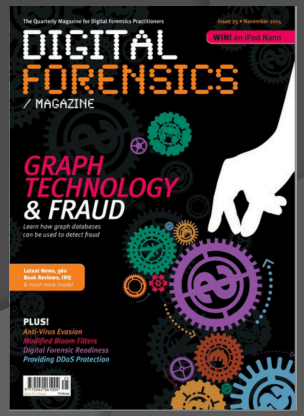
Advanced Mobile Devices Analysis Using JTAG and Chip-off

Forensics Ninja

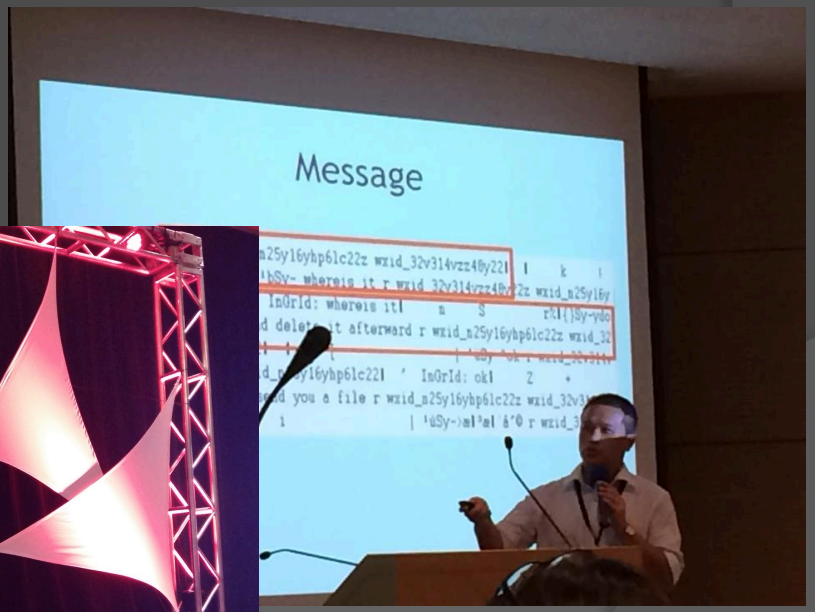
Who am I

- Captain a.k.a Forensics Ninja
- Research since 2010
- 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)



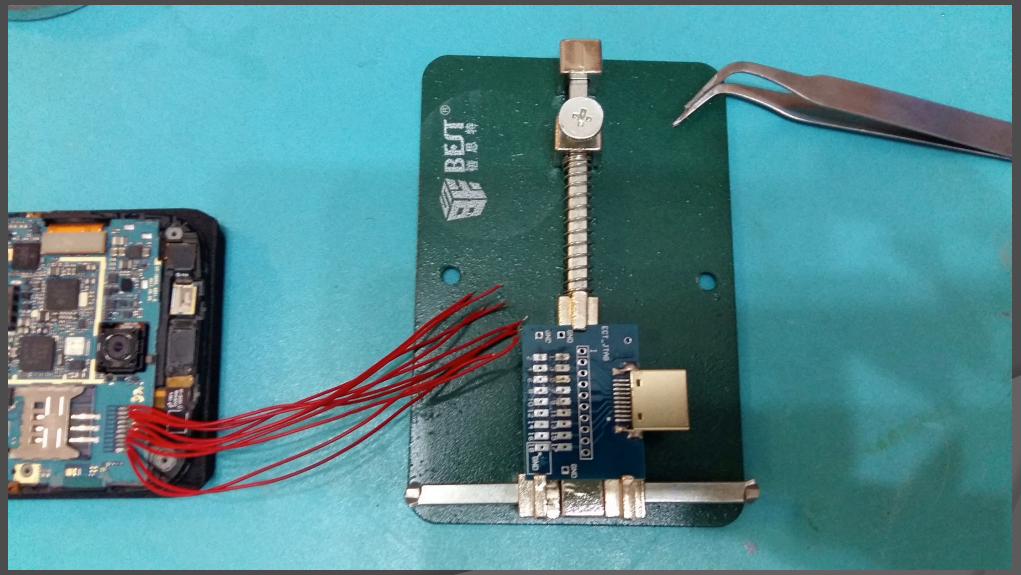
Speaker@

- SANS DFIR
- DefCON 20
- HITCON
- AVTokyo
- APWG
- HTCIA
- VXCON



Agenda

- Introduction to JTAG and Chip Off
- Analysis on JTAG and eMMC dump
- Demo



Training Course

- TeelTech Advanced JTAG / Chip-Off Mobile Forensics
- Cellebrite JTAG Extraction and Decoding
- H11 JTAG Data Recovery and Mobile Phone Repair
- XRY Advanced Acquisition Training
- viaforensics (NowSecure) until 2012
- Course Fee around USD4,000

Why JTAG / Chip-Off?

- Physical vs Logical vs Forensics tools
- Bricked
- Locked without debugging mode
- Damaged
- Special cases

What is JTAG?

- Joint Test Action Group
- Test Access Ports (TAPs) to collect raw data from a memory chips
- Not chip-off and ISP
- Extreme physical data acquisition
- Advanced technique
- Soldering and De-soldering

Price lists

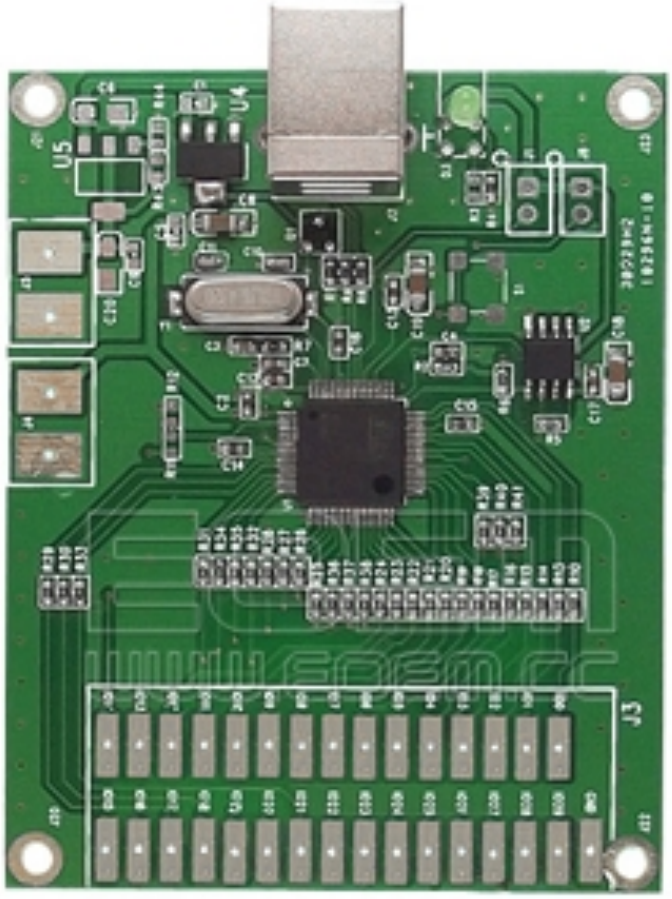
- Source from NowSecure
- US dollars

Soldering iron and stand $50
Solder and solder wick $15
Kynar wire $15
Magnifying light $65
Power supply $100
Tool Kit $35
Multimeter tool $40
Jumper wires $45
PC Header $5
RIFF Box JTAG $170
Medusa JTAG $160
Optional adapters $80

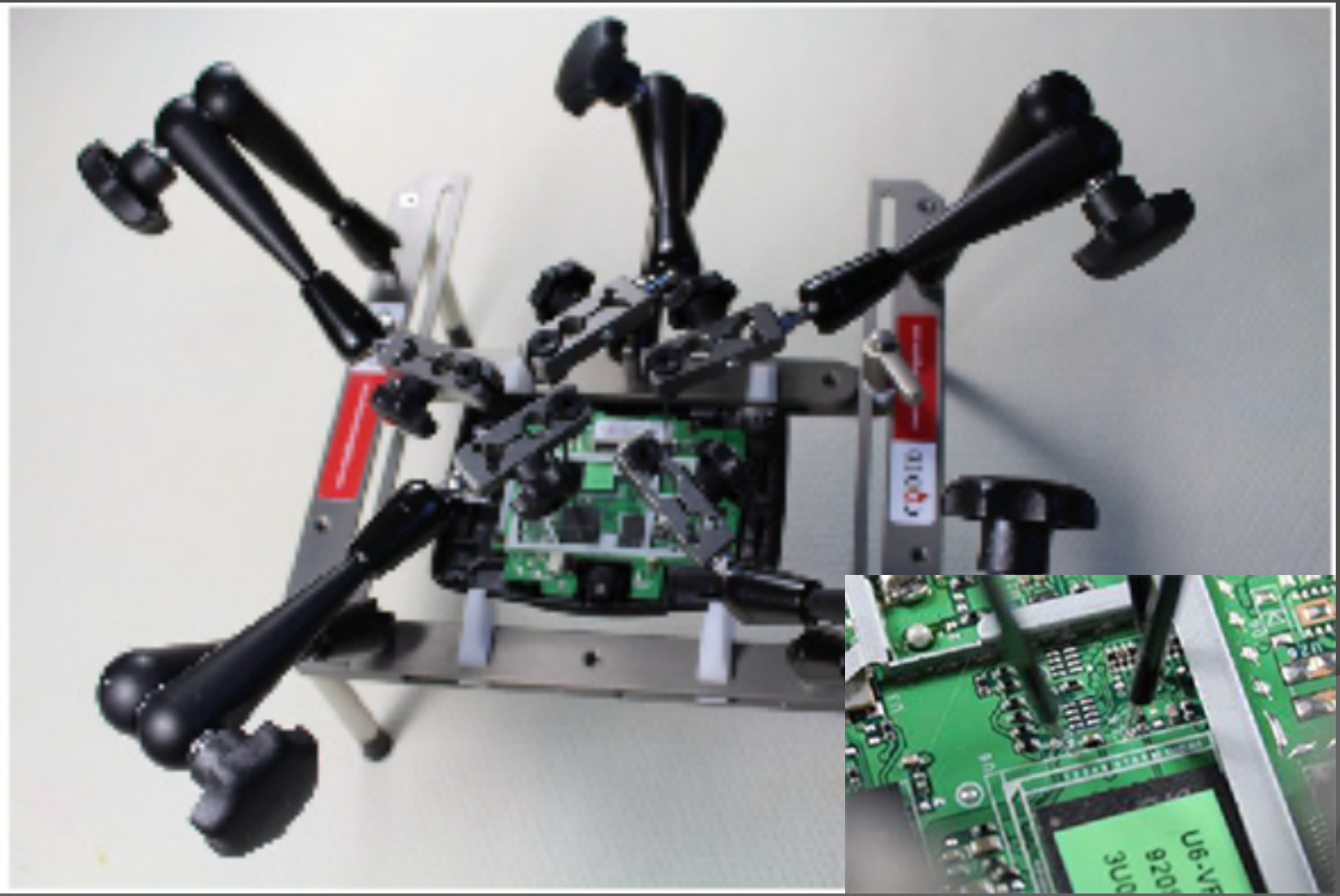
Total: $780

JTAG Box

JTAG Finder

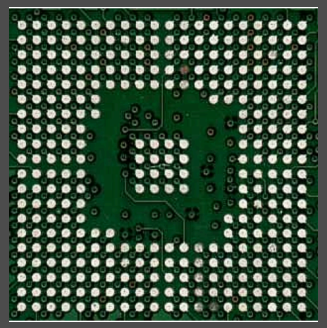


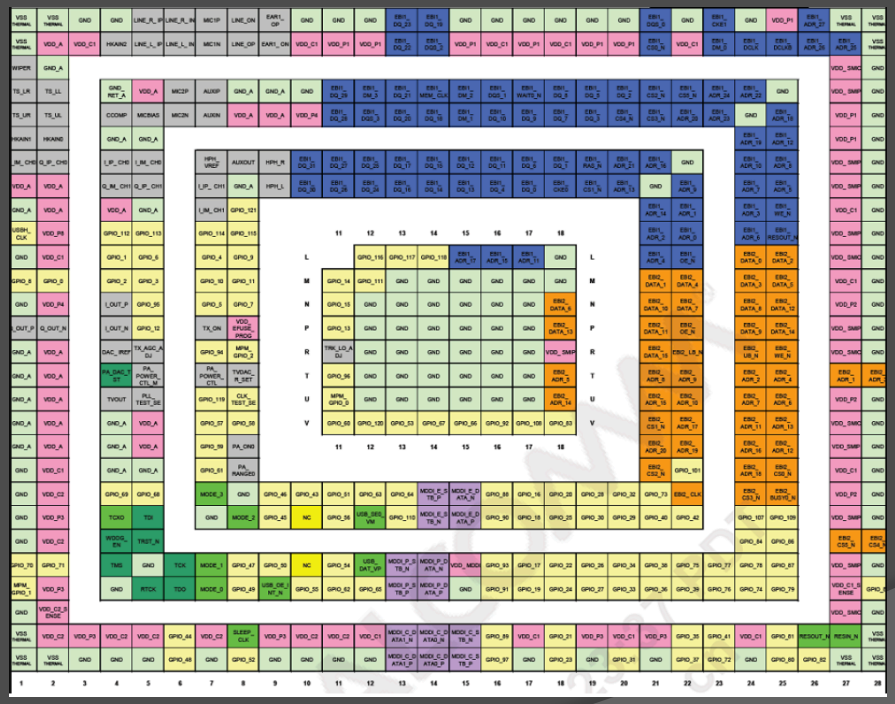
Mounting Frame & Arms



BGA (eg 162 or 169)

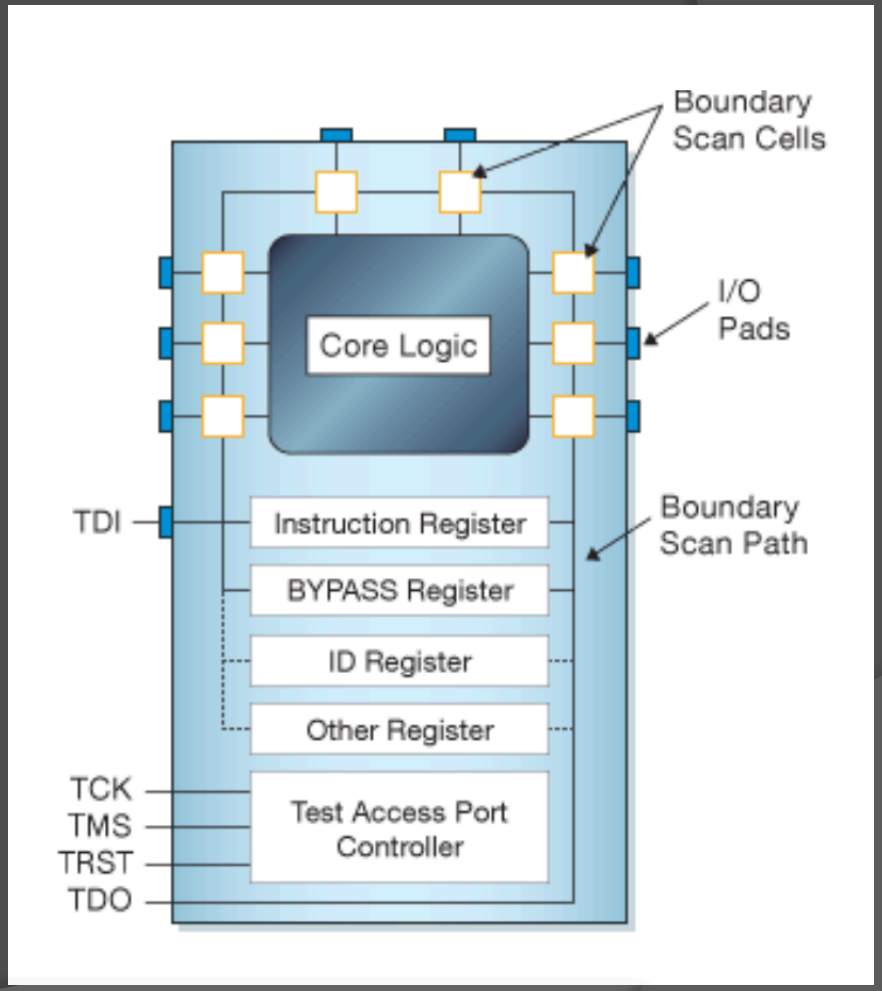
- Ball Grid Array



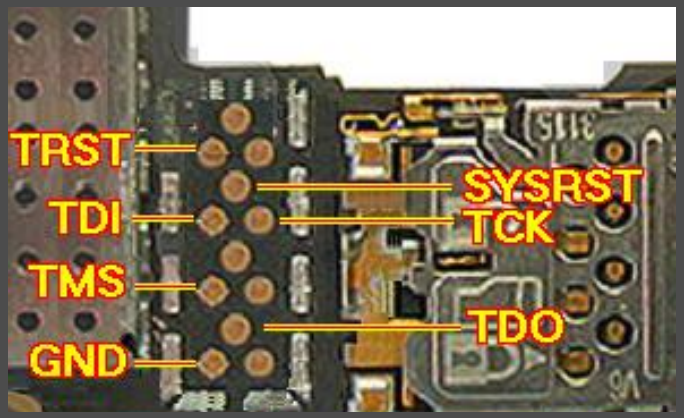


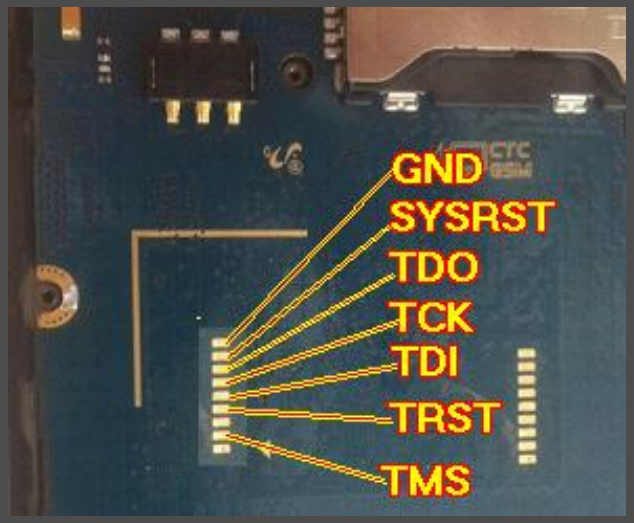
TAP

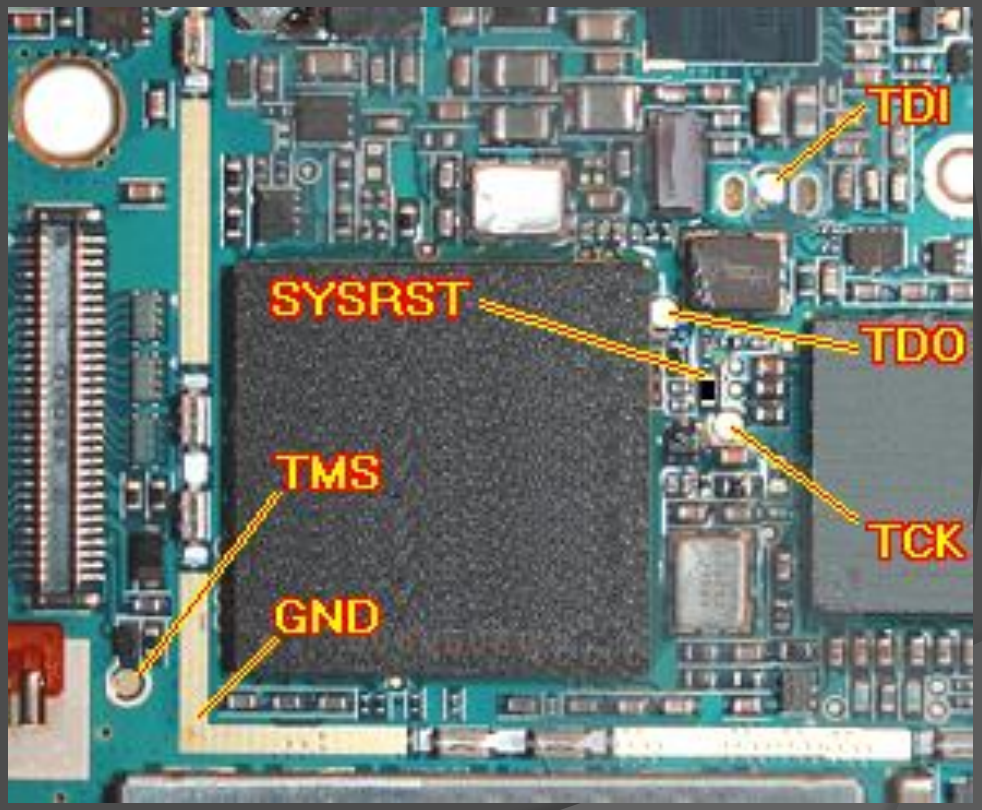
- TCK – test clock
- TMS – test mode state
- TDI – test data in
- TDO – test data out
- TRST – test reset
- NRST – normal reset
- RTCK – return clock
- GND – ground



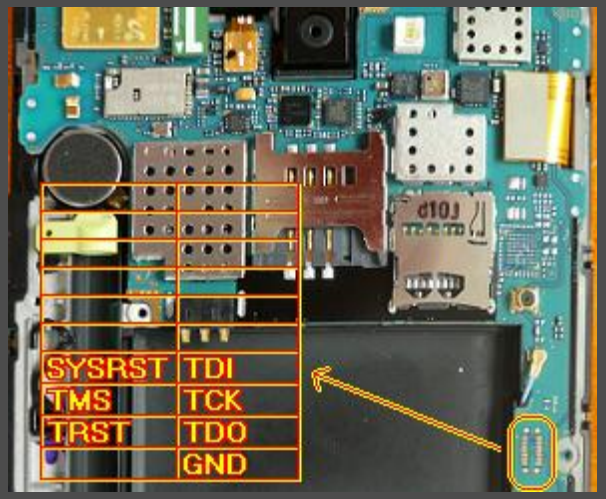
JTAG Pinout

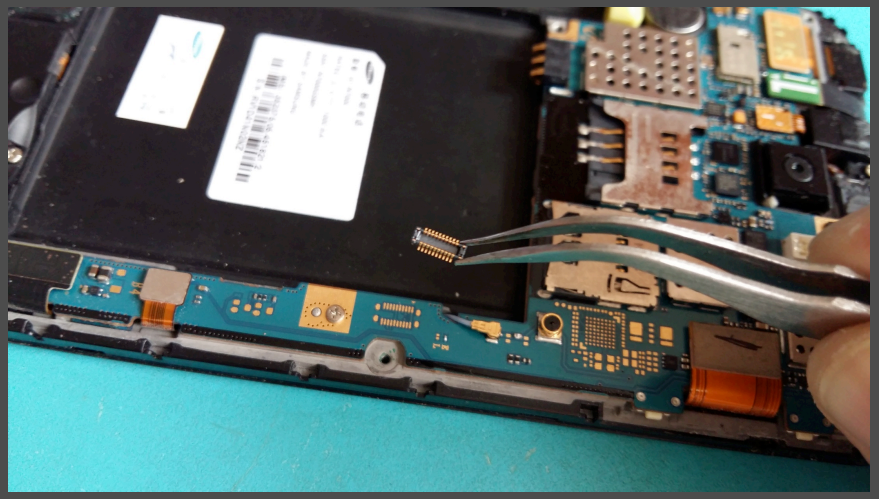

TRST
TDI
TMS
GND
SYSRST
TCK
TDO

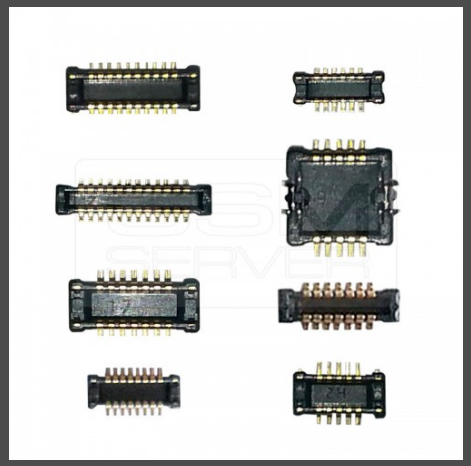

GND
SYSRST
TDO
TCK
TDI
TRST
TMS


TDI
SYSRST
TDO
TMS
TCK
GND

JTAG Molex and Jig

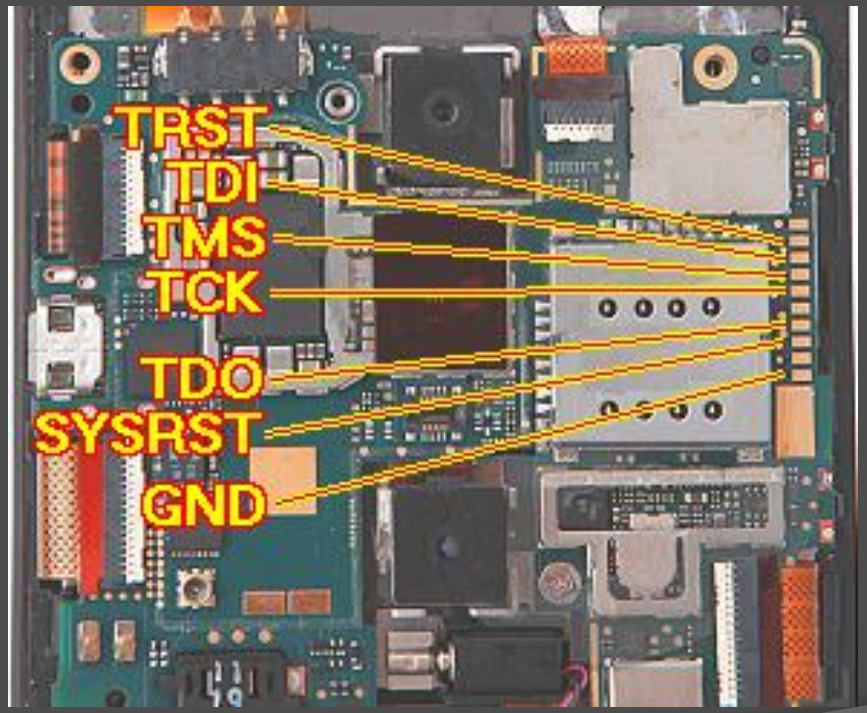






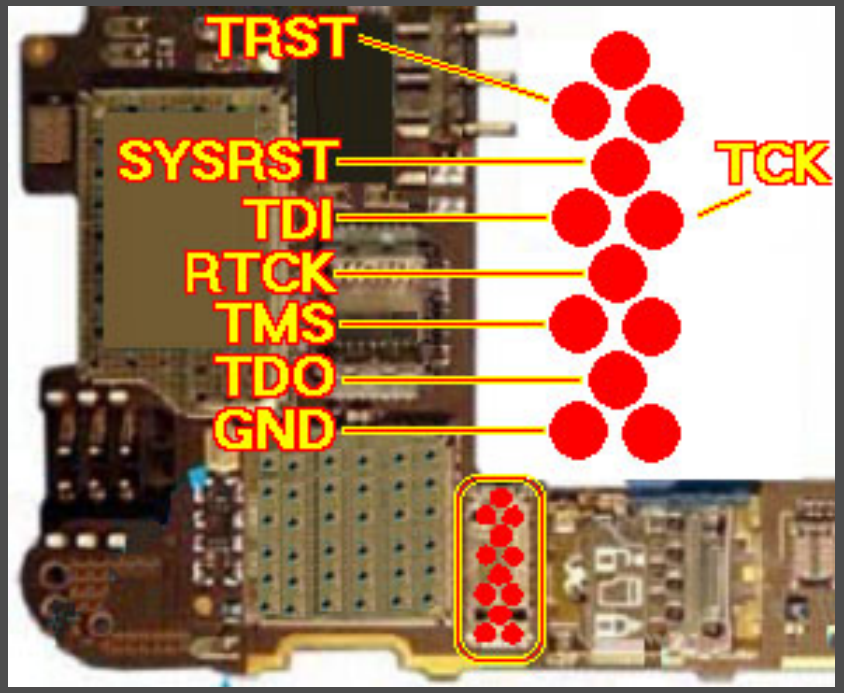
Demonstration using Riff Box

- HTC EVO 3G
- Android OS



Demonstation using Riff Box

- Lumia 620
- Windows 8 OS




JTAG Manager for RIFF Box Version: 1.56
Resurrection
JTAG Read/Write
DCC Read/Write
Useful Plugins
Box Service
Open serial port...OK
Connecting to the RIFF Box...OK
Firmware Version: 1.37, JTAG Manager Version: 1.56
Selected Resurrector: [Nokia Lumia 520 V1.0.5149.18900]
Connecting to the dead body...ERROR
Set I/O voltage reads as 1.79V, TCK Frequency is RTCK
ERROR: The RTCK Signal does not respond.
JTAG TCK Speed:
RTCK
Sample at MAX
Resurrector Settings
NOKIA
Nokia Lumia 520
Custom Target Settings
DCC Loader USB Interface
Target (Core):
SNAPDRAGON S4 ARM7TDMI
Reset Method:
RESET, Wait 0 ms, Special
JTAG I/O Voltage:
1.80V
TAP # (Multichain position):
0
Target Go
Target Continue
Write Memory
Read Memory
Halt the Target
Reset the Target
Read ICE Regs
Target Reset & Go
Execute Script
Analyze JTAG Chain
Connect & Get ID
Address: 0x0000 0000
Length: 0x0000 8FFF
Source File: C:\Documents and Settings\user\桌面\HTC EVO.bin
0%
Press CTRL+F for Fast Search
0 kB/s
RIFF Box
www.riffbox.org

Acquisition of the Flash Rom

```
Detected dead body ID: 0x104210E1 - CORRECT!
Set I/O Voltage reads as 1.79V, TCK Frequency is RTCK
Adaptive Clocking RTCK Sampling is: [Sample at MAX]
Settings Code: 0x00010000000000000000000020000000

Resurrection sequence started.
Establish communication with the phone...OK
Initializing internal hardware configuration...OK
Uploading resurrector data into memory...OK
Starting communication with resurrector...OK

Detected an Initialized FLASH1 Chip, ID: 0x0090/0x004A (HYNIX, 0x000090000000 Bytes = 2.25 GB)

Reading FLASH1 address space from 0x000000000000 to 0x00001FFFFFFF
```

JTAG TCK Speed:
RTCK
Sample at MAX
Resurrector Settings
HTC
HTC EVO3D (PG8630000)
Custom Target Settings

```
Resurrection sequence started.
Establish communication with the phone...OK
Initializing internal hardware configuration...OK
Uploading resurrector data into memory...OK
Starting communication with resurrector...OK

Detected an Initialized FLASH1 Chip, ID: 0x0090/0x014A (H8G2D, 0x0001CE800000 Bytes = 7.23 GB)
Detected an Initialized FLASH2 Chip, ID: 0x0090/0x014A (H8G2D, 0x000000200000 Bytes = 2.00 MB)

Looking for the RIFF BOX DCCLoader USB Interface Port...FAILED
The DCCLoader USB Interface is not found. Communication continues over the DCC Interface

Reading FLASH1 address space from 0x000000000000 to 0x0001CE7FFFFF
```

JTAG TCK Speed:
RTCK
Sample at 200 kHz
Resurrector Settin
NOKIA
Nokia Lumia 620
Custom Target Se

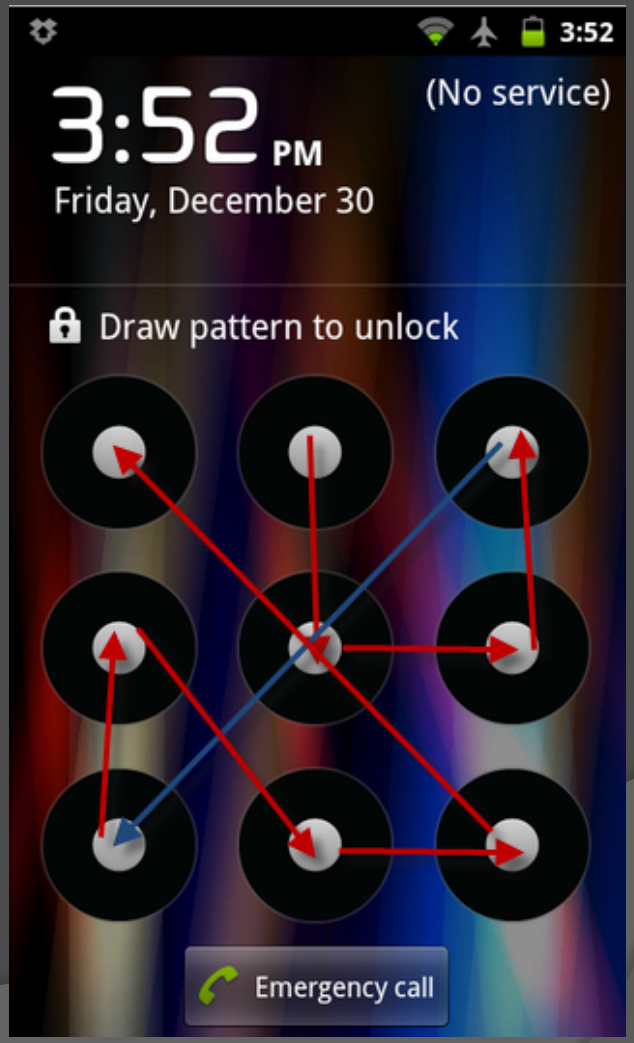
Retrieved Data from phone

Lumia 620 - Win8.bin

```
Offset
00737024  rl0   U %  0   +       0   U    ÿ      0$  U    0 ¤ 0 1 0   U
00737088   TSA2048-1-530   *▌H▌÷       ▌▌ JkùêXÂD 1▌y▌+▌¿▌¬ Ö LÍ°▌Xnß )£^È
00737152  Ê▌ ç R ïG'/ 8°äÉ▌N▌Ô"b ÷?7!Op1▌ñ▌8▌³èè▌ þÏU▌N$Ô©'Nz®·aAó*ÎçÉÙ^Ý»
00737216  +▌>µ▌µÙáWÿ¾´Å~õÏ ▌ã▌þ+Ó;R  8'÷?J0▌ ï0▌ ×          %0   *▌H▌÷
00737280    041 0   U    Nokia1"0   U    Nokia Software Signing CA0   1208
00737344  28112615Z  170823112350Z0Q1 0   U    Nokia1?0=  U   6Nokia Windo
00737408  ws Phone UEFI Application Signing Authority0▌ "0   *▌H▌÷       ▌
00737472     0▌    ▌    ▌ã«Û▌uq Èæ&(¨cßv¤'▌Á· Æ▌¤L▌P*¥▌  P=Ù0▌øù]¸▌?wô- °ý£e
00737536  ▌ç# zÈR  }▌ê1_▌▌]ëåñ▌r· ç´¹}&ÃÅÏ%  ▌øßÿü3ÚÀý.¾▌:Ú-@I Ó-³ Ãkã´ :%
00737600  ¨▌¼ÊìR¤½▌'té [)▌M ó  .×▌|&q-ó¯▌¼ï#_ï@m▌   0ÿ<ã0 :x ¯x4Q 3R¢714m¥
00737664  c ▌▌▌jÑ#  0ÚMt  G  ÏËBö▌+1b ± sh,j¹ íi%  q5> à^ý▌u®▌îdù▌oK»`u©ãþ
00737728  ▌½ÃRPËÔ«▌B(!     £▌ë0▌è0V  +        J0H0"  +     0 ▌ http://ocsp
00737792  0.nokia.com0"  +     0 ▌ http://ocsp1.nokia.com0   U    0 0   +
00737856     ^ 1  e0   U    ÿ     ▌0$  U %  ÿ  0   +    ^ 1      +       0
00737920     U #  0 ▌ ¾8¨ »~ã OEuÔç^ÉË m%Ç0   U      'Iªöåm'kEé^y▌ËËo ▌cz0
00737984     *▌H▌÷       ▌    ý▌®{2ÕÃÜ~ U▌&▌¸?¯Ñ¦ùõ & öbàOQDB▌É@d|ä `2VOÚB
00738048  MÎr;®kNÃÅyý I,WQX,  ▌9T²ÜýÖYclËb▌ ØÝ,´c»ÁCGý³▌._Ó¬î A\BVFn &/ôOg
```

Decoding the Lock Pattern

- gesture.key
- 20 bytes in length
- open source tools



Gesture.key

HTC EVO Full.bin **OVERWRITE MODE**

Hex | Text

Find: A8 A2 A0 7B 64 C8 97 9D BA 07 6B 28 EC 31 58 3A 61 83 52 FA

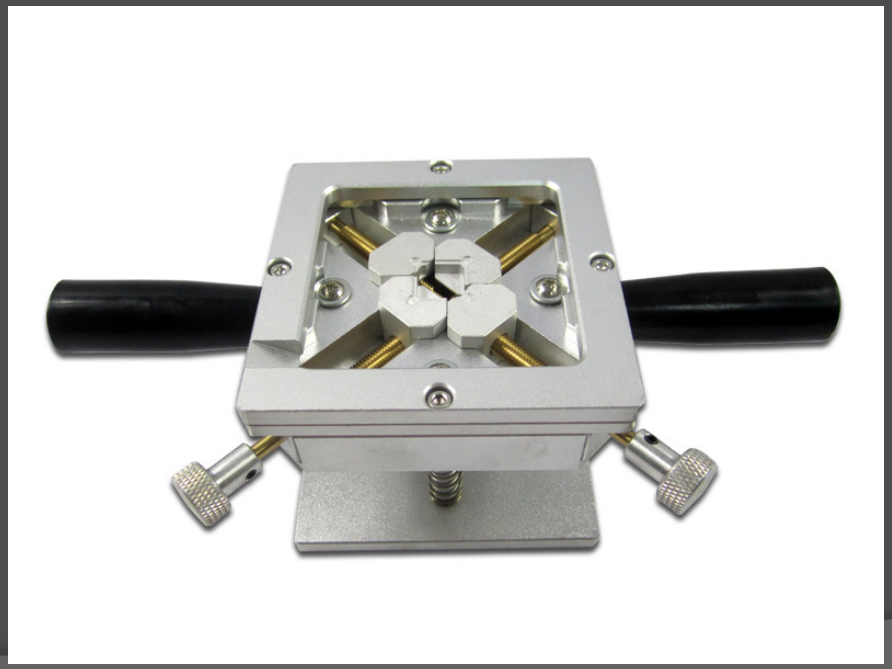
Replace:

Replace All | Replace | Replace & Find | Previous | Next

```
1819192584 616D696E 675F616C 6C6F7765 64061E03 41016C6F 63617469 6F6E5F70 726F7669 64657273 5F616C6C 6F776564  aming_allowed   A location_providers_allowed
1819192628 051B033B 01696E73 74616C6C 5F6E6F6E 5F6D6172 6B65745F 61707073 0414032D 01726F61 6D696E67 5F736F75  ; install_non_market_apps   - roaming_sou
1819192672 6E645F6F 6E031000 00001F1C 033D016C 6F636B73 63726565 6E2E7061 7373776F 72645F74 79706548 0000001D  nd_on        = lockscreen.password_typeH
1819192716 00000000 FFA2FB24 7B80EB49 6D3BE512 8110E5F5 0A000000 2000D900 00D900E9 01090118 01310144 015B0170  ˜¢˚${ÄÎIm;Å Å Å ı      Ÿ  Ÿ È     1 D [ p
1819192760 01810199 01B501CF 01E001F9 0210022F 024E0267 0284029B 02AF02C9 02DC02FB 031F033C 03530374 039603B2  Å ô µ æ ‡ ˘   / N g Ñ õ Ø … ‹ ˚   < S t ñ ≤
1819192804 03C703E6 006B03AF 03BF03D1 03E80000 00000000 001C033D 01646566 61756C74 5F696E73 74616C1C 033D016C  « Ê k Ø ø – Ë         = default_instal  = l
1819192848 6F636B73 63726565 6E2E7061 7373776F 72645F74 79706548 19033701 6C6F636B 5F706174 7465726E 5F617574  ockscreen.password_typeH  7 lock_pattern_aut
1819192892 6F6C6F63 6B471F03 4301616C 6C6F7765 645F6765 6F6C6F63 6174696F 6E5F6F72 6967696E 73412303 4B016874  olockG  C allowed_geolocation_originsA# K ht
1819192936 635F6572 726F725F 7265706F 72745F70 720F0323 01616462 5F656E61 626C6564 321F0343 01616C6C 6F776564  c_error_report_pr  # adb_enabled2  C allowed
1819192980 5F67656F 6C6F6361 74696F6E 5F6F7269 67696E73 410E0321 01616E64 726F6964 5F69642C 18033501 61737369  _geolocation_originsA  ! android_id,  5 assi
1819193024 73746564 5F677073 5F656E61 626C6564 0E120329 01626163 6B75705F 656E6162 6C65641D 16033101 6261636B  sted_gps_enabled   ) backup_enabled   1 back
1819193068 75705F70 726F7669 73696F6E 65643514 032D0162 61636B75 705F7472 616E7370 6F72741E 10032501 626C7565  up_provisioned5  - backup_transport   % blue
1819193112 746F6F74 685F6F6E 01170333 01626F74 685F6E65 74776F72 6B5F6F70 74696F6E 3A1B033B 0163646D 615F6365  tooth_on   3 both_network_option:  ; cdma_ce
1819193156 6C6C5F62 726F6164 63617374 5F736D73 15190337 01636675 5F717565 72795F77 68656E5F 63616D70 6F6E1C10  ll_broadcast_sms   7 cfu_query_when_campon
1819193200 03250164 6174615F 726F616D 696E6702 18033501 64617461 5F726F61 6D696E67 5F616C6C 6F776564 06160331  % data_roaming   5 data_roaming_allowed   1
1819193244 01646174 615F726F 616D696E 675F6775 6172641A 1E034101 64617461 5F726F61 6D696E67 5F677561 72645F61  data_roaming_guard   A data_roaming_guard_a
1819193288 6C6C6F77 6564071E 03410164 6174615F 726F616D 696E675F 67756172 645F626C 6F636B65 64081803 35016465  llowed   A data_roaming_guard_blocked   5 de
1819193332 6661756C 745F696E 7075745F A8A2A07B 64C8979D BA076B28 EC31583A 618352FA 00000000 00000000 00000000  fault_input_®¢†{d»óù∫ k(Ï1X:aÉR˙
1819193376 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
```

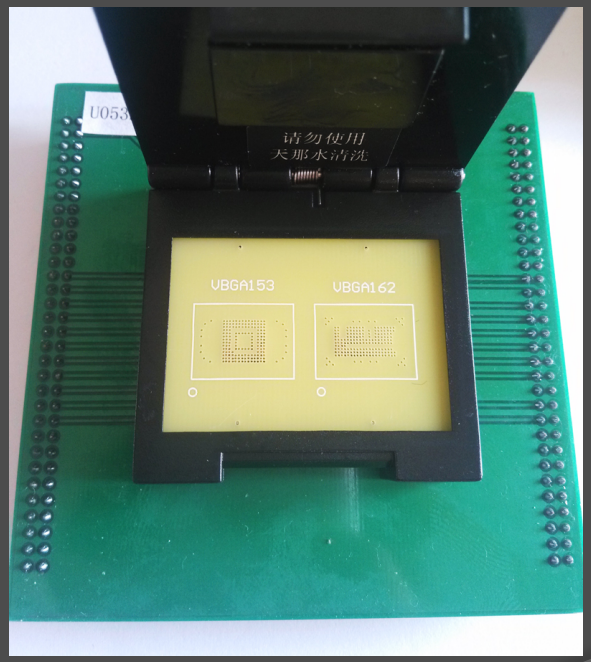
What is Chip-Off?

- eMMC chip
- NAND Flash
- Disassemble & Re-balling



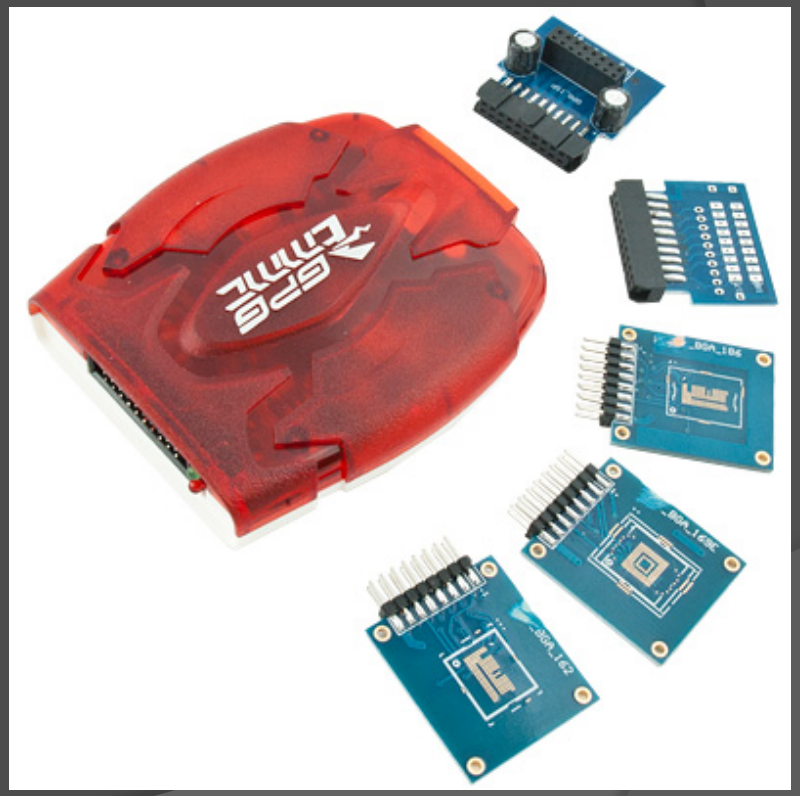
Heating Machine / Stand

eMMC Programmer & Adapters

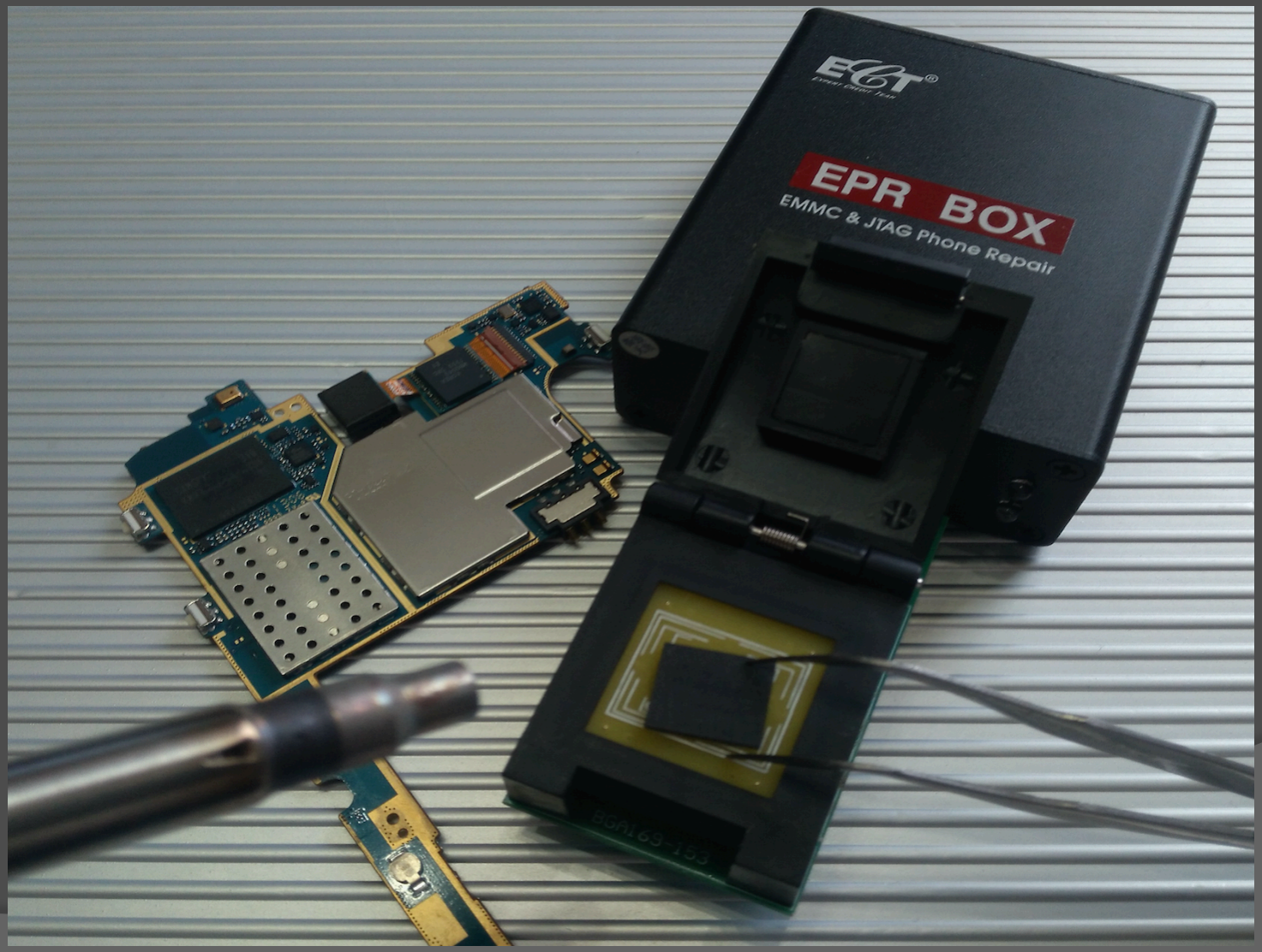


eMMC Box

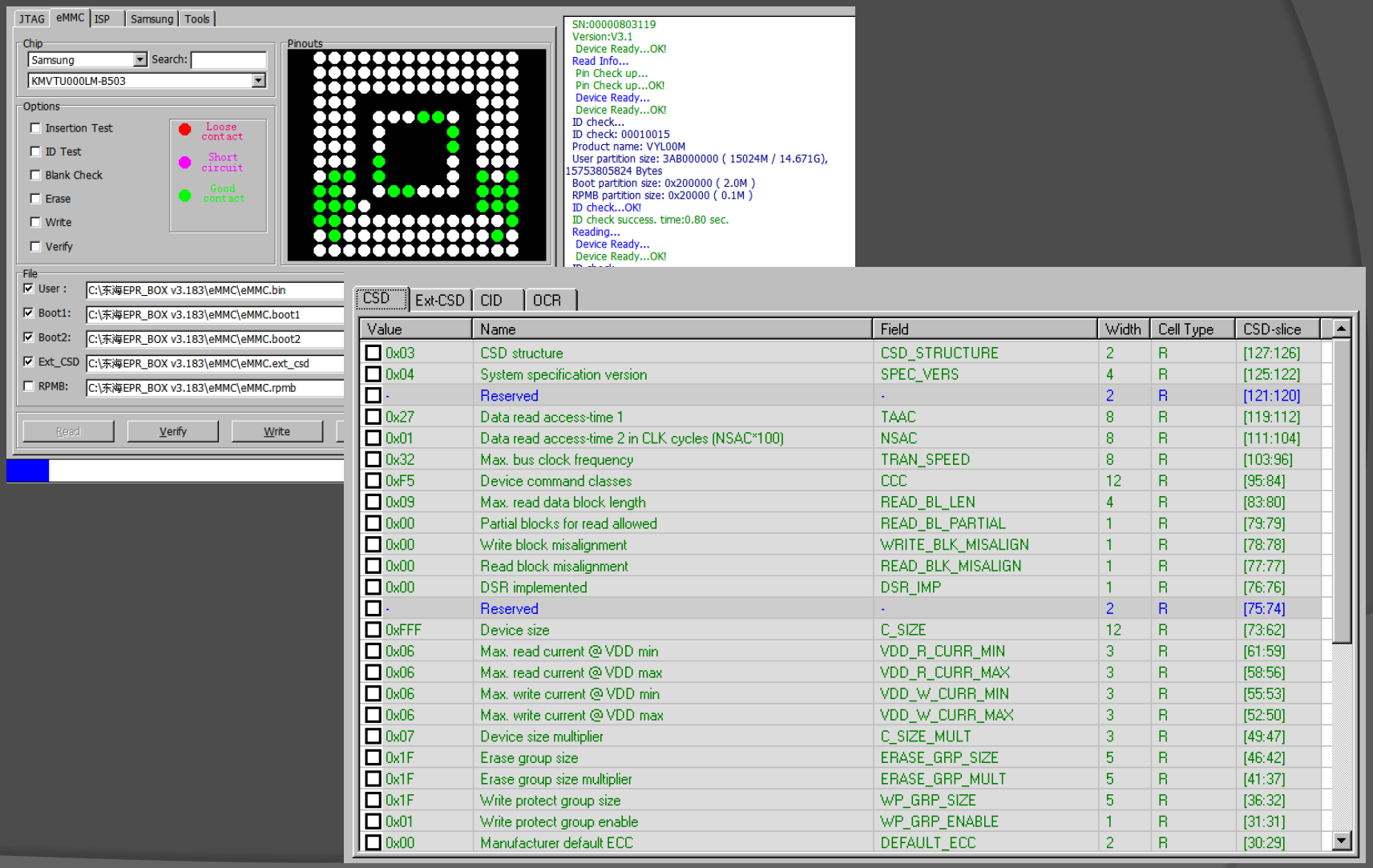

EPR BOX
EMMC & JTAG Phone Repair
大连东海通讯技术有限公司荣誉出品
www.eastsea.com.cn



EPR Box & BGA 169e adaptor

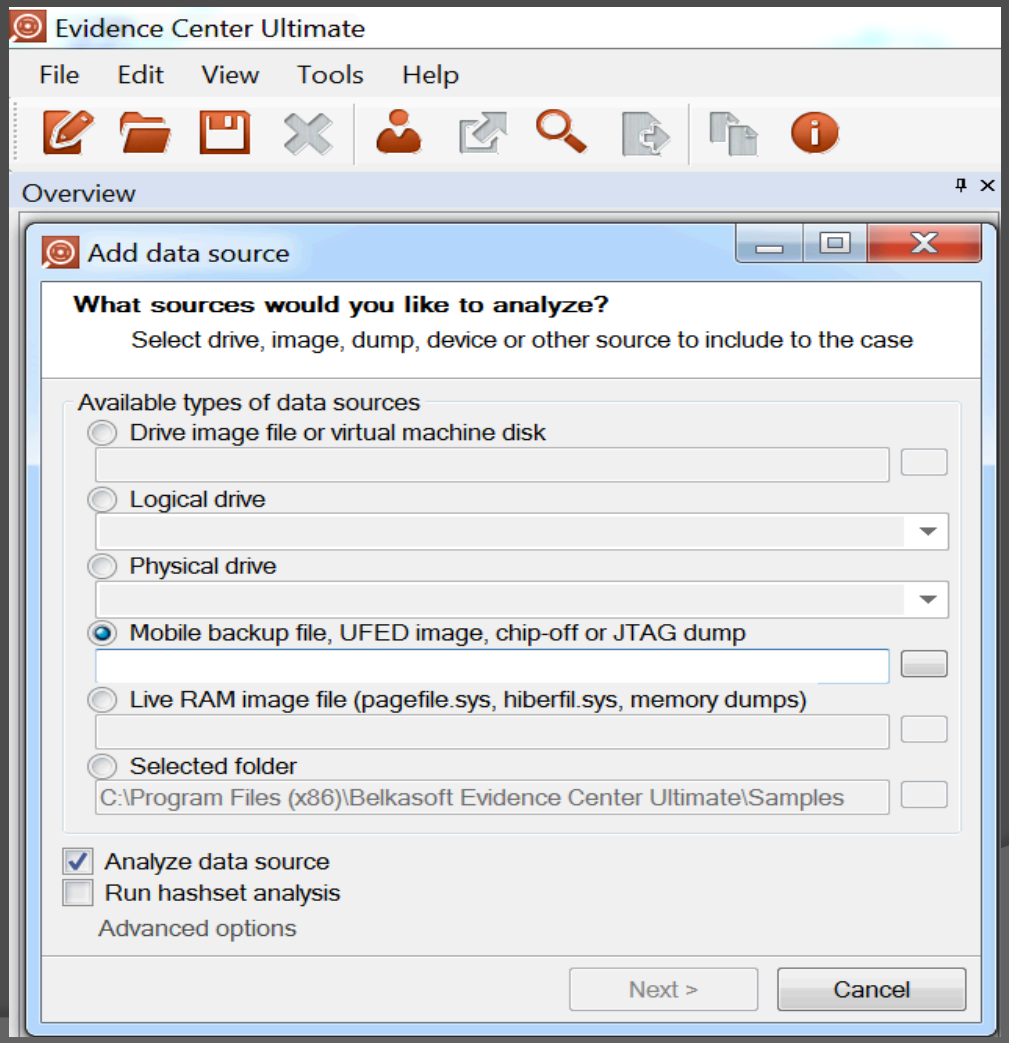


Demonstration

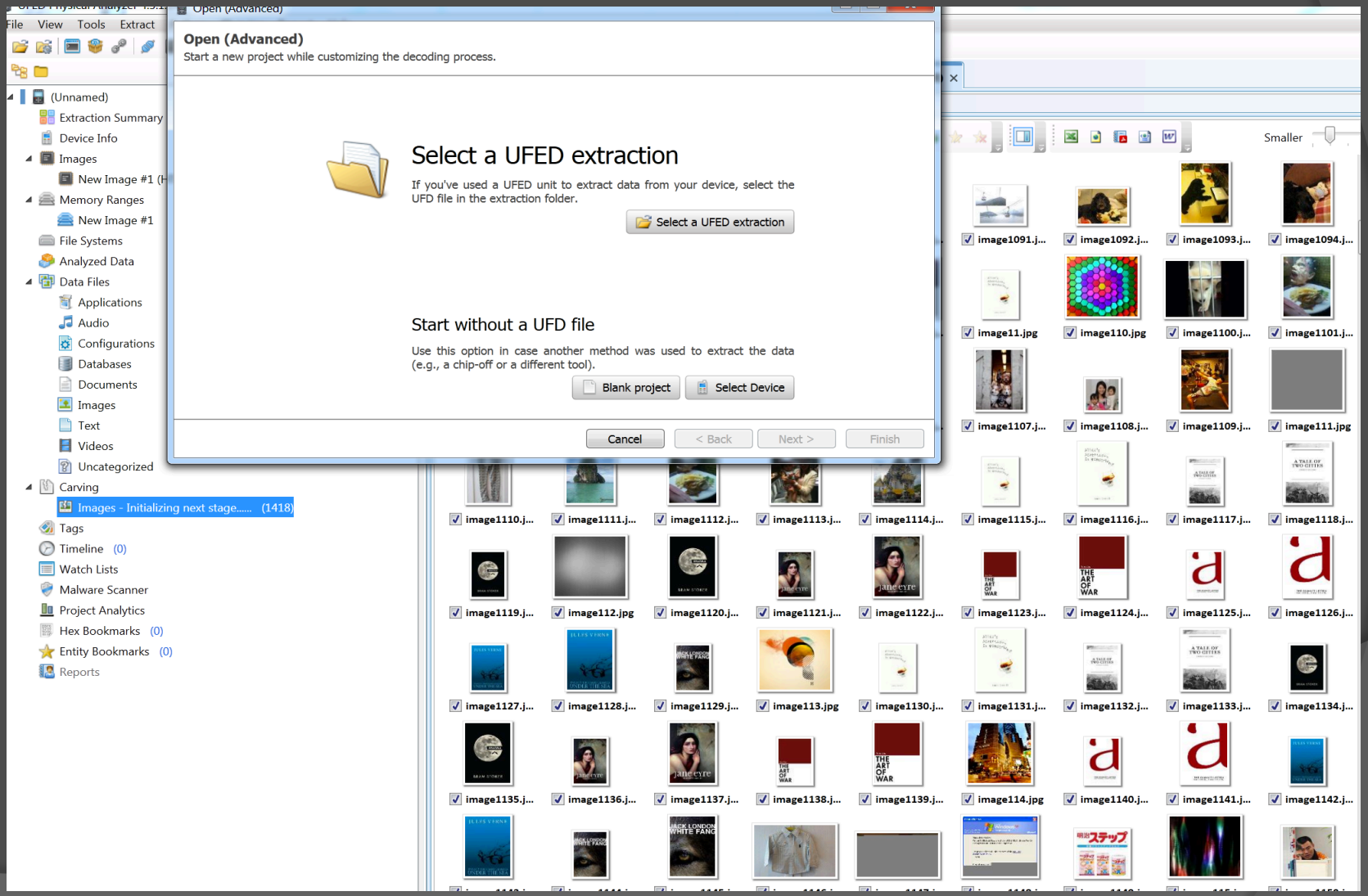


Value	Name	Field	Width	Cell Type	CSD-slice
0x03	CSD structure	CSD_STRUCTURE	2	R	[127:126]
0x04	System specification version	SPEC_VERS	4	R	[125:122]
-	Reserved	-	2	R	[121:120]
0x27	Data read access-time 1	TAAC	8	R	[119:112]
0x01	Data read access-time 2 in CLK cycles (NSAC*100)	NSAC	8	R	[111:104]
0x32	Max. bus clock frequency	TRAN_SPEED	8	R	[103:96]
0xF5	Device command classes	CCC	12	R	[95:84]
0x09	Max. read data block length	READ_BL_LEN	4	R	[83:80]
0x00	Partial blocks for read allowed	READ_BL_PARTIAL	1	R	[79:79]
0x00	Write block misalignment	WRITE_BLK_MISALIGN	1	R	[78:78]
0x00	Read block misalignment	READ_BLK_MISALIGN	1	R	[77:77]
0x00	DSR implemented	DSR_IMP	1	R	[76:76]
-	Reserved	-	2	R	[75:74]
0xFFF	Device size	C_SIZE	12	R	[73:62]
0x06	Max. read current @ VDD min	VDD_R_CURR_MIN	3	R	[61:59]
0x06	Max. read current @ VDD max	VDD_R_CURR_MAX	3	R	[58:56]
0x06	Max. write current @ VDD min	VDD_W_CURR_MIN	3	R	[55:53]
0x06	Max. write current @ VDD max	VDD_W_CURR_MAX	3	R	[52:50]
0x07	Device size multiplier	C_SIZE_MULT	3	R	[49:47]
0x1F	Erase group size	ERASE_GRP_SIZE	5	R	[46:42]
0x1F	Erase group size multiplier	ERASE_GRP_MULT	5	R	[41:37]
0x1F	Write protect group size	WP_GRP_SIZE	5	R	[36:32]
0x01	Write protect group enable	WP_GRP_ENABLE	1	R	[31:31]
0x00	Manufacturer default ECC	DEFAULT_ECC	2	R	[30:29]

Belkasoft Evidence Center



UFED Physical Analyzer



HITCON Training (Wish)

- November 2016
- One Day (6 hours)

Question?

forensicsninja@gmail.com