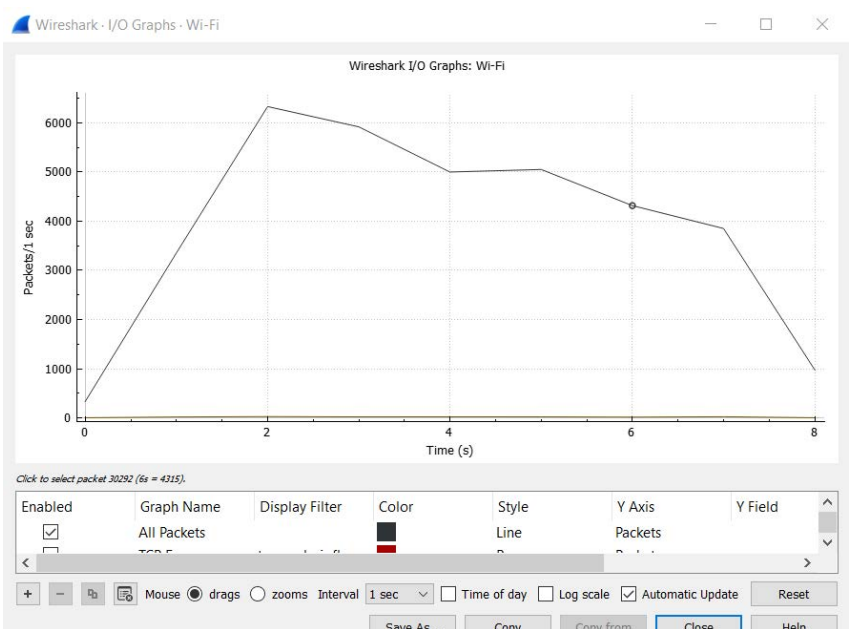


Wireshark packet list table showing network traffic details including No., Time, Source, Destination, Protocol, Length, and Info.

Frame 2214: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits) on interface \Device\NPF... Ethernet II, Src: IntelCor\_f2:42:a2 (c8:b2:9b:f2:42:a2), Dst: All-HSRP-routers\_31 (00:00:0c:07:ac:25)

Hypertext Transfer Protocol

Wireshark I/O Graphs - Wi-Fi



Frame 2214: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits) on interface \Device\NPF... Interface id: 0 (Device NPF\_{IDB9E288-86E7-46E8-A0A9-C62914CE7C8E}) Encapsulation type: Ethernet (1) Arrival Time: Jul 30, 2022 14:22:14.190069000 India Standard Time [Time shift for this packet: 0.000000000 seconds] Epoch Time: 1659171194.190069000 seconds [Time delta from previous captured frame: 0.000616000 seconds] [Time delta from previous displayed frame: 0.000616000 seconds] [Time since reference or first frame: 1.817861000 seconds] Frame Number: 2214 Frame Length: 487 bytes (3896 bits) Capture Length: 487 bytes (3896 bits) [Frame is marked: False] [Frame is ignored: False] [Protocols in frame: eth:ethertype:ip:tcp:http] [Coloring Rule Name: HTTP] [Coloring Rule String: http || tcp.port == 80 || http2] Ethernet II, Src: IntelCor\_f2:42:a2 (c8:b2:9b:f2:42:a2), Dst: All-HSRP-routers\_31 (00:00:0c:07:ac:31) Destination: All-HSRP-routers\_31 (00:00:0c:07:ac:31) Source: IntelCor\_f2:42:a2 (c8:b2:9b:f2:42:a2) Type: IPv4 (0x0800) Internet Protocol Version 4, Src: 10.5.33.243, Dst: 8.255.130.254 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 473 Identification: 0x4348 (17224) > Flags: 0x40, Don't fragment ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 128 Protocol: TCP (6) Header Checksum: 0x0000 [validation disabled] [Header checksum status: Unverified] Source Address: 10.5.33.243 Destination Address: 8.255.130.254 Transmission Control Protocol, Src Port: 51017, Dst Port: 80, Seq: 418, Ack: 919, Len: 433 Source Port: 51017 Seq: 418 Len: 433, Connection: Keep-Alive\r\n Accept: \*/\*\r\n Range: bytes=292814848-293076991\r\n User-Agent: Microsoft-Delivery-Optimization/10.0\r\n MS-CV: 6a8/bKLPkaSJCVE.1.1.33.90.7.10.1.2\r\n Content-Length: 0\r\n Host: tlu.dl.delivery.mp.microsoft.com\r\n\r\n [Full request URI [truncated]: http://tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/c3352b3e-dbb3-450c-a243-795700e29fdb?P1=16591799858P2=404&P3=16591799858P4=16591799858P5=16591799858P6=16591799858P7=16591799858P8=16591799858P9=16591799858P10=16591799858P11=16591799858P12=16591799858P13=16591799858P14=16591799858P15=16591799858P16=16591799858P17=16591799858P18=16591799858P19=16591799858P20=16591799858P21=16591799858P22=16591799858P23=16591799858P24=16591799858P25=16591799858P26=16591799858P27=16591799858P28=16591799858P29=16591799858P30=16591799858P31=16591799858P32=16591799858P33=16591799858P34=16591799858P35=16591799858P36=16591799858P37=16591799858P38=16591799858P39=16591799858P40=16591799858P41=16591799858P42=16591799858P43=16591799858P44=16591799858P45=16591799858P46=16591799858P47=16591799858P48=16591799858P49=16591799858P50=16591799858P51=16591799858P52=16591799858P53=16591799858P54=16591799858P55=16591799858P56=16591799858P57=16591799858P58=16591799858P59=16591799858P60=16591799858P61=16591799858P62=16591799858P63=16591799858P64=16591799858P65=16591799858P66=16591799858P67=16591799858P68=16591799858P69=16591799858P70=16591799858P71=16591799858P72=16591799858P73=16591799858P74=16591799858P75=16591799858P76=16591799858P77=16591799858P78=16591799858P79=16591799858P80=16591799858P81=16591799858P82=16591799858P83=16591799858P84=16591799858P85=16591799858P86=16591799858P87=16591799858P88=16591799858P89=16591799858P90=16591799858P91=16591799858P92=16591799858P93=16591799858P94=16591799858P95=16591799858P96=16591799858P97=16591799858P98=16591799858P99=16591799858P100=16591799858P101=16591799858P102=16591799858P103=16591799858P104=16591799858P105=16591799858P106=16591799858P107=16591799858P108=16591799858P109=16591799858P110=16591799858P111=16591799858P112=16591799858P113=16591799858P114=16591799858P115=16591799858P116=16591799858P117=16591799858P118=16591799858P119=16591799858P120=16591799858P121=16591799858P122=16591799858P123=16591799858P124=16591799858P125=16591799858P126=16591799858P127=16591799858P128=16591799858P129=16591799858P130=16591799858P131=16591799858P132=16591799858P133=16591799858P134=16591799858P135=16591799858P136=16591799858P137=16591799858P138=16591799858P139=16591799858P140=16591799858P141=16591799858P142=16591799858P143=16591799858P144=16591799858P145=16591799858P146=16591799858P147=16591799858P148=16591799858P149=16591799858P150=16591799858P151=16591799858P152=16591799858P153=16591799858P154=16591799858P155=16591799858P156=16591799858P157=16591799858P158=16591799858P159=16591799858P160=16591799858P161=16591799858P162=16591799858P163=16591799858P164=16591799858P165=16591799858P166=16591799858P167=16591799858P168=16591799858P169=16591799858P170=16591799858P171=16591799858P172=16591799858P173=16591799858P174=16591799858P175=16591799858P176=16591799858P177=16591799858P178=16591799858P179=16591799858P180=16591799858P181=16591799858P182=16591799858P183=16591799858P184=16591799858P185=16591799858P186=16591799858P187=16591799858P188=16591799858P189=16591799858P190=16591799858P191=16591799858P192=16591799858P193=16591799858P194=16591799858P195=16591799858P196=16591799858P197=16591799858P198=16591799858P199=16591799858P200=16591799858P201=16591799858P202=16591799858P203=16591799858P204=16591799858P205=16591799858P206=16591799858P207=16591799858P208=16591799858P209=16591799858P210=16591799858P211=16591799858P212=16591799858P213=16591799858P214=16591799858P215=16591799858P216=16591799858P217=16591799858P218=16591799858P219=16591799858P220=16591799858P221=16591799858P222=16591799858P223=16591799858P224=16591799858P225=16591799858P226=16591799858P227=16591799858P228=16591799858P229=16591799858P230=16591799858P231=16591799858P232=16591799858P233=16591799858P234=16591799858P235=16591799858P236=16591799858P237=16591799858P238=16591799858P239=16591799858P240=16591799858P241=16591799858P242=16591799858P243=16591799858P244=16591799858P245=16591799858P246=16591799858P247=16591799858P248=16591799858P249=16591799858P250=16591799858P251=16591799858P252=16591799858P253=16591799858P254=16591799858P255=16591799858P256=16591799858P257=16591799858P258=16591799858P259=16591799858P260=16591799858P261=16591799858P262=16591799858P263=16591799858P264=16591799858P265=16591799858P266=16591799858P267=16591799858P268=16591799858P269=16591799858P270=16591799858P271=16591799858P272=16591799858P273=16591799858P274=16591799858P275=16591799858P276=16591799858P277=16591799858P278=16591799858P279=16591799858P280=16591799858P281=16591799858P282=16591799858P283=16591799858P284=16591799858P285=16591799858P286=16591799858P287=16591799858P288=16591799858P289=16591799858P290=16591799858P291=16591799858P292=16591799858P293=16591799858P294=16591799858P295=16591799858P296=16591799858P297=16591799858P298=16591799858P299=16591799858P300=16591799858P301=16591799858P302=16591799858P303=16591799858P304=16591799858P305=16591799858P306=16591799858P307=16591799858P308=16591799858P309=16591799858P310=16591799858P311=16591799858P312=16591799858P313=16591799858P314=16591799858P315=16591799858P316=16591799858P317=16591799858P318=16591799858P319=16591799858P320=16591799858P321=16591799858P322=16591799858P323=16591799858P324=16591799858P325=16591799858P326=16591799858P327=16591799858P328=16591799858P329=16591799858P330=16591799858P331=16591799858P332=16591799858P333=16591799858P334=16591799858P335=16591799858P336=16591799858P337=16591799858P338=16591799858P339=16591799858P340=16591799858P341=16591799858P342=16591799858P343=16591799858P344=16591799858P345=16591799858P346=16591799858P347=16591799858P348=16591799858P349=16591799858P350=16591799858P351=16591799858P352=16591799858P353=16591799858P354=16591799858P355=16591799858P356=16591799858P357=16591799858P358=16591799858P359=16591799858P360=16591799858P361=16591799858P362=16591799858P363=16591799858P364=16591799858P365=16591799858P366=16591799858P367=16591799858P368=16591799858P369=16591799858P370=16591799858P371=16591799858P372=16591799858P373=16591799858P374=16591799858P375=16591799858P376=16591799858P377=16591799858P378=16591799858P379=16591799858P380=16591799858P381=16591799858P382=16591799858P383=16591799858P384=16591799858P385=16591799858P386=16591799858P387=16591799858P388=16591799858P389=16591799858P390=16591799858P391=16591799858P392=16591799858P393=16591799858P394=16591799858P395=16591799858P396=16591799858P397=16591799858P398=16591799858P399=16591799858P400=16591799858P401=16591799858P402=16591799858P403=16591799858P404=16591799858P405=16591799858P406=16591799858P407=16591799858P408=16591799858P409=16591799858P410=16591799858P411=16591799858P412=16591799858P413=16591799858P414=16591799858P415=16591799858P416=16591799858P417=16591799858P418=16591799858P419=16591799858P420=16591799858P421=16591799858P422=16591799858P423=16591799858P424=16591799858P425=16591799858P426=16591799858P427=16591799858P428=16591799858P429=16591799858P430=16591799858P431=16591799858P432=16591799858P433=16591799858P434=16591799858P435=16591799858P436=16591799858P437=16591799858P438=16591799858P439=16591799858P440=16591799858P441=16591799858P442=16591799858P443=16591799858P444=16591799858P445=16591799858P446=16591799858P447=16591799858P448=16591799858P449=16591799858P450=16591799858P451=16591799858P452=16591799858P453=16591799858P454=16591799858P455=16591799858P456=16591799858P457=16591799858P458=16591799858P459=16591799858P460=16591799858P461=16591799858P462=16591799858P463=16591799858P464=16591799858P465=16591799858P466=16591799858P467=16591799858P468=16591799858P469=16591799858P470=16591799858P471=16591799858P472=16591799858P473=16591799858P474=16591799858P475=16591799858P476=16591799858P477=16591799858P478=16591799858P479=16591799858P480=16591799858P481=16591799858P482=16591799858P483=16591799858P484=16591799858P485=16591799858P486=16591799858P487=16591799858P488=16591799858P489=16591799858P490=16591799858P491=16591799858P492=16591799858P493=16591799858P494=16591799858P495=16591799858P496=16591799858P497=16591799858P498=16591799858P499=16591799858P500=16591799858P501=16591799858P502=16591799858P503=16591799858P504=16591799858P505=16591799858P506=16591799858P507=16591799858P508=16591799858P509=16591799858P510=16591799858P511=16591799858P512=16591799858P513=16591799858P514=16591799858P515=16591799858P516=16591799858P517=16591799858P518=16591799858P519=16591799858P520=16591799858P521=16591799858P522=16591799858P523=16591799858P524=16591799858P525=16591799858P526=16591799858P527=16591799858P528=16591799858P529=16591799858P530=16591799858P531=16591799858P532=16591799858P533=16591799858P534=16591799858P535=16591799858P536=16591799858P537=16591799858P538=16591799858P539=16591799858P540=16591799858P541=16591799858P542=16591799858P543=16591799858P544=16591799858P545=16591799858P546=16591799858P547=16591799858P548=16591799858P549=16591799858P550=16591799858P551=16591799858P552=16591799858P553=16591799858P554=16591799858P555=16591799858P556=16591799858P557=16591799858P558=16591799858P559=16591799858P560=16591799858P561=16591799858P562=16591799858P563=16591799858P564=16591799858P565=16591799858P566=16591799858P567=16591799858P568=16591799858P569=16591799858P570=16591799858P571=16591799858P572=16591799858P573=16591799858P574=16591799858P575=16591799858P576=16591799858P577=16591799858P578=16591799858P579=16591799858P580=16591799858P581=16591799858P582=16591799858P583=16591799858P584=16591799858P585=16591799858P586=16591799858P587=16591799858P588=16591799858P589=16591799858P590=16591799858P591=16591799858P592=16591799858P593=16591799858P594=16591799858P595=16591799858P596=16591799858P597=16591799858P598=16591799858P599=16591799858P600=16591799858P601=16591799858P602=16591799858P603=16591799858P604=16591799858P605=16591799858P606=16591799858P607=16591799858P608=16591799858P609=16591799858P610=16591799858P611=16591799858P612=16591799858P613=16591799858P614=16591799858P615=16591799858P616=16591799858P617=16591799858P618=16591799858P619=16591799858P620=16591799858P621=16591799858P622=16591799858P623=16591799858P624=16591799858P625=16591799858P626=16591799858P627=16591799858P628=16591799858P629=16591799858P630=16591799858P631=16591799858P632=16591799858P633=16591799858P634=16591799858P635=16591799858P636=16591799858P637=16591799858P638=16591799858P639=16591799858P640=16591799858P641=16591799858P642=16591799858P643=16591799858P644=16591799858P645=16591799858P646=16591799858P647=16591799858P648=16591799858P649=16591799858P650=16591799858P651=16591799858P652=16591799858P653=16591799858P654=16591799858P655=16591799858P656=16591799858P657=16591799858P658=16591799858P659=16591799858P660=16591799858P661=16591799858P662=16591799858P663=16591799858P664=16591799858P665=16591799858P666=16591799858P667=16591799858P668=16591799858P669=16591799858P670=16591799858P671=16591799858P672=16591799858P673=16591799858P674=16591799858P675=16591799858P676=16591799858P677=16591799858P678=16591799858P679=16591799858P680=16591799858P681=16591799858P682=16591799858P683=16591799858P684=16591799858P685=16591799858P686=16591799858P687=16591799858P688=16591799858P689=16591799858P690=16591799858P691=16591799858P692=165917998



Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

| No. | Time     | Source         | Destination    | Protocol | Length | Info                   |
|-----|----------|----------------|----------------|----------|--------|------------------------|
| 5   | 0.150297 | 10.5.33.243    | 20.198.118.190 | TLSv1.2  | 153    | Application Data       |
| 21  | 0.213415 | 20.198.118.190 | 10.5.33.243    | TLSv1.2  | 223    | Application Data       |
| 23  | 0.215150 | 10.5.33.243    | 13.107.4.52    | TCP      | 66     | 51014 → 80 [SYN] Seq=  |
| 24  | 0.220144 | 10.5.33.243    | 8.8.8.8        | TCP      | 66     | 51013 → 53 [SYN] Seq=  |
| 25  | 0.249284 | 8.8.8.8        | 10.5.33.243    | TCP      | 66     | 53 → 51013 [SYN, ACK]  |
| 26  | 0.249284 | 13.107.4.52    | 10.5.33.243    | TCP      | 66     | 80 → 51014 [SYN, ACK]  |
| 27  | 0.249360 | 10.5.33.243    | 8.8.8.8        | TCP      | 54     | 51013 → 53 [ACK] Seq=  |
| 28  | 0.249465 | 10.5.33.243    | 13.107.4.52    | TCP      | 54     | 51014 → 80 [ACK] Seq=  |
| 29  | 0.249467 | 10.5.33.243    | 8.8.8.8        | DNS      | 90     | Standard query 0x0000  |
| 30  | 0.249753 | 10.5.33.243    | 13.107.4.52    | HTTP     | 208    | GET /connecttest.txt   |
| 31  | 0.267241 | 10.5.33.243    | 20.198.118.190 | TCP      | 54     | 53253 → 443 [ACK] Seq= |
| 32  | 0.278086 | 8.8.8.8        | 10.5.33.243    | TCP      | 60     | 53 → 51013 [ACK] Seq=  |
| 33  | 0.282498 | 8.8.8.8        | 10.5.33.243    | DNS      | 106    | Standard query respon  |
| 34  | 0.282498 | 13.107.4.52    | 10.5.33.243    | TCP      | 60     | 80 → 51014 [ACK] Seq=  |
| 35  | 0.283096 | 10.5.33.243    | 8.8.8.8        | TCP      | 54     | 51013 → 53 [FIN, ACK]  |
| 36  | 0.285066 | 13.107.4.52    | 10.5.33.243    | HTTP     | 593    | HTTP/1.1 200 OK (tex   |
| 37  | 0.285066 | 13.107.4.52    | 10.5.33.243    | TCP      | 60     | 80 → 51014 [FIN, ACK]  |
| 38  | 0.285233 | 10.5.33.243    | 13.107.4.52    | TCP      | 54     | 51014 → 80 [ACK] Seq=  |
| 39  | 0.285277 | 10.5.33.243    | 13.107.4.52    | TCP      | 54     | 51014 → 80 [FIN, ACK]  |
| 40  | 0.311593 | 8.8.8.8        | 10.5.33.243    | TCP      | 60     | 53 → 51013 [FIN, ACK]  |
| 41  | 0.311635 | 10.5.33.243    | 8.8.8.8        | TCP      | 54     | 51013 → 53 [ACK] Seq=  |
| 42  | 0.317767 | 13.107.4.52    | 10.5.33.243    | TCP      | 60     | 80 → 51014 [ACK] Seq=  |
| 46  | 0.621051 | 10.5.33.243    | 8.255.130.254  | TCP      | 66     | 59574 → 80 [SYN] Seq=  |
| 47  | 0.684008 | 8.255.130.254  | 10.5.33.243    | TCP      | 66     | 80 → 59574 [SYN, ACK]  |
| 48  | 0.684079 | 10.5.33.243    | 8.255.130.254  | TCP      | 54     | 59574 → 80 [ACK] Seq=  |
| 49  | 0.684242 | 10.5.33.243    | 8.255.130.254  | HTTP     | 471    | GET /filestreamingser  |
| 50  | 0.761821 | 8.255.130.254  | 10.5.33.243    | HTTP     | 971    | HTTP/1.1 206 Partial   |
| 51  | 0.762598 | 10.5.33.243    | 8.255.130.254  | HTTP     | 487    | GET /filestreamingser  |
| 52  | 0.835361 | 8.255.130.254  | 10.5.33.243    | TCP      | 1440   | 80 → 59574 [PSH, ACK]  |
| 53  | 0.835361 | 8.255.130.254  | 10.5.33.243    | TCP      | 1440   | 80 → 59574 [PSH, ACK]  |
| 54  | 0.835361 | 10.5.33.243    | 8.255.130.254  | TCP      | 54     | 59574 → 80 [ACK] Seq=  |

< >

> Frame 5: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface \Device\NPF\_{1DB9E2B8-86E7-46E8-A0A9-C62914CE7CBE}

> Ethernet II, Src: IntelCor\_f2:42:a2 (c8:b2:9b:f2:42:a2), Dst: All-HSRP-routers\_31 (00:00:0c:07:ac:31)

> Internet Protocol Version 4, Src: 10.5.33.243, Dst: 20.198.118.190

> Transmission Control Protocol, Src Port: 53253, Dst Port: 443, Seq: 1, Ack: 1, Len: 99

> Transport Layer Security

< >

Transmission Control Protocol: Protocol | Packets: 35120 · Displayed: 35036 (99.8%) · Dropped: 0 (0.0%) | Profile: Default

Frame 5: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface \Device\NPF\_{1DB9E2B8-86E7-46E8-A0A9-C62914CE7CBE}

> Interface id: 0 (\Device\NPF\_{1DB9E2B8-86E7-46E8-A0A9-C62914CE7CBE})

Encapsulation type: Ethernet (1)

Arrival Time: Jul 30, 2022 14:23:12.522505000 India Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1659171192.522505000 seconds

[Time delta from previous captured frame: 0.000066000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 0.150297000 seconds]

Frame Number: 5

Frame Length: 153 bytes (1224 bits)

Capture Length: 153 bytes (1224 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:tls]

[Coloring Rule Name: TCP]

[Coloring Rule String: tcp]

> Ethernet II, Src: IntelCor\_f2:42:a2 (c8:b2:9b:f2:42:a2), Dst: All-HSRP-routers\_31 (00:00:0c:07:ac:31)

> Destination: All-HSRP-routers\_31 (00:00:0c:07:ac:31)

> Source: IntelCor\_f2:42:a2 (c8:b2:9b:f2:42:a2)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 10.5.33.243, Dst: 20.198.118.190

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 139

Identification: 0x68ab (26795)

> Flags: 0x40, Don't fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

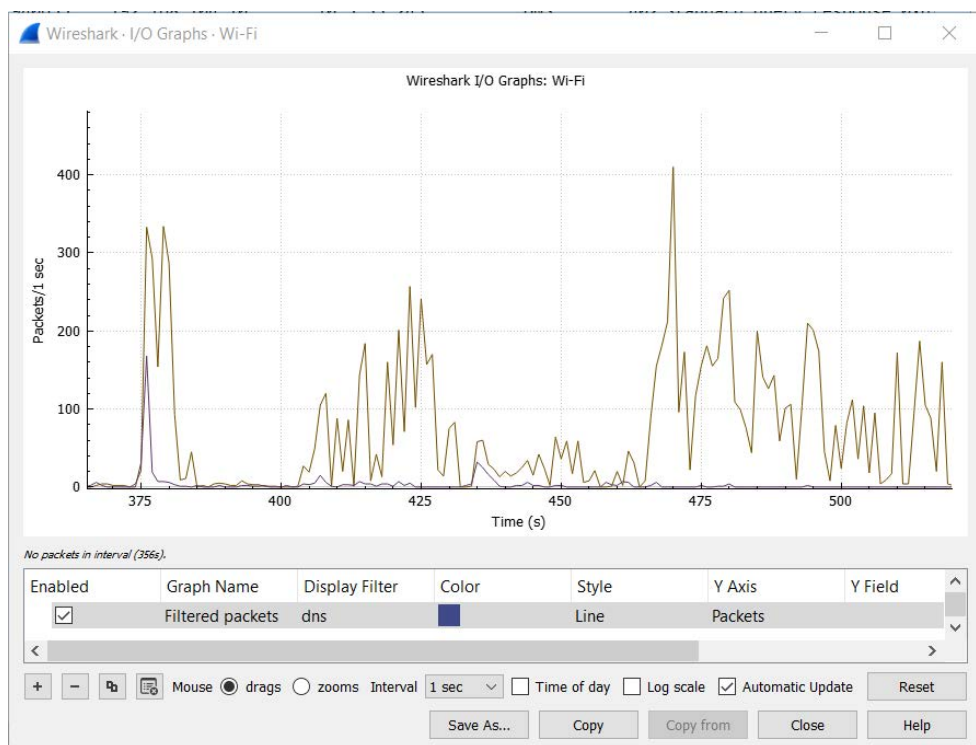
Protocol: TCP (6)

Header Checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source Address: 10.5.33.243

Destination Address: 20.198.118.190





Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

| No.     | Time       | Source         | Destination    | Protocol | Length | Info                             |
|---------|------------|----------------|----------------|----------|--------|----------------------------------|
| 1571... | 758.459214 | 192.168.104.10 | 10.5.33.243    | DNS      | 326    | Standard query response 0x594b A |
| 1571... | 758.452825 | 10.5.33.243    | 192.168.104.10 | DNS      | 92     | Standard query 0x594b A mobile.e |
| 1491... | 743.185885 | 192.168.104.10 | 10.5.33.243    | DNS      | 146    | Standard query response 0x6c10 M |
| 1491... | 743.121757 | 10.5.33.243    | 192.168.104.10 | DNS      | 71     | Standard query 0x6c10 A wpad.dhc |
| 1460... | 737.069796 | 192.168.104.10 | 10.5.33.243    | DNS      | 336    | Standard query response 0x4f6a A |
| 1460... | 737.063441 | 10.5.33.243    | 192.168.104.10 | DNS      | 86     | Standard query 0x4f6a A checkapp |
| 1444... | 734.051329 | 192.168.104.10 | 10.5.33.243    | DNS      | 146    | Standard query response 0xb739 M |
| 1444... | 733.982982 | 10.5.33.243    | 192.168.104.10 | DNS      | 71     | Standard query 0xb739 A wpad.dhc |
| 1444... | 733.980457 | 192.168.104.10 | 10.5.33.243    | DNS      | 112    | Standard query response 0x10c2 A |
| 1444... | 733.978136 | 10.5.33.243    | 192.168.104.10 | DNS      | 70     | Standard query 0x10c2 A dns.goog |
| 1324... | 713.025359 | 192.168.104.10 | 10.5.33.243    | DNS      | 332    | Standard query response 0x15a3 A |
| 1324... | 713.017875 | 10.5.33.243    | 192.168.104.10 | DNS      | 92     | Standard query 0x15a3 A mobile.e |
| 1218... | 692.878361 | 192.168.104.10 | 10.5.33.243    | DNS      | 336    | Standard query response 0x37f4 A |
| 1218... | 692.855946 | 10.5.33.243    | 192.168.104.10 | DNS      | 92     | Standard query 0x37f4 A mobile.e |
| 1055... | 663.099809 | 192.168.104.10 | 10.5.33.243    | DNS      | 236    | Standard query response 0x018f A |
| 1055... | 663.095508 | 10.5.33.243    | 192.168.104.10 | DNS      | 103    | Standard query 0x018f A img-proc |
| 1050... | 662.110099 | 8.8.8.8        | 10.5.33.243    | DNS      | 182    | Standard query response 0xd6b2 A |
| 1050... | 662.080986 | 192.168.104.10 | 10.5.33.243    | DNS      | 272    | Standard query response 0xd6b2 A |
| 1050... | 662.042661 | 10.5.33.243    | 8.8.8.8        | DNS      | 71     | Standard query 0xd6b2 A arc.msn. |
| 1049... | 662.016407 | 10.5.33.243    | 192.168.104.10 | DNS      | 71     | Standard query 0xd6b2 A arc.msn. |
| 1041... | 660.382032 | 192.168.104.10 | 10.5.33.243    | DNS      | 398    | Standard query response 0x8b7d A |
| 1041... | 660.375835 | 10.5.33.243    | 192.168.104.10 | DNS      | 85     | Standard query 0x8b7d A login.mi |
| 8774... | 629.015752 | 192.168.104.10 | 10.5.33.243    | DNS      | 336    | Standard query response 0x2131 A |
| 8774... | 629.011200 | 10.5.33.243    | 192.168.104.10 | DNS      | 92     | Standard query 0x2131 A mobile.e |
| 7936... | 613.181491 | 192.168.104.10 | 10.5.33.243    | DNS      | 146    | Standard query response 0xd710 M |
| 7933... | 613.119376 | 10.5.33.243    | 192.168.104.10 | DNS      | 71     | Standard query 0xd710 A wpad.dhc |
| 7694... | 608.413550 | 192.168.104.10 | 10.5.33.243    | DNS      | 108    | Standard query response 0x9e72 A |
| 7694... | 608.408871 | 10.5.33.243    | 192.168.104.10 | DNS      | 76     | Standard query 0x9e72 A dns.msft |
| 7522... | 605.072368 | 192.168.104.10 | 10.5.33.243    | DNS      | 352    | Standard query response 0xbd46 A |
| 7521... | 605.046403 | 10.5.33.243    | 192.168.104.10 | DNS      | 94     | Standard query 0xbd46 A umuafce  |

< >

> Frame 316200: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface \Device\NPF\_{1DB9E2B8-86E7-46E8-A0A9-C62914CE7CBE}

> Ethernet II, Src: Cisco\_b0:95:41 (70:6b:b9:b0:95:41), Dst: IntelCor\_f2:42:a2 (c8:b2:9b:f2:42:a2)

> Internet Protocol Version 4, Src: 192.168.104.10, Dst: 10.5.33.243

> User Datagram Protocol, Src Port: 53, Dst Port: 63716

> Domain Name System (response)

< >

Domain Name System: Protocol

Packets: 1604695 · Displayed: 732 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

Frame 316200: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface \Device\NPF\_{1DB9E2B8-86E7-46E8-A0A9-C62914CE7CBE}

Interface id: 0 (\Device\NPF\_{1DB9E2B8-86E7-46E8-A0A9-C62914CE7CBE})

Encapsulation type: Ethernet (1)

Arrival Time: Jul 30, 2022 14:11:55.156914000 India Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1659170515.156914000 seconds

[Time delta from previous captured frame: 0.002043000 seconds]

[Time delta from previous displayed frame: 0.087761000 seconds]

[Time since reference or first frame: 475.424452000 seconds]

Frame Number: 316200

Frame Length: 146 bytes (1168 bits)

Capture Length: 146 bytes (1168 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:udp:dns]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

Ethernet II, Src: Cisco\_b0:95:41 (70:6b:b9:b0:95:41), Dst: IntelCor\_f2:42:a2 (c8:b2:9b:f2:42:a2)

Destination: IntelCor\_f2:42:a2 (c8:b2:9b:f2:42:a2)

Source: Cisco\_b0:95:41 (70:6b:b9:b0:95:41)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.104.10, Dst: 10.5.33.243

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 132

Identification: 0x3e0b (15883)

Flags: 0x40, Don't fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 63

Protocol: UDP (17)

Header Checksum: 0xa8b3 [validation disabled]

[Header checksum status: Unverified]

User Datagram Protocol, Src Port: 53, Dst Port: 63716

Source Port: 53

Destination Port: 63716

Length: 112

Checksum: 0x55b4 [unverified]

[Checksum Status: Unverified]

[Stream index: 273]

[Timestamps]

UDP payload (104 bytes)

Domain Name System (response)

Transaction ID: 0x6e5d

Flags: 0x8183 Standard query response, No such name

Questions: 1

Answer RRs: 0

Authority RRs: 1

Additional RRs: 0

Queries

Authoritative nameservers

[Request In: 315882]

[Time: 0.087761000 seconds]

< >

Domain Name System: Protocol

Packets: 1604695 · Displayed: 732 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp contains kiit

| No. | Time     | Source        | Destination   | Protocol | Length | Info         |
|-----|----------|---------------|---------------|----------|--------|--------------|
| 85  | 5.012856 | 10.5.33.243   | 34.93.223.163 | TLSv1.2  | 571    | Client Hello |
| 86  | 5.013112 | 10.5.33.243   | 34.93.223.163 | TLSv1.2  | 571    | Client Hello |
| 99  | 5.439186 | 10.5.33.243   | 34.93.223.163 | TLSv1.2  | 571    | Client Hello |
| 120 | 5.734030 | 34.93.223.163 | 10.5.33.243   | TLSv1.2  | 1440   | Server Hello |
| 125 | 5.747685 | 34.93.223.163 | 10.5.33.243   | TLSv1.2  | 1440   | Server Hello |
| 135 | 5.954061 | 34.93.223.163 | 10.5.33.243   | TLSv1.2  | 1440   | Server Hello |
| 152 | 6.218623 | 10.5.33.243   | 34.93.223.163 | TLSv1.2  | 571    | Client Hello |
| 160 | 6.226094 | 10.5.33.243   | 34.93.223.163 | TLSv1.2  | 571    | Client Hello |
| 166 | 6.420485 | 34.93.223.163 | 10.5.33.243   | TLSv1.2  | 1440   | Server Hello |

Server Name list length: 32  
Server Name Type: host\_name (0)  
Server Name length: 29  
Server Name: kiitportal.kiituniversity.net  
Extension: extended\_master\_secret (len=0)

00b0 00 20 00 00 1d 6b 69 69 74 70 6f 72 74 61 6c 2e .....kiitportal.  
00c0 6b 69 69 74 75 6e 69 76 65 72 73 69 74 79 2e 6e .....kiituniversity.n  
00d0 65 74 00 17 00 00 ff 01 00 01 00 00 0a 00 0a 00 .....et  
00e0 08 ea ea 0d 1d 00 17 00 18 00 0b 00 02 01 00 00 .....  
00f0 23 00 00 00 10 00 0e 00 0c 02 68 32 08 68 74 74 .....# .....h2-htt  
0100 70 2f 31 2e 31 00 05 00 05 01 00 00 00 00 0d .....p/1.1 .....  
0110 00 12 00 10 04 03 08 04 04 01 05 03 08 05 05 01 .....  
0120 08 06 06 01 00 12 00 00 00 33 00 2b 00 29 ea ea .....-3+.) .....  
0130 00 01 00 00 1d 00 20 ee 61 72 b8 b2 60 7b c7 87 .....ar-{} .....  
0140 75 6a c0 14 a1 90 8a 6d df a1 5d 0d fa 25 6d 03 .....uj-...m-]-.%m-  
0150 0f b6 54 3d 0d a3 21 00 2d 00 02 01 01 00 2b 00 .....-T-...!- .....+  
0160 07 06 5a 5a 03 04 03 03 00 1b 00 03 02 00 02 44 .....-ZZ- .....D  
0170 69 00 05 00 03 02 68 32 da da 00 01 00 00 15 00 .....i .....h2 .....  
0180 ba 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
Bytes 181-209: Server Name (tls.handshake.extensions\_server\_name) | Packets: 5642 · Displayed: 11 (0.2%) · Dropped: 0 (0.0%) | Profile: Default

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp contains facebook

| No.   | Time       | Source      | Destination    | Protocol | Length | Info                             |
|-------|------------|-------------|----------------|----------|--------|----------------------------------|
| 7926  | 81.736376  | 10.5.33.243 | 31.13.79.35    | TLSv1.3  | 571    | Client Hello                     |
| 8007  | 82.828686  | 10.5.33.243 | 31.13.79.35    | TLSv1.3  | 571    | Client Hello                     |
| 8017  | 82.976187  | 10.5.33.243 | 31.13.79.35    | TCP      | 571    | [TCP Retransmission] 53854 → 443 |
| 8029  | 83.105775  | 10.5.33.243 | 31.13.79.35    | TLSv1.3  | 571    | Client Hello                     |
| 20617 | 160.393161 | 10.5.33.243 | 157.240.228.16 | TLSv1.3  | 571    | Client Hello                     |
| 20622 | 160.442696 | 10.5.33.243 | 157.240.228.15 | TLSv1.3  | 571    | Client Hello                     |
| 22669 | 162.825160 | 10.5.33.243 | 157.240.228.15 | TLSv1.3  | 571    | Client Hello                     |

Server Name list length: 19  
Server Name Type: host\_name (0)  
Server Name length: 16  
Server Name: www.facebook.com  
Extension: extended\_master\_secret (len=0)

0080 bf c6 00 20 6a 6a 13 01 13 02 13 03 c0 2b c0 2f ...jj- .....+/  
0090 c0 2c 00 c0 30 cc a9 cc a8 c0 13 c0 14 00 9c 00 9d ...0 .....  
00a0 00 2f 00 35 01 00 01 93 3a 3a 00 00 00 00 00 15 .../5 .....  
00b0 00 13 00 00 10 77 77 77 2e 66 61 63 65 62 6f 6f .....www.facebook  
00c0 6b 2e 63 6f 6d 00 17 00 00 ff 01 00 01 00 00 0a .....k.com .....  
00d0 00 0a 00 08 ea ea 00 1d 00 17 00 18 00 0b 00 02 .....  
00e0 01 00 00 23 00 00 00 10 00 0e 00 0c 02 68 32 08 .....# .....h2-  
00f0 68 74 74 70 2f 31 2e 31 00 05 00 05 01 00 00 00 .....http/1.1 .....  
0100 00 00 0d 00 12 00 10 04 03 08 04 04 01 05 03 08 .....  
0110 05 05 01 08 06 06 01 00 12 00 00 00 33 00 2b 00 .....-3+.) .....  
0120 29 ea ea 00 01 00 00 1d 00 20 fa 3a 50 df 0b 03 .....-P .....  
0130 93 ae c0 82 3d 20 f0 0a 5c 8d 9a b6 27 59 6f 54 .....-...-\'YoT  
0140 68 af 54 f1 76 e5 14 2c 67 63 00 2d 00 02 01 01 .....h-T-v-...gc-  
0150 00 2b 00 07 06 0a 0a 03 04 03 03 00 1b 00 03 02 .....+ .....  
0160 00 02 44 69 00 05 00 03 02 68 32 9a 9a 00 01 00 .....-Di .....h2 .....  
Server Name (tls.handshake.extensions\_server\_name), 16 bytes | Packets: 25129 · Displayed: 7 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp contains mail

| No.  | Time      | Source         | Destination      | Protocol | Length | Info                            |
|------|-----------|----------------|------------------|----------|--------|---------------------------------|
| 1289 | 33.097271 | 10.5.33.243    | 172.217.160.1... | TLSv1.3  | 571    | Client Hello                    |
| 1746 | 35.135693 | 204.79.197.200 | 10.5.33.243      | TCP      | 1440   | 443 → 53938 [PSH, ACK] Seq=1387 |
| 2040 | 36.207188 | 204.79.197.200 | 10.5.33.243      | TCP      | 1440   | 443 → 53942 [PSH, ACK] Seq=1387 |

Server Name list length: 18  
Server Name Type: host\_name (0)  
Server Name length: 15  
Server Name: mail.google.com  
Extension: extended\_master\_secret (len=0)

00b0 00 12 00 00 0f 6d 61 69 6c 2e 67 6f 6f 67 6c 65 .....mai l.google  
00c0 2e 63 6f 6d 00 17 00 00 ff 01 00 01 00 00 0a 00 .....com .....  
00d0 0a 00 08 fa fa 00 1d 00 17 00 18 00 0b 00 02 01 .....  
00e0 00 00 23 00 00 00 10 00 0e 00 0c 02 68 32 08 68 .....# .....h2-h  
00f0 74 74 70 2f 31 2e 31 00 05 00 05 01 00 00 00 00 .....ttp/1.1 .....  
0100 00 0d 00 12 00 10 04 03 08 04 04 01 05 03 08 05 .....  
0110 05 01 08 06 06 01 00 12 00 00 00 33 00 2b 00 29 .....-3+.) .....  
0120 fa fa 00 01 00 00 1d 00 20 30 eb db d4 91 b3 f6 .....0 .....  
0130 72 ec 9c 93 f7 12 fa 35 5e 04 25 ed 6c 28 ec a4 .....r .....5 ^%1(..  
0140 28 52 24 38 e6 86 b4 9a 29 00 2d 00 02 01 01 00 .....(R\$ .....)- .....  
0150 2b 00 07 06 ba ba 03 04 03 03 00 1b 00 03 02 00 .....+ .....  
0160 02 44 69 00 05 00 03 02 68 32 ea ea 00 01 00 00 .....Di .....h2 .....  
0170 15 00 c8 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
Server Name (tls.handshake.extensions\_server\_name), 15 bytes | Packets: 5642 · Displayed: 3 (0.1%) · Dropped: 0 (0.0%) | Profile: Default