

**NAME:** S.PRIYADHARSHINI

**ROLL NO.:** CB.EN.P2CYS22010

**DATE:** 10.12.2022

## **INTERNET PROTOCOL LAB – 10**

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

**AIM:**

To analyze peer to peer network traffic using various network sniffers.

**TOOLS REQUIRED:**

Wireshark, BitTorrent.

**PROCEDURE:**

- 1. Download the BitTorrent software from the given link <https://www.bittorrent.com/>.**
- 2. Then download any one Torrent file and then save it on your device.**
- 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.**

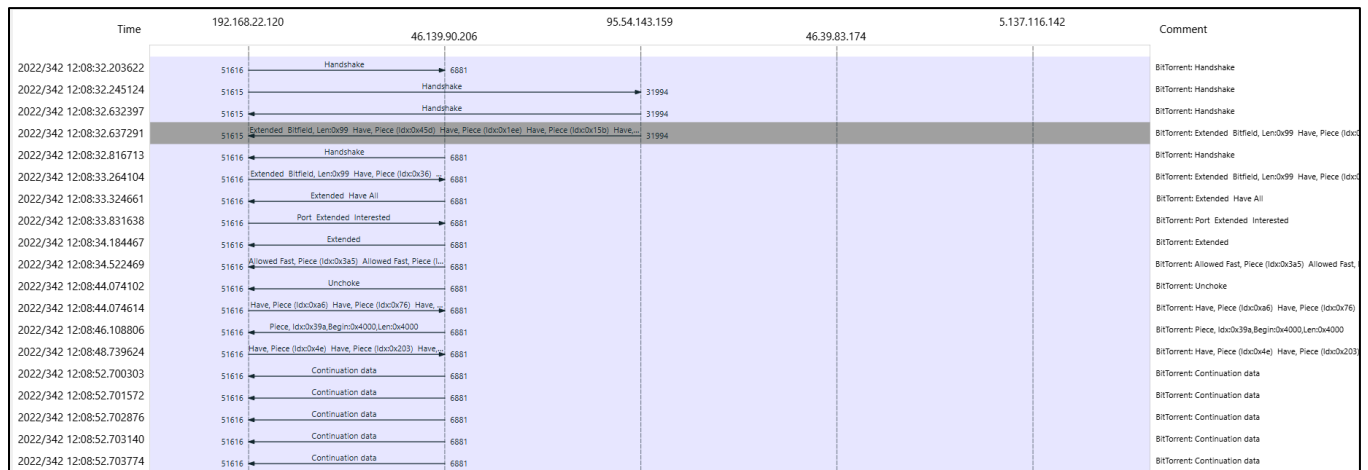
BitTorrent is a peer-to-peer protocol, which means that the computers in a BitTorrent “swarm” (a group of computers downloading and uploading the same torrent file) transfer data between each other without the need for a central server.

**b. Working of BitTorrent.**

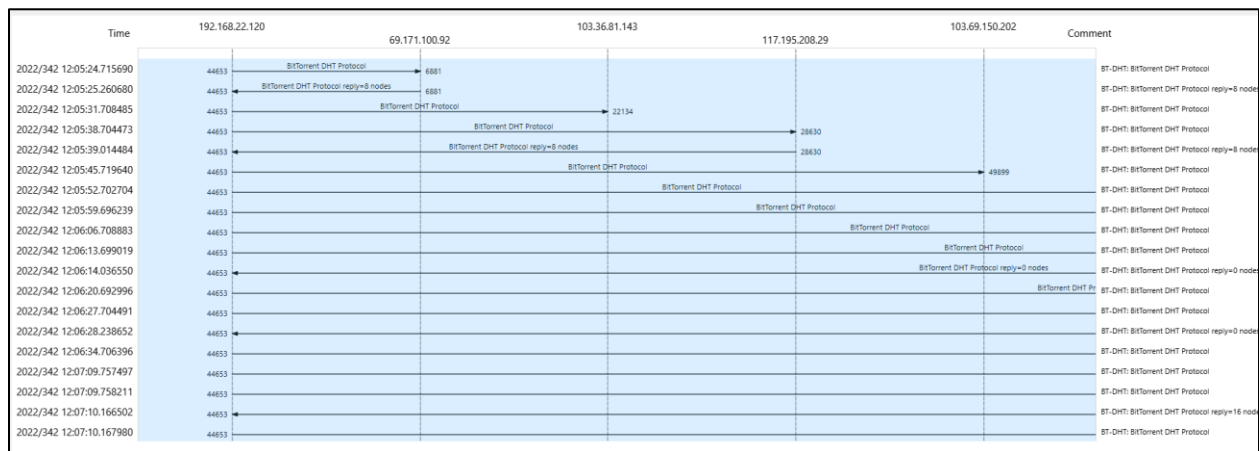
- The Client contacts a tracker specified in the .torrent file. The tracker is a special server that keeps track of the connected computers.
- The tracker shares their IP addresses with other BitTorrent clients in the swarm, allowing them to connect to each other.
- Once connected, a BitTorrent client 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.

### c. Protocol Level Analysis.

The filter 'bittorrent' is used here. This is the flow graph.



The filter 'bt-dht' is used here. This is the flow graph.



### 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
```

### e. DHT status.

When downloading the status of DHT is displayed as working.

1

Minecraft

152 MB

Downloading 2.8 %

345.3 KB/s

0.7 KB/s

29m 27s

0.206

Files

Info

Peers

Trackers

Graphs

Name	Status	Update In	Seeds	Peers	Download...
[DHT]	working	20m 17s	6	127	0
[Local Peer Discovery]	working		0	2	0
[Peer Exchange]	working		0	3	0
udp://tracker.openbittorrent.com:80/ann...	working	28m 20s	24	4	N/A
udp://tracker.opentracker.org:1337/annou...	working	26m 57s	20	4	2406
udp://tracker.publicbt.com:80/announce	No such host i...	19m 31s	0	0	0

When downloading and seeding is finished the status of DHT is displayed as inactive.

Minecraft

152 MB

Finished

0.204

Files

Info

Peers

Trackers

Graphs

Name	Status	Update In	Seeds	Peers	Download...
[DHT]	inactive		28	132	0
[Local Peer Discovery]	inactive		0	4	0
[Peer Exchange]	inactive		2	7	0
udp://tracker.openbittorrent.com:80/ann...	Connection ti...	updating...	0	0	0
udp://tracker.opentracker.org:1337/annou...	scrape ok	updating...	24	3	2407
udp://tracker.publicbt.com:80/announce	No such host i...	updating...	0	0	0
wss://tracker.btorrent.xyz	scrape ok	updating...	1	0	0

### f. Identify other peers involved in the communication.

59899 2022/342 12:08:31.386479 218.214.204.195	28270 192.168.22.120	44653 BT-DHT	395 BitTorrent DHT Protocol reply=8 nodes reply=3 peers
--	----------------------	--------------	---

Here it is displayed as reply from 8 nodes and 3 peers. We can see the id, IP address, port number information of the peers and nodes.

Value: 8 nodes

Node 1 (id: 25f24850d6f776683cb9eda6bc3f8bde7698692a, IPv4/Port: 42.105.172.57:41734)  
Node 2 (id: 25f25b9449c0f469a547def3f4381fb67db43f3f, IPv4/Port: 80.249.176.100:6881)  
Node 3 (id: 25f264e7f1f37e93e9fab94e9bfe4c634283b726, IPv4/Port: 106.206.190.167:29351)  
Node 4 (id: 25f27fb43dd6f5258d224b0211c529e0cbe790aa, IPv4/Port: 160.154.246.250:56305)  
Node 5 (id: 25f20430e950dca201011b2ad57a0e7d9b2c2de3, IPv4/Port: 24.250.52.25:17550)  
Node 6 (id: 25f21294cf9fb78d96c099b39d9f24457eefd053, IPv4/Port: 182.106.40.206:1025)  
Node 7 (id: 25f22df02753c289a765230cbd8632bed0e5783f, IPv4/Port: 46.219.224.80:14493)  
Node 8 (id: 25f232747edebf8891639083a71d89aeb75f7e6a, IPv4/Port: 180.74.216.168:31401)  
Node 9 (id: 25f232747edebf8891639083a71d89aeb75f7e6a, IPv4/Port: 180.74.216.168:31401)

values: 3 peers

Key: values

Value: 3 peers

Peer 1 (IP/Port: 193.106.1.145:49394)  
IP: 193.106.1.145  
Port: 49394  
Peer 2 (IP/Port: 89.113.140.161:6754)  
IP: 89.113.140.161  
Port: 6754  
Peer 3 (IP/Port: 94.181.246.57:32716)  
IP: 94.181.246.57  
Port: 32716  
Terminator: e  
Terminator: e

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

bt-dht.bencoded.string== 25f241c88bdc49c9b05da6f145164018a22f050a

No.	Time	Source	Source port	Destination	Destn port	Protocol	Length	Info
59675	2022/342 12:08:30.202825	192.168.22.120	44653	188.151.13.237	11414	BT-DHT	148	BitTorrent DHT Protocol
59676	2022/342 12:08:30.203031	192.168.22.120	44653	37.20.172.101	62899	BT-DHT	148	BitTorrent DHT Protocol
59770	2022/342 12:08:30.618490	192.168.22.120	44653	47.188.72.200	51413	BT-DHT	148	BitTorrent DHT Protocol
59771	2022/342 12:08:30.618868	192.168.22.120	44653	62.11.166.9	51413	BT-DHT	148	BitTorrent DHT Protocol

SHA1 Hash of info dictionary: 25f241c88bdc49c9b05da6f145164018a22f050a

The hash information of the file downloaded is found. When this is used in display filter we can see the name of the file downloaded.

```

BitTorrent DHT Protocol
  Request arguments: Dictionary...
    Key: a
    Value: Dictionary...
      id: c19ccbd6ae529049f1f1bbe9ebb3a6db3c870ce1
        Key: id
        Value: c19ccbd6ae529049f1f1bbe9ebb3a6db3c870ce1
      implied_port: 1
        Key: implied_port
        Terminator: e
        Value: 1
      info_hash: 25f241c88bdc49c9b05da6f145164018a22f050a
        Key: info_hash
        Value: 25f241c88bdc49c9b05da6f145164018a22f050a
      name: Minecraft
        Key: name
        Value: Minecraft
      port: 44653
        Key: port
        Terminator: e
        Value: 44653
      token: da39a3ee5e6b4b0d3255bfef95601890afd80709
        Key: token
        Value: da39a3ee5e6b4b0d3255bfef95601890afd80709
        Terminator: e

```

**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.**

## **RESULT:**

Thus, various network sniffers have been successfully used to analyze the network traffic in peer to peer networking.