**Fiddler工具的介绍及使用**

# 一、Fiddler的基本介绍

　　Fiddler官方网站提供了大量的帮助文档和视频教程， 这是学习Fiddler的最好资料。

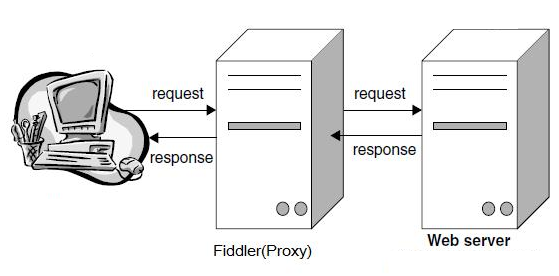
　　Fiddler是最强大最好用的Web调试工具之一，它能记录所有客户端和服务器的http和https请求，允许你监视，设置断点，甚至修改输入输出数据。

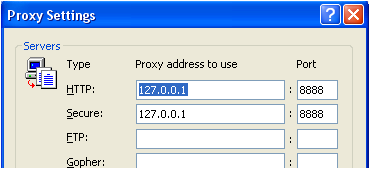
Fiddler无论对开发人员或者测试人员来说，都是非常有用的工具。

Fiddler是一个[http协议](http://baike.baidu.com/view/70545.htm)调试代理工具，它能够记录并检查所有你的电脑和互联网之间的http通讯，设置断点，查看所有的“进出”Fiddler的数据（指[cookie](http://baike.baidu.com/subview/835/5062332.htm),html,js,css等文件，这些都可以让你胡乱修改的意思）。 Fiddler 要比其他的网络调试器要更加简单，因为它不仅仅暴露http通讯还提供了一个用户友好的格式。

# 二、Fiddler的工作原理

　　Fiddler 是以代理web服务器的形式工作的，它使用代理地址:127.0.0.1，端口:8888。当Fiddler退出的时候它会自动注销，这样就不会影响别的程序。不过如果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下Fiddler。





# 三、同类的其它工具

　　同类的工具有: httpwatch, firebug, wireshark

# 四、Fiddler 开启原理

左下角的capturing显示，表示开，不显示表示关，也可以用F12进行开关，或者File菜单下Capture Traffic被勾选，勾选后fiddler才能监控浏览器的一举一动。

代理开关为开：可以抓到包，代理开关为关：抓不到包

浏览器的代理设置默认是关着的，工具--Internet选项--连接--局域网设置--代理服务器

Fiddler在操作时，通过修改注册表的方式，将系统的一些VRnet的代理模式全部给修改掉，改到Tools--Telerik Fiddler Options--Connections自己的代理端口上，默认端口为8888。

如果修改端口，需重启软件件才会生效，就是每次重新开启软件，它会根据你填写的端口打开一个自己的的代理，此时在通过代理开关，比如IE或者系统软件。只要你走系统代理，都可以抓到数据包。

# 版本说明

Fiddler一共2个版本，一个是Fiddler2，一个是Fiddler4，两个版本没有太大的区别，系统底层支持是不一样的，Framework版本不同（.net版本）

Fiddler4支持win8以上

Fiddler2支持winXP（.netk只有2.X版本）、win7（.netk只有3.X版本）

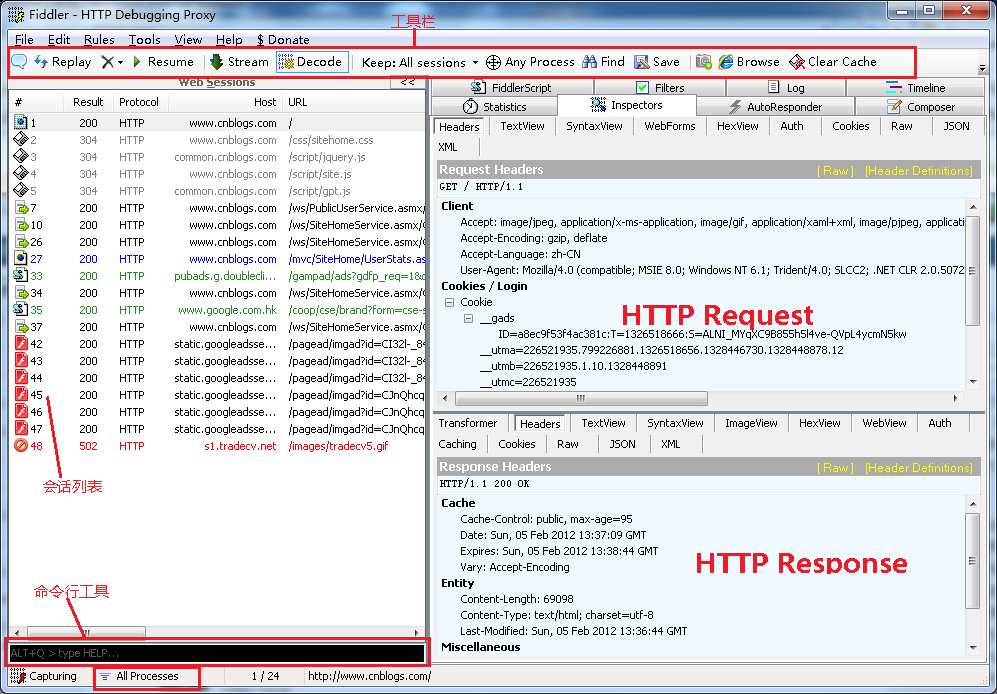
如果win7要安装Fiddler4，会提示安装.net 4.0以上版本

底层并没有太大的区别，最终会影响在做Fiddler插件，因为Framework版本最终决定Fiddler插件版本

建议使用Fiddler4版本，只要升级Framework框架版本到4.0即可。

# 六、Fiddler[界面详解](http://www.cnblogs.com/chengchengla1990/p/5681775.html)

<http://www.cnblogs.com/chengchengla1990/p/5681775.html>



　　QuickExec命令行的使用

　　Fiddler的左下角有一个命令行工具叫做QuickExec，允许你直接输入命令。

　　常见得命令有：

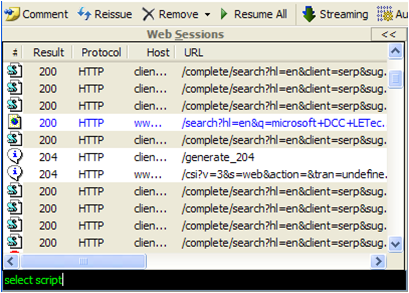
　　help  打开官方的使用页面介绍，所有的命令都会列出来

　　cls    清屏  (Ctrl+x 也可以清屏)

　　select  选择会话的命令

　　?.png  用来选择png后缀的图片

　　bpu  截获request



1. 左边区域：会话列表，记录每一次请求，Fiddler只能抓到HTTP协议和HTTPS协议，自定义的协议抓不到
2. 右边上面两排是功能标签

Inspectors可以看到左侧会话的详细请求

Request出去的请求

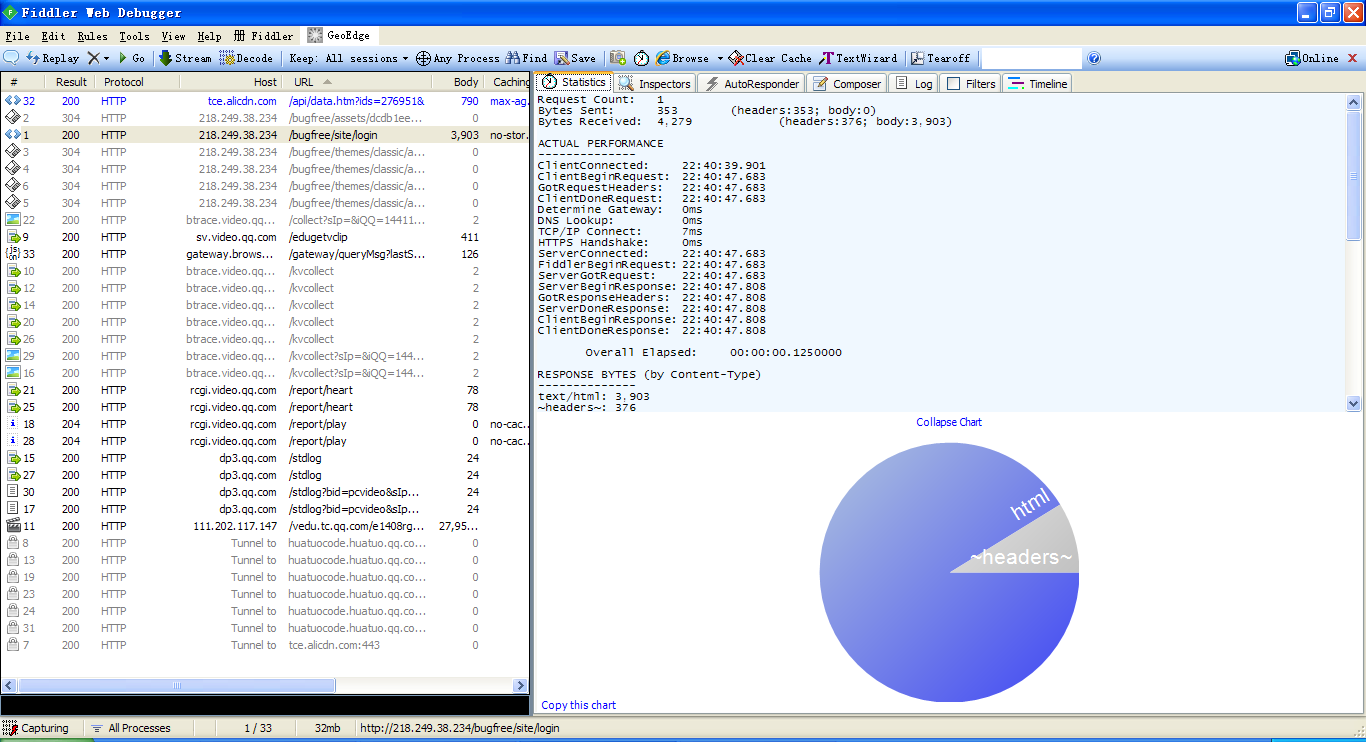
Response返回的信息

Inspectors分上下两部分，Request和Response，中间的标答为显示的格式，内容都是相同的，只是展示的形式不同

1. 下面黑色的是快捷命令，类似于系统中的命令行，中间可以输入命令
2. 最下面的是状态栏

右侧：

1、statistics数据统计



请求数量

发送字节数

服务器响应字节数（响应头-字节，响应正文）

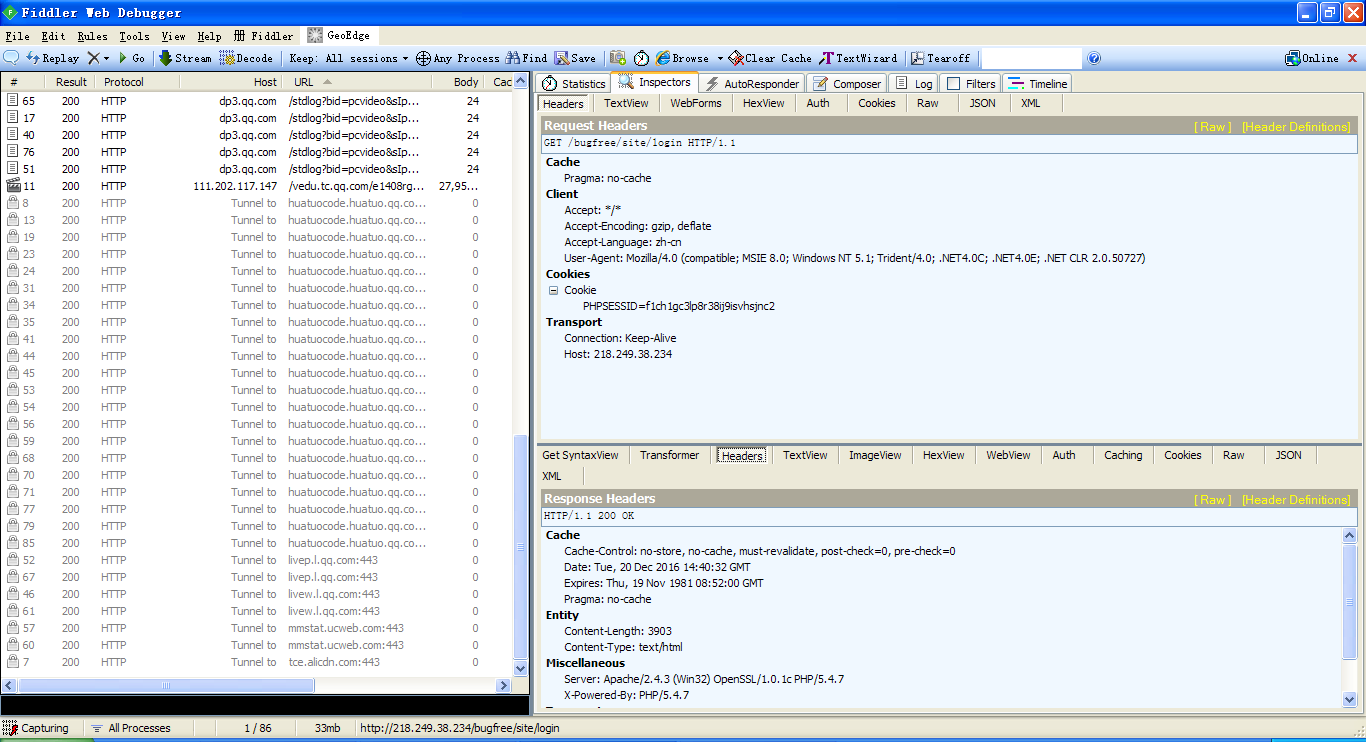
底下是时间片

再往下是不同国家访问这个网站花的时间

2、Inspectors对请求和响应进行查看和分析，监控的请求和响应的内容，上面是请求，下面是响应

Headers上面是请求的头，下面是响应的头

TextView上面的请求的正文，下面是响应的正文，get没有请求的正文，Post有请求的正文，



WebForms显示表单

HexView按16进制显示

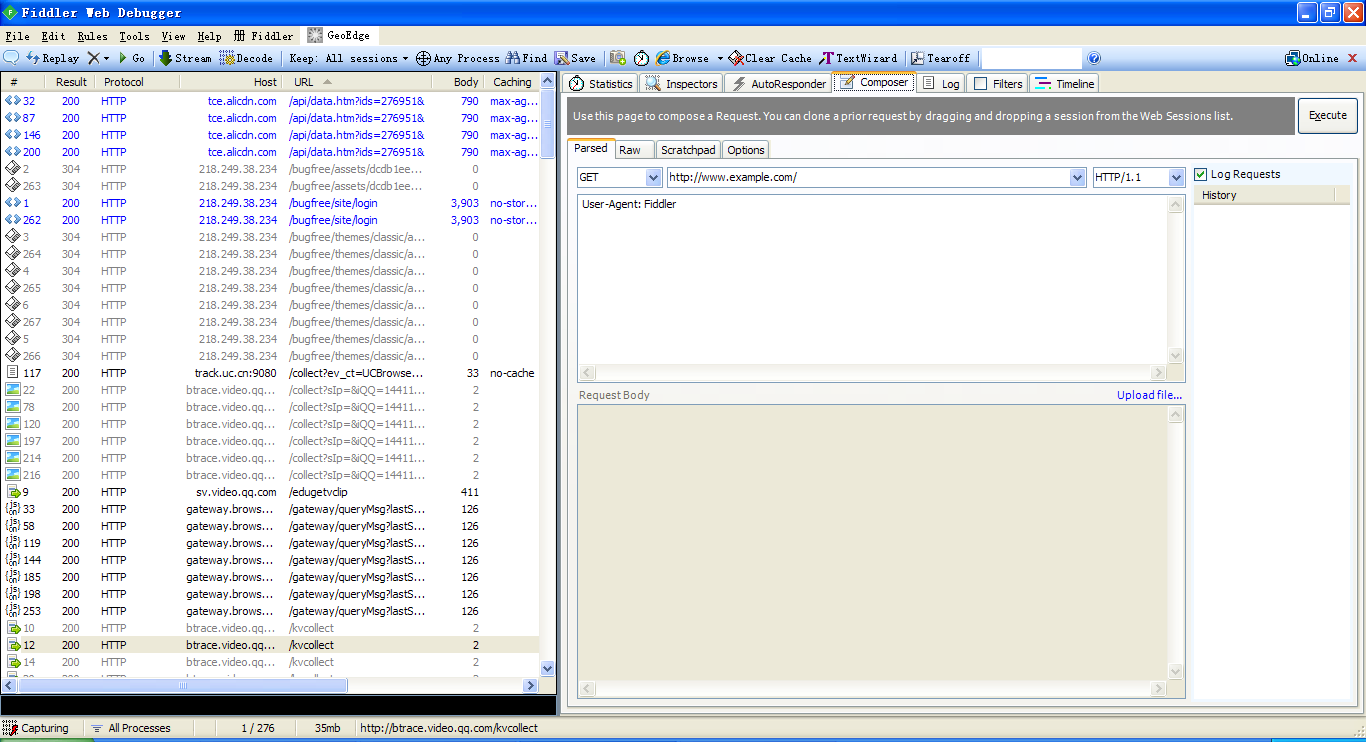
Auth显示网页认证

webView以浏览器的形式查看，目前这个功能在Fiddler4里还有点问题，显示不出来

cookies发送给服务器端的cookies

Raw上面是最原始的请求的内容，下面是最原始的响应的内容

3、Composer对请求进行编辑



选中左侧Post请求，右键Replay—Reissue and Edit(重新编辑和发布请求)

# 抓包代理设置

1. 火狐拥有一套独立的代理，它使用的不是系统代理，所有代理开关，开或者关，都抓不到包

火狐：工具--选项--高级--设置--使用系统代理设置，或手动配置代理设置，这样无论代理开/关都可以抓到包

1. 本机安装Fiddler，抓取其他机器上的浏览器数据包方法？

手动配置代理设置，输入对方机器的IP和端口，Fiddler默认只会开启本地，不会开启远程的。

如何开启远程？

Tools--Telerik Fiddler Options中勾选Allow remote computers to connect勾选后会弹出警告，让重启Fiddler，如果还是访问不通的话，注意把防火墙关掉。

Fiddler监听IP：cmd中输入netstat ano | find “9999”

0.0.0.0:9999意思是无论内网外网都可以连

192.168.0.0：9999只能连内网

# 手机抓包

1. 勾选Allow remote computers to connect
2. 安卓手机打开wifi，长按一个网络，打开高级选项，选择手动代理，填写Fiddler所在机器的IP和Fiddler端口，前提是手机和电脑在同一个网络，同一个wifi肯定是可以的。
3. 苹果IOS，打开wifi，选择网络，设置为手动代理，填写ip和端口

# HTTPS抓包设置

SSL安全套接协议

https是用SSL加密保护的，电脑与服务器之间收发的信息传输将更加安全。

Http与https使用不同的连接方式，端口也不一样，http端口是80，https端口443，更安全，加密传输，身份证认的网络协议。

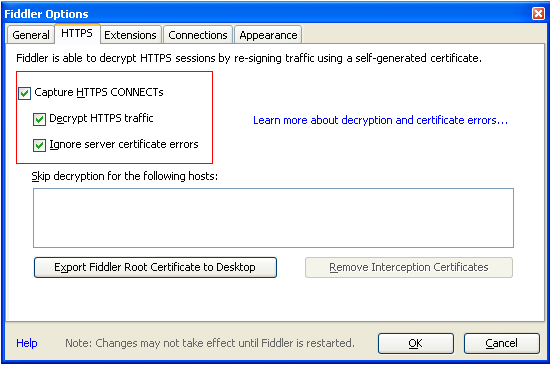
如何解密：<https://www.baidu.com>

Tools--Telerik Fiddler Options 勾选Decrypt Https traffic

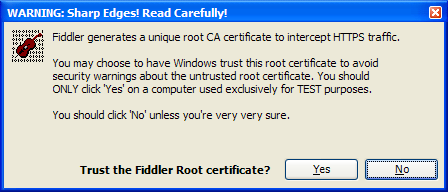
在握手的时候做了一个浏览器和服务器之间做了证书的密钥交换。Ie和Fiddler用的都是windows底层的证书管理，如果其他浏览器用的也是系统自带的证书，也是可以抓包的。

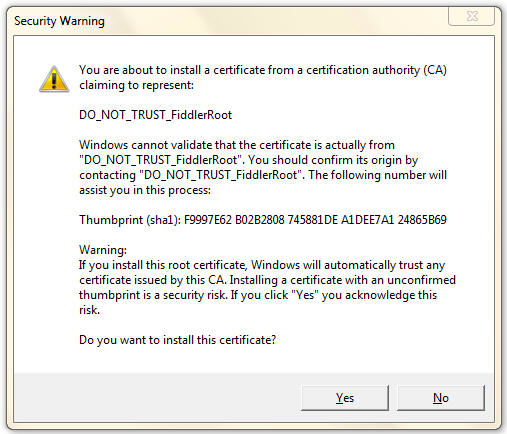
火狐是一个全面独立的浏览器，没办法抓包，因为证书不一样。

　　默认下，Fiddler不会捕获HTTPS会话，需要你设置下， 打开Fiddler  Tool->Fiddler Options->HTTPS tab



　　选中checkbox， 弹出如下的对话框，点击"YES"





　　点击"Yes" 后，就设置好了。

# Firefox下HTTPS抓包

Firefox与Fiddler证书不一致，如何抓包？

导出证书：Tools--Telerik Fiddler Options 勾选Decrypt https traffic，点击Actions--Export Root Certificate to Desktop导出到桌面，然后再导入到火狐证书中：工具--选项--高级--证书--证书机构--导入--桌面的FiddlerRoot.cer--勾选第1个“信任使用止CA标识的网站”--确认--确定。

再次访问百度，就可以解密，因为我们把Fiddler的证书拷贝给火狐了。

# 抓取手机端HTTPS包

跟火狐一样，因为证书不一样，所以抓不到

因为无法给手机导入证书，需要用浏览器访问一个地址，然后直接安装一个证书，地址是Fiddler的ip和端口，http://192.168.31.118:8888/

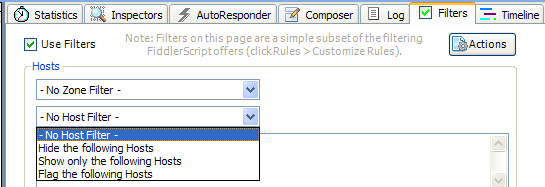
访问后看最下面一行是证书的地址，FiddlerRoot certificate点击证书地址，安装证书时会根据手机情况让输入解锁密码，如果没有需要设置，安装证书一定要用手机默认的浏览器。

# 域名过滤

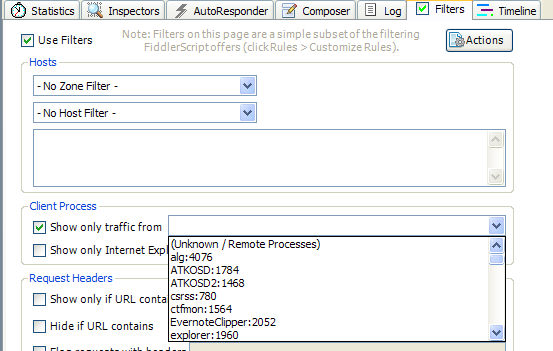
Hide the following Hosts隐藏host，就是写了哪个host，就不显示哪个

Show only the following Hosts只显示写出来的host

Flag the following Hosts标记，显示出来，但是可以打个标记



# 进程过滤



# Fiddler中设置断点修改Request

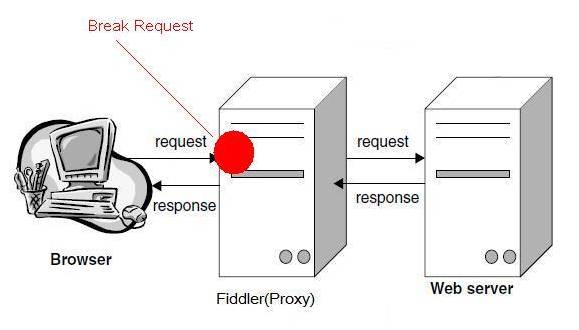
　　Fiddler最强大的功能莫过于设置断点了，设置好断点后，你可以修改httpRequest的任何信息包括host, cookie或者表单中的数据。设置断点有两种方法：

　　第一种：打开Fiddler 点击Rules-> Automatic Breakpoint  ->Before Requests(这种方法会中断所有的会话)

　　如何消除命令呢？  点击Rules-> Automatic Breakpoint  ->Disabled

　　第二种:  在命令行中输入命令:  bpu www.baidu.com   (这种方法只会中断www.baidu.com)

　　如何消除命令呢？  在命令行中输入命令 bpu



　　看个实例，模拟博客园的登录， 在IE中打开博客园的登录页面，输入错误的用户名和密码，用Fiddler中断会话，修改成正确的用户名密码。这样就能成功登录：

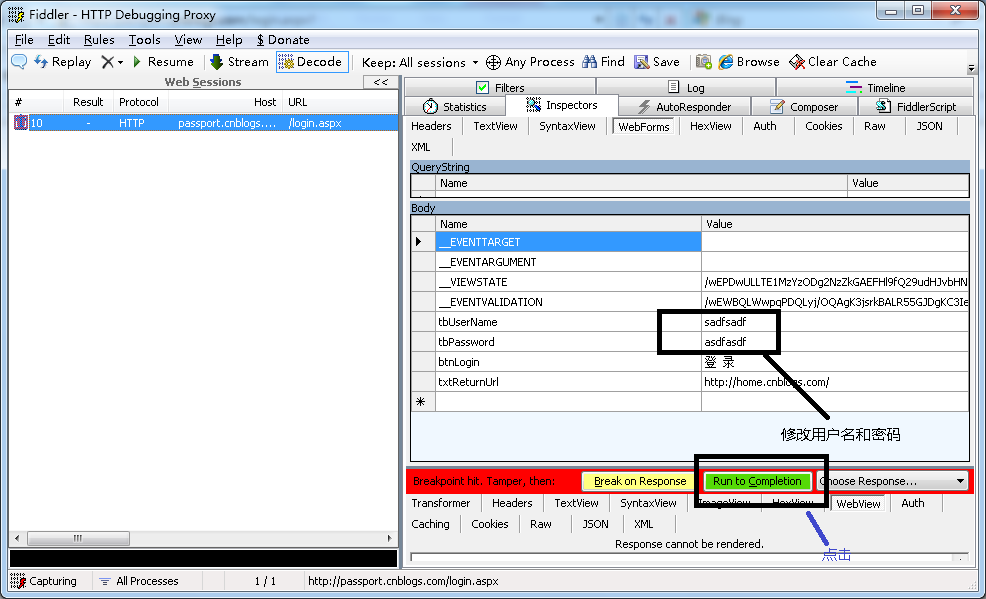
　　1. 用IE 打开博客园的登录界面  http://passport.cnblogs.com/login.aspx

　　2. 打开Fiddler,  在命令行中输入bpu http://passport.cnblogs.com/login.aspx

　　3. 输入错误的用户名和密码，点击登录

　　4. Fiddler 能中断这次会话，选择被中断的会话，点击Inspectors tab下的WebForms tab 修改用户名密码，然后点击Run to Completion 如下图所示。

　　5. 结果是正确地登录了博客园



# Fiddler中设置断点修改Response

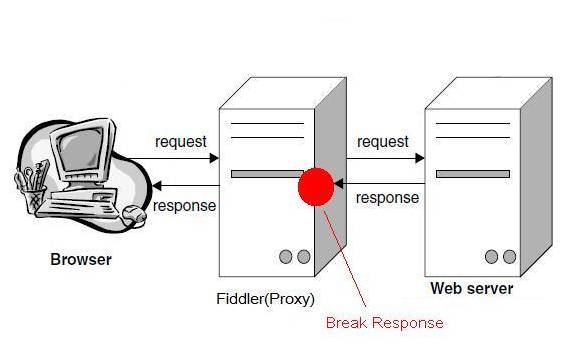
　　当然Fiddler中也能修改Response：

　　第一种：打开Fiddler 点击Rules-> Automatic Breakpoint  ->After Response  (这种方法会中断所有的会话)

　　如何消除命令呢？  点击Rules-> Automatic Breakpoint  ->Disabled

　　第二种:  在命令行中输入命令:  bpuafter www.baidu.com   (这种方法只会中断www.baidu.com)

　　如何消除命令呢？  在命令行中输入命令 bpuafter,



　　具体用法和上节差不多，就不多说了。

# Fiddler中创建AutoResponder规则

　　Fiddler 的AutoResponder tab允许你从本地返回文件，而不用将http request 发送到服务器上。

　　看个实例：

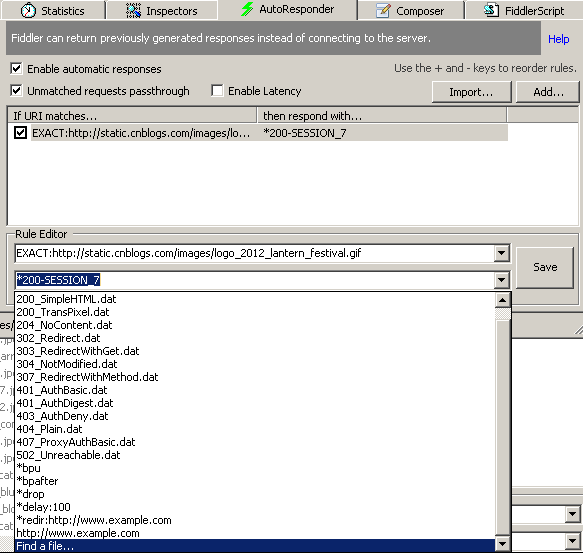
　　1. 打开博客园首页，把博客园的logo图片保存到本地，并且对图片做些修改。

　　2. 打开Fiddler 找到logo图片的会话， http://static.cnblogs.com/images/logo\_2012\_lantern\_festival.gif，  把这个会话拖到AutoResponer Tab下

　　3. 选择Enable automatic reaponses 和Unmatched requests passthrough

　　4. 在下面的Rule Editor 下面选择 Find a file... 选择本地保存的图片.  最后点击Save 保存下。

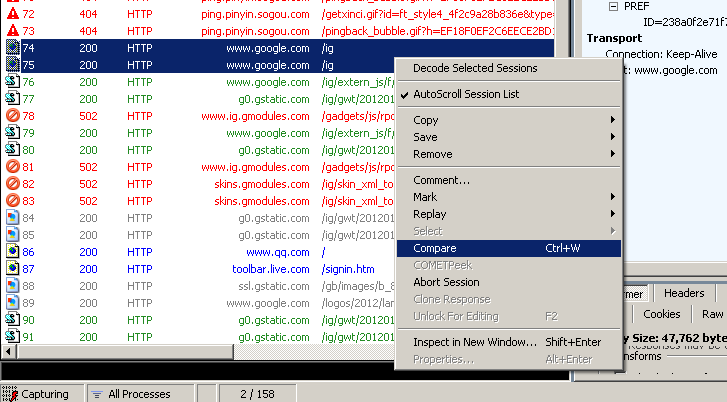
　　5.   再用IE博客园首页， 你会看到首页的图片用的是本地的。





# Fiddler中会话比较功能

　　选中2个会话，右键然后点击Compare，就可以用WinDiff来比较两个会话的不同了（当然需要你安装WinDiff）



# Fiddler中查询会话

　　用快捷键Ctrl+F打开Find Sessions的对话框，输入关键字查询你要的会话。 查询到的会话会用黄色显示。



# Fiddler中保存会话

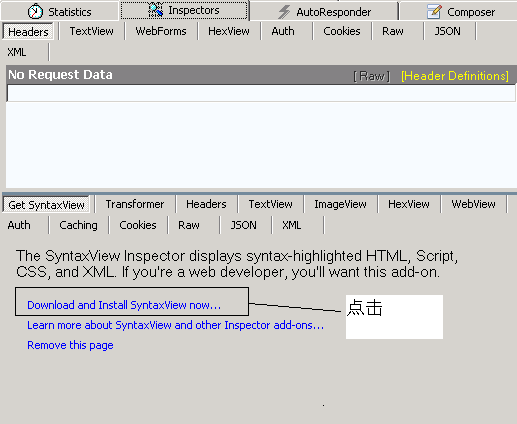
　　有些时候我们需要把会话保存下来，以便发给别人或者以后去分析。  保存会话的步骤如下：

　　选择你想保存的会话，然后点击File->Save->Selected Sessions

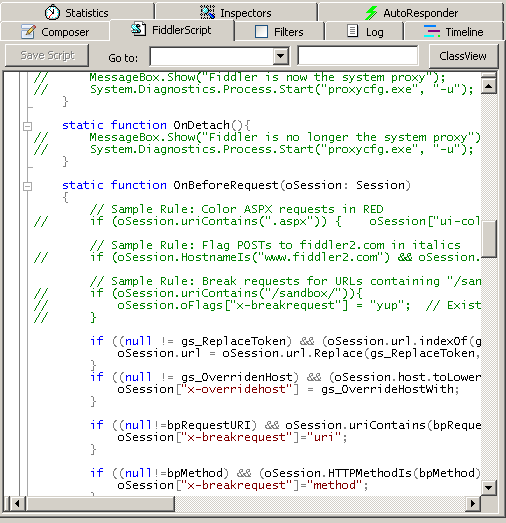
# Fiddler的script系统

　　Fiddler最复杂的莫过于script系统了，官方的帮助文档:<http://www.fiddler2.com/Fiddler/dev/ScriptSamples.asp>。

　　首先先安装SyntaxView插件，Inspectors tab->Get SyntaxView tab->Download and Install SyntaxView Now... 如下图



　　安装成功后Fiddler 就会多了一个Fiddler Script tab，如下图：



　　在里面我们就可以编写脚本了， 看个实例让所有cnblogs的会话都显示红色。

　　把这段脚本放在OnBeforeRequest(oSession: Session) 方法下，并且点击"Save script"

if (oSession.HostnameIs("www.cnblogs.com")) {

　　oSession["ui-color"] = "red";

}

　　这样所有的cnblogs的会话都会显示红色。

# 如何在VS调试网站的时候使用Fiddler

　　我们在用visual stuido 开发ASP.NET网站的时候也需要用Fiddler来分析HTTP， 默认的时候Fiddler是不能嗅探到localhost的网站。不过只要在localhost后面加个点号，Fiddler就能嗅探到。

　　例如：原本ASP.NET的地址是 http://localhost:2391/Default.aspx，  加个点号后，变成 http://localhost.:2391/Default.aspx 就可以了

