21CY681– Internet Protocol lab -10

Name: Ramya Ajay

Roll No: CB.EN.P2CYS22004

Title: Analyzing bit torrent and BHT protocols using wireshark

Date: 10/12/2022

3. Open Wireshark in the background by choosing the appropriate interface.

4. Then open your torrent file and start the download at least 20%. Stop the capture and document the answers to the following questions:

a. Give a detailed study about the working of BitTorrent in your downloading scenario.

BitTorrent peer-to-peer (P2P) protocol **finds users with files other users want and then downloads pieces of the files from those users simultaneously**.

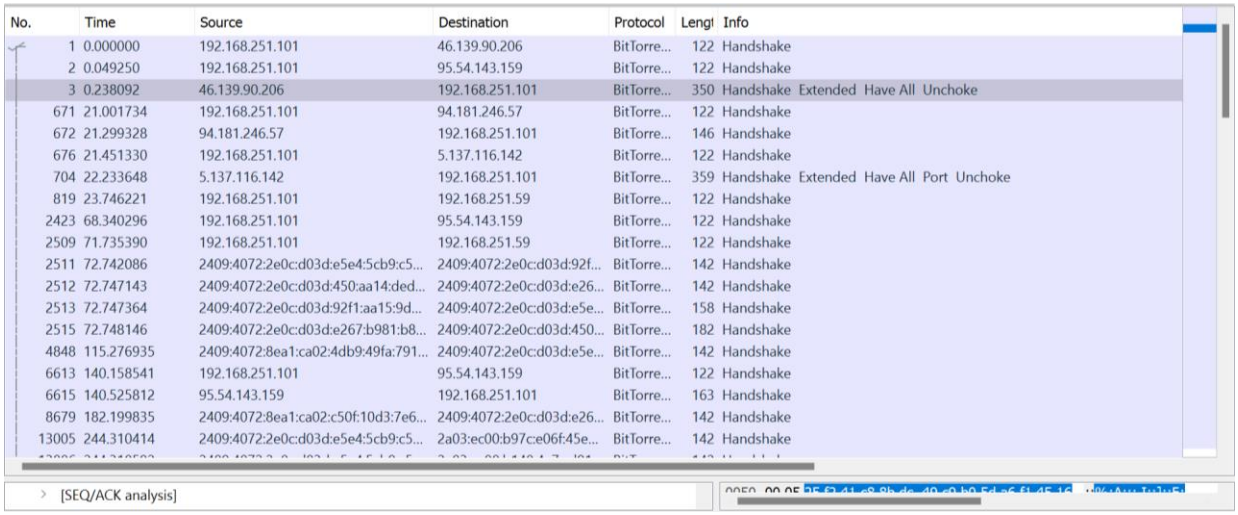
Once connected, a BitTorrent client downloads bits of the files in the torrent in small pieces, downloading all the data it can get. Once the BitTorrent client has some data, it can then begin to upload that data to other BitTorrent clients in the swarm. In this way, everyone downloading a torrent is also uploading the same torrent. This speeds up everyone's download speed.

b. Working of BitTorrent.

BitTorrent is a peer-to-peer protocol, which means that the computers in a BitTorrent "swarm" (a group of computers downloading and uploading the same torrent) transfer data between each other without the need for a central server.

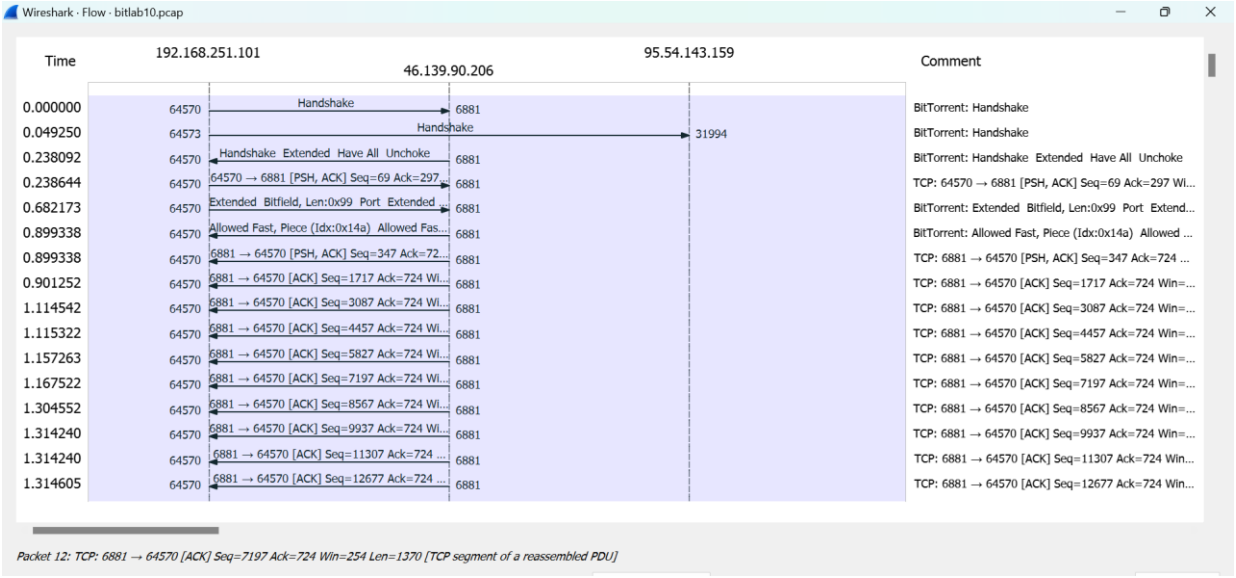
c. Protocol Level Analysis

BITTORENT –

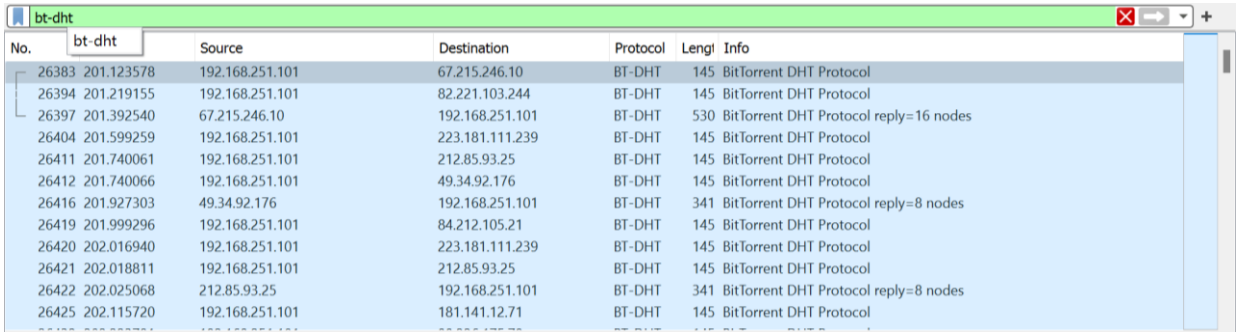


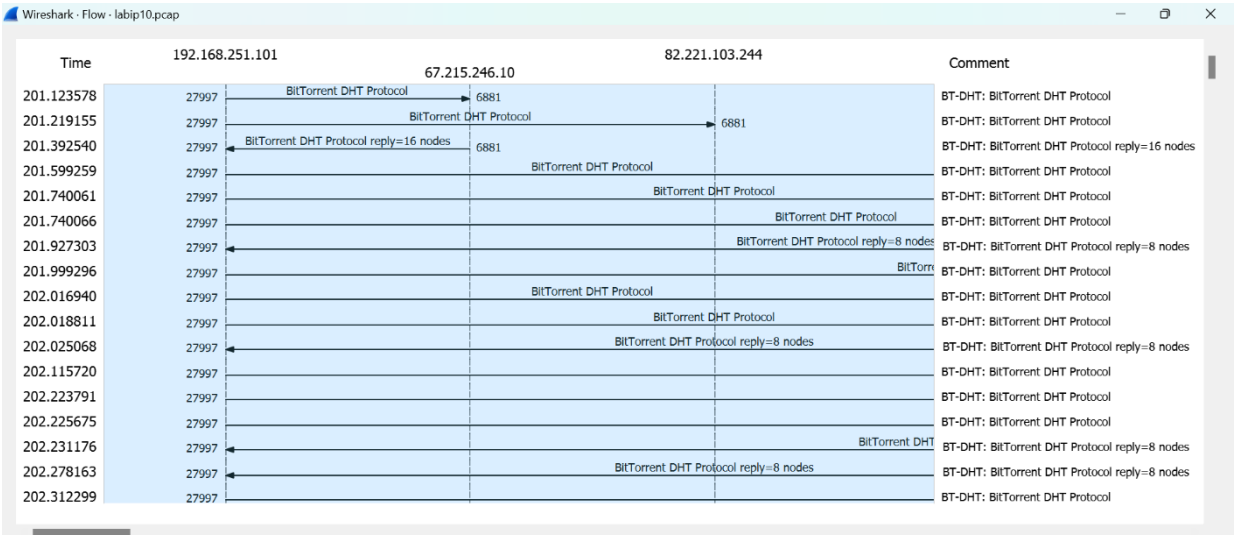
No.	Time	Source	Destination	Protocol	Lengt	Info
1	0.000000	192.168.251.101	46.139.90.206	BitTorre...	122	Handshake
2	0.049250	192.168.251.101	95.54.143.159	BitTorre...	122	Handshake
3	0.238092	46.139.90.206	192.168.251.101	BitTorre...	350	Handshake Extended Have All Unchoke
671	21.001734	192.168.251.101	94.181.246.57	BitTorre...	122	Handshake
672	21.299328	94.181.246.57	192.168.251.101	BitTorre...	146	Handshake
676	21.451330	192.168.251.101	5.137.116.142	BitTorre...	122	Handshake
704	22.233648	5.137.116.142	192.168.251.101	BitTorre...	359	Handshake Extended Have All Port Unchoke
819	23.746221	192.168.251.101	192.168.251.59	BitTorre...	122	Handshake
2423	68.340296	192.168.251.101	95.54.143.159	BitTorre...	122	Handshake
2509	71.735390	192.168.251.101	192.168.251.59	BitTorre...	122	Handshake
2511	72.742086	2409:4072:2e0c:d03d:e5e4:5cb9:c5...	2409:4072:2e0c:d03d:92f...	BitTorre...	142	Handshake
2512	72.747143	2409:4072:2e0c:d03d:450:aa14:ded...	2409:4072:2e0c:d03d:e26...	BitTorre...	142	Handshake
2513	72.747364	2409:4072:2e0c:d03d:92f1:aa15:9d...	2409:4072:2e0c:d03d:e5e...	BitTorre...	158	Handshake
2515	72.748146	2409:4072:2e0c:d03d:e267:b981:b8...	2409:4072:2e0c:d03d:450...	BitTorre...	182	Handshake
4848	115.276935	2409:4072:8ea1:ca02:4db9:49fa:791...	2409:4072:2e0c:d03d:e5e...	BitTorre...	142	Handshake
6613	140.158541	192.168.251.101	95.54.143.159	BitTorre...	122	Handshake
6615	140.525812	95.54.143.159	192.168.251.101	BitTorre...	163	Handshake
8679	182.199835	2409:4072:8ea1:ca02:c50f:10d3:7e6...	2409:4072:2e0c:d03d:e26...	BitTorre...	142	Handshake
13005	244.310414	2409:4072:2e0c:d03d:e5e4:5cb9:c5...	2a03:ec00:b97c:e06f:45e...	BitTorre...	142	Handshake

[SEQ/ACK analysis]

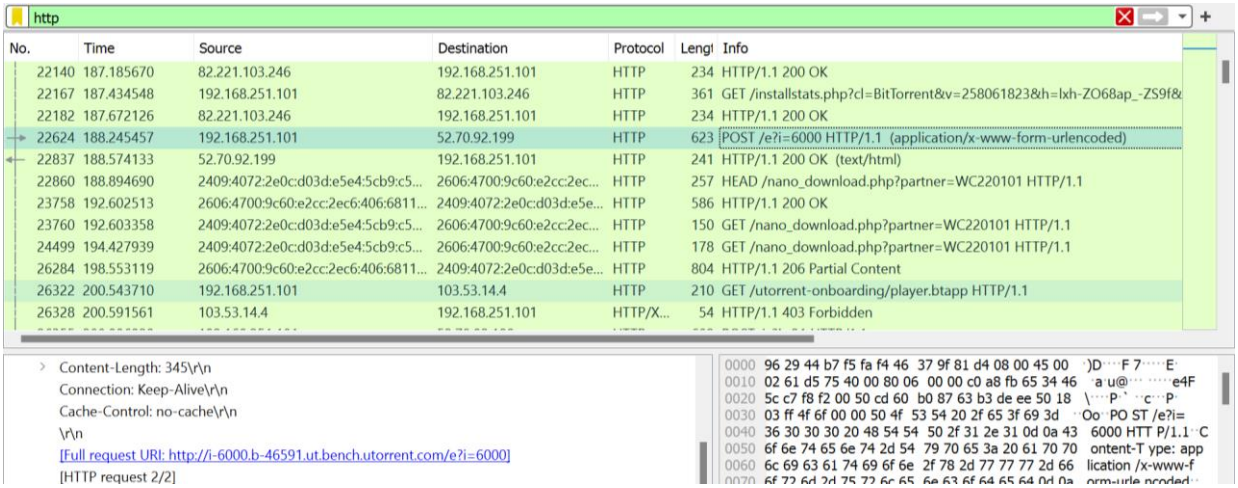

Wireshark · Flow · bitlab10.pcap
Time
192.168.251.101
46.139.90.206
95.54.143.159
Comment
0.000000 64570 Handshake 6881 BitTorrent: Handshake
0.049250 64573 Handshake 31994 BitTorrent: Handshake
0.238092 64570 Handshake Extended Have All Unchoke 6881 BitTorrent: Handshake Extended Have All Unchoke
0.238644 64570 64570 → 6881 [PSH, ACK] Seq=69 Ack=297 6881 TCP: 64570 → 6881 [PSH, ACK] Seq=69 Ack=297 Wi...
0.682173 64570 Extended Bitfield, Len:0x99 Port Extended 6881 BitTorrent: Extended Bitfield, Len:0x99 Port Extend...
0.899338 64570 Allowed Fast, Piece (Idx:0x14a) Allowed Fas... 6881 BitTorrent: Allowed Fast, Piece (Idx:0x14a) Allowed ...
0.899338 64570 6881 → 64570 [PSH, ACK] Seq=347 Ack=72... 6881 TCP: 6881 → 64570 [PSH, ACK] Seq=347 Ack=724 ...
0.901252 64570 6881 → 64570 [ACK] Seq=1717 Ack=724 Wi... 6881 TCP: 6881 → 64570 [ACK] Seq=1717 Ack=724 Win=...
1.114542 64570 6881 → 64570 [ACK] Seq=3087 Ack=724 Wi... 6881 TCP: 6881 → 64570 [ACK] Seq=3087 Ack=724 Win=...
1.115322 64570 6881 → 64570 [ACK] Seq=4457 Ack=724 Wi... 6881 TCP: 6881 → 64570 [ACK] Seq=4457 Ack=724 Win=...
1.157263 64570 6881 → 64570 [ACK] Seq=5827 Ack=724 Wi... 6881 TCP: 6881 → 64570 [ACK] Seq=5827 Ack=724 Win=...
1.167522 64570 6881 → 64570 [ACK] Seq=7197 Ack=724 Wi... 6881 TCP: 6881 → 64570 [ACK] Seq=7197 Ack=724 Win=...
1.304552 64570 6881 → 64570 [ACK] Seq=8567 Ack=724 Wi... 6881 TCP: 6881 → 64570 [ACK] Seq=8567 Ack=724 Win=...
1.314240 64570 6881 → 64570 [ACK] Seq=9937 Ack=724 Wi... 6881 TCP: 6881 → 64570 [ACK] Seq=9937 Ack=724 Win=...
1.314240 64570 6881 → 64570 [ACK] Seq=11307 Ack=724 ... 6881 TCP: 6881 → 64570 [ACK] Seq=11307 Ack=724 Win...
1.314605 64570 6881 → 64570 [ACK] Seq=12677 Ack=724 ... 6881 TCP: 6881 → 64570 [ACK] Seq=12677 Ack=724 Win...
Packet 12: TCP: 6881 → 64570 [ACK] Seq=7197 Ack=724 Win=254 Len=1370 [TCP segment of a reassembled PDU]

DHT


bt-dht
No. Source Destination Protocol Leng Info
26383 201.123578 192.168.251.101 67.215.246.10 BT-DHT 145 BitTorrent DHT Protocol
26394 201.219155 192.168.251.101 82.221.103.244 BT-DHT 145 BitTorrent DHT Protocol
26397 201.392540 67.215.246.10 192.168.251.101 BT-DHT 530 BitTorrent DHT Protocol reply=16 nodes
26404 201.599259 192.168.251.101 223.181.111.239 BT-DHT 145 BitTorrent DHT Protocol
26411 201.740061 192.168.251.101 212.85.93.25 BT-DHT 145 BitTorrent DHT Protocol
26412 201.740066 192.168.251.101 49.34.92.176 BT-DHT 145 BitTorrent DHT Protocol
26416 201.927303 49.34.92.176 192.168.251.101 BT-DHT 341 BitTorrent DHT Protocol reply=8 nodes
26419 201.999296 192.168.251.101 84.212.105.21 BT-DHT 145 BitTorrent DHT Protocol
26420 202.016940 192.168.251.101 223.181.111.239 BT-DHT 145 BitTorrent DHT Protocol
26421 202.018811 192.168.251.101 212.85.93.25 BT-DHT 145 BitTorrent DHT Protocol
26422 202.025068 212.85.93.25 192.168.251.101 BT-DHT 341 BitTorrent DHT Protocol reply=8 nodes
26425 202.115720 192.168.251.101 181.141.12.71 BT-DHT 145 BitTorrent DHT Protocol


Wireshark · Flow · labip10.pcap
Time
192.168.251.101
67.215.246.10
82.221.103.244
Comment
201.123578 27997 BitTorrent DHT Protocol 6881 BT-DHT: BitTorrent DHT Protocol
201.219155 27997 BitTorrent DHT Protocol 6881 BT-DHT: BitTorrent DHT Protocol
201.392540 27997 BitTorrent DHT Protocol reply=16 nodes 6881 BT-DHT: BitTorrent DHT Protocol reply=16 nodes
201.599259 27997 BitTorrent DHT Protocol BT-DHT: BitTorrent DHT Protocol
201.740061 27997 BitTorrent DHT Protocol BT-DHT: BitTorrent DHT Protocol
201.740066 27997 BitTorrent DHT Protocol BT-DHT: BitTorrent DHT Protocol
201.927303 27997 BitTorrent DHT Protocol reply=8 nodes BT-DHT: BitTorrent DHT Protocol reply=8 nodes
201.999296 27997 BitTorr BT-DHT: BitTorrent DHT Protocol
202.016940 27997 BitTorrent DHT Protocol BT-DHT: BitTorrent DHT Protocol
202.018811 27997 BitTorrent DHT Protocol BT-DHT: BitTorrent DHT Protocol
202.025068 27997 BitTorrent DHT Protocol reply=8 nodes BT-DHT: BitTorrent DHT Protocol reply=8 nodes
202.115720 27997 BT-DHT: BitTorrent DHT Protocol
202.223791 27997 BT-DHT: BitTorrent DHT Protocol
202.225675 27997 BT-DHT: BitTorrent DHT Protocol
202.231176 27997 BitTorrent DHT BT-DHT: BitTorrent DHT Protocol reply=8 nodes
202.278163 27997 BitTorrent DHT Protocol reply=8 nodes BT-DHT: BitTorrent DHT Protocol reply=8 nodes
202.312299 27997 BT-DHT: BitTorrent DHT Protocol

d. Tracker's status.

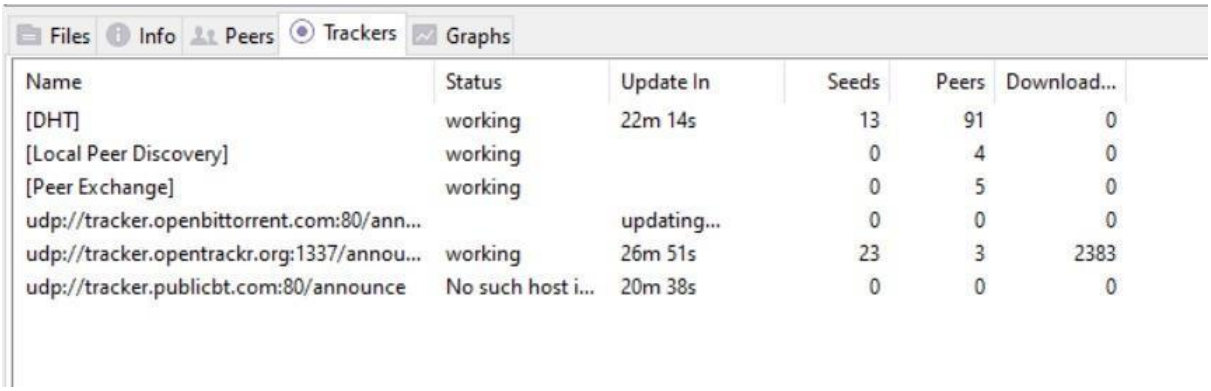


No.	Time	Source	Destination	Protocol	Lengt	Info
22140	187.185670	82.221.103.246	192.168.251.101	HTTP	234	HTTP/1.1 200 OK
22167	187.434548	192.168.251.101	82.221.103.246	HTTP	361	GET /installstats.php?cl=BitTorrent&v=258061823&h=lxh-ZO68ap_-ZS9f&
22182	187.672126	82.221.103.246	192.168.251.101	HTTP	234	HTTP/1.1 200 OK
22624	188.245457	192.168.251.101	52.70.92.199	HTTP	623	POST /e?i=6000 HTTP/1.1 (application/x-www-form-urlencoded)
22837	188.574133	52.70.92.199	192.168.251.101	HTTP	241	HTTP/1.1 200 OK (text/html)
22860	188.894690	2409:4072:2e0c:d03d:e5e4:5cb9:c5...	2606:4700:9c60:e2cc:2ec...	HTTP	257	HEAD /nano_download.php?partner=WC220101 HTTP/1.1
23758	192.602513	2606:4700:9c60:e2cc:2ec6:406:6811...	2409:4072:2e0c:d03d:e5e...	HTTP	586	HTTP/1.1 200 OK
23760	192.603358	2409:4072:2e0c:d03d:e5e4:5cb9:c5...	2606:4700:9c60:e2cc:2ec...	HTTP	150	GET /nano_download.php?partner=WC220101 HTTP/1.1
24499	194.427939	2409:4072:2e0c:d03d:e5e4:5cb9:c5...	2606:4700:9c60:e2cc:2ec...	HTTP	178	GET /nano_download.php?partner=WC220101 HTTP/1.1
26284	198.553119	2606:4700:9c60:e2cc:2ec6:406:6811...	2409:4072:2e0c:d03d:e5e...	HTTP	804	HTTP/1.1 206 Partial Content
26322	200.543710	192.168.251.101	103.53.14.4	HTTP	210	GET /utorrent-onboarding/player.btapp HTTP/1.1
26328	200.591561	103.53.14.4	192.168.251.101	HTTP/X...	54	HTTP/1.1 403 Forbidden

Content-Length: 345\r\n
Connection: Keep-Alive\r\n
Cache-Control: no-cache\r\n
\r\n
[Full request URI: http://i-6000.b-46591.ut.bench.utorrent.com/e?i=6000]
[HTTP request 2/2]

Here we can be able to see that the name of the tracker is i-6000.b- 46591.ut.bench.utorrent.com

e. DHT status



Files | Info | Peers | Trackers | Graphs

Name	Status	Update In	Seeds	Peers	Download...
[DHT]	working	22m 14s	13	91	0
[Local Peer Discovery]	working		0	4	0
[Peer Exchange]	working		0	5	0
udp://tracker.openbittorrent.com:80/ann...		updating...	0	0	0
udp://tracker.opentrackr.org:1337/annou...	working	26m 51s	23	3	2383
udp://tracker.publicbt.com:80/announce	No such host i...	20m 38s	0	0	0

Here we can see that while downloading the torrent file the DHT status is set to working.

Files | Info | Peers | Trackers | Graphs

Name	Status	Update In	Seeds	Peers	Download...
[DHT]	disabled		0	0	0
[Local Peer Discovery]	working		0	5	0
[Peer Exchange]	working		0	2	0
udp://tracker.openbittorrent.com:80/ann...	No such host i...	18m 7s	0	0	0
udp://tracker.opentrackr.org:1337/annou...	No such host i...	17m 8s	0	0	0
udp://tracker.publicbt.com:80/announce	No such host i...	17m 9s	0	0	0

Here while seeding the DHT status is set as disabled.

f. Identify other peers involved in the communication

From the below screenshot we can see that there are sevreral nodes which represents a peer and it sip address and port number is shown

labip10.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: bt-dht

No.	Time	Source	Destination	Protocol	Lengt	Info
28661	220.337789	85.174.207.192	192.168.251.101	BT-DHT	320	BitTorrent DHT Protocol reply=8 nodes
28662	220.337789	95.29.6.102	192.168.251.101	BT-DHT	341	BitTorrent DHT Protocol reply=8 nodes
28663	220.348338	223.238.7.37	192.168.251.101	BT-DHT	341	BitTorrent DHT Protocol reply=8 nodes
28668	220.366735	109.200.137.126	192.168.251.101	BT-DHT	331	BitTorrent DHT Protocol reply=8 nodes

```
nodes: 8
    Key: nodes
    Value: 8 nodes
        Node 1 (id: 2900000023480000be18000084670000e14a0000, IPv4/Port: 188.19.14.6...
        Node 2 (id: 290001e8d44dc8414a40fa915f98eb03b729b027, IPv4/Port: 83.215.126....
        Node 3 (id: 29000ed071d6e6193410704a23370563aa3ff2fd, IPv4/Port: 79.166.249.1...
        Node 4 (id: 29001aa386c9de3566a02a302d1060c918f00957, IPv4/Port: 67.167.240....
        Node 5 (id: 290029efdd113090676d6d26ffd6d63821afd88c, IPv4/Port: 109.255.25.3:...
        Node 6 (id: 2900347d2af08a45b0a100ccba5618d844c4b64f, IPv4/Port: 81.228.36.14...
        Node 7 (id: 290065f607a5bb461af2de112bd690a44aefce42, IPv4/Port: 49.35.244.24...
        Node 8 (id: 29006b19b138c43ca5afff785f62ee99538c0f40, IPv4/Port: 173.242.115.1...
```

```
0000  f4 46 37 9f 81 d4 96 29  44 b7 f5 fa 08 00 45 28   ·F7····) D·····E(
0010  01 32 a2 57 00 00 6b 11  ca be 55 ae cf c0 c0 a8   ·2·W··k· ··U·····
0020  fb 65 0e fa 6d 5d 01 1e  67 c8 64 31 3a 72 64 32   ·e··m]·· g·d1:rd2
0030  3a 69 64 32 30 3a 29 00  eb 90 71 e3 eb 67 0c 31   :id20:)· ··q··g·1
0040  a9 fe 27 fd ed c9 66 eb  87 8e 35 3a 6e 6f 64 65   ··'···f· ··5:node
0050  73 32 30 38 3a 29 00 00  00 23 48 00 00 be 18 00   s208:)·· ·#H·····
0060  00 84 67 00 00 e1 4a 00  00 bc 13 0e 42 75 0b 29   ··g···J· ····Bu·)
0070  00 01 e8 d4 4d c8 41 4a  40 fa 91 5f 98 eb 03 b7   ····M·AJ @··_····
0080  29 b0 27 53 d7 7e 4e c4  91 29 00 0e d0 71 d6 e6   )·'S·~N· ·)···q··
0090  19 34 10 70 4a 23 37 05  63 aa 3f f2 fd 4f a6 f9   ·4·pJ#7· c·?··O··
00a0  0b c1 1b 29 00 1a a3 86  c9 de 35 66 a0 2a 30 2d   ···)···· ··5f·*0-
00b0  10 60 c9 18 f0 09 57 43  a7 f0 18 23 32 29 00 29   ·`····WC ···#2)·)
00c0  ef dd 11 30 90 67 6d 6d  26 ff d6 d6 38 21 af d8   ···0·gmm &···8!··
00d0  8c 6d ff 19 03 04 06 29  00 34 7d 2a f0 8a 45 b0   ·m·····) ·4}*··E·
00e0  a1 00 cc ba 56 18 d8 44  c4 b6 4f 51 e4 24 8d 10   ····V··D ··OQ·$··
```

Current filter: bt-dht

No.	Time	Source	Destination	Protocol	Lengt	Info
28661	220.337789	85.174.207.192	192.168.251.101	BT-DHT	320	BitTorrent DHT Protocol reply=8 nodes
28662	220.337789	95.29.6.102	192.168.251.101	BT-DHT	341	BitTorrent DHT Protocol reply=8 nodes
28663	220.348338	223.238.7.37	192.168.251.101	BT-DHT	341	BitTorrent DHT Protocol reply=8 nodes
28668	220.366735	109.200.137.126	192.168.251.101	BT-DHT	331	BitTorrent DHT Protocol reply=8 nodes

```
nodes: 8
    Key: nodes
    Value: 8 nodes
        Node 1 (id: 2900000023480000be18000084670000e14a0000, IPv4/Port: 188.19.14.6...
            ID: 2900000023480000be18000084670000e14a0000
            IP: 188.19.14.66
            Port: 29963
```

```
0000  f4 46 37 9f 81 d4 96 29  44 b7 f5 fa 08 00 45 28   ·F7····) D·····E(
0010  01 32 a2 57 00 00 6b 11  ca be 55 ae cf c0 c0 a8   ·2·W··k· ··U·····
0020  fb 65 0e fa 6d 5d 01 1e  67 c8 64 31 3a 72 64 32   ·e··m]·· g·d1:rd2
0030  3a 69 64 32 30 3a 29 00  eb 90 71 e3 eb 67 0c 31   :id20:)· ··q··g·1
0040  a9 fe 27 fd ed c9 66 eb  87 8e 35 3a 6e 6f 64 65   ··'···f· ··5:node
0050  73 32 30 38 3a 29 00 00  00 23 48 00 00 be 18 00   s208:)·· ·#H·····
0060  00 84 67 00 00 e1 4a 00  00 bc 13 0e 42 75 0b 29   ··g···J· ····Bu·)
0070  00 01 e8 d4 4d c8 41 4a  40 fa 91 5f 98 eb 03 b7   ····M·AJ @··_····
0080  29 b0 27 53 d7 7e 4e c4  91 29 00 0e d0 71 d6 e6   )·'S·~N· ·)···q··
```

g. Try to identify the name of the file downloded

bt-dht.bencoded.string == 25f241c88bdc49c9b05da6f145164018a22f050a

```
  ⌄ info_hash: 25f241c88bdc49c9b05da6f145164018a22f050a
      Key: info_hash
      Value: 25f241c88bdc49c9b05da6f145164018a22f050a
```

```
⌄ BitTorrent DHT Protocol
  ⌄ Request arguments: Dictionary...
      Key: a
    ⌄ Value: Dictionary...
      ⌄ id: dff503d6ae529049f1f1bbe9ebb3a6db3c870ce1
          Key: id
          Value: dff503d6ae529049f1f1bbe9ebb3a6db3c870ce1
      ⌄ implied_port: 1
          Key: implied_port
          Terminator: e
          Value: 1
      ⌄ info_hash: 25f241c88bdc49c9b05da6f145164018a22f050a
          Key: info_hash
          Value: 25f241c88bdc49c9b05da6f145164018a22f050a
      ⌄ name: Minecraft
          Key: name
          Value: Minecraft
```

5. Try to export the 20% of data you have captured as traffic in Wireshark while downloading files in Torrent.

6. After the Download completes and when it starts seeding, open the Wireshark and analyze the information being transferred in that traffic. Document the difference in Network traffic.

2320	2022/344 09:20:37.449239	2409:4072:e95:dba2:…	55082	2404:6800:4007:819:…	443	TCP	86 [TCP Dup ACK 2318#1] 55082 → 443 [ACK] Seq=3 Ack=74 Win=510 Len=0 SLE=1 SRE=74
2321	2022/344 09:20:37.459217	192.168.137.150	27835	176.96.249.117	37076	BT-uTP	62 Connection ID:57312 [Fin] Seq=27001 Ack=26484 Win=50000 Len=0
2322	2022/344 09:20:37.461204	35.213.12.39	443	192.168.137.150	55233	TLSv1.2	85 Encrypted Alert
2323	2022/344 09:20:37.461204	35.213.12.39	443	192.168.137.150	55233	TCP	54 443 → 55233 [FIN, ACK] Seq=560 Ack=1535 Win=501 Len=0
2324	2022/344 09:20:37.461293	192.168.137.150	55233	35.213.12.39	443	TCP	54 55233 → 443 [ACK] Seq=1535 Ack=561 Win=510 Len=0
2325	2022/344 09:20:37.461493	2404:6800:4007:819:…	443	2409:4072:e95:dba2:…	55082	TCP	74 443 → 55082 [FIN, ACK] Seq=74 Ack=3 Win=282 Len=0
2326	2022/344 09:20:37.461555	2409:4072:e95:dba2:…	55082	2404:6800:4007:819:…	443	TCP	74 55082 → 443 [ACK] Seq=3 Ack=75 Win=510 Len=0
2327	2022/344 09:20:37.509723	138.199.14.86	443	192.168.137.150	55009	TCP	66 [TCP Dup ACK 332#5] 443 → 55009 [ACK] Seq=2 Ack=1 Win=501 Len=0 SLE=0 SRE=1
2328	2022/344 09:20:38.262704	192.168.137.150	55374	91.232.158.75	11327	TCP	66 [TCP Retransmission] [TCP Port numbers reused] 55374 → 11327 [SYN] Seq=0 Win=64240 Len=0 MSS=1460

Here we didn't get any packets for seeding. Since there wasn't any seeding done by our system.