SYNACKTIV

WP n'a de protected que le nom

HackSecuReims

29/03/2024

Paul VIEL

Whoami

SYNACKTIV

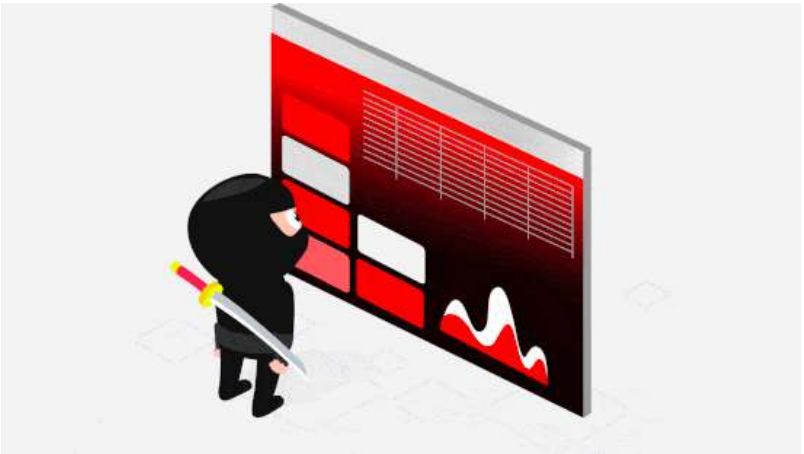
- Paul Viel (Dvorhack)
- Reverser at Synacktiv
- CTF Player HackUTT, Hexagon, MadeInFrance, PwnStars

Thanks to BZHugs

Synacktiv

SYNACKTIV

- Entreprise de cybersécurité offensive
- + de 160 ninjas
- Plusieurs pôles: Reverse, Pentest, Dev, CSIRT
- Sur 5 lieux: Paris, Rennes, Lyon, Toulouse et Lille



On Recrute !!

Pioneer - IVI (In-Vehicle Infotainment)

SYNACKTIV

- $1,300
- En vente au USA et Canada uniquement

Pioneer - IVI (In-Vehicle Infotainment)

Surface d'attaque

SYNACKTIV

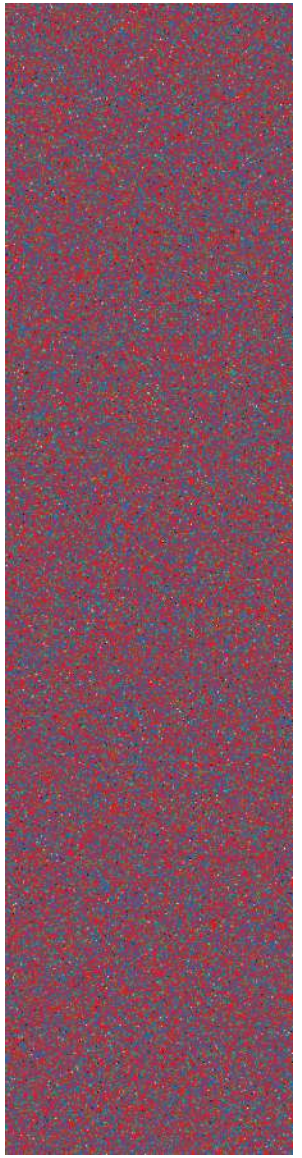
- Wifi (Client + Server)
- Bluetooth
- Browser
- USB
- OBD

Pioneer - IVI

Firmware

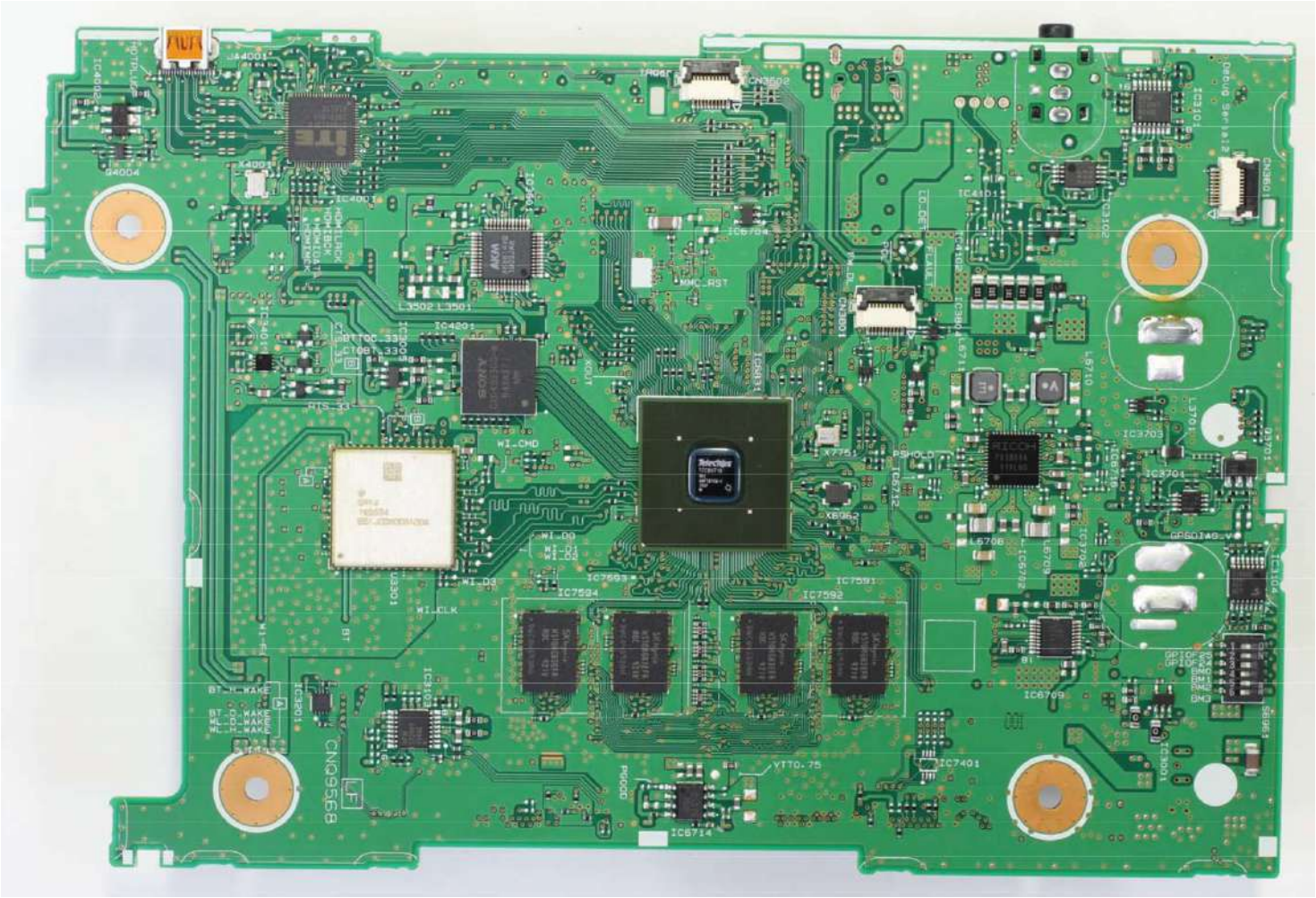
SYNACKTIV

- Public mais ….
- Entropie de 0.99 après le header



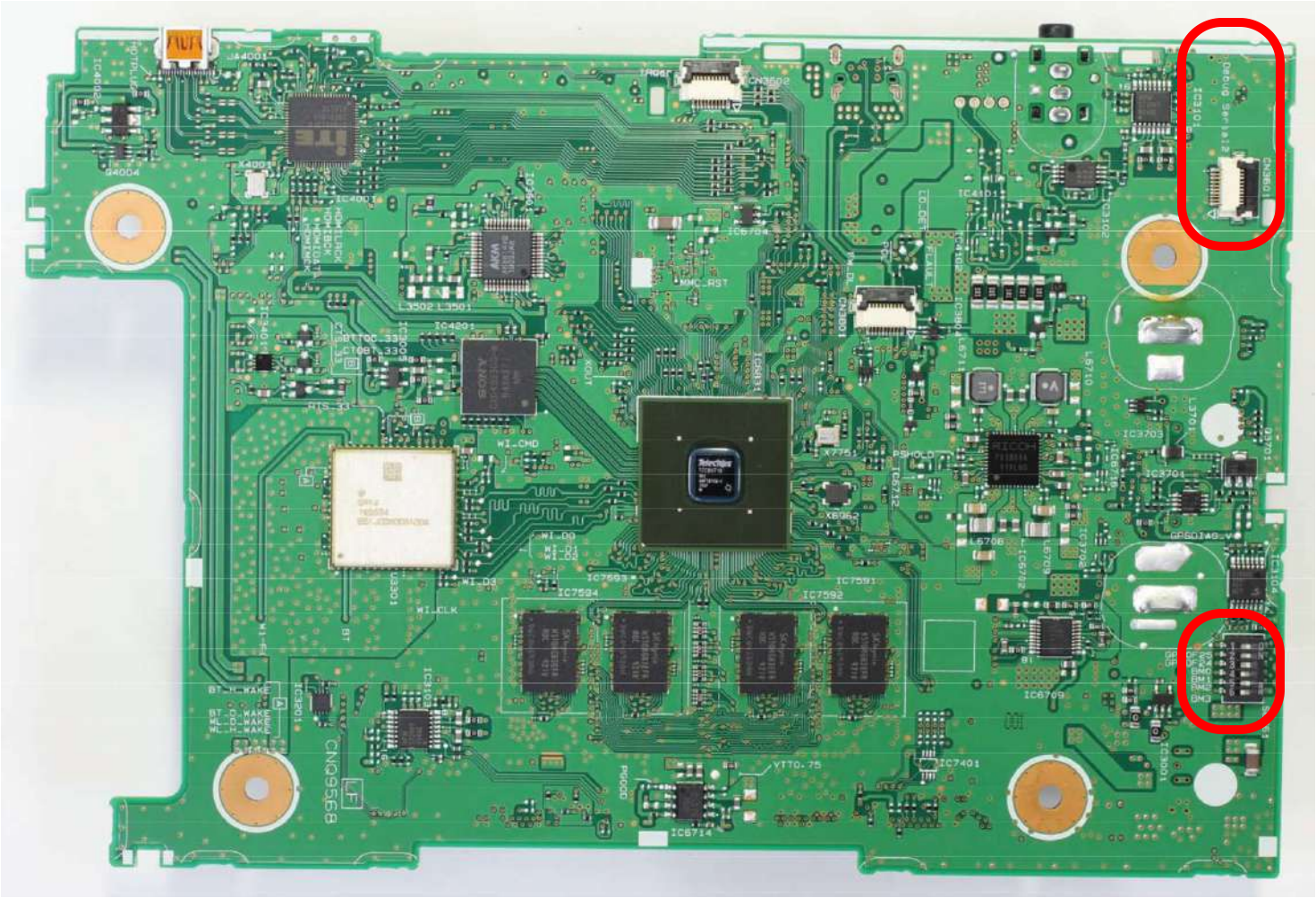
FCC Pictures

hardware front



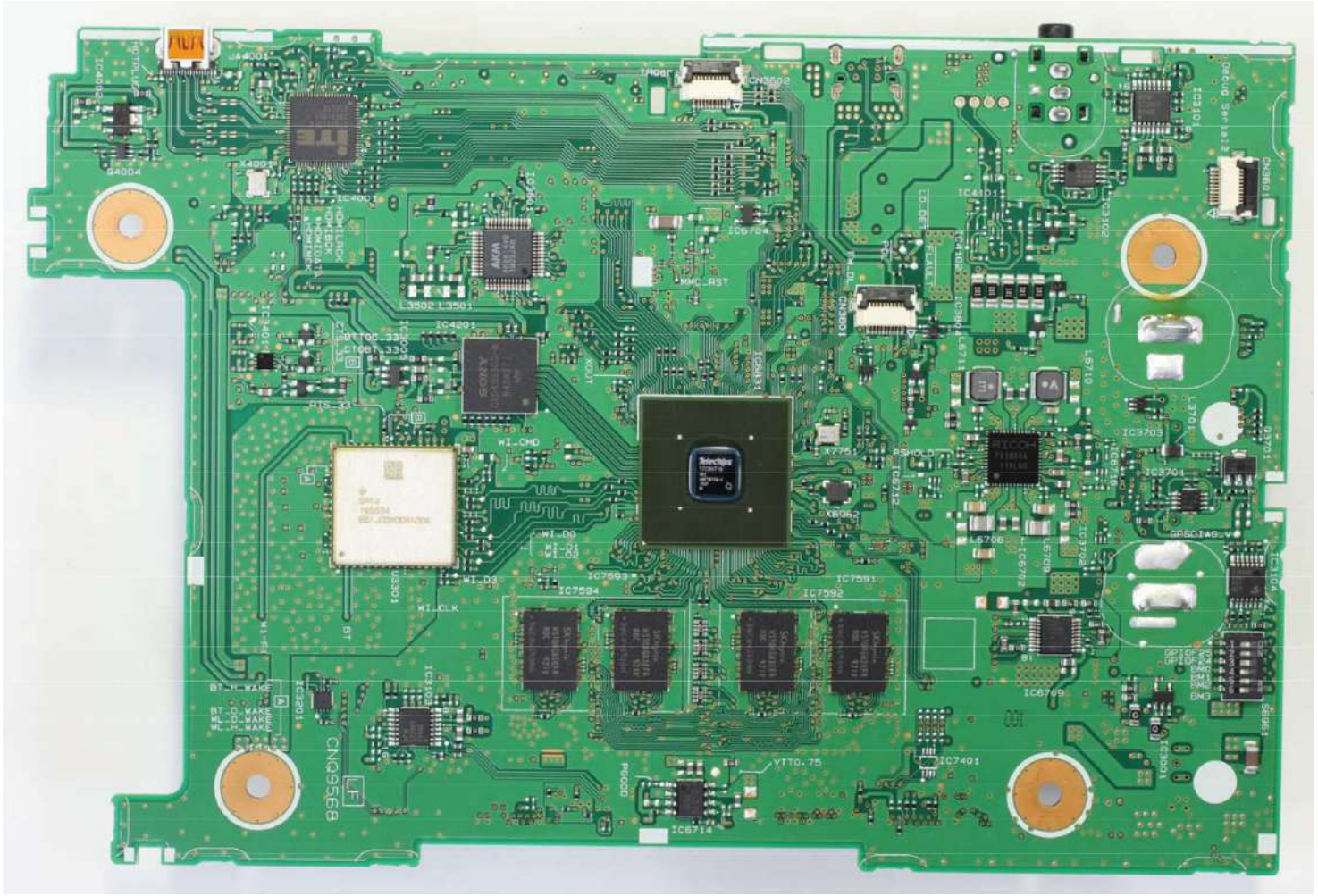
FCC Pictures

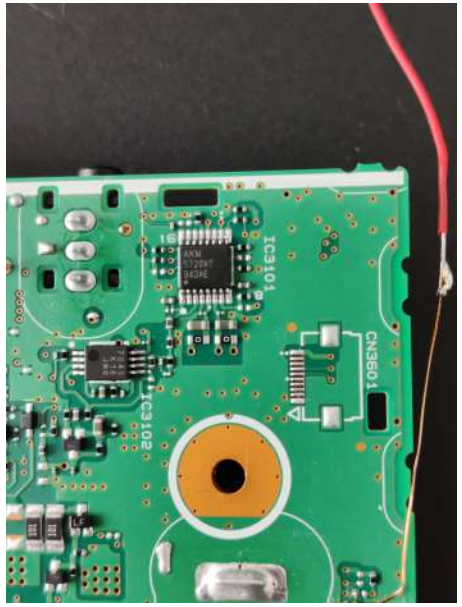
hardware front



Pioneer - IVI

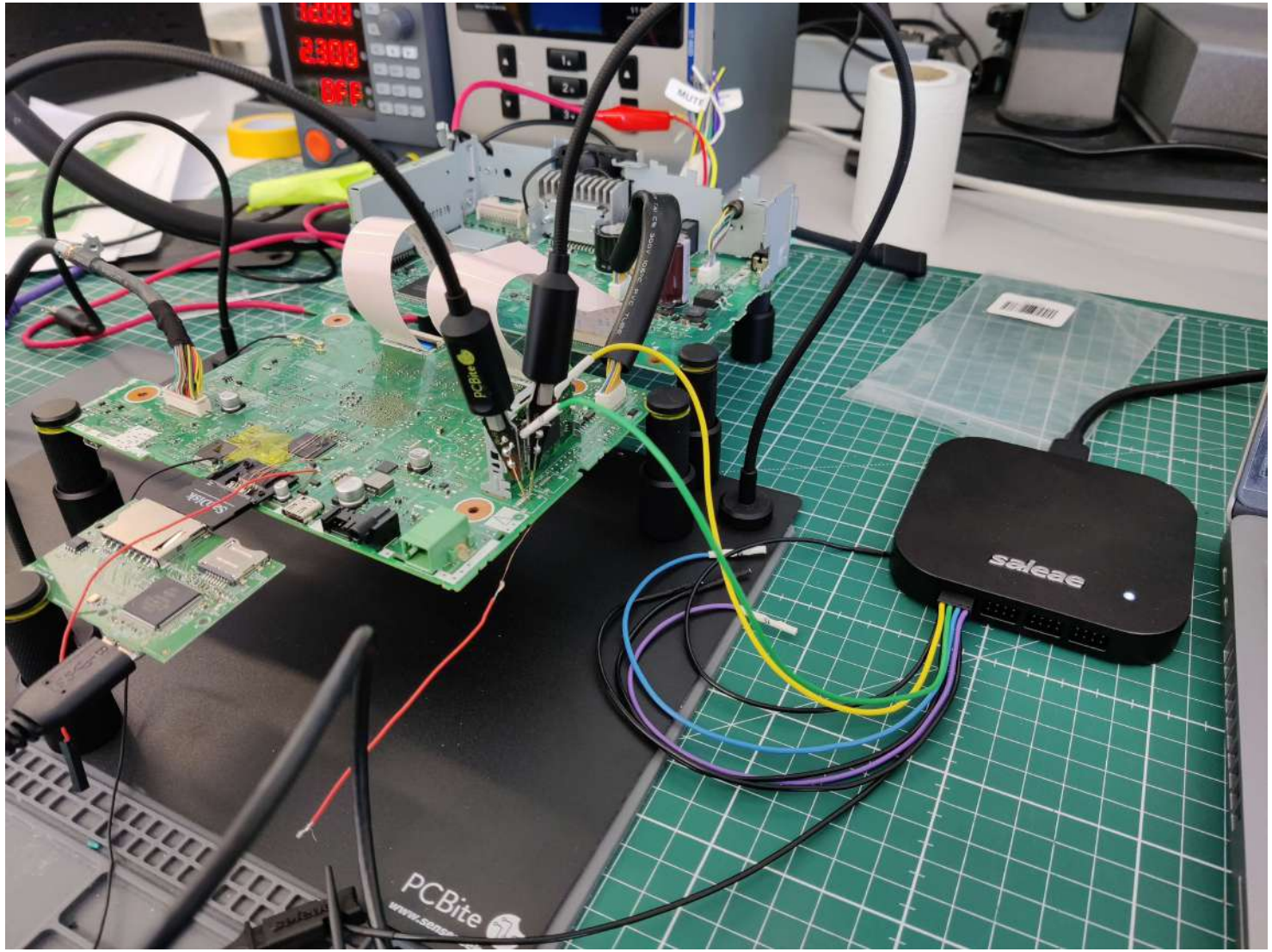
hardware front





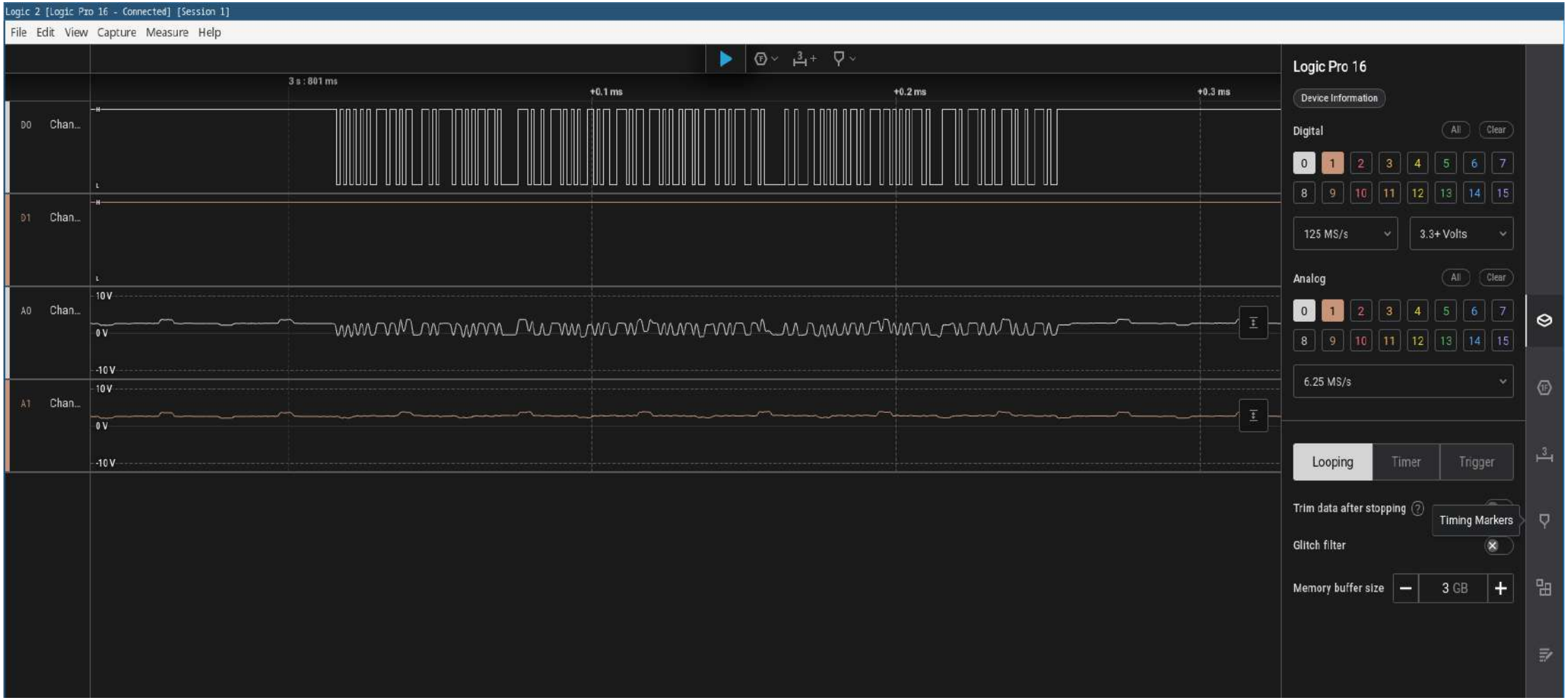
Pioneer - IVI

Logic analyzer



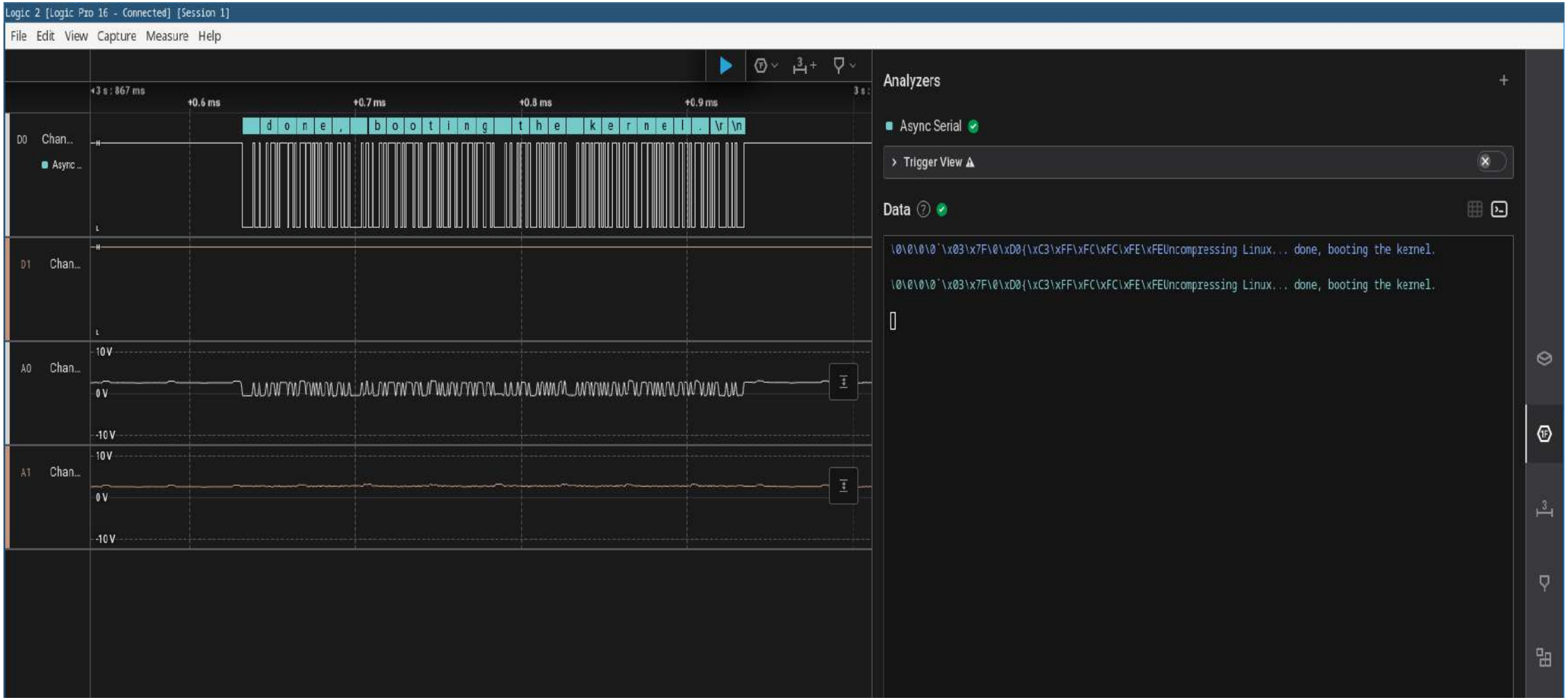
Pioneer - IVI

Logic analyzer



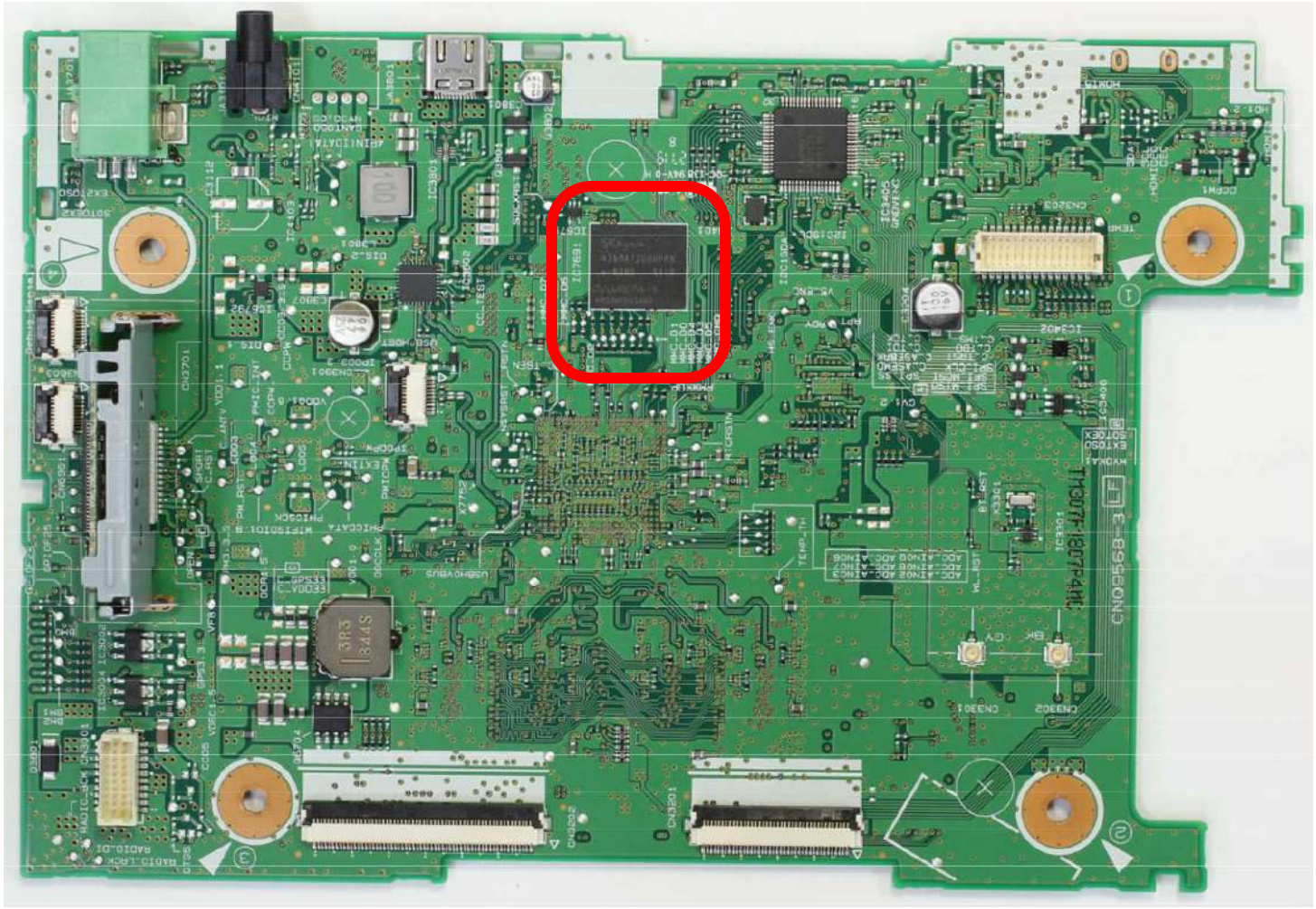
Pioneer - IVI

Logic analyzer



Pioneer - IVI

hardware back



Pioneer - IVI

dump eMMC

SYNACKTIV

Dump eMMC sans désouder la flash:

- eMMC RESET
- eMMC CMD
- eMMC CLK
- eMMC DATA0(-7)

Contraintes:

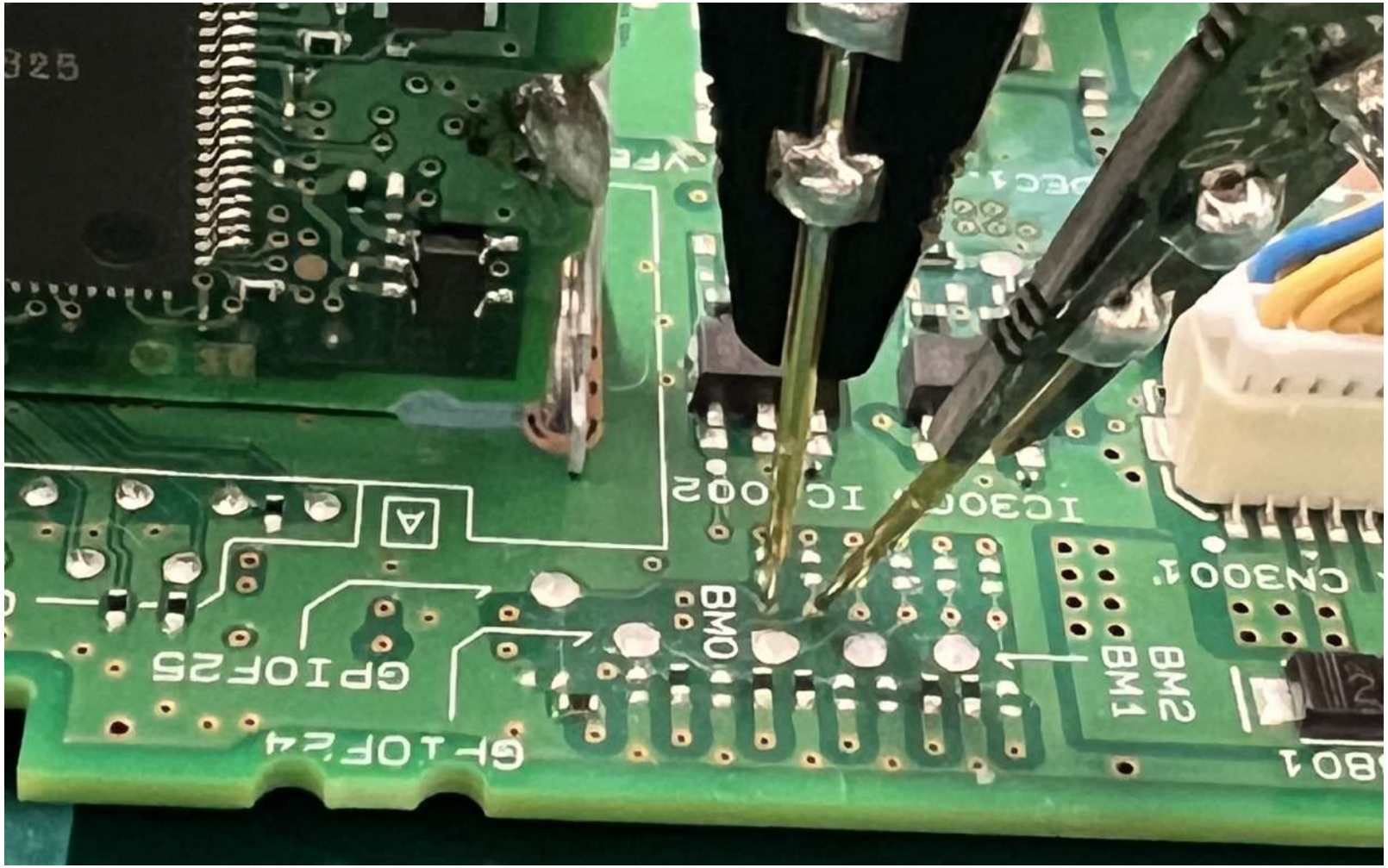
- l'eMMC doit être alimentée
- le CPU ne doit pas driver la flash -> CPU en RESET

Pioneer - IVI

dump eMMC

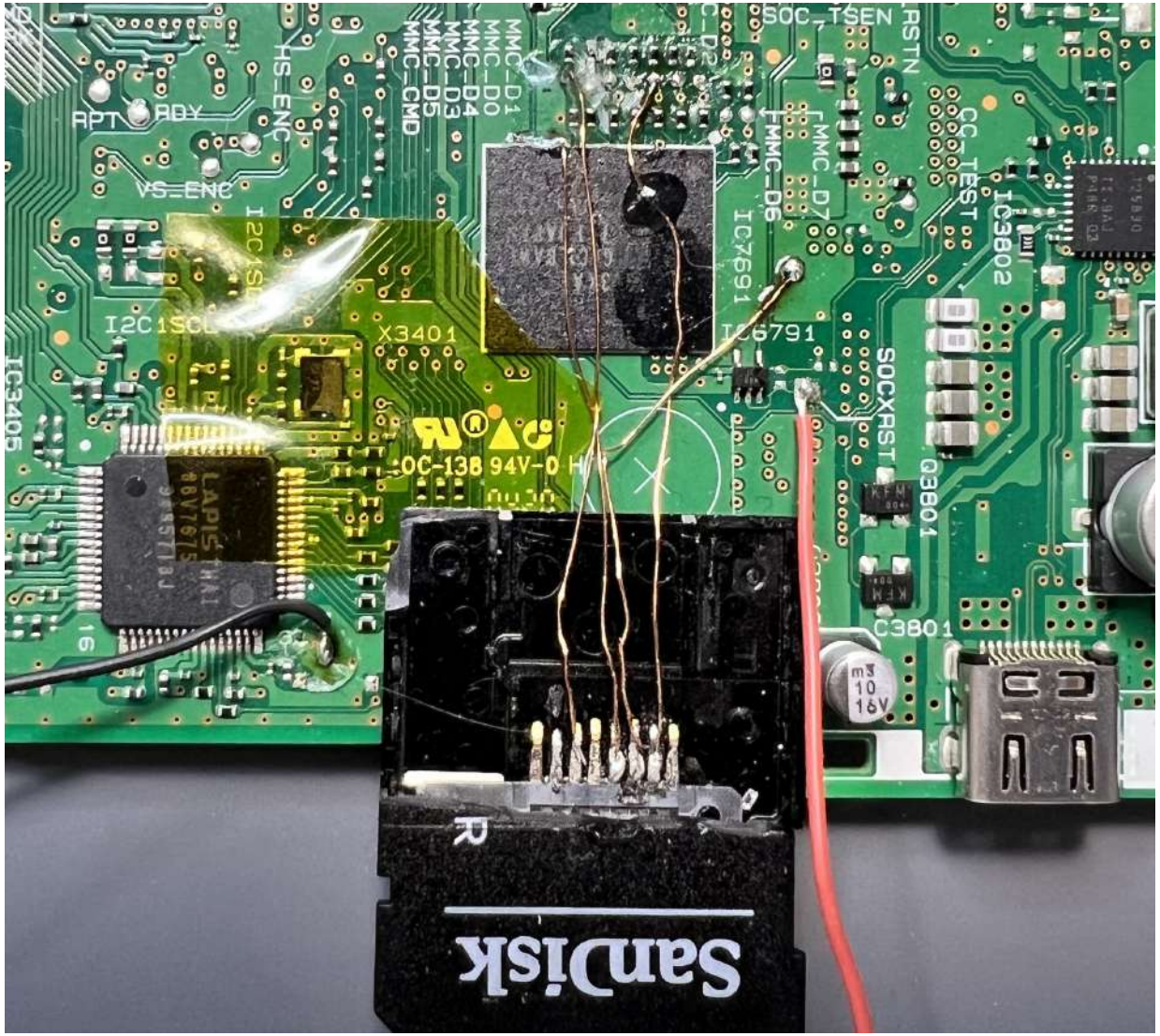
Pioneer - IVI

Boot Mode



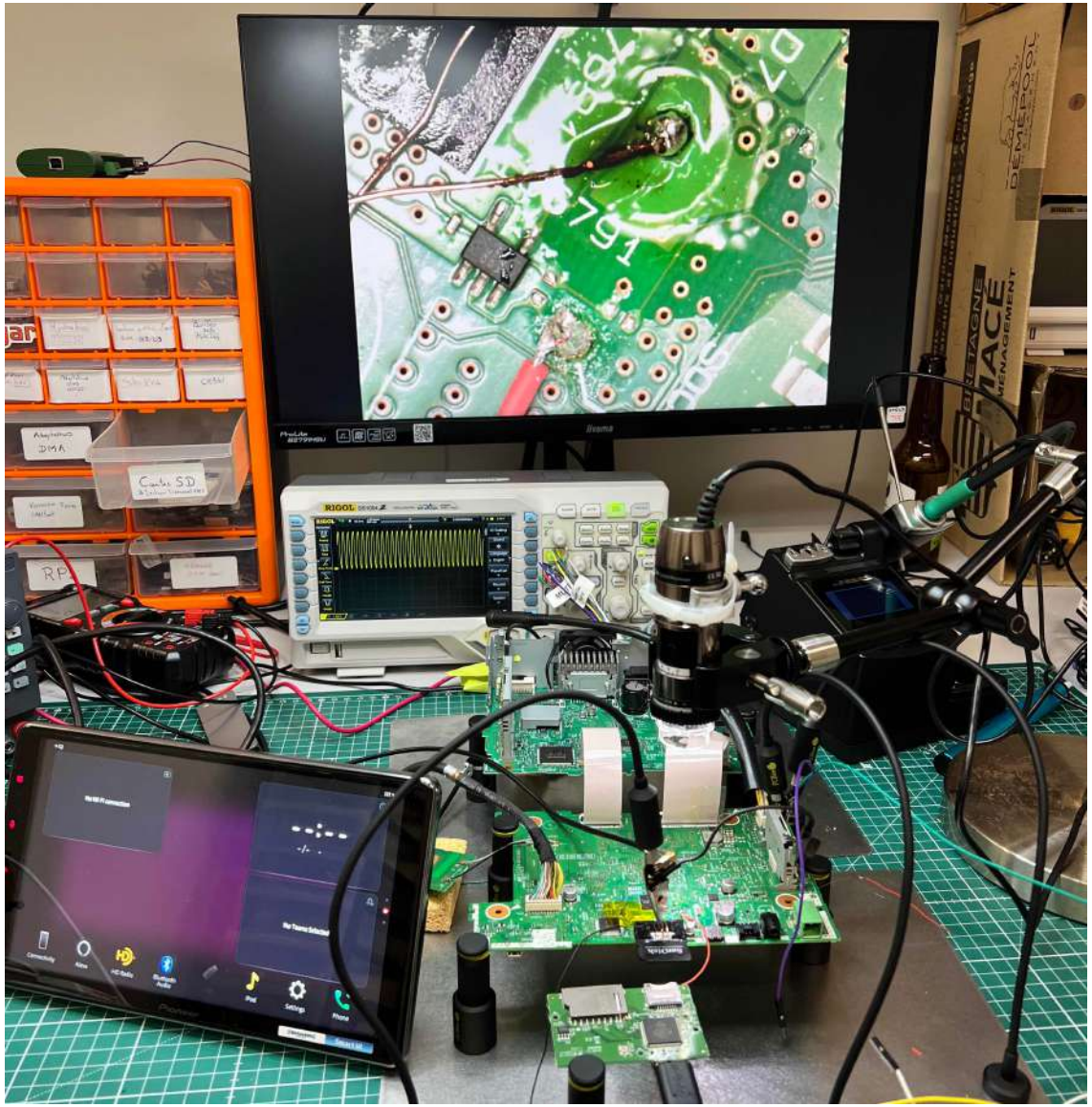
Pioneer - IVI

dump eMMC



Pioneer - IVI

lab eMMC



Pioneer - IVI

hardware / eMMC

SYNACKTIV

Problèmes rencontrés

- Glitch de voltage après ~8 secondes (Watchdog hardware PMIC)
- Fenêtre d'utilisation du disque de 8 secondes seulement
- Impossible de dump tout le disque de manière rapide et sans erreurs

Notre solution

- Dump des tables de partitions
- Dump de la liste des fichiers présents sur les partitions
- Dump fichier par fichier en se basant sur les noms qui semblent être intéressants

Pioneer - IVI

OTA retro ingénierie

SYNACKTIV

```
void __fastcall CUPD_ENT_DU_DecryptReq::DoAction(CUPD_ENT_DU_DecryptReq *this)
{
  int v2; // r0
  const __int16 *v3; // r5
  int v4; // r8
  int v5; // r0
  int v6; // r5
  int v7; // r5
  int v8; // r0
  int v9; // r9
  const __int16 *v10; // [sp+0h] [bp-40h]
  char v11[4]; // [sp+Ch] [bp-34h] BYREF
  int v12; // [sp+10h] [bp-30h]
  char v13[4]; // [sp+14h] [bp-2Ch] BYREF
  int v14; // [sp+18h] [bp-28h]

  *(&v10 - 3071) = 0;
  NString::NString((NString *)v11);
  AL_Log::Output();
  v10 = (const __int16 *)(this->m.field_2AC + 12);
  AL_Log::Output();
  if ( this->vtable->CUPD_ENT_DU_DecryptReq__CheckFirmwareHeader(this, &this->m.fw_file) )
  {
    NString::NString((NString *)v13);
    v6 = this->vtable->CUPD_ENT_DU_DecryptReq__DecryptFirmwareBody(this, &this->m.fw_file, v13);
    v10 = (const __int16 *)(v14 + 12);
    AL_Log::Output();
    if ( v6 )
    {
      v7 = CUPD_ENT_DU_ReadingReq::UnzipFirmwareBody(this, v13, v11);
      v10 = (const __int16 *)(v14 + 12);
      AL_Log::Output();
      v10 = (const __int16 *)(v12 + 12);
      AL_Log::Output();
      if ( !v7 )
```

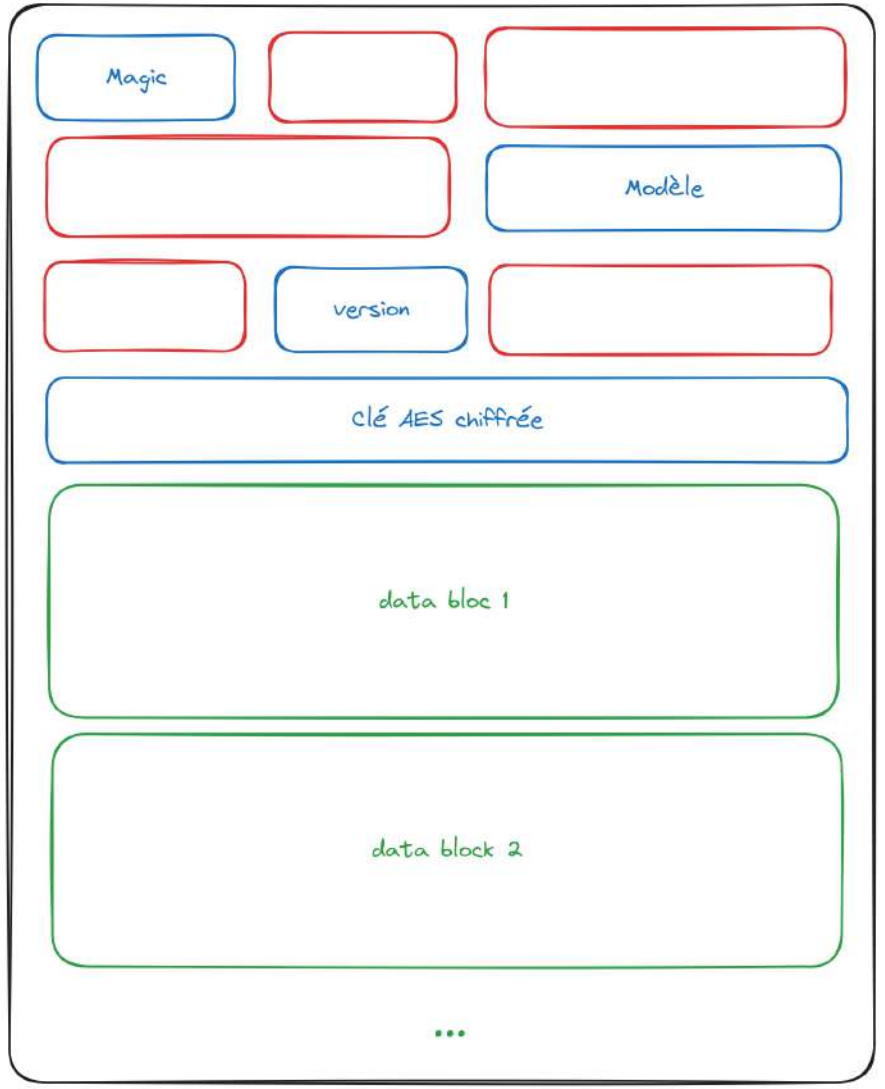
Pioneer - IVI

OTA retro ingénierie

SYNACKTIV

Pioneer - IVI

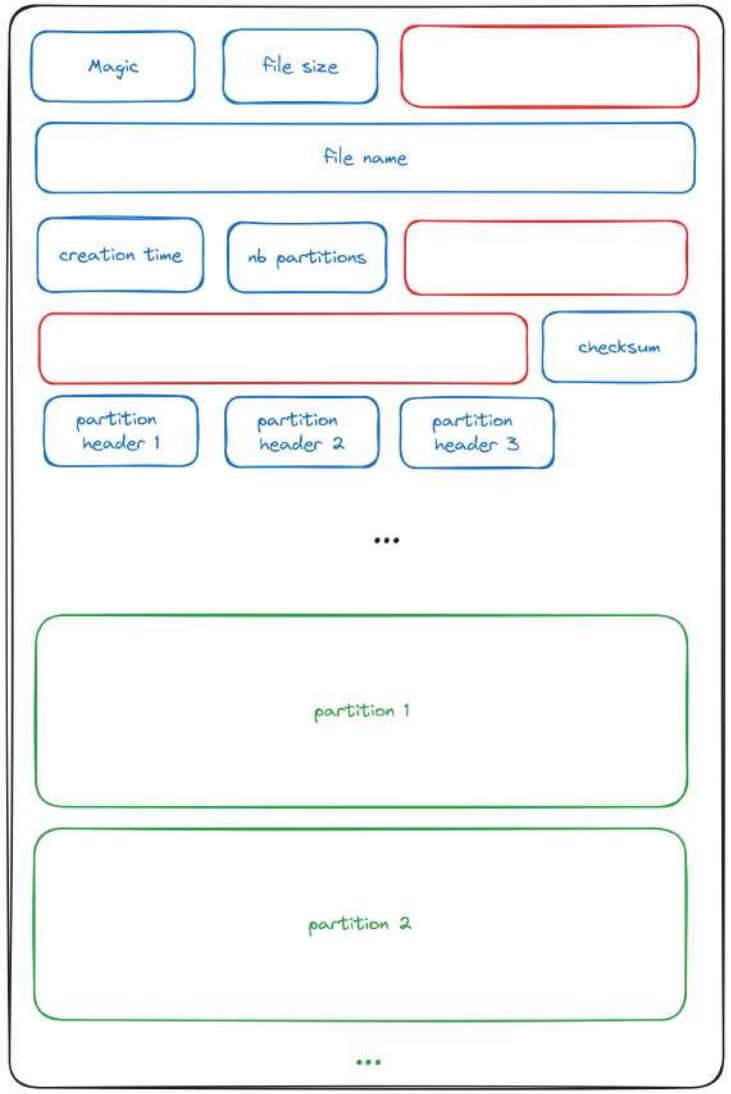
OTA retro ingénierie



Pioneer - IVI

OTA retro ingénierie

SYNACKTIV



Pioneer - IVI

OTA retro ingénierie

SYNACKTIV

- Noyau Linux 3.18.24
- lk bootloader
- Device Tree
- T-kernel (Bluetooth)
- rootfs
- Firmware GPS

T-Kernel

Pioneer - IVI

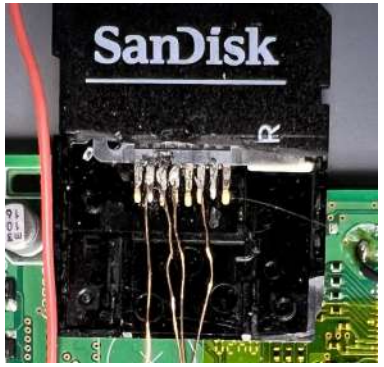
Implant d'une backdoor

SYNACKTIV

- Montage du disque en RW
- Ecriture de la backdoor

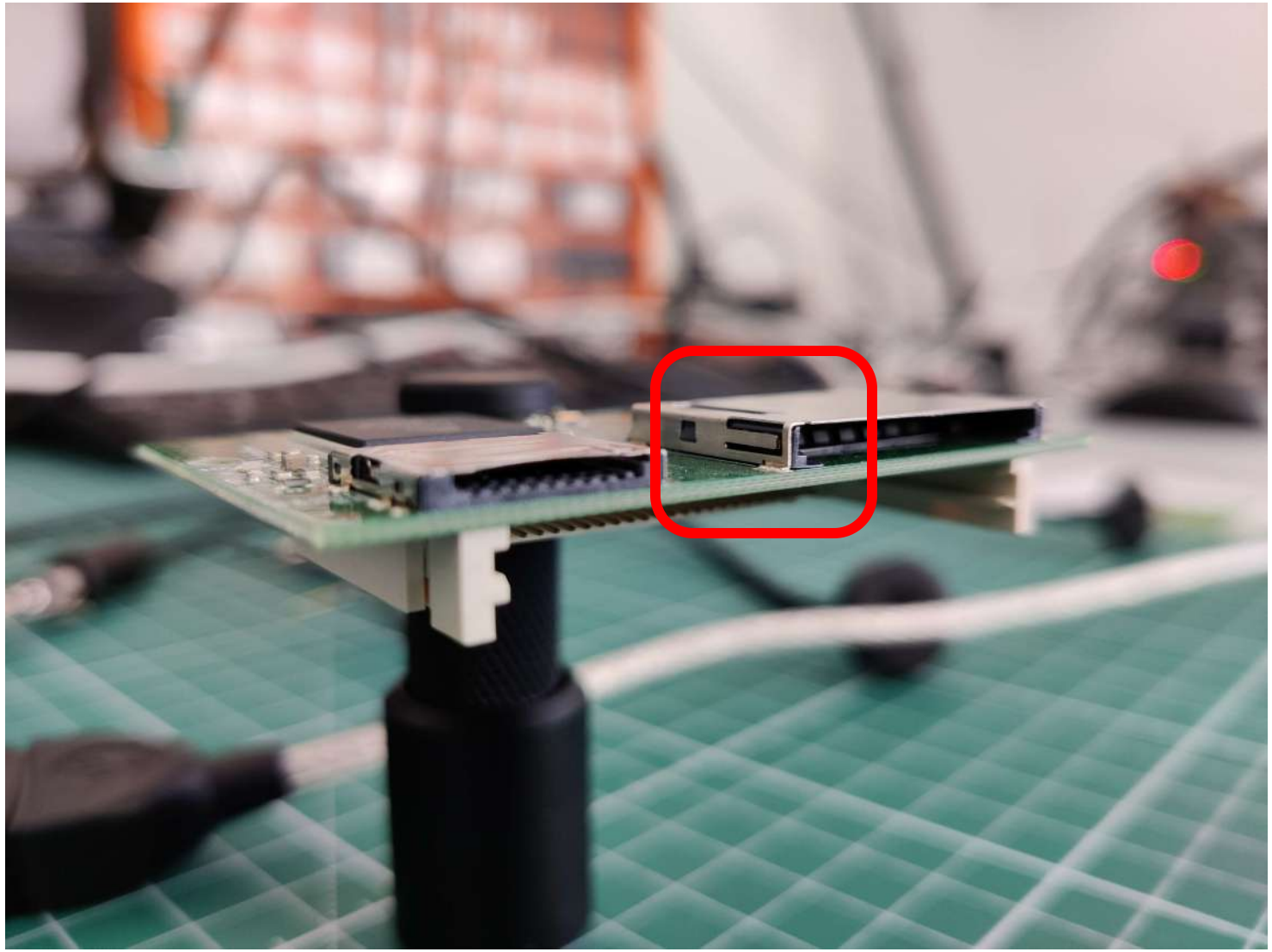
Write Protected !

- Impossible d'écrire sur le disque ...



Pioneer - IVI

Implant d'une backdoor



Pioneer - IVI

Implant d'une backdoor

SYNACKTIV

Recherche de solutions ...

- ~~Forcer le RW en étant root~~
- ~~Patch du driver linux~~ (oui, mais non)
- ~~Refaire toutes les soudures~~ HELL no !

No WAY !!

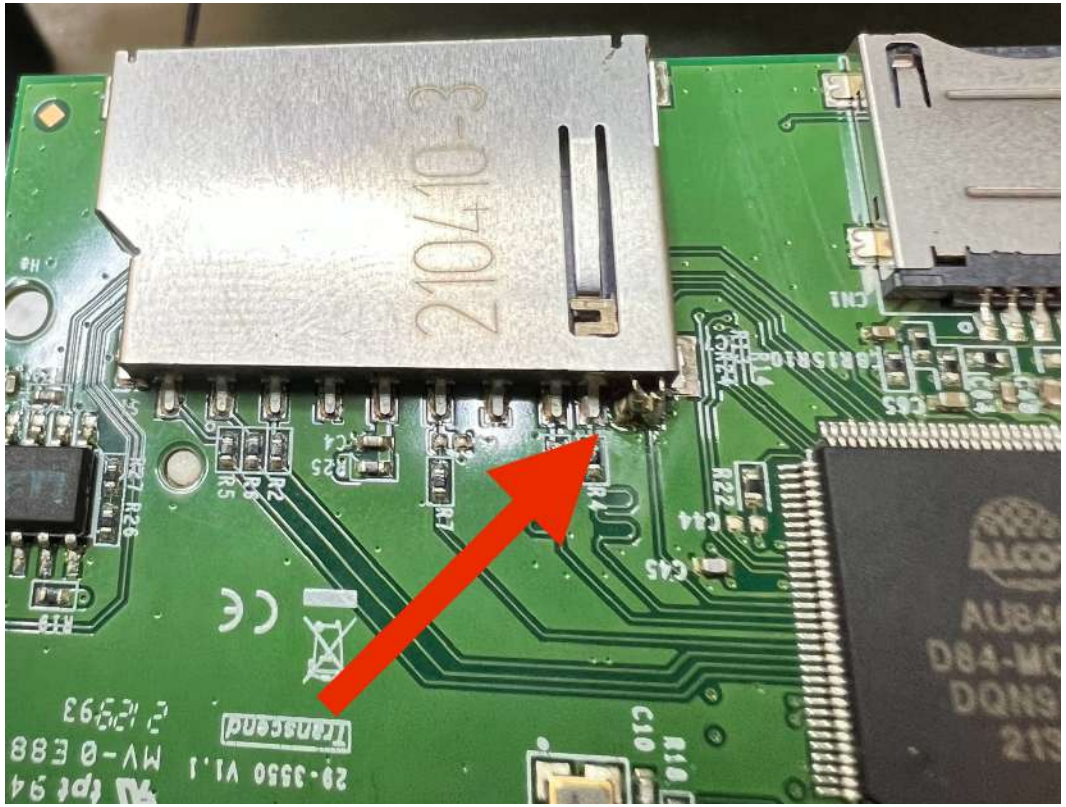
- Lecteur de carte SD qui force le RO
- Changer de lecteur de carte ? :)

Pioneer - IVI

Implant d'une backdoor

SYNACKTIV

Hold my beer



Pioneer - IVI

Implant d'une backdoor

SYNACKTIV

- Montage en RW
- Upload socat
- Modification init.d
- Reverse shell

Pioneer - IVI

Implant d'une backdoor

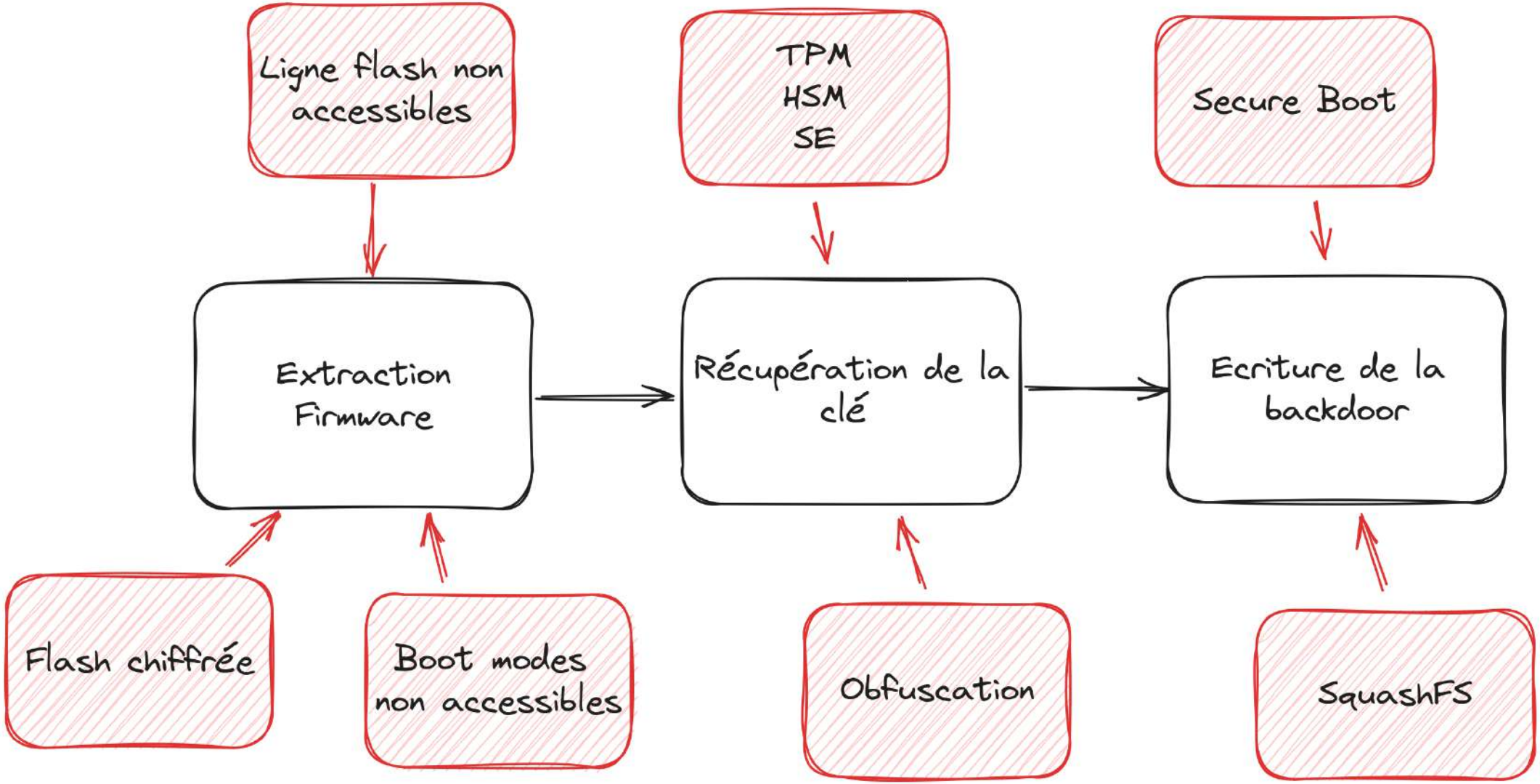
SYNACKTIV

- Backdoor success!

```
root@telechips-triton:/usr/local/bin# id
uid=0(root) gid=0(root)
root@telechips-triton:/usr/local/bin# uname -a
Linux telechips-triton 3.18.24-tcc #01100400 SMP PREEMPT Wed Mar 25 10:57:42 JST 2020 armv7l GNU/Linux
root@telechips-triton:/usr/local/bin#
```

Pioneer - IVI

résumé



SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://twitter.com/synacktiv

https://synacktiv.com