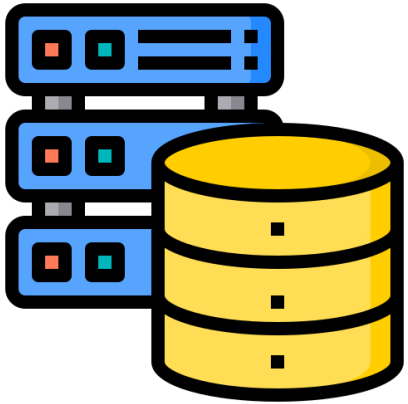
Contournement d’une authentification à double facteur

…

Avec une voiture

Un audit compliqué ?

~~Hameconnae~~
~~Ingéniérie sociale~~
~~Vulnérabilités~~



Un audit pas si compliqué !

Base de travail

Ford SYNC 2

Système multimédia embarqué

Production :
2011 – 2017

Véhicules dotés :
C-Max, Focus, Fiesta

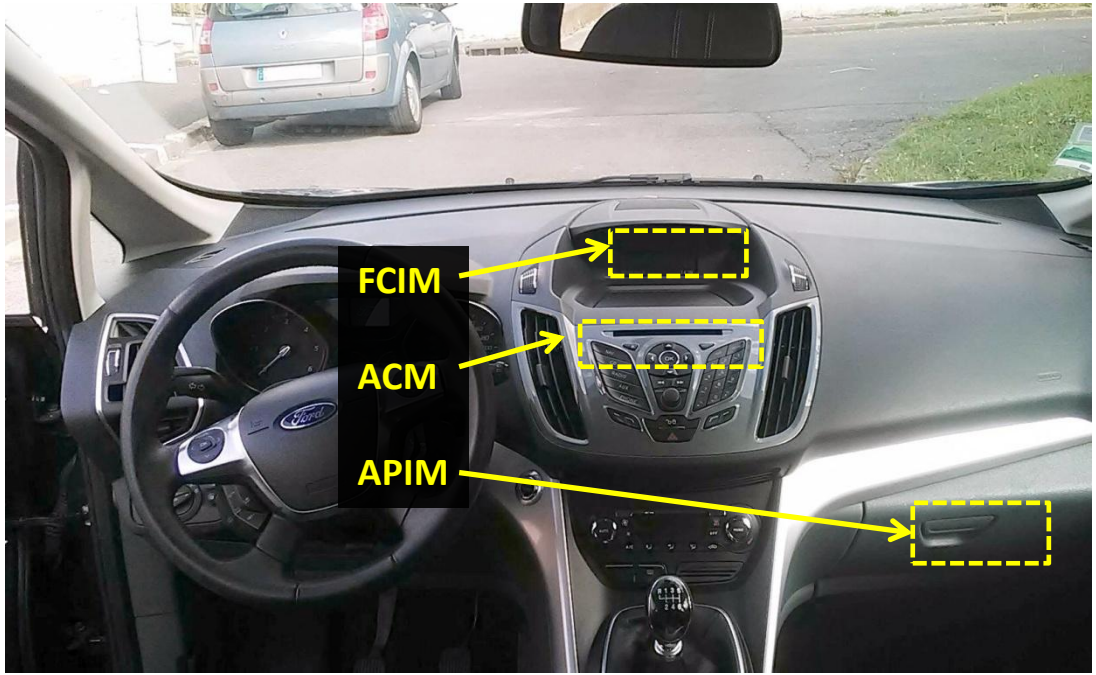
Un système, plusieurs ECUs

Architecture

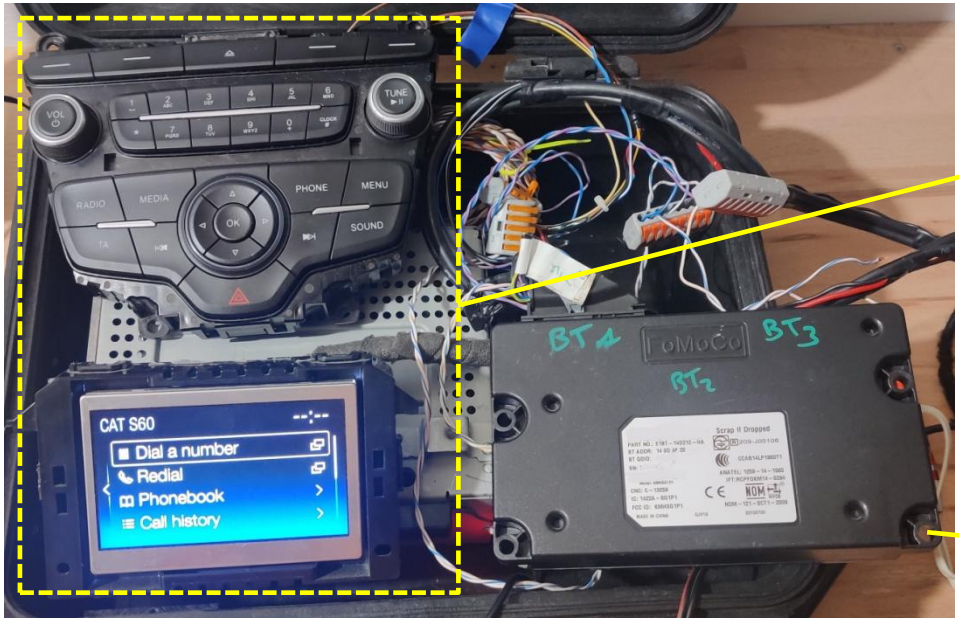
3 ECUs
- **FCIM** : Front Controls Interface Module
- **APIM** : Aux. Protocols Interface Module
- **ACM** : Audio Control Module

OS : Windows Automotive 4.0

Connectivités :
- USB
- Bluetooth



Détail des ECUs

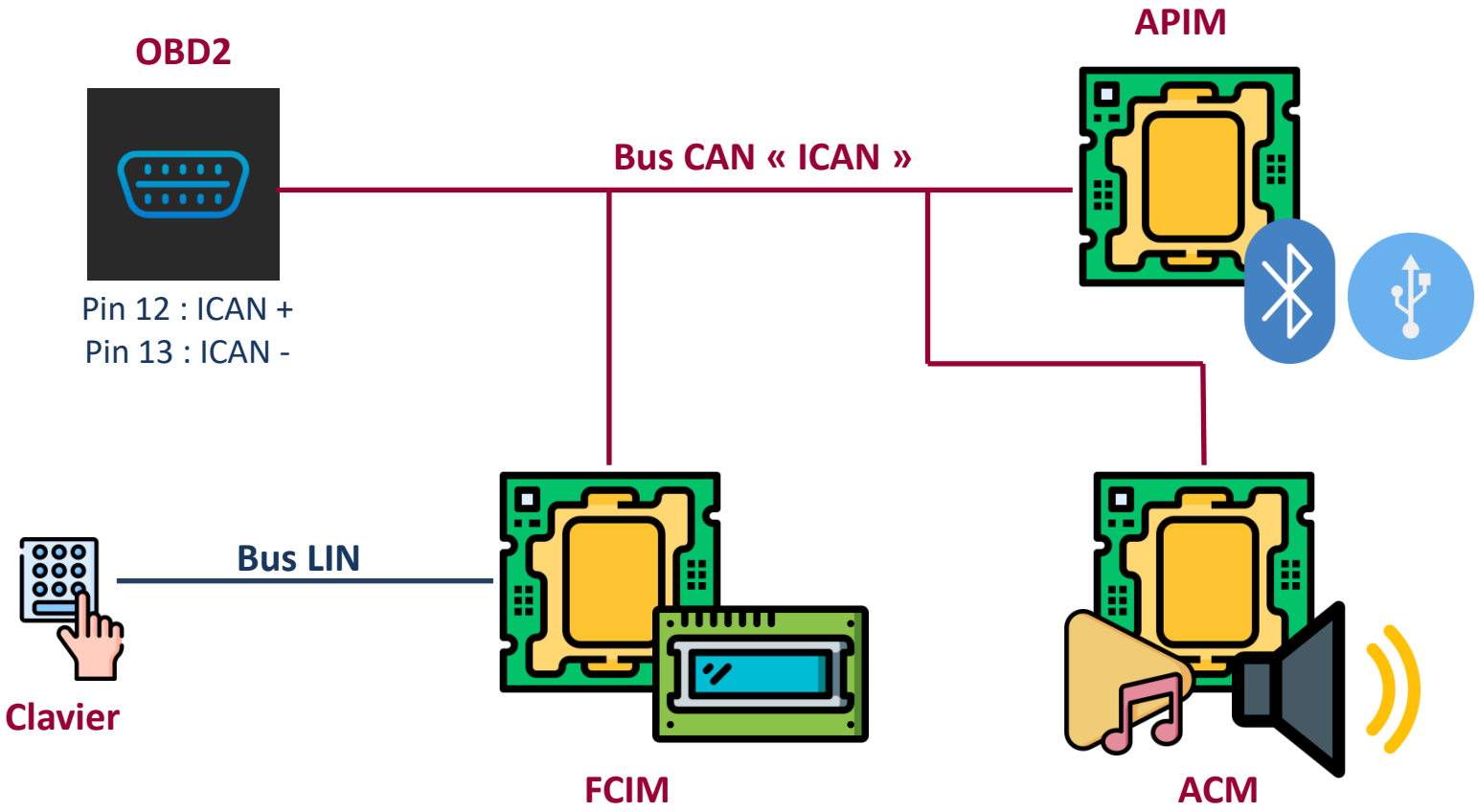


FCIM

APIM

Microcontroleurs :
Freescale MC9s12X
Freescale SCIMX3
Renesas 72691X266FP
Mémoire Flash NAND : S34ML

Architecture




DU BUS CAN
VOILA QUI
EST PROMETTEUR
imgflip.com

Les différents réseaux automobiles

Les ECU sont interconnectés sur un ou plusieurs réseaux :

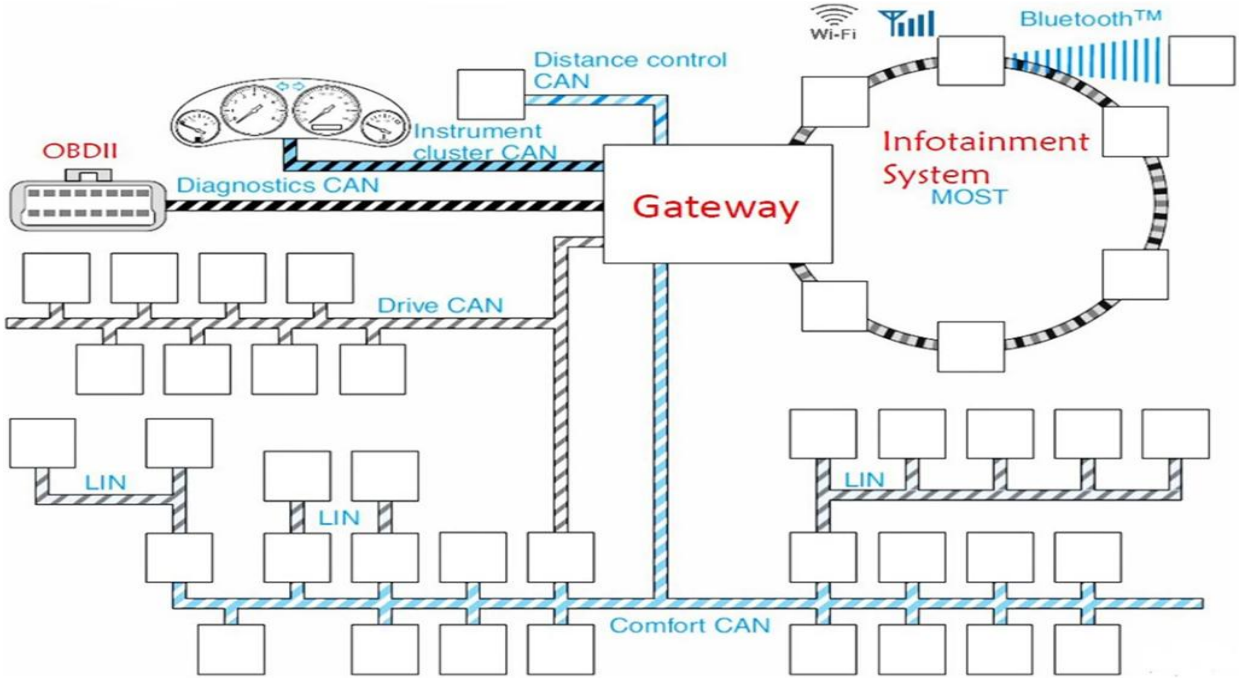
- **CAN**
Controller Area Network

- **LIN**
Local Interconnect Network

- **MOST**
Media Oriented
Systems Transport

- **FLEXRAY**

- **DoIP**



Il est courant de trouver 3 à 4 réseaux CAN différents dans un véhicule, filtrés ou non par une gateway

La minute Bus CAN

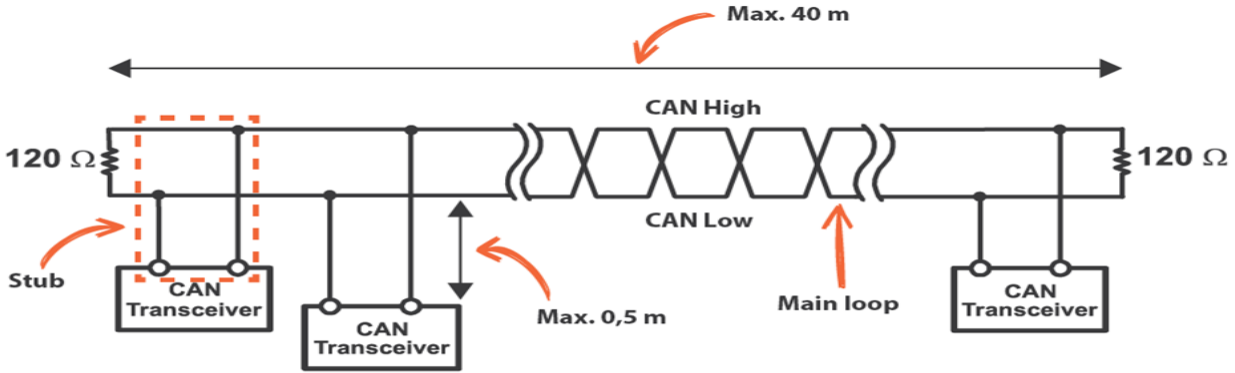
Bus CAN : liaison série asynchrone half-duplex, normalisé par la norme ISO 11898

Physiquement, c'est une paire torsadée avec un fil **CAN-High** et un fil **CAN-Low**, reliant différents ECU et terminé de part et d'autres par des résistances de **120 Ohms**.

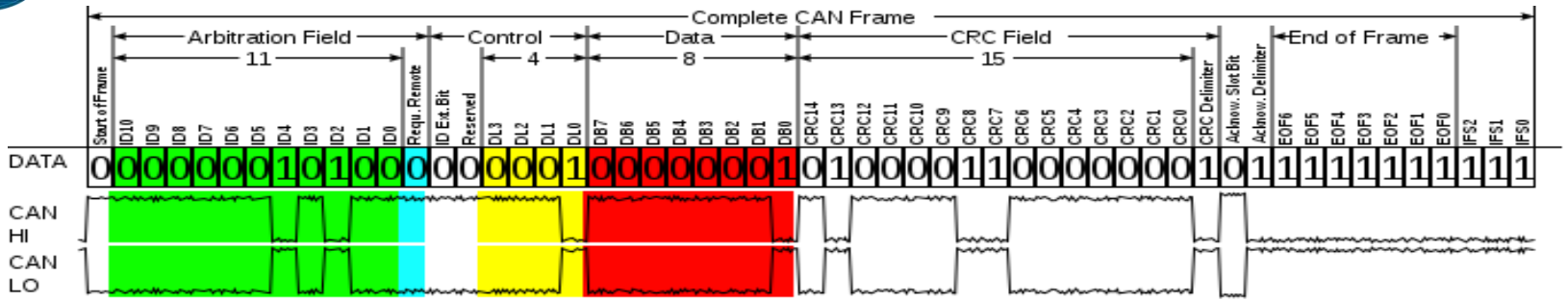
Le signal est une **tension différentiée** entre **CAN-H** et **CAN-L**.

Chaque message est **broadcasté** sur le bus, avec une gestion de priorité via **l'Arbitration ID.**

Signal	CAN-H	CAN-L
1	2.5V	2.5V
0	3.5V	1.5V



Trames CAN



4 types de trames: data, error, remote et overload.

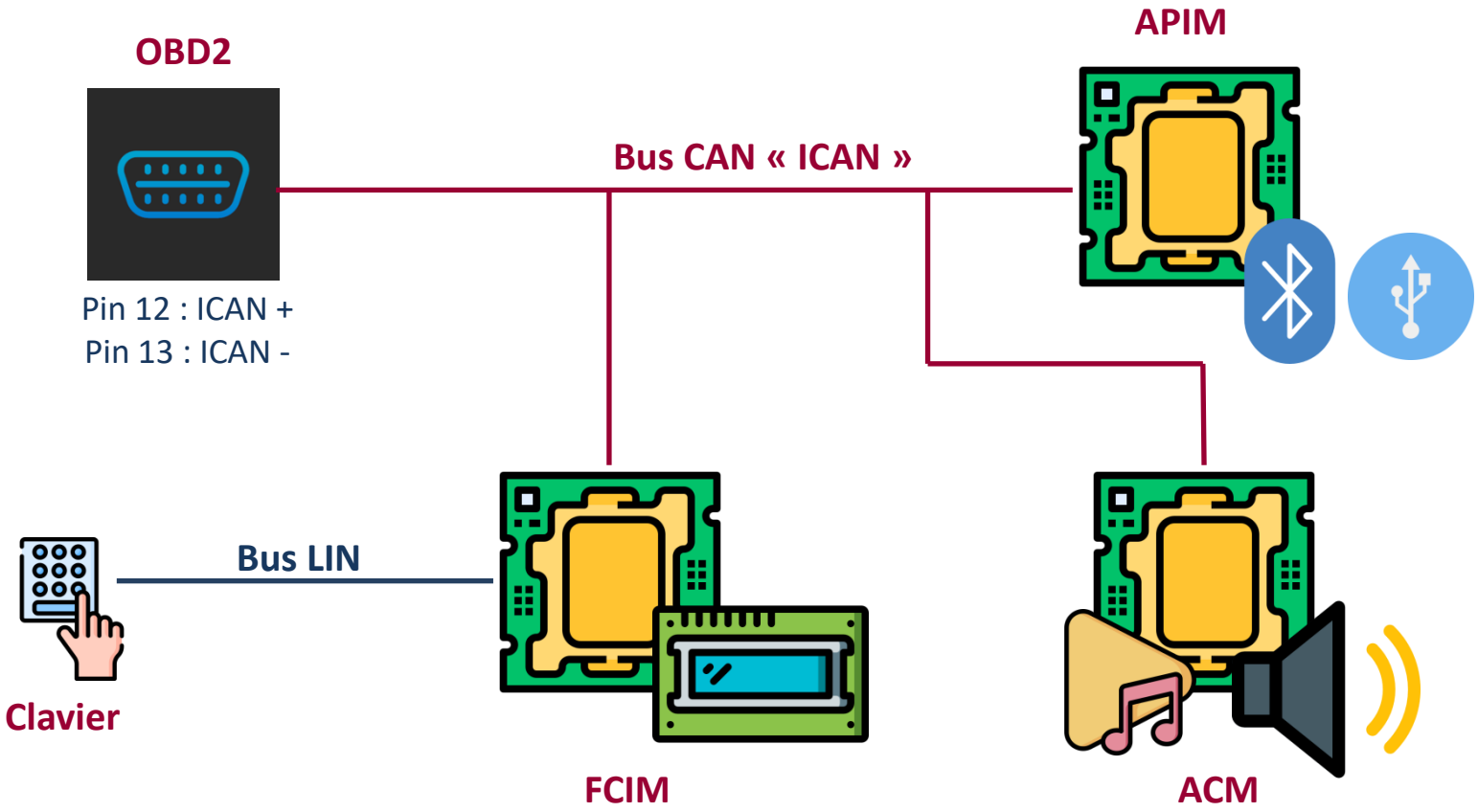
Arbitration ID : 11 bits (0x0 – 0x7FF) ou 29 bits (extended ID 0x0 – 0x1FFF FFFF)
Data: 1 à 8 octets

Exemple d'une lecture de trames can, via candump :

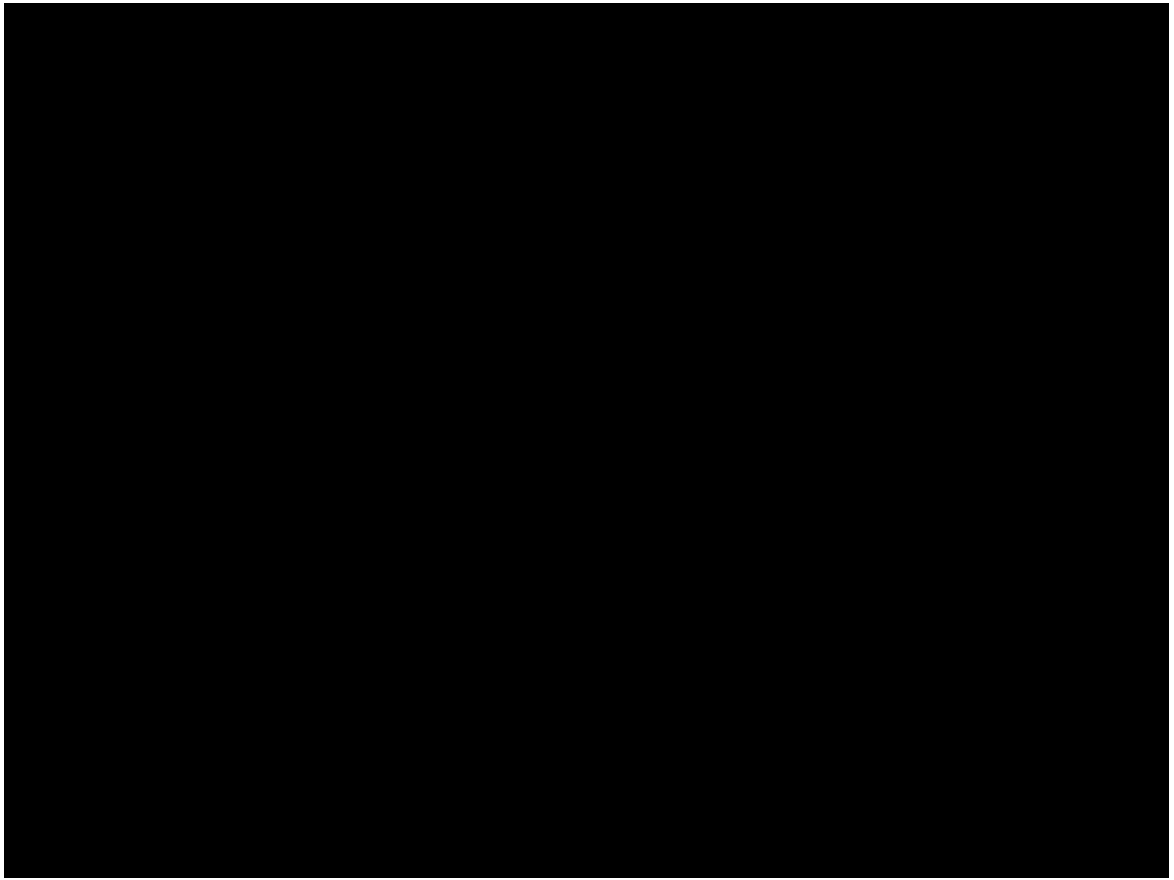
```
$ candump can0
can0  123   [8]  DE AD BE EF 01 02 03 04
```

Arbitration ID **Données**

Architecture



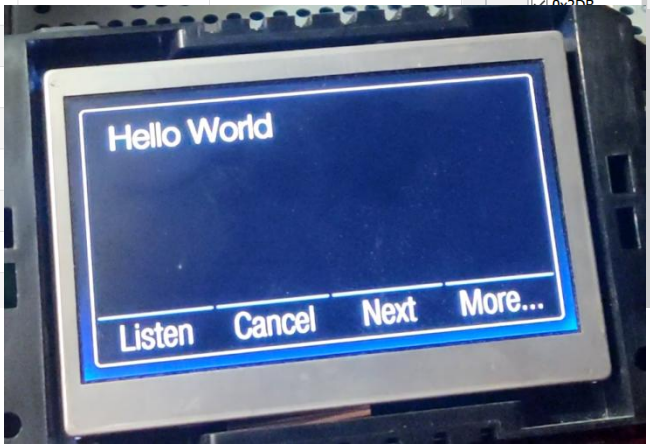
Test de lecture d’un SMS



Capture du Bus CAN

748	162997958708...	0x198	0	0	Rx	0	8	.....	01 DC 01 E5 00 1A 00 00
749	162997958708...	0x197	0	0	Rx	0	8	.....	DC 01 01 00 00 00 00 00
750	162997958710...	0x2A3	0	0	Rx	0	8	...t ...	01 0C 00 74 20 05 00 10
751	162997958716...	0x2CD	0	0	Rx	0	8	.%...Hel	10 25 DC 01 00 48 65 6C
752	162997958717...	0x2CD	0	0	Rx	0	8	!lo Worl	21 6C 6F 20 57 6F 72 6C
753	162997958718...	0x2CD	0	0	Rx	0	8	"d...Can	22 64 00 A0 00 43 61 6E
754	162997958719...	0x2CD	0	0	Rx	0	8	#cel.Nex	23 63 65 6C 00 4E 65 78
755	162997958720...	0x2CD	0	0	Rx	0	8	$t.More.	24 74 00 4D 6F 72 65 2E
756	162997958721...	0x2CD	0	0	Rx	0	8	%.....	25 2E 2E 00 00 00 00 00
757	162997958723...	0x288	0	0	Rx	0	8		
758	162997958724...	0x405	0	0	Rx	0	8		
759	162997958725...	0x400	0	0	Rx	0	8		
760	162997958725...	0x5E2	0	0	Rx	0	8		
761	162997958726...	0x290	0	0	Rx	0	8		
762	162997958742...	0x288	0	0	Rx	0	8		
763	162997958746...	0x5DB	0	0	Rx	0	8		

- 0x197
- 0x198
- 0x1E6
- 0x222
- 0x223
- 0x229
- 0x22D
- 0x288
- 0x290
- 0x2A3
- 0x2CD
- 0x2D5
- 0x2D6
- 0x2D7
- 0x2D8
- 0x2D9
- 0x2DA

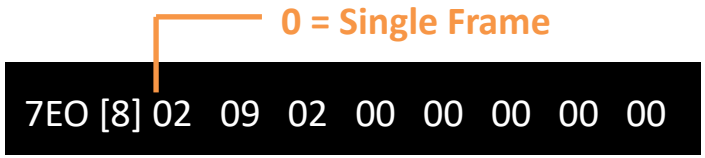



```
790 (1629979587.615069) can0 2DC#01FFF800FF000000
791 (1629979587.615427) can0 2DE#0100000003FFFFFF
792 (1629979587.615783) can0 2E6#0000000000000000
793 (1629979587.616149) can0 2F2#0000000000000000
794 (1629979587.616498) can0 2F3#1400000000000000
795 (1629979587.616854) can0 2F5#1008000000000000
796 (1629979587.617262) can0 2F7#0001000000000400
797 (1629979587.617503) can0 288#63FF03FF03FF0000
798 (1629979587.617765) can0 3E8#4088000000000000
799 (1629979587.618130) can0 4D0#2080003400000000
800 (1629979587.664901) can0 290#0000000000000000
801 (1629979587.752154) can0 400#1300000007020102
802 (1629979587.812400) can0 288#63FF03FF03FF0000
803 (1629979587.864906) can0 290#0000000000000000
804 (1629979587.992039) can0 405#1246533530323534
805 (1629979588.002966) can0 288#63FF03FF03FF0000
806 (1629979588.003429) can0 400#1402020100000301
807 (1629979588.064776) can0 290#0000000000000000
808 (1629979588.197297) can0 288#63FF03FF03FF0000
809 (1629979588.242462) can0 405#01664DA67C96F6FF
810 (1629979588.252250) can0 400#1500010202020001
811 (1629979588.253871) can0 5E2#E200FFFFFFFFFFFF
812 (1629979588.264721) can0 290#0000000000000000
813 (1629979588.386386) can0 288#63FF03FF03FF0000
814 (1629979588.460719) can0 5DB#DB00FFFFFFFFFFFF
815 (1629979588.464632) can0 192#B010000000000000
816 (1629979588.464905) can0 229#0000020000000000
817 (1629979588.465181) can0 290#0000000000000000
818 (1629979588.465443) can0 2A3#010C007420050010
819 (1629979588.465713) can0 2E3#0200000000000000
820 (1629979588.465987) can0 321#0000000000000000
821 (1629979588.466282) can0 322#0000000000000000
822 (1629979588.466530) can0 3DA#0000000000000000
823 (1629979588.466787) can0 4D3#5130542000000000
824 (1629979588.491773) can0 405#02FF0100320112C4
825 (1629979588.502669) can0 400#1600000100000004
```

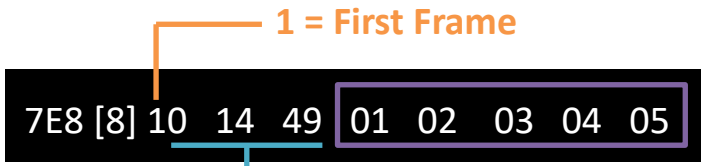
Protocole ISO-TP

Le protocole **ISO-TP** (ISO 15765-2) permet d'envoyer des messages de plus de 8 octets, limité à **4096** octets

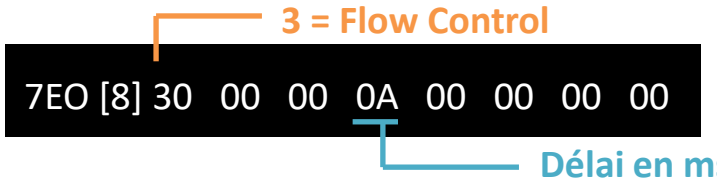
Requête initiale :



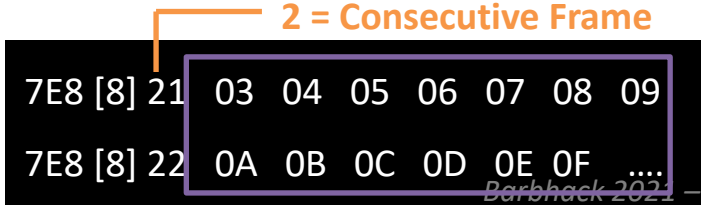
Réponse de l'ECU :



Envoi du flow control :



Messages complémentaires :



K.I.S.S.

Dumper
la mémoire
et reverser ?

Can-utils!

Analyse des trames transmises

Action sur le clavier :

Touche

Etat (84 / 44)

106 [8] 02 84 70 00 00 00 00 00 — **FDIM**

Menu actif :

Element sélectionné

Menu actif

203 [8] 01 00 70 00 20 04 00 10 — **FDIM (Cyclique)**

Demande d'affichage :

198 [8] 01 A4 01 E5 00 00 00 00 — **APIM**

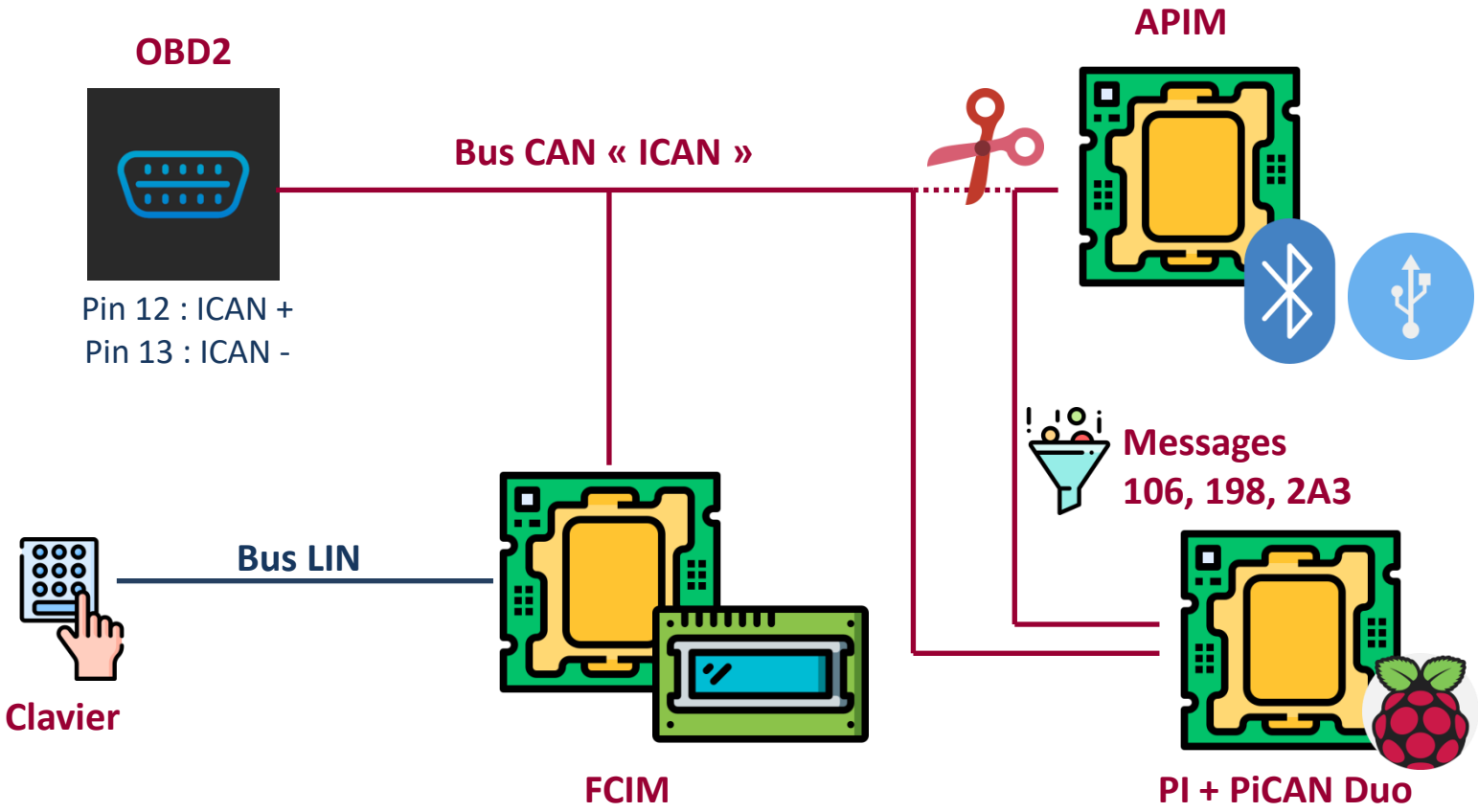
Acquittement demande :

197 [8] A4 01 01 00 00 00 00 00 — **FDIM**

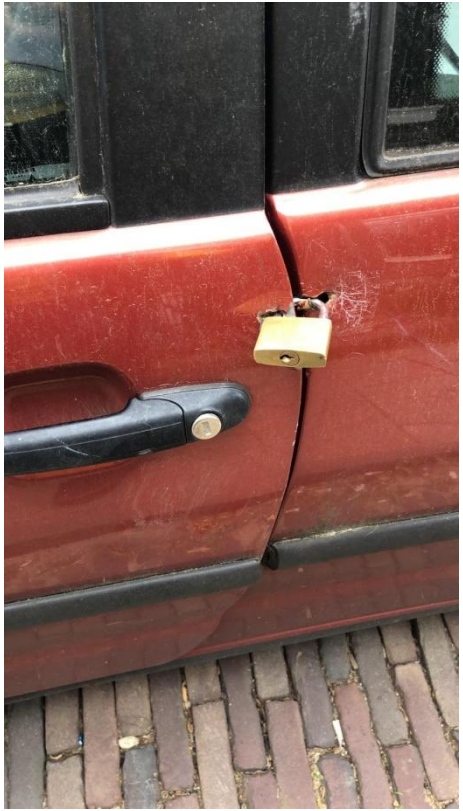
Message à afficher :

2CD [8] 10 25 DC 01 00 48 65 6C — **APIM**

POC


OBD2
Pin 12 : ICAN +
Pin 13 : ICAN -
Bus CAN « ICAN »
APIM
Messages
106, 198, 2A3
Bus LIN
Clavier
FCIM
PI + PiCAN Duo

La serrure, la seule sécurité ?



Comment accéder à l'habitacle ?

Ingénierie sociale :
Flotte de société

Crochetage :
Lishi & co

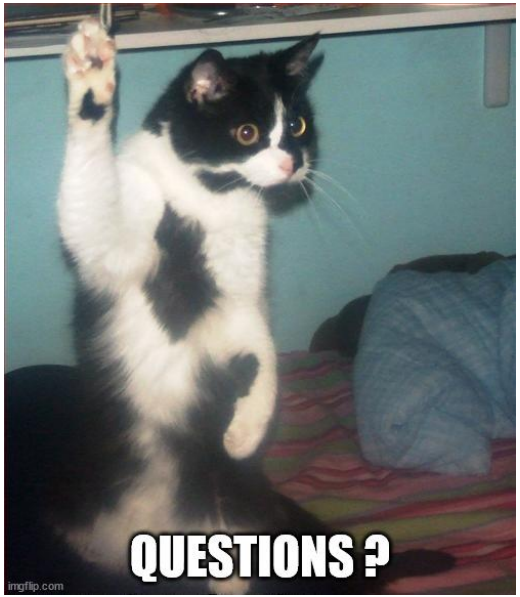
Rolljam:
Brouillage / rejeu de la télécommande

Bus CAN :
Envoi de trames sur le bus HS via un faisceau « accessible »

Démo !

Q & R

MERCI !



@Phil_BARR3TT

Pour en savoir plus :

Car Hacking Village : https://www.carhackingvillage.com/

Car Hacker Handbook : http://opengarages.org/handbook/

Illmatics – adventure in car hacking : http://illmatics.com/carhacking.html