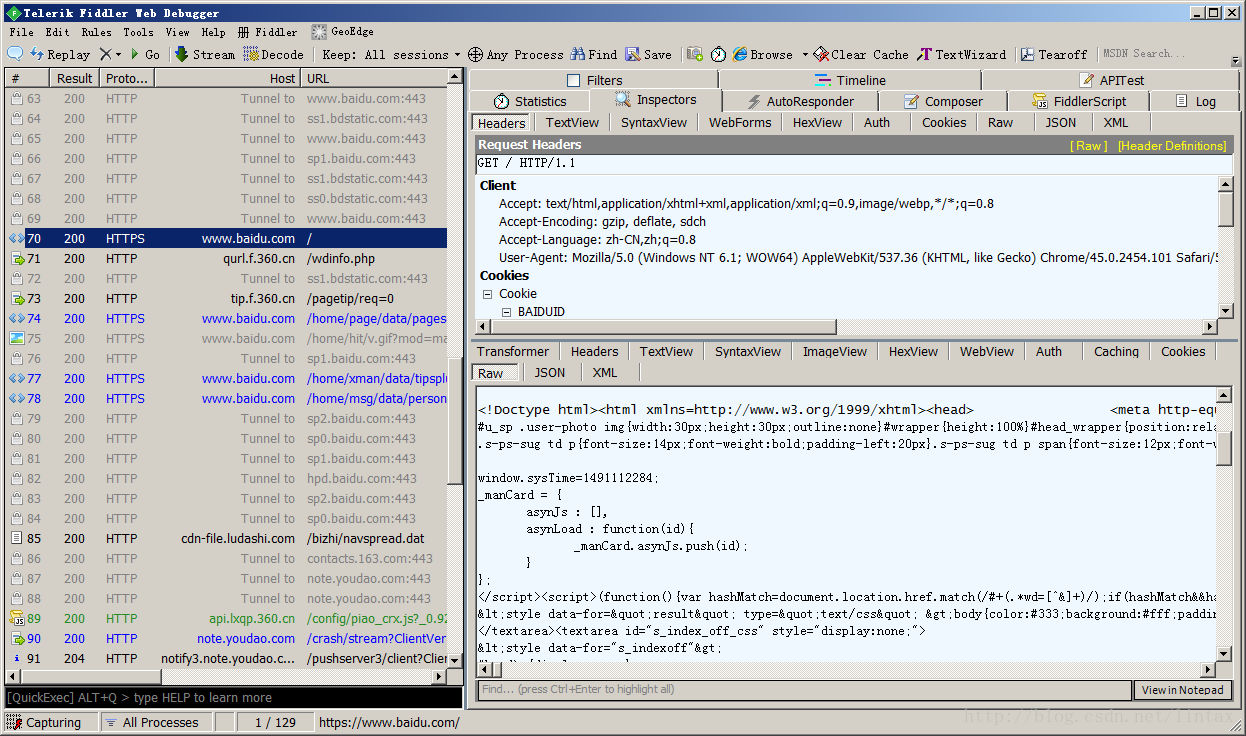
在Android开发过程中，经常会调整网络接口，这时就需要测试网络请求的正常、异常各种情况的处理，是否都符合我们的预期。通常情况下，是跟服务器端来一起联调，然而，有些时候却不具备条件，或者由于服务器端还没有开发好，或者某些异常不好出现，这时候，如果能模拟服务器端的各种返回情况就好了。幸好，已经有了这种工具了，例如Fiddler。

Fiddler是一个http调试代理，它能够记录所有的经过它代理的http通讯数据，包括电脑上浏览器访问互联网，或者手机通过wifi代理上网的数据。相比较于监视所有通过网卡的数据的Wireshark来说，Fiddler 要更加简单，因为它仅仅暴露http通讯，并且还提供了一个用户友好的界面。

下面，我就如何对手机上的网络调试来说明下步骤：

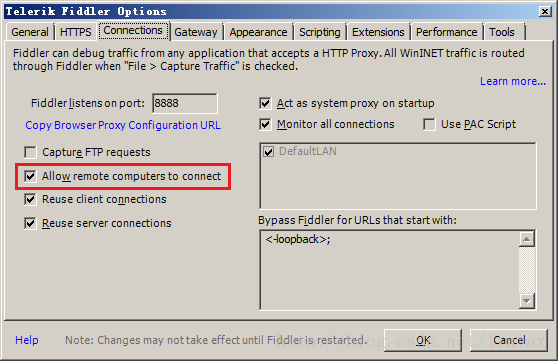
一、安装Fiddler

1. 下载Fiddler，其官方下载地址：<https://www.telerik.com/download/fiddler>。
2. 下载完成后，安装到电脑，按默认步骤按照即可。
3. 打开Fiddler软件，界面效果图如下：   
   

选中查看的那条请求是[https://www.baidu.com](https://www.baidu.com/)的，看右侧分上下两部分，上部分是http的Header，下部分是html页面内容，熟悉html的同学多看看，就知道那其实就是百度的主页面啦。当然，更好的方式是直接在百度页面下，查看下源码，比较一下，完全一样的啦。

二、使用Fiddler对手机抓包

下面我们就进入重点了，对手机的http请求进行抓包。   
1，首先，确保安装 Fiddler 的电脑和要调试的手机在同一局域网内，因为Fiddler只是一个代理，需要将手机的代理指向 PC 机。我是在电脑上插了个随身wifi，运行起来，然后手机连接上这个wifi来上网。   
2，开启Fiddler的远程连接，Fiddler 主菜单 Tools ->Fiddler Options…-> Connections页签，选中Allowremotecomputers to connect。效果图如下：

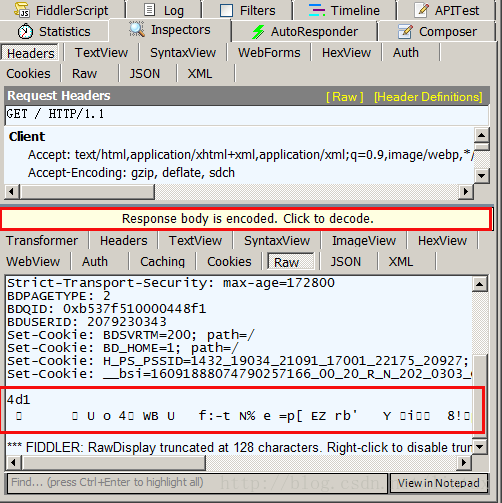


3， 开启好远程连接之后，重启Fiddler，不然就不会更新你刚开启的远程配置   
4，下面开始设置手机端了，获取PC的IP地址，我的IP地址是：192.168.2.121   
5，打开你的手机设置界面：

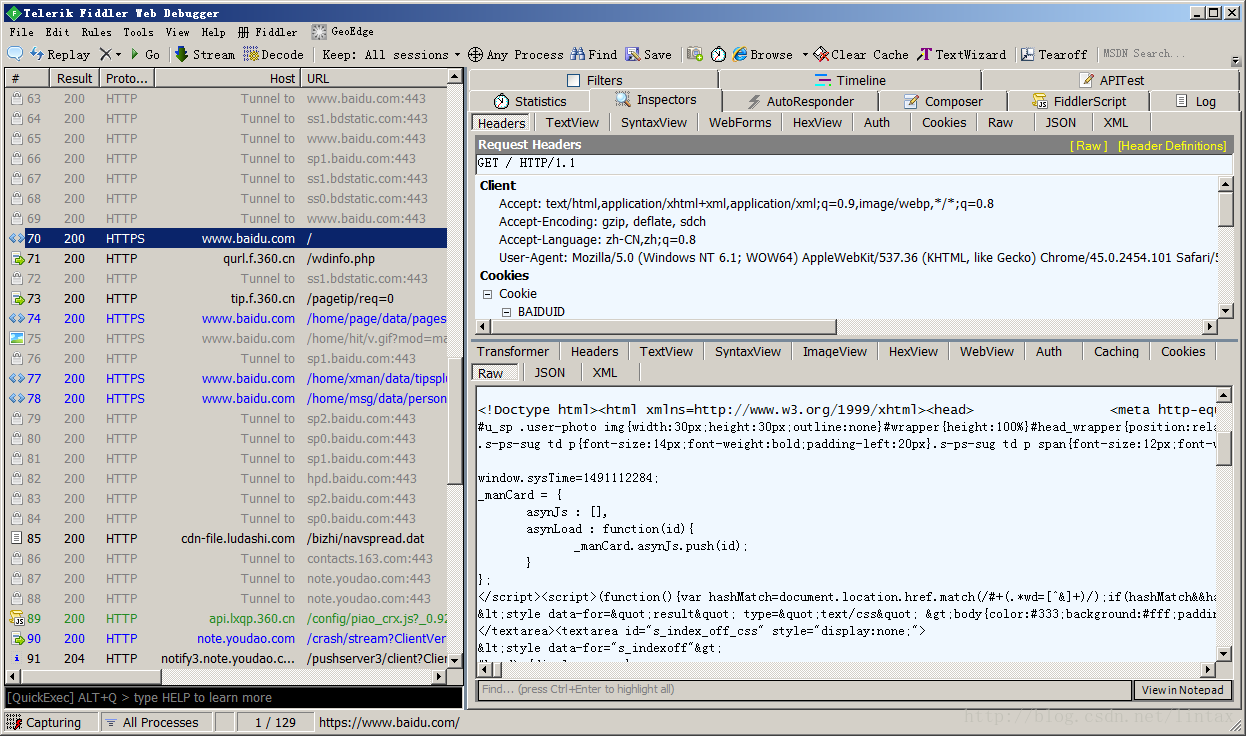




6，现在就可以开始抓包了：打开Fiddler软件，然后启动android设备中的浏览器，访问百度的首页，在fiddler中可以看到完成的请求和响应数据。   
不过，我下载的fiddler版本，对于收取到的服务器的响应数据，还需要做一次解码，见下图：



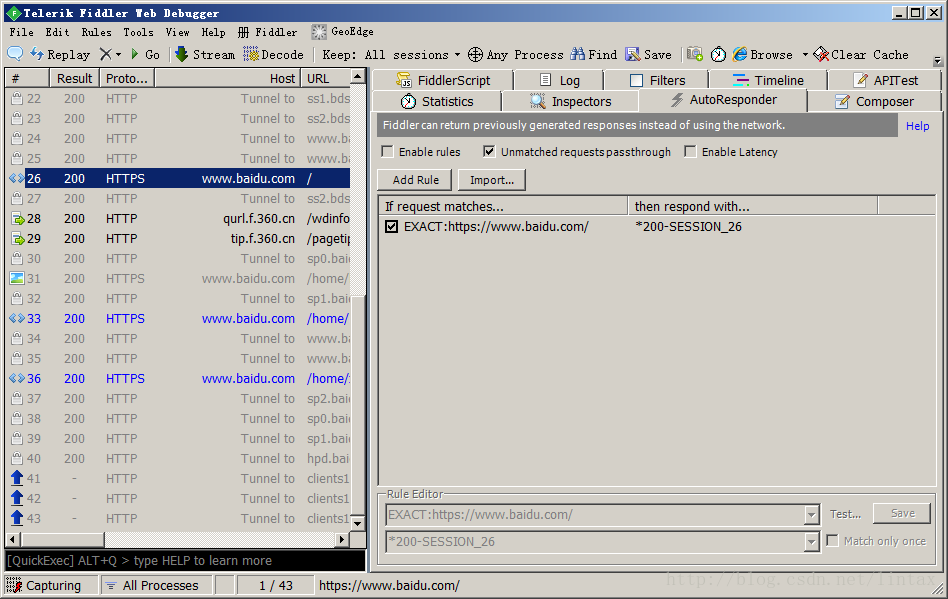
下面那个红框里面是乱码，需要进行一次解码，就是在上面红框那里点击一次，才能看到返回的body数据。   
下图是解码后的：



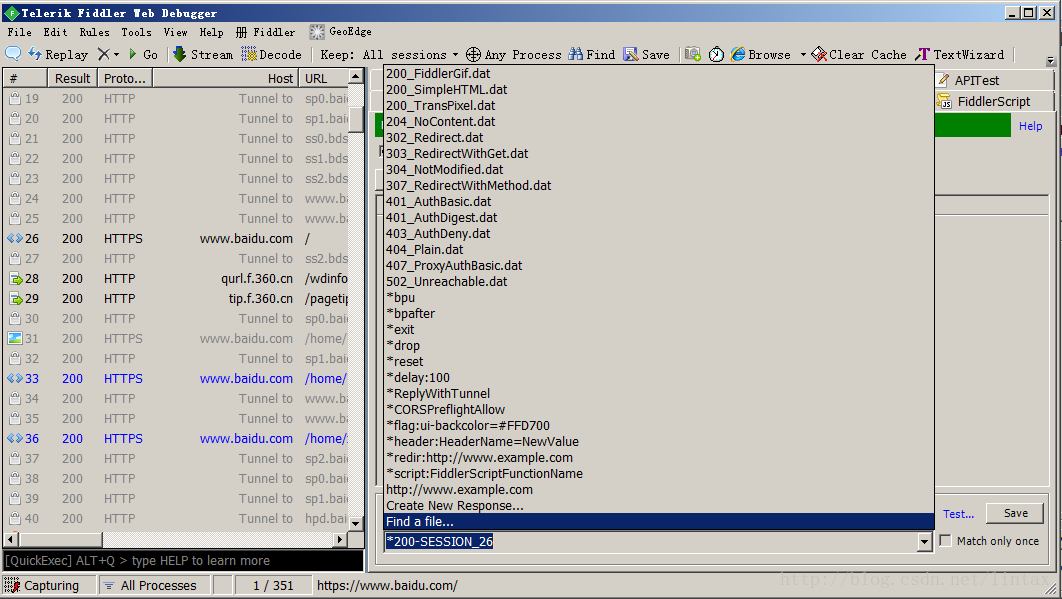
三、使用fiddler模拟服务端返回

现在，我们来修改下请求的返回：   
选中访问百度的那条http请求，在右侧选择AutoResponder的tab页，有没有看到界面上有两个复选框？第一个的作用是开启或禁用自动重定向功能，我们就可以在下面添加重定向规 则了。第二个复选框框勾上时，不影响那些没满足我们处理条件的请求。

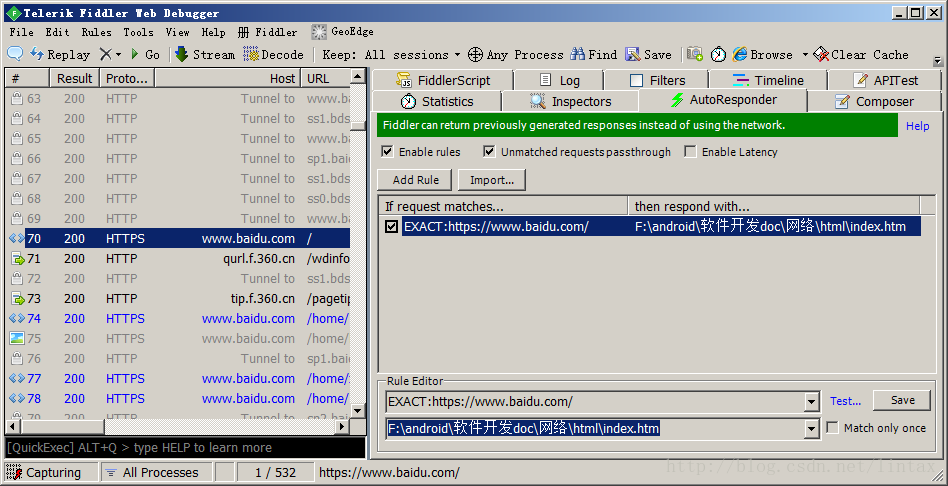
然后创建重定向规则：   
我们可以通过“Add…”按钮手动添加规则，不过这个URL已经出现在我们的session列表中，可以直接拖动过来。在左侧的Session列表 中选择第一步找到的session，拖动到AutoResponse标签中。这样就创建了一个针对这个URL的规则。



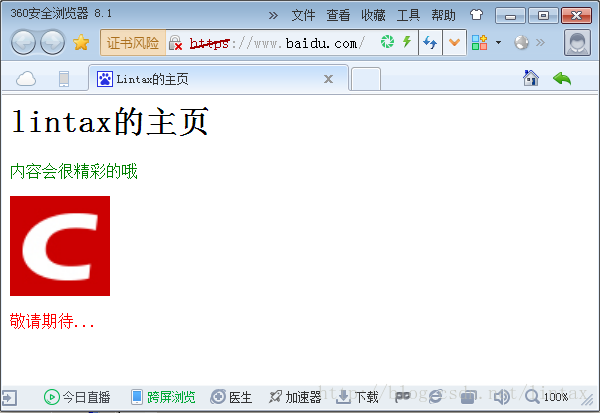
Fiddler帮我们生成的规则是：   
当URL为：<https://www.baidu.com/>   
返回200，使用和Session 26一模一样的内容返回   
· 我们可以修改这个规则：



· 选择“Find a file…”，就可以选择本地的文件作为返回的body内容。

选择一个我们自己写的html页面，例如我用的是一个index.htm。   
刷新一下浏览器页面，看一下session列表，如果像下面这样，那么恭喜你，你已经成功将这个请求重定向到本地文件了！   


让我们来看看效果吧，从浏览器里面输入www.baidu.com，回车执行，结果如下：



页面中的地址是<https://www.baidu.com/>，但是页面里面的内容，是我写的一个简单的页面，内容如下：

<html>

<head>

<title>Lintax的主页</title>

</head>

<body>

<h1>lintax的主页</h1>

<p><font color="green">内容会很精彩的哦</font></p>

<img src="http://c.csdnimg.cn/public/favicon.ico" width="100" />

<p><font color="red">敬请期待...</font></p>

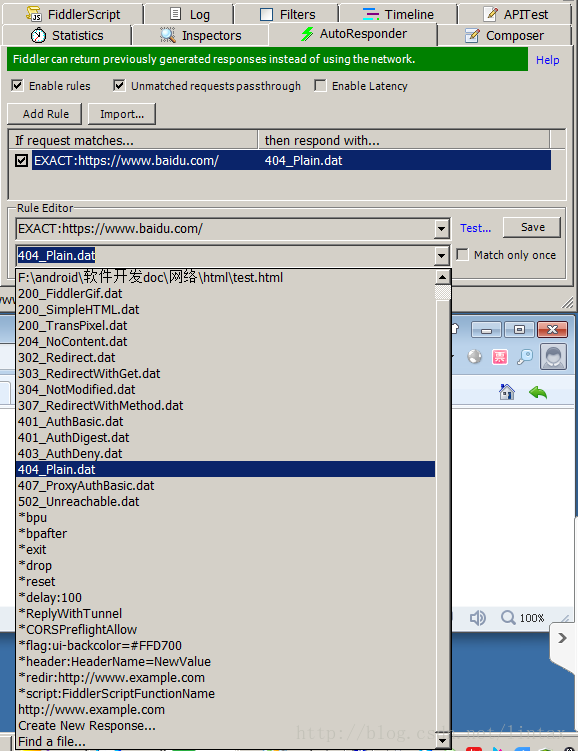
</body>

</html>

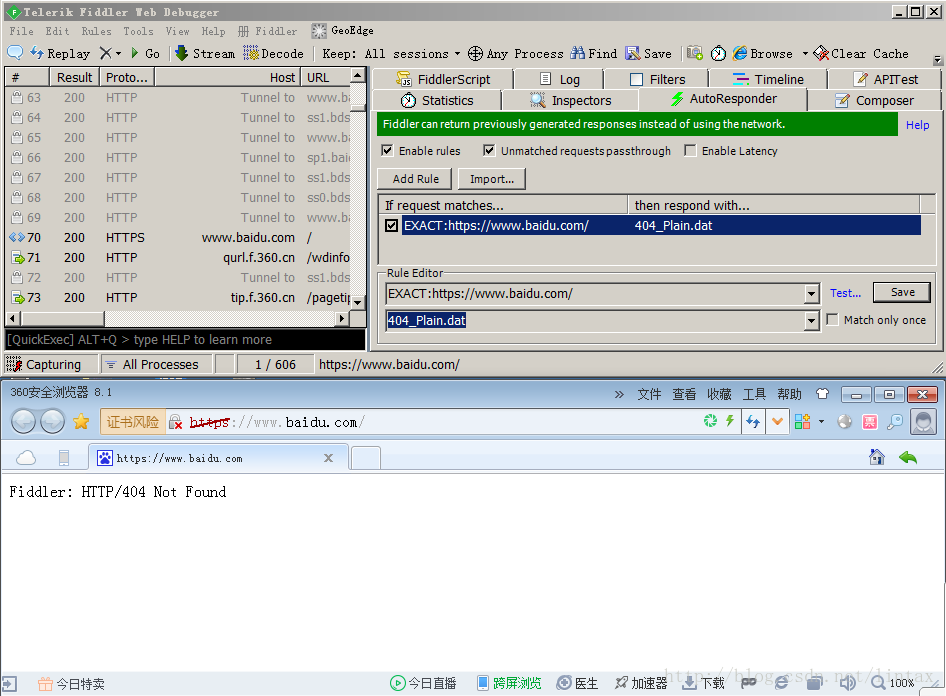
* 1
* 2
* 3
* 4
* 5
* 6
* 7
* 8
* 9
* 10
* 11

这样的效果是不是很震撼，不了解内情的人，直接就懵比了！   
这在网络攻防里面有个名称，叫“中间人攻击”，中间人就是代理，就是咱们使用的fiddler啦。   
当然，从图片中能看到有一个明显的异常，标红的，就是地址前面的图标，以及报出的“证书风险”，这是因为百度的访问使用的https，会有证书检查，发现异常了。若是没有是有https的，从地址栏那里是完全看不出问题来的。   
所以，大家使用手机时，不要随意使用不清楚来由的wifi哦。对于自建的网站，尽量的使用https吧，否则，数据都被中间人截取到了。

当然，我们关注的还是返回数据进行调试Android程序，接下来，就是模拟一些异常的返回：



这里，我们以返回404错误为例，设置上之后，“save”一下，然后再次在浏览器输入www.baidu.com，回车执行，结果如下：



这样设置好之后，对应的，在android端调试，就可以跟踪相关的调试信息了，看这种异常逻辑分支是否能正常处理。

至此，本文总结了如何使用Fiddler对手机进行抓包分析，以及模拟服务器端返回数据及异常的方法，在实际工作中，fiddler能有效提升我们对网络的调试效率。

参考：

<http://blog.csdn.net/zshq280017423/article/details/8928616>   
<http://www.51testing.com/html/84/359684-852462.html>   
<http://www.aliued.cn/?p=2581>