

21CY681– Internet Protocol lab

ASSIGNMENT -10

Name: Rahul Raj

Register Number : CYS22011

Title: Analyzing bittorrent and bht protocols using wireshark

Date of Assignment provided: 10/12/2022

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 communication protocol for peer-to-peer file sharing (P2P), which enables users to distribute data and electronic files over the Internet in a decentralized manner. 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

BITTORRENT-

Time	192.168.36.42	46.139.90.206	Comment
28.379021	50806	Handshake	6881 BitTorrent: Handshake
29.348906	50806	Handshake Extended Have All Unchoke	6881 BitTorrent: Handshake Extended Have All Unchoke
30.719125	50806	Extended Bitfield Len:0x99 Port Extended Interested Req	6881 BitTorrent: Extended Bitfield Len:0x99 Port Extended Inter...
31.368856	50806	Choke	6881 BitTorrent: Choke
32.064795	50806	Allowed Fast Piece (Idx:0x422) Allowed Fast Piece (Idx:0x0)	6881 BitTorrent: Allowed Fast Piece (Idx:0x422) Allowed Fast Pie...
32.978978	50806	Piece (Idx:0xd1 Begin:0x0 Len:0x4000)	6881 BitTorrent: Piece (Idx:0xd1 Begin:0x0 Len:0x4000)
33.419666	50806	Piece (Idx:0xd1 Begin:0x0 Len:0x4000)	6881 BitTorrent: Piece (Idx:0xd1 Begin:0x0 Len:0x4000)
33.516706	50806	Extended	6881 BitTorrent: Extended
33.819364	50806	Piece (Idx:0xd1 Begin:0x8000 Len:0x4000)	6881 BitTorrent: Piece (Idx:0xd1 Begin:0x8000 Len:0x4000)
34.189845	50806	Piece (Idx:0xd1 Begin:0x0 Len:0x4000)	6881 BitTorrent: Piece (Idx:0xd1 Begin:0x0 Len:0x4000)
34.413670	50806	Piece (Idx:0xd1 Begin:0x10000 Len:0x4000)	6881 BitTorrent: Piece (Idx:0xd1 Begin:0x10000 Len:0x4000)
34.629185	50806	Piece (Idx:0xd1 Begin:0x14000 Len:0x4000)	6881 BitTorrent: Piece (Idx:0xd1 Begin:0x14000 Len:0x4000)
34.630089	50806	Have Piece (Idx:0x107) Have Piece (Idx:0x26f) Have Piece	6881 BitTorrent: Have Piece (Idx:0x107) Have Piece (Idx:0x26f) ...
34.836113	50806	Piece (Idx:0xd1 Begin:0x18000 Len:0x4000)	6881 BitTorrent: Piece (Idx:0xd1 Begin:0x18000 Len:0x4000)
35.049350	50806	Piece (Idx:0xd1 Begin:0x1c000 Len:0x4000)	6881 BitTorrent: Piece (Idx:0xd1 Begin:0x1c000 Len:0x4000)
35.872713	50806	Piece (Idx:0x1bd Begin:0x0 Len:0x4000)	6881 BitTorrent: Piece (Idx:0x1bd Begin:0x0 Len:0x4000)
36.085800	50806	Piece (Idx:0x1bd Begin:0x0 Len:0x4000)	6881 BitTorrent: Piece (Idx:0x1bd Begin:0x0 Len:0x4000)
36.317084	50806	Piece (Idx:0x1bd Begin:0x8000 Len:0x4000)	6881 BitTorrent: Piece (Idx:0x1bd Begin:0x8000 Len:0x4000)
36.500202	50806	Piece (Idx:0x1bd Begin:0xc000 Len:0x4000)	6881 BitTorrent: Piece (Idx:0x1bd Begin:0xc000 Len:0x4000)
36.709254	50806	Piece (Idx:0x1bd Begin:0x10000 Len:0x4000)	6881 BitTorrent: Piece (Idx:0x1bd Begin:0x10000 Len:0x4000)
36.710334	50806	Have Piece (Idx:0xf3) Have Piece (Idx:0xd1) Request Piece	6881 BitTorrent: Have Piece (Idx:0xf3) Have Piece (Idx:0xd1) Re...
36.749838	50806	Piece (Idx:0x1bd Begin:0x14000 Len:0x4000)	6881 BitTorrent: Piece (Idx:0x1bd Begin:0x14000 Len:0x4000)

DHT –

Time	192.168.137.150	183.204.155.208	191.179.126.142	116.255.102.168	157.33.225.235	Comment
2022/3/42 06:26:01.818716	27835	BitTorrent DHT Protocol	53757			BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:01.818730	27835	BitTorrent DHT Protocol	53757			BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:02.085888	27835	BitTorrent DHT Protocol: reply=8 nodes	53757			BT-DHT: BitTorrent DHT Protocol: reply=8 nodes
2022/3/42 06:26:08.810431	27835	BitTorrent DHT Protocol	6881			BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:08.810443	27835	BitTorrent DHT Protocol	6881			BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:09.238659	27835	BitTorrent DHT Protocol: reply=8 nodes	6881			BT-DHT: BitTorrent DHT Protocol: reply=8 nodes
2022/3/42 06:26:15.812910	27835	BitTorrent DHT Protocol		49566		BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:15.812915	27835	BitTorrent DHT Protocol		49566		BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:16.291657	27835	BitTorrent DHT Protocol: reply=8 nodes		49566		BT-DHT: BitTorrent DHT Protocol: reply=8 nodes
2022/3/42 06:26:22.814575	27835	BitTorrent DHT Protocol			49379	BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:22.814580	27835	BitTorrent DHT Protocol			49379	BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:22.998476	49379	Destination unreachable (Port unreachable)			27835	ICMP: Destination unreachable (Port unreachable)
2022/3/42 06:26:25.833870	27835	BitTorrent DHT Protocol				BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:25.833875	27835	BitTorrent DHT Protocol				BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:25.834173	27835	BitTorrent DHT Protocol				BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:25.834177	27835	BitTorrent DHT Protocol				BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:25.834342	27835	BitTorrent DHT Protocol				BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:25.834347	27835	BitTorrent DHT Protocol				BT-DHT: BitTorrent DHT Protocol
2022/3/42 06:26:25.834498	27835	BitTorrent DHT Protocol				BT-DHT: BitTorrent DHT Protocol

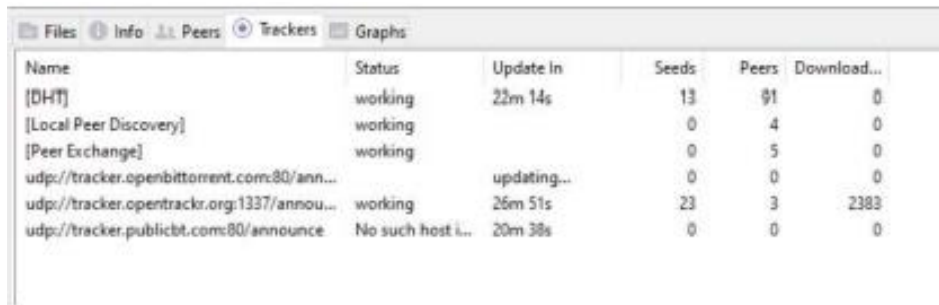
d. Tracker's status.

```

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]

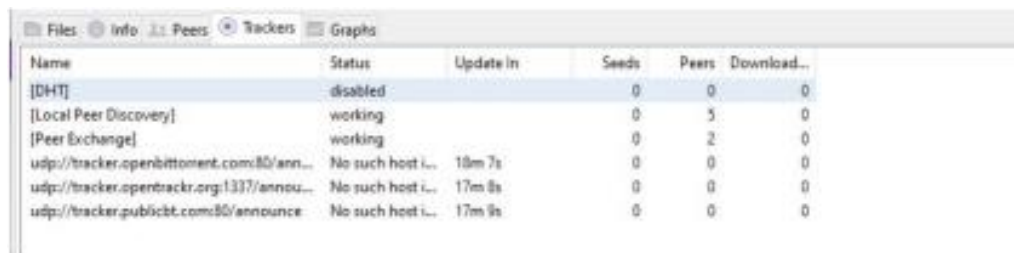
```

e. DHT status.



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.opentracker.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.



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

While seeding the DHT status is set as disabled.

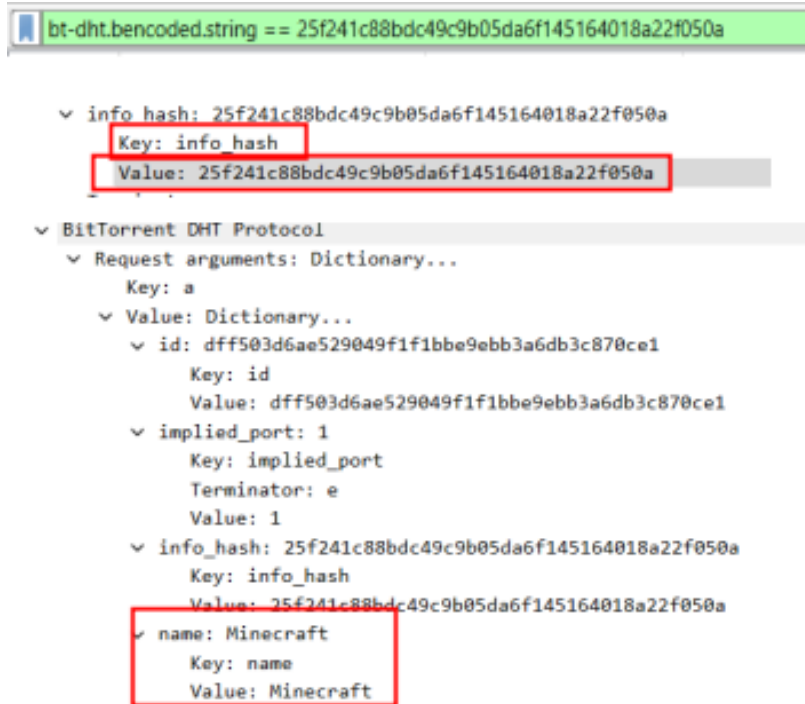
f. Identify other peers involved in the communication

From the below screenshot we can see that there are several nodes which represent a peer and its IP address and port number is shown

```
Key: nodes
v Value: 8 nodes
  > Node 1 {id: dfe04db3460fb98d315cbeaa4539e187b92626a7, IPv4/Port: 86.41.10.163:53020}
  > Node 2 {id: dfe0bee587f8f3564f342a6ecf155ab146c41286, IPv4/Port: 223.109.186.214:6884}
  > Node 3 {id: dfe15bed3bf19c251cf5deb99627aa6f6628c7de, 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: dfe283abd9f97e4450ec636f21351e0920844efb, IPv4/Port: 35.139.52.195:6881}
  > Node 7 {id: dfe34745b5103072aa9c29eb0d3fbc08759a4e1e, IPv4/Port: 121.170.44.25:7890}
  > Node 8 {id: dfe3e29bc55a2853958a91d730417607565b8156, IPv4/Port: 82.65.162.139:6881}
Terminator: e
section ID: a8530000

v Value: 8 nodes
  > Node 1 {id: dfc3c164940003cd8c9e12312aa7b00c02a2a6b3, IPv4/Port: 119.193.226.69:8003}
    ID: dfc3c164940003cd8c9e12312aa7b00c02a2a6b3
    IP: 119.193.226.69
    Port: 8003
  > Node 2 {id: dfc66a15d53c851bfff95cdbc4cf9d6611ade402, IPv4/Port: 121.179.12.75:7795}
    ID: dfc66a15d53c851bfff95cdbc4cf9d6611ade402
    IP: 121.179.12.75
    Port: 7795
  > Node 3 {id: dfc085c6ab80e2cdcb473480e19572ee344121a, IPv4/Port: 69.114.169.254:33806}
  > Node 4 {id: dfc504adfc126eb1ecb59245b21bd341f7fcc0f, IPv4/Port: 221.145.147.185:41070}
```

g. Try to identify the name of the file downloaded



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.

Time	Source	Destination	Protocol	Length	Info
0.000	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.001	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.002	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.003	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.004	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.005	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.006	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.007	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.008	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.009	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.010	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.011	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.012	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.013	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.014	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.015	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.016	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.017	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.018	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.019	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.020	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.021	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.022	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.023	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.024	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.025	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.026	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.027	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.028	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.029	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.030	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.031	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.032	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.033	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.034	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.035	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.036	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.037	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.038	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.039	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.040	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.041	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.042	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.043	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.044	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.045	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.046	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.047	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.048	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.049	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.050	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.051	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.052	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.053	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.054	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.055	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.056	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.057	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.058	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.059	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.060	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.061	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.062	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.063	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.064	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.065	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.066	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.067	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.068	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.069	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.070	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.071	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.072	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.073	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.074	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.075	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.076	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.077	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.078	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.079	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.080	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.081	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.082	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.083	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.084	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.085	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.086	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.087	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.088	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.089	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.090	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.091	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.092	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.093	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.094	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.095	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.096	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.097	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.098	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
0.099	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
0.100	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1