Analysis with TCP dump

TCPdump is a command-line tool that like wireshark, can be used to capture network traffic and view and analyse PCAP files.

tcpdump -D -> this command is used to see the interfaces available to see on the tcpdump

tcpdump -i interface -> tcpdump a specific interface

tcpdump -r -v -> -r used to read a file; -v to increase the verbosity

Specify TCP flags:

```
tcp[tcpfalgs] == tcp-ack/tcp-syn/tcp-fin/tcp-push/tcp-urg/tcp-rst)

Example of full command:
        tcpdump -r FTP.pcap "tcp[tcpflags] == tcp-ack"
```

Other flags:

```
-A -> Display packet contents in ASCII
-x -> print the hex dump of the packet
-X -> Print both above
t ; -tt ; -ttt; -tttt; -ttttt -> manage timestamps
```

Grep command:

```
We can use grep to find specific words in the output of tcp dump
```