XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectivas

Car Hacking
sobre CAN BUS

ccn-cert
centro criptológico nacional

- Jordi Serra Ruiz
- Universitat Oberta de Catalunya y CYBERCAT Barcelona
- jserrai@uoc.edu

- Amador Aparicio de la Fuente
- Centro de FP Salesianos de Villamuriel (PALENCIA).
- amador@4ck.es

Índice

1. Inicios del Car Hacking.

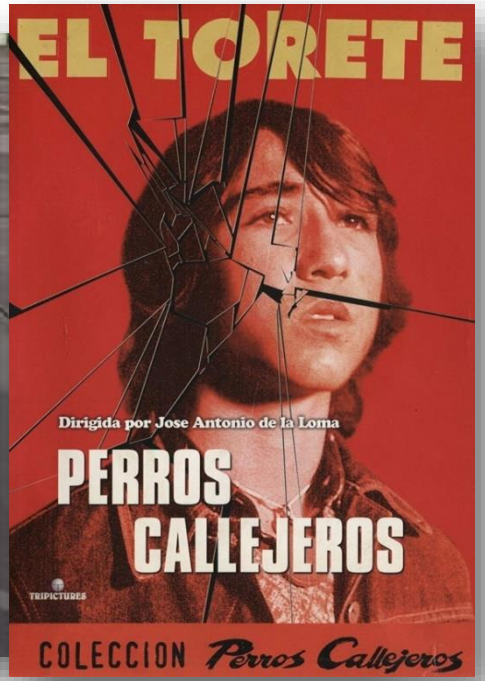
2. Vectores de Ataque.

3. Protocolo CAN Bus.

4. OBD2.

5. Ataques a redes CAN en vehículos.

Inicios del Car Hacking



Inicios del Car Hacking

Social Hacking

Identificación de vectores de ataque

Ataque de intrusión por fuerza bruta

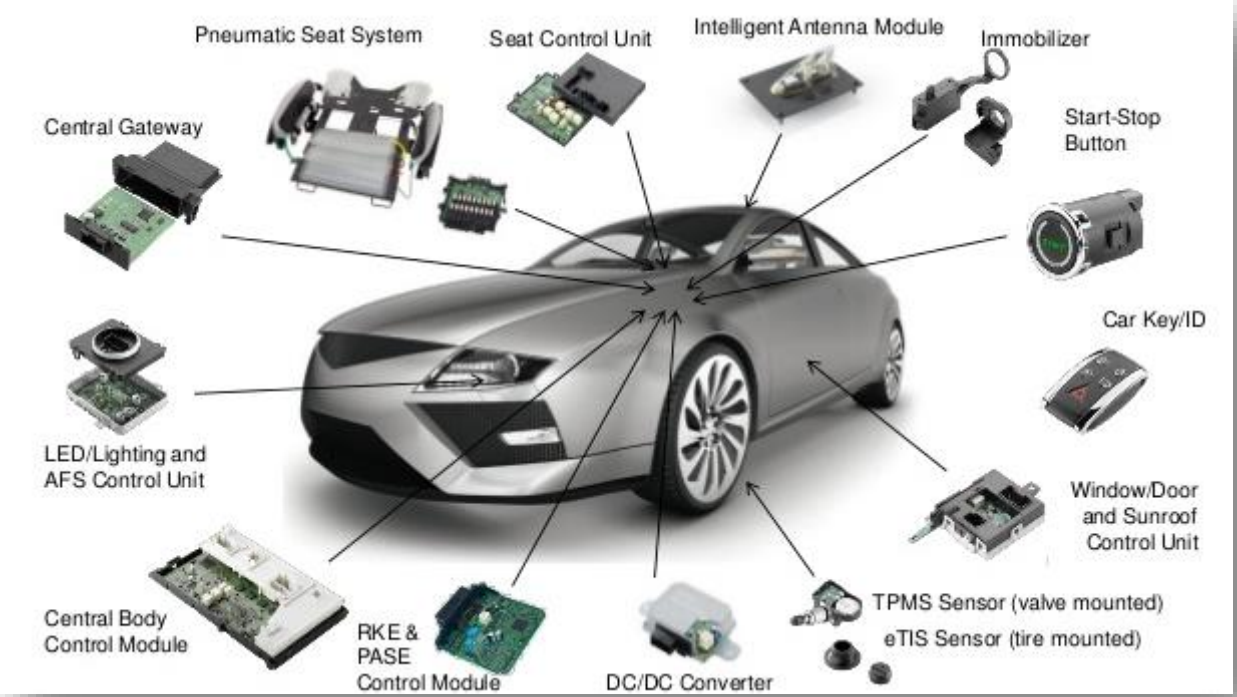
Técnicas anti-IDS

Bypass del Firewall

Buscando el CAN BUS!!

Inyectando tramas

Nuevos Vectores de Ataque



Robo por transmisión de señal de llave

Amplificadores y repetidores
de radiofrecuencia

Robo por transmisión de señal de llave

Protocolo CAN Bus

- Bosch, 1986, Controller Area Network (CAN) serial bus system at the Society of Automotive Engineers (SAE) congress.
- En 1987 Intel crea el primer CHIP para el Bus Can: 82526.
- En 2003 crean la primera ISO-11898, que actualizan en 2015.
- Los coches actuales tienen entre 70 y 100 ECUs.

Protocolo CAN Bus

- Usado en entornos con mucho ruido (interferencias).
- Disminución de cables en Automóviles.

  Par trenzado (interferencias).
- Dos señales diferenciales.

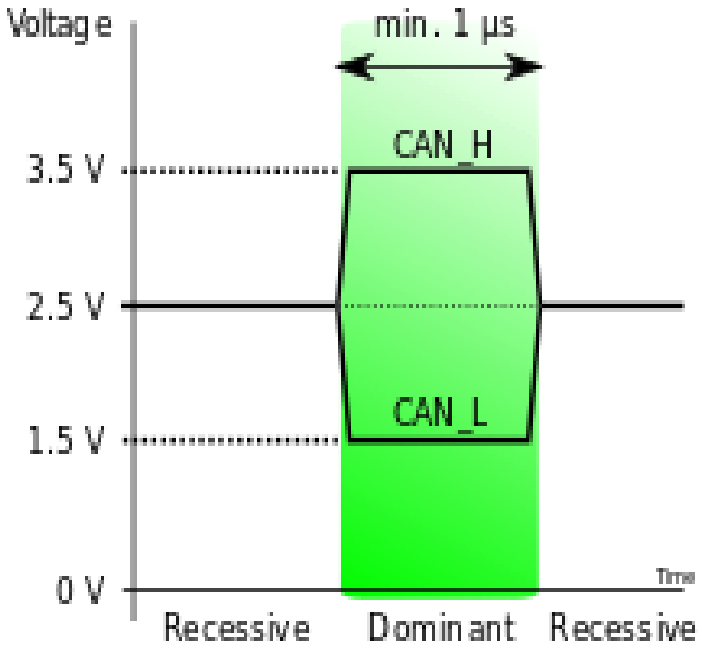
  Can-H y Can-L
- Comunicación entre sensores y actuadores.

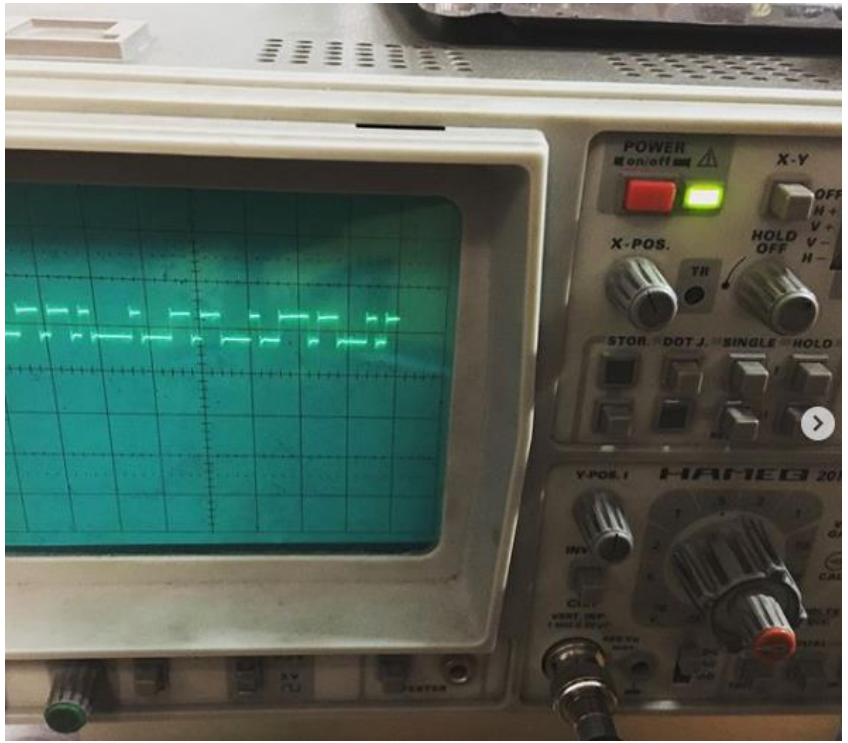
  Tramas de datos

Protocolo CAN Bus

Protocolo CAN Bus

Señal CAN Bus

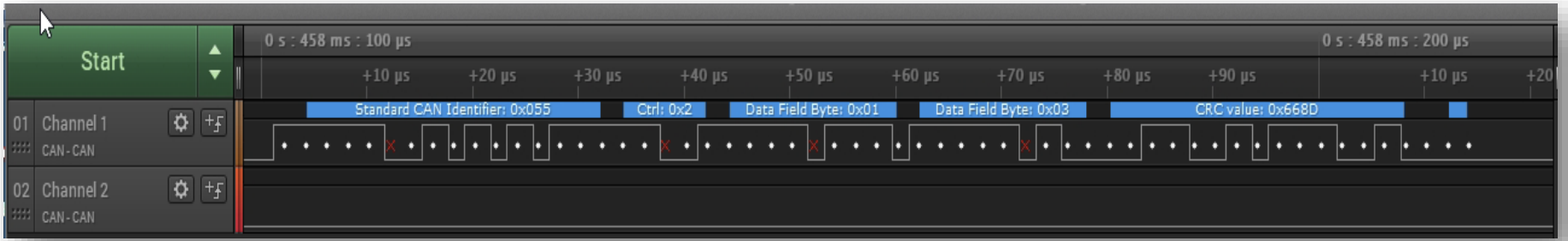




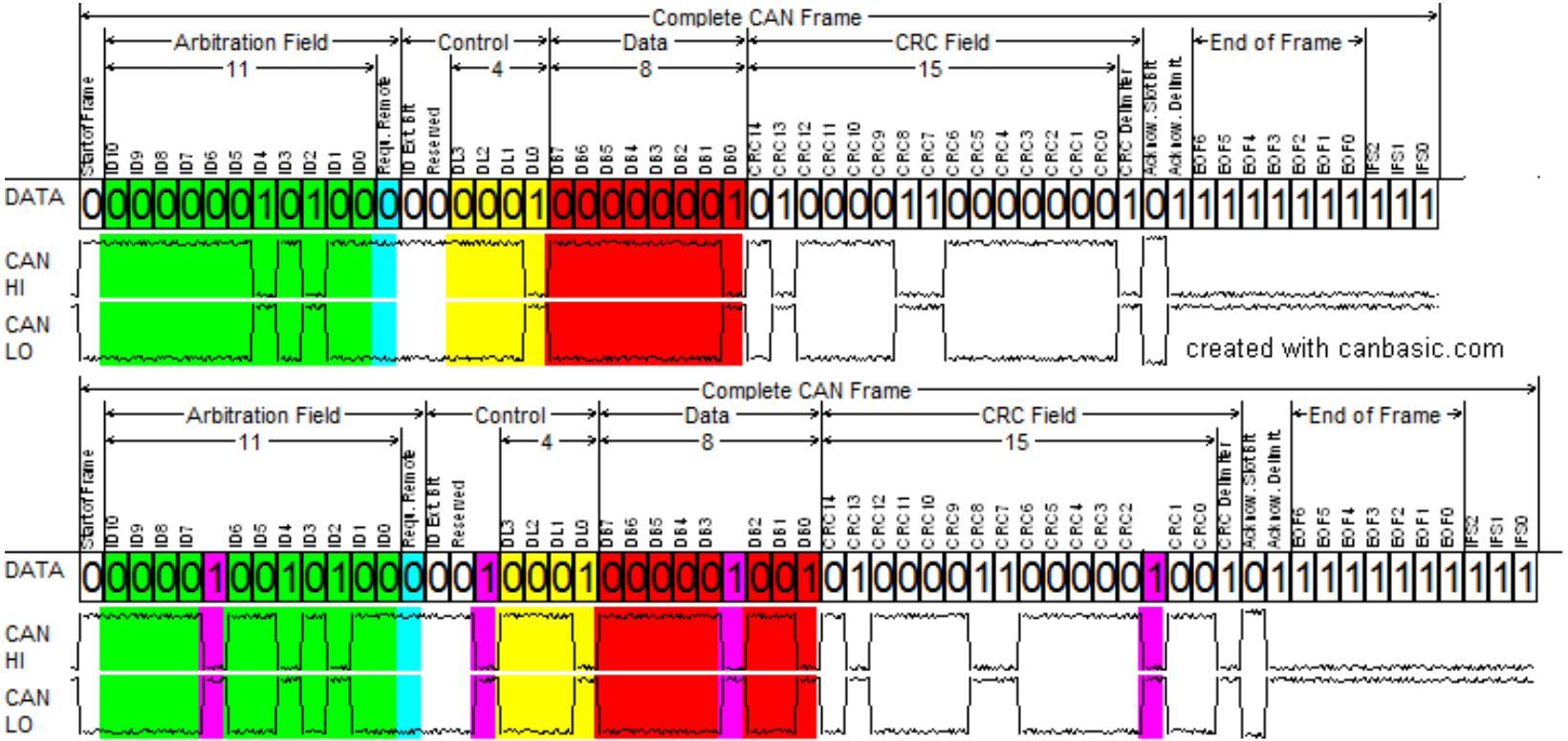
Tramas CAN Bus

- Las tramas viajan en texto plano.
- Las tramas tienen los siguientes campos interesantes:
  - ID: identificador de la trama
  - DLC: cantidad de bytes de información
  - DATA: datos presentes en la trama
  - CRC: código para detectar errores
- Implementa “bit stuffing”

Tramas CAN Bus



Tramas CAN Bus



OBD2 - On Board Diagnosis

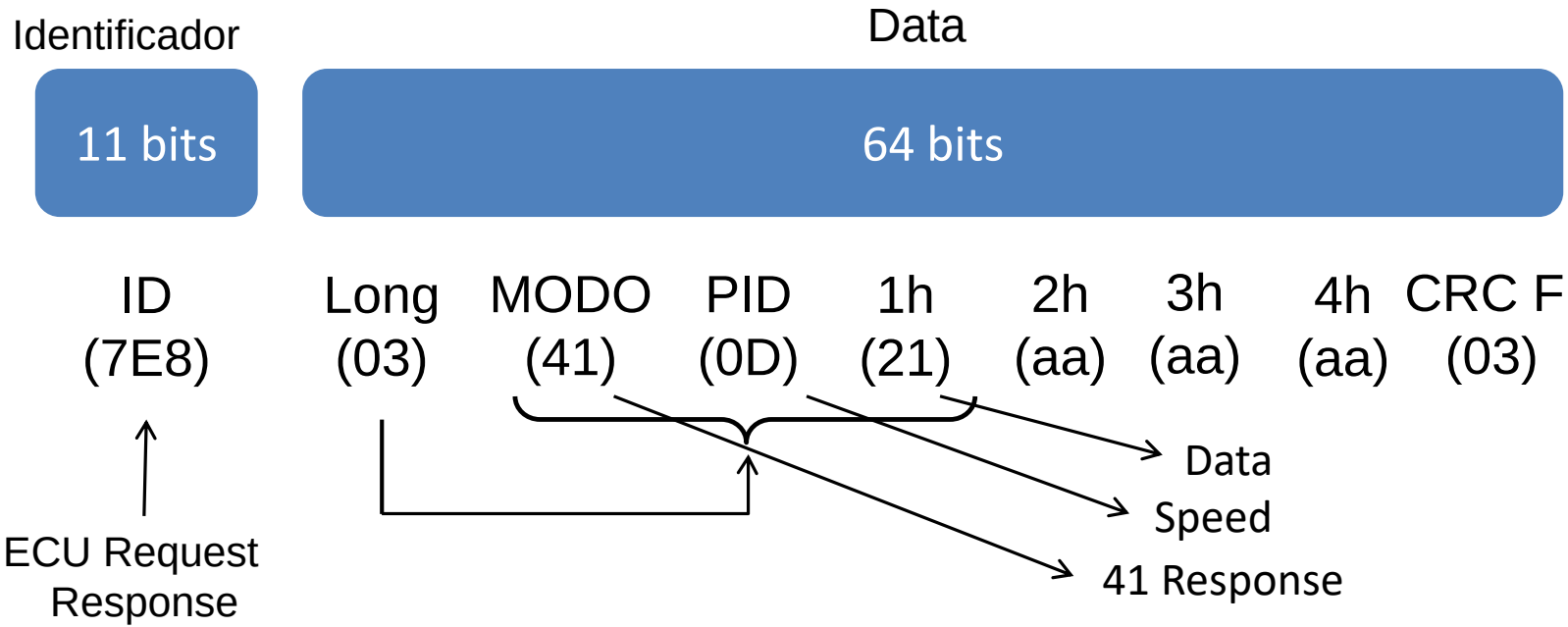
REQUEST EXAMPLE

```
7E0 02 01 0D 55 55 55 55 55
```

RESPONSE EXAMPLE

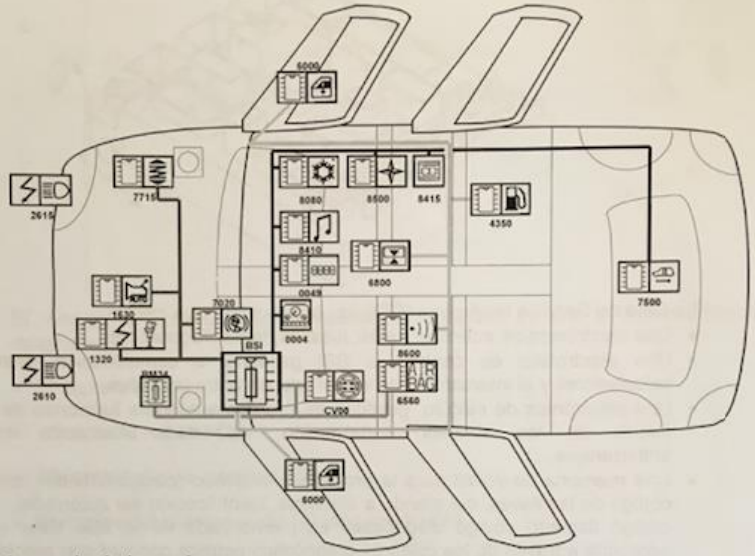
```
7E8 03 41 0D 21 aa aa aa aa
```

OBD2 - On Board Diagnosis

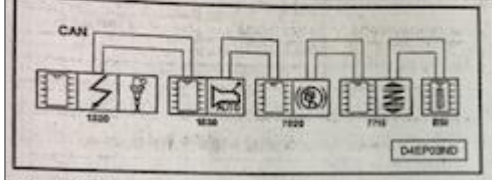


Redes internas del Vehículo

III - ARQUITECTURA MULTIPLEXADA DEL VEHICULO E IMPLANTACION DE LOS CALCULADORES

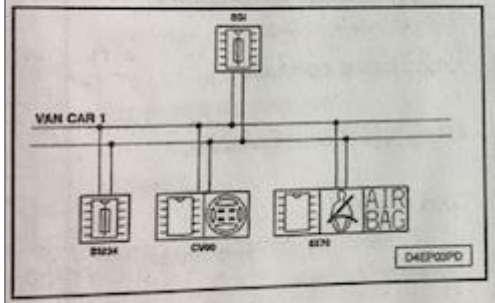


Sinóptico de la arquitectura red

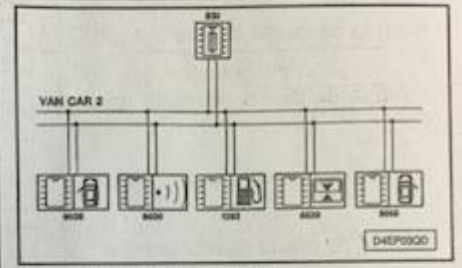


Red CAN.

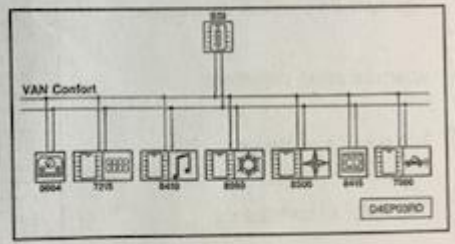
NOTA.- VAN (Vehicle Area Network).



Red VAN CARROCERÍA 1.



Red VAN CARROCERÍA 2.



Red VAN CONFORT.

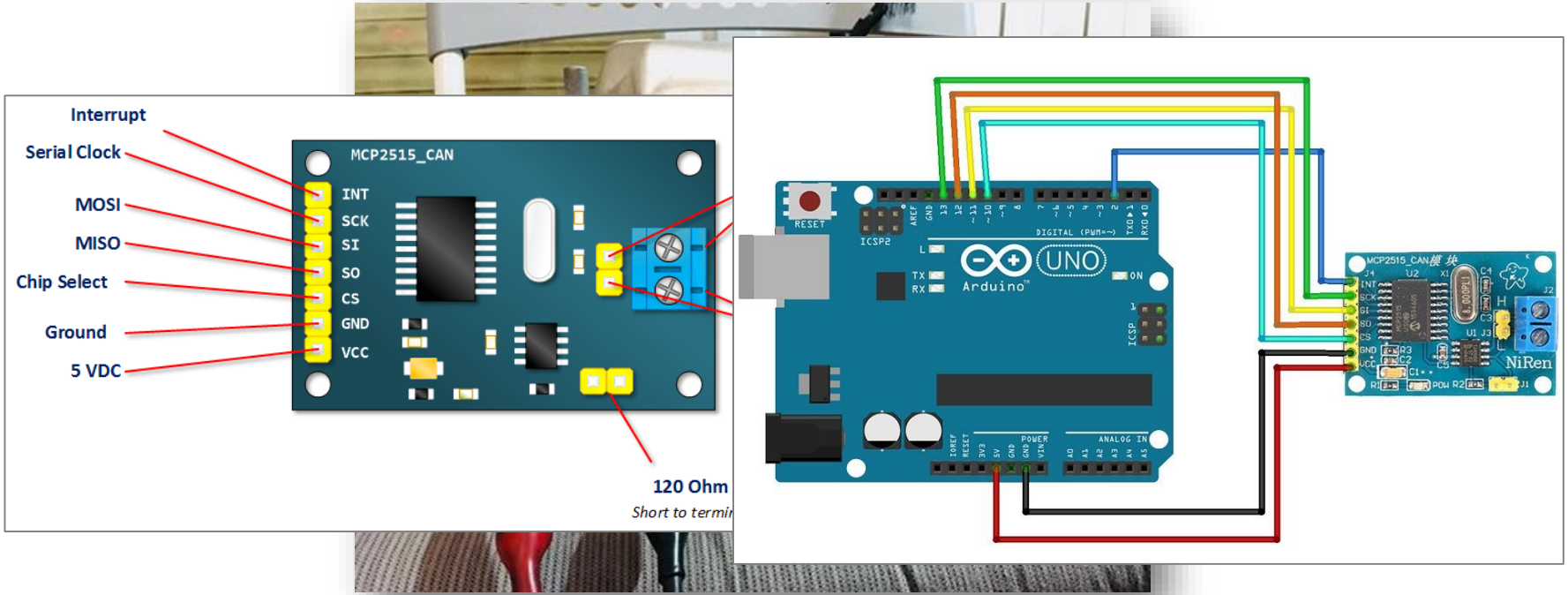
Trama	ID	Total	%
Tramas del Sensor de oxígeno 5 A: Voltaje, B: Ajuste de combustible a corto plazo	0x18	312	18.91 %
Tramas del Estado del aire secundario controlador	0x12	204	12.36 %
Tramas del Sensor de oxígeno 6 AB: Relación equivalente de combustible - aire CD: Voltaje	0x29	204	12.36 %
Tramas del Sensor de oxígeno 2 AB: Relación equivalente de combustible - aire CD: Actual	0x35	120	7.27 %
Tramas de RPM del motor	0x0C	104	6.30 %
Tramas del Tiempo desde que se puso en marcha el motor	0x1F	104	6.30 %
Tramas de la Distancia recorrida con la luz indicadora de falla (Malfunction Indicator Lamp, MI	0x21	102	6.18 %
Tramas del Sensor de oxígeno 1 AB: Relación equivalente de combustible - aire CD: Voltaje	0x24	102	6.18 %
Tramas de la Velocidad del combustible del motor	0x5E	62	3.76 %
Tramas de la Sincronización de la inyección de combustible	0x5D	50	3.03 %
Tramas del Sensor de oxígeno 6 AB: Relación equivalente de combustible - aire CD: Actual	0x39	41	2.48 %
Tramas del Sensor de flujo de aire masivo	0x66	31	1.88 %
Tramas de la Temperatura del enfriador del motor	0x67	31	1.88 %
Tramas de Presión de entrada del compresor del turbocargador	0x6F	31	1.88 %
Tramas del valor máximo de la relación de equivalencia de combustible - aire, voltaje del sen:	0x4F	20	1.21 %
Tramas del Valor máximo de la velocidad de flujo de aire del sensor de flujo de aire masivo	0x50	20	1.21 %
Tramas de la presión absoluta del vapor del sistema de evaporación	0x53	20	1.21 %
Tramas de la Velocidad del combustible del motor: 10	0x55	20	1.21 %
Tramas del Sensor de temperatura de aire de entrada	0x68	20	1.21 %
Tramas de Ajuste del sensor de oxígeno secundario de plazo largo. A: banco 1. B: banco 3	0x56	11	0.67 %
Tramas del Porcentaje de torque actual del motor	0x62	11	0.67 %
Tramas de Tipo de combustible	0x51	10	0.61 %
Tramas del Ajuste del sensor de oxígeno secundario de plazo largo. A: banco 2. B: banco 4	0x58	10	0.61 %
Tramas de la Entrada / salida auxiliar implementada	0x65	10	0.61 %
TOTAL		1650	100.00 %

Primera Tentativa

- ECU (Engine Control Unit)

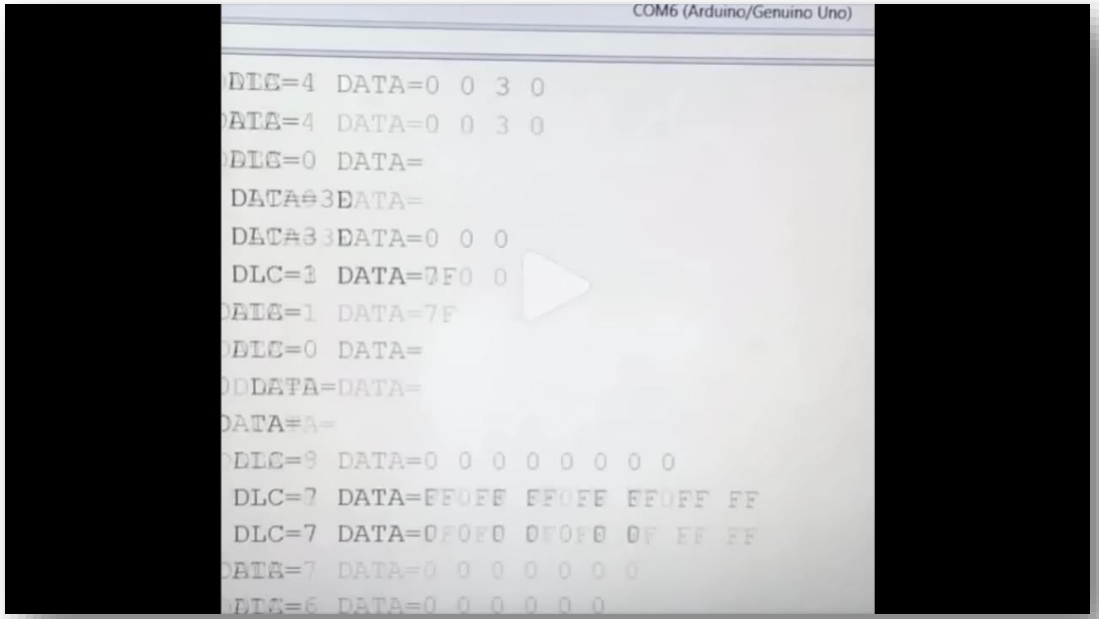
Primera Tentativa

- Obtención de Tramas de la ECU.



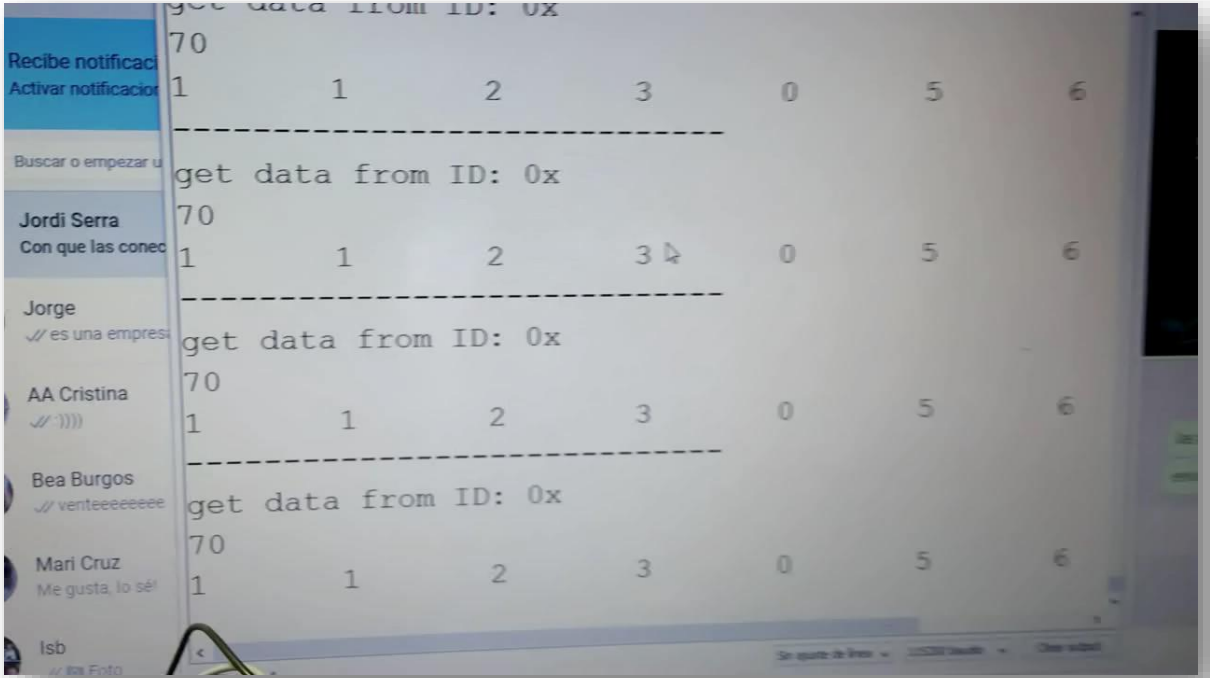
Primera Tentativa

- Obtención de Tramas de la ECU.

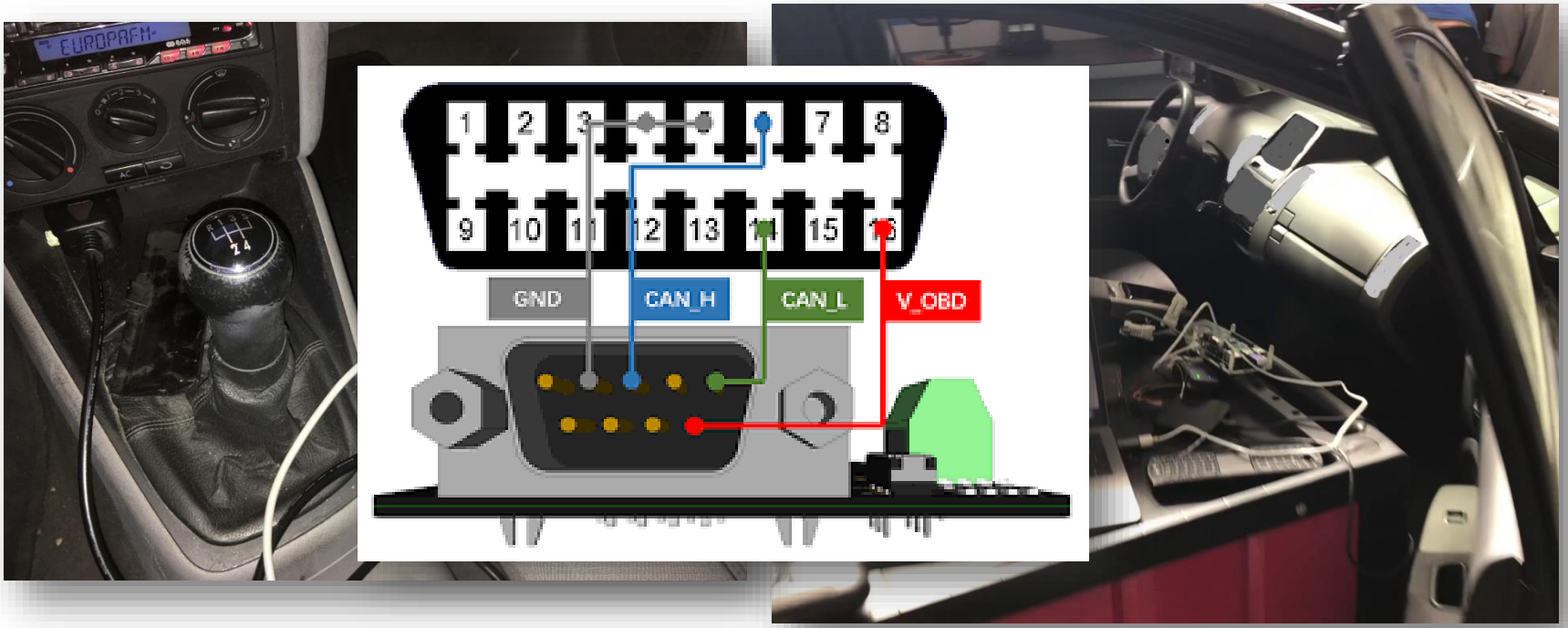


Segunda Tentativa

- Construcción de una red CAN Bus con dos nodos.



Sniffing de Tramas CAN BUS en un coche real



Sniffing de Tramas CAN BUS en un coche real

Inyección de tramas CAN BUS en un coche real

Inyección de tramas CAN BUS en un coche real

XII Jornadas STIC CCN-CERT

Ciberseguridad, hacia una respuesta y disuasión efectivas

- **E-Mails**
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - oc.ccn.cni.es
- **Síguenos en**

centro criptológico nacional