

APPLICATION NOTE

PCAP Replay

Reproduce your own reality with Vulcan PCAP Replay

How to capture traffic into PCAP files and replay on Xena's Vulcan traffic generation & analysis platform to reproduce your own reality for stateful performance verification.



Contents

Application Note
Capture Real-World Traffic Into PCAP 4
Launch Wireshark4
Get Ready With the Application5
Select Interface and Capture5
Select the Traffic You Want to Replay7
Make PCAP Comforming to Xena REplay Rules10
Use PCAP File for Replay 11
Create Relay Scenario
Scale Your Traffic12
Compose Your Own Playlist with Multiple PCAP Files13
Loop Your PCAP14
Things You Should Know About Xena PCAP Replay15
Payload Replay15
Preserved Payload
New Connection
Reliable Delivery15
Congestion Control
TCP and UDP Replay15
Replay with Speed-Up or Slow-Down15



APPLICATION NOTE

Stateful PCAP replay is an effective way to reproduce reality to your system under test and test the behaviors of your devices that are not visible with modeled traffic. Vulcan's advanced Layer 4 replay provides a platform to replay your own PCAP with flexibility and scalability. In case of packet loss by the network, which is a normal behavior of any IP networks, Vulcan's stateful TCP stack makes sure that the information delivery is reliable by means of TCP retransmission. Adaptive congestion control can be enabled with the measurement of round-trip latency between the client and the server.

This application note describes how to make your or PCAP file that conform to Vulcan's replay engine, and how to use Vulcan's replay scenario to scale up the traffic for high-performance testing.



CAPTURE REAL-WORLD TRAFFIC INTO PCAP

The simplest way to quickly generate a PCAP file is to use a network traffic analysis software, e.g. Wireshark, or other similar tools. We will use Wireshark in this section to demonstrate how to capture the traffic we want to replay.

This section will describe how to capture traffic into a PCAP file using Wireshark. In-depth use of Wireshark is out of the scope of this section. For more on how to use Wireshark, please refer to https://www.wireshark.org

LAUNCH WIRESHARK

Launch Wireshark and you should see the window as shown Figure 1. On this window, you are presented with options to select from which network interface you would like to capture traffic. Figure 1 shows that there are two network interfaces on the demo PC, Ethernet and Wi-Fi. The activity indicators show whether there is any traffic on that interface. You can see that the Wi-Fi interface is active while the Ethernet interface shows no traffic. Thus, we will use the Wi-Fi interface to capture traffic.

a 🚄 The Wireshark Network Analyzer	– 🗆 X
Eile Edit View Go Capture Analyze Statistics Telephony Wireless Iools Help	
▲ ■ Q Q Q 🔤 🖉 🐵 🕾 🕾 🛬 🧮 Q Q Q 🕮	
Apply a display filter <ctrl-></ctrl->	Expression +
Welcome to Wireshark	
Capture	
using this filter: 📗 Enter a capture filter	
Ethernet	
WIFT Mululum under	
1 ann	
Users source ' Wiki ' Questionis and Answers' ' training Lists Viu are numini Micrebark' 2 5 for / 2 5-for 23/do-53 You reveals a utomatic undates	
rectar taining michain Lizio ("Lizio o graduccuji tou tecche distuninge dybutesi	
Ready to load or capture No Packets	Profile: Default

Figure 1. Launch Wireshark



GET READY WITH THE APPLICATION

Before capturing traffic, you should have an idea what to capture. If you want to capture traffic from YouTube, you should launch your web browser and prepare to enter the URL. If you want to capture traffic from Netflix, you should have the program ready.

Preparing the application, you want to capture traffic from, before starting Wireshark is a good practice because once you start capturing, packets will pour into the buffer and it might affect the performance of your PC. Thus, get things ready in advance will save you some effort from struggling with a slow computer.

SELECT INTERFACE AND CAPTURE

Once you think the application you want to capture traffic from is ready, you can begin to initiate the capture. As shown in Figure 2, select the interface and then click the "Start capturing packets" button.

A	
I he Wireshark Network Analyzer	— — ;
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help	
Apry a display filter <ctrl-></ctrl->	Expression
Welcome to Wireshark	
Cambrid	
Capture	
using this filter: 📕 Enter a capture filter	¥
cunernet	
Wi-Fi	/\
Learn	
User's Guide · Wiki · Questions and Answers · Mailing Lists	
You are running Wireshark 2.2.6 (v2.2.6-0-g32dac6a). You receive automatic u	odates.
Ready to load or capture	No Packets Profile: Default

Figure 2. Select the interface and start capturing packets

As soon as you start the capture, you will see packets being shown in the program window. At this time, you can start your application and all the traffic between your PC and the server will be recorded, as shown in Figure 3.



🙍 Capt	uring from Wi-Fi						-	- 0	×
<u>F</u> ile <u>E</u> d	lit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> ta	atistics Telephon <u>y W</u> ireless	<u>T</u> ools <u>H</u> elp						
<u> </u>	፩ : 🖲 🔝 🕅 🗖 🔍 ⇔ 👄 ≦	🛎 🗿 👲 🚍 📃 O. Q. (ə, 🎹						
Apply	a display filter <ctrl-></ctrl->							Expression	. +
No.	Time	Source	Src Port	Destination	Dst Port	Length Host		Protocol	^
175	8.248469000	31.13.72.14	443	192.168.1.63	55178	1464		TCP	
175	6 8.248470000	31.13.72.14	443	192.168.1.63	55178	1464		TLSv1.2	
• 175	8.248471000	31.13.72.14	443	192.168.1.63	55178	1464		TCP	
175	8.248471000	31.13.72.14	443	192.168.1.63	55178	1464		TCP	
175	9 8.248472000	31.13.72.14	443	192.168.1.63	55178	1464		TCP	
176	8.248581000	192.168.1.63	55178	31.13.72.14	443	54		TCP	
• 176	8.249415000	31.13.72.14	443	192.168.1.63	55178	1464		TCP	
• 176	8.249415000	31.13.72.14	443	192.168.1.63	55178	1464		TLSv1.2	
176	8.249416000	31.13.72.14	443	192.168.1.63	55178	1464		TCP	
176	8.249417000	31.13.72.14	443	192.168.1.63	55178	1464		TLSv1.2	
176	5 8.249418000	31.13.72.14	443	192.168.1.63	55178	1464		TLSv1.2	
176	6 8.249418000	31.13.72.14	443	192.168.1.63	55178	1464		TLSv1.2	
176	8.249419000	31.13.72.14	443	192.168.1.63	55178	1464		TCP	
176	8.249419000	31.13.72.14	443	192.168.1.63	55178	1464		TCP	~
<									>
> Fra	me 1762: 1464 bytes on wi	re (11712 bits), 14	64 bytes	captured (11712 bit	s) on int	erface 0			^
> Ethe	ernet II, Src: Routerbo_3	3:1e:64 (d4:ca:6d:3	3:1e:64),	Dst: 3a:8d:e6:2c:6	5c:5c (3a:	8d:e6:2c:6c:5c)		
> Inte	ernet Protocol Version 4,	Src: 31.13.72.14,	Dst: 192.	168.1.63					
> Trai	nsmission Control Protoco	1, Src Port: 443, D	st Port:	55178, Seq: 79000,	Ack: 2085	, Len: 1410			
> [6	Reassembled TCP Segments	(8029 bytes): #1756	(1360), #	1757(1410), #1758(1	410), #17	59(1410), #176	1(1410), #1762(1029)]	~
0000	3a 8d e6 2c 6c 5c d4 ca	6d 33 1e 64 08 00	45 00	:1\ m3.dE.					^
0010	05 aa 20 3e 40 00 5a 06	d2 0d 1f 0d 48 0e	c0 a8	>@.ZH					
0020	01 3f 01 bb d7 8a 30 8f	db 0f 3a c7 0a 8b	50 10	.?					
0030	00 8c bc 97 00 00 79 86	79 82 0a 46 ed 75	43 33	y. yF.uC3					
0040	39 09 ca 11 80 70 bf 48	07 3b e5 a3 b4 16	2d 83	9р.Н .;					
0050	87 a8 f1 f6 c0 32 02 d8	0b e8 4e 44 09 97	a0 80	2ND					
0060	7f 25 29 16 24 94 d4 53	a8 f6 df 16 16 ec	51 f2	.%).\$SQ.					
0070	7b 38 6c 96 0c 8c ee 53	1d 23 b1 a3 8f 50	d1 1a	{81S .#P					
0080	8t a1 26 2d 77 43 9c c5	ce t6 38 tb d5 81	ed 9a	&-wC8					
6090 Erama (1	11 ao Do co ao 1a do 2o		1a 62	b					~
	Wi-Fit < live canture in progress >)			П	Packets: 3824 · Displayed	3824 (100.0%)	Profile: Def	fault
	with sive capture in progression					rucketa, Jozi – Diapidyeu	502 (100/0 /0)	Frome: Del	uult .:





SELECT THE TRAFFIC YOU WANT TO REPLAY

When you have captured the traffic you want, you can stop capturing by clicking the red "stop" button.

There will be many packets from different applications in Wireshark. This is simply because your PC runs not only the application you want, but also many other applications (visible or hidden) that you may not notice. If your Wireshark is in promiscuous mode, it may also capture broadcast packet such as ARP.

You need to filter out the traffic/sessions you want to replay from the mess. Click Statistics tab and go to Conversation, as shown in Figure 4.

Wr.fi - □ × He Edit View Go Capture Analyce Statistics Telephory Wireless Tools Help No. The Edit View Go Capture Analyce Capture File Propertie Cut-Ah-Shit-C No. The Edit View Go Capture Analyce Capture File Propertie Cut-Ah-Shit-C No. The Statistics Telephory Wireless Tools Help Potocol Potocol S225 12.4093411060 Conversations File Edit View Go Capture Analyce Potocol S226 12.4093106060 Potocol Potocol Potocol Potocol S326 12.4093106060 Potocol Potocol Potocol Potocol Potocol S329 12.415251060 Potocol	· · · · · · · · · · · · · · · · · · ·				
File Edit View Go Capture Andres Builtitis Telephony Wirdless Tools Help Image: Capture Andres Builtitis Telephony Wirdless Tools Help Capture Allery A	🚄 *Wi-Fi				- 🗆 ×
Image: Solution of the sector of the sec	File Edit View Go Capture Analyze	Statistics Telephony Wireless Tools Hel	p		
Image: No. The method Addresses Produced Hearchy Produced Hearchy 3525 12.409311000 Endpoints 31.13.72.37 443 180 TLSv1.7 3526 12.40931000 Endpoints 31.13.72.37 443 180 TLSv1.7 3528 12.409390000 Brack telength 31.13.72.37 443 180 TLSv1.7 3529 12.409390000 Service Response Time 31.13.72.37 443 96 TLSv1.7 3530 12.41525000 DHCP (BOTP) Statics 00K-BPC Programs 31.13.72.37 443 97 TLSv1.7 3533 12.415250000 DHCP (BOTP) Statics 00K-BPC Programs 31.13.72.37 443 92 TLSv1.7 3533 12.438705000 AKP 31.13.72.37 443 92 TLSv1.7 3535 12.438705000 ONS 13.13.72.37 443 92 TLSv1.7 3535 12.438705000 ONS 13.13.72.37 443 92 TLSv1.7 3537 12.4388704000 Caleed 192.168.1.63 S5182 92 TLSv1.7	🚄 🔳 🖉 💿 📙 🔚 🗙 🖨 🔍 👄 🖷	Capture File Properties Ctrl+Alt+Shift+	c		
No. Time Potocol Herarchy 3525 12.4093410000 Conversations 31.13.72.37 443 180 TLSV1.2 3526 12.409129000 Packet lengths 31.13.72.37 443 100 TLSV1.2 3527 12.409129000 Packet lengths 31.13.72.37 443 100 TLSV1.2 3528 12.409129000 Service Respons Time 31.13.72.37 443 96 TLSV1.2 3529 12.409336000 Service Respons Time 31.13.72.37 443 979 TLSV1.2 3531 12.415520000 OHCP (BOOTP) Statistics 00C-RPC Programs 192.168.1.63 55182 112 TLSV1.2 3533 12.438704000 BACnet 192.168.1.63 55182 92 TLSV1.2 3535 12.438704000 BACnet 192.168.1.63 55182 92 TLSV1.2 3536 12.438704000 DNS 131.13.72.37 443 54 TCP 3536 12.438704000 DNS 131.13.72.37 443 54 TCP 3537 12.43817000 DNS	Apply a display filter <ctrl-></ctrl->	Resolved Addresses			Expression +
3525 12.403411000 Conversions 3526 12.409320000 Endpoints 3527 12.409320000 Findpoints 3528 12.409320000 Service Response Time 3529 12.409320000 Service Response Time 3530 12.415251000 DHC (BOOTP) Statistics 010C-RPC Programs 13.13.72.37 443 100 3533 12.415251000 DHC (BOOTP) Statistics 192.168.1.63 55182 132 3533 12.41525000 DHC-RPC Programs 192.168.1.63 55182 135 TLSv1.2 3534 12.438299000 BACnet 192.168.1.63 55182 135 TLSv1.2 3535 12.43870600 DHKP 31.13.72.37 443 54 TCP 3535 12.43870600 BACnet 192.168.1.63 55182 92 TLSv1.2 3536 12.438870600 DHS 31.13.72.37 443 54 TCP 3537 12.4388170600 DHS 31.13.72.37 443 54 TCP 3538 12.45184040 DHS 31.13.72.37	No. Time	Protocol Hierarchy	Destination Dst Port	Length Host	Protocol
5526 12.409067080 Indpoints 31.13.72.37 443 107 TLSv1.2 3527 12.409126800 Packet Lengths 31.13.72.37 443 100 TLSv1.2 3528 12.409396000 Service Response Time 31.13.72.37 443 96 TLSv1.2 3530 12.415252000 Service Response Time 31.13.72.37 443 979 TLSv1.2 3531 12.415252000 OHCP (BODP) Statistics 00C-RPC Programs 31.13.72.37 443 94 TLSv1.2 3532 12.415350000 ANCP 31.13.72.37 443 54 TCP 3533 12.415379000 ANCP 31.13.72.37 443 54 TCP 3534 12.438796900 Collectd 192.168.1.63 55182 92 TLSv1.2 3535 12.438706900 DNS 131.13.72.37 443 54 TCP 3536 12.438706900 DNS 131.13.72.37 443 54 TCP 3537 12.43817060 DNS 131.32.72.37 443 54 TCP 3538	3525 12.403411000	Conversations	31.13.72.37 443	180	TLSv1.2
3527 12.409129800 Packet Lengths 31.13.72.37 443 100 TLSv1.2 3528 12.409168000 Backet Lengths 31.13.72.37 443 96 TLSv1.2 3529 12.409268000 Backet Lengths 31.13.72.37 443 96 TLSv1.2 3530 12.415252000 DHCP (800TP) Statistics 0NC-RPC Programs 31.13.72.37 443 92 TLSv1.2 3533 12.415552000 ANCP 31.13.72.37 443 92 TLSv1.2 3534 12.4382704000 ANCP 31.13.72.37 443 92 TLSv1.2 3535 12.438705000 ANCP 31.13.72.37 443 92 TLSv1.2 3536 12.438705000 Colectd 192.168.1.63 55182 92 TLSv1.2 3537 12.438170600 NS 51.13.72.37 443 54 TCP 3538 12.463108000 Colectd 192.168.1.63 55182 92 TLSv1.2 3538 12.463108000 Sisson Control Proto Sisson Control Proto Sisson Control Proto Sist 3a:8d:e6:2c:6c:5c (3a:8d	3526 12.409007000	Endpoints	31.13.72.37 443	107	TLSv1.2
3528 12.409168000 VO Graph 31.13.72.37 443 96 TLSv1.2 3530 12.415525000 Bervice Response Time 31.13.72.37 443 979 TLSv1.2 3531 12.415525000 DHC (BOOTP) Statistics 000 32.12.157.12 132.168.1.63 55182 312 3533 12.41579000 AKCP 31.13.72.37 443 92 TLSv1.2 3534 12.43879000 BACnet 31.13.72.37 443 54 TCP 3535 12.43879000 BACnet 192.168.1.63 55182 92 TLSv1.2 3536 12.43878000 DNS 13.13.72.37 443 54 TCP 3536 12.43878000 DNS 13.13.72.37 443 54 TCP 3537 12.438817000 DNS 13.13.72.37 443 54 TCP 3538 12.43878000 DNS 13.13.72.37 443 54 TCP 31.13.72.37 443 54 TCP 159.16 160 TLSv1.2 3536 12.43878000 DNS <	3527 12.409129000	Packet Lengths	31.13.72.37 443	110	TLSv1.2
3529 12.499396000 serice Response Time → 31.13.72.37 443 979 TLSv1.2 3531 12.415252000 ONC-RPC Programs 31.13.72.37 443 943 512 3532 12.415334000 ONC-RPC Programs 31.13.72.37 443 943 TLSv1.2 3533 12.43579000 ANCP 31.13.72.37 443 94 TLSv1.2 3534 12.438704000 BACnet + 31.13.72.37 443 54 TCP 3536 12.438704000 BACnet + 192.168.1.63 55182 96 TLSv1.2 3537 12.438817000 DNS 31.13.72.37 443 54 TCP 3538 12.438704000 DNS 31.13.72.37 443 54 TCP 3537 12.438817000 DNS 31.13.72.37 443 54 TCP 3538 12.438704080 DNS 31.13.72.37 443 54 TCP 400 DNS 31.13.72.37 443 54 TCP TLSv1.2 3537 12.438704080	3528 12.409168000	I/O Graph	31.13.72.37 443	96	TLSv1.2
3530 12.415251000 DHCP (800TP) Statistics 192.168.1.63 55182 312 TLSv1.2 3531 12.41552000 ONC-RPC Programs 31.13.72.37 443 54 TCP 3533 12.415579000 ANCP 31.13.72.37 443 54 TCP 3535 12.438704000 BACnet 192.168.1.63 55182 92 TLSv1.2 3536 12.438704000 Collectd 192.168.1.63 55182 92 TLSv1.2 3537 12.438817000 ONS 31.13.72.37 443 54 TCP 3538 12.438705000 ONS 31.13.72.37 443 54 TCP 3538 12.438817000 DNS 31.13.72.37 443 54 TCP 3538 12.438817000 DNS 31.13.72.37 443 54 TCP 3538 12.458170800 DNS 31.13.72.37 443 54 TCP 3536 12.438817000 DNS 31.13.72.37 443 54 TCP 3537 12.43881700 DNS 31.13.72.37 <td< td=""><td>3529 12.409396000</td><td>Service Response Time</td><td>▶ 31.13.72.37 443</td><td>979</td><td>TLSv1.2</td></td<>	3529 12.409396000	Service Response Time	▶ 31.13.72.37 443	979	TLSv1.2
3531 12.415252000 DNC.PBC Programs 192.168.1.63 55182 135 TLSv1.2 3533 12.415530400 2West 31.13.72.37 443 92 TLSv1.2 3534 12.43579000 ANCP 31.13.72.37 443 92 TLSv1.2 3534 12.438704000 BACnet 192.168.1.63 55182 92 TLSv1.2 3535 12.438704000 BACnet 192.168.1.63 55182 92 TLSv1.2 3536 12.438704000 BACnet 192.168.1.63 55182 92 TLSv1.2 3537 12.43817000 DNS 31.13.72.37 443 54 TCP 3538 12.438704000 BACnet 192.168.1.63 55182 92 TLSv1.2 3538 12.43870400 DNS 31.13.72.37 443 54 TCP 3537 12.43817000 DNS 31.13.72.37 443 54 TCP 3538 12.6210800 PNS TISv1.2 TSV1.2 TSV1.2 TSV1.2 17.8 Feame 1762: 1464 bytes on HTFP St	3530 12.415251000		192.168.1.63 55182	312	TLSv1.2
3532 12.415334000 DVK-tP0 programs 3533 12.415579000 29Wet > 3534 12.430299000 ANCP 31.13.72.37 443 54 TCP 3534 12.430299000 BACnet > 192.168.1.63 55182 92 TLSv1.2 3535 12.438705000 Collecti 93.113.72.37 443 54 TCP 3537 12.438817000 DNS 91.168.1.63 55182 92 TLSv1.2 3538 12.463108000 Fow Graph HART.P HHEEDS HHEEDS HHEEDS HHEEDS HHEEDS HHEEDS HHEEDS HHEEDS HUDP Multicat Streams 178.58cq 79000, Ack: 2085, Len: 1410 TCP N 3600 36 de 2 dc 5 c 5 c d4 HDP Multicat Streams ,1,	3531 12.415252000	DHCP (BOOTP) Statistics	192.168.1.63 55182	135	TLSv1.2
3533 12.415579000 29Wett ANCP 3534 12.4380299000 BACnet 31.13.72.36 443 54 TCP 3535 12.438704000 BACnet 192.168.1.63 55182 92 TLSv1.2 3537 12.438817000 DNS 192.168.1.63 55182 96 TLSv1.2 3538 12.438817000 DNS 13.13.72.37 443 54 TCP 3537 12.438817000 DNS 13.13.72.37 443 54 TCP 3538 12.438817000 DNS 13.13.72.37 443 54 TCP 3538 12.438817000 DNS 13.13.72.37 443 54 TCP 92.168.1.63 55182 96 TLSv1.2 12.13.72.37 443 54 TCP 92.168.1.63 55185 196 TLSv1.2 192.168.1.63 55182 96 TLSv1.2 93 TLSv1.2 TLSv1.2 TLSv1.2 TLSv1.2 11.13.72.37 443 54 TCP 93 TLSv1.2 TLSv1.2 TLSv1.2 TLSv1.2	3532 12.415334000	ONC-RPC Programs	31.13.72.37 443	54	TCP
3534 12.4380299000 ANCP 31.13.72.36 443 54 TCP 3535 12.438704000 BACnet 192.168.1.63 55182 92 TLSv1.2 3536 12.438704000 BACnet 192.168.1.63 55182 96 TLSv1.2 3537 12.438704000 DNS 11.13.72.36 443 54 TCP 3538 12.438704000 DNS 11.13.72.36 443 54 TLSv1.2 3538 12.438704000 DNS 11.13.72.36 443 54 TCP 3538 12.438704000 DNS 11.13.72.37 443 54 TCP 3538 12.438705000 DNS 11.13.72.36 443 54 TCP 3537 12.438817060 DNS 11.13.72.37 443 54 TCP 3538 12.43870400 DNS 11.13.72.36 443 54 TCP 1709 HATLP HATLP HATLP HATLP HATLP HATLP HATLP St: 38:812:6:6:2:6:5:C St: 38:81:6:6:2:6:5:C St: 38:81:6:6:2:6:5:C St: 38:81:6:6:2:6:5:	3533 12.415579000	29West	31.13.72.37 443	92	TLSv1.2
3535 12.438704000 BACnet 192.168.1.63 55182 92 TLSv1.2 3536 12.438705000 Collectd 192.168.1.63 55182 96 TLSv1.2 3537 12.4387075000 DNS 31.13.72.37 443 54 TCP 3538 12.4387075000 DNS 31.13.72.37 443 54 TCP 3538 12.4380765000 DNS 192.168.1.63 55165 1464 TCP 3537 12.4380765000 DNS 31.13.72.37 443 54 TCP 3536 12.438076500 DNS 192.168.1.63 55165 1464 TCP 3537 12.438076500 HITP + st: 3a:8d:e6:2c:6c:5c (3a:8d:e6:2c:6c:5c) > > > 3536 166 Sametime TCP Steeme Graphs - + + + + >	3534 12.430299000	ANCP	31.13.72.36 443	54	ТСР
3536 12.438705000 Collectd 192.168.1.63 55182 96 TLSv1.2 3537 12.438817000 DNS 31.13.72.37 443 54 TCP > Frame 1762: 1464 bytes on HART-P HART-P 192.168.1.63 55165 1464 TCP > > Frame 1762: 1464 bytes on HPFEEDS ptured (11712 bits) on interface 0 > <td< td=""><td>3535 12.438704000</td><td>BACnet</td><td>192.168.1.63 55182</td><td>92</td><td>TLSv1.2</td></td<>	3535 12.438704000	BACnet	192.168.1.63 55182	92	TLSv1.2
3537 12.438817000 3538 12.463108000 Frame 1762: 1464 bytes on Flow Graph Frame 1762: 1464 bytes on HART-IP HART-IP HPFEDS HTTP + St: 3a:8d:e6:2c:6c:5c (3a:8d:e6:2c:6c:5c) Internet Protocol Version HTTP Transmission Control Proto Sametime [6 Reassembled TCP Segment TCP Stream Graphs UDP Multicast Streams UDP Multicast Streams UDP Multicast Streams	3536 12.438705000	Collectd	192.168.1.63 55182	96	TLSv1.2
3538 12.463108000 Flow Graph 192.168.1.63 55165 1464 TCP * 9 Frame 1762: 1464 bytes on HART-IP + HART-IP +	3537 12.438817000	DNS	31.13.72.37 443	54	TCP
HART-IP → Frame 1762: 1464 bytes on HART-IP HPFEEDS → Frame 1762: 1464 bytes on Internet II, Src: Routerbo > Internet Protocol Version HTTP2 Sametime Transmission Control Proto > [6 Reassembled TCP Segment COP00 3a 8d e6 2c 6c 5c d4 0000 3a 8d e6 2c 6c 5c d4 0010 05 aa 20 3e 40 00 5a 0020 01 3f 01 bb d7 8a 30 IPv6 Statistics IVV6 Statistics	3538 12.463108000	Flow Graph	192.168.1.63 55165	5 1464	TCP
> Frame 1762: 1464 bytes on HPFEEDS ptured (11712 bits) on interface 0 ∧ > Ethernet II, Src: Routerbo HTTP , st: 3a:8d:e6:2c:6c:5c (3a:8d:e6:2c:6c:5c) ∧ > Internet Protocol Version HTTP , st: 3a:8d:e6:2c:6c:5c (3a:8d:e6:2c:6c:5c) ∧ > Transmission Control Proto Sametime 178, Seq: 79000, Ack: 2085, Len: 1410 ∧ 0000 3a 8d e6 2c 6c 5c d4 UDP Multicast Streams , 1/\m3.dE. ∧ 0010 05 aa 20 3e 40 00 5a PV4 Statistics ,	×	HART-IP			/
> Ethernet II, Src: Routerbo HTTP + st: 3a:8d:e6:2c:6c:5c (3a:8d:e6:2c:6c:5c) > Internet Protocol Version HTTP + st: 3a:8d:e6:2c:6c:5c (3a:8d:e6:2c:6c:5c) > Internet Protocol Version HTTP + st: 3a:8d:e6:2c:6c:5c (3a:8d:e6:2c:6c:5c) > Internet Protocol Version HTTP + st: 3a:8d:e6:2c:6c:5c (3a:8d:e6:2c:6c:5c) > Internet Protocol Version HTTP + st: 3a:8d:e6:2c:6c:5c (3a:8d:e6:2c:6c:5c) > Internet Protocol Version Sametime 178, Seq: 79000, Ack: 2085, Len: 1410 > [6 Reassembled TCP Segment TP: Statistics + ifts: Seq: 79000, Ack: 2085, Len: 1410 0010 65 aa 20 3e 40 00 5a UDP Multicast Streams + ifts: Maid:e6:2c:6c:5c (3a:8d:e6:2c:6c:5c) 0020 01 3f 01 bb d7 8a 30 IDP Multicast Streams + ifts: Maid:e6:2c:6c:5c (3a:8d:e6:2c:6c:5c) 0030 00 8c bc 97 00 00 79 IDP Multicast Streams + ifts: Maid:e6:2c:6c:5c (3a:8d:e6:2c:6c:5c) 0040 39 09 ca 11 80 70 bf 48 07 3b 5e 3a 3b 416 2d 83 9p.H .; 0 0050 87 a8 16 6 6 d7 16 16 ec 51 f2 %).\$s. c. 0 0060 71 25 29 16 24 94 d4 53 a8 f6 df 16 16 ec 51 f2 %).\$s. e. e.	> Frame 1762: 1464 bytes on	HPFEEDS	ptured (11712 bits) on i	nterface 0	·
> Internet Protocol Version > Transmission Control Proto > [6 Reassembled TCP Segment 0000 3a 8d e6 2c 6c 5c d4 0010 05 aa 20 3e 40 00 5a 0020 01 3f 01 bb d7 8a 30 0030 00 8c bc 97 00 00 79 PA4 Statistics Pv4 Statistics Pv6 Statistics Pv7 b 38 6c 96 0c 8c ee 53 1d 23 b1 a3 8f 50 d1 1a {81	> Ethernet II, Src: Routerbo	НТТР	<pre>st: 3a:8d:e6:2c:6c:5c (3a)</pre>	a:8d:e6:2c:6c:5c)	
> Transmission Control Proto Sametime 178, Seq: 79000, Ack: 2085, Len: 1410 > [6 Reassembled TCP Segment Sametime 178, Seq: 79000, Ack: 2085, Len: 1410 0000 3a 8d e6 2c 6c 5c d4	> Internet Protocol Version	HTTP2	8.1.63		
> [6 Reassembled TCP Segment TCP Stream Graphs 0000 3a 8d e6 2c 6c 5c d4 0010 05 aa 20 3e 40 00 5a 0020 01 3f 01 bb d7 8a 30 0020 01 3f 01 bb d7 8a 30 0040 39 09 ca 11 80 70 bf 48 0070 7 3b e5 a3 b4 16 2d 83 0060 7f 25 29 16 24 94 44 53 0070 7b 38 6c 96 0c 8c ee 53 0070 7b 38 6c 96 0c 8c ee 53 0080 8f a1 26 2d 77 43 9c c5 0080 8f a1 26 2d 77 43 9c c5 0080 8f a1 26 2d 77 43 9c c5 0080 8f a1 26 2d 77 43 9c c5 0080 8f a1 26 2d 77 43 9c c5 0080 8f a1 26 2d 77 43 9c c5 011 a6 b0 c6 a5 1 ad 32 3 87 a5 0a 11 ca bf a62 0080 8f a1 26 2d 77 43 9c c5 0080 8f a1 26 2d 77 43 9c c5 081 bd fa 62 # 0080 8f a1 26 2d 77 43 9c c5 075 (10678-9321-H12c 48072-8002-801252	> Transmission Control Proto	Sametime	178, Seq: 79000, Ack: 20	85, Len: 1410	()) -
00000 3a 8d e6 2c 6c 5c d4 UDP Multicast Streams ,1\m3.dE. 0010 05 aa 20 3e 40 00 5a IPv4 Statistics ,	> [6 Reassembled TCP Segment	TCP Stream Graphs	, 57(1410), #1758(1410), #1	1759(1410), #1761(1410), #1762	(1029)]
0010 05 aa 20 3e 40 00 5a IPv4 Statistics >0	0000 3a 8d e6 2c 6c 5c d4	UDP Multicast Streams	1\ m3.dE.		,
0020 01 3f 01 bb d7 8a 30 { IPv6 Statistics	0010 05 aa 20 3e 40 00 5a (ID: 4 Statistics	>@.ZH		
0030 00 & & & & & bc 97 00 00 79 1 Invo statutes , y. y. F. uC3 0040 39 09 ca 11 80 70 bf 48 07 3b e5 a3 b4 16 2d 83 9 , y. y. F. uC3 0050 87 a8 f1 f6 c0 32 02 d8 0b e8 4e 44 09 97 a0 80 2ND 0060 7f 25 29 16 24 94 d4 53 a8 f6 df 16 16 ec 51 f2 .%).\$. SQ. 0070 7b 38 6c 96 0c 8c ee 53 1d 23 b1 a3 8f 50 d1 1a {81S. #P 4. 0080 8f a1 26 2d 77 43 9c c5 ce f6 38 fb d5 81 ed 9a#b #b 0090 f1 a6 b0 c6 a5 1a d3 23 87 a5 0a 11 ca bd fa 62#b	0020 01 3f 01 bb d7 8a 30 \$	ID of Charlinking	0:P.		
0040 39 09 ca 11 80 70 bf 48 07 3b e5 a3 b4 16 2d 83 9p.H .; 0050 87 a8 f1 f6 c0 32 02 d8 0b e8 4e 44 09 97 a0 80 2ND 0060 7f 25 29 16 24 94 d4 53 a8 f6 df 16 16 ec 51 2	0030 00 8c bc 97 00 00 79 8	IPV0 Statistics	y. yF.uC3		
0050 87 a8 f1 f6 c0 32 02 d8 00 e8 44 09 7 a0 a0	0040 39 09 ca 11 80 70 bf 4	18 07 3b e5 a3 b4 16 2d 83	9p.H .;		
0060 77 25 29 16 24 94 d4 53 a8 f6 df 16 16 c < 51	0050 87 a8 f1 f6 c0 32 02 d	18 0b e8 4e 44 09 97 a0 80	2ND		
0080 8f a1 26 2d 77 43 9c c5 ce f6 38 fb d5 81 ed 9a	0050 /T 25 29 16 24 94 d4 9	3 a8 T6 dT 16 16 ec 51 t2	.70).55Q. [8] 5 # P		
0090 f1 a6 b0 c6 a5 1a d3 23 87 a5 0a 11 ca b1 fa 62 # b Frame (1464 bytes) Reasembled TCP (8029 bytes) # b Image: Comparison of the compa	0080 8f a1 26 2d 77 43 9c d	-5 ce f6 38 fb d5 81 ed 9a	δ-ωC 8		
Frame (1464 bytes) Reassembled TCP (8029 bytes)	0090 f1 a6 b0 c6 a5 1a d3 2	23 87 a5 0a 11 ca bd fa 62	#b		
Q wireshark_52E10678-3921-412C-88D7-21BC1A20F840_20170602162450_a01252 Packets: 4189 • Displayed: 4189 (100.0%) Profile: Default	Frame (1464 bytes) Reassembled TCP (8029 by	/tes)			
	Wireshark_52E10678-3921-412C-8BD7-2	1BC1A20FB40_20170602162450_a01252		Packets: 4189 ' Displayed: 4189 (100.0%)	Profile: Default

Figure 4. Use Statistics->Conversation to select the traffic you want



After click the Conversation, Wireshark will analyze the captured traffic and present conversations (sessions) for you, as shown in Figure 5. In this window, you will see the conversation on different network layers, Ethernet, IPv4, IPv6, TCP and UDP. The number beside each tab shows how many conversation there are, seen from this layer.

WITESHALK	Conve	sations	• wiresna	ark_52E10	078-392	1-412C-8	BD1-21BC1A20	·B40_20170602	162450_a01252				-	- ⊔	
Ethernet • 26	IPv	4 • 66	IPv6 ·	5 TC	· 82	UDP · 52									
ddress A	Port A	Addres	s B	Port B	Packets	Bytes	Packets $A \rightarrow B$	Bytes A \rightarrow B	$Packets \; B \to A$	Bytes B \rightarrow A	Rel Start	Duration	$Bits/s\:A\toB$	Bits/s B \rightarrow A	ι.
92.168.1.63	64029	52.210.	197.109	443	18	1571	9	803	9	768	0.676131	30.1486	213	20	03
92.168.1.63	52082	192.168	3.1.45	445	2	121	1	55	1	66	4.189192	0.0066	67 k	80) k
92.168.1.63	55093	172.217	.22.163	443	20	2721	9	1167	11	1554	4.559551	0.2212	42 k	56	í k
2.168.1.63	55138	45.79.1	80.95	443	9	493	8	433	1	60	4.632912	18.9004	183	1	25
92.168.1.63	55140	45.79.1	80.95	443	9	493	8	433	1	60	4.633145	18.9043	183	1	25
2.168.1.63	55139	45.79.1	80.95	443	9	493	8	433	1	60	4.633269	18.9009	183	1	25
92.168.1.63	55141	45.79.1	80.95	443	2	108	2	108	0	0	4.633371	0.0000	_	-	-
2.168.1.63	55142	45.79.1	80.95	443	2	108	2	108	0	0	4.633476	0.0001	_	-	_
2.168.1.63	55089	216.58.2	201.174	443	2	108	2	108	0	0	4.633727	0.0000	_	-	-
2.168.1.63	55109	216.58.2	209.110	443	2	108	2	108	0	0	4.633890	0.0000	_	-	-
2.168.1.63	55108	216.58.	209.110	443	2	108	2	108	0	0	4.633999	0.0000	_	-	-
2.168.1.63	55137	216.58.	209.142	443	2	108	2	108	0	0	4.634169	0.0000	_	-	-
2.168.1.63	55146	216.58.	201.163	443	2	108	2	108	0	0	4.634522	0.0000	_	-	-
2.168.1.63	55115	216.58.	211.129	443	2	108	2	108	0	0	4.634668	0.0000	_	-	-
2.168.1.63	55116	216.58.	211.129	443	2	108	2	108	0	0	4.634798	0.0000	_	-	-
2.168.1.63	55102	216.58.	209.99	443	2	108	2	108	0	0	4.634925	0.0000	_	-	-
2.168.1.63	55101	216.58.2	209.99	443	2	108	2	108	0	0	4.635054	0.0000	_	-	-
2.168.1.63	55114	216.58.2	201.161	443	2	108	2	108	0	0	4.635170	0.0000	_		-
2.168.1.63	55113	216.58.2	201.161	443	2	108	2	108	0	0	4.635284	0.0000	_	-	-
2.168.1.63	55099	216.58.2	201.174	443	2	108	2	108	0	0	4.635420	0.0000	_		-
2.168.1.63	55100	216.58.2	201.174	443	2	108	2	108	0	0	4.635517	0.0000	_	-	_
2.168.1.63	55105	216.58.2	209.110	443	2	108	2	108	0	0	4.635636	0.0000	_	-	-
2.168.1.63	55103	216.58.2	209.110	443	2	108	2	108	0	0	4.635752	0.0000	_	-	_
2.168.1.63	55145	216.58.	211.142	443	2	108	2	108	0	0	4.635872	0.0000	_		_
2.168.1.63	55088	172.217	.22.163	443	2	108	2	108	0	0	4.635987	0.0000	_	-	_
2.168.1.63	55086	172.217	.22.163	443	2	108	2	108	0	0	4.636098	0.0000	_		_
Name resolu	ition		Limit to	display fil	ter		osolute start time						Co	onversation Ty	/P
									Сору	- Follow	Stream	Graph	Close	He	lp

Figure 5. Conversation/session analysis

Look through the list of conversations and find the correct one(s) you want to save into a PCAP file. You can right-click on the conversation as shown in Figure 6 and select Apply as Filter -> Selected. Wireshark will automatically create a display filter for you and show you only the traffic you are interested in, as shown in Figure 7.



hernet • 26	IPv	4 • 66	IPv6 ·	5 TCF	• 82	UDP • 52								
Idress A	Port A	Address	В	Port B	Packets	Bytes	Packets A → B B	Bytes A → B	Packets B \rightarrow A	Bytes $B \rightarrow A$	Rel Start	Duration	$Bits/s\:A\toB$	$Bits/s \mathrel{B} \to A$
2.168.1.63	55088	172.217.2	22.163	443	2	108	2	10	3 0		4.635987	0.0000	_	-
2.168.1.63	55086	172.217.2	22.163	443	2	108	2	10	3 0		4.636098	0.0000	-	-
2.168.1.63	55094	172.217.2	22.163	443	2	108	2	10	3 0		4.636218	0.0000	_	-
2.168.1.63	55095	172.217.2	22.163	443	2	108	2	10	3 0		4.636326	0.0000	-	-
2.168.1.63	55091	172.217.2	22.163	443	2	108	2	10	3 0		4.636437	0.0000	-	-
2.168.1.63	55092	172.217.2	22.163	443	2	108	2	10	3 0		4.636539	0.0000	_	-
2.168.1.63	55096	172.217.2	22.163	443	2	108	2	10	3 0	(4.636649	0.0000	— —	-
2.168.1.63	55112	172.217.2	22.163	443	2	108	2	10	3 0	(4.636763	0.0000	— —	-
2.168.1.63	55111	172.217.2	22.163	443	2	108	2	10	3 0	(4.636856	0.0000	-	-
2.168.1.63	55110	172.217.2	2.163	443	2	108	2	10	3 0	(4.636982	0.0000	_	-
2.168.1.63	55161	216.58.21	1.133	443	30	7203	15	193	15	527	4.638107	0.1398	110 k	301
2.168.1.63	55162	173.194.2	222.94	443	38	8746	19	255	19	619	4.705195	0.9241	22 k	53
2.168.1.63	55163	216.58.21	1.132	443	29	8492	15	1562	. 14	693	4.719869	0.0991	126 k	559
2.168.1.63	55164	31.13.72.	36	443	13	4888	6	662	. 7	422	5 5.160071	0.0613	86 k	551
2.168.1.63	55165	31.13.72.	36	443	2,568	2694 k	470		: 2,098	2620	5.160205	18.4124	32 k	1138
2.168.1.63	55166	31.13.72.	36	443	13	48	Apply as Filter	r 🔸 🗌	Selected	•	Δ	0.0536	98 k	631
2.168.1.63	55167	31.13.72.	36	443	13	48	Propare a Filte		March and		A⇔D	0.0457	115 k	739
2.168.1.63	55131	216.58.20	9.110	443	64	18	Frepare a fille		Not Selected	•	$A \rightarrow B$	7.3144	13 k	684
2.168.1.63	55168	31.13.72.	12	443	366	328	Find		and Selected	•	B → A	5.1463	17 k	492
2.168.1.63	55169	31.13.72.	14	443	136	134	Colorize	•	or Selected	•		0.1235	259 k	8458
2.168.1.63	55170	31.13.72.	14	443	15	4997	8		and and Cale of			0.0629	98 k	537
2.168.1.63	55171	31.13.72.	14	443	15	4997	8		and not select	ted 🕐	A → Any	0.0630	98 k	536
2.168.1.63	55172	31.13.72.	14	443	15	4998	8		or not Selecte	d 🕨	Any → A	0.0634	97 k	533
2,168,1.63	55173	31.13.72.	14	443	15	4997	8	77	2 7		Anv ↔ B	0.0630	98 k	536
2,168,1.63	55174	31.13.72.	14	443	15	4997	8	77	2 7			0.0631	97 k	536
2.168.1.63	55175	31.13.72.	14	443	17	5194	7	72	2 10		Any → B	0.0895	64 k	399
											B → Any			

Figure 6. Select the conversation and apply as filter.

After filtering out the traffic you want to save, click File -> Export Specified Packets, and save the displayed packets into a PCAP file.

📕 *Wi-Fi								- 🗆	×
File Edit View Go Captur	re Analyze St	atistics Telephony Wireless	Tools Help						
Open	Ctrl+O	🛯 🗿 🛃 🚍 🗨 Q, Q							
Open Recent	•	addr==31.13.72.36 && tcp.port==4	143					Expression.	
Merge		Source	Src Port	Destination	Dst Port	Length	Host	Protocol	^
Import from Hex Dump		31.13.72.36	443	192.168.1.63	55165	892		TLSv1.2	
Close	Ctrl+W	192.168.1.63	55165	31.13.72.36	443	54		TCP	
Salve	Ctrl+S	31.13.72.36	443	192.168.1.63	55165	96		TLSv1.2	
Save Ar	Ctrl Shift S	31.13.72.36	443	192.168.1.63	55165	577		TLSv1.2	
Jave As	Cur+3mit+3	192.168.1.63	55165	31.13.72.36	443	54		TCP	
File Set	•	192.168.1.63	55165	31.13.72.36	443	188		TLSv1.2	
Export Specified Packets		192.168.1.63	55165	31.13.72.36	443	145		TLSv1.2	
Export Packet Dissections		31.13.72.36	443	192.168.1.63	55165	96		TLSv1.2	
Export Packet Bytes	Ctrl+H	31.13.72.36	443	192.168.1.63	55165	1339		TLSv1.2	
Export PDUs to File	Current	192.168.1.63	55165	31.13.72.36	443	54		TCP	
Export SSI Service Keyr		31.13.72.36	443	192.168.1.63	55165	1464		TCP	
Export Objects	•	31.13.72.36	443	192.168.1.63	55165	1464		TLSv1.2	
Export Objects		31.13.72.36	443	192.168.1.63	55165	318		TLSv1.2	
Print	Ctrl+P	192 168 1 63	55165	31 13 72 36	443	54		TCP	*
Quit	Ctrl+Q	(432 bits), 54 byte	s capture	d (432 bits) on in	terface 0)			
> Ethernet II, Src:	3a:8d:e6:2	c:6c:5c (3a:8d:e6:2c	:6c:5c), [Dst: Routerbo 33:1	e:64 (d4:	ca:6d:	33:1e:64)		
> Internet Protocol	Version 4,	Src: 192.168.1.63,	Dst: 31.13	3.72.36			,		
> Transmission Contr	ol Protoco	l, Src Port: 55165,	Dst Port:	443, Seq: 6735, A	ck: 84542	2, Len	: 0		
0000 d4 ca 6d 33 1	e 64 3a 8d	e6 2c 6c 5c 08 00 4	4500 1501 (.m3.d:,1\E.					
0010 00 28 25 50 40 0020 48 24 d7 7d 0	0 00 80 08 1 bb 84 89	70 96 99 26 30 26 1	той .(5010 н¢	(#P@					
0030 09 5b e4 7b 0	0 00 04 05	10 00 00 80 00 20 .		.{					
O 2 wireshark_52E10678-392	1-412C-88D7-218C	1A20FB40_20170602162450_a0125	2			Packets: 418	39 · Displayed: 2568 (61.3%) · Droppe	d: 0 (0.0%) Profile: Def	fault

Figure 7. Save the displayed packets into a PCAP file



MAKE PCAP COMFORMING TO XENA REPLAY RULES

There are some rules for the PCAP file to be properly parsed and replay. Make sure your PCAP conforms to the following rules:

- 1. Max number of segments per PCAP:
 - o 1 million segments for VulcanCompact,
 - 2 million segments for VulcanBay.
- 2. Max number of connections per PCAP:
 - o 256 for VulcanCompact
 - o 256 for VulcanBay
- 3. Max size per PCAP file

The maximum size of the PCAP file depends on the average TCP/UDP segment size. PCAP files larger than 1GB are in generate supported, as long as the number of segments and connections are within the range defined by (1) and (2).

- One source IP address (one-client-to-many-servers communication)
 You can either capture your traffic on a PC like Figure 8 (A), or capture traffic after a NAT router as in Figure 8 (B). Both cases will have one-to-many traffic.
- 5. No IP fragmentation
- 6. Recorded TCP maximum segment size/UDP packet size should below:
 - o 1460 bytes (TCP+IPv4)
 - o 1440 bytes (TCP+IPv6)
 - o 1472 bytes (UDP+IPv4)
 - 1452 bytes (UDP+IPv6)
- 7. PCAP should contain either IPv4 or IPv6, but not both in one file.
- 8. Only TCP and UDP packets will be replayed.



Figure 8. Traffic should be one-to-many

IF YOUR PCAP FILE VIOLATES ANY OF THE RULES ABOVE, THE PARSER WILL REPORT IT WHEN THE PCAP HAS BEEN UPLOADED TO THE CHASSIS.



USE PCAP FILE FOR REPLAY

This section describes how to import a PCAP file for Layer 4 PCAP relay using VulcanManager. More details about how to use VulcanManager can be found here:

https://xenanetworks.com/vulcanmanager-users-manual/

CREATE RELAY SCENARIO

Add a Replay scenario into a test case as shown in Figure 9. Notice that you need to select the IP version beforehand. After clicking OK, you can find your PCAP file in the dialog window.



Figure 10. PCAP import dialog window

We will see the PCAP import dialog window as in Figure 10 showing the progress. The PCAP will first be uploaded to the chassis. Then the PCAP parser will parse and analyze the file. When the import is finished, you will be able to see the analysis result including number of connections, Layer 4 protocols, number of segments, and total payload size. Click OK to proceed.



🚔 💾 🗵 🗵 🗮		PCAP - Replay - Vulcar	Manager			- 🗆 ×
File Test Configuration Test Execution	Statistics and Rep	orting				0
Chassis Test Add Add Testcase Scenario	Scenario lissing ing ation Status					
Test Explorer	Test case 0					Client - Server
d Collapse						
Name	Description		Testo	ase		
 PCAP - Replay 	Name: Te	s PCAP file import		Users:	C	
Device under test		Washing and		Connections:	C	
► 👬 Subnets 🔶 🕂	Distribution of total users	ETB analysis download E00MP as		Profile		
Thest case 0		rir_passive_download_Jourins.pc	apng			
		Opticianty peap title: 1 + 3 + 6 Waiting to parts: 3186each Waiting to verify replay defini Connections: Transport protocol(b): Total segments: Total payload:	Idb-40f1-9ea7-cde4a2ae18fb tion: 3186eaae-14db-40f1-9ec 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		No series added	
	Identity	Subnets - Ports			Load Profile Line F	Column Groups
	Active Type Name	Client Subnet Sen	ver Subnet Client	Port Server Port	Users Cli	 Subnets - Ports Load Profile Line Rate Utilization
🛍 Chassis Explorer 🖃 Test Explorer					•	

Figure 10. PCAP import dialog window

SCALE YOUR TRAFFIC

As shown in Figure 11, you have successfully created a replay scenario using the PCAP file you have made. By default, the number of users is set to 100,000, which means the tester will duplicate the PCAP traffic 100,000 times, each of which is assigned a new IP address. This is the reason for Rule 3 (one-to-many communication) because the replay engine can scale the traffic.



Figure 11. PCAP import dialog window



COMPOSE YOUR OWN PLAYLIST WITH MULTIPLE PCAP FILES

You can also build your own "playlist" by importing multiple PCAP files into one test case. Repeatedly creating Replay scenarios into one test case will allow you to simultaneously play or sequentially play PCAP files.

Figure 12 shows an example of two Replay scenarios in one test case. By configuring the load profile for each replay scenario, you can simultaneously or sequentially play your PCAP files. Make sure to assign different subnet ranges to the server side to avoid socket conflict.



Figure 12. Make your own "playlist" by creating multiple replay scenarios in one test case



LOOP YOUR PCAP

You can loop the replay of a PCAP file with either the same source IP address or different source IP addresses by configuring "User Updates" in the "Connection Establishment" entry of the test scenario, as shown in Figure 13.

Click the "Connection Establishment" entry under the scenario and find "User Updates" section. Choose among "No rebirth", "With same Src IP", and "With new Src IP", and input repetitions. If the repetition is set to 0 or left empty, the loop will continue till the end of the test.







THINGS YOU SHOULD KNOW ABOUT XENA PCAP REPLAY

Xena PCAP replay is Layer-4 payload replay (more can be read on <u>http://xenanetworks.com/advanced-stateful-layer-4-replay-white-paper/</u>), thus it is different from stateless packet replay.

PAYLOAD REPLAY

Xena PCAP replay parser extracts the layer-4 payloads, and replay them with new headers. Thus, the replayed traffic may have different Ethernet headers, IP headers, and TPC/UDP headers, depending on how you configure the new MAC addresses and IP addresses. Destination ports are preserved, but source port numbers are replaced by ports in the ephemeral source port range suggested by the Internet Assigned Numbers Authority (IANA).

PRESERVED PAYLOAD

The payload is replayed as is. Users cannot modify the payload for replay.

New Connection

TCP handshake (SYN, SYN-ACK, ACK) and teardown (FIN, ACK) will be added to the TCP session if no handshake/ teardown is present in the file.

RELIABLE DELIVERY

In case of packet loss, Xena TCP stack will retransmit.

CONGESTION CONTROL

TCP congestion control can be turned on or off according to users' need.

TCP AND UDP REPLAY

Only TCP and UDP packets are replayed. If there are packets such as ARP in the PCAP, they will not be replayed.

REPLAY WITH SPEED-UP OR SLOW-DOWN

Usually the PCAP file is recorded with a certain bandwidth, e.g. capturing a streaming content at 1 Mbps rate (Layer 1 rate) for 600 seconds. When replaying this PCAP at a high bandwidth, e.g. 1Gbps, the duration of the replay will be shortened to 0.6 second (speed-up). If you want to maintain the same duration as it is in the PCAP file, you should remember to modify the rate to a lower value (slow-down). Read more on <u>https://xenanetworks.com/vulcanmanager-users-manual/</u>