Google Hacking

Agenda

Introduction
The Basic
Google Hacking Techniques
How to Protect your Websites

Introduction

- First step in attacking websites or penetration testing is reconnaisance

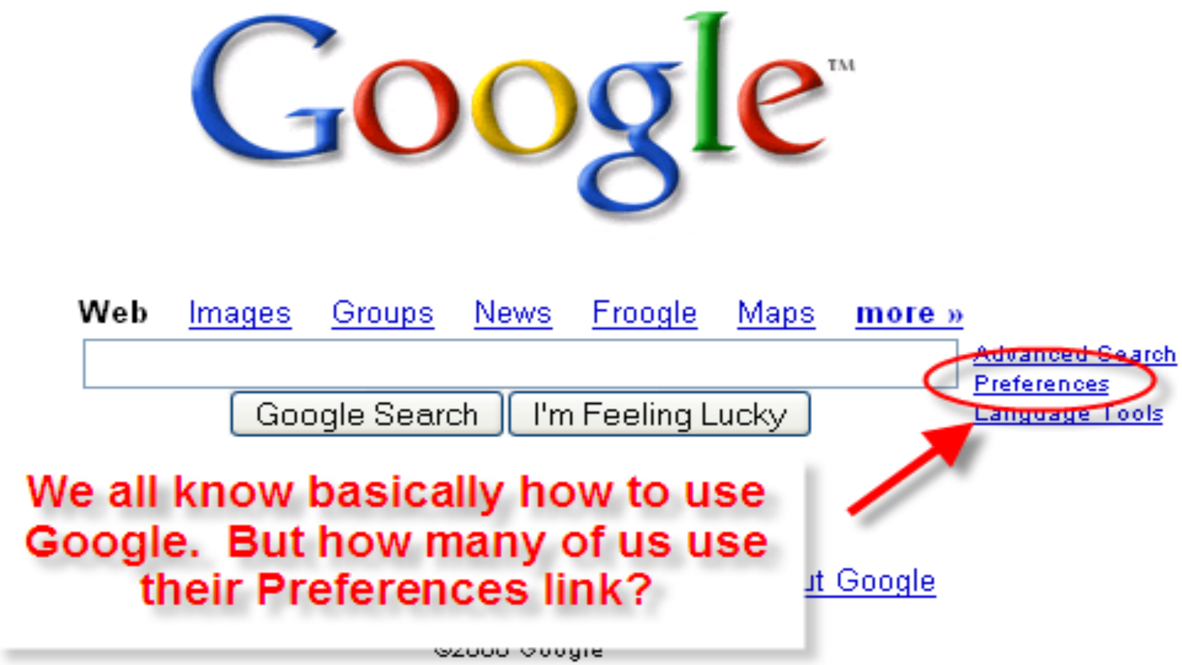
- Google is an ideal tool for this

- If done carefully, targets wont event notice they were being profiled and examined on their week points.

The Basics

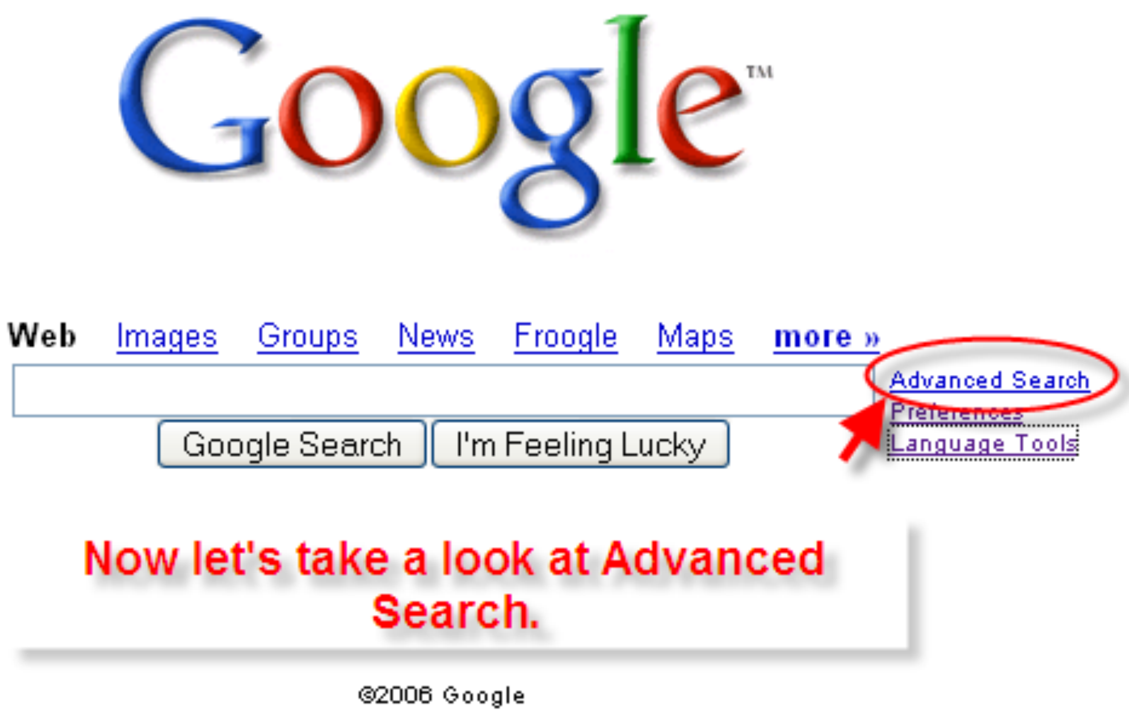
- To set the stage for what I will demo, it is necessary to understand some of Google’s advanced search functions.
- This will not be an exhaustive list, just an intro.
- Creative use of these functions is the key to successful Google Hacking.

The Basics



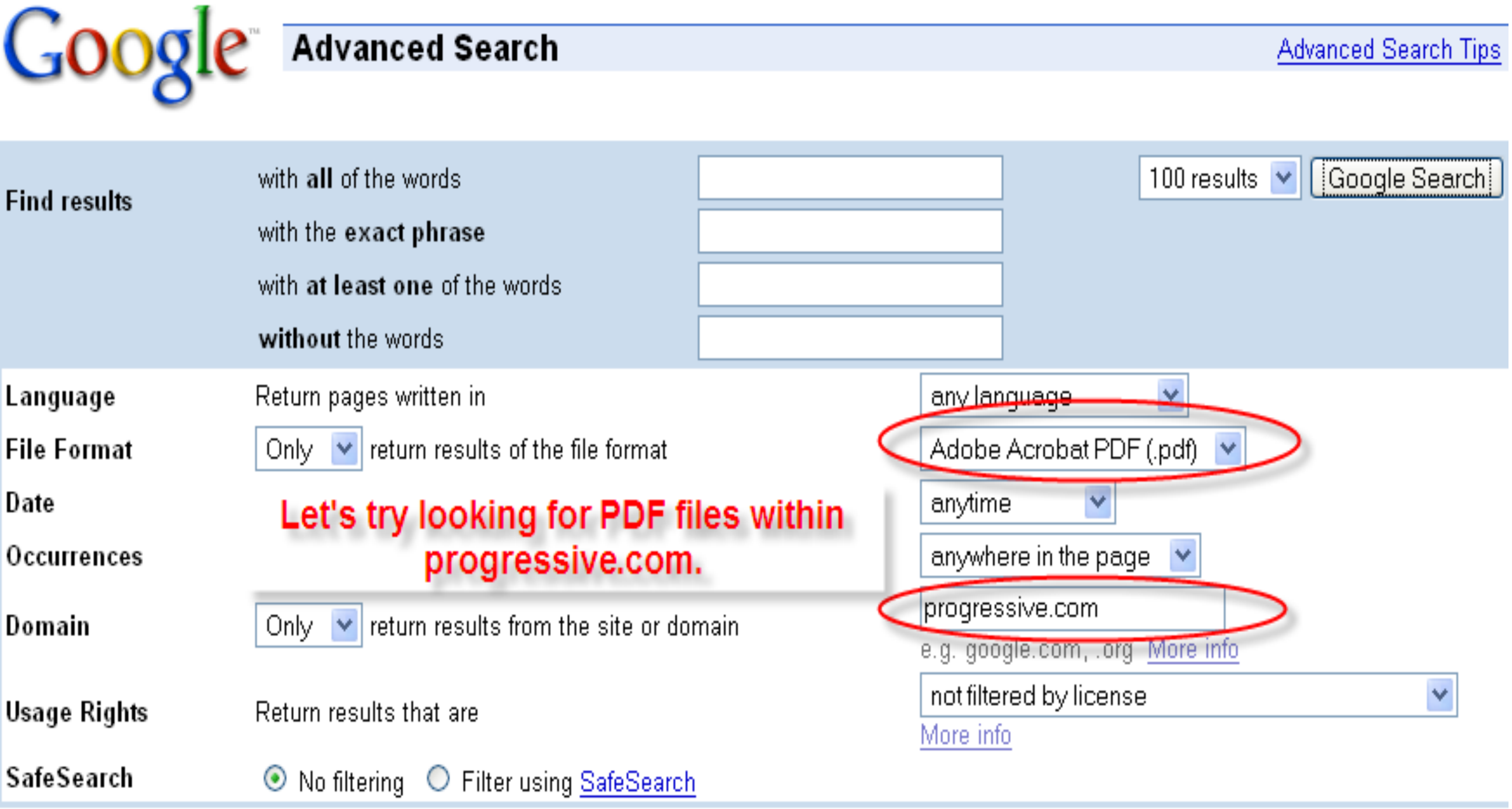
We all know basically how to use Google. But how many of us use their Preferences link?

The Basics



Now let's take a look at Advanced Search.

The Basics



Advanced Search

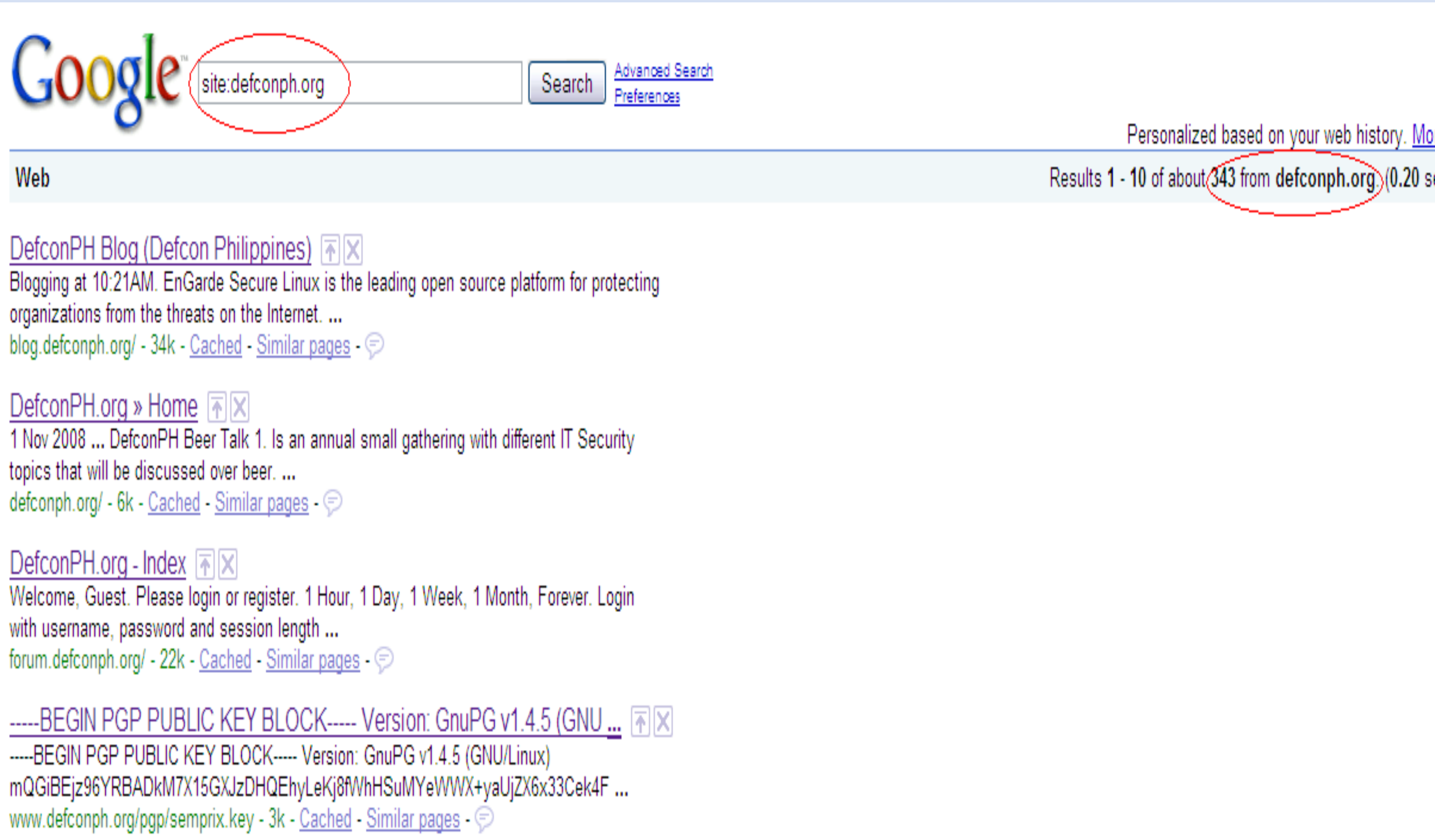
Advanced Search Tips

Find results	with **all** of the words	
	with the **exact phrase**	
	with **at least one** of the words	
	without the words	
Language	Return pages written in	any language
File Format	Only return results of the file format	Adobe Acrobat PDF (.pdf)
Date		anytime
Occurrences		anywhere in the page
Domain	Only return results from the site or domain	progressive.com e.g. google.com, .org More info
Usage Rights	Return results that are	not filtered by license More info
SafeSearch	● No filtering ○ Filter using SafeSearch	

Let's try looking for PDF files within progressive.com.

The Basics

Now its time to take a close look on the interesting Google Search Commands



site:defconph.org

Personalized based on your web history. Mo

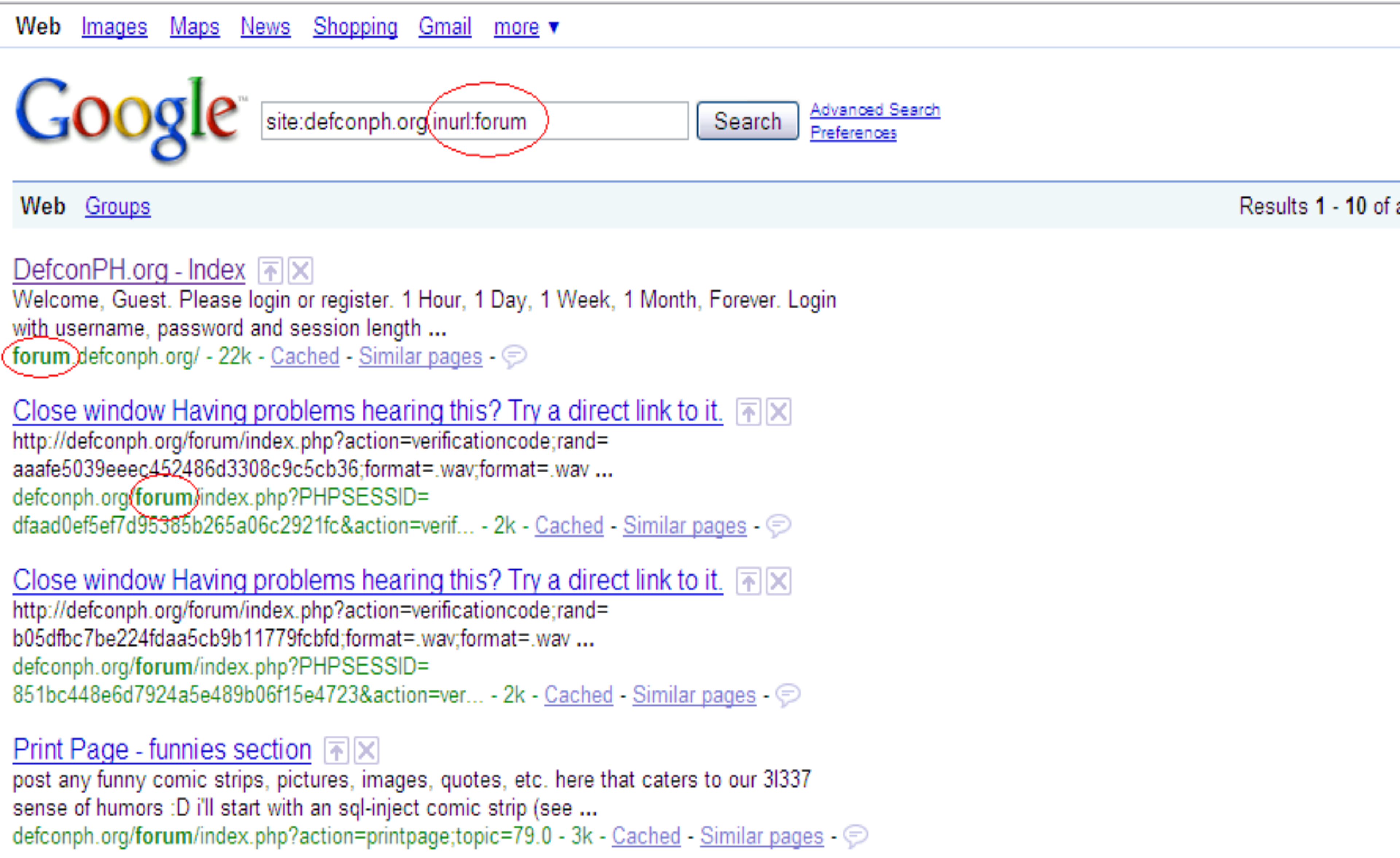
Results **1** - **10** of about **343** from **defconph.org**. (0.20 s

DefconPH Blog (Defcon Philippines)
Blogging at 10:21AM. EnGarde Secure Linux is the leading open source platform for protecting organizations from the threats on the Internet. **...**
blog.defconph.org/ - 34k - Cached - Similar pages -

DefconPH.org » Home
1 Nov 2008 **...** DefconPH Beer Talk 1. Is an annual small gathering with different IT Security topics that will be discussed over beer. **...**
defconph.org/ - 6k - Cached - Similar pages -

DefconPH.org - Index
Welcome, Guest. Please login or register. 1 Hour, 1 Day, 1 Week, 1 Month, Forever. Login with username, password and session length **...**
forum.defconph.org/ - 22k - Cached - Similar pages -

-----BEGIN PGP PUBLIC KEY BLOCK----- Version: GnuPG v1.4.5 (GNU **...**
-----BEGIN PGP PUBLIC KEY BLOCK----- Version: GnuPG v1.4.5 (GNU/Linux) mQGiBEjz96YRBADkM7X15GXJzDHQEhyLeKj8fWhHSuMYeWWX+yaUjZX6x33Cek4F **...**
www.defconph.org/pgp/semprix.key - 3k - Cached - Similar pages -



site:defconph.org inurl:forum

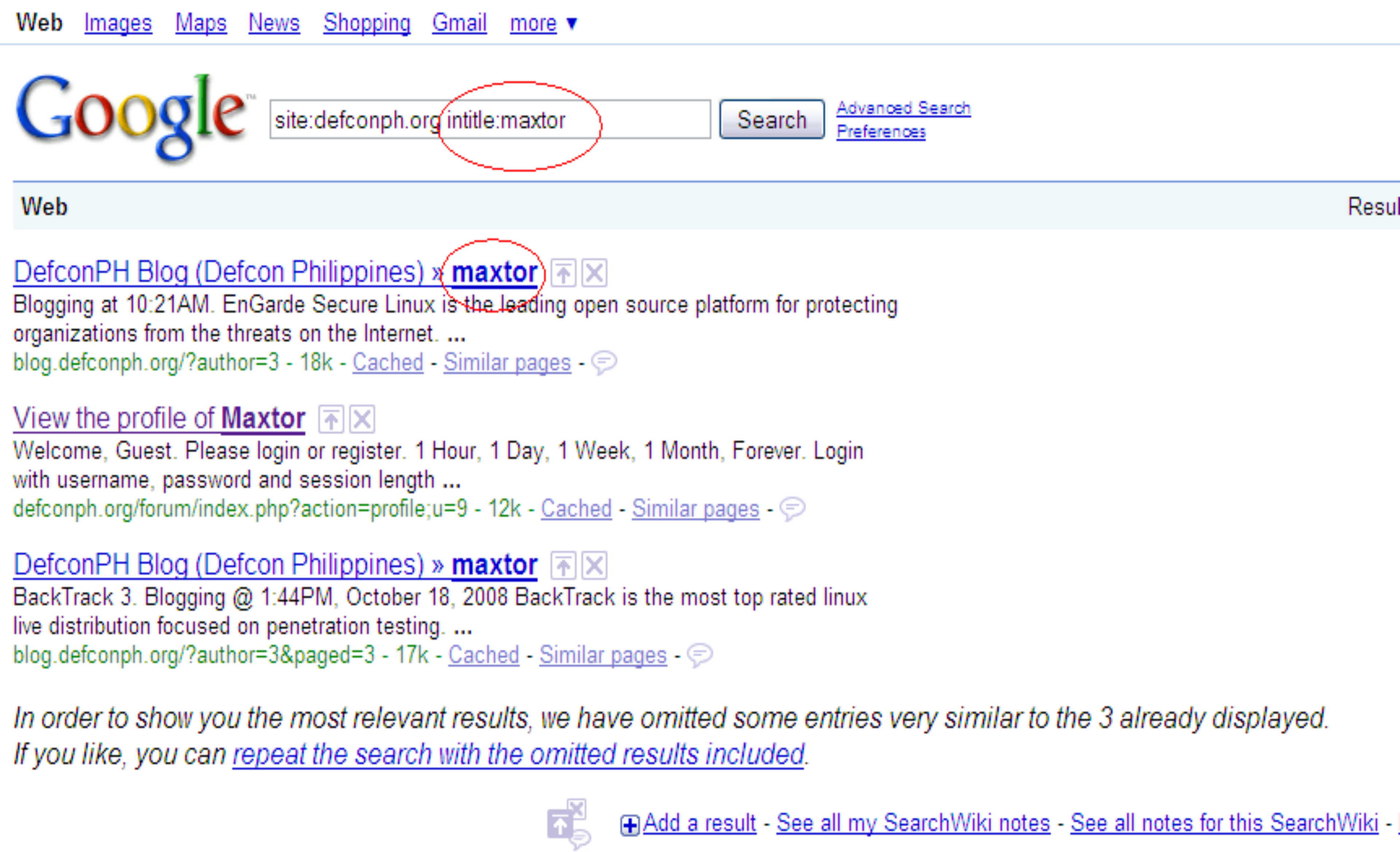
Results **1** - **10** of a

DefconPH.org - Index
Welcome, Guest. Please login or register. 1 Hour, 1 Day, 1 Week, 1 Month, Forever. Login with username, password and session length **...**
forum.defconph.org/ - 22k - Cached - Similar pages -

Close window Having problems hearing this? Try a direct link to it.
http://defconph.org/forum/index.php?action=verificationcode;rand= aaafe5039eeec452486d3308c9c5cb36;format=.wav;format=.wav **...**
defconph.org/**forum**/index.php?PHPSESSID= dfaad0ef5ef7d95385b265a06c2921fc&action=verif... - 2k - Cached - Similar pages -

Close window Having problems hearing this? Try a direct link to it.
http://defconph.org/forum/index.php?action=verificationcode;rand= b05dfbc7be224fdaa5cb9b11779fcbfd;format=.wav;format=.wav **...**
defconph.org/**forum**/index.php?PHPSESSID= 851bc448e6d7924a5e489b06f15e4723&action=ver... - 2k - Cached - Similar pages -

Print Page - funnies section
post any funny comic strips, pictures, images, quotes, etc. here that caters to our 3l337 sense of humors :D i'll start with an sql-inject comic strip (see **...**
defconph.org/**forum**/index.php?action=printpage;topic=79.0 - 3k - Cached - Similar pages -



site:defconph.org intitle:maxtor

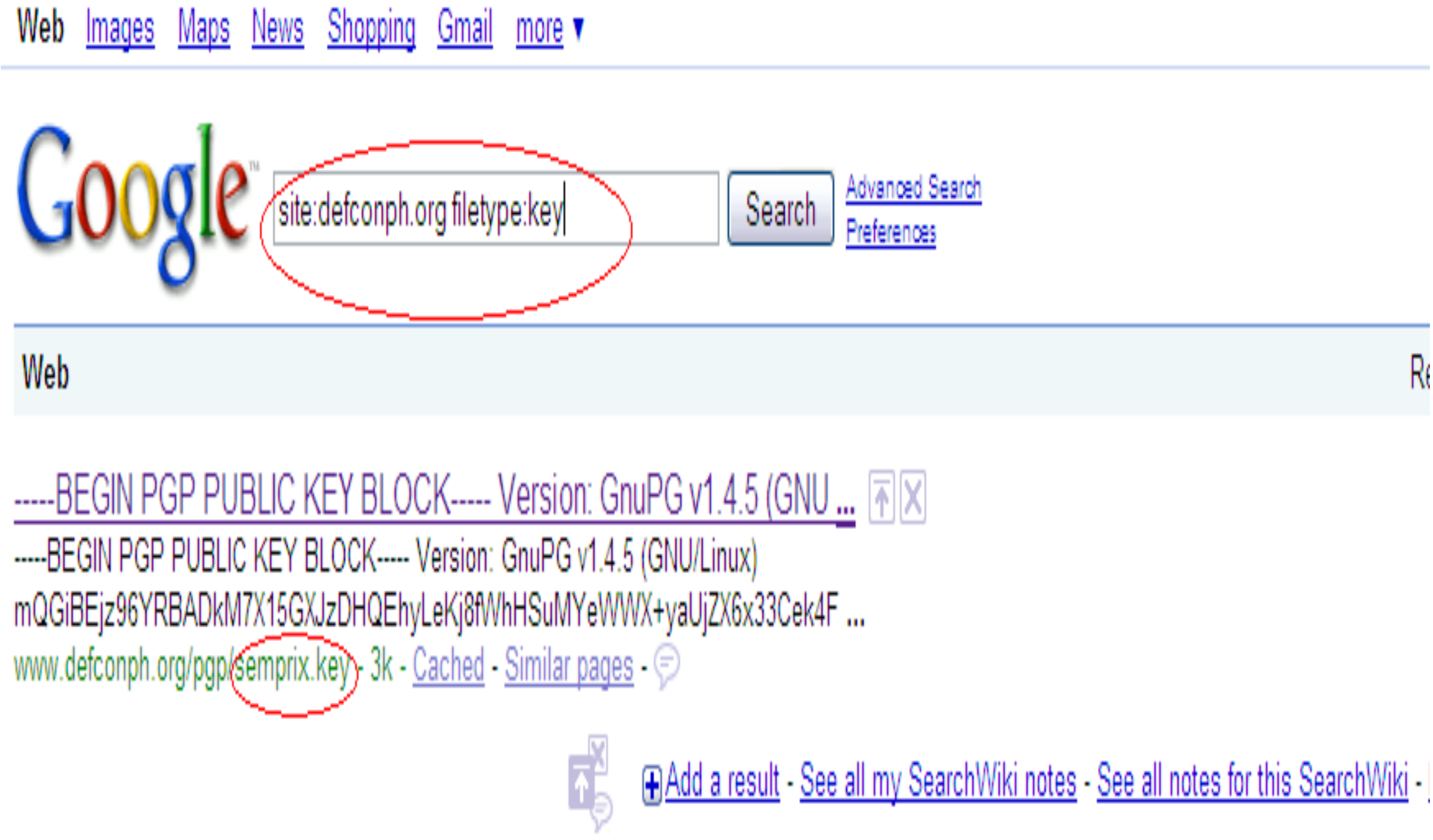
DefconPH Blog (Defcon Philippines) » **maxtor**
Blogging at 10:21AM. EnGarde Secure Linux is the leading open source platform for protecting organizations from the threats on the Internet. **...**
blog.defconph.org/?author=3 - 18k - Cached - Similar pages -

View the profile of **Maxtor**
Welcome, Guest. Please login or register. 1 Hour, 1 Day, 1 Week, 1 Month, Forever. Login with username, password and session length **...**
defconph.org/forum/index.php?action=profile;u=9 - 12k - Cached - Similar pages -

DefconPH Blog (Defcon Philippines) » **maxtor**
BackTrack 3. Blogging @ 1:44PM, October 18, 2008 BackTrack is the most top rated linux live distribution focused on penetration testing. **...**
blog.defconph.org/?author=3&paged=3 - 17k - Cached - Similar pages -

In order to show you the most relevant results, we have omitted some entries very similar to the 3 already displayed.
If you like, you can repeat the search with the omitted results included.

⊞ Add a result - See all my SearchWiki notes - See all notes for this SearchWiki -



site:defconph.org filetype:key

-----BEGIN PGP PUBLIC KEY BLOCK----- Version: GnuPG v1.4.5 (GNU ...

-----BEGIN PGP PUBLIC KEY BLOCK----- Version: GnuPG v1.4.5 (GNU/Linux) mQGiBEjz96YRBADkM7X15GXJzDHQEhyLeKj8fWhHSuMYeWWX+yaUjZX6x33Cek4F ...

www.defconph.org/pgp/semprix.key - 3k - Cached - Similar pages -

The Basics

There are many more advanced operators

http://www.googleguide.com/advanced_operators_reference.html

The Basics

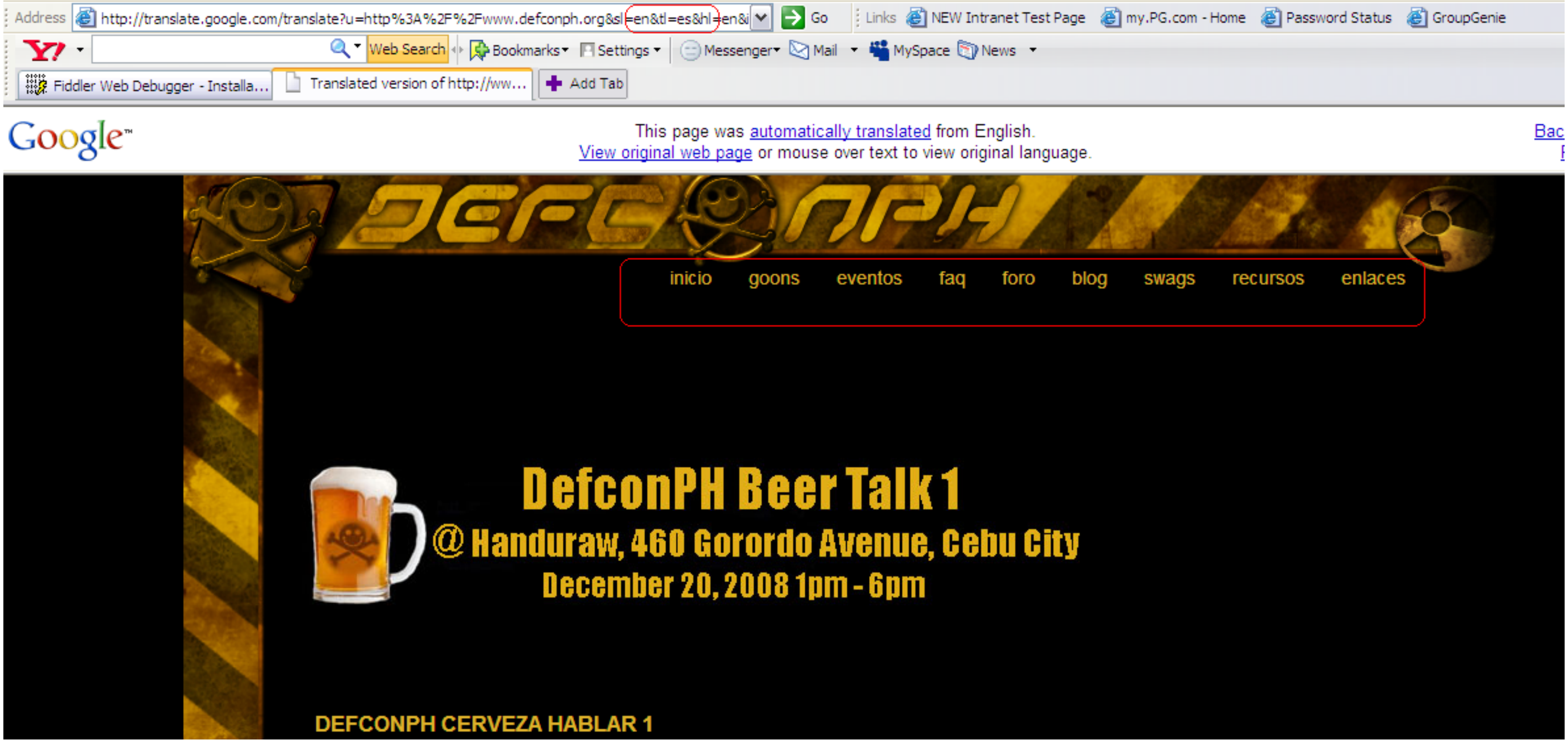
- Some other things to keep in mind
  - Google queries are not case sensitive.
  - The * wildcard represents any *word*
    - Example: “* hacker quote”
  - Google stems words automatically
    - Example: “hacker blog quote” brings up sites with “hacker … “.

The Basics

- The + symbol forces inclusion of a certain word.
  - “blog defconph +defconph”
- We’ve already seen the – symbol.
- The | symbol provides boolean OR logic.
  - “blog defconph +inurl:(defconph | maxtor)”

This is getting boring already, lets get this stuff out of the way and get some Google Hacking.

Google as Anonymouse Proxy

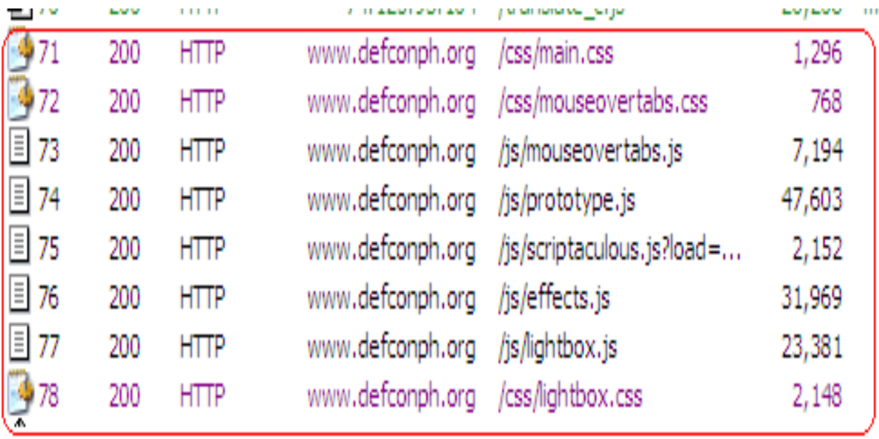


This page was automatically translated from English.
View original web page or mouse over text to view original language.

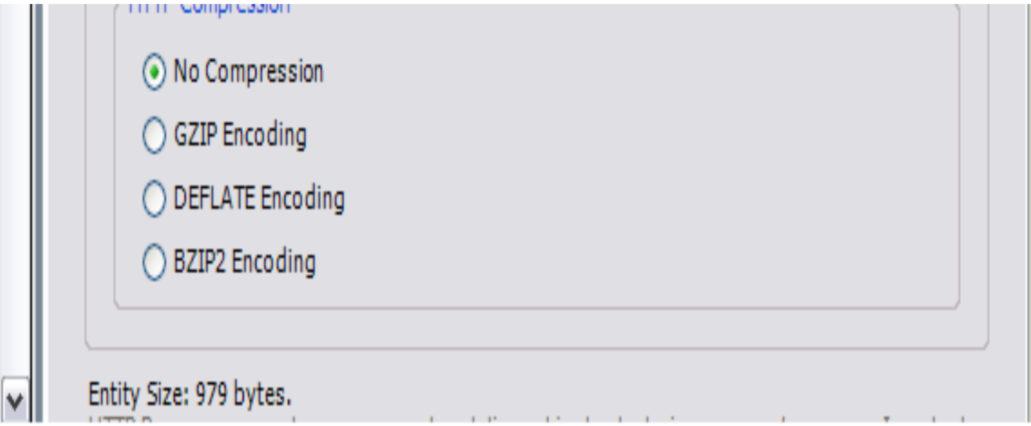
DefconPH Beer Talk 1
@ Handuraw, 460 Gorordo Avenue, Cebu City
December 20, 2008 1pm - 6pm

DEFCONPH CERVEZA HABLAR 1

We will check if we are anonymous



71	200	HTTP	www.defconph.org	/css/main.css	1,296
72	200	HTTP	www.defconph.org	/css/mouseovertabs.css	768
73	200	HTTP	www.defconph.org	/js/mouseovertabs.js	7,194
74	200	HTTP	www.defconph.org	/js/prototype.js	47,603
75	200	HTTP	www.defconph.org	/js/scriptaculous.js?load=...	2,152
76	200	HTTP	www.defconph.org	/js/effects.js	31,969
77	200	HTTP	www.defconph.org	/js/lightbox.js	23,381
78	200	HTTP	www.defconph.org	/css/lightbox.css	2,148



HTTP Compression

● No Compression

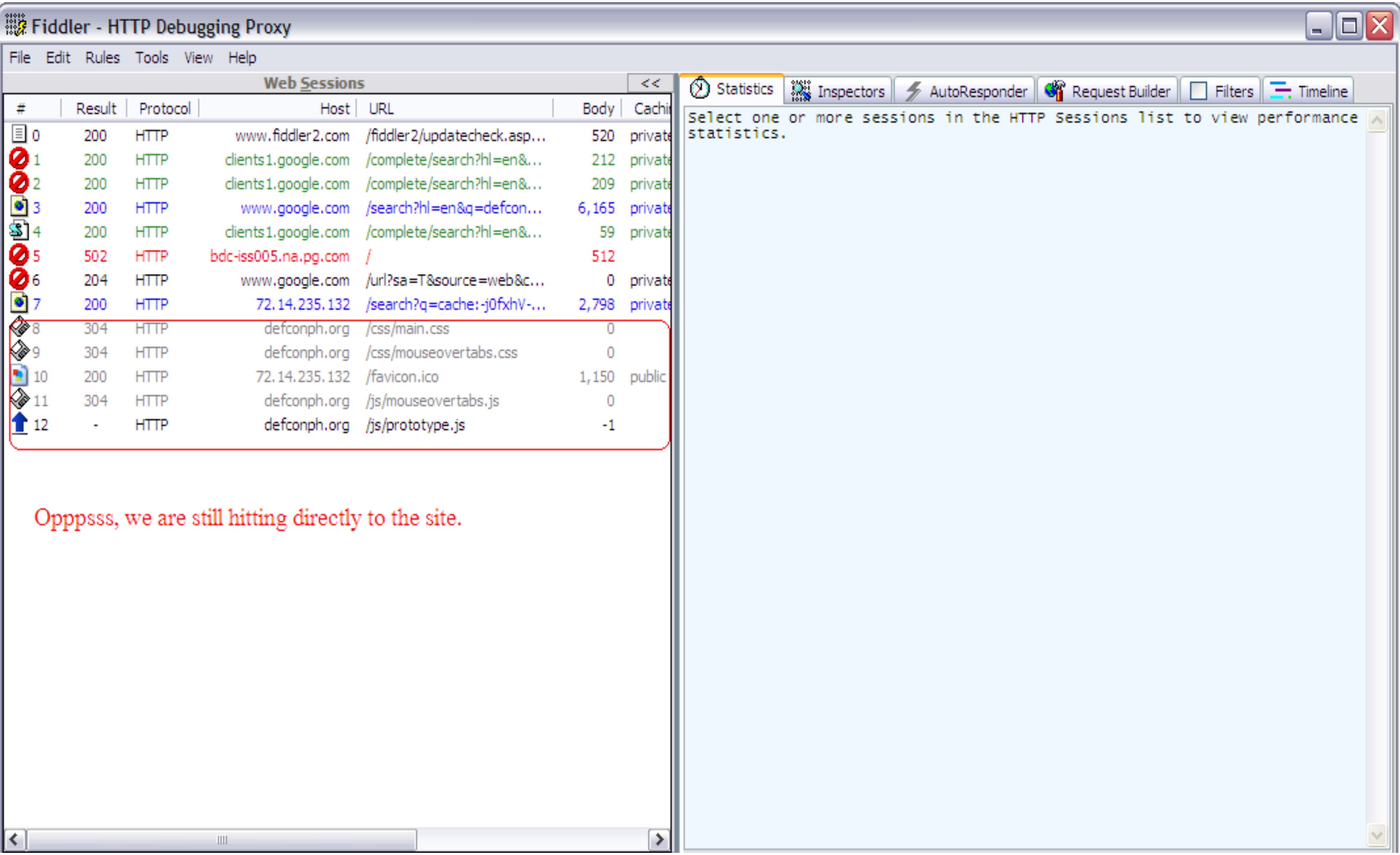
○ GZIP Encoding

○ DEFLATE Encoding

○ BZIP2 Encoding

Entity Size: 979 bytes.

We used Fiddler to Debug our session
We will check if Google cache allows us to become anonymous.

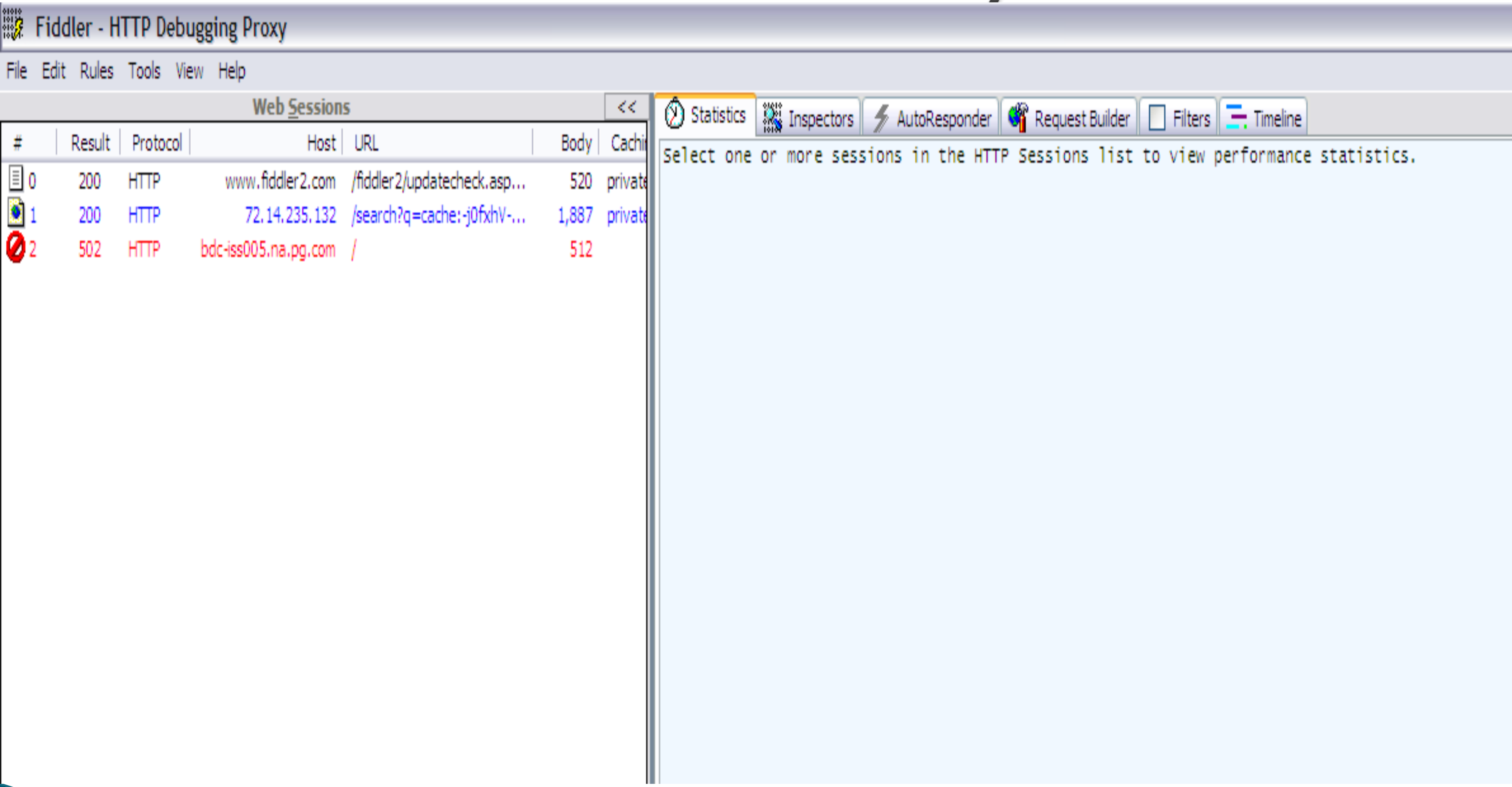


#	Result	Protocol	Host	URL	Body	Cachi
0	200	HTTP	www.fiddler2.com	/fiddler2/updatecheck.asp...	520	private
1	200	HTTP	clients1.google.com	/complete/search?hl=en&...	212	private
2	200	HTTP	clients1.google.com	/complete/search?hl=en&...	209	private
3	200	HTTP	www.google.com	/search?hl=en&q=defcon...	6,165	private
4	200	HTTP	clients1.google.com	/complete/search?hl=en&...	59	private
5	502	HTTP	bdc-iss005.na.pg.com	/	512	
6	204	HTTP	www.google.com	/url?sa=T&source=web&c...	0	private
7	200	HTTP	72.14.235.132	/search?q=cache:-j0fxhV-...	2,798	private
8	304	HTTP	defconph.org	/css/main.css	0	
9	304	HTTP	defconph.org	/css/mouseovertabs.css	0	
10	200	HTTP	72.14.235.132	/favicon.ico	1,150	public
11	304	HTTP	defconph.org	/js/mouseovertabs.js	0	
12	-	HTTP	defconph.org	/js/prototype.js	-1	

Opppsss, we are still hitting directly to the site.

Select one or more sessions in the HTTP Sessions list to view performance statistics.

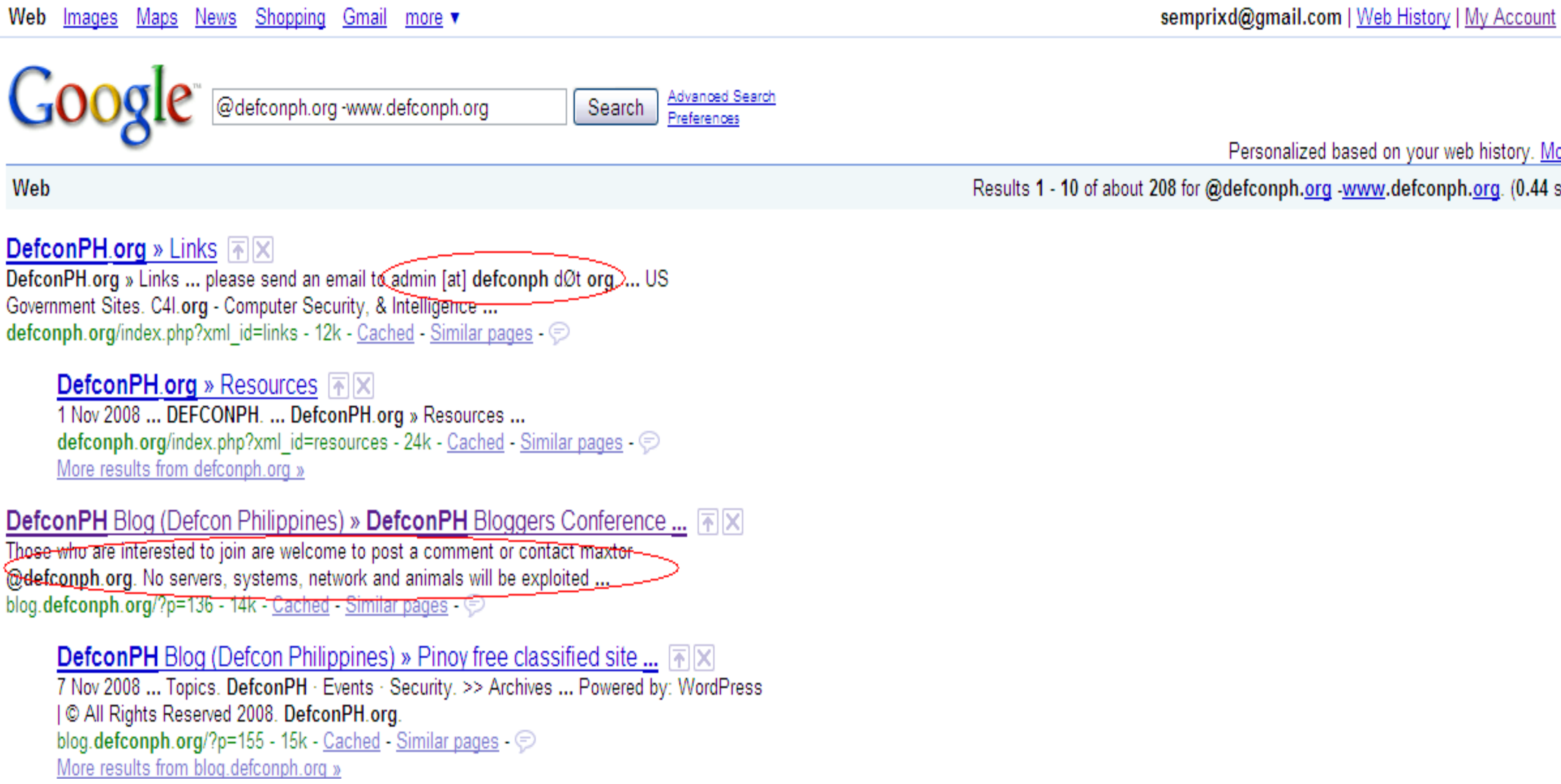
Cached with Text only version



#	Result	Protocol	Host	URL	Body	Cachi
0	200	HTTP	www.fiddler2.com	/fiddler2/updatecheck.asp...	520	private
1	200	HTTP	72.14.235.132	/search?q=cache:-j0fxhV-...	1,887	private
2	502	HTTP	bdc-iss005.na.pg.com	/	512	

```
Select one or more sessions in the HTTP Sessions list to view performance statistics.
```

Trolling Emails on Google


Web Images Maps News Shopping Gmail more ▾
semprixd@gmail.com | Web History | My Account
Google
Search
Advanced Search
Preferences

@defconph.org -www.defconph.org

Personalized based on your web history. Mo

Web

Results **1** - **10** of about **208** for **@defconph.org -www.defconph.org**. (**0.44** s

DefconPH.org » Links

DefconPH.org » Links ... please send an email to admin [at] **defconph** dØt **org** ... US Government Sites. C4I.**org** - Computer Security, & Intelligence ...

defconph.org/index.php?xml_id=links - 12k - Cached - Similar pages -

DefconPH.org » Resources

1 Nov 2008 ... DEFCONPH. ... **DefconPH.org** » Resources ...

defconph.org/index.php?xml_id=resources - 24k - Cached - Similar pages -

More results from defconph.org »

DefconPH Blog (Defcon Philippines) » **DefconPH** Bloggers Conference ...

Those who are interested to join are welcome to post a comment or contact maxtor **@defconph.org**. No servers, systems, network and animals will be exploited ...

blog.**defconph.org**/?p=136 - 14k - Cached - Similar pages -

DefconPH Blog (Defcon Philippines) » Pinoy free classified site ...

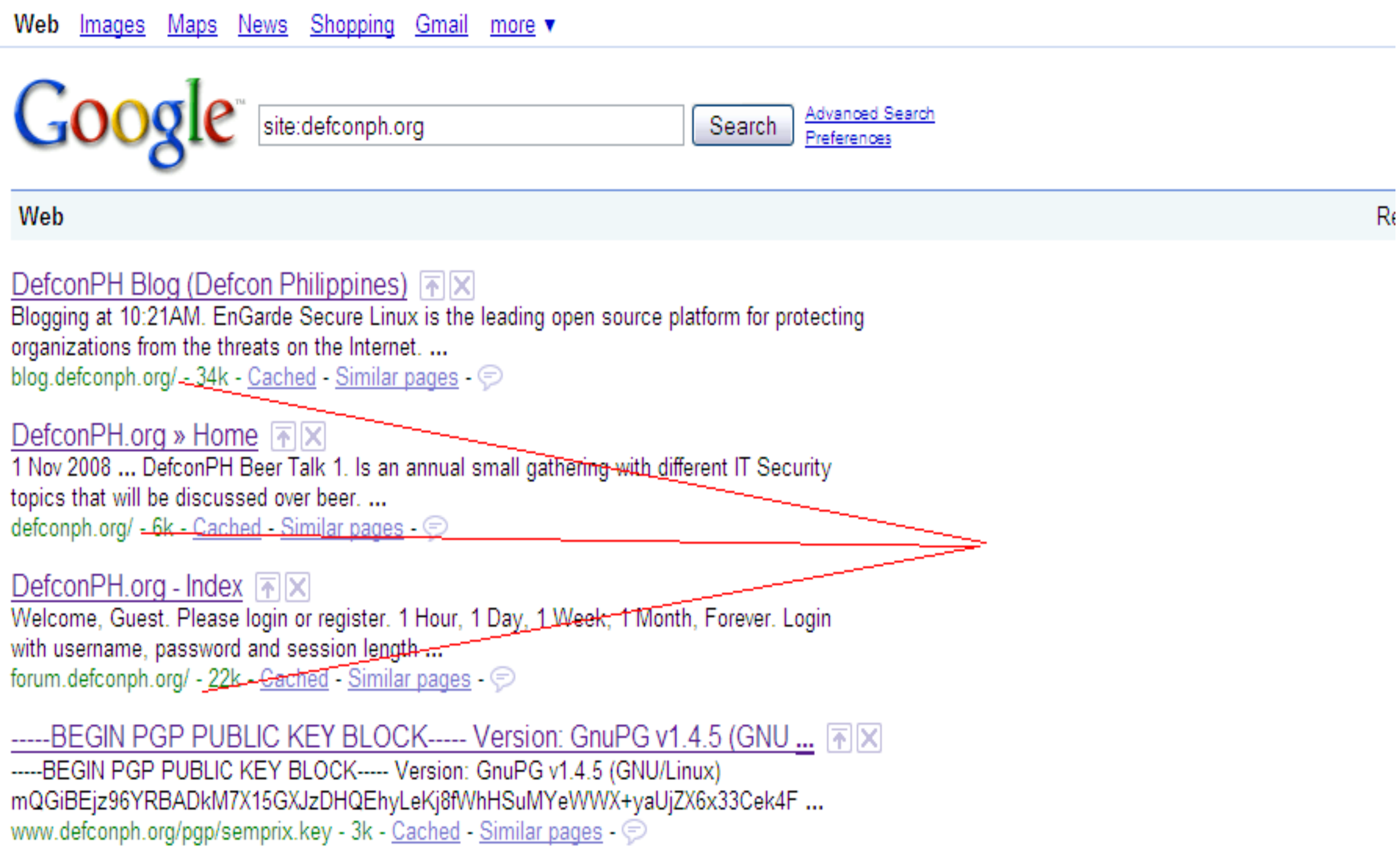
7 Nov 2008 ... Topics. **DefconPH** · Events · Security. >> Archives ... Powered by: WordPress | © All Rights Reserved 2008. **DefconPH.org**.

blog.**defconph.org**/?p=155 - 15k - Cached - Similar pages -

More results from blog.defconph.org »

Network Mapping

- A hacker could use Google to obtain a list of all defconph.org domain names that are indexed by Google.
- Some interesting domain names may be found deep within the search results.



site:defconph.org

DefconPH Blog (Defcon Philippines)
Blogging at 10:21AM. EnGarde Secure Linux is the leading open source platform for protecting organizations from the threats on the Internet. ...
blog.defconph.org/ - 34k - Cached - Similar pages -

DefconPH.org » Home
1 Nov 2008 ... DefconPH Beer Talk 1. Is an annual small gathering with different IT Security topics that will be discussed over beer. ...
defconph.org/ - 6k - Cached - Similar pages -

DefconPH.org - Index
Welcome, Guest. Please login or register. 1 Hour, 1 Day, 1 Week, 1 Month, Forever. Login with username, password and session length ...
forum.defconph.org/ - 22k - Cached - Similar pages -

-----BEGIN PGP PUBLIC KEY BLOCK----- Version: GnuPG v1.4.5 (GNU ...
-----BEGIN PGP PUBLIC KEY BLOCK----- Version: GnuPG v1.4.5 (GNU/Linux) mQGiBEjz96YRBADkM7X15GXJzDHQEhyLeKj8fWhHSuMYeWWX+yaUjZX6x33Cek4F ...
www.defconph.org/pgp/semprix.key - 3k - Cached - Similar pages -

Automated Google Hacking

- It would be easy write a script that automates these types of queries against google.com and compiles the results.
- Lots of sample code is available, including C# code.
- A tool called GooScan does this.
- But this goes against Google's Terms of Use.
- Google is rumored to keep a "black list" of bad IP addresses, so be careful!

Google Query APIs

- Google used to provide a web service API for doing automated queries.
- This API is no longer available.
- Alternatives that break Google’s Terms of Use:
  - Evil API
  - Aura API

DNS-Mine.pl

- Attempts to get a list of domain names, similar to what I just demonstrated manually.
- Written by Roelof Temmingh of Sensepost.com
- Uses Google API

Sitedigger

- Automated Google hacking tool from Foundstone
- Uses Google API
- Written in .Net
- Uses Google Hacking Database

Google Hacking Database

- Located at johnny.ihackstuff.com
- Contains list of Google hacks, constantly updated
- Demo

How To Protect Your Websites From Google Hackers

- In general, be very careful about what content you place on your Internet–facing websites.
- Do not display detailed error messages.
- Do not allow directory browsing.

How To Protect Your Websites From Google Hackers

- Keep all of your links environment specific
- Keep your name and email out of HTML comments and don’t post on Google Groups with your work email account.
- Configure your web server to only serve up a list of “safe” file types and to respond with “File Not Found” for any unsafe types.

For More Info

- “Google Hacking For Penetration Testers” Volume 2 by Johnny Long
- http://johnny.ihackstuff.com
- http://www.sensepost.com
- http://www.foundstone.com
- http://www.google.com

QUESTIONS ?????????????????