CS 4431

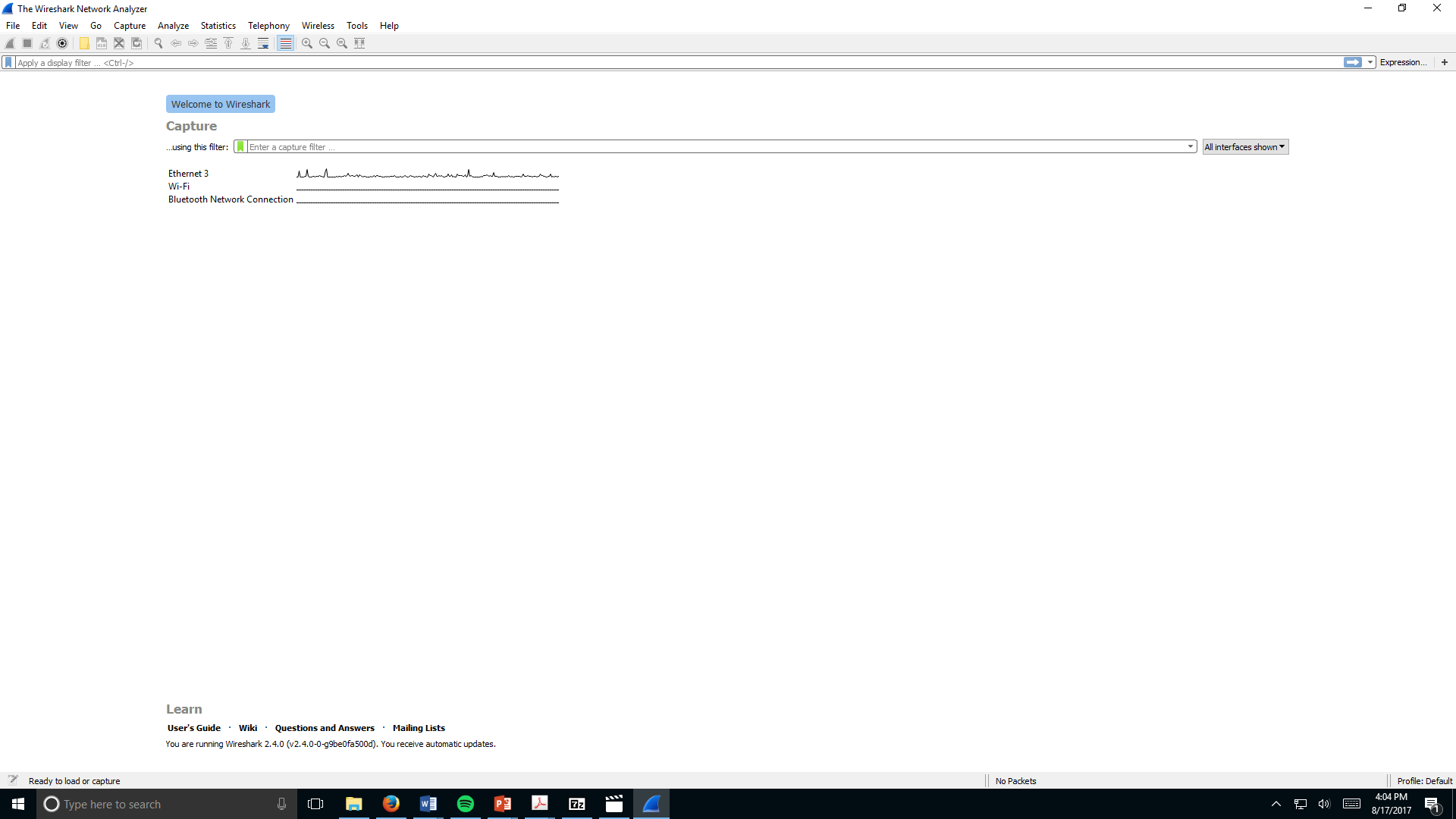
Fall 2017

Using Wireshark

You should download a copy of wireshark at Wireshark website at https://www.wireshark.org/download.html.

Getting started

Once you have downloaded Wireshark, launch it:

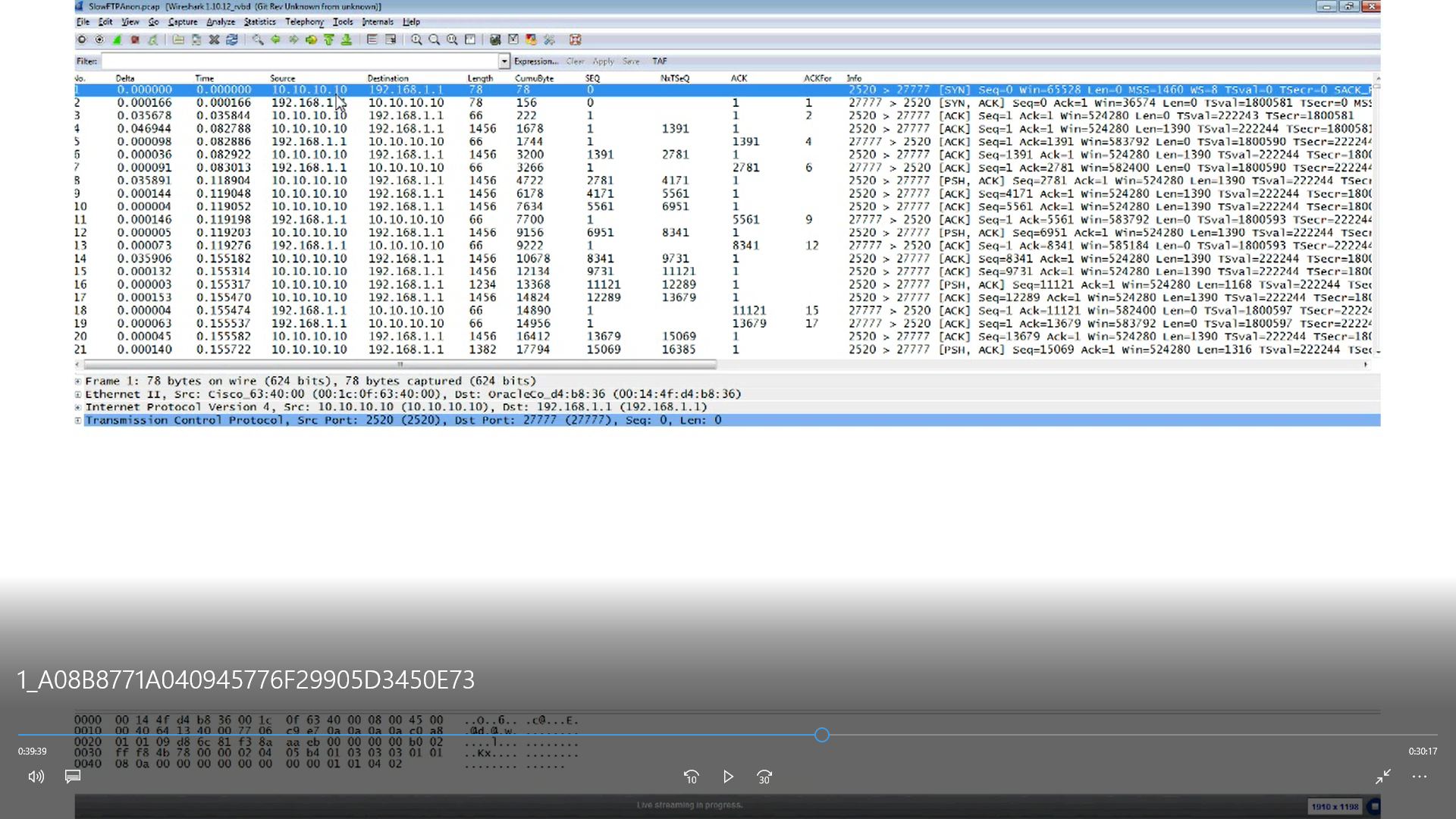


What do the menu bar items mean and how do I get to a form like this?



The columns can be created/edited under Edit then Preferences. The default is as shown.

What can you see in this presentation? Let’s look at a sample



**What HTTP client is your Browser running?**

Capture while you browse the internet, and find any GET request your browser does (which means "hello, I want something"). If you have many packets that make it hard to see such requests you can find them by filtering on "http.request.method==GET".

In the packet list you'll see that the info column says "GET / HTTP/1.1" or "GET / HTTP/1.0".