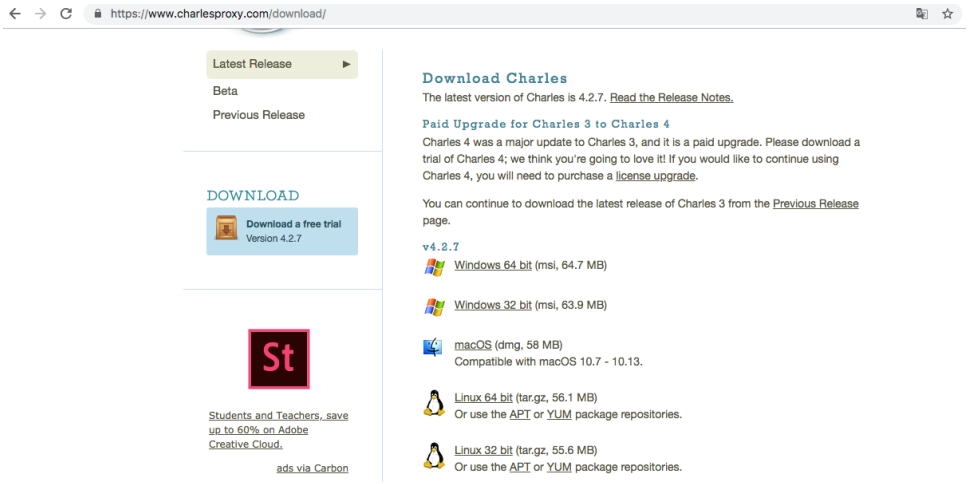
Charles抓包说明

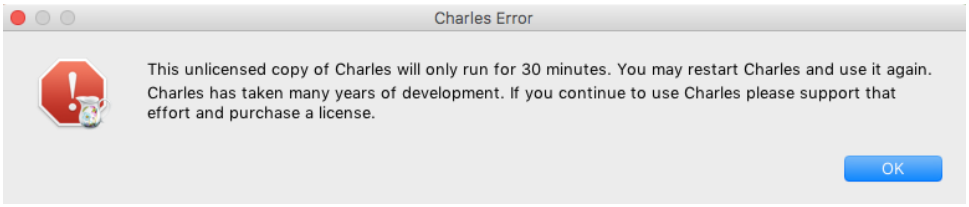
> 「官网说明」Charles is an HTTP proxy / HTTP monitor / Reverse Proxy that enables a developer to view all of the HTTP and SSL / HTTPS traffic between their machine and the Internet. This includes requests, responses and the HTTP headers (which contain the cookies and caching information).
>
> 「百度百科」Charles是一个HTTP代理服务器 / HTTP监视器 / 反转代理服务器，当浏览器连接Charles的代理访问互联网时，Charles可以监控浏览器发送和接收的所有数据。它允许一个开发者查看所有连接互联网的HTTP通信，这些包括request, response和HTTP headers。

1. 安装

下载地址: https://www.charlesproxy.com/download/



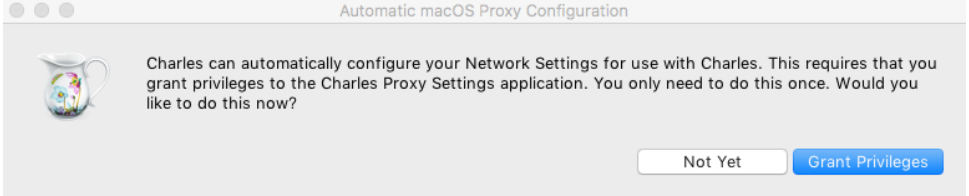
根据自己的电脑类型，选择合适的版本进行下载。需注意，免费版本每次只能使用30min，30min结束后Charles自动关闭，但可以重新打开继续使用，只是前30min的请求数据将不会保存。



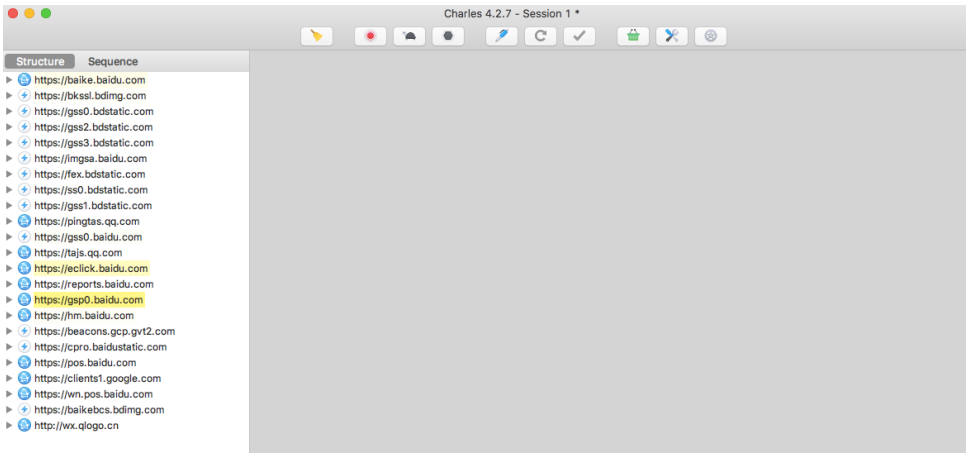
PS：Mac版本与Win版本相差无几，本文以Mac版本为例进行说明。

2. PC抓包配置

第一次打开Charles，可能弹出如下窗口。若出现，点击`Grant Privileges`：



默认情况下，Charles将自动监控PC端的请求和响应，即通过本机发出的请求和获得的响应均会出现在界面的左侧，如下图所示。可以通过菜单栏的「Proxy」→「MacOS proxy」关闭对本机的监控。



点击「红色圈圈」暂停监控，再次点击则恢复监控；点击「扫帚」清空左侧所有请求记录。

具体的配置步骤：

- 打开菜单栏的「Proxy」→「SSL Proxying Settings」→「Add」，`Host`输入`*`，`Port`输入`*`即可，保存；
- 在菜单栏选择「Help」→「SSL Proxying」→「Install Charles Root Certificate」，Mac将弹出「钥匙串访问」界面，并自动导入Charles Proxy CA证书（可能需要输开机密码）；
- 接着点击左下角「种类」中的「证书」，找到刚刚导入的Charles Proxy CA，双击，点击「信任」下拉菜单，将「加密套接字协议层(SSL)」设置为「始终信任(Always Trust)」；
- 关闭、输入密码后保存即可。

现在Charles可以抓取PC端的HTTP与HTTPS请求了。

3. Mobile抓包配置

- 确保Mac与手机处于同一局域网内(可以连接同一路由器，或者电脑创建热点让手机连接)；
- 打开Mac上的Charles，点击「Help」→「Local IP Address」，获取本地IP地址；
- 打开「Proxy」→「SSL Proxying Settings」，确认「HTTP Proxy」的「Port」，默认是8888；
- 打开手机，连接指定网络，并设置代理，即添加上一步获取的代理IP地址和端口号；

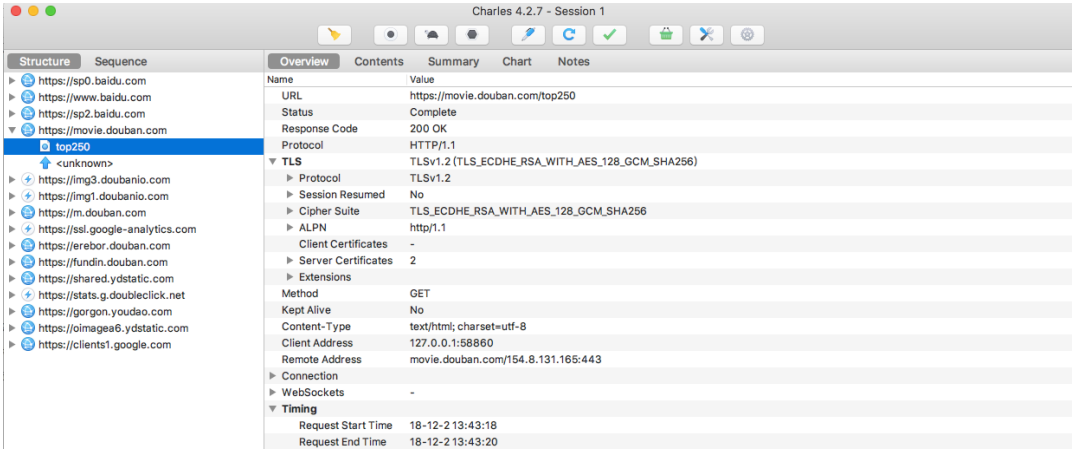
- 在手机上随意使用一次网络，Charles将会跳出「Connection from xxx」的窗口，点击「Allow」；
- HTTPS抓包需要继续配置：点击Charles菜单来「Help」→「SSL Proxying」→「Install Charles Root Certificate on a Mobile Device or a Remote Browser」，将弹出一个窗口；
- 根据窗口提示，用Safari浏览器访问http://chls.pro/ssl，Safari浏览器会自动下载证书并提示安装，根据提示进行安装，注意证书会被添加到手机的「设置」→「通用」→「描述文件」；
- 信任该证书：手机端，「设置」→「关于本机」→「证书信任设置」→「完全信任」；

至此Charles可以抓取PC端和Mobile端的HTTP与HTTPS请求了。

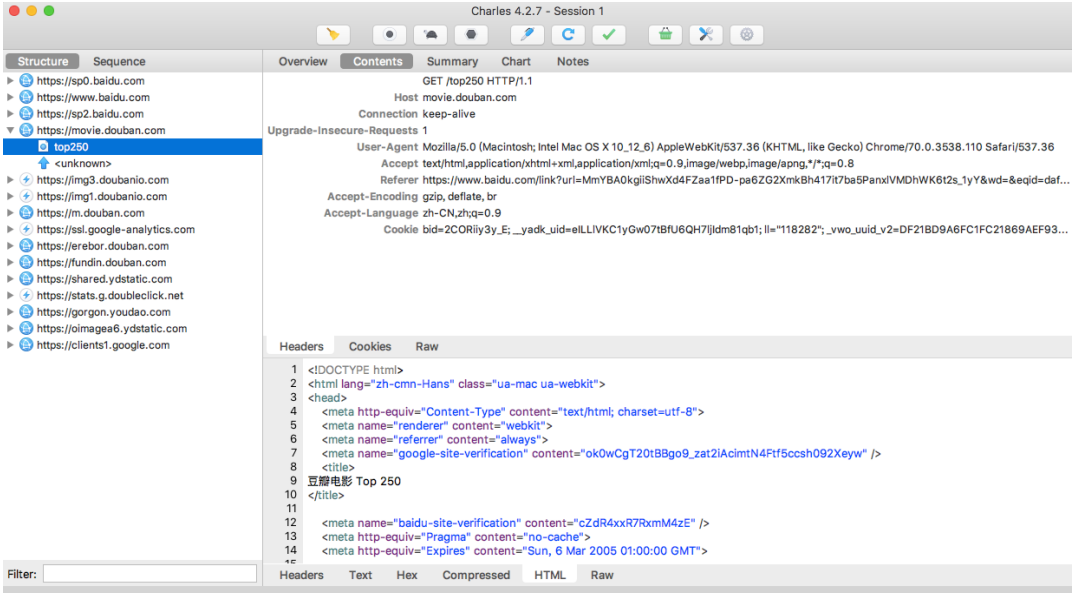
4. 简单使用

查看目标请求和响应的信息时，经常使用「Overview」和「Contents」两个模块。

「Overview」：请求的基本信息，包括请求的Url，响应状态信息和状态码等等。



「Contents」：请求报文和响应报文的具体内容。



By DraymondG