CSC358 Wireshark Assignment 4 Solution

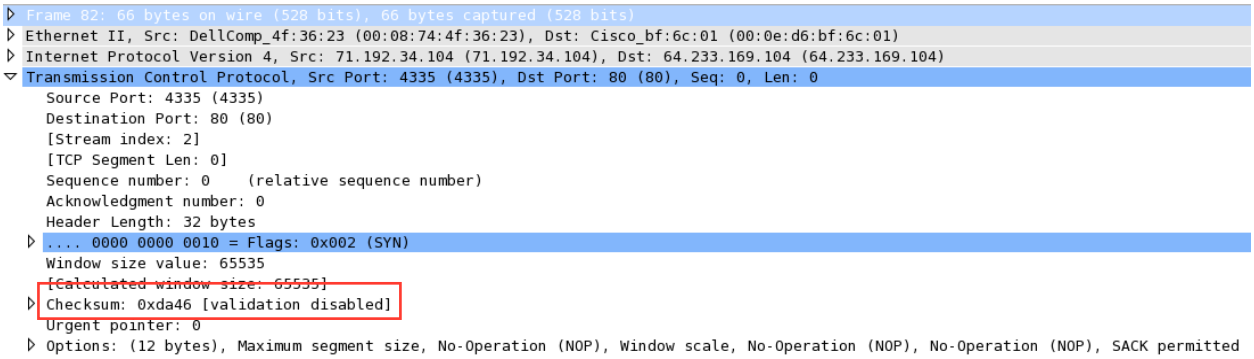
1. What is the client ip on the home side? And what is the client ip on the ISP side? What's the relationship between them?

Solution:
client ip on the home side: 192.168.1.100
client ip on the ISP side: 71.192.34.104
relationship: 71.192.34.104 is the external IP of internal host 192.168.1.100.

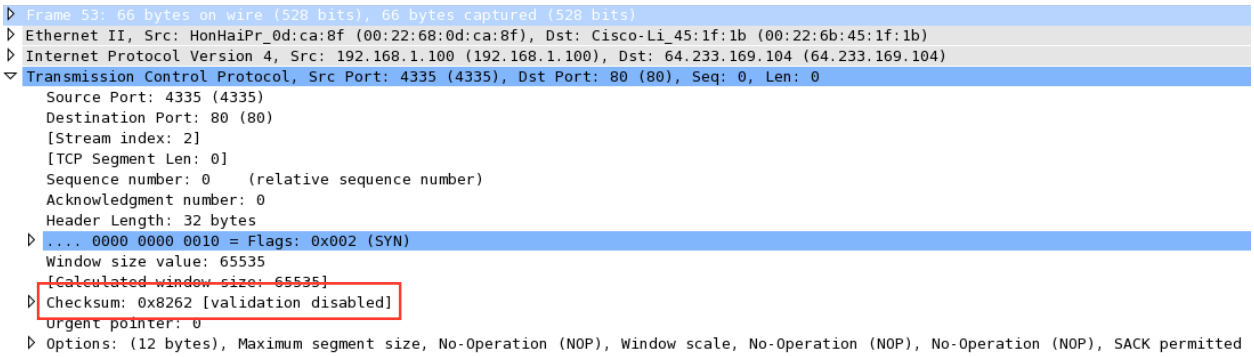
2. For the first packet of this TCP stream, is there anything changed in the TCP header between home side and ISP side? If so, name the header field(s).

Solution:
The “Checksum” field is different.

ISP side:



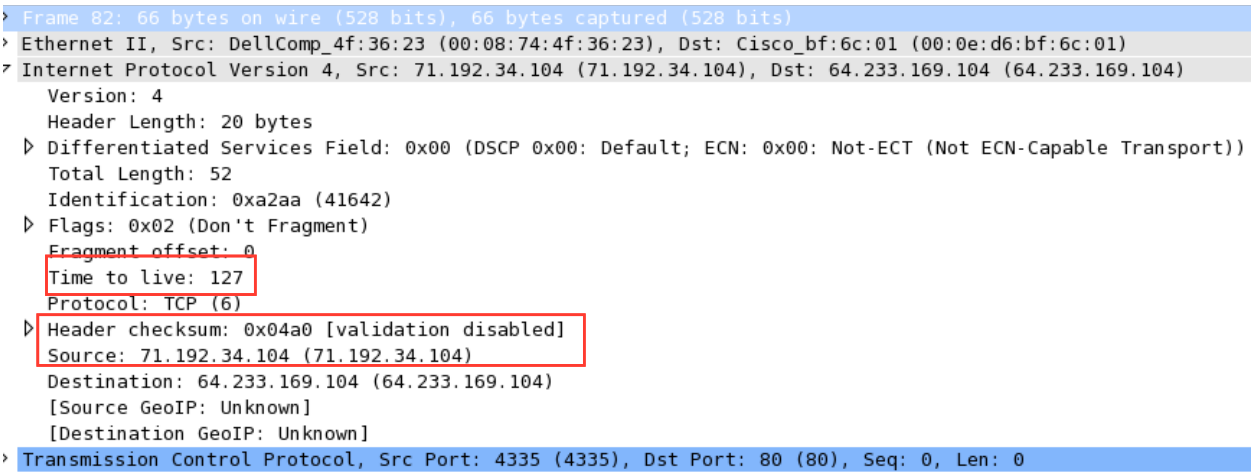
home side:



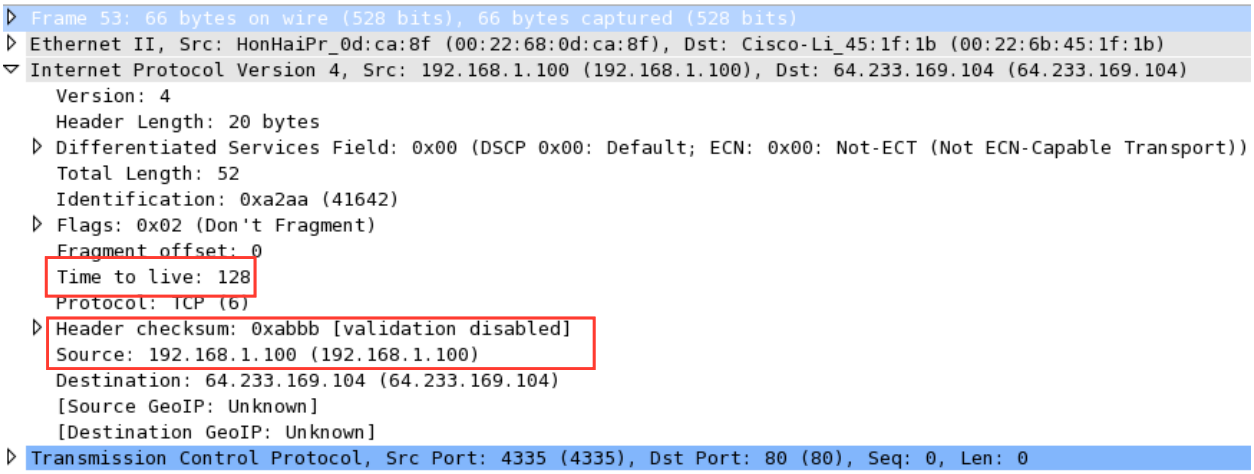
3. Focus on the same packet, is there anything changed in the IP header? If so, name the header field(s), and explain why they are changed?

Solution:
Different fields: Time to live, Header checksum, Source.
Since the IP source address has changed, and the checksum includes the value of the source IP address, the checksum has changed.

ISP side:



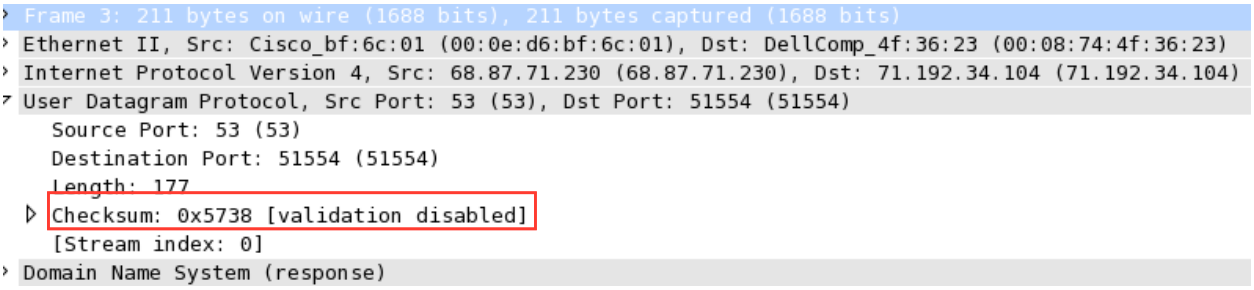
home side:



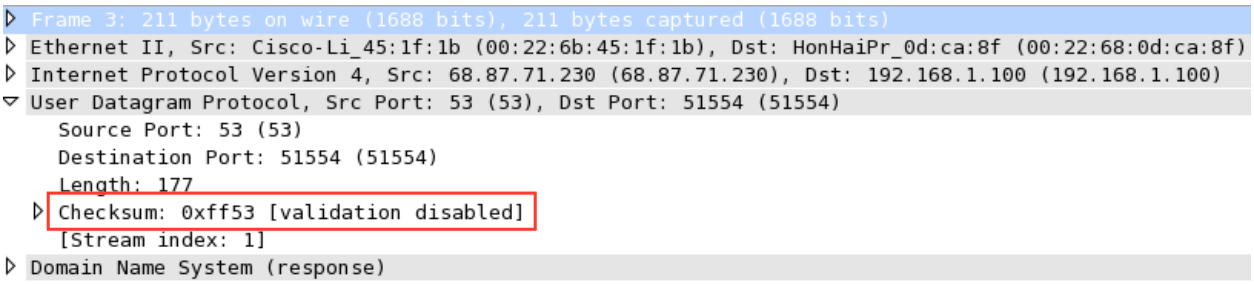
4. For the first packet of this UDP stream, is there anything changed in the UDP header between home side and ISP side? If so, name the header field(s). Is any other udp header or data changed? If not, explain why udp checksum changed.

Solution:
The field of “Checksum” is different.
UDP has a checksum that covers all the data they carry, as well as the UDP header, plus a "pseudo-header" that contains the source and destination IP addresses of the packet carrying the TCP/UDP header. Since the source IP contained in the “pseudo-header” changes, the checksum is also changed correspondingly. It is worth mentioning that no other headers or data is changed.

ISP side:



home side:



5. For the tcp and udp streams we discussed above, for all the packets that the client sent, is the tcp/udp source port ever changed by the router? If not, is it mandatory to keep the same port before and after NAT translation?

Solution:
It is not mandatory to preserve port number for both TCP and UDP, as long as the router can distinguish each stream and forward packet to corresponding internal hosts.

6. Why is it that an ICMP packet does not have source and destination port number?

Solution:
The ICMP packet does not have source and destination port numbers because it was designed to communicate network-layer information between hosts and routers, not between application layer processes. Each ICMP packet has a "Type" and a "Code". The Type/Code combination identifies the specific message being received. Since the network software itself interprets all ICMP messages, no port numbers are needed to direct the ICMP message to an application layer process.

7. Choose one of the ping request packets sent by your host, what are the ICMP type and code numbers? Find the corresponding ping reply, what are the type and code numbers?

Solution:
ping request:
type: 8
code number: 0

ping reply:
type: 0
code number: 0

ping request:

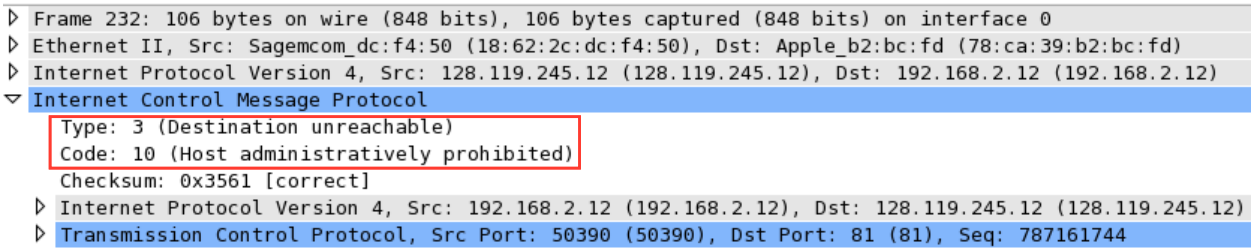
```
▷ Frame 234: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▷ Ethernet II, Src: Apple_b2:bc:fd (78:ca:39:b2:bc:fd), Dst: Sagemcom_dc:f4:50 (18:62:2c:dc:f4:50)
▷ Internet Protocol Version 4, Src: 192.168.2.12 (192.168.2.12), Dst: 128.119.245.12 (128.119.245.12)
▽ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4e6a [correct]
    Identifier (BE): 27654 (0x6c06)
    Identifier (LE): 1644 (0x066c)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    [Response frame: 235]
    Timestamp from icmp data: Mar  5, 2016 23:06:06.347901000 EST
    [Timestamp from icmp data (relative): 0.000059000 seconds]
  ▷ Data (48 bytes)
```

ping reply:

```
▷ Frame 235: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▷ Ethernet II, Src: Sagemcom_dc:f4:50 (18:62:2c:dc:f4:50), Dst: Apple_b2:bc:fd (78:ca:39:b2:bc:fd)
▷ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.2.12 (192.168.2.12)
▽ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x566a [correct]
    Identifier (BE): 27654 (0x6c06)
    Identifier (LE): 1644 (0x066c)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    [Request frame: 234]
    [Response time: 39.385 ms]
    Timestamp from icmp data: Mar  5, 2016 23:06:06.347901000 EST
    [Timestamp from icmp data (relative): 0.039444000 seconds]
  ▷ Data (48 bytes)
```

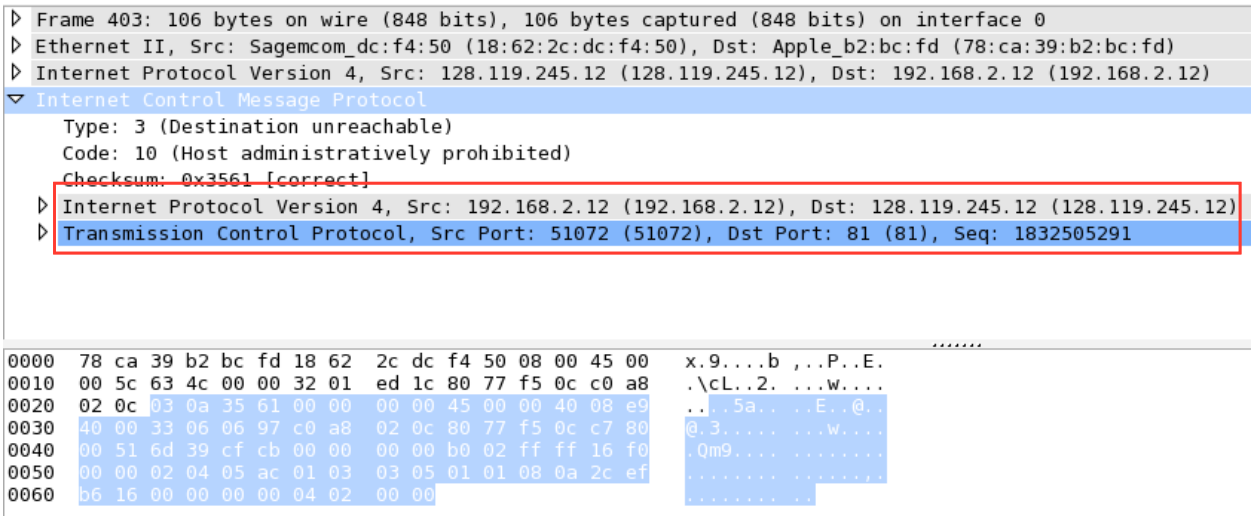
8. During the browser trying to loading the page, did your host receive any ICMP. If yes, what are the type and code of these ICMP packets?

Solution:
Yes.
Type: 3
code: 10



9. Apart from the ICMP headers, what is in the data field of these ICMP packets?

Solution:
The data field contains the IP header and first 8 bytes of original datagram's data.



From wiki:

Destination unreachable message[3]:3

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type = 3								Code								Header checksum															
unused																Next-hop MTU															
IP header and first 8 bytes of original datagram's data																															

10. Image the case when a NAT router receives one of the above ICMP packets on its external interface,how does the router know which internal host to forward this packet to?

Solution:
For ICMP query/reply type messages like Echoes (pings), NAT uses the ICMP Query ID (sometimes just called the ICMP ID) the same way it would use a TCP or UDP port number. For ICMP error messages such as Destination Unreachable, it uses the ICMP packet's internal copy of the headers of the frame that caused the error to figure out which mapping in the NAT table to use to translate it.