

Name:- MOHAMMED TOUSIF  
Roll No:- CB.EN.P2CYS22008

## ANALYZING PEER TO PEER NETWORK TRAFFIC USING VARIOUS NETWORK SNIFFERS

Date :- 10-12-2022

Aim :- To analyze peer to peer network traffic using various network sniffers.

Tools Required :- Windows OS , Wireshark.

Procedure :-

### **b. Working of BitTorrent**

BitTorrent is a hyper distribution communications protocol for peer-to-peer file sharing ("P2P") which is used to distribute data and electronic files over the Internet. Bittorrent takes the stress of transferring large data files from one massive server to every user over an extremely robust network connection and splits it up to multiple normal PCs and multiple smaller network connections.

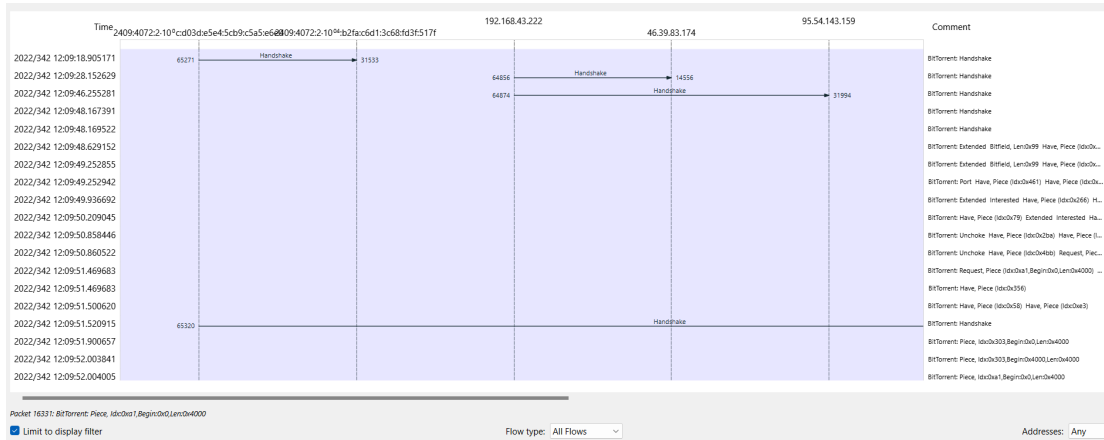
Seed is the user that have the complete file downloaded already and are now sharing the file with peers but not downloading any parts of the file from others.

Leechers are those who are downloading and uploading at the same time.

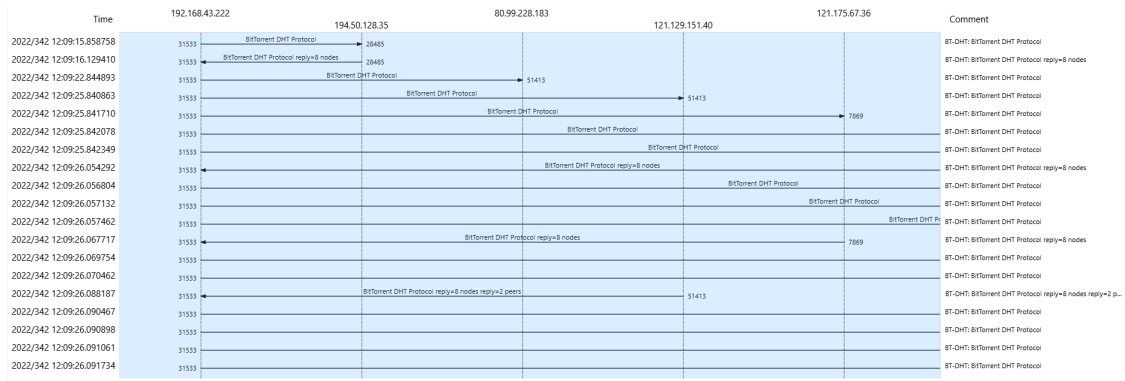
Files are downloaded in pieces. When a user downloads some parts, he then automatically starts uploading it. A file will be downloaded quicker if more users are involved in the process.

### c. Protocol Level Analysis

bittorent:



bt-dht:



#### d. Tracker’s status

Below we can see the trackers's status.

```

v Hypertext Transfer Protocol
  > POST /e?i=38 HTTP/1.1\r\n
    Host: i-38.b-46591.bt.bench.utorrent.com\r\n
    User-Agent: ut_core BenchHttp (ver:46591)\r\n
    Connection: close\r\n
  > Content-Length: 225\r\n
    \r\n
    [Full request URI: http://i-38.b-46591.bt.bench.utorrent.com/e?i=38]

```

---

#### 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

DHT status is displaying **working** while the file is downloading.

Name	Status	Update In	Seeds	Peers	Download...
[DHT]	waiting for an...		0	0	0
[Local Peer Discovery]	working		0	6	0
[Peer Exchange]	working		0	0	0

DHT status is **waiting for announce** while the file status is inactive.

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

DHT status is **disabled** while seeding.

## f. Identify other peers involved in the communication

- Value: 8 nodes
    - > Node 1 (id: f7007beeec874d6dea61e45ef83f0346571add7e, IPv4/Port: 92.37.143.24:12424)
    - > Node 2 (id: f7000495173ef7b66a6a4787f02d401908b85cb8, IPv4/Port: 84.236.126.255:18891)
    - > Node 3 (id: f700d5d6ae529049f1f1bbe9ebb3a6db3c870ce1, IPv4/Port: 176.114.219.163:16813)
    - > Node 4 (id: f7000988dc4648338b6a89a5d5ea307a3a55601a, IPv4/Port: 122.107.127.109:41404)
    - > Node 5 (id: f7005ca40acb07b72ec4a461cada2df757a6ab57, IPv4/Port: 118.220.239.16:8033)
    - > Node 6 (id: f70040a1095e36a36d4caddacbef72833a7e2ec3, IPv4/Port: 96.40.167.77:50321)
    - > Node 7 (id: f700125567e123175e301f79bf080112325684d6, IPv4/Port: 218.153.113.231:41007)
    - > Node 8 (id: f700a239021948424b84feca3830c749527ded5a, IPv4/Port: 112.147.222.5:8075)
- Node 1 (id: f7007beeec874d6dea61e45ef83f0346571add7e, IPv4/Port: 92.37.143.24:12424)
    - ID: f7007beeec874d6dea61e45ef83f0346571add7e
    - IP: 92.37.143.24
    - Port: 12424
  - > Node 2 (id: f7000495173ef7b66a6a4787f02d401908b85cb8, IPv4/Port: 84.236.126.255:18891)
  - > Node 3 (id: f700d5d6ae529049f1f1bbe9ebb3a6db3c870ce1, IPv4/Port: 176.114.219.163:16813)

## g. Try to identify the name of the file downloaded

```
bt-dht.bencoded.string == 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

**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 09:20:17.449219	2409:8072::e95:dba2::...	55082	2404:6800:8007:819::...	443	TCP	86 [TCP Dup ACK 2310#1] 55082 → 443 [ACK] Seq=3 Ack=78 Win=510 Len=0 SLE=1 SRE=74
2321	2022/344 09:20:17.450217	192.168.137.150	27035	176.96.249.117	37076	BT-UTP	62 Connection ID:57312 [Fin] Seq=27001 Ack=26484 Win=50000 Len=0
2322	2022/344 09:20:17.461204	35.213.12.39	443	192.168.137.150	55233	TLSv1.2	85 Encrypted Alert
2323	2022/344 09:20:17.461204	35.213.12.39	443	192.168.137.150	55233	TCP	54 643 → 55233 [FIN, ACK] Seq=500 Ack=1535 Win=501 Len=0
2324	2022/344 09:20:17.461293	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 09:20:17.461493	2404:6800:8007:819::...	443	2409:8072::e95:dba2::...	55082	TCP	74 443 → 55082 [FIN, ACK] Seq=74 Ack=3 Win=282 Len=0
2326	2022/344 09:20:17.461555	2409:8072::e95:dba2::...	55082	2404:6800:8007:819::...	443	TCP	74 55082 → 443 [ACK] Seq=3 Ack=75 Win=510 Len=0
2327	2022/344 09:20:17.500723	138.199.14.86	443	192.168.137.150	55080	TCP	66 [TCP Dup ACK 332#5] 443 → 55080 [ACK] Seq=2 Ack=1 Win=501 Len=0 SLE=0 SRE=1
2328	2022/344 09:20:18.243704	192.168.137.150	55174	91.232.150.70	11372	TCP	66 [TCP Retransmission] [TCP Peer's window received] 55174 → 11372 [SYN] Seq=0 Win=64240 Len=0 MSS=1460

**Result :** Thus , analyzing peer to peer network traffic using various network sniffers is successfully done.