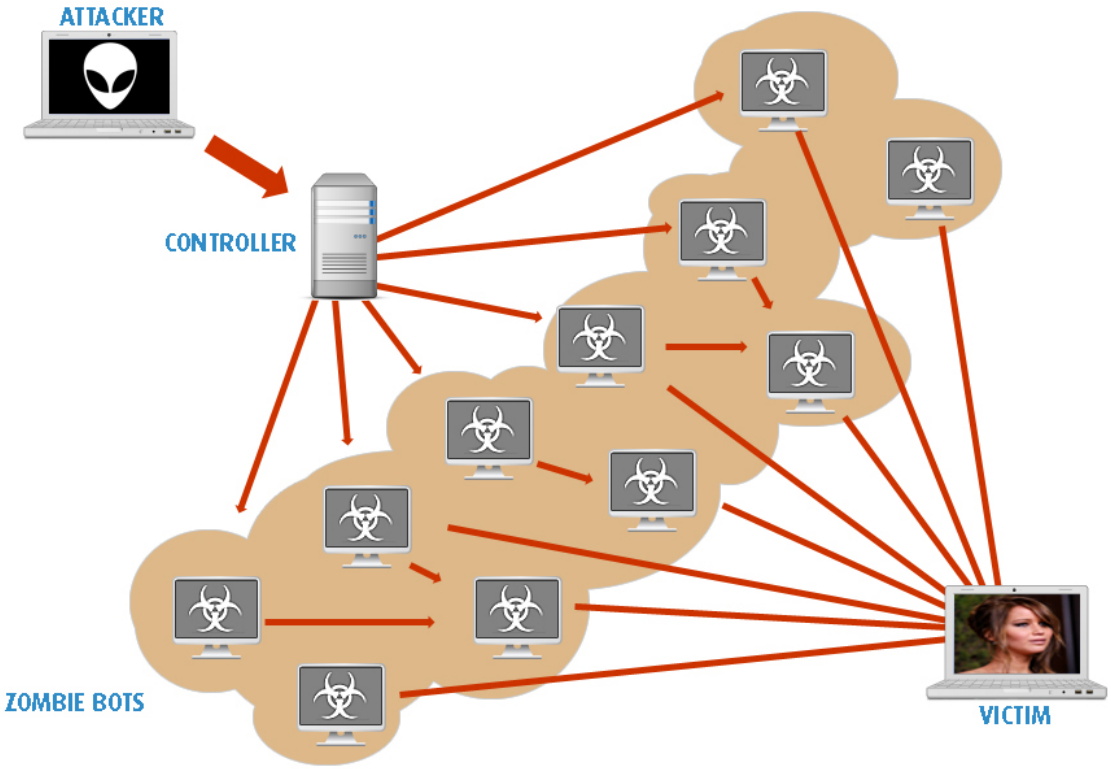
DDoS Testing with ValkyrieManager

Step by Step Guide

Distributed **D**enial **o**f **S**ervice (DDoS)

Multiple compromised systems – usually infected with a Trojan – are used to target a single system causing a Denial of Service (DoS) attack.



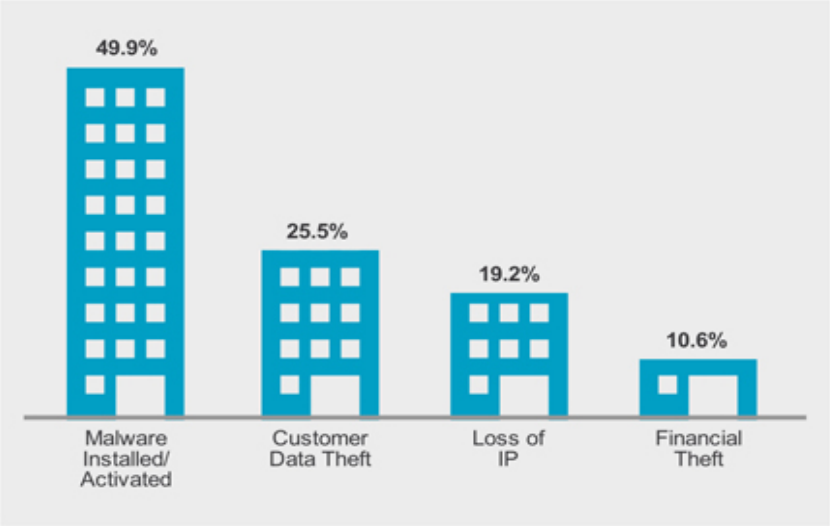
DDoS – THE RISKS

DDoS Threat Landscape

FROST & SULLIVAN ARBOR NETWORKS

Rise in Use of DDoS as Diversionary Tactic

Business Affected (%)



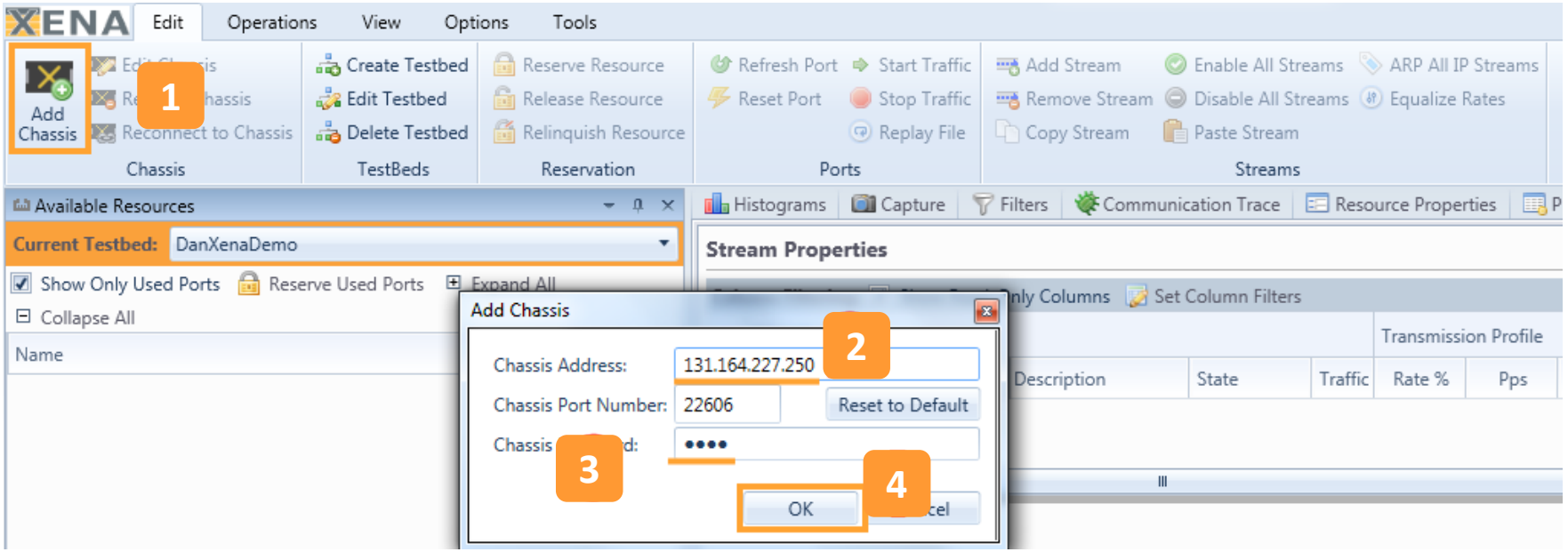
55% of DDoS victims targeted for data theft activities

6,000 DDoS attacks per day

SOURCE: Frost & Sullivan's Analysis of the Global Denial of Service (DDoS) Mitigation Market, July 2014 (NDD2-74)

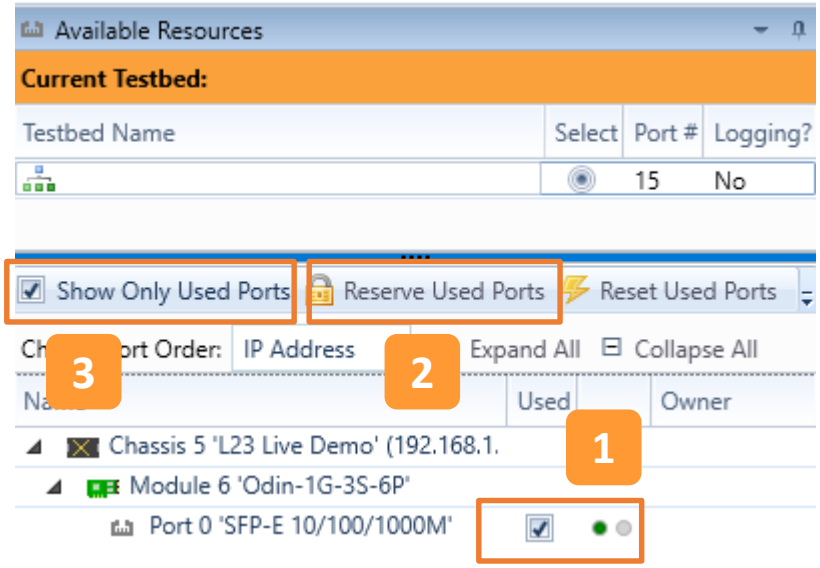
DDoS – CHASSIS CONNECTION

1. Click “Add Chassis”
2. Insert Xena Management Port IP address
3. Insert password (Default = “xena”)
4. Click “OK”



DDoS – PORT RESERVATION

1. Choose port to be used for the attack.
2. Click “Reserve Used Ports” to reserve the selected “Used” port.
3. Eliminate the view of other ports by checking “Show Only Used Ports”



DDoS Category

The following DDoS attacks will be covered in this guide:

- **SYN Flood**
- **UDP Flood**
- **Teardrop Attack**
- **Smurf Attack**
- **Ping of Death**
- **Ping Flood**
- **ARP Spoofing**
- **TCP Attack**

DDoS – SYN FLOOD

SYN Flood

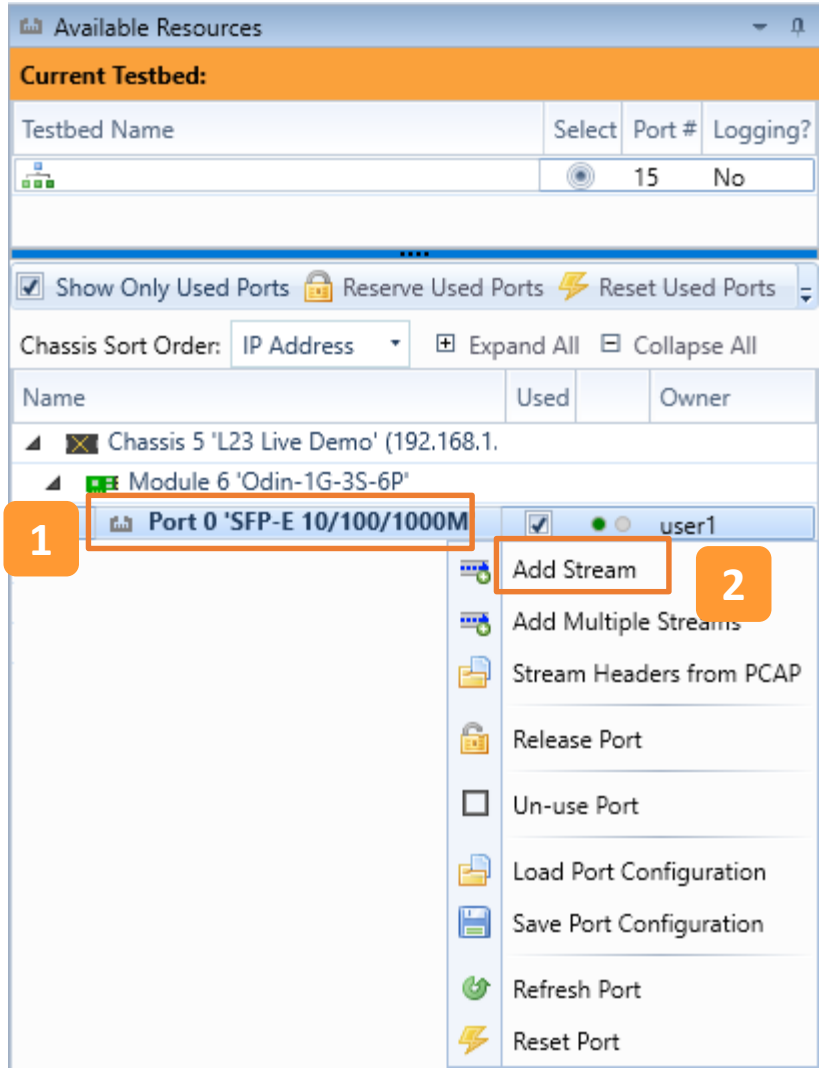
A classic DDoS attack that sends rapid amounts of packets to a machine in an attempt to keep connections from being closed.

The sending machine does not close the connection, and eventually that connection times out.

If the attack is strong enough it will consume all resources on the server and send the website offline.

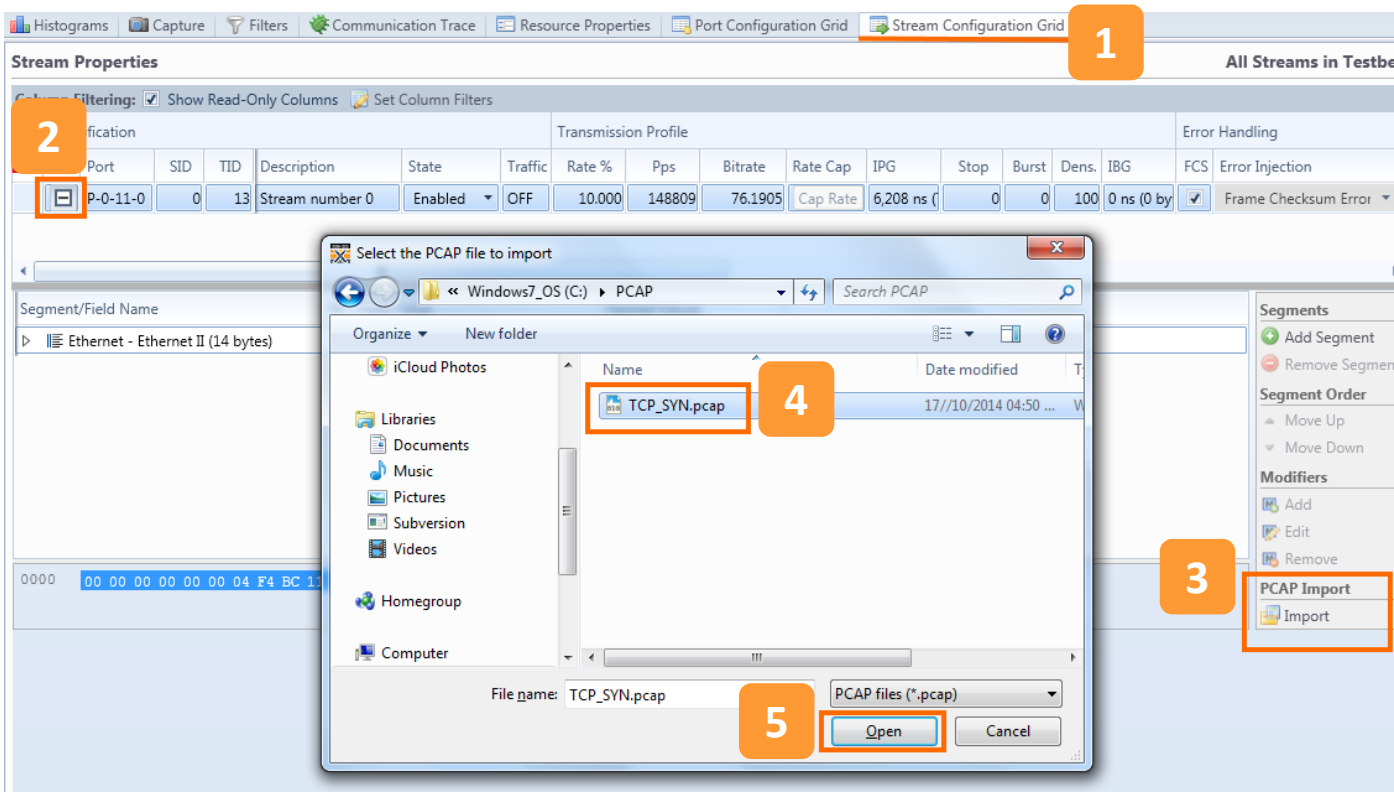
DDoS – SYN FLOOD

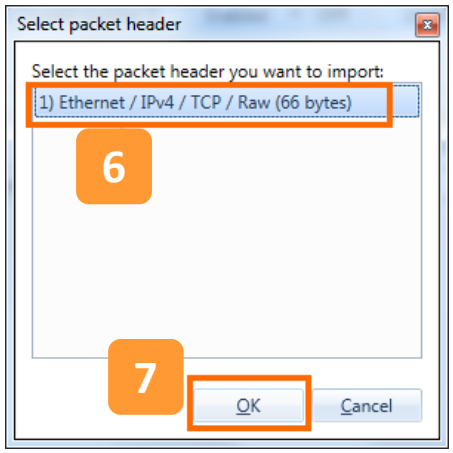
1. Right-click on Attacking port.
2. Click “Add Stream”



DDoS – SYN FLOOD

1. Go to “Stream Configuration Grid” tab.
2. Click “+”.
3. Click “Import”
4. Select TCP_SYN.pcap
5. Click “Open”
6. Click First row
7. Click “OK”

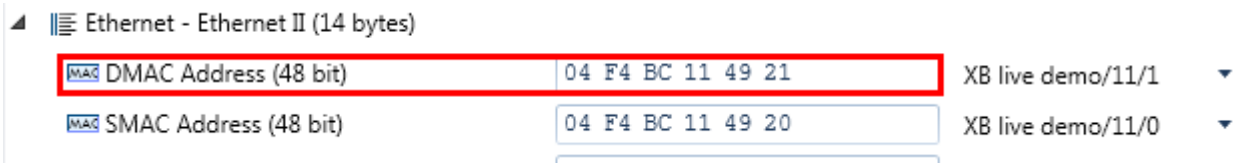


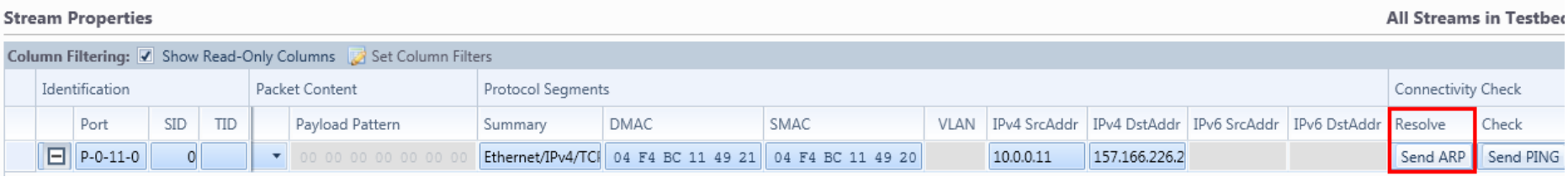


DDoS – SYN FLOOD

1 Configure D.MAC by either

1. Manually writing the Address
2. Click the ARP button to ARP the GW configured for the port.

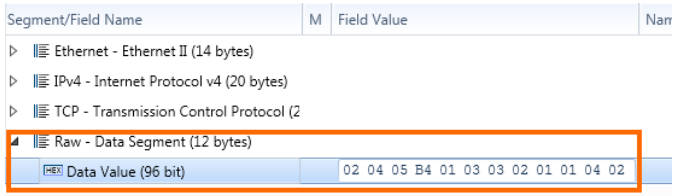


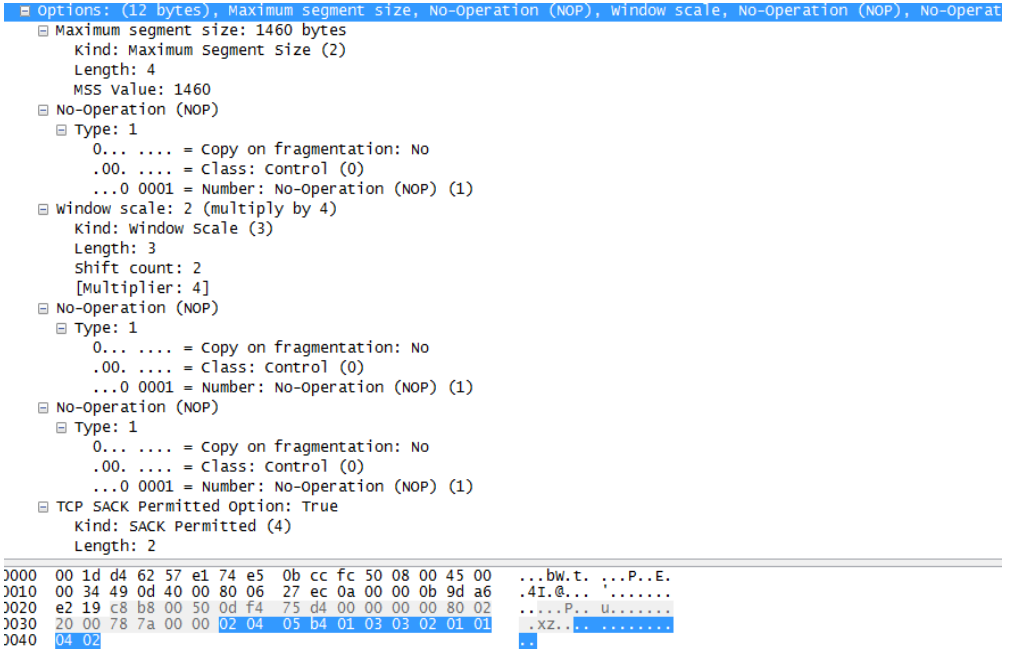


DDoS – SYN FLOOD

1. 12B Raw header = TCP options and may be removed to generate smaller SYN Packets. (Note that some devices might see that as an illegal TCP Packet)

2. TID(20B) may be removed for the same reason and since Packet Loss/Latency/Jitter… are not important in this test case scenario.



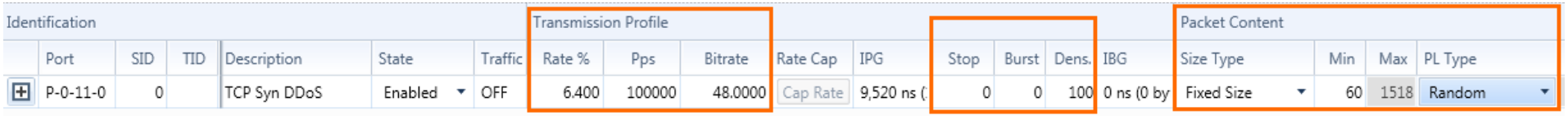


DDoS – SYN FLOOD

1. Select Rate – Pps recommended.
   Rate can be configured as Bursty as well.
   Select Burst size and density – the Transmission Rate will become the Average rate)

2. Select Packet Size Type.
   Packet size range 60 B -16,383 B.

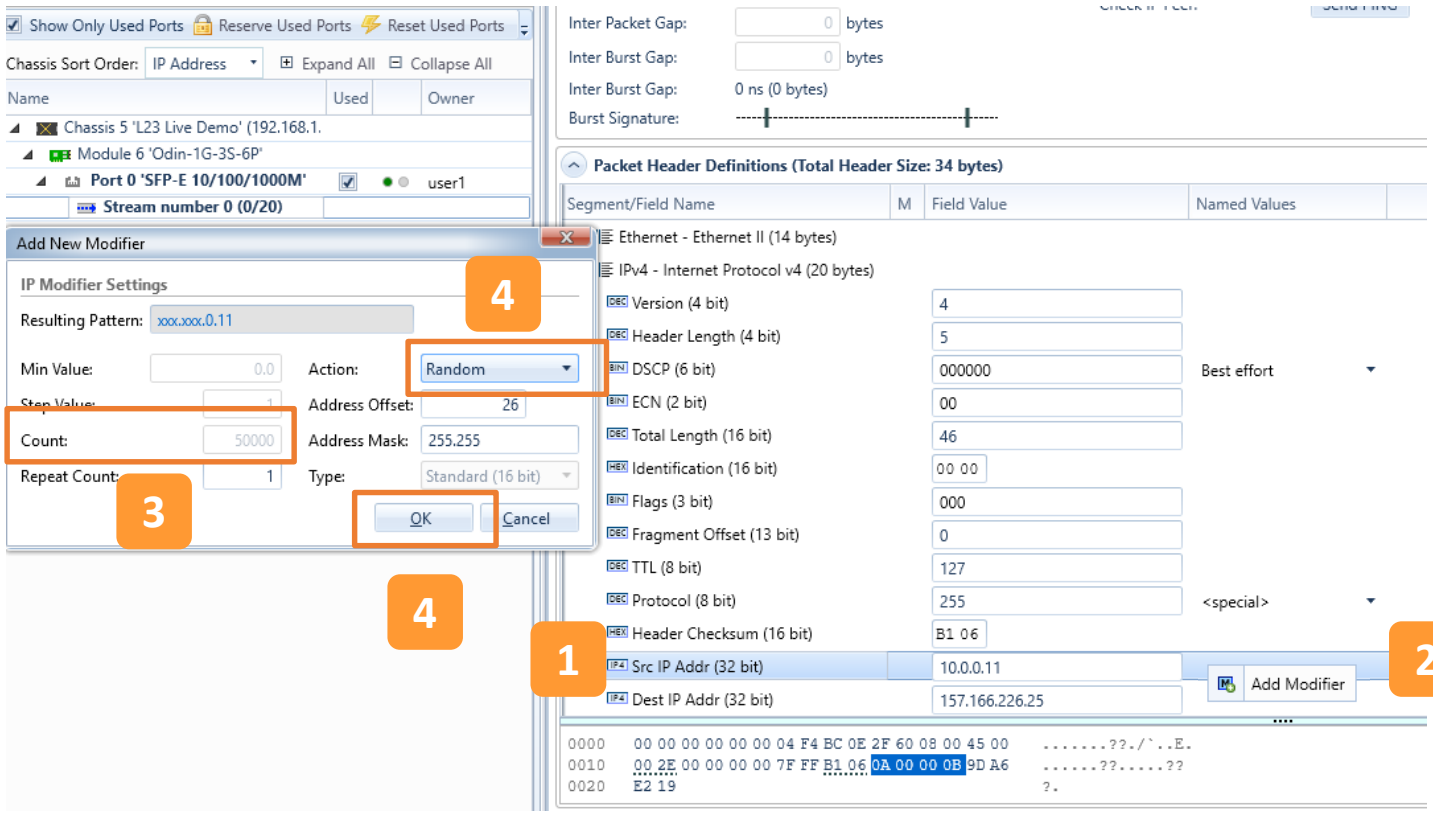
3. Select the Payload Type.
   Random recommended.



Identification						Transmission Profile								Packet Content			
	Port	SID	TID	Description	State	Traffic	Rate %	Pps	Bitrate	Rate Cap	IPG	Stop	Burst	Dens.	IBG	Size Type	Min	Max	PL Type
⊞	P-0-11-0	0		TCP Syn DDoS	Enabled	OFF	6.400	100000	48.0000	Cap Rate	9,520 ns (	0	0	100	0 ns (0 by	Fixed Size	60	1518	Random

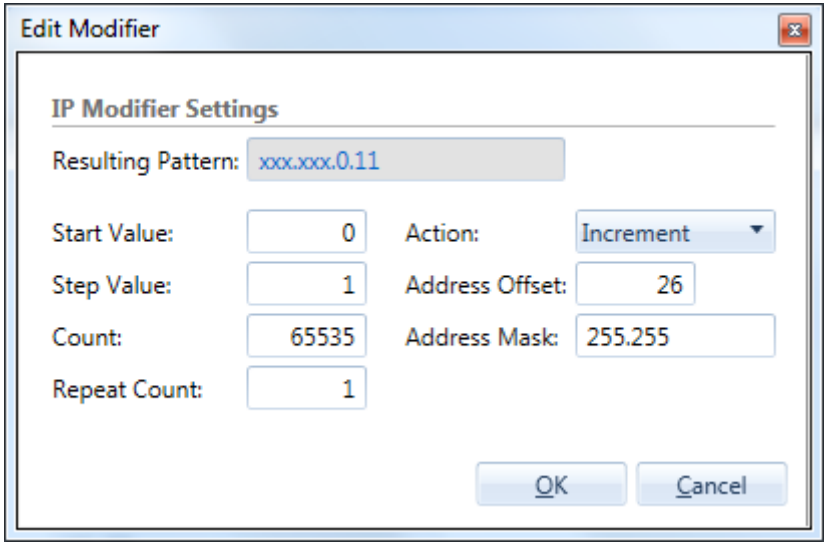
DDoS – SYN FLOOD

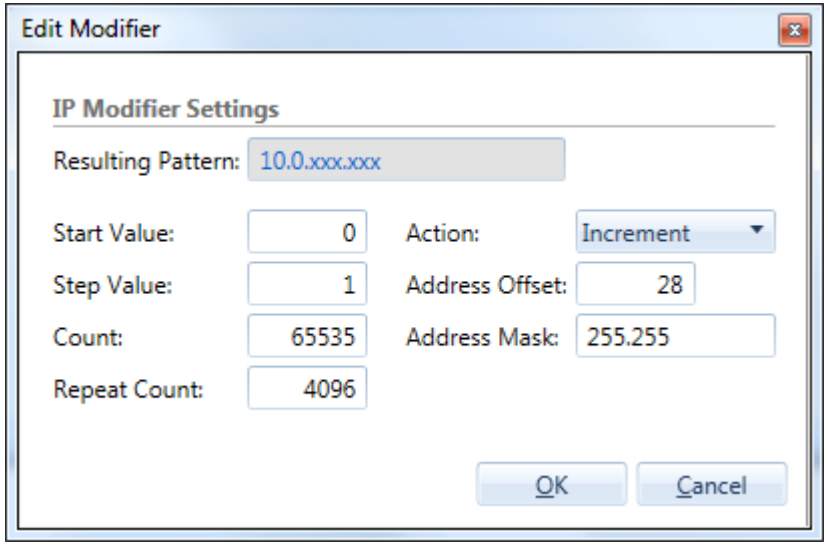
1. Right click on “Src IP Addr”
2. Click “Add Modifier”
3. Select #of Src Ip`s
4. Select Address Action (Random Recommended)
5. Click “OK”.



DDoS – SYN FLOOD

1 To achieve 65K*4096 (~268.3M) addresses, add additional Modifier configured as follows:





DDoS – UDP FLOOD

UDP Flood

A DoS attack using the User Datagram Protocol (UDP), a sessionless/connectionless computer networking protocol.

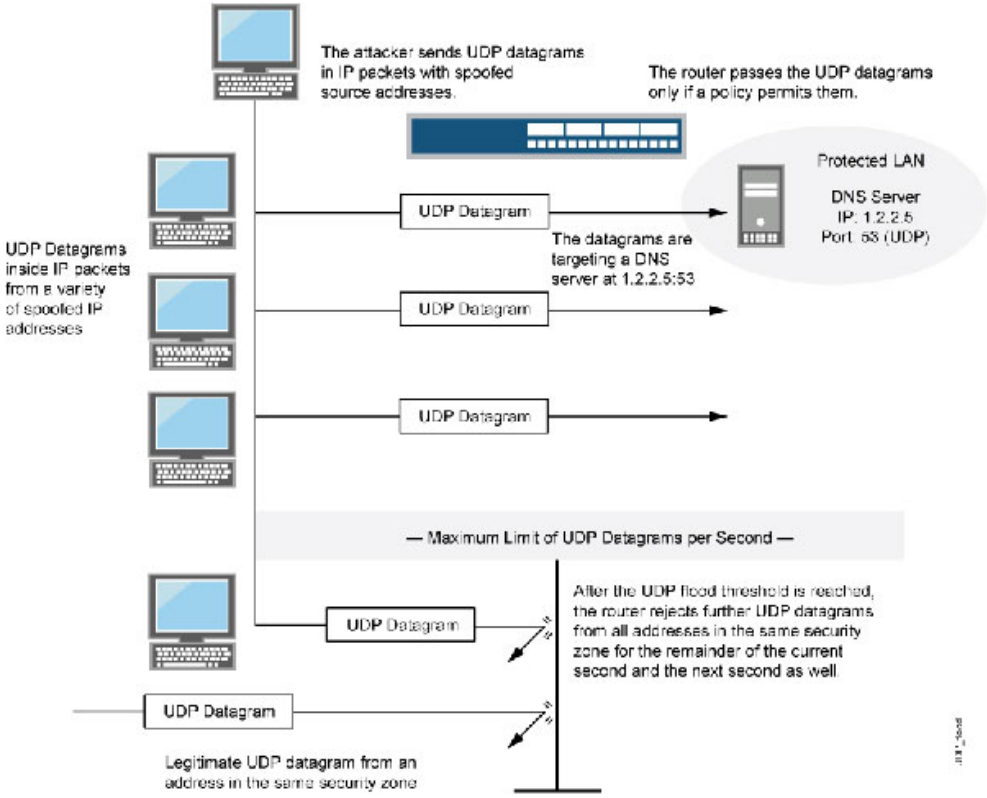
A UDP flood attack can be initiated by sending a large number of UDP packets to random ports on a remote host.

The victimized system will be forced into sending many ICMP packets, eventually leading it to be unreachable by other clients.

DDoS – UDP FLOOD

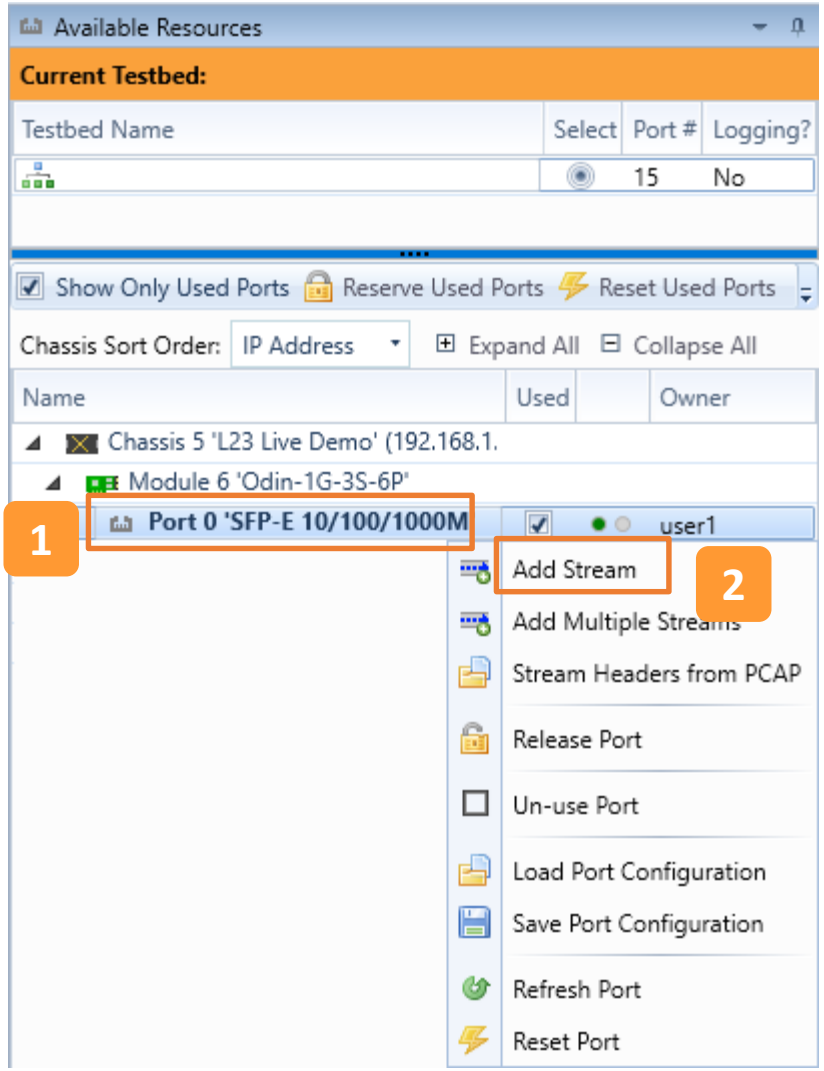
UDP Flood (Attached IPv6 DNS Query)

A User Datagram Protocol Flood works by flooding ports on a target machine with packets that make the machine listen for applications on those ports and send back an ICMP packet.



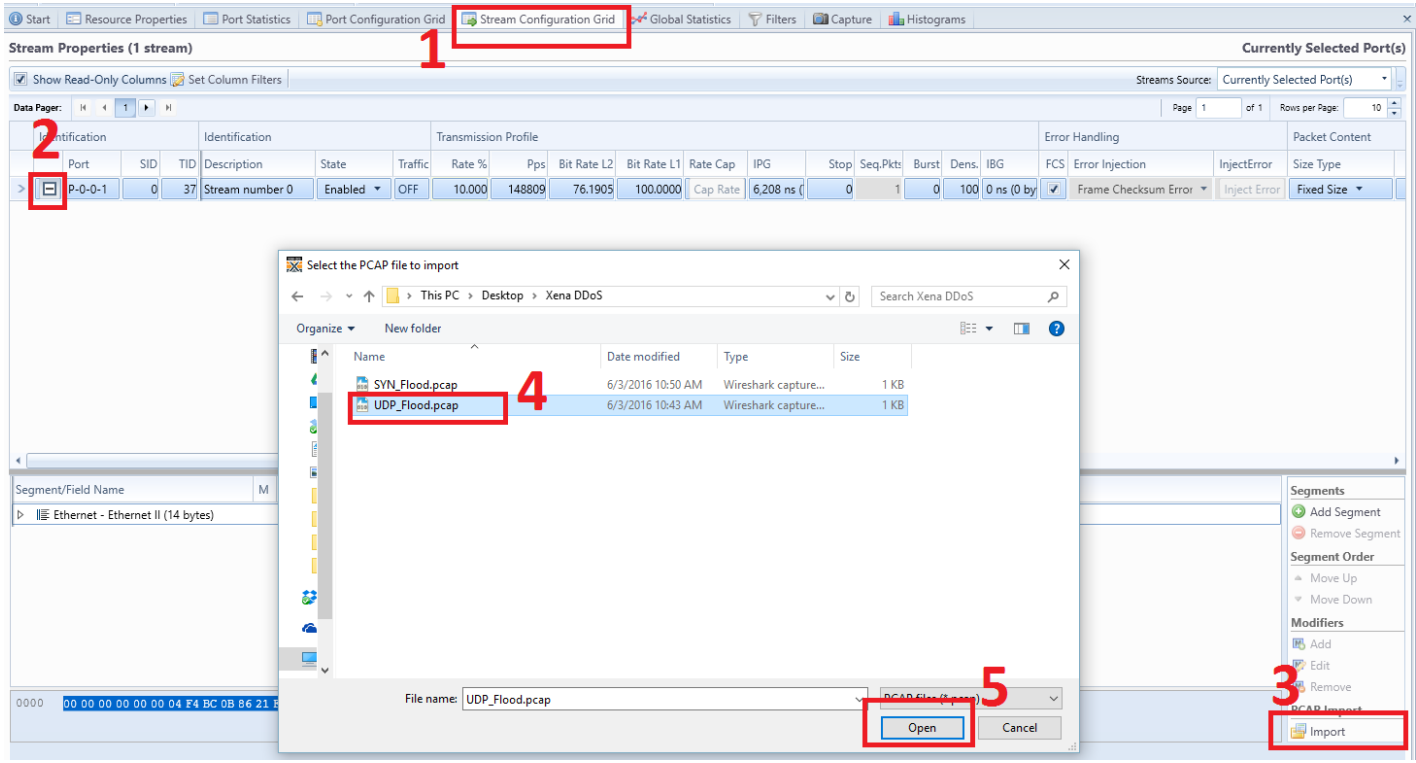
DDoS – UDP FLOOD

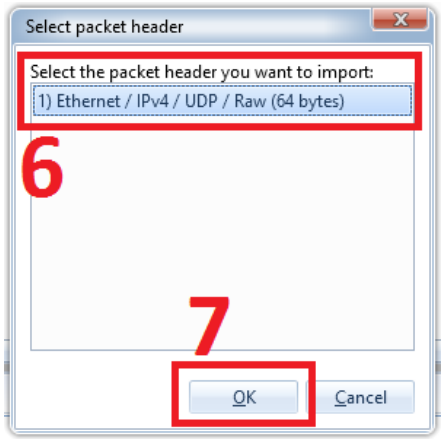
1. Right-click on Attacking port.
2. Click “Add Stream”



DDoS – UDP FLOOD

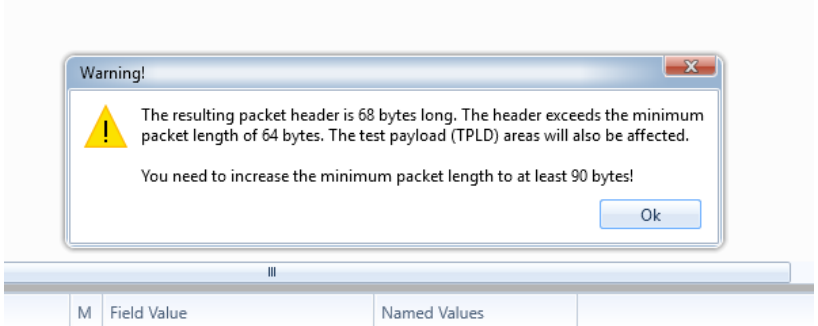
1. Go to “Stream Configuration Grid” tab.
2. Click “+”.
3. Click “Import”
4. Select UDP_Flood.Pcap
5. Click “Open”
6. Click First row
7. Click “OK”

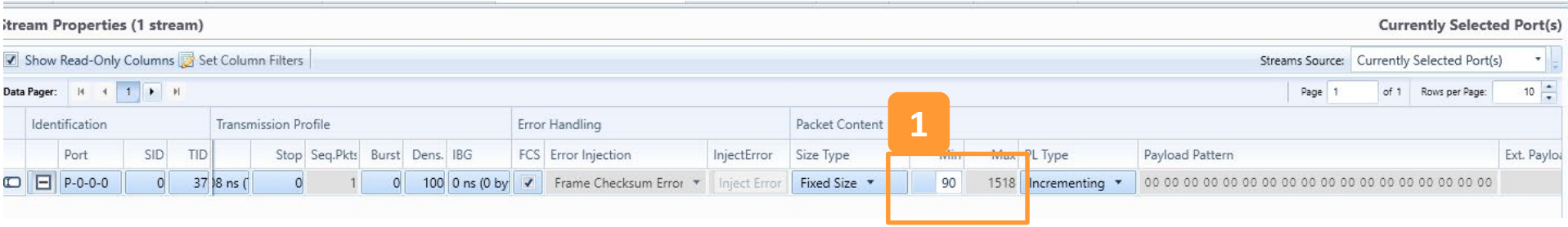




DDoS – UDP FLOOD

1 You may see the alert telling you to increase the minimum packet length. Change the minimum size to 90 bytes.

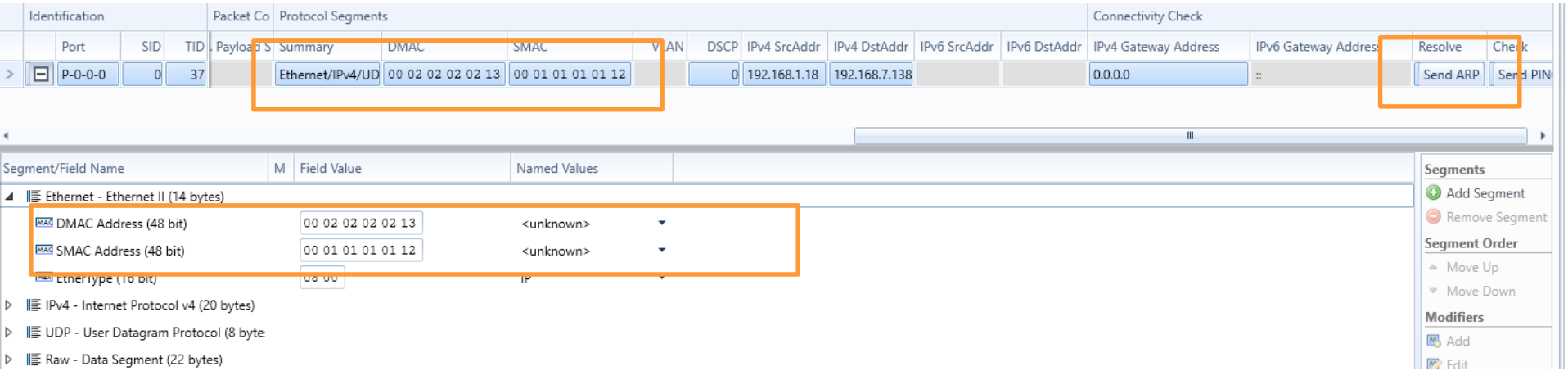




DDoS – UDP FLOOD

1 Configure D.MAC by either

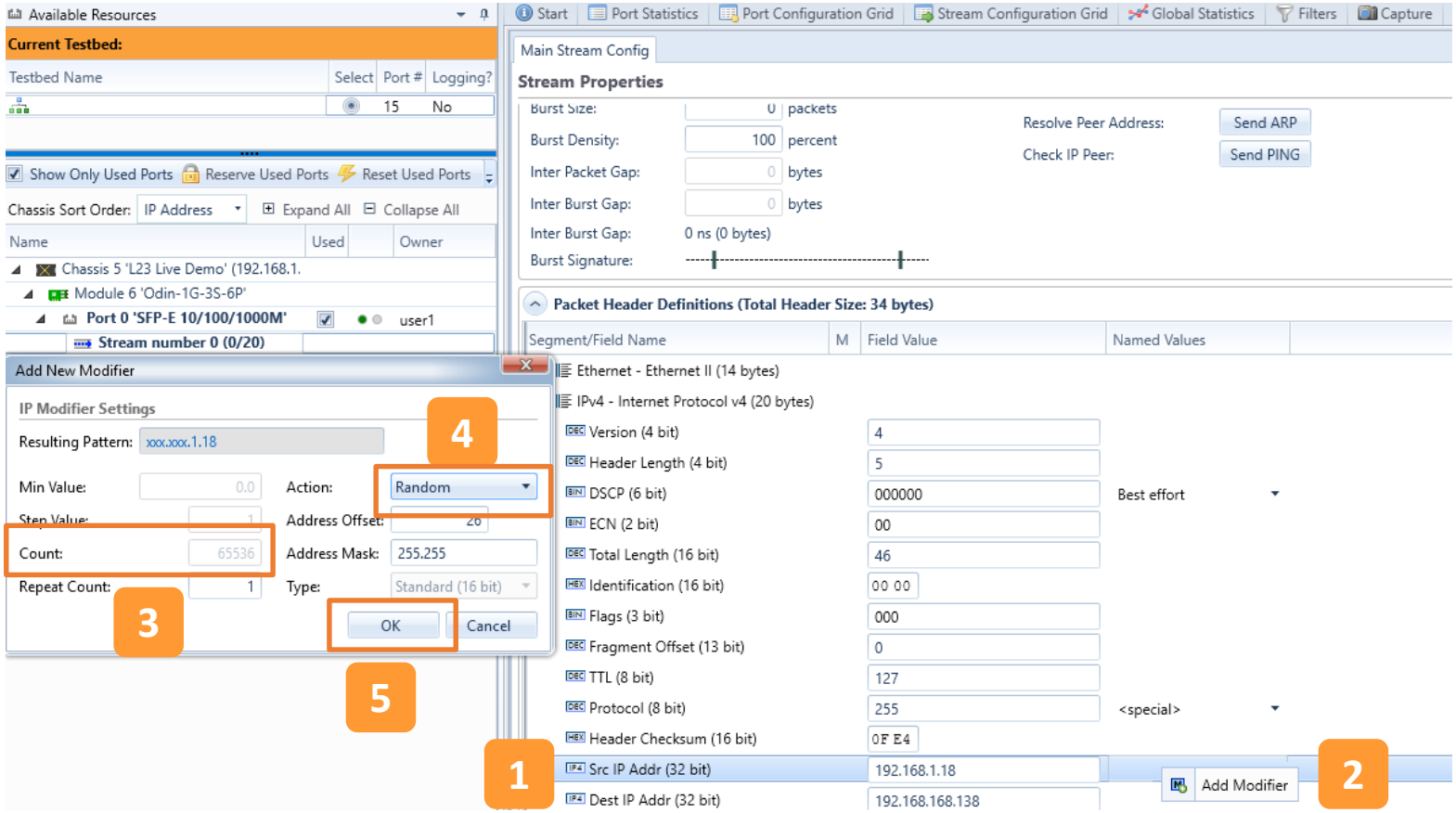
1. Manually writing the Address
2. Click the ARP button to ARP the GW configured for the port.



DDoS – UDP FLOOD

Randomize Source IP Address

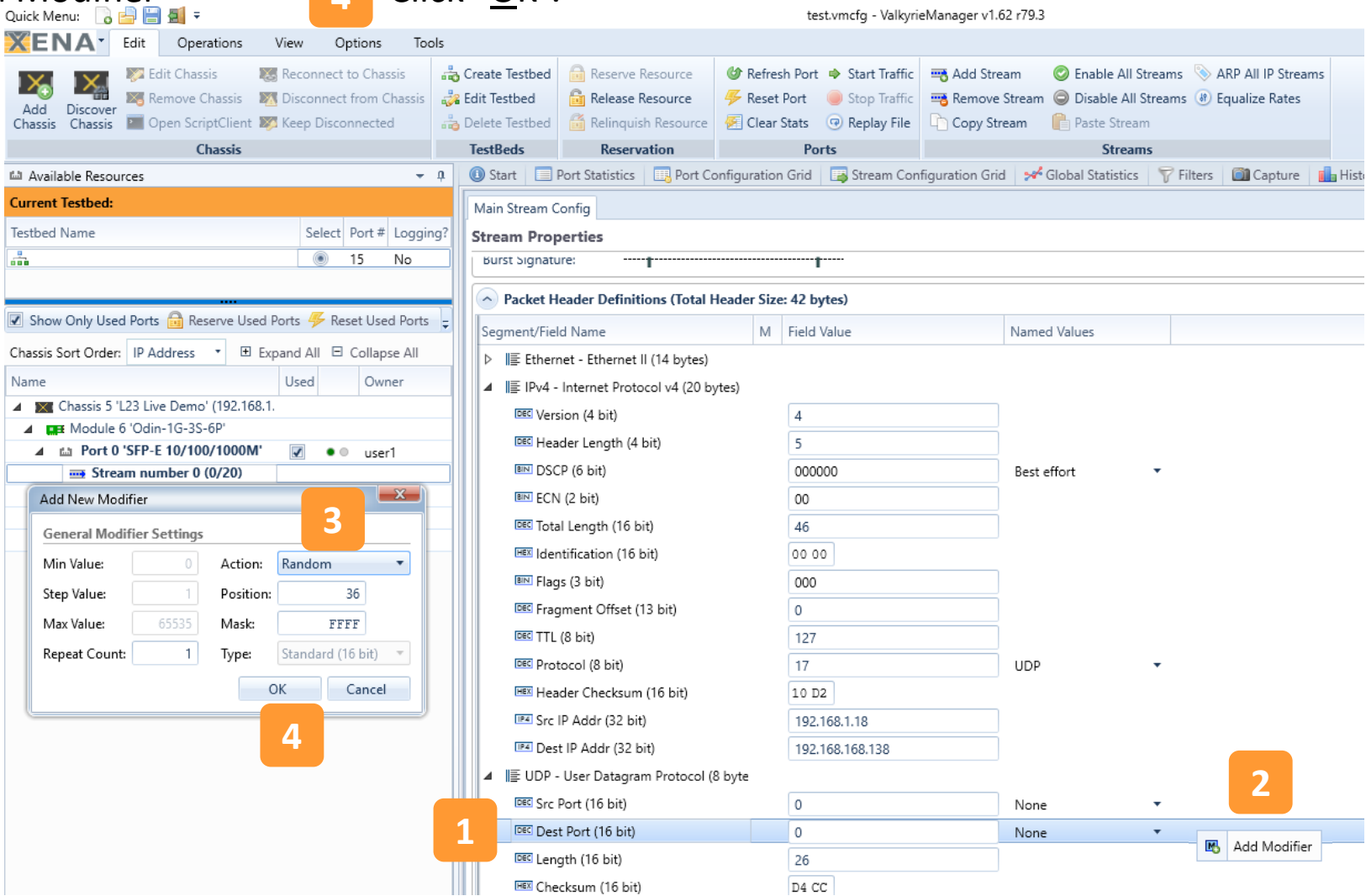
1. Right click on “Src IP Addr”
2. Click “Add Modifier”
3. Select #of Src Ip`s
4. Select Address Action (Random Recommended)
5. Click “OK”.



DDoS – UDP FLOOD

Randomize Dest Port Number (optional)

1. Right click on “Dest Port”
2. Click “Add Modifier”
3. Select Port Action (Random Recommended)
4. Click “OK”.



DDoS – TEARDROP ATTACK

Teardrop (IP Fragment Overlap) Attack

When two fragments contained within the same IP datagram have offsets that indicate that they overlap each other in positioning within the datagram.

Some operating systems do not properly handle fragments that overlap in this manner and may throw exceptions or behave in other undesirable ways upon receipt of overlapping fragments.

DDoS – TEARDROP ATTACK

Teardrop Attack

A legitimate host has no reason of producing overlapping fragments.

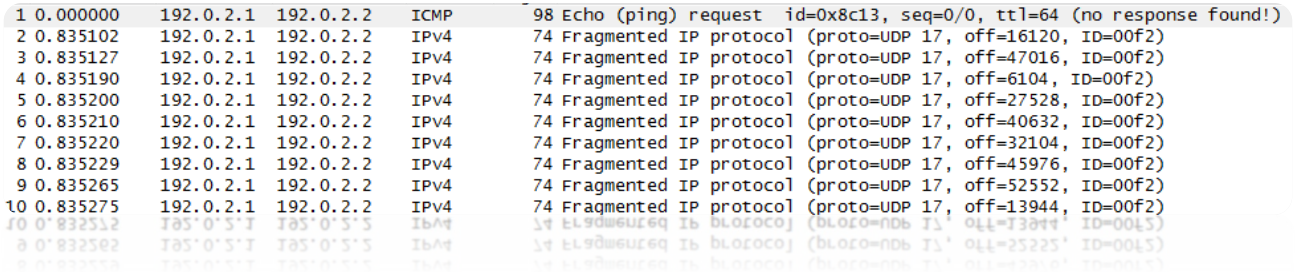
A receiver has no reason to accept them.

RFC5722 recommends that overlapping fragments should be totally disallowed:

- *...the entire datagram (as well as any constituent fragments, including those not yet received) must be silently discarded.*

If fragmentation overlapping is handled differently by different OS, if manipulated properly can lead to:

- OS Fingerprinting
- IDS Insertion / Evasion
- Firewall Evasion
- DoS due to consumption of the resources.
- DoS due to ...kernel crashes.
- Even ...remote code execution



1	0.000000	192.0.2.1	192.0.2.2	ICMP	98 Echo (ping) request id=0x8c13, seq=0/0, ttl=64 (no response found!)
2	0.835102	192.0.2.1	192.0.2.2	IPv4	74 Fragmented IP protocol (proto=UDP 17, off=16120, ID=00f2)
3	0.835127	192.0.2.1	192.0.2.2	IPv4	74 Fragmented IP protocol (proto=UDP 17, off=47016, ID=00f2)
4	0.835190	192.0.2.1	192.0.2.2	IPv4	74 Fragmented IP protocol (proto=UDP 17, off=6104, ID=00f2)
5	0.835200	192.0.2.1	192.0.2.2	IPv4	74 Fragmented IP protocol (proto=UDP 17, off=27528, ID=00f2)
6	0.835210	192.0.2.1	192.0.2.2	IPv4	74 Fragmented IP protocol (proto=UDP 17, off=40632, ID=00f2)
7	0.835220	192.0.2.1	192.0.2.2	IPv4	74 Fragmented IP protocol (proto=UDP 17, off=32104, ID=00f2)
8	0.835229	192.0.2.1	192.0.2.2	IPv4	74 Fragmented IP protocol (proto=UDP 17, off=45976, ID=00f2)
9	0.835265	192.0.2.1	192.0.2.2	IPv4	74 Fragmented IP protocol (proto=UDP 17, off=52552, ID=00f2)
10	0.835275	192.0.2.1	192.0.2.2	IPv4	74 Fragmented IP protocol (proto=UDP 17, off=13944, ID=00f2)

DDoS – TEARDROP ATTACK

Teardrop Attack

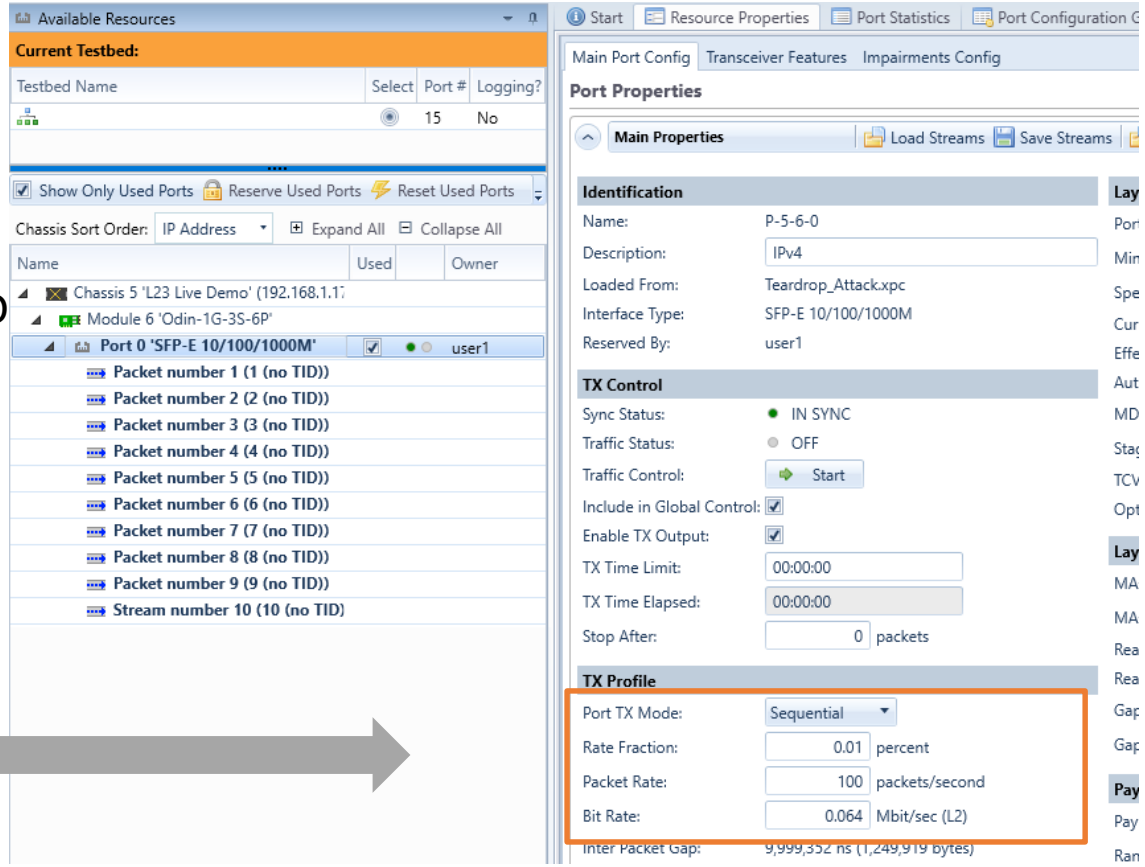
1 Load configuration file

Teardrop_Attack.xpc

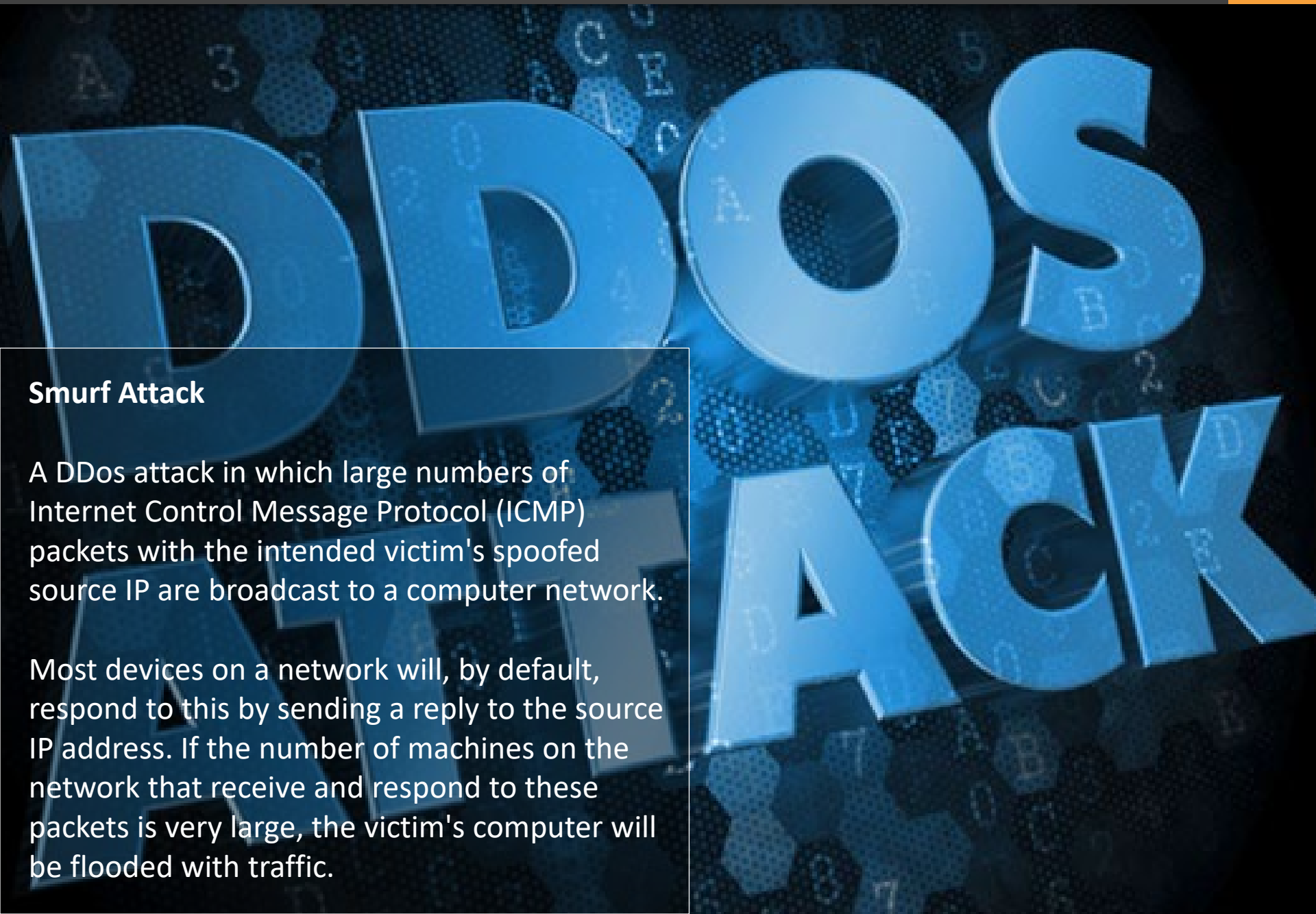
It will add Streams with no TID

and set port Tx Mode to:

Sequential



DDoS – SMURF ATTACK



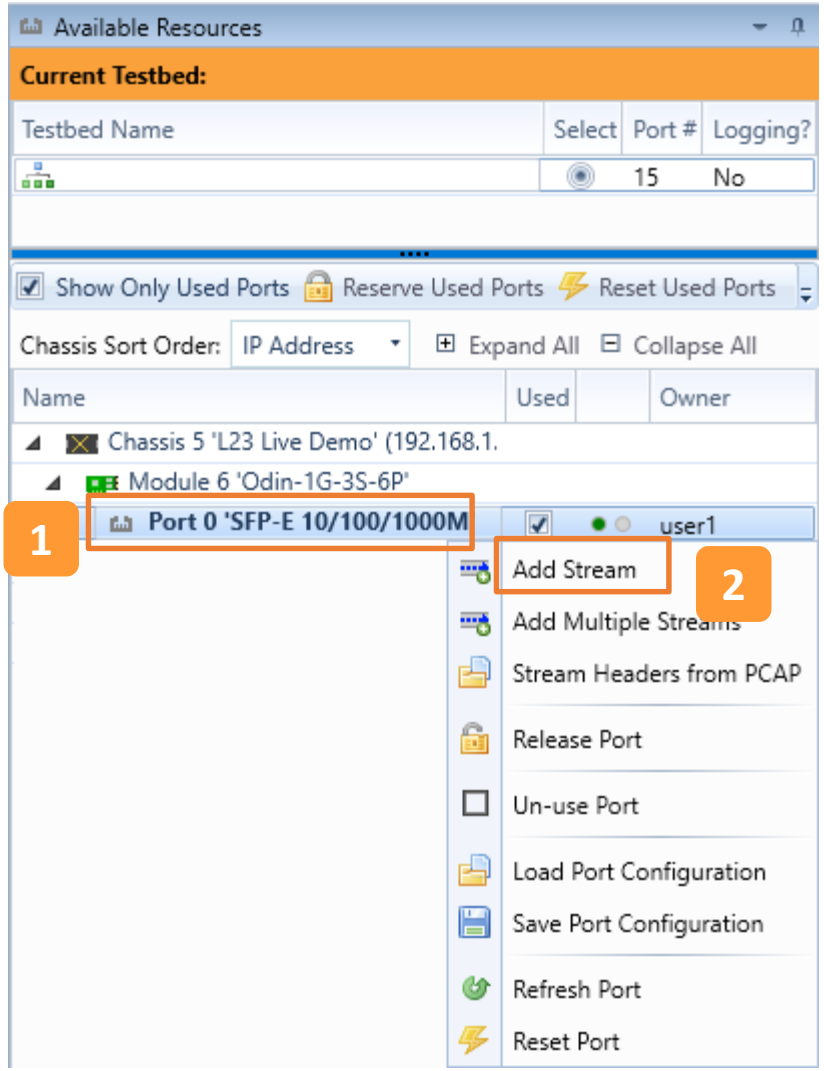
Smurf Attack

A DDos attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network.

Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic.

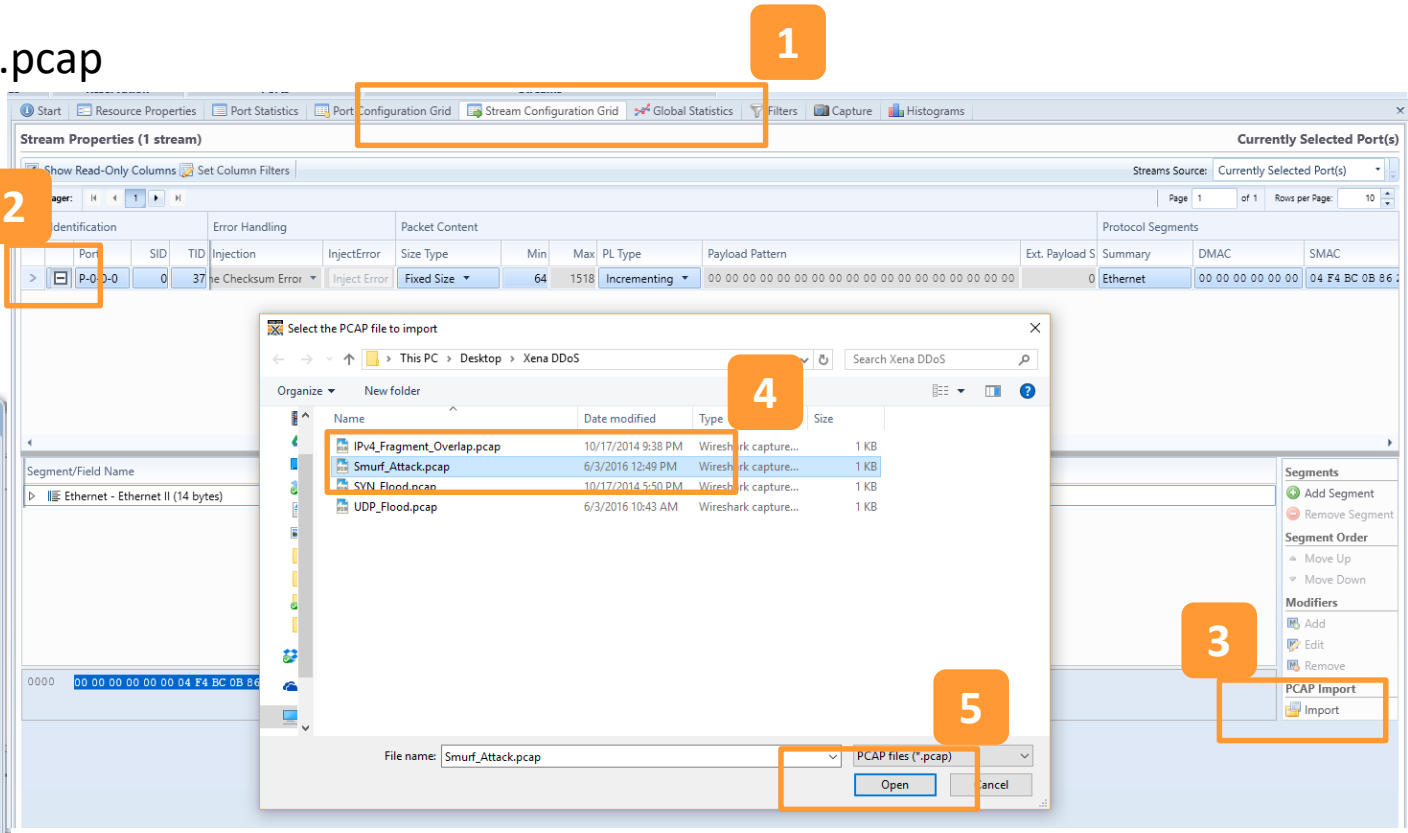
DDoS – SMURF ATTACK

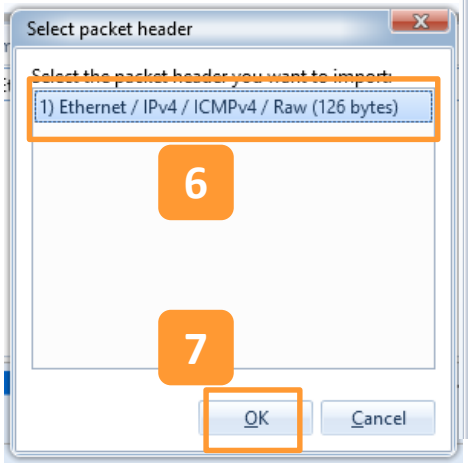
1. Right-click on Attacking port.
2. Click “Add Stream”



DDoS – SMURF ATTACK

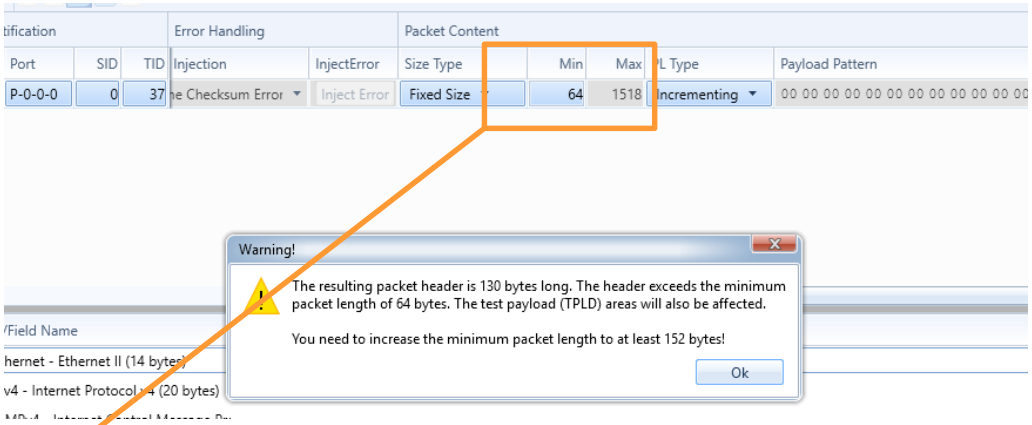
1. Go to “Stream Configuration Grid” tab.
2. Click “+”.
3. Click “Import”
4. Select Smurf_Attack.pcap
5. Click “Open”
6. Click First row
7. Click “OK”

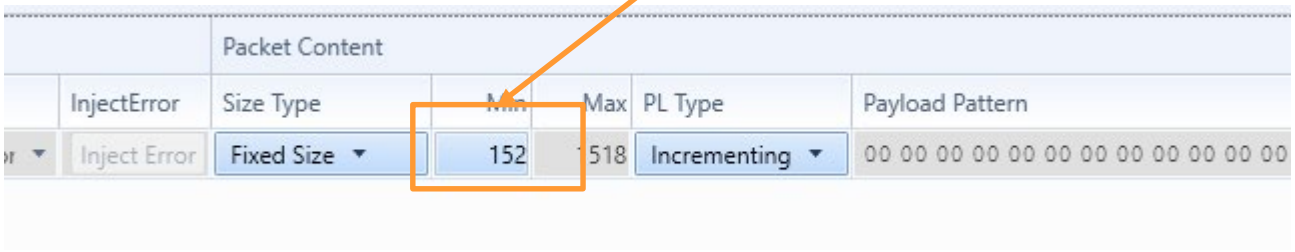




DDoS – SMURF ATTACK

1 You may see the alert telling you to increase the minimum packet length. Change the minimum size to 152 bytes.

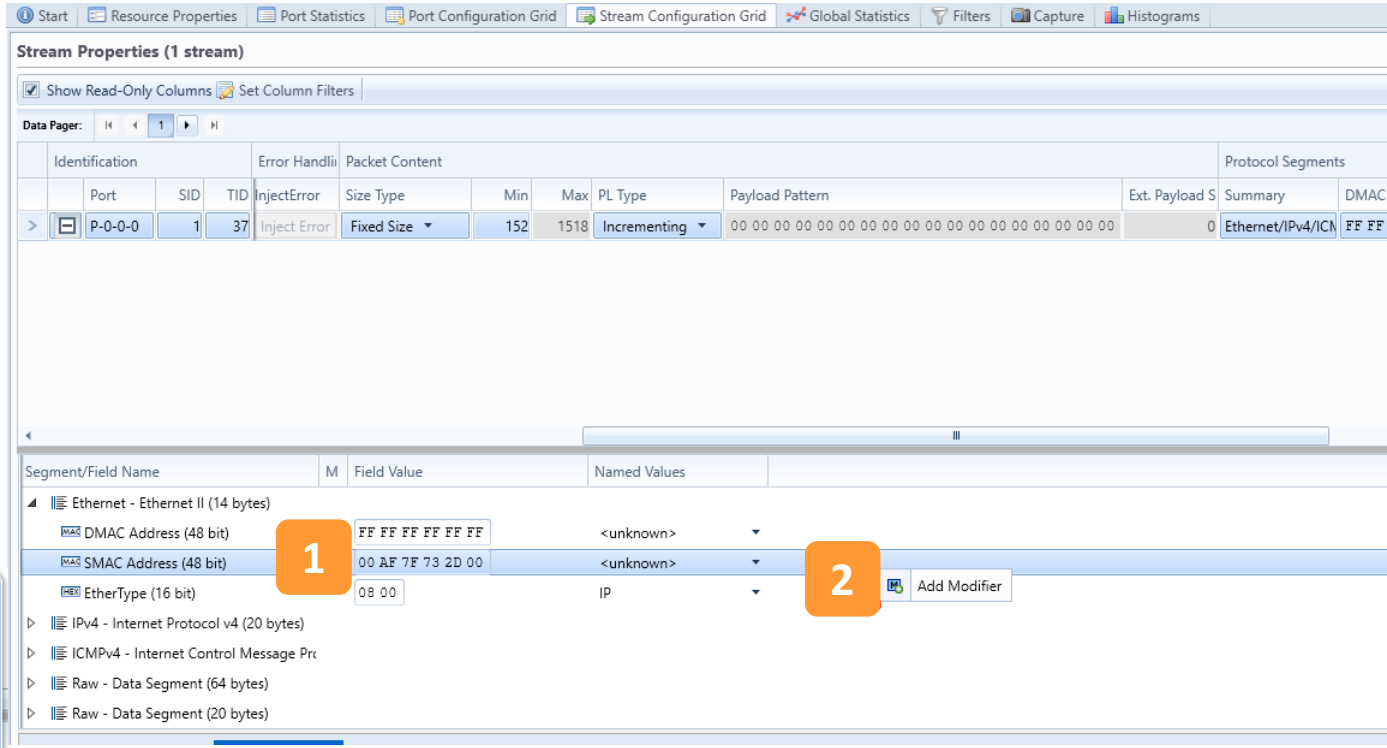


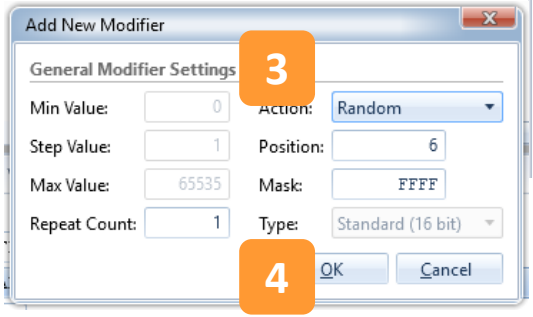


DDoS – SMURF ATTACK

Randomize Source MAC Address

1. Right click on “SMAC Address”
2. Click “Add Modifier”
3. Select Action (Random Recommended)
4. Click “OK”.

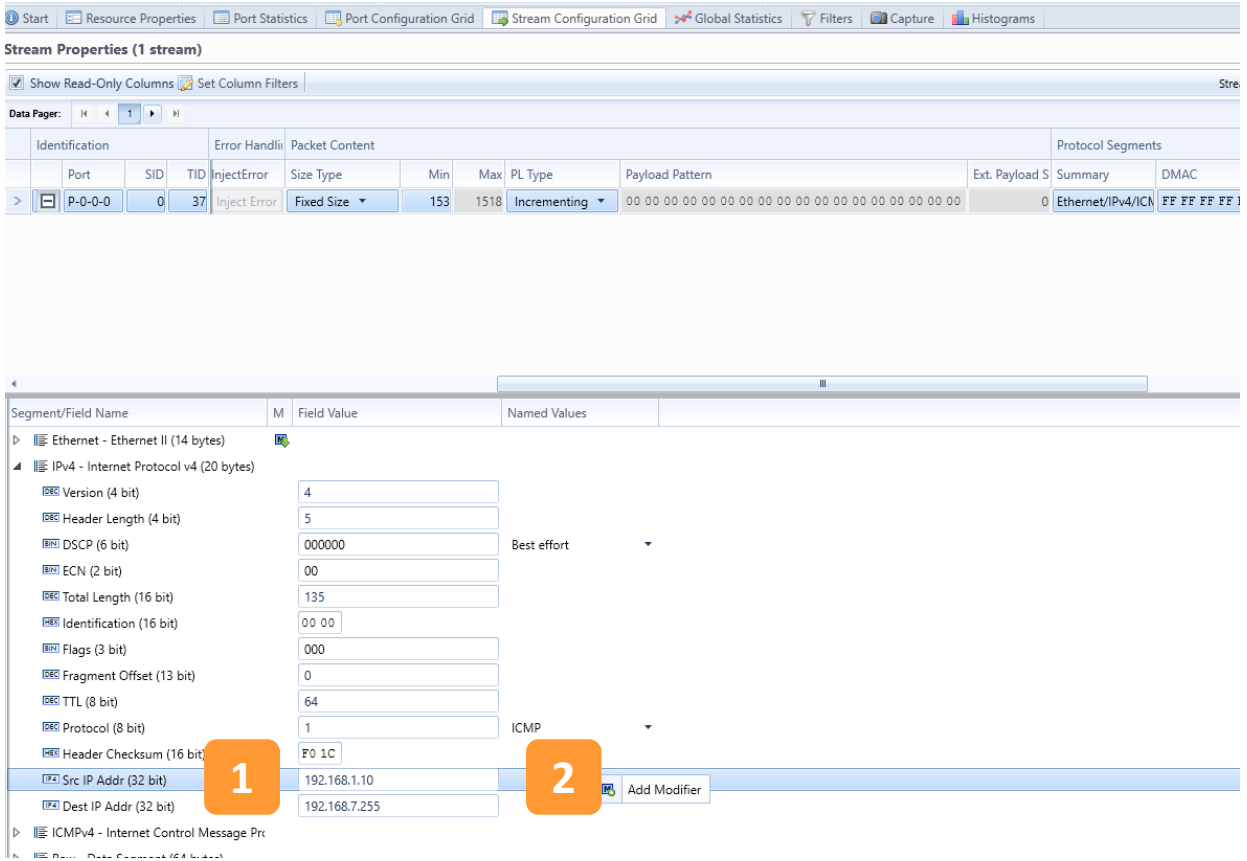


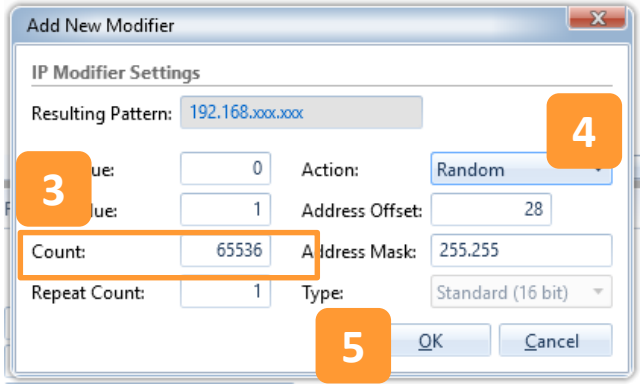


DDoS – SMURF ATTACK

Randomize Source IP Address

1. Right click on “Src IP Addr”
2. Click “Add Modifier”
3. Select #of Src Ip`s
4. Select Address Action (Random Recommended)
5. Click “OK”.





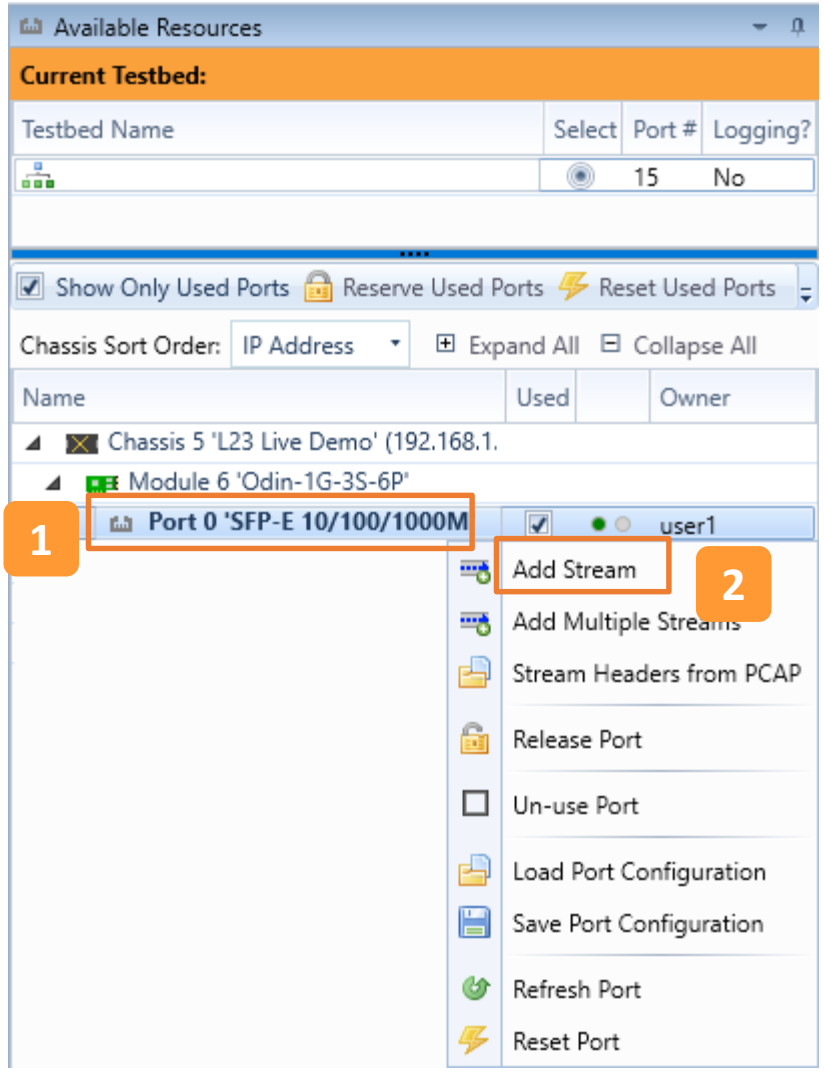
DDoS – PING OF DEATH

Ping of Death

A type of attack on a computer system that involves sending a malformed or otherwise malicious ping to a computer.

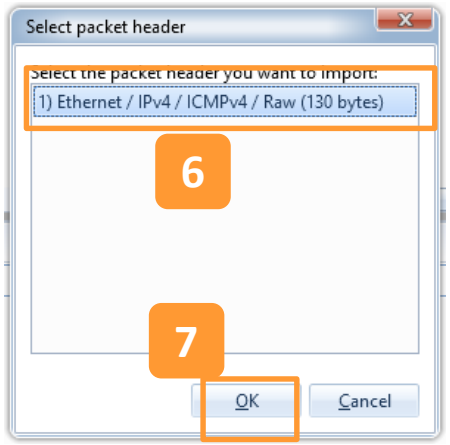
DDoS – PING OF DEATH

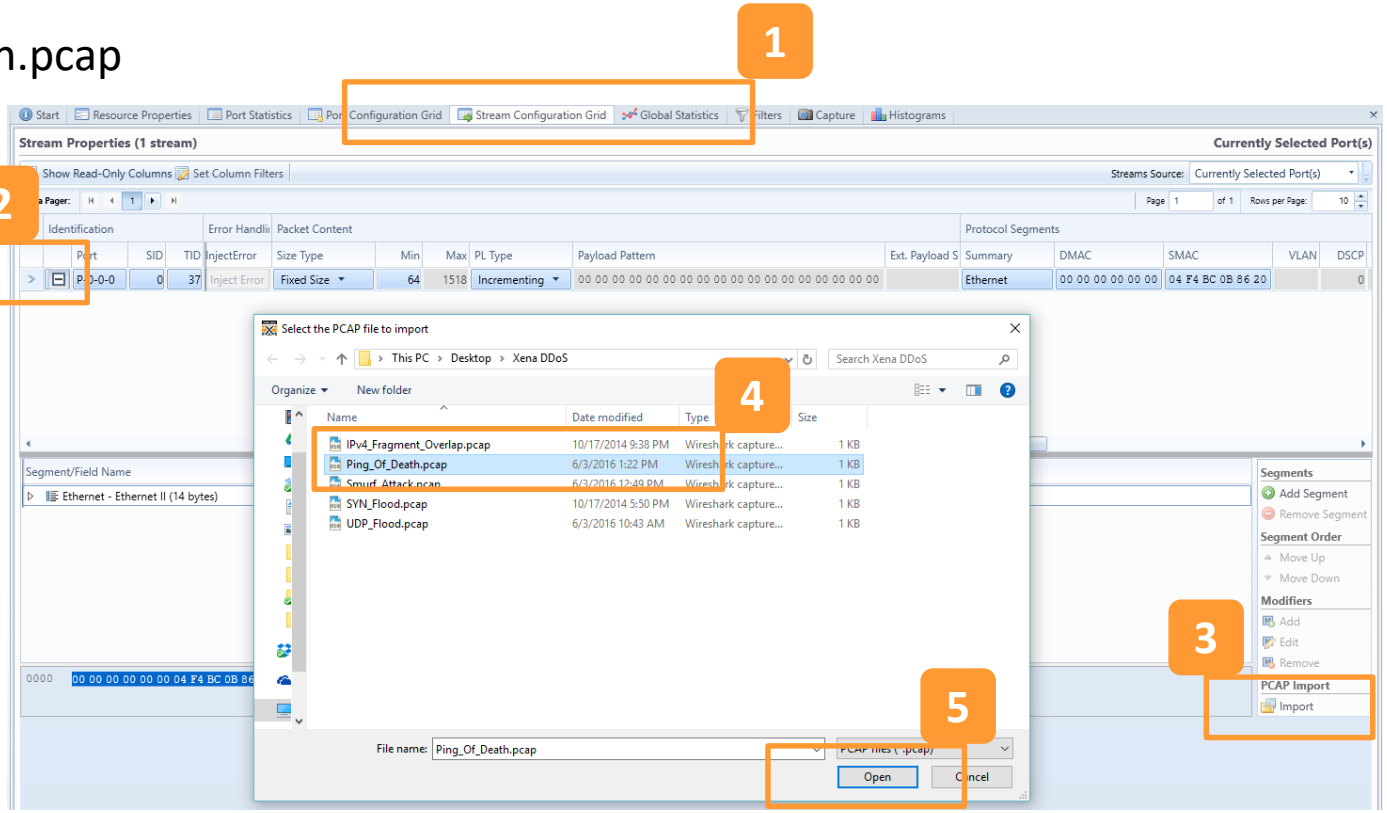
1. Right-click on Attacking port.
2. Click “Add Stream”



DDoS – PING OF DEATH

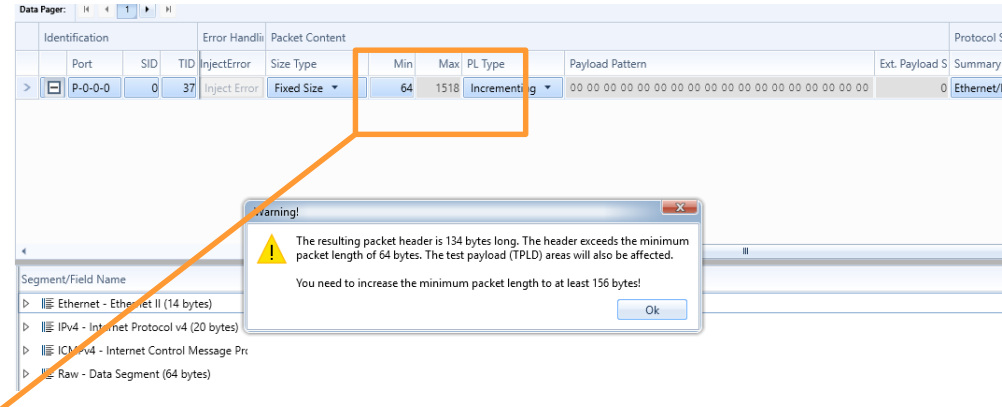
1. Go to “Stream Configuration Grid” tab.
2. Click “+”.
3. Click “Import”
4. Select Ping_Of_Death.pcap
5. Click “Open”
6. Click First row
7. Click “OK”

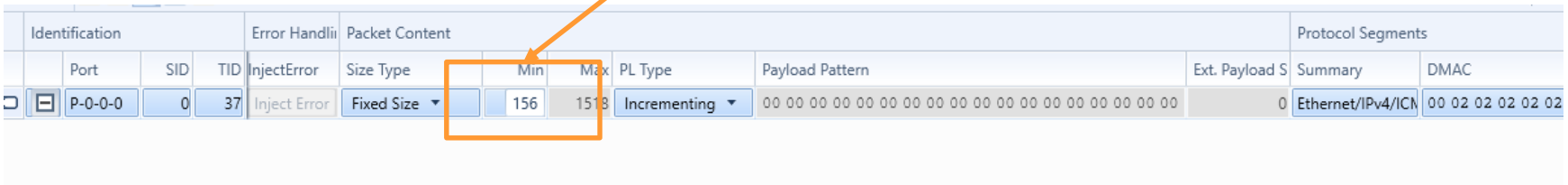




DDoS – PING OF DEATH

1 You may see the alert telling you to increase the minimum packet length. Change the minimum size to 156 bytes.





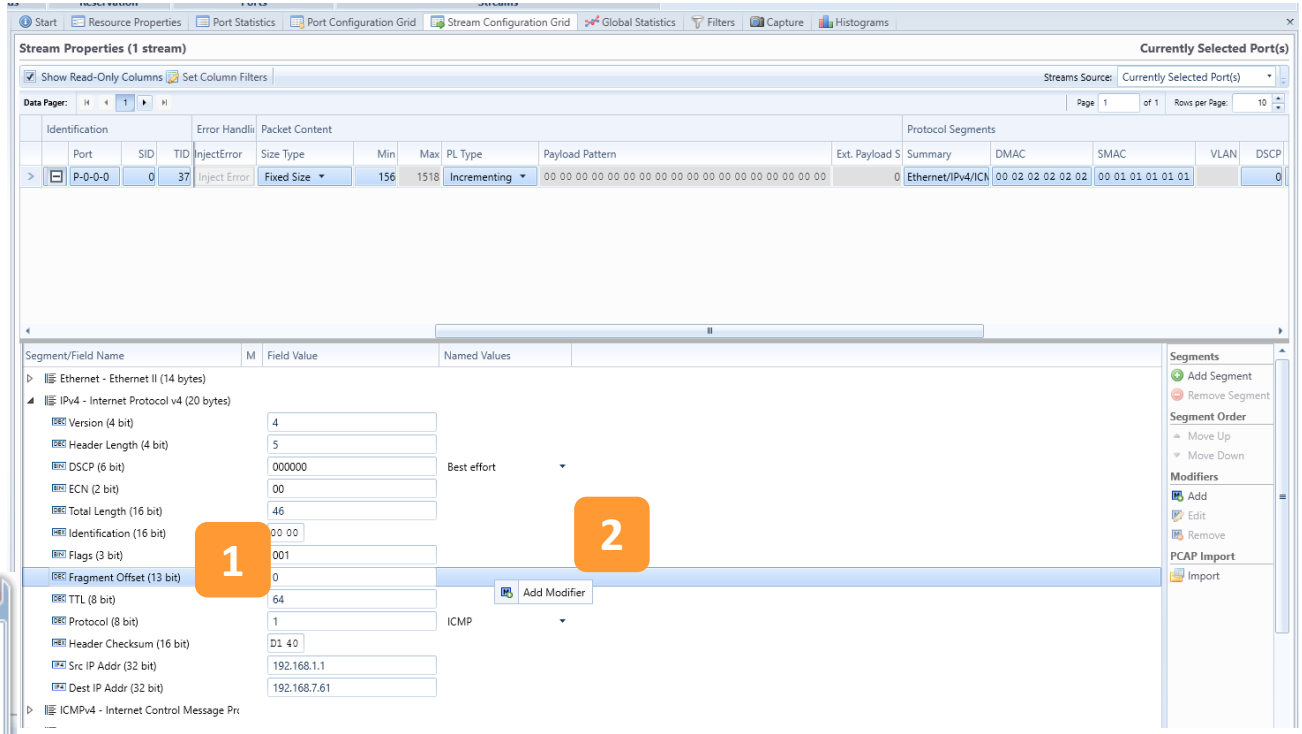
DDoS – PING OF DEATH

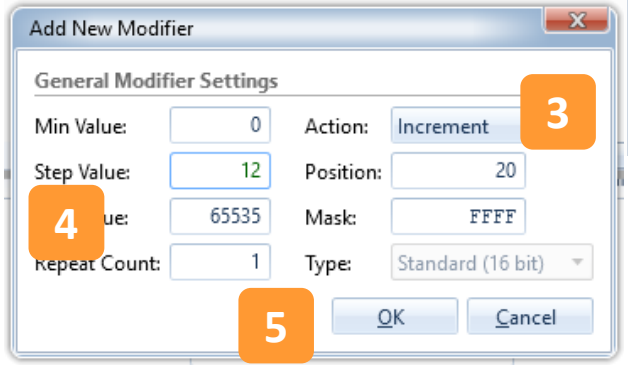
Increase IP Fragment Offset

1. Right click on “Fragment Offset”
2. Click “Add Modifier”
3. Select Action

(Increment Recommended)

4. Set ”Step Value” to 12.
5. Click “OK”.





DDoS – PING FLOOD

Ping Flood (ICMP Flood)

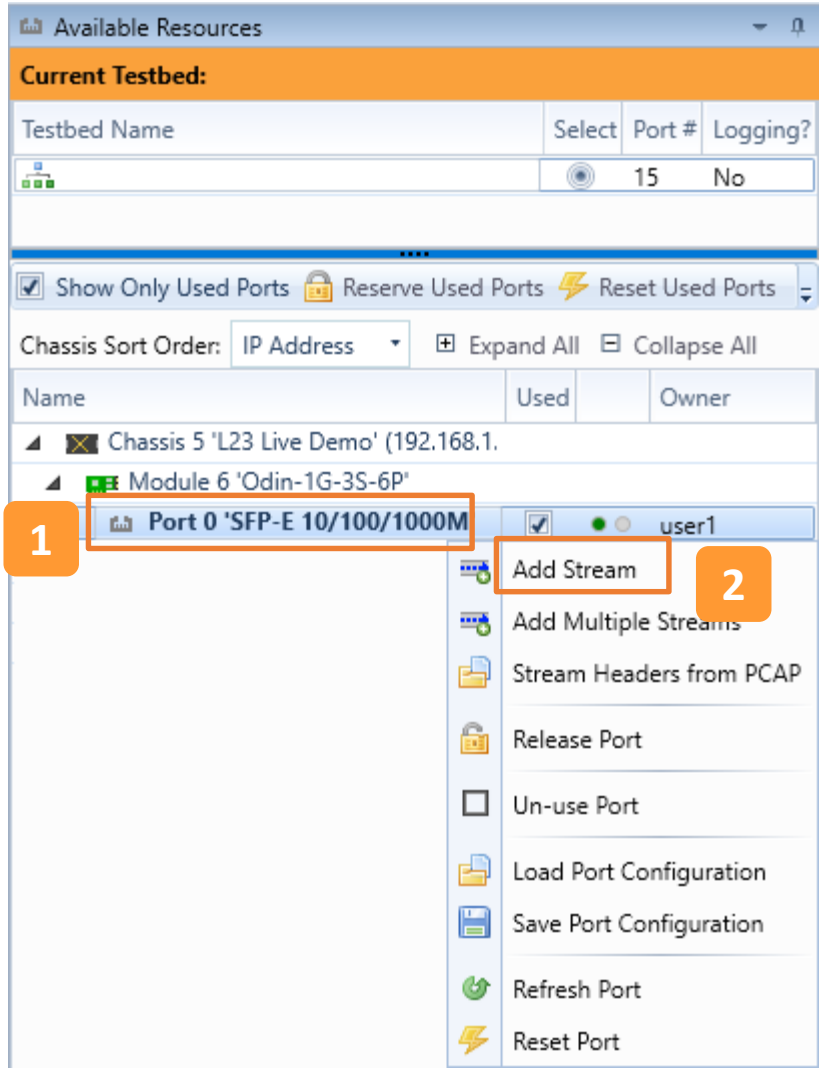
A simple denial-of-service attack where the attacker overwhelms the victim with ICMP Echo Request (ping) packets.

This is most effective by using the flood option of ping which sends ICMP packets as fast as possible without waiting for replies.

If the target system is slow enough, it is possible to consume enough of its CPU cycles for a user to notice a significant slowdown.

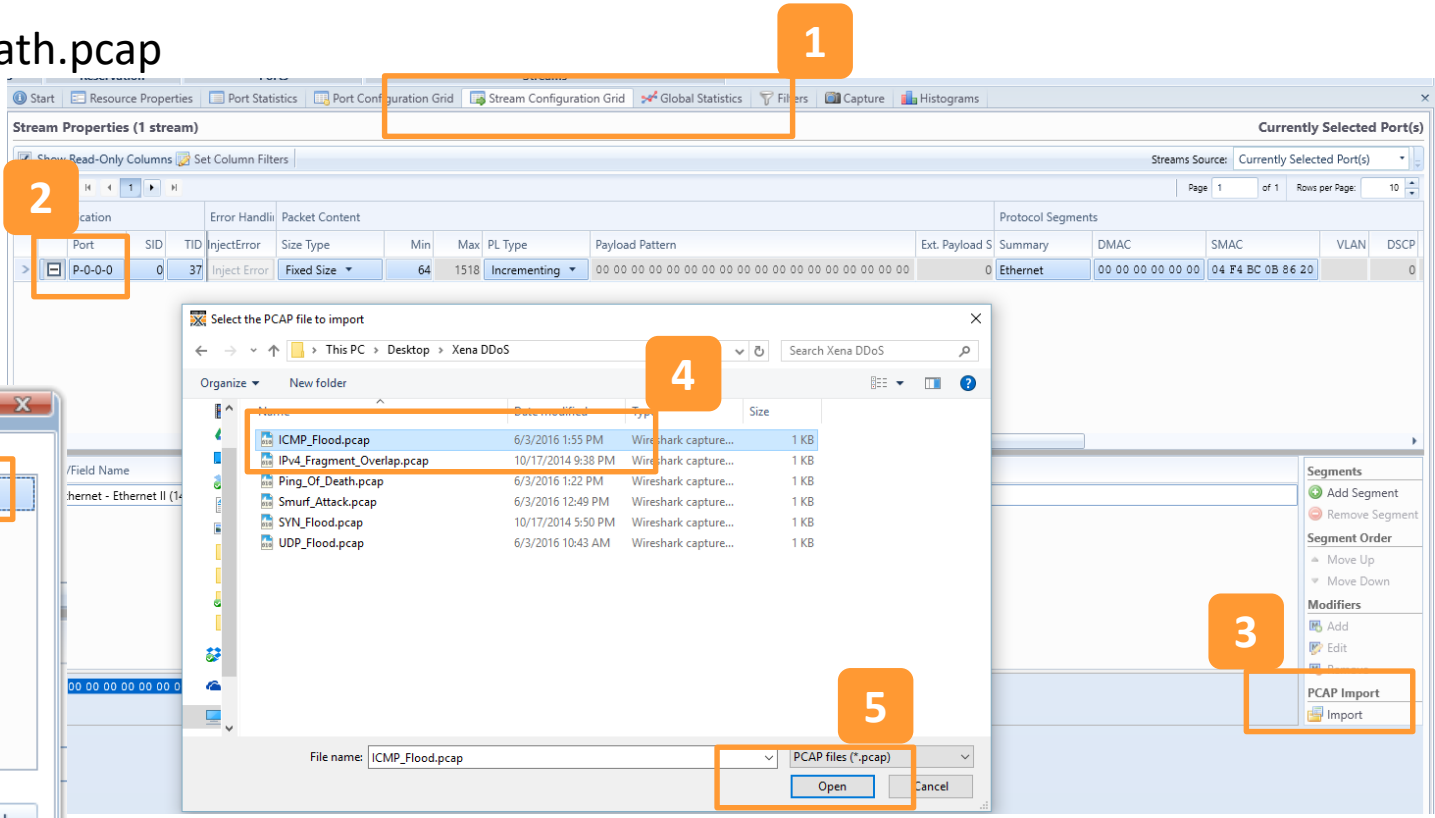
DDoS – PING FLOOD

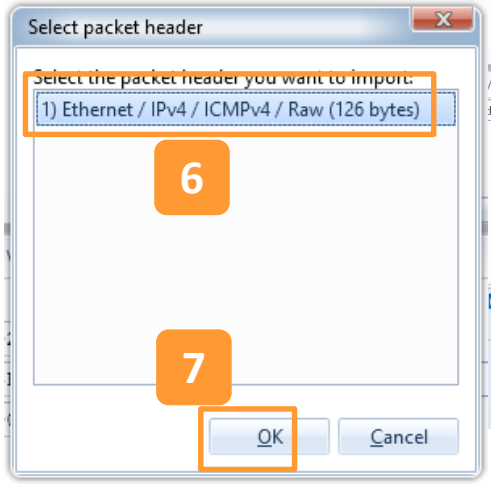
1. Right-click on Attacking port.
2. Click “Add Stream”



DDoS – PING FLOOD

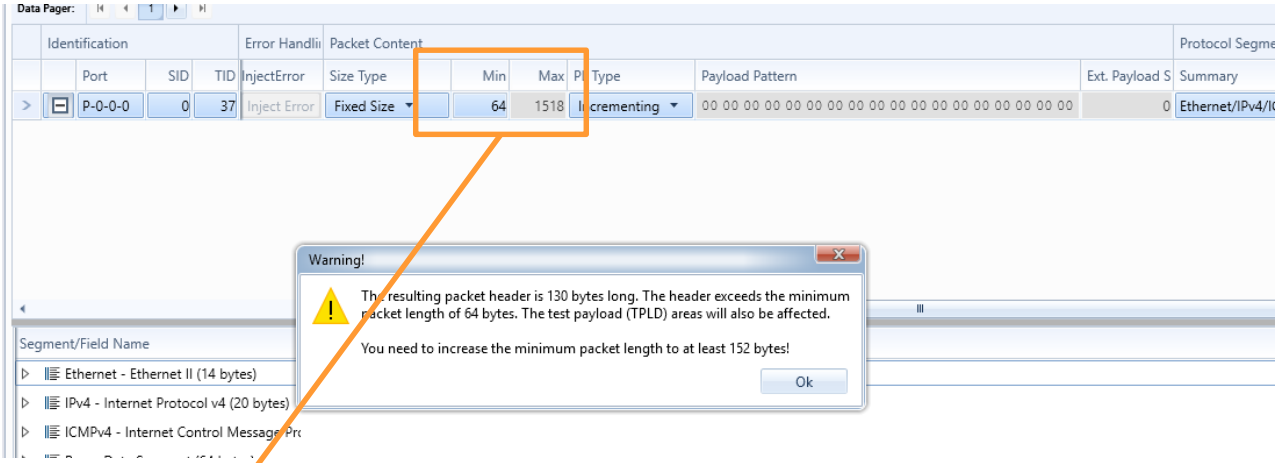
1. Go to “Stream Configuration Grid” tab.
2. Click “+”.
3. Click “Import”
4. Select Ping_Of_Death.pcap
5. Click “Open”
6. Click First row
7. Click “OK”

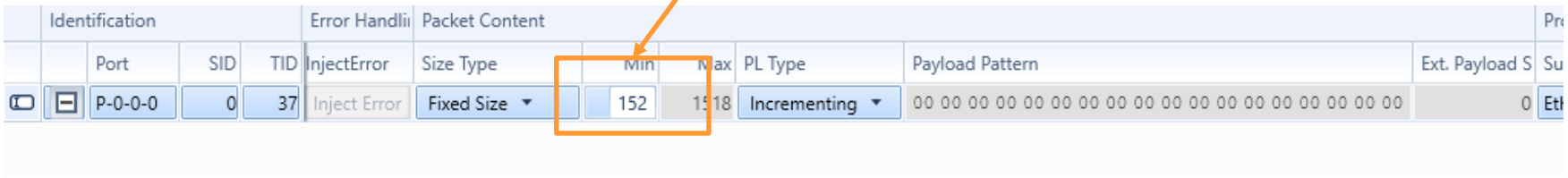




DDoS – PING FLOOD

1 You may see the alert telling you to increase the minimum packet length. Change the minimum size to 152 bytes.





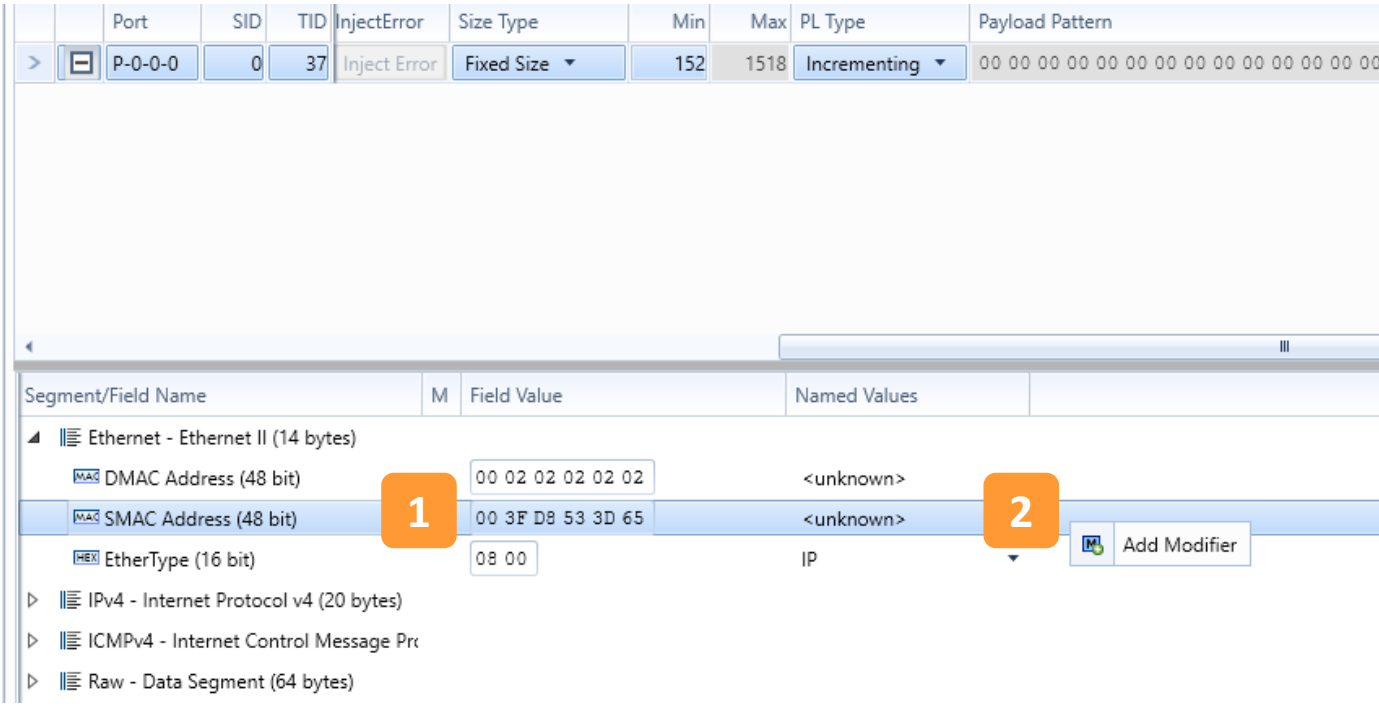
DDoS – PING FLOOD

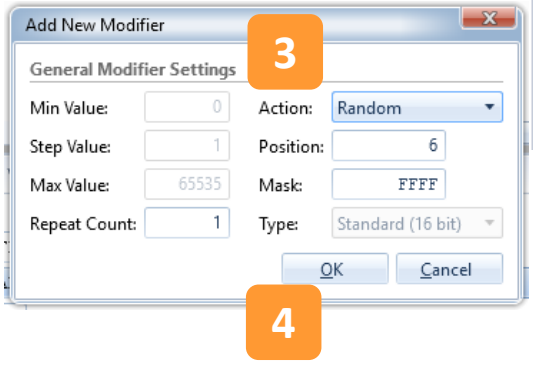
Randomize Source MAC Address

1. Right click on “SMAC Address”
2. Click “Add Modifier”
3. Select Action

(Random Recommended)

4. Click “OK”.

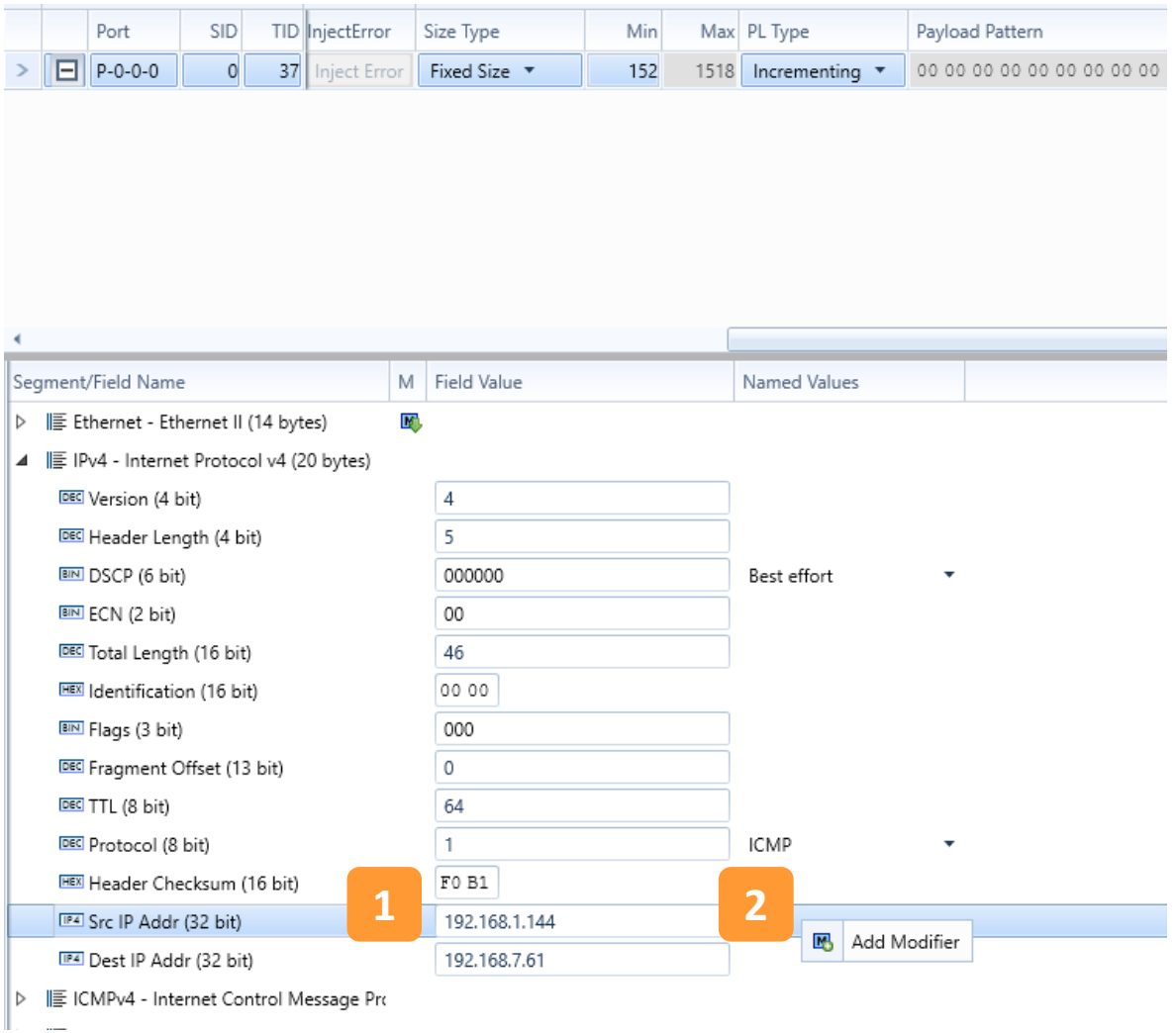


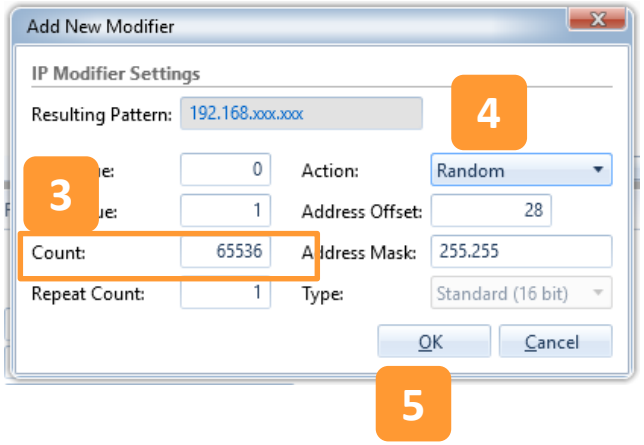


DDoS – PING FLOOD

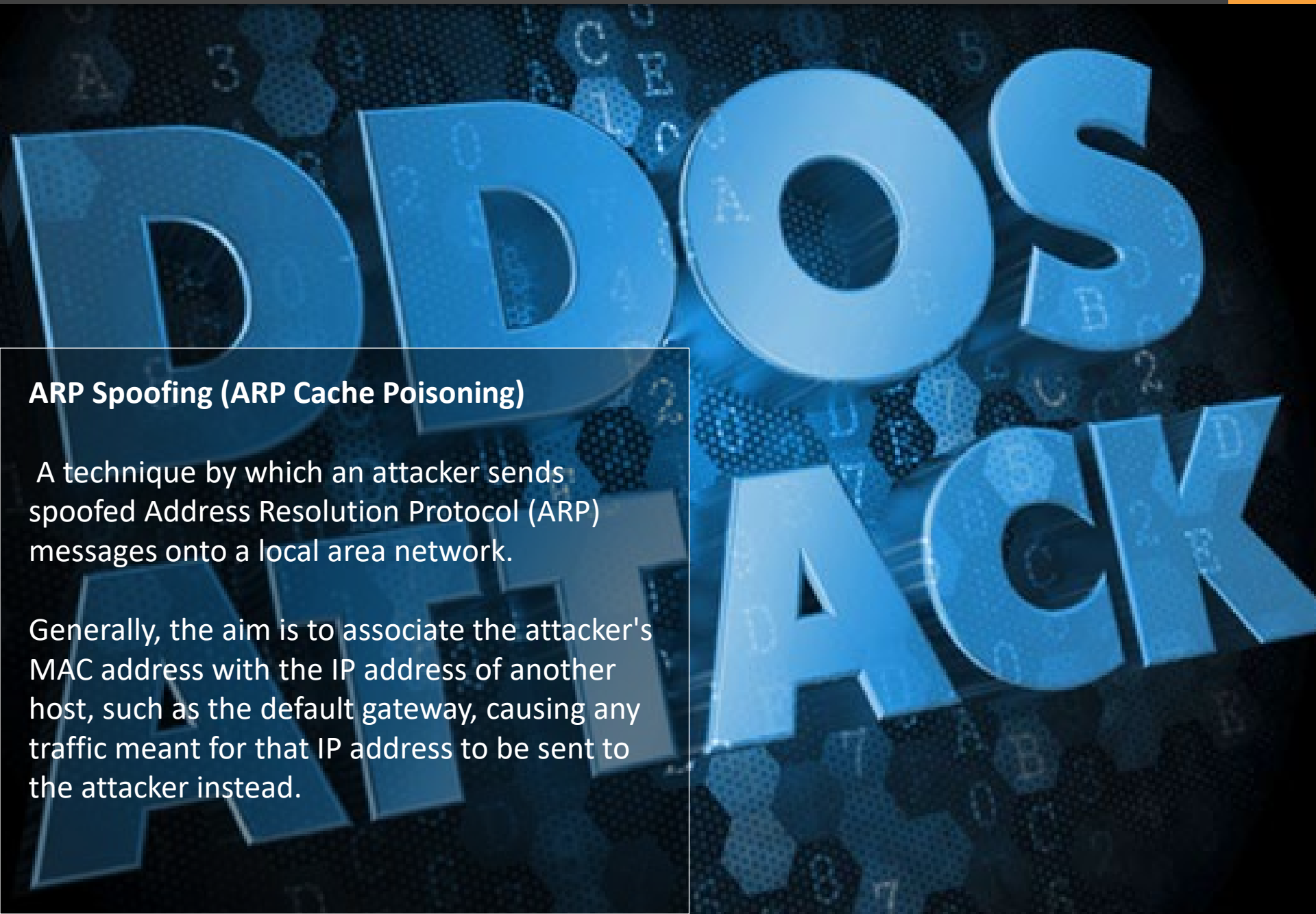
Randomize Source IP Address

1. Right click on “Src IP Addr”
2. Click “Add Modifier”
3. Select #of Src Ip`s
4. Select Address Action (Random Recommended)
5. Click “OK”.





DDoS – ARP SPOOFING



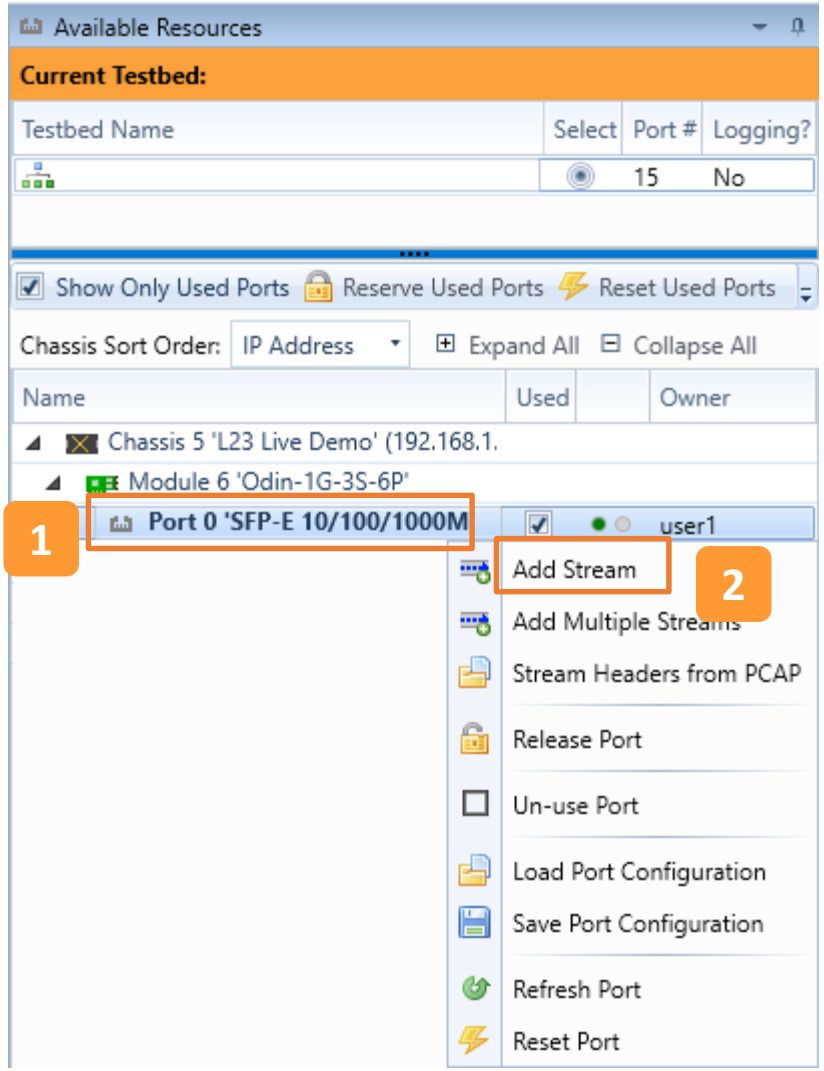
ARP Spoofing (ARP Cache Poisoning)

A technique by which an attacker sends spoofed Address Resolution Protocol (ARP) messages onto a local area network.

Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

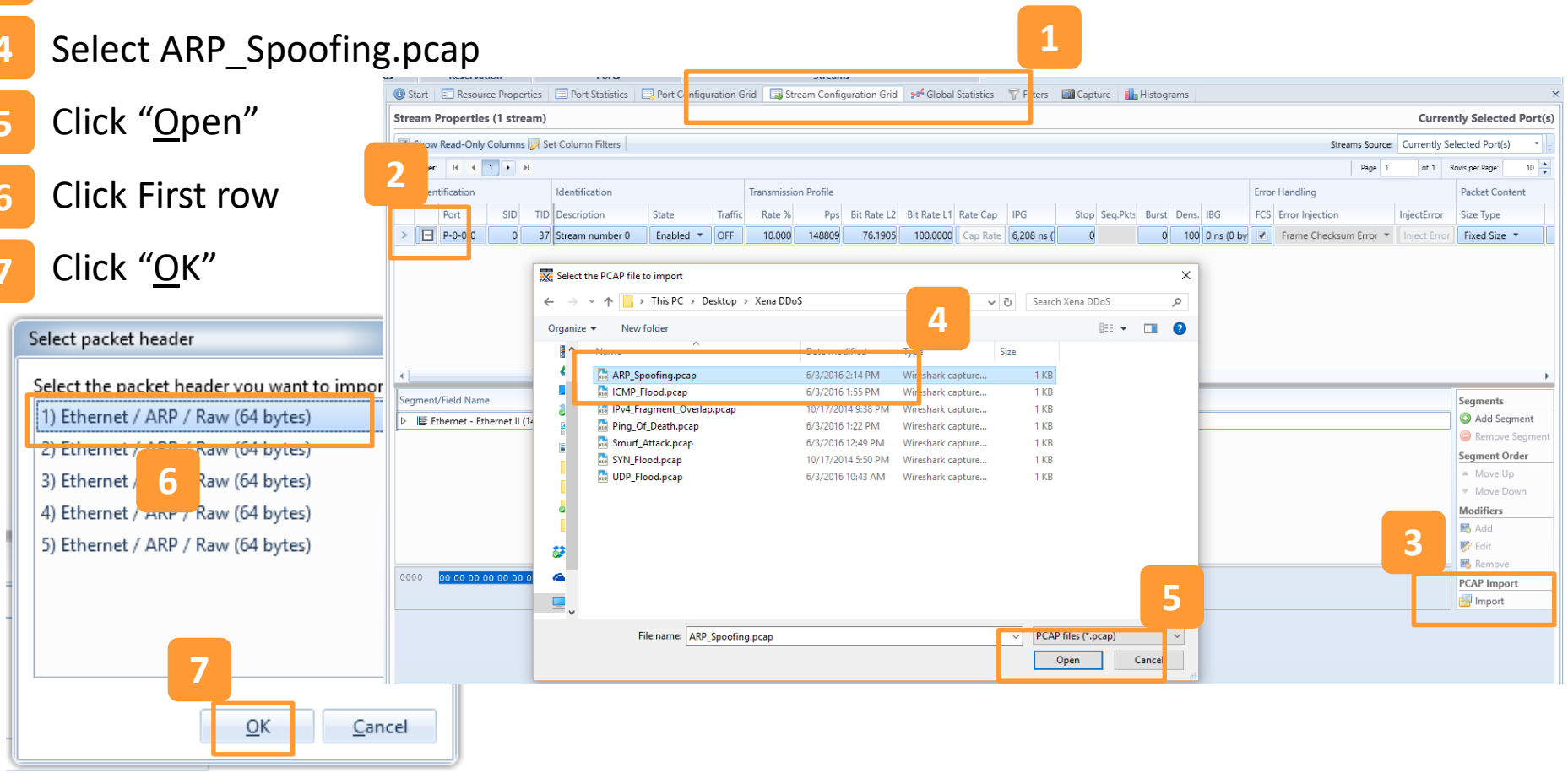
DDoS – ARP SPOOFING

1. Right-click on Attacking port.
2. Click “Add Stream”



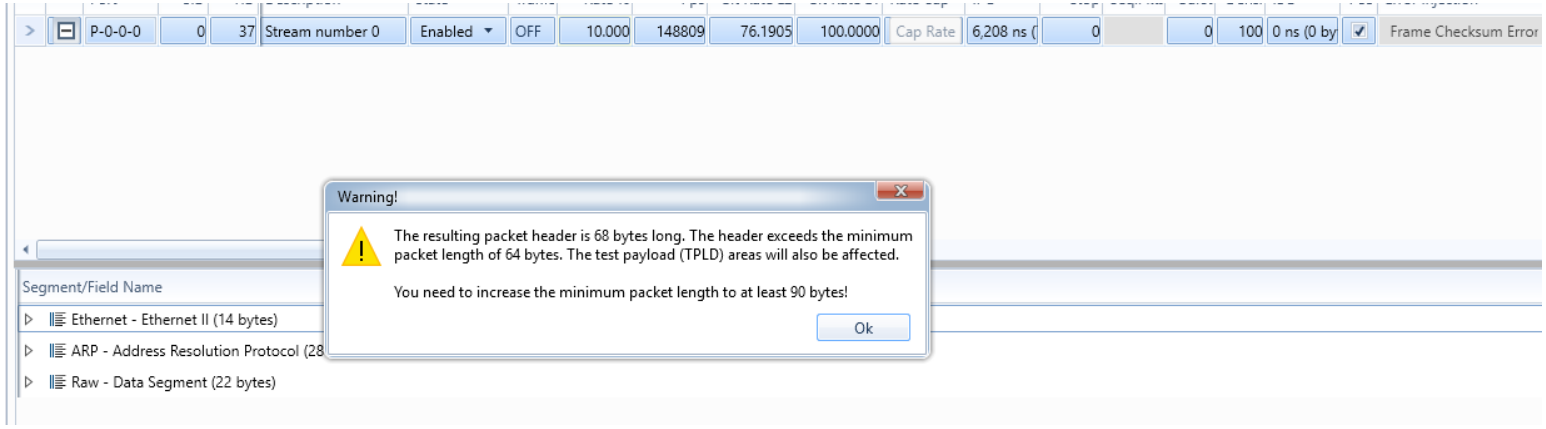
DDoS – ARP SPOOFING

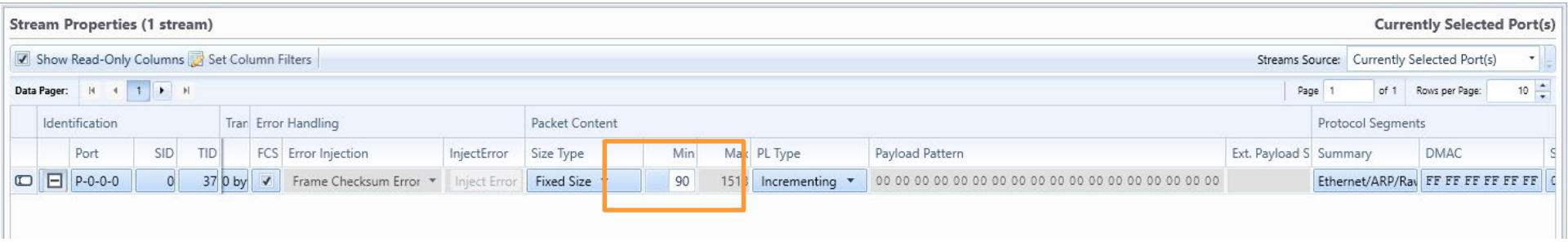
1. Go to “Stream Configuration Grid” tab.
2. Click “+”.
3. Click “Import”
4. Select ARP_Spoofing.pcap
5. Click “Open”
6. Click First row
7. Click “OK”



DDoS – ARP SPOOFING

1 You may see the alert telling you to increase the minimum packet length. Change the minimum size to 90 bytes.





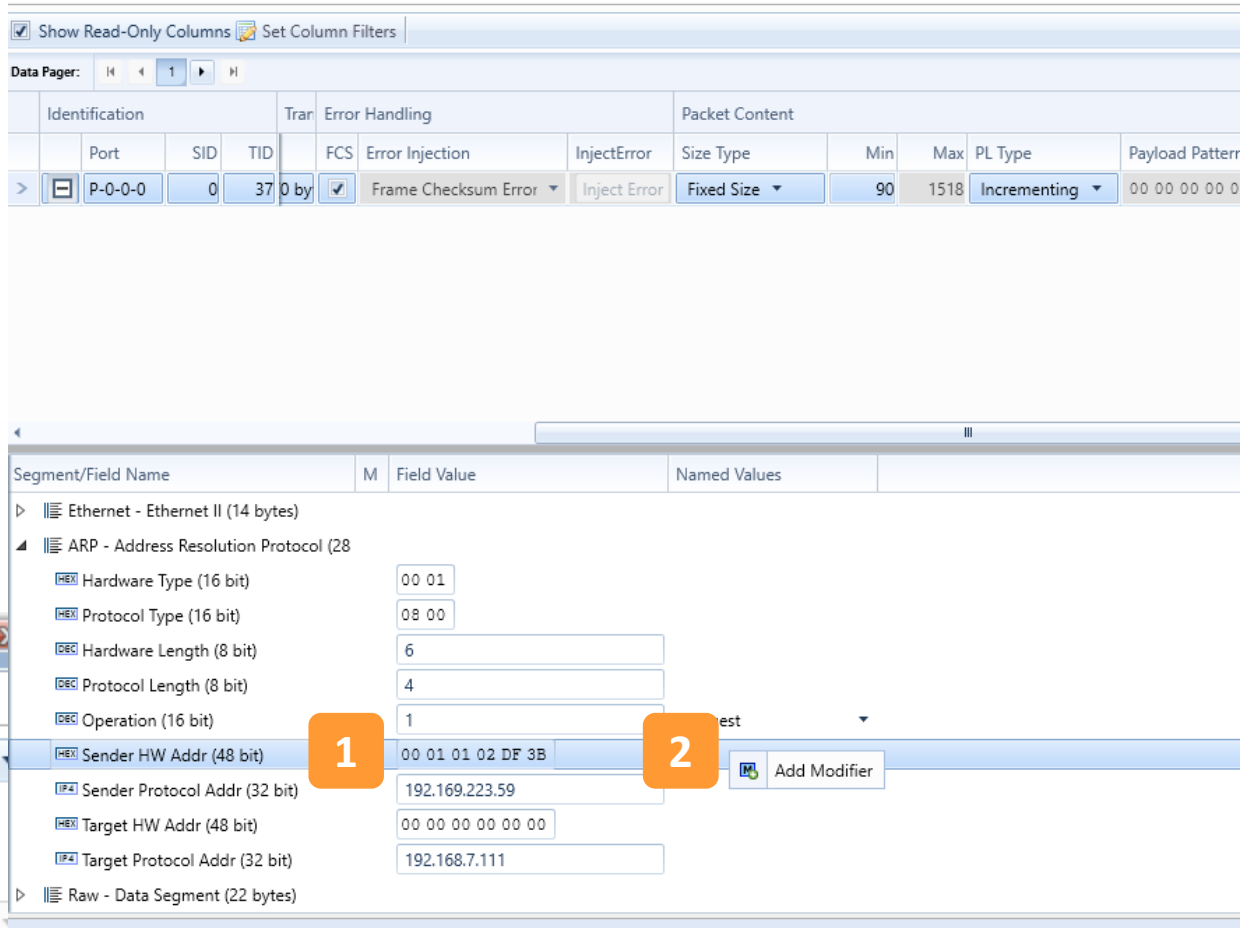
DDoS – ARP SPOOFING

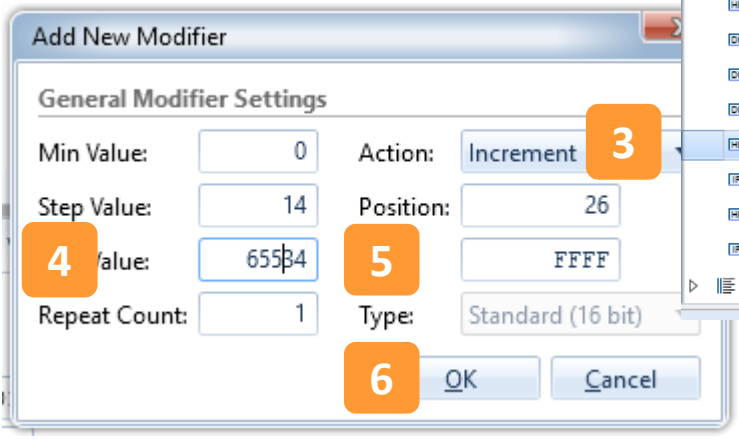
Increase Sender HW Address

1. Right click on “Sender HW Addr”
2. Click “Add Modifier”
3. Select Action

(Increment Recommended)

4. Set ”Step Value” to 14.
5. Set ”Position” to 26.
6. Click “OK”.





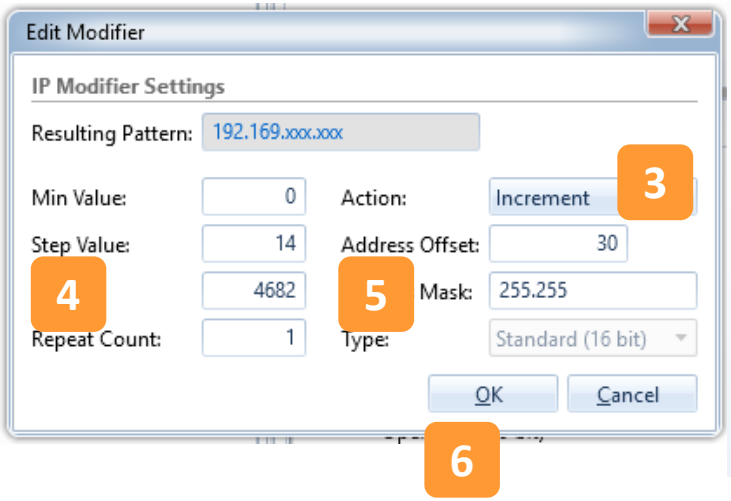
DDoS – ARP SPOOFING

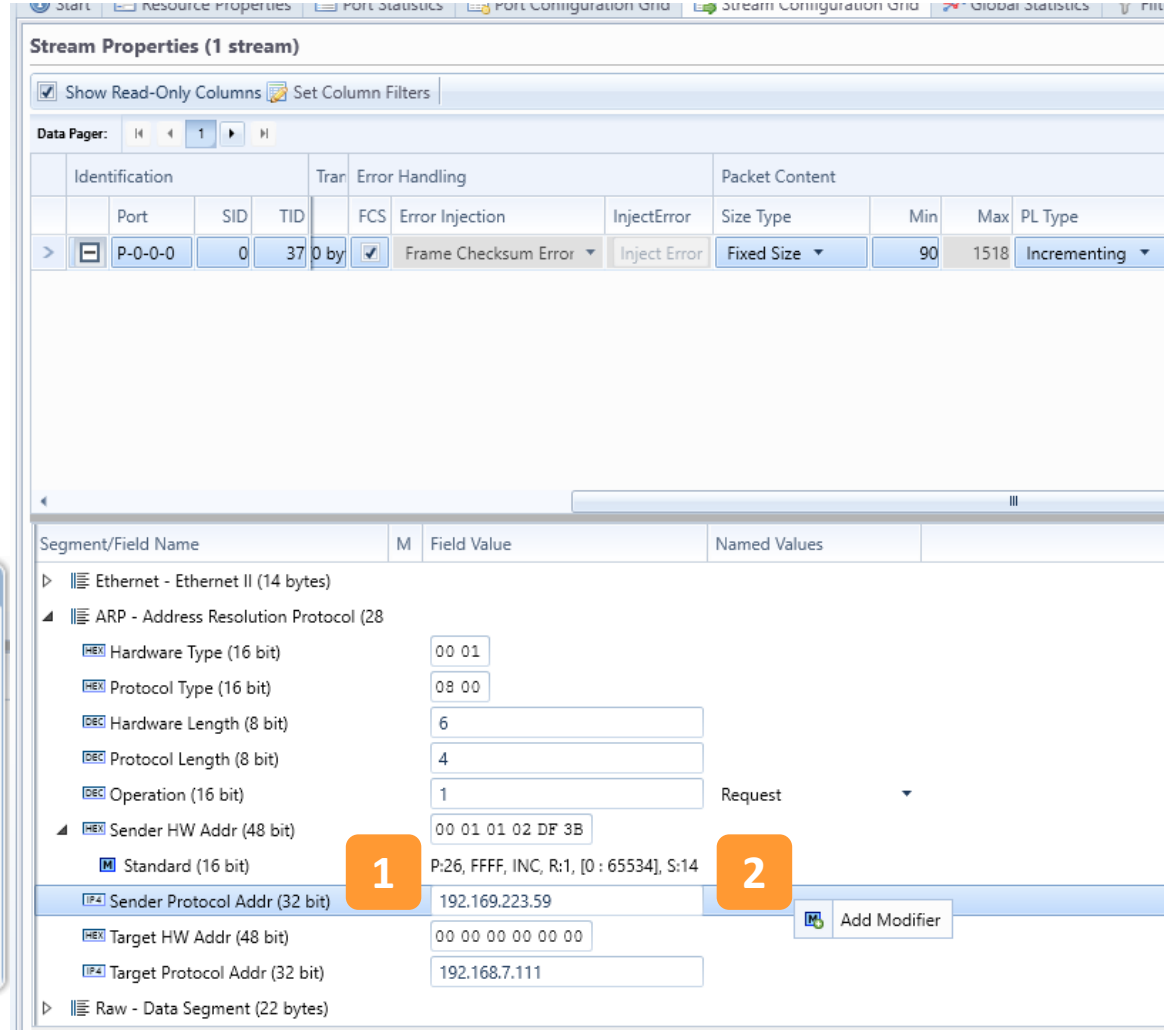
Increase Sender Protocol Address

1. Right click on “Sender Protocol Addr”
2. Click “Add Modifier”
3. Select Action

(Increment Recommended)

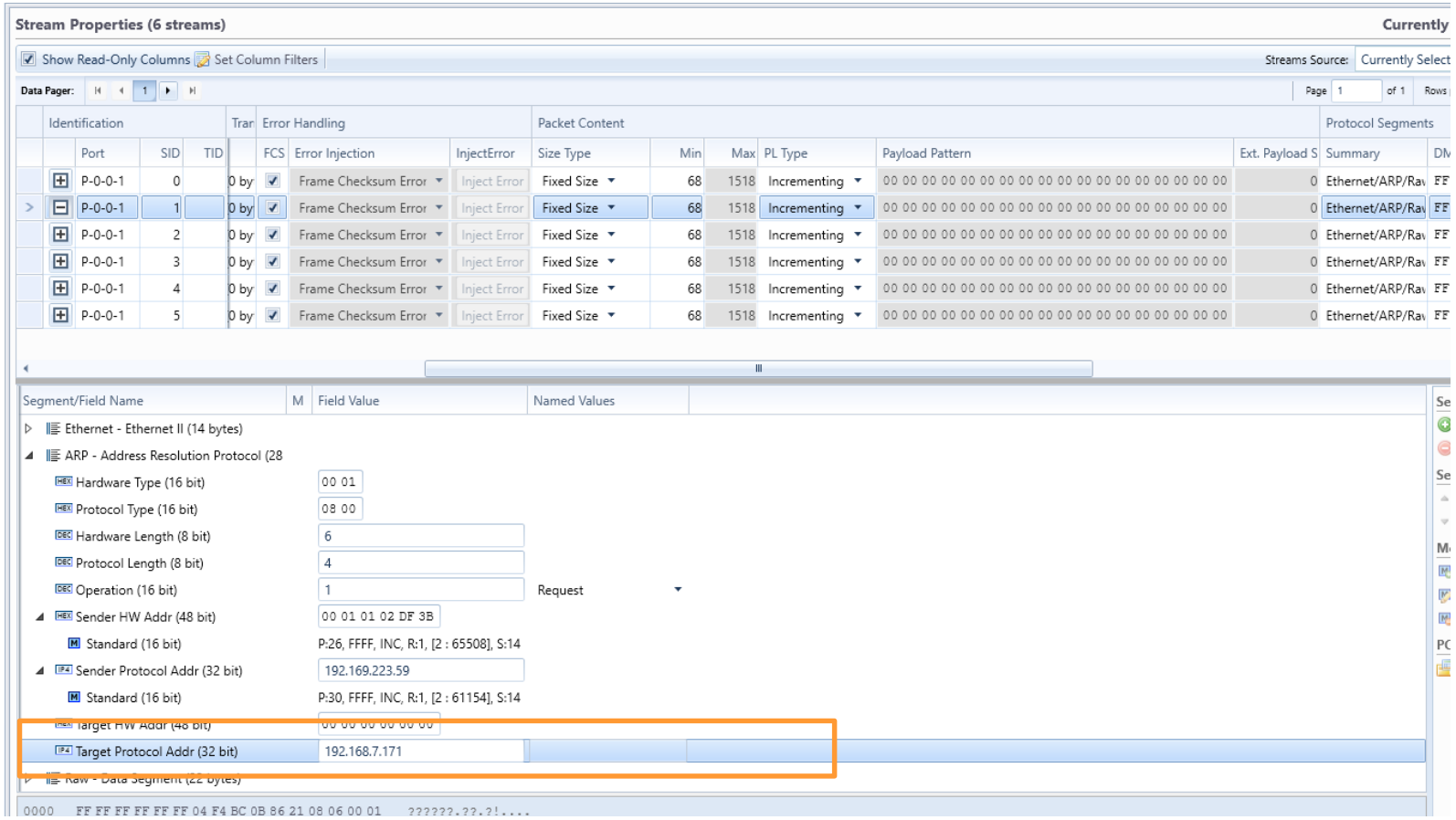
4. Set ”Step Value” to 14.
5. Set ”Address Offset” to 30.
6. Click “OK”.



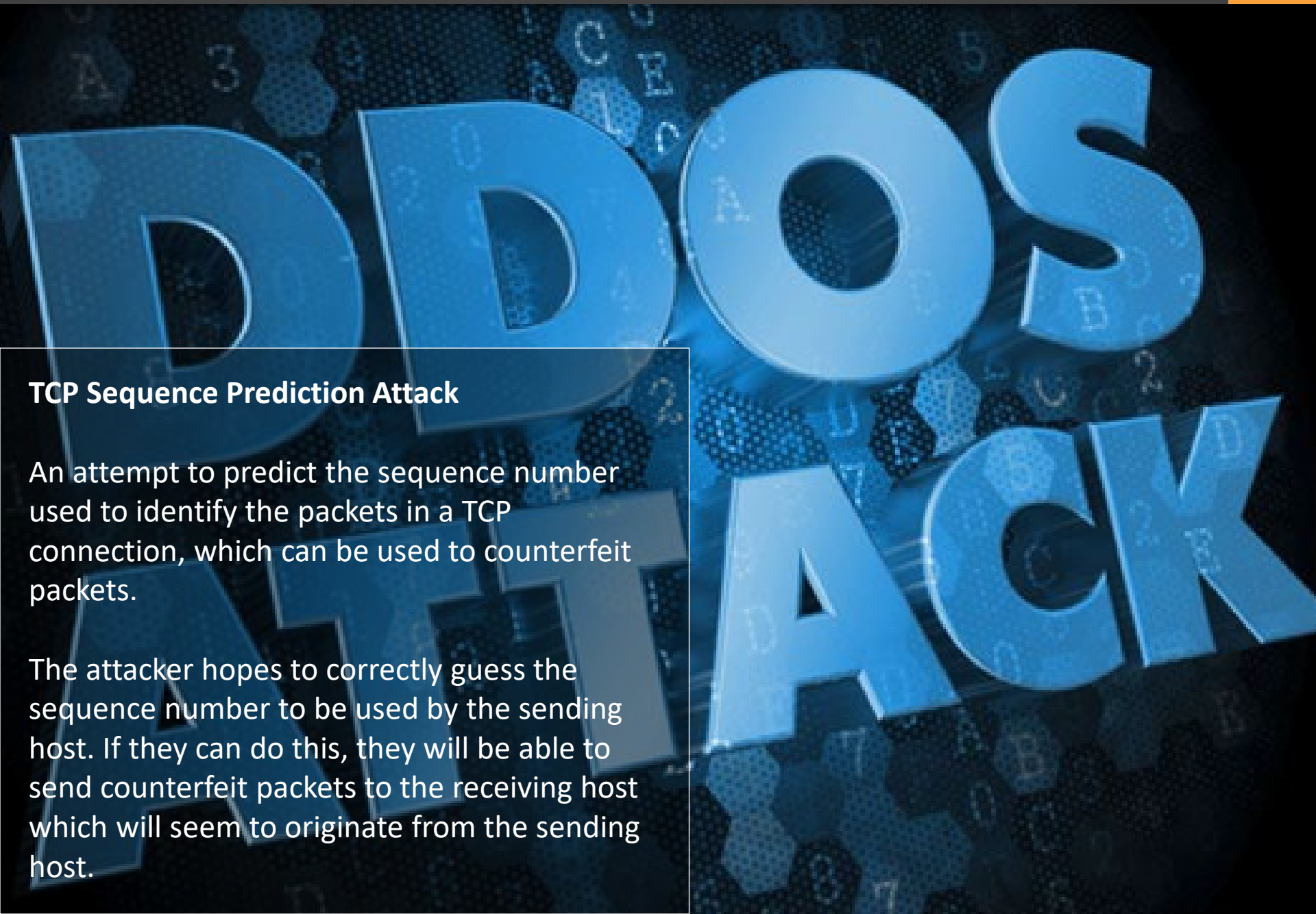


DDoS – ARP SPOOFING

1 Repeat the previous steps, you can add as many stream as you want.
Remember to change the “Target Protocol Addr” to a different address.



DDoS – TCP SEQUENCE PREDICTION ATTACK



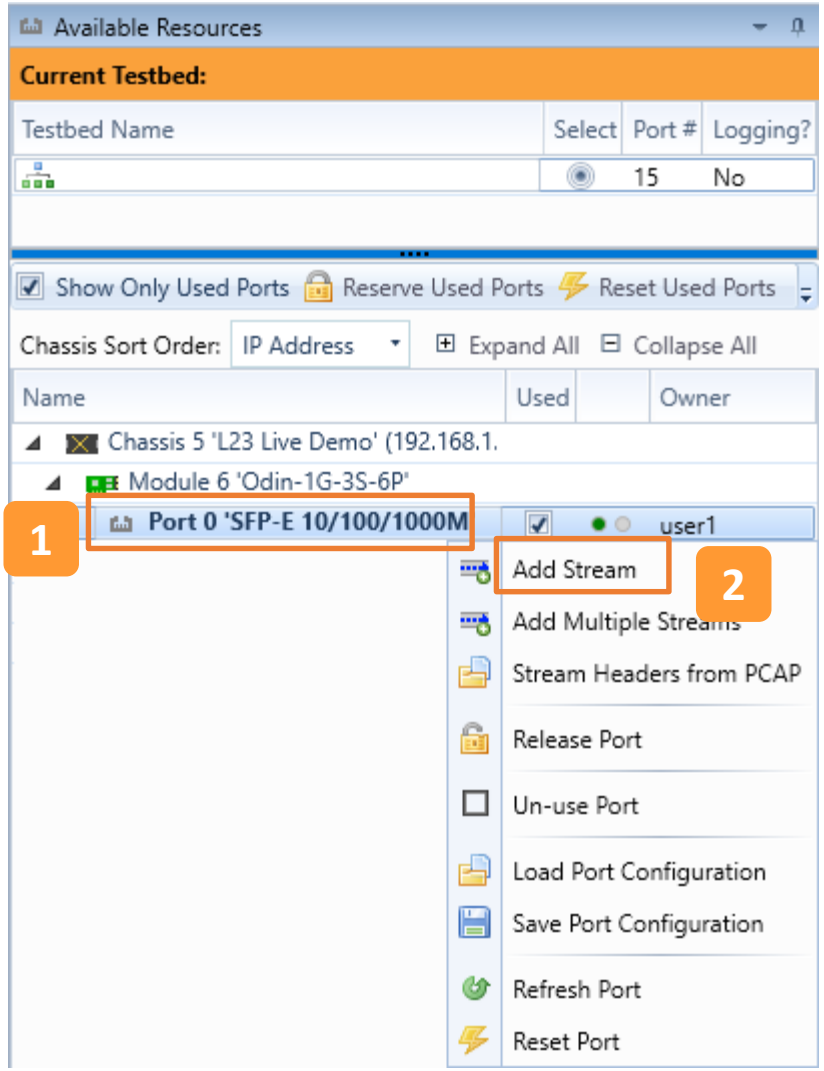
TCP Sequence Prediction Attack

An attempt to predict the sequence number used to identify the packets in a TCP connection, which can be used to counterfeit packets.

The attacker hopes to correctly guess the sequence number to be used by the sending host. If they can do this, they will be able to send counterfeit packets to the receiving host which will seem to originate from the sending host.

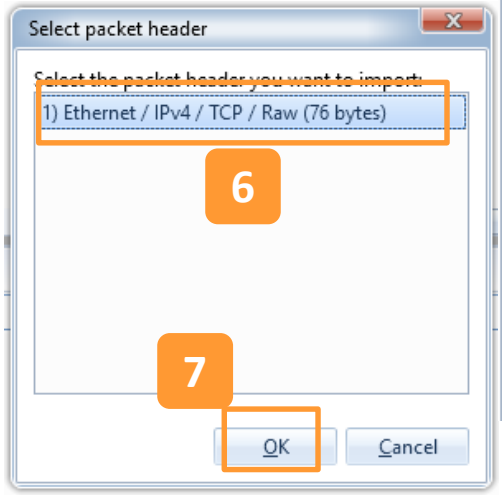
DDoS – TCP SEQUENCE PREDICTION ATTACK

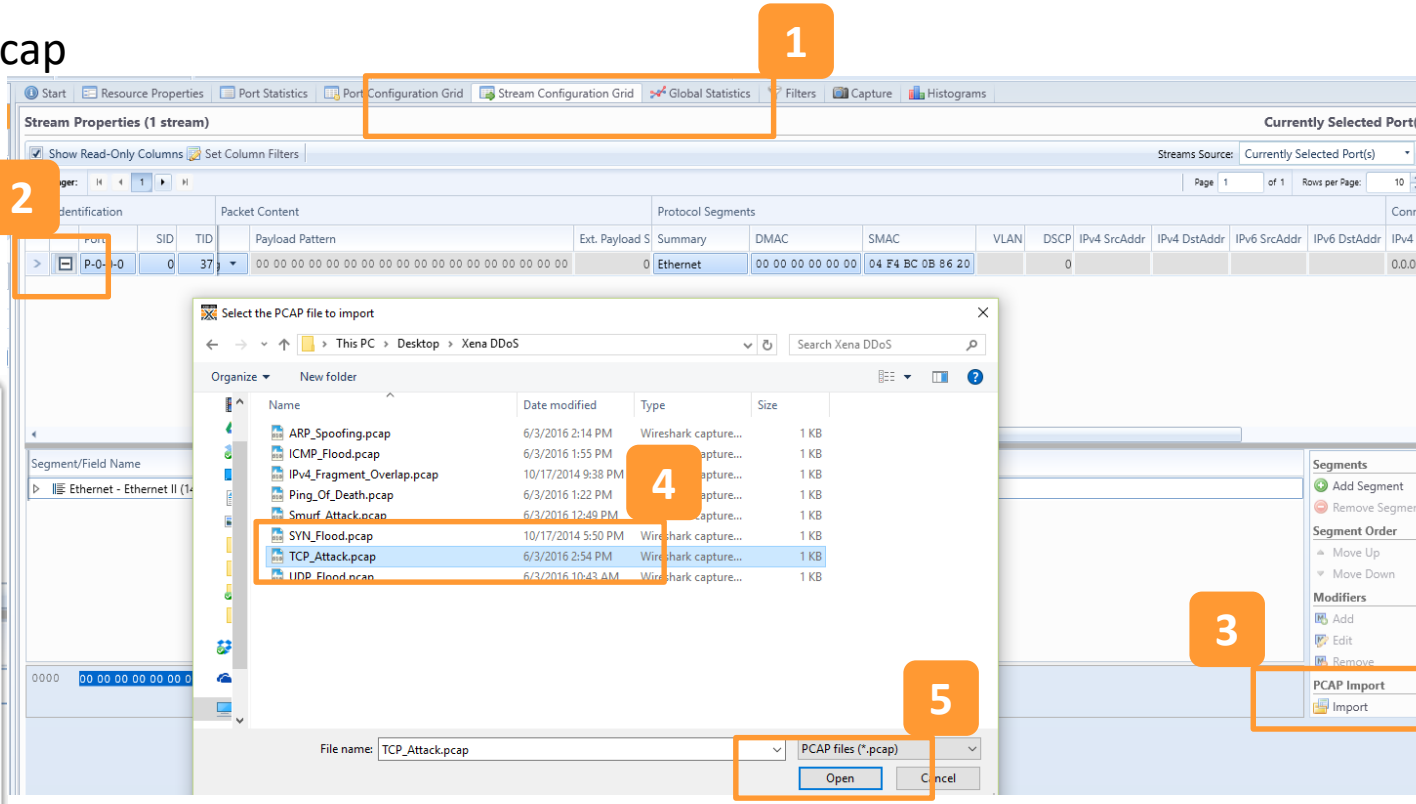
1. Right-click on Attacking port.
2. Click “Add Stream”



DDoS – TCP SEQUENCE PREDICTION ATTACK

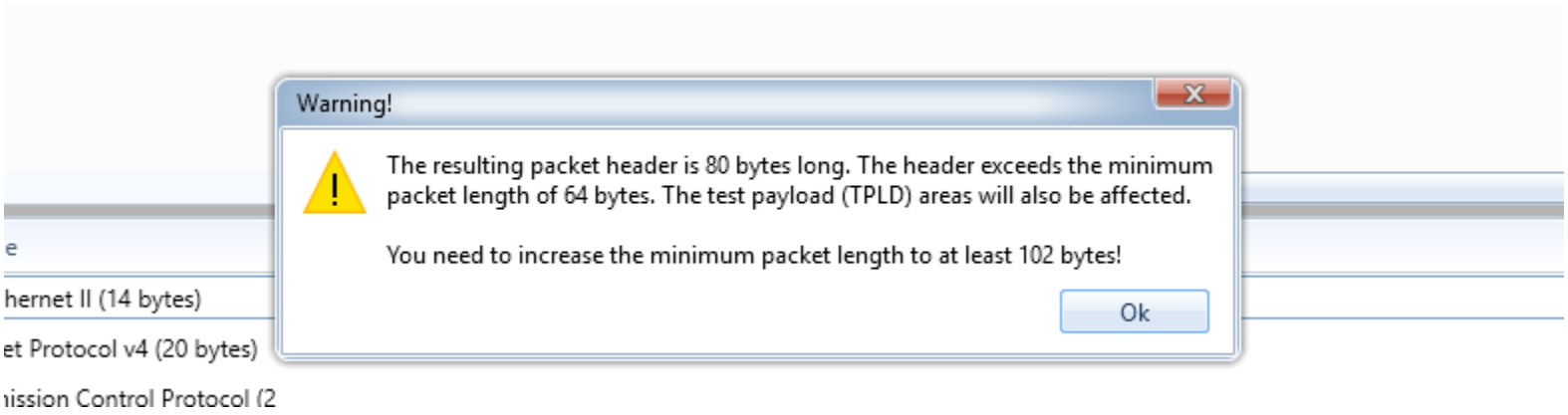
1. Go to “Stream Configuration Grid” tab.
2. Click “+”.
3. Click “Import”
4. Select TCP_Attack.pcap
5. Click “Open”
6. Click First row
7. Click “OK”

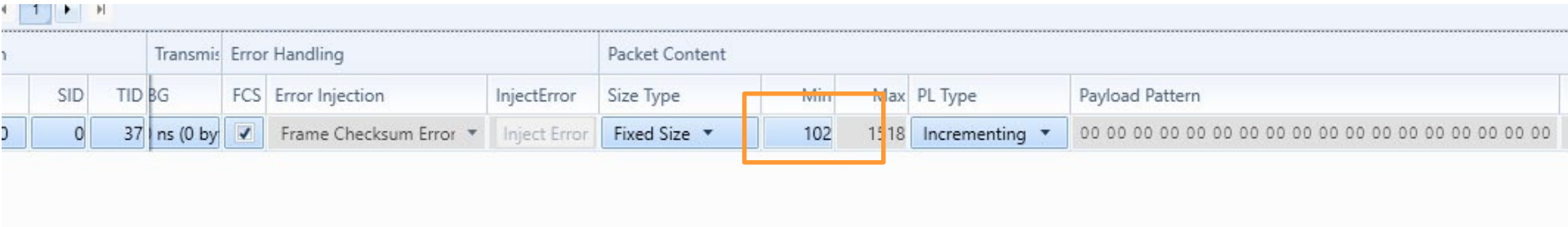




DDoS – TCP SEQUENCE PREDICTION ATTACK

1 You may see the alert telling you to increase the minimum packet length. Change the minimum size to 102 bytes.





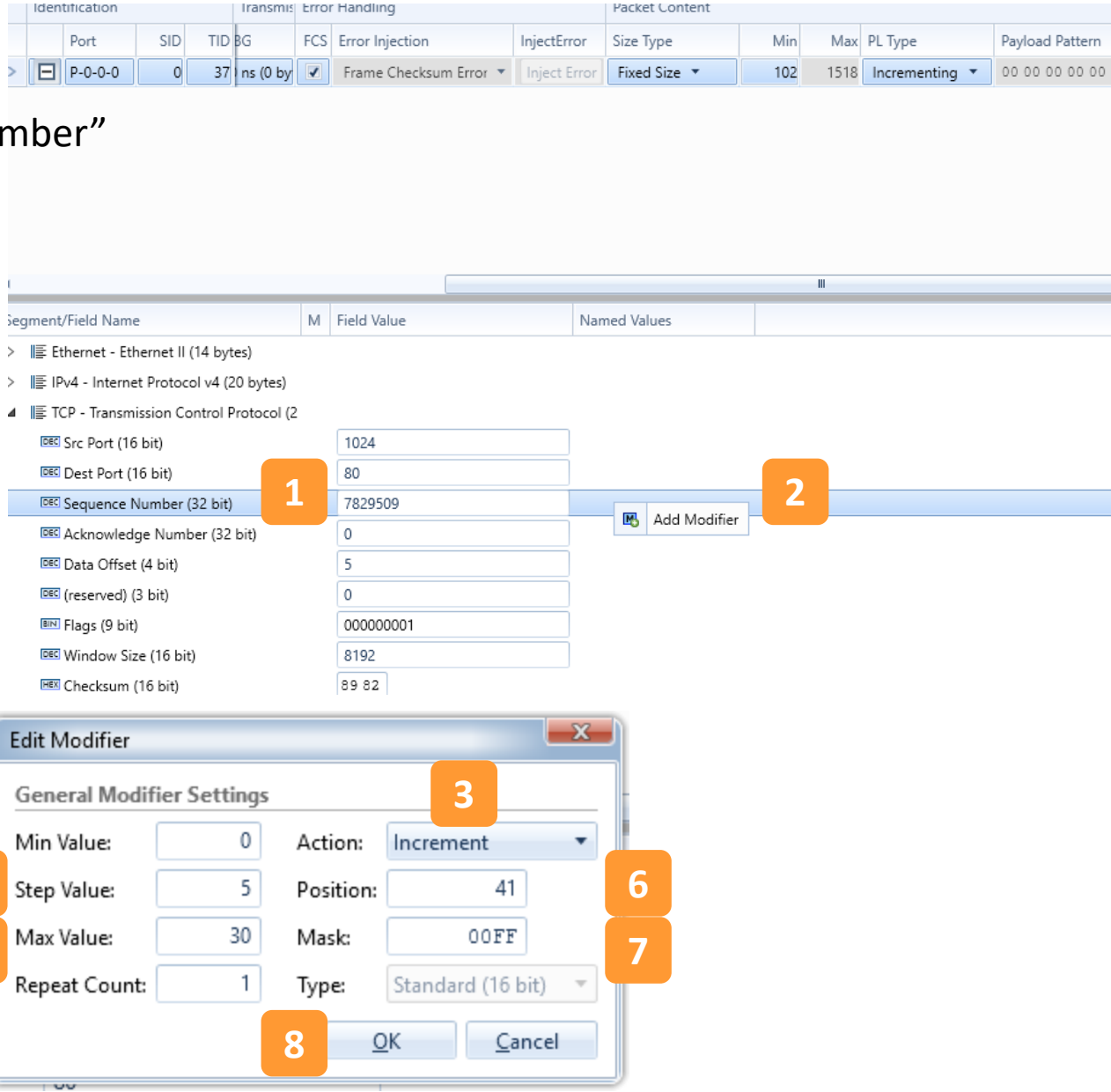
DDoS – TCP SEQUENCE PREDICTION ATTACK

Increase TCP Sequence Number

1. Right click on “Sequence Number”
2. Click “Add Modifier”
3. Select Action

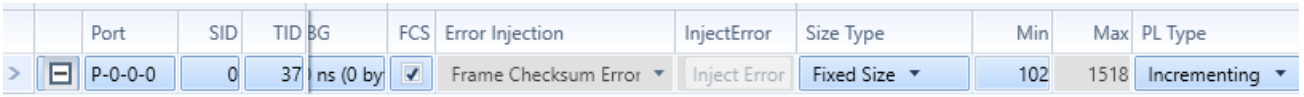
(Increment Recommended)

4. Set ”Step Value” to 5.
5. Set ”Max Value” to 30.
6. Set ”Position” to 41.
7. Set ”Mask” to 00FF.
8. Click “OK”.



DDoS – TCP SEQUENCE PREDICTION ATTACK

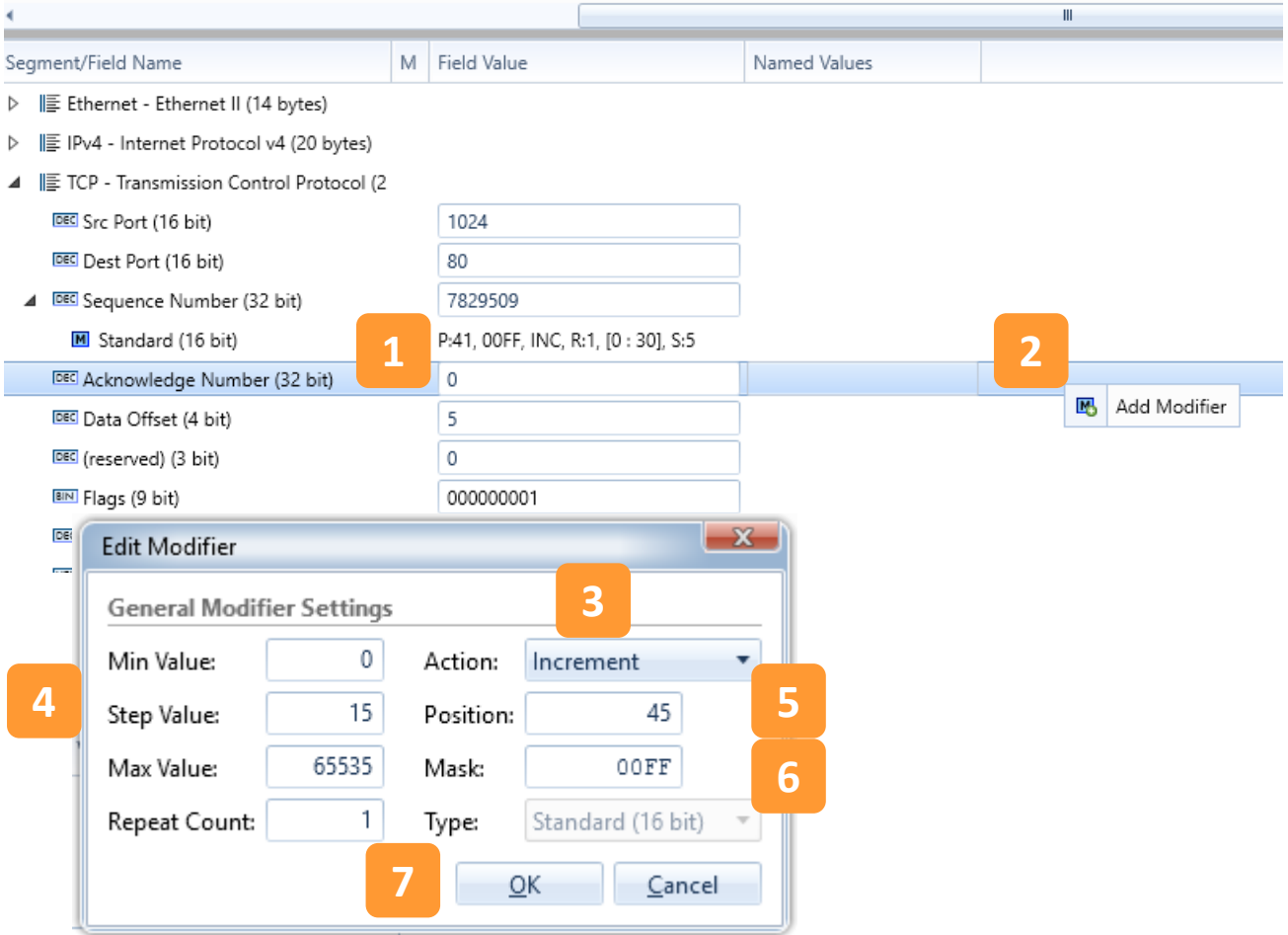
Increase TCP ACK Number



1. Right click on “Acknowledge Number”
2. Click “Add Modifier”
3. Select Action

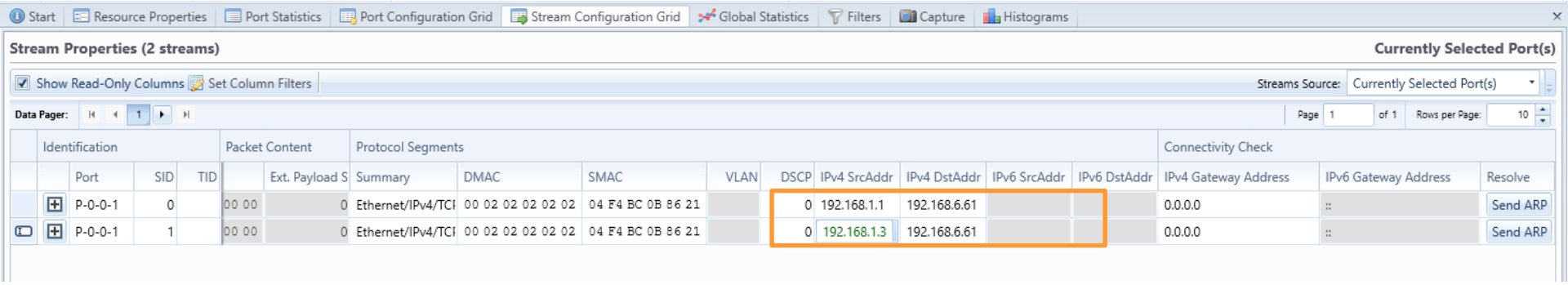
(Increment Recommended)

4. Set ”Step Value” to 5.
5. Set ”Position” to 45.
6. Set ”Mask” to 00FF.
7. Click “OK”.



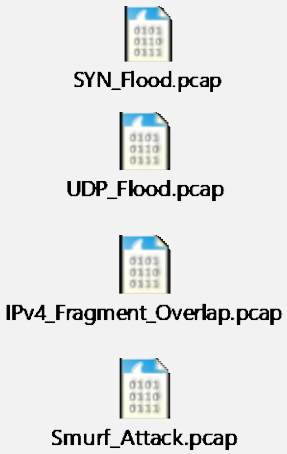
DDoS – TCP SEQUENCE PREDICTION ATTACK

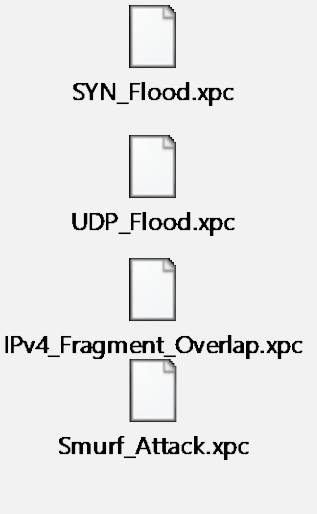
1 Repeat the previous steps, you can add as many stream as you want.
Remember to change the “Target Protocol Addr” to a different address.



DDoS – PCAP FILES

1 Attached:





Please also visit DDOS section of https://xenanetworks.com/other-downloads/

2 For additional Attacks/Malware traffic captures:

NETRESEC www.netresec.com/?page=PcapFiles

WANT MORE INFORMATION?

Visit our website:

www.xenanetworks.com

Contact us:

support@xenanetworks.com