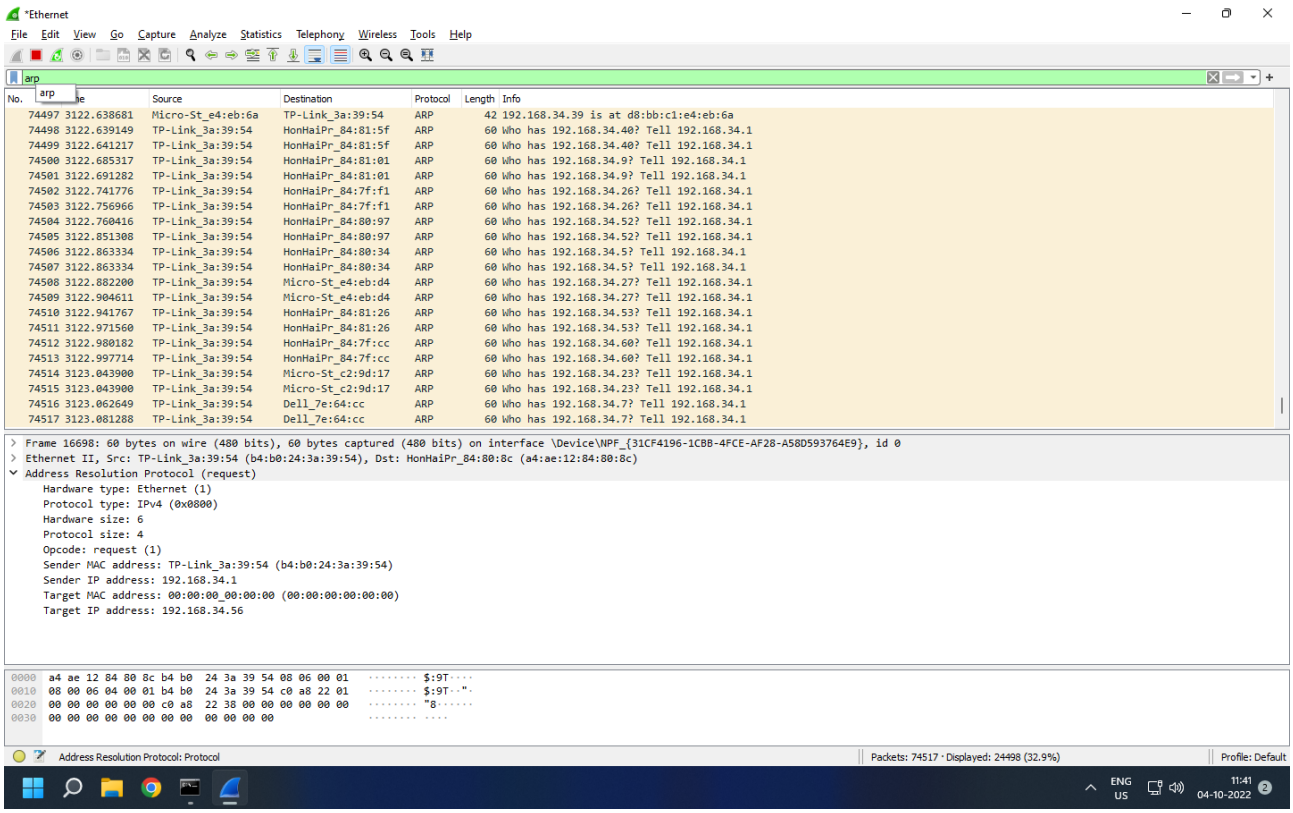
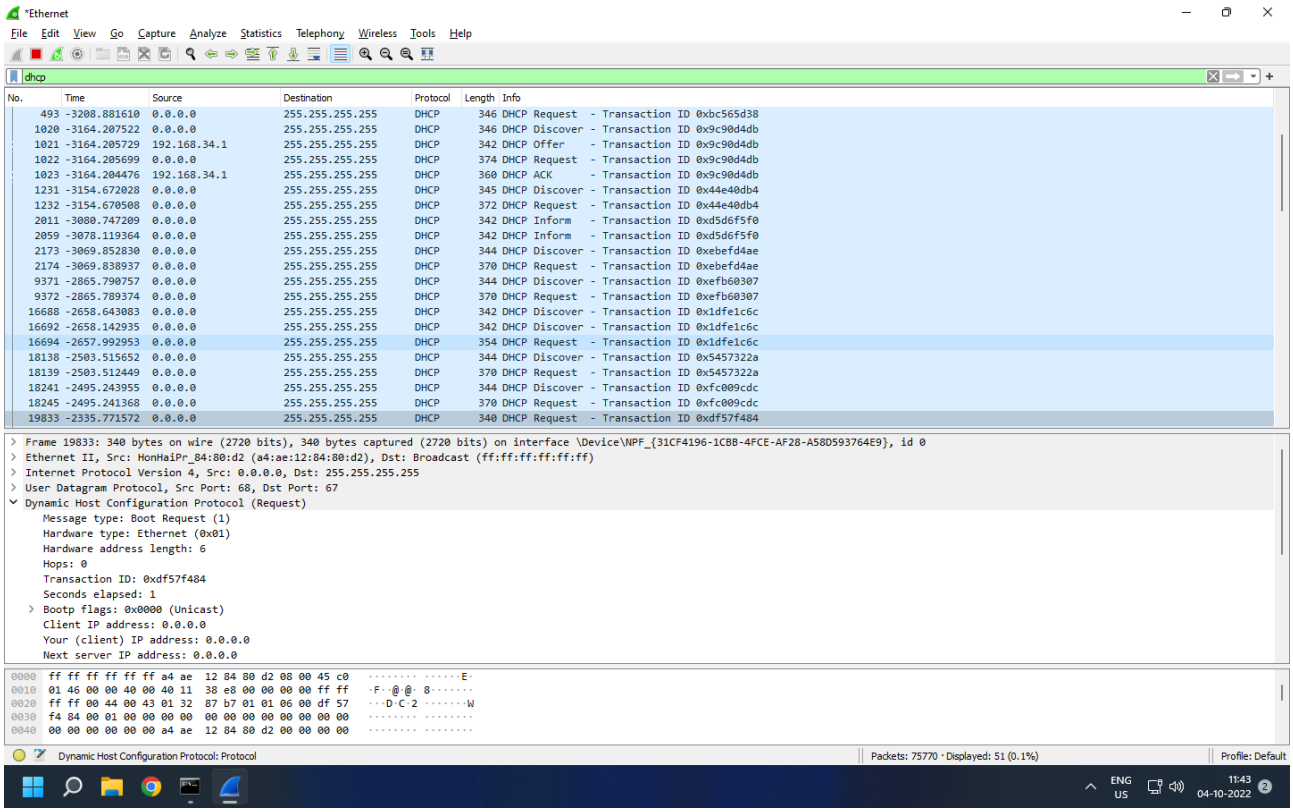
Computer Networks
Experiment - 9

Outputs:-

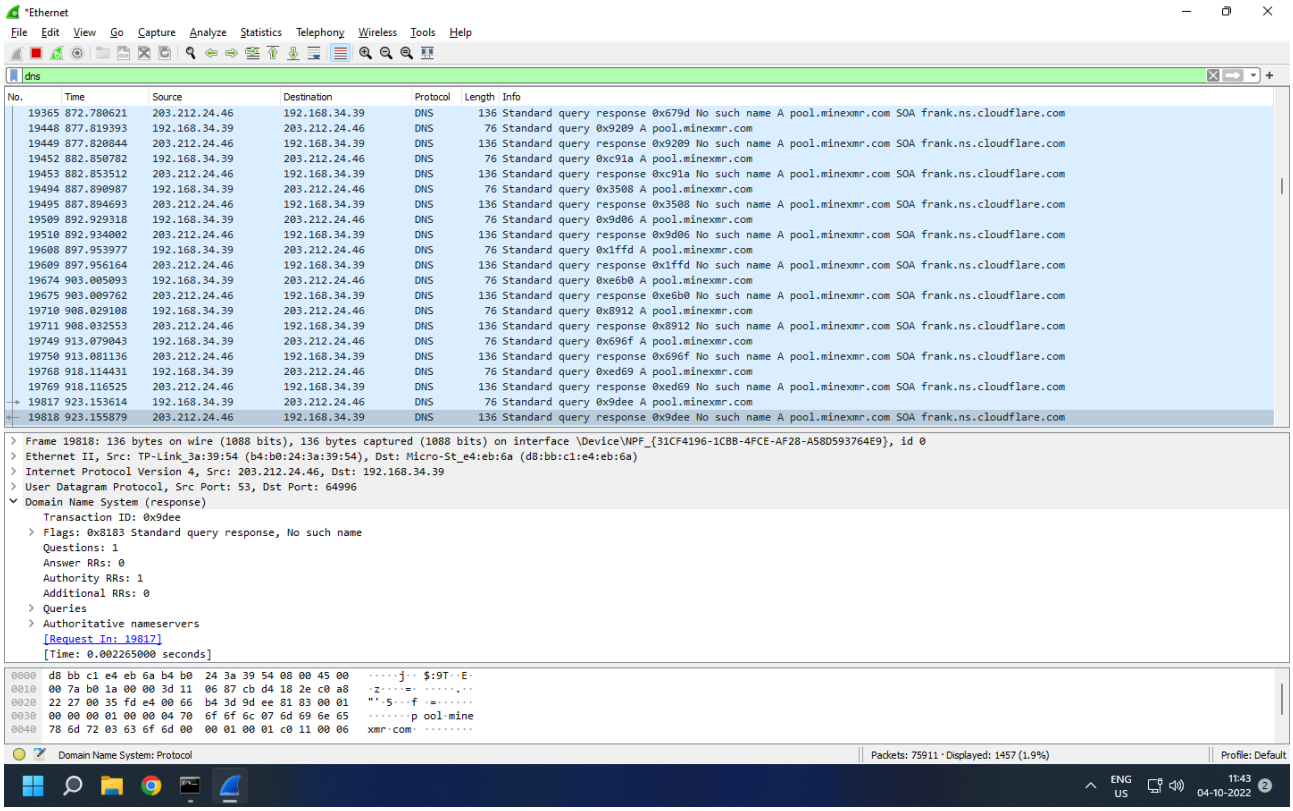
ARP:-



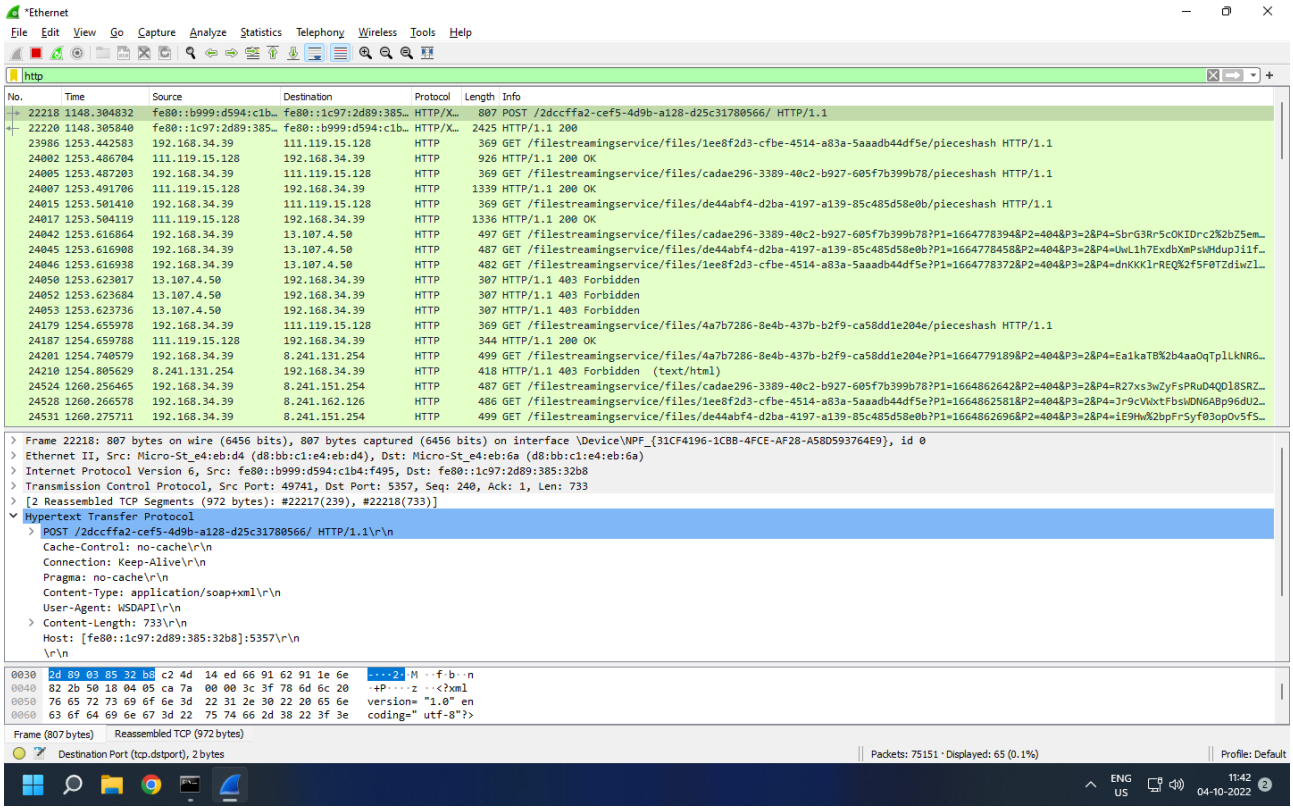
DHCP:-



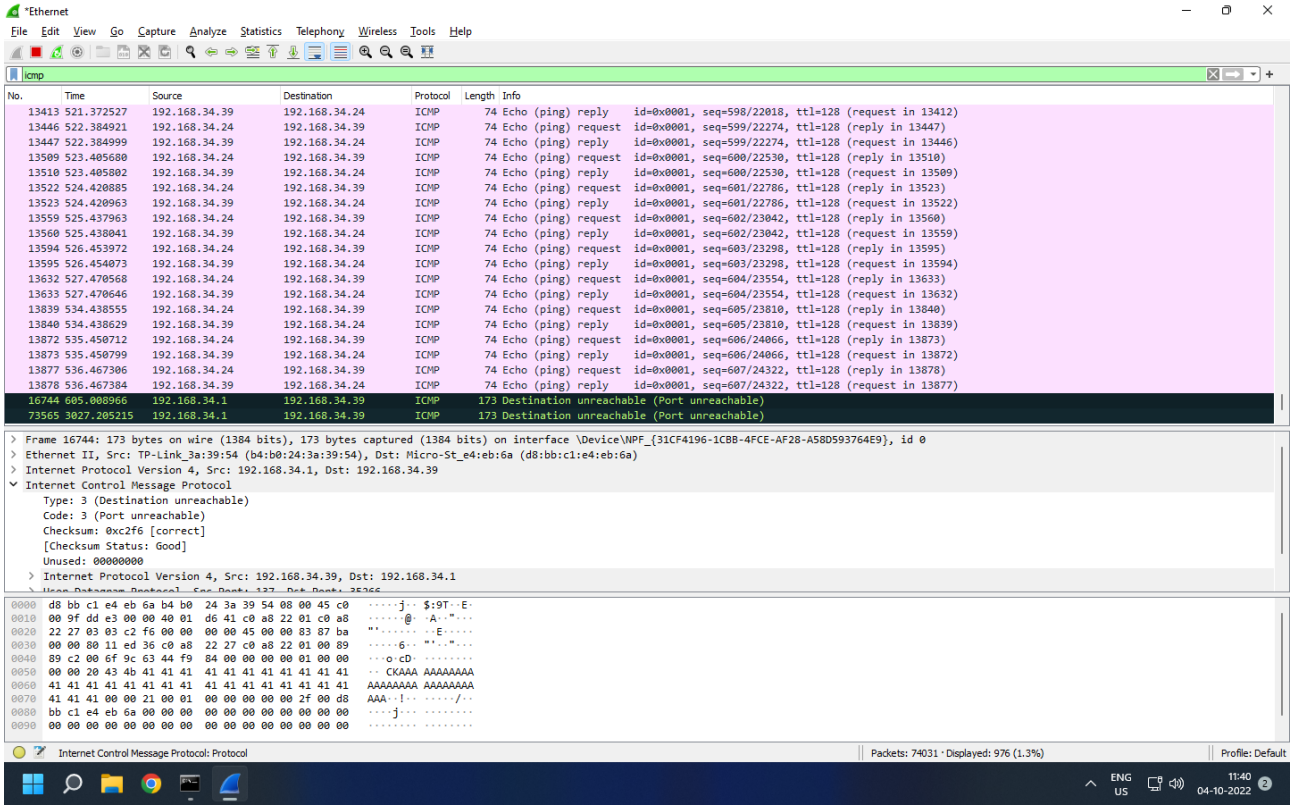
DNS:-


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
19365 872.780621 203.212.24.46 192.168.34.39 DNS 136 Standard query response 0x679d No such name A pool.minexmr.com SOA frank.ns.cloudflare.com
19448 877.819393 192.168.34.39 203.212.24.46 DNS 76 Standard query 0x9209 A pool.minexmr.com
19449 877.820844 203.212.24.46 192.168.34.39 DNS 136 Standard query response 0x9209 No such name A pool.minexmr.com SOA frank.ns.cloudflare.com
19452 882.850782 192.168.34.39 203.212.24.46 DNS 76 Standard query 0xc91a A pool.minexmr.com
19453 882.853512 203.212.24.46 192.168.34.39 DNS 136 Standard query response 0xc91a No such name A pool.minexmr.com SOA frank.ns.cloudflare.com
19494 887.890987 192.168.34.39 203.212.24.46 DNS 76 Standard query 0x3508 A pool.minexmr.com
19495 887.894693 203.212.24.46 192.168.34.39 DNS 136 Standard query response 0x3508 No such name A pool.minexmr.com SOA frank.ns.cloudflare.com
19509 892.929318 192.168.34.39 203.212.24.46 DNS 76 Standard query 0x9d06 A pool.minexmr.com
19510 892.934002 203.212.24.46 192.168.34.39 DNS 136 Standard query response 0x9d06 No such name A pool.minexmr.com SOA frank.ns.cloudflare.com
19608 897.953977 192.168.34.39 203.212.24.46 DNS 76 Standard query 0x1ffd A pool.minexmr.com
19609 897.956164 203.212.24.46 192.168.34.39 DNS 136 Standard query response 0x1ffd No such name A pool.minexmr.com SOA frank.ns.cloudflare.com
19674 903.005093 192.168.34.39 203.212.24.46 DNS 76 Standard query 0xe6b0 A pool.minexmr.com
19675 903.009762 203.212.24.46 192.168.34.39 DNS 136 Standard query response 0xe6b0 No such name A pool.minexmr.com SOA frank.ns.cloudflare.com
19710 908.029108 192.168.34.39 203.212.24.46 DNS 76 Standard query 0x8912 A pool.minexmr.com
19711 908.032553 203.212.24.46 192.168.34.39 DNS 136 Standard query response 0x8912 No such name A pool.minexmr.com SOA frank.ns.cloudflare.com
19749 913.079043 192.168.34.39 203.212.24.46 DNS 76 Standard query 0x696f A pool.minexmr.com
19750 913.081136 203.212.24.46 192.168.34.39 DNS 136 Standard query response 0x696f No such name A pool.minexmr.com SOA frank.ns.cloudflare.com
19768 918.114431 192.168.34.39 203.212.24.46 DNS 76 Standard query 0xed69 A pool.minexmr.com
19769 918.116525 203.212.24.46 192.168.34.39 DNS 136 Standard query response 0xed69 No such name A pool.minexmr.com SOA frank.ns.cloudflare.com
19817 923.153614 192.168.34.39 203.212.24.46 DNS 76 Standard query 0x9dee A pool.minexmr.com
19818 923.155879 203.212.24.46 192.168.34.39 DNS 136 Standard query response 0x9dee No such name A pool.minexmr.com SOA frank.ns.cloudflare.com
Frame 19818: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface \Device\NPF_{31CF4196-1CBB-4FCE-AF28-A58D593764E9}, id 0
Ethernet II, Src: TP-Link_3a:39:54 (b4:b0:24:3a:39:54), Dst: Micro-St_e4:eb:6a (d8:bb:c1:e4:eb:6a)
Internet Protocol Version 4, Src: 203.212.24.46, Dst: 192.168.34.39
User Datagram Protocol, Src Port: 53, Dst Port: 64996
Domain Name System (response)
Transaction ID: 0x9dee
Flags: 0x8183 Standard query response, No such name
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
Authoritative nameservers
[Request In: 19817]
[Time: 0.002265000 seconds]
0000 d8 bb c1 e4 eb 6a b4 b0 24 3a 39 54 08 00 45 00 .....j.. $:9T..E.
0010 00 7a b0 1a 00 00 3d 11 06 87 cb d4 18 2e c0 a8 .z....=. ....
0020 22 27 00 35 fd e4 00 66 b4 3d 9d ee 81 83 00 01 "'.5...f .=......
0030 00 00 00 01 00 00 04 70 6f 6f 6c 07 6d 69 6e 65 ....p ool.mine
0040 78 6d 72 03 63 6f 6d 00 00 01 00 01 c0 11 00 06 xmr.com. ....
Domain Name System: Protocol
Packets: 75911 · Displayed: 1457 (1.9%)
Profile: Default
ENG US
11:43
04-10-2022

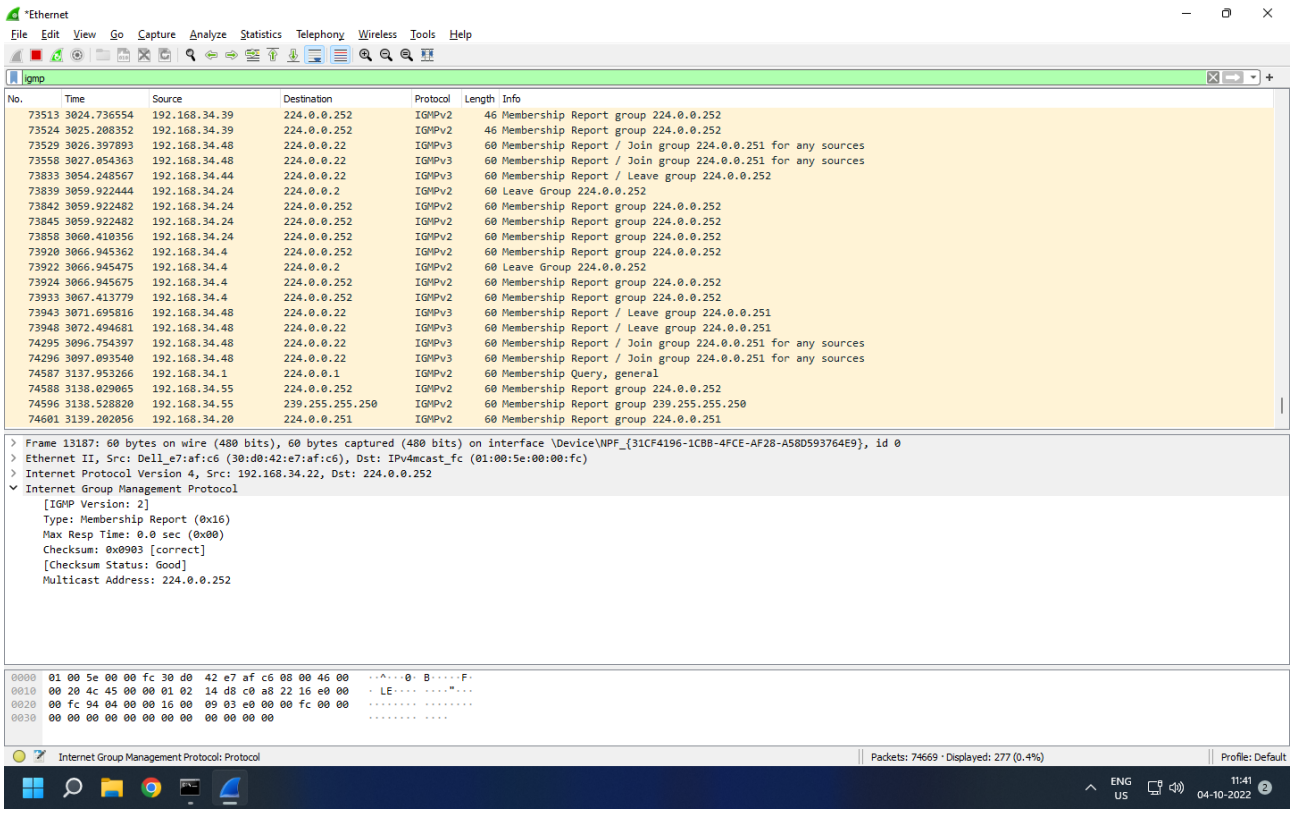
HTTP:-


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
22218 1148.304832 fe80::b999:d594:c1b… fe80::1c97:2d89:385… HTTP/X… 807 POST /2dccffa2-cef5-4d9b-a128-d25c31780566/ HTTP/1.1
22220 1148.305840 fe80::1c97:2d89:385… fe80::b999:d594:c1b… HTTP/X… 2425 HTTP/1.1 200
23986 1253.442583 192.168.34.39 111.119.15.128 HTTP 369 GET /filestreamingservice/files/1ee8f2d3-cfbe-4514-a83a-5aaadb44df5e/pieceshash HTTP/1.1
24002 1253.486704 111.119.15.128 192.168.34.39 HTTP 926 HTTP/1.1 200 OK
24005 1253.487203 192.168.34.39 111.119.15.128 HTTP 369 GET /filestreamingservice/files/cadae296-3389-40c2-b927-605f7b399b78/pieceshash HTTP/1.1
24007 1253.491706 111.119.15.128 192.168.34.39 HTTP 1339 HTTP/1.1 200 OK
24015 1253.501410 192.168.34.39 111.119.15.128 HTTP 369 GET /filestreamingservice/files/de44abf4-d2ba-4197-a139-85c485d58e0b/pieceshash HTTP/1.1
24017 1253.504119 111.119.15.128 192.168.34.39 HTTP 1336 HTTP/1.1 200 OK
24042 1253.616864 192.168.34.39 13.107.4.50 HTTP 497 GET /filestreamingservice/files/cadae296-3389-40c2-b927-605f7b399b78?P1=1664778394&P2=404&P3=2&P4=SbrG3Rr5cOKIDrc2%2bZ5em…
24045 1253.616908 192.168.34.39 13.107.4.50 HTTP 487 GET /filestreamingservice/files/de44abf4-d2ba-4197-a139-85c485d58e0b?P1=1664778458&P2=404&P3=2&P4=UwL1h7ExdbXmPsWHdupJi1f…
24046 1253.616938 192.168.34.39 13.107.4.50 HTTP 482 GET /filestreamingservice/files/1ee8f2d3-cfbe-4514-a83a-5aaadb44df5e?P1=1664778372&P2=404&P3=2&P4=dnKKKlrREQ%2f5F0TZdiwZl…
24050 1253.623017 13.107.4.50 192.168.34.39 HTTP 307 HTTP/1.1 403 Forbidden
24052 1253.623684 13.107.4.50 192.168.34.39 HTTP 307 HTTP/1.1 403 Forbidden
24053 1253.623736 13.107.4.50 192.168.34.39 HTTP 307 HTTP/1.1 403 Forbidden
24179 1254.655978 192.168.34.39 111.119.15.128 HTTP 369 GET /filestreamingservice/files/4a7b7286-8e4b-437b-b2f9-ca58dd1e204e/pieceshash HTTP/1.1
24187 1254.659788 111.119.15.128 192.168.34.39 HTTP 344 HTTP/1.1 200 OK
24201 1254.740579 192.168.34.39 8.241.131.254 HTTP 499 GET /filestreamingservice/files/4a7b7286-8e4b-437b-b2f9-ca58dd1e204e?P1=1664779189&P2=404&P3=2&P4=Ea1kaTB%2b4aaOqTplLkNR6…
24210 1254.805629 8.241.131.254 192.168.34.39 HTTP 418 HTTP/1.1 403 Forbidden (text/html)
24524 1260.256465 192.168.34.39 8.241.151.254 HTTP 487 GET /filestreamingservice/files/cadae296-3389-40c2-b927-605f7b399b78?P1=1664862642&P2=404&P3=2&P4=R27xs3wZyFsPRuD4QDl8SRZ…
24528 1260.266578 192.168.34.39 8.241.162.126 HTTP 486 GET /filestreamingservice/files/1ee8f2d3-cfbe-4514-a83a-5aaadb44df5e?P1=1664862581&P2=404&P3=2&P4=Jr9cVWxtFbsWDN6ABp96dU2…
24531 1260.275711 192.168.34.39 8.241.151.254 HTTP 499 GET /filestreamingservice/files/de44abf4-d2ba-4197-a139-85c485d58e0b?P1=1664862696&P2=404&P3=2&P4=iE9Hw%2bpFrSyf03opOv5fS…
Frame 22218: 807 bytes on wire (6456 bits), 807 bytes captured (6456 bits) on interface \Device\NPF_{31CF4196-1CBB-4FCE-AF28-A58D593764E9}, id 0
Ethernet II, Src: Micro-St_e4:eb:d4 (d8:bb:c1:e4:eb:d4), Dst: Micro-St_e4:eb:6a (d8:bb:c1:e4:eb:6a)
Internet Protocol Version 6, Src: fe80::b999:d594:c1b4:f495, Dst: fe80::1c97:2d89:385:32b8
Transmission Control Protocol, Src Port: 49741, Dst Port: 5357, Seq: 240, Ack: 1, Len: 733
[2 Reassembled TCP Segments (972 bytes): #22217(239), #22218(733)]
Hypertext Transfer Protocol
POST /2dccffa2-cef5-4d9b-a128-d25c31780566/ HTTP/1.1\r\n
Cache-Control: no-cache\r\n
Connection: Keep-Alive\r\n
Pragma: no-cache\r\n
Content-Type: application/soap+xml\r\n
User-Agent: WSDAPI\r\n
Content-Length: 733\r\n
Host: [fe80::1c97:2d89:385:32b8]:5357\r\n
\r\n
0030 2d 89 03 85 32 b8 c2 4d 14 ed 66 91 62 91 1e 6e -...2..M ..f.b..n
0040 82 2b 50 18 04 05 ca 7a 00 00 3c 3f 78 6d 6c 20 .+P....z ..<?xml
0050 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e version= "1.0" en
0060 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e coding=" utf-8"?>
Frame (807 bytes) Reassembled TCP (972 bytes)
Destination Port (tcp.dstport), 2 bytes
Packets: 75151 · Displayed: 65 (0.1%)
Profile: Default
ENG US
11:42
04-10-2022

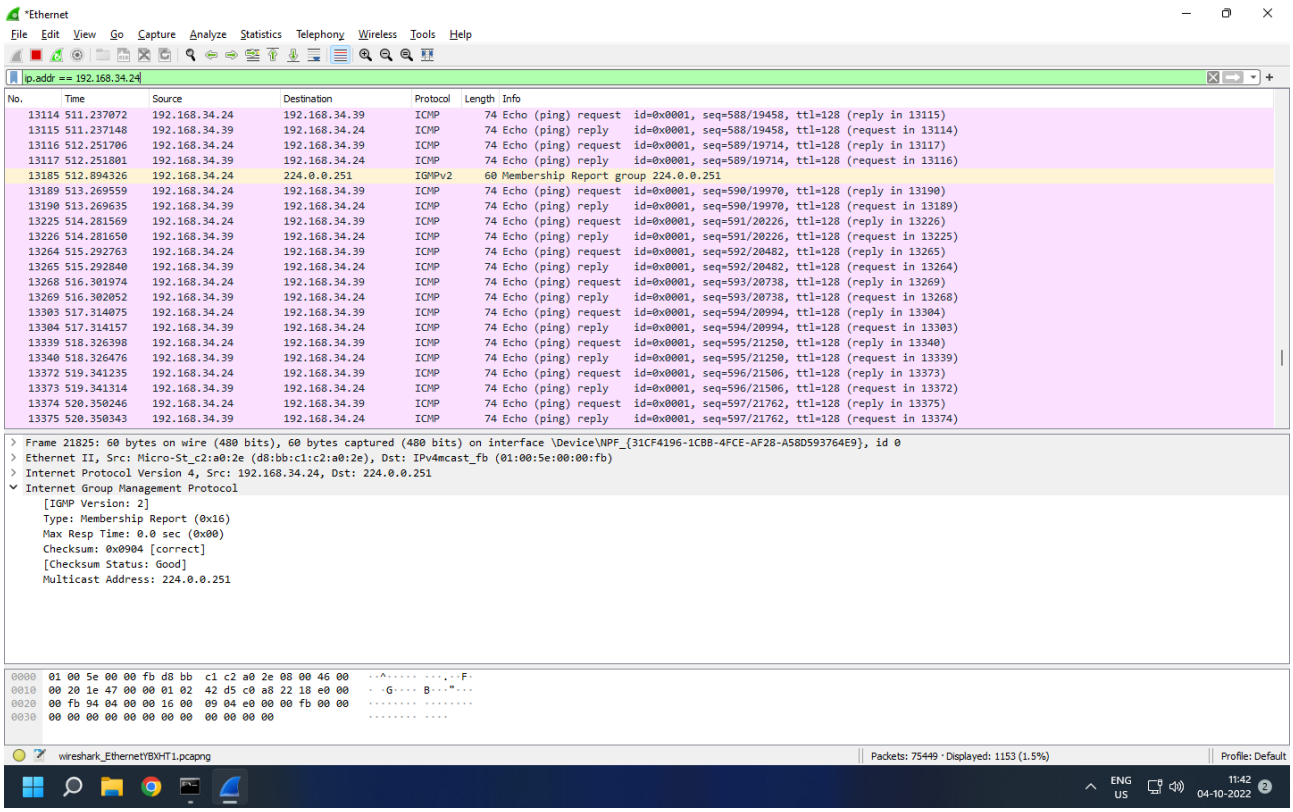
ICMP:-


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
13413 521.372527 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=598/22018, ttl=128 (request in 13412)
13446 522.384921 192.168.34.24 192.168.34.39 ICMP 74 Echo (ping) request id=0x0001, seq=599/22274, ttl=128 (reply in 13447)
13447 522.384999 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=599/22274, ttl=128 (request in 13446)
13509 523.405680 192.168.34.24 192.168.34.39 ICMP 74 Echo (ping) request id=0x0001, seq=600/22530, ttl=128 (reply in 13510)
13510 523.405802 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=600/22530, ttl=128 (request in 13509)
13522 524.420885 192.168.34.24 192.168.34.39 ICMP 74 Echo (ping) request id=0x0001, seq=601/22786, ttl=128 (reply in 13523)
13523 524.420963 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=601/22786, ttl=128 (request in 13522)
13559 525.437963 192.168.34.24 192.168.34.39 ICMP 74 Echo (ping) request id=0x0001, seq=602/23042, ttl=128 (reply in 13560)
13560 525.438041 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=602/23042, ttl=128 (request in 13559)
13594 526.453972 192.168.34.24 192.168.34.39 ICMP 74 Echo (ping) request id=0x0001, seq=603/23298, ttl=128 (reply in 13595)
13595 526.454073 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=603/23298, ttl=128 (request in 13594)
13632 527.470568 192.168.34.24 192.168.34.39 ICMP 74 Echo (ping) request id=0x0001, seq=604/23554, ttl=128 (reply in 13633)
13633 527.470646 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=604/23554, ttl=128 (request in 13632)
13839 534.438555 192.168.34.24 192.168.34.39 ICMP 74 Echo (ping) request id=0x0001, seq=605/23810, ttl=128 (reply in 13840)
13840 534.438629 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=605/23810, ttl=128 (request in 13839)
13872 535.450712 192.168.34.24 192.168.34.39 ICMP 74 Echo (ping) request id=0x0001, seq=606/24066, ttl=128 (reply in 13873)
13873 535.450799 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=606/24066, ttl=128 (request in 13872)
13877 536.467306 192.168.34.24 192.168.34.39 ICMP 74 Echo (ping) request id=0x0001, seq=607/24322, ttl=128 (reply in 13878)
13878 536.467384 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=607/24322, ttl=128 (request in 13877)
16744 605.008966 192.168.34.1 192.168.34.39 ICMP 173 Destination unreachable (Port unreachable)
73565 3027.205215 192.168.34.1 192.168.34.39 ICMP 173 Destination unreachable (Port unreachable)
Frame 16744: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface \Device\NPF_{31CF4196-1CBB-4FCE-AF28-A58D593764E9}, id 0
Ethernet II, Src: TP-Link_3a:39:54 (b4:b0:24:3a:39:54), Dst: Micro-St_e4:eb:6a (d8:bb:c1:e4:eb:6a)
Internet Protocol Version 4, Src: 192.168.34.1, Dst: 192.168.34.39
Internet Control Message Protocol
Type: 3 (Destination unreachable)
Code: 3 (Port unreachable)
Checksum: 0xc2f6 [correct]
[Checksum Status: Good]
Unused: 00000000
Internet Protocol Version 4, Src: 192.168.34.39, Dst: 192.168.34.1
0000 d8 bb c1 e4 eb 6a b4 b0 24 3a 39 54 08 00 45 c0
0010 00 9f dd e3 00 00 40 01 d6 41 c0 a8 22 01 c0 a8
0020 22 27 03 03 c2 f6 00 00 00 00 45 00 00 83 87 ba
0030 00 00 80 11 ed 36 c0 a8 22 27 c0 a8 22 01 00 89
0040 89 c2 00 6f 9c 63 44 f9 84 00 00 00 00 01 00 00
0050 00 00 20 43 4b 41 41 41 41 41 41 41 41 41 41 41
0060 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
0070 41 41 41 00 00 21 00 01 00 00 00 00 00 2f 00 d8
0080 bb c1 e4 eb 6a 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Internet Control Message Protocol: Protocol
Packets: 74031 · Displayed: 976 (1.3%)
Profile: Default
ENG US
11:40
04-10-2022

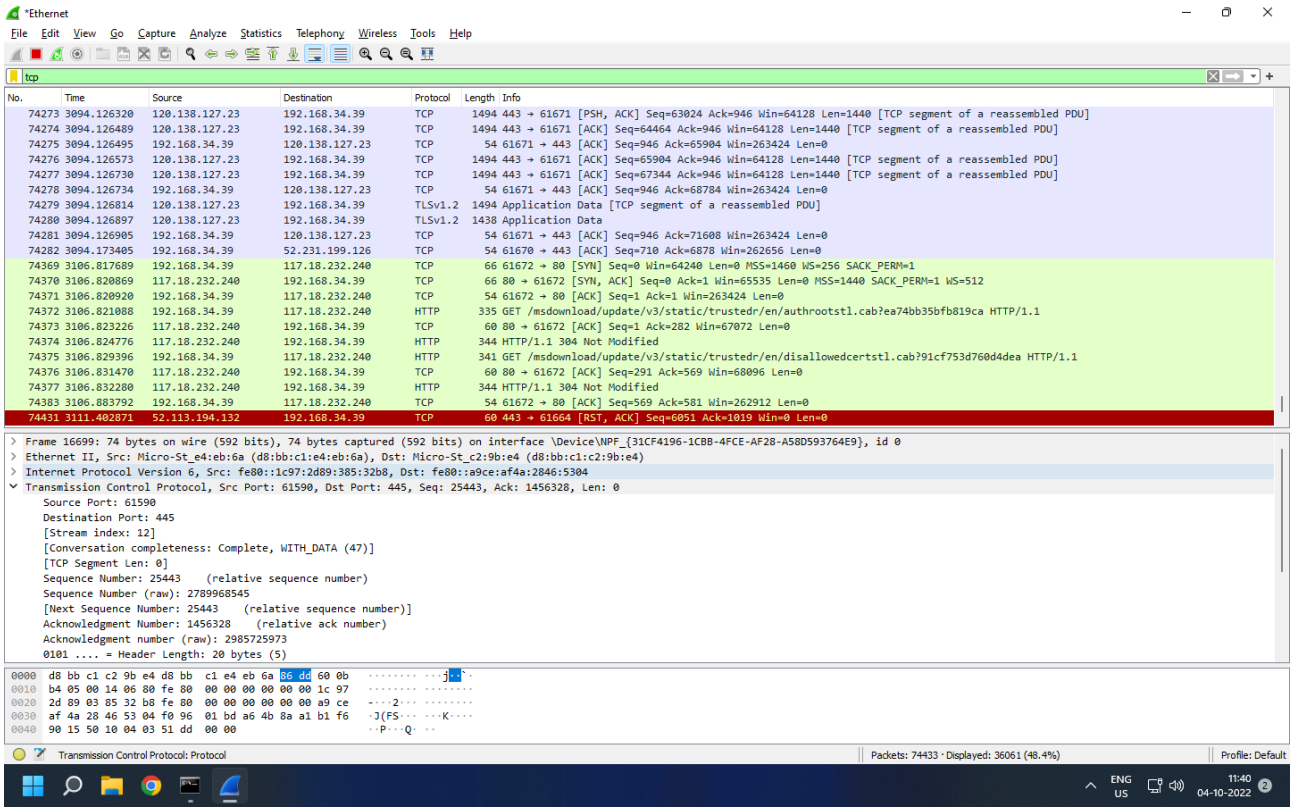
IGMP:-


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
igmp
No. Time Source Destination Protocol Length Info
73513 3024.736554 192.168.34.39 224.0.0.252 IGMPv2 46 Membership Report group 224.0.0.252
73524 3025.208352 192.168.34.39 224.0.0.252 IGMPv2 46 Membership Report group 224.0.0.252
73529 3026.397893 192.168.34.48 224.0.0.22 IGMPv3 60 Membership Report / Join group 224.0.0.251 for any sources
73558 3027.054363 192.168.34.48 224.0.0.22 IGMPv3 60 Membership Report / Join group 224.0.0.251 for any sources
73833 3054.248567 192.168.34.44 224.0.0.22 IGMPv3 60 Membership Report / Leave group 224.0.0.252
73839 3059.922444 192.168.34.24 224.0.0.2 IGMPv2 60 Leave Group 224.0.0.252
73842 3059.922482 192.168.34.24 224.0.0.252 IGMPv2 60 Membership Report group 224.0.0.252
73845 3059.922482 192.168.34.24 224.0.0.252 IGMPv2 60 Membership Report group 224.0.0.252
73858 3060.410356 192.168.34.24 224.0.0.252 IGMPv2 60 Membership Report group 224.0.0.252
73920 3066.945362 192.168.34.4 224.0.0.252 IGMPv2 60 Membership Report group 224.0.0.252
73922 3066.945475 192.168.34.4 224.0.0.2 IGMPv2 60 Leave Group 224.0.0.252
73924 3066.945675 192.168.34.4 224.0.0.252 IGMPv2 60 Membership Report group 224.0.0.252
73933 3067.413779 192.168.34.4 224.0.0.252 IGMPv2 60 Membership Report group 224.0.0.252
73943 3071.695816 192.168.34.48 224.0.0.22 IGMPv3 60 Membership Report / Leave group 224.0.0.251
73948 3072.494681 192.168.34.48 224.0.0.22 IGMPv3 60 Membership Report / Leave group 224.0.0.251
74295 3096.754397 192.168.34.48 224.0.0.22 IGMPv3 60 Membership Report / Join group 224.0.0.251 for any sources
74296 3097.093540 192.168.34.48 224.0.0.22 IGMPv3 60 Membership Report / Join group 224.0.0.251 for any sources
74587 3137.953266 192.168.34.1 224.0.0.1 IGMPv2 60 Membership Query, general
74588 3138.029065 192.168.34.55 224.0.0.252 IGMPv2 60 Membership Report group 224.0.0.252
74596 3138.528820 192.168.34.55 239.255.255.250 IGMPv2 60 Membership Report group 239.255.255.250
74601 3139.202056 192.168.34.20 224.0.0.251 IGMPv2 60 Membership Report group 224.0.0.251
Frame 13187: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{31CF4196-1CBB-4FCE-AF28-A58D593764E9}, id 0
Ethernet II, Src: Dell_e7:af:c6 (30:d0:42:e7:af:c6), Dst: IPv4mcast_fc (01:00:5e:00:00:fc)
Internet Protocol Version 4, Src: 192.168.34.22, Dst: 224.0.0.252
Internet Group Management Protocol
[IGMP Version: 2]
Type: Membership Report (0x16)
Max Resp Time: 0.0 sec (0x00)
Checksum: 0x0903 [correct]
[Checksum Status: Good]
Multicast Address: 224.0.0.252
0000 01 00 5e 00 00 fc 30 d0 42 e7 af c6 08 00 46 00
0010 00 20 4c 45 00 00 01 02 14 d8 c0 a8 22 16 e0 00
0020 00 fc 94 04 00 00 16 00 09 03 e0 00 00 fc 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
Internet Group Management Protocol: Protocol
Packets: 74669 · Displayed: 277 (0.4%)
Profile: Default
ENG US
11:41
04-10-2022

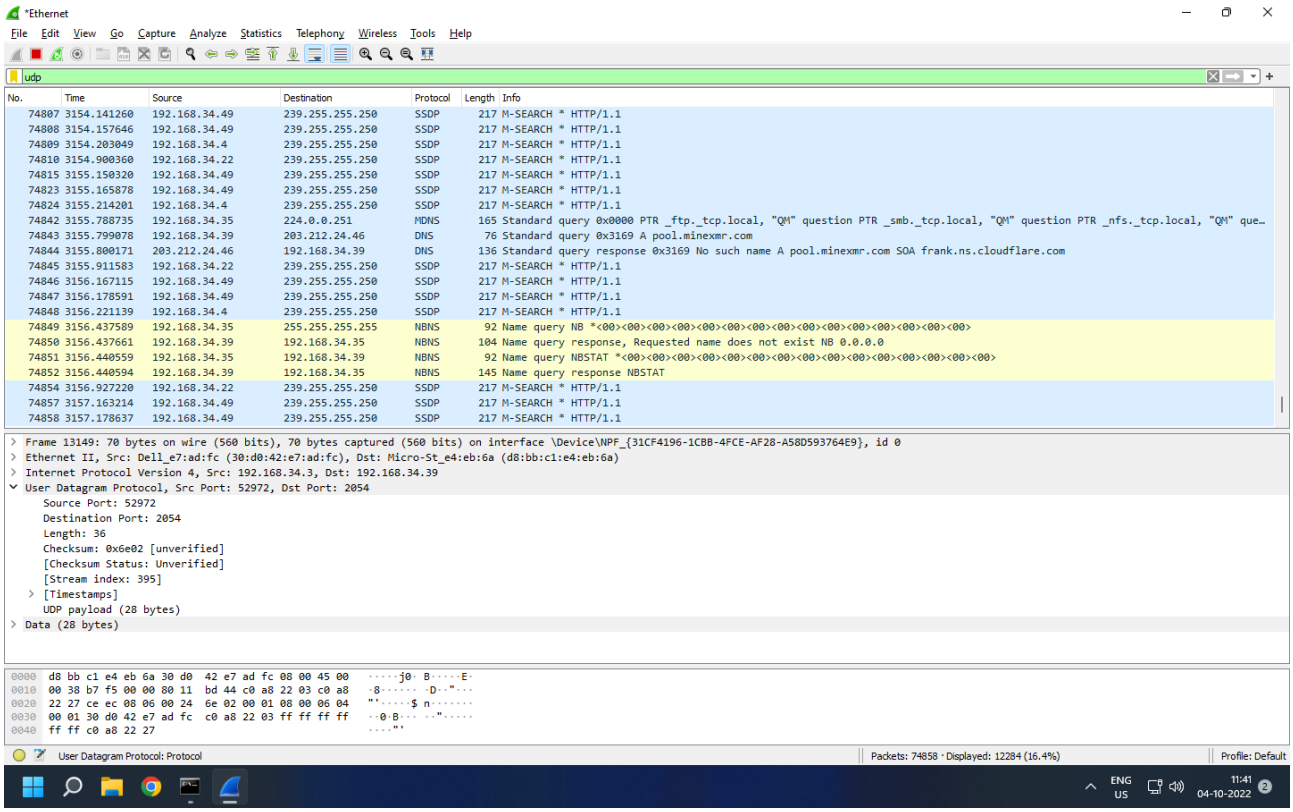
IP:-


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.34.24
No. Time Source Destination Protocol Length Info
13114 511.237072 192.168.34.24 192.168.34.39 ICMP 74 Echo (ping) request id=0x0001, seq=588/19458, ttl=128 (reply in 13115)
13115 511.237148 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=588/19458, ttl=128 (request in 13114)
13116 512.251706 192.168.34.24 192.168.34.39 ICMP 74 Echo (ping) request id=0x0001, seq=589/19714, ttl=128 (reply in 13117)
13117 512.251801 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=589/19714, ttl=128 (request in 13116)
13185 512.894326 192.168.34.24 224.0.0.251 IGMPv2 60 Membership Report group 224.0.0.251
13189 513.269559 192.168.34.24 192.168.34.39 ICMP 74 Echo (ping) request id=0x0001, seq=590/19970, ttl=128 (reply in 13190)
13190 513.269635 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=590/19970, ttl=128 (request in 13189)
13225 514.281569 192.168.34.24 192.168.34.39 ICMP 74 Echo (ping) request id=0x0001, seq=591/20226, ttl=128 (reply in 13226)
13226 514.281650 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=591/20226, ttl=128 (request in 13225)
13264 515.292763 192.168.34.24 192.168.34.39 ICMP 74 Echo (ping) request id=0x0001, seq=592/20482, ttl=128 (reply in 13265)
13265 515.292840 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=592/20482, ttl=128 (request in 13264)
13268 516.301974 192.168.34.24 192.168.34.39 ICMP 74 Echo (ping) request id=0x0001, seq=593/20738, ttl=128 (reply in 13269)
13269 516.302052 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=593/20738, ttl=128 (request in 13268)
13303 517.314075 192.168.34.24 192.168.34.39 ICMP 74 Echo (ping) request id=0x0001, seq=594/20994, ttl=128 (reply in 13304)
13304 517.314157 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=594/20994, ttl=128 (request in 13303)
13339 518.326398 192.168.34.24 192.168.34.39 ICMP 74 Echo (ping) request id=0x0001, seq=595/21250, ttl=128 (reply in 13340)
13340 518.326476 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=595/21250, ttl=128 (request in 13339)
13372 519.341235 192.168.34.24 192.168.34.39 ICMP 74 Echo (ping) request id=0x0001, seq=596/21506, ttl=128 (reply in 13373)
13373 519.341314 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=596/21506, ttl=128 (request in 13372)
13374 520.350246 192.168.34.24 192.168.34.39 ICMP 74 Echo (ping) request id=0x0001, seq=597/21762, ttl=128 (reply in 13375)
13375 520.350343 192.168.34.39 192.168.34.24 ICMP 74 Echo (ping) reply id=0x0001, seq=597/21762, ttl=128 (request in 13374)
Frame 21825: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{31CF4196-1CBB-4FCE-AF28-A58D593764E9}, id 0
Ethernet II, Src: Micro-St_c2:a0:2e (d8:bb:c1:c2:a0:2e), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
Internet Protocol Version 4, Src: 192.168.34.24, Dst: 224.0.0.251
Internet Group Management Protocol
[IGMP Version: 2]
Type: Membership Report (0x16)
Max Resp Time: 0.0 sec (0x00)
Checksum: 0x0904 [correct]
[Checksum Status: Good]
Multicast Address: 224.0.0.251
0000 01 00 5e 00 00 fb d8 bb c1 c2 a0 2e 08 00 46 00
0010 00 20 1e 47 00 00 01 02 42 d5 c0 a8 22 18 e0 00
0020 00 fb 94 04 00 00 16 00 09 04 e0 00 00 fb 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
wireshark_EthernetYBXHT1.pcapng
Packets: 75449 · Displayed: 1153 (1.5%)
Profile: Default
ENG US
11:42
04-10-2022

TCP:-


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
74273 3094.126320 120.138.127.23 192.168.34.39 TCP 1494 443 → 61671 [PSH, ACK] Seq=63024 Ack=946 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
74274 3094.126489 120.138.127.23 192.168.34.39 TCP 1494 443 → 61671 [ACK] Seq=64464 Ack=946 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
74275 3094.126495 192.168.34.39 120.138.127.23 TCP 54 61671 → 443 [ACK] Seq=946 Ack=65904 Win=263424 Len=0
74276 3094.126573 120.138.127.23 192.168.34.39 TCP 1494 443 → 61671 [ACK] Seq=65904 Ack=946 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
74277 3094.126730 120.138.127.23 192.168.34.39 TCP 1494 443 → 61671 [ACK] Seq=67344 Ack=946 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
74278 3094.126734 192.168.34.39 120.138.127.23 TCP 54 61671 → 443 [ACK] Seq=946 Ack=68784 Win=263424 Len=0
74279 3094.126814 120.138.127.23 192.168.34.39 TLSv1.2 1494 Application Data [TCP segment of a reassembled PDU]
74280 3094.126897 120.138.127.23 192.168.34.39 TLSv1.2 1438 Application Data
74281 3094.126905 192.168.34.39 120.138.127.23 TCP 54 61671 → 443 [ACK] Seq=946 Ack=71608 Win=263424 Len=0
74282 3094.173405 192.168.34.39 52.231.199.126 TCP 54 61670 → 443 [ACK] Seq=710 Ack=6878 Win=262656 Len=0
74369 3106.817689 192.168.34.39 117.18.232.240 TCP 66 61672 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
74370 3106.820869 117.18.232.240 192.168.34.39 TCP 66 80 → 61672 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM=1 WS=512
74371 3106.820920 192.168.34.39 117.18.232.240 TCP 54 61672 → 80 [ACK] Seq=1 Ack=1 Win=263424 Len=0
74372 3106.821088 192.168.34.39 117.18.232.240 HTTP 335 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?ea74bb35bfb819ca HTTP/1.1
74373 3106.823226 117.18.232.240 192.168.34.39 TCP 60 80 → 61672 [ACK] Seq=1 Ack=282 Win=67072 Len=0
74374 3106.824776 117.18.232.240 192.168.34.39 HTTP 344 HTTP/1.1 304 Not Modified
74375 3106.829396 192.168.34.39 117.18.232.240 HTTP 341 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?91cf753d760d4dea HTTP/1.1
74376 3106.831470 117.18.232.240 192.168.34.39 TCP 60 80 → 61672 [ACK] Seq=291 Ack=569 Win=68096 Len=0
74377 3106.832280 117.18.232.240 192.168.34.39 HTTP 344 HTTP/1.1 304 Not Modified
74383 3106.883792 192.168.34.39 117.18.232.240 TCP 54 61672 → 80 [ACK] Seq=569 Ack=581 Win=262912 Len=0
74431 3111.402871 52.113.194.132 192.168.34.39 TCP 60 443 → 61664 [RST, ACK] Seq=6051 Ack=1019 Win=0 Len=0
Frame 16699: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{31CF4196-1CBB-4FCE-AF28-A58D593764E9}, id 0
Ethernet II, Src: Micro-St_e4:eb:6a (d8:bb:c1:e4:eb:6a), Dst: Micro-St_c2:9b:e4 (d8:bb:c1:c2:9b:e4)
Internet Protocol Version 6, Src: fe80::1c97:2d89:385:32b8, Dst: fe80::a9ce:af4a:2846:5304
Transmission Control Protocol, Src Port: 61590, Dst Port: 445, Seq: 25443, Ack: 1456328, Len: 0
Source Port: 61590
Destination Port: 445
[Stream index: 12]
[Conversation completeness: Complete, WITH_DATA (47)]
[TCP Segment Len: 0]
Sequence Number: 25443 (relative sequence number)
Sequence Number (raw): 2789968545
[Next Sequence Number: 25443 (relative sequence number)]
Acknowledgment Number: 1456328 (relative ack number)
Acknowledgment number (raw): 2985725973
0101 .... = Header Length: 20 bytes (5)
0000 d8 bb c1 c2 9b e4 d8 bb c1 e4 eb 6a 86 dd 60 0b
0010 b4 05 00 14 06 80 fe 80 00 00 00 00 00 00 1c 97
0020 2d 89 03 85 32 b8 fe 80 00 00 00 00 00 00 a9 ce
0030 af 4a 28 46 53 04 f0 96 01 bd a6 4b 8a a1 b1 f6
0040 90 15 50 10 04 03 51 dd 00 00
Transmission Control Protocol: Protocol
Packets: 74433 · Displayed: 36061 (48.4%)
Profile: Default
ENG US
11:40
04-10-2022

UDP:-


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
No. Time Source Destination Protocol Length Info
74807 3154.141260 192.168.34.49 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
74808 3154.157646 192.168.34.49 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
74809 3154.203049 192.168.34.4 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
74810 3154.900360 192.168.34.22 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
74815 3155.150320 192.168.34.49 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
74823 3155.165878 192.168.34.49 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
74824 3155.214201 192.168.34.4 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
74842 3155.788735 192.168.34.35 224.0.0.251 MDNS 165 Standard query 0x0000 PTR _ftp._tcp.local, "QM" question PTR _smb._tcp.local, "QM" question PTR _nfs._tcp.local, "QM" que…
74843 3155.799078 192.168.34.39 203.212.24.46 DNS 76 Standard query 0x3169 A pool.minexmr.com
74844 3155.800171 203.212.24.46 192.168.34.39 DNS 136 Standard query response 0x3169 No such name A pool.minexmr.com SOA frank.ns.cloudflare.com
74845 3155.911583 192.168.34.22 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
74846 3156.167115 192.168.34.49 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
74847 3156.178591 192.168.34.49 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
74848 3156.221139 192.168.34.4 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
74849 3156.437589 192.168.34.35 255.255.255.255 NBNS 92 Name query NB *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
74850 3156.437661 192.168.34.39 192.168.34.35 NBNS 104 Name query response, Requested name does not exist NB 0.0.0.0
74851 3156.440559 192.168.34.35 192.168.34.39 NBNS 92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
74852 3156.440594 192.168.34.39 192.168.34.35 NBNS 145 Name query response NBSTAT
74854 3156.927220 192.168.34.22 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
74857 3157.163214 192.168.34.49 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
74858 3157.178637 192.168.34.49 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
Frame 13149: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{31CF4196-1CBB-4FCE-AF28-A58D593764E9}, id 0
Ethernet II, Src: Dell_e7:ad:fc (30:d0:42:e7:ad:fc), Dst: Micro-St_e4:eb:6a (d8:bb:c1:e4:eb:6a)
Internet Protocol Version 4, Src: 192.168.34.3, Dst: 192.168.34.39
User Datagram Protocol, Src Port: 52972, Dst Port: 2054
Source Port: 52972
Destination Port: 2054
Length: 36
Checksum: 0x6e02 [unverified]
[Checksum Status: Unverified]
[Stream index: 395]
[Timestamps]
UDP payload (28 bytes)
Data (28 bytes)
0000 d8 bb c1 e4 eb 6a 30 d0 42 e7 ad fc 08 00 45 00
0010 00 38 b7 f5 00 00 80 11 bd 44 c0 a8 22 03 c0 a8
0020 22 27 ce ec 08 06 00 24 6e 02 00 01 08 00 06 04
0030 00 01 30 d0 42 e7 ad fc c0 a8 22 03 ff ff ff ff
0040 ff ff c0 a8 22 27
User Datagram Protocol: Protocol
Packets: 74858 · Displayed: 12284 (16.4%)
Profile: Default
ENG US
11:41
04-10-2022