Digging Deep: How to Find and Exploit Bugs in IoT Devices

Kelvin WONG

Speaker@

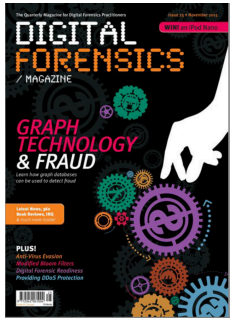
- SANS DFIR Summit
- DFRWS EU
- HTICA US
- DefCON 20
- HITCON
- CodeBule
- AVTokyo
- APWG
- ISC^2 APAC Congress

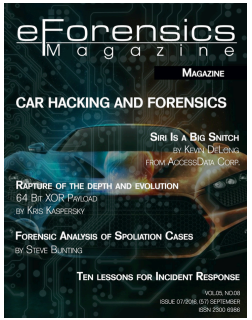
ISLA (Asia Pacific)

2016 Honoree

Publications

- 10 years experience in Digital Forensics
- Facebook Forensics (2011) on Hakin9 Magazine
- Mac Memory Forensics (2014) on Digital Forensics Magazine
- Investigation and Intelligence Framework (2015) on Forensics Focus
- Advanced Mobile Devices Analysis Using JTAG and Chip-Off (2016) on eForensics Magazine





Hacking IoT ?

Attack Vector on IoT

- Ecosystem
- Device Memory
- Device Physical Interfaces
- Device Web Interface
- Device Firmware
- Etc…(OWASP IoT project)

Protocol / Software based

- Wifi
- BLE
- Zigbee
- RF
- NFC
- HCE

Hardware Based ?

Cherry Blossom – Page 124, Para 13

13.2 (S) Firmware Inspection

(S) To be able to inspect a firmware image that is loaded on a device, an adversary would need to disassemble the device, solder a JTAG header onto the board, and extract the firmware from the flash chip through the JTAG using JTAG extraction software. The team has been able to successfully solder a JTAG and extract the firmware from a Linksys WRT54G.

Hardware based method?

- UART
- JTAG
- ISP
- Chip-off

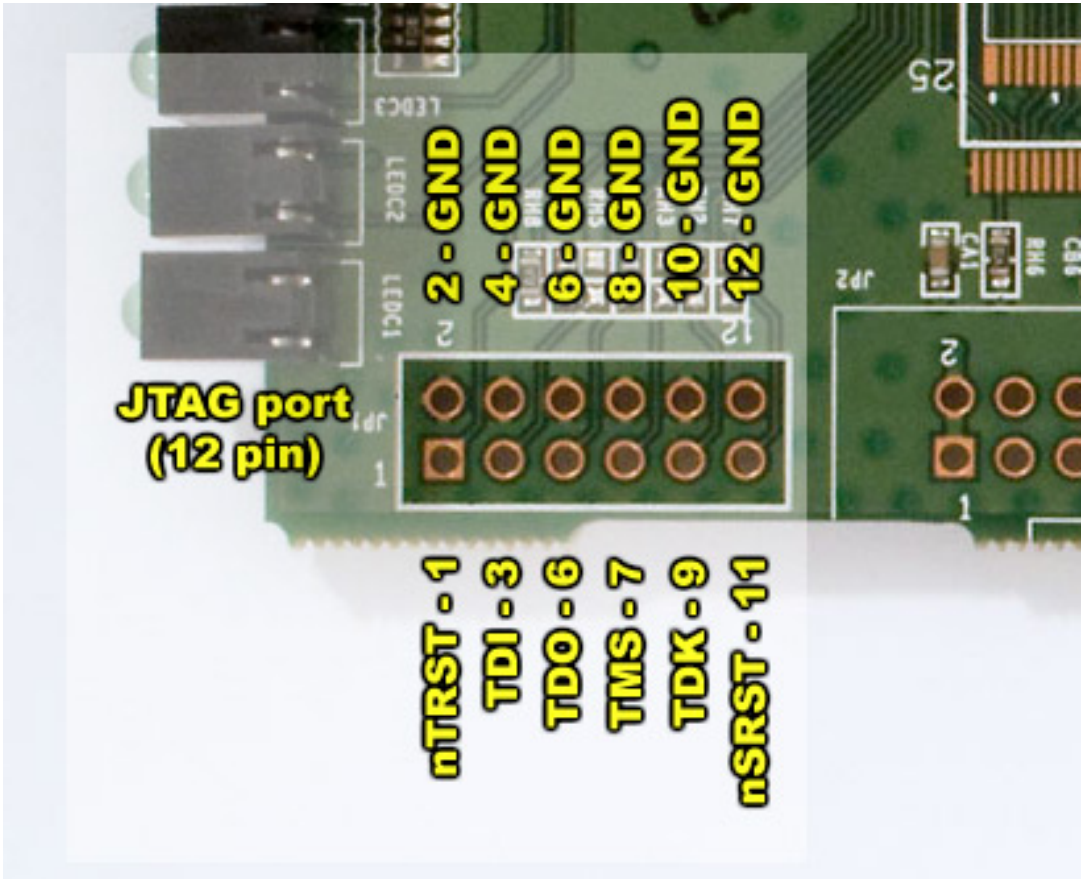
JTAG

- Joint Test Action Group
- Communicate with memory chips through Test Access Ports(TAPs)
- Physical data acquisition
- Have different pins

Test Access Port (TAP)

- TCK – test clock
- TMS – test mode state
- TDI – test data in
- TDO – test data out
- TRST – test reset
- NRST – normal reset
- RTCK – return clock
- GND – ground

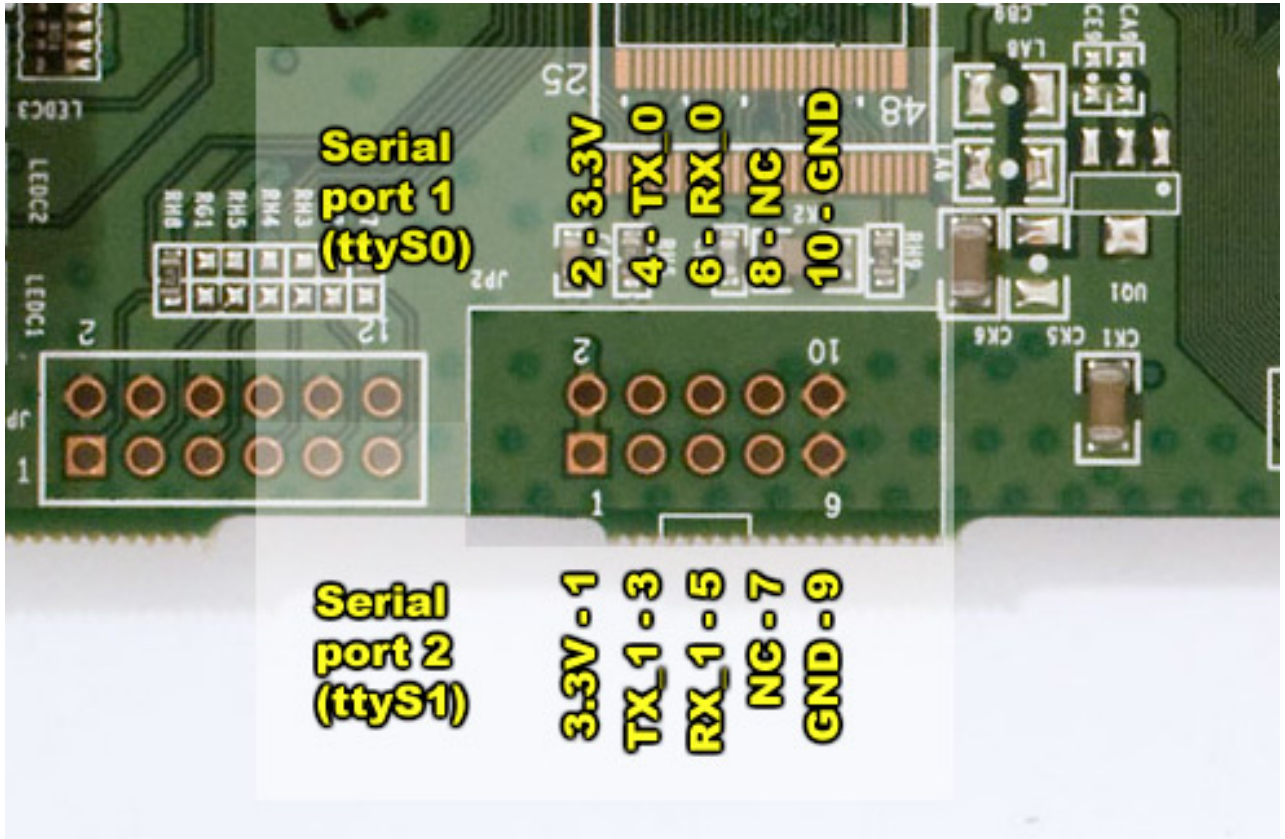
Linksys Router JTAG pins

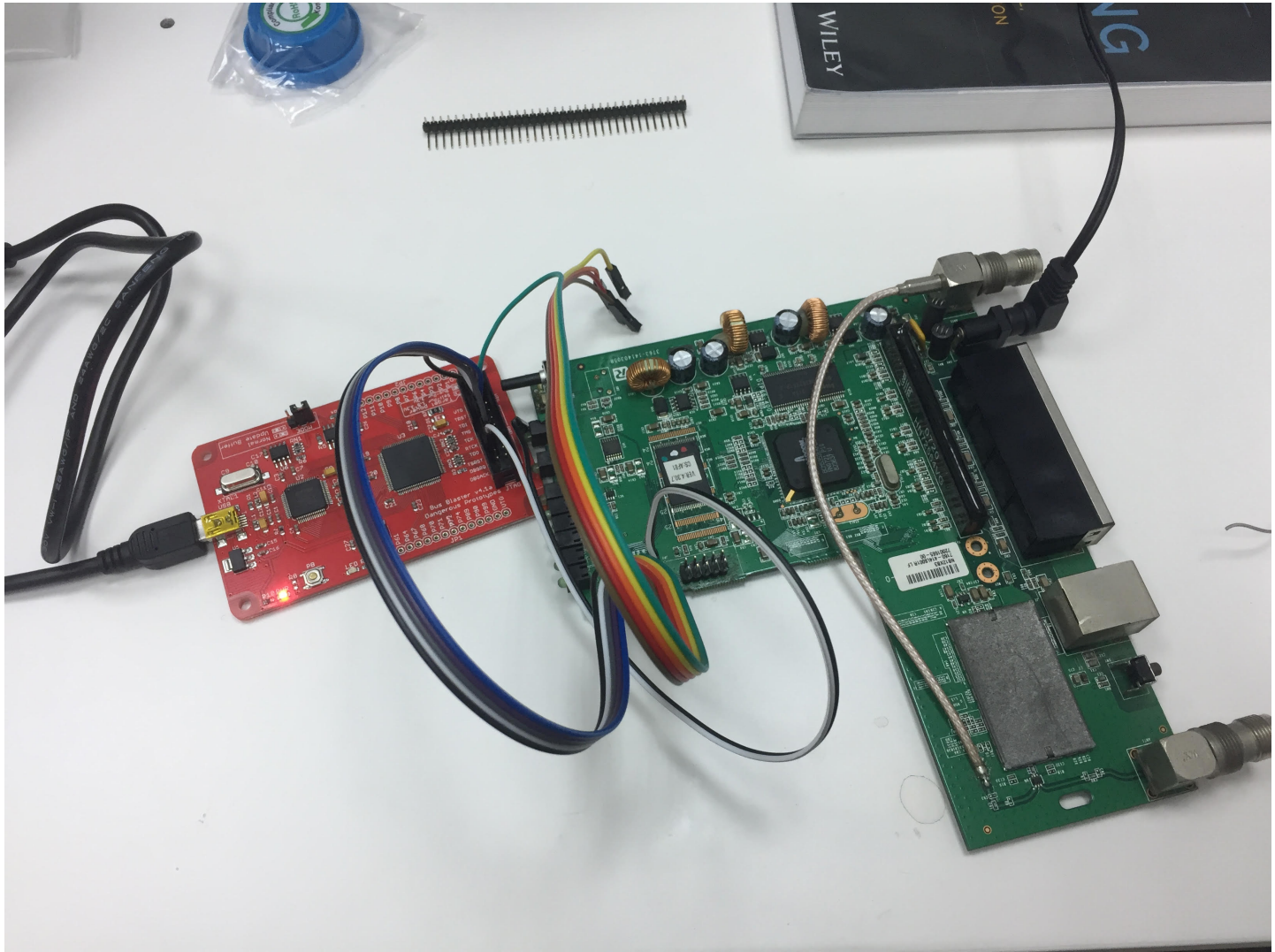


UART

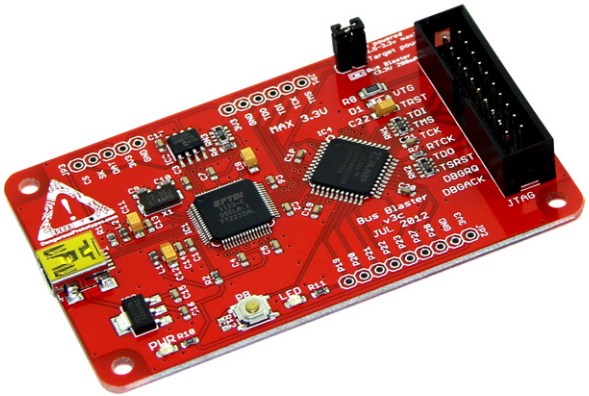
- serial communications over a computer or peripheral device serial port
- Transmitting and receiving serial data
- See the output from console

UART pins


Serial
port 1
(ttyS0)
2 - 3.3V
4 - TX_0
6 - RX_0
8 - NC
10 - GND
Serial
port 2
(ttyS1)
3.3V - 1
TX_1 - 3
RX_1 - 5
NC - 7
GND - 9


WILEY

BusBlaster



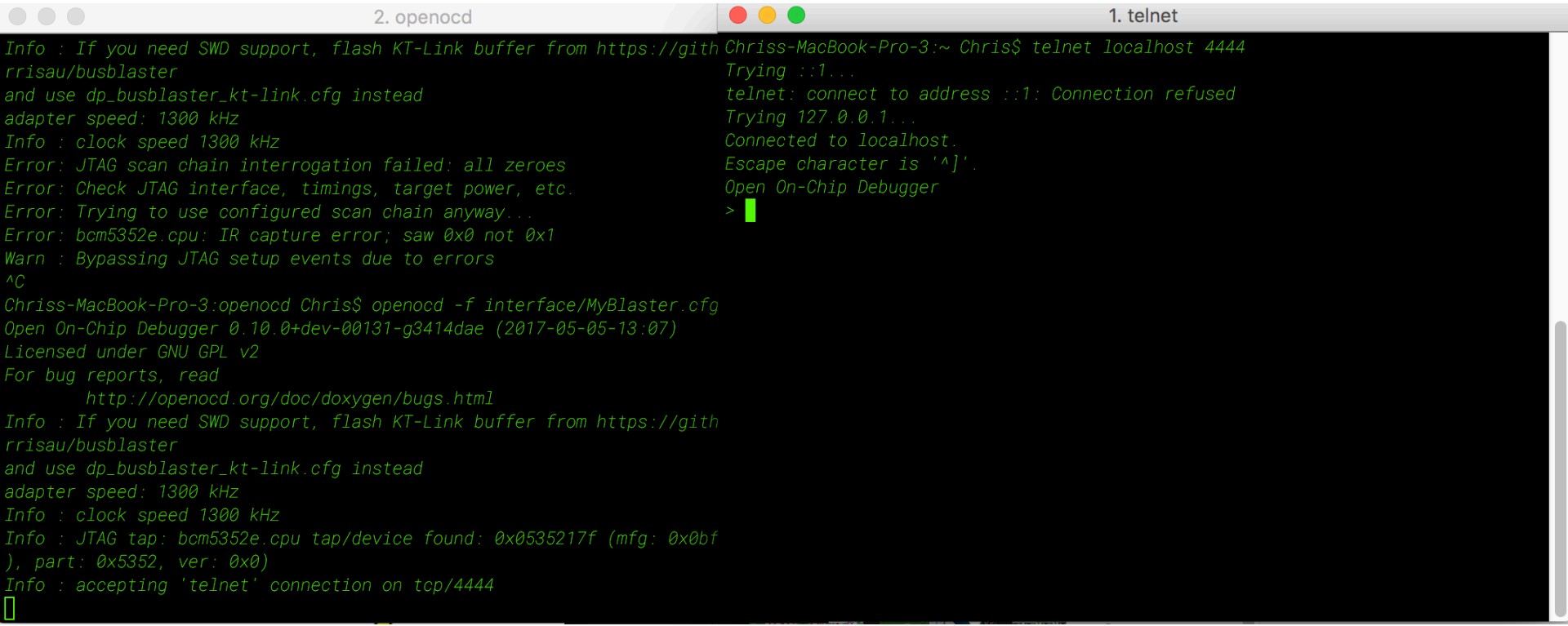
Attify

Etc.....

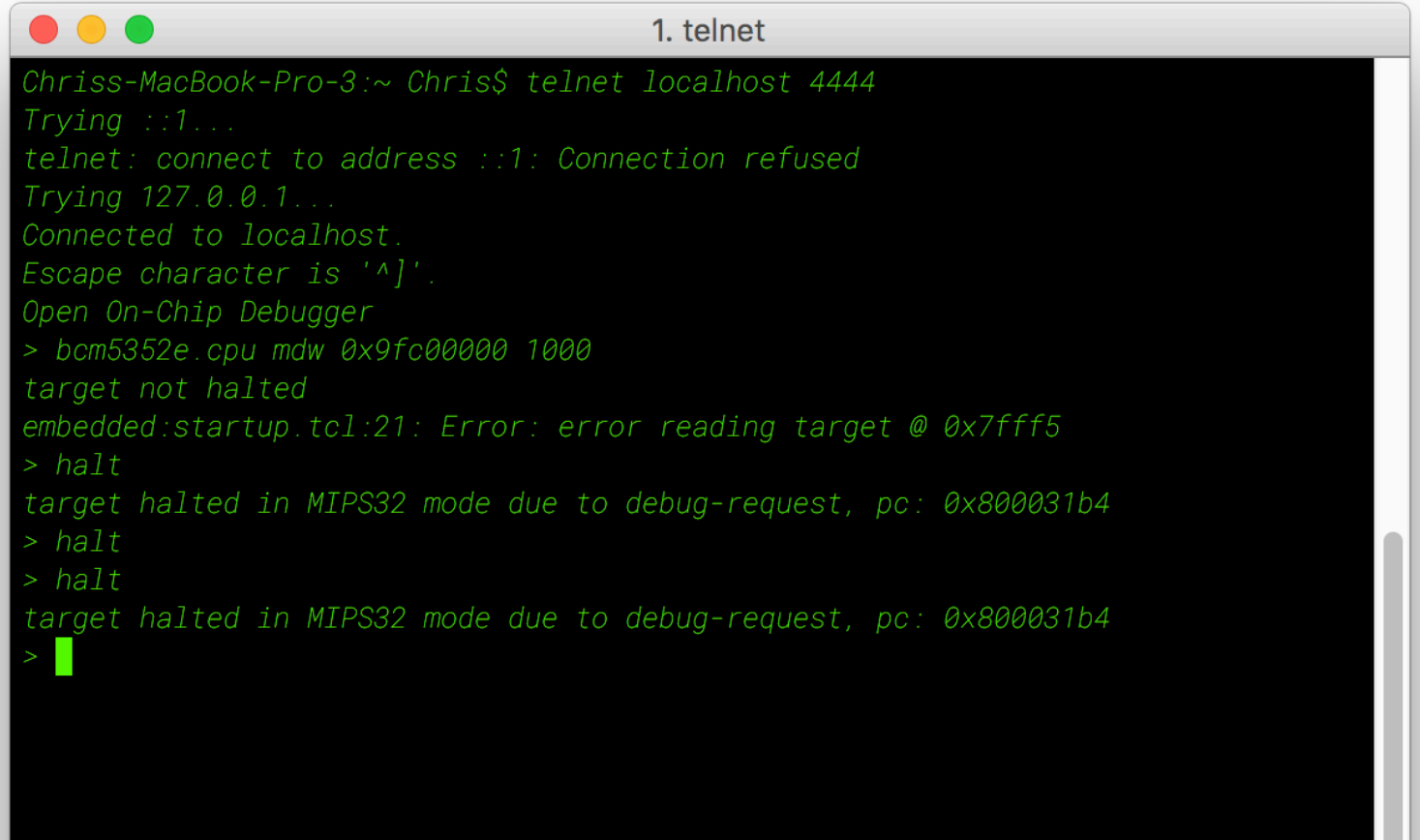
OpenOCD

- Open Source
- Open On-chip Debugger tool
- Provide debugging, in system programming and boundary-scan test
- Work with a list of debug adapter
- Support a list of router/chips configuration

```
Chriss-MacBook-Pro-3:openocd Chris$ openocd -f interface/MyBlaster.cfg
Open On-Chip Debugger 0.10.0+dev-00131-g3414dae (2017-05-05-13:07)
Licensed under GNU GPL v2
For bug reports, read
        http://openocd.org/doc/doxygen/bugs.html
Info : If you need SWD support, flash KT-Link buffer from https://github.com/bha
rrisau/busblaster
and use dp_busblaster_kt-link.cfg instead
adapter speed: 1300 kHz
Info : clock speed 1300 kHz
Info : JTAG tap: bcm5352e.cpu tap/device found: 0x0535217f (mfg: 0x0bf (Broadcom
), part: 0x5352, ver: 0x0)
```


2. openocd
Info : If you need SWD support, flash KT-Link buffer from https://gith
rrisau/busblaster
and use dp_busblaster_kt-link.cfg instead
adapter speed: 1300 kHz
Info : clock speed 1300 kHz
Error: JTAG scan chain interrogation failed: all zeroes
Error: Check JTAG interface, timings, target power, etc.
Error: Trying to use configured scan chain anyway...
Error: bcm5352e.cpu: IR capture error; saw 0x0 not 0x1
Warn : Bypassing JTAG setup events due to errors
^C
Chriss-MacBook-Pro-3:openocd Chris$ openocd -f interface/MyBlaster.cfg
Open On-Chip Debugger 0.10.0+dev-00131-g3414dae (2017-05-05-13:07)
Licensed under GNU GPL v2
For bug reports, read
http://openocd.org/doc/doxygen/bugs.html
Info : If you need SWD support, flash KT-Link buffer from https://gith
rrisau/busblaster
and use dp_busblaster_kt-link.cfg instead
adapter speed: 1300 kHz
Info : clock speed 1300 kHz
Info : JTAG tap: bcm5352e.cpu tap/device found: 0x0535217f (mfg: 0x0bf
), part: 0x5352, ver: 0x0)
Info : accepting 'telnet' connection on tcp/4444
1. telnet
Chriss-MacBook-Pro-3:~ Chris$ telnet localhost 4444
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Open On-Chip Debugger
>

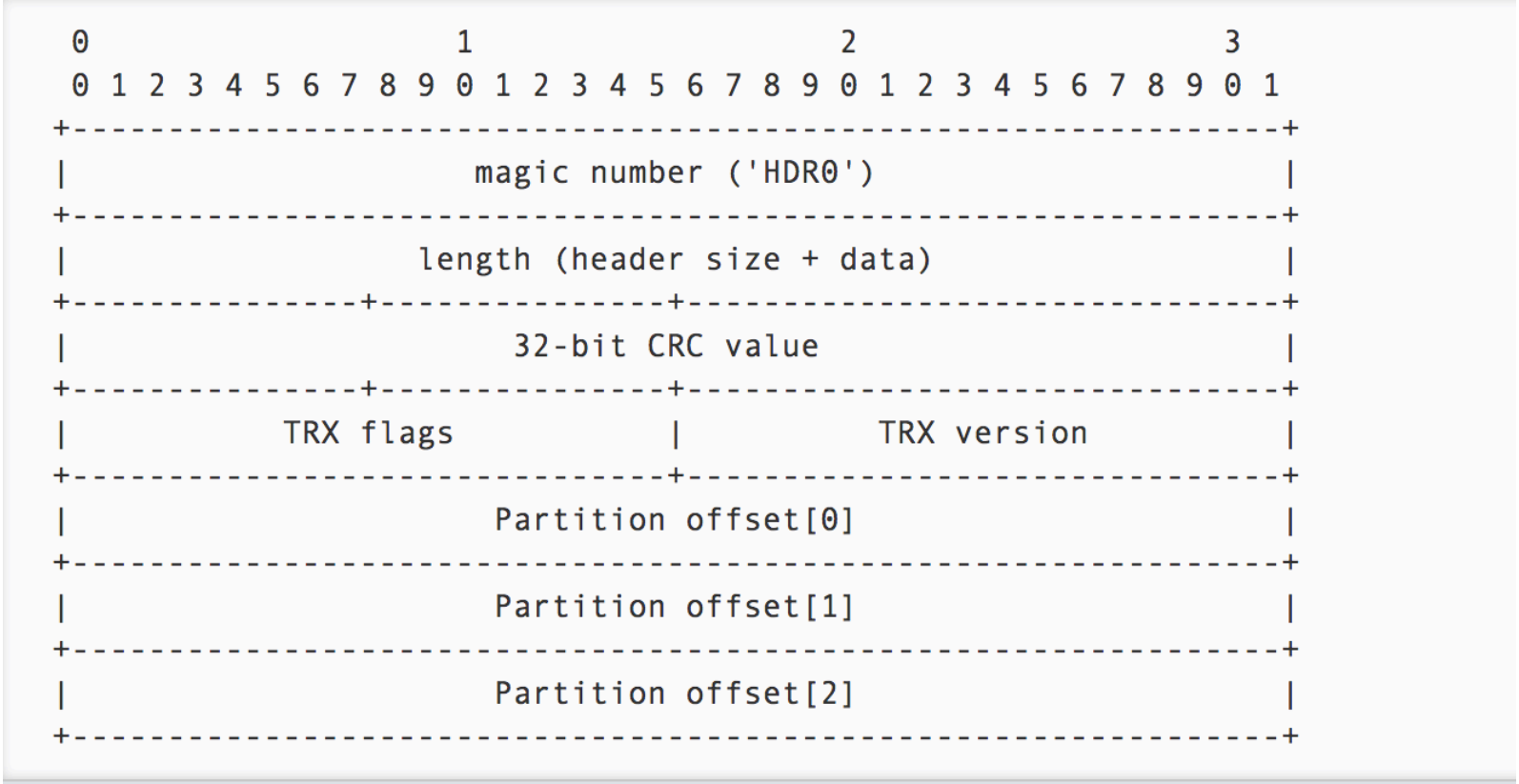
Kill the watchdog and halt system



Print the kernel address value

```
Open On-Chip Debugger
> bcm5352e.cpu mdw 0x9fc40000 100
0x9fc40000 30524448 0035f000 ba4a80fc 00010000 HDR0..5...J.....
0x9fc40010 0000001c 000b9a74 00000000 08088b1f ....t...........
0x9fc40020 568f4a82 69700302 00796767 6c7f5aec .J.V..piggy..Z.l
0x9fc40030 7f76751c debb333b 76321b24 31dac736 .uv.;3..$.2v6..1
0x9fc40040 f599c778 c2e8602e ade9872d 8271b0ca x....`..-.....q.
0x9fc40050 83e568a9 a8af4aa8 f039dada 4029535d .h...J....9.]S)@
0x9fc40060 da5d2342 e03b5b9b 571e26f6 cdab54b2 B#]..[;..&.W.T..
0x9fc40070 15fe7bb5 1c78dbd3 35e9ae63 00842b14 .{....x.c..5.+..
0x9fc40080 aab3d715 c7288953 2221c9b9 8b51157a ....S.(...!"z.Q.
0x9fc40090 4c72384a 3be66f3f 8938c6f6 153aff69 J8rL?o.;..8.i.:.
0x9fc400a0 bceed64b efbefbef 3be3fdfb 4a2452ab K..........;.R$J
0x9fc400b0 f67dfd9f ffdfd9f7 7f8bbfcf 06f1d061 ..}.........a...
0x9fc400c0 81bd7cc3 d6f746be 790d9bd4 9a72fcea .|...F....y..r.
0x9fc400d0 2a1c77e8 328c1836 3240df37 99da3519 .w.*6..27.@2.5..
0x9fc400e0 b9a37cb2 fcfc5f39 be6d6dd7 7fba772c .|..9_...mm.,w..
0x9fc400f0 fbe8b694 4ea34e8e 97c0ca82 388d248d .....N.N....$.8
0x9fc40100 d0ce7893 b23d4398 4ee34ad1 9a59cf05 .x...C=..J.N..Y.
```

Magic Header of Kernel Section



Memory Dump

- firmware-recovery script from Openocd
- Image_dump(If address do not match)
- CFE Memory: 0x9fc00000,size:0x40000
  KERNEL Memory : 0x9fc40000, size: 0x1B0000
  NVRAM Memory : 0x9fDF0000, size: 0x10000

linksys_KERNEL.bin | linksys_NVRAM.bin

Edit As: Hex | Run Script | Run Template

	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	0123456789012345
9040h:	68	5F	6D	6F	64	65	3D	6E	6F	6E	65	00	70	70	74	70	h_mode=none.pptp
9050h:	5F	67	65	74	5F	69	70	3D	00	70	70	74	70	5F	70	61	_get_ip=.pptp_pa
9060h:	73	73	3D	31	00	70	70	70	5F	6B	65	65	70	61	6C	69	ss=1.ppp_keepali
9070h:	76	65	3D	30	00	6D	74	75	5F	65	6E	61	62	6C	65	3D	ve=0.mtu_enable=
9080h:	30	00	64	31	31	67	5F	72	74	73	3D	32	33	34	37	00	0.d11g_rts=2347.
9090h:	62	6C	6F	63	6B	5F	61	63	74	69	76	65	78	3D	30	00	block_activex=0.
90A0h:	77	6C	30	5F	72	78	63	68	61	69	6E	5F	70	77	72	73	wl0_rxchain_pwrs
90B0h:	61	76	65	5F	65	6E	61	62	6C	65	3D	31	00	61	67	30	ave_enable=1.ag0
90C0h:	3D	30	78	30	32	00	68	74	74	70	5F	70	61	73	73	77	=0x02.http_passw
90D0h:	64	3D	61	64	6D	69	6E	00	77	6C	5F	77	70	61	5F	70	d=admin.wl_wpa_p
90E0h:	73	6B	3D	00	72	65	6D	6F	74	65	5F	6D	67	74	5F	68	sk=.remote_mgt_h
90F0h:	74	74	70	73	3D	30	00	62	6C	6F	63	6B	5F	77	61	6E	ttps=0.block_wan
9100h:	3D	31	00	6C	61	6E	5F	73	74	70	3D	30	00	77	6C	30	=1.lan_stp=0.wl0
9110h:	5F	77	6D	65	5F	61	70	5F	76	69	3D	37	20	31	35	20	_wme_ap_vi=7 15
9120h:	31	20	36	30	31	36	20	33	30	30	38	20	6F	66	66	00	1 6016 3008 off.
9130h:	77	6C	30	5F	62	73	73	5F	6D	61	78	61	73	73	6F	63	wl0_bss_maxassoc
9140h:	3D	31	32	38	00	77	6C	5F	6D	6F	64	65	3D	61	70	00	=128.wl_mode=ap.
9150h:	73	6B	69	70	5F	61	6D	64	5F	63	68	65	63	6B	3D	30	skip_amd_check=0
9160h:	00	77	6C	30	5F	63	6C	6F	73	65	64	3D	30	00	77	6C	.wl0_closed=0.wl
9170h:	30	5F	72	61	74	65	3D	30	00	77	6C	30	5F	70	6C	63	0_rate=0.wl0_plc
9180h:	70	68	64	72	3D	6C	6F	6E	67	00	77	61	6E	5F	70	70	phdr=long.wan_pp
9190h:	74	70	5F	67	61	74	65	77	61	79	3D	00	77	6C	30	5F	tp_gateway=.wl0_
91A0h:	6D	61	63	6D	6F	64	65	3D	64	69	73	61	62	6C	65	64	macmode=disabled
91B0h:	00	64	31	31	67	5F	72	61	74	65	73	65	74	3D	64	65	.d11g_rateset=de
91C0h:	66	61	75	6C	74	00	77	6C	5F	77	70	61	5F	67	74	6B	fault.wl_wpa_gtk
91D0h:	5F	72	65	6B	65	79	3D	33	36	30	30	00	73	65	6C	5F	_rekey=3600.sel

linksys_KERNEL.bin | **linksys_NVRAM.bin**

Edit As: Hex | Run Script | Run Template

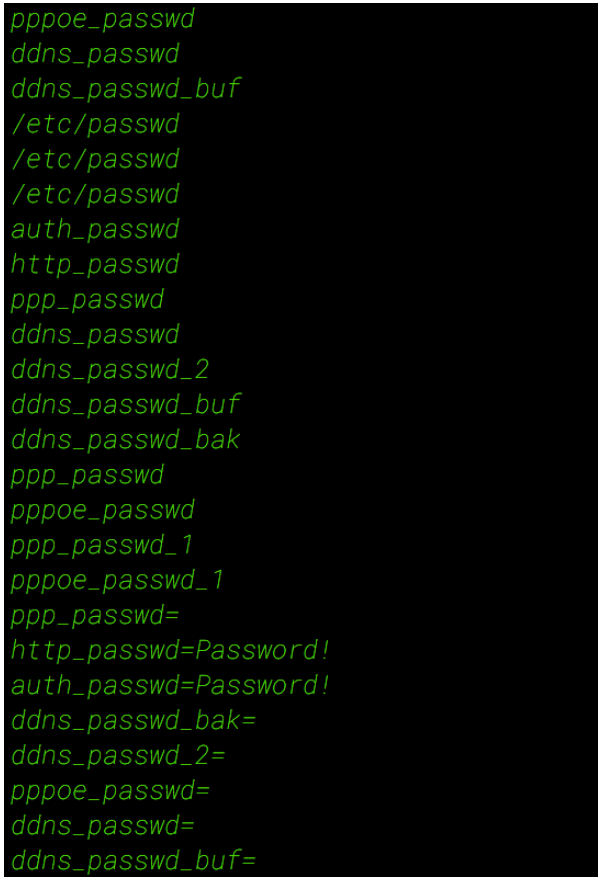
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	0123456789012345
9E00h:	76	6C	3D	30	00	73	64	72	61	6D	5F	63	6F	6E	66	69	vl=0.sdram_confi
9E10h:	67	3D	30	78	30	30	36	32	00	6C	6F	67	5F	65	6E	61	g=0x0062.log_ena
9E20h:	62	6C	65	3D	30	00	70	70	70	5F	61	63	3D	00	77	6C	ble=0.ppp_ac=.wl
9E30h:	30	5F	63	6F	75	6E	74	72	79	3D	57	6F	72	6C	64	77	0_country=Worldw
9E40h:	69	64	65	00	66	69	6C	74	65	72	5F	77	65	62	5F	75	ide.filter_web_u
9E50h:	72	6C	31	30	3D	00	76	6C	61	6E	31	70	6F	72	74	73	rl10=.vlan1ports
9E60h:	3D	34	20	35	00	64	6D	7A	5F	69	70	61	64	64	72	3D	=4 5.dmz_ipaddr=
9E70h:	30	00	77	6C	5F	77	64	73	3D	00	73	65	63	75	72	69	0.wl_wds=.securi
9E80h:	74	79	5F	6D	6F	64	65	5F	6C	61	73	74	3D	00	65	6F	ty_mode_last=.eo
9E90h:	75	5F	70	72	69	76	61	74	65	5F	6B	65	79	3D	31	64	u_private_key=1d
9EA0h:	66	30	32	64	37	33	30	61	31	61	66	36	38	36	64	34	f02d730a1af686d4
9EB0h:	33	30	35	32	66	38	66	63	63	37	63	33	36	35	32	34	3052f8fcc7c36524
9EC0h:	35	36	62	61	33	64	31	35	61	35	33	38	61	31	35	31	56ba3d15a538a151
9ED0h:	31	65	34	64	35	37	36	32	39	33	31	34	37	64	66	38	1e4d576293147df8
9EE0h:	39	66	37	37	30	34	31	34	64	38	37	34	64	35	32	36	9f770414d874d526
9EF0h:	30	66	39	38	66	39	63	63	38	30	65	61	38	38	31	66	0f98f9cc80ea881f
9F00h:	33	33	33	31	63	66	34	64	32	36	63	39	65	35	39	64	3331cf4d26c9e59d
9F10h:	33	36	37	63	31	30	64	38	30	36	35	35	31	36	33	39	367c10d806551639
9F20h:	32	32	31	33	63	34	61	32	32	30	66	35	63	61	65	38	2213c4a220f5cae8
9F30h:	64	38	63	33	34	38	33	64	38	64	38	34	37	32	63	66	d8c3483d8d8472cf
9F40h:	30	38	65	62	65	35	62	30	33	63	34	30	65	39	64	36	08ebe5b03c40e9d6
9F50h:	65	62	31	38	65	33	37	30	36	61	64	66	62	61	62	64	eb18e3706adfbabd
9F60h:	38	31	61	30	62	65	36	36	30	34	31	35	63	31	32	32	81a0be660415c122
9F70h:	34	64	66	39	32	39	63	34	62	31	30	35	63	30	32	33	4df929c4b105c023
9F80h:	32	36	66	32	61	30	36	36	37	64	36	63	38	31	66	66	26f2a0667d6c81ff

Whole FLASH sturture

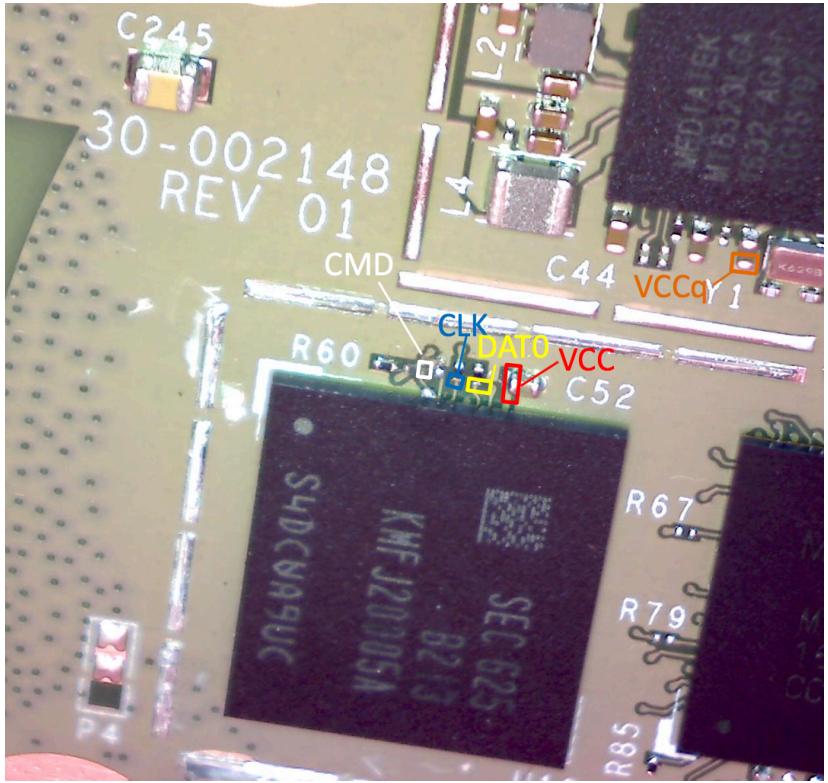
- Common Firmware Environment (CFE) - bootloader
- Kernel - firmware
- NVRAM - store variable information

Secret

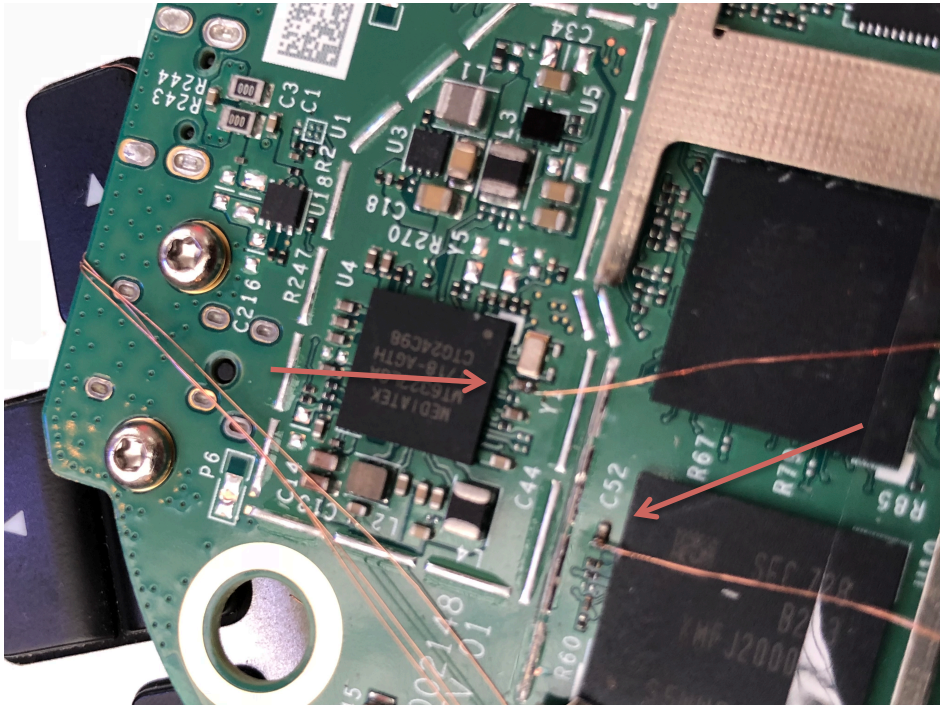
- Plaintext username and password
- No authentication is required for console login
- RAM address: 0x80000000 size: 0x01000000

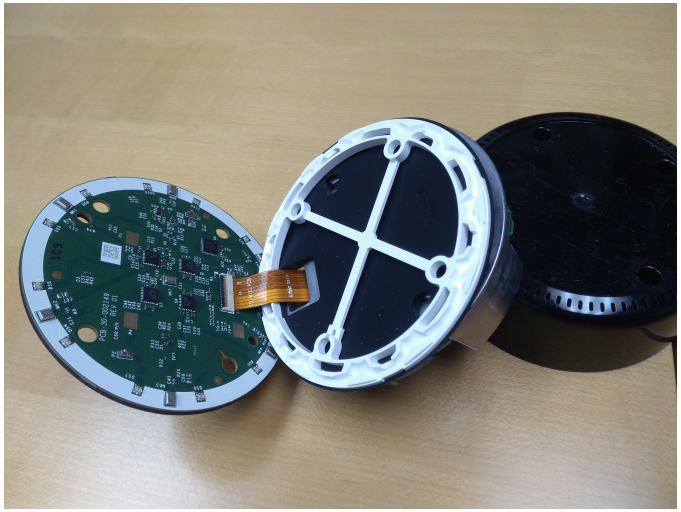


ISP – In System Circuit Programming

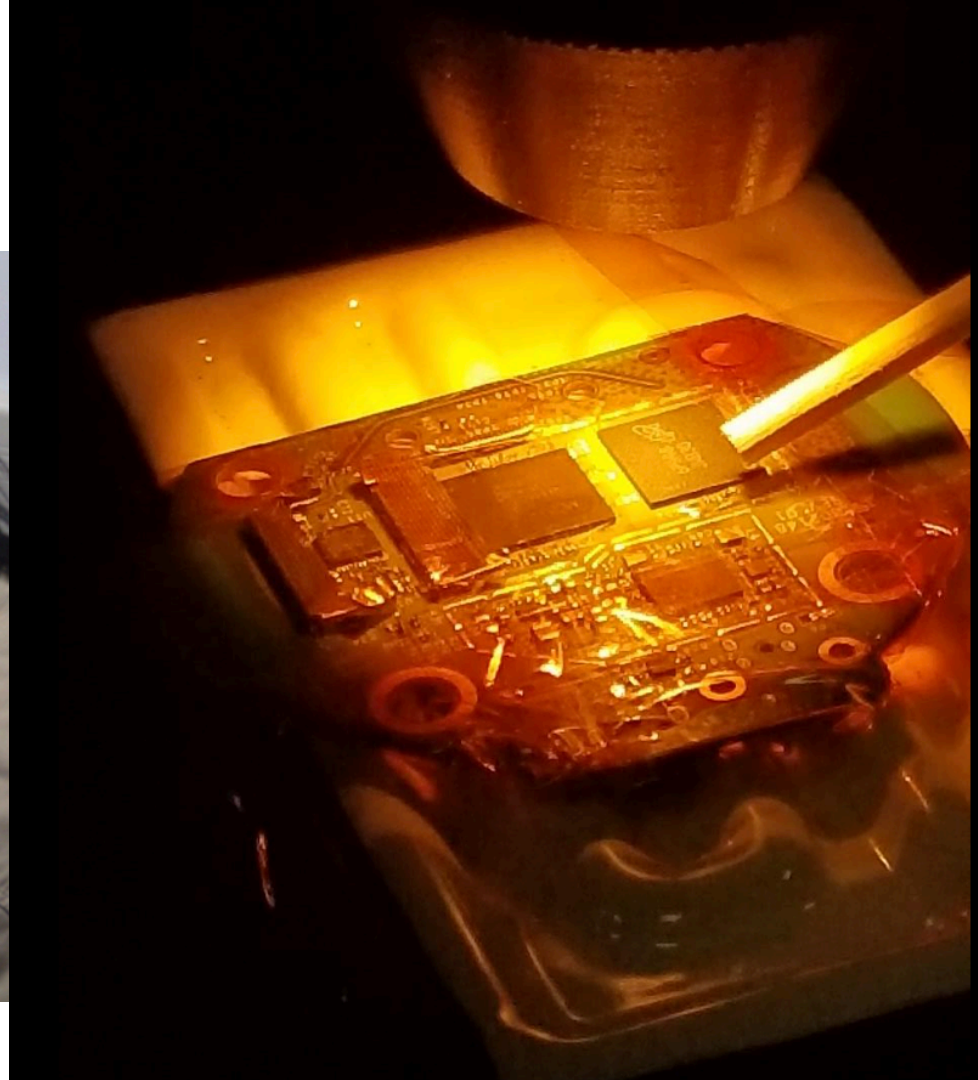


Amazon Alexa

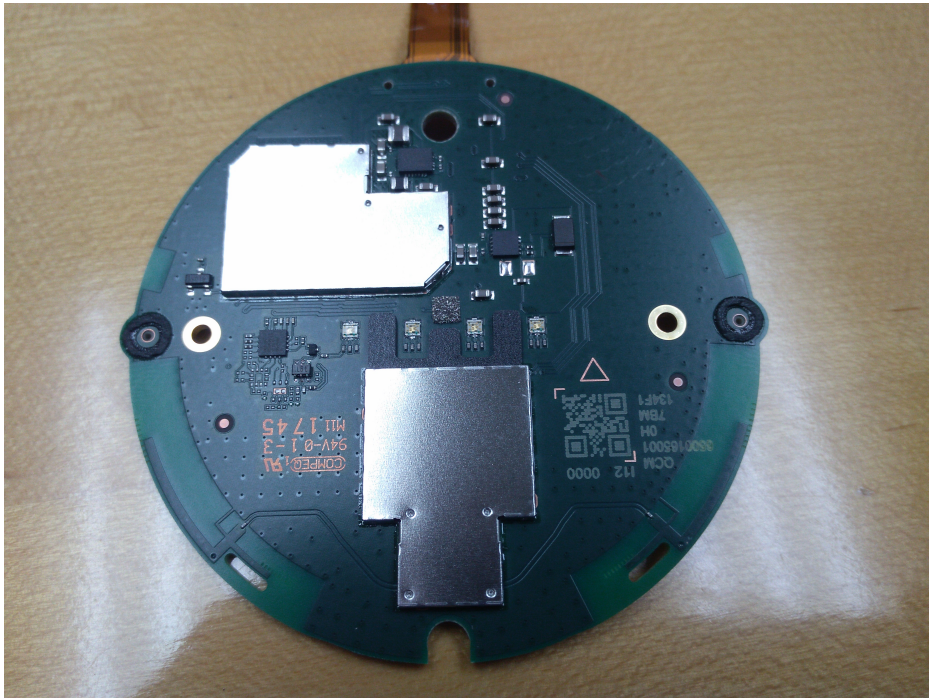




Chip-Off



Google Home Mini



Chip-off Village by VXRL

VXCON on 21-22 April in Hong Kong

Discount code for HITB AMS

‘hitb@ams_@vxcon2018’

https://www.eventbrite.hk/e/vxcon-2018-tickets-43644511910

Or www.vxcon.hk for agenda

Thank You!