CAN Fuzzer & Vehicle Spy Я3D

How to do Fuzz Testing with Vehicle Spy

CAN Fuzzing for Vehicle Systems Testing

- Introduction
- What is Fuzz Testing
- Vehicle Spy Я3D
- How CAN Fuzzing work for your ECUs

Introduction

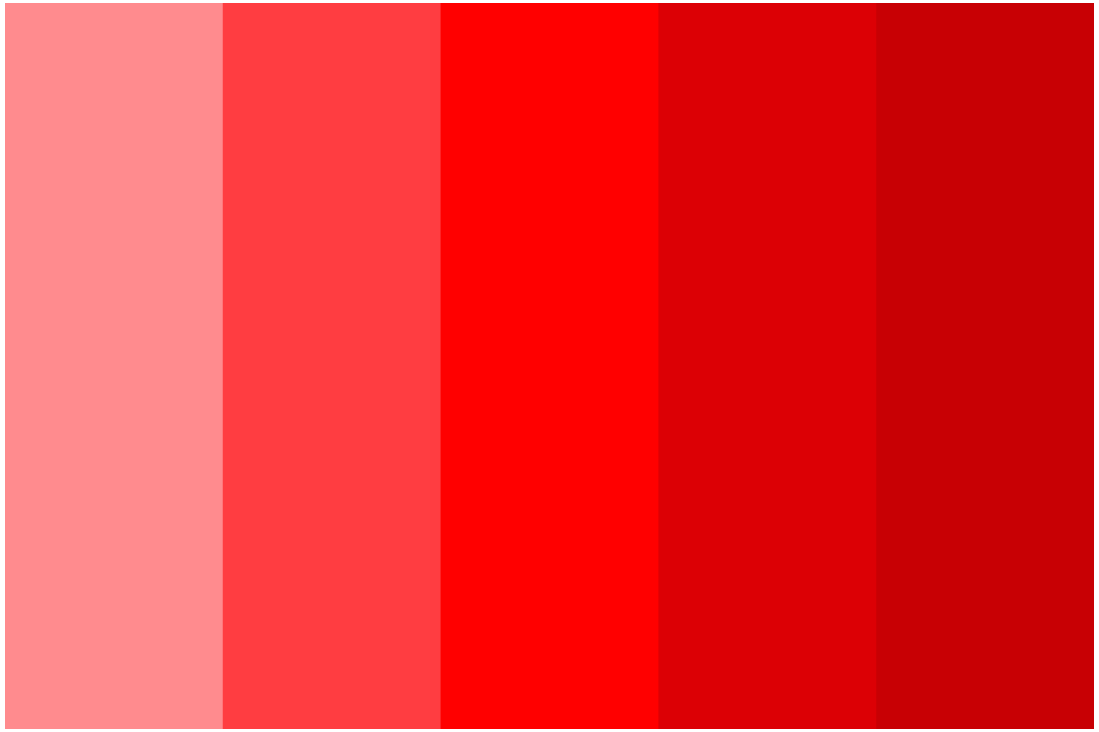
- Started working with Vehicle Spy in 2005.
- Started Hacking Cars soon after
- Founded Car Hacking Village
- Trainer of “Car Hacking Hands-on” at Black Hat USA
- Working to integrate more Cyber Security tools into Vehicle Spy.

What is Fuzzing

- OWASP defines fuzzing as:
  - *"Fuzz testing or Fuzzing is a Black Box software testing technique, which basically consists in finding implementation bugs using malformed/semi-malformed data injection in an automated fashion."*
- Fuzzing will find bugs and security holes

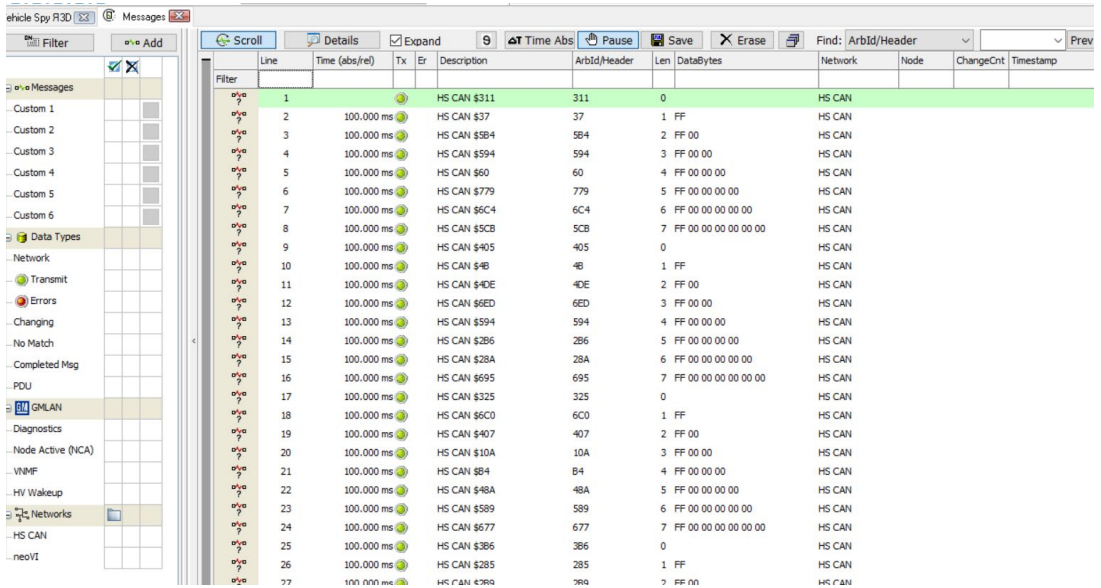
What is Vehicle Spy Я3D

- Automotive Penetration Testing Suite of Tools
- Goals:
  - CAN Fuzzer (in Beta)
  - Ethernet (including TCP/IP) Fuzzer
  - Diagnostic Scanner/Tester
  - IDS Tester (TBD)



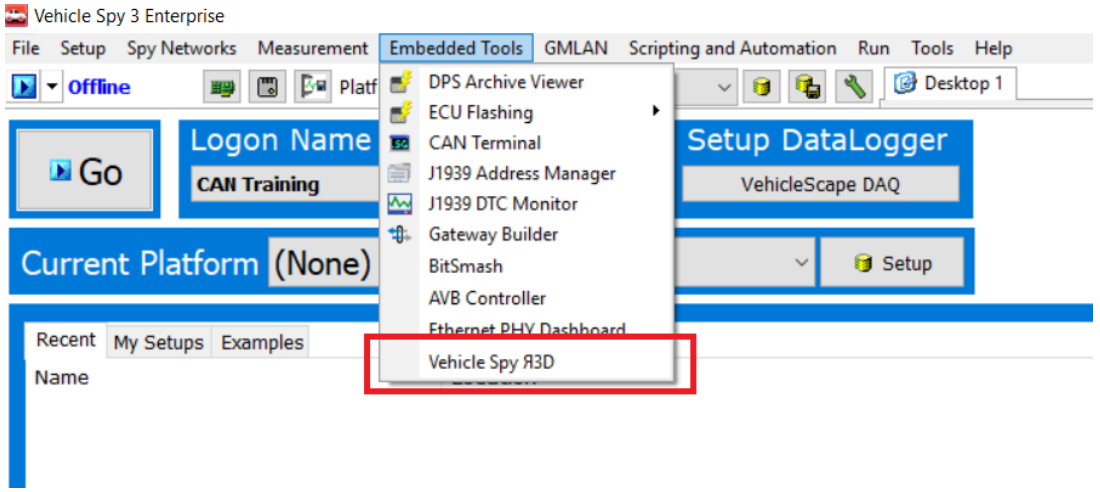
Live Demo !!!

- This will be a live Demo of a Beta product.
- Are you scared? I know I am!



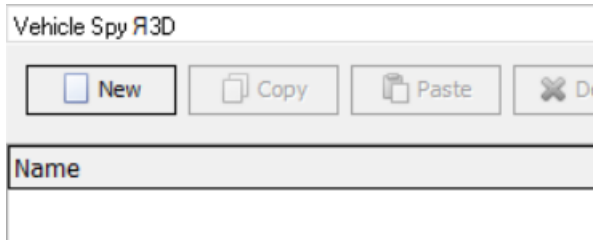
Opening the Vehicle Spy Red View

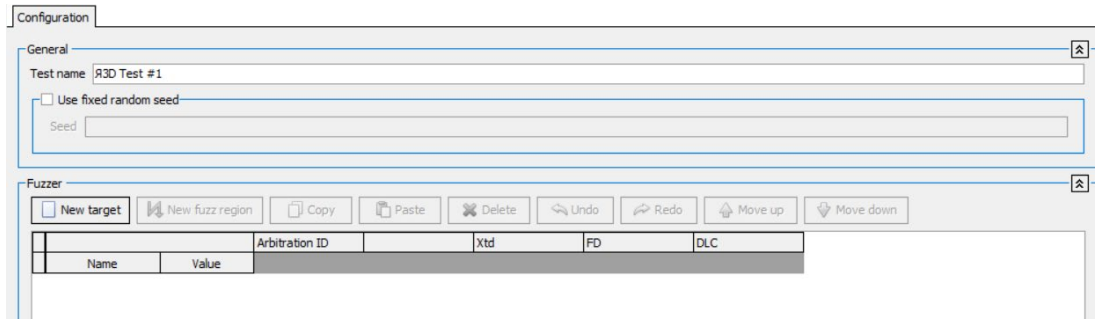
- Found under the Embedded Tools Section of Vehicle Spy (Currently in Beta).



Creating New Tests

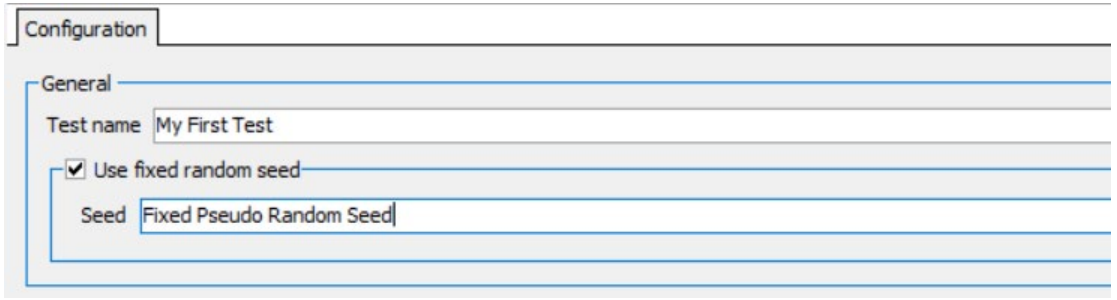
- Tests are Generated by Clicking New Button
- Individual tests can be named for reference.





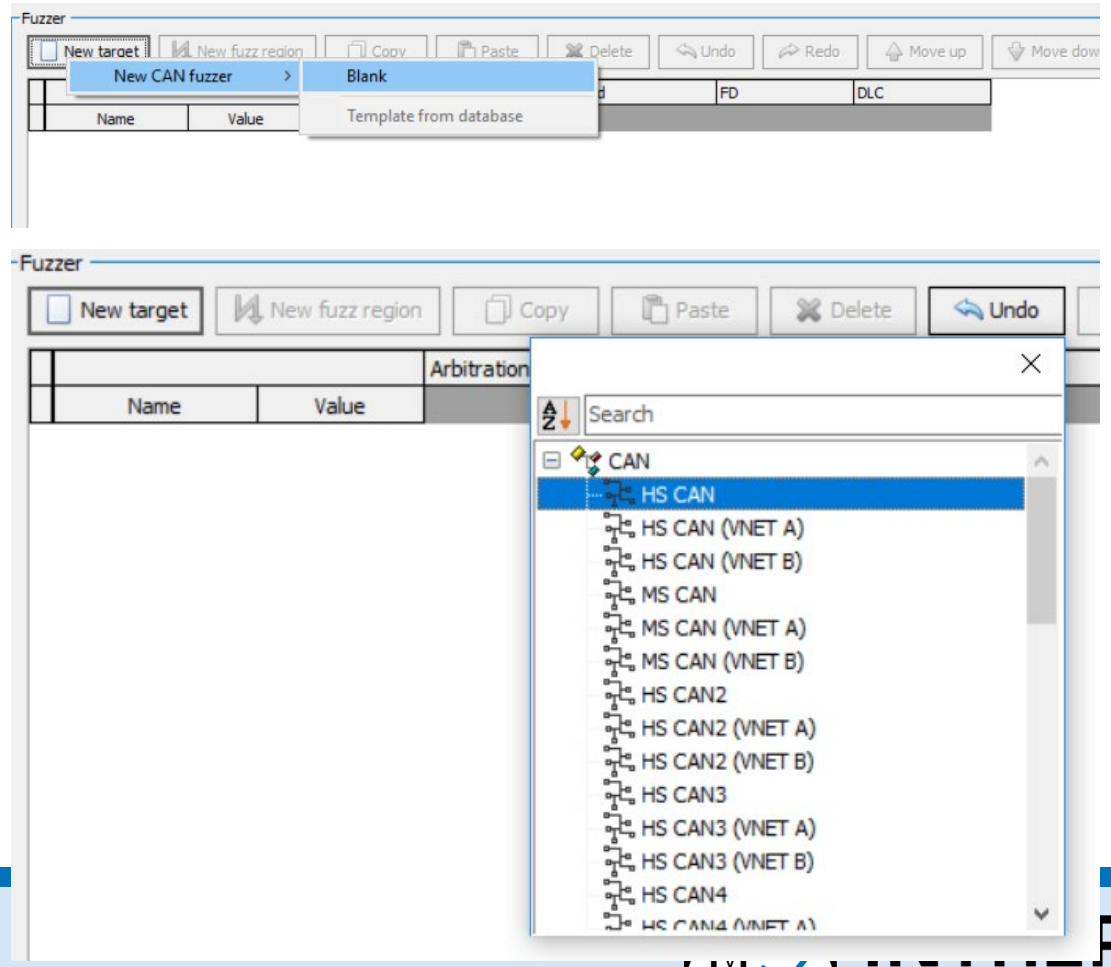
Pseudo Random Seed

- Random is important
- Random is bad
- Pseudo Random is the answer
  - Randomization
  - Reproduceable
- If no seed given, a random seed will be generated for the test.



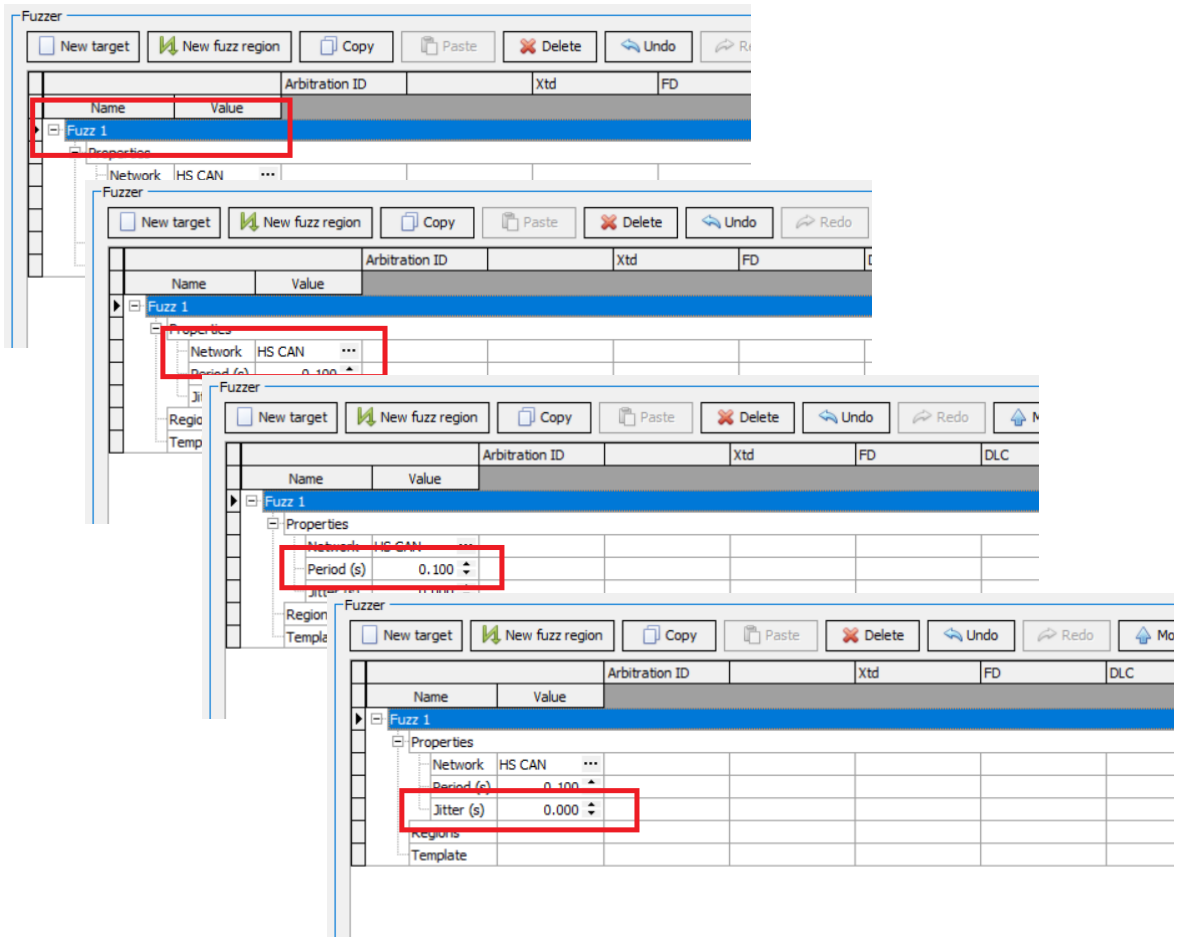
Generating a Target For the Fuzzer

- Targets are:
  - Networks (HS CAN, HS CAN 2, etc.)
  - Database Messages (In Development).



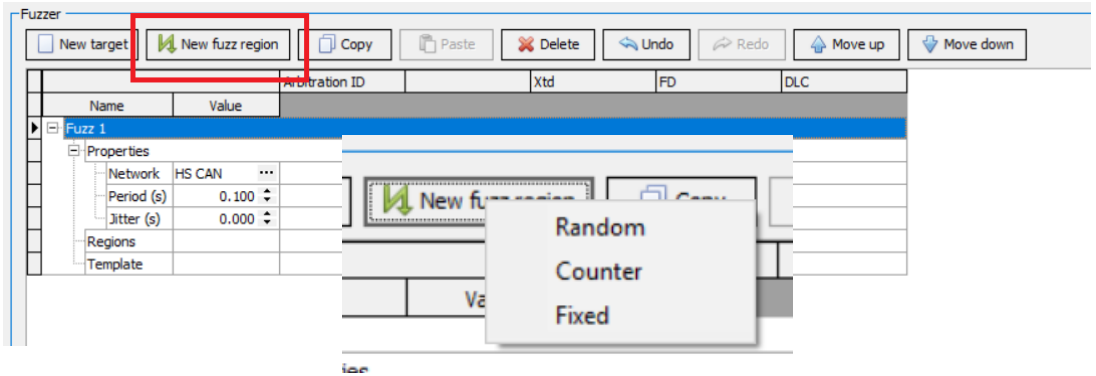
Configuring Target

- Update Target's Name
- Modify Target's Network
- Configure Target's Periodicity
- Add Simulated Pseudo Random Jitter.



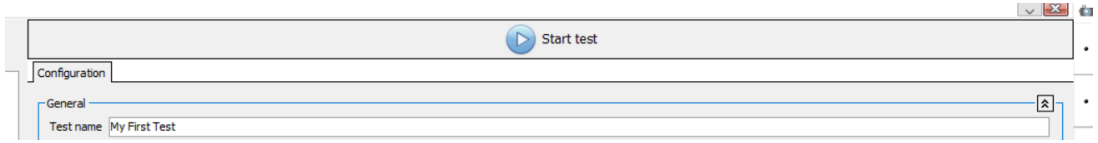
Creating Fuzz Regions

- Three Types of Fuzz Regions:
  - Random (Using Seed)
  - Counter
  - Fixed.

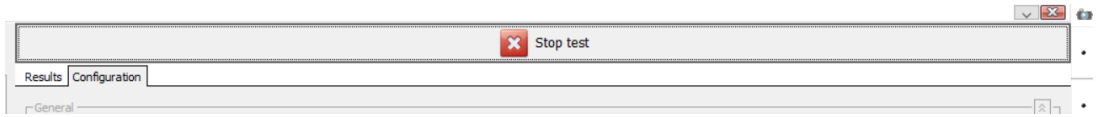


Starting and Stopping Tests

- To Activate press the “Start Test” Button

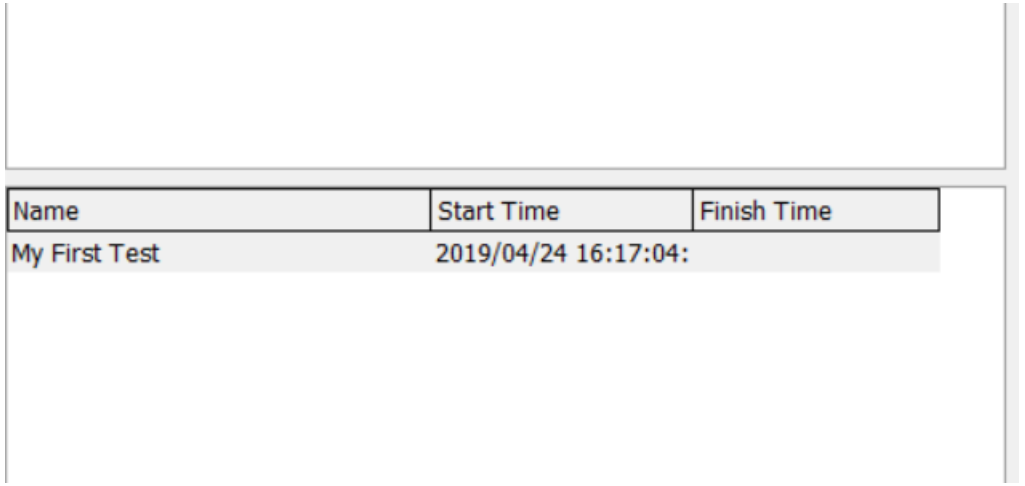


- To Stop press the “Stop Test” Button.



Test Information and Results

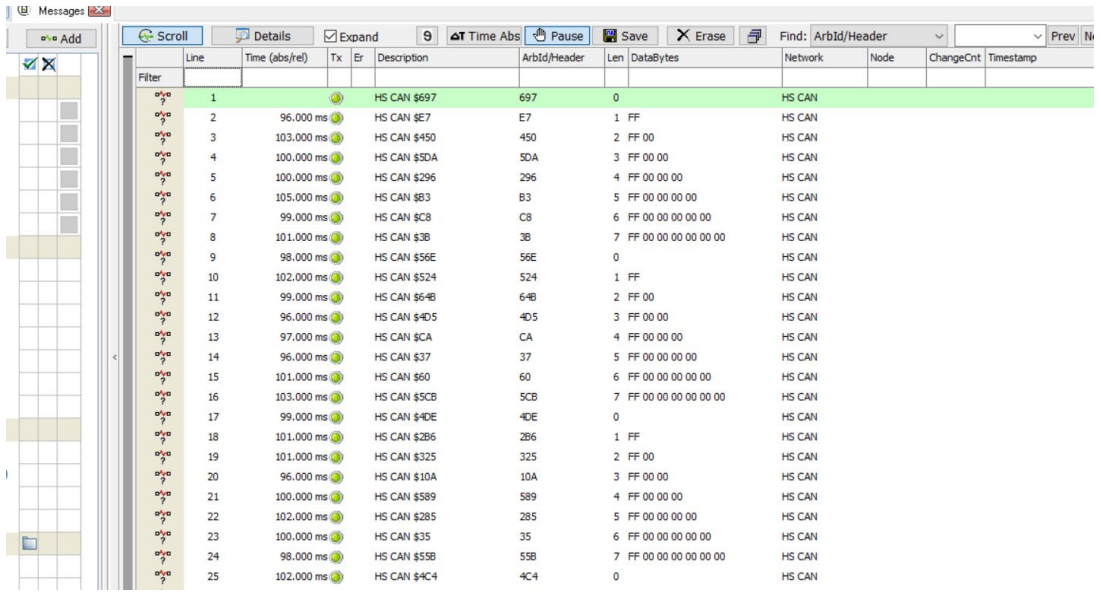
- Tests have Start/Stop Time
- Each test will hold the results of the tests message data.



Name	Start Time	Finish Time
My First Test	2019/04/24 16:17:04:	

CAN Fuzzing Results

- Messages are transmitted on the Corresponding Target Network
- Results are reproduceable
  - Periodicity
  - Jitter
  - Fuzz Regions.



What's Next

- Still in Beta and not 100% done
- All Data will be captured and stored in the Results Tab
- Test Automation will be added to Function Blocks
- Adding Test Conditions to give Pass-Fail information on Test.
- Looking for feedback from Customers.

Future Features of Vehicle Spy Я3D

- Ethernet Fuzzing
- Diagnostic Scanning
- Diagnostic Fuzzing (UDS)
- IDS Tester
- Much more.

Questions/Quick Mentions

- Fuzz Tester is being Demoed now
- Questions?