The idea for this homework is to collect a pcap file and analyse it and practice using the tiny core environment. Tinycore is a virtual machine that can connect to the Internet through the host machine, and it is configured to automatically monitor the network traffic and store it in a pcap file.

You can download the files you need here:
`https://cspages.ucalgary.ca/~joel.reardon/526/tinycore.tar.gz`
It is a gzipped tarball containing two files:

- `tinycore`: the script to launch VM
- `tc.qcow2`: the VM image itself.

On a linuxlab machine download the tarball:

```
wget https://cspages.ucalgary.ca/~joel.reardon/526/tinycore.tar.gz
```

Then extract the data:

```
tar zxvf tinycore.tar.gz
```

This provides you the tinycore and image file. To launch the VM, run the following command: `./tinycore -f tc.qcow2 -c [output.pcap] &`

The trailing ampersand is optional and if used launches the program in the background and gives you back the prompt; otherwise, as long as the VM is running you won't have the prompt. You can ssh into the VM as long as you are doing it from the same machine that is running it. The port and information to ssh into the VM are outputed at the command line when it starts. The file `output.pcap` will store the network traffic and will be overwritten when you launch the VM. You are free to change the filename as you see fit, e.g., based on assignment or exercise name.

A note for doing this work over ssh. Remember that `linuxlab.cs.ucalgary.ca` is a pseudo host that uses load balancing to put you to a particular machine in the group. For instance, if you log in you might see a prompt like this: `username@linux02-eb:~$` . In this case, `linux02-eb` is the actual machine you are connected to. If you launch the VM on that machine, you'll need to connect to it again in order to see the VM. So to connect to it again, first ssh into `linuxlab.cs.ucalgary.ca`, where you might end up on `linux11-wc`, then ssh into your first machine again. Also for running the VM remotely, you must enable X-forwarding. On linux system, the `-X` command for ssh should do it. It is different on other machines and your TA can help you get it working during tutorial.

Question 1: Why Tinycore?

For security reasons you cannot monitor the network traffic coming from the undergraduate machines. Why would that be?

Question 2: Get a pcap

In tinycore, open firefox and go to a website of your choice. After you load the website, shut down the tinycore and look at the pcap file. If the file is not empty, there is some data that has been captured. Open it with the tool `wireshark` and find the DNS query associated with looking up your website as well as the TCP SYN to the IP that was retrieved.

Wireshark allows packet to be filtered by the fields. Once you find the IP for the server, you can enter `ip.src == W.X.Y.Z || ip.dst = W.X.Y.Z` as the filter to only look at packets of that form. You can filter for `http` with `tcp.port == 80` and for `dns` with `udp.port == 53`. Note that if you use `HTTPS` in lieu of `HTTP` you won't see traffic on port 80.