Mobile Forensic

Acquisition Technique

- Physical
- Logical

Case

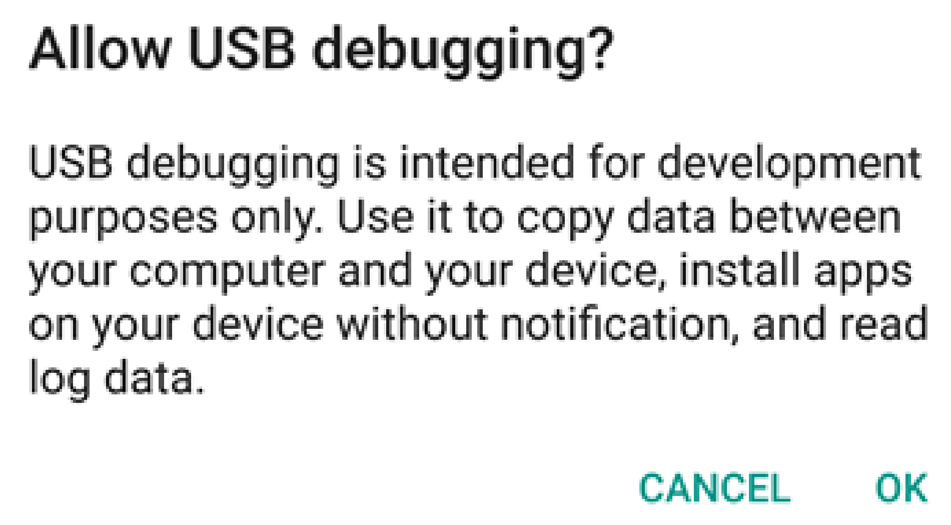
- Volatile
- Non Volatile

Physical Acquisition

Chipp Off

JTAG

ISP



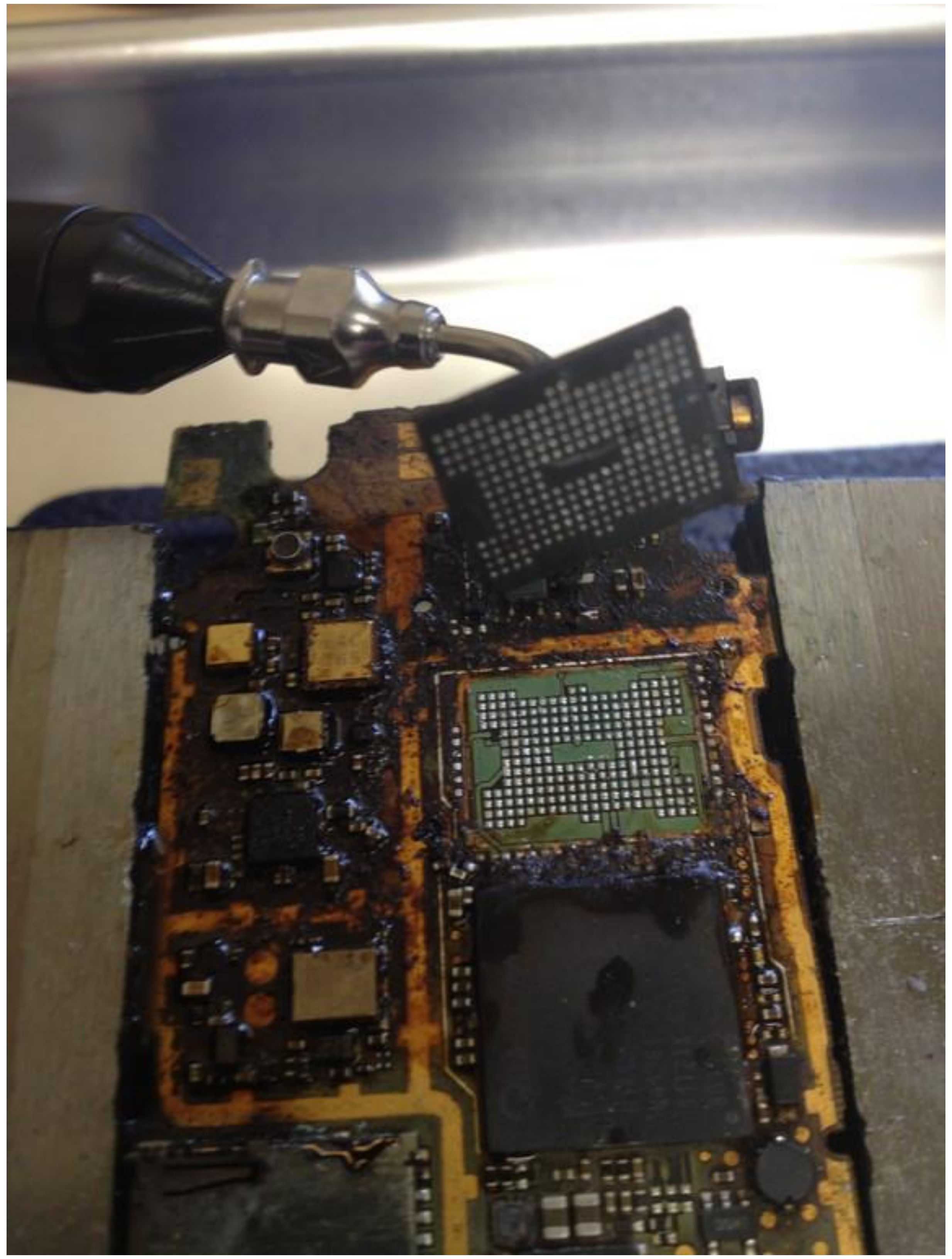
Allow USB debugging?

USB debugging is intended for development purposes only. Use it to copy data between your computer and your device, install apps on your device without notification, and read log data.

#root access
with dd

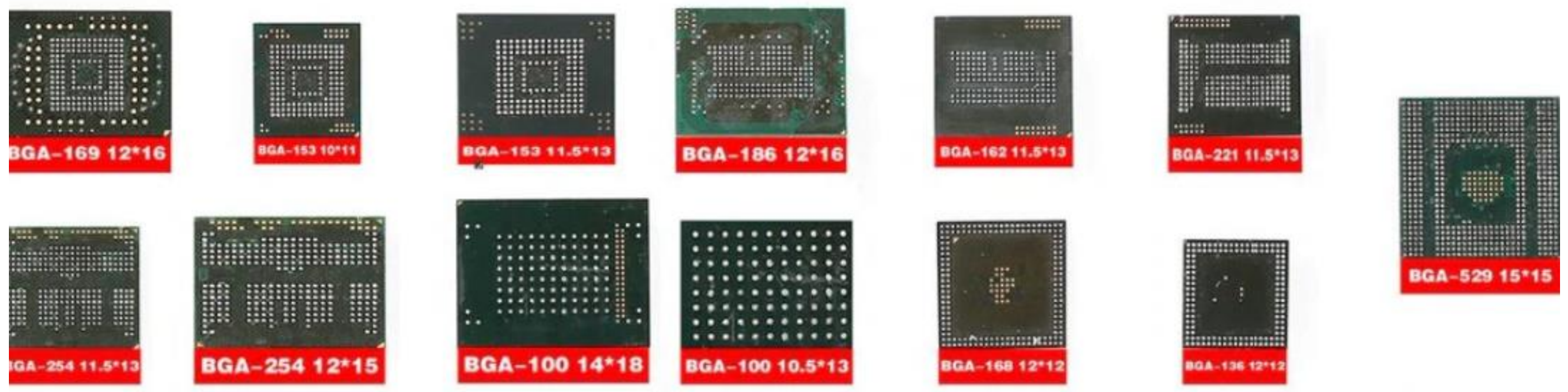
Chip-Off

- Identification **TAP (Test Access Ports)**
- Functions as a more easily



Acquisition Flow

EMMC Socket adapter/reader → EMMC Box → Physical extraction tool
--> RAW Image : .dd, .raw, etc



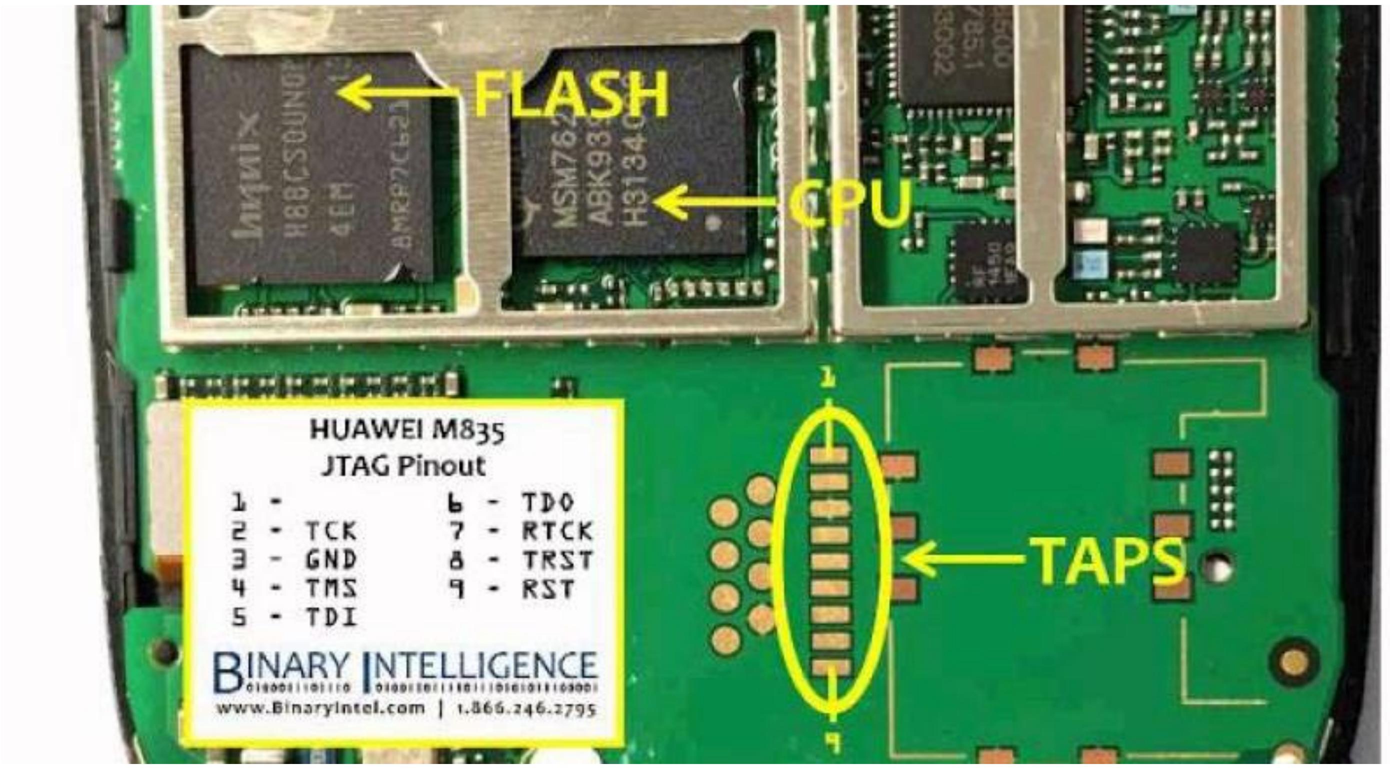
1. EMMC

2. emmc BGA socket

3. EMMC Box : RIFF, UFI Box, Z3X Easy JTAG

JTAG (Join Test Action Group)

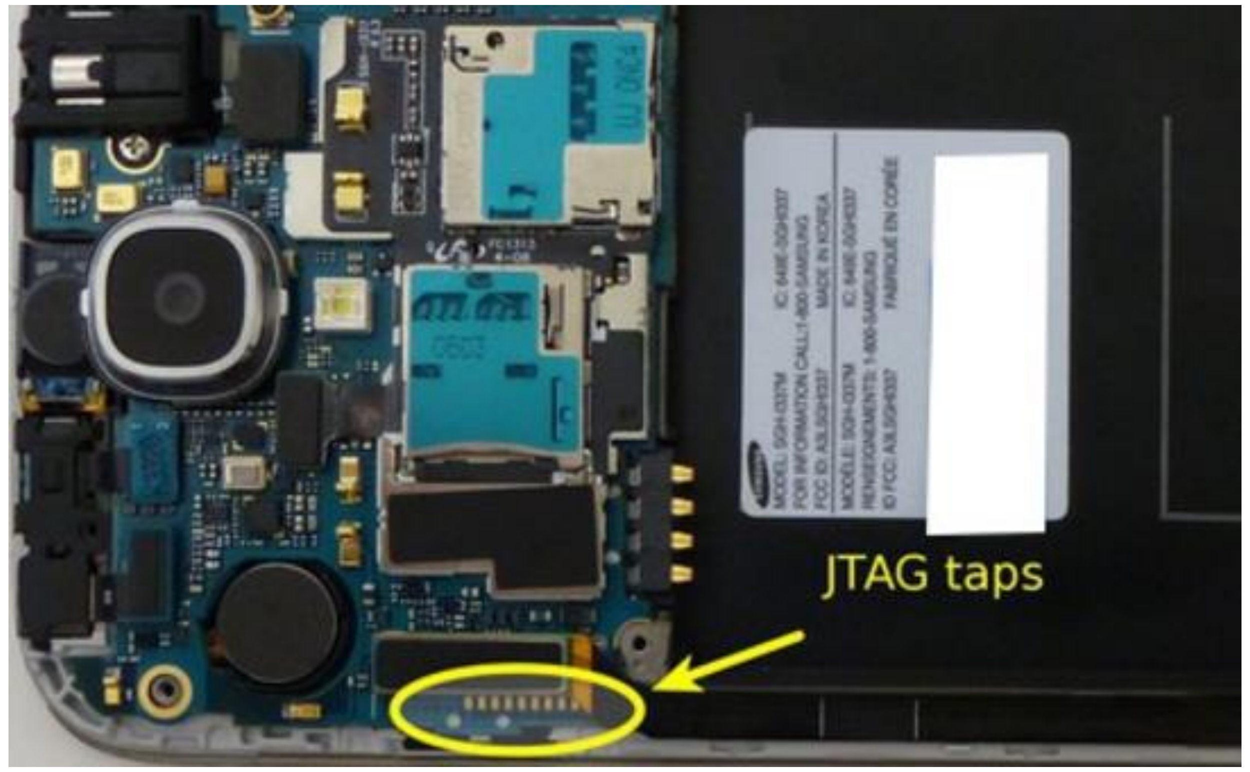
- Identification **TAP (Test Access Ports)**
- Functions as a more easily



HUAWEI M835
JTAG Pinout

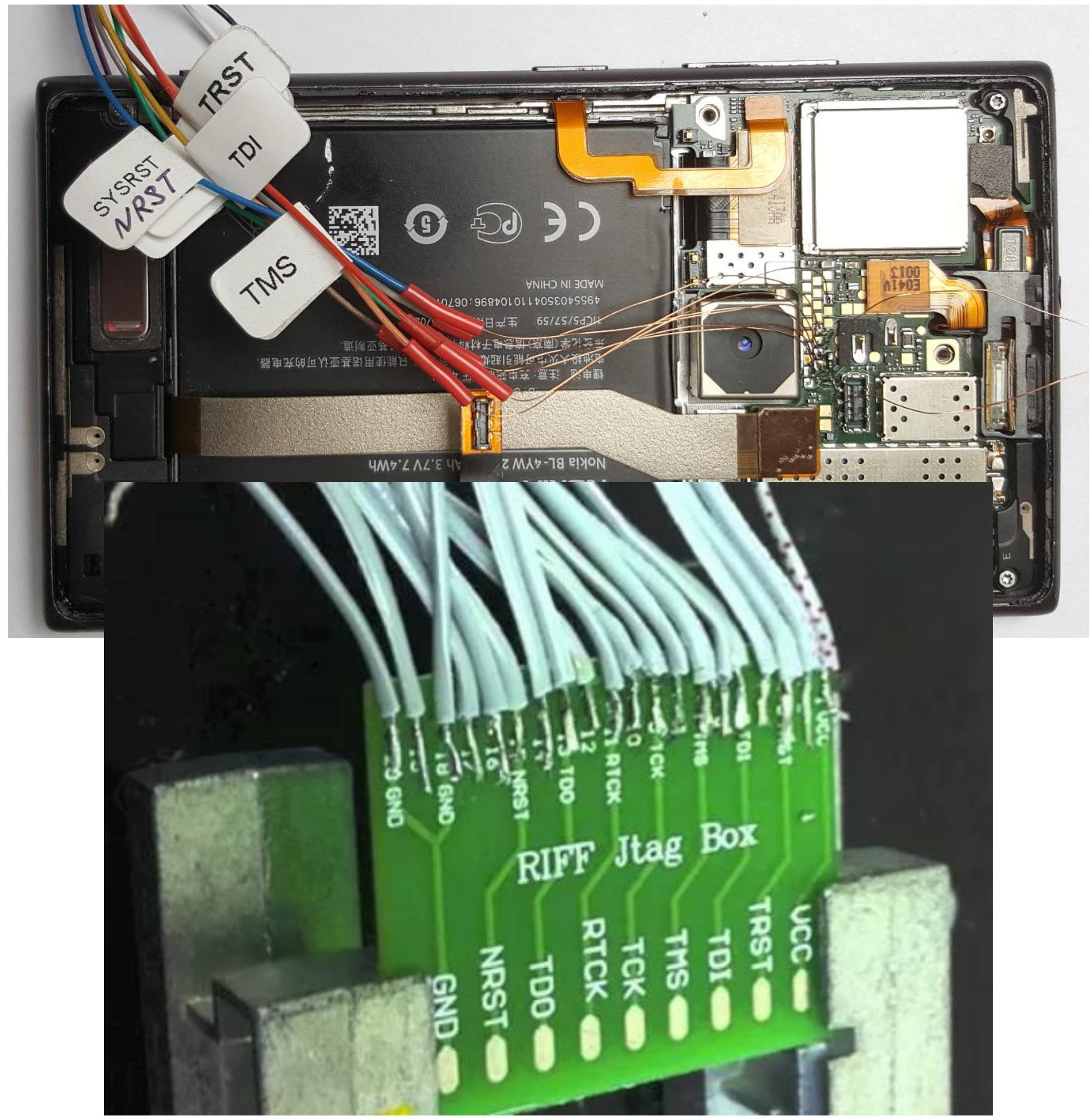
1 -	6 - TDO
2 - TCK	7 - RTCK
3 - GND	8 - TRST
4 - TMS	9 - RST
5 - TDI	

BINARY INTELLIGENCE
www.BinaryIntel.com | 1.866.246.2795

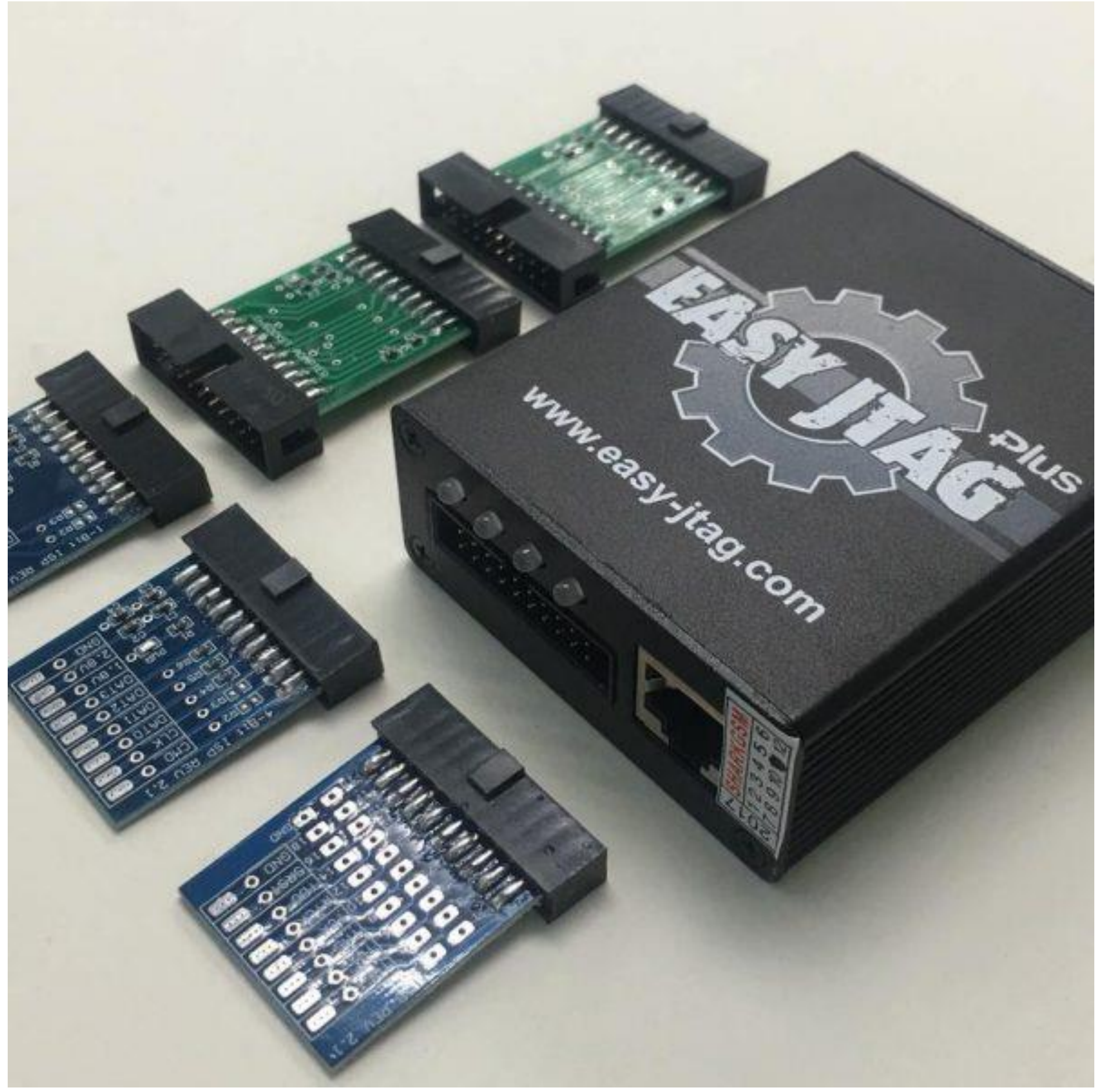


Acquisition Flow

JTAG TAP → PCB (via Solder, molex, jig) → JTAG Box
--> RAW Image : .dd, .raw, etc



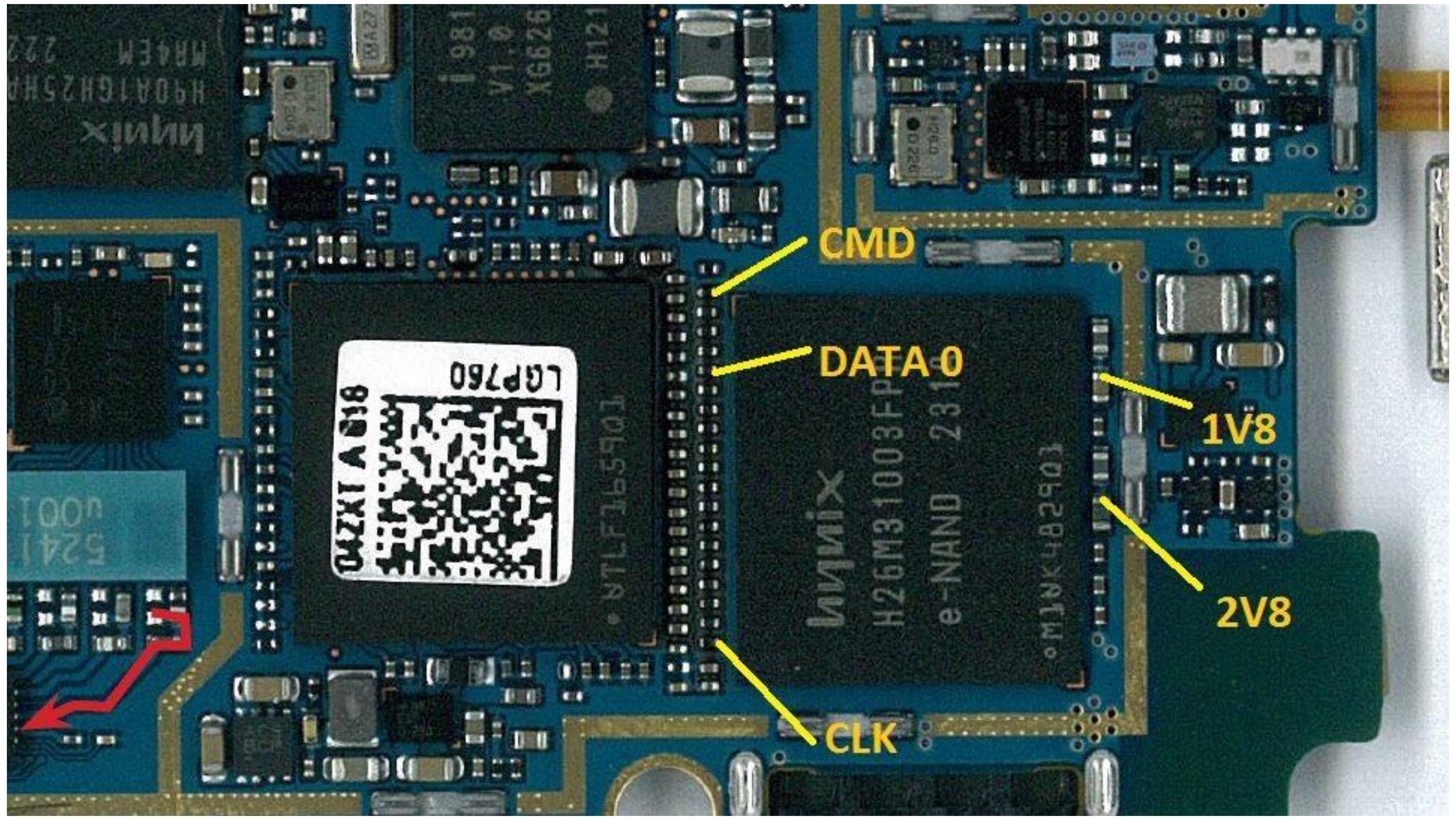
1. Connecting JTAG TAP to PCB / JTAG Adapter

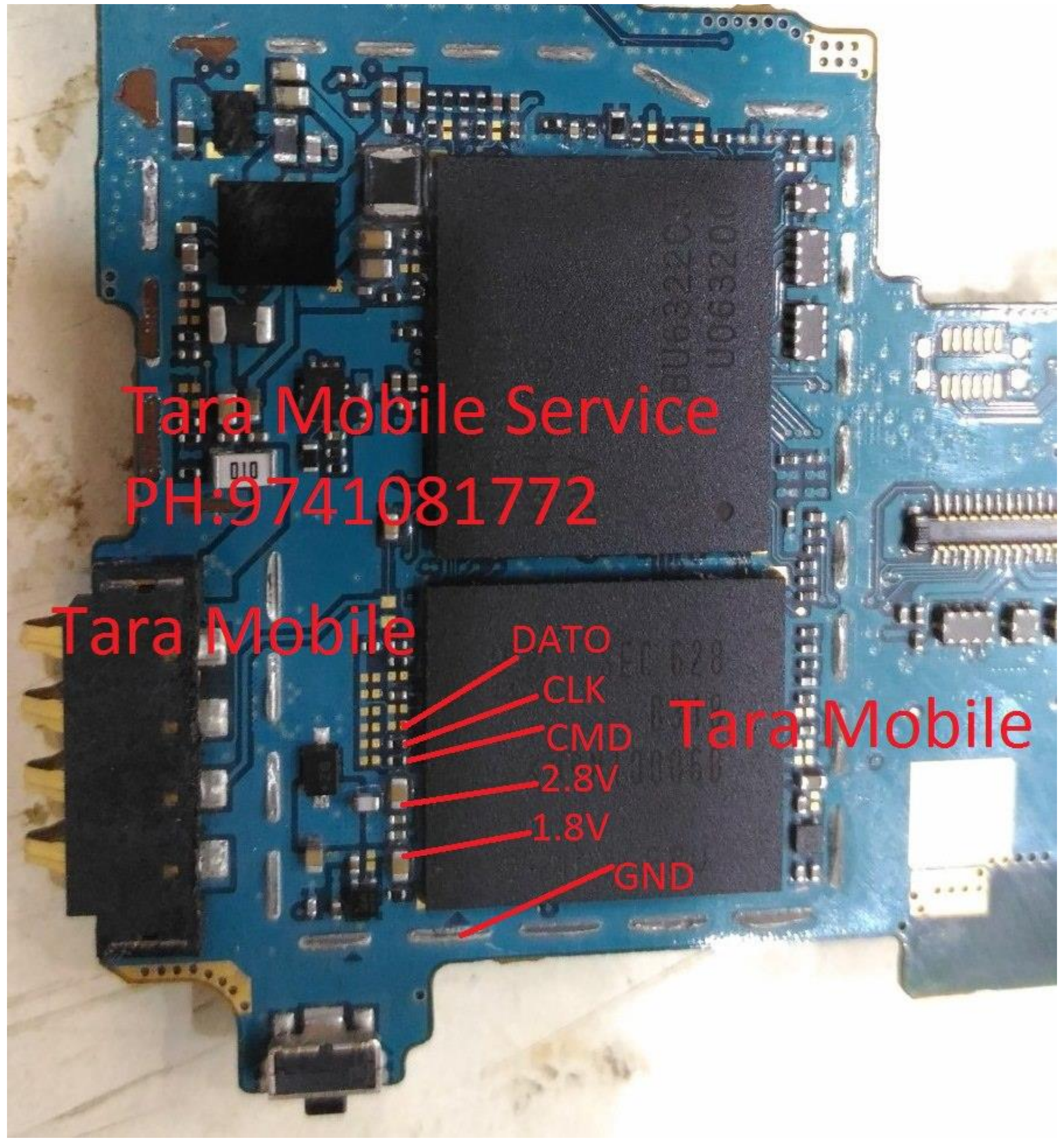


2. JTAG Box : RIFF, UFI Box, Z3X Easy JTAG

ISP (In-system programming)

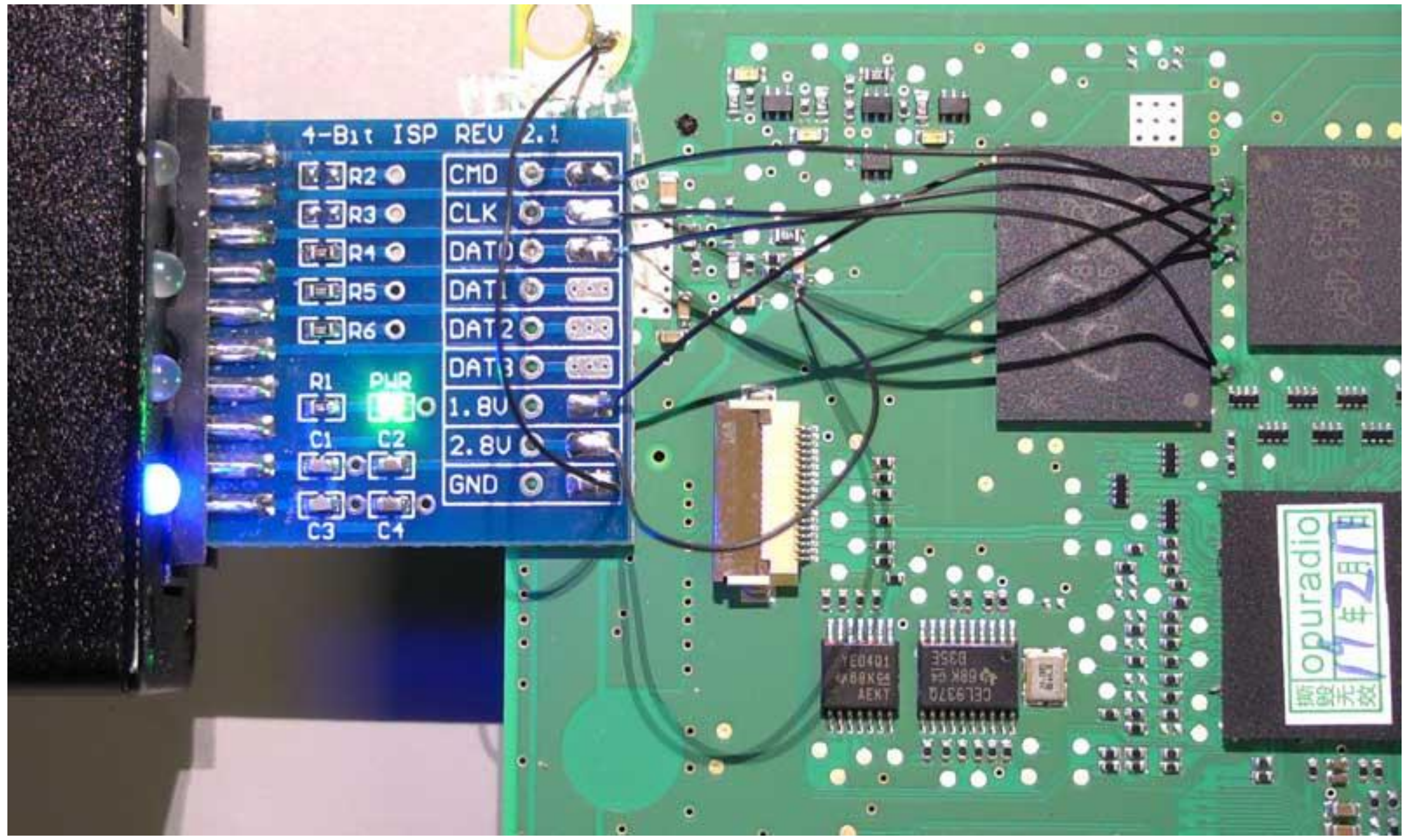
- ➤ Identification **ISP Pinout**
- ➤ Functions as a mo



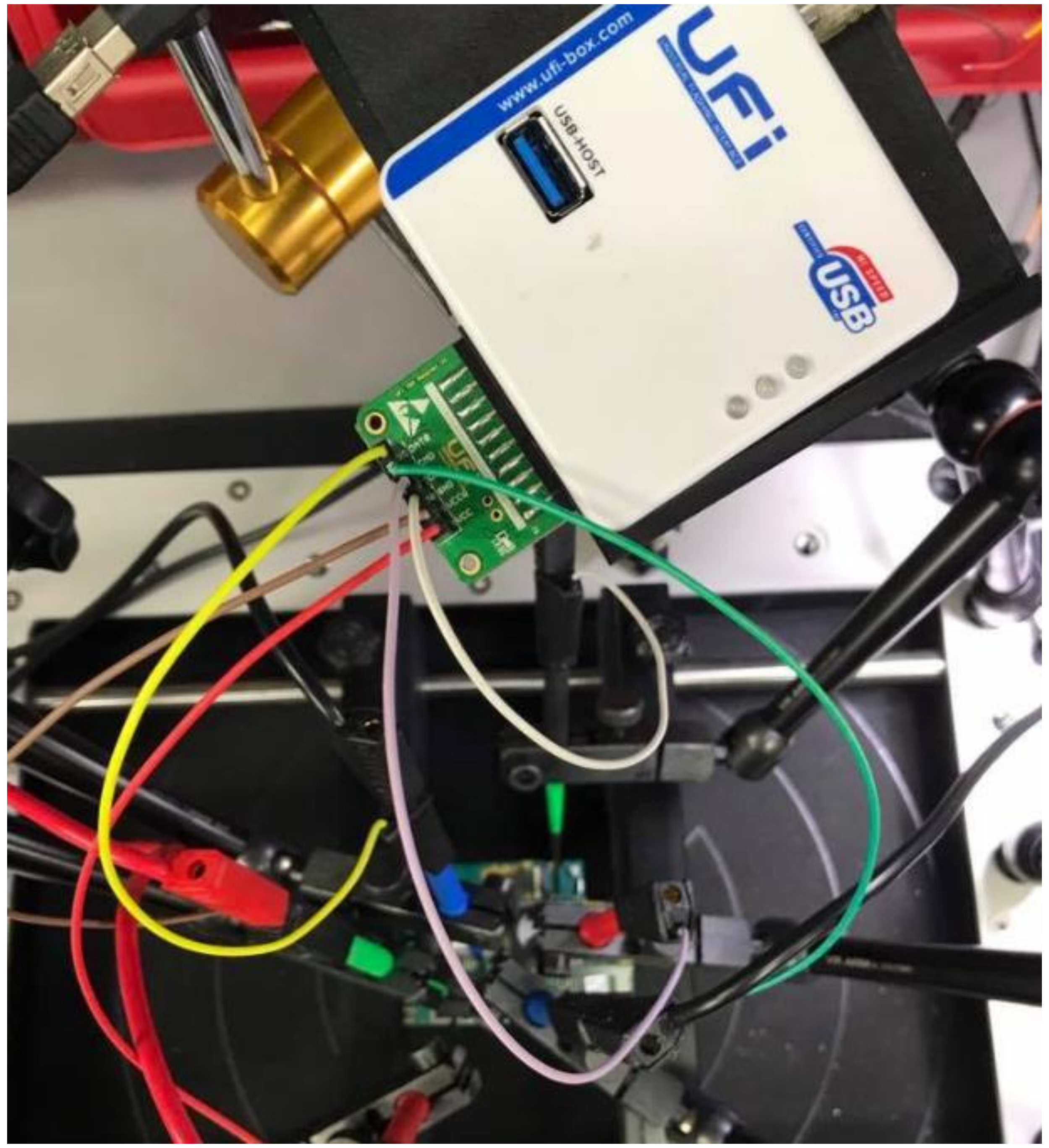


Acquisition Flow

Direct Pinout ISP/EMMC → Socket adapter/reader
--> RAW Image : .dd, .raw, etc



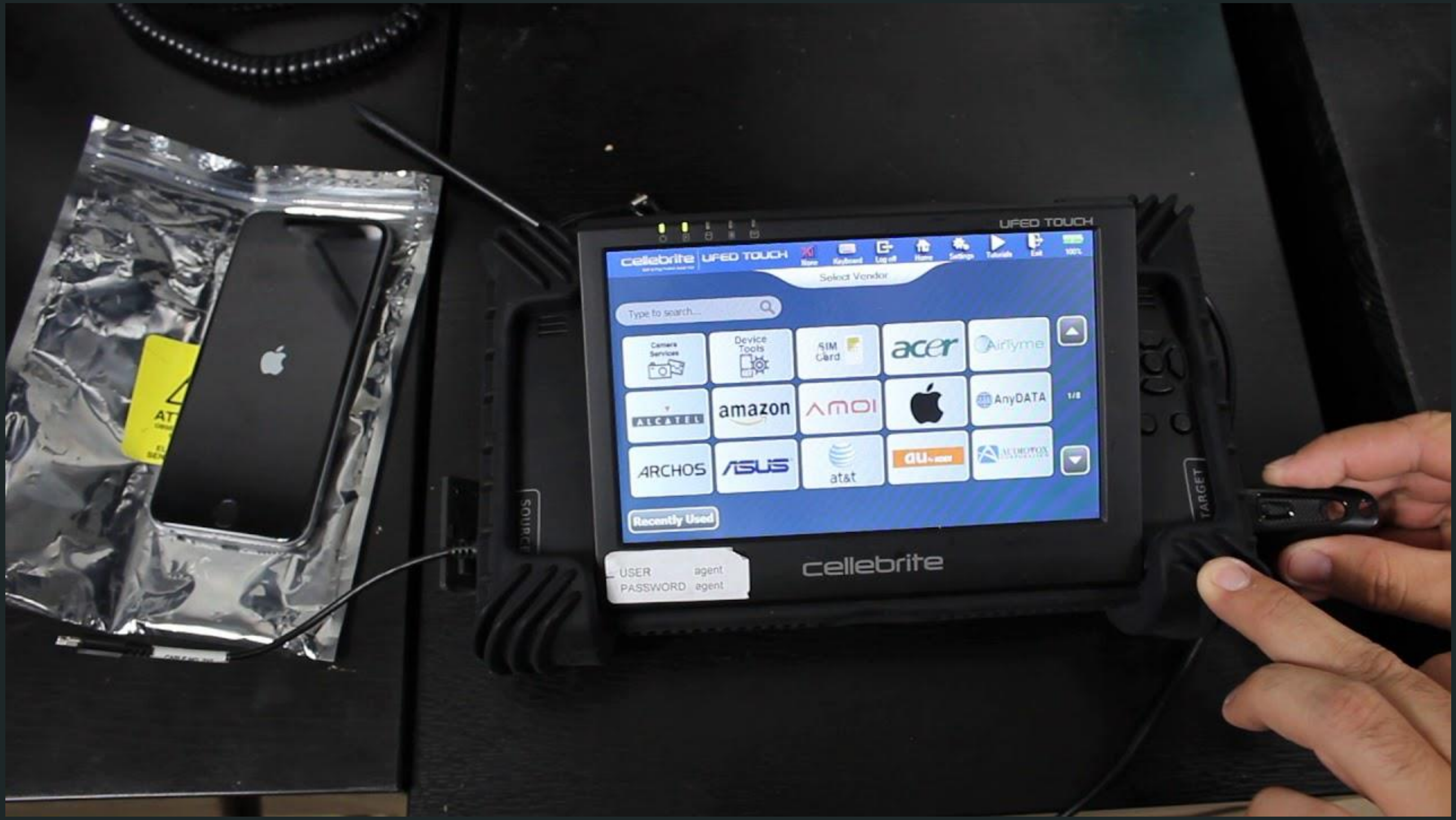
2. emmc BGA socket



3. EMMC Box : RIFF, UFI Box, Z3X Easy JTAG

Cellebrite UFED touch

http://www.onretrieval.com/images/PDF_s/Cellebrite_OnRetrieval_UFED_Touch_manual_usuario.pdf



Analysis RAW Image

AUTOPSY
DIGITAL FORENSICS

DFF

OXYGEN
FORENSICS

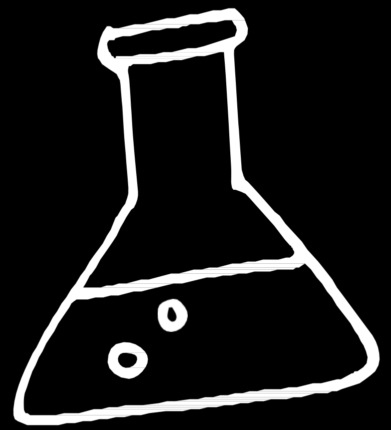
MOBILedit
FORENSIC
EXPRESS

Cellebrite

Challenge #1
‘Logical Analysis’

Android Artifacts

- ☑ /data/data
- ☑ /Android/data



.db

.store

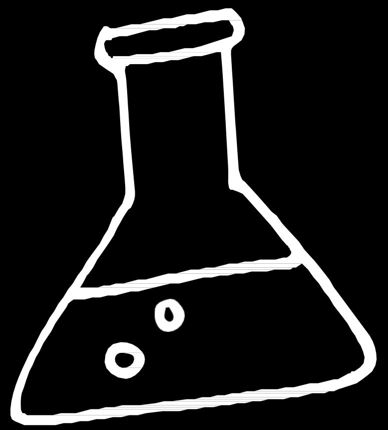
Challenge #2

‘Physical Image Analysis’

Android Artifacts

☑ /data/data

☑ /Android/data



.db

.store

#KNTL

Keep Never Tired
Learning