

# Why are we interested in HTTP?

The Facebook logo, consisting of the word "facebook" in white lowercase letters on a blue rectangular background.The Yahoo! logo, featuring the word "YAHOO!" in red uppercase letters with a red exclamation point, set against a white background.The Twitter logo, with the word "twitter" in a light blue, lowercase, rounded font with a white outline.The Myspace.com logo, featuring a blue square with a white icon of three people and the text "myspace.com" in white, with the tagline "a place for friends" in smaller white text below.

Because nearly everything a typical user does on the Internet uses HTTP

The CNN.com logo, with "CNN" in red and "com" in white, both in a bold, sans-serif font, set against a black background.The Google Earth logo, with "Google" in its multi-colored font and "Earth" in green below it, set against a white background.The @mail.ru logo, with "@mail.ru" in white lowercase letters on a blue rectangular background.The Wikipedia logo, featuring a globe made of puzzle pieces with various characters on them, above the text "WIKIPEDIA" and "The Free Encyclopedia" in a serif font.The Gmail logo, with "Gmail" in its multi-colored font, "by Google" in smaller text below, and "BETA" in a small box to the right, set against a white background.

# Why are we interested in HTTP?

- Almost all web-browsing uses HTTP:
  - Internet surfing
  - Webmail (Yahoo/Hotmail/Gmail/etc.)
  - OSN (Facebook/MySpace/etc.)
  - Internet Searching (Google/Bing/etc.)
  - Online Mapping (Google Maps/Mapquest/etc.)

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

# XKS HTTP Activity Search

Another common query is analysts who want to see all traffic from a given IP address (or IP addresses) to a specific website.

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

# XKS HTTP Activity Search

- For example let's say we want to see all traffic from IP Address 1.2.3.4 to the website [www.website.com](http://www.website.com)
- While we can just put the IP address and the "host" into the search form, remember what we saw before about the various host names for a given website

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL