

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.

```
tcpdump -i eth2 -B 64000 dst host 239.0.12.1 and port 1234 and multicast -w /home/ts_capture_test.pcap
```

From:

<http://cameraangle.co.uk/> - WalkerWiki - wiki.alanwalker.uk

Permanent link:

<http://cameraangle.co.uk/doku.php?id=wiki:tcpdump&rev=1480623913>

Last update: **2023/03/09 22:35**

