

Hacking Cars with Python

Eric Evenchick
PyCon 2017

Hi



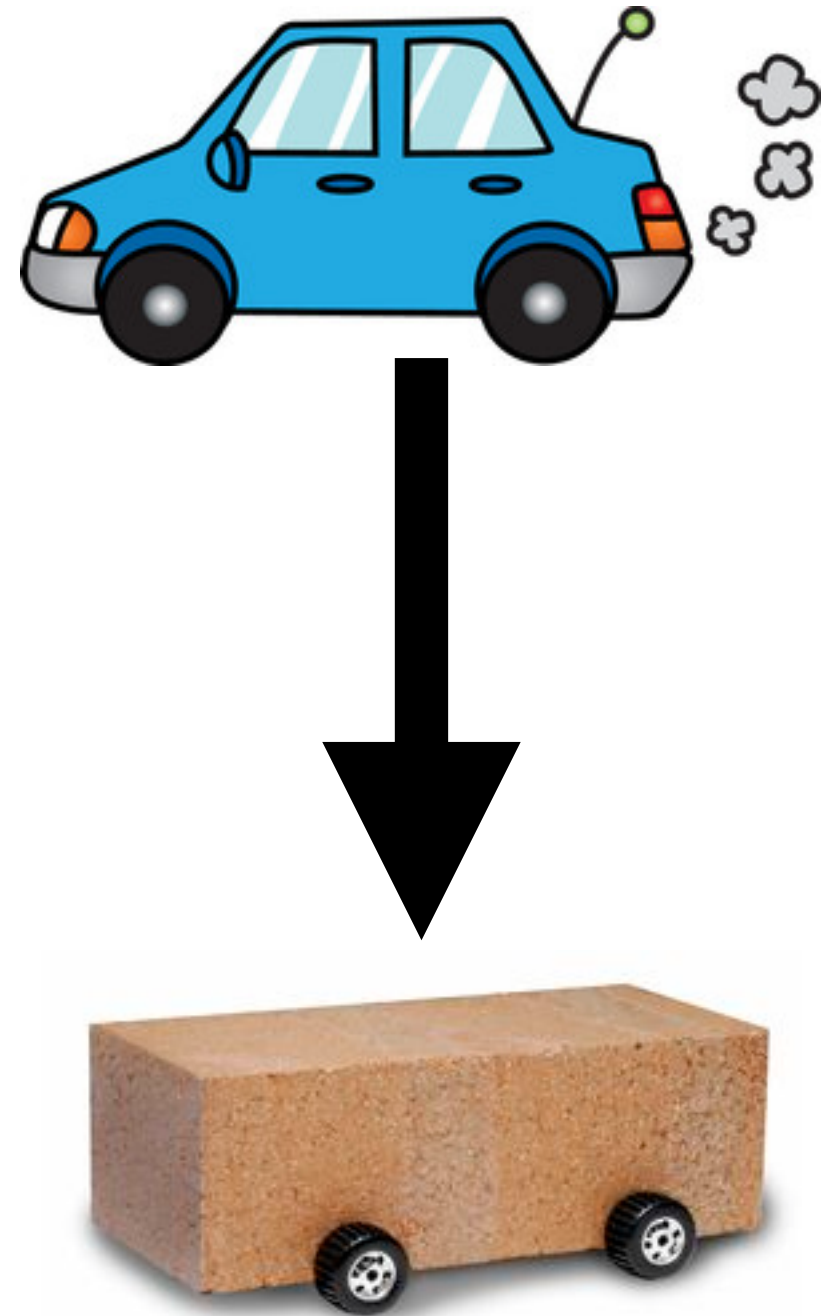
linklayer



HACKADAY

Disclaimer

- You can brick a car via diagnostics
- You can modify a safety critical system via diagnostics
- Some diagnostic actions may be illegal in certain jurisdictions
- Proceed at your own risk



Cars are Computers

Cars are Computers



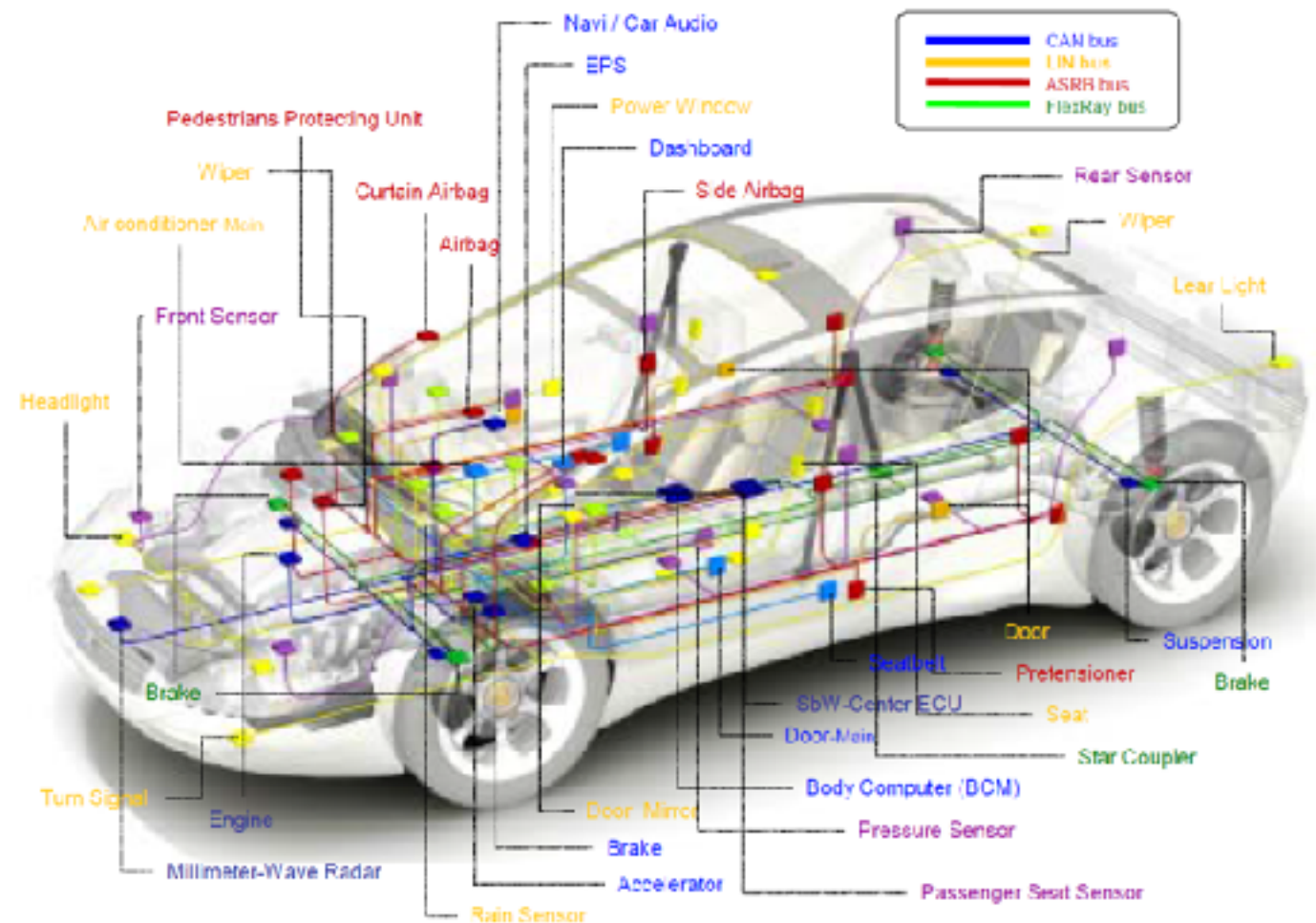
- Safety
- Advanced Features
- **Emissions**



Cars are Networks

Automotive Networks

- Up to 100 Electronic Control Units (ECUs)
- Typically Controller Area Network (CAN bus)

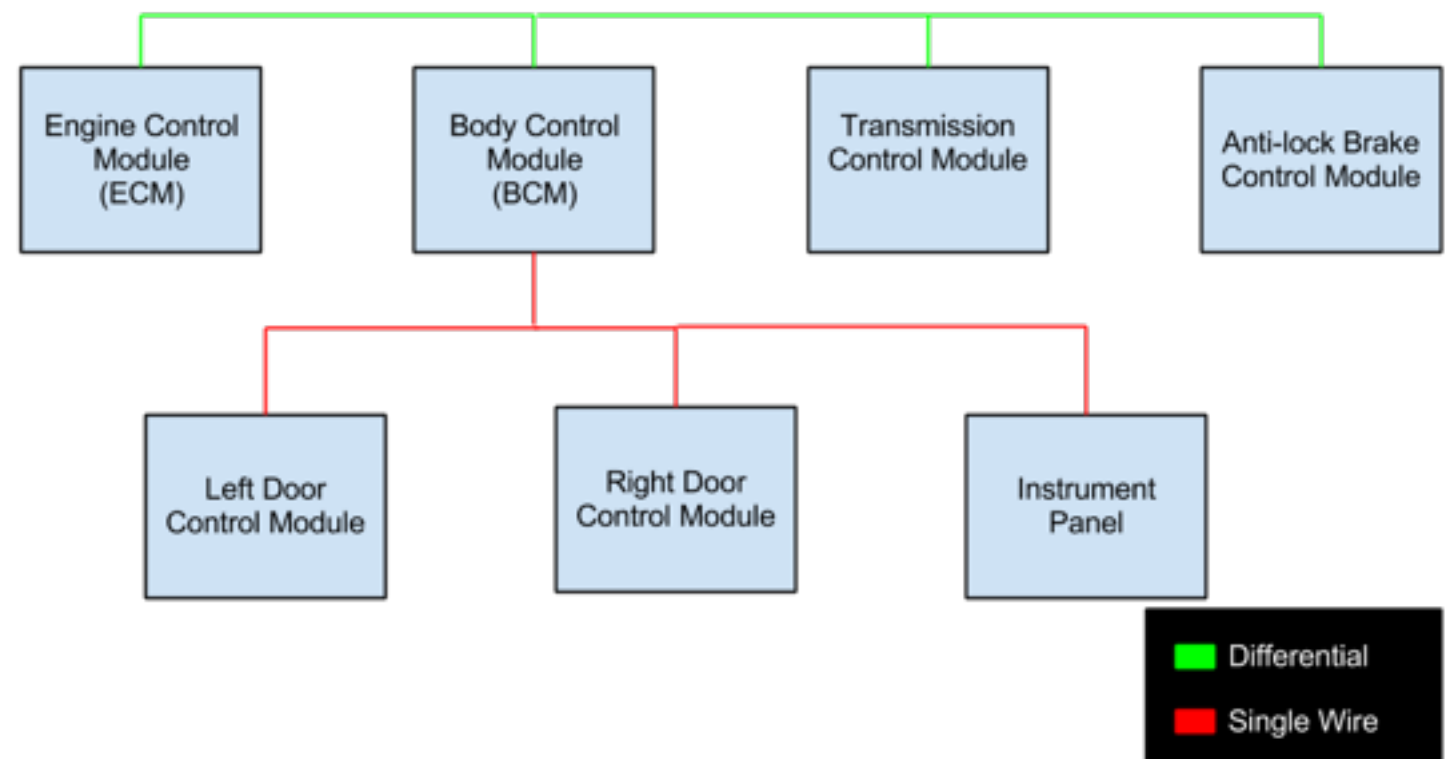


CAN Bus

- Controller Area Network
- Low cost, integrated controllers

- Types:

- High speed (differential)
- Low speed (single ended)
- Fault Tolerant
- CAN FD



CAN

- **Controller:** Network Node
- **Bus:** Collection of Controllers
- **Frame:** PDU containing:
 - ID
 - Type
 - Data Length Code
 - Data

ID	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7
0x123	0x05	0xDC	0xDE	0xAD	0xBE	0xEF	0xDE	0xAD

Communication Types

Operational

- Used during normal operation
- Relays data between ECUs
- Periodic, statically defined frames

Diagnostics

- Used at specific times, not normal operations
- Allows special interactions with ECUs
- Client / Server protocol

Operational

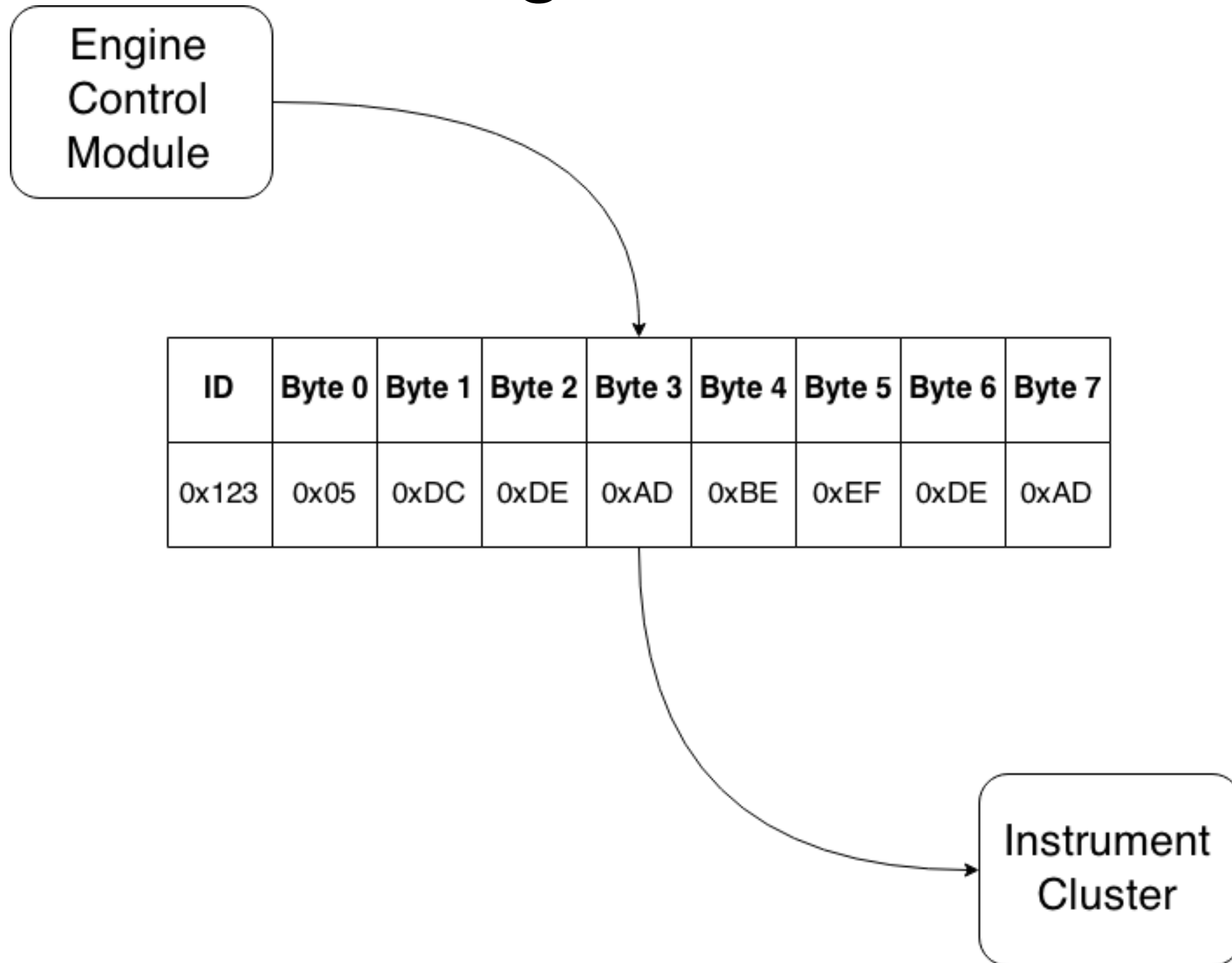
- Broadcast periodically by ECUs
- Makes everything work during normal operation
- Proprietary Encoding using CAN Database

Operational

- Lets us:
 - Get vehicle state
 - Log data
 - Control automotive components

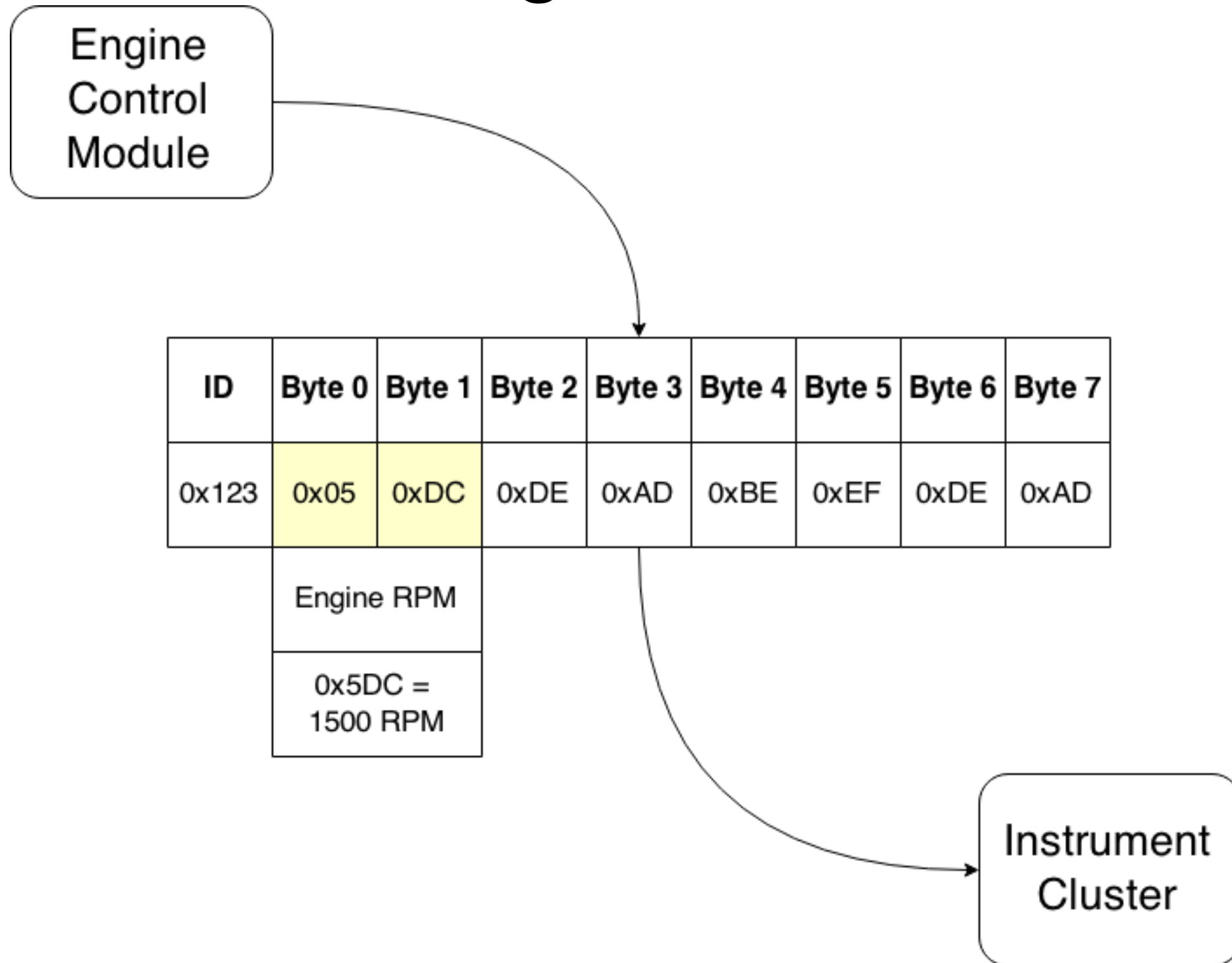
How CAN Works

Message Structure



How CAN Works

Message Structure





Automotive Diagnostics

Diagnostics

- Used during:
 - Manufacturing
 - Service
 - End-of-life
 - Forensics
- Allows a wide range of features
- Requires specialized tools



ISOTP

- How do we encode a 17 character VIN? Send firmware?
- Combines frames into longer data
- Up to 4095 bytes
- Flow Control
- Also called CANTP



Diagnostic Standards

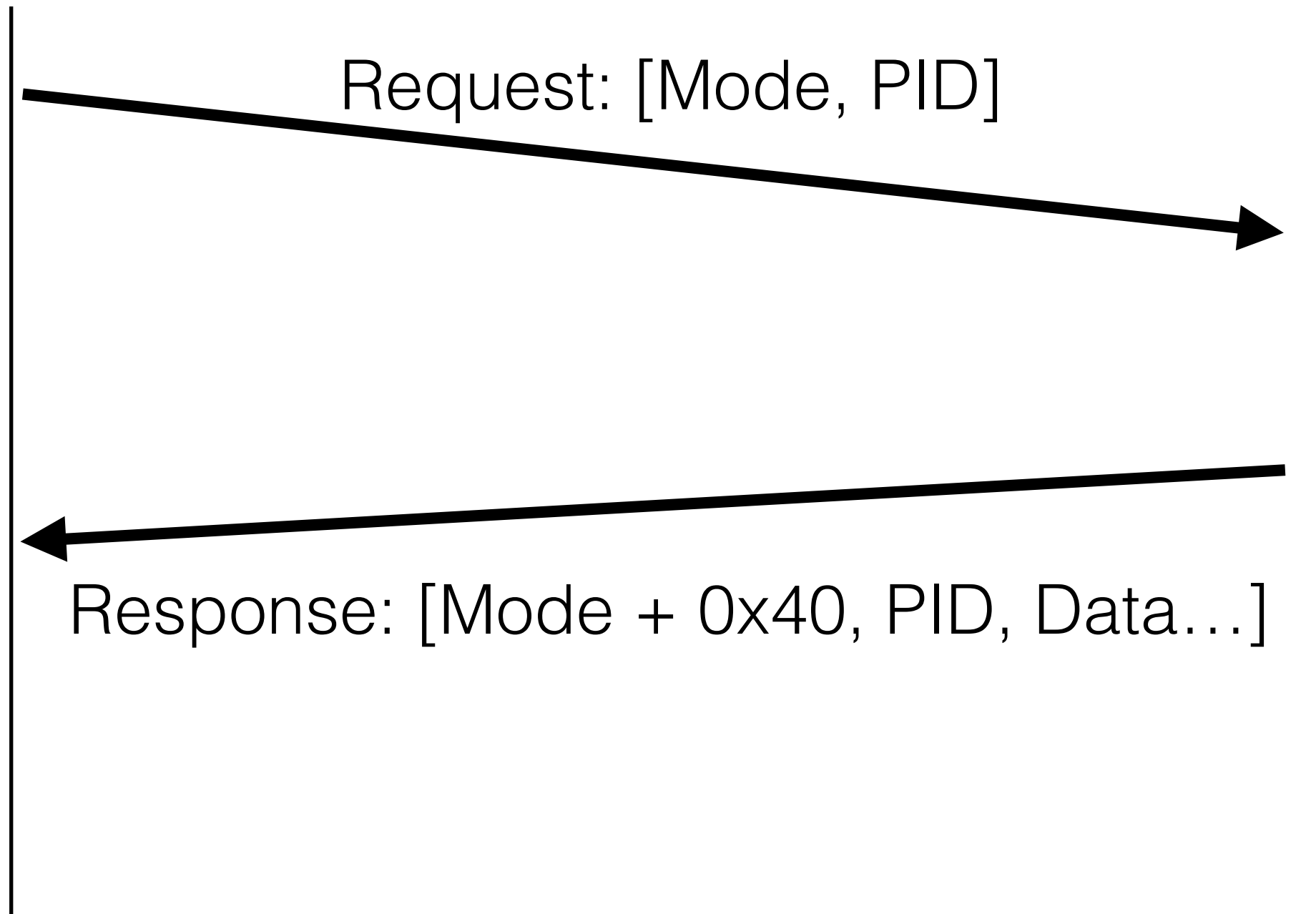
- **J1979 (OBD-II)**
- SAE J1850
- ISO 9141: K-Line / KWP2000
- **ISO 14229: Unified Diagnostic Services (UDS)**
- and many more...

OBD-II



- Read Parameters (PIDs)
- Clear Fault Codes
- Full list of PIDs: wikipedia.org/wiki/OBD-II_PIDs

OBD Session



Scan Tool (Client)

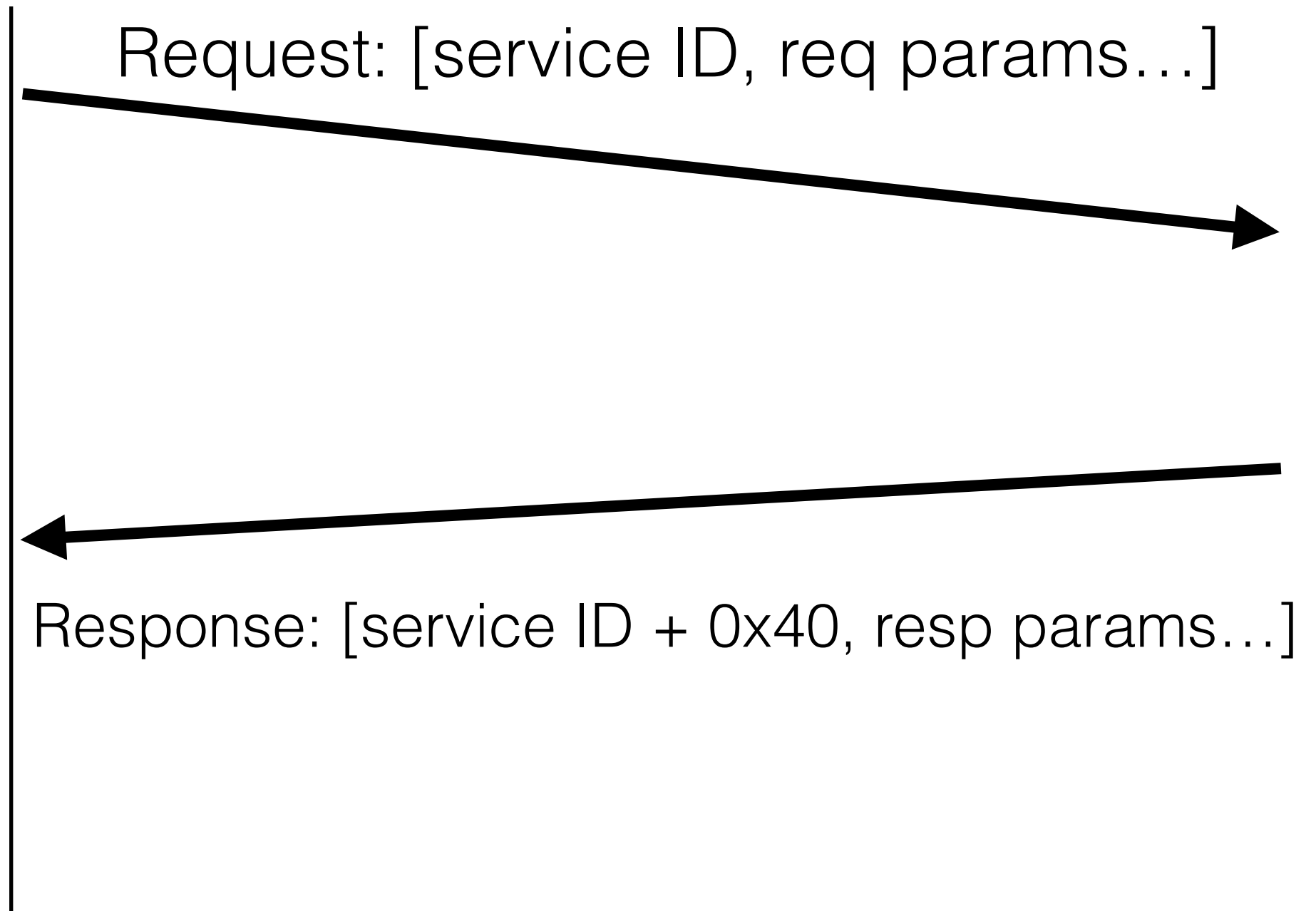
ECU (Server)

Unified Diagnostic Services

- Client / Server protocol for diagnostics
 - Client = Scan Tool
 - Server = ECU
- Defines 4 Functional Units containing 25 Services
- Available from ISO as a PDF
 - 198CHF :(



UDS Session



Scan Tool (Client)

ECU (Server)

UDS - Diagnostic and Communication Management Functional Unit

- DiagnosticSessionControl
- ECUReset
- SecurityAccess
- CommunicationControl
- TesterPresent
- AccessTimingParameter
- SecuredDataTransmission
- ControlDTCSetting
- ResponseOnEvent
- LinkControl

UDS - Data Transmission Functional Unit

- ReadDataByIdentifier
- ReadMemoryByAddress
- ReadScalingDataByIdentifier
- ReadDataByPeriodicIdentifier
- DynamicallyDefineDataIdentifier
- WriteDataByIdentifier
- WriteMemoryByAddress

UDS: Stored Data Transmission Functional Unit

- ClearDiagnosticInformation
- ReadDTCInformation

UDS: InputOutput Control Functional Unit

- InputOutputControlByIdentifier

UDS: Remote Activation of Routine Functional Unit

- RoutineControl

UDS: Upload Download Functional Unit

- RequestDownload
- RequestUpload
- TransferData
- RequestTransferExit

Tools

Tool Types

- Scan Tools
 - Official: expensive
 - Cheap options: usually OBD only
- USB to CAN adapters:
 - Still need ISOTP and UDS...



pyvit

- Python Vehicle Interface Toolkit
- CAN, ISOTP, and UDS support

I Python

Request ECU Serial Number

```
In [57]: udsif.request(  
        ReadDataByIdentifier.Request(0xF18C))  
{ 'dataIdentifier': 61836,  
  'dataRecord': [248, 18, 131, 68]}
```

I Python

ECU Hard Reset

```
In [62]: udsif.request(ECUReset.Request(  
          ECUReset.ResetType.hardReset))  
{ 'resetType': 1 }
```

UDS Decoding

```
( 37.167999 ) can0 6E0#021003000000000000
( 37.178001 ) can0 51C#065003002800C800
( 43.181999 ) can0 6E0#021003000000000000
( 43.194000 ) can0 51C#065003002800C800
( 43.222000 ) can0 6E0#0322F1000000000000
( 43.234001 ) can0 51C#0762F100000050103
( 43.263000 ) can0 6E0#0322F1320000000000
( 43.293999 ) can0 51C#037F2278000050103
( 43.324001 ) can0 51C#100D62F132363832
( 43.342999 ) can0 6E0#300000000000000000
( 43.363998 ) can0 51C#2133333533354143
( 43.402000 ) can0 6E0#0322F1500000000000
( 43.433998 ) can0 51C#037F227833354143
( 43.464001 ) can0 51C#0662F15013080043
```

UDS Decoding

(37.167999)	can0	6E0#021003000000000000
(37.178001)	can0	51C#065003002800C800
(43.181999)	can0	6E0#021003000000000000
(43.194000)	can0	51C#065003002800C800
(43.222000)	can0	6E0#0322F1000000000000
(43.234001)	can0	51C#0762F100000050103
(43.263000)	can0	6E0#0322F1320000000000
(43.293999)	can0	51C#037F2278000050103
(43.324001)	can0	51C#100D62F132363832
(43.342999)	can0	6E0#300000000000000000
(43.363998)	can0	51C#2133333533354143
(43.402000)	can0	6E0#0322F1500000000000
(43.433998)	can0	51C#037F227833354143
(43.464001)	can0	51C#0662F15013080043

Timestamp

CAN ID

Data

UDS Decoding

6E0#021003000000000000
51C#065003002800C800
6E0#021003000000000000
51C#065003002800C800
6E0#0322F1000000000000
51C#0762F100000050103
6E0#0322F1320000000000
51C#037F227800050103
51C#100D62F132363832
6E0#300000000000000000
51C#2133333533354143
6E0#0322F1500000000000
51C#037F227833354143
51C#0662F15013080043

ISOTP Bytes

Service ID

Data

**Negative Response
Codes**

Invalid Bytes

UDS Decoding

6E0#021003000000000000

51C#065003002800C800

6E0#021003000000000000

51C#0650030

6E0#0322F10

51C#0762F10

6E0#0322F13

51C#037F227800050103

51C#100D62F132363832

6E0#300000000000000000

51C#2133333533354143

6E0#0322F1500000000000

51C#037F227833354143

51C#0662F15013080043

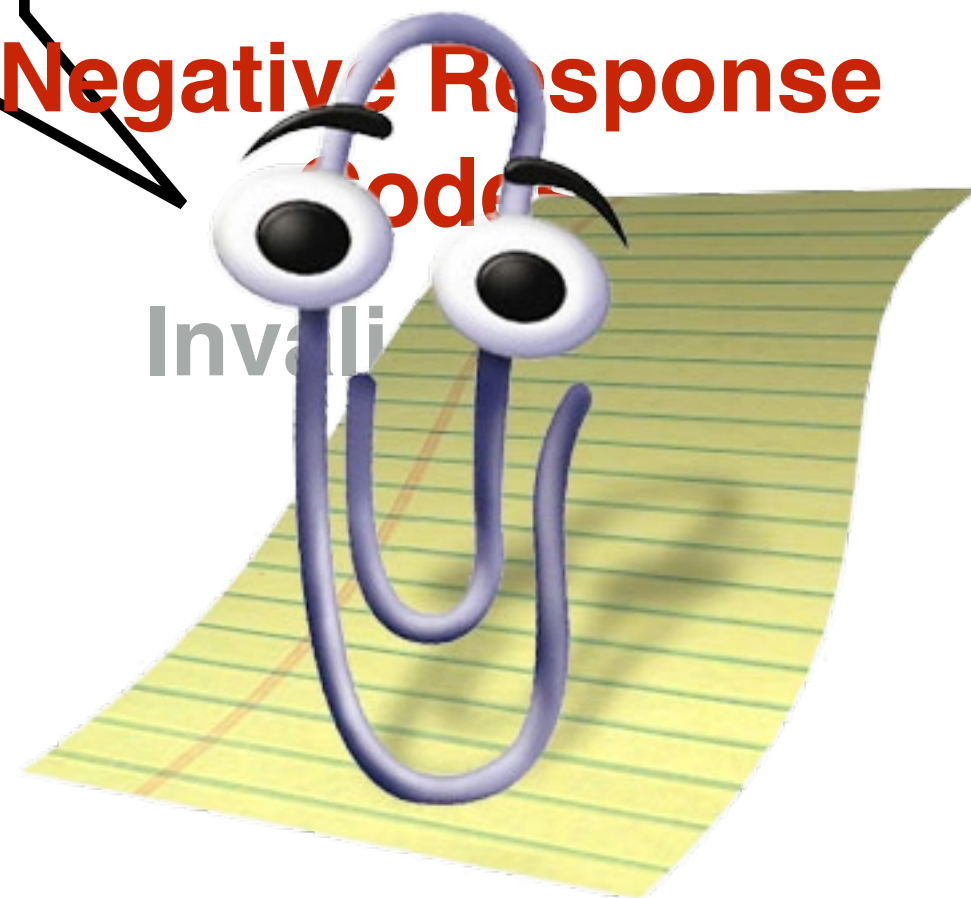
It looks like
you're trying to
decode UDS...

ISOTP Bytes

Service ID

**Negative Response
Code**

Invalid



```
[->] Request [DiagnosticSessionControl / 0x10]
      diagnosticSessionType: 3
[<-] Response [DiagnosticSessionControl / 0x10]
      sessionParameterRecord: [0, 40, 0, 200]
      diagnosticSessionType: 3
```

```
[->] Request [DiagnosticSessionControl / 0x10]
      diagnosticSessionType: 3
[<-] Response [DiagnosticSessionControl / 0x10]
      sessionParameterRecord: [0, 40, 0, 200]
      diagnosticSessionType: 3
```

```
[->] Request [ReadDataByIdentifier / 0x22]
      dataIdentifier: 61696
[<-] Response [ReadDataByIdentifier / 0x22]
      dataRecord: [0, 5, 1, 3]
      dataIdentifier: 61696
```

```
[->] Request [ReadDataByIdentifier / 0x22]
      dataIdentifier: 61746
[<-] Response [ReadDataByIdentifier / 0x22]
      dataRecord: [54, 56, 50, 51, 51, 53, 51, 53, 65, 67]
      dataIdentifier: 61746
```

“68233535AC”

```
[->] Request [ReadDataByIdentifier / 0x22]
      dataIdentifier: 61776
[<-] Response [ReadDataByIdentifier / 0x22]
      dataRecord: [19, 8, 0]
      dataIdentifier: 61776
```




68233535AC



All

Maps

Videos

Images

Shopping

More

Settings

Tools

About 106 results (0.23 seconds)

Module-Occupant Restraint | Genuine Mopar | 68233535AD ...

www.mymoparparts.com › MOPAR 68233535AD ▼

\$188.78

Manufacturer: Mopar; Part Number: 68233535AD; Part: Module-Occupant Restraint; Replaces: 68233535AA, 68233535AB, 68233535AC, 68105432AE, ...

CHRYSLER OEM Supplemental Restraint System-diagnostic Module ...

<https://www.ebay.com> › ... › Car & Truck Parts › Safety & Security › Air Bag Parts ▼

Find great deals for CHRYSLER OEM Supplemental Restraint System-diagnostic Module 68233535AC. Shop with confidence on eBay!

68233535AC - Genuine Mopar MODULE-OCCUPANT RESTRAINT

<https://www.moparpartsgiant.com/.../mopar-module-occupant-restraint~68233535ac....> ▼

MoparPartsGiant.com offers the best deal for genuine Mopar parts, 68233535AC. MODULE-OCCUPANT RESTRAINT for \$185.60. All parts are backed by the ...

Conclusions

Practical Stuff

- Get an OBD-II device
- Fault codes, clear MIL
- Right to Repair
- OpenGarages, DEF CON Car Hacking Village



The Future

- Ethernet Based Diagnostics: DoIP
- CAN FD
- Vehicle APIs
 - Tesla
 - Ford OpenXC
- More tools based on pyvit :)

Thanks! Questions?

<https://github.com/linklayer/pyvit>

eric@evenchick.com

@ericevenchick

<https://linklayer.com>

<https://atredis.com>