Active class 1: Magic behind accessing World Wide Web

The learning objective of this class is to learn the role of networking in accessing world wide web (and Internet applications).

At the end of this activity, you should be able to:

1. Use your browser's developer tools to analyse the network transactions when accessing a webpage.
2. Use Wireshark to analyse packet transfers occurring in a device when browsing the internet.
3. Identify the protocol followed when accessing the WWW and internet applications.

This class activity is designed to be worked through active participation and collaborating with peers under the guidance of the teaching team in the class. The active classes are designed to be interactive, and they are here for you to extend your learning. However, these classes will only help you to enhance your learning if you come prepared. **To work on the class activities, you will be expected to have completed the Introduction module.** You need to have a basic understanding of layered model, TCP/IP, how it works and using the relevant tools. If you are not familiar with any of the above, please head to the Introduction Module in the CloudDeakin unit site and complete it before starting this active class.

The active classes are related to assessment tasks on OnTrack. After learning about different concepts from the content provided in the unit site, you will expand on this knowledge by working on activities designed to put these concepts into practice during the active classes and submit the completed task to OnTrack in the same week. The teaching team will guide and support your learning during these activities. This will help you manage your time and tasks better to avoid tasks piling up towards the deadlines. If you do not complete these activities in class, you will need to work on them in your own time, with limited support from us available.

The class activities are split into three parts. First, you will conduct a group discussion and a role play to understand the layered structure and responsibilities of each layer. Then, you will unpack the steps involve in accessing a webpage using a Chrome Developers tool. Finally, you will use Wireshark to further analyse the entire operation of accessing a webpage.

Activity 1:

This activity is a group activity. Therefore, you need to form a group of four (4)~ five (5) people. At your table (or in MS team chat) discuss the following questions and activities with your group members. Remember to take notes as they will help you prepare your task submissions.

1. Why we need protocols to communicate? What are the five layers in the Internet protocol stack?
2. What are the key responsibilities of each of the layers we have in TCP/IP stack? To carry on this discussion, Let us do a small role play.
    a. Each group member can act as a single layer, make sure each layer is assigned to at least one member.
    b. Let us assume we want to send a message "Hello" from Device one (source/ host) to device two (destination/server).
    c. Each member acting as a specific layer needs to discuss his/her responsibilities in sending and receiving message in Device 1 and Device 2, respectively.
    d. You can start the discussion with the application layer (the person who is acting as the application layer). Then, the application layer should pass the information to the next layer. Continue the process until message "Hello" is passed from device 1 to device 2. Each person (the relevant layer) needs to discuss their responsibility and name the protocols he/she would like to use to carry his/her job.
    e. As a group, you can also work out a diagram to show how these layers are interconnected with each other and encapsulation process of sending the message "Hello" from the source to destination.

Activity 2:

You can discover the behind-the-scenes process in accessing a web page using your web browser's developer's mode. We use Google Chrome as our browser (if you have not installed Google Chrome, please install it now). You need to use Chrome developer tools' network analysis features to analyse the magic we discussed in the Introduction module.

How to access: Open Google Chrome, View -> Developer -> Developer Tools

1. Open Google Chrome browser and Clear browsing history/ cache
2. Open developer tools
3. Type a URL of a Web page that your team would like to access into your Web browser
4. Analyse what happened behind the scenes using Network analyse feature. You need to explain the messages received/ sent between your device and other network devices to access the webpage you requested. You can use the following attributes/features for your discussions. Name of the file/request, Method, Status, Protocol, Scheme, domain, Type, size, time, connection Id (TCP), Waterfall (Timing sequence of the messages), total response time, byte transferred, and number of requests shown at the bottom of the panel.

5. Please make sure to save screenshots and your results as you need those for your task submissions (as part of your learning evidence).

Activity 3:

In Activity 3, you are using Wireshark **to further analyse the packet transfers occurred in your devices when you browse Internet. Wireshark is the packet sniffer that we are going to use in this unit to analyse various protocols.** You should have downloaded and installed Wireshark by now.

If you have not, please visit https://www.wireshark.org/#download to download Wireshark. We use the current stable release of Wireshark which is 3.4.5. Please download the relevant file that is suitable for your operating system and install Wireshark in your device.

More details on the Wireshark and the user guide can be access via https://www.wireshark.org/docs/wsug_html/

Wireshark cannot directly decrypt HTTPS. There is way to enable that, and we will look at the method when we talk about the transport layer protocols. Therefore, make sure that you use http rather than https when you type the URL in your browser for the packet capture.

1. Your group can choose a web page (make sure to use http) that you are going to access and use for analyses.
2. Follow the instructions provided in Introduction module in capturing the packets while you are browsing the web page.
3. List four different protocols that appear in the protocol column.
4. How long did it take to receive the HTTP OK reply from the HTTP GET message was sent?
5. What is the IP address of the Web server you accessed? What is the IP address of your computer? Provide the relevant screenshot to show this information in Wireshark.
6. Can you find the similar information in Chrome's Developer tools? Support your explanation with screenshots of Chrome's developer tools.

Provide a summary of your learning and evidence that you have achieved each of the learning objectives listed at the top of this activity. You can use the discussions/ screenshots that you have had while completing the activity as part of the evidence you need to provide in the lesson review.