

# Google Hacking for Penetration Testers

Using Google as a Security Testing Tool

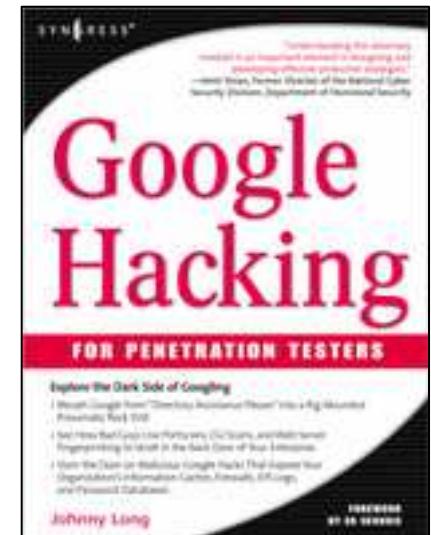
Johnny Long

[johnny@ihackstuff.com](mailto:johnny@ihackstuff.com)

---

## What we're doing

- I hate pimpin', but we're covering many techniques covered in the "Google Hacking" book.
- For much more detail, I encourage you to check out "Google Hacking for Penetration Testers" by Syngress Publishing.



# Advanced Operators

Before we can walk, we must run. In Google's terms this means understanding advanced operators.

---

## **Advanced Operators**

- Google advanced operators help refine searches.
- They are included as part of a standard Google query.
- Advanced operators use a syntax such as the following:

**operator:search\_term**

- There's no space between the operator, the colon, and the search term!

# Advanced Operators at a Glance

Advanced operators can be combined in some cases.

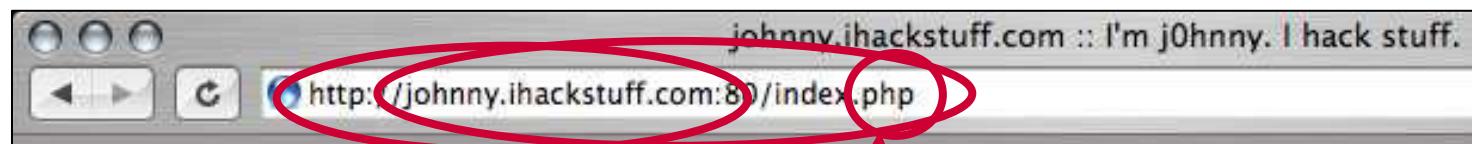
In other cases, mixing should be avoided.

Operator	Purpose	Mixes with other operators?	Can be used alone?	Does search work in			
				Web	Images	Groups	News
intitle	Search page title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	Search specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

Some operators can only be used to search specific areas of Google, as these columns show.

## Crash course in advanced operators

Some operators search overlapping areas. Consider site, inurl and filetype.



SITE:

INURL:

FILETYPE:

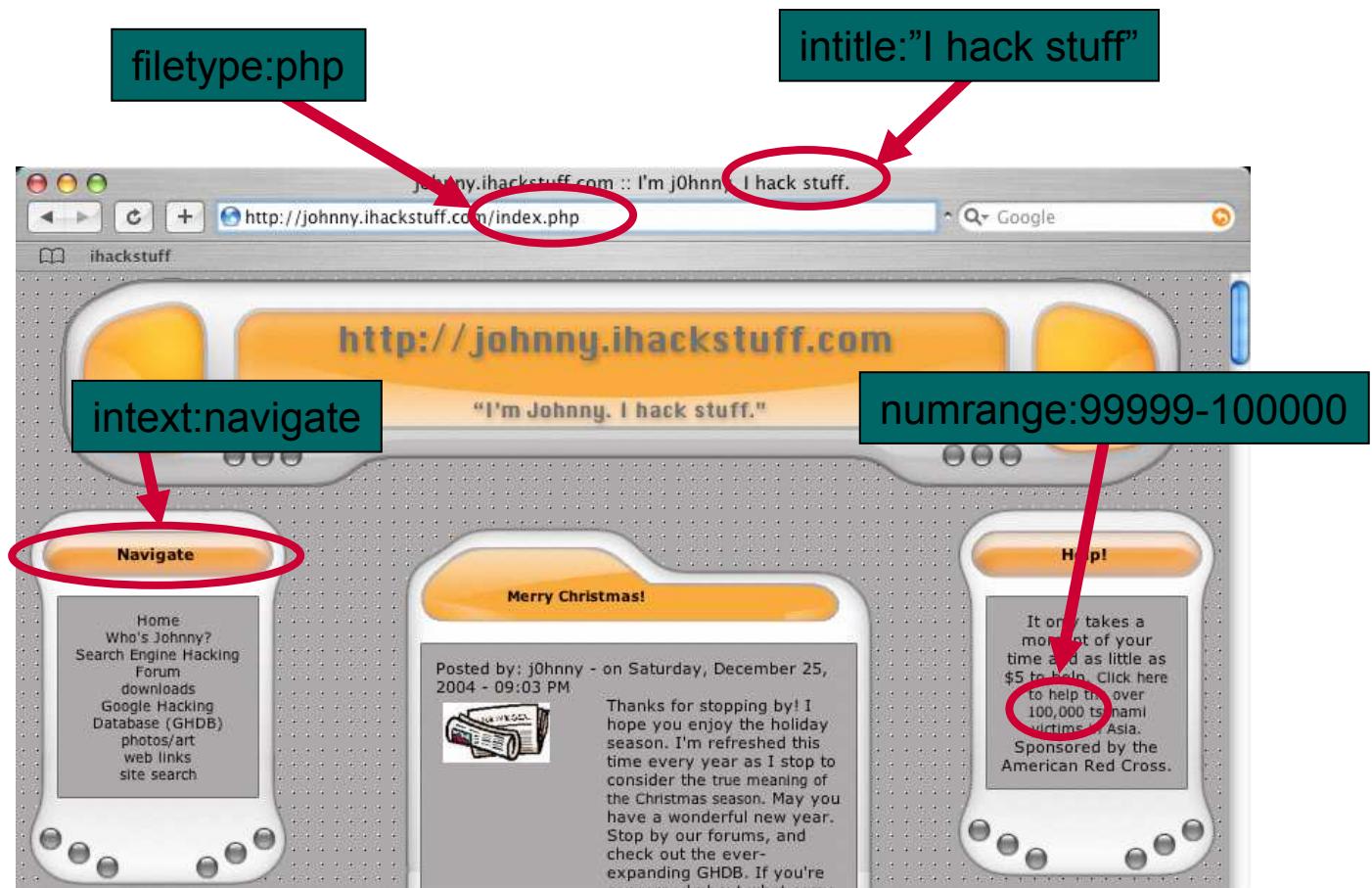
Site can not search port.

Inurl can search the whole URL, including port and filetype.

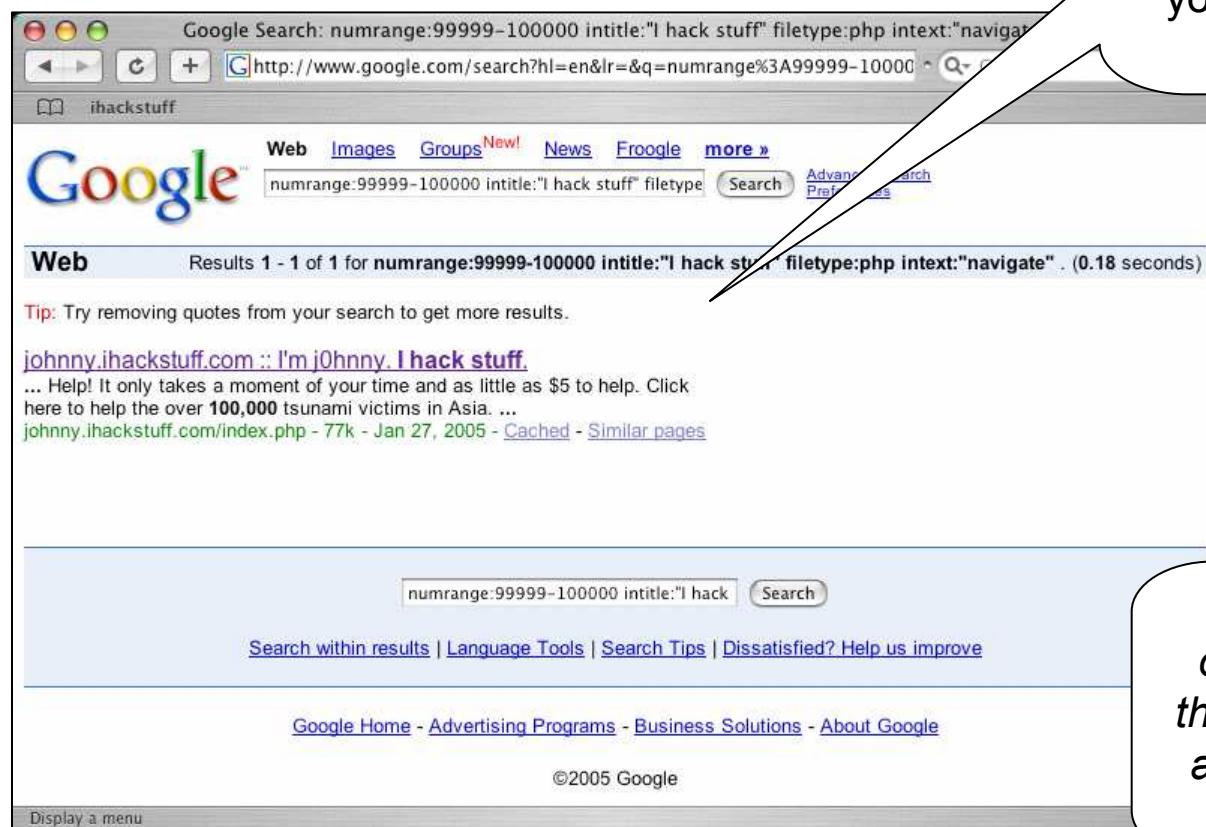
Filetype can only search file extension, which may be hard to distinguish in long URLs.

# Advanced Google Searching

There are many ways to find the same page. These individual queries could all help find the same page.



# Advanced Google Searching



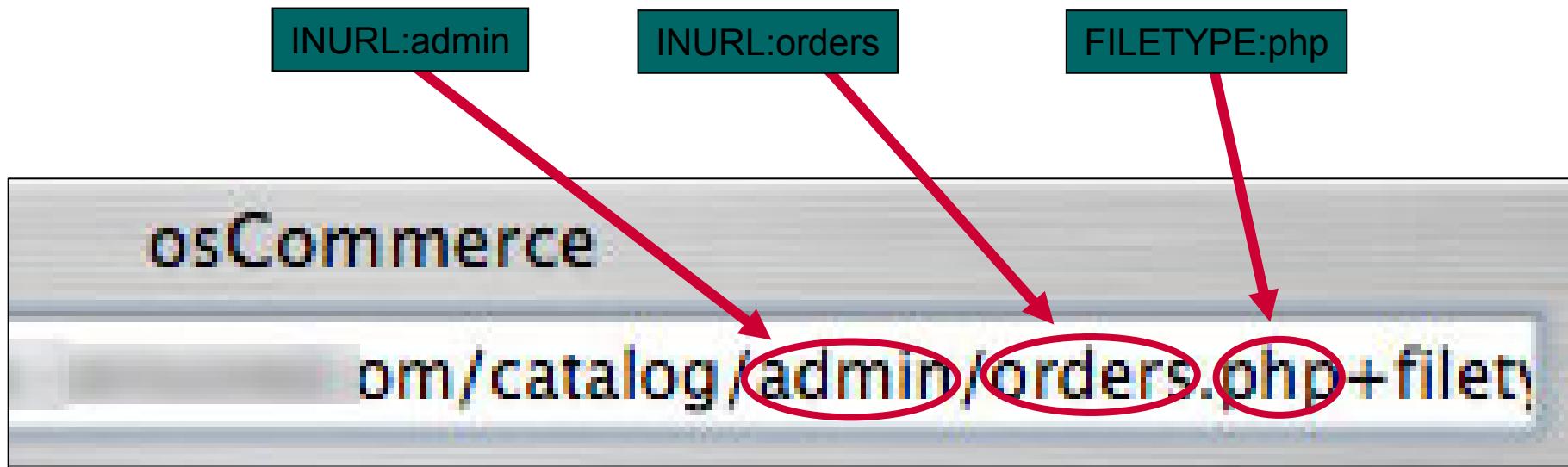
Put those individual queries together into one monster query and you only get that one specific result.

***Adding advanced operators reduces the number of results adding focus to the search.***

---

## Google Hacking Basics

Putting operators together in intelligent ways can cause a seemingly innocuous query...



# Google Hacking Basics

...can return  
devastating results!

The screenshot shows a Google search result for the query "filetype:php inurl:admin inurl:orders". The result is a cached page from an osCommerce website. The page title is "osCommerce". The main content of the cache is a snippet from the osCommerce admin panel showing a list of orders. A speech bubble labeled "Customer names" points to the list of customer names in the cache. Another speech bubble labeled "Order Amounts" points to the list of order totals. A third speech bubble labeled "Payment details!" points to the payment method information at the bottom of the order list.

This is Google's cache of <http://www.7oI19sFkJ:www.com/catalog/admin/orders.php>.  
Google's cache is the snapshot that we took of the page as we crawled the web.  
The page may have changed since that time. Click here for the [current page](#) without highlighting.  
This cached page may reference images which are no longer available. Click here for the [cached text](#) only.  
To link to or bookmark this page, use the following url: <http://www.google.com/search?q=cache:Vc-7oI19sFkJ:www.com/catalog/admin/orders.php+filetype:php+inurl:admin+inurl:orders&hl=en>

Google is not affiliated with the authors of this page nor responsible for its content.

These search terms have been highlighted: **orders**  
These terms only appear in links pointing to this page: **admin**

Administration Configuration My Store Minimum Values Maximum Values Images Customer Details Shipping/Packaging Product Listing Stock Logging Cache E-Mail Options Download Display a menu

Support Site | Online Catalog | Administration

Order ID:   
Status: AllOrders

Customers	Order Total	Date Purchased	Status	Action
Peter Matts	\$56.30	07/01/2004 20:19:33	Delivered	[Edit] [Delete] [Details]
John Evans	\$81.90	06/17/2004 11:22:22	Delivered	[Edit] [Delete] [Details]
Andrew Hewitt	\$69.50	06/16/2004 22:38:20	Pending	[Edit] [Delete] [Details]
Elan Kelson	\$45.25	04/23/2004 02:08:24	Delivered	[Edit] [Delete] [Details]
Igor Vega	\$159.15	04/16/2004 22:37:00	Delivered	[Edit] [Delete] [Details]

Date Created: 07/01/2004  
Last Modified: 07/06/2004  
Payment Method: Bank

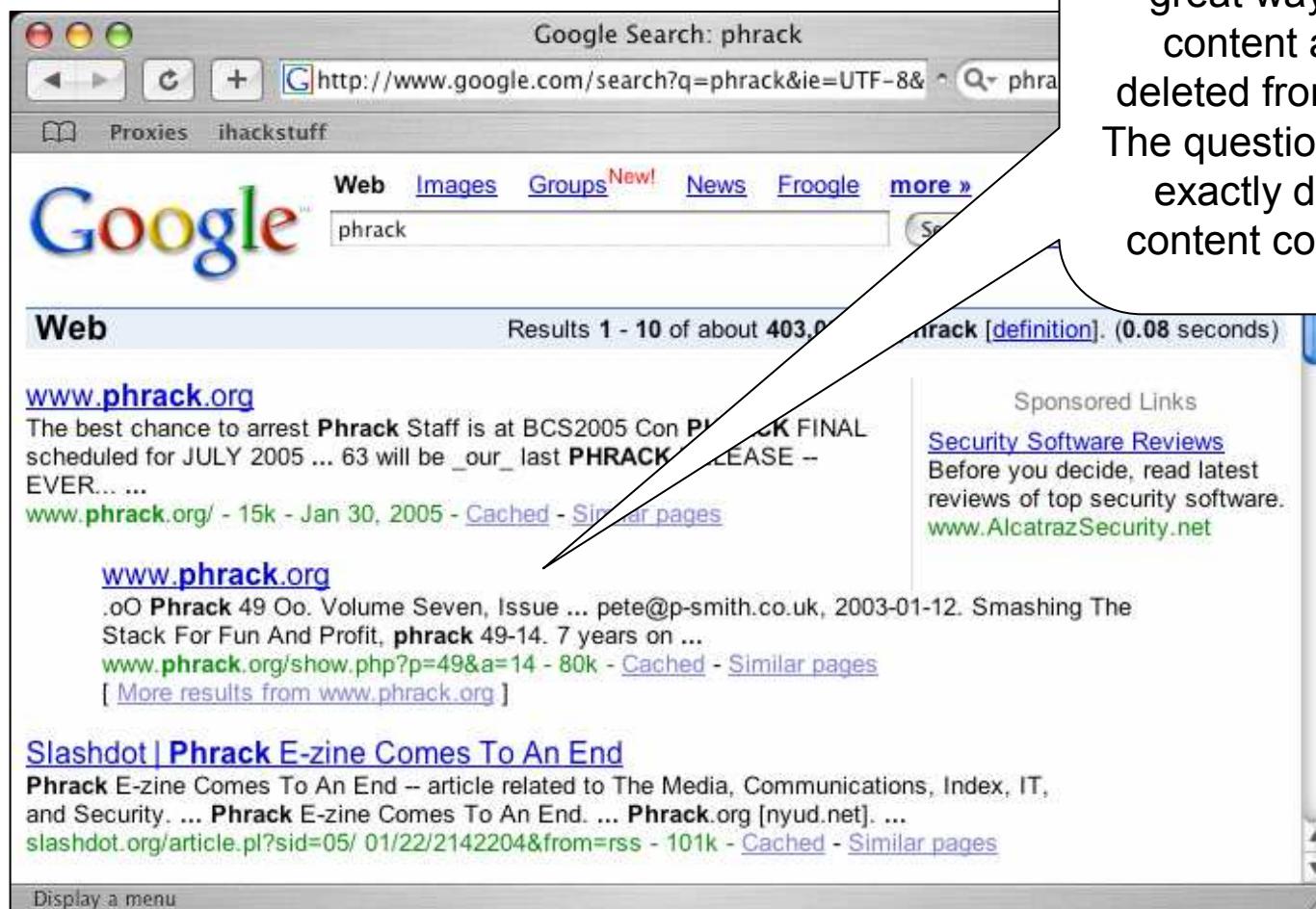
# Google Hacking Basics

Let's take a look at some basic techniques:

Anonymous Googling

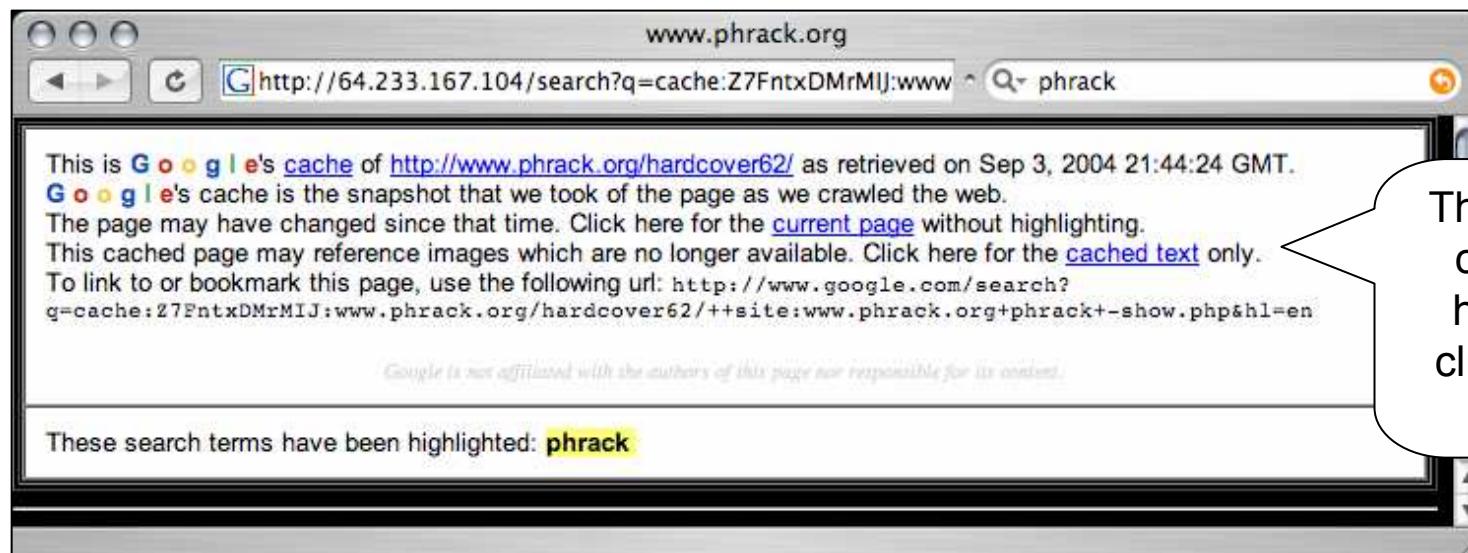
Special Characters

# Anonymous Googling



## Anonymous Googling

- Some folks use the cache link as an anonymizer, thinking the content comes from Google. Let's take a closer look.



---

## Anonymous Googling

This tcpdump output shows our network traffic while loading that *cached* page.

```
21:39:24.648422 IP 192.168.2.32.51670 > 64.233.167.104.80
21:39:24.719067 IP 64.233.167.104.80 > 192.168.2.32.51670
21:39:24.720351 IP 64.233.167.104.80 > 192.168.2.32.51670
21:39:24.731503 IP 192.168.2.32.51670 > 64.233.167.104.80
21:39:24.897987 IP 192.168.2.32.51672 > 82.165.25.125.80
21:39:24.902401 IP 192.168.2.32.51671 > 82.165.25.125.80
21:39:24.922716 IP 192.168.2.32.51673 > 82.165.25.125.80
21:39:24.927402 IP 192.168.2.32.51674 > 82.165.25.125.80
21:39:25.017288 IP 82.165.25.125.80 > 192.168.2.32.51672
21:39:25.019111 IP 82.165.25.125.80 > 192.168.2.32.51672
21:39:25.019228 IP 192.168.2.32.51672 > 82.165.25.125.80
21:39:25.023371 IP 82.165.25.125.80 > 192.168.2.32.51671
21:39:25.025388 IP 82.165.25.125.80 > 192.168.2.32.51671
21:39:25.025736 IP 192.168.2.32.51671 > 82.165.25.125.80
21:39:25.043418 IP 82.165.25.125.80 > 192.168.2.32.51673
21:39:25.045573 IP 82.165.25.125.80 > 192.168.2.32.51673
21:39:25.045707 IP 192.168.2.32.51673 > 82.165.25.125.80
21:39:25.052853 IP 82.165.25.125.80 > 192.168.2.32.51674
```

This is Google.

This is Phrack.

We touched Phrack's web server. We're not anonymous.

---

## Anonymous Googling

- Obviously we touched the site, but why?
- Here's more detailed tcpdump output:

0x0040 0d6c 4745 5420 2f67 7266 782f 3831 736d	An image loaded!
0x0050 626c 7565 2e6a 7067 2048 5454 502f 312e	
0x0060 310d 0a48 6f73 743a 2077 7777 2e70 6872	
0x0070 6163 6b2e 6f72 670d 0a43 6f6e 6e65 6374	ack.org..Connect
0x0080 696f 6e3a 206b 6565 702d 616c 6976 650d	ion:.keep-alive.
0x0090 0a52 6566 6572 6572 3a20 6874 7470 3a2f	.Referer:.http:/
0x00a0 2f36 342e 3233 332e 3136 312e 3130 342f	/64.233.161.104/
0x00b0 7365 6172 6368 3f71 3d63 6163 6865 3a4c	search?q=cache:L
0x00c0 4251 5a49 7253 6b4d 6755 4a3a 7777 772e	BQZIrSkMgUJ:www.
0x00d0 7068 7261 636b 2e6f 7267 2f2b 2b73 6974	phrack.org/++sit
0x00e0 653a 7777 772e 7068 7261 636b 2e6f 7267	e:www.phrack.org
0x00f0 2b70 6872 6163 6b26 686c 3d65 6e0d 0a55	+phrack&hl=en..U

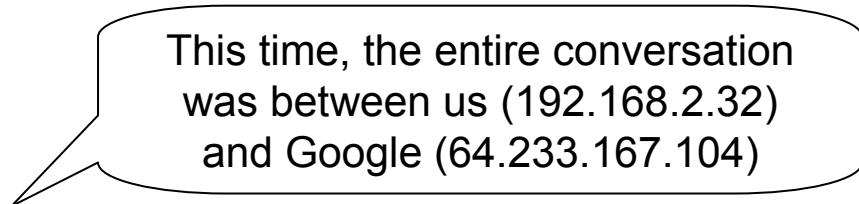
---

## Anonymous Googling



---

## Anonymous Googling



This time, the entire conversation  
was between us (192.168.2.32)  
and Google (64.233.167.104)

```
23:46:53.996067 IP 192.168.2.32.52912 > 64.233.167.104.80
23:46:54.025277 IP 64.233.167.104.80 > 192.168.2.32.52912
23:46:54.025345 IP 192.168.2.32.52912 > 64.233.167.104.80
23:46:54.025465 IP 192.168.2.32.52912 > 64.233.167.104.80
23:46:54.094007 IP 64.233.167.104.80 > 192.168.2.32.52912
23:46:54.124930 IP 64.233.167.104.80 > 192.168.2.32.52912
23:46:54.127202 IP 64.233.167.104.80 > 192.168.2.32.52912
23:46:54.128762 IP 64.233.167.104.80 > 192.168.2.32.52912
23:46:54.128836 IP 192.168.2.32.52912 > 64.233.167.104.80
23:47:54.130200 IP 192.168.2.32.52912 > 64.233.167.104.80
23:47:54.154500 IP 64.233.167.104.80 > 192.168.2.32.52912
23:47:54.154596 IP 192.168.2.32.52912 > 64.233.167.104.80
```

---

## Anonymous Googling

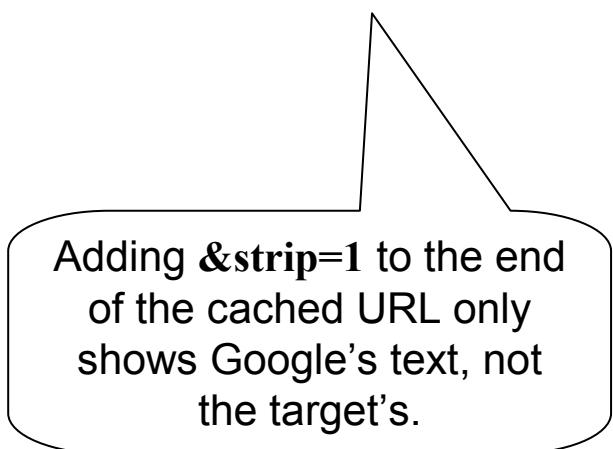
- What made the difference? Let's compare the two URLs:

- Original:

<http://64.233.187.104/search?q=cache:Z7FntxDMrMIJ:www.phrack.org/hardcover62/+phrack+hardcover62&hl=en>

- Cached Text Only:

<http://64.233.187.104/search?q=cache:Z7FntxDMrMIJ:www.phrack.org/hardcover62/+phrack+hardcover62&hl=en&lr=&strip=1>



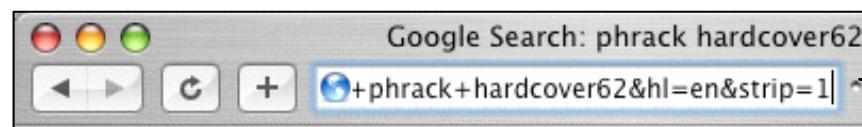
Adding **&strip=1** to the end of the cached URL only shows Google's text, not the target's.

## Anonymous Googling

- Anonymous Googling can be helpful, especially if combined with a proxy. Here's a summary.



Perform a Google search.



Right-click the cached link and copy the link to the clipboard.

Paste the URL to the address bar, add &strip=1, hit return. You're only touching Google now...

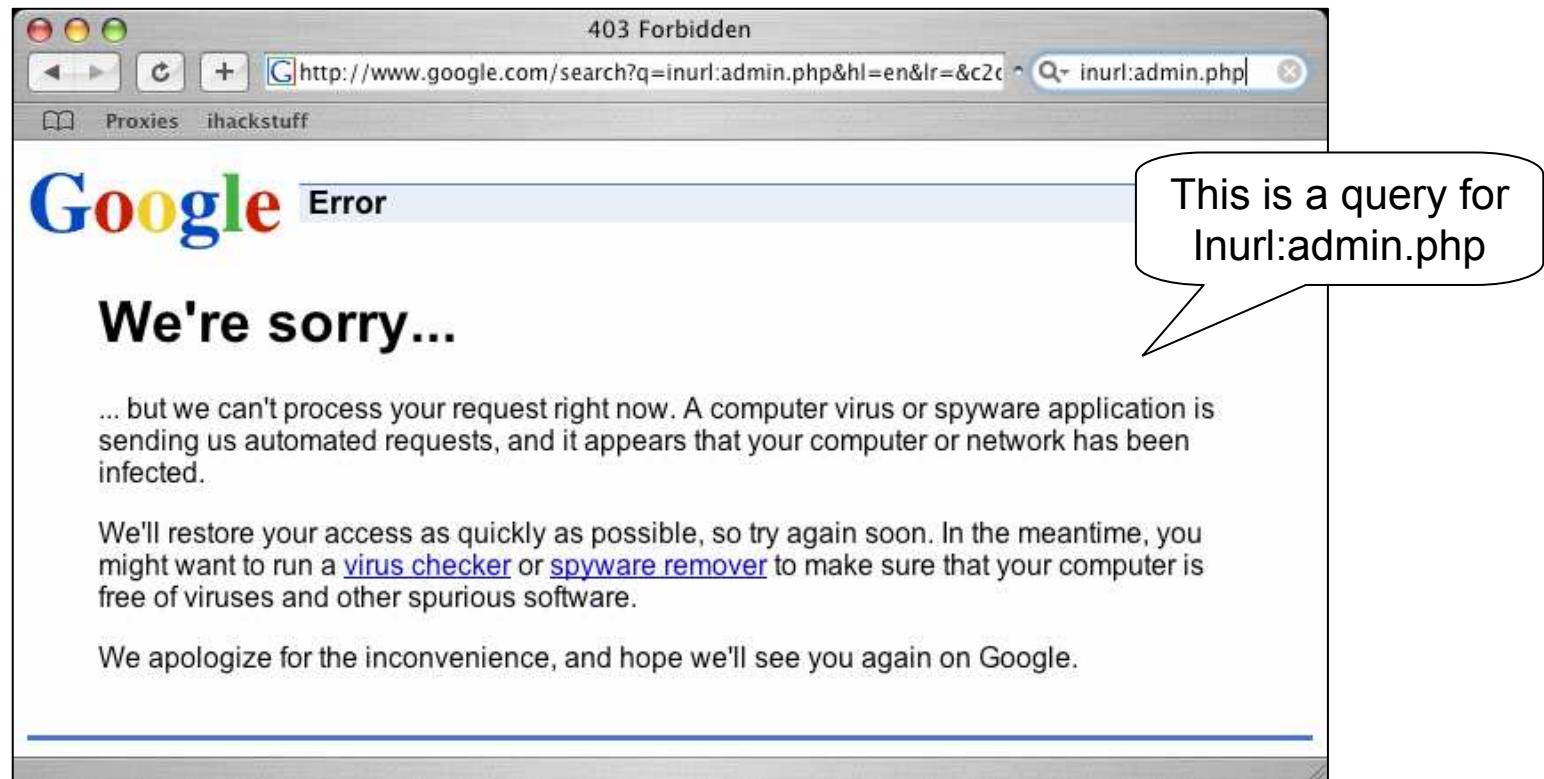
---

## Special Search Characters

- We'll use some special characters in our examples. These characters have special meaning to Google.
- Always use these characters without surrounding spaces!
  - ( + ) force inclusion of something common
  - ( - ) exclude a search term
  - ( " ) use quotes around search phrases
  - ( . ) a single-character wildcard
  - ( \* ) any word
  - ( | ) boolean 'OR'
  - Parenthesis group queries ("master card" | mastercard)

## Google's PHP Blocker: "We're Sorry..."

- Google has started blocking queries, most likely as a result of worms that slam Google with 'evil queries.'



---

## Google Hacker's workaround

- Our original query looks like this:

`http://www.google.com/search?q=inurl:admin.php&hl=en&lr=&c2coff=1&start=10&sa=N`

- Stripped down, the query looks like this:

`http://www.google.com/search?q=inurl:admin.php&start=10`

- We can modify our query (`inurl:something.php` is bad) by changing the case of the file extension, like so:

`http://www.google.com/search?q=inurl:admin.PHP&start=10`

`http://www.google.com/search?q=inurl:admin.pHp&start=10`

`http://www.google.com/search?q=inurl:admin.PhP&start=10`

This works in the web interface as well.

# Pre-Assessment

There are many things to consider before testing a target, many of which Google can help with. One shining example is the collection of email addresses and usernames.

## Trolling for Email Addresses

- A seemingly simple search uses the @ sign followed by the primary domain name.

The screenshot shows a Mac OS X desktop with a Google search results page. The search bar at the top contains "Google Search: '@gmail.com'" and the URL "http://www.google.com/search?hl=en&lr=&c2co=&q=%40gmail.com". Below the search bar, the Google logo is visible, along with navigation links for Web, Images, Groups, News, Froogle, and more. The search query "@gmail.com" is entered in the search field, and the "Search" button is highlighted. The results section shows "Web Results 1 - 100 of about 2,900,000 for '@gmail.com'. (0.20 seconds)". The first result is a link to "Welcome to Gmail" with the description: "Welcome to Gmail, A Google approach to email. Gmail is an experiment in a new kind of webmail, built on the idea that you should ...". Below this is a link to "gmail.google.com/ - 12k - Jan 30, 2005 - Cached - Similar pages". Another result is "gmail swap" with the description: "... the gates. Why settle for g\_r\_a\_m\_o\_p\_43fp@gmail.com when you could sneak in early and nab gramophone@gmail.com? Everyone's talking ..." and a link to "www.gmailswap.com/ - 10k - Cached - Similar pages". To the right of the search results, there is a "Sponsored Links" section with a link to "Gmail - New From Google" which reads: "Introducing a Free Webmail Service: 1000 MB of Storage & Google Search" and a link to "gmail.google.com". A speech bubble points from the search bar to the sponsored link, containing the text "The ‘@’ sign doesn’t translate well...". Another speech bubble points from the bottom right of the search results area to the bottom right of the slide, containing the text "But we can still use the results...".

---

## Automated Trolling for Email Addresses

- We could use a lynx to automate the download of the search results:

```
lynx -dump http://www.google.com/search?q=@gmail.com > test.html
```

- We could then use regular expressions (like this puppy by Don Ranta) to troll through the results:

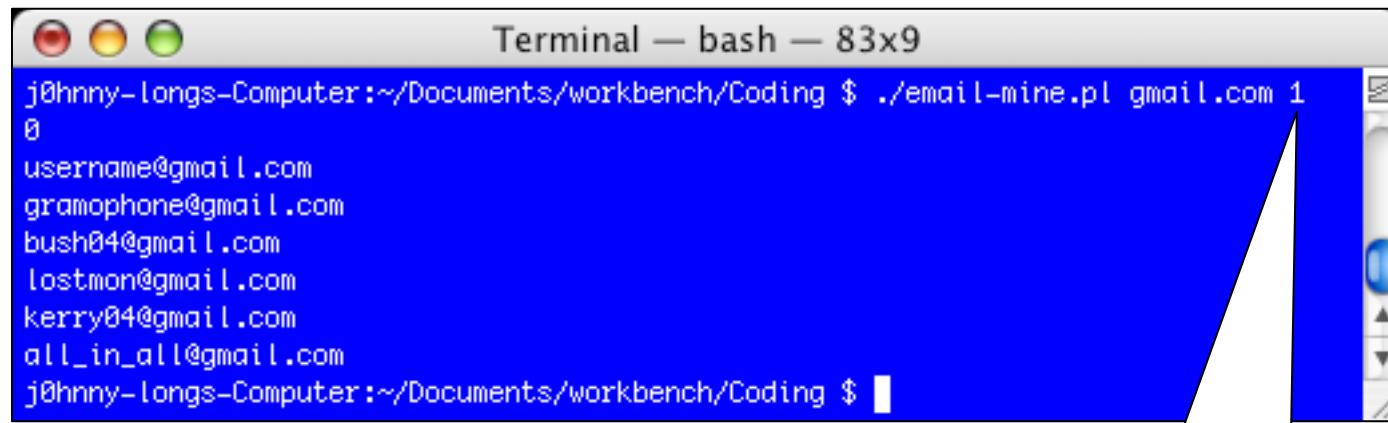
```
[a-zA-Z0-9._-]+@[([a-zA-Z0-9_-]{2,99}\.)([a-zA-Z]{2,4})|(([25][0-5]|2[0-4])[0-9]1[0-9][0-9]|([1-9][0-9])[1-9])|(([25][0-5]|2[0-4])[0-9]1[0-9][0-9][1-9]|([25][0-5]|2[0-4])[0-9]1[0-9][0-9][1-9])|(([25][0-5]|2[0-4])[0-9]1[0-9][0-9][1-9][0-9])|(([25][0-5]|2[0-4])[0-9]1[0-9][0-9][1-9][0-9]))
```

- Run through grep, this regexp would effectively find email addresses (including addresses containing IP numbers)

---

## More Email Automation

- The ‘email miner’ PERL script by Roelof Temmingh at sensepost will effectively do the same thing, but via the Google API:



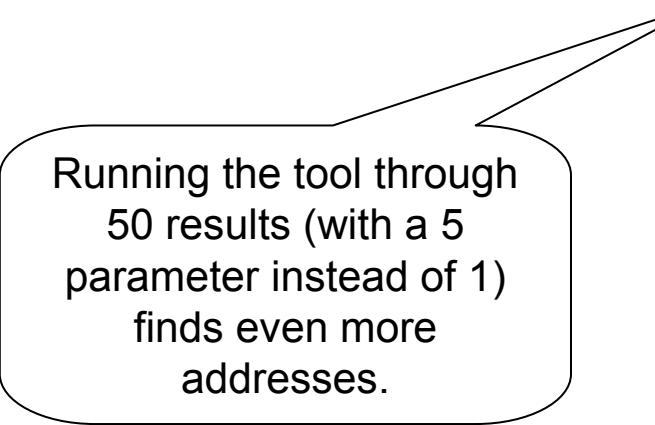
The screenshot shows a Mac OS X terminal window titled "Terminal — bash — 83x9". The window has three colored window control buttons (red, yellow, green) at the top left. The terminal area displays the following command and its output:

```
j0hnny-longs-Computer:~/Documents/workbench/Coding $ ./email-mine.pl gmail.com 1
0
username@gmail.com
gramophone@gmail.com
bush04@gmail.com
lostmon@gmail.com
kerry04@gmail.com
all_in_all@gmail.com
j0hnny-longs-Computer:~/Documents/workbench/Coding $
```

This searches the first ten Google results... with only one hit against your API key.

---

## More Email Automation



Running the tool through  
50 results (with a 5  
parameter instead of 1)  
finds even more  
addresses.

movabletype@gmail.com  
fakubabe@gmail.com  
lostmon@gmail.com  
label@gmail.com  
charlescapps@gmail.com  
billgates@gmail.com  
ymtang@gmail.com  
tonyedgecombe@gmail.com  
ryawillifor@gmail.com  
jruderman@gmail.com  
itchy@gmail.com  
gramophone@gmail.com  
poojara@gmail.com  
london2012@gmail.com  
bush04@gmail.com  
fengfs@gmail.com  
username@gmail.com  
madrid2012@gmail.com  
somelabel@gmail.com  
bartjcannon@gmail.com  
fillmybox@gmail.com  
silverwolfwsc@gmail.com  
all\_in\_all@gmail.com  
mentzer@gmail.com  
kerry04@gmail.com  
presidentbush@gmail.com  
prabhav78@gmail.com

## More email address locations

Query	Description
"Internal Server Error" "server at"	Apache server error could reveal admin e-mail address
intitle:"Execution of this script not permitted"	Cgiwrap script can reveal lots of information, including e-mail addresses and even phone numbers
e-mail address filetype:csv csv	CSV files that could contain e-mail addresses
intitle:index.of dead.letter	dead.letter UNIX file contains the contents of unfinished e-mails that can contain sensitive information
inurl:fcgi-bin/echo	fastcgi echo script can reveal lots of information, including e-mail addresses and server information
filetype:pst pst -from -to -date	Finds Outlook PST files, which can contain e-mails, calendaring, and address information
intitle:index.of inbox	Generic "inbox" search can locate e-mail caches
intitle:"Index Of" -inurl:maillog maillog size	Maillog files can reveal usernames, e-mail addresses, user login/logout times, IP addresses, directories on the server, and more
inurl:email filetype:mdb	Microsoft Access databases that could contain e-mail information
filetype:xls inurl:"email.xls"	Microsoft Excel spreadsheets containing e-mail addresses
filetype:xls username password email	Microsoft Excel spreadsheets containing the words <i>username</i> , <i>password</i> , and <i>email</i>
intitle:index.of inbox dbx	Outlook Express cleanup.log file can contain locations of e-mail information

These queries locate email addresses in more “interesting” locations...

## More email address locations

Query	Description
<code>filetype:eml eml +intext: "Subject" +intext:"From"</code>	Outlook express e-mail files contain e-mails with full headers
<code>intitle:index.of inbox dbx</code>	Outlook Express e-mail folder
<code>filetype:wab wab</code>	Outlook Mail address books contain sensitive e-mail information
<code>filetype:pst inurl:"outlook.pst"</code>	Outlook PST files can contain e-mails, calendaring, and address information
<code>filetype:mbx mbx intext:Subject</code>	Outlook versions 1–4 or Eudora mailbox files contain sensitive e-mail information
<code>inurl:cgi-bin/printenv</code>	Printenv script can reveal lots of information, including e-mail addresses and server information
<code>inurl:forward filetype:forward -cvs</code>	UNIX user e-mail forward files can list e-mail addresses
<code>( filetype:mail   filetype:eml   filetype:mbox   filetype:mbx ) intext:password subject</code>	Various generic e-mail files
<code>"Most Submitted Forms and Scripts" "this section"</code>	WebTrends statistics pages reveal directory information, client access statistics, e-mail addresses, and more
<code>filetype:reg reg +intext: "internet account manager"</code>	Windows registry files can reveal information such as usernames, POP3 passwords, e-mail addresses, and more
<code>"This summary was generated by wwwstat"</code>	Wwwstat statistics information can reveal directory info, client access statistics, e-mail addresses, and more

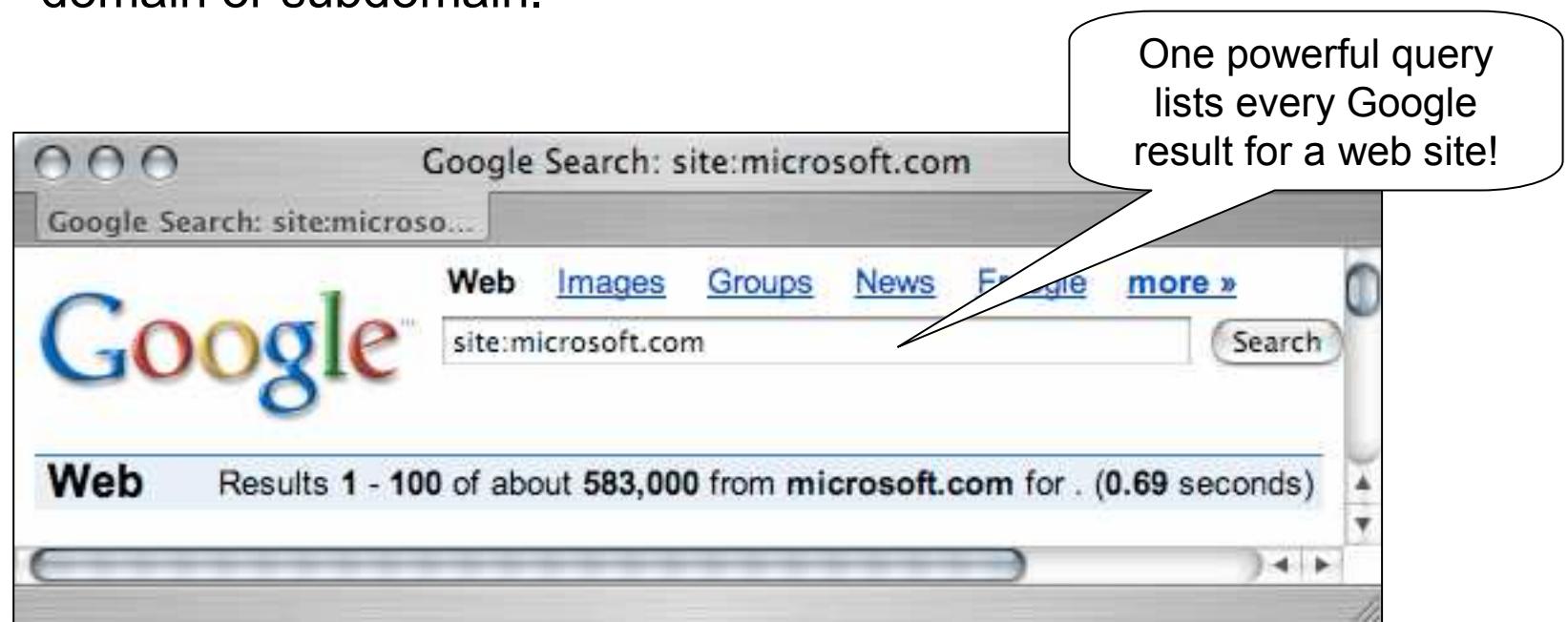
These queries locate email addresses in more “interesting” locations...

# Network Mapping

Google is an indispensable tool for mapping out an Internet-connected network.

## Basic Site Crawling

- the site: operator narrows a search to a particular site, domain or subdomain.



**site: microsoft.com**

# Basic Site Crawling

The screenshot shows a Google search results page for the query "site:microsoft.com". The results are filtered to show only pages from the Microsoft website. The top result is a link to Microsoft's system requirements for Windows Media Player 9 on Mac OS X. Below it is a link to the Microsoft Small Business Support Center. Further down are links to Microsoft Office trademarks, a PasteFace method for PowerPoint, the IRTCPProfile2 interface, a CTimeSpan operator, and MSN Messenger for Mac.

Most often, a site search makes the *obvious* stuff float to the top.

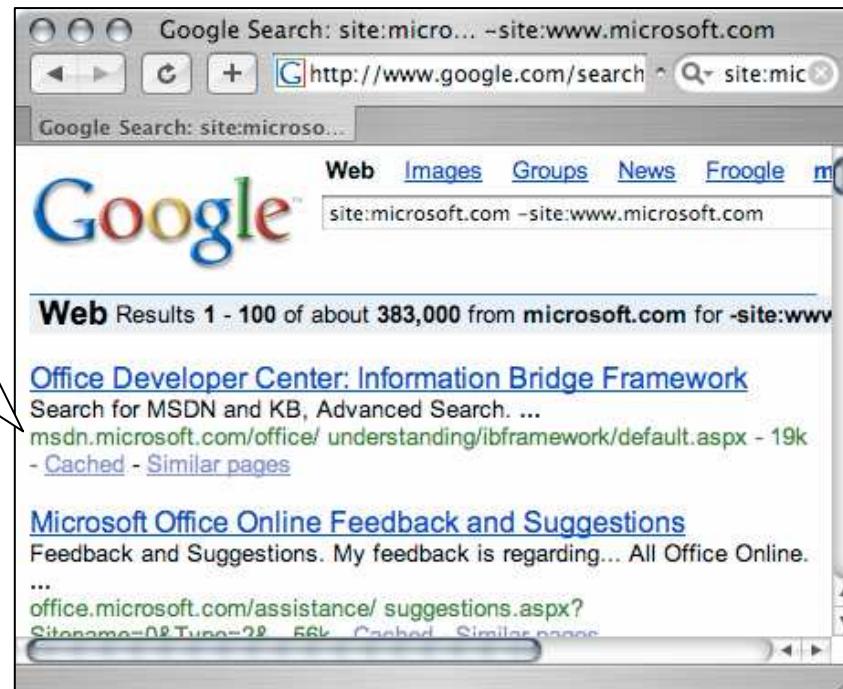
As a security tester, we need to get to the *less obvious* stuff.

[www.microsoft.com](http://www.microsoft.com) is way too obvious...

## Basic Site Crawling

- To get rid of the more obvious crap, do a negative search.

Notice that the  
obvious “www” is  
missing, replaced  
by more interesting  
domains.



**site: microsoft.com  
-site:www.microsoft.com**

---

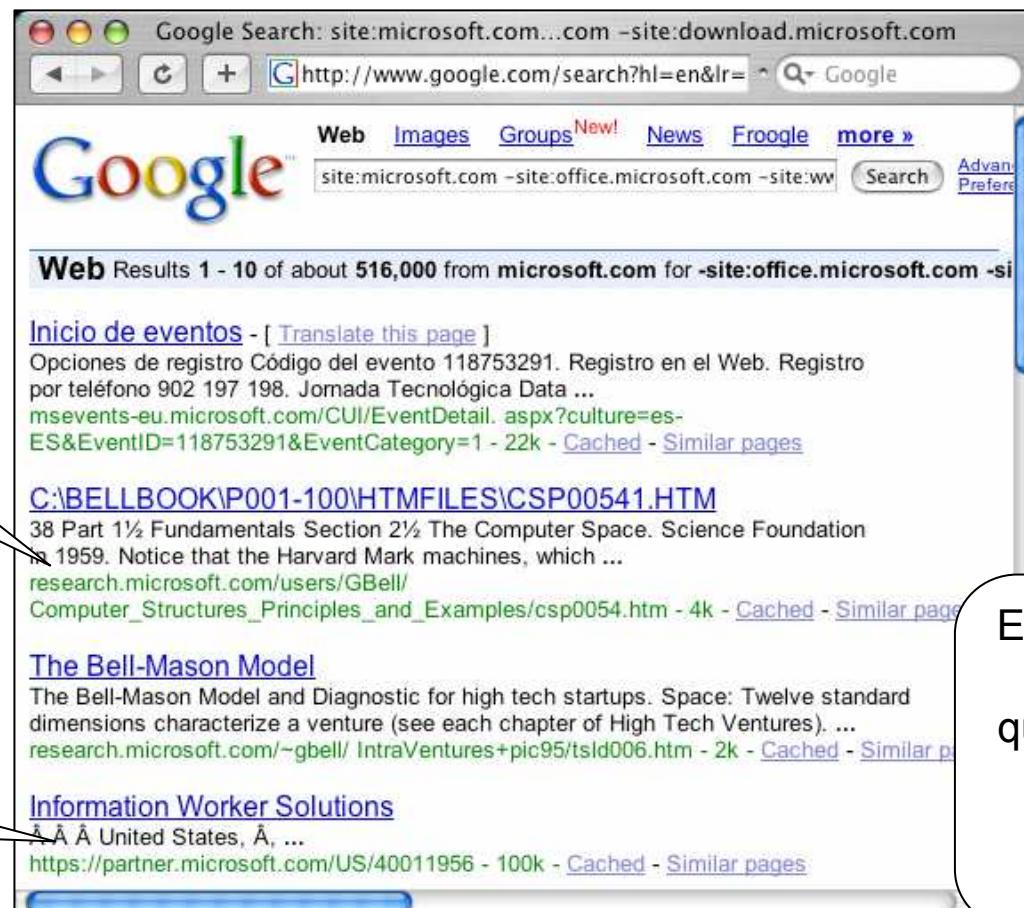
## Basic Site Crawling

- Repeating this process of site reduction, tracking what floats to the top leads to nasty big queries like:

site:microsoft.com  
-site:www.microsoft.com  
-site:msdn.microsoft.com  
-site:support.microsoft.com  
-site:download.microsoft.com  
-site:office.microsoft.com  
  
...

## Basic Site Crawling

- The results of such a big query reveal more interesting results...

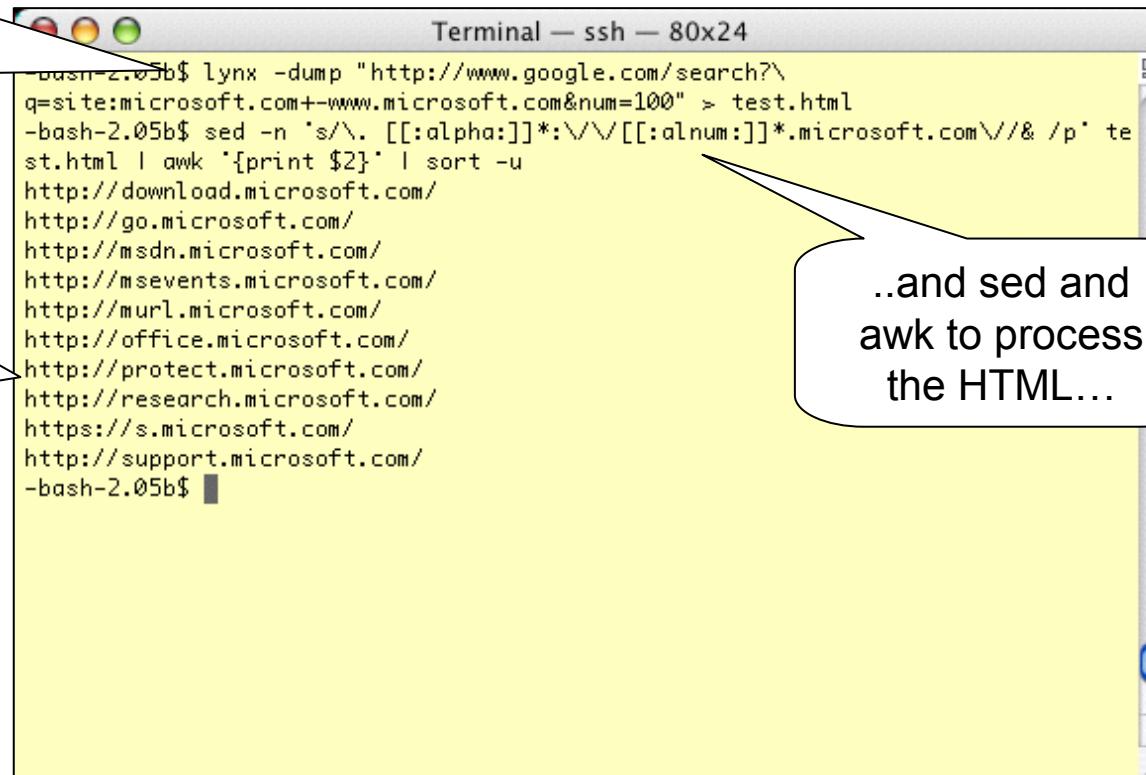


## Intermediate Site Crawling

Using lynx to capture the Google results page...

...returns the same results.

...and sed and awk to process the HTML...



```
Terminal — ssh — 80x24
-bash-2.05b$ lynx -dump "http://www.google.com/search?q=site:microsoft.com+www.microsoft.com&num=100" > test.html
-bash-2.05b$ sed -n 's/\.[[:alpha:]]*:\//\[[[:alnum:]]*\].microsoft.com\//&/p' test.html | awk '{print $2}' | sort -u
http://download.microsoft.com/
http://go.microsoft.com/
http://msdn.microsoft.com/
http://msevents.microsoft.com/
http://murl.microsoft.com/
http://office.microsoft.com/
http://protect.microsoft.com/
http://research.microsoft.com/
https://s.microsoft.com/
http://support.microsoft.com/
-bash-2.05b$
```

---

## So what?

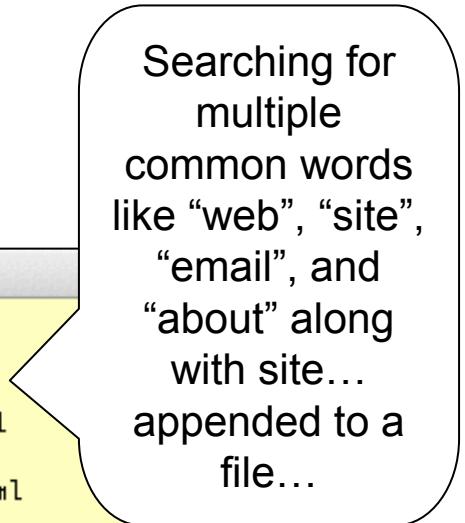
- Well, honestly, host and domain enumeration isn't new, but we're doing this without sending any packets to the target we're analyzing.
- This has several benefits:
  - Low profile. The target can't see your activity.
  - Results are "ranked" by Google. This means that the most public stuff floats to the top. Some more "interesting stuff" tucks near the bottom.
  - "Hints" for follow-up recon. You aren't just getting hosts and domain names, you get application information just by looking at the snippet returned from Google. One results page can be processed for many types of info.. Email addresses, names, etc.. More on this later on...
  - Since we're getting data from several sources, we can focus on non obvious relationships. This is huge!
- Some down sides:
  - In some cases it may be faster and easier as a good guy to use traditional techniques and tools that connect to the target, but remember- the bad guys can still *find and target you via Google!*

---

## **Advanced Site Crawling**

- Google frowns on automation, unless you use tools written with their API. Know what you're running unless you don't care about their terms of service.
- We could easily modify our lynx retrieval command to pull more results, but in many cases, more results won't equal more unique hosts.
- So, we could also use another technique to locate hosts... plain old fashion common word queries.

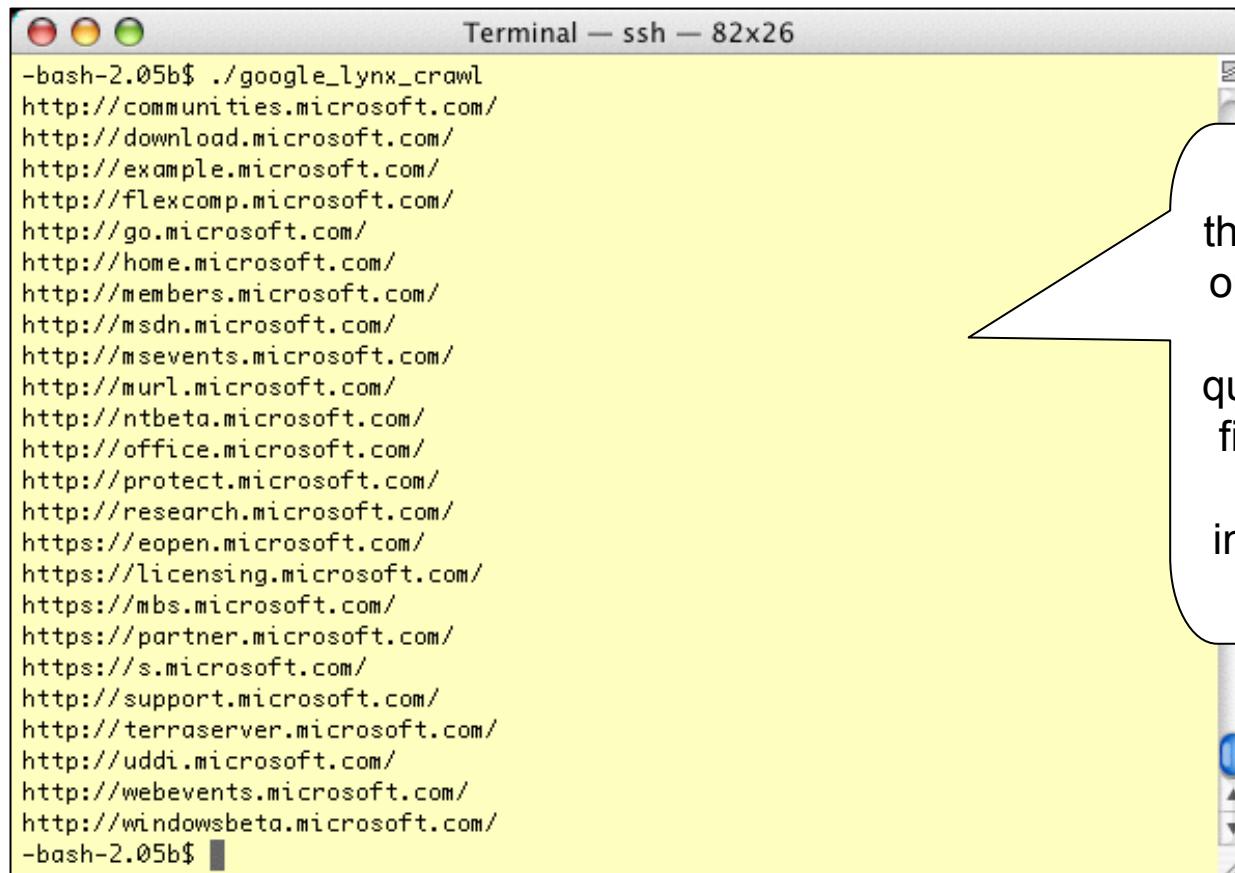
## Advanced Site Crawling



```
Terminal — ssh — 80x13
-bash-2.05b$ lynx -dump "http://www.google.com/search?\q=site:microsoft.com+www.microsoft.com&num=100" > test.html
-bash-2.05b$ lynx -dump "http://www.google.com/search?\q=site:microsoft.com+www.microsoft.com+web&num=100" >> test.html
-bash-2.05b$ lynx -dump "http://www.google.com/search?\q=site:microsoft.com+www.microsoft.com+site&num=100" >> test.html
-bash-2.05b$ lynx -dump "http://www.google.com/search?\q=site:microsoft.com+www.microsoft.com+email&num=100" >> test.html
-bash-2.05b$ lynx -dump "http://www.google.com/search?\q=site:microsoft.com+www.microsoft.com+about&num=100" >> test.html
-bash-2.05b$
```

Searching for multiple common words like “web”, “site”, “email”, and “about” along with site... appended to a file...

## Advanced Site Crawling



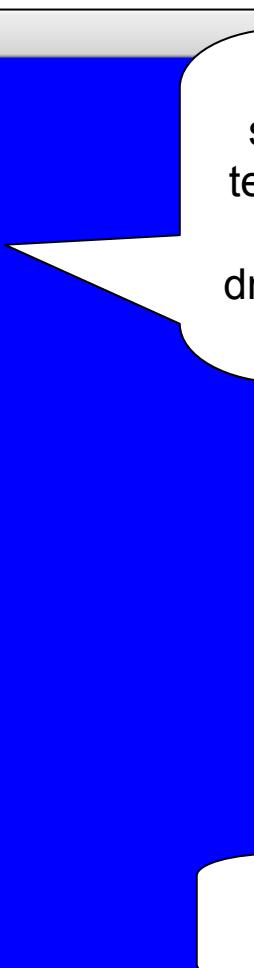
The image shows a terminal window titled "Terminal — ssh — 82x26". The window contains the following text:

```
-bash-2.05b$ ./google_lynx_crawl
http://communities.microsoft.com/
http://download.microsoft.com/
http://example.microsoft.com/
http://flexcomp.microsoft.com/
http://go.microsoft.com/
http://home.microsoft.com/
http://members.microsoft.com/
http://msdn.microsoft.com/
http://msevents.microsoft.com/
http://murl.microsoft.com/
http://ntbeta.microsoft.com/
http://office.microsoft.com/
http://protect.microsoft.com/
http://research.microsoft.com/
https://eopen.microsoft.com/
https://licensing.microsoft.com/
https://mbs.microsoft.com/
https://partner.microsoft.com/
https://s.microsoft.com/
http://support.microsoft.com/
http://terraserver.microsoft.com/
http://uddi.microsoft.com/
http://webevents.microsoft.com/
http://windowsbeta.microsoft.com/
-bash-2.05b$
```

A callout bubble points from the right side of the terminal window towards the text in the middle-right of the slide. The text inside the bubble reads:

Sifting through the output from those queries, we find many more interesting hits.

## Advanced Site Crawling



```
Terminal — bash — 88x30
-----
DNS names:
-----
v5.windowsupdate.microsoft.com
dgl.microsoft.com
www.beta.microsoft.com
g.microsoft.com
msevents.microsoft.com
www.microsoft.com
windowsbeta.microsoft.com
office.microsoft.com
netscan.research.microsoft.com
go.microsoft.com
webevents.microsoft.com
msdn.microsoft.com
partnering.one.microsoft.com
beta.microsoft.com
officebeta.microsoft.com
activex.microsoft.com
oca.microsoft.com
eopen.microsoft.com
lab.msdn.microsoft.com
download.microsoft.com
terraserver.microsoft.com
murl.microsoft.com
ntbeta.microsoft.com
v4.windowsupdate.microsoft.com
home.microsoft.com
support.microsoft.com
research.microsoft.com
```

Roelof Temmingh from sensepost.com coded this technique into a PERL (API-based) script called dns-mine.pl to achieve much more efficient results.

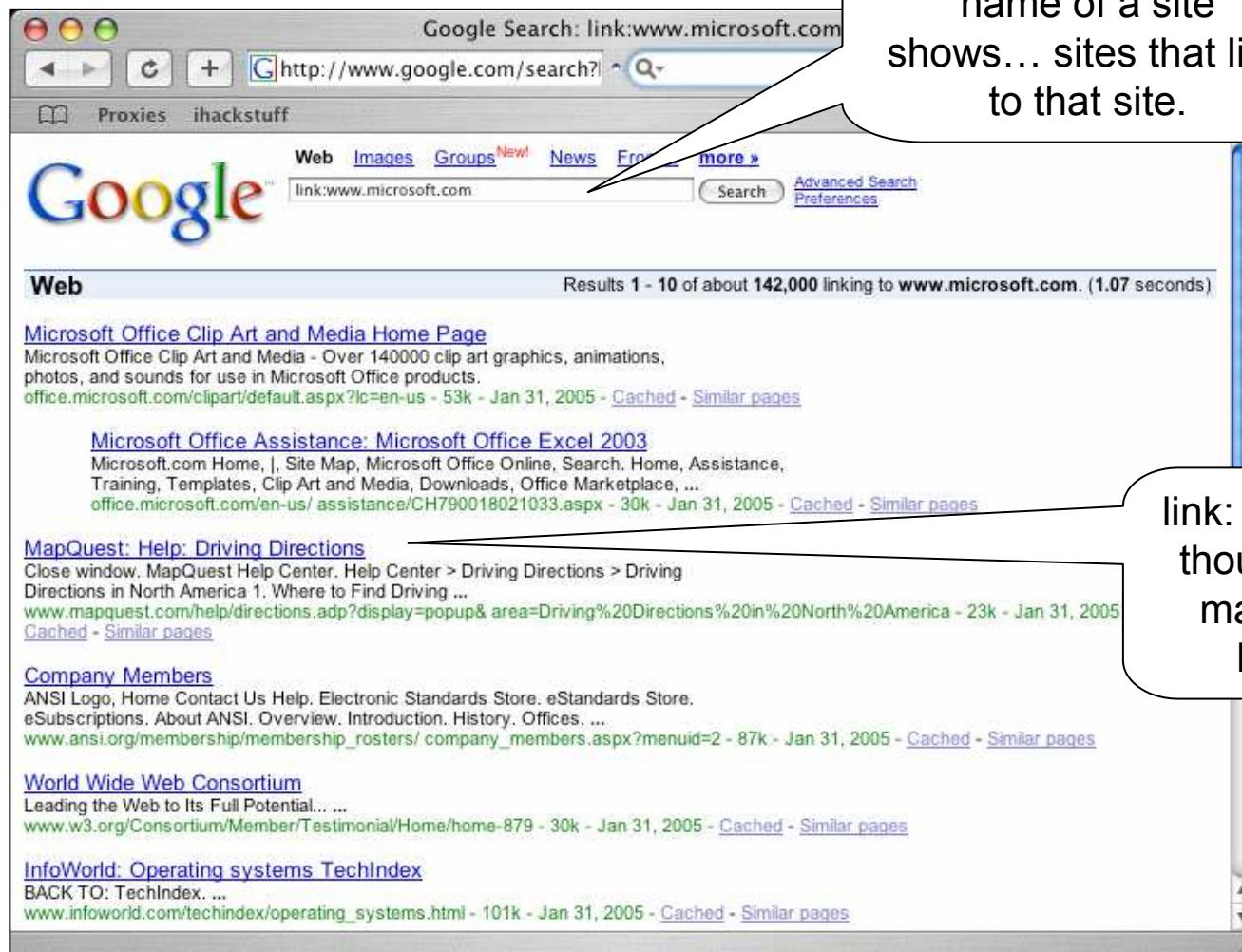
We'll look more at coding later...

---

## **Too much noise, not enough signal...**

- Getting lists of hosts and (sub)domains is great. It gives you more targets, but there's another angle.
  - Most systems are only as secure as their weakest link.
  - If a poorly-secured company has a trust relationship with your target, that's your way in.
- 
- Question: How can we determine site relationships with Google?
  - One Answer: the “link” operator.

# Raw Link Usage



link: combined with the name of a site shows... sites that link to that site.

link: has limits though. See mapquest here?

## Link has limits

The screenshot shows a Google search results page with the following details:

- Search Query:** link:www.microsoft.com site:mapquest.com
- Results:** Your search - link:www.microsoft.com site:mapquest.com - did not match any documents.
- Suggestions:**
  - Make sure all words are spelled correctly.
  - Try different keywords.
  - Try more general keywords.
  - Try fewer keywords.
- Help:** Also, you can try [Google Answers](#) for expert help with your search.

A callout bubble points to the search bar with the text: "...combining link: with site: doesn't seem to work..."

## Link has limits

Google Search: link:www.microsoft.com -site:microsoft.com

http://www.google.com ^ Google

Proxies ihackstuff

Web Images Groups New! News Froogle more »

link:www.microsoft.com -site:microsoft.com

Search Advanced S Preferences

**Web** Results 1 - 10 of about 1,740 for link:www.microsoft.com -site:microsoft.com

[Quick Reference Guide to Internet Search Engine Operators](#)

... Fields, Link, eg, link:www.microsoft.com [Shows pages linking to the URL]; Cache, eg, cache:www.microsoft.com [Shows page used to provide content used to judge ...]  
[www.utm.edu/departments/acadpro/library/information\\_pages/syntax.html](http://www.utm.edu/departments/acadpro/library/information_pages/syntax.html) - 76k -  
[Cached](#) - [Similar pages](#)

[Favorite link link](#)

... Yea, this is rather small but when viewing "My Favorite Link" ([www.Microsoft.com](http://www.Microsoft.com)) or the "Home Page" in the View Profile mode it's hyperlinked to <http://www.anetforums.com/posts.aspx?ThreadId=12227> - 16k - [Cached](#) - [Similar pages](#)

[Examples of Links That Lie](#)

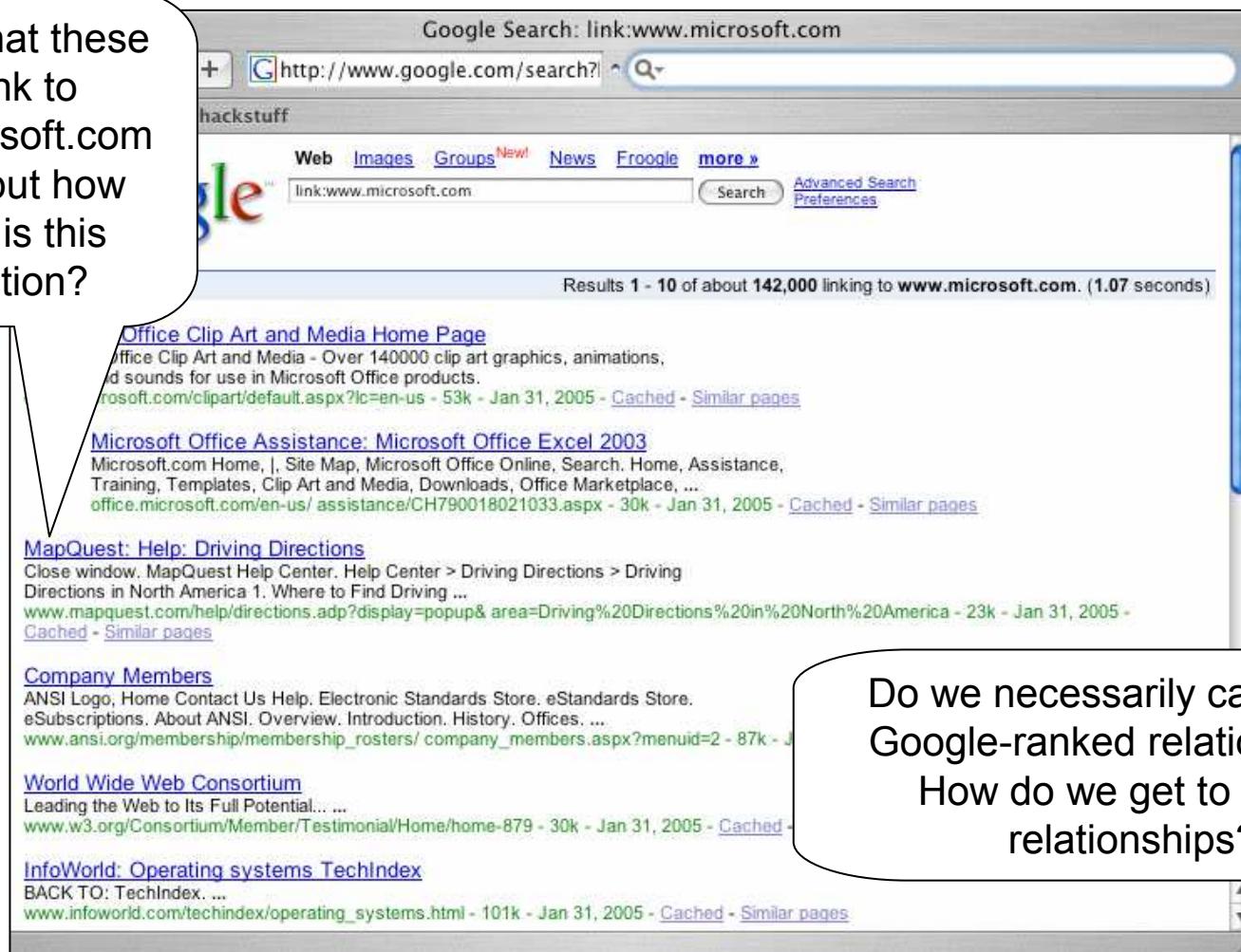
... The text displayed for the link does not have to be the real destination. For example, this link [www.microsoft.com](http://www.microsoft.com) really takes you to my home page. ...  
[www.michaelhorowitz.com/linksthatlie.html](http://www.michaelhorowitz.com/linksthatlie.html) - 20k - Feb 1, 2005 - [Cached](#) - [Similar pages](#)

Display a menu

Link: gets treated like normal search text (not a search modifier) when combined with other operators.

## Link has other limits

Knowing that these sites link to www.microsoft.com is great, but how relevant is this information?



Do we necessarily care about Google-ranked relationships?  
How do we get to REAL relationships?

---

## Non-obvious site relationships

- Sensepost to the rescue again! =)
- BiLE (the Bi-directional Link Extractor), available from [http://www.sensepost.com/garage\\_portal.html](http://www.sensepost.com/garage_portal.html) helps us gather together links from Google and piece together these relationships.
- There's much more detail on this process in their whitepaper, but let's cover the basics...

---

## **Non-obvious site relationships**

- A link from a site weighs more than a link to a site
  - Anyone can link to a site if they own web space (which is free to all)
- A link from a site with a lot of links weighs less than a link from a site with a small amount of links
  - This means specifically outbound links.
  - If a site has few outbound links, it is probably lighter.
  - There are obvious exceptions like link farms.

---

## Non-obvious site relationships

- A link to a site with a lot of links to the site weighs less than a link to a site with a small amount of links to the site.
  - If external sources link to a site, it must be important (or more specifically popular)
  - This is basically how Google weighs a site.
- The site that was given as input parameter need not end up with the highest weight – a good indication that the provided site is not the central site of the organization.”
  - If after much research, the site you are investigating doesn’t weight the most, you’ve probably missed the target’s main site.

# Who is Sensepost?

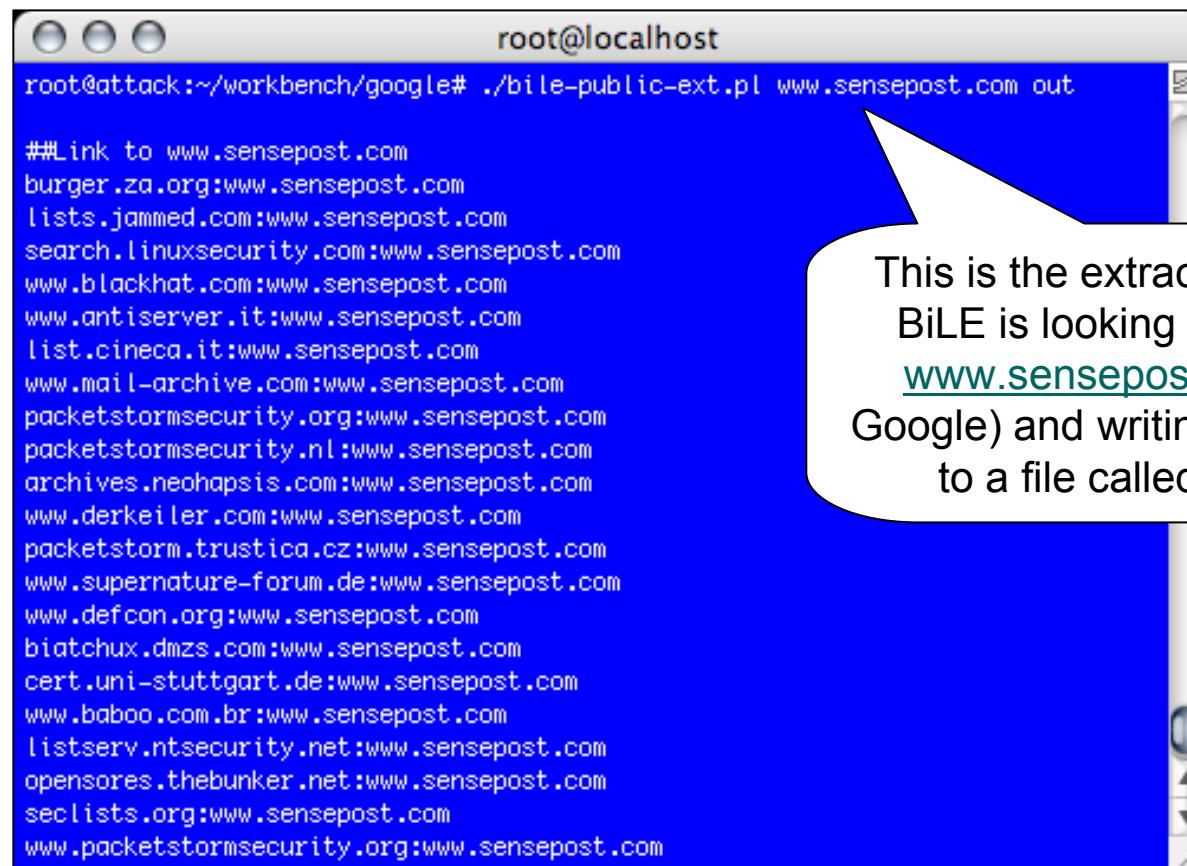
The screenshot shows a Mac OS X desktop with a Google search results window open. The window title is "Google Search: sensepost". The search bar contains "sensepost". The results are filtered under the "Web" tab, showing approximately 6,490 results. The first few results are:

- SensePost**  
... for such threats. HackRack is a innovative, cutting edge automated scanner designed and maintained by **SensePost**. It encapsulates ...  
[www.sensepost.com/automatedscanning.html](http://www.sensepost.com/automatedscanning.html) - 21k - [Cached](#) - [Similar pages](#)  
[ [More results from www.sensepost.com](#) ]
- SQL insertion**  
... During the time that we were preparing for BlackHat, Haroon Meer ([haroon@sensepost.com](mailto:haroon@sensepost.com)) started extensive fiddling with SQL insertion. ... **SensePost** IT Security. ...  
[www.cgisecurity.com/lib/SQLInsertion.htm](http://www.cgisecurity.com/lib/SQLInsertion.htm) - 40k - [Cached](#) - [Similar pages](#)
- SensePost**  
The Garage : Downloads, Defcon/BlackHat 2003 Las Vegas  
(Putting the Tea back into CyberTerrorism ...  
[168.210.134.6/garage.html](http://168.210.134.6/garage.html) - 21k - [Cached](#) - [Similar pages](#)
- SensePost**  
The Garage : News, Check out the New York Times Article on computer security mentioning **SensePost**. ... **SensePost** talks on Cyber-terrorism at BlackHat. ...  
[168.210.134.6/garage\\_news.html](http://168.210.134.6/garage_news.html) - 22k - [Cached](#) - [Similar pages](#)  
[ [More results from 168.210.134.6](#) ]
- Index of /nf0/convention\_cdroms/defcon11/SensePost**  
Index of /nf0/convention\_cdroms/defcon11/SensePost. Name Last modified Size  
Description Parent Directory 08-Dec-2004 15:36 - dc-11 ...  
[mediawhore.wi2600.org/nf0/convention\\_cdroms/defcon11/SensePost/](http://mediawhore.wi2600.org/nf0/convention_cdroms/defcon11/SensePost/) - 2k - [Cached](#) - [Similar pages](#)

Relying on Google's 6400+ results can be daunting... and misleading.

## Non-obvious site relationships

- It seems dizzying to pull all this together, but BiLE does wonders. Let's point it at sensepost.com:



The screenshot shows a terminal window titled "root@localhost". The command entered is "root@attack:~/workbench/google# ./bile-public-ext.pl www.sensepost.com out". The output of the command is a list of URLs, each preceded by a "#Link to". The list includes various websites such as burger.za.org, lists.jammed.com, search.linuxsecurity.com, www.blackhat.com, www.antiserver.it, list.cineca.it, www.mail-archive.com, packetstormsecurity.org, packetstormsecurity.nl, archives.neohapsis.com, www.derkeiler.com, packetstorm.trustica.cz, www.supernature-forum.de, www.defcon.org, biatchux.dmnzs.com, cert.uni-stuttgart.de, www.baboo.com.br, listserv.ntsecurity.net, opensores.thebunker.net, seclists.org, and www.packetstormsecurity.org, all pointing to www.sensepost.com.

```
root@localhost
root@attack:~/workbench/google# ./bile-public-ext.pl www.sensepost.com out

##Link to www.sensepost.com
burger.za.org:www.sensepost.com
lists.jammed.com:www.sensepost.com
search.linuxsecurity.com:www.sensepost.com
www.blackhat.com:www.sensepost.com
www.antiserver.it:www.sensepost.com
list.cineca.it:www.sensepost.com
www.mail-archive.com:www.sensepost.com
packetstormsecurity.org:www.sensepost.com
packetstormsecurity.nl:www.sensepost.com
archives.neohapsis.com:www.sensepost.com
www.derkeiler.com:www.sensepost.com
packetstorm.trustica.cz:www.sensepost.com
www.supernature-forum.de:www.sensepost.com
www.defcon.org:www.sensepost.com
biatchux.dmnzs.com:www.sensepost.com
cert.uni-stuttgart.de:www.sensepost.com
www.baboo.com.br:www.sensepost.com
listserv.ntsecurity.net:www.sensepost.com
opensores.thebunker.net:www.sensepost.com
seclists.org:www.sensepost.com
www.packetstormsecurity.org:www.sensepost.com
```

This is the extraction phase.  
BiLE is looking for links to  
[www.sensepost.com](http://www.sensepost.com) (via  
Google) and writing the results  
to a file called “out”...

## Non-obvious site relationships

- This is the weigh phase. BiLE takes the output from the extraction phase...

The screenshot shows a terminal window titled "root@localhost:~/file/final — ssh — %3". The command run is "./bile-public-weigh.pl www.sensepost.com out new". The output lists various websites and their scores, indicating their relationship strength to the target site. The list includes:

```
root@attack:~/workbench/google# ./bile-public-weigh.pl www.sensepost.com out new
root@attack:~/workbench/google# more new
www.sensepost.com:144.600
www.blackhat.com:18.000
biatchux.dmxs.com:18.000
packetstormsecurity.org:11.400
packetstormsecurity.nl:11.400
securitylab.ru:10.800
www.packetstormsecurity.org:9.346
dewil.ru:7.817
lists.virus.org:7.726
search.linuxsecurity.com:7.344
lists.jammed.com:7.344
list.cineca.it:7.344
www.securityfocus.com:7.298
www.mail-archive.com:7.298
archives.neohapsis.com:7.298
www.supernature-forum.de:7.200
www.derkeiler.com:7.200
www.defcon.org:7.200
www.baboo.com.br:7.200
www.antiserver.it:7.200
seclists.org:7.200
packetstorm.trustica.cz:7.200
--More--(9%)
```

And weighs the results using the four main criteria of weighing discussed above... aided primarily by Google searches.

This shows the strongest relationships to our target site first, which during an assessment equate to secondary targets, especially for information gathering.

## The next step...



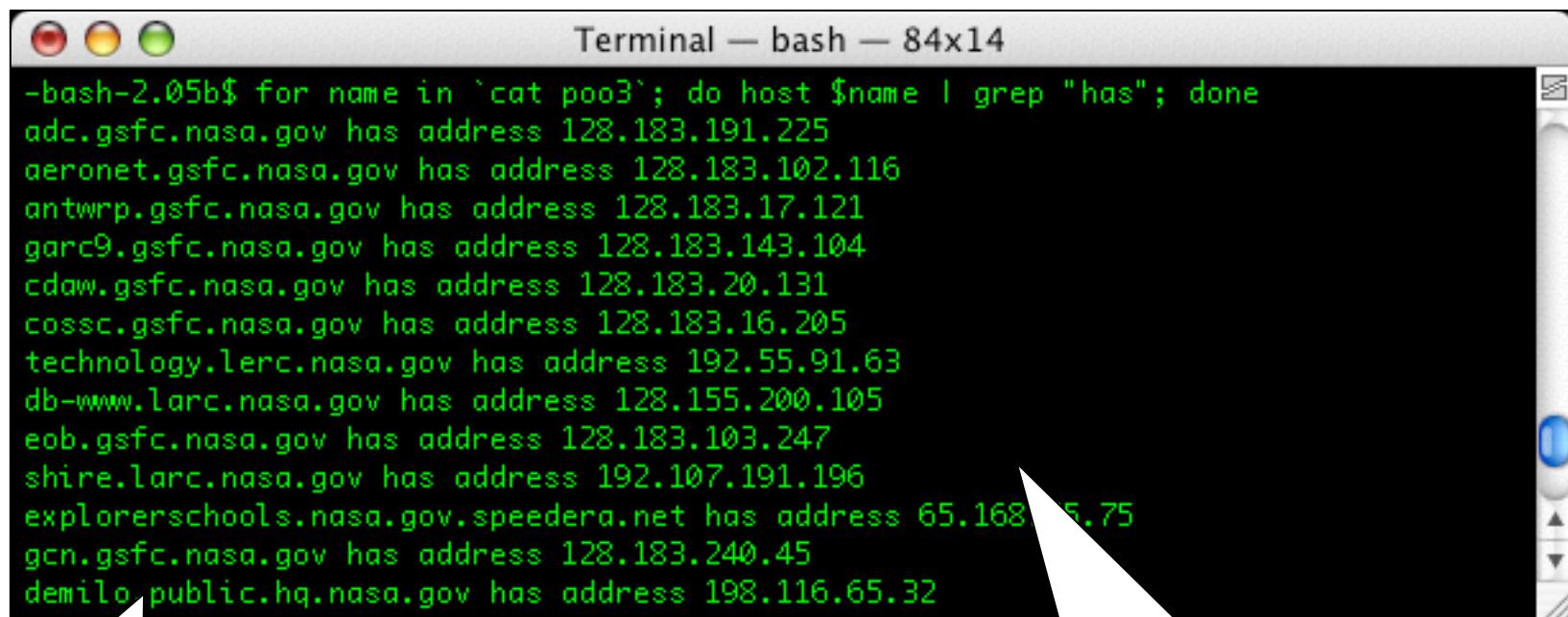
Let's say we're looking at NASA....

We could use 'googleturd' searches, like site:nasa to locate typos which may be real sites...

How can we verify these???

## Host verification...

- Cleaning the names and running DNS lookups is one way...



The screenshot shows a Mac OS X terminal window titled "Terminal — bash — 84x14". The window contains a command-line session where the user has run a script to perform DNS lookups. The output lists several host names along with their corresponding IP addresses. The hosts listed include adc.gsfc.nasa.gov, aeronet.gsfc.nasa.gov, antwrp.gsfc.nasa.gov, garc9.gsfc.nasa.gov, cdaw.gsfc.nasa.gov, cosscc.gsfc.nasa.gov, technology.lerc.nasa.gov, db-www.larc.nasa.gov, eob.gsfc.nasa.gov, shire.larc.nasa.gov, explorerschools.nasa.gov.speedera.net, gcn.gsfc.nasa.gov, and demilo.public.hq.nasa.gov. The IP addresses range from 128.183.x.x to 192.107.x.x and 198.116.x.x.

```
-bash-2.05b$ for name in `cat poo3`; do host $name | grep "has"; done
adc.gsfc.nasa.gov has address 128.183.191.225
aeronet.gsfc.nasa.gov has address 128.183.102.116
antwrp.gsfc.nasa.gov has address 128.183.17.121
garc9.gsfc.nasa.gov has address 128.183.143.104
cdaw.gsfc.nasa.gov has address 128.183.20.131
cosscc.gsfc.nasa.gov has address 128.183.16.205
technology.lerc.nasa.gov has address 192.55.91.63
db-www.larc.nasa.gov has address 128.155.200.105
eob.gsfc.nasa.gov has address 128.183.103.247
shire.larc.nasa.gov has address 192.107.191.196
explorerschools.nasa.gov.speedera.net has address 65.168.5.75
gcn.gsfc.nasa.gov has address 128.183.240.45
demilo.public.hq.nasa.gov has address 198.116.65.32
```

Pay dirt! Now what???

We could further expand  
on these IP ranges via  
DNS queries as well...

---

## Expanding out...

- Once armed with a list of sites and domains, we could expand out the list in several ways. DNS queries are helpful, but what else can we do to get more names to try?
- From whatever source, let's say we get two names from verizon, 'foundation' and investor'...

[\[PDF\] Verizon's 2003 Annual Report - Investor Information](#)

File Format: PDF/Adobe Acrobat

Page 1. Registered Shareowner Services Questions or requests for assistance regarding changes to or transfers of your registered ...

[investor.verizon.com/2003annual/\\_download/vz\\_investor\\_info.pdf](http://investor.verizon.com/2003annual/_download/vz_investor_info.pdf) - [Similar pages](#)

[foundation.verizon.com/cybergrants/plsql/incomm.info?x\\_type\\_flag=DELETE](http://foundation.verizon.com/cybergrants/plsql/incomm.info?x_type_flag=DELETE)

[Similar pages](#)

# Google Sets

- Although this is a simple example, we can throw these two words into Google Sets....

The screenshot shows a Mac OS X window titled "Google Sets". The URL in the address bar is <http://labs.google.com/sets>. The page displays the Google logo and the text "Automatically create sets of items from a few examples." Below this, instructions say "Enter a few items from a set of things. ([example](#)) Next, press *Large Set* or *Small Set* and we'll try to predict other items in the set." A list of five items is shown, each preceded by a bullet point and an input field:

- investor
- foundation
- 
- 
- 

A link "(clear all)" is located below the list. At the bottom, there are two buttons: "Large Set" and "Small Set (15 items or fewer)". The status bar at the bottom of the window says "Display a menu".

Predicted Items
<a href="#">Investor</a>
<a href="#">foundation</a>
<a href="#">Second Foundation</a>
<a href="#">Intermediate</a>
<a href="#">Entrepreneur</a>
<a href="#">Self Employed</a>
<a href="#">Advanced</a>
<a href="#">Roof</a>
<a href="#">framing</a>
<a href="#">Alliances</a>
<a href="#">Careers</a>
<a href="#">Community</a>
<a href="#">columns</a>
<a href="#">Completion</a>
<a href="#">Lender</a>
<a href="#">Excavation</a>
<a href="#">BOARD MEMBERS</a>
<a href="#">walls</a>
<a href="#">Application</a>
<a href="#">Earnings Reports</a>
<a href="#">IPOs</a>
<a href="#">Financial</a>
<a href="#">Certificate</a>
<a href="#">professional</a>
<a href="#">Blusher</a>
<a href="#">Research</a>
<a href="#">groundwork</a>
<a href="#">fundament</a>
<a href="#">roof structure</a>
<a href="#">Business Directory</a>
<a href="#">floors</a>
<a href="#">P F</a>
<a href="#">Contact Us</a>
<a href="#">Metal Roof</a>
<a href="#">FOGA FOPA</a>
<a href="#">Owner Occupied</a>
<a href="#">STEM Methodology</a>
<a href="#">TEACHERS</a>
<a href="#">DISTRIBUTION</a>

## Expanding

- Then, we can take all these words and perform DNS host lookups against each of these combinations:

```
Terminal — ssh — 83x14
-bash-2.05b$ for name in `cat list3`; do host $name.verizon.com | grep "has"; done
Business.verizon.com has address 206.46.230.36
foundation.verizon.com has address 216.251.248.19
Investor.verizon.com has address 198.92.149.185
Foundation.verizon.com has address 216.251.248.19
-bash-2.05b$
```

..this leads to a new hit,  
'business.verizon.com'.

Google sets allows  
you to expand on a  
list once you run out  
of options.

---

## Fuzzing

- Given hosts with numbers and “predictable” names, we could fuzz the numbers, performing DNS lookups on those names...
- I’ll let Roelof at sensepost discuss this topic, however... =)

[bhst03.verizon.com/](http://bhst03.verizon.com/)

[Similar pages](#)

<https://www33.verizon.com/wi-fi/login/locations/locations-remote.jsp>

[Similar pages](#)

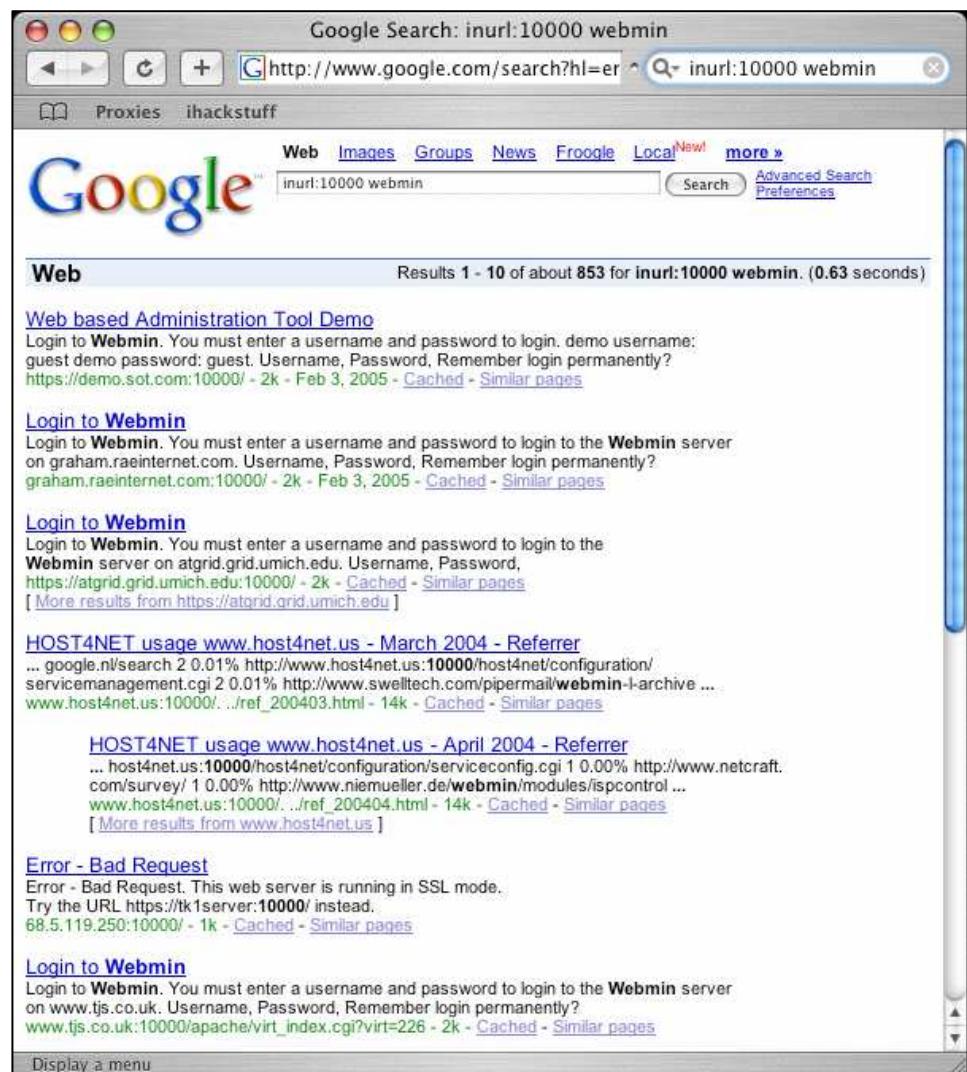
---

## **Limitless mapping possibilities...**

- Once you get rolling with Google mapping, especially automated recursive mapping, you'll be AMAZED at how deep you can dig into the layout of a target.

## Port scanning

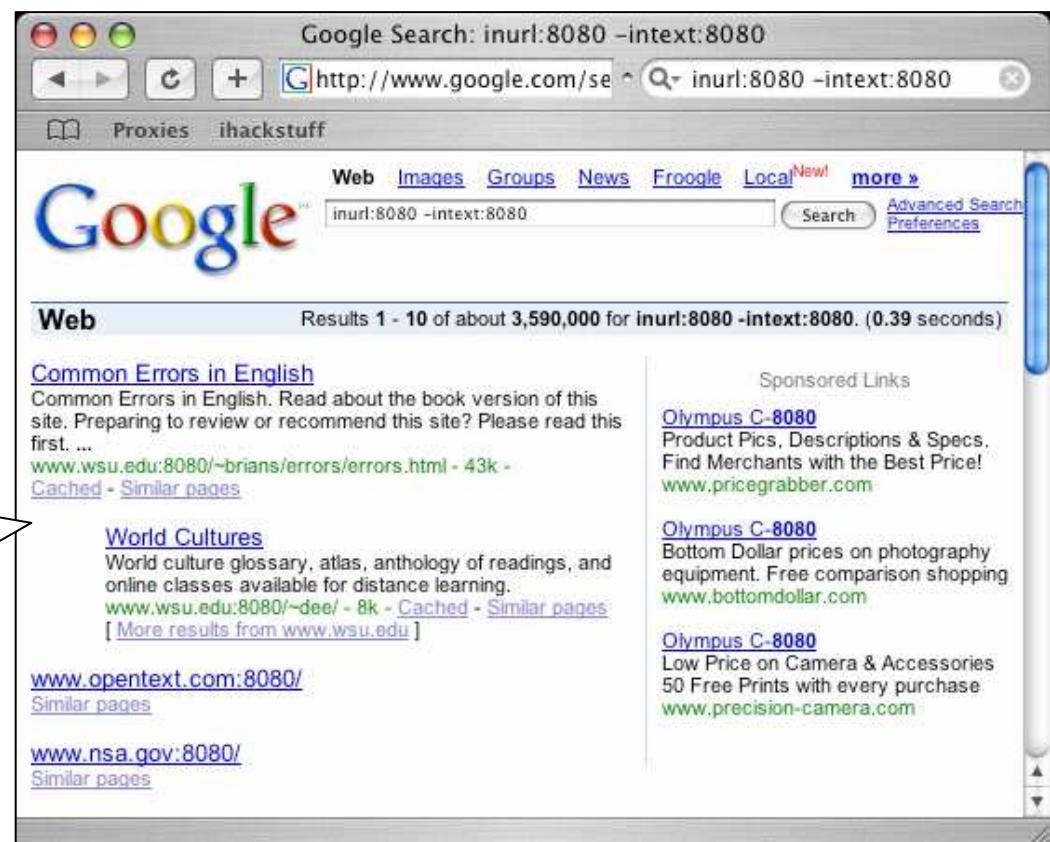
- Although crude, there are ways to do basic “portscanning” with Google.
- First, combine inurl searches for a port with the name of a service that commonly listens on that port... (optionally combined with the site operator)



## Inurl -intext scanning

- Another way to go is to use a port number with inurl, combined with a negative intext search for that port number.

This search locates servers listening on port 8080.



## Third party scanners

- When all else fails, Google for servers that can do your portscan for you!

Google Search: filetype:php inurl:nqt intext:"Network Query Tool"

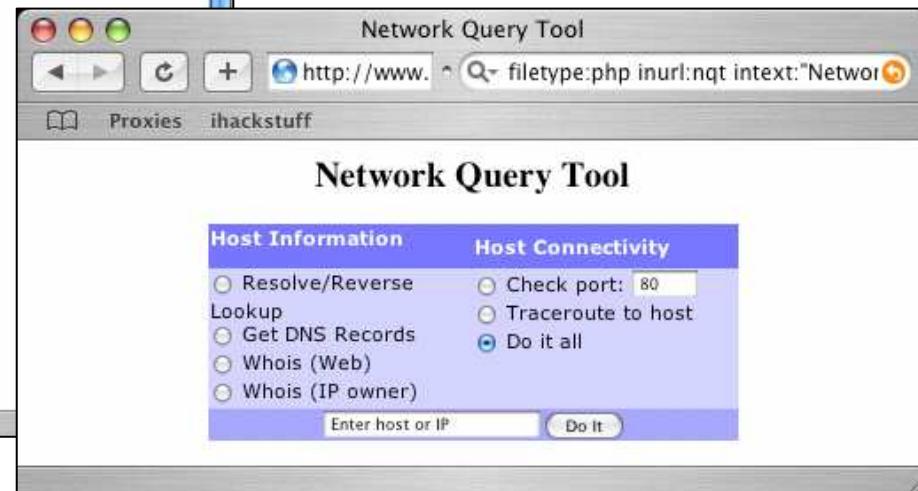
Results 1 - 10 of about 124 for filetype:php inurl:nqt intext:"Network Query Tool". (0.31 seconds)

**Network Query Tool**  
Network Query Tool. Host Information NQT20030507, Host Connectivity. Resolve/Reverse Lookup Get DNS Records Whois (Web) Whois (IP owner) ...  
[www.serversanddomains.net/nqt.php](http://www.serversanddomains.net/nqt.php) - 3k - [Cached](#) - [Similar pages](#)

**Obsolete Laboratory**  
... Network Query Tool. Host Information, Host Connectivity. Resolve/Reverse Lookup Get DNS Records Whois (Web) Whois (IP owner). Check ...  
[www.obsoletelab.com/nqt.php](http://www.obsoletelab.com/nqt.php) - 19k - [Cached](#) - [Similar pages](#)

**Exponetic Ltd - East London Web Design, Internet Development ...**  
... Error: You did not specify a valid target host or IP. NQT20021115 Network Query Tool 1.5 Copyright 2002 shaun@shat.net. Satisfied ...  
[www.exponetic.com/resources/nqt.php](http://www.exponetic.com/resources/nqt.php) - 14k - Feb 3, 2005 - [Cached](#) - [Similar pages](#)

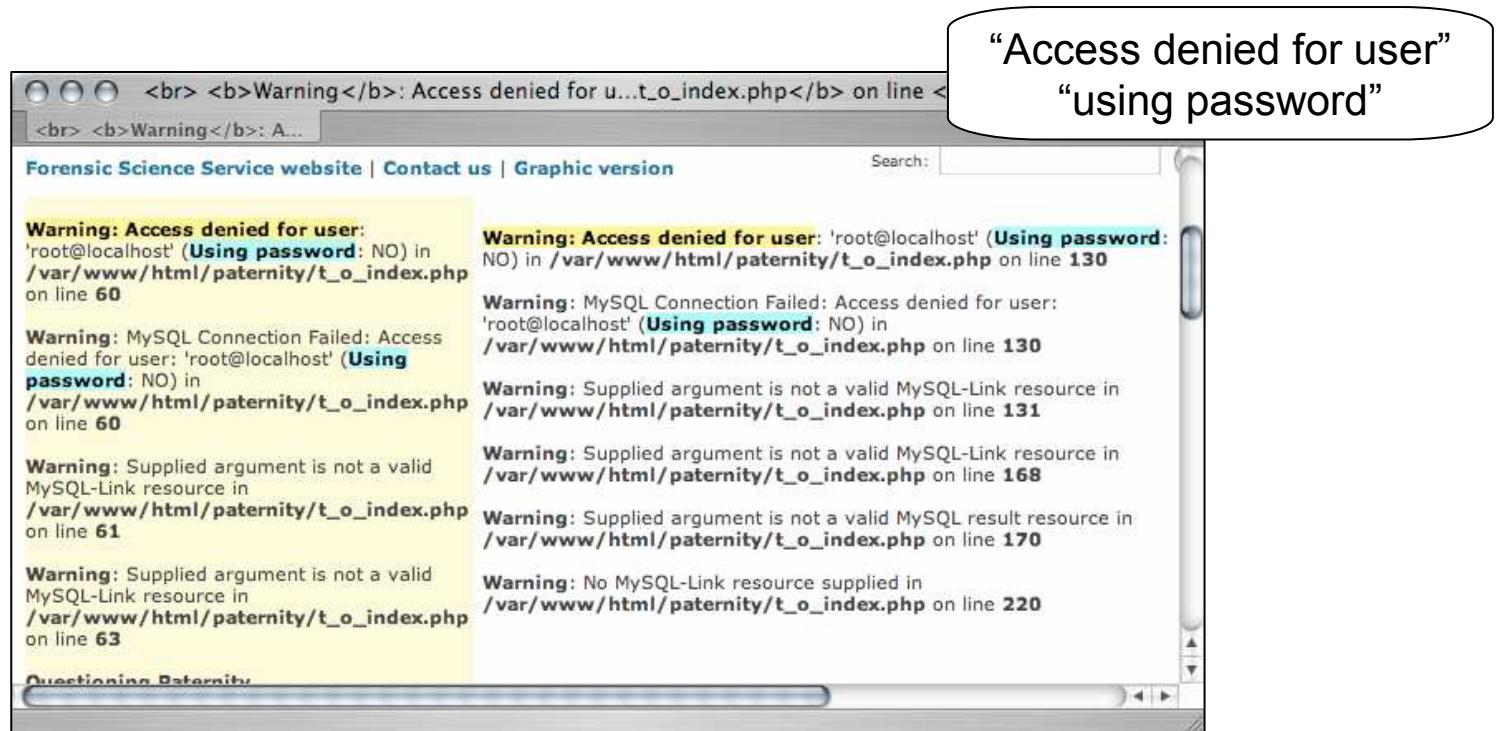
**Network Query Tool**  
... However, future versions may not support this any longer. in /home/sites/site119/web/cgi-bin/nqt/nqt.php on line 281. Network Query Tool. ...  
[www.seerit.org/cgi-bin/nqt/nqt.php](http://www.seerit.org/cgi-bin/nqt/nqt.php) - 7k - [Cached](#) - [Similar pages](#)



# Document Grinding and Database Digging

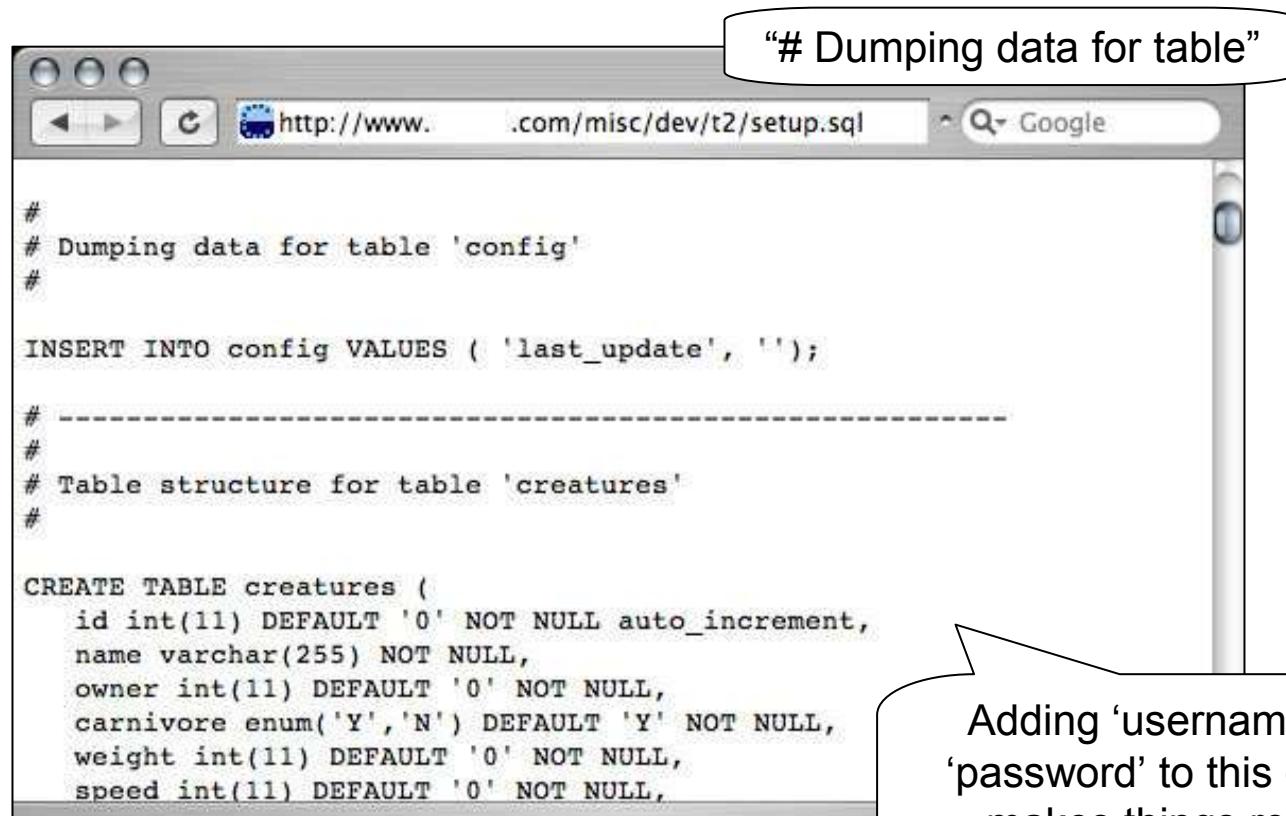
Documents and databases contain a wealth of information.  
Let's look at ways to foster abuse of SQL databases with Google.

# SQL Usernames



## SQL Schemas

- Entire SQL Database dumps



The screenshot shows a web browser window with the URL <http://www. .com/misc/dev/t2/setup.sql>. The page content is an SQL dump. A callout bubble points to the first line of the dump with the text "# Dumping data for table". Another callout bubble points to the bottom of the dump with the text "Adding 'username' or 'password' to this query makes things really interesting."

```
# Dumping data for table 'config'  
#  
  
INSERT INTO config VALUES ( 'last_update', '' );  
  
# -----  
#  
# Table structure for table 'creatures'  
#  
  
CREATE TABLE creatures (  
    id int(11) DEFAULT '0' NOT NULL auto_increment,  
    name varchar(255) NOT NULL,  
    owner int(11) DEFAULT '0' NOT NULL,  
    carnivore enum('Y','N') DEFAULT 'Y' NOT NULL,  
    weight int(11) DEFAULT '0' NOT NULL,  
    speed int(11) DEFAULT '0' NOT NULL,
```

Adding 'username' or  
'password' to this query  
makes things really  
interesting.

Improper command termination can be abused quite easily by an attacker.

## SQL injection hints

```
ERROR : ORA-00933: SQL command not properly ended  
:42000 -errorcodes :1  
  
ERROR : ORA-00933: SQL command not properly ended  
:42000 -errorcodes :1  
  
ERROR : ORA-00933: SQL command not properly ended  
:42000 -errorcodes :1  
  
ERROR : ORA-00933: SQL command not properly ended  
:42000 -errorcodes :1  
  
[Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark before the character string '>Mrs. Prisbrey's Second Grade Class v'.
```

"ORA-00933:  
SQL command  
not properly  
ended"

```
SQL = "SELECT LinkBuilder_Enabled, FK_E  
INNER JOIN TB_Teacher ON TB_ClassPage  
WHERE PK_ClassPageID = 30365 AND Lin  
Class v"
```

"Unclosed quotation  
mark before the  
character string"

Error Detail: [MERANT][ODBC SQL  
Server Driver][SQL Server]Unclosed  
quotation mark before the character string  
'Discover Platinum Card'.

## SQL source

- Getting lines of SQL source can aid an attacker.

The image shows two overlapping error dialog boxes from a web application. The top dialog has a title bar 'Error Occurred While Processing Request' and a message: 'The error occurred in D:\INET\fun\_site\\_NEW\\_f\_main.cfm: line 87'. Below this, it lists three call stack entries: 'Called from D:\INET\fun\_site\\_NEW\\_f\_index.cfm: line 13', 'Called from D:\INET\fun\_site\\_NEW\\_f\_index.cfm: line 14', and 'Called from D:\INET\fun\_site\\_NEW\\_f\_index.cfm: line 200'. Lines 85 through 89 of the code are shown:  
85 : SELECT  
86 : FROM wal...  
87 : WHERE id  
88 : </cfquery>  
89 : </cfloop>

The bottom dialog also has a title bar 'Error Occurred While Processing Request' and a message: 'SQL = "SELECT'. It displays the full SQL query that was generated, which includes multiple SELECT statements and WHERE clauses. A callout bubble points to the first SELECT statement in the bottom dialog with the text: 'intitle:"Error Occurred" "The error occurred in"'.

```
intitle:"Error  
Occurred" "The  
error occurred in"
```

```
SQL = "SELECT  
i.id,i.thumbnail_filename,i.item_description,i.item_graphic_filename,i.item_addnl_...  
i.item_addnl_field_2,i.item_addnl_field_3,i.item_addnl_field_4,i.item_addnl_field_5,  
i.is_a_service,i.price,i.merchant_id,i.thumbnail_link_text FROM (SELECT  
id,thumbnail_filename,item_description,item_graphic_filename,item_addnl_field_...  
item_addnl_field_2,item_addnl_field_3,item_addnl_field_4,item_addnl_field_5,  
is_a_service,price,merchant_id,thumbnail_link_text FROM item WHERE control_id =  
3505 AND status in ('AVAILABLE','NOSTOCK')) i, (SELECT id, control_id FROM item_group WHERE id = 46694 AND control_id = 3505) ig, (SELECT item_id FROM item_group WHERE item_group_id = 46694 ) igi WHERE i.id = igi.item_id ORDER BY i.item_description"
```

## Going after SQL passwords

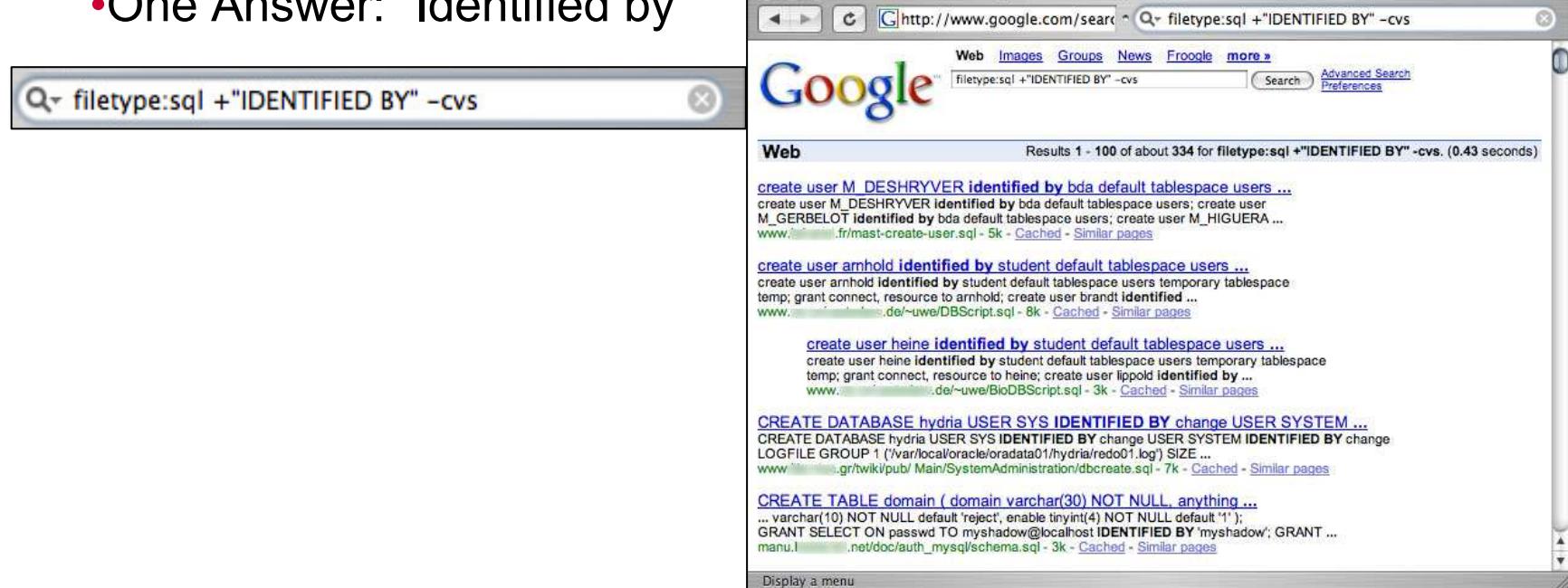
The screenshot shows a web browser window with the URL `http://216.239.41.1...ysql_connect&hl=e` in the address bar. A search bar below it contains `http://216.239.41.104/sear...`. A search result is displayed, showing a snippet of PHP code:

```
<?php  
$host="";  
$user="cs3projo";  
$password="tTnM76mx5"  
$database="cs3projo"  
  
mysql_connect($host,$user,$password);  
@mysql_select_db($database) or die ("I cannot  
?>
```

A callout bubble points to the line `mysql_connect($host,$user,$password);` with the text: "Include files with cleartext passwords...".

## More SQL Passwords

- Question: What's the SQL syntax that can be used to set a password?
- (TWO WORDS)
- One Answer: “Identified by”



## More SQL Passwords

- The slightly more hardcore version...

A screenshot of a search results page from a web browser. The search query in the bar is "filetype:sql +\"IDENTIFIED BY\" ("Grant \* on \*" | "create user")". The results are listed under the "Web" tab, showing 1 - 84 of about 255 results. The results include several snippets of SQL code, such as:

- `create user M_DESHRYVER identified by bda default tablespace users ...`
- `create user M_DESHRYVER identified by bda default tablespace users; create user M_GERBELOT identified by bda default tablespace users; create user M_HIGUERA ...`
- `CREATE DATABASE hydria USER SYS IDENTIFIED BY change USER SYSTEM`
- `... EXECUTE ON DBMS_PIPE TO PUBLIC; GRANT EXECUTE ON DBMS_LOCK TO PUBLIC ... ROLLBACK SEGMENT RBS ONLINE; CREATE USER HYDRO IDENTIFIED BY VALUES '4F1807D5B6FB986E' ...`
- `create user arnhold identified by student default tablespace users ...`
- `create user heine identified by student default tablespace users ...`
- `REM Akadia AG, Zieglerstrasse 34, CH-3007 Bern REM ...`
- `REM Akadia AG, Zieglerstrasse 34, CH-3007 Bern REM ...`

The right side of the page features a "Sponsored Links" sidebar with an advertisement for "Database Management Trial" and a link to "www.dbartisan.com". Below the sidebar is a message: "\$20.000 Free Grant Money Never Repay Guaranteed! Use For Any Purpose. Register Today Online www.RealCashPrograms.com See your message here...".

# Various database detection queries

Query	Description
<code>inurl:nuke filetype:sql</code>	php-nuke or postnuke CMS dumps
<code>filetype:sql password</code>	SQL database dumps or batched SQL commands
<code>filetype:sql "IDENTIFIED BY" -cvs</code>	SQL database dumps or batched SQL commands, focus on "IDENTIFIED BY", which can locate passwords
<code>"# Dumping data for table (username user users password)"</code>	SQL database dumps or batched SQL commands, focus on interesting terms
<code>"#mysql dump" filetype:sql</code>	SQL database dumps
<code>"# Dumping data for table"</code>	SQL database dumps
<code>"# phpMyAdmin MySQL-Dump"</code>	SQL database dumps created by phpMyAdmin
<code>filetype:txt</code>	
<code>"# phpMyAdmin MySQL-Dump"</code>	SQL database dumps created by phpMyAdmin (variation)
<code>"INSERT INTO" -"the"</code>	phpMyAdmin (variation)

SQL dump detection

Query	Description
<code>filetype:cfm "cfapplication name"</code>	ColdFusion source code
<code>password</code>	
<code>filetype:mdb inurl:users.mdb</code>	Microsoft Access user database
<code>inurl:email filetype:mdb</code>	Microsoft Access e-mail database
<code>inurl:backup filetype:mdb</code>	Microsoft Access backup databases
<code>inurl:forum filetype:mdb</code>	Microsoft Access forum databases
<code>inurl:/db/main.mdb</code>	ASP-Nuke databases
<code>inurl:profiles filetype:mdb</code>	Microsoft Access user profile databases
<code>filetype:asp DBQ=" * Server.</code>	Microsoft Access database connection
<code>MapPath("*.mdb")</code>	string search
<code>allinurl: admin mdb</code>	Microsoft Access administration databases

Database detection

# Automation

Page Scraping in Perl  
API querying in Perl

---

## Page Scraping with Perl

- This Perl code, by James Foster, provides a good framework for “page scraping” Google results.
- This method relies on manually querying Google, and searching the resultant HTML for the “interesting stuff.”

```
#!/usr/bin/perl -w
use IO::Socket;

#Section 2
$query = '/search?hl=en&q=dog';
$server = 'www.google.com';
$port = 80;
```

We will be making socket calls. We need IO::Socket.

We hardcode our query (which we can make a parameter later), our Google server and our port number.

---

# Page Scraping with Perl

```
sub socketInit()
{
    $socket = IO::Socket::INET->new(
        Proto => 'tcp',
        PeerAddr => $server,
        PeerPort => $port,
        Timeout => 10,
    );

    unless($socket)
    {
        die("Could not connect to $server:$port");
    }

    $socket->autoflush(1);
}
```

Next we have a very generic  
socket initialization  
subroutine.

# Page Scraping with Perl

```
sub sendQuery($)
{
my ($myquery) = @_;
print $socket ("GET $myquery HTTP/1.0\n\n");
while ($line = <$socket>)
{
    if ($line =~ /Results.*of/about/)
    {
        return $line;
    }
}
```

This subroutine sends the Google query (hardcoded above) and accepts one parameter, the Google query.

Google returned HTML is processed, and the line containing “of about” (our result line) is returned from this routine.

Results 1 - 10 of about 46,600 for "[james foster](#)". (0.49 seconds)

## Page Scraping with Perl

```
sub getTotalHits($)
{
my ($ourline) = @_;
$hits="";
$index = index($ourline, "of about");
$str = substr($ourline, $index, 30);
@buf=split(//,$str);
for ($i = 0; $i < 30; $i++)
{
    if ($buf[$i] =~ /[0-9]/)
    {
        $hits=$hits.$buf[$i];
    }
}
return $hits;
}
```

This subroutine takes one parameter (the results line from the Sendquery)

"of about is located"...

...the next 30 characters are grabbed...

... all the digits are removed....

...stored in \$hits...

...and returned.

Results 1 - 10 of about 46,600 for "[james foster](#)". (0.49 seconds)

## Page Scraping with Perl

```
socketInit();  
$String = sendQuery($query);  
$Totalhits = getTotalHits($String);  
  
#Printing to STDOUT the Total Hits Retrieved from Google  
print ($Totalhits);
```

The socket is initialized...

...the query is sent...

This piece of code drives all the subroutines.

...the total hits are determined...

...and printed out.

## CGI Scanning

```
/iisadmpwd/  
/iisadmpwd/achg.htr  
/iisadmpwd/aexp.htr  
/iisadmpwd/aexp2.htr  
/iisadmpwd/aexp2b.htr
```

Another automation example might involve chopping up a CGI scanner's vulnerability file...

```
inurl:/iisadmpwd/  
inurl:/iisadmpwd/achg.htr  
inurl:/iisadmpwd/aexp.htr  
inurl:/iisadmpwd/aexp2.htr  
inurl:/iisadmpwd/aexp2b.htr
```

... converting the checks into Google queries, sending these queries to a Google scanner.

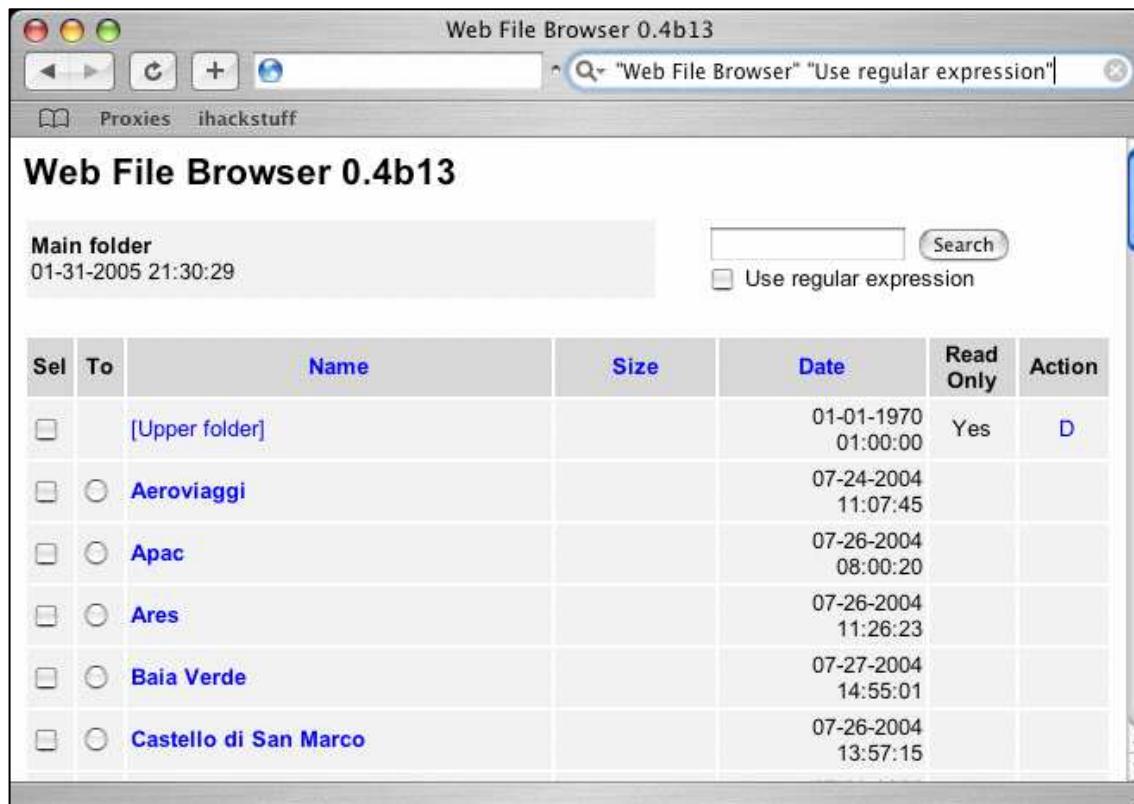
```
intitle:index.of /iisadmpwd/  
intitle:index.of /iisadmpwd/achg.htr  
intitle:index.of /iisadmpwd/aexp.htr  
intitle:index.of /iisadmpwd/aexp2.htr  
intitle:index.of /iisadmpwd/aexp2b.htr
```

# Web Servers, Login Portals, Network Hardware

Network devices can be soooo much fun to Google for...

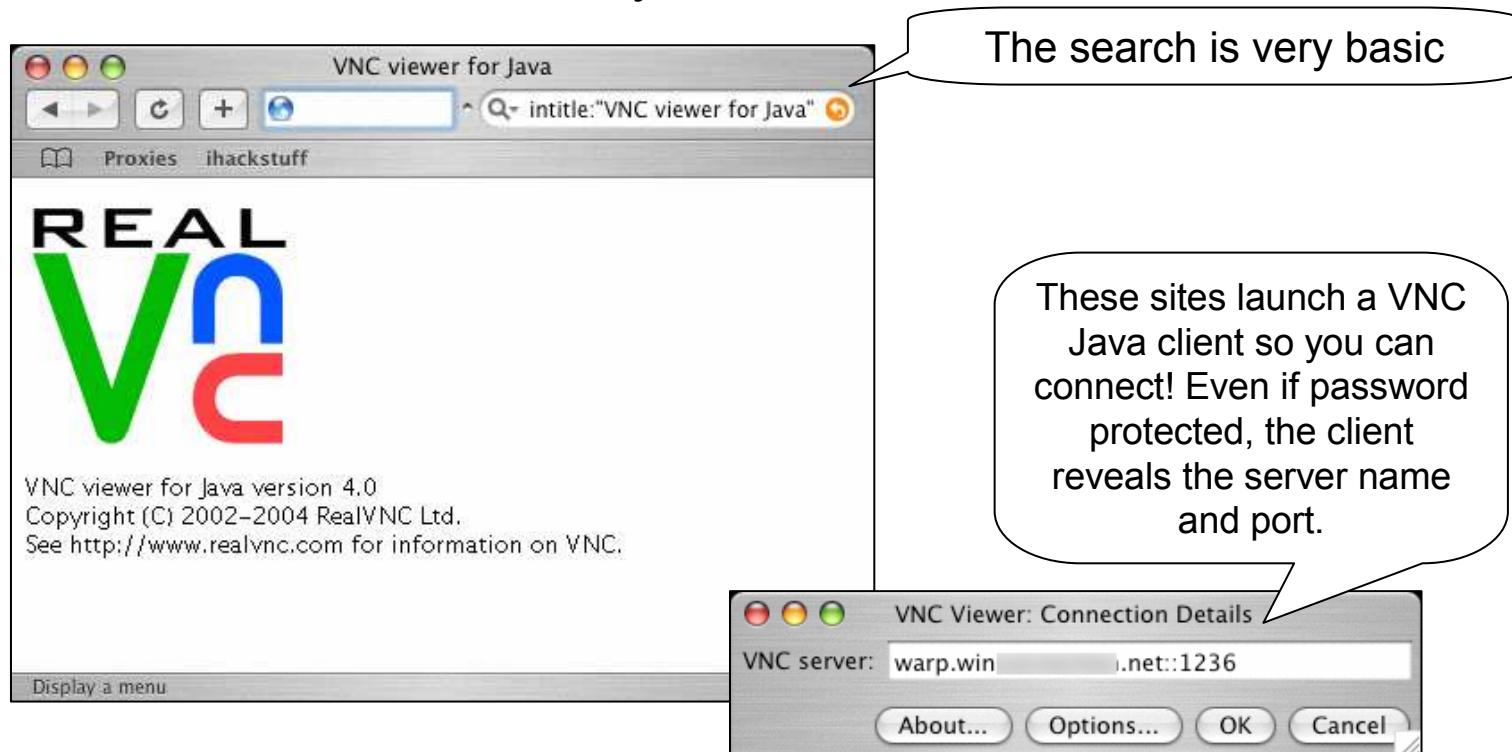
## Web File Browser

- This program allows directory walking, file uploading, and more.



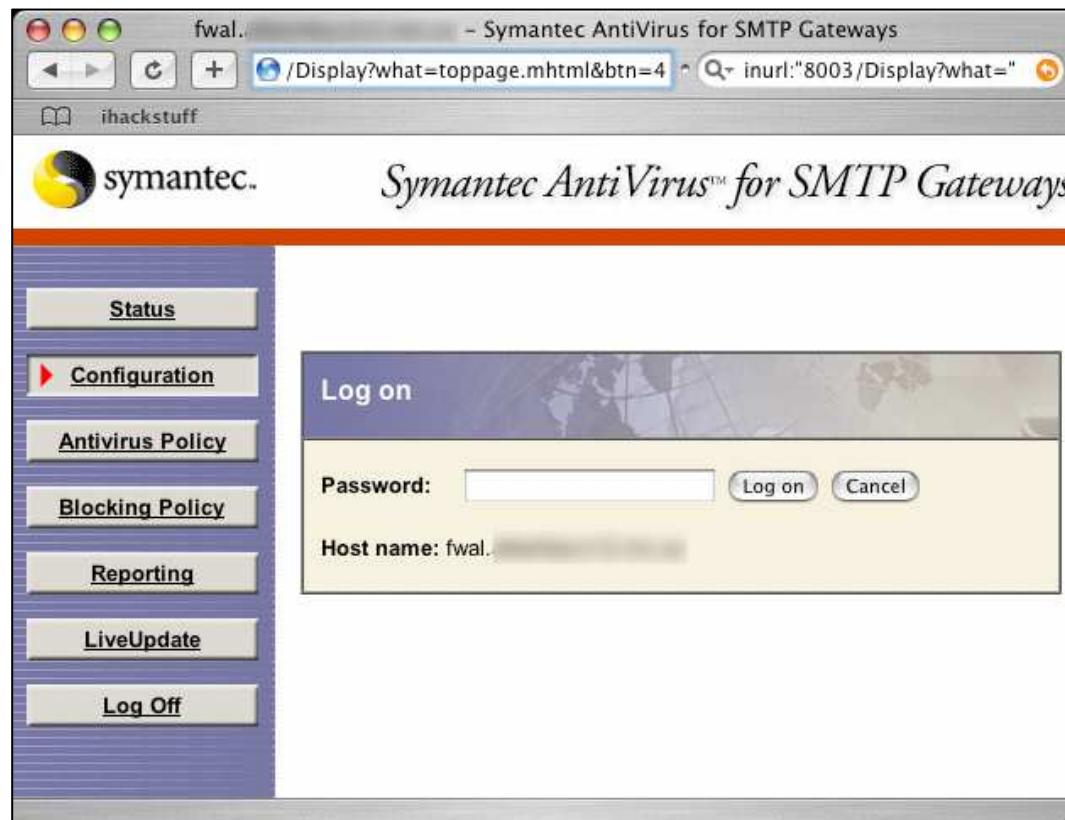
## VNC Servers (with client)

- VNC (Virtual Network Computing) allows you to control a workstation remotely.



Thanks to lester for  
this one!

# Symantec Anti-Virus SMTP Gateways



# Axis Print Servers

A screenshot of a web-based Network Print Server interface. The title bar says "Network Print Server". The search bar contains the query "[intitle:"Network Print Server" filetype:shtm](#)". Below the search bar are links for "Proxies" and "ihackstuff". The main content area has a yellow header "Printer Overview". On the left, a sidebar menu has "Printer Overview" selected. Other options in the menu are "Print Jobs" and "General Help". At the bottom of the sidebar are buttons for "user" and "admin", and a "USER GROUP" icon. The main content area shows a diagram of a network connection between "Ethernet" and a "Print Server" (represented by a printer icon). The "Print Server" is labeled "AXIS 540+/542+" and has an "LPT1" port. To the right of the diagram, the printer's details are listed: "Print Server Name: AXIS42AA7F", "System Location: 301A-EGRC", and "Serial Number: 00:40:8C:42:AA:7F". A "Configuration Wizard" button is at the bottom right of this section. A speech bubble in the top right corner says "Print server administration, Google-style!". A speech bubble in the bottom right corner says "Thanks to murfie for this one!".

Print server administration, Google-style!

Thanks to murfie for this one!

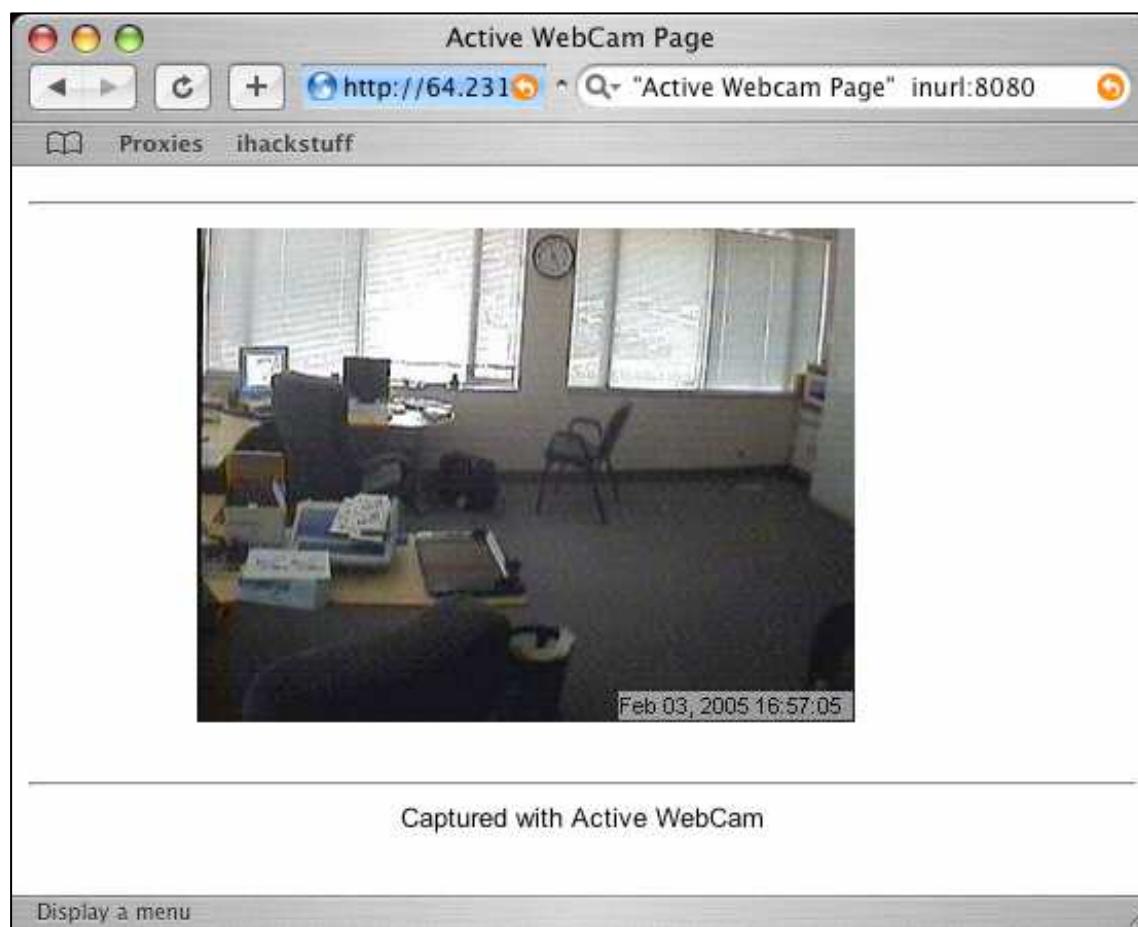
# Xenix, Sweex, Orite Web Cams



One query,  
many  
brands of  
live cams!

Thanks to  
server1 for  
this one!

# Active WebCam



Thanks  
klouw!

---

## Toshiba Network Cameras



intitle:"toshiba  
network camera -  
User Login"

Found by  
WarriorClown!

## Speedstream DSL Routers

- Home broadband connectivity... Googled.

The screenshot shows a web browser window titled "SpeedStream Router Management Interface". The URL bar contains "intitle:"SpeedStream Router Management Interface"" followed by a search icon. The page itself has a yellow header with the "SpeedStream" logo and the "Efficient NETWORKS" logo. A sidebar on the left lists "5100", "Home", "Login", "Status and Statistics", and "Reboot". The main content area displays "System Summary" with the following information:  
System Type: SpeedStream 5100-Series  
Config Part #: 003-6145-505  
Firmware Part #: 004-E141-A1Z  
MAC Address: 00:0B:23:0A:DF:6D

A speech bubble points to the "Disconnect" button for a connection entry:

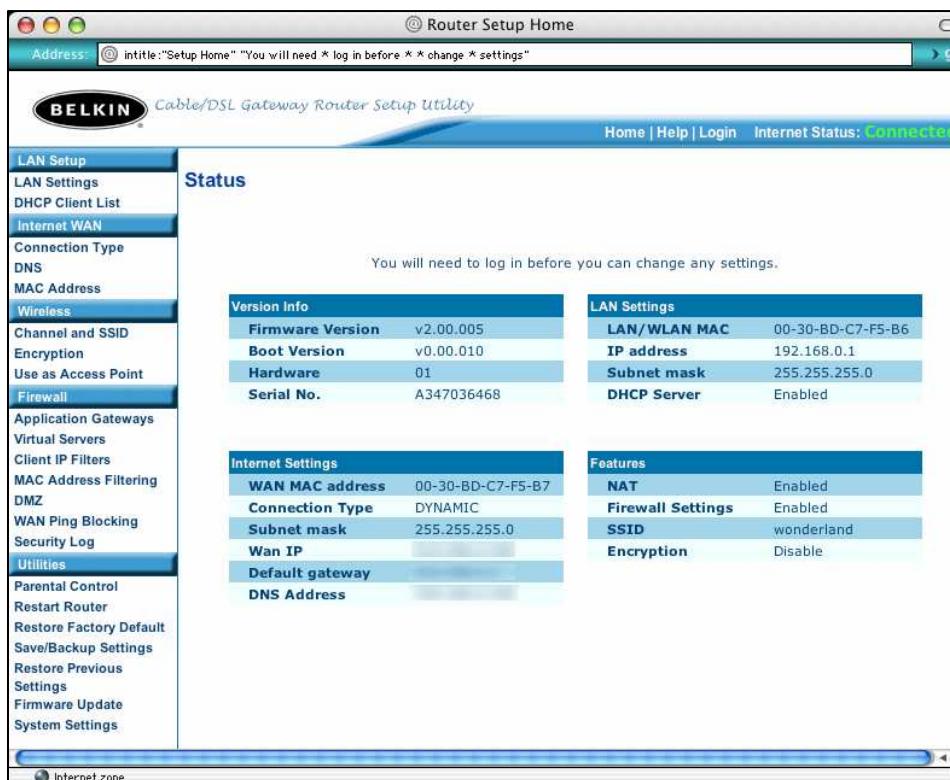
Who do you want to disconnect today?

Point to Point Connection Summary:  
PPPoA(0) 80.53.144.169 Disconnect

Found by m00d!

# Belkin Routers

- Belkin routers have become a household name in connected households. The management interface shouldn't show up on Google... but it does.



Thanks to  
darksun for  
this one!



## Printers

- Trolling printers through Google can be fun, especially when you can see and download what others are printing...

Web Image Monitor

inurl:webArch/mainFrame.cgi

Proxies ihackstuff

RICOH Aficio 2027

Printer Job History

Display items : 20

Total jobs : 20

ID	User Name	User ID	Document Name	Prints	Started At	Pages
77	---	?	Microsoft Word - Recent Religion Work.doc	Print Complete	Jan 31, 2005 2:05:56 PM	
76	---	?	Microsoft Word - JC Lectures.doc	Print Complete	Jan 31, 2005 11:59:57	
75	---	?	Microsoft Word - JC Lectures.doc	Print Complete	Jan 30, 2005 11:16:48	
74	---	?	Microsoft Word - Document6	Print Complete	Jan 26, 2005 3:11:20 PM	
73	---	?	Microsoft Word - Document6	Print Complete	Jan 26, 2005 3:11:13 PM	
72	---	?	Microsoft Word - JC Lectures.doc	Print Complete	Jan 26, 2005 11:22:23 PM	
71	---	?	http://www.123clicks.com/galleries/malika.mspg /aphrodisia	Print Complete	Jan 26, 2005 11:48:44 AM	
70	---	?	http://www.123clicks.com/galleries/malika.mspg /aphrodisia	Print Complete	Jan 26, 2005 11:48:09 AM	
69	---	?	C:\Documents and Settings\Relig.PDF	Print Complete	Jan 26, 2005 10:44:01 AM	
68	---	?	Microsoft Word - JC Lectures.doc	Print Complete	Jan 25, 2005 4:19:29 PM	

Religion...

And aphrodisiacs?  
Hrmmm...

Thanks  
JimmyNeutron!

# Firewalls - Smoothwall

A screenshot of a web browser window titled "Main page - SmoothWall Express". The URL in the address bar is <https://212.226.171.43:441/cgi-bin/>. The search bar contains the query "intitle:Smoothwall Express inurl:cgi-bin "up \* days"". The browser's back button is visible.

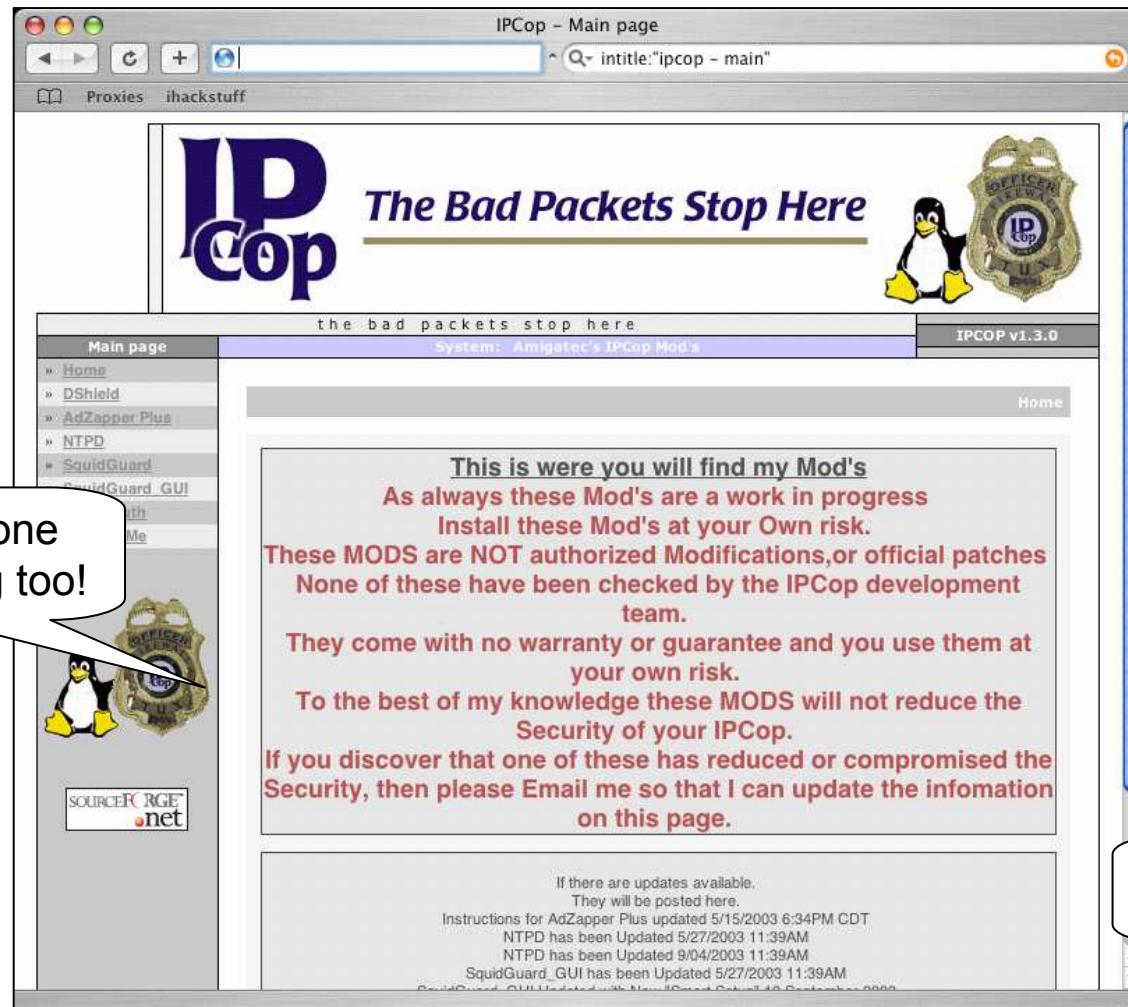
The SmoothWall Express 2.0 interface features a yellow header bar with tabs for "control", "about your smoothie", "services", "networking", "vpn", "logs", "tools", and "maintenance". Below the header are links for "home" and "credits", and buttons for "shutdown" and "help".

The main content area displays a welcome message: "Welcome to SmoothWall Express 2.0. This is your gateway to configuring and administering your SmoothWall firewall. Please make sure you read the Administration Guide before reconfiguring your SmoothWall — the guide is available with our other documentation from our website." A "BrandNew!" badge is visible on the left.

A large yellow box in the center contains a 3D cube icon and a "Refresh" button. A red exclamation mark icon points to a message at the bottom of the box: "Your update file is 13d 6h 50m 43s old. We recommend you update it on the 'Updates' page."

At the bottom of the page, there is footer information: "1:16am up 41 days, 2:21, 0 users, load average: 0.04, 0.01, 0.00". Logos for "SmoothWall.net", "U.S.Robotics", and "FUJITSU" are shown, along with the text "Produced in association with". The footer also includes "express 2.0 p5 ui-3.6.1" and "SmoothWall™ is a trademark of SmoothWall Limited." On the right side, there is a copyright notice: "© 2000 - 2003 The SmoothWall Team". A speech bubble on the left says "Uh oh... this firewall needs updating..." and a speech bubble on the right says "Thanks Milkman!".

# Firewalls - IPCop



# IDS Data: ACID

- SNORT IDS data delivered graphically, served up fresh

The screenshot illustrates the integration of search results and real-time monitoring. On the left, a Google search results page for 'ACID "by Roman Danyliw" filetype:php' is shown, listing various ACID-related pages. On the right, a separate window titled 'ACID: Query Results: 15 Last Alerts' displays a list of 15 recent alerts. A callout bubble highlights the search query from the search results page.

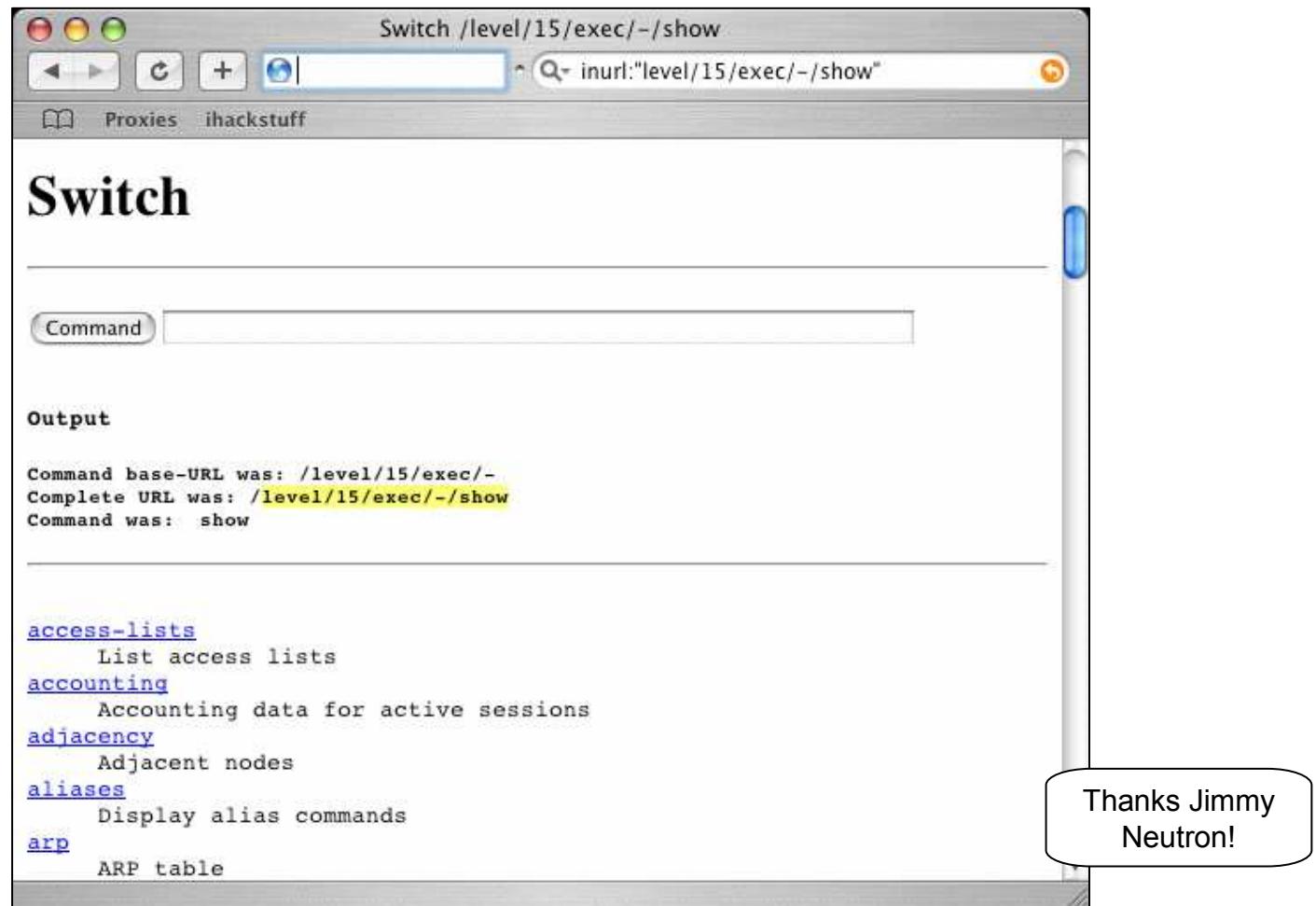
**ACID "by Roman Danyliw" filetype:php**

Google Search: ACID "by Roman Danyliw" filetype:php  
http://www.google.com/search?num=100&hl=en&lr=&ie=UTF-8&safe=c

**ACID: Query Results: 15 Last Alerts**

#	Alert Description	Date	Time	IP Address
1	[snort] (http_inspect) IIS UNICODE (1- CODEPOINT ENCODING)	2004-07-20	13:47:42	76637
2	[snort] (http_inspect) IIS UNICODE (1- CODEPOINT ENCODING)	2004-07-20	13:47:42	76636
3	[snort] (http_inspect) IIS UNICODE (1- CODEPOINT ENCODING)	2004-07-20	13:47:42	218.163.74.20:1235 76635
4	[snort] (http_inspect) IIS UNICODE (1- CODEPOINT ENCODING)	2004-07-20	13:47:42	218.163.74.20:1236 76634
5	[snort] (http_inspect) IIS UNICODE (1- CODEPOINT ENCODING)	2004-07-20	13:47:42	218.163.74.20:1235 76633
6	[snort] (http_inspect) IIS UNICODE (1- CODEPOINT ENCODING)	2004-07-20	13:47:42	218.163.74.20:1236 76632
7	[snort] (http_inspect) IIS UNICODE (1- CODEPOINT ENCODING)	2004-07-20	13:47:42	218.163.74.20:1236 76631
8	[snort] (http_inspect) IIS UNICODE	2004-07-20		

# Open Cisco Devices



# Cisco Switches

The screenshot shows a web browser window titled "Switch Home Page". The address bar contains the URL <http://64.233.161.104/search>. The search query in the search bar is "intitle:"switch home page" "cisco systems" "Telnet - to)". Below the search results, the first item is a link to "Cisco Systems". The page content for this link includes the title "Cisco Systems" and the heading "Accessing Cisco WS-C3550-48 "Switch"". It lists several management options: "Web Console" (underlined), "Telnet" (underlined), "Show interfaces" (underlined), "Show diagnostic log" (underlined), "Monitor the router" (underlined), "Extended Ping" (underlined), and "Show tech-support" (underlined). A horizontal line separates this content from a "Help resources" section at the bottom. In the bottom right corner of the browser window, there is a speech bubble containing the text "Thanks Jimmy Neutron!".

Switch Home Page

http://64.233.161.104/search intitle:"switch home page" "cisco systems" "Telnet - to"

Cisco Systems

Accessing Cisco WS-C3550-48 "Switch"

[Web Console](#) - Manage the Switch through the web interface.

[Telnet](#) - to the router.

[Show interfaces](#) - display the status of the interfaces.

[Show diagnostic log](#) - display the diagnostic log.

[Monitor the router](#) - HTML access to the command line interface at level [0](#), [1](#), [2](#), [3](#), [4](#), [5](#), [6](#), [7](#), [8](#), [9](#), [10](#), [11](#), [12](#), [13](#), [14](#), [15](#)

Connectivity test - unavailable, no valid nameserverdefined.

[Extended Ping](#) - Send extended ping commands.

[Show tech-support](#) - display information commonly needed by tech support.

Help resources

Thanks Jimmy Neutron!

## Wide Open PHP Nuke Sites

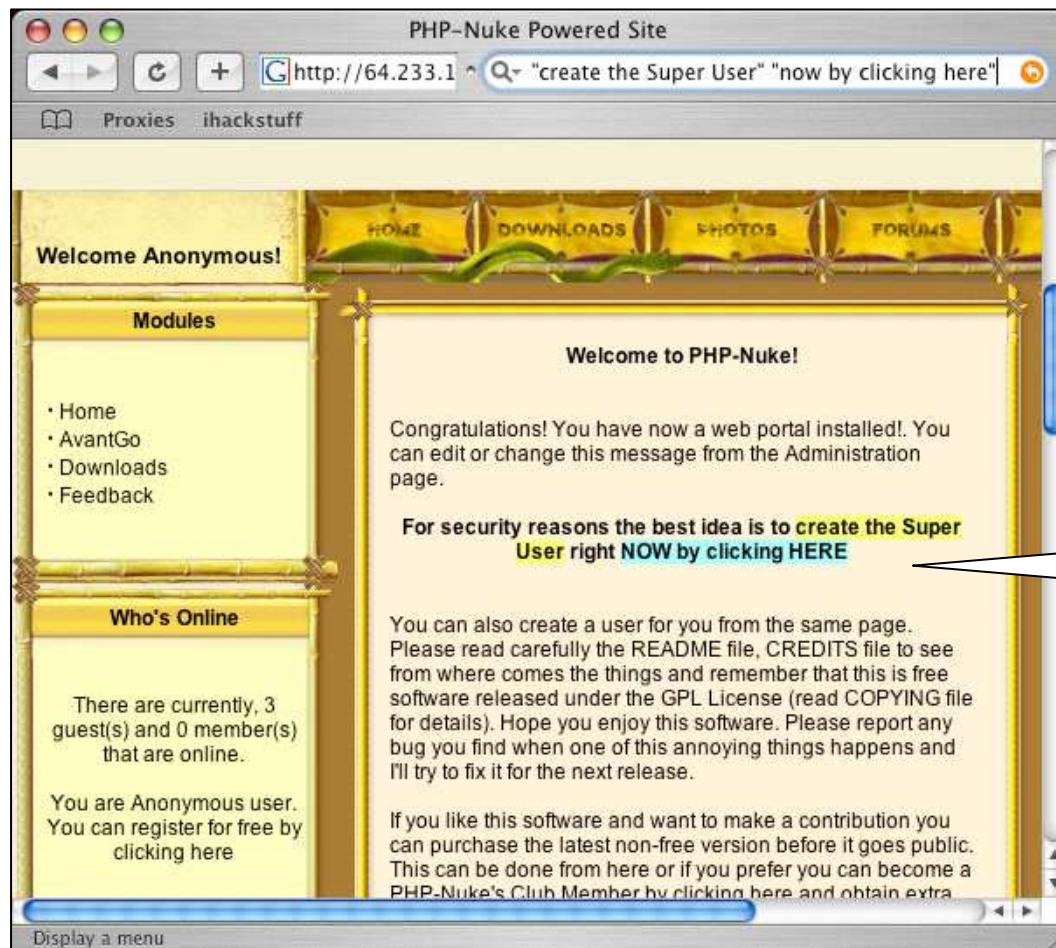
- PHP Nuke allows for the creation of a full-featured web site with little effort.



Too lazy to install  
PHP Nuke? Own  
someone else's site  
instead!

Thanks to  
arrested for  
this beauty!

# Open PHP Nuke... another way...



Click here,  
create  
superuser!

## Security Cameras

- Although many cameras are multi-purpose, certain brands tend to be used more for security work.



# Security Cameras



## Time-lapse video recorders

- A staple of any decent security system, these camera control units have gotten high-tech.. And Googable...

The search is no big deal...

Then there's the pesky login box...

Google Search: intitle:"everfocus edsr applet"  
http://www.google.com/search?q=intitle%22+intitle:"everfocus+edsr+applet%"

Proxies ihackstuff

Web Images Groups New! News Froogle more » Advanced Search Preferences

intitle:"everfocus edsr applet"

Search

Results 1 - 10 of about 18 for intitle:"everfocus edsr applet". (0.24 sec)

[EverFocus EDSR Applet \(1.3\)](#)  
/ - 1k - Cached - Similar pages

[EverFocus EDSR Applet \(1.3\)](#)  
/ - 1k - Cached - Similar pages

[EverFocus EDSR Applet \(1.2\)](#)  
/ - 1k - Cached - Similar pages

[EverFocus EDSR Applet \(1.2\)](#)  
/ - 1k - Cached - Similar pages

[EverFocus EDSR Applet \(1.2\)](#)  
- 1k - Cached - Similar pages

Sponsored Links

[Everfocus products](#)  
Cameras, DVRs accessories  
Inexpensive quality  
cu1.com

[Applet Downloads](#)  
Professional Applet Downloads  
for your web pages.  
www.jpowered.com

Login

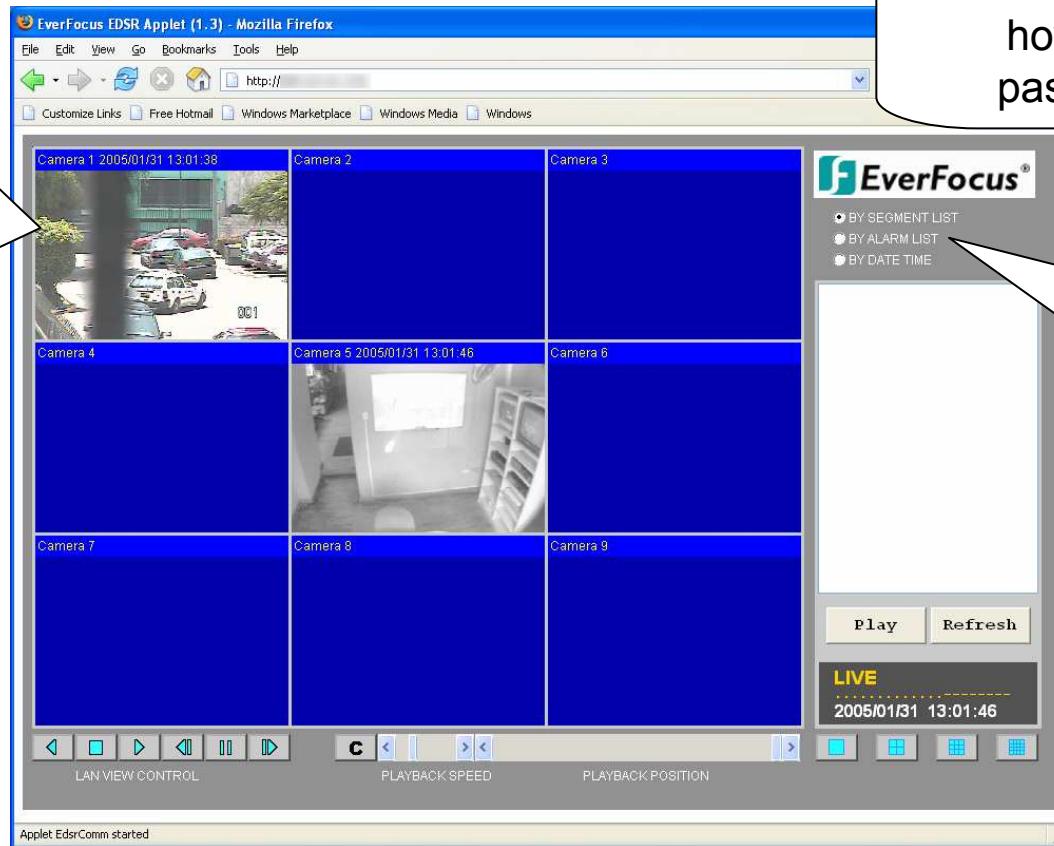
User

Password

Submit

Best View Quality: IE5, 1024x768

# Time lapse video recorders



...multiple  
live security  
camera  
views...

Even doofus hackers know  
how to use default  
passwords to get...

...and historical  
records of  
recorded video  
feeds

Thanks to  
stonersavant  
for this beauty!

# UPS Monitors

Getting personal with Power System monitors...

The screenshot shows a web browser window titled "Tue Feb 01 23:37:19 WEST 2005 on tibs:3551". The URL bar contains "ihackstuff" and a search term "intitle:"Multimon UPS status page"". The main content area displays monitoring information for a SMART-UPS 1000 unit. It includes:

- Battery Capacity:** 100% (green bar)
- Run Time Remaining:** 112.0 mins (black bar)
- UPS Load:** 11.4 % (red bar)

Other details shown include:

- Monitoring: Tibs
- UPS Model: SMART-UPS 1000
- UPS Name: UPS\_IDEN
- APCUPSD: Version 3.10.16
- Status: ONLINE
- Last UPS Self Test: NO
- Last Test Date: Not found
- Utility Voltage: 230.1 VAC
- Line Minimum: 227.5 VAC
- Line Maximum: 232.7 VAC
- Output Freq: 50.0 Hz
- UPS Temp: 32.8 °C

Most recent events log:

- Thu Nov 13 12:37:04 WEST 2003 apcupsd shutdown succeeded
- Thu Nov 13 12:37:04 WEST 2003 apcupsd exiting, signal 2
- Thu Nov 13 12:36:41 WEST 2003 apcupsd 3.10.7 (08 November 2003) cygwin startup succeeded
- Mon Oct 27 09:00:31 WEST 2003 apcupsd 3.10.6 (10 October 2003) cygwin startup succeeded
- Mon Oct 27 08:59:13 WEST 2003 apcupsd 3.10.6 (10 October 2003) cygwin startup succeeded

Thanks  
yeseins!

# UPS Monitors

Oh wait.. Wrong kind of  
UPS...this is package  
tracking hacking... =P

Google Search: site:ups.com intitle:"Ups Pack... tracking" intext:"1Z ##### # ##### # ##### #"

http://www. ihackstuff

Proxies ihackstuff

Web Images Groups News Froogle more x Advanced Search Preferences

site:ups.com intitle:"Ups Package tracking" intext:"1Z ##### # ##### # ##### #". (0.12 seconds)

**UPS Package Tracking**  
... Tracking Number. Unable to track shipment "1Z 159 922 03 4217 324 6". UPS could not locate the shipment details for your request. Please ...  
[wwwapps.ups.com/etracking/tracking.cgi?tracknum=1Z1599220342173246](http://wwwapps.ups.com/etracking/tracking.cgi?tracknum=1Z1599220342173246) - 22k - Cached - Similar pages

**UPS Package Tracking**  
... Tracking Number. Status. Delivery Information. 1. 1Z A17 53V 03 6432 655 2. Delivered.  
Delivered on: Dec 7, 2004 7:04 PM. Delivered to: CUMBERLAND, RI, US. ...  
[wwwapps.ups.com/etracking/tracking.cgi?&TypeOfInquiryNumber=T&HTMLVersion=4.0&InquiryNumber1=...](http://wwwapps.ups.com/etracking/tracking.cgi?&TypeOfInquiryNumber=T&HTMLVersion=4.0&InquiryNumber1=...) - 29k - Cached - Similar pages

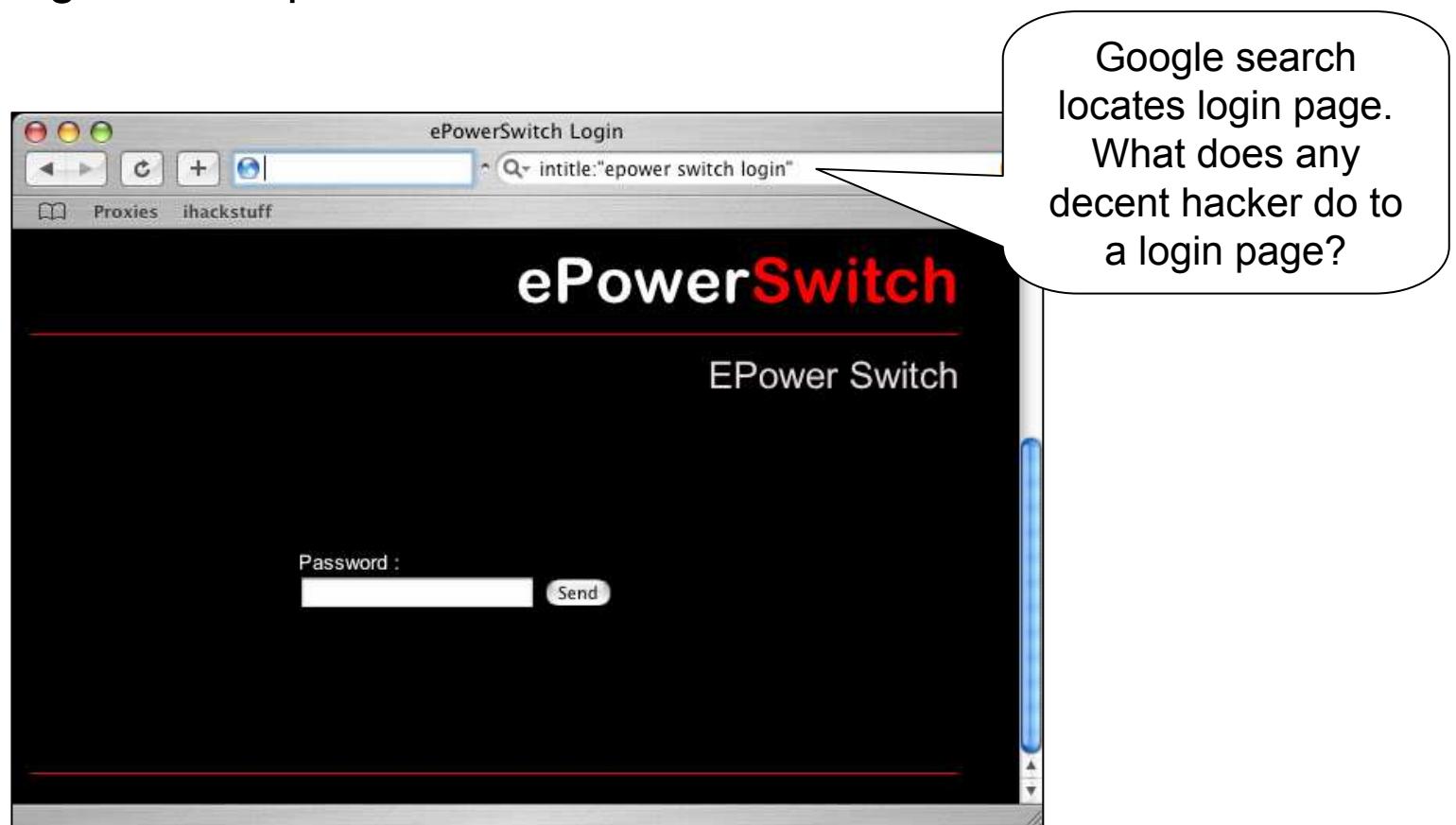
**UPS Package Tracking**  
... Tracking Number. Status. Delivery Information. 1. 1Z X77 386 03 5395 335 8. Delivered.  
Delivered on: Aug 4, 2004 3:39 PM. Delivered to: ODESSA, TX, US. ...  
[wwwapps.ups.com/etracking/tracking.cgi?&TypeOfInquiryNumber=T&HTMLVersion=4.0&InquiryNumber1=...](http://wwwapps.ups.com/etracking/tracking.cgi?&TypeOfInquiryNumber=T&HTMLVersion=4.0&InquiryNumber1=...) - 29k - Cached - Similar pages

**UPS Package Tracking**  
... Detail" link. Tracking Number. Status. Delivery Information. 1. 1Z V8V 384 03  
4290 853 2. Exception. Service Type: GROUND. Tracking results ...  
[wwwapps.ups.com/etracking/tracking.cgi?&TypeOfInquiryNumber=T&HTMLVersion=4.0&InquiryNumber1=...](http://wwwapps.ups.com/etracking/tracking.cgi?&TypeOfInquiryNumber=T&HTMLVersion=4.0&InquiryNumber1=...) - 28k - Cached - S

Thanks Digital Spirit!

## Hacking POWER Systems!

- Ain't technology grand? This product allows web management of power outlets!



# Hacking Power Systems!

The screenshot shows a Mozilla Firefox browser window displaying the ePowerSwitch 8 web interface. The title bar reads "ePowerSwitch 8". The main content area has tabs for "Device 1", "Device 2", "Device 3", "Device 4", and "Device 5". The "Device 1" tab is active, showing a list of power outlets labeled "Socket 1-1" through "Socket 1-8". Each outlet has an "ON" status indicator and two buttons: "Power" and "Restart". To the right of the outlets, the text "ePowerSwitch M8 (Master)" is displayed. A speech bubble on the left asks "Who do you want to power off today?", pointing to the "Power" button of the first outlet. A speech bubble on the right thanks "JimmyNeutron for this beauty!".

Who do you want to power off today?

ePowerSwitch M8 (Master)

Socket	Power	Restart	
1-1	ON	[Power]	[Restart]
1-2	ON	[Power]	[Restart]
1-3	ON	[Power]	[Restart]
1-4	ON	[Power]	[Restart]
1-5	ON	[Power]	[Restart]
1-6	ON	[Power]	[Restart]
1-7	ON	[Power]	[Restart]
1-8	ON	[Power]	[Restart]

Thanks to JimmyNeutron for this beauty!

---

## Google Phreaking

- Question... Which is easier to hack with a web browser?

A: Sipura SPA  
2000 IP  
Telephone

B: Vintage  
1970's Rotary  
Phone

QuickTime™ and a  
TIFF (Uncompressed) decompressor  
are needed to see this picture.

QuickTime™ and a  
TIFF (Uncompressed) decompressor  
are needed to see this picture.

# Sipura SPA IP Telephone

The image shows two screenshots of the Sipura SPA Configuration software. The left screenshot displays the 'Info' tab with 'System Information' and 'Product Information'. The right screenshot shows the 'Line 1' tab with 'Line 1 Status' details.

**System Information**

DHCP:	Enabled	Current IP:	192.168.1.111
Host Name:	spa3000_vp	Domain:	gateway.zwire.net
Current Netmask:	255.255.0.0	Current Gateway:	172.16.0.1
Primary DNS:	66.234.228.150		
Secondary DNS:	66.234.228.151		

**Product Information**

Product Name:	SPA-3000	Serial N:	
Software Version:	2.0.10(GWc)	Hardwa:	
MAC Address:	000E08CAF0D2E	Client C:	

**System Status**

Current Time:	9/27/2004 10:53:34	Elapsed:	
Broadcast Pkts Sent:	6	Broadc:	
Broadcast Pkts Recv:	9873	Broadc:	
Broadcast Pkts Dropped:	0	Broadc:	
RTP Packets Sent:	303959	RTP By:	
RTP Packets Recv:	452249	RTP By:	
SIP Messages Sent:	6300	SIP By:	
SIP Messages Recv:	6310	SIP By:	
External IP:			

**Line 1 Status**

Hook State:	On	Registration State:	Registered
Last Registration At:	9/27/2004 10:16:05	Next Registration In:	1321 s
Message Waiting:	No	Call Back Active:	No
Last Called Number:	*123	Last Caller Number:	4 80 451
Mapped SIP Port:			
Call 1 State:	Idle	Call 2 State:	Idle
Call 1 Tone:	None	Call 2 Tone:	None
Call 1 Encoder:		Call 2 Encoder:	
Call 1 Decoder:		Call 2 Decoder:	
Call 1 FAX:		Call 2 FAX:	
Call 1 Type:		Call 2 Type:	
Call 1 Remote Hold:		Call 2 Remote Hold:	
Call 1 Callback:		Call 2 Callback:	
Call 1 Peer Name:		Call 2 Peer Name:	
Call 1 Peer Phone:		Call 2 Peer Phone:	
Call 1 Duration:		Call 2 Duration:	
Call 1 Packets Sent:		Call 2 Packets Sent:	

How about Googling for the last number your friend dialed?

Or the last number that dialed them?

Thanks stonersavant!!!

# Videoconferencing

A screenshot of a web browser window titled "TANDBERG: METROEXPRESS AAR". The address bar shows a search query: "intext:"Videoconference Management System" ext:htm". Below the address bar are links for "Bookmarks", "Proxies", and "ihackstuff". The main content area features a dark background with several icons: a blue globe, a green telephone handset, a red telephone handset with a red 'X' over it, and a yellow question mark icon. To the right of these icons is the word "TANDBERG" vertically oriented. On the left side, there is a sidebar with the text "Videoconference Management System on METROEXPRESS AAR" followed by a list of menu items. On the right side, there is a section titled "Our Vision" with a descriptive paragraph. A speech bubble on the left asks "Who do you want to disconnect today?", with an arrow pointing to the "Disconnect" menu item. A speech bubble on the right says "Thanks yeseins!!!".

Who do you want to disconnect today?

**Videoconference Management System on METROEXPRESS AAR**

- ▶ [Call Management](#)
- ▶ [Connect](#)
- ▶ [Disconnect](#)
- ▶ [Edit Directory](#)
- ▶ [Call Status](#)
- ▶ [MCU Services](#)
- ▶ [MCU Status](#)
- ▶ [Streaming](#)
- ▶ [Snapshots](#)
- ▶ [Text Chat](#)
- ▶ [System Configuration](#)

reliability • ease of use • quality • value

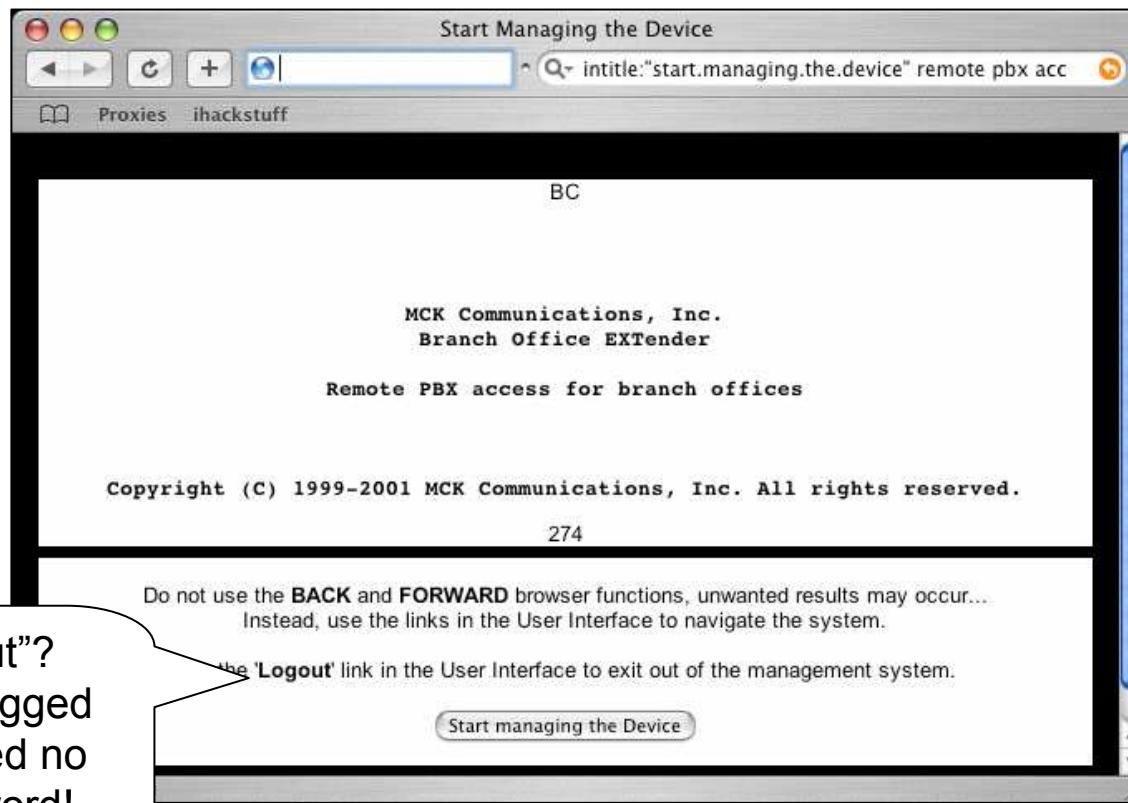
**Our Vision**

To provide innovative, high quality videoconferencing solutions that are reliable, easy to use and represent a significant value for our partners and customers.

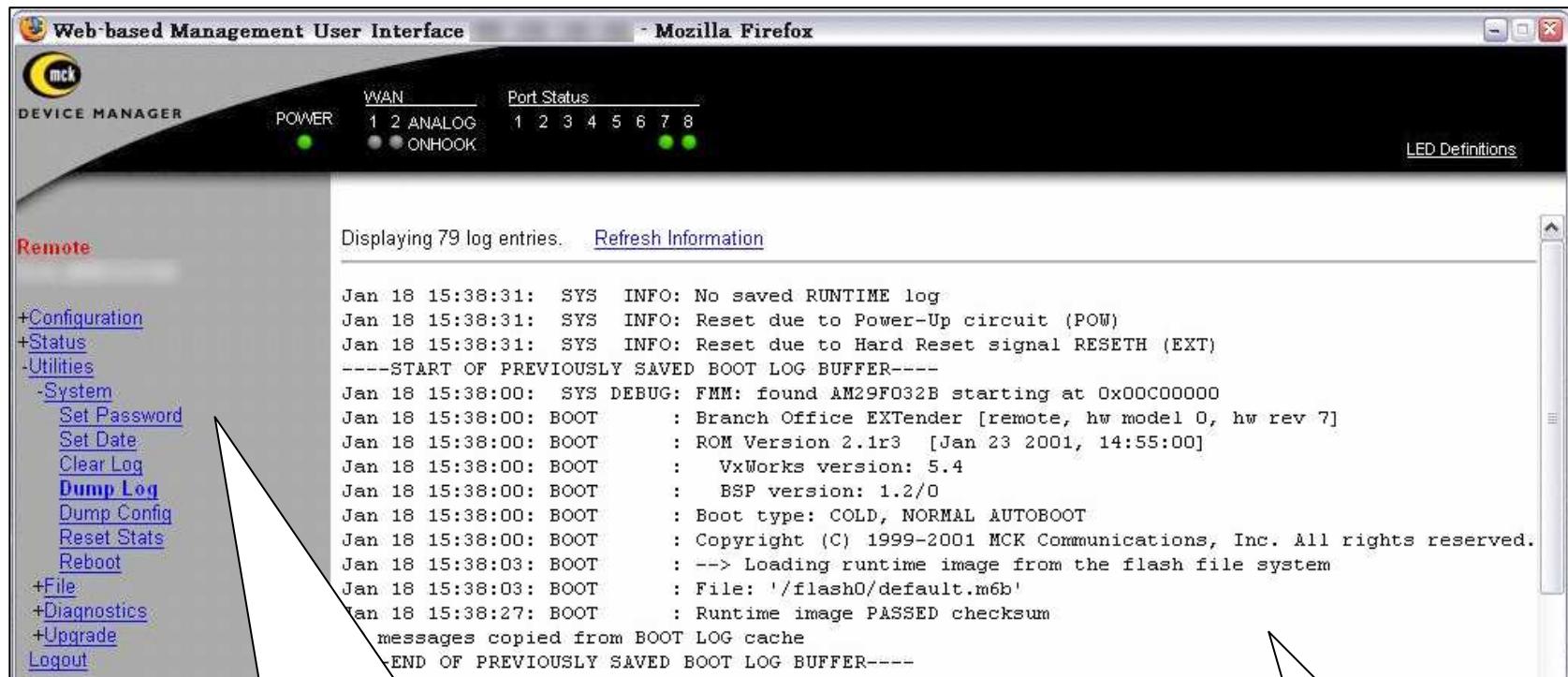
Thanks yeseins!!!

## PBX Systems

- Web-based management interfaces open the door for a creative Google Hacker.



# PBX Systems



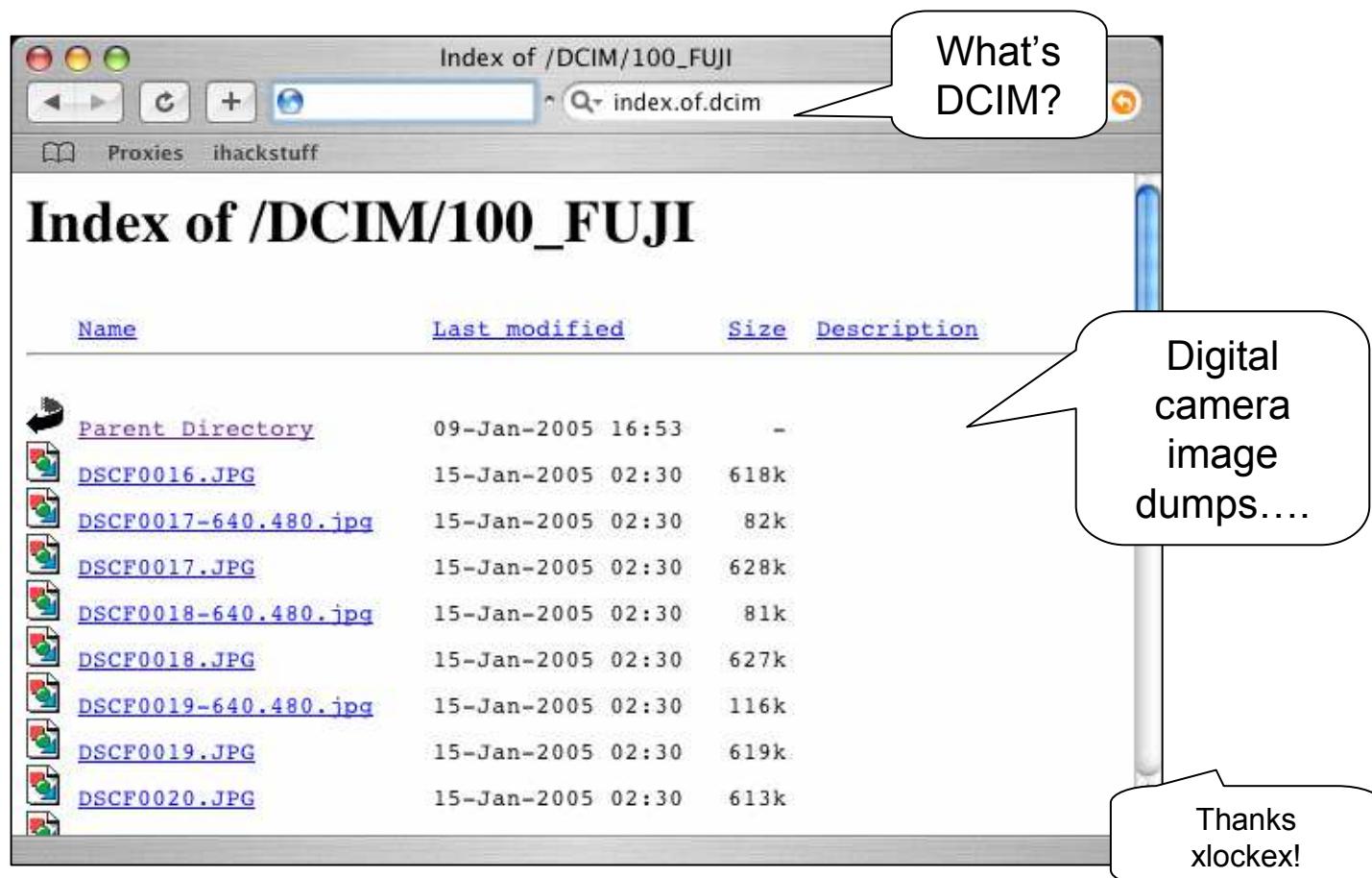
No password required.  
Even a novice web surfer  
can become a “PBX  
hacker”. =)

Thanks to  
stonersavant for this  
great find!

# Usernames, Passwords and Secret Stuff, oh my!

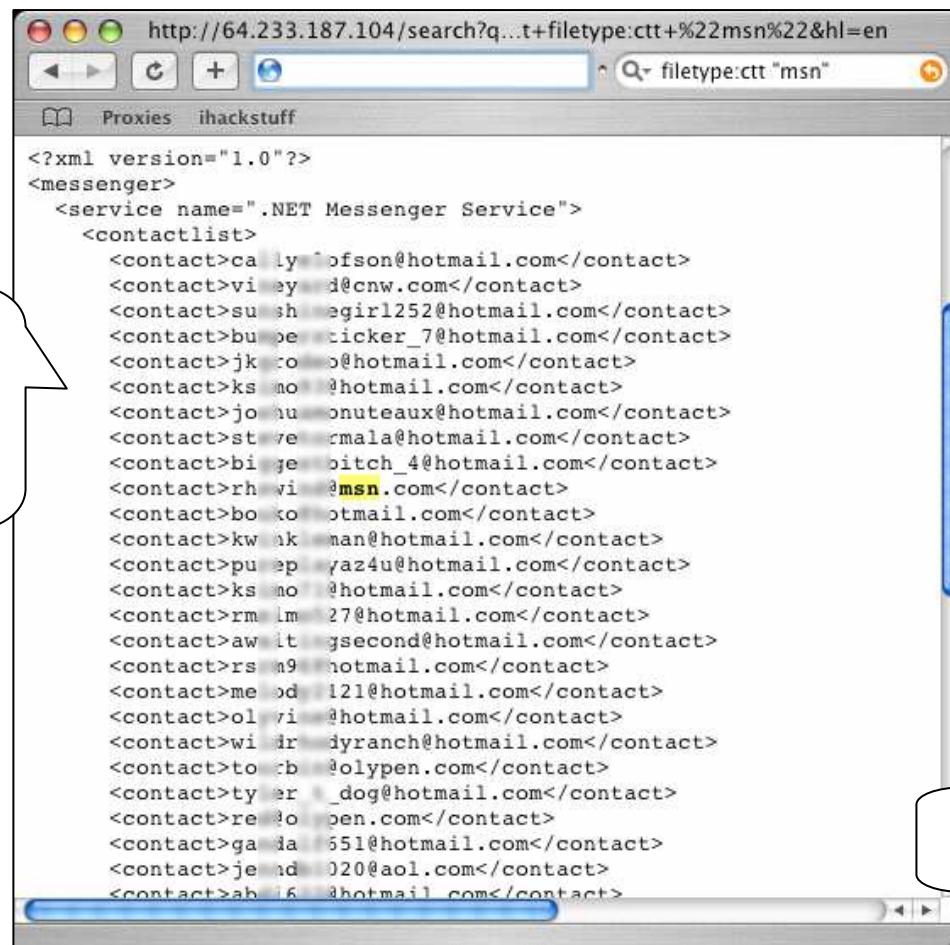
There's all sorts of stuff out there that people probably didn't mean to make public. Let's take a look at some examples...

# DCIM



# MSN Contact Lists

MSN contact lists allow an attacker to get 'personal'

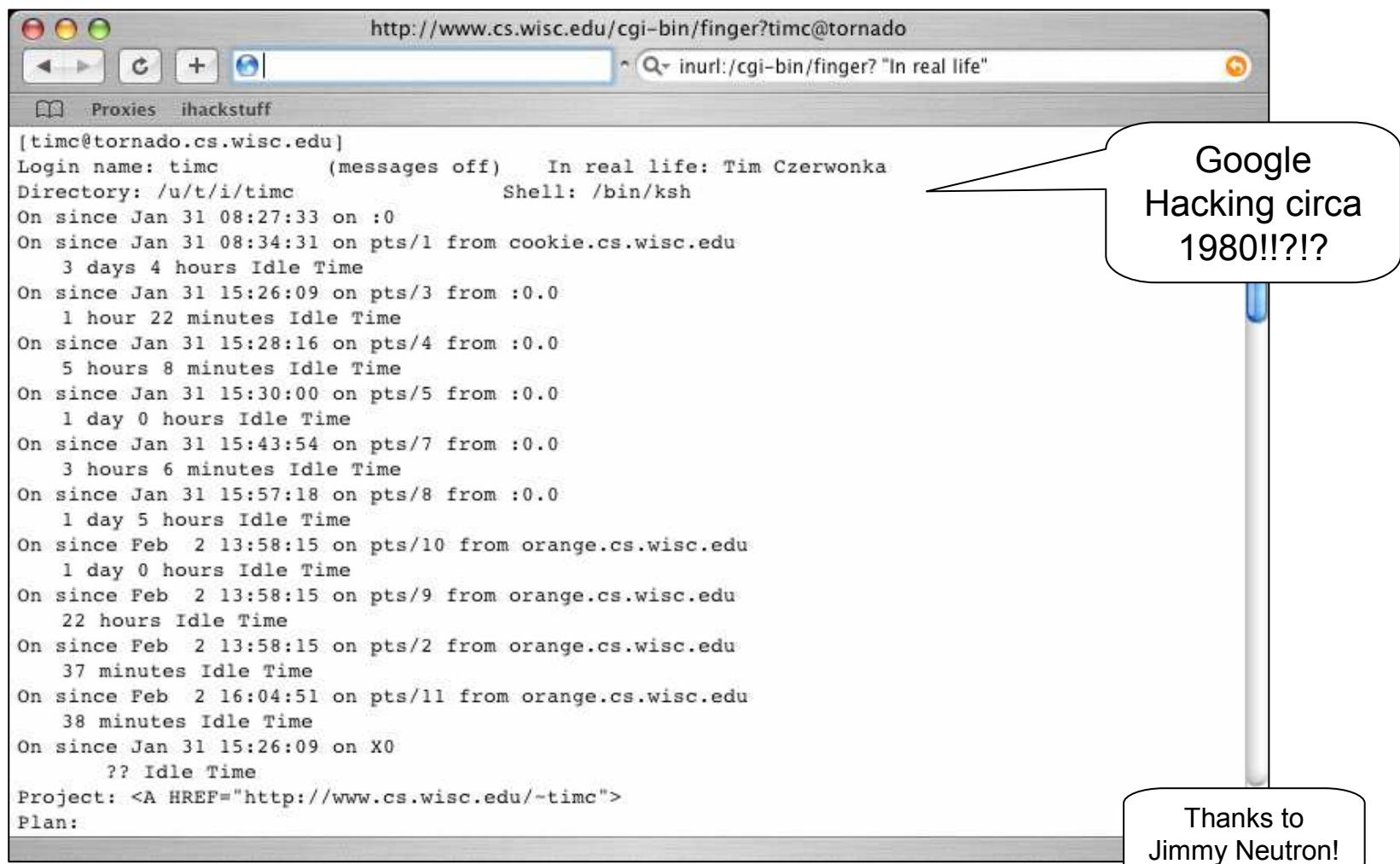


A screenshot of a web browser window displaying an XML document. The URL in the address bar is `http://64.233.187.104/search?q=t+filetype:ctt+%22msn%22&hl=en`. The search query in the search bar is `filetype:ctt "msn"`. The XML content is as follows:

```
<?xml version="1.0"?>
<messenger>
  <service name=".NET Messenger Service">
    <contactlist>
      <contact>ca ly bofson@hotmail.com</contact>
      <contact>vi ey d@cnw.com</contact>
      <contact>su sh egirl1252@hotmail.com</contact>
      <contact>bu be ticker_7@hotmail.com</contact>
      <contact>jk ro o@hotmail.com</contact>
      <contact>ks mo n@hotmail.com</contact>
      <contact>jo hu onuteaux@hotmail.com</contact>
      <contact>st ve rmaila@hotmail.com</contact>
      <contact>bi je bitch_4@hotmail.com</contact>
      <contact>rh vi @msn.com</contact>
      <contact>bo ro otmail.com</contact>
      <contact>kw nk han@hotmail.com</contact>
      <contact>pu ep yaz4u@hotmail.com</contact>
      <contact>ks mo @hotmail.com</contact>
      <contact>rm lm 27@hotmail.com</contact>
      <contact>aw it gsecond@hotmail.com</contact>
      <contact>rs n9 hotmail.com</contact>
      <contact>me od 121@hotmail.com</contact>
      <contact>ol ri @hotmail.com</contact>
      <contact>wi ir dyrranch@hotmail.com</contact>
      <contact>to ob @olypen.com</contact>
      <contact>ty er _dog@hotmail.com</contact>
      <contact>re bo pen.com</contact>
      <contact>ga ia 651@hotmail.com</contact>
      <contact>je id 020@aol.com</contact>
      <contact>ah 16 @hotmail.com</contact>
```

Thanks to  
harry-aac!

## Old School! Finger...



# Norton AntiVirus Corporate Passwords

The screenshot shows a Google search results page with the query "inurl:'GRC.DAT' intext:'password'" entered into the search bar. The results are filtered under the "Web" category, showing 5 results. Each result is a URL containing a password hash preceded by "[KEYS] !KEY!=\$REGROOT\$". The results are from various sources, including Snav, Ssoftzone, Spc002.w2.bo.infn.it, and a Norton AntiVirus support forum. A speech bubble on the right side of the screen says "Encrypted, but yummy (and crackable)!". Another speech bubble at the bottom right says "Thanks MILKMAN!".

Google Search: inurl:"GRC.DAT" intext:"password"

http://www. Google

Proxies ihackstuff

Web Images Groups New! News Froogle more »

inurl:"GRC.DAT" intext:"password" Search Advanced Search Preferences

**Web** Results 1 - 5 of 5 for inurl:"GRC.DAT" intext:"password". (0.11 seconds)

Tip: Try removing quotes from your search to get more results.

[KEYS] !KEY!=\$REGROOT\$ LicenseNumber=S00141V-11CQ-1112 Connected ...  
... D1 Description=Snav Location=S IPAddress=S10.1.2.110 Subnet=D0 SubnetMask=D0  
Type=D2 Login=Scd **Password**=S105F3CD589B39EBDF8120110348 PasswordIsEncrypted=D1 ! ...  
www. edu/updates/GRC.DAT - 10k - Cached - Similar pages

[KEYS] !KEY!=\$REGROOT\$ FullGRCUpdateCounter=D1 LicenseNumber ...  
... D1 UpdateNow=D1 SourceCount=D1 Description=S Location=S IPAddress=S Subnet=D0  
SubnetMask=D0 Type=D0 Login=S **Password**=S0004F627A3B PasswordIsEncrypted=D1 !KEY ...  
Iss. www. edu/~sara/GRC.DAT - 8k - Cached - Similar pages

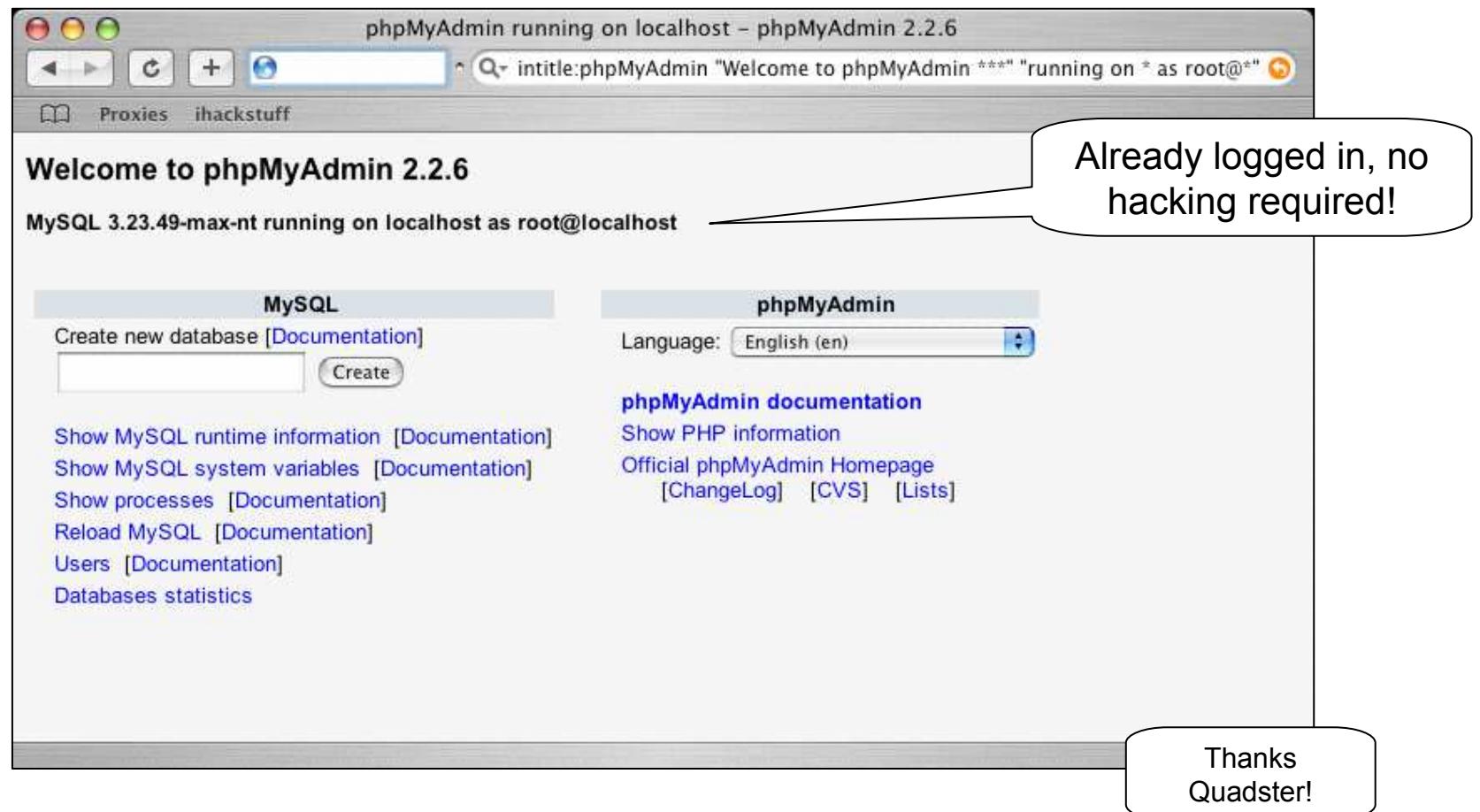
[KEYS] !KEY!=\$REGROOT\$ FullGRCUpdateCounter=D1 LicenseNumber ...  
... 492000=D0 !KEY!=\$REGROOT\$\\LiveUpdateSource Description=Ssoftzone Location=S  
IPAddress=S\\Softzone\\Site-open\\Navupdt! **Password**=S0004F627A3B PasswordIsEncrypted ...  
www. www. ch/services/ pcsupport/anleitungen/virus/GRC.DAT - 7k - Cached - Similar pages

[KEYS] !KEY!=\$REGROOT\$ FullGRCUpdateCounter=D1 LicenseNumber ...  
... Description=S Location=S IPAddress=Spc002.w2.bo.infn.it **Password**=  
S3118D39BF29E8897D0E0A8A62A16DA73353C31CC83A219A04A456222464 PasswordIsEncrypted= ...  
www. www. it/calcolo/helpdesk/antivirus/GRC.DAT - 5k - Cached - Similar pages

Encrypted, but  
yummy (and  
crackable)!

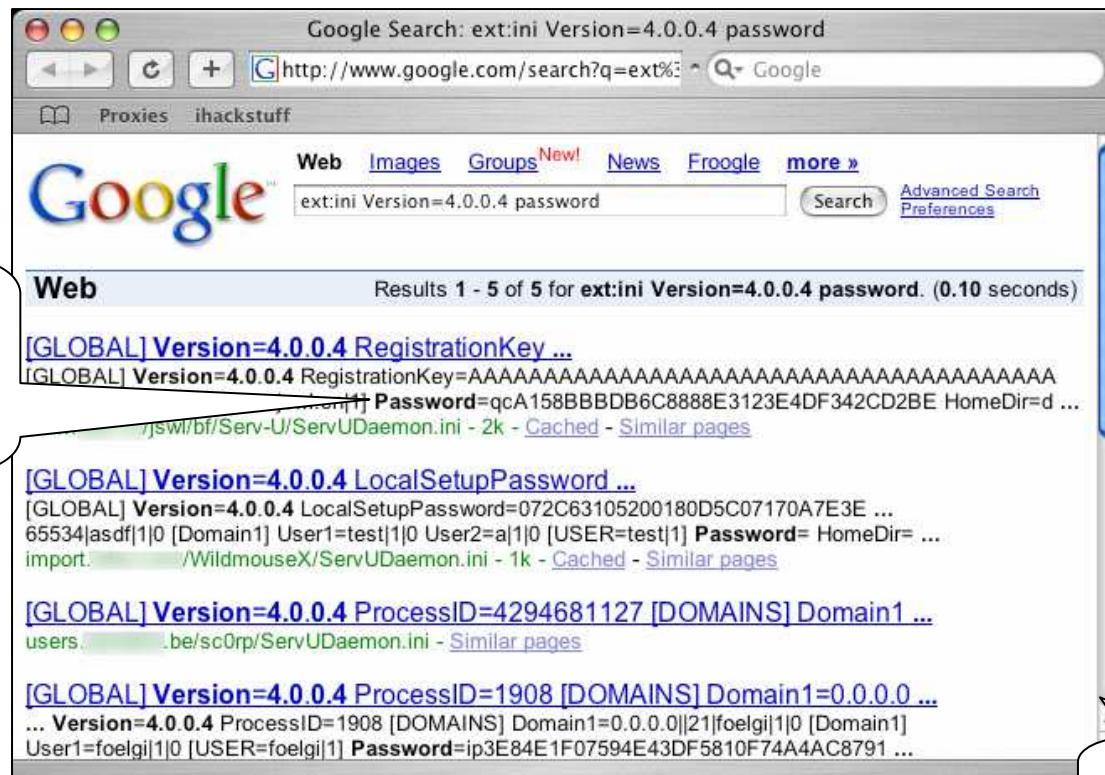
Thanks  
MILKMAN!

# Open SQL servers



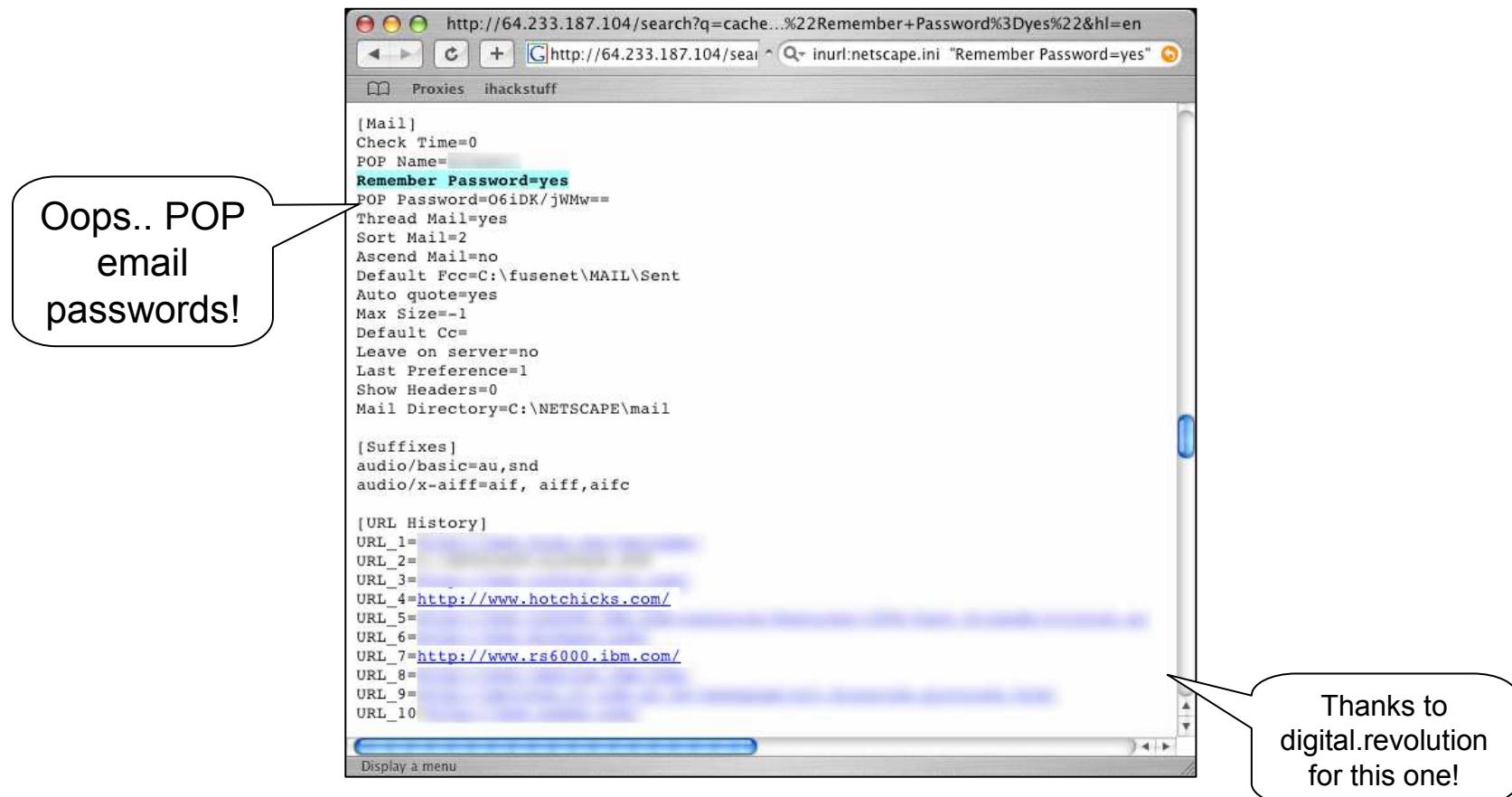
# ServU FTP Passwords

ServU FTP  
Daemon  
passwords, super  
encrypto! =P



Thanks to  
vs1400 for this  
one!

# Netscape History Files



# IPSec Final Encryption Keys

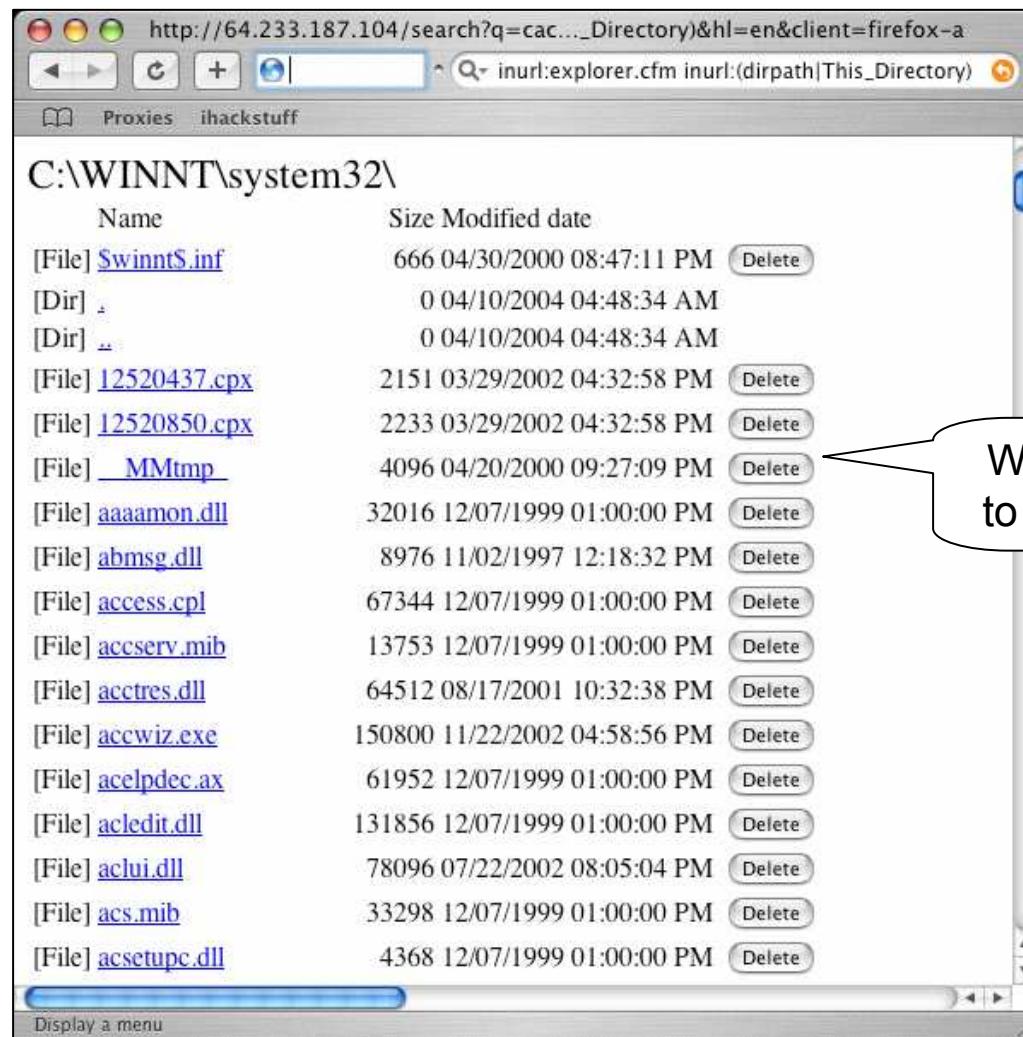
```
http://64.233.187.104/search?q=cach...tion+key%22+&hl=en&client=firefox-a
G http://64.233.187.104/sea ext:log "Final encryption key"

IP; Final encryption key[16] = 0x9d98d976 863415fe 5a7db2f6 7e768880
IP; IV hash .= g^xi[128] = 0xc22b1613 ee439b8f elalcbc8 0635e197 f2c9004e 4
IP; IV hash .= g^xr[128] = 0x977296f7 dffe428e 4da9351c 25a36bde 75f6cb09 0
IP; Output of IV hash[16] = 0x8dc0c413 0f7bed0c f1301102 bf03381e
IP; HASH_I hash .= g^xi[128] = 0xc22b1613 ee439b8f elalcbc8 0635e197 f2c900
IP; HASH_I hash .= g^xr[128] = 0x977296f7 dffe428e 4da9351c 25a36bde 75f6cb
IP; HASH_I hash .= CKY-I[8] = 0x1c2fa64d 8700001e
IP; HASH_I hash .= CKY-R[8] = 0xf7b61f69 alac09ea
IP; HASH_I hash .= SAI_b[1248] = 0x00000001 00000001 000004d8 00010824 1c2f
IP; Encoding ID = der_asn1_dn(any:0,[0..88]=C=DE, CN=Dipl. Ing. Reinhard Mo
IP; HASH_I hash .= IDii_b[93] = 0x09000000 3057310b 30090603 55040613 02444
IP; Output of HASH_I hash[20] = 0x366d1353 a2722990 0d71b2cd 70ac9eda 7d283
IP; Asynchronous public key operation started
IP; Restart packet
IP; Version = 1.0, Input packet fields = 0052 KE CR NONCE
IP; Encode pac
IP; Encode pac
version = 1.0, flags = 0x00000001
cket[93] = 0x09000000 3057310b 30090603 55040613 02444531
ding = 4, data[869] = 0x30820361 308202ca a0030201 020
] = 0x6f90b7d1 93a498fa e21422c0 0eceaa41 ec9ec230 b
proto = 1, type = 24578, spi[16] = 0x1c2fa64d
```

I only skimmed 'Applied Cryptography'.. But this looks bad...

Thanks MILKMAN!

# Explorer. EXPLORER!?!?



What do you want  
to delete today???

Thanks  
JimmyNeutron!

## More Explorers?!?!

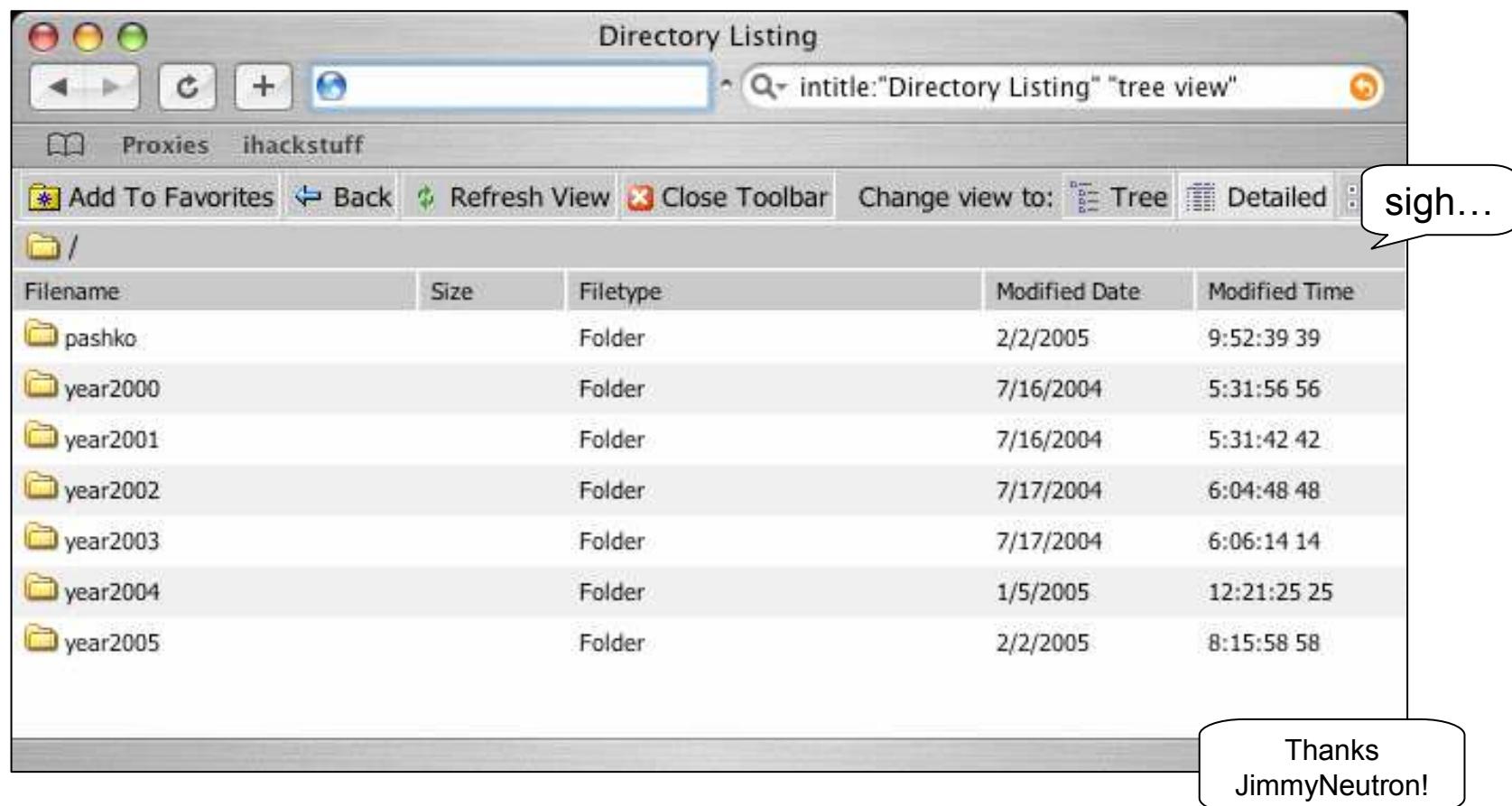
The screenshot shows a window titled "phpRemoteView: C:/Program Files/Ensim/Sitedata/hackersg/Ietpub/wwwroot/" with a search bar containing the query "intitle:phpremoteview filetype:php Name, Size, Type, Modify". Below the search bar are tabs for "Proxies" and "ihackstuff". The main area displays a file list for the directory "C:/Program Files/Ensim/Sitedata/hackersg/Ietpub/wwwroot/". The file list includes:

Name	Size	Type	Modify	Owner/Group	Perms
_vti_cnf		DIR	18/02/04 20:40	0/0	0
_vti_script		DIR	18/02/04 20:40	0/0	0
taam		DIR	29/09/04 03:42	0/0	0
tool		DIR	22/09/04 20:54	0/0	0
util		DIR	15/11/04 08:55	0/0	0
xxx		DIR	29/09/04 01:08	0/0	0
2p0pOPF4.zip	1 427 105	FILE	11/09/04 23:02	0/0	0
graphcount.php	3 854	FILE	29/09/04 02:58	0/0	0
test.php	90 895	FILE	28/09/04 22:06	0/0	0
Z_nakeR2.zip	91 425	FILE	11/09/04 23:02	0/0	0

At the bottom of the window, there are links for "Setup", "PHP eval", "phpinfo()", "Shell", "Char map", and "Language: English/Russian". A copyright notice at the bottom reads "phpRemoteView © Dmitry Borodin (version 2003-04-22) Free download - http://php.spb.ru/remview/".

A callout bubble on the left says "Why hack when you can... click? =)". A callout bubble on the right says "Thanks MacUK!".

## More Explorers?!?!



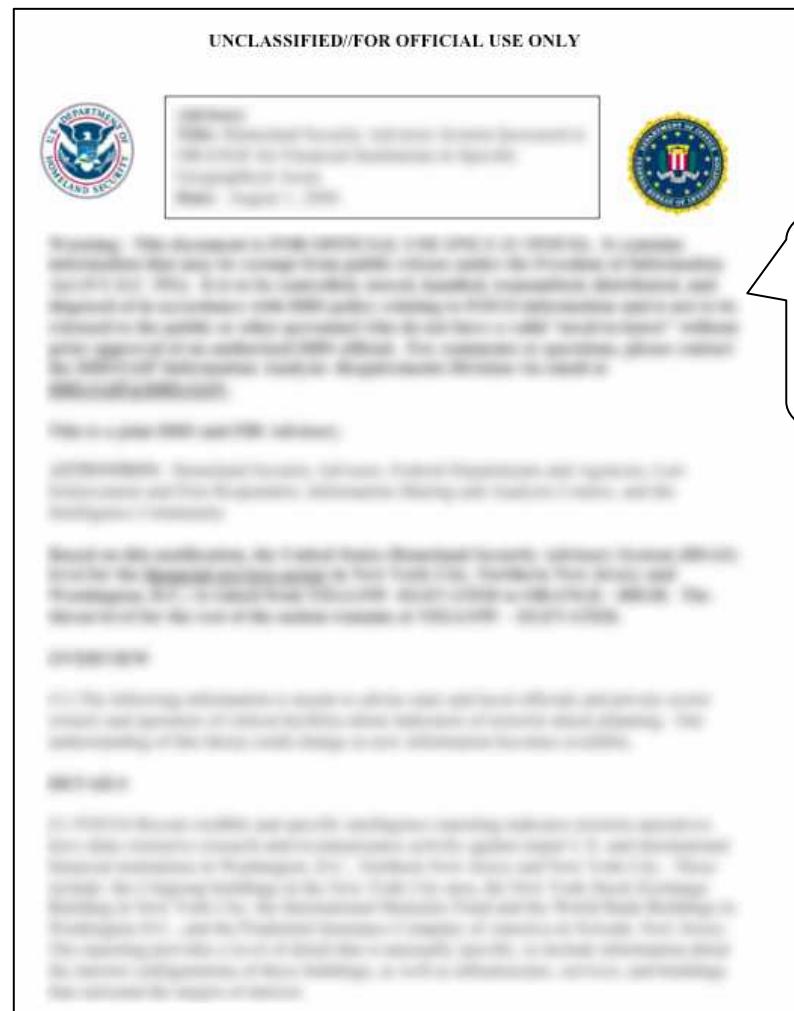
# Sensitive Government Documents

- Question: Are sensitive, non-public Government documents on the web?
- Answer: Yes.



Once these documents hit the Net, the media has a feeding frenzy, and people start copying and posting the docs...

## FOUO Documents



Although unclassified,  
this document was  
obviously not meant  
to be posted online.

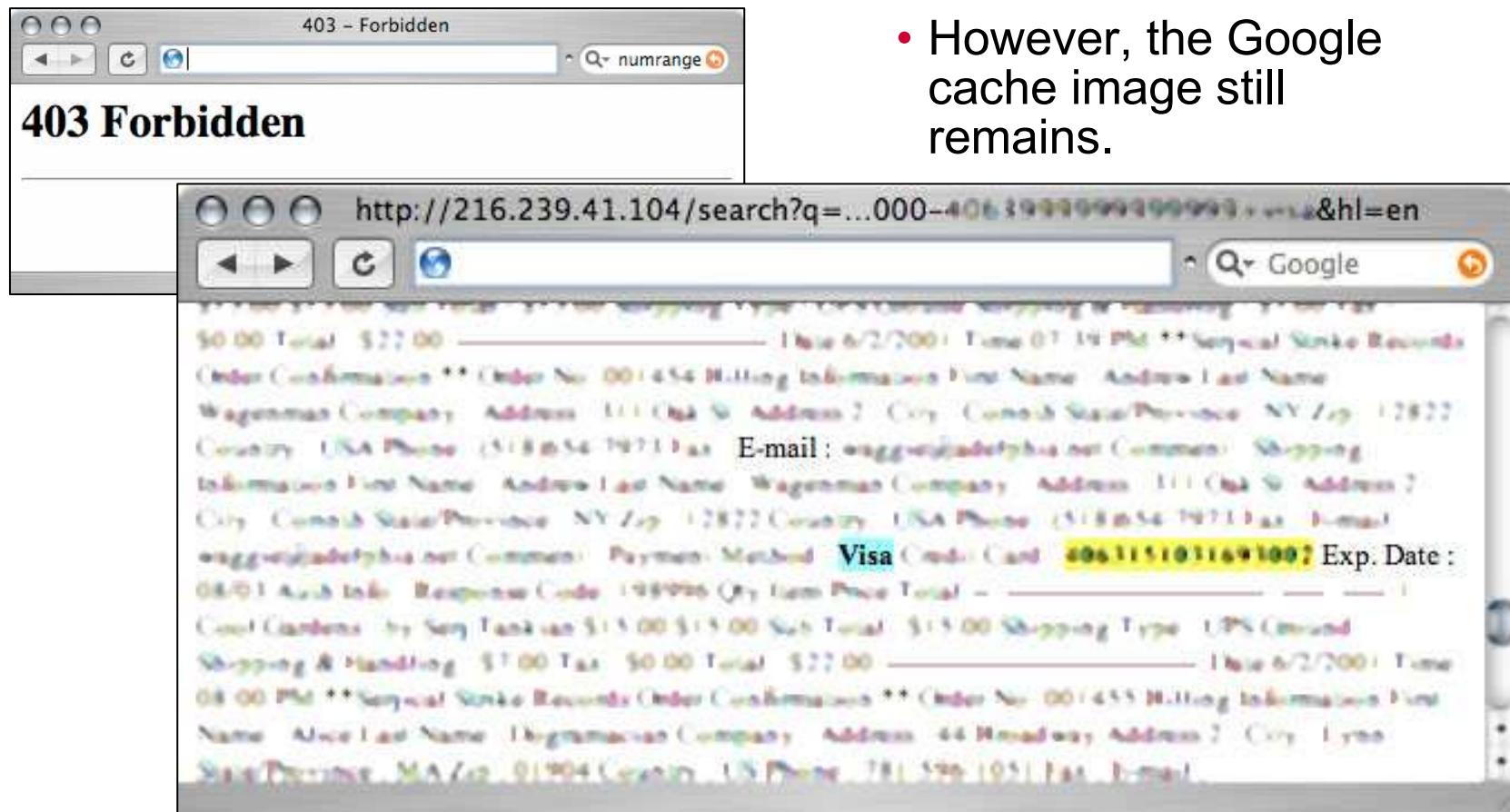
## FOUO Documents



FOUO “Prevention Guides”, like this 19 page beauty, can give bad guys horrible ideas.

## Locked out!

- Some sites lock down sensitive data..



- However, the Google cache image still remains.

---

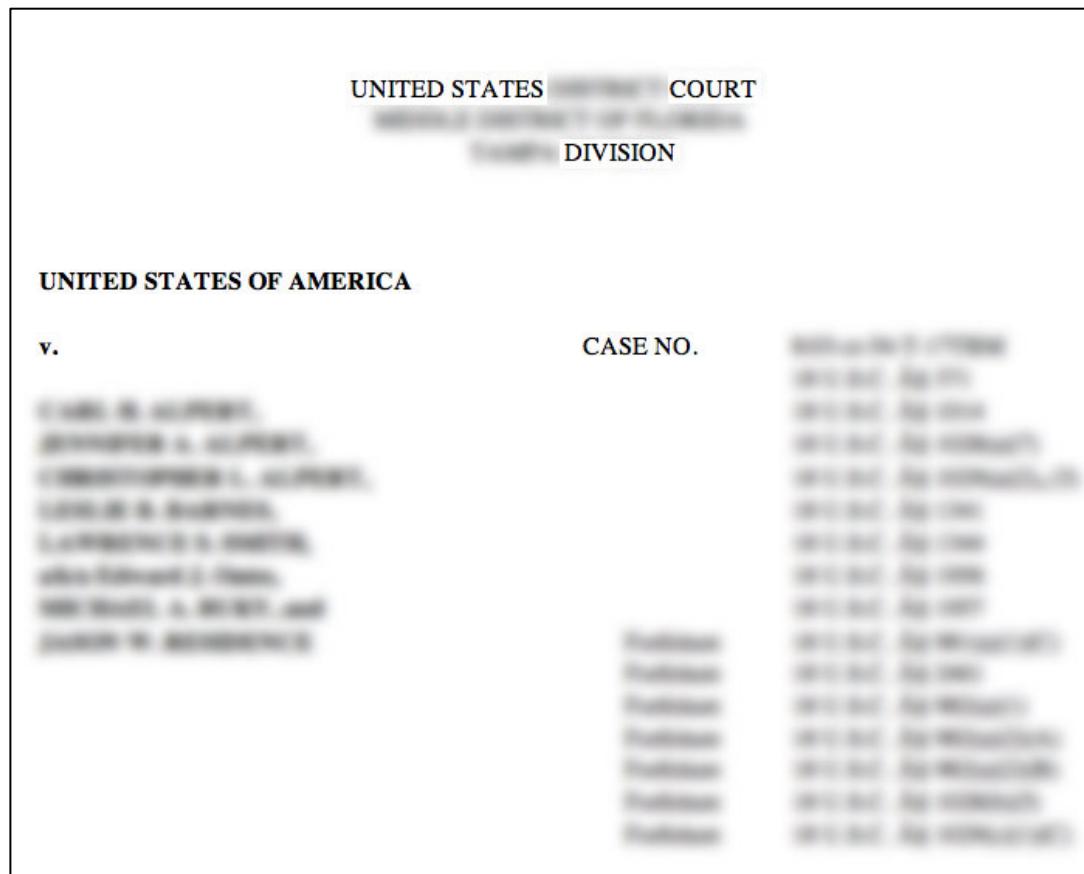
## **Credit card info on the web?**

- How can this happen? Let's take a tour of some of the possibilities...

---

## Court Documents

- Court cases sometimes give TONS of detail about cases, especially fraud.



---

## Court Documents

Platinum [REDACTED]  
account number : [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] account # [REDACTED]  
[REDACTED] account  
#: [REDACTED]  
[REDACTED] account # [REDACTED]  
[REDACTED]  
[REDACTED] account  
#: [REDACTED]  
[REDACTED] statement [REDACTED] account # [REDACTED]  
[REDACTED]  
Bank # [REDACTED]

---

## Court Documents

- How much detail is too much detail? =)

CREDIT CARD	ACCOUNT NUMBER	ACCOUNT NAME	AMOUNT
	1382 23		\$ .00
Bank	0590 13		\$ .00
Bank	0040 97		\$ .00
Bank	0590 13		\$ .00
Bank	00 96		\$ .00
Bank	00 96		\$ .00
Bank	0590 13		\$ .00
Bank	00 64		\$ .00
Bank	7100 17		\$ .00
Bank	100 64		\$ .00
Bank	081 019		\$ .00

---

## Court Documents

- Of course, fraud accounts are closed pretty quickly, no?

BANK	ACCOUNT NUMBER	ACCOUNT NAME	AMOUNT
Bank	051 13		\$1
	131 23		\$3
Bank	901 97		\$7
Bank	711 02		\$2
Bank	101 96		\$1
Bank	281 27		\$11
Bank	63 91		\$2
	901 10		\$:

---

## A tale of a corn snake

- Is this for real? Either way it's pretty sad...



## Getting shell.. the easy way

- Now I've heard the term 'using your credit card online' but this is ridiculous!

**applying for a shell acct**

---

• To: [pwing.wak@pwing.org](mailto:pwing.wak@pwing.org)  
• Subject: applying for a shell acct  
• From: "power prosecutor" <[pwing.wak@pwing.org](mailto:pwing.wak@pwing.org)>  
• Date: Sat, 09 Oct 1999 14:19:17 (GMT)

hi there i am interested to buy a shell acct for my son.  
i m 2 busy because of some reasons. This is my only way to communicate  
with my son... so i want 2 buy a shell acct using my creditcard

the login name and password will be:  
login name: [mycomp.com](http://mycomp.com)  
password: [qdog.com](http://qdog.com)

Down here will be the details about me.

Address: [Lorraine Blvd](http://Lorraine Blvd)  
[#615 Monterey Rd](http://#615 Monterey Rd)  
Fortuna, CA, 95540

tel#: 707-523-  
Billing Information:  
Name on card: [Lorraine Blvd](http://Lorraine Blvd)  
credit card #: 42800160198162  
expiration date: 01/00  
type of card: [visa](http://visa)

Thank you and I hope to hear from you soon.

# Some people just don't get it....

**Questions & Offers Board**

Our Questions & Offers board is the place to view questions and offers between other buyers and the seller. Please review this board before you [make an offer](#) or [ask the seller a question](#).

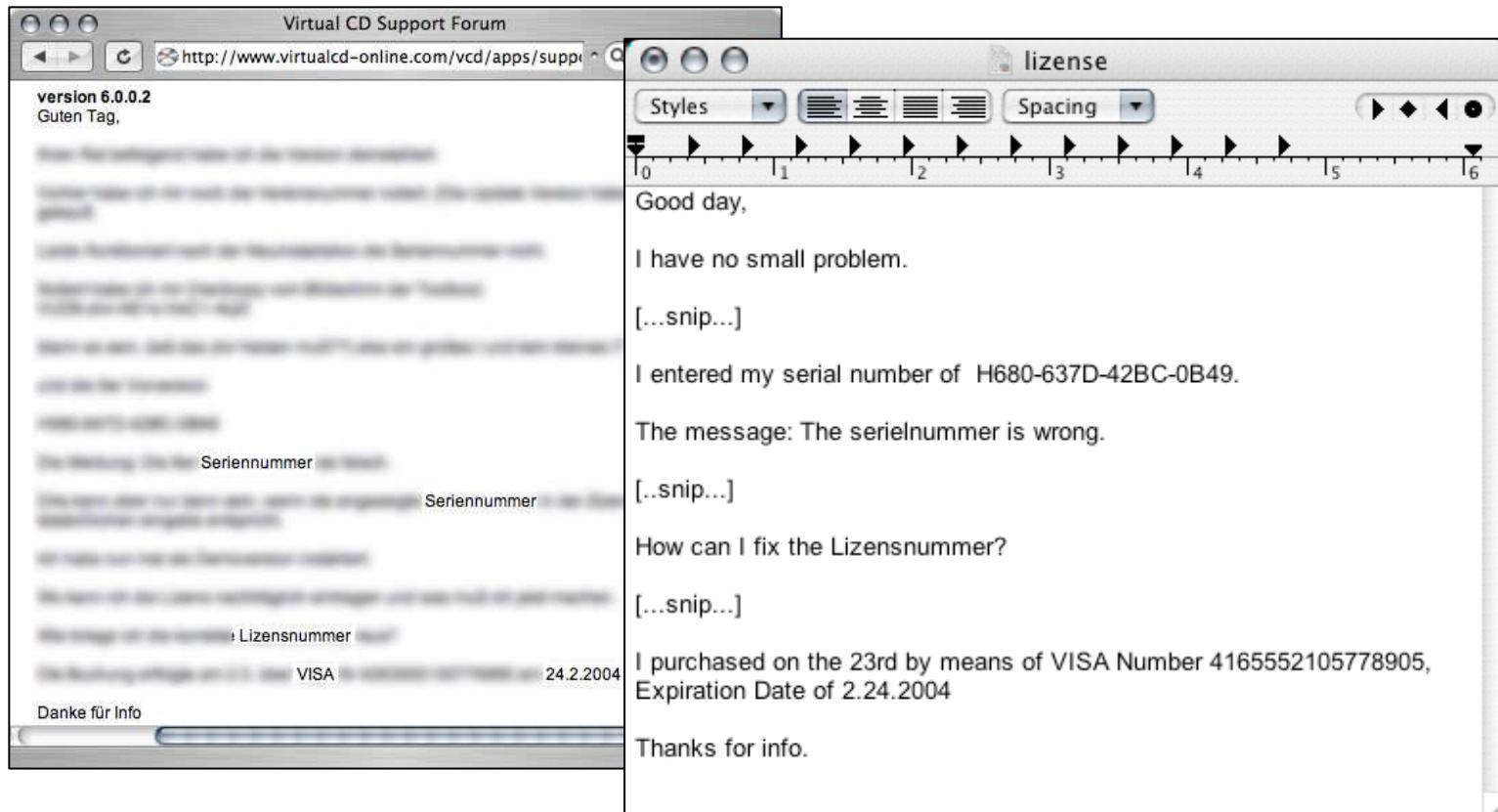
**Questions & Offers between [REDACTED] and the Seller**

**Buyer** **Question:** hi there here is my credit card details below : name on card : [REDACTED] card number : [REDACTED] expire date : 10/05 CVV2 number : [REDACTED]  
card type : **Visa** name on card : [REDACTED] card number : [REDACTED] expire date : 02/05 cyy2 number : [REDACTED] card type : **Visa** please let me know if you finished charge my credit card. thanks Mar 23 14:10PDT

**Seller** **Answer:** Ok, I will attempt to charge your card first thing tomorrow when I am back at the office. Also, what address do you want this shipped to? Thanks Mar 23 16:27PDT

## Getting serialz... wha-hay!! and MORE!

- This is a very generous person. He's willing to give his software serial numbers and his credit card info to the whole world. Generosity like this could change the world.



---

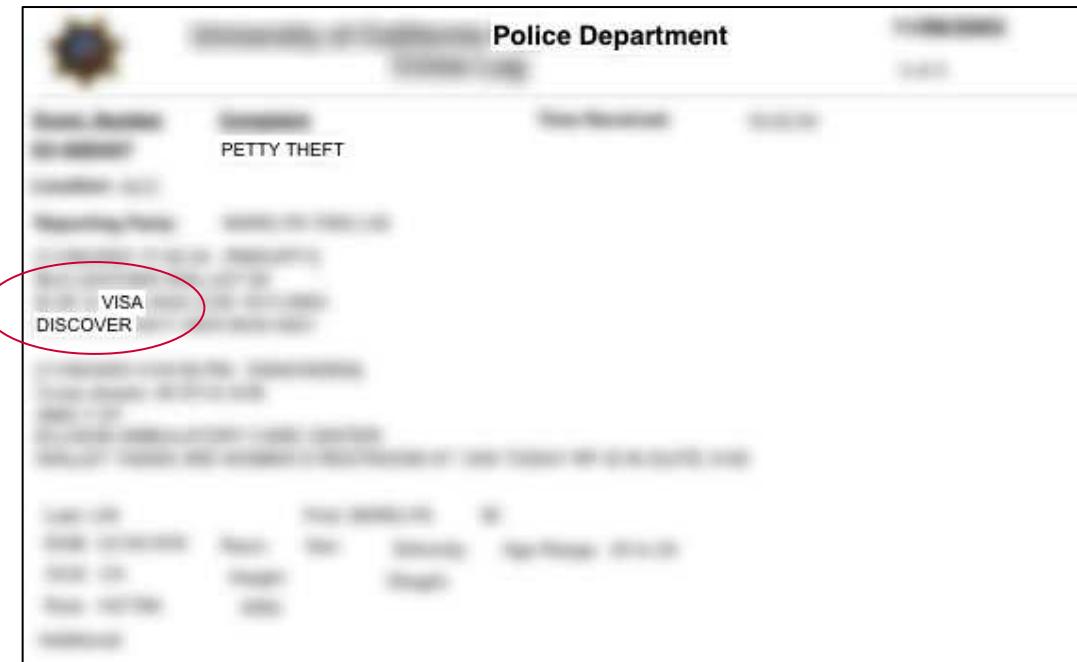
## **Police Crime reports**

- Two questions:
- Are police reports public record?
- YES.
- Are they on the web?
- YES.
- Many states have begun placing campus police crime reports on the web. Students have a right to know what crimes take place on campus.

---

## Crime shouldn't pay...

- I'm thinking there should be a process for filtering these reports.



- A few might fall through the cracks....

Results 1 - 28 of 28

# Expense Reports

- It's not uncommon for expense reports to be generated. This one is for a county.

EXPE[RE]NCE County REPORT

ACCT

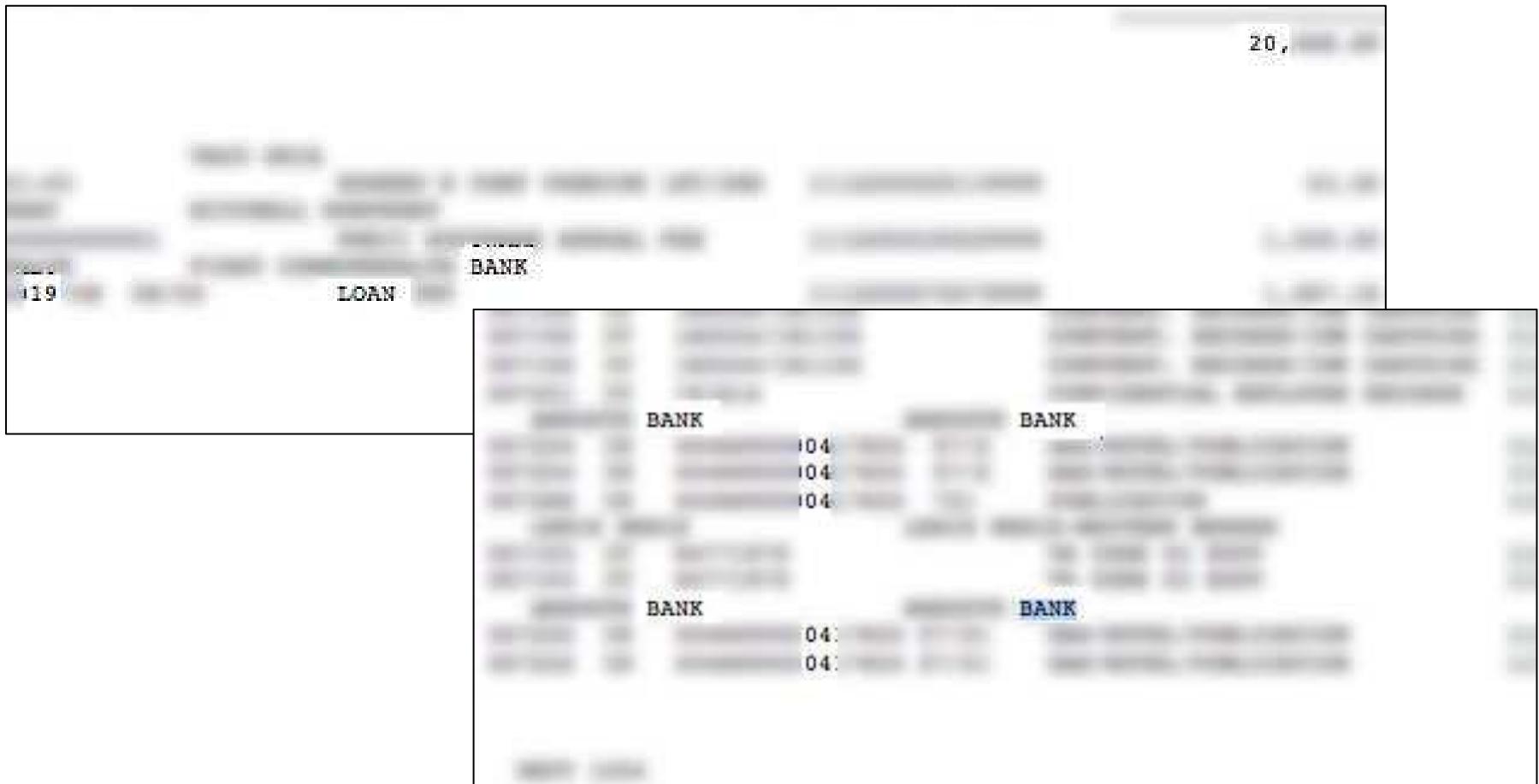
	194	15
	194	35
	194	35
	194	35
	194	35
	194	145
	194	145
	194	155

# Expense Reports

- Bank account numbers....

## Expense Reports

- Bank loan information... \$20,000 + transactions



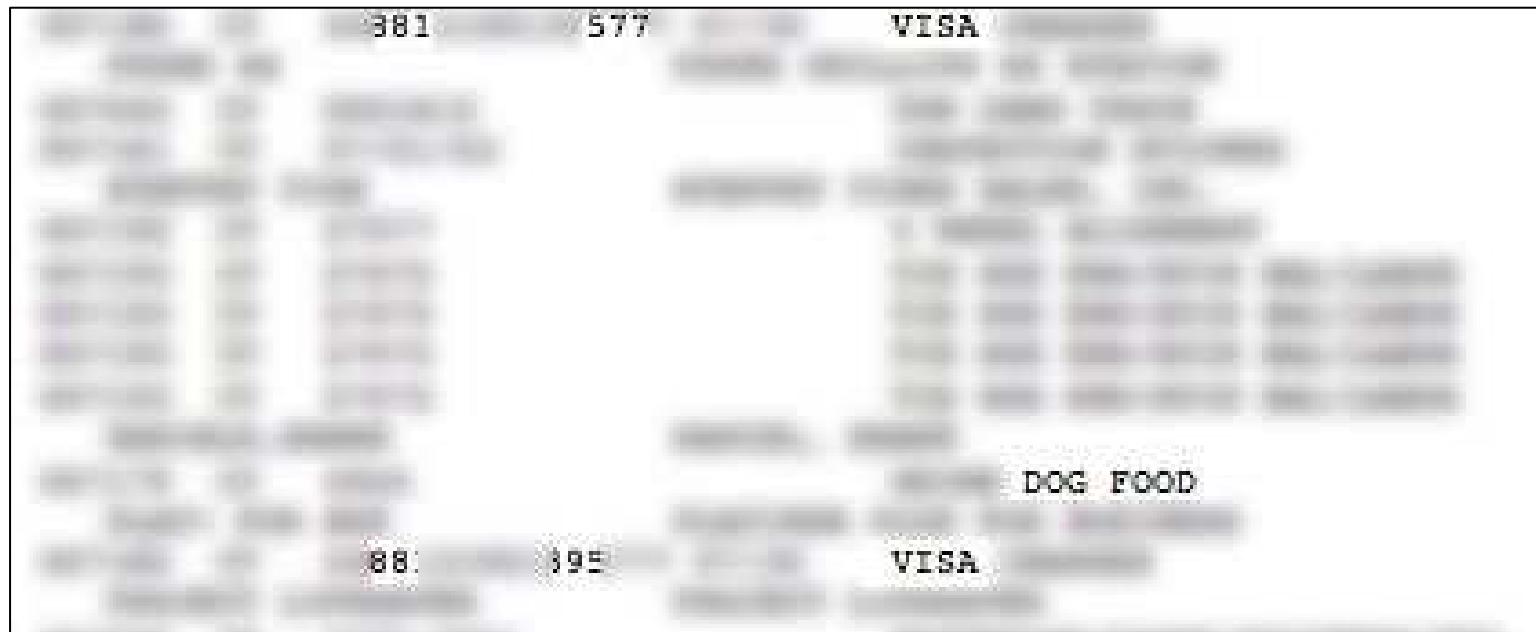
# Expense Reports

- Oh boy...

---

## Expense Reports...

- Somebody has to pay for all this stuff....



---

## Expense Reports

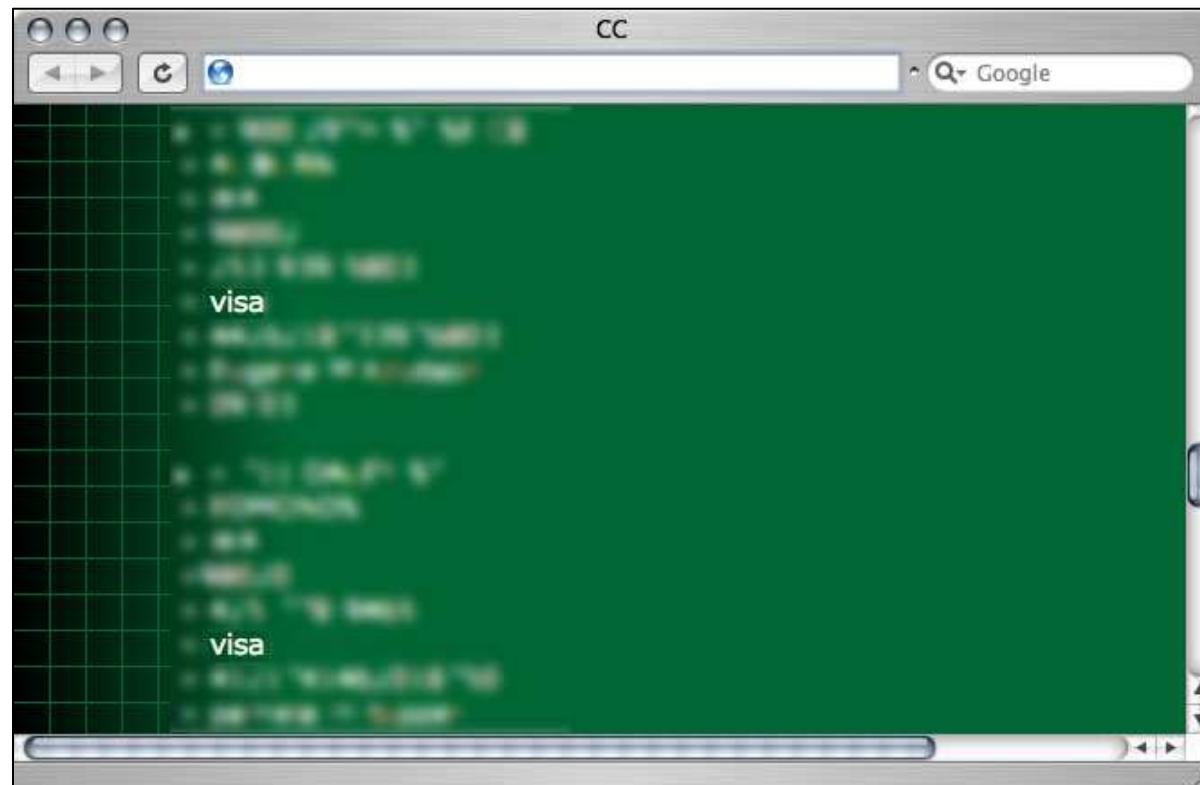
- That's one heck of a video series.... \$300+

VIDEO SERIES	9400:	39	3
VIDEO SERIES	9400:	39	3
VIDEO SERIES	9400:	39	3
VIDEO SERIES	9400:	39	3
VIDEO SERIES	9400:	39	3
		49	
		49	

---

## Credit cards... Google hacker's gold...

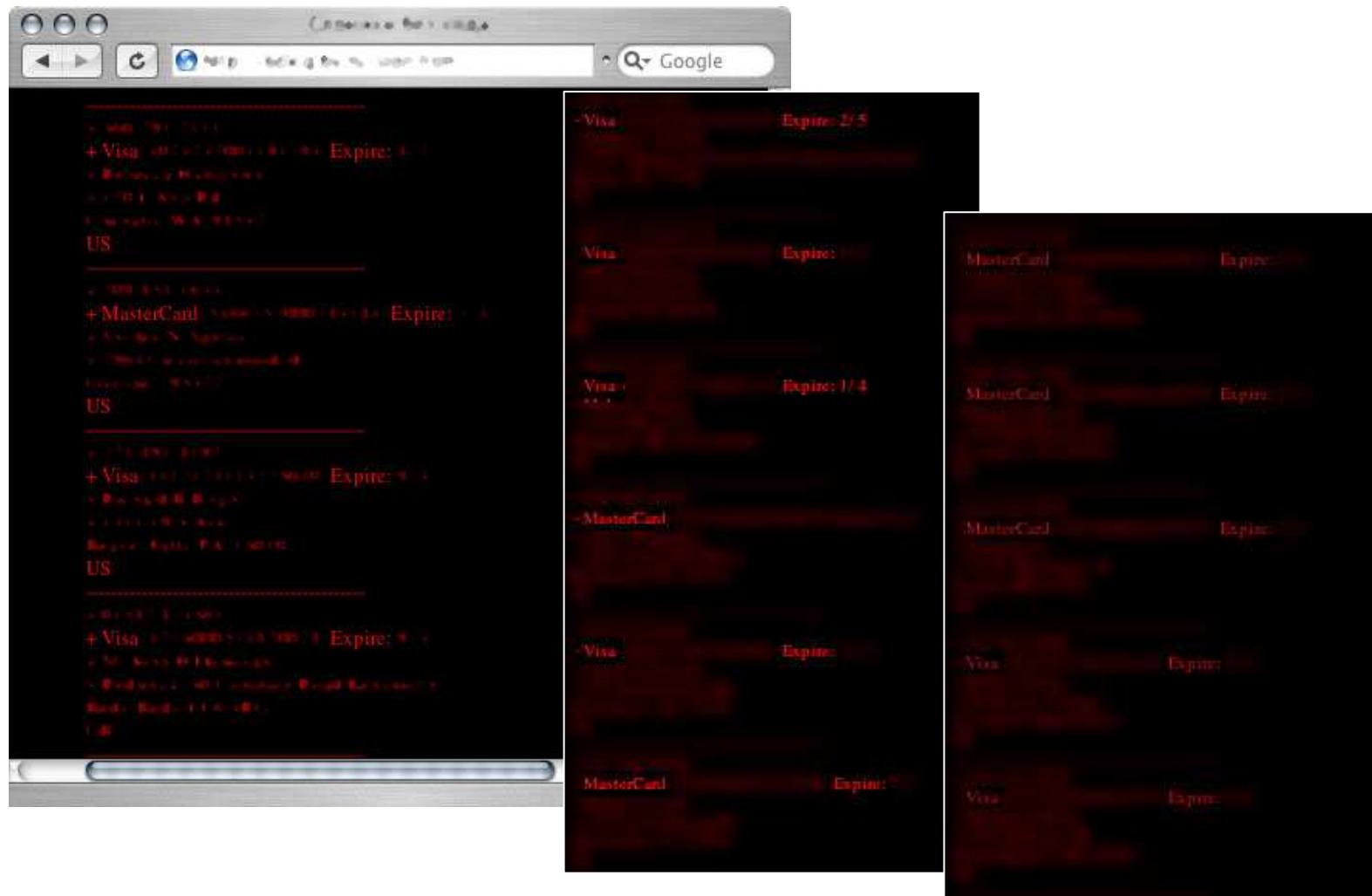
- The legend of finding credit cards online is true...
- I just get bored sifting through them all....

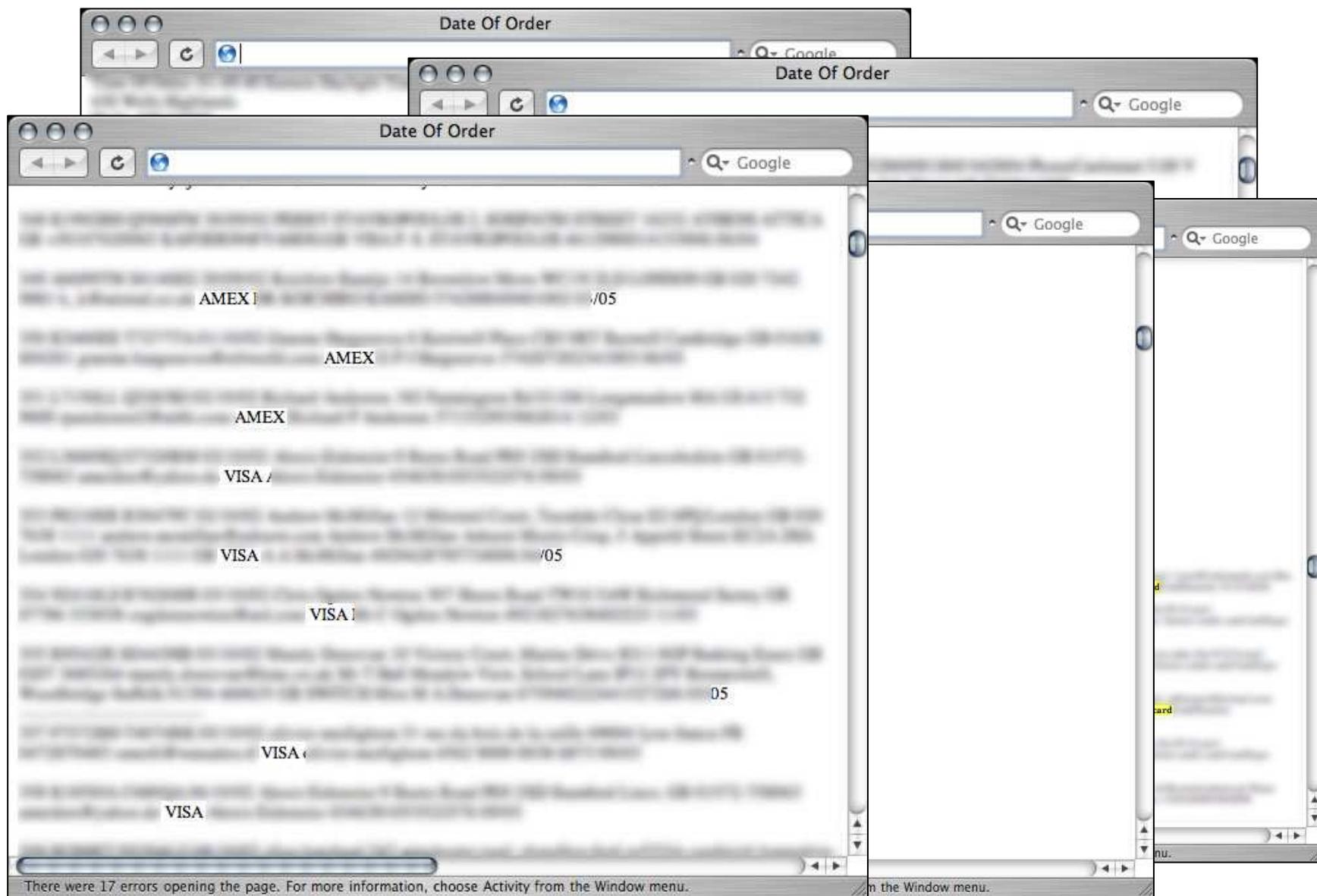


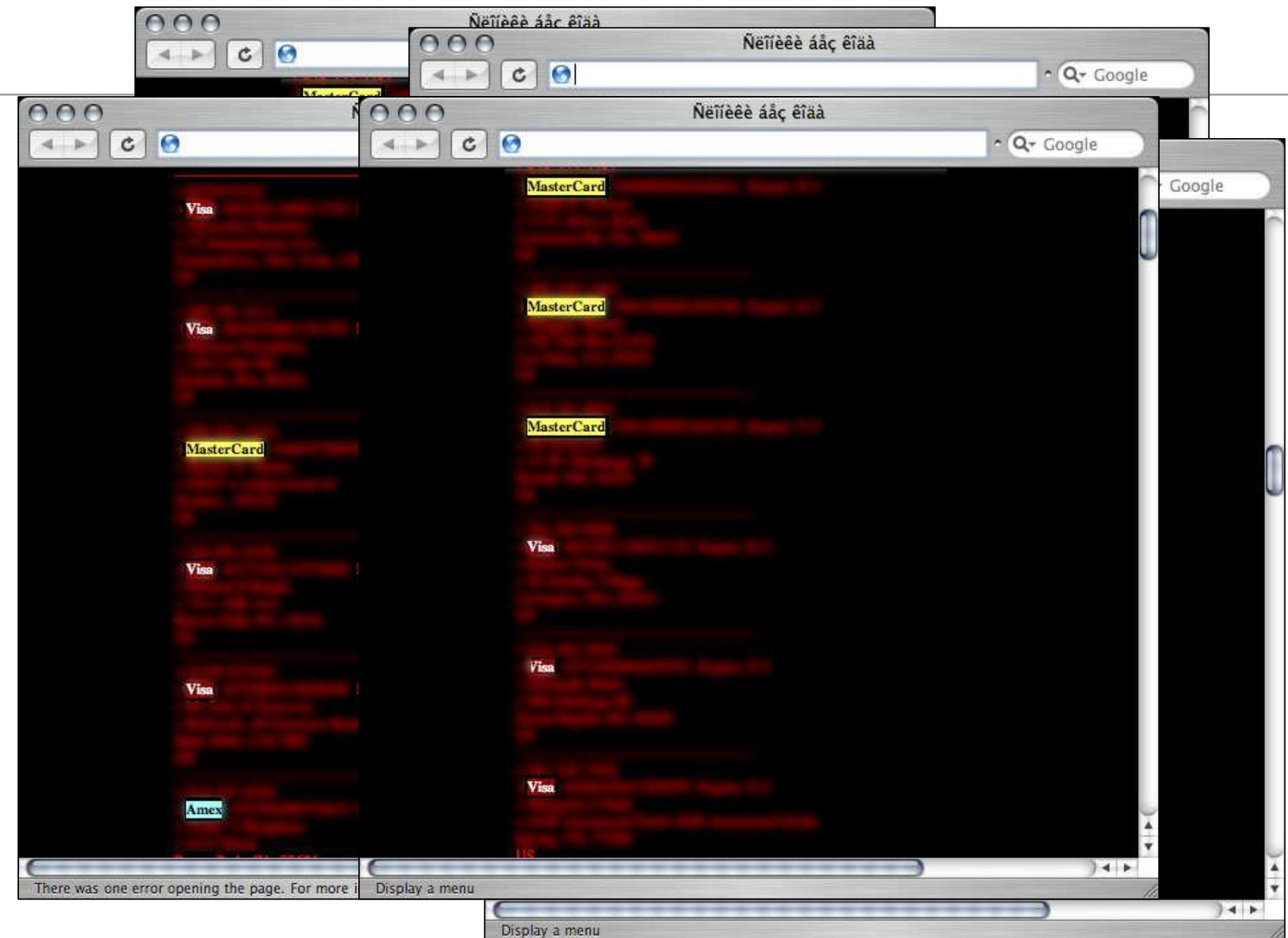
Submitted \$100.00 Shipping and Handling \$4.00 Total \$104.00 Order placed at Sun Aug 19 10:17:30 2007 Authorize.net Order ID: 1040448194 United States Shipping Method: Ground F fedex ground@yourshipnow.com Authorize.net Order ID: 1040448194 Credit Card Information: Visa Number: 40001234567890 Expire: 06/08 phone: 400-1234	Mastercard
Submitted \$100.00 Shipping and Handling \$4.00 Total \$104.00 Order placed at Sun Aug 19 10:17:30 2007 Authorize.net Order ID: 1040448194 United States Shipping Method: Ground F fedex ground@yourshipnow.com Authorize.net Order ID: 1040448194 Credit Card Information: Visa Number: 40001234567890 Expire: 06/08 phone: 400-1234	Visa
Submitted \$100.00 Shipping and Handling \$4.00 Total \$104.00 Order placed at Sun Aug 19 10:17:30 2007 Authorize.net Order ID: 1040448194 United States Shipping Method: Ground F fedex ground@yourshipnow.com Authorize.net Order ID: 1040448194 Credit Card Information: Visa Number: 40001234567890 Expire: 06/08 phone: 400-1234	Mastercard
Submitted \$100.00 Shipping and Handling \$4.00 Total \$104.00 Order placed at Sun Aug 19 10:17:30 2007 Authorize.net Order ID: 1040448194 United States Shipping Method: Ground F fedex ground@yourshipnow.com Authorize.net Order ID: 1040448194 Credit Card Information: Visa Number: 40001234567890 Expire: 06/08 phone: 400-1234	Visa
Submitted \$100.00 Shipping and Handling \$4.00 Total \$104.00 Order placed at Sun Aug 19 10:17:30 2007 Authorize.net Order ID: 1040448194 United States Shipping Method: Ground F fedex ground@yourshipnow.com Authorize.net Order ID: 1040448194 Credit Card Information: Mastercard Number: 40001234567890 Expire: 06/08 phone: 400-1234	Mastercard
Submitted \$100.00 Shipping and Handling \$4.00 Total \$104.00 Order placed at Sun Aug 19 10:17:30 2007 Authorize.net Order ID: 1040448194 United States Shipping Method: Ground F fedex ground@yourshipnow.com Authorize.net Order ID: 1040448194 Credit Card Information: Visa Number: 40001234567890 Expire: 06/08 phone: 400-1234	Visa
Submitted \$100.00 Shipping and Handling \$4.00 Total \$104.00 Order placed at Sun Aug 19 10:17:30 2007 Authorize.net Order ID: 1040448194 United States Shipping Method: Ground F fedex ground@yourshipnow.com Authorize.net Order ID: 1040448194 Credit Card Information: Visa Number: 40001234567890 Expire: 06/08 phone: 400-1234	Visa
Submitted \$100.00 Shipping and Handling \$4.00 Total \$104.00 Order placed at Sun Aug 19 10:17:30 2007 Authorize.net Order ID: 1040448194 United States Shipping Method: Ground F fedex ground@yourshipnow.com Authorize.net Order ID: 1040448194 Credit Card Information: Visa Number: 40001234567890 Expire: 06/08 phone: 400-1234	Mastercard

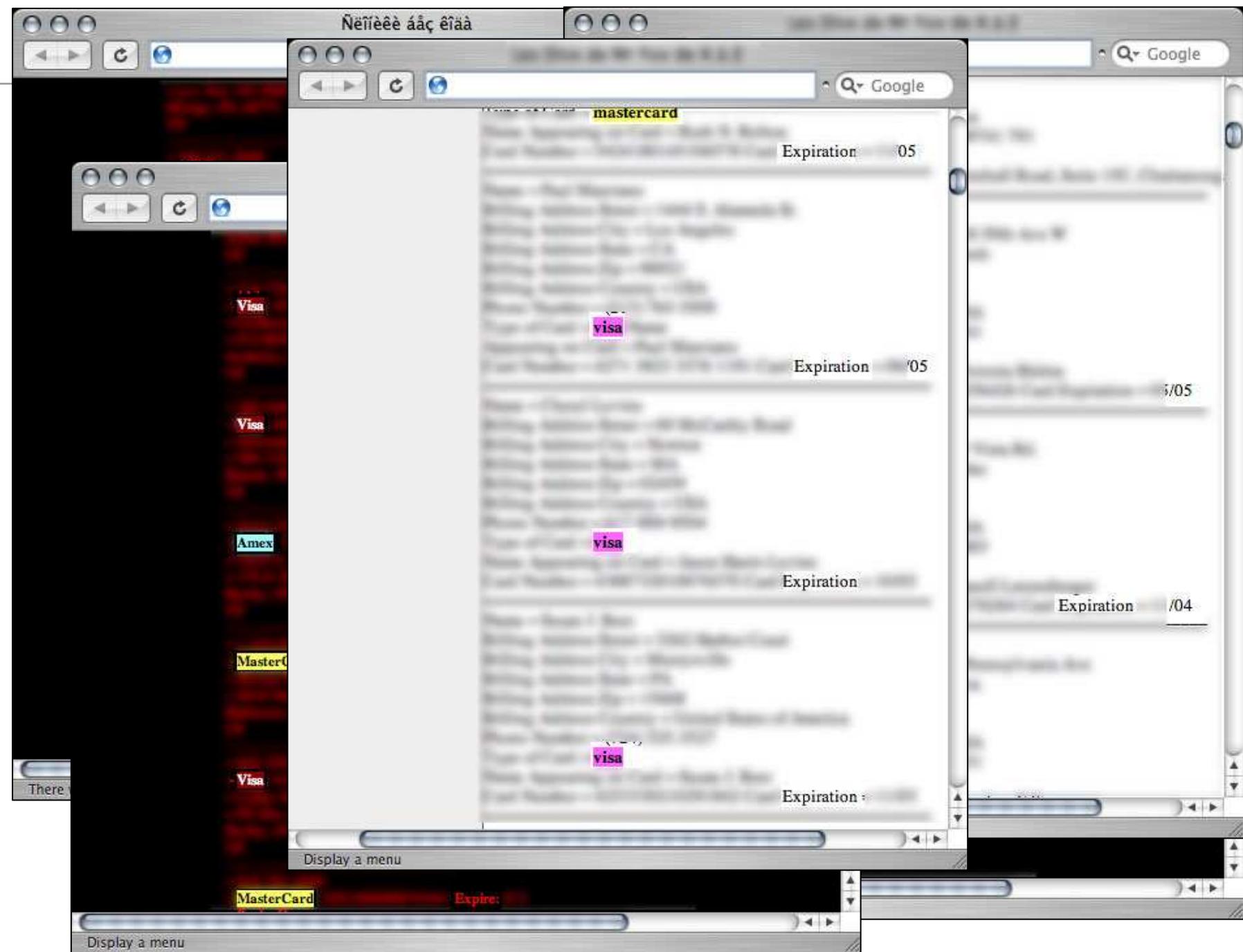
Card No	Visa	Expire
VISA		
	Visa	expire:
Card Number:	Visa:	Expire
VISA	Visa	Expire
	visa	

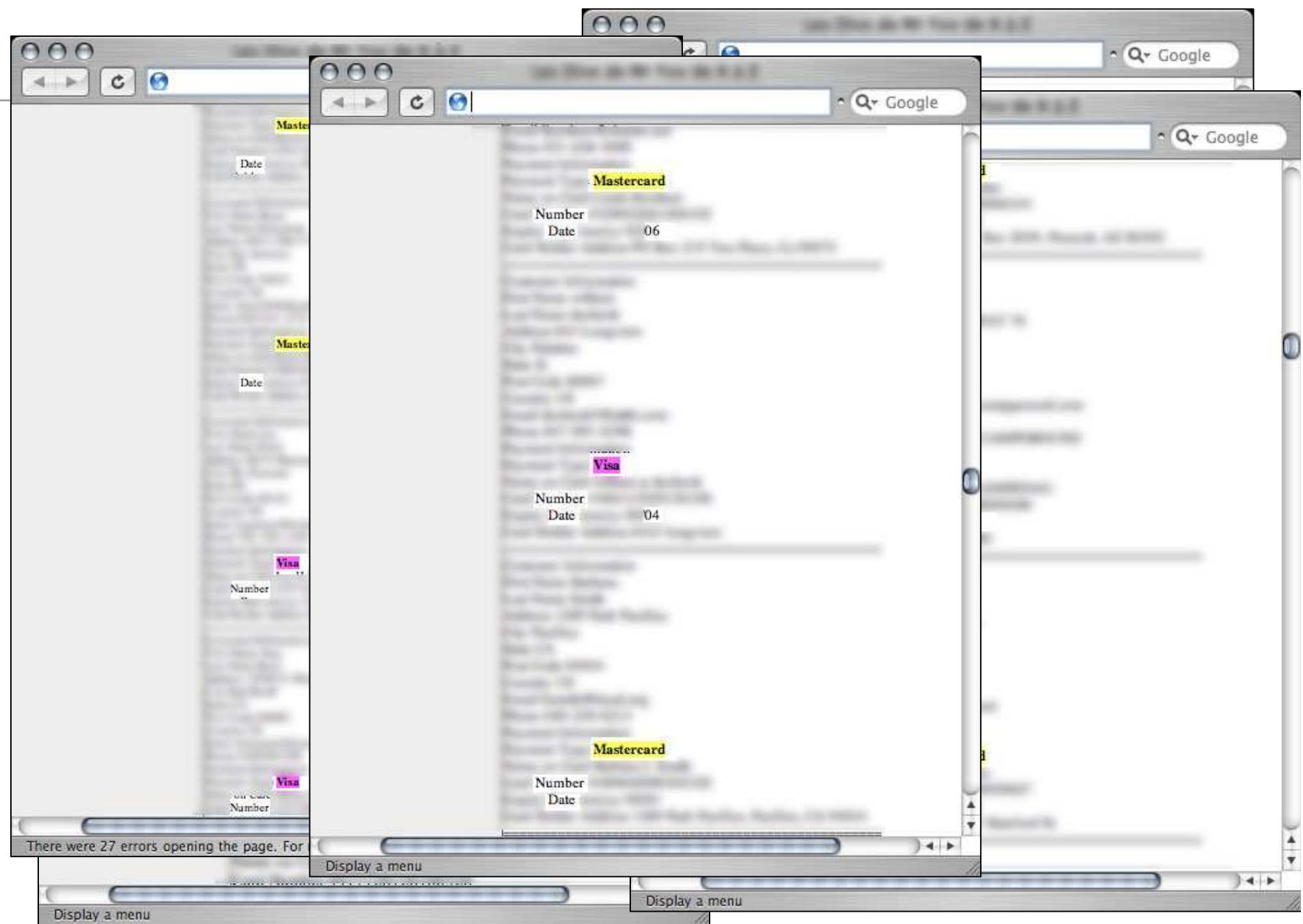
# Credit Listings





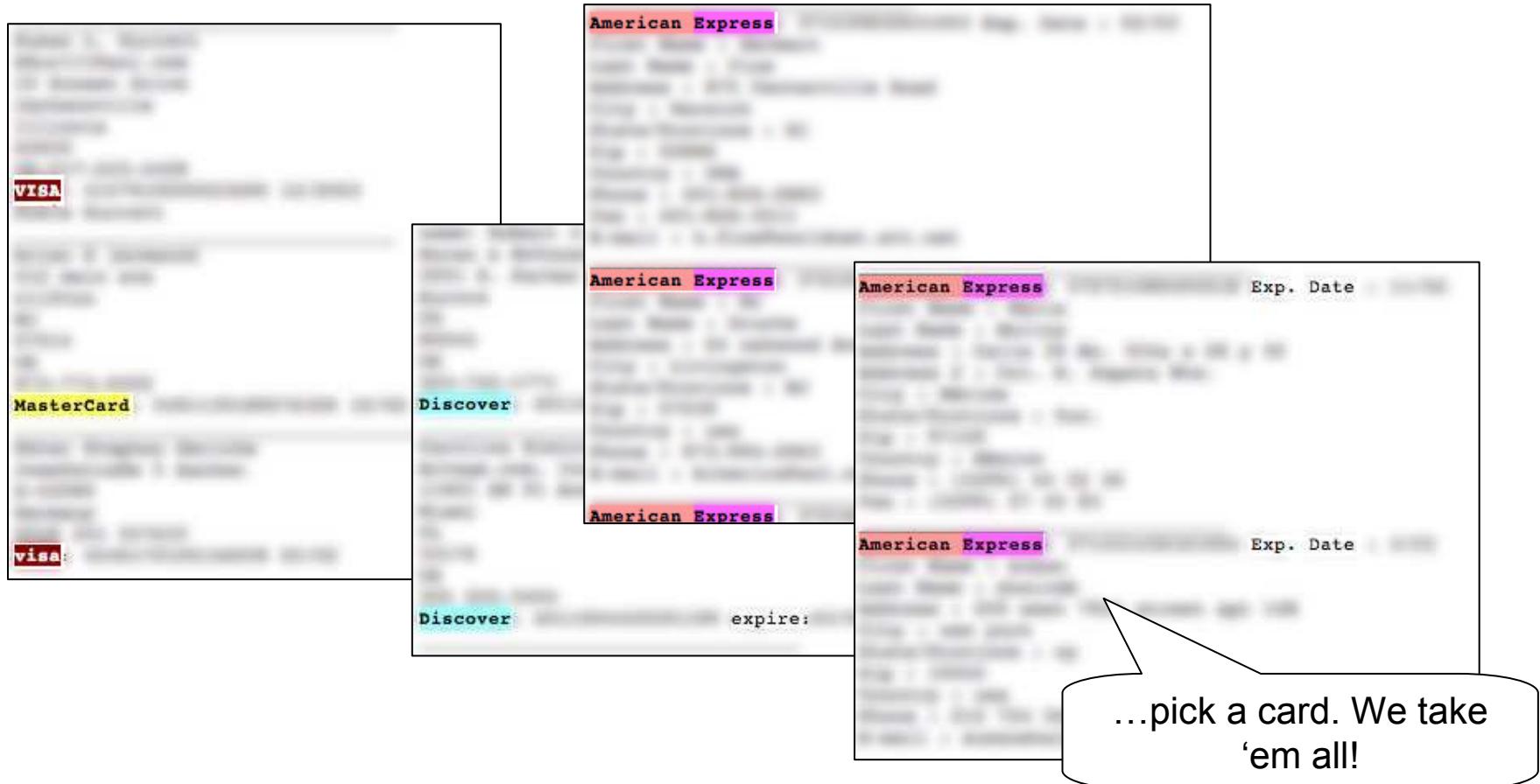






---

## Pick a card any card...



---

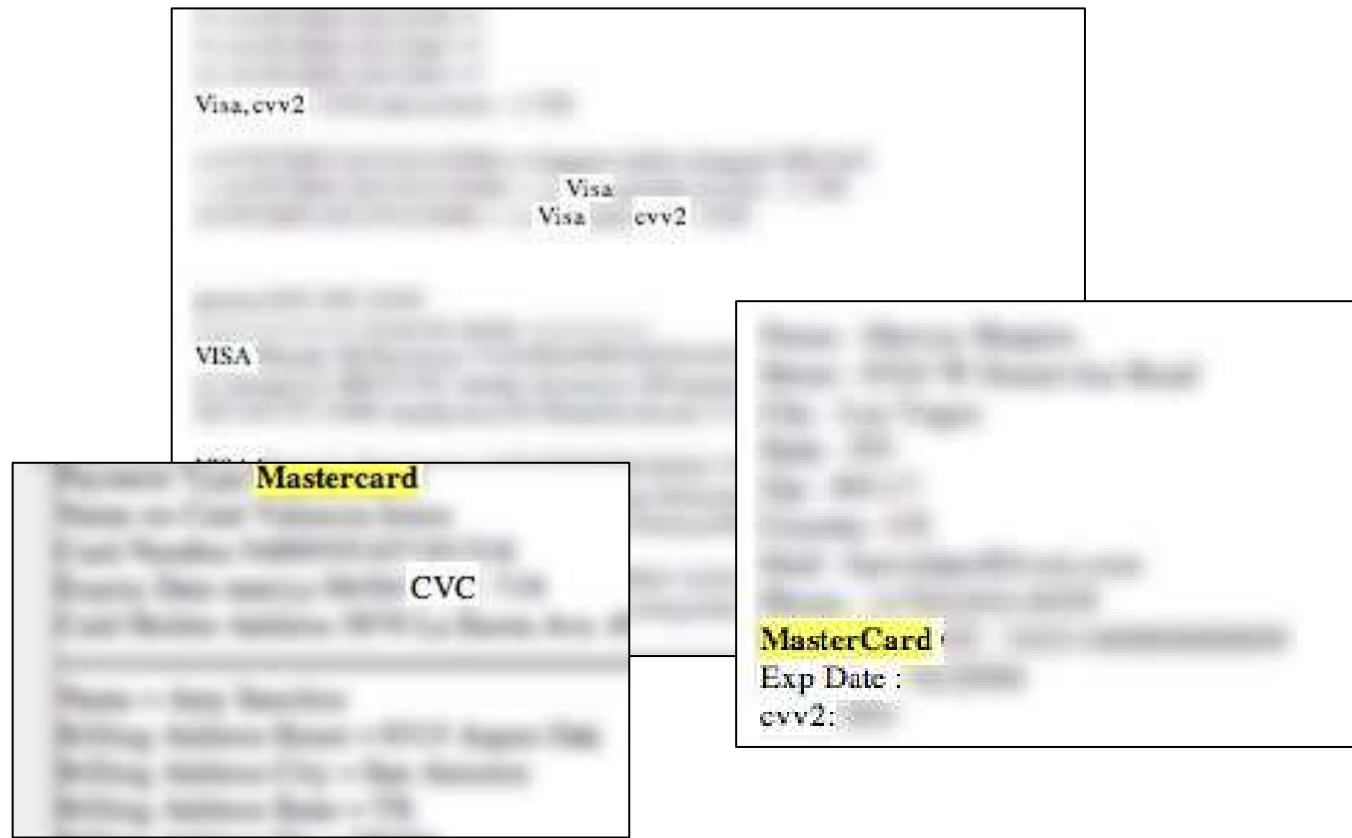
## Credit Validation

Question: What keeps someone from using a pilfered credit card number and expiration date to make an online purchase?

- Answer: That little code on the back of the card.
- Bonus question: What's that code called?
- Answer: A “CVV” code.

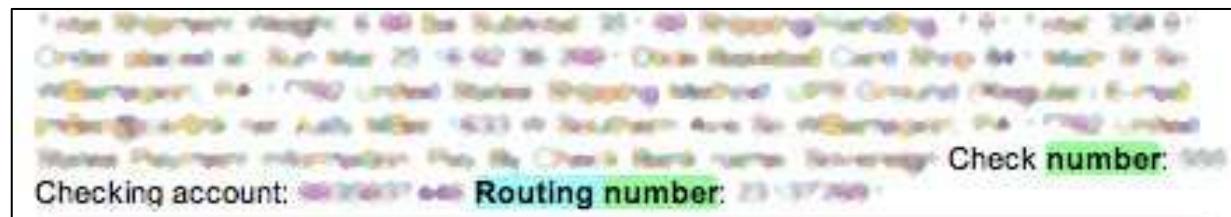
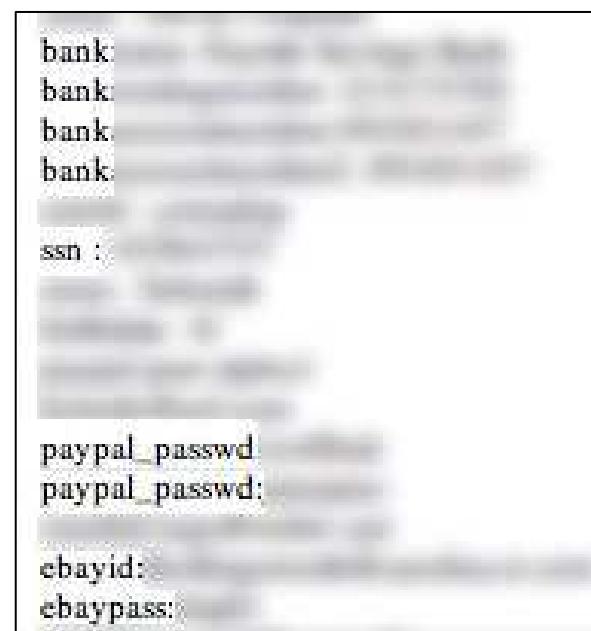
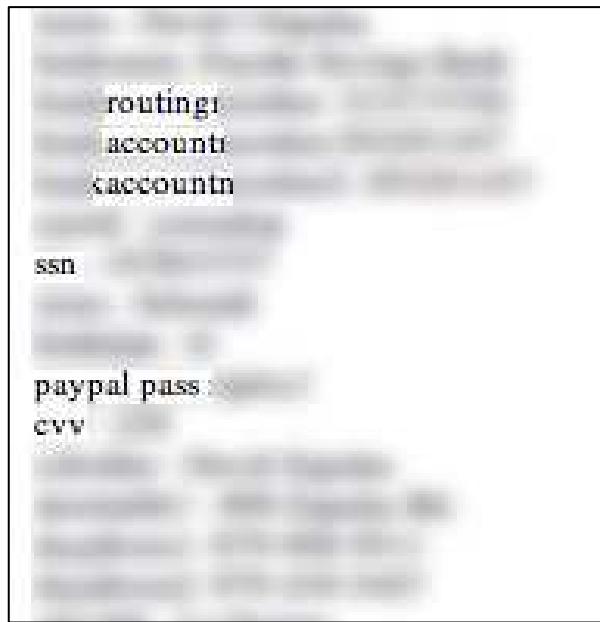
---

## Credit Card Numbers, Expiration Date and CVV numbers, oh my!



## That's not all....

- Credit cards are sooo 1990's =)



---

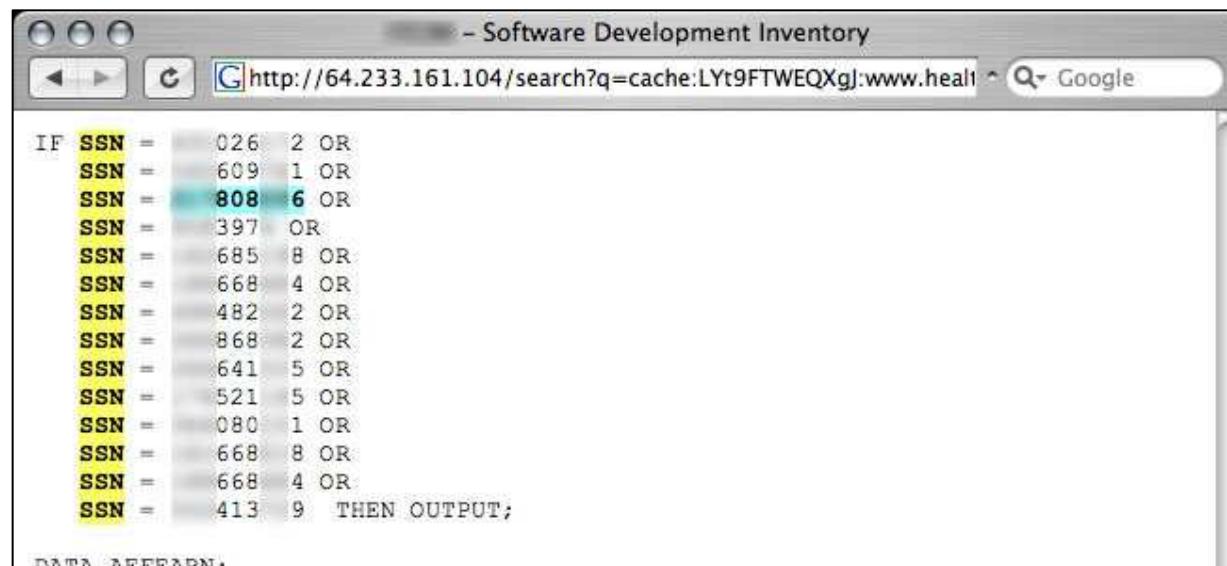
## **Getting more personal**

- Question: What's the one 9 digit number you shouldn't give to ANYONE?
  - Answer: SSN
  - Bonus question: What can you do with someone's SSN?
  - Answer: Steal their identity.
- 
- How do SSN's get on the web? Let's take a look at some possibilities.

---

## SSN's in source code

- Well, they could be hardcoded into a healthcare system... and uhmmm... put on the web...

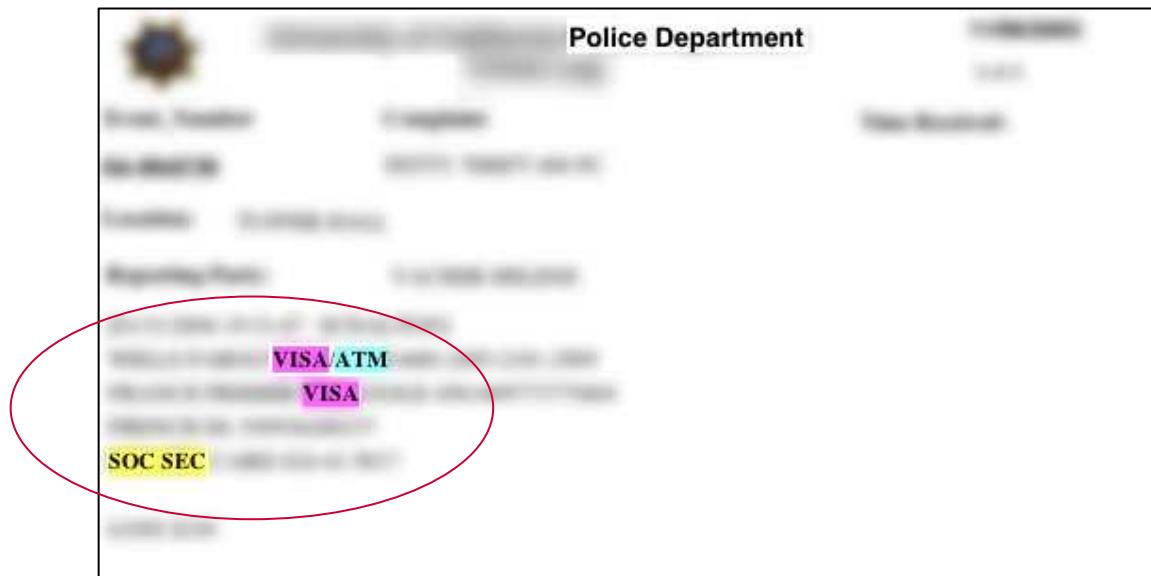


The screenshot shows a window titled "Software Development Inventory". The address bar indicates the URL is <http://64.233.161.104/search?q=cache:LYt9FTWEQXgJ:www.healthcare.com>. The main content area displays a list of SSN values, each preceded by the text "IF SSN =". The list includes:  
IF SSN = 026 2 OR  
IF SSN = 609 1 OR  
IF SSN = 808 6 OR  
IF SSN = 397 OR  
IF SSN = 685 8 OR  
IF SSN = 668 4 OR  
IF SSN = 482 2 OR  
IF SSN = 868 2 OR  
IF SSN = 641 5 OR  
IF SSN = 521 5 OR  
IF SSN = 080 1 OR  
IF SSN = 668 8 OR  
IF SSN = 668 4 OR  
IF SSN = 413 9 THEN OUTPUT;  
DATA AEEARN.

---

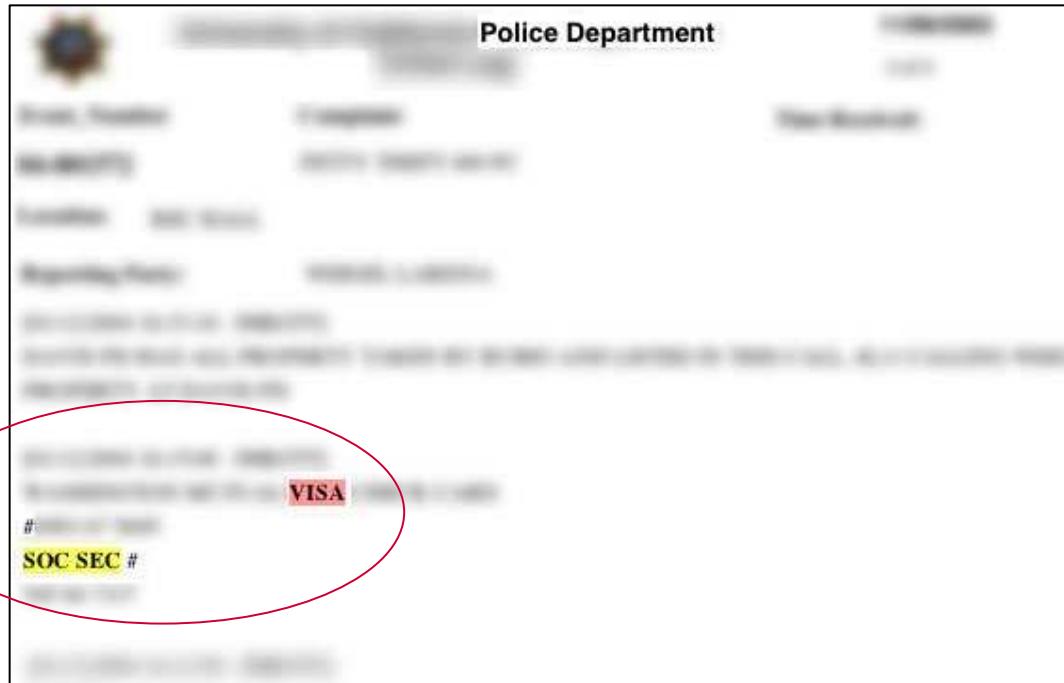
## Crime shouldn't pay...

- Remember the police reports? Since the credit card accounts in them are no good, maybe we should troll them some more....



---

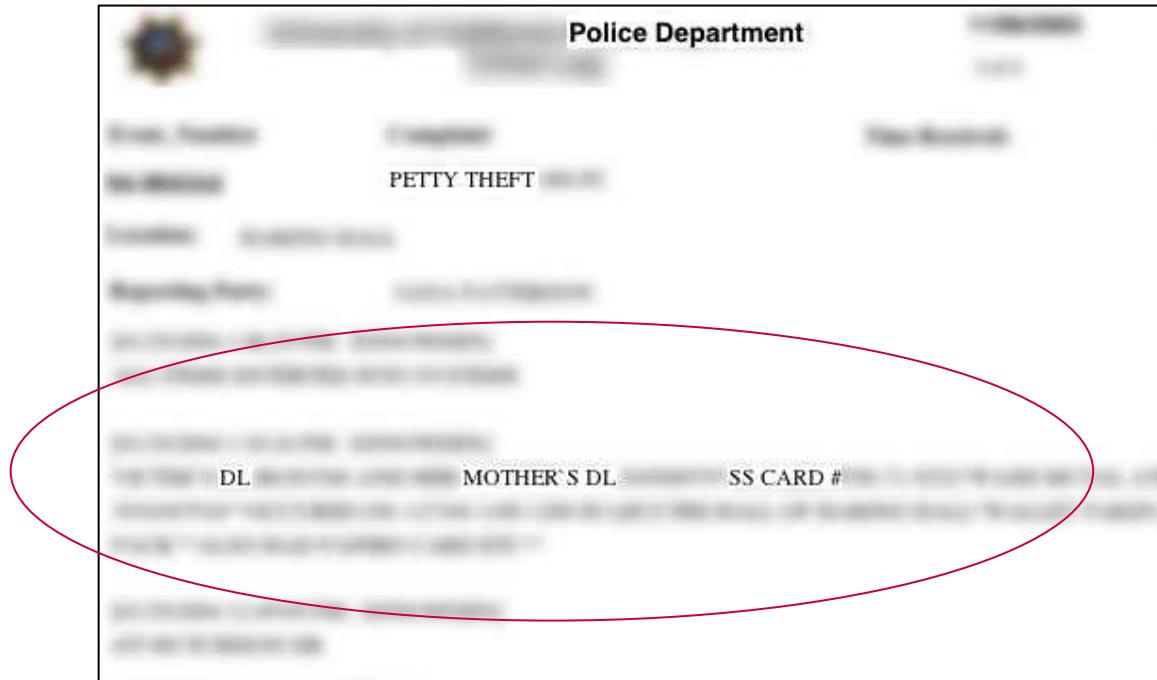
## SSN's - Police Reports



---

## SSN's

- Students have a right to know...

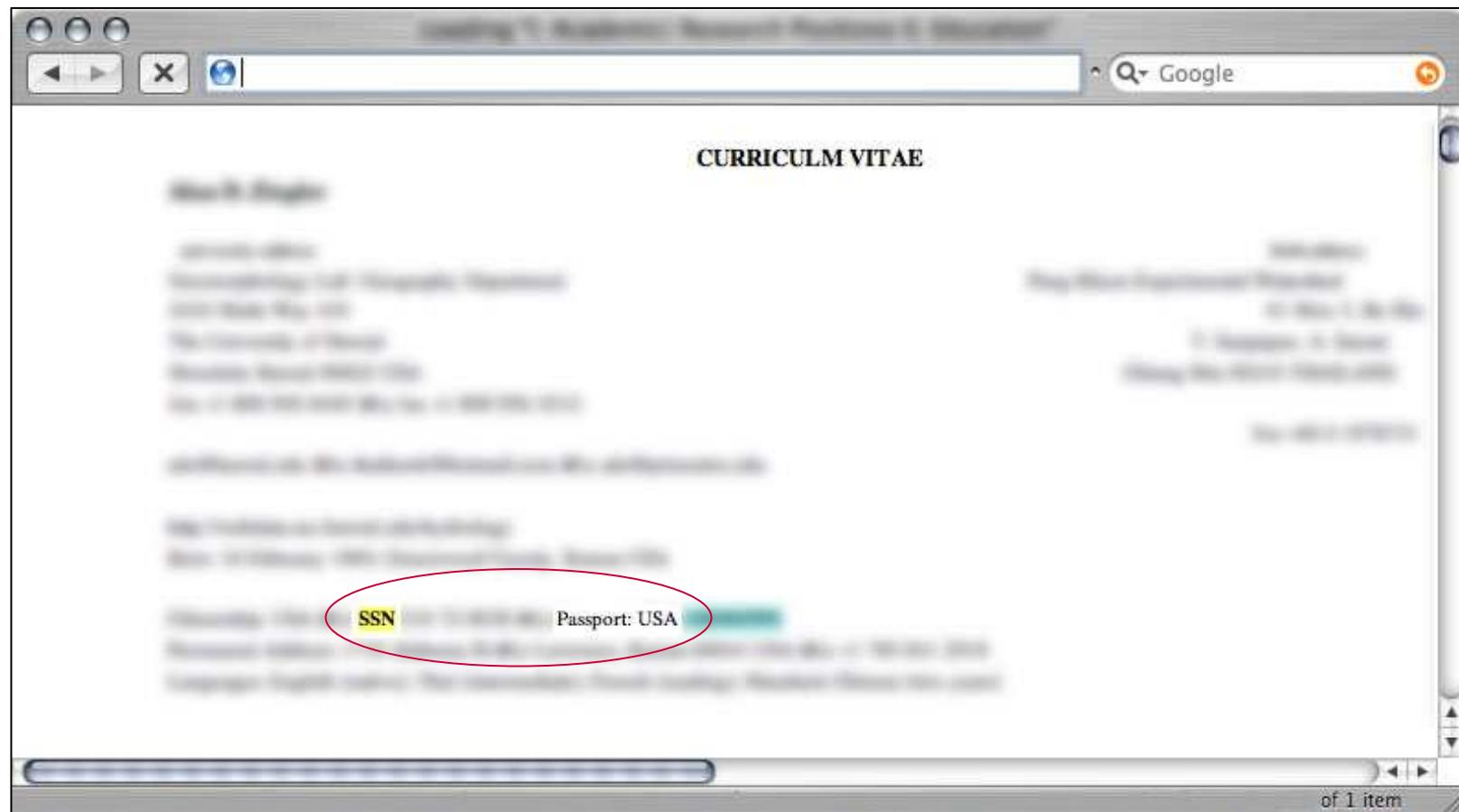


Results 1 - 28 of 28

---

## Social Security Numbers

- Many privacy violations are self-inflicted...



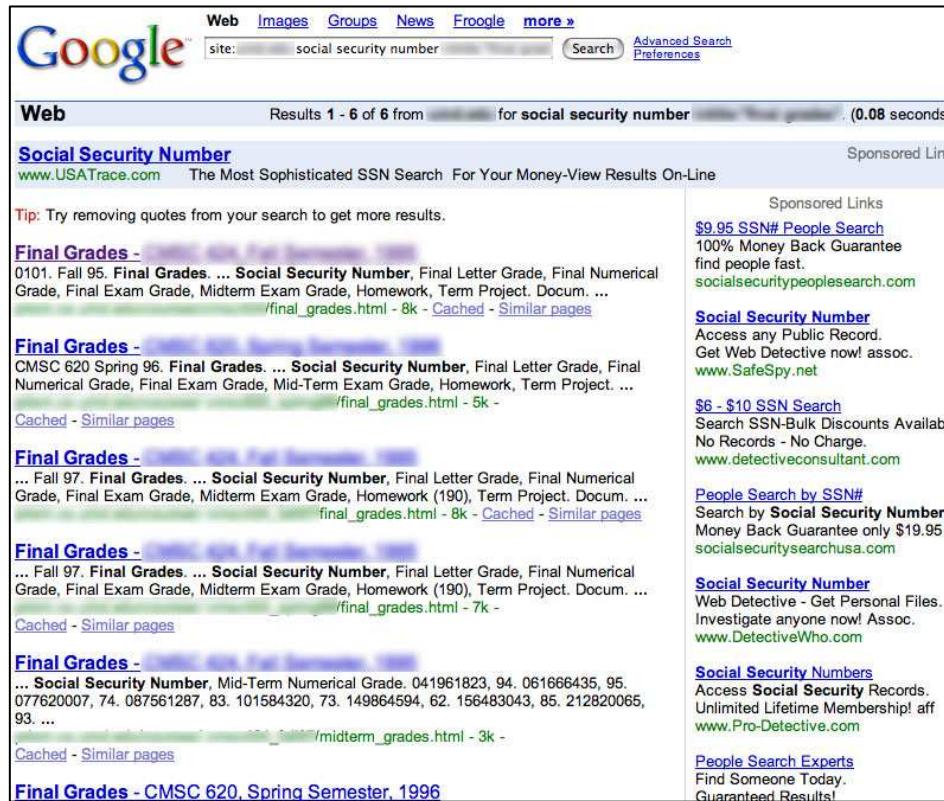
## Social Security Numbers

- Schools are notorious... Grades posted w/ student's SSN's

Social Security Number	Final Letter Grade	Final Numerical Grade	Final Exam Grade	Midterm Exam Grade	Homework	Term Project			
						Docum.	Complex.	Accomplish.	Grade
-00-	0				140				
768	Y	A	90	88	90	136	A	A	A
009	Y	A	91	84	92	137	A+	A	A+
000	Y	A	89	93	80	127	A+	A	A+
763	Y	B	76	71	80	135	C++	C	B
547	Y	A	89	85	89	119	A++	A++	A++
726	Y	A	88	77	90	128	A+	A	A+
401	Y	F	43	-	48	28	A+	A	B
867		C	73	67	58	124	A-	A	A+
602	Y	A	91	88	85	137	A++	A++	A++
028	Y	C	73	65	61	129	A-	A	A-
042	Y	B	75	56	78	116	A	A	A-
117	Y	B	80	72	77	110	A	B++	A
276	Y	B	80	74	74	118	A	B++	A
134	Y	A	87	86	84	127	A-	A	A-
214	Y	C	71	57	63	117	A-	A	A-
456	Y	A	93	97	88	134	A+	A	A+
889	Y	B	76	62	75	124	A	B++	A
763	Y	A	86	82	87	111	A	B	A-
028	Y	B	83	81	76	129	A	B++	A
359	Y	B	77	65	69	129	A+	A	A+
333	Y	B	78	77	64	111	A-	A	A
336	Y	A	85	88	83	124	A+	A	B
729	Y	B	80	69	81	110	A-	B++	A-
786	Y	D	63	53	56	72	B-	C	C-

# Social Security Numbers

- Once you get a lock on a grade list, the results fan out as you explore the site.



A screenshot of a Google search results page. The search query is "social security number". The results are filtered to show only web pages. The first result is a sponsored link from USATrace.com titled "Social Security Number" which claims to be "The Most Sophisticated SSN Search For Your Money-View Results On-Line". Below this are several regular search results, each titled "Final Grades -" followed by a URL like "/final\_grades.html". To the right of the main results, there are two columns of sponsored links. The top column is titled "Sponsored Link" and includes a link to "socialsecuritypeoplesearch.com" for "\$9.95 SSN# People Search". The bottom column is also titled "Sponsored Links" and includes links to "SafeSpy.net" for "Social Security Number", "detectiveconsultant.com" for "\$6 - \$10 SSN Search", "socialsecuritysearchusa.com" for "People Search by SSN#", "DetectiveWho.com" for "Social Security Number", "Pro-Detective.com" for "Social Security Numbers", and "People Search Experts" for "Find Someone Today. Guaranteed Results!".

# Social Security Numbers

Mid-Term Grades	
Mid-Term Exam Average Grade = 73.22	
Mid-Term Exam Median Grade = 83	
Upper Quartile >= 93	
2nd Quartile >= 83	
3rd Quartile >= 68	
Lower Quartile <= 65	
High Grade = 97	
Low Grade = 27	
Social Security Number	Mid-Term Num
43	68
90	61
15	71
39	86
11	93
98	71
04	79
35	95
64	43
61	97
45	91
17	86
04	69
02	65

http://www. .... http://www. .... edu site:umi

SSN	Final Exam	Course Grade
88 724	A	A
72 690	A	B+
78 552	C	B
68 902	B	B
80 067	C	B
80 354	B+	B
84 959	C	C+
72 932	B	B
62 340	C-	C
72 701	A	A
82 193	F	F
62 577	B	B
78 544	C	C
80 508	B	B
70 561	C	C+
70 057	F	D
74 146	C-	C
90 786	C-	D
55 901	B	B
74 573	B	B
84 791	B	B
78 085	C+	B
78 323	D	C
72 380	B	C
72 104	TF	
66 158	C+	C
74 520	C	C+
80 055	C	B
62 603	F	C
70 191	A	B
84 185	B	B
84 508	A	A
27 152	C	B
66 414	C+	C
72 051	C	C+
76 981	C	C+
72 253	B+	A
62 380	B	A
72 062	C	C
76 930	D	C
76 240	B	B
76 651	C-	C
74 780	D	D

There's no shortage of examples...

---

## Social Security Numbers

- In order to steal someone's identity, you need names.  
SSN's with names are usually blocked... aren't they?



# Social Security Numbers

Google's cache says otherwise...		
Record Number	SSN	Student Name
100	54 43	
100	64 69	
200	nd	nds
200	64 15	
200	nd	nds
200	70 09	
200	nd	nds
200	80 90	
200	60 22	
300	62 23	cot
300	62 23	cot
300	80 60	cot
400	86 10	er
400	70 24	er
500	84 22	ticut
500	76 33	ticut
500	82 84	
500	76 71	
700	60 34	JCC
200	93 08	jutas
300	12 66	luzaga

Page 1

Google's  
cache says  
otherwise...

## A tale of one city

- A city document outlining residents who are in debt to the city... A little report of names, addresses, amount owed and SSN numbers...



ACCT #	NAME	SSN	ADDRESS	AMT DUE
123-456-7890	John Doe	123456789	123 Main St, Anytown, USA	\$100.00
123-456-7891	Jane Doe	123456789	123 Main St, Anytown, USA	\$100.00
123-456-7892	Bob Smith	123456789	123 Main St, Anytown, USA	\$100.00
123-456-7893	Sarah Smith	123456789	123 Main St, Anytown, USA	\$100.00
123-456-7894	Mike Johnson	123456789	123 Main St, Anytown, USA	\$100.00
123-456-7895	Sarah Johnson	123456789	123 Main St, Anytown, USA	\$100.00
123-456-7896	David Johnson	123456789	123 Main St, Anytown, USA	\$100.00
123-456-7897	Emily Johnson	123456789	123 Main St, Anytown, USA	\$100.00
123-456-7898	Mark Johnson	123456789	123 Main St, Anytown, USA	\$100.00
123-456-7899	Christina Johnson	123456789	123 Main St, Anytown, USA	\$100.00

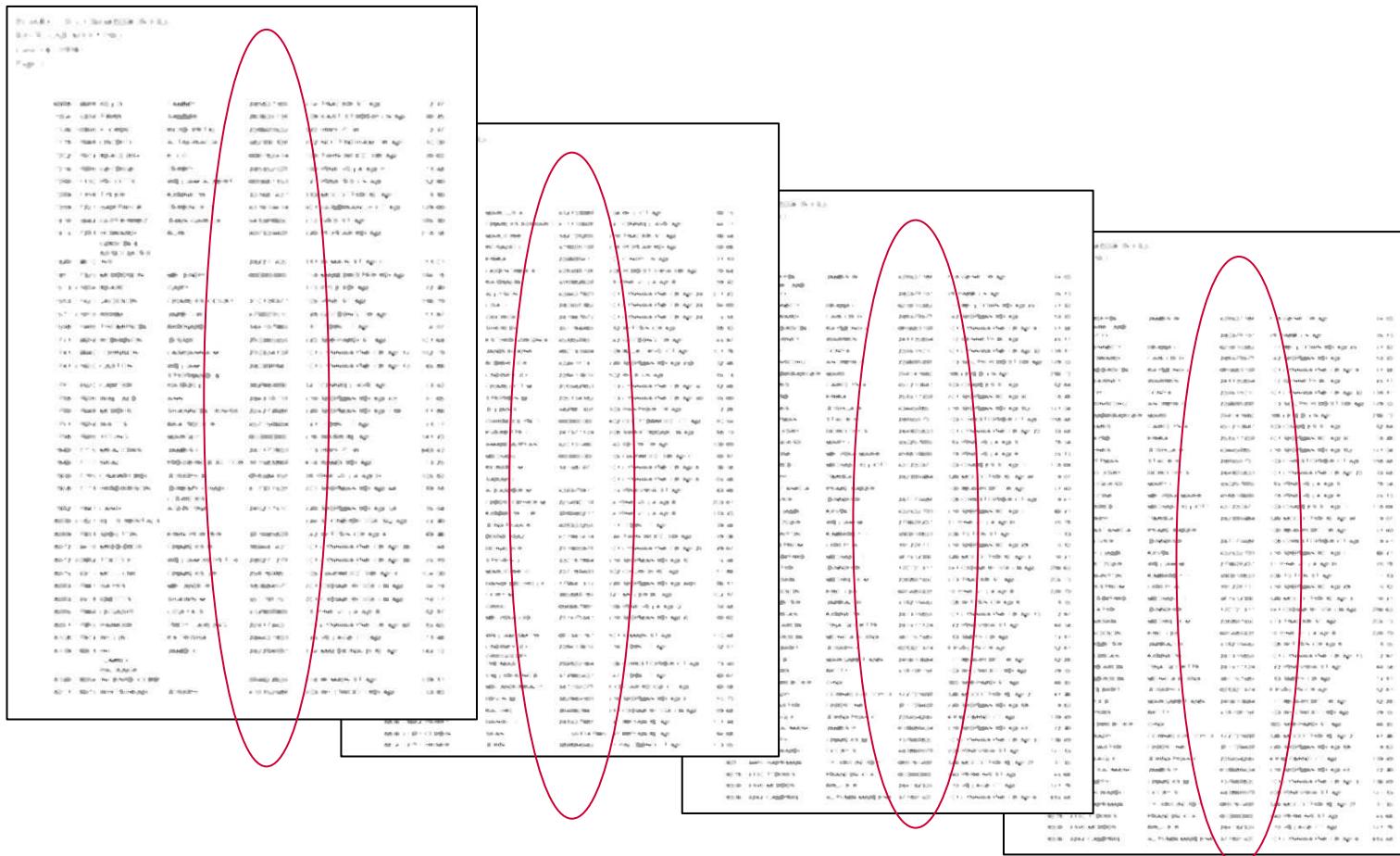
# A tale of one city

- Or perhaps more than a little report...

id	name	lat	lon	id	name	lat	lon
1	1	45.85	109.09	1	1	45.85	109.09
2	2	45.85	109.36	2	2	45.85	109.36
3	3	45.85	109.32	3	3	45.85	109.32
4	4	45.85	109.43	4	4	45.85	109.43
5	5	45.85	109.14	5	5	45.85	109.14
6	6	45.85	109.25	6	6	45.85	109.25
7	7	45.85	109.53	7	7	45.85	109.53
8	8	45.85	109.27	8	8	45.85	109.27
9	9	45.85	109.14	9	9	45.85	109.14
10	10	45.85	109.50	10	10	45.85	109.50
11	11	45.85	109.05	11	11	45.85	109.05
12	12	45.85	109.30	12	12	45.85	109.30
13	13	45.85	109.00	13	13	45.85	109.00
14	14	45.85	109.10	14	14	45.85	109.10
15	15	45.85	109.69	15	15	45.85	109.69
16	16	45.85	109.59	16	16	45.85	109.59
17	17	45.85	109.38	17	17	45.85	109.38
18	18	45.85	109.41	18	18	45.85	109.41
19	19	45.85	109.409	19	19	45.85	109.409
20	20	45.85	109.471	20	20	45.85	109.471
21	21	45.85	109.689	21	21	45.85	109.689
22	22	45.85	109.460	22	22	45.85	109.460
23	23	45.85	109.000	23	23	45.85	109.000
24	24	45.85	109.193	24	24	45.85	109.193
25	25	45.85	109.486	25	25	45.85	109.486
26	26	45.85	109.415	26	26	45.85	109.415
27	27	45.85	109.539	27	27	45.85	109.539
28	28	45.85	109.511	28	28	45.85	109.511
29	29	45.85	109.480	29	29	45.85	109.480
30	30	45.85	109.482	30	30	45.85	109.482
31	31	45.85	109.442	31	31	45.85	109.442
32	32	45.85	109.279	32	32	45.85	109.279
33	33	45.85	109.495	33	33	45.85	109.495
34	34	45.85	109.457	34	34	45.85	109.457
35	35	45.85	109.415	35	35	45.85	109.415
36	36	45.85	109.490	36	36	45.85	109.490
37	37	45.85	109.443	37	37	45.85	109.443
38	38	45.85	109.431	38	38	45.85	109.431
39	39	45.85	109.469	39	39	45.85	109.469
40	40	45.85	109.631	40	40	45.85	109.631
41	41	45.85	109.589	41	41	45.85	109.589

# A tale of one city

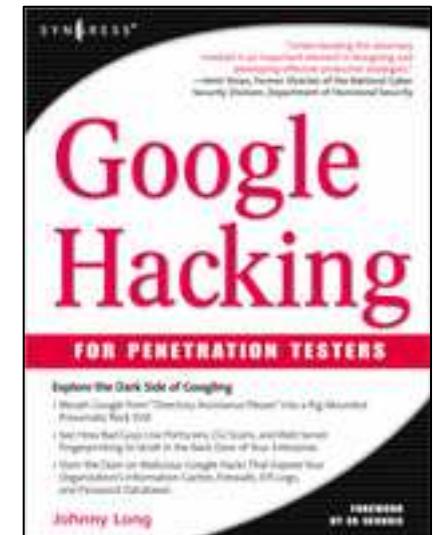
- Hundreds of city residents' personal information posted to the web... 90% including SSN and address.



---

## What we've done...

- We've skimmed “Google Hacking for Penetration Testers” by Syngress Publishing, which doesn’t seem to suck.
- We’ve looked at some great tools by Roelof Temmingh. Check out Sensepost.com.
- We’ve invaded the privacy of millions.
- We’re all still awake. Right?



---

## Thanks!

- Thanks to God for the gift of life.
- Thanks to my family for the gift of love.
- Thanks to my friends for filling in the blanks.
- Thanks to the moderators of ihackstuff.com: Murfie, Jimmy Neutron, ThePsyko, Wasabi, l0om, Stonersavant
- Thanks to Roelof T for the great code, and to the current Google Masters: murfie, jimmyneutron, klouw, l0om, stonersavant, MILKMAN, ThePsyko, cybercide, yeseins, wolveso, Deadlink, crash\_monkey, zoro25, digital.revolution, Renegade334, wasabi, urban, sfd, mlynch, Peefy, Vipsta, noAcces, brasileiro, john, Z!nCh