INTERNET PROTOCOL LAB ASSIGNMNET -10

Name: Siriparapu Sparshika

Roll No: CYS22006

Date: 10-12-2022

TASKS:

To Analyzing BitTorrent and bht protocols using Wireshark

Tools Used:

Wireshark

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:

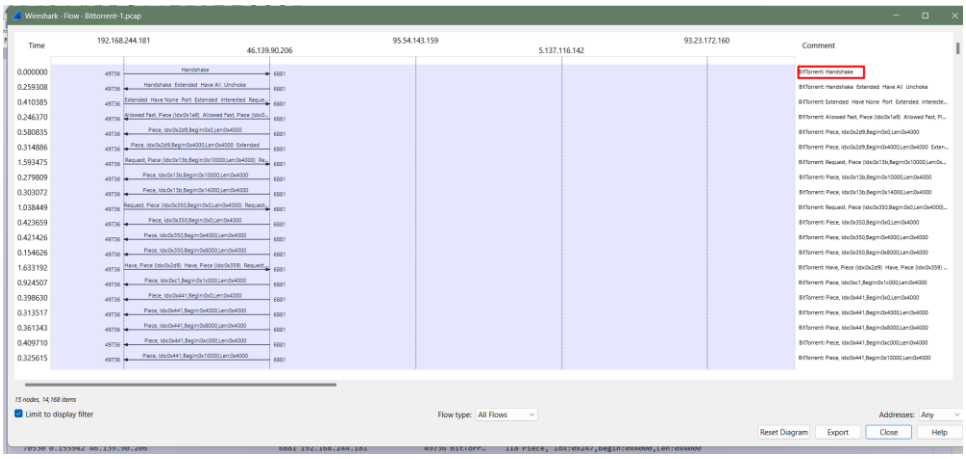
a. Give a detailed study about the working of BitTorrent in your downloading scenario.

Peer-to-peer BitTorrent - one person is downloading the amazon movie, they will install Client on other system (user - client s/o) - seeding happens.

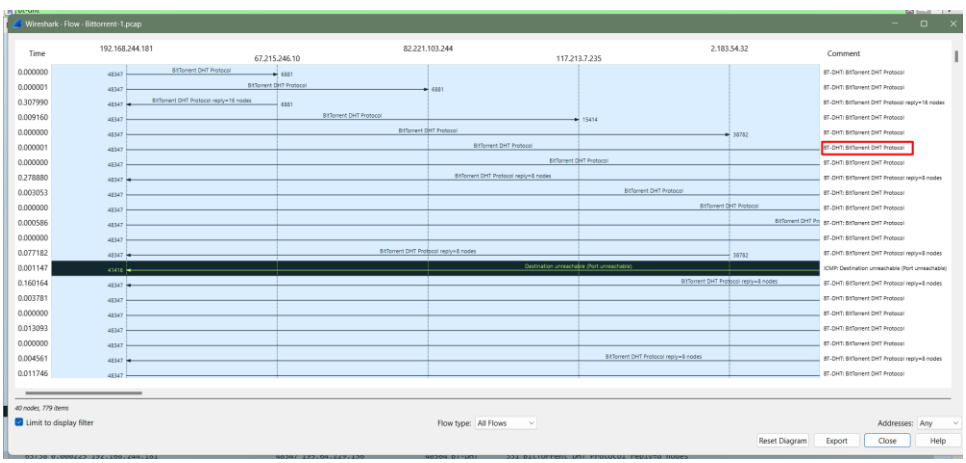
b. Working of BitTorrent.

BitTorrent is a peer-to-peer protocol, which means that the computers in a BitTorrent “swarm” transfer data between each other without the need for a central server.

c. Protocol Level Analysis



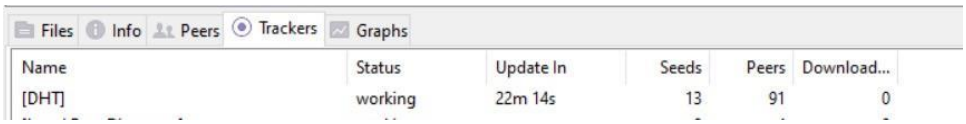
DHT-



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]
```

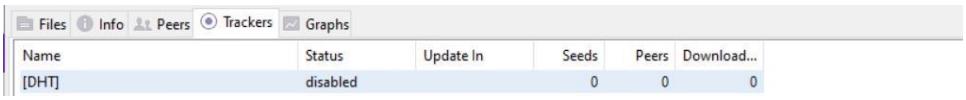
e. DHT status



Files | Info | Peers | Trackers | Graphs

Name	Status	Update In	Seeds	Peers	Download...
[DHT]	working	22m 14s	13	91	0

And below diagrams shows the disabled status



Files | Info | Peers | Trackers | Graphs

Name	Status	Update In	Seeds	Peers	Download...
[DHT]	disabled		0	0	0

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 it sip address and port number are 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)
  Terminator: e
saction ID: a8530000
```

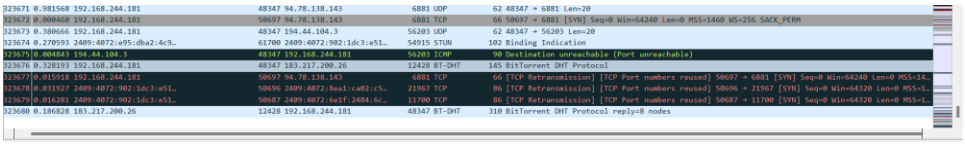
Ip address will be 119.193.226.69

g. Try to identify the name of the file downloaded

```
⌄ 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.



323671	0.981568	192.168.244.181	48347 94.78.138.143	6881 UDP	62 48347 → 6881 Len=20
323672	0.000460	192.168.244.181	50697 94.78.138.143	6881 TCP	66 50697 → 6881 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
323673	0.300666	192.168.244.181	48347 194.44.104.3	56203 UDP	62 48347 → 56203 Len=20
323674	0.270593	2409:4072:e95:dba2:4c9…	61700 2409:4072:902:1dc3:e51…	54915 STUN	102 Binding Indication
323675	0.004843	194.44.104.3	48347 192.168.244.181	56203 ICMP	90 Destination unreachable (Port unreachable)
323676	0.328193	192.168.244.181	48347 183.217.200.26	12428 BT-DHT	145 BitTorrent DHT Protocol
323677	0.015918	192.168.244.181	50697 94.78.138.143	6881 TCP	66 [TCP Retransmission] [TCP Port numbers reused] 50697 → 6881 [SYN] Seq=0 Win=64240 Len=0 MSS=14…
323678	0.031927	2409:4072:902:1dc3:e51…	50696 2409:4072:8ea1:ca02:c5…	21967 TCP	86 [TCP Retransmission] [TCP Port numbers reused] 50696 → 21967 [SYN] Seq=0 Win=64320 Len=0 MSS=1…
323679	0.016281	2409:4072:902:1dc3:e51…	50687 2409:4072:6e1f:2484:6c…	11700 TCP	86 [TCP Retransmission] [TCP Port numbers reused] 50687 → 11700 [SYN] Seq=0 Win=64320 Len=0 MSS=1…
323680	0.186828	183.217.200.26	12428 192.168.244.181	48347 BT-DHT	310 BitTorrent DHT Protocol reply=8 nodes

Here I didn’t get any packets for seeding. Since there wasn’t any seeding.

<u>Result:</u>

Hence successfully analyzed BitTorrent and bht protocols using Wireshark.