22/5/2018 Week 2:

Review how to install programs by installing wireshark. It will fail when they try to run it, as they don't have permission to capture packets. Introduce them to the concept of user permissions and the use of groups to apply a permission to lots of people at once. Get them to use the adduser command to add themselves to the wireshark group. They can then run wireshark and capture some packets.

Explain how computer networks send information as discrete packets. Compare this with the old phone system, which required a continuous connection between each phone. Packets allow one wire the be shared between multiple connections, as the packets for each connection can fit between each other on the wire.

Explain the meaning of each column on the screen: timestamp, source address, destination address, ... Explain the meaning of each portion of the screen: packet stream, contents of the packet and the bits on the wire.

Pick a packet (eg a DNS packet) and look at an example of how a packet is constructed, and how each nested header represents a different layer in the network (Ethernet, IP, UDP, DNS,...) Different upper level protocols are are wrapped by lower level protocols until the packet is finally wrapped by an Ethernet header, which the physical network knows how to send and receive.

Explain the protocol column, and how the network can carry many different types of messages, these different types of messages being wrapped to look like Ethernet packets. Get the students to capture packets and see how many protocols they can spot (use the protocols column). Explain each protocol as they find them (ARP, BOOTP, DNS, ...)

Introduce the man command, to read the manual page for any command. Introduce the -k option to search for manual pages by keyword.