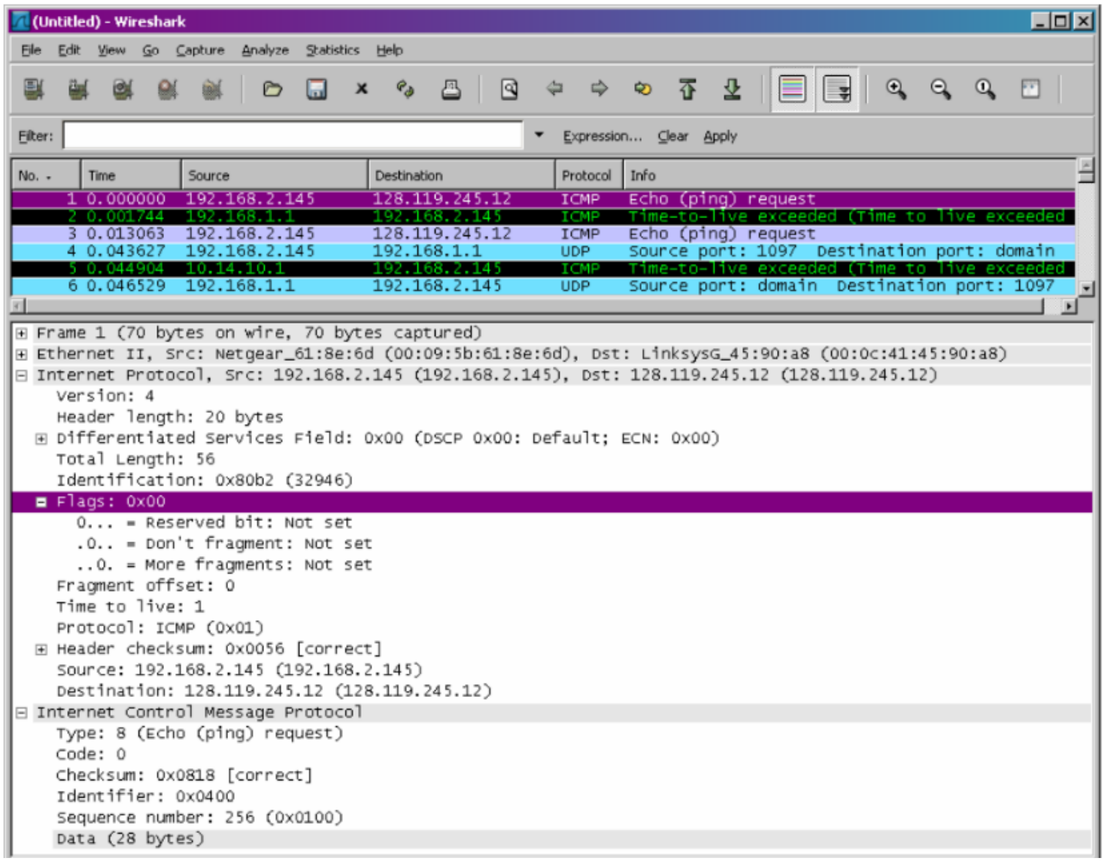
CS425A-Assignment 3

Shrey Mehta (200580)

Abstract

Report for the third assignment of CS425A 2022-23-II offering.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.2.145	128.119.245.12	ICMP	Echo (ping) request
2	0.001744	192.168.1.1	192.168.2.145	ICMP	Time-to-live exceeded (Time to live exceeded
3	0.013063	192.168.2.145	128.119.245.12	ICMP	Echo (ping) request
4	0.043627	192.168.2.145	192.168.1.1	UDP	Source port: 1097 Destination port: domain
5	0.044904	10.14.10.1	192.168.2.145	ICMP	Time-to-live exceeded (Time to live exceeded
6	0.046529	192.168.1.1	192.168.2.145	UDP	Source port: domain Destination port: 1097

```
⊞ Frame 1 (70 bytes on wire, 70 bytes captured)
⊞ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: LinksysG_45:90:a8 (00:0c:41:45:90:a8)
⊟ Internet Protocol, Src: 192.168.2.145 (192.168.2.145), Dst: 128.119.245.12 (128.119.245.12)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 56
    Identification: 0x80b2 (32946)
  ⊟ Flags: 0x00
      0... = Reserved bit: Not set
      .0.. = Don't fragment: Not set
      ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 1
    Protocol: ICMP (0x01)
  ⊞ Header checksum: 0x0056 [correct]
    Source: 192.168.2.145 (192.168.2.145)
    Destination: 128.119.245.12 (128.119.245.12)
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x0818 [correct]
    Identifier: 0x0400
    Sequence number: 256 (0x0100)
    Data (28 bytes)
```

Question 1

Within the IP packet header, the value in the upper layer protocol field is ICMP (0x01).This can be seen from the line in the image "Protocol: ICMP (0x01). Here, ICMP stands for Internet Control Message Protocol.

Question 2

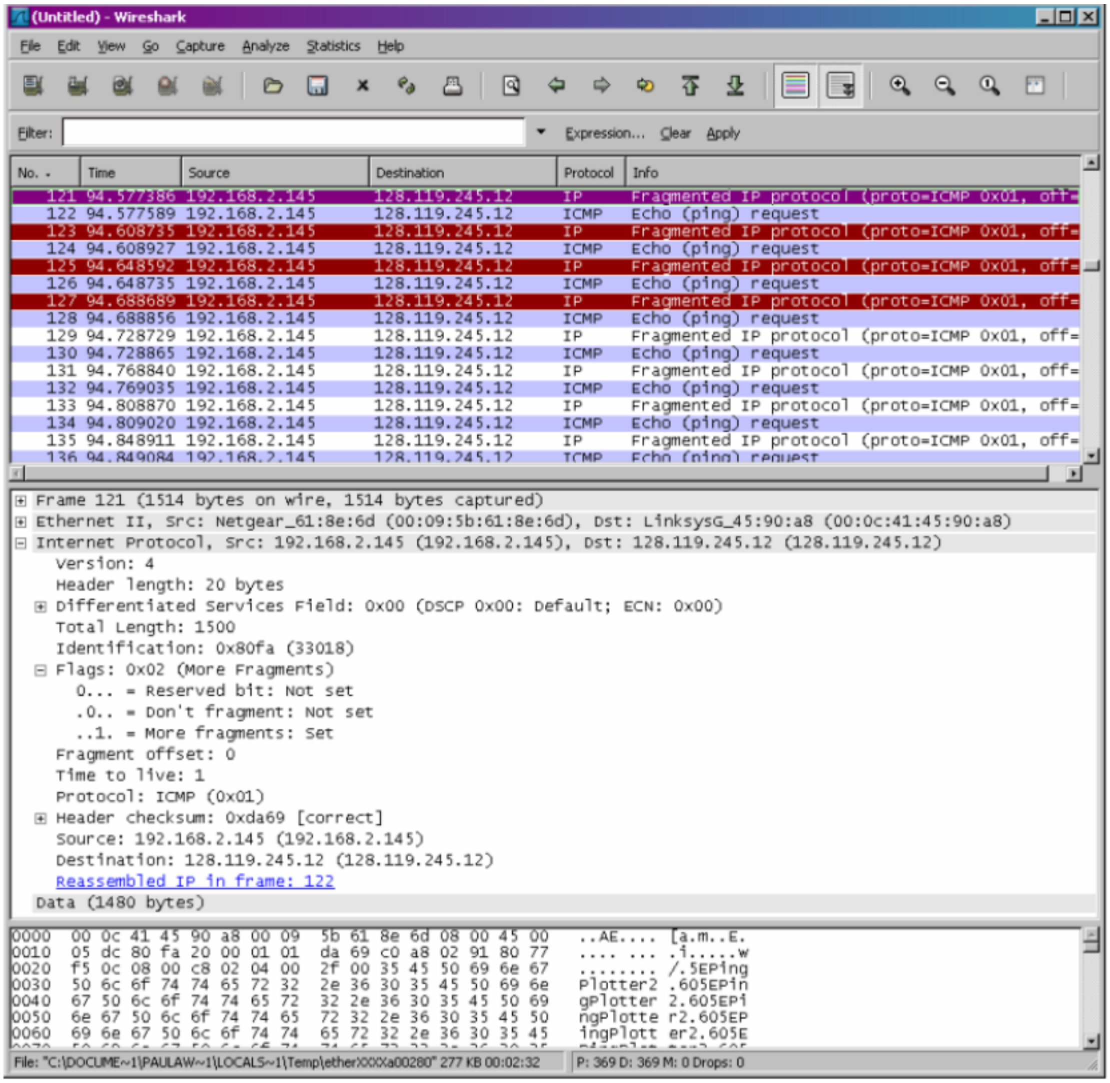
As seen from the image, the IP Header is of 20 bytes, which can been seen from the "Header Length" field. The total length of the Internet Protocol is 56 bytes, which can be seen from the "Total Length" field in the image. So, the number of bytes in the payload of the IP datagram is 56 - 20 = 36 bytes, which can also be obtained by adding the bytes of the ICMP "Type" (8 bytes) field and "Data" (28 bytes) field.

Question 3

The IP datagram has not been fragmented as the More Fragments (MF) field is not set and also, the "Fragment Offset" field is 0.

Question 4

As seen from the image, the value in "Identification" field is 0x80b2 (32946) and that in "TTL" (Time to live) field is 1.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. .  Time      Source          Destination      Protocol Info
  121 94.577386 192.168.2.145   128.119.245.12   IP       Fragmented IP protocol (proto=ICMP 0x01, off=
  122 94.577589 192.168.2.145   128.119.245.12   ICMP     Echo (ping) request
  123 94.608735 192.168.2.145   128.119.245.12   IP       Fragmented IP protocol (proto=ICMP 0x01, off=
  124 94.608927 192.168.2.145   128.119.245.12   ICMP     Echo (ping) request
  125 94.648592 192.168.2.145   128.119.245.12   IP       Fragmented IP protocol (proto=ICMP 0x01, off=
  126 94.648735 192.168.2.145   128.119.245.12   ICMP     Echo (ping) request
  127 94.688689 192.168.2.145   128.119.245.12   IP       Fragmented IP protocol (proto=ICMP 0x01, off=
  128 94.688856 192.168.2.145   128.119.245.12   ICMP     Echo (ping) request
  129 94.728729 192.168.2.145   128.119.245.12   IP       Fragmented IP protocol (proto=ICMP 0x01, off=
  130 94.728865 192.168.2.145   128.119.245.12   ICMP     Echo (ping) request
  131 94.768840 192.168.2.145   128.119.245.12   IP       Fragmented IP protocol (proto=ICMP 0x01, off=
  132 94.769035 192.168.2.145   128.119.245.12   ICMP     Echo (ping) request
  133 94.808870 192.168.2.145   128.119.245.12   IP       Fragmented IP protocol (proto=ICMP 0x01, off=
  134 94.809020 192.168.2.145   128.119.245.12   ICMP     Echo (ping) request
  135 94.848911 192.168.2.145   128.119.245.12   IP       Fragmented IP protocol (proto=ICMP 0x01, off=
  136 94.849084 192.168.2.145   128.119.245.12   ICMP     Echo (ping) request
```

```
⊞ Frame 121 (1514 bytes on wire, 1514 bytes captured)
⊞ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: LinksysG_45:90:a8 (00:0c:41:45:90:a8)
⊟ Internet Protocol, Src: 192.168.2.145 (192.168.2.145), Dst: 128.119.245.12 (128.119.245.12)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 1500
    Identification: 0x80fa (33018)
  ⊟ Flags: 0x02 (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: ICMP (0x01)
  ⊞ Header checksum: 0xda69 [correct]
    Source: 192.168.2.145 (192.168.2.145)
    Destination: 128.119.245.12 (128.119.245.12)
    Reassembled IP in frame: 122
  Data (1480 bytes)
```

```
0000  00 0c 41 45 90 a8 00 09  5b 61 8e 6d 08 00 45 00   ..AE.... [a.m..E.
0010  05 dc 80 fa 20 00 01 01  da 69 c0 a8 02 91 80 77   .... ... .i.....w
0020  f5 0c 08 00 c8 02 04 00  2f 00 35 45 50 69 6e 67   ........ /.5EPing
0030  50 6c 6f 74 74 65 72 32  2e 36 30 35 45 50 69 6e   Plotter2 .605EPin
0040  67 50 6c 6f 74 74 65 72  32 2e 36 30 35 45 50 69   gPlotter 2.605EPi
0050  6e 67 50 6c 6f 74 74 65  72 32 2e 36 30 35 45 50   ngPlotte r2.605EP
0060  69 6e 67 50 6c 6f 74 74  65 72 32 2e 36 30 35 45   ingPlott er2.605E
```

File: "C:\DOCUME~1\PAULAW~1\LOCALS~1\Temp\etherXXXXa00280" 277 KB 00:02:32 | P: 369 D: 369 M: 0 Drops: 0

Question 5

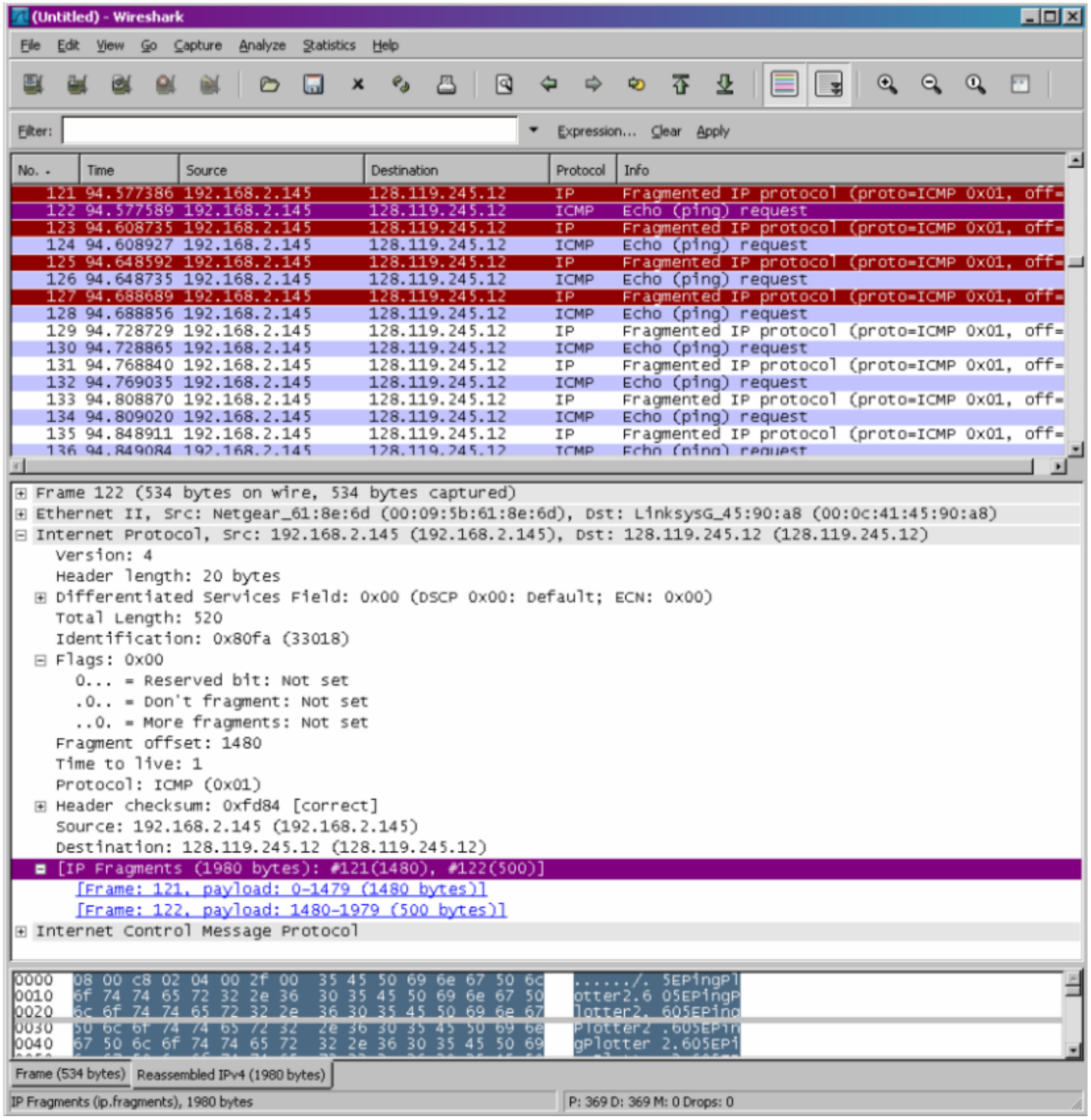
The message corresponding to the above packet has been fragmented as the "More fragments" filed bit has been set to 1.

Question 6

The "More fragments" bit being set to 1 indicates that the datagram has been fragmented.

Question 7

The "Fragment Offset" field being set to 0 under the IP Header shows that this is the first fragment and not any later one.



```
No. -  Time      Source         Destination     Protocol Info
  121 94.577386 192.168.2.145 128.119.245.12  IP       Fragmented IP protocol (proto=ICMP 0x01, off=
  122 94.577589 192.168.2.145 128.119.245.12  ICMP     Echo (ping) request
  123 94.608735 192.168.2.145 128.119.245.12  IP       Fragmented IP protocol (proto=ICMP 0x01, off=
  124 94.608927 192.168.2.145 128.119.245.12  ICMP     Echo (ping) request
  125 94.648592 192.168.2.145 128.119.245.12  IP       Fragmented IP protocol (proto=ICMP 0x01, off=
  126 94.648735 192.168.2.145 128.119.245.12  ICMP     Echo (ping) request
  127 94.688689 192.168.2.145 128.119.245.12  IP       Fragmented IP protocol (proto=ICMP 0x01, off=
  128 94.688856 192.168.2.145 128.119.245.12  ICMP     Echo (ping) request
  129 94.728729 192.168.2.145 128.119.245.12  IP       Fragmented IP protocol (proto=ICMP 0x01, off=
  130 94.728865 192.168.2.145 128.119.245.12  ICMP     Echo (ping) request
  131 94.768840 192.168.2.145 128.119.245.12  IP       Fragmented IP protocol (proto=ICMP 0x01, off=
  132 94.769035 192.168.2.145 128.119.245.12  ICMP     Echo (ping) request
  133 94.808870 192.168.2.145 128.119.245.12  IP       Fragmented IP protocol (proto=ICMP 0x01, off=
  134 94.809020 192.168.2.145 128.119.245.12  ICMP     Echo (ping) request
  135 94.848911 192.168.2.145 128.119.245.12  IP       Fragmented IP protocol (proto=ICMP 0x01, off=
  136 94.849084 192.168.2.145 128.119.245.12  ICMP     Echo (ping) request
```

```
⊞ Frame 122 (534 bytes on wire, 534 bytes captured)
⊞ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: LinksysG_45:90:a8 (00:0c:41:45:90:a8)
⊟ Internet Protocol, Src: 192.168.2.145 (192.168.2.145), Dst: 128.119.245.12 (128.119.245.12)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 520
    Identification: 0x80fa (33018)
  ⊟ 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: ICMP (0x01)
  ⊞ Header checksum: 0xfd84 [correct]
    Source: 192.168.2.145 (192.168.2.145)
    Destination: 128.119.245.12 (128.119.245.12)
  ⊟ [IP Fragments (1980 bytes): #121(1480), #122(500)]
      [Frame: 121, payload: 0-1479 (1480 bytes)]
      [Frame: 122, payload: 1480-1979 (500 bytes)]
⊞ Internet Control Message Protocol
```

```
0000  08 00 c8 02 04 00 2f 00  35 45 50 69 6e 67 50 6c   ....../. 5EPingPl
0010  6f 74 74 65 72 32 2e 36  30 35 45 50 69 6e 67 50   otter2.6 05EPingP
0020  6c 6f 74 74 65 72 32 2e  36 30 35 45 50 69 6e 67   lotter2. 605EPing
0030  50 6c 6f 74 74 65 72 32  2e 36 30 35 45 50 69 6e   Plotter2 .605EPin
0040  67 50 6c 6f 74 74 65 72  32 2e 36 30 35 45 50 69   gPlotter 2.605EPi
```

Frame (534 bytes)
Reassembled IPv4 (1980 bytes)
IP Fragments (ip.fragments), 1980 bytes
P: 369 D: 369 M: 0 Drops: 0

Question 8

The "Fragment Offset" field being set to 1480 under the IP Header shows that this is a later fragment and not the first one. For the datagram to be the first fragment, we require the "Fragment offset" field to be 0.

Question 9

The "More fragments" field bit is set to 0, which shows that there are no more fragments.

Question 10

The following fields change in the IP header between the first and second fragment :

1. Total Length (1500 in the first one and 520 in the second one)
2. More fragments bit under the Flags field (1 in the first one and 0 in the second one causing the Flags field to change with 0x02 in the first one to 0x00 in the second one)
3. Fragment offset (0 in the first one and 1480 in the second one)
4. Header checksum (0xda69 in the first one and 0xfd84 in the second one)