

Demo Box Manual

V1.0

VisualThreat

Chapter 1

1. Demo Box System

1.1. System Overview

The demo box system consists of: the Demo Box device, the power cable, the OBD cable and the OBD splitter, as illustrated in the following figure.



Fig. 1 Demo Box

1.2. Demo Box Components

Table 1: Testing System Component

Component	Quantity
Demo Box	1
OBD cable	1
OBD splitter	1
Power Cable	1

1.3. Product Specification

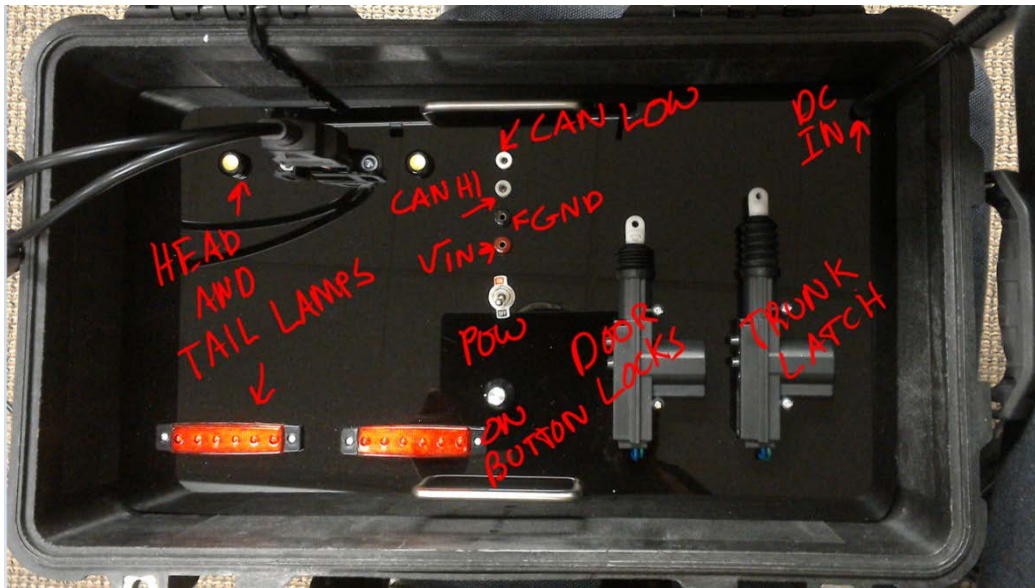


Fig. 2 Auto-X Labels-1



Fig. 3 Auto-X Labels-2

As illustrated in Figure 2, the Demo Box includes two Head Light lamps, two tail lamps, a pair of CAN High/Low pins, a pair of POWER/GND pins, power ON/OFF button, Door Locks, Trunk Latch and DC IN pin. In Figure 3, the Dashboard of Demo Box includes the RPM gauge, speedometer and fuel gauge. All the items in the Demo Box can be controlled using methods in Chapter 4.

1.4. Accessories



Fig. 3 OBD splitter



Fig.4 Power Adapter

Chapter 2

2. Connect to Demo Box



Fig.5 Device Connection

2.1. Power on the Demo Box

1. Unpack the power cable and connect it to the AC adapter which is located on the right of the Dashboard.
2. Plug the AC adapter into the DC in pin on the Demo Box and the power cable to an outlet.
3. Power on the Demo Box with the ON/OFF button making sure the toggle switch is in the on position.

2.2. Connect the OBD splitter

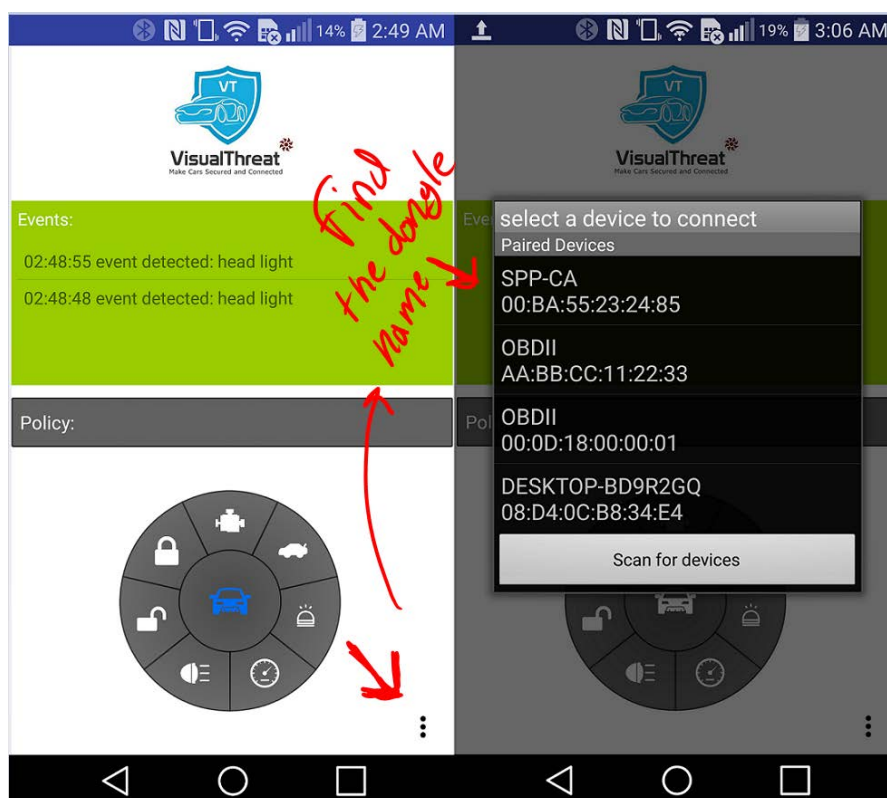
Connect the OBD splitter with the OBD interface on the Demo Box, then there will be two OBD interfaces.

Chapter 3

3. Operations on Demo Box

Control the Demo Box using the phone app

Double check that the WIFI OBD dongle is attached to the demo box and that everything is properly connected and on. Install the android app and open the phone app. Click the menu button in the bottom left corner and select the device that matches the name on the dongle connected to the Demo Box.



Once the phone is connected, test it by pressing one of the buttons on the control dial and see that the demo box reacts. The dashboard, lights and locks of the Demo Box can be controlled by using the corresponding CAN frames.

Chapter 4 (optional)

4. Testing Demo Box using VT Auto-X Box(optional package)

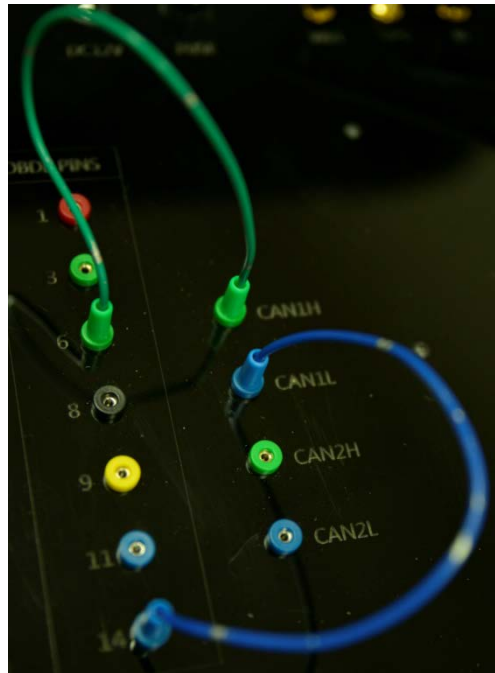


Visualthreat Auto-X box works with a web portal to control the Demo Box, easily sending the CAN frames in Chapter 3 and to bring some useful and important test cases.

4.1. Connecting the Demo Box to the VT Auto-X Box.

4.1.1 Making sure both boxes are off; connect the OBD II splitter to the OBD port on the demo box and one end of the splitter to the OBD port on the Auto-X box.

4.1.2 Using the banana cables provided, connect pin 6 to CAN 1 HI and pin 14 to CAN 1 LOW



4.1.3 Next connect the USB cable from a computer to the Auto-X box and the Wifi dongle to the other end of the OBD II splitter.



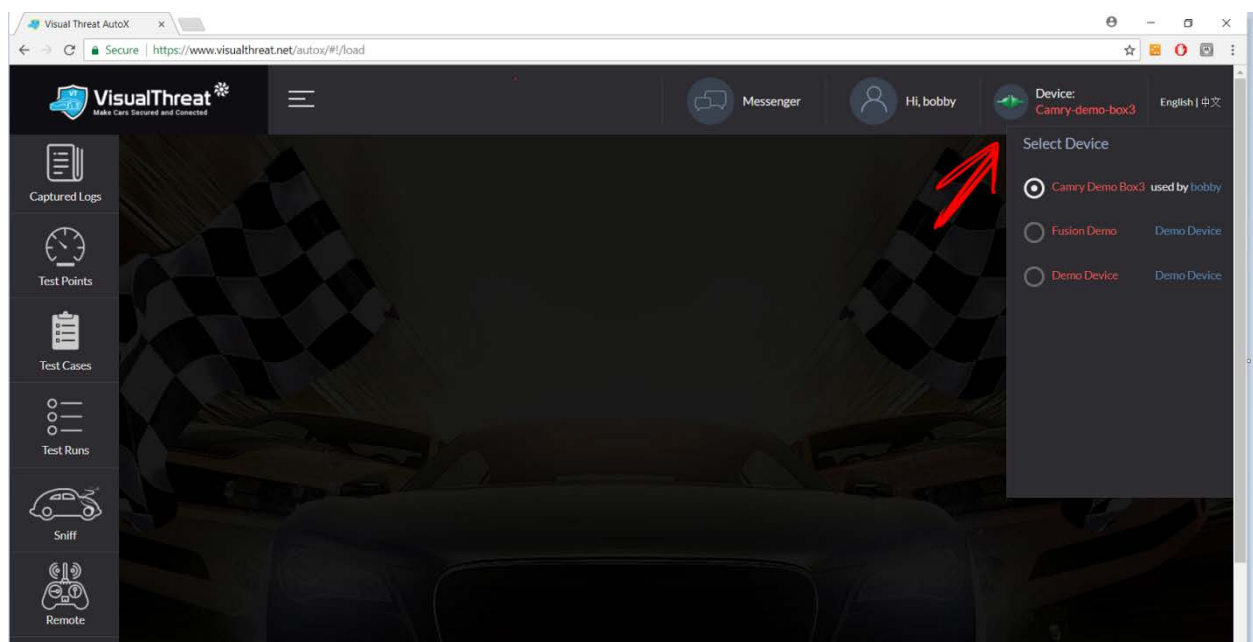
4.1.4 Connect the power cable to the demo box. With the toggle switch on the Auto-X box in the OBD II power position, turn on both the demo and Auto-X boxes.



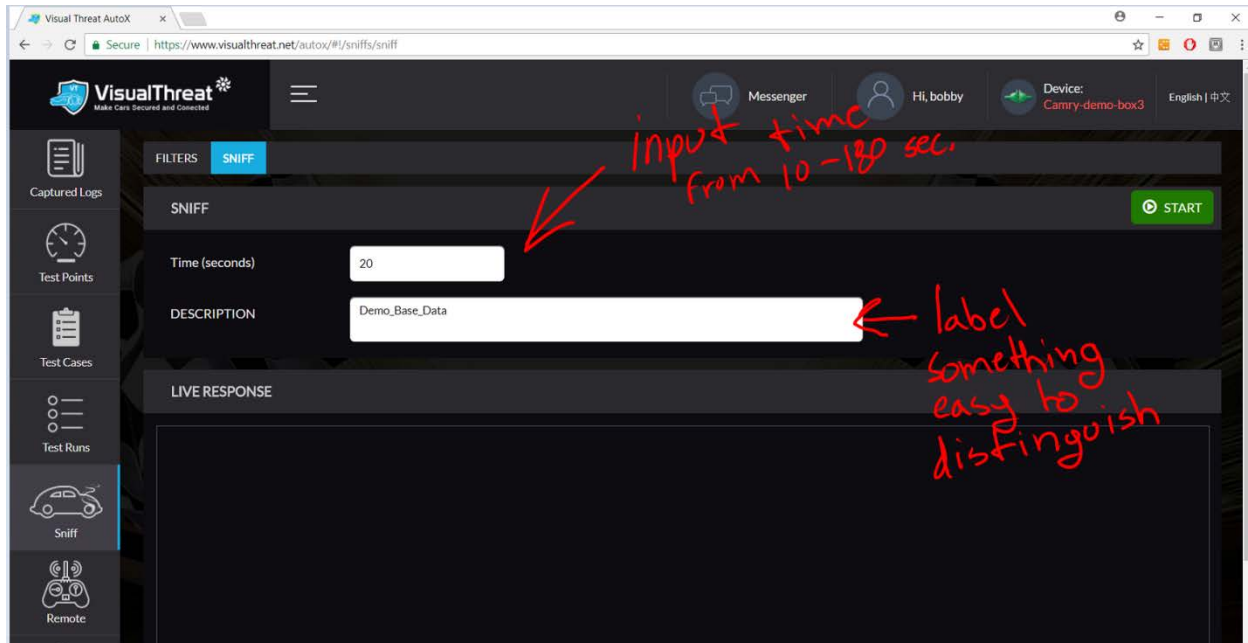
4.2. Testing Cases.

4.2.1 Collecting the initial CAN Bus data

With everything connected create a base ECU scan of the demo box. Login to the Visual Threat web app at www.visualthreat.net then select the device that the computer is connected to by clicking the cord icon in the upper right corner.

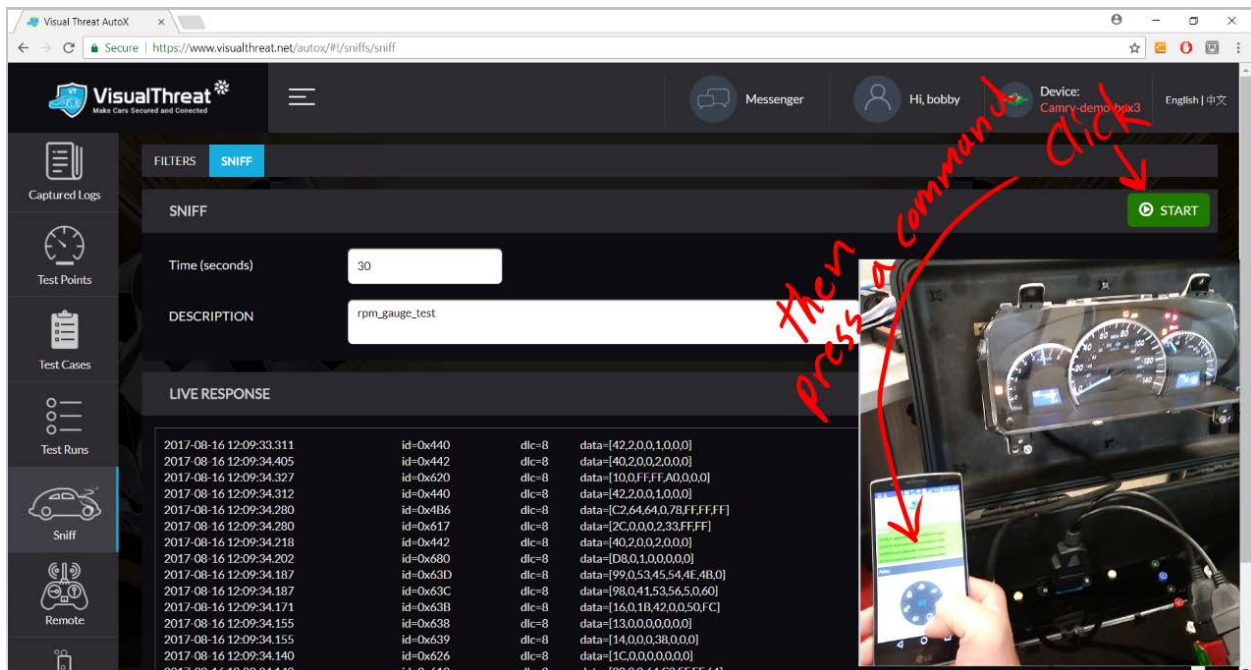


Next click the “Sniff” icon. Here a time duration will be set as well as a label for the scan. Input a time in seconds less than 180, and label the scan clearly so it is easy to find later. In this case something such as Base_Data_Scan. Then click start.



4.2.2 Collecting traffic from the Demo Box

With a phone connected to the demo box and the app open, select sniff icon from the website. Set a time and give the session a label of the CAN message that is expected to be received. In this example, the label will be rpm_gauge. Click start and while the scan is running give a command to the demo box from the phone app. The CAN bus data should be saved in the scan.

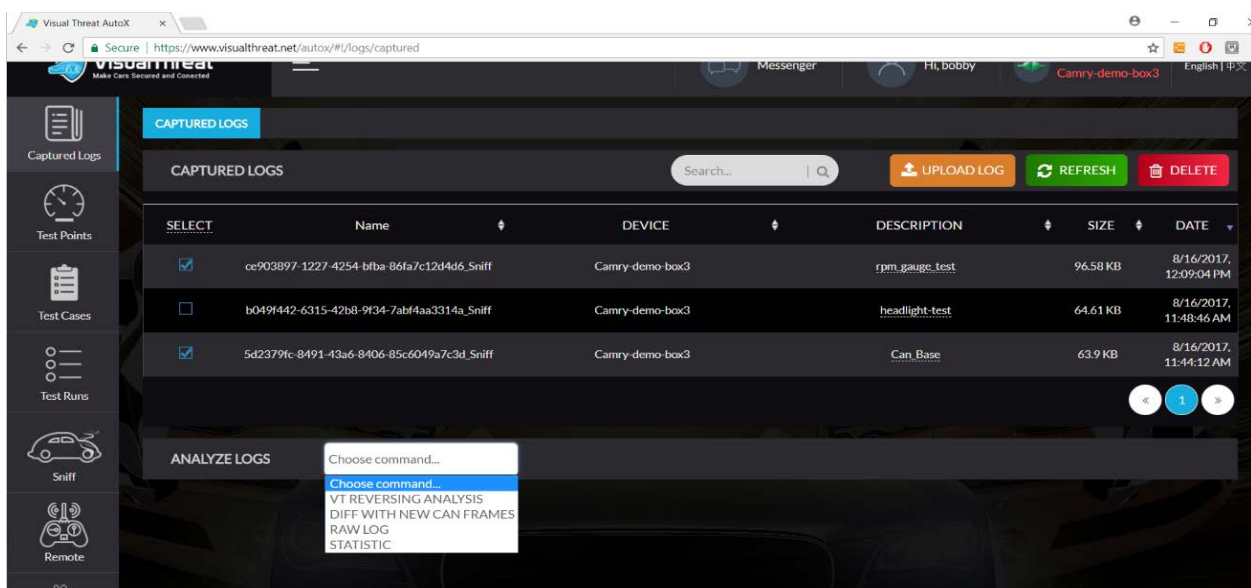


4.2.4 Reverse Engineering CAN Messages

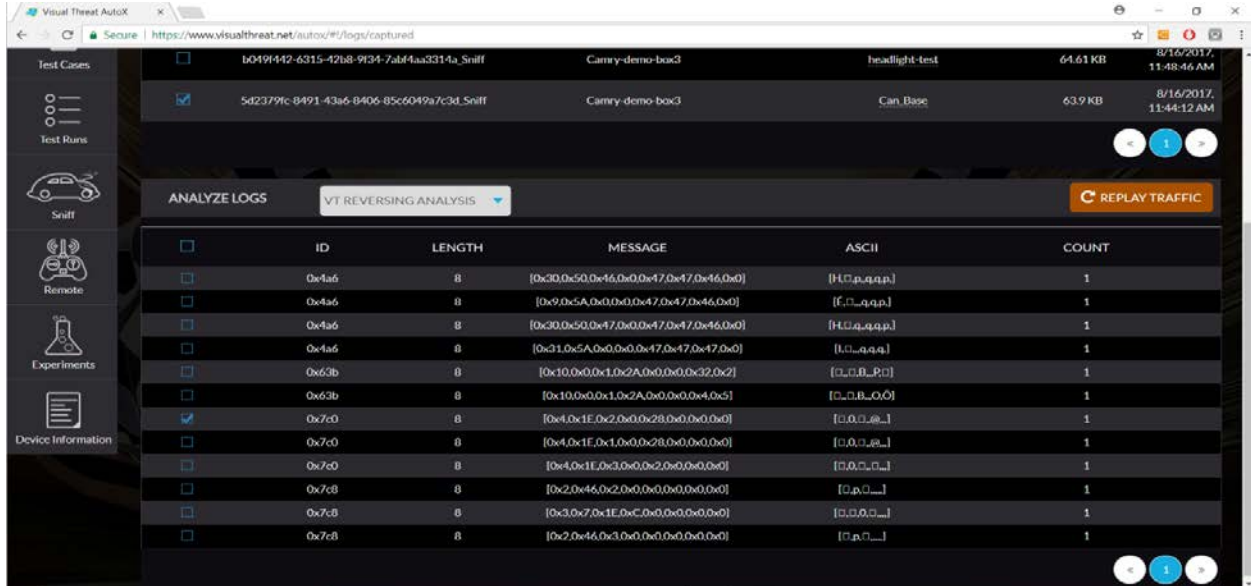
Using CAN bus data and traffic to control the demo box from the Visual Threat web app.

After traffic has been collected from the demo box while using the phone app, reverse engineer the CAN messages that control the demo box.

Click "Captured Logs" in the upper left on the Visual Threat website. Then select the base data log from earlier and at least one other traffic log. In the drop down menu next to "Analyze" select VT REVERSING ANALYSIS.



After, a list will pop up with different CAN bus messages and replay traffic button that sends the selected messages to the demo box. Messages can be selected individually or sent all at once to find which one controls the corresponding output on the demo box.



The screenshot displays the VisualThreat AutoX web interface. On the left, a sidebar contains navigation icons for Test Cases, Test Runs, Sniff, Remote, Experiments, and Device Information. The main area shows a list of captured messages at the top, including details like ID, length, message, ASCII, and count. Below this, there is a section titled 'ANALYZE LOGS' with a dropdown menu set to 'VT REVERSING ANALYSIS' and a 'REPLAY TRAFFIC' button. A table of logs is displayed below the analysis section.

ID	LENGTH	MESSAGE	ASCII	COUNT
0x4a6	8	[0x30,0x50,0x46,0x0,0x47,0x47,0x46,0x0]	[H,q,q,q,p]	1
0x4a6	8	[0x9,0x5A,0x0,0x0,0x47,0x47,0x46,0x0]	[f,q,q,q,p]	1
0x4a6	8	[0x30,0x50,0x47,0x0,0x47,0x47,0x46,0x0]	[H,q,q,q,p]	1
0x4a6	8	[0x31,0x5A,0x0,0x0,0x47,0x47,0x46,0x0]	[l,q,q,q,q]	1
0x63b	8	[0x10,0x0,0x1,0x2A,0x0,0x0,0x32,0x2]	[C,C,B,P,D]	1
0x63b	8	[0x10,0x0,0x1,0x2A,0x0,0x0,0x4,0x5]	[C,C,B,O,O]	1
0x7c0	8	[0x4,0x1E,0x2,0x0,0x28,0x0,0x0,0x0]	[C,C,C,_]	1
0x7c0	8	[0x4,0x1E,0x1,0x0,0x28,0x0,0x0,0x0]	[C,C,C,_]	1
0x7c0	8	[0x4,0x1E,0x3,0x0,0x2,0x0,0x0,0x0]	[C,C,C,_]	1
0x7c8	8	[0x2,0x46,0x2,0x0,0x0,0x0,0x0,0x0]	[p,p,_]	1
0x7c8	8	[0x3,0x7,0x1E,0x0,0x0,0x0,0x0,0x0]	[C,C,C,_]	1
0x7c8	8	[0x2,0x46,0x3,0x0,0x0,0x0,0x0,0x0]	[p,p,_]	1

Contact Us



email : info@visualthreat.com

web : www.visualthreat.com