

RIFF BOX JTAG firmware/hardware supports communication with single or multichained TAP controllers. All currently supported cores, according to IEEE 1149.1 Test Access Port standard, put 0b1 data into IR register upon CAPTURE state. Thus it makes possible automatic detection of IR register size of each TAP present on the JTAG chain. In this case IR 'pre-' and 'post-' stuffing bit sizes are not required to be specified by user and are determined automatically. All is needed is a TAP controller position number of the device user is trying to connect to.

Here are ARM cores currently supported by the RIFF BOX JTAG firmware:

- ARM926
- ARM920T
- ARM1136
- PXA312
- PXA270
- OMAP3x (has TAP Router module)

Supported chipsets based on those ARM cores with RIFF DCC Loader functionality (that is NAND memory operations through custom chip's NAND controller):

- Intel XScale PXA312;
- Intel XScale PXA270;
- Qualcomm MSM62xx (except MSM6250x group);
- Qualcomm MSM6250x ;
- Samsung S3C2440;
- Samsung S3C6410;
- Broadcomm BCM21xxx;
- OneNAND (not chipset, but still...).

In short, if you have a device in hands which has supported chipset inside and if this chipset's core belongs to the supported ARM cores list, then you can connect and read/write memory of your device over JTAG link.

Currently supported models by Necromancer software are listed in Table 1 ("*supported*" means there is available resurrector DLL for each specified model).

Please note: in case you have a not supported device in hands you can use this table for quick reference in order to search for a possible match. If you can't find an exact match (Target ID and FLASH memory type) you still can write own hardware initialization script for your device and then use one of the pre-compiled DCC Loaders (according to loader RAM base and NAND type it manages). For this, use *Custom Target Settings* feature and *DCC Loader Settings* button; assemble proper binary file with bootcore and other data needed for successful resurrection (or read data from exactly same alive model) and flash device manually.

Pre-compiled DCC Loaders, which are included into RIFF Box software package do not contain any hardware initialization routines, what means it is assumed that target hardware is already initialized (DRAM/SRAM/DDR/Whatever RAM is configured and functional, FLASH memory GPIO access pins (if any) are configured) prior a DCC Loader is being uploaded and executed.

For example, you have a dead device based on the Qualcomm MSM6280 chipset; device uses NAND memory, which is visible to MCU through the chipset's embedded NAND controller. Generally, upon reset, DDR memory is not visible to the core, and chipset's DDR controller has to be configured first in order to be able to access DDR RAM memory.

There is MSM6280_01000000.enc DCC Loader file available. "MSM6280" means it can access NAND memory through the MSM6280 Chipset's NAND Controller. Value 0x01000000 means this loader is compiled to be executed from 0x01000000 RAM base address.

In this case you shall do:

- manually create H/W initialization script which will write proper data into proper registers;
- make sure after H/W initialization the RAM areas in range 0x01000000 to 0x12000000 are accessible;
- use DCC Loader Settings button to setup paths to DCC Loader file, H/W initialization script, loader RAM base, initial TCK frequency, etc.;
- use the Read Memory, Write Memory and Erase Memory features in order to write proper data into the dead device's memory.

What to do if your device has no RAM exactly at 0x01000000 address but has somewhere at other addresses? There are such options:

- configure core's MMU module (which is available in ARM architectures starting from ARM9 and higher) in that way, that core can access virtual memory at 0x01000000 address (that is add coprocessor CP15 MMU configuration instructions to H/W Initialization script and upload TLB translation table into physical RAM);
- contact RIFF support to order new pre-compiled DCC Loader which will work at given physical RAM addresses.

Table 1 List of Available resurrector DLLs

Model Name	Platform	Target ID, hex	Multichain position, TAP#	I/O Voltage, V	FLASH Access	OneNAND Base Address
Samsung C5510	QSC6240, ARM926	0x4015F0E1	0x00	2.6V	Chipset	-
Samsung F500 Modem	MSM, ARM926	0x300600E1	0x00	2.6V	Chipset	-
Samsung G810 Modem	MSM, ARM926	0x100D00E1	0x00	2.6V	Chipset	-
Samsung G810 PDA	OMAP2430, ARM11	0x07B3602F	0x01	1.8V	OneNAND	0x00000000
Samsung i450 Modem	MSM, ARM926	0x100D00E1	0x00	2.6V	Chipset	-
Samsung i450 PDA	OMAP2430, ARM11	0x07B3602F	0x01	1.8V	OneNAND	0x00000000
Samsung i550 Modem	MSM, ARM926	0x100D00E1	0x00	2.6V	Chipset	-
Samsung i550 PDA	OMAP2430, ARM11	0x07B3602F	0x01	1.8V	OneNAND	0x00000000
Samsung i710	PXA270	0x79265013	0x00	3.0V	OneNAND	0x00000000
Samsung i740 PDA	PXA312	0x1E649013	0x00	3.3V	Chipset	-
Samsung i900 Modem	MSM, ARM926	0xA00C00E1	0x00	2.6V	Chipset	-
Samsung i900 PDA	PXA312	0x2E649013	0x00	3.3V	OneNAND	0x10000000
Samsung i8910 Modem	MSM, ARM926	0x101C00E1	0x00	2.6V	Chipset	-
Samsung i8910 PDA	OMAP3430, Cortex-A8	0x0B6D602F	0x01	1.8V	OneNAND	0x08000000
Samsung S3310	BCM2133x, ARM926	0x07926F0F	0x00	3.0V	Chipset	-
Samsung S5230	BCM2133x, ARM926	0x07926F0F	0x00	3.0V	Chipset	-
Samsung S5600	MSM, ARM926	0x200C00E1	0x00	2.6V	OneNAND	0x40000000
Samsung S7070	BCM2133x, ARM926	0x07926F0F	0x00	3.0V	Chipset	-
Samsung S7350	MSM, ARM926	0xA00C00E1	0x00	2.6V	OneNAND	0x40000000
Samsung S7350i	MSM, ARM926	0xA00C00E1	0x00	2.6V	OneNAND	0x40000000
Samsung S8000	S3C6410, ARM926	0x07B76F0F	0x01	2.6V	Chipset	-
Samsung S8300	MSM, ARM926	0xA00C00E1	0x00	2.6V	OneNAND	0x40000000
Samsung T919	MSM, ARM926	0x101C00E1	0x00	2.6V	OneNAND	0x40000000
Samsung U700	MSM, ARM926	0x100D00E1	0x00	2.6V	Chipset	-
Samsung U900V	MSM, ARM926	0x200C00E1	0x00	2.6V	OneNAND	0x40000000

RIFF BOX JTAG Preview

Huawei Modem E1550	MSM, ARM926	0x401200E1	0x00	2.6V	Chipset	-
Eten X800	S3C2440, ARM920T	0x0032409D	0x00	2.6V	Chipset	-
ZTE Modem MF100	MSM, ARM926	0x401200E1	0x00	3.3V	Chipset	-
ZTE Modem MF622	MSM, ARM926	0x200C00E1	0x00	2.6V	Chipset	-
ZTE Modem MF626	MSM, ARM926	0x201200E1	0x00	3.3V	Chipset	-

