

User Manual for

USBJTAG NT

November 2019

(0.89)

Preface

Disclaimer

The information in this document is subject to change without notice. The manufacture makes no representations or warranties with respect to contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. The manufacture reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

Use USBJTAG NT and USB BDM NT at your own risk. Nothing is implied outside this document.

The manufacture is not responsive for any damage using the USBJTAG NT USBBDM NT software and hardware.

There are more information on <http://www.usbjtag.com>. Newer videos are also added to youtube channel <http://www.youtube.com/usbbdm>.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) Author USB BDM

www.usbjtag.com

All rights reserved.

Terms

In this document, **target** or **target board** refers to any device that has MIPS, ST20, ST40 ARM9 (ARM11 in the future) core CPU. Eg. Broadcom, LSI, etc. USB JTAG and USB EJTAG are both used for USB JTAG device. EJTAG is the JTAG name for MIPS core. DCU is the JTAG name for ST20 core.

For USBBDM NT hardware, **target** or **target board** refers to any device that has Motorola CPU like MC6833x

Only power on the JTAG (or BDM) and the target **AFTER** the JTAG (or BDM) and the target are connected. Connecting the JTAG (or BDM) and the target with either of their power on could burn either the JTAG (or BDM) or the target.

Warranty

For normal usage the devices can last very long. But since this is testing device and you are making contact to another powered device, there is a risk that hardware might get burnt out. The devices offer **three months** free repair. After three months, a fee needs to repair the USB JTAG NT or USB BDM NT. Warranty voided if covered is removed.

TABLE OF CONTENTS

Disclaimer	2
Chapter 1 Basic concept.....	5
1.1 What is JTAG	5
1.2 What is BDM	5
1.3 What can be done with USBJTAG NT.....	5
1.4 What can be done with USBBDM NT	6
Chapter 2 Install USBJTAG NT (USBBDM NT).....	6
2.1 Setup software.....	6
2.2 Activation.....	6
2.3 Install hardware.....	7
Chapter 3. Using USBJTAG NT software.....	8
3.1 Software layout.	8
Check the version of software.....	11
Configure the software.....	11
3.2 GUI Usage	13
Range selection	13
Speed selection.....	13
Toolbar.....	13
3.3 Commands	14
Most used commands.....	14
3.4 JTAG Usage.....	20
Program flash.....	20
3.4 Bug report.	20
Chapter 4 Script.....	21
4.1 Basic script.....	21

Chapter 1 Basic concept

1.1 What is JTAG

Here is the quote from <<MIPS EJTAG Specification>>

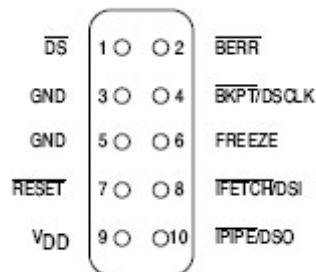
EJTAG is a hardware/software subsystem that provides comprehensive debugging and performance tuning capabilities to MIPS® microprocessors and to system-on-a-chip components having MIPS processor cores. It exploits the infrastructure provided by the IEEE 1149.1 JTAG Test Access Port (TAP) standard to provide an external interface, and extends the MIPS instruction set and privileged resource architectures to provide a standard software architecture for integrated system debugging.

USB JTAG NT supports MIPS 32, MIPS 64, ST20 and ST40 core from STMicroelectronics. Arm 9. USB JTAG NT can also be used as SPI programming programmer. For more information, please visit <http://www.usbjtag.com>.

USB JTAG NT software runs on mainstream OS like Microsoft Windows, Linux and MacOS.

1.2 What is BDM

BDM stands for Background Debugging Mode. Here is the pin layout of 10 pin BDM.



For detailed BDM information, please refer to chapter 5 of MC68331Ref.pdf. Recently users are using USB BDM NT for programming MC6833X based Engine Control Unit (ECU) or Transmission Control Unit (TCU)

USB JTAG NT software support both USB JTAG NT and USB BDM NT hardware.

1.3 What can be done with USBJTAG NT

USB JTAG provides an affordable yet powerful enough tool to have most functions that a professional JTAG tool can provide. It allows you to

1. Read memory from target board. This is to capture the state of the CPU.
2. Modify memory to target board.
3. Program flash using target CPU and memory. (Gain fast speed)
4. Do simple debugging. Break and single step the target in its execution. (MIPS32 only for now)

1.4 What can be done with USBBDM NT

USB BDM provides an affordable yet powerful enough tool to have most functions that a professional BDM tool can provide. It allow you to

1. View the registers of the target CPU.
2. Single step the target CPU.
3. Read memory from target board.
4. Write memory to target board.
5. Program flash using target CPU and memory.

Chapter 2 Install USBJTAG NT (USBBDM NT)

2.1 Setup software

First time installation (Windows):

Download proper USB driver from

<http://www.usbjtag.com/filedownload/index.php>, extract it.

Download the setup.rar file from <http://www.usbjtag.com/filedownload/usbjtag-nt-setup.php>, extract the setup.exe file and run it.

Plug in the USB, when it ask for driver, select the folder of the driver you have extracted. Select the appropriate OS version. (Windows 7/8/10).

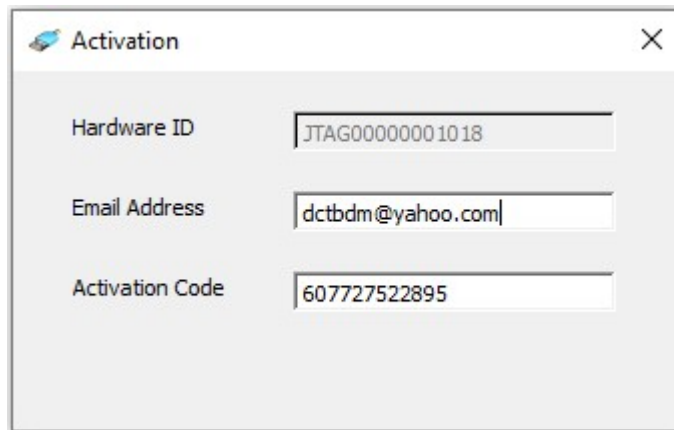
Update:

If you have installed older version of software, you need to uninstall the older software and reinstall the new one. Your previous configuration or activation info will not get lost during uninstallation.

USB JTAG NT configuration data are stored at %appdata%\usbjtag\. In case you need to manually add to any of xml, here you can find the files.

2.2 Activation

Your activation code is a unique number working with your **email address** (case sensitive and your **hardware ID**).



Hardware ID	JTAG00000001018
Email Address	dctbdm@yahoo.com
Activation Code	607727522895

1. When you do not have the code, enter email address and click “**Email Activation**” and it will popup your email software and send out the email request.

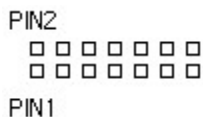
- If you do not have integrated email app, send email to activation@usbjtag.com with **hardware ID and email address** to get the code.
2. If you get the code then enter the code manually (*Email is case sensitive*). Click **OK when done**.
 3. If you have activated before and you lost your activation code, you can enter email address and click “**Online Activation**”. It will try to get the code from the online database.
 4. The software does not limit the number of computer you run on. You can install as many computers as you like.

When manually send email to activation@usbjtag.com to request activation, please specify the hardware ID in the email.

2.3 Install hardware

USBJTAG NT

The EJTAG connector on the board matches the standard Broadcom 14 pin EJTAG connector.



Here are the definitions of EJTAG.

Pin1 – TRST

Pin3 – TDI

Pin5 - TDO

Pin7 – TMS

Pin9 – TCK

Pin11 – RESET

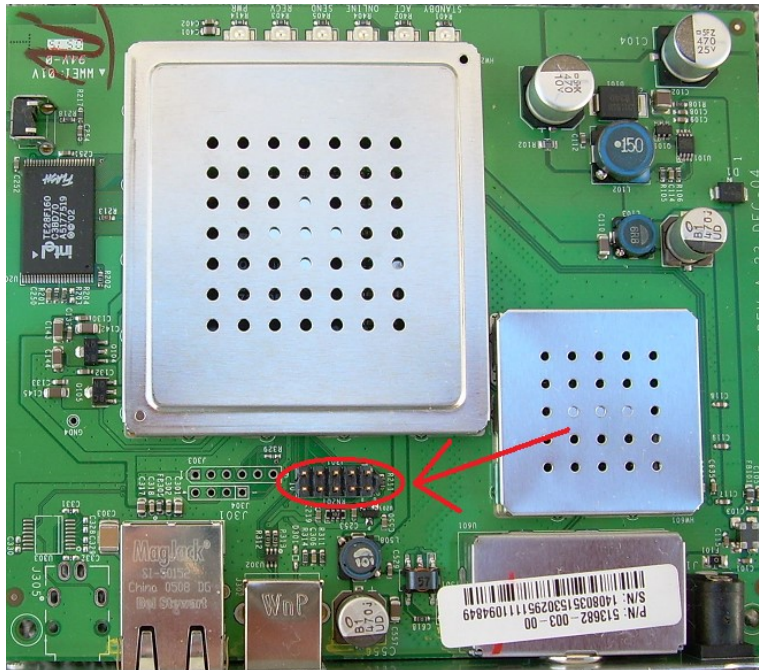
Pin13 – DEBUG (Not used)

Pin 2, 4,6,8,10 Ground. Pin 14 NC.

On back of the USB JTAG NT module, printed labels are used to indicate pin 1. The preconnected ribbon cable has a red pin indicate pin 1, too.

If your target does not have the same pinout, you need to make a connector to match your target.

Some board might not have JTAG connector and you need to solder a connector for it. Here is an example for sb5101 cable modem with a JTAG connector soldered on.



1. Power off the target board.
2. Plug the JTAG connector to the JTAG connector on target board
Improper connecting to the target will not work and might kill your target or USB JTAG NT.
3. Connect the USB JTAG NT into one of the PC's USB slot.
4. Power on the target board.

USBBDM NT

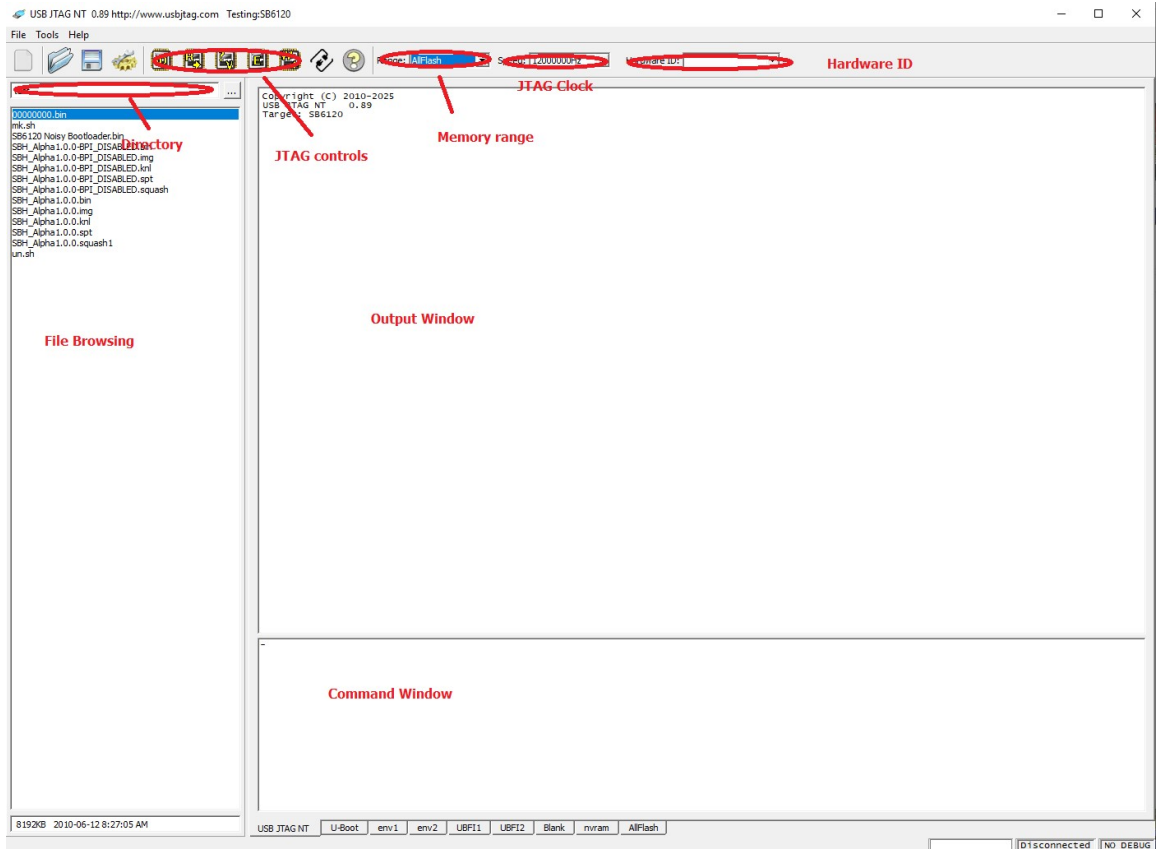
1. Power off the target board.
2. Plug the BDM connector to the BDM connector on target board. Make sure pin 1 matches the pin 1 on the target BDM connector. Reversing the BDM will cause the BDM to not function properly. If this happened, power off the target and plug back in.
3. Connect the USB BDM NT to one of the PC's USB port.
4. Power on the target board.

Chapter 3. Using USBJTAG NT software

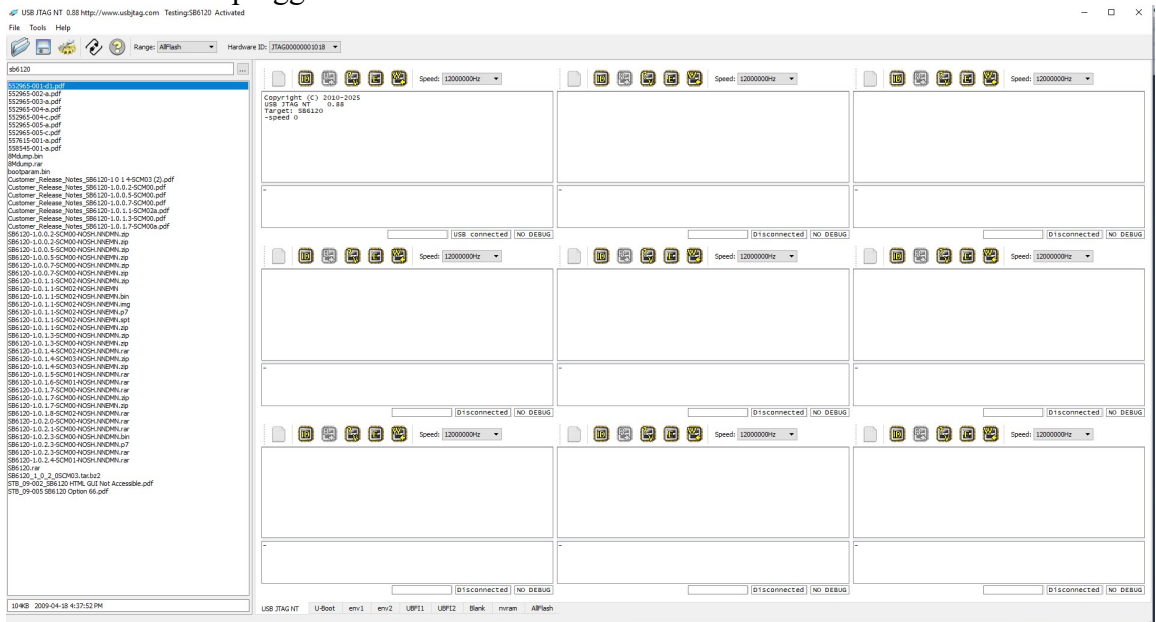
3.1 Software layout.

Start from 0.88. USB JTAG NT has two major working mode. Single JTAG mode and multi-JTAG mode. Most people will use single JTAG mode. Multi JTAG mode is for production line that program multiple device at the same time with one PC.

This is single JTAG view.



This is 9 JTAG view. You need to **plug in all your JTAG** when you start the software. If not single JTAG mode will be used. The number of JTAG displayed will depends on the number of JTAG plugged in when software is started.



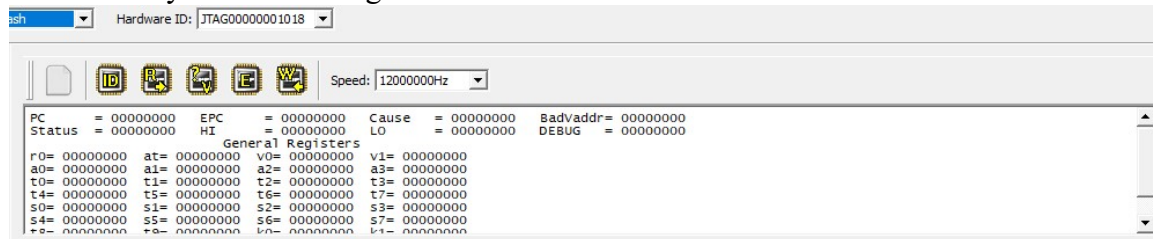
Normal view.

-

Memory view.

You can view the memory and also execute commands with the right click the memory tab to trigger pull down menu.

To read file you can use drag from the left file browser or external file browser.

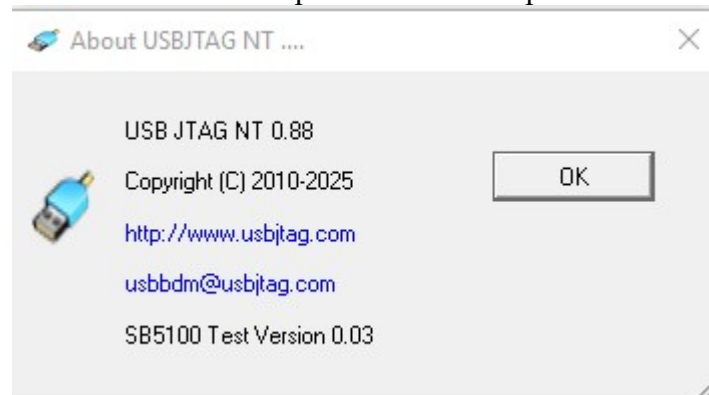


Register view, display MIPS (Or MC6833X) register values when in debug mode.

Note: For some board when power on and you see *DEBUG ON*, type “r” command. If PC is 0xBFC00000 then type “g” or press F5 to run the target.

Check the version of software

Help->about, version of the software printed out. Example



USB JTAG NT is the main application. Test module is the plug in DLL. If present, a new pull down menu exists after the “Tools” menu. **The plug in DLL must exist in the same folder as the main USB JTAG application.**

Configure the software

Before the software can be used, configuration must be done based on your target.

Xml configuration files exists under the config directory.

When select the target you can.

1. Type any word in “Search Target For” (eg.”510”), you can then select the target in the “Target select” (like, 510,SB5100, SB5101,SB5101Mod,SB5102, SB5102Mod)

2. Select target based on Category or Protocol. You can select Modem, then all supported modem will be on the “Target select”. You can also select EJTAG, then all EJTAG targets will be on the right.

The current supported protocols are:

EJTAG (MIPS)

DCU(ST20)

EJTAG64(MIPS64) – limited targeted tested.

BDM

SPIFlash

ARM7 –limited

ARM9

EJTAGPIC (PIC32MX)

ST20C1

EEPROM – Direct program the EEPROM.

XBOX360 – NAND programming

PPC- (DM500)

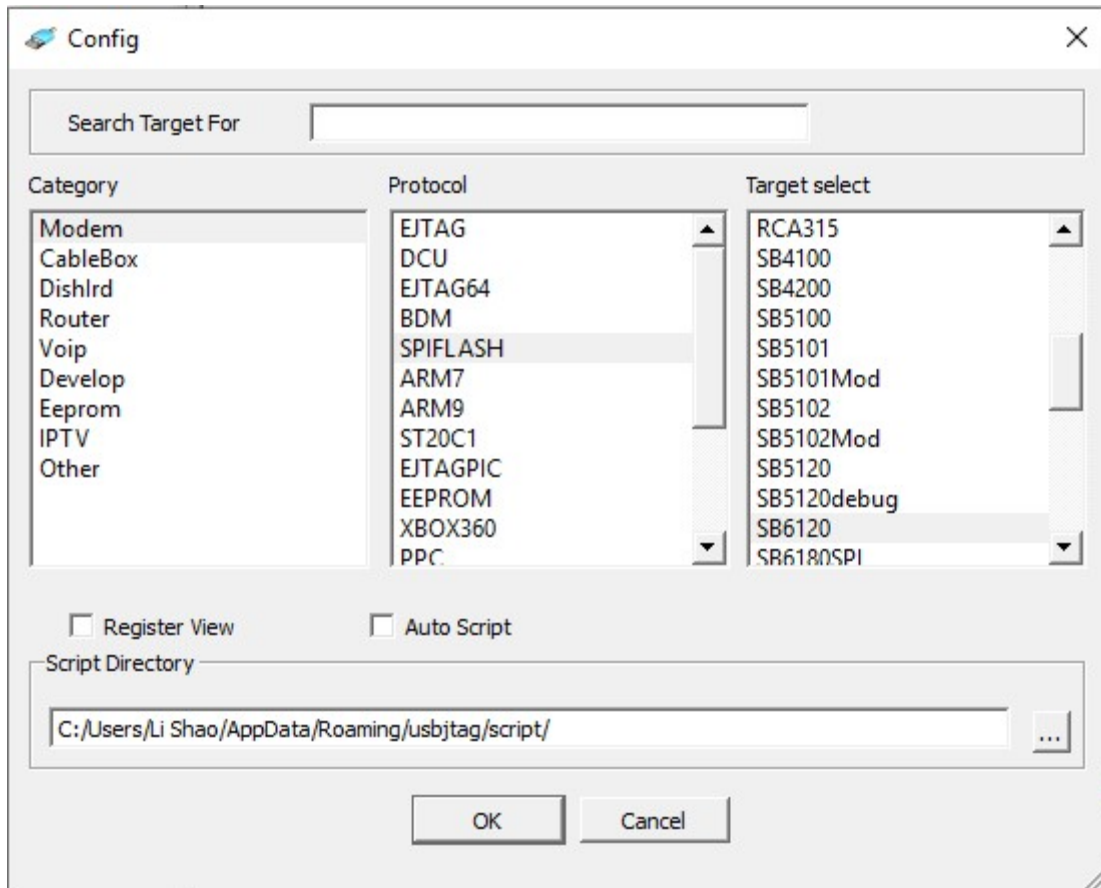
CPLD (JAM file playing)

ST40

ATMEGAICSP (under development)

SPI LCD (Experimental for Nokia 5110 LCD)

BDM PPC (under development).



3.2 GUI Usage

Even though the command line interface provides more power, many of its functions can be simplified by the included GUI interface.

Range selection

Memory access needs the start address and the length of the target memory. In the tool bar there is a drop down box that contains predefined start addresses and length with sudo-names. One can also click the tabs under the middle window of the picture shown above to determine what range selection is used.

Speed selection

This is to select the JTAG (BDM) clock speed. Even though we normally need high speed to program the target, it is needed sometime (especially when target is bricked) to use slower speed. The current hardware allows you to select three JTAG (BDM) speed.

Toolbar

Going from left to right

- Open file (command line equivalent: ldram)
- Save file (command line equivalent: save)
- Tools → configuration (command line equivalent: config)
- Target id detection (command line equivalent: detect)
- Read (command line equivalent: getram)
- Verify (command line equivalent: cmpram)
- Erase flash/EEPROM (command line equivalent: erase)
- Program flash (command line equivalent: program/sprogram)
- Connection. Show how to connect the target.
- About/Copyright info

3.3 Commands

USB EJTAG NT software is command driven. In command window typing “help” will give you all the command available. Type “help” and then a command will give you details of that command. Up, Down arrow keys can be used to go through the command history in the command window. Some commands are only available for certain target. “help” will always give you the exact command sets that can be used. Auto completion is incorporated, you can type partial command and hit tab to complete or toggle between commands that start with the same letters. Eg. Type “fl” + tab will give you flshdct.

Most used commands

1. **d:** Display the address.
Syntax: d address (in hexadecimal)
Example: d 9fc80000
2. **exit:** Exit the whole application.
Syntax: exit
3. **help:** prints command help.
Syntax: help — This will print all the command names.
Syntax: help (cmd) — This will print the usage of the cmd.
Example: help flshdct
4. **reset:** Reset the target.
Syntax: reset
Note: Not all the target board has the reset pin connected to JTAG port and even if the JTAG pin is connected to the JTAG port, the reset command might not reset the target for some other reasons. If this happened a power off/on will do the same work as reset.
5. **detect:** Detect the target CPU and possible flash types. If there are memory tabs defined as flash then a flash detect command is also issued.
Syntax: detect
Shortcut: F1
Example: (sb5101)
-detect
IDCODE 334917F

```
Broadcom BCM3349
IMPCODE 800904
DMA supported
Found Address= 9fc00000 Intel 28F160C3B
```

6. **search:** Search the memory block. This is ONLY used for an unknown target and you want to find the memory map. Most important to find where the firmware starts. For most users this **command** should not be used.

Syntax: search start end step.

Example:

```
-SEARCH 90000000 a0000000 200000
Address 90000000 data=FFFFFFFF
Address 90200000 data=FFFFFFFF
. . . . .
Address 9E000000 data=0BF00004
Address 9E200000 data=0BF00004
Address 9E400000 data=0BF00004
Address 9E600000 data=0BF00004
Address 9E800000 data=0BF00004
Address 9EA00000 data=0BF00004
Address 9EC00000 data=0BF00004
Address 9EE00000 data=0BF00004
Address 9F000000 data=0BF00004
Address 9F200000 data=0BF00004
Address 9F400000 data=0BF00004
Address 9F600000 data=0BF00004
Address 9F800000 data=0BF00004
Address 9FA00000 data=0BF00004
Address 9FC00000 data=0BF00004
Address 9FE00000 data=0BF00004
```

By further analyzing the firmware we can then figure out that the firmware starts at 9fc00000. For MIPS CPU they also map as 1fc00000 or Bfc00000.

7. **flshdct:** Detect the flash type.

Syntax: flshdct tabname
flshdct address

Example:

```
-flshdct boot
Found Address= 9fc00000 Intel 28F160C3B
-flshdct 9fc00000
Found Address= 9fc00000 Intel 28F160C3B
```

8. **flshset:** Set a flash type to the tab. This is used when the target is complete dead and normal rescue method cannot be used.

Syntax: flshdct tabname value1 value2. (Value1 and value2 will be the same value otherwise flshdct is used. Manufacture ID and chip ID).

Example:

```
-FLSHSET boot 89 8891
Found Address= 9fc00000 Intel 28F160C3B
-configshow
```

```

Test name:      SB5100
Test DLL:  SB5100.dll
IRLength:  5
Endian:     Big
Boot        Flash=Intel 28F160C3B
cfg         Flash=Intel 28F160C3B
Image0      Flash=Intel 28F160C3B
Image1      Flash=Intel 28F160C3B
log         Flash=Intel 28F160C3B

```

9. **init.** This is to initialize the target (in dll or in xml).
10. **initusb:** Initialize the USB PORT. This will trigger USB PORT to reinitialize the USB JTAG. It might take several seconds to get back “JTAG connected” state.
Syntax: initusb
11. **getram:** Read memory from target to PC. This is lengthy operation and the progress bar will show roughly where you are. After completion of the memory read, the memory in the tabs will be updated. You can view and edit the memory in the memory tabs. Be careful when editing the memory map, since most flash firmware have complicated checksum to avoid data corruption, simply editing the firmware and programming it back might not work.
Syntax: getram tab
 getram start length
Example: getram boot
 getram 9fc00000 200000
12. **save:** Save the PC memory to a file. The default file extension is “.bin”
Syntax: save tabname
 save start length
Example: save boot
 save 9fc00000 200000
13. **ldram:** Load binary file to PC memory. This is opposite to “save” command.
Syntax: ldram tabname (filename)
 ldram address
Example: ldram boot
 ldram 9fc00000
14. **cmpram:** Compare the PC memory with target memory. This is very useful especially for programming flash. If you use EJTAG you cannot do cmpram right after the programming if non-DMA is used. The OK means the memory are identical between PC and the target. Otherwise the failed address will be displayed.
Syntax: cmpram tabname
 cmpram address length
Example: cmpram boot
 cmpram 9fc00000 200000
15. **setram:** Opposite to getram, this set the target memory from PC. *This can only be used for ram not for flash. For flash you can only use “program” or “sprogram” to alter the target memory.*
Syntax: setram tabname

- setram address length
- Example: setram 80000000 200
16. **peek:** Get one word from target.
 Syntax: peek address
 Example: peek 80000000
 17. **pokeh:** Poke two bytes.
 Syntax: pokeh address value
 18. **pokeb:** Poke one byte.
 Syntax: pokeb address value
 19. **peekh:** Peek two bytes.
 Syntax: peekh address
 20. **peekb:** Peek one byte
 Syntax: peekb address
 21. **poke:** Set one word to target.
 Syntax: poke address value
 22. **flshlist:** List all the flash types that are defined in flash.def
 Syntax: flshlist
 23. **config:** Start configuration dialog to configure the target and view.
 24. **about:** Display the about dialog box.
 Syntax: about
 25. **cls:** Clear the screen
 Syntax: cls
 26. **e:** Edit data in PC memory. To update to the target ram or flash you need to use
 “setram” or “program” commands.
 Syntax: e address data1 data2
 Example: -e 9fc08000 11 22 33 44
 27. **f:** Fill data in PC memory. To update the target ram or flash you need to use
 “setram” or “program” commands.
 Syntax: f tabname value
 f start length value
 Example: f bootff
 f 9fc00000 200000 ff
 28. **s:** Search patterns in PC memory.
 Syntax: s tabname string
 s tabname data1 data2 ...
 s start length string
 s start length data1 data2 ...
 Example:
 -s image1 "SB5100"
 -s image1 40 08 80
 -s 9fd00000 100000 "SB5100"
 -s 9fd00000 100000 40 08 80
 29. **configshow:** Show all the configuration.
 Syntax: configshow
 Example:
 -CONFIGSHOW

```

Test name:      SB5100
Test DLL:  SB5100.dll
IRLength:  5
Endian:      Big
Boot        Flash=Intel  28F160C3B
cfg         Flash=Intel  28F160C3B
Image0      Flash=Intel  28F160C3B
Image1      Flash=Intel  28F160C3B
log         Flash=Intel  28F160C3B

```

30. **erase:** Erase the flash. The erase command is used with sprogram. Normal program command auto erase the flash. This command is only used when normal program command does not work. ST20 target must use erase/sprogram to program the flash. Please note that the erase command does not have feedback while erasing. And normally erase take quite a long time. A 2M flash's erase normally will take up to 20-40 seconds. If after a long time the program does not return something has gone wrong and you need to stop the program and start again.

Syntax: erase tabname
erase address length

Example:

```

-ERASE image0
Erase starts
Erase time  00:00:08 .021

```

31. **sprogram:** Slow program. This is slow program compared to normal program. In EJTAG this method is not used to target ram. In EJTAG when the boot is not in setup and the initialization sequence to access ram is unknown, sprogram is normally used for program a boot block. Make sure the target flash is erased.

Syntax: sprogram tabname
sprogram start length

Example:

```

-ERASE boot
Erase starts
Erase time  00:00:00 .031
-SPROGRAM boot
Program Starts...
Program time 00:00:08 .084
-CMPRAM boot
Compair data OK

```

32. **program:** Programs the flash or eeprom. If you program the flash make sure you have executed "flshdct" or "detect" command. The right flash type must be set to the memory.

Syntax: program tabname
program address length

Example: program boot
program 9fc00000 200000
program eeprom
-PROGRAM image0

- Erase starts...
- Erase time 00:00:08 .071
- Program speed 138.26 KB/s
- Program time 00:00:07 .081
- Program pass, if no further programming needed, power off/on the target
33. **bk:** Breakpoint in the target. Normally use this with register view enabled.
 Syntax: bk
 Shortcut: F6
 34. **r:** Read registers or set register value to the target
 Syntax: r
 r register value
 Example: r r1 8000200
 35. **t:** Single step. (Not for EJTAG64)
 Syntax: t
 Shortcut: F10
 36. **g:** Execute in full speed.
 Syntax: g
 Shortcut: F5
 37. **tap:** Send tap command to the device (Used for de-bricking MIPS device).
 Syntax: tap x (y)
 Example: tap c
 tap a ffffffff
 38. **blkchk:** Check if the flash is blanked. If the result is not blanked do not try to use program.
 Syntax: blkchk tabname
 blkchk start length
 Example:
 -blkchk flash
 Flash blanked
 39. **flshdcth:** This happens on IRD6000 dish receiver, while there were two flash chip and one hold the high word of data and another flash hold lower word of data. flshdcth uses different routine to detect the flash. In the usbjtag.def the "Protocol=DCU" and "HiLo=1". If not the flshdcth will not get the right result.
 Syntax: flshdcth tabname
 40. **ldramh:** This is the same reason as for flshdcth. When file saved in high word or lower word. You can use ldramh command to only load to high word or lower word of the memory in pc.
 Syntax: ldram address
 Example:
 -ldramh 7fc00000 (lower word file)
 -ldramh 7fc00002 (high word file.)
 41. **speed:** Select JTAG speed.
 -speed 2 (select 3MHz JTAG or 1.5MHz BDM)

3.4 JTAG Usage

1. Read memory
Use “getram” command. Eg. “getram u22”
2. Write memory
Use “setram” command. Eg. “setram nvram”

Program flash

The flash contains all the essential programs for your target to work properly. Therefore it is very important to understand the process of programming flash. In most case, you can burn flash in fast mode. But if the flash is accidentally erased and no initialization is known, then a slow mode might be used. First you need to make sure that watchdog is disabled. For known board with proper initialization a “detect” command will both detect the CPU and initialize the target. IT IS VERY IMPORTANT EACH TIME TARGET IS PLUGGED IN, A “DETECT” needs to be executed. F1 is the short cut key.

EJTAG only.

If it is the first time you program the flash, type the command “bk”, this command puts the CPU in “DEBUG ON” mode. Please do nothing for at least 30 seconds. If “debug on” stays, then the watch dog is disabled and you can program the flash safely. You only need to do this once for each type of target. If DEBUG goes off, then the watchdog is not disabled and program the flash is unsafe. Before you do some real programming, make sure the data is valid. (“bk” is break command and “g” is run to normal command).

You can then program the flash by typing the command “program tabname or program start length”. It is highly recommend the first time find a non-used sector to program and compare to make sure you have can program properly.

3.4 Bug report.

Please report bug to usbbdm@usbjtag.com . Since there are so many targets out there and people use them in different way, there will be bugs in the software. (Especially when using scripts). So if you find a bug or want to make an enhancement request, do not hesitate to write to me. The support forum can also be used.

<http://www.usbjtag.com/phpbb3/index.php>

Chapter 4 Script

USB JTAG NT supports very complicated script so it can automate a lot of the jobs. If you are programming a large number of devices, using script can save you a lot of time.

4.1 Basic script.

Basic script does not use controls and only have commands. Here is an example of basic script. (5101a.usp)

```
// *****  
// sb5100 restore script  
// *****  
detect  
ldram 9fc00000 %1  
echo Press enter to program, any other character with return exit the script.  
pause  
program 9fc00000 200000
```

In the command window you type in

```
sb5101a backup1.bin
```

Which the script will take one parameter as backup1.bin. Here is the explanation of how the script works.

```
// *****  
// sb5100 restore script  
// *****
```

These lines only displays the output to screen. (Echo does the same thing but will not display “Echo”)

```
detect
```

Execute command “detect”

```
ldram 9fc00000 %1
```

Equivalent to ldram 9fc00000 backup.bin

```
echo Press enter to program, any other character with return exit the script.
```

Display a prompt.

```
pause
```

Pause for you to hit “Enter”. You can enter any character and Enter to exit the script.

```
program 9fc00000 200000
```

Do the programming.

For further support on script, please contact usbbdm@usbjtag.com or go to <http://www.usbjtag.com> and join the forum.