Techniques for Learning a Vehicle's CAN Database

Presented By:

Colt Correa

Vice President – Business Development

Intrepid Control Systems, Inc.

Email : ccorrea@intrepidcs.com

Presentation Overview

A. Introduction

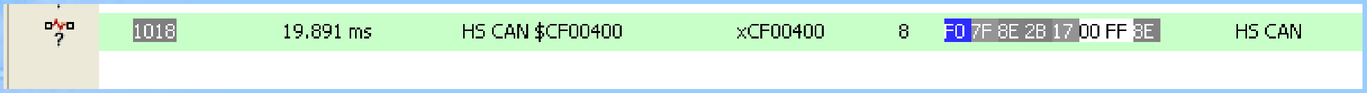
1. What is a CAN database?
2. Who needs a network database?
3. Is reverse engineering always EVIL?
4. Legal aspects of reverse engineering

B. Reverse Engineering on a Vehicle Network (CAN)

1. Types of data to reverse engineer
2. Assets for reverse engineering
3. Step1: Determine response to stimulus
4. Step2: Find data bytes add scaling for engineering units

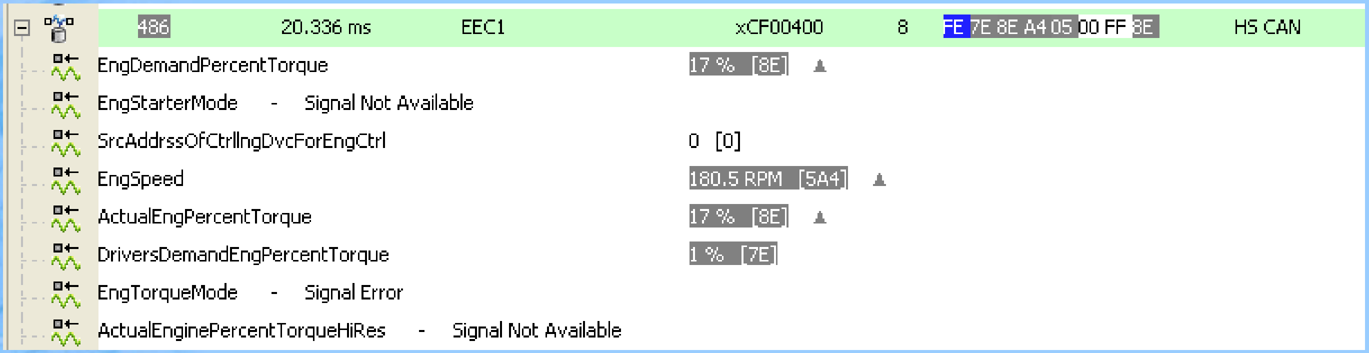
C. Conclusion

What is a CAN database?



```
1018    19.891 ms    HS CAN $CF00400    xCF00400    8    F0 7F 8E 2B 17 00 FF 8E    HS CAN
```

Without Database



```
486    20.336 ms    EEC1    xCF00400    8    FE 7E 8E A4 05 00 FF 8E    HS CAN
  EngDemandPercentTorque                                17 %   [8E]
  EngStarterMode    -    Signal Not Available
  SrcAddrssOfCtrllngDvcForEngCtrl                       0   [0]
  EngSpeed                                              180.5 RPM   [5A4]
  ActualEngPercentTorque                                17 %   [8E]
  DriversDemandEngPercentTorque                         1 %   [7E]
  EngTorqueMode    -    Signal Error
  ActualEnginePercentTorqueHiRes    -    Signal Not Available
```

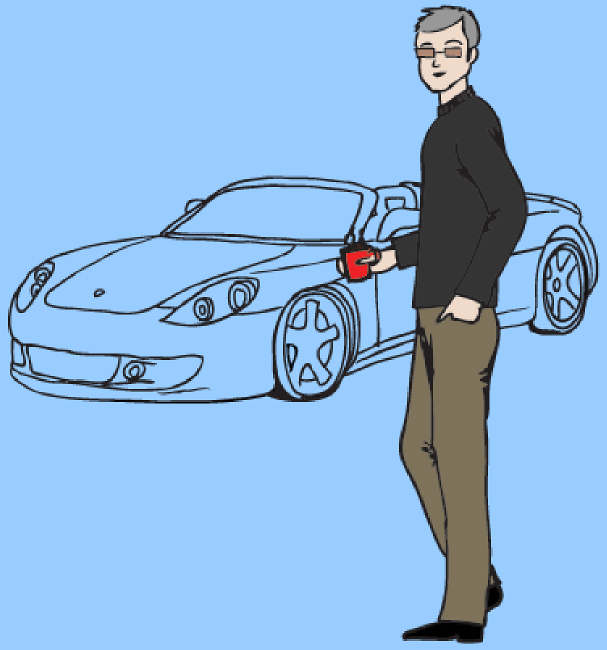
With Database

Short Answer: A database makes network data human readable.

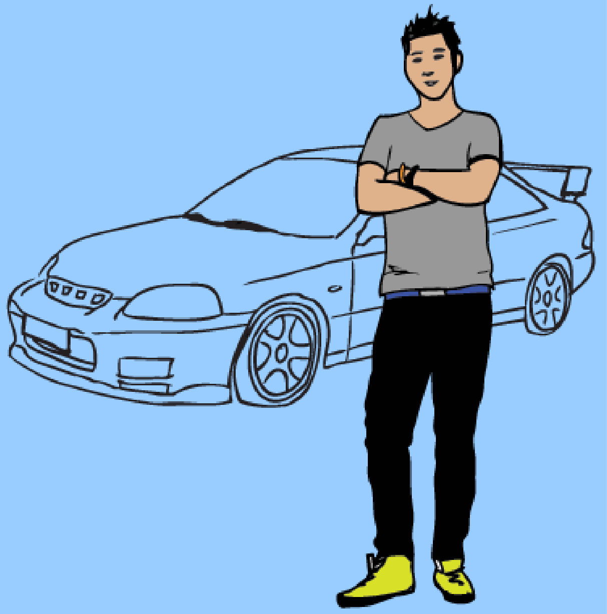
Who needs a database?

UH OH: The tuners!!

Detroit Tuners



European Tuners



Asian Tuners

Who needs a database?

Aftermarket accessories:

Mirrors
Hoods
Tailgates Trunk Lids
Header & Nose Panels
Tail Lights
Radiator Supports
Step Bumpers
Grilles
A/C Condensers
Bumpers
Headlights
Fenders
Radiators
Doors

As electronics becomes a larger part of the vehicle, it also is becoming a larger part in aftermarket accessories.

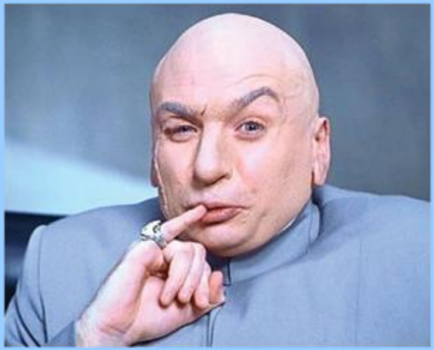
Who needs a database?

SURPRISE: OEMs are our largest customer base for reverse engineering.

REASONS:

1. All OEM perform competitive analysis
2. Flow of information inside large multi-national OEMs is not perfect. Often it is easier to reverse engineer a network than get the database from the headquarters.

Is reverse engineering EVIL?



Where's the data?

- Almost all vehicle data can be found in two types of messaging:
  - **Normal Messaging** – Messages on network present for normal operation of vehicle *(focus of this presentation)*
  - **Diagnostic Messaging** – Messages that appear when a requests in a specific format are made

Finding your data

- The data may not be present in normal messaging because there is no need for ECUs to share it
- Data in normal messaging is best because its already there and you do not have to affect the system by sending requests.
- Normal messaging is often faster to acquire

Your best assets

- Vehicle Spy (of course)
  - Online editing of database with “live” data
  - Activity highlighting
- Common sense and experience
  - The lower the CAN ID the higher the priority
  - The more you know about what you are looking for the better

Step1: Find your data

Determine response to stimulus

Step2: Determine data bytes, add scaling

Basic “Details View” features

Step2: Determine data bytes, add scaling

Signal Tracking in “Details View”

Conclusions

- There is no easy “silver bullet”
- Gets much easier with experience
- After doing one OEM, other vehicles from the same OEM are generally similar

Questions?

- **Technical Support:**
  - moreinfo@intrepidcs.com
  - www.intrepidsupport.com
  - (586) 731-7950 x1
- **Sales:**
  - moreinfo@intrepidcs.com
  - (586) 731-7950 x2