

CMPT371 Project 2 Lab

Weida Pan 301295773

IP

1.

2-06	21:37:33.9151530	192.168.0.104	142.58.102.68	UDP	70	Source port: 52609	Destination port: 33437
2-06	21:37:38.9160690	192.168.0.104	142.58.102.68	UDP	70	Source port: 52609	Destination port: 33438
2-06	21:37:38.9295630	64.59.150.9	192.168.0.104	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)	
2-06	21:37:38.9300530	192.168.0.104	142.58.102.68	UDP	70	Source port: 52609	Destination port: 33439
2-06	21:37:38.9437540	64.59.150.9	192.168.0.104	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)	
2-06	21:37:38.9438830	192.168.0.104	142.58.102.68	UDP	70	Source port: 52609	Destination port: 33440
2-06	21:37:38.9560370	64.59.150.9	192.168.0.104	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)	
2-06	21:37:38.9561020	192.168.0.104	142.58.102.68	UDP	70	Source port: 52609	Destination port: 33441
2-06	21:37:38.9671940	66.163.74.85	192.168.0.104	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)	
2-06	21:37:38.9676060	192.168.0.104	192.168.0.1	DNS	85	Standard query 0xc8fa PTR 85.74.163.66.in-addr.arpa	
2-06	21:37:38.9936970	192.168.0.1	192.168.0.104	DNS	160	Standard query response 0xc8fa No such name	
2-06	21:37:38.9943690	192.168.0.104	142.58.102.68	UDP	70	Source port: 52609	Destination port: 33442
2-06	21:37:39.0058980	66.163.74.109	192.168.0.104	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)	
2-06	21:37:39.0064060	192.168.0.104	142.58.102.68	UDP	70	Source port: 52609	Destination port: 33443
2-06	21:37:39.0201510	66.163.74.89	192.168.0.104	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)	
2-06	21:37:39.0206710	192.168.0.104	192.168.0.1	DNS	85	Standard query 0xd273 PTR 89.74.163.66.in-addr.arpa	
2-06	21:37:39.0444210	192.168.0.1	192.168.0.104	DNS	160	Standard query response 0xd273 No such name	

> Frame 20: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0

> Ethernet II, Src: Apple_03:53:db (a0:99:9b:03:53:db), Dst: D-LinkIn_ac:23:a8 (b8:a3:86:ac:23:a8)

> Internet Protocol Version 4, Src: 192.168.0.104 (192.168.0.104), Dst: 142.58.102.68 (142.58.102.68)

Version: 4

Header Length: 20 bytes

> Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))

Total Length: 56

Identification: 0xcd85 (52613)

> Flags: 0x00

Fragment offset: 0

> Time to live: 2

Protocol: UDP (17)

> Header checksum: 0x35a1 [validation disabled]

Source: 192.168.0.104 (192.168.0.104)

My computer IP address is 192.168.0.104.

2.

See the screen shot in Q1.

The value is UDP.

3.

See the screen shot in Q1.

Header length is 20 bytes. Payload is total length minus header length is 36 bytes.

4.

Identification: 0xcd86 (52614)

▽ Flags: 0x00

0... .. = Reserved bit: Not set

.0... .. = Don't fragment: Not set

..0. = More fragments: Not set

Fragment offset: 0

Since more fragments is not set, this IP datagram is not fragmented.

5.

Identification, time to live and checksum.

6.

Version, header length, total length, flags, fragment offset, protocol, source and destination stay constant. Version, header length, total length, flags, fragment offset, UDP protocol, source and destination must stay constant. Reason are, respectively, we use IPv4, according to the protocol, we set total bytes as 56 bytes, according to protocol, datagram is not fragmented, upper layer protocol is UDP, source IP is the IP of this computer which is fixed, destination IP is also fixed.

Identification, time to live, checksum must change. The first and third change in order to distinguish each packet, the second is because the distance of the packets is going further.

7.

Total Length: 56

Identification: 0xcd8f (52623)

-- --

Identification is a 16

bits number. And the value increases by one as is in the next packet.

8.

```
Version: 4
Header Length: 20 bytes
▷ Differentiated Services Field: 0x0
Total Length: 56
Identification: 0xae99 (44697)
▽ Flags: 0x00
    0... .. = Reserved bit: Not set
    .0... .. = Don't fragment: Not set
    ..0. .... = More fragments: Not set
Fragment offset: 0
Time to live: 57
Protocol: ICMP (1)
```

The value

of Identification is 44697. The value of TTL is 57.

9.

The first packet:

Version: 4

Header Length: 20 bytes

▷ Differentiated Services Field: 0x0

Total Length: 56

Identification: 0xae99 (44697)

▽ Flags: 0x00

0... .. = Reserved bit: Not set

.0... .. = Don't fragment: Not set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 57

Protocol: ICMP (1)

The

```

    version: 4
    Header Length: 20 bytes
    ▸ Differentiated Services Field: 0x00
    Total Length: 56
    Identification: 0xaea5 (44709)
    ▽ Flags: 0x00
        0... .. = Reserved bit: Not set
        .0... .. = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 57
    Protocol: ICMP (1)

```

second packet: .

The third packet:

Version: 4

Header Length: 20 bytes

▷ Differentiated Services Field: 0x00

Total Length: 56

Identification: 0xae4 (44724)

▽ Flags: 0x00

0... .. = Reserved bit: Not set

.0... .. = Don't fragment: Not set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 57

Protocol: ICMP (1)

The

Identifications change, but not TTL. These packets are different, and identification is used to distinguish them. But the distance remains the same, so TTL doesn't change.

10.

8	2015-12-06 21:38:17.5236770	192.168.0.104	142.58.102.68	UDP	534 Source port: 52648 Destination port: 3343
9	2015-12-06 21:38:17.7185220	192.168.0.104	24.244.4.88	TCP	54 56336-443 [ACK] Seq=1 Ack=1 Win=4096 Len=
10	2015-12-06 21:38:17.7409250	24.244.4.88	192.168.0.104	TCP	66 [TCP ACKed unseen segment] 443-56336 [ACK
11	2015-12-06 21:38:19.9113030	192.168.0.105	255.255.255.255	DB-LSP-DI	147 Dropbox LAN sync Discovery Protocol
12	2015-12-06 21:38:19.9113060	192.168.0.105	192.168.0.255	DB-LSP-DI	147 Dropbox LAN sync Discovery Protocol
13	2015-12-06 21:38:21.9313220	192.168.0.104	216.58.216.142	TCP	54 56337-443 [ACK] Seq=1 Ack=1 Win=4103 Len=
14	2015-12-06 21:38:21.9489950	216.58.216.142	192.168.0.104	TCP	66 [TCP ACKed unseen segment] 443-56337 [ACK
15	2015-12-06 21:38:22.5239750	192.168.0.104	142.58.102.68	IPv4	1514 Fragmented IP protocol (proto=UDP 17, off
16	2015-12-06 21:38:22.5239760	192.168.0.104	142.58.102.68	UDP	534 Source port: 52648 Destination port: 3343
17	2015-12-06 21:38:27.5241500	192.168.0.104	142.58.102.68	IPv4	1514 Fragmented IP protocol (proto=UDP 17, off

```
> Frame 7: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: Apple_03:53:db (a0:99:9b:03:53:db), Dst: D-LinkIn_ac:23:a8 (b8:a3:86:ac:23:a8)
> Internet Protocol Version 4, Src: 192.168.0.104 (192.168.0.104), Dst: 142.58.102.68 (142.58.102.68)
  Version: 4
  Header Length: 20 bytes
  ▷ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 1500
  Identification: 0xcda9 (52649)
  ▽ Flags: 0x01 (More Fragments)
    0... .. = Reserved bit: Not set
    .0... .. = Don't fragment: Not set
    ..1. .... = More fragments: Set
  Fragment offset: 0
  ▷ Time to live: 1
  Protocol: UDP (17)
```

Yes.

11.

```
▼ Internet Protocol Version 4, Src: 192.168.0.104 (192.168.0.104), Dst: 142.58.102.68 (142.58.102.68)
  Version: 4
  Header Length: 20 bytes
  ▸ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 1500
    Identification: 0xcdaa (52650)
  ▼ Flags: 0x01 (More Fragments)
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..1. .... = More fragments: Set
    Fragment offset: 0
  ▸ Time to live: 1
    Protocol: UDP (17)
  ▸ Header checksum: 0x10d8 [validation disabled]
    Source: 192.168.0.104 (192.168.0.104)
    Destination: 142.58.102.68 (142.58.102.68)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

In the flag field, more segments is set.

The fragment offset being 0 indicates this fragment is the first.

This datagram is in total 1500 bytes.

12.

```
▼ Internet Protocol Version 4, Src: 192.168.0.104 (192.168.0.104), Dst: 142.58.102.68 (142.58.102.68)
  Version: 4
  Header Length: 20 bytes
  ▸ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 520
    Identification: 0xcdaa (52650)
  ▼ Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    Fragment offset: 1480
  ▸ Time to live: 1
    Protocol: UDP (17)
  ▸ Header checksum: 0x33f3 [validation disabled]
    Source: 192.168.0.104 (192.168.0.104)
    Destination: 142.58.102.68 (142.58.102.68)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

The fragment offset being 1480 indicates this is not the first fragment. But there is no more fragments since more fragments in this datagram is not set.

13.

Total length, flag, fragment offset, header checksum.

14.

No.	Time	Source	Destination	Protocol	Length	Info
1	2015-12-06 21:39:00.0336490	192.168.0.104	142.58.102.68	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, len=1514)
2	2015-12-06 21:39:00.0336500	192.168.0.104	142.58.102.68	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=148, len=1514)
3	2015-12-06 21:39:00.0336500	192.168.0.104	142.58.102.68	UDP	554	Source port: 52690 Destination port: 33435
4	2015-12-06 21:39:03.2522820	192.168.0.104	24.244.4.88	TCP	54	56336->443 [ACK] Seq=1 Ack=1 Win=4096 Len=0
5	2015-12-06 21:39:03.2777680	24.244.4.88	192.168.0.104	TCP	66	[TCP ACKed unseen segment] 443->56336 [ACK] Seq=1
6	2015-12-06 21:39:05.0339250	192.168.0.104	142.58.102.68	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, len=1514)
7	2015-12-06 21:39:05.0339260	192.168.0.104	142.58.102.68	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=148, len=1514)
8	2015-12-06 21:39:05.0339270	192.168.0.104	142.58.102.68	UDP	554	Source port: 52690 Destination port: 33436

Totally three fragments.

15.

Flag, total length, fragment offset, header checksum.