

CAN Fuzzer & Vehicle Spy R3D

How to do Fuzz Testing with Vehicle Spy

1

CAN Fuzzing for Vehicle Systems Testing

- Introduction
- What is Fuzz Testing
- Vehicle Spy R3D
- 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.



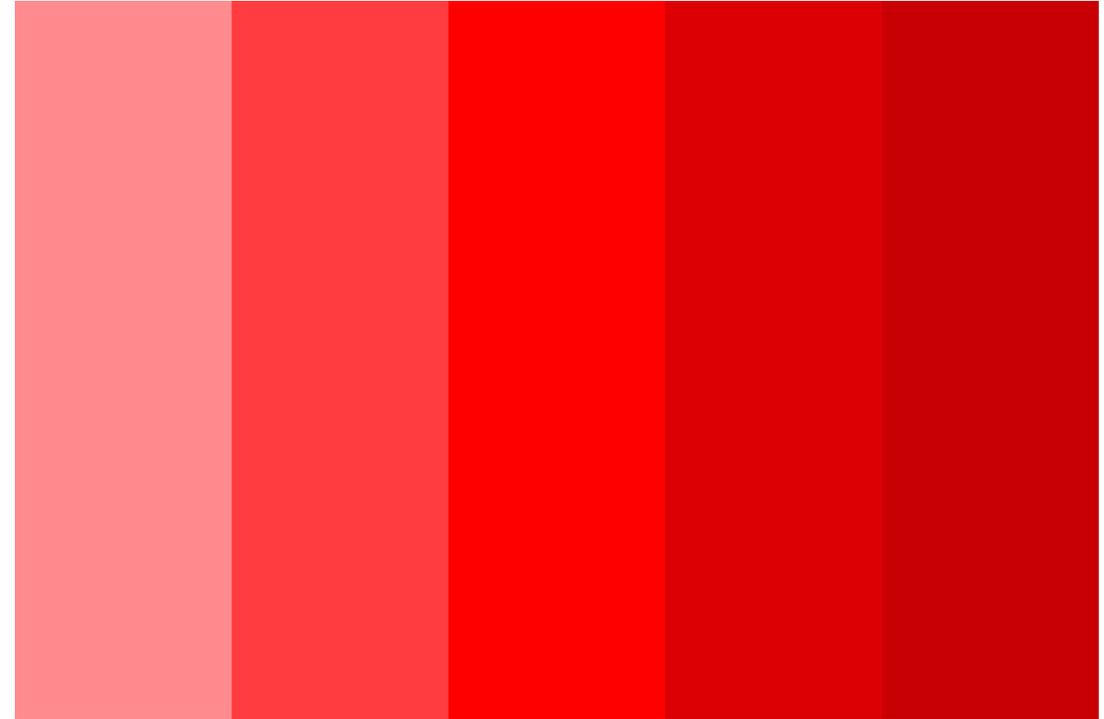
3

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

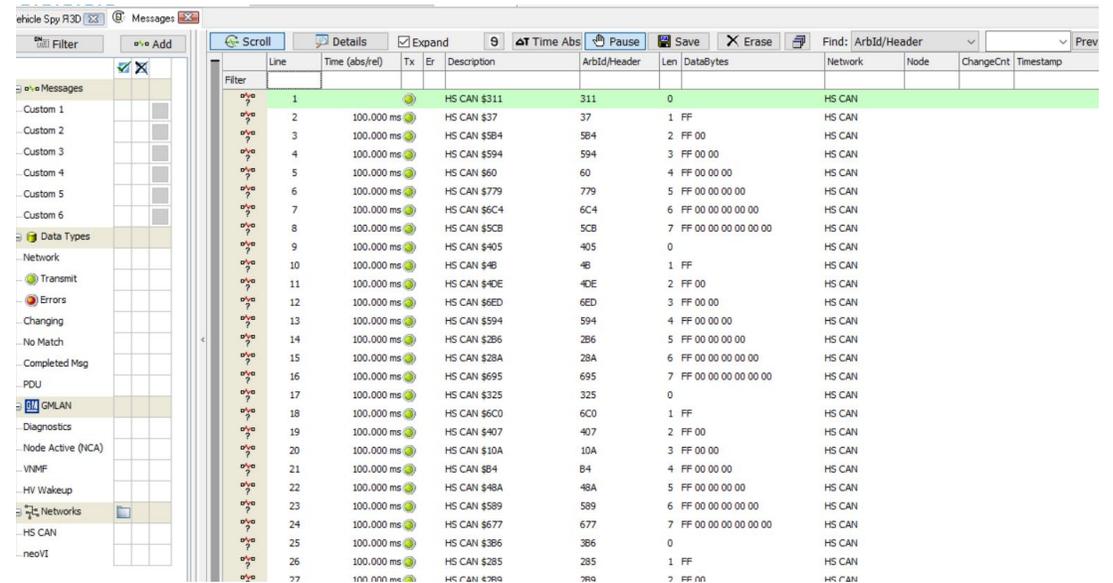
What is Vehicle Spy R3D

- 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!

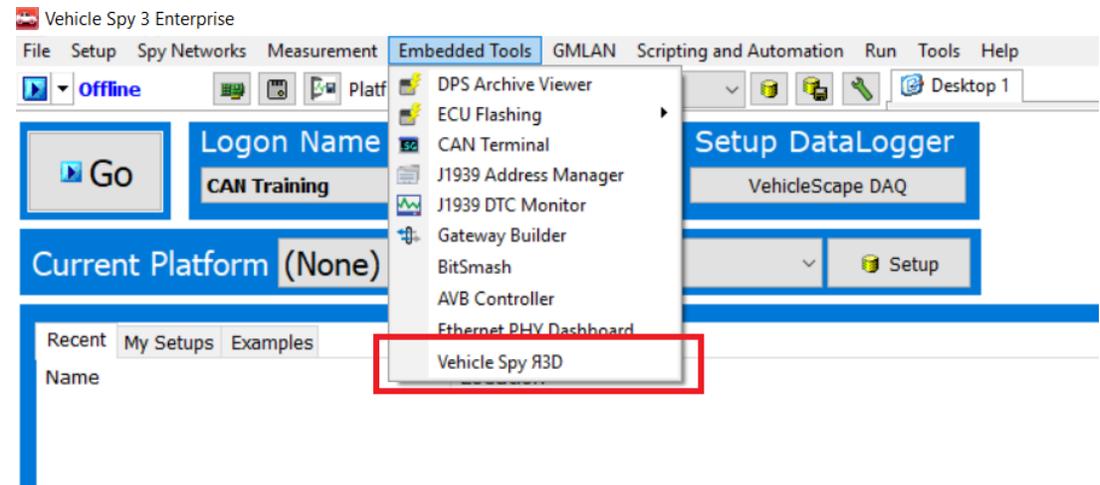


The screenshot shows the Vehicle Spy R3D software interface. The main window displays a list of messages captured on the HS CAN network. The messages are organized into a table with columns for Line, Time (abs/rel), Tx, Er, Description, Arbid/Header, Len, DataBytes, Network, Node, ChangeCnt, and Timestamp. The messages are filtered to show only those on the HS CAN network. The first message (Line 1) is highlighted in green and shows a transmission of 311 bytes. The subsequent messages show various data bytes and lengths, including error frames (FF) and data frames with varying lengths and data values.

Line	Time (abs/rel)	Tx	Er	Description	Arbid/Header	Len	DataBytes	Network	Node	ChangeCnt	Timestamp
1				HS CAN \$311	311	0		HS CAN			
2	100.000 ms			HS CAN \$37	37	1	FF	HS CAN			
3	100.000 ms			HS CAN \$584	584	2	FF 00	HS CAN			
4	100.000 ms			HS CAN \$594	594	3	FF 00 00	HS CAN			
5	100.000 ms			HS CAN \$60	60	4	FF 00 00 00	HS CAN			
6	100.000 ms			HS CAN \$779	779	5	FF 00 00 00 00	HS CAN			
7	100.000 ms			HS CAN \$6C4	6C4	6	FF 00 00 00 00 00	HS CAN			
8	100.000 ms			HS CAN \$5CB	5CB	7	FF 00 00 00 00 00 00	HS CAN			
9	100.000 ms			HS CAN \$405	405	0		HS CAN			
10	100.000 ms			HS CAN \$4B	4B	1	FF	HS CAN			
11	100.000 ms			HS CAN \$4DE	4DE	2	FF 00	HS CAN			
12	100.000 ms			HS CAN \$6ED	6ED	3	FF 00 00	HS CAN			
13	100.000 ms			HS CAN \$594	594	4	FF 00 00 00	HS CAN			
14	100.000 ms			HS CAN \$286	286	5	FF 00 00 00 00	HS CAN			
15	100.000 ms			HS CAN \$28A	28A	6	FF 00 00 00 00 00	HS CAN			
16	100.000 ms			HS CAN \$695	695	7	FF 00 00 00 00 00 00	HS CAN			
17	100.000 ms			HS CAN \$325	325	0		HS CAN			
18	100.000 ms			HS CAN \$6C0	6C0	1	FF	HS CAN			
19	100.000 ms			HS CAN \$407	407	2	FF 00	HS CAN			
20	100.000 ms			HS CAN \$10A	10A	3	FF 00 00	HS CAN			
21	100.000 ms			HS CAN \$B4	B4	4	FF 00 00 00	HS CAN			
22	100.000 ms			HS CAN \$48A	48A	5	FF 00 00 00 00	HS CAN			
23	100.000 ms			HS CAN \$589	589	6	FF 00 00 00 00 00	HS CAN			
24	100.000 ms			HS CAN \$677	677	7	FF 00 00 00 00 00 00	HS CAN			
25	100.000 ms			HS CAN \$386	386	0		HS CAN			
26	100.000 ms			HS CAN \$285	285	1	FF	HS CAN			
27	100.000 ms			HS CAN \$700	700	2	FF 00	HS CAN			

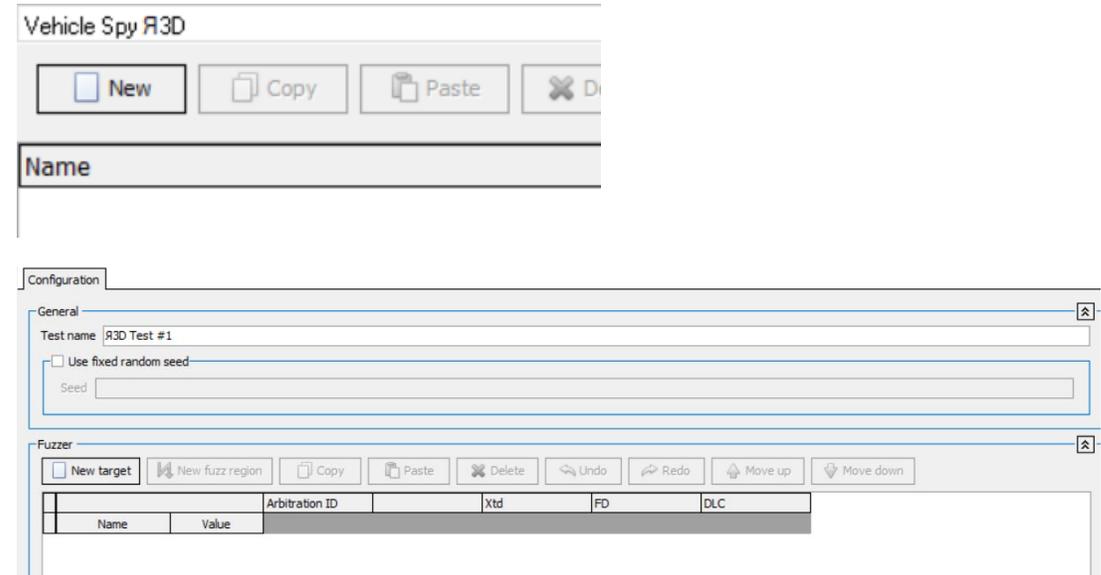
Opening the Vehicle Spy Red View

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



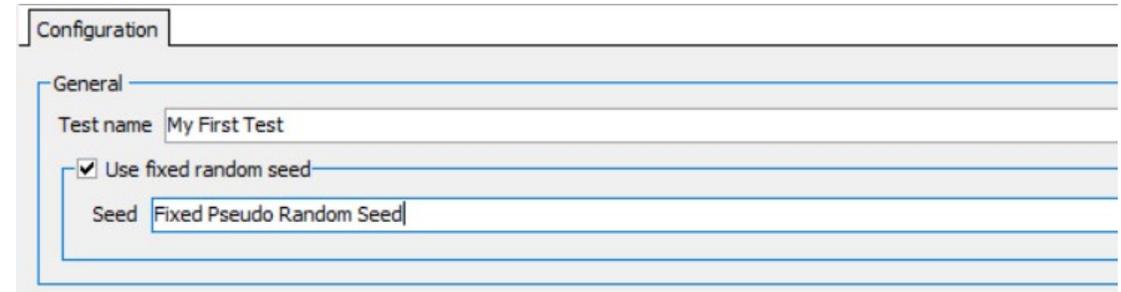
Creating New Tests

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



Pseudo Random Seed

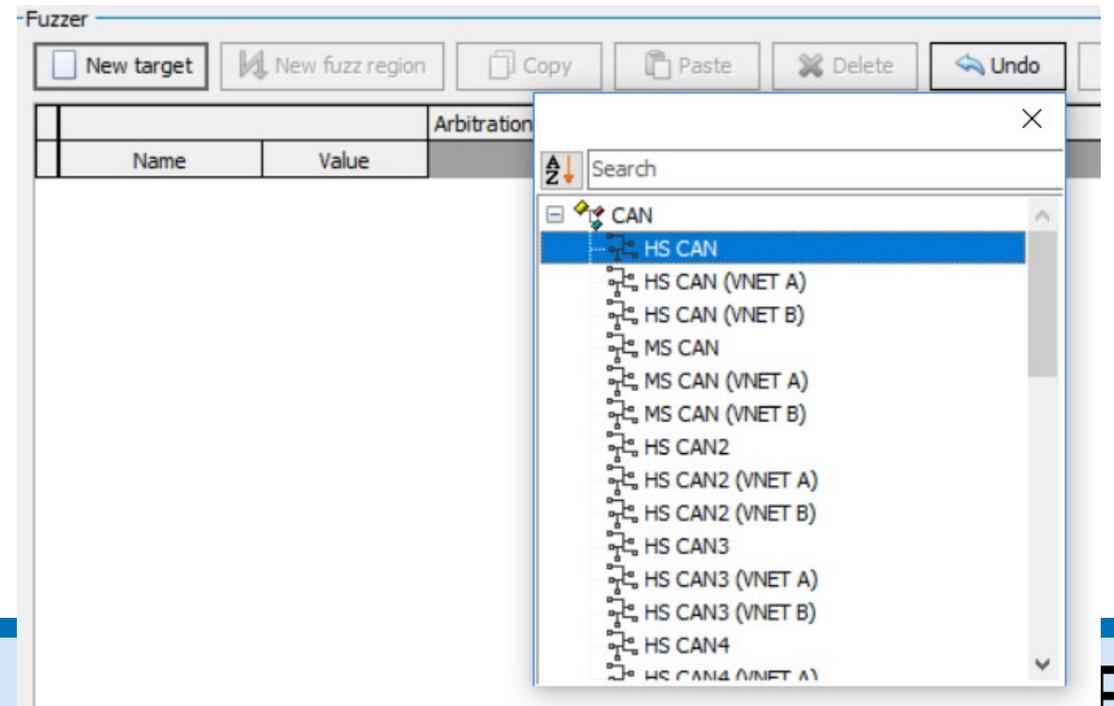
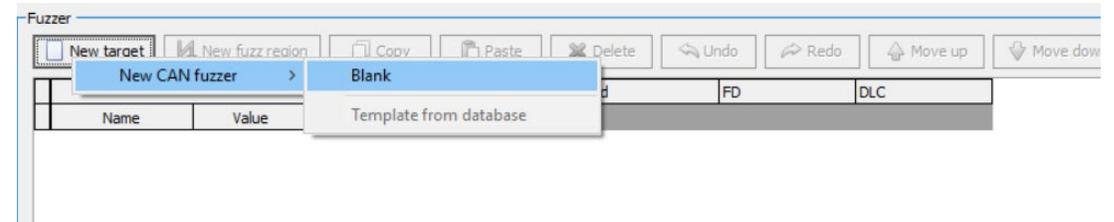
- Random is important
- Random is bad
- Pseudo Random is the answer
 - Randomization
 - Reproduceable
- If no seed given, a random seed will be generated for the test.



The image shows a configuration window titled "Configuration" with a "General" tab selected. The "Test name" field contains "My First Test". The "Use fixed random seed" checkbox is checked. The "Seed" field contains "Fixed Pseudo Random Seed".

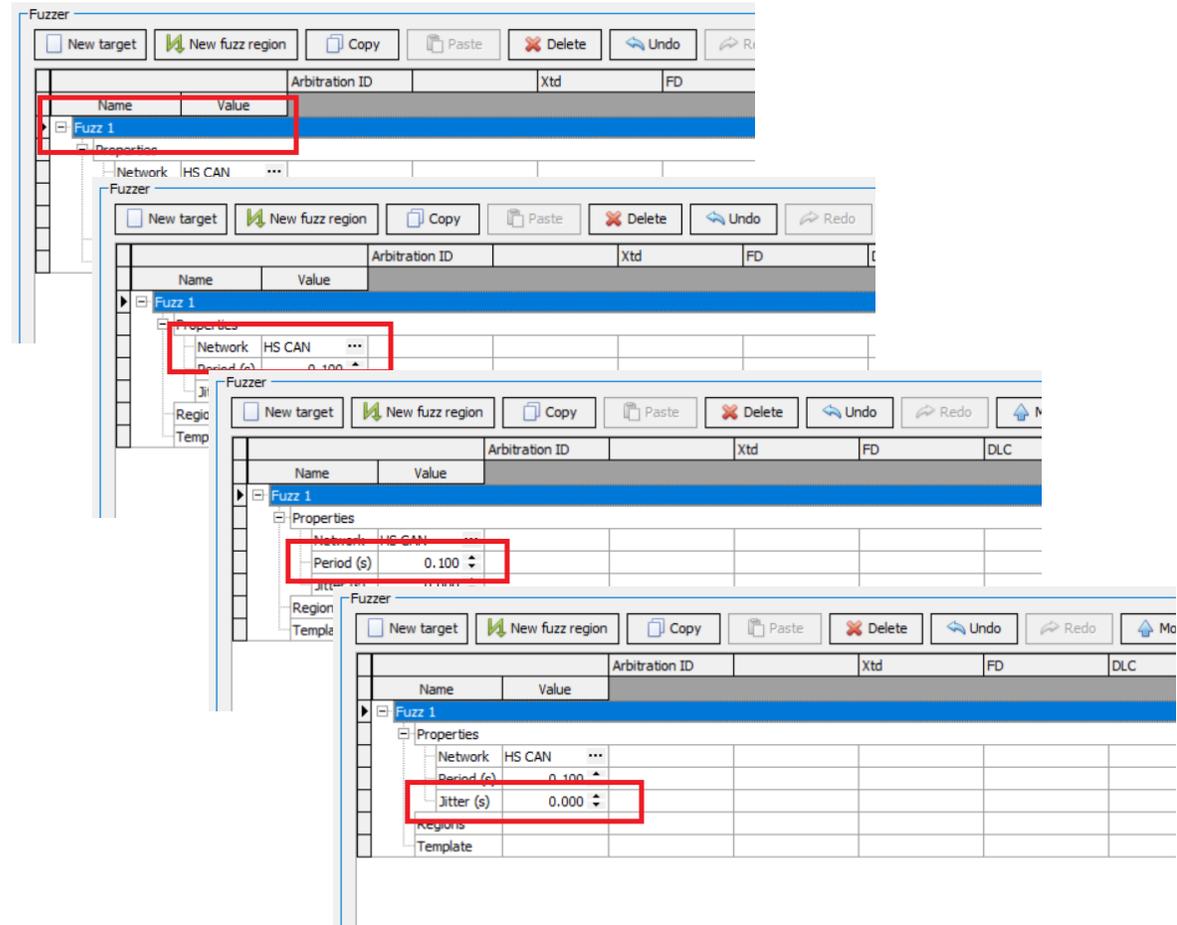
Generating a Target For the Fuzzer

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



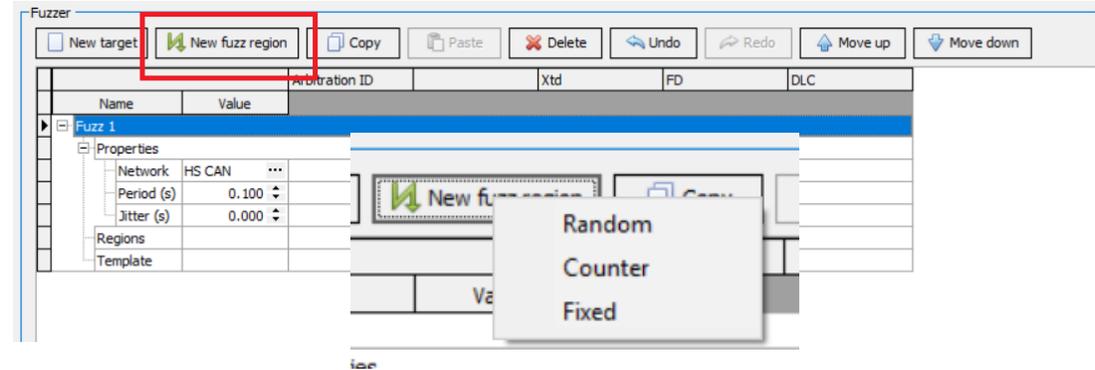
Configuring Target

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



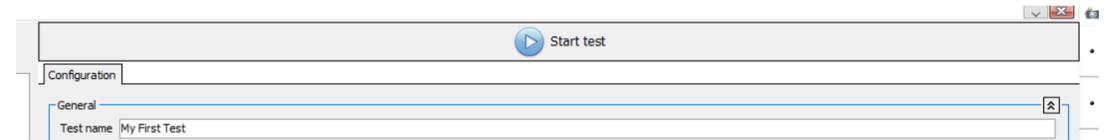
Creating Fuzz Regions

- 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.



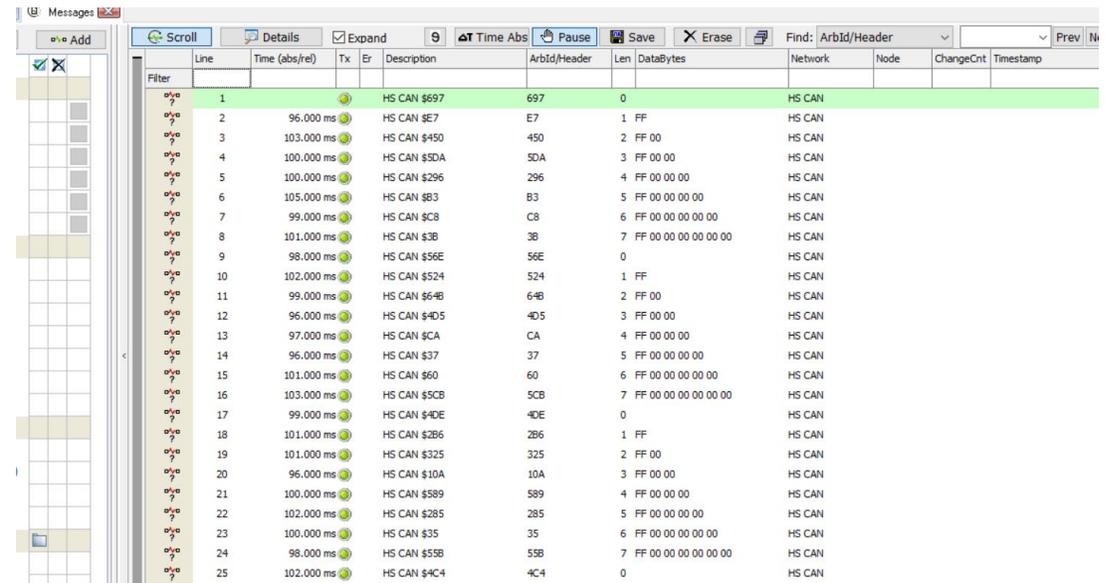
Test Information and Results

- 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 reproducible
 - Periodicity
 - Jitter
 - Fuzz Regions.



Line	Time (abs/rel)	Tx	Er	Description	ArbId/Header	Len	DataBytes	Network	Node	ChangeCnt	Timestamp
1				HS CAN \$697	697	0		HS CAN			
2	96.000 ms			HS CAN \$E7	E7	1	FF	HS CAN			
3	103.000 ms			HS CAN \$450	450	2	FF 00	HS CAN			
4	100.000 ms			HS CAN \$5DA	5DA	3	FF 00 00	HS CAN			
5	100.000 ms			HS CAN \$296	296	4	FF 00 00 00	HS CAN			
6	105.000 ms			HS CAN \$B3	B3	5	FF 00 00 00 00	HS CAN			
7	99.000 ms			HS CAN \$C8	C8	6	FF 00 00 00 00 00	HS CAN			
8	101.000 ms			HS CAN \$3B	3B	7	FF 00 00 00 00 00 00	HS CAN			
9	98.000 ms			HS CAN \$56E	56E	0		HS CAN			
10	102.000 ms			HS CAN \$524	524	1	FF	HS CAN			
11	99.000 ms			HS CAN \$64B	64B	2	FF 00	HS CAN			
12	96.000 ms			HS CAN \$4D5	4D5	3	FF 00 00	HS CAN			
13	97.000 ms			HS CAN \$CA	CA	4	FF 00 00 00	HS CAN			
14	96.000 ms			HS CAN \$37	37	5	FF 00 00 00 00	HS CAN			
15	101.000 ms			HS CAN \$60	60	6	FF 00 00 00 00 00	HS CAN			
16	103.000 ms			HS CAN \$5CB	5CB	7	FF 00 00 00 00 00 00	HS CAN			
17	99.000 ms			HS CAN \$4DE	4DE	0		HS CAN			
18	101.000 ms			HS CAN \$2B6	2B6	1	FF	HS CAN			
19	101.000 ms			HS CAN \$325	325	2	FF 00	HS CAN			
20	96.000 ms			HS CAN \$10A	10A	3	FF 00 00	HS CAN			
21	100.000 ms			HS CAN \$589	589	4	FF 00 00 00	HS CAN			
22	102.000 ms			HS CAN \$285	285	5	FF 00 00 00 00	HS CAN			
23	100.000 ms			HS CAN \$35	35	6	FF 00 00 00 00 00	HS CAN			
24	98.000 ms			HS CAN \$55B	55B	7	FF 00 00 00 00 00 00	HS CAN			
25	102.000 ms			HS CAN \$4C4	4C4	0		HS CAN			

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?