For this assignment we will monitor traffic on a network interface between the tinycore VM and the host machine in the cslinux environment as we have with assignment 1. The premise is to capture and analyse a pcap file using *wireshark*. You will submit your pcap file and answers to specific questions about the pcap file for both questions 1 and 2

Question 1: TCP Eavesdropping (18 marks)

Recall the client / server code from the first tutorial. Take the code and make the following changes:

- have the server listen on port 3XXXX where XXXX is the last four digits of your UCID
- have the client send data to the server; have the server prints out the received data

Note: It is important that you make both of these changes for the next assignment!

Start tinycore and compile the client on tinycore and the server on the host. Run the server program on the host and have the client run on the tinycore VM and connect to the host. Using the pcap capture for tinycore, obtain the pcap file. Using wireshark answer the following questions *about the communication between your client and the server programs*:

1. What is the packet number for the initial SYN for your client connection?
2. What is the packet number for the response SYN-ACK?
3. What is the ISN used by the client?
4. What is the ISN used by the server?
5. What is the client's port number used to connect to the server?
6. What is the packet number that is the first to include actual data that is sent or received by the programs themselves?
7. Does the connection close with a FIN or a RST? What are the relevant packet numbers for the closing of the connection?
8. Who initiates the FIN, the client or the server? What is the relevant packet number?
9. What is the client's relative sequence number for its FIN?

Question 2: Low-Level Protocol Analysis (30 marks)

This question involves looking at the traffic involved in a single web request.

Important: a single web request involves many actual connections to get images, download advertisements, contact web trackers, etc. There are also connections that occur just starting the browser, e.g., looking for updates. It can be useful to wait a conspicuous amount of time before starting and matching that delay in the pcap file. Make sure to use the DNS

request so you know the correct IP address about which to answer these questions. Moreover, you cannot rely on looking up the IP at one point in point or at a different compute, as they may change, due to load balancing, etc., so be sure to match the IP from the relevant DNS request in your pcap.

Start tinycore and using the GUI launch *firefox*. Wait for it to start and visit `www.bbc.com/news` while collecting the `pcap`. Close firefox and tinycore. Avoid running firefox longer or doing more browsing or you will unnecessarily create a large pcap file. Answer the following questions based on your collected pcap. *Answer this in written answers; do not simply take screenshots of wireshark.*

1. Are there *any* OCSP requests in the pcap? If so, choose one and provide the *hostname* and IP being contacted (i.e., IP and hostname of the OCSP service). Indicate the packet number of the OCSP request (No. column in wireshark).
2. What is the serial number for the cert that is being checked?
3. What is the certStatus in the corresponding response?
4. What is the *hostname* for the the certificate that is being checked (i.e., the "Bob" that is being contacted, not the "Trent" that is checking the validity)?
5. You connected to `www.bbc.com`. Was there a DNS resolution prior to a TCP connection for its IP? If so give the packet numbers for the latest DNS resolution for `www.bbc.com` that occurs prior to the first TCP connection to the resolved IP.
6. Does the tinycore machine appear to use randomize DNS query IDs and randomize DNS client ports? Justify your answer with an explanation or evidence.
7. Did Firefox automatically use HTTPS or was there an initial request done over HTTP with a 302 redirect to HTTPS? What are the packet numbers of the 302 if that is the case?
8. What is the serial number for the certificate for `www.bbc.com`?
9. Did the certificate for `www.bbc.com` get checked with a separate OCSP server, did the certificate arrive with an OCSP stapling, or did neither happen? What is the relevant packet number for the OCSP reply or OCSP stapling if one of these checks occurred.
10. If available, what is the organization name corresponding to `www.bbc.com`?
11. If there was an organization name, find another certificate that does not provide an organization name for its subject and give its packet number and common name. If there was not an organization name, find another certificate that does provide an organization name for its subject and give its packet number and common name.
12. What is the common name of the root certificate authority that signed the certificate for the `www.bbc.com`?
13. What is the home country for the root certificate authority?

Submit both your pcap file and written answers to this question.

Virtual Machine The virtual machine is accessible from the undergrad computing environment available on the `linuxlab.cpsc.ucalgary.ca` server. Make sure you use X forwarding when you connect via ssh.

`/usr/local/tinycore/tinycore -f <snapshot file> -c <capture file>`

The snapshot file is used to store the state of the VM and the capture file stores the live output of `tcpdump` as the VM runs. You can use the same snapshot file for the rest of the course, just don't use a file that already exists or it won't be able to launch the VM (it will try to use this file as its state and not be able to parse it).

If you see

```
Unable to init server: Could not connect: Connection refused
gtk initialization failed
```

it means that you are not using X forwarding.

Once the VM is launched, all of its network traffic is recorded to the *capture file*. This a packet capture file that can be viewed and analyzed with the open-source tool `wireshark`, or you can write your own programs using `libpcap`.

You can `ssh` into the VM by following the instructions. It should be `ssh tc@localhost -p <VM's ssh port>` and the password should be `CPSC526Pass`. The port is dynamically assigned and printed to the console when it starts.

Remote access to the VM will have a very laggy GUI, so you should only it to do the question on visiting `www.bbc.com`. For the server/client program, you should ssh into the VM instead, not open a console inside the GUI.

Your account should automatically allow you to run commands prefixed by `sudo` to grant super user privileges on the tinycore VM. Note that the use of ssh and similar commands generates network traffic which is recorded in the pcap file. Wireshark supports "filters" to remove this easily identifiable traffic to help you see what is important. *It is recommended to spend some time learning how to use wireshark's features.*

The VM may not have `gcc` available to compile your programs. To install it, run the following from *inside* the VM: `tce-load -wi compiletc`

Because of quirks of networking, you cannot run the server and the client both on the VM and correctly monitor the traffic. Consequently, run the server on the host machine (linuxlab) and the client on the VM. Thus, the program running on the VM connects to the server which is running on IP of the machine that launched the VM.

Don't save data on the VM Do not work on the files inside the VM as no guarantees are made on its storage. Work on your files in your normal lab environment, and copy them to the VM using `scp`:

`scp -P <VM's ssh port> <filename> tc@localhost:`

or

`scp -P <VM's ssh port> -r <directory> tc@localhost:`

Repeating: **do not store your work inside the VM and expect it to remain available**. If you shutdown the VM using the GUI screen your data should persist. Maybe. Who knows. **Do not rely on this**. Don't store data on the VM.

VM SSH Key Change It can happen that you see the TOFU-error for SSH:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
```

This happens whenever the public key for the VM changes (which can happen if it gets reset). This is how ssh uses public keys. When you first connect you see:

```
ECDSA key fingerprint is SHA256:p7tU6g/OhEMUB8Py6c3Od70MaO4Ktz/1Eijq37aaVNE.
Are you sure you want to continue connecting (yes/no)?
```

Typing yes means you either (i) verified that this is the correct key, or, more likely, (ii) use TOFU as your security model. The all-caps warning is the warning when the TOFU-model detects that the key is changed, indicating a possible man-in-the-middle attack. In this case, it is just that the VM reset and has a new key. After the warning it includes the instructions to remove it:

```
Offending ECDSA key in /home/<your home dir>/.ssh/known_hosts:X
```

where X is a line number. If you remove that line from that file you can log in again.

Editcap Your pcap file may be much larger than necessary if you do not, for example, use different ones for the different questions. In this case you can use the `editcap` command to remove parts of the pcap.

```
editcap -A "2018-10-28 15:12:00" <infile.pcap> <outfile.pcap>
```

This creates a file outfile.pcap consisting of only the packets after (-A) the specified time. A similar `-B time` can be used for packets before a specified time. Check with wireshark that you did not remove any packets relevant to the submission. *If you remove packets, you will change packet numbers. Be sure you submit correct packet numbers for the pcap you submit.*