FIRMWARE HACKING,

SLASH +he PINEAPPLE FOR FUN

by @smrx86

Bali, 22 September 2015

We believe protecting the information security of our customers is our key contribution in making the world a safer place for global collaboration

www.noosc.co.id

Graha Mandiri, 2nd floor
Jl. Imam Bonjol No. 61
Jakarta, 10310, Indonesia
Phone: +62 21-39833771

Firmware Hacking

(maybe)

“an act to customizing firmware content that later have to rewrite/flash into rom memory of related devices”

noosc

Firmware Hacking

(maybe)

“an act to customizing firmware content that later have to rewrite/flash into rom memory of related devices”

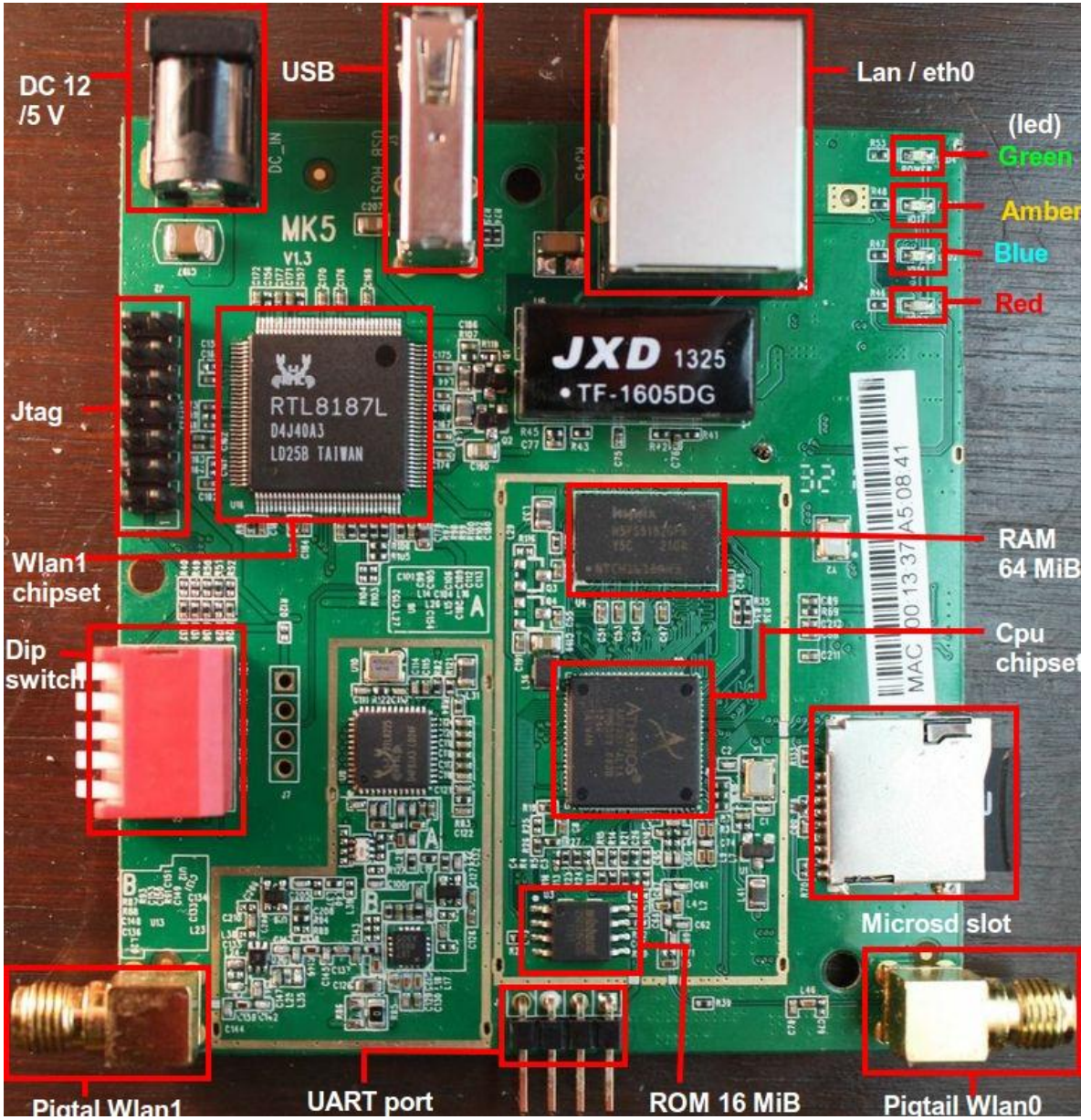
noosc

Firmware Hacking

noosc

Pineapple mk 5

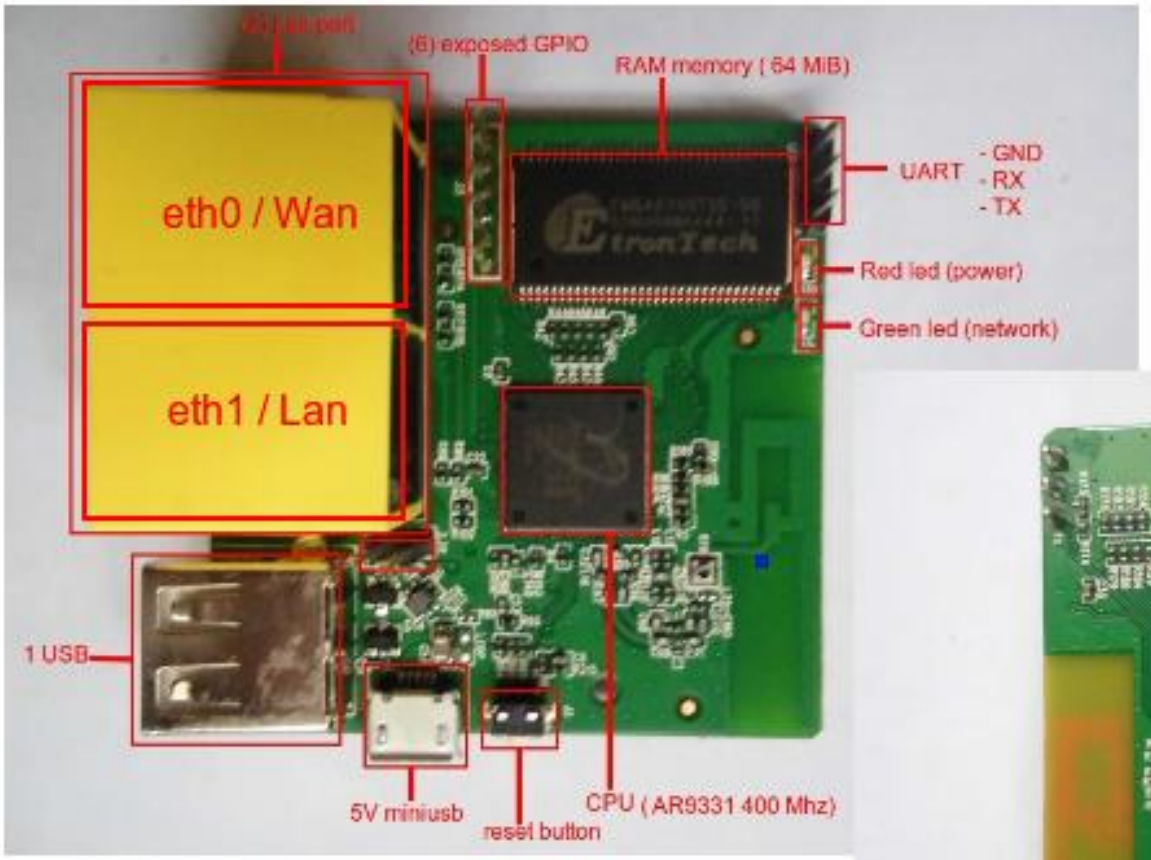
(router 4 hacking)

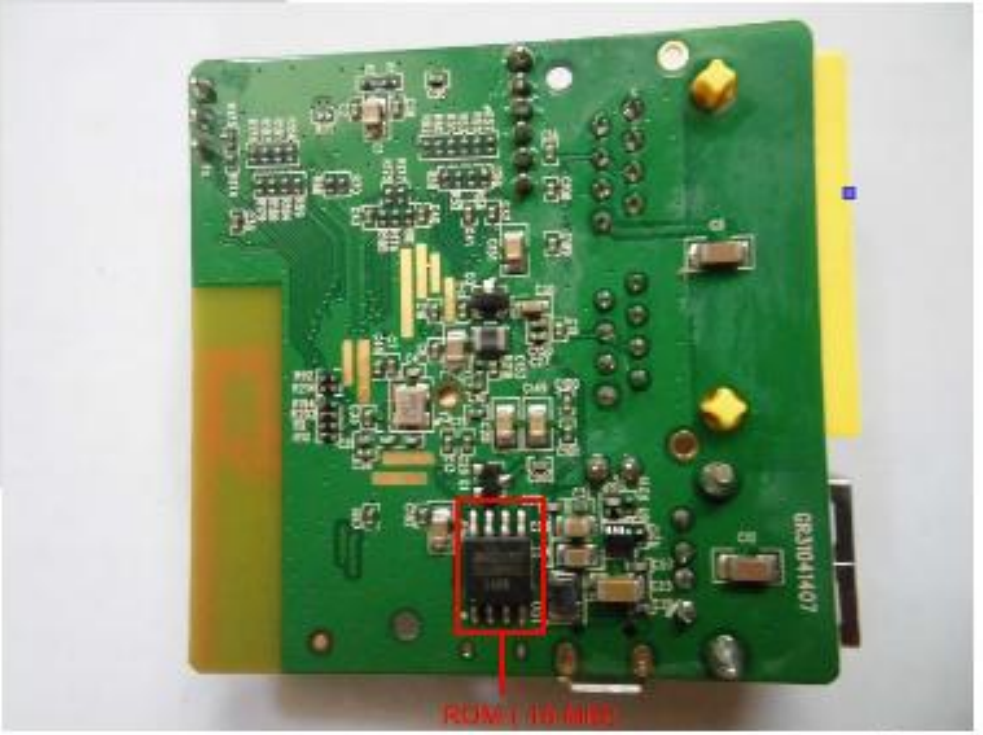


noosc

GL-inet

(just 3g home router)





noosc

The steps

RECONNAISSANCE

EXTRACTING

SORTING & FIND UNIQUE FILE

DEBUGGING

EXPLOITATION

REPACKING

noosc

The Tools

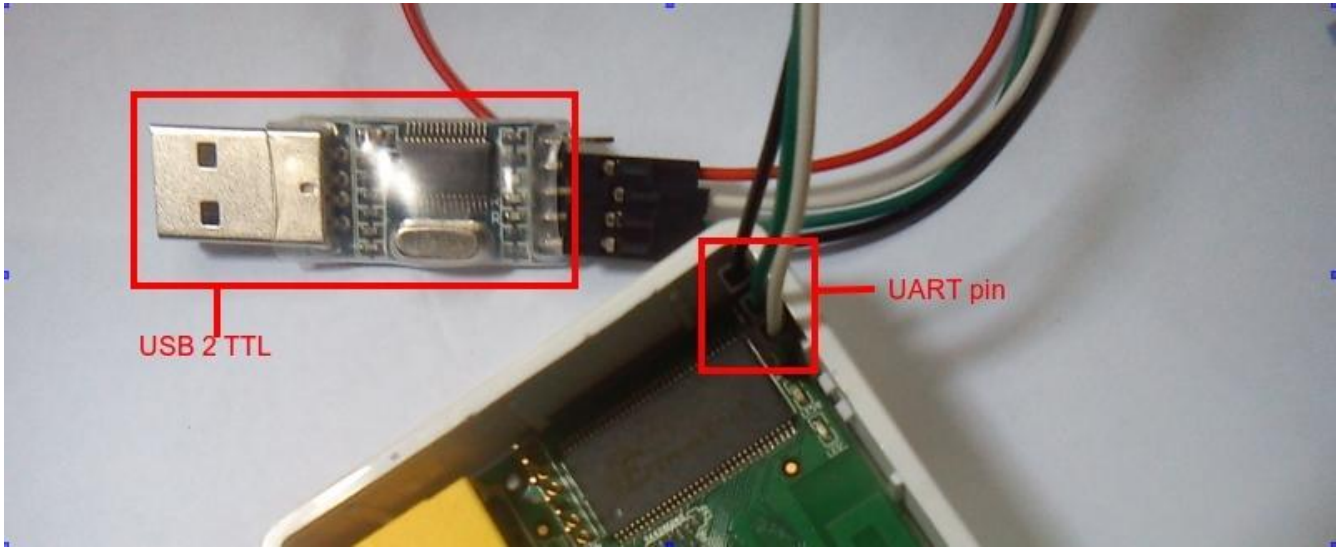
- Binwalk 2.1.0

*(analysis = good, unpack/repack = bad)

- Firmware mod kit

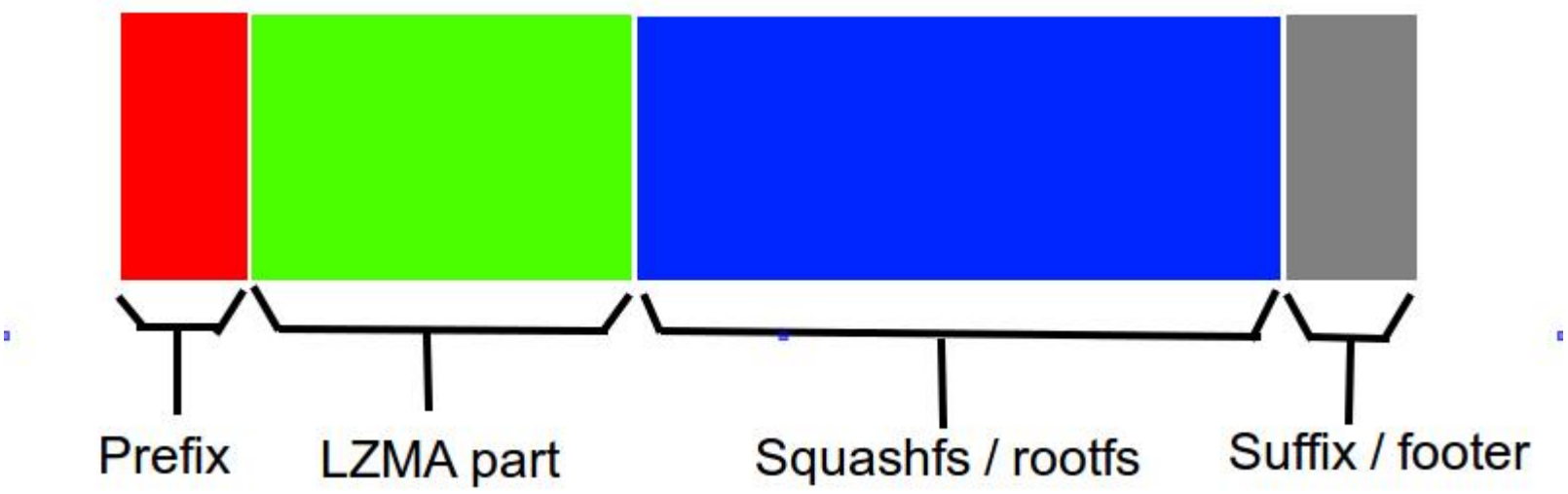
*(analysis = bad, unpack/repack =good)

- Usb2TTL dongle *(ur safenet)



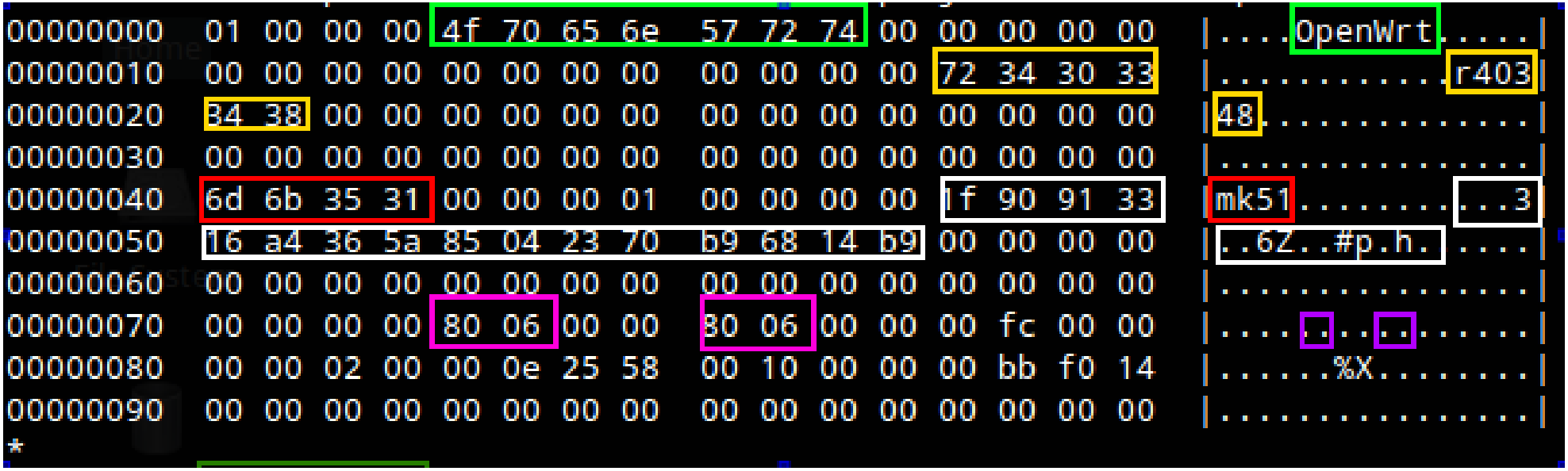
noosc

Openwrt Firmware



noosc

Prefix content



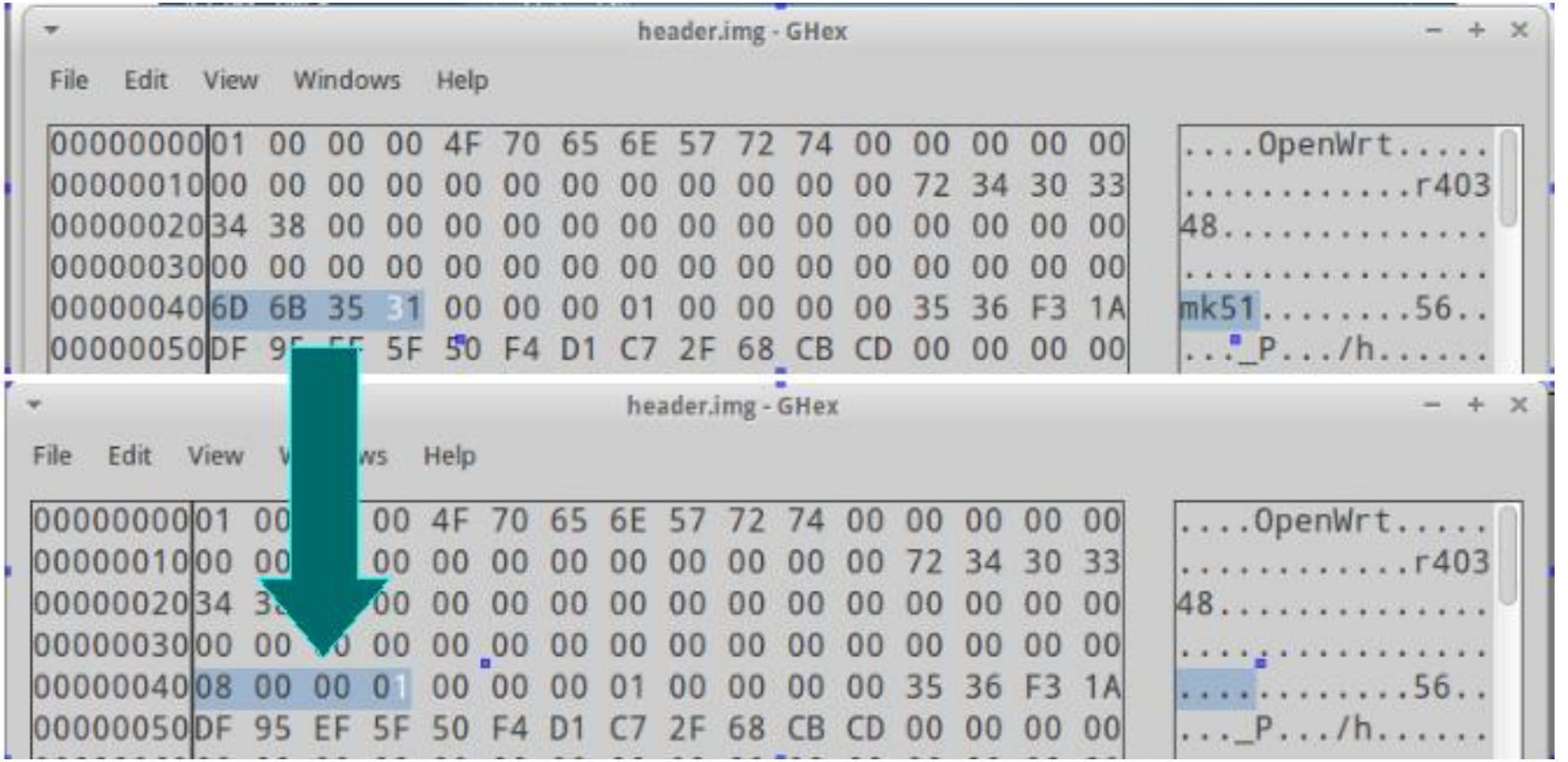
Vendor Name
Firmware version
Hardware_id

MD5SUM
Kernel_la
Kernel_ep

noosc

Debugging

- Change Hardware_id first (prefix)



* change value 0x0040 from 6D6B3531 to 08000001

noosc

Debugging

Is there any protection???

noosc

Debugging

- Trace the protection script

$ grep -lr -e 'wrong pattern entered' *

includes/welcome/welcome.inc.php

```
190  function verifyPineapple($post)
191  {
192      $action_array = array('off', 'on', 'blink');
193      if (isset($_SESSION['verify_pattern'])
194          && isset($post['amber'])
195          && isset($post['blue'])
196          && isset($post['red'])
197      ) {
198          $current_state = str_split($_SESSION['verify_pattern']);
199          if (array_search($post['amber'], $action_array) == $current_state[0]
200              && array_search($post['blue'], $action_array) == $current_state[1]
201              && array_search($post['red'], $action_array) == $current_state[2]
202          ) {
203              $_SESSION['verified'] = true;
204              return passwordForm();
205          }
206      }
207      generateLEDpattern();
208      return verifyForm(true);
209  }
```

noosc

Exploitation

- Edit welcome.inc.php

```
function verifyPineapple($post)
{
    $action_array = array('off', 'on', 'blink');
    if (isset($_SESSION['verify_pattern'])
        && isset($post['amber'])
        && isset($post['blue'])
        && isset($post['red'])
    ) {
        $current_state = str_split($_SESSION['verify_pattern']);
        if (array_search($post['amber'], $action_array) == 2
            && array_search($post['blue'], $action_array) == 0
            && array_search($post['red'], $action_array) == 1
        ) {
            $_SESSION['verified'] = true;
            return passwordForm();
        }
    }
```

***In version 2.4.0, we just need to change the equation "==" to "! =" below the resetDips() function**

noosc

Exploitation

- Edit fstab (etc/config/fstab)

```
$  cat ./fmk/rootfs/etc/config/fstab
config global automount
        option from_fstab 1
        option anon_mount 1

config global autoswap
        option from_fstab 1
        option anon_swap 0

config mount
        option target   /sd
        option device   /dev/sda1
        option fstype   auto
        option options  rw,sync
        option enabled  1
        option enabled_fsck 0

config swap
        option device   /dev/sda2
        option enabled  1
```

noosc

Exploitation

- Edit format_sd

(pineapple/components/system/resources/includes/files/format_sd)

```
touch /tmp/sd_format.progress

reset_sd
sleep 5

umount /sd
swapoff /dev/sda2

sleep 2
cat
/pineapple/components/system/resources/includes/files/fdisk_instructions   |
fdisk /dev/sda
sleep 2

umount /sd
mkfs.ext4 /dev/sda1
sleep 2
mkfs.ext4 /dev/sda2


mkswap /dev/sda2

mount /dev/sda1 /sd
swapon /dev/sda2
```

noosc

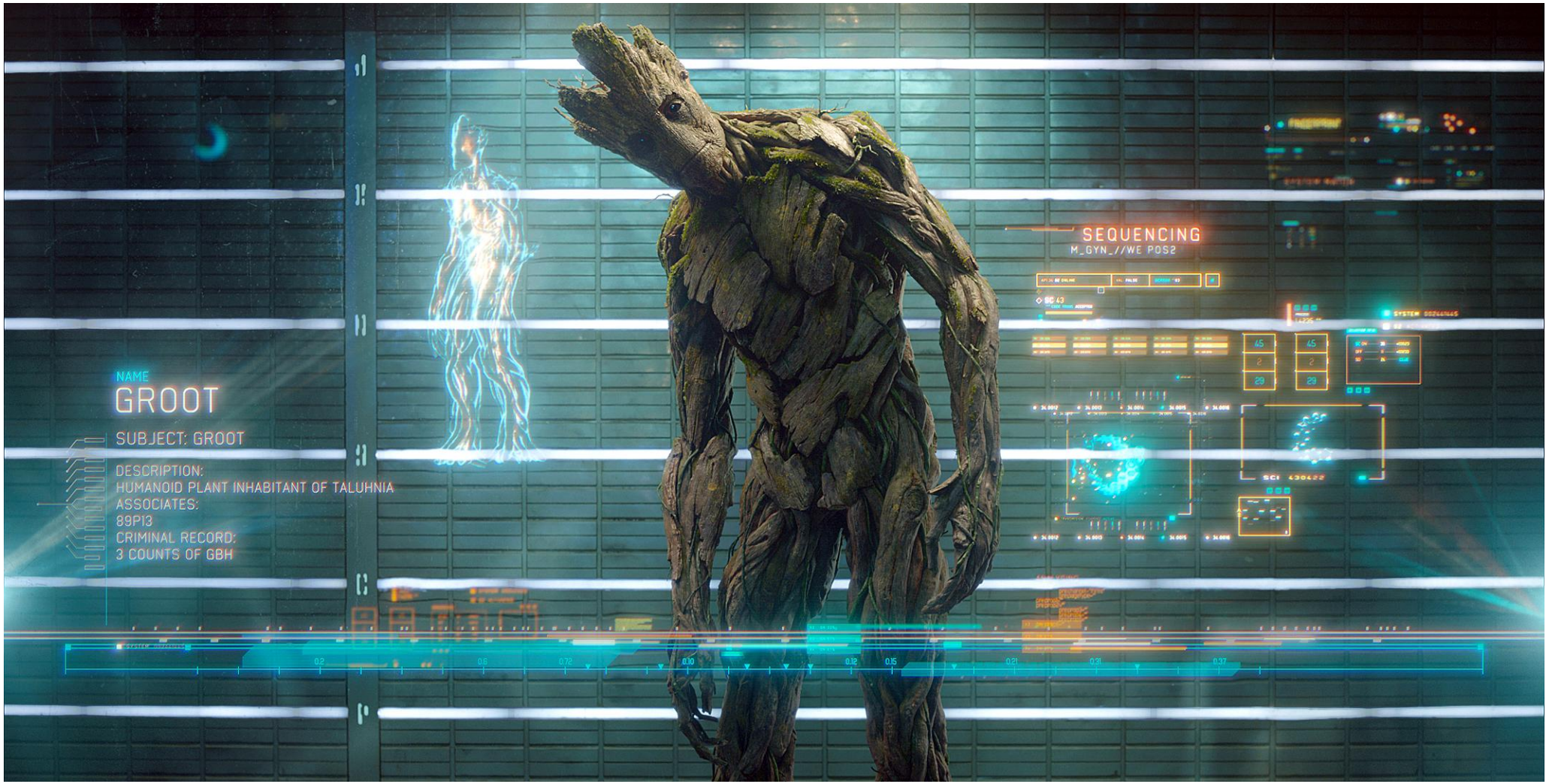
Repacking (FMK)

$ sudo ./build-firmware.sh fmk/

***If output size too big, delete some files or use “-min” option**

noosc

Download link:
https://github.com/smrx86/STPF2/tree/master/firmware



USE IT WISELY.... OKKai

noosc