

Wireshark CN: Lab 4

Submitted By: Stuti Garg (SE22UCSE263)

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window".

- IP address is 10.70.29.162 and TCP port number is 49891 that is being used by the client computer that is transferring the file to gaia.cs.umass.edu.

No.	Time	Source	Destination	Protocol	Length	Info
385	27.292191	10.70.29.162	128.119.245.12	HTTP	587	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
421	27.513500	128.119.245.12	10.70.29.162	HTTP	831	HTTP/1.1 200 OK (text/html)

- - ▼ Frame 385: 587 bytes on wire (4696 bits), 587 bytes captured (4696 bits) on interface \Device\NPF_{85D361EE-6564-750D-0A58-000000000000} (ethertype: IP (0x0800))
 - Section number: 1
 - > Interface id: 0 (\Device\NPF_{85D361EE-6564-750D-0A58-000000000000})
 - Encapsulation type: Ethernet (1)
 - Arrival Time: Feb 19, 2025 11:43:09.770480000 India Standard Time
 - UTC Arrival Time: Feb 19, 2025 06:13:09.770480000 UTC
 - Epoch Arrival Time: 1739945589.770480000
 - [Time shift for this packet: 0.000000000 seconds]
 - [Time delta from previous captured frame: 0.000000000 seconds]
 - [Time delta from previous displayed frame: 0.000000000 seconds]
 - [Time since reference or first frame: 27.292191000 seconds]
 - Frame Number: 385
 - Frame Length: 587 bytes (4696 bits)
 - Capture Length: 587 bytes (4696 bits)
 - [Frame is marked: False]
 - [Frame is ignored: False]
 - [Protocols in Frame: eth:ethertype:ip:tcp:http:mime:multipart:data:text-lines]
 - [Coloring Rule Name: HTTP]
 - [Coloring Rule String: http || tcp.port == 80 || http2]
 - > Ethernet II, Src: Microsoft_7F:AD:FC (78:BC:10:F7:AD:FC), Dst: 12:01:00:00:01:00 (12:01:00:00:01:00)
 - > Internet Protocol Version 4, Src: 10.70.29.162, Dst: 128.119.245.12
 - > Transmission Control Protocol, Src Port: 49891, Dst Port: 80, Seq: 152524, Ack: 1, Len: 533
 - > [112 Reassembled TCP Segments (153056 bytes): #189(721), #190(1382), #191(1382), #192(1382), #193(1382), #194(1382), #195(1382), #196(1382), #197(1382), #198(1382), #199(1382), #200(1382), #201(1382), #202(1382), #203(1382), #204(1382), #205(1382), #206(1382), #207(1382), #208(1382), #209(1382), #210(1382), #211(1382), #212(1382), #213(1382), #214(1382), #215(1382), #216(1382), #217(1382), #218(1382), #219(1382), #220(1382), #221(1382), #222(1382), #223(1382), #224(1382), #225(1382), #226(1382), #227(1382), #228(1382), #229(1382), #230(1382), #231(1382), #232(1382), #233(1382), #234(1382), #235(1382), #236(1382), #237(1382), #238(1382), #239(1382), #240(1382), #241(1382), #242(1382), #243(1382), #244(1382), #245(1382), #246(1382), #247(1382), #248(1382), #249(1382), #250(1382), #251(1382), #252(1382), #253(1382), #254(1382), #255(1382), #256(1382), #257(1382), #258(1382), #259(1382), #260(1382), #261(1382), #262(1382), #263(1382), #264(1382), #265(1382), #266(1382), #267(1382), #268(1382), #269(1382), #270(1382), #271(1382), #272(1382), #273(1382), #274(1382), #275(1382), #276(1382), #277(1382), #278(1382), #279(1382), #280(1382), #281(1382), #282(1382), #283(1382), #284(1382), #285(1382), #286(1382), #287(1382), #288(1382), #289(1382), #290(1382), #291(1382), #292(1382), #293(1382), #294(1382), #295(1382), #296(1382), #297(1382), #298(1382), #299(1382), #300(1382), #301(1382), #302(1382), #303(1382), #304(1382), #305(1382), #306(1382), #307(1382), #308(1382), #309(1382), #310(1382), #311(1382), #312(1382), #313(1382), #314(1382), #315(1382), #316(1382), #317(1382), #318(1382), #319(1382), #320(1382), #321(1382), #322(1382), #323(1382), #324(1382), #325(1382), #326(1382), #327(1382), #328(1382), #329(1382), #330(1382), #331(1382), #332(1382), #333(1382), #334(1382), #335(1382), #336(1382), #337(1382), #338(1382), #339(1382), #340(1382), #341(1382), #342(1382), #343(1382), #344(1382), #345(1382), #346(1382), #347(1382), #348(1382), #349(1382), #350(1382), #351(1382), #352(1382), #353(1382), #354(1382), #355(1382), #356(1382), #357(1382), #358(1382), #359(1382), #360(1382), #361(1382), #362(1382), #363(1382), #364(1382), #365(1382), #366(1382), #367(1382), #368(1382), #369(1382), #370(1382), #371(1382), #372(1382), #373(1382), #374(1382), #375(1382), #376(1382), #377(1382), #378(1382), #379(1382), #380(1382), #381(1382), #382(1382), #383(1382), #384(1382), #385(1382), #386(1382), #387(1382), #388(1382), #389(1382), #390(1382), #391(1382), #392(1382), #393(1382), #394(1382), #395(1382), #396(1382), #397(1382), #398(1382), #399(1382), #400(1382), #401(1382), #402(1382), #403(1382), #404(1382), #405(1382), #406(1382), #407(1382), #408(1382), #409(1382), #410(1382), #411(1382), #412(1382), #413(1382), #414(1382), #415(1382), #416(1382), #417(1382), #418(1382), #419(1382), #420(1382), #421(1382), #422(1382), #423(1382), #424(1382), #425(1382), #426(1382), #427(1382), #428(1382), #429(1382), #430(1382), #431(1382), #432(1382), #433(1382), #434(1382), #435(1382), #436(1382), #437(1382), #438(1382), #439(1382), #440(1382), #441(1382), #442(1382), #443(1382), #444(1382), #445(1382), #446(1382), #447(1382), #448(1382), #449(1382), #450(1382), #451(1382), #452(1382), #453(1382), #454(1382), #455(1382), #456(1382), #457(1382), #458(1382), #459(1382), #460(1382), #461(1382), #462(1382), #463(1382), #464(1382), #465(1382), #466(1382), #467(1382), #468(1382), #469(1382), #470(1382), #471(1382), #472(1382), #473(1382), #474(1382), #475(1382), #476(1382), #477(1382), #478(1382), #479(1382), #480(1382), #481(1382), #482(1382), #483(1382), #484(1382), #485(1382), #486(1382), #487(1382), #488(1382), #489(1382), #490(1382), #491(1382), #492(1382), #493(1382), #494(1382), #495(1382), #496(1382), #497(1382), #498(1382), #499(1382), #500(1382), #501(1382), #502(1382), #503(1382), #504(1382), #505(1382), #506(1382), #507(1382), #508(1382), #509(1382), #510(1382), #511(1382), #512(1382), #513(1382), #514(1382), #515(1382), #516(1382), #517(1382), #518(1382), #519(1382), #520(1382), #521(1382), #522(1382), #523(1382), #524(1382), #525(1382), #526(1382), #527(1382), #528(1382), #529(1382), #530(1382), #531(1382), #532(1382), #533(1382), #534(1382), #535(1382), #536(1382), #537(1382), #538(1382), #539(1382), #540(1382), #541(1382), #542(1382), #543(1382), #544(1382), #545(1382), #546(1382), #547(1382), #548(1382), #549(1382), #550(1382), #551(1382), #552(1382), #553(1382), #554(1382), #555(1382), #556(1382), #557(1382), #558(1382), #559(1382), #560(1382), #561(1382), #562(1382), #563(1382), #564(1382), #565(1382), #566(1382), #567(1382), #568(1382), #569(1382), #570(1382), #571(1382), #572(1382), #573(1382), #574(1382), #575(1382), #576(1382), #577(1382), #578(1382), #579(1382), #580(1382), #581(1382), #582(1382), #583(1382), #584(1382), #585(1382), #586(1382), #587(1382), #588(1382), #589(1382), #590(1382), #591(1382), #592(1382), #593(1382), #594(1382), #595(1382), #596(1382), #597(1382), #598(1382), #599(1382), #600(1382), #601(1382), #602(1382), #603(1382), #604(1382), #605(1382), #606(1382), #607(1382), #608(1382), #609(1382), #610(1382), #611(1382), #612(1382), #613(1382), #614(1382), #615(1382), #616(1382), #617(1382), #618(1382), #619(1382), #620(1382), #621(1382), #622(1382), #623(1382), #624(1382), #625(1382), #626(1382), #627(1382), #628(1382), #629(1382), #630(1382), #631(1382), #632(1382), #633(1382), #634(1382), #635(1382), #636(1382), #637(1382), #638(1382), #639(1382), #640(1382), #641(1382), #642(1382), #643(1382), #644(1382), #645(1382), #646(1382), #647(1382), #648(1382), #649(1382), #650(1382), #651(1382), #652(1382), #653(1382), #654(1382), #655(1382), #656(1382), #657(1382), #658(1382), #659(1382), #660(1382), #661(1382), #662(1382), #663(1382), #664(1382), #665(1382), #666(1382), #667(1382), #668(1382), #669(1382), #670(1382), #671(1382), #672(1382), #673(1382), #674(1382), #675(1382), #676(1382), #677(1382), #678(1382), #679(1382), #680(1382), #681(1382), #682(1382), #683(1382), #684(1382), #685(1382), #686(1382), #687(1382), #688(1382), #689(1382), #690(1382), #691(1382), #692(1382), #693(1382), #694(1382), #695(1382), #696(1382), #697(1382), #698(1382), #699(1382), #700(1382), #701(1382), #702(1382), #703(1382), #704(1382), #705(1382), #706(1382), #707(1382), #708(1382), #709(1382), #710(1382), #711(1382), #712(1382), #713(1382), #714(1382), #715(1382), #716(1382), #717(1382), #718(1382), #719(1382), #720(1382), #721(1382), #722(1382), #723(1382), #724(1382), #725(1382), #726(1382), #727(1382), #728(1382), #729(1382), #730(1382), #731(1382), #732(1382), #733(1382), #734(1382), #735(1382), #736(1382), #737(1382), #738(1382), #739(1382), #740(1382), #741(1382), #742(1382), #743(1382), #744(1382), #745(1382), #746(1382), #747(1382), #748(1382), #749(1382), #750(1382), #751(1382), #752(1382), #753(1382), #754(1382), #755(1382), #756(1382), #757(1382), #758(1382), #759(1382), #760(1382), #761(1382), #762(1382), #763(1382), #764(1382), #765(1382), #766(1382), #767(1382), #768(1382), #769(1382), #770(1382), #771(1382), #772(1382), #773(1382), #774(1382), #775(1382), #776(1382), #777(1382), #778(1382), #779(1382), #780(1382), #781(1382), #782(1382), #783(1382), #784(1382), #785(1382), #786(1382), #787(1382), #788(1382), #789(1382), #790(1382), #791(1382), #792(1382), #793(1382), #794(1382), #795(1382), #796(1382), #797(1382), #798(1382), #799(1382), #800(1382), #801(1382), #802(1382), #803(1382), #804(1382), #805(1382), #806(1382), #807(1382), #808(1382), #809(1382), #810(1382), #811(1382), #812(1382), #813(1382), #814(1382), #815(1382), #816(1382), #817(1382), #818(1382), #819(1382), #820(1382), #821(1382), #822(1382), #823(1382), #824(1382), #825(1382), #826(1382), #827(1382), #828(1382), #829(1382), #830(1382), #831(1382), #832(1382), #833(1382), #834(1382), #835(1382), #836(1382), #837(1382), #838(1382), #839(1382), #840(1382), #841(1382), #842(1382), #843(1382), #844(1382), #845(1382), #846(1382), #847(1382), #848(1382), #849(1382), #850(1382), #851(1382), #852(1382), #853(1382), #854(1382), #855(1382), #856(1382), #857(1382), #858(1382), #859(1382), #860(1382), #861(1382), #862(1382), #863(1382), #864(1382), #865(1382), #866(1382), #867(1382), #868(1382), #869(1382), #870(1382), #871(1382), #872(1382), #873(1382), #874(1382), #875(1382), #876(1382), #877(1382), #878(1382), #879(1382), #880(1382), #881(1382), #882(1382), #883(1382), #884(1382), #885(1382), #886(1382), #887(1382), #888(1382), #889(1382), #890(1382), #891(1382), #892(1382), #893(1382), #894(1382), #895(1382), #896(1382), #897(1382), #898(1382), #899(1382), #900(1382), #901(1382), #902(1382), #903(1382), #904(1382), #905(1382), #906(1382), #907(1382), #908(1382), #909(1382), #910(1382), #911(1382), #912(1382), #913(1382), #914(1382), #915(1382), #916(1382), #917(1382), #918(1382), #919(1382), #920(1382), #921(1382), #922(1382), #923(1382), #924(1382), #925(1382), #926(1382), #927(1382), #928(1382), #929(1382), #930(1382), #931(1382), #932(1382), #933(1382), #934(1382), #935(1382), #936(1382), #937(1382), #938(1382), #939(1382), #940(1382), #941(1382), #942(1382), #943(1382), #944(1382), #945(1382), #946(1382), #947(1382), #948(1382), #949(1382), #950(1382), #951(1382), #952(1382), #953(1382), #954(1382), #955(1382), #956(1382), #957(1382), #958(1382), #959(1382), #960(1382), #961(1382), #962(1382), #963(1382), #964(1382), #965(1382), #966(1382), #967(1382), #968(1382), #969(1382), #970(1382), #971(1382), #972(1382), #973(1382), #974(1382), #975(1382), #976(1382), #977(1382), #978(1382), #979(1382), #980(1382), #981(1382), #982(1382), #983(1382), #984(1382), #985(1382), #986(1382), #987(1382), #988(1382), #989(1382), #990(1382), #991(1382), #992(1382), #993(1382), #994(1382), #995(1382), #996(1382), #997(1382), #998(1382), #999(1382), #1000(1382), #1001(1382), #1002(1382), #1003(1382), #1004(1382), #1005(1382), #1006(1382), #1007(1382), #1008(1382), #1009(1382), #1010(1382), #1011(1382), #1012(1382), #1013(1382), #1014(1382), #1015(1382), #1016(1382), #1017(1382), #1018(1382), #1019(1382), #1020(1382), #1021(1382), #1022(1382), #1023(1382), #1024(1382), #1025(1382), #1026(1382), #1027(1382), #1028(1382), #1029(1382), #1030(1382), #1031(1382), #1032(1382), #1033(1382), #1034(1382), #1035(1382), #1036(1382), #1037(1382), #1038(1382), #1039(1382), #1040(1382), #1041(1382), #1042(1382), #1043(1382), #1044(1382), #1045(1382), #1046(1382), #1047(1382), #1048(1382), #1049(1382), #1050(1382), #1051(1382), #1052(1382), #1053(1382), #1054(1382), #1055(1382), #1056(1382), #1057(1382), #1058(1382), #1059(1382), #1060(1382), #1061(1382), #1062(1382), #1063(1382), #1064(1382), #1065(1382), #1066(1382), #1067(1382), #1068(1382), #1069(1382), #1070(1382), #1071(1382), #1072(1382), #1073(1382), #1074(1382), #1075(1382), #1076(1382), #1077(1382), #1078(1382), #1079(1382), #1080(1382), #1081(1382), #1082(1382), #1083(1382), #1084(1382), #1085(1382), #1086(1382), #1087(1382), #1088(1382), #1089(1382), #1090(1382), #1091(1382), #1092(1382), #1093(1382), #1094(1382), #1095(1382), #1096(1382), #1097(1382), #1098(1382), #1099(1382), #1100(1382), #1101(1382), #1102(1382), #1103(1382), #1104(1382), #1105(1382), #1106(1382), #1107(1382), #1108(1382), #1109(1382), #1110(1382), #1111(1382), #1112(1382), #1113(1382), #1114(1382), #1115(1382), #1116(1382), #1117(1382), #1118(1382), #1119(1382), #1120(1382), #1121(1382), #1122(1382), #1123(1382), #1124(1382), #1125(1382), #1126(1382), #1127(1382), #1128(1382), #1129(1382), #1130(1382), #1131(1382), #1132(1382), #1133(1382), #1134(1382), #1135(1382), #1136(1382), #1137(1382), #1138(1382), #1139(1382), #1140(1382), #1141(1382), #1142(1382), #1143(1382), #1144(1382), #1145(1382), #1146(1382), #1147(1382), #1148(1382), #1149(1382), #1150(1382), #1151(1382), #1152(1382), #1153(1382), #1154(1382), #1155(1382), #1156(1382), #1157(1382), #1158(1382), #1159(1382), #1160(1382), #1161(1382), #1162(1382), #1163(1382), #1164(1382), #1165(1382), #1166(1382), #1167(1382), #1168(1382), #1169(1382), #1170(1382), #1171(1382), #1172(1382), #1173(1382), #1174(1382), #1175(1382), #1176(1382), #1177(1382), #1178(1382), #1179(1382), #1180(1382), #1181(1382), #1182(1382), #1183(1382), #1184(1382), #1185(1382), #1186(1382), #1187(1382), #1188(1382), #1189(1382), #1190(1382), #1191(1382), #1192(1382), #1193(1382), #1194(1382), #1195(1382), #1196(1382), #1197(1382), #1198(1382), #1199(1382), #1200(1382), #1201(1382), #1202(1382), #1203(1382), #1204(1382), #1205(1382), #1206(1382), #1207(1382), #1208(1382), #1209(1382), #1210(1382), #1211(1382), #1212(1382), #1213(1382), #1214(1382), #1215(1382), #1216(1382), #1217(1382), #1218(1382), #1219(1382), #1220(1382), #1221(1382), #1222(1382), #1223(1382), #1224(1382), #1225(1382), #1226(1382), #1227(1382), #1228(1382), #1229(1382), #1230(1382), #1231(1382), #1232(1382), #1233(1382), #1234(1382), #1235(1382), #1236(1382), #1237(1382), #1238(1382), #1239(1382), #1240(1382), #1241(1382), #1242(1382), #1243(1382), #1244(1382), #1245(1382), #1246(1382), #1247(1382), #1248(1382), #1249(1382), #1250(1382), #1251(1382), #1252(1382), #1253(1382), #1254(1382), #1255(1382), #1256(1382), #1257(1382), #1258(1382), #1259(1382), #1260(1382), #1261(1382), #1262(1382), #1263(1382), #1264(1382), #1265(1382), #1266(1382), #1267(1382), #1268(1382), #1269(1382), #1270(

- - ▼ Transmission Control Protocol, Src Port: 49891, Dst Port: 80, Seq: 152524, Ack: 1, Len: 533
 - Source Port: 49891
 - Destination Port: 80
 - [Stream index: 9]
 - [Conversation completeness: Incomplete (30)]
 - [TCP Segment Len: 533]
 - Sequence Number: 152524 (relative sequence number)
 - Sequence Number (raw): 3887976164
 - [Next Sequence Number: 153057 (relative sequence number)]
 - Acknowledgment Number: 1 (relative ack number)
 - Acknowledgment number (raw): 1459396136
 - 0101 = Header Length: 20 bytes (5)
 - Flags: 0x018 (PSH, ACK)
 - Window: 512
 - [Calculated window size: 512]
 - [Window size scaling factor: -1 (unknown)]
 - Checksum: 0x78c9 [unverified]

3. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?

- The IP address is 128.119.245.12.
- The TCP port number used by the client computer to transfer the file to gaia.cs.umass.edu is 49891.

- - ▼ Transmission Control Protocol, Src Port: 49891, Dst Port: 80, Seq: 152524, Ack: 1, Len: 533
 - Source Port: 49891
 - Destination Port: 80
 - [Stream index: 9]
 - [Conversation completeness: Incomplete (30)]
 - [TCP Segment Len: 533]
 - Sequence Number: 152524 (relative sequence number)
 - Sequence Number (raw): 3887976164
 - [Next Sequence Number: 153057 (relative sequence number)]
 - Acknowledgment Number: 1 (relative ack number)
 - Acknowledgment number (raw): 1459396136
 - 0101 = Header Length: 20 bytes (5)
 - ▼ Flags: 0x018 (PSH, ACK)
 - 000. = Reserved: Not set
 - ...0 = Accurate ECN: Not set
 - 0... = Congestion Window Reduced: Not set
 -0.. = ECN-Echo: Not set

4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

- The sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu is 4236540160.

tcp.flags.syn == 1 && tcp.flags.ack == 0

No.	Time	Source	Destination	Protocol	Length	Info
474	24.811093	192.168.1.109	128.119.240.12	TCP	110	2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1011	32.808574	192.168.1.109	128.119.240.19	TCP	110	2541 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1034	32.869262	192.168.1.109	128.119.240.19	TCP	110	2542 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1119	32.957207	192.168.1.109	128.119.240.19	TCP	110	2544 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1121	32.958198	192.168.1.109	128.119.240.19	TCP	110	2545 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1142	32.981949	192.168.1.109	64.233.187.104	TCP	110	2546 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1153	33.001575	192.168.1.109	128.119.240.19	TCP	110	2547 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1262	33.099063	192.168.1.109	128.119.240.19	TCP	110	2548 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1280	33.115208	192.168.1.109	128.119.240.19	TCP	110	2549 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1714	49.020356	128.119.101.5	192.168.1.109	TCP	108	80 → 2543 [SYN, PSH, ECE, AE] Seq=0 Win=7504 [Malformed Packet]

[Coloring Rule String: tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && ...]

> Radiotap Header v0, Length 24

> 802.11 radio information

> IEEE 802.11 QoS Data, Flags:R..TC

> Logical-Link Control

> Internet Protocol Version 4, Src: 192.168.1.109, Dst: 64.233.187.104

> Transmission Control Protocol, Src Port: 2546, Dst Port: 80, Seq: 0, Len: 0

Source Port: 2546

Destination Port: 80

[Stream index: 7]

> [Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 4236540160

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 0

Acknowledgment number (raw): 0

0111 = Header Length: 28 bytes (7)

> Flags: 0x002 (SYN)

000. = Reserved: Not set

...0 = Accurate ECN: Not set

.... 0... = Congestion Window Reduced: Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...0 = Acknowledgment: Not set

.... 0... = Push: Not set

.... 0.. = Reset: Not set

>1. = Syn: Set

....0 = Fin: Not set

[TCP Flags:S.]

Window: 16384

[Calculated window size: 16384]

Checksum: 0x04f1 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

- The segment identified as SYN is set to 1 under the flags section.

Sequence Number (raw): 4236540160

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 0

Acknowledgment number (raw): 0

0111 = Header Length: 28 bytes (7)

> Flags: 0x002 (SYN)

000. = Reserved: Not set

...0 = Accurate ECN: Not set

.... 0... = Congestion Window Reduced: Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...0 = Acknowledgment: Not set

.... 0... = Push: Not set

.... 0.. = Reset: Not set

>1. = Syn: Set

....0 = Fin: Not set

[TCP Flags:S.]

Window: 16384

[Calculated window size: 16384]

Checksum: 0x04f1 [unverified]

[Checksum Status: Unverified]

- Urgent Pointer: 0

5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the ACKnowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

- The sequence number of the SYNACK segment sent by the gaia.cs.umass.edu to the client computer in reply to the SYN is 3887976164.
- The value of the Acknowledgement field in the SYNACK segment is (client's initial sequence number + 1) that is 1459396136.
- gaia.cs.umass.edu determines the ACK number in the SYN-ACK by taking the client's Initial Sequence Number (ISN) + 1, acknowledging the next expected byte. This follows TCP's rule that a SYN flag consumes one sequence number.
- The segment that identifies it is under the Transmission Control Protocol section.

✓ Transmission Control Protocol, Src Port: 49891, Dst Port: 80, Seq: 152524, Ack: 1, Len: 533

Source Port: 49891

Destination Port: 80

[Stream index: 9]

➤ [Conversation completeness: Incomplete (30)]

[TCP Segment Len: 533]

Sequence Number: 152524 (relative sequence number)

Sequence Number (raw): 3887976164

[Next Sequence Number: 153057 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 1459396136

0101 = Header Length: 20 bytes (5)

○

- The SYN and ACK flags must be set to 1.

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 691643676

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 2313716653

0111 = Header Length: 28 bytes (7)

✓ Flags: 0x012 (SYN, ACK)

000. = Reserved: Not set

...0 = Accurate ECN: Not set

.... 0... = Congestion Window Reduced: Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgment: Set

.... 0... = Push: Not set

....0.. = Reset: Not set

➤1. = Syn: Set

....0 = Fin: Not set

[TCP Flags:A..S.]

Window: 5840

[Calculated window size: 5840]

Checksum: 0x5372 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

✓ Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted

➤ TCP Option - Maximum segment size: 1460 bytes

○

6. What is the sequence number of the TCP segment containing the HTTP POST command?
Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

- The sequence number of the TCP segment containing the HTTP POST command is 1274860846.

```

Transmission Control Protocol, Src Port: 49799, Dst Port: 80, Seq: 1, Ack: 1, Len: 470
  Source Port: 49799
  Destination Port: 80
  [Stream Index: 65]
  > [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 470]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 1274860846
  [Next Sequence Number: 471 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 4286598160
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
  000. .... = Reserved: Not set
  ....0... = Accurate ECN: Not set
  ....0... = Congestion Window Reduced: Not set
  ....0... = ECH-Echo: Not set
  ....0... = Urgent: Not set
  ....1... = Acknowledgment: Set
  ....1... = Push: Set
  ....0... = Reset: Not set

```

7. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received? Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of the six segments? What is the EstimatedRTT value after the receipt of each ACK?

- The sequence numbers of the first six segments in the TCP connection are- 1, 459, 1841, 3223, 64240, 65535.
- The segment times for the first six sequence numbers- 1, 459, 1841, 3223, 64240, 65535 are 0.023109, 2.775555, 2.775555, 2.775555, 2.934224, 2.934428 respectively.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.70.29.162	52.110.15.140	TCP	55	65114 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1
2	0.023109	52.110.15.140	10.70.29.162	TCP	66	443 → 65114 [ACK] Seq=1 Ack=2 Win=16384 Len=0 SLE=1 SRE=2
3	0.345437	184.26.54.155	10.70.29.162	UDP	108	443 → 62683 Len=66
4	1.239248	10.70.29.162	34.144.254.29	TCP	55	65403 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP PDU reassembled in 1486]
5	1.259431	34.144.254.29	10.70.29.162	TCP	66	443 → 65403 [ACK] Seq=1 Ack=2 Win=1039 Len=0 SLE=1 SRE=2
6	2.656316	10.70.29.162	34.144.254.29	TCP	55	65357 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1
7	2.678754	34.144.254.29	10.70.29.162	TCP	66	443 → 65357 [ACK] Seq=1 Ack=2 Win=1050 Len=0 SLE=1 SRE=2
8	2.775313	10.70.29.162	52.182.143.213	TLSv1.2	512	Application Data
9	2.775555	10.70.29.162	52.182.143.213	TCP	1436	64627 → 443 [ACK] Seq=459 Ack=1 Win=1024 Len=1382 [TCP PDU reassembled in 40]
10	2.775555	10.70.29.162	52.182.143.213	TCP	1436	64627 → 443 [ACK] Seq=1841 Ack=1 Win=1024 Len=1382 [TCP PDU reassembled in 40]
11	2.775555	10.70.29.162	52.182.143.213	TCP	1436	64627 → 443 [ACK] Seq=3223 Ack=1 Win=1024 Len=1382 [TCP PDU reassembled in 40]
12	2.934224	10.70.29.162	10.59.121.144	TCP	66	49750 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
13	2.935084	10.70.29.162	10.59.121.144	TCP	66	49751 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

- EstimatedRTT=(1-α)×EstimatedRTT+α×SampleRTT (alpha = 0.125)
- Calculations:

Segment	Sample RTT (ms)	Estimated RTT Calculations	Estimated RTT (ms)
1	2.752446	Initial RTT	2.752446
2	2.752446	No change	2.752446
3	2.752446	No change	2.752446
4	0.158669	(0.875 × 2.752446) + (0.125 × 0.158669)	2.4229

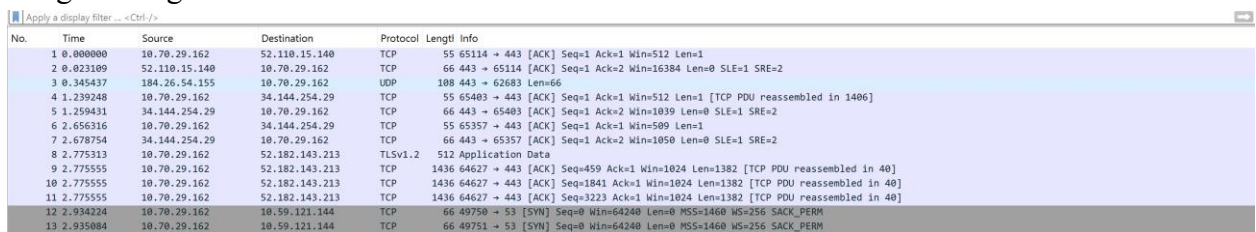
5	0.000204	$(0.875 \times 2.4229) + (0.125 \times 0.000204)$	2.1190
---	----------	---	--------

Estimated RTT after each segment:

- After 1st segment: 2.752 ms
- After 4th segment: 2.422 ms
- After 5th segment: 2.119 ms

8. What is the length of each of the first six TCP segments?

- Length of segment 1: 66
- Length of segment 2: 1436
- Length of segment 3: 1436
- Length of segment 4: 1436
- Length of segment 5: 66
- Length of segment 6: 2186



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.70.29.162	52.110.15.140	TCP	55	65114 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1
2	0.023109	52.110.15.140	10.70.29.162	TCP	66	443 → 65114 [ACK] Seq=1 Ack=2 Win=16384 Len=0 SLE=1 SRE=2
3	0.345437	184.26.54.155	10.70.29.162	UDP	108	443 → 62683 Len=66
4	1.239248	10.70.29.162	34.144.254.29	TCP	55	65403 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP PDU reassembled in 1406]
5	1.259431	34.144.254.29	10.70.29.162	TCP	66	443 → 65403 [ACK] Seq=1 Ack=2 Win=1039 Len=0 SLE=1 SRE=2
6	2.656316	10.70.29.162	34.144.254.29	TCP	55	65357 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1
7	2.678754	34.144.254.29	10.70.29.162	TCP	66	443 → 65357 [ACK] Seq=1 Ack=2 Win=1050 Len=0 SLE=1 SRE=2
8	2.775313	10.70.29.162	52.182.143.213	TLShv1.2	512	Application Data
9	2.775555	10.70.29.162	52.182.143.213	TCP	1436	64627 → 443 [ACK] Seq=459 Ack=1 Win=1024 Len=1382 [TCP PDU reassembled in 40]
10	2.775555	10.70.29.162	52.182.143.213	TCP	1436	64627 → 443 [ACK] Seq=1841 Ack=1 Win=1024 Len=1382 [TCP PDU reassembled in 40]
11	2.775555	10.70.29.162	52.182.143.213	TCP	1436	64627 → 443 [ACK] Seq=3223 Ack=1 Win=1024 Len=1382 [TCP PDU reassembled in 40]
12	2.934224	10.70.29.162	10.59.121.144	TCP	66	49750 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
13	2.935084	10.70.29.162	10.59.121.144	TCP	66	49751 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

9. What is the minimum amount of available buffer space advertised at the receiver for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

- The minimum amount of available buffer space advertised at the receiver for the entire trace is 5840 bytes
- Yes, due to the lack of receiver buffer space, sender was throttled.
- The presence of Zero Window packets indicates that the receiver's buffer space was exhausted, forcing the sender to pause data transmission.
- This behavior helps prevent packet loss and congestion but can also lead to temporary delays in data transfer.
- .

tcp.window_size.value

No.	Time	Source	Destination	Protocol	Length	Info
474	24.811093	192.168.1.109	128.119.245.12	TCP	110	2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
476	24.827751	128.119.245.12	192.168.1.109	TCP	110	80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM
478	24.828024	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
480	24.828253	192.168.1.109	128.119.245.12	HTTP	537	GET /wireshark-labs/alice.txt HTTP/1.1
482	24.846898	128.119.245.12	192.168.1.109	TCP	108	80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
484	24.847171	128.119.245.12	192.168.1.109	TCP	108	[TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
486	24.848829	128.119.245.12	192.168.1.109	TCP	415	80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP PDU reassembled in 868]
488	24.850314	128.119.245.12	192.168.1.109	TCP	1562	80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
489	24.850809	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
490	24.851398	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
492	24.851620	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
494	24.851828	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=1774 Win=17520 Len=0
495	24.852081	192.168.1.109	128.119.245.12	TCP	102	[TCP Dup ACK 494#1] 2538 → 80 [ACK] Seq=436 Ack=1774 Win=17520 Len=0
497	24.852817	128.119.245.12	192.168.1.109	TCP	1562	[TCP Spurious Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
501	24.873619	128.119.245.12	192.168.1.109	TCP	1562	80 → 2538 [ACK] Seq=1774 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
502	24.874444	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=1774 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
504	24.874700	128.119.245.12	192.168.1.109	TCP	1562	80 → 2538 [ACK] Seq=3234 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
507	24.875690	128.119.245.12	192.168.1.109	TCP	1562	80 → 2538 [ACK] Seq=4694 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
509	24.875810	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=4694 Win=17520 Len=0
511	24.894483	199.83.245.12	192.168.1.109	TCP	1562	80 → 2538 [ACK] Seq=1 Ack=1 Win=6432 Len=1460
513	24.895561	128.119.245.12	192.168.1.109	TCP	1562	80 → 2538 [ACK] Seq=6154 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
514	24.896643	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=6154 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
516	24.896869	128.119.245.12	192.168.1.109	TCP	1562	80 → 2538 [ACK] Seq=7614 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]

802.11 radio information

IEEE 802.11 QoS Data, Flags: ..MP..F.C

Logical-Link Control

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.109

Transmission Control Protocol, Src Port: 80, Dst Port: 2538, Seq: 0, Ack: 1, Len: 0

Source Port: 80

Destination Port: 2538

[Stream Index: 0]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 2928664127

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 1907346759

0111 = Header Length: 28 bytes (7)

Flags: 0x012 (SYN, ACK)

Window: 5840

[Calculated window size: 5840]

Checksum: 0x5a5 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 208

Options: (8 bytes), CC.ECHO, No-Operation (NOP), No-Operation (NOP), SACK permitted

[Timestamps]

[Time since first frame in this TCP stream: 0.016658000 seconds]

10. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

- Yes, there are retransmitted segments in the trace file as given in the screenshot below.
- Used filter tcp.analysis.retransmission to find re-transmitted packets.
- I also checked for duplicate sequence numbers, Higher-than-normal RTT values and TCP Fast Retransmission events.

No.	Time	Source	Destination	Protocol	Length	Info
489	24.820809	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
490	24.851390	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
492	24.851620	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
497	24.852817	128.119.245.12	192.168.1.109	TCP	1562	[TCP Spurious Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
502	24.874444	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=1774 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
514	24.896643	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=6154 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
519	24.897323	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=7614 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
520	24.897809	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=7614 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
521	24.898438	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=7614 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
528	24.916437	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [PSH, ACK] Seq=10534 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
529	24.916694	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [PSH, ACK] Seq=10534 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
533	24.918536	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=11994 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
538	24.920563	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=13454 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
540	24.921816	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=13454 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
543	24.922688	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=14914 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
544	24.923437	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=14914 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
545	24.924148	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=14914 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
550	24.926498	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [PSH, ACK] Seq=16374 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
554	24.928186	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=17834 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
555	24.929138	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=17834 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
612	24.971060	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=42654 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
613	24.972436	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=42654 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]
616	24.973670	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [PSH, ACK] Seq=44114 Ack=436 Win=6432 Len=1460 [TCP PDU reassembled in 868]

[Coloring Rule String: tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && < > Radiotap Header v0, Length 24 > IEEE 802.11 radio information > IEEE 802.11 QoS Data, Flags:R.F.C > Logical-Link Control > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.109 > Transmission Control Protocol, Src Port: 80, Dst Port: 2538, Seq: 314, Ack: 436, Len: 1460 > Source Port: 80 > Destination Port: 2538 > [Stream index: 0] > [Conversation completeness: Complete, WITH_DATA (31)] > [TCP Segment Len: 1460] > Sequence Number: 314 (relative sequence number) > Sequence Number (raw): 292866441 > [Next Sequence Number: 1774 (relative sequence number)] > Acknowledgment Number: 436 (relative ack number) > Acknowledgment number (raw): 1907347194 > 0101 = Header Length: 20 bytes (5) > Flags: 0x010 (ACK) > 000. = Reserved: Not set >0. = Accurate ECN: Not set >0. = Congestion Window Reduced: Not set >0. = ECN-Echo: Not set >0. = Urgent: Not set >1. = Acknowledgment: Set >0. = Push: Not set	0050 09 ea ae 8f d7 79 71 af ce fa 50 10 19 20 38 cfyq. .P. 8- 0060 00 00 20 20 20 20 20 20 20 20 20 20 20 20 0070 20 20 41 4c 49 43 45 27 53 20 41 44 56 45 4a ALICE' S ADVENT 0080 55 52 45 53 20 49 4e 20 57 4f 4e 44 45 52 4c 41 URES IN WONDERLA 0090 4e 44 00 0a 0d 0a 20 20 20 20 20 20 20 20 20 ND.... 00a0 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 00b0 4c 65 77 69 73 20 43 61 72 72 6f 6c 6c 0d 0a 0e Lewis Ca rroll... 00c0 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 THE MILL ENIUM F 00d0 54 48 45 20 4d 49 4c 4c 45 4e 4e 49 55 4d 20 46 THE MILL ENIUM F 00e0 55 4c 43 52 55 4d 20 45 44 49 54 49 4f 4e 20 33 ULCRUM E DITION 3 00f0 2e 30 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 20 20 20 .0..... 0100 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 CHAPTER 0110 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0120 49 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 I.... 0130 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 Down 0140 74 68 65 20 52 61 62 62 69 74 2d 48 6f 6c 65 0d the Rabb it-Hole- 0150 0a 0d 0a 0d 0a 20 20 41 6c 69 63 65 20 77 61 73 A lice was 0160 20 62 65 67 69 6e 6e 6e 6e 67 20 74 6f 20 67 65 beginni ng to ge 0170 74 20 76 65 72 79 20 74 69 72 65 64 20 6f 66 20 very t ired of 0180 73 69 74 69 6e 67 20 62 79 20 68 65 72 20 73 sitting by her s 0190 69 73 74 65 72 0d 0a 6f 6e 20 74 68 65 20 62 61 ister- o n the ba 01a0 6e 6b 2c 20 61 6e 64 20 6f 66 20 68 61 76 69 6e nk, and of havin 01b0 67 20 6e 6f 74 68 69 6e 67 20 74 6f 20 64 6f 3a g nothing g to do: 01c0 64 69 6e 67 2c 20 62 75 74 20 69 74 20 68 61 64 ding, but it had 01d0 73 68 65 20 68 61 64 0d 0a 70 65 65 70 65 64 20 she had- peeped 01e0 69 6e 74 6f 20 74 68 65 20 62 6f 6f 6b 20 68 65 into the book he 01f0 72 20 73 69 73 74 65 72 20 77 61 73 20 72 65 61 r sister was rea 0200 64 69 6e 67 2c 20 62 75 74 20 69 74 20 68 61 64 ding, but it had 0210 20 6e 6f 0d 0a 70 69 63 74 75 72 65 73 20 6f 72 no- pic- tures or 0220 3a 6f 6e 6a 76 6c 65 73 61 74 60 6f 6a 73 70 60 cove nant- ations i
--	--

11. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment.

- The receiver acknowledges 1460 bytes of data.
- Yes, but some cases existed where the receiver ACKs every two segments (2920 bytes).
- Also, the raw acknowledgement number received is 1907347194.

No.	Time	Source	Destination	Protocol	Length	Info
476	24.827751	128.119.245.12	192.168.1.109	TCP	118	80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM
478	24.828024	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
482	24.846898	128.119.245.12	192.168.1.109	TCP	108	80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
494	24.851828	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=1774 Win=17520 Len=0
509	24.875810	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=4694 Win=17520 Len=0
517	24.896969	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=7614 Win=17520 Len=0
525	24.899178	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=10534 Win=17520 Len=0
536	24.918998	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=13454 Win=17520 Len=0
547	24.924360	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=16374 Win=17520 Len=0
557	24.929354	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=19294 Win=17520 Len=0
563	24.939319	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=22214 Win=17520 Len=0
569	24.943806	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=25134 Win=17520 Len=0
575	24.946773	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=28054 Win=17520 Len=0
581	24.951244	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=30974 Win=17520 Len=0
589	24.957906	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=33894 Win=17520 Len=0
597	24.960597	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=36814 Win=17520 Len=0
605	24.968317	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=39734 Win=17520 Len=0
609	24.969423	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=42654 Win=17520 Len=0
618	24.973883	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=45574 Win=17520 Len=0
626	24.977191	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=48494 Win=17520 Len=0
635	24.980006	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=51414 Win=17520 Len=0
643	24.989280	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=54334 Win=17520 Len=0
649	24.992092	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=57254 Win=17520 Len=0

Radiotap Header v0, Length 24 > IEEE 802.11 radio information > IEEE 802.11 QoS Data, Flags:F.C > Logical-Link Control > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.109 > Transmission Control Protocol, Src Port: 80, Dst Port: 2538, Seq: 1, Ack: 436, Len: 0 > Source Port: 80 > Destination Port: 2538 > [Stream index: 0] > [Conversation completeness: Complete, WITH_DATA (31)] > [TCP Segment Len: 0] > Sequence Number: 1 (relative sequence number) > Sequence Number (raw): 2928664128 > [Next Sequence Number: 1 (relative sequence number)] > Acknowledgment Number: 436 (relative ack number) > Acknowledgment number (raw): 1907347194 > 0101 = Header Length: 20 bytes (5) > Flags: 0x010 (ACK) > 000. = Reserved: Not set >0. = Accurate ECN: Not set >0. = Congestion Window Reduced: Not set >0. = ECN-Echo: Not set >0. = Urgent: Not set >1. = Acknowledgment: Set >0. = Push: Not set	0000 00 00 18 00 ee 58 00 00 10 6c 85 09 c0 0d 9cX. .1..... 0010 5d 00 00 3e 9c de 38 ae 88 02 28 00 13 02 d1]-> .8. .(..... 0020 b6 4f 00 16 b6 f7 1d 51 00 16 b6 f4 eb a0 50 c3 0.....Q.....P- 0030 00 01 aa 03 00 00 00 00 00 45 00 00 28 17 d9E.(..... 0040 40 01 31 06 fa 5d 80 77 f5 0c 00 a0 6d 00 50 @1-1.]w.....m-P 0050 09 ea ae 8f de 40 71 af ce fa 50 19 20 87 66q.....f 0060 00 00 00 00 00 00 00 9c de 38 ae8.
---	--

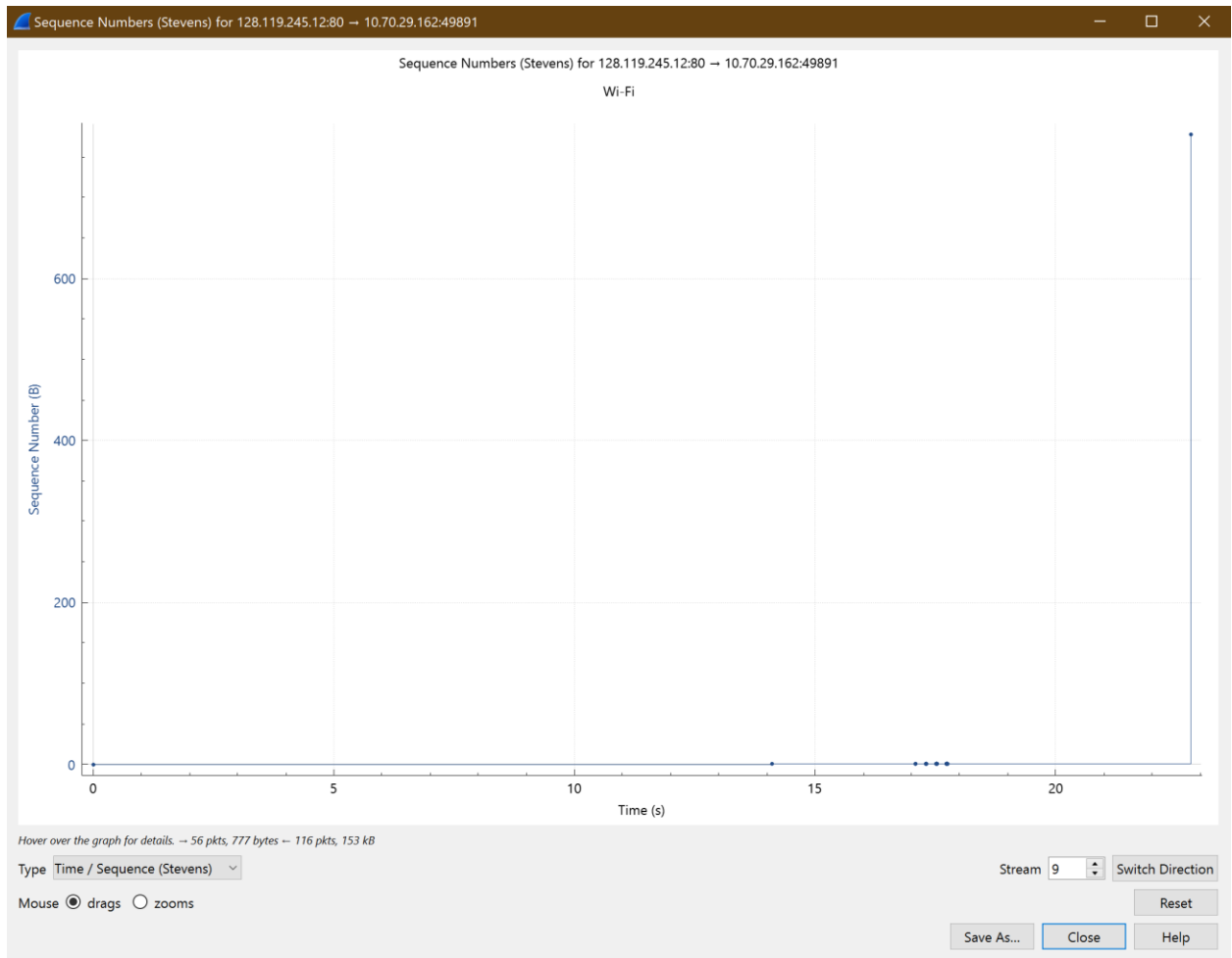
12. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

- Throughput measures how much data is transferred per unit time in a TCP connection. It is calculated using the total bytes sent and the duration of the transfer.
- I opened Wireshark and went to Statistics - Conversations - TCP Tab to find the Total Bytes Transferred. I noted the timestamp of the first and last packet to calculate the Total Time Taken by subtracting the first timestamp from the last.
- I used the formula $\text{Throughput} = \text{Total Bytes Transferred} / \text{Total Time Taken}$ to determine the throughput in bytes per second (Bps).
- When it was needed, I converted Bps to bps by multiplying by 8.
- Total Bytes Transferred: 180154.
- Total Time Taken: 21.4611
- Therefore: Throughput is 8394.4439 bytes/sec

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A	Flows
128.119.101.5	80	192.168.1.109	2543	5	2 kB	4	16	31.25%	2	2 kB	3	306 bytes	32.903185	0.1882	67 kbps	13 kbps	4
192.168.1.109	2546	64.233.187.104	80	8	3 kB	7	19	42.11%	5	1 kB	3	2 kB	32.981949	0.4386	24 kbps	37 kbps	4
192.168.1.109	2541	128.119.240.19	80	8	1 kB	2	23	34.78%	5	920 bytes	3	326 bytes	32.808574	0.1233	59 kbps	21 kbps	2
192.168.1.109	2542	128.119.240.19	80	6	632 bytes	3	23	26.09%	3	306 bytes	3	326 bytes	32.869262	0.0955	25 kbps	27 kbps	2
192.168.1.109	2544	128.119.240.19	80	4	422 bytes	5	8	50.00%	2	204 bytes	2	218 bytes	32.957207	0.0599	27 kbps	29 kbps	1
192.168.1.109	2545	128.119.240.19	80	12	1 kB	6	32	37.50%	10	1 kB	2	218 bytes	32.958196	0.1625	50 kbps	10 kbps	1
192.168.1.109	2547	128.119.240.19	80	9	938 bytes	8	28	32.14%	6	612 bytes	3	326 bytes	33.001575	0.1308	37 kbps	19 kbps	2
192.168.1.109	2548	128.119.240.19	80	5	530 bytes	9	11	45.45%	2	204 bytes	3	326 bytes	33.099063	0.0648	25 kbps	40 kbps	2
192.168.1.109	2549	128.119.240.19	80	6	632 bytes	10	13	46.15%	3	306 bytes	3	326 bytes	33.115208	0.0701	34 kbps	37 kbps	2
192.168.1.109	2538	128.119.245.12	80	60	8 kB	0	230	26.09%	56	6 kB	4	2 kB	24.811093	20.1274	2270 bits/s	736 bits/s	4

13. Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP's slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behavior of TCP that we've studied in the text.

- In the Time-Sequence Graph (Stevens), I observed a slow increase in the sequence number initially, indicating the congestion avoidance phase, where TCP increases the congestion window linearly. TCP's slow start begins at time $t = 14$ seconds and ends at $t = 25$ seconds.
- At time $t = 25$ s, there was a sudden rise, suggesting a possible transition to fast recovery or a retransmission event, where TCP injected more data into the network after detecting lost or delayed packets.
- This behavior differs from the ideal TCP model, where slow start should show exponential growth until reaching a threshold. In my trace, the linear growth before the sudden rise suggests that external factors like network conditions, RTT variations, or delayed ACKs influenced TCP's behavior.
-



14. Answer each of two questions above for the trace that you have gathered when you transferred a file from your computer to gaia.cs.umass.edu

- In my trace, I observed a sudden exponential growth in the sequence number vs. time plot, which indicates the TCP slow start phase.
- Compared to the ideal TCP model, my measured data showed some variations in growth due to network delay, packet loss, or varying RTTs, which are not always accounted for in theoretical models.

