# HTTPS

HTTP是明文传输的，也就意味着，介于发送端、接收端中间的任意节点都可以知道你们传输的内容是什么。这些节点可能是路由器、代理等。

密码学中的“密码”术语与网站登录时用的密码（password）是不一样的概念，password 翻译过来其实是“口令”，它是用于认证用途的一组文本字符串。而密码学中的密码（cipher）是一套算法(algorithm)，这套算法用于对消息进行加密和解密，从明文到密文的过程称之为加密，密文反过来生成明文称之为解密，加密算法与解密算法合在一起称为**密码算法**。有关密码和认证机构等相关知识，请参见密码和加密-《HTTPS 为什么更安全，先看这些》一文。

HTTPS其实就是**secure http**的意思，也就是HTTP的安全升级版。HTTP是应用层协议，位于HTTP协议之下是传输协议TCP。TCP负责传输，HTTP则定义了数据如何进行包装。HTTPS相对于HTTP其实就是在HTTP跟TCP中间加多了一层加密层**TLS/SSL**。

SSL是个加密套件，负责对HTTP的数据进行加密。TLS是SSL的升级版。现在提到HTTPS，加密套件基本指的是TLS。

具体的内容可以参见密码和加密-《HTTPS 科普扫盲帖》。

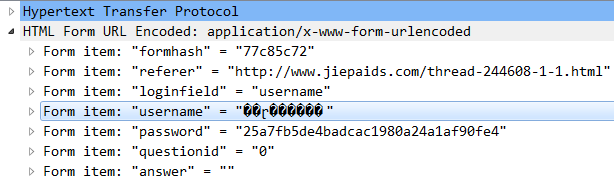
# 同源策略(跨域)

同源策略/SOP（Same origin policy）是一种约定，由Netscape公司1995年引入浏览器，它是浏览器最核心也最基本的安全功能，如果缺少了同源策略，浏览器很容易受到XSS、CSFR等攻击。所谓同源是指"协议+域名+端口"三者相同，即便两个不同的域名指向同一个ip地址，也非同源(只要三者不相同，其实都是跨域)。

## 抓包

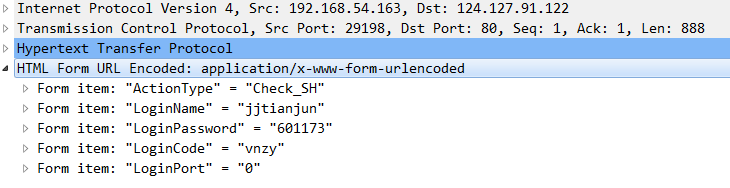
有时，有的网站并不是简单地就可以抓取，而是需要登录后才能操作，如何获取登录时需要的参数呢，这时我们就需要使用抓包工具来进行了。

抓包工具有很多，小到最常用的web调试工具firebug，还有fiddler，大到通用的强大的抓包工具wireshark。我们使用的是wireshark：



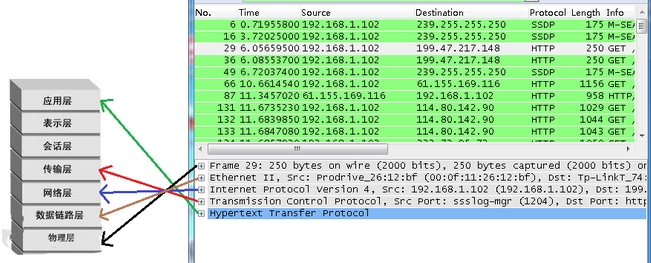
应该可以看出参数了。

我用基金的试了一下：



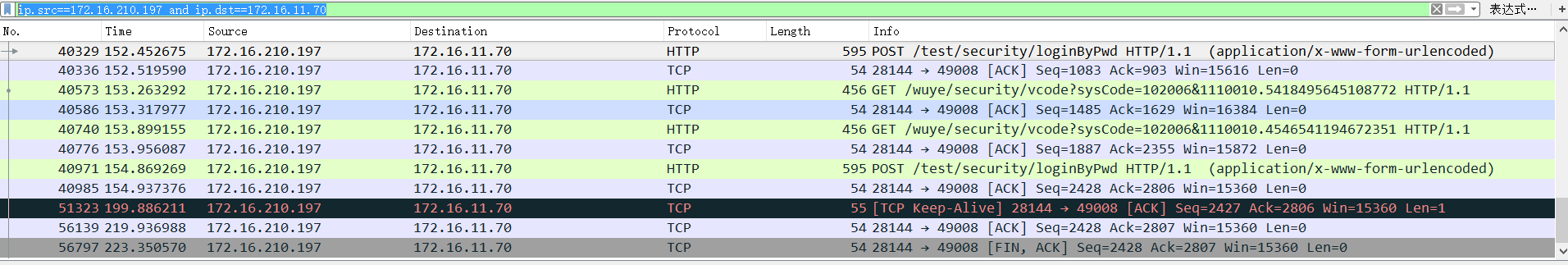
“帮助”-“wiki”：可以打开Wireshark wiki。

### Wireshark详细信息的层与对应OSI七层模型

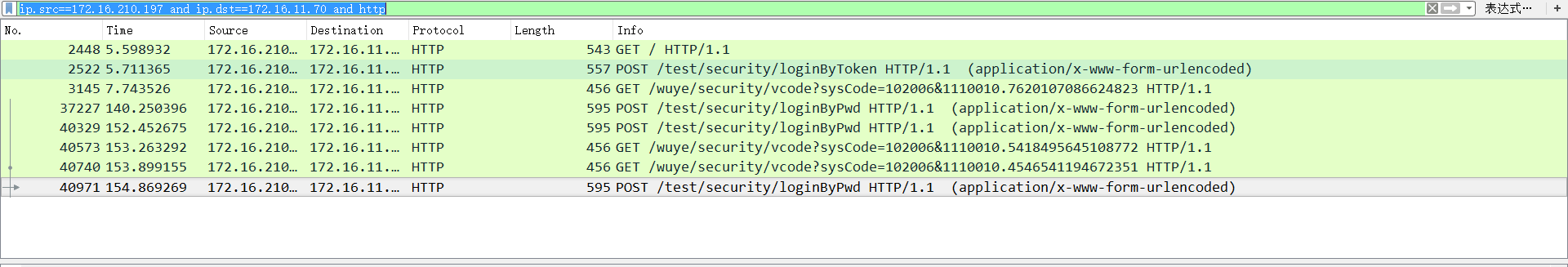


### 过滤器

ip.src==172.16.210.197 and ip.dst==172.16.11.70



ip.src==172.16.210.197 and ip.dst==172.16.11.70 and http



每次更换过滤规则要按一下右侧的箭头或回车。

http.host=="jj.chinapostdoctor.org.cn" and http

访问基金网。

