

# Capturing Packets:

The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

Capture

...using this filter:  All interfaces shown

Wi-Fi

Adapter for loopback traffic capture

Local Area Connection\* 10

Local Area Connection\* 9

Local Area Connection\* 8

Local Area Connection\* 2

Local Area Connection\* 1

Local Area Connection

USBCap1

USBCap2

Cisco remote capture

Event Tracing for Windows (ETW) reader

Random packet generator

SSH remote capture

UDP Listener remote capture

Wi-Fi remote capture

Extcap interface: sshdump.exe  
No capture filter

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.2.6 (v4.2.6-0-g2acd1a854bab). You receive automatic updates.

Ready to load or capture

No Packets

Profile: Default

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
777	27.370383	142.250.195.106	172.16.11.137	UDP	68	443 → 53965 Len=26
778	27.573630	172.16.11.137	142.250.195.106	UDP	71	53965 → 443 Len=29
779	27.589090	142.250.195.106	172.16.11.137	UDP	68	443 → 53965 Len=26
780	27.791969	172.16.11.137	142.250.195.106	UDP	71	53965 → 443 Len=29
781	27.810488	142.250.195.106	172.16.11.137	UDP	68	443 → 53965 Len=26
782	28.026776	172.16.11.137	142.250.195.106	UDP	71	53965 → 443 Len=29
783	28.031391	172.16.9.75	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
784	28.037663	Dell_34:d4:19	Broadcast	ARP	60	Who has 172.16.9.185? Tell 172.16.9.188
785	28.050207	142.250.195.106	172.16.11.137	UDP	68	443 → 53965 Len=26
786	28.463475	172.16.11.137	142.250.195.106	UDP	71	53965 → 443 Len=29

> Frame 1: 71 bytes on wire (568 bytes captured) on interface eth0

> Ethernet II, Src: CloudNetworks (08:00:27:00:00:00), Dst: 01:00:5e:00:00:11

> Internet Protocol Version 4, Src: 172.16.11.137, Dst: 142.250.195.106

> User Datagram Protocol, Src Port: 53965, Dst Port: 443

> Data (29 bytes)

0000 7c 5a 1c cf be 45 cc 5e f8 d1 ca 1d 08 00 45 00 |Z...E.^.....E.

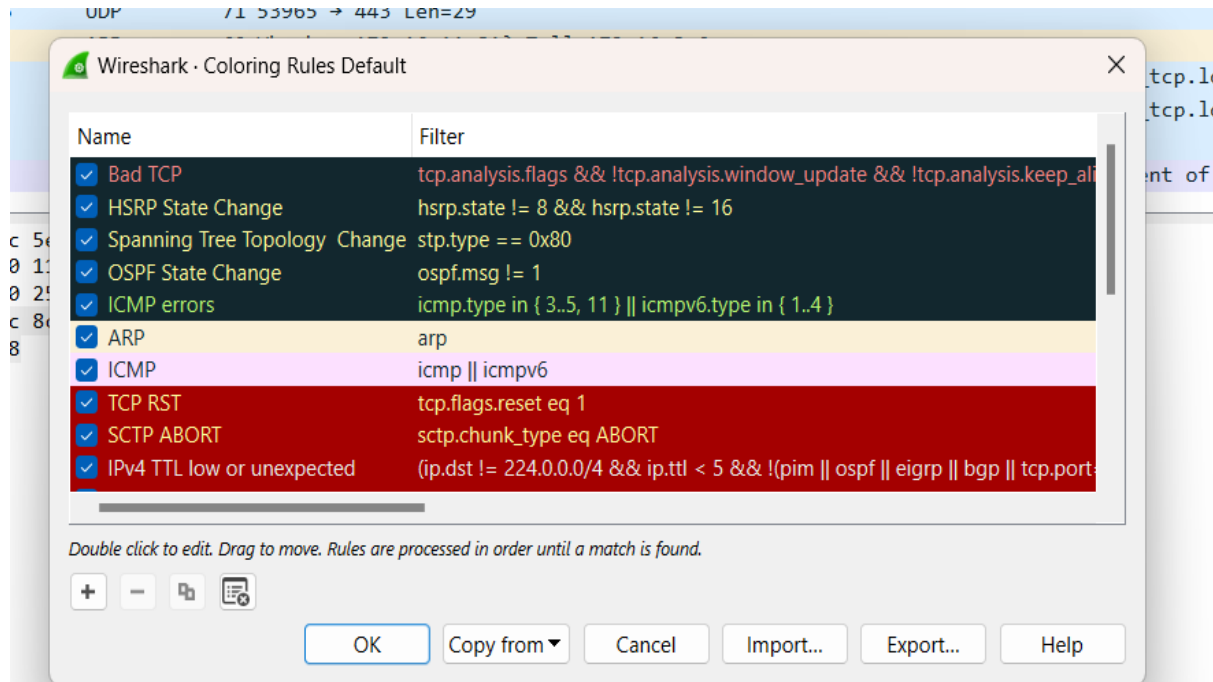
0010 00 39 93 d3 40 00 80 11 5c e2 ac 10 0b 89 8e fa |.9..@... \.....

0020 c3 6a d2 cd 01 bb 00 25 03 11 4b ef e0 6d 57 8b |.j....%..K..mW.

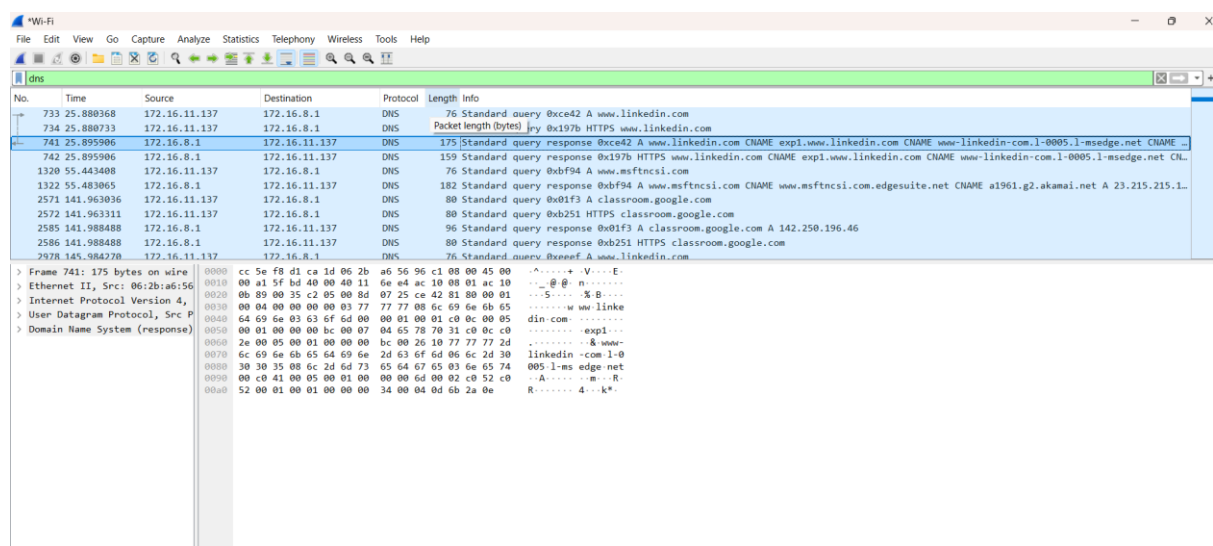
0030 6d dc ed 01 5d 1e cc 8c f0 09 30 80 e7 d2 53 2a |m...]... ..0...S\*

0040 40 4b 95 82 6c 44 78 @K...lDx

## Color Coding:



## Filtering packets



Wireshark - Display Filters

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	eth.type == 0x0806
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1	ip.addr != 192.0.2.1
IPv6 only	ipv6
IPv6 address 2001:db8::1	ipv6.addr == 2001:db8::1

<C:\Users\quhan\AppData\Roaming\Wireshark\filters>

OK Cancel Help

Wireshark - Follow TCP Stream (tcp.stream eq 2) - Wi-Fi

Packet 736, 33 client pkts, 88 server pkts, 41 turns. Click to select.

Entire conversation (67 kB) Show data as ASCII Stream 2

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

# Inspecting Packets:

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: \_ws.col.info == "Hello Retry Request, Change Cipher Spec"

No.	Time	Source	Destination	Protocol	Length	Info
15	3.106246	13.78.111.198	172.16.11.137	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
1073	51.163135	13.107.137.11	172.16.11.137	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
2498	136.669806	20.42.73.27	172.16.11.137	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
2735	143.717185	13.107.137.11	172.16.11.137	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
3811	183.284581	20.42.73.27	172.16.11.137	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
9784	246.118658	52.104.144.53	172.16.11.137	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
10325	268.345919	20.42.73.27	172.16.11.137	TLSv1.3	153	Hello Retry Request, Change Cipher Spec

> Frame 9784: 153 bytes on wire (1224 bytes captured) on interface 0  
> Ethernet II, Src: Sophos\_cf:b8:67:eb, Dst: 08:00:27:00:00:00  
> Internet Protocol Version 4, Src: 52.104.144.53, Dst: 172.16.11.137  
> Transmission Control Protocol, Src Port: 443, Dst Port: 443, Seq: 3123456789, Len: 153  
> Transport Layer Security, Protocol: TLSv1.3, Version: 3, Length: 153, Content Type: Change Cipher Spec, Content Length: 153

0000 cc 5e f8 d1 ca 1d 7c 5a 1c cf be 45 08 00 45 00 .^...|Z...E...E-  
0010 00 0b 1f 2e 40 00 40 06 9f 08 34 68 90 35 ac 10 ....@...4h-5-..  
0020 0b 89 01 bb f2 6b ba 29 0b 0c 3f f0 59 86 50 18 ....k...)??Y-P..  
0030 00 ed b0 5e 00 00 16 03 03 00 58 02 00 00 54 03 ....A...X...T..  
0040 03 cf 21 ad 74 e5 9a 61 11 be 1d 8c 02 1e 65 b8 ...!t-a.....e-  
0050 91 c2 a2 11 16 7a bb 8c 5e 07 9e 09 e2 c8 a8 33 ....z-^.....3  
0060 9c 20 2d 96 a4 98 87 e4 c3 67 29 99 80 10 af 16 .......g).....  
0070 cc 1b 1c ae e0 f3 b8 c2 17 d8 c6 79 35 45 54 bd .......y5ET-..  
0080 72 f0 13 02 00 00 0c 00 2b 00 02 03 04 00 33 00 .....+.....3-  
0090 02 00 18 14 03 03 00 01 01 .....

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: \_ws.col.info == "Hello Retry Request, Change Cipher Spec"

No.	Time	Source	Destination	Protocol	Length	Info
15	3.106246	13.78.111.198	172.16.11.137	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
1073	51.163135	13.107.137.11	172.16.11.137	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
2498	136.669806	20.42.73.27	172.16.11.137	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
2735	143.717185	13.107.137.11	172.16.11.137	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
3811	183.284581	20.42.73.27	172.16.11.137	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
9784	246.118658	52.104.144.53	172.16.11.137	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
10325	268.345919	20.42.73.27	172.16.11.137	TLSv1.3	153	Hello Retry Request, Change Cipher Spec

> Frame 9784: 153 bytes on wire (1224 bytes captured) on interface 0  
> Ethernet II, Src: Sophos\_cf:b8:67:eb, Dst: 08:00:27:00:00:00  
> Internet Protocol Version 4, Src: 52.104.144.53, Dst: 172.16.11.137  
> Transmission Control Protocol, Src Port: 443, Dst Port: 443, Seq: 3123456789, Len: 153  
> Transport Layer Security, Protocol: TLSv1.3, Version: 3, Length: 153, Content Type: Change Cipher Spec, Content Length: 153

0000 cc 5e f8 d1 ca 1d 7c 5a 1c cf be 45 08 00 45 00 .^...|Z...E...E-  
0010 00 0b 1f 2e 40 00 40 06 9f 08 34 68 90 35 ac 10 ....@...4h-5-..  
0020 0b 89 01 bb f2 6b ba 29 0b 0c 3f f0 59 86 50 18 ....k...)??Y-P..  
0030 00 ed b0 5e 00 00 16 03 03 00 58 02 00 00 54 03 ....A...X...T..  
0040 03 cf 21 ad 74 e5 9a 61 11 be 1d 8c 02 1e 65 b8 ...!t-a.....e-  
0050 91 c2 a2 11 16 7a bb 8c 5e 07 9e 09 e2 c8 a8 33 ....z-^.....3  
0060 9c 20 2d 96 a4 98 87 e4 c3 67 29 99 80 10 af 16 .......g).....  
0070 cc 1b 1c ae e0 f3 b8 c2 17 d8 c6 79 35 45 54 bd .......y5ET-..  
0080 72 f0 13 02 00 00 0c 00 2b 00 02 03 04 00 33 00 .....+.....3-  
0090 02 00 18 14 03 03 00 01 01 .....

Capture File Properties  
Resolved Addresses  
Protocol Hierarchy  
Conversations  
Endpoints  
Packet Lengths  
I/O Graphs  
Service Response Time  
DHCP (BOOTP) Statistics  
NetPerfMeter Statistics  
ONC-RPC Programs  
29West  
ANCP  
BACnet  
Collectd  
DNS  
Flow Graph  
HART-IP  
HPFEEDS  
HTTP  
HTTP2  
Sametime  
TCP Stream Graphs  
UDP Multicast Streams  
Reliable Server Pooling (RSerPool)  
SOME/IP  
DTN  
F5  
IPv4 Statistics  
IPv6 Statistics

Ctrl+Alt+Shift+C

o Retry Request, Change Cipher Spec  
o Retry Request, Change Cipher Spec  
o Retry Request, Change Cipher Spec  
o Retry Request, Change Cipher Spec  
o Retry Request, Change Cipher Spec  
o Retry Request, Change Cipher Spec  
o Retry Request, Change Cipher Spec

45 00 .^...|Z...E...E-  
ac 10 ....@...4h-5-..  
50 18 ....k...)??Y-P..  
54 03 ....A...X...T..  
55 b8 ...!t-a.....e-  
a8 33 ....z-^.....3  
af 16 .......g).....  
54 bd .......y5ET-..  
33 00 .....+.....3-  
.....

# Graph Analysis:

