Although coloring rules are not actual fields in a packet, you can still filter on them. Right click on either the coloring rule name or the coloring rule string to create a display filter based on these two elements.

> **Coloring Rules are Processed in Order Top to Bottom**
>
> *Coloring rules are processed in order so you need to be careful when you create and rearrange coloring rules. For example, using the default coloring rules, an HTTP packet that contains a TCP retransmission will be processed by the Bad TCP coloring rule, not the HTTP rule because the Bad TCP coloring rule is listed above the HTTP coloring rule.*

Create a "Butt Ugly" Coloring Rule for HTTP Errors

Although Wireshark contains a number of default coloring rules, there are some packets that should be screaming at you to get your attention. HTTP errors would be a good example. Any HTTP response that contains a numerical code between 400 and 499 indicates a client error. HTTP responses between 500 and 599 indicates server errors.

Let's go step-by-step to create a single coloring rule to call attention to HTTP error responses. Refer to Figure 106 to see the steps as you work through this process.

Step 1: Open ***http-espn2011.pcapng*** (available in the Download section of *www.wiresharkbook.com*)

Step 2: In the Packet List pane select Packet 9 (an HTTP response). In the Packet Details pane right click on the **Hypertext Transfer Protocol** line and choose **Expand subtrees** so you can see the "Status Code: 301" line.

Step 3: Ⓐ Right click on "**Status Code: 301**" and select **Colorize with Filter | New Coloring Rule**. Wireshark opens the Coloring Rules window and Edit Color Filter window. In addition, your coloring rule string is filled out based on the field you selected in this step.

Step 4: Ⓑ Enter **`T-HTTP Errors`** in the name field. Enter **`http.response.code > 399`** in the string field.

Step 5: Ⓒ Click the **Background Color** button. In the Color name field, type in **orange** and click **OK**. Click **OK** to close the Edit Color Filter window and **OK** to close the Coloring Rules window.

Step 6: Ⓓ Your coloring rule will be highlighted with a blue background. Click the **Up** or **Down** button to move your butt-ugly coloring rule to the top of the coloring rules list.[61]

Step 7: Open *http-500error.pcapng*. If your "butt ugly" coloring rule is configured properly, packet 9 should match the rule.

[61] As of Wireshark 1.8 your new coloring rules are placed at the top of the list by default. This is a welcome change!