Test Setup 1: Individual PC

This tutorial/laboratory practice is designed for individual completion on one's own device during the designated lab session. This setup has been validated for use on the Windows operating system. For this purpose, the following tools must be installed on the user's device:

1. **Wireshark** is a tool for network traffic sniffing, packet visualisation, and analysis. It can be downloaded from https://www.wireshark.org/download.html.
2. **ColaSoft PacketBuilder:** This graphical user interface (GUI)-based tool is intended for editing and replaying network packets, allowing modification of both raw packet header fields and the payload. This tool requires the installation of **Npcap** (https://npcap.com/#download); therefore, Npcap must be installed first.
3. **Bit-Twist** is a simple yet powerful command-line interface (CLI) utility, based on libpcap, for packet editing and replay. It can be downloaded from https://bittwist.sourceforge.io/. This tool doesn't require installation and can be simply run using the command window.
4. **IED Scout** from Omicron: This GUI-based tool functions as an IED simulator. A 30-day trial version is available for download from: https://www.omicronenergy.com/en/products/iedscout/. It acts as an IED simulator and includes:
    - A Simulator Tab, which can be utilised to simulate the MMS server and the GOOSE publisher.
    - A Browser Tab, which can be utilised to simulate the MMS client and the GOOSE subscriber.

Lab MITM (Man-In-The-Middle): Malicious/False Command Injection (FCI) on GOOSE XCBR Position Control value

Tactic: Impact

The adversary is attempting to manipulate, disrupt, or compromise your ICS systems, data, and their surrounding environment.

Technique: Manipulation of Control.

Adversaries may manipulate physical process control within the industrial environment. Methods of manipulating control can include changes to set point values, tags, or other parameters. Methods of Manipulation of Control include:

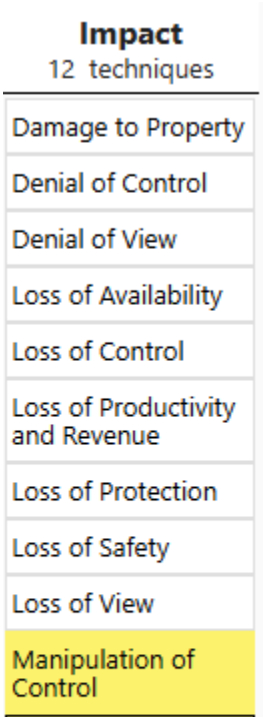
- Man-in-the-middle
- Spoof command message
- Changing setpoints

In this case, the MITM is considered to inject malicious GOOSE packets into the network, which would result in the “Manipulation of Control".

Tools Required:

1. **IED Scout:** GOOSE Publisher/ Subscriber
2. **ColaSoft Packet Builder:** To edit the GOOSE packets (.pcap file)
3. **Wireshark:** To sniff the GOOSE traffic and save it in .pcap format for play later.
4. **Bit-Twist:** To play the captured traffic (.pcap file)

MITRE ATT&CK Mapping



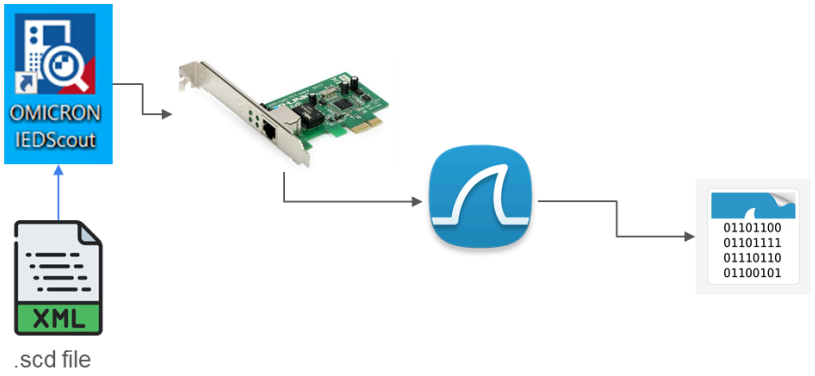
Two approaches can be used to demonstrate this:

1. Capture the live GOOSE traffic first and then use it in the next step.
2. Using the already available .pcap files for the GOOSE traffic to manipulate the control and play back directly.

1. Capture the live traffic

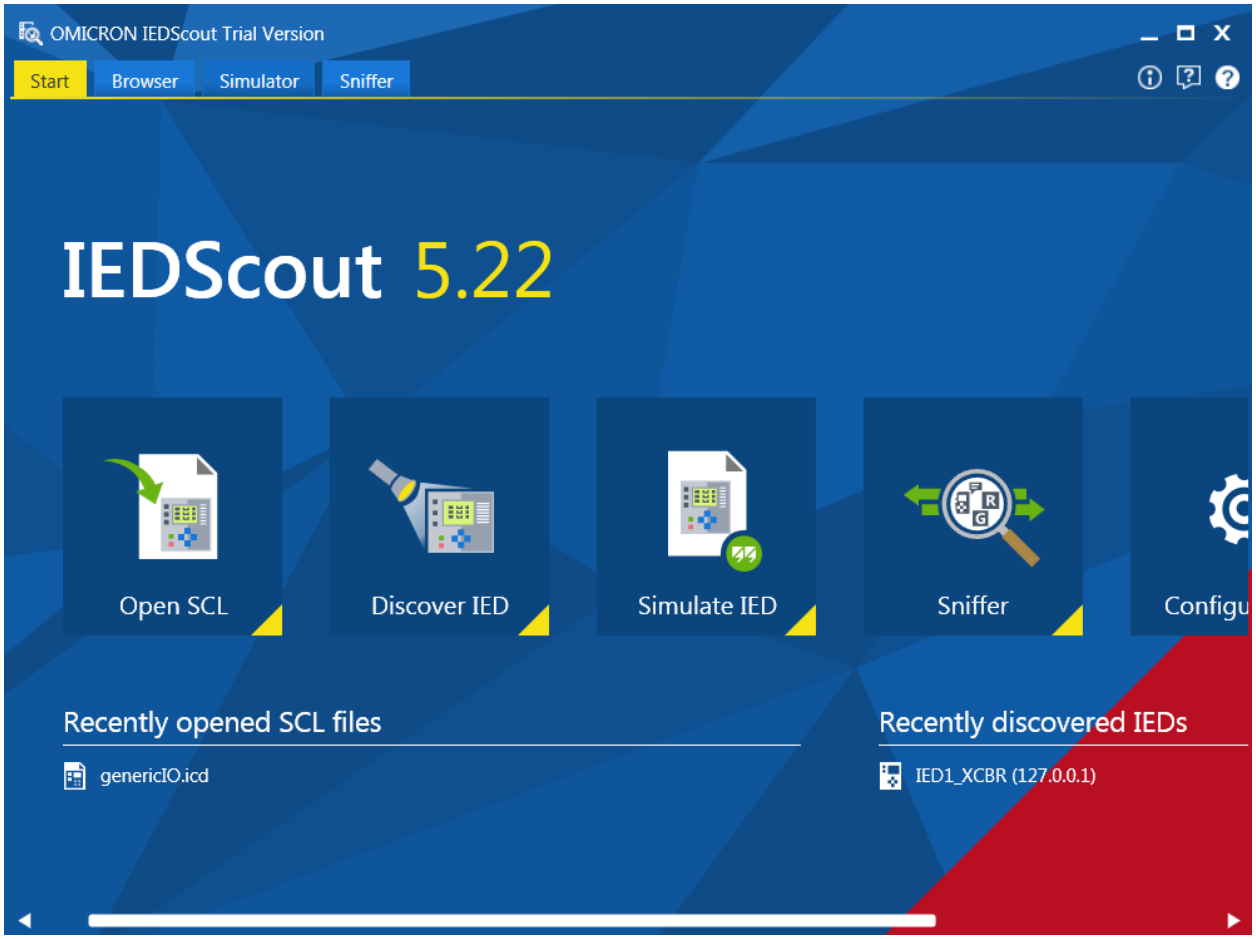
Tools required:

- **IEDScout:** GOOSE Publisher/ Subscriber both.
- **Wireshark:** To sniff the GOOSE traffic and save it in .pcap format for later use.



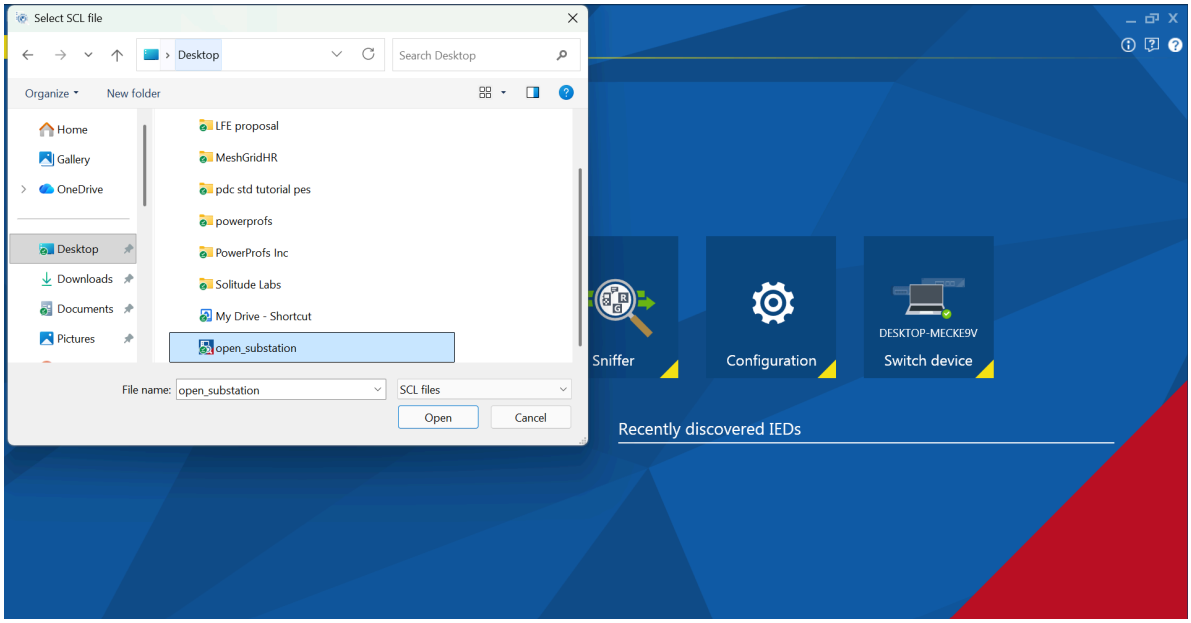
GOOSE live capture generation.

1.1 Run the IEDScout software

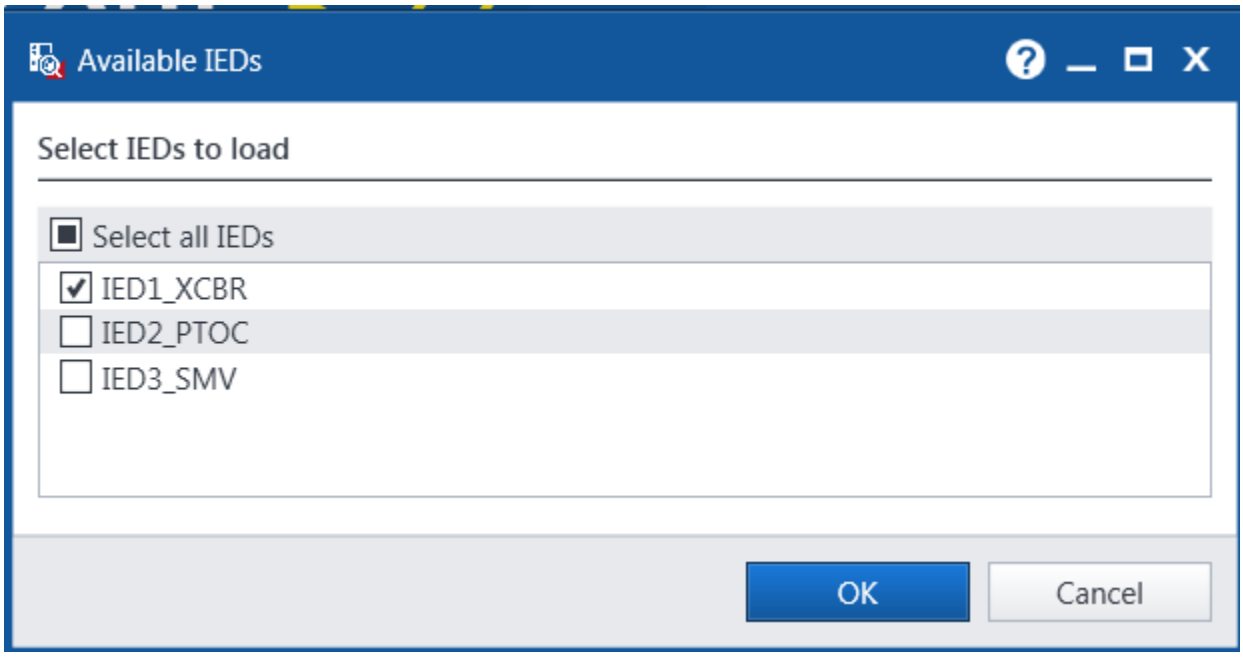


1. Click on the “**Simulate IED**” option.

2. Select the .scd file name **“open_substation.scd”**

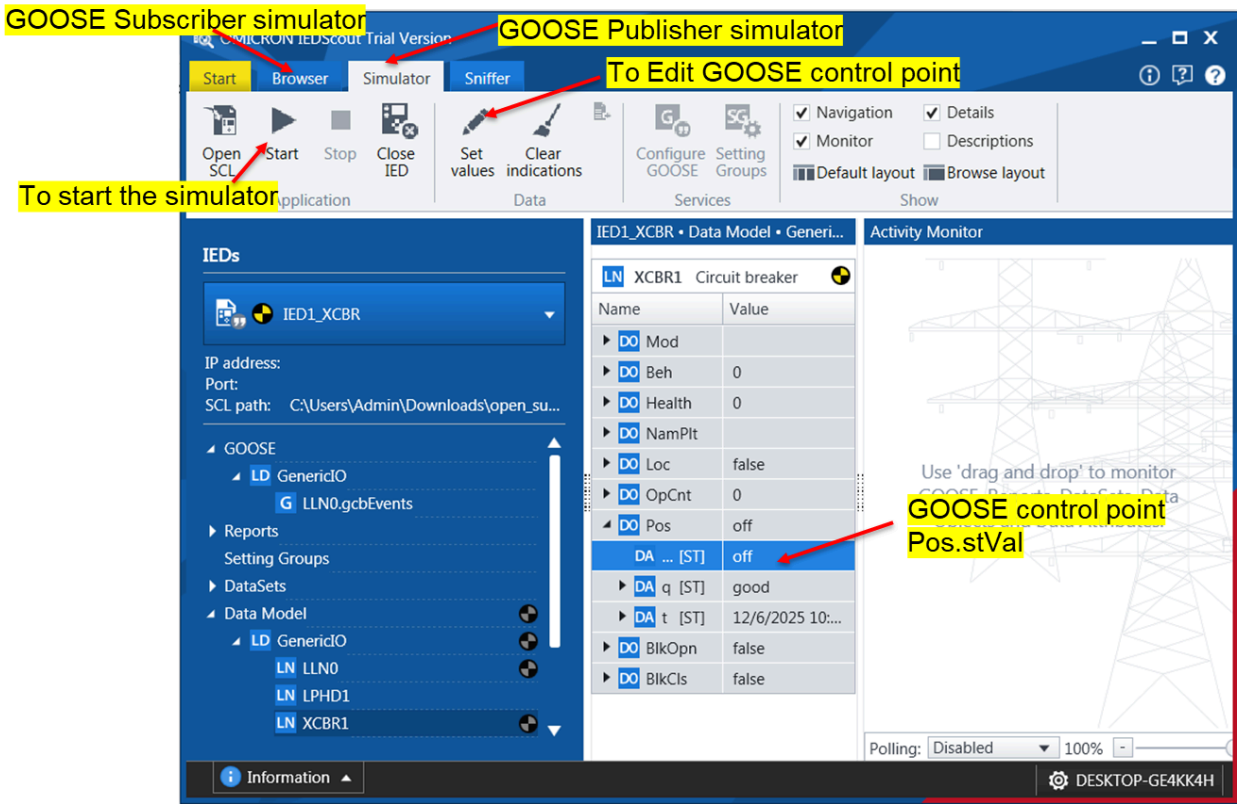


3. It will display the list of IEDs available from the .scd file. Select at least **IED_XCBR** (or) you can select all as well, then click on “**OK**”

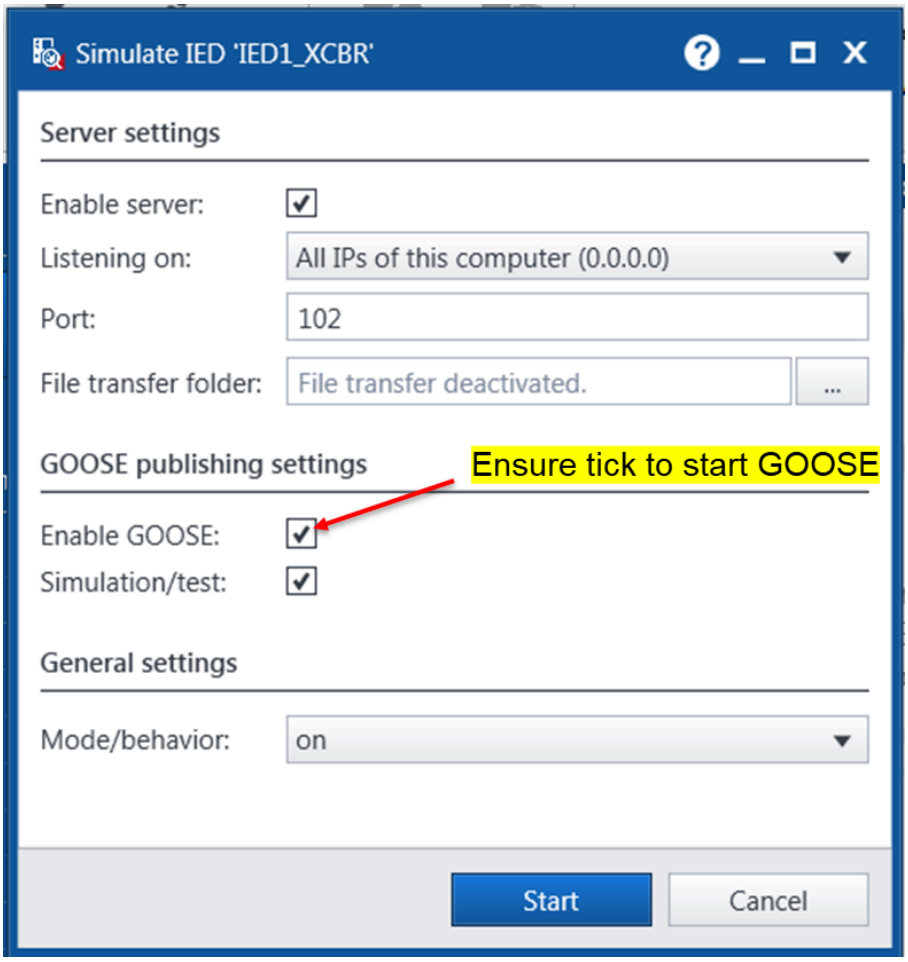


1.2 Start the GOOSE simulator

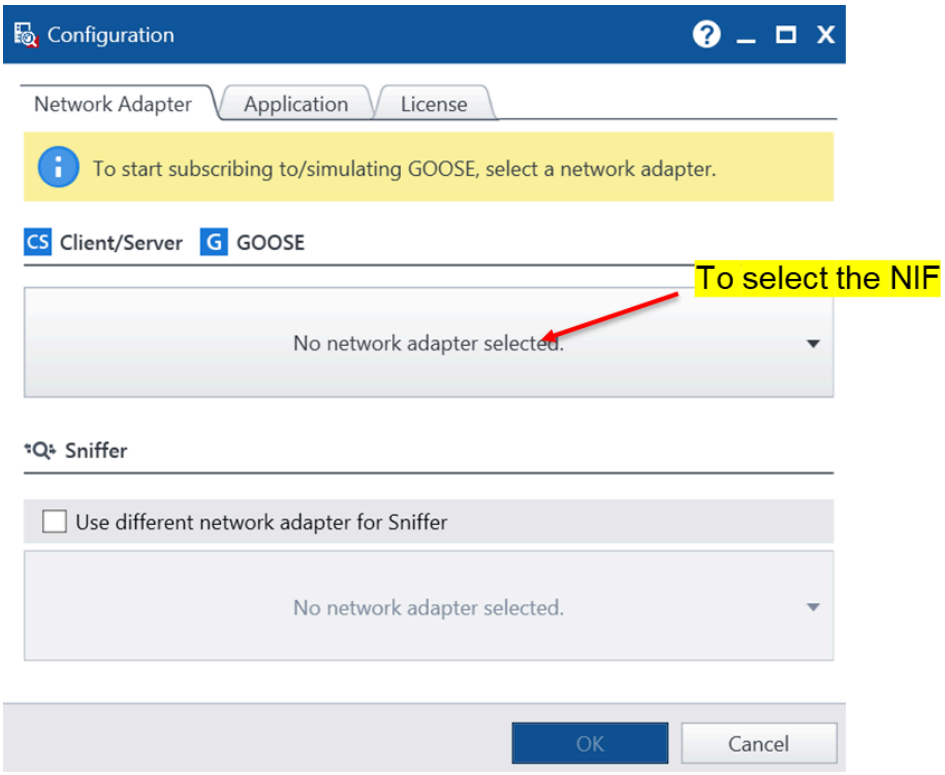
4. Click on the “**Start**” Button from the Top Toolbar menu to start the IED simulator.



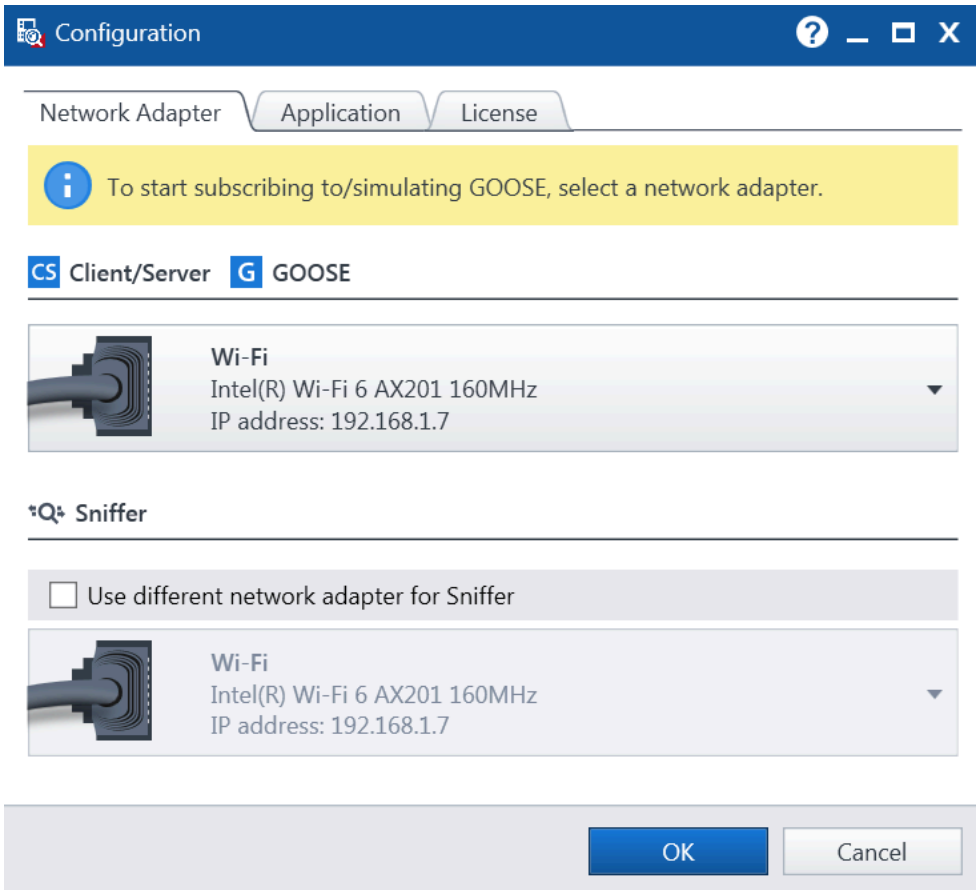
5. A configuration menu will appear; ensure the "**Enable GOOSE**" option is selected before clicking the "**Start**" button.



6. Select the network interface (NIF) from the list available by clicking on the dropdown list as shown below

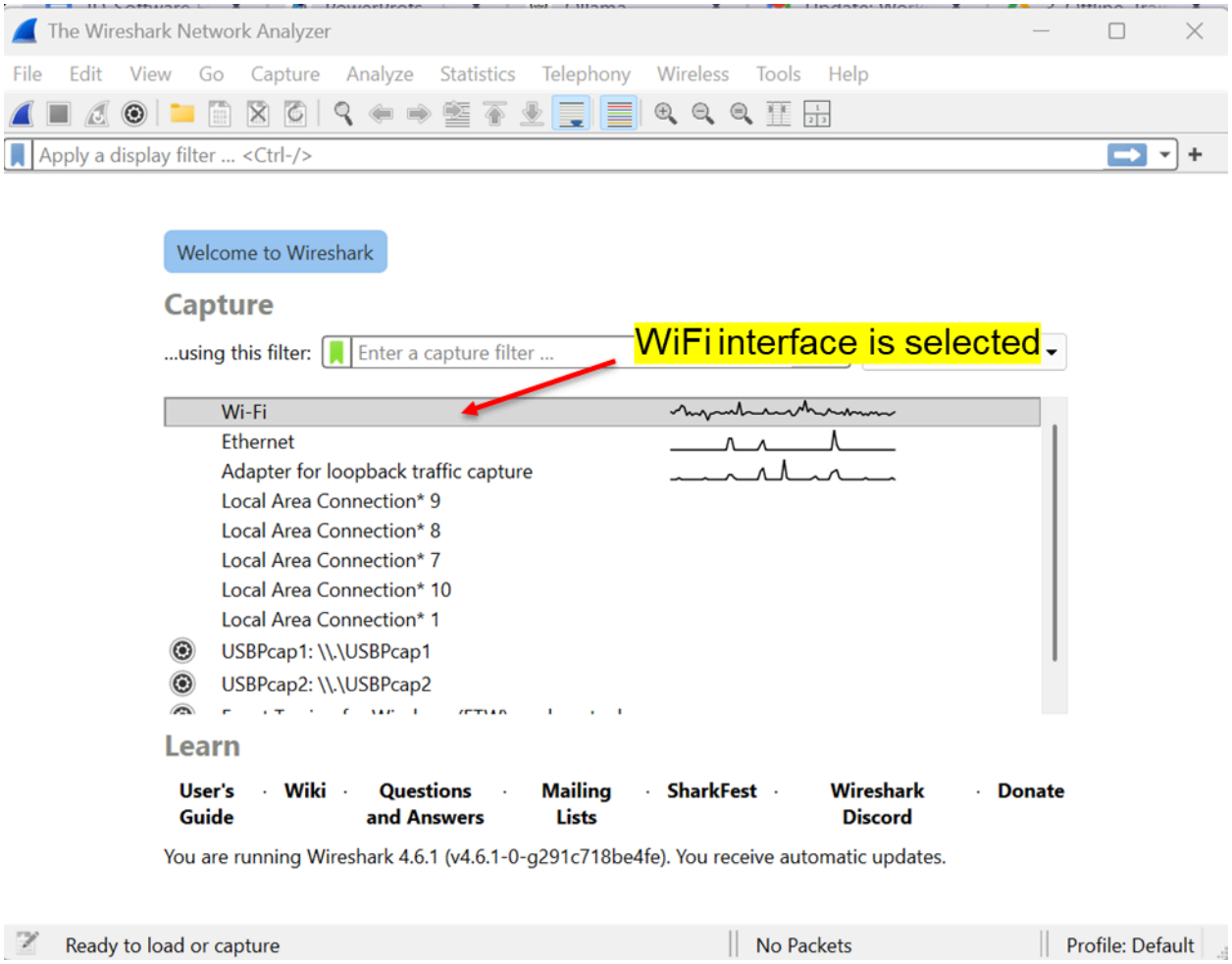


7. In this case, the **Wi-Fi interface** is selected from the list

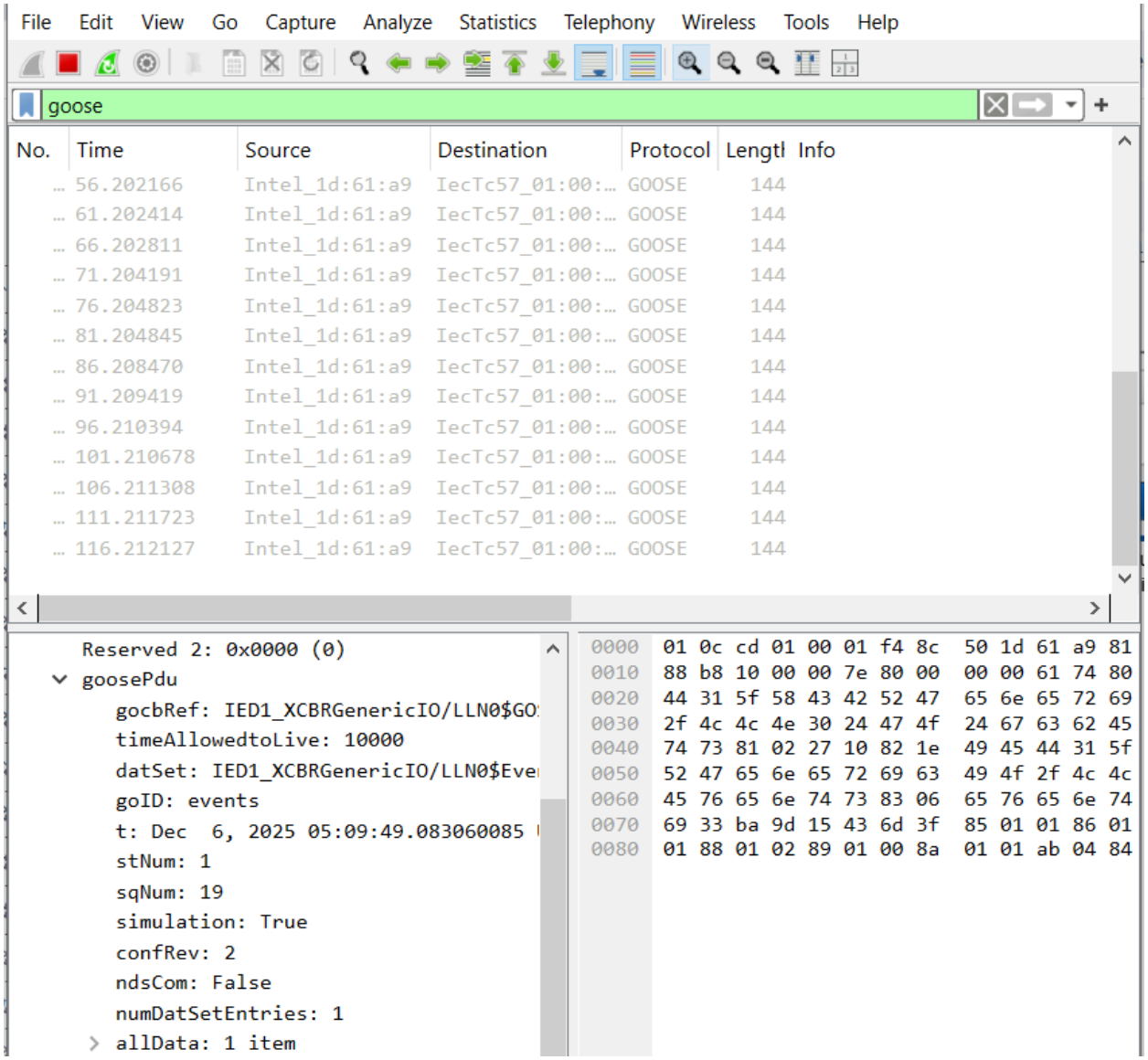


1.3 Packet Capture with Wireshark

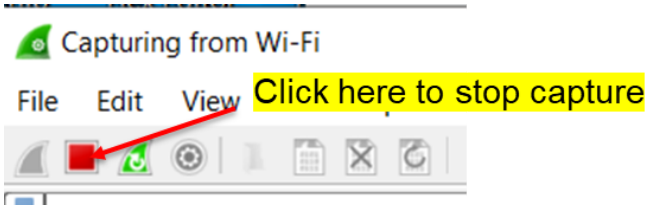
8. Open Wireshark and select the **same NIF to capture**.



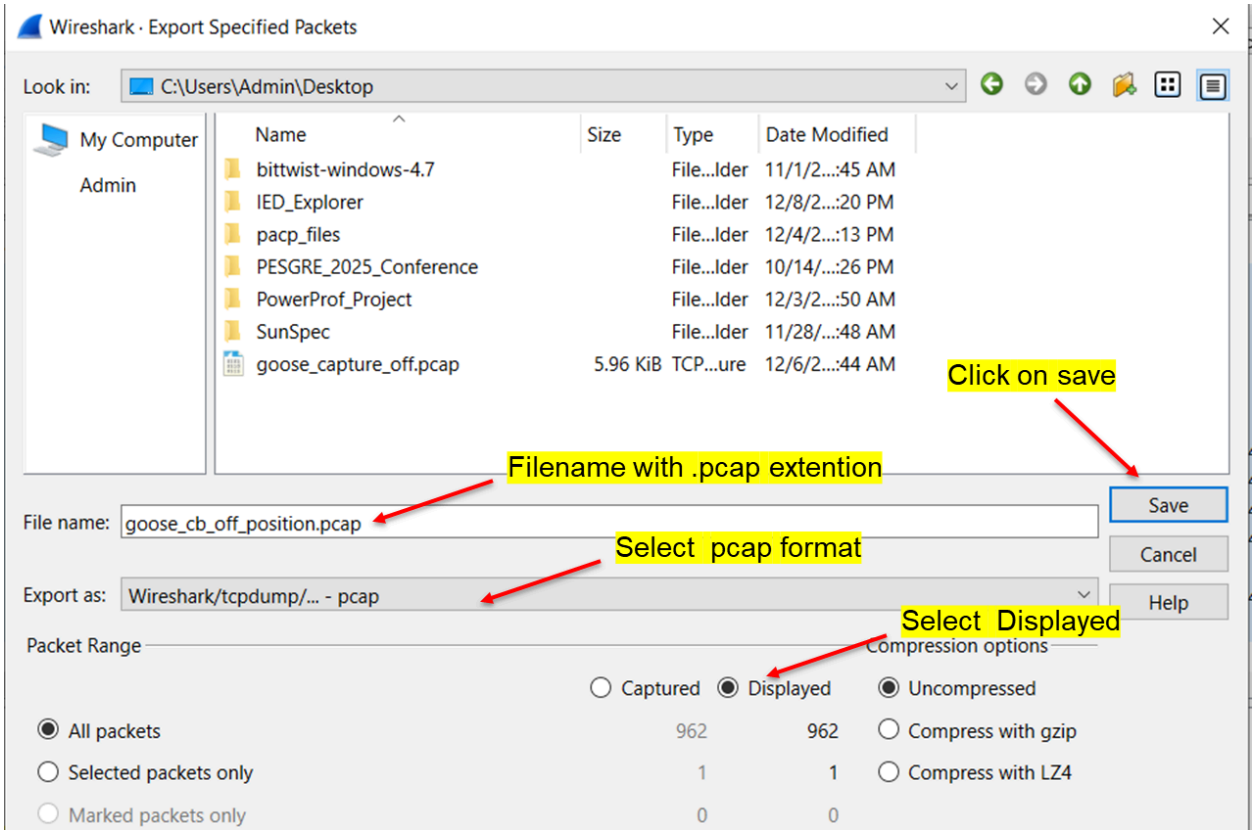
9. You would be able to observe the packet capture. To filter out only GOOSE packets from others, enter "**goose**" in the filter box



10. After a minute, STOP capture by pressing the red button in Wireshark.



11. Now go to the **File** option, select the "**Export Specified Packets**" option, and save the file in .pcap format.



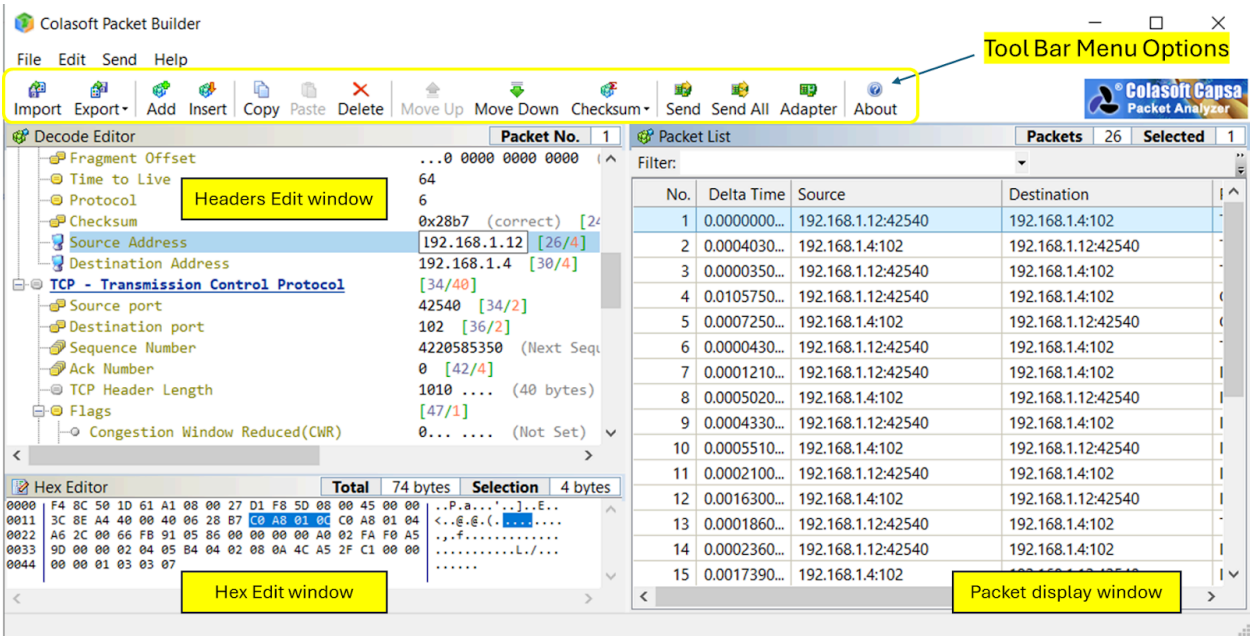
Note: bittwist only supports the .pcap files. Therefore, when saving packet captures using Wireshark, select the .pcap format. By default, the latest Wireshark saves captures in .pcapng format, which is not compatible with Bit-Twist.

2. Edit the GOOSE packet (Control Manipulation)

To edit the packet fields, Colasoft PacketBuilder is used.

This tool can be used for packet editing and packet replay purposes. It is a GUI-based tool that allows editing of both raw packet header fields and payload. This tool relies on the npcap tool https://npcap.com/#download. Therefore, we need to install Npcap first in case it is not already installed by Wireshark.

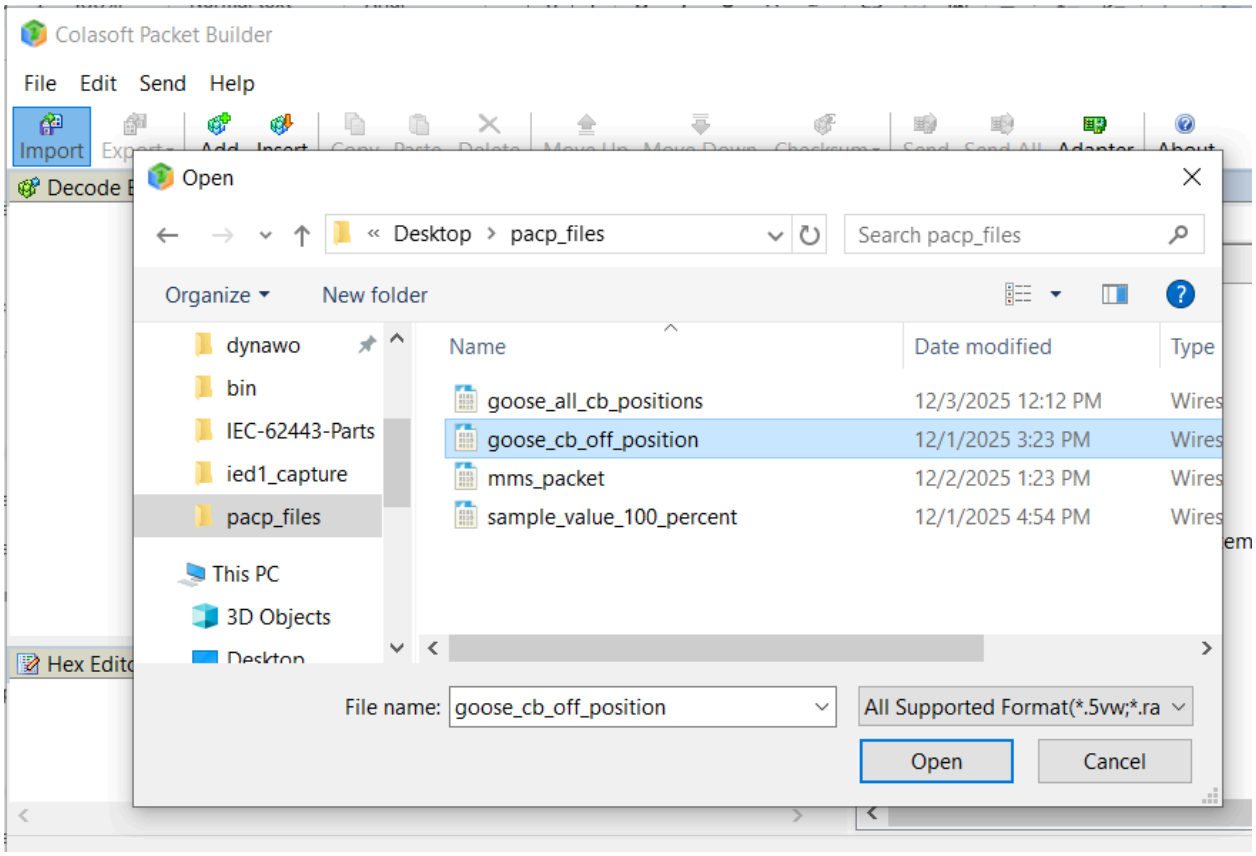
Editing packet headers: directly on the blocks
Editing packet payload/message: using the Hex editor



Procedure:

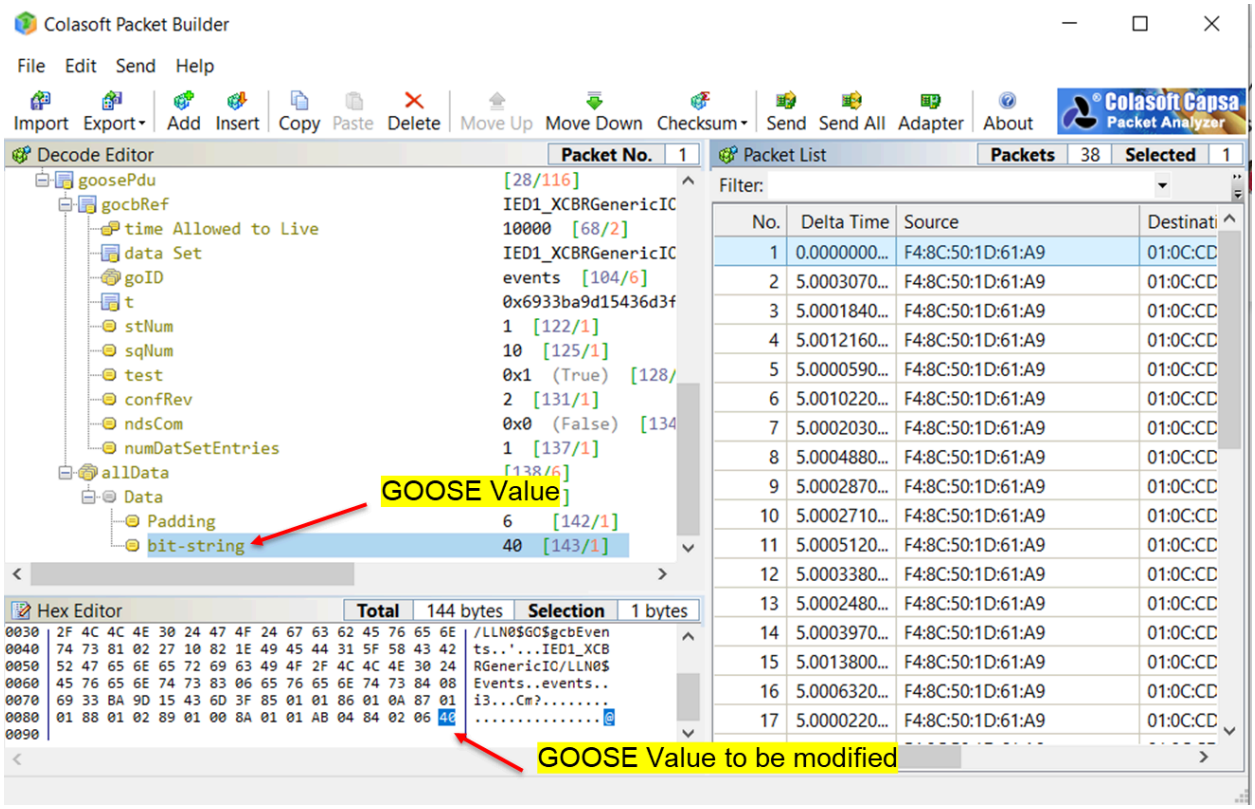
2.1 Import packet

1. **“Import”** the .pcap file for the corresponding GOOSE traffic (saved in the previous setp) into the ColaSoft Packet Builder.



2.2 Edit Packet

2. Since the modifications are being done at the payload level, we need to use the "**Hex Editor**" window to modify the GOOSE control value

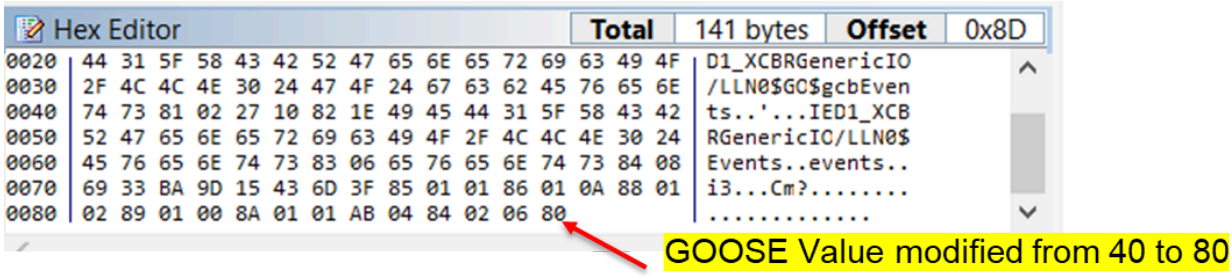


The value interpretation of the CB position value (represented in Hex code) is as follows:

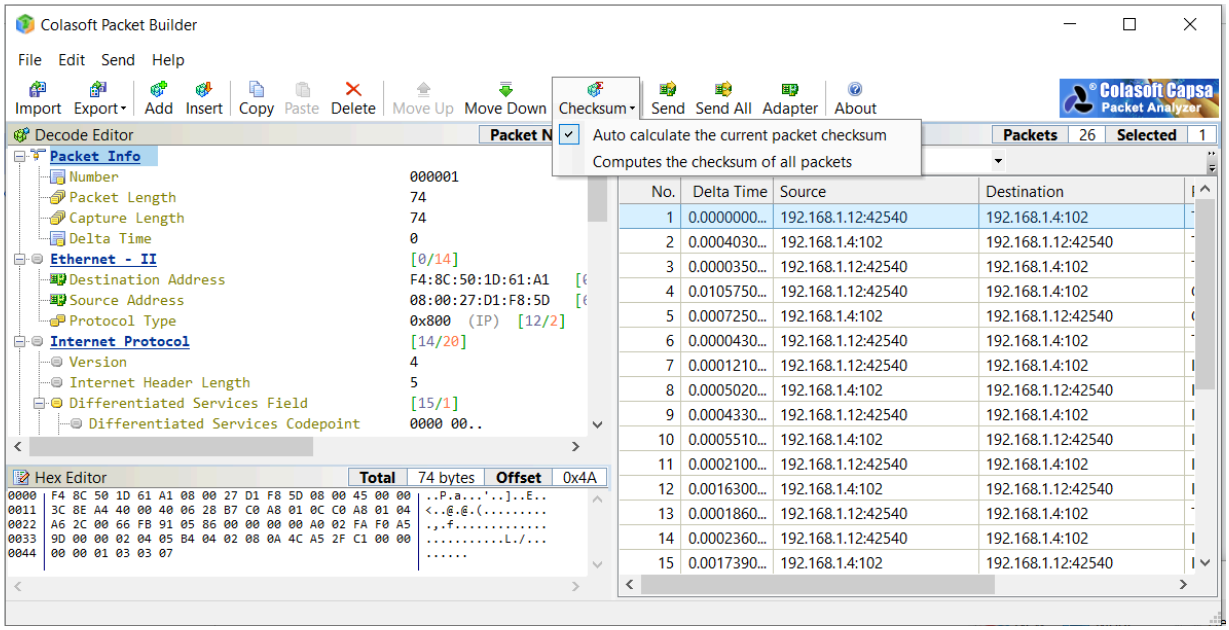
1. 80 → ON position (10 >> 1000 0000)
2. 40 → OFF position (01 >> 0100 0000)
3. 00 → Intermediate State (00 >> 0000 0000)
4. C0 → Bad State (11 >> 1100 0000)

Manipulate the Hex code value as per the requirement in this example case, the value has been changed to 80 → “ON”

Since the editing is at the payload level, you need to carry out the manipulation on every packet. Therefore it is recommended to perform packet manipulation for 1 packet and export only that single packet.

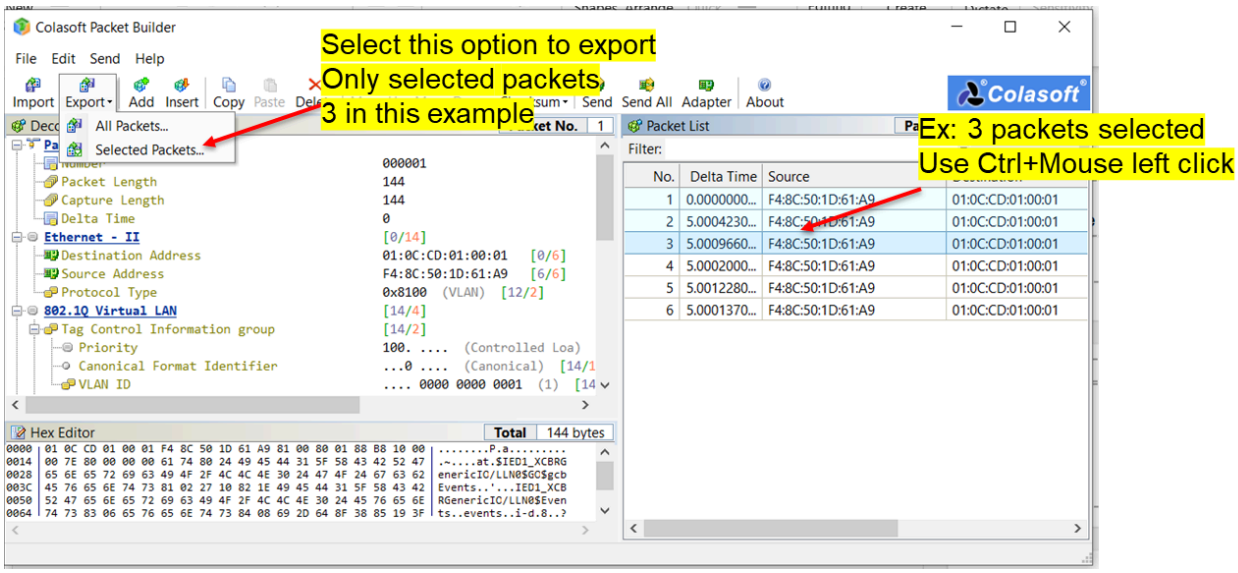


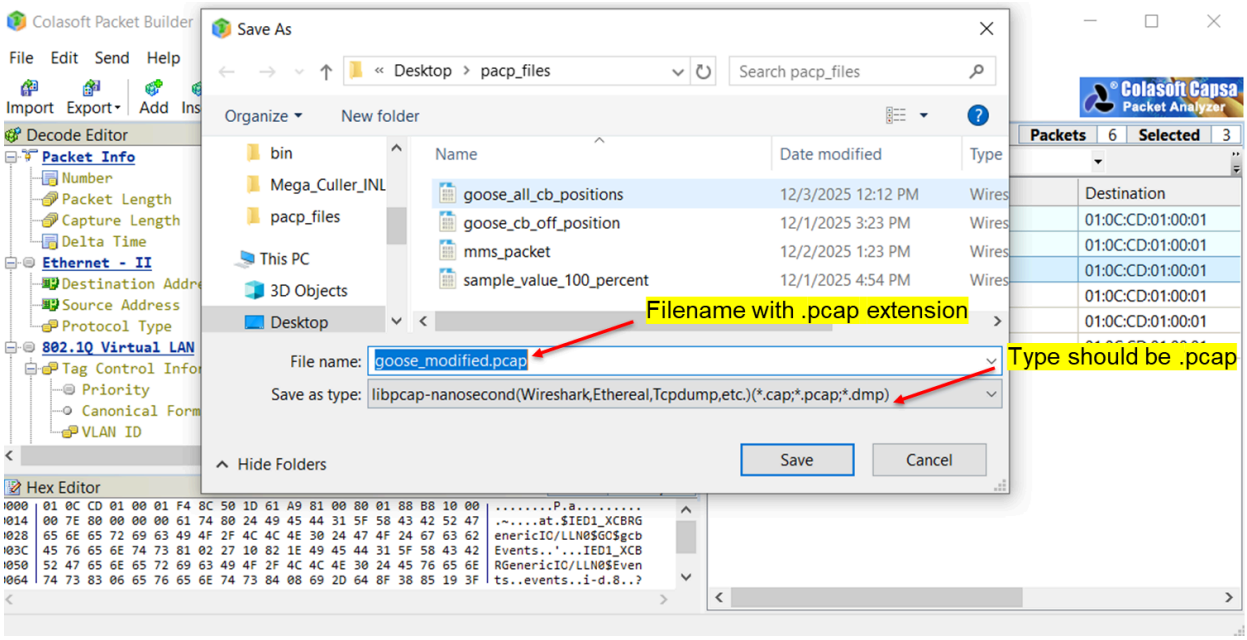
4. After editing is completed, use the **“CheckSum”** menu option on the toolbar, click, and then select **“Computes the checksum for all packets.”**



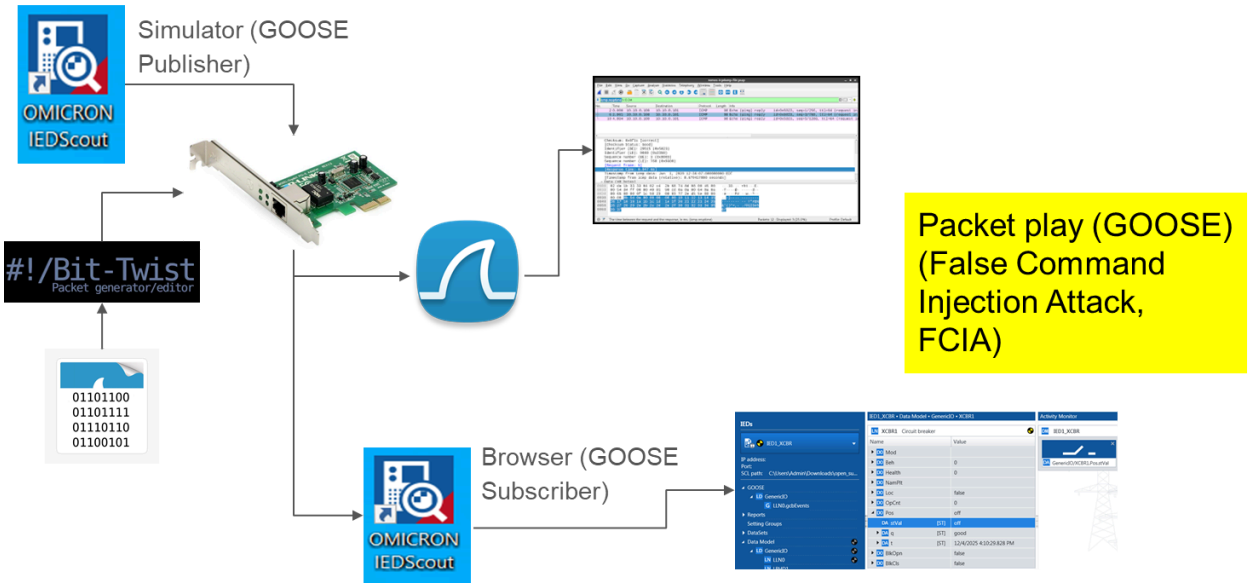
2.3 Export Packet

5. Use the **Export** menu option in the toolbar to save the modified packet and save it in **.pcap** format. Here it is also possible to select specific packets and export them.



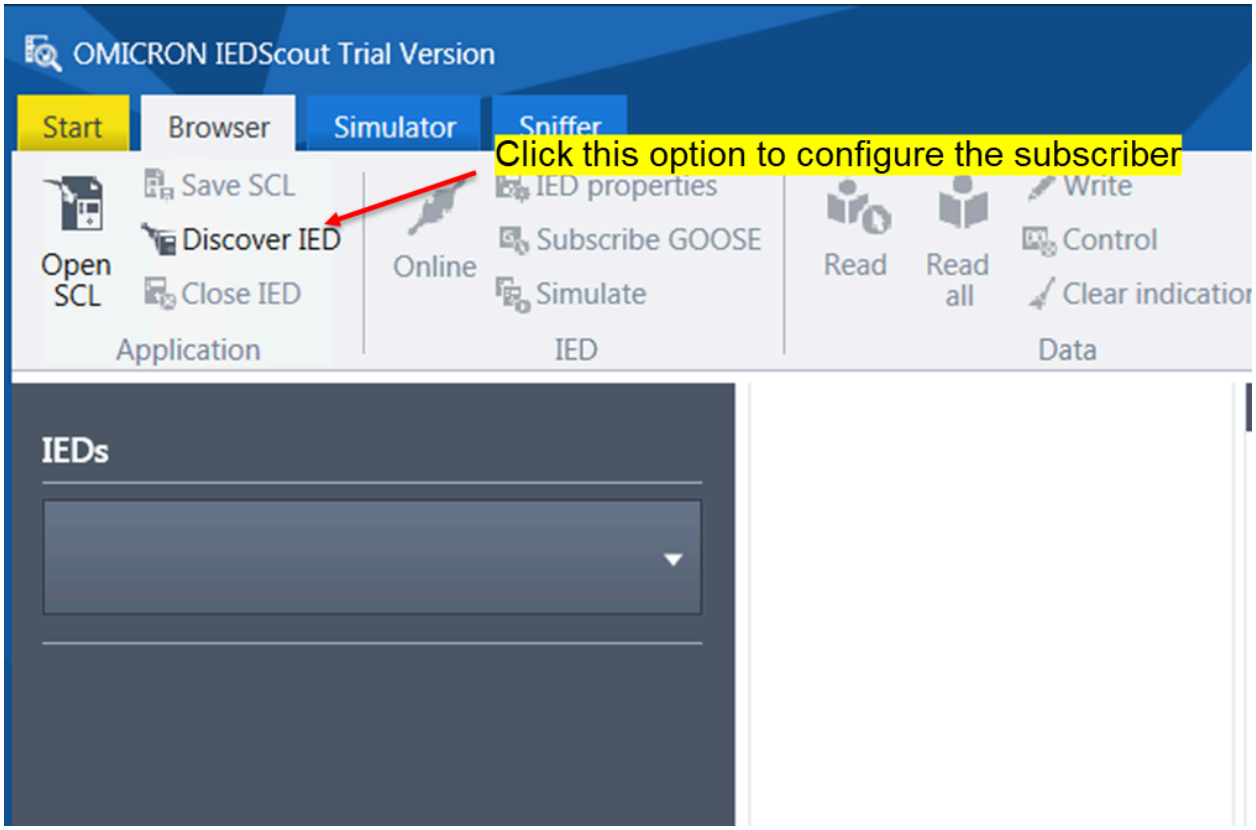


3. Playback the Modified Traffic

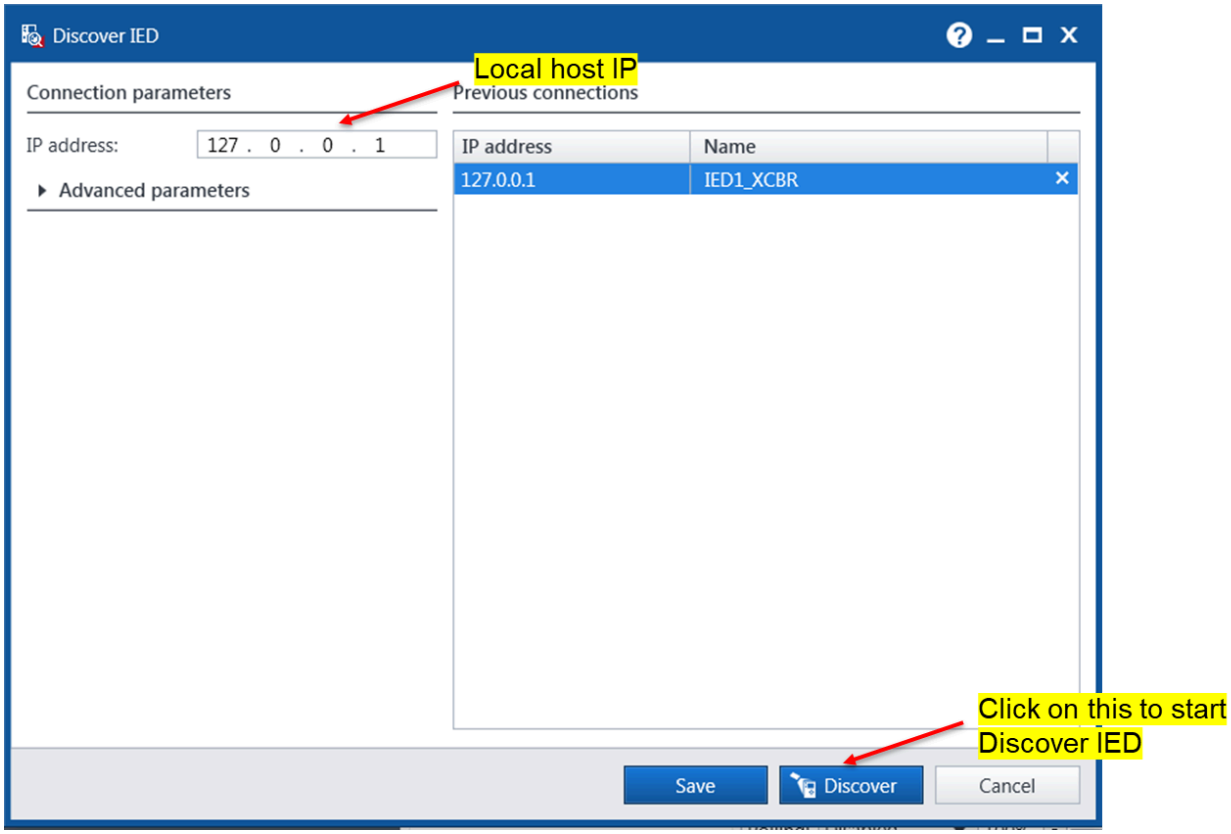


3.1 Start IEDScout GOOSE Subscriber

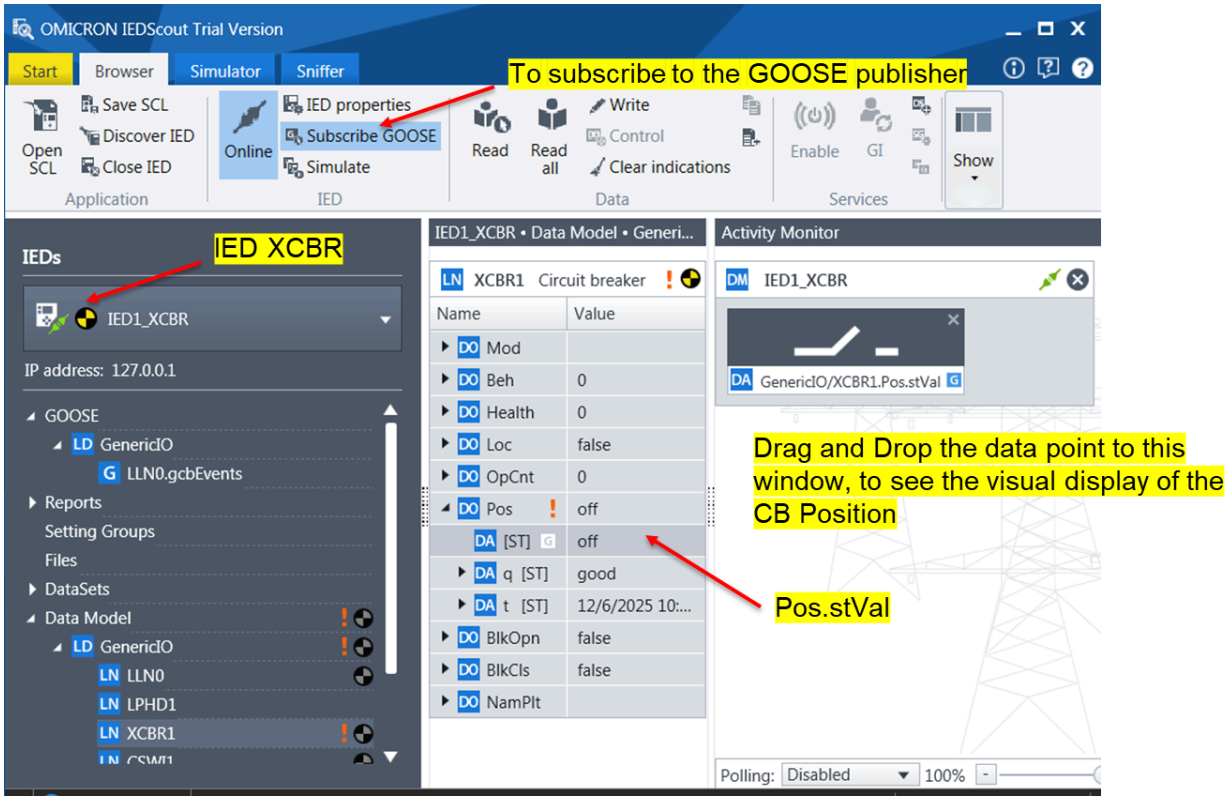
1. Open the IEDScout “Browser” Tab and click on the “Discover IED” option



2. In the configuration pop-up enter the local host IP address **127.0.0.1**, since we are running IED simulator on the same local host, then click on "**Discover**" button



3. If the IED has been successfully detected, it will be shown in the IEDs window. Now click on "**Subscribe GOOSE**" to enable the GOOSE control subscription.



4. Explore the Tree structure to locate the GOOSE control point. Drag and drop the "Pos.stVal" point (from the middle window) onto the **"Activity Monitor"** window (right window) to visually track the changes in the Circuit Breaker (CB) position in response to the published GOOSE control message.

3.2 Play Manipulated Packet with Bit-twist

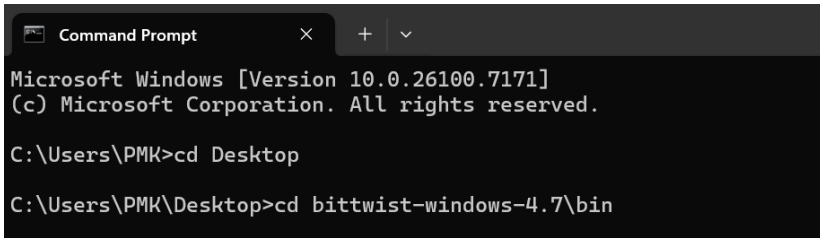
5. Now, we will use command prompt to playback the malicious GOOSE packets using the bit-twist tool. We will playback the modified GOOSE traffic in a continuous loop on the same NIF interface.

   Windows + R

   cmd # To open the command prompt

   cd Desktop # Actually, change to the location where the downloaded BitTwist folder is stored. In this case, it is on the Desktop.

   cd bittwist-windows-4.7\bin # to change to the bin folder, where the executable is available.

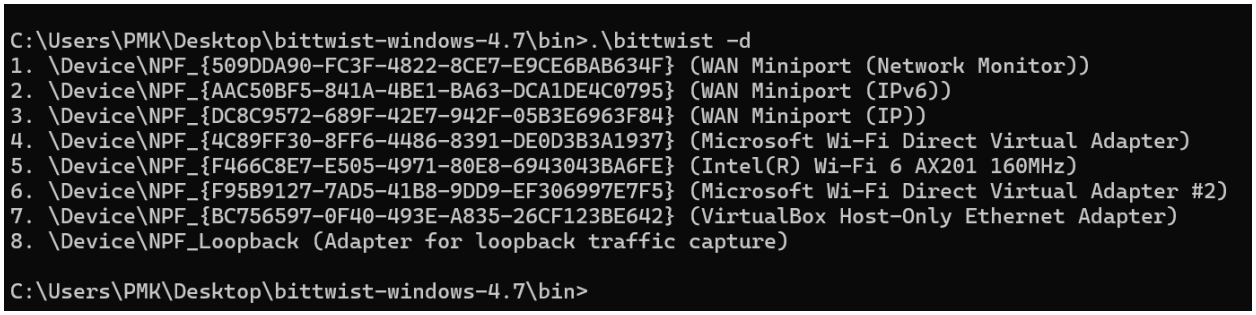


The Bit-Twist bin folder contains 2 executables available.

- bittwist - for packet play
- bittwiste - for packet editing (we don't need this for this tutorial, since we used Colasoft for packet editing)

6. Run the below command to see the list of network interfaces available

   .\bittwist -d # to list the available network interfaces



7. Run the below command to play back the traffic in loop and the syntax is as given below

.\bittwist -i <interface_number> <pcap-file full path> # command syntax for packet play.

.\bittwist -i 5 -l 0 -p 1 C:\Users\Admin\Desktop\goose_modified.pcap

Note: the interface number should be selected based on the list of interfaces detected in the previous step and is device specific, it could be different from one device to another. Further, provide the full path of the .pcap file, based on where you have saved the manipulated goose pcap file "goose_modified.pcap) on your device.

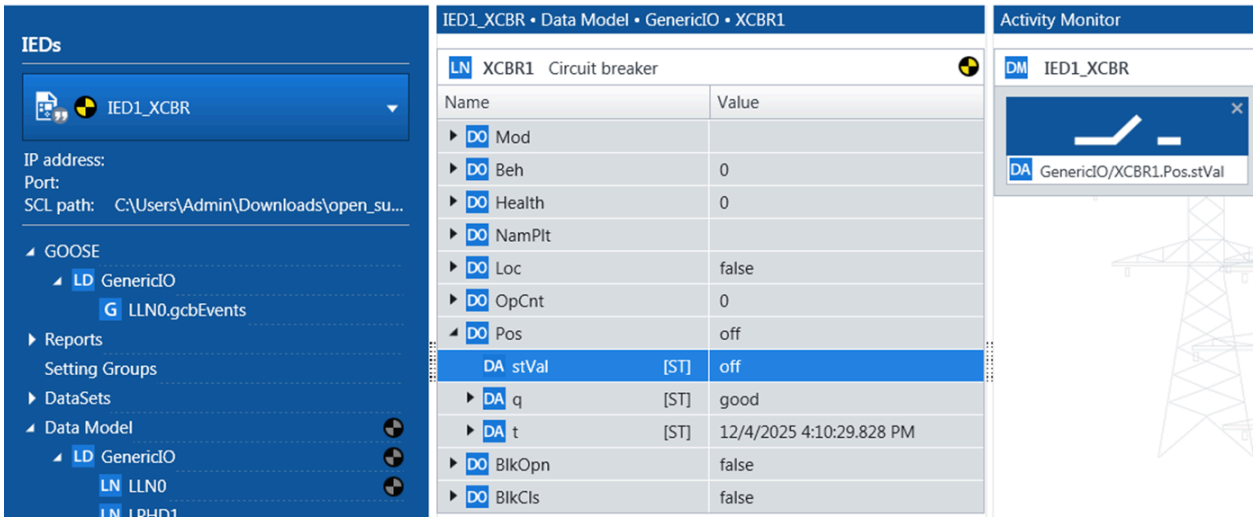
-i 5 (Interface Intel (R) Wi-Fi 6 AX201 160MHz)
-l 0 (-l → loop, 0 → infinite/continuous)
-p 1 (-p → packets per second pps, 1 → 1 packet/second)

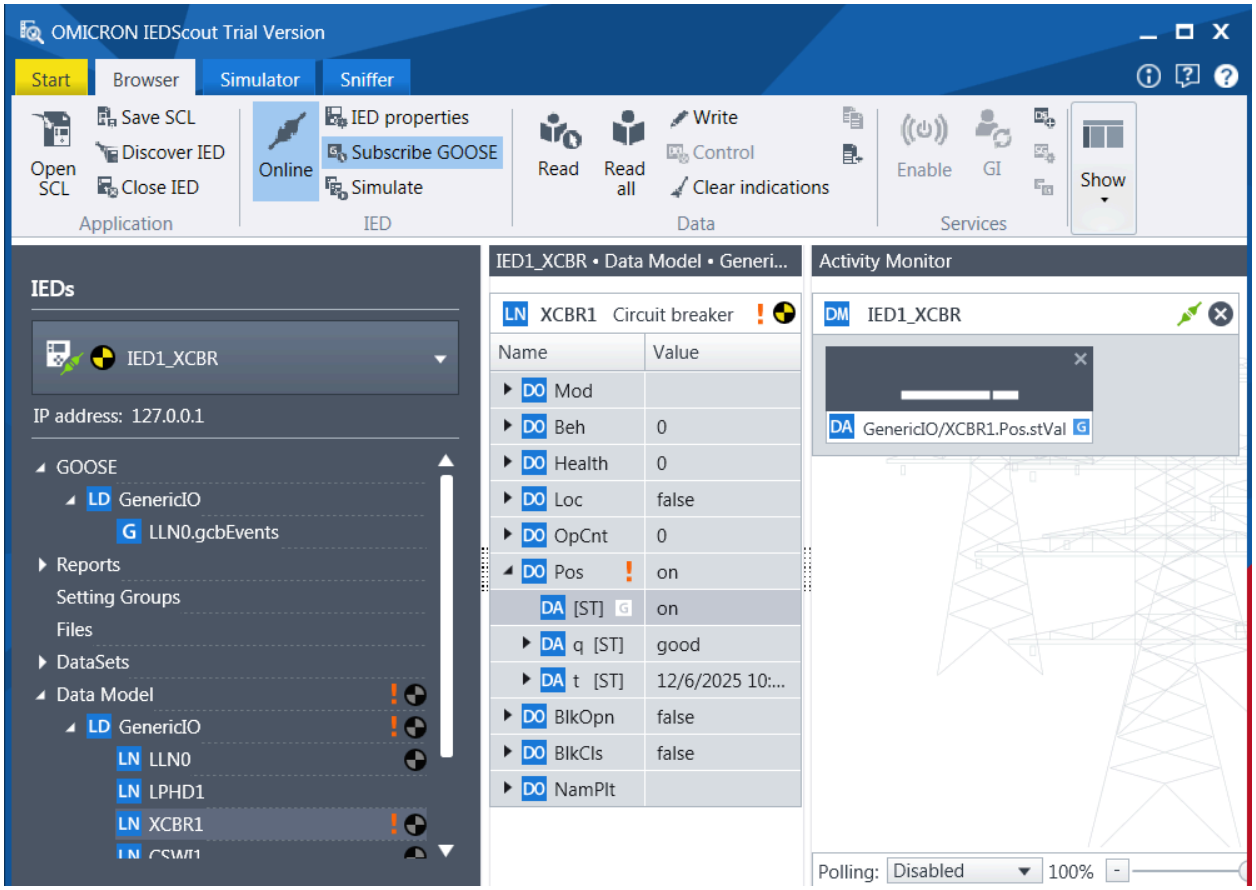
```
C:\Users\PMK\Desktop\bittwist-windows-4.7\bin>.\bittwist -i 5 C:\Users\PMK\Desktop\goose_modified.pcap
sending packets through \Device\NPF_{F466C8E7-E505-4971-80E8-6943043BA6FE}

sent = 1 packets, 1152 bits, 144 bytes
throughput = 0 pps, inf Mbps, inf Gbps
elapsed time = 0.000000 seconds
```

3.3 Visualization in IED Scout Activity Monitor

6. Subsequently, observe that the CB position is toggling between **"ON"** and **"OFF."** This behavior occurs because the actual IED is publishing a GOOSE message indicating the CB status as "OFF," while the manipulated GOOSE control value, injected via bit-twisting, is simultaneously publishing the CB status as "ON." Consequently, the CB position alternates between "ON" and "OFF," reacting to the two conflicting GOOSE messages, with the latest received GOOSE control value determining the momentary status.




OMICRON IEDScout Trial Version
Start
Browser
Simulator
Sniffer
Open SCL
Save SCL
Discover IED
Close IED
Application
Online
IED properties
Subscribe GOOSE
Simulate
IED
Read
Read all
Write
Control
Clear indications
Data
Enable
GI
Show
Services
IEDs
IED1_XCBR
IP address: 127.0.0.1
GOOSE
GenericIO
LLN0.gcbEvents
Reports
Setting Groups
Files
DataSets
Data Model
GenericIO
LLN0
LPHD1
XCBR1
IED1_XCBR • Data Model • Generi...
XCBR1 Circuit breaker
Name
Value
Mod
Beh 0
Health 0
Loc false
OpCnt 0
Pos on
[ST] on
q [ST] good
t [ST] 12/6/2025 10:...
BlkOpn false
BlkCls false
NamPlt
Activity Monitor
IED1_XCBR
GenericIO/XCBR1.Pos.stVal
Polling: Disabled
100%