03_抓包工具的使用

==========

背景：

抓包：

主要抓取网络之间传输在应用层的用户数据。

价值：在软件测试中，特别是APP客户端（IOS与Android）和H5页面与后端服务之间进行HTTP通信的时候，

抓包这个操作应该是最常见的，这项技术的掌握可以说是测试人员的一门必修课，为什么这么说呢？

至少下面的三个因素是最重要的：

1. 通过抓包我们能清晰的知道前后端交互的数据细节。
2. 通过抓包我们对Http接口进行测试。
3. 当我们发现系统有bug的时候，可以通过抓包来鉴定问题是出现在客户端还是服务端。

通常业界的抓包工具也较多比如wireshark, charles, Fiddler等，但相对charles用得比较多，我们这个文档以charles来举例就好。

Charles 通过将自己设置成系统的网络访问代理服务器，使得所有的网络访问请求都通过它来完成，从而实现了网络封包的截取和分析。

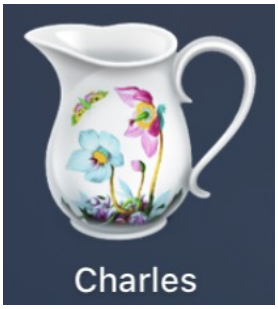
抓包工具charles的获取

由于互联网的研发工程师基本使用的是mac电脑，本教程以mac笔记本为例子来编写。

下载链接：https://www.charlesproxy.com/download/

打开上述的链接找到对应的操作系统版本即可，这里选择macOS,dmg版本，下载到本机直接安装即可。

下载完后在本机的桌面可以看到一个茶壶的图标，表明安装是成功的。



默认安装的版本是一个试用版，只有30天的试用期，当然破解是很简单的，各位网上随便搜搜就好。

==========

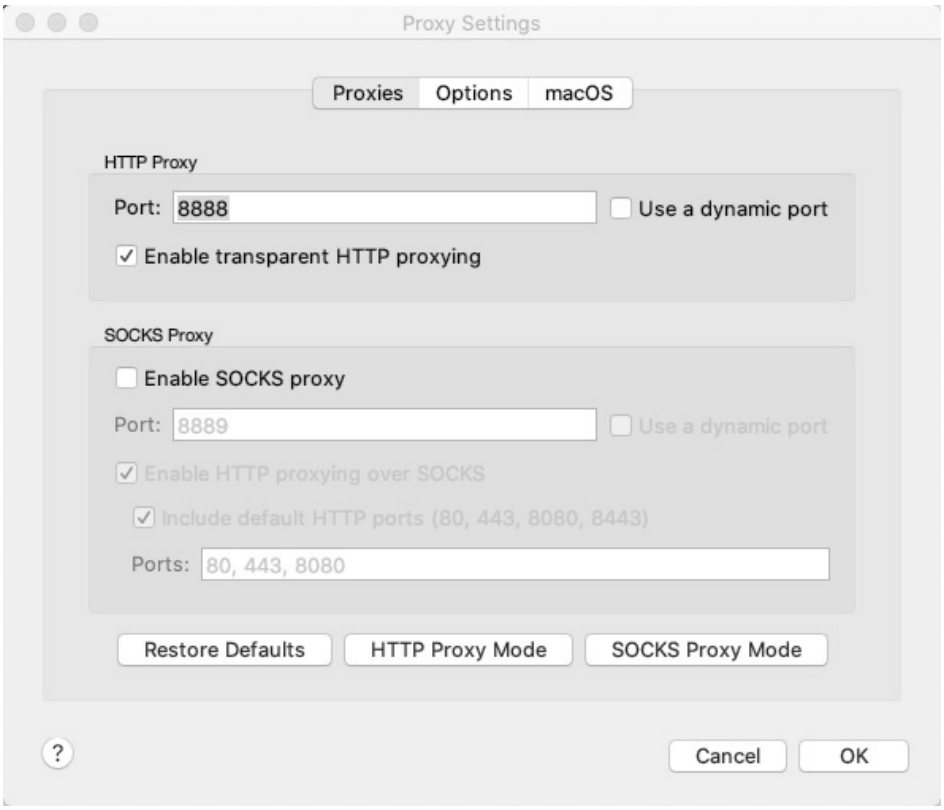
我是分隔区域

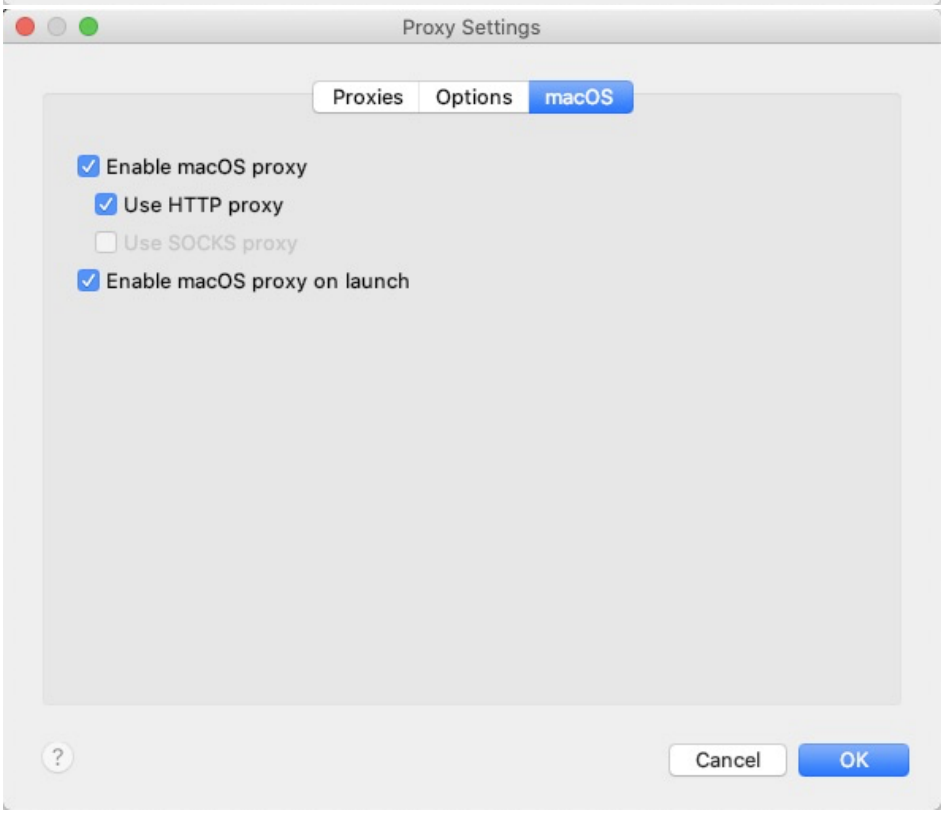
==========

Charles 的配置

- Step1: 在本机安装安装证书文件。 Help→SSL Proxying→ install Charles Root Certificate，按下面的截图全部信任。

- Step2: 配置代理：proxy→Proxy Settings, 按照下面的截图配置即可。



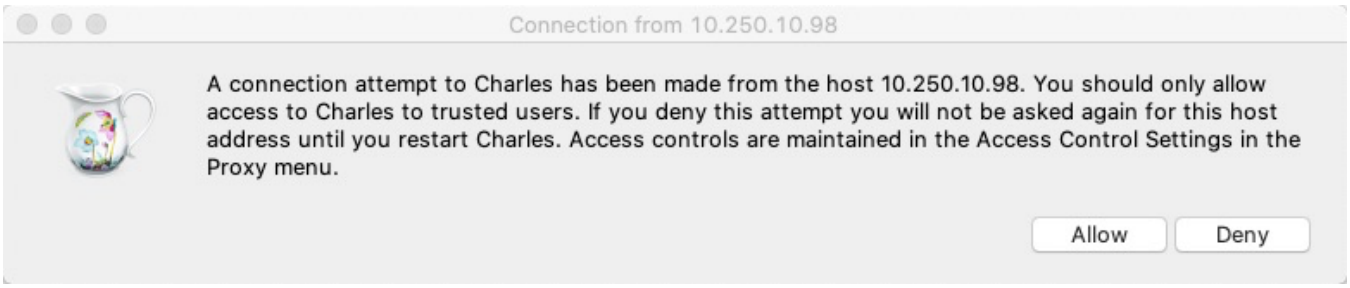


- Step3: 在手机端设置代理访问（前提：手机和笔记本mac连接的是同一个wifi热点）

以iPhone为例，安卓机型类推，先获得macbook的IP地址：charles Help → Local IP Address

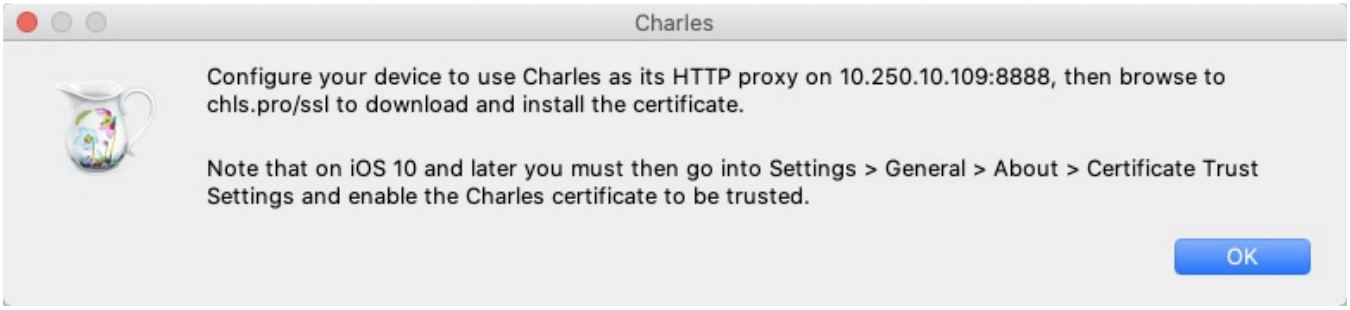
设置 → 无限局域网 → 点击wifi热点hipac-port 最右边的 感叹号小图标，进入一个新的页面往下拉，找到HTTP代理（配置代理）点击 → 点击“手动”

在下面的服务器一栏中输入MAC IP 地址，端口一栏中输入8888后点击右上角的存储退出。这时会在charles这边弹出一个框点击 “Allow”。



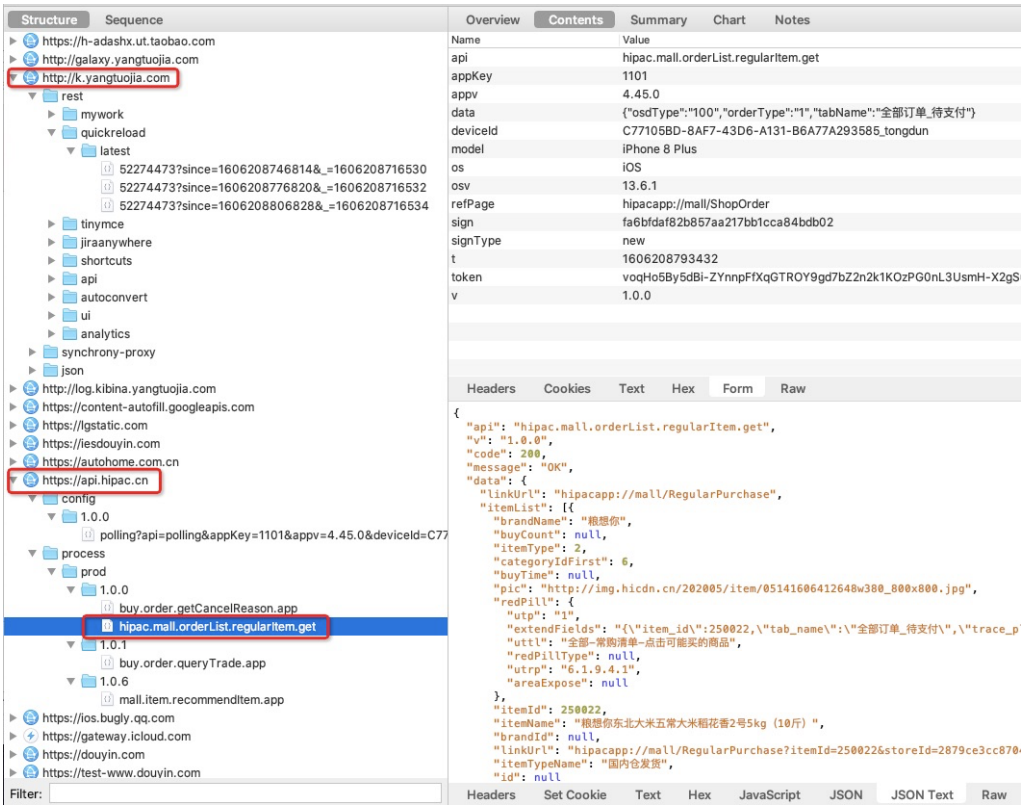
正常到这里手机上面操作就能在charles上抓到手机端发送的请求信息了，但是只能是http协议的，对于https协议需要在手机端再安装证书才能抓到。

- step4: charles 点击菜单 Help→SSL Proxying→ Install Charles Root Certicate on a Mobile Device or Remote Brower， 点击ok按钮。



- step5: 按照步骤4中的提示，在手机端打开一个浏览器输入 chls.pro/ssl, 这个时候会提示安装手机的证书，点击允许后在点击下载即可。
- step6: 打开iPhone 设置 → 通用 → 描述文件， 点击刚刚下载的证书（charles Proxy CA...），在新的页面点击右上角的安装。安装完成后会显示已验证。
- step7: 打开iPhone 设置 → 通用 → 关于本机 → 证书信任设置 开启证书的信任。

这时所有的设置结束，能正常的抓取http和https的数据包。



安卓机型类似的方式设置

==
====

我是分隔区域～～～～

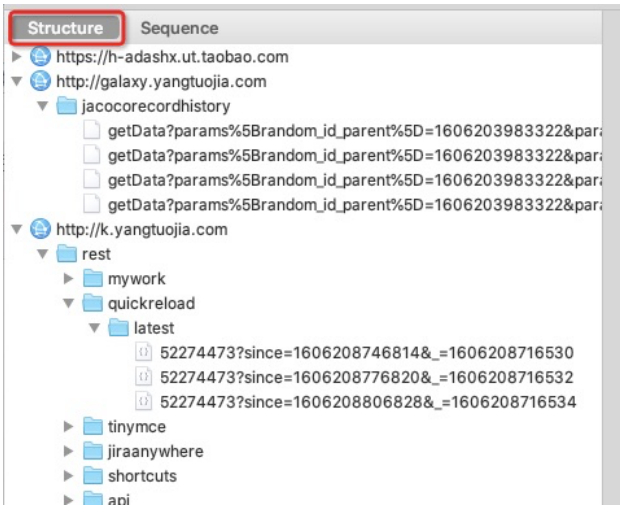
==
====

数据包怎么看？

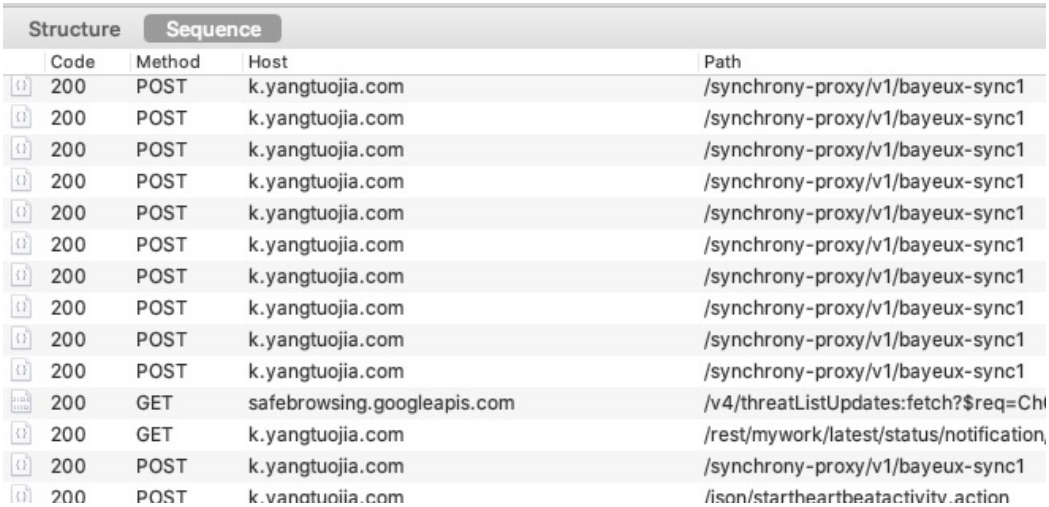
charles支持两个格式查看包数据

Structure：按照数据包的请求地址的结构分层次的展示，相同的请求会被放入同一个目录下面。

Sequence：按照时间线的维度展示请求信息，后发送的请求在先发送的请求后面。



- https://h-adashx.ut.taobao.com
- http://galaxy.yangtuojia.com
  - jacocorecordhistory
    - getData?params%5Brandom_id_parent%5D=1606203983322&par
    - getData?params%5Brandom_id_parent%5D=1606203983322&par
    - getData?params%5Brandom_id_parent%5D=1606203983322&par
    - getData?params%5Brandom_id_parent%5D=1606203983322&par
- http://k.yangtuojia.com
  - rest
    - mywork
    - quickreload
      - latest
        - 52274473?since=1606208746814&_=1606208716530
        - 52274473?since=1606208776820&_=1606208716532
        - 52274473?since=1606208806828&_=1606208716534
    - tinymce
    - jiraanywhere
    - shortcuts
    - api

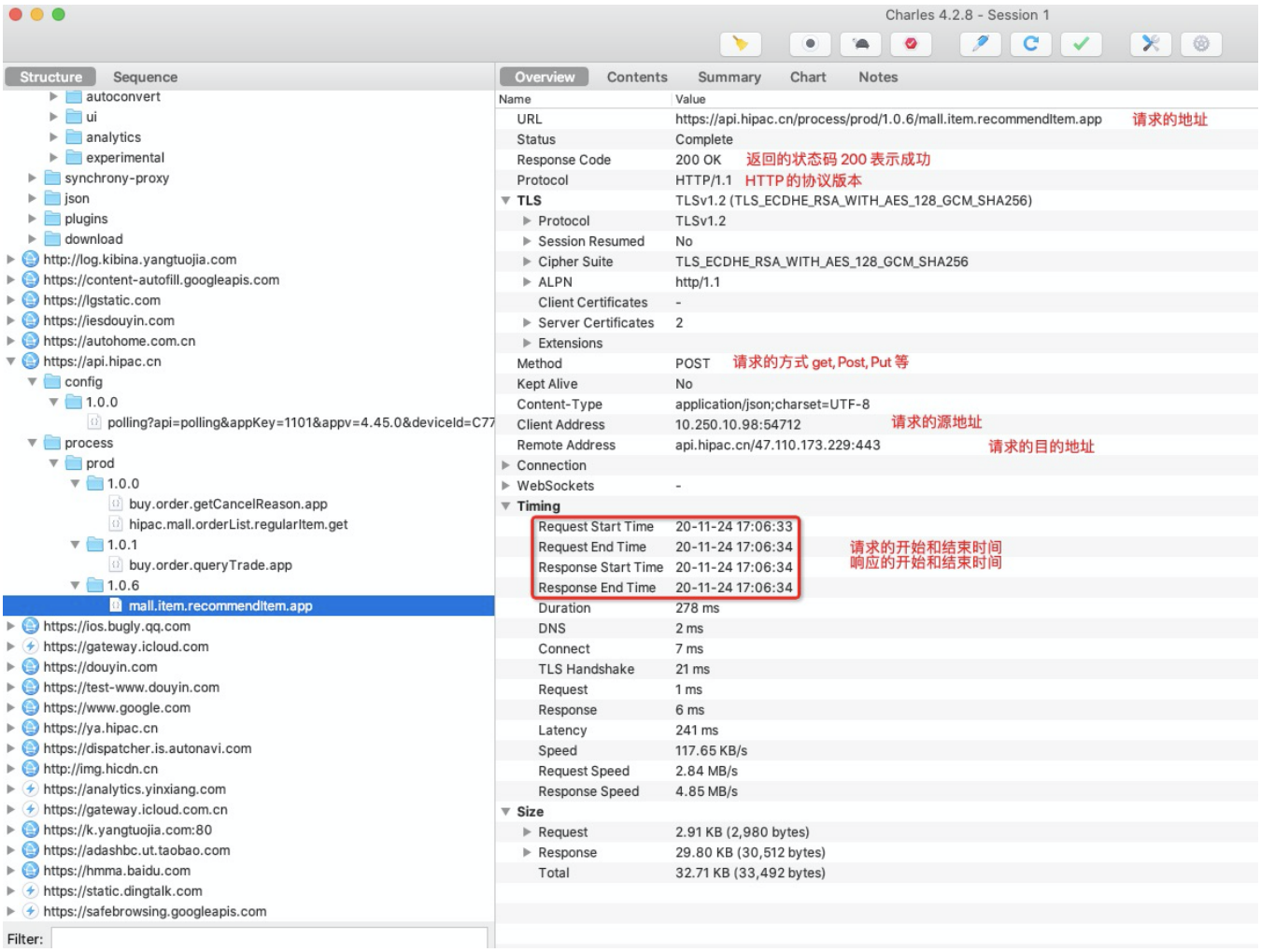


Code	Method	Host	Path
200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
200	GET	safebrowsing.googleapis.com	/v4/threatListUpdates:fetch?$req=Ch
200	GET	k.yangtuojia.com	/rest/mywork/latest/status/notification
200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
200	POST	k.yangtuojia.com	/json/startheartbeatactivity.action

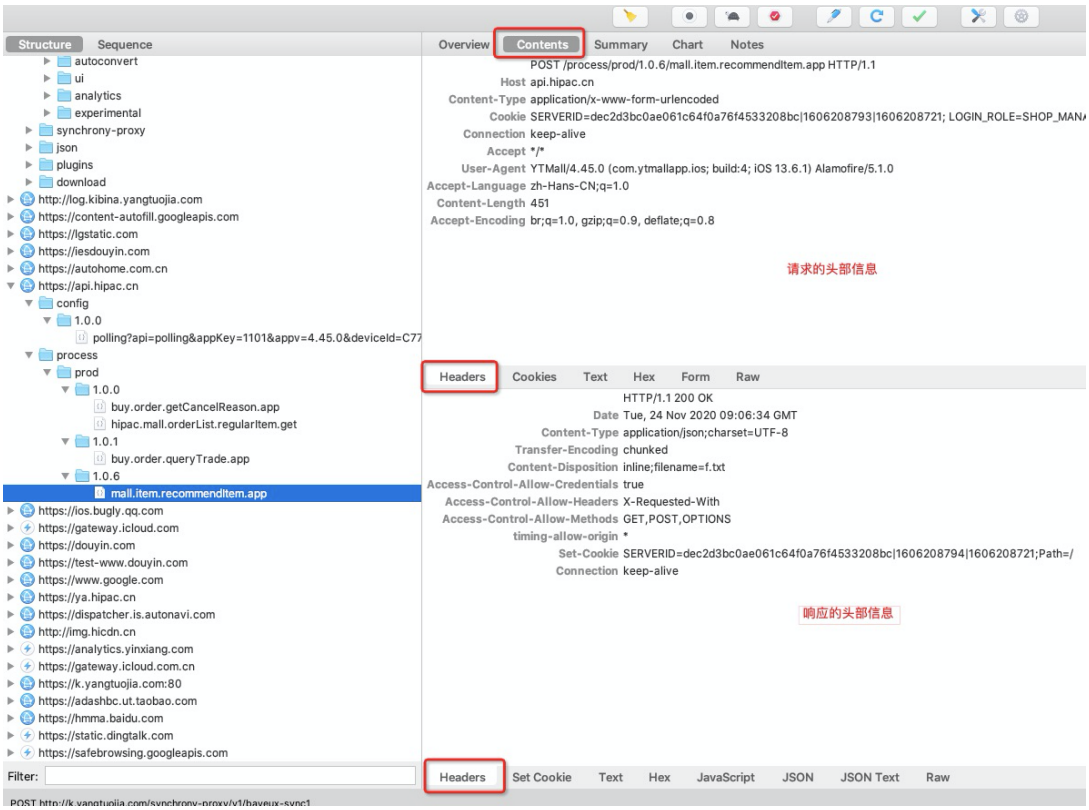
每一条请求数据怎么看？

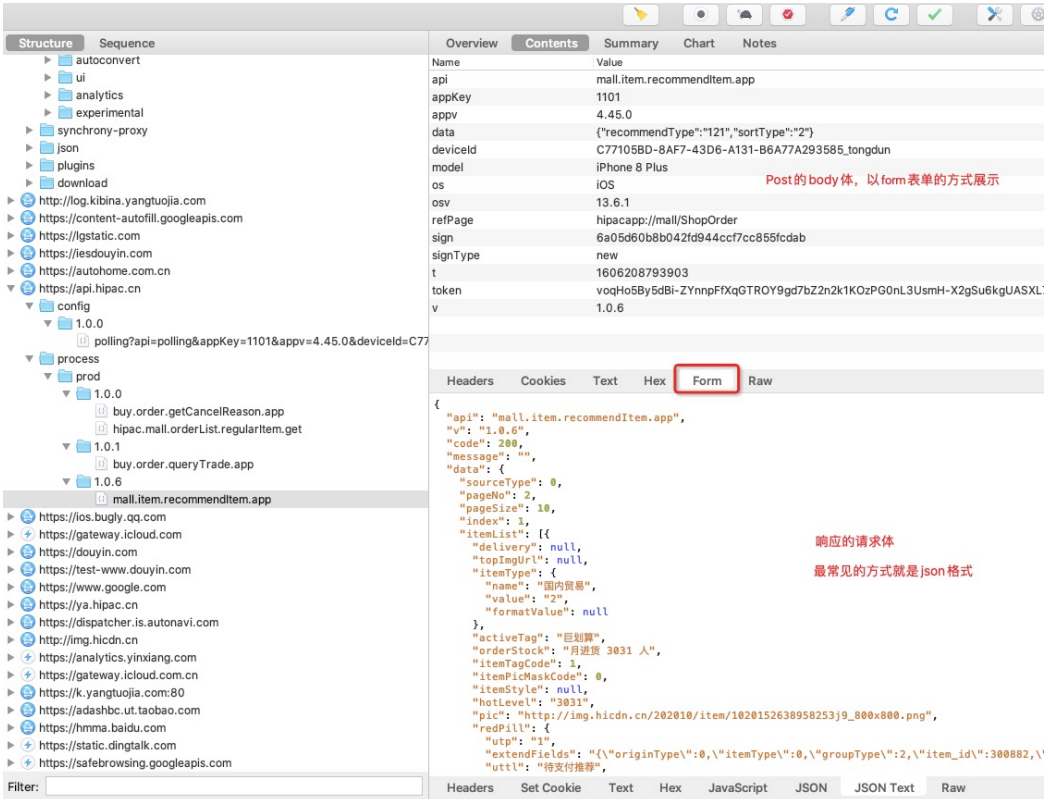
我们以structure格式为例：随机点击一个请求，右边会有一个详情框显示出来。

先看OverView标签的内容有哪些，我们把经常关注的信息标示出来了。



Contents 标签内容，右边框内的上半部分是请求的body内容，下半部分是响应的body部分，具体的数据支持多种格式呈现。





至此你已经知道如何去查看一个数据包的具体内容了。

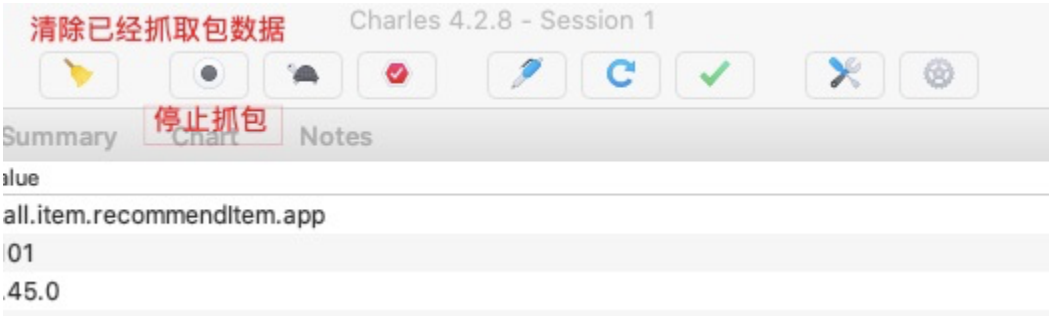
==========

我是分隔区域～～～～

==========

charles其他基本功能

- 抓包的基本设置

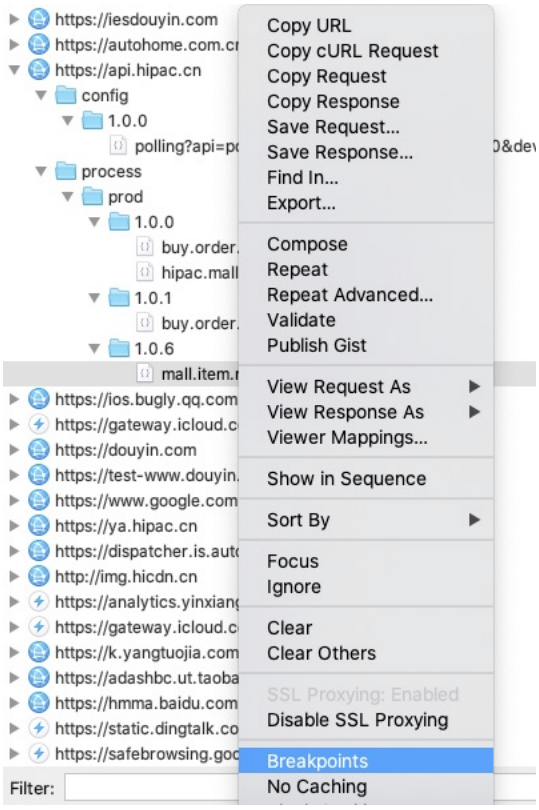


- 模糊查找数据包：

Edit → Find, 在打开的对话框中输入你想要查找的任意内容，charles会搜索出来所有跟关键匹配的请求。

它支持按包路径查找，也支持指定的消息列表中查找，搜索的关键词支持正则表达式，大小写是否敏感等。

- 请求过程中修改请求参数：这个功能非常有价值，类似于代码中调试断点功能，在需要断点的请求上右击选择BreakPoints



设置之后当有这条请求发送的时候会停下来，你可以从容的修改请求head和body，修改后再发送，也可以修改response的head和json数据。

这个功能在后端功能没有完全开发好之前验证前端非常管用。

- repeat功能：重复发送请求，这个可以让你不用从客户端操作，直接在charles中重发就行，该功能最常和Breakpoints配合使用。

其他比如模拟网络延时，数据包过滤，映射等功能可以参照互联网的知识文档查看，更多功能需要你更深入的使用才能理解和掌握

==========

作业:

1.自己负责抓取mall app的测试环境请求的hop地址的url,入参,返回,并进行网络延迟,返回结果的mock

结束