Use tcpdump & wireshark to show DNS traffic

1. Tcpdump

    Open a NEW connection to your resolv.grpX machine (log in a second time), so that you can have both windows side-by-side.

    In the first window, you will be logged in to "auth1"

    In the second window, you will be logged in to "resolv"

    In the second window, run the following command (you must be 'root', that's why we use sudo):

```
$ sudo tcpdump -n -s 1500 udp and port 53
```

    This shows all packets going in and out of your machine for UDP port 53 (DNS).

    Now in the first window (auth1), repeat some of the 'dig' queries from earlier:

```
    $ dig @resolv.grpXX.dns.nsrc.org www.MYTLD.
    $ dig @resolv.grpXX.dns.nsrc.org www.OTHER_DOMAIN_IN_THE_CLASS.
```

    (for example)

    Look at the output of tcpdump, check the source and destination IP address of each packet:

Explanation:

    -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 96 bytes)

    udp and port 53
        A filter which matches only packets to/from UDP port 53

2. Tshark

    Let's try the same thing, but using tshark

    If required, stop the above tcpdump (CTRL+C), then run:

```
$ sudo tshark -n -s 1500 udp and port 53
```

    Try to run a few queries using dig from another window:

```
    $ dig @resolv.grpXX.dns.nsrc.org www.MYTLD.
    $ dig @resolv.grpXX.dns.nsrc.org www.OTHER_DOMAIN_IN_THE_CLASS.
```

    etc...

    stop tshark (CTRL+C), and run it with different options:

```
$ sudo tshark -V -n -s 1500 udp and port 53
```

Run some queries again, as above.
Do you see how much data is now being printed ?

## 3. Wireshark

Let's try this with the graphical interface, wireshark.

First, let's create a remote desktop instance:

```
$ vncserver
```

You will be asked to create a password - use the same as in class!

At this point, you will need to get a VNC client to connect
to your remote desktop. For example:

Windows: http://www.realvnc.com/cgi-bin/download.cgi
(Choose Installer or ZIP for the Standalone viewer)

Linux: Ubuntu / Debian: apt-get install xvnc4viewer

MacOS X: http://sourceforge.net/projects/cotvnc/files/latest/download

Follow the instructions to install your client, then connect to:

resolv.grpX.dns.nsrc.org:1

... where X is the number of your group.

When asked for a password, type in the password you provided earlier

Normally, a desktop with a terminal (xterm) window should appear.

If not, ask the instructor for assistance

Now, run wireshark:

```
$ sudo wireshark
```

A warning will pop up about running as root - just click ok!

Now, start a capture - press CTRL+K

At the top, choose `eth0` as your interface.

In the Capture Filter field below, type:

```
port 53
```

(we only want to see DNS traffic)

Start the capture by pressing Start at the bottom.

From your auth1 server run some `dig` commands like you did earlier:

```
$ dig @resolv.grpXX.dns.nsrc.org www.MYTLD.
$ dig @resolv.grpXX.dns.nsrc.org www.OTHER_DOMAIN_IN_THE_CLASS.
```

You should start to see packets appear in the wireshark window.

To stop the capture, press the red "Stop" button (4th from the left on the list of buttons at the top).

Now, you can explore the packet capture, save it, decode it, etc...