Wireshark Tracing

Filters

Simply filtering for a particular SIP host, for example all traffic from and to a PBX, could be achieved using the following filter:

Filter a specific host

```
host 192.168.2.25
```

This filter could be used to filter all packets from and to a particular subnet, for example a subnet with a PBX and extensions:

Filter a subnet

```
net 192.168.2
```

If several trunks are present, it may be necessary to filter all SIP packets. This cannot be done reliably by capturing only port 5060 - this will miss extremely large SIP messages (in particular INVITE) in some setups - the UDP packet may be fragmented, and some of the message will be missing.

Filter all SIP packets

```
port 5060 or ip[6:2] & 0x1fff != 0
```

Command Line Tracing

List Interfaces

The following command can be used to list all interfaces for tracing from the command line with the -i option:

List all Interfaces

```
"C:\Program Files\Wireshark\dumpcap" -D
```

Howto: create a wireshark rotating dump file with a fixed size

This can be useful, to create wireshark traces on a machine where a problem is being analysed, but the trace must be left running for a long time.

This command specifies the interface to use (-i), includes a capture filter (-f), and limits the number of files to 10, and the file size to 100000KB.

```
"C:\Program Files\Wireshark\dumpcap" -i 1 -f "host 192.168.2.25" -b files:10 -b filesize:100000 -w hosttrace.cap
```