...But First: Helpful tools

- `ifconfig` – See your host’s network interfaces
- `dig`, `whois` – Lookup ip by host
- `ipcalc -h`, `nslookup` – Lookup host by ip
HTTP Wireshark Example
“Transport Layer Security” protocol
Standard protocol for encrypting Internet traffic
Previously known as SSL (Secure Sockets Layer), which has been around since 1994
TLS is a slightly modified version of SSL version 3
Used for HTTPS (HTTP Secure) traffic
Supported by nearly every web browser
SSL and TCP/IP

- SSL provides application programming interface (API) to applications
- C and Java SSL libraries/classes readily available
Purposes for TLS

- Provides encrypted TCP connection
- Data integrity
- End-point authentication
TLS and CONNECT

- HTTP CONNECT is used to establish a two-way connection “tunnel” between two parties
- After this, a “triple handshake” is performed over the tunnel
- After the handshake, the two parties can communicate securely
- We’ll take a closer look at this handshake
**Purpose**

1. server authentication
2. negotiation: agree on crypto algorithms
3. establish keys
4. client authentication (optional)
SSL record protocol

- **record header**: content type; version; length
- **MAC**: includes sequence number, MAC key $M_x$
- **fragment**: each SSL fragment $2^{14}$ bytes (~16 Kbytes)
HTTPS Wireshark Example