ISAA LAB ASSIGNMENT - 4

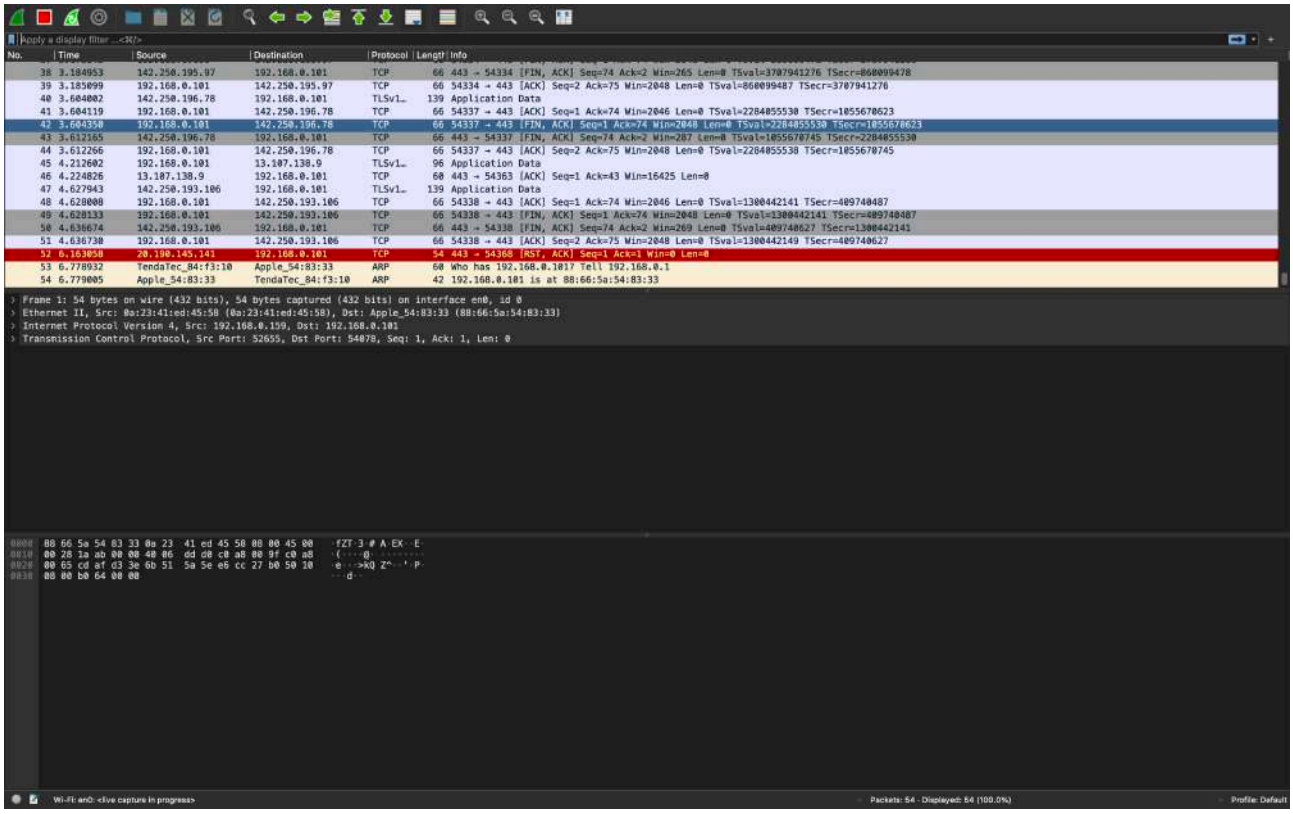
NAME	APOORVA REDDY BAGEPALLI
REGISTRATION NUMBER	19BCE2196

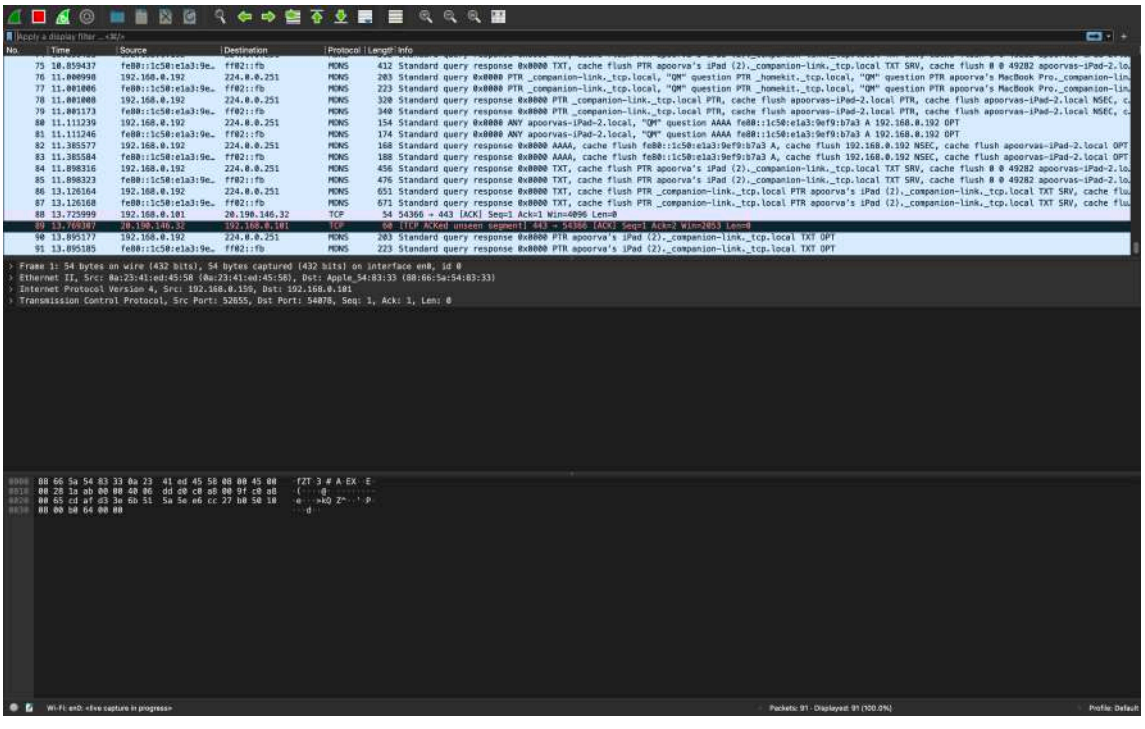
APOORVA REDDY 19BCE2196

Network Packet using Wireshark

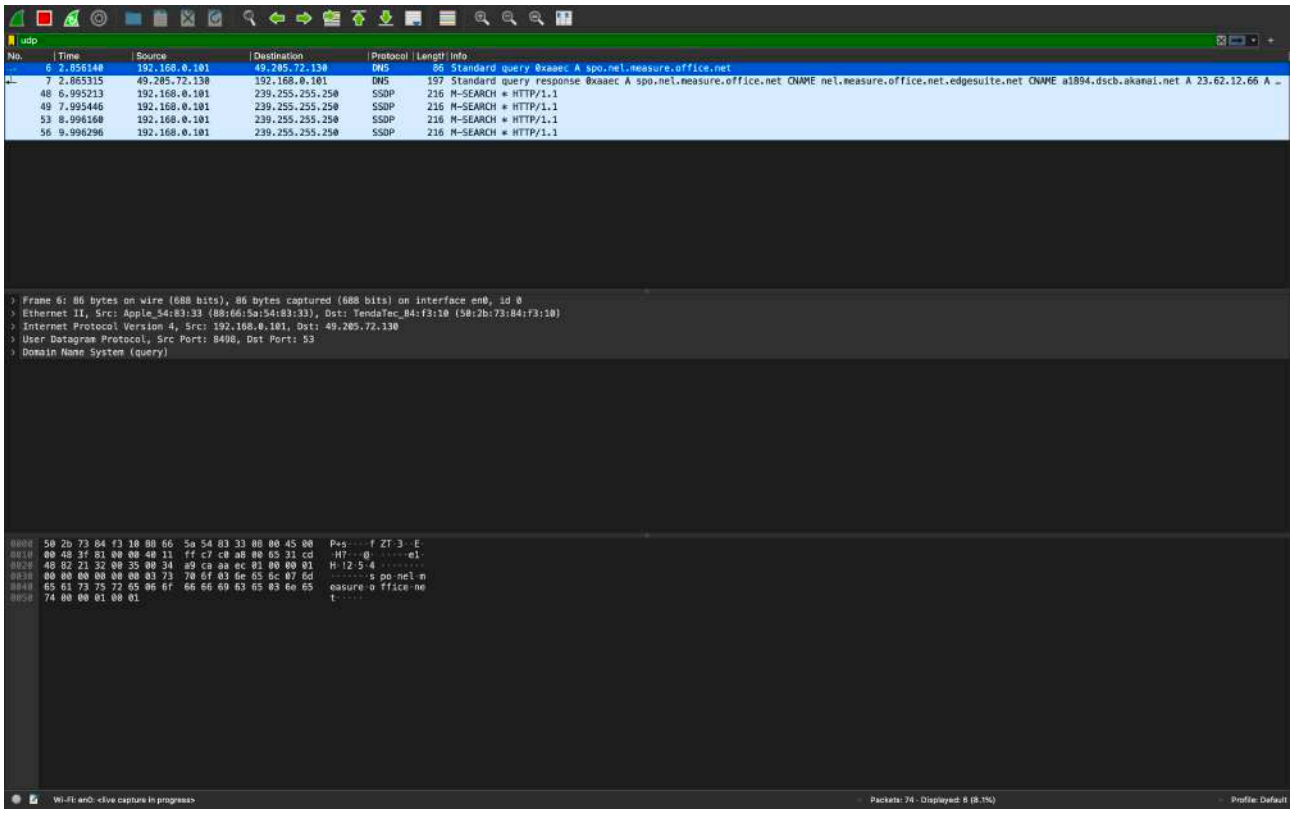
A)Interfaces
B)Apply a filter which shows the packet which belong to any one of the categories(ICMP, ARP,TCP,UDP)
C) Receive the packets which belong to HTTP
D) You have to apply a filter which is able to capture the packets from a particular website
E) Receive the packet which belong to ICMP

SCREENSHOT
A)

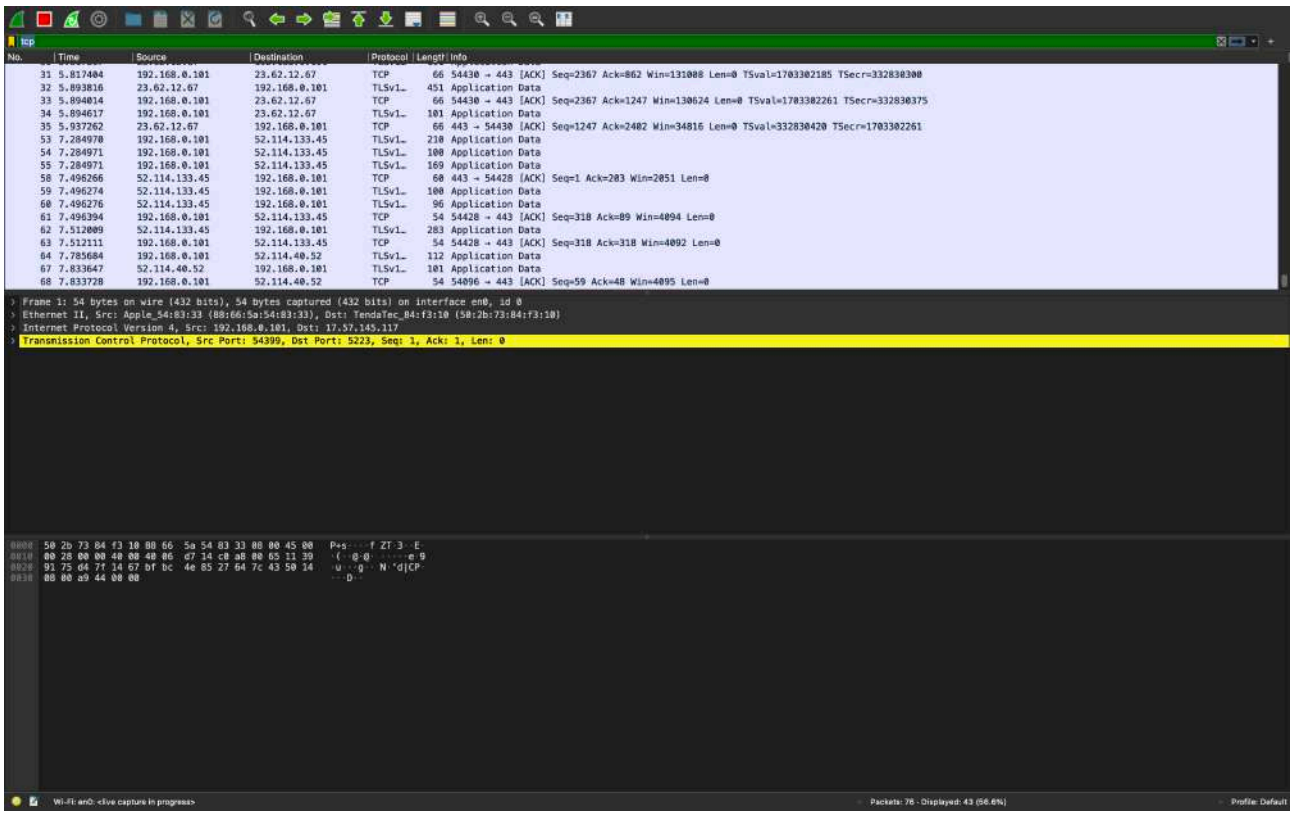




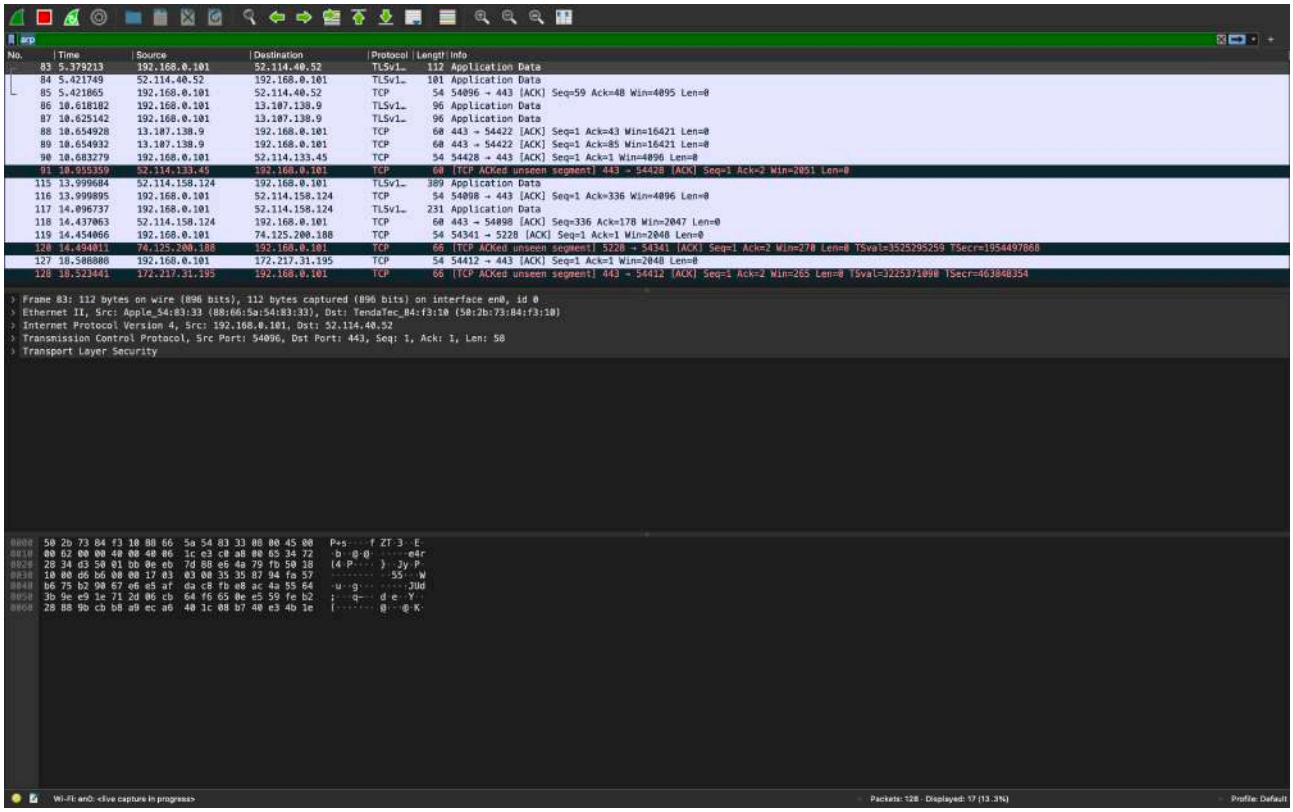
B)
UDP


udp
No. Time Source Destination Protocol Length Info
6 2.856140 192.168.0.101 49.205.72.130 DNS 86 Standard query 0xaaec A spo.nel.measure.office.net
7 2.865315 49.205.72.130 192.168.0.101 DNS 197 Standard query response 0xaaec A spo.nel.measure.office.net CNAME nel.measure.office.net.edgesuite.net CNAME a1894.dscb.akamai.net A 23.62.12.66 A
48 6.995213 192.168.0.101 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
49 7.995446 192.168.0.101 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
53 8.996160 192.168.0.101 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
56 9.996296 192.168.0.101 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
Frame 6: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface en0, id 0
Ethernet II, Src: Apple_54:83:33 (88:66:5a:54:83:33), Dst: TendaTec_84:f3:10 (50:2b:73:84:f3:10)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 49.205.72.130
User Datagram Protocol, Src Port: 8498, Dst Port: 53
Domain Name System (query)
0000 50 2b 73 84 f3 10 88 66 5a 54 83 33 08 00 45 00
0010 00 48 3f 81 00 00 40 11 ff c7 c0 a8 00 65 31 cd
0020 48 82 21 32 00 35 00 34 a9 ca aa ec 01 00 00 01
0030 00 00 00 00 00 00 03 73 70 6f 03 6e 65 6c 07 6d
0040 65 61 73 75 72 65 06 6f 66 66 69 63 65 03 6e 65
0050 74 00 00 01 00 01
Wi-Fi: en0: <live capture in progress>
Packets: 74 · Displayed: 8 (8.1%)
Profile: Default

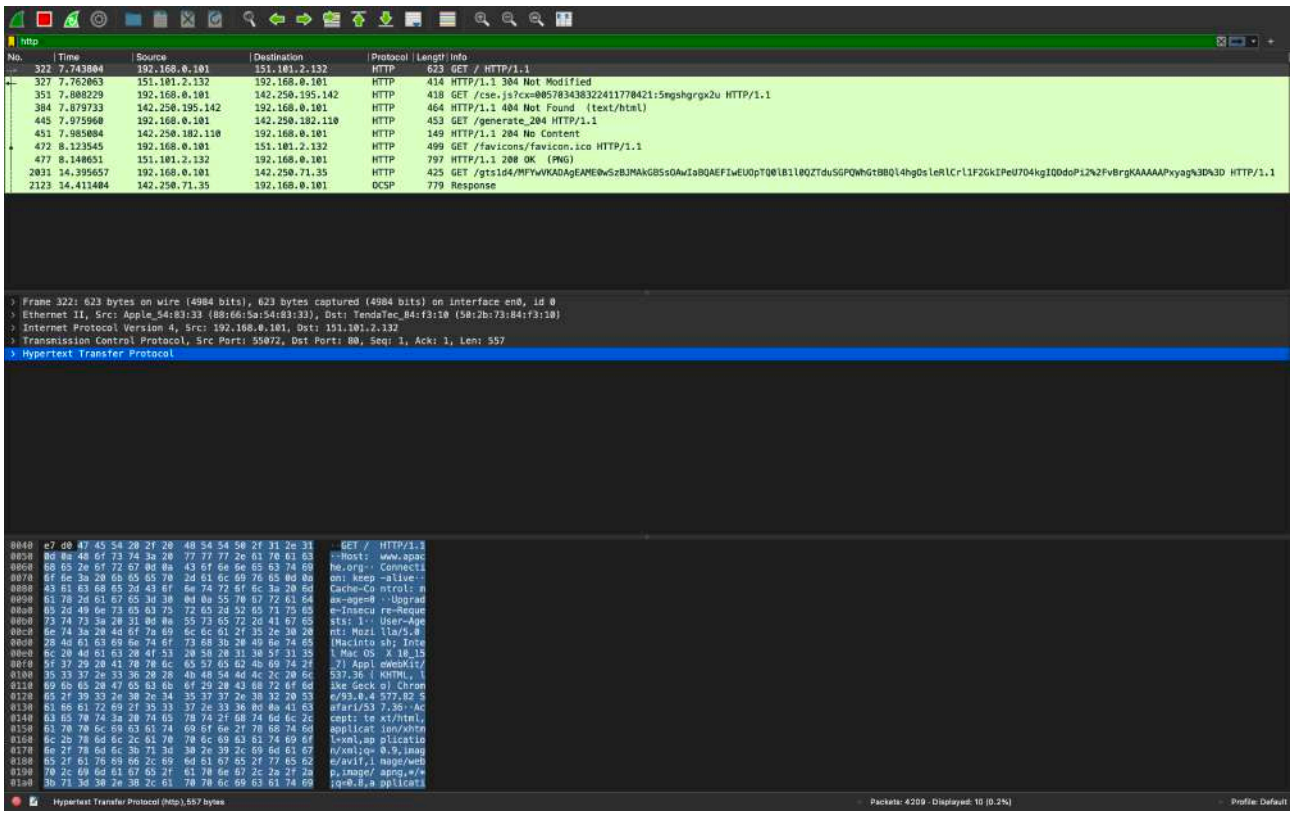
TCP

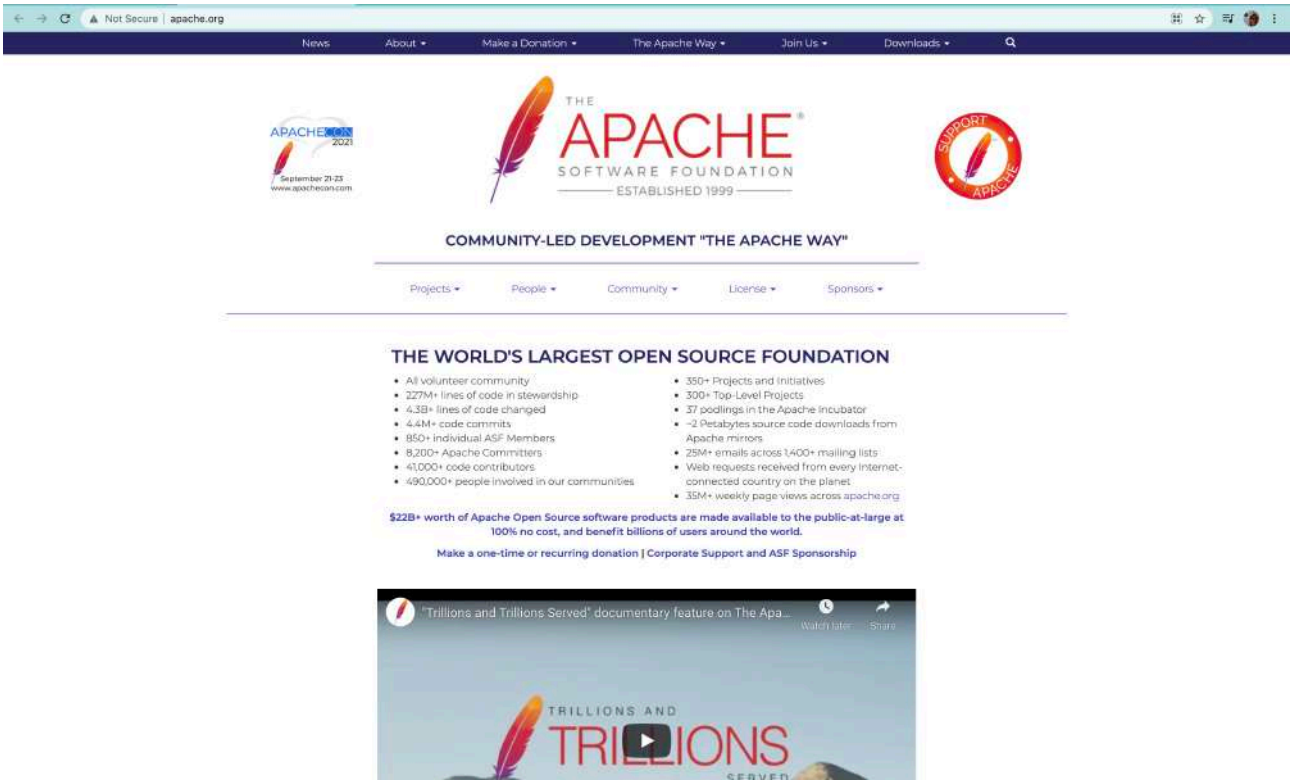

tcp
No. Time Source Destination Protocol Length Info
31 5.817404 192.168.0.101 23.62.12.67 TCP 66 54430 → 443 [ACK] Seq=2367 Ack=862 Win=131008 Len=0 TSval=1703302185 TSecr=332830300
32 5.893816 23.62.12.67 192.168.0.101 TLSv1… 451 Application Data
33 5.894014 192.168.0.101 23.62.12.67 TCP 66 54430 → 443 [ACK] Seq=2367 Ack=1247 Win=130624 Len=0 TSval=1703302261 TSecr=332830375
34 5.894617 192.168.0.101 23.62.12.67 TLSv1… 101 Application Data
35 5.937262 23.62.12.67 192.168.0.101 TCP 66 443 → 54430 [ACK] Seq=1247 Ack=2402 Win=34816 Len=0 TSval=332830420 TSecr=1703302261
53 7.284970 192.168.0.101 52.114.133.45 TLSv1… 210 Application Data
54 7.284971 192.168.0.101 52.114.133.45 TLSv1… 100 Application Data
55 7.284971 192.168.0.101 52.114.133.45 TLSv1… 169 Application Data
58 7.496266 52.114.133.45 192.168.0.101 TCP 60 443 → 54428 [ACK] Seq=1 Ack=203 Win=2051 Len=0
59 7.496274 52.114.133.45 192.168.0.101 TLSv1… 100 Application Data
60 7.496276 52.114.133.45 192.168.0.101 TLSv1… 96 Application Data
61 7.496394 192.168.0.101 52.114.133.45 TCP 54 54428 → 443 [ACK] Seq=318 Ack=89 Win=4094 Len=0
62 7.512009 52.114.133.45 192.168.0.101 TLSv1… 283 Application Data
63 7.512111 192.168.0.101 52.114.133.45 TCP 54 54428 → 443 [ACK] Seq=318 Ack=318 Win=4092 Len=0
64 7.785684 192.168.0.101 52.114.40.52 TLSv1… 112 Application Data
67 7.833647 52.114.40.52 192.168.0.101 TLSv1… 101 Application Data
68 7.833728 192.168.0.101 52.114.40.52 TCP 54 54096 → 443 [ACK] Seq=59 Ack=48 Win=4095 Len=0
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en0, id 0
Ethernet II, Src: Apple_54:83:33 (88:66:5a:54:83:33), Dst: TendaTec_84:f3:10 (50:2b:73:84:f3:10)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 17.57.145.117
Transmission Control Protocol, Src Port: 54399, Dst Port: 5223, Seq: 1, Ack: 1, Len: 0
0000 50 2b 73 84 f3 10 88 66 5a 54 83 33 08 00 45 00
0010 00 28 00 00 40 00 40 06 d7 14 c0 a8 00 65 11 39
0020 91 75 d4 7f 14 67 bf bc 4e 85 27 64 7c 43 50 14
0030 08 00 a9 44 00 00
Wi-Fi: en0: <live capture in progress>
Packets: 76 · Displayed: 43 (56.6%)
Profile: Default

ARP

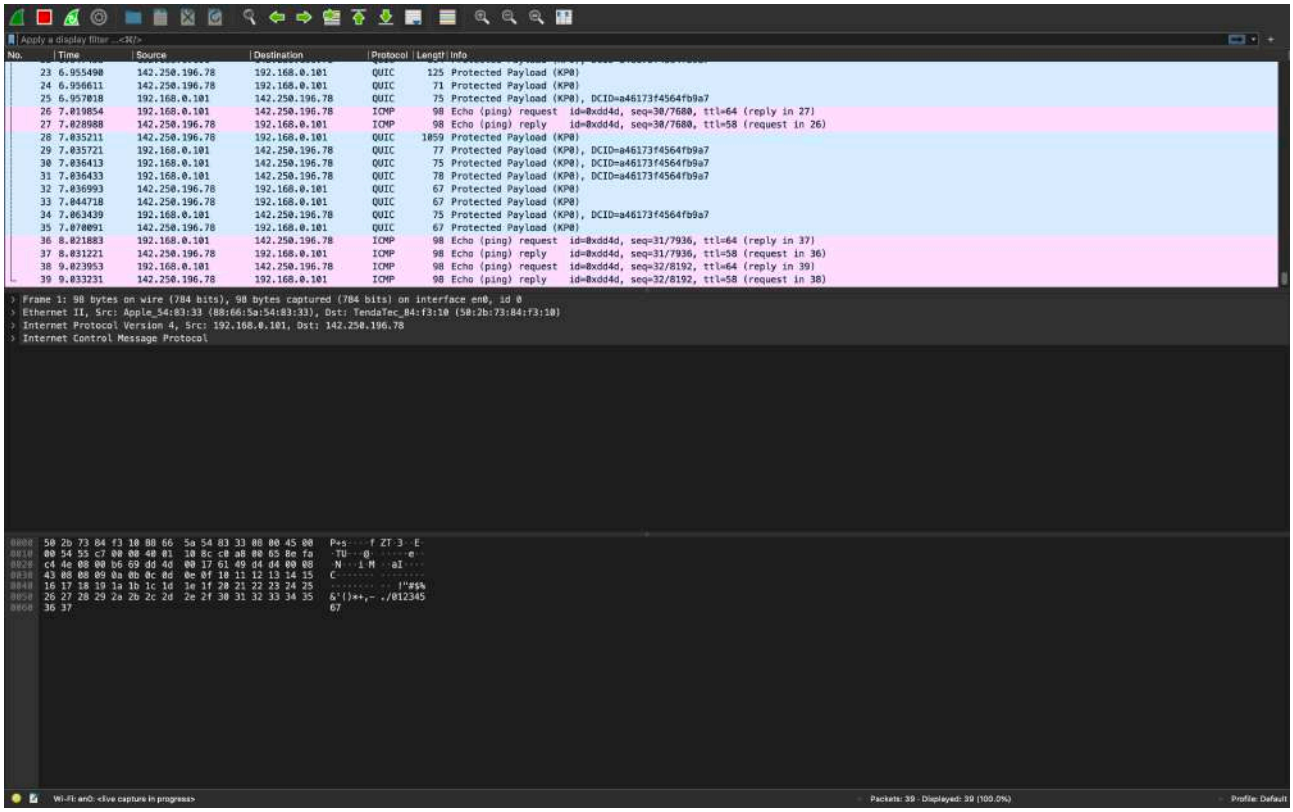

arp
No. Time Source Destination Protocol Length Info
83 5.379213 192.168.0.101 52.114.40.52 TLSv1… 112 Application Data
84 5.421749 52.114.40.52 192.168.0.101 TLSv1… 101 Application Data
85 5.421865 192.168.0.101 52.114.40.52 TCP 54 54096 → 443 [ACK] Seq=59 Ack=48 Win=4095 Len=0
86 10.618182 192.168.0.101 13.107.138.9 TLSv1… 96 Application Data
87 10.625142 192.168.0.101 13.107.138.9 TLSv1… 96 Application Data
88 10.654928 13.107.138.9 192.168.0.101 TCP 60 443 → 54422 [ACK] Seq=1 Ack=43 Win=16421 Len=0
89 10.654932 13.107.138.9 192.168.0.101 TCP 60 443 → 54422 [ACK] Seq=1 Ack=85 Win=16421 Len=0
90 10.683279 192.168.0.101 52.114.133.45 TCP 54 54428 → 443 [ACK] Seq=1 Ack=1 Win=4096 Len=0
91 10.955359 52.114.133.45 192.168.0.101 TCP 60 [TCP ACKed unseen segment] 443 → 54428 [ACK] Seq=1 Ack=2 Win=2051 Len=0
115 13.999684 52.114.158.124 192.168.0.101 TLSv1… 389 Application Data
116 13.999895 192.168.0.101 52.114.158.124 TCP 54 54098 → 443 [ACK] Seq=1 Ack=336 Win=4096 Len=0
117 14.096737 192.168.0.101 52.114.158.124 TLSv1… 231 Application Data
118 14.437063 52.114.158.124 192.168.0.101 TCP 60 443 → 54098 [ACK] Seq=336 Ack=178 Win=2047 Len=0
119 14.454066 192.168.0.101 74.125.200.188 TCP 54 54341 → 5228 [ACK] Seq=1 Ack=1 Win=2048 Len=0
120 14.494011 74.125.200.188 192.168.0.101 TCP 66 [TCP ACKed unseen segment] 5228 → 54341 [ACK] Seq=1 Ack=2 Win=270 Len=0 TSval=3525295259 TSecr=1954497868
127 18.508088 192.168.0.101 172.217.31.195 TCP 54 54412 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
128 18.523441 172.217.31.195 192.168.0.101 TCP 66 [TCP ACKed unseen segment] 443 → 54412 [ACK] Seq=1 Ack=2 Win=265 Len=0 TSval=3225371090 TSecr=463840354
Frame 83: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface en0, id 0
Ethernet II, Src: Apple_54:83:33 (88:66:5a:54:83:33), Dst: TendaTec_84:f3:10 (50:2b:73:84:f3:10)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 52.114.40.52
Transmission Control Protocol, Src Port: 54096, Dst Port: 443, Seq: 1, Ack: 1, Len: 58
Transport Layer Security
Wi-Fi: en0: <live capture in progress>
Packets: 128 · Displayed: 17 (13.3%)
Profile: Default

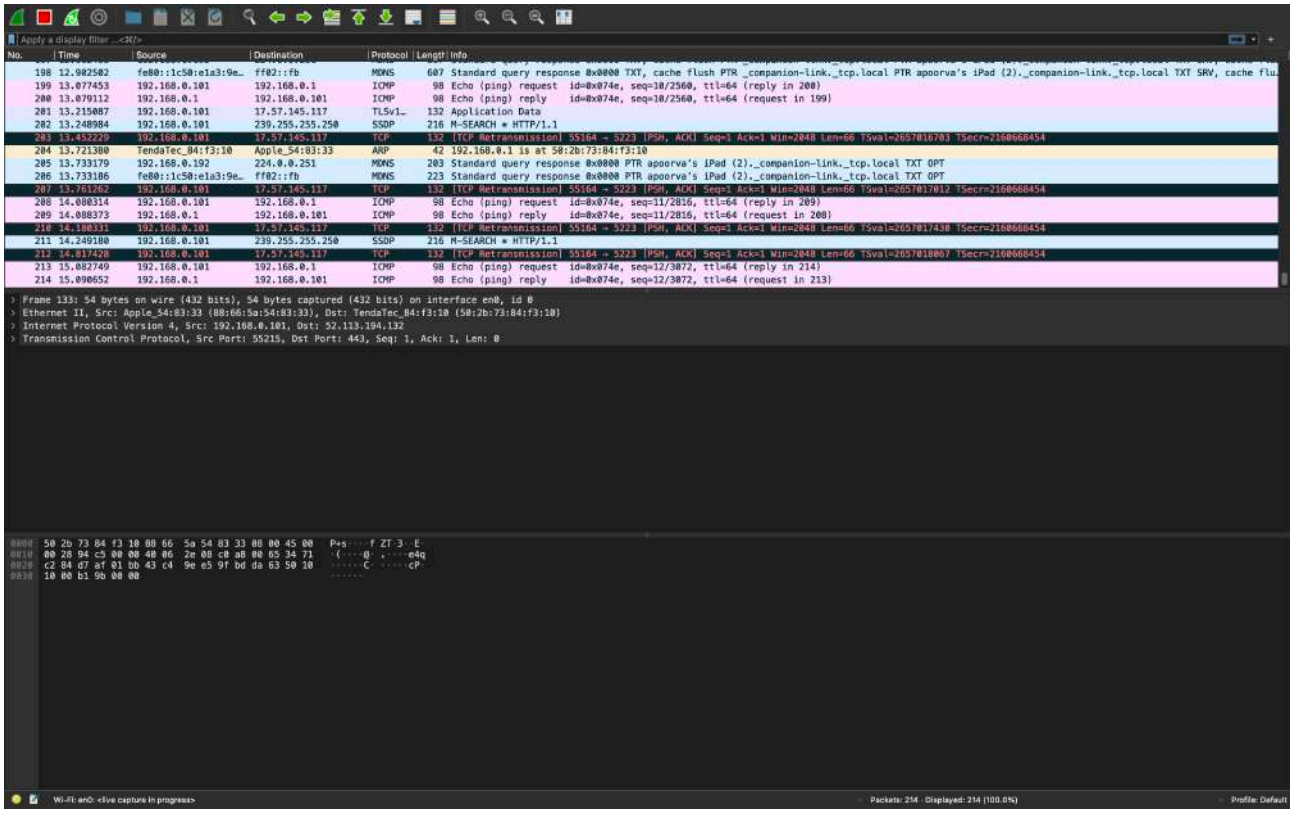
C)


http
No. Time Source Destination Protocol Length Info
322 7.743804 192.168.0.101 151.101.2.132 HTTP 623 GET / HTTP/1.1
327 7.762063 151.101.2.132 192.168.0.101 HTTP 414 HTTP/1.1 304 Not Modified
351 7.808229 192.168.0.101 142.250.195.142 HTTP 418 GET /cse.js?cx=005783438322411770421:5mgshgrgx2u HTTP/1.1
384 7.879733 142.250.195.142 192.168.0.101 HTTP 464 HTTP/1.1 404 Not Found (text/html)
445 7.975960 192.168.0.101 142.250.182.110 HTTP 453 GET /generate_204 HTTP/1.1
451 7.985084 142.250.182.110 192.168.0.101 HTTP 149 HTTP/1.1 204 No Content
472 8.123545 192.168.0.101 151.101.2.132 HTTP 499 GET /favicons/favicon.ico HTTP/1.1
477 8.140651 151.101.2.132 192.168.0.101 HTTP 797 HTTP/1.1 200 OK (PNG)
2031 14.395657 192.168.0.101 142.250.71.35 HTTP 425 GET /gts1d4/MFYwVKADAgEAME0wSzBJMAkGBSsOAwIaBQAEFIwEUOpTQ0lBll0QZTduSGPQWhGtBBQl4hgOsleRlCrl1F2GkIPeU7O4kgIQDdoPi2%2FvBrgKAAAAAPxyag%3D%3D HTTP/1.1
2123 14.411404 142.250.71.35 192.168.0.101 OCSP 779 Response
Frame 322: 623 bytes on wire (4984 bits), 623 bytes captured (4984 bits) on interface en0, id 0
Ethernet II, Src: Apple_54:83:33 (88:66:5a:54:83:33), Dst: TendaTec_84:f3:10 (50:2b:73:84:f3:10)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 151.101.2.132
Transmission Control Protocol, Src Port: 55072, Dst Port: 80, Seq: 1, Ack: 1, Len: 557
Hypertext Transfer Protocol
Hypertext Transfer Protocol (http),557 bytes
Packets: 4209 · Displayed: 10 (0.2%)
Profile: Default

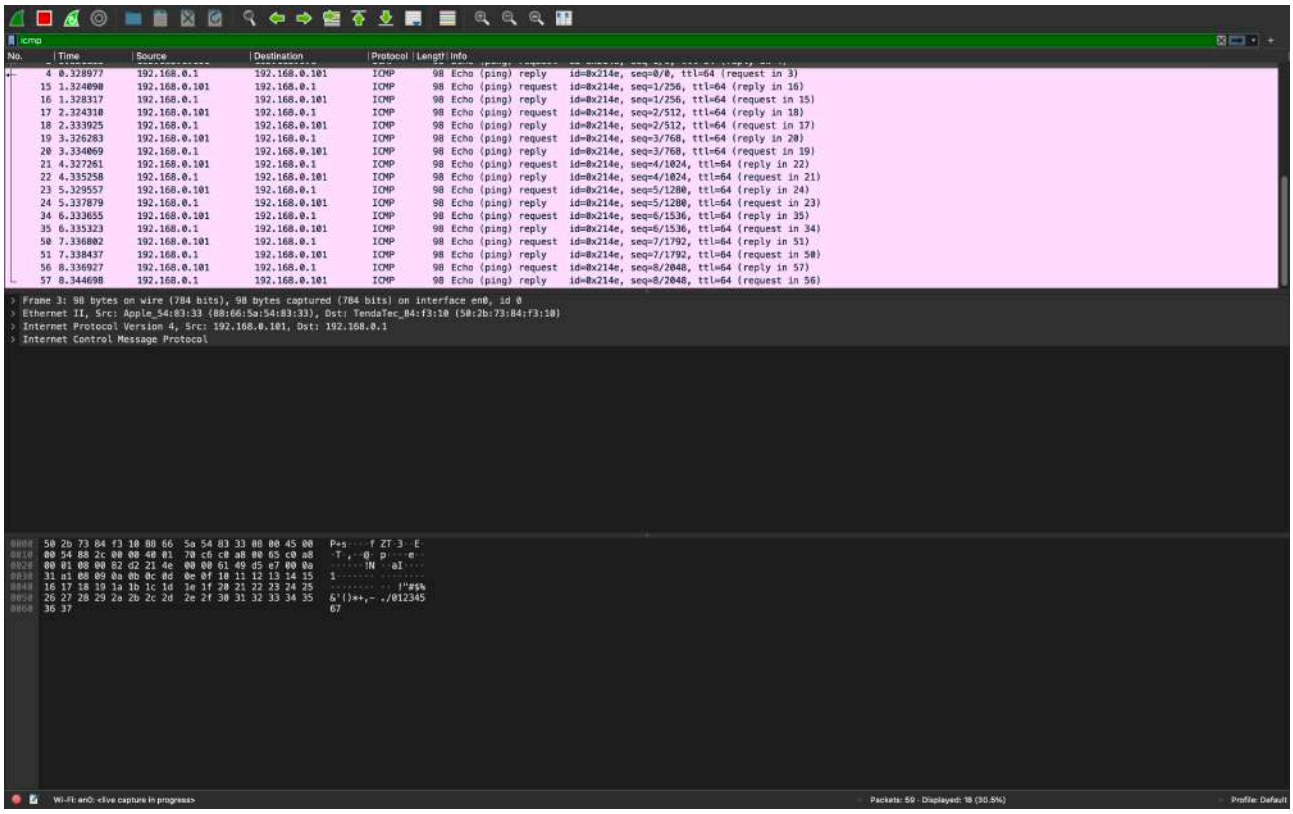

Not Secure | apache.org
News
About
Make a Donation
The Apache Way
Join Us
Downloads
APACHECON 2021
September 21-23
www.apachecon.com
THE APACHE SOFTWARE FOUNDATION
ESTABLISHED 1999
SUPPORT APACHE
COMMUNITY-LED DEVELOPMENT "THE APACHE WAY"
Projects
People
Community
License
Sponsors
THE WORLD'S LARGEST OPEN SOURCE FOUNDATION
All volunteer community
227M+ lines of code in stewardship
4.3B+ lines of code changed
4.4M+ code commits
850+ individual ASF Members
8,200+ Apache Committers
41,000+ code contributors
490,000+ people involved in our communities
350+ Projects and Initiatives
300+ Top-Level Projects
37 podlings in the Apache Incubator
~2 Petabytes source code downloads from Apache mirrors
25M+ emails across 1,400+ mailing lists
Web requests received from every Internet-connected country on the planet
35M+ weekly page views across apache.org
$22B+ worth of Apache Open Source software products are made available to the public-at-large at 100% no cost, and benefit billions of users around the world.
Make a one-time or recurring donation | Corporate Support and ASF Sponsorship
"Trillions and Trillions Served" documentary feature on The Apa...
Watch later
Share
TRILLIONS AND
TRILLIONS
SERVED

D)


Apply a display filter ...<⌘/>
No. Time Source Destination Protocol Length Info
23 6.955490 142.250.196.78 192.168.0.101 QUIC 125 Protected Payload (KP0)
24 6.956611 142.250.196.78 192.168.0.101 QUIC 71 Protected Payload (KP0)
25 6.957018 192.168.0.101 142.250.196.78 QUIC 75 Protected Payload (KP0), DCID=a46173f4564fb9a7
26 7.019854 192.168.0.101 142.250.196.78 ICMP 98 Echo (ping) request id=0xdd4d, seq=30/7680, ttl=64 (reply in 27)
27 7.028988 142.250.196.78 192.168.0.101 ICMP 98 Echo (ping) reply id=0xdd4d, seq=30/7680, ttl=58 (request in 26)
28 7.035211 142.250.196.78 192.168.0.101 QUIC 1059 Protected Payload (KP0)
29 7.035721 192.168.0.101 142.250.196.78 QUIC 77 Protected Payload (KP0), DCID=a46173f4564fb9a7
30 7.036413 192.168.0.101 142.250.196.78 QUIC 75 Protected Payload (KP0), DCID=a46173f4564fb9a7
31 7.036433 192.168.0.101 142.250.196.78 QUIC 78 Protected Payload (KP0), DCID=a46173f4564fb9a7
32 7.036993 142.250.196.78 192.168.0.101 QUIC 67 Protected Payload (KP0)
33 7.044718 142.250.196.78 192.168.0.101 QUIC 67 Protected Payload (KP0)
34 7.063439 192.168.0.101 142.250.196.78 QUIC 75 Protected Payload (KP0), DCID=a46173f4564fb9a7
35 7.070091 142.250.196.78 192.168.0.101 QUIC 67 Protected Payload (KP0)
36 8.021883 192.168.0.101 142.250.196.78 ICMP 98 Echo (ping) request id=0xdd4d, seq=31/7936, ttl=64 (reply in 37)
37 8.031221 142.250.196.78 192.168.0.101 ICMP 98 Echo (ping) reply id=0xdd4d, seq=31/7936, ttl=58 (request in 36)
38 9.023953 192.168.0.101 142.250.196.78 ICMP 98 Echo (ping) request id=0xdd4d, seq=32/8192, ttl=64 (reply in 39)
39 9.033231 142.250.196.78 192.168.0.101 ICMP 98 Echo (ping) reply id=0xdd4d, seq=32/8192, ttl=58 (request in 38)
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
Ethernet II, Src: Apple_54:83:33 (88:66:5a:54:83:33), Dst: TendaTec_84:f3:10 (50:2b:73:84:f3:10)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 142.250.196.78
Internet Control Message Protocol
0000 50 2b 73 84 f3 10 88 66 5a 54 83 33 08 00 45 00 P+s····f ZT·3··E
0010 00 54 55 c7 00 00 40 01 10 8c c0 a8 00 65 8e fa ·TU···@· ·····e··
0020 c4 4e 08 00 b6 69 dd 4d 00 17 61 49 d4 d4 00 00 ·N···i·M ··aI····
0030 43 08 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 C····· ········
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ········ ··· !"#$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,- ./012345
0060 36 37 67
Wi-Fi: en0: <live capture in progress>
Packets: 39 · Displayed: 39 (100.0%)
Profile: Default


No. Time Source Destination Protocol Length Info
198 12.982582 fe80::1c50:e1a3:9e… ff02::fb MDNS 607 Standard query response 0x0000 TXT, cache flush PTR _companion-link._tcp.local PTR apoorva's iPad (2)._companion-link._tcp.local TXT SRV, cache flu…
199 13.077453 192.168.0.101 192.168.0.1 ICMP 98 Echo (ping) request id=0x074e, seq=10/2560, ttl=64 (reply in 200)
200 13.079112 192.168.0.1 192.168.0.101 ICMP 98 Echo (ping) reply id=0x074e, seq=10/2560, ttl=64 (request in 199)
201 13.215087 192.168.0.101 17.57.145.117 TLSv1… 132 Application Data
202 13.248984 192.168.0.101 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
203 13.452229 192.168.0.101 17.57.145.117 TCP 132 [TCP Retransmission] 55164 → 5223 [PSH, ACK] Seq=1 Ack=1 Win=2048 Len=66 TSval=2057016703 TSecr=2160668454
204 13.721380 TendaTec_84:f3:10 Apple_54:83:33 ARP 42 192.168.0.1 is at 50:2b:73:84:f3:10
205 13.733179 192.168.0.192 224.0.0.251 MDNS 203 Standard query response 0x0000 PTR apoorva's iPad (2)._companion-link._tcp.local TXT OPT
206 13.733186 fe80::1c50:e1a3:9e… ff02::fb MDNS 223 Standard query response 0x0000 PTR apoorva's iPad (2)._companion-link._tcp.local TXT OPT
207 13.761262 192.168.0.101 17.57.145.117 TCP 132 [TCP Retransmission] 55164 → 5223 [PSH, ACK] Seq=1 Ack=1 Win=2048 Len=66 TSval=2057017012 TSecr=2160668454
208 14.080314 192.168.0.101 192.168.0.1 ICMP 98 Echo (ping) request id=0x074e, seq=11/2816, ttl=64 (reply in 209)
209 14.080373 192.168.0.1 192.168.0.101 ICMP 98 Echo (ping) reply id=0x074e, seq=11/2816, ttl=64 (request in 208)
210 14.180111 192.168.0.101 17.57.145.117 TCP 132 [TCP Retransmission] 55164 → 5223 [PSH, ACK] Seq=1 Ack=1 Win=2048 Len=66 TSval=2057017438 TSecr=2160668454
211 14.249180 192.168.0.101 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
212 14.817428 192.168.0.101 17.57.145.117 TCP 132 [TCP Retransmission] 55164 → 5223 [PSH, ACK] Seq=1 Ack=1 Win=2048 Len=66 TSval=2057018067 TSecr=2160668454
213 15.082749 192.168.0.101 192.168.0.1 ICMP 98 Echo (ping) request id=0x074e, seq=12/3072, ttl=64 (reply in 214)
214 15.090652 192.168.0.1 192.168.0.101 ICMP 98 Echo (ping) reply id=0x074e, seq=12/3072, ttl=64 (request in 213)
Frame 133: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en0, id 0
Ethernet II, Src: Apple_54:83:33 (88:66:5a:54:83:33), Dst: TendaTec_84:f3:10 (50:2b:73:84:f3:10)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 52.113.194.132
Transmission Control Protocol, Src Port: 55215, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
0000 50 2b 73 84 f3 10 88 66 5a 54 83 33 08 00 45 00 P+s····f ZT·3··E
0010 00 28 94 c5 00 00 40 06 2e 08 c0 a8 00 65 34 71 ·(····@· ·····e4q
0020 c2 84 d7 af 01 bb 43 c4 9e e5 9f bd da 63 50 10 ····· C· ·····cP
0030 10 00 b1 9b 00 00 ····· ·····
Wi-Fi: en0: <live capture in progress>
Packets: 214 · Displayed: 214 (100.0%)
Profile: Default

E)


icmp
No. Time Source Destination Protocol Length Info
4 0.328977 192.168.0.1 192.168.0.101 ICMP 98 Echo (ping) reply id=0x214e, seq=0/0, ttl=64 (request in 3)
15 1.324090 192.168.0.101 192.168.0.1 ICMP 98 Echo (ping) request id=0x214e, seq=1/256, ttl=64 (reply in 16)
16 1.328317 192.168.0.1 192.168.0.101 ICMP 98 Echo (ping) reply id=0x214e, seq=1/256, ttl=64 (request in 15)
17 2.324310 192.168.0.101 192.168.0.1 ICMP 98 Echo (ping) request id=0x214e, seq=2/512, ttl=64 (reply in 18)
18 2.333925 192.168.0.1 192.168.0.101 ICMP 98 Echo (ping) reply id=0x214e, seq=2/512, ttl=64 (request in 17)
19 3.326283 192.168.0.101 192.168.0.1 ICMP 98 Echo (ping) request id=0x214e, seq=3/768, ttl=64 (reply in 20)
20 3.334069 192.168.0.1 192.168.0.101 ICMP 98 Echo (ping) reply id=0x214e, seq=3/768, ttl=64 (request in 19)
21 4.327261 192.168.0.101 192.168.0.1 ICMP 98 Echo (ping) request id=0x214e, seq=4/1024, ttl=64 (reply in 22)
22 4.335258 192.168.0.1 192.168.0.101 ICMP 98 Echo (ping) reply id=0x214e, seq=4/1024, ttl=64 (request in 21)
23 5.329557 192.168.0.101 192.168.0.1 ICMP 98 Echo (ping) request id=0x214e, seq=5/1280, ttl=64 (reply in 24)
24 5.337879 192.168.0.1 192.168.0.101 ICMP 98 Echo (ping) reply id=0x214e, seq=5/1280, ttl=64 (request in 23)
34 6.333655 192.168.0.101 192.168.0.1 ICMP 98 Echo (ping) request id=0x214e, seq=6/1536, ttl=64 (reply in 35)
35 6.335323 192.168.0.1 192.168.0.101 ICMP 98 Echo (ping) reply id=0x214e, seq=6/1536, ttl=64 (request in 34)
50 7.336802 192.168.0.101 192.168.0.1 ICMP 98 Echo (ping) request id=0x214e, seq=7/1792, ttl=64 (reply in 51)
51 7.338437 192.168.0.1 192.168.0.101 ICMP 98 Echo (ping) reply id=0x214e, seq=7/1792, ttl=64 (request in 50)
56 8.336927 192.168.0.101 192.168.0.1 ICMP 98 Echo (ping) request id=0x214e, seq=8/2048, ttl=64 (reply in 57)
57 8.344698 192.168.0.1 192.168.0.101 ICMP 98 Echo (ping) reply id=0x214e, seq=8/2048, ttl=64 (request in 56)
Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
Ethernet II, Src: Apple_54:83:33 (88:66:5a:54:83:33), Dst: TendaTec_84:f3:10 (50:2b:73:84:f3:10)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
Internet Control Message Protocol
0000 50 2b 73 84 f3 10 88 66 5a 54 83 33 08 00 45 00 P+s····f ZT·3··E
0010 00 54 88 2c 00 00 40 01 70 c6 c0 a8 00 65 c0 a8 ·T·,··@· p····e··
0020 00 01 08 00 82 d2 21 4e 00 00 61 49 d5 e7 00 0a ····!N ··aI····
0030 31 a1 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 1·· ·· ·· ·· ·· ··
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ·· ·· ·· ·· ·· !"#$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,- ./012345
0060 36 37 67
Wi-Fi: en0: <live capture in progress>
Packets: 59 · Displayed: 18 (30.5%)
Profile: Default