Problem 1

Solution

1.a.

My IP Address is 192.168.0.18

```
No.     Time           Source                Destination           Protocol Length Info
    118 27.169984129   192.168.0.18          139.57.100.6          ICMP     534    Echo (ping) request  id=0x0001, seq=1/256,
ttl=1 (no response found!)
Frame 118: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface wlx9cd643004b89, id 0
Ethernet II, Src: D-LinkIn_00:4b:89 (9c:d6:43:00:4b:89), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
Internet Protocol Version 4, Src: 192.168.0.18, Dst: 139.57.100.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 520
    Identification: 0x3fbb (16315)
    Flags: 0x00b9
        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 (1)
    Header checksum: 0xc787 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.18
    Destination: 139.57.100.6
    [2 IPv4 Fragments (1980 bytes): #117(1480), #118(500)]
Internet Control Message Protocol
```

1.b.

The value in the upper layer protocol field of the IP packet header is ICMP(1)

```
No.     Time           Source                Destination           Protocol Length Info
    118 27.169984129   192.168.0.18          139.57.100.6          ICMP     534    Echo (ping) request  id=0x0001, seq=1/256,
ttl=1 (no response found!)
Frame 118: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface wlx9cd643004b89, id 0
Ethernet II, Src: D-LinkIn_00:4b:89 (9c:d6:43:00:4b:89), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
Internet Protocol Version 4, Src: 192.168.0.18, Dst: 139.57.100.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 520
    Identification: 0x3fbb (16315)
    Flags: 0x00b9
        0... .... .... .... = Reserved bit: Not set
        .0.. .... .... .... = Don't fragment: Not set
        ..0. .... .... .... = More fragments: Not set
    Fragment offset: 1480
    Time to live: 1
        [Expert Info (Note/Sequence): "Time To Live" only 1]
            ["Time To Live" only 1]
            [Severity level: Note]
            [Group: Sequence]
    Protocol: ICMP (1)
    Header checksum: 0xc787 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.18
    Destination: 139.57.100.6
    [2 IPv4 Fragments (1980 bytes): #117(1480), #118(500)]
        [Frame: 117, payload: 0-1479 (1480 bytes)]
        [Frame: 118, payload: 1480-1979 (500 bytes)]
        [Fragment count: 2]
        [Reassembled IPv4 length: 1980]
        [Reassembled IPv4 data: 08006a9a0001000148494a4b4c4d4e4f5051525354555657…]
Internet Control Message Protocol
```

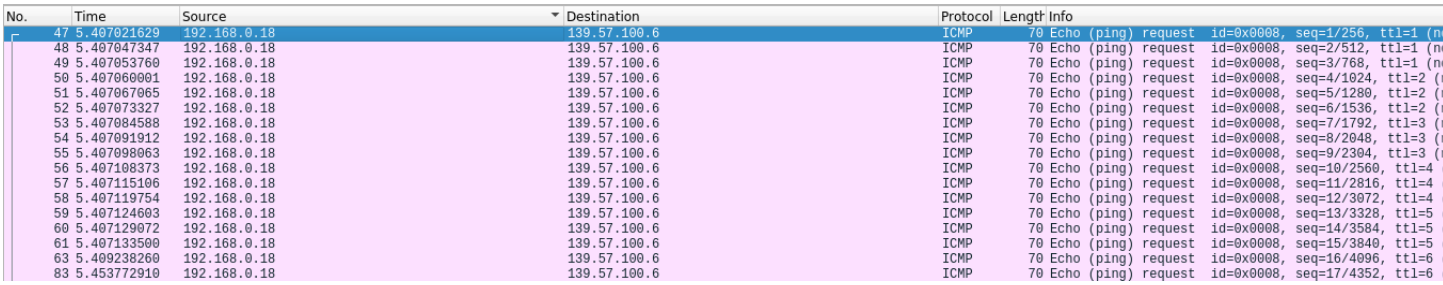
1.c.
20 Bytes in the IP Header. 56 Bytes Total Length. 56 - 20 = 36 Bytes in the Payload

```
No.     Time           Source                Destination           Protocol Length Info
     25 5.625944102    192.168.0.18          139.57.100.6          ICMP     70     Echo (ping) request  id=0x0004, seq=1/256,
ttl=1 (no response found!)
Frame 25: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface wlx9cd643004b89, id 0
Ethernet II, Src: D-LinkIn_00:4b:89 (9c:d6:43:00:4b:89), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
Internet Protocol Version 4, Src: 192.168.0.18, Dst: 139.57.100.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 56
    Identification: 0x631d (25373)
    Flags: 0x0000
        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 (1)
    Header checksum: 0xa6ae [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.18
    Destination: 139.57.100.6
Internet Control Message Protocol
```

1.d.
No this IP Datagram has not been fragmented. The "More Fragments" flag has not been set.

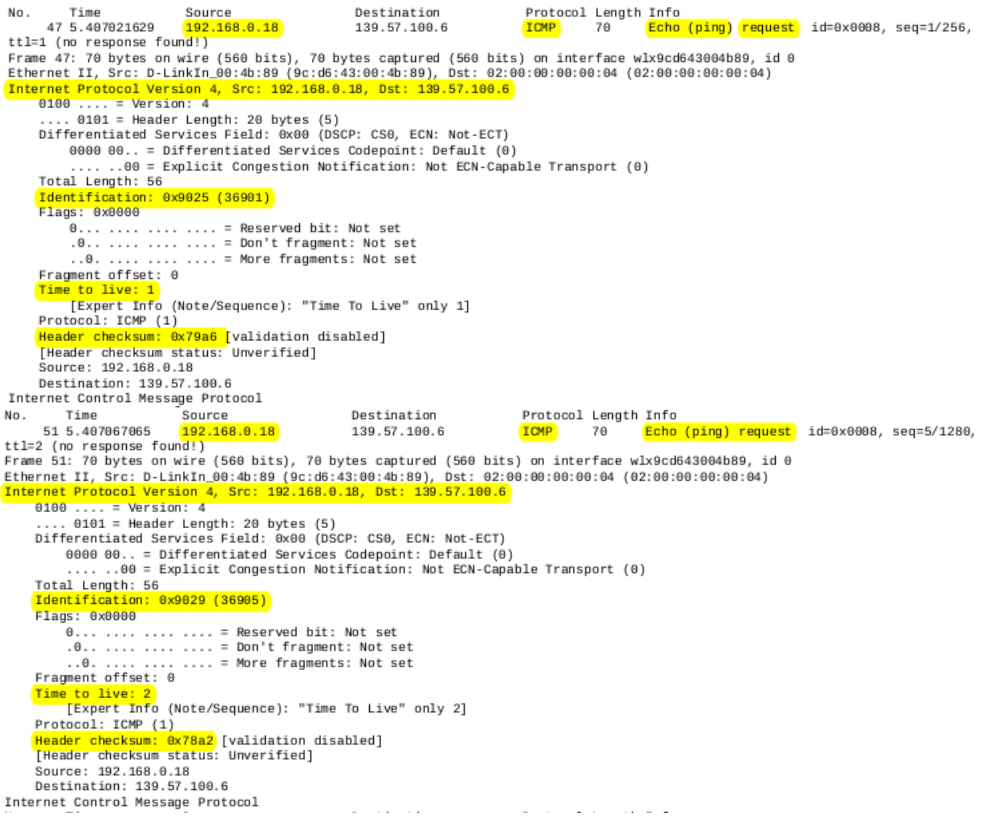
```
No.     Time           Source                Destination           Protocol Length Info
     25 5.625944102    192.168.0.18          139.57.100.6          ICMP     70     Echo (ping) request  id=0x0004, seq=1/256,
ttl=1 (no response found!)
Frame 25: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface wlx9cd643004b89, id 0
Ethernet II, Src: D-LinkIn_00:4b:89 (9c:d6:43:00:4b:89), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
Internet Protocol Version 4, Src: 192.168.0.18, Dst: 139.57.100.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 56
    Identification: 0x631d (25373)
    Flags: 0x0000
        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 (1)
    Header checksum: 0xa6ae [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.18
    Destination: 139.57.100.6
Internet Control Message Protocol
```

1.e.
Identification, Time To Live (TTL), and Header Checksum



No.	Time	Source	Destination	Protocol	Length	Info
47	5.407021629	192.168.0.18	139.57.100.6	ICMP	70	Echo (ping) request id=0x0008, seq=1/256, ttl=1 (n
48	5.407047347	192.168.0.18	139.57.100.6	ICMP	70	Echo (ping) request id=0x0008, seq=2/512, ttl=1 (n
49	5.407053760	192.168.0.18	139.57.100.6	ICMP	70	Echo (ping) request id=0x0008, seq=3/768, ttl=1 (n
50	5.407060001	192.168.0.18	139.57.100.6	ICMP	70	Echo (ping) request id=0x0008, seq=4/1024, ttl=2 (
51	5.407067065	192.168.0.18	139.57.100.6	ICMP	70	Echo (ping) request id=0x0008, seq=5/1280, ttl=2 (
52	5.407073327	192.168.0.18	139.57.100.6	ICMP	70	Echo (ping) request id=0x0008, seq=6/1536, ttl=2 (
53	5.407084588	192.168.0.18	139.57.100.6	ICMP	70	Echo (ping) request id=0x0008, seq=7/1792, ttl=3 (
54	5.407091912	192.168.0.18	139.57.100.6	ICMP	70	Echo (ping) request id=0x0008, seq=8/2048, ttl=3 (
55	5.407098063	192.168.0.18	139.57.100.6	ICMP	70	Echo (ping) request id=0x0008, seq=9/2304, ttl=3 (
56	5.407108373	192.168.0.18	139.57.100.6	ICMP	70	Echo (ping) request id=0x0008, seq=10/2560, ttl=4
57	5.407115106	192.168.0.18	139.57.100.6	ICMP	70	Echo (ping) request id=0x0008, seq=11/2816, ttl=4
58	5.407119754	192.168.0.18	139.57.100.6	ICMP	70	Echo (ping) request id=0x0008, seq=12/3072, ttl=4
59	5.407124603	192.168.0.18	139.57.100.6	ICMP	70	Echo (ping) request id=0x0008, seq=13/3328, ttl=5
60	5.407129072	192.168.0.18	139.57.100.6	ICMP	70	Echo (ping) request id=0x0008, seq=14/3584, ttl=5
61	5.407133500	192.168.0.18	139.57.100.6	ICMP	70	Echo (ping) request id=0x0008, seq=15/3840, ttl=5
63	5.409238260	192.168.0.18	139.57.100.6	ICMP	70	Echo (ping) request id=0x0008, seq=16/4096, ttl=6
83	5.453772910	192.168.0.18	139.57.100.6	ICMP	70	Echo (ping) request id=0x0008, seq=17/4352, ttl=6

TTL changing on the right of the image



```
No.     Time           Source                Destination           Protocol Length Info
     47 5.407021629    192.168.0.18          139.57.100.6          ICMP     70     Echo (ping) request  id=0x0008, seq=1/256,
ttl=1 (no response found!)
Frame 47: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface wlx9cd643004b89, id 0
Ethernet II, Src: D-LinkIn_00:4b:89 (9c:d6:43:00:4b:89), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
Internet Protocol Version 4, Src: 192.168.0.18, Dst: 139.57.100.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 56
    Identification: 0x9025 (36901)
    Flags: 0x0000
        0... .... .... .... = Reserved bit: Not set
        .0.. .... .... .... = Don't fragment: Not set
        ..0. .... .... .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 1
        [Expert Info (Note/Sequence): "Time To Live" only 1]
    Protocol: ICMP (1)
    Header checksum: 0x79a6 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.18
    Destination: 139.57.100.6
Internet Control Message Protocol
No.     Time           Source                Destination           Protocol Length Info
     51 5.407067065    192.168.0.18          139.57.100.6          ICMP     70     Echo (ping) request  id=0x0008, seq=5/1280,
ttl=2 (no response found!)
Frame 51: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface wlx9cd643004b89, id 0
Ethernet II, Src: D-LinkIn_00:4b:89 (9c:d6:43:00:4b:89), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
Internet Protocol Version 4, Src: 192.168.0.18, Dst: 139.57.100.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 56
    Identification: 0x9029 (36905)
    Flags: 0x0000
        0... .... .... .... = Reserved bit: Not set
        .0.. .... .... .... = Don't fragment: Not set
        ..0. .... .... .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 2
        [Expert Info (Note/Sequence): "Time To Live" only 2]
    Protocol: ICMP (1)
    Header checksum: 0x78a2 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.18
    Destination: 139.57.100.6
Internet Control Message Protocol
```

Two Samples showing different TTL, Checksums and Identifications

These screenshot can also be used for **1.f** below

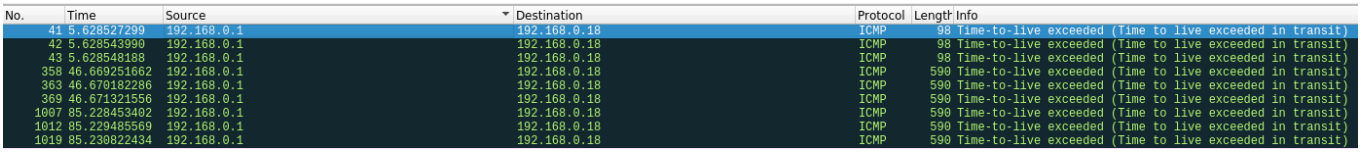
1.f.

The fields that stay constant are also the fields that must stay constant. They are:
Version - Same Version of ICMP protocol (4)
Header Length - Always 20 bits
Source IP Address - Always sending from the same place
Destination IP Address - Always sending to the same place
Differentiated Services - same services
Upper Layer Protocol - Always ICMP here
The fields that must change are:
Identification - each packet needs its own ID
TTL - traceroute increments the TTL between packets
Header Checksum - Since the packets are not identical they will have different Checksum values

1.g.

The pattern is that the Identification Field increases by 1 each time

1.h.



No.	Time	Source	Destination	Protocol	Length	Info
41	5.628527299	192.168.0.1	192.168.0.18	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
42	5.628543990	192.168.0.1	192.168.0.18	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
43	5.628548188	192.168.0.1	192.168.0.18	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
358	46.669251662	192.168.0.1	192.168.0.18	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
363	46.670182286	192.168.0.1	192.168.0.18	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
369	46.671321556	192.168.0.1	192.168.0.18	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
1007	85.228453402	192.168.0.1	192.168.0.18	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
1012	85.229485569	192.168.0.1	192.168.0.18	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
1019	85.230822434	192.168.0.1	192.168.0.18	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)

```
No.     Time           Source                Destination           Protocol Length Info
     41 5.628527299    192.168.0.1           192.168.0.18          ICMP     98     Time-to-live exceeded (Time to live exceeded
in transit)
Frame 41: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlx9cd643004b89, id 0
Ethernet II, Src: 02:00:00:00:00:04 (02:00:00:00:00:04), Dst: D-LinkIn_00:4b:89 (9c:d6:43:00:4b:89)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.18
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xecca (60618)
    Flags: 0x0000
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x0bbb [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.1
    Destination: 192.168.0.18
Internet Control Message Protocol
```

Identification: 0xecca (60618)
TTL: 64

1.i.

This ICMP Echo message has been fragmented into 2 IPv4 Fragments of size 1480 and 500. 1480+500+20(header) = 2000 bytes.

```
No.     Time           Source                Destination           Protocol Length Info
     48 10.755616427   192.168.0.18          139.57.100.6          ICMP     534    Echo (ping) request  id=0x0007, seq=1/256,
ttl=1 (no response found!)
Frame 48: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface wlx9cd643004b89, id 0
Ethernet II, Src: D-LinkIn_00:4b:89 (9c:d6:43:00:4b:89), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
Internet Protocol Version 4, Src: 192.168.0.18, Dst: 139.57.100.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 520
    Identification: 0xcf9b (53147)
    Flags: 0x00b9
        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 (1)
    Header checksum: 0x37a7 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.18
    Destination: 139.57.100.6
    [2 IPv4 Fragments (1980 bytes): #47(1480), #48(500)]
        [Frame: 47, payload: 0-1479 (1480 bytes)]
        [Frame: 48, payload: 1480-1979 (500 bytes)]
        [Fragment count: 2]
        [Reassembled IPv4 length: 1980]
        [Reassembled IPv4 data: 08006a940007000148494a4b4c4d4e4f5051525354555657…]
Internet Control Message Protocol
```

1.j.

The "More Fragments" Flag is set, indicating that the data has been fragmented.
The "Fragment Offset" is set to 0 indicating this is the first fragment.
This IP Datagram has length 1500.

```
No.     Time           Source                Destination           Protocol Length Info
     47 10.755605506   192.168.0.18          139.57.100.6          IPv4     1514   Fragmented IP protocol (proto=ICMP 1, off=0
ID=cf9b) [Reassembled in #48]
Frame 47: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface wlx9cd643004b89, id 0
Ethernet II, Src: D-LinkIn_00:4b:89 (9c:d6:43:00:4b:89), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
Internet Protocol Version 4, Src: 192.168.0.18, Dst: 139.57.100.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xcf9b (53147)
    Flags: 0x2000, More fragments
        0... .... .... .... = Reserved bit: Not set
        .0.. .... .... .... = Don't fragment: Not set
        ..1. .... .... .... = More fragments: Set
    Fragment offset: 0
    Time to live: 1
        [Expert Info (Note/Sequence): "Time To Live" only 1]
            ["Time To Live" only 1]
            [Severity level: Note]
            [Group: Sequence]
    Protocol: ICMP (1)
    Header checksum: 0x148c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.18
    Destination: 139.57.100.6
    Reassembled IPv4 in frame: 48
```

1.k.

There are no more fragments since the "More Fragments" flag is set to 0.

The Fragment Offset is set to 1480 indicating that we have already received the first 1480 bytes of the fragmented message.

We can also see that there are 2 fragments, in frame 47 and 48. This is Frame 48 indicating this is the final fragment.

```
No.     Time           Source                Destination           Protocol Length Info
     48 10.755616427   192.168.0.18          139.57.100.6          ICMP     534    Echo (ping) request  id=0x0007, seq=1/256,
ttl=1 (no response found!)
Frame 48: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface wlx9cd643004b89, id 0
Ethernet II, Src: D-LinkIn_00:4b:89 (9c:d6:43:00:4b:89), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
Internet Protocol Version 4, Src: 192.168.0.18, Dst: 139.57.100.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 520
    Identification: 0xcf9b (53147)
    Flags: 0x00b9
        0... .... .... .... = Reserved bit: Not set
        .0.. .... .... .... = Don't fragment: Not set
        ..0. .... .... .... = More fragments: Not set
    Fragment offset: 1480
    Time to live: 1
        [Expert Info (Note/Sequence): "Time To Live" only 1]
            ["Time To Live" only 1]
            [Severity level: Note]
            [Group: Sequence]
    Protocol: ICMP (1)
    Header checksum: 0x37a7 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.18
    Destination: 139.57.100.6
    [2 IPv4 Fragments (1980 bytes): #47(1480), #48(500)]
        [Frame: 47, payload: 0-1479 (1480 bytes)]
        [Frame: 48, payload: 1480-1979 (500 bytes)]
        [Fragment count: 2]
        [Reassembled IPv4 length: 1980]
        [Reassembled IPv4 data: 08006a940007000148494a4b4c4d4e4f5051525354555657…]
Internet Control Message Protocol
```

1.l.

The fields that changed are:

Flags

Header Checksum
Fragment Offset
Total Length
This can be verified from the screenshots from **1.j** and **1.k**

1.m.

3 Fragments were created

```
No.     Time           Source                Destination           Protocol Length Info
     16 6.040817915    192.168.0.18          139.57.100.6          ICMP     554    Echo (ping) request  id=0x0009, seq=1/256,
ttl=1 (no response found!)
Frame 16: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface wlx9cd643004b89, id 0
Ethernet II, Src: D-LinkIn_00:4b:89 (9c:d6:43:00:4b:89), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
Internet Protocol Version 4, Src: 192.168.0.18, Dst: 139.57.100.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 540
    Identification: 0xa37b (41851)
    Flags: 0x0172
        0... .... .... .... = Reserved bit: Not set
        .0.. .... .... .... = Don't fragment: Not set
        ..0. .... .... .... = More fragments: Not set
    Fragment offset: 2960
    Time to live: 1
        [Expert Info (Note/Sequence): "Time To Live" only 1]
    Protocol: ICMP (1)
    Header checksum: 0x62fa [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.18
    Destination: 139.57.100.6
    [3 IPv4 Fragments (3480 bytes): #14(1480), #15(1480), #16(520)]
        [Frame: 14, payload: 0-1479 (1480 bytes)]
        [Frame: 15, payload: 1480-2959 (1480 bytes)]
        [Frame: 16, payload: 2960-3479 (520 bytes)]
        [Fragment count: 3]
        [Reassembled IPv4 length: 3480]
        [Reassembled IPv4 data: 0800b2ef0009000148494a4b4c4d4e4f5051525354555657…]
Internet Control Message Protocol
```

1.n.

The fields that change are Length (between the first 2 fragments and the last), the "more fragments" flag, the fragment offset, and the header checksum

```
No.     Time           Source                Destination           Protocol Length Info
     14 6.040806844    192.168.0.18          139.57.100.6          IPv4     1514   Fragmented IP protocol (proto=ICMP 1, of
ID=a37b) [Reassembled in #16]
Frame 14: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface wlx9cd643004b89, id 0
Ethernet II, Src: D-LinkIn_00:4b:89 (9c:d6:43:00:4b:89), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
Internet Protocol Version 4, Src: 192.168.0.18, Dst: 139.57.100.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xa37b (41851)
    Flags: 0x2000, 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 (1)
    Header checksum: 0x40ac [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.18
    Destination: 139.57.100.6
    Reassembled IPv4 in frame: 16
```

```
No.     Time           Source                Destination           Protocol Length Info
     15 6.040815019    192.168.0.18          139.57.100.6          IPv4     1514   Fragmented IP protocol (proto=ICMP 1,
off=1480, ID=a37b) [Reassembled in #16]
Frame 15: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface wlx9cd643004b89, id 0
Ethernet II, Src: D-LinkIn_00:4b:89 (9c:d6:43:00:4b:89), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
Internet Protocol Version 4, Src: 192.168.0.18, Dst: 139.57.100.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xa37b (41851)
    Flags: 0x20b9, More fragments
        0... .... .... .... = Reserved bit: Not set
        .0.. .... .... .... = Don't fragment: Not set
        ..1. .... .... .... = More fragments: Set
    Fragment offset: 1480
    Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x3ff3 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.18
    Destination: 139.57.100.6
    Reassembled IPv4 in frame: 16
No.     Time           Source                Destination           Protocol Length Info
     16 6.040817915    192.168.0.18          139.57.100.6          ICMP     554    Echo (ping) request  id=0x0009, seq=1/256,
ttl=1 (no response found!)
Frame 16: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface wlx9cd643004b89, id 0
Ethernet II, Src: D-LinkIn_00:4b:89 (9c:d6:43:00:4b:89), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
Internet Protocol Version 4, Src: 192.168.0.18, Dst: 139.57.100.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 540
    Identification: 0xa37b (41851)
    Flags: 0x0172
        0... .... .... .... = Reserved bit: Not set
        .0.. .... .... .... = Don't fragment: Not set
        ..0. .... .... .... = More fragments: Not set
    Fragment offset: 2960
    Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x62fa [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.18
```

Problem 2

Solution

2.a.

The client IP Address is 192.168.1.100

I looked at the very first Source IP Address at Time 0 to determine this.

```
No.     Time           Source                Destination           Protocol Length Info
     1 0.000000       192.168.1.100         10.119.240.64         SNMP     120    get-request 1.3.6.1.2.1.25.3.2.1.5.1
1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
Frame 1: 120 bytes on wire (960 bits), 120 bytes captured (960 bits)
Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 10.119.240.64
User Datagram Protocol, Src Port: 1028, Dst Port: 161
Simple Network Management Protocol
```

2.b.

Source IP: 192.168.1.100

Dest IP: 64.233.169.104

TCP Source Port: 4335

TCP Dest Port: 80

```
No.     Time           Source                Destination           Protocol Length Info
     56 7.109267       192.168.1.100         64.233.169.104        HTTP     689    GET / HTTP/1.1
Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
Hypertext Transfer Protocol
```

2.c.
Time: 7.158797
Source IP: 64.233.169.104
Dest IP: 192.168.1.100
TCP Source Port: 80
TCP Dest Port: 4335

```
No.     Time           Source                Destination           Protocol Length Info
     60 7.158797       64.233.169.104        192.168.1.100         HTTP     814    HTTP/1.1 200 OK  (text/html)
Frame 60: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits)
Ethernet II, Src: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b), Dst: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
Internet Protocol Version 4, Src: 64.233.169.104, Dst: 192.168.1.100
Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760
[3 Reassembled TCP Segments (3620 bytes): #58(1430), #59(1430), #60(760)]
Hypertext Transfer Protocol
Line-based text data: text/html (12 lines)
```

2.d.
Time: 7.075657
Source IP: 192.168.1.100
Dest IP: 64.233.169.104
TCP Source Port: 4335
TCP Dest Port: 80

```
No.     Time           Source                Destination           Protocol Length Info
     53 7.075657       192.168.1.100         64.233.169.104        TCP      66     4335 → 80 [SYN]
SACK_PERM=1
Frame 53: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 4335
    Destination Port: 80
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 4164040420
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x002 (SYN)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...0 .... = Acknowledgment: Not set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ··········S·]
    Window: 65535
```

Time: 7.108986
Source IP: 64.233.169.104
Dest IP: 192.168.1.100
TCP Source Port: 80
TCP Dest Port: 4335

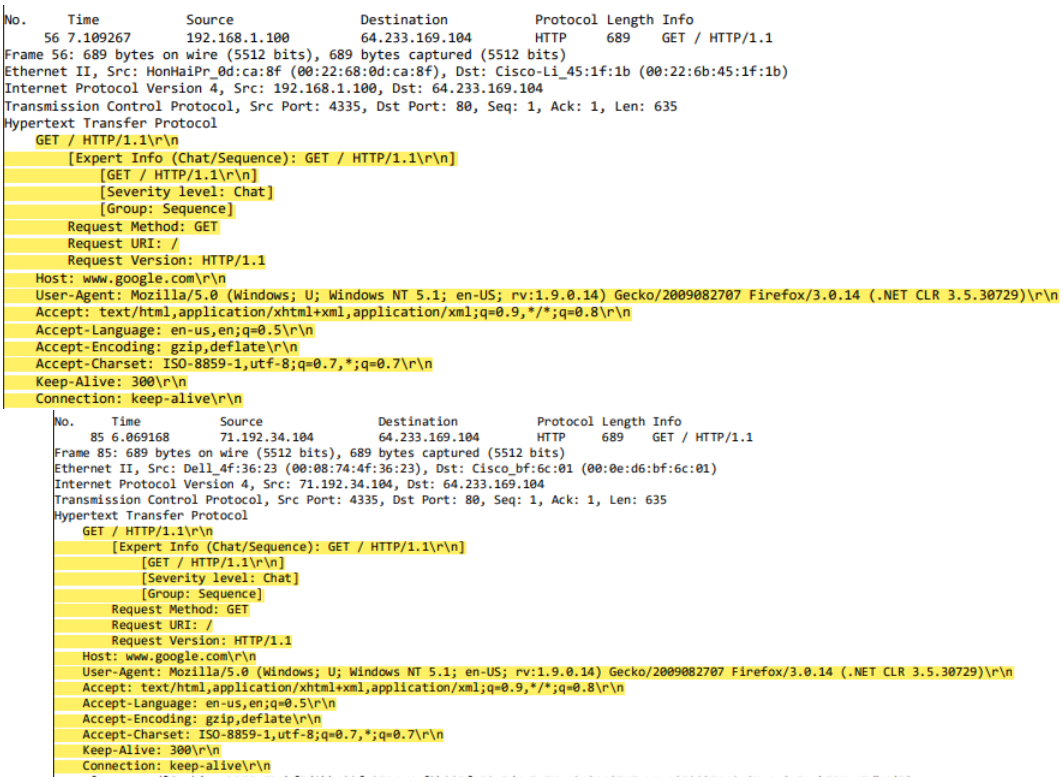
```
No.     Time           Source                Destination           Protocol Length Info
     54 7.108986       64.233.169.104        192.168.1.100         TCP      66     80 → 4335 [SYN, ACK]
MSS=1430 SACK_PERM=1 WS=64
Frame 54: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b), Dst: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
Internet Protocol Version 4, Src: 64.233.169.104, Dst: 192.168.1.100
Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 4335
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 3914283156
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 4164040421
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x012 (SYN, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·····A··S·]
```

2.e.
Time: 6.069168
Source IP: 71.192.34.104
Dest IP: 64.233.169.104
TCP Source Port: 4335
TCP Dest Port: 80

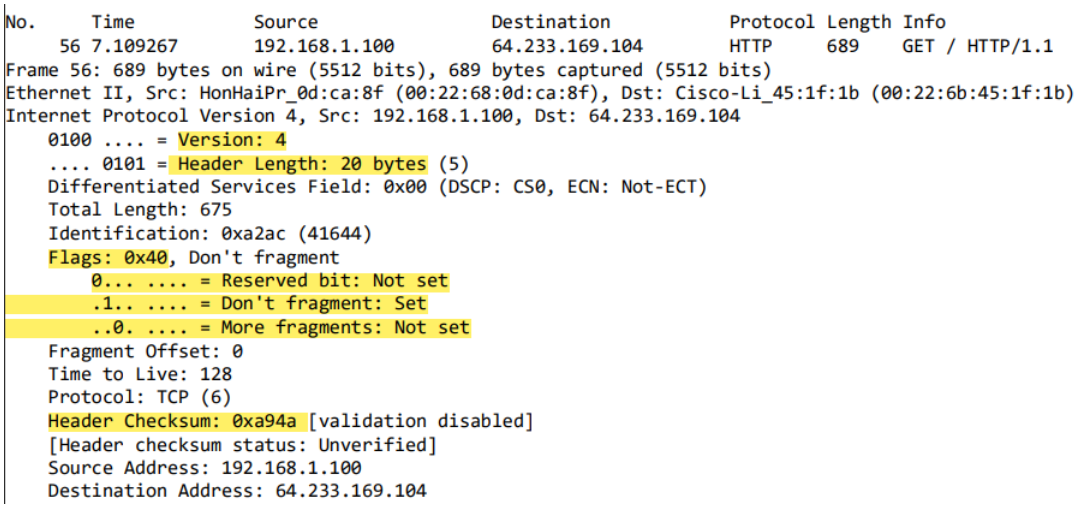
```
No.     Time           Source                Destination           Protocol Length Info
     85 6.069168       71.192.34.104         64.233.169.104        HTTP     689    GET / HTTP/1.1
Frame 85: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
Hypertext Transfer Protocol
```

The Source IP Address is the only difference between here and the 3rd question

2.f.
No. The two HTTP GET messages are below. The first is the home side, the second ISP side. They are identical messages.



Version: No
Header Length: No
Flags: No
Checksum: Yes
The Checksum value is different because the Source IP value is different from before. Since we use the Source IP as part of the Checksum calculation, it will change the final value of the Checksum. Images below. First is home, second is ISP.



```
No.     Time           Source                Destination           Protocol Length Info
     85 6.069168       71.192.34.104         64.233.169.104        HTTP     689    GET / HTTP/1.1
Frame 85: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 675
    Identification: 0xa2ac (41644)
    Flags: 0x40, Don't fragment
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 127
    Protocol: TCP (6)
    Header Checksum: 0x022f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 71.192.34.104
    Destination Address: 64.233.169.104
```

2.g.

Depending on the definition of "first" the time is 6.117570 or 6.308118. If you are asking for the first 200 OK HTTP response in general it is 6.117570 although this response contains no actual content and was used as part of setting up the connection. If you are asking for the first 200 OK HTTP response that contains data the answer is 6.308118. In either case the Source IP/Port and Destination IP/Port are the same.
Source IP: 64.233.169.104
Dest IP: 192.168.1.100
TCP Source Port: 80
TCP Dest Port: 4335
The only difference is the Destination IP Address (from 2d, Destination IP is 192.168.1.100)

```
No.     Time           Source                Destination           Protocol Length Info
     85 6.069168       71.192.34.104         64.233.169.104        HTTP     689    GET / HTTP/1.1
Frame 85: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
Hypertext Transfer Protocol
No.     Time           Source                Destination           Protocol Length Info
     90 6.117570       64.233.169.104        71.192.34.104         HTTP     814    HTTP/1.1 200 OK  (text/html)
Frame 90: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits)
Ethernet II, Src: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104
Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760
[3 Reassembled TCP Segments (3620 bytes): #88(1430), #89(1430), #90(760)]
Hypertext Transfer Protocol
Line-based text data: text/html (12 lines)
No.     Time           Source                Destination           Protocol Length Info
     93 6.241357       71.192.34.104         64.233.169.104        HTTP     719    GET /intl/en_ALL/images/logo.gif HTTP/1.1
Frame 93: 719 bytes on wire (5752 bits), 719 bytes captured (5752 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 636, Ack: 3621, Len: 665
Hypertext Transfer Protocol
No.     Time           Source                Destination           Protocol Length Info
    103 6.308118       64.233.169.104        71.192.34.104         HTTP     226    HTTP/1.1 200 OK  (GIF89a)
Frame 103: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)
Ethernet II, Src: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104
Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 12262, Ack: 1301, Len: 172
[8 Reassembled TCP Segments (8813 bytes): #94(255), #95(1430), #96(1430), #97(1236), #100(1430), #101(1430), #102(1430), #103(172)]
Hypertext Transfer Protocol
```

2.h.

SYN

Source IP: 71.192.34.104
Dest IP: 64.233.169.104
TCP Source Port: 4335
TCP Dest Port: 80
ACK
Source IP: 64.233.169.104
Dest IP: 71.192.34.104
TCP Source Port: 80
TCP Dest Port: 4335
Differences from 2d are:
SYN: Source IP Address is different. (64.233.169.104 in 2d)
ACK: Destination IP Address is different. (192.168.1.100 in 2d)

```
No.     Time           Source                Destination           Protocol Length Info
     82 6.035475       71.192.34.104         64.233.169.104        TCP      66     4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4
SACK_PERM=1
Frame 82: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0
No.     Time           Source                Destination           Protocol Length Info
     83 6.067775       64.233.169.104        71.192.34.104         TCP      66     80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0
MSS=1430 SACK_PERM=1 WS=64
Frame 83: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104
Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 0, Ack: 1, Len: 0
```

2.i.

WAN Side	LAN Side
71.192.34.104, 4335	192.168.1.100, 4335

Table 1: NAT Translation Table