

I'm feeling lucky! **Google**

Google HACKING

&

Penetration testing



PIOTR KONIECZNY

konieczny@gmail.com

Dziennik Internautów, Koło Naukowe KERNEL (AGH)

Google Hacking & Penetration Testing

O czym będziemy mówić?

- **Historia jest ważna**, *choć nikt jej nie lubi...*
- **A usług to jest dużo**. *Poważnie... jest ich w ch#lerę!*
- **Szukać to znaczy...**
- **Zaawansowane operatory**
- **Google Hacking!** I'm feeling lucky! 
- **Internetowa antykoncepcja**, *czyli zapobieganie atakom*
- **SEO**, *stron WWW „pozycjonowanie” i Google'a chorowanie*
- **Ciekawostek kilka**, *żeby na koniec obudzić śpiochów :-)*

Google History

<http://www.google.com/intl/en/corporate/history.html>

<http://www-db.stanford.edu/~backrub/google.html>

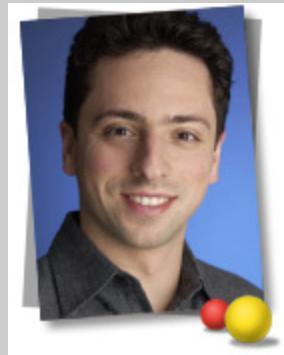
BackRub, styczeń 1996r.

Larry Page i Sergey Brin, Stanford University

CEO: Eric Schmidt, wcześniej Novell



1998 Googol to jedynka i zer stoooooooooooo...oo

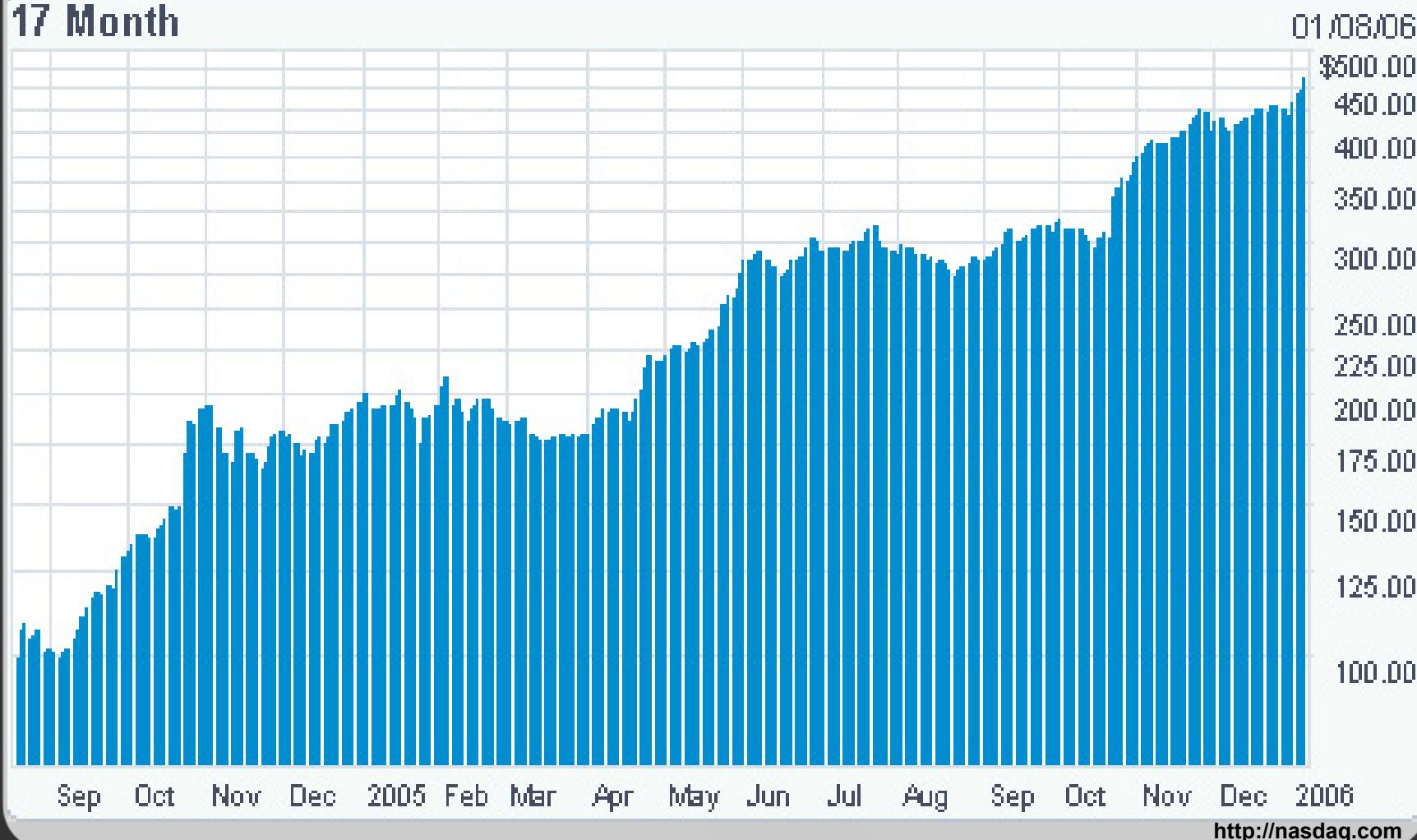


Pierwsi klienci: *Yahoo, Sun Microsystems == \$100,000*

Obecni klienci: 1 mld przez 380 mln w 112 domenach i 100 językach na m/c

Google History

17 Month



Google Services

*„Google's mission is to **organize** the world's **information** and make it universally **accessible** and **useful**“*

Do NO evil!

<http://www.google.com/press/descriptions.html>



Google Services

AdWords & AdSense

<http://answers.google.com/>
<http://www.google.com/alerts>
<http://www.base.google.com>
<http://www.google.com/blogsearch>

<http://books.google.com/>
<http://catalogs.google.com/>
<http://www.google.com/dirhp>
<http://froogle.google.com/>

<http://gmail.google.com/>
<http://www.google.com/talk/>

<http://groups.google.com/>
<http://images.google.com/>

\$\$\$, zapraszamy do reklamy

\$\$\$, dochodowy interes
WWW, news, groups

\$\$\$, znana także jako Print

katalog DMOZ


2,5++ GiB
Jabber/XMPP

Usenet od 1981r.

Google Services

<http://maps.google.com/>

<http://earth.google.com/>

<http://www.google.com/transit>

<http://labs.google.com/ridefinder>

local search, Directions

rozbudowane mapy w 3D

komunikacja miejska

TAXI

<http://mobile.google.com/>

<http://www.google.com/sms/>

<http://www.google.com/glm/>

<http://www.dodgeball.com/>

tylko UK i USA; 46645 == GOOGL

local for mobile

I'm feeling lucky!



<http://news.google.com/>

<http://www.google.com/ig>

<http://www.google.com/psearch>

<http://www.google.com/reader>

personalized Homepage

personalized Search, History, Trends

czytnik RSS via WWW

<http://video.google.com/>

\$\$\$, nie ma niczego ciekawego w TV? ;-)

Google Services

- <http://www.google.com/webhp?complete=1> *suggest*
- <http://labs.google.com/sets> *bliskoznacznie*
- <http://www.google.com/services/siteflavored.html>
- <http://scholar.google.com/>
<http://www.google.com/options/specialsearches.html>
US, Linux, MS, BSD, Apple, Universities
- <http://www.blogger.com/>
<http://www.orkut.com>
- <http://code.google.com/>
<http://code.google.com/apis.html>



AdWords; Blogger; Deskbar; Google Desktop; Earth; Froogle; Gmail; Google Homepage API; Groups; Maps; News; Search Appliance; Talk; Web search; Video;

Google Services

<http://desktop.google.com/>

<http://toolbar.google.com/>

<http://toolbar.google.com/desobar/>

<http://toolbar.google.com/firefox/extensions/>

<http://toolbar.google.com/dc/offerdc.html>

<http://pack.google.com/>

programy

<http://picasa.google.com/index.html>

<http://www.hello.com/>

photo IM

http://www.google.com/language_tools

<http://webaccelerator.google.com/>

<http://services.google.com/tcbin/tc.py>

przetłumacz



Google **Business** Search
Appliance / Mini

Wi-Fi

A screenshot of the Google Dashboard interface, showing various services and news items:

- Email:** Graduating soon and embarking on a trip (Diana Stewart, 1 hr ago); I'm back in town! (Michael Anderson, 5 hrs ago); Change in plans for meeting tomorrow (Derek Jones, Aug 12).
- News:** Assessing the Effect of Taxes on the Economy (San Francisco Chron, 4 hrs ago); Swiss shares close higher, trackin Wall St (Forbes, 4 min ago); Intelset in talks to buy New Skies-source (Reuters, 4 min ago).
- Web Clips:** Australia 2-2 Scotland (BBC Sport, 1 hr ago); Oil prices fall by more than 4% (CNN News, 2 hrs ago); A Bar at the Heart of the Milky Way (Scientific American, 2 hrs ago).
- Scratch Pad:** - Buy Flowers; - Get the car washed.
- Photos:** A large image of a red tulip.
- Stocks:** DJIA 10562.25 +48.80 Today; May be delayed up to 20 minutes.
- Weather:** Mountain View, CA (77° | 59° Today; 72°F | 74° | 58° Thu).
- Quick View:** Sandras_analysis.xls; http://www.nytimes.com; NewYorkTravel_0805.doc; http://www.blogger.com; SalesDeck01.ppt; Sunset05.jpg.

Type to search

Google Services

Usługi dla webmasterów:

<http://www.google.com/analytics/>

<https://www.google.com/webmasters/sitemaps/login>

...ale o tym wspomniemy później.



A

B

C

D

E

Google search interface showing a search for "google address mountain view". The results page includes links for Web, Images, Groups, News, Froogle, Local, more, Advanced Search, and Preferences.

F - Web Results 1 - 10 of about 87,500 for google [address +mountain view](#). (0.31 seconds)

G - Tip: Find maps by searching for a street address with city or zip code

News results for [google](#)



[Google Slices and Dices by Locality](#) - InternetNews.com - 1 hour ago

[Google Rolls Out System To Improve Local Search Results](#) - InternetWeek.com - 5 hours ago

H

I - [Google](#)

... Advertise with Us - Business Solutions - Services & Tools - Jobs, Press, & Help ©2004 Google - Searching 4,285,199,774 web pages.

<http://www.google.com/> - 3k - [Cached](#) - [Similar pages](#)

K

L

M

N

J

O - [Google Corporate Information: Google Offices](#)

... 1600 Amphitheatre Parkway Mountain View, CA 94043. ... Turn right onto CHARLESTON Drive past Landings Drive; Turn left into driveway at the "Google" sign at ...

<http://www.google.com/corporate/address.html> - 15k - [Cached](#) - [Similar pages](#)

[[More results from www.google.com](#)] P

Google Search

Wyszukiwarka Google udostępnia m.in.:

Boolean logic

Spell checker

Cached links

Similar sites

Web page translation

Inteligent guessing -- Stock quotes, Books, Movies, Froogle, IMGs

<http://google.com/search?q=birthplace+of+John+Paul+II>

<http://google.com/search?q=population+of+Poland>

<http://google.com/search?q=gas+Ukraine>

Street maps

Calculator

Definitions

Search by number *Travel*

Phone book

<http://google.com/search?q=0141>

Google Search

Z czym to się je? Założenia i operatory:

NOT case sensitive

(CZE pOkliKash? == cze poklikash?)

Automatyczne założenie iloczynu "**AND**" (+)

(patrz URL)

Automatyczne wykluczenie popularnych słów

operator + przywraca słowo

| (pipe lub **OR**)

== suma/alternatywa

- (minus)

== wykluczenie terminu

~ (tylda)

== synonim

"wyrażenia" lub . (kropka)

== dokładne wyrażenie

* (gwiazdka)

== dowolne słowo

http://google.pl/search?q=mam+*+lat

Wariacje słowne

(**smieszne reklamy** == **śmieszne reklamy**)

Google Search

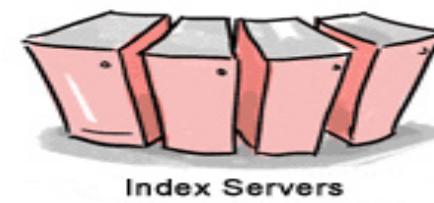


3. The search results are returned to the user in a fraction of a second.

1. The web server sends the query to the index servers. The content inside the index servers is similar to the index in the back of a book - it tells which pages contain the words that match the query.



2. The query travels to the doc servers, which actually retrieve the stored documents. Snippets are generated to describe each search result.



Google Search

Google Grid / Google FileSystem

The Power Behind Google (*Michael Feldman, HPCWire*)

kudos to Olaf

<http://news.taborcommunications.com/msgget.jsp?mid=534736>

Google Compute (*with Stanford University*)

!!! obsolete !!!

<http://toolbar.google.com/dc/offerdc.html>

Google BruteForce Indexing???

:)



```
crawl-66-249-65-70.googlebot.com - - [08/Jan/2006:08:30:02 -0500] "GET /paper/?N=D  
HTTP/1.1" 200 863 "-" "Mozilla/5.0 (compatible; Googlebot/2.1;  
+http://www.google.com/bot.html)"
```

```
crawl-66-249-71-1.googlebot.com - - [08/Jan/2006:00:36:49 -0500] "GET / HTTP/1.0"  
200 6591 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
```

```
crawl-66-249-65-70.googlebot.com - - [08/Jan/2006:05:54:26 -0500] "GET / HTTP/1.1"  
200 6591 "-" "Mediapartners-Google/2.1"
```

Google Search

URL prawdę Ci powie...

http://foo.bar?parametr1=wartosc1&p2=w2

hl=en -- header language / interface (*ustawienia przeglądarki*)

lr=lang_pl -- język stron WWW, w których szukamy

num=50 -- ilość wyników na stronie z rezultatami

btnI -- I'm lucky mode [REDIRECT]



strip=1 -- gdy oglądamy stronę z cache [ANONYMOUS (?) PROXY]

http://www.google.com/webhp?complete=1 -- *Google Suggest*

Google Search

Zaawansowane operatory

OPERATOR: PYTANIE

inurl:

allinurl:

intitle:

allintitle:

intext:

inanchor:

filetype:

<http://google.pl/search?q=sex+filetype:jpg>

numrange:

date:

define:

site:

link:

cache:

info:

<http://google.pl/search?q=85103100000..85103199999>

każdy ma PESEL

3,6,12, bądź zakres

I'm feeling lucky!



<http://google.pl/search?q=define:WTF>

które są zaindeksowane?

<http://google.pl/search?q=site:piko.jogger.pl>

gdzie o nas mówią?

<http://google.pl/search?q=link:piko.jogger.pl>

[http://google.pl/search?q=cache:piko.jogger.pl &strip=1](http://google.pl/search?q=cache:piko.jogger.pl&strip=1)

co Google o nas wie?

<http://google.pl/search?q=info:piko.jogger.pl>

Google Search

Niektóre z obsługiwanych formatów:

HyperText Markup Language (**html**)

Adobe Portable Document Format, PostScript (**pdf, ps**)

Lotus 1-2-3 (**wk1, wk2, wk3, wk4, wk5, wki, wks, wku, lwp**)

MacWrite (**mw**)

Microsoft Office (**xls, ppt**)

Microsoft Word (doc) + <http://lcamtuf.coredump.cx/soft/therenv.tgz> = :-)

Microsoft Works (**wks, wps, wdb**)

Microsoft Write (**wri**)

Rich Text Format (**rtf**)

Shockwave Flash (**swf**)

Text (**ans, txt**)



...i dużo więcej!

!!! Google umożliwia niekiedy konwersję w/w do HTML

Calculator

* Konwersje

0x7d3 in roman

<http://google.com/search?q=0x7d3+%2B+3+in+roman>

* Równania

0x3 + 0b010 in decimal

<http://google.pl/search?q=0x3+%2B+0b010+in+decimal>

* Przelicznik walut

1GBP in PLN

<http://google.pl/search?q=1GBP+in+PLN>

...ale brak obliczania masek podsieci :(

A screenshot of a Google search results page. At the top, there's a navigation bar with links for Web, Images, Groups, News, Froogle, Local, and more. Below the search bar, it says "half a cup in teaspoons". On the right, there are buttons for Search, Advanced Search, and Preferences. The main content area shows a "Web" result with a calculator icon and the text "half (1 US cup) = 24 US teaspoons".

Web



half (1 US cup) = 24 US teaspoons

[More about calculator.](#)

Google HACKING

- * **Google pobiera dane ze stron WWW...**
...a strony WWW z Internetu i z Opery
(wyłącz reklamy AdSense lub zrób upgrade przeglądarki do najnowszej, darmowej wersji)
<http://opera.com>
- * **To nie jest wina Google, że znajduje poufne informacje**
(nauczmy się, jak nie dopuścić do tzw. **information leak**)

I'm feeling lucky! 
Czym wg Ciebie jest hacking?

^G "czym * ciebie jest (hacking|haking)" group:alt.pl.comp.os.hacking

„Hacking to robienie czegoś z4j3b15c13 dobrze!”

kudos to Bulba @ apcoh

Google HACKING

Znajdziemy i bezwzględnie wykorzystamy :-)

Serwery podatne na atak

nasz główny cel

Błędy w aplikacjach WWW

o przydatne dane, przydatne!

Pliki i katalogi

zawierające hasła, dane osobowe, logi firewalla, mp3

Ciekawe narzędzia

pomocne atakującemu

Numery kart kredytowych

*ale nie w trakcie wykładu *EG**

Urządzenia sieciowe

routery, switche, i inne

I'm feeling lucky!



Google HACKING

Let's do the evil!

^G index.of mp3 ich.troje

(113 sępów miłości na chwilę obecną)

<http://www.google.com/search?q=intitle%3Aindex.of+mp3+ich.troje>

^G inurl:microsoft filetype:iso

(spróbuj z windows)

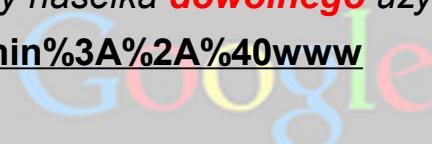
<http://www.google.com/search?q=inurl%3Amicrosoft+filetype%3Aiso>

^G http://admin:*@www

(i mamy hasło **dowolnego** użytkownika!)

<http://www.google.com/search?q=http%3A%2F%2Fadmin%3A%2A%40www>

I'm feeling lucky!



^G "sets mode: +k"

(IRC anybody?)

<http://www.google.com/search?q=%22sets+mode%3A+%2Bk%22>

^G filetype:bak inurl:"htaccess|passwd|shadow|htusers"

(OMG!)

<http://google.com/search?q=filetype%3Abak+inurl%3A%22htaccess%7Cpasswd%7Cshadow%7Chtusers>

Google HACKING

Zbieraj plony -- niezabezpieczone katalogi na serwerach TPSA

^G intitle:index.of server.at site:tpsa.pl

Struktury katalogów, adresy usług SSH/FTP z loginami a czasem hasłami

^G cd ls bash_history

Naucz się wykorzystywać wadliwe skrypty cgi do listowania plików

^G allinurl:/random_banner/index.cgi

Żeruj na ludzkiej głupocie

^G intitle:index.of inurl:admin inurl:backup

^G passwd.bak intitle:index.of

^G intitle:index.of secring.pgp

^G intitle:index.of..etc passwd

^G "admin account info" filetype:log

^G "Access denied for user" "using password"



(honeypots...)

(SQL!)

Poznaj nametags serwerów i wykorzystaj ich błędy

^G allintitle:Welcome to Windows NT 4.0 Option Pack

Google HACKING

Plik Edycja Widok Zakładki RSS Narzędzia Okno Pomoc

http://www.virtustest.de/Server/server.log

onet sz-r pk/jog Cspk IS DI hkin' apcoh Gm AdS ppo mp G the typewriter-keyb...

Gmail - [KERNEL...], PANEL REDAKT..., The Lemon Battery, OceanStore, The Power Behin... Gi

----- log started at 07-08-05 18:06 -----

```
07-08-05 18:06:12,ALL,Info,server,      Server init initialized
07-08-05 18:06:12,ALL,Info,server,      Server version: 2.0.20.1 Win32
07-08-05 18:06:13,WARNING,Info,SQL,     created table ts2_servers
07-08-05 18:06:13,WARNING,Info,SQL,     created table ts2_server_privileges
07-08-05 18:06:13,WARNING,Info,SQL,     created table ts2_channels
07-08-05 18:06:13,WARNING,Info,SQL,     created table ts2_channel_privileges
07-08-05 18:06:13,WARNING,Info,SQL,     created table ts2_clients
07-08-05 18:06:13,WARNING,Info,SQL,     created table ts2_bans
07-08-05 18:06:13,ALL,Info,server,      Starting VirtualServer id:1 with port:8767
07-08-05 18:06:13,WARNING,Info,SERVER,   Default VirtualServer created
07-08-05 18:06:13,WARNING,Info,SERVER,   admin account info: username: admin password: [REDACTED]
07-08-05 18:06:13,WARNING,Info,SERVER,   superadmin account info: username: superadmin password: [REDACTED]
07-08-05 18:06:13,ALL,Info,server,      Server init finished
07-08-05 18:07:48,ERROR,All,frmMain,    unable to detect external ip
```



We're sorry...

... but we can't process your request right now. A computer virus or spyware application is sending us automated requests, and it appears that your computer or network has been infected.

We'll restore your access as quickly as possible, so try again soon. In the meantime, you might want to run a [virus checker](#) or [spyware remover](#) to make sure that your computer is free of viruses and other spurious software.

We apologize for the inconvenience, and hope we'll see you again on Google.

Google HACKING

Złe robale! -- dzięki nim Google blokuje nam wyniki

^G "powered by PHPbb2 2.0.6..10"

^G inurl:index.php AND inurl:phpbb

Hacking Google Hacking :-)

...bo wiele jest dróg...

^G "p_o_w_e_r_e_d by PHPbb2 2.0.6..10"

^G iNdEx inurl:PHPbb filetype:php

Do czego może się przydać szukanie wulgaryzmów?

^G site:wp.pl dupa



Spam harvesters – chrońcie się!

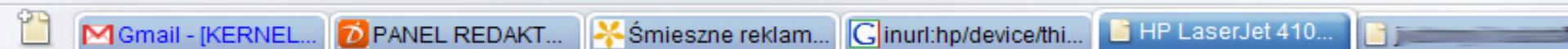
^G emails.xls

jakie mogą być inne nazwy pliku?

^G *.gmail.com

Panie administratorze, podrukujemy razem?

<http://google.com/search?q=inurl:hp/device/this.LCDDispatcher>



HP LaserJet 4100 Series / [REDACTED] HP LaserJet 4100 Series

[Home](#) [Device](#) [Networking](#)[Printer Status](#)[Configuration Page](#)[Supplies Status](#)[Event Log](#)[Device Information](#)[Other Links](#)[My Printer](#)[Order Supplies](#)[Solve A Problem](#)

Printer Status

[Supplies](#)[Media](#)[Capabilities](#)

Control Panel

READY

Ready

Data

Attention

[Control Panel Help](#)[Refresh Control Panel](#)[Help](#)

Set Refresh Rate:

0 minutes

[Apply](#)[Cancel](#)

Supplies

% of Life Remaining

Black



74%

Media

Status
OK
OK
OK
OK

Input/Output

Size

Type

TRAY 3

LETTER

PLAIN

TRAY 2

LETTER

PLAIN

TRAY 1

LETTER

PLAIN

STANDARD OUTBIN

N/A

N/A

OPTIONAL BIN 1

N/A

N/A

Google HACKING

- intitle:phpMyAdmin "Welcome to phpMyAdmin ***" "running on * as root@*" 

 - inurl:explorer.cfm inurl:(dirpath|This_Directory) 

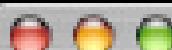
intext:SQLiteManager inurl:main.php

Counterstrike Server Configs

 http://66.102.7.104/search?q=cache:L...r.cfg++rcon+password&hl=de&start=11



- inurl:server.cfg rcon password



Proxies ihackstuff

Switch

Command

Output

```
Command base-URL was: /level/15/exec/-  
Complete URL was: /level/15/exec/-/show  
Command was: show
```

access-lists

 List access lists

accounting

 Accounting data for active sessions

adjacency

 Adjacent nodes

aliases

 Display alias commands

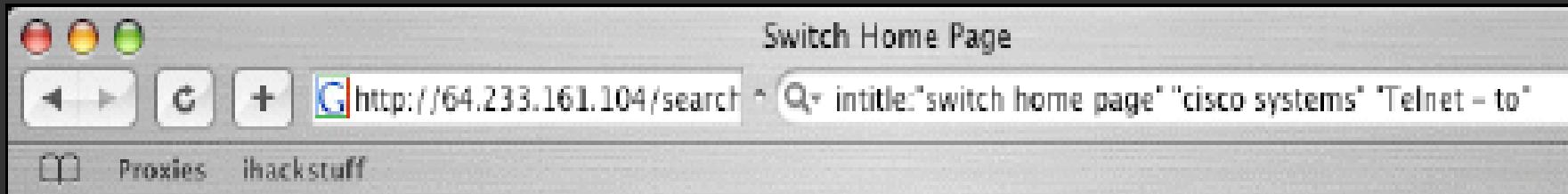
arp

 ARP table

CISCO Switch

Kudos to Jimmy Neutron

Google HACKING



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.

Google HACKING

Co jeszcze możemy popsuć razem z Google?

Simple Redirect i zero prywatności

<http://google.com/search?q=%C5%9Bmieszne+reklamy+telewizyjne&btnI>

```
195.85.229.2 -- [09/Jan/2006:10:20:45 -0500] "GET / HTTP/1.1" 200 6591 "-" "Opera/8.10  
(X11; Linux i686; U; en)" //nasze IP
```

Anonymous (?) Proxy

<http://216.239.51.104/search?q=cache:piko.jogger.pl&strip=1>

<http://translate.google.com/translate?u=http://sztuka-reklamy.info&langpair=pl|pl>

```
216.239.36.136 -- [09/Jan/2006:10:18:43 -0500] "GET / HTTP/1.0" 200 6591 "--"  
"Opera/8.10 (X11; Linux i686; U; en),gzip(gfe) (via translate.google.com)"
```

```
195.85.229.2 -- [09/Jan/2006:10:18:43 -0500] "GET /piko.css HTTP/1.1" 304 - "--"  
"Opera/8.10 (X11; Linux i686; U; en)" //to już nasze IP!
```

```
195.85.229.2 -- [09/Jan/2006:10:18:44 -0500] "GET /_img/tv.jpg HTTP/1.1" 304 - "--"  
"Opera/8.10 (X11; Linux i686; U; en)" //to już nasze IP!
```

Google HACKING

Honeypots

trzeba mieć oczy dookoła serwera i wiedzieć co w trawie piszczy!

Cache sliding

gdy strona zniknie, a cache: rozplynie się we mgle...

alternatywnie: <http://www.archive.org/web/web.php>

Authorization bypassing

teoria gridowego spisku? :-)

Internetowe Robale

czy Google może blokować zapytania? -- TAK! (ale już to obeszliśmy)



Co kraj, to obyczaj

różne języki, różne wyniki... pokombinuj z ustawieniami i porównaj!

Googlebombing (metodą walki politycznej?)

kretyń ze zbrodniarzem zachorowali na ptasią grypę, co za failure!

Google HACKING



[WWW](#) [Grafika](#) [Grupy dyskusyjne](#) [Katalog](#)

failure

Szukaj

[Szukanie zaawansowane](#)
[Ustawienia](#)

Szukaj w Internecie Szukaj na stronach kategorii: Polski

[WWW](#)

[Biography of President George W. Bush](#)

Biography of the 43rd President of the United States.

[www.whitehouse.gov/president/gwbbio.html](#) - 25k - [Kopia](#) - [Podobne strony](#)



[WWW](#) [Grafika](#) [Grupy dyskusyjne](#) [Katalog](#)

zbrodniarz

Szukaj

[Szukanie zaawansowane](#)
[Ustawienia](#)

Szukaj w Internecie Szukaj na stronach kategorii: Polski

[WWW](#)

[pl.wikipedia.org/wiki/Władimir_Putin](#)

[Podobne strony](#)

Google HACKING



[WWW](#) [Grafika](#) [Grupy dyskusyjne](#) [Katalog](#)

ptasia grypa

[Szukanie zaawansowane](#)
[Ustawienia](#)

Szukaj w Internecie Szukaj na stronach kategorii: Polski

WWW

[Lech Kaczyński - Prezydent IV Rzeczypospolitej](#)

Aktualności z kampanii wyborczej i urzęduowania, życiorys, program wyborczy.

www.lechkaczynski.pl/ - 13k - [Kopia](#) - [Podobne strony](#)

[WWW](#) [Grafika](#) [Grupy dyskusyjne](#) [Katalog](#)

kretyn

[Szukanie zaawansowane](#)
[Ustawienia](#)

Szukaj w Internecie Szukaj na stronach kategorii: Polski

WWW

[Posel: Andrzej Lepper](#)

Posel Andrzej Lepper, Następny · Poprzedni. [Andrzej Lepper](#). Data i miejsce

urodzenia: 13-06-1954, Stowiącino Stan cywilny: żonaty ...

www.sejm.gov.pl/poslowie/posel5/189.htm - 7k - [Kopia](#) - [Podobne strony](#)

Google DNS discovering

Kto pyta, nie błędzi...

Using lynx to capture the Google results page...

...returns the same results.

Terminal — ssh — 80x24

```
root@esxi5b:~$ 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 $2}' | sort -u
http://download.microsoft.com/
http://go.microsoft.com/
http://msdn.microsoft.com/
http://msevents.microsoft.com/
http://murl.microsoft.com/
http://office.microsoft.com/
http://protect.microsoft.com/
http://research.microsoft.com/
https://a.microsoft.com/
http://support.microsoft.com/
-bash-2.05b$
```

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

Google HACKING – OBRONA

Polityka bezpieczeństwa

(but business is business...)

Opracowujemy schemat przepływu i zarządzania informacją w firmie

Edukujemy wszystkich pracowników, nie tylko panią Halinkę z kadr

Krytyczne i poufne dane trzymamy w INTRANECIE.

Używamy kryptografii i autoryzacji -- i pamiętamy o pilnowaniu kluczy :>

Usuwamy metadane z plików MS Office przed publikacją/wysłaniem !!!

Regularnie wykonujemy Information Assesments: Penetration testing & Ethical hacking

tj. automatycznie i świadomie odpytujemy ^G poprzez specjalne skanery.

Google zabrania automatycznego odpytywania swojej wyszukiwarki.

Trzeba postarać się o licencję dla programów korzystających z Google API.

Google HACKING – OBRONA

Plik .htaccess

```
xerror@szynszyl:~/public_html> ls -al
-rw-r--r--  1 xerror  ftjgrp        90 Jan  4 20:29 .htaccess
-rw-r--r--  1 xerror  ftjgrp      113 Jan  5 16:38 head.html
-rw-r--r--  1 xerror  ftjgrp      15 Jan  5 16:38 tail.html
```

```
xerror@szynszyl:~/public_html> cat .htaccess
HeaderName head.html
IndexOptions +FancyIndexing +SuppressHTMLPreamble
ReadmeName tail.html
```

```
xerror@szynszyl:~/public_html> cat head.html
<html>
<head><title>foobar</title></head>
Pliki w katalogu
```

```
xerror@szynszyl:~/public_html> cat tail.html
<b>foo</b> bar -- <i>Niestraszni nam szablonowi Googleszperacze!</i>
```



Google HACKING – OBRONA

Plik Edycja Widok Zakładki RSS Narzędzia Okno Pomoc

http://[REDACTED]/~xerror/

onet sz-r pk/jog C&pk IS DI hkin' apcoh Gm AdS ppo

Gmail - goog... PANEL RED... Śmieszne re... inurl:hp/devic... HP LaserJ

Pliki w katalogu

	Name	Last modified	Size	Description
[DIR]	Parent Directory	04-Jan-2006 20:23	-	
[TXT]	head.html	09-Jan-2006 17:49	1k	
[TXT]	tail.html	09-Jan-2006 17:50	1k	

foo bar! -- Niestraszni nam szablonowi Googleszperacze!

Google HACKING – OBRONA

Plik Robots.txt

Przestrzega go większość robotów internetowych.

```
User-agent: Googlebot | * | Googlebot-Image  
Disallow: / | /lemury | /*.gif$ | /*?
```

Nagłówek strony WWW

```
<META NAME="ROBOTS" CONTENT="NOINDEX,NOFOLLOW,NOARCHIVE">  
<META NAME="GOOGLEBOT" CONTENT="NOINDEX, NOFOLLOW">  
<a href="http://www.przyklad.com/" rel="nofollow">Bez spamu mi tu!</a>
```

Usuwamy stronę z wyników Google'a

<http://www.google.com/webmasters/remove.html>

Search Engine Optimization

WWW [Grafika](#) [Grupy dyskusyjne](#) [Katalog](#)
 [Szukanie zaawansowane](#)
 Szukaj w Internecie Szukaj na stronach kategorii: Polski

WWW Wyniki 1 - 10 spośród około 3,920,000 w języku Polski dla zapytanie pozycjonowanie. (Znaleziono w 0,04 sek.)

Skuteczne Pozycjonowanie
www. [.pl](#) Wskocz na pierwsze miejsca Lata doświadczeń, bogate portfolio

pozycjonowanie stron - TANIO - pozycjonowanie stron ...
Pozycjonowanie, tworzenie stron, pozycjonowanie stron. Oferujemy tanio: tworzenie stron, wysokie pozycjonowanie stron w wyszukiwarkach - Google, Onet, WP, ...
www. [.pl](#) - 11k - [Kopia](#) - [Podobne strony](#)

Pozycjonowanie i Optymalizacja - SEO Forum, Hosting, Webhosting ...
Pozycjonowanie stron internetowych. Pozycjonowanie i Optymalizacja Forum -
Pozycjonowanie i optymalizacja stron internetowych. Otwarta rozmowa na temat ...
forum.optymalizacja.com/ - 58k - 11 2006 - [Kopia](#) - [Podobne strony](#)

Pozycjonowanie stron www - Skuteczne i tanie ...
Pozycjonowanie stron - Oferujemy profesjonalne i niedrogie pozycjonowanie stron www.
Dzięki nam Twoja strona będzie pierwsza! Reklama witryn, pozycjonowanie ...
pozycjonowanie [.pl](#) - 8k - [Kopia](#) - [Podobne strony](#)

Wyszukiwarki i pozycjonowanie stron - kilka użytecznych porad
Pozycjonowanie stron zaliczamy do form promocji o największym współczynniku zysk/cena. Poznaj sekrety pozycjonowania i ciesz się wysoką oglądalnością.
www. [.pl](#) - 24k - 11 2006 - [Kopia](#) - [Podobne strony](#)

Link sponsorowany

Linki sponsorowane

- pozycjonowanie
Poważne podejście do tematu
Strategia, optymalizacja, raporty.
www. [.pl](#)

Pozycjonowanie stron www
Skuteczne pozycjonowanie stron
Kampanie reklamowe w sieci
www. [.pl](#)

Darmowe pozycjonowanie
Pozycjonuj własną stronę i zarabiaj
Darmowy program wymiany linków.
www. [.pl](#)

Pozycjonowanie
Pozycjonowanie stron www
Tania i skuteczna reklama w sieci
www. [.pl](#)

Kampanie internetowe
Wy promuj swoją firmę w Internecie

Search Engine Optimization

Jeden z **największych** problemów Google

Etyczne dopuszczalne, moralnie haniebne? (spam!)

Bilans **zysków i strat** ale okraszony współczynnikiem **ryzyka**

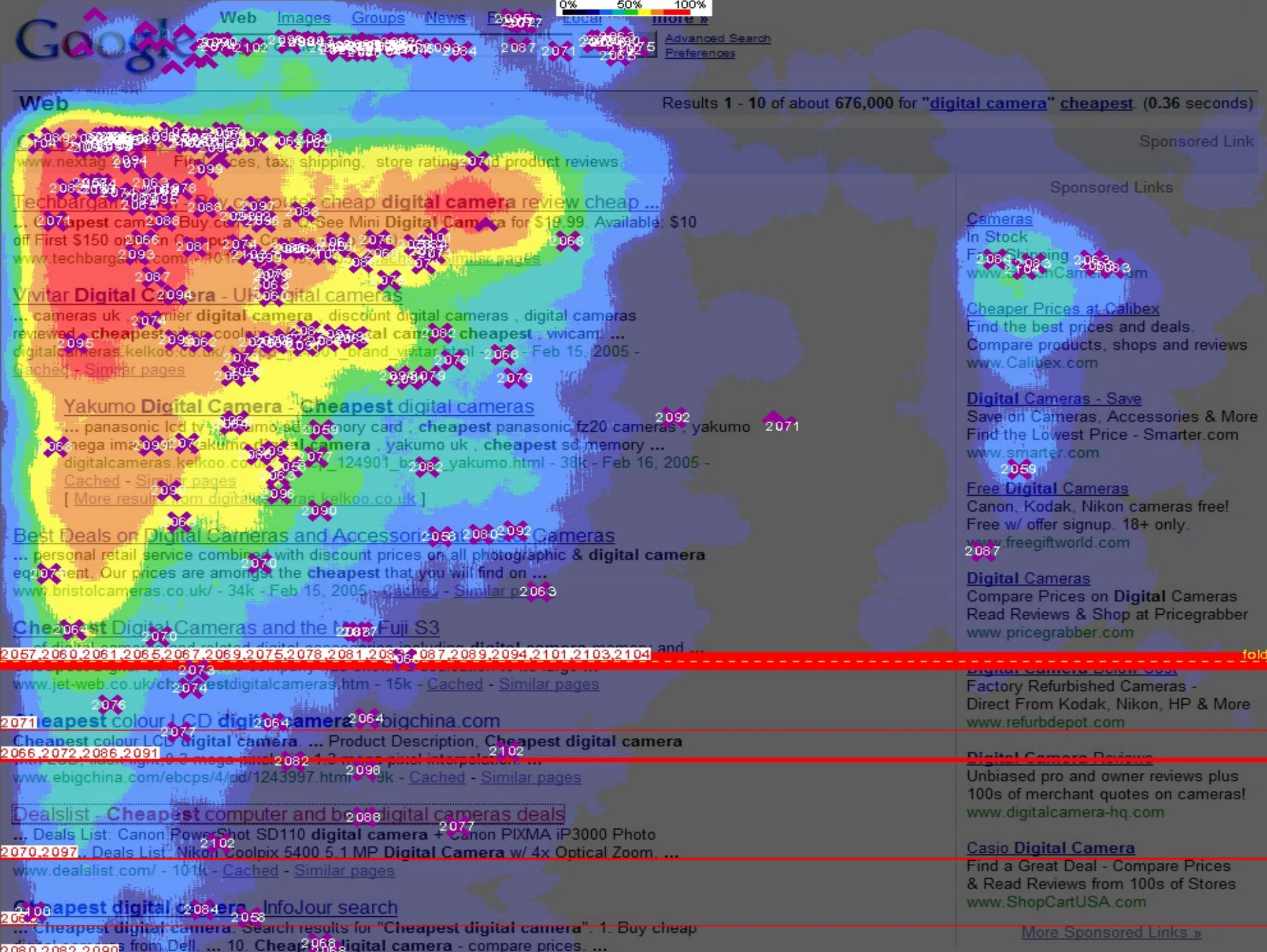
-- *pozycjonowanie narusza regulamin Google*

-- *nasza strona może trafić do tzw. **sandbox***



Czy warto więc pozycjonować strony WWW?

Wszystko stanie się jasne, kiedy spojrzymy na wykresy...



Search Engine Optimization

Technologia Google

- PageRank *pozycja strony nie zależy od niego!*
- Analiza dopasowań hipertekstowych
- Linki, linki, linki!

http://en.wikipedia.org/wiki/List_of_websites_with_a_high_PageRank

Techniki SEO:

Cloaking; Doorway/jump pages,,

Link spam: programy wymiany linków/reklamy, księgi gości/fora

<http://www.google.com/addurl/?continue=/addurl>

<https://www.google.com/webmasters/sitemaps/>

<http://www.google.com/analytics/>

<http://www.google.com/intl/en/webmasters/>

<http://www.google.com/contact/spamreport.html>

<http://www.mcdar.net/dance/>

http://www.webworkshop.net/pagerank_calculator.php3



w wielu datacenter

Pluginy do przeglądarek pokazujące PageRank

Opera: <http://piko.jogger.pl/comment.php?eid=140360>

Search Engine Optimization

Dobrze dobrana domena!

(nazwa, wiek)

Przemyślana kompozycja strony

Wyszczególnione słowa kluczowe

```
<title> <hX> <b> <strong> <em> <i> <u> <li> <dfn>
```

Opisane linki i multimedia

```
<a href="http://sztuka-reklamy.info"  
    title="śmieszne reklamy">
```

śmieszne reklamy telewizyjne

```

```

...dużo linków do naszej strony i trochę czasu.

Search Engine Optimization

Najbardziej poszukiwane w 2005:

Świat:

1. janet jackson
2. hurricane katrina
3. tsunami
4. xbox 360
5. brad pitt
6. michael jackson
7. american idol
8. **britney spears**
9. angelina jolie
10. harry potter

Polska:

1. wikipedia
2. harry potter
3. wróżby andrzejkowe
4. britney spears
5. paris hilton
6. media markt
7. suknie ślubne
8. opony
9. kolorowanki
10. ptasia grypa



<http://www.google.com/intl/en/press/zeitgeist.html>

Tsunami

Earthquake

Hurricane

Tsunami

Rita September 18-25

Katrina August 23-30

Wilma October 15-25

Indian Ocean 9.0 earthquake Dec 26

Hurricane Dennis

December 04

Sumatra 8.7 quake March 28

Kashmir region 7.6 quake October 8

December 05

Google'a PLANY NA PRZYSZŁOŚĆ

Do no evil ----??"--> *Make people think we do no evil*

Google wyznaje zasadę zabawy:

Zbudujmy narzędzie, które będzie popularne. Zyski przyjdą same.

Budowanie narzędzia jest interaktywne.

Użytkownicy bawiąc się usługą określają jej charakter.

Google chce być miejscem, gdzie przechowujesz życie:

Altruizm czy strategia? centralizacja czy monopol?

Liczne serwisy i usługi – nie tylko elektroniczne!

Coraz więcej zbieranych i _przetwarzanych_ danych

por. <http://oceanstore.cs.berkeley.edu/index.html> – kudos to erfi

Setki kilometrów nieużywanych światłowodów ciągnących się przez całą Amerykę...

Nowe usługi/programy potrzebują większej przepustowości?

Uzależnienie użytkowników poprzez stanie się ISP?

Google Linux Based Operating System?

Google'a PLANY NA PRZYSZŁOŚĆ

A może własna przeglądarka? :-)

```
xerror@szynszyl:~$ whois gbrowser.com
```

```
[...]
```

Registrant:

Google Inc. (DOM-1278108)
1600 Amphitheatre Parkway
Mountain View CA 94043
US

```
[...]
```

I'm feeling lucky!



Created on.....: 2004-Apr-26.

Expires on.....: 2006-Apr-26.

Record last updated on...: 2004-Apr-26 16:46:39.

```
[...]
```

Google BASED

Logle

<http://www.logogle.com/>

Piotr Konieczny

[Web](#) [Images](#) [Groups](#) [News](#) [Froogle](#) [Local](#) [Logogle\(top\) »](#)

Google Search

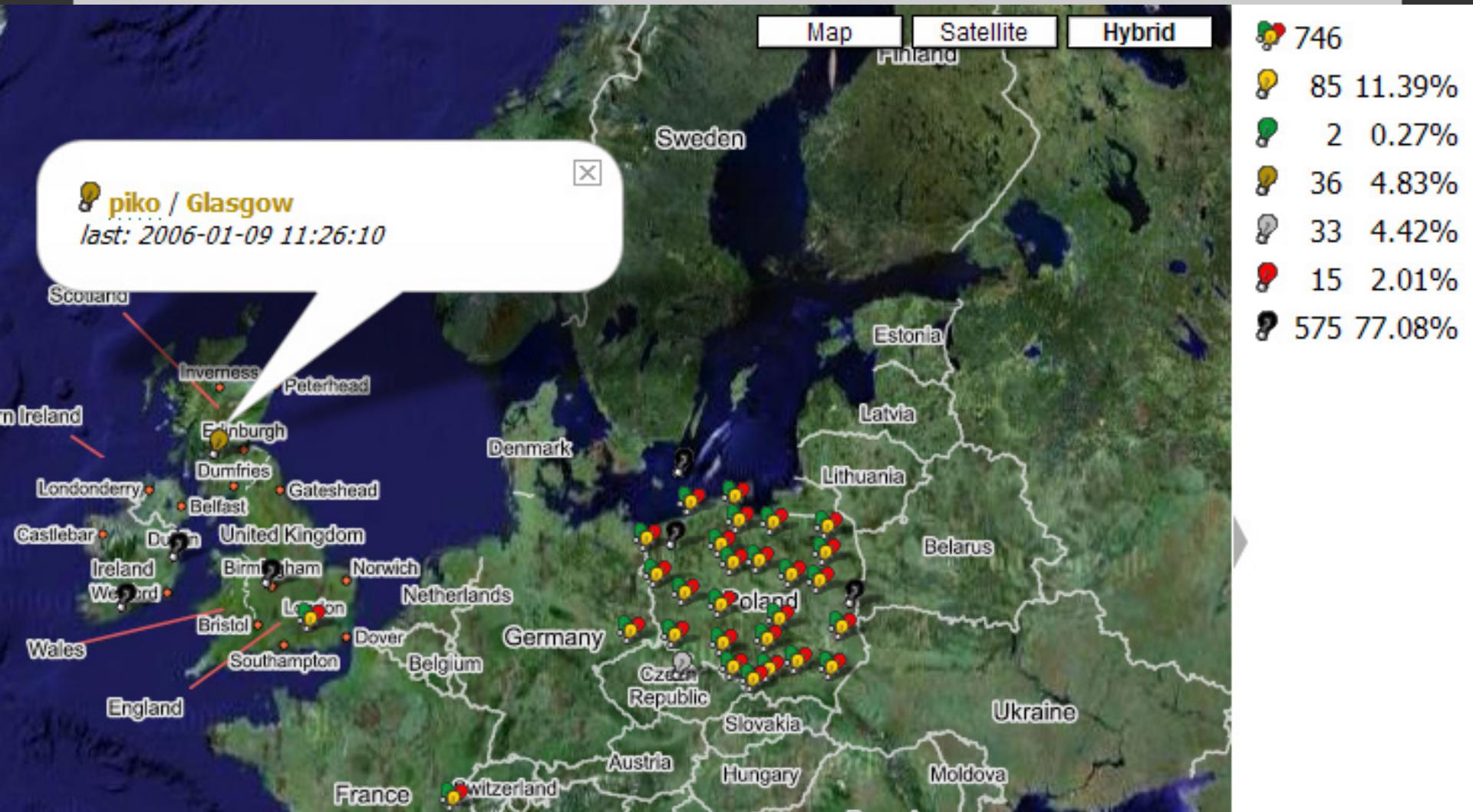
[BookMark\(for IE\)](#) - [Google Logo Maker](#)

©2005 Logogle

Google BASED

Jobble

<http://jobble.uaznia.net>



Google BASED

Google Fight

<http://www.googlefight.com/>

Results on Google :

firefox

145,000,000 results

opera

258,000,000 results

firefox

opera

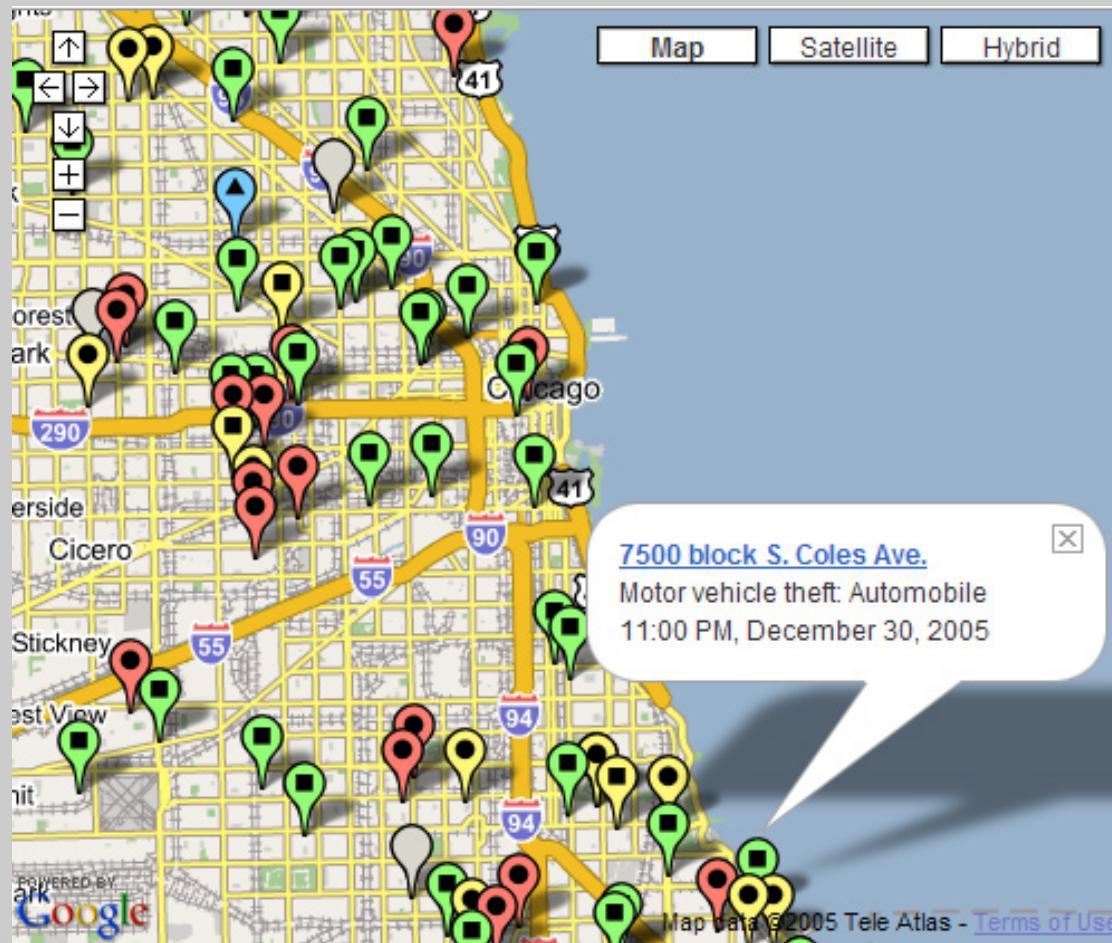
Make a fight

gle

Google BASED

Chicago Crimes

<http://www.chicagocrime.org/map/>



Filter crimes

All locations

All crime types

All districts

Oct. 2, 2005 to Dec. 30, 2005

Midnight to Next midnight

Crime classifications key

- (Red circle) Person
- (Yellow circle) Person (domestic)
- (Green square) Property
- (Yellow square) Property (domestic)
- (Blue triangle) Society
- (Yellow triangle) Society (domestic)

Google BASED

Catty

<http://lcamtuf.coredump.cx/c3.shtml>



Catty v3

Copyright (C) 2001-2004 by Michal Zalewski (lcamtuf@coredump.cx)

Now talking with 195.85.229.2 (conversation counter: 134979).

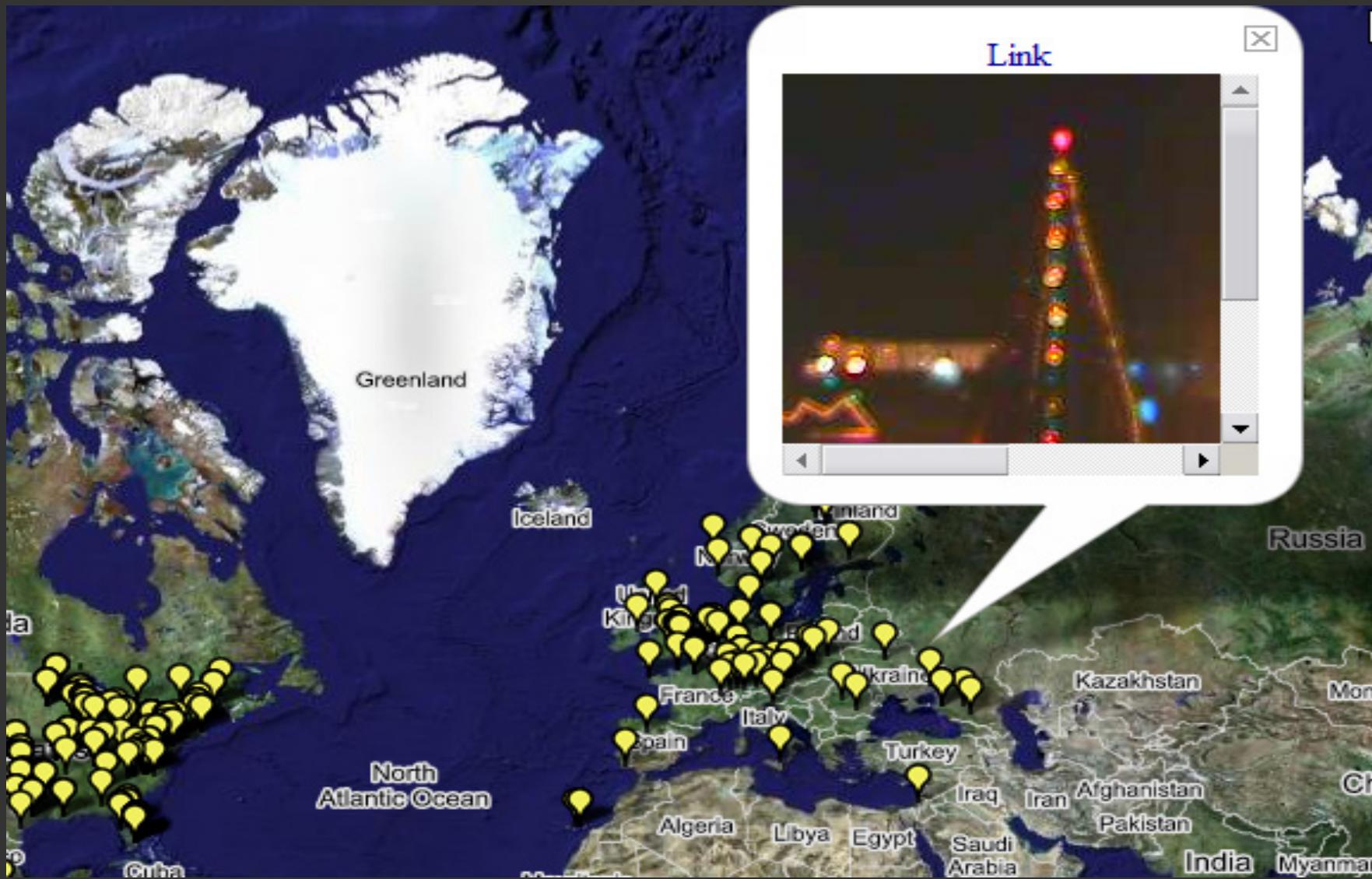
[You] say hello to people who are watching my lecture

[cat] It's probably too late to say this, but please do not feel insulted.

[You] |

[README](#) | [Your recent log](#) | [Full logs](#) | [Download](#) | [Other bots](#) | [Blog trouble?](#) | [Evil](#) | [CB Challenge](#) | [20q](#)

Google HACKING BASED



Google LINKS

Further information:

<http://johnny.ihackstuff.com>

<http://googleblog.blogspot.com/>

<http://www.google-store.com/index.php>

<http://www.google.com/intl/en/contact/newsletter.html>

<http://www.googlesightseeing.com/>

<http://googlemapsmania.blogspot.com/>

<http://hobbiton.thisside.net/advmap.html>

<http://www.butterfat.net/goocam/>

Artykuł w Dzienniku Internautów podsumowujący zmiany w Google w roku 2005:

<http://di.com.pl/news/12404.html>

Skrypt do przeglądarki Opera pokazujący graficzny PageRank stron WWW:

<http://piko.jogger.pl/comment.php?eid=140360>

Pytania?

I will use Google before asking dumb questions. www.mrburns.nl before asking dumb questions. I will use Google before asking dumb questions.



Kontakt



Dziękuję za uwagę!

Piotr Konieczny

E-mail: konieczny@gmail.com

Website: http://piko.jogger.pl

JabberID: xerror@gentoo.pl

GG: 2147700

[MAIL](#) [PLAINTEXT](#)

I'm feeling lucky! Google

Sponsorzy wykładów LUMD:



Dziennik Internautów
www.di.com.pl

Sprawdź kolejne wykłady z cyku

Linux -- U mnie działa!

<http://LUMD.linux.pl>
<http://kernel.agh.edu.pl>



I'm feeling lucky! **Google**

The image shows a Google search results page with a large, semi-transparent watermark of the letter 'G' in the background. The main text 'I'm feeling lucky!' is in a small, light font, followed by the Google logo in its signature colors. A small number '1' and the text 'Search results' are visible in the bottom right corner.

1

Search results

Google HACKING

&

Penetration testing

I'm feeling lucky! 

PIOTR KONIECZNY
konieczny@gmail.com
Dziennik Internautów, Koło Naukowe KERNEL (AGH)

2

©Search 2005

Google Hacking & Penetration Testing

O czym będziemy mówić?

- **Historia jest ważna**, chociaż nikt jej nie lubi...
- **A usług to jest dużo**. Poważnie... jest ich w ch#lerę!
- **Szukać to znaczy...**
- **Zaawansowane operatory**
- **Google Hacking!** I'm feeling lucky! 
- **Internetowa antykonsepcja**, czyli zapobieganie atakom
- **SEO**, stron WWW „pozycjonowanie” i Google'a chorowanie
- **Ciekawostek kilka**, żeby na koniec obudzić śpiochów :-)

Google History

<http://www.google.com/intl/en/corporate/history.html>
<http://www-db.stanford.edu/~backrub/google.html>

BackRub, styczeń 1996r.

Larry Page i Sergey Brin, Stanford University

CEO: Eric Schmidt, wcześniej Novell



1998 Googol to jedynka i zer stoooooooooooo...oo



Pierwsi klienci: Yahoo, Sun Microsystems == \$100,000

Obecni klienci: 1 mld przez 380 mln w 112 domenach i 100 językach na m/c₄

© 2005 Google Inc.

Googol created by Milton Sirotta, nephew of American mathematician Edward Kasner, popularized in the book, *Mathematics and the Imagination* by Kasner and James Newman.

Yahoo CEO powiedział: Nasi użytkownicy nie są zainteresowani wyszukiwaniem informacji w sieci.

Obecnie Google ma 1 miliard odsłon w miesiącu, generowany przez 380 milionów unikalnych użytkowników ze 112 TLDs (100 języków).

Google History

17 Month



01/08/06

\$500.00
450.00
400.00
350.00
300.00
250.00
225.00
200.00
175.00
150.00
125.00
100.00

Sep Oct Nov Dec 2005 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2006

<http://nasdaq.com>

© March 2005

Wartości akcji od wejścia spółki na giełdę do chwili obecnej

Google Services

*„Google's mission is to **organize** the world's **information**
and make it universally **accessible** and **useful**“*

Do NO evil!

<http://www.google.com/press/descriptions.html>



6

© 2005 Google Inc.

Google Services

AdWords & AdSense

<http://answers.google.com/>

<http://www.google.com/alerts>

<http://www.base.google.com>

<http://www.google.com/blogsearch>

<http://books.google.com/>

<http://catalogs.google.com/>

<http://www.google.com/dirhp>

<http://froogle.google.com/>

<http://gmail.google.com/>

<http://www.google.com/talk/>

<http://groups.google.com/>

<http://images.google.com/>

\$\$\$, zapraszamy do reklamy

\$\$\$, dochodowy interes

WWW, news, groups

\$\$\$, znana także jako Print

katalog DMOZ



I'm feeling lucky!

2,5++ GiB

Jabber/XMPP

Usenet od 1981r.

Google Services

<http://maps.google.com/>

<http://earth.google.com/>

<http://www.google.com/transit>

<http://labs.google.com/ridefinder>

local search, Directions

rozbudowane mapy w 3D

komunikacja miejska

TAXI

<http://mobile.google.com/>

<http://www.google.com/sms/>

<http://www.google.com/glm/>

<http://www.dodgeball.com/>

tylko UK i USA; 46645 == GOOGL

local for mobile

<http://news.google.com/>

<http://www.google.com/ig>

<http://www.google.com/psearch>

<http://www.google.com/reader>

personalized Homepage

personalized Search, History, Trends

czytnik RSS via WWW

<http://video.google.com/>

\$\$\$, nie ma niczego ciekawego w TV? ;-)

I'm feeling lucky! 

Google Services

<http://www.google.com/webhp?complete=1> suggest
<http://labs.google.com/sets> bliskoznacznie
<http://www.google.com/services/siteflavored.html>

<http://scholar.google.com/>
<http://www.google.com/options/specialsearches.html>
US, Linux, MS, BSD, Apple, Universities

<http://www.blogger.com/> ale Jogger.pl i tak lepszy! :-)
<http://www.orkut.com> I'm feeling lucky!

<http://code.google.com/> Jingle!
<http://code.google.com/apis.html>

AdWords; Blogger; Desktop; Google Desktop; Earth; Froogle; Gmail; Google Homepage API; Groups; Maps; News; Search Appliance; Talk; Web search; Video;

9

© 2005 Google

Do niektórych API wymagany jest klucz/licencja (darmowa, ale z ograniczeniami np. na liczbę odpytywania serwerów Google w ciągu doby)

Google Services

<http://desktop.google.com/>
<http://toolbar.google.com/>
 <http://toolbar.google.com/desktop/>
 <http://toolbar.google.com/firefox/extensions/>
 <http://toolbar.google.com/dc/offerdc.html>
<http://pack.google.com/>

<http://picasa.google.com/index.html>
<http://www.hello.com/>

http://www.google.com/language_tools

g lucky! 

<http://webaccelerator.google.com/>
<http://services.google.com/tcbin/tc.py>



Google **Business** Search
Appliance / Mini

programy

photo IM

przetłumacz

Wi-Fi



Używając reverse engineering z Google Appliance/Mini można wyciągnąć ciekawe informacje

Google Services

Usługi dla webmasterów:

<http://www.google.com/analytics/>

<https://www.google.com/webmasters/sitemaps/login>

...ale o tym wspomniemy później.

I'm feeling lucky! 

11

© 2005 Google Inc.

Na nich skupimy się w części wykładu poświęconej pozycjonowaniu stron WWW



Nie ma co wyjaśniać, kto nie widział Google? :-)

Google Search

Wyszukiwarka Google udostępnia m.in.:

Boolean logic

Spell checker

Cached links

Similar sites

Web page translation

Intelligent guessing -- Stock quotes, Books, Movies, Froogle, IMGs

<http://google.com/search?q=birthplace+of+John+Paul+II>

<http://google.com/search?q=population+of+Poland>

<http://google.com/search?q=gas+Ukraine>

Street maps

Calculator

Definitions

Search by number *Travel*

Phone book

<http://google.com/search?q=0141>

Google Search

Z czym to się je? Założenia i operatory:

NOT case sensitive

(CZE pOkliKasH? == cze poklikash?)

Automatyczne założenie iloczynu "**AND**" (+)

(patrz URL)

Automatyczne wykluczenie popularnych słów

operator + przywraca słowo

| (pipe lub **OR**)

== suma/alternatywa

- (minus)

== wykluczenie terminu

~ (tylda)

I'm feeling lucky!
== synonim

"wyrażenia" lub . (kropka)

== dokładne wyrażenie

* (gwiazdka)

== dowolne słowo

http://google.pl/search?q=mam+*+lat

Wariacje słowne

(**s**mieszne reklamy == śmieszne reklamy)

14

© 2005 Google Inc.

Do tego dochodzą nawiasy grupujące wyrażenia, nadając im priorytet pierwszeństwa parsowania.

Google Search

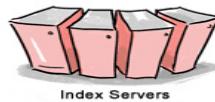
3. The search results are returned to the user in a fraction of a second.

1. The web server sends the query to the index servers. The content inside the index servers is similar to the index in the back of a book - it tells which pages contain the words that match the query.

2. The query travels to the doc servers, which actually retrieve the stored documents. Snippets are generated to describe each search result.



Doc Servers



Index Servers

<http://google.com>

© Google 2005

Wszystko w dużo mniej niż sekundę!

Google Search

Google Grid / Google FileSystem

The Power Behind Google (*Michael Feldman, HPCWire*)

kudos to Olaf

<http://news.taborcommunications.com/msgget.jsp?mid=534736>

Google Compute (*with Stanford University*)

!!! obsolete !!!

<http://toolbar.google.com/dc/offerdc.html>

Google BruteForce Indexing???

(:-)

I'm feeling lucky! 

```
crawl-66-249-65-70.googlebot.com - - [08/Jan/2006:08:30:02 -0500] "GET /paper/?N=D  
HTTP/1.1" 200 863 "-" "Mozilla/5.0 (compatible; Googlebot/2.1;  
+http://www.google.com/bot.html)"
```

```
crawl-66-249-71-1.googlebot.com - - [08/Jan/2006:00:36:49 -0500] "GET / HTTP/1.0"  
200 6591 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
```

```
crawl-66-249-65-70.googlebot.com - - [08/Jan/2006:05:54:26 -0500] "GET / HTTP/1.1"  
200 6591 "-" "Mediapartners-Google/2.1"
```

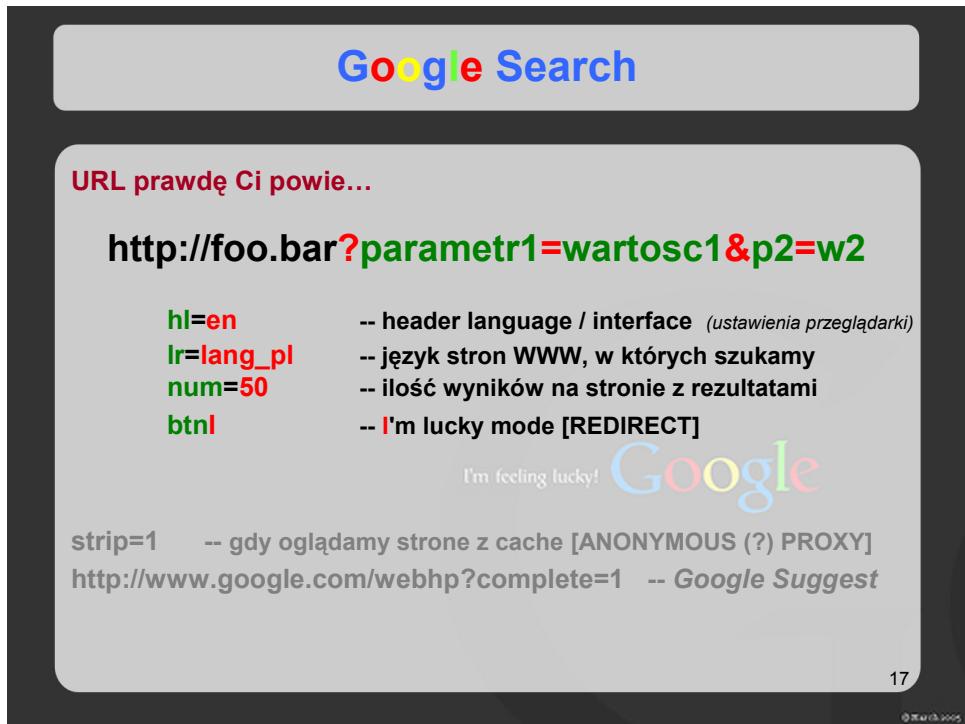
16

© 2006 Google

Ille różnych robotów posiada Google?

Normalny do stron, do obrazków, do AdSense.

Używają wielu IP, czasem przedstawiają się innym User-Agent



17

© 2005

Podstawą pracy z aplikacjami webowymi jest poznanie składni/budowy URL.
Nas interesuje:

? - po nim następują parametry wywołania programu/skryptu
parametry są postaci NAZWA_PARAMETRU=WARTOŚĆ
& - ampersand oddziela poszczególne parametry od siebie

Oprócz tego, w GoogleHacking przydatna jest znajomość składni:

PROTOKÓŁ://LOGIN:HASŁO@SERWER.COM
np. ftp://filmy:divx@telewizja.kablowa.com

UWAGA!

Hasło i login wysyłane są przez przeglądarkę plain-textem!!!

Google Search

Zaawansowane operatory

OPERATOR:PYTANIE

inurl:	intitle:	intext:	filetype:
allinurl:	allintitle:	inanchor:	
http://google.pl/search?q=sex+filetype:jpg			
numrange:		http://google.pl/search?q=8510310000..85103199999 każdy ma PESEL	
date:		3,6,12, bądź zakres	
define:		http://google.pl/search?q=define:WTF	
site:		http://google.pl/search?q=site:piko.jogger.pl które są zaindeksowane?	
link:		http://google.pl/search?q=link:piko.jogger.pl gdzie o nas mówią?	
cache:		http://google.pl/search?q=cache:piko.jogger.pl &strip=1	
info:		http://google.pl/search?q=info:piko.jogger.pl co Google o nas wie?	

18

© 2005

Szczegółowe omówienie (żmudne i bez praktyki) mija się z celem. Dlatego zachęcam do testowania operatorów, ew. Poczytania o nich na stronach Google.com – AFAIK nie ma lepszego opisu.

<http://www.google.com/help/operators.html>

Ponieważ nie wszystkie operatory są przez Google opisane, z innymi należy eksperymentować...

Google Search

Niektóre z obsługiwanych formatów:

HyperText Markup Language (**html**)

Adobe Portable Document Format, PostScript (**pdf, ps**)

Lotus 1-2-3 (**wk1, wk2, wk3, wk4, wk5, wki, wks, wku, lwp**)

MacWrite (**mw**)

Microsoft Office (**xls, ppt**)

Microsoft Word (doc) + <http://lcamtuf.coredump.cx/soft/therenv.tgz> = :-)

Microsoft Works (**wks, wps, wdb**)

Microsoft Write (**wri**) I'm feeling lucky!

Rich Text Format (**rtf**)

Shockwave Flash (**swf**)

Text (**ans, txt**)

...i dużo więcej!

!!! Google umożliwia niekiedy konwersję w/w do **HTML**

19



Problem z metadanymi np. pakietu Office narasta i będzie narastać.

Calculator

* Konwersje **0x7d3 in roman**

<http://google.com/search?q=0x7d3+%2B+3+in+roman>

* Równania **0x3 + 0b010 in decimal**

<http://google.pl/search?q=0x3+%2B+0b010+in+decimal>

* Przelicznik walut **1GBP in PLN**

<http://google.pl/search?q=1GBP+in+PLN>

...ale brak obliczania maski podsieci :(



Web



half (1 US cup) = 24 US teaspoons

[More about calculator](#)

Ciekawym uzupełnieniem byłoby wprowadzenie funkcjonalności kalkulatora sieciowego. Obliczanie podsieci, I hostów, bitowych operacji na adresach IP

Google HACKING

- * Google pobiera dane ze stron WWW...

...a strony WWW z Internetu i z Opery

(wyłącz reklamy AdSense lub zrób upgrade przeglądarki do najnowszej, darmowej wersji)

<http://opera.com>

- * To nie jest wina Google, że znajduje poufne informacje

(nauczmy się, jak nie dopuścić do tzw. **information leak**)

I'm feeling lucky! 
Czym wg Ciebie jest hacking?

^G "czym * ciebie jest (hacking|haking)" group:alt.pl.comp.os.hacking

,,"Hacking to robienie czegoś z4j3b15c13 dobrze!"

kudos to Bulba @ ap01

© 2005

Google HACKING

Znajdziemy i bezwzględnie wykorzystamy :-)

Serwery podatne na atak

nasz główny cel

Błędy w aplikacjach WWW

o przydatne dane, przydatne!

Pliki i katalogi

zawierające hasła, dane osobowe, logi firewalla, mp3

Ciekawe narzędzia

pomocne atakującemu

Numery kart kredytowych

*I'm feeling lucky! ale nie w trakcie wykładu *EG**

Urządzenia sieciowe

routery, switche, i inne



Google HACKING

Let's do the evil!

^G index.of mp3 ich.troje (113 sępów miłości na chwilę obecną)
<http://www.google.com/search?q=intitle%3Aindex.of+mp3+ich.troje>

^G inurl:microsoft filetype:iso (spróbuj z windows)
<http://www.google.com/search?q=inurl%3Amicrosoft+filetype%3Aiso>

^G http://admin:*@www (i mamy haselka dowolnego użytkownika!)
<http://www.google.com/search?q=http%3A%2F%2Fadmin%3A%2A%40www>

^G "sets mode: +k" (IRC anybody?)
<http://www.google.com/search?q=%22sets+mode%3A+%2Bk%22>

^G filetype:bak inurl:"htaccess|passwd|shadow|htusers" (OMG!)
<http://google.com/search?q=filetype%3Abak+inurl%3A%22htaccess%7Cpasswd%7Cshadow%7Chtusers>

Google HACKING

Zbieraj plony -- niezabezpieczone katalogi na serwerach TPSA

^G intitle:index.of server.at site:tpsa.pl

Struktury katalogów, adresy usług SSH/FTP z loginami a czasem hasłami

^G cd ls bash_history

Naucz się wykorzystywać wadliwe skrypty cgi do listowania plików

^G allinurl:/random_banner/index.cgi

Żeruj na ludzkiej głupocie

^G intitle:index.of inurl:admin inurl:backup

^G passwd.bak intitle:index.of

^G intitle:index.of secring.pgp

^G intitle:index.of..etc passwd

^G "admin account info" filetype:log

^G "Access denied for user" "using password"

(SQL!)

Poznaj nametags serwerów i wykorzystaj ich błędy

^G allintitle:Welcome to Windows NT 4.0 Option Pack

24

© 2005

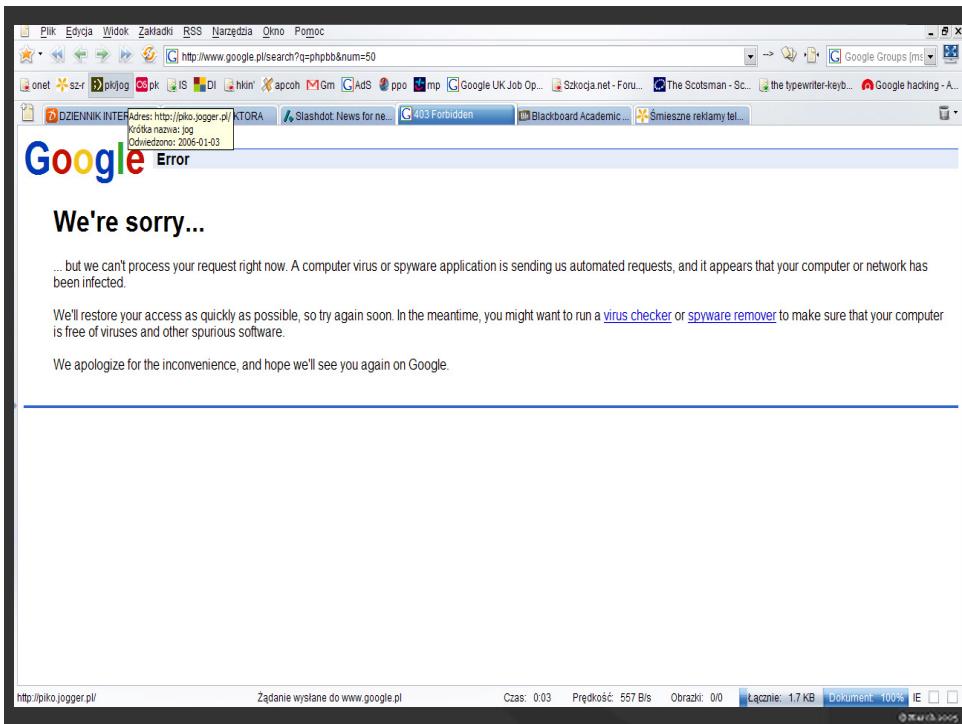
Uwaga na honeypoty! (nie wiesz co to, sprawdz w wikipedii! -- nie wiesz co to wikipedia, sprawdź w Google!)

Zainstalowanie honeypota u siebie może być ciekawym doświadczeniem...

The screenshot shows a web browser window with the title "Google HACKING". The address bar contains the URL "http://www.google.com/stde/1/compromis/Server/server.log". The page content is a log file from a server. The log starts with "----- log started at 07-08-05 18:06 -----". It then lists several entries:

```
07-08-05 18:06:12,ALL,Info,server,      Server init initialized
07-08-05 18:06:12,ALL,Info,server,      Server version: 2.0.20.1 Win32
07-08-05 18:06:13,WARNING,Info,SQL,     created table ts2_servers
07-08-05 18:06:13,WARNING,Info,SQL,     created table ts2_server_privileges
07-08-05 18:06:13,WARNING,Info,SQL,     created table ts2_channels
07-08-05 18:06:13,WARNING,Info,SQL,     created table ts2_channel_privileges
07-08-05 18:06:13,WARNING,Info,SQL,     created table ts2_clients
07-08-05 18:06:13,WARNING,Info,SQL,     created table ts2_bans
07-08-05 18:06:13,ALL,Info,server,      Starting VirtualServer id:1 with port:8767
07-08-05 18:06:13,WARNING,Info,SERVER,   Default VirtualServer created
07-08-05 18:06:13,WARNING,Info,SERVER,   admin account info: username: admin password: [REDACTED]
07-08-05 18:06:13,WARNING,Info,SERVER,   superadmin account info: username: superadmin password: [REDACTED]
07-08-05 18:06:13,ALL,Info,server,      Server init finished
07-08-05 18:07:48,ERROR,All,frmMain,    unable to detect external ip
```

Hasła w plaintext lub w postaci zaszyfrowanej (ale banalnej do złamania) zapisywane są w wielu logach, plikach. Wystarczy tylko znaleźć cechy charakterystyczne danego zbioru informacji dot. szukanego pliku i umiejętnie zadać pytanie wyszukiwarce, licząc na to, że ktoś "udostępnił" chcący bądź niechcący dany plik.



"Sometimes shit happens." -- Dzień Świra.

Google HACKING

Złe robale! -- dzięki nim Google blokuje nam wyniki

^G "powered by PHPbb2 2.0.6..10"

^G inurl:index.php AND inurl:phpbb

Hacking Google Hacking :-)

...bo wiele jest dróg...

^G "p_o_w_e_r_e_d by PHPbb2 2.0.6..10"

^G iNdEx inurl:PHPbb filetype:php

Do czego może się przydać szukanie wulgaryzmów?

^G site:wp.pl dupa

I'm feeling lucky!



Spam harvesters – chrońcie się!

^G emails.xls

jakie mogą być inne nazwy pliku?

^G *.gmail.com

Panie administratorze, podrukujemy razem?

<http://google.com/search?q=inurl:hp/device/this.LCDDispatcher>

27

© 2005

Robale i Chińczycy wpływają na cenzurę wyszukiwarki. Zadanie nieodpowiedniego pytania skutkuje komunikatem błędu.

Z komunikatem błędu, jak z każdym błędem można sobie poradzić...

Wulgaryzmy są często stosowane przez webmasterów/programistów sieciowych. Namierzając wulgaryzmy możemy często trafić na szablon strony w ciągle testowanym systemie, który "przypadkiem" został zaindeksowany. Wulgaryzmy są używane jako tzw. tekst wypełniający, por. "Lorem ipsum"

Do zbierania e-maili za pomocą Google powstała niezliczona ilość plików. M.in. dzięki temu codziennie w skrzynce możemy zobaczyć ciepłe słowa od księcia Zimbabwe i Australijki sprzedającej viagrę po okazyjnej cenie!

Pamiętaj, spam jest zły!

Plik Edycja Widok Zakładki RSS Narzędzia Okno Pomoc

onet sz-r pk/jog os_pk IS DI hkin' apcoh Gm AdS ppo mp the typewriter...
Gmail - [KERNEL...] PANEL REDAKT... Śmieszne reklam... inurl:hp/device/thi... HP LaserJet 410...

HP LaserJet 4100 Series / **HP LaserJet 4100 Series**

Printer Status Configuration Page Supplies Status Media Capabilities

Control Panel

READY

Ready Data Attention

Go

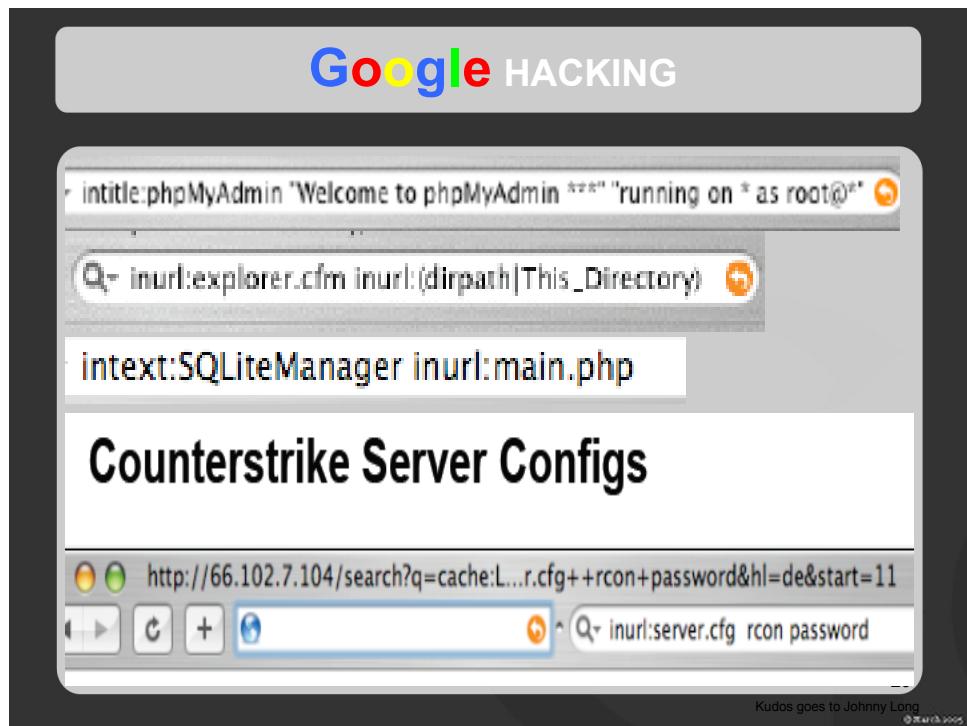
Control Panel Help Set Refresh Rate:
Refresh Control Panel 0 minutes
Help Apply Cancel

Supplies % of Life Remaining

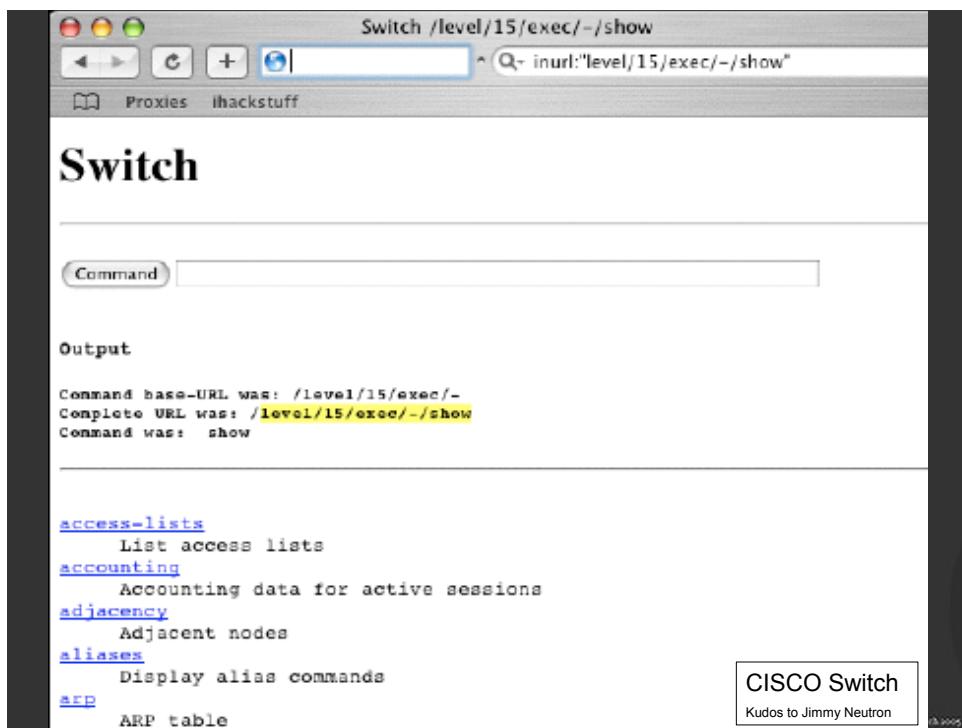
Black		74%
-------	---	-----

Media

Status	Input/Output	Size	Type
OK	TRAY 3	LETTER	PLAIN
OK	TRAY 2	LETTER	PLAIN
OK	TRAY 1	LETTER	PLAIN
OK	STANDARD OUTBIN	N/A	N/A
OK	OPTIONAL BIN 1	N/A	N/A



Inne przykłady zapytań. Nowe można tworzyć samemu ...lub znaleźć w sieci. Modyfikacja niektórych, wraz z np. kolejną wersją usługi/programu jest dobrym pomysłem.



Kto powiedział, że sniffing w sieciach przełączanych jest ciężki? *EG* :P

Google HACKING

Switch Home Page
http://64.233.161.104/search intitle:"switch home page" "cisco systems" "Telnet - to"
Proxies ihackstuff

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.

Kudos to Jimmy Neutron © search005

Google HACKING

Co jeszcze możemy popsuć razem z Google?

Simple Redirect i zero prywatności

<http://google.com/search?q=%C5%9Bmieszne+reklamy+telewizyjne&btnI>

```
195.85.229.2 -- [09/Jan/2006:10:20:45 -0500] "GET / HTTP/1.1" 200 6591 "--" "Opera/8.10  
(X11; Linux i686; U; en)" //nasze IP
```

Anonymous (!?) Proxy

<http://216.239.51.104/search?q=cache:piko.jogger.pl&strip=1>

<http://translate.google.com/translate?u=http://sztuka-reklamy.info&langpair=pl|pl>

```
216.239.36.136 -- [09/Jan/2006:10:18:43 -0500] "GET / HTTP/1.0" 200 6591 "--"  
"Opera/8.10 (X11; Linux i686; U; en),gzip(gfe) (via translate.google.com)"
```

```
195.85.229.2 -- [09/Jan/2006:10:18:43 -0500] "GET /piko.css HTTP/1.1" 304 --  
"Opera/8.10 (X11; Linux i686; U; en)" //to już nasze IP!
```

```
195.85.229.2 -- [09/Jan/2006:10:18:44 -0500] "GET /_img/tv.jpg HTTP/1.1" 304 --  
"Opera/8.10 (X11; Linux i686; U; en)" //to już nasze IP!
```

32

© 2006-2008

Redirect by Google, to raczej zabawa niż cokolwiek użytecznego. Ciekawsze są już tinyurl i hugeurl (pogooglaj za nimi)

Google oferuje dwie możliwości skorzystania z niego jako z proxy.

Pierwsza to cache: -- ale trzeba liczyć się z tym, że dane mogą być nieaktualne a przede wszystkim mogły jeszcze nie zostać zaindeksowane... Jak widać kiepskie to proxy.

I tu dochodzi uwaga o parametrze &strip=1 w URL. Jeśli go użyjemy otrzymamy tylko wyciąg tekstowy ze strony, dzięki czemu nasza przeglądarka nie połączy się z serwerem który chcemy obejrzeć (np. dociągając obrazki czy arkusze stylów). Dzięki temu nasze IP nie zostanie w logach serwera.

Druga możliwość: -- użycie usługi tłumaczeń. Poniżej wyciąg z logów Apache'a dot. wejścia na stronę za pomocą tej drugiej opcji. Proszę zauważać, że kiedy nasza przeglądarka pobiera arkusz stylów i obrazek, ujawnia nasze IP. Aby tego uniknąć można napisać skrypt filtrujący ruch, lub skonfigurować odpowiednio przeglądarkę (do zrobienia w Operze)

Google HACKING

Honeypots

trzeba mieć oczy dookoła serwera i wiedzieć co w trawie piszczy!

Cache sliding

gdy strona zniknie, a cache: rozpływnie się we mgle...

alternatywnie: <http://www.archive.org/web/web.php>

Authorization bypassing

teoria gridowego spisku? :-)

Internetowe Robale

czy Google może blokować zapytania? -- TAK! (ale już to obeszliśmy)

Co kraj, to obyczaj

różne języki, różne wyniki... pokombinuj z ustawieniami i porównaj!

Googlebombing (metodą walki politycznej?)

kretyń ze zbrodniarzem zachorowali na ptasią grypę, co za failure!

33

© 2005

O Honeypotach już wspomnieliśmy wcześniej. Patrz wikipedia :-)

Cache sliding. Czasem może zostać uznane jako trzecia opcja wykorzystania Google'a jako proxy. Niekiedy strona którą chcemy zobaczyć nie posiada już zawartości online, albo jest ona zabezpieczona. Odpytując Google o cache, również możemy się zdziwić – cache nie będzie działać/będzie usunięty (to się zdarza!). Należy zatem skorzystać z wyciągu, który Google prezentuje na stronie rezultatów – dwie linie pod tytułem każdego wyniku.

Odpytując Google o kolejne słowa, ów wyciąg (snippet) przesuwa się. Zadając odpowiednio wiele pytań otrzymujemy (co prawda w uciążliwy sposób) zawartość tekstu strony.

Alternatywnie można skorzystać z innych usług w sieci WWW, np. webarchive.

Authorization bypassing. Jak to się dzieje, że Google wie co jest na stronie, do której obecnie jest dostęp na hasło? Dwie możliwości: User-Agent determinuje mechanizm autoryzacji. Google posiada obrzydliwie wielką moc obliczeniową (patrz wcześniejszy opis Google Gridu) i używając Brute Force łamie hasło ;-)

O robakach internetowych już mówiliśmy wcześniej i generalnie ich nie lubimy, bo Google blokuje ich pytania.

Poeksperimentuj z ustawieniami językowymi (ustawienia przeglądarki HL=en/pl oraz lokal na Google: LR=lang_pl) Wyniki w różnią się w zależności od ustawień językowych, ale czy powinny? (por. Advanced Search – link z Google.com)

Google HACKING



WWW [Grafika](#) [Grupy dyskusyjne](#) [Katalog](#)
failure Szukaj [Szukanie zaawansowane](#)
 Szukaj w Internecie Szukaj na stronach kategorii: Polski

WWW

[Biography of President George W. Bush](#)

Biography of the 43rd President of the United States.

www.whitehouse.gov/president/gwbbio.html - 25k - [Kopia](#) - [Podobne strony](#)



WWW [Grafika](#) [Grupy dyskusyjne](#) [Katalog](#)
zbrodniarz Szukaj [Szukanie zaawansowane](#)
 Szukaj w Internecie Szukaj na stronach kategorii: Polski

WWW

[pl.wikipedia.org/wiki/Władimir_Putin](#)

[Podobne strony](#)

© Google 2005

Google HACKING



WWW [Grafika](#) [Grupy dyskusyjne](#) [Katalog](#)

ptasia grypa

Szukaj

[Szukanie zaawansowane](#)

[Ustawienia](#)

Szukaj w Internecie Szukaj na stronach kategorii: Polski

WWW

[Lech Kaczyński - Prezydent IV Rzeczypospolitej](#)

Aktualności z kampanii wyborczej i urzęduowania, życiorys, program wyborczy.

[www.lechkaczynski.pl/](#) - 13k - [Kopia](#) - [Podobne strony](#)



WWW [Grafika](#) [Grupy dyskusyjne](#) [Katalog](#)

kretyn

Szukaj

[Szukanie zaawansowane](#)

[Ustawienia](#)

Szukaj w Internecie Szukaj na stronach kategorii: Polski

WWW

[Posel: Andrzej Lepper](#)

Posel Andrzej Lepper, Następny · Poprzedni. Andrzej Lepper. Data i miejsce

urodzenia: 13-06-1954, Stowiącino Stan cywilny: żonaty ...

[www.sejm.gov.pl/poslowie/posel5/189.htm](#) - 7k - [Kopia](#) - [Podobne strony](#)

© Google 2005

Google DNS discovering

Kto pyta, nie błądzi...

Using lynx to capture the Google results page...

...returns the same results.

```
Terminal — ssh - 80x24
john@john-OptiPlex-5090:~$ lynx -dump 'http://www.google.com/search?q=site:microsoft.com+www.microsoft.com&num=100' > test.html
john@john-OptiPlex-5090:~$ sed -n '/</, /</>/ {alpha};>\\n</>{beta};' test.html | sort -u
http://download.microsoft.com/
http://go.microsoft.com/
http://msdn.microsoft.com/
http://nsevents.microsoft.com/
http://murl.microsoft.com/
http://offices.microsoft.com/
http://protect.microsoft.com/
http://research.microsoft.com/
https://e.microsoft.com/
http://support.microsoft.com/
john@john-OptiPlex-5090:~$
```

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

36

Kudos to Johnny Long ©SearchSecurity

Google może posłużyć jako odkrywca nowych domen. Dla atakującego każda nowa domena (która może okazać się osobną maszyną) jest cenną informacją.

Najpierw parsujemy wyniki wyszukiwania, łapiąc tylko to co nas interesuje.

Potem za pomocą Google Sets (adres na początku prezentacji) lub własnego IQ szukamy wzoru na podstawie którego dobierane są nazwy domen.

Potem piszemy skrypt i testujemy czy ów domena istnieje. Pasywnie/Aktywnie.

Wg badań Johnnego Longa, odkrywa się tą metodą przy pomocy Google ok. 30% domen, o których Google nie ma pojęcia!

Google HACKING – OBRONA

Polityka bezpieczeństwa

(but business is business...)

Opracowujemy schemat przepływu i zarządzania informacją w firmie

Edukujemy wszystkich pracowników, nie tylko panią Halinkę z kadr

Krytyczne i poufne dane trzymamy w INTRANECIE.

Używamy kryptografii i autoryzacji -- i pamiętamy o pilnowaniu kluczy :>

Usuwamy metadane z plików MS Office przed publikacją/wysłaniem !!!

Regularnie wykonujemy Information Assesments: Penetration testing & Ethical hacking

tj. automatycznie i świadomie odpytujemy ^G poprzez specjalne skanery.

Google zabrania automatycznego odpytywania swojej wyszukiwarki.

Trzeba postarać się o licencję dla programów korzystających z Google API.

37

© 2014-2015

Zmora każdego działu IT i każdego działu produkcji. Walka pomiędzy wydajnością, opłacalnością, szybkością a bezpieczeństwem informatycznym.

Kiedyś ludzie zrozumieją, że nie należy ignorować technologii

Używajmy specjalnych programów (ew. piszmy je sami) sprawdzających spójność i otwartość naszej sieci. Testujmy information leaks m.in. poprzez zapytania Google'a, a przede wszystkim unikajmy błędów w oprogramowaniu sieciowym/aplikacjach web..

Google HACKING – OBRONA

Plik .htaccess

```
xerror@szynszyl:~/public_html> ls -al
-rw-r--r--  1 xerror  ftjgrp        90 Jan  4 20:29 .htaccess
-rw-r--r--  1 xerror  ftjgrp      113 Jan  5 16:38 head.html
-rw-r--r--  1 xerror  ftjgrp      15 Jan  5 16:38 tail.html
```

```
xerror@szynszyl:~/public_html> cat .htaccess
HeaderName head.html
IndexOptions +FancyIndexing +SuppressHTMLPreamble
ReadmeName tail.html
```

```
I'm feeling lucky! Google
xerror@szynszyl:~/public_html> cat head.html
<html>
<head><title>foobar</title></head>
Pliki w katalogu
```

```
xerror@szynszyl:~/public_html> cat tail.html
<b>foo</b> bar -- <i>Niestraszni nam szablonowi Googleszperacze!</i>
```

38

© SearchMe

Indywidualnie, kiedy nie jesteśmy administratorem serwera.

Google HACKING – OBRONA

Plik Edycja Widok Zakładki RSS Narzędzia Okno Pomoc

onet sz-r pk/jog os pk IS DI hkin' apcoh Gm AdS ppo +
Gmail - goog... PANEL RED... Śmieszne re... inurl:hp/devic... HP LaserJ

Pliki w katalogu

<input type="checkbox"/>	Name	Last modified	Size	Description
[DIR]	Parent Directory	04-Jan-2006 20:23	-	
[TXT]	head.html	09-Jan-2006 17:49	1k	
[TXT]	tail.html	09-Jan-2006 17:50	1k	

foo bar! -- Niestraszni nam szablonowi Googleszperacze!

Pozbywając się "Index of" mamy mniejsze prawdopodobieństwo, że ktoś trafi do nas po standardowym Google Hack'u, czyli zapytaniu o listingi katalogów na podstawie frazy "Index of"

Usunąć też możemy sygnature/nazwę serwera. To pomocne – im trudniej atakującemu odgadnąć wersję serwera, tym trudniej dobrać exploit ;-)

Google HACKING – OBRONA

Plik Robots.txt

Przestrzega go większość robotów internetowych.

```
User-agent: Googlebot | * | Googlebot-Image  
Disallow: / | /lemury | /*.gif$ | /*?
```

Nagłówek strony WWW

```
<META NAME="ROBOTS" CONTENT="NOINDEX,NOFOLLOW,NOARCHIVE">  
<META NAME="GOOGLEBOT" CONTENT="NOINDEX, NOFOLLOW">  
<a href=http://www.przyklad.com/ rel="nofollow">Bez spamu mi tu!</a>
```

Usuwamy stronę z wyników Google'a

<http://www.google.com/webmasters/remove.html>

40

© 2005

Czy istnieją w sieci niewidzialne Google? Rządowe np.? Czy ich roboty przestrzegają pliku robots.txt (Agencja monitoringu mediów elektronicznych ma/miała popsu tego robota... -- DDoS)

Na nic zdadzą się sztuczki spamów/specjalistów od SEO, jeśli ustawimy rel=nofollow w każdym z dostępnych miejsc na naszej stronie, które edytować mogą goście.

Search Engine Optimization

The screenshot shows a Google search results page for the query "pozycjonowanie". The results are filtered for the Polish language ("Wyniki 1 - 10 spośród około 3,920,000 w języku Polski dla zapytanie pozycjonowanie. (Znaleziono w 0,04 sek.)"). The results are grouped into several categories:

- Skuteczne Pozycjonowanie**:
 - [www.interneta.pl](#) Wskocz na pierwsze miejsca Lata doświadczeń, bogate portfolio
 - [pozycjonowanie stron - TANIO - pozycjonowanie stron ...](#) Pozycjonowanie, tworzenie stron, pozycjonowanie stron. Oferujemy tanio: tworzenie stron, wysokie pozycjonowanie stron w wyszukiwarkach - Google, Onet, WP, ...
 - [pozycjonowanie i Optymalizacja - SEO Forum, Hosting, Webhosting ...](#) Pozycjonowanie stron internetowych. Pozycjonowanie i Optymalizacja Forum - Pozycjonowanie i optymalizacja stron internetowych. Otwarta rozmowa na temat ... forum.optymalizacja.com/ - 58k - 11 2006 - [Kopia - Podobne strony](#)
 - [Pozycjonowanie stron www - Skuteczne i tanie ...](#) Pozycjonowanie stron - Oferujemy profesjonalne i niedrogie pozycjonowanie stron www. Dzięki nam Twoja strona będzie pierwsza! Reklama witryn, pozycjonowanie ...
 - [pozycjonowanie - 8k - Kopia - Podobne strony](#)
- Wyszukiwarki i pozycjonowanie stron - kilka użytecznych porad**:
 - Pozycjonowanie stron zaliczamy do form promocji o największym współczynniku zysk/cena. Poznaj sekrety pozycjonowania i ciesz się wysoką oglądalnością!
- Linki sponsorowane**:
 - [pozycjonowanie](#) Poważne podejście do tematu Strategia, optymalizacja, raporty.
 - [pozycjonowanie stron www](#) Skuteczne pozycjonowanie stron Kampanie reklamowe w sieci
 - [Darmowe pozycjonowanie](#) Pozycjonuj własną stronę i zarabiaj Darmowy program wymiany linków.
 - [pozycjonowanie](#) Pozytywne strony www Tania i skuteczna reklama w sieci
 - [Kampanie internetowe](#) Wypromuj swoją firmę w Internecie

Jak widać biznes kwitnie

Search Engine Optimization

Jeden z **największych** problemów Google

Etyczne dopuszczalne, moralnie haniebne? (spam!)

Bilans zysków i strat ale okraszony współczynnikiem ryzyka

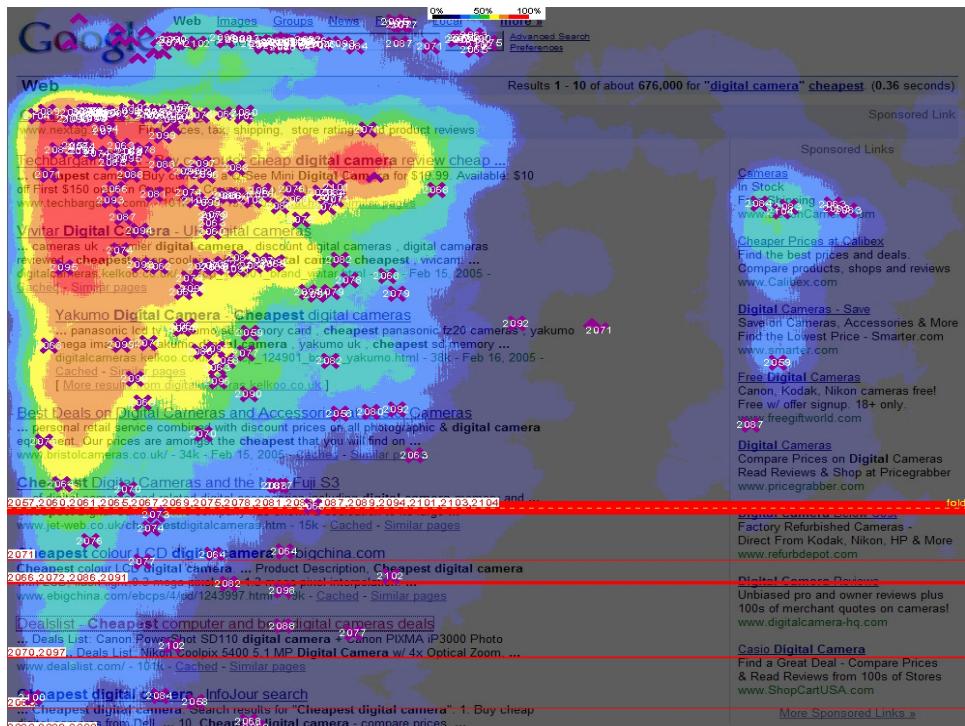
-- pozycjonowanie narusza regulamin Google

-- nasza strona może trafić do tzw. **sandbox**

I'm feeling lucky! 

Czy warto więc pozycjonować strony WWW?

Wszystko stanie się jasne, kiedy spojrzymy na wykresy...



Raport Enquiero, Did-it i Eyetools.

Wyniki badań pokazują wzór ruchu oka użytkownika używającego wyszukiwarki. Przypomina on literę "F". Góra część wyników była zauważona przez 100% badanych (50-osobowa próbka).

Wyniki wyszukiwania:

1 – 100%	2 - 100%
3 – 100%	4 - 85%
5 – 60%	6 - 50%
7 – 50%	8 - 30%
9 – 30%	10 - 20%

Reklamy po prawej:

1 – 50%	2 - 40%
3 – 30%	4 - 20%
5 – 10%	6 - 10%
7 – 10%	8 - 10%

Search Engine Optimization

Technologia Google

- **PageRank** pozycja strony nie zależy od niego!
- Analiza dopasowań hipertekstowych
- **Linki, linki, linki!**

http://en.wikipedia.org/wiki/List_of_websites_with_a_high_PageRank

Techniki SEO:

Cloaking; Doorway/jump pages,,

Link spam: programy wymiany linków/reklamy, księgi gości/fora

<http://www.google.com/addurl/?continue=/addurl>
<https://www.google.com/webmasters/sitemaps/>
<http://www.google.com/analytics/>
<http://www.google.com/intl/en/webmasters/>
<http://www.google.com/contact/spamreport.html>
<http://www.mcdar.net/dance/>
http://www.webworkshop.net/pagerank_calculator.php3



w wielu datacenter

Pluginy do przeglądarek pokazujące PageRank

Opera: <http://piko.jogger.pl/comment.php?eid=140360>

44

© 2004-2005

Technologia PageRank: PageRank dokonuje obiektywnej oceny ważności stron internetowych, rozwiązuje równania z ponad 500 milionami zmiennymi i 2 miliardami terminów. Zamiast zliczać bezpośrednie linki, PageRank interpretuje link ze strony A do strony B jako "głos" oddany na stronę B przez stronę A. W ten sposób PageRank ocenia wagę stron: na podstawie liczby oddanych na nią głosów.

Uwzględnia również wagę stron oddających głos, ponieważ uznaje się, że głosy pewnych stron mają większą wartość, co zwiększa również wartość stron, na które "głosują". Ważne strony uzyskują wyższe notowanie PageRank i są wyświetlane na początku listy wyników wyszukiwania. W celu określenia ważności strony technologia Google wykorzystuje całosciowo informacyjne zasoby Internetu. **Ludzie nie wpływają na wyniki wyszukiwania ani nimi nie manipulują - dlatego użytkownicy darzą Google zaufaniem**, uznając firmę za źródło obiektywnych informacji, nieskażone sprzedażą miejsc w rankingu.

Wyszukiwarka Google analizuje również zawartość stron. Zamiast jednak sczytywać po prostu tekst na stronie (którym wydawcy mogą manipulować przy użyciu tagów meta), technologia Google analizuje pełną zawartość strony, z uwzględnieniem czcionek, sekcji i dokładnego położenia każdego słowa. Aby zapewnić trafne wyniki wyszukiwania, **Google analizuje także zawartość sąsiednich stron internetowych**.

Search Engine Optimization

Dobrze dobrana domena!

(nazwa, wiek)

Przemyślana kompozycja strony

Wyszczególnione słowa kluczowe

```
<title> <hX> <b> <strong> <em> <i> <u> <li> <dfn>
```

Opisane linki i multimedia

```
<a href="http://sztuka-reklamy.info"  
    title="śmieszne reklamy">Google  
śmieszne reklamy telewizyjne </a>
```

```

```

...dużo linków do naszej strony i trochę czasu.

45

© 2010 G. Bošić

Ponieważ niektórzy żyją z pozycjonowania stron, nie opisałem tu wszystkiego a przede wszystkim najważniejszego ;-) Za inne, bardziej zaawansowane metody, trzeba zapłacić... Ważne żeby wiedzieć ile i komu.

Search Engine Optimization

Najbardziej poszukiwane w 2005:

Świat:

1. janet jackson
2. hurricane katrina
3. tsunami
4. xbox 360
5. brad pitt
6. michael jackson
7. american idol
8. **britney spears**
9. angelina jolie
10. harry potter

Polska:

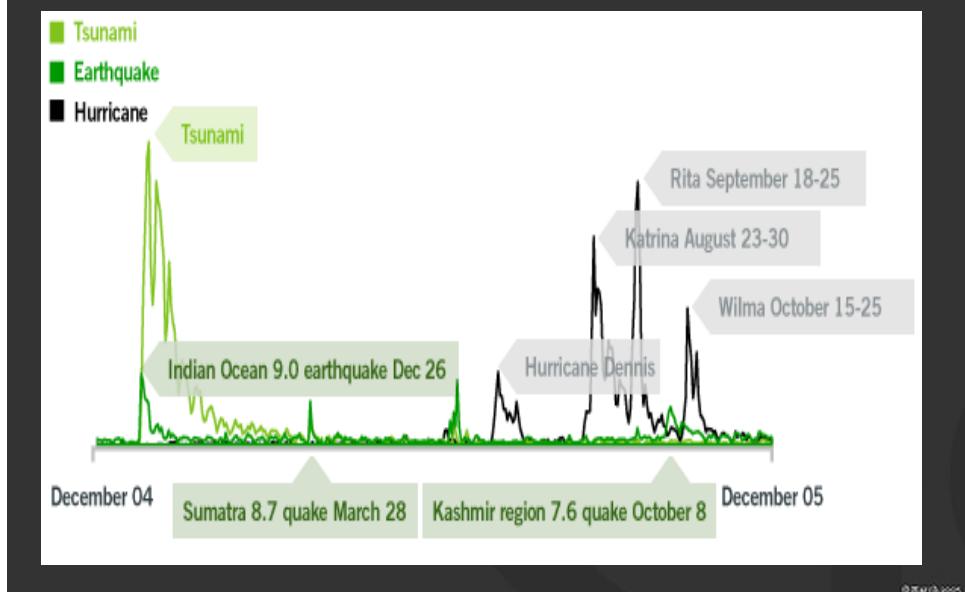
1. wikipedia
2. harry potter
3. wróżby andrzejkowe
4. britney spears
5. paris hilton
6. media markt
7. suknie ślubne
8. opony
9. kolorowanki
10. ptasia grypa

46

© 2005

Britney Spears od 4 lat jest na topie! Słowa piosenki *Hit me baby one more time* nabierają nowego znaczenia w kontekście internetowym :-)

<http://www.google.com/intl/en/press/zeitgeist.html>



Google prowadzi statystyki. Znaczy to również, że zapisuje pytania które mu zadajemy. Ile raz się pomyliłeś wpisując w pole wyszukiwania poufną informację/dane osobowe?

Google twierdzi, że zbiera dane do szacunków, takich jak ten powyżej. Dzięki czemu widać trendy na świecie, ale informacje o poszczególnych użytkownikach nie są ujawniane – czy zatem nikt nie może zidentyfikować Cię jako osoby która szuka p0rn0 w sieci np. w godzinach pracy?

Google'a PLANY NA PRZYSZŁOŚĆ

Do no evil ---???--> Make people think we do no evil

Google wyznaje zasadę zabawy:

Zbudujmy narzędzie, które będzie popularne. Zyski przyjdą same.

Budowanie narzędzia jest interaktywne.

Użytkownicy bawiąc się usługą określają jej charakter.

Google chce być miejscem, gdzie przechowujesz życie:

Altruizm czy strategia? centralizacja czy monopol?

Liczne serwisy i usługi – nie tylko elektroniczne!

Coraz więcej zbieranych i przetwarzanych danych

por. <http://oceanstore.cs.berkeley.edu/index.html> – kudos to erfi

Setki kilometrów nieużywanych światłowodów ciągnących się przez całą Amerykę...

Nowe usługi/programy potrzebują większej przepustowości?

Uzależnienie użytkowników poprzez stanie się ISP?

Google Linux Based Operating System?

48

© 2005

Zasada zabawy obowiązuje w firmie. Przyjemne warunki pracy, część czasu pracy można poświęcić na rozwój własnych pasji przy wykorzystaniu technologii firmy.

Niecodzienna rekrutacja poprzez zagadki i łamigłówki IT.

Google wkracza na rynek pozainternetowy (usługi gospodarcze, przemysł, handel, oprogramowanie -- GooglePack). Czy nowe usługi również będą popularne? Cóż... logo Google jest znane.

Google'a PLANY NA PRZYSZŁOŚĆ

A może własna przeglądarka? :-)

```
xerror@szynszyl:~$ whois gbrowser.com
[...]
Registrant:
    Google Inc. (DOM-1278108)
    1600 Amphitheatre Parkway
    Mountain View CA 94043
    US
[...]           I'm feeling lucky! 
Created on.....: 2004-Apr-26.
Expires on.....: 2006-Apr-26.
Record last updated on...: 2004-Apr-26 16:46:39.
[...]
```

49

© 2004-2005

Aktywne wsparcie dla Firefoksa, ale ciężko jest zapanować nad Open Source.
Z Opery też nic nie wyszło (propozycja zakupu to raczej wybieg PR-owy)

Google BASED

Lologle

<http://www.logogle.com/>

Piotr Konieczny

Web [Images](#) [Groups](#) [News](#) [Froogle](#) [Local](#) [Logogle\(top\) »](#)

Google Search

[BookMark\(for IE\) - Google Logo Maker](#)

©2005 Logogle

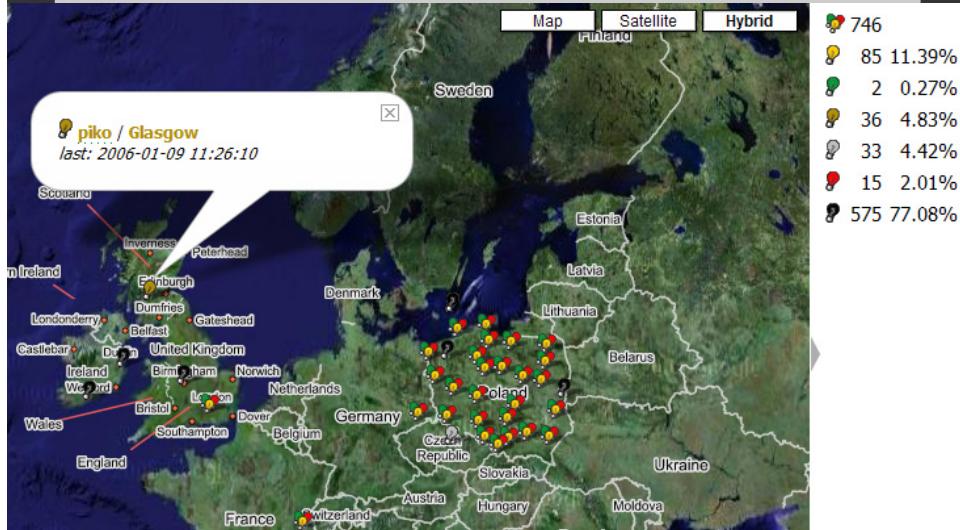
50

©2005 Logogle

Google BASED

Jobble

<http://jobble.uaznia.net>



Google BASED

Google Fight

<http://www.googlefight.com/>



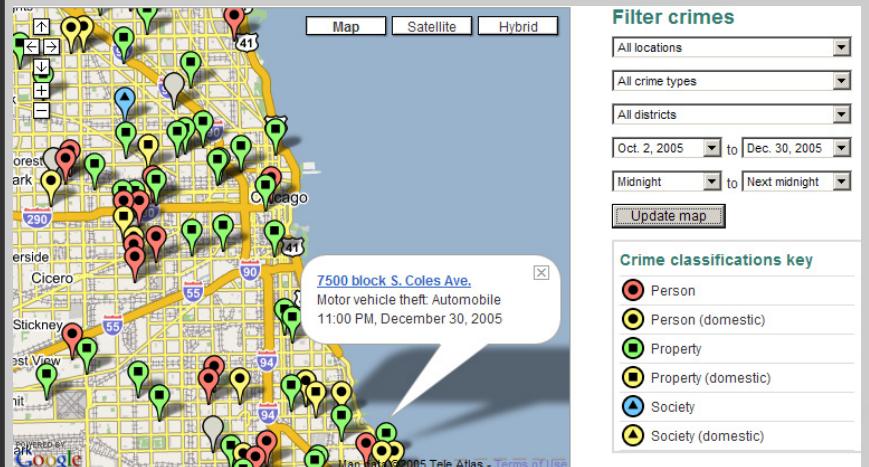
52

© 2006 Google

Google BASED

Chicago Crimes

<http://www.chicagocrime.org/map/>



© 2005 Google

Google BASED

Catty

<http://lcamtuf.coredump.cx/c3.shtml>

Catty v3

Copyright (C) 2001-2004 by Michal Zalewski (lcamtuf@coredump.cx)

Now talking with [195.85.229.2](#) (conversation counter: 134979).

[You] say hello to people who are watching my lecture

[Cat] It's probably too late to say this, but please do not feel insulted.

[You] [REDACTED]

[README](#) | [Your recent log](#) | [Full logs](#) | [Download](#) | [Other bots](#) | [Blog trouble?](#) | [Evil](#) | [CB Challenge](#) | [20g](#)

34

© 2004-2005

Google HACKING BASED



Google Hack + Google Maps API – CCTV / Monitoring który nie powinien być dostępny online.

Google LINKS

Further information:

<http://johnny.ihackstuff.com>
<http://googleblog.blogspot.com/>
<http://www.google-store.com/index.php>
<http://www.google.com/intl/en/contact/newsletter.html>
<http://www.googlesightseeing.com/>
<http://googlemapsmania.blogspot.com/>
 <http://hobbiton.thisside.net/advmap.html>
<http://www.butterfat.net/goocam/>

I'm feeling lucky! 
Artykuł w Dzienniku Internautów podsumowujący zmiany w Google w roku 2005:
<http://di.com.pl/news/12404.html>

Skrypt do przeglądarki Opera pokazujący graficzny PageRank stron WWW:
<http://piko.jogger.pl/comment.php?eid=140360>

Pytania?

I will use Google before asking dumb questions. www.mrburns.nl before asking dumb questions. I will use Google before asking dumb questions.



Kontakt



Dziękuję za uwagę!

Piotr Konieczny

E-mail: konieczny@gmail.com

Website: <http://piko.jogger.pl>

JabberID: [xerror@gentoo.pl](xmpp:xerror@gentoo.pl)

GG: 2147700

[MAIL](#) [PLAINTEXT](#)

I'm feeling lucky!

Sponsorzy wykładów LUMD:



Dziennik Internautów
www.di.com.pl

Sprawdź kolejne wykłady z cyku

Linux -- U mnie działa!

<http://lumd.linux.pl>
<http://kernel.agh.edu.pl>

58

[RFC001](#) [PICO](#) [GENFOR](#) [HACKER](#) [ARCHIVES](#)

Wszelki kontakt w sprawach związanych z tą prezentacją, zaproszenia do wygłoszenia prelekcji na Państwa imprezach/szkoleniach, oraz resztę spraw dot. mojej osoby proszę kierować najpierw na adres e-mail podany powyżej

Na stronach cyku LUMD (<http://lumd.linux.pl/prelegenci.php#prel3>) znajdziecie Państwo również inne moje prezentacje/wykłady, które wygłosiłem podczas spotkań Linux – U mnie działa!

Ponieważ na w/w stronach nie są udostępniane wszystkie moje prelekcje, w szczegółowych sprawach proszę o kontakt e-mailowy.