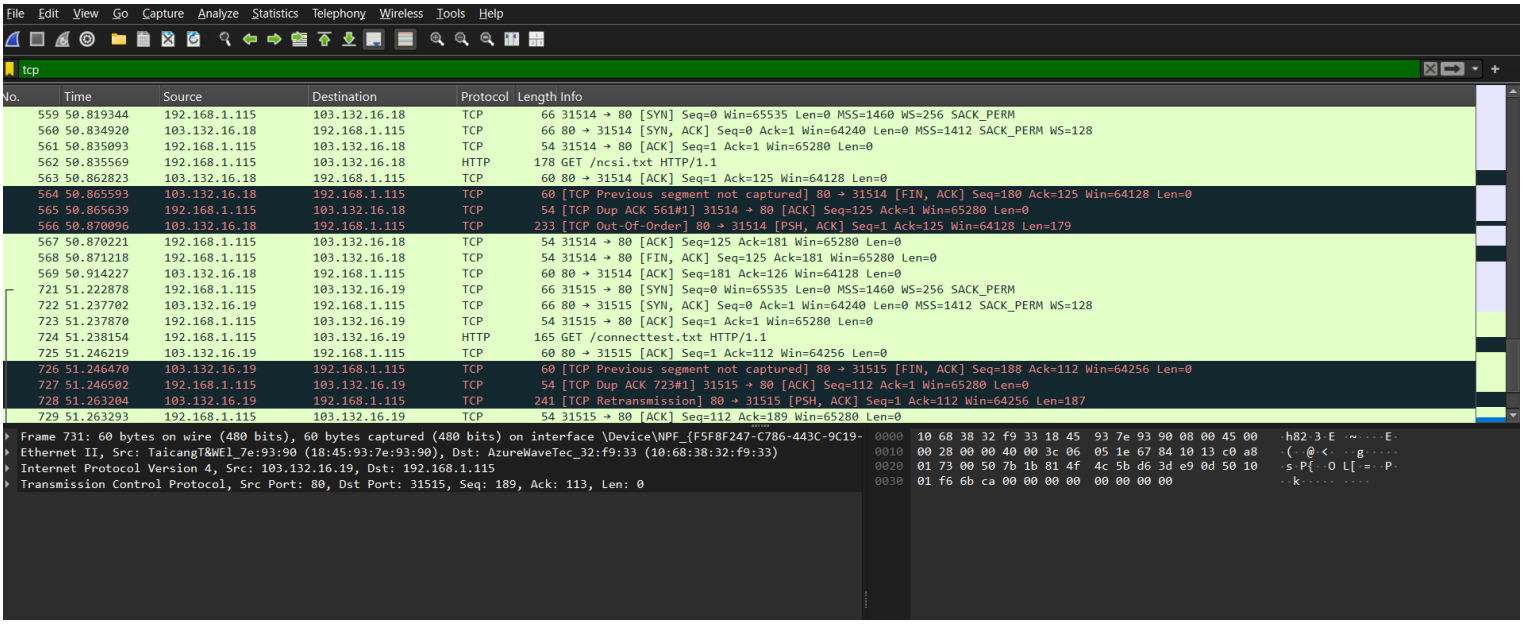
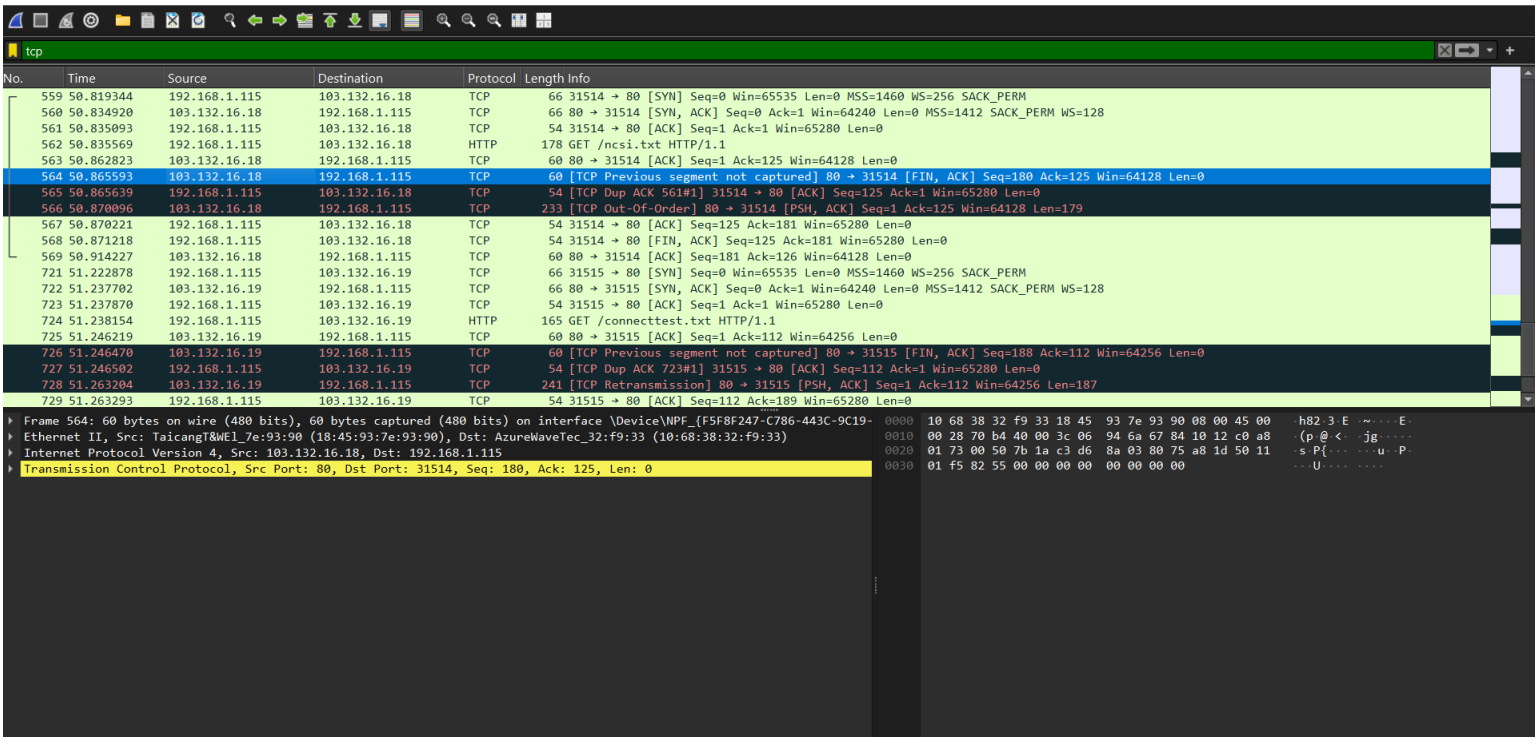
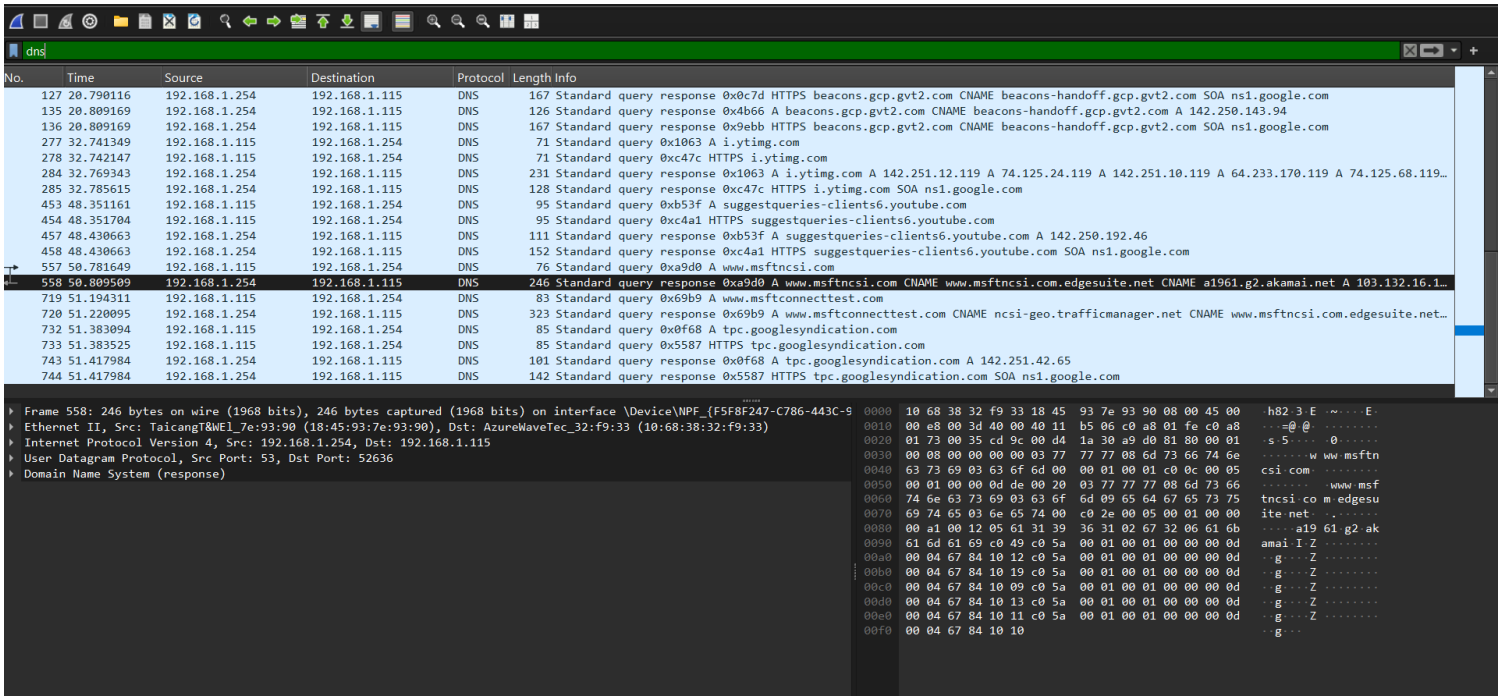
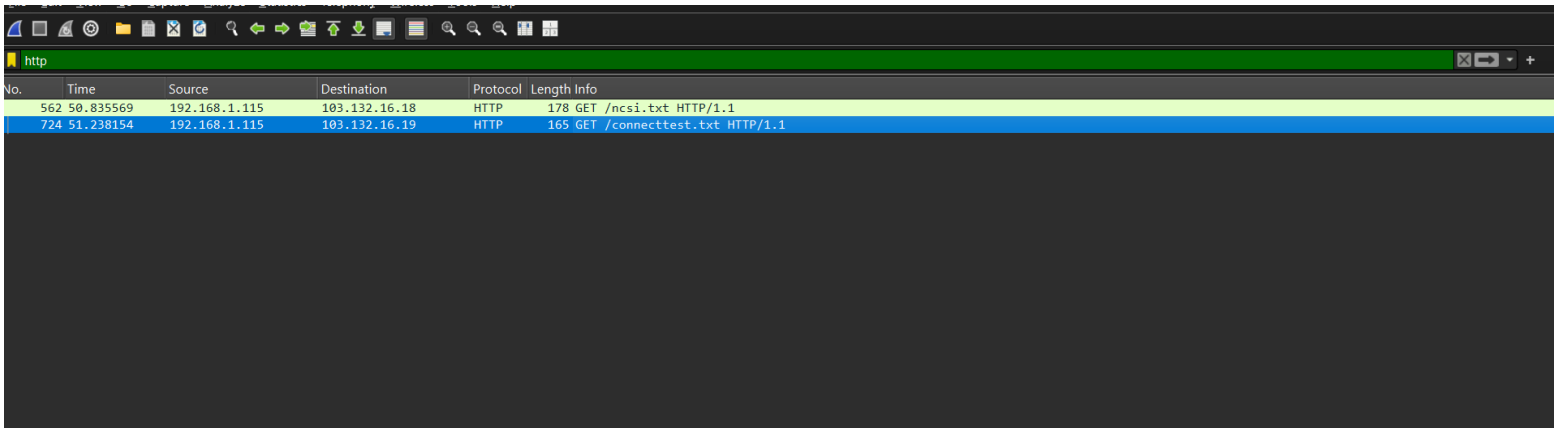
TCP and HTTP Traffic





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-9
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: 192.168.1.254, Dst: 192.168.1.115
User Datagram Protocol, Src Port: 53, Dst Port: 52636
Domain Name System (response)
0000 10 68 38 32 f9 33 18 45 93 7e 93 90 08 00 45 00
0010 00 e8 00 3d 40 00 40 11 b5 06 c0 a8 01 fe c0 a8
0020 01 73 00 35 cd 9c 00 d4 1a 30 a9 d0 81 80 00 01
0030 00 08 00 00 00 00 03 77 77 77 08 6d 73 66 74 6e
0040 63 73 69 03 63 6f 6d 00 00 01 00 01 c0 0c 00 05
0050 00 01 00 00 0d de 00 20 03 77 77 77 08 6d 73 66
0060 74 6e 63 73 69 03 63 6f 6d 09 65 64 67 65 73 75
0070 69 74 65 03 6e 65 74 00 c0 2e 00 05 00 01 00 00
0080 00 a1 00 12 05 61 31 39 36 31 02 67 32 06 61 6b
0090 61 6d 61 69 c0 49 c0 5a 00 01 00 01 00 00 00 0d
00a0 00 04 67 84 10 12 c0 5a 00 01 00 01 00 00 00 0d
00b0 00 04 67 84 10 19 c0 5a 00 01 00 01 00 00 00 0d
00c0 00 04 67 84 10 09 c0 5a 00 01 00 01 00 00 00 0d
00d0 00 04 67 84 10 13 c0 5a 00 01 00 01 00 00 00 0d
00e0 00 04 67 84 10 11 c0 5a 00 01 00 01 00 00 00 0d
00f0 00 04 67 84 10 10


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