CAN bus

Attack Traffic Generation(ATG) tool

-Start Guide

Instruction on Using the ATG

testbed

Jun. 2018

Tables of Contents

[**1 Getting Started** - 3 -](#_Toc517776133)

[**1.1 Current Version** - 3 -](#_Toc517776134)

[**1.2 CAN Interface** - 3 -](#_Toc517776135)

[**1.3 Installing Drivers** - 3 -](#_Toc517776136)

[**2 Using ATG** - 4 -](#_Toc517776137)

[**2.1 Activate Interface** - 4 -](#_Toc517776138)

[**2.2 Packets Sniffer** - 4 -](#_Toc517776139)

[**2.2.1 Starting tracing** - 4 -](#_Toc517776140)

[**2.2.2 Changing display style** - 5 -](#_Toc517776141)

[**2.2.3 Packets Logging** - 5 -](#_Toc517776142)

[**2.2 Playback** - 6 -](#_Toc517776143)

[**2.3 Attack Tool** - 6 -](#_Toc517776144)

[**2.3.1 DoS attack** - 6 -](#_Toc517776145)

[**2.3.1 Fuzzing attack** - 6 -](#_Toc517776146)

[**2.3.2 Spoofing attack** - 6 -](#_Toc517776147)

[**2.3.4 Automatic attack** - 7 -](#_Toc517776148)

[**2.4 CAN Matrix Convert** - 9 -](#_Toc517776149)

[**2.5 Dataset Format Convert** - 9 -](#_Toc517776150)

[**3 About more** - 9 -](#_Toc517776151)

# **1 Getting Started**

ATG is a vehicle CAN bus packet analyzer and attack packets generator. ATG enable researchers to begin to explore automotive cyber-physical system rapidly. To a certain extent, it can verify the cyber security solution of in-vehicle CAN bus and ECUs with different attack modes. For some novel IDS countermeasures, it is also a good tool to generate a dataset, and test it in python environment.

**1.1 Current Version**

This specification is based on ATG version Beta (released 15 Nov. 2017), running on Windows XP, Vista, 7, 8, 10 (64 and 32).

**1.2 CAN Interface**

USB2CAN is the default CAN bus interface of ATG. It provides drivers for Windows and Linux system. Meanwhile, for the developer, it provides DLL (Dynamic Link Library) for windows application and Socket CAN drivers for Linux application.

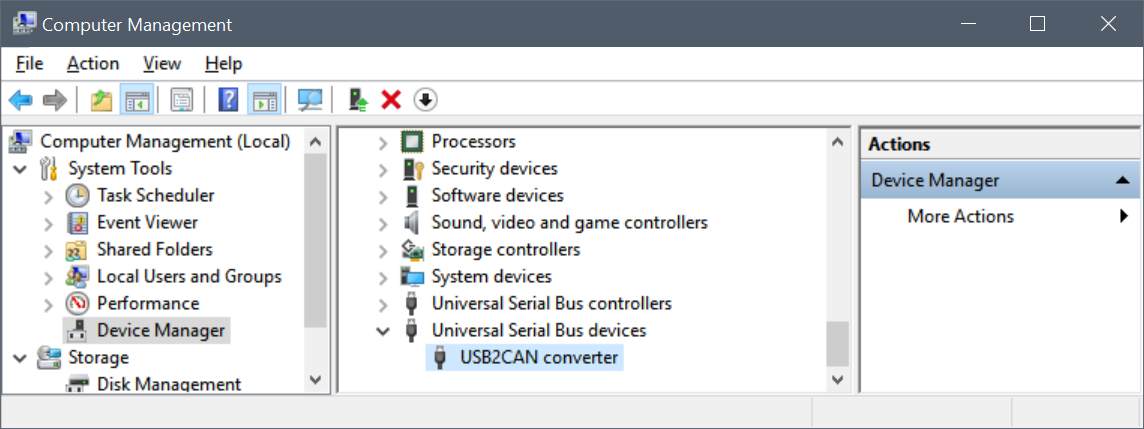
You can buy this device from 8device website: <http://www.8devices.com/products/usb2can> The price is only $65.

**1.3 Installing Drivers**

Firstly, you should install the drivers on windows. You can download the drivers from 8device website:

64bit:<http://www.8devices.com/media/products/usb2can/downloads/usb2can_win64_v1.0.2.1.zip>

32bit:<http://www.8devices.com/media/products/usb2can/downloads/usb2can_win32_v1.0.2.1.zip>

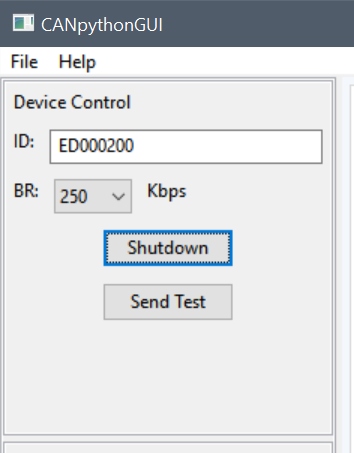


You can see the device information in Device Manager when you success to install the drivers.

**2 Using ATG**

**2.1 Activate Interface**

After connecting the CAN device to the computer and running ATG, you should check the device id at the back of the device and input it in ***ID*** input box. And then, select the suitable baud rate (range from 10 to 1000 Kbps). At last, you can click the ***Open*** button to activate interface. If the text changes to ***Shutdown***, it means there is no problem. When the device is at activated state, the LED color on the USB2CAN become green. Otherwise it is still red.

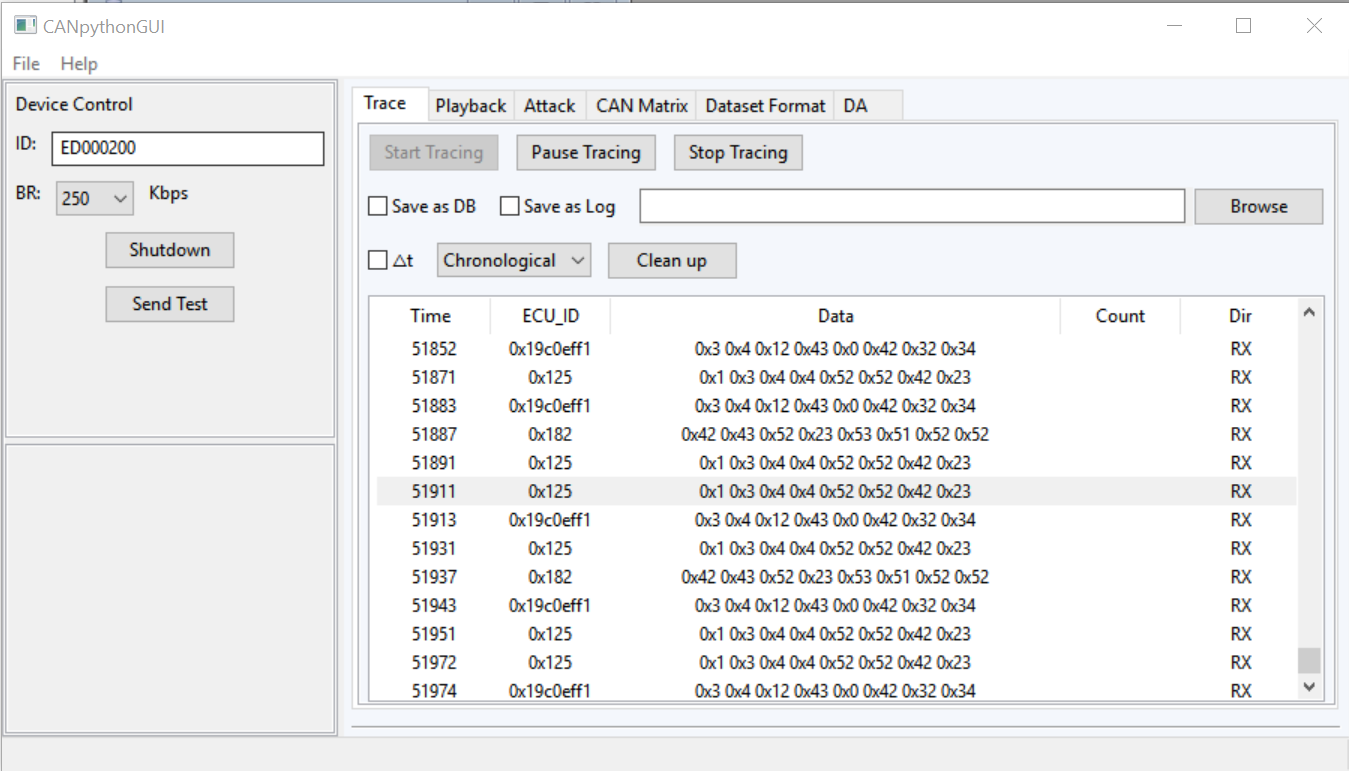
 

**2.2 Packets Sniffer**

This is the basic function of ATG. It can collect the packets in real time and display in a different way.

**2.2.1 Starting tracing**

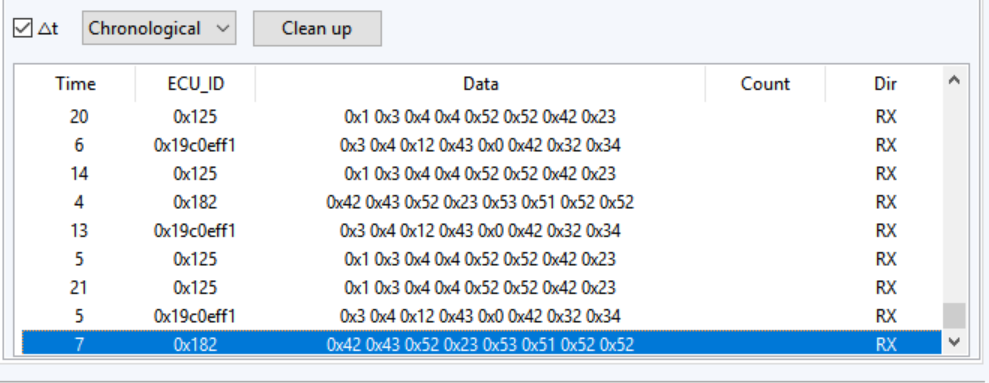
When you click the ***Start Tracing*** button, the trace window shows the packets including ***Time(ms)***, ***ECU\_ID***, ***Data***, and ***Dir*** (RX denote Receiving, TX denote Transmitting) information.



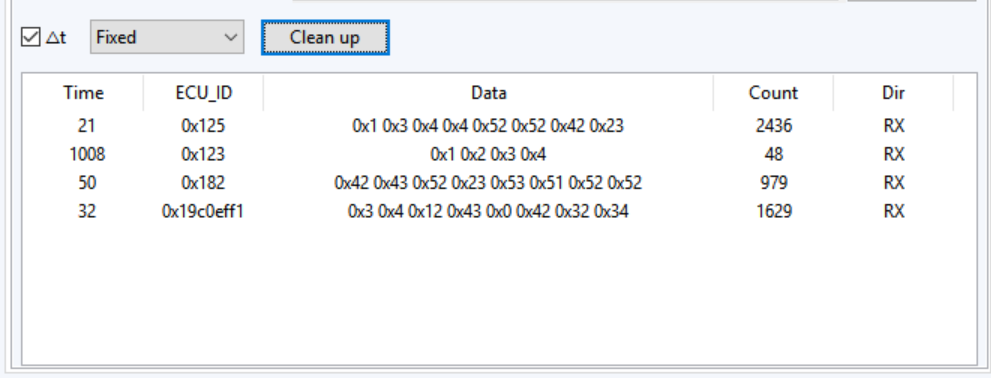
**2.2.2 Changing display style**

You can click the ***checked box*** ***△t*** to switch thetime type between interval and timestamp. You can select the message refresh mode in the choice box, ***Chronological mode*** record and show all packets, ***Fixed mode classify*** packets by ID and fix the position with each kind of packet. Following figures show the difference between two modes.

***Chronological mode:***



***Fixed mode:***



**2.2.3 Packets Logging**

To make it possible and easy to analyze the entire packets after you get these from a real vehicle, ATG supports two kinds of logging file formats, database file(.db) and log file(.log). You can check ***Save as DB*** or ***Save as log*** checkbox and select the storage path. This can show and store packets at the same time after you click ***Start Tracking*** button. When you complete logging, you can open log file in Notepad and database file in database view software, such as SQLite Expert Personal 3. Another difference between these two formats is that only the log format file can label the attack packets when you launch attacks and playback.

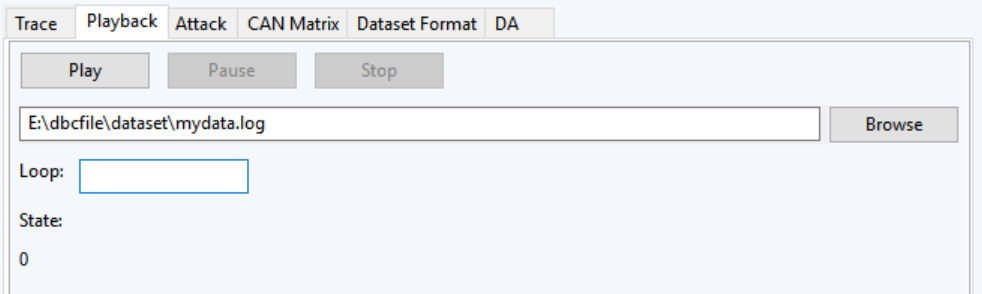
Comparing to other software logging feature the advantages of ATG are:

1. Candump module of can-utils[[1]](#footnote-1) (<https://github.com/linux-can/can-utils>) just can logging data, it cannot generate attack packets and label them.
2. CANoe[[2]](#footnote-2) store packets as \*.blf/\*.asc/\*.mf4 binary format file. You cannot analysis directly, and the Adaptive CAN interface is expensive.

ATG not only guarantee the performance to store a huge number of packets but also make it easy to modify and analyze the dataset.

**2.2 Playback**

Playback function can help you to replay the log file. After you select the log file, you can click ***Play*** button to launch the data into CAN bus. You can also pause or stop it.



**2.3 Attack Tool**

**2.3.1 DoS attack**

In the DoS attack mode, ATG can inject the highest priority packet of 0x0 CAN ID every 1 millisecond.

**2.3.2 Fuzzing attack**

In the Fuzzing attack mode, ATG can inject the random ID and random data.

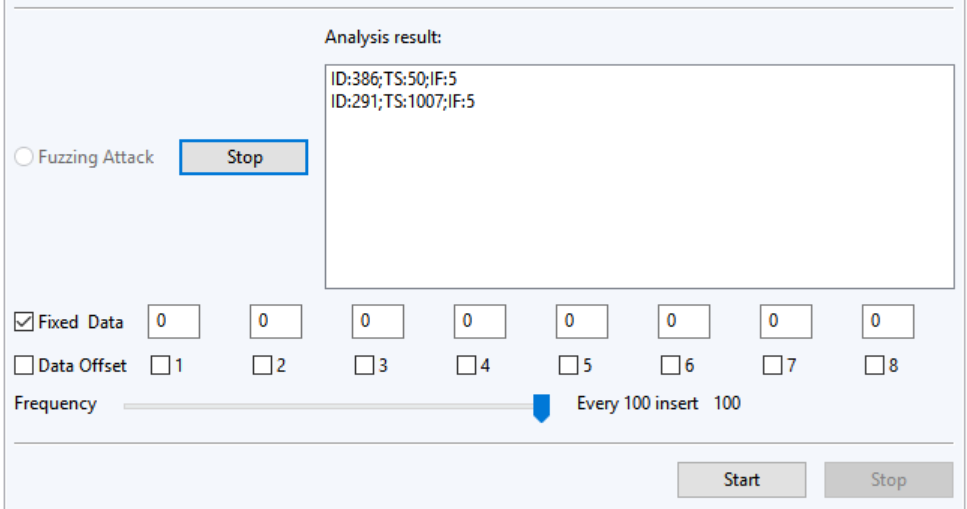
**2.3.3 Spoofing attack**

After sniffing and marking the control field in a control frame, it is easy to use a reverse engineering. ATG can inject the malicious message in a shorter interval than the normal nodes, which causes the receiving node to execute a dangerous operation.

The step to launch fuzzing attack is as follows.

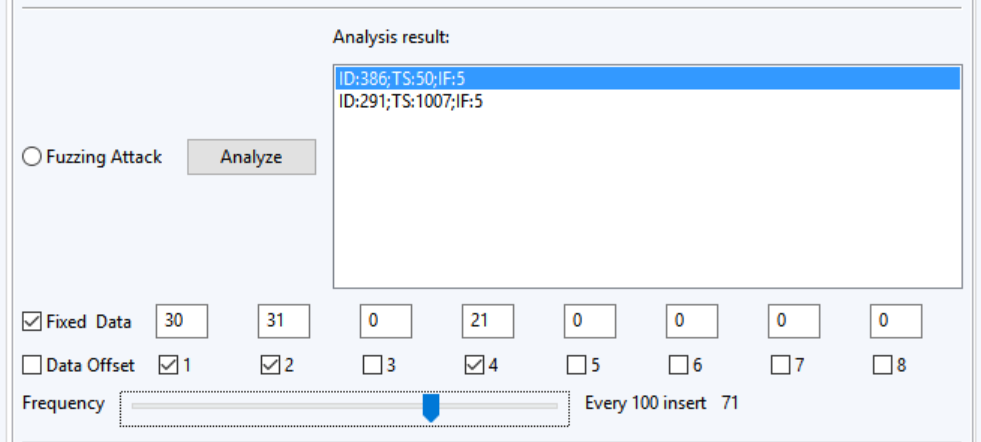
1. Analyzing the packets

In the ***Attack Tab***, you can click ***Analyze button*** to get and classify the packets. For example, in the following figure, you can see there are two kinds of packets 386(0x182) ID and 291(0x123) ID, ***TS*** is the interval, ***IF*** is a flag to judge whether this packet is cyclic, 5 means it is.



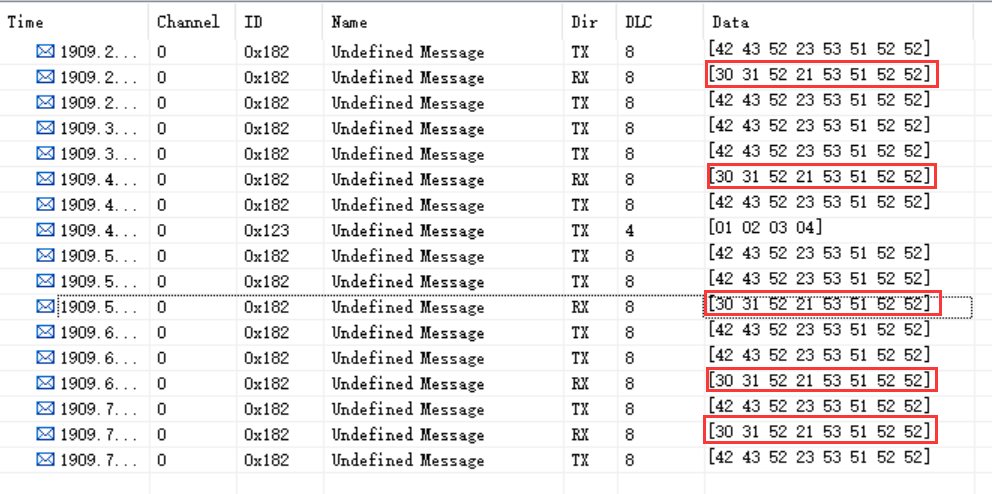
1. Selecting target packet and Configuring parameters

You can select the target message in the analysis result box. And then you can configure the appointed byte of attack packet. Shown as following, you can input 30, 31 and 21 in the first, second and fourth input box, and check the checkbox under them. The default mode is ***Fixed Data***, under this mode, it just replaces the selected byte of original data to a preset value. Under the ***Data Offset*** mode, it adds the value to the original data. You can also change the frequency of attack by the slider to make the injected messages difficult to find.



1. Launching attack

You can check the ***Spoofing Attack*** Radio button and click ***Start*** button to launch such attack. In the following picture, I use another software to check the attack messages.



**2.3.4 Automatic attack**

Usually, it is not convenient to manually launch an attack event by previous way. So ATG provides attack config function. You can define the attack events in an XML file. ATG can load it and trigger them one by one.

The config format is similar to the attack config above:

1. DoS attack

Sample:

<attack type ="DoS">

<start\_time>2</start\_time>

<end\_time>4</end\_time>

</attack>

In the attack node, define the type attribute as “DoS”, then set the start time and end time (s).

1. Fuzzing attack

Sample:

<attack type ="Fuzzing">

<start\_time>60</start\_time>

<end\_time>70</end\_time>

<message type ="fixed">

<target\_id>19C0EFF1</target\_id>

<active\_byte>AA</active\_byte>

<frequency>21</frequency>

</message>

</attack>

In the attack node, Define the type attribute as “Fuzzing”, then set the start time and end time. In the message node, the type attribute can be configured as “random” or “fixed”. Random mode denotes the ID and Data are randomly generated; fixed mode means the relevant bytes would be randomly generated then define the target\_id . active\_byte and frequency.

1. Spoofing attack

Sample:

<attack type ="Spoofing">

<start\_time>80</start\_time>

<end\_time>110</end\_time>

<message type ="offset">

<target\_id>125</target\_id>

<data>00 00 00 00 21 23 21 11</data>

<active\_byte>0F</active\_byte>

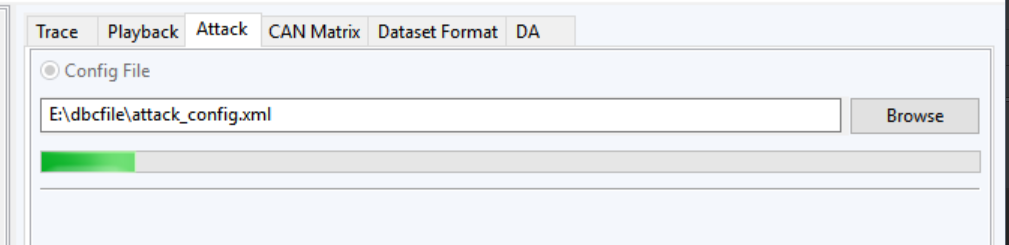
<frequency>21</frequency>

</message>

</attack>

In the attack node, Define the type attribute as “Spoofing”, then set the start time and end time. In the message node, you can define the type attribute as “fixed” or “offset”, then define the target\_id, data, active\_byte and frequency. Fixed mode denotes the target bytes can be modified to fixed value; Offset indicates adding offset value on the original value of target bytes (offset value can be minus).

When you launch an automatic attack, there is a progress bar shows the attack progress.



**2.4 CAN Matrix Convert**

CAN Matrix can convert can matrix file among different format.

It is an open source project on GitHub. You can get more information on the website: <https://github.com/ebroecker/canmatrix>.

ATG only call it and make it easy to use in window interface. With this tool, you can convert a can matrix file to an XML file which can be easy to load in an embedded IDS (Intrusion Detection System) as the detection rules.

**2.5 Dataset Format Convert**

A Database file is not a general format of the dataset, so you can use this tool to convert the database file to a .CSV (Comma-Separated Values) file. You can share this file with other researchers in more general ways.

**3 About more**

1. ATG based on python which is the popular language in analysis and AI research field. If you want to develop an IDS system by machine learning method, ATG is the best way to achieve your goal.
2. For the CAN bus interface, USB2CAN is the only available interface in the beta version. To improve the performance, in the later version we will support more interfaces such as Kvaser, PCAN and so on.

1. A CAN bus utilities and tools on Linux(<https://github.com/linux-can/can-utils>) [↑](#footnote-ref-1)
2. CANoe is a development and testing software tool from Vector Informatik GmbH. [↑](#footnote-ref-2)