

# Fiddler 移动设备抓包

南京游戏中心

Exported on 08/12/2019

# Table of Contents

本文参考文档：

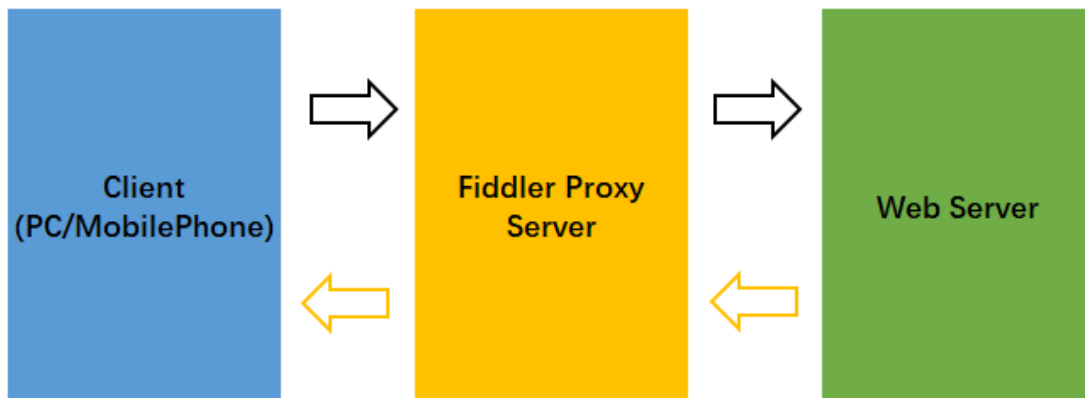
<https://www.cnblogs.com/yyhh/p/5140852.html#l02>

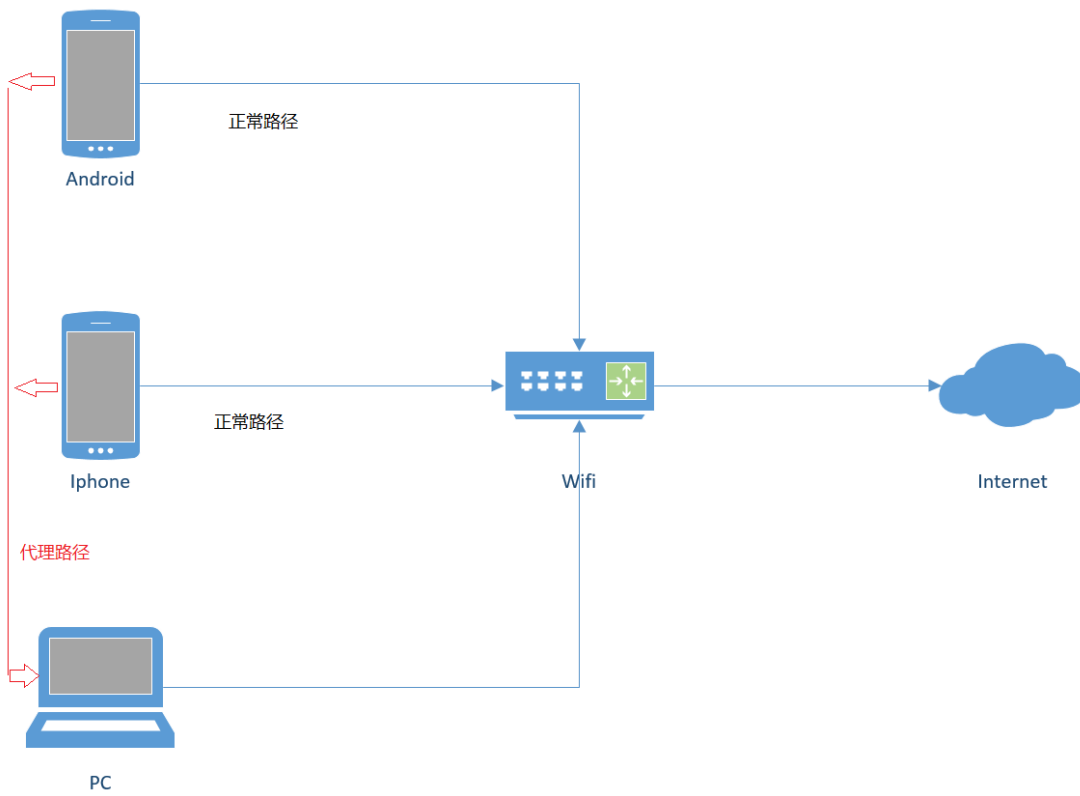
目的：

研发场景一，有时我们需要对移动端和服务端的http/https请求进行查看，确认接口的调用，参数的传递，服务的响应符合我们的预期；

研发场景二，有时，我们需要对移动端的请求进行截断，修改某些请求内容。或者是拦截服务端的响应，修改某些响应内容。来满足我们特定的开发/测试场景。

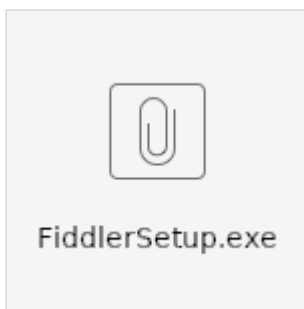
原理：





## 一、Fiddler的安装

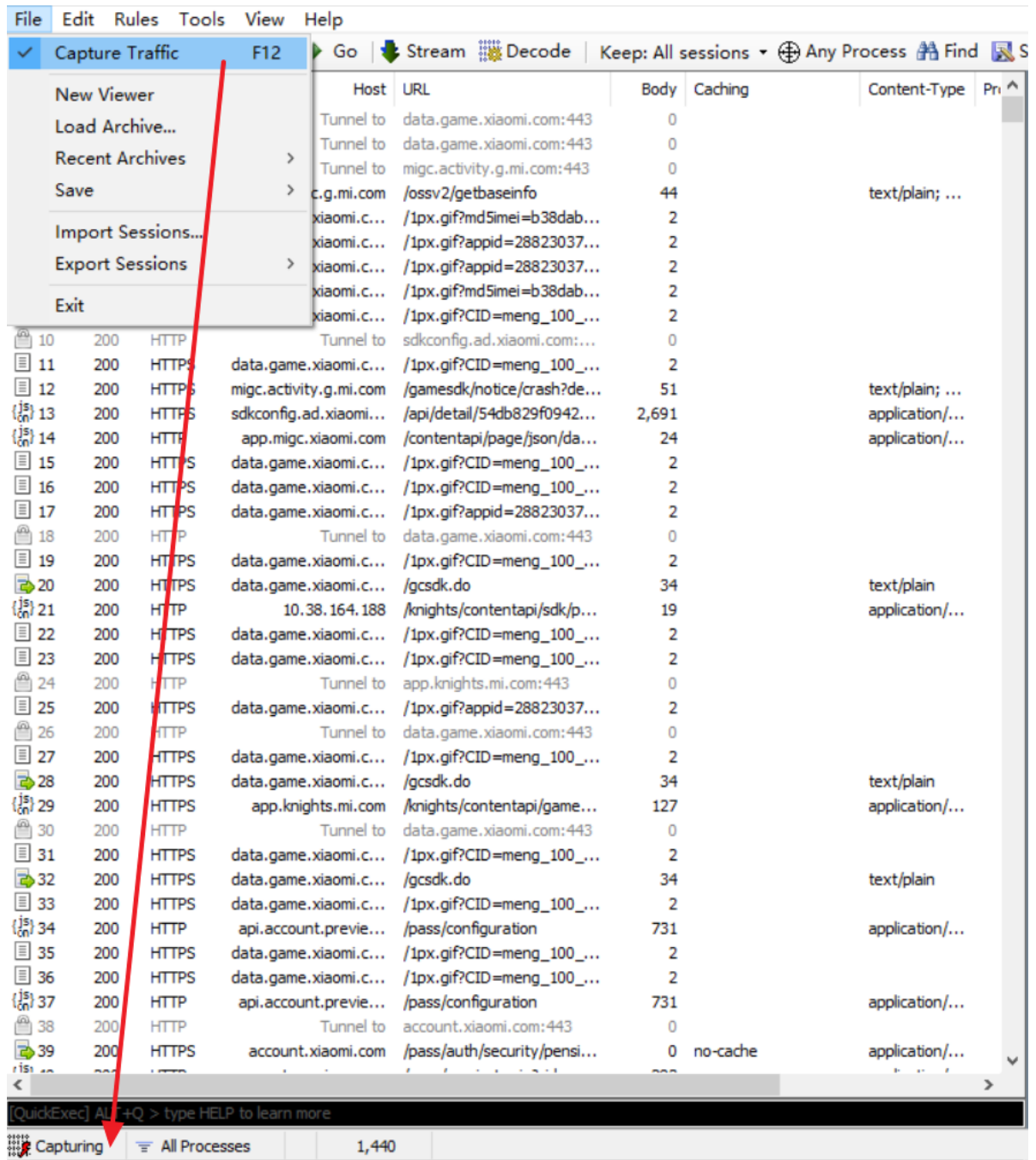
<https://www.telerik.com/download/fiddler>



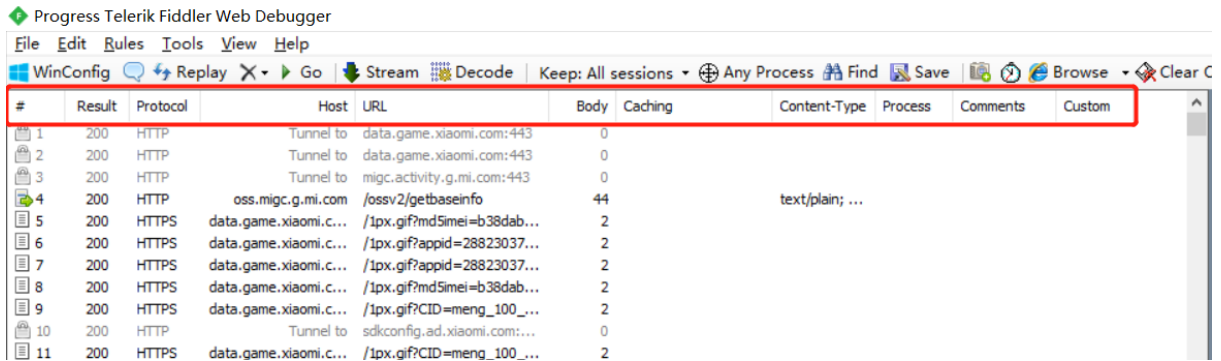
## 二、基本功能介绍

1. 确保Capture Traffic的开启

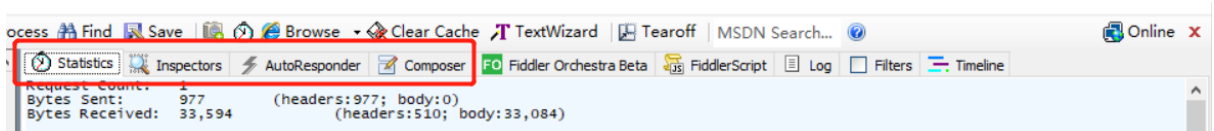
Progress Telerik Fiddler Web Debugger



## 2. 字段含义



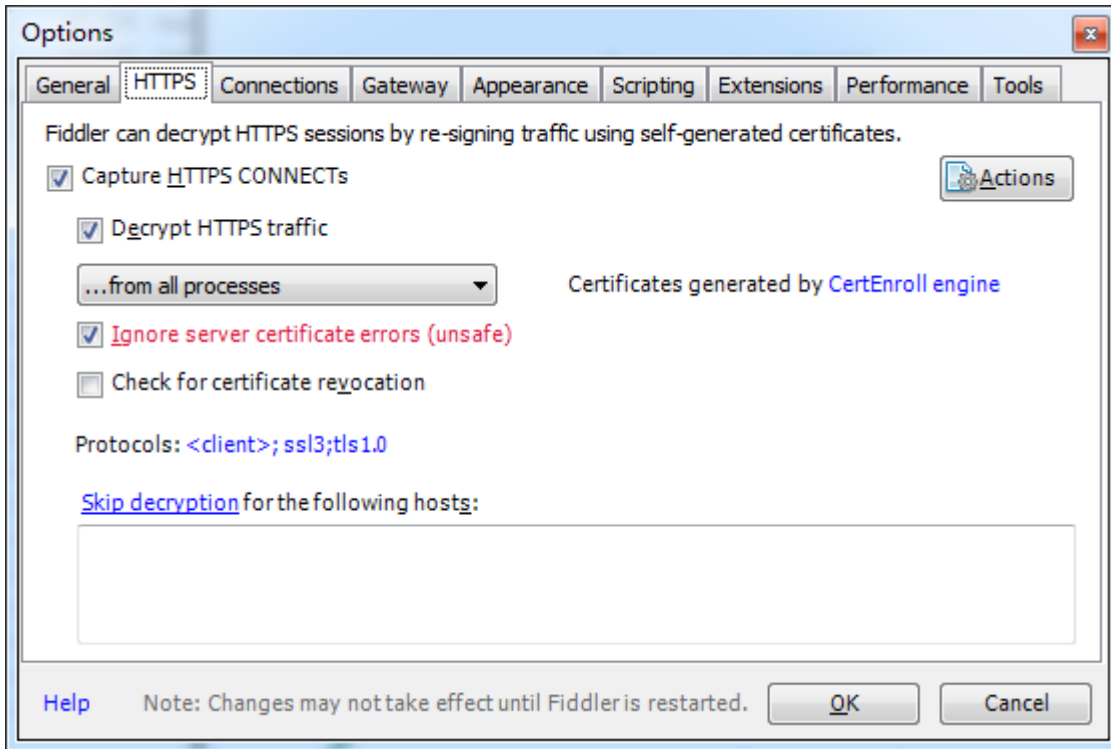
名称	含义
#	抓取HTTP Request的顺序, 从1开始, 以此递增
Result	HTTP状态码
Protocol	请求使用的协议, 如HTTP/HTTPS/FTP等
Host	请求地址的主机名
URL	请求资源的位置
Body	该请求的大小
Caching	请求的缓存过期时间或者缓存控制值
Content-Type	请求响应的类型
Process	发送此请求的进程: 进程ID
Comments	允许用户为此回话添加备注
Custom	允许用户设置自定义值



名称	含义
Statistics	请求的性能数据分析
Inspectors	查看请求/响应数据内容
AutoResponder	允许拦截指定规则的请求

Composer	自定义请求发送服务器
Filters	请求过滤规则

### 三、https请求获取设置



### 四、移动设备抓包

1. 确保手机和PC在同一网络下(连接相同的wifi)
2. 获取PC 无线IP地址
3. 手机wifi连接配置代理, (pc IP + Fiddler监听端口8888)
4. 手机浏览器访问PC IP : Fiddler监听端口, 下载证书
5. 手机安全设置中导入证书
6. 手机端的http/https请求, 均能被Fiddler正常记录

