

# **21CY681 - INTERNET PROTOCOL LAB - X**

Name: Surya S Nair

Register Number: CB.EN.P2CYS22007

Date: 10th December 2022

Assignment Topic: Analyzing bittorrent and bht protocols using wireshark

## **AIM:**

Analyzing bittorrent and bht protocols using wireshark

## **TOOLS REQUIRED:**

Bit-torrent

## **PROCEDURE:**

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

### b. Working of BitTorrent.

### c.Protocol Level Analysis

Time	192.168.137.150	46.139.90.206	94.181.246.57	5.137.116.142	95.54.143.159	Comment
2022/3/42 06:26:48.072007	56309	Handshake	6881			BitTorrent Handshake
2022/3/42 06:26:48.093005	56310	Handshake	32716			BitTorrent Handshake
2022/3/42 06:26:48.202456	56302	Handshake		1191		BitTorrent Handshake
2022/3/42 06:26:48.320192	56309	Handshake Extended Have All Unchoke	6881			BitTorrent Handshake Extended Have All Unchoke
2022/3/42 06:26:48.754084	56309	Extended Bitfield, Len=0x9 Have, Piece (idx=0x3c)	6881			BitTorrent Extended Bitfield, Len=0x9 Have, Piece (idx=0x3c)
2022/3/42 06:26:48.972076	56309	Allowed Fast, Piece (idx=0x23a) Allowed Fast, Piece (idx=0x23a)	6881			BitTorrent Allowed Fast, Piece (idx=0x23a) Allowed Fast, Piece (idx=0x23a)
2022/3/42 06:26:49.385798	56309	Piece, idx=0x148, Begin=0x0, Len=0x4000	6881			BitTorrent Piece, idx=0x148, Begin=0x0, Len=0x4000
2022/3/42 06:26:49.582771	56309	Piece, idx=0x148, Begin=0x4000, Len=0x4000	6881			BitTorrent Piece, idx=0x148, Begin=0x4000, Len=0x4000
2022/3/42 06:26:49.582771	56309	Extended	6881			BitTorrent Extended
2022/3/42 06:26:49.836090	56309	Piece, idx=0x148, Begin=0x8000, Len=0x4000	6881			BitTorrent Piece, idx=0x148, Begin=0x8000, Len=0x4000
2022/3/42 06:26:49.863876	56309	Piece, idx=0x148, Begin=0xc000, Len=0x4000	6881			BitTorrent Piece, idx=0x148, Begin=0xc000, Len=0x4000
2022/3/42 06:26:50.102118	56309	Piece, idx=0x148, Begin=0x10000, Len=0x4000	6881			BitTorrent Piece, idx=0x148, Begin=0x10000, Len=0x4000
2022/3/42 06:26:50.103792	56309	Have, Piece (idx=0x20f) Have, Piece (idx=0x30b) Have, Piece (idx=0x30b)	6881			BitTorrent Have, Piece (idx=0x20f) Have, Piece (idx=0x30b) Have, Piece (idx=0x30b)
2022/3/42 06:26:50.110643	56315	Handshake			31994	BitTorrent Handshake
2022/3/42 06:26:50.290373	56309	Piece, idx=0x148, Begin=0x14000, Len=0x4000	6881			BitTorrent Piece, idx=0x148, Begin=0x14000, Len=0x4000
2022/3/42 06:26:50.344170	56309	Piece, idx=0x148, Begin=0x18000, Len=0x4000	6881			BitTorrent Piece, idx=0x148, Begin=0x18000, Len=0x4000
2022/3/42 06:26:50.364421	56309	Piece, idx=0x148, Begin=0x1c000, Len=0x4000	6881			BitTorrent Piece, idx=0x148, Begin=0x1c000, Len=0x4000
2022/3/42 06:26:50.417399	56315	Handshake			31994	BitTorrent Handshake
2022/3/42 06:26:50.444607	56315	Extended Bitfield, Len=0x9 Have, Piece (idx=0x362) Have, Piece (idx=0x19f) Have, Piece (idx=0x20d) Have, Piece (idx=0x16f) Have, Piece (idx=0x245) Have, Piece (idx=0x380) Have, Piece (idx=0x405) Have, Piece (idx=0x405)			31994	BitTorrent Extended Bitfield, Len=0x9 Have, Piece (idx=0x362) Have, Piece (idx=0x19f) Have, Piece (idx=0x20d) Have, Piece (idx=0x16f) Have, Piece (idx=0x245) Have, Piece (idx=0x380) Have, Piece (idx=0x405) Have, Piece (idx=0x405)

Time	192.168.137.150	183.204.155.208	191.179.126.142	116.255.102.168	157.33.25.235	Comment
2022/3/42 06:26:01.818716	7835	BitTorrent DHT Protocol	55757			BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:01.818730	7835	BitTorrent DHT Protocol	55757			BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:02.085888	7835	BitTorrent DHT Protocol reply=8 nodes	55757			BT-DHT: BitTorrent DHT Protocol reply=8 nodes
2022/3/42 06:26:08.810431	7835	BitTorrent DHT Protocol	6881			BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:08.810443	7835	BitTorrent DHT Protocol	6881			BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:09.238659	7835	BitTorrent DHT Protocol reply=8 nodes	6881			BT-DHT: BitTorrent DHT Protocol reply=8 nodes
2022/3/42 06:26:15.812910	7835	BitTorrent DHT Protocol	49566			BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:15.812915	7835	BitTorrent DHT Protocol	49566			BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:16.291657	7835	BitTorrent DHT Protocol reply=8 nodes	49566			BT-DHT: BitTorrent DHT Protocol reply=8 nodes
2022/3/42 06:26:22.814575	7835	BitTorrent DHT Protocol	49379			BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:22.814580	7835	BitTorrent DHT Protocol	49379			BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:22.998476	49379	Destination unreachable (Port unreachable)				ICMP Destination unreachable (Port unreachable)
2022/3/42 06:26:25.833870	7835	BitTorrent DHT Protocol			27355	BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:25.833875	7835	BitTorrent DHT Protocol				BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:25.834173	7835	BitTorrent DHT Protocol				BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:25.834177	7835	BitTorrent DHT Protocol				BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:25.834342	7835	BitTorrent DHT Protocol				BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:25.834347	7835	BitTorrent DHT Protocol				BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:25.834498	7835	BitTorrent DHT Protocol				BT-DHT: BitTorrent DHT Protocol

d. Tracker's status.

```
▼ Hypertext Transfer Protocol
  > POST /e?i=38 HTTP/1.1\r\n
    Host: i-38.b-46613.bt.bench.utorrent.com\r\n
    User-Agent: ut_core BenchHttp (ver:46613)\r\n
    Connection: close\r\n
  > Content-Length: 227\r\n
    \r\n
    [Full request URI: http://i-38.b-46613.bt.bench.utorrent.com/e?i=38]
    [HTTP request 1/1]
```

Here we can be able to see that the name of the tracker is i-38.b-46613.bt.bench.utoorent.com

e.DHT status

Files Info Peers <b>Trackers</b> 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.

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.opentracker.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 several nodes which represents a peer and its IP address and port number is shown

```

Key: nodes
v Value: 8 nodes
  > Node 1 (id: dfe04db3460fb98d315cbeaa4539e187b92626a7, IPv4/Port: 86.41.10.163:53020)
  > Node 2 (id: dfe0bee587f8f3564f342a6ecf155ab146c41206, IPv4/Port: 223.109.186.214:6884)
  > Node 3 (id: dfe15bed3bf19c251cf5deb99627aa6f6620c7de, IPv4/Port: 95.79.124.208:21303)
  > Node 4 (id: dfe1d2c2ab35c73fe05a538e66b4b2545c262b01, IPv4/Port: 98.242.168.96:27033)
  > Node 5 (id: dfe201c9b22a34aae27b81935c0118f944d893b8, IPv4/Port: 185.149.90.126:52007)
  > Node 6 (id: dfe283abd9f97e4450ec636f21351e0920044efb, IPv4/Port: 35.139.52.195:6881)
  > Node 7 (id: dfe34745b5103072aa9c29eb0d3fbc8d8759a4e1e, IPv4/Port: 121.170.44.25:7890)
  > Node 8 (id: dfe3e29bc55a2853958a91d730417607565b8156, IPv4/Port: 82.65.162.139:6881)
Terminator: e
saction ID: a8530000

v Value: 8 nodes
  v Node 1 (id: dfc3c164940003cd8c9e12312aa7b00c02a2a6b3, IPv4/Port: 119.193.226.69:8003)
    ID: dfc3c164940003cd8c9e12312aa7b00c02a2a6b3
    IP: 119.193.226.69
    Port: 8003
  v Node 2 (id: dfc66a15d53c851bff95cdbcd4cf9d6611ade402, IPv4/Port: 121.179.12.75:7795)
    ID: dfc66a15d53c851bff95cdbcd4cf9d6611ade402
    IP: 121.179.12.75
    Port: 7795
  > Node 3 (id: dfc085c6ab80e2cdcbc473480e19572ee344121a, IPv4/Port: 69.114.169.254:33806)
  > Node 4 (id: dfc504adfc126eb1ecb59245b21bd341f7fcc0f, IPv4/Port: 221.145.147.185:41070)

```

g. Try to identify the name of the file downloaded

```
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 23194] 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	55089	TCP	66 [TCP Dup ACK 33295] 443 → 55089 [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 R

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

**RESULT:** Analyzed bittorrent and bht protocols using wireshark.