Remote capture using tcpdump and Wireshark

On **server**

Create a named pipe:

```
# mkfifo /tmp/tcpdump
```

make it readable only by a local user that will connect from remote

```
# chown lele /tmp/tcpdump
# chmod 600 /tmp/tcpdump
```

Run tcpdump as root and redirect the packets to the named pipe:

```
# tcpdump -s 0 -U -n -w - -i eth0 not port 22 > /tmp/tcpdump
```

On **client**

Create a named pipe:

```
$ mkfifo /tmp/remote
```

Start wireshark from the command line pointing at the created pipe

```
$ wireshark -k -i /tmp/remote &
```

Tunnel data via ssh from remote pipe to local pipe:

```
$ ssh unprivuser@firewall "cat /tmp/tcpdump" > /tmp/remote
```

Nota

Le pipe si aprono quando vengono lette da wireshark e vengono chiuse (compreso il processo che sta scrivendo e cioe' tcpdump) quando wireshark ferma la cattura.