

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

By
@unapibageek and @cholesec



HITBSecConf

Who we are?
And
Where we are from?







When we start
with this?



Illegal (or maybe not)

WILHELM

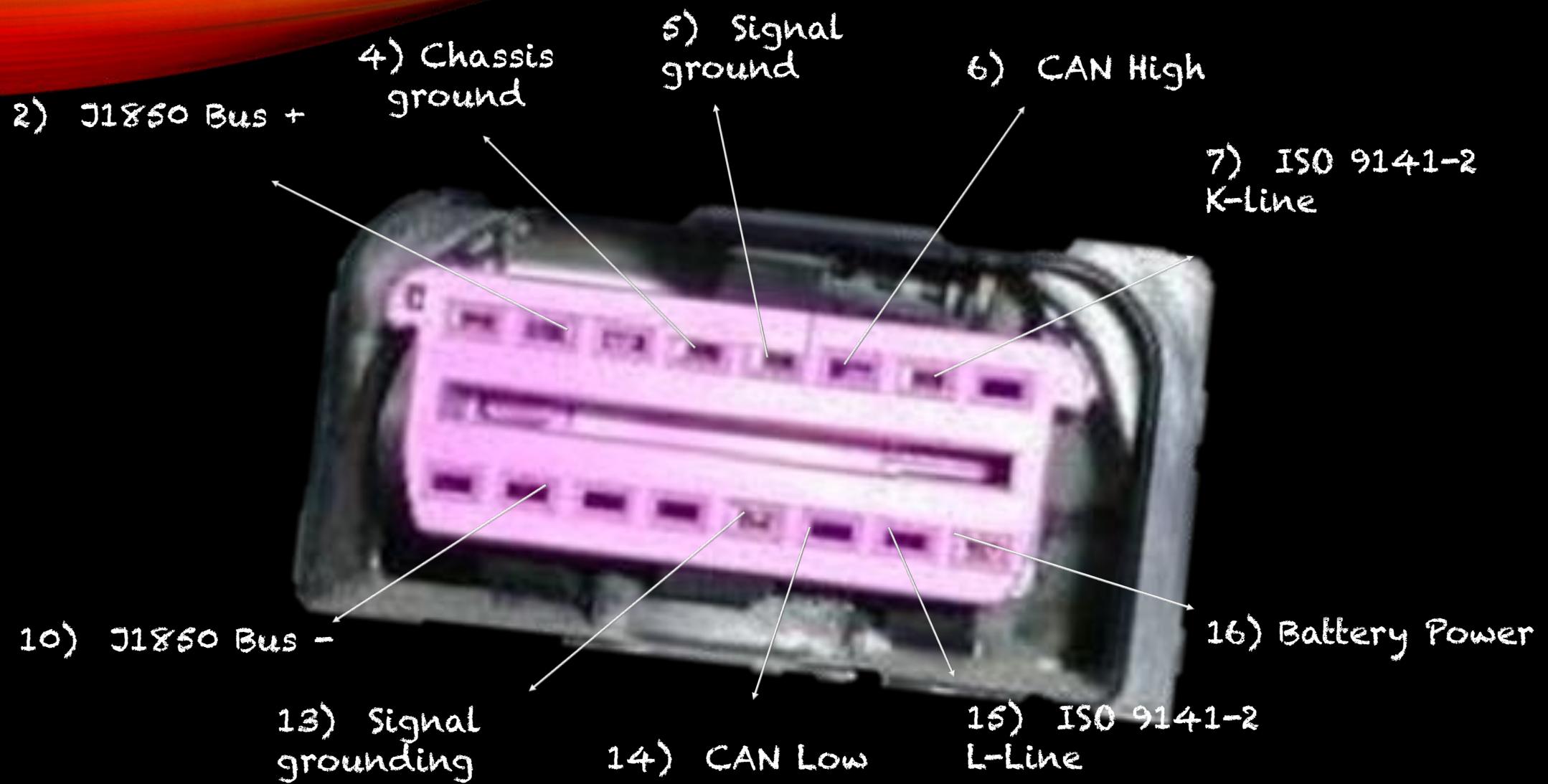


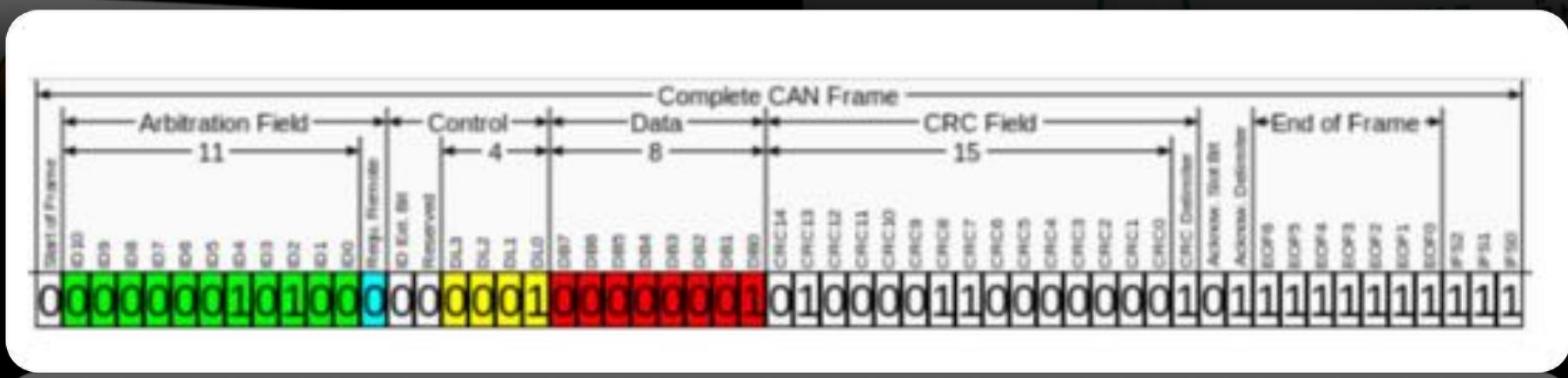
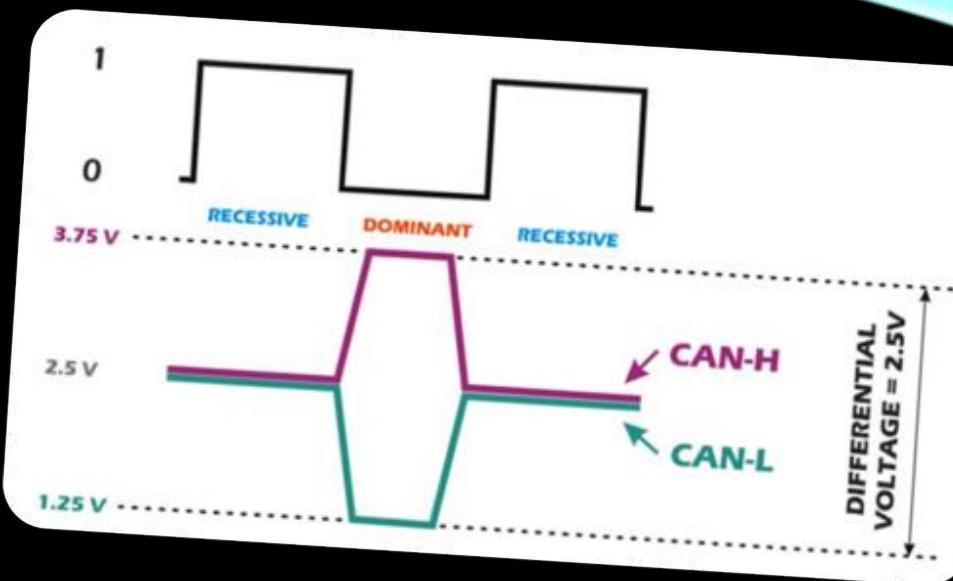
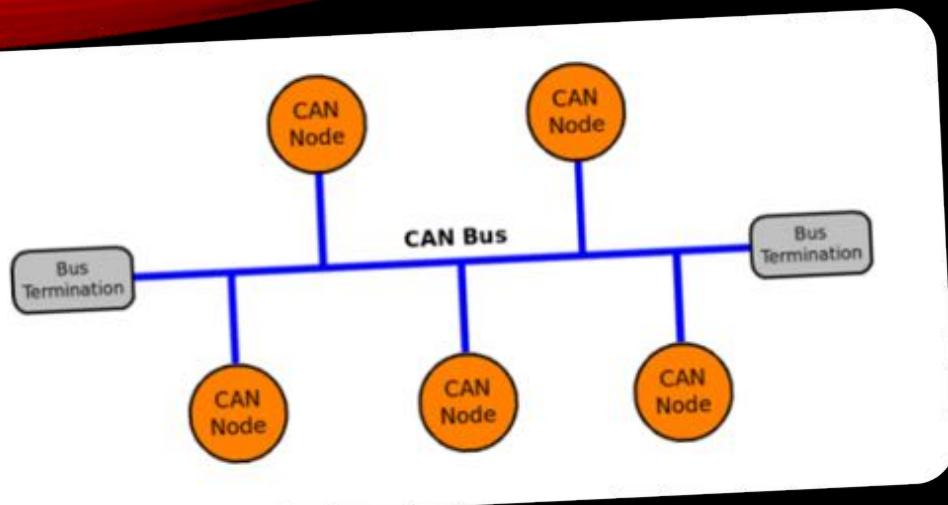






A quick reviews





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



CAN BUS Analyzer

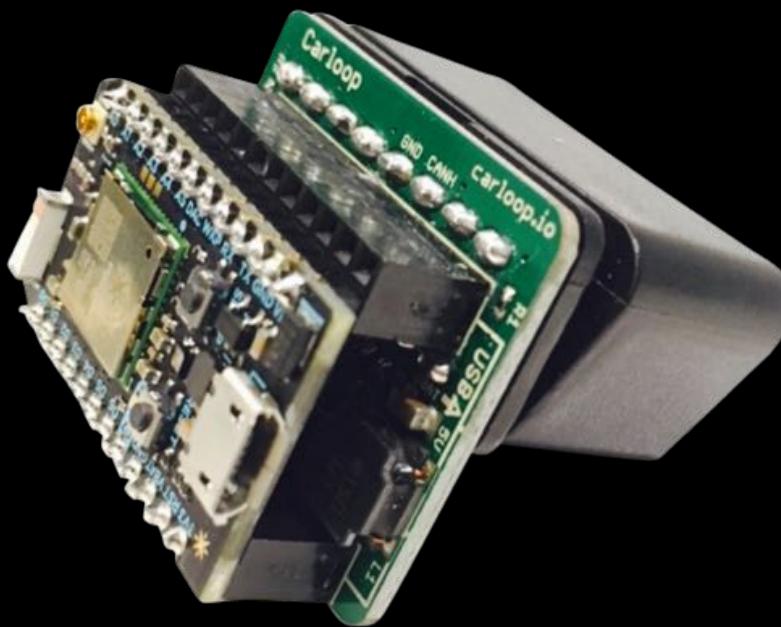
File View Tools Setup Help

Recent Trace

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	0.029	24713
RX	0x5C5	8	0x40	0x00	0x2E	0xC3	0x06	0xFC	0x00	0x53	507.0082	0.099	4987
RX	0x284	8	0x00	0x00	0x00	0x00	0x00	0x00	0xCB	0x51	507.0112	0.029	24749
RX	0x285	8	0x00	0x00	0x00	0x00	0x00	0x00	0xCB	0x52	507.0112	0.029	24702
RX	0x212	6	0x00	0x00	0x00	0x00	0x00	0x0C			507.0172	0.029	24830
RX	0x354	8	0x00	0x00	0x00	0x00	0x00	0x00	0x04	0x00	506.9912	0.049	12330
RX	0x215	6	0x31	0x00	0x00	0x0A	0x11	0x00			507.0172	0.029	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	0xE0	0x30	0xA3	0x3A	0x22	0x00	0x00	506.9992	0.099	4963
RX	0x600	8	0x44	0x16	0x00	0x00	0x3F	0x52	0x02	0x00	506.9202	0.100	5174
RX	0x625	6	0x82	0x40	0xE8	0x11	0x00	0x00			506.9383	0.100	4960
RX	0x526	6	0x80	0x00	0x10	0x00	0x0A	0x40			506.9392	0.101	4944
RX	0x6F8	5	0x00	0x00	0x00	0x02	0xFF				506.9392	0.100	4964
RX	0x350	8	0x90	0x03	0x00	0x00	0x08	0x00	0x53	0x00	506.9892	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

FORMAT	ID	DLC	DATA 0	DATA 1	DATA 2	DATA 3	DATA 4	DATA 5	DATA 6	DATA 7	PERIOD (msec)	REPEAT	TRANSMIT	COUNTER
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	0x1C	0x00	0x00	0x3F	0x51	0x02	0x00	809.2122	0.099		8336
RX	0x625	6	0x82	0x00	0xC8	0x31	0x00	0x00			809.2672	0.100		7984
RX	0x625	6	0x80	0x00	0x10	0x00	0x5A	0x40			809.2672	0.100		7970
RX	0x5F8	5	0x00	0x00	0x00	0x02	0xFF				809.2672	0.099		7989
RX	0x150	8	0x30	0x03	0x00	0x00	0x08	0x00	0x53	0x00	809.2822	0.100		7987

ToolConnected

500 Kbps

Tx Name

TX (ERR: 0) RX (ERR: 0) Termination: ON Trace Active Logging Inactive ID in HEX DATA in HEX

Tool Connected

200 Kbps

Run Mon

TX (ERR: 0) RX (ERR: 0) NO: baudrate Termination: ON Trace Active Logging Inactive ID in HEX DATA in HEX

RX

18

0x20

0x03

0x00

0x00

0x08

0x00

0x23

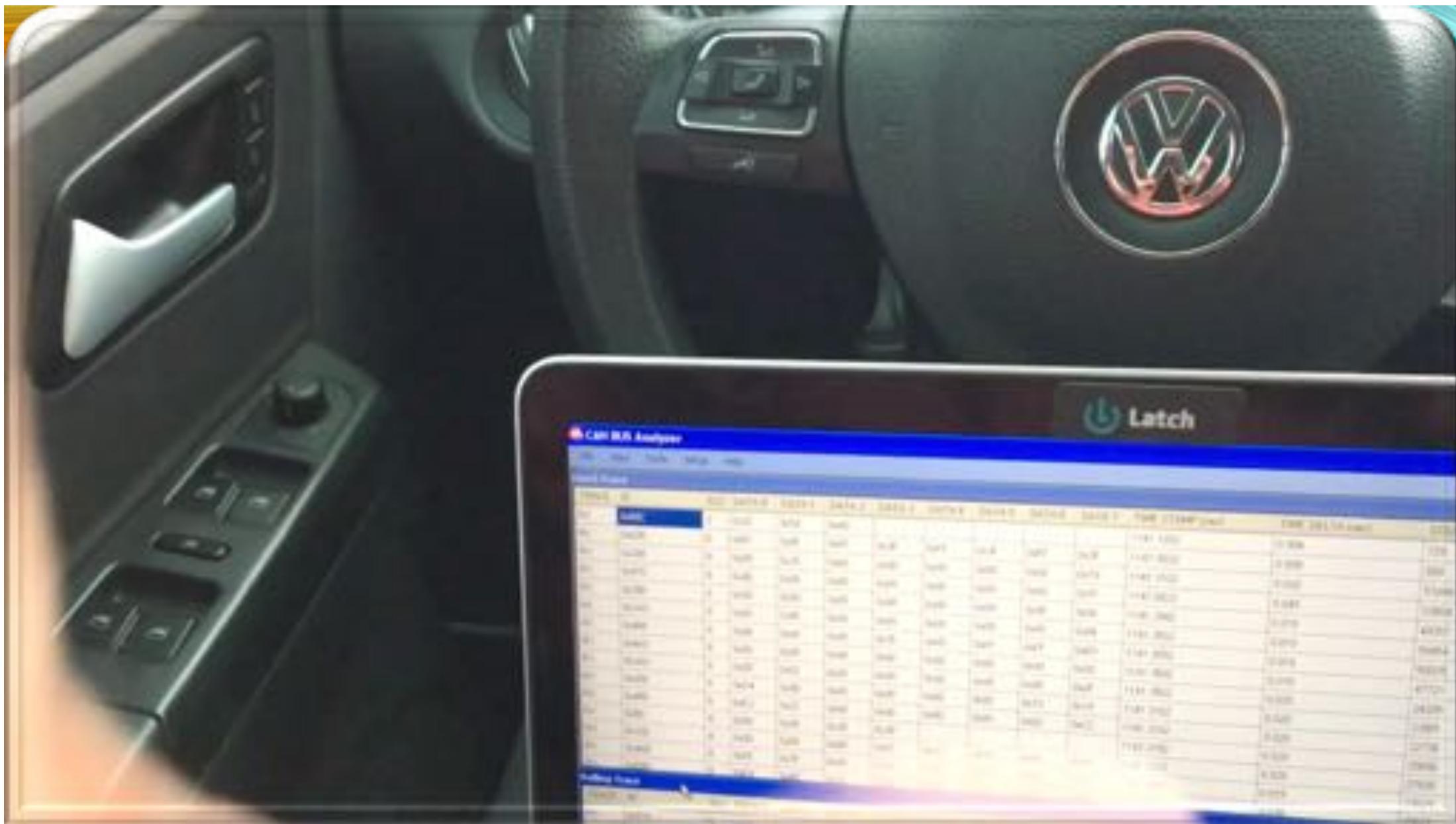
0x00

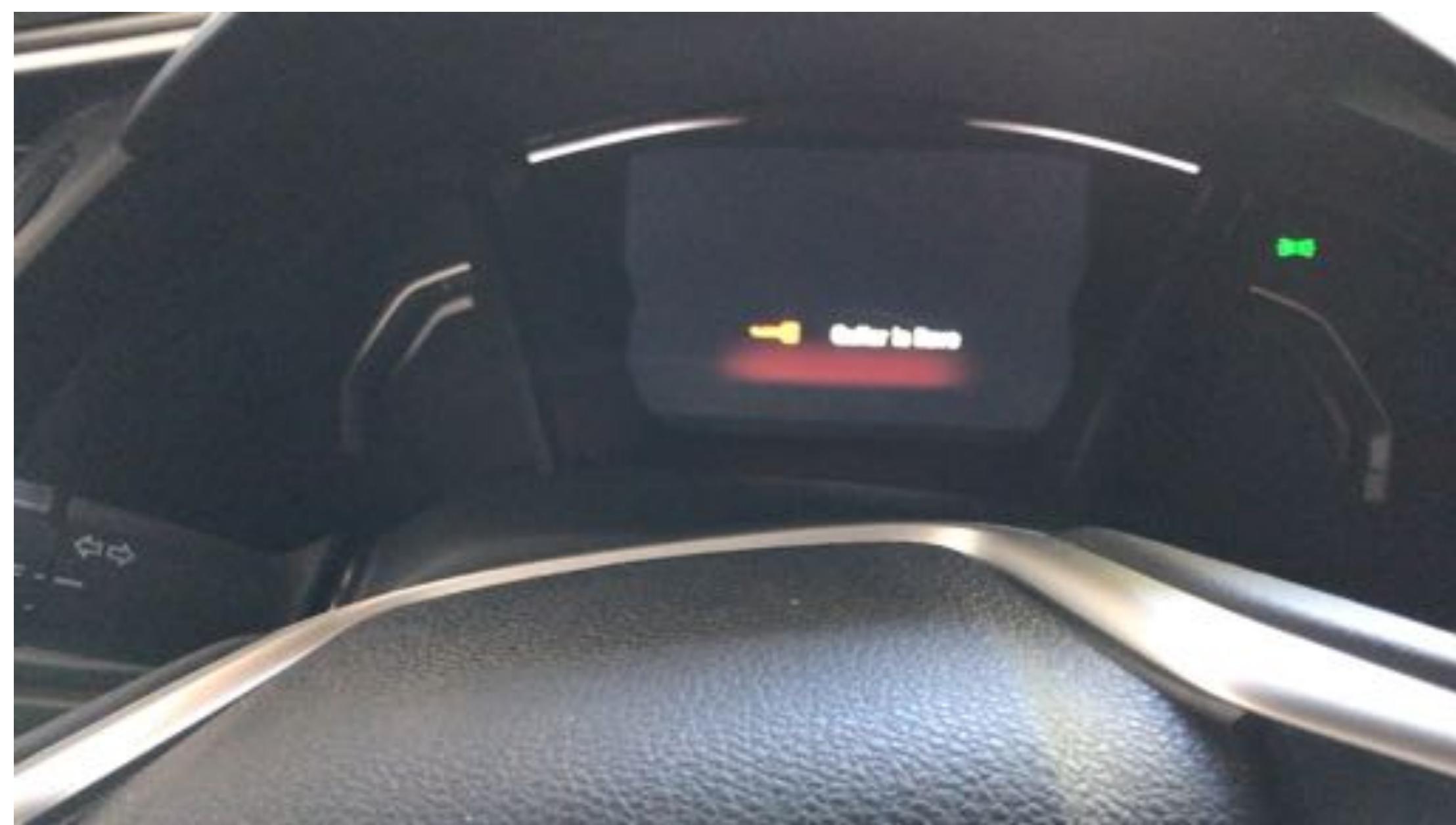
809.2822

0.100

1221





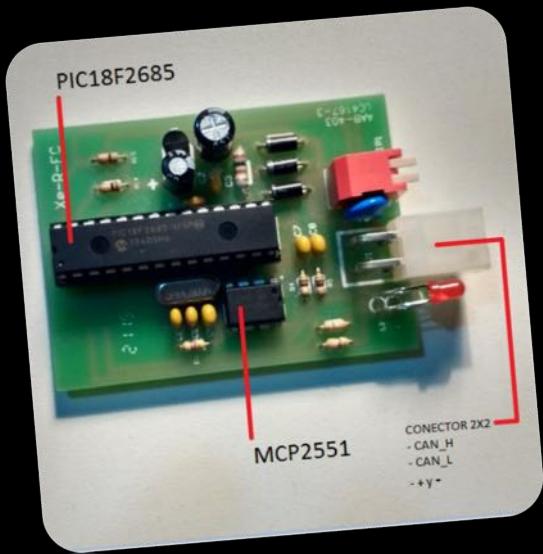


Backdooring
the CAN bus
for remote car control



NO ESEN



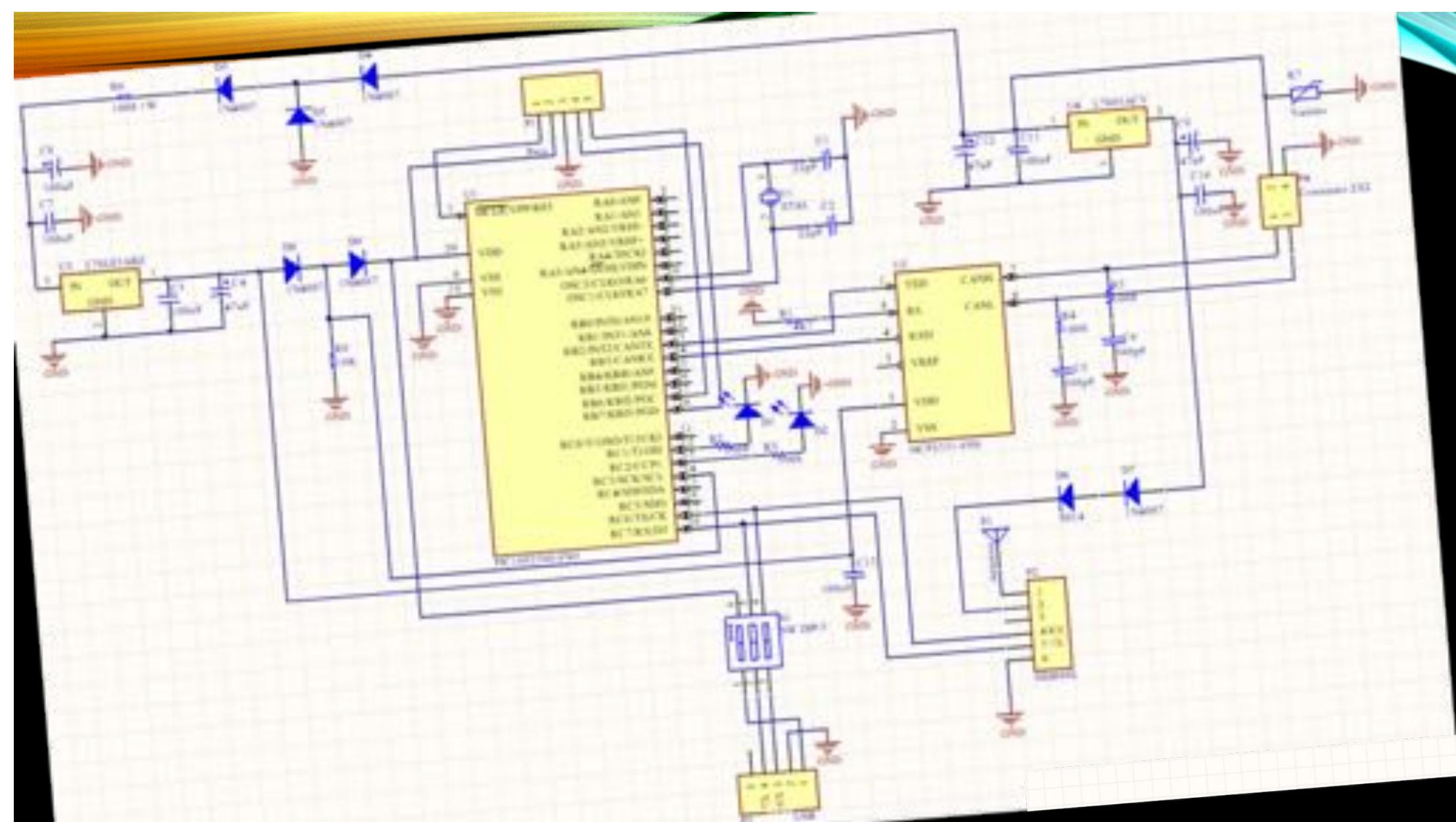


Version 1

FNGIN

190
197
198
199
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323





```
312 ;*****  
313 ;USART RECEPTION SUBROUTINE  
314 ;*****  
315  
316 VERDAT
```

MODO HACK (VERDATOS).

```
2139    BSF      INTCON,PEIE      ;Activa interrupción de periféricos  
2140    BSF      INTCON,GIE      ;Activa interrupciones  
2141  
2142    BSF      IPRI1,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



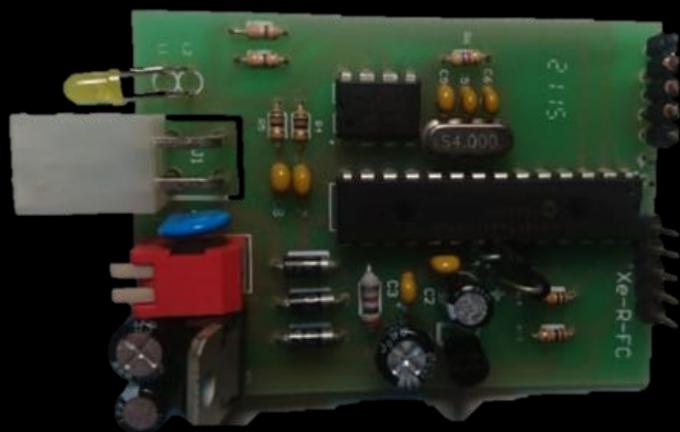
Version 2

For HITB Conference

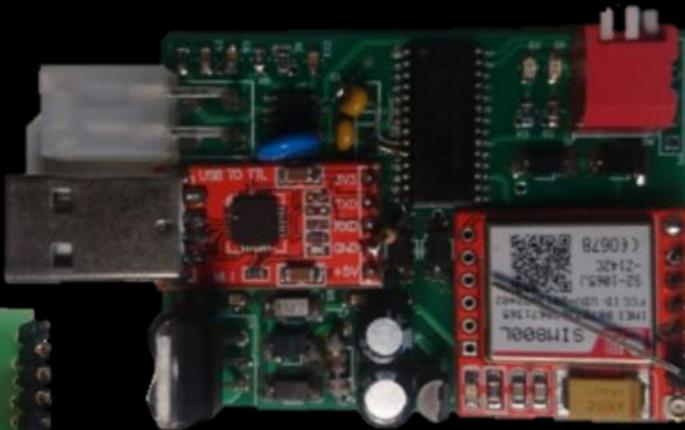


Version 3

The Evolution



Version 1



Version 2



Version 3



The added value

Car Backdoor Maker v1.0

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
2	60D	8	46	1E	00	00	43	4F	02	00
3	651	2	04	FO						CNON
4										
5										

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):

1
 2
 3

When the target passes near the following coordinates:

Latitude: -34.603465

Longitude: -58.381549

24%

24%

Car Backdoor Maker v1.0
By @UnaPharGeek - @holzzer

Status:

CONNECTED



Device:

Connect

Write

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): **3**

When the following frame is detected on CAN bus:

ID	DLC	-	1	2	3	4	5	6	7	8
161	8		90	03	00	00	18	00	53	00
match?:	<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): **3**

When the target passes near the following coordinates:

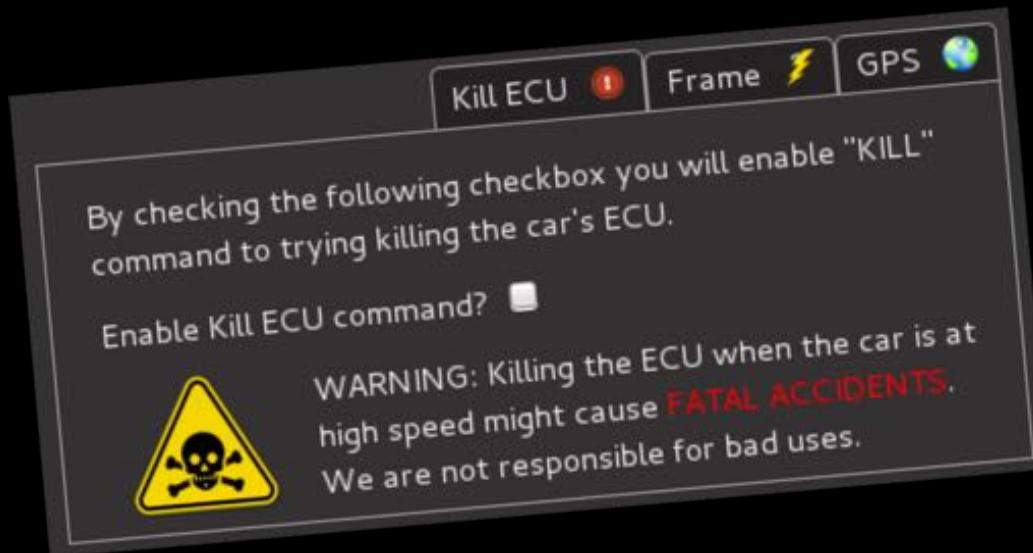
Latitude:

-34.603465

Longitude:

-58.381549

For HITB Conference





The WTF Things

Search

Brand

Model

Country/Regi...

Q. CAN FRAME



HOLESEC

LOGOUT

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)

your Car Model

Brand

Acura

I'm not a robot



your Vector

I'm not a robot



MIT VECTOR

New CAN frames



NOT VERIFIED

2017-09-27

from Argentina



NOT VERIFIED

2017-09-27

from Argentina



NOT VERIFIED

2017-09-27

from Argentina



NOT VERIFIED

2017-09-27

from Argentina

SHOW ALL

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
Berka
@unapibaGeek

Claudio
Caracciolo
@holesec