

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.

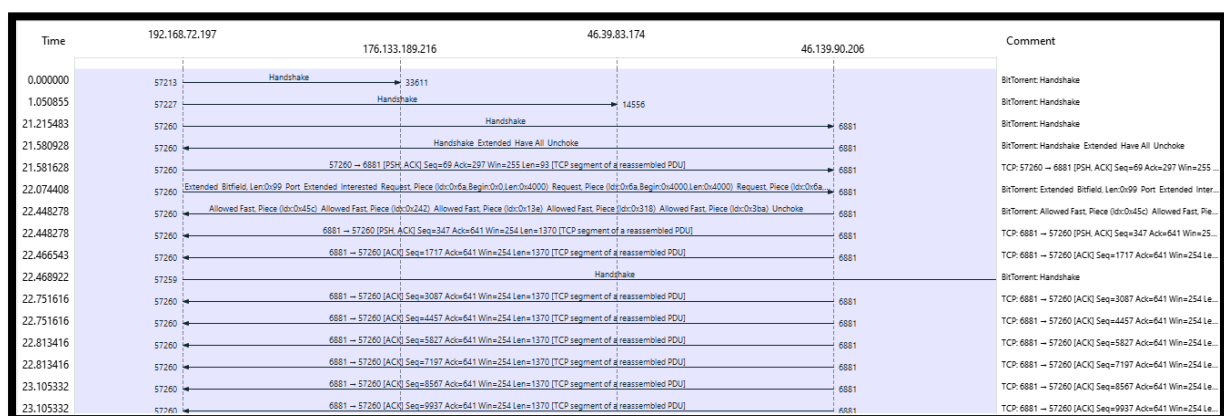
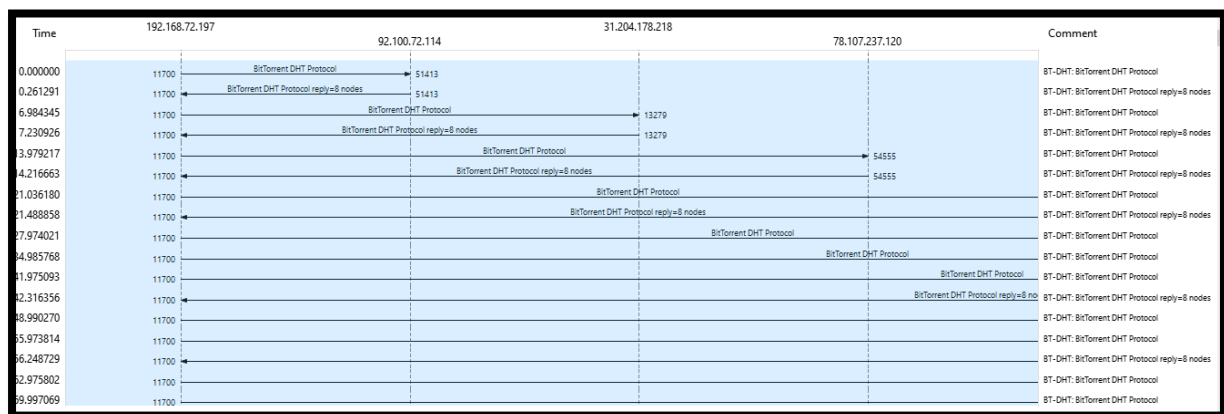
Bit Torrent trackers provide a list of files available for transfer and allow the client to find peer users, known as "seeds", who may transfer the files.

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.

```
Hypertext Transfer Protocol
> POST /e?i=38 HTTP/1.1\r\n
Host: i-38.b-46613.bt.bench.utorrent.com\r\n
<Host: i-38.b-46613.bt.bench.utorrent.com\r\n>
User-Agent: ut_core BenchHttp (ver:46613)\r\n
<User-Agent: ut_core BenchHttp (ver:46613)\r\n>
Connection: close\r\n
<Connection: close\r\n>
> Content-Length: 225\r\n
<Content-Length: 225\r\n>
\r\n
[Full request URI: http://i-38.b-46613.bt.bench.utorrent.com/e?i=38]
```

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.

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

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

Here while seeding the DHT status is set as disabled.

f) Identify other peers involved in the communication.

```
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: dfe34745b5103072aa9c29eb0d3fbc8759a4e1e, IPv4/Port: 121.170.44.25:7890)
    > Node 8 (id: dfe3e29bc55a2853958a91d730417607565b8156, IPv4/Port: 82.65.162.139:6881)
Terminator: e
saction ID: a8530000
```

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

```
bt-dht.bencoded.string == 25f241c88bdc49c9b05da6f145164018a22f050a
```

```
BitTorrent DHT Protocol
  Request arguments: Dictionary...
    Key: a
    Value: Dictionary...
      id: 45b463c843bb8ba61f035a7d0938251f5dd4cb12
        Key: id
        Value: 45b463c843bb8ba61f035a7d0938251f5dd4cb12
      implied_port: 1
        Key: implied_port
        Terminator: e
        Value: 1
```

```
    implied_port: 1
      Key: implied_port
      Terminator: e
      Value: 1
    info_hash: 25f241c88bdc49c9b05da6f145164018a22f050a
      Key: info_hash
      Value: 25f241c88bdc49c9b05da6f145164018a22f050a
    name: Minecraft
      Key: name
      Value: Minecraft
```

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.

No.	Time	Source	Source port	Destination	Destination port	Protocol	Length	Info
1	0.0000...	192.168.72.1...	11700	92.100.72.1...	51413	BT-D...	145	BitTorrent DHT Protocol
2	0.2612...	92.100.72.1...	51413	192.168.72.1...	11700	BT-D...	310	BitTorrent DHT Protocol reply=8 nodes
3	1.2962...	192.168.72.1...	55791	192.168.72.1...	53	DNS	82	Standard query 0x79d2 A www9.smartadserver.com
4	1.2966...	192.168.72.1...	57354	192.168.72.1...	53	DNS	82	Standard query 0x383a AAAA www9.smartadserver.com
5	1.3933...	192.168.72.1...	53	192.168.72.1...	55791	DNS	216	Standard query response 0x79d2 A www9.smartadserver.com CNAME geo-eu-us.
6	1.3941...	192.168.72.1...	57354	192.168.72.1...	53	DNS	82	Standard query 0x383a AAAA www9.smartadserver.com
7	1.3964...	192.168.72.1...	53	192.168.72.1...	57354	DNS	169	Standard query response 0x383a AAAA www9.smartadserver.com CNAME geo-eu-
8	1.3996...	192.168.72.1...	57096	185.86.137.1...	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.