8.3. Capture Traffic at Command Line

Use *dumpcap.exe* or *tshark.exe* to capture traffic at the command line when Wireshark can't keep up with the traffic (drops appear on the Status Bar), or you are deploying a streamlined remote capture host, or you are scripting an unattended capture.

Dumpcap or Tshark?

This is an interesting question. dumpcap is a capture tool only. When you run Tshark, it actually calls *dumpcap.exe* for capture functionality. Tshark contains extra post-capture parameters which makes it a better option for many situations. If you are really struggling with memory limitations, just use dumpcap directly. Otherwise, Tshark is the answer.

You can run either tool at the command line to capture traffic to *.pcapng* files. Both tools are located in the Wireshark program file directory (see **Help | About Wireshark | Folders | Program** to locate this directory). Both can use capture filters and various other capture settings.

To use dumpcap or Tshark from any directory, add the Wireshark program directory to your path[55]. Open the command prompt/terminal window and navigate to the folder where you want to save trace files. Run both tools from this directory.

Capture at the Command Line with Dumpcap

Type **`dumpcap -h`** to view dumpcap parameters.

Type **`dumpcap -D`** to view your available interfaces, as shown in Figure 129. Use the number preceding the interface name when you capture. In the image below, we can use **1**, **2**, **3**, or **4** to select an interface for capture.

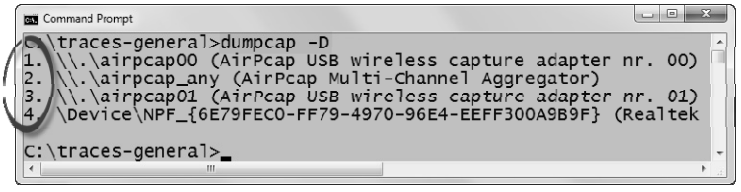

*Figure 129. Use **`dumpcap -D`** to view available interfaces.*

Use the `-c` option to stop capturing after a certain number of packets have been captured. For example, `dumpcap -c 2000 -w smallcap.pcapng` will automatically stop the capture after 2,000 packets have been captured to a file called *smallcap.pcapng*.

Use the `-a` option with `duration:`*n* (seconds) or `filesize:`*n* (KB) to stop capturing after a certain number of seconds have elapsed or until your trace file has reached a certain size. For example, in Figure 130 we typed `dumpcap -i1 -a filesize:1000 -w 1000kb.pcapng` to automatically stop the capture as soon as the file size reaches 1000 KB.

---

55 We keep mentioning this—have you done it yet?