## Fillder简介

Fiddler基本界面包括如下区域。

（1)主菜单栏：菜单中几乎可以启动所有的Fiddler功能，后续章节会对其进行讲解。

（2）工具栏：提供了很多常见的命令。

（3）Web Sessions列表（会话列表）：显示捕捉到的每个Session的简短信息。平常都

需要在这里选择一个或者多个Session后再进行操作。

（4）功能面板：这里有很多选项卡，提供了很多功能。我们常用的是Inspectors选

项卡。

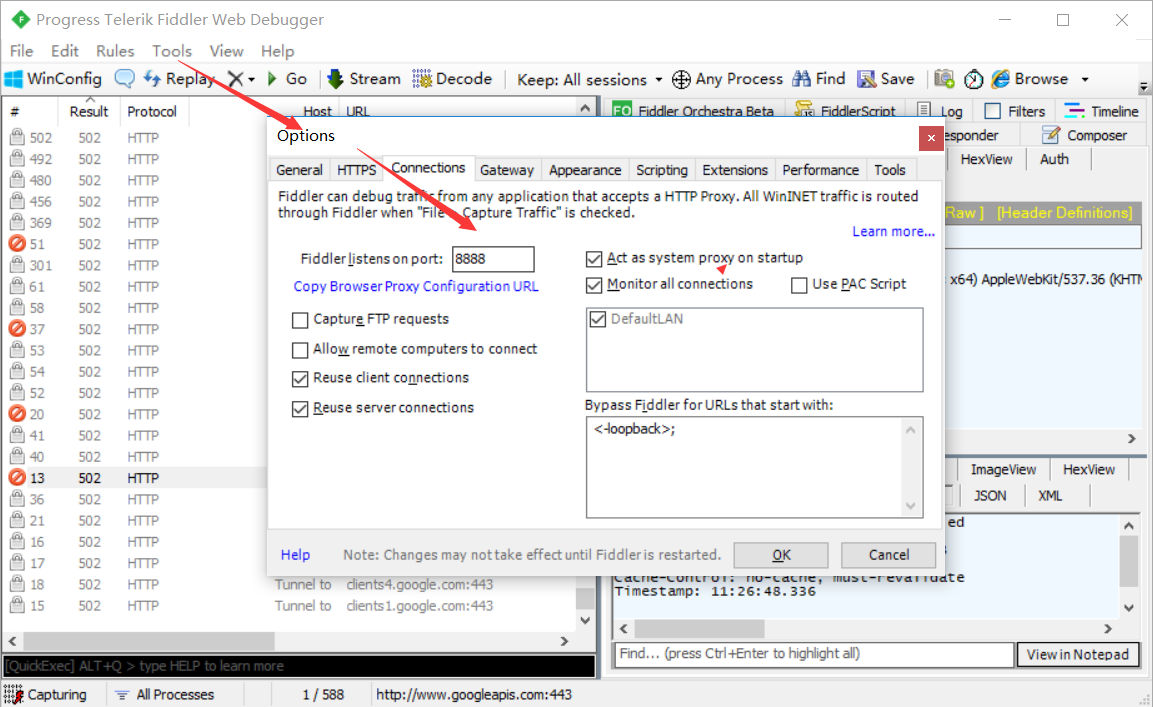
（5）QuickExec：命令行工具，可以输入简单的命令，例如输入cls可以清空Web Sessions。

（6）状态栏：上面显示了Fiddler的一些配置信息。\

df

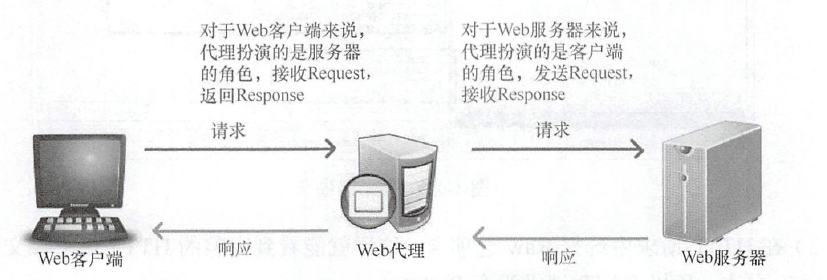
### Fiddler 抓包的原理

Fiddler 为什么能抓包呢？ Fiddler 本质上是一个Web 代理服务器。它的默认工作端口是8888



### 什么是代理服务器

Web 代理（ Proxy Server ）服务器是网络的中间实体。代理位于Web 客户端和Web 服务器之间，扮演“中间人”的角色。



代理服务器是网络信息的中转站，它具有以下功能。

（1）共享网络。能解决仅仅有一条线路、一个公有IP的问题。在公有IP资源严重不

足的情况下，可以满足局域网大量用户同时共享上网的需求。

（2）提高了访问速度。因为大部分的代理服务器都有缓冲功能，可以直接读取，

无须再连接到远程Web服务器。这样可以达到加快访问网站的速度、节约通信带宽的

目的。

（3）突破了访问限制。当访问权限受到限制时，可以使用有权限的代理服务器。

（4）隐藏身份。内部网的用户要对外发布信息，就需要使用代理服务器的反向代理功

能。这样就不会影响内部网络的安全性能，起到隐藏身份的目的。

### Fiddler 的工作原理



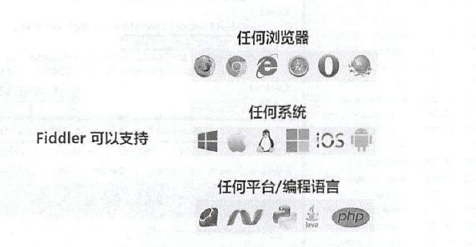
Fiddler启动的时候，会偷偷地把Internet选项中的代理修改为127.0.0.1，端口：8888。

当Fiddler退出的时候，它会自动在Internet选项中取消代理，这样就不会影响别的程序。如果Fiddler 非正常退出，这时候因为Fiddler没有自动注销，会造成网页无法访问。解决的办法是重新启动Fiddler。

### Fiddler 能捕获哪些设备的HTTP 数据包

任何支持代理的HTTP请求都能被Fiddler 捕获到，首先Fiddler能捕获各种浏览器，比如IE、Firefox、Chrome发出来的数据包。

Fiddler 还能捕获各种移动设备，比如Android手机、苹果手机、iPad等发出的数据包。

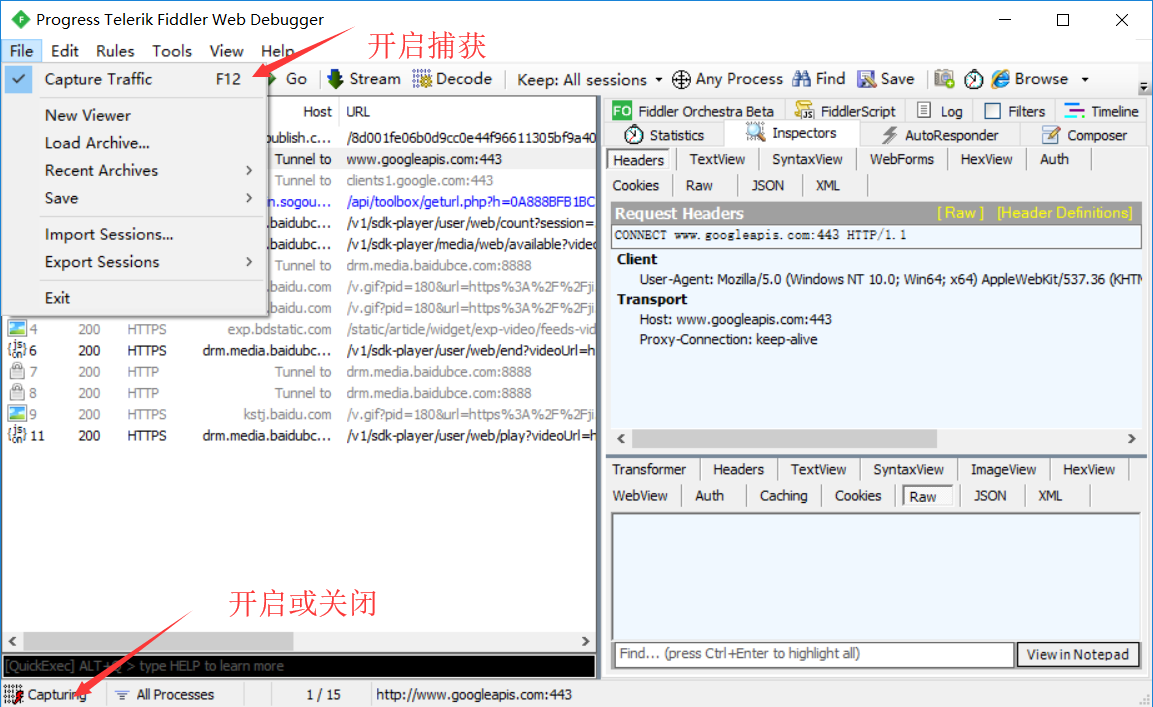


## 功能面板

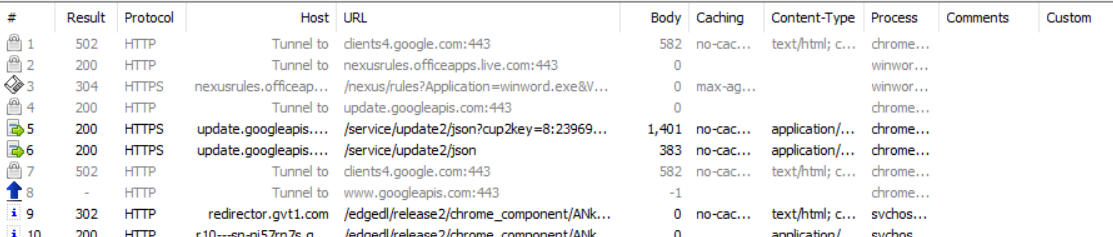
### capture traffic

我们把捕HTTP数据包的过程简称为抓包。在Fiddler的使用过程中，当我们已经抓到自己想要的数据包后，可以停止抓包，以避免抓到一些不需要的数据包。接下来介绍两种设置方法。

快捷键:F12



## web session



Fiddler 窗口的左边是Web Sessions列表，是Fiddler中最重要的部分，显示了每Session的摘要信息。Fiddler中的大部分操作都需要在Web Sessions阿表中选择一个或者多个Session,再进行其他操作。Web Sessions列表中的表头可以排序。

（1）#：这是Fiddler生成的ID（最好是按顺序排列）。

（2）Result：响应的状态码。

（3）Protocol：使用的协议HTTP或者HTTPS。

（4）Host:服务器的主机名和端口号。

（5）URL：URL的路径。

（6）Body:HTTP响应中包含的字节数。

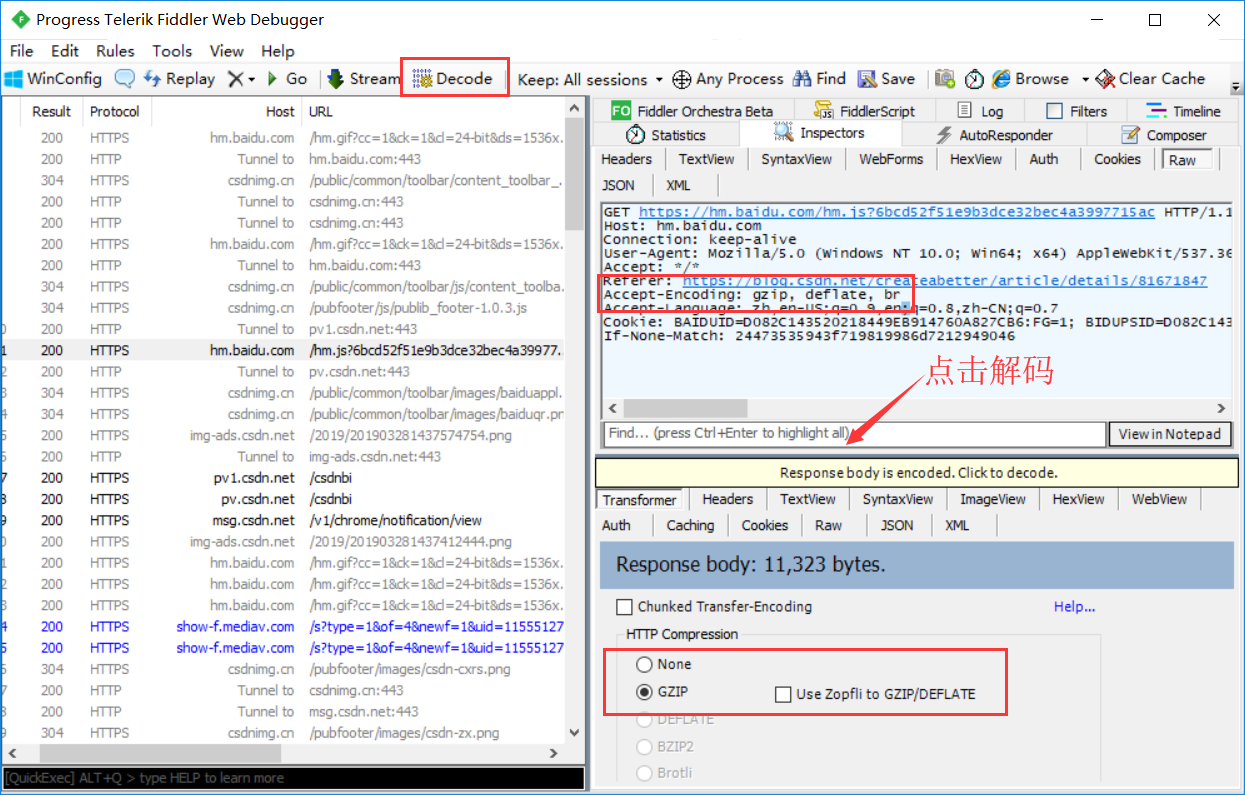
（7）Caching:跟缓存相关的字段的值。

（8）Content-Type:响应中Content-Type的值。

（9）Process:对应本地Windows的进程。

### 乱码（解压HTTP 响应）

在Fiddler抓包的过程中，我们经常看到HTTP响应是乱码，单击“Response body iencoded.Click to decode.”

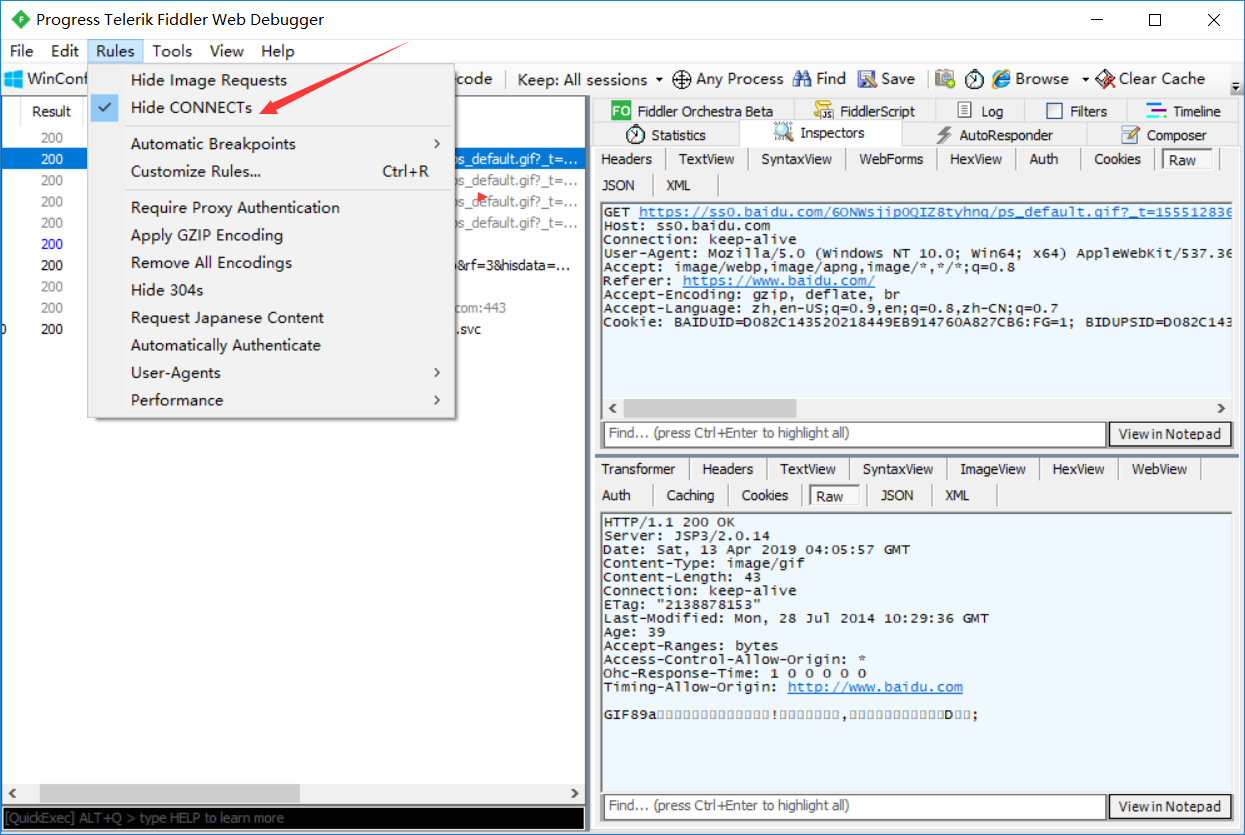


### Fiddler 可以捕获HTTPS 的握手验证请求

当浏览器访问HTTPS网页的时候，Fiddler能捕获到很多握手验证的请求，比如用浏览器打开https://www.baidu.com，在Fiddler中就能抓到很多“Tunnel to”的请求。

HTTP Tunnel(也叫HTTP 隧道、HTTP穿梭）是这样一种技术：它用HTTP协议在要通信的Client和Server 建立起一条“Tunnel”，然后Client 和Server之间的通信都是在这条Tunnel的基础之上实现的。

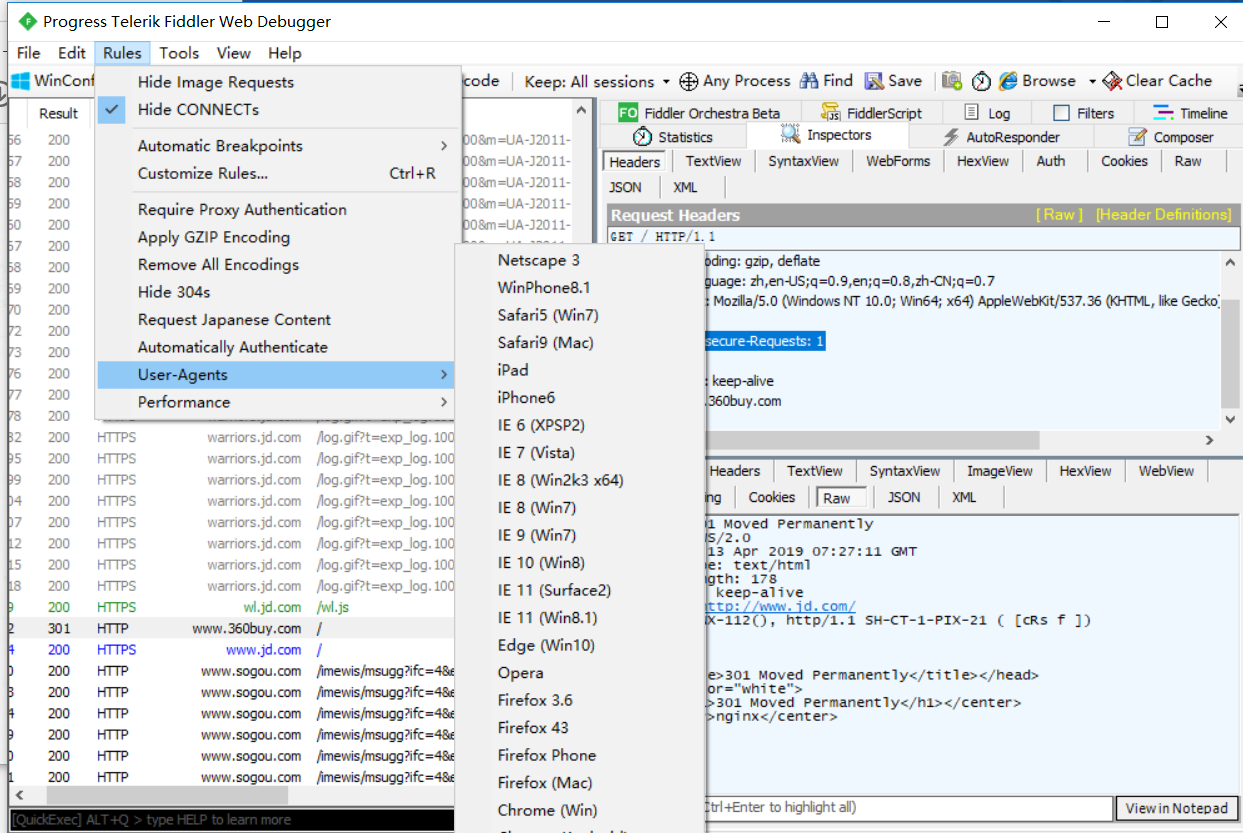
简单来说，当Fiddler当作代理转发HTTPS请求的时候，就会产生“CONNECTTunnels”。这些握手验证请求对我们没什么用处，可以选择在Fiddler中将其隐藏掉。如图2-15所示，选择菜单栏中的Rules->Hide CONNECTS。



## get请求

get方法

## 伪装客户端



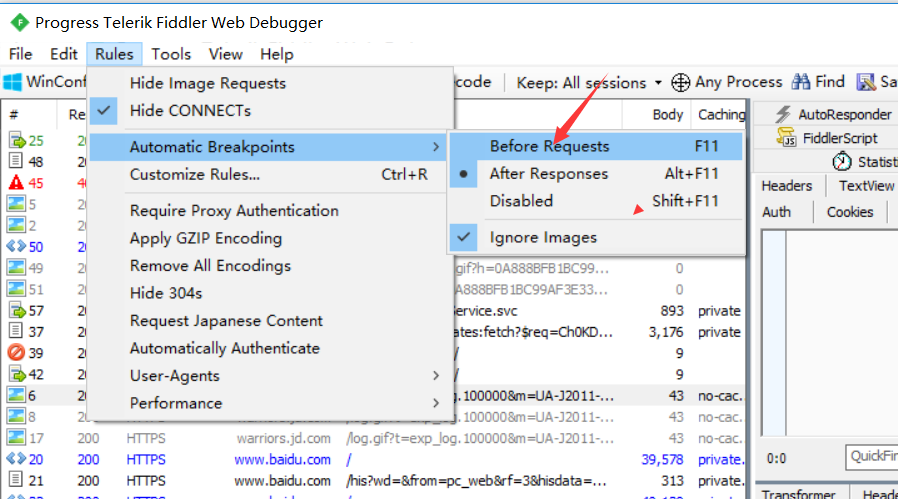
## Fillder修改报文

### 全局断点

第一种叫全局断点。启动Fiddler，单击菜单栏中的Rules->Automatic Breakpoint>Before Requests,或者使用快捷键F11，这种方法会拦截所有的会话。

开启：F11

取消：shift+F11



### 单个断点

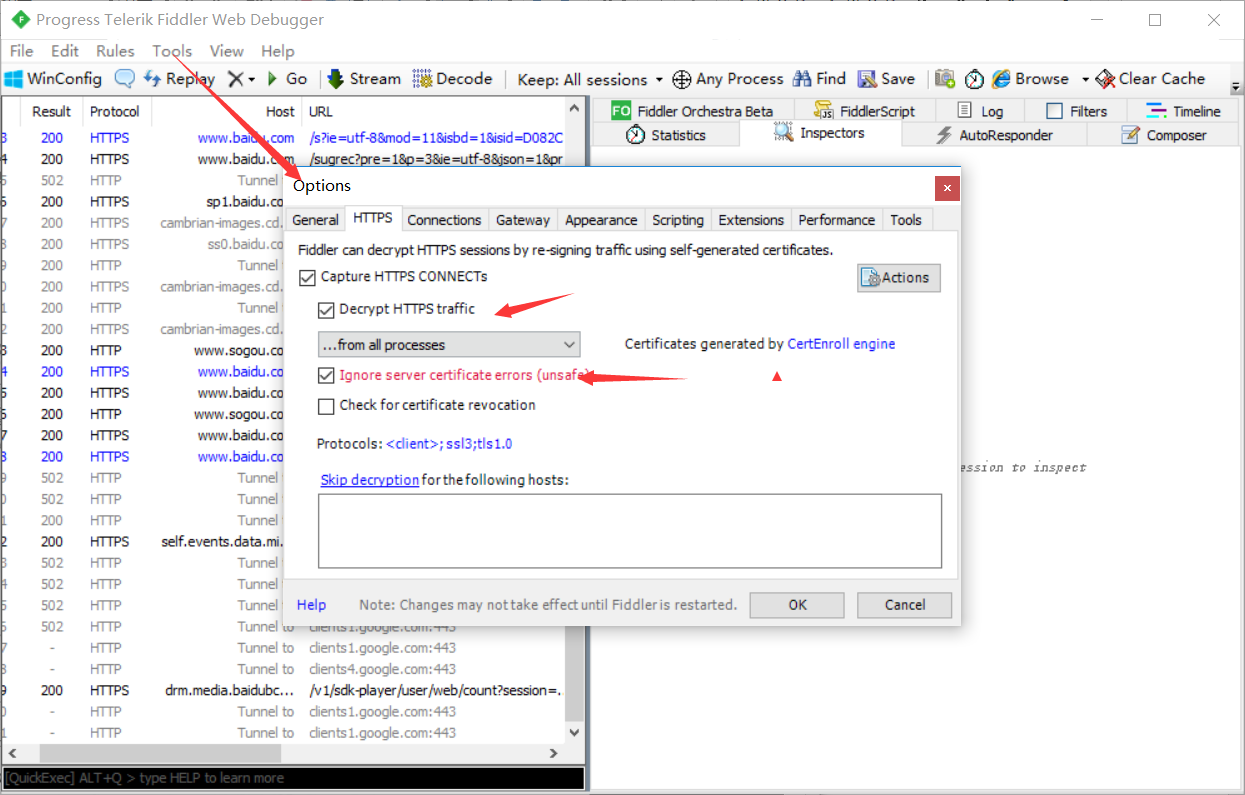
第二种叫单个断点。已知某个请求的URL地址，这时候只需要针对这一个请求打断点调试，其他的请求不拦截。

在Fiddler左下角的QuickExec命令行中输入命令“bpu www.baidu.com”，

所示，这种方法只会拦截www.baidu.com。

## https协议抓包

### 设置

‘’

## QQ抓包

Fiddler能抓到QQ发出的包，当然QQ中发的聊天消息是抓不到的，因为QQ中的聊天信息使用的是OICQ协议，不是HTTP协议。只要在QQ中设置代理服务器即可实现抓包。

### 设置端口

