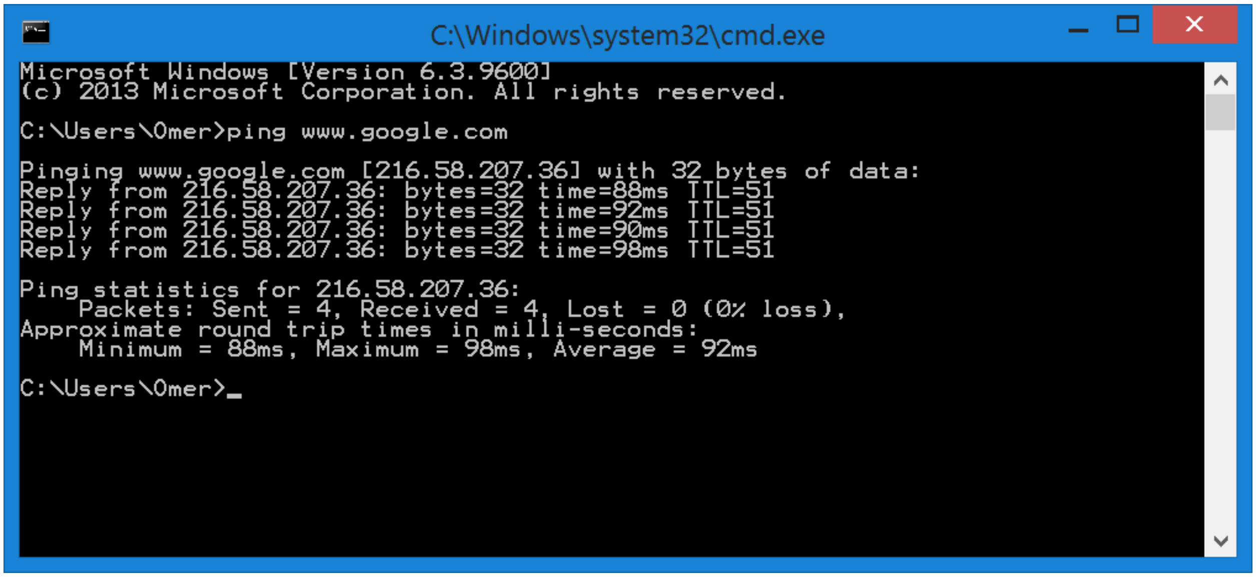
Wireshark Lab – Graded Exercise
Ping & PCAP

Ping is a useful utility to check for remote servers' connectivity.
To use it, run the command line. This page explains how to do that in Windows

Now, we can try to ping <address> using the command line. By default in windows, ping sends 4 requests and waits for a **pong** answer.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Omer>ping www.google.com

Pinging www.google.com [216.58.207.36] with 32 bytes of data:
Reply from 216.58.207.36: bytes=32 time=88ms TTL=51
Reply from 216.58.207.36: bytes=32 time=92ms TTL=51
Reply from 216.58.207.36: bytes=32 time=90ms TTL=51
Reply from 216.58.207.36: bytes=32 time=98ms TTL=51

Ping statistics for 216.58.207.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 88ms, Maximum = 98ms, Average = 92ms

C:\Users\Omer>_
```

In the command line above, I've written the command **ping www.google.com.**
We can see that Google has responded with four replies. The time it took for the message to return varied between 88 and 98 milliseconds.

Ping is useful to determine whether a remote service is available, and how fast it is to reach that service. If it takes a very long time to reach a reliable server such as google.com, we might have a connectivity problem.

Run the following command from your ubuntu command line (or terminal):
ping -c 1 www.google.com

Use wireshark to answer the following questions:

1) What protocol does the ping utility use?
Internet control message protocol ICMP

2) Using only wireshark, compute the RTT (Round Trip Time) – how long it took since your ping request was sent and until the ping reply was received?

43.573 ms
43.578/43.578/43.578/0.000 ms
Next, run the following command:

```
ping -c 1 -s 342 www.google.com
```

3) What is the main difference between the packet sent by this command, and the packet sent by the previous command? Where in wireshark can you see this difference, inspecting the packets?
48 byes in previous command
334 bytes in this command

4) What is the content (data) provided in the ping request packet? What is the content provided in the ping response packet?

Data:
52cc030000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b…

Data:
52cc030000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b…

Download the PCAP file from LMS.

Answer the following questions:

5) How many packets were sent to 192.168.1.3?
276

6) What frames are ARP frames? Provide the frame numbers.
87
134
135
3 Packets found.

7) How many packets have we captured overall?
292 packets

8) How many of these packets are TCP (Transmission Control Protocol) packets?
234 packets from tcp and tlsv1.2