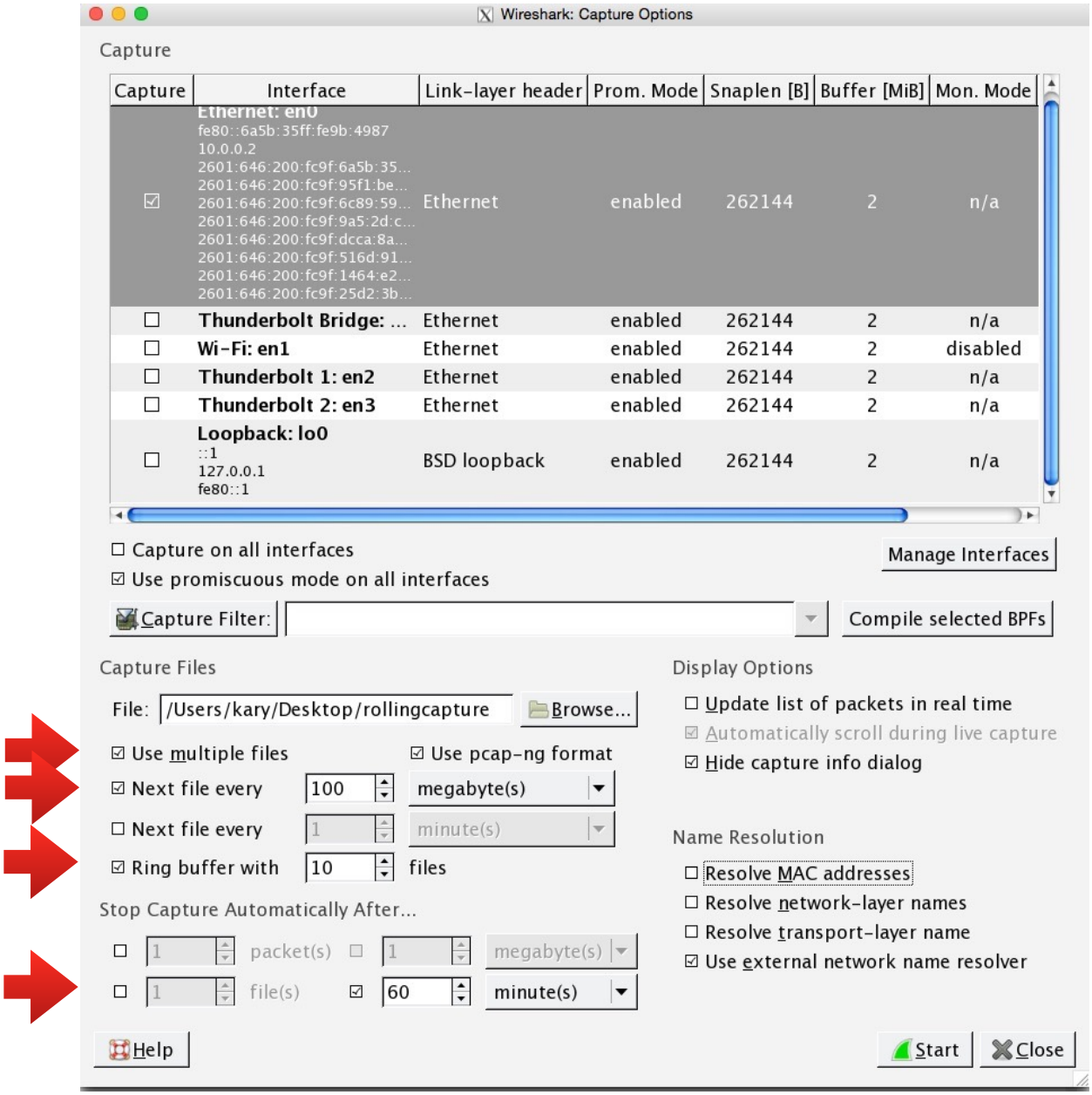
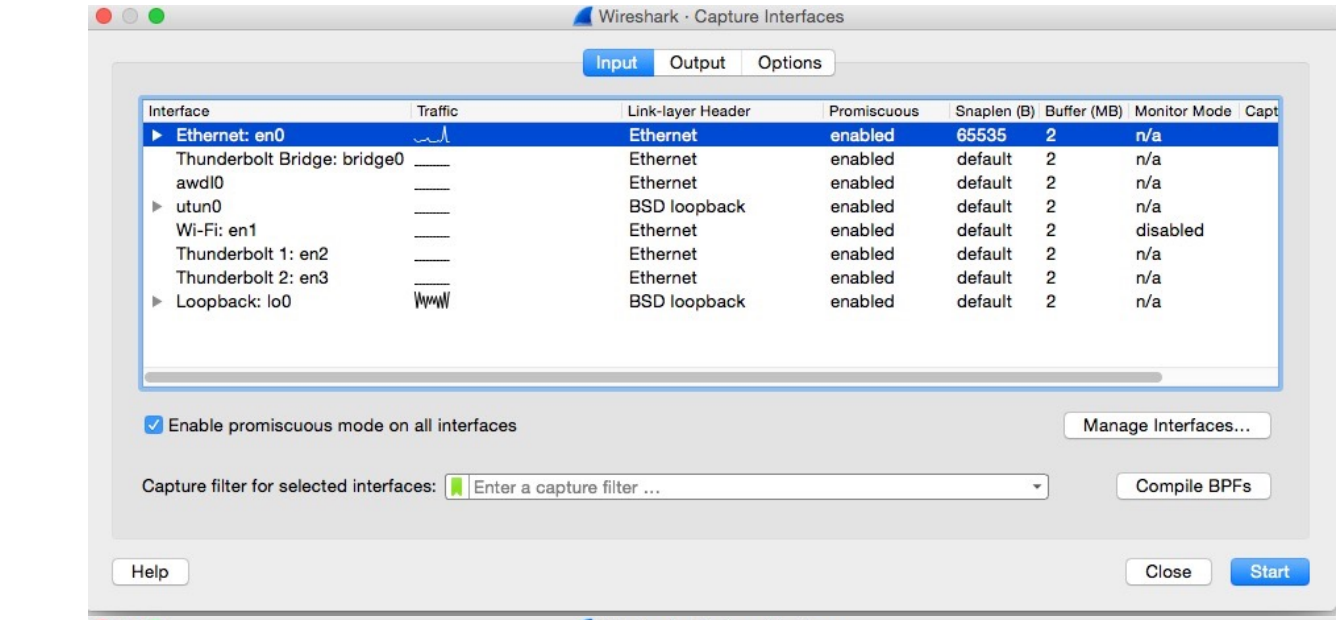
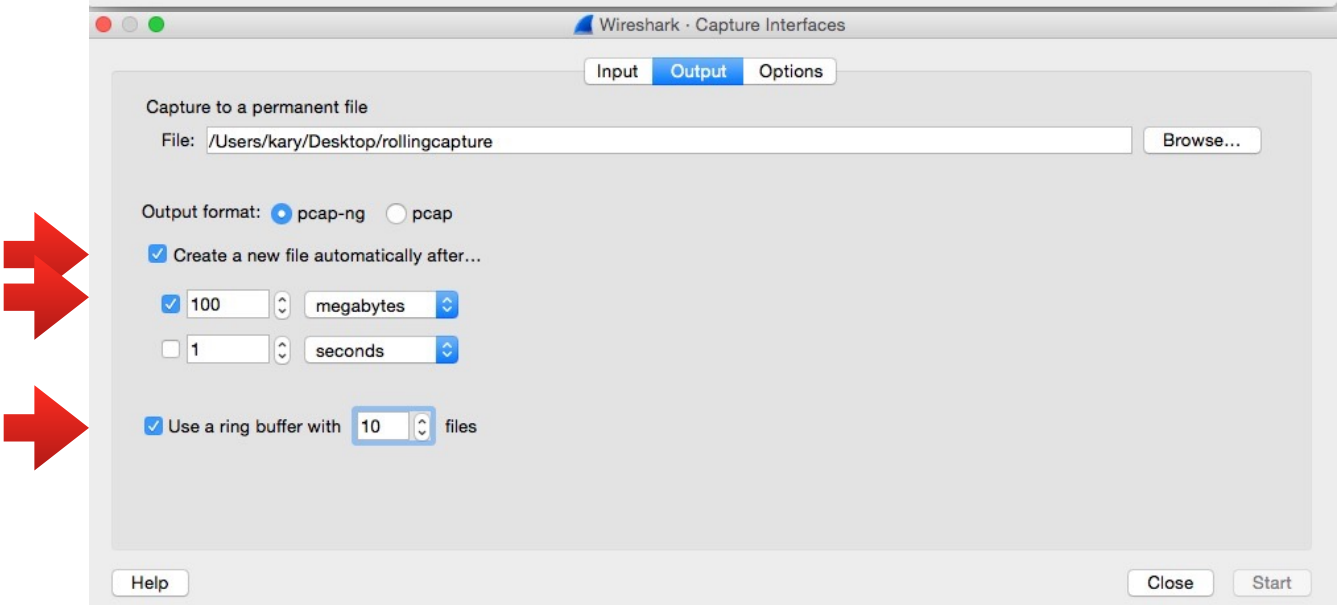
Rolling Capture How-To

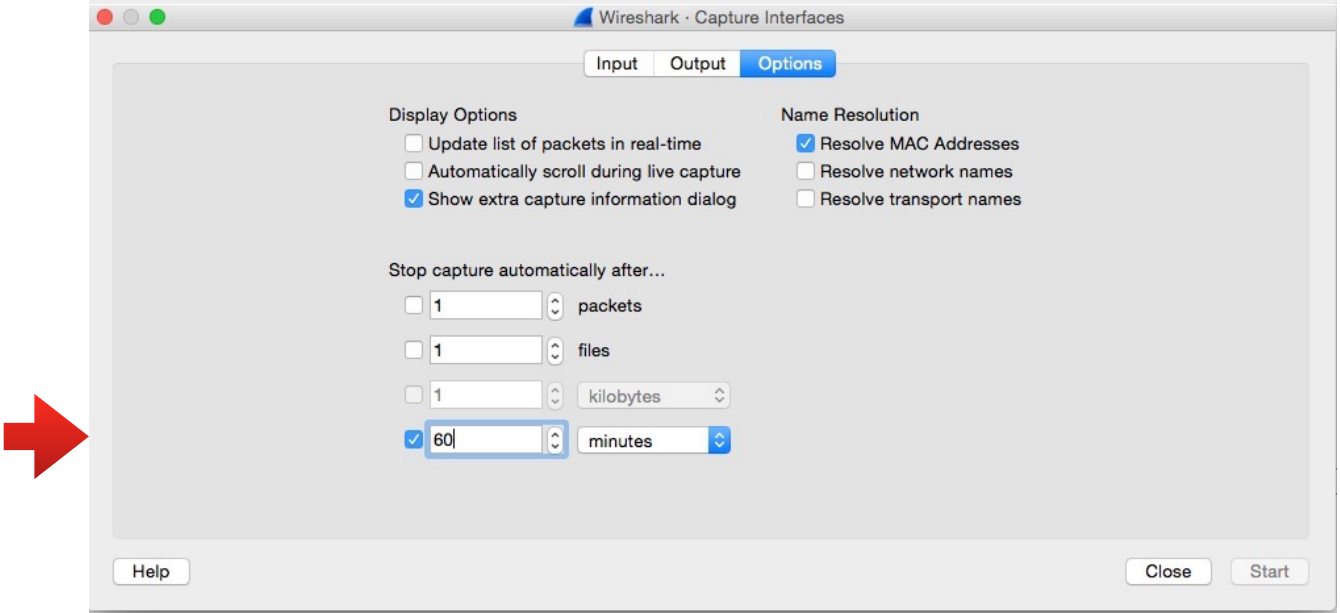
Wireshark 1.x on Mac OS X



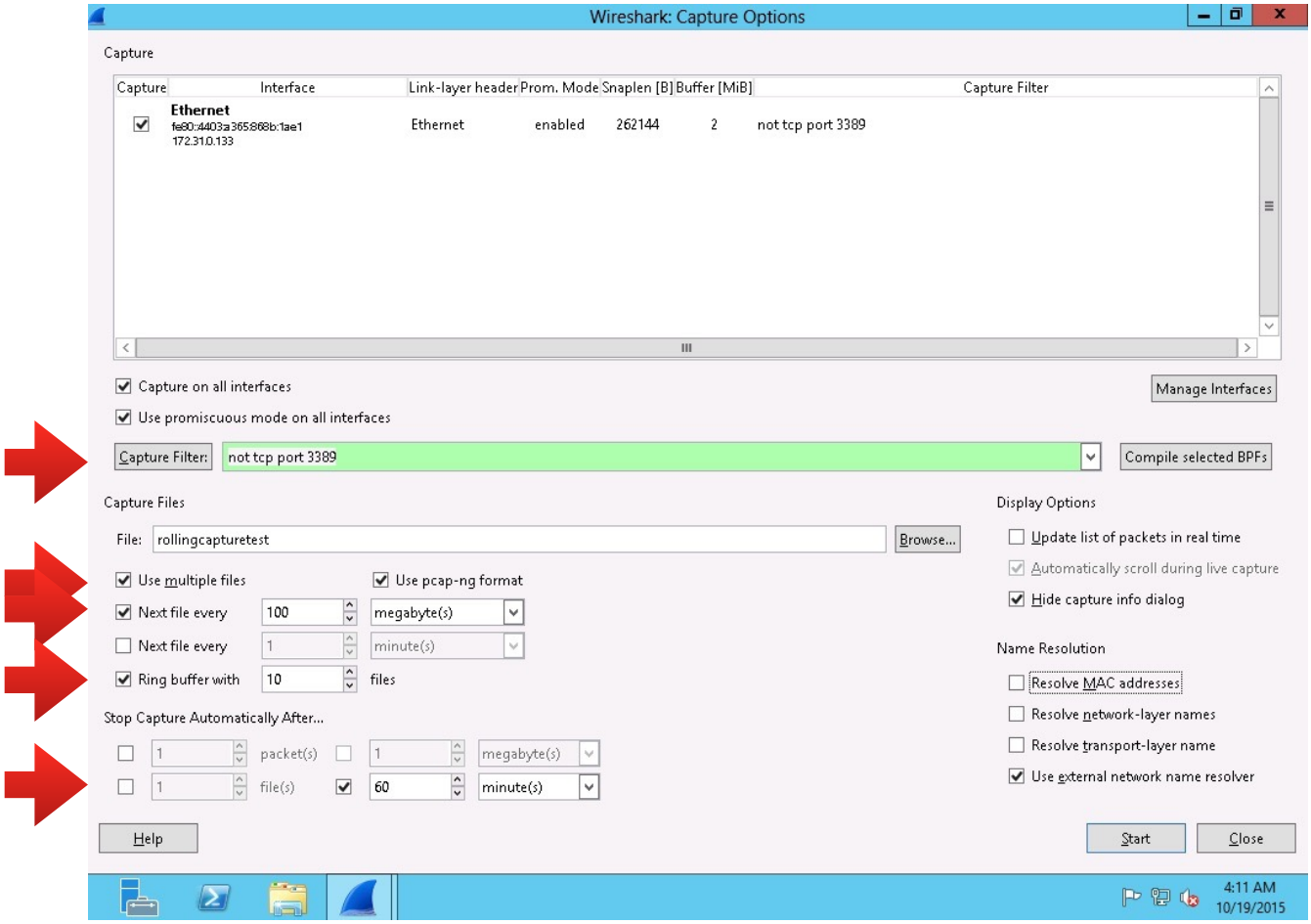
Wireshark 2.x on Mac OS X



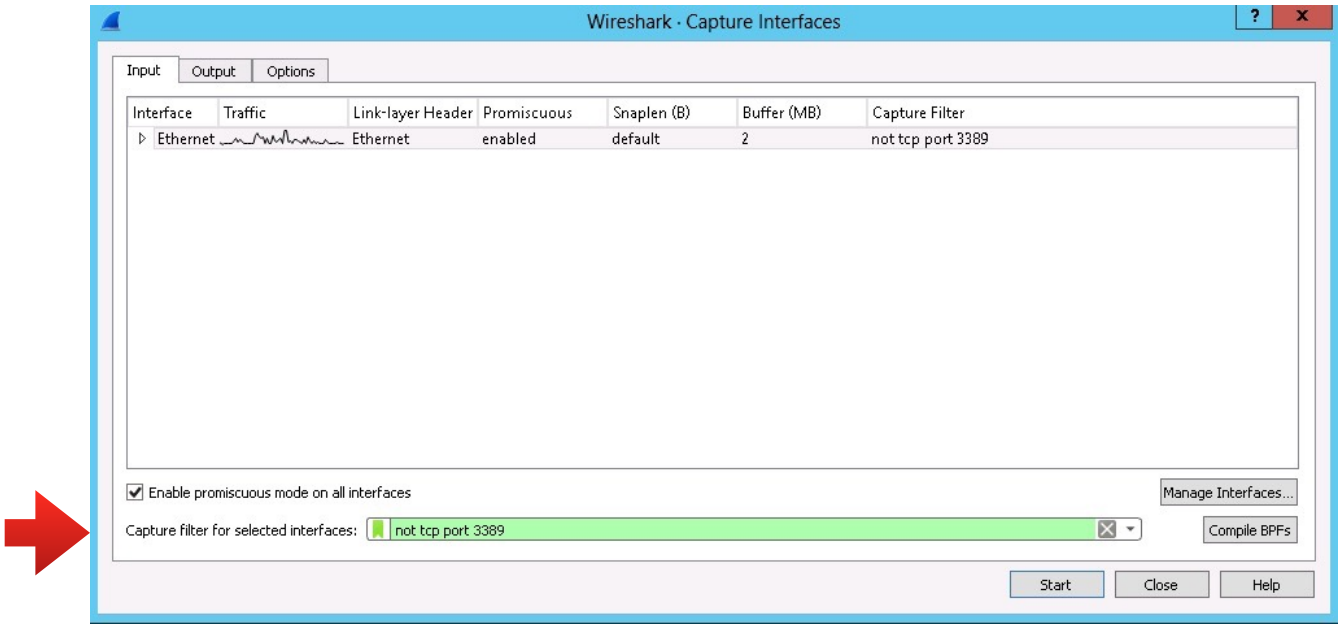


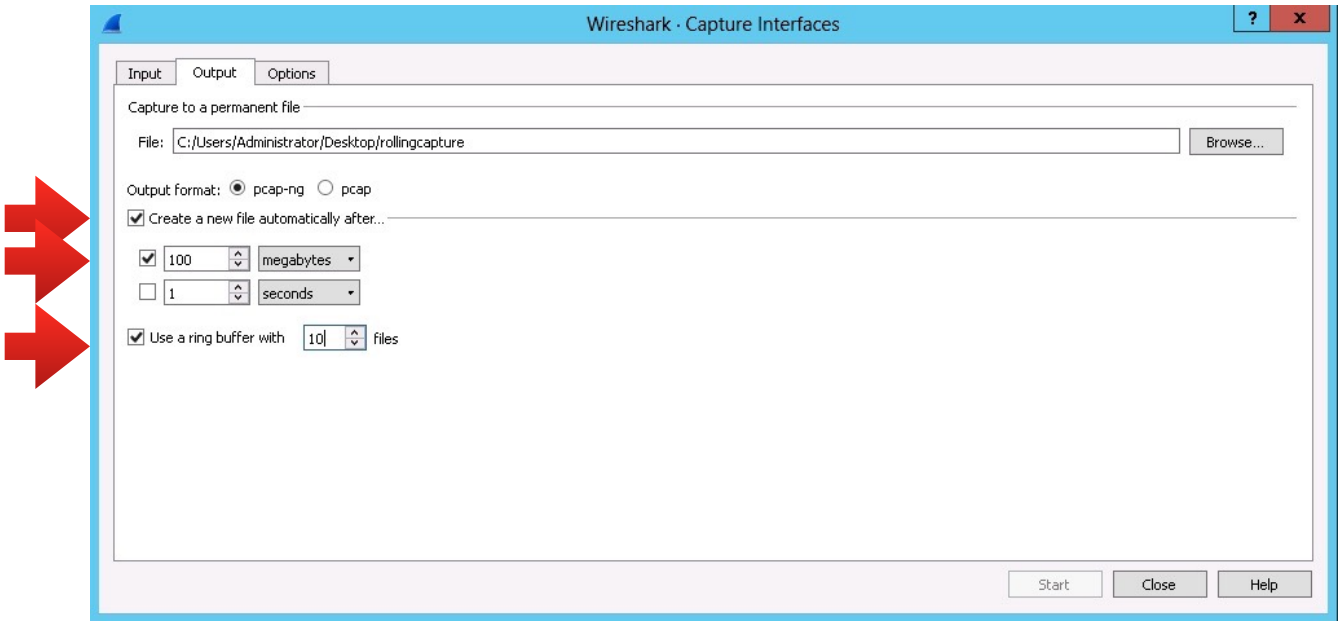


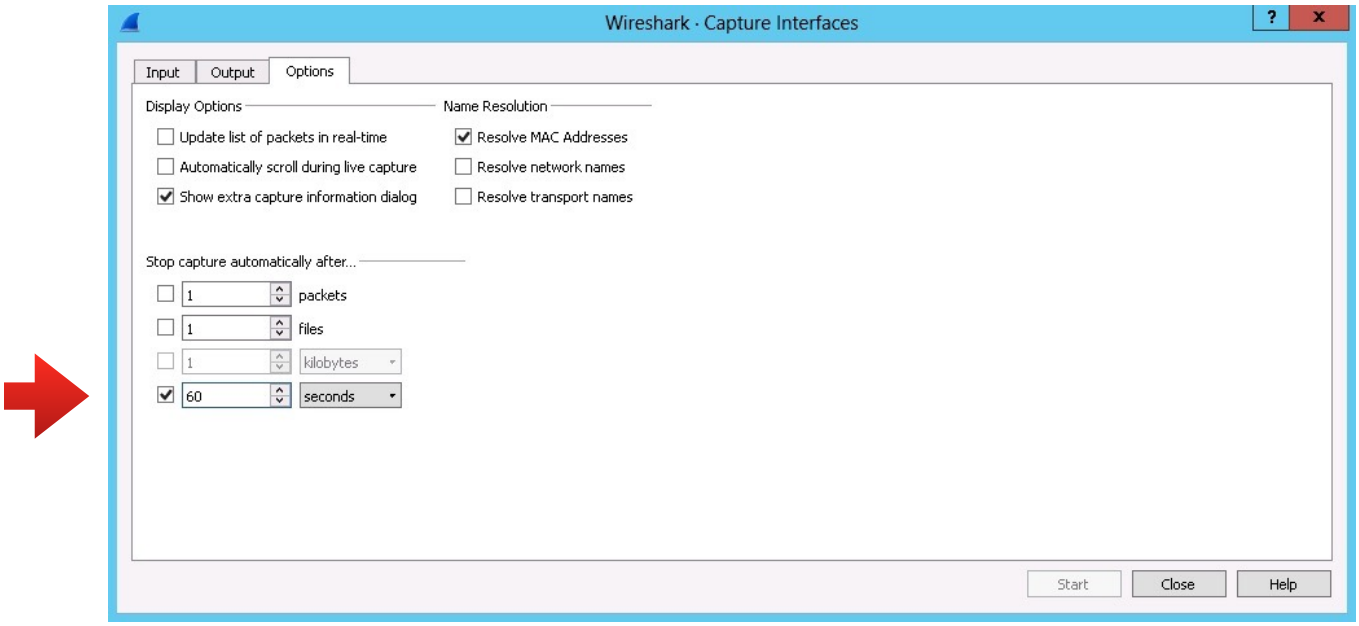
Wireshark 1.x on Windows 2012



Wireshark 2.x on Windows 2012







You'll notice the capture dialogues on Windows and Mac are almost identical. The options in 1.x and 2.x are also almost identical but spread across multiple tabs. In both cases, you'll want to check "Use multiple files." Set "Next file every" to the size of each file e.g. 100 MB. Set "Ring buffer with" to an appropriate number of files for the amount of free disk space.

If you set "Next file every" to 100MB and "Ring buffer with" to 10 files, you'll use a total of 1GB of disk space.

Wireshark also has the option of automatically stopping the capture after a certain number of packets, bytes, number of files, or time. In this example it is set to stop after 60 minutes.

Notice that in the Windows example, I'm using an example of an exclusive capture filter: `not tcp port 3389`. Since I'm using remote desktop to connect to this server, I do not want to capture remote desktop traffic.

Dumpcap on Windows

Dumpcap uses less resources than Wireshark and is preferable for long running rolling 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 -b filesize:100000 -b
files:10 -a duration:3600 -w rollingcapture.pcap
Capturing on 'Ethernet'
File: rollingcapture_00001_20151019045131.pcap
```

The options used here match the same options used in the Wireshark interface above:

- `-b filesize:100000` is 100MB file size
- `-b files:10` is a ring buffer with 10 files
- `-a duration:3600` is automatically stopping at 60 minutes (3600 seconds)

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

tcpdump Rolling Captures

tcpdump is another good low resource alternative to Wireshark. It has a different set of options but the same approach.

```
$ tcpdump -ni eth0 -C 100 -W 10 -w rollingcapture.pcap
```

- `-C 100` is 100MB file size
- `-W 10` is a ring buffer of 10 files

This will rotate through 10 files of 100MB each until you stop the capture manually. tcpdump can also save files based on capture time with the `-G sec` option, but you can't combine both file size and capture time to stop after a time period like you can with dumpcap.

References:

- dumpcap reference
- tcpdump reference
- dumpcap tutorial
- tcpdump examples