DNS Exercise 1

1. Configure the resolver on your workstation

Create `/etc/resolv.conf` containing:

```
search e1.ws.afnog.org
nameserver 196.200.219.200
nameserver 196.200.222.1
```

2. Issue DNS queries using 'dig'

2a. For each command find the /answer/ section and write down the result. Note the TTL as well. Repeat the command. Is the TTL the same?

Are the responses Authoritative?

RESULT

```
# dig www.tiscali.co.uk. a

# dig afnog.org. mx

# dig news.bbc.co.uk. a

# dig <domain of your choice> a

# dig <domain of your choice> mx

# dig tiscali.co.uk. txt

# dig ripe.net. txt

# dig geek.tiscali.co.uk. a
```

2b. Now send some queries to another caching server. How long did it take each answer to be received?

```
# dig @158.152.1.58 news.bbc.co.uk. a

# dig @isp1.4u.com.gh. yahoo.com. a

# dig @<a server of your choice> <domain of your choice> a
```

3. Reverse DNS lookups

Now try some reverse DNS lookups. Remember to reverse the four parts of the IP address, add '*.in-addr.arpa.*', and ask for a *PTR* resource record.

(For 212.74.112.66)
```
# dig 66.112.74.212.in-addr.arpa. ptr
```

Repeat for an IP address of your choice.

Now try the short form of dig using the '-x' flag for reverse lookups:

```
# dig -x 212.74.112.66

# dig @<server of your choice> -x <IP address of your choice>
```

4. Use tcpdump to show DNS traffic

In a separate window, run the following command (you must be 'root')

```
# tcpdump -n -s 1500 -i sis0 udp port 53
```

This shows all packets going in and out of your machine for UDP port 53 (DNS). Now go to another window and repeat some of the 'dig' queries from earlier. Look at the output of tcpdump, check the source and destination IP address of each packet

-n
    Prevents tcpdump doing reverse DNS lookups on the packets it receives, which would generate additional (confusing) DNS traffic
-s 1500
    Read the entire packet (otherwise tcpdump only reads the headers)
-i sis0
    Which interface to listen on (use ifconfig to determine the name of your ethernet interface)
udp port 53
    A filter which matches only packets to/from UDP port 53