

Table Of Contents

Table Of Contents	1
-------------------------	---

[Home](#) > [Faq](#) > [Apache](#)

Monitor or sniff Apache http packets

Posted by [Vivek Gite](#) <vivek@nixcraft.com>

Q. For my academic project I would like to monitor and analyze data transferred via HTTP. How do I monitor HTTP Packets?

A. The easiest way is to use **tcpdump** program/command, which dumps traffic on a network. Tcpdump prints out the headers of packets on a network interface that match the given criteria such as monitor port 80 for http.

It can also be run with the **-w** flag, which causes it to save the packet data to a file for later analysis, and/or with the **-r** flag, which causes it to read from a saved packet file rather than to read packets from a network interface.

Type the following command at shell prompt:

```
# tcpdump -n -i eth0 -s 0 -w output.txt src or dst port 80
```

Where,

- **-n** : Don't convert addresses (i.e., host addresses, port numbers, etc.) to names.
- **-i eth0** : Specify interface to capture data.
- **-s 0** : Snarf snaplen bytes of data from each packet rather than the default of 68. Setting to 0 means use the required length to catch whole packets.
- **-w output.txt** : Save data to output.txt file
- **src or dst port 80** : Capture port 80.

Now open a browser and run your site and do other stuff. When finished stop tcpdump and open output.txt file for analyze data.

4000+ howtos and counting! Want to read more Linux / UNIX howtos, tips and tricks? Subscribe to our [daily email](#) newsletter or [weekly newsletter](#) to make sure you don't miss a single tip/tricks. Alternatively, subscribe via [RSS/XML](#) feed.

Article printed from Frequently Asked Questions About Linux / UNIX: <http://www.cyberciti.biz/faq/>

URL to article: <http://www.cyberciti.biz/faq/howto-monitor-sniff-apache-http-packets/>
