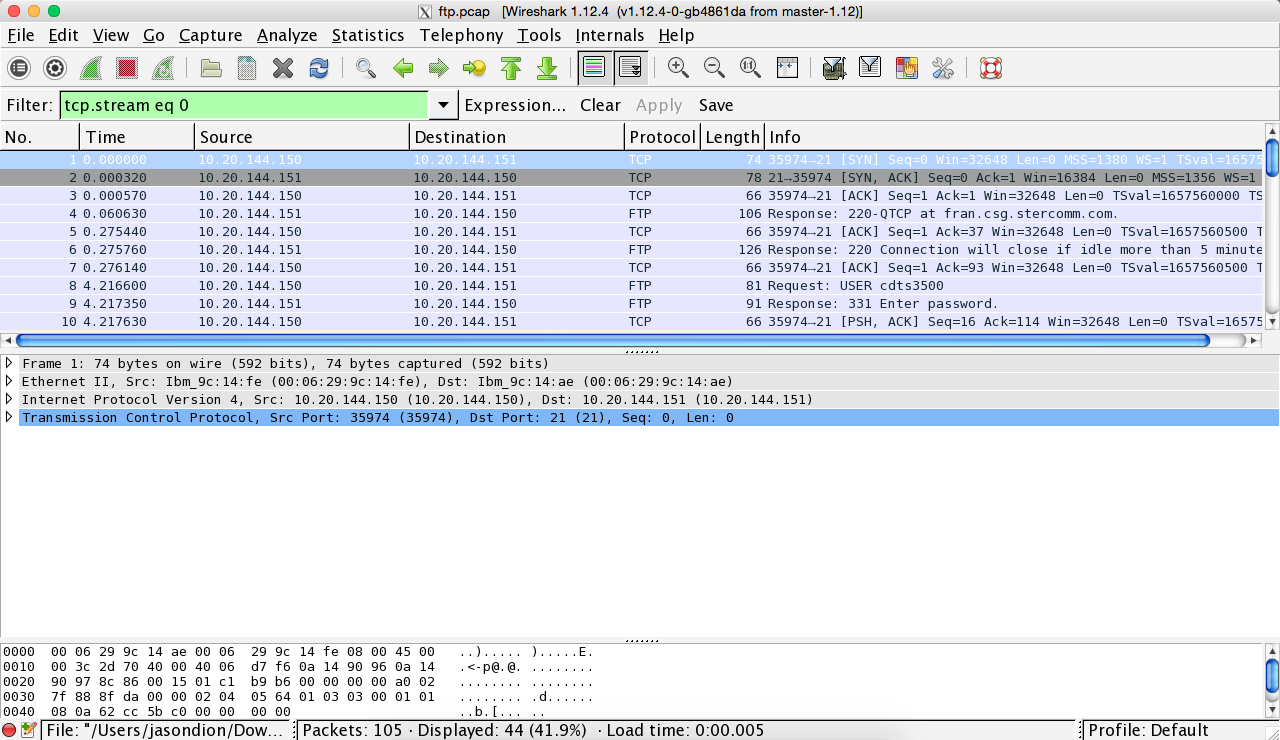
Reviewing Packet Captures

Reviewing Packet Captures

The best way to learn about any new piece of software is to try it out! To ensure everyone has the same content to analyze, we will use "pre-captured" traffic instead of capturing our own. Wireshark has the ability to capture live network traffic for analysis, or to open a packet capture (.PCAP) file.

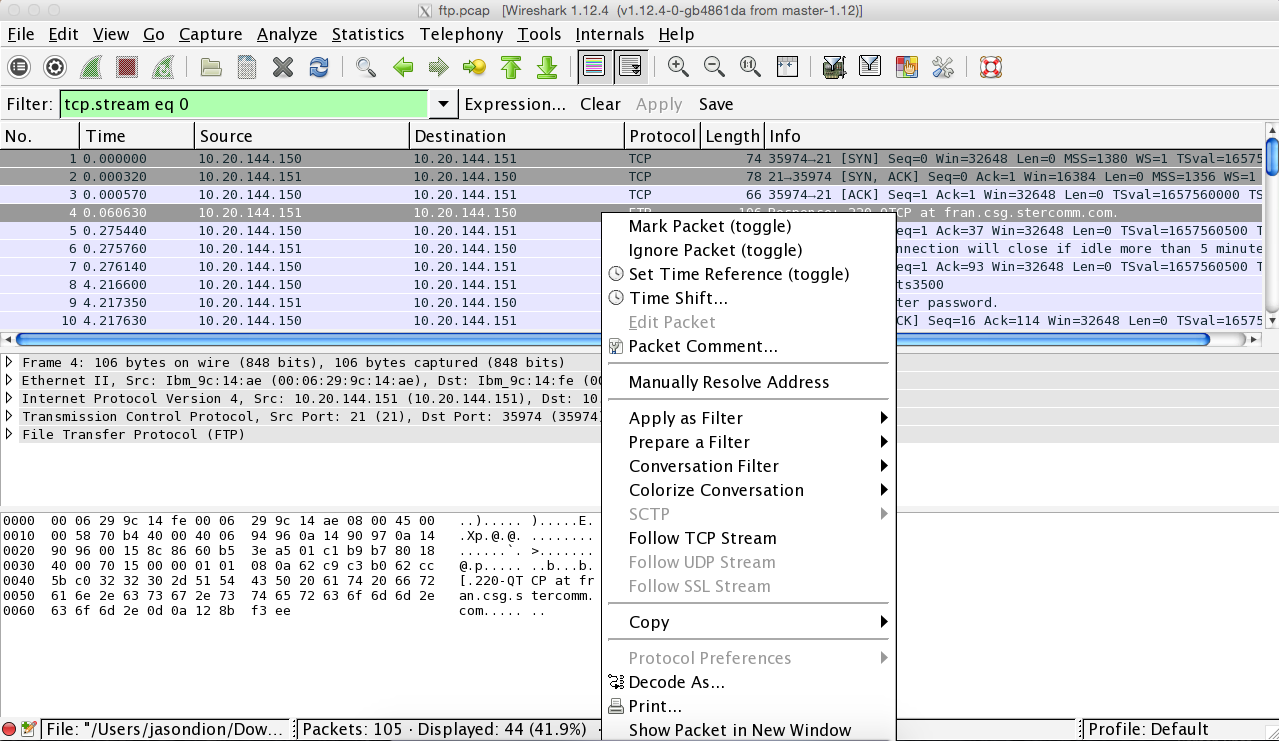
1) Download the following packet capture file: [FTP.pcap](https://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=get&target=FTPv6-1.cap)

2) From the Wireshark menu, click FILE, the OPEN. Select FTP.pcap, and open the file. Your screen should look similar to this:



3) In the middle pane, we can see the various layers of the OSI Reference Model, and the data contained for each packet of information captured at each layer. As we look to the bottom pane, we see the hexadecimal representation of the 1's and 0's that made up the packet, and the right hand of the bottom pane shows the UTF-8 representation of the data.

4) Right-click on one of the FTP protocols listed in the top pane.



5) Next, click Follow TCP Stream, and all the information related to that particular FTP session will appear, such as below:

