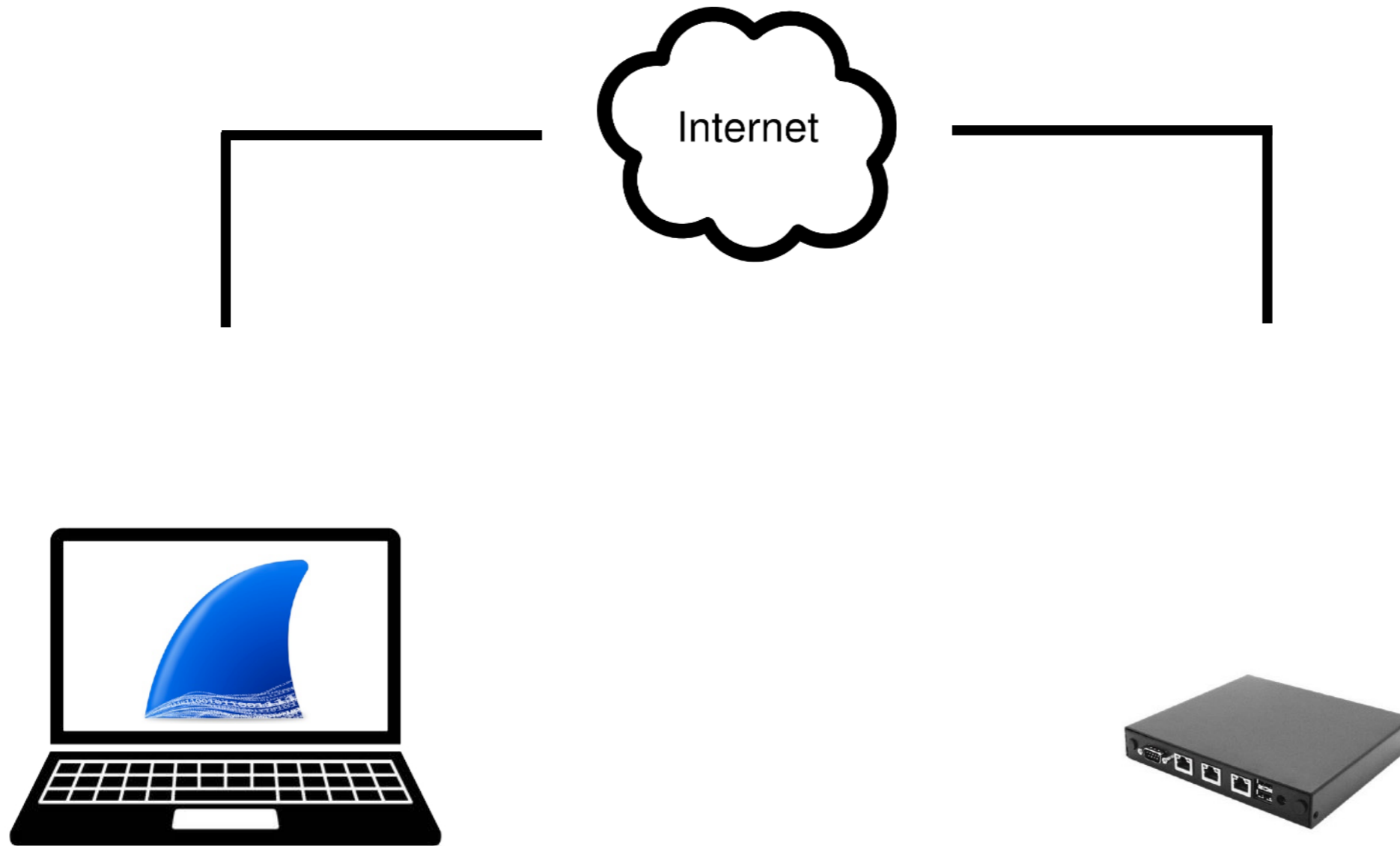


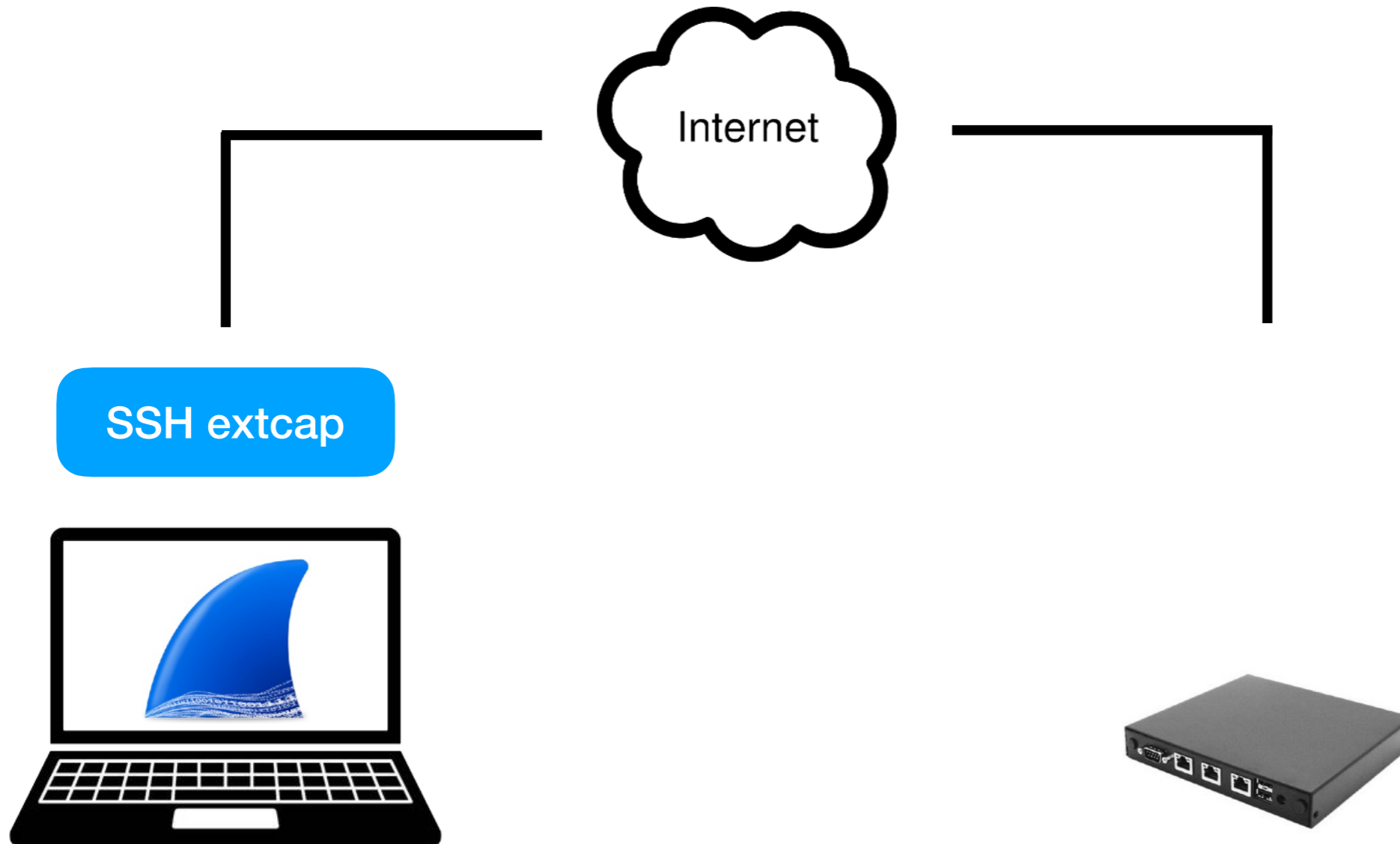
ntop Extcap: Where Wireshark Meets DPI and HW-Based BPF



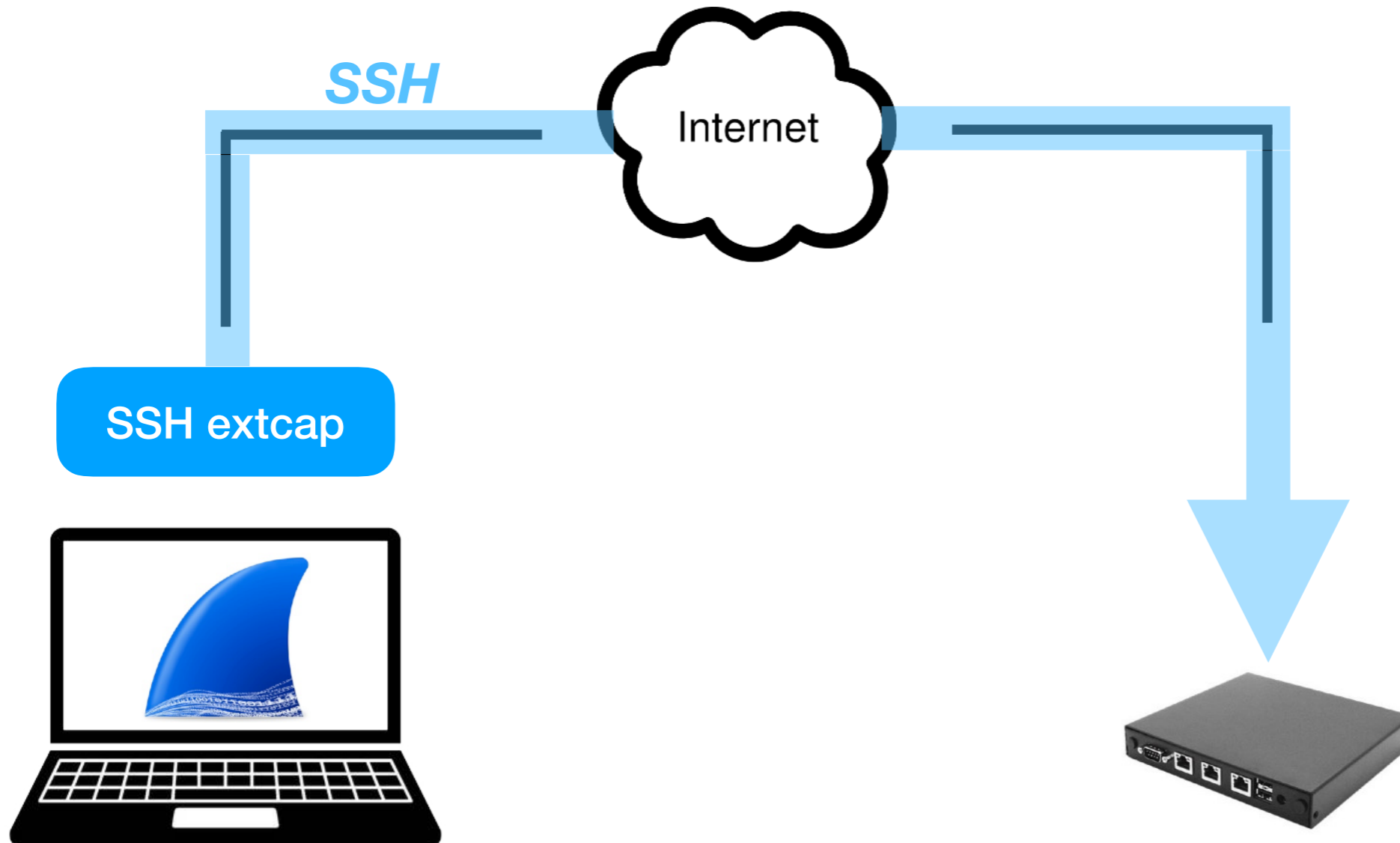
Topology



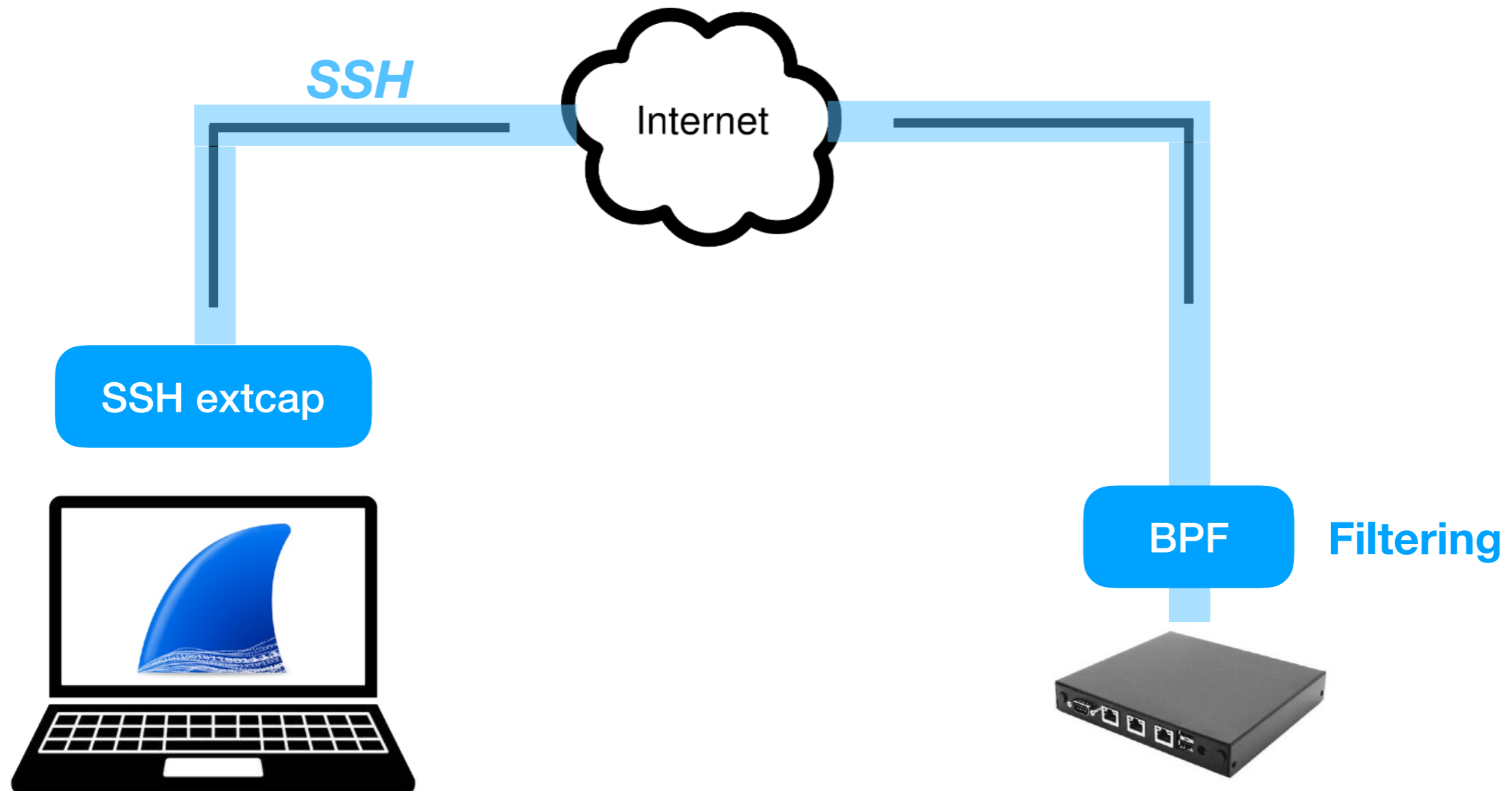
SSH Extcap



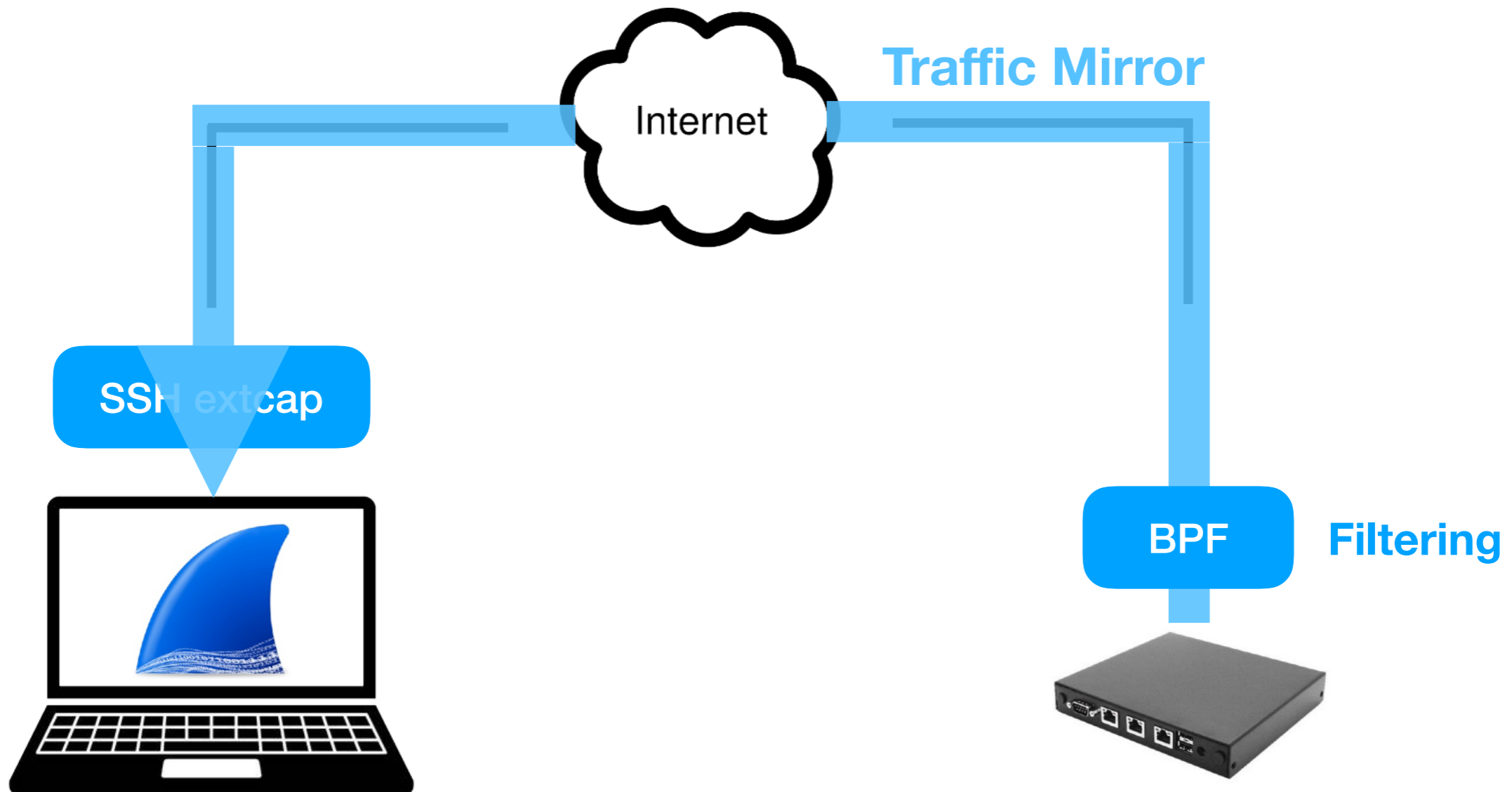
SSH Extcap



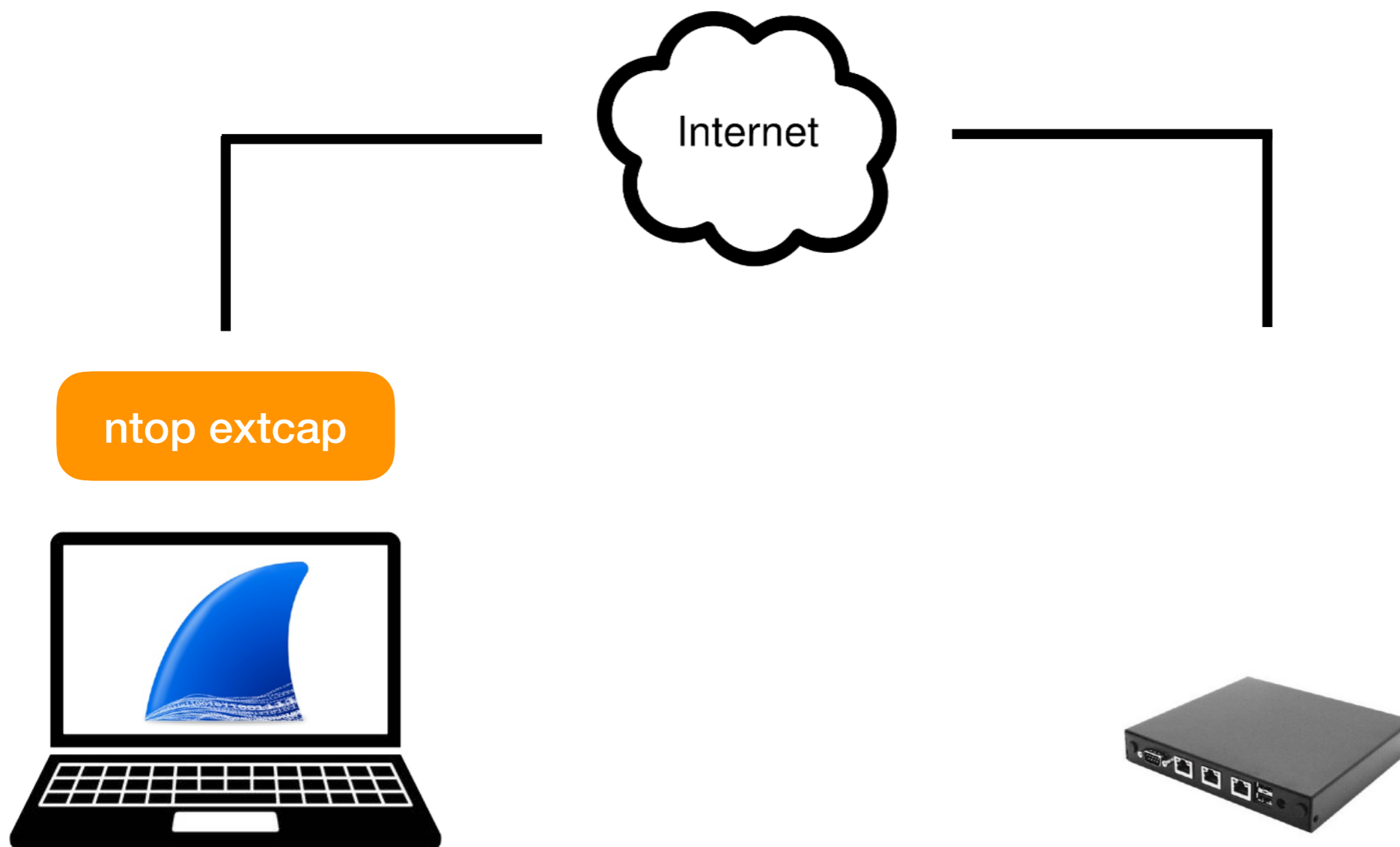
SSH Extcap



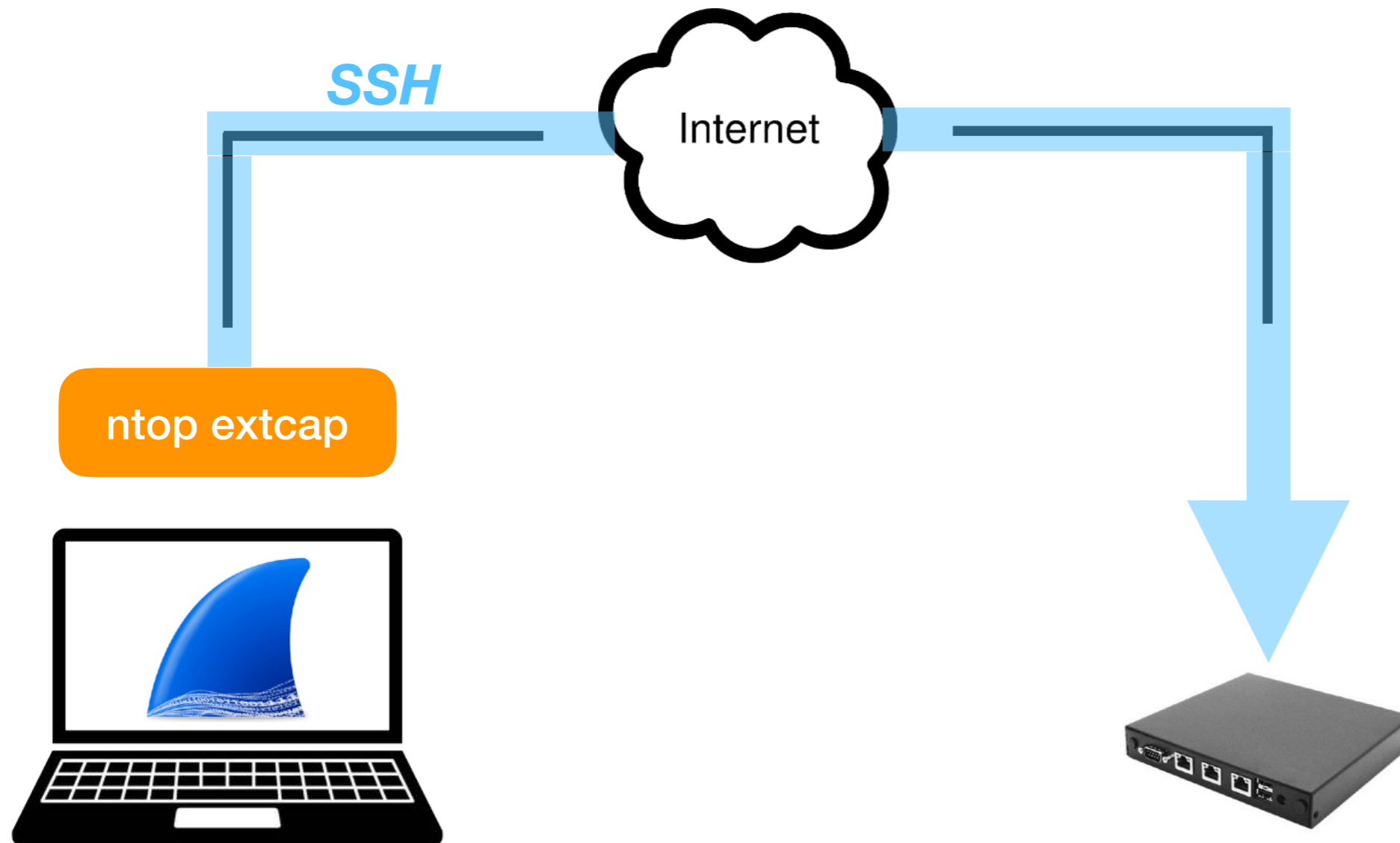
SSH Extcap



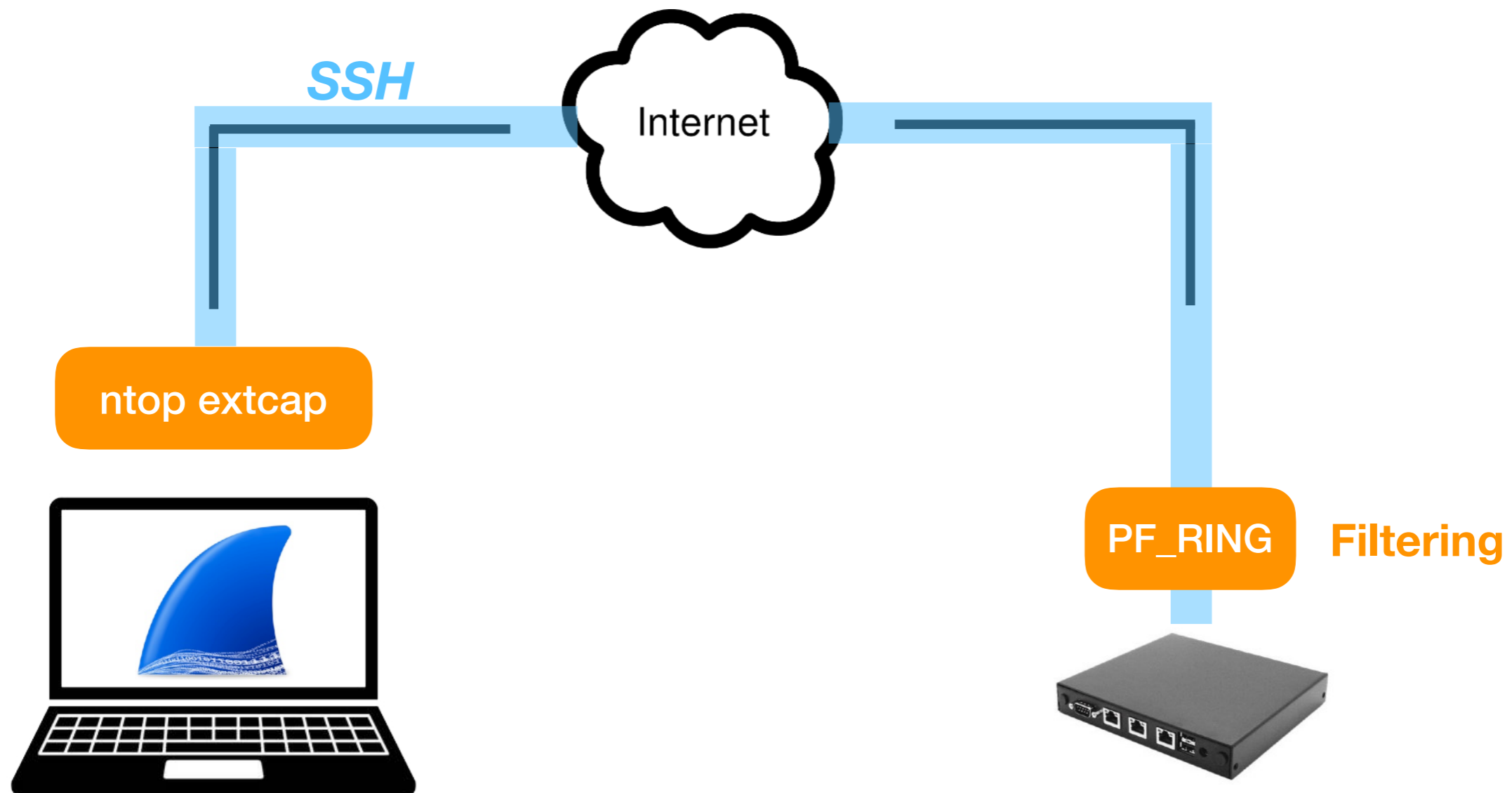
Ntop Remote Extcap



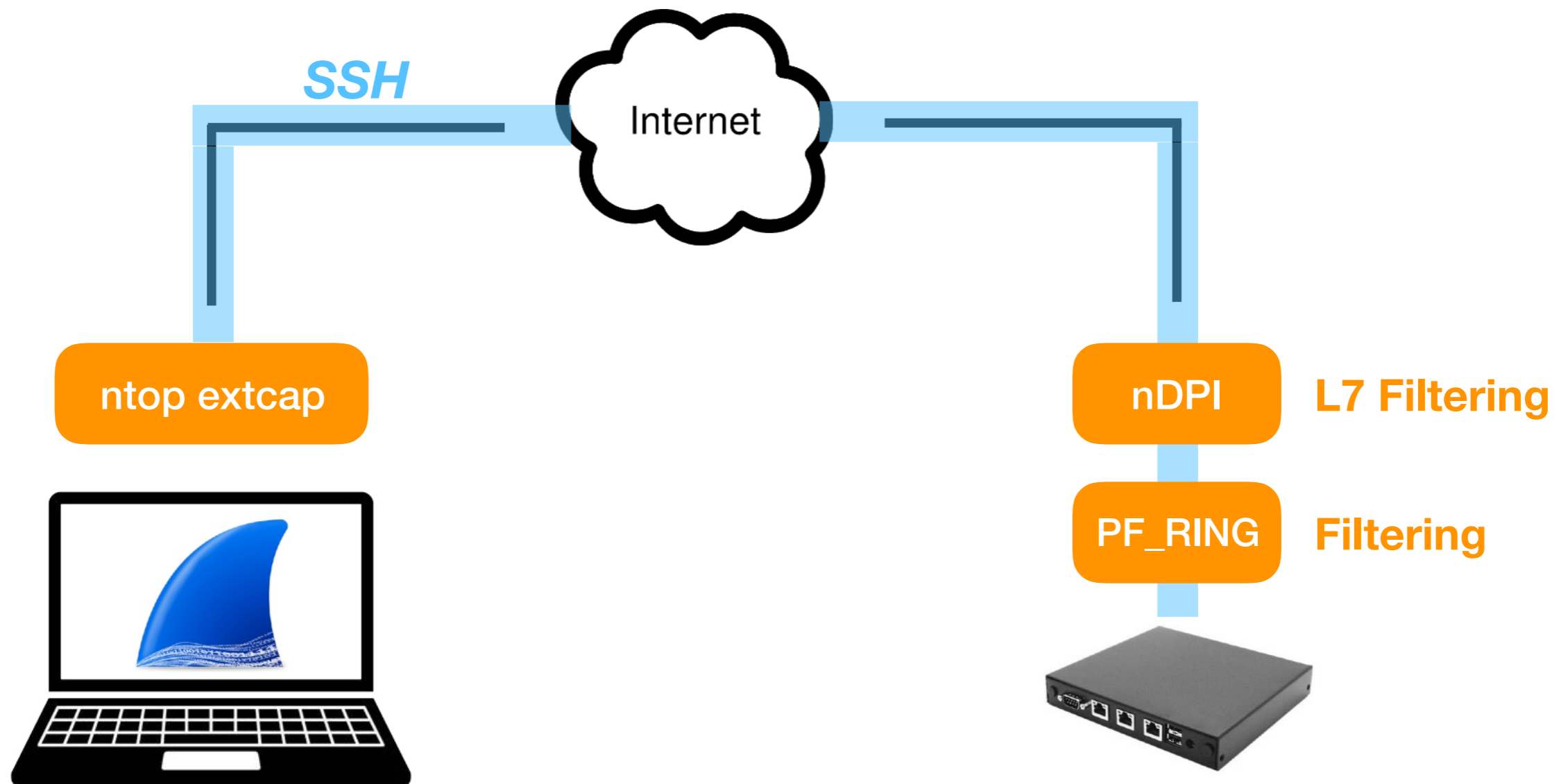
Ntop Remote Extcap



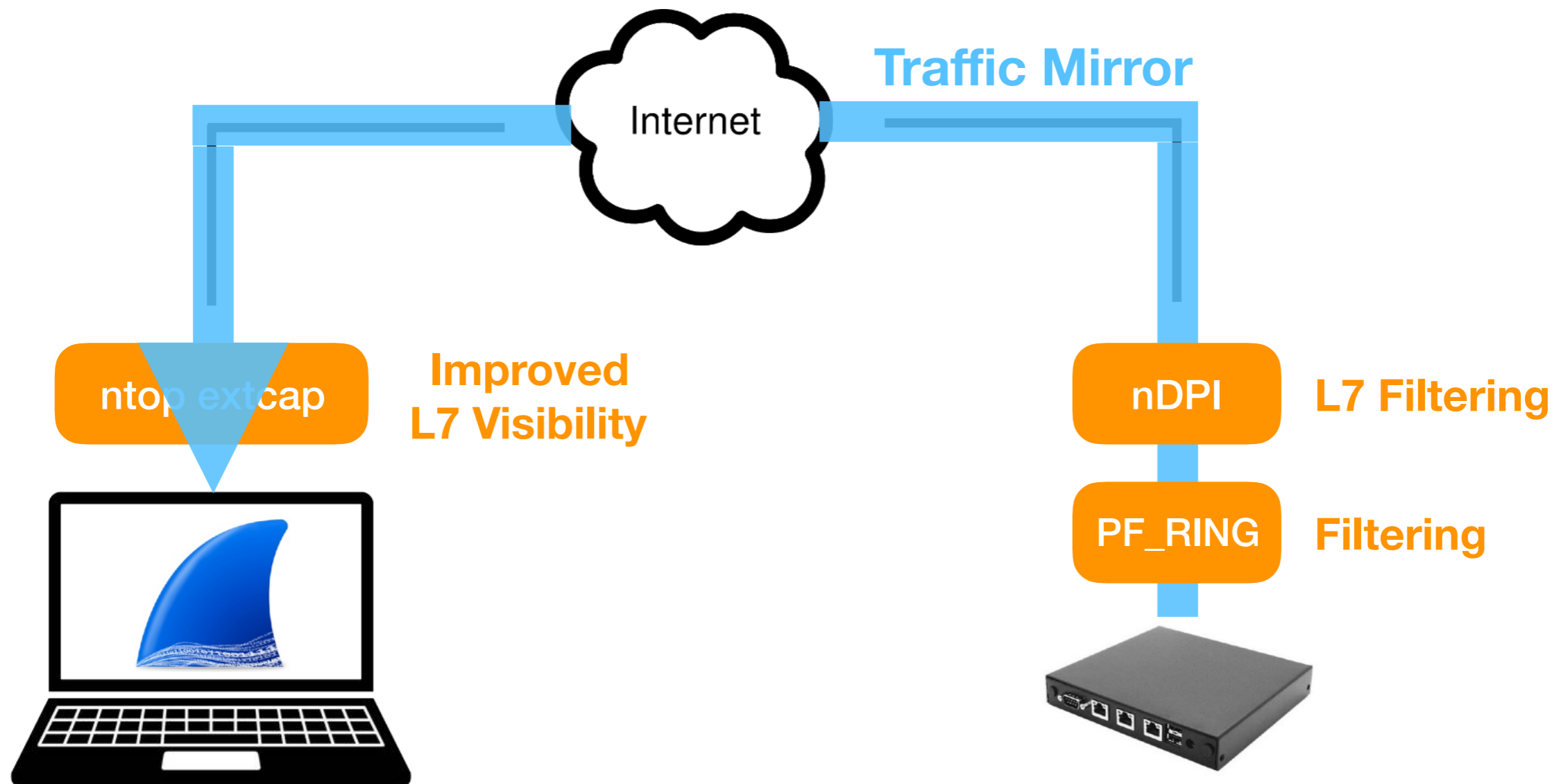
Ntop Remote Extcap



Ntop Remote Extcap



Ntop Remote Extcap



Advantages

- Improved L7 visibility
 - HTTP requests for www.facebook.com are marked as HTTP.Facebook)
 - Protocol detection on non-standard ports
- L7 filtering on the remote machine
- Support for FPGA cards, with hw filtering (when available)



1. Install the ntop “remote” extcap module

```
git clone https://github.com/ntop/n2disk.git n2disk-pub
cd n2disk-pub/wireshark/extcap/ && make
cp remotentopdump /Applications/Wireshark.app/Contents/MacOS/extcap/
```

2. Install the nDPI plugin

```
git clone https://github.com/ntop/nDPI.git ~/nDPI
mkdir -p ~/.wireshark/plugins
cp ~/nDPI/wireshark/ndpi.lua ~/.wireshark/plugins
```



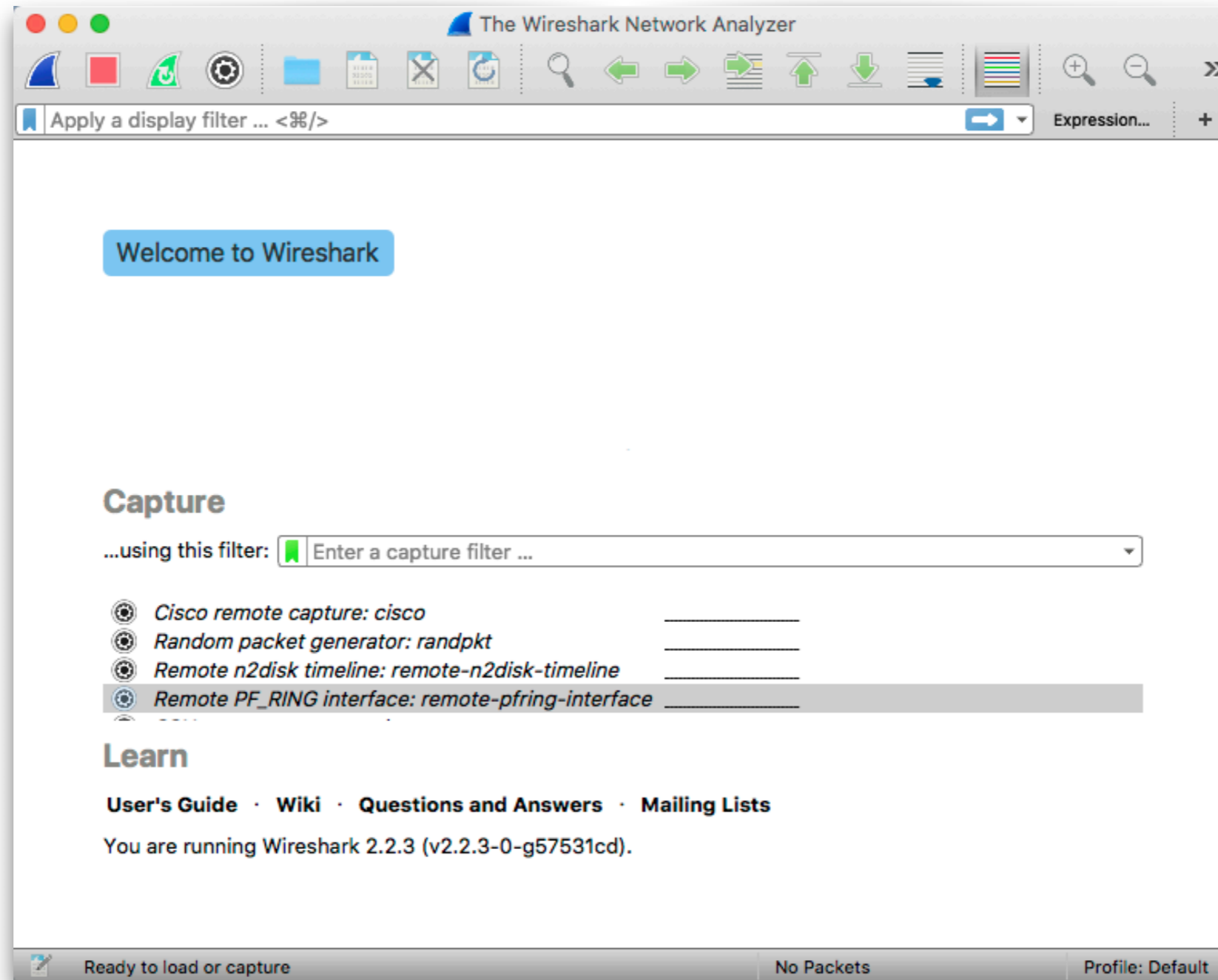
1. Install PF_RING tools

```
git clone https://github.com/ntop/PF_RING.git ~/PF_RING
cd ~/PF_RING/kernel && make && sudo insmod ./pf_ring.ko
cd ~/PF_RING/userland/lib && ./configure && make
cd ~/PF_RING/userland/libpcap && ./configure && make
cd ~/PF_RING/userland/examples && make && sudo make install
```

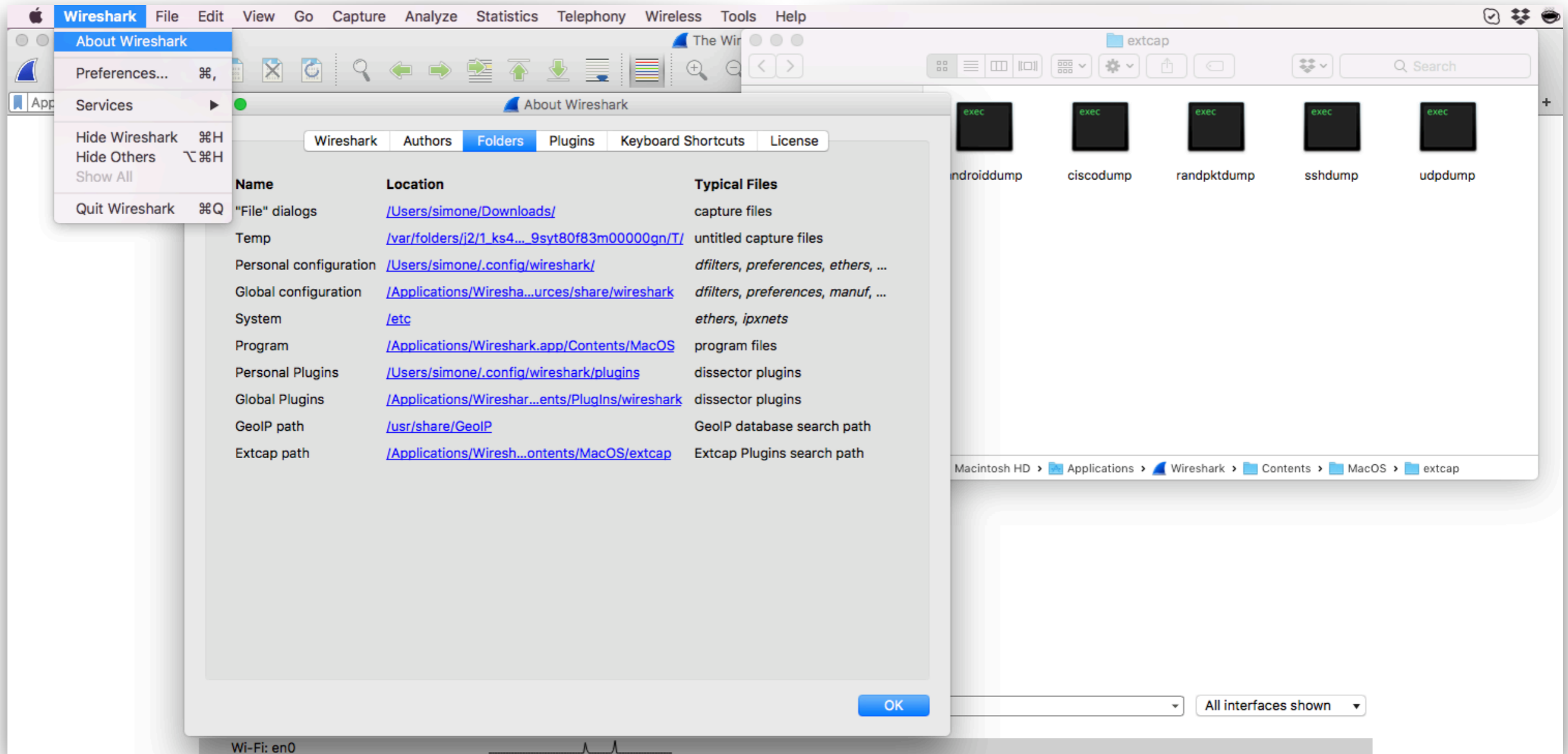
2. Install nDPI tools

```
git clone https://github.com/ntop/nDPI.git ~/nDPI
cd ~/nDPI && ./autogen.sh && ./configure && make
cd ~/nDPI/example && sudo make install
```

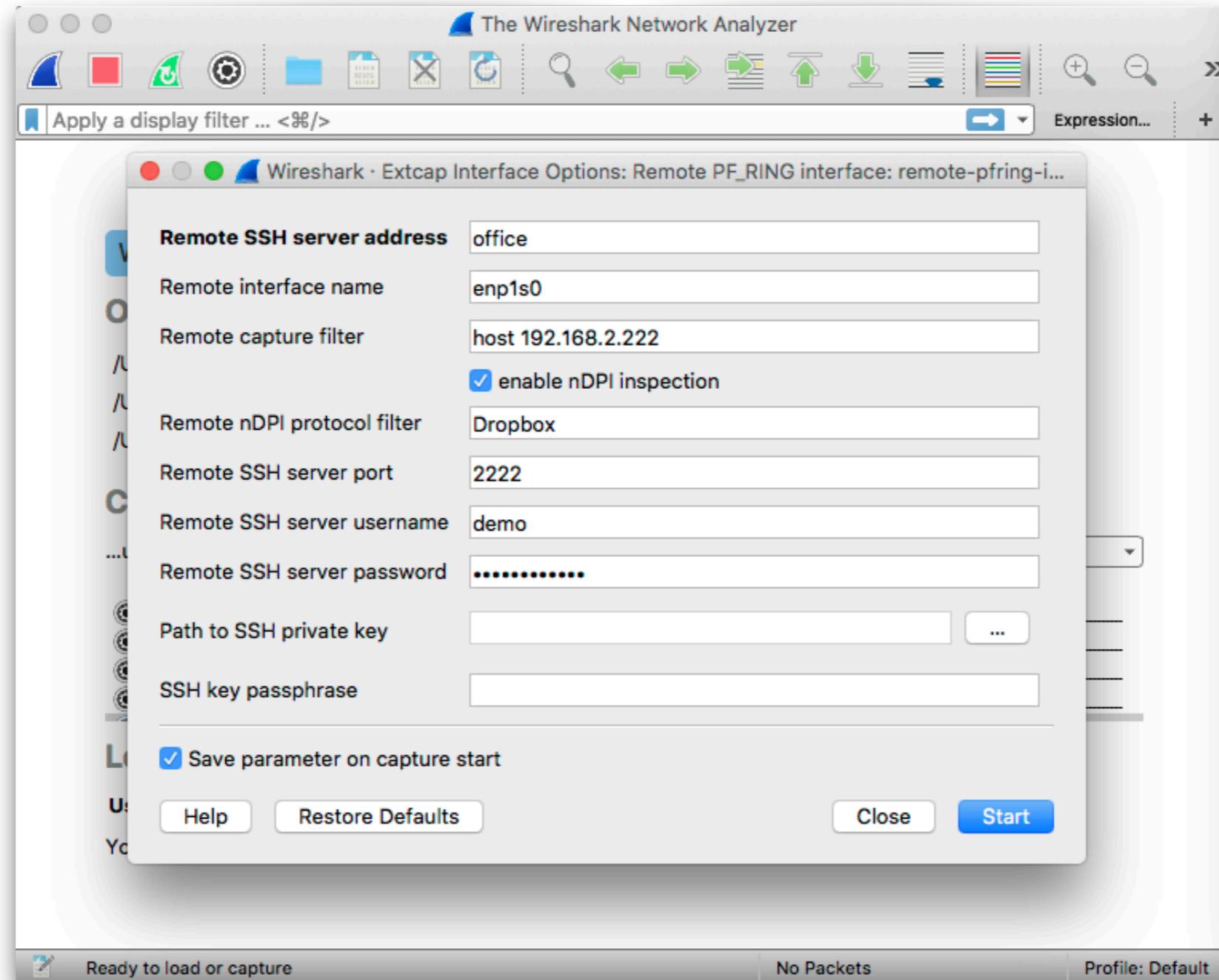
Demo



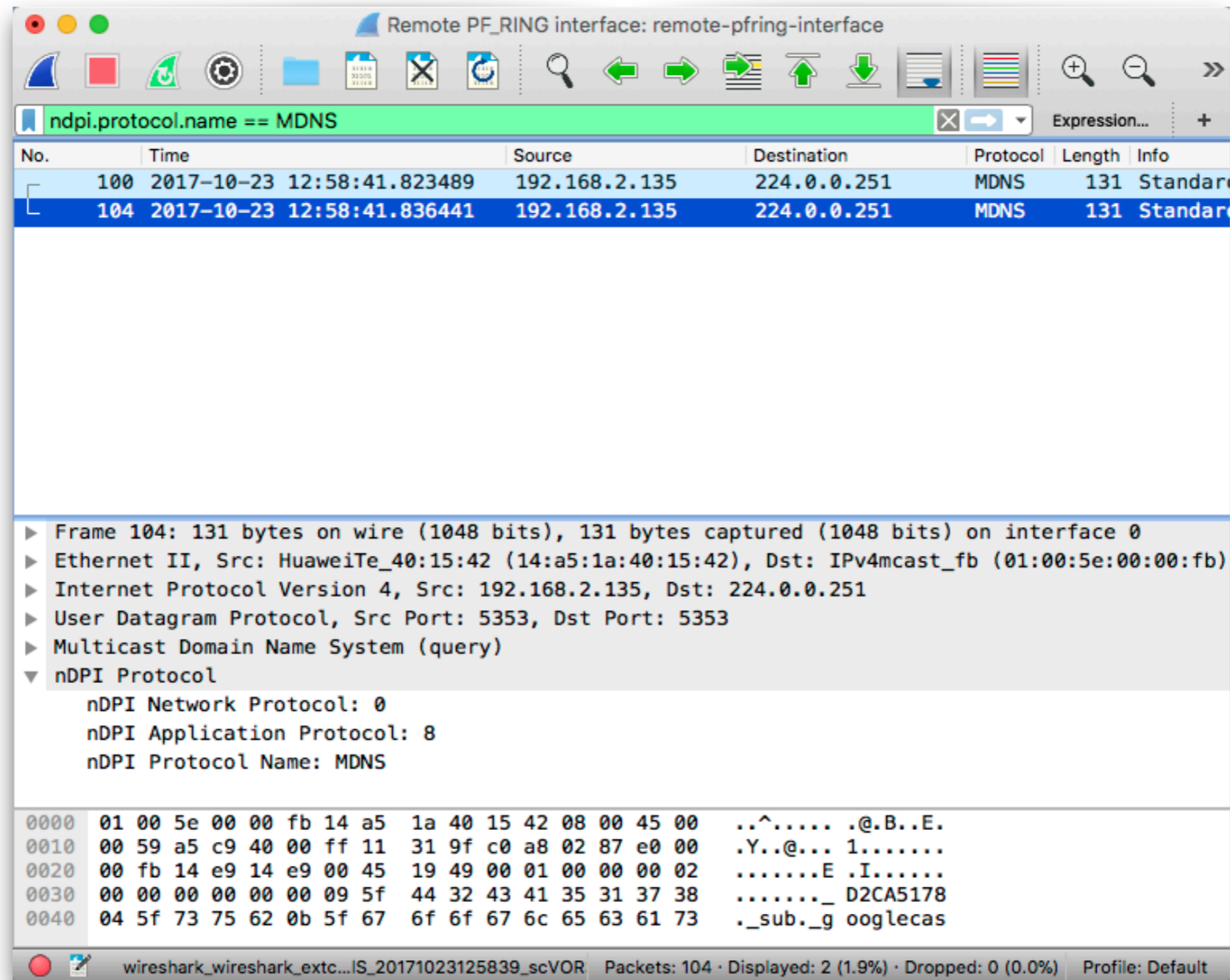
Demo



Demo



Demo



Remote PF_RING interface: remote-pfring-interface

Filter: ndpi.protocol.name == MDNS

No.	Time	Source	Destination	Protocol	Length	Info
100	2017-10-23 12:58:41.823489	192.168.2.135	224.0.0.251	MDNS	131	Standard
104	2017-10-23 12:58:41.836441	192.168.2.135	224.0.0.251	MDNS	131	Standard

Frame 104: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits) on interface 0

- Ethernet II, Src: HuaweiTe_40:15:42 (14:a5:1a:40:15:42), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
- Internet Protocol Version 4, Src: 192.168.2.135, Dst: 224.0.0.251
- User Datagram Protocol, Src Port: 5353, Dst Port: 5353
- Multicast Domain Name System (query)
- nDPI Protocol
 - nDPI Network Protocol: 0
 - nDPI Application Protocol: 8
 - nDPI Protocol Name: MDNS

```
0000  01 00 5e 00 00 fb 14 a5 1a 40 15 42 08 00 45 00  ..^..... .@.B..E.
0010  00 59 a5 c9 40 00 ff 11 31 9f c0 a8 02 87 e0 00  .Y..@... 1.....
0020  00 fb 14 e9 14 e9 00 45 19 49 00 01 00 00 00 02  .....E .I.....
0030  00 00 00 00 00 00 09 5f 44 32 43 41 35 31 37 38  ....._ D2CA5178
0040  04 5f 73 75 62 0b 5f 67 6f 6f 67 6c 65 63 61 73  ._sub._g ooglecas
```

wireshark_wireshark_extc...IS_20171023125839_scVOR Packets: 104 · Displayed: 2 (1.9%) · Dropped: 0 (0.0%) Profile: Default

