Custom Rom

- Custom BlackView BV4800
- Modification LK.bin to erease Orange state and confirmation boot

Custom BlackView BV4800

Lets modify file in ROM

Installa Magiskboot

https://aur.archlinux.org/packages/magiskboot-bin

```
yay -S magiskboot-bin
```

Change picture on boot

download file from rom like boot.bin , vbmeta.bin , super.bin

use command to unpack file

```
magiskboot unpack magisk_patched-26100_biB8t.img
```

use command to repack file

```
magiskboot repack magisk_patched-26100_biB8t.img
```

Composition ROM BV4800

├── boot_a.bin
├── boot_b.bin
├── boot_para.bin

```
├── dtbo_a.bin
├── dtbo_b.bin
├── expdb.bin
├── flashinfo.bin
├── frp.bin
├── gpt_backup.bin
├── gpt.bin
├── gz_a.bin
├── gz_b.bin
├── init_boot_a.bin
├── init_boot_b.bin
├── lk_a.bin
├── lk_b.bin
├── logo.bin
├── md1img_a.bin
├── md1img_b.bin
├── md_udc.bin
├── metadata.bin
├── nvcfg.bin
├── nvdata.bin
├── nvram.bin
├── otp.bin
├── para.bin
├── persist.bin
├── proinfo.bin
├── protect1.bin
├── protect2.bin
├── scp_a.bin
├── scp_b.bin
├── sec1.bin
├── seccfg.bin
├── spmfw_a.bin
├── spmfw_b.bin
├── sspm_a.bin
├── sspm_b.bin
├── super.bin
├── tee_a.bin
├── tee_b.bin
├── vbmeta_a.bin
├── vbmeta_b.bin
├── vbmeta_system_a.bin
├── vbmeta_system_b.bin
├── vbmeta_vendor_a.bin
├── vbmeta_vendor_b.bin
├── vendor_boot_a.bin
└── vendor_boot_b.bin
```

++ user_data.bin

Fichier du firmware --> super.bin

Fichier gestion des erreur green / yellow / orange /red --> lk_a.bin

Modification firmware --> super.bin

la modification et le flash de de ce fichier ne reset pas le tel

on peut modifier le fichier avec nan oet le flash direct sans crash

Modification Erreur state --> lk_a.bin

Si on modifier le fichier cela empêche le téléphone de boot correctement

il faut donc le modifier avec délicatesse

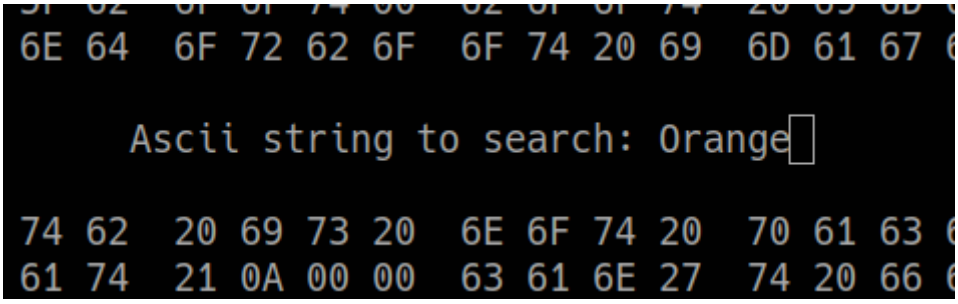
Si on suit a la lettre ce poste on peut le modifier

https://www.hovatek.com/forum/thread-31664.html

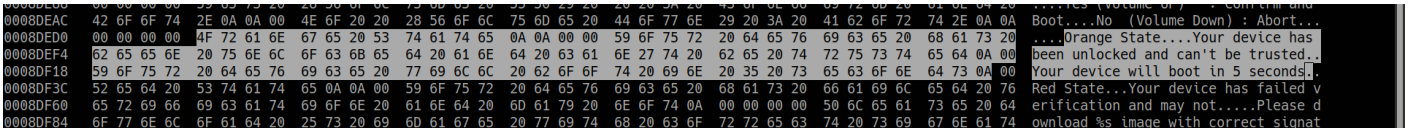
Retirer Orange State :

```
hexedit lk_a.bin
```

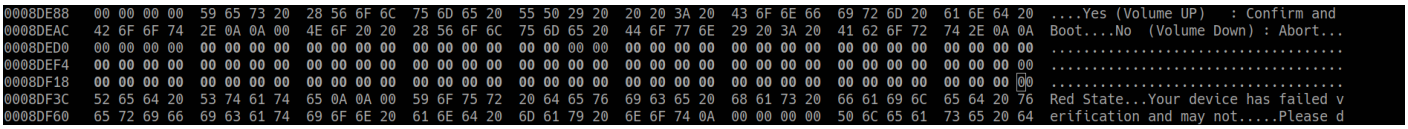
Utiliser la touche "tab" pour passer du coté ASCII faire une recherche avec la touche "/" et recherche le mot "Orange" puis entré pour confimé.



Supprimé la notification de l'erreur Orange State en remplacent l'hexa du text par des 0



comme ceci.



Enregistré avec CTR+X et yes

Flash avec MTKclient le nouveau fichié lk_a.bin

```
python mtk w lk_a lk_a.bin
```

reboot le tel

```
python mtk reset
```

rechherche d'hexa correspond a laction

08 B5 D8 B1 03 68 1B 68 02 2B

ligne : 00042D74 -->

08 B5 0E 4B 7B 44 1B 68 1B 68 02 2B

nouveau demandé -->

08B5002008BD1B681B68022B

test un a un : 08B50E4B08BD1B681B68022B

08BD--> cliqué sur power off cela va directement reboot le téléphone

test un a un : 08B500207B441B681B68022B

0020 --> si on remplace seulement dans tout les cas après 5sec le tel s'éteint meme si click power off

test un a un : 08B5000000001B681B68022B

00000000 --> le tel setein a 5sec sauf si click power off

test un a un : 08B5000008BD1B681B68022B

000008BD --> cliqué sur power off cela va directement reboot le téléphone

test un a un : 08B5002000001B681B68022B

00200000 --> le tel setein a 5sec sauf si click power off

test un a un : 08B50E4B00001B681B68022B

0E4B0000 --> le tel setein a 5sec sauf si click power off

test un a un : 08B50E4B00BD1B681B68022B

0E4B00BD -->le tel setein a 5sec

test un a un : 08B50E4B08001B681B68022B

0E4B0800 -->le tel setein a 5sec sauf si click power off

test un a un : 08B5002008001B681B68022B

00200800 -->le tel setein a 5sec sauf si click power off

test un a un : 08B5002000BD1B681B68022B

002000BD -->le tel setein a 5sec

test un a un : 08B500207BBD1B681B68022B

00207BBD -->le tel setein a 5sec

test un a un : 08B5002008441B681B68022B

00200844 -->le tel setein a 5sec sauf si click power off

test un a un : 08B5002000441B681B68022B

00200044 -->le tel setein a 5sec sauf si click power off

test un a un : 08 B5 0E 4B 7B 00 00 00 00 00 02 2B

test un a un : 08 B5 0E 4B 00 00 00 00 00 00 02 2B

test un a un : 08 B5 0E 00 00 00 00 00 00 00 02 2B

test un a un : 08 B5 00 00 00 00 00 00 00 00 02 2B

test un a un : 08 B5 00 00 00 00 00 00 00 00 00 00

test un a un : 08B5002008BD1B681B68012B

ouverture du fichier super

ligne original

```
    # Disable dm-verity hash prefetching, since it doesn't help performance
    # Read more in b/136247322
    write /sys/module/dm_verity/parameters/prefetch_cluster 0
```

ligne modifier

```
    # Disable dm-verity hash prefetching, since it doesn't help performance
    # Read more in b/136247322
    write /sys/module/dm_verity/parameters/prefetch_cluster 1
```

ligne original

```
  # Load trusted keys from dm-verity protected partitions
    exec -- /system/bin/fsverity_init --load-verified-keys
```

ligne modifier

```
  # Load trusted keys from dm-verity protected partitions
  #exec -- /system/bin/fsverity_init --load-verified-keys
```

ligne original

```
# Update dm-verity state and set partition.*.verified properties.
    verity_update_state
```

ligne modifier

```
# Update dm-verity state and set partition.*.verified properties.
#    verity_update_state
```

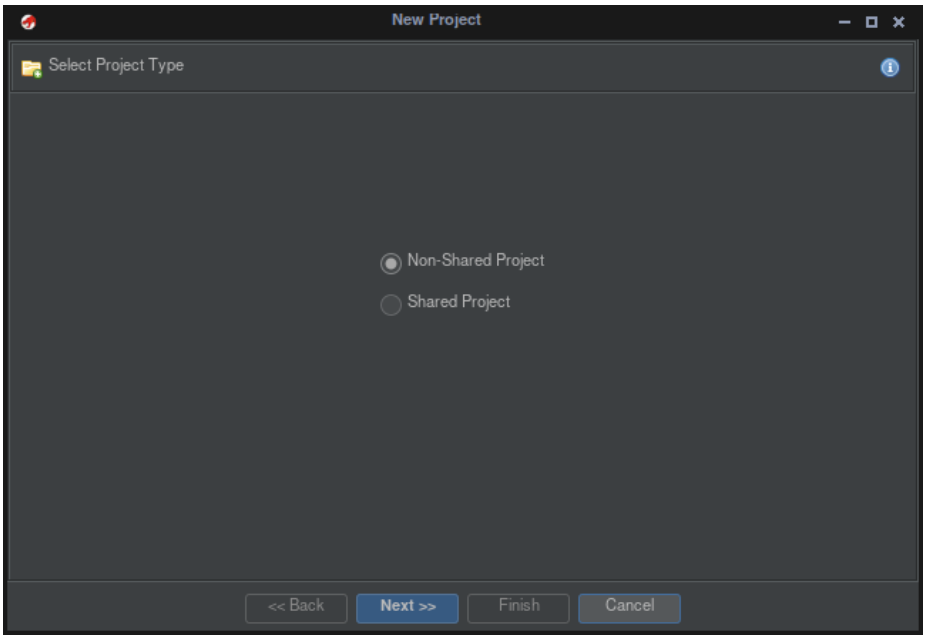
Modification LK.bin to erease Orange state and confirmation boot

Bypass Confirmation Boot

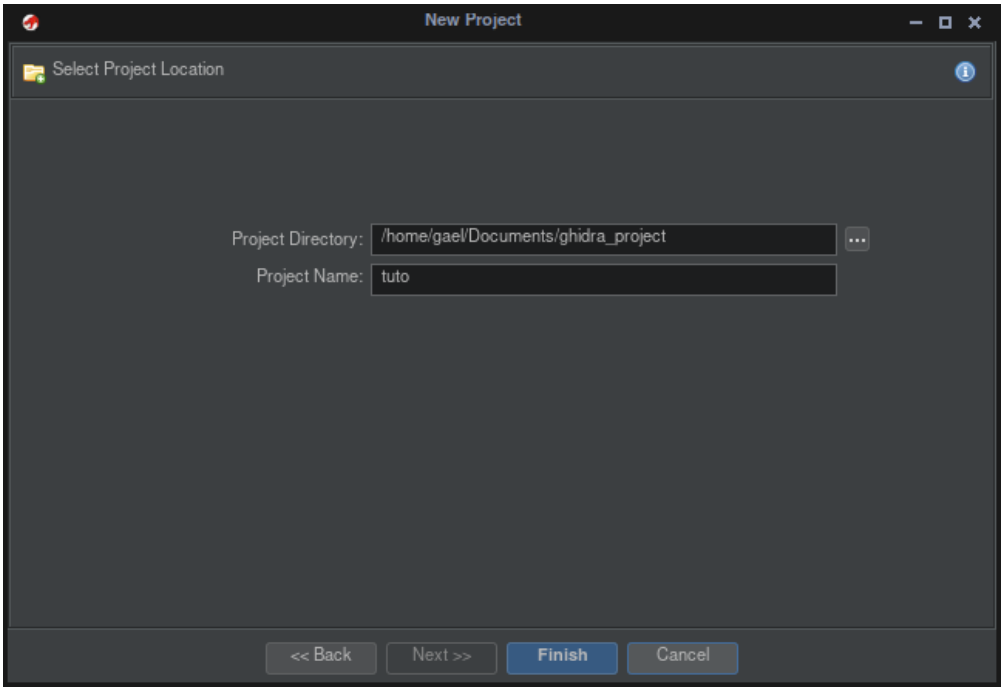
> Tool necessary : Ghidra
> Download and install here : https://github.com/NationalSecurityAgency/ghidra

Open file lk.bin in Ghidra

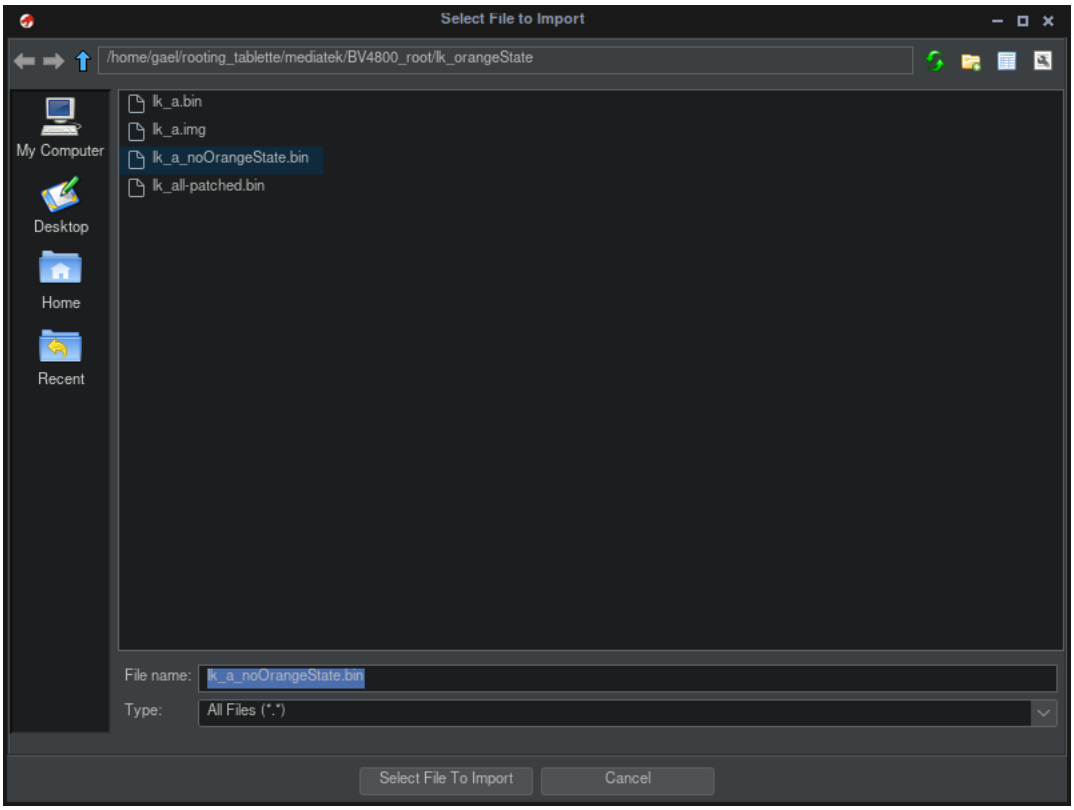
- File --> new project
- Non-Shared Project --> Next



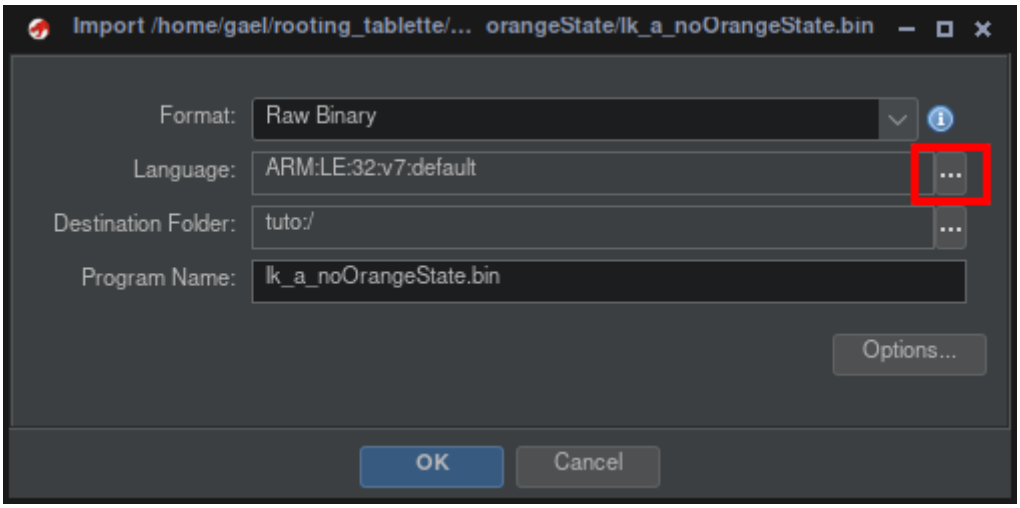
- Give a name to your project --> Next

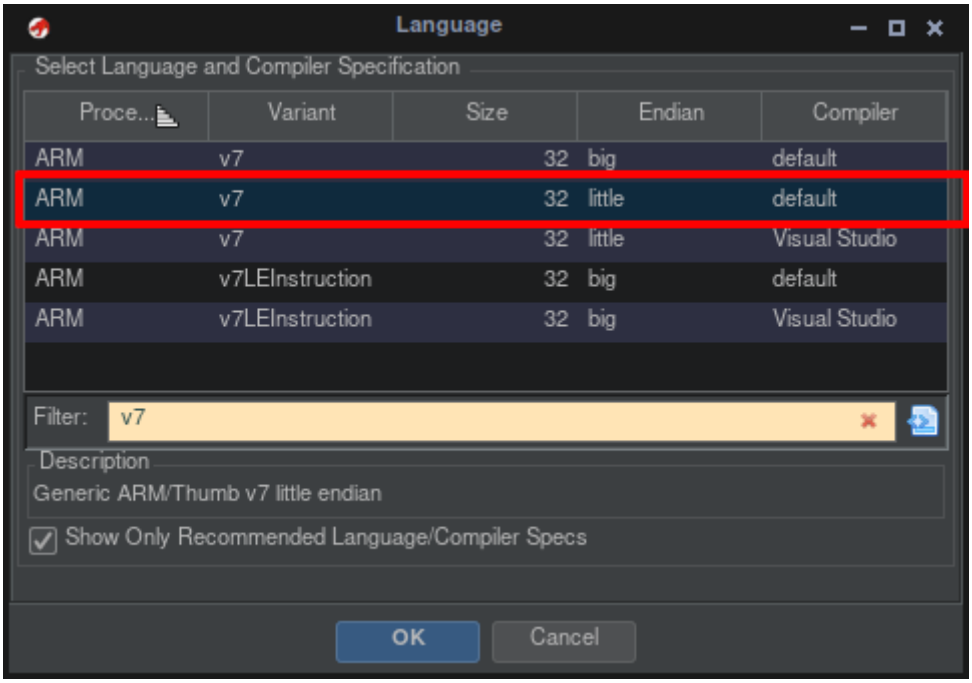


- File --> import File
- Import File lk.bin you want patch

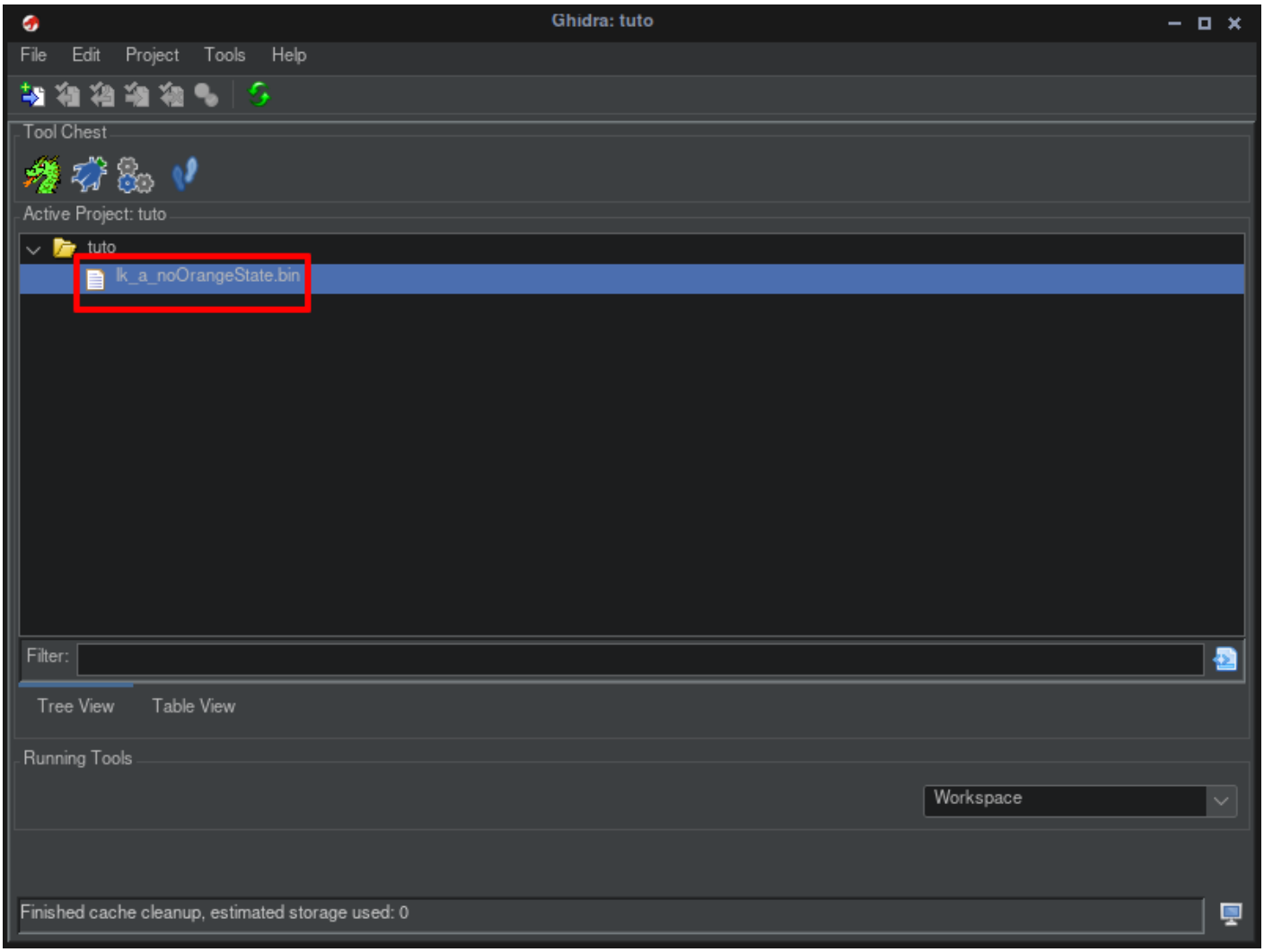


- Select Langage --> ARM v7 | 32 | little | default

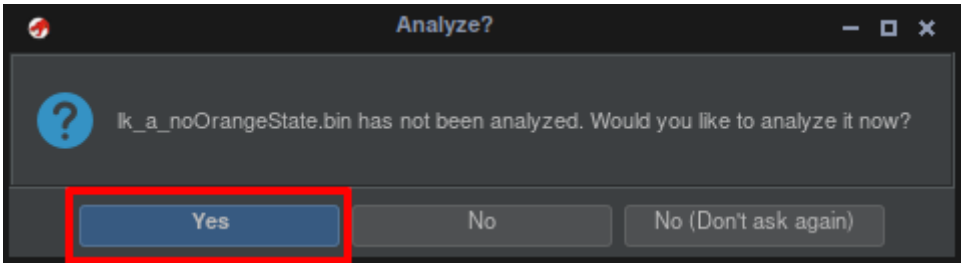




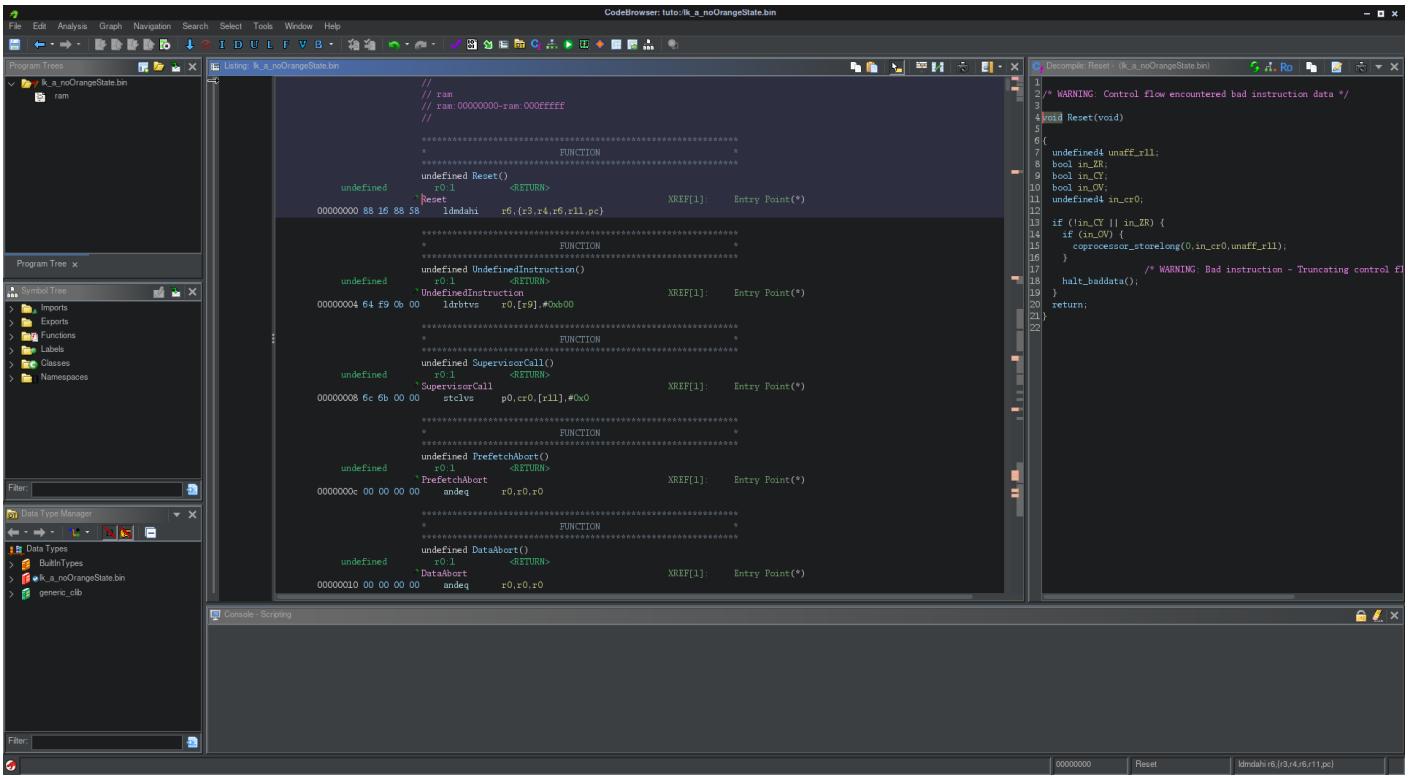
- Double click on file



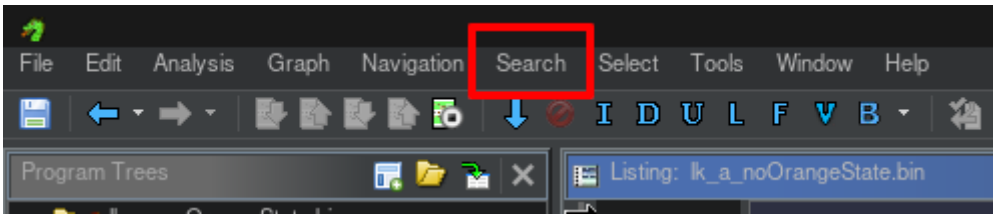
- respond yes to analyzed



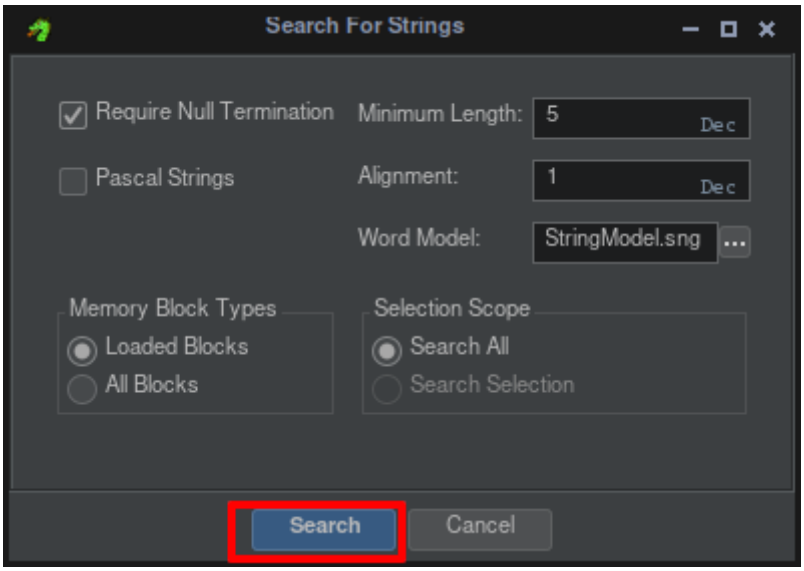
- We will get



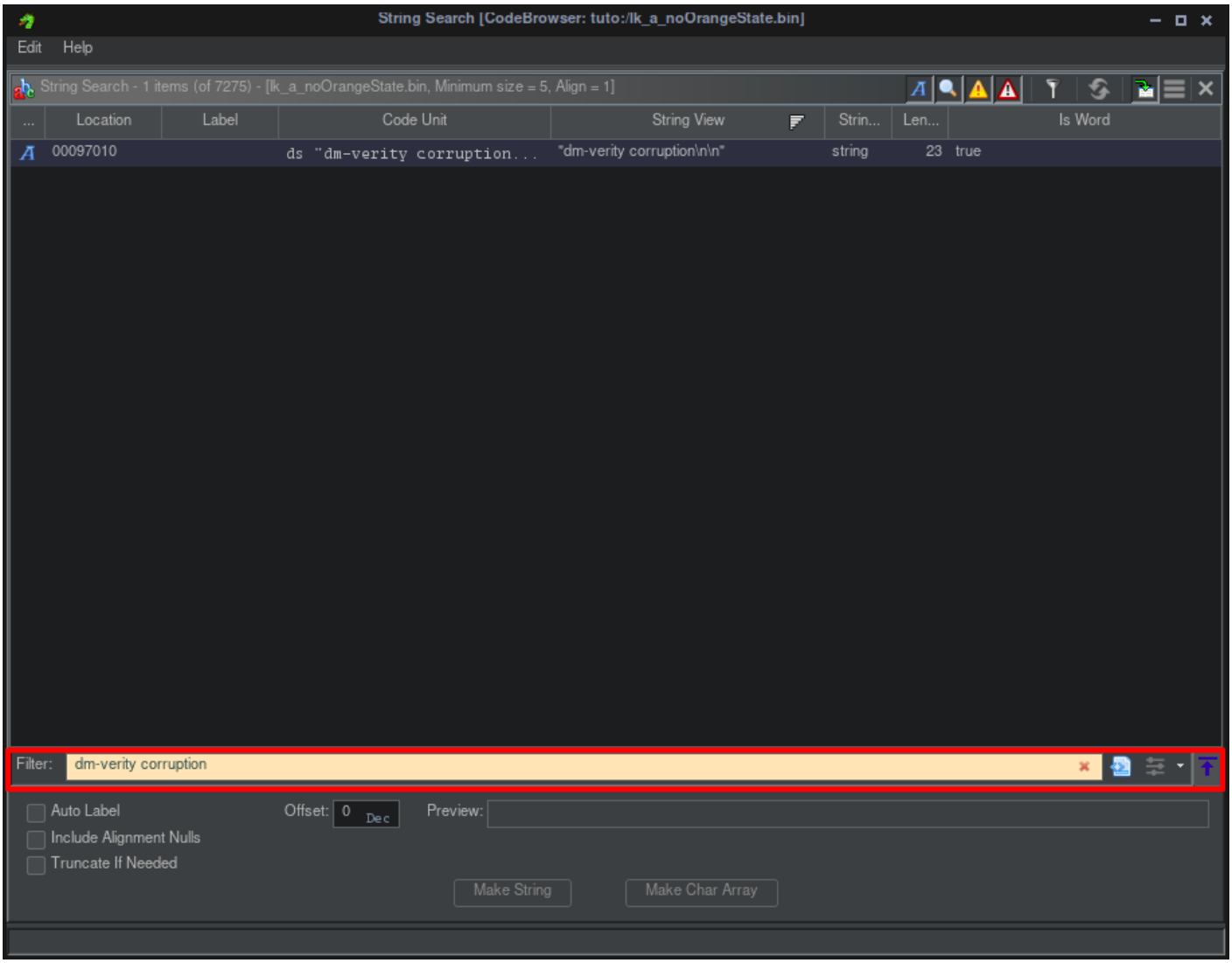
- Search --> for String



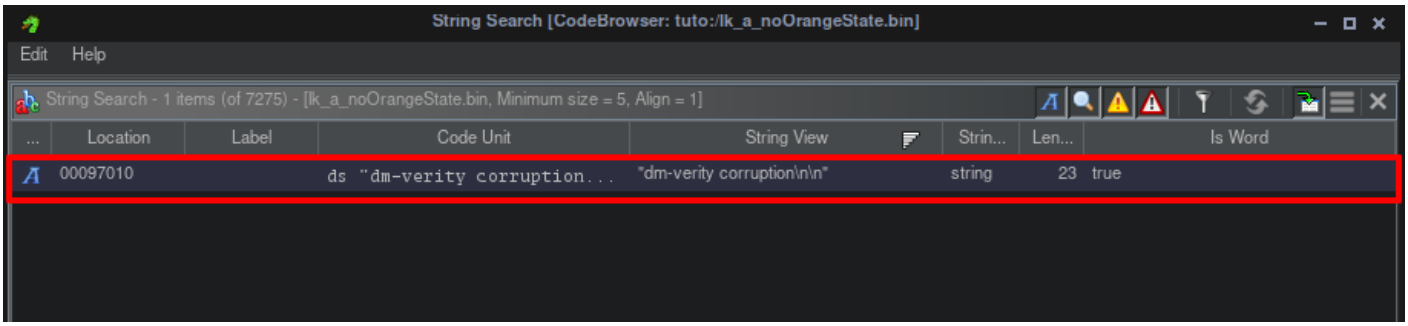
- continue with clicking on Search



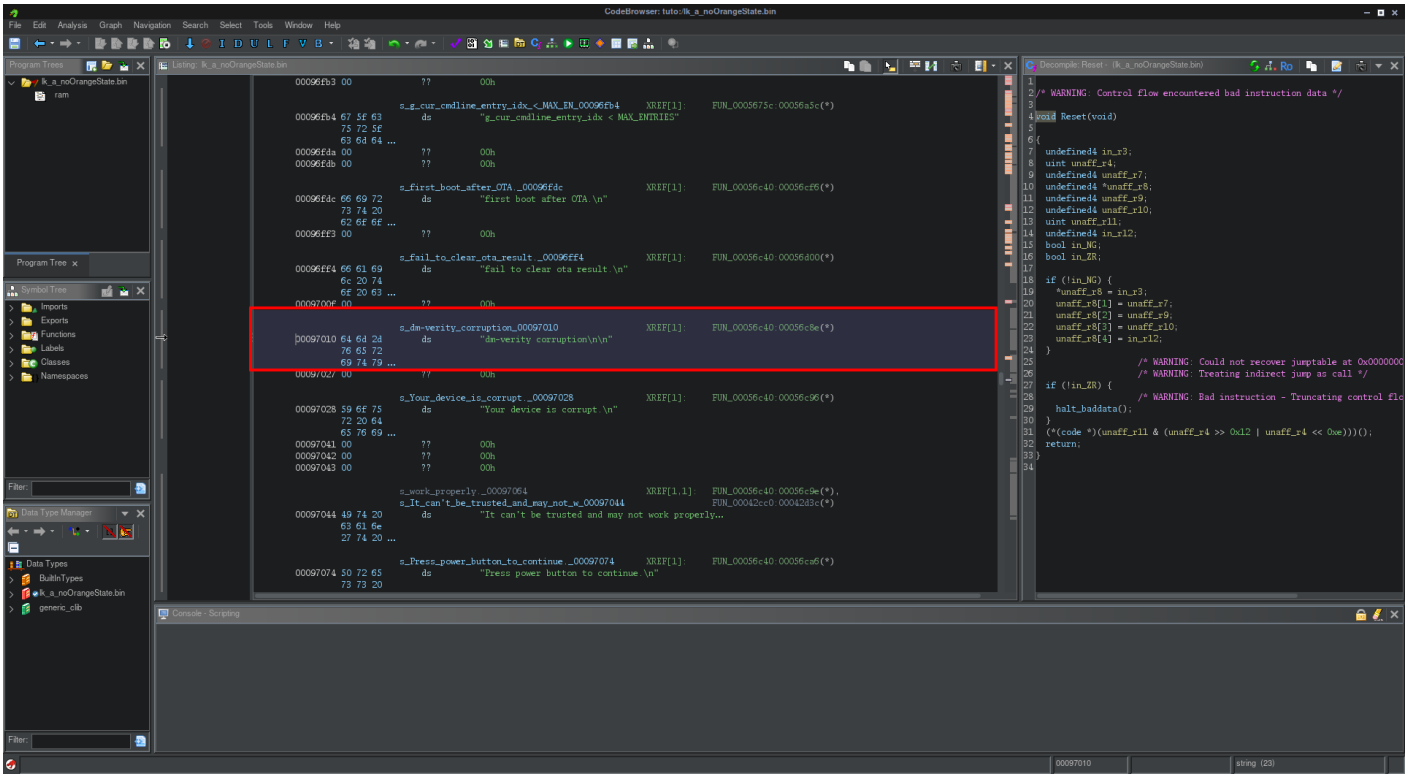
- type "dm-verity corruption" on filter



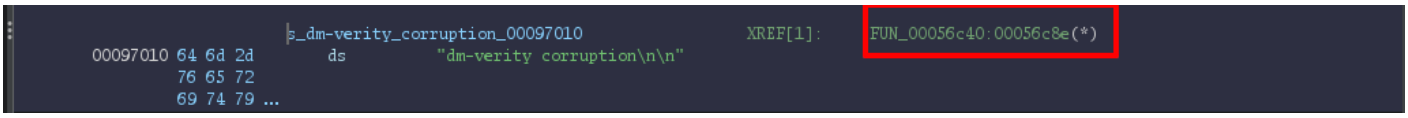
- One final will find --> click on line find



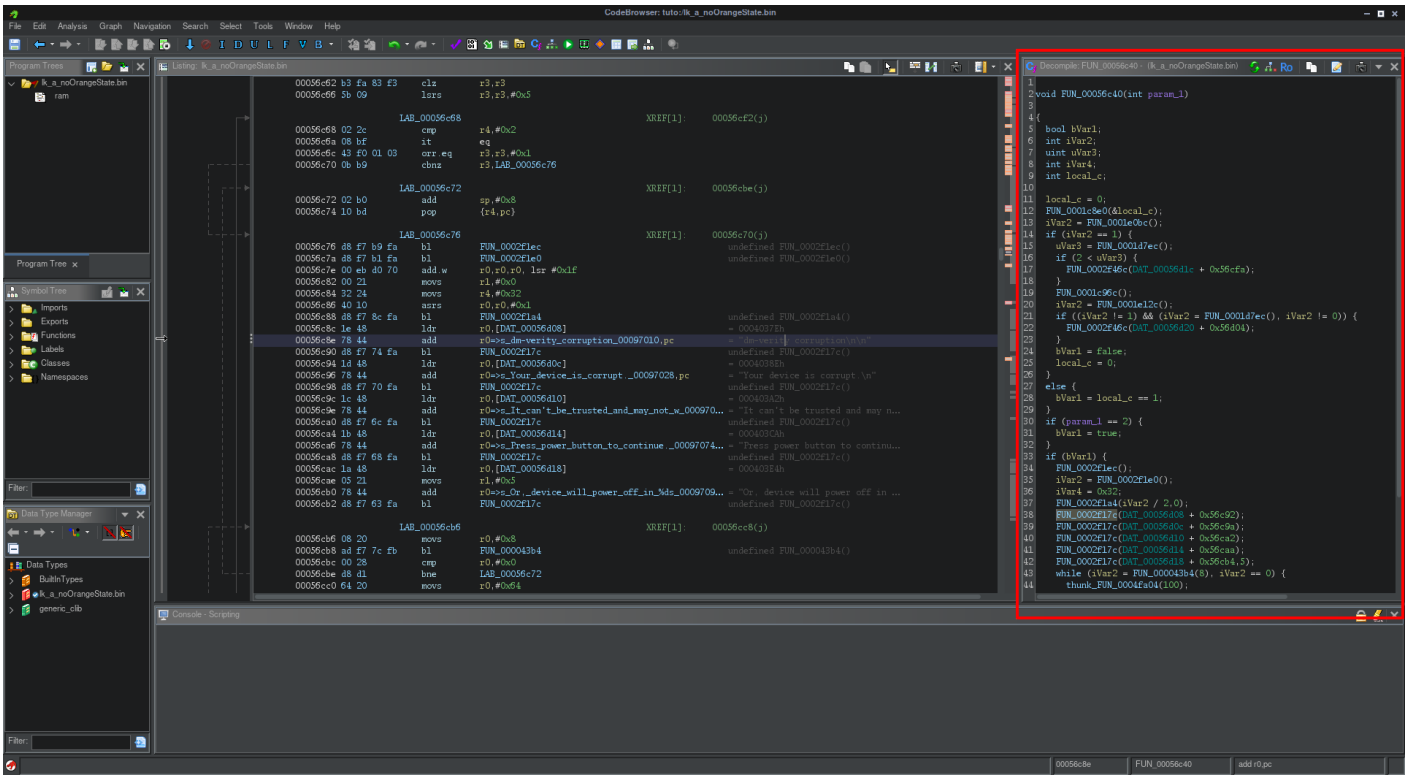
- this will give



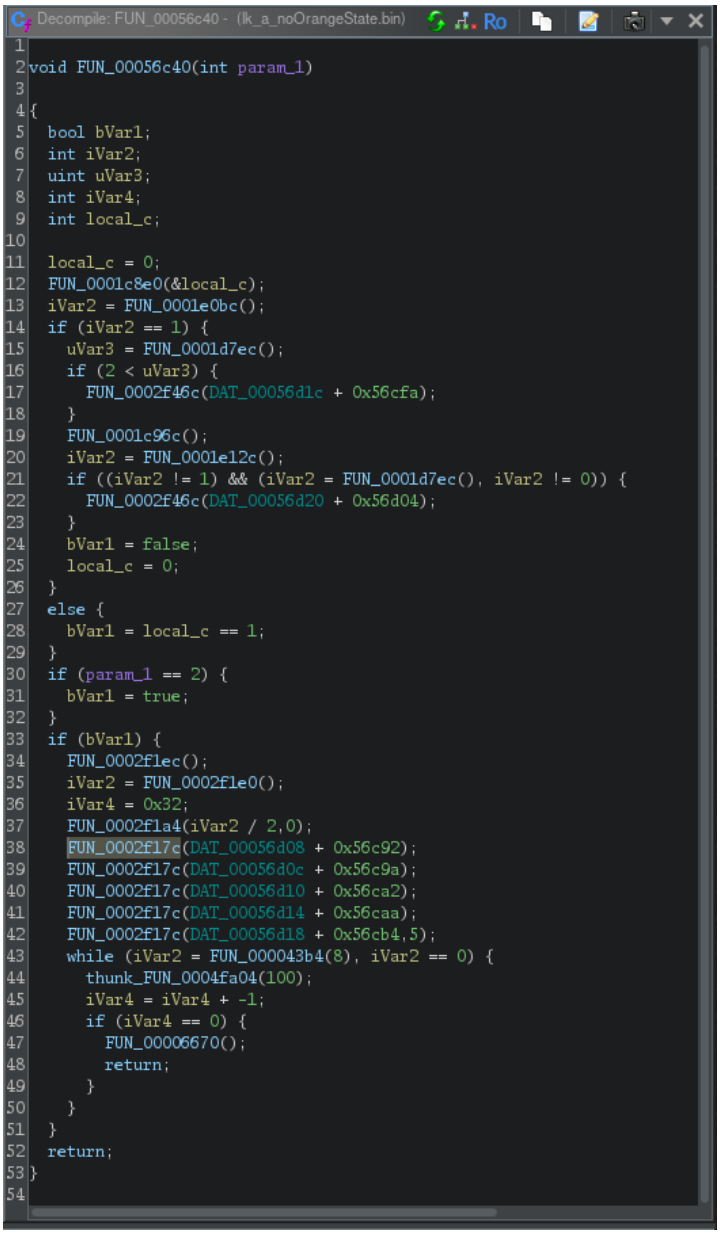
- Go to the fonction who call the string "dm-verity corruption" with double click on hexa (FUN_00056c40:00056c8e)



- This will give



- We get the fonction we need on right



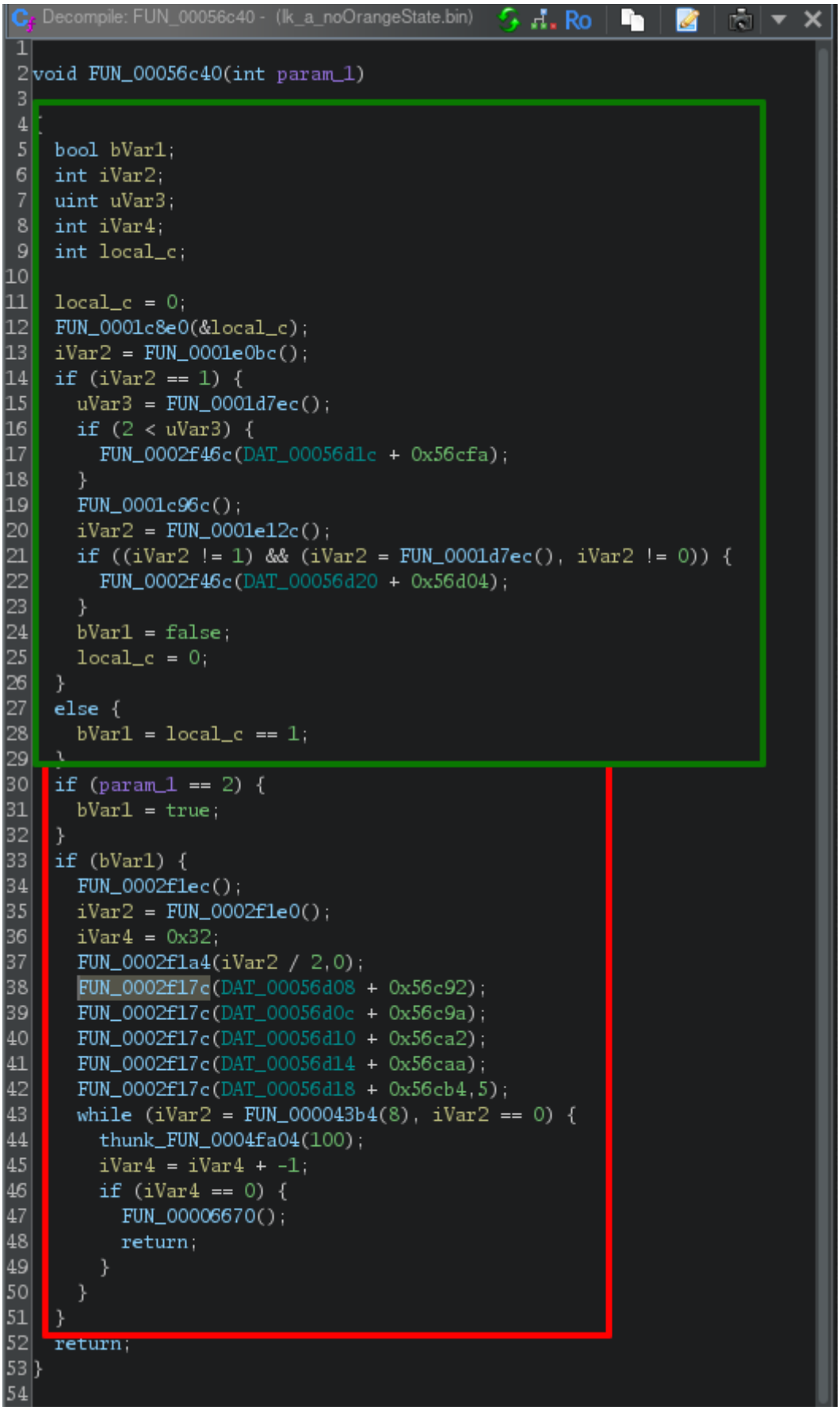
- The fonction who call string dm-verity is highlighted

```
FUN_0002f17c(DAT_00056d08 + 0x56c92);
```

- We can understand if the boot not start correctly

the var `param_1 == 2` and give `bVar1 = true;`

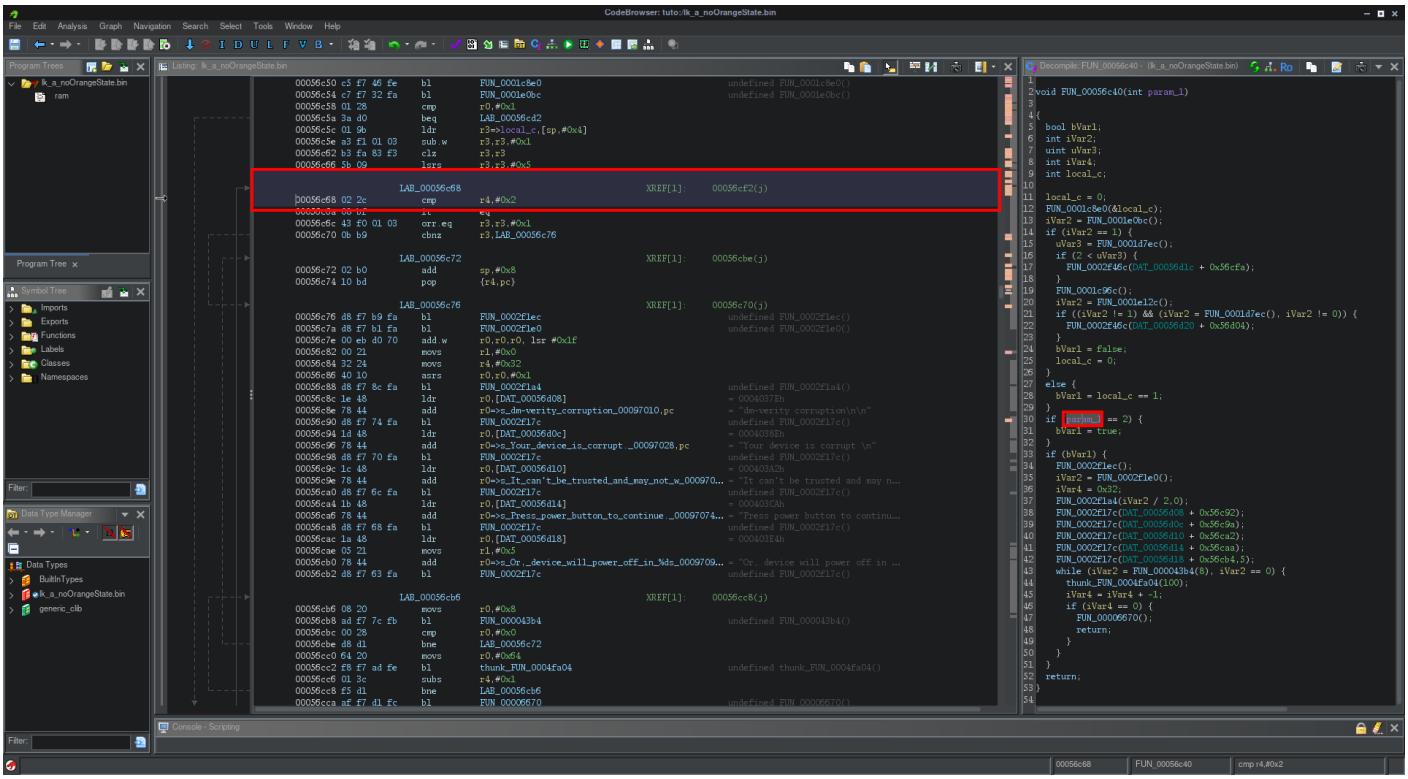
so the first an green is if boot is corectly and an red if we got an error



- We therefore need to modify one of these variables so that it is no longer used in the function.

`param_1 == 2` or `bVar1 = true;`

- In the function, if we click on the desired variable, we move to the line where it is in the file.



- Right Click on line --> Patch instruction
- Change value of condition

```
                    LAB_00056c68                                    XREF[1]:     00056cf2(j)
00056c68 02 2c          cmp         r4,#0x2
```

- We can do like this

```
                    LAB_00056c68                                    XREF[1]:     00056cf2(j)
00056c68 05 2c          cmp         r4,#0x5
```

```
if (param_1 == 5) {
  bVar1 = true;
}
```

- After this we can save file quit

- For export with menu project
- Right click on file --> select export
- You can choose Format Original File

Find the warning string

https://github.com/R0rt1z2/lkpatcher

https://lkpatcher.r0rt1z2.com/

https://blog.r0rt1z2.com/patch-mediatek-bootloader-images-lk.html