

PCAP to TS

Sometimes it is useful to capture the video streams we are generating (or someone else is generating) that are present on the network. Using a Dektec is useful here, however we don't always have the opportunity to use an analyser.

For example, if you want to capture the input or the output of the MFEL, you cannot use a Dektec if the unit is remote. But you can use a tool preinstalled on the MFEL called **tcpdump**.

tcpdump creates the same **.pcap** format files that **Wireshark** produces (so this guide will work for Wireshark also).

Using tcpdump to create .pcap files

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.

Convert .pcap to .ts

Having created a .pcap file means we have all of the information we need to replay and analyse any captured stream. However before we access the stream we need to extract the Transport Stream from the .pcap file and save it as a .ts.

There is a tool available called **Extractor.exe** that we can use to extract the TS from the .pcap file.

Before we extract the TS data, we need to know what the **original multicast** details are (multicast:port) as we will need these for the extractor to work. If you know these details then fine, if not you may need to open the .pcap file in Wireshark to work out the exact multicast and port.

To use the extractor, use the following syntax:

```
extractor source_file.pcap output.ts multicast port
```

If I have a source file called **mfel.pcap** and I want to extract this to **mfel.ts**, assuming the original multicast details are 239.0.12.1:1234 then my command line will be:

```
extractor mfel.pcap mfel.ts 239.0.12.1 1234  
If successful then you will see an output
```

```
SkyStream Networks sniffer-to-MPEG Extractor Utility  
Built May 5 2005 11:29:37  
File had 119658 packets, 119658 extracted
```

The number of packets will change of course, but you should now have an extracted TS file.

Finally, see the FFMPEG section where you can convert .ts files to .mpg files (great for converting captures for replay on TVs via USB).[FFMPEG](#)

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

Permanent link:
http://cameraangle.co.uk/doku.php?id=pcap_to_ts&rev=1481788803

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

