常用的抓包工具有哪些?

終端研發部 今天

收錄於話題

#數據庫 37 #抓包工具 2 #微服務 66 #架構 54 #互聯網 22

點擊上方關注“

設為“

正文

在我們做接口測試的時候，經常需要驗證發送的消息是否正確，或者在出現問題的時候，查看手機客戶端發送給server端的包內容是否正確，就需要用到 而工程師和程序常用的抓包工具有哪些呢？今天我們就來簡單聊一聊。今天我們主要就來介紹一下fiddler、httpwatch和wireshark。Charles，Proxyman，Wireshark，HttpCanary，tcpdump，瀏覽器自帶的“開發者工具”

Fiddler抓包工具

Fiddler是以代理web服務器的形式工作的，它使用代理地址:127.0.0.1，端口:8888。當啟動fiddler，程序將會把自己作為一個代理，所以的http請求在達到目標服務器之前都會經過fiddler，同樣的，所有的http響應都會在返回客戶端之前流經fiddler。

Tips：默認情況下，fiddler是不會捕獲https會話的。常見的主要功能有：

1.Fiddler中設置斷點修改Request。

Fiddler最強大的功能莫過於設置斷點，設置好斷點後，你可以修復httpRequest的任何消息包括host，cookie或者表單中的數據。設置斷點有兩種方法。

第一種：打開fiddler點擊Rules->Automatic Breakpoint->Before Requests(這種方法會中斷所有的會話)

消除辦法：點擊Rules->Automatic Breakpoint->Disabled

第二種：在命令行中輸入命令：bpu www.taobao.com(這種方法只會中斷www.baidu.com)

消除辦法：在命令行中輸入bpu

2.設置斷點修改Response

fiddler中也能修改Response。方法如下：

第一種：打開Fiddler點擊Rules->Automatic Breakpoint->After Respinse(這種方法會中斷所有的會話)

消除辦法：點擊Rules->Automatic Breakpoint ->Disabled

第二種：在命令行中輸入命令：bpafter www.taobao.com(這種方法會中斷www.taobao.com)

消除辦法：命令行中輸入命令bpafter

修改Response方法：

選擇Rules-> Automatic Breakpoint->After Respinse，手機點擊操作，發送query。

选中左区的query，点击右边的Raw，修改Raw里面的返回结果，运行“Run to Completion”

fiddler下载地址：

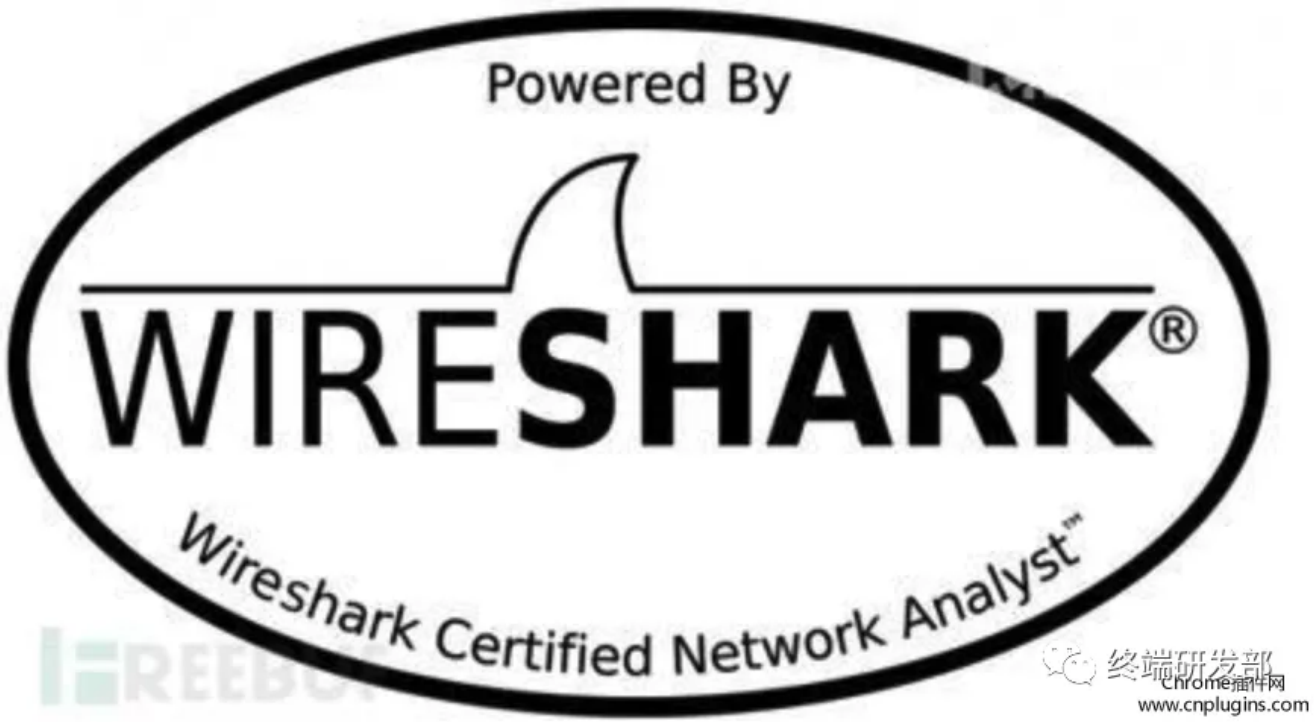
fiddler for Mac

fiddler for Linux

fidder for window

Wireshark抓包工具

Wireshark是世界上最流行的网络分析工具。这个强大的工具可以捕捉网络中的数据，并为用户提供关于网络和上层协议的各种信息。与很多其他网络工具一样，Wireshark也使用pcapnetwork library来进行封包捕捉。可破解局域网内QQ、邮箱、msn、账号等的密码！！wireshark能获取HTTP，也能获取HTTPS，但是不能解密HTTPS，所以wireshark看不懂HTTPS中的内容，总结，如果是处理HTTP,HTTPS 还是用Fiddler, 其他协议比如TCP,UDP 就用wireshark。



不过，Wireshark配置起来比fiddler麻烦一些，如果不配代理，需要安装个Connectify来建立热点，然后再安装wireshark进行抓包，如果配置了代理，直接安装wireshark即可。Wireshark（前称Ethereal）是一个网络封包分析软件。网络封包分析软件的功能是撷取网络封包，并尽可能

显示出最为详细的网络封包资料。Wireshark使用WinPCAP作为接口，直接与网卡进行数据报文交换。

网络管理员会使用wireshark来检查网络问题；软件测试工程师使用wireshark抓包，来分析自己测试的软件；从事socket编程的工程师会用wireshark来调试

听说，华为，中兴的大部分工程师都会用到wireshark。（毕竟小编以前也是从事通信行业的高级工程师啊）。

普通使用者使用Wireshark来学习网络协定的相关知识。

WireShark 主要分为这几个界面：

1. Display Filter(显示过滤器)， 用于过滤

2. Packet List Pane(封包列表)， 显示捕获到的封包， 有源地址和目标地址，端口号。颜色不同，代表

3. Packet Details Pane(封包详细信息), 显示封包中的字段

4. Dissector Pane(16进制数据)

5. Miscellanous(地址栏，杂项)

使用过滤是非常重要的， 初学者使用wireshark时，将会得到大量的冗余信息，在几千甚至几万条记录中，以至于很难找到自己需要的部分。搞得晕头转向。过滤器会帮助我们在大量的数据中迅速找到我们需要的信息。过滤器有两种：

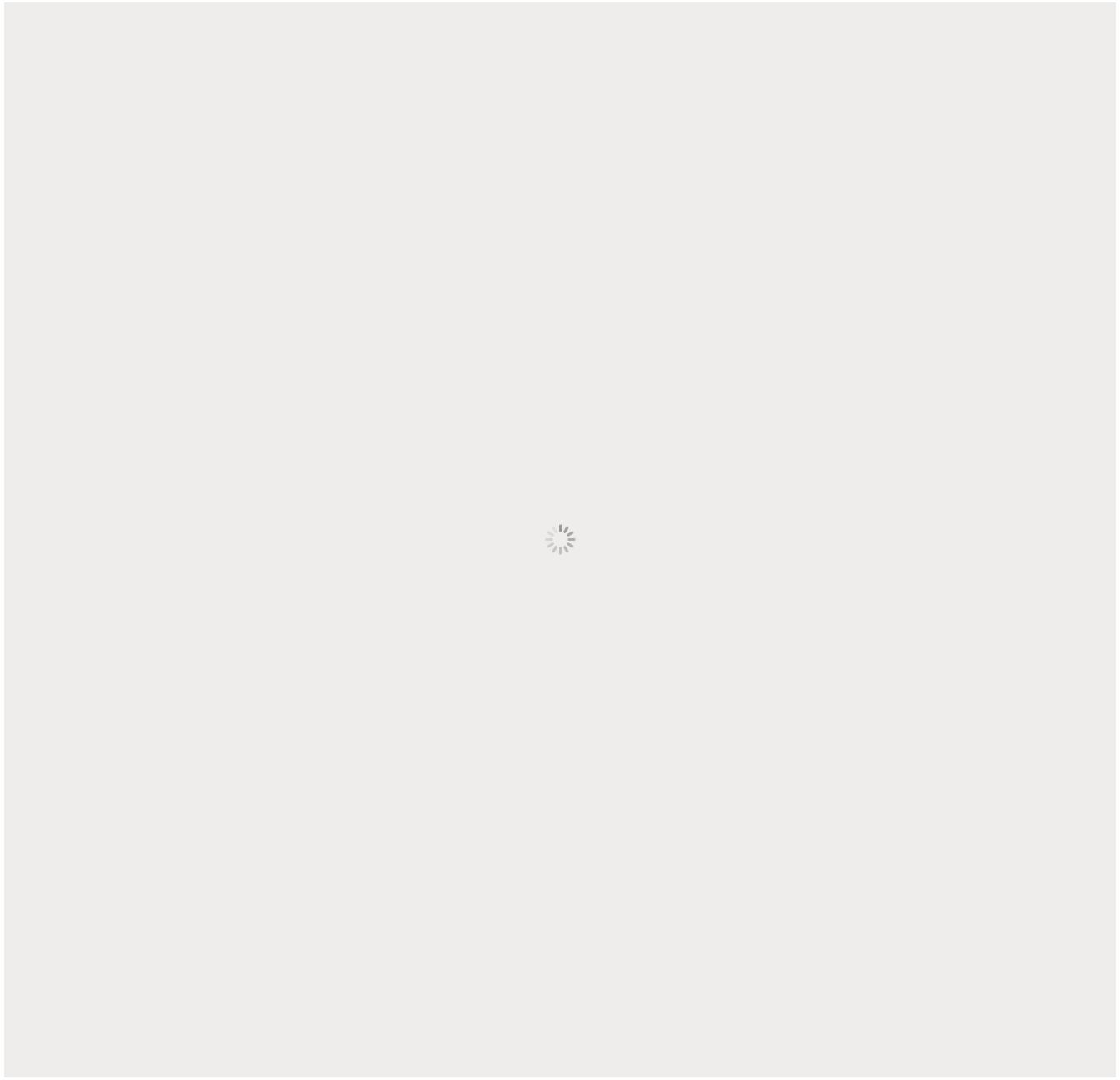
1. 一种是显示过滤器，就是主界面上那个，用来在捕获的记录中找到所需要的记录
2. 一种是捕获过滤器，用来过滤捕获的封包，以免捕获太多的记录。在Capture -
   > Capture Filters 中设置

Wireshare官网下载地址：

https://www.wireshark.org/

HttpWatch抓包工具

HttpWatch是强大的网页数据分析工具，集成在Internet Explorer工具栏。它不用代理服务器或一些复杂的网络监控工具，就能够在显示网页同时显示网页请求和回应的日志信息。甚至可以显示浏览器缓存和IE之间的交换信息。集成在Internet Explorer工具栏。它不仅界面美观且安装后使用也特别方便，shift+12可调出界面（个人觉得类似firebug），和firebug一样获取http请求信息时不需要通过代理服务器或其他网络监控工具。ctrl+F5可以强制刷新时从服务器重新获取资源而不是读取缓存信息。



只需要选择相应的网站，软件就可以对网站与IE之间的需求回复的通讯情况进行分析并在同一界面显示其相应日志记录。每一个HTTP记录都可以详细的分析其 Cookies、消息头、字符查询等信息。支持HTTPS及分析报告输出为XML、CSV等格式。使用方法:打开IE浏览器，选择菜单"查看-浏览器栏"，再选择"HttpWatch Professional"即可。

日志中有少量内容还是英文，汉化后会出错，故保留。提示:授权文件已经在根目录下的"httpwatch.lic"

SmartSniff抓包工具

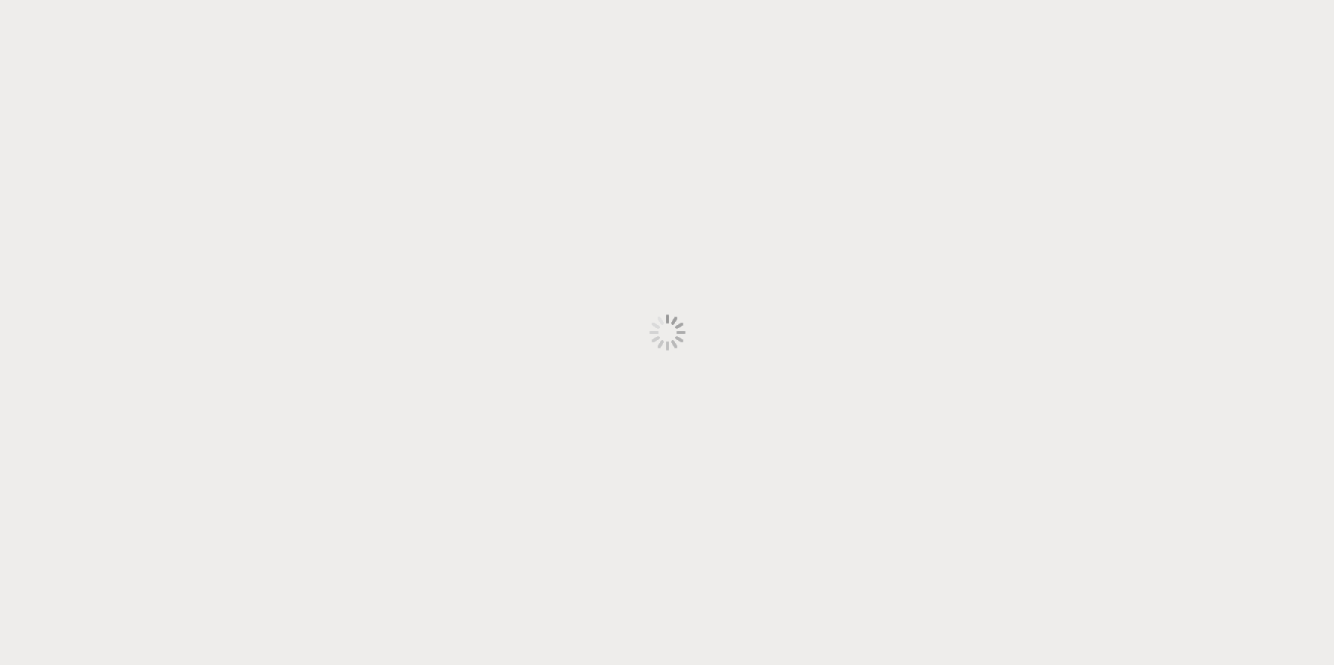
SmartSniff 是一款 TCP/IP 数据包捕获软件,允许你检查经过你的网络适配器的网络传输.该软件的双层界面显示了捕获的数据包和在 ASCII 或者十六进制格式下的详细的信息.额外的功能包括本地和远程传输的彩色代码,导出到 HTML 以及更多功能. SmartSniff 可以用于 Windows 2000/SP Raw Sockets 或者用于其它的 Windows 版本的 WinPcap.这是一款基本的,但是非常小且独立的协议分析软件。
下载地址:

firebug抓包工具

firebug是浏览器firefox浏览器自带插件，安装使用方便，支持多种浏览器，快捷键F12便可打开，方便我们一般对系统进行调试或对获取到信息调试。实际我自己在工作中也经常用到。

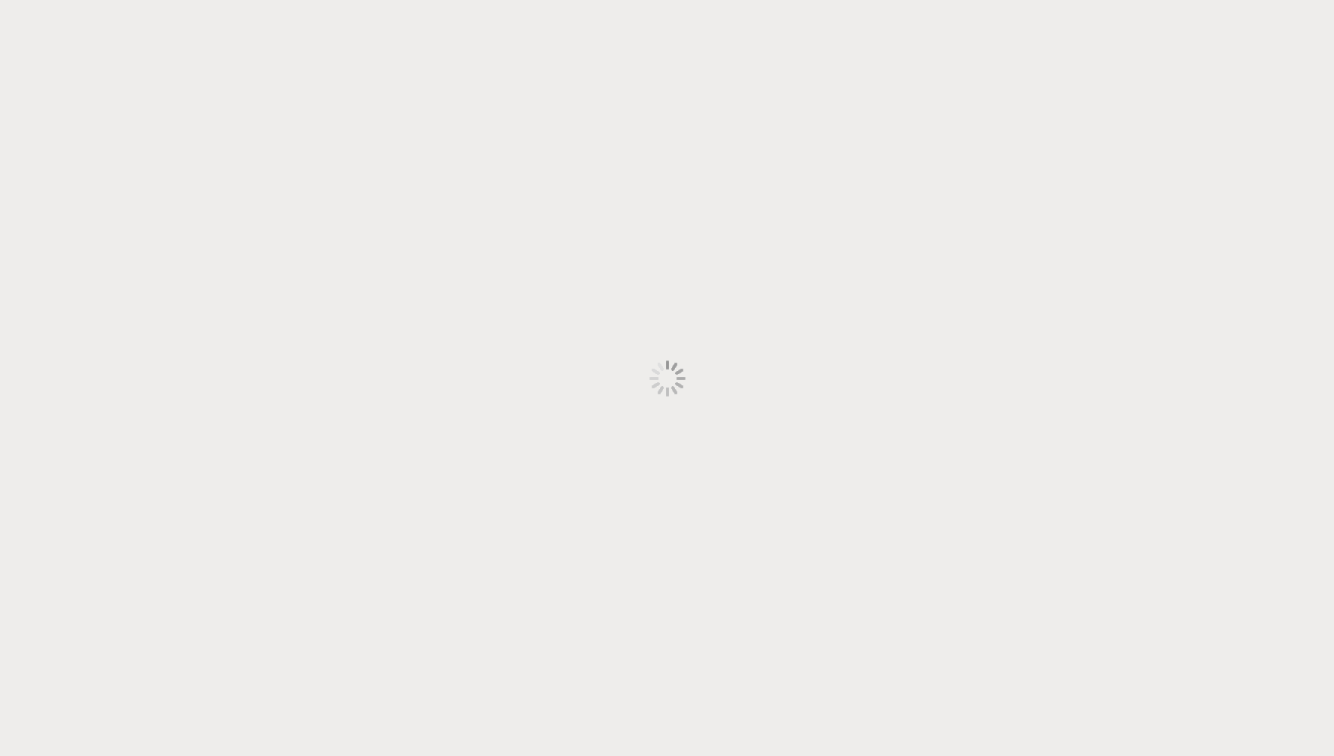
Charles

Charles是由JAVA开发的，可以运行在window Linux MacOS，但它是收费的，和Fiddler工具很类似，很多MacOS用户喜欢用这个软件



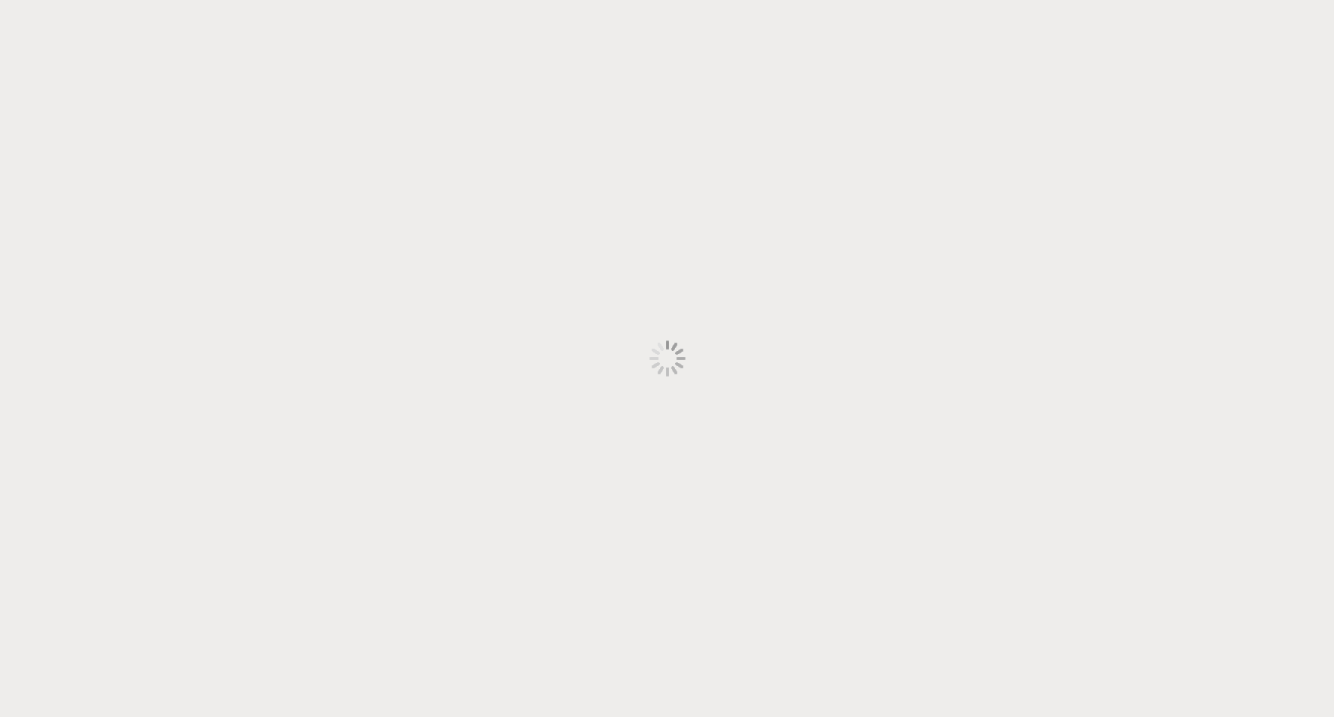
Proxyman

Proxyman是一款MacOS系统下一款非常优秀的抓包软件，免费使用，而且界面非常好看，强烈推荐



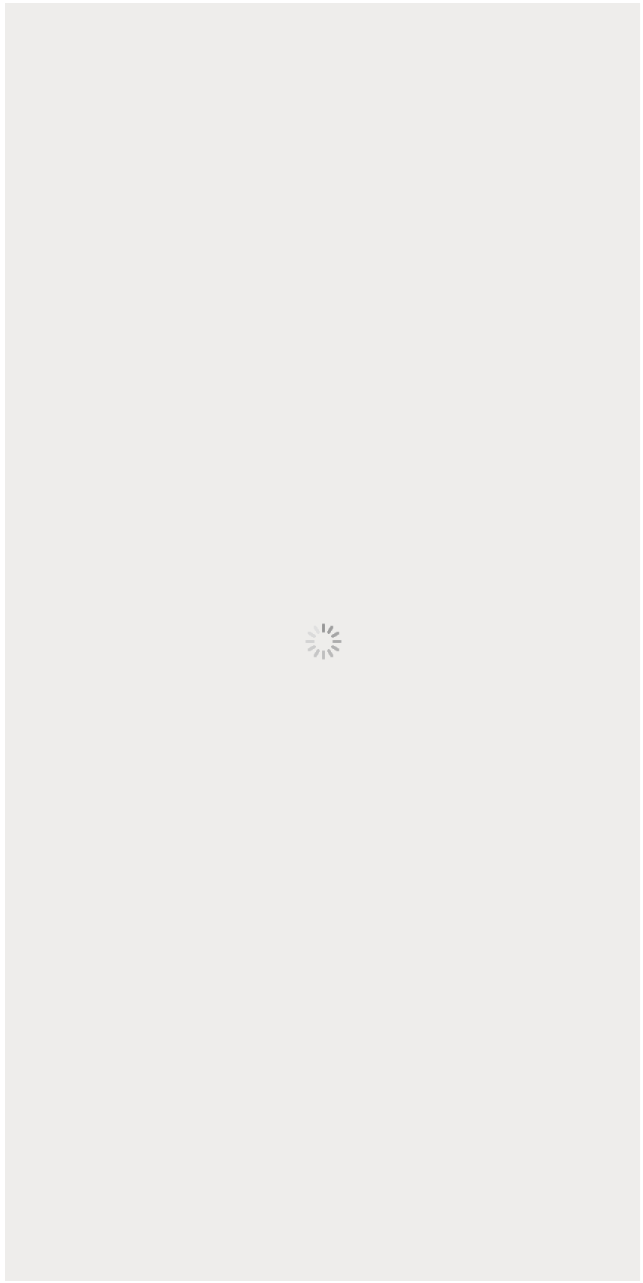
Wireshark

Wiresark 是一款超级厉害的抓包工具，是从事网络工程师必用工具，也是一款跨平台的工具，Windows Linux macOS 都可以使用。它不仅可以分析http/https的数据，它还可以分析网络2层以上都可以看到，比如tcp的三次握手等，但是如果你只是分析http协议，可以不用这么专业的工具，以免增加筛选请求成本和学习成本



HttpCanary

HttpCanary 是一款安卓端抓包软件，不用root，免费版可以基本满足日常抓包需求，如果想拿手机直接抓包的话，可以尝试用下

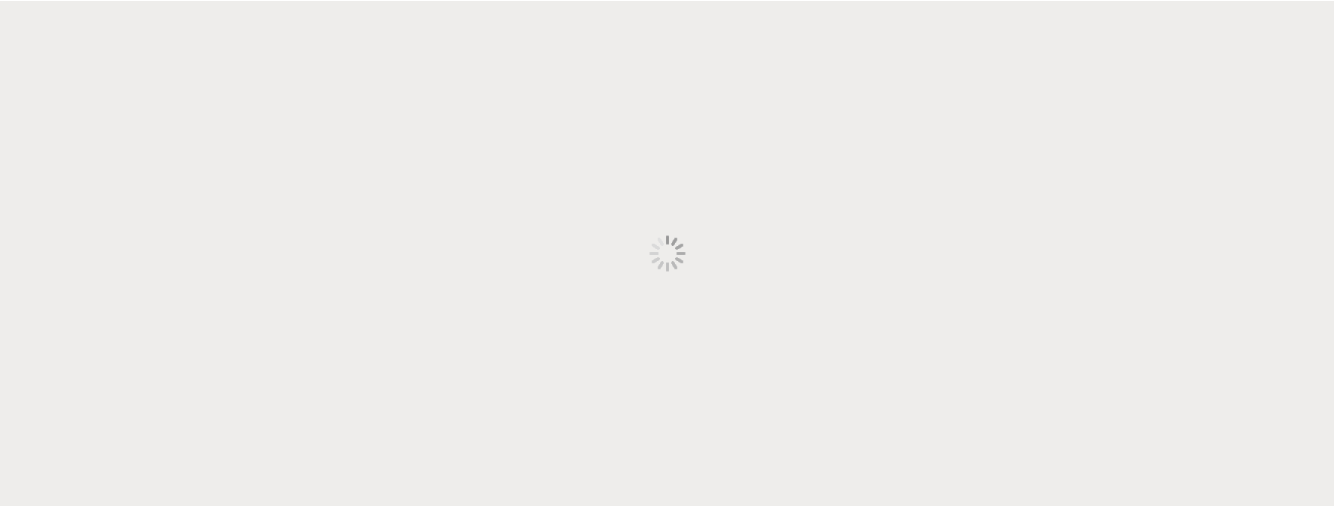


tcpdump

tcpdump 是Linux下常用的抓包工具，它是一个命令行工具，可以抓取和Wireshark类似的数据，而且保存的数据包，可以放到Wireshark中分析。如果你的Linux服务器需要抓包分析问题，它是一个非常好的选择。

浏览器自带的“开发者工具”

电脑端所有的浏览器都带有开发者工具，如果不是特别高的需求，用浏览器自带的开发者工具，基本可以满足日常生活的抓包需要



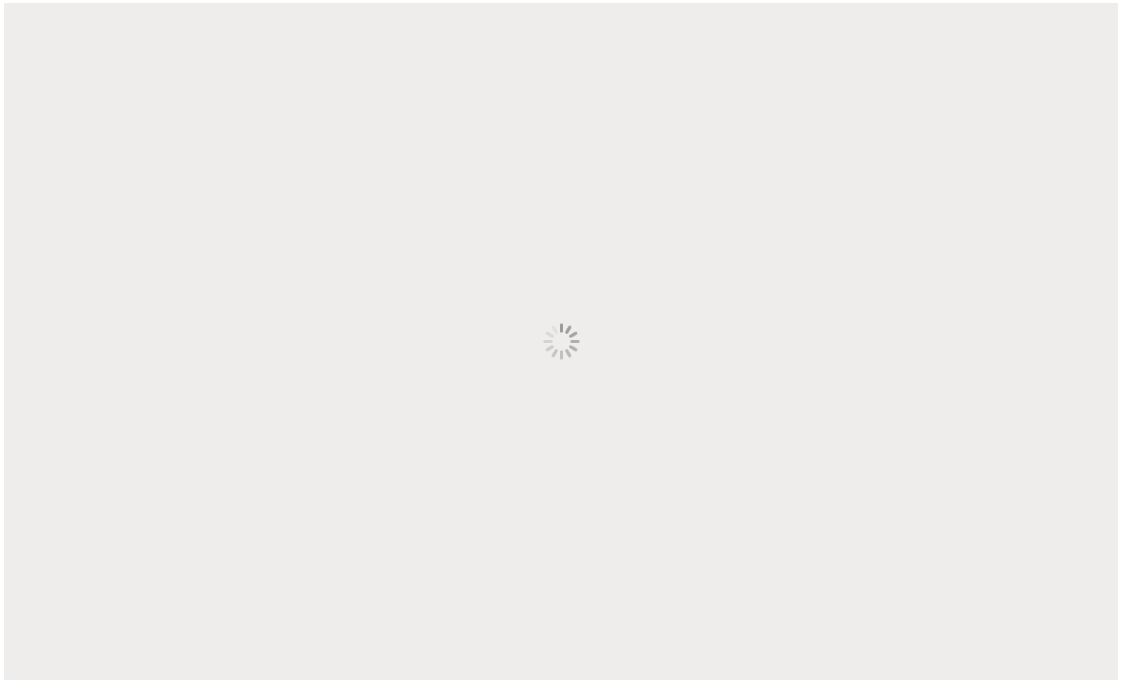
常用的抓包工具总结

抓包工具有很多，小到最常用的web调试工具firebug，达到通用的强大的抓包工具wireshark。大家在选择抓包工具时，一定要定位好自己的需求。Firebug虽然可以抓包，但是对于分析http请求的详细信息，不够强大。模拟http请求的功能也不够，且firebug常常是需要“无刷新修改”，如果刷新了页面，所有的修改都不会保存。Wireshark是通用的抓包工具，但是比较庞大，对于只需要抓取http请求的应用来说，似乎有些大材小用。Httpwatch也是比较常用的http抓包工具，但是只支持IE和firefox浏览器（其他浏览器可能会有相应的插件），对于想要调试**chrome浏览器**的http请求，似乎稍显无力，而Fiddler2 是一个使用本地 127.0.0.1:8888 的 HTTP 代理，任何能够设置 HTTP 代理为 127.0.0.1:8888 的浏览器和应用程序都可以使用 Fiddler。

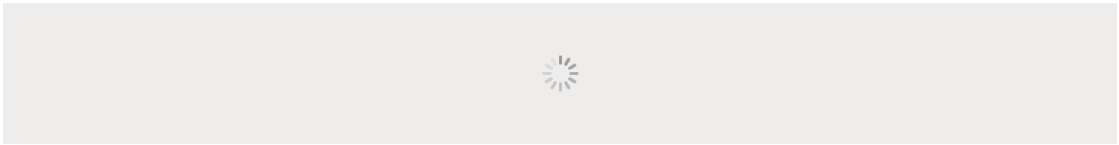
参考：

https://zhuanlan.zhihu.com/p/346667471

https://www.cnplugins.com/zhuanti/zhuabao.html

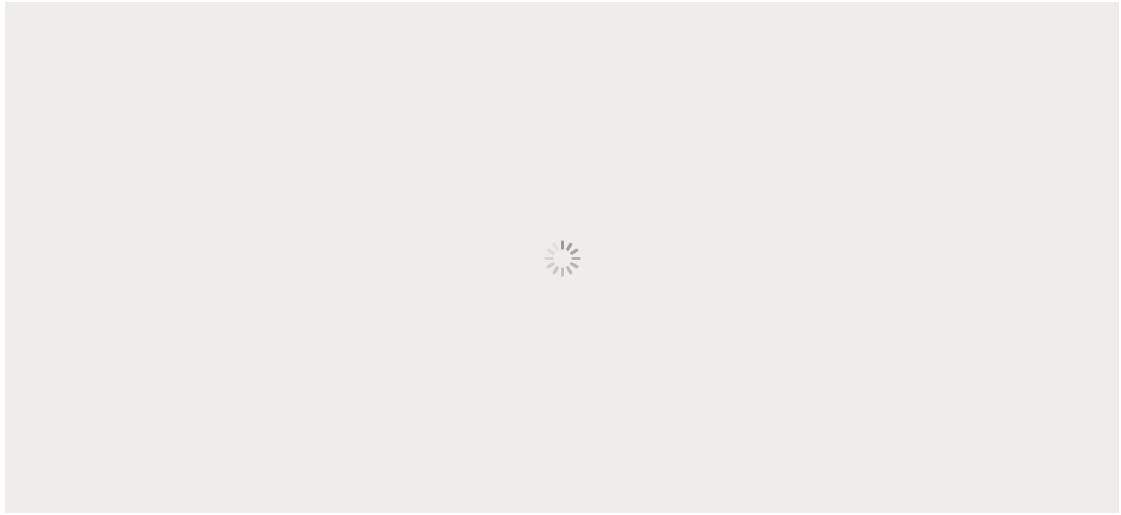


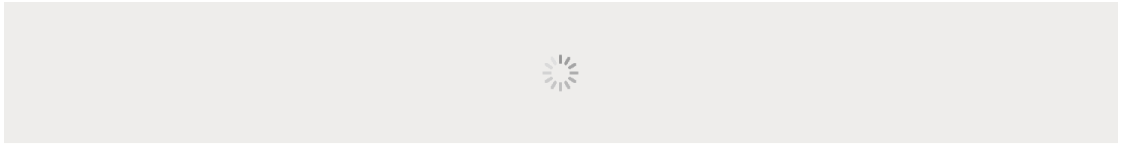
想获取 Java大厂面试题学习资料
扫下方二维码回复「**BAT**」就好了



回复 **【加群】**获取github掘金交流群
回复 **【电子书】**获取2020电子书教程
回复 **【C】**获取全套C语言学习知识手册
回复 **【Java】**获取java相关的视频教程和资料
回复 **【爬虫】**获取SpringCloud相关多的学习资料
回复 **【Python】**即可获得Python基础到进阶的学习教程
回复 **【idea破解】**即可获得intellij idea相关的破解教程

关注我gitHub掘金，每天发掘一篇好项目，学习技术不迷路！





回复 【idea激活】 即可获得idea的激活方式

回复 【Java】 获取java相关的视频教程和资料

回复 【SpringCloud】 获取SpringCloud相关多的学习资料

回复 【python】 获取全套0基础Python知识手册

回复 【2020】 获取2020java相关面试题教程

回复 【加群】 即可加入终端研发部相关的技术交流群

阅读原文

Vue中文社區

網工必知：（5）juniper SRX 防火牆PPPOE撥號配置

網絡之路博客