
VANIER COLLEGE – Computer Engineering Technology – Winter 2021

Network Fundamentals (247-409-VA)

Leonardo Fusser (1946995)

LABORATORY EXPERIMENT 6

Capturing and Understanding Network Traffic

NOTE:

To be completed in one lab session of 3 hrs.

To be submitted using the typical lab format, one week later – at the start of your respective lab session.

This exercise is to be done individually except where specified in the procedure. **Each** student must submit a lab report with original observations and conclusions.

OBJECTIVES:

After performing this experiment, the student will be able to:

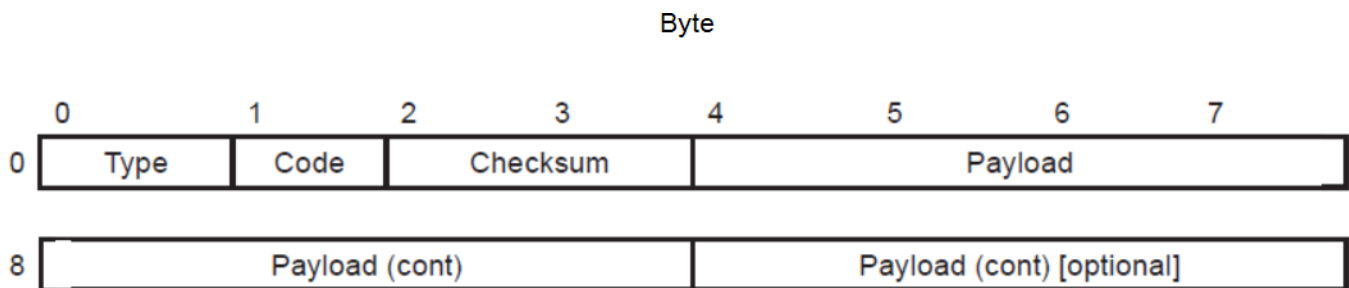
1. Perform further PDU capturing and analysis of network traffic using Wireshark.
2. Explore various expect of ICMP messages generated by Ping and Traceroute programs.
3. Understand the format and contents of an ICMP message.
4. Understand basic application protocols such as HTTP and FTP.

BACKGROUND

The Ping program in the source host sends a packet to the target IP address; if the target is live, the Ping program in the target host responds by sending a packet back to the source host. As you have observed in previous lab, both of these Ping packets are ICMP packets.

Traceroute program can be used to figure out the path a packet takes from source to destination. Traceroute is implemented in different ways in Unix/Linux/macOS and in Windows. In Windows, the source sends a series of ICMP packets to the target destination. For both operating systems, the program sends the first packet with TTL=1, the second packet with TTL=2, and so on. A router will decrement a packet's TTL value as the packet passes through the router. When a packet arrives at a router with TTL=1, the router sends an ICMP error packet back to the source.

The Internet Control Message Protocol, or ICMP, is used primarily for diagnostics. ICMP messages are carried in an IP payload with the IP datagram protocol field set to 1. The ICMP header and packet follows this format:



Type – The ICMP request type. Since the primary goal will be to respond to ping requests, the two codes are: 0x00-Echo Reply and 0x08-Echo Request. There are many more requests.

Code – If a destination is unreachable, this field denotes at which level (host, protocol, port, etc).

Checksum – A checksum of the ICMP header and data. The IP header checksum algorithm is used.

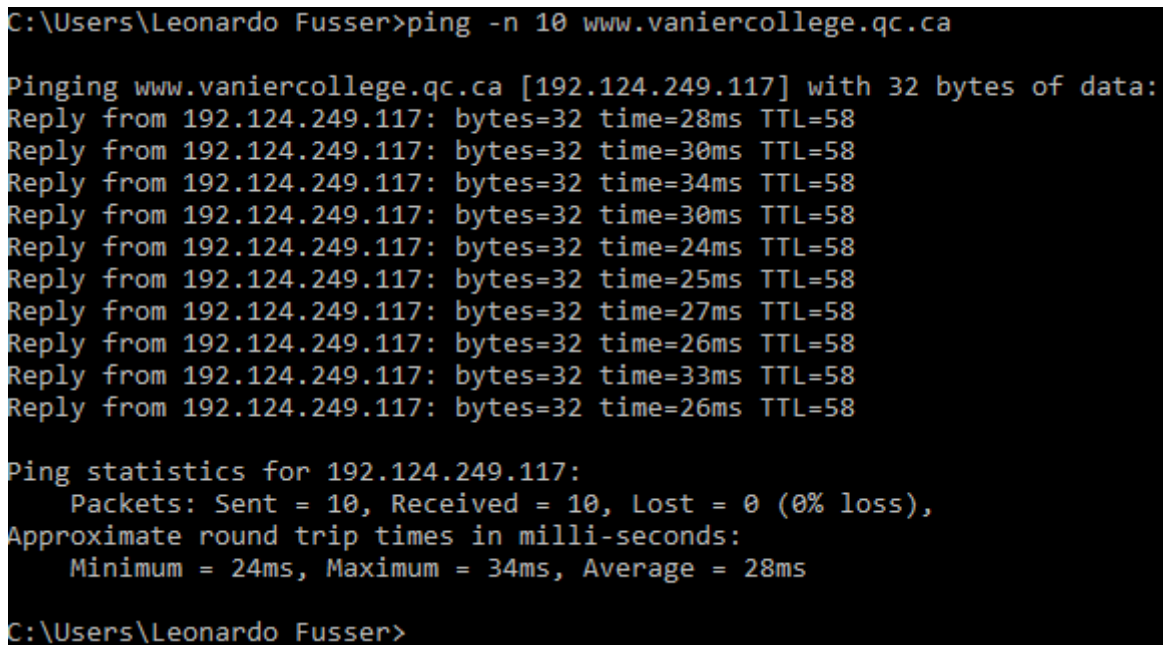
Payload – A minimum of eight bytes. When making an echo request/reply, the first two bytes are the identifier and the next two bytes are the sequence number.

PROCEDURE

**** For Part A & B, you will have to do it at Home.**

Part A: ICMP and Ping

1. Start up the Wireshark Packet Sniffer and begin Wireshark packet capture on the interface that provides you internet.
2. In your MS-DOS command line, run the command "ping -n 10 www.vaniercollege.qc.ca". Provide screenshot of your result.



```
C:\Users\Leonardo Fusser>ping -n 10 www.vaniercollege.qc.ca

Pinging www.vaniercollege.qc.ca [192.124.249.117] with 32 bytes of data:
Reply from 192.124.249.117: bytes=32 time=28ms TTL=58
Reply from 192.124.249.117: bytes=32 time=30ms TTL=58
Reply from 192.124.249.117: bytes=32 time=34ms TTL=58
Reply from 192.124.249.117: bytes=32 time=30ms TTL=58
Reply from 192.124.249.117: bytes=32 time=24ms TTL=58
Reply from 192.124.249.117: bytes=32 time=25ms TTL=58
Reply from 192.124.249.117: bytes=32 time=27ms TTL=58
Reply from 192.124.249.117: bytes=32 time=26ms TTL=58
Reply from 192.124.249.117: bytes=32 time=33ms TTL=58
Reply from 192.124.249.117: bytes=32 time=26ms TTL=58

Ping statistics for 192.124.249.117:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 24ms, Maximum = 34ms, Average = 28ms

C:\Users\Leonardo Fusser>
```

Result of ping command sent to www.vaniercollege.qc.ca shown above.

From this window you can observed that the source ping program sent 10 query packets and received 10 responses.

- a. What is the IP address of www.vaniercollege.qc.ca?
 - 192.124.249.117
- b. What is the meaning round trip times as shown in each ping?
 - It refers to the amount of time it takes for the ICMP packet to be sent to www.vaniercollege.qc.ca and the time it takes for www.vaniercollege.qc.ca to acknowledge that it received the ICMP packet to be sent back to my computer.
- c. What is your average RTT (round trip time) for the 10 packets?
 - My average RTT for the 10 ICMP packets sent to www.vaniercollege.qc.ca is 28mS.

3. When the Ping program terminates, stop the packet capture in Wireshark. Provides screenshot of your results, both from command prompt and Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
2567	35.020618	192.166.4.183	192.124.249.117	ICMP	74	Echo (ping) request id=0x0001, seq=71/18176, ttl=128 (reply in 2568)
2568	35.049052	192.124.249.117	192.166.4.183	ICMP	74	Echo (ping) reply id=0x0001, seq=71/18176, ttl=58 (request in 2567)
2574	36.025337	192.166.4.183	192.124.249.117	ICMP	74	Echo (ping) request id=0x0001, seq=72/18432, ttl=128 (reply in 2575)
2575	36.055292	192.124.249.117	192.166.4.183	ICMP	74	Echo (ping) reply id=0x0001, seq=72/18432, ttl=58 (request in 2574)
2581	37.032227	192.166.4.183	192.124.249.117	ICMP	74	Echo (ping) request id=0x0001, seq=73/18688, ttl=128 (reply in 2582)
2582	37.066329	192.124.249.117	192.166.4.183	ICMP	74	Echo (ping) reply id=0x0001, seq=73/18688, ttl=58 (request in 2581)
2594	38.043592	192.166.4.183	192.124.249.117	ICMP	74	Echo (ping) request id=0x0001, seq=74/18944, ttl=128 (reply in 2595)
2595	38.073619	192.124.249.117	192.166.4.183	ICMP	74	Echo (ping) reply id=0x0001, seq=74/18944, ttl=58 (request in 2594)
2609	39.059119	192.166.4.183	192.124.249.117	ICMP	74	Echo (ping) request id=0x0001, seq=75/19200, ttl=128 (reply in 2610)
2610	39.083626	192.124.249.117	192.166.4.183	ICMP	74	Echo (ping) reply id=0x0001, seq=75/19200, ttl=58 (request in 2609)
2614	40.068723	192.166.4.183	192.124.249.117	ICMP	74	Echo (ping) request id=0x0001, seq=76/19456, ttl=128 (reply in 2615)
2615	40.094470	192.124.249.117	192.166.4.183	ICMP	74	Echo (ping) reply id=0x0001, seq=76/19456, ttl=58 (request in 2614)
2619	41.081623	192.166.4.183	192.124.249.117	ICMP	74	Echo (ping) request id=0x0001, seq=77/19712, ttl=128 (reply in 2620)
2620	41.109262	192.124.249.117	192.166.4.183	ICMP	74	Echo (ping) reply id=0x0001, seq=77/19712, ttl=58 (request in 2619)
2672	42.101188	192.166.4.183	192.124.249.117	ICMP	74	Echo (ping) request id=0x0001, seq=78/19968, ttl=128 (reply in 2673)
2673	42.127542	192.124.249.117	192.166.4.183	ICMP	74	Echo (ping) reply id=0x0001, seq=78/19968, ttl=58 (request in 2672)
2679	43.115297	192.166.4.183	192.124.249.117	ICMP	74	Echo (ping) request id=0x0001, seq=79/20224, ttl=128 (reply in 2680)
2680	43.148521	192.124.249.117	192.166.4.183	ICMP	74	Echo (ping) reply id=0x0001, seq=79/20224, ttl=58 (request in 2679)
2683	44.126428	192.166.4.183	192.124.249.117	ICMP	74	Echo (ping) request id=0x0001, seq=80/20480, ttl=128 (reply in 2684)
2684	44.152829	192.124.249.117	192.166.4.183	ICMP	74	Echo (ping) reply id=0x0001, seq=80/20480, ttl=58 (request in 2683)

> Frame 2567: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{D733F949-C238-4AC5-AE94-C51AA932E8C9}, id 0
 > Ethernet II, Src: Dell_49:6b:1b (d0:67:e5:49:6b:1b), Dst: WatchGua_41:87:3c (00:90:7f:41:87:3c)
 > Internet Protocol Version 4, Src: 192.166.4.183, Dst: 192.124.249.117
 > Internet Control Message Protocol

0000	00 00 7f 41 87 3c d0 67 e5 49 6b 1b 08 00 45 00	...A-<g·Ik...E·
0010	00 3c c8 ed 00 00 80 01 00 00 c0 a6 04 b7 c0 7c	<.....
0020	f9 75 08 00 4d 14 00 01 00 47 61 62 63 64 65 66	·u·M····Gabcdef
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

Result of ping command sent to www.vaniercollege.qc.ca from my command prompt on my PC in Wireshark shown above. Command prompt result can be found on the previous page.

4. Analysis of your Wireshark capture. When answering the questions 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. The printout can be either screenshot, or to print a packet in text form, 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.

- a. What is the IP address of your host? Confirm this with a screen shot of your ipconfig /all
- My computer's IP address is 192.166.4.183 (assigned via DHCP). See screenshot below.

```
C:\Users\Leonardo Fusser>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : E5420-Leonardo
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : loffer.DATA

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . : loffer.DATA
    Description . . . . . : Broadcom NetXtreme 57xx Gigabit Controller
    Physical Address. . . . . : D0-67-E5-49-6B-1B
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IPv4 Address. . . . . : 192.166.4.183(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : April 14, 2021 7:23:39 PM
    Lease Expires . . . . . : April 14, 2021 10:23:37 PM
    Default Gateway . . . . . : 192.166.4.1
    DHCP Server . . . . . : 192.166.4.1
    DNS Servers . . . . . : 192.166.4.1
    NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Leonardo Fusser>
```

Result of ipconfig /all command done on my computer shown above. All details of my enabled network adapters are shown. There is only one network adapter enabled (named Ethernet).

- b. What is the IP address of the destination host?
- The IP address of www.vaniercollege.qc.ca is 192.124.249.117

c. Examine one of the ping request packets sent by your host.

i. What is the protocol number and name of your IP PDU?

- The protocol number is 4 and the name of my IP PDU is Internet Protocol Version 4 (for ping request). See screenshot below.

```

▼ Internet Protocol Version 4, Src: 192.166.4.183, Dst: 192.124.249.117
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xc8f6 (51446)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.166.4.183
    Destination Address: 192.124.249.117

```

Screenshot of IP PDU for ping request from Wireshark shown above.

ii. What is the type and code of your ICMP PDU?

- The type is 8 and the code is 0 for my ICMP PDU (for ping request). See screenshot below.

```

▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4d0b [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 80 (0x0050)
  Sequence Number (LE): 20480 (0x5000)
  [Response frame: 2684]
▼ Data (32 bytes)
  Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
  [Length: 32]

```

Screenshot of ICMP PDU for ping request from Wireshark shown above.

iii. How many bytes are the checksum, sequence number and identifier fields?

- The checksum, sequence number and identifier are 2 bytes long. See screenshot above.

- iv. Using a diagram, illustrate the format and information contain in the header ICMP PDU, based on your Wireshark capture. Compare and comment your results with the one shown in theory part.

8	0	0x4d14	abcd...
...			...

➤ See screenshot above under 4cii.

- d. Examine the corresponding ping reply packets.

- i. What is the type and code of your ICMP PDU?

➤ The type is 0 and the code is 0 for my ICMP PDU (for ping reply). See screenshot below.

```

v Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x550b [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 80 (0x0050)
  Sequence Number (LE): 20480 (0x5000)
  [Request frame: 2683]
  [Response time: 26.401 ms]
v Data (32 bytes)
  Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
  [Length: 32]

```

Screenshot of ICMP PDU for ping reply from Wireshark shown above.

- ii. What other fields does this ICMP packet have? **To check**

➤ In addition to what is already shown above, there is as well a "request frame" and "response time" in place of the "response frame" that is shown in the previous screenshot on the previous page (see 4Cii).

- iii. How many bytes are the checksum, sequence number and identifier fields?

➤ They are still 2 bytes long. Same as before.

Part B: ICMP and Traceroute

5. Repeat procedure #1, 2 & 3, on command "tracert www.vaniercollege.qc.ca". *Ignore the questions in previous steps that do not apply here.*

```
C:\Users\Leonardo Fusser>tracert www.vaniercollege.qc.ca

Tracing route to www.vaniercollege.qc.ca [192.124.249.117]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    192.166.4.1
  1  11 ms     13 ms     11 ms     modemcable001.239-157-24.mc.videotron.ca [24.157.239.1]
  2   9 ms     10 ms     10 ms     216.113.122.141
  3  13 ms      9 ms     11 ms     et-4-3-0.cr0-mtl1.ip4.gtt.net [69.174.17.221]
  4  21 ms     21 ms     23 ms     ae12.cr2-was1.ip4.gtt.net [89.149.130.157]
  5  22 ms     22 ms     25 ms     ip4.gtt.net [173.205.46.86]
  6  23 ms     24 ms     25 ms     cloudproxy10117.sucuri.net [192.124.249.117]

Trace complete.

C:\Users\Leonardo Fusser>
```

Result of tracert command sent to www.vaniercollege.qc.ca shown above. Seven hops were needed to reach www.vaniercollege.qc.ca.

- a. What is the IP address of www.vaniercollege.qc.ca?

➤ 192.124.249.117

b. Result from Wireshark:

No.	Time	Source	Destination	Protocol	Length	Info
156	22.984352	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=92/23552, ttl=1 (no response found!)
157	22.984723	192.166.4.1	192.166.4.183	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
158	22.985420	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=93/23808, ttl=1 (no response found!)
159	22.985551	192.166.4.1	192.166.4.183	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
160	22.986126	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=94/24064, ttl=1 (no response found!)
161	22.986255	192.166.4.1	192.166.4.183	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
244	30.076183	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=95/24320, ttl=2 (no response found!)
245	30.087265	24.157.239.1	192.166.4.183	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
246	30.088748	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=96/24576, ttl=2 (no response found!)
247	30.101679	24.157.239.1	192.166.4.183	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
248	30.103663	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=97/24832, ttl=2 (no response found!)
249	30.114967	24.157.239.1	192.166.4.183	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
291	31.663224	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=98/25088, ttl=3 (no response found!)
292	31.672822	216.113.122.141	192.166.4.183	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
293	31.673756	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=99/25344, ttl=3 (no response found!)
294	31.684477	216.113.122.141	192.166.4.183	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
295	31.686300	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=100/25600, ttl=3 (no response found!)
296	31.696621	216.113.122.141	192.166.4.183	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
311	33.027757	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=101/25856, ttl=4 (no response found!)
312	33.040621	69.174.17.221	192.166.4.183	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
313	33.042148	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=102/26112, ttl=4 (no response found!)
314	33.051607	69.174.17.221	192.166.4.183	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
315	33.052660	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=103/26368, ttl=4 (no response found!)
316	33.063525	69.174.17.221	192.166.4.183	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
332	34.473602	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=104/26624, ttl=5 (no response found!)
333	34.495808	89.149.130.157	192.166.4.183	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
334	34.497678	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=105/26880, ttl=5 (no response found!)
335	34.518735	89.149.130.157	192.166.4.183	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
336	34.520534	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=106/27136, ttl=5 (no response found!)
337	34.544147	89.149.130.157	192.166.4.183	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
346	36.237175	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=107/27392, ttl=6 (no response found!)
347	36.259496	173.205.46.86	192.166.4.183	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
348	36.261153	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=108/27648, ttl=6 (no response found!)
349	36.283315	173.205.46.86	192.166.4.183	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
350	36.285146	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=109/27904, ttl=6 (no response found!)
351	36.310282	173.205.46.86	192.166.4.183	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
364	37.757980	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=110/28160, ttl=7 (reply in 365)
365	37.781475	192.124.249.117	192.166.4.183	ICMP	106	Echo (ping) reply id=0x0001, seq=110/28160, ttl=58 (request in 364)
366	37.783386	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=111/28416, ttl=7 (reply in 367)
367	37.807482	192.124.249.117	192.166.4.183	ICMP	106	Echo (ping) reply id=0x0001, seq=111/28416, ttl=58 (request in 366)
368	37.809236	192.166.4.183	192.124.249.117	ICMP	106	Echo (ping) request id=0x0001, seq=112/28672, ttl=7 (reply in 369)
369	37.834026	192.124.249.117	192.166.4.183	ICMP	106	Echo (ping) reply id=0x0001, seq=112/28672, ttl=58 (request in 368)

> Frame 156: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{D733F949-C238-4AC5-AE94-C51AA932E8C9}, id 0

> Ethernet II, Src: Dell_49:6b:1b (d0:67:e5:49:6b:1b), Dst: WatchGua_41:87:3c (00:90:7f:41:87:3c)

> Internet Protocol Version 4, Src: 192.166.4.183, Dst: 192.124.249.117

> Internet Control Message Protocol


```

0000  00 90 7f 41 87 3c d0 67 e5 49 6b 1b 08 00 45 00  ...A<.g.Ik...E.
0010  00 5c c9 01 00 00 01 01 00 00 c0 a6 04 b7 c0 7c  ...\\.....|
0020  f9 75 08 00 f7 a2 00 01 00 5c 00 00 00 00 00 00  ...u.....\.....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
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  .....

```

Result of tracert (trace route) command sent to www.vaniercollege.qc.ca from my command prompt on my PC in Wireshark shown above. Command prompt result can be found on the previous page.

6. Analysis of your Wireshark capture. Attach and annotate any necessary screenshot/text of your results to support your answers below.

- a. For each TTL value, how many probe packets that the source program sends?
 - For each TTL value, there are 3 probe packets sent.
- b. Examine one of the ICMP echo packet (request) sent by the host. Is this different from the ICMP ping query packets in the part A of this lab? If yes, how?
 - Yes, it is different. See screenshots below.

```
> Frame 156: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{D733F949-C238-4AC5-AE94-C51AA932E8C9}, id 0
> Ethernet II, Src: Dell_49:6b:1b (d0:67:e5:49:6b:1b), Dst: WatchGua_41:87:3c (00:90:7f:41:87:3c)
v Internet Protocol Version 4, Src: 192.166.4.183, Dst: 192.124.249.117
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 92
  Identification: 0xc901 (51457)
  > Flags: 0x00
  Fragment Offset: 0
  > Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.166.4.183
  Destination Address: 192.124.249.117
v Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xf7a2 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 92 (0x005c)
  Sequence Number (LE): 23552 (0x5c00)
  > [No response seen]
  > Data (64 bytes)
```

Echo (ping) request packet breakdown for Part B shown above.

```
> Frame 2567: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{D733F949-C238-4AC5-AE94-C51AA932E8C9}, id 0
> Ethernet II, Src: Dell_49:6b:1b (d0:67:e5:49:6b:1b), Dst: WatchGua_41:87:3c (00:90:7f:41:87:3c)
v Internet Protocol Version 4, Src: 192.166.4.183, Dst: 192.124.249.117
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 60
  Identification: 0xc8ed (51437)
  > Flags: 0x00
  Fragment Offset: 0
  Time to Live: 128
  Protocol: ICMP (1)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.166.4.183
  Destination Address: 192.124.249.117
v Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4d14 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 71 (0x0047)
  Sequence Number (LE): 18176 (0x4700)
  [Response frame: 2568]
  > Data (32 bytes)
```

Echo (ping) request packet breakdown for Part A shown above.

- Aside from some minor details, the major difference between the two screenshots above is that the TTL for Part B is 1 while the TTL for Part A is 128. Other small details can be seen above in the two screenshots (such as the data size).

- c. Examine the ICMP error packet. It has more fields than the ICMP echo packet (reply). What is included in those fields?

➤ See screenshot below.

```
> Frame 157: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{D733F949-C238-4AC5-AE94-C51AA932E8C9}, id 0
> Ethernet II, Src: WatchGua_41:87:3c (00:90:7f:41:87:3c), Dst: Dell_49:6b:1b (d0:67:e5:49:6b:1b)
v Internet Protocol Version 4, Src: 192.166.4.1, Dst: 192.166.4.183
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 56
  Identification: 0x5f7d (24445)
  > Flags: 0x00
  Fragment Offset: 0
  Time to Live: 64
  Protocol: ICMP (1)
  Header Checksum: 0x9143 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.166.4.1
  Destination Address: 192.166.4.183
v Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0xf4ff [correct]
  [Checksum Status: Good]
  Unused: 00000000
v Internet Protocol Version 4, Src: 192.166.4.183, Dst: 192.124.249.117
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 92
  Identification: 0xc901 (51457)
  > Flags: 0x00
  Fragment Offset: 0
  > Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x7150 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.166.4.183
  Destination Address: 192.124.249.117
v Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xf7a2 [unverified] [in ICMP error packet]
  [Checksum Status: Unverified]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 92 (0x005c)
  Sequence Number (LE): 23552 (0x5c00)
```

Typical ICMP error packet breakdown shown above. (Error packets can be seen in screenshot under Q5b – the dark and green packets).

- The difference that can be observed is under the “Internet Control Message Protocol” submenu. In an ICMP error packet, additional headers such as TTL is present and more submenus details about the ICMP packet are present.
- d. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?
- These packets are different than the ICMP error packets because these packets represent that they reached the destination host, so there are no error packets associated with it (like what was seen in packets prior).

**** For Part C & D, you are required to connect to Eagle Server using the same set up as previous lab, as shown in Figure 1 below.**

***** Enable ONLY your network port to D-265!!**

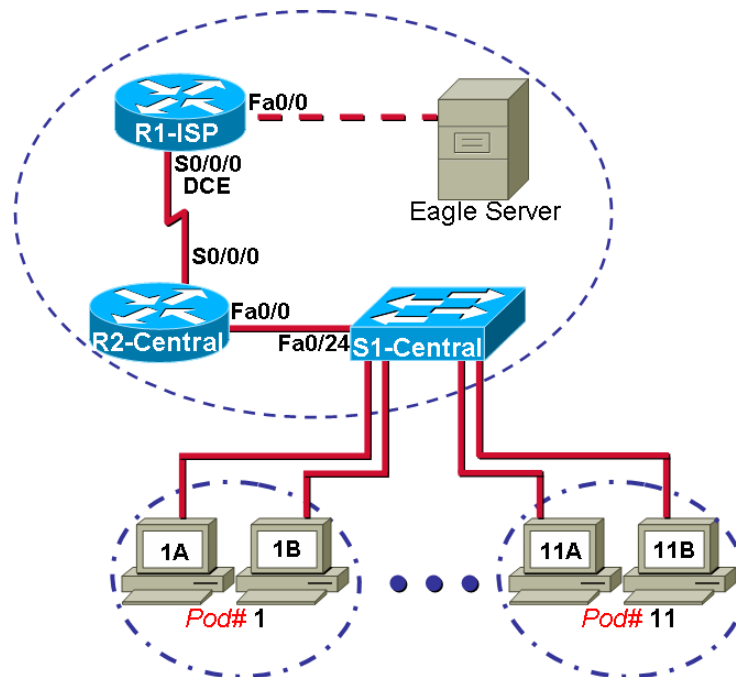


Figure 1: Eagle Server Topology

Addressing table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/A
	Fa0/0	192.168.254.253	255.255.255.0	N/A
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	10.10.10.6
	Fa0/0	172.16.255.254	255.255.0.0	N/A
Eagle Server	N/A	192.168.254.254	255.255.255.0	192.168.254.253
	N/A	172.31.24.254	255.255.255.0	N/A
hostPod	N/A	172.16.Pod#.1	255.255.0.0	172.16.255.254
S1-Central	N/A	172.16.254.1	255.255.0.0	172.16.255.254

Part C: FTP PDU Capture

7. Start Wireshark packet capture. At command line of your computer, enter **ftp 192.168.254.254**. When connection is established, enter **anonymous** as the user without a password.
8. When successfully logged in, type **get /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe** **<enter>**. This will start downloading the file from the ftp server.
9. When the file download is complete, enter *quit* to end the ftp session.
10. Stop the Wireshark capture, and **SAVE IT**. Examine the PDUs associated with file download. These will be the PDUs from the *Layer 4 protocol TCP* and the *Layer 7 protocol FTP*.
 - a. Identify the three groups of PDUs associated with the file transfer. If you performed the step above (step 7, 8 and 9), match the packets with the messages and prompts in the FTP command.

No.	Time	Source	Destination	Protocol	Length	Info
40	25.968950	192.168.254.254	172.16.22.1	FTP	100	Response: 220 Welcome to the eagle-server FTP service.
41	25.972098	172.16.22.1	192.168.254.254	FTP	68	Request: OPTS UTF8 ON
43	25.972904	192.168.254.254	172.16.22.1	FTP	92	Response: 530 Please login with USER and PASS.
75	48.284982	172.16.22.1	192.168.254.254	FTP	70	Request: USER anonymous
76	48.286067	192.168.254.254	172.16.22.1	FTP	88	Response: 331 Please specify the password.
78	50.109065	172.16.22.1	192.168.254.254	FTP	61	Request: PASS
79	50.111572	192.168.254.254	172.16.22.1	FTP	77	Response: 230 Login successful.
1143	133.764144	172.16.22.1	192.168.254.254	FTP	80	Request: PORT 172,16,22,1,225,149
1146	133.932479	192.168.254.254	172.16.22.1	FTP	105	Response: 200 PORT command successful. Consider using PASV.
1148	133.936963	172.16.22.1	192.168.254.254	FTP	107	Request: RETR /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe
1154	134.227287	192.168.254.254	172.16.22.1	FTP	163	Response: 150 Opening BINARY mode data connection for /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe (6967072 bytes).
8339	149.766623	192.168.254.254	172.16.22.1	FTP	73	Response: 226 File send OK.
8399	182.003441	172.16.22.1	192.168.254.254	FTP	60	Request: QUIT
8401	182.004373	192.168.254.254	172.16.22.1	FTP	68	Response: 221 Goodbye.

Three groups of PDUs associated with the FTP process done from the command prompt on my computer shown in Wireshark above. Red box shows the connection phase to the FTP server. Yellow box shows the file being retrieved from the FTP server. Green box shows myself disconnecting from the FTP server.

- b. The first group is associated with the "connection" phase and logging into the server. List examples of messages exchanged in this phase.
 - Some messages that have been exchanged in this phase are "Welcome to the eagle-server FTP service.", "Please login with USER and PASS.", "Please specify the password." and "Login successful."
- c. Locate and list examples of messages exchanged in the second phase that is the actual download request and the data transfer.
 - Some messages that have been exchanged in this phase are "200 PORT command successful. Consider using PASV.", "150 Opening BINARY mode data connection for /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe (6967072 bytes)." and "226 File send ok."
- d. The third group of PDUs relate to logging out and "breaking the connection". List examples of messages exchanged during this process.
 - One message that has been exchanged in this phase is "221 Goodbye."

11. Examine packet details:

- a. Select (highlight) a packet on the list associated with the first phase of the FTP process. View the packet details in the Details pane.
 - i. What are the protocols encapsulated in the frame?
 - Some protocols that are encapsulated in this frame are IPv4 (Internet Protocol version 4), TCP (Transmission Control Protocol) and FTP (File Transfer Protocol).
 - ii. Highlight the packets containing the username and password. Examine the highlighted portion in the Packet Byte pane. What does this say about the security of this FTP login process?
 - Basically, what there is to be said about the security of the FTP login process is not much. The only thing that can be said is that it is very weak because it exposes all the login information! This shows that anyone who has a network analyzer/packet analyzer (like Wireshark) can easily obtain this information and potentially do some harm. See screenshot below.

75	48.284982	172.16.22.1	192.168.254.254	FTP	70 Request: USER anonymous
76	48.286067	192.168.254.254	172.16.22.1	FTP	88 Response: 331 Please specify the password.
78	50.109065	172.16.22.1	192.168.254.254	FTP	61 Request: PASS

FTP's level of security shown above. As mentioned before, FTP is not secure at all because it shows all the login information including username and password.

- b. Highlight a packet associated with the second phase.
 - i. From any pane, locate the packet containing the file name. What is the filename?
 - The filename is "gaim-1.5.0.exe".
 - ii. Highlight a packet containing the actual file content - note the plain text in Byte pane.
 - See screenshot below.

1155	134.230569	192.168.254.254	172.16.22.1	FTP-DATA	1514 FTP Data: 1460 bytes (PORT) (RETR /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe)
1156	134.233628	192.168.254.254	172.16.22.1	FTP-DATA	1514 FTP Data: 1460 bytes (PORT) (RETR /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe)
1161	134.383644	192.168.254.254	172.16.22.1	FTP-DATA	1514 FTP Data: 1460 bytes (PORT) (RETR /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe)
1162	134.386750	192.168.254.254	172.16.22.1	FTP-DATA	1514 FTP Data: 1460 bytes (PORT) (RETR /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe)
1164	134.389832	192.168.254.254	172.16.22.1	FTP-DATA	1514 FTP Data: 1460 bytes (PORT) (RETR /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe)
1166	134.539843	192.168.254.254	172.16.22.1	FTP-DATA	1514 FTP Data: 1460 bytes (PORT) (RETR /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe)
1167	134.542954	192.168.254.254	172.16.22.1	FTP-DATA	1514 FTP Data: 1460 bytes (PORT) (RETR /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe)
1169	134.546021	192.168.254.254	172.16.22.1	FTP-DATA	1514 FTP Data: 1460 bytes (PORT) (RETR /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe)
1171	134.622589	192.168.254.254	172.16.22.1	FTP-DATA	1514 FTP Data: 1460 bytes (PORT) (RETR /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe)
1172	134.625658	192.168.254.254	172.16.22.1	FTP-DATA	1514 FTP Data: 1460 bytes (PORT) (RETR /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe)
1174	134.702210	192.168.254.254	172.16.22.1	FTP-DATA	1514 FTP Data: 1460 bytes (PORT) (RETR /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe)
1175	134.705332	192.168.254.254	172.16.22.1	FTP-DATA	1514 FTP Data: 1460 bytes (PORT) (RETR /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe)
1177	134.708423	192.168.254.254	172.16.22.1	FTP-DATA	1514 FTP Data: 1460 bytes (PORT) (RETR /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe)
1179	134.784957	192.168.254.254	172.16.22.1	FTP-DATA	1514 FTP Data: 1460 bytes (PORT) (RETR /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe)
1180	134.788082	192.168.254.254	172.16.22.1	FTP-DATA	1514 FTP Data: 1460 bytes (PORT) (RETR /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe)
1182	134.791162	192.168.254.254	172.16.22.1	FTP-DATA	1514 FTP Data: 1460 bytes (PORT) (RETR /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe)
1183	134.794233	192.168.254.254	172.16.22.1	FTP-DATA	1514 FTP Data: 1460 bytes (PORT) (RETR /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe)

Multiple packets in relation to the file content of the file "gaim-1.5.0.exe". If someone were to recuperate these packets all together, they can possibly reconstruct the original file and use it. This also further shows that FTP is not the most secure protocol.

Part D: HTTP PDU Capture

12. Start a new Wireshark capture. Launch a web browser on the computer. Enter the IP address of the Eagle Server, 192.168.254.254. After the web page has fully downloaded, stop the Wireshark packet capture, and **SAVE IT**.
13. Locate and identify the TCP and HTTP packets associated with the downloaded web page. Note the similarity between this message exchange and the FTP exchange.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.662783	172.16.22.1	52.170.57.27	TCP	66	57778 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5	0.663934	10.10.10.6	172.16.22.1	ICMP	70	Destination unreachable (Host unreachable)
25	2.676531	172.16.22.1	52.170.57.27	TCP	66	[TCP Retransmission] 57778 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
26	2.677682	10.10.10.6	172.16.22.1	ICMP	70	Destination unreachable (Host unreachable)
75	6.681059	172.16.22.1	52.170.57.27	TCP	66	[TCP Retransmission] 57778 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
76	6.682158	10.10.10.6	172.16.22.1	ICMP	70	Destination unreachable (Host unreachable)
82	9.495533	172.16.22.1	192.168.254.254	TCP	66	57779 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
83	9.496377	192.168.254.254	172.16.22.1	TCP	66	80 → 57779 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=4
84	9.496427	172.16.22.1	192.168.254.254	TCP	54	57779 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
85	9.496487	172.16.22.1	192.168.254.254	HTTP	424	GET / HTTP/1.1
86	9.498101	192.168.254.254	172.16.22.1	TCP	60	80 → 57779 [ACK] Seq=1 Ack=371 Win=6912 Len=0
87	9.499299	192.168.254.254	172.16.22.1	HTTP	199	HTTP/1.1 304 Not Modified
88	9.499299	192.168.254.254	172.16.22.1	TCP	60	80 → 57779 [FIN, ACK] Seq=146 Ack=371 Win=6912 Len=0
89	9.499325	172.16.22.1	192.168.254.254	TCP	54	57779 → 80 [ACK] Seq=371 Ack=147 Win=261888 Len=0
90	9.499342	172.16.22.1	192.168.254.254	TCP	54	57779 → 80 [FIN, ACK] Seq=371 Ack=147 Win=261888 Len=0
91	9.500126	192.168.254.254	172.16.22.1	TCP	60	80 → 57779 [ACK] Seq=147 Ack=372 Win=6912 Len=0
92	9.510493	172.16.22.1	192.168.254.254	TCP	66	57780 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
93	9.511332	192.168.254.254	172.16.22.1	TCP	66	80 → 57780 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=4
94	9.511388	172.16.22.1	192.168.254.254	TCP	54	57780 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
95	9.511537	172.16.22.1	192.168.254.254	HTTP	278	GET /favicon.ico HTTP/1.1
96	9.512822	192.168.254.254	172.16.22.1	TCP	60	80 → 57780 [ACK] Seq=1 Ack=225 Win=6912 Len=0
97	9.514466	192.168.254.254	172.16.22.1	HTTP	524	HTTP/1.1 404 Not Found (text/html)
98	9.514466	192.168.254.254	172.16.22.1	TCP	60	80 → 57780 [FIN, ACK] Seq=471 Ack=225 Win=6912 Len=0
99	9.514491	172.16.22.1	192.168.254.254	TCP	54	57780 → 80 [ACK] Seq=225 Ack=472 Win=261632 Len=0
100	9.514508	172.16.22.1	192.168.254.254	TCP	54	57780 → 80 [FIN, ACK] Seq=225 Ack=472 Win=261632 Len=0
101	9.515296	192.168.254.254	172.16.22.1	TCP	60	80 → 57780 [ACK] Seq=472 Ack=226 Win=6912 Len=0
116	14.692095	172.16.22.1	52.170.57.27	TCP	66	[TCP Retransmission] 57778 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
117	14.693285	10.10.10.6	172.16.22.1	ICMP	70	Destination unreachable (Host unreachable)

Shown in the shaded green area above, the TCP and HTTP packets associated with the downloaded web page.

14. In the packet list pane, highlight an HTTP packet that has the notation "(text/html)" in the Info column. In the packet details pane, click the + box next to Line-based text data: html.

a. When this information expands, what is displayed?

➤ What is displayed is the HTML code for the web page.

15. Quit Wireshark. Make sure you save your Wireshark captured for Part B & C. This information will be required to complete upcoming assignment.