

Ahsanullah University of Science & Technology



Department of Computer Science & Engineering

Program: Bachelor of Science in Computer Science and Engineering

Assignment on Wireshark

Course No : CSE 4102
Course Title : Computer Networks Lab
Topic Name : Wireshark
Date of Submission : 04.09.2022

Submitted to:

Raihan Tanvir

Lecturer, Department of CSE, AUST.

Mr. Tanvir Ahmed

Assistant Professor, Department of CSE, AUST.

Submitted by:

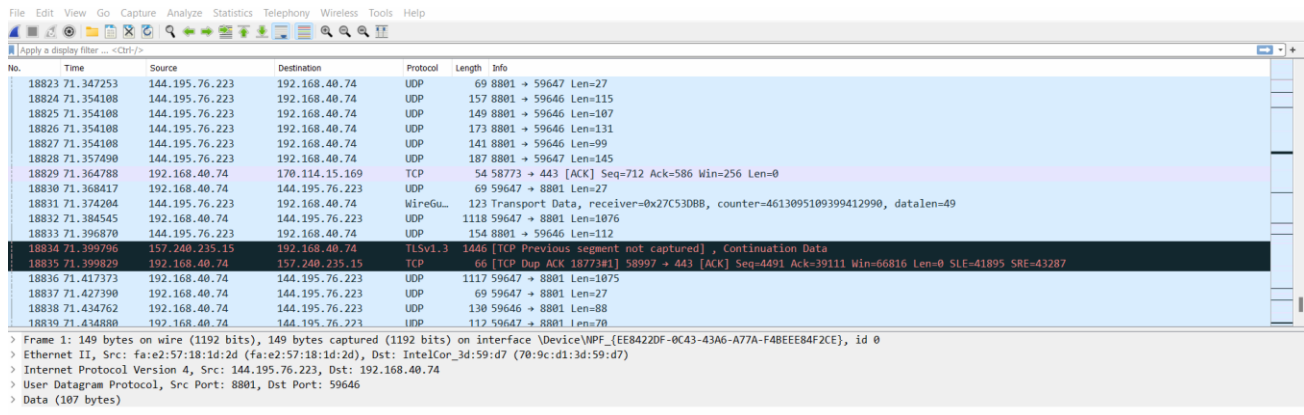
Name: S. M. Tasnimul Hasan

ID : 18.02.04.142

Question:a

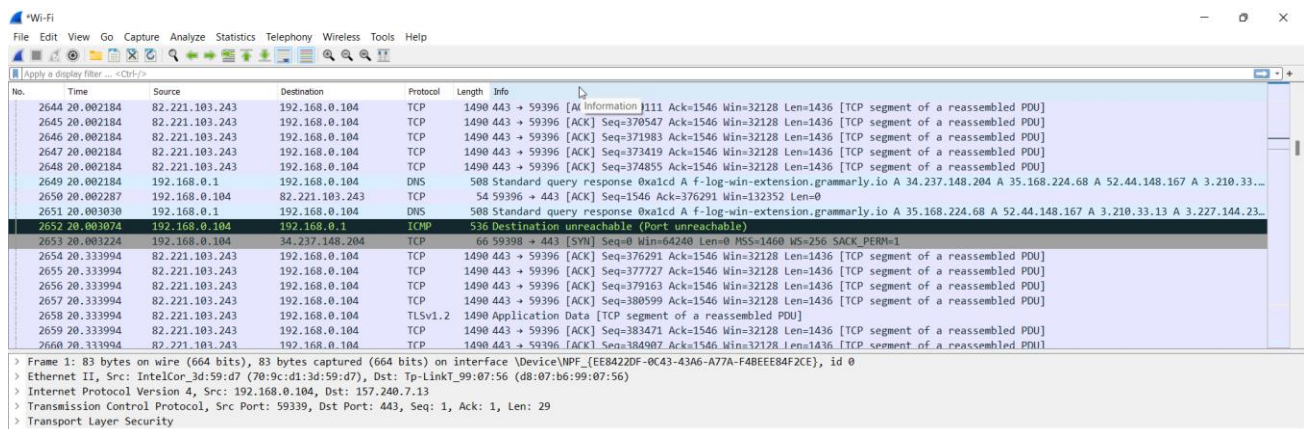
Start your web browser and start Wireshark and capture packets. Browse some websites and list 10 different protocols that appear in the protocol column in the unfiltered packet-listing window.

Answer:



No.	Time	Source	Destination	Protocol	Length	Info
18823	71.347253	144.195.76.223	192.168.40.74	UDP	69	8801 → 59647 Len=27
18824	71.354108	144.195.76.223	192.168.40.74	UDP	157	8801 → 59646 Len=115
18825	71.354108	144.195.76.223	192.168.40.74	UDP	149	8801 → 59646 Len=107
18826	71.354108	144.195.76.223	192.168.40.74	UDP	173	8801 → 59646 Len=131
18827	71.354108	144.195.76.223	192.168.40.74	UDP	141	8801 → 59646 Len=99
18828	71.357490	144.195.76.223	192.168.40.74	UDP	187	8801 → 59647 Len=145
18829	71.364788	192.168.40.74	170.114.15.169	TCP	54	58773 → 443 [ACK] Seq=712 Ack=586 Win=256 Len=0
18830	71.368417	192.168.40.74	144.195.76.223	UDP	69	59647 → 8801 Len=27
18831	71.374204	144.195.76.223	192.168.40.74	WireGu...	123	Transport Data, receiver=0x27C53DB8, counter=4613095109399412990, datalen=49
18832	71.384545	192.168.40.74	144.195.76.223	UDP	1118	59647 → 8801 Len=1076
18833	71.396870	144.195.76.223	192.168.40.74	UDP	154	8801 → 59646 Len=112
18834	71.399796	157.240.235.15	192.168.40.74	TLSv1.3	1446	[TCP Previous segment not captured], Continuation Data
18835	71.399829	192.168.40.74	157.240.235.15	TCP	66	[TCP Dup ACK 18773#1] 58997 → 443 [ACK] Seq=4491 Ack=39111 Win=66816 Len=0 SLE=41895 SRE=43287
18836	71.417373	192.168.40.74	144.195.76.223	UDP	1117	59647 → 8801 Len=1075
18837	71.427390	192.168.40.74	144.195.76.223	UDP	69	59647 → 8801 Len=27
18838	71.434762	192.168.40.74	144.195.76.223	UDP	130	59646 → 8801 Len=88
18839	71.434880	192.168.40.74	144.195.76.223	UDP	117	59647 → 8801 Len=70

> Frame 1: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{EE8422DF-0C43-43A6-A77A-F4BEE84F2CE}, id 0
> Ethernet II, Src: fa:e2:57:18:1d:2d (fa:e2:57:18:1d:2d), Dst: IntelCor_3d:59:d7 (70:9c:d1:3d:59:d7)
> Internet Protocol Version 4, Src: 144.195.76.223, Dst: 192.168.40.74
> User Datagram Protocol, Src Port: 8801, Dst Port: 59646
> Data (107 bytes)



No.	Time	Source	Destination	Protocol	Length	Info
2644	20.002184	82.221.103.243	192.168.0.104	TCP	1490	443 → 59396 [A Information #111 Ack=1546 Win=32128 Len=1436 [TCP segment of a reassembled PDU]
2645	20.002184	82.221.103.243	192.168.0.104	TCP	1490	443 → 59396 [ACK] Seq=370547 Ack=1546 Win=32128 Len=1436 [TCP segment of a reassembled PDU]
2646	20.002184	82.221.103.243	192.168.0.104	TCP	1490	443 → 59396 [ACK] Seq=371983 Ack=1546 Win=32128 Len=1436 [TCP segment of a reassembled PDU]
2647	20.002184	82.221.103.243	192.168.0.104	TCP	1490	443 → 59396 [ACK] Seq=373419 Ack=1546 Win=32128 Len=1436 [TCP segment of a reassembled PDU]
2648	20.002184	82.221.103.243	192.168.0.104	TCP	1490	443 → 59396 [ACK] Seq=374855 Ack=1546 Win=32128 Len=1436 [TCP segment of a reassembled PDU]
2649	20.002184	192.168.0.1	192.168.0.104	DNS	508	Standard query response 0xa1cd A f-log-win-extension.grammarly.io A 34.237.148.204 A 35.168.224.68 A 52.44.148.167 A 3.210.33.13
2650	20.002287	192.168.0.104	82.221.103.243	TCP	54	59396 → 443 [ACK] Seq=1546 Ack=376291 Win=132352 Len=0
2651	20.003030	192.168.0.1	192.168.0.104	DNS	508	Standard query response 0xa1cd A f-log-win-extension.grammarly.io A 35.168.224.68 A 52.44.148.167 A 3.210.33.13 A 3.227.144.23
2652	20.003074	192.168.0.104	192.168.0.1	ICMP	536	Destination unreachable (Port unreachable)
2653	20.003224	192.168.0.104	34.237.148.204	TCP	66	59398 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2654	20.333994	82.221.103.243	192.168.0.104	TCP	1490	443 → 59396 [ACK] Seq=376291 Ack=1546 Win=32128 Len=1436 [TCP segment of a reassembled PDU]
2655	20.333994	82.221.103.243	192.168.0.104	TCP	1490	443 → 59396 [ACK] Seq=377727 Ack=1546 Win=32128 Len=1436 [TCP segment of a reassembled PDU]
2656	20.333994	82.221.103.243	192.168.0.104	TCP	1490	443 → 59396 [ACK] Seq=379163 Ack=1546 Win=32128 Len=1436 [TCP segment of a reassembled PDU]
2657	20.333994	82.221.103.243	192.168.0.104	TCP	1490	443 → 59396 [ACK] Seq=380599 Ack=1546 Win=32128 Len=1436 [TCP segment of a reassembled PDU]
2658	20.333994	82.221.103.243	192.168.0.104	TLSv1.2	1490	Application Data [TCP segment of a reassembled PDU]
2659	20.333994	82.221.103.243	192.168.0.104	TCP	1490	443 → 59396 [ACK] Seq=383471 Ack=1546 Win=32128 Len=1436 [TCP segment of a reassembled PDU]
2660	20.333994	82.221.103.243	192.168.0.104	TCP	1490	443 → 59396 [ACK] Seq=384907 Ack=1546 Win=32128 Len=1436 [TCP segment of a reassembled PDU]

> Frame 1: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{EE8422DF-0C43-43A6-A77A-F4BEE84F2CE}, id 0
> Ethernet II, Src: IntelCor_3d:59:d7 (70:9c:d1:3d:59:d7), Dst: Tp-LinkT_99:07:56 (d8:07:b6:99:07:56)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 157.240.7.13
> Transmission Control Protocol, Src Port: 59393, Dst Port: 443, Seq: 1, Ack: 1, Len: 29
> Transport Layer Security

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl>F

No.	Time	Source	Destination	Protocol	Length	Info
4184	55.352397	157.240.7.13	192.168.0.104	TCP	60	443 → 59339 [ACK] Seq=226 Ack=643 Win=365 Len=0
4185	55.458147	192.168.0.104	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.258 for any sources
4186	57.217357	192.168.0.104	18.161.94.173	TLSv1.3	401	Application Data
4187	57.217533	192.168.0.104	18.161.94.173	TLSv1.3	528	Application Data
4188	57.411852	192.168.0.104	82.221.103.243	TCP	55	[TCP Keep-Alive] 59397 → 443 [ACK] Seq=643 Ack=5803 Win=132096 Len=1
4189	57.414123	18.161.94.173	192.168.0.104	TCP	60	443 → 59402 [ACK] Seq=6589 Ack=1344 Win=70144 Len=0
4190	57.414123	18.161.94.173	192.168.0.104	TCP	60	443 → 59402 [ACK] Seq=6589 Ack=1818 Win=71168 Len=0
4191	57.415657	Tp-LinkT_99:07:56	IntelCor_3d:59:d7	ARP	42	Who has 192.168.0.104? Tell 192.168.0.1
4192	57.415699	IntelCor_3d:59:d7	Tp-LinkT_99:07:56	ARP	42	192.168.0.104 is at 70:9c:d1:3d:59:d7
4193	57.460801	18.161.94.173	192.168.0.104	TLSv1.3	523	Application Data
4194	57.501687	192.168.0.104	18.161.94.173	TLSv1.3	401	Application Data
4195	57.501758	192.168.0.104	192.168.0.1	DNS	77	Standard query 0x5a6b A api.playanext.com
4196	57.501885	192.168.0.104	18.161.94.173	TLSv1.3	421	Application Data
4197	57.535234	192.168.0.104	192.168.0.1	DNS	77	Standard query 0x5a6b A api.playanext.com
4198	57.620558	192.168.0.1	192.168.0.104	DNS	478	Standard query response 0x5a6b A api.playanext.com CNAME diatxiff5avezsq.cloudfront.net A 54.182.0.115 A 54.182.0.10 A 54.182.0.1
4199	57.621721	192.168.0.104	54.182.0.115	TCP	66	59404 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4200	57.663567	82.221.103.243	192.168.0.104	TCP	66	[TCP Keep-Alive] ACK 443 → 59397 [ACK] Seq=5803 Ack=644 Win=30336 Len=0 SIF=643 SRF=644

> Frame 1: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{EE8422DF-0C43-43A6-A77A-F48EE84F2CE}, id 0
 > Ethernet II, Src: IntelCor_3d:59:d7 (70:9c:d1:3d:59:d7), Dst: Tp-LinkT_99:07:56 (d8:07:b6:99:07:56)
 > Internet Protocol Version 4, Src: 192.168.0.104, Dst: 157.240.7.13
 > Transmission Control Protocol, Src Port: 59339, Dst Port: 443, Seq: 1, Ack: 1, Len: 29
 > Transport Layer Security

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl>F

No.	Time	Source	Destination	Protocol	Length	Info
2326	13.471422	192.168.0.104	82.221.103.243	TCP	54	59396 → 443 [ACK] Seq=1546 Ack=73295 Win=132352 Len=0
2327	13.471521	192.168.0.104	13.227.138.29	TCP	54	59386 → 443 [ACK] Seq=5124 Ack=1310708 Win=132096 Len=0
2328	13.471562	192.168.0.104	82.221.103.243	TCP	54	59396 → 443 [ACK] Seq=1546 Ack=80475 Win=132352 Len=0
2329	13.498540	192.168.0.104	13.227.138.29	TLSv1.3	188	Application Data
2330	13.501300	192.168.0.104	13.227.138.29	TLSv1.3	160	Application Data
2331	13.502285	192.168.0.104	13.227.138.29	TLSv1.3	123	Application Data
2332	13.505121	192.168.0.104	13.227.138.29	TLSv1.3	157	Application Data
2333	13.507094	192.168.0.104	13.227.138.29	TLSv1.3	161	Application Data
2334	13.630967	192.168.0.104	192.168.0.255	NBNS	92	Name query NB SAMIT-PC<lc>
2335	13.801096	192.168.0.104	13.227.138.29	TCP	573	[TCP Retransmission] 59386 → 443 [PSH, ACK] Seq=5124 Ack=1310708 Win=132096 Len=519
2336	13.802123	13.227.138.29	192.168.0.104	TLSv1.3	624	Application Data
2337	13.802123	13.227.138.29	192.168.0.104	TCP	60	443 → 59386 [ACK] Seq=1311278 Ack=5643 Win=77824 Len=0
2338	13.802123	13.227.138.29	192.168.0.104	TLSv1.3	624	Application Data
2339	13.802123	13.227.138.29	192.168.0.104	TCP	1494	443 → 59386 [ACK] Seq=1311848 Ack=5643 Win=77824 Len=1440 [TCP segment of a reassembled PDU]
2340	13.802123	13.227.138.29	192.168.0.104	TLSv1.3	239	Application Data
2341	13.802123	13.227.138.29	192.168.0.104	TLSv1.3	85	Application Data
2342	13.802123	13.227.138.29	192.168.0.104	TCP	1494	443 → 59386 [ACK] Seq=1313504 Ack=5643 Win=77824 Len=1440 [TCP segment of a reassembled PDU]

> Frame 1: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{EE8422DF-0C43-43A6-A77A-F48EE84F2CE}, id 0
 > Ethernet II, Src: IntelCor_3d:59:d7 (70:9c:d1:3d:59:d7), Dst: Tp-LinkT_99:07:56 (d8:07:b6:99:07:56)
 > Internet Protocol Version 4, Src: 192.168.0.104, Dst: 157.240.7.13
 > Transmission Control Protocol, Src Port: 59339, Dst Port: 443, Seq: 1, Ack: 1, Len: 29
 > Transport Layer Security

List of 10 different protocols:

1. TCP
2. ICMP
3. TLSv1.2
4. UDP
5. ARP
6. Wire Ground
7. DNS
8. TLSv1.3
9. IGMPv3
10. NBNS

Question:b

Filter the packets having DNS in protocol field, select a row and answer the following questions.

i. Which port is used as source port?

ii. What is the size of IPv4 header length?

Answer:

i) Source port: 57577

The screenshot shows the Wireshark interface with a packet capture of DNS traffic. The packet list pane shows a list of packets, with the selected packet (No. 10) having a source port of 57577. The packet details pane shows the following information:

- Frame 10: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF-{EE8422DF-0C43-43A6-A77A-F4BEE84F2CE}, id 0
- Ethernet II, Src: IntelCor_3d:59:d7 (70:9c:d1:3d:59:d7), Dst: Tp-LinkT_99:07:56 (d8:07:b6:99:07:56)
- Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.1
- User Datagram Protocol, Src Port: 57577, Dst Port: 53
- Source Port: 57577
- Destination Port: 53
- Length: 42
- Checksum: 0x81f5 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 2]
- [Timestamps]
- UDP payload (34 bytes)
- Domain Name System (query)

ii) IPv4 Header Length: 20 bytes

The screenshot shows the Wireshark interface with a packet capture of DNS traffic. The packet list pane shows a list of packets, with the selected packet (No. 10) having a source port of 57577. The packet details pane shows the following information:

- Frame 10: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF-{EE8422DF-0C43-43A6-A77A-F4BEE84F2CE}, id 0
- Ethernet II, Src: IntelCor_3d:59:d7 (70:9c:d1:3d:59:d7), Dst: Tp-LinkT_99:07:56 (d8:07:b6:99:07:56)
- Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.1
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 62
- Identification: 0x5ea9 (24233)
- Flags: 0x00
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 128
- Protocol: UDP (17)
- Header Checksum: 0x0000 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.0.104
- Destination Address: 192.168.0.1
- User Datagram Protocol, Src Port: 57577, Dst Port: 53
- Domain Name System (query)

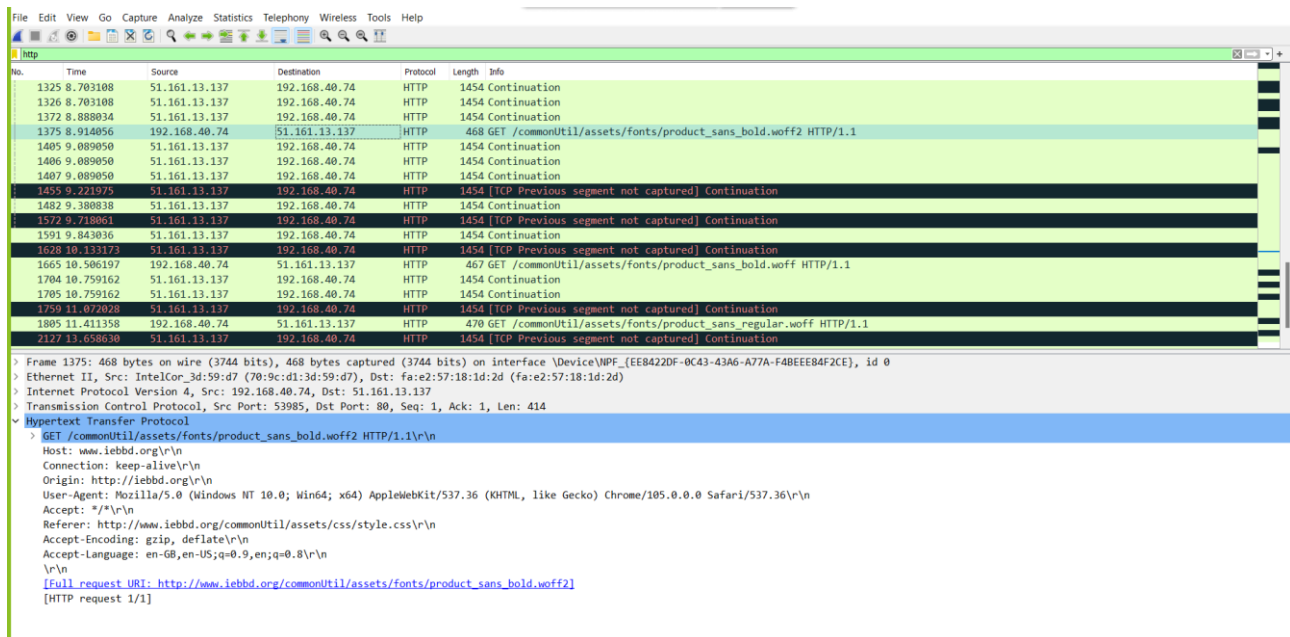
Question: c

Browse iebbdd.org and answer the following questions.

- What is the IP address of iebbdd.org.
- How long did it take from when the first HTTP GET message was sent until the HTTP OK reply was received? In case, HTTP OK is not received then check for last HTTP Continuation.
- What is the frame length of first HTTP GET message.
- Now, visit the login page and enter your ID in the Member ID field and your name in password field. Then hit the “login” button. Find out the data that was entered in the form using Wireshark. (include snapshot of the login form with data filled in)
- Find out the port number on which the HTTP requests are made.

Answer :

i) IP address of iebbdd.org is: 51.161.13.137



ii) It takes $2.2996s - 0.7074s = 1.5922s$

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: http

No.	Time	Source	Destination	Protocol	Length	Info
1326	8.783108	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1372	8.888934	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1375	8.914056	192.168.40.74	51.161.13.137	HTTP	468	GET /commonUtil/assets/fonts/product_sans_bold.woff2 HTTP/1.1
1405	9.089050	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1406	9.089050	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1407	9.089050	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1455	9.221975	51.161.13.137	192.168.40.74	HTTP	1454	[TCP Previous segment not captured] Continuation
1482	9.380838	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1572	9.718061	51.161.13.137	192.168.40.74	HTTP	1454	[TCP Previous segment not captured] Continuation
1591	9.843036	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1628	10.133173	51.161.13.137	192.168.40.74	HTTP	1454	[TCP Previous segment not captured] Continuation
1665	10.506197	192.168.40.74	51.161.13.137	HTTP	467	GET /commonUtil/assets/fonts/product_sans_bold.woff HTTP/1.1
1784	10.759162	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1785	10.759162	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1759	11.072020	51.161.13.137	192.168.40.74	HTTP	1454	[TCP Previous segment not captured] Continuation
1805	11.411358	192.168.40.74	51.161.13.137	HTTP	470	GET /commonUtil/assets/fonts/product_sans_regular.woff HTTP/1.1
2127	13.658630	51.161.13.137	192.168.40.74	HTTP	1454	[TCP Previous segment not captured] Continuation
2129	13.659030	51.161.13.137	192.168.40.74	HTTP	1454	Continuation

▼ Frame 1665: 467 bytes on wire (3736 bits), 467 bytes captured (3736 bits) on interface \Device\NPF_{EE8422DF-0C43-43A6-A77A-F4BEE84F2CE}, id 0

> Interface id: 0 (\Device\NPF_{EE8422DF-0C43-43A6-A77A-F4BEE84F2CE})

Encapsulation type: Ethernet (1)

Arrival Time: Sep 4, 2022 23:01:02.299600000 Bangladesh Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1662310862.299600000 seconds

[Time delta from previous captured frame: 0.000324000 seconds]

[Time delta from previous displayed frame: 0.37024000 seconds]

[Time since reference or first frame: 10.506197000 seconds]

Frame Number: 1665

Frame Length: 467 bytes (3736 bits)

Capture Length: 467 bytes (3736 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_3d:59:d7 (70:9c:d1:3d:59:d7), Dst: fa:e2:57:18:1d:2d (fa:e2:57:18:1d:2d)

> Internet Protocol Version 4, Src: 192.168.40.74, Dst: 51.161.13.137

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: http

No.	Time	Source	Destination	Protocol	Length	Info
1326	8.783108	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1372	8.888934	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1375	8.914056	192.168.40.74	51.161.13.137	HTTP	468	GET /commonUtil/assets/fonts/product_sans_bold.woff2 HTTP/1.1
1405	9.089050	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1406	9.089050	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1407	9.089050	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1455	9.221975	51.161.13.137	192.168.40.74	HTTP	1454	[TCP Previous segment not captured] Continuation
1482	9.380838	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1572	9.718061	51.161.13.137	192.168.40.74	HTTP	1454	[TCP Previous segment not captured] Continuation
1591	9.843036	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1628	10.133173	51.161.13.137	192.168.40.74	HTTP	1454	[TCP Previous segment not captured] Continuation
1665	10.506197	192.168.40.74	51.161.13.137	HTTP	467	GET /commonUtil/assets/fonts/product_sans_bold.woff HTTP/1.1
1784	10.759162	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1785	10.759162	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1759	11.072020	51.161.13.137	192.168.40.74	HTTP	1454	[TCP Previous segment not captured] Continuation
1805	11.411358	192.168.40.74	51.161.13.137	HTTP	470	GET /commonUtil/assets/fonts/product_sans_regular.woff HTTP/1.1
2127	13.658630	51.161.13.137	192.168.40.74	HTTP	1454	[TCP Previous segment not captured] Continuation
2129	13.659030	51.161.13.137	192.168.40.74	HTTP	1454	Continuation

▼ Frame 1375: 468 bytes on wire (3744 bits), 468 bytes captured (3744 bits) on interface \Device\NPF_{EE8422DF-0C43-43A6-A77A-F4BEE84F2CE}, id 0

> Interface id: 0 (\Device\NPF_{EE8422DF-0C43-43A6-A77A-F4BEE84F2CE})

Encapsulation type: Ethernet (1)

Arrival Time: Sep 4, 2022 23:01:00.707467000 Bangladesh Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1662310860.707467000 seconds

[Time delta from previous captured frame: 0.012971000 seconds]

[Time delta from previous displayed frame: 0.02602000 seconds]

[Time since reference or first frame: 8.914056000 seconds]

Frame Number: 1375

Frame Length: 468 bytes (3744 bits)

Capture Length: 468 bytes (3744 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_3d:59:d7 (70:9c:d1:3d:59:d7), Dst: fa:e2:57:18:1d:2d (fa:e2:57:18:1d:2d)

> Internet Protocol Version 4, Src: 192.168.40.74, Dst: 51.161.13.137

iii) Frame length of the first HTTP GET message: 543 bytes

No.	Time	Source	Destination	Protocol	Length	Info
1405	9.089050	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1406	9.089050	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1407	9.089050	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1455	9.221975	51.161.13.137	192.168.40.74	HTTP	1454	[TCP Previous segment not captured] Continuation
1482	9.380838	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1572	9.718001	51.161.13.137	192.168.40.74	HTTP	1454	[TCP Previous segment not captured] Continuation
1591	9.843036	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1628	10.133173	51.161.13.137	192.168.40.74	HTTP	1454	[TCP Previous segment not captured] Continuation
1704	10.759162	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1705	10.759162	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
1759	11.072028	51.161.13.137	192.168.40.74	HTTP	1454	[TCP Previous segment not captured] Continuation
2122	13.659030	51.161.13.137	192.168.40.74	HTTP	1454	[TCP Previous segment not captured] Continuation
2129	13.659030	51.161.13.137	192.168.40.74	HTTP	1454	Continuation
821	5.576459	192.168.40.74	51.161.13.137	HTTP	543	GET / HTTP/1.1
1170	7.802141	192.168.40.74	51.161.13.137	HTTP	471	GET /commonUtil/assets/fonts/product_sans_regular.woff2 HTTP/1.1
1375	8.914056	192.168.40.74	51.161.13.137	HTTP	468	GET /commonUtil/assets/fonts/product_sans_bold.woff2 HTTP/1.1
1665	10.506197	192.168.40.74	51.161.13.137	HTTP	467	GET /commonUtil/assets/fonts/product_sans_bold.woff HTTP/1.1
1805	11.411358	192.168.40.74	51.161.13.137	HTTP	470	GET /commonUtil/assets/fonts/product_sans_regular.woff HTTP/1.1

Frame 821: 543 bytes on wire (4344 bits), 543 bytes captured (4344 bits) on interface \Device\NPF_{EE8422DF-0C43-43A6-A77A-F4BEE84F2CE}, id 0
Interface id: 0 (\\Device\NPF_{EE8422DF-0C43-43A6-A77A-F4BEE84F2CE})
Encapsulation type: Ethernet (1)
Arrival Time: Sep 4, 2022 23:00:57.369870000 Bangladesh Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1662310857.369870000 seconds
[Time delta from previous captured frame: 0.000351000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 5.576459000 seconds]
Frame Number: 821
Frame Length: 543 bytes (4344 bits)
Capture Length: 543 bytes (4344 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_3d:59:d7 (70:9c:d1:3d:59:d7), Dst: fa:e2:57:18:1d:2d (fa:e2:57:18:1d:2d)
> Internet Protocol Version 4, Src: 192.168.40.74, Dst: 51.161.13.137
Transfer Size: 543 bytes, Seq: 3000, Port: 80, Src: 192.168.40.74, Dst: 51.161.13.137

iv) Login form

IEB : The Institution of Engineers

← → ↻ 🔒 Not secure | iebd.org/member/login.jsp

Blood Bank Use App Contact Search Login

About Membership Networks Publications Committees News & Events Gallery Old Site

Member Login Instructions

- ✓ Please Enter IEB Membership ID and password to Login into the Member Account Dashboard.
- ✓ If you are Fellow, Member or Associate Member, Member ID Should start with F, M or A, then put the numerical character without using and special characters like (/,-, space). Example: F54787. If your ID number has only 4 digits numerical character, then just add a "0" before the numerical character and after F, M or A. Example: M09239.)
- ✓ If you don't have the password Click Forgot password or Get existing password, then follow as instructed in the next page.

Member Login

Member ID or Password does not match>Please follow the instructions listed in the left

180204142

Login

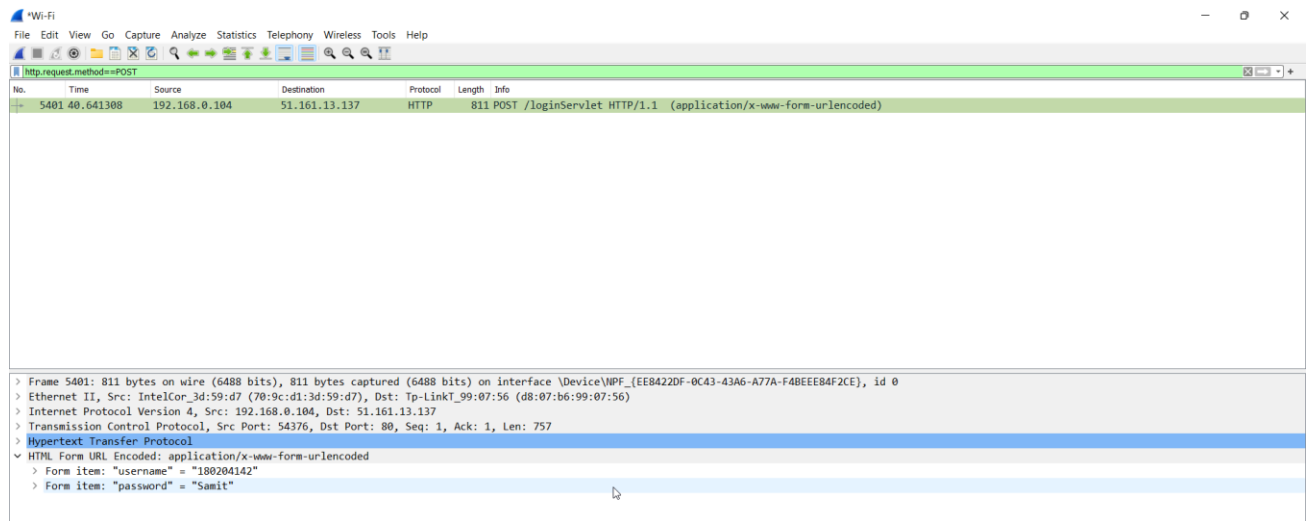
[Forgot password?](#)

[Get existing member password](#)

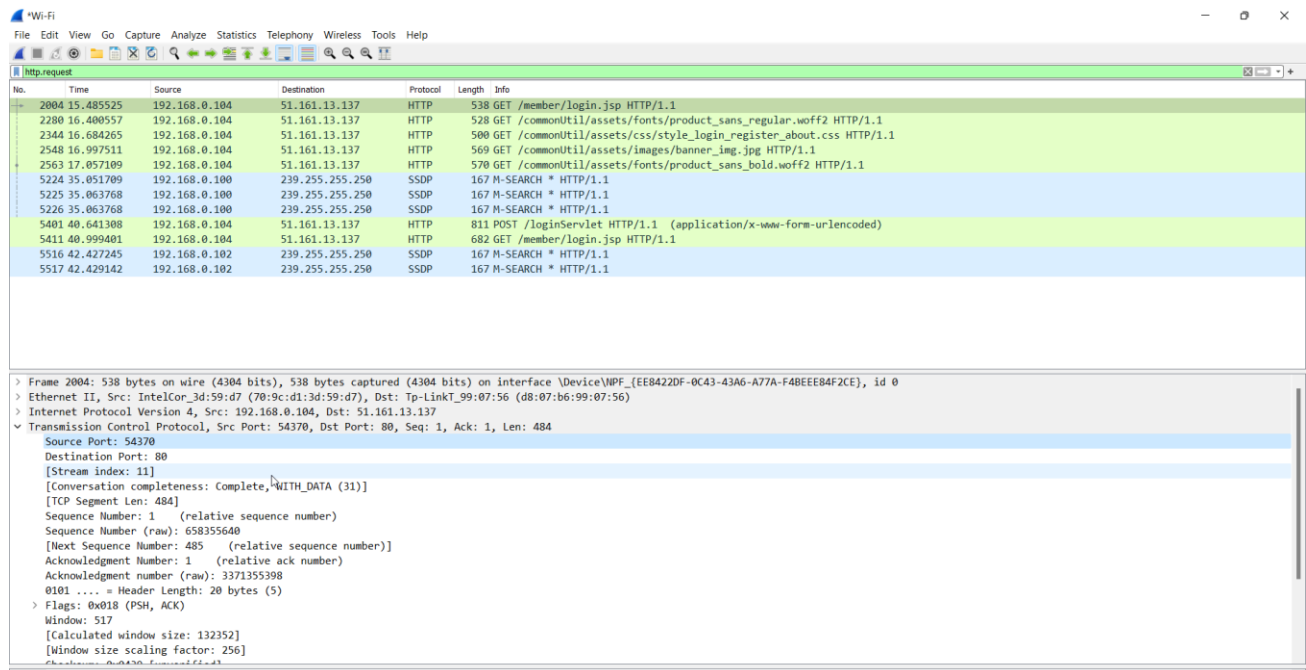
[Apply Membership](#)

Username: 180204142

Password: Samit



v) Port number on which the HTTP requests are made: 54370



Question :d

Start your torrent client application (qBittorrent, utorrent, etc.). Set incoming port address to last five digits of your student ID from the preference/option. Download any content from any torrent site if you just installed the torrent client. Now filter the packets transmitted using the torrent client.

Answer :

The image shows two screenshots. The top screenshot is the qBittorrent Options dialog, and the bottom screenshot is a Wireshark packet capture.

qBittorrent Options Dialog:

- Peer connection protocol:** TCP and µTP
- Listening Port:** Port used for incoming connections: 4032 (Random)
- ☒ Use UPnP / NAT-PMP port forwarding from my router
- Connections Limits:**
 - ☒ Global maximum number of connections: 500
 - ☒ Maximum number of connections per torrent: 100
 - ☒ Global maximum number of upload slots: 20
 - ☒ Maximum number of upload slots per torrent: 4
- Proxy Server:**
 - Type: (None) Host: 0.0.0.0 Port: 8080
 - ☐ Use proxy for peer connections
 - ☐ Use proxy only for torrents
 - ☐ Authentication
 - Username: Password: Info: The password is saved unencrypted
- IP Filtering:**
 - ☐ Filter path (.dat, .p2p, .p2b):
 - Manually banned IP addresses...

Wireshark Packet Capture:

The packet capture shows a list of packets. The selected packet is 2631, which is a BitTorrent handshake. The packet details pane shows the following information:

- Frame 2631: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface \Device\NPF_{CA122675-0979-4AA3-8AD8-B254058FC51F}, id 0
- Ethernet II, Src: LiteonTe_73:06:ed (b8:ee:65:73:06:ed), Dst: Tp-LinkT_92:c4:1e (40:3f:8c:92:c4:1e)
- Internet Protocol Version 4, Src: 192.168.0.105, Dst: 47.54.53.227
- Transmission Control Protocol, Src Port: 65164, Dst Port: 6881, Seq: 1, Ack: 1, Len: 68
- BitTorrent

The packet bytes pane shows the raw data of the handshake, including the BitTorrent protocol version (1), the client version (qBittorrent/2.10.0), and the peer ID.