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.

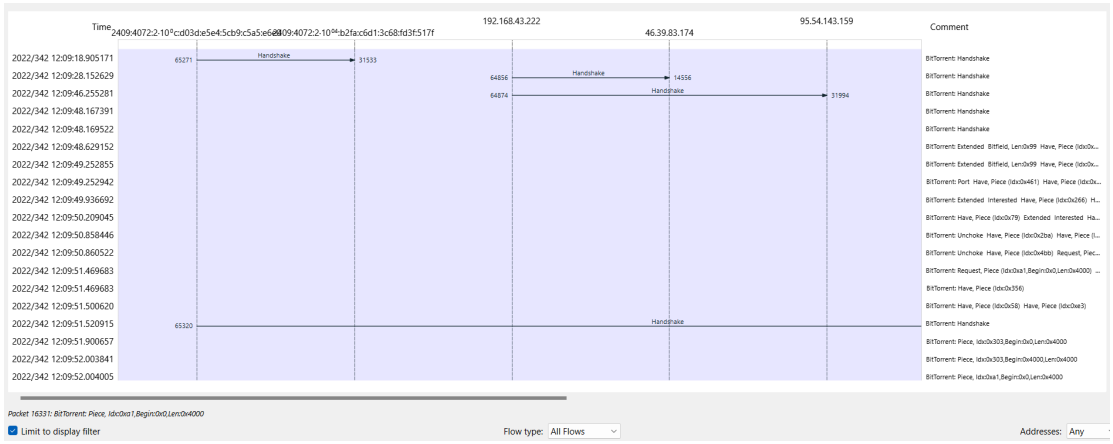
Seed is the user that have the complete file downloaded already and are now sharing the file with peers but not downloading any parts of the file from others.

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

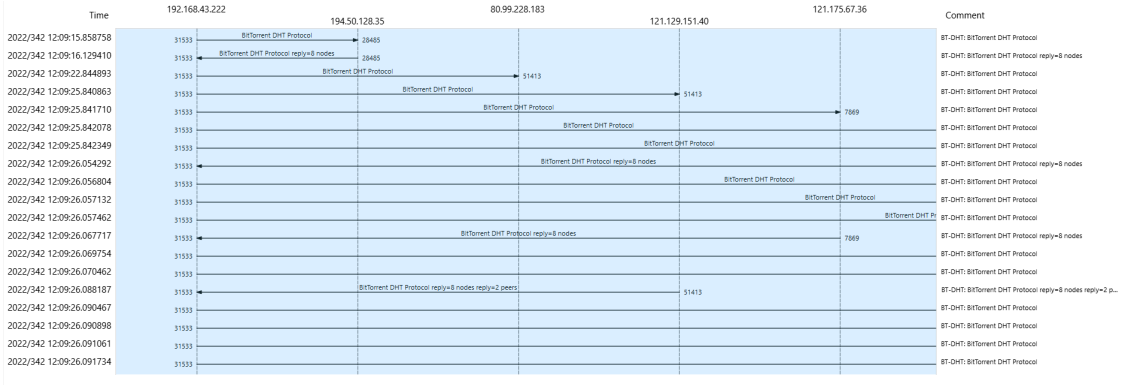
Files are downloaded in pieces. When a user downloads some parts, he then automatically starts uploading it. A file will be downloaded quicker if more users are involved in the process.

c. Protocol Level Analysis

bittorent:



bt-dht:

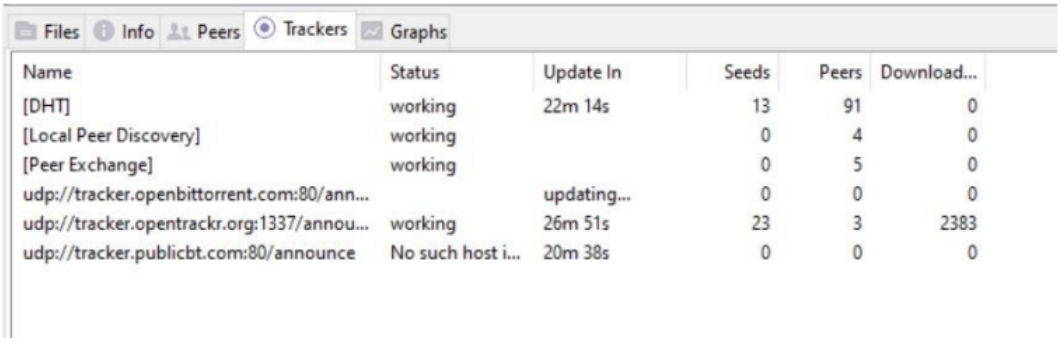


d. Tracker's status

Below we can see the trackers's status.

```
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

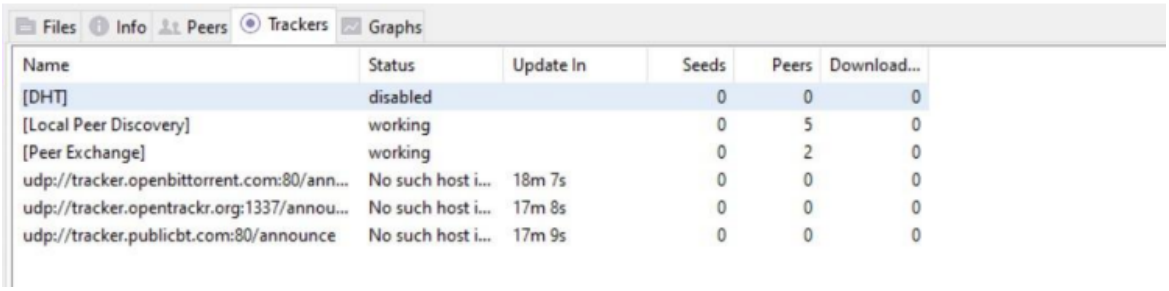


Name	Status	Update In	Seeds	Peers	Download...
[DHT]	working	22m 14s	13	91	0
[Local Peer Discovery]	working		0	4	0
[Peer Exchange]	working		0	5	0
udp://tracker.openbittorrent.com:80/ann...		updating...	0	0	0
udp://tracker.opentrackr.org:1337/annou...	working	26m 51s	23	3	2383
udp://tracker.publicbt.com:80/announce	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.



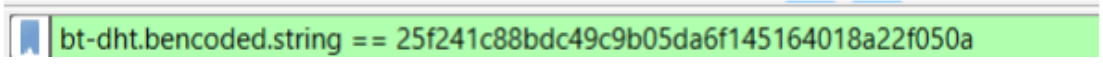
DHT status is **disabled** while seeding.

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)
```

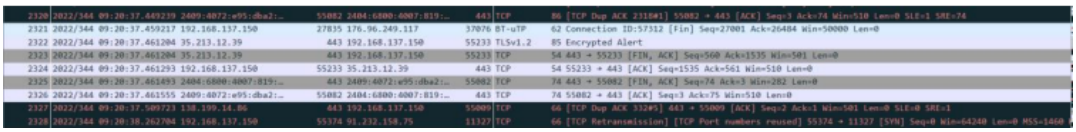
g. Try to identify the name of the file downloaded



```
  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
```

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.



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