Filter on TCP Expert Information Elements

Apply a display filter for **`tcp.analysis.flags`** to show packets that match the Expert Info Notes and Warnings triggers.

Figure 178 shows the result of applying a `tcp.analysis.flags` display filter to an entire trace file. This is a fast method to detect TCP-based problems in a trace file.

Use a `tcp.analysis.flags` Filter Expression Button

*Consider creating and saving this display filter as a filter expression button called **Bad TCP**. To be most accurate, add `&& !tcp.analysis.window_update` to the filter. When you open trace files, click your new Bad TCP Filter Expression button to locate the most common TCP-related network problems.Expert Infos window*

You can create a display filter to examine packets that meet a specific Expert Info severity level. The following provides examples of the four severity level filters ("Details" and "Packet Comments" are not considered a severity levels):

```
expert.severity==error
expert.severity==warn
expert.severity==note
expert.severity==chat
```

Another display filter is available for packets that are part of a specific Expert Info group. The syntax is `expert.group==<group>`. Some of the Wireshark Expert Info groups are:

- Checksum—a checksum was invalid
- Sequence—sequence number was not correct or indicated a retransmission
- Malformed—malformed packet or dissector bug
- Protocol—invalid field value (possible violation of specification)

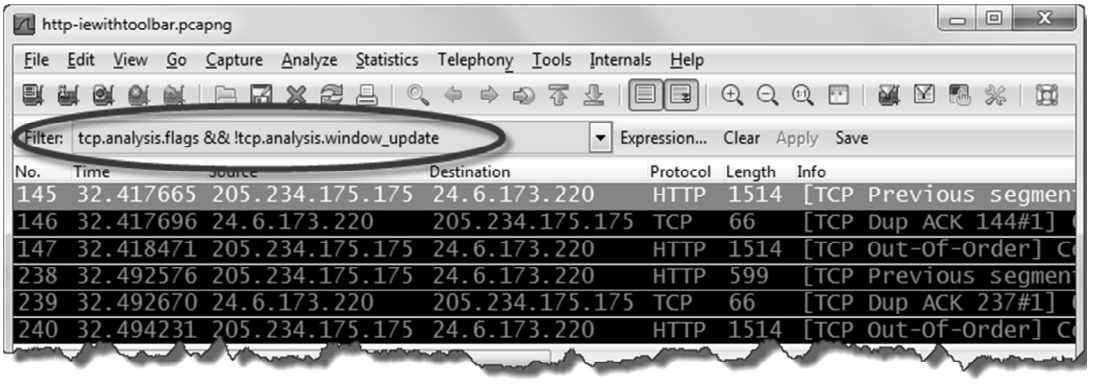

Figure 178. A display filter shows TCP problems [http-iewithtoolbar.pcapng]