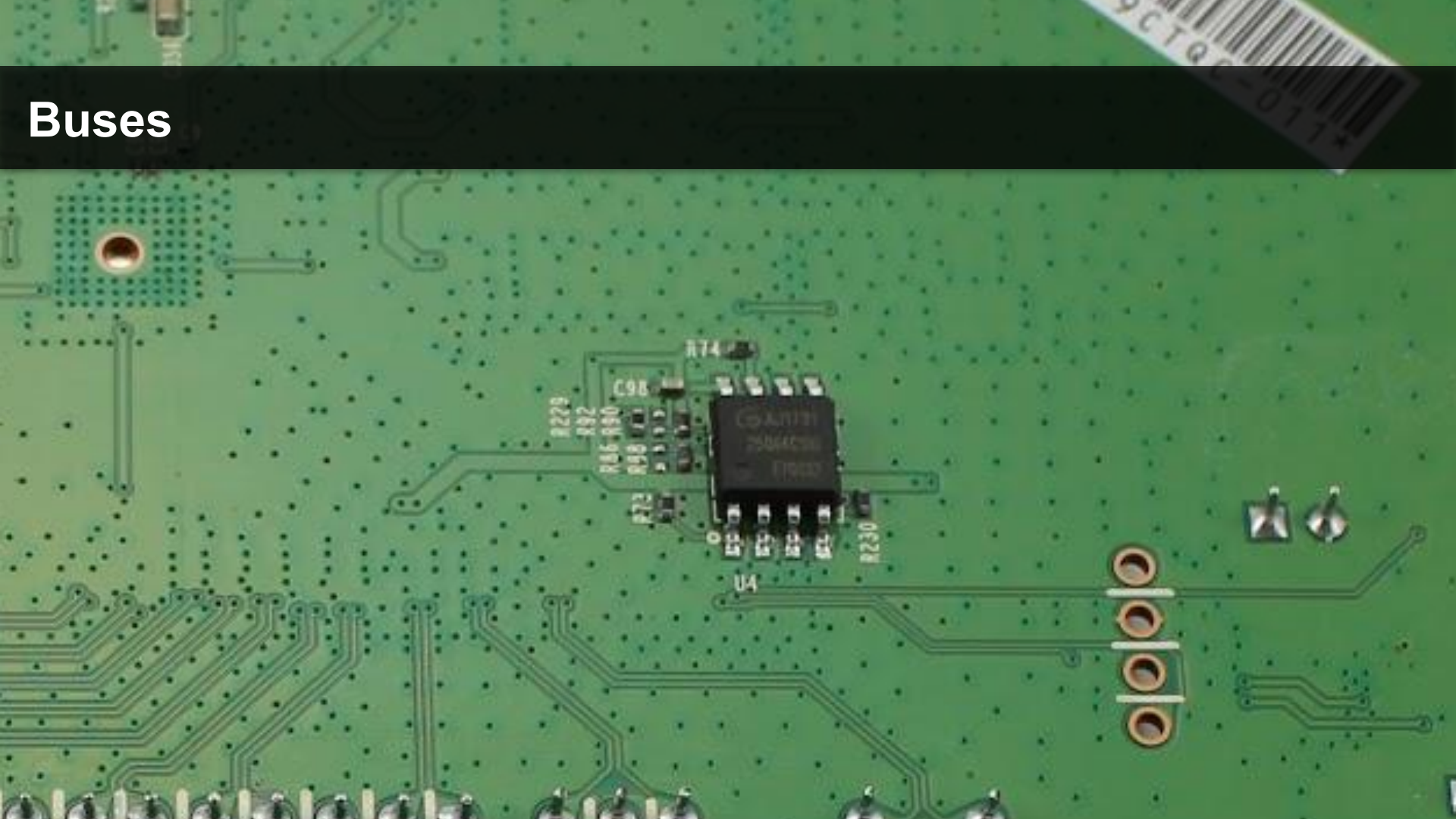
Buses


MikroTik
UART
TX GND
RX 3V3
J901
TCK GND 3V3
JTRST TDI TDO TMS
E-JTAG
J900
WLAN
P1
P2
P3
P4
P5
LD900
LD901
LD902
LD903
LD904
LD905
LD906
LD907
LD1000
Q1002
Q1003
Q1004
Q901
D1002
C1005
C1006
C1002
C526
C524
C406
R401
C749
Q400
FB401
U901
SW701

Buses


PCB MADE IN CHINA
BTC-202 B
94V-0
E220370
U12
J402
J304
SW401
SW302
U220

Buses

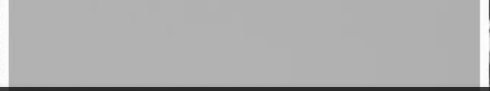


Supply Chain

Supply Chain

Supply Chain

Supply Chain




Supply Chain

PCB

IC

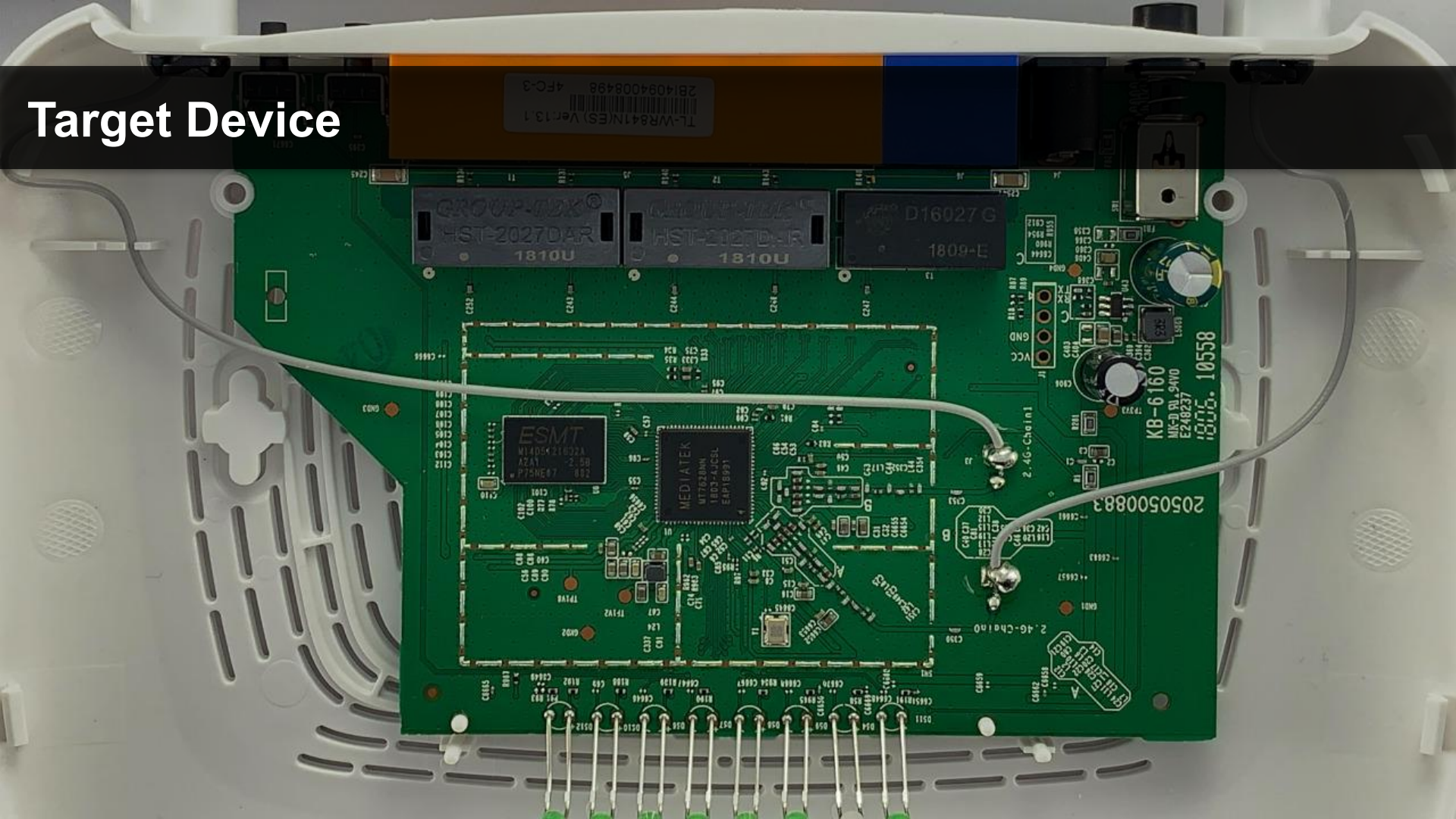
Assembly

Firmware

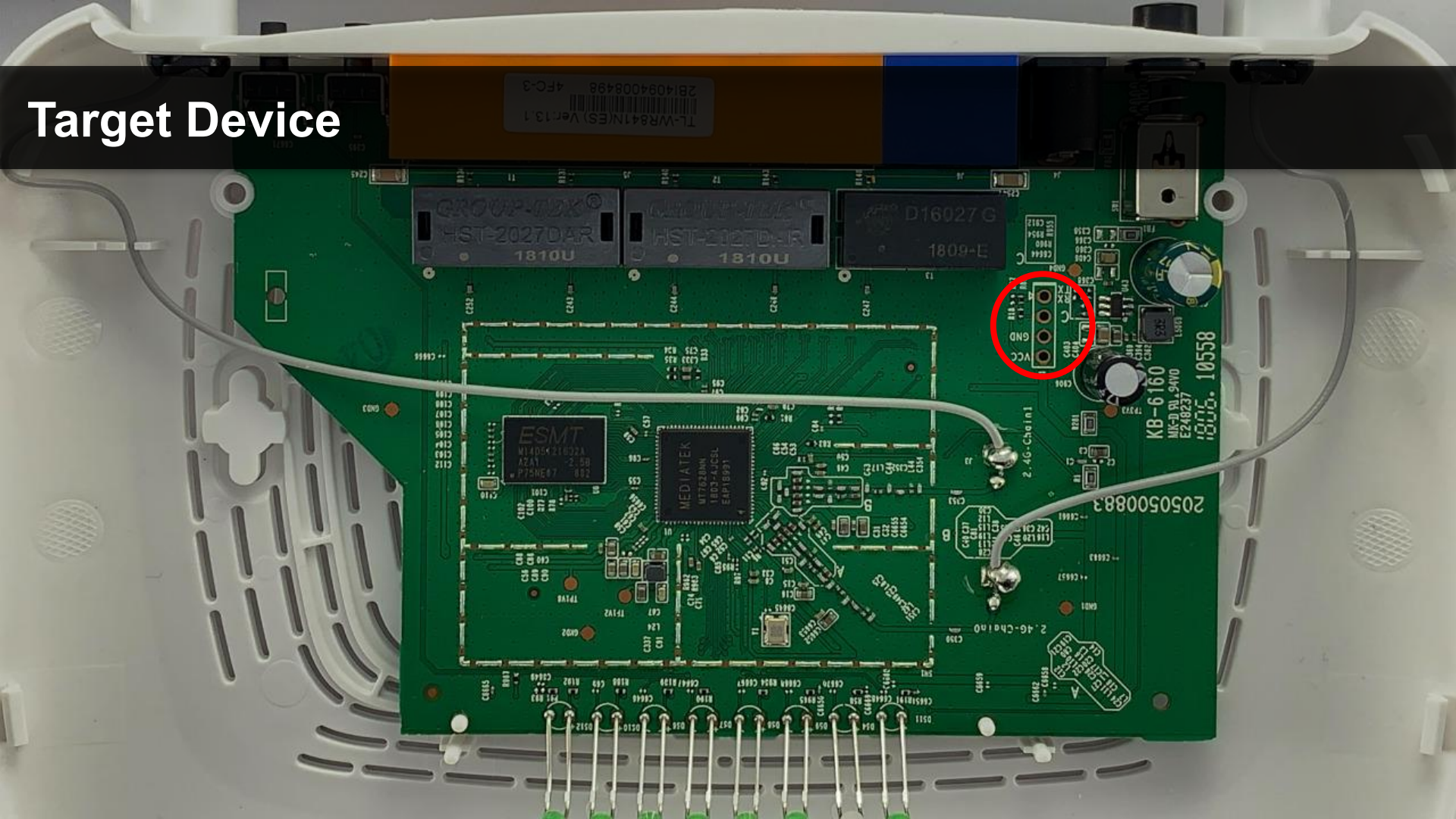
Device

The Recipe

Target Device



Target Device



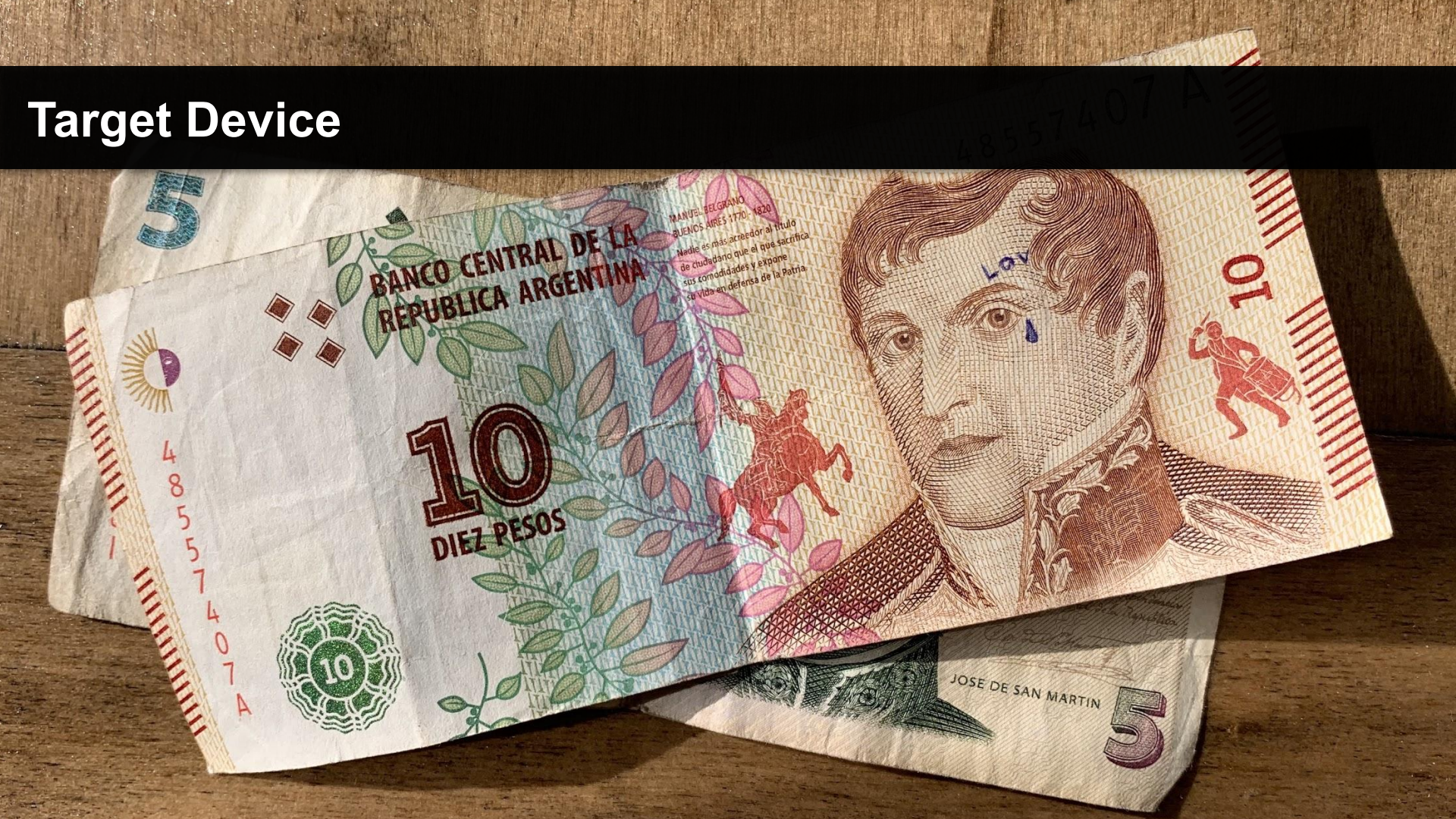
Target Device

```
RESET MT7628 PHY!!! 0
TODO, Read MAC Address from Flash

MT7628 # help
?       - alias for 'help'
base    - print or set address offset
bdinfo  - print Board Info structure
bootm   - boot application image from memory
bootp   - boot image via network using BootP/TFTP protocol
coninfo - print console devices and information
cp      - memory copy
crc32   - checksum calculation
erase   - erase SPI FLASH memory
go      - start application at address 'addr'
help    - print online help
loadb   - load binary file over serial line (kermit mode)
loop    - infinite loop on address range
md      - memory display
mdio    - Ralink PHY register R/W command !!
mm      - memory modify (auto-incrementing)
mtest   - simple RAM test
nm      - memory modify (constant address)
printenv- print environment variables
rarpboot- boot image via network using RARP/TFTP protocol
reset   - Perform RESET of the CPU
rf      - read/write rf register
saveenv - save environment variables to persistent storage
setenv  - set environment variables
sleep   - delay execution for some time
spi     - spi command
tftpboot- boot image via network using TFTP protocol
version - print monitor version
MT7628 #
```

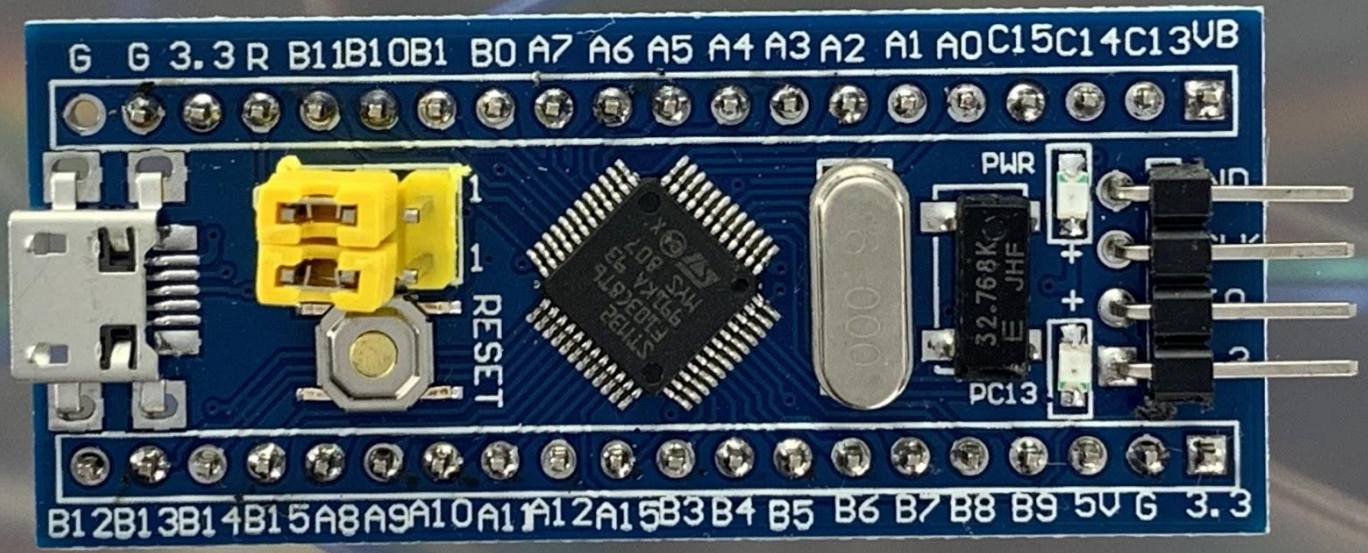
Target Device

```
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
iptables: Bad rule (does a matching rule exist in that chain?).
sh: can't create /proc/tplink/echan: nonexistent directory
[ getPidFromPidFile ] 112:  Cann't open file: /var/run/zebra.pid.
sh: can't create /proc/tplink/echan: nonexistent directory
[ getPidFromPidFile ] 112:  Cann't open file: /var/run/ripd.pid.
iptables: No chain/target/match by that name.
iptables: Bad rule (does a matching rule exist in that chain?).
iptables: Bad rule (does a matching rule exist in that chain?).
iptables: Bad rule (does a matching rule exist in that chain?).
ip6tables: Bad rule (does a matching rule exist in that chain?).
iptables: Bad rule (does a matching rule exist in that chain?).
iptables: Bad rule (does a matching rule exist in that chain?).
iptables: Bad rule (does a matching rule exist in that chain?).
nf_nat_rtsp v0.6.21 loading
enable switch phyport...
Set: phy[0].reg[0] = 3900
Set: phy[1].reg[0] = 3900
Set: phy[2].reg[0] = 3900
Set: phy[3].reg[0] = 3900
Set: phy[4].reg[0] = 3900
Set: phy[0].reg[0] = 3300
Set: phy[1].reg[0] = 3300
Set: phy[2].reg[0] = 3300
Set: phy[3].reg[0] = 3300
Set: phy[4].reg[0] = 3300
resetMiiPortV over.
Will output 1024 bit rsa secret key to '/var/tmp/dropbear/dropbear_rsa_host_key'
Generating key, this may take a while...
Will output 1024 bit dss secret key to '/var/tmp/dropbear/dropbear_dss_host_key'
Generating key, this may take a while...

~ #
```

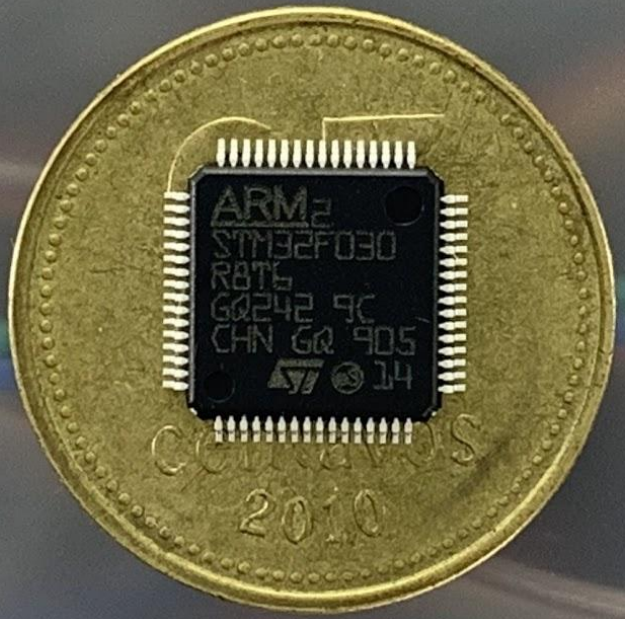
Target Device



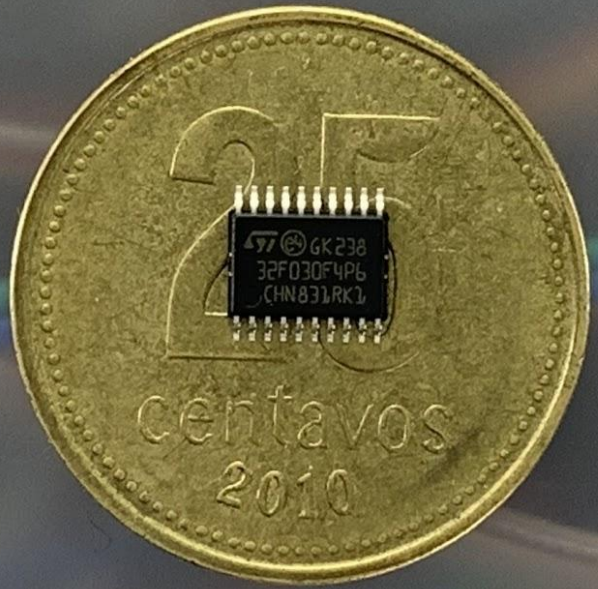
Components


G G 3.3 R B11 B10 B1 B0 A7 A6 A5 A4 A3 A2 A1 A0 C15 C14 C13 VB
PWR
RESET
32.768K
PC13
B12 B13 B14 B15 A8 A9 A10 A11 A12 A15 B3 B4 B5 B6 B7 B8 B9 5V G 3.3

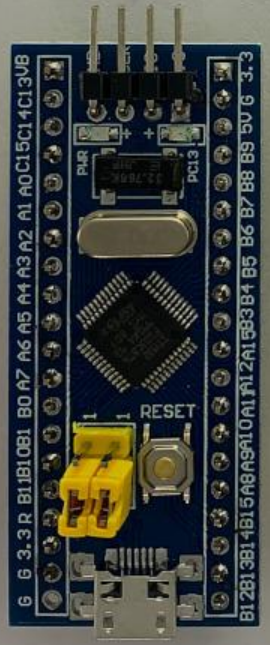
Components

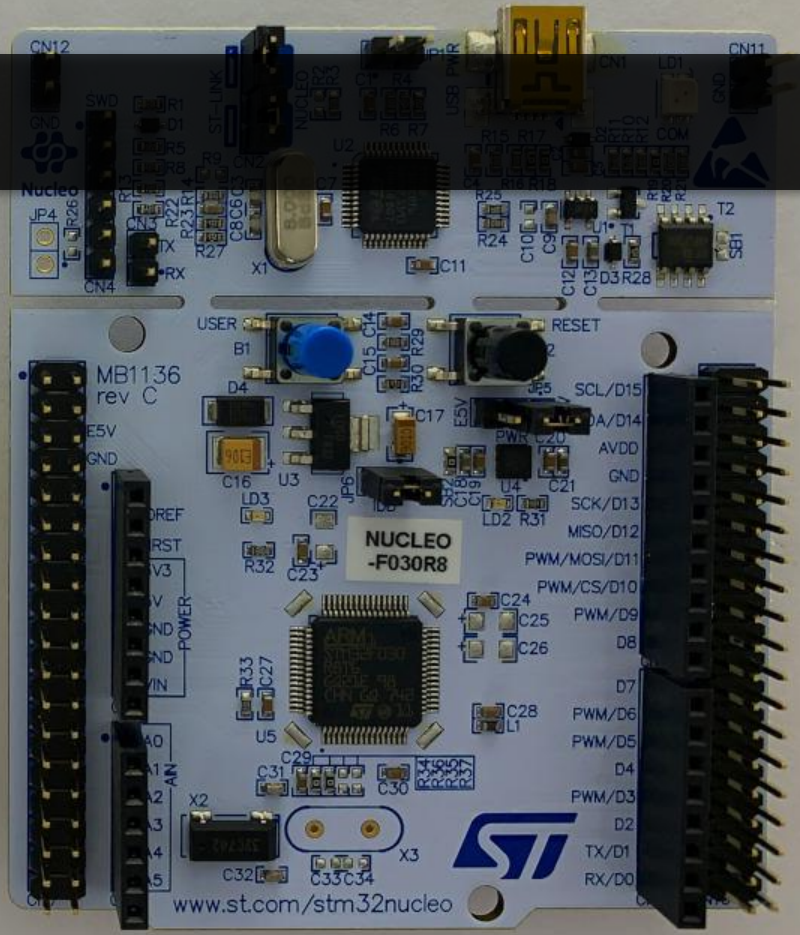


Components

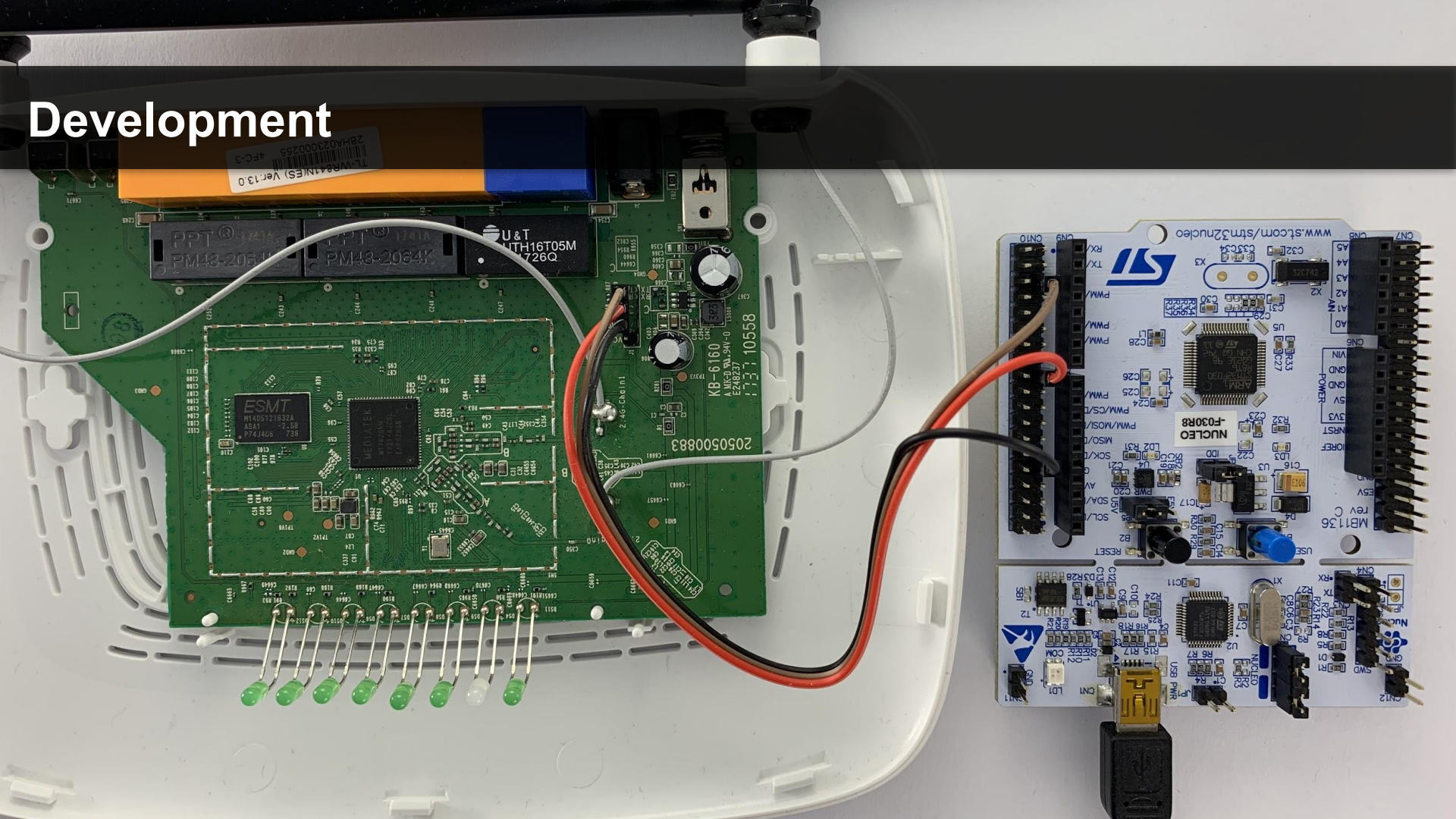


Development





Development



Development

STM32 CubeMX File Window Help

Home > STM32F030F4Px > STM32F030F4.ioc - Pinout & Configuration

GENERATE CODE

Pinout & Configuration | Clock Configuration | Project Manager | Tools

Additional Software | Pinout

Categories | A->Z

- System Core
- Analog
- Timers
- Connectivity
  - I2C1
  - IRTIM
  - SPI1
  - USART1
- Computing
- Middleware

USART1 Mode and Configuration

Mode

Mode: Asynchronous

Hardware Flow Control (RS232): Disable

Hardware Flow Control (RS485)

Configuration

Reset Configuration

Parameter Settings | User Constants | NVIC Settings | DMA Settings | GPIO Settings

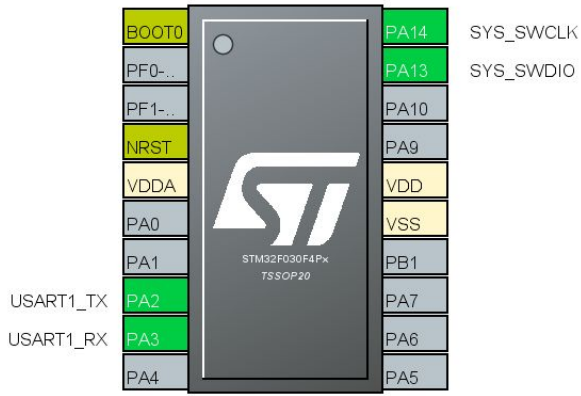
DMA Request	Channel	Direction	Priority
USART1_RX	DMA1 Channel 3	Peripheral To Memory	Low
USART1_TX	DMA1 Channel 2	Memory To Peripheral	Low

Add | Delete

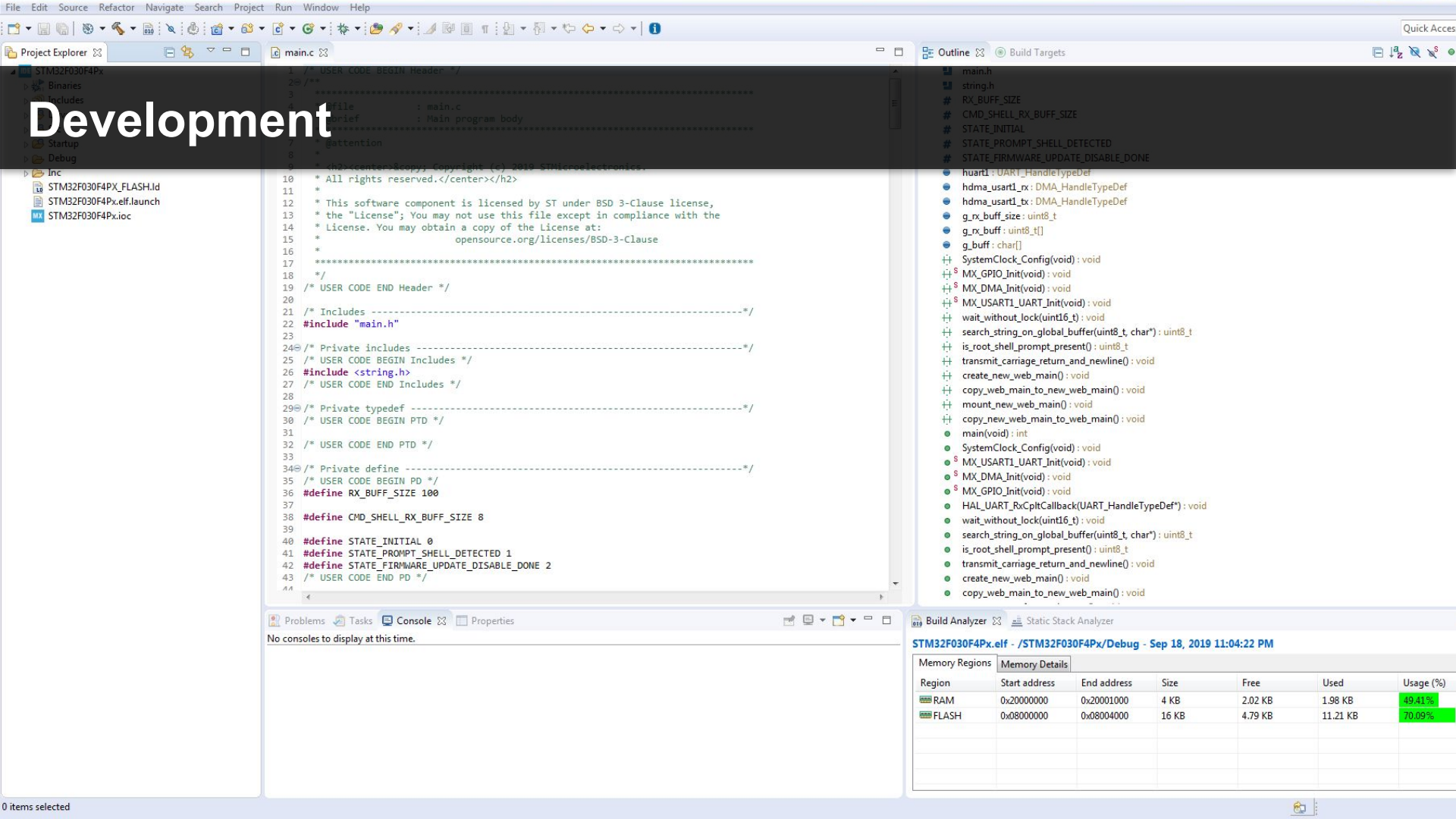
DMA Request Settings

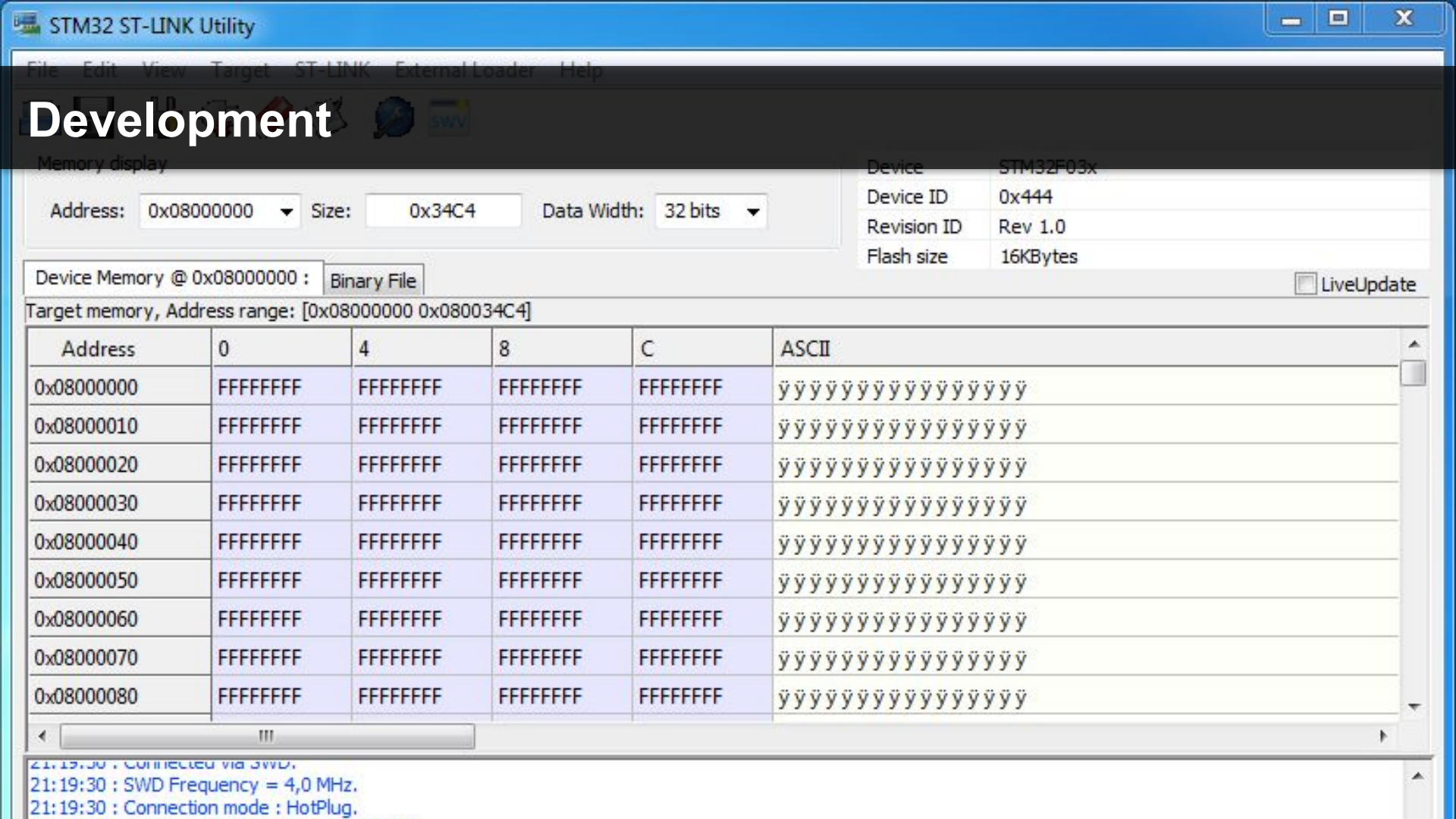
	Peripheral	Memory
Mode		
Increment Address		
Data Width		

Pinout view | System view

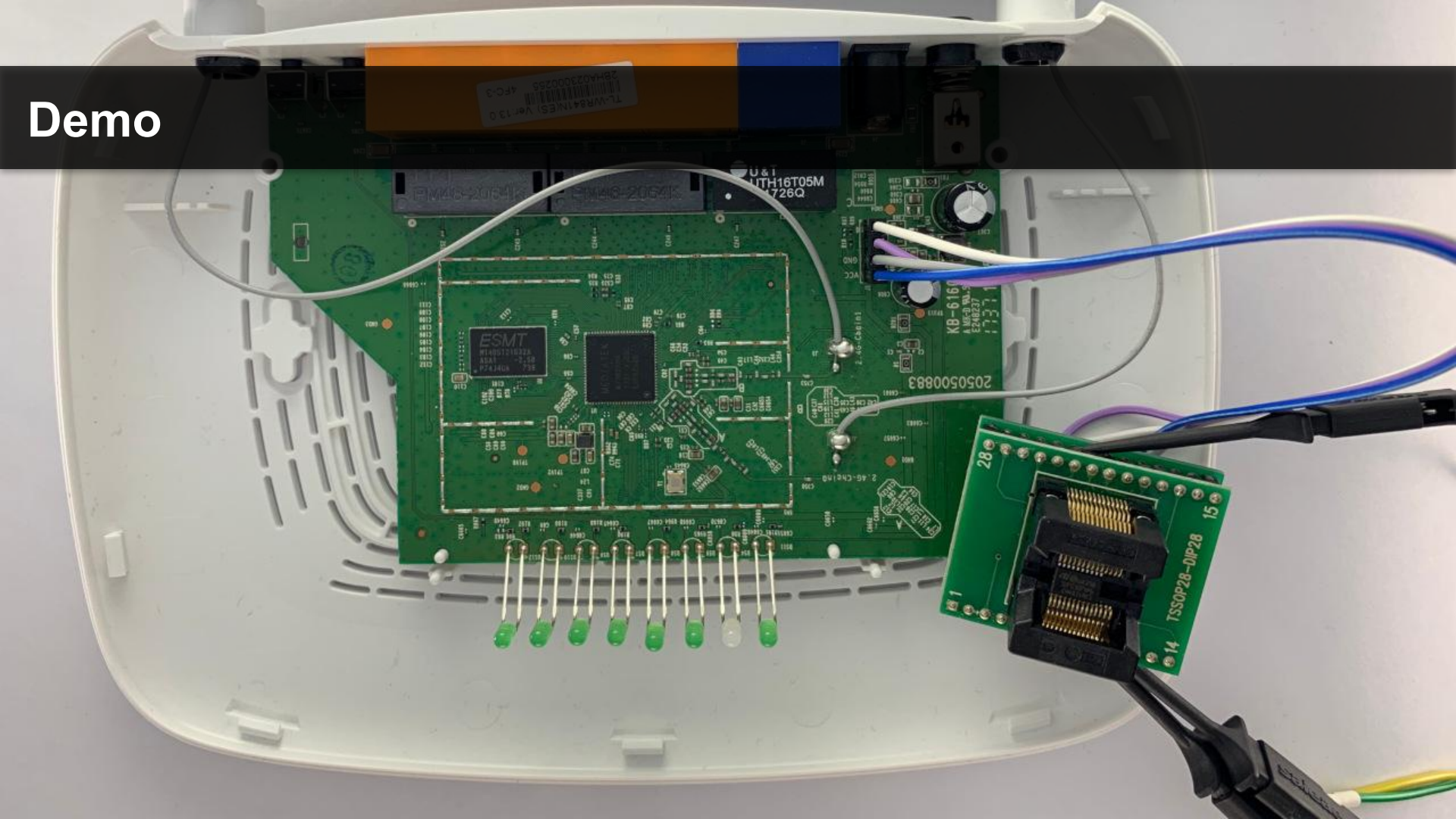


Development

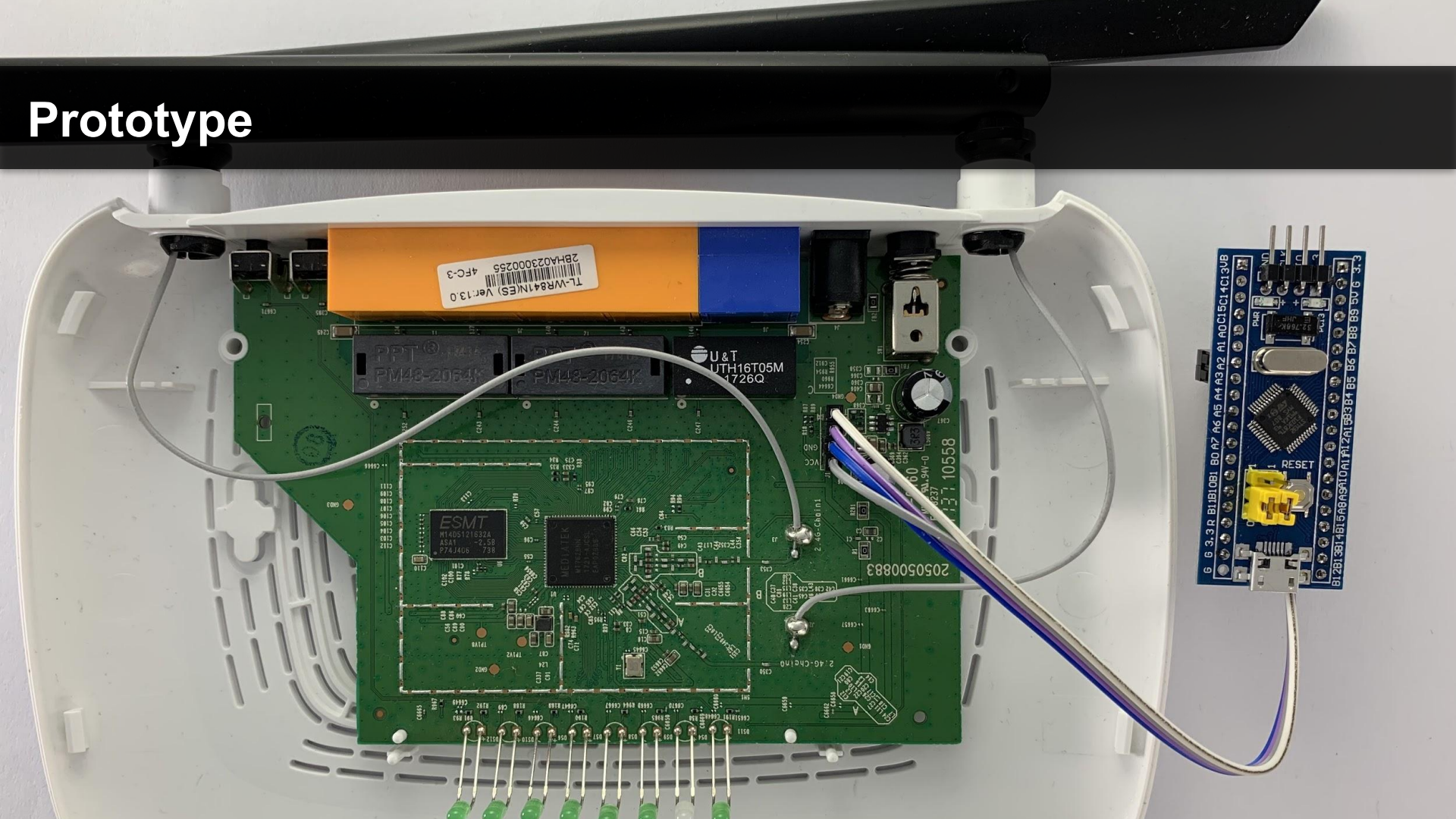



STM32 ST-LINK Utility
File Edit View Target ST-LINK External Loader Help
Development
Memory display
Address: 0x08000000 Size: 0x34C4 Data Width: 32 bits
Device STM32F03x
Device ID 0x444
Revision ID Rev 1.0
Flash size 16KBytes
Device Memory @ 0x08000000 : Binary File
LiveUpdate
Target memory, Address range: [0x08000000 0x080034C4]
Address 0 4 8 C ASCII
0x08000000 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x08000010 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x08000020 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x08000030 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x08000040 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x08000050 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x08000060 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x08000070 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x08000080 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
21:19:30 : SWD Frequency = 4,0 MHz.
21:19:30 : Connection mode : HotPlug.

Demo

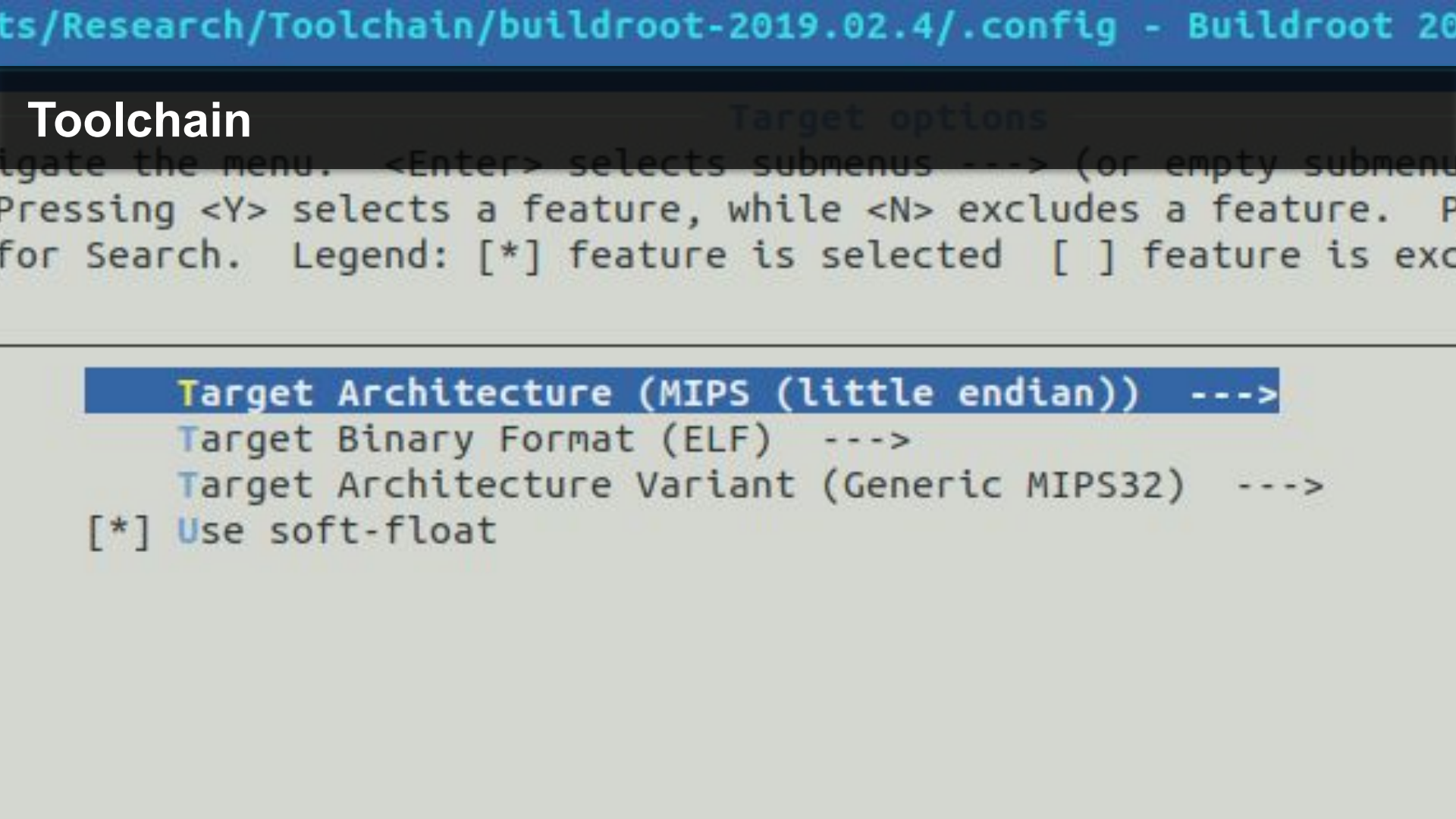


Prototype



Environment

```
        BusyBox is a multi-call binary that combines many common Unix
        utilities into a single executable.  Most people will create a
        link to busybox for each function they wish to use and BusyBox
        will act like whatever it was invoked as.

Currently defined functions:
        arping, ash, brctl, cat, chmod, cp, date, df, echo, free, getty, halt,
        ifconfig, init, insmod, ipcrm, ipcs, kill, killall, linuxrc, login, ls,
        lsmod, mkdir, mount, netstat, pidof, ping, ping6, poweroff, ps, reboot,
        rm, rmmod, route, sh, sleep, taskset, telnetd, tftp, top, umount,
        vconfig

~ # cat /proc/cpuinfo
system type             : MT7628
processor               : 0
cpu model               : MIPS 24Kc V5.5
BogoMIPS                : 386.04
wait instruction        : yes
microsecond timers      : yes
tlb_entries             : 32
extra interrupt vector  : yes
hardware watchpoint     : yes, count: 4, address/irw mask: [0x0000, 0x0b28, 0x0498, 0x08b8]
ASEs implemented        : mips16 dsp
shadow register sets    : 1
core                    : 0
VCED exceptions         : not available
VCEI exceptions         : not available

~ # cat /proc/version
Linux version 2.6.36 (tomcat@buildserver) (gcc version 4.6.3 (Buildroot 2012.11.1) ) #1 Mon Nov 7 20:36:01 CST
```


ts/Research/Toolchain/buildroot-2019.02.4/.config - Buildroot 20
Toolchain
Target options
igate the menu. <Enter> selects submenus ---> (or empty submenu
Pressing <Y> selects a feature, while <N> excludes a feature. P
for Search. Legend: [*] feature is selected [ ] feature is exc
Target Architecture (MIPS (little endian)) --->
Target Binary Format (ELF) --->
Target Architecture Variant (Generic MIPS32) --->
[*] Use soft-float

Persistence

Persistence

```
0x00402924      lw   gp, (var_18h)
0x00402928      lw   v0, (s0)          ; 0x42221c
                                       ; obj.g_http_author_default
0x0040292c      lui  a1, 0x41          ; 'A'
0x00402930      lw   t9, -sym.http_alias_addEntryByArg(gp) ; 0x42248c
0x00402934      lw   a3, -sym.http_rpm_conferr(gp) ; 0x4224a0
0x00402938      addiu a0, zero, 2      ; arg1
0x0040293c      addiu a1, a1, -0x4d80 ; 0x40b280 ; "/cgi/bnr" ; arg2 ; str.cgi_bnr
0x00402940      move a2, zero
0x00402944      bal  sym.http_alias_addEntryByArg
0x00402948      sw   v0, (var_10h)
0x0040294c      lw   gp, (var_18h)
0x00402950      lw   v0, (s0)          ; 0x42221c
                                       ; obj.g_http_author_default
0x00402954      lui  a1, 0x41          ; 'A'
0x00402958      lw   t9, -sym.http_alias_addEntryByArg(gp) ; 0x42248c
0x0040295c      lw   a3, -sym.http_rpm_update(gp) ; 0x4224a4
0x00402960      addiu a0, zero, 2
0x00402964      addiu a1, a1, -0x4d74 ; 0x40b28c ; "/cgi/softup" ; str.cgi_softup
0x00402968      move a2, zero
0x0040296c      bal  sym.http_alias_addEntryByArg
0x00402970      sw   v0, (var_10h)
0x00402974      lw   gp, (var_18h)
0x00402978      lw   v0, (s0)          ; 0x42221c
                                       ; obj.g_http_author_default
0x0040297c      lui  a1, 0x41          ; 'A'
0x00402980      lw   t9, -sym.http_alias_addEntryByArg(gp) ; 0x42248c
0x00402984      lw   a3, -sym.http_rpm_softerr(gp) ; 0x4224a8
0x00402988      addiu a0, zero, 2
0x0040298c      addiu a1, a1, -0x4d68 ; 0x40b298 ; "/cgi/softburn" ; str.cgi_softburn
0x00402990      move a2, zero
0x00402994      bal  sym.http_alias_addEntryByArg
0x00402998      sw   v0, (var_10h)
0x0040299c      lw   gp, (var_18h)
```

Persistence

DESCRIPTION top

The **ptrace**() system call provides a means by which one process (the "tracer") may observe and control the execution of another process (the "tracee"), and examine and change the tracee's memory and registers. It is primarily used to implement breakpoint debugging and system call tracing.

A tracee first needs to be attached to the tracer. Attachment and subsequent commands are per thread: in a multithreaded process, every thread can be individually attached to a (potentially different) tracer, or left not attached and thus not debugged. Therefore, "tracee" always means "(one) thread", never "a (possibly multithreaded) process". Ptrace commands are always sent to a specific tracee using a call of the form

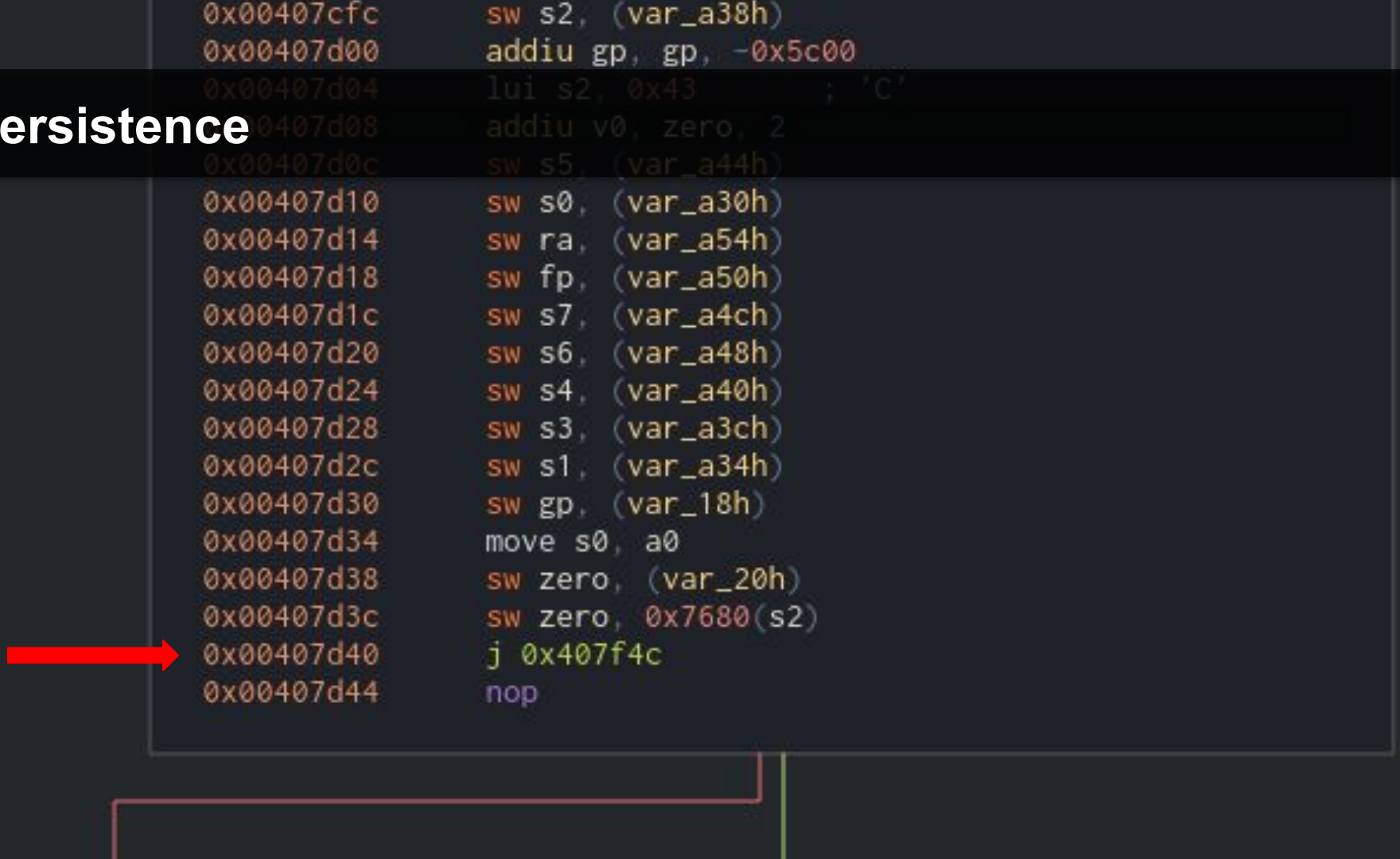
```
ptrace(PTRACE_foo, pid, ...)
```

where *pid* is the thread ID of the corresponding Linux thread.

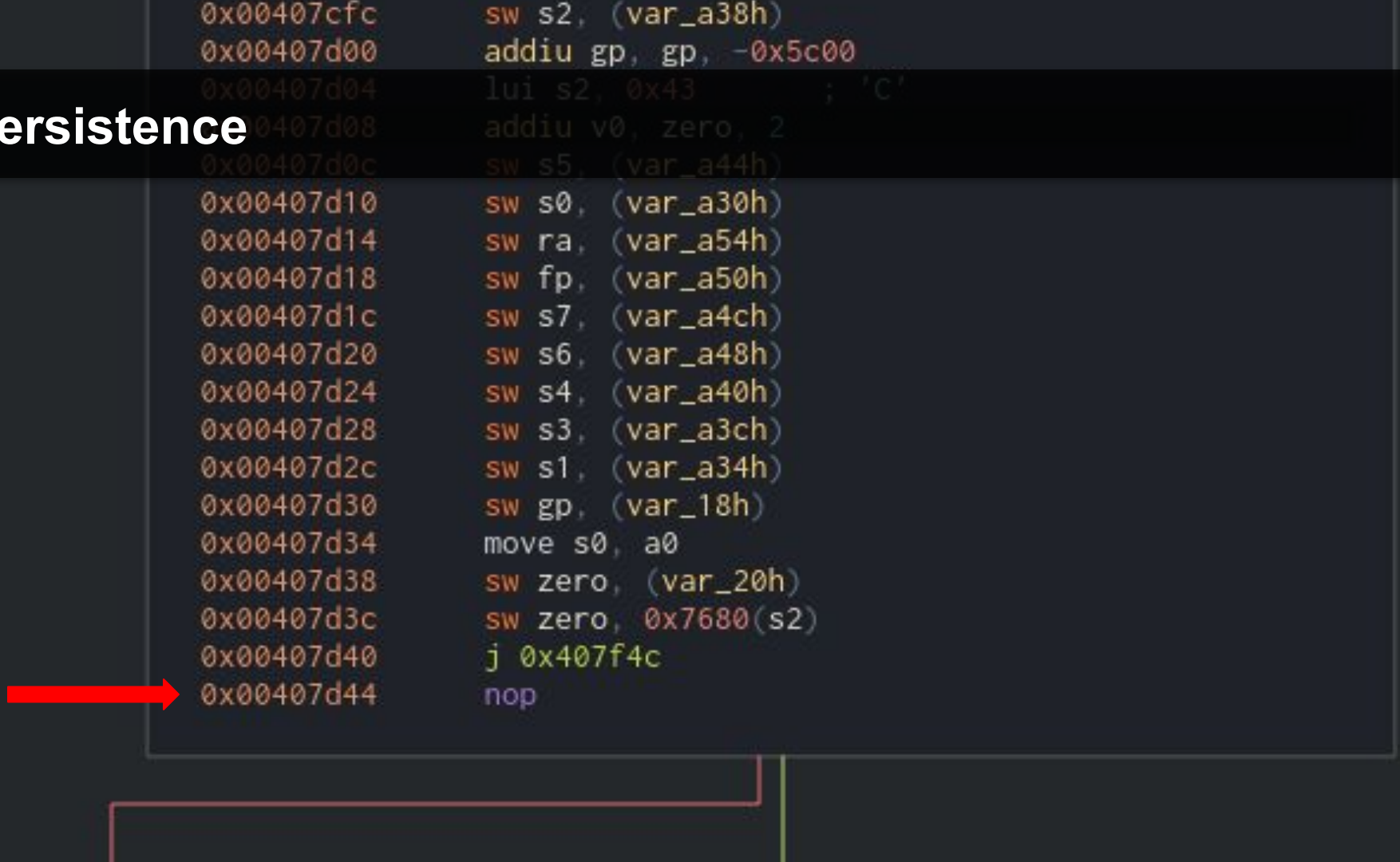
Persistence

```
    sscanf(baddr_aux, "%p", &baddr);
}

int inject(pid_t pid, char *src, void *dst, int len){
    int i;
    u_int32_t *source = (u_int32_t *) src;
    u_int32_t *destination = (u_int32_t *) dst;

    for(i=0; i < len; i+=4, source++, destination++){

        if ((ptrace(PTRACE_POKETEXT, pid, destination, *source)) < 0){
            printf("[ERROR] Unexpected error while injecting the shellcod
            return -1;
        }
    }
    return 0;
}
```

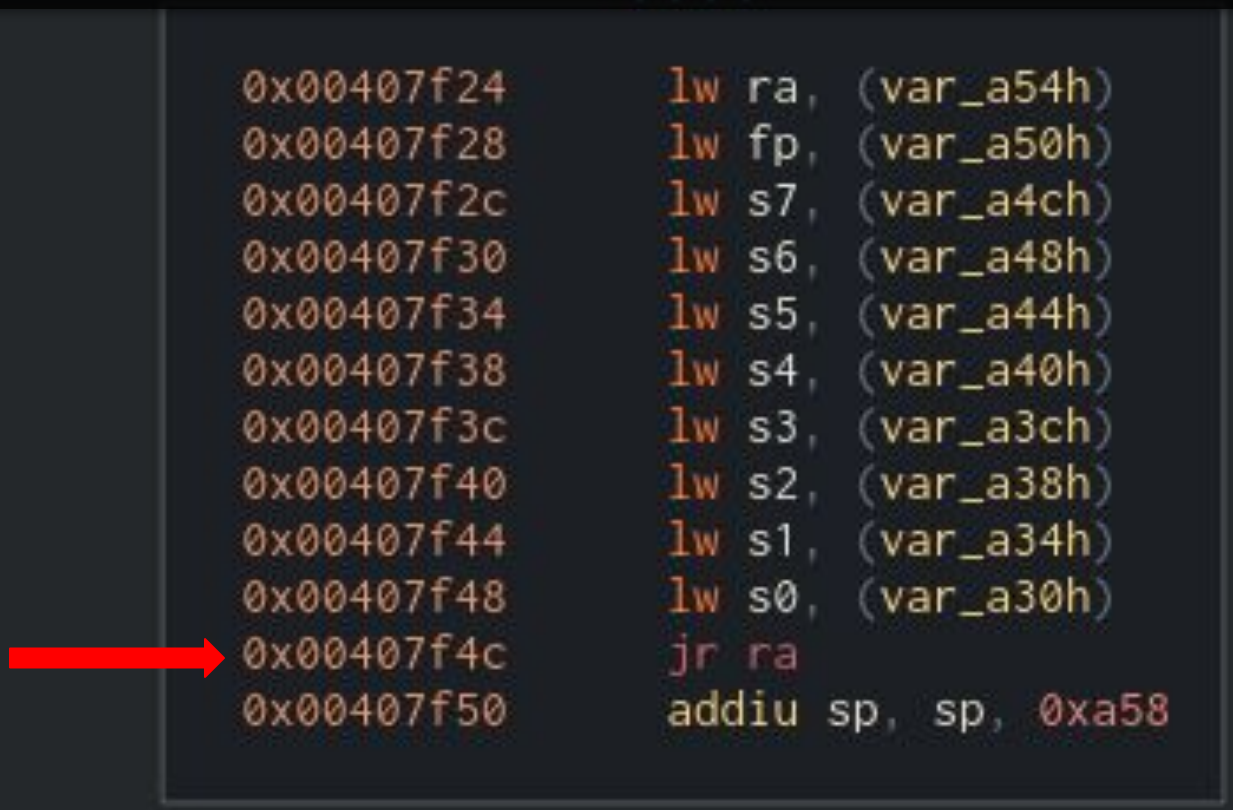
Persistence



Persistence



Persistence



Common People Supply Chain Attacks

Common People Supply Chain Attacks

$ 1.199

Router Wifi Tp-link TI-wr841n 300mbps

$ 1.254

Llega hoy

Router Tp Link Wr 841n 300 Mbps Wifi B/g/n 2 Antenas Wireles

$ 1.254

Llega hoy

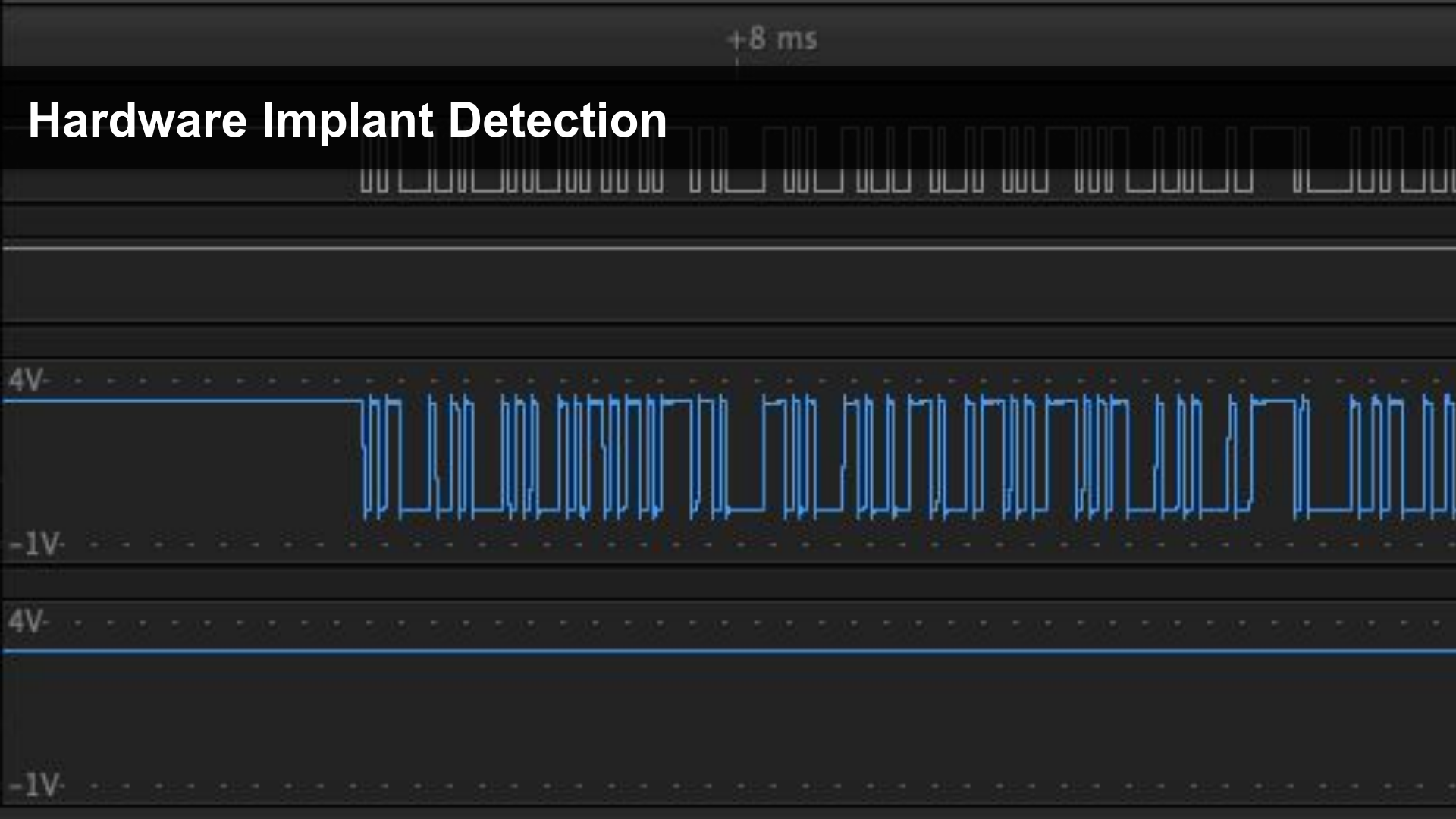
Router Wi-fi Tp-link Wr841n 300mbps - Tp Link 841n

Common People Supply Chain Attacks

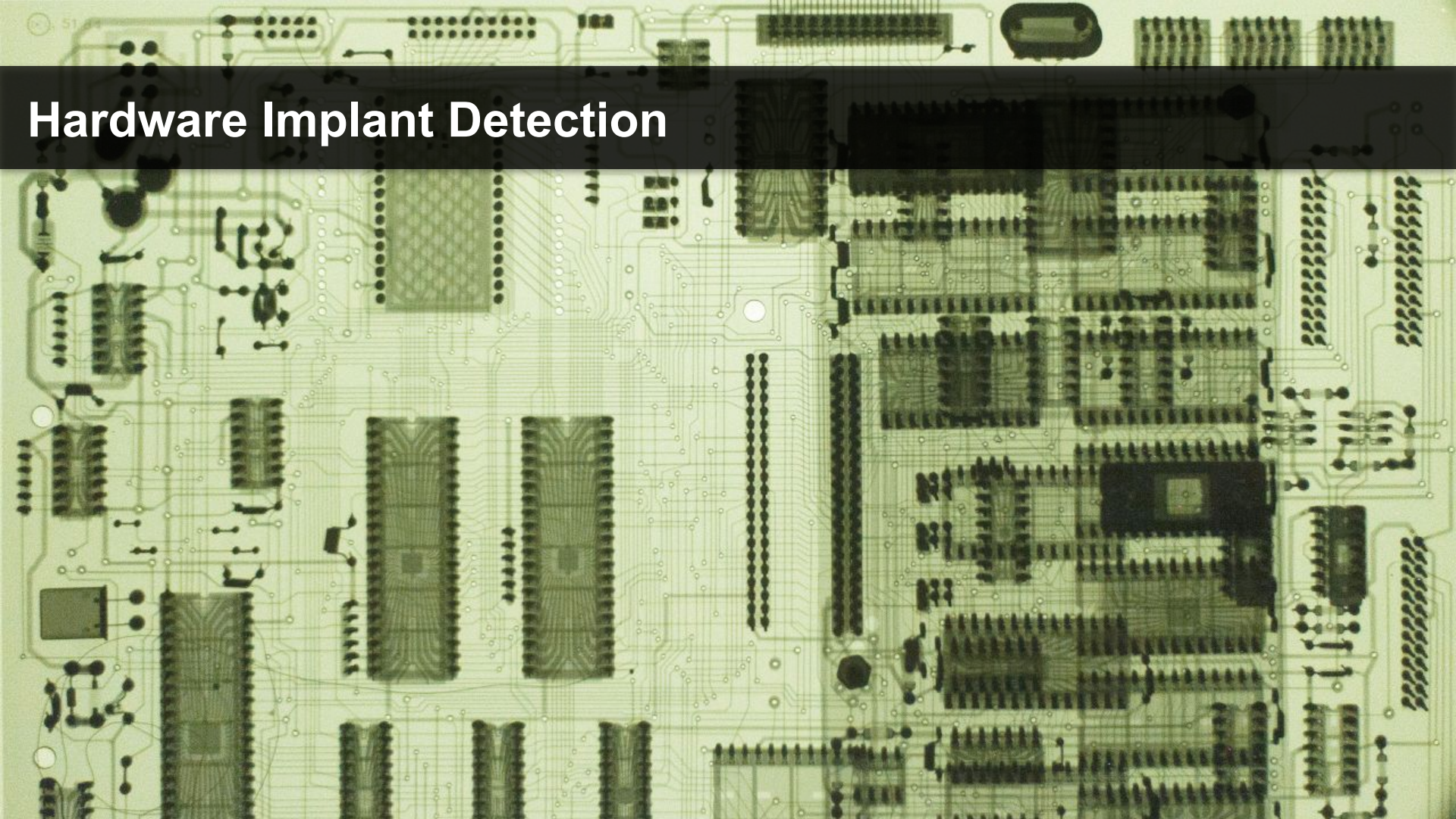
Hardware Implant Detection

24	174.181451327	fe80::8c4:e62b:8a79…	ff02::fb	MDNS	177	Standard q
25	174.184723530	192.168.0.158	224.0.0.251	MDNS	157	Standard q
26	174.795467009	192.168.0.158	224.0.0.22	IGMPv3	54	Membership
27	[illegible]	[illegible]	224.0.0.251	IGMPv3	56	Membership
28	175.104779508	192.168.0.158	224.0.0.251	MDNS	157	Standard q
29	175.245076517	192.168.0.125	224.0.0.22	IGMPv3	54	Membership
30	175.307374858	192.168.0.61	224.0.0.22	IGMPv3	54	Membership
31	175.819555266	192.168.0.158	224.0.0.22	IGMPv3	54	Membership
32	176.843596264	192.168.0.158	224.0.0.22	IGMPv3	54	Membership
33	176.844130880	192.168.0.61	224.0.0.22	IGMPv3	54	Membership
34	176.845709996	192.168.0.1	224.0.0.251	IGMPv3	56	Membership
35	177.765191569	192.168.0.158	224.0.0.22	IGMPv3	54	Membership
36	177.766990966	192.168.0.158	224.0.0.22	IGMPv3	54	Membership
37	177.767023437	192.168.0.1	224.0.0.251	IGMPv3	56	Membership
38	177.797034268	192.168.0.125	224.0.0.22	IGMPv3	54	Membership
39	178.072587593	fe80::8c4:e62b:8a79…	ff02::fb	MDNS	177	Standard q
40	178.074159111	192.168.0.158	224.0.0.251	MDNS	157	Standard q
41	178.379522380	192.168.0.61	224.0.0.22	IGMPv3	54	Membership
42	178.789267264	192.168.0.158	224.0.0.22	IGMPv3	54	Membership
43	183.808742627	192.168.0.1	224.0.0.251	IGMPv3	56	Membership
44	184.236991079	192.168.0.125	224.0.0.22	IGMPv3	54	Membership
45	184.728163919	192.168.0.61	224.0.0.22	IGMPv3	54	Membership
46	184.830717483	192.168.0.158	224.0.0.22	IGMPv3	54	Membership
47	187.083758726	fe80::8c4:e62b:8a79…	ff02::fb	MDNS	177	Standard q
48	187.085719960	192.168.0.158	224.0.0.251	MDNS	157	Standard q
49	190.824037273	192.168.0.125	239.255.255.250	SSDP	208	M-SEARCH *

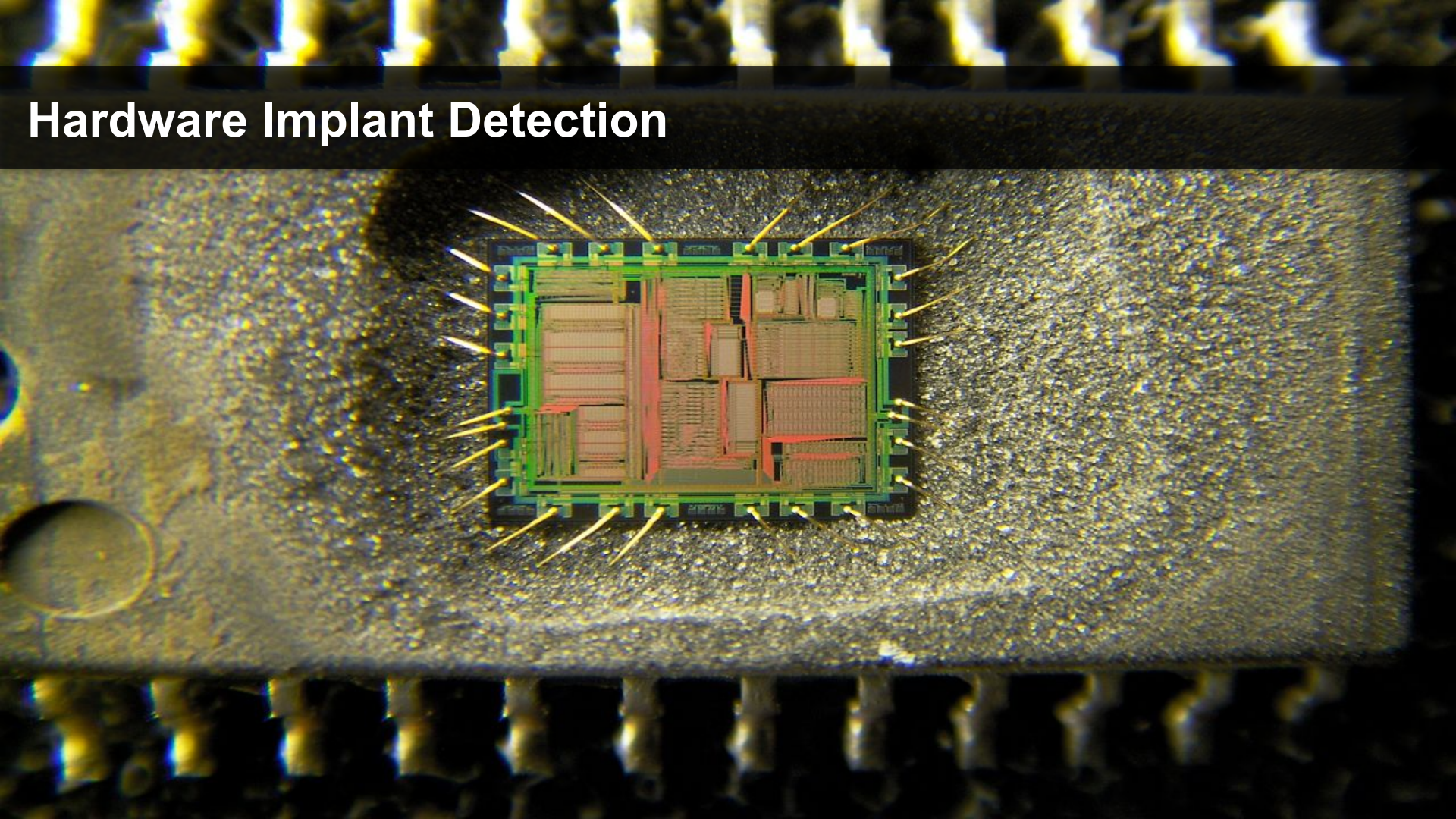
Hardware Implant Detection



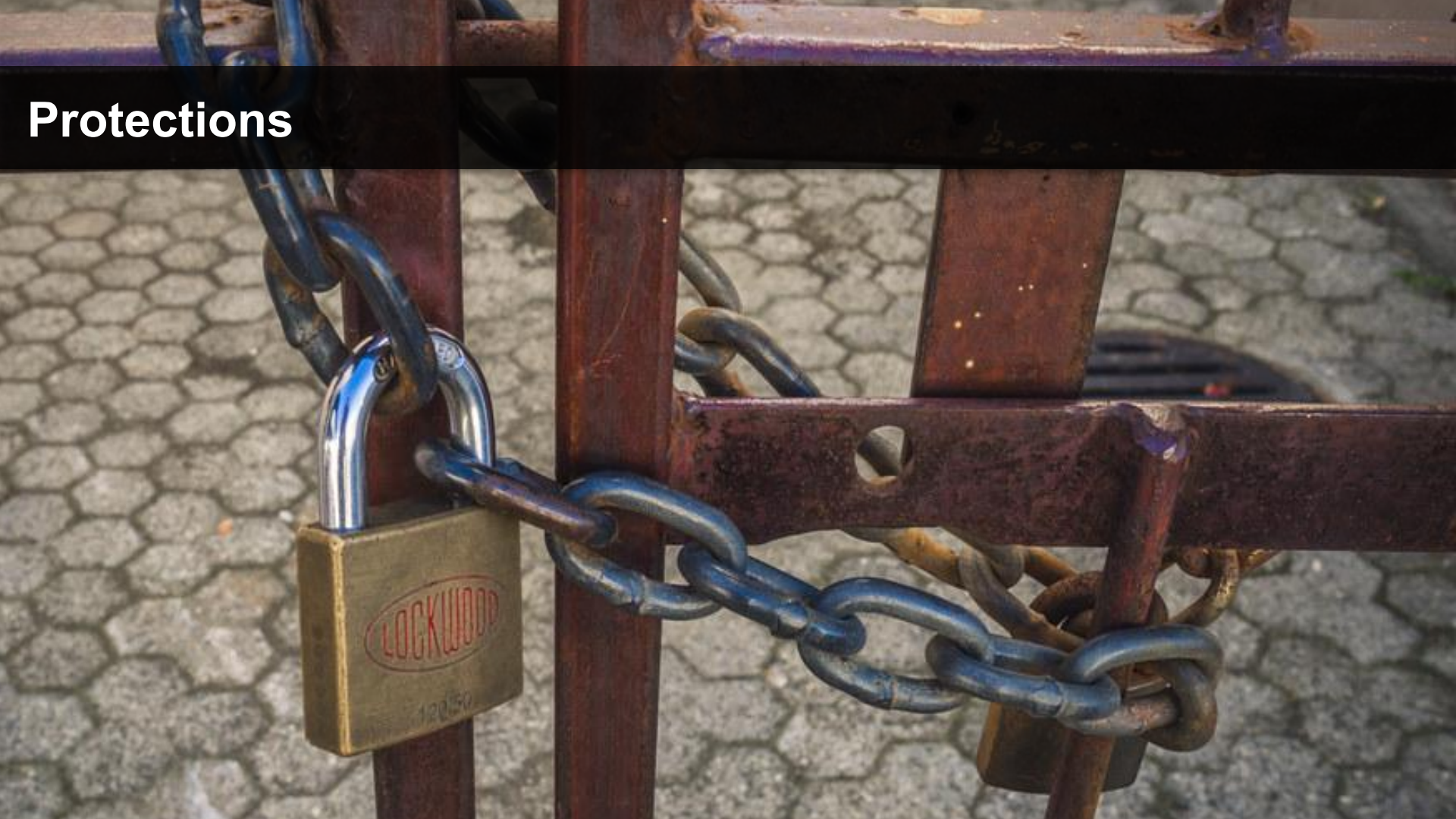
Hardware Implant Detection



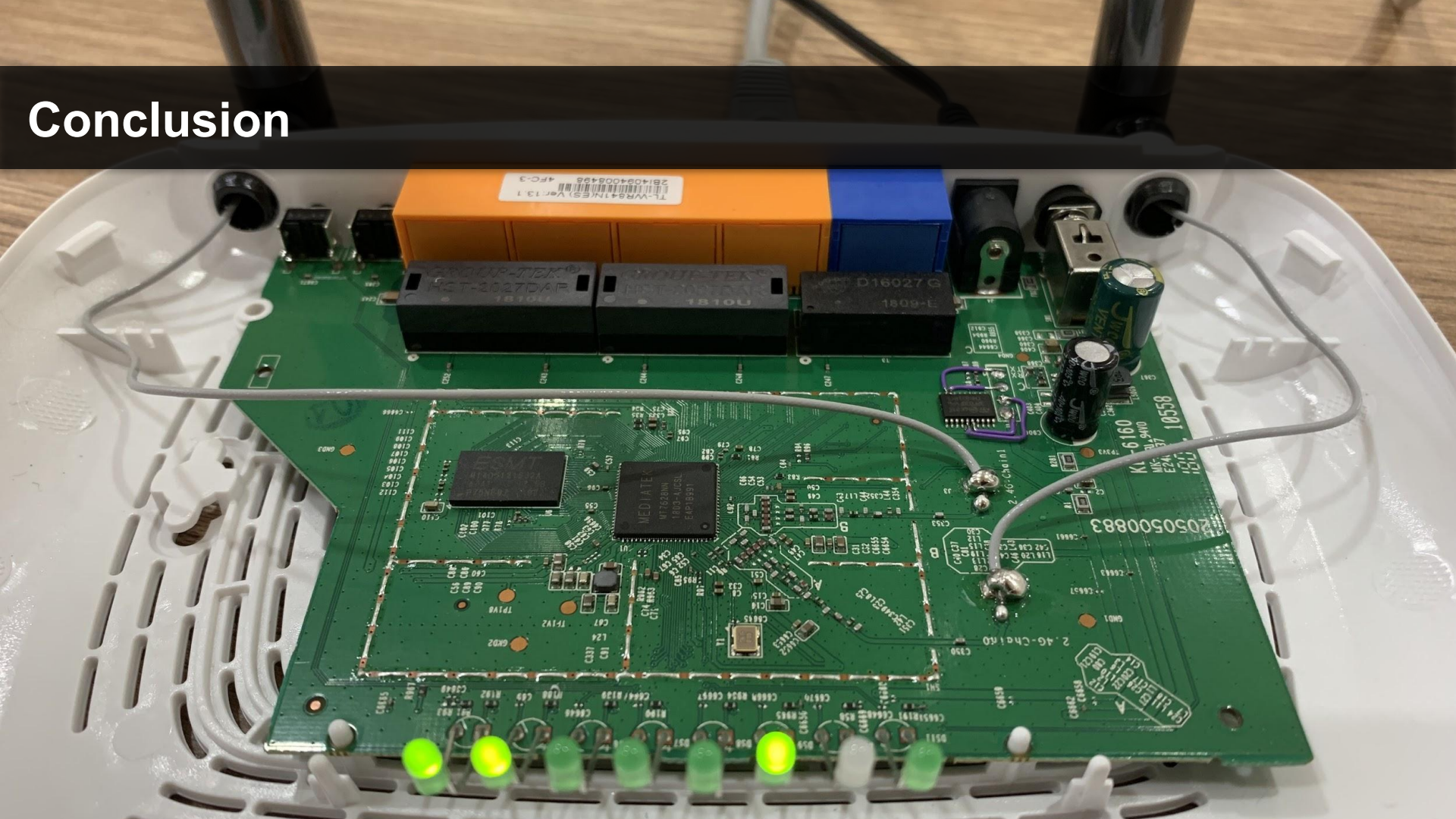
Hardware Implant Detection



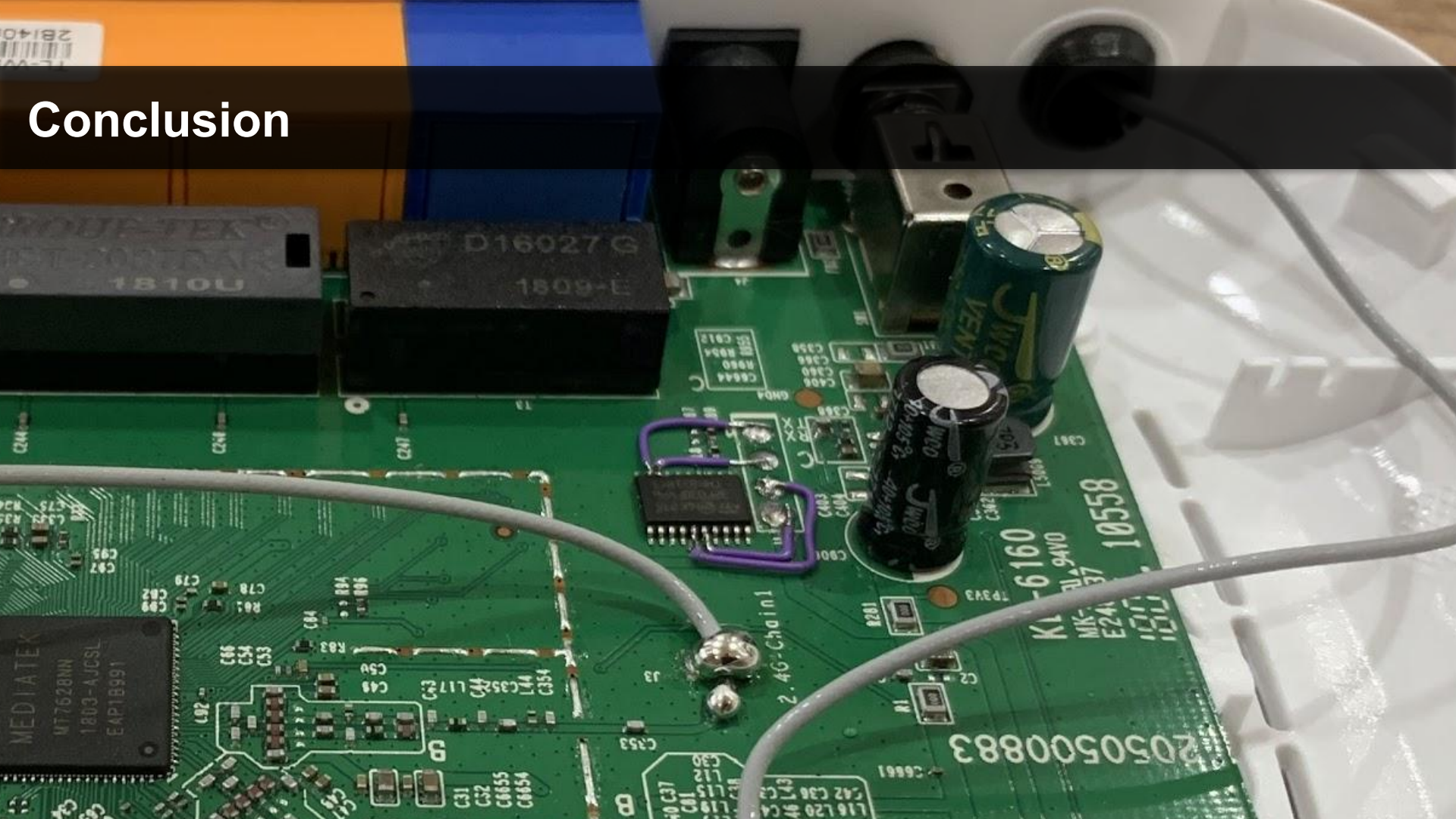
Protections



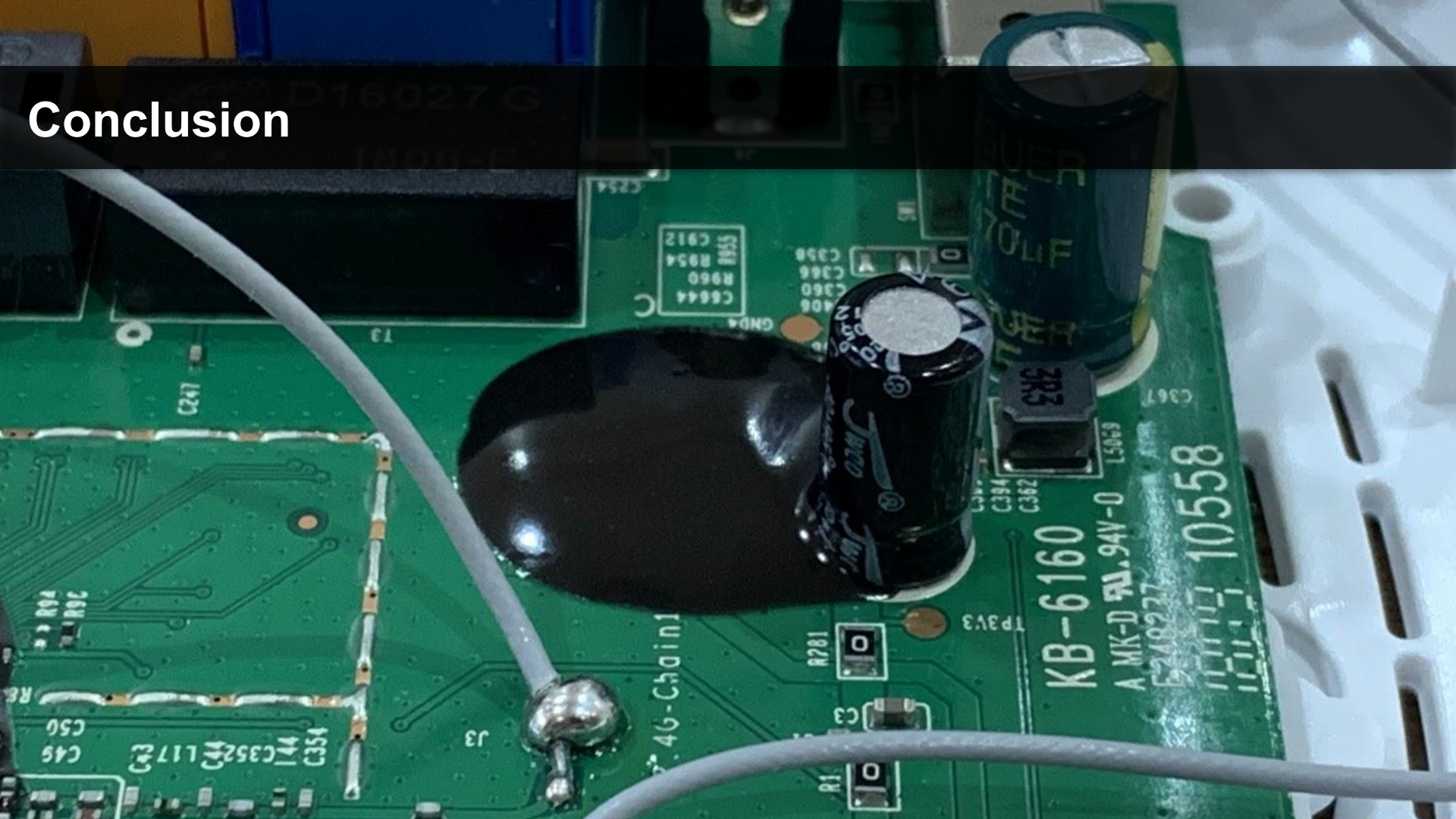
Conclusion



Conclusion



Conclusion



Questions

@6e726d

@lautarofain