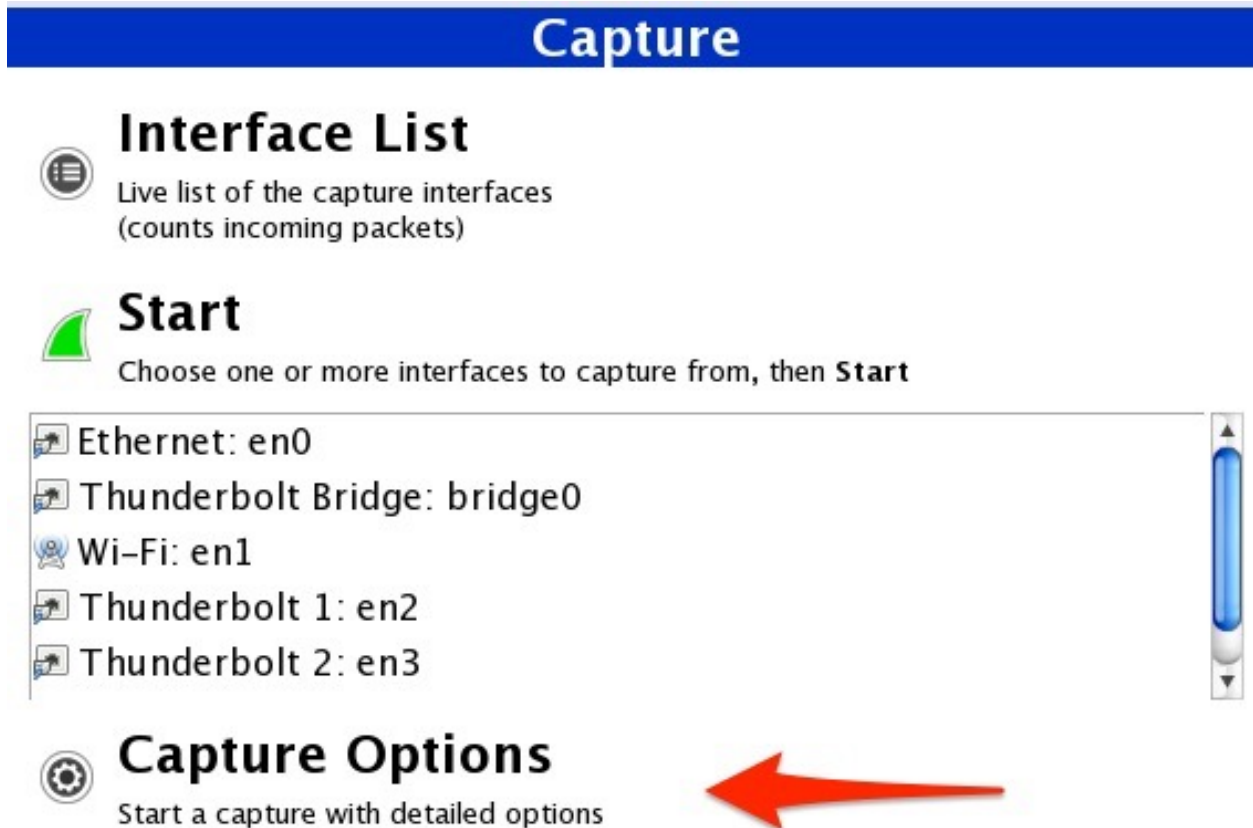


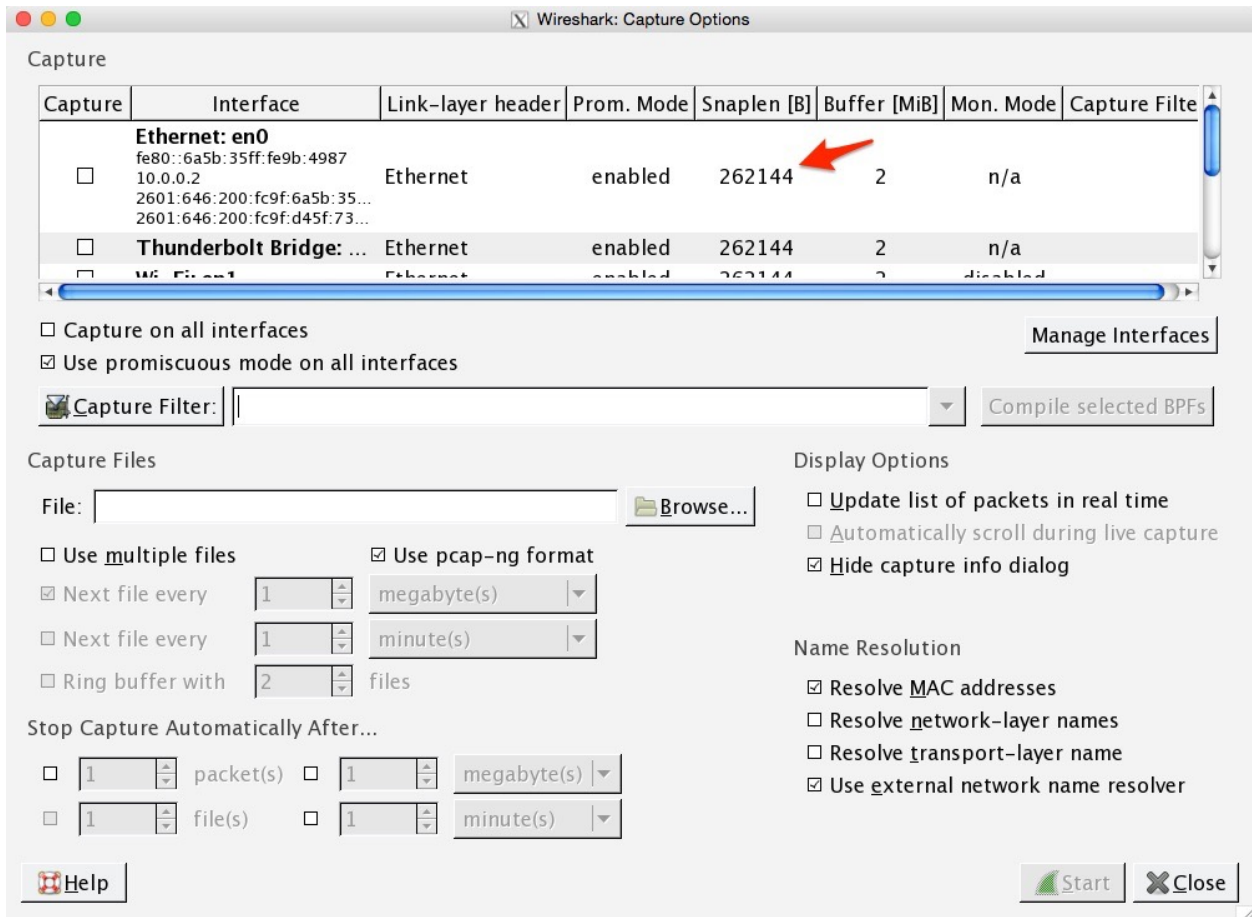
# Snaptlength How-To

## With Wireshark 1.x

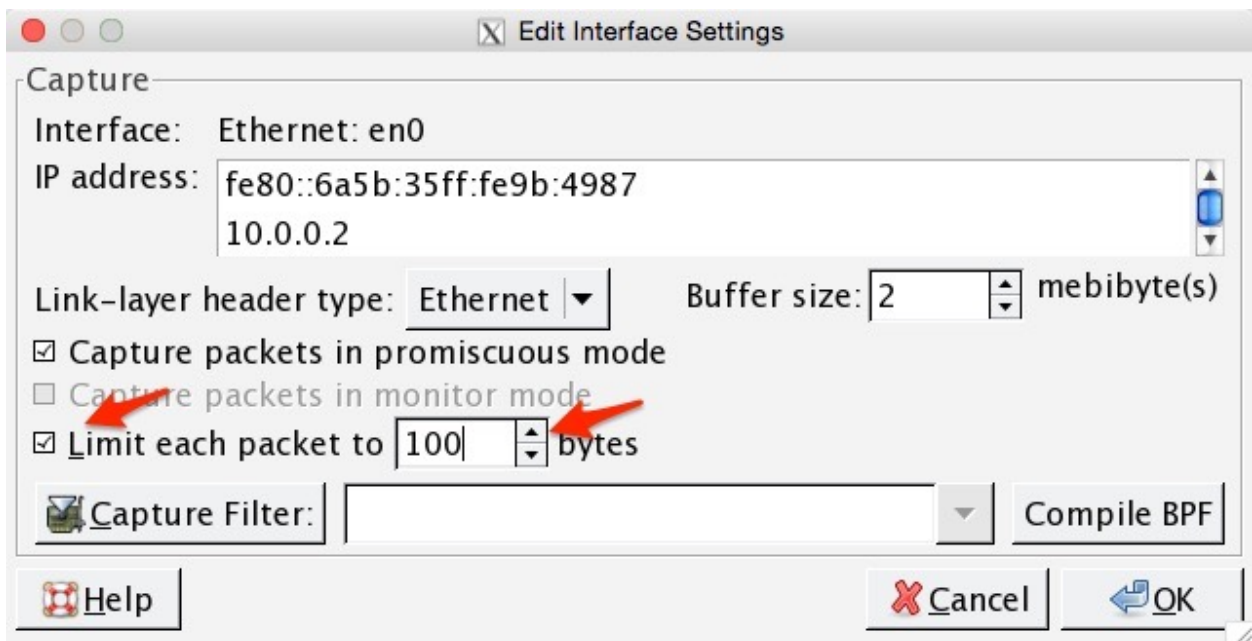
1. Open the Capture Options



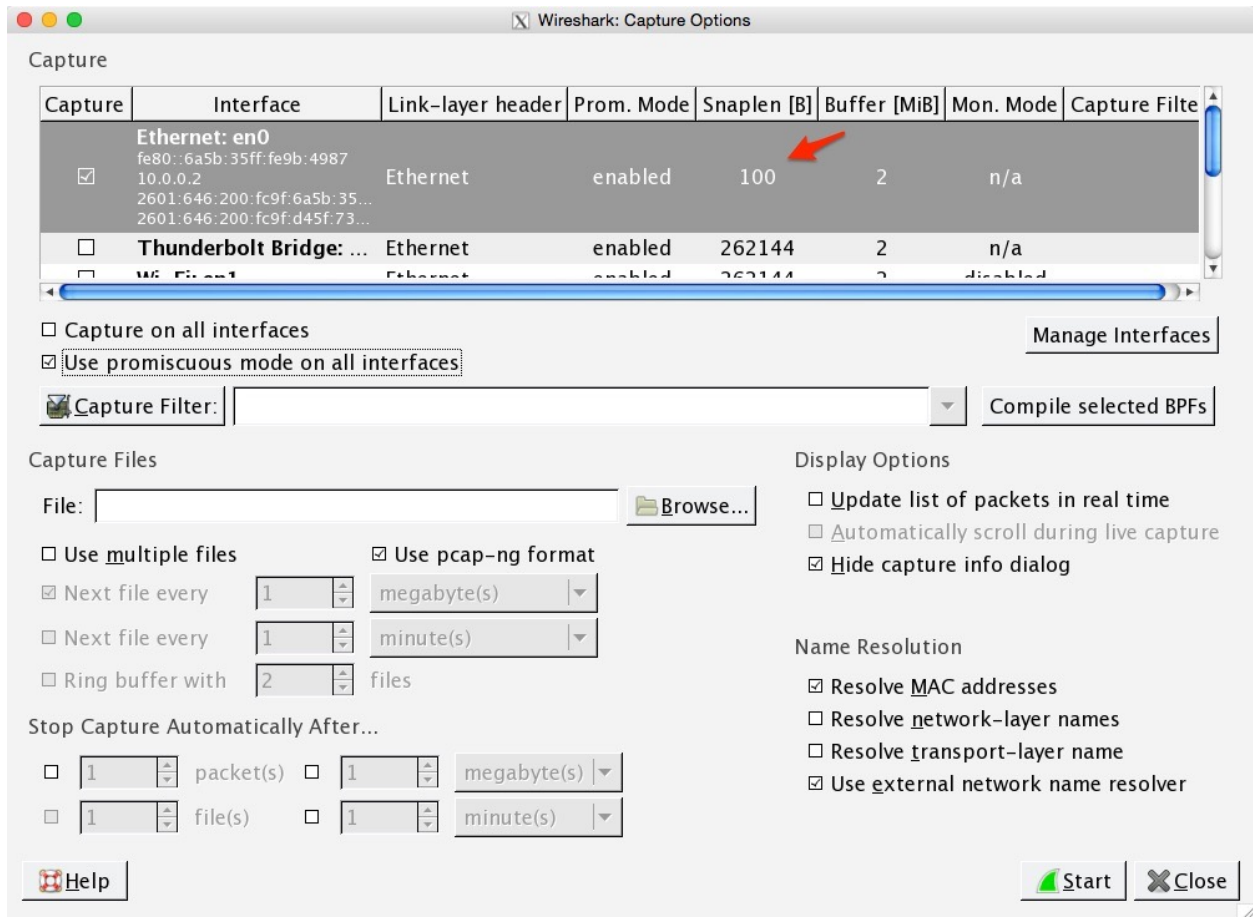
2. See what the snaplength is set to and double click the interface to change it



3. Set the snaplength by limiting the number of bytes saved for each packet

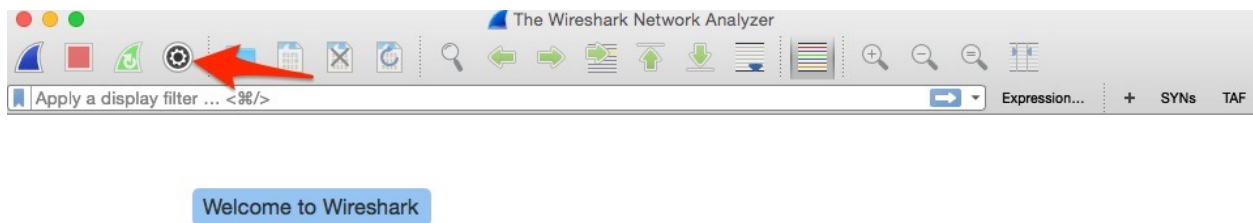


#### 4. Hit OK and verify the snaplength has been updated

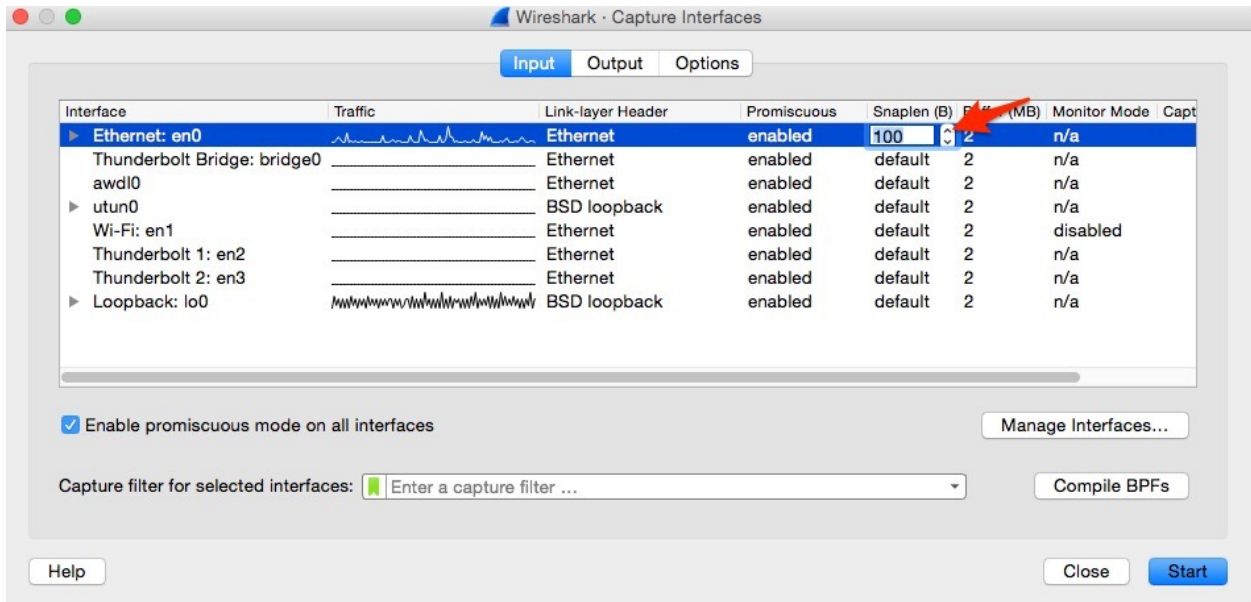
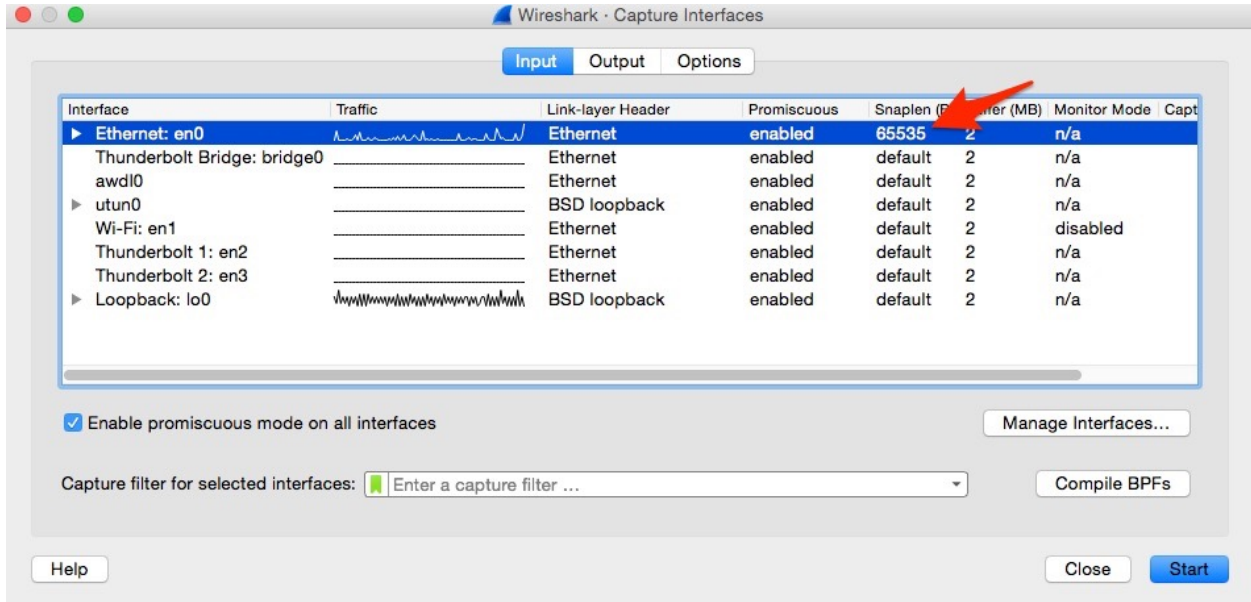


## With Wireshark 2.x

#### 1. Open the Capture Options



2. See what the snaplength is set to for the interface and double click it to change it



## With dumpcap on Windows

Dumpcap uses less resources than Wireshark and is preferable for long running or large captures.

First, find the interface you want to capture on by running dumpcap with -D:

```
C:\Program Files\Wireshark>dumpcap -D
1. \Device\NPF_{5D21FB4F-D9BF-47AC-AD3E-CE2E172F27A0} (Ethernet)
```

To capture on that interface, use the -i option with the number of the interface:

```
C:\Program Files\Wireshark>dumpcap -n -i 1 -s 100 -w
save100bytes.pcap
Capturing on 'Ethernet'
File: save100bytes.pcap
```

This same syntax will work on Windows, Mac, and Linux.

## With tcpdump

tcpdump is another good low resource alternative to Wireshark. It also uses the -s option to set a snaplength.

```
$ tcpdump -ni eth0 -s 100 -w save100bytes.pcap
```

## References:

- [dumpcap reference](#)
- [tcpdump reference](#)
- [dumpcap tutorial](#)