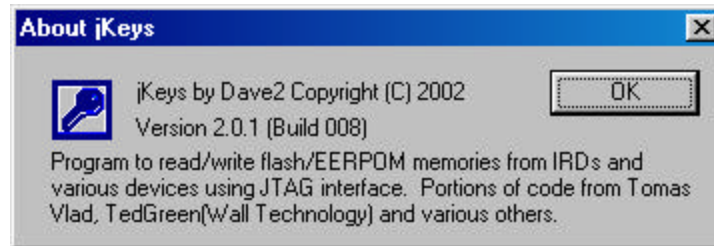


How-To use jKeys 2.0.1 (Basic)

By: do999 – September 29th, 2002 version 1.00



Credit: jKeys Version 2.0.1 by Dave2

Straight from the ReadMe file:

- jKeys is a program primarily used to access memory on IRDs. It works by utilizing processor diagnostic devices via the JTAG port. This software has been used on STMicroelectronics STiXXXX (ST20 based core) and LSI SC2000 processors.
- works on Windows 95/98/Me/NT/2K/XP
- auto detects STMicroelectronics ST20 base processors and LSI SC2000
- (ST micros STi5500, STi5505, STi5508, STi5510, STi5518, ST20-TP2, ST20-TP4, ST20-GP6) (LSI micro SC2000).
- auto detects most Echostar IRDs (2700, 2800, 3700, 3800, 3900, 4700, 4900, 501/5100, 301/3100, 6000)
- for IRDs detected, automatically read IRD number, Box Keys, Build Config, Model ID, Boot Strap and Software version
- works on several DTV IRDs (DRD420RE, DRD431RG, DRD220)
- for all IRDs known by jKeys, base memory flash configuration is provided
- allows flash reads for non-16 bit wide memory layouts
- reads memory and saves to file
- parallel port diagnostics
- start jkeys

Scope:

This is not a troubleshooting guide. This how to will walk you through the steps necessary to extract your boxkeys from an IRD and also provide the steps necessary to backup your TSOP and EEPROM. The steps outlined will show examples for the 2700 and 3100 IRD. Others are similar but not specifically shown.

Assumptions:

- That you understand the terminology used. If not, read one of the newbie guides first.
- That you have the necessary JTAG cable to connect between your computer and receiver (IRD).
- That you know how to properly connect your JTAG cable to your IRD. They are not all the same, there are many commercial ones with various connectors and switch settings. You can of course make your own as well. **Connecting the JTAG to the IRD will NOT be covered here.**
- That you have downloaded jKeys 2.01 software and have it unzipped and are ready to go.

BoxKey Extraction Step-By-Step

Step 1: Boot up your computer and get ready to run jKeys but do not launch the program just yet.

Step 2: Connect your JTAG cable to your computer's parallel (printer) port.

Step 3: Connect your JTAG cable to your IRD ensuring you have it configured correctly for the model of IRD you have and that you have the correct Pin/Pad placement.

Step 4: Plug in A/C power to the IRD. Note that if you have a 2700 series IRD you should ground PAD 1 to disable the boot sequence of the firmware if you intend to write to the TSOP. Do not ground Pad 1 on a 3100 IRD. If you are only extracting the boxkeys, don't bother grounding PAD 1. Note: The power LED does NOT need to be lit at this point. The IRD needs to be plugged in but not necessary turned on.

Step 5: Run the jKeys software. If everything is correct up to this point then you should see a window similar to the following:

Example 1: 2700 Model

The screenshot shows the 'jKeys by D2' software window. The 'JTAG Info' section displays 'Device ID' as 0x2D4C9041 and 'Device' as ST15500, with a 'Detect' button below. The 'IRD Info' section shows 'IRD Model' as 2700, 'IRD #' as R 00 1234 5678-12, 'Box Keys' as D1 1F C0 35 D5 31 1F D5, 'Build Cfg' as COCA Boot Strap 12B8, and 'Model ID' as 10G Software NE355, with a 'Detect' button below. The 'Save Memory' section includes a 'Region' dropdown set to 'Flash 1(29F400)', 'Start' at 7FF80000, 'Bytes' at 80000, 'Width' at 16 bits, 'Delta' at 2, and 'Offset' at 0, with a 'Save Mem' button. On the right, there are buttons for 'Flash Programming', 'EEPROM Programming', and 'Development Panel'.

Example 2: 3100 Model

The screenshot shows the 'jKeys by D2' software window. The 'JTAG Info' section displays 'Device ID' as 0x5400006D and 'Device' as LSI SC2000, with a 'Detect' button below. The 'IRD Info' section shows 'IRD Model' as 301-3100, 'IRD #' as R 00 1234 5678-12, 'Box Keys' as D1 1F C0 35 D5 31 1F D5, 'Build Cfg' as EAEA Boot Strap 13EB, and 'Model ID' as 10U Software NE339, with a 'Detect' button below. The 'Save Memory' section includes a 'Region' dropdown set to 'Flash 1(IC22-29LV160)', 'Start' at 1FE00000, 'Bytes' at 200000, 'Width' at 16 bits, 'Delta' at 2, and 'Offset' at 0, with a 'Save Mem' button. On the right, there are buttons for 'Flash Programming', 'EEPROM Programming', and 'Development Panel'.

Note that the information should be filled in immediately without any other actions. A quick check to ensure that your IRD# matches the information on the label is a simply way to verify that the information was read correctly.

Print the screen or write down the BoxKey information and put it in a safe place. Attaching a label to the IRD is a great idea so that you do not misplace the information.

If all you required was the boxkeys, then you can stop here.

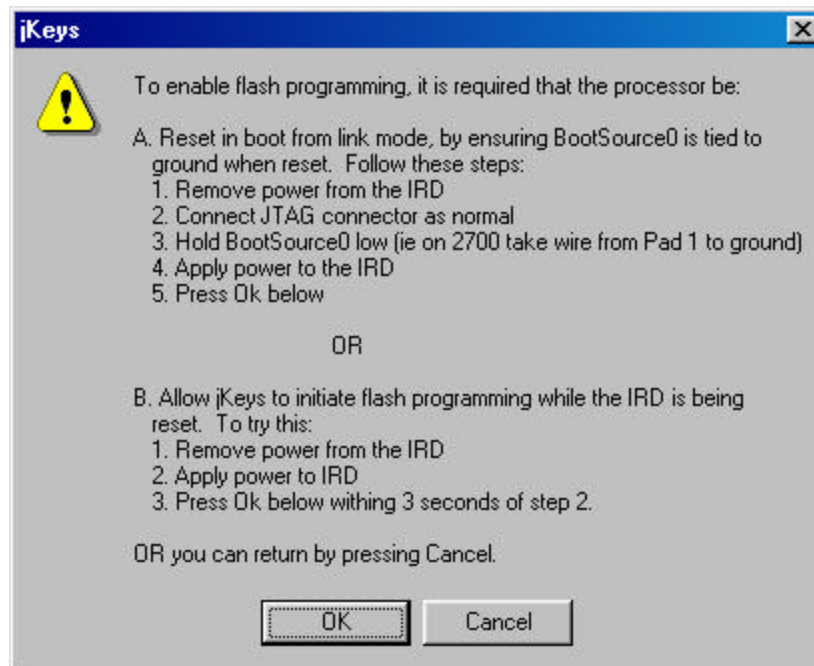
Disconnect: If you are not proceeding, then unplug the IRD, exit the jKeys software and disconnect the JTAG cable.

TSOP Backup Step-By-Step

From the main jKeys window it is possible to backup the TSOP within the IRD.

Step 1: Follow all the steps listed above to connect the JTAG cable and load jKeys. If your IRD # is correct then proceed to step 2.

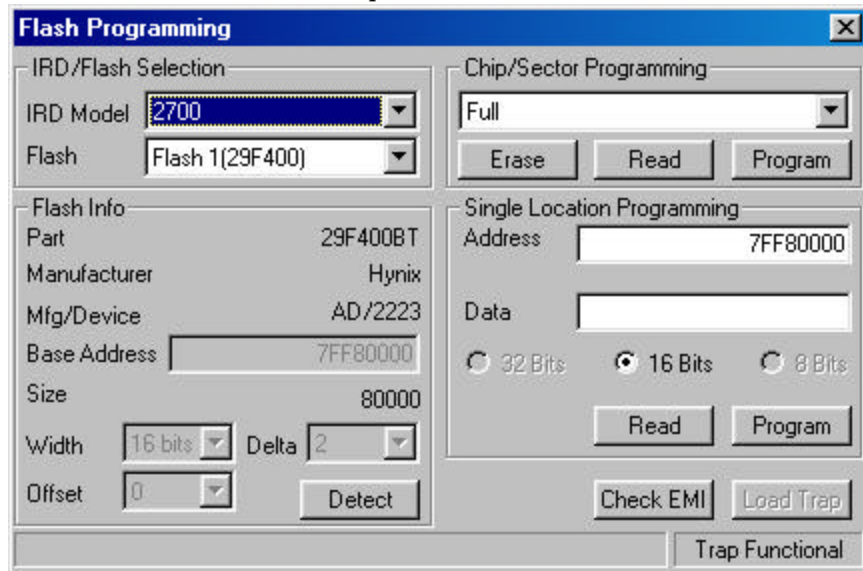
Step 2: Click on the “Flash Programming” button on the lower right side of the screen. If you have a 2700 IRD the following message will appear:



If you have not already grounded PAD 1 then follow the directions as listed now. Press “OK” when you are ready to continue. Note: This message does not appear if you are running a 3100 IRD.

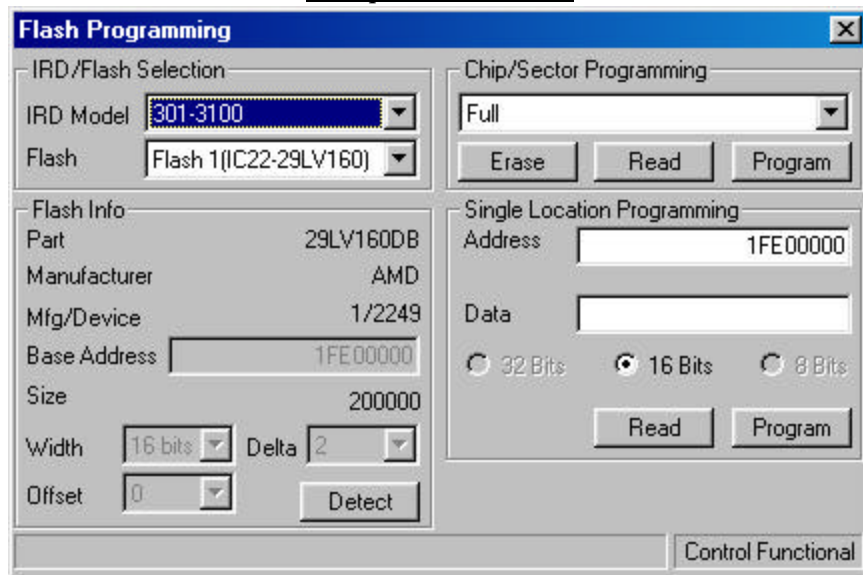
Step 3: The Flash Programming screen. The following window will appear:

Example 3: 2700 Model



The screenshot shows the 'Flash Programming' window for the 2700 Model. It is divided into several sections: 'IRD/Flash Selection' with dropdowns for 'IRD Model' (2700) and 'Flash' (Flash 1(29F400)); 'Flash Info' with fields for 'Part' (29F400BT), 'Manufacturer' (Hynix), 'Mfg/Device' (AD/2223), 'Base Address' (7FF80000), 'Size' (80000), 'Width' (16 bits), 'Delta' (2), and 'Offset' (0) with a 'Detect' button; 'Chip/Sector Programming' with a 'Full' dropdown and 'Erase', 'Read', and 'Program' buttons; 'Single Location Programming' with 'Address' (7FF80000), 'Data' field, and radio buttons for '32 Bits', '16 Bits' (selected), and '8 Bits', plus 'Read' and 'Program' buttons; and a 'Check EMI' button and a 'Trap Functional' checkbox at the bottom right.

Example 4: 3100 Model

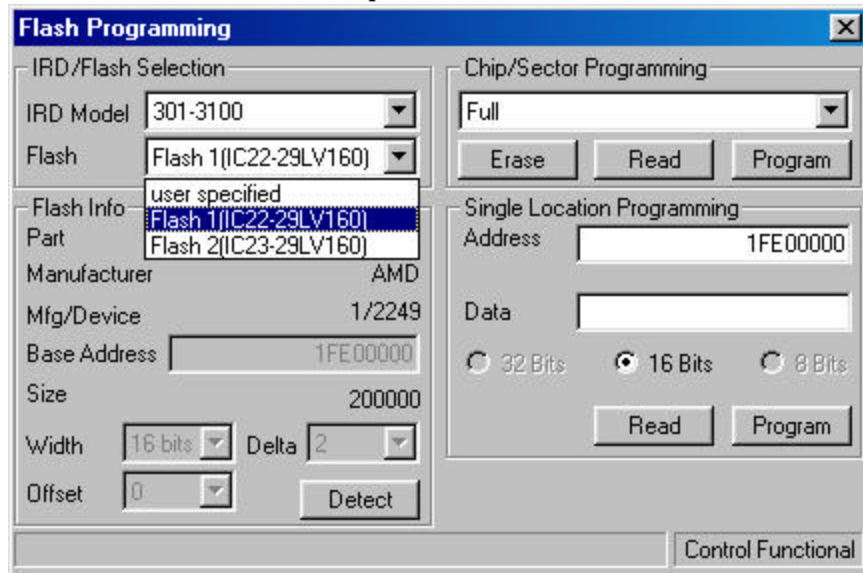


The screenshot shows the 'Flash Programming' window for the 3100 Model. It follows a similar layout to Example 3: 'IRD/Flash Selection' with 'IRD Model' (301-3100) and 'Flash' (Flash 1(IC22-29LV160)); 'Flash Info' with 'Part' (29LV160DB), 'Manufacturer' (AMD), 'Mfg/Device' (1/2249), 'Base Address' (1FE00000), 'Size' (200000), 'Width' (16 bits), 'Delta' (2), and 'Offset' (0) with a 'Detect' button; 'Chip/Sector Programming' with a 'Full' dropdown and 'Erase', 'Read', and 'Program' buttons; 'Single Location Programming' with 'Address' (1FE00000), 'Data' field, and radio buttons for '32 Bits', '16 Bits' (selected), and '8 Bits', plus 'Read' and 'Program' buttons; and a 'Control Functional' checkbox at the bottom right.

Note that the 2700 model IRD only has one TSOP, which is labeled Flash 1. The 3100 have two TSOPs, Flash 1 and Flash 2 and you can select which one will be erased, read or programmed using the drop down box. If the IRD model was correctly detected, then there is no need to play with any of the memory address or lengths. Simply select the Flash from the drop down box.

Here is an example of what the options look like:

Example 5: 3100 Model



Step 4: Backup the TSOP. Note the JTAG must remain in place throughout the entire procedure.

For the 2700, since there is only one TSOP, click on the “Read” button. You will be prompted to enter a path and filename to save the information from the TSOP to. The default value for the filename is probably a good one to use. The process should take approximately 2 minutes to complete.

For the 3100, select one TSOP (Flash 1 or Flash 2) and save the information to a file. Then select the other TSOP and save that information to a second file. Each flash will take approximately 4 minutes to complete. If using a press-on style JTAG cable, be prepared to hold it in place without moving for that length of time.

Verification: Use a hex editor or a tool such as FlashEdit to load the files that you just created. The IRD # and BoxKeys displayed in FlashEdit should match the information previously displayed by jKeys. While this is not a 100% guarantee that the backup is good, it is pretty close.

Disconnect: If you are not proceeding, then unplug the IRD, exit the jKeys software and disconnect the JTAG cable.

This document does not cover writing a saved flash back to the TSOP, however, the process is similar except you would use the “Erase” button to clear the TSOP and then use the “Program” button to write the saved file. Since I don’t want to get into the troubleshooting, I won’t mention it further.

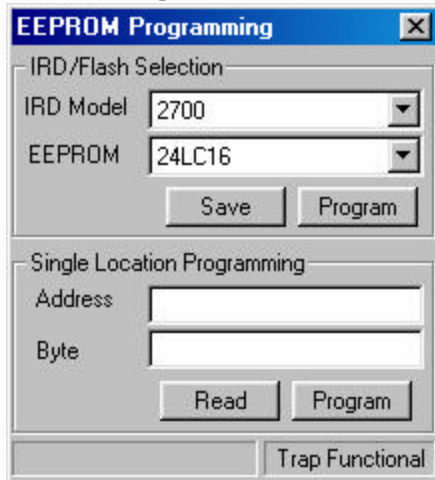
EEPROM Backup Step-By-Step

From the main jKeys window it is possible to backup the EEPROM chip within the IRD.

Step 1: Follow all the steps listed above to connect the JTAG cable and load jKeys. If your IRD # is correct then proceed to step 2.

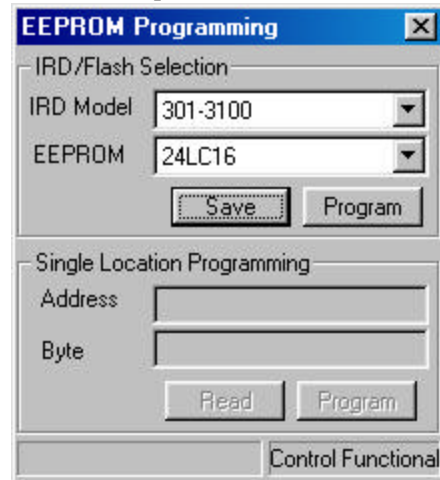
Step 2: Click on the “EEPROM Programming” button on the lower right side of the screen. The following window should appear:

Example 6: 2700 Model



The screenshot shows the "EEPROM Programming" window for the 2700 Model. It has a title bar with a close button. The window is divided into two main sections. The top section, "IRD/Flash Selection", contains two dropdown menus: "IRD Model" set to "2700" and "EEPROM" set to "24LC16". Below these are "Save" and "Program" buttons. The bottom section, "Single Location Programming", contains two text input fields: "Address" and "Byte". Below these are "Read" and "Program" buttons. At the very bottom is a checkbox labeled "Trap Functional".

Example 7: 3100 Model



The screenshot shows the "EEPROM Programming" window for the 3100 Model. It has a title bar with a close button. The window is divided into two main sections. The top section, "IRD/Flash Selection", contains two dropdown menus: "IRD Model" set to "301-3100" and "EEPROM" set to "24LC16". Below these are "Save" and "Program" buttons. The bottom section, "Single Location Programming", contains two text input fields: "Address" and "Byte". Below these are "Read" and "Program" buttons. At the very bottom is a checkbox labeled "Control Functional".

Step 3: Click on the “Save” button and enter a filename to which the information in the EEPROM will be written.

Verification: Use a hex editor to load the file that you just created. The Build Config (4 character code) should be displayed as the first four characters in the file. While this is not a 100% guarantee that the backup is good, it is pretty close.

Disconnect: Unplug the IRD, exit the jKeys software and disconnect the JTAG cable.

This document does not cover writing a saved file back to the EEPROM, however, the process is similar except you would use the “Program” button to write the saved file. Since I don’t want to get into the troubleshooting, I won’t mention it further.