

Google
www.google.com

www.google.com

www.google.com

www.google.com

www.google.com

www.google.com

www.google.com

www.google.com

www.google.com

www.google.com

www.google.com

www.google.com

www.google.com

www.google.com

www.google.com

www.google.com

www.google.com

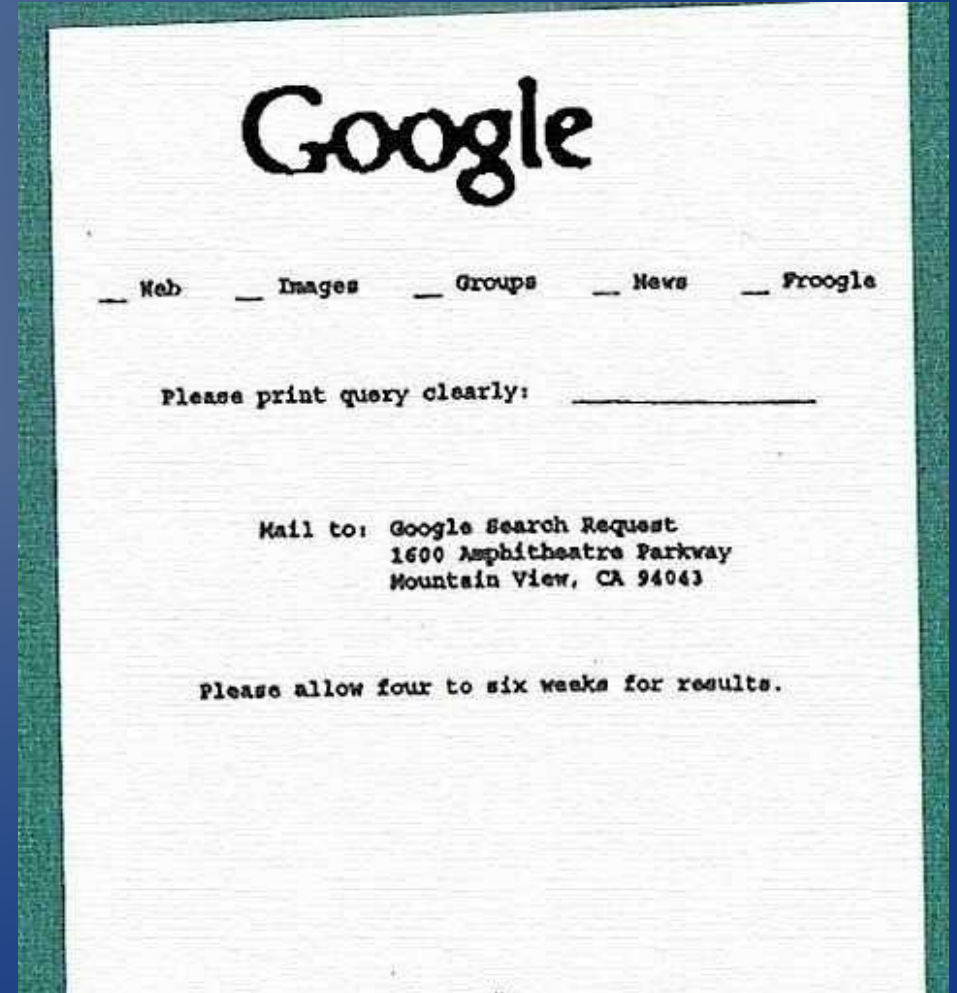
www.google.com

Google™
Toolbar:
The NARC Within

Google Toolbar: The NARC Within

“The” Google

What would we do
without them/it?



Google Toolbar: The NARC Within

The problem:
URLS are the
geek tool?
URLs, URLs
everywhere...
Home, work,
on the go?



Google Toolbar: The NARC Within

Google Toolbar is the
Solution?



Google Toolbar: The NARC Within

Or just a tease?



Google Toolbar: The NARC Within

Of course it's good, it's
free!

Adobe Flash Player



Install Adobe Flash Player

Adobe Flash Player version 9.0.124.0
Windows, Internet Explorer
Different operating system or browser?

1.5MB

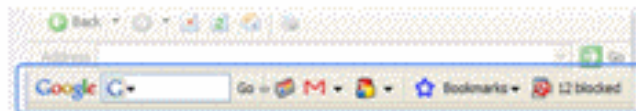
[Learn more](#) | [System requirements](#) | [Distribute Flash Player](#) | [Installation instructions](#)



Also install:

Free Google Toolbar (optional)

0.8MB



Search Google from any web page, block pop-ups

[Learn more](#) | [Privacy policy](#) | [License](#)

You must close all other browser windows before installing.
Download time estimate: 2 minutes @ 56K modem

↓ Agree and install now

Total:
1.5MB

Google Toolbar: The NARC Within

Installs easy..

Stores URLs..

Access them
wherever, whenever
you need it

No more lost URLs!

Happy!



~ **SOME DAYS** ~
they just start better than others

Google Toolbar: The NARC Within

Time passes....

You bookmark your
discoveries

Happy!



Google Toolbar: The NARC Within

bookmark any pr0n?



Google Toolbar: The NARC Within

Next day at work...

You log in to google
and of course use the
toolbar with all your
handy bookmarked
urls.



Corporate Security

You probably have
a corporate
security
department?



They probably
watch you?

Corporate Security



Maybe they watch
you closely?

Web proxies?

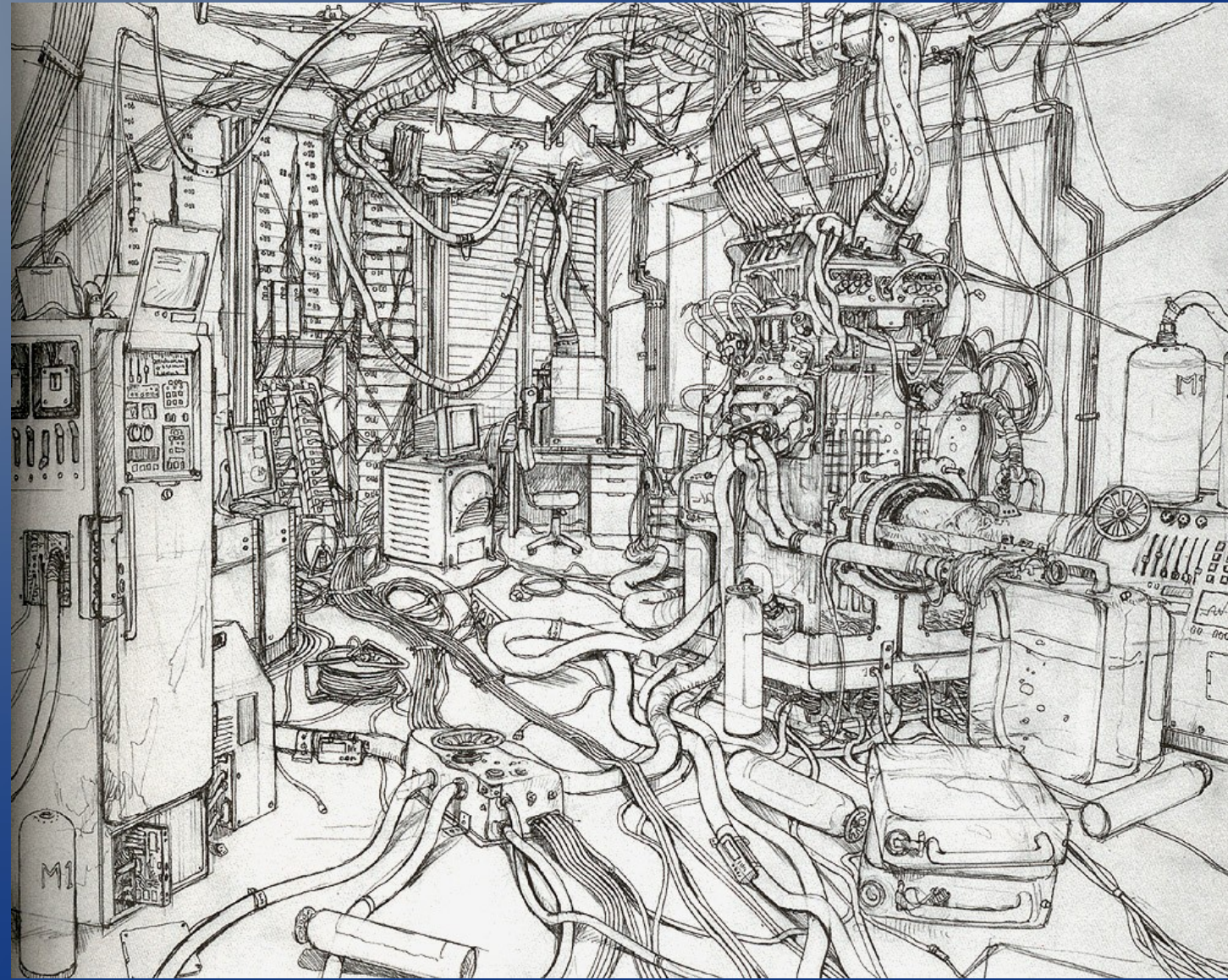
Web filtering?

Web reporting?

Toolbar Traffic

What happens
when you access
the toolbar?

Lets untangle...

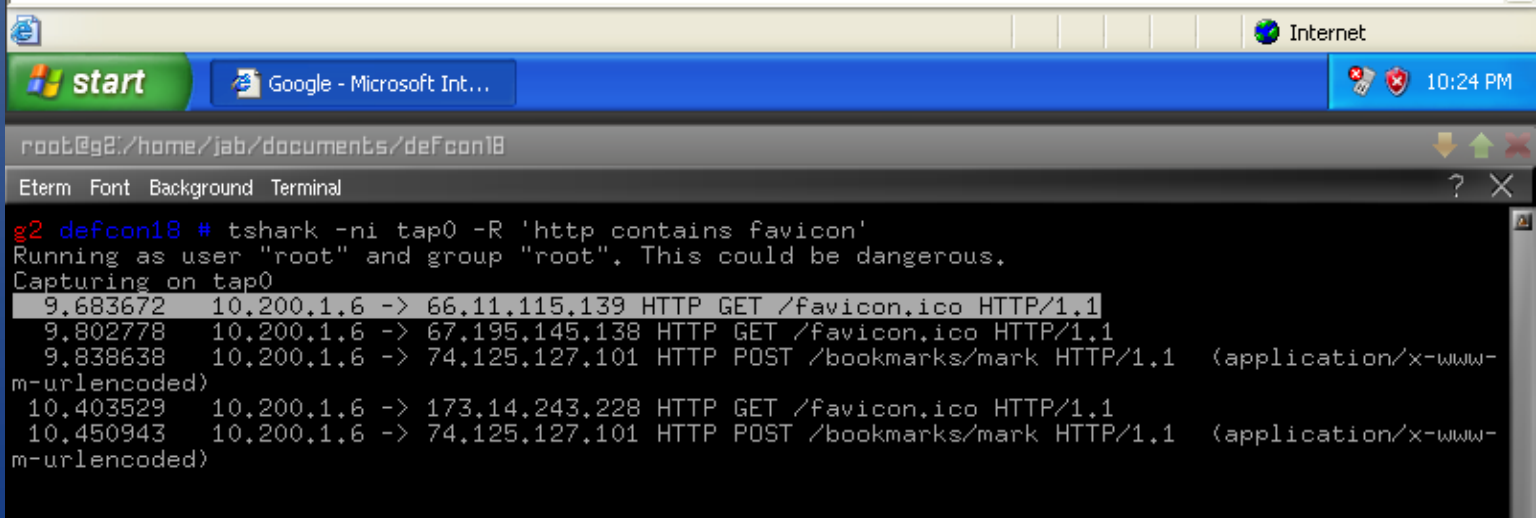
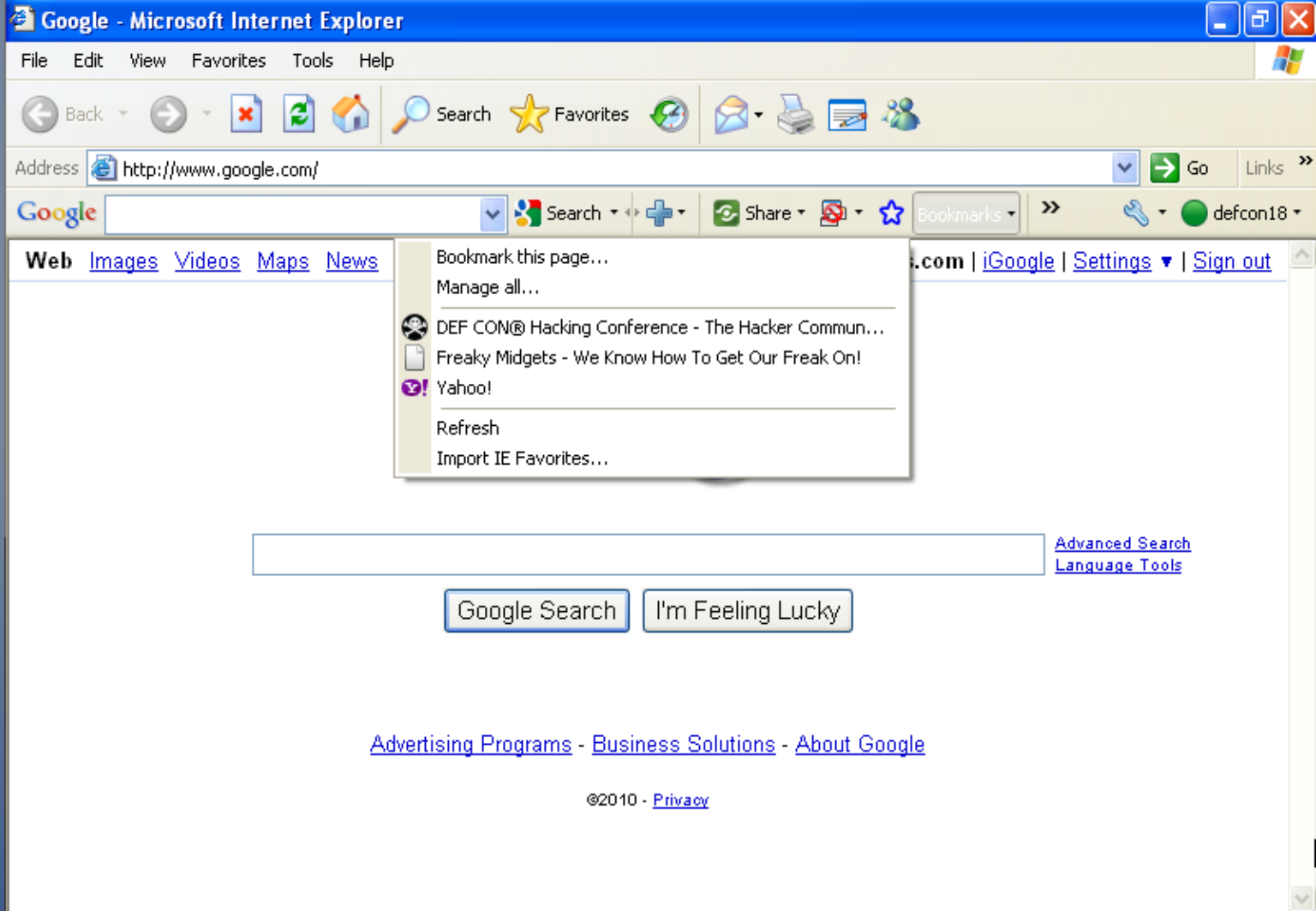


Demonstration



What we saw

For every url, google attempts a hit to the favicon.gif or favicon.ico url





Filter: + Expression... Clear Apply

No. .	Time	Source	Destination	Protocol	Info
184	2010-06-19 23:01:47.135391	72.14.213.138	10.200.1.6	HTTP/XML	HTTP/1.1 200 OK
215	2010-06-19 23:01:49.154271	10.200.1.6	173.14.243.228	HTTP	GET /favicon.ico HTTP/1.1
228	2010-06-19 23:01:49.300198	10.200.1.6	67.195.145.137	HTTP	GET /favicon.ico HTTP/1.1

```

HTTP chunked response
  Data chunk (1032 octets)
  End of chunked encoding
eXtensible Markup Language
  <?xml
  <xml_api_reply
    version="1"
    <bookmarks
      <bookmark
        <title
          DEF CON\302\256 Hacking Conference - The Hacker Commun...
        </title>
        <url>
        <timestamp>
        <id>
        <attributes>
          </bookmark>
      </bookmark>
    <bookmark>
      <title
        Freaky Midgets - We Know How To Get Our Freak On!
      </title>
      <url>
      <timestamp>
      <id>
      <attributes>
        <attribute>
          <name>
            favicon_url
          </name>
          <value>
            http://www.freakymidgets.com/favicon.ico
          </value>
        </attribute>
      </attributes>
    </bookmark>
  </bookmarks>
</xml_api_reply>

```


So?



Fascinating!

Corporate Security

A close-up photograph of a yellow Muppet character, likely from the Muppet Show. The character has a large, black, fuzzy hat and large, round, white eyes with black pupils. The background is a warm, orange-brown color.

Remember they
watch you?

Top 10 porn
viewers now likely
includes you?

Even though you
didn't do anything.

Forensics

When they
investigate you
what will they see?



Bluecoat

Bluecoat one liner to watch traffic in realtime:

```
wget --user=admin --password=supersecret --no-check-certificate -O - -q  
https://10.1.1.1:8082/Accesslog/tail-f//Access-Log
```

Pipe it through grep to narrow the target

```
| grep "10.2.2.2" | grep favicon
```

Forensics

index.dat files?

Nope..the toolbar generated the traffic, not IE.

The image shows a Wireshark capture of a network packet. The packet list pane shows four packets, with packet 236 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol, Transmission Control Protocol, and Hypertext Transfer Protocol. The HTTP request is for a favicon from www.freakymidgets.com, generated by GoogleToolbar.

Favicon.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: http contains favicon

No. .	Time	Source	Destination	Protocol	Info
184	2010-06-19 23:01:47.135391	72.14.213.138	10.200.1.6	HTTP/XML	HTTP/1.1 200 OK
215	2010-06-19 23:01:49.154271	10.200.1.6	173.14.243.228	HTTP	GET /favicon.ico HTTP/1.1
228	2010-06-19 23:01:49.300198	10.200.1.6	67.195.145.137	HTTP	GET /favicon.ico HTTP/1.1
236	2010-06-19 23:01:49.380124	10.200.1.6	66.11.115.139	HTTP	GET /favicon.ico HTTP/1.1

Frame 236 (239 bytes on wire, 239 bytes captured)

- Ethernet II, Src: RealtekU_00:ee:92 (52:54:00:00:ee:92), Dst: 0a:d9:9a:b5:ff:61 (0a:d9:9a:b5:ff:61)
- Internet Protocol, Src: 10.200.1.6 (10.200.1.6), Dst: 66.11.115.139 (66.11.115.139)
- Transmission Control Protocol, Src Port: mil-2045-47001 (1581), Dst Port: http (80), Seq: 1, Ack: 1, Len: 185
- Hypertext Transfer Protocol
 - GET /favicon.ico HTTP/1.1\r\n
 - User-Agent: Mozilla/4.0 (compatible; GoogleToolbar 6.4.1321.1732; Windows XP 5.1; MSIE 6.0.2900.2180)\r\n
 - Host: www.freakymidgets.com\r\n
 - Connection: Keep-Alive\r\n
 - \r\n

Workarounds

Firefox Plugins to the rescue?:

Places pack from Andy Halford:

SyncPlaces:

<https://addons.mozilla.org/en-US/firefox/addon/8426/>

CheckPlaces:


<https://addons.mozilla.org/en-US/firefox/addon/10897/>

SortPlaces:

<https://addons.mozilla.org/en-US/firefox/addon/9275/>

WebDav or file=rsync

SyncPlaces 4.0.7

 <http://www.andyhalford.com/syncplaces>

Remote


Last sent
Last received

Local

XBEL

Status

SyncPlaces 4.0.7

 <http://www.andyhalford.com/syncplaces>

Server Options Advanced

Connection Synchronization

Protocol http https ftp file

Host

User

Password

Run Wizard next time

favicon.ico?

Stored in the .json file generated by syncplaces:

```
{"iconData": [  
  {"uri": "http://s.com/", "faviconuri": "http://s.com/favicon.ic  
o",  
  "mimeType": {"value": "image/png"}, "data":  
  [137,80,78,71,13,10,26,10,0,0,0,13,73,72.....
```

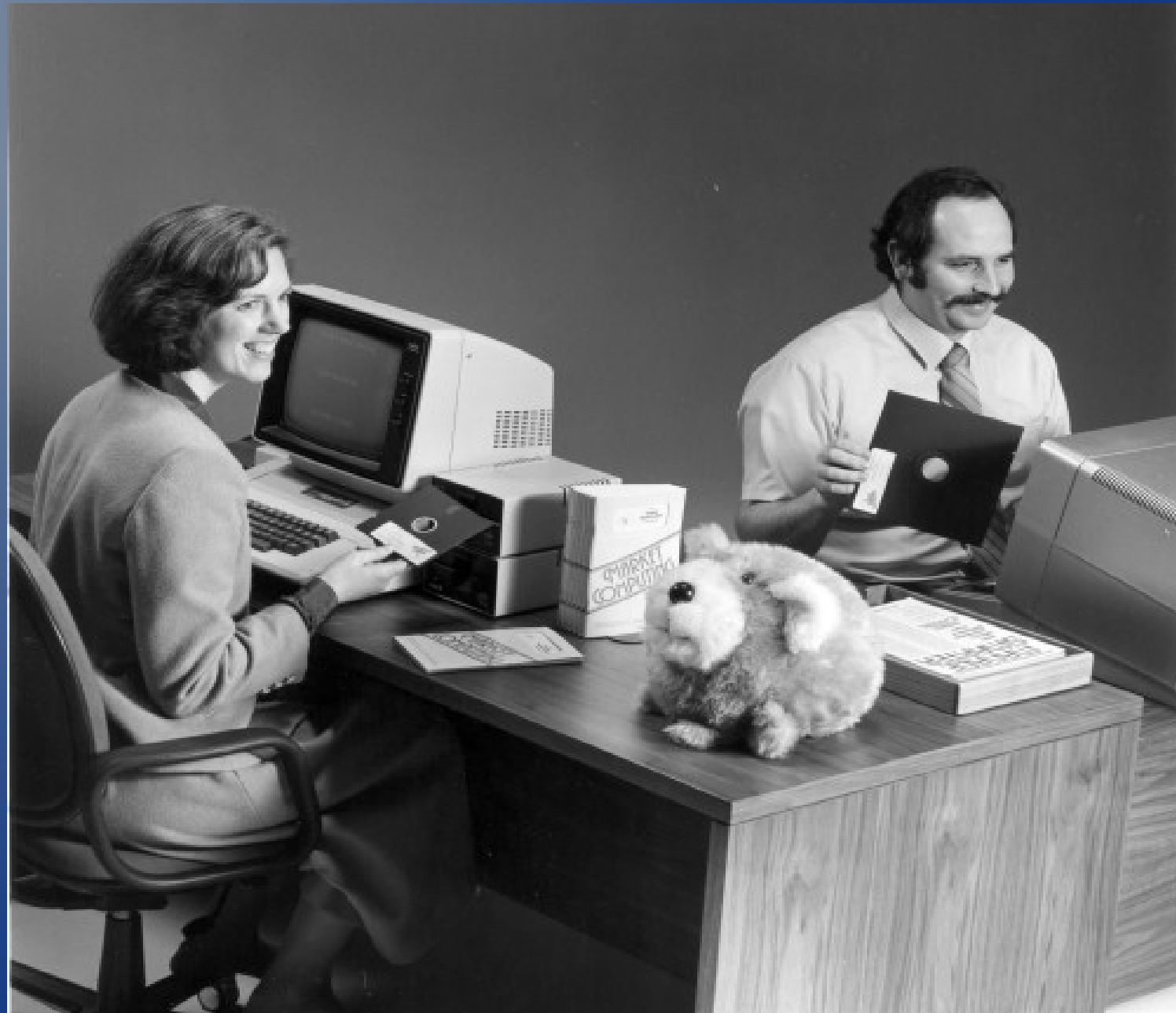

Not so fast...

Retrieve, import
bookmarks via
syncplaces also
triggers firefox to
attempt favicon hits
just like google
toolbar.



What to do?

Duh...
quit
looking
at porn!



What else to do?

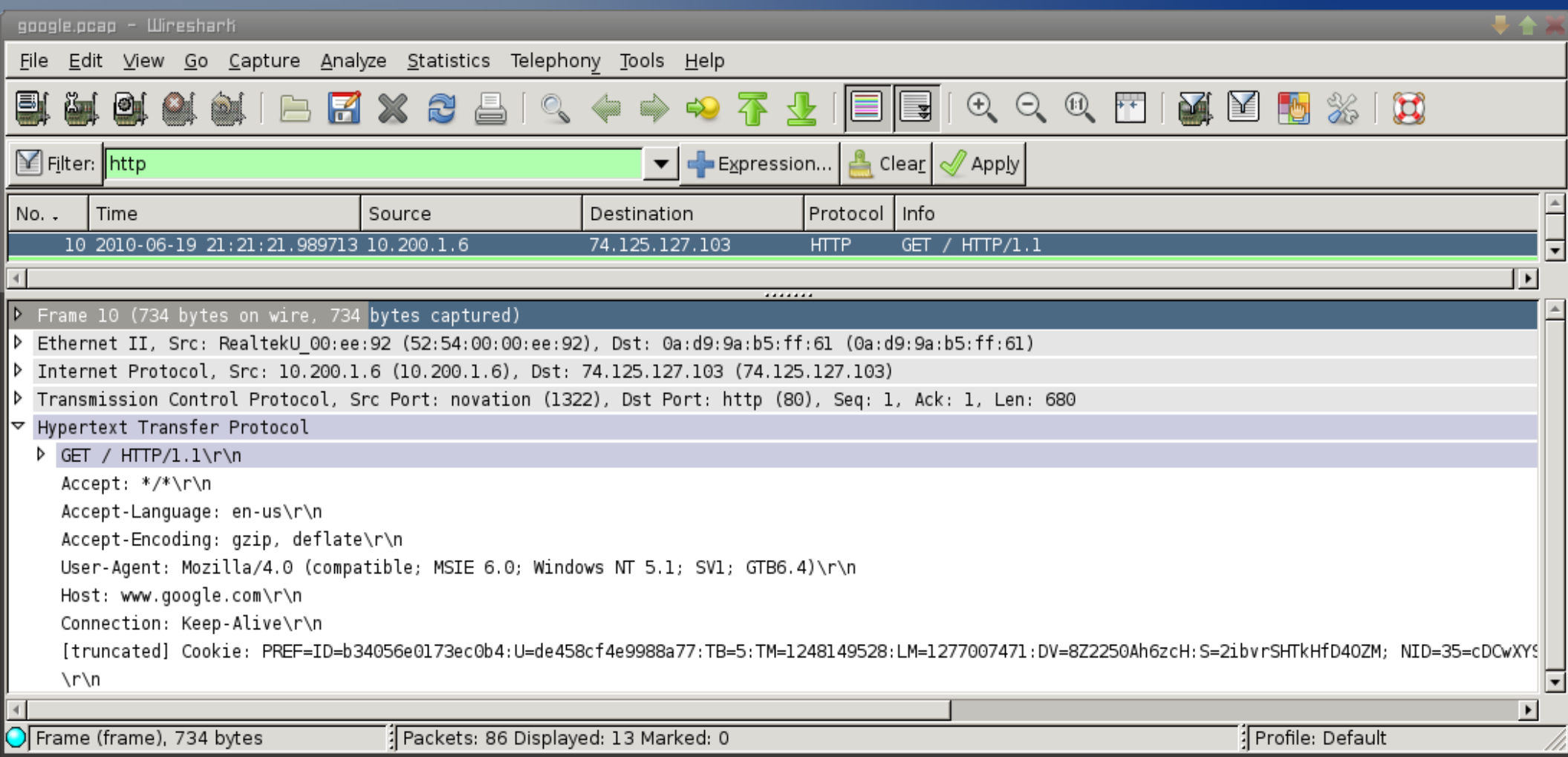
Or, write some code to straighten up the .json and remove bookmarks that you don't want ending up at work.



Toolbar p0wnage?

So what else can we do with this toolbar information?

Normal user agent:



google.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: http

No. .	Time	Source	Destination	Protocol	Info
10	2010-06-19 21:21:21.989713	10.200.1.6	74.125.127.103	HTTP	GET / HTTP/1.1

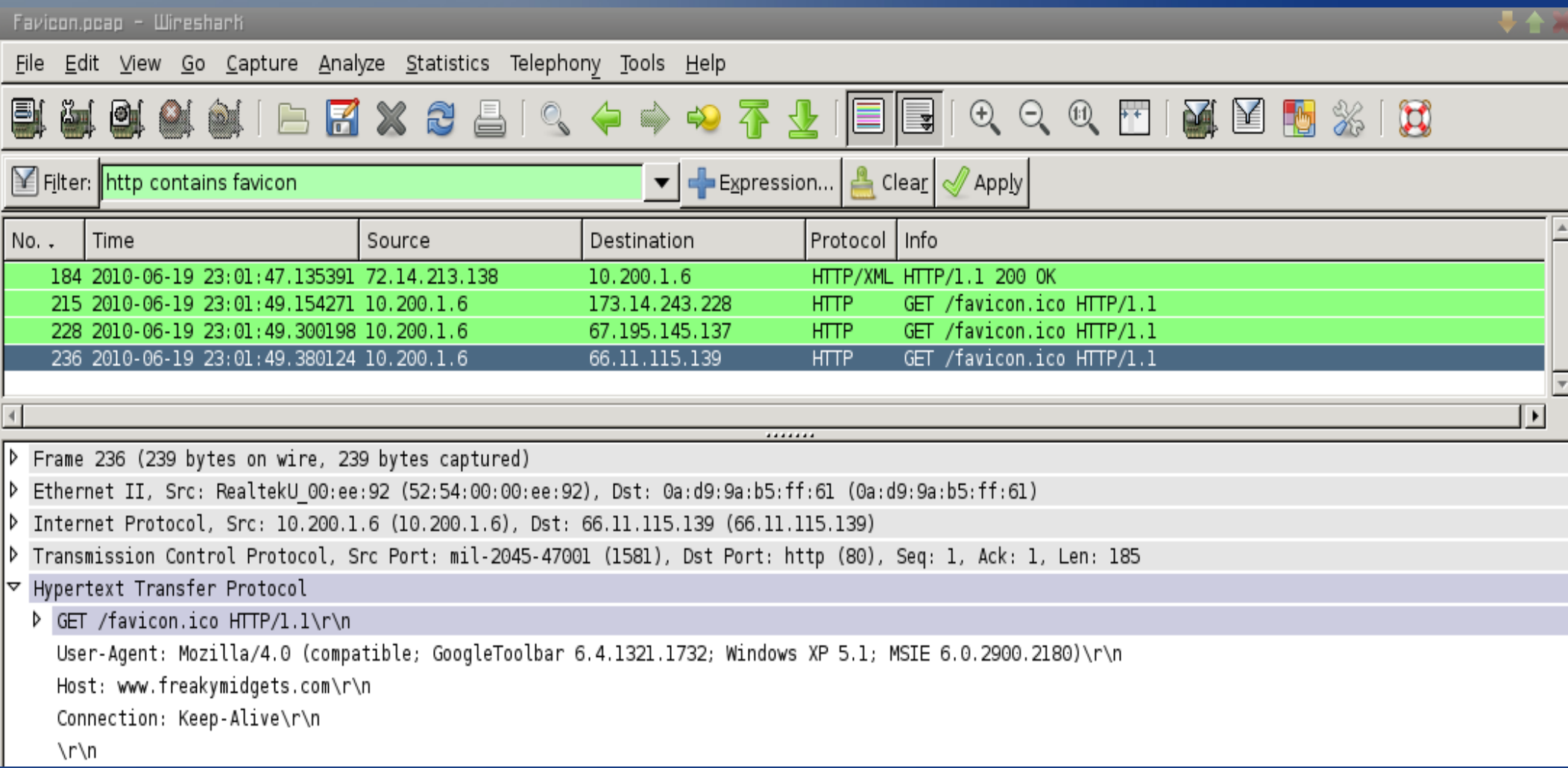
Frame 10 (734 bytes on wire, 734 bytes captured)

- Ethernet II, Src: RealtekU_00:ee:92 (52:54:00:00:ee:92), Dst: 0a:d9:9a:b5:ff:61 (0a:d9:9a:b5:ff:61)
- Internet Protocol, Src: 10.200.1.6 (10.200.1.6), Dst: 74.125.127.103 (74.125.127.103)
- Transmission Control Protocol, Src Port: novation (1322), Dst Port: http (80), Seq: 1, Ack: 1, Len: 680
- Hypertext Transfer Protocol
 - GET / HTTP/1.1\r\n
 - Accept: */*\r\n
 - Accept-Language: en-us\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GTB6.4)\r\n
 - Host: www.google.com\r\n
 - Connection: Keep-Alive\r\n
 - [truncated] Cookie: PREF=ID=b34056e0173ec0b4:U=de458cf4e9988a77:TB=5:TM=1248149528:LM=1277007471:DV=8Z2250Ah6zcH:S=2ibvrSHTkHfD40ZM; NID=35=cDCwXYs\r\n

Frame (frame), 734 bytes | Packets: 86 Displayed: 13 Marked: 0 | Profile: Default

Toolbar p0wnage?

Quite detailed client version info from google:



The image shows a Wireshark capture of a network packet. The packet list pane shows four packets, with the fourth packet (No. 236) selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section shows a GET request for /favicon.ico with a User-Agent string that includes 'GoogleToolbar 6.4.1321.1732; Windows XP 5.1; MSIE 6.0.2900.2180'.

Filter: http contains favicon

No.	Time	Source	Destination	Protocol	Info
184	2010-06-19 23:01:47.135391	72.14.213.138	10.200.1.6	HTTP/XML	HTTP/1.1 200 OK
215	2010-06-19 23:01:49.154271	10.200.1.6	173.14.243.228	HTTP	GET /favicon.ico HTTP/1.1
228	2010-06-19 23:01:49.300198	10.200.1.6	67.195.145.137	HTTP	GET /favicon.ico HTTP/1.1
236	2010-06-19 23:01:49.380124	10.200.1.6	66.11.115.139	HTTP	GET /favicon.ico HTTP/1.1

Frame 236 (239 bytes on wire, 239 bytes captured)

- Ethernet II, Src: RealtekU_00:ee:92 (52:54:00:00:ee:92), Dst: 0a:d9:9a:b5:ff:61 (0a:d9:9a:b5:ff:61)
- Internet Protocol, Src: 10.200.1.6 (10.200.1.6), Dst: 66.11.115.139 (66.11.115.139)
- Transmission Control Protocol, Src Port: mil-2045-47001 (1581), Dst Port: http (80), Seq: 1, Ack: 1, Len: 185
- Hypertext Transfer Protocol
 - GET /favicon.ico HTTP/1.1\r\n
 - User-Agent: Mozilla/4.0 (compatible; GoogleToolbar 6.4.1321.1732; Windows XP 5.1; MSIE 6.0.2900.2180)\r\n
 - Host: www.freakymidgets.com\r\n
 - Connection: Keep-Alive\r\n
 - \r\n

Profiling/Dating? (aka stalking)

IP/Bookmark tag cloud from coffee shop wifi?

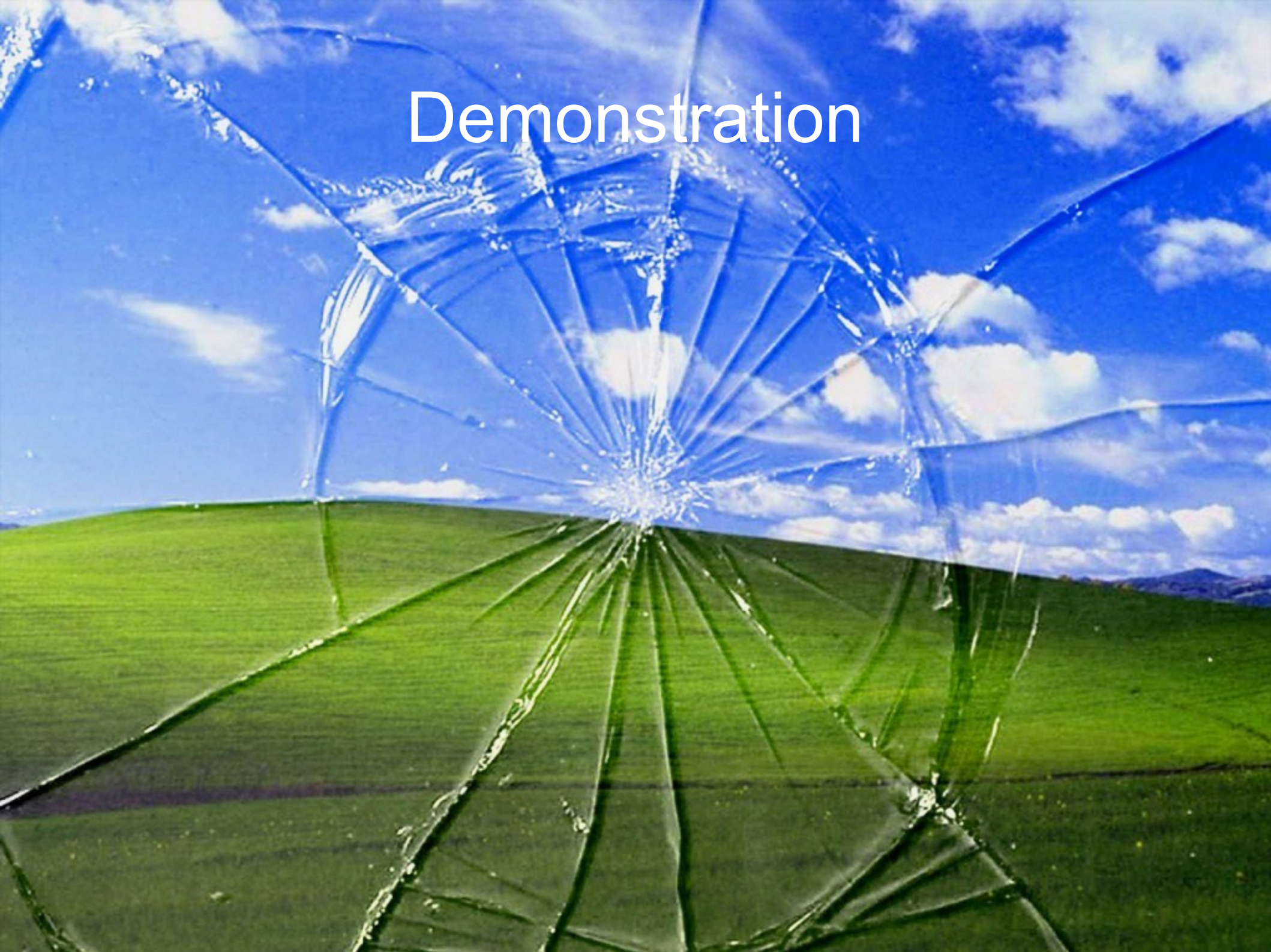
<http://tagcrowd.com/>

<http://www.wordle.net/create>

Python/regex= new tool gtoolbarsnoop.py?

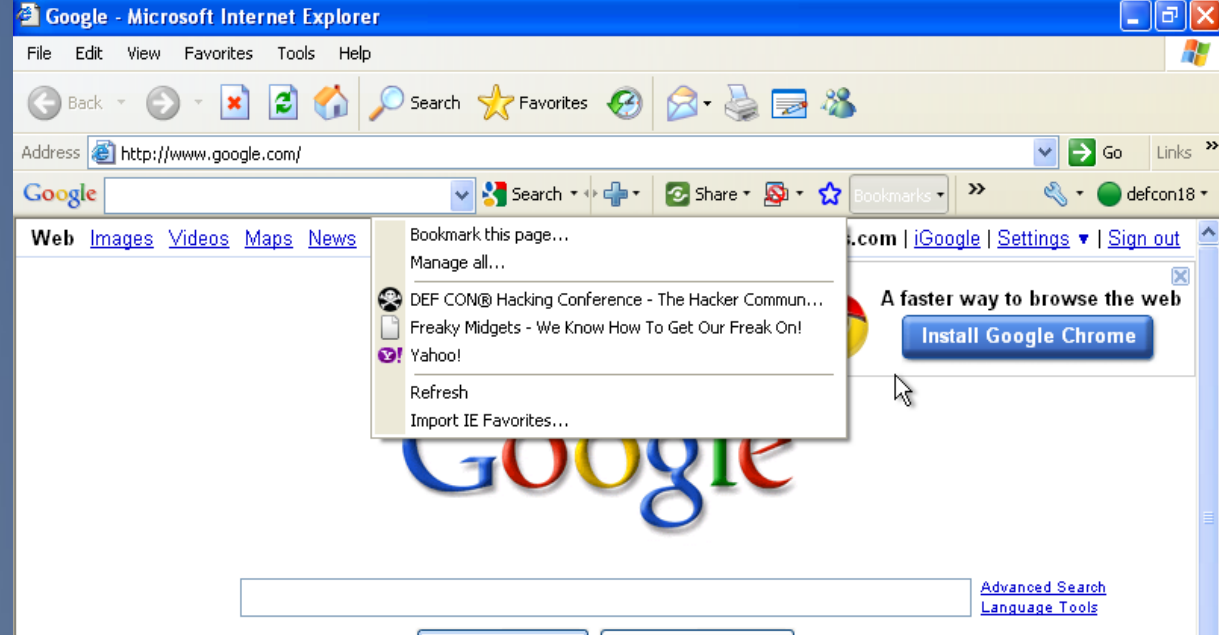
```
tcpdump -i eth0 -s0 -w - port 80 | ./gtoolbarsnoop.py --icons --titles -f -
```

Demonstration



What else?

Deleted Bookmarks?!



```
root@g2:/home/jab/documents/defcon18
Eterm Font Background Terminal
Cookie: PREF=ID=e803865fce68b192;TM=1277612210;LM=1277612210;S=5BNdweKgtwmyfNSg; NID=36=R-zoyxjFY0
BHiIzNSRvrgm05kz55GtYxZg_IdIqeZpGnSonQ0vYQV6e0G; SID=DQAAAHwAAABBDwYRd-DLLpAFJFJxJic2Xs9e21Zi0C1Mk
P-kPBzJE-Vz3To-Dktcnb0q2AWonw6GE2RYILXpRvTp1FqMy053Yre_a0h_aH7YZPEUg; HSID=AnHW1W_d3Jdzg8cQJ

gtoolbarsnoop: found bookmarks
Conversation: (('192.168.1.11', 2561), ('74.125.127.102', 80))
clientIP: 192.168.1.11
HTTP/1.1 200 OK
Pragma: no-cache
Cache-Control: private, no-cache, no-cache="Set-Cookie", proxy-revalidate
Expires: Fri, 04 Aug 1978 12:00:00 GMT
Content-Type: text/xml; charset=UTF-8
Set-Cookie: PREF=ID=e803865fce68b192;U=e26ddc48b8626389;TM=1277612210;LM=1277612225;DV=8Z2250Ah6zch
omain=.google.com
X-Content-Type-Options: nosniff
Date: Sun, 27 Jun 2010 04:17:05 GMT
Server: Search-History HTTP Server
X-XSS-Protection: 1; mode=block
Transfer-Encoding: chunked

d44
<?xml version="1.0"?><xml_api_reply version="1"><bookmarks><bookmark><title>DEF CON@ Hacking Conf
<timestamp>1277012341026006</timestamp><id>450503270071876824</id><attributes><attribute><name>fav
bute</attributes></bookmark><bookmark><title>Yahoo!</title><url>http://www.yahoo.com/?r0=12770108
2</id><attributes><attribute><name>favicon_url</name><value>http://www.yahoo.com/favicon.ico</value
- We Know How To Get Our Freak On!</title><url>http://www.freakymidgets.com/tour.html?h?tsid=43382
d>5156140249493760326</id><attributes><attribute><name>favicon_url</name><value>http://www.freakymi
kmark<title>The Church of Jesus Christ of Latter-day Saints</title><url>http://www.lds.org/ldsorg
timestamp>1277010823575646</timestamp><id>12064102051571604541</id><labels><label>^k</label></label
s.org/favicon.ico</value></attribute><attribute><name>favicon_timestamp</name><value></value></attr
twitter</title><url>https://twitter.com/_defcon_</url><timestamp>1277010823575646</timestamp><id>292
ttribute<name>favicon_url</name><value>http://twitter.com/favicon.ico</value></attribute><attribu
es></bookmark><bookmark><title>Yahoo!</title><url>http://www.yahoo.com/</url><timestamp>12770108235
el</label>^k</label></labels><attributes><attribute><name>favicon_url</name><value>http://www.yaho
><title>MSN.com</title><url>http://www.msn.com/</url><timestamp>1277010823575646</timestamp><id>13
attribute<name>favicon_url</name><value>http://col.stc.s-msn.com/br/sc/i/DF/854F4951FCBF6C45089203
ame><value></value></attribute></attributes></bookmark><bookmark><title>BP Global | BP</title><url
55</url><timestamp>1277010823575646</timestamp><id>17521067242763822402</id><labels><label>^k</labe
lue></attribute><attribute><name>favicon_timestamp</name><value>1277006535</value></attribute></att
</title><url>http://www.xxxmidgetporn.com/</url><timestamp>1277010799508737</timestamp><id>10504804
<attributes><attribute><name>favicon_url</name><value></value></attribute><attribute><name>favicon
ookmark</bookmark></bookmarks></xml_api_reply>
```


Bookmark forensics

Allocated bookmark:

```
<bookmark>
```

```
  <title>Yahoo!</title>
```

```
  <url>http://www.yahoo.com/?r0=1277010878</url>
```

```
  <timestamp>1277012340477390</timestamp>
```

```
  <id>17266698985382022972</id>
```

```
  <attributes>
```

```
    <attribute>
```

```
      <name>favicon_url</name>
```

```
      <value>http://www.yahoo.com/favicon.ico</value>
```

```
    </attribute>
```

```
  </attributes>
```

```
</bookmark>
```

Bookmark forensics

Deleted bookmark:

```
<bookmark>
  <title>BP Global | BP</title>
  <url>http://www.bp.com/bodycopyarticle.do?
categoryId=1&contentId=7052055</url>
  <timestamp>1277010823575646</timestamp>
  <id>17521067242763822402</id>
  <labels>
    <label>^k</label>
  </labels>
  <attributes>
    <attribute>
      <name>favicon_url</name>
      <value/>
    </attribute>
    <attribute>
      <name>favicon_timestamp</name>
      <value>1277006535</value>
    </attribute>
  </attributes>
</bookmark>
```

Shocking



Sad



What to do?



Questions?

