21CY681 - INTERNET PROTOCOL LAB - III

Name: KARTHIKA P Date: 10th December 2022

Assignment Topic: To USE WIRESHARK AND BIT TORRENT TO ANALYSE VARIOUS NETWORK TRAFFIC .

Register Number: CB. EN. P2CYS22001

AIM:

To use Wireshark and Bit torrent to analyse various network traffic.

APPARATUS REQUIRED:

NETWORK MINER

WIRESHARK

BIT TORRENT

QUESTIONS:

Document the answers to the following questions:

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

Bit Torrent 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. To send or receive files, users use a BitTorrent client on their Internet-connected computer.

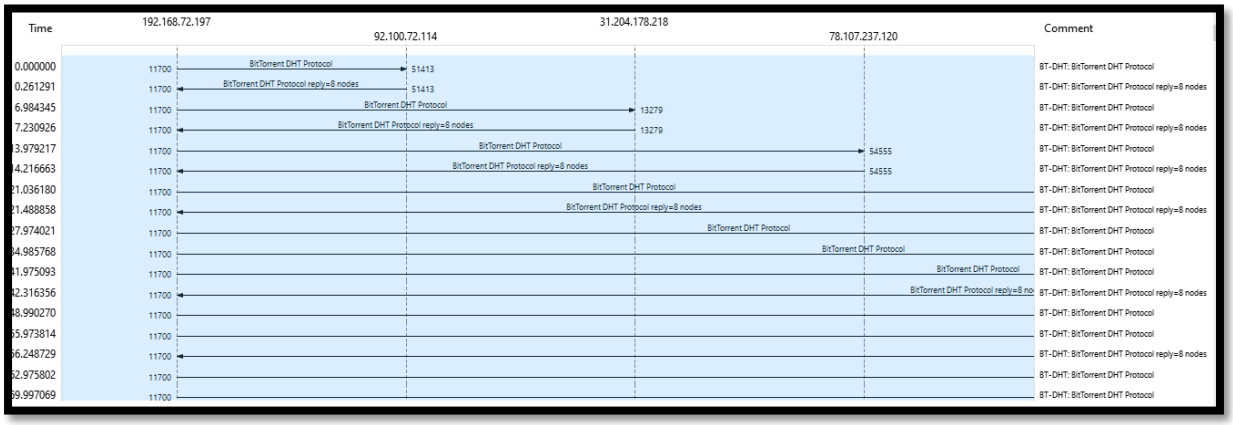
Bit Torrent trackers provide a list of files available for transfer and allow the client to find peer users, known as "seeds", who may transfer the files.

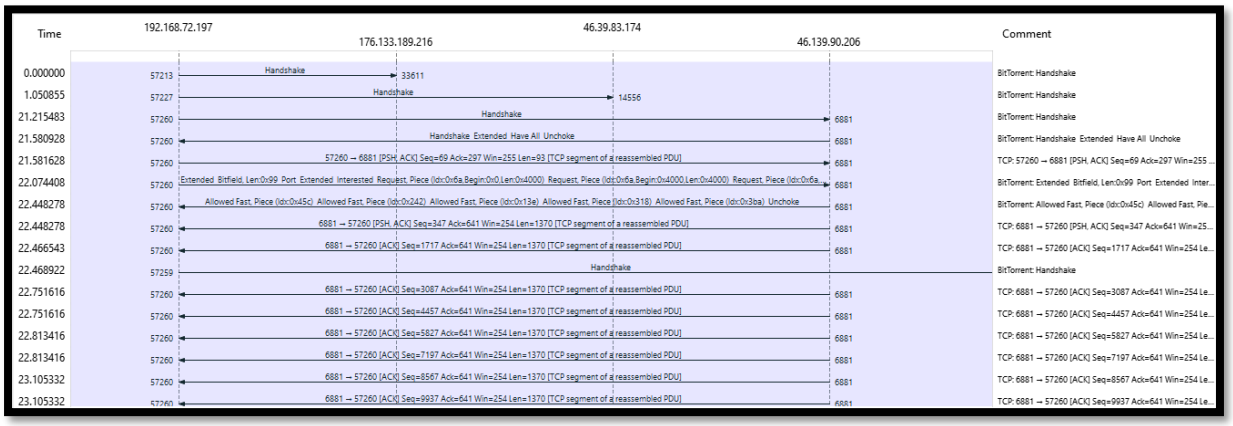
Bit Torrent makes many small data requests over different IP connections to different machines, while server-client downloading is typically made via a single TCP connection to a single machine. Different parts of the file can be obtained from different peers which is used to download in faster way.

b)Working of BitTorrent.

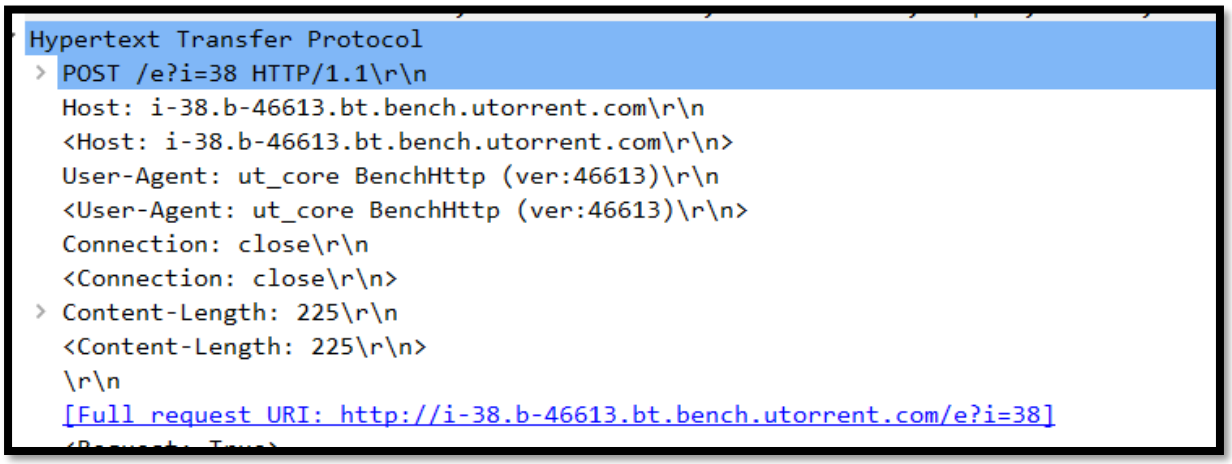
BitTorrent is a protocol (a set of rules that different computer systems agree to use based on P2P that can be used to share large files very efficiently The computer that hosts the original file, in its entirety, is called a seed and it splits the file up into lots of pieces. All the computers cooperating in this way at any time are called a swarm. Each client uploads their part of the file to other clients while simultaneously downloading bits of the file they don't have from other clients. All the clients work together as a swarm to share the file.

c) Protocol Level Analysis





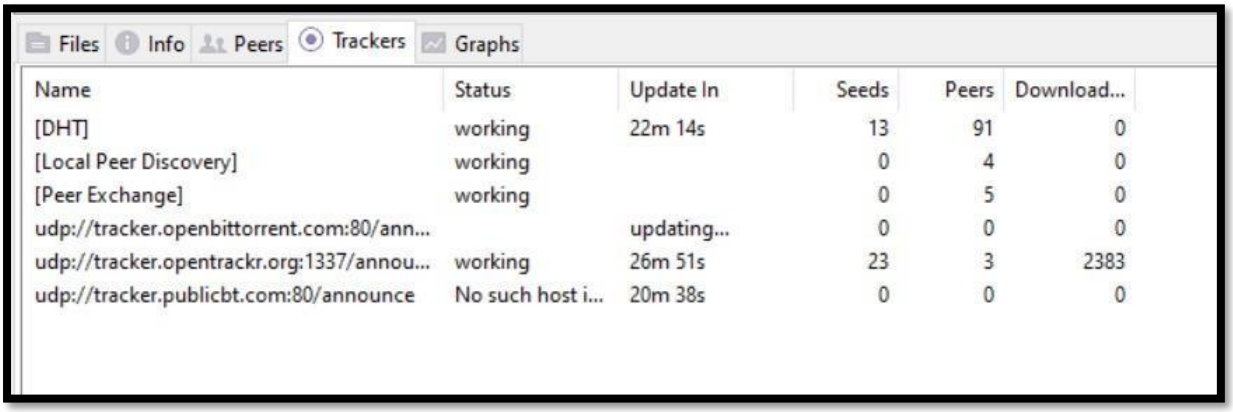
d) Tracker's status.

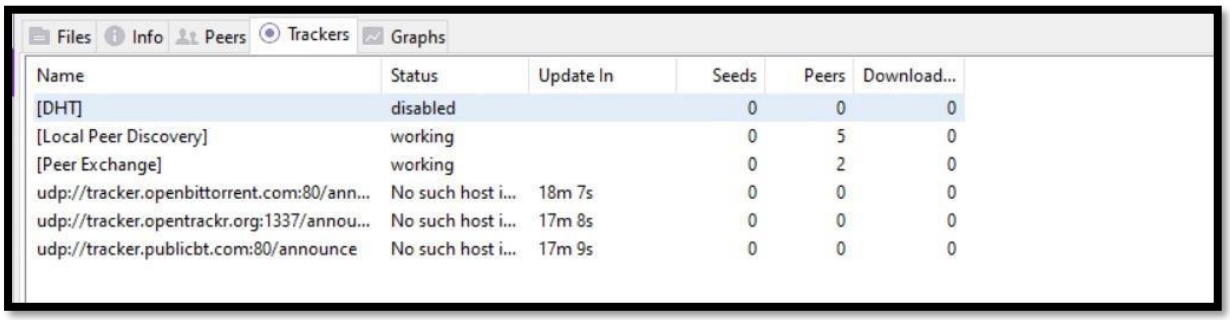


we can see that the name of the tracker is i-38.b□46613.bt.bench.utoorent.com

e)DHT status

Here we can see that while downloading the torrent file the DHT status is set to working.

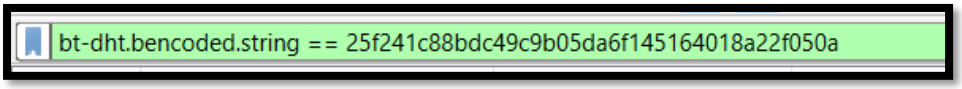


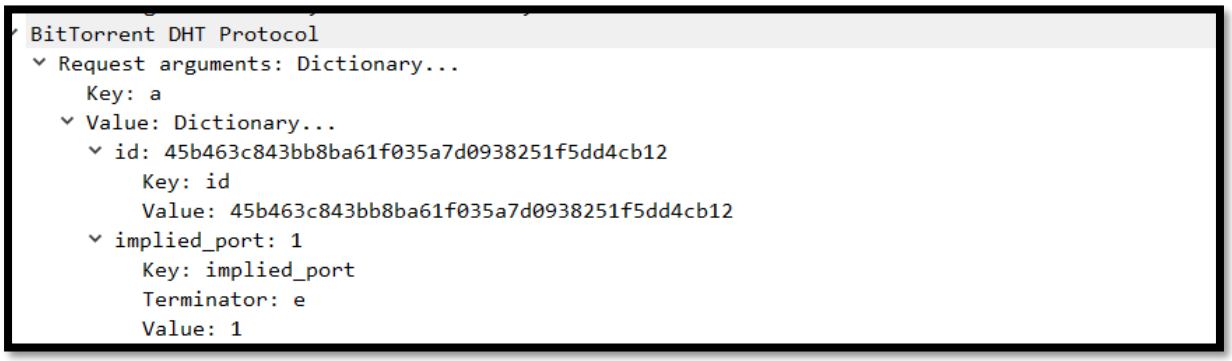


Here while seeding the DHT status is set as disabled.

f)Identify other peers involved in the communication.

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



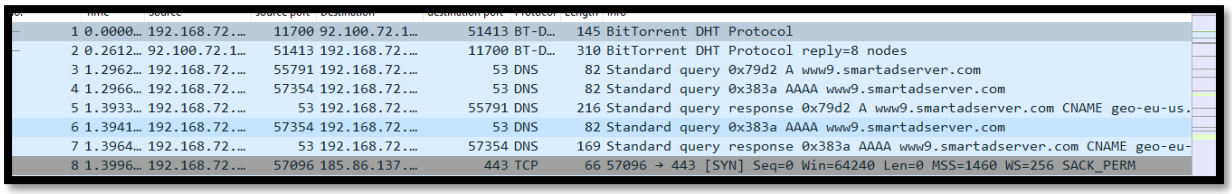


Here we got the file name as minecraft.

5)Try to export the 20% of data you have captured as traffic in Wireshark while downloading files in Torrent.

Packet	Hostname	Content Type	Size	Filename
106	i-38.b-46613.bt.bench.utorrent.com		225 bytes	e?i=38
150	i-38.b-46613.bt.bench.utorrent.com	text/html	21 bytes	e?i=38
222	i-38.b-46613.bt.bench.utorrent.com		227 bytes	e?i=38
276	i-38.b-46613.bt.bench.utorrent.com	text/html	21 bytes	e?i=38
618	i-38.b-46613.bt.bench.utorrent.com		225 bytes	e?i=38
702	i-38.b-46613.bt.bench.utorrent.com	text/html	21 bytes	e?i=38
803	i-38.b-46613.bt.bench.utorrent.com		227 bytes	e?i=38
846	i-38.b-46613.bt.bench.utorrent.com	text/html	21 bytes	e?i=38
1176	i-72.b-46613.bt.bench.utorrent.com		358 bytes	e?i=72
1230	i-72.b-46613.bt.bench.utorrent.com	text/html	21 bytes	e?i=72
1308	i-38.b-46613.bt.bench.utorrent.com		225 bytes	e?i=38
1321	i-38.b-46613.bt.bench.utorrent.com	text/html	21 bytes	e?i=38
1344	i-38.b-46613.bt.bench.utorrent.com		227 bytes	e?i=38
1358	i-38.b-46613.bt.bench.utorrent.com	text/html	21 bytes	e?i=38

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.



1	0.0000…	192.168.72.…	11700	92.100.72.1…	51413	BT-D…	145	BitTorrent DHT Protocol
2	0.2612…	92.100.72.1…	51413	192.168.72.…	11700	BT-D…	310	BitTorrent DHT Protocol reply=8 nodes
3	1.2962…	192.168.72.…	55791	192.168.72.…	53	DNS	82	Standard query 0x79d2 A www9.smartadserver.com
4	1.2966…	192.168.72.…	57354	192.168.72.…	53	DNS	82	Standard query 0x383a AAAA www9.smartadserver.com
5	1.3933…	192.168.72.…	53	192.168.72.…	55791	DNS	216	Standard query response 0x79d2 A www9.smartadserver.com CNAME geo-eu-us.
6	1.3941…	192.168.72.…	57354	192.168.72.…	53	DNS	82	Standard query 0x383a AAAA www9.smartadserver.com
7	1.3964…	192.168.72.…	53	192.168.72.…	57354	DNS	169	Standard query response 0x383a AAAA www9.smartadserver.com CNAME geo-eu-
8	1.3996…	192.168.72.…	57096	185.86.137.…	443	TCP	66	57096 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

Here we didn’t get any packets for seeding. Since there wasn’t any seeding done by our system.