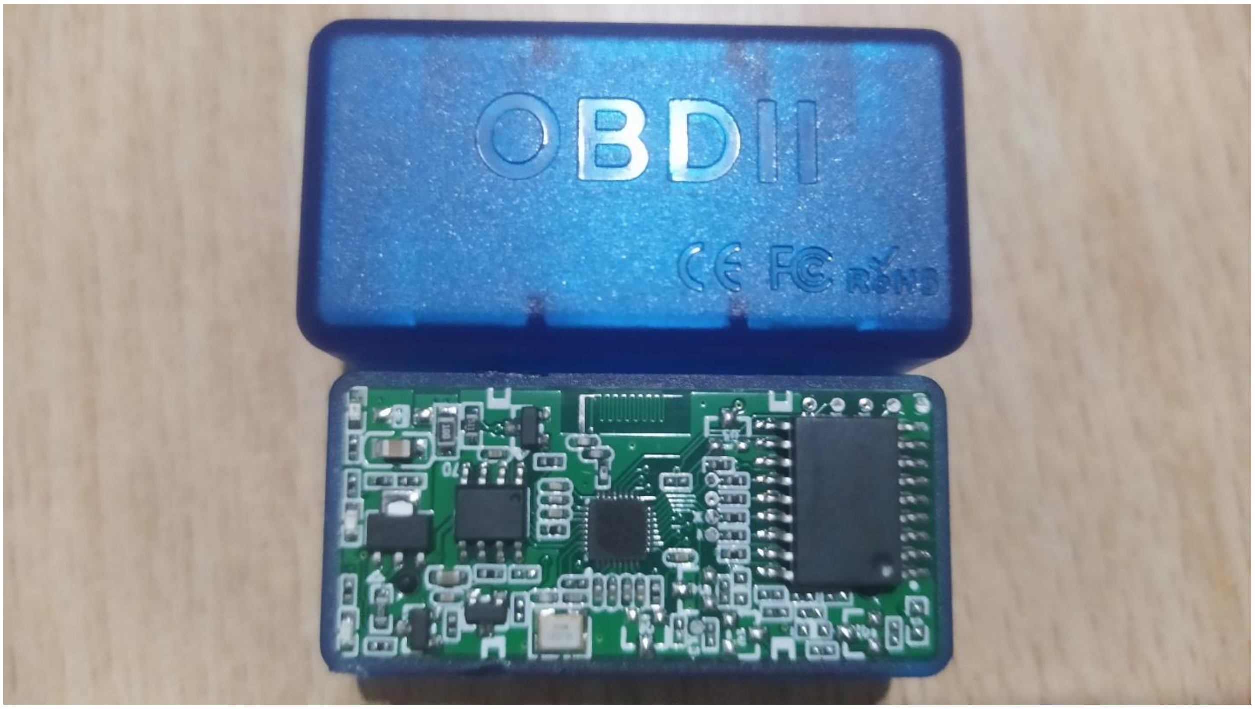
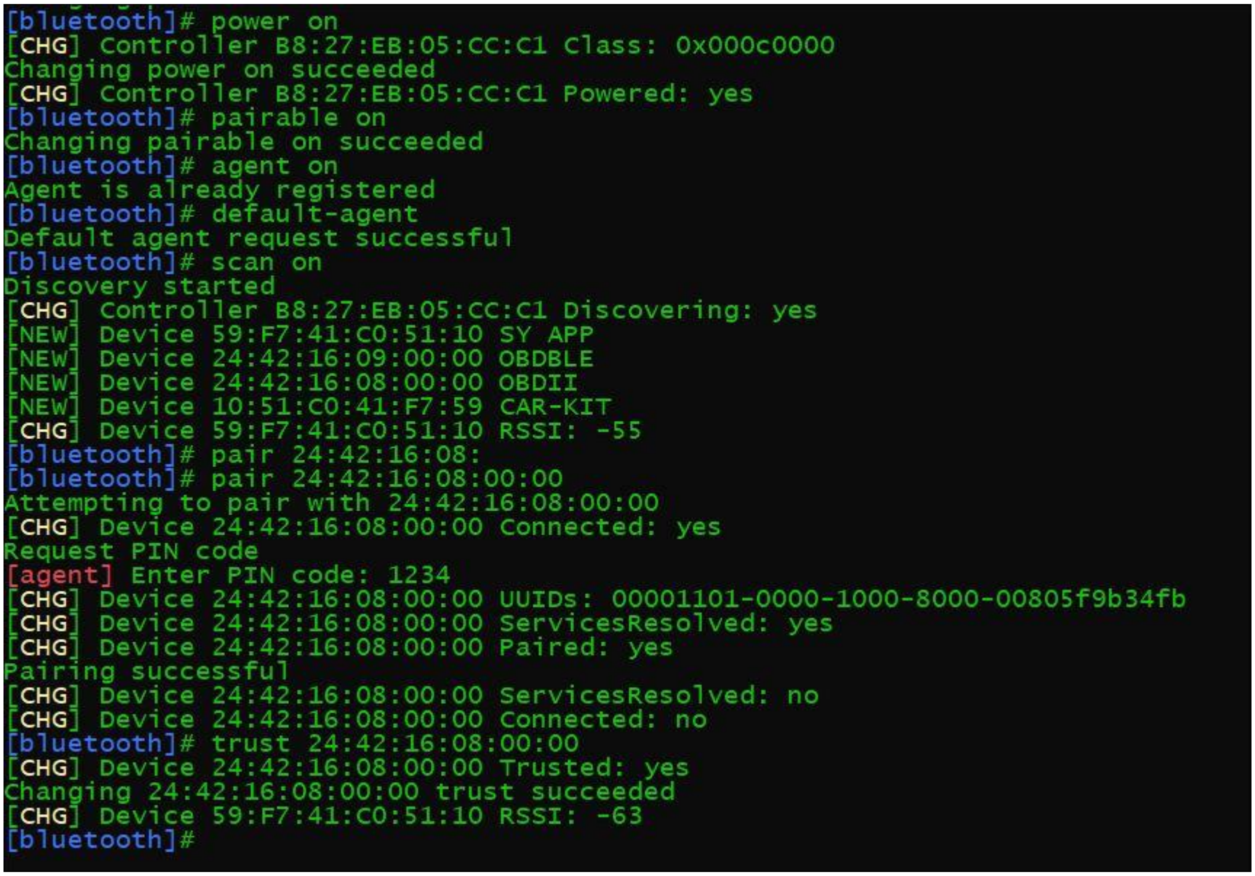
CAN-bus sniffing Using ELM327 mini OBD2 Bluetooth Module

Devices

- OBD dongle -> ELM 327 Bluetooth Adaptor
- Vehicle -> Honda City 2004
- Raspberry Pi 3 B+



First, I make Bluetooth communication between raspberry and ELM 327 Bluetooth module. I used “bluetoothctl” command.



```
[bluetooth]# power on
[CHG] Controller B8:27:EB:05:CC:C1 Class: 0x000c0000
Changing power on succeeded
[CHG] Controller B8:27:EB:05:CC:C1 Powered: yes
[bluetooth]# pairable on
Changing pairable on succeeded
[bluetooth]# agent on
Agent is already registered
[bluetooth]# default-agent
Default agent request successful
[bluetooth]# scan on
Discovery started
[CHG] Controller B8:27:EB:05:CC:C1 Discovering: yes
[NEW] Device 59:F7:41:C0:51:10 SY APP
[NEW] Device 24:42:16:09:00:00 OBDBLE
[NEW] Device 24:42:16:08:00:00 OBDII
[NEW] Device 10:51:C0:41:F7:59 CAR-KIT
[CHG] Device 59:F7:41:C0:51:10 RSSI: -55
[bluetooth]# pair 24:42:16:08:
[bluetooth]# pair 24:42:16:08:00:00
Attempting to pair with 24:42:16:08:00:00
[CHG] Device 24:42:16:08:00:00 Connected: yes
Request PIN code
[agent] Enter PIN code: 1234
[CHG] Device 24:42:16:08:00:00 UUIDs: 00001101-0000-1000-8000-00805f9b34fb
[CHG] Device 24:42:16:08:00:00 ServicesResolved: yes
[CHG] Device 24:42:16:08:00:00 Paired: yes
Pairing successful
[CHG] Device 24:42:16:08:00:00 ServicesResolved: no
[CHG] Device 24:42:16:08:00:00 Connected: no
[bluetooth]# trust 24:42:16:08:00:00
[CHG] Device 24:42:16:08:00:00 Trusted: yes
Changing 24:42:16:08:00:00 trust succeeded
[CHG] Device 59:F7:41:C0:51:10 RSSI: -63
[bluetooth]#
```

Next, I bind Bluetooth adaptor to serial port

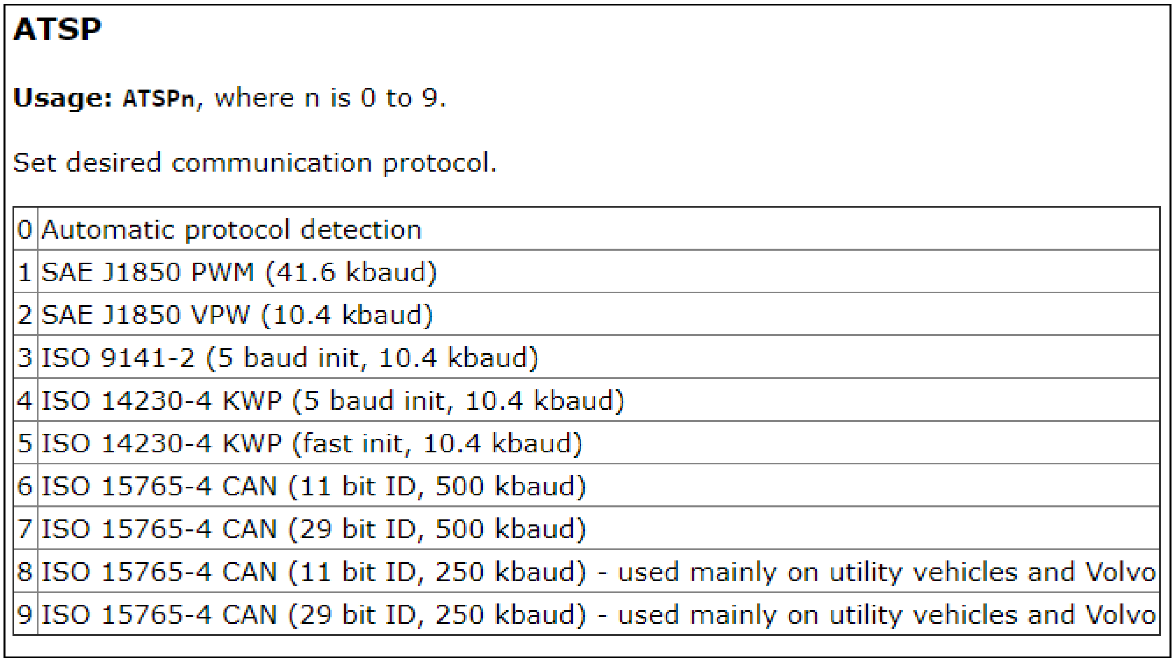
- sudo rfcomm bind rfcomm0 <OBD2 port mac address>

Communication processes I used “Screen” Software

- sudo apt-get install screen
- screen /dev/rfcomm0

I used ELM-USB OBD2 Interface commands For Communication. And I used following commands.

- atz --device ID
- atl1 -- line feed
- ath1 -- display header
- atsp -- how to communicate with port [atsp0 --automatic detections]



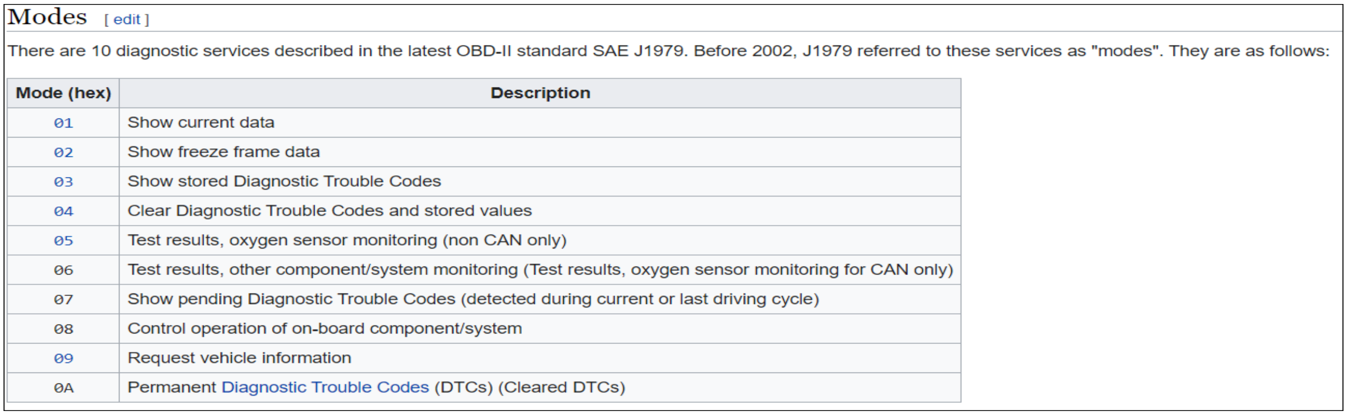
ATSP

Usage: **ATSPn**, where n is 0 to 9.

Set desired communication protocol.

0	Automatic protocol detection
1	SAE J1850 PWM (41.6 kbaud)
2	SAE J1850 VPW (10.4 kbaud)
3	ISO 9141-2 (5 baud init, 10.4 kbaud)
4	ISO 14230-4 KWP (5 baud init, 10.4 kbaud)
5	ISO 14230-4 KWP (fast init, 10.4 kbaud)
6	ISO 15765-4 CAN (11 bit ID, 500 kbaud)
7	ISO 15765-4 CAN (29 bit ID, 500 kbaud)
8	ISO 15765-4 CAN (11 bit ID, 250 kbaud) - used mainly on utility vehicles and Volvo
9	ISO 15765-4 CAN (29 bit ID, 250 kbaud) - used mainly on utility vehicles and Volvo

Next, I used OBD-2 Parameter IDs to request data from a vehicle, it contains 4 HEX values (FF FF). First 2 represents the mode, next 2 represents parameter ID.

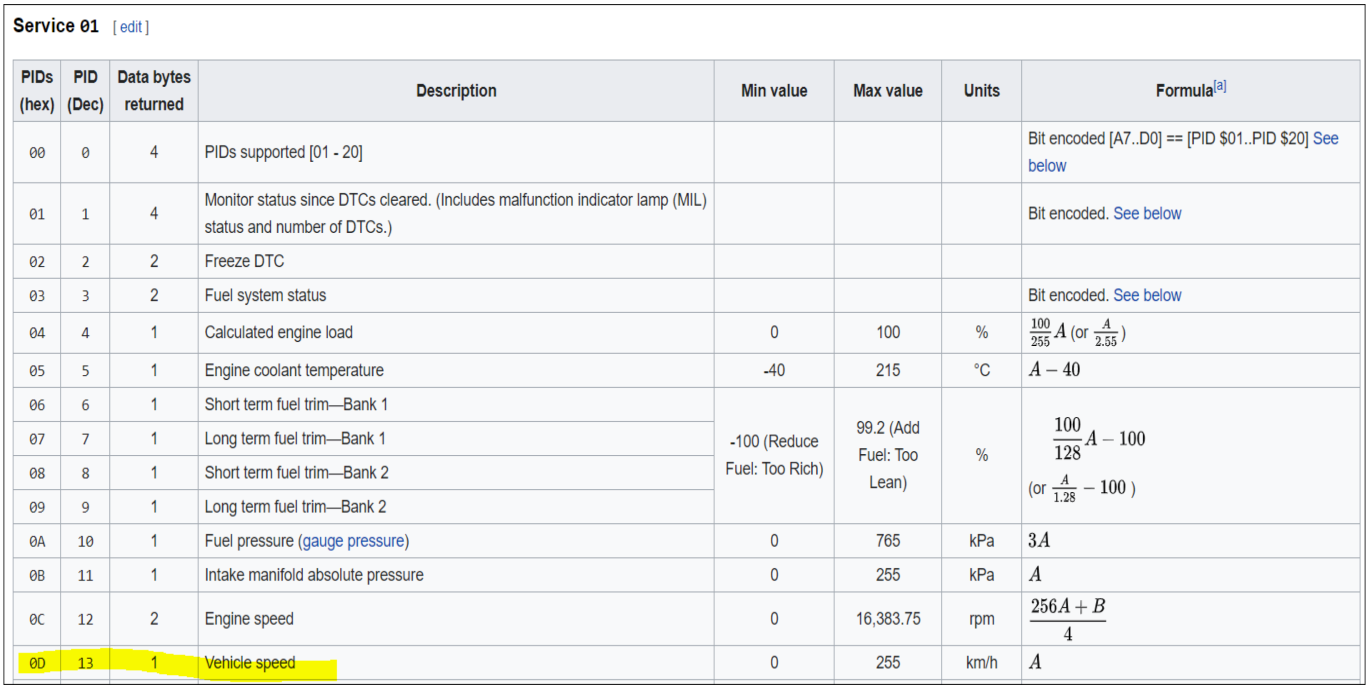


Modes [edit]

There are 10 diagnostic services described in the latest OBD-II standard SAE J1979. Before 2002, J1979 referred to these services as "modes". They are as follows:

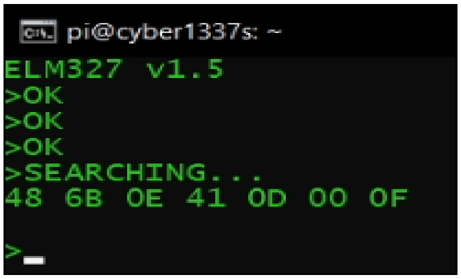
Mode (hex)	Description
01	Show current data
02	Show freeze frame data
03	Show stored Diagnostic Trouble Codes
04	Clear Diagnostic Trouble Codes and stored values
05	Test results, oxygen sensor monitoring (non CAN only)
06	Test results, other component/system monitoring (Test results, oxygen sensor monitoring for CAN only)
07	Show pending Diagnostic Trouble Codes (detected during current or last driving cycle)
08	Control operation of on-board component/system
09	Request vehicle information
0A	Permanent Diagnostic Trouble Codes (DTCs) (Cleared DTCs)

In this case I used 01, next I get the vehicle speed using “01 0D” command It give following result



Service 01 [edit]

PIDs (hex)	PID (Dec)	Data bytes returned	Description	Min value	Max value	Units	Formula[a]
00	0	4	PIDs supported [01 - 20]				Bit encoded [A7..D0] == [PID $01..PID $20] See below
01	1	4	Monitor status since DTCs cleared. (Includes malfunction indicator lamp (MIL) status and number of DTCs.)				Bit encoded. See below
02	2	2	Freeze DTC				
03	3	2	Fuel system status				Bit encoded. See below
04	4	1	Calculated engine load	0	100	%	$\frac{100}{255}A$ (or $\frac{A}{2.55}$)
05	5	1	Engine coolant temperature	-40	215	°C	$A-40$
06	6	1	Short term fuel trim—Bank 1	-100 (Reduce Fuel: Too Rich)	99.2 (Add Fuel: Too Lean)	%	$\frac{100}{128}A-100$ (or $\frac{A}{1.28}-100$)
07	7	1	Long term fuel trim—Bank 1				
08	8	1	Short term fuel trim—Bank 2				
09	9	1	Long term fuel trim—Bank 2				
0A	10	1	Fuel pressure (gauge pressure)	0	765	kPa	$3A$
0B	11	1	Intake manifold absolute pressure	0	255	kPa	A
0C	12	2	Engine speed	0	16,383.75	rpm	$\frac{256A+B}{4}$
0D	13	1	Vehicle speed	0	255	km/h	A



```
pi@cyber1337s: ~
ELM327 v1.5
>OK
>OK
>OK
>SEARCHING...
48 6B 0E 41 0D 00 0F

>_
```

48 6B OE < -- Header Value

41 < -- Response Mood

0D < -- Speed Request that I sent

00 < -- Result(speed) in HEX