测试文档：

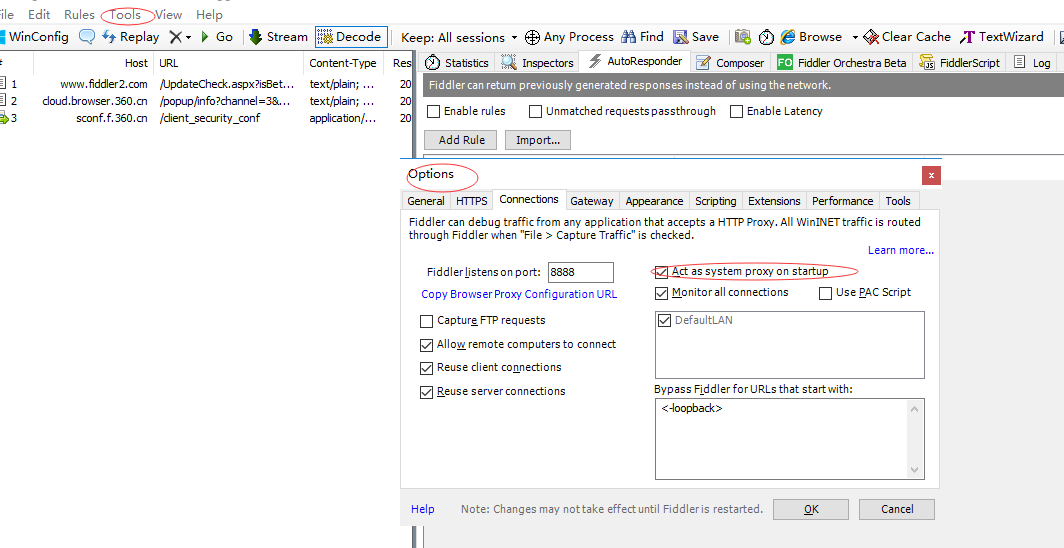
工号：GOS0537

邮箱：wb.fuzaohe@mesg.corp.netease.com

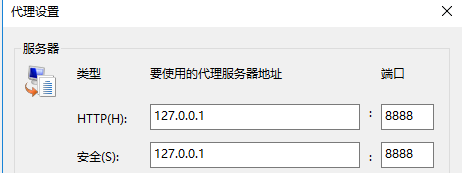
Fiddler配置代理，断点，自动回复功能，https代理功能，报文头和报文体查看，响应体查看。

1：Fiddler设置代理方法：当浏览器访问时，就可以实现http浏览器抓包。

第一步：Toos->options->勾选Act as system proxy on startup



第二步：点击需要代理的浏览器端口和地址，该端口必须和上图的端口一致才可以实现抓包效果（8888），默认情况下代理是自己启动的，除了火狐浏览器

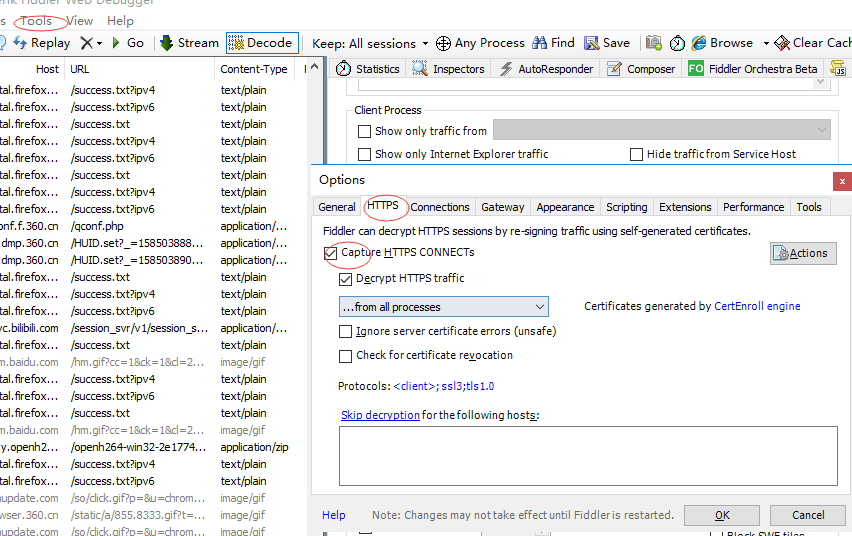


火狐浏览器配置方法：

打开浏览器后，点击工具->选项->高级->网络->设置或者直接在设置搜索框中去搜索：代理服务器，并点击手动配置将上面的地址和端口进行填写。

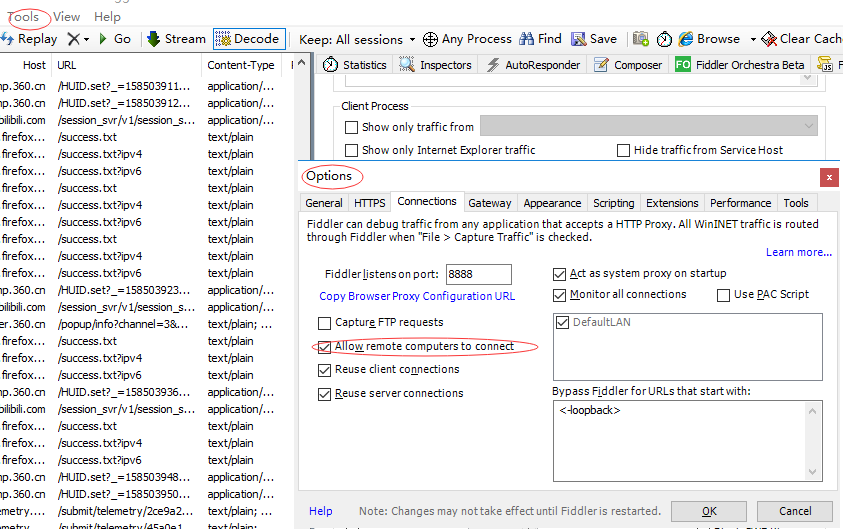


如果需要去捕捉Https的包，可以通过设置：Tool -> Options -> HTTPS，勾选上“Decrypt HTTPS traffic”设置图下图所示：

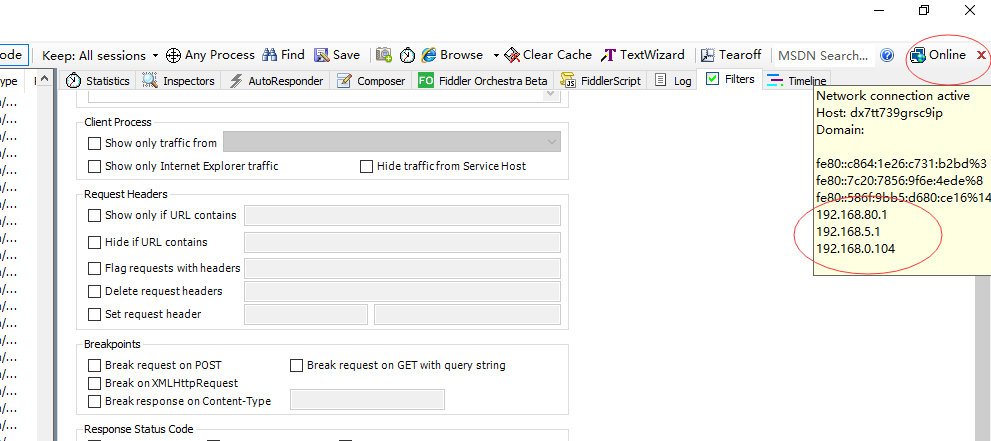


1. 移动端的抓包方法：

第一步：Toos->options->勾选Allow remote computers to connect

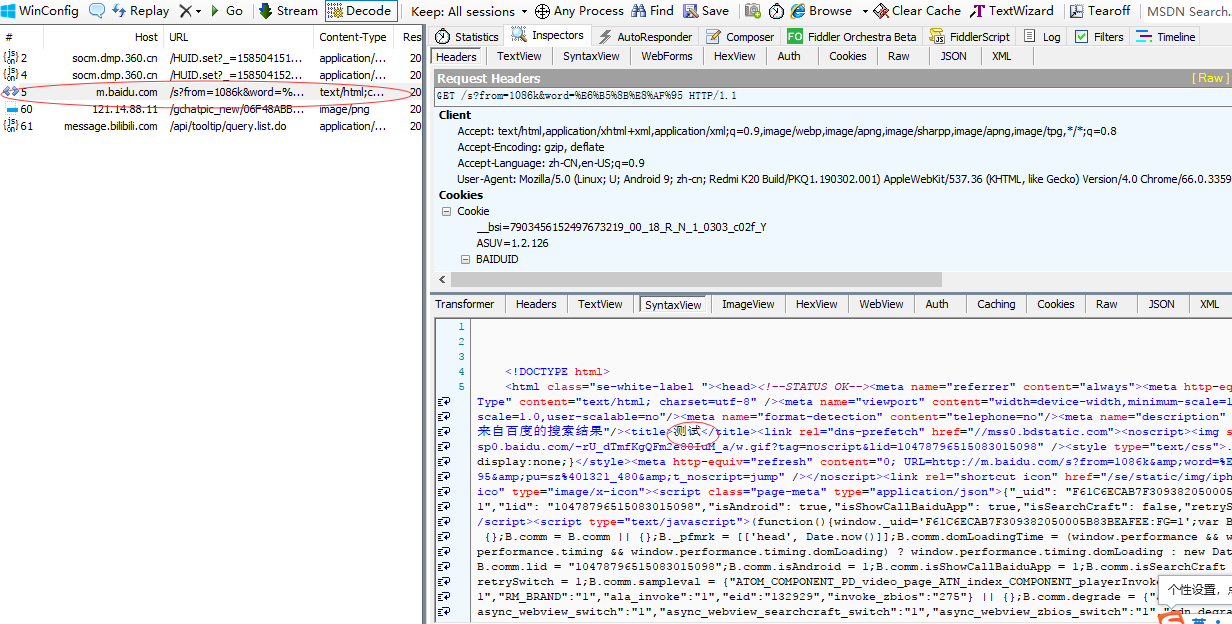


第二步：获取本电脑机器的IP地址 即命令行中输入ipconfig可以查看。或者在fiddler界面的Online中可以查看（这里要求电脑连接的网络要跟手机的网络要求是同一个网络）



第三步：打开手机的wifi并且设置他的端口号和IP地址：

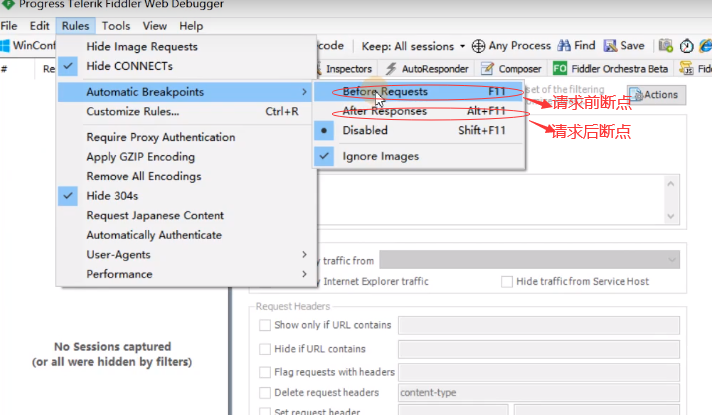


手机进行访问，就可以抓到手机端的包了（这里我们访问www.baidu.com输入测试）

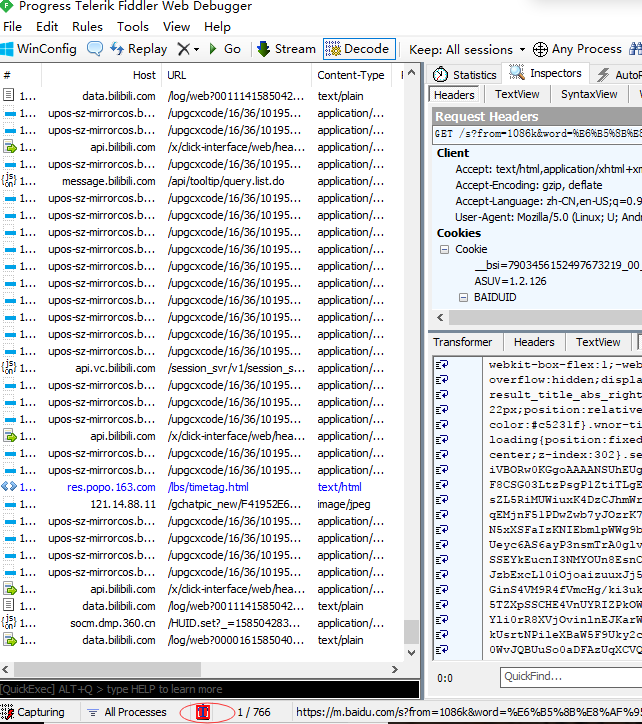
注意：如果想要抓https的包需要在手机浏览器中输入该电脑的地址加端口号进行安装证书。

2：断点的应用：用于接口调试做数据篡改用。

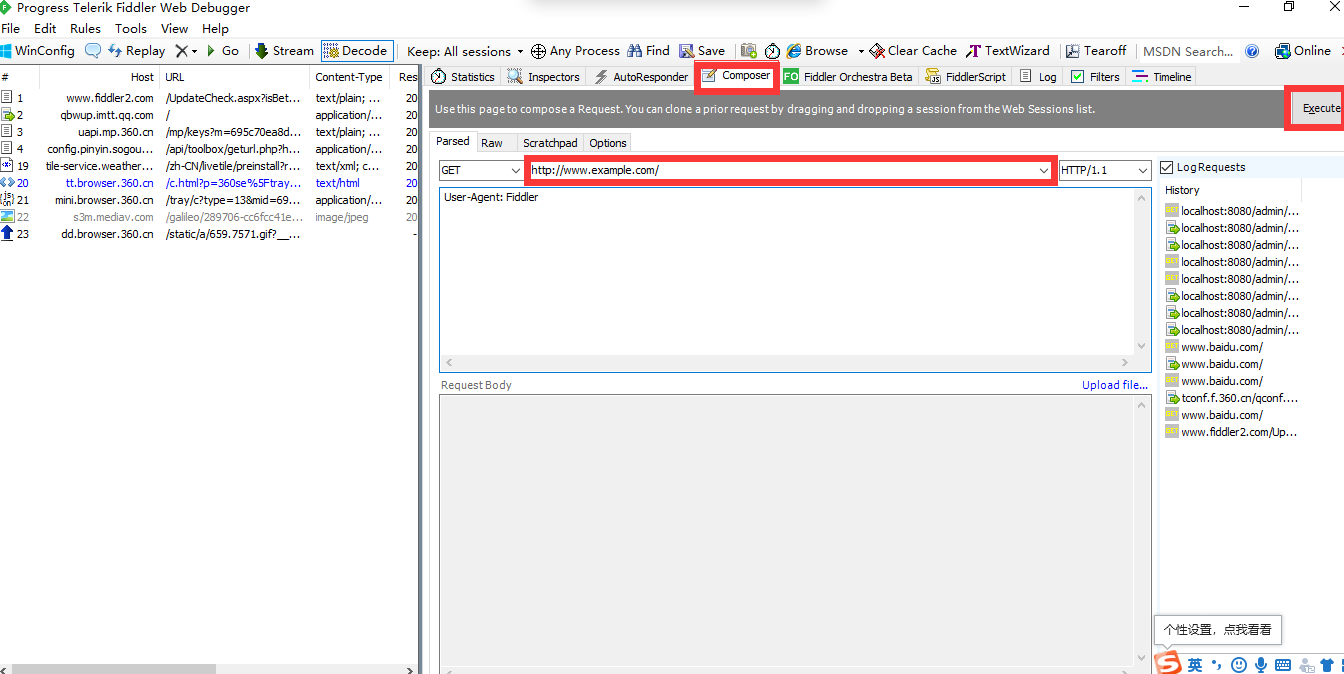
Rules->Automatic Breakpoints->Before Requests



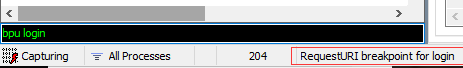
也可以点击图中圈出来的进行断点的设置:



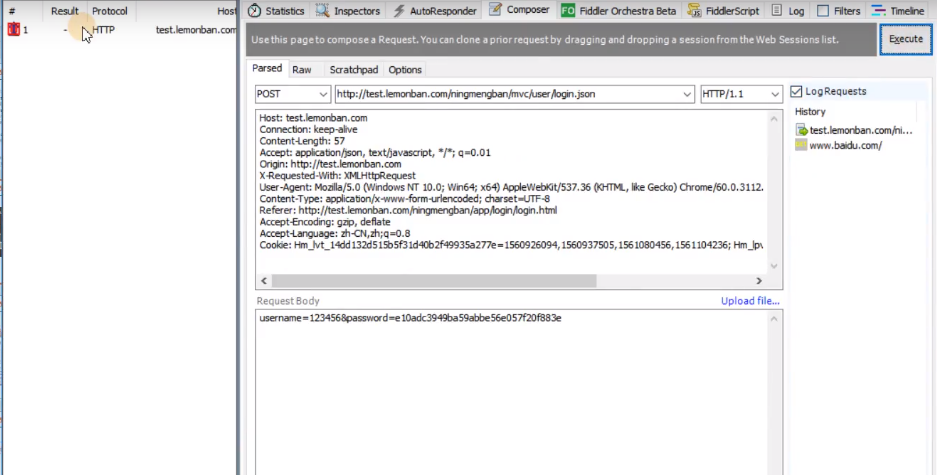
将接口地址拿到后，我们就可以结合断点调试，通过模拟客户端向服务器发出请求:



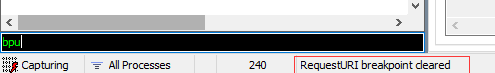
上面第一种断点方式为全局断点，但是我们一般都会去用局部进行断点调试，可以在命令行中输入（bpu 关键字）进行有选取的断点。



当访问页面时，该网页（包含login关键字的网站）将自动断点。



当在输入bpu 断点则被取消。



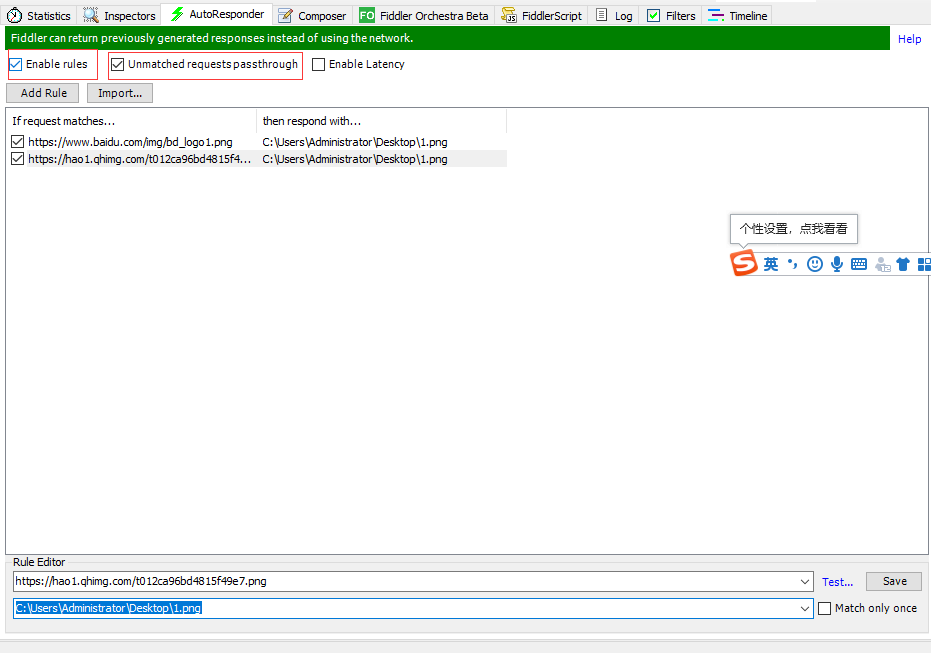
响应后断点：bpafter 关键词 操作跟上面的一样。



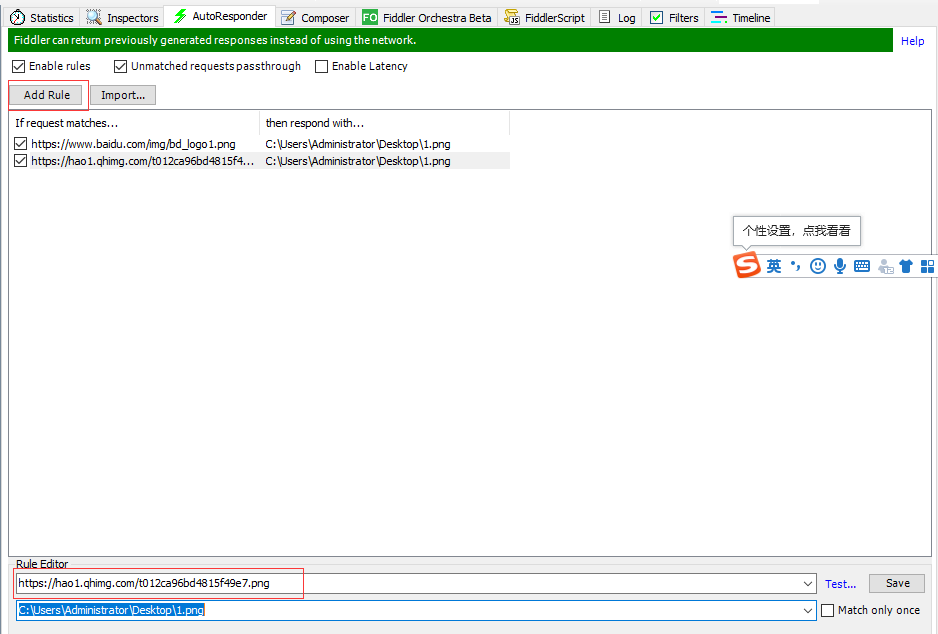
3：自动回复功能（AutoResponder）作用：

1. 重定向到本地的资源
2. 使用Fiddler的内置相应
3. 自定义相应

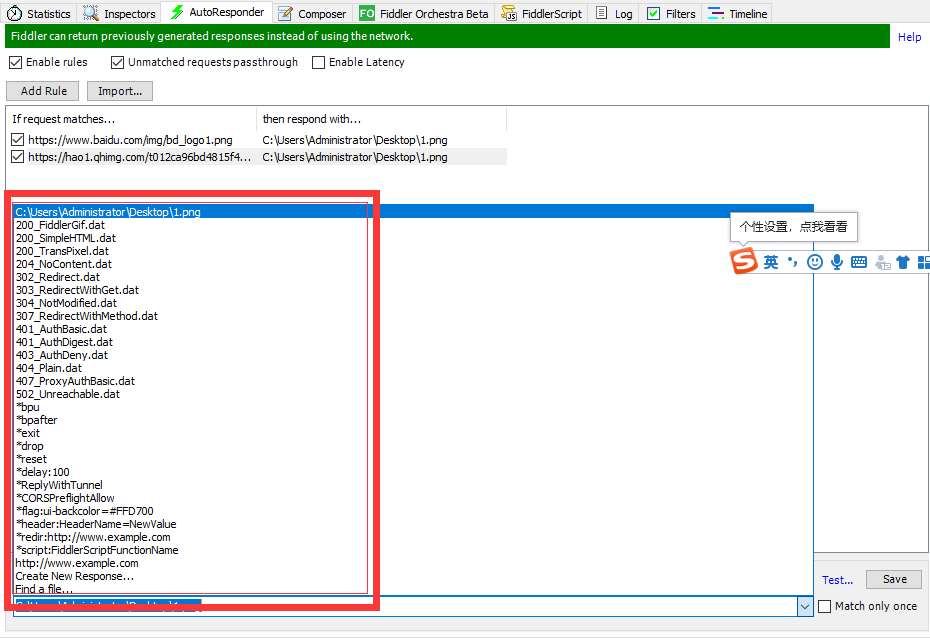
第一步：点击下图中框内的提示内容。



第二步：复制需要访问的网页。并增加规则。

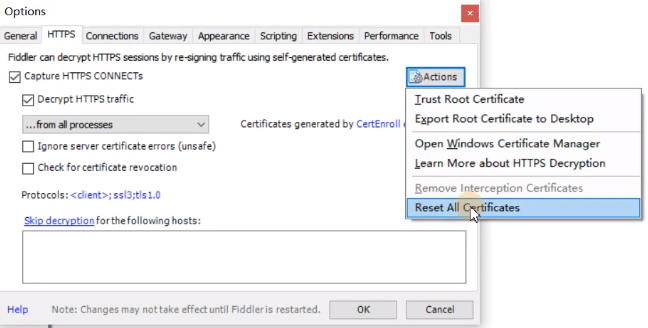


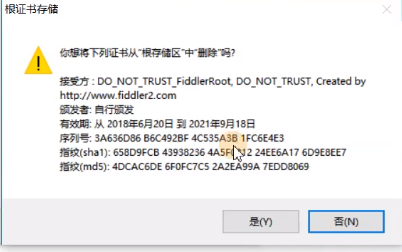
第三步：选择自动返回的类型并保存(选择最后一项可以自定义进行内容的篡改，当访问网页时，网页将显示我们自定义想要显示的内容)：



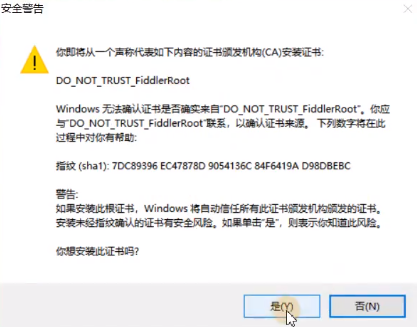
4：https代理功能：

需要点击Toos->Options->Decrypt HTTPS traffic选择Actions安装根证书，步骤如图：

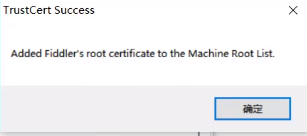




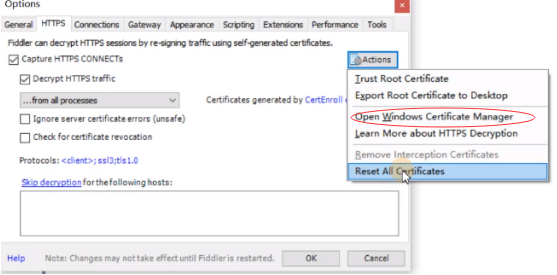


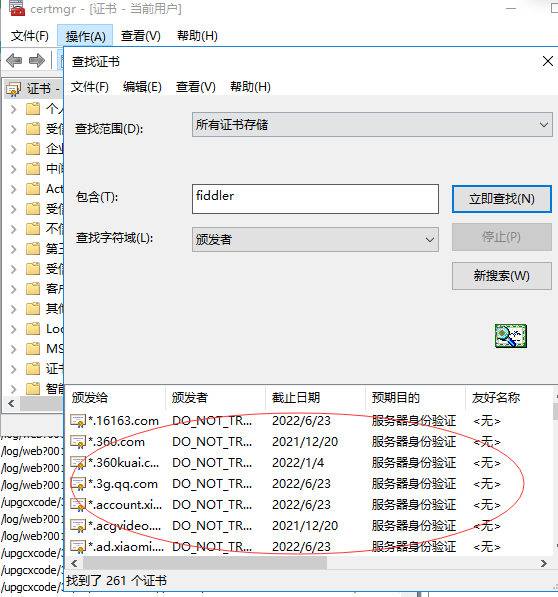






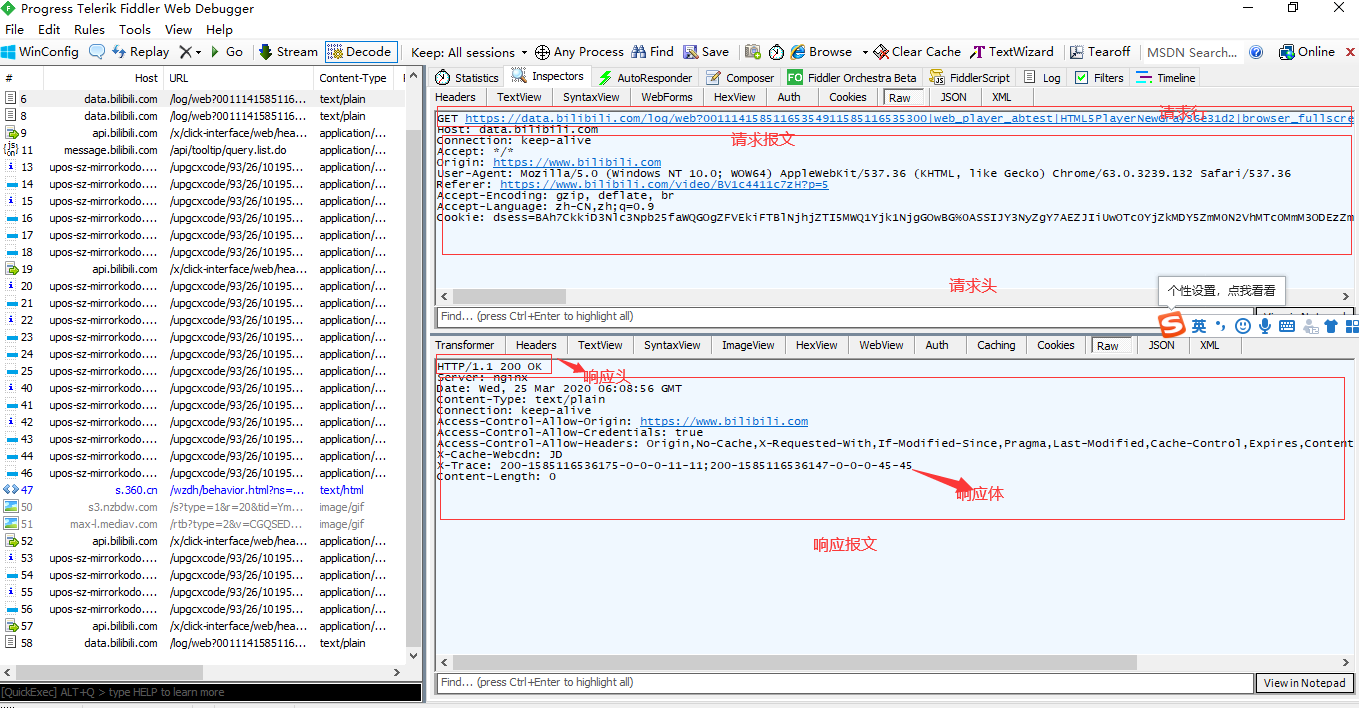
安装成功后，我们查看证书是否存在：





1. 报文头和报文体查看，响应体查看。

点击要查看的包。点击Raw可以查看



请求方法：

Get:获取资源

Post：提交资源

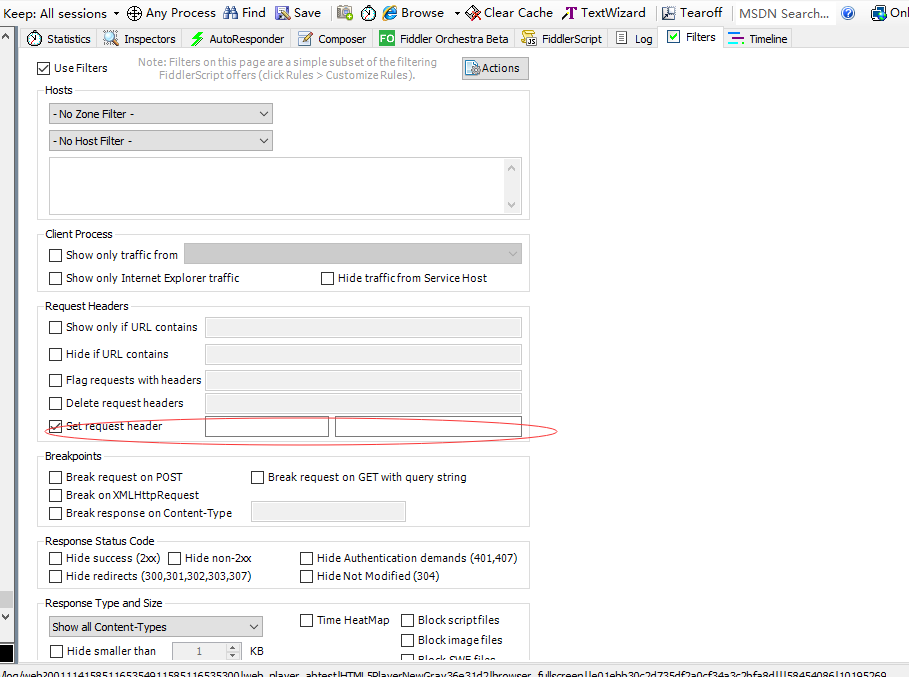
Put：修改资源

Delet：删除资源

请求头：



如果想在请求头中添加信息：选择过滤器中Filters



响应报文：





响应体根据上面的格式信息判断有没有BUG

