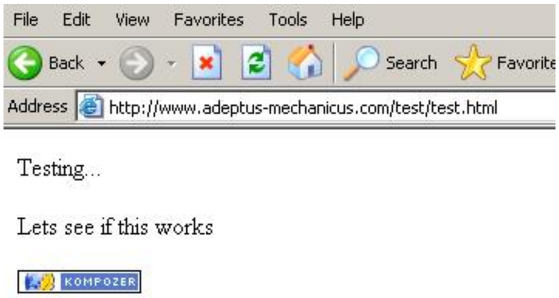
ATTACKING USERS - WEB IFRAMES

I had always heard the term *"attacking the web user"* and acknowledged it with a academic understanding. But recently I have had to update my perception as I am seeing for myself how such attacks can cause damage to a company and to a person. I admit freely that my web security skills are not great but I have been motivated to learn more, as I try to get to grips with this. Lets start off with a "thought experiment".

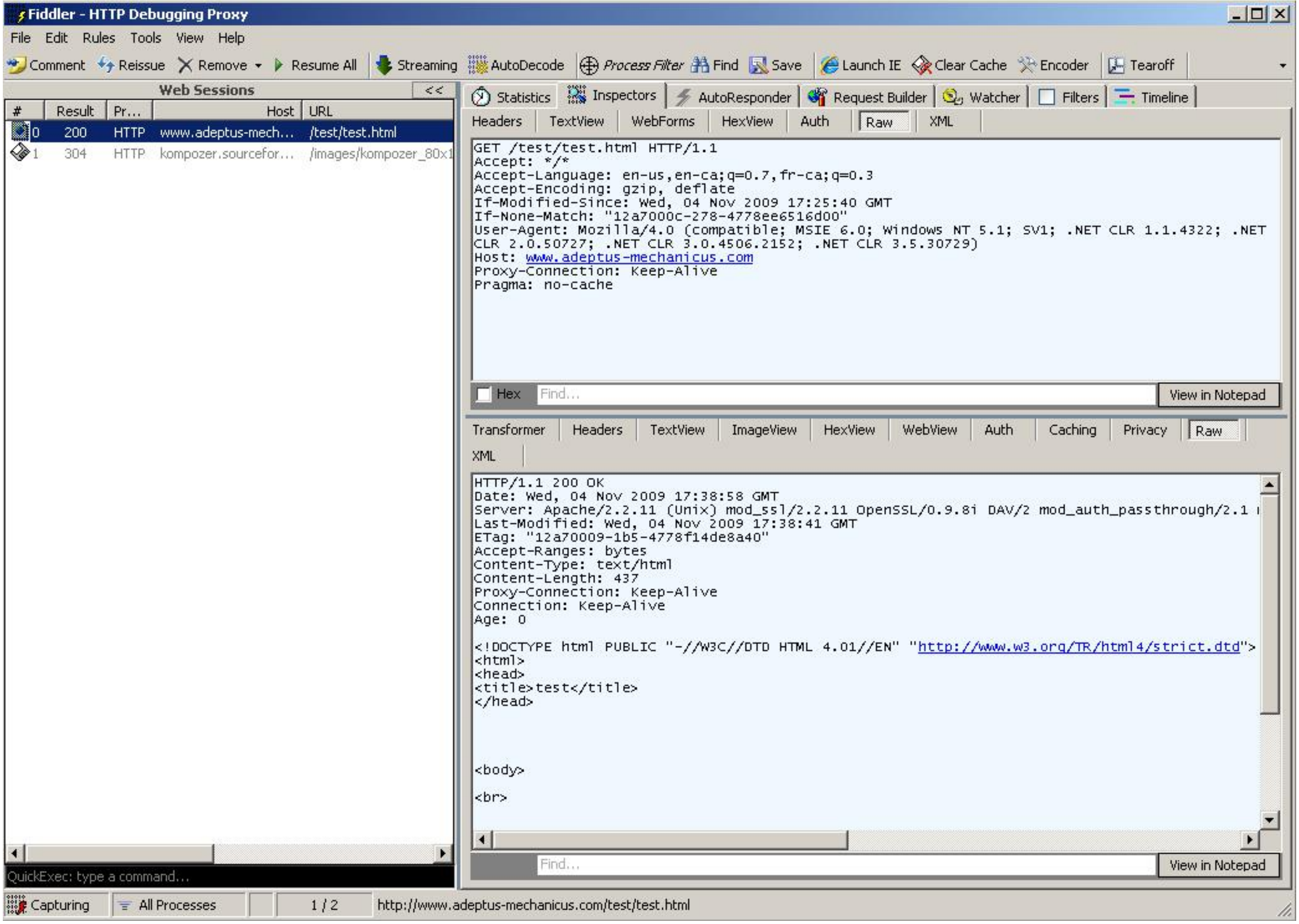
You are browsing a site, and you get to a screen like this..



Testing...

Lets see if this works

Now also lets imagine you just happened to also be running a local type of web proxy, say something like *fiddler* (see here), what you would expect to see is something like this..

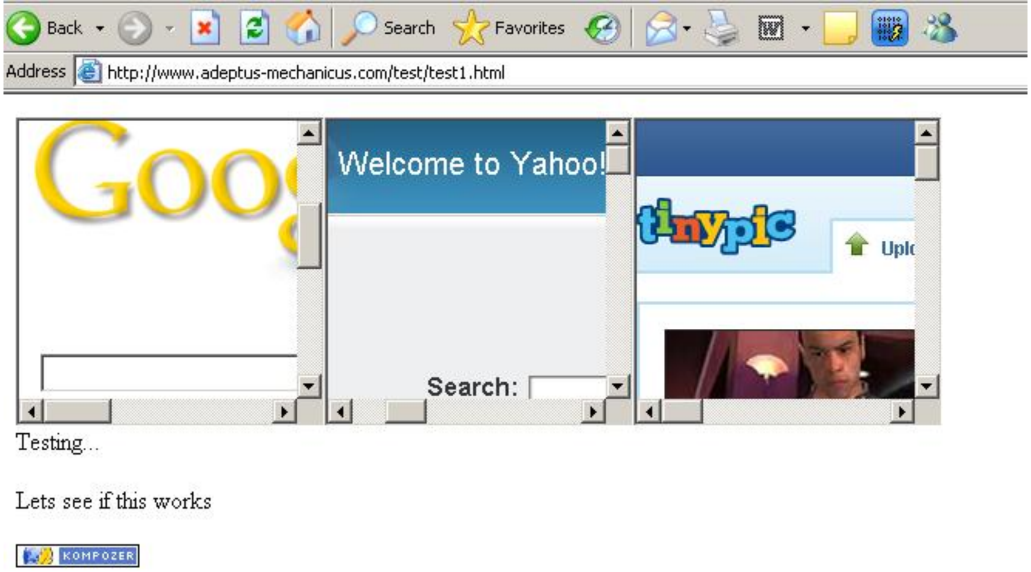


#	Result	Pr...	Host	URL
0	200	HTTP	www.adeptus-mech...	/test/test.html
1	304	HTTP	kompozer.sourcefor...	/images/kompozer_80x1

```
GET /test/test.html HTTP/1.1
Accept: */*
Accept-Language: en-us,en-ca;q=0.7,fr-ca;q=0.3
Accept-Encoding: gzip, deflate
If-Modified-Since: Wed, 04 Nov 2009 17:25:40 GMT
If-None-Match: "12a7000c-278-4778ee6516d00"
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET
CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: www.adeptus-mechanicus.com
Proxy-Connection: Keep-Alive
Pragma: no-cache
```

```
HTTP/1.1 200 OK
Date: Wed, 04 Nov 2009 17:38:58 GMT
Server: Apache/2.2.11 (Unix) mod_ssl/2.2.11 OpenSSL/0.9.8i DAV/2 mod_auth_passthrough/2.1
Last-Modified: Wed, 04 Nov 2009 17:38:41 GMT
ETag: "12a70009-1b5-4778f14de8a40"
Accept-Ranges: bytes
Content-Type: text/html
Content-Length: 437
Proxy-Connection: Keep-Alive
Connection: Keep-Alive
Age: 0

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<title>test</title>
</head>



<body>

<br>
```

All fine and well, as to be expected. Now stop for a bit. Think about if you were a firewall admin, the web proxy admin, whoever would have cause to review traffic. If you had seen this session, you would have seen the user access that webpage. Great. Now lets move forward. Lets assume the initial page was a little different, say it looked like this..



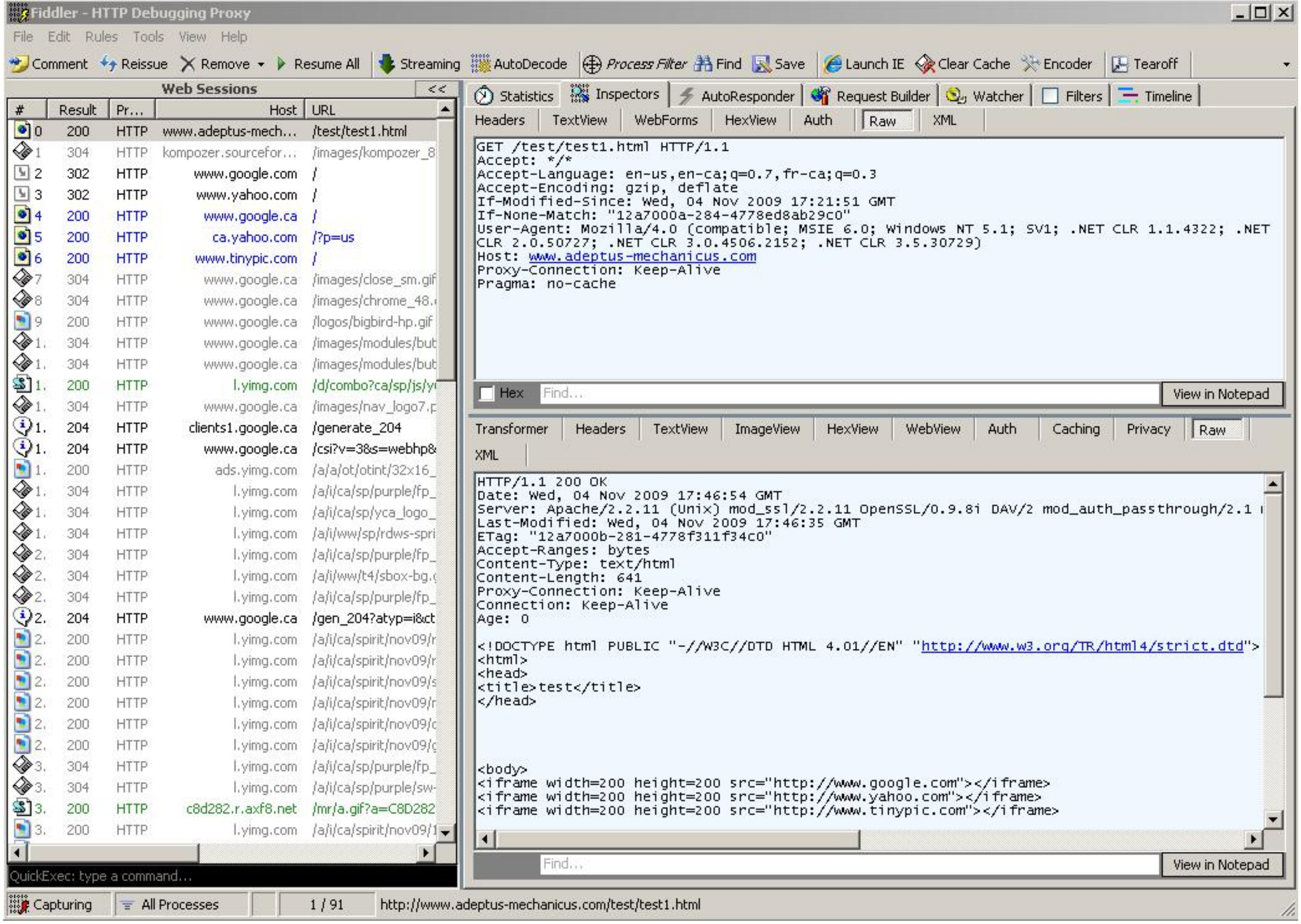
Testing...

Lets see if this works

Hmmm. There are 3 Iframes embedded into the page to three popular sites, the actual html code for this is..

```
<iframe width=200 height=200 src="http://www.google.com"></iframe>
<iframe width=200 height=200 src="http://www.yahoo.com"></iframe>
<iframe width=200 height=200 src="http://www.tinypic.com"></iframe>
```

As for your web traffic..



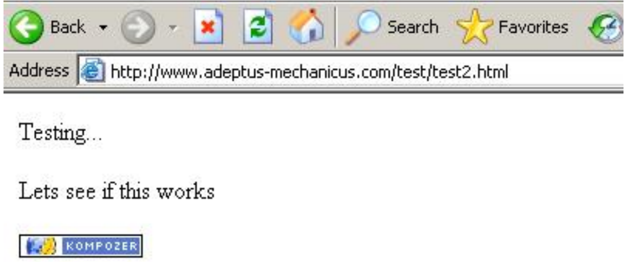
#	Result	Pr...	Host	URL
0	200	HTTP	www.adeptus-mech...	/test/test1.html
1	304	HTTP	kompozer.sourcefor...	/images/kompozer_8
2	302	HTTP	www.google.com	/
3	302	HTTP	www.yahoo.com	/
4	200	HTTP	www.google.ca	/
5	200	HTTP	ca.yahoo.com	/?p=us
6	200	HTTP	www.tinypic.com	/
7	304	HTTP	www.google.ca	/images/close_sm.gif
8	304	HTTP	www.google.ca	/images/chrome_48.
9	200	HTTP	www.google.ca	/logos/bigbird-hp.gif
1.	304	HTTP	www.google.ca	/images/modules/but
1.	304	HTTP	www.google.ca	/images/modules/but
1.	200	HTTP	l.yimg.com	/d/combo?ca/sp/js/y
1.	304	HTTP	www.google.ca	/images/nav_logo7.p
1.	204	HTTP	clients1.google.ca	/generate_204
1.	204	HTTP	www.google.ca	/csi?v=3&s=webhp&
1.	200	HTTP	ads.yimg.com	/a/a/ot/otint/32x16_
1.	304	HTTP	l.yimg.com	/a/i/ca/sp/purple/fp_
1.	304	HTTP	l.yimg.com	/a/i/ca/sp/yca_logo_
1.	304	HTTP	l.yimg.com	/a/i/ww/sp/rdws-spri
2.	304	HTTP	l.yimg.com	/a/i/ca/sp/purple/fp_
2.	304	HTTP	l.yimg.com	/a/i/ww/t4/sbox-bg.
2.	304	HTTP	l.yimg.com	/a/i/ca/sp/purple/fp_
2.	204	HTTP	www.google.ca	/gen_204?atyp=i&ct
2.	200	HTTP	l.yimg.com	/a/i/ca/spirit/nov09/r
2.	200	HTTP	l.yimg.com	/a/i/ca/spirit/nov09/r
2.	200	HTTP	l.yimg.com	/a/i/ca/spirit/nov09/s
2.	200	HTTP	l.yimg.com	/a/i/ca/spirit/nov09/r
2.	200	HTTP	l.yimg.com	/a/i/ca/spirit/nov09/c
2.	200	HTTP	l.yimg.com	/a/i/ca/spirit/nov09/g
3.	304	HTTP	l.yimg.com	/a/i/ca/sp/purple/fp_
3.	304	HTTP	l.yimg.com	/a/i/ca/sp/purple/sw-
3.	200	HTTP	c8d282.r.axf8.net	/mr/a.gif?a=C8D282
3.	200	HTTP	l.yimg.com	/a/i/ca/spirit/nov09/1

```
GET /test/test1.html HTTP/1.1
Accept: */*
Accept-Language: en-us,en-ca;q=0.7,fr-ca;q=0.3
Accept-Encoding: gzip, deflate
If-Modified-Since: Wed, 04 Nov 2009 17:21:51 GMT
If-None-Match: "12a7000a-284-4778ed8ab29c0"
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET
CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: www.adeptus-mechanicus.com
Proxy-Connection: Keep-Alive
Pragma: no-cache
```

```
HTTP/1.1 200 OK
Date: Wed, 04 Nov 2009 17:46:54 GMT
Server: Apache/2.2.11 (Unix) mod_ssl/2.2.11 OpenSSL/0.9.8i DAV/2 mod_auth_passthrough/2.1
Last-Modified: Wed, 04 Nov 2009 17:46:35 GMT
ETag: "12a7000b-281-4778f311f34c0"
Accept-Ranges: bytes
Content-Type: text/html
Content-Length: 641
Proxy-Connection: Keep-Alive
Connection: Keep-Alive
Age: 0

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<title>test</title>
</head>



<body>
<iframe width=200 height=200 src="http://www.google.com"></iframe>
<iframe width=200 height=200 src="http://www.yahoo.com"></iframe>
<iframe width=200 height=200 src="http://www.tinypic.com"></iframe>
```

So what we can see, is that without you clicking on anything on the initial page, the site got your browser to intiate connections out to other sites.

But so what you ask, I can see it, sure it badly designed, but so what? Lets just tweak the html a bit and try a new page, it looks like this..

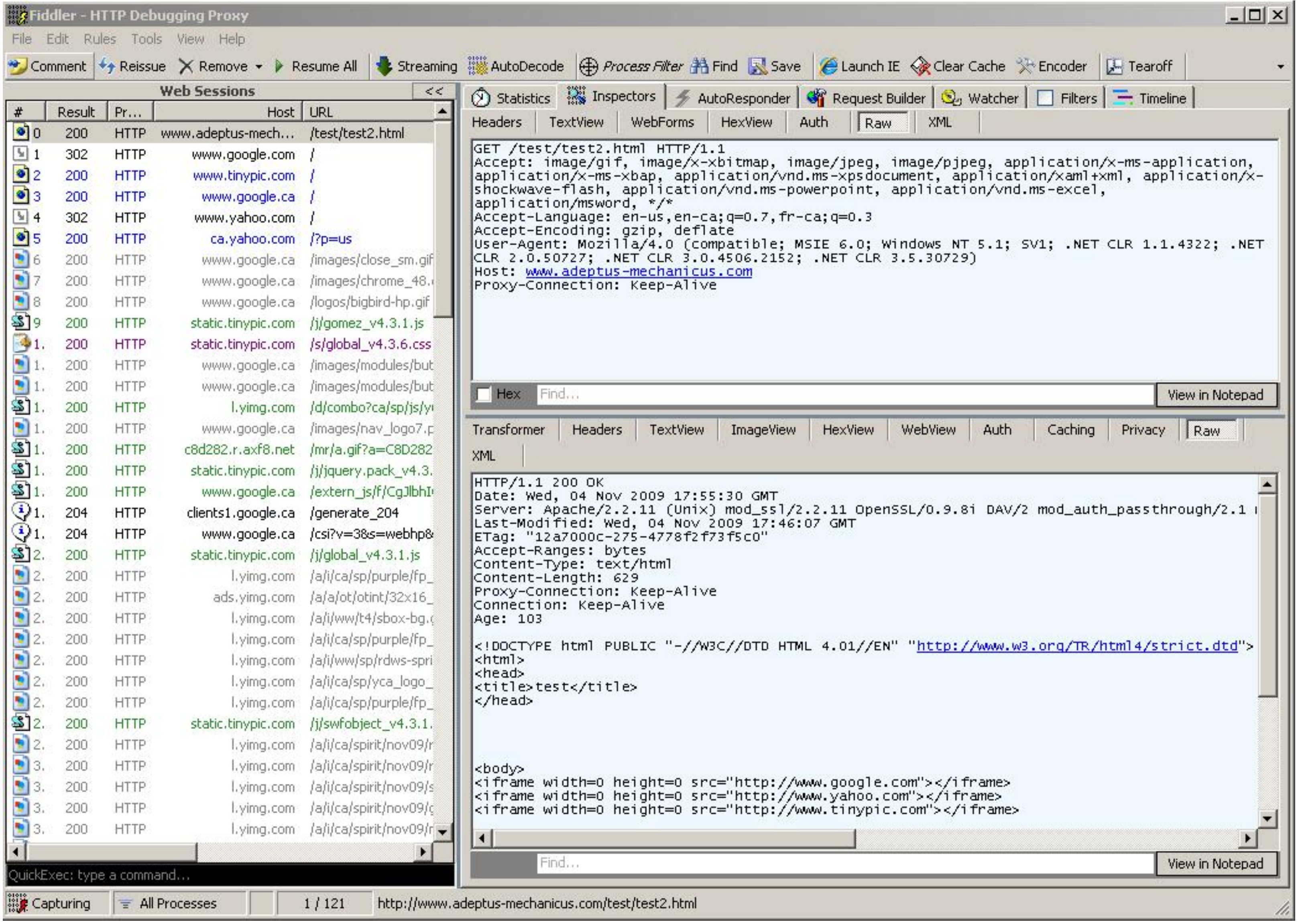


http://www.adeptus-mechanicus.com/test/test2.html

Testing...

Lets see if this works

Looks a lot like the first screen? But what does your proxy show? Lets take a look..


Fiddler - HTTP Debugging Proxy
File Edit Rules Tools View Help
Comment Reissue Remove Resume All Streaming AutoDecode Process Filter Find Save Launch IE Clear Cache Encoder Tearoff
Web Sessions
Statistics Inspectors AutoResponder Request Builder Watcher Filters Timeline
Headers TextView WebForms HexView Auth Raw XML
Hex
View in Notepad
Transformer Headers TextView ImageView HexView WebView Auth Caching Privacy Raw
XML
View in Notepad
QuickExec: type a command...
Capturing
All Processes

#	Result	Pr...	Host	URL
0	200	HTTP	www.adeptus-mech...	/test/test2.html
1	302	HTTP	www.google.com	/
2	200	HTTP	www.tinypic.com	/
3	200	HTTP	www.google.ca	/
4	302	HTTP	www.yahoo.com	/
5	200	HTTP	ca.yahoo.com	/?p=us
6	200	HTTP	www.google.ca	/images/close_sm.gif
7	200	HTTP	www.google.ca	/images/chrome_48.
8	200	HTTP	www.google.ca	/logos/bigbird-hp.gif
9	200	HTTP	static.tinypic.com	/j/gomez_v4.3.1.js
1.	200	HTTP	static.tinypic.com	/s/global_v4.3.6.css
1.	200	HTTP	www.google.ca	/images/modules/but
1.	200	HTTP	www.google.ca	/images/modules/but
1.	200	HTTP	l.yimg.com	/d/combo?ca/sp/js/y
1.	200	HTTP	www.google.ca	/images/nav_logo7.p
1.	200	HTTP	c8d282.r.axf8.net	/mr/a.gif?a=C8D282
1.	200	HTTP	static.tinypic.com	/j/jquery.pack_v4.3.
1.	200	HTTP	www.google.ca	/extern_js/f/CgJlbhI
1.	204	HTTP	clients1.google.ca	/generate_204
1.	204	HTTP	www.google.ca	/csi?v=3&s=webhp&
2.	200	HTTP	static.tinypic.com	/j/global_v4.3.1.js
2.	200	HTTP	l.yimg.com	/a/i/ca/sp/purple/fp_
2.	200	HTTP	ads.yimg.com	/a/a/ot/otint/32x16_
2.	200	HTTP	l.yimg.com	/a/i/ww/t4/sbox-bg.
2.	200	HTTP	l.yimg.com	/a/i/ca/sp/purple/fp_
2.	200	HTTP	l.yimg.com	/a/i/ww/sp/rdws-spri
2.	200	HTTP	l.yimg.com	/a/i/ca/sp/yca_logo_
2.	200	HTTP	l.yimg.com	/a/i/ca/sp/purple/fp_
2.	200	HTTP	static.tinypic.com	/j/swfobject_v4.3.1.
2.	200	HTTP	l.yimg.com	/a/i/ca/spirit/nov09/r
3.	200	HTTP	l.yimg.com	/a/i/ca/spirit/nov09/r
3.	200	HTTP	l.yimg.com	/a/i/ca/spirit/nov09/s
3.	200	HTTP	l.yimg.com	/a/i/ca/spirit/nov09/g
3.	200	HTTP	l.yimg.com	/a/i/ca/spirit/nov09/r

```
GET /test/test2.html HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-ms-application,
application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, application/x-
shockwave-flash, application/vnd.ms-powerpoint, application/vnd.ms-excel,
application/msword, */*
Accept-Language: en-us,en-ca;q=0.7,fr-ca;q=0.3
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET
CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: www.adeptus-mechanicus.com
Proxy-Connection: Keep-Alive
```

```
HTTP/1.1 200 OK
Date: Wed, 04 Nov 2009 17:55:30 GMT
Server: Apache/2.2.11 (Unix) mod_ssl/2.2.11 OpenSSL/0.9.8i DAV/2 mod_auth_passthrough/2.1
Last-Modified: Wed, 04 Nov 2009 17:46:07 GMT
ETag: "12a7000c-275-4778f2f73f5c0"
Accept-Ranges: bytes
Content-Type: text/html
Content-Length: 629
Proxy-Connection: Keep-Alive
Connection: Keep-Alive
Age: 103

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<title>test</title>
</head>



<body>
<iframe width=0 height=0 src="http://www.google.com"></iframe>
<iframe width=0 height=0 src="http://www.yahoo.com"></iframe>
<iframe width=0 height=0 src="http://www.tinypic.com"></iframe>
```

1 / 121

http://www.adeptus-mechanicus.com/test/test2.html

Interesting. So what we see is that while you saw nothing, your browser still made requests to those 3 sites. This is done very simply by changing the previous code for the iframes to..

```
<iframe width=0 height=0 src="http://www.google.com"></iframe>
<iframe width=0 height=0 src="http://www.yahoo.com"></iframe>
<iframe width=0 height=0 src="http://www.tinypic.com"></iframe>
```

Now lets stop and think again. You are firewall admin and you see this user visiting a banned site, but did he? A user has accessed a malware page, but did he? Or from another point of view, if you can modify the code of a popular site, or even if you are the admin of a popular site, you put a couple of iframes in the code and add in a refresh metatag, point the iframes to a site you want to DOS, and away you go. The target will never see traffic coming from you, since all the client browsers are initiating the sessions. Or say you wanted to push up your online ad revenue, you could point visitors to ad-links, and the users would never know they visited the page and made you a little richer. And have no doubt there are many ways to skin this cat, you could use javascript to accomplish the same thing, except put a delay between each iframe so that not everything is fired off at once. And with the amount of legimate websites getting hacked (google that and have fun reading), things get interesting.

Final Words

I realise this is old hat for many people, but it just once agian brought home to me a couple of things;

- Remember you can only check for what you know. If you do not know this, then according to your logs -which do not lie- the user is guilty
- Remember attackers go for bulk, if not then no home users would get hit, but we all know that is not true. Everyone is a target.
- Be careful what you take as evidence, things can very easily be more then they appear.

As always, try it out, have fun and learn.