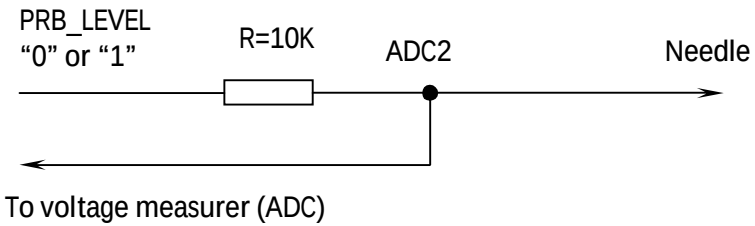
Probe(0) means voltage measured on ADC2 point while *PRB_LEVEL* signal is set to logic '0' level;

Probe(1) means voltage measured on ADC2 point while *PRB_LEVEL* signal is set to logic '1' level;




Finding JTAG pinout with such Probe method is much safer than using pin-finder solutions, since here no matter what pad is being tested it is connected to box through the 10K resistor, what means that peak 'harmful' current value applied to a pad is not more than 0.25 *mA* for 2.6V logic levels. *This method is fine when there is visually detected a definite island with pads which are most probably are JTAG pins but yet unknown.*

Bellow listed measured values of JTAG Pins. Voltage values are shown in the following form: *V1*/*V2*, where *V1* is voltage measured for *Probe*(0) and *V2* is voltage measured for *Probe*(1). In model name "+C" means USB Cable is connected, "+B" means battery is inserted.

For example, let's analyze the Huawei C2806M readings:

1) TRST signal has Probe(0) = 0.00V and Probe(1) = 2.27V; it is clear that 2.27V is lower than '1' = 2.6V which is due to voltage drop on probe's 10K resistor. This means TRST signal is input and has no pull-up resistor connected somewhere on the board.
2) TDI, TMS and TCK signals have same readings: Probe(0) = 0.31V and Probe(1) = 2.59V. We can see, that though Probe(0) was set '0', the real reading on probe's 10K resistor is 0.31V which is result of pull-up resistor connected

to TDI, TMS and TCK somewhere on the board. That's why Probe(1) reads as 2.59V and not drops slightly as with TRST case;

3) RTCK signal has Probe(0) = 0.08V and Probe(1) = 0.09V. This means no matter what level is set on Probe the resulting voltage on probe's 10K resistor not changes – that is we connected to some output signal which stays in '0' logic state;
4) TDO signal normally strays in Z state, that's why we read 0.00 for Probe(0) and 2.60 for Probe(1) – for Z state there is no current, so no voltage drops at all;
5) NRST signal has Probe(0) = 1.45V and Probe(1) = 2.62V; so high value of Probe(0) reading (while it is still considerably less than logic '1' voltage (2.60V) means there is quite strong pull-up is used to pull-up the NRST signal to logic '1'

P.S. We can see that NRST signal for Samsung B7330 or S5230 is not distinguishable between output mode and input: this is ok though, it means only that 10K resistor value used for probe is so big that such strong pull-up resistor value which is used for NRST pull-up on these devices not allows to detect whether the pin is really an input (with pull-up) or an output (in logic '1' state) pin.

So, generally this is the algorithm to be used to find JTAG pinout:

1. Use multitester to measure voltage levels on pads under question – thus find out the I/O levels current device is uses for JTAG (for example Qualcomm chips are usually 2.6V, OMAP – 1.8V, S5PCxxx – 2.8V, etc.);
2. Set voltage level in the JTAG I/O Voltage field (for this you need select Custom Target Settings);
3. Click Star Probing
4. Select PAD Type Sensor mode
5. Connect separate GND signal to board (for example if you connect device to PC with USB – do not rely on common GND which thus connects BOX-PC-Device; in order to get more accurate measurements solder dedicated GND from RJ-45 to the Device;
6. Touch with the Probe Needle the pads on device's board
7. Use your logic or shown advices to interpret readings correctly.
8. For example, there are found TRST, RTCK and TDO with big probability of truth. Usually TDI TMS and TCK are having same parameters, thus these have to be checked manually. For this:

8.1. Solder TRST, GND, RTCK and TDO to the JTAG connector and connect it to RIFF BOX.
8.2. Out of 3 pins (since it is yet unknown which one is TDI, which on is TCK and which is TMS) pick any and connect it to TCK on RIFF BOX.
8.3. Click Analize JTAG chain: in case TCK is found ok it will report None Found error, otherwise there will be RTCK does not respond error.
8.4. In such way in 3 attempts TCK is found.
8.5. Now remains only 2 attempts to find which pin out of remaining 2 is TDI and which is TMS.

| Model | MCU | TRST | TDI | TMS | TCK | RTCK | TDO | NRST |
|---|---|---|---|---|---|---|---|---|
| HTC HD2 + C + B | QSD8250 | 0.13/2.11 | 0.29/2.64 | 0.29/2.64 | 0.29/2.64 | 0.14/0.15 | 0.00/2.61 | 1.45/2.62 |
| HTC HD + C | MSM7201A | 0.00/2.25 | 0.31/2.59 | 0.31/2.59 | 0.31/2.59 | 0.00/0.00 | 0.00/2.60 | 1.35/2.62 |
| HTC HD + C + B | MSM7201A | 0.01/2.27 | 0.30/2.63 | 0.30/2.63 | 0.30/2.63 | 0.08/0.09 | 0.00/2.60 | 1.38/2.65 |
| Huawei C2806M + C | QSC6010 | 0.00/2.28 | 0.37/2.59 | 0.37/2.59 | 0.37/2.59 | 0.00/0.00 | 0.00/2.60 | 1.23/2.57 |
| Samsung B7330 + C + B | MSM7225 | 0.01/2.24 | 0.32/2.62 | 0.32/2.62 | 0.32/2.62 | 0.03/0.04 | 0.00/2.60 | 2.64/2.66 |
| Samsung U700 | MSM6280 | 0.00/2.26 | 0.32/2.60 | 0.32/2.60 | 0.32/2.60 | 0.00/0.00 | 0.00/2.60 | 1.23/2.60 |
| | | | | | | | | |
| Samsung I9000 | S5PC110 | 0.05/2.34 | 0.37/2.86 | 0.37/2.86 | 0.05/2.35 | – | 0.01/2.80 | 0.37/2.85 |
| | | | | | | | | |
| Samsung i900 PDA + C | PXA312 | 1.92/3.30 | 0.34/3.30 | 0.34/3.30 | 0.05/1.65 | – | 0.00/3.28 | 0.44/3.26 |
| | | | | | | | | |
| Samsung S5230 + C | BCM2133x | 0.00/1.89 | 1.37/2.96 | 1.37/2.96 | 0.00/1.88 | 0.00/0.00 | 0.27/2.97 | 2.93/2.95 |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |