

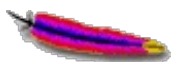
Table Of Contents


Table Of Contents 1

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

Monitor HTTP Packets (packet sniffing)

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

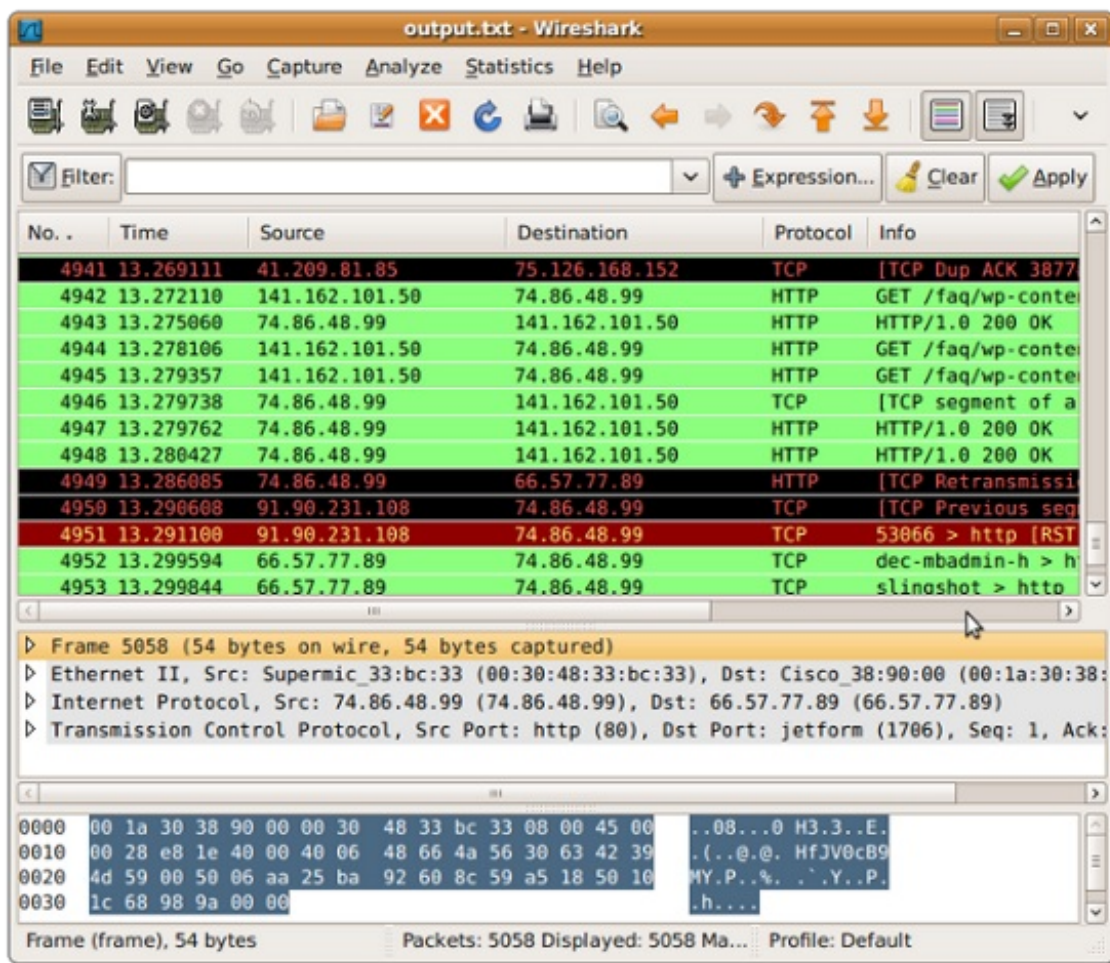
How do I monitor and analyze data transferred via HTTP (apache or lighttpd or nginx webserver) for debugging and security purposes?  [1]

You can use old good tcpdump program to monitor port 80 (http port) traffic and packets. This can be done over console or remote session via ssh login. If possible, eliminate accesses to the web server other than a test client. Make sure you use port 80 (not port 443 / https) i.e. the connection must be unencrypted so that the data can be analyzed. Also, note that usernames and passwords are logged in plain text.  [2]

Login as a root and type the following command at console:

```
# tcpdump -n -i {INTERFACE} -s 0 -w {OUTPUT.FILE.NAME} src or dst port 80
# tcpdump -n -i eth1 -s 0 -w output.txt src or dst port 80
```

Feel free to modify the interface eth1 and file name output.txt according to your setup. Now, you start a web browser and generate traffic. To stop tcpdump press CTRL+C. To examine the finished file output.txt use any text editor. I strongly suggest you import the file (output.txt) into the ethereal program (update: ethereal is renamed as wireshark) where, by right-clicking, it can be displayed in TCP packets ("Follow TCP Stream") in a reader-friendly form.



[3]

Fig.01 - Wireshark in action: Displaying output.txt tcpdump file

[See wireshark documentation](#) [4] for further details.

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/linux-unix-bsd-apache-tcpdump-http-packets-sniffing/>

URLs in this post:

[1] Image: <http://www.cyberciti.biz/faq/category/apache/>

[2] Image: <http://www.cyberciti.biz/faq/category/nginx/>

[3] Image: <http://www.cyberciti.biz/faq/linux-unix-bsd-apache-tcpdump-http-packets-sniffing/wireshark-output/>

[4] See wireshark documentation: http://www.wireshark.org/docs/wsug_html_chunked/index.html

Copyright © 2006-2010 [nixCraft](#). All rights reserved. This print / pdf version is for personal non-commercial use only. More details <http://www.cyberciti.biz/tips/copyright>.