Explication de la panne de blocage ou Mise à jour

Un medianav qui restait bloqué sur le logo du boot. cette panne est causé par une erreur sur l'une des partitions du medianav.

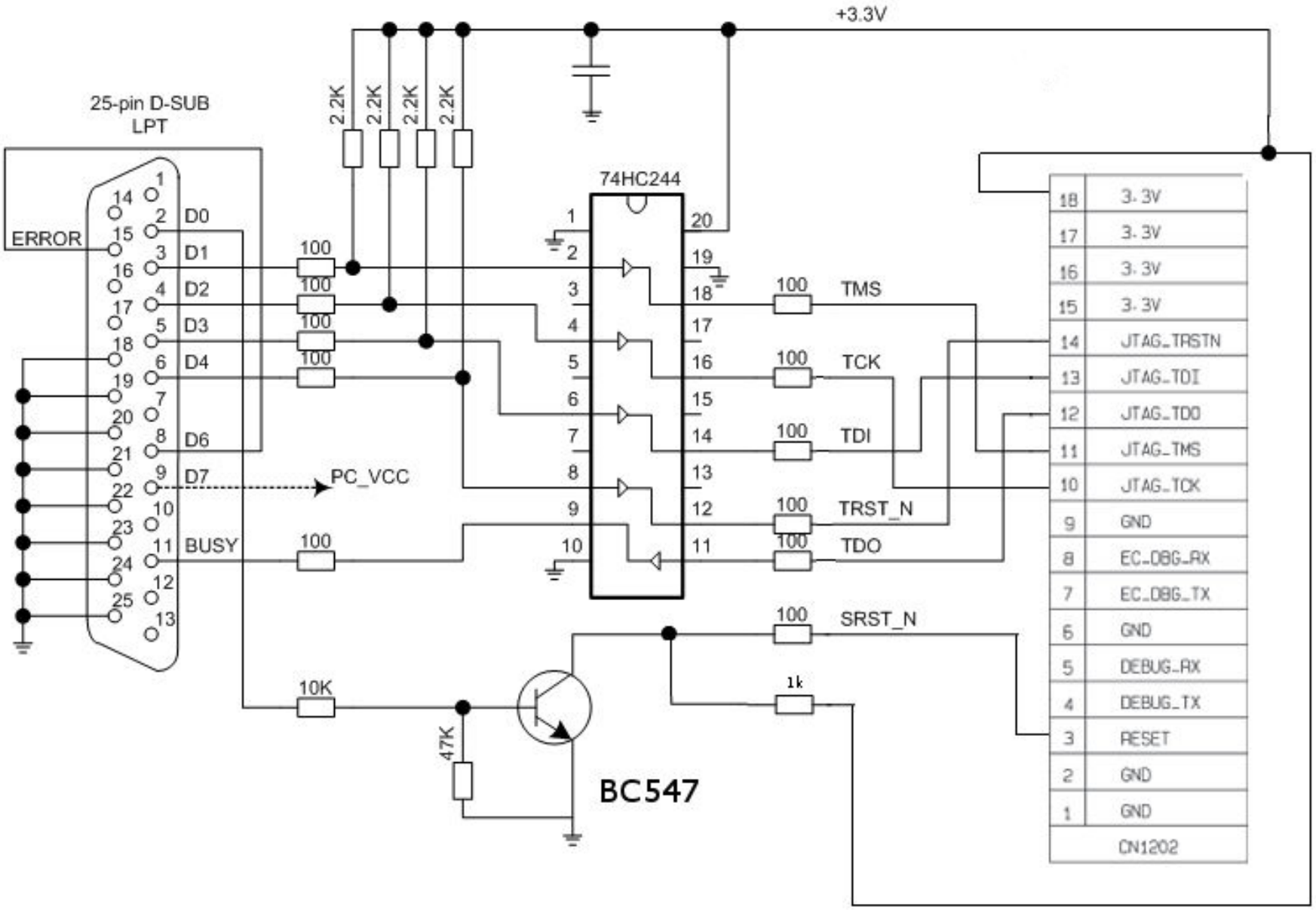
Ses symptômes, blocage au logo du boot, mise à jour bloqué ou medianav qui reboot sans cesse, ces pannes peuvent-être réparées par cette méthode

I) Dépannage :

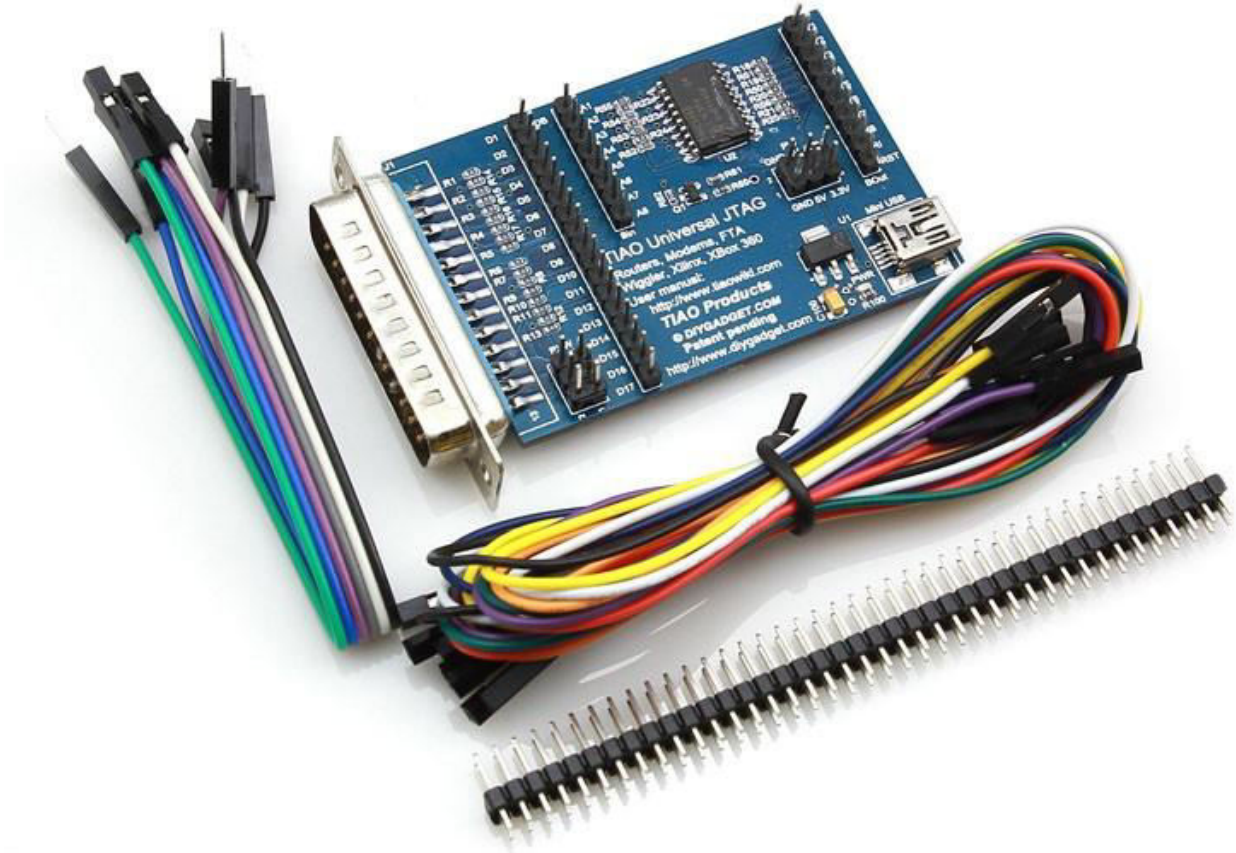
Le Storage card2 avait des secteurs défectueux ... et bloquait son démarrage.
donc dans l'ordre:

1) préparation de l'interface jtag

WIGGLER JTAG Medianav



je n'ai pas câbler srst_n ni la boucle sur le port // et ça fonctionne très bien
on peut en acheter une toute faite



2) configuration de windows en mode test

pour utiliser le port // nous sommes obligé de passer windows en mode test le driver n'a pas été signé par Microsoft:
Lancer dans une console administrateur sous windows 10 et reboot

bcdedit.exe /set TESTSIGNING ON

Pour revenir en mode normal

bcdedit.exe /set TESTSIGNING OFF

3) sauvegarde début du bootloader original

on alimente pas le medianav avec le 12v mais par la prise jtag en 3.3v ben faite non on alimente en 12v normal c'est plus simple pour accrocher le mode debug du µp

Télécharger :

Name : zjtag_md_29.01.2016.zip

Size : 0.35 MB

https://mega.nz/#!NVRy3aRK!c0bfLwC_qjaRFh4KV4eiL1_GXo7GzcEvrs0RFZW-bwk

zjtag -backup:custom /window:1fc00000 /length:00010000 /wiggler /port:378 /safemode /noerase /initcpu /srst /waitbrk /nocfi /fc:002 /start:1fc00000

Télécharger :

Name: CUSTOM.BIN.SAVED_64k.original.txt

Size: 0.06 MB

https://mega.nz/#!NVpRSL5K!S8S9VDZkPHpbTIEgyPrt21-oE8vGDkdzQ2WhRvLs7eI

Il va générer un fichier wholeflash.bin que l'on devra modifier.

4) modification de wholeflash.bin

Télécharger :

Name: CUSTOM.BIN.SAVED_64k.patched.rar

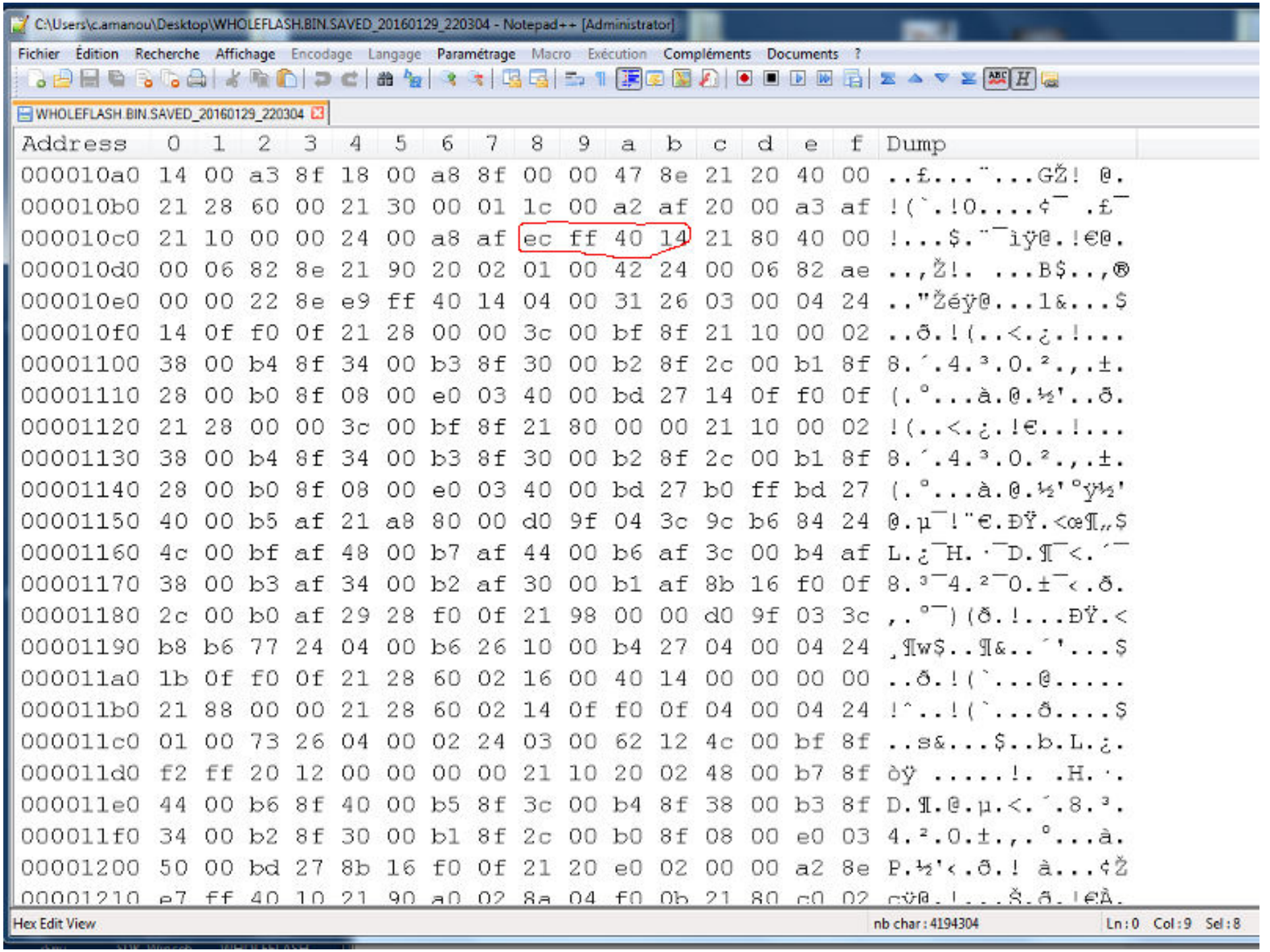
Size: 0.03 MB

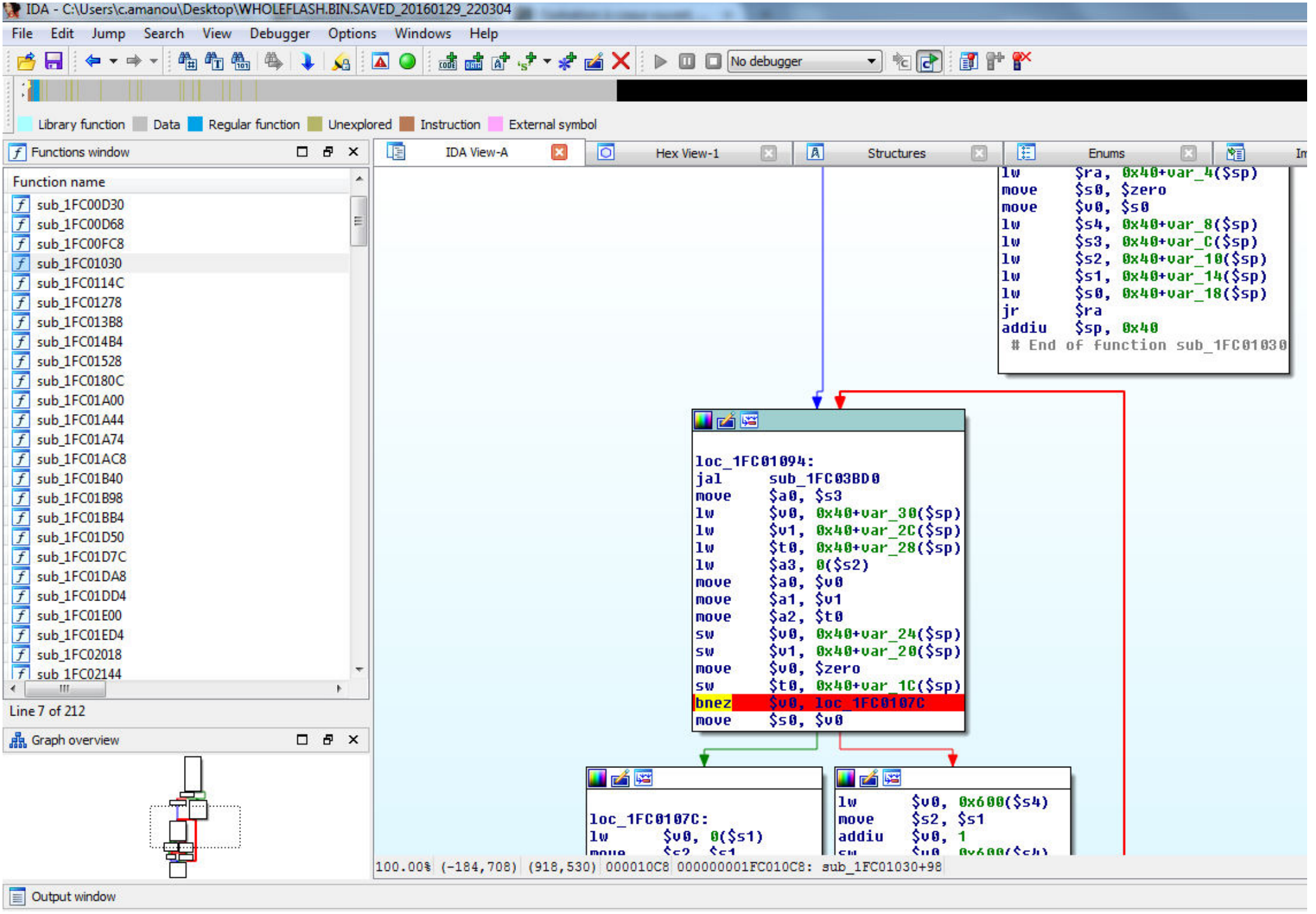
https://mega.nz/#!kBRA2Dhb!89OCBhkUcYw97FabczEp-ZRbmYFH3Qb_lGvXEwtP6xg

supprimé l'appel à une fonction en mettant le registre v0 à 0 ^^ on ouvre le fichier avec un editeur hexadecimal et on recherche E6 0C F0 0F proche de l'offset 10cc

l'Offset peu varier d'un bootloader à l'autre mais est proche de 0x10cc, on remplace donc E6 0C F0 0F move v0, zero (21 10 00 00).

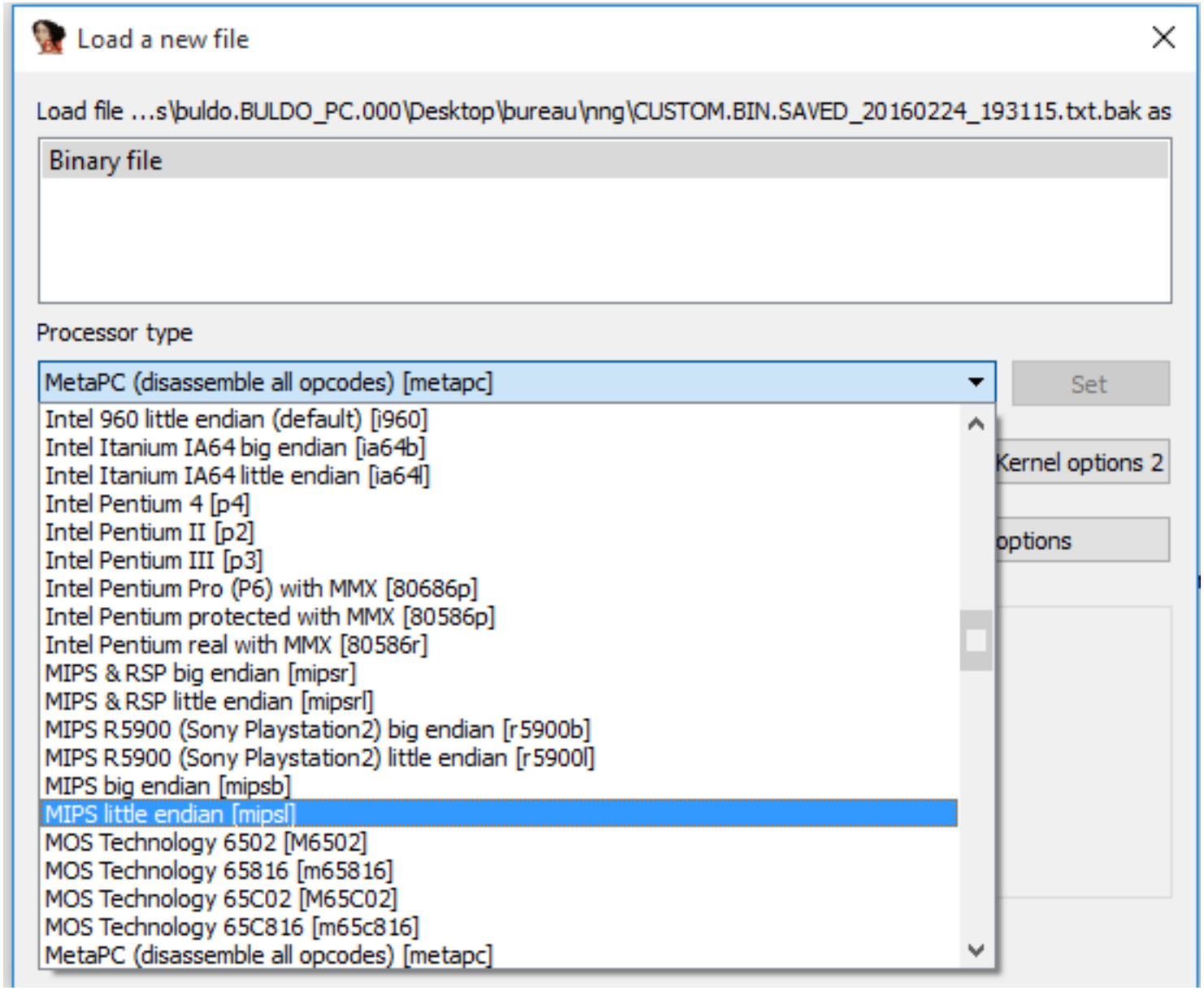
Malheureusement le code est différent suivant les versions. voici un 2ème exemple avec des valeurs différentes


C:\Users\c.amanou\Desktop\WHOLEFLASH.BIN.SAVED_20160129_220304 - Notepad++ [Administrator]
Fichier Édition Recherche Affichage Encodage Langage Paramétrage Macro Exécution Compléments Documents ?
WHOLEFLASH.BIN.SAVED_20160129_220304
Address 0 1 2 3 4 5 6 7 8 9 a b c d e f Dump
000010a0 14 00 a3 8f 18 00 a8 8f 00 00 47 8e 21 20 40 00 ..£...¨...GŽ! @.
000010b0 21 28 60 00 21 30 00 01 1c 00 a2 af 20 00 a3 af !(`.!0....¢¯ .£¯
000010c0 21 10 00 00 24 00 a8 af ec ff 40 14 21 80 40 00 !...$.¨¯ìÿ@.!€@.
000010d0 00 06 82 8e 21 90 20 02 01 00 42 24 00 06 82 ae ..‚Ž!. ...B$..,®
000010e0 00 00 22 8e e9 ff 40 14 04 00 31 26 03 00 04 24 .."Žéÿ@...1&...$
000010f0 14 0f f0 0f 21 28 00 00 3c 00 bf 8f 21 10 00 02 ..ð.!(..<.¿.!...
00001100 38 00 b4 8f 34 00 b3 8f 30 00 b2 8f 2c 00 b1 8f 8.´.4.³.0.².,.±.
00001110 28 00 b0 8f 08 00 e0 03 40 00 bd 27 14 0f f0 0f (.°...à.@.½'..ð.
00001120 21 28 00 00 3c 00 bf 8f 21 80 00 00 21 10 00 02 !(..<.¿.!€..!...
00001130 38 00 b4 8f 34 00 b3 8f 30 00 b2 8f 2c 00 b1 8f 8.´.4.³.0.².,.±.
00001140 28 00 b0 8f 08 00 e0 03 40 00 bd 27 b0 ff bd 27 (.°...à.@.½'°ÿ½'
00001150 40 00 b5 af 21 a8 80 00 d0 9f 04 3c 9c b6 84 24 @.µ¯!¨€.ÐŸ.<œ¶„$
00001160 4c 00 bf af 48 00 b7 af 44 00 b6 af 3c 00 b4 af L.¿¯H.·¯D.¶¯<.´¯
00001170 38 00 b3 af 34 00 b2 af 30 00 b1 af 8b 16 f0 0f 8.³¯4.²¯0.±¯‹.ð.
00001180 2c 00 b0 af 29 28 f0 0f 21 98 00 00 d0 9f 03 3c ,.°¯)(ð.!...ÐŸ.<
00001190 b8 b6 77 24 04 00 b6 26 10 00 b4 27 04 00 04 24 ¸¶w$..¶&..´'...$
000011a0 1b 0f f0 0f 21 28 60 02 16 00 40 14 00 00 00 00 ..ð.!(`...@.....
000011b0 21 88 00 00 21 28 60 02 14 0f f0 0f 04 00 04 24 !ˆ..!(`...ð....$
000011c0 01 00 73 26 04 00 02 24 03 00 62 12 4c 00 bf 8f ..s&...$..b.L.¿.
000011d0 f2 ff 20 12 00 00 00 00 21 10 20 02 48 00 b7 8f òÿ .....!. .H.·.
000011e0 44 00 b6 8f 40 00 b5 8f 3c 00 b4 8f 38 00 b3 8f D.¶.@.µ.<.´.8.³.
000011f0 34 00 b2 8f 30 00 b1 8f 2c 00 b0 8f 08 00 e0 03 4.².0.±.,.°...à.
00001200 50 00 bd 27 8b 16 f0 0f 21 20 e0 02 00 00 a2 8e P.½'‹.ð.! à...¢Ž
00001210 e7 ff 40 10 21 90 a0 02 8a 04 f0 0b 21 80 c0 02 çÿ@.!.. Š.ð.!€À.
Hex Edit View
nb char : 4194304
Ln : 0 Col : 9 Sel : 8

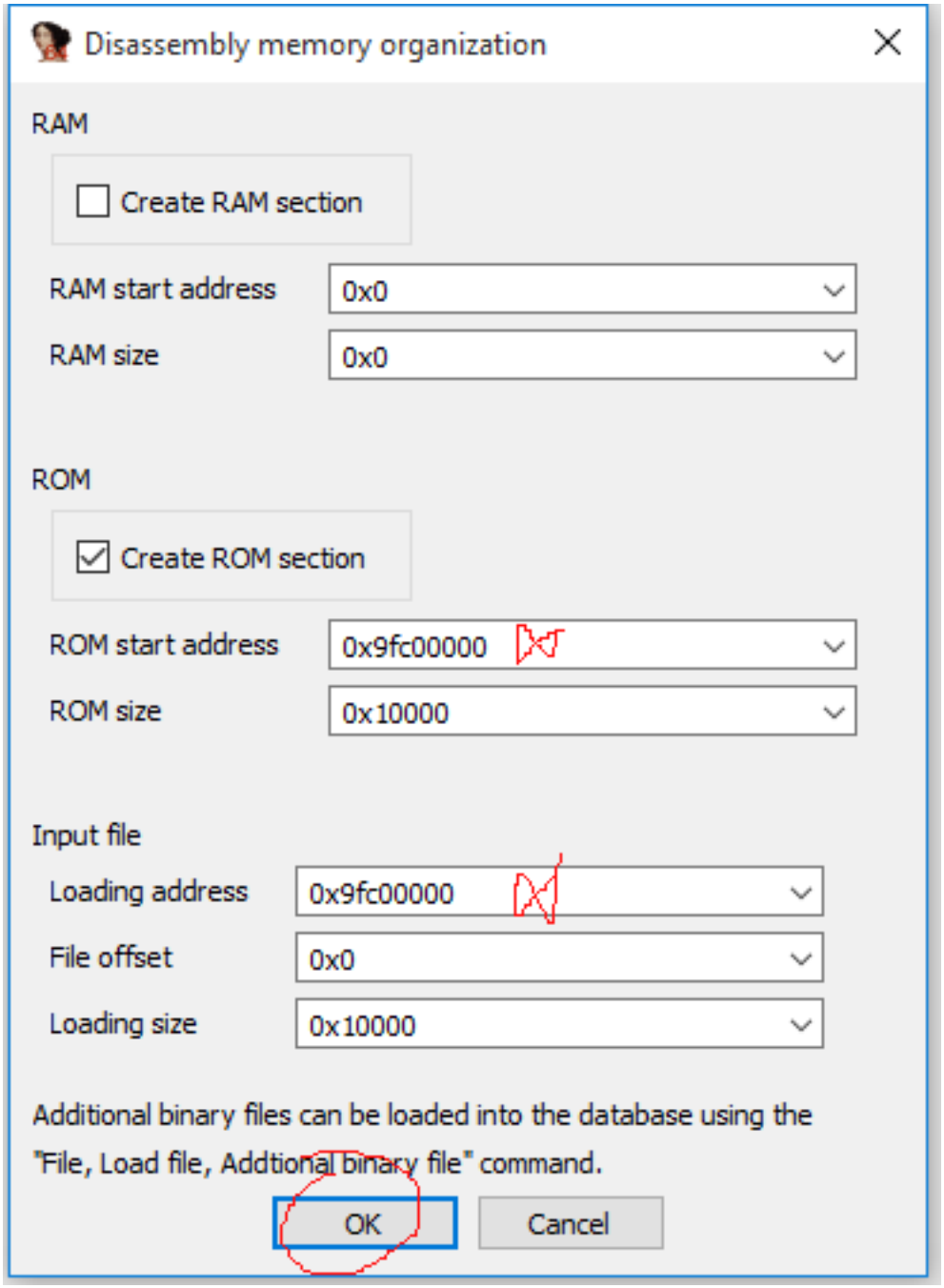

IDA - C:\Users\c.amanou\Desktop\WHOLEFLASH.BIN.SAVED_20160129_220304
File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
Function name
sub_1FC00D30
sub_1FC00D68
sub_1FC00FC8
sub_1FC01030
sub_1FC0114C
sub_1FC01278
sub_1FC013B8
sub_1FC014B4
sub_1FC01528
sub_1FC0180C
sub_1FC01A00
sub_1FC01A44
sub_1FC01A74
sub_1FC01AC8
sub_1FC01B40
sub_1FC01B98
sub_1FC01BB4
sub_1FC01D50
sub_1FC01D7C
sub_1FC01DA8
sub_1FC01DD4
sub_1FC01E00
sub_1FC01ED4
sub_1FC02018
sub_1FC02144
Line 7 of 212
Graph overview
IDA View-A
Hex View-1
Structures
Enums
lw $ra, 0x40+var_4($sp)
move $s0, $zero
move $v0, $s0
lw $s4, 0x40+var_8($sp)
lw $s3, 0x40+var_C($sp)
lw $s2, 0x40+var_10($sp)
lw $s1, 0x40+var_14($sp)
lw $s0, 0x40+var_18($sp)
jr $ra
addiu $sp, 0x40
# End of function sub_1FC01030
loc_1FC01094:
jal sub_1FC03BD0
move $a0, $s3
lw $v0, 0x40+var_30($sp)
lw $v1, 0x40+var_2C($sp)
lw $t0, 0x40+var_28($sp)
lw $a3, 0($s2)
move $a0, $v0
move $a1, $v1
move $a2, $t0
sw $v0, 0x40+var_24($sp)
sw $v1, 0x40+var_20($sp)
move $v0, $zero
sw $t0, 0x40+var_1C($sp)
bnez $v0, loc_1FC0107C
move $s0, $v0
loc_1FC0107C:
lw $v0, 0($s1)
lw $v0, 0x600($s4)
move $s2, $s1
addiu $v0, 1
100.00% (-184,708) (918,530) 000010C8 000000001FC010C8: sub_1FC01030+98
Output window

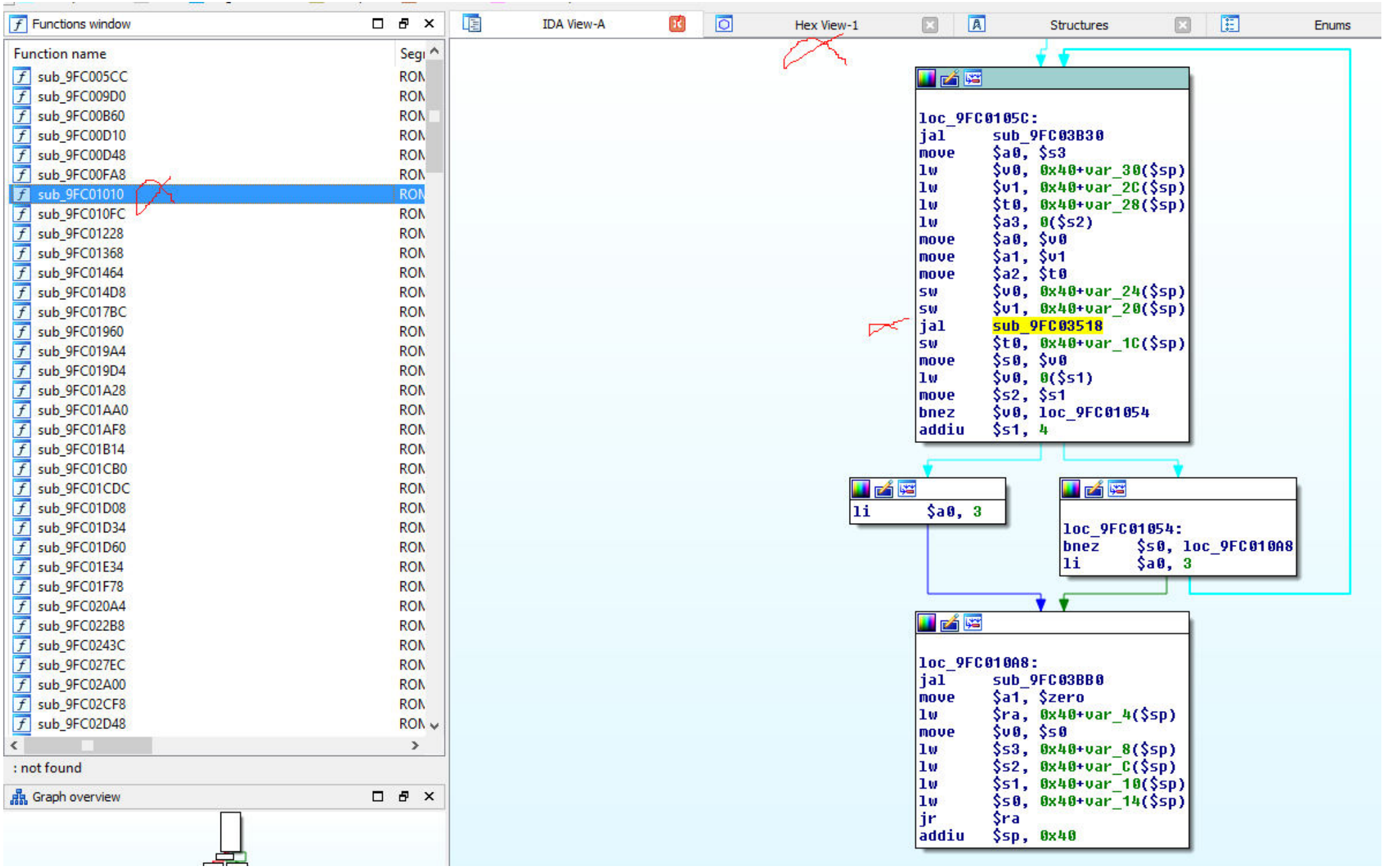
en utilisant ida :

1



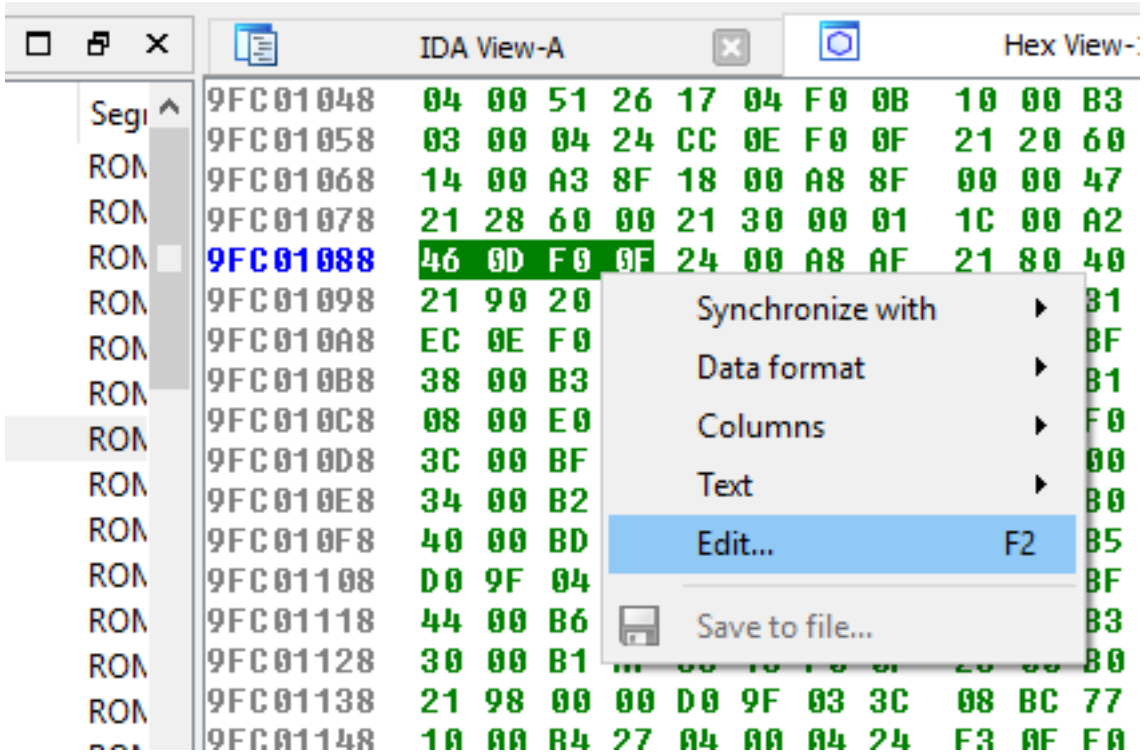
2


Disassembly memory organization
RAM
Create RAM section
RAM start address
0x0
RAM size
0x0
ROM
Create ROM section
ROM start address
0x9fc00000
ROM size
0x10000
Input file
Loading address
0x9fc00000
File offset
0x0
Loading size
0x10000
Additional binary files can be loaded into the database using the
"File, Load file, Addtional binary file" command.
OK
Cancel

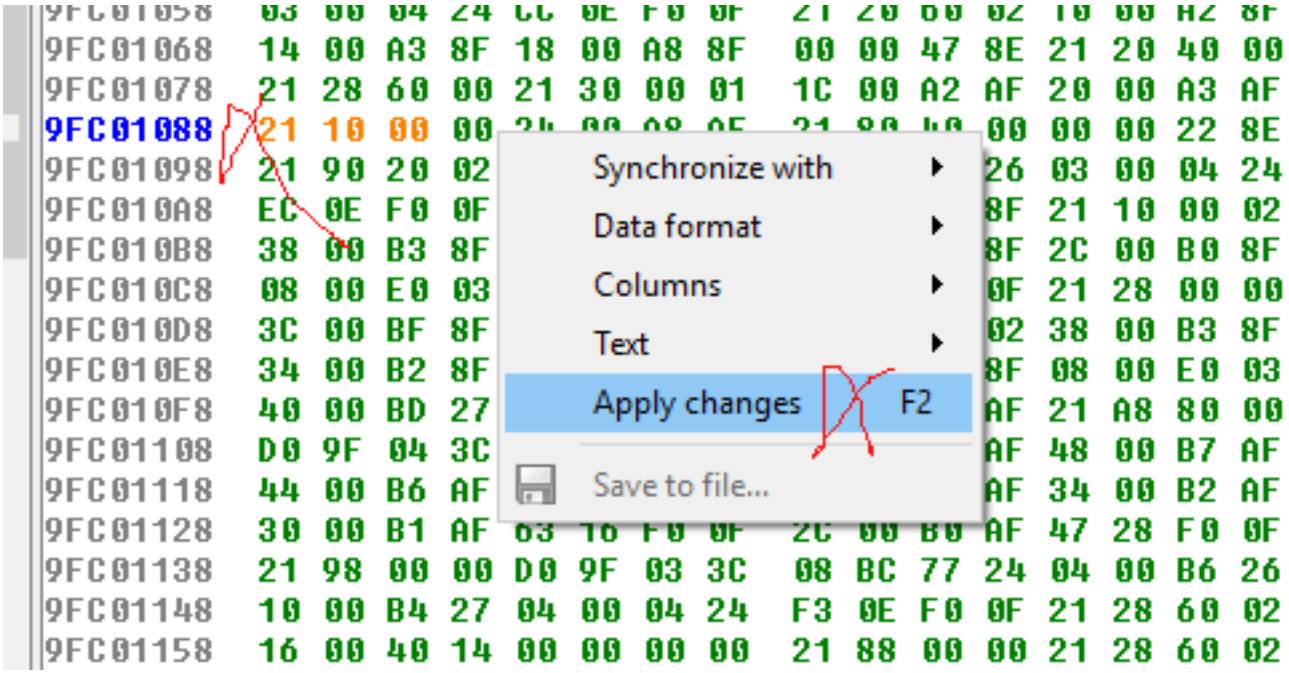

Functions window
Function name
Seg
sub_9FC005CC
sub_9FC009D0
sub_9FC00B60
sub_9FC00D10
sub_9FC00D48
sub_9FC00FA8
sub_9FC01010
sub_9FC010FC
sub_9FC01228
sub_9FC01368
sub_9FC01464
sub_9FC014D8
sub_9FC017BC
sub_9FC01960
sub_9FC019A4
sub_9FC019D4
sub_9FC01A28
sub_9FC01AA0
sub_9FC01AF8
sub_9FC01B14
sub_9FC01CB0
sub_9FC01CDC
sub_9FC01D08
sub_9FC01D34
sub_9FC01D60
sub_9FC01E34
sub_9FC01F78
sub_9FC020A4
sub_9FC022B8
sub_9FC0243C
sub_9FC027EC
sub_9FC02A00
sub_9FC02CF8
sub_9FC02D48
: not found
Graph overview
IDA View-A
Hex View-1
Structures
Enums
loc_9FC0105C:
jal sub_9FC03B30
move $a0, $s3
lw $v0, 0x40+var_30($sp)
lw $v1, 0x40+var_2C($sp)
lw $t0, 0x40+var_28($sp)
lw $a3, 0($s2)
move $a0, $v0
move $a1, $v1
move $a2, $t0
sw $v0, 0x40+var_24($sp)
sw $v1, 0x40+var_20($sp)
jal sub_9FC03518
sw $t0, 0x40+var_1C($sp)
move $s0, $v0
lw $v0, 0($s1)
move $s2, $s1
bnez $v0, loc_9FC01054
addiu $s1, 4
li $a0, 3
loc_9FC01054:
bnez $s0, loc_9FC010A8
li $a0, 3
loc_9FC010A8:
jal sub_9FC03BB0
move $a1, $zero
lw $ra, 0x40+var_4($sp)
move $v0, $s0
lw $s3, 0x40+var_8($sp)
lw $s2, 0x40+var_C($sp)
lw $s1, 0x40+var_10($sp)
lw $s0, 0x40+var_14($sp)
jr $ra
addiu $sp, 0x40

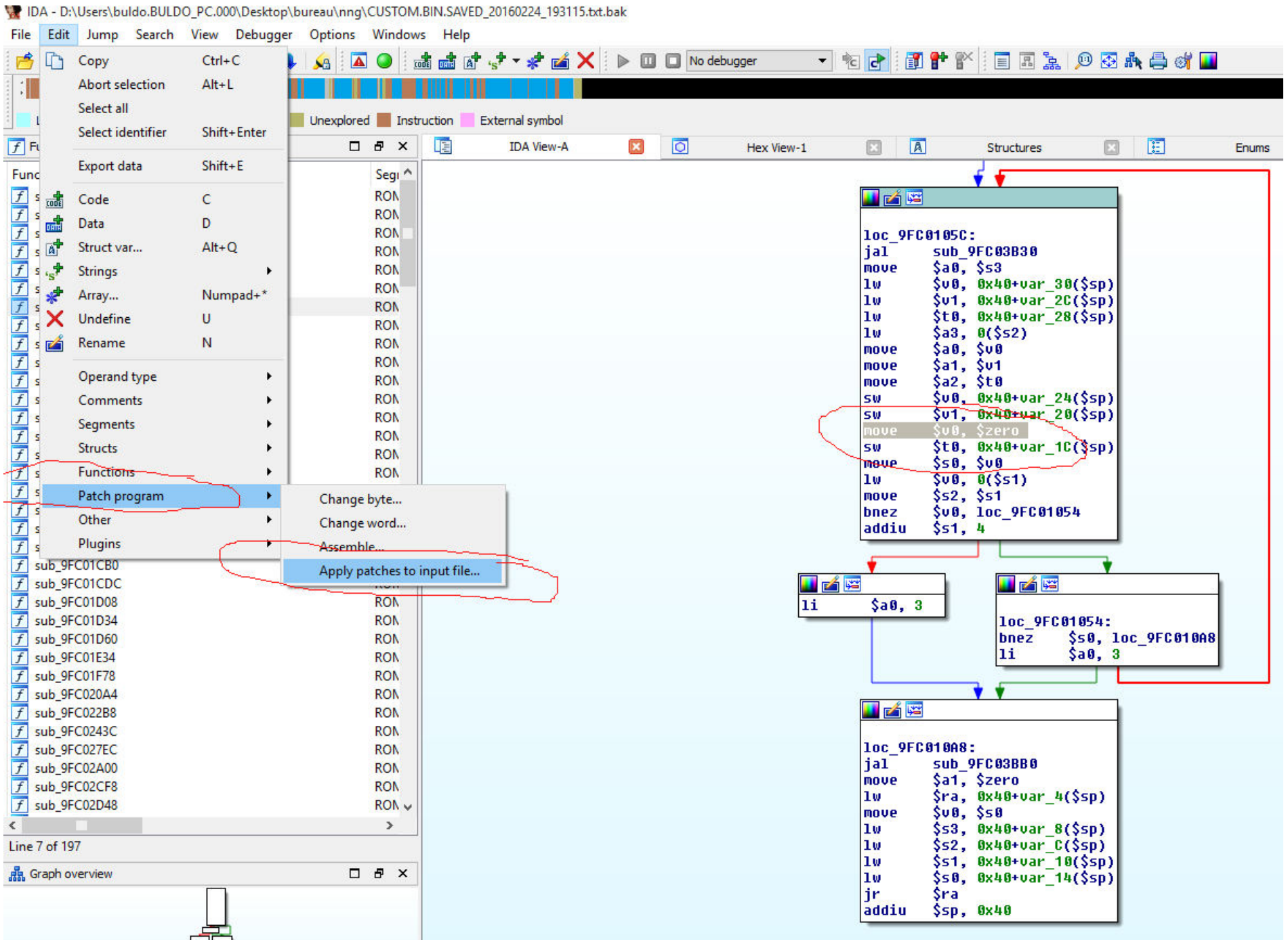
Graphique

4


IDA View-A
Hex View-
9FC01048 04 00 51 26 17 04 F0 0B 10 00 B3
9FC01058 03 00 04 24 CC 0E F0 0F 21 20 60
9FC01068 14 00 A3 8F 18 00 A8 8F 00 00 47
9FC01078 21 28 60 00 21 30 00 01 1C 00 A2
9FC01088 46 0D F0 0F 24 00 A8 AF 21 80 40
9FC01098 21 90 20
9FC010A8 EC 0E F0
9FC010B8 38 00 B3
9FC010C8 08 00 E0
9FC010D8 3C 00 BF
9FC010E8 34 00 B2
9FC010F8 40 00 BD
9FC01108 D0 9F 04
9FC01118 44 00 B6
9FC01128 30 00 B1
9FC01138 21 98 00 00 D0 9F 03 3C 08 BC 77
Synchronize with
Data format
Columns
Text
Edit... F2
Save to file...

5


9FC01068 14 00 A3 8F 18 00 A8 8F 00 00 47 8E 21 20 40 00
9FC01078 21 28 60 00 21 30 00 01 1C 00 A2 AF 20 00 A3 AF
9FC01088 21 10 00 00
9FC01098 21 90 20 02
9FC010A8 EC 0E F0 0F
9FC010B8 38 00 B3 8F
9FC010C8 08 00 E0 03
9FC010D8 3C 00 BF 8F
9FC010E8 34 00 B2 8F
9FC010F8 40 00 BD 27
9FC01108 D0 9F 04 3C
9FC01118 44 00 B6 AF
9FC01128 30 00 B1 AF
9FC01138 21 98 00 00 D0 9F 03 3C 08 BC 77 24 04 00 B6 26
9FC01148 10 00 B4 27 04 00 04 24 F3 0E F0 0F 21 28 60 02
9FC01158 16 00 40 14 00 00 00 00 21 88 00 00 21 28 60 02
Synchronize with
Data format
Columns
Text
Apply changes
F2
Save to file...


IDA - D:\Users\buldo.BULDO_PC.000\Desktop\bureau\nng\CUSTOM.BIN.SAVED_20160224_193115.txt.bak
File Edit Jump Search View Debugger Options Windows Help
Copy Ctrl+C
Abort selection Alt+L
Select all
Select identifier Shift+Enter
Export data Shift+E
Code C
Data D
Struct var... Alt+Q
Strings
Array... Numpad+*
Undefine U
Rename N
Operand type
Comments
Segments
Structs
Functions
Patch program
Other
Plugins
Change byte...
Change word...
Assemble...
Apply patches to input file...
No debugger
Unexplored Instruction External symbol
IDA View-A
Hex View-1
Structures
Enums
loc_9FC0105C:
jal sub_9FC03B30
move $a0, $s3
lw $v0, 0x40+var_30($sp)
lw $v1, 0x40+var_2C($sp)
lw $t0, 0x40+var_28($sp)
lw $a3, 0($s2)
move $a0, $v0
move $a1, $v1
move $a2, $t0
sw $v0, 0x40+var_24($sp)
sw $v1, 0x40+var_20($sp)
move $v0, $zero
sw $t0, 0x40+var_1C($sp)
move $s0, $v0
lw $v0, 0($s1)
move $s2, $s1
bnez $v0, loc_9FC01054
addiu $s1, 4
li $a0, 3
loc_9FC01054:
bnez $s0, loc_9FC010A8
li $a0, 3
loc_9FC010A8:
jal sub_9FC03BB0
move $a1, $zero
lw $ra, 0x40+var_4($sp)
move $v0, $s0
lw $s3, 0x40+var_8($sp)
lw $s2, 0x40+var_C($sp)
lw $s1, 0x40+var_10($sp)
lw $s0, 0x40+var_14($sp)
jr $ra
addiu $sp, 0x40
sub_9FC01CB0
sub_9FC01CDC
sub_9FC01D08
sub_9FC01D34
sub_9FC01D60
sub_9FC01E34
sub_9FC01F78
sub_9FC020A4
sub_9FC022B8
sub_9FC0243C
sub_9FC027EC
sub_9FC02A00
sub_9FC02CF8
sub_9FC02D48
Line 7 of 197
Graph overview

cette opération va permettre de pouvoir booter à l'aide d'une clé usb

5) effacement de la première plage mémoire

zjtag -erase:custom /window:1fc00000 /length:00010000 /wiggler /port:378 /safemode /initcpu /srst /waitbrk /nocfi /fc:002 /bypass /start:1fc00000
avant d'écrire dans la mémoire, il faut commencer par vider son contenu, c'est obligatoire. donc on efface le secteur que l'on veut réécrire

6) écriture du nouveau secteur :

renommer le fichier wholeflash.bin en custom.bin
En console administrateur
zjtag -flash:custom /window:1fc00000 /length:00010000 /wiggler /port:378 /safemode /noerase /initcpu /srst /waitbrk /nocfi /fc:002 /bypass /start:1fc00000

7) préparation de la clé usb

Pour recevoir le nk.bin pour le démarrage du système formatage fat32 + copier le nk.bin sur la clé

Reboot du médianav

8) Réparation, sauvagarde de storage card2

dans wince, démonter le 2 ème disque, faire un scan, réparer, formater, remonter
dans le menu démarrer, panneau de config, storage manager, dismount part01, properties, scan, format, remount
pendant qu'on y est on peut vérifier aussi les autres partitions.
dans le menu démarrer, panneau de config, storage manager, dismount part0x, properties, scan, remount

9) formatage et réinstallation de la partition

Recopier la sauvegarde faite sur la clé

10) reboot avec un nk.bin en 4.0.3

on place un nk.bin sur la clé usb

11) remplacement du nk.bin du medianav sur la clé usb

On recopie sur la clé celui du médianav

Ou on peut essayer celui là pour tomber sur le bureau de wince

Télécharger :

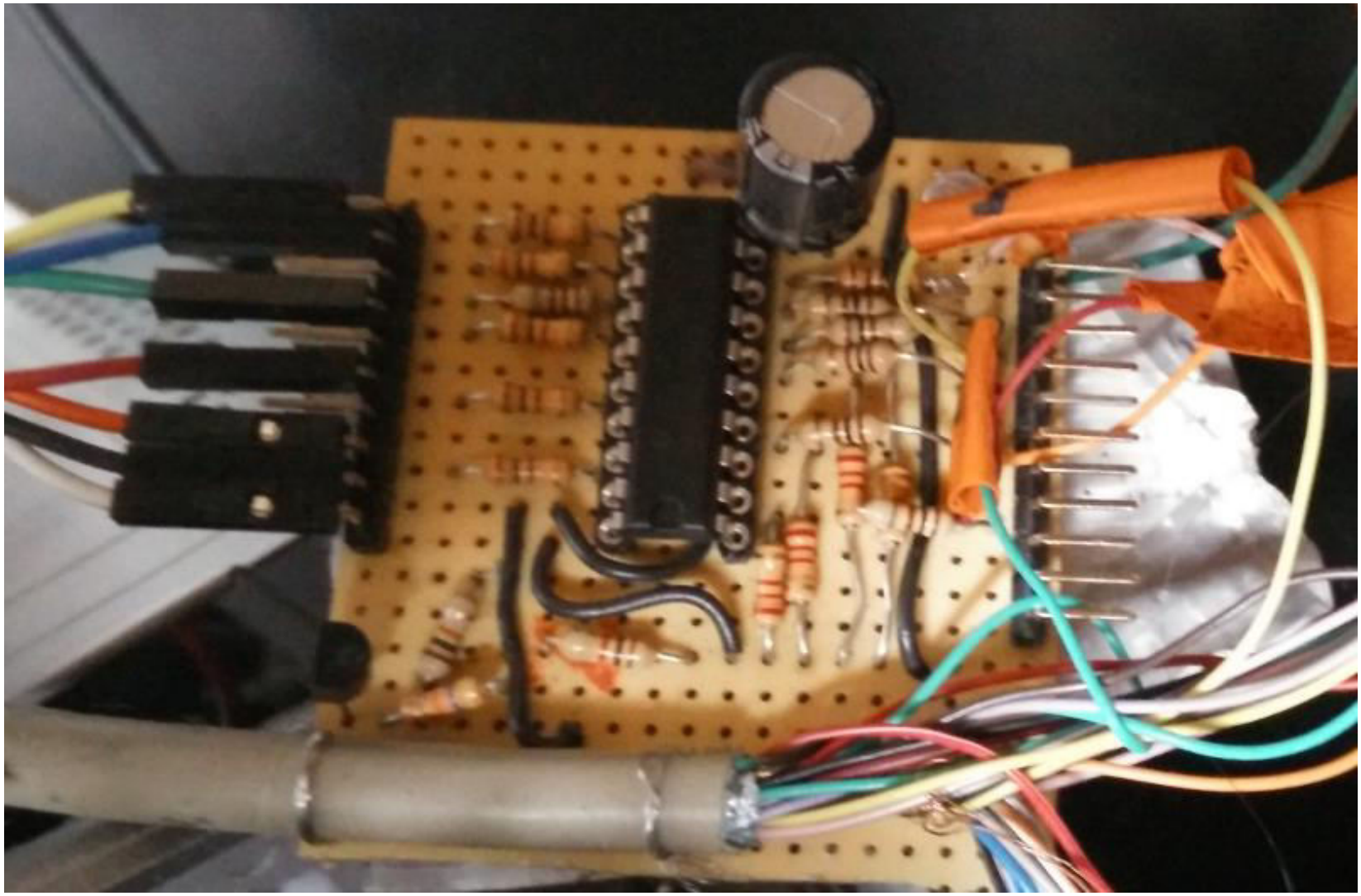
Name: NK_ulc_launcher_disable.zip

Size: 7.15 MB

https://mega.nz/#!ZZZDFJzA!W3b2eBcHBYyM1Rr-rOaDpZlEg8lSdLDpNxGsZlAQe4E

Reboot du medianav et


Version du système
01:00
Version du logiciel: 4.0.2



Donc Medianav 4.0.2 réparé

II) Annexe :

-Quelques outils pour le nk.bin

et t'a flasher quoi au juste (modifier) sur le bootloader ?
le initcpu le l'ai déjà quand au commande c'est port:378 au lieu de port:c100 qui passe

```
    ================================================
        zJTAG EJTAG Debrick Utility v1.8 RC3
    ================================================

cable=wiggler, cabletype=3
Selected port = 0x378
Detected IR chain length = 32

There are 1 device(s) in the JTAG chain
 IDCODE for device 1 is 0x00000000 (IR length:1)

Probing bus ... Done

Defined IR Length is 5 bits

CPU assumed running under LITTLE endian

CPU Chip ID: 00011000000010000000010001001001 (0x18080449)
*** Found a Raza manufactured AU1320 REV 01 CPU ***

  - EJTAG IMPCODE ..... : 00100000010000000100000000000000 (0x20404000)
  - EJTAG Version ..... : 2.5
  - EJTAG DMA Support ... : No
  - EJTAG Implementation flags: R4k ASID_8 NoDMA MIPS32
```

Issuing Processor / Peripheral Reset ... Done
Enabling Memory Writes ... Skipped
Halting Processor ... <Processor Entered Debug Mode!> ... Done
Clearing Watchdog ... Done
Loading CPU Configuration Code ... Done
*** Manually Selected a MX29LV320ET 2Mx16 TopB (4MB) from Macronix

- Flash Chip Window Start .... : 1FC00000
- Flash Chip Window Length ... : 00400000
- Selected Area Start ..... : 1FC00000
- Selected Area Length ..... : 00010000

*** You Selected to Backup the CUSTOM.BIN ***
==========
Backup Routine Started
==========

Saving CUSTOM.BIN.SAVED_20160116_222951 to Disk...
3% bytes = 2320

Télécharger :
Name : zjtag_md_29.01.2016.zip
Size : 0.35 MB
https://mega.nz/#!NVRy3aRK!c0bfLwC_qjaRFh4KV4eiL1_GXo7GzcEvrs0RFZW-bwk
Name : binmod_patched.zip
Size : 27.54 ko
https://mega.nz/#!oUxGEAoJ!8lb9xEwg4gm83uKFUjAtEbm4VRchaRU3ZAAApfyjGDQ
Name : bump_rom.rar
Size : 79 ko
https://mega.nz/#!REYHTQJI!zVqW_O3_K77rWVHIHePF3gB3qEht_hwyKp1wcFUh36s