

Porting constants for dyn_const

Porting constants for dyn_const

by [myrzeug](#) on 06 Nov 2008 21:22

SE Developers Team Note:

This tutorial is a translation (with some more tips and points) of the MiniTutorial submitted by den_po on mobilefree.ru

Porting constants has no direct relation to VKP patches , but due to a big amount of doubts and non tutorials submitted, the Team has decided to include this in the Beginner's forum, with the big help of **myrzeug**

Tools:

IDA 5.x

sub / page finder (Plugin for IDA), assistant (thanks to den_po)

saveevents.elf annexed into the tablet (thanks to den_po)

For the edition of itself dyn_const

DYNeditor v1-1 (thanks to UltraShot)

Materials:

-Main Firmware (.raw) of the phone with the missing constants(let's call it Firm A)

- its dyn_const

-Main Firmware (.raw) of the complete dyn (constants to be ported present) (let's call it Firm B)

-its dyn_const

First of all:

You must place the plugin "pagesub.plw" in C: \ ... \ IDA \ Plugins

1. Run saveevents.elf on the phone (Firm A, or phone with missing constants) and find the file that is generated: Events.txt

(This elf creates a basis of certain constants, which serve as a guide for the rest ..., then it closes)

2. Open Firm A in IDA ([url=http://sedevelopers.oxyhost.com/showthread.php?tid=147]here a tutorial[url])

Then run the getevents.idc (Edit-> File IDC ...), with Event.txt

3. Wait until the process is complete....

Then in IDA go to: Edit-> Plugins-> sub / page finder

4. Do the same thing with Firm B (opening with IDA and run the plugin

5. Open the dyn_const of the Firm B, and find the constant you want to port to Firm A (the value is the important)

6. Now, go to addresses for each constant in both firmware (find adress in the list below), compare the structure, find the similarities and differences, and the you can say the values of the constants! in FirmA from those found in the FirmB in step 5

Here nothing is written, only practice will allow them to succeed with the correct values

Clarification:

The plugin, looking structures of events throughout the firmware, labeled by evtlst_XXXXX

When applying Events.txt file with the *. idc and run the plugin, what it does is "to recognize some of these constants (values that will see green in IDA), giving a guide to find the remaining constants

7. Once you have found the right value of the constant, you can edit the dyn_const of the Fim A with the DYNeditor and include its value (with the same position than in dyn form Frim B)and save, then your dyn will be updated....

(You can also use the DCE.elf to introduce the value found for the constant directly with the phone)

list for the constants (published by den_po):

[CALLMANAGER_CALL_END_SET_CALLTIME_EVENT](#)

evtlst_StandbyBook_Base

[CALLMANAGER_KILL_CALLBOOK_EVENT](#)

evtlst_DataBrowser_Base

evtlst_MSG_UI_Default

[CAMERA_APPLICATION_START_EVENT](#)

[RESPONSE_CAMERA_APPLICATION_START](#)

[MEDIAPLAYER_APPLICATION_START_EVENT](#)

[RESPONSE_MEDIAPLAYER_APPLICATION_START](#)

MISSED_CALL_EVENT

pg_InformBusy: AGE_ENTER_EVENT
evtlst_MMTApplicationBook_Base

ONGOINGCALL_CALL_CONNECTED_EVENT

evtlst_SetupCall

ONGOINGCALL_CALL_START_EVENT

evtlst_SetupCall
evtlst_Manager_Base
evtlst_UICLH_OGCallBook_Base
evtlst_UICLH_OGCallBook_RetrieveHeld
evtlst_Diverting
evtlst_MTCall_Base
evtlst_InformCallWaiting
evtlst_InformVideoCallWaiting
evtlst_InformMissedCalls

ONGOINGCALL_SET_CALLCOST_EVENT

evtlst_UICLH_OGCallBook_Base

ONGOINGCALL_SET_CALLTIME_EVENT

evtlst_UICLH_OGCallBook_Base

ONGOINGCALL_SPEAKER_ONOFF_EVENT

evtlst_UICLH_OGCallBook_Base

ON_CALLMANAGER_EVENT

evtlst_VC_AnswerRecognition

SOUNDHANDLER_APPLICATION_START_EVENT

RESPONSE_SOUNDHANDLER_APPLICATION_START

UI_CONNECTIONMANAGER_SESSION_ESTABLISHED_EVENT

evtlst_UIConMgr_Default

UI_CONNECTIONMANAGER_SESSION_TERMINATE_EVENT

evtlst_UIConMgr_Default

UI_MEDIAPLAYER_NEXT_TRACK_EVENT

evtlst_MediaPlayer_Audio_Bk_Base
evtlst_MediaPlayer_Video_Base

UI_MEDIAPLAYER_PREV_TRACK_EVENT

evtlst_MediaPlayer_Audio_Bk_Base

evtlst_MediaPlayer_Video_Base

UI_SLEEPMODE_ACTIVATED_EVENT

evtlst_StandbyBook_Base

pg_Screensaver_Sleep: AGE_ENTER_EVENT

Example:

Here you'll see the port of the constant

UI_CONNECTIONMANAGER_SESSION_ESTABLISHED_EVENT from w850 to w810.

According to the list we must go to evtlst_UIConMgr_Default found in 45C58F60 (w850) and 445405C0 (W810):

W810

[non-available image posted]

W850

[non-available image posted]

In w850 the constant value is 10D4, in this case is found on the first block and we can easily say that correct value for W810 is CB9

comment by den_po:

it's important to check event handlers (functions near event numbers) because tables may contain records in other order.

page/sub finder is also usable for porting patches because it gives understandable names for thousands of functions

Notes:

-> How to go to the constant address ?

*easiest way is find it in N Names list

-> It's not important the DB in this case of porting (unlike patch porting)

you can port constants from DB2020 to db2010 and vice versa without any notorious difficulty.

(c) myrzeug

Attachments

[pagesub.zip](#)

(38.17 KiB)

[DYNeditorv1-1.rar](#)

(43.09 KiB)

RE: How to port constants?

by [myrzeug](#) on 21 Nov 2008 21:50

First, run the plugin by den_po, the structures of events will be created, and you can see the name "evtlst_MediaPlayer_Audio_Bk_Base" in this tab "NAMES" in IDA, There you will find the offset of the structure