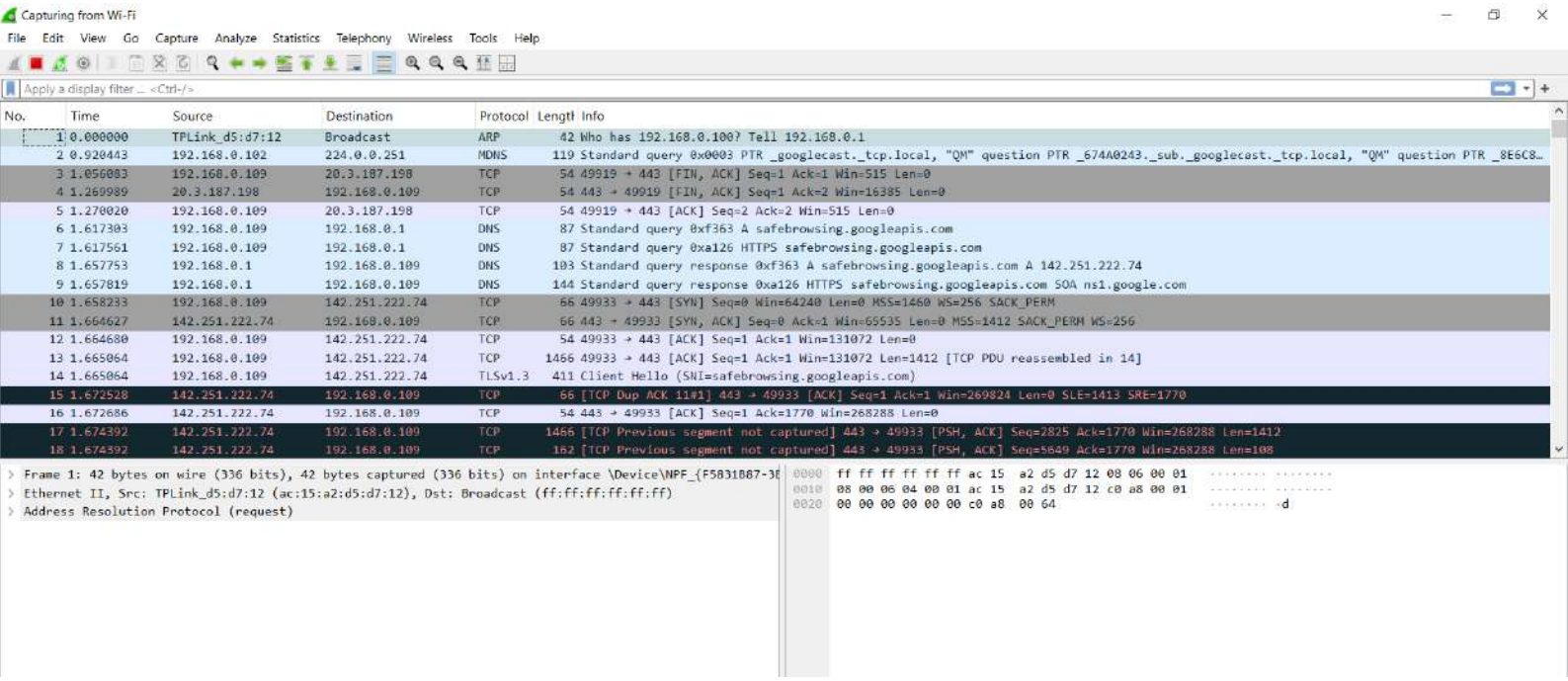
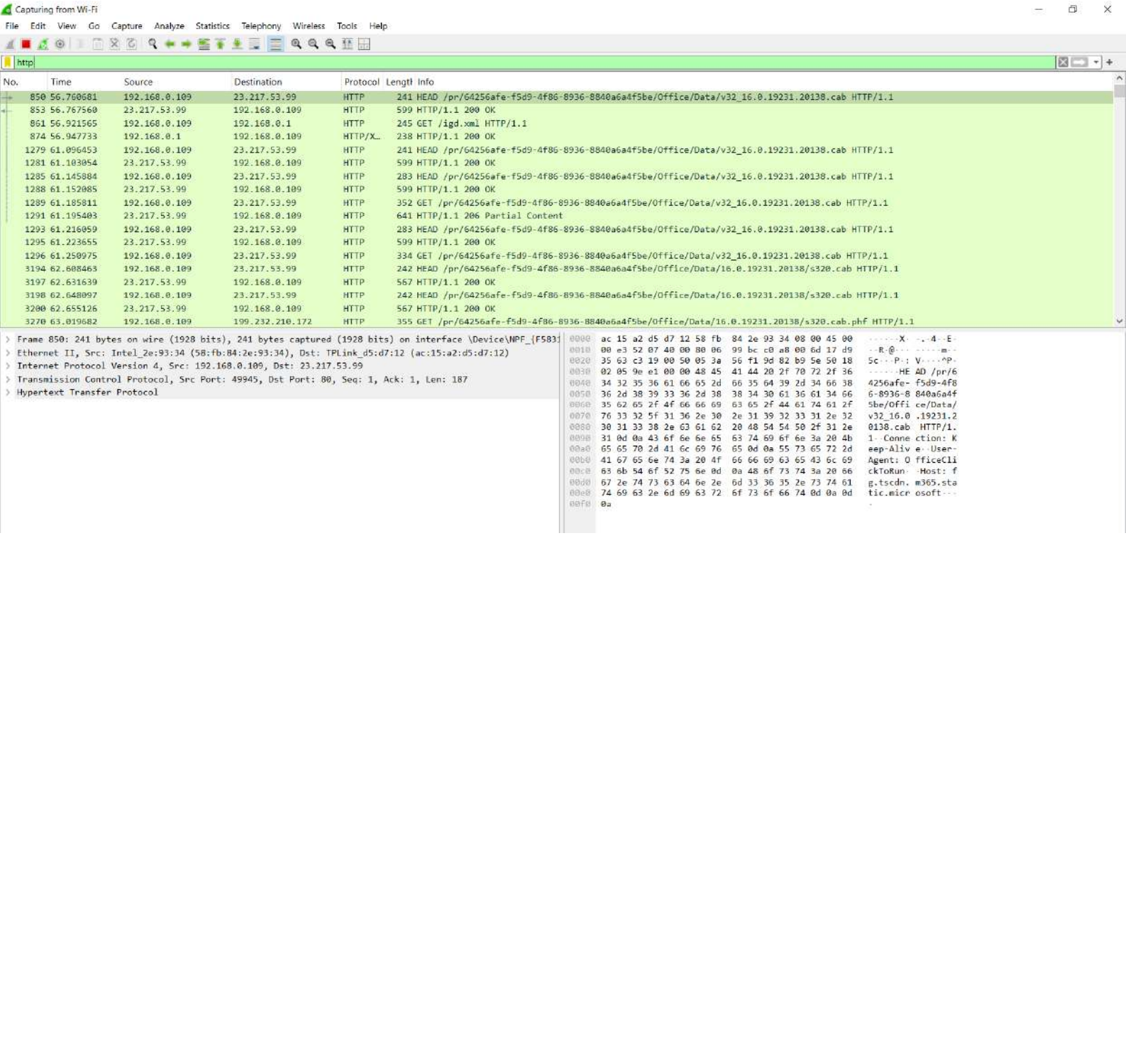
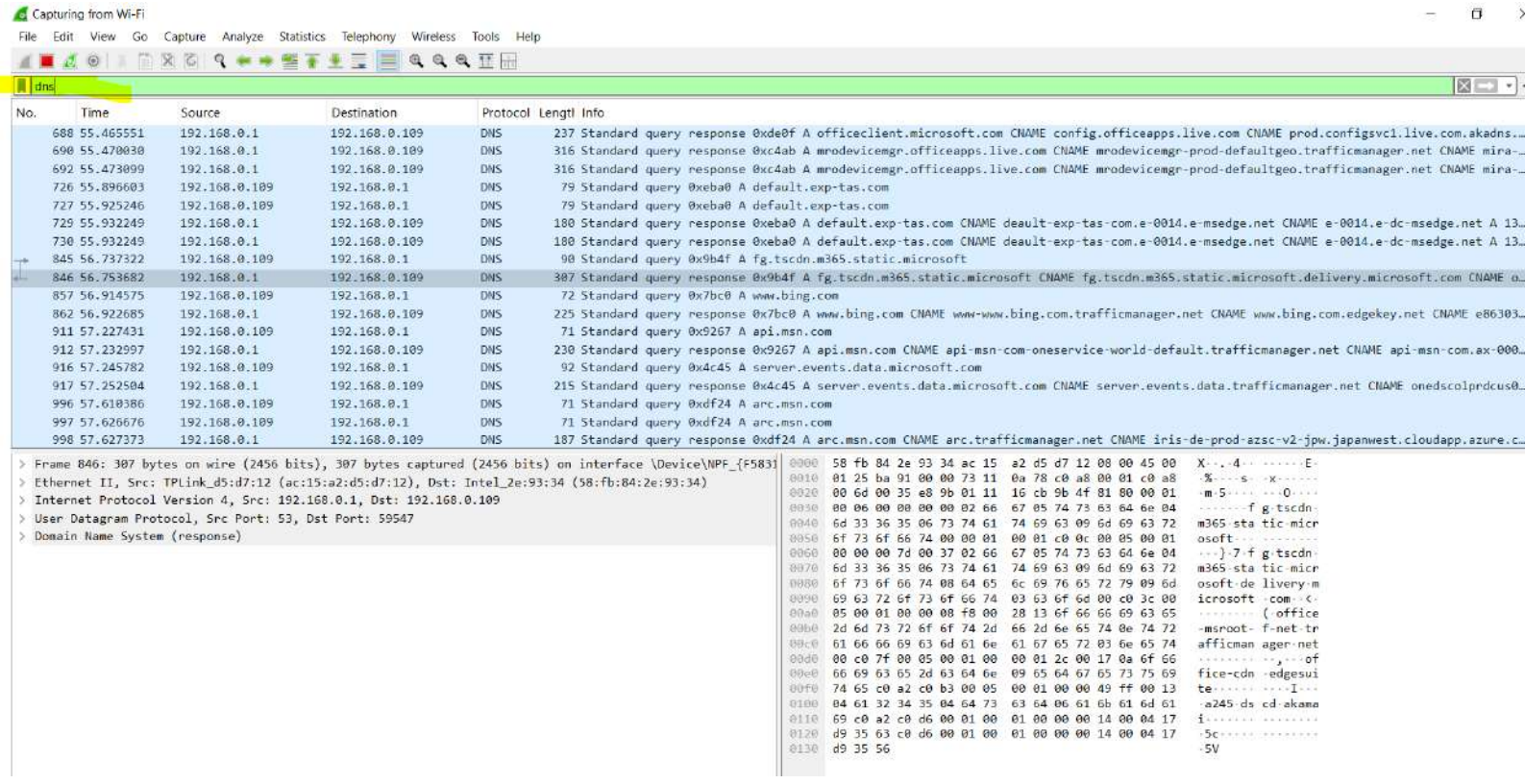
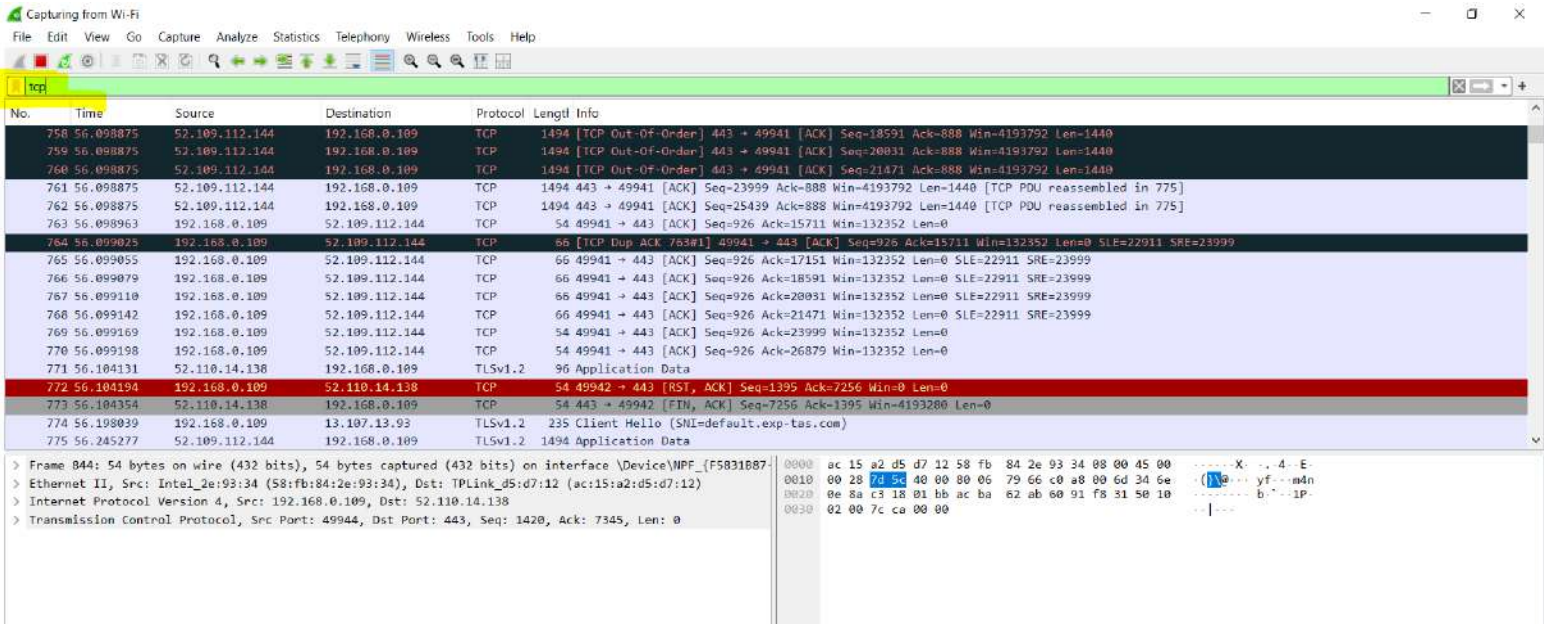

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 TPLink_d5:d7:12 Broadcast ARP 42 Who has 192.168.0.100? Tell 192.168.0.1
2 0.920443 192.168.0.102 224.0.0.251 MDNS 119 Standard query 0x0003 PTR _googlecast._tcp.local, "QM" question PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6C8…
3 1.056083 192.168.0.109 20.3.187.198 TCP 54 49919 → 443 [FIN, ACK] Seq=1 Ack=1 Win=515 Len=0
4 1.269989 20.3.187.198 192.168.0.109 TCP 54 443 → 49919 [FIN, ACK] Seq=1 Ack=2 Win=16385 Len=0
5 1.270020 192.168.0.109 20.3.187.198 TCP 54 49919 → 443 [ACK] Seq=2 Ack=2 Win=515 Len=0
6 1.617303 192.168.0.109 192.168.0.1 DNS 87 Standard query 0xf363 A safebrowsing.googleapis.com
7 1.617561 192.168.0.109 192.168.0.1 DNS 87 Standard query 0xa126 HTTPS safebrowsing.googleapis.com
8 1.657753 192.168.0.1 192.168.0.109 DNS 103 Standard query response 0xf363 A safebrowsing.googleapis.com A 142.251.222.74
9 1.657819 192.168.0.1 192.168.0.109 DNS 144 Standard query response 0xa126 HTTPS safebrowsing.googleapis.com SOA ns1.google.com
10 1.658233 192.168.0.109 142.251.222.74 TCP 66 49933 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
11 1.664627 142.251.222.74 192.168.0.109 TCP 66 443 → 49933 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
12 1.664680 192.168.0.109 142.251.222.74 TCP 54 49933 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
13 1.665064 192.168.0.109 142.251.222.74 TCP 1466 49933 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=1412 [TCP PDU reassembled in 14]
14 1.665064 192.168.0.109 142.251.222.74 TLSv1.3 411 Client Hello (SNI=safebrowsing.googleapis.com)
15 1.672528 142.251.222.74 192.168.0.109 TCP 66 [TCP Dup ACK 11#1] 443 → 49933 [ACK] Seq=1 Ack=1 Win=269824 Len=0 SLE=1413 SRE=1770
16 1.672686 142.251.222.74 192.168.0.109 TCP 54 443 → 49933 [ACK] Seq=1 Ack=1770 Win=268288 Len=0
17 1.674392 142.251.222.74 192.168.0.109 TCP 1466 [TCP Previous segment not captured] 443 → 49933 [PSH, ACK] Seq=2825 Ack=1770 Win=268288 Len=1412
18 1.674392 142.251.222.74 192.168.0.109 TCP 162 [TCP Previous segment not captured] 443 → 49933 [PSH, ACK] Seq=5649 Ack=1770 Win=268288 Len=108
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{F5831B87-3
Ethernet II, Src: TPLink_d5:d7:12 (ac:15:a2:d5:d7:12), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff ac 15 a2 d5 d7 12 08 06 00 01
0010 08 00 06 04 00 01 ac 15 a2 d5 d7 12 c0 a8 00 01
0020 00 00 00 00 00 00 c0 a8 00 64
.d


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
850 56.760681 192.168.0.109 23.217.53.99 HTTP 241 HEAD /pr/64256afe-f5d9-4f86-8936-8840a6a4f5be/Office/Data/v32_16.0.19231.20138.cab HTTP/1.1
853 56.767560 23.217.53.99 192.168.0.109 HTTP 599 HTTP/1.1 200 OK
861 56.921565 192.168.0.109 192.168.0.1 HTTP 245 GET /igd.xml HTTP/1.1
874 56.947733 192.168.0.1 192.168.0.109 HTTP/X... 238 HTTP/1.1 200 OK
1279 61.096453 192.168.0.109 23.217.53.99 HTTP 241 HEAD /pr/64256afe-f5d9-4f86-8936-8840a6a4f5be/Office/Data/v32_16.0.19231.20138.cab HTTP/1.1
1281 61.103054 23.217.53.99 192.168.0.109 HTTP 599 HTTP/1.1 200 OK
1285 61.145884 192.168.0.109 23.217.53.99 HTTP 283 HEAD /pr/64256afe-f5d9-4f86-8936-8840a6a4f5be/Office/Data/v32_16.0.19231.20138.cab HTTP/1.1
1288 61.152085 23.217.53.99 192.168.0.109 HTTP 599 HTTP/1.1 200 OK
1289 61.185811 192.168.0.109 23.217.53.99 HTTP 352 GET /pr/64256afe-f5d9-4f86-8936-8840a6a4f5be/Office/Data/v32_16.0.19231.20138.cab HTTP/1.1
1291 61.195403 23.217.53.99 192.168.0.109 HTTP 641 HTTP/1.1 206 Partial Content
1293 61.216059 192.168.0.109 23.217.53.99 HTTP 283 HEAD /pr/64256afe-f5d9-4f86-8936-8840a6a4f5be/Office/Data/v32_16.0.19231.20138.cab HTTP/1.1
1295 61.223655 23.217.53.99 192.168.0.109 HTTP 599 HTTP/1.1 200 OK
1296 61.250975 192.168.0.109 23.217.53.99 HTTP 334 GET /pr/64256afe-f5d9-4f86-8936-8840a6a4f5be/Office/Data/v32_16.0.19231.20138.cab HTTP/1.1
3194 62.608463 192.168.0.109 23.217.53.99 HTTP 242 HEAD /pr/64256afe-f5d9-4f86-8936-8840a6a4f5be/Office/Data/16.0.19231.20138/s320.cab HTTP/1.1
3197 62.631639 23.217.53.99 192.168.0.109 HTTP 567 HTTP/1.1 200 OK
3198 62.648097 192.168.0.109 23.217.53.99 HTTP 242 HEAD /pr/64256afe-f5d9-4f86-8936-8840a6a4f5be/Office/Data/16.0.19231.20138/s320.cab HTTP/1.1
3200 62.655126 23.217.53.99 192.168.0.109 HTTP 567 HTTP/1.1 200 OK
3270 63.019682 192.168.0.109 199.232.210.172 HTTP 355 GET /pr/64256afe-f5d9-4f86-8936-8840a6a4f5be/Office/Data/16.0.19231.20138/s320.cab.phf HTTP/1.1
Frame 850: 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on interface \Device\NPF_{F583
Ethernet II, Src: Intel_2e:93:34 (58:fb:84:2e:93:34), Dst: TPLink_d5:d7:12 (ac:15:a2:d5:d7:12)
Internet Protocol Version 4, Src: 192.168.0.109, Dst: 23.217.53.99
Transmission Control Protocol, Src Port: 49945, Dst Port: 80, Seq: 1, Ack: 1, Len: 187
Hypertext Transfer Protocol
0000 ac 15 a2 d5 d7 12 58 fb 84 2e 93 34 08 00 45 00 ·····X· ·.·4··E·
0010 00 e3 52 07 40 00 80 06 99 bc c0 a8 00 6d 17 d9 ··R·@··· ·····m··
0020 35 63 c3 19 00 50 05 3a 56 f1 9d 82 b9 5e 50 18 5c···P·: V····^P·
0030 02 05 9e e1 00 00 48 45 41 44 20 2f 70 72 2f 36 ·····HE AD /pr/6
0040 34 32 35 36 61 66 65 2d 66 35 64 39 2d 34 66 38 4256afe- f5d9-4f8
0050 36 2d 38 39 33 36 2d 38 38 34 30 61 36 61 34 66 6-8936-8 840a6a4f
0060 35 62 65 2f 4f 66 66 69 63 65 2f 44 61 74 61 2f 5be/Offi ce/Data/
0070 76 33 32 5f 31 36 2e 30 2e 31 39 32 33 31 2e 32 v32_16.0 .19231.2
0080 30 31 33 38 2e 63 61 62 20 48 54 54 50 2f 31 2e 0138.cab HTTP/1.
0090 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 1··Conne ction: K
00a0 65 65 70 2d 41 6c 69 76 65 0d 0a 55 73 65 72 2d eep-Aliv e··User-
00b0 41 67 65 6e 74 3a 20 4f 66 66 69 63 65 43 6c 69 Agent: O fficeCli
00c0 63 6b 54 6f 52 75 6e 0d 0a 48 6f 73 74 3a 20 66 ckToRun· ·Host: f
00d0 67 2e 74 73 63 64 6e 2e 6d 33 36 35 2e 73 74 61 g.tscdn. m365.sta
00e0 74 69 63 2e 6d 69 63 72 6f 73 6f 66 74 0d 0a 0d tic.micr osoft···
00f0 0a ·


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Lengtl Info
688 55.465551 192.168.0.1 192.168.0.109 DNS 237 Standard query response 0xde0f A officeclient.microsoft.com CNAME config.officeapps.live.com CNAME prod.configsvc1.live.com.akadns...
690 55.470030 192.168.0.1 192.168.0.109 DNS 316 Standard query response 0xc4ab A mrodevicemgr.officeapps.live.com CNAME mrodevicemgr-prod-defaultgeo.trafficmanager.net CNAME mira-...
692 55.473099 192.168.0.1 192.168.0.109 DNS 316 Standard query response 0xc4ab A mrodevicemgr.officeapps.live.com CNAME mrodevicemgr-prod-defaultgeo.trafficmanager.net CNAME mira-...
726 55.896603 192.168.0.109 192.168.0.1 DNS 79 Standard query 0xeba0 A default.exp-tas.com
727 55.925246 192.168.0.109 192.168.0.1 DNS 79 Standard query 0xeba0 A default.exp-tas.com
729 55.932249 192.168.0.1 192.168.0.109 DNS 180 Standard query response 0xeba0 A default.exp-tas.com CNAME deault-exp-tas-com.e-0014.e-msedge.net CNAME e-0014.e-dc-msedge.net A 13...
730 55.932249 192.168.0.1 192.168.0.109 DNS 180 Standard query response 0xeba0 A default.exp-tas.com CNAME deault-exp-tas-com.e-0014.e-msedge.net CNAME e-0014.e-dc-msedge.net A 13...
845 56.737322 192.168.0.109 192.168.0.1 DNS 90 Standard query 0x9b4f A fg.tscdn.m365.static.microsoft
846 56.753682 192.168.0.1 192.168.0.109 DNS 307 Standard query response 0x9b4f A fg.tscdn.m365.static.microsoft CNAME fg.tscdn.m365.static.microsoft.delivery.microsoft.com CNAME o...
857 56.914575 192.168.0.109 192.168.0.1 DNS 72 Standard query 0x7bc0 A www.bing.com
862 56.922685 192.168.0.1 192.168.0.109 DNS 225 Standard query response 0x7bc0 A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com.edgekey.net CNAME e86303...
911 57.227431 192.168.0.109 192.168.0.1 DNS 71 Standard query 0x9267 A api.msn.com
912 57.232997 192.168.0.1 192.168.0.109 DNS 230 Standard query response 0x9267 A api.msn.com CNAME api-msn-com-oneservice-world-default.trafficmanager.net CNAME api-msn-com.ax-000...
916 57.245782 192.168.0.109 192.168.0.1 DNS 92 Standard query 0x4c45 A server.events.data.microsoft.com
917 57.252504 192.168.0.1 192.168.0.109 DNS 215 Standard query response 0x4c45 A server.events.data.microsoft.com CNAME server.events.data.trafficmanager.net CNAME onedscolprdcus0...
996 57.610386 192.168.0.109 192.168.0.1 DNS 71 Standard query 0xdf24 A arc.msn.com
997 57.626676 192.168.0.109 192.168.0.1 DNS 71 Standard query 0xdf24 A arc.msn.com
998 57.627373 192.168.0.1 192.168.0.109 DNS 187 Standard query response 0xdf24 A arc.msn.com CNAME arc.trafficmanager.net CNAME iris-de-prod-azsc-v2-jpw.japanwest.cloudapp.azure.c...
Frame 846: 307 bytes on wire (2456 bits), 307 bytes captured (2456 bits) on interface \Device\NPF_{F5831
Ethernet II, Src: TPLink_d5:d7:12 (ac:15:a2:d5:d7:12), Dst: Intel_2e:93:34 (58:fb:84:2e:93:34)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.109
User Datagram Protocol, Src Port: 53, Dst Port: 59547
Domain Name System (response)
0000 58 fb 84 2e 93 34 ac 15 a2 d5 d7 12 08 00 45 00
0010 01 25 ba 91 00 00 73 11 0a 78 c0 a8 00 01 c0 a8
0020 00 6d 00 35 e8 9b 01 11 16 cb 9b 4f 81 80 00 01
0030 00 06 00 00 00 00 02 66 67 05 74 73 63 64 6e 04
0040 6d 33 36 35 06 73 74 61 74 69 63 09 6d 69 63 72
0050 6f 73 6f 66 74 00 00 01 00 01 c0 0c 00 05 00 01
0060 00 00 00 7d 00 37 02 66 67 05 74 73 63 64 6e 04
0070 6d 33 36 35 06 73 74 61 74 69 63 09 6d 69 63 72
0080 6f 73 6f 66 74 08 64 65 6c 69 76 65 72 79 09 6d
0090 69 63 72 6f 73 6f 66 74 03 63 6f 6d 00 c0 3c 00
00a0 05 00 01 00 00 08 f8 00 28 13 6f 66 66 69 63 65
00b0 2d 6d 73 72 6f 6f 74 2d 66 2d 6e 65 74 0e 74 72
00c0 61 66 66 69 63 6d 61 6e 61 67 65 72 03 6e 65 74
00d0 00 c0 7f 00 05 00 01 00 00 01 2c 00 17 0a 6f 66
00e0 66 69 63 65 2d 63 64 6e 09 65 64 67 65 73 75 69
00f0 74 65 c0 a2 c0 b3 00 05 00 01 00 00 49 ff 00 13
0100 04 61 32 34 35 04 64 73 63 64 06 61 6b 61 6d 61
0110 69 c0 a2 c0 d6 00 01 00 01 00 00 00 14 00 04 17
0120 d9 35 63 c0 d6 00 01 00 01 00 00 00 14 00 04 17
0130 d9 35 56


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
758 56.098875 52.109.112.144 192.168.0.109 TCP 1494 [TCP Out-Of-Order] 443 → 49941 [ACK] Seq=18591 Ack=888 Win=4193792 Len=1440
759 56.098875 52.109.112.144 192.168.0.109 TCP 1494 [TCP Out-Of-Order] 443 → 49941 [ACK] Seq=20031 Ack=888 Win=4193792 Len=1440
760 56.098875 52.109.112.144 192.168.0.109 TCP 1494 [TCP Out-Of-Order] 443 → 49941 [ACK] Seq=21471 Ack=888 Win=4193792 Len=1440
761 56.098875 52.109.112.144 192.168.0.109 TCP 1494 443 → 49941 [ACK] Seq=23999 Ack=888 Win=4193792 Len=1440 [TCP PDU reassembled in 775]
762 56.098875 52.109.112.144 192.168.0.109 TCP 1494 443 → 49941 [ACK] Seq=25439 Ack=888 Win=4193792 Len=1440 [TCP PDU reassembled in 775]
763 56.098963 192.168.0.109 52.109.112.144 TCP 54 49941 → 443 [ACK] Seq=926 Ack=15711 Win=132352 Len=0
764 56.099025 192.168.0.109 52.109.112.144 TCP 66 [TCP Dup ACK 763#1] 49941 → 443 [ACK] Seq=926 Ack=15711 Win=132352 Len=0 SLE=22911 SRE=23999
765 56.099055 192.168.0.109 52.109.112.144 TCP 66 49941 → 443 [ACK] Seq=926 Ack=17151 Win=132352 Len=0 SLE=22911 SRE=23999
766 56.099079 192.168.0.109 52.109.112.144 TCP 66 49941 → 443 [ACK] Seq=926 Ack=18591 Win=132352 Len=0 SLE=22911 SRE=23999
767 56.099110 192.168.0.109 52.109.112.144 TCP 66 49941 → 443 [ACK] Seq=926 Ack=20031 Win=132352 Len=0 SLE=22911 SRE=23999
768 56.099142 192.168.0.109 52.109.112.144 TCP 66 49941 → 443 [ACK] Seq=926 Ack=21471 Win=132352 Len=0 SLE=22911 SRE=23999
769 56.099169 192.168.0.109 52.109.112.144 TCP 54 49941 → 443 [ACK] Seq=926 Ack=23999 Win=132352 Len=0
770 56.099198 192.168.0.109 52.109.112.144 TCP 54 49941 → 443 [ACK] Seq=926 Ack=26879 Win=132352 Len=0
771 56.104131 52.110.14.138 192.168.0.109 TLSv1.2 96 Application Data
772 56.104194 192.168.0.109 52.110.14.138 TCP 54 49942 → 443 [RST, ACK] Seq=1395 Ack=7256 Win=0 Len=0
773 56.104354 52.110.14.138 192.168.0.109 TCP 54 443 → 49942 [FIN, ACK] Seq=7256 Ack=1395 Win=4193280 Len=0
774 56.198039 192.168.0.109 13.107.13.93 TLSv1.2 235 Client Hello (SNI=default.exp-tas.com)
775 56.245277 52.109.112.144 192.168.0.109 TLSv1.2 1494 Application Data
Frame 844: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{F5831B87
Ethernet II, Src: Intel_2e:93:34 (58:fb:84:2e:93:34), Dst: TPLink_d5:d7:12 (ac:15:a2:d5:d7:12)
Internet Protocol Version 4, Src: 192.168.0.109, Dst: 52.110.14.138
Transmission Control Protocol, Src Port: 49944, Dst Port: 443, Seq: 1420, Ack: 7345, Len: 0
0000 ac 15 a2 d5 d7 12 58 fb 84 2e 93 34 08 00 45 00
0010 00 28 7d 5c 40 00 80 06 79 66 c0 a8 00 6d 34 6e
0020 0e 8a c3 18 01 bb ac ba 62 ab 60 91 f8 31 50 10
0030 02 00 7c ca 00 00