

- - - 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

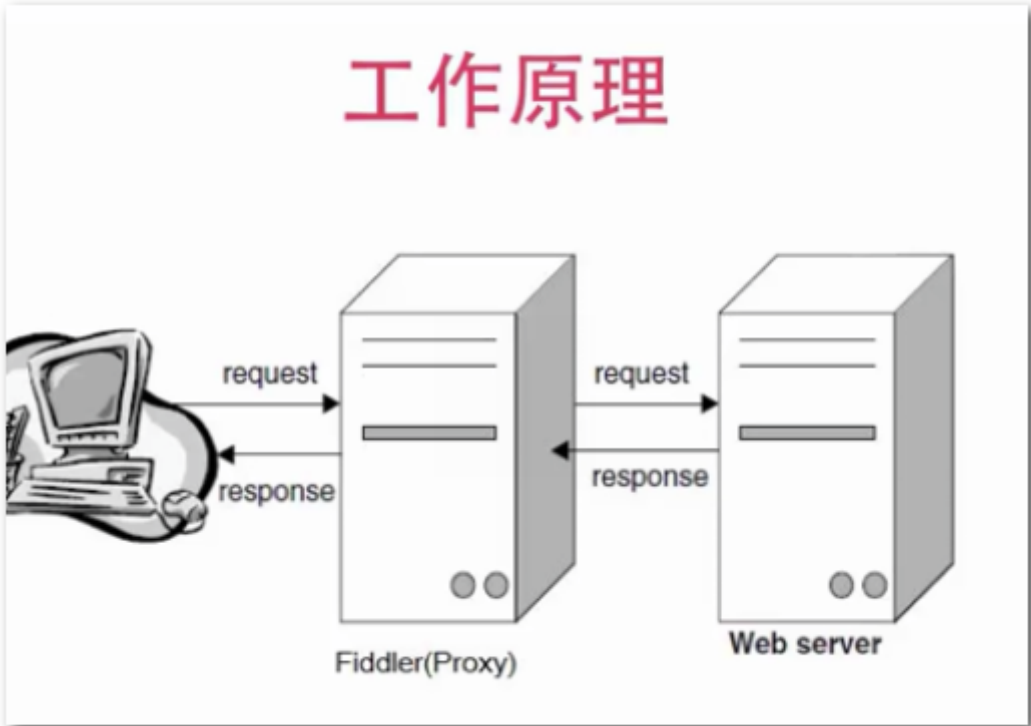
优点:

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，

手动设置代理

将代理服务器用于以太网或 Wi-Fi 连接。这些设置不适用于 VPN 连接。

使用代理服务器

☒ 开

地址

http=127.0.0.1:8888;http

端口

请勿对以下列条目开头的地址使用代理服务器。若有多个条目，请使用英文分号 (;) 来分隔。

<-loopback>

☐ 请勿将代理服务器用于本地(Intranet)地址

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.

自动检测设置

☒ 关

使用设置脚本

☒ 开

脚本地址

保存

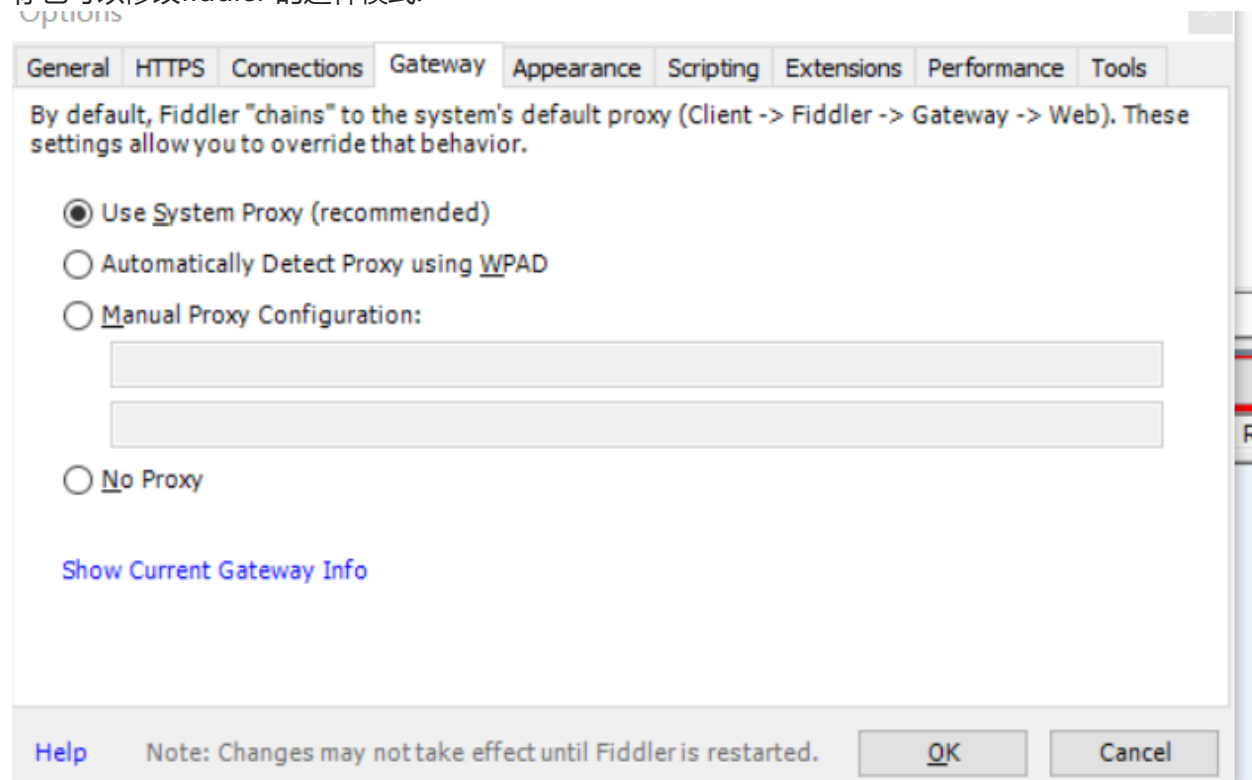
手动设置代理

将代理服务器用于以太网或 Wi-Fi 连接。这些设置不适用于 VPN 连接。

使用代理服务器

☒ 关

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。

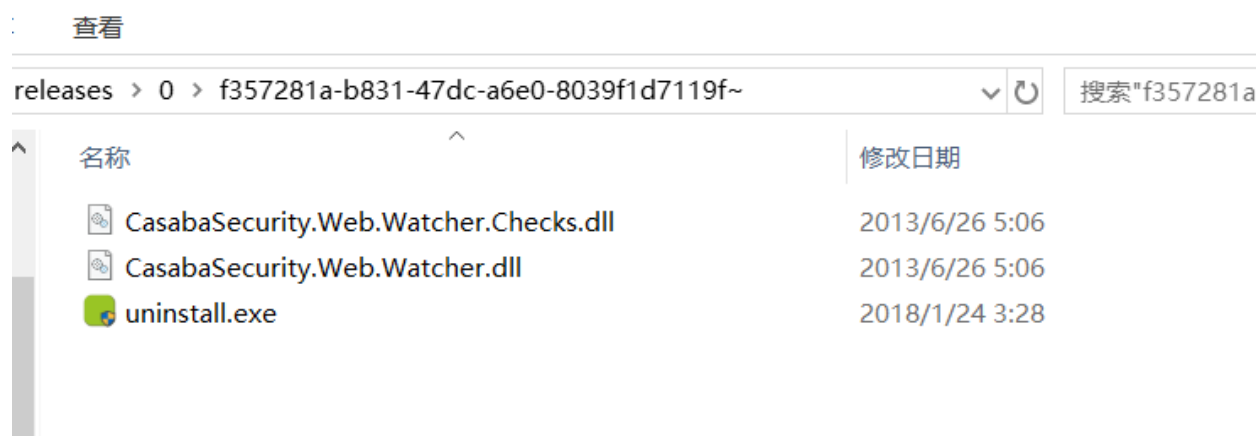
fidder 设置要远程代理和https链接。

然后关闭fidder 的capture 捕获数据包的功能。

插件:

watcher:

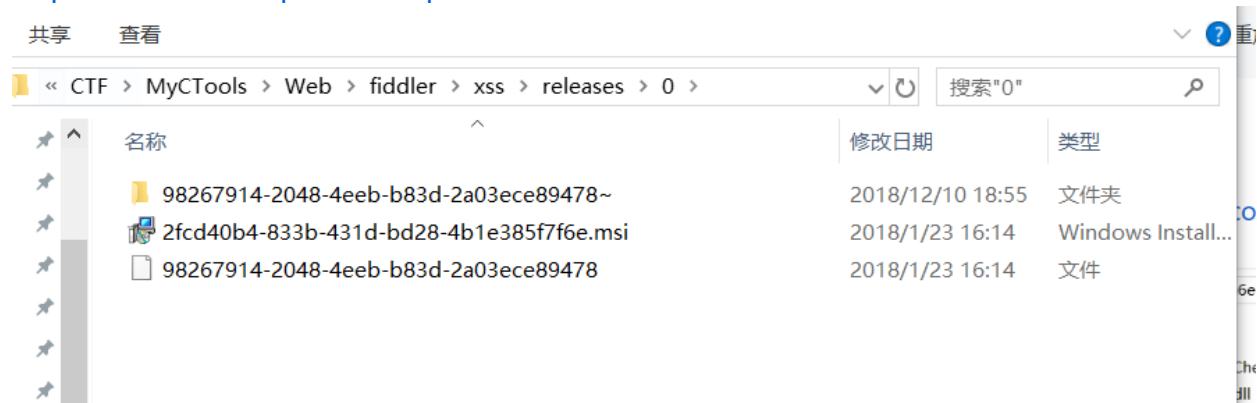
<https://casaba.com/products/watcher/>



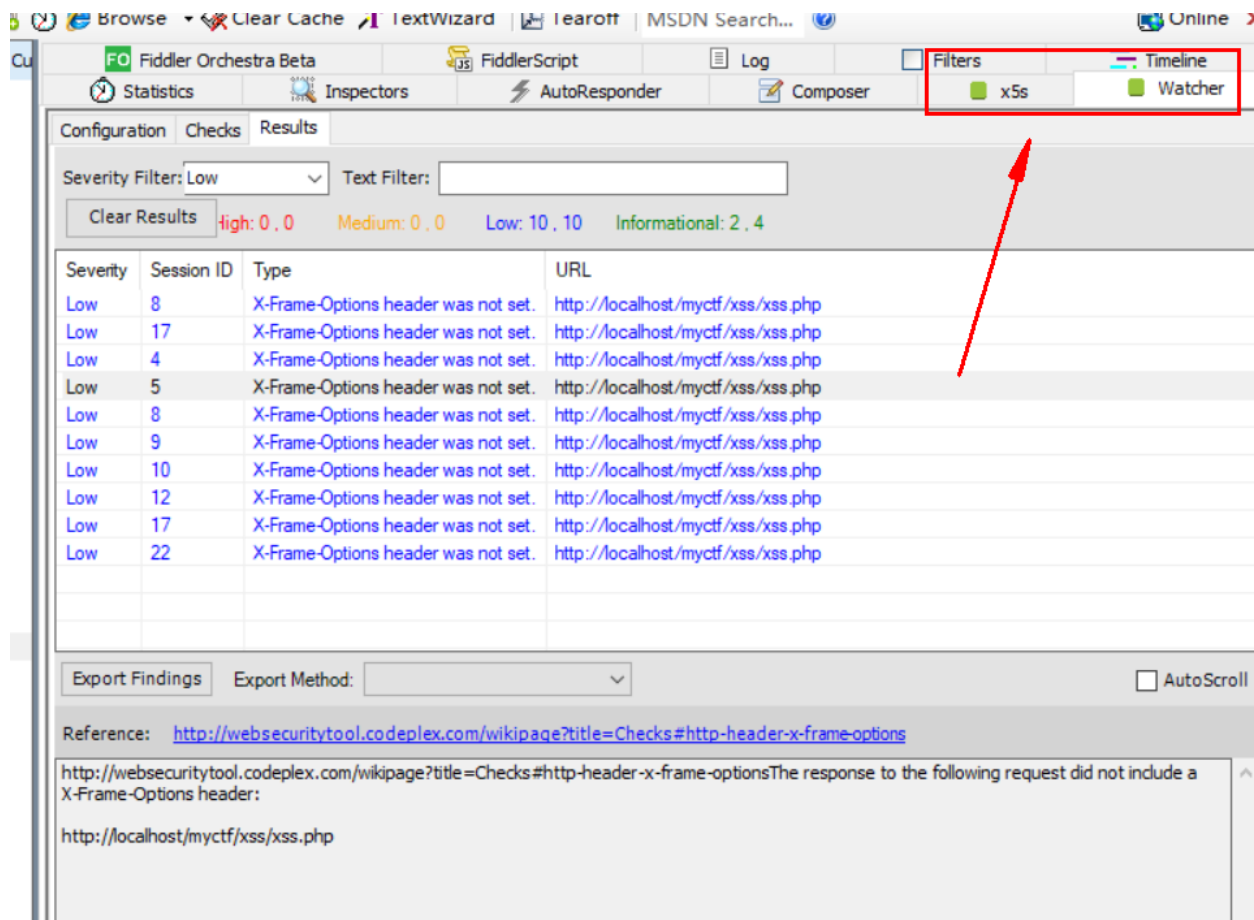
解压其中一个包，会有两个dll,将dll放到fiddler安装目录下的scripts文件夹即可。

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

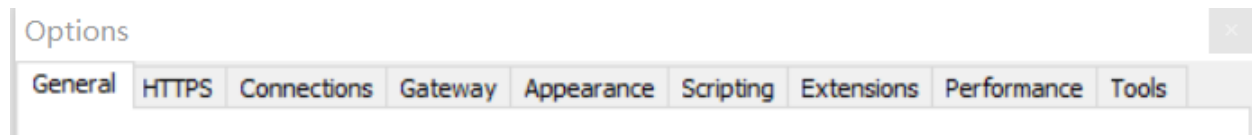
select ,copy等操作

RULEs

过滤url 的规则。

比如过滤图片，过滤ua

TOOLS



general:更新

☒ Capture HTTPS CONNECTs

☒ Decrypt HTTPS traffic

Certificates gener

☒ Ignore server certificate errors (unsafe)

☒ Check for certificate revocation

Protocols: <client>; ssl3;tls1.0

[Skip decryption](#) for the following hosts:

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:

Settings allow you to override that behavior.

- ☒ Use System Proxy (recommended)
- ☐ Automatically Detect Proxy using WPAD
- ☐ Manual Proxy Configuration:
-
-
- ☐ No Proxy

[Show Current Gateway Info](#)

Appearances

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

scripts: 自动加载插件脚本。 Extensions: 扩展

Performances

- show memory panel in status bar
- parse

Tools

Options

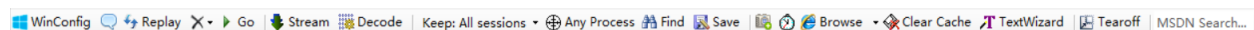
Text Editor: notepad++.exe

FiddlerScript Editor: C:\Users\j-luojiang\AppData\Local\Programs\Fiddler\ScriptEditor\FSE2.exe

File Diff Tool: windiff.exe

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。

AppContainer Loopback Exemption Utility

For security and reliability reasons, Windows blocks "Immersive" apps from sending network traffic to the local computer. This utility enables removal of this restriction for debugging purposes.

Refresh Exempt All Exempt None Save Changes

DisplayName	Description	Package	AC Na	AC SID	AC User(s)	Binaries
<input type="checkbox"/> AsyncTextService	AsyncTextService	Microsoft.AsyncTextService_10.0.17134.1...	micros...	S-1-15-2-3...	Administrator;...	(None)
<input type="checkbox"/> CameraBarcodeScannerPreview	Camera Barcode Scanner Pre...	Windows.CBSPreview_10.0.17134.48_neu...	windo...	S-1-15-2-1...	CORP\j-luojia	(None)
<input type="checkbox"/> Candy Crush Soda Saga	Candy Crush Soda Saga	king.com.CandyCrushSodaSaga_1.118.40...	king.c...	S-1-15-2-3...	Administrator	(None)
<input type="checkbox"/> CapturePicker	CapturePicker	Microsoft.Windows.CapturePicker_10.0.1...	micros...	S-1-15-2-3...	CORP\j-luojia	(None)
<input type="checkbox"/> Cortana (小娜)	搜索互联网和 Windows	Microsoft.Windows.Cortana_1.10.7.17134...	Micros...	S-1-15-2-1...	Administrator;...	(None)
<input type="checkbox"/> Credential Dialog	Credential Dialog	Microsoft.CredDialogHost_10.0.17134.1...	Micros...	S-1-15-2-9...	Administrator;...	(None)
<input type="checkbox"/> Dolby Access	Dolby Access	DolbyLaboratories.DolbyAccess_2.3.317...	Dolby...	S-1-15-2-8...	Administrator;...	(None)
<input type="checkbox"/> EdgeDevtoolsPlugin	EdgeDevtoolsPlugin	Microsoft.EdgeDevtoolsPlugin_10.0.1713...	micros...	S-1-15-2-3...	CORP\j-luojia	(None)
<input type="checkbox"/> Eye Control	Eye Control	Microsoft.ECApp_10.0.17134.1_neutral_8...	Micros...	S-1-15-2-3...	Administrator;...	(None)
<input checked="" type="checkbox"/> Groove 音乐	Groove 音乐	Microsoft.ZuneMusic_10.18091.10321.0_x...	Micros...	S-1-15-2-3...	Administrator;...	(None)
<input checked="" type="checkbox"/> HP JumpStart	HP JumpStart	AD2F1837.HPJumpStart_1.4.464.0_x86_v...	ad2f1...	S-1-15-2-9...	Administrator;...	(None)
<input type="checkbox"/> HP Power Manager	HP Power Manager	AD2F1837.HPPowerManager_1.0.67.1000...	ad2f1...	S-1-15-2-1...	Administrator;...	(None)
<input type="checkbox"/> Hidden City: Hidden Object Adventure	Hidden City: Hidden Object ...	828B5831.HiddenCityMysteryofShadows...	828b5...	S-1-15-2-9...	Administrator	(None)
<input type="checkbox"/> LinkedIn	LinkedIn	7EE7776C.LinkedInforWindows_2.1.7098...	7ee77...	S-1-15-2-1...	Administrator;...	C:\Windows\sys...
<input type="checkbox"/> MSN 天气	MSN 天气	Microsoft.BingWeather_4.26.12153.0_x64...	Micros...	S-1-15-2-2...	Administrator;...	(None)
<input type="checkbox"/> Microsoft Edge	Microsoft Edge	Microsoft.MicrosoftEdge_42.17134.1.0_n...	Micros...	S-1-15-2-3...	Administrator;...	(None)
<input type="checkbox"/> Microsoft Edge DevTools 客户端	Microsoft Edge DevTools 客	Microsoft.MicrosoftEdgeDevToolsClient...	micros...	S-1-15-2-1...	CORP\j-luojia	(None)
<input type="checkbox"/> Microsoft Pay	Microsoft Pay	Microsoft.Wallet_2.2.18065.0_x64_8weky...	micros...	S-1-15-2-5...	Administrator;...	C:\WINDOWS\sys...
<input type="checkbox"/> Microsoft Solitaire Collection	Microsoft Solitaire Collection	Microsoft.MicrosoftSolitaireCollection_4...	micros...	S-1-15-2-1...	Administrator;...	(None)
<input type="checkbox"/> Microsoft Sticky Notes	Microsoft Sticky Notes	Microsoft.MicrosoftStickyNotes_3.0.118.0...	Micros...	S-1-15-2-3...	Administrator;...	(None)
<input type="checkbox"/> Microsoft Store	Microsoft Store	Microsoft.WindowsStore_11809.1001.8.0...	micros...	S-1-15-2-1...	Administrator;...	(None)

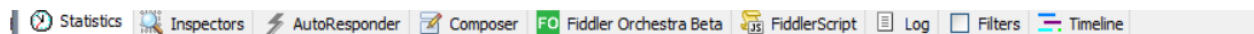
Click Save Changes to commit updates.

2. comment

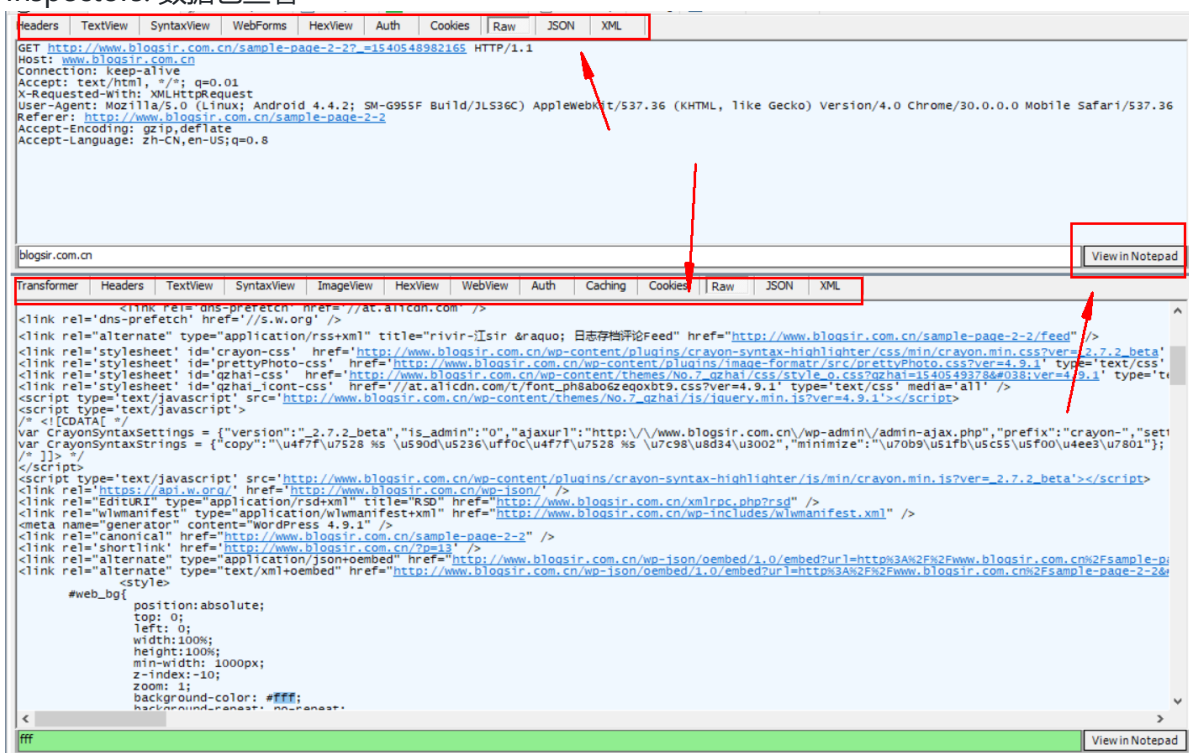
3. Replay: 重放

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. browser: 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>