



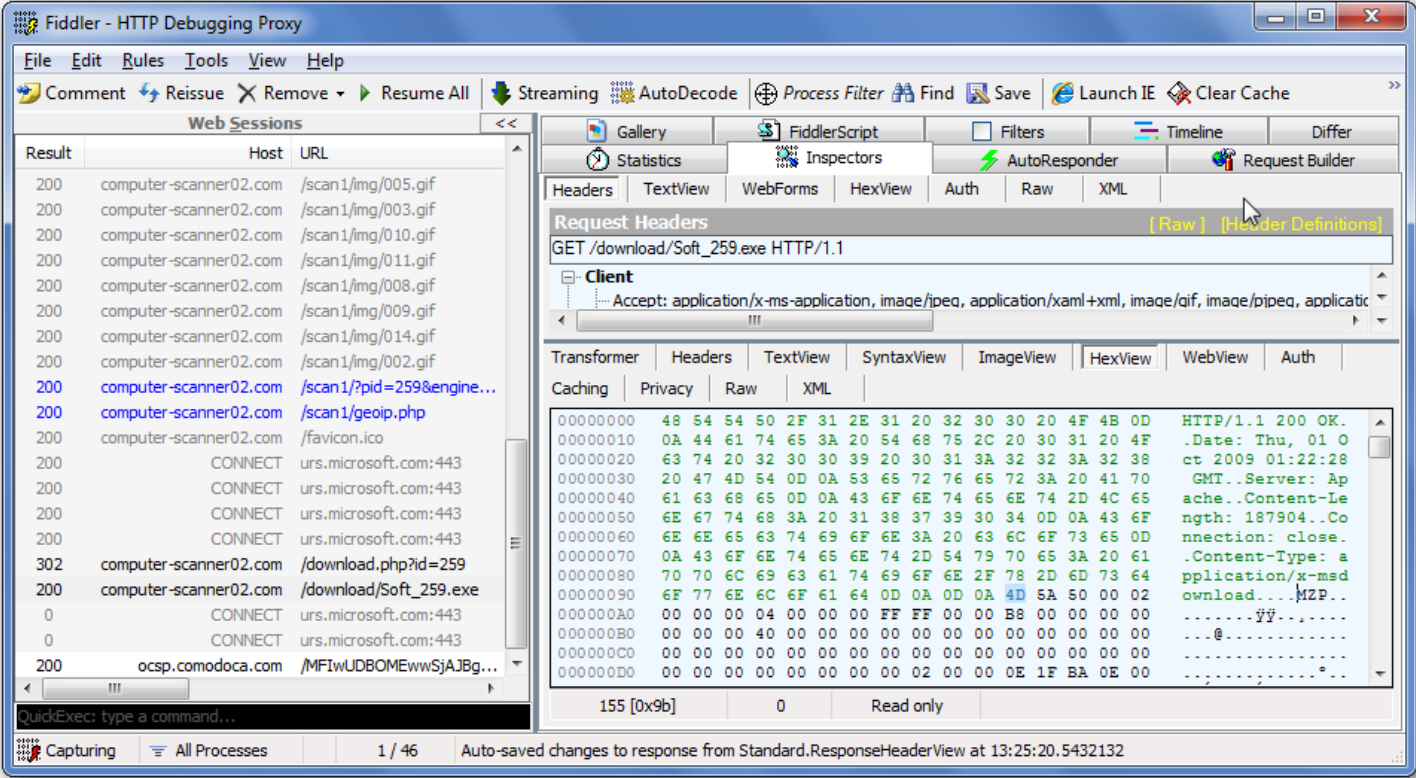
# Fiddler

## 使用经验分享

Prepared by hua.qiu



# Fiddler



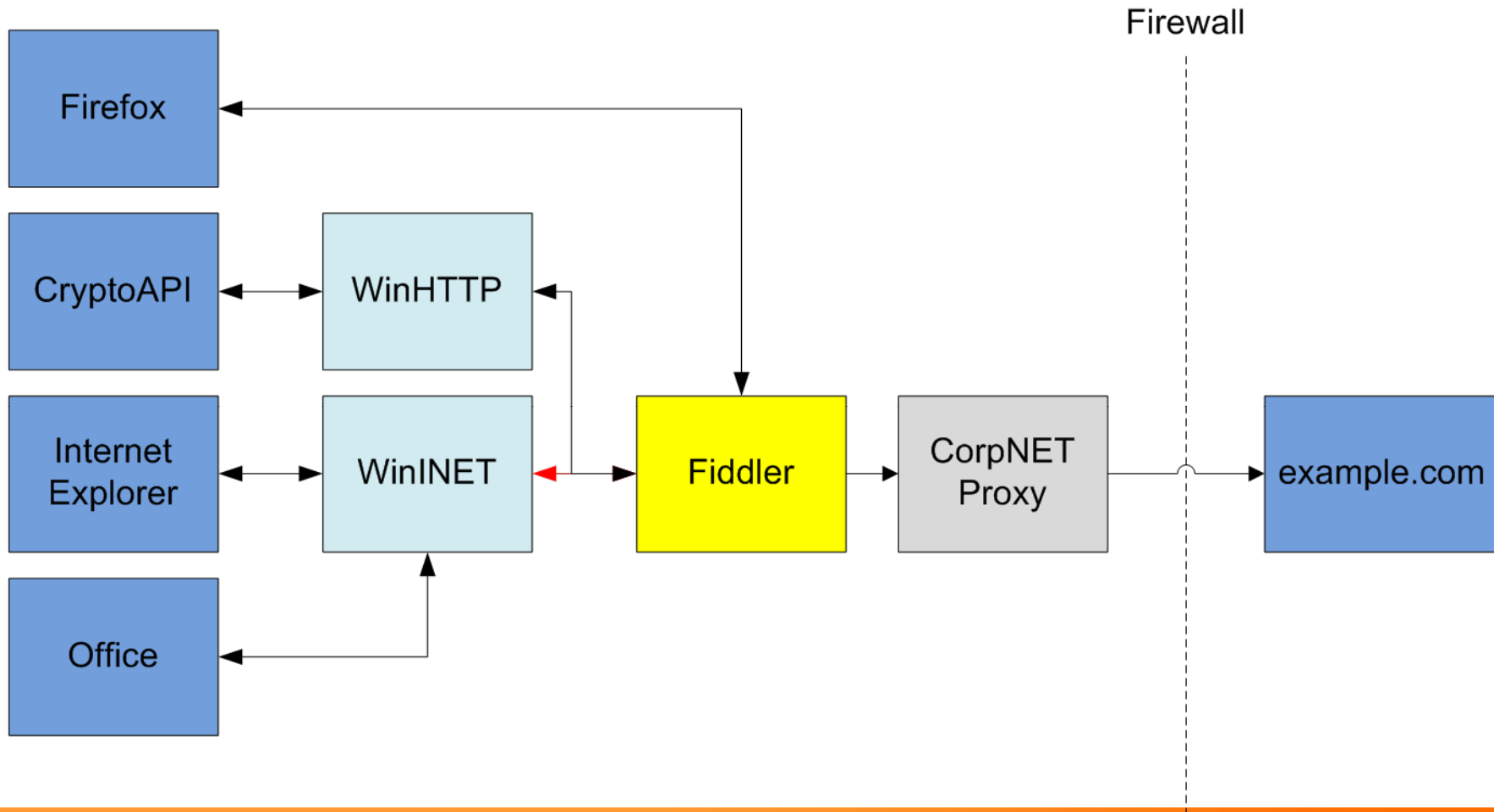
# Fiddler，是什么？

- HTTP/HTTPS 调试器
- 以HTTP代理方式，在本机或服务器运行
- C#编写 (.NET Framework v2.0)
- 从这里免费下载

<http://www.fiddler2.com>



# Fiddler 是什么工作原理？



# 那，Fiddler 有什么用？

- HTTP/HTTPS 流记录和分析
- 修改请求和响应
- 构造网络访问
- 一些工具



# Fiddler的界面和功能



**Fiddler**  
Web Debugging Proxy



# Session 列表

| # | Result | Protocol | Host                 | URL                              |
|---|--------|----------|----------------------|----------------------------------|
|   | 200    | HTTP     | www.fiddler2.com     | /fiddler2/updatecheck.asp?isBe   |
|   | 200    | HTTP     | www.bayden.com       | /                                |
|   | 304    | HTTP     | www.bayden.com       | /Bayden.css                      |
|   | 200    | HTTP     | CONNECT              | urs.microsoft.com:443            |
|   | 200    | HTTP     | CONNECT              | urs.microsoft.com:443            |
|   | 200    | HTTPS    | urs.microsoft.com    | /urs.asmx?MSURS-Client-Key=      |
|   | 200    | HTTPS    | urs.microsoft.com    | /urs.asmx?MSURS-Client-Key=      |
|   | 200    | HTTP     | www.ysgyfarnog.co.uk | /utilities/mousegestures/versior |

- 显示所有数据流
- URLs, size, 和关键信息

## • 状态图标

- Request is being sent to the server
- Downloading response from server
- Request is paused at a breakpoint.
- Response is paused at a breakpoint.
- Response was HTML
- Response was an image
- Response was a script
- Response was Cascading Style Sheet
- Response was XML
- Generic Response successful
- Response was HTTP/300,301,302,303 or 307 redirect
- Response was HTTP/304: Use cached version
- Response was a request for client credentials
- Response was a server error
- Session was aborted by the client, Fiddler, or the Server.



# 查看器

The screenshot displays the Fiddler web debugging proxy interface. On the left, the 'Response Headers' pane shows the following details:

- Cache: Cache-control: private, Date: Sat, 10 Oct 2009 20:46:27 GMT
- Entity: Content-Length: 377, Content-Type: text/plain
- Miscellaneous: MicrosoftOfficeWebServer: 5.0\_Pub, Server: Microsoft-IIS/6.0, X-Powered-By: ASP.NET
- Transport: Connection: Keep-Alive, Proxy-Connection: Keep-Alive, Via: 1.1 RED-PRXY-21

At the top, the 'HTTP Compression' settings are shown with 'GZIP Encoding' selected. The main pane displays the 'SyntaxView' of the response body, which is HTML code:

```
4 <head>
5 <link REL="StyleSheet" HREF="Bayden.css" TYPE="text/css">
6
7 <title>Bayden Systems</title>
8
9 <link REL="alternate" HREF="http://baydensystems.blogspot.com/atom.xml"
10
11
12 </head>
13 <body BGCOLOR="#FFFFFF" LEFTMARGIN="0" TOPMARGIN="0" MARGINHEIGHT="0" M
14
15 <!--Graphic Masthead-->
```

Below the HTML view, a hex dump of the response data is visible:

|          |   |                   |
|----------|---|-------------------|
| 00000000 | 48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D | HTTP/1.1 200 OK.  |
| 00000010 | 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 | .Content-Type: t  |
| 00000020 | 65 78 74 2F 68 74 6D 6C 0D 0A 43 61 63 68 65 2D | ext/html..Cache-  |
| 00000030 | 63 6F 6E 74 72 6F 6C 3A 20 70 72 69 76 61 74 65 | control: private  |
| 00000040 | 0D 0A 43 6F 6E 74 65 6E 74 2D 45 6E 63 6F 64 69 | ..Content-Encodi  |
| 00000050 | 6E 67 3A 20 67 7A 69 70 0D 0A 0D 0A 1F 8B 08 00 | ng: gzip.....     |
| 00000060 | F1 F2 D0 4A 00 FF 95 58 6D 73 DB B8 11 FE EC 9B | řòØJ.ÿ.XmsÛ, .pi. |
| 00000070 | B9 FF 80 E3 4D E2 76 6A 91 92 ED 9C 1D 5B 54 4E | ÿ.ãMávj...í...[TN |
| 00000080 | 96 18 5B AD FC 72 92 AE 69 3F 65 20 12 22 51 93 | ..[-ür.©i?e_."Q.  |

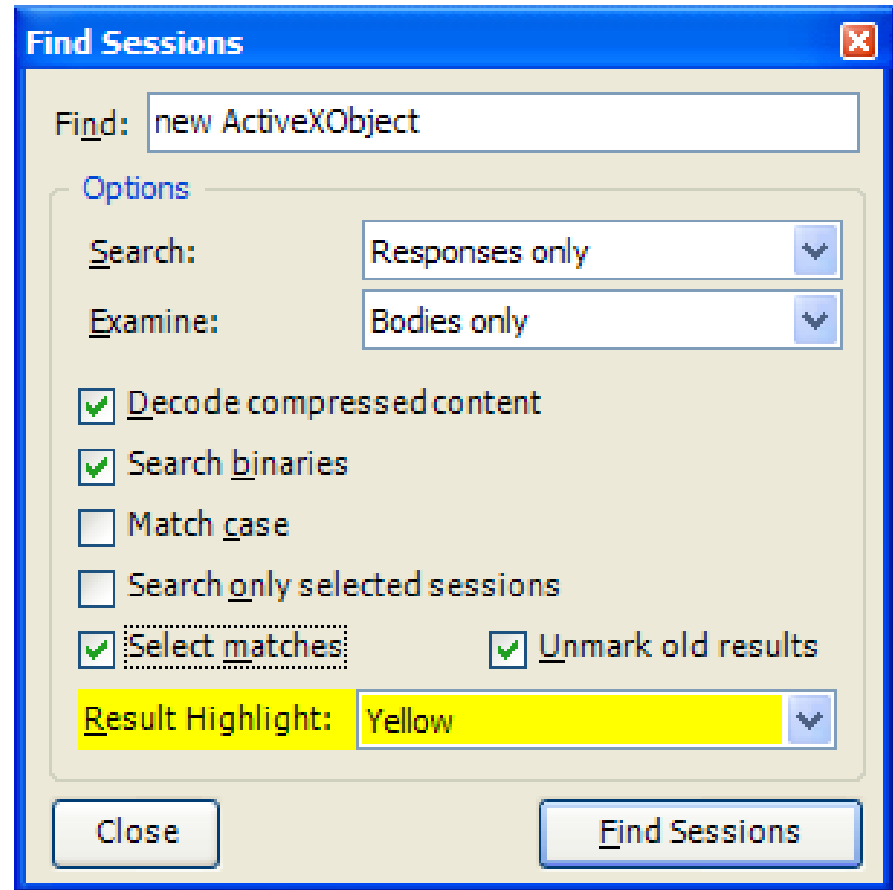
查看器利用很多种形式，让我们查看请求数据的内容





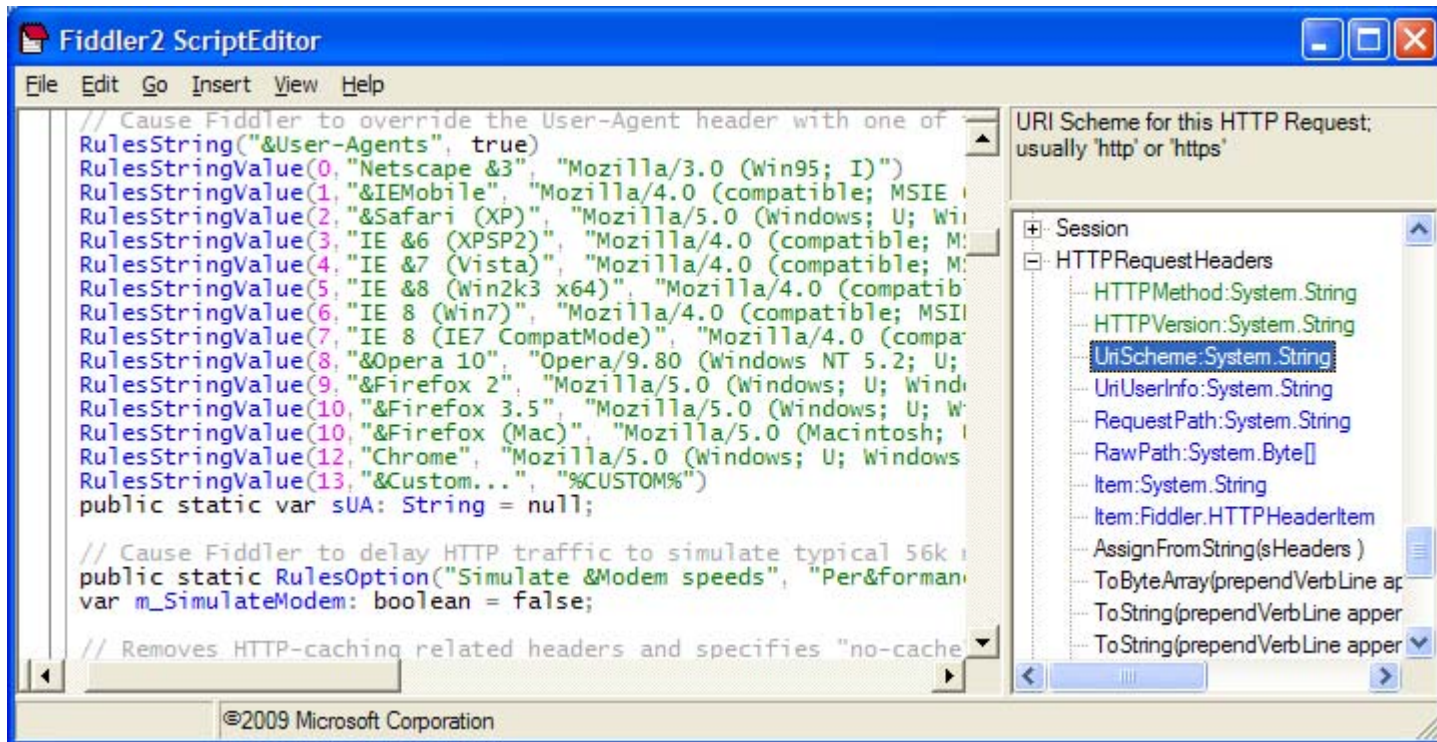
# 搜索

搜索包含有某个  
词语的数据流



# FiddlerScript 规则

- 规则是Fiddler最强大和有趣的功能!
- 使用JavaScript语法，操纵所有的魔术!

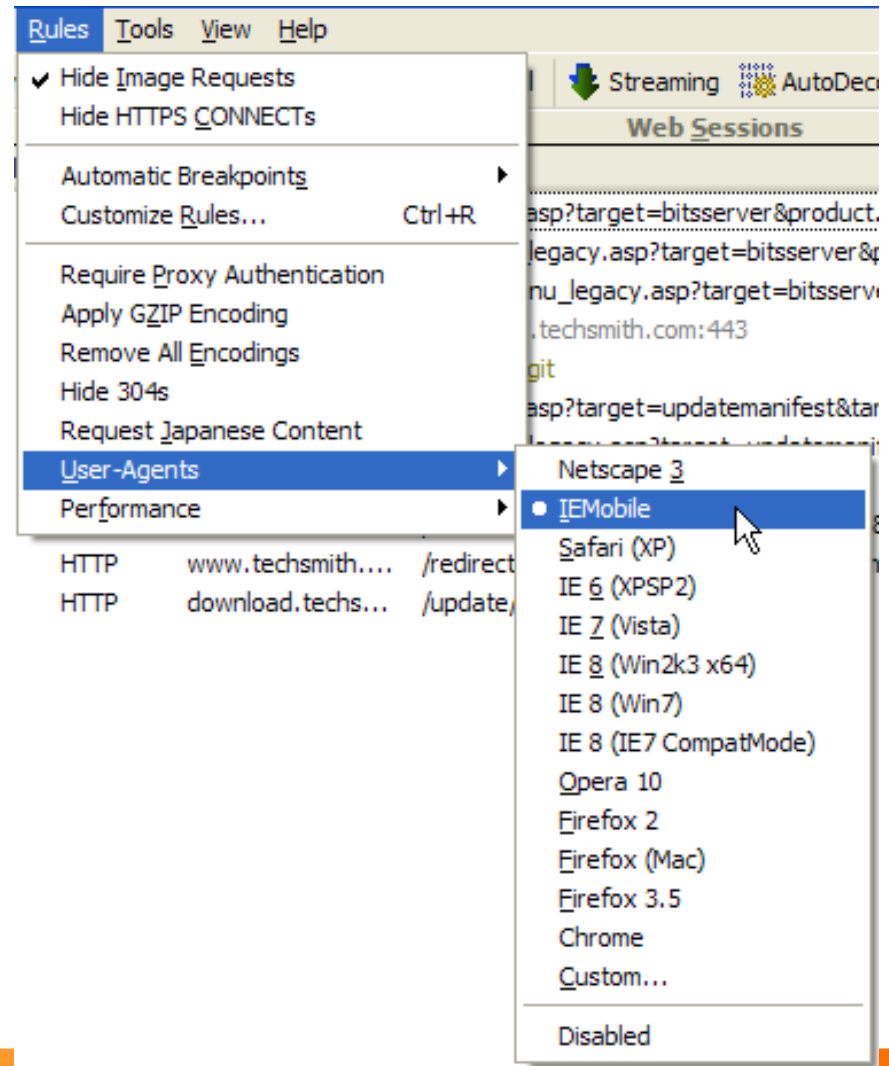


# 界面可以扩展的哦

可以添加新的菜单项  
和tab

Plugins:

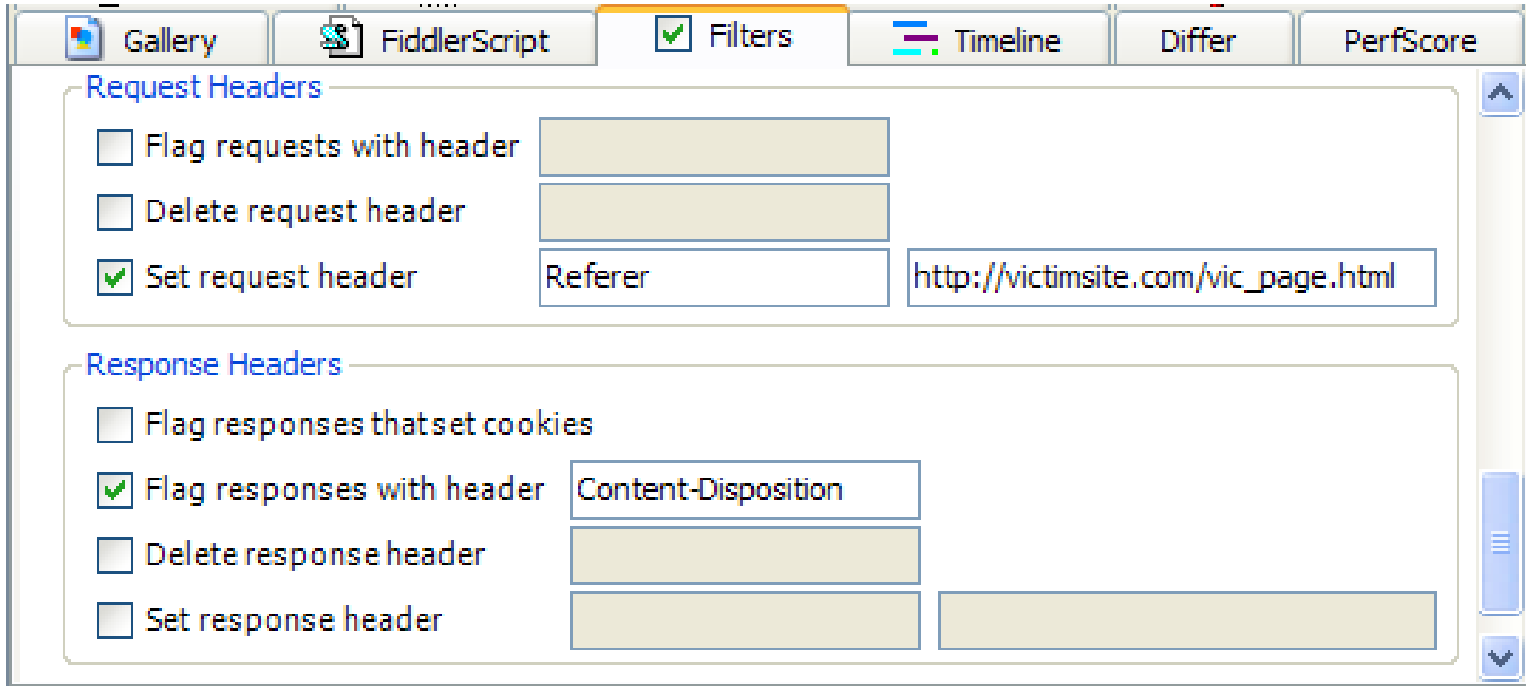
<http://www.fiddlertool.com/Fiddler2/extensions.asp>



**Fiddler**  
Web Debugging Proxy



# 过滤器



- 标记、修改、或隐藏指定特征的数据流



# AutoResponder

Fiddler can return previously generated responses instead of connecting to the server. [Help](#)

Enable automatic responses Use the + and - keys to reorder rules.

Permit passthrough for unmatched requests

| If URI matches...   | then respond with... |
|---|----------------------|
| <input checked="" type="checkbox"/> EXACT:http://s.fsdn.com/sd/ie8-idle.css?T_2_5_0_254a              | 404_Plain.dat        |
| <input checked="" type="checkbox"/> EXACT:http://s.fsdn.com/sd/idlecore-tidied.css?T_2_5_0_254a       | 404_Plain.dat        |
| <input checked="" type="checkbox"/> regex:(?insx).*\.(png jpg)\$ #Match strings ending with img types | 200_FiddlerGif.dat   |
| <input checked="" type="checkbox"/> TargetFile.js   | *bpafter             |

Rule Editor

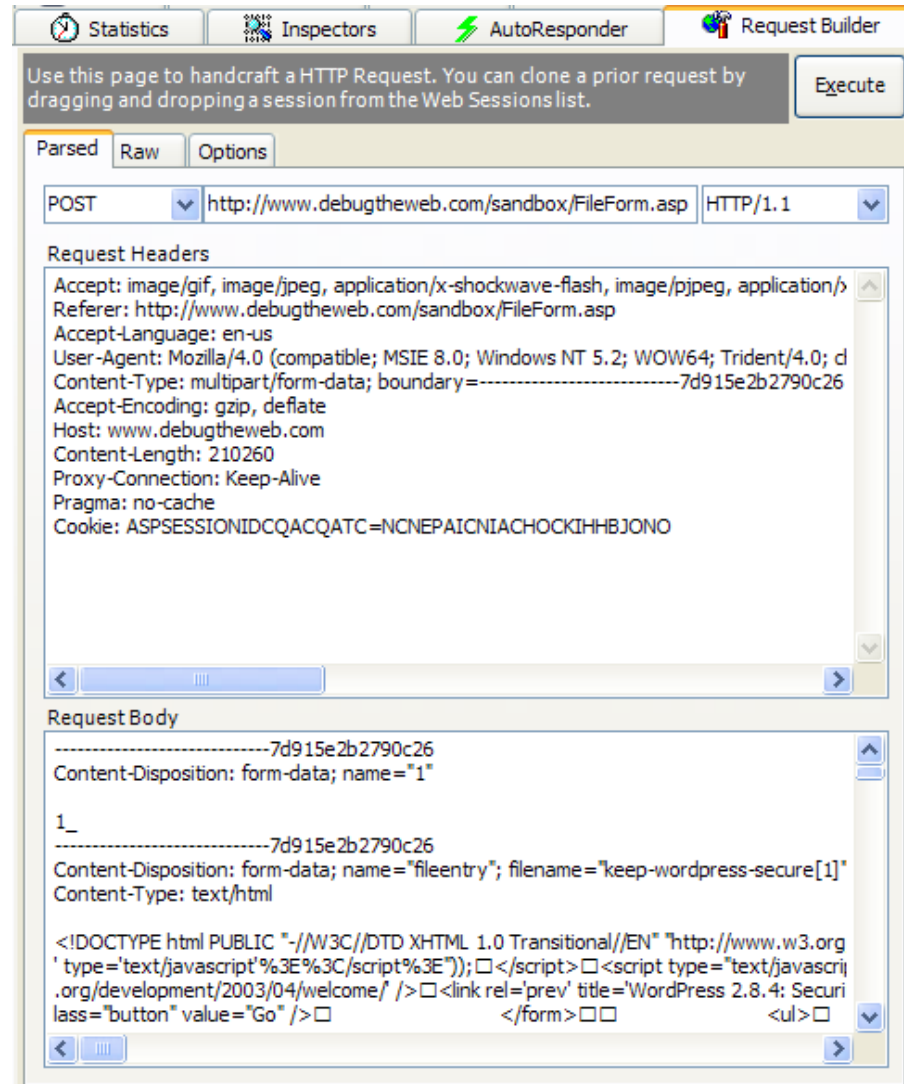
regex:(?insx).\*\.(png) 200\_FiddlerGif.dat

- 改写返回数据，最实用的功能



# Request Builder

手动创建一个请求,  
或者修改后重发一个  
请求



The screenshot shows the Fiddler Request Builder interface. At the top, there are tabs for Statistics, Inspectors, AutoResponder, and Request Builder. Below the tabs is a grey bar with the text: "Use this page to handcraft a HTTP Request. You can clone a prior request by dragging and dropping a session from the Web Sessions list." and an "Execute" button.

The main area is divided into three tabs: "Parsed", "Raw", and "Options". The "Parsed" tab is selected. It shows a dropdown menu set to "POST" and a text field containing the URL "http://www.debugtheweb.com/sandbox/FileForm.asp". To the right of the URL is another dropdown menu set to "HTTP/1.1".

Below the URL field is a section titled "Request Headers". It contains a list of headers:

- Accept: image/gif, image/jpeg, application/x-shockwave-flash, image/pjpeg, application/
- Referer: http://www.debugtheweb.com/sandbox/FileForm.asp
- Accept-Language: en-us
- User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; WOW64; Trident/4.0; d
- Content-Type: multipart/form-data; boundary=-----7d915e2b2790c26
- Accept-Encoding: gzip, deflate
- Host: www.debugtheweb.com
- Content-Length: 210260
- Proxy-Connection: Keep-Alive
- Pragma: no-cache
- Cookie: ASPSESSIONIDCQACQATC=NCNEPAICNIACHOCKIHBJONO

Below the headers is a section titled "Request Body". It shows a multipart form-data structure:

```
-----7d915e2b2790c26
Content-Disposition: form-data; name="1"

1_
-----7d915e2b2790c26
Content-Disposition: form-data; name="fileentry"; filename="keep-wordpress-secure[1]"
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org
' type='text/javascript'%3E%3C/script%3E");</script><script type='text/javascrri
.org/development/2003/04/welcome/' /><link rel='prev' title='WordPress 2.8.4: Securi
lass="button" value="Go" /><
</form><
<ul><
```



# 比较数据流

使用比较器比较不同数据流  
的请求和返回的数据。

The screenshot shows the 'Web Sessions' window in Fiddler. It contains a table with columns 'Host' and 'URL'. The first two rows are for 'www.bayden.com /ua.aspx' and the third is for 'www.ysgyfarno... /utilities/mou'. A context menu is open over the second row, listing actions like 'Decode Selected Sessions', 'AsText', 'Refresh Selected Sessions', 'AutoScroll Session List', 'Copy', 'Save', 'Remove', 'Comment...', 'Mark', 'Replay', 'Select', and 'Compare' (highlighted in blue with 'Ctrl+W').

| Host             | URL            | Bo  |
|------------------|----------------|-----|
| www.bayden.com   | /ua.aspx       | 6,6 |
| www.bayden.com   | /ua.aspx       | 6,6 |
| www.ysgyfarno... | /utilities/mou |     |

- Decode Selected Sessions
- AsText
- Refresh Selected Sessions
- ✓ AutoScroll Session List
- Copy
- Save
- Remove
- Comment...
- Mark
- Replay
- Select
- Compare Ctrl+W

The screenshot shows the WinDiff application window. The title bar says 'WinDiff'. The menu bar includes 'File', 'Edit', 'View', 'Expand', 'Options', 'Mark', and 'Help'. The main window shows a comparison of two files: 's1\_1.txt' and 's2\_6.txt'. The comparison is displayed in a table with columns for line numbers and the content of each file. The content is HTML code, including a heading and browser user-agent information for IE8 and Firefox 3.5.3.

| Line | s1_1.txt | s2_6.txt  |
|------|----------|---|
| 91   | <!       | <hr/><font face="Verdana" size="2"><b>Your browser sent the following |
| [91] | !>       | <hr/><font face="Verdana" size="2"><b>Your browser sent the following |
| 92   | <!       | Type = IE8  |
| 93   | <!       | Name = IE   |
| 94   | <!       | Version = 8.0   |
| 95   | <!       | Major Version = 8   |
| 96   | <!       | Minor Version = 0   |
|      | !>       | Type = Firefox3.5.3   |
|      | !>       | Name = Firefox  |
|      | !>       | Version = 3.5.3   |
|      | !>       | Major Version = 3   |
|      | !>       | Minor Version = 0.5   |
| 97   |          | Platform = WinNT  |
| 98   |          | Is Beta = False   |



# 文本编码和解码

## 一些常用的文本 编码转换

TextWizard [540 => 404 chars]

```
ZnVuY3Rpb24gX19TZW5kWG1sSHR0cFJlcXVlc3QodXJsKQ0Kew0KICAgdmFyl  
HhthbGh0dHA9bnVsbDsNCiAgIGlmCh3aW5kb3cuWE1MSHR0cFJlcXVlc3QpDQog  
ICB7Ly8gY29kZSBmb3IgRmlyZWZveCwgT3BlcmEslEiFNywgZXRjLg0KICAgICAge  
G1saHR0cD1uZXcgWE1MSHR0cFJlcXVlc3QoKTsNCiAgIH0NCiAgIGVsc2UgaW  
YgKHdpbmRvdy5BY3RpdmVYT2JqZWNOkQ0KICAgey8vIGNvZGUgZm9yIEiFNiw  
gSUU1DQogICAgICB4bWxodHRwPW5ldyBBY3RpdmVYT2JqZWNOkCJNaWNyb3  
NvZnQuWE1MSFRUUCIpOw0KICAgfQ0KDQogICBpZiAoeG1saHR0cCE9bnVsbC  
kNCiAgIHsNCiAgICAgIHhthbGh0dHAub3BibigiR0VUlix1cmwsdHJ1ZSk7DQogICAg  
CB4bWxodHRwLnNlbnQobnVsbCk7DQogICB9DQp9DQo=
```

To Base64  
 From Base64  
 URLEncode  
 URLDecode  
 HexEncode  
 To JS string  
 From JS string  
 HTML Encode  
 HTML Decode  
 To UTF-7  
 From UTF-7  
 To DeflatedSAML  
 From DeflatedSAML  
 View bytes

```
function __SendXmlHttpRequest(url)  
{  
    var xmlhttp=null;  
    if (window.XMLHttpRequest)  
        {  
        // code for Firefox, Opera, IE7, etc.  
        xmlhttp=new XMLHttpRequest();  
        }  
    else if (window.ActiveXObject)  
        {  
        // code for IE6, IE5  
        xmlhttp=new ActiveXObject("Microsoft.XMLHTTP");  
        }  
    if (xmlhttp!=null)  
        {  
        xmlhttp.open("GET",url,true);  
        xmlhttp.send(null);  
        }  
}
```



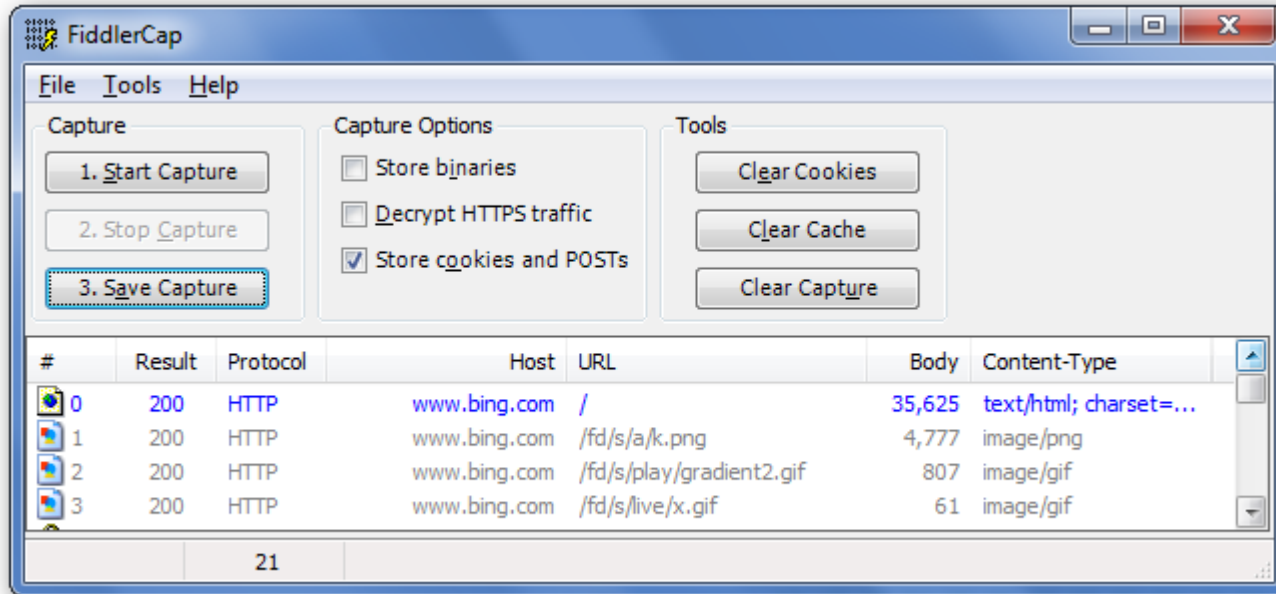


# SAZ Files

- “Session Archive ZIP” 文件保存数据流.
- SAZ 文件压缩数据，可以设密码保护.
- SAZ 文件可以由Fiddler重新打开.
- FiddlerCap可以由远程（一般是用户）录制，开发工程师打开分析数据流.



# FiddlerCap



FiddlerCap用来嗅探和保存

[www.fiddlercap.com](http://www.fiddlercap.com)



来点实例吧！



**Fiddler**  
Web Debugging Proxy



# 案例1：分析页面性能



# 案例2：不绑定，调试js程序



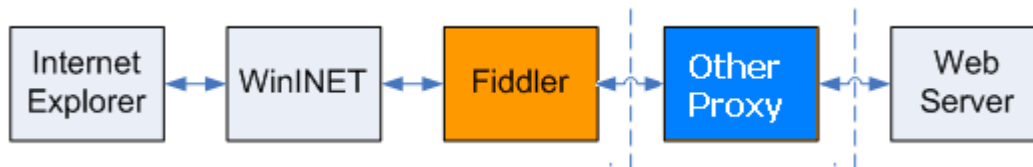
# 案例3：模拟慢速网络

- Modem
- Server is down



# tips

- Firefox
- Non-Windows
- Fiddler和其他代理服务器一起工作



# 更高级的内容





- https嗅探
- Fiddler rule编写
- 插件开发
- Fiddler 作为反向代理服务器



# Q&A



**Fiddler**  
Web Debugging Proxy



Thank you!



**Fiddler**  
Web Debugging Proxy

