2.7. Reduce the Amount of Traffic You have to Work With

Rather than prepare for a week of sifting through packets, consider reducing the work load significantly by capturing at the proper location and filtering during the capture process.

If you must capture traffic inside the enterprise or on a server that is very busy, you may find that Wireshark cannot keep up with the traffic rate.

Detect When Wireshark Can't Keep Up

Wireshark launches *Dumpcap.exe* to capture traffic. Wireshark pulls the traffic from Dumpcap. If Dumpcap cannot keep up with the traffic during a capture process (most likely because Wireshark is not pulling the traffic from Dumpcap fast enough), the phrase "Dropped: x" will appear on Wireshark's Status Bar in the center column.

Most likely, your trace file will contain numerous *ACKed Lost Segment* indications. You cannot work with a faulty trace file. Your assumptions and analysis would be as incomplete as the data from which you worked. Such a trace file is unusable.

This is a perfect time to apply capture filters.[27] Figure 54 shows that capture filters are applied before the packets are sent to the capture engine. By applying capture filters at this point, you have a better chance of avoiding dropped packets.

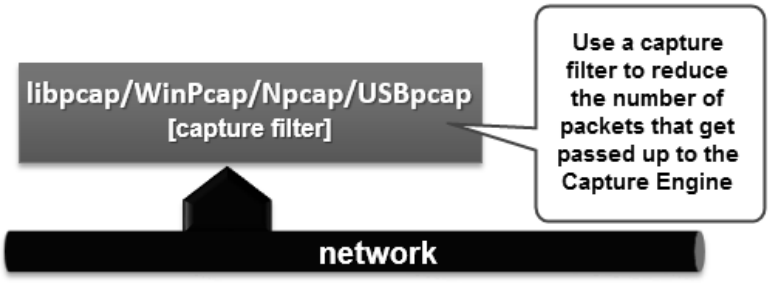

Figure 54. Capture filters reduce the load on the Capture Engine.

[27] I generally tell folks to avoid capture filters whenever possible. This is because you can't get those packets back after you filter them out. An ideal time to use capture filters is when Dumpcap can't keep up with the traffic. So let's lighten up the load heading to the Capture Engine.