tcpdump

tcpdump is a tool to capture IP Packets at a command line level, its similar to the PCAP used by Wireshark (Wireshark is just a GUI to control PCAP). I say just a GUI, its rather good and saying it is 'just' a GUI is a little harsh.

On the MFEL, we can use tcpdump to capture either the IP Input or the IP Output. There are many commands available for tcpdump, and I will list some later on this page, but first lets just look at a working example, because this might be all you need for now.

To capture an IP Output (ensure you have started your service) use the following example. The following example is for eth2, where a multicast exists on 239.0.12.1 port 1234.

```
The format for tcpdump is - tcpdump -i <interface> -s 65535 -w <some-file>
tcpdump -i eth2 -B 64000 dst host 239.0.12.1 and port 1234 and multicast -w /home/ts_capture_test.pcap
if the syntax is correct, the tcpdump will start:
tcpdump: listening on eth2, link-type EN10MB (Ethernet), capture size 65535 bytes
```

running the previous command will start the capture, and it will capture until stopped (using CTRL-C)

Pressing CTRL-C stops the output, and you will see something like the following:

```
119658 packets captured
119663 packets received by filter
0 packets dropped by kernel
```

The capture is a pcap file, the same format that would have been captured if you were using Wireshark, to get the video from this you will have to extract it first.