Google dork

What is Dorking?

A Google dork query, sometimes just referred to as a dork, is a search string that uses advanced search operators to find information that is not readily available on a website. Google **dorking**, also known as Google hacking, can return information that is difficult to locate through simple search queries.

What is meant by Google dorks?

A **Google dork** is an employee who unknowingly exposes sensitive corporate information on the Internet. As a passive attack method, **Google** dorking can return usernames and passwords, email lists, sensitive documents, personally identifiable financial information (PIFI) and website vulnerabilities.

Google dork query

A Google dork query, sometimes just referred to as a dork, is a search string that uses advanced search operators to find information that is not readily available on a website.

Google dorking, also known as Google hacking, can return information that is difficult to locate through simple search queries. That description includes information that is not intended for public viewing but that has not been adequately protected.

As a passive attack method, Google dorking can return usernames and passwords, email lists, sensitive documents, personally identifiable financial information (PIFI) and website vulnerabilities. That information can be used for any number of illegal activities, including cyberterrorism, industrial espionage, identity theft and cyberstalking.

A search parameter is a limitation applied to a search. Here are a few examples of advanced search parameters:

- *site:* returns files located on a particular website or domain.
- *filetype:* followed (without a space) by a file extension returns files of the specified type, such as DOC, PDF, XLS and INI. Multiple file types can be searched for simultaneously by separating extensions with "|".
- *inurl:* followed by a particular string returns results with that sequence of characters in the URL.
- *intext:* followed by the searcher's chosen word or phrase returns files with the string anywhere in the text.

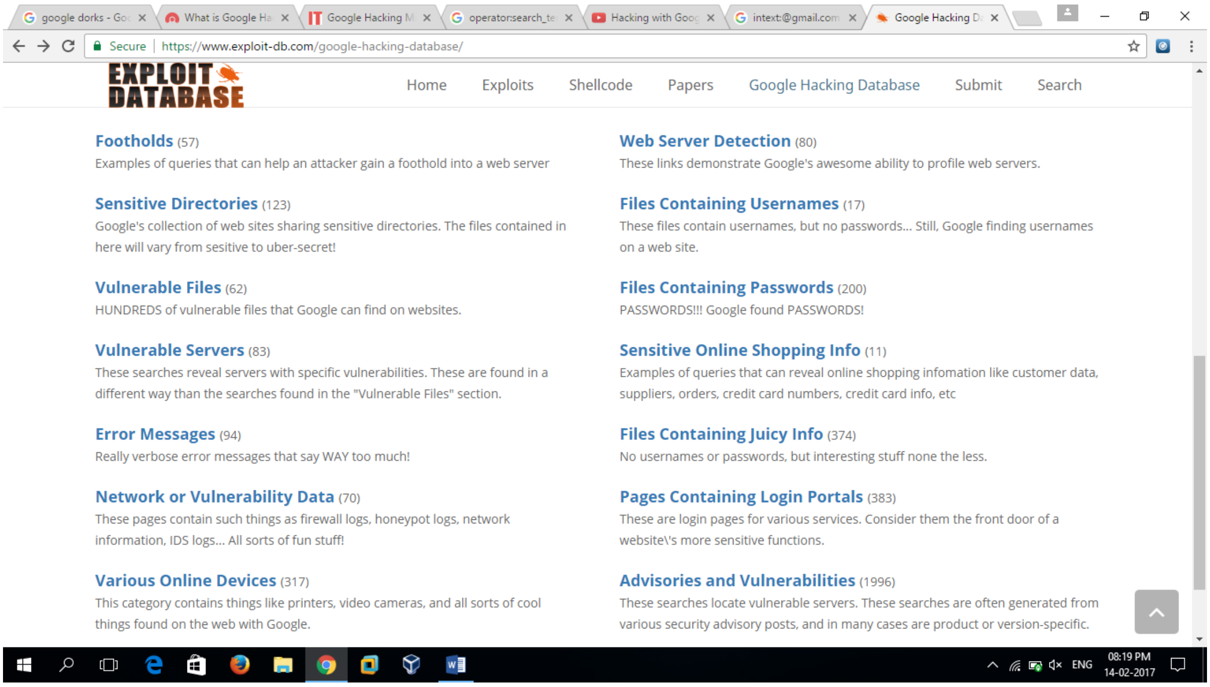
Multiple parameters can be used, for example, to search for files of a certain type on a certain website or domain. The Public Intelligence website provides this example:

"sensitive but unclassified" filetype:pdf site:publicintelligence.net

Those search parameters return PDF documents on that website's servers with the string "sensitive but unclassified" anywhere in the document text.

Access to internal documents can yield further sensitive information. For example, document metadata often contains more information than the author is aware of, such as revision history, deletions, dates and author / updater names. Because an intruder with the requisite know-how and / or tools can access such information, it's a good practice to ensure that it is actually removed from documents before they are published or shared. The practice of document sanitization is designed to make sure that only the intended information can be accessed.

https://www.exploit-db.com/google-hacking-databas


https://www.exploit-db.com/google-hacking-database/

Footholds (57)
Examples of queries that can help an attacker gain a foothold into a web server

Sensitive Directories (123)
Google's collection of web sites sharing sensitive directories. The files contained in here will vary from sesitive to uber-secret!

Vulnerable Files (62)
HUNDREDS of vulnerable files that Google can find on websites.

Vulnerable Servers (83)
These searches reveal servers with specific vulnerabilities. These are found in a different way than the searches found in the "Vulnerable Files" section.

Error Messages (94)
Really verbose error messages that say WAY too much!

Network or Vulnerability Data (70)
These pages contain such things as firewall logs, honeypot logs, network information, IDS logs... All sorts of fun stuff!

Various Online Devices (317)
This category contains things like printers, video cameras, and all sorts of cool things found on the web with Google.

Web Server Detection (80)
These links demonstrate Google's awesome ability to profile web servers.

Files Containing Usernames (17)
These files contain usernames, but no passwords... Still, Google finding usernames on a web site.

Files Containing Passwords (200)
PASSWORDS!!! Google found PASSWORDS!

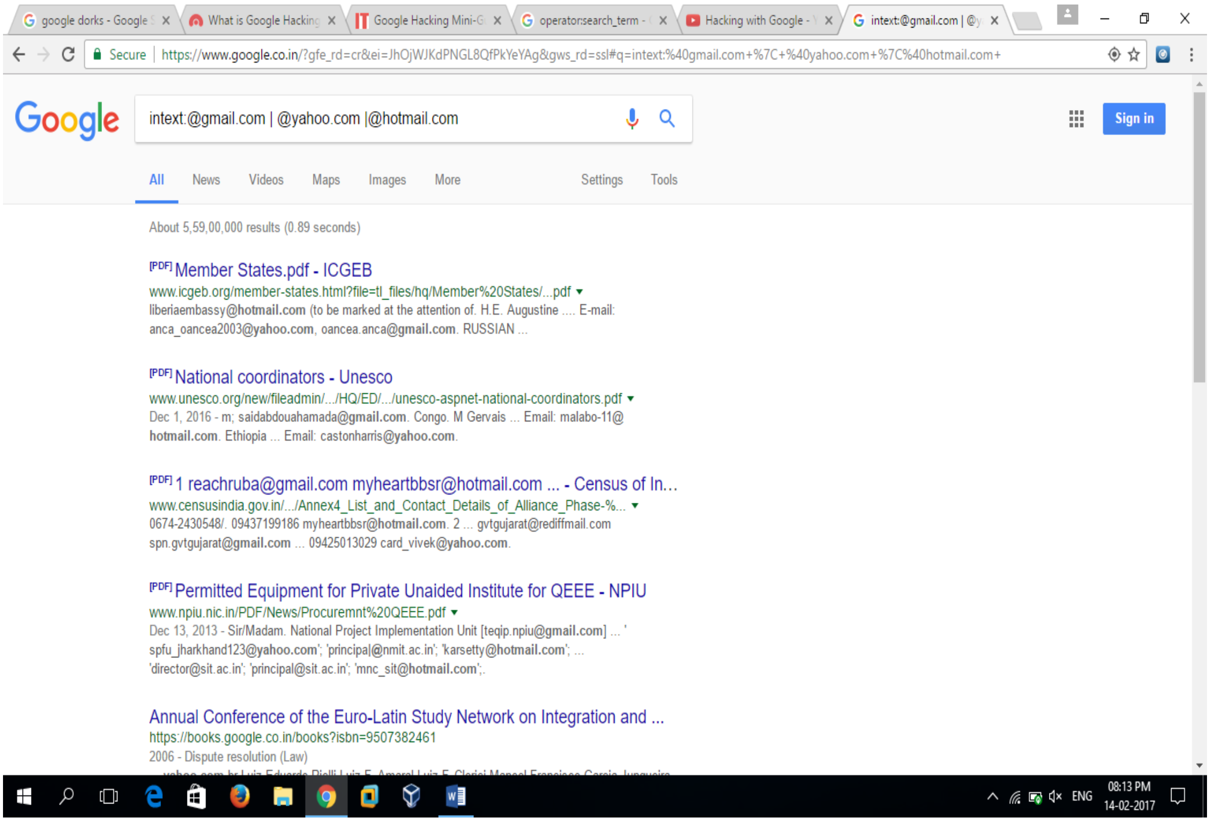
Sensitive Online Shopping Info (11)
Examples of queries that can reveal online shopping infomation like customer data, suppliers, orders, credit card numbers, credit card info, etc

Files Containing Juicy Info (374)
No usernames or passwords, but interesting stuff none the less.

Pages Containing Login Portals (383)
These are login pages for various services. Consider them the front door of a website\'s more sensitive functions.

Advisories and Vulnerabilities (1996)
These searches locate vulnerable servers. These searches are often generated from various security advisory posts, and in many cases are product or version-specific.

Examples:


https://www.google.co.in/?gfe_rd=cr&ei=JhOjWJKdPNGL8QfPkYeYAg&gws_rd=ssl#q=intext:%40gmail.com+%7C+%40yahoo.com+%7C%40hotmail.com+

intext:@gmail.com | @yahoo.com |@hotmail.com

About 5,59,00,000 results (0.89 seconds)

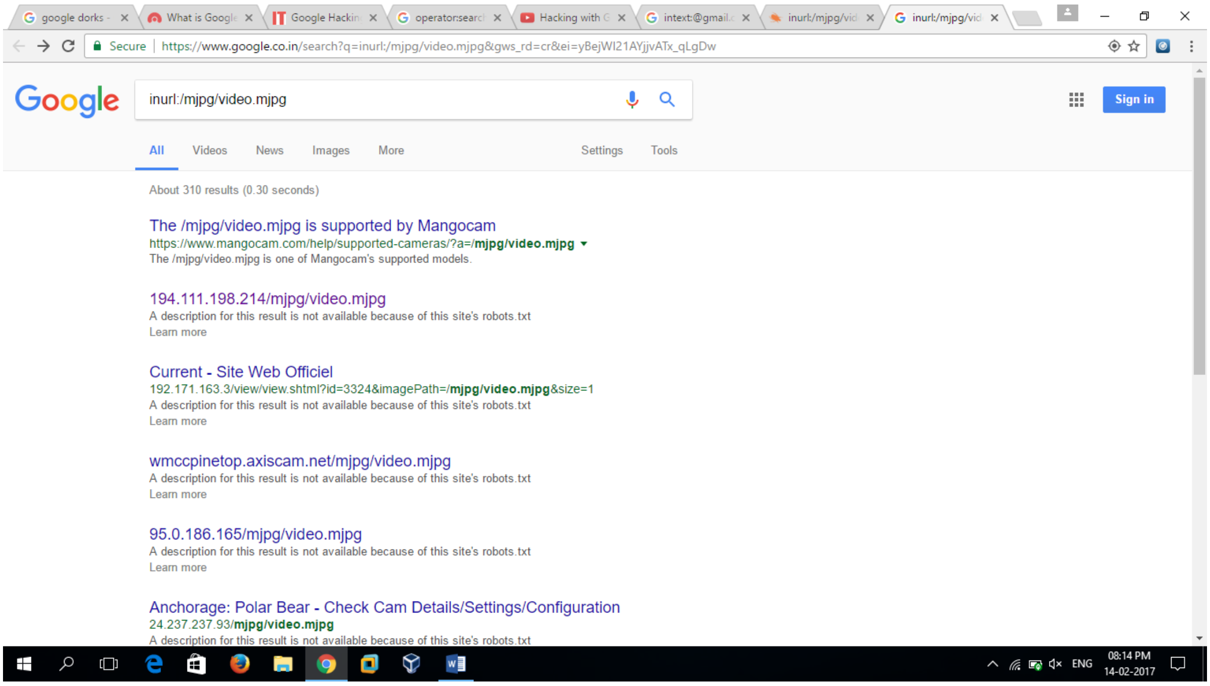
[PDF] Member States.pdf - ICGEB
www.icgeb.org/member-states.html?file=tl_files/hq/Member%20States/...pdf
liberiaembassy@**hotmail.com** (to be marked at the attention of. H.E. Augustine .... E-mail: anca_oancea2003@**yahoo.com**, oancea.anca@**gmail.com**. RUSSIAN ...

[PDF] National coordinators - Unesco
www.unesco.org/new/fileadmin/.../HQ/ED/.../unesco-aspnet-national-coordinators.pdf
Dec 1, 2016 - m; saidabdouahamada@**gmail.com**. Congo. M Gervais ... Email: malabo-11@ **hotmail.com**. Ethiopia ... Email: castonharris@**yahoo.com**.

[PDF] 1 reachruba@gmail.com myheartbbsr@hotmail.com ... - Census of In...
www.censusindia.gov.in/.../Annex4_List_and_Contact_Details_of_Alliance_Phase-%...
0674-2430548/. 09437199186 myheartbbsr@**hotmail.com**. 2 ... gvtgujarat@rediffmail.com spn.gvtgujarat@**gmail.com** ... 09425013029 card_vivek@**yahoo.com**.

[PDF] Permitted Equipment for Private Unaided Institute for QEEE - NPIU
www.npiu.nic.in/PDF/News/Procuremnt%20QEEE.pdf
Dec 13, 2013 - Sir/Madam. National Project Implementation Unit [teqip.npiu@**gmail.com**] ... ' spfu_jharkhand123@**yahoo.com**'; 'principal@nmit.ac.in'; 'karsetty@**hotmail.com**'; ... 'director@sit.ac.in'; 'principal@sit.ac.in'; 'mnc_sit@**hotmail.com**';.

Annual Conference of the Euro-Latin Study Network on Integration and ...
https://books.google.co.in/books?isbn=9507382461
2006 - Dispute resolution (Law)



https://www.google.co.in/search?q=inurl:/mjpg/video.mjpg&gws_rd=cr&ei=yBejWI21AYjjvATx_qLgDw

inurl:/mjpg/video.mjpg

About 310 results (0.30 seconds)

The /mjpg/video.mjpg is supported by Mangocam
https://www.mangocam.com/help/supported-cameras/?a=/**mjpg/video.mjpg**
The /mjpg/video.mjpg is one of Mangocam's supported models.

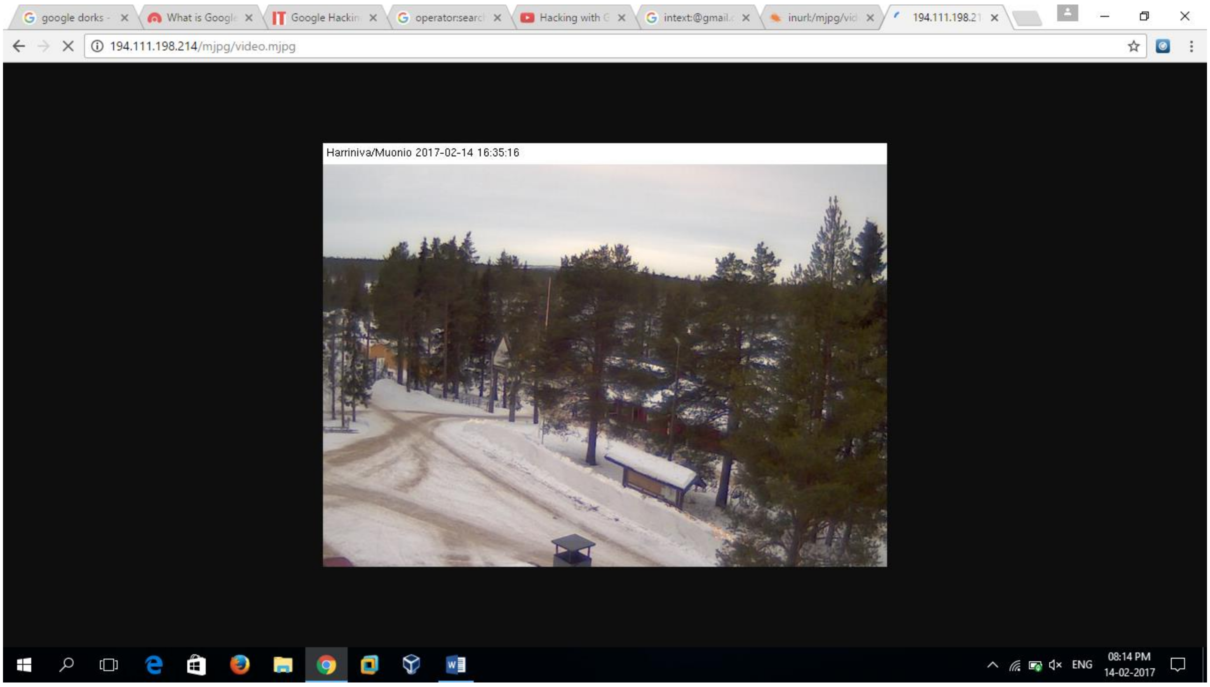
194.111.198.214/mjpg/video.mjpg
A description for this result is not available because of this site's robots.txt
Learn more

Current - Site Web Officiel
192.171.163.3/view/view.shtml?id=3324&imagePath=/**mjpg/video.mjpg**&size=1
A description for this result is not available because of this site's robots.txt
Learn more

wmccpinetop.axiscam.net/mjpg/video.mjpg
A description for this result is not available because of this site's robots.txt
Learn more

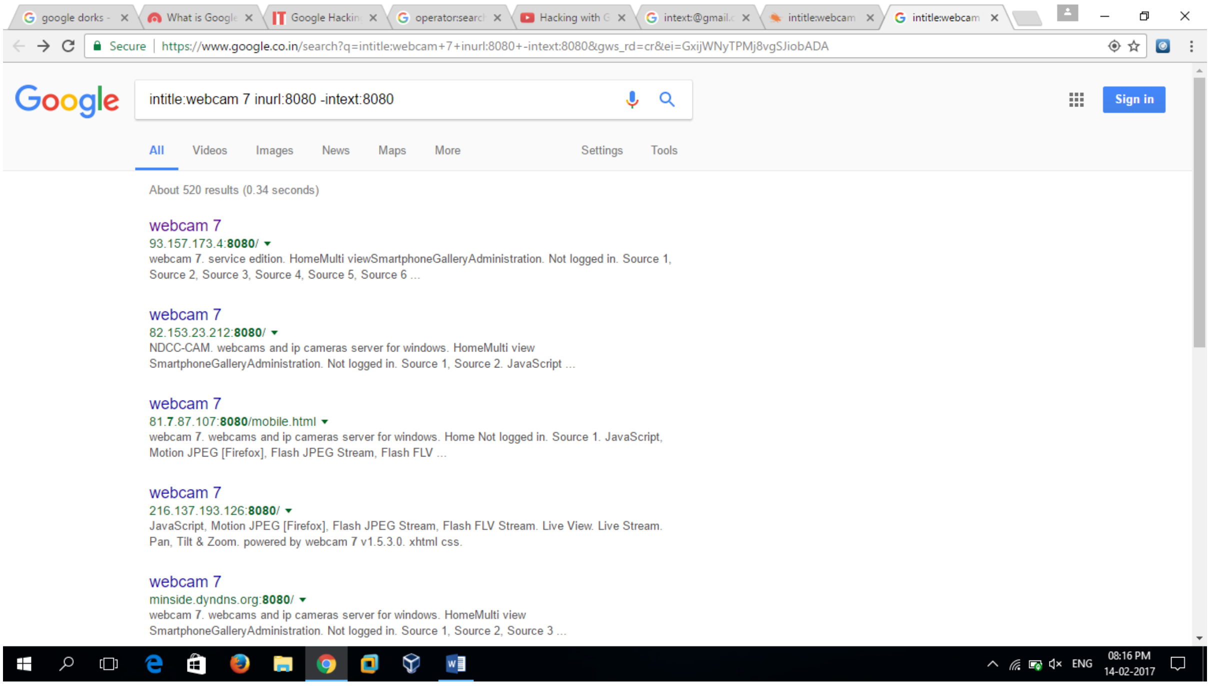
95.0.186.165/mjpg/video.mjpg
A description for this result is not available because of this site's robots.txt
Learn more

Anchorage: Polar Bear - Check Cam Details/Settings/Configuration
24.237.237.93/**mjpg/video.mjpg**
A description for this result is not available because of this site's robots.txt



194.111.198.214/mjpg/video.mjpg

Harriniva/Muonio 2017-02-14 16:35:16



intitle:webcam 7 inurl:8080 -intext:8080

About 520 results (0.34 seconds)

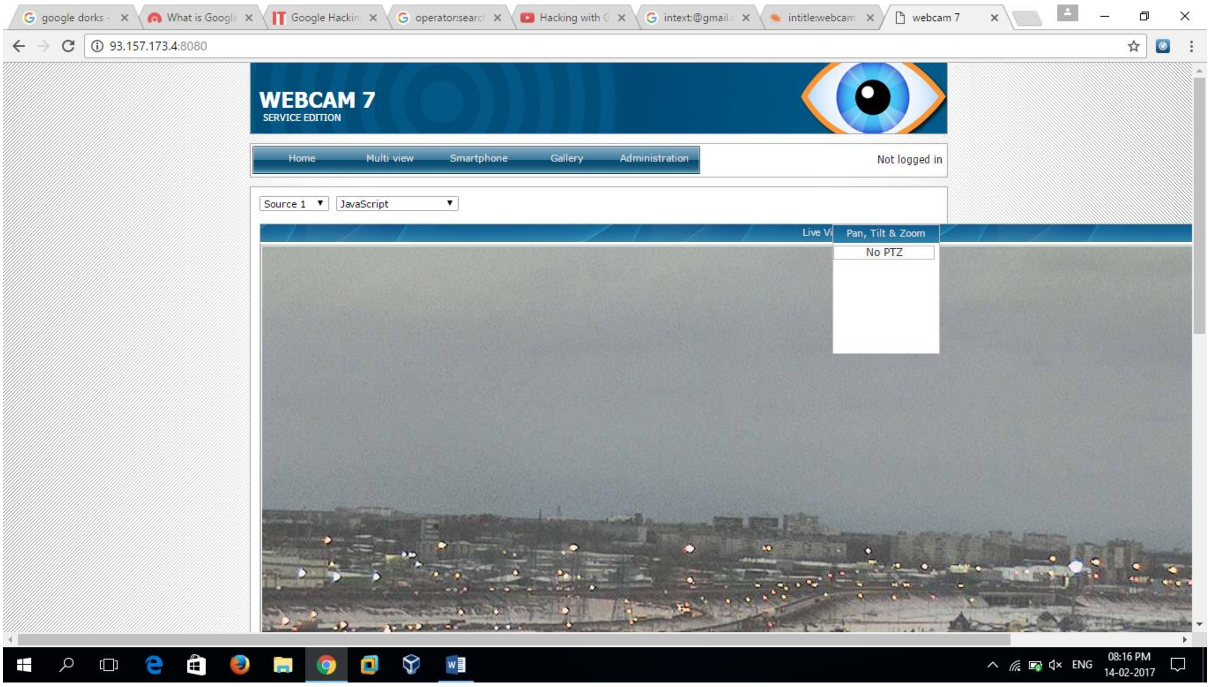
webcam 7
93.157.173.4:**8080**/
webcam 7. service edition. HomeMulti viewSmartphoneGalleryAdministration. Not logged in. Source 1, Source 2, Source 3, Source 4, Source 5, Source 6 ...

webcam 7
82.153.23.212:**8080**/
NDCC-CAM. webcams and ip cameras server for windows. HomeMulti view SmartphoneGalleryAdministration. Not logged in. Source 1, Source 2. JavaScript ...

webcam 7
81.**7**.87.107:**8080**/mobile.html
webcam 7. webcams and ip cameras server for windows. Home Not logged in. Source 1. JavaScript, Motion JPEG [Firefox], Flash JPEG Stream, Flash FLV ...

webcam 7
216.137.193.126:**8080**/
JavaScript, Motion JPEG [Firefox], Flash JPEG Stream, Flash FLV Stream. Live View. Live Stream. Pan, Tilt & Zoom. powered by webcam 7 v1.5.3.0. xhtml css.

webcam 7
minside.dyndns.org:**8080**/
webcam 7. webcams and ip cameras server for windows. HomeMulti view SmartphoneGalleryAdministration. Not logged in. Source 1, Source 2, Source 3 ...



google dorks
What is Google
Google Hackin
operator:search
Hacking with G
intext:@gmail.
intitle:webcam
webcam 7
93.157.173.4:8080
WEBCAM 7
SERVICE EDITION
Home
Multi view
Smartphone
Gallery
Administration
Not logged in
Source 1
JavaScript
Live Vi
Pan, Tilt & Zoom
No PTZ
ENG
08:16 PM
14-02-2017