Wireshark Lab 2
ICMP and DNS

In this lab we will explore several aspects of the ICMP protocol:

1. ICMP messages generated by the `ping` program
2. ICMP messages generated by the `traceroute` program
3. the format and contents of an ICMP message

as well as DNS.

1 ICMP and `ping`

The program `ping` allows anyone 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 live, `ping` in the target host responds by sending a packet back to the source host. Both of these `ping` packets are ICMP packets.

Start Wireshark, give the command

```
ping -n 10 hostname
```

where you can use any hostname that works for you, and once `ping` has stopped executing, stop the packet capture in Wireshark.

1. Why did Wireshark capture 20 packets, even thought "10 were sent"?
2. Why do the IP datagrams within the packets have protocol number 01?
3. Why is it that the ICMP packets do not have source and destination port numbers?
4. 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?
5. 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?

2 ICMP and `traceroute`

The `traceroute` program can be used to figure out the path a packet takes from source to destination. Like before, turn Wireshark on to capture the following command:

```
traceroute math.ucsd.edu
```

1. What is the IP of the host and of the destination?
2. Is the source sending ICMP or UDP packets? (Note that the answer to this is OS dependent.)
3. Are there links whose delay is significantly longer than others?
4. Can you guess the geographic locations of the links?

3 DNS and `ipconfig` and `nslookup`

1. Run `nslookup` to obtain the IP address of a Web server in Asia. What is the IP address of that server?
2. Run `nslookup` to determine the authoritative DNS servers for a university in Europe.
3. Run `nslookup` so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

Now do the following:

- Use `ipconfig` to empty the DNS cache in your host.
- Open your browser and empty your browser cache.
- Open Wireshark and enter `ip.addr == your_IP_address` into the filter, where you obtain `your_IP_address` with `ipconfig`. This filter removes all packets that neither originate nor are destined to your host.
- Start packet capture in Wireshark.
- With your browser, visit the Web page: `http://www.ietf.org`
- Stop packet capture.

and answer the following questions:

1. Locate the DNS query and response messages. Are then sent over UDP or TCP?

2. What is the destination port for the DNS query message? What is the source port of DNS response message?

3. To what IP address is the DNS query message sent? Use `ipconfig` to determine the IP address of your local DNS server. Are these two IP addresses the same?

4. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

5. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?