

Open Firmware with IDA

Open Firmware with IDA

by [Edgpaez](#) on 20 Dec 2008 02:46

This is a basic step in order to create or port basic and advanced patches for ANY phone.

First of all you must download IDA (The Interactive Disassembler)

[url=http://www.4shared.com/get/28118661/3668f237/IDA_PRO_500879.html;jsessionid=6A9924565733E944445D103BF824F670.dc113]Here[/url]

First of all you must Convert your Main file into .raw, with

[url=http://rapidshare.com/files/152893865/babe2raw.rar]THIS[/url] program, just Drag .mbn file into it and it will create it on its own.

Then install IDA, after the installation is done, we can continue:

1. You open IDA:

[non-available image posted]

And click Go to Work on you own.

2. File->Open:

Select your .raw file (the one converted before from the .mbn)

[non-available image posted]

3. In Processor type choose ARM Processors: ARM710a and click Set.

[non-available image posted]

Then click Processor options and mark:

"Disable pointer dereferencing"

[non-available image posted]

Then click OK and OK again....

4. Here you must input Base and length address:

->In "ROM Start Address" and "Loading Address" you must put the Base of your Firmware (0x44140000 for ALL db2020 Main files)

->In "ROM Size" and "Loading Size" there's an original value with an Hex calculator add to it 100000 hex, the result does in here, for Db2020 is 0x01DC0001

[non-available image posted]

Then click OK.

When you see "Generating list of strings" Dialogue click on Cancel

5. In menu, go Options > General...

and in Number of opcode bytes replace 0 for 4 and click OK

[non-available image posted]

6. Define data type:

In menu, Options > Setup Data Types...

and **Unmark**: - 1 Byte, and 2 Word

[non-available image posted]

7. To change view between ARM and THUMB

press ALT + G and replace Value to 1 to see in Thumb.

To open and see the code press C (functions start at XXB5;being XX any byte)

[non-available image posted]

Then you go Menu, and File->Save and wait....

then when you want to close mark "Don't pack database" and "DON'T SAVE the database" and OK.

Tip:

ONLY for DB2020 users, you can use

[url=http://www.4shared.com/file/90166598/f6101117/ida_babeldr.html]THIS[/url] plugin by den_po.

According to your IDA version (if it's the one posted here use 5.x)put the babeldr.ldw file in your IDA/loaders folder before the whole process, and jump to step **4**

NOTE:

This has to be done with all the main files you're going to use, wether it is the origin FW or the destiny.

(c) Shadow Player

Best wishes,

SE Develoepers

Disassembling the whole firmware

by [Drknzz](#) on 26 Mar 2010 13:30

Hi guys!

Im trying to Create a new patch for w980, i have the main idea (More SWFs on the external screen), but first i have to find the hook.

Ive tried searching with smelter for Text, and i get a couple of references to SWF on the main, problem is, i get no XRefs from any of them (My guess is that ida hasnt analyzed the code that calls those SWF references), so i need to disassemble the whole thing, isnt there a way that is more efficient than just press C like a madman?

Thanks in advance!

by [Crusader](#) on 26 Mar 2010 17:03

Use page/sub finder..

it will disassemble lots of functions automaticly...

by [cherylfoster](#) on 05 Jan 2011 19:33

It could also be interesting to play with the disassembler to analyze the code a little longer, and generate lists of good cross between parts of code and code and data.