Network Traffic Capture

tshark can be used to dump network traffic into capture files for later processing. For this, we need to tell tshark which interface to listen to and which traffic to capture. This is an example.
[crayon-6a9d5859ae645579868962/]

- The -f flag is used to specify a network capture filter (more on filters later). Packets that do not verify the condition following the -f flag will not be captured. In this example, only IP packets that are coming from or going to TCP port 80 are captured.
- The -w flag is used to specify a file where the captured traffic will be saved for later processing.