
NETWORK SECURITY EXPERIMENT REPORT

Course Title and Number:

Computer Networks

Project Title:

Packet Analysis of Facebook and YouTube Traffic

Virtual private network (VPN) For Remote Access

Group Members:

M FUZAIL RAZA (39091)

M WAQAS ZAFAR (38605)

Riphah International University, Lahore

Submission Deadline:

07 January 2023.

WIRESHARK REPORT

WIRESHARK:

Wireshark is a network protocol analyzer that allows you to capture and inspect the data traveling back and forth on a computer network in real-time. It is an open-source tool commonly used for network troubleshooting, analysis, software development, and education. Wireshark supports a wide range of network protocols and can display the captured data in a detailed and readable format.

Usage:

1. **Network Troubleshooting:** Wireshark is often used to identify and troubleshoot network issues by analyzing the packets exchanged between devices.
2. **Security Analysis:** Security professionals use Wireshark to detect and analyze malicious activities on a network, such as unauthorized access or suspicious traffic patterns.
3. **Protocol Development:** Developers use Wireshark to understand and debug the communication between different devices or software components by examining the protocol messages.
4. **Educational Purposes:** Wireshark is commonly used in networking courses and training programs to teach students about network protocols, packet analysis, and network security.

5. Performance Optimization: It helps in optimizing network performance by identifying bottlenecks, latency issues, or inefficient data transfers.

Experiment Location:

Conducted at: Home

Type of Computer:

Hardware: AMD A8-4500M APU with Radeon(tm) HD Graphics (with SSE4.2)

OS: 64-bit Windows 10 (22H2), build 19045

Application: Dump cap (Wireshark) 4.2.0 (v4.2.0-0-g54eedfc63953)

CAPTURE FILE PROPERTIES:

Name: C:\Users\MFC~1\AppData\Local\Temp\wireshark_Wi-FiT67TG2.pcapng

Length: 18 MB

Hash cace611c5799d14cbb473a84647362a02a8dfe4a4ee6027510acc3d2
(SHA256): 54daa2b1

Hash 34e16cabb90969af3a98f59b12efacb05e926c04
(SHA1):

Format: Wireshark/... - pcapng

Encapsulation: Ethernet

Time

First packet: 2024-01-07 15:49:33

Last packet: 2024-01-07 16:23:33

Elapsed: 00:34:00

Capture

Hardware: AMD A8-4500M APU with Radeon(tm) HD Graphics (with SSE4.2)

OS: 64-bit Windows 10 (22H2), build 19045

Application: Dumpcap (Wireshark) 4.2.0 (v4.2.0-0-g54eedfc63953)

Interfaces

| <u>Interface</u> | <u>Dropped packets</u> | <u>Capture filter</u> | <u>Link type</u> | <u>Packet size limit (snaplen)</u> |
|------------------|------------------------|-----------------------|------------------|------------------------------------|
| Wi-Fi | 0 (0.0%) | none | Ethernet | 262144 bytes |

Statistics

| <u>Measurement</u> | <u>Captured</u> | <u>Displayed</u> | <u>Marked</u> |
|------------------------|-----------------|-------------------|---------------|
| Packets | 28321 | 28321 (100.0%) | — |
| Time span, s | 2040.020 | 2040.020 | — |
| Average pps | 13.9 | 13.9 | — |
| Average packet size, B | 634 | 634 | — |
| Bytes | 17946836 | 17946836 (100.0%) | 0 |

| | | | |
|-----------------|------|------|---|
| Average bytes/s | 8797 | 8797 | — |
| Average bits/s | 70 k | 70 k | — |

Conversation:

The overall packet send and receive across the networks:

| Ethernet · 17 IPv4 · 75 IPv6 · 7 TCP · 151 UDP · 390 | | | | | | | | | | | | | |
|--|--------|-----------------|--------|---------|-----------|-----------|---------------|-------------|---------------|-------------|-----------|-----------|--------|
| Address A | Port A | Address B | Port B | Packets | Bytes | Stream ID | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | Rel Start | Duration | Bits/s |
| 192.168.181.113 | 51724 | 157.240.227.21 | 443 | 608 | 270 kB | 1 | 298 | 249 kB | 310 | 21 kB | 0.088081 | 97.3997 | 20 |
| 192.168.181.113 | 51732 | 157.240.227.56 | 443 | 111 | 100 kB | 2 | 36 | 2 kB | 75 | 98 kB | 0.252091 | 65.1703 | 251 |
| 192.168.181.113 | 51735 | 157.240.227.1 | 443 | 408 | 204 kB | 3 | 159 | 15 kB | 249 | 188 kB | 1.020435 | 99.5675 | 1230 |
| 192.168.181.113 | 51697 | 51.89.98.179 | 443 | 40 | 2 kB | 4 | 22 | 1 kB | 18 | 1 kB | 1.219286 | 98.0634 | 97 |
| 192.168.181.113 | 51722 | 157.240.227.1 | 443 | 31 | 2 kB | 5 | 18 | 1 kB | 13 | 898 bytes | 5.283998 | 95.6346 | 111 |
| 192.168.181.113 | 51723 | 157.240.227.1 | 443 | 42 | 4 kB | 6 | 23 | 2 kB | 19 | 2 kB | 5.790833 | 94.1339 | 134 |
| 192.168.181.113 | 51728 | 157.240.227.21 | 443 | 47 | 7 kB | 7 | 25 | 5 kB | 22 | 1 kB | 8.255262 | 91.9214 | 445 |
| 20.192.44.78 | 443 | 192.168.181.113 | 50608 | 1 | 290 bytes | 8 | 1 | 290 bytes | 0 | 0 bytes | 13.034955 | 0.0000 | |
| 192.168.181.113 | 51731 | 20.192.44.78 | 443 | 32 | 2 kB | 9 | 19 | 2 kB | 13 | 872 bytes | 13.498653 | 84.8142 | 146 |
| 192.168.181.113 | 51707 | 173.194.76.188 | 5228 | 7 | 404 bytes | 10 | 4 | 218 bytes | 3 | 186 bytes | 18.909408 | 60.3714 | 28 |
| 192.168.181.113 | 51713 | 157.240.227.1 | 443 | 5 | 271 bytes | 11 | 3 | 163 bytes | 2 | 108 bytes | 21.111483 | 15.2103 | 85 |
| 192.168.181.113 | 51716 | 34.159.167.110 | 443 | 10 | 640 bytes | 12 | 5 | 295 bytes | 5 | 345 bytes | 27.784035 | 30.1728 | 78 |
| 20.198.118.190 | 443 | 192.168.181.113 | 51700 | 3 | 673 bytes | 13 | 2 | 486 bytes | 1 | 187 bytes | 28.075202 | 0.1437 | 27 |
| 192.168.181.113 | 51718 | 111.119.184.209 | 443 | 7 | 380 bytes | 14 | 4 | 218 bytes | 3 | 162 bytes | 28.304989 | 48.7395 | 35 |
| 192.168.181.113 | 51736 | 157.240.227.61 | 443 | 61 | 12 kB | 15 | 27 | 2 kB | 34 | 10 kB | 28.423005 | 4.0036 | 4485 |
| 192.168.181.113 | 51719 | 121.91.41.83 | 443 | 7 | 380 bytes | 16 | 4 | 218 bytes | 3 | 162 bytes | 28.888005 | 48.1572 | 36 |
| 192.168.181.113 | 51720 | 121.91.40.83 | 443 | 7 | 380 bytes | 17 | 4 | 218 bytes | 3 | 162 bytes | 29.157989 | 47.8872 | 36 |
| 192.168.181.113 | 51740 | 157.240.227.60 | 443 | 131 | 71 kB | 18 | 69 | 5 kB | 62 | 66 kB | 33.524863 | 1028.9215 | 36 |
| 192.168.181.113 | 51739 | 163.70.137.60 | 443 | 32 | 6 kB | 19 | 20 | 2 kB | 12 | 4 kB | 33.524863 | 1042.8886 | 13 |
| 192.168.181.113 | 51741 | 157.240.227.60 | 443 | 30 | 6 kB | 20 | 18 | 2 kB | 12 | 4 kB | 33.525438 | 1037.2727 | 12 |
| 192.168.181.113 | 51742 | 163.70.132.60 | 443 | 32 | 6 kB | 21 | 20 | 2 kB | 12 | 4 kB | 33.525548 | 1046.4446 | 13 |
| 192.168.181.113 | 51743 | 121.91.41.99 | 443 | 28 | 6 kB | 22 | 18 | 1 kB | 10 | 4 kB | 33.526014 | 1029.7010 | 11 |
| 192.168.181.113 | 51744 | 111.119.184.224 | 443 | 47 | 8 kB | 23 | 26 | 2 kB | 21 | 5 kB | 33.526182 | 1029.9067 | 17 |
| 192.168.181.113 | 51745 | 157.240.227.60 | 443 | 28 | 5 kB | 24 | 19 | 2 kB | 9 | 4 kB | 33.526353 | 1034.9097 | 11 |
| 192.168.181.113 | 51746 | 121.91.41.99 | 443 | 47 | 8 kB | 25 | 26 | 2 kB | 21 | 5 kB | 33.526607 | 1029.8896 | 17 |
| 192.168.181.113 | 51747 | 121.91.40.99 | 443 | 29 | 6 kB | 26 | 19 | 2 kB | 10 | 4 kB | 33.526853 | 1029.4525 | 11 |
| 192.168.181.113 | 51748 | 111.119.184.224 | 443 | 28 | 6 kB | 27 | 18 | 1 kB | 10 | 4 kB | 33.527173 | 1029.7172 | 11 |
| 192.168.181.113 | 51749 | 121.91.41.99 | 443 | 29 | 6 kB | 28 | 19 | 2 kB | 10 | 4 kB | 33.527535 | 1029.7169 | 11 |
| 192.168.181.113 | 51750 | 121.91.40.99 | 443 | 42 | 7 kB | 29 | 23 | 2 kB | 19 | 5 kB | 33.527989 | 1024.6408 | 16 |
| 192.168.181.113 | 51751 | 111.119.184.224 | 443 | 29 | 6 kB | 30 | 19 | 2 kB | 10 | 4 kB | 33.528381 | 1029.8877 | 11 |
| 192.168.181.113 | 51752 | 121.91.41.99 | 443 | 30 | 6 kB | 31 | 19 | 2 kB | 11 | 4 kB | 33.528715 | 1024.6402 | 11 |
| 192.168.181.113 | 51753 | 121.91.40.99 | 443 | 30 | 6 kB | 32 | 19 | 2 kB | 11 | 4 kB | 33.529749 | 1031.7567 | 11 |
| 192.168.181.113 | 51754 | 111.119.184.224 | 443 | 30 | 6 kB | 33 | 20 | 2 kB | 10 | 4 kB | 33.529934 | 1029.4495 | 12 |
| 192.168.181.113 | 51755 | 121.91.40.99 | 443 | 28 | 6 kB | 34 | 18 | 1 kB | 10 | 4 kB | 33.530101 | 1028.3380 | 11 |
| 192.168.181.113 | 51756 | 157.240.227.61 | 5222 | 30 | 3 kB | 35 | 13 | 1 kB | 17 | 2 kB | 33.597778 | 15.0434 | 608 |
| 192.168.181.113 | 51717 | 157.240.227.13 | 443 | 9 | 526 bytes | 36 | 5 | 271 bytes | 4 | 255 bytes | 37.536979 | 21.3089 | 101 |
| 192.168.181.113 | 51726 | 20.212.88.117 | 443 | 12 | 855 bytes | 37 | 10 | 723 bytes | 2 | 132 bytes | 40.740910 | 92.1950 | 62 |

WIRESHARK FILTERS:

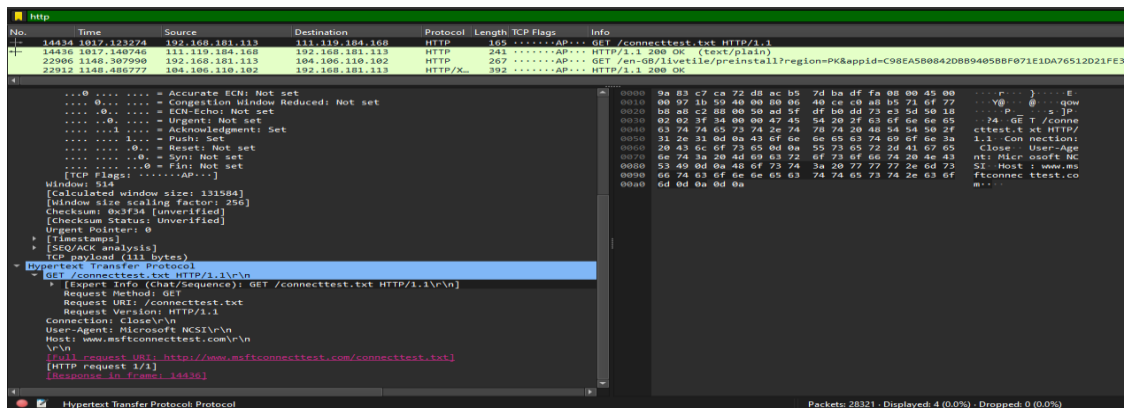
FACEBOOK:

HTTP PACKETS:

Total displayed = 4 Packets

Filter: http

The filter **http** is applied to display HTTP packets, revealing a total of 4 packets in the captured network traffic



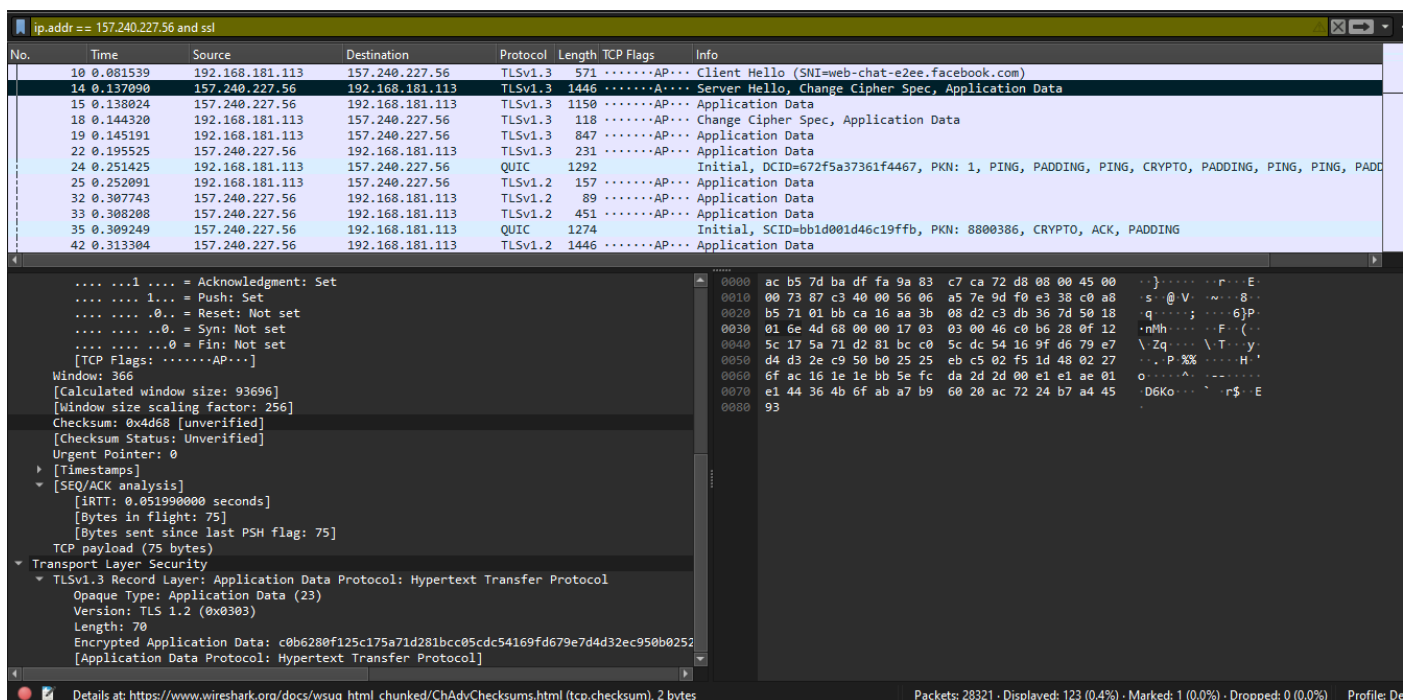
SSL PACKETS:

The filter **ip.addr == 157.240.227.56 and ssl** is used to capture SSL packets associated with the IP address **157.240.227.56**. In the captured data, 123 bytes are displayed, constituting **0.4%** of the total traffic.

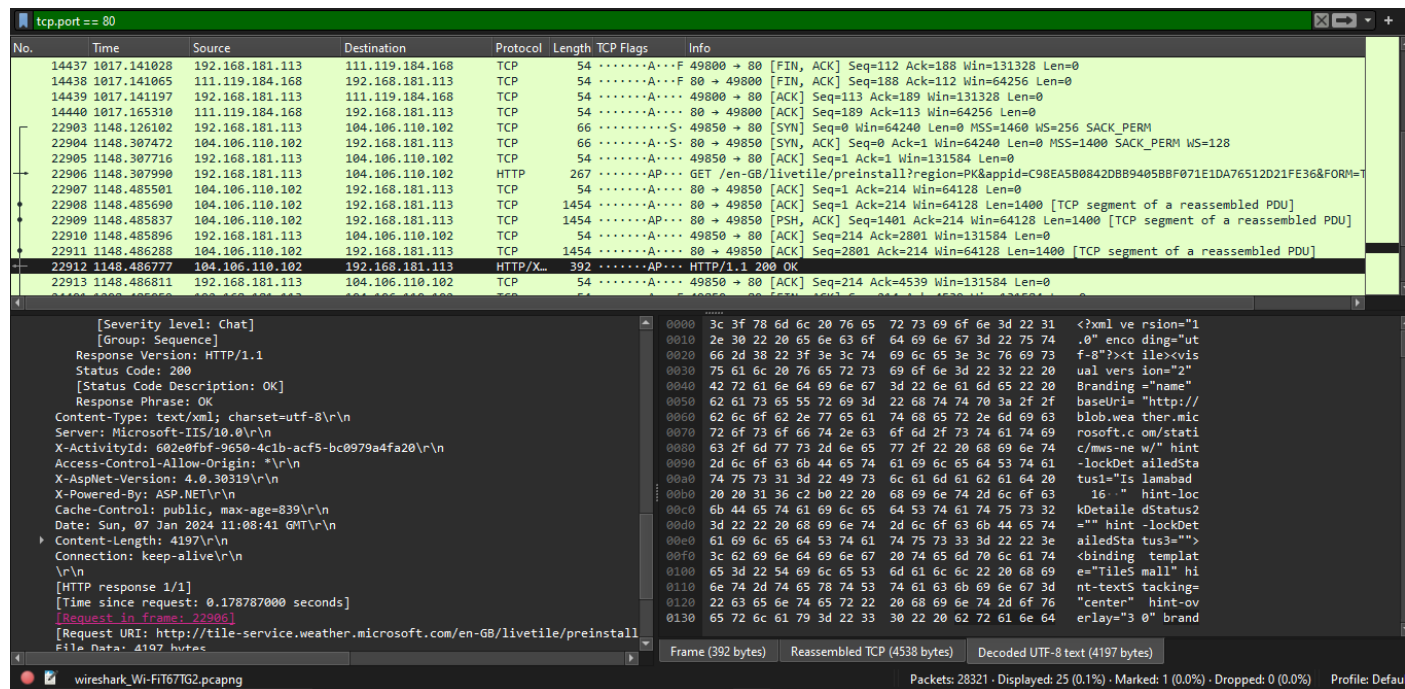
ip.addr == 157.240.227.56 and ssl

Displayed: 123 bytes

Fraction: 0.4%



Then use display filters to separate the subset of TCP packets that are also HTTP packets.

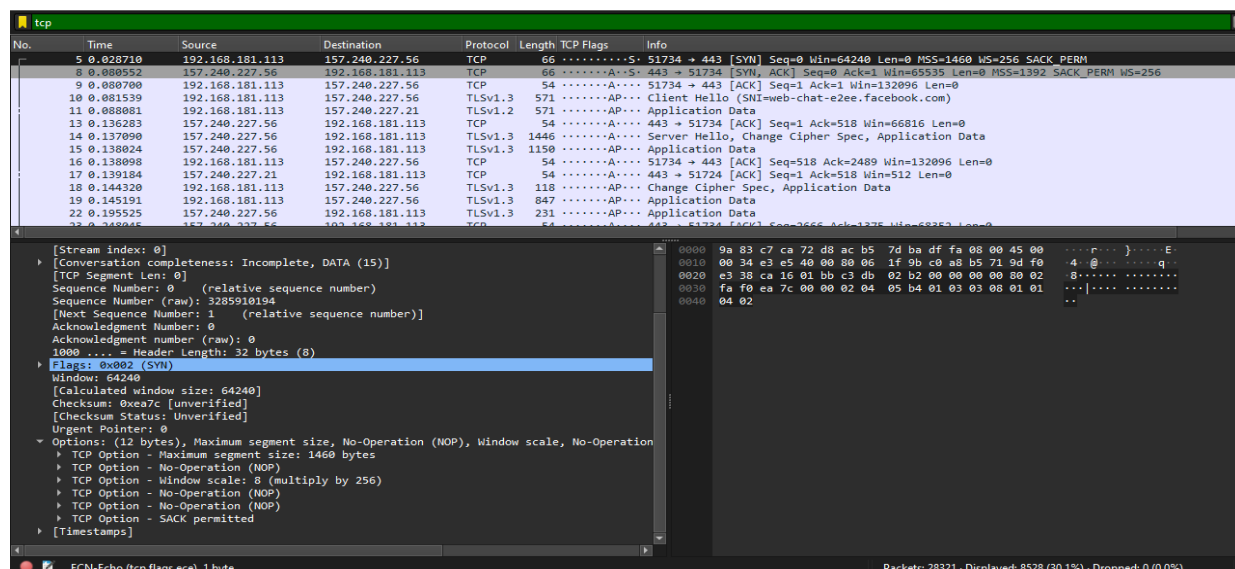


Displayed: 25 bytes

Fraction: 0.1%

TCP to/from Facebook:

The filter `tcp` is applied to capture TCP packets to and from the IP address 157.240.227.56. In total, 8528 packets matching this filter are displayed in the captured network traffic.



Filter from src to destination:

FROM MY PC TO FACEBOOK:

The filter `tcp and ip.src == 192.168.181.113 && ip.dst == 157.240.227.56` is applied to capture TCP packets sent from your computer (source IP: 192.168.181.113) to Facebook (destination IP: 157.240.227.56). A total of 148 packets matching this filter are displayed, constituting 0.5% of the total traffic.

tcp and ip.src == 192.168.181.113 && ip.dst == 157.240.227.56

Total displayed: 148

Fraction: 0.5%

| No. | Time | Source | Destination | Protocol | Length | TCP Flags | Info |
|-----|----------|-----------------|----------------|----------|--------|------------|---|
| 5 | 0.028710 | 192.168.181.113 | 157.240.227.56 | TCP | 66 |S. | 51734 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 9 | 0.080700 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51734 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0 |
| 10 | 0.081539 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 571 |AP... | Client Hello (SNI=web-chat-e2ee.facebook.com) |
| 16 | 0.138098 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51734 → 443 [ACK] Seq=518 Ack=2489 Win=132096 Len=0 |
| 18 | 0.144320 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 118 |AP... | Change Cipher Spec, Application Data |
| 19 | 0.145191 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 847 |AP... | Application Data |
| 25 | 0.252091 | 192.168.181.113 | 157.240.227.56 | TLSv1.2 | 157 |AP... | Application Data |
| 29 | 0.298261 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51734 → 443 [ACK] Seq=1375 Ack=2606 Win=131840 Len=0 |
| 34 | 0.308250 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=433 Win=514 Len=0 |
| 43 | 0.313478 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=3217 Win=516 Len=0 |
| 52 | 0.328578 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=11569 Win=516 Len=0 |
| 58 | 0.340314 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=17137 Win=516 Len=0 |
| 62 | 0.346354 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=19921 Win=516 Len=0 |
| 66 | 0.359048 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=24097 Win=516 Len=0 |
| 69 | 0.362379 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=26881 Win=516 Len=0 |
| 71 | 0.365585 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=28273 Win=516 Len=0 |
| 74 | 0.369367 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=31057 Win=516 Len=0 |
| 82 | 0.375434 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=33841 Win=516 Len=0 |
| 85 | 0.463556 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=36625 Win=516 Len=0 |
| 88 | 0.463877 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=39409 Win=516 Len=0 |
| 91 | 0.464232 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=42193 Win=516 Len=0 |
| 94 | 0.464600 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=44977 Win=516 Len=0 |
| 97 | 0.464896 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=47761 Win=516 Len=0 |
| 100 | 0.465273 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=50545 Win=516 Len=0 |
| 103 | 0.465635 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=53329 Win=516 Len=0 |
| 106 | 0.466014 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=56113 Win=516 Len=0 |
| 109 | 0.466399 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=58897 Win=516 Len=0 |
| 112 | 0.466748 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=61681 Win=516 Len=0 |
| 115 | 0.467112 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A.... | 51732 → 443 [ACK] Seq=104 Ack=64465 Win=516 Len=0 |

Handshake Type: Client Hello (1)

Length: 508

Version: TLS 1.2 (0x0303)

Random: 04bf18131d0d3a70ac6361a6b354ed7c6ec99aaef3cd776e1b89c61022808be

Session ID Length: 32

Session ID: f487d4d274cbc5456cfc447518edae4ae370c75274735669f71bcc23c95c57396

Cipher Suites Length: 32

Cipher Suites (16 suites)

0010 02 2d e3 e7 40 00 00 06 1d a0 c0 a8 b5 71 9d f0 @ q

0020 e3 38 ca 16 01 bb c3 db 02 b3 a4 3a fc 35 50 18 8 : 5P

0030 02 04 f9 27 00 00 16 03 01 02 00 01 00 01 fc 03 6 k5N

0040 03 04 bf a1 31 31 d0 d3 a7 0a c6 36 1a 6b 35 4e 'L TV -GQ

0050 d7 c6 ec 99 aa ef 3c d7 76 e1 b8 9c 61 02 28 08 7 u'G5 f q <

0060 be 20 f4 87 d4 27 4c bc 54 56 cf c4 47 51 8e da s + /

0070 e4 ae 37 0c 75 27 47 35 66 9f 71 bc c2 3c 95 c5 , 0

0080 73 96 00 20 0a 0a 13 01 13 02 13 03 c0 2b c0 2f

0090 c0 2c c0 30 cc a9 cc a8 c0 13 c0 14 00 9c 00 9d

From Facebook to Computer:

The filter `tcp and ip.src == 157.240.227.56 && ip.dst == 192.168.181.113` is used to capture TCP packets sent from Facebook (source IP: 157.240.227.56) to your computer (destination IP: 192.168.181.113). A total of 186 packets matching this filter are displayed, constituting 0.7% of the total traffic.

tcp and ip.src == 157.240.227.56 && ip.dst == 192.168.181.113

Total Displayed: 186 (0.7%)

The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. The filter bar at the top shows the filter: `tcp and ip.src == 157.240.227.56 && ip.dst == 192.168.181.113`. The packet list shows various protocols including TCP, TLSv1.3, and TLSv1.2. The bottom pane shows a detailed view of a selected packet (No. 10), which is a TCP segment. The details pane shows the following information:

- [TCP Segment Len: 0]
- Sequence Number: 0 (relative sequence number)
- Sequence Number (raw): 2855992372
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 3285910195
- 1000 = Header Length: 32 bytes (8)
- Flags: 0x012 (SYN, ACK)
- Window: 65535
- [Calculated window size: 65535]
- Checksum: 0x3f31 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK p
- TCP Option - Maximum segment size: 1392 bytes
- TCP Option - No-Operation (NOP)
- TCP Option - No-Operation (NOP)
- TCP Option - SACK permitted
- TCP Option - No-Operation (NOP)
- TCP Option - Window scale: 8 (multiply by 256)
- [Timestamps]
- [SEQ/ACK analysis]

The packet bytes pane shows the raw data of the TCP segment, including the header and options.

HTTP to/from facebook:

The filter ``ip.addr == 157.240.227.56 && tcp.port == 443`` is applied to capture HTTP packets to and from Facebook on port 443 (HTTPS). A total of 334 packets matching this filter are displayed, constituting **1.2%** of the total traffic. The source port is 51734, and the destination port is 443.

Total displayed: **334 packets (1.2%)**

The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. The filter bar at the top shows the filter: `ip.addr == 157.240.227.56 && tcp.port == 443`. The packet list shows various protocols including TCP, TLSv1.3, and TLSv1.2. The bottom pane shows a detailed view of a selected packet (No. 10), which is a TLSv1.3 Client Hello packet. The details pane shows the following information:

- Internet Protocol Version 4, Src: 192.168.181.113, Dst: 157.240.227.56
- Transmission Control Protocol, Src Port: 51734, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
- Source Port: 51734
- Destination Port: 443
- [Stream index: 0]
- [Conversation completeness: Incomplete, DATA (15)]
- [TCP Segment Len: 517]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 3285910195
- [Next Sequence Number: 518 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 2855992373
- 0101 = Header Length: 20 bytes (5)
- Flags: 0x018 (PSH, ACK)
- Window: 516
- [Calculated window size: 132096]
- [Window size scaling factor: 256]

The packet bytes pane shows the raw data of the TLSv1.3 Client Hello packet, including the header and the Client Hello message.

Conversation filter between pc to Facebook:

ip.addr eq 192.168.181.113 and ip.addr eq 157.240.227.56

| ip.addr eq 192.168.181.113 and ip.addr eq 157.240.227.56 | | | | | | | | | |
|--|----------|-----------------|-----------------|----------|--------|------------|--|--|--|
| No. | Time | Source | Destination | Protocol | Length | TCP Flags | Info | | |
| 5 | 0.028710 | 192.168.181.113 | 157.240.227.56 | TCP | 66 |S. | 51734 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM | | |
| 8 | 0.080552 | 157.240.227.56 | 192.168.181.113 | TCP | 66 |A..S. | 443 → 51734 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1392 SACK_PERM WS=256 | | |
| 9 | 0.080700 | 192.168.181.113 | 157.240.227.56 | TCP | 54 |A... | 51734 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0 | | |
| 10 | 0.081539 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 571 |AP... | Client Hello (SNI=web-chat-e2ee.facebook.com) | | |
| 13 | 0.136283 | 157.240.227.56 | 192.168.181.113 | TCP | 54 |A... | 443 → 51734 [ACK] Seq=1 Ack=518 Win=66816 Len=0 | | |
| 14 | 0.137090 | 157.240.227.56 | 192.168.181.113 | TLSv1.3 | 1446 |A... | Server Hello, Change Cipher Spec, Application Data | | |
| 15 | 0.138024 | 157.240.227.56 | 192.168.181.113 | TLSv1.3 | 1150 |AP... | Application Data | | |

TLSv1.3 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 122

Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 118

Version: TLS 1.2 (0x0303)

Random: ddb7e4dc20817882da7672cab9beb9037a9c10b41b1cdfc9d1e0578a3c712b8

Session ID Length: 32

Session ID: f487d4274cbc5456cfc447518edae4ae370c7527435669f71bcc23c95c57396

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

Compression Method: null (0)

Extensions Length: 46

Extension: supported_versions (len=2) TLS 1.3

Extension: key_share (len=36) x25519

[JA3S Fullstring: 771,4865,43-51]

[JA3S: f4febcs5ea12b31ae17cfb7e614afda8]

TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec

Content Type: Change Cipher Spec (20)

Version: TLS 1.2 (0x0303)

Length: 1

Change Cipher Spec Message

TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol

Opaque Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 1817

Encrypted Application Data [truncated]: 0104bdf410f4f5a3685320b8c7c41f20cf0516499b0

[Application Data Protocol: Hypertext Transfer Protocol]

TLS segment data (237 bytes)

0020 b5 71 01 bb ca 16 aa 3a fc 35 c3 db 04 b8 50 10

0030 01 05 51 ed 00 00 16 03 03 00 7a 02 00 00 76 03

0040 03 db b7 e4 dc 20 81 78 82 da 76 72 ca b9 be b9

0050 03 7a 79 c1 0b 41 b1 cd fc 9d 1e 05 78 a3 c7 12

0060 b8 20 f4 87 d4 27 4c bc 54 56 cf c4 47 51 8e da

0070 e4 ae 37 0c 75 27 47 35 66 9f 71 bc c2 3c 95 c5

0080 73 96 13 01 00 00 2e 00 2b 00 02 03 04 00 33 00

0090 24 00 1d 00 20 9a 28 31 ed 0c 81 a4 78 a4 e4 81

00a0 ba 39 df 3b 10 8f 28 02 e4 4d db 0b cf 48 30 f9

00b0 30 7c be ba 51 14 03 03 00 01 01 17 03 03 03 f9

00c0 01 04 bd f4 10 1f 4f 5a 36 85 32 0b 8c 7c 41 f2

00d0 0c fd 05 16 49 9b b1 09 8f 7a 95 ee cf bc c0 e8

00e0 d1 78 93 e0 ab a5 3e 30 b7 b1 cb 0b b8 5b d9 00

00f0 0a 8b b8 74 8c 94 70 98 41 86 31 6a 66 d3 c0

0100 f5 38 ff 5f bc ab c0 24 ce e2 48 05 41 46 d5 1e

0110 43 a5 23 2b a4 15 72 ba c3 95 e3 35 d4 50 fc c6

0120 f3 5d e0 1d 06 c3 6d a6 dc 9b 05 67 6f a7 6b 73

0130 f6 5f 9e 57 b2 91 5a 5b 2f 21 d0 c3 80 09 56 f6

0140 11 81 8d 95 5c 0b 24 e2 f9 10 55 37 d0 1c 87 4f

0150 33 1b a0 6c 41 03 46 b6 4e 25 60 71 13 4b af 48

0160 b3 ee 6d ea 96 ed fe 39 85 71 f3 2b f5 20 5a 2c

0170 de 6f e1 f2 60 80 a0 56 6c 48 77 da ba d4 1f 9b

0180 cd 40 71 bf 76 a7 6f 81 dd 0f b4 6c fb 14 90 57

0190 0c 1b 63 b6 cd 56 4f 7f 90 ed 74 94 28 d3 ff 99

01a0 98 c4 12 44 e6 23 92 8f 5c 45 11 0b 96 8d a4 92

01b0 42 99 e6 74 d8 e1 53 08 89 2a e0 9a 2e ff dc

01c0 4d df 91 f8 88 1d ad 1d 55 98 c2 3e 18 b5 2c ed

01d0 6c c9 83 00 d7 41 12 70 fd 96 0a ea cb 2f b9 c7

01e0 7f 07 f9 aa 36 91 6e 7b 88 92 c4 ec 2e b5 c1 b0

01f0 ba 4e 55 72 96 b5 49 1d 80 ea c0 0f a4 83 bf 0d

FLAGS:

The filter **ip.addr == 157.240.227.56 and tcp.analysis.flags** in Wireshark is designed to display TCP packets to and from the IP address 157.240.227.56 while also showing additional information related to TCP flags analysis.

| ip.addr == 157.240.227.56 and tcp.analysis.flags | | | | | | | | | |
|--|------------|-----------------|-----------------|----------|--------|------------|---|--|--|
| No. | Time | Source | Destination | Protocol | Length | TCP Flags | Info | | |
| 6949 | 38.792743 | 157.240.227.56 | 192.168.181.113 | TCP | 125 |AP... | [TCP Spurious Retransmission] 443 → 51734 [PSH, ACK] Seq=3600 Ack=13406 Win=93696 Len=71 | | |
| 6950 | 38.792806 | 192.168.181.113 | 157.240.227.56 | TCP | 66 |A... | [TCP Dup ACK 6948#1] 51734 → 443 [ACK] Seq=13406 Ack=3671 Win=130816 Len=0 SLE=3600 SRE=3 | | |
| 7093 | 45.538132 | 192.168.181.113 | 157.240.227.56 | TCP | 55 |A... | [TCP Keep-Alive] 51732 → 443 [ACK] Seq=103 Ack=93967 Win=516 Len=1 | | |
| 7096 | 45.773273 | 157.240.227.56 | 192.168.181.113 | TCP | 54 |A... | [TCP Keep-Alive ACK] 443 → 51732 [ACK] Seq=93967 Ack=104 Win=265 Len=0 | | |
| 13375 | 131.768622 | 192.168.181.113 | 157.240.227.56 | TCP | 123 |AP... | [TCP Retransmission] 51734 → 443 [PSH, ACK] Seq=13612 Ack=3961 Win=132096 Len=69 | | |

Frame 6950: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF...
Ethernet II, Src: liteonTechno ba:d5:fa (ac:b5:7d:ba:d5:fa), Dst: 9a:83:c7:ca:72:d8 (9a:83:c7:ca:72:d8)
Internet Protocol Version 4, Src: 192.168.181.113, Dst: 157.240.227.56
Transmission Control Protocol, Src Port: 51734, Dst Port: 443, Seq: 13406, Ack: 3671, Len: 0
Source Port: 51734
Destination Port: 443
[Stream index: 0]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 13406 (relative sequence number)
Sequence Number (raw): 3285923600
[Next Sequence Number: 13406 (relative sequence number)]
Acknowledgment Number: 3671 (relative ack number)
Acknowledgment number (raw): 2855996043
1000 = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window: 511
[Calculated window size: 130816]
[Window size scaling factor: 256]
Checksum: 0x9bb0 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), SACK
TCP Option - No-Operation (NOP)
TCP Option - No-Operation (NOP)
TCP Option - SACK 3600-3671
[Timestamps]
[Seq/Ack analysis]

0000 9a 83 c7 ca 72 d8 ac b5 7d ba df fa 00 00 45 00

0010 00 34 e4 85 40 00 80 06 1e fb c0 a8 b5 71 9d f0

0020 e3 38 ca 16 01 bb c3 db 37 10 aa 3b 0a 8b 80 10

0030 01 ff 9b b0 00 00 01 01 05 0a aa 3b 0a 44 aa 3b

0040 0a 8b

Source Port (tcp.srcport), 2 bytes

Packets: 28321 - Displayed: 5 (0.0%) - Dropped: 0 (0.0%)

SYN FLAG:

The filter `ip.addr == 157.240.227.56 and tcp.flags.syn == 1` is used to capture TCP packets with the SYN flag set sent to or from the IP address 157.240.227.56. A total of 4 packets matching this filter are displayed, constituting 0.0% of the total 28321 SYN-flagged packets.

`ip.addr == 157.240.227.56 and tcp.flags.syn == 1`

Displayed: 4 packets

Fraction: 0.0% because total are 28321

The image shows a Wireshark packet capture interface. The top bar displays the filter `ip.addr == 157.240.227.56 and tcp.flags.syn == 1`. The packet list shows four packets, with the third packet (No. 8) selected. The packet details pane shows the following information:

- Ethernet II, Src: 9a:83:c7:ca:72:d8 (9a:83:c7:ca:72:d8), Dst: LiteonTechno_ba:df:fa (ac:b5:40:00:00:00)
- Internet Protocol Version 4, Src: 157.240.227.56, Dst: 192.168.181.113
- Transmission Control Protocol, Src Port: 443, Dst Port: 51734, Seq: 0, Ack: 1, Len: 0
 - Source Port: 443
 - Destination Port: 51734
 - [Stream index: 0]
 - [Conversation completeness: Incomplete, DATA (15)]
 - [TCP Segment Len: 0]
 - Sequence Number: 0 (relative sequence number)
 - Sequence Number (raw): 2855992372
 - [Next Sequence Number: 1 (relative sequence number)]
 - Acknowledgment Number: 1 (relative ack number)
 - Acknowledgment number (raw): 3285910195
 - 1000 = Header Length: 32 bytes (8)
 - Flags: 0x012 (SYN, ACK)
 - Window: 65535
 - [Calculated window size: 65535]
 - Checksum: 0x3f31 [unverified]
 - [Checksum Status: Unverified]
 - Urgent Pointer: 0
 - Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK
 - TCP Option - Maximum segment size: 1392 bytes
 - TCP Option - No-Operation (NOP)
 - TCP Option - No-Operation (NOP)
 - TCP Option - SACK permitted
 - TCP Option - No-Operation (NOP)
 - TCP Option - Window scale: 8 (multiply by 256)
 - [Timestamps]
 - [SEQ/ACK analysis]
 - [This is an ACK to the segment in frame: 5]
 - [The RTT to ACK the segment was: 0.051842000 seconds]
 - [iRTT: 0.051990000 seconds]

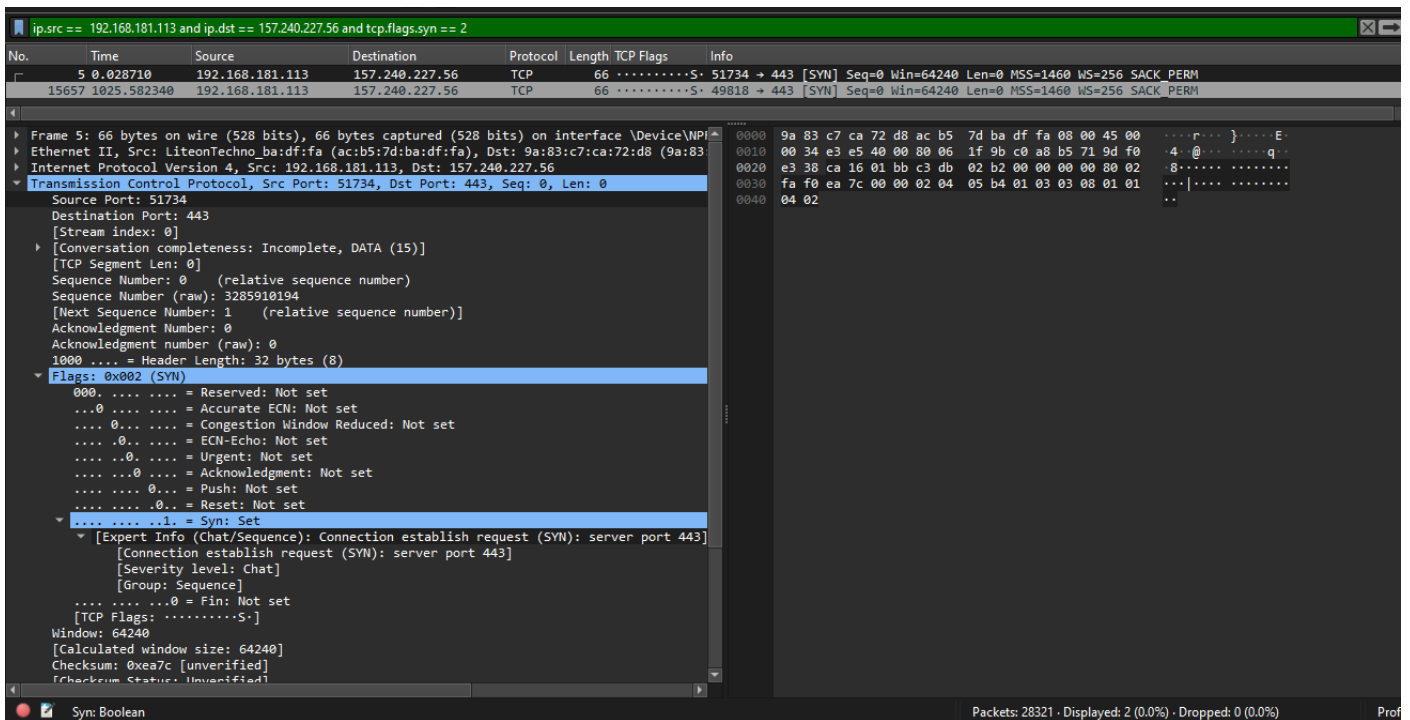
The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, and TCP header.

From Pc to Facebook:

`ip.src == 192.168.181.113 and ip.dst == 157.240.227.56 and tcp.flags.syn == 2`
`ip.src == 192.168.181.113 and ip.dst == 157.240.227.56 and tcp.flags.syn == 3`

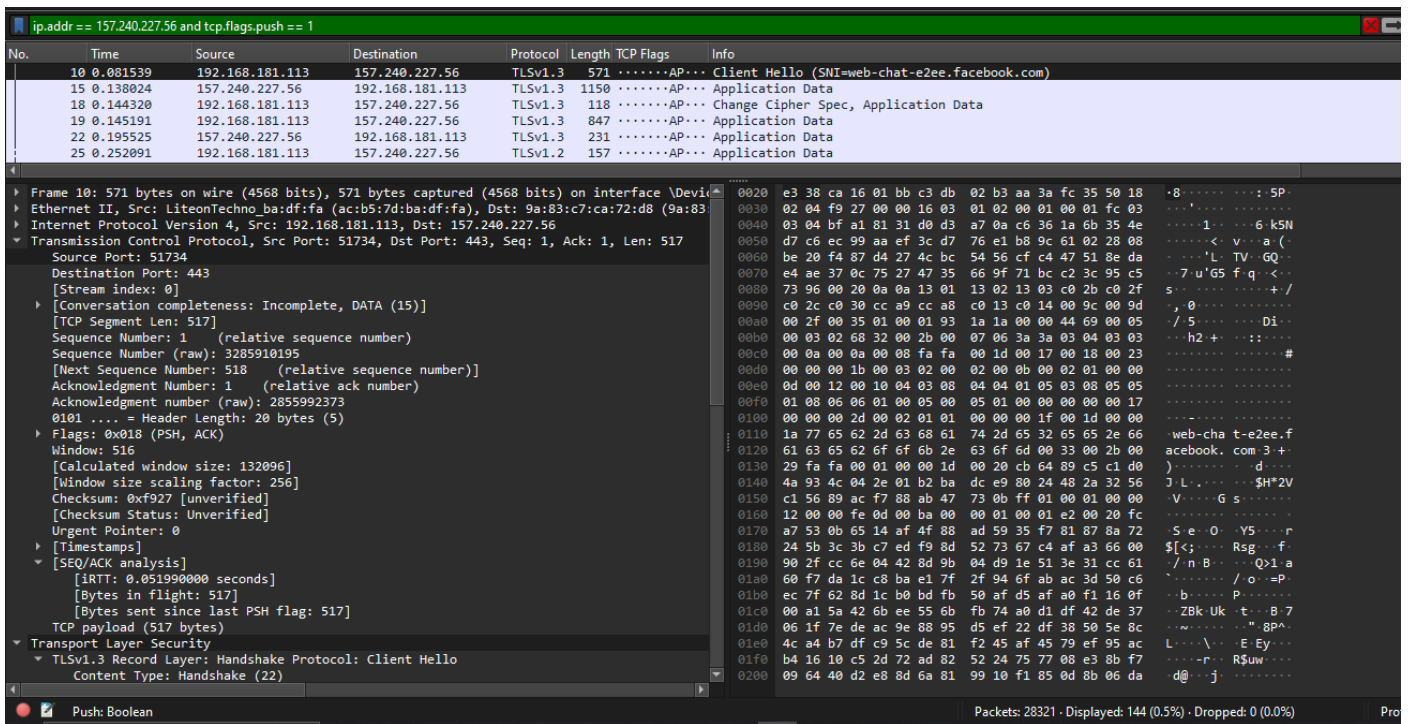
Displayed: 2

Fraction: 0.2 %



PUSH FLAG:

The filter `ip.addr == 157.240.227.56 and tcp.flags.push == 1` is applied to capture TCP packets with the PUSH flag set sent to or from the IP address 157.240.227.56. A total of 144 packets matching this filter are displayed, constituting 0.5% of the total traffic.



**ip.addr == 157.240.227.56 and
tcp.flags.push == 1**

Displayed packets: 144

Fraction: 0.5%

From PC to Facebook:

**ip.src == 192.168.181.113 and ip.dst ==
157.240.227.56 and tcp.flags.push == 3**

**ip.src == 192.168.181.113 and ip.dst ==
157.240.227.56 and tcp.flags.push == 2**

Displayed: 53

Fraction: 0.2%

ip.src == 192.168.181.113 and ip.dst == 157.240.227.56 and tcp.flags.push == 3

| No. | Time | Source | Destination | Protocol | Length | TCP Flags | Info |
|-------|-------------|-----------------|----------------|----------|--------|------------|--|
| 10 | 0.081539 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 571 |AP... | Client Hello (SNI=web-chat-e2ee.facebook.com) |
| 18 | 0.144320 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 118 |AP... | Change Cipher Spec, Application Data |
| 19 | 0.145191 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 847 |AP... | Application Data |
| 25 | 0.252091 | 192.168.181.113 | 157.240.227.56 | TLSv1.2 | 157 |AP... | Application Data |
| 505 | 1.844489 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 125 |AP... | Application Data |
| 633 | 2.802037 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 172 |AP... | Application Data |
| 634 | 2.816537 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 107 |AP... | Application Data |
| 642 | 2.816820 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 560 |AP... | Application Data |
| 828 | 3.433614 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 132 |AP... | Application Data |
| 6945 | 38.084544 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 123 |AP... | Application Data |
| 7126 | 46.784657 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 122 |AP... | Application Data |
| 8593 | 62.924739 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 123 |AP... | Application Data |
| 12645 | 89.173826 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 123 |AP... | Application Data |
| 13336 | 126.957529 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 123 |AP... | Application Data |
| 13375 | 131.768622 | 192.168.181.113 | 157.240.227.56 | TCP | 123 |AP... | [TCP Retransmission] 51734 → 443 [PSH, ACK] Seq=13612 Ack=3961 Win=132096 Len=69 |
| 15784 | 1025.820016 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 750 |AP... | Client Hello (SNI=web-chat-e2ee.facebook.com) |
| 15876 | 1025.990342 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 118 |AP... | Change Cipher Spec, Application Data |
| 15921 | 1026.028381 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 935 |AP... | Application Data |
| 16203 | 1026.700641 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 125 |AP... | Application Data |
| 16262 | 1027.072268 | 192.168.181.113 | 157.240.227.56 | TLSv1.3 | 172 |AP... | Application Data |

Frame 633: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits) on interface \Device\NPF...
Ethernet II, Src: LiteonTechno_ba:df:fa (ac:b5:7d:ba:df:fa), Dst: 9a:83:c7:ca:72:d8 (9a:83:c7:ca:72:d8)
Internet Protocol Version 4, Src: 192.168.181.113, Dst: 157.240.227.56
Transmission Control Protocol, Src Port: 51734, Dst Port: 443, Seq: 2838, Ack: 3230, Len: 118
Source Port: 51734
Destination Port: 443
[Stream index: 0]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 118]
Sequence Number: 2838 (relative sequence number)
Sequence Number (raw): 3285913032
[Next Sequence Number: 2956 (relative sequence number)]
Acknowledgment Number: 3230 (relative ack number)
Acknowledgment number (raw): 2855995602
0101 ... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 513

Frame (172 bytes) Reassembled TCP (1510 bytes)

Packets: 28321 · Displayed: 53 (0.2%) · Dropped: 0 (0.0%) Profile: Default

Reset:

The filter **ip.addr == 157.240.227.56 and tcp.flags.reset == 1** is used to capture TCP packets with the Reset (RST) flag set sent to or from the IP address 157.240.227.56. However, in the provided analysis, no packets matching this filter are displayed, indicating that there are no TCP packets with the RST flag set in the specified communication with Facebook.

Reset flag does not display any packets.

```
ip.addr == 157.240.227.56 and  
tcp.flags.reset == 1
```

From Computer to the Facebook:

```
ip.src == 192.168.181.113 and ip.dst ==  
157.240.227.56 and tcp.flags.reset == 1  
ip.src == 192.168.181.113 and ip.dst ==  
157.240.227.56 and tcp.flags.reset == 2  
ip.src == 192.168.181.113 and ip.dst ==  
157.240.227.56 and tcp.flags.reset == 3  
0 displayed
```

Facebook Statistics for Set Flags:

| FLAGS | COUNT | FRACTION |
|--------------|--------------|-----------------|
| SYN | 4 | 0.0% |
| PSH | 144 | 0.5% |
| RST | 0 | 0% |

From YouTube:

Capture Properties:

Name: E:\University\Smester 5\computer network\youtube.pcapng

Length: 219 MB

Hash c3970028d87fc75da568d7c704729c83462ef91bdf96daf5975a1afd
(SHA256): 298c70a2

Hash 2aa2ce529f2f39f6be8ef4ee05cd17f083cdd56c
(SHA1):

Format: Wireshark/... - pcapng

Encapsulation: Ethernet

Time

First packet: 2024-01-08 20:31:07

Last packet: 2024-01-08 21:02:26

Elapsed: 00:31:18

Capture

Hardware: AMD A8-4500M APU with Radeon(tm) HD Graphics (with SSE4.2)

OS: 64-bit Windows 10 (22H2), build 19045

Application: Dumpcap (Wireshark) 4.2.0 (v4.2.0-0-g54eedfc63953)

Interfaces

| <u>Interface</u> | <u>Dropped packets</u> | <u>Capture filter</u> | <u>Link type</u> | <u>Packet size limit (snaplen)</u> |
|------------------|------------------------|-----------------------|------------------|------------------------------------|
| Wi-Fi | 0 (0.0%) | none | Ethernet | 262144 bytes |

Statistics

| <u>Measurement</u> | <u>Captured</u> | <u>Displayed</u> | <u>Marked</u> |
|------------------------|-----------------|-----------------------|---------------|
| Packets | 208212 | 208212 (100.0%) | — |
| Time span, s | 1878.976 | 1878.976 | — |
| Average pps | 110.8 | 110.8 | — |
| Average packet size, B | 1020 | 1020 | — |
| Bytes | 212411107 | 212411107 (100.0%) | 0 |
| Average bytes/s | 113 k | 113 k | — |
| Average bits/s | 904 k | 904 k | — |

HTTP Protocol Filter for YouTube:

1. http

You'll notice that all the packets in the list show HTTP for the protocol.

To display all the HTTP traffic you need to use the following protocol and port display filter:

```
tcp.dstport == 80
```


http

| No. | Time | Source | Destination | Protocol | Length | TCP Flags | Info |
|-------|------------|-----------------|-----------------|-----------|--------|------------|--|
| 2766 | 38.610475 | 192.168.181.113 | 23.207.193.174 | HTTP/X... | 326 |AP... | POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1 |
| 4605 | 59.928373 | 192.168.181.113 | 23.207.193.174 | HTTP/X... | 326 |AP... | POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1 |
| 9290 | 81.242257 | 192.168.181.113 | 23.207.193.174 | HTTP/X... | 326 |AP... | POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1 |
| 15129 | 102.939662 | 192.168.181.113 | 23.207.193.174 | HTTP/X... | 714 |AP... | POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1 |
| 15159 | 103.112363 | 23.207.193.174 | 192.168.181.113 | HTTP | 350 |AP... | [TCP Fast Retransmission] HTTP/1.1 302 Moved Temporarily |
| 20451 | 127.534252 | 192.168.181.113 | 23.207.193.174 | HTTP/X... | 270 |AP... | POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1 |
| 20474 | 127.676821 | 23.207.193.174 | 192.168.181.113 | HTTP | 350 |AP... | HTTP/1.1 302 Moved Temporarily |
| 24446 | 149.289431 | 192.168.181.113 | 23.207.193.174 | HTTP/X... | 1298 |AP... | POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1 |
| 24460 | 149.439402 | 23.207.193.174 | 192.168.181.113 | HTTP | 350 |AP... | HTTP/1.1 302 Moved Temporarily |
| 36144 | 170.950672 | 192.168.181.113 | 23.207.193.174 | HTTP/X... | 326 |AP... | POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1 |
| 39114 | 192.346551 | 192.168.181.113 | 23.207.193.174 | HTTP/X... | 78 |AP... | POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1 |
| 39168 | 192.503548 | 23.207.193.174 | 192.168.181.113 | HTTP | 350 |AP... | HTTP/1.1 302 Moved Temporarily |
| 60461 | 358.230122 | 111.119.184.19 | 192.168.181.113 | HTTP | 220 |AP... | HTTP/1.1 204 No Content |
| 60462 | 358.230974 | 192.168.181.113 | 111.119.184.19 | HTTP | 78 |AP... | Continuation |
| 60723 | 359.033385 | 111.119.184.19 | 192.168.181.113 | HTTP | 220 |AP... | HTTP/1.1 204 No Content |
| 60724 | 359.033906 | 192.168.181.113 | 111.119.184.19 | HTTP | 78 |AP... | Continuation |
| 94918 | 514.489081 | 192.168.181.113 | 23.207.193.174 | HTTP/X... | 326 |AP... | POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1 |
| 94924 | 514.752932 | 23.207.193.174 | 192.168.181.113 | HTTP | 350 |AP... | HTTP/1.1 302 Moved Temporarily |
| 99263 | 536.472770 | 192.168.181.113 | 23.207.193.174 | HTTP/X... | 78 |AP... | POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1 |
| 99265 | 536.727854 | 23.207.193.174 | 192.168.181.113 | HTTP | 350 |AP... | HTTP/1.1 302 Moved Temporarily |
| 1041_ | 558.164574 | 192.168.181.113 | 23.207.193.174 | HTTP/X... | 326 |AP... | POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1 |
| 1083_ | 579.936709 | 192.168.181.113 | 104.124.110.65 | HTTP/X... | 326 |AP... | POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1 |

Frame 2766: 326 bytes on wire (2608 bits), 326 bytes captured (2608 bits) on interface
 Ethernet II, Src: LiteonTechno_ba:df:fa (ac:b5:7d:ba:df:fa), Dst: 9a:83:c7:ca:72:d8 (9
 Internet Protocol Version 4, Src: 192.168.181.113, Dst: 23.207.193.174
 Transmission Control Protocol, Src Port: 50452, Dst Port: 80, Seq: 1747, Ack: 1, Len
 [3 Reassembled TCP Segments (2018 bytes): #2764(346), #2765(1400), #2766(272)]
 Hypertext Transfer Protocol
 POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1\r\n
 [Expert Info (Chat/Sequence): POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1
 Request Method: POST
 Request URI: /fwlink/?LinkID=252669&clcid=0x409
 Request Version: HTTP/1.1
 Connection: Keep-Alive\r\n
 Content-Type: text/xml; charset="UTF-16LE"\r\n
 User-Agent: MICROSOFT_DEVICE_METADATA_RETRIEVAL_CLIENT\r\n
 SOAPAction: "http://schemas.microsoft.com/windowsmetadata/services/2007/09/18/dms/D
 Content-Length: 1672\r\n
 Host: go.microsoft.com\r\n
 \r\n
 [Full request URI: http://go.microsoft.com/fwlink/?LinkID=252669&clcid=0x409]
 [HTTP request 1/1]
 File Data: 1672 bytes
 eXtensible Markup Language

Frame (326 bytes) Reassembled TCP (2018 bytes) Decoded UTF-16LE text (838 bytes)

Packets: 208212 · Displayed: 33 (0.0%)

tcp.dstport == 80

| No. | Time | Source | Destination | Protocol | Length | TCP Flags | Info |
|------|-----------|-----------------|-----------------|----------|--------|------------|--|
| 10 | 2.114089 | 192.168.181.113 | 138.91.171.81 | TCP | 66 |S | 50428 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 825 | 14.950145 | 192.168.181.113 | 192.229.221.95 | TCP | 54 |A...F | 50389 → 80 [FIN, ACK] Seq=1 Ack=1 Win=512 Len=0 |
| 826 | 14.950359 | 192.168.181.113 | 23.195.61.71 | TCP | 54 |A...F | 50390 → 80 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0 |
| 827 | 14.950457 | 192.168.181.113 | 111.119.184.168 | TCP | 54 |A...F | 50388 → 80 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0 |
| 828 | 14.950556 | 192.168.181.113 | 111.119.184.168 | TCP | 54 |A...F | 50392 → 80 [FIN, ACK] Seq=1 Ack=1 Win=511 Len=0 |
| 829 | 14.950650 | 192.168.181.113 | 111.119.184.168 | TCP | 54 |A...F | 50398 → 80 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0 |
| 833 | 14.972868 | 192.168.181.113 | 111.119.184.168 | TCP | 54 |A... | 50398 → 80 [ACK] Seq=2 Ack=2 Win=513 Len=0 |
| 834 | 14.972968 | 192.168.181.113 | 111.119.184.168 | TCP | 54 |A... | 50392 → 80 [ACK] Seq=2 Ack=2 Win=511 Len=0 |
| 835 | 14.973070 | 192.168.181.113 | 111.119.184.168 | TCP | 54 |A... | 50388 → 80 [ACK] Seq=2 Ack=2 Win=513 Len=0 |
| 845 | 15.073631 | 192.168.181.113 | 192.229.221.95 | TCP | 54 |A... | 50389 → 80 [ACK] Seq=2 Ack=2 Win=513 Len=0 |
| 847 | 15.100859 | 192.168.181.113 | 23.195.61.71 | TCP | 54 |A... | 50390 → 80 [ACK] Seq=2 Ack=2 Win=513 Len=0 |
| 2756 | 38.499139 | 192.168.181.113 | 23.207.193.174 | TCP | 66 |S | 50452 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 2763 | 38.606490 | 192.168.181.113 | 23.207.193.174 | TCP | 54 |A... | 50452 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0 |
| 2764 | 38.610186 | 192.168.181.113 | 23.207.193.174 | TCP | 400 |AP... | 50452 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=346 [TCP segment of s |

Frame 2766: 326 bytes on wire (2608 bits), 326 bytes captured (2608 bits) on interface
 Ethernet II, Src: LiteonTechno_ba:df:fa (ac:b5:7d:ba:df:fa), Dst: 9a:83:c7:ca:72:d8 (9
 Internet Protocol Version 4, Src: 192.168.181.113, Dst: 23.207.193.174
 Transmission Control Protocol, Src Port: 50452, Dst Port: 80, Seq: 1747, Ack: 1, Len
 [3 Reassembled TCP Segments (2018 bytes): #2764(346), #2765(1400), #2766(272)]
 Hypertext Transfer Protocol
 POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1\r\n
 [Expert Info (Chat/Sequence): POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1\r
 Request Method: POST
 Request URI: /fwlink/?LinkID=252669&clcid=0x409
 Request Version: HTTP/1.1
 Connection: Keep-Alive\r\n
 Content-Type: text/xml; charset="UTF-16LE"\r\n
 User-Agent: MICROSOFT_DEVICE_METADATA_RETRIEVAL_CLIENT\r\n
 SOAPAction: "http://schemas.microsoft.com/windowsmetadata/services/2007/09/18/dms/D
 Content-Length: 1672\r\n
 Host: go.microsoft.com\r\n
 \r\n
 [Full request URI: http://go.microsoft.com/fwlink/?LinkID=252669&clcid=0x409]
 [HTTP request 1/1]
 File Data: 1672 bytes
 eXtensible Markup Language

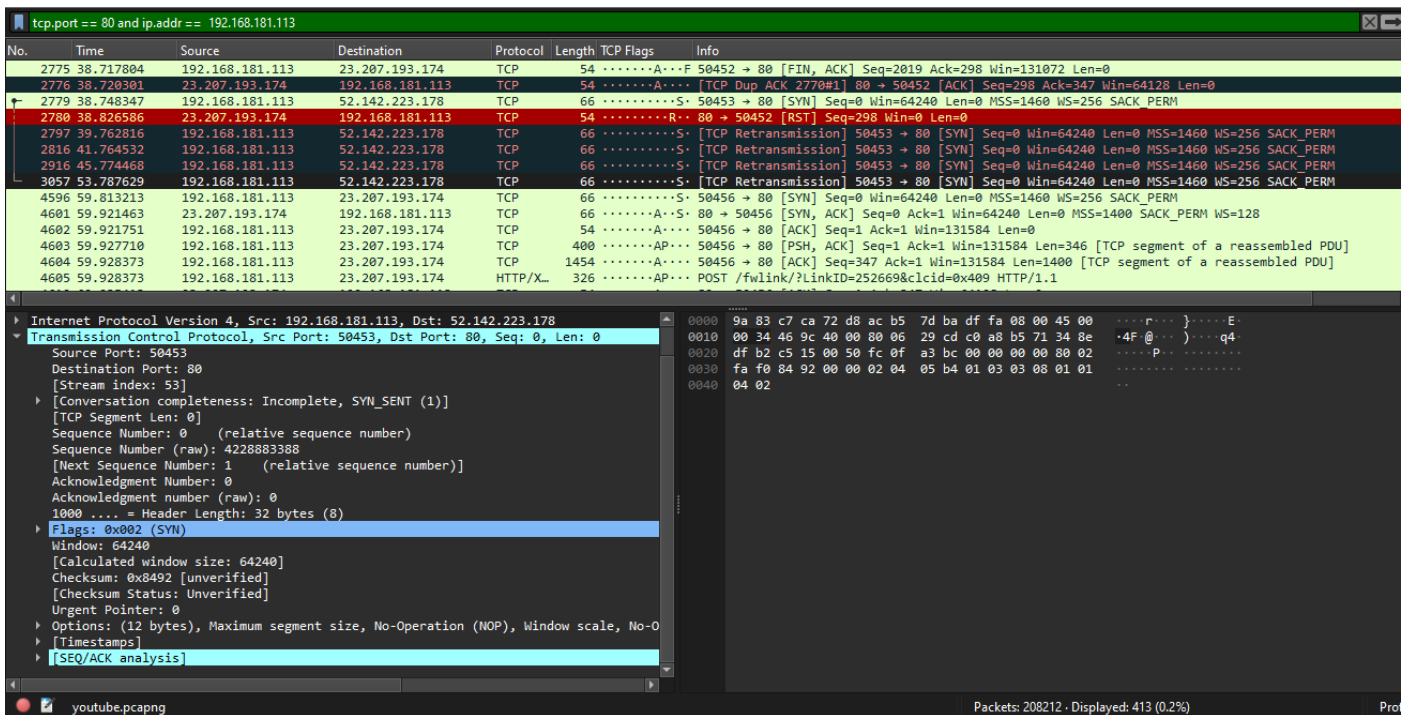
Frame (326 bytes) Reassembled TCP (2018 bytes) Decoded UTF-16LE text (838 bytes)

Packets: 208212 · Displayed: 280 (0.1%)

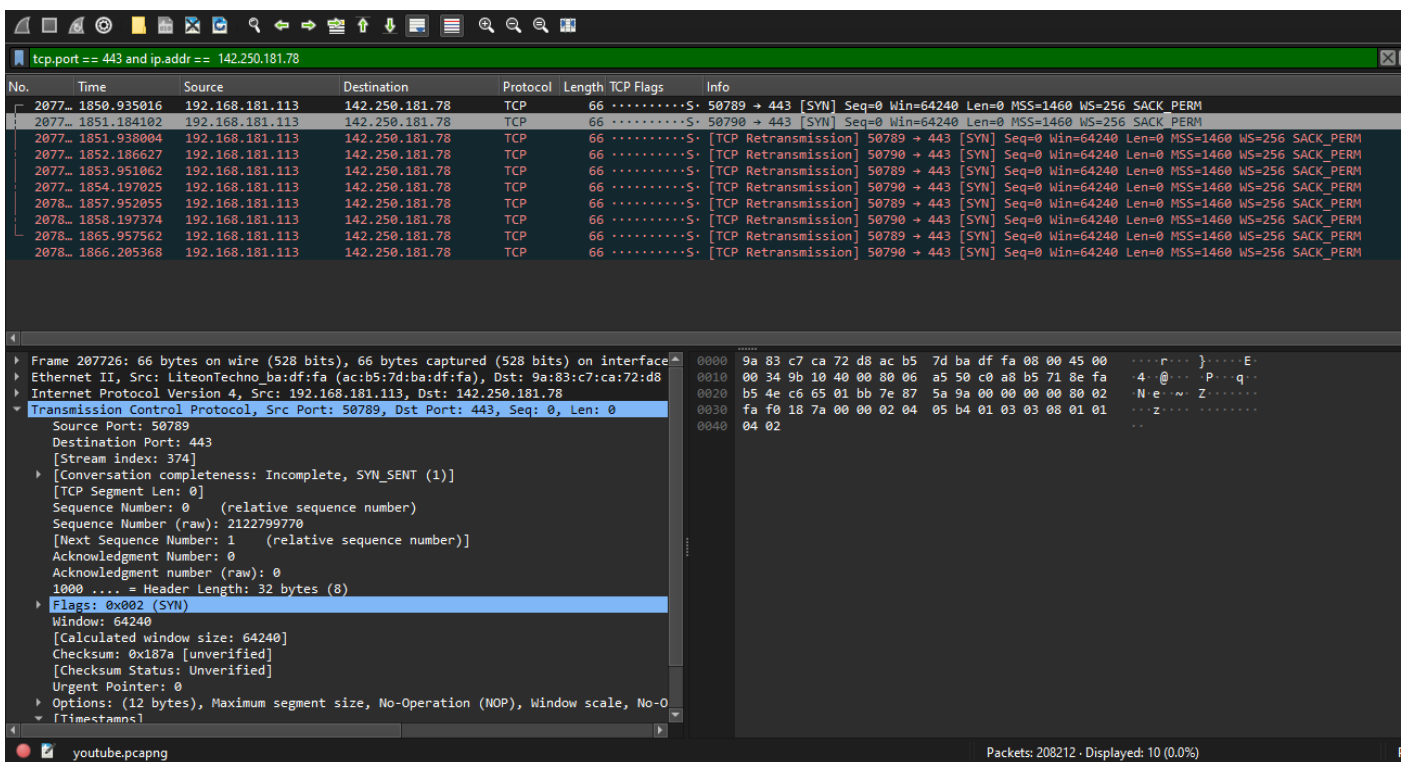
Filtering HTTP Traffic to and from Specific IP Address in Wireshark

If you want to filter for all HTTP traffic exchanged with a specific you can use the “and” operator. If, for example, you wanted to see all HTTP traffic related to a site at you could use the following filter:

```
tcp.port == 80 and ip.addr == 192.168.181.113
```



From YouTube tcp.port == 443 and ip.addr == 142.250.181.78



HTTP Method Filter

if you want to dig into your HTTP traffic you can filter for things like GET, PUT, POST, DELETE, HEAD, OPTIONS, CONNECT, and TRACE. To filter for these methods use the following filter syntax:

http.request.method == "GET"

http.request.method == "GET"

| No. | Time | Source | Destination | Protocol | Length | TCP Flags | Info |
|------|-------------|-----------------|--------------|----------|--------|------------|---|
| 1143 | 699.875574 | 192.168.181.113 | 2.23.27.37 | HTTP | 267 |AP... | GET /en-GB/livetile/preinstall?region=PK&appid=C98EA580842D8B94058BF071E1DA76512D21FE34 |
| 1846 | 1253.530101 | 192.168.181.113 | 178.79.238.0 | HTTP | 336 |AP... | GET /msdownload/update/v3/static/trusted/en/pinrulesstl.cab?ce09e6c88a6a5ad6 HTTP/1.1 |

[Window size scaling factor: 256]
Checksum: 0xee76 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0

Timestamps
[Time since first frame in this TCP stream: 0.155120000 seconds]
[Time since previous frame in this TCP stream: 0.000801000 seconds]

SEQ/ACK analysis
[iRTT: 0.154319000 seconds]
[Bytes in flight: 213]
[Bytes sent since last PSH flag: 213]
TCP payload (213 bytes)

Hypertext Transfer Protocol
GET /en-GB/livetile/preinstall?region=PK&appid=C98EA580842D8B94058BF071E1DA76512D21FE34
[Expert Info (Chat/Sequence): GET /en-GB/livetile/preinstall?region=PK&appid=C98EA580842D8B94058BF071E1DA76512D21FE34
[GET /en-GB/livetile/preinstall?region=PK&appid=C98EA580842D8B94058BF071E1DA76512D21FE34
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /en-GB/livetile/preinstall?region=PK&appid=C98EA580842D8B94058BF071E1DA76512D21FE34
Request URI Path: /en-GB/livetile/preinstall
Request URI Query: region=PK&appid=C98EA580842D8B94058BF071E1DA76512D21FE34
Request URI Query Parameter: region=PK
Request URI Query Parameter: appid=C98EA580842D8B94058BF071E1DA76512D21FE34
Request URI Query Parameter: FORM=Threshold
Request Version: HTTP/1.1
Connection: Keep-Alive\r\n\r\nUser-Agent: Microsoft-WINS/10.0\r\n\r\nHost: tile-service.weather.microsoft.com\r\n\r\n\r\n[Full request URI: http://tile-service.weather.microsoft.com/en-GB/livetile/preinstall?region=PK&appid=C98EA580842D8B94058BF071E1DA76512D21FE34
[HTTP request 1/1]
[Response in frame: 114414]

This packet will be responded in the packet with this number (http.response_in)

Packets: 208212 · Displayed: 2 (0.0%)

POST:

http.request.method == "POST"

| No. | Time | Source | Destination | Protocol | Length | TCP Flags | Info |
|-------|------------|-----------------|----------------|----------|--------|------------|--|
| 9290 | 81.242257 | 192.168.181.113 | 23.207.193.174 | HTTP/X.. | 326 |AP... | POST /fwlink/?LinkId=252669&clcid=0x409 HTTP/1.1 |
| 15129 | 102.939662 | 192.168.181.113 | 23.207.193.174 | HTTP/X.. | 714 |AP... | POST /fwlink/?LinkId=252669&clcid=0x409 HTTP/1.1 |
| 20451 | 127.534252 | 192.168.181.113 | 23.207.193.174 | HTTP/X.. | 270 |AP... | POST /fwlink/?LinkId=252669&clcid=0x409 HTTP/1.1 |
| 24446 | 149.289431 | 192.168.181.113 | 23.207.193.174 | HTTP/X.. | 1298 |AP... | POST /fwlink/?LinkId=252669&clcid=0x409 HTTP/1.1 |
| 36144 | 170.950672 | 192.168.181.113 | 23.207.193.174 | HTTP/X.. | 326 |AP... | POST /fwlink/?LinkId=252669&clcid=0x409 HTTP/1.1 |
| 39114 | 192.346551 | 192.168.181.113 | 23.207.193.174 | HTTP/X.. | 78 |AP... | POST /fwlink/?LinkId=252669&clcid=0x409 HTTP/1.1 |
| 94918 | 514.489081 | 192.168.181.113 | 23.207.193.174 | HTTP/X.. | 326 |AP... | POST /fwlink/?LinkId=252669&clcid=0x409 HTTP/1.1 |
| 99263 | 536.472770 | 192.168.181.113 | 23.207.193.174 | HTTP/X.. | 78 |AP... | POST /fwlink/?LinkId=252669&clcid=0x409 HTTP/1.1 |
| 1041 | 558.164574 | 192.168.181.113 | 23.207.193.174 | HTTP/X.. | 326 |AP... | POST /fwlink/?LinkId=252669&clcid=0x409 HTTP/1.1 |
| 1083 | 579.936709 | 192.168.181.113 | 104.124.110.65 | HTTP/X.. | 326 |AP... | POST /fwlink/?LinkId=252669&clcid=0x409 HTTP/1.1 |
| 1084 | 589.138668 | 192.168.181.113 | 104.124.110.65 | HTTP/X.. | 714 |AP... | POST /fwlink/?LinkId=252669&clcid=0x409 HTTP/1.1 |
| 1112 | 631.699097 | 192.168.181.113 | 104.124.110.65 | HTTP/X.. | 270 |AP... | POST /fwlink/?LinkId=252669&clcid=0x409 HTTP/1.1 |
| 1123 | 653.131373 | 192.168.181.113 | 104.124.110.65 | HTTP/X.. | 1298 |AP... | POST /fwlink/?LinkId=252669&clcid=0x409 HTTP/1.1 |
| 1133 | 674.575271 | 192.168.181.113 | 104.124.110.65 | HTTP/X.. | 326 |AP... | POST /fwlink/?LinkId=252669&clcid=0x409 HTTP/1.1 |

[Expert Info (Chat/Sequence): POST /fwlink/?LinkId=252669&clcid=0x409 HTTP/1.1
[POST /fwlink/?LinkId=252669&clcid=0x409 HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: POST
Request URI: /fwlink/?LinkId=252669&clcid=0x409
Request URI Path: /fwlink/
Request URI Query: LinkID=252669&clcid=0x409
Request URI Query Parameter: LinkID=252669
Request URI Query Parameter: clcid=0x409
Request Version: HTTP/1.1
Connection: Keep-Alive\r\n\r\nContent-Type: text/xml; charset="UTF-16LE"\r\n\r\nUser-Agent: MICROSOFT_DEVICE_METADATA_RETRIEVAL_CLIENT\r\n\r\nSOAPAction: "http://schemas.microsoft.com/windowsmetadata/services/2007/09/18/dms"
Content-Length: 2060\r\n\r\nHost: go.microsoft.com\r\n\r\n\r\n[Full request URI: http://go.microsoft.com/fwlink/?LinkId=252669&clcid=0x409
[HTTP request 1/1]
[Response in frame: 15159]
File Data: 2060 bytes

Frame (714 bytes) Reassembled TCP (2406 bytes) Decoded UTF-16LE text (1032 bytes)

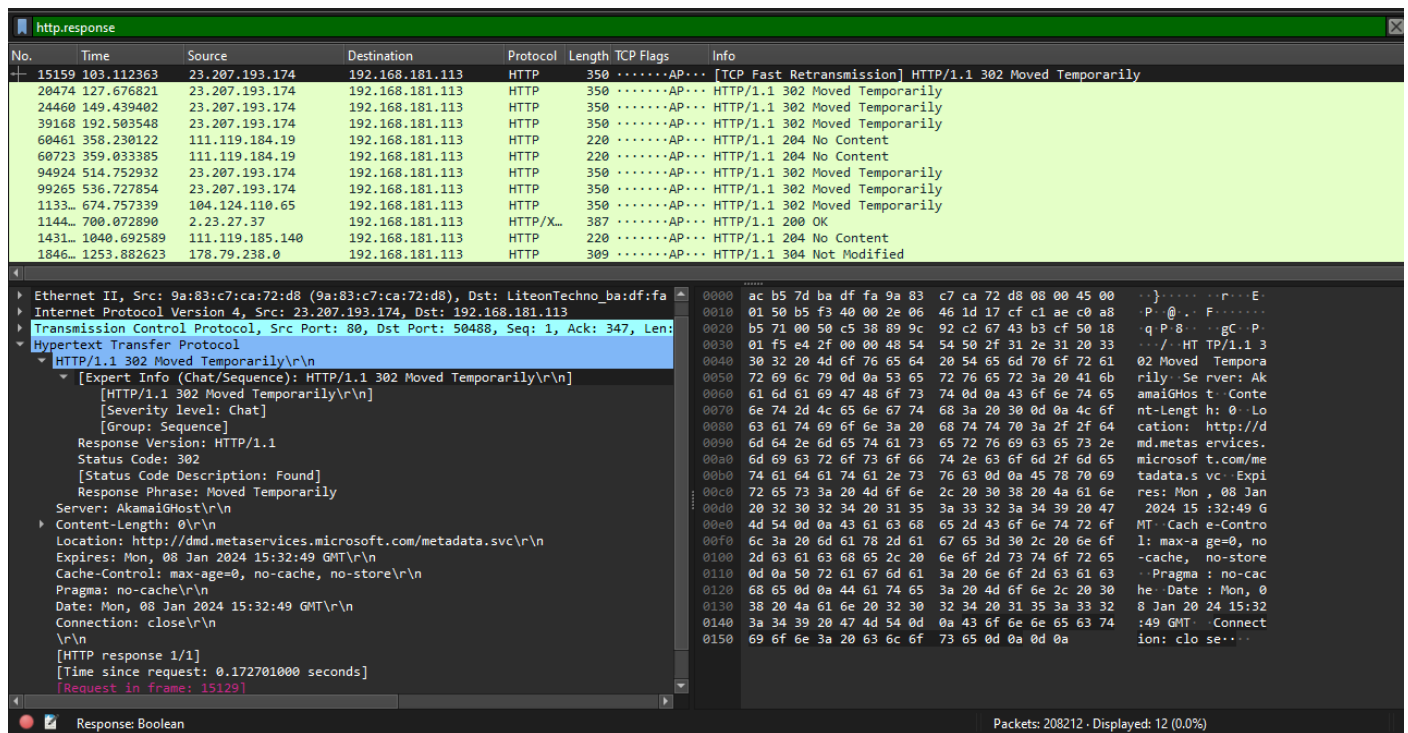
Packets: 208212 · Displayed: 16 (0.0%) Prof

HTTP RESPONSE FILTER:

One of the many valuable bits of information in a HTTP conversation is the response. This is the code a website returns that tells the status of the asset that was requested. You've probably seen things like Error 404 (Not Found) and 403 (Forbidden). These are HTTP responses and only a couple of the many that exist.

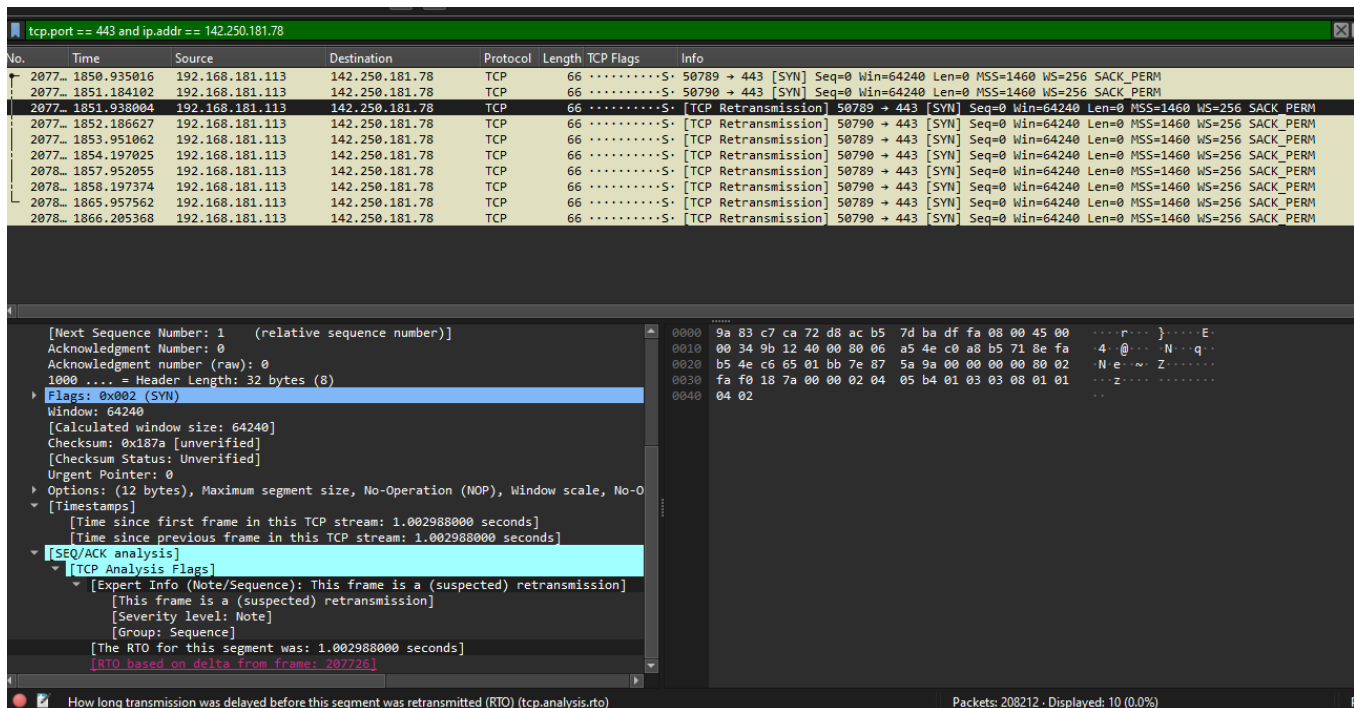
To filter for all responses enter the following display filter:

`http.response`



The Wireshark display filter `http.response.code == 200` is used to filter and display only those packets where the HTTP response code is 200. This filter is particularly useful when you want to focus on successful HTTP responses, as HTTP response code 200 indicates a successful request.

DISPLAYED: 10 Packets
Filters TCP traffic on port 443 with a source or destination IP address of 142.250.181.78, displaying a total of 10 packets meeting these criteria.



| No. | Time | Source | Destination | Protocol | Length | TCP Flags | Info |
|------|-------------|-----------------|----------------|----------|--------|-----------|--|
| 2077 | 1850.935016 | 192.168.181.113 | 142.250.181.78 | TCP | 66 |S. | 50789 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 2077 | 1851.184102 | 192.168.181.113 | 142.250.181.78 | TCP | 66 |S. | 50790 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 2077 | 1851.938004 | 192.168.181.113 | 142.250.181.78 | TCP | 66 |S. | [TCP Retransmission] 50789 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 2077 | 1852.186627 | 192.168.181.113 | 142.250.181.78 | TCP | 66 |S. | [TCP Retransmission] 50790 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 2077 | 1853.951062 | 192.168.181.113 | 142.250.181.78 | TCP | 66 |S. | [TCP Retransmission] 50789 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 2077 | 1854.197025 | 192.168.181.113 | 142.250.181.78 | TCP | 66 |S. | [TCP Retransmission] 50790 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 2078 | 1857.952055 | 192.168.181.113 | 142.250.181.78 | TCP | 66 |S. | [TCP Retransmission] 50789 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 2078 | 1858.197374 | 192.168.181.113 | 142.250.181.78 | TCP | 66 |S. | [TCP Retransmission] 50790 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 2078 | 1865.957562 | 192.168.181.113 | 142.250.181.78 | TCP | 66 |S. | [TCP Retransmission] 50789 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 2078 | 1866.205368 | 192.168.181.113 | 142.250.181.78 | TCP | 66 |S. | [TCP Retransmission] 50790 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |

[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
Window: 64240
[Calculated window size: 64240]
Checksum: 0x187a [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation
[Timestamps]
[Time since first frame in this TCP stream: 1.002988000 seconds]
[Time since previous frame in this TCP stream: 1.002988000 seconds]
[SEQ/ACK analysis]
[TCP Analysis Flags]
[Expert Info (Note/Sequence): This frame is a (suspected) retransmission]
[This frame is a (suspected) retransmission]
[Severity level: Note]
[Group: Sequence]
[The RTO for this segment was: 1.002988000 seconds]
[RTO based on delta from frame: 207726]

How long transmission was delayed before this segment was retransmitted (RTO) (tcp.analysis.rto) Packets: 208212 · Displayed: 10 (0.0%)

Capture TCP traffic from computer to YouTube servers:

ip.src == 192.168.181.113 and ip.dst == 142.250.181.78
Displayed: 1958 (0.9%)

Captures TCP traffic from the local computer (source IP 192.168.181.113) to YouTube servers (destination IP 142.250.181.78), displaying 1958 packets, and representing 0.9% of the total captured traffic.

ip.src == 192.168.181.113 and ip.dst == 142.250.181.78

| No. | Time | Source | Destination | Protocol | Length | TCP Flags | Info |
|-----|----------|-----------------|----------------|----------|--------|-----------|---|
| 125 | 6.916123 | 192.168.181.113 | 142.250.181.78 | QUIC | 1292 | | Initial, DCID=e9de82fddbf9cf6f, PKN: 1, PADDING, CRYPTO, PADDING, PING, PADDING, CRYPTO, CRYPTO |
| 144 | 6.951961 | 192.168.181.113 | 142.250.181.78 | QUIC | 123 | | 0-RTT, DCID=e9de82fddbf9cf6f |
| 166 | 7.004007 | 192.168.181.113 | 142.250.181.78 | QUIC | 1288 | | 0-RTT, DCID=e9de82fddbf9cf6f |
| 167 | 7.004249 | 192.168.181.113 | 142.250.181.78 | QUIC | 769 | | 0-RTT, DCID=e9de82fddbf9cf6f |
| 179 | 7.087169 | 192.168.181.113 | 142.250.181.78 | QUIC | 121 | | Handshake, DCID=e9de82fddbf9cf6f |
| 180 | 7.087510 | 192.168.181.113 | 142.250.181.78 | QUIC | 73 | | Protected Payload (KP0), DCID=e9de82fddbf9cf6f |
| 182 | 7.117055 | 192.168.181.113 | 142.250.181.78 | QUIC | 74 | | Protected Payload (KP0), DCID=e9de82fddbf9cf6f |
| 184 | 7.169369 | 192.168.181.113 | 142.250.181.78 | QUIC | 74 | | Protected Payload (KP0), DCID=e9de82fddbf9cf6f |
| 209 | 7.273668 | 192.168.181.113 | 142.250.181.78 | QUIC | 75 | | Protected Payload (KP0), DCID=e9de82fddbf9cf6f |
| 212 | 7.274006 | 192.168.181.113 | 142.250.181.78 | QUIC | 77 | | Protected Payload (KP0), DCID=e9de82fddbf9cf6f |
| 213 | 7.274165 | 192.168.181.113 | 142.250.181.78 | QUIC | 73 | | Protected Payload (KP0), DCID=e9de82fddbf9cf6f |
| 228 | 7.292079 | 192.168.181.113 | 142.250.181.78 | QUIC | 73 | | Protected Payload (KP0), DCID=e9de82fddbf9cf6f |
| 230 | 7.292343 | 192.168.181.113 | 142.250.181.78 | QUIC | 73 | | Protected Payload (KP0), DCID=e9de82fddbf9cf6f |
| 233 | 7.292982 | 192.168.181.113 | 142.250.181.78 | QUIC | 73 | | Protected Payload (KP0), DCID=e9de82fddbf9cf6f |
| 238 | 7.295257 | 192.168.181.113 | 142.250.181.78 | QUIC | 73 | | Protected Payload (KP0), DCID=e9de82fddbf9cf6f |

[Checksum Status: Unverified]
[Stream index: 16]
[Timestamps]
[Time since first frame: 0.171046000 seconds]
[Time since previous frame: 0.001070000 seconds]
UDP payload (79 bytes)
QUIC IEIF
QUIC Connection Information
[Packet Length: 79]
1... .. = Header Form: Long Header (1)
1... .. = Fixed Bit: True
..10... .. = Packet Type: Handshake (2)
Version: 1 (0x00000001)
Destination Connection ID Length: 8
Destination Connection ID: e9de82fddbf9cf6f
Source Connection ID Length: 0
Length: 62
[Expert Info (Warning/Decryption): Failed to create decryption context: Secrets are not available]
[Failed to create decryption context: Secrets are not available]
[Severity level: Warning]
[Group: Decryption]
Remaining Payload: c885571b956278417abfecb5c9e10c57c565fb2be64689d4b0b7a9bd29ca

youtube.pcapng

Packets: 208212 · Displayed: 1958 (0.9%)

Capture TCP traffic from YouTube servers to your computer:

ip.src == 142.250.181.78 and ip.dst == 192.168.181.113

DISPLAYED: 5762 (2.8%)

Captures TCP traffic from YouTube servers (source IP 142.250.181.78) to your computer (destination IP 192.168.181.113), displaying 5762 packets, and constituting 2.8% of the total captured traffic.

ip.src == 142.250.181.78 and ip.dst == 192.168.181.113

| No. | Time | Source | Destination | Protocol | Length | TCP Flags | Info |
|-----|----------|----------------|-----------------|----------|--------|-----------|--|
| 164 | 6.999662 | 142.250.181.78 | 192.168.181.113 | QUIC | 1292 | | Initial, SCID=e9de82fddbf9cf6f, PKN: 1, ACK, PADDING |
| 175 | 7.085798 | 142.250.181.78 | 192.168.181.113 | QUIC | 1292 | | Protected Payload (KP0) |
| 176 | 7.085798 | 142.250.181.78 | 192.168.181.113 | QUIC | 846 | | Protected Payload (KP0) |
| 177 | 7.085798 | 142.250.181.78 | 192.168.181.113 | QUIC | 204 | | Protected Payload (KP0) |
| 178 | 7.086099 | 142.250.181.78 | 192.168.181.113 | QUIC | 66 | | Protected Payload (KP0) |
| 183 | 7.138963 | 142.250.181.78 | 192.168.181.113 | QUIC | 166 | | Protected Payload (KP0) |
| 206 | 7.272969 | 142.250.181.78 | 192.168.181.113 | QUIC | 1288 | | Protected Payload (KP0) |
| 207 | 7.273252 | 142.250.181.78 | 192.168.181.113 | QUIC | 1292 | | Protected Payload (KP0) |
| 208 | 7.273471 | 142.250.181.78 | 192.168.181.113 | QUIC | 1288 | | Protected Payload (KP0) |
| 210 | 7.273730 | 142.250.181.78 | 192.168.181.113 | QUIC | 1292 | | Protected Payload (KP0) |
| 211 | 7.273730 | 142.250.181.78 | 192.168.181.113 | QUIC | 87 | | Protected Payload (KP0) |
| 224 | 7.291367 | 142.250.181.78 | 192.168.181.113 | QUIC | 1287 | | Protected Payload (KP0) |
| 225 | 7.291683 | 142.250.181.78 | 192.168.181.113 | QUIC | 1292 | | Protected Payload (KP0) |
| 226 | 7.291871 | 142.250.181.78 | 192.168.181.113 | QUIC | 1292 | | Protected Payload (KP0) |
| 227 | 7.291871 | 142.250.181.78 | 192.168.181.113 | QUIC | 1292 | | Protected Payload (KP0) |

Ethernet II, Src: 9a:83:c7:ca:72:d8 (9a:83:c7:ca:72:d8), Dst: LiteonTechno_ba:df:fa:83:c7:ca:72:d8
Internet Protocol Version 4, Src: 142.250.181.78, Dst: 192.168.181.113
User Datagram Protocol, Src Port: 443, Dst Port: 52434
Source Port: 443
Destination Port: 52434
Length: 170
Checksum: 0x6af6 [unverified]
[Checksum Status: Unverified]
[Stream index: 16]
[Timestamps]
[Time since first frame: 0.169675000 seconds]
[Time since previous frame: 0.000000000 seconds]
UDP payload (162 bytes)
QUIC IEIF
QUIC Connection information
[Connection Number: 1]
[Packet Length: 162]
QUIC Short Header
0... .. = Header Form: Short Header (0)
1... .. = Fixed Bit: True
..0... .. = Spin Bit: False
Remaining Payload [truncated]: 29e5d12c544dd63894026a6d95ed10614a1e3a31c3c99c293c

youtube.pcapng

Packets: 208212 · Displayed: 5762 (2.8%)

Capture TCP traffic on port 19305 (commonly used for YouTube RTMFP - Real-Time Messaging Protocol):

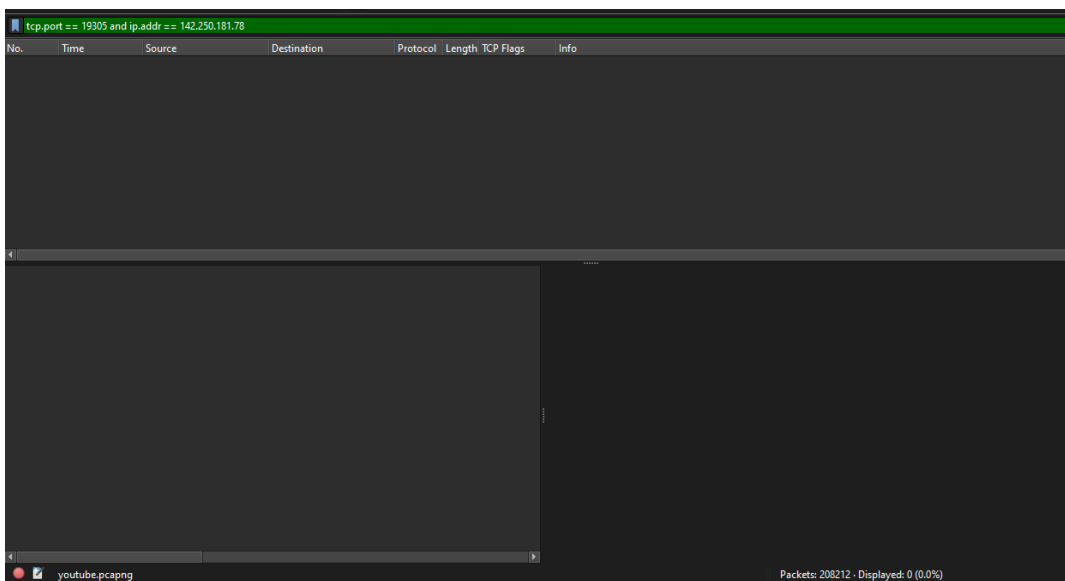
You are seeing zero displayed packets, there could be several reasons for this:

1. No RTMFP Traffic:

- It's possible that there is no RTMFP traffic on the network during the time of your capture. RTMFP is specific to applications that use Adobe technologies, and not all applications or websites utilize this protocol.

2. Encryption or Other Protocols:

- RTMFP traffic may be encrypted or encapsulated within another protocol, making it harder to capture or recognize using a simple port-based filter.



Capture TCP traffic with a specific sequence number range:

```
tcp.seq >=1000 and tcp.seq <= 2000
```

Captures TCP traffic with sequence numbers between 1000 and 2000, focusing on a specific range of sequence numbers for analysis.

| tcp.seq >= 1000 and tcp.seq <= 2000 | | | | | | | | | |
|-------------------------------------|----------|-----------------|-----------------|----------|--------|------------|--------------------|--|------------------------------------|
| No. | Time | Source | Destination | Protocol | Length | TCP Flags | Info | | |
| 21 | 2.783159 | 20.212.88.117 | 192.168.181.113 | TCP | 1454 |AP... | 443 → 50431 | [PSH, ACK] Seq=1401 Ack=615 Win=15616 Len=1400 | [TCP segment of a reassembled PDU] |
| 49 | 3.745553 | 192.168.181.113 | 204.79.197.239 | TCP | 1454 |A.... | 50432 → 443 | [ACK] Seq=1029 Ack=155 Win=131328 Len=1400 | [TCP segment of a reassembled PDU] |
| 62 | 4.204803 | 204.79.197.239 | 192.168.181.113 | TLSv1.2 | 834 |AP... | Application Data | | |
| 87 | 5.087356 | 20.190.145.140 | 192.168.181.113 | TCP | 1454 |A.... | 443 → 50433 | [ACK] Seq=1401 Ack=567 Win=12582400 Len=1400 | [TCP segment of a reassembled PDU] |
| 96 | 5.227990 | 192.168.181.113 | 20.190.145.140 | TLSv1.2 | 1293 |AP... | Application Data | | |
| 133 | 6.947066 | 192.168.181.113 | 20.189.173.6 | TCP | 1454 |A.... | 50405 → 443 | [ACK] Seq=1401 Ack=1 Win=514 Len=1400 | [TCP segment of a reassembled PDU] |
| 195 | 7.234065 | 192.168.181.113 | 142.250.181.138 | TLSv1.3 | 128 |AP... | Change Cipher Spec | Application Data | |
| 266 | 7.335353 | 192.168.181.113 | 142.250.181.138 | TCP | 54 |A.... | 50436 → 443 | [ACK] Seq=1138 Ack=1350 Win=130048 Len=0 | |
| 405 | 9.254111 | 192.168.181.113 | 20.189.173.3 | TCP | 54 |A.... | 50425 → 443 | [ACK] Seq=1376 Ack=40 Win=511 Len=0 | |
| 422 | 9.591146 | 192.168.181.113 | 20.189.173.3 | TLSv1.2 | 89 |AP... | Application Data | | |
| 423 | 9.600794 | 192.168.181.113 | 20.189.173.3 | TLSv1.2 | 138 |AP... | Application Data | | |
| 424 | 9.600912 | 192.168.181.113 | 20.189.173.3 | TLSv1.2 | 850 |AP... | Application Data | | |

| | | | | |
|---|------|---|------------|---------------|
| [Checksum Status: Unverified] | 0000 | 9a 83 c7 ca 72 d8 ac b5 7d ba df fa 08 00 45 00 |} |E |
| Urgent Pointer: 0 | 0010 | 00 72 97 5f 40 00 00 06 a8 87 c0 a8 b5 71 8e fa |q | |
| [Timestamps] | 0020 | b5 8a c5 04 01 bb 32 88 ec 6c db 15 73 5e 50 18 |2 |s^P |
| [Time since first frame in this TCP stream: 0.232616000 seconds] | 0030 | 02 00 2a 76 00 00 14 03 03 00 01 01 17 03 03 00 |v | |
| [Time since previous frame in this TCP stream: 0.005843000 seconds] | 0040 | 3f f7 98 4a a1 df fd aa ff e1 36 47 e2 36 df b4 |J |6G 6 |
| [SEQ/ACK analysis] | 0050 | a0 8a 2a 47 c1 50 1d 95 7a a1 80 9d c5 1a 2f 33 |*G-P |z...../3 |
| [This is an ACK to the segment in frame: 194] | 0060 | 52 f7 42 7f 63 da 19 18 91 b9 23 68 1a 4a f0 b1 |R B c |#h J |
| [The RTT to ACK the segment was: 0.005843000 seconds] | 0070 | dc c4 c5 dd 5d 17 98 a7 03 3e 73 1d 0b 79 6c 5a |] |>s yLZ |
| [iRTT: 0.054647000 seconds] | | | | |
| [Bytes in flight: 74] | | | | |
| [Bytes sent since last PSH flag: 74] | | | | |
| TCP payload (74 bytes) | | | | |
| Transport Layer Security | | | | |
| TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec | | | | |
| Content Type: Change Cipher Spec (20) | | | | |
| Version: TLS 1.2 (0x0303) | | | | |
| Length: 1 | | | | |
| Change Cipher Spec Message | | | | |
| TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol | | | | |
| Opaque Type: Application Data (23) | | | | |
| Version: TLS 1.2 (0x0303) | | | | |
| Length: 63 | | | | |
| Encrypted Application Data: f7984aa1dfffdaaffe13647e236dfb4a08a2a47c1501d957aa1 | | | | |
| [Application Data Protocol: Hypertext Transfer Protocol] | | | | |

Capture TCP traffic with specific TCP flags set (e.g., SYN and ACK):

```
tcp[13] == 18
DISPLAYED: 36728 (17.6%)
```

Captures TCP traffic with specific flags set (e.g., SYN and ACK) by filtering on the 13th byte of the TCP header, displaying 36,728 packets, representing 17.6% of the total captured traffic. Filters TCP traffic with specific flags set, focusing on the 13th byte of the TCP header to capture packets with intricate flag combinations (e.g., SYN and ACK). The displayed count of 36,728 packets accounts for 17.6% of the total captured traffic, providing insights into nuanced TCP communications.

| No. | Time | Source | Destination | Protocol | Length | TCP Flags | Info |
|-----|----------|-----------------|-----------------|----------|--------|------------|--|
| 136 | 6.947378 | 192.168.181.113 | 20.189.173.6 | TLSv1.2 | 93 |AP... | Application Data |
| 143 | 6.947502 | 192.168.181.113 | 20.189.173.6 | TLSv1.2 | 1358 |AP... | Application Data |
| 148 | 6.953478 | 192.168.181.113 | 20.189.173.6 | TLSv1.2 | 1451 |AP... | Application Data |
| 156 | 6.953775 | 192.168.181.113 | 20.189.173.6 | TLSv1.2 | 670 |AP... | Application Data |
| 171 | 7.058227 | 192.168.181.113 | 142.250.181.138 | TLSv1.3 | 1117 |AP... | Client Hello (SNI=fonts.googleapis.com) |
| 194 | 7.228222 | 142.250.181.138 | 192.168.181.113 | TLSv1.3 | 435 |AP... | Server Hello, Change Cipher Spec, Application Data |
| 195 | 7.234065 | 192.168.181.113 | 142.250.181.138 | TLSv1.3 | 128 |AP... | Change Cipher Spec, Application Data |
| 204 | 7.270787 | 20.189.173.6 | 192.168.181.113 | TLSv1.2 | 93 |AP... | Application Data |
| 223 | 7.287556 | 142.250.181.138 | 192.168.181.113 | TLSv1.3 | 1022 |AP... | Application Data, Application Data |
| 234 | 7.293558 | 20.189.173.6 | 192.168.181.113 | TLSv1.2 | 89 |AP... | Application Data |
| 271 | 7.604250 | 20.189.173.6 | 192.168.181.113 | TLSv1.2 | 542 |AP... | Application Data, Application Data |
| 397 | 8.895289 | 192.168.181.113 | 20.189.173.3 | TLSv1.2 | 138 |AP... | Application Data |

| | |
|---|---|
| [Calculated window size: 67840] [Window size scaling factor: 256] Checksum: 0xa0a5 [unverified] [Checksum Status: Unverified] Urgent Pointer: 0 [Timestamps] [Time since first frame in this TCP stream: 0.226773000 seconds] [Time since previous frame in this TCP stream: 0.114012000 seconds] [SEQ/ACK analysis] [iRTT: 0.054647000 seconds] [Bytes in flight: 381] [Bytes sent since last PSH flag: 381] TCP payload (381 bytes) Transport Layer Security TLSv1.3 Record Layer: Handshake Protocol: Server Hello Content Type: Handshake (22) Version: TLS 1.2 (0x0303) Length: 128 Handshake Protocol: Server Hello TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec Content Type: Change Cipher Spec (20) Version: TLS 1.2 (0x0303) Length: 1 Change Cipher Spec Message TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol | 0000 ac b5 7d ba df fa 9a 83 c7 ca 72 d8 08 00 45 80E 0010 01 a5 23 e5 00 00 73 06 67 4f 8e fa b5 8a c0 a8s g0 0020 b5 71 01 bb c5 04 db 15 71 e1 32 88 ec 6c 50 18q 2 1P 0030 01 09 a0 a5 00 00 16 03 03 00 00 02 00 00 7c 03 0040 03 ef ab ce 98 4f 3c 29 d9 33 9c 58 2c ce 67 3e0< 3 X, g> 0050 af 3c 3e ab 25 76 8d 82 a1 f8 a7 9b d2 a1 30 ce< %v0 0060 06 20 5c a2 4f 40 94 3e e0 64 3d 21 ad f1 19 11\ 0@ > d=!< 0070 65 e1 4a 8b d0 5e d2 91 ad 24 33 07 e4 56 43 fce J ^ ^ \$3 VC 0080 37 02 13 01 00 00 34 00 29 00 02 00 00 00 33 0074j 0090 24 00 1d 00 20 82 ce 50 4e e4 0c 5d 45 8c 06 74\$P Nt 00a0 3a ec 3b 99 17 58 13 80 f6 64 fd 69 3f 4f fb 86;Xd i20 00b0 91 5d b7 20 00 00 2b 00 02 03 04 14 03 03 00 01]+ 00c0 01 17 03 03 00 ed ef 57 c4 47 a9 2f a0 59 e0 18W G / Y 00d0 ac c7 d6 b8 4d 57 72 02 f0 3d 3f 99 25 ec a9 efM> X 00e0 60 19 1f 76 4a 5d fd c1 73 42 48 8f 0e 34 ba 39vsB4 9 00f0 dc 18 87 58 38 4a ae 20 c7 73 8c d2 ed 7a 38 7bXsz 0100 8a 33 15 e1 70 a6 75 50 ad 84 6f 5a 5b 53 2f 933p uPoZ [5 0110 55 6c eb 67 05 00 43 54 8b 8a a7 72 9e 6e 99 9dUgCTr n 0120 a7 98 ab d7 83 79 72 08 56 b7 86 22 51 9e 2c 3cyrVQ< 0130 f4 fa b2 dd 59 ab f2 d2 a0 93 74 dd 91 64 5c deYtd 0140 0d 94 61 4f f6 06 9e ba 1d 06 dd 01 b8 30 41 b6a0 0150 4f bf d2 bc 68 ab bd 78 c6 9c 8c 63 99 ab 71 30Ohxc Kq0 0160 68 09 58 e1 e2 9e 6d 7c 57 dc d3 bc e3 95 47 0ehXmWG 0170 fe 7e 18 6d 8c 94 58 b4 c7 3f f1 1f cb cd 80 c7X? 0180 35 f3 6a 36 82 cb 55 2e b8 2e 69 dd 0e 18 88 5b5j6U1[|
|---|---|

Filter for DNS queries:

udp.port == 53
Displayed: 2013 (1%)

Filters DNS queries by capturing UDP traffic on port 53, displaying 2013 packets, constituting 1% of the total captured traffic.

| No. | Time | Source | Destination | Protocol | Length | TCP Flags | Info |
|------|-----------|-----------------|-----------------|----------|--------|-----------|--|
| 1156 | 17.775390 | 192.168.181.22 | 192.168.181.113 | DNS | 218 | | Standard query response 0xf744 HTTPS www.tubebuddy.com CNAME www.tubebuddy.com.edgekey.net CNAME |
| 1493 | 21.027141 | 192.168.181.113 | 192.168.181.22 | DNS | 77 | | Standard query 0xeba5 A sirius.mvbsys.com |
| 1494 | 21.051048 | 192.168.181.22 | 192.168.181.113 | DNS | 173 | | Standard query response 0xeba5 A sirius.mvbsys.com A 3.218.212.197 A 3.212.50.70 A 54.156.156.13 |
| 1712 | 24.694122 | 192.168.181.113 | 192.168.181.22 | DNS | 74 | | Standard query 0x5cc0 A www.google.com |
| 1713 | 24.695451 | 192.168.181.113 | 192.168.181.22 | DNS | 74 | | Standard query 0x5cc5 HTTPS www.google.com |
| 1714 | 24.696496 | 192.168.181.113 | 192.168.181.22 | DNS | 77 | | Standard query 0xa4b6 A www.google.com.pk |
| 1715 | 24.697037 | 192.168.181.113 | 192.168.181.22 | DNS | 77 | | Standard query 0x97e3 HTTPS www.google.com.pk |
| 1716 | 24.727069 | 192.168.181.22 | 192.168.181.113 | DNS | 90 | | Standard query response 0x5cc0 A www.google.com A 142.250.181.68 |
| 1717 | 24.727069 | 192.168.181.22 | 192.168.181.113 | DNS | 99 | | Standard query response 0x5cc5 HTTPS www.google.com HTTPS |
| 1719 | 24.727069 | 192.168.181.22 | 192.168.181.113 | DNS | 93 | | Standard query response 0xa4b6 A www.google.com.pk A 172.217.19.195 |
| 1720 | 24.727069 | 192.168.181.22 | 192.168.181.113 | DNS | 137 | | Standard query response 0x97e3 HTTPS www.google.com.pk SOA ns1.google.com |
| 1735 | 24.845412 | 192.168.181.113 | 192.168.181.22 | DNS | 85 | | Standard query 0x6134 A lh6.googleusercontent.com |

| | |
|---|--|
| Frame 1098: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF{...} | 0000 9a 83 c7 ca 72 d8 ac b5 7d ba df fa 08 00 45 00E |
| Ethernet II, Src: LiteonTechno ba:df:fa (ac:b5:7d:ba:df:fa), Dst: 9a:83:c7:ca:72:d8 (98:9f:fa:83:c7:ca:72:d8) | 0010 00 3f 57 82 00 00 80 11 f7 52 c0 a8 b5 71 c0 a8?WRq |
| Internet Protocol Version 4, Src: 192.168.181.113, Dst: 192.168.181.22 | 0020 b5 16 c2 57 00 35 00 2b 67 a0 3a bb 01 00 00 01W 5 + g : |
| User Datagram Protocol, Src Port: 49751, Dst Port: 53 | 0030 00 00 00 00 00 03 77 77 77 09 74 75 62 65 62w w-tubeb |
| Source Port: 49751 Destination Port: 53 Length: 43 Checksum: 0x67a0 [unverified] [Checksum Status: Unverified] [Stream index: 48] [Timestamps] [Time since first frame: 0.000000000 seconds] [Time since previous frame: 0.000000000 seconds] UDP payload (35 bytes) Domain Name System (query) Transaction ID: 0x3abb Flags: 0x0100 Standard query Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries [Response In: 1100] | 0040 75 64 64 79 03 63 6f 6d 00 00 01 00 01udycomE |

udp.port == 53 and dns.qry.name contains "youtube"

Displayed: 178

Filters DNS queries related to YouTube by capturing UDP traffic on port 53 and checking if the DNS query name contains "YouTube", displaying 178 relevant packets.

Wireshark packet capture showing DNS queries to YouTube. The filter is "udp.port == 53 and dns.qry.name contains 'youtube'". The packet list shows 178 packets. The packet details pane shows a DNS query response for "www.youtube.com".

| No. | Time | Source | Destination | Protocol | Length | TCP Flags | Info |
|------|-----------|-----------------|-----------------|----------|--------|-----------|--|
| 967 | 16.680022 | 192.168.181.113 | 192.168.181.22 | DNS | 75 | | Standard query 0x492f A www.youtube.com |
| 968 | 16.692445 | 192.168.181.22 | 192.168.181.113 | DNS | 272 | | Standard query response 0xa529 A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.19.206 |
| 970 | 16.708754 | 192.168.181.22 | 192.168.181.113 | DNS | 272 | | Standard query response 0x492f A www.youtube.com CNAME youtube-ui.l.google.com A 142.250.181.116 |
| 1048 | 17.170867 | 192.168.181.113 | 192.168.181.22 | DNS | 75 | | Standard query 0x8646 A www.youtube.com |
| 1050 | 17.172553 | 192.168.181.113 | 192.168.181.22 | DNS | 75 | | Standard query 0x871e A www.youtube.com |
| 1051 | 17.181129 | 192.168.181.22 | 192.168.181.113 | DNS | 272 | | Standard query response 0x8646 A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.19.14 |
| 1052 | 17.217873 | 192.168.181.22 | 192.168.181.113 | DNS | 272 | | Standard query response 0x871e A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.19.174 |
| 1909 | 25.960034 | 192.168.181.113 | 192.168.181.22 | DNS | 95 | | Standard query 0xcaf6 A suggestqueries-clients6.youtube.com |
| 1990 | 25.962745 | 192.168.181.113 | 192.168.181.22 | DNS | 95 | | Standard query 0x8b27 HTTPS suggestqueries-clients6.youtube.com |
| 1991 | 25.988668 | 192.168.181.22 | 192.168.181.113 | DNS | 111 | | Standard query response 0xcaf6 A suggestqueries-clients6.youtube.com A 142.250.181.78 |
| 1992 | 25.995229 | 192.168.181.22 | 192.168.181.113 | DNS | 152 | | Standard query response 0x8b27 HTTPS suggestqueries-clients6.youtube.com SOA ns1.google.com |
| 2577 | 31.398544 | 192.168.181.113 | 192.168.181.22 | DNS | 80 | | Standard query 0xacb5 A accounts.youtube.com |

Query Class (dns.qry.class), 2 bytes

Packets: 208212 · Displayed: 178 (0.1%)

Profile: Default

Filter for ICMP (ping) packets:

Wireshark packet capture showing ICMP (ping) packets. The filter is "icmp". The packet list shows 7 packets. The packet details pane shows an ICMP echo request.

| No. | Time | Source | Destination | Protocol | Length | TCP Flags | Info |
|--------|-------------|----------------|-----------------|----------|--------|------------|---|
| 2075.. | 1819.608099 | 192.168.181.22 | 192.168.181.113 | ICMP | 161 |AP... | Destination unreachable (Network unreachable) |
| 2075.. | 1819.609248 | 192.168.181.22 | 192.168.181.113 | ICMP | 590 |AP... | Destination unreachable (Network unreachable) |
| 2075.. | 1824.498986 | 192.168.181.22 | 192.168.181.113 | ICMP | 117 |AP... | Destination unreachable (Network unreachable) |
| 2078.. | 1859.865051 | 192.168.181.22 | 192.168.181.113 | ICMP | 94 |S... | Destination unreachable (Network unreachable) |
| 2078.. | 1862.830650 | 192.168.181.22 | 192.168.181.113 | ICMP | 82 |A...F | Destination unreachable (Network unreachable) |
| 2078.. | 1866.044918 | 192.168.181.22 | 192.168.181.113 | ICMP | 83 |A...F | Destination unreachable (Network unreachable) |
| 2080.. | 1870.606456 | 192.168.181.22 | 192.168.181.113 | ICMP | 94 |S... | Destination unreachable (Network unreachable) |

Sequence Number: 1561884819
[Stream index: 185]
[Conversation completeness: Complete, WITH_DATA (47)]
Acknowledgment Number: 433411796 (relative ack number)
Acknowledgment number (raw): 433411796
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 509
[Calculated window size: 509]
[Window size scaling factor: 256]
Checksum: 0x5b3e [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 851.232401000 seconds]
[Time since previous frame in this TCP stream: 0.001119000 seconds]
TCP payload (79 bytes)
Transport Layer Security
TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
Opaque Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 74
Encrypted Application Data: 12b676d366f5ede93532af8d99ff030513a290d38d5774a
[Application Data Protocol: Hypertext Transfer Protocol]

youtube.pcapng

Packets: 208212 · Displayed: 7 (0.0%)

Pro

SSL:

Filter for SSL/TLS traffic with specific SSL/TLS version:

`ssl.record.version == 0x0303`

Filters SSL/TLS traffic for packets using the specific SSL/TLS version 0x0303 (TLS 1.2) in the SSL record version field.

Wireshark capture showing SSL/TLS traffic filtered by `ssl.record.version == 0x0303`. The packet list shows several TLSv1.2 records. The packet details pane shows the structure of a TLSv1.2 Record Layer: Handshake Protocol: Server Hello, including the Change Cipher Spec Protocol: Change Cipher Spec and the Encrypted Handshake Message.

`ip.addr == 142.250.181.78 and ssl`

Wireshark capture showing SSL/TLS traffic filtered by `ip.addr == 142.250.181.78 and ssl`. The packet list shows a QUIC packet. The packet details pane shows the structure of a QUIC packet, including the QUIC Short Header and the Remaining Payload.

Filters and displays SSL/TLS traffic associated with the IP address 142.250.181.78.

FLAGS:

SYN FLAG:

(captured under item #1,#2,#3)

```
tcp.flags.syn == 1
```

Displayed: 815 Fraction: 0.4%

Captures and displays TCP packets with the SYN flag set, resulting in 815 packets, constituting 0.4% of the total captured traffic (items #1, #2, #3).

The image shows a Wireshark packet capture interface. The top pane displays a list of captured packets, with the filter 'tcp.flags.syn == 1' applied. The middle pane shows the details of a selected SYN packet, including sequence numbers, window size, and flags. The bottom pane shows the raw packet data in hexadecimal and ASCII.

| No. | Time | Source | Destination | Protocol | Length | TCP Flags | Info |
|-----|----------|-----------------|-----------------|----------|--------|------------|--|
| 1 | 0.000000 | 192.168.181.113 | 59.103.129.81 | TCP | 66 |S. | 50420 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 4 | 0.249895 | 192.168.181.113 | 59.103.129.81 | TCP | 66 |S. | 50421 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 5 | 1.051490 | 192.168.181.113 | 59.103.129.81 | TCP | 66 |S. | 50424 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 10 | 2.114089 | 192.168.181.113 | 138.91.171.81 | TCP | 66 |S. | 50428 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 15 | 2.510683 | 192.168.181.113 | 20.212.88.117 | TCP | 66 |S. | 50431 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 16 | 2.638190 | 20.212.88.117 | 192.168.181.113 | TCP | 66 |A..S. | 443 → 50431 [SYN, ACK] Seq=0 Ack=1 Win=16060 Len=0 MSS=1400 SACK_PERM WS=256 |
| 41 | 3.477629 | 192.168.181.113 | 204.79.197.239 | TCP | 66 |S. | 50432 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 42 | 3.607636 | 204.79.197.239 | 192.168.181.113 | TCP | 66 |A..S. | 443 → 50432 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM |
| 77 | 4.805745 | 192.168.181.113 | 20.190.145.140 | TCP | 66 |S. | 50433 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 78 | 4.941732 | 20.190.145.140 | 192.168.181.113 | TCP | 66 |A..S. | 443 → 50433 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM |
| 109 | 6.003405 | 192.168.181.113 | 59.103.129.75 | TCP | 66 |S. | 50434 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 110 | 6.256963 | 192.168.181.113 | 59.103.129.75 | TCP | 66 |S. | 50435 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 165 | 7.001449 | 192.168.181.113 | 142.250.181.138 | TCP | 66 |S. | 50436 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 168 | 7.018331 | 192.168.181.113 | 59.103.129.75 | TCP | 66 |S. | [TCP Retransmission] 50434 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 169 | 7.055308 | 142.250.181.138 | 192.168.181.113 | TCP | 66 |A..S. | 443 → 50436 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM WS=256 |
| 172 | 7.061874 | 192.168.181.113 | 59.103.129.75 | TCP | 66 |S. | 50437 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 203 | 7.269630 | 192.168.181.113 | 59.103.129.75 | TCP | 66 |S. | [TCP Retransmission] 50435 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |

Destination Port: 443
[Stream index: 3]
[Conversation completeness: Incomplete, SYN_SENT (1)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 3027006324
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
Window: 64240
[Calculated window size: 64240]
Checksum: 0x52b8 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation
[Timestamps]
[Time since first frame in this TCP stream: 0.000000000 seconds]
[Time since previous frame in this TCP stream: 0.000000000 seconds]

Syn: Boolean

Packets: 208212 · Displayed: 815 (0.4%)

From PC to YouTube:

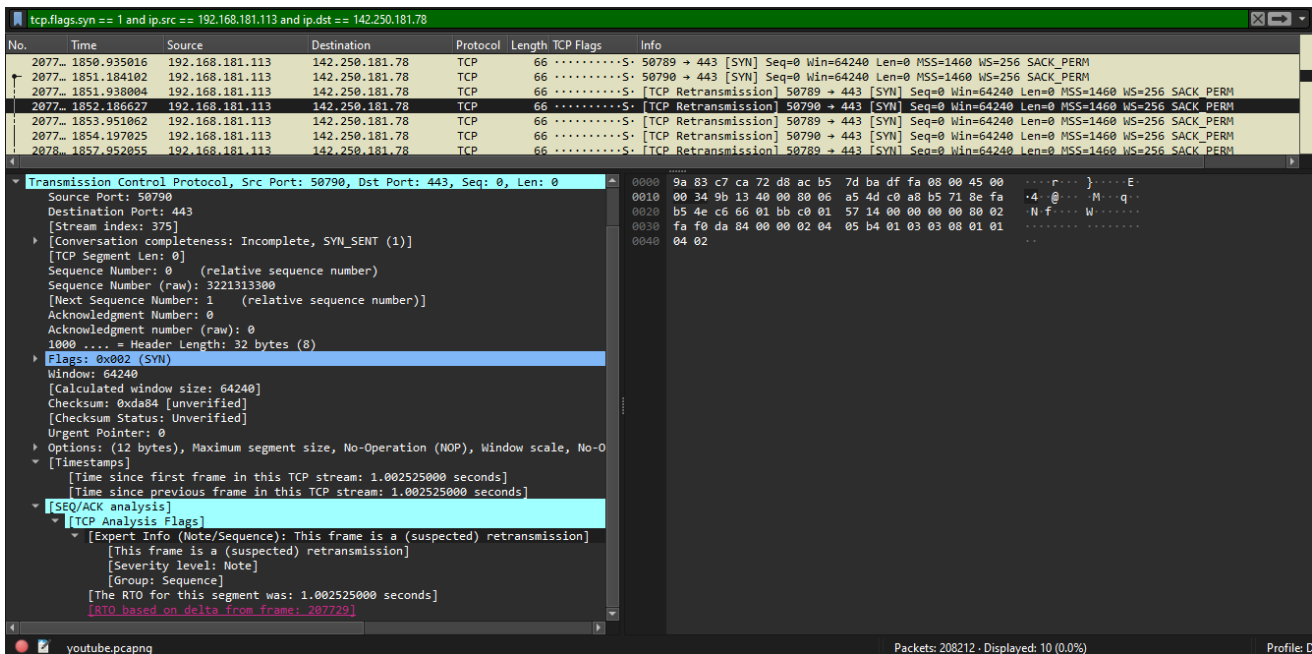
```
tcp.flags.syn == 1
```

```
and ip.src == 192.168.181.113 and ip.dst == 142.250.181.78
```

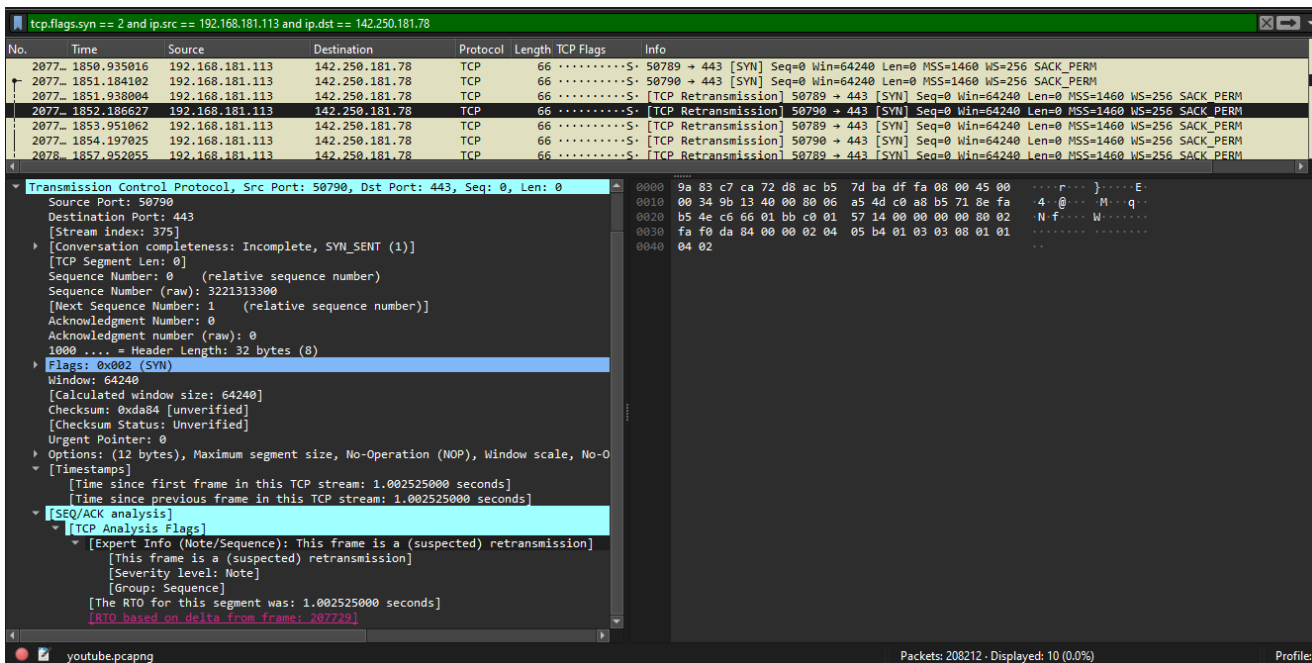
Displayed: 10

Fraction: 0.0%

Captures TCP packets from a PC to YouTube with the SYN flag set, displaying 10 packets, representing 0.0% of the total captured traffic.



`tcp.flags.syn == 2`
`and ip.src == 192.168.181.113 and ip.dst == 142.250.181.78`
 Filters TCP packets from a PC to YouTube with the SYN flag set to 2, focusing on specific SYN values in the TCP handshake.



`tcp.flags.syn == 3`
`and ip.src == 192.168.181.113 and ip.dst == 142.250.181.78`

Filters TCP packets from a PC to YouTube with the SYN flag set to 3, targeting a specific condition in the TCP handshake.

The image shows a Wireshark packet capture with a filter: `tcp.flags.syn == 3 and ip.src == 192.168.181.113 and ip.dst == 142.250.181.78`. The packet list shows several TCP packets, with the selected packet being a SYN packet (Seq=0, Win=64240, Len=0, MSS=1460, WS=256, SACK_PERM) from 192.168.181.113 to 142.250.181.78. The packet details pane shows the following information:

- Source Port: 50790
- Destination Port: 443
- [Stream index: 375]
- [Conversation completeness: Incomplete, SYN_SENT (1)]
- [TCP Segment Len: 0]
- Sequence Number: 0 (relative sequence number)
- Sequence Number (raw): 3221313300
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 0
- Acknowledgment number (raw): 0
- 1000 = Header Length: 32 bytes (8)
- Flags: 0x002 (SYN)
- Window: 64240
- [Calculated window size: 64240]
- Checksum: 0xda84 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-O
- [Timestamps]
- [Time since first frame in this TCP stream: 1.002525000 seconds]
- [Time since previous frame in this TCP stream: 1.002525000 seconds]
- [SEQ/ACK analysis]
- [TCP Analysis Flags]
- [Expert Info (Note/Sequence): This frame is a (suspected) retransmission]
- [This frame is a (suspected) retransmission]
- [Severity level: Note]
- [Group: Sequence]
- [The RTO for this segment was: 1.002525000 seconds]
- [RTO based on delta from frame: 207729]

The packet bytes pane shows the raw data of the packet, including the header and the payload.

FROM YouTube to PC:

0 for #3

The provided information "0 for #3" suggests that there were no TCP packets from YouTube to the PC with the specified conditions (SYN flag set to 3, source IP 192.168.181.113, and destination IP 142.250.181.78) in the captured data under item #3.

The image shows a Wireshark packet capture with a filter: `tcp.flags.syn == 3 and ip.src == 142.250.181.78 and ip.dst == 192.168.181.113`. The packet list is empty, indicating that no packets were captured matching these criteria.

0 displayed for #2

0 displayed for #1

```
tcp.flags.syn == 1
and ip.src == 142.250.181.78 and ip.dst ==
192.168.181.113
```

Indicates that there were no displayed packets for item #2 and item #1 with the provided filters. The specific filter `tcp.flags.syn == 1 and ip.src == 142.250.181.78 and ip.dst == 192.168.181.113` focuses on capturing TCP packets with the SYN flag set from YouTube to the PC.

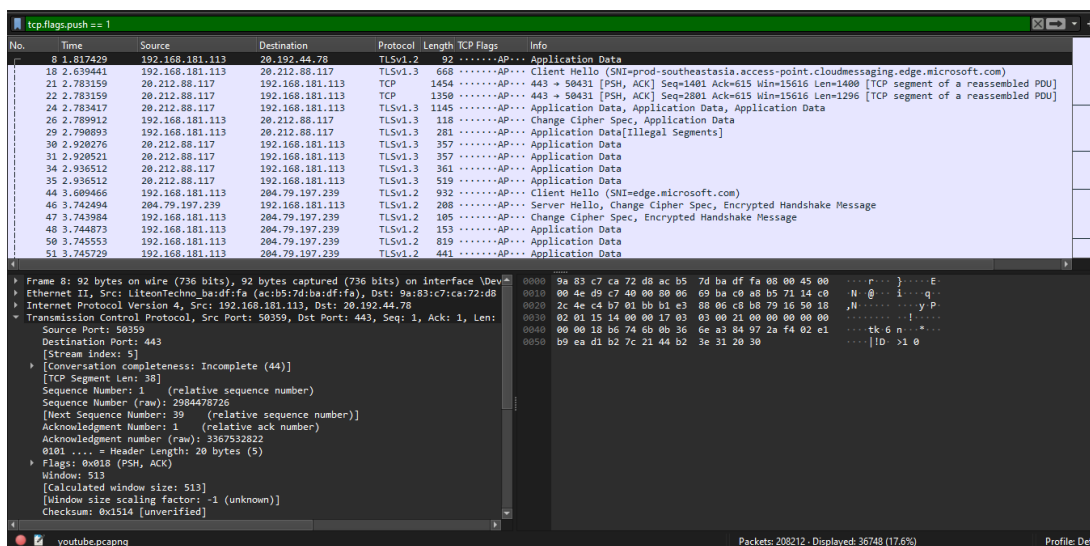
PUSH:

(captured under item #1,#2,#3)

From PC to YouTube:

```
tcp.flags.push == 1
displayed: 36748 Fraction: 17.6%
```

Captures and displays TCP packets with the PUSH flag set from the PC to YouTube, resulting in 36,748 packets, representing 17.6% of the total captured traffic under items #1, #2, and #3.




```
tcp.flags.push == 2
```

The filter `tcp.flags.push == 2` focuses on capturing TCP packets where the PUSH flag is set to 2, targeting a specific condition related to the PUSH flag in the TCP protocol.

| No. | Time | Source | Destination | Protocol | Length | TCP Flags | Info |
|-----|----------|-----------------|-----------------|----------|--------|------------|---|
| 8 | 1.817429 | 192.168.181.113 | 20.192.44.78 | TLSv1.2 | 92 |AP... | Application Data |
| 18 | 2.639441 | 192.168.181.113 | 20.212.88.117 | TLSv1.3 | 668 |AP... | Client Hello (SNI=prod-southeastasia.access-point.cloudmessaging.edge.microsoft.com) |
| 21 | 2.783159 | 20.212.88.117 | 192.168.181.113 | TCP | 1454 |AP... | 443 → 50431 [PSH, ACK] Seq=1401 Ack=615 Win=15616 Len=1400 [TCP segment of a reassembled PDU] |
| 22 | 2.783159 | 20.212.88.117 | 192.168.181.113 | TCP | 1350 |AP... | 443 → 50431 [PSH, ACK] Seq=2801 Ack=615 Win=15616 Len=1296 [TCP segment of a reassembled PDU] |
| 24 | 2.783417 | 20.212.88.117 | 192.168.181.113 | TLSv1.3 | 1145 |AP... | Application Data, Application Data, Application Data |
| 26 | 2.789912 | 192.168.181.113 | 20.212.88.117 | TLSv1.3 | 118 |AP... | Change Cipher Spec, Application Data |
| 29 | 2.790893 | 192.168.181.113 | 20.212.88.117 | TLSv1.3 | 281 |AP... | Application Data[Illegal Segments] |
| 30 | 2.920276 | 20.212.88.117 | 192.168.181.113 | TLSv1.3 | 357 |AP... | Application Data |
| 31 | 2.920521 | 20.212.88.117 | 192.168.181.113 | TLSv1.3 | 357 |AP... | Application Data |
| 34 | 2.936512 | 20.212.88.117 | 192.168.181.113 | TLSv1.3 | 361 |AP... | Application Data |
| 35 | 2.936512 | 20.212.88.117 | 192.168.181.113 | TLSv1.3 | 519 |AP... | Application Data |
| 44 | 3.609466 | 192.168.181.113 | 204.79.197.239 | TLSv1.2 | 932 |AP... | Client Hello (SNI=edge.microsoft.com) |
| 46 | 3.742494 | 204.79.197.239 | 192.168.181.113 | TLSv1.2 | 208 |AP... | Server Hello, Change Cipher Spec, Encrypted Handshake Message |
| 47 | 3.743984 | 192.168.181.113 | 204.79.197.239 | TLSv1.2 | 105 |AP... | Change Cipher Spec, Encrypted Handshake Message |
| 48 | 3.744873 | 192.168.181.113 | 204.79.197.239 | TLSv1.2 | 153 |AP... | Application Data |
| 50 | 3.745553 | 192.168.181.113 | 204.79.197.239 | TLSv1.2 | 819 |AP... | Application Data |
| 51 | 3.745729 | 192.168.181.113 | 204.79.197.239 | TLSv1.2 | 441 |AP... | Application Data |

| 0101 = Header Length: 20 bytes (5) | |
|--|------------------|
| Flags: | 0x018 (PSH, ACK) |
| Window: | 513 |
| [Calculated window size: 513] | |
| [Window size scaling factor: -1 (unknown)] | |
| Checksum: 0x1514 [unverified] | |
| [Checksum Status: Unverified] | |
| Urgent Pointer: 0 | |
| [Timestamps] | |
| [SEQ/ACK analysis] | |
| [Bytes in flight: 38] | |
| [Bytes sent since last PSH flag: 38] | |
| TCP payload (38 bytes) | |
| Transport Layer Security | |
| TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol | |
| Content Type: Application Data (23) | |
| Version: TLS 1.2 (0x0303) | |
| Length: 33 | |
| Encrypted Application Data: 0000000000000018b6746b0b366ea384972af402e1b9ead1b2 | |
| [Application Data Protocol: Hypertext Transfer Protocol] | |

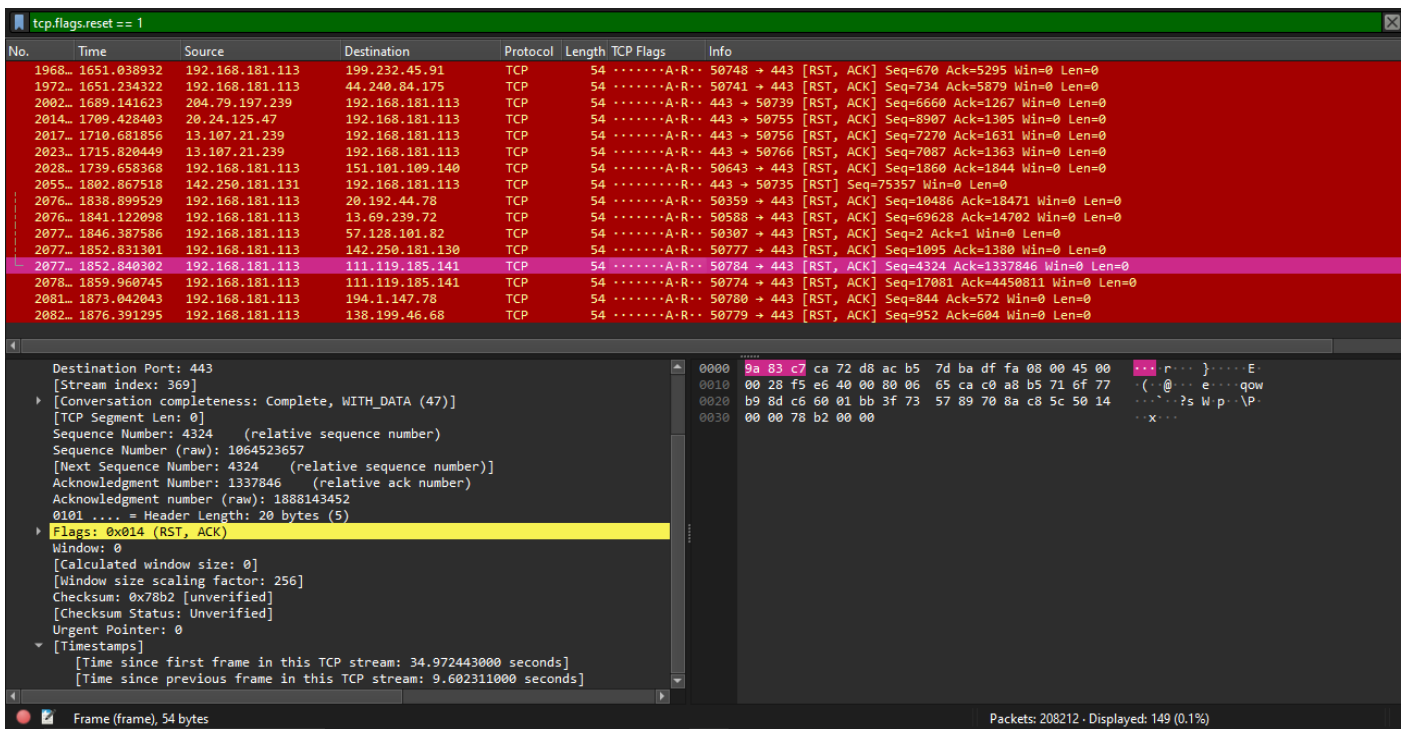
RESET:

```
tcp.flags.reset == 1
```

Displayed: 149 Fraction:0.1%

Same display and fraction for the Capture Item #2 and #3.

Captures and displays TCP packets with the RESET (RST) flag set to 1. The displayed count is 149 packets, constituting 0.1% of the total captured traffic, and the same applies for Capture Items #2 and #3. Captures TCP packets with the RESET (RST) flag set to 1, displaying 149 packets, constituting 0.1% of the total traffic, consistent across Capture Items #2 and #3. This filter helps identify reset events in the TCP communication.



YouTube Table for set flags for capture item #1

| FLAGS | COUNT | FRACTION |
|-------|-------|----------|
| SYN | 10 | 0.0% |
| PSH | 36748 | 17.6% |
| RST | 149 | 0.1% |

Reference Videos:

<https://youtu.be/u4ht-E-Kihk?si=4SBxFQ9y8TPN8S9e>

<https://youtu.be/5qecyZHL-GU?si=89GhFkp3VLI0bHWZ>

VPN PROJECT

Introduction:

A Virtual Private Network (VPN) is a service designed to create a secure, encrypted connection to ensure privacy and anonymity while utilizing the internet. VPNs extend a private network across a public network, enabling users to securely send and receive data.

II. Why use a VPN?

1. **Privacy and Anonymity:** VPNs hide a user's browser history, IP address, and geographical location, enhancing security and preventing unauthorized access to personal data.
2. **Bypassing Geographical Restrictions:** VPNs enable access to restricted content based on location, allowing users to visit otherwise unavailable websites.
3. **Remote Access:** VPNs provide secure remote access to a company's network, facilitating work from home or while traveling.
4. **Public WiFi Security:** VPNs protect users on public WiFi networks from hackers and cybercriminals attempting to intercept sensitive information.

III. How VPNs Work:

1. **Tunneling Protocols:** VPNs utilize tunneling protocols like OpenVPN, SSTP, and IKEv2 for data encryption and decryption.

2. **Encryption:** VPNs use encryption to secure data transmitted over the internet, preventing unauthorized reading without the decryption key.
3. **IP Address Masking:** VPNs replace a user's IP address with that of the VPN server, maintaining anonymity and preventing tracking.

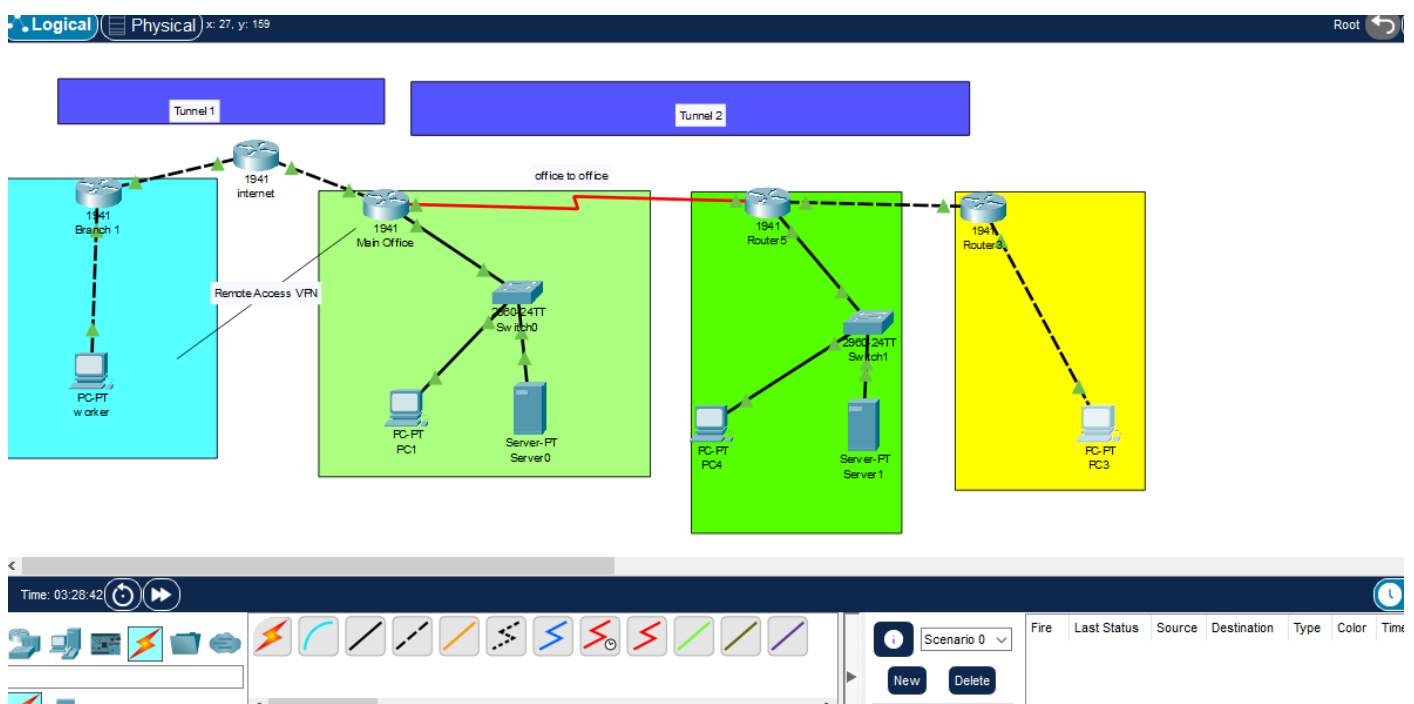
IV. Types of VPNs:

1. **Remote Access VPNs:** Allow individual users to securely connect to a private network over the internet.
2. **Site-to-Site VPNs:** Connect entire networks in different locations, ensuring secure communication between them.
3. **Hardware VPNs:** Physical devices providing VPN functionality, commonly used for added security in enterprise environments.

Software Used:

Cisco Packet Tracer

Visual Representation:



Process:

In this scenario, specific network devices were chosen, including Cisco 1941 routers, a 2960-24 switch with a battery backup, and a server. The reasons behind these choices are:

Cisco 1941 Routers:

- *High-Performance Routing:* Known for high-performance capabilities suitable for routing tasks.
- *Scalability:* Offers scalability to accommodate growing network needs.
- *Security Features:* Advanced security features for firewall capabilities, access control, and VPN support.
- *Modular Design:* Flexibility in adding modules for specific functionalities.
- *Reliability:* Ensures uninterrupted connectivity and minimizes downtime.

Cisco 2960-24 Switch:

- *Network Switching:* Used for local network switching, providing high-performance and low-latency communication.
- *Port Density:* With 24 ports, accommodates numerous devices within the local network.
- *Battery Backup:* Ensures continuous power supply, crucial for maintaining network operations during power outages.

Server:

The server serves various purposes, contributing to the overall functionality, efficiency, and management of the network:

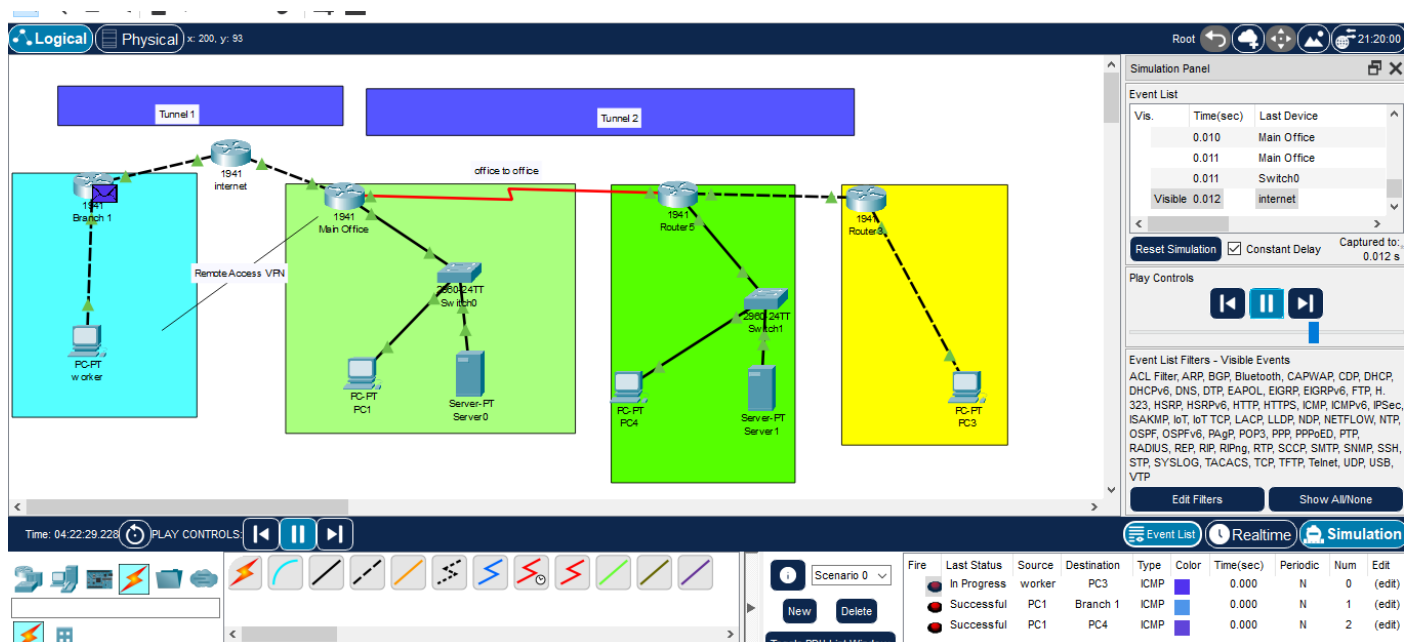
- *Centralized Resource Hosting*

- *User Authentication and Authorization*
- *Network Services*
- *Data Storage and Backup*
- *Application Hosting*
- *Security Management*
- *Power Resilience and Controlled Shutdown*
- *Centralized Updates and Patch Management*
- *Network Administration and Monitoring*

WORKING

Network Connectivity:

The Cisco 1941 routers are responsible for routing traffic within your network. They facilitate communication between different subnets and connect your local network to the internet.

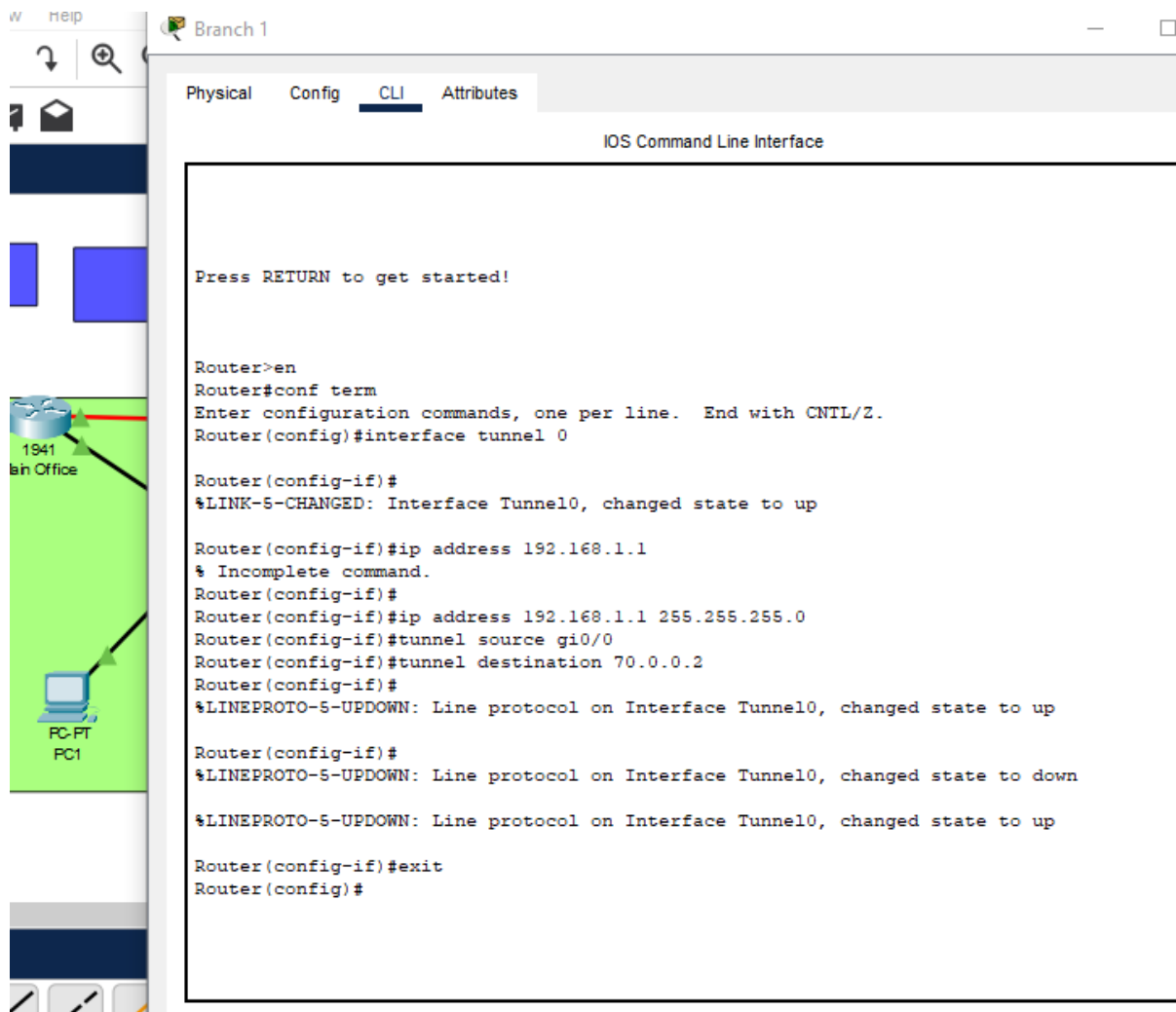


VPN Tunnel Configuration:

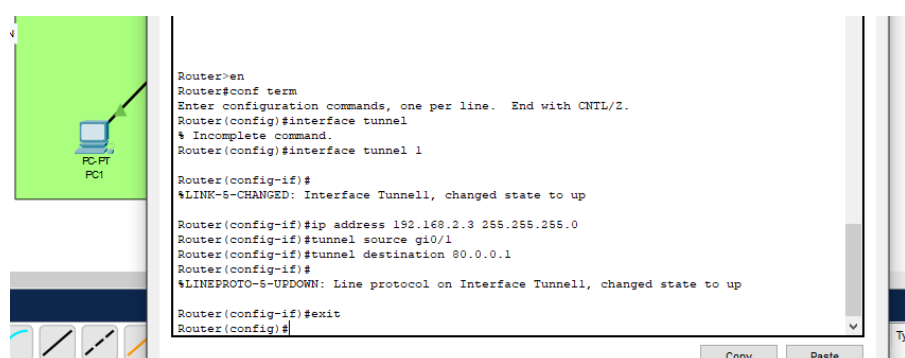
The routers are configured to establish an IPsec VPN tunnel

between them. This tunnel allows secure communication between the routers, even if they have duplicate LAN subnets. The VPN ensures that data exchanged between the routers is encrypted and secure.

BRANCH 1:



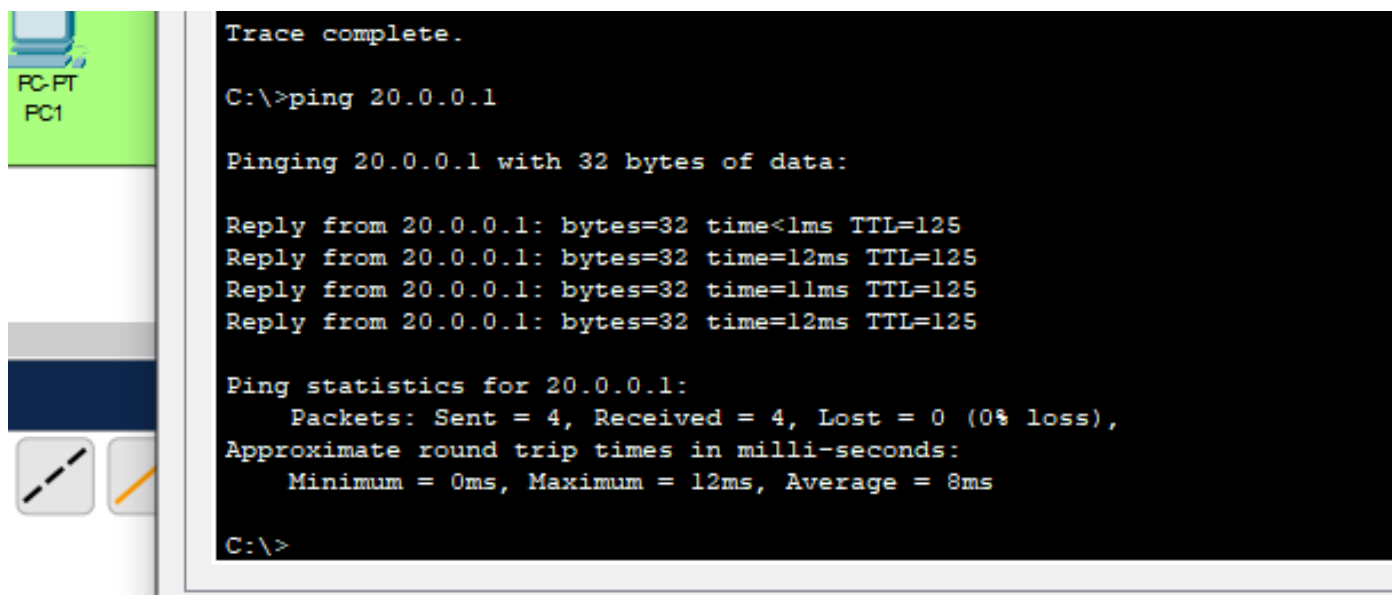
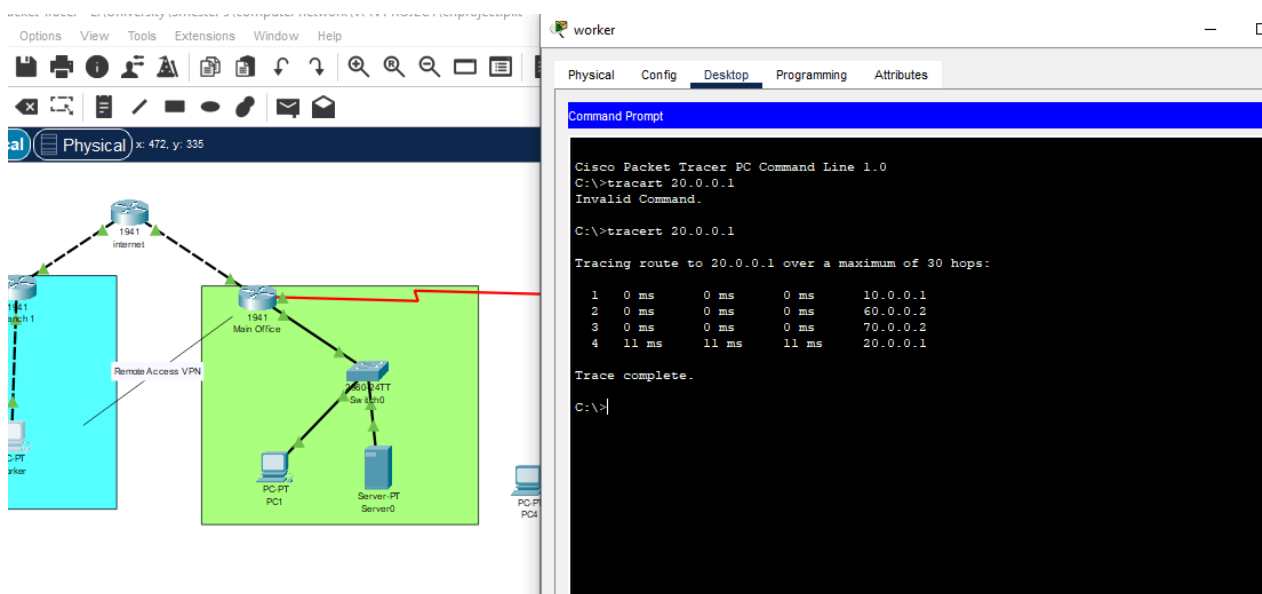
Last Router:



Switching and Local Network Connectivity:

The Cisco 2960-24 switch is used for local network switching. It provides efficient communication between devices within your local network, allowing devices to connect, communicate, and share resources seamlessly

Worker 1 to Main Office:



Worker 1 is remotely accessing the main office, bypassing the router for direct connectivity. This streamlined connection enhances efficiency in accessing essential resources from the main office.

```

Pinging 20.0.0.2 with 32 bytes of data:

Reply from 20.0.0.2: bytes=32 time<1ms TTL=124
Reply from 20.0.0.2: bytes=32 time=20ms TTL=124
Reply from 20.0.0.2: bytes=32 time=10ms TTL=124
Reply from 20.0.0.2: bytes=32 time=1ms TTL=124

Ping statistics for 20.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 20ms, Average = 7ms

C:\>tracert 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    10.0.0.3
  1  *        *        *        Request timed out.
  2  *        *        *        Request timed out.
  3  *        *        *        Request timed out.
  4  *        *        *        Request timed out.
  5  *        *        *        Request timed out.
  6  *        *        *        Request timed out.
  7  *        *        *        Request timed out.
  8  16 ms    12 ms    12 ms    192.168.1.2

Trace complete.

C:\>tracert 192.168.1.2

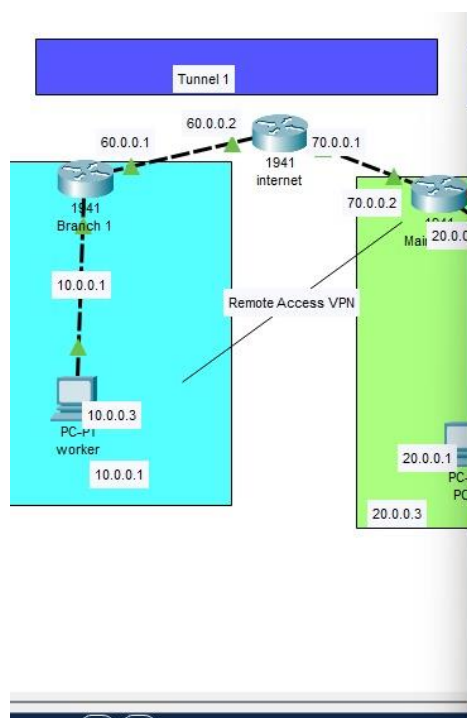
Tracing route to 192.168.1.2 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    10.0.0.3
  1  0 ms    0 ms    0 ms    192.168.1.2

Trace complete.

C:\>

```



```

  1  0 ms    0 ms    0 ms    10.0.0.1
  2  0 ms    0 ms    0 ms    60.0.0.2
  3  1 ms    0 ms    0 ms    70.0.0.2
  4  0 ms    0 ms    0 ms    20.0.0.1

Trace complete.

C:\>tracert 20.0.0.1

Tracing route to 20.0.0.1 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    10.0.0.1
  1  0 ms    1 ms    0 ms    60.0.0.2
  2  0 ms    0 ms    0 ms    70.0.0.2
  3  21 ms   0 ms    10 ms   20.0.0.1

Trace complete.

C:\>tracert 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    10.0.0.1
  1  0 ms    0 ms    0 ms    192.168.1.2

Trace complete.

C:\>tracert 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops:

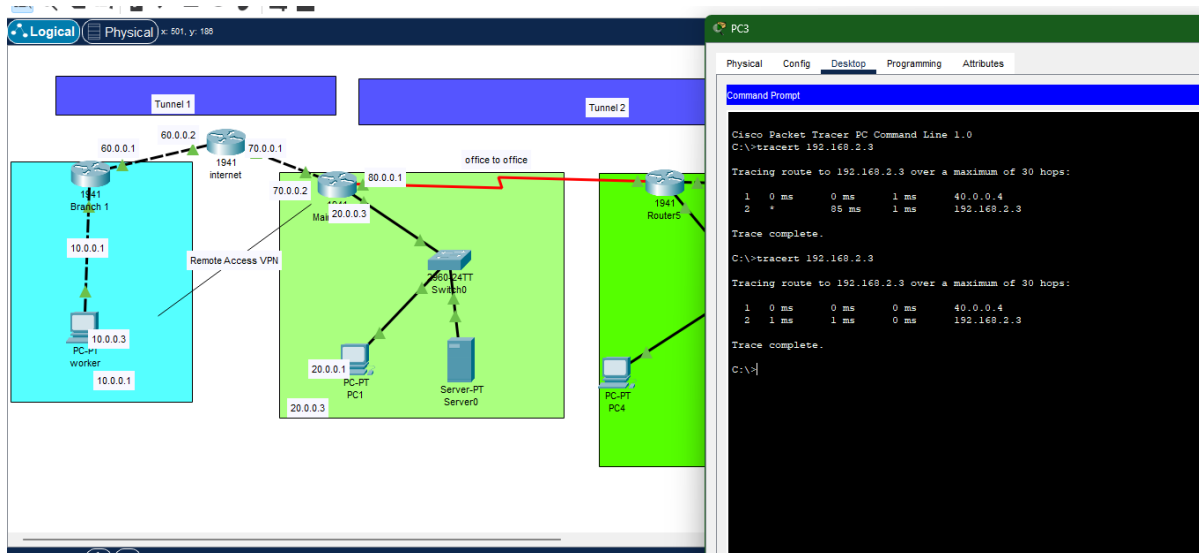
  0  0 ms    0 ms    0 ms    10.0.0.1
  1  0 ms    0 ms    0 ms    192.168.1.2

Trace complete.

C:\>

```

TUNNEL 2 ACCESSING FROM LAST Branch/WORKER:



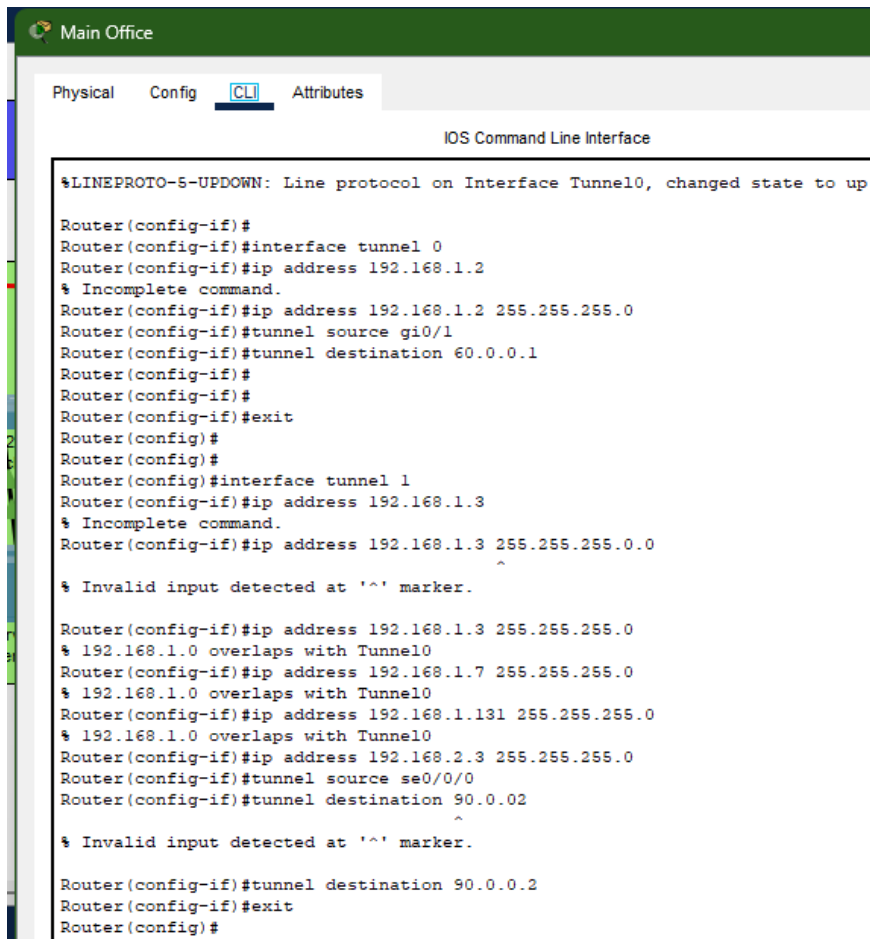
Setting Tunnel 2 for Last worker (PC3) and Main Office:

```
Router3
Physical Config CLI Attributes
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up

Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#interface tunnel 1
Router(config-if)#ip address 192.168.2.4
% Incomplete command.
Router(config-if)#ip address 192.168.2.4 255.255.255.0
Router(config-if)#tunnel source gi0/1
Router(config-if)#tunnel destination 80.0.0.1
Router(config-if)#exit
Router(config)#
```

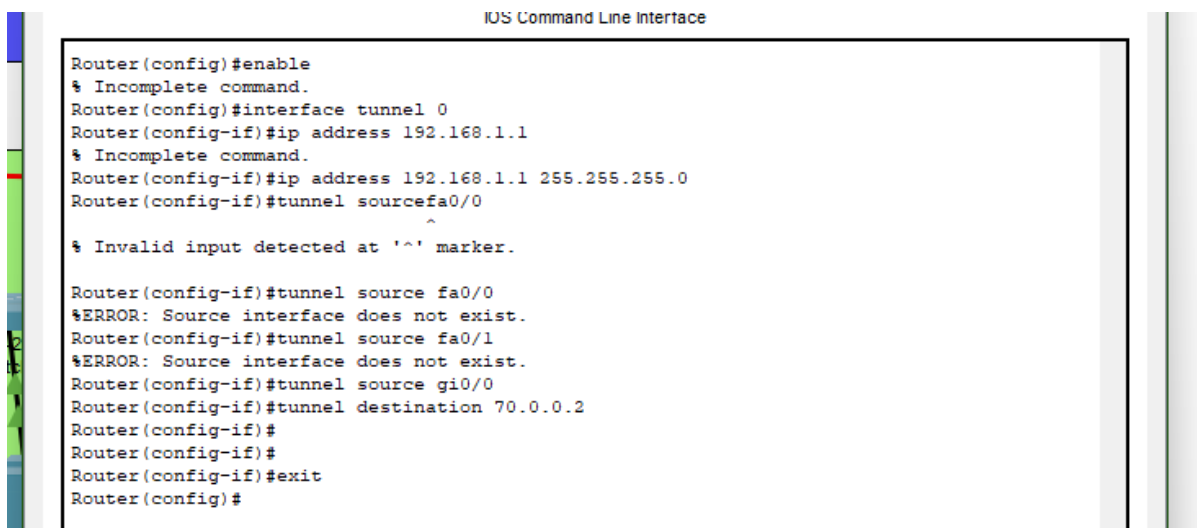
Main Office Tunnel Configuration:



The screenshot shows the 'Main Office' application window with the 'CLI' tab selected. The title bar indicates 'IOS Command Line Interface'. The terminal output shows the following commands and responses:

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
Router(config-if)#
Router(config-if)#interface tunnel 0
Router(config-if)#ip address 192.168.1.2
% Incomplete command.
Router(config-if)#ip address 192.168.1.2 255.255.255.0
Router(config-if)#tunnel source gi0/1
Router(config-if)#tunnel destination 60.0.0.1
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#interface tunnel 1
Router(config-if)#ip address 192.168.1.3
% Incomplete command.
Router(config-if)#ip address 192.168.1.3 255.255.255.0
% Invalid input detected at '^' marker.
Router(config-if)#ip address 192.168.1.3 255.255.255.0
% 192.168.1.0 overlaps with Tunnel0
Router(config-if)#ip address 192.168.1.7 255.255.255.0
% 192.168.1.0 overlaps with Tunnel0
Router(config-if)#ip address 192.168.1.131 255.255.255.0
% 192.168.1.0 overlaps with Tunnel0
Router(config-if)#ip address 192.168.2.3 255.255.255.0
Router(config-if)#tunnel source se0/0/0
Router(config-if)#tunnel destination 90.0.0.2
% Invalid input detected at '^' marker.
Router(config-if)#tunnel destination 90.0.0.2
Router(config-if)#exit
Router(config)#
```

Setting Tunnel 0 configuration in Branch 1:



The screenshot shows the 'IOS Command Line Interface' window with the following commands and responses:

```
Router(config)#enable
% Incomplete command.
Router(config)#interface tunnel 0
Router(config-if)#ip address 192.168.1.1
% Incomplete command.
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#tunnel source fa0/0
% Invalid input detected at '^' marker.
Router(config-if)#tunnel source fa0/0
%ERROR: Source interface does not exist.
Router(config-if)#tunnel source fa0/1
%ERROR: Source interface does not exist.
Router(config-if)#tunnel source gi0/0
Router(config-if)#tunnel destination 70.0.0.2
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#
```

Server Functionality:

The server serves as a centralized hub for hosting various resources, including applications, databases, and shared files. It

provides a platform for user authentication and authorization,
ensuring secure access to network resources.

ACCESSING SERVER FROM WORKER 1:

The image displays two screenshots of a network simulation environment, likely Packet Tracer, showing a network topology and a web browser interface.

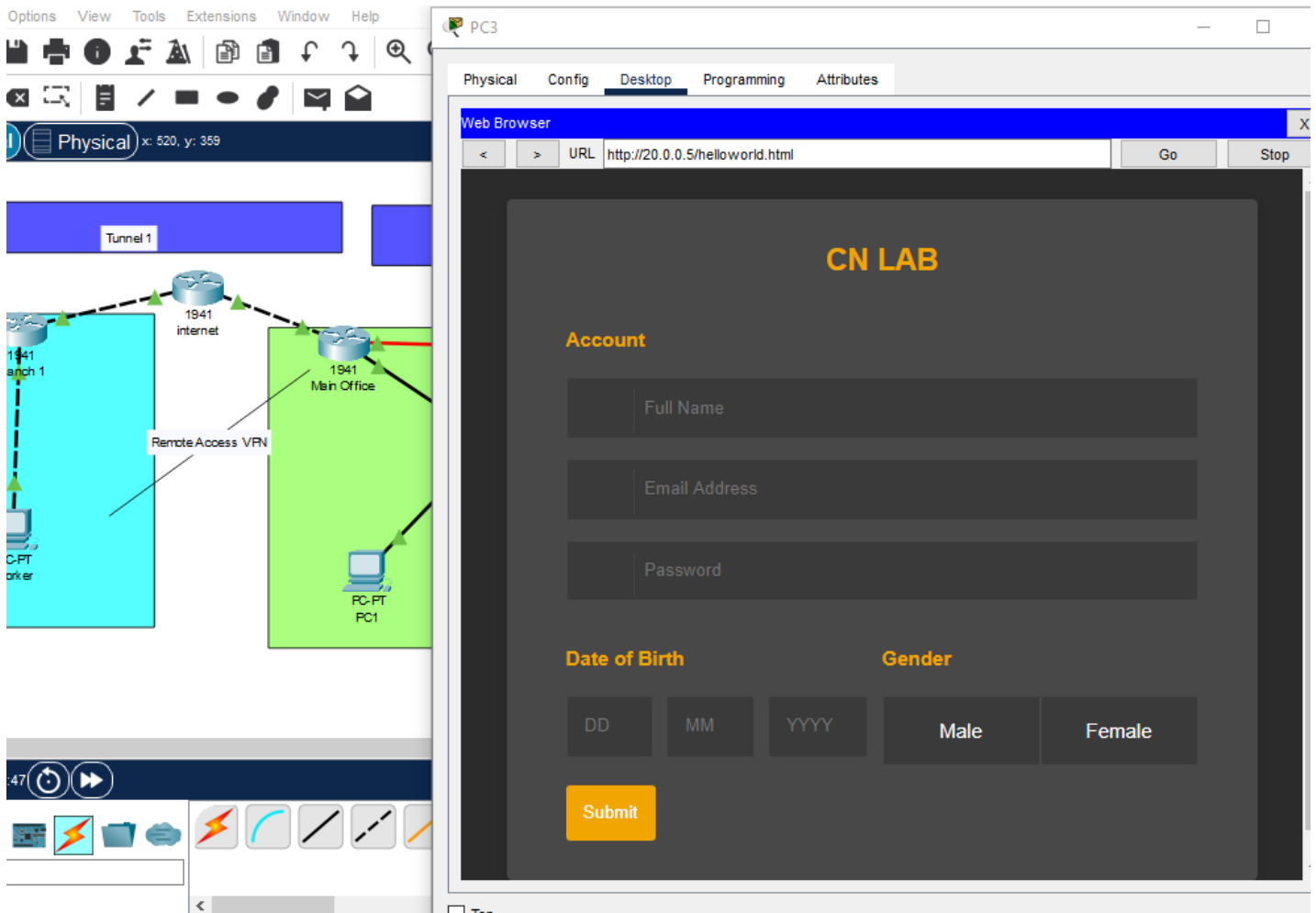
Top Screenshot:

- Network Diagram:** Shows a network topology with a central "1941 Internet" cloud. On the left, "Branch 1" (1941) is connected to the Internet. On the right, "Main Office" (1941) is connected to the Internet. A "Remote Access VPN" is established between Branch 1 and Main Office. A "PC-PT worker" is connected to Branch 1, and a "PC-PT PC1" is connected to Main Office. A "Tunnel 1" is shown at the top.
- Web Browser:** A "Web Browser" window is open, displaying the "CN LAB" login page. The URL is `http://www.login1.com/helloworld.html`. The page includes fields for "Full Name", "Email Address", and "Password". Below these are "Date of Birth" fields (DD, MM, YYYY) and "Gender" options (Male, Female). A "Submit" button is at the bottom.

Bottom Screenshot:

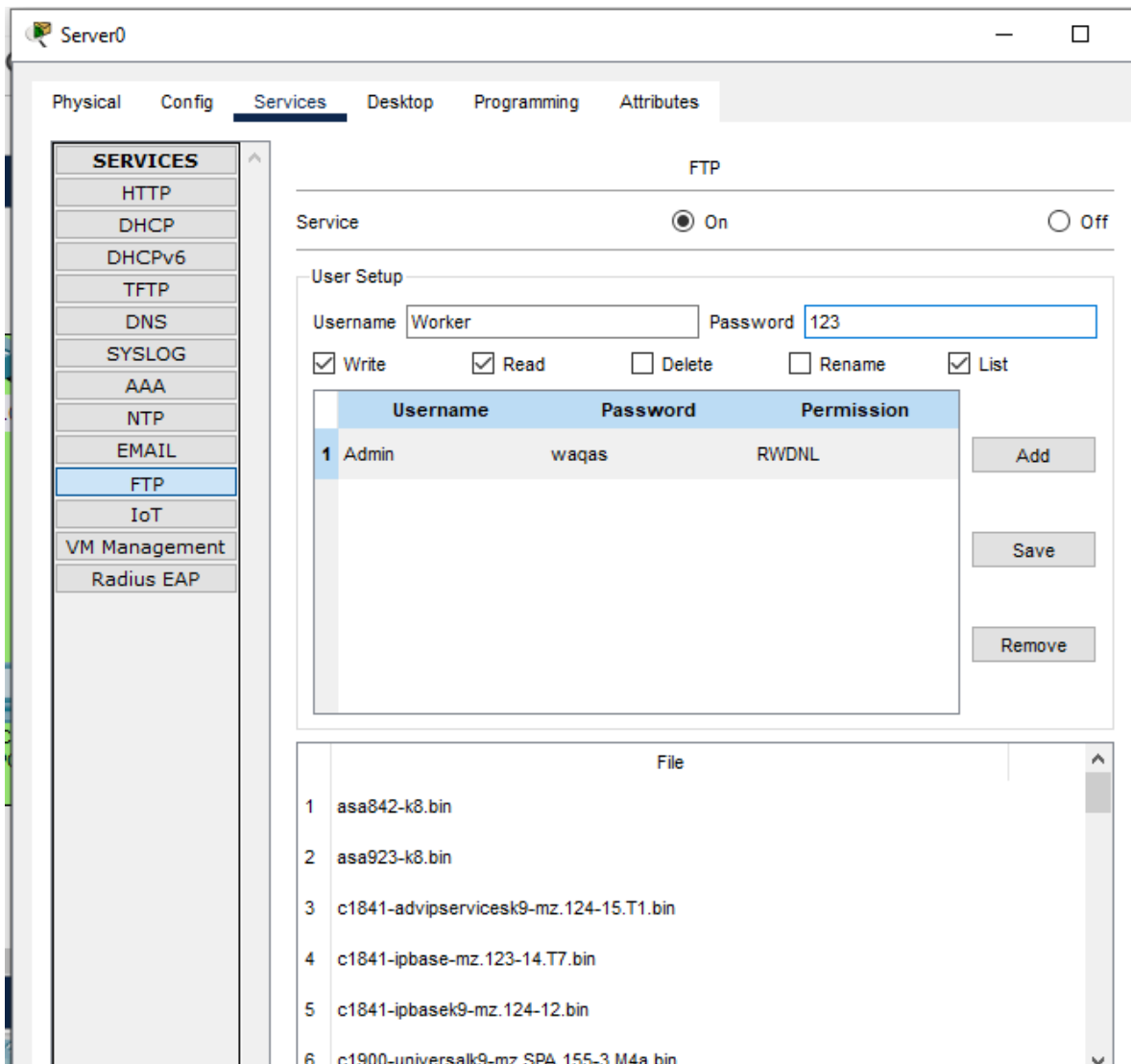
- Network Diagram:** Similar to the top screenshot, but the "PC-PT worker" is now connected to the "Main Office" (1941) via the "Remote Access VPN".
- Web Browser:** A "Web Browser" window is open, displaying the "CN LAB" login page. The URL is `http://20.0.0.5/helloworld.html`. The page includes fields for "Full Name", "Email Address", and "Password". Below these are "Date of Birth" fields (DD, MM, YYYY) and "Gender" options (Male, Female). A "Submit" button is at the bottom.

Worker 3 to Main Office:

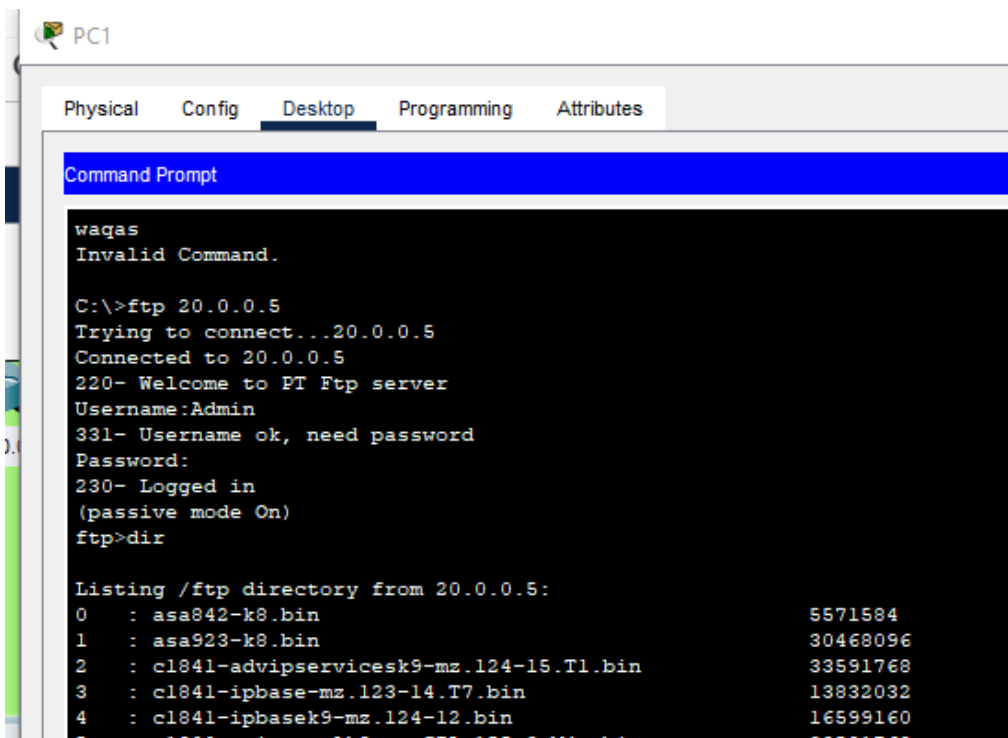


Setting Up the FTP (File Transfer Protocol):

FTP (File Transfer Protocol) is a standard network protocol used for the seamless transfer of files between a client and a server on a computer network. It provides a reliable method for sharing files over the internet or an intranet, allowing users to upload, download, and manage files efficiently. FTP is commonly employed in scenarios where large files or numerous files need to be transferred between devices or servers.



Accessing Directory through Admin PC:



File Uploading & Downloading from through admin pc:

```
30 : ir800_yocto-1.7.2_python-2.7.3.tar 69120
31 : pt1000-i-mz.122-28.bin 55718
32 : pt3000-i6q412-mz.121-22.EA4.bin 31173
ftp>put ADMIN.txt

Writing file ADMIN.txt to 20.0.0.5:
File transfer in progress...

[Transfer complete - 425 bytes]

425 bytes copied in 0.026 secs (16346 bytes/sec)
ftp>
```

```
31 : ir800_yocto-1.7.2_python-2.7.3.tar
32 : pt1000-i-mz.122-28.bin
33 : pt3000-i6q412-mz.121-22.EA4.bin
ftp>get ADMIN.txt

Reading file ADMIN.txt from 20.0.0.5:
File transfer in progress...

[Transfer complete - 425 bytes]

425 bytes copied in 0.003 secs (141666 bytes/sec)
ftp>
```

Setting up the email (SMTP) on Server 2:

ADMIN:

PC4

Physical Config **Desktop** Programming Attributes

Configure Mail [X]

User Information

Your Name:

EmailAddress

Server Information

Incoming Mail Server

Outgoing Mail Server

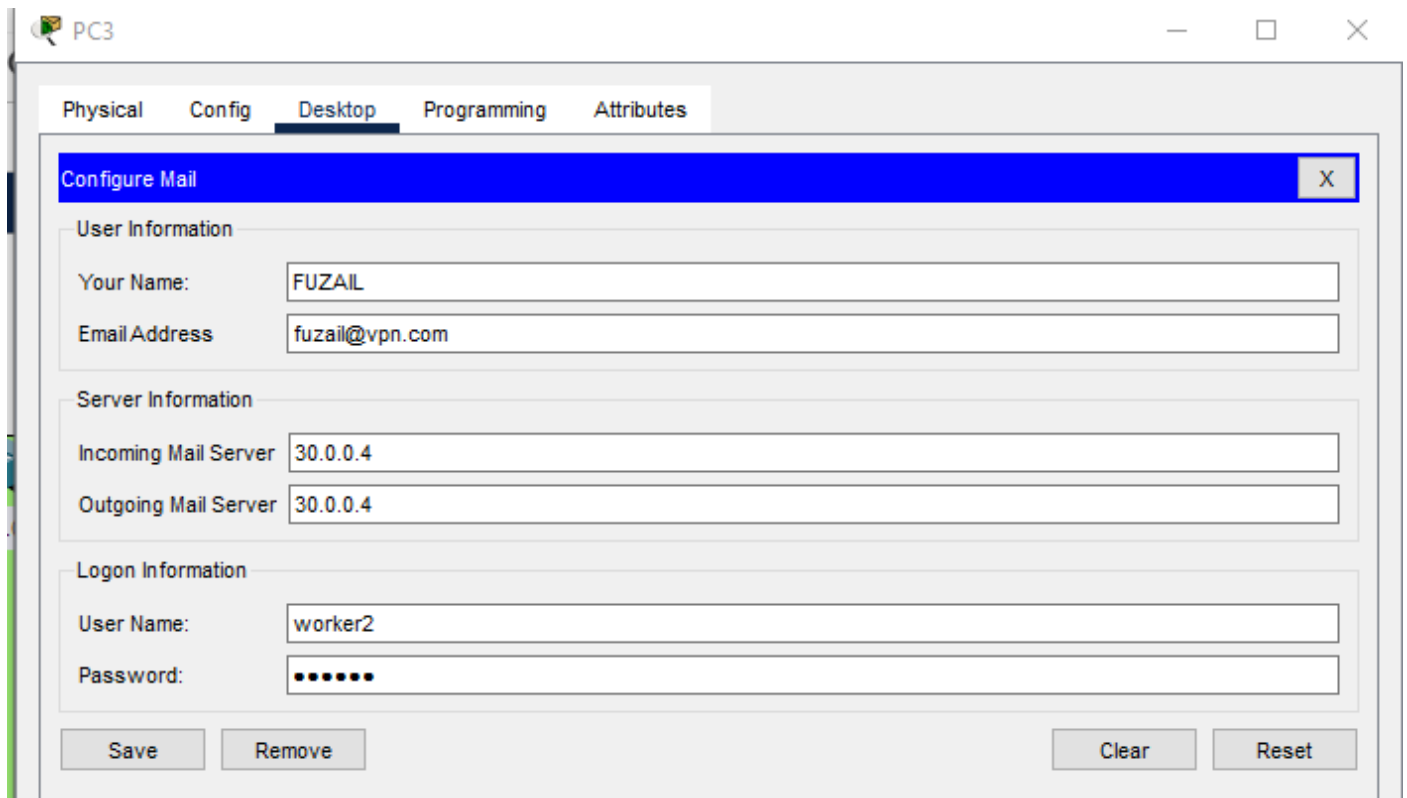
Logon Information

User Name:

Password:

Save Remove Clear Reset

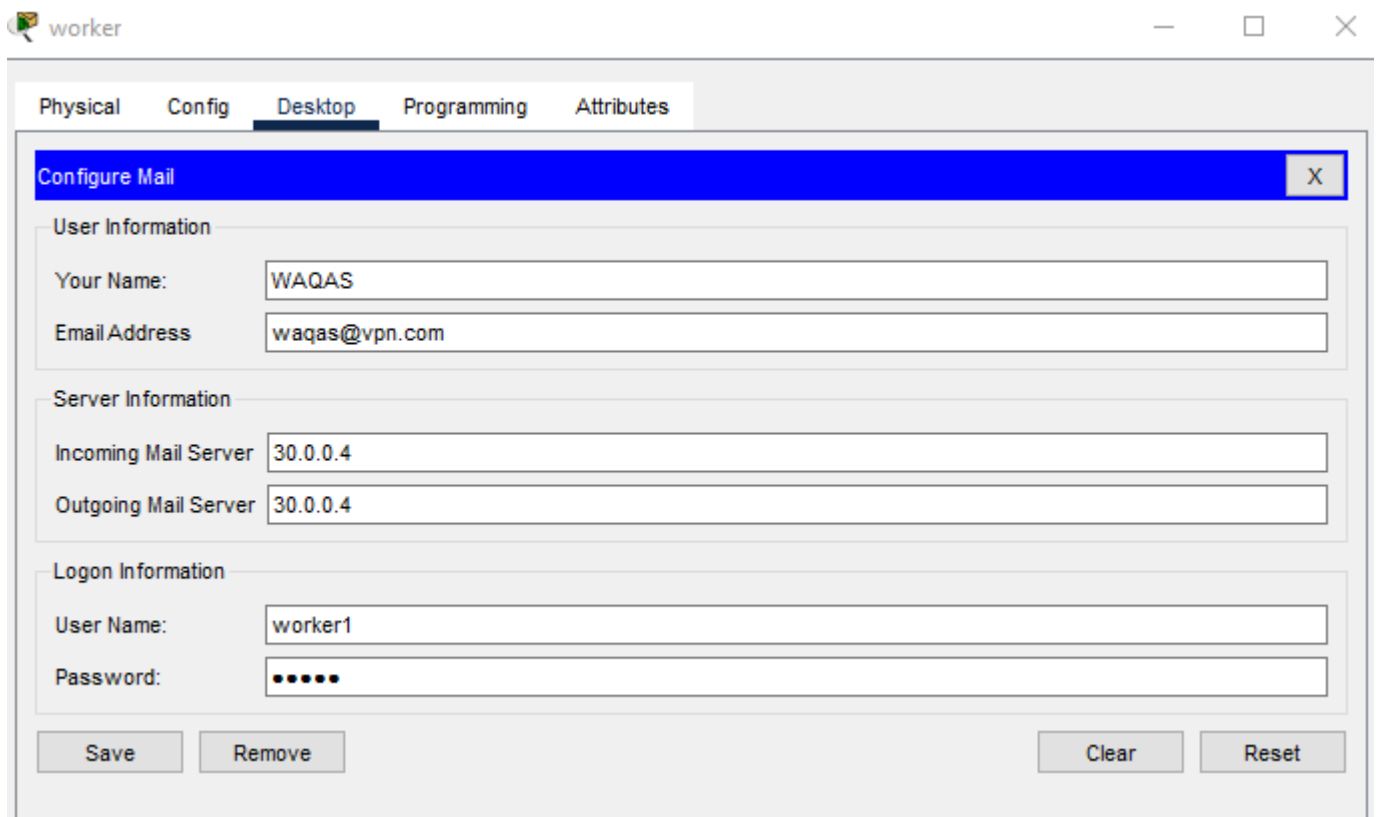
Worker1:



The screenshot shows a window titled 'PC3' with a tabbed interface. The 'Desktop' tab is selected. A 'Configure Mail' dialog box is open, featuring a blue title bar with a close button (X). The dialog is organized into three sections: 'User Information', 'Server Information', and 'Logon Information'. In the 'User Information' section, 'Your Name' is 'FUZAIL' and 'Email Address' is 'fuzail@vpn.com'. In the 'Server Information' section, both 'Incoming Mail Server' and 'Outgoing Mail Server' are set to '30.0.0.4'. In the 'Logon Information' section, 'User Name' is 'worker2' and 'Password' is masked with dots. At the bottom, there are four buttons: 'Save', 'Remove', 'Clear', and 'Reset'.

| Section | Field | Value |
|--------------------|----------------------|----------------|
| User Information | Your Name: | FUZAIL |
| | Email Address | fuzail@vpn.com |
| Server Information | Incoming Mail Server | 30.0.0.4 |
| | Outgoing Mail Server | 30.0.0.4 |
| Logon Information | User Name: | worker2 |
| | Password: | |

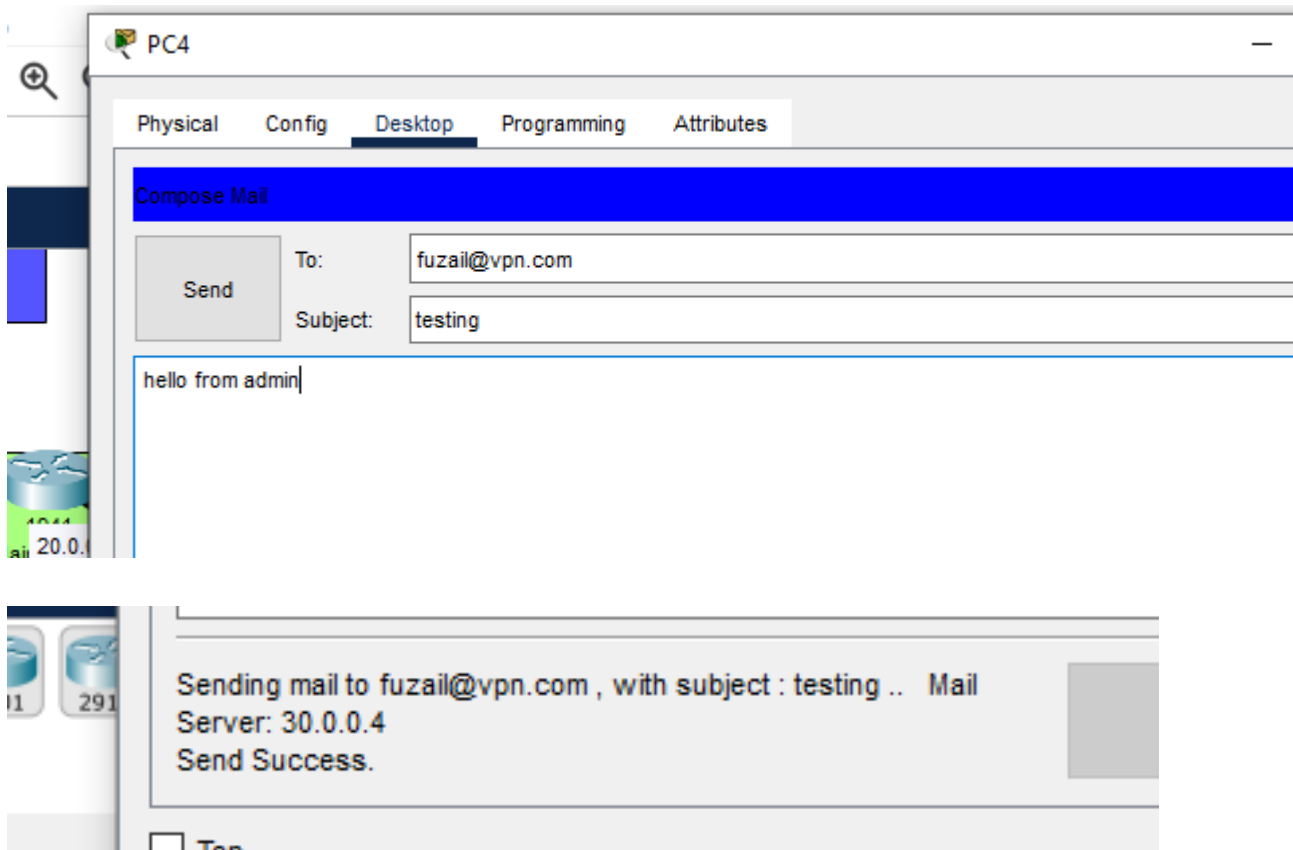
Worker2:



The screenshot shows a window titled 'worker' with a tabbed interface. The 'Desktop' tab is selected. A 'Configure Mail' dialog box is open, featuring a blue title bar with a close button (X). The dialog is organized into three sections: 'User Information', 'Server Information', and 'Logon Information'. In the 'User Information' section, 'Your Name' is 'WAQAS' and 'Email Address' is 'waqas@vpn.com'. In the 'Server Information' section, both 'Incoming Mail Server' and 'Outgoing Mail Server' are set to '30.0.0.4'. In the 'Logon Information' section, 'User Name' is 'worker1' and 'Password' is masked with dots. At the bottom, there are four buttons: 'Save', 'Remove', 'Clear', and 'Reset'.

| Section | Field | Value |
|--------------------|----------------------|---------------|
| User Information | Your Name: | WAQAS |
| | Email Address | waqas@vpn.com |
| Server Information | Incoming Mail Server | 30.0.0.4 |
| | Outgoing Mail Server | 30.0.0.4 |
| Logon Information | User Name: | worker1 |
| | Password: | |

Sending mail from admin to worker 1:



Conclusion:

In conclusion, the successful implementation of this project relies on the Cisco 1941 routers, which play a pivotal role in establishing a secure and efficient network infrastructure. Through the deployment of IPsec VPN tunnels, the project ensures data confidentiality and integrity, addressing challenges related to duplicate LAN subnets. The routers excel in routing tasks, enhancing network scalability and reliability. Emphasizing the strategic use of Cisco 1941 routers, the project showcases their adaptability, high-performance routing, and security features, particularly in firewall configurations and intrusion prevention. This streamlined approach underscores the routers' cost-effectiveness, providing a resilient and secure network infrastructure.

Reference Video:

Concept From: <https://youtu.be/LIL2DkFkACo?si=IPsOMUctbyxPouGO>

<https://youtu.be/SYGdxsDApyM?si=zbzzzsL6C5M8rKBF>

<https://youtu.be/lkUq6Pl6his?si=1F5TJhH2QunpZBRV>

<https://youtu.be/8uWmFkrn6qE?si=eLMZ46x2v4IG6UuO>