Google Hacking

Google Inc.

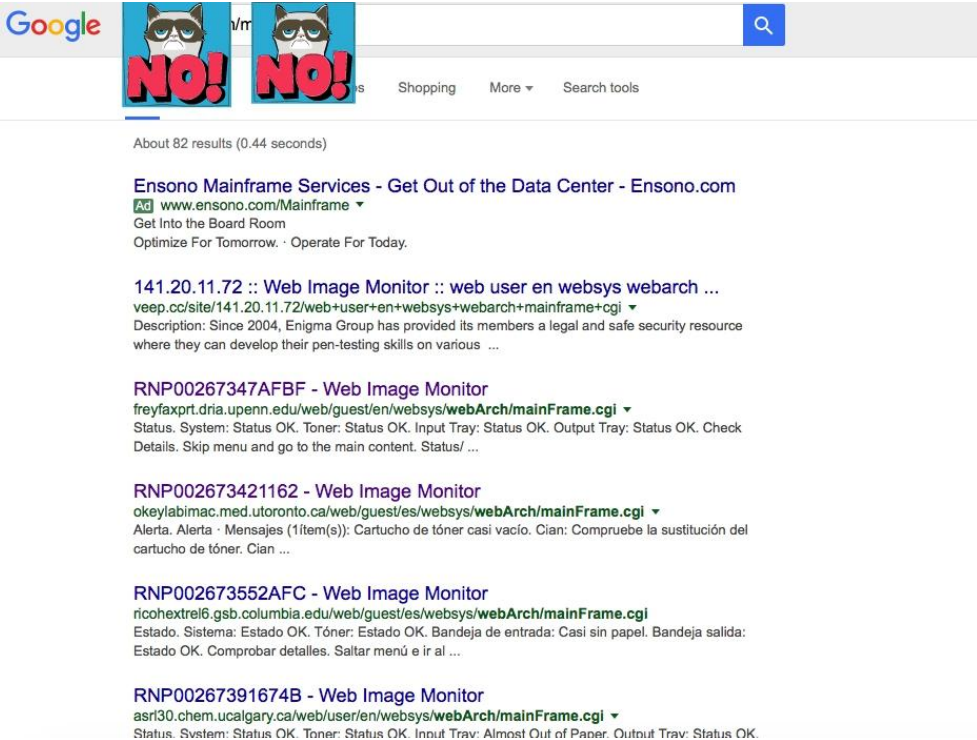
Founded on September 4th, 1998

Founders: Larry Page, Sergey Brin

Have you heard of
"googol"?

Crazy Things that Google lets you do: Example 1

Some interesting command :



About 82 results (0.44 seconds)

Ensono Mainframe Services - Get Out of the Data Center - Ensono.com
Ad www.ensono.com/Mainframe ▾
Get Into the Board Room
Optimize For Tomorrow. · Operate For Today.

141.20.11.72 :: Web Image Monitor :: web user en websys webarch ...
veep.cc/site/141.20.11.72/web+user+en+websys+webarch+mainframe+cgi ▾
Description: Since 2004, Enigma Group has provided its members a legal and safe security resource where they can develop their pen-testing skills on various ...

RNP00267347AFBF - Web Image Monitor
freyfaxprt.dria.upenn.edu/web/guest/en/websys/**webArch/mainFrame.cgi** ▾
Status. System: Status OK. Toner: Status OK. Input Tray: Status OK. Output Tray: Status OK. Check Details. Skip menu and go to the main content. Status/ ...

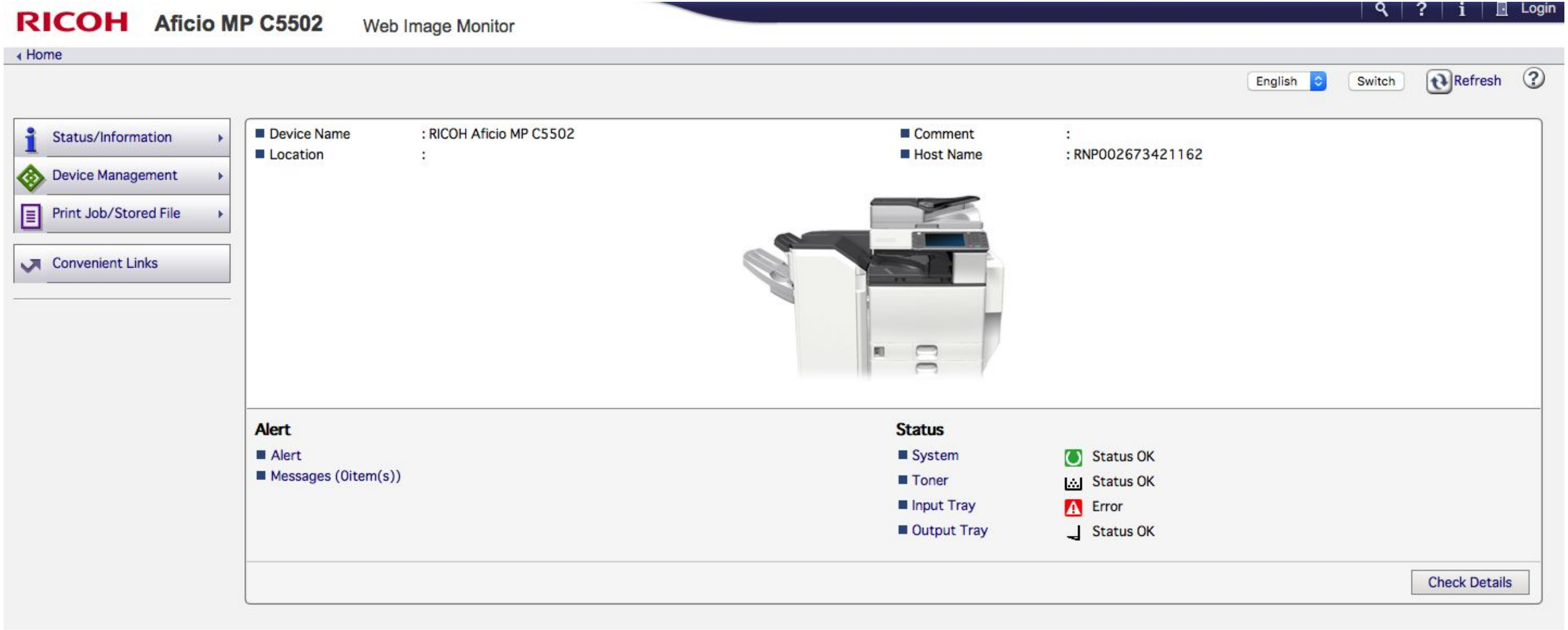
RNP002673421162 - Web Image Monitor
okeylabimac.med.utoronto.ca/web/guest/es/websys/**webArch/mainFrame.cgi** ▾
Alerta. Alerta · Mensajes (1ítem(s)): Cartucho de tóner casi vacío. Cian: Compruebe la sustitución del cartucho de tóner. Cian ...

RNP002673552AFC - Web Image Monitor
ricohextrel6.gsb.columbia.edu/web/guest/es/websys/**webArch/mainFrame.cgi**
Estado. Sistema: Estado OK. Tóner: Estado OK. Bandeja de entrada: Casi sin papel. Bandeja salida: Estado OK. Comprobar detalles. Saltar menú e ir al ...

RNP00267391674B - Web Image Monitor
asrl30.chem.ucalgary.ca/web/user/en/websys/**webArch/mainFrame.cgi** ▾
Status. System: Status OK. Toner: Status OK. Input Tray: Almost Out of Paper. Output Tray: Status OK.

Crazy Things that Google lets you do: Example 1

What nasty things can you do with somebody’s printer?



- Device Name : RICOH Aficio MP C5502
- Location :
- Comment :
- Host Name : RNP002673421162

Alert

- Alert
- Messages (0item(s))

Status

System	Status OK
Toner	Status OK
Input Tray	Error
Output Tray	Status OK

Crazy Things that Google lets you do: Examples 2&3

Demo: inurl:passwd filetype:txt

Demo: index.of.dcim -- What is DCIM folder?

Questions for you

Can you imagine how much power Google has?

Once something is on the Internet, Google KNOWS about it

Do you think it is possible to delete it?

Google Search Explained by Google guy

Terminology:

Google indexing, link;

Searching: keywords;

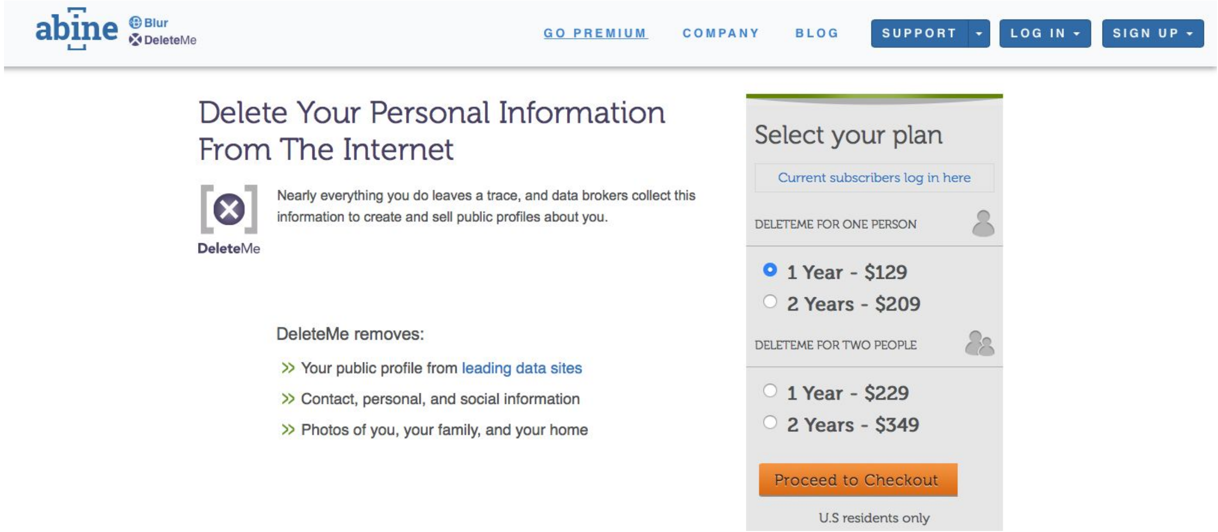
URL

https://www.youtube.com/watch?v=BNHR6IQJGZs

How can you delete ‘stuff’ from Google?

Ideas? Note that *Google is not the original source*

Some people get paid for this!



Delete Your Personal Information From The Internet

Nearly everything you do leaves a trace, and data brokers collect this information to create and sell public profiles about you.

DeleteMe removes:

- Your public profile from leading data sites
- Contact, personal, and social information
- Photos of you, your family, and your home

Select your plan

Current subscribers log in here

DELETEME FOR ONE PERSON

● 1 Year - $129
○ 2 Years - $209

DELETEME FOR TWO PEOPLE

○ 1 Year - $229
○ 2 Years - $349

Proceed to Checkout

U.S residents only

Searching with Google Directives

Try to find ANY information about Sergey Brin from Google servers (first few results!)

- Why does simply typing “Sergey Brin” in Google search box doesn’t work?

Searching with Google Directives (continued)

Now try this:

“Sergey Brin site:google.com” Syntax is important

Compare the two results!

So what does **site** directive do?

Directives we learned

site:*domain term(s) to search* -returns only the results that are pulled directly from the target (google.com) domain

Searching with Google Directives (continued)

Do you want to google anonymously? Google Cache is your friend!

Try “cache:apple.com”

Note that if you click on any of the link, it will bring you to the live website, not the cached version!

Read messages carefully! (images)

Add “&strip=1” to the URL to see text only

Directives we learned

site:*domain term(s) to search* -returns only the results that are pulled directly from the target (google.com) domain

cache:domain- returns results from the Google cache

Searching with Google Directives (continued)

What if you really want to find only .ppt files?

For example, you want lectures from CMU on *Network Security* course.

Try to find them!

CMU==Carnegie Mellon University

cmu.edu

Searching with Google Directives (continued)

Now try

“ filetype:ppt site:cmu.edu Network Security”

How quickly does Google return you results in both cases?

How many results do you get?

Directives we learned

site:*domain term(s) to search* -returns only the results that are pulled directly from the target (google.com) domain

cache:*domain*- returns results from the Google cache

filetype: *filetype* - finds files of a specified type

Searching with Google Directives (continued)

Try the following searches. What happens?

“intitle:index.of site:cmu.edu”

“inurl:admin intext:login”

“daterange: 2457567.1348-2457597.1348 Donald Trump”

“location: Boston Apple”

“define:hacking”

Directives we learned

site:*domain term(s) to search* -returns only the results that are pulled directly from the target (google.com) domain

cache:*domain*- returns results from the Google cache

filetype: *filetype* - finds files of a specified type

intitle:*keyword* -searches for the keyword in page titles

intitle:index.of- returns directory listings

inurl:*keyword* - searches for the URLs that contain keywords

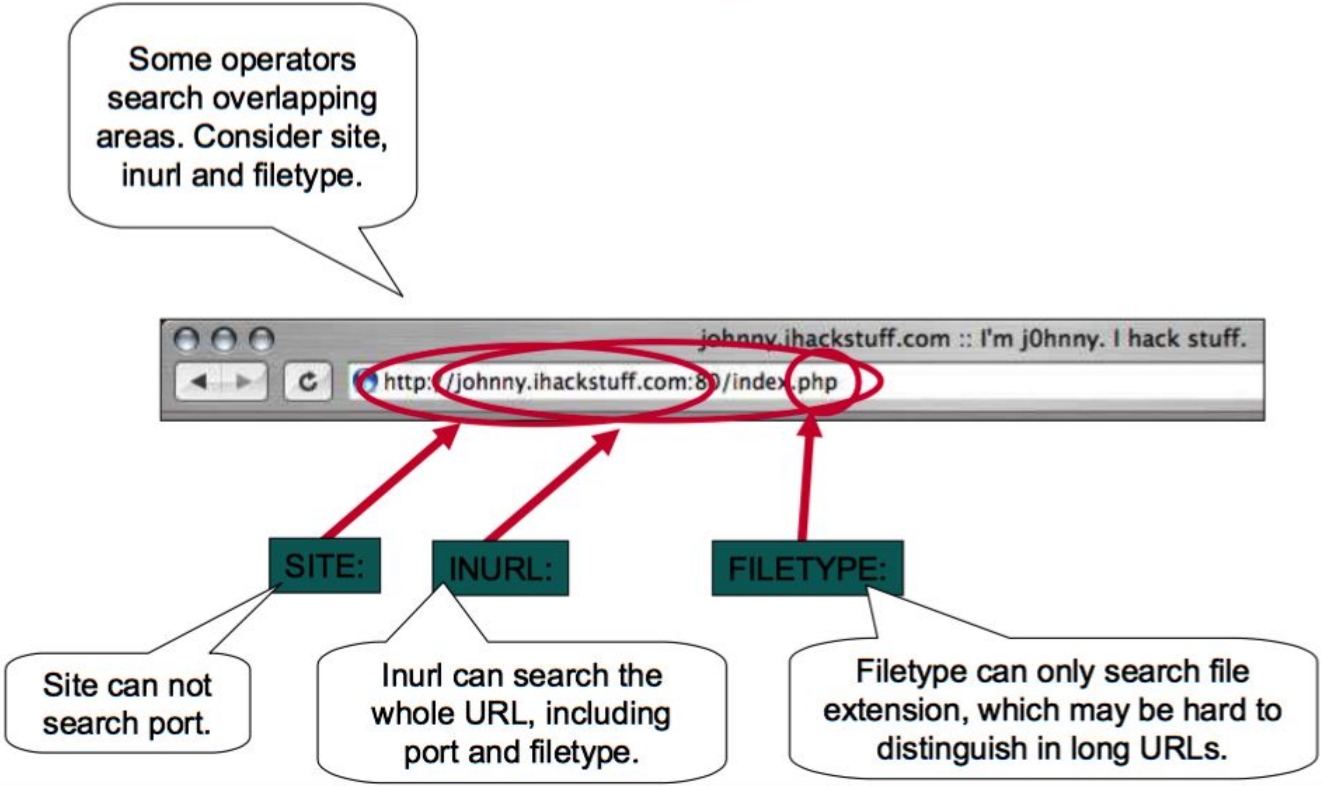
intext:*keyword*-searches for the keyword in page bodies

location:*keyword* - search by location

daterange:*time interval in Julian format* -defines a time frame for your search

define:*keyword* - gives you definitions of the keyword

Searching with Google Directives (recap)


johnny.ihackstuff.com :: I'm j0hnny. I hack stuff.
http://johnny.ihackstuff.com:80/index.php
SITE:
INURL:
FILETYPE:

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

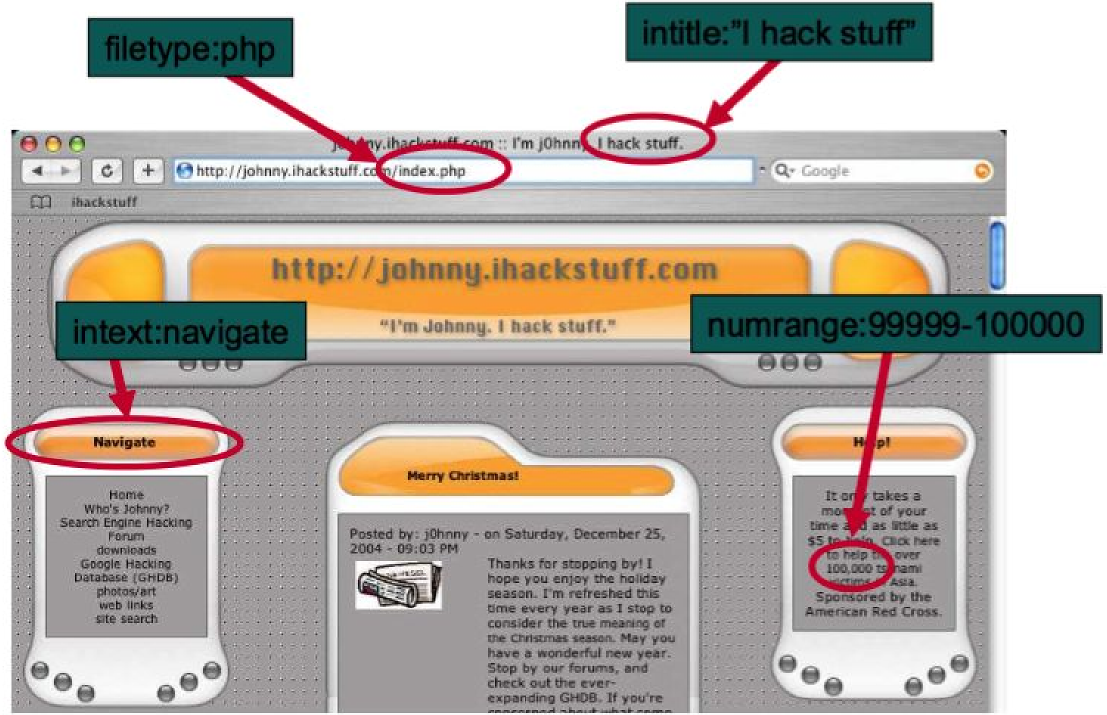
Site can not search port.

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.

Searching with Google Directives (recap)

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



filetype:php

intitle:"I hack stuff"

intext:navigate

numrange:99999-100000

j   ny.ihac   .com :: I'm j0hnn   I hack stuff.
http://johnny.ihackstuff.co m/index.php
Google
ihackstuff
http://johnny.ihackstuff.com
"I'm Johnny. I hack stuff."
Navigate
Home
Who's Johnny?
Search Engine Hacking
Forum
downloads
Google Hacking Database (GHDB)
photos/art
web links
site search
Merry Christmas!
H p!

Posted by: j0hnny - on Saturday, December 25, 2004 - 09:03 PM

Thanks for stopping by! I hope you enjoy the holiday season. I'm refreshed this time every year as I stop to consider the true meaning of the Christmas season. May you have a wonderful new year. Stop by our forums, and check out the ever-expanding GHDB. If you're concerned about what some

It on takes a mo nt of your time a d as little as $5 t h p. Click here to help t over 100,000 ts nami victims   Asia. Sponsored by the American Red Cross.

Advanced Google Search

“” - to only include keywords in the same form and the same order

- - to exclude a word

AND - similar to logical ‘and’

.. - to set an interval

* - placeholder for any unknown or wildcard terms

Google Hacking Lab

https://github.com/BUCodeBreakers/2017/blob/master/GoogleHackingLab2017.txt