Old Topic: http://forums.se-nse.net/topic/39110-apap
(Markross is no longer the developer of this tool, vitor_boss is now the developer)

New Topic: http://forums.se-nse.net/topic/56232-advanced-porting-tools/

Advanced Porting Tools

Started by vitor_boss, Mar 29 2011 12:53 AM

Advanced Porting Tools



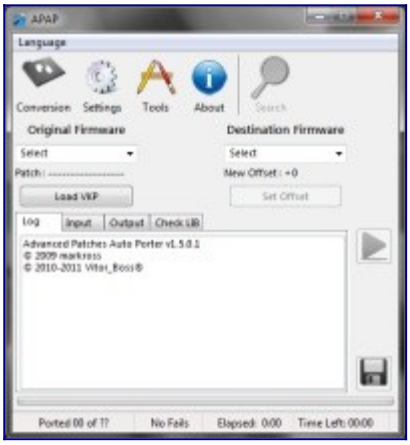
Hi everyone, this is a tool to HELP on patch porting. If is your first time on porting section read HERE. It was made to be simple, but sometimes difficult a little.

First of all sorry by bad English.

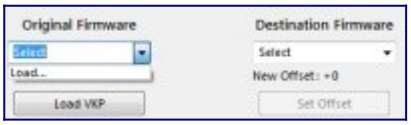
This tool have at moment 9 functions:

- - Patch porting with individual settings for simple, advanced and LIB patches;
- - Pattern Search;
- - Lib Comparator;
- - Bytes reverser with automatic mode;
- - Hex Calculator;
- - Text Conversion Hex to Ascii/Unicode and Ascii/Unicode to Hex with character counter;
- - Patch Compiler (ASM to VKP directly);
- - Base changer, you can remove Base from patch or increase with only 2 or 3 clicks;
- - Include file creator, generate file "Xxxx_Fxxxxxx.inc"(phone model_phone fw.inc) from LIB patch.

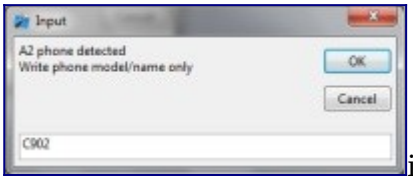
Patch Porting



This is the beginner feature of this tool, made by Markross and continued by me.
This have a very simple interface, a lot of small functions and a very simple usage.
How to use:

First at all load the FW clicking on the combo areas: 

Important: This is a necessary step to use almost functions of this application.
If selected FW is A1 then the name is get automatically if not will appear this request:

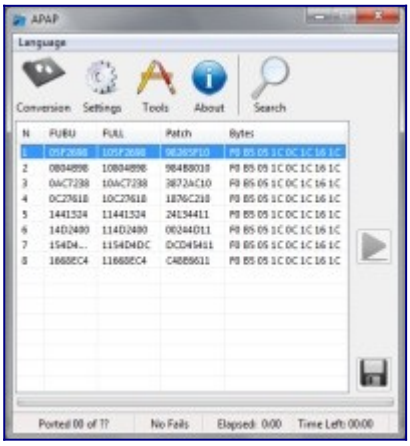


in that case i wrote C902 as my phone model.
After select FW listed on Original Patch and the target FW you are ready to load patch. There is 2 ways to read a patch:

- Just click on "Load VKP" button and select the patch file.
- Copy patch on browser and paste on "Input" tab;

You can edit patch in any moment;
Go to settings and wrote your name on place of "your nick here" this is your (p)orter nick and will appear on every ported patch;
If you need use the Base just select "Base needed", if you want read detailed porting LOG click on "Store LOG on txt file" wen this options is marked will appear the option "Destination Folder Output" this option save the LOG file on same folder as the 'Destionation Firmware' if not selected will save on application path;
You are ready to start porting by clicking on Start button;

Pattern Search

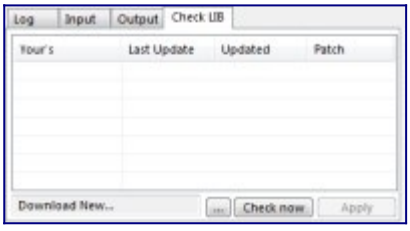


This is a multi pattern search engine, to use it you must have selected the 'Destination FW'.
You can use many kind of patterns like:
Byte:
- F0B5051C0C1C161C
- F0;B5;05;1C;0C;1C;16;1C or you can use other character to delimiter the bytes like '.', ',' , '|' or white space.
You can use the ?? as any like 'F0??051C0C1C161C' and ?x or x? to accurate the search like 'F0B? 051C0C1C161C' this will show any all existent combinations to B?;

IDA generated code:
- Just copy the code from IDA and paste and search.

Text:
- Enter the text for Ascii. Like 'test'
- Enter the text with @ for Unicode. Like '@test'
* This is case sensitive and will differ upper and lower cases characters.

Lib Comparator



Simple LIB comparator, made by me to compare my ported LIB version with the perk11.info version.

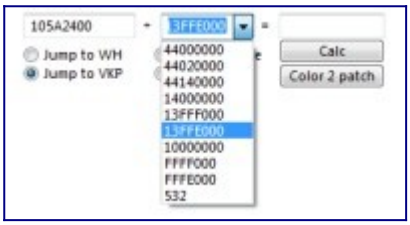
How to use:
Select the Original Firmware and click "Check Now" to compare with perk11.info version or click on "..." to select a LIB file to compare. The apply button will replace the old functions by the new ones;

Bytes reverser with automatic mode



This is simple to use, write any offset with 8 characters length and reverse by clicking on arrow image, after reversed the offset will be copied in clipboard. To make this automatically just select the option 'Get and Revert Automatically', then when you copy an offset this will be reversed and putted back in clipboard using a timer;

Hex Calculator



Made by markross this is useful to calculate hex offsets. [Decription Here]

Text Conversion



This is made to convert text from/to patch;
This support Unicode texts, if you forgot mark 'Unicode' option and the input was Unicode the options is marked automatically on a Text to Hex conversion;
On a Hex to Text conversion you don't need specify if is unicode or not, it is recognized at conversion;

Patch Compiler



The tool made to simplicity, this is a ASM compiler dedicated to ARM instructions based on FASM for ARM compiler. More details at http://arm.flatassembler.net/
This use another 2 settings, 'Base needed' and the selected FW at "Original FW" to read the bytes. You can read, edit, save and compile ASM files. The result is stored at 'VKP' tab.

Base changer

Build to be simple too, just select if you will 'Remove Base from patch' or 'Increase Base', for increase you must write the base on text box. Now just load the patch and have fun.

Include file creator

This a developer section, this generate a '.inc' file from LIB, this can generate file 'Externs.h' if selected.

All at moment.
Hope useful for you, if not share your idea for a new function and I'll build it with pleasure.

Download Here.

Feedback is needed. Thank you by patience;

Att. Vitor_Boss®

New Version! v1.5.1.1 11/05/2012

Changelog

```
- Improved Search speed, now is up to 2x faster;
- Improved Offest jump porting;
- Improve speed for branch detection and comparison;
- Improve detection of unicode strings pattern, now the pattern lenght is same as
text;
- Improved "Include Creator" tool, added option to output a ASM file.
- Fixed get wrong address to port;
- Fixed db32xx porting;
```