NAME____

Introduction to Computer Networks
Project #3 15 points
Due: Oct. 29, 2019
Hand in: answers to Part A questions 1 – 15, answers to Part B questions 1 – 4
Submit at: a hardcopy report in class

Note: The report should include

- your name, the project number, date, and etc.;
- the original questions and your answers right under the questions. Remember to include supporting materials for your answers. You have to explain how you get each answer by showing diagrams/screenshots (0.5pts) when appropriate and highlighting the related fields (0.5pts).
- ***60% of the points count for answering each question, and 40% of the points count for printing out the right supporting material.***
- *This is a group project, and two students a group.*

Part A: DHCP.

DHCP is used extensively in corporate, university and home-network wired and wireless LANs to dynamically assign IP addresses to hosts. In this part, we take a quick look at DHCP, and you are required to use a computer that acquires its IP address dynamically. A good candidate is your home computer or your personal computer, if you don't have access to a computer, then use the trace that have been uploaded to the dropbox (`DHCP-project2.pcap`).

In order to observe DHCP in action, we'll perform several DHCP-related commands and capture the DHCP messages exchanged as a result of executing these commands. Do the following:

1. Begin by opening the Windows Command Prompt application (which can be launched by click start->run->'cmd' or can be found in your Accessories folder). As shown in Figure 1, enter "*ipconfig /release*". The executable for *ipconfig* is in *C:\windows\system32*. This command releases your current IP address.
2. Start up the Wireshark packet sniffer, as described in the introductory Wireshark lab and begin Wireshark packet capture.
3. Now go back to the Windows Command Prompt and enter "*ipconfig /renew*". This instructs your host to obtain a network configuration, including a new IP address. In Figure 1, the host obtains the IP address 129.252.11.208
4. Wait until the "*ipconfig /renew*" has terminated. Then enter the command "*ipconfig/release*" to release the previously-allocated IP address to your computer.
5. Finally, enter "*ipconfig /renew*" to again be allocated an IP address for your computer.
6. Stop Wireshark packet capture.

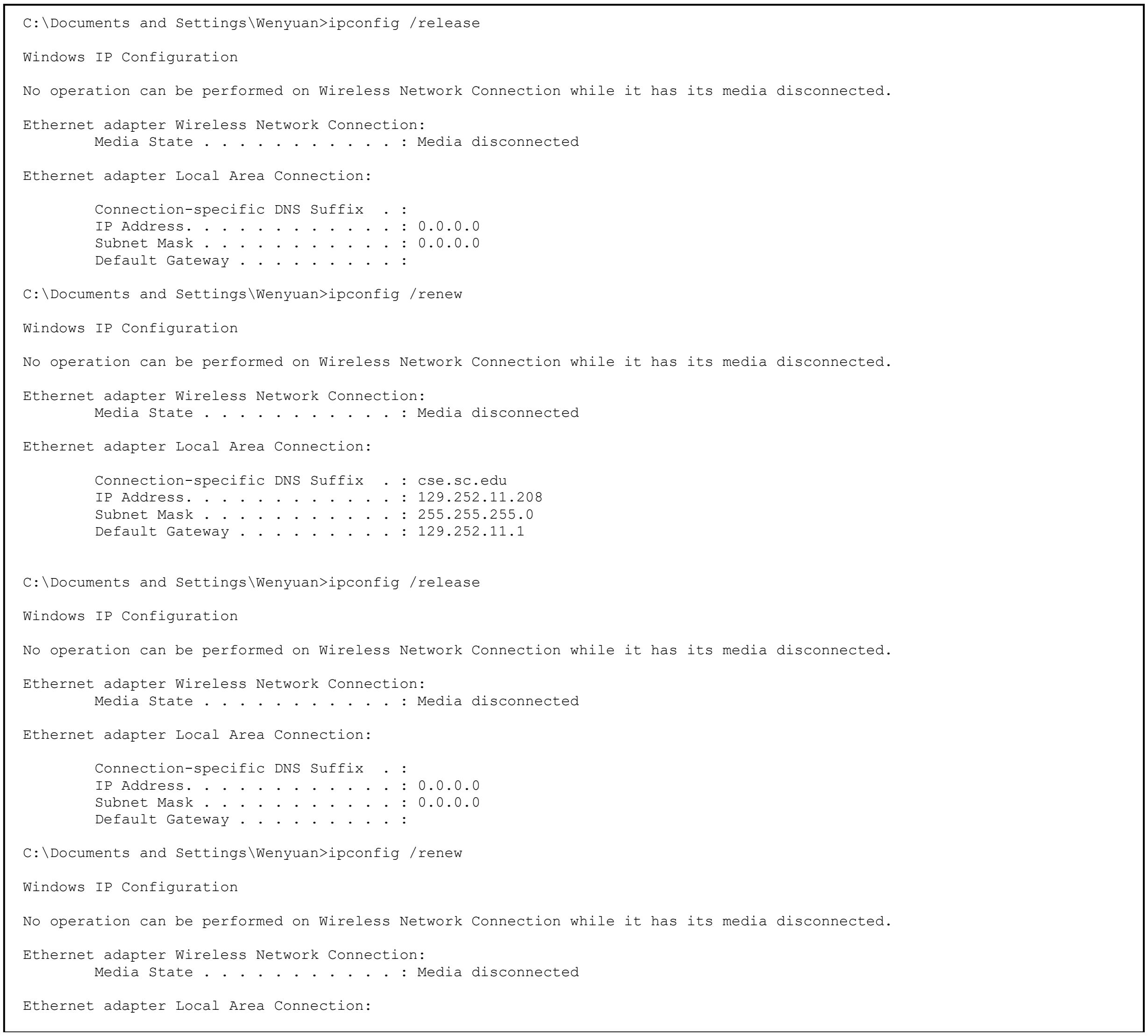
Now let's take a look at the resulting Wireshark window. To see only the DHCP packets, enter into the filter field "bootp". (DHCP derives from an older protocol called BOOTP. Both BOOTP and DHCP use the same port numbers, 67 and 68. To see DHCP packets in the current version of Wireshark, you need to enter "bootp" and not "dhcp" in the filter.) We see from Figure 2 that the first *ipconfig* renew command caused four DHCP packets to be generated: a DHCP Discover packet, a DHCP Offer packet, a DHCP Request packet, and a DHCP ACK packet.

What to hand in:

(1). You should hand in a screen shot of the ***Command Prompt window*** similar to Figure 1.

(2) Whenever possible, when answering a question below, you ***should hand in a printout of the packet(***s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer. To print a packet, use File->Print, choose Selected packet only, choose Packet summary line, and select the minimum amount of packet detail that you need to answer the question.

NAME____



```
C:\Documents and Settings\Wenyuan>ipconfig /release

Windows IP Configuration

No operation can be performed on Wireless Network Connection while it has its media disconnected.

Ethernet adapter Wireless Network Connection:
        Media State . . . . . . . . . . . : Media disconnected

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\Wenyuan>ipconfig /renew

Windows IP Configuration

No operation can be performed on Wireless Network Connection while it has its media disconnected.

Ethernet adapter Wireless Network Connection:
        Media State . . . . . . . . . . . : Media disconnected

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : cse.sc.edu
        IP Address. . . . . . . . . . . . : 129.252.11.208
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 129.252.11.1


C:\Documents and Settings\Wenyuan>ipconfig /release

Windows IP Configuration

No operation can be performed on Wireless Network Connection while it has its media disconnected.

Ethernet adapter Wireless Network Connection:
        Media State . . . . . . . . . . . : Media disconnected

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\Wenyuan>ipconfig /renew

Windows IP Configuration

No operation can be performed on Wireless Network Connection while it has its media disconnected.

Ethernet adapter Wireless Network Connection:
        Media State . . . . . . . . . . . : Media disconnected

Ethernet adapter Local Area Connection:
```

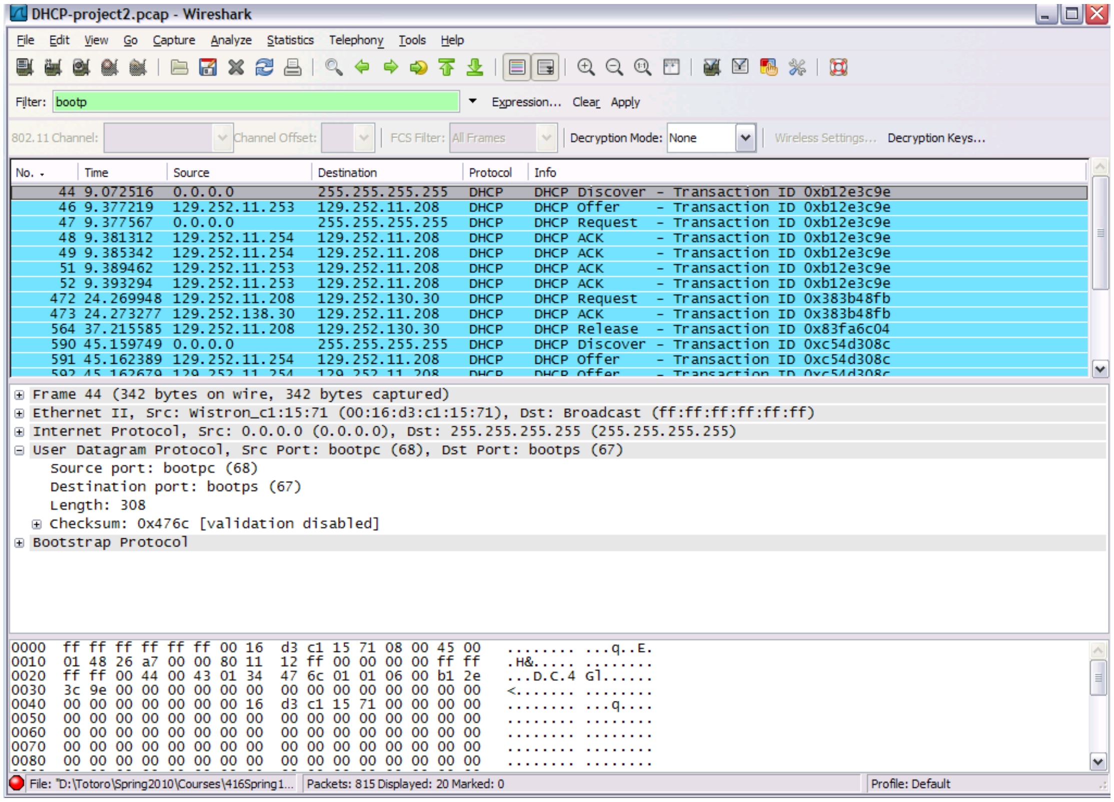
Figure 1: Command Prompt window showing sequence of ipconfig commands that you should enter

Answer the following questions:

1. Are DHCP messages sent over UDP or TCP? Which field in the IP header indicates the type?
2. Which version of IP protocol has been used?
3. Select the first four-packet Discover/Offer/Request/ACK packets. From those packets, determine how many fields there are in the UDP/TCP header. Name these fields.
4. What is the LENGTH field in UDP header? What does the value of the LENGTH field in the UDP header mean: header size, or datagram payload size? Verify your claim with the Discover packet.
5. What are the source and destination port numbers of the DHCP Discover packet and the HDCP Offer packets?
6. What is the largest possible source port number?
7. What is the Ethernet MAC address of the client?
8. Note that the client uses DHCP to obtain and IP address, among other things. But a client's IP address is not confirmed until the end of the four-message exchange. If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.
9. What is the IP address of your computer after sending the DHCP Discover packet?
10. Are all four packets being broadcasted? If some of them are unicasted, explain how each packet can reach its destination?
11. What is the IP address the DHCP server offered?
12. What are the transaction-IDs in all captured packets? Are they the same? What is the purpose of the ID?
13. When DHCP server is not directly connected on the same subnet as the client, a DHCP relay agent is used to relay DHCP messages between the client and the DHCP server. What is the IP address of the DHCP server in your experiment? Is there a relay agent in your experiment? If so what is the IP address of the agent?

NAME____

14. Explain the purpose of the router and subnet mask lines in the DHCP offer message. What is the maximum number of hosts possible on this subnet?
15. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP release request?



```
No.   Time      Source          Destination      Protocol Info
   44 9.072516  0.0.0.0         255.255.255.255  DHCP     DHCP Discover - Transaction ID 0xb12e3c9e
   46 9.377219  129.252.11.253  129.252.11.208   DHCP     DHCP Offer    - Transaction ID 0xb12e3c9e
   47 9.377567  0.0.0.0         255.255.255.255  DHCP     DHCP Request  - Transaction ID 0xb12e3c9e
   48 9.381312  129.252.11.254  129.252.11.208   DHCP     DHCP ACK      - Transaction ID 0xb12e3c9e
   49 9.385342  129.252.11.254  129.252.11.208   DHCP     DHCP ACK      - Transaction ID 0xb12e3c9e
   51 9.389462  129.252.11.253  129.252.11.208   DHCP     DHCP ACK      - Transaction ID 0xb12e3c9e
   52 9.393294  129.252.11.253  129.252.11.208   DHCP     DHCP ACK      - Transaction ID 0xb12e3c9e
  472 24.269948 129.252.11.208  129.252.130.30   DHCP     DHCP Request  - Transaction ID 0x383b48fb
  473 24.273277 129.252.138.30  129.252.11.208   DHCP     DHCP ACK      - Transaction ID 0x383b48fb
  564 37.215585 129.252.11.208  129.252.130.30   DHCP     DHCP Release  - Transaction ID 0x83fa6c04
  590 45.159749 0.0.0.0         255.255.255.255  DHCP     DHCP Discover - Transaction ID 0xc54d308c
  591 45.162389 129.252.11.254  129.252.11.208   DHCP     DHCP Offer    - Transaction ID 0xc54d308c
  592 45.162679 129.252.11.254  129.252.11.208   DHCP     DHCP Offer    - Transaction ID 0xc54d308c

⊞ Frame 44 (342 bytes on wire, 342 bytes captured)
⊞ Ethernet II, Src: Wistron_c1:15:71 (00:16:d3:c1:15:71), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊟ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
    Source port: bootpc (68)
    Destination port: bootps (67)
    Length: 308
  ⊞ Checksum: 0x476c [validation disabled]
⊞ Bootstrap Protocol

0000  ff ff ff ff ff ff 00 16  d3 c1 15 71 08 00 45 00   ........ ...q..E.
0010  01 48 26 a7 00 00 80 11  12 ff 00 00 00 00 ff ff   .H&..... ........
0020  ff ff 00 44 00 43 01 34  47 6c 01 01 06 00 b1 2e   ...D.C.4 Gl......
0030  3c 9e 00 00 00 00 00 00  00 00 00 00 00 00 00 00   <....... ........
0040  00 00 00 00 00 00 00 16  d3 c1 15 71 00 00 00 00   ........ ...q....
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

File: "D:\Totoro\Spring2010\Courses\416Spring1... Packets: 815 Displayed: 20 Marked: 0 Profile: Default

Figure 2 Wireshark window with first DHCP packet

Part B: Ping

The Ping program is simple tool that allows anyone (for example, a network administrator) to verify if a host is live or not. The Ping program in the source host sends a packet to the target IP address; if the target is alive, the Ping program in the target host responds by sending a packet back to the source host.

Do the following to capture the packets generated by the Ping program (you can also use the trace that have been uploaded to the dropbox (`ping-project2.pcap`):

- Opening the Windows Command Prompt application (which can be found in your Accessories folder).
- Start up the Wireshark packet sniffer, and begin Wireshark packet capture.
- Type "ping –n 10 hostname" in the MS-DOS command line (without quotation marks), where hostname is www.cse.sc.edu. The argument "-n 10" indicates that 10 ping messages should be sent. Then run the Ping program by typing return.
- When the Ping program terminates, stop the packet capture in Wireshark.

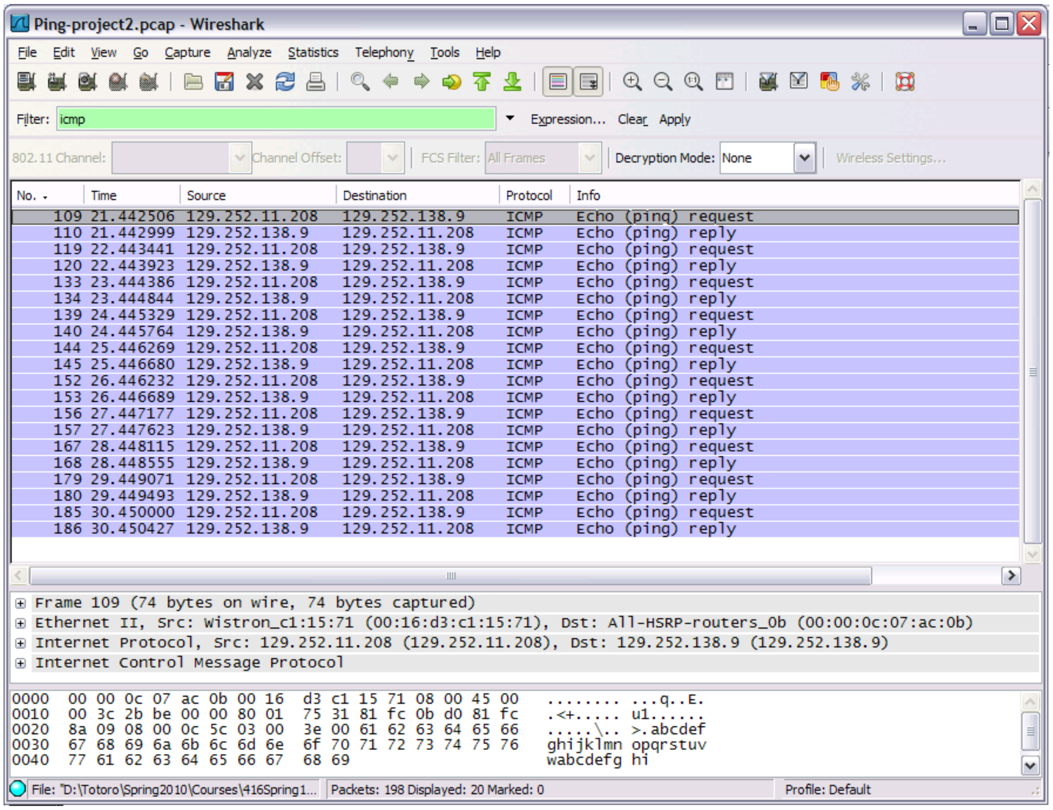
```
C:\Documents and Settings\Wenyuan>ping -n 10 www.cse.sc.edu

Pinging marion.cse.sc.edu [129.252.138.9] with 32 bytes of
data:

Reply from 129.252.138.9: bytes=32 time<1ms TTL=254
Reply from 129.252.138.9: bytes=32 time<1ms TTL=254
Reply from 129.252.138.9: bytes=32 time<1ms TTL=254
Reply from 129.252.138.9: bytes=32 time<1ms TTL=254
Reply from 129.252.138.9: bytes=32 time<1ms TTL=254
Reply from 129.252.138.9: bytes=32 time<1ms TTL=254
Reply from 129.252.138.9: bytes=32 time<1ms TTL=254
Reply from 129.252.138.9: bytes=32 time<1ms TTL=254
Reply from 129.252.138.9: bytes=32 time<1ms TTL=254
Reply from 129.252.138.9: bytes=32 time<1ms TTL=254

Ping statistics for 129.252.138.9:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 3 Command Prompt window after entering Ping command.

At the end of the experiment, your Command Prompt Window should look something like Figure 3. In this example, the source ping program is in `129.252.11.208` and the destination Ping program is in `129.252.138.9`. From this window, we see that the source ping program sent 10 query packets and received 10 responses. Note also that for each response, the source calculates the round-trip time (RTT), which for the 10 packets is on average 1 msec.

Figure 4 provides a screenshot of the Wireshark output, after "icmp" has been entered into the filter display window. Note that the packet listing shows 20 packets: the 10 Ping queries sent by the source and the 10 Ping responses received by the source.

NAME____


Ping-project2.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply
802.11 Channel:
Channel Offset:
FCS Filter: All Frames
Wireless Settings...

Filter: icmp

Decryption Mode: None

```
No. -  Time      Source          Destination     Protocol Info
  109 21.442506 129.252.11.208  129.252.138.9   ICMP     Echo (ping) request
  110 21.442999 129.252.138.9   129.252.11.208  ICMP     Echo (ping) reply
  119 22.443441 129.252.11.208  129.252.138.9   ICMP     Echo (ping) request
  120 22.443923 129.252.138.9   129.252.11.208  ICMP     Echo (ping) reply
  133 23.444386 129.252.11.208  129.252.138.9   ICMP     Echo (ping) request
  134 23.444844 129.252.138.9   129.252.11.208  ICMP     Echo (ping) reply
  139 24.445329 129.252.11.208  129.252.138.9   ICMP     Echo (ping) request
  140 24.445764 129.252.138.9   129.252.11.208  ICMP     Echo (ping) reply
  144 25.446269 129.252.11.208  129.252.138.9   ICMP     Echo (ping) request
  145 25.446680 129.252.138.9   129.252.11.208  ICMP     Echo (ping) reply
  152 26.446232 129.252.11.208  129.252.138.9   ICMP     Echo (ping) request
  153 26.446689 129.252.138.9   129.252.11.208  ICMP     Echo (ping) reply
  156 27.447177 129.252.11.208  129.252.138.9   ICMP     Echo (ping) request
  157 27.447623 129.252.138.9   129.252.11.208  ICMP     Echo (ping) reply
  167 28.448115 129.252.11.208  129.252.138.9   ICMP     Echo (ping) request
  168 28.448555 129.252.138.9   129.252.11.208  ICMP     Echo (ping) reply
  179 29.449071 129.252.11.208  129.252.138.9   ICMP     Echo (ping) request
  180 29.449493 129.252.138.9   129.252.11.208  ICMP     Echo (ping) reply
  185 30.450000 129.252.11.208  129.252.138.9   ICMP     Echo (ping) request
  186 30.450427 129.252.138.9   129.252.11.208  ICMP     Echo (ping) reply
```

```
⊞ Frame 109 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: Wistron_c1:15:71 (00:16:d3:c1:15:71), Dst: All-HSRP-routers_0b (00:00:0c:07:ac:0b)
⊞ Internet Protocol, Src: 129.252.11.208 (129.252.11.208), Dst: 129.252.138.9 (129.252.138.9)
⊞ Internet Control Message Protocol
```

```
0000  00 00 0c 07 ac 0b 00 16  d3 c1 15 71 08 00 45 00   ........ ...q..E.
0010  00 3c 2b be 00 00 80 01  75 31 81 fc 0b d0 81 fc   .<+..... u1......
0020  8a 09 08 00 0c 5c 03 00  3e 00 61 62 63 64 65 66   .....\.. >.abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

File: "D:\Totoro\Spring2010\Courses\416Spring1... Packets: 198 Displayed: 20 Marked: 0 Profile: Default

Figure 4 Wireshark output for Ping program

What to Hand In:

(1) A screen shot of the Command Prompt window similar to Figure 3 above.

(2) Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer.

You should answer the following questions:

1. Which field in the IP header indicates this is an ICMP packet?
2. Why is it that an ICMP packet does not have source and destination port numbers?
3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?
4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?