

WIRESHARKlab1.pcapng

http

No.	Time	Source	Destination	Protocol	Length	Info
361	9.986191	2001:16a2:c056:5...	2600:1f13:37c:14...	HTTP	560	GET /online HTTP/1.1
363	10.301470	2600:1f13:37c:14...	2001:16a2:c056:5...	HTTP	619	HTTP/1.1 301 Moved Permanently (text/html)
368	10.310103	2001:16a2:c056:5...	2600:1f13:37c:14...	HTTP	561	GET /online/ HTTP/1.1
400	10.584683	2600:1f13:37c:14...	2001:16a2:c056:5...	HTTP	203	HTTP/1.1 200 OK (text/html)
407	10.731653	2001:16a2:c056:5...	2600:1f13:37c:14...	HTTP	528	GET /favicon.ico HTTP/1.1
414	10.997888	2600:1f13:37c:14...	2001:16a2:c056:5...	HTTP	490	HTTP/1.1 200 OK (PNG)

```

> Frame 361: 560 bytes on wire (4480 bits), 560 bytes captured (4480 bits) on interface en0
> Ethernet II, Src: Apple_7c:06:f6 (f4:d4:88:7c:06:f6)
> Internet Protocol Version 6, Src: 2001:16a2:c056:5...
> Transmission Control Protocol, Src Port: 54554, Dst Port: 80
> Hypertext Transfer Protocol
  > GET /online HTTP/1.1\r\n
    Host: coolwonderousfresheclipse.neverssl.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,ar-AE;q=0.8,ar;q=0.7\r\n
  [Response in frame: 363]
  [Full request URI: http://coolwonderousfresheclipse.neverssl.com/online]
```

0040 2c e5 50 18 10 00 89 73 00 00 47 45 54 20 2f  
0050 6e 6c 69 6e 65 20 48 54 54 50 2f 31 2e 31 0d  
0060 48 6f 73 74 3a 20 63 6f 6f 6c 77 6f 6e 64 65  
0070 6f 75 73 66 72 65 73 68 65 63 6c 69 70 73 65  
0080 6e 65 76 65 72 73 73 6c 2e 63 6f 6d 0d 0a 43  
0090 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d  
00a0 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49  
00b0 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73  
00c0 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a  
00d0 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 4d 61  
00e0 69 6e 74 6f 73 68 3b 20 49 6e 74 65 6c 20 4d  
00f0 63 20 4f 53 20 58 20 31 30 5f 31 35 5f 37 29  
0100 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37  
0110 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65  
0120 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 31  
0130 32 2e 30 2e 30 2e 30 20 53 61 66 61 72 69 2f  
0140 33 37 2e 33 36 0d 0a 41 63 63 65 70 74 3a 20  
0150 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63  
0160 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2d  
0170 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b

Http req/  
resp

Wireshark - Follow TCP Stream (tcp.stream eq 7) · WIRESHARKlab1.pcapng

tcp.stream eq 7

No.	Time	Source	Destination
279	7.367224	2600:1f13:37c:14...	2001:16a2:c056:5...
281	7.367661	2001:16a2:c056:5...	2600:1f13:37c:14...
361	9.986191	2001:16a2:c056:5...	2600:1f13:37c:14...
362	10.301468	2600:1f13:37c:14...	2001:16a2:c056:5...
363	10.301470	2600:1f13:37c:14...	2001:16a2:c056:5...
364	10.301761	2001:16a2:c056:5...	2600:1f13:37c:14...
368	10.310103	2001:16a2:c056:5...	2600:1f13:37c:14...
399	10.584680	2600:1f13:37c:14...	2001:16a2:c056:5...
400	10.584683	2600:1f13:37c:14...	2001:16a2:c056:5...
401	10.584960	2001:16a2:c056:5...	2600:1f13:37c:14...
407	10.731653	2001:16a2:c056:5...	2600:1f13:37c:14...
414	10.997888	2600:1f13:37c:14...	2001:16a2:c056:5...
415	10.998180	2001:16a2:c056:5...	2600:1f13:37c:14...
553	15.989688	2600:1f13:37c:14...	2001:16a2:c056:5...
554	15.989836	2001:16a2:c056:5...	2600:1f13:37c:14...
605	21.740746	2001:16a2:c056:5...	2600:1f13:37c:14...
641	22.007403	2600:1f13:37c:14...	2001:16a2:c056:5...

Acknowledgment number: 1+20 (160L)  
Acknowledgment number (raw): 38402873  
0101 .... = Header Length: 20 bytes (160 bits)  
Flags: 0x011 (FIN, ACK)

- 000.... = Reserved: Not set
- ...0.... = Accurate ECN: Not set
- ....0.... = Congestion Window
- ....0.... = ECM-Echo: Not set
- ....0.... = Urgent: Not set
- ....0.... = Acknowledgment: Set
- ....0.... = Push: Not set
- ....0.... = Reset: Not set
- ....0.... = Syn: Not set

> ....0.... = Fin: Set  
> [TCP Flags: ....A-F]  
Window: 236  
[Calculated window size: 30208]  
[Window size scaling factor: 128]

```

GET /online HTTP/1.1
Host: coolwonderousfresheclipse.neverssl.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,ar-AE;q=0.8,ar;q=0.7

HTTP/1.1 301 Moved Permanently
Date: Sun, 02 Feb 2025 09:22:31 GMT
Server: Apache/2.4.62 ()
Location: http://coolwonderousfresheclipse.neverssl.com/online/
Content-Length: 261
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://coolwonderousfresheclipse.neverssl.com/online/">here</a>.</p>
</body></html>

GET /online HTTP/1.1
Host: coolwonderousfresheclipse.neverssl.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,ar-AE;q=0.8,ar;q=0.7

3 client pkts, 4 server pkts, 5 turns.
```

Entire conversation (3907 bytes) Show as ASCII No delta times

Find: Case sensitive

Tcp  
stream

Three handshake

Source	Destination	Protocol	Length	Info
2001:16a2:c056:5...	2a00:1450:4006:8...	TCP	98	54550 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1390 WS=128
2a00:1450:4006:8...	2001:16a2:c056:5...	TCP	86	443 → 54550 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
2001:16a2:c056:5...	2a00:1450:4006:8...	TCP	74	54550 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2001:16a2:c056:5...	2a00:1450:4006:8...	TCP	1464	54550 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=1390 [TCP Spurious Retransmission]
2001:16a2:c056:5...	2a00:1450:4006:8...	TLSv1.2	472	Client Hello (SNI=ogs.google.com)
2a00:1450:4006:8...	2001:16a2:c056:5...	TCP	86	[TCP Dup ACK 25#1] 443 → 54550 [ACK] Seq=1 Ack=1 Win=65535
2a00:1450:4006:8...	2001:16a2:c056:5...	TCP	74	443 → 54550 [ACK] Seq=1 Ack=1789 Win=267776 Len=0
2001:16a2:c056:5...	2a00:1450:4006:8...	TCP	1464	[TCP Spurious Retransmission] 54550 → 443 [ACK] Seq=1 Ack=1 Win=262144
2a00:1450:4006:8...	2001:16a2:c056:5...	TLSv1.2	1294	Server Hello
2001:16a2:c056:5...	2a00:1450:4006:8...	TCP	74	54550 → 443 [ACK] Seq=1789 Ack=1221 Win=260864 Len=0

Fin/ack packets

No.	Time	Source	Destination	Protocol	Length	Info
196	5.691486	2001:4860:4802:3...	2001:16a2:c056:5...	TCP	86	443 → 54541 [FIN, ACK] Seq=1 Ack=1 Win=65535
197	5.691487	2001:4860:4802:3...	2001:16a2:c056:5...	TCP	86	443 → 54540 [FIN, ACK] Seq=1 Ack=1 Win=65535
198	5.691488	64:ff9b::2275:c9...	2001:16a2:c056:5...	TCP	86	443 → 54537 [FIN, ACK] Seq=5097 Ack=1
236	7.116683	2001:16a2:c056:5...	2001:4860:4802:3...	TCP	86	54541 → 443 [FIN, ACK] Seq=1 Ack=2 Win=65535
237	7.116749	2001:16a2:c056:5...	2001:4860:4802:3...	TCP	86	54540 → 443 [FIN, ACK] Seq=1 Ack=2 Win=65535
311	7.585163	2001:16a2:c056:5...	2a00:1450:4006:8...	TCP	74	54555 → 443 [FIN, ACK] Seq=1840 Ack=1
335	7.694723	2a00:1450:4006:8...	2001:16a2:c056:5...	TCP	74	443 → 54555 [FIN, ACK] Seq=8820 Ack=1
336	7.694996	2001:16a2:c056:5...	2a00:1450:4006:8...	TCP	148	[TCP Spurious Retransmission] 54555 → 443 [FIN, ACK] Seq=1126 Ack=1
465	14.093924	2001:16a2:c056:5...	64:ff9b::14e9:53...	TCP	74	54557 → 443 [FIN, ACK] Seq=1126 Ack=1
471	14.161318	2001:16a2:c056:5...	64:ff9b::14e9:53...	TCP	105	[TCP Spurious Retransmission] 54557 → 443 [FIN, ACK] Seq=4744 Ack=1
473	14.162914	64:ff9b::14e9:53...	2001:16a2:c056:5...	TCP	74	443 → 54557 [FIN, ACK] Seq=4744 Ack=1
510	15.015577	2001:16a2:c056:5...	64:ff9b::14e9:53...	TCP	74	54558 → 443 [FIN, ACK] Seq=1038 Ack=1
517	15.094551	64:ff9b::14e9:53...	2001:16a2:c056:5...	TCP	74	443 → 54558 [FIN, ACK] Seq=4799 Ack=1
518	15.094715	2001:16a2:c056:5...	64:ff9b::14e9:53...	TCP	105	[TCP Spurious Retransmission] 54558 → 443 [FIN, ACK] Seq=2481 Ack=1
553	15.989688	2600:1f13:37c:14...	2001:16a2:c056:5...	TCP	74	80 → 54554 [FIN, ACK] Seq=2481 Ack=1
578	21.726617	2001:16a2:c056:5...	2a00:1450:400c:c...	TCP	86	54536 → 5228 [FIN, ACK] Seq=1 Ack=1
579	21.727187	2001:16a2:c056:5...	2a00:1450:4006:8...	TCP	74	54556 → 443 [FIN, ACK] Seq=4342 Ack=1

Destination Port: 54541  
[Stream index: 3]  
> [Conversation completeness: Incomplete (20)]  
[TCP Segment Len: 0]  
Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 2665256384  
[Next Sequence Number: 2 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment number (raw): 3279525256  
1000 .... = Header Length: 32 bytes (8)  
> Flags: 0x011 (FIN, ACK)  
Window: 1049  
[Calculated window size: 1049]  
[Window size scaling factor: -1 (unknown)]  
Checksum: 0x003f [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0

## Udp header

```
✗ User Datagram Protocol, Src Port: 443, Dst Port:  
  Source Port: 443  
  Destination Port: 58243  
  Length: 32  
  Checksum: 0xbff8c [unverified]  
  [Checksum Status: Unverified]  
  [Stream index: 14]  
  [Stream Packet Number: 9]  
> [Timestamps]  
  UDP payload (24 bytes)
```

## Tcp header

```
Source Port: 54537  
Destination Port: 443  
[Stream index: 1]  
> [Conversation completeness: Incomplete (60)]  
  [TCP Segment Len: 0]  
  Sequence Number: 1 (relative sequence number)  
  Sequence Number (raw): 689240094  
  [Next Sequence Number: 1 (relative sequence number)]  
  Acknowledgment Number: 2717 (relative ack number)  
  Acknowledgment number (raw): 3445471964  
  1011 .... = Header Length: 44 bytes (11)  
> Flags: 0x010 (ACK)  
  Window: 2048  
  [Calculated window size: 2048]  
  [Window size scaling factor: -1 (unknown)]  
  Checksum: 0xdb18 [unverified]  
  [Checksum Status: Unverified]  
  Urgent Pointer: 0
```

Feature	TCP	UDP
Use Cases	- Web browsing (HTTP/HTTPS) - File transfer (FTP, SFTP) - Email (SMTP, IMAP, POP3) - Remote access (SSH, Telnet)	- Live streaming, VoIP - Online gaming - DNS queries - IoT sensor data transmission
Performance	- Reliable, ensures data integrity - Connection-oriented (3-way handshake) - Resends lost packets - Higher latency due to error checking	- Faster, minimal overhead - Connectionless, no handshake - No retransmission, can drop packets - Lower latency, suitable for real-time apps