[Fiddler抓取HTTPs流量](http://blog.csdn.net/mosmovon/article/details/48469871)

标签： [流量](http://www.csdn.net/tag/%e6%b5%81%e9%87%8f)[fiddler](http://www.csdn.net/tag/fiddler)[心得](http://www.csdn.net/tag/%e5%bf%83%e5%be%97)

2015-09-15 16:50 1062人阅读 [评论](http://blog.csdn.net/mosmovon/article/details/48469871#comments)(0) [收藏](javascript:void(0);) [举报](http://blog.csdn.net/mosmovon/article/details/48469871#report)

http://static.blog.csdn.net/images/category_icon.jpg 分类：

读书心得（2） http://static.blog.csdn.net/images/arrow_triangle%20_down.jpg

版权声明：本文为博主原创文章，未经博主允许不得转载。

**Fiddler抓取HTTPS流量的原理**

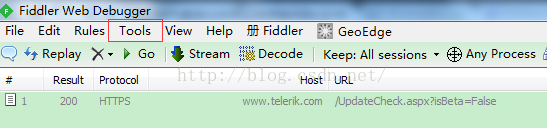
TLS是一种端到端的传输层加密协议，是HTTPS协议的一个组成部分。访问HTTPS站点时，HTTP请求、响应都通过TLS协议在浏览器和服务器之间加密传输，并且通过数字证书技术保证数据的保密性和完整性；任何“中间人”、包括代理服务器都只能转发数据，而无法窃听或者篡改数据。

要抓取HTTPS流量的明文内容，Fiddler必须解密HTTPS流量。但是，浏览器将会检查数字证书，并发现会话遭到窃听。为了骗过浏览器，Fiddler通过使用另一个数字证书重新加密HTTPS流量。Fiddler被配置为解密HTTPS流量后，会自动生成一个名为DO\_NOT\_TRUST\_FiddlerRoot的CA证书，并使用该CA颁发每个域名的TLS证书。若DO\_NOT\_TRUST\_FiddlerRoot证书被列入浏览器或其他软件的信任CA名单内，则浏览器或其他软件就会认为HTTPS会话是可信任的、而不会再弹出“证书错误”警告。

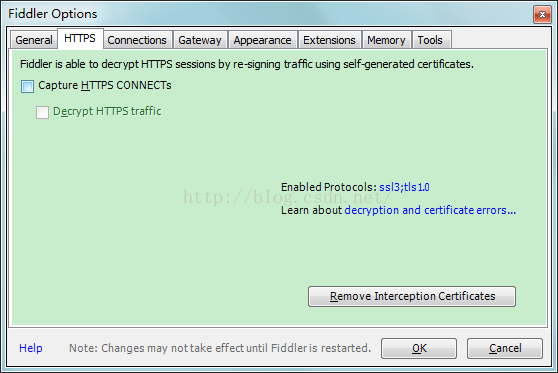
开启HTTPS流量解密功能后，Fiddler将会提示用户将DO\_NOT\_TRUST\_FiddlerRoot证书列入IE浏览器的信任CA名单。用于调试客户端时，这已经足够了；Firefox用户也可以很方便的手动导入DO\_NOT\_TRUST\_FiddlerRoot证书。但是，若要在服务器上抓取ASP[**.NET**](http://lib.csdn.net/base/dotnet)发出的HTTPS请求，这是不够的——你必须将DO\_NOT\_TRUST\_FiddlerRoot证书导入“机器帐号”的信任CA名单。

**Fiddler抓取移动端设备HTTPS流量步骤**

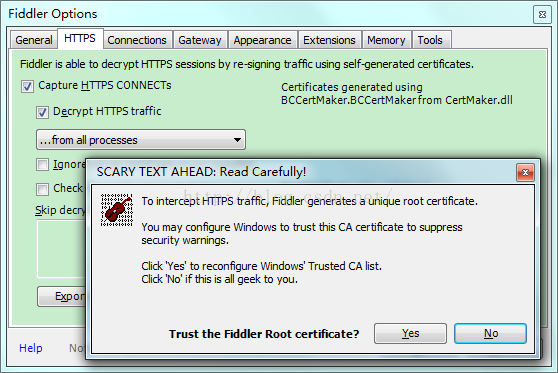
打开tools->FiddlerOptions->HTTPS



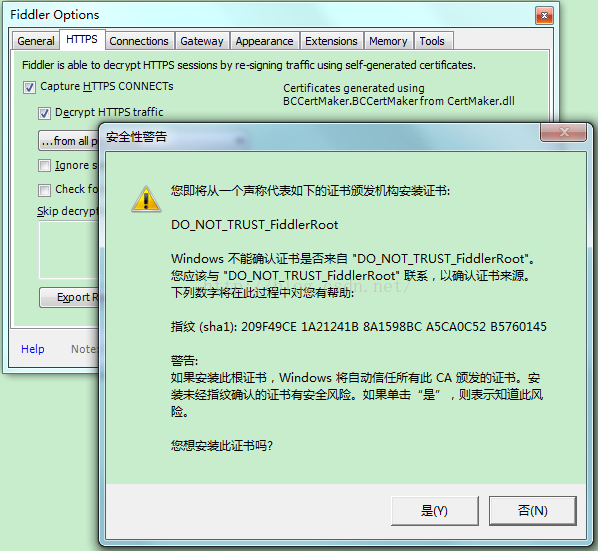
勾选上Capture HTTPS CONNECTs和Decrypt HTTPS traffic



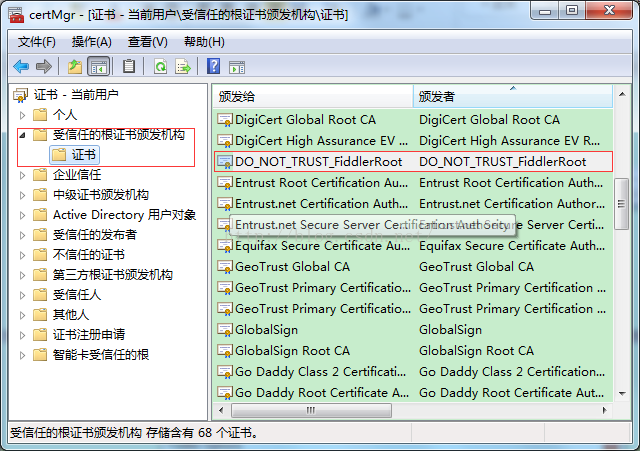
然后会提示安装证书，点击yes



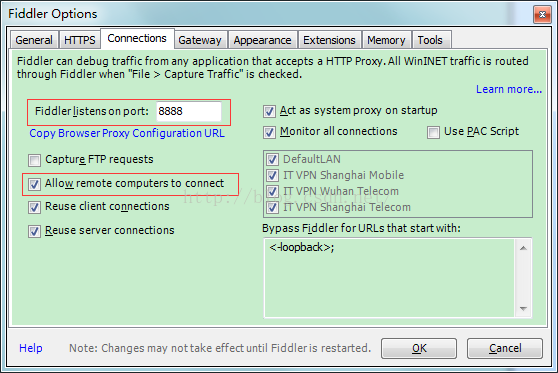
点击是安装证书



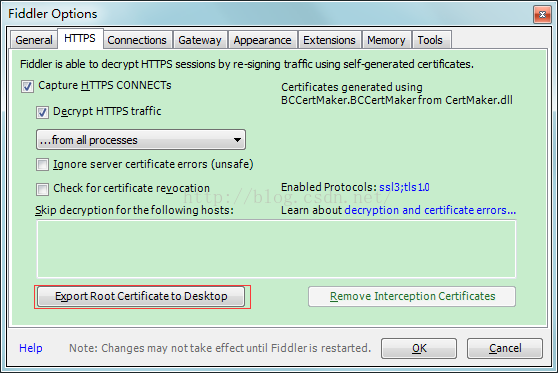
打开certMgr.msc可以管理  PC上的所有证书，在受信任的根证书颁发机构->证书中会有一个DO\_NOT\_TRUST\_FiddlerRoot证书，表明证书安装成功



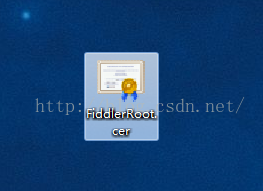
然后在Connections中将Fiddler的监听端口设置为8888，同时勾选上Allow remote computers to connect允许远程连接



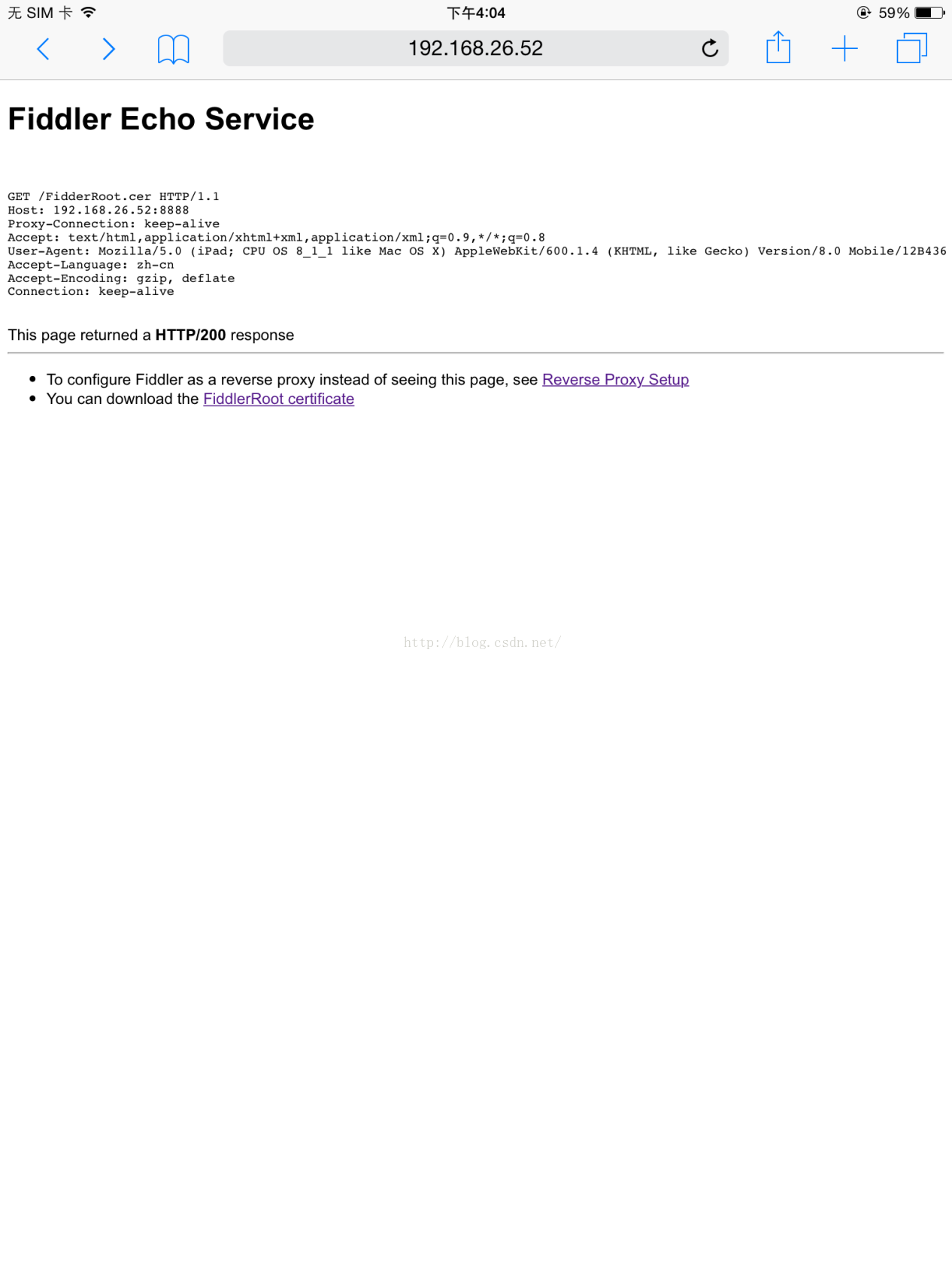
然后在HTTPS中点击Export Root Certificate to Desktop



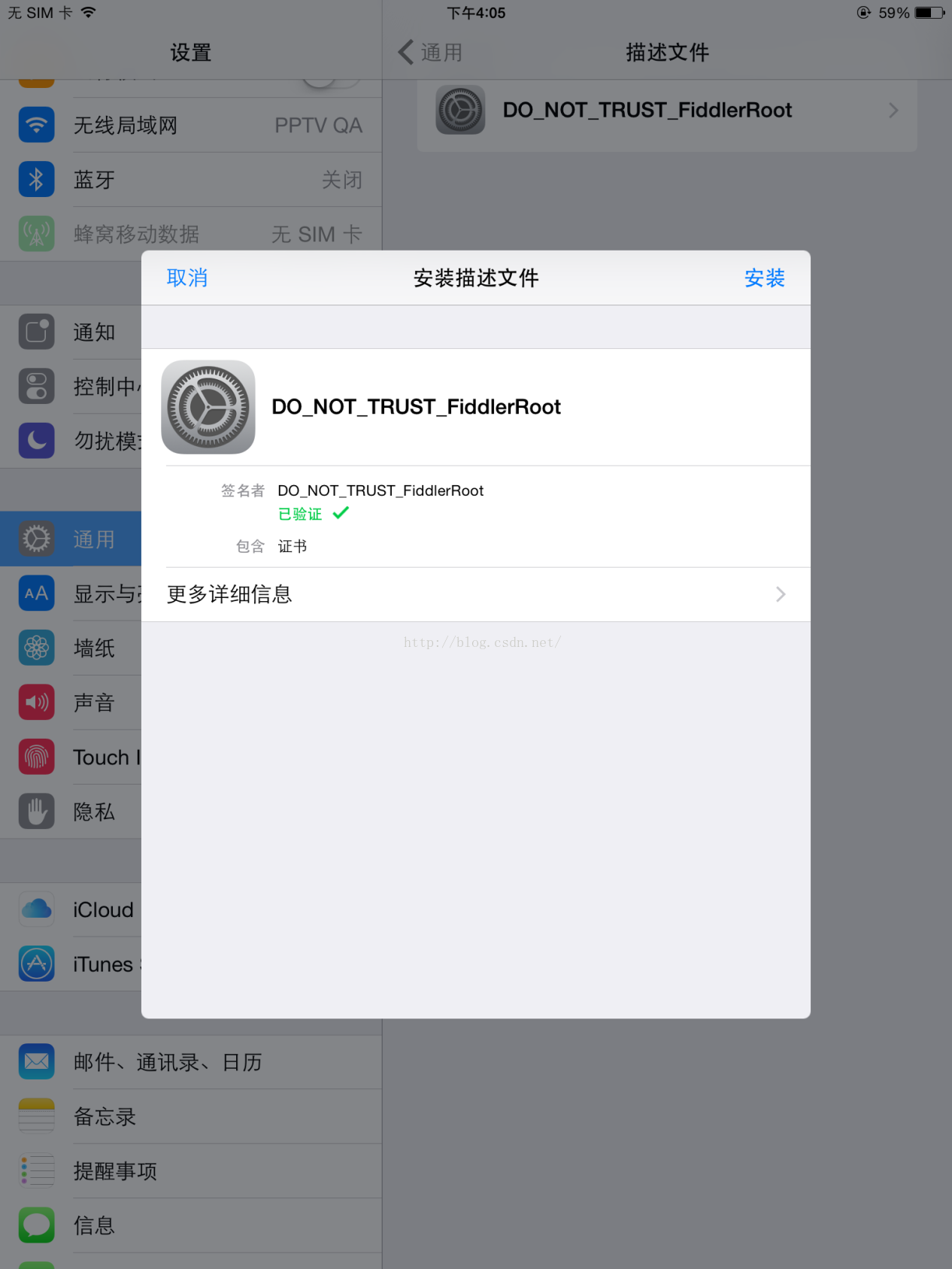
然后桌面上会生成一个FiddlerRoot.cer的证书



下面需要将证书导入到移动设备中，以ipad为例，假设我的电脑在局域网中的ip是192.168.26.52，将Fiddler打开监听在8888端口上，通过在safari的地址栏中输入[http://192.168.26.52:8888/FiddlerRoot.cer](http://192.168.26.52:8888/FiddlerRoot.cer%E5%8F%AF%E4%BB%A5%E5%B0%86%E8%AF%81%E4%B9%A6%E5%AF%BC%E5%85%A5%E5%88%B0ipad" \t "_blank)可以看到Fiddler服务正常开启，然后点击FiddlerRoot certificate将证书导入



点击安装



安装成功会有如下描述文件同时签名会通过认证



最后，在ipad的网络中设置手动代理，ip填写本机ip，端口填写8888即可抓取HTTPS包了

关于高版本Fiddler导出的证书在ipad上安装显示未验证的问题，Google原文如下：

**Q:Can Fiddler intercept traffic from Apple [iOS](http://lib.csdn.net/base/ios" \o "iOS知识库" \t "_blank) devices like iPad/iPhone/iPodTouch and**[**Android**](http://lib.csdn.net/base/android)**devices?**

A: Yes, but these devices may not becompatible with the default certificates Fiddler generates.

To resolve the incompatibility, you mayreplace Fiddler's default certificate generator with one that generatescertificates containing flags (e.g. AKID, SKID) that are compatible with theseplatforms. Simply download and install the newCertificateMaker and restart Fiddler.

安装一个证书生成器，下载地址：<http://www.enhanceie.com/dl/FiddlerCertMaker.exe>

然后重启Fiddler重新导出证书即可