-
  -
    - Fiddler原理
    - 快捷键/命令
    - 手机抓包
      - 安卓模拟器
    - 插件:
      - watcher:
      - x5s:
    - 功能
      - FILE
      - EDIT
      - RULEs
      - TOOLS
      - 第一排按钮
      - 第二排按钮

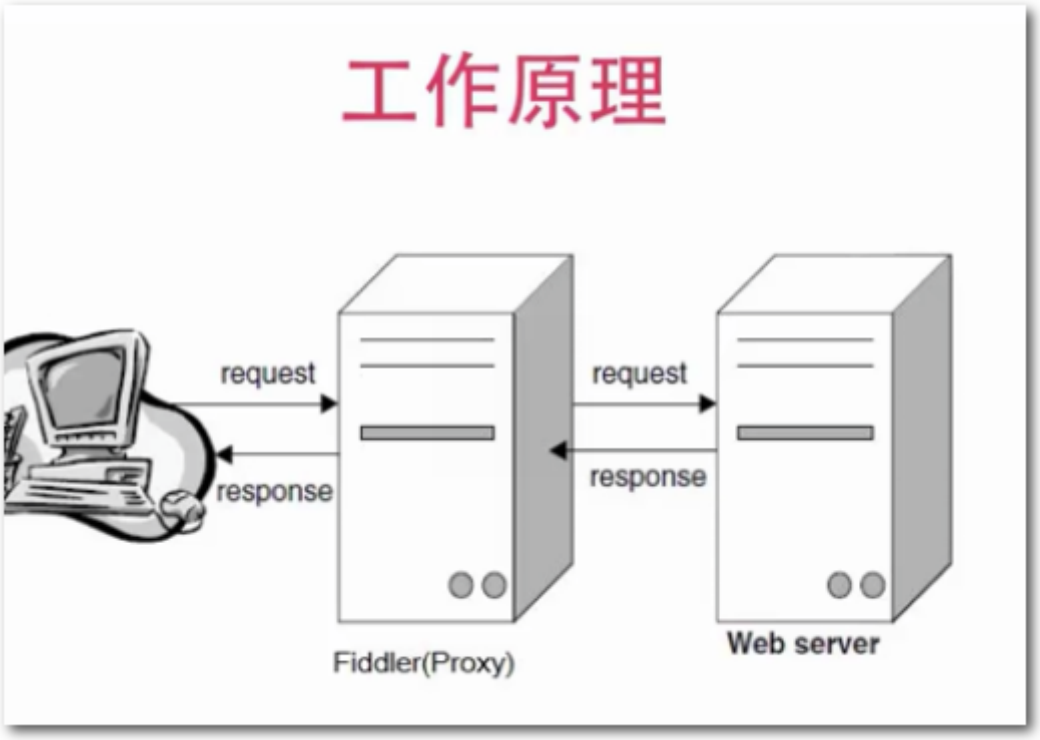
优点:

1. fiddler可以轻易的抓取和分析https网站，相比burp倒入证书方便许多
2. fiddler可以指定应用程序进行抓包分析，而burp必须借助第三方代理程序，兼容性、稳定性都和小提琴相差甚远
3. fiddler 可以很方便抓取app的应用包。

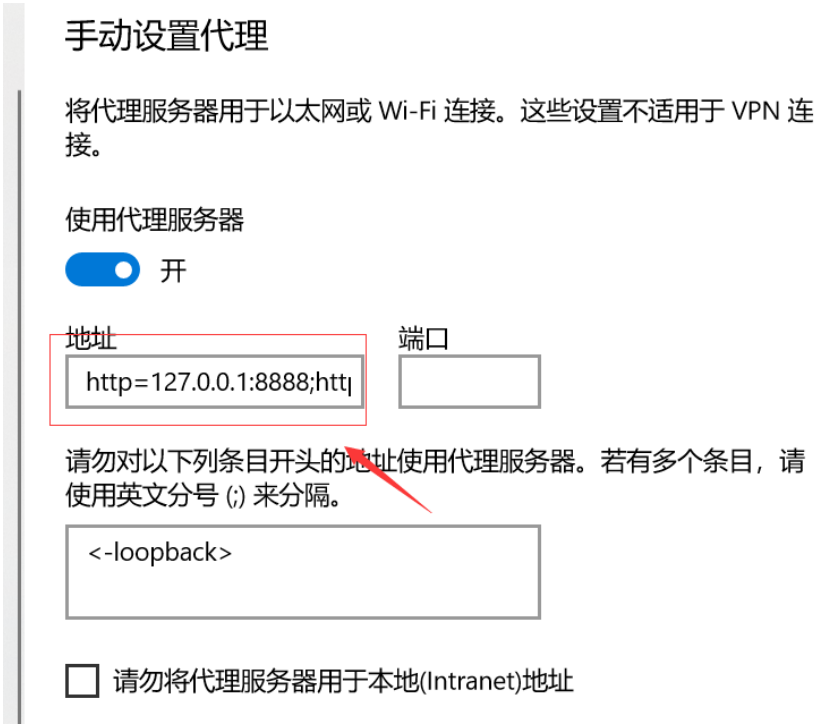
fiddler 工具: https://www.cnblogs.com/milantgh/p/4397976.html

Fiddler原理

在本机开启一个http的代理服务器，然后它会转发所有的http请求和响应到最终的服务器,如图所示

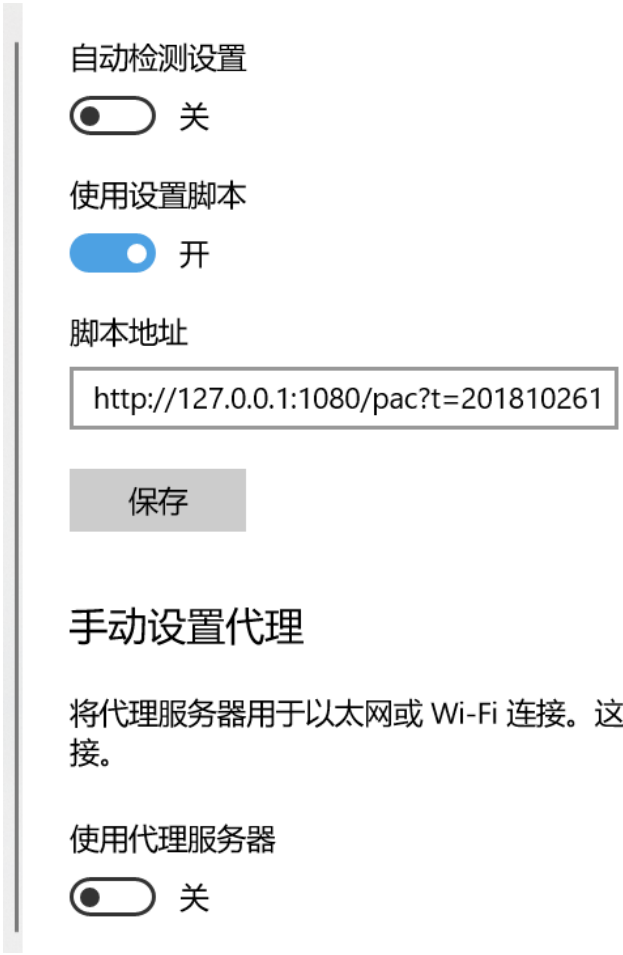


打开Fiddler后，Fiddler会自动篡改代理，

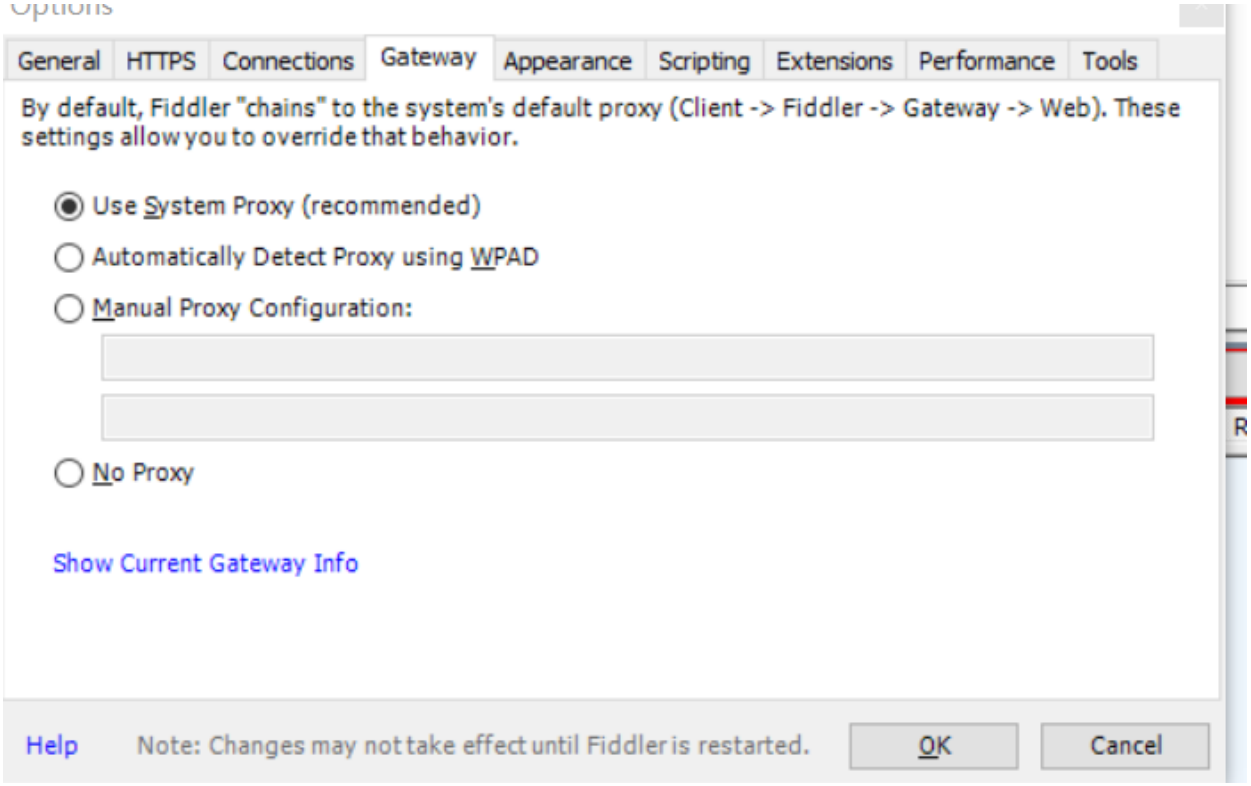


修改系统代理为: `http=127.0.0.1:8888;https=127.0.0.1:8888`

f12关闭捕获数据包后又恢复到ss pac脚本代理的模式了.



你也可以修改fiddler 的这种模式:



快捷键/命令

Referer: http://docs.telerik.com/fiddler/knowledgebase/quickexec

```
ctrl+x : 清空面板

R: 重放(要点击左边的链接重放)
```

命令:

```
clear/cls: 清楚session

?searchtext 搜索

=301 <-- Select 301 redirect responses
=POST <-- Select POST requests

//Break any response where the RequestURI contains /favicon.ico
bpafter /favicon.ico

//Break any response where the status code matches
bps 202

//Create a request breakpoint for the specified HTTP method
bpv POST

//dump all sessions to a zip archive in C:\
dump

//Resume all breakpointed sessions
g/go

//Register as the system proxy
start


//Set up an additional listener on another port, optionally secured by a HTTPS
certificate
!listen 8889
!listen 4443 localhost
!listen 444 secure.example.com
```

手机抓包

安卓模拟器

Nox 夜神模拟器: 经常崩溃，对商场类app很不友好。

优点: 界面做的挺好，有自己的商店可以下载应用。

网易mumu： http://mumu.163.com/

安装证书:

手机输入: 代理ip:8888, 下载证书安装即可。

如果不安装证书的话遇到https 的站点，会显示证书不安全。

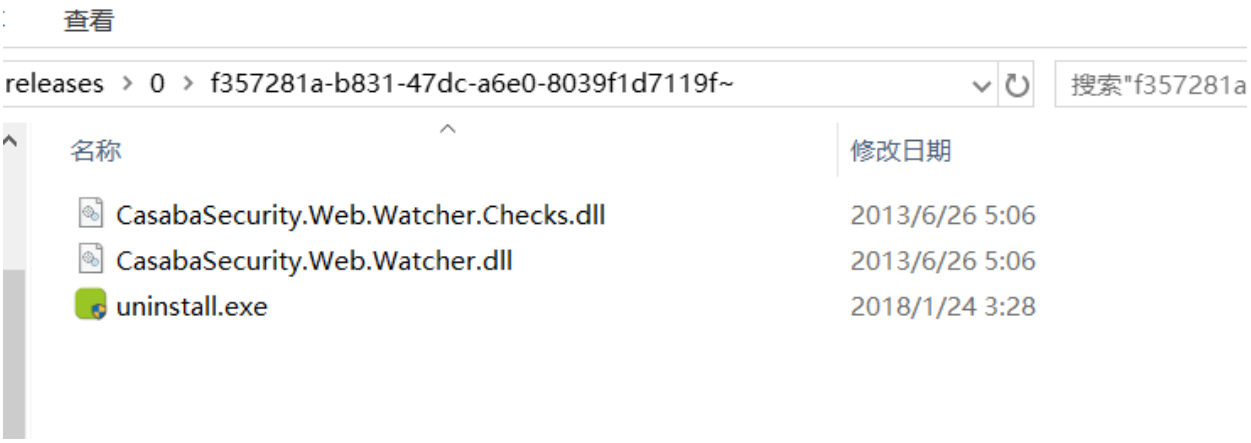
fidder 设置要远程代理和https链接。

然后关闭fidder 的capture 捕获数据包的功能。

插件:

watcher:

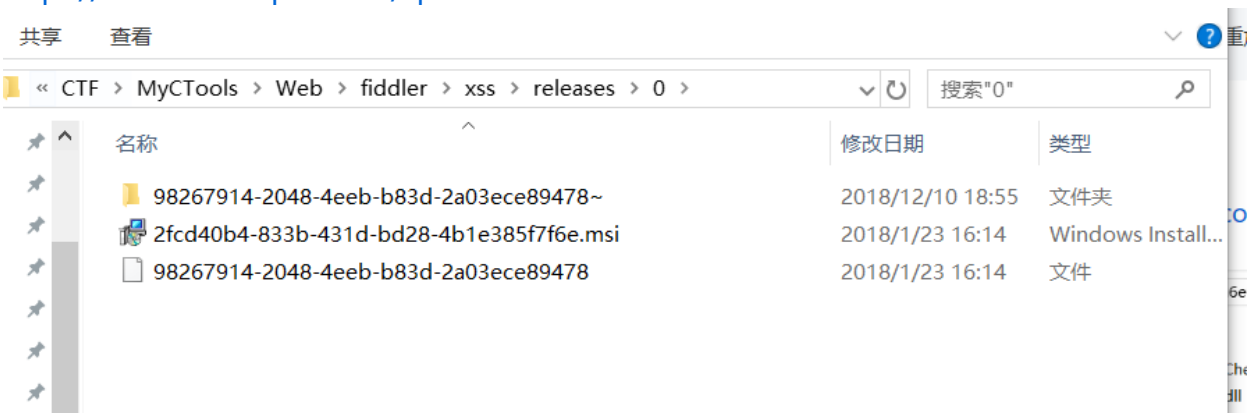
https://casaba.com/products/watcher/



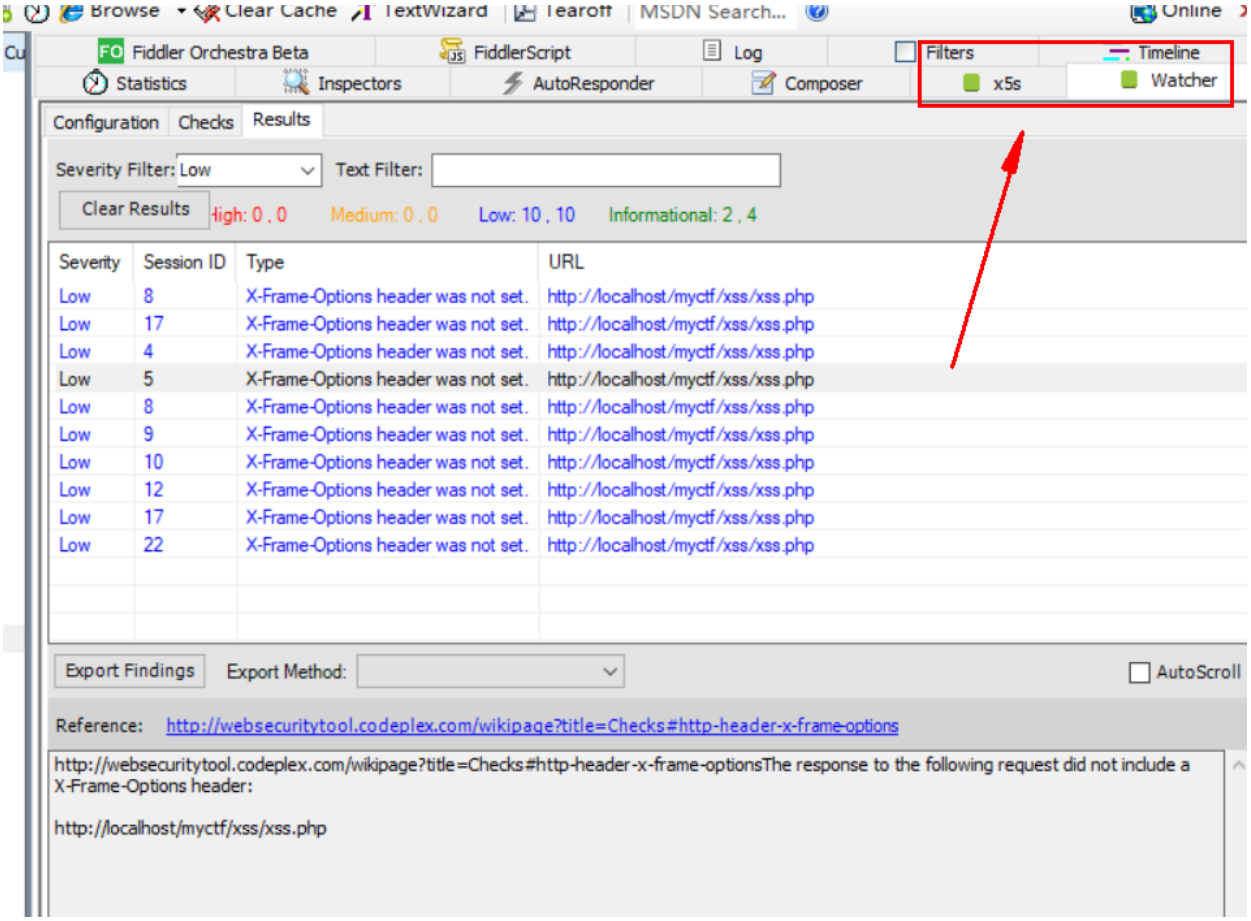
解压其中一个包，会有两个dll,将dll放到fiddler安装目录下的scripts文件夹即可。

x5s:

https://archive.codeplex.com/?p=xss



将2f的一个目录改名为msi文件，



然而实际效果用起来体验很差。

Referer: XSS 自动化检测 Fiddler Watcher & x5s & ccXSScan 初识
https://www.cnblogs.com/milantgh/p/4397976.html

功能

FILE

Capture Traffic

session相关

EDIT

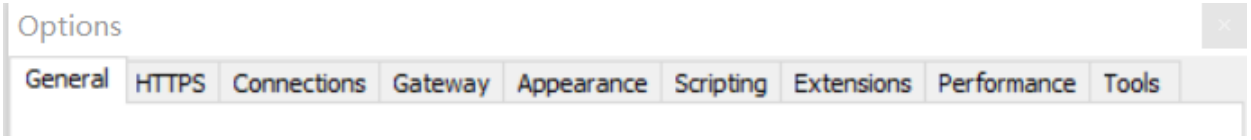
select ,copy等操作

RULEs

过滤url 的规则。

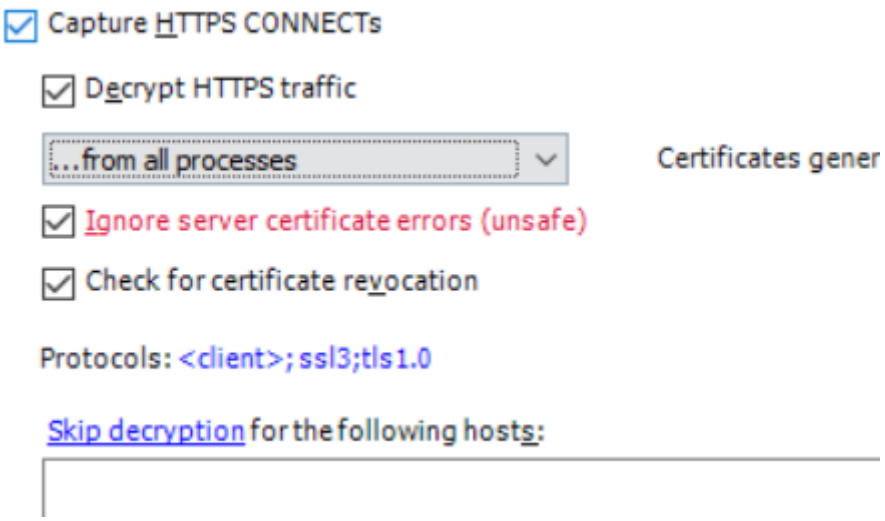
比如过滤图片，过滤ua

TOOLS



general:更新

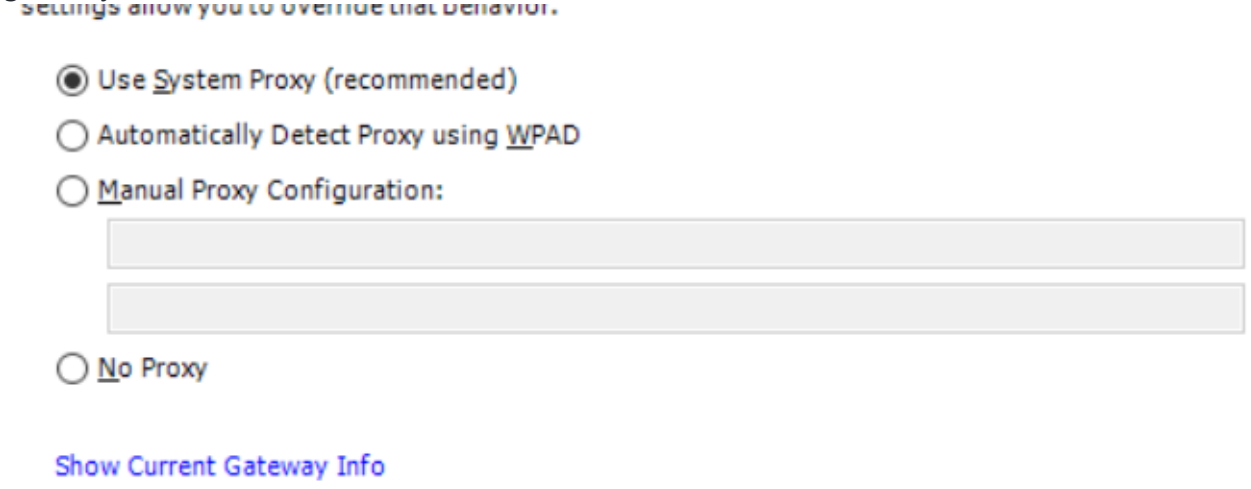
https:



collection:

- 开启远程连接: (app)
- capture ftp connections
- reuse client connections
- reuse server connections
- act as a system proxy on startup
- monitor all connectoins
- bypass filter
- use pac scripts

gateway:



Appearences

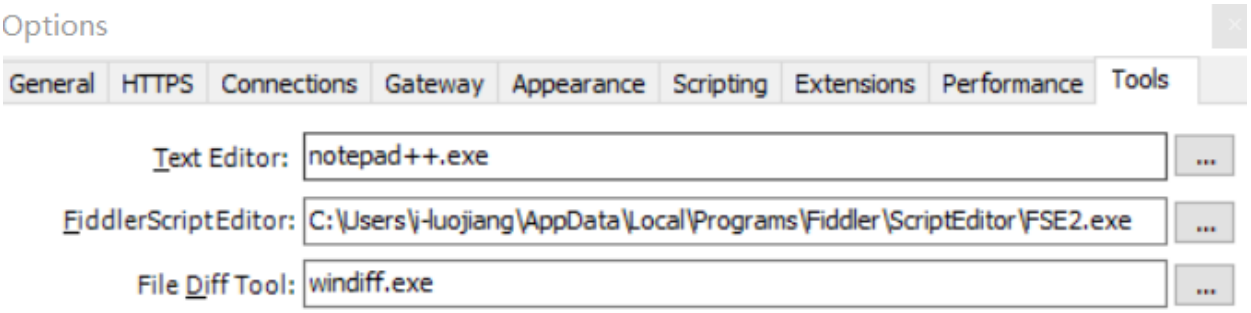
- Hide Fiddler when mini
- reset setssion id on ctrl+x

scripts: 自动加载插件脚本。 Extensions: 扩展

Performances

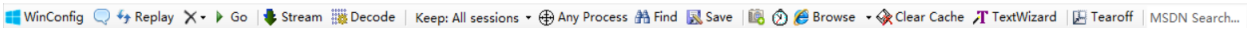
- show memory pannel in status bar
- parse

Tools

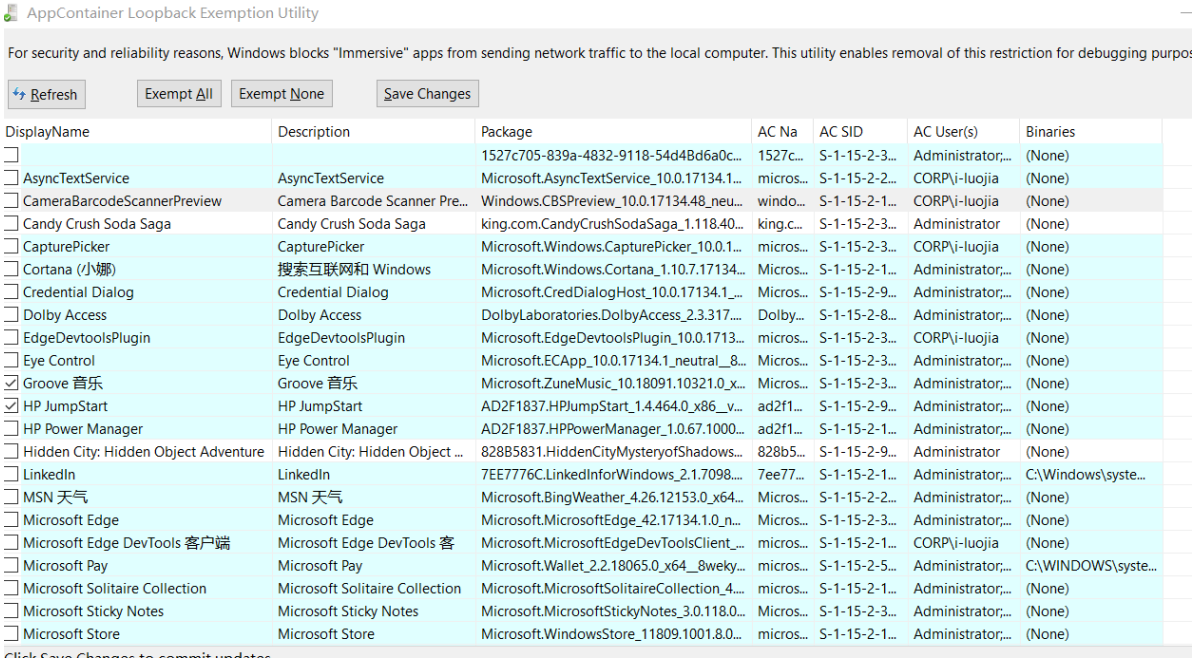


> 设置好后在inspectors 页面中可以直接view in notepad 在notepad++中打开数据包。

第一排按钮



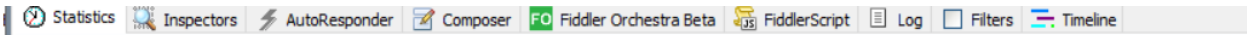
1. WinConfig: window 默认软件。



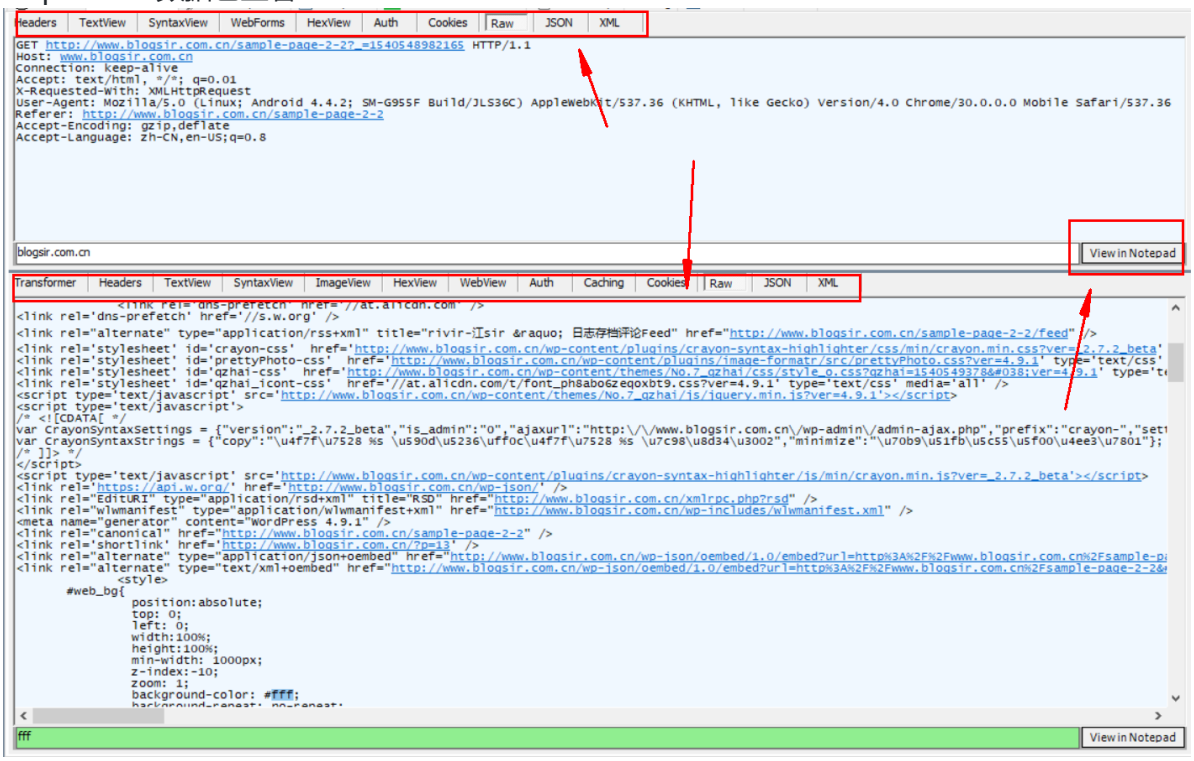
2. comment
3. Replay: 重放

4. Filter
5. Go: 让拦住的所有请求都放行。
6. Stream 切换模式
7. decode
8. keep all sessions
9. Any Process
10. find sessions
11. save session
12. broswer ： 在浏览器中打开选定的链接。
13. TextWizard: 文本加解密工具
14. MSDN Search

第二排按钮



- statistics: 数据分析
- Inspectors: 数据包查看



- AutoResponder 文件代理
- composer: 没搞明白
- Fiddler Orchestra Beta
- Fiddler scripts
- Log
- Filters
- Timeline

参考: https://www.jianshu.com/p/573b23bfb0c2