

# TCP and HTTP Traffic

No.	Time	Source	Destination	Protocol	Length	Info
559	50.819344	192.168.1.115	103.132.16.18	TCP	66	31514 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
560	50.834920	103.132.16.18	192.168.1.115	TCP	66	80 → 31514 [FIN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1412 SACK_PERM WS=128
561	50.835093	192.168.1.115	103.132.16.18	TCP	64	31514 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
562	50.835569	192.168.1.115	103.132.16.18	HTTP	178	GET /v1.txt HTTP/1.1
563	50.862823	103.132.16.18	192.168.1.115	TCP	60	80 → 31514 [ACK] Seq=1 Ack=125 Win=64128 Len=0
564	50.865593	103.132.16.18	192.168.1.115	TCP	60	[TCP Previous segment not captured] 80 → 31514 [FIN, ACK] Seq=188 Ack=125 Win=64128 Len=0
565	50.865639	192.168.1.115	103.132.16.18	TCP	54	[TCP Dup ACK 561#1] 31514 → 80 [ACK] Seq=125 Ack=1 Win=65280 Len=0
566	50.870096	103.132.16.18	192.168.1.115	TCP	233	[TCP Out-Of-Order] 80 → 31514 [PSH, ACK] Seq=1 Ack=125 Win=64128 Len=179
567	50.870221	192.168.1.115	103.132.16.18	TCP	54	31514 → 80 [ACK] Seq=125 Ack=181 Win=65280 Len=0
568	50.871218	192.168.1.115	103.132.16.18	TCP	54	31514 → 80 [FIN, ACK] Seq=125 Ack=181 Win=65280 Len=0
569	50.914227	103.132.16.18	192.168.1.115	TCP	60	80 → 31514 [ACK] Seq=181 Ack=126 Win=64128 Len=0
721	51.222878	192.168.1.115	103.132.16.19	TCP	66	31515 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
722	51.237702	103.132.16.19	192.168.1.115	TCP	66	80 → 31515 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1412 SACK_PERM WS=128
723	51.237870	192.168.1.115	103.132.16.19	TCP	54	31515 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
724	51.238154	192.168.1.115	103.132.16.19	HTTP	165	GET /connecttest.txt HTTP/1.1
725	51.246219	103.132.16.19	192.168.1.115	TCP	60	80 → 31515 [ACK] Seq=1 Ack=112 Win=64256 Len=0
726	51.246470	103.132.16.19	192.168.1.115	TCP	60	[TCP Previous segment not captured] 80 → 31515 [FIN, ACK] Seq=188 Ack=112 Win=64256 Len=0
727	51.246502	192.168.1.115	103.132.16.19	TCP	54	[TCP Dup ACK 723#1] 31515 → 80 [ACK] Seq=112 Ack=1 Win=65280 Len=0
728	51.263204	103.132.16.19	192.168.1.115	TCP	241	[TCP Retransmission] 80 → 31515 [PSH, ACK] Seq=1 Ack=112 Win=64256 Len=187
729	51.263293	192.168.1.115	103.132.16.19	TCP	54	31515 → 80 [ACK] Seq=112 Ack=189 Win=65280 Len=0

# Frame 731: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF\_{F5FBF247-C786-443C-9C19-...}

Ethernet II, Src: TaiwangMI\_7e:93:90 (18:45:93:7e:93:90), Dst: AzureWaveTec\_32:f9:33 (10:68:38:32:f9:33)

Internet Protocol Version 4, Src: 103.132.16.19, Dst: 192.168.1.115

Transmission Control Protocol, Src Port: 80, Dst Port: 31515, Seq: 189, Ack: 113, Len: 0

```

0000  10 68 38 32 f9 33 18 45   93 7e 93 90 08 00 45 00  -h82 3 E .....E.
0010  00 28 00 00 40 0c 06 05   1e 67 84 10 13 c0 a8    -( _@ < . g.....
0020  01 73 00 50 7b 1b 81 4f   4c 5b d6 3d e9 dd 50 10  -s P[.O L]= :P.
0030  01 f6 6b ca 00 00 00 00   00 00 00 00              -k.....

```

The screenshot displays the Wireshark network protocol analyzer interface. The top bar shows standard application icons. The main window is divided into three panes:

- Packet List Pane (Left):** Displays a list of captured packets. The selected packet is 564, which is a TCP segment from 192.168.1.115 to 103.132.16.18.
- Packet Details Pane (Middle):** Provides a hierarchical view of the selected packet's structure. It shows the Ethernet II header, Internet Protocol Version 4 header, and the Transmission Control Protocol (TCP) segment. The TCP segment is identified as a FIN segment (Seq=180, Win=64128, Len=0).
- Packet Bytes Pane (Right):** Shows the raw data of the selected packet in hexadecimal and ASCII format.

The packet details pane for the selected packet (564) shows the following information:

- Ethernet II:** Src: TaiCangT&WEL\_7e:93:90 (18:45:93:7e:93:90), Dst: AzureWaveTec\_32:f9:33 (10:68:38:32:f9:33)
- Internet Protocol Version 4:** Src: 103.132.16.18, Dst: 192.168.1.115
- Transmission Control Protocol:** Src Port: 80, Dst Port: 31514, Seq: 180, Ack: 125, Len: 0

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and the TCP segment.

# DNS Traffic

dns					
No.	Time	Source	Destination	Protocol	Length Info
127	20.790116	192.168.1.254	192.168.1.115	DNS	167 Standard query response 0x0c7d HTTPS beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com SOA ns1.google.com
135	20.809169	192.168.1.254	192.168.1.115	DNS	126 Standard query response 0x4b66 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 142.250.143.94
136	20.809169	192.168.1.254	192.168.1.115	DNS	167 Standard query response 0x9ebb HTTPS beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com SOA ns1.google.com
277	32.741349	192.168.1.115	192.168.1.254	DNS	71 Standard query 0x1063 A i.ytimg.com
278	32.742147	192.168.1.115	192.168.1.254	DNS	71 Standard query 0xc47c HTTPS i.ytimg.com
284	32.769343	192.168.1.254	192.168.1.115	DNS	231 Standard query response 0x1063 A i.ytimg.com A 142.251.12.119 A 74.125.24.119 A 142.251.10.119 A 64.233.170.119 A 74.125.68.119...
285	32.785615	192.168.1.254	192.168.1.115	DNS	128 Standard query response 0xc47c HTTPS i.ytimg.com SOA ns1.google.com
453	48.351161	192.168.1.115	192.168.1.254	DNS	95 Standard query 0xb53f A suggestqueries-clients6.youtube.com
454	48.351704	192.168.1.115	192.168.1.254	DNS	95 Standard query 0xc4a1 HTTPS suggestqueries-clients6.youtube.com
457	48.430663	192.168.1.254	192.168.1.115	DNS	111 Standard query response 0xb53f A suggestqueries-clients6.youtube.com A 142.250.192.46
458	48.430663	192.168.1.254	192.168.1.115	DNS	152 Standard query response 0xc4a1 HTTPS suggestqueries-clients6.youtube.com SOA ns1.google.com
557	50.781649	192.168.1.115	192.168.1.254	DNS	76 Standard query 0xa9d0 A www.msftncsi.com
558	50.809509	192.168.1.254	192.168.1.115	DNS	246 Standard query response 0xa9d0 A www.msftncsi.com CNAME www.msftncsi.com.edgesuite.net CNAME a1961.g2.akamai.net A 103.132.16.1...
719	51.194311	192.168.1.115	192.168.1.254	DNS	83 Standard query 0x69b9 A www.msftconnecttest.com
720	51.220095	192.168.1.254	192.168.1.115	DNS	323 Standard query response 0x69b9 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net...
732	51.383094	192.168.1.115	192.168.1.254	DNS	85 Standard query 0x0f68 A tpc.googlesyndication.com
733	51.383525	192.168.1.115	192.168.1.254	DNS	85 Standard query 0x5587 HTTPS tpc.googlesyndication.com
743	51.417984	192.168.1.254	192.168.1.115	DNS	101 Standard query response 0x0f68 A tpc.googlesyndication.com A 142.251.42.65
744	51.417984	192.168.1.254	192.168.1.115	DNS	142 Standard query response 0x5587 HTTPS tpc.googlesyndication.com SOA ns1.google.com

Frame 558: 246 bytes on wire (1968 bits), 246 bytes captured (1968 bits) on interface \Device\NPF\_{F5F8F247-C786-443C-5000} 10 68 38 32 f9 33 18 45 93 7e 93 90 08 00 45 00 .h82 3 E ..... E

Ethernet II, Src: TalcangT&E1\_7e:93:90 (18:45:93:7e:93:90), Dst: AzureWaveTec\_32:f9:33 (10:68:38:32:f9:33) 0010 00 e8 00 3d 40 00 40 11 b5 06 c0 a8 01 fe c0 a8 ...= @ .....

Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.115 0020 01 73 00 35 cd 9c 00 d4 1a 30 a9 00 81 80 00 01 ...s 5 ..... 0 .....

User Datagram Protocol, Src Port: 53, Dst Port: 52636 0030 00 08 00 00 00 00 03 77 77 77 08 6d 73 66 74 6e .....w ww msftn

Domain Name System (response) 0040 63 73 69 03 63 6f 6d 00 00 01 00 01 c0 0c 00 05 csi com .....

0050 00 01 00 00 0d de 00 20 03 77 77 77 08 6d 73 66 ..... www msf

0060 74 6e 63 73 69 03 63 6f 6d 09 65 64 67 65 73 75 tncsi co m edgesu

0070 69 74 65 03 6e 65 74 00 c0 2e 00 05 00 01 00 00 ite net .....

0080 00 a1 00 12 05 61 31 39 36 31 02 67 32 06 61 6b ...a19 61 g2 ak

0090 61 6d 61 69 c0 49 c0 5a 00 01 00 01 00 00 00 0d amai I Z .....

00a0 00 04 67 84 10 12 c0 5a 00 01 00 01 00 00 00 0d g...Z .....

00b0 00 04 67 84 10 19 c0 5a 00 01 00 01 00 00 00 0d g...Z .....

00c0 00 04 67 84 10 09 c0 5a 00 01 00 01 00 00 00 0d g...Z .....

00d0 00 04 67 84 10 13 c0 5a 00 01 00 01 00 00 00 0d g...Z .....

00e0 00 04 67 84 10 11 c0 5a 00 01 00 01 00 00 00 0d g...Z .....

00f0 00 04 67 84 10 10 g... ..

http					
No.	Time	Source	Destination	Protocol	Length Info
562	50.835569	192.168.1.115	103.132.16.18	HTTP	178 GET /ncsi.txt HTTP/1.1
724	51.238154	192.168.1.115	103.132.16.19	HTTP	165 GET /connecttest.txt HTTP/1.1