

D2072A Unlocking Guide rev 1.0

Performed on Windows 7 OS

Required: USB thumb drive and USB cable (included with Oscilloscope.)

Optional: Rigol software disk (included with Oscilloscope.)

Preface

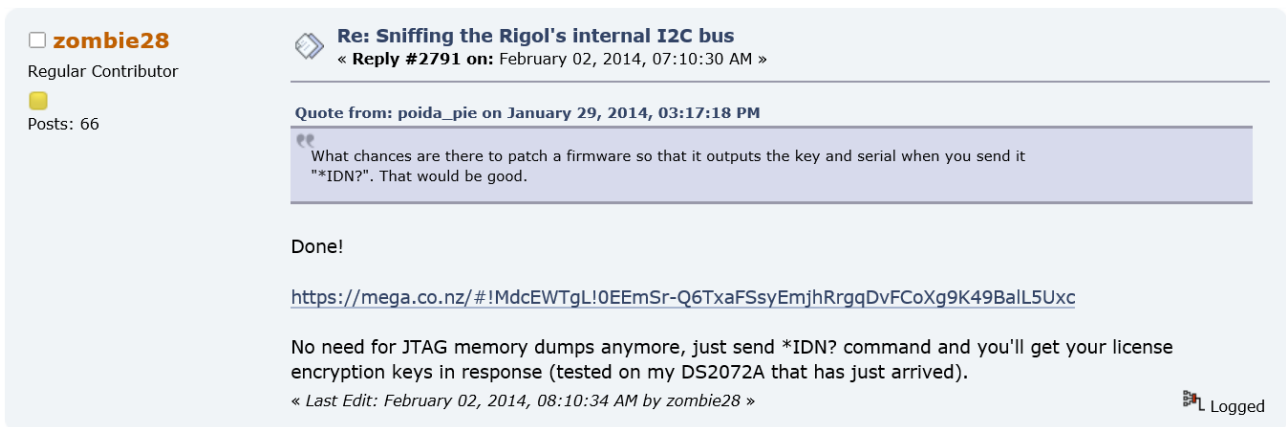
After completing this guide your DS2xxxA model oscilloscope will have all options available and an increased bandwidth, up to 300MHz. All credit goes towards the members of the EEVBlog community whom spent their time investigating and developing all of the software along with the knowledge provided in this guide.

Forum discussing the unlocking of Rigol oscilloscopes:

<http://www.eevblog.com/forum/testgear/sniffing-the-rigol's-internal-i2c-bus/>

It was discovered that all DS2xxxA series oscilloscopes had unique private keys, as opposed to the older non 'A' models which shared a common key. Custom firmware was developed by a forum member that allows a user to find their systems keys without needing to open up their device for a memory dump (which required addition hardware, i.e. a USB Bus blaster.) The modified firmware would return scrambled keys when the SCPI command `*IDN?` was sent over USB connection. A multifunction program created through the collaboration of a couple of users was capable of unscrambling the keys and then use a keygen to produce the license keys desired by the user.

Step 1: Installing The Modified Firmware



The screenshot shows a forum post from a user named 'zombie28', a regular contributor with 66 posts. The post title is 'Re: Sniffing the Rigol's internal I2C bus' and it is a reply to post #2791, dated February 02, 2014, at 07:10:30 AM. The post contains a quote from user 'poida_pie' dated January 29, 2014, at 03:17:18 PM, which asks: 'What chances are there to patch a firmware so that it outputs the key and serial when you send it `*IDN?`. That would be good.' The user 'zombie28' responds with 'Done!' and provides a link to a Mega.nz file: <https://mega.co.nz/#!MdcEWTgL!0EEEmSr-Q6TxaFSsyEmjhRrgqDvFCoXg9K49BalL5Uxc>. The post concludes with the text: 'No need for JTAG memory dumps anymore, just send `*IDN?` command and you'll get your license encryption keys in response (tested on my DS2072A that has just arrived).' The post was last edited on February 02, 2014, at 08:10:34 AM by 'zombie28'. A 'Logged' status icon is visible in the bottom right corner.

Figure 1: User posting link to modified firmware

<https://mega.co.nz/#!MdcEWTgL!0EEEmSr-Q6TxaFSsyEmjhRrgqDvFCoXg9K49BalL5Uxc>

1. Download and extract the modified firmware 'DS2000Update.GEL' from the link above. Move the file into the root directory of a FAT32 format USB thumb drive. (Note: Not all USB drives will work, you should plug in and test before attempting to update)
2. Power on the oscilloscope using the front panel power button - all the buttons will light up. Immediately after pressing the power button you need to press the orange 'help' button twice in very quick succession. If performed correctly all button lights except 'SINGLE' will turn off and the screen will remain blank. The oscilloscope is ready for the firmware update.

3. Put the USB into the oscilloscope and eventually the 'CH1' button will begin flashing, indicating the oscilloscope is updating. The process is complete once all button lights become active, this may take several minutes.
4. Turn off the oscilloscope and remove the USB thumb drive. Power the device up again and check that the firmware has been installed by viewing **Detailed System Information**.
 - a. Press the Menu in the trigger section and set Type to Edge.



Figure 2: Location of Trigger 'Menu' button

- b. In quick succession press the following sequence of buttons:
[Menu 7][Menu 6][Menu 7][Utility]



Figure 3: Detailed System Information buttons

- c. From the Utility menu that was just entered, press System and then System Info. Software version should be 00.02.01.00.03.

Step 2: Installing Ultra Sigma & Retrieving Scrambled Keys

In order to retrieve the scrambled keys from the device a program provided by Rigol has to be installed. You can obtain the program from either the software CD provided or from their website.

Ultra Sigma Software

Version:00.01.05.10

Installation guide: 1.Install NIVISA driver; 2.Install Ultra sigma software

2013-09-13

<http://www.rigol.com/prodserv/Digital%20Oscilloscopes/software/>

Once you have installed the Ultra Sigma program, (You can view the readme.txt for any installation information) power up the oscilloscope and attach the USB cable to the computer and oscilloscope. After a moment the program should recognise the oscilloscope, right click on the device and Open SCPI Control Panel.

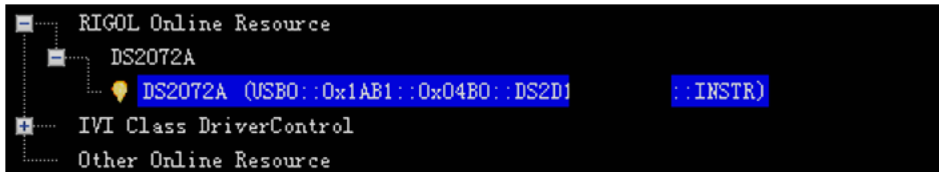


Figure 4: Device visible in Ultra Sigma

In the Control Panel press the 'Send & Read', the information returned will have your serial number followed by a very large HEX string. Keep this information for later use.

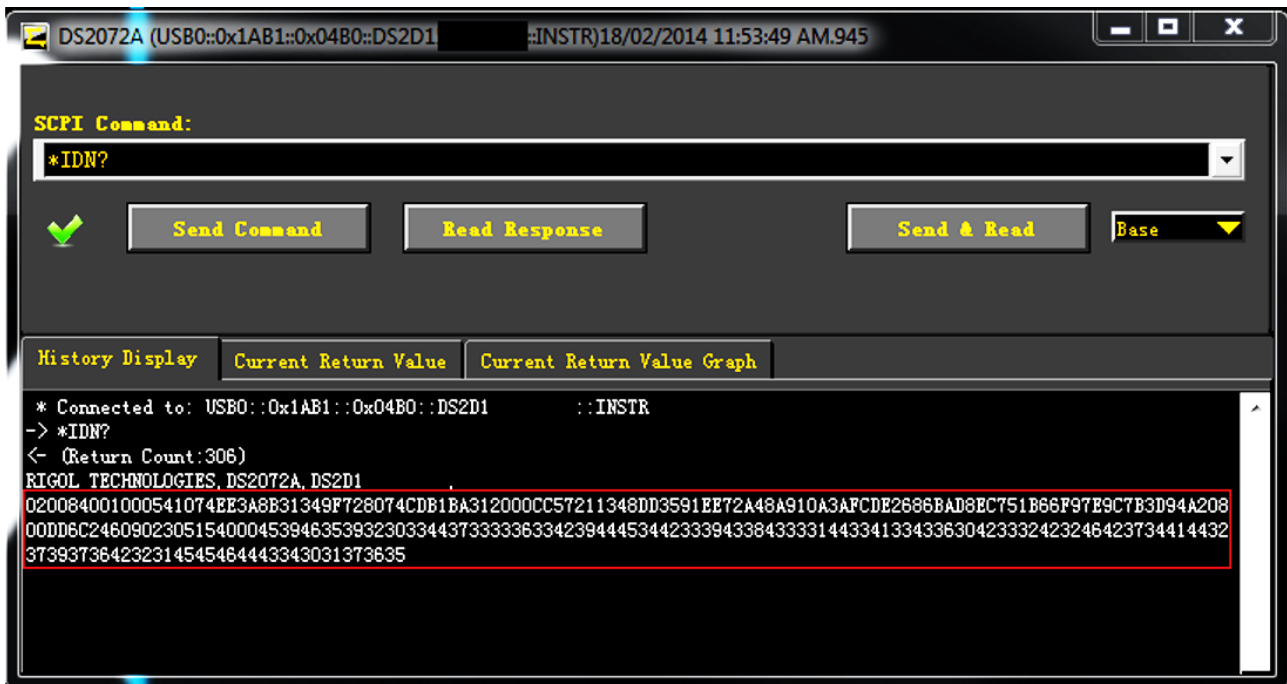


Figure 5: Information returned after *IDN? command

Step 3: Converting Scrambled Keys into Correct Format

To use the information returned by the modified firmware in the keygen program it has to be modified into binary format. A free program HxD is used:

<http://mh-nexus.de/en/hxd/>

Create a new file in HxD, you will notice there are three columns. The left column is in blue text and has 'Offset (h)' written at the top, this is the address column. In the centre is the data column (16 8-bit HEX values in each row.) On the right is the data in the format selected from the drop down menu (This format doesn't need to be modified.)

In the centre column after the existing information (don't remove this) paste in your very large HEX string. In the right column at the end paste your serial number (DS2Dxxxxxxx) as is and finally in the middle column append a '0', it will appear as 00 in HEX (Note: use the regular number keys, my numpad '0' was mapped to '03'.) Your file should look like Fig. 6, save this as key.bin.

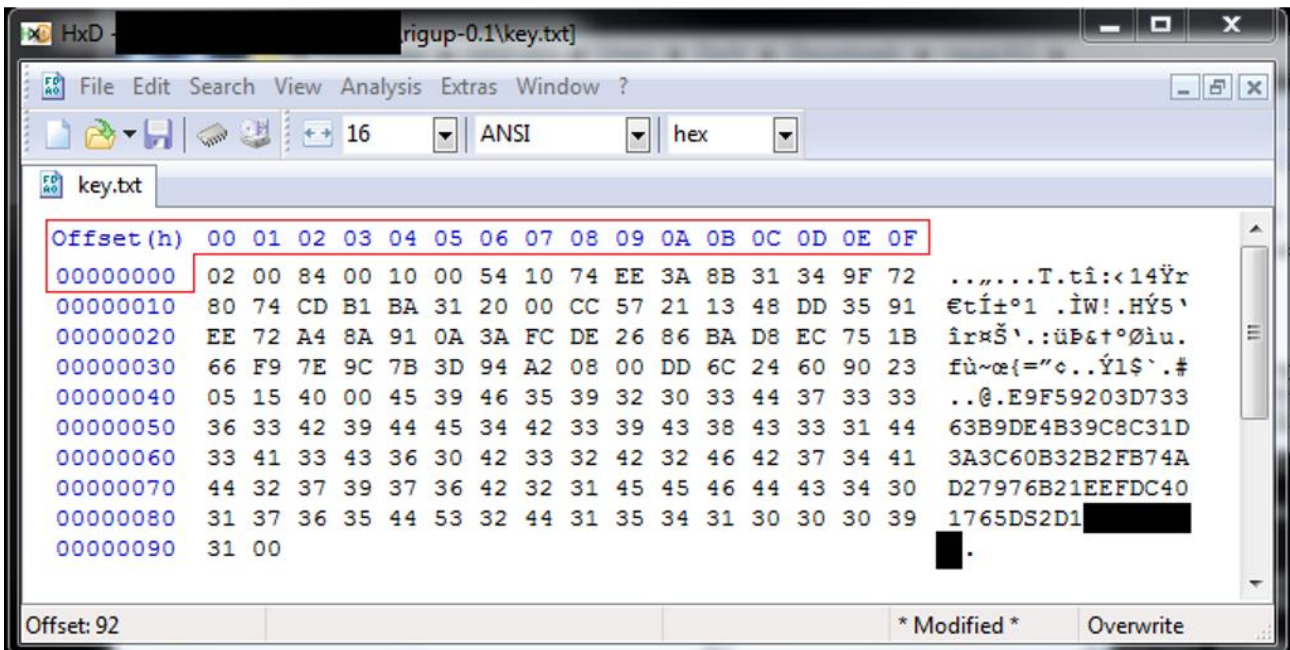


Figure 6: Correctly formatted key.bin file

Step 4: Generating Licence Keys & Applying to Device

tirulerbach
Contributor
Posts: 32

Re: Sniffing the Rigol's internal I2C bus
« Reply #2802 on: February 03, 2014, 02:03:20 AM »

Quote from: zombie28 on February 02, 2014, 08:25:36 AM

“ You can use either my first firmware patch (<https://mega.co.nz/#!FFk10SCY!UuWPXyqZwmca00pa2clOth1ryh1Z-AAqJg2yibfoUw0>) with old keygen (riglol.3owl.com) or my newest patch from the post above with the new tirulerbach's keygen (if he decides to publish it).

Decided: <https://mega.co.nz/#!qAkUkTZB!XG12bUKhIz4CmQt6DbBnGRMvEe5AvUjEaBxi4R03tw8> 😊

Logged

<https://mega.co.nz/#!qAkUkTZB!XG12bUKhIz4CmQt6DbBnGRMvEe5AvUjEaBxi4R03tw8>

After extracting the rigup program move your key.bin into the same directory as rigup.exe. Open the command prompt at that location (In Windows you can type cmd in the windows explorer file path and it will launch cmd prompt with that directory.) Type the following command:

rigup scan key.bin

If steps are followed correctly to this point rigup will return a list of keys from the string in the file. Copy all of this as is and save in another text file as keydecoded.txt (Format: ANSI) in the same directory. Back in command prompt:

rigup license keydecoded.txt NSxx

A license key will be returned with dashes.

<p>NSEH - All Options NSER - All Options + 100MHz NSEQ - All Options + 200MHz NS8H - All Options + 300MHz</p>

Copy the code and return to the Ultra Sigma Control Panel for your device, as before. Remove *IDN? and enter the following:

:SYSTem:OPTion:INSTall 'enter licence key here'

Do not include the quotation marks or any dashes when entering the code, just enter as a continuous line of characters after one space after INSTall.

Hit the send button and you should see a progress bar appear on the oscilloscope screen, once completed restart your oscilloscope and your options should be applied.

To uninstall all the options

:SYSTem:OPTion:UNINSTall

Congratulations you have completed the guide and added value and additional function to your oscilloscope.