21CY681 - INTERNET PROTOCOL LAB - X

Name: Surya S Nair

Register Number: CB.EN.P2CYS22007

Date: 10th December 2022

Assignment Topic: Analyzing bittorent and bht protocols using wireshark

AIM:

Analyzing bittorent 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

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.

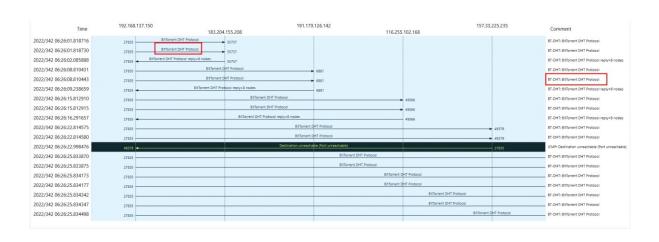
BitTorrent is a peer-to-peer protocol, which means that the computers in a BitTorrent "swarm" (a group of computers downloading and uploading the same torrent) transfer data between each other without the need for a central server.

c.Protocol Level Analysis

BITTORENT -



DHT -



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

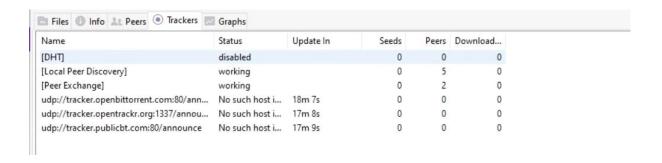
[Full request URI: http://i-38.b-46613.bt.bench.utorrent.com/e?i=38]
[HTTP request 1/1]
```

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

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.



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

```
Key: nodes
 ∨ 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: dfe34745b5103072aa9c29eb0d3fbcd8759a4e1e, IPv4/Port: 121.170.44.25:7890)
    > Node 8 (id: dfe3e29bc55a2853958a91d730417607565b8156, IPv4/Port: 82.65.162.139:6881)
saction ID: a8530000
    ∨ Value: 8 nodes
       V Node 1 (id: dfc3c164940003cd8c9e12312aa7b00c02a2a6b3, IPv4/Port: 119.193.226.69:8003)
             ID: dfc3c164940003cd8c9e12312aa7b00c02a2a6b3
            IP: 119.193.226.69
            Port: 8003
       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: dfc504adfcb126eb1ecb59245b21bd341f7fcc0f, IPv4/Port: 221.145.147.185:41070)
```

g. Try to identify the name of the file downloded

bt-dht.bencoded.string == 25f241c88bdc49c9b05da6f145164018a22f050a v 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 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:		443		
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 2484:6800:4007:819:	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		66 [TCP Retransmission] [TCP Port numbers reused] 55374 * 11327 [SYN] Seq=0 Win=64240 Len=0 MSS=1

Here we didn't get any packets done by our system.	s for seeding. Since the	re wasn't any seeding
RESULT: Analyzed bittorent as	nd bht protocols using w	vireshark.