OSINT Dark Arts and Privacy in CyberSpace

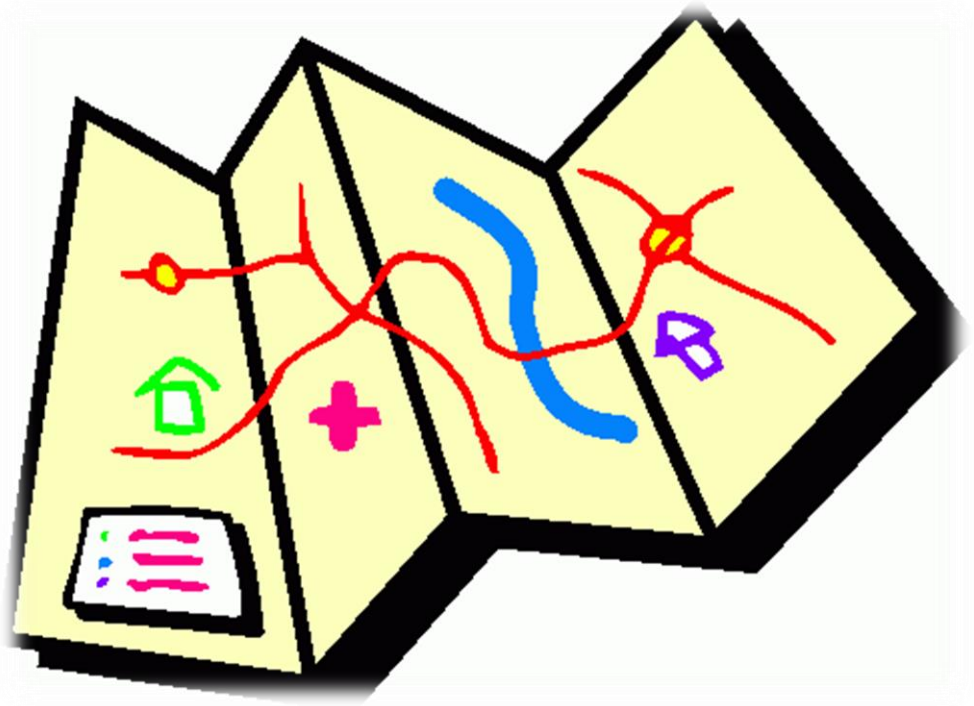
Dhanith Krishna B

“Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all information required about the enemy”

- Al Qaeda training manual

#Roadmap

- Food for thought
- OSINT
- Techniques & Tools
- Protecting yourself
- TODO



Food for Thought

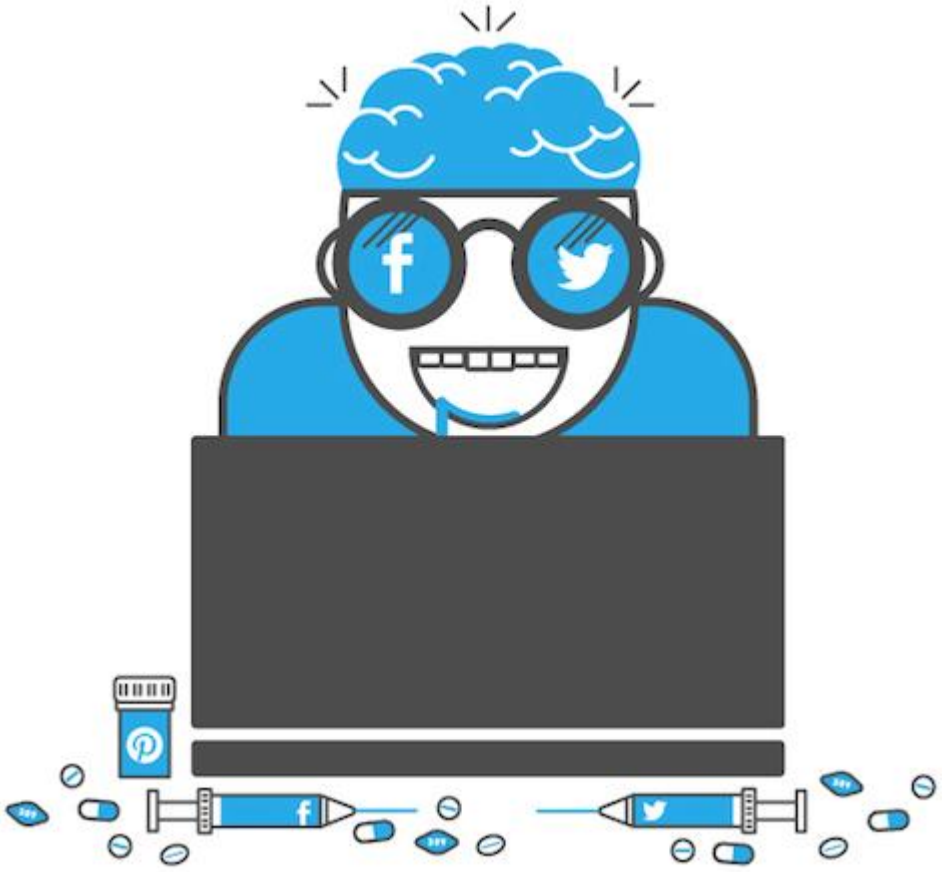
- Social Media
- Shopping
- Banking
- Learning
- Dating
- Business

ONLINE WEDDING!!!!

Doctor please tell me
boy or girl?
i want to update
status on facebook
Facebook

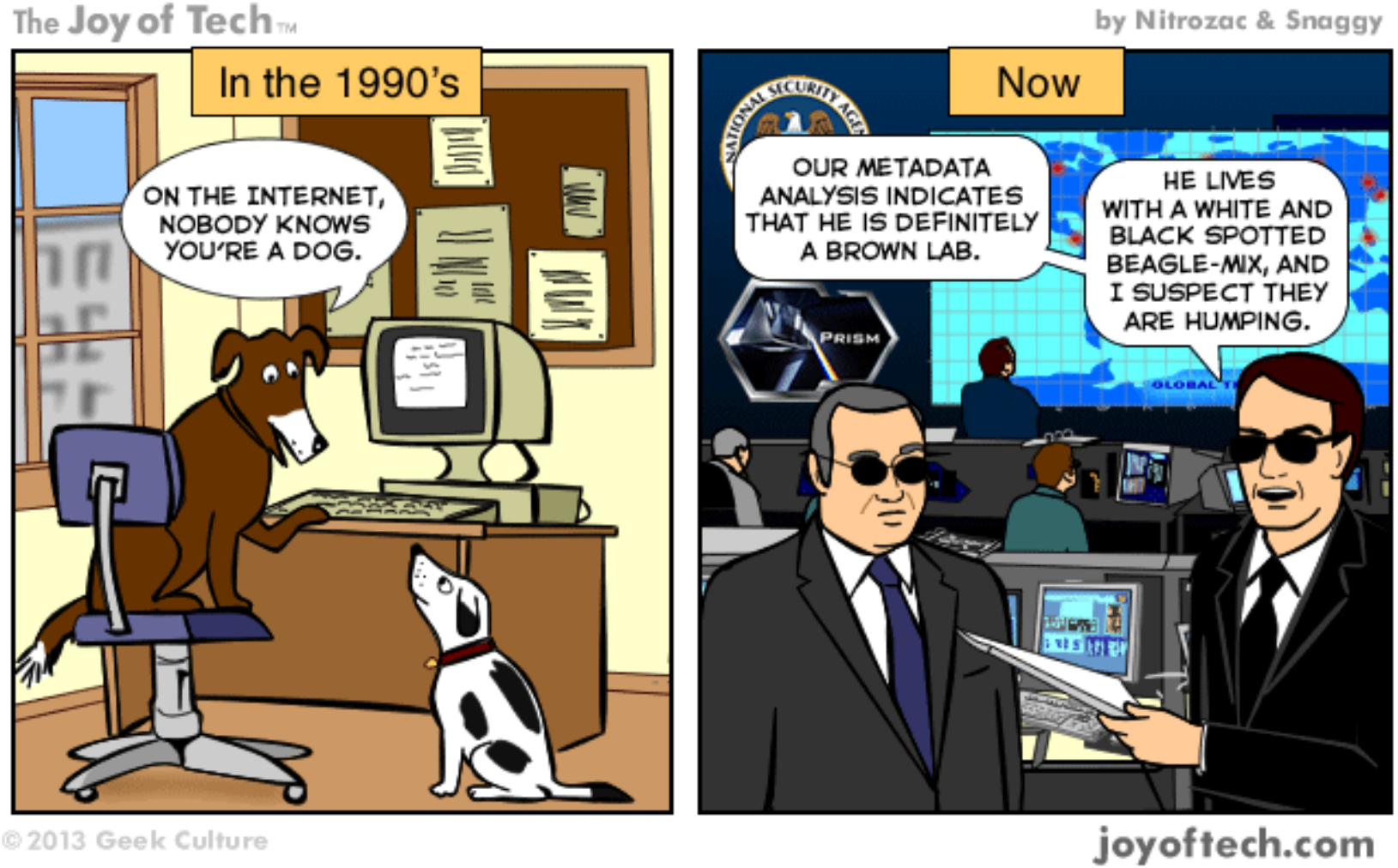
Data we intentionally give

- Text
- Picture
- Audio
- Video
- Geospatial Data
- Juicy P I I



Data collected without our knowledge

- Smart Phone
  - Contacts
  - SMS
  - Personal Information
- IOT
  - Medical Data
  - Usage Trends
  - What not?


The Joy of Tech™
by Nitrozac & Snaggy
In the 1990's
ON THE INTERNET, NOBODY KNOWS YOU'RE A DOG.
Now
OUR METADATA ANALYSIS INDICATES THAT HE IS DEFINITELY A BROWN LAB.
HE LIVES WITH A WHITE AND BLACK SPOTTED BEAGLE-MIX, AND I SUSPECT THEY ARE HUMPING.
PRISM
© 2013 Geek Culture
joyoftech.com

OSINT

OSINT is defined by both the U.S. Director of National Intelligence and the U.S. Department of Defense (DoD), as "produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."

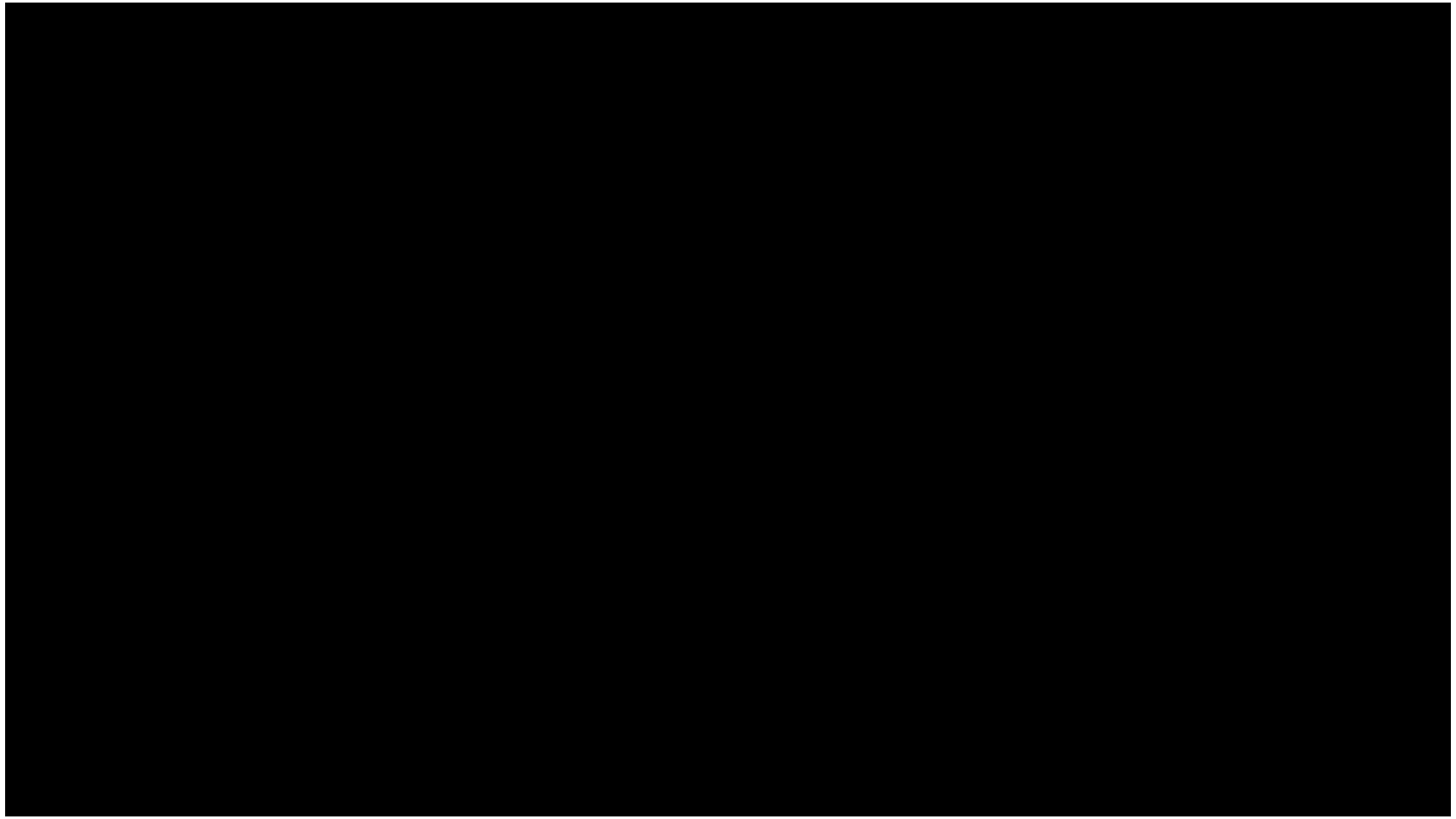
In simple words deriving actionable intelligence from public information sources.

Beneficiaries

- Governments , Militaries and Intelligence Agencies
- Big Corporations
- Market study and Analysis
- Political parties
- Information Security Consultants
- Black hats and Hacktivists
- Fraudsters

How OSINT can be used against you

- Identity Theft
- Financial Loss
- Cyber Bullying
- Fraud

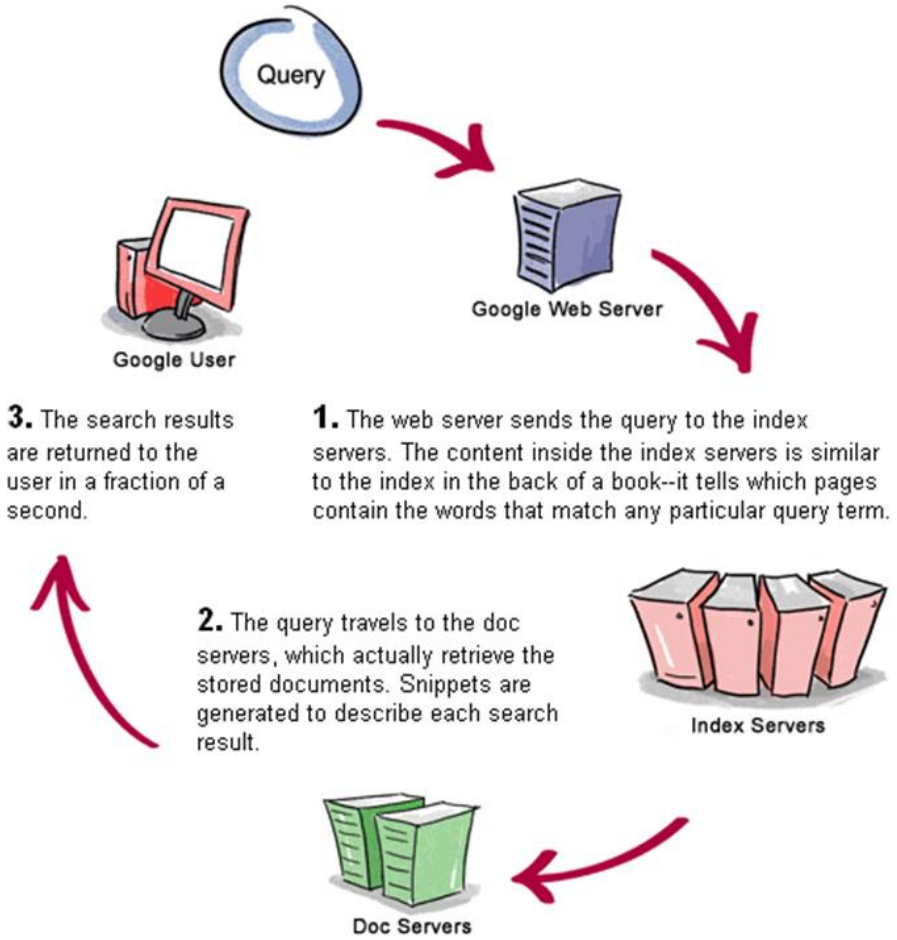


Tools & Techniques

Search Engines

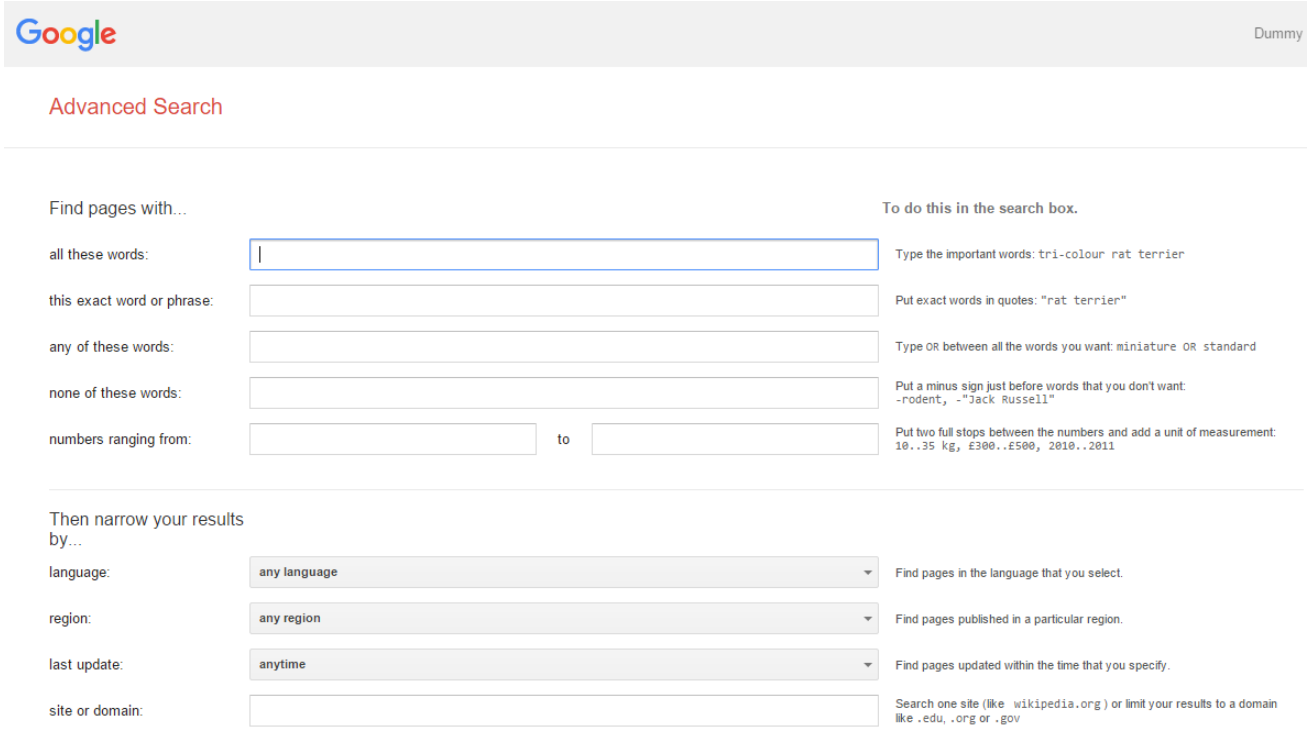
- Google
- Yahoo
- Bing
- Baidu
- Yandex
- DuckDuckGo

How google works?

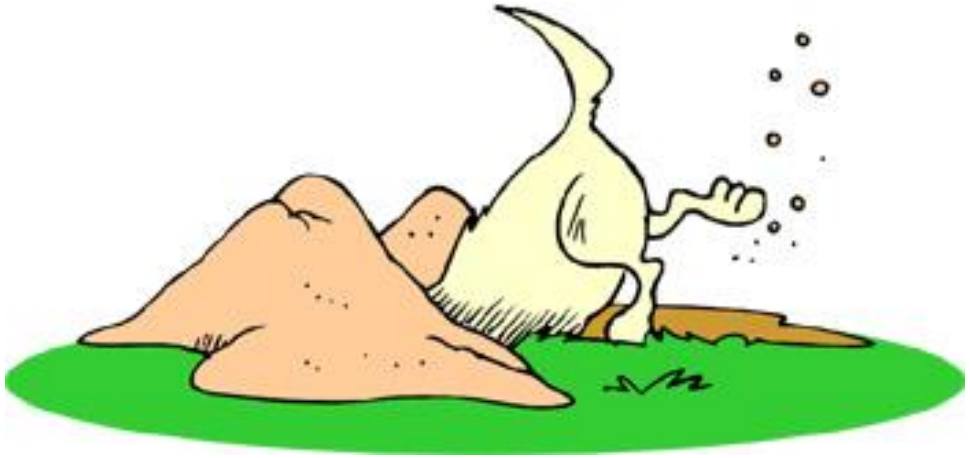


Copyright © 2003 Google Inc. Used with permission.

Google advanced search



Dorking



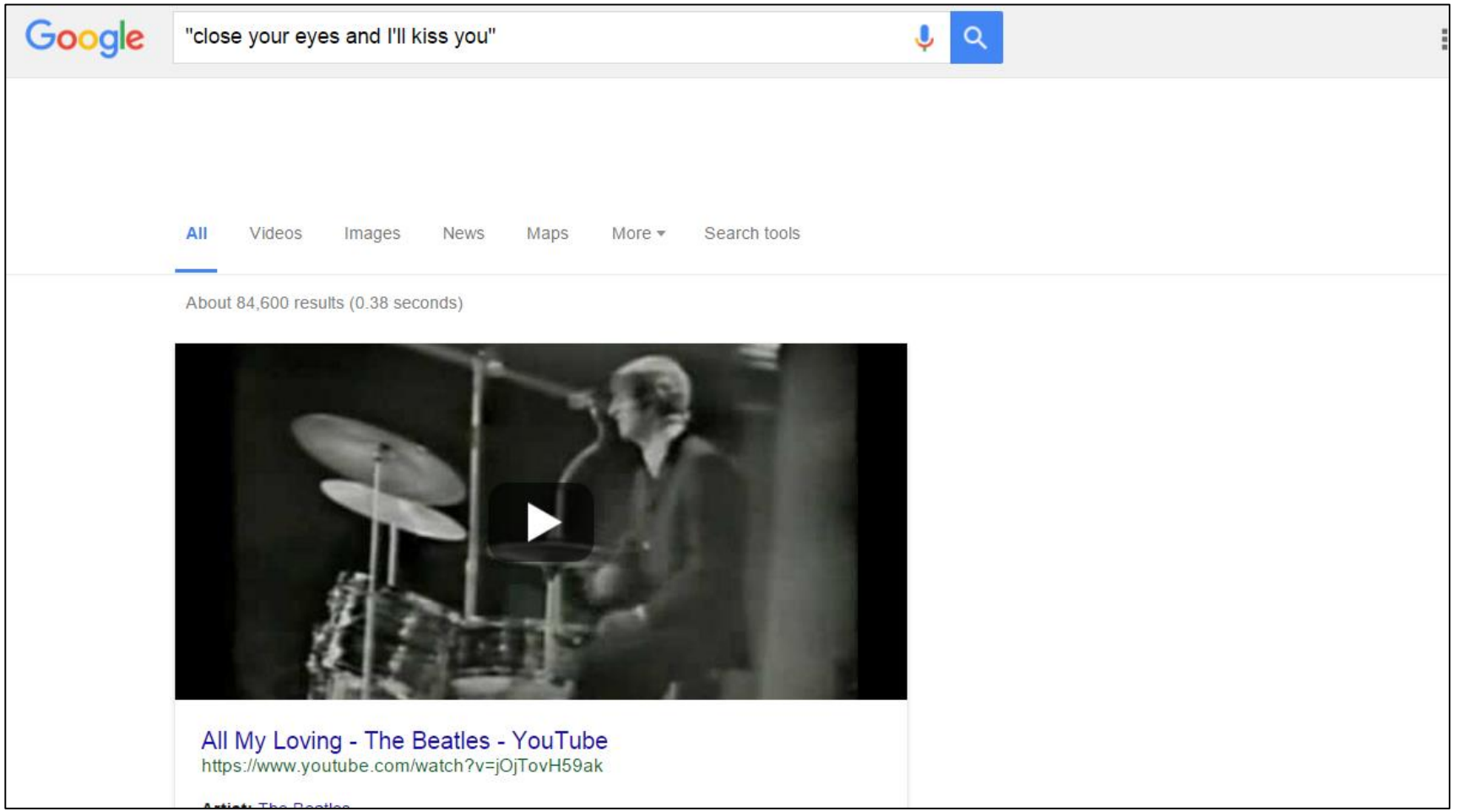
Dork is a special search string that uses advanced search operators to find information that is not readily available.

-Johnny Long
Wrote Google Hacking for Penetration Testers; ISBN 1931836361

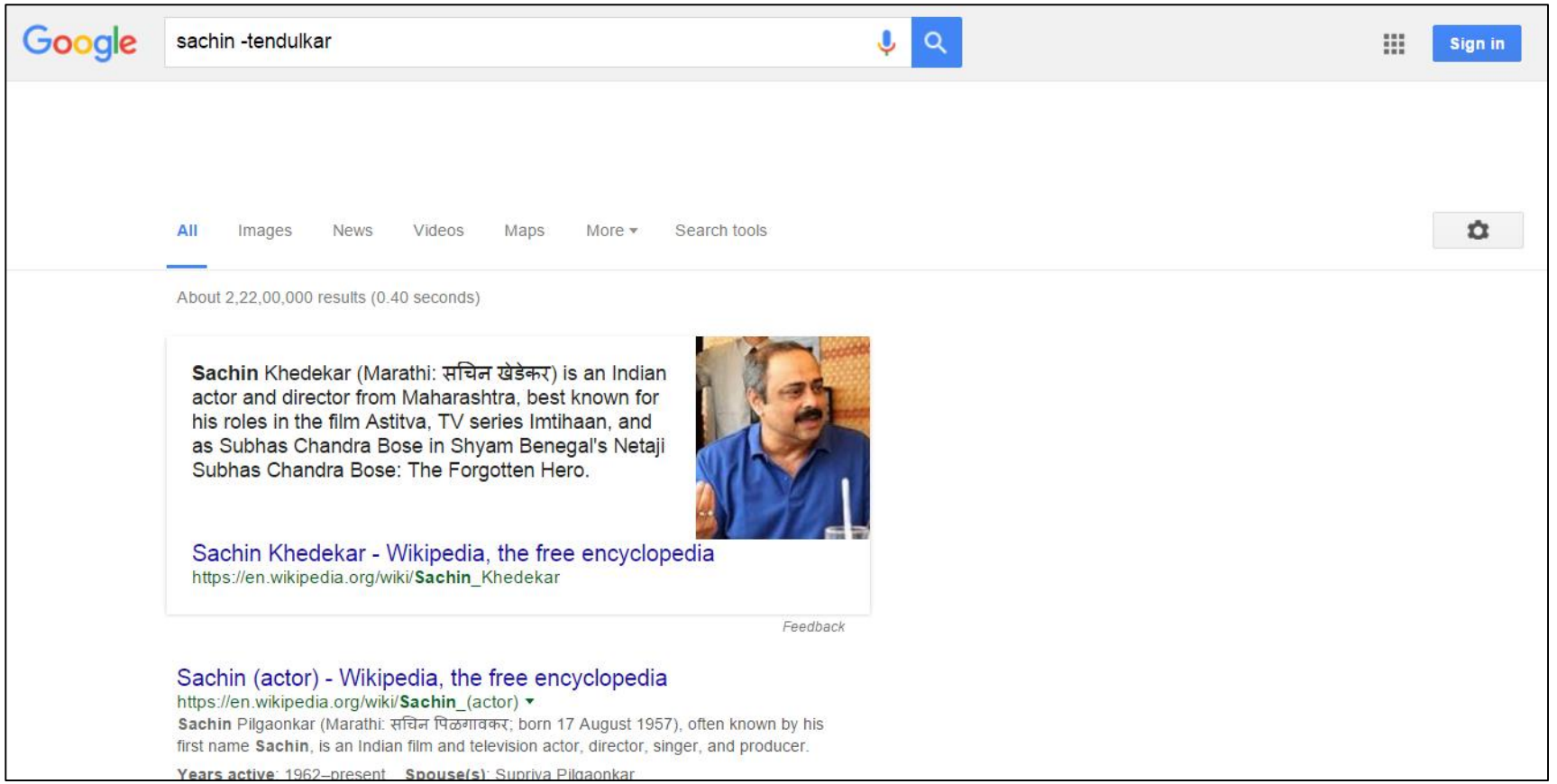
Special Characters

Operator	Description
“ ”	Must include
-	Don’t include
~	Synonym
|	Pizza or burger
..	Range
*	Multi character wildcard

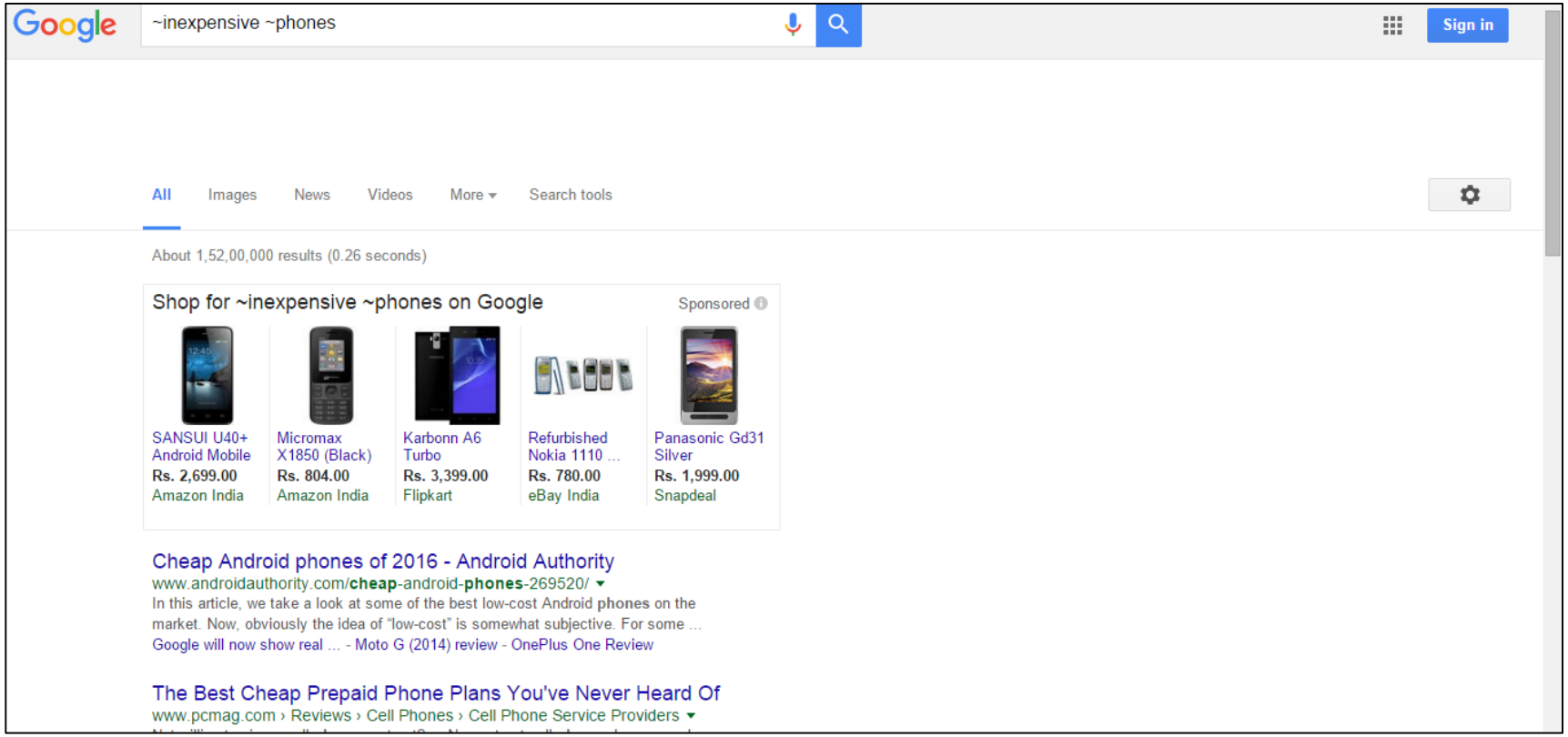
“ ” operator


Google
"close your eyes and I'll kiss you"
All
Videos
Images
News
Maps
More
Search tools
About 84,600 results (0.38 seconds)
All My Loving - The Beatles - YouTube
https://www.youtube.com/watch?v=jOjTovH59ak

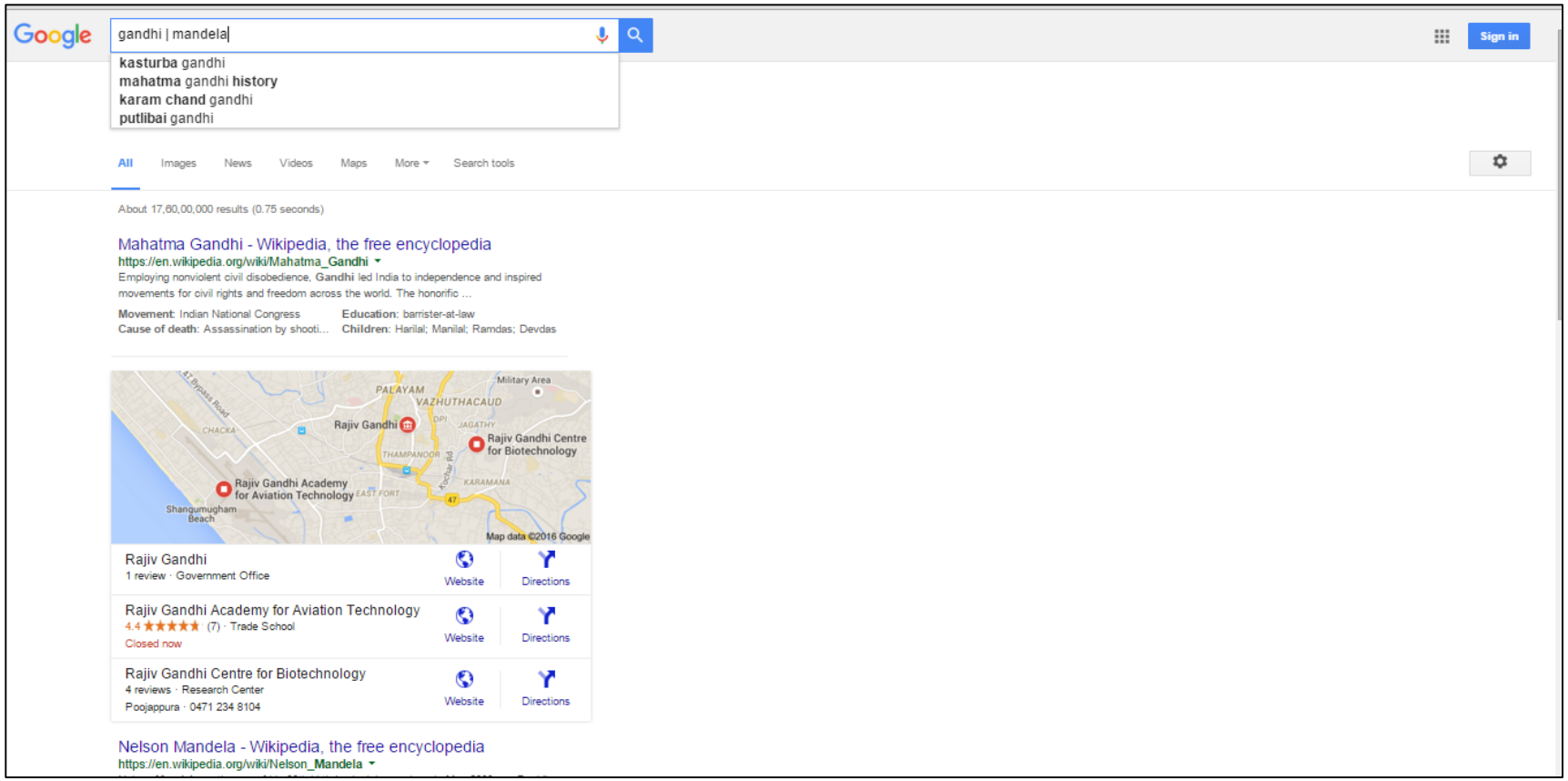
- operator


Google
sachin -tendulkar
Sign in
All
Images
News
Videos
Maps
More
Search tools
About 2,22,00,000 results (0.40 seconds)
Sachin Khedekar (Marathi: सचिन खेडेकर) is an Indian actor and director from Maharashtra, best known for his roles in the film Astitva, TV series Imtihaan, and as Subhas Chandra Bose in Shyam Benegal's Netaji Subhas Chandra Bose: The Forgotten Hero.
Sachin Khedekar - Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/Sachin_Khedekar
Feedback
Sachin (actor) - Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/Sachin_(actor)
Sachin Pilgaonkar (Marathi: सचिन पिळगावकर; born 17 August 1957), often known by his first name Sachin, is an Indian film and television actor, director, singer, and producer.
Years active: 1962–present Spouse(s): Supriya Pilgaonkar

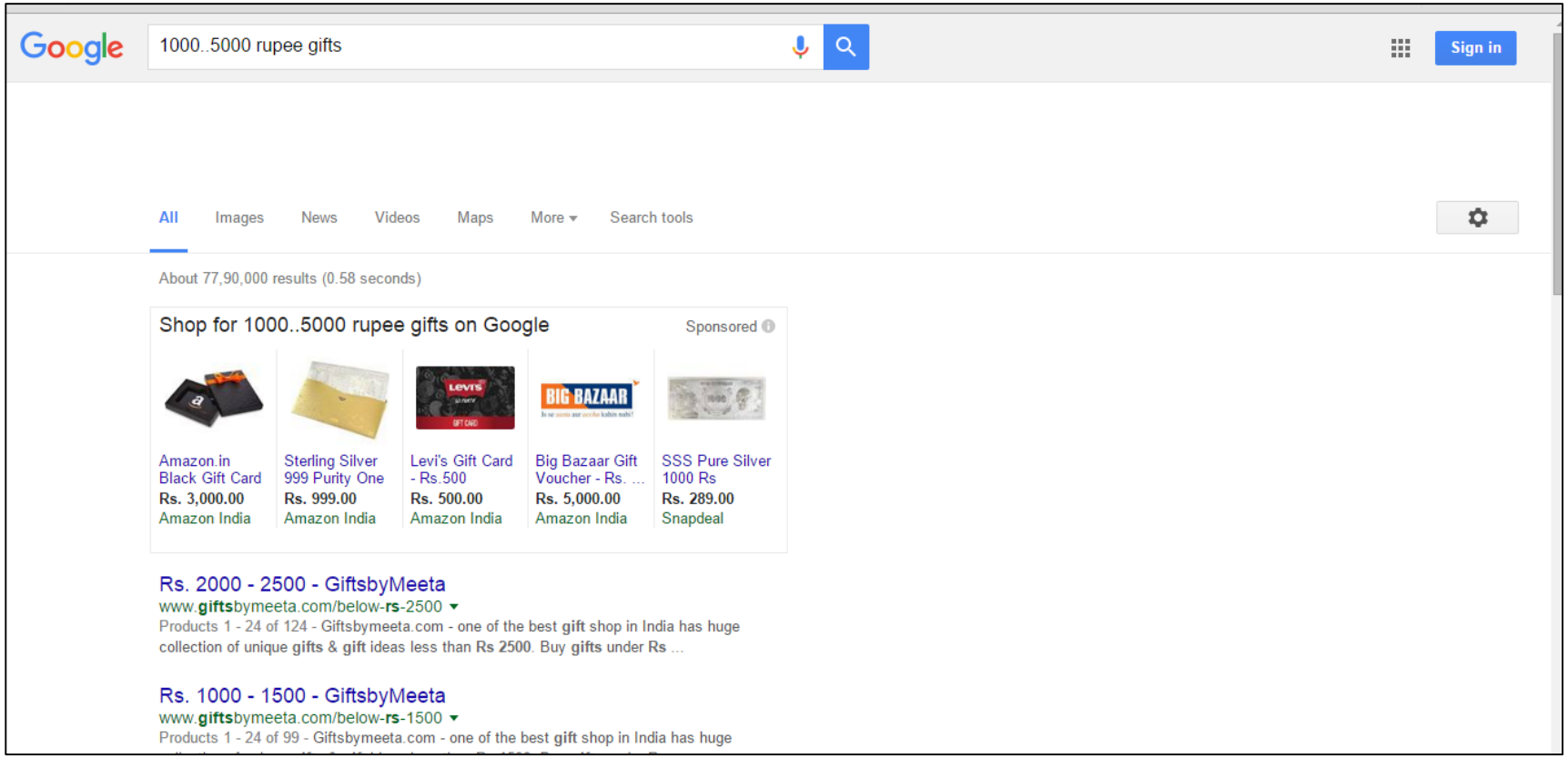
~ operator


Google
~inexpensive ~phones
Sign in
All
Images
News
Videos
More
Search tools
About 1,52,00,000 results (0.26 seconds)
Shop for ~inexpensive ~phones on Google
Sponsored
SANSUI U40+ Android Mobile
Rs. 2,699.00
Amazon India
Micromax X1850 (Black)
Rs. 804.00
Amazon India
Karbonn A6 Turbo
Rs. 3,399.00
Flipkart
Refurbished Nokia 1110 ...
Rs. 780.00
eBay India
Panasonic Gd31 Silver
Rs. 1,999.00
Snapdeal
Cheap Android phones of 2016 - Android Authority
www.androidauthority.com/cheap-android-phones-269520/
In this article, we take a look at some of the best low-cost Android phones on the market. Now, obviously the idea of "low-cost" is somewhat subjective. For some ...
Google will now show real ... - Moto G (2014) review - OnePlus One Review
The Best Cheap Prepaid Phone Plans You've Never Heard Of
www.pcmag.com › Reviews › Cell Phones › Cell Phone Service Providers

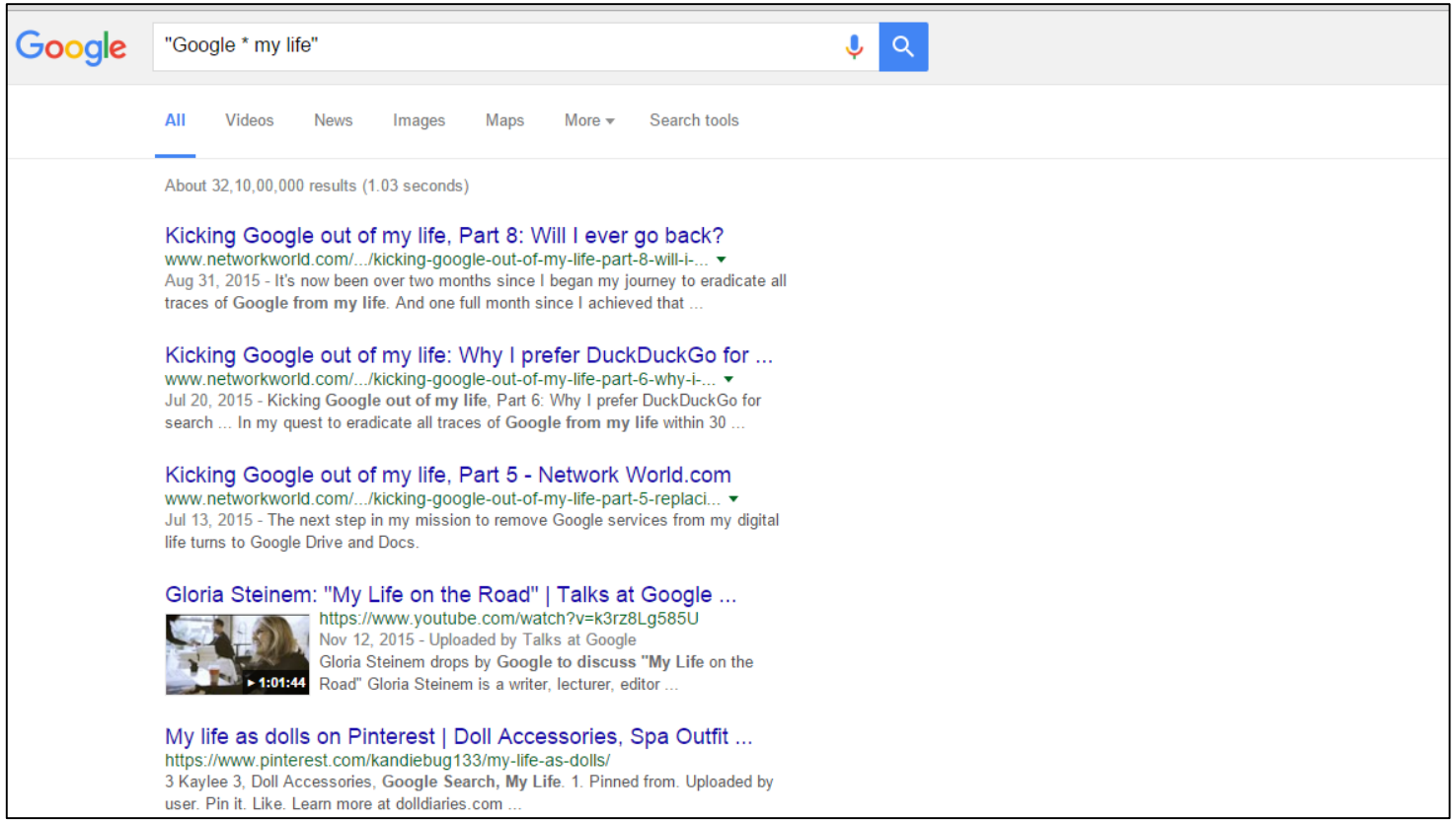
| operator


Google
gandhi | mandela
kasturba gandhi
mahatma gandhi history
karam chand gandhi
putlibai gandhi
Sign in
All
Images
News
Videos
Maps
More
Search tools
About 17,60,00,000 results (0.75 seconds)
Mahatma Gandhi - Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/Mahatma_Gandhi
Employing nonviolent civil disobedience, Gandhi led India to independence and inspired movements for civil rights and freedom across the world. The honorific ...
Movement: Indian National Congress
Education: barrister-at-law
Cause of death: Assassination by shooti...
Children: Harilal; Manilal; Ramdas; Devdas
PALAYAM
VAZHUTHACAUD
Military Area
Rajiv Gandhi
Rajiv Gandhi Centre for Biotechnology
Rajiv Gandhi Academy for Aviation Technology
Shanumugham Beach
Map data ©2016 Google
Rajiv Gandhi
1 review · Government Office
Website
Directions
Rajiv Gandhi Academy for Aviation Technology
4.4 (7) · Trade School
Closed now
Website
Directions
Rajiv Gandhi Centre for Biotechnology
4 reviews · Research Center
Poojappura · 0471 234 8104
Website
Directions
Nelson Mandela - Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/Nelson_Mandela

.. operator


Google
1000..5000 rupee gifts
Sign in
All
Images
News
Videos
Maps
More
Search tools
About 77,90,000 results (0.58 seconds)
Shop for 1000..5000 rupee gifts on Google
Sponsored
Amazon.in Black Gift Card
Rs. 3,000.00
Amazon India
Sterling Silver 999 Purity One
Rs. 999.00
Amazon India
Levi's Gift Card - Rs.500
Rs. 500.00
Amazon India
Big Bazaar Gift Voucher - Rs. ...
Rs. 5,000.00
Amazon India
SSS Pure Silver 1000 Rs
Rs. 289.00
Snapdeal
Rs. 2000 - 2500 - GiftsbyMeeta
www.giftsbymeeta.com/below-rs-2500
Products 1 - 24 of 124 - Giftsbymeeta.com - one of the best gift shop in India has huge collection of unique gifts & gift ideas less than Rs 2500. Buy gifts under Rs ...
Rs. 1000 - 1500 - GiftsbyMeeta
www.giftsbymeeta.com/below-rs-1500
Products 1 - 24 of 99 - Giftsbymeeta.com - one of the best gift shop in India has huge

* operator


Google
"Google * my life"
All
Videos
News
Images
Maps
More
Search tools
About 32,10,00,000 results (1.03 seconds)
Kicking Google out of my life, Part 8: Will I ever go back?
www.networkworld.com/.../kicking-google-out-of-my-life-part-8-will-i-...
Aug 31, 2015 - It's now been over two months since I began my journey to eradicate all traces of Google from my life. And one full month since I achieved that ...
Kicking Google out of my life: Why I prefer DuckDuckGo for ...
www.networkworld.com/.../kicking-google-out-of-my-life-part-6-why-i-...
Jul 20, 2015 - Kicking Google out of my life, Part 6: Why I prefer DuckDuckGo for search ... In my quest to eradicate all traces of Google from my life within 30 ...
Kicking Google out of my life, Part 5 - Network World.com
www.networkworld.com/.../kicking-google-out-of-my-life-part-5-replaci...
Jul 13, 2015 - The next step in my mission to remove Google services from my digital life turns to Google Drive and Docs.
Gloria Steinem: "My Life on the Road" | Talks at Google ...
1:01:44
https://www.youtube.com/watch?v=k3rz8Lg585U
Nov 12, 2015 - Uploaded by Talks at Google
Gloria Steinem drops by Google to discuss "My Life on the Road" Gloria Steinem is a writer, lecturer, editor ...
My life as dolls on Pinterest | Doll Accessories, Spa Outfit ...
https://www.pinterest.com/kandiebug133/my-life-as-dolls/
3 Kaylee 3, Doll Accessories, Google Search, My Life. 1. Pinned from. Uploaded by user. Pin it. Like. Learn more at dolldiaries.com ...

More Special Characters

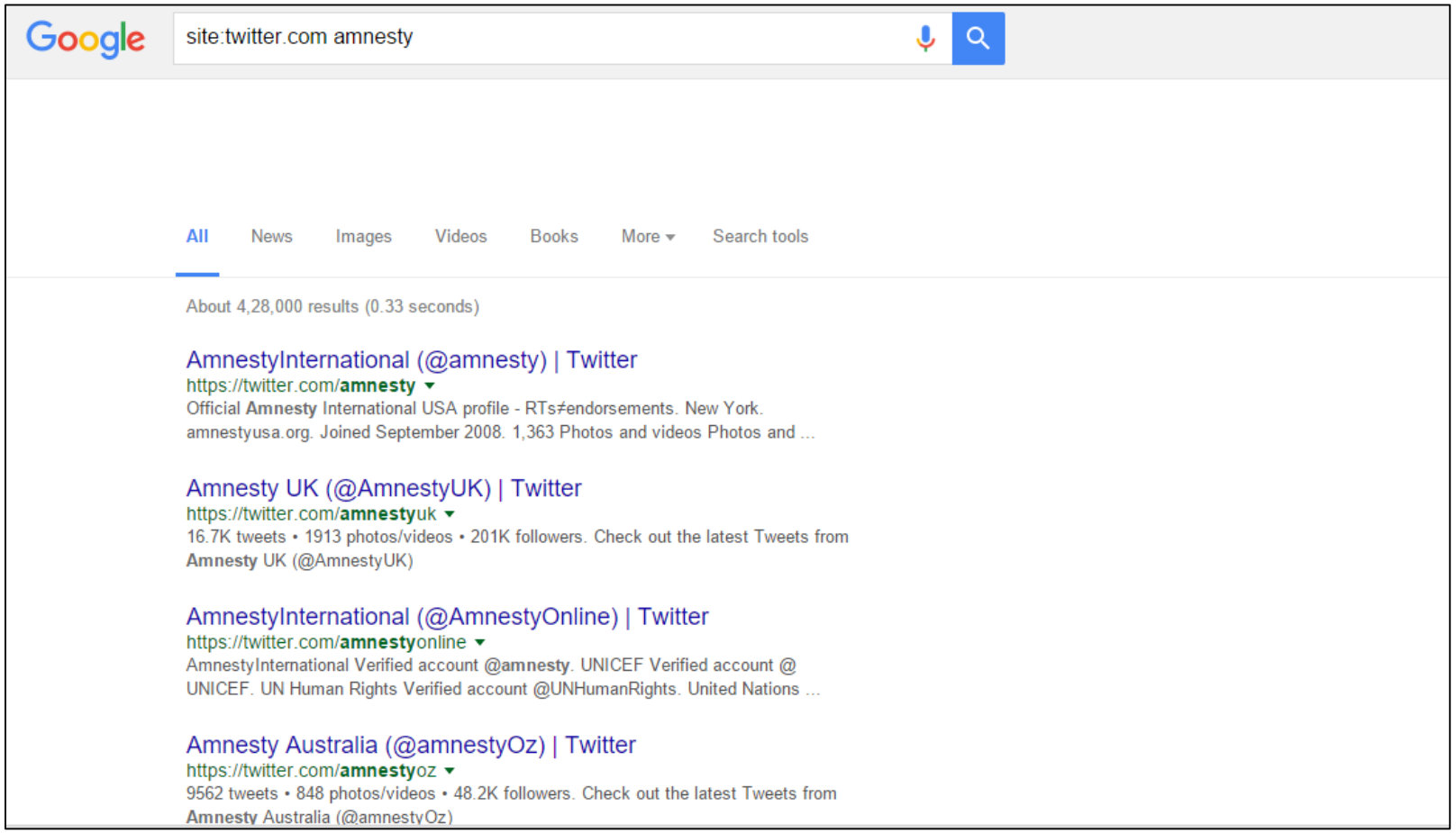
Operator	Description
@	Twitter accounts
$	price
#	Hash tags

Special Operators

Operator
Inurl:
Intext:
Intitle:
Filetype:
Site:
Related:
Link:
Movie:
Cache:

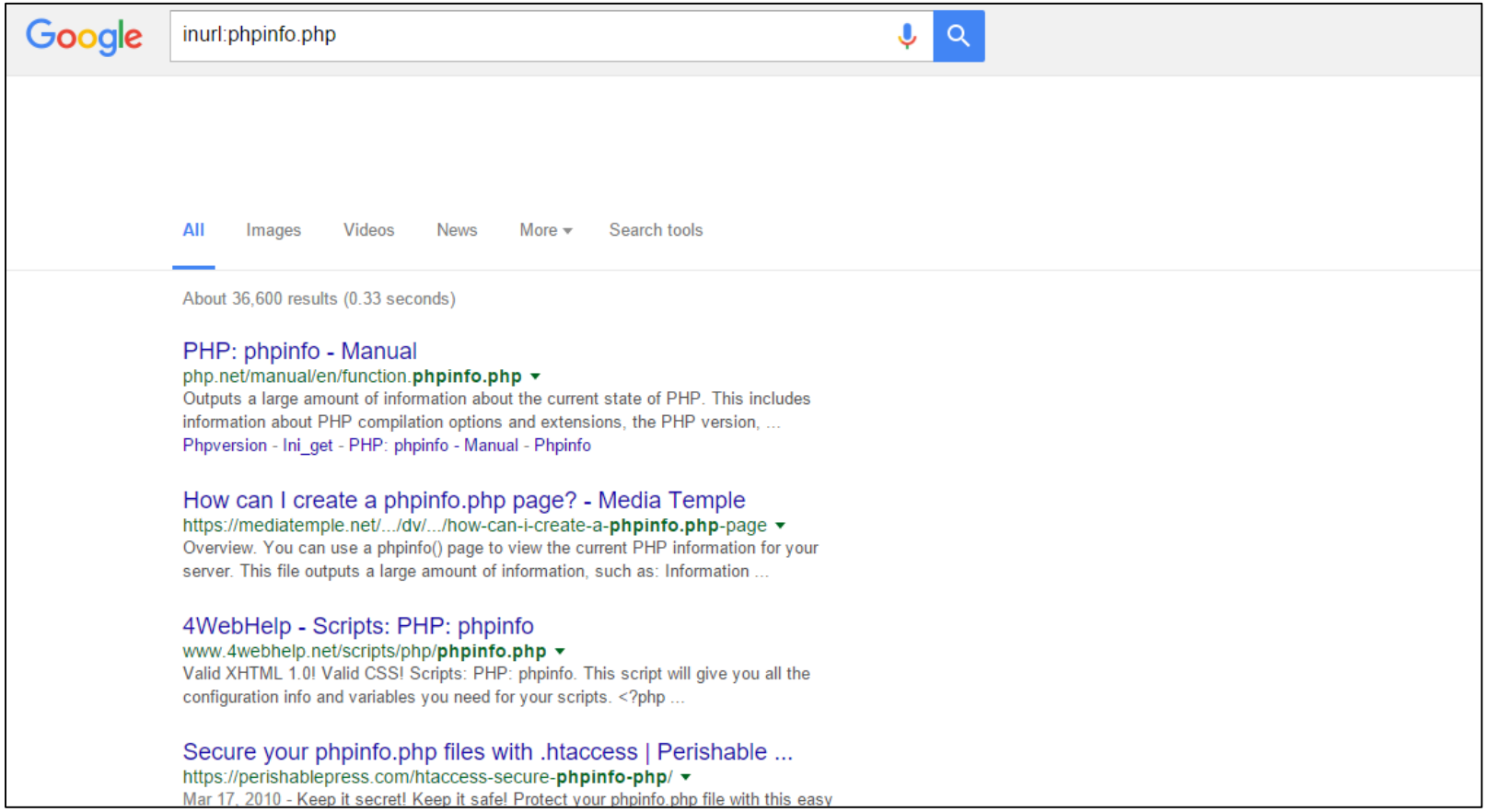
Site: Operator

For filtering result to a particular domain.



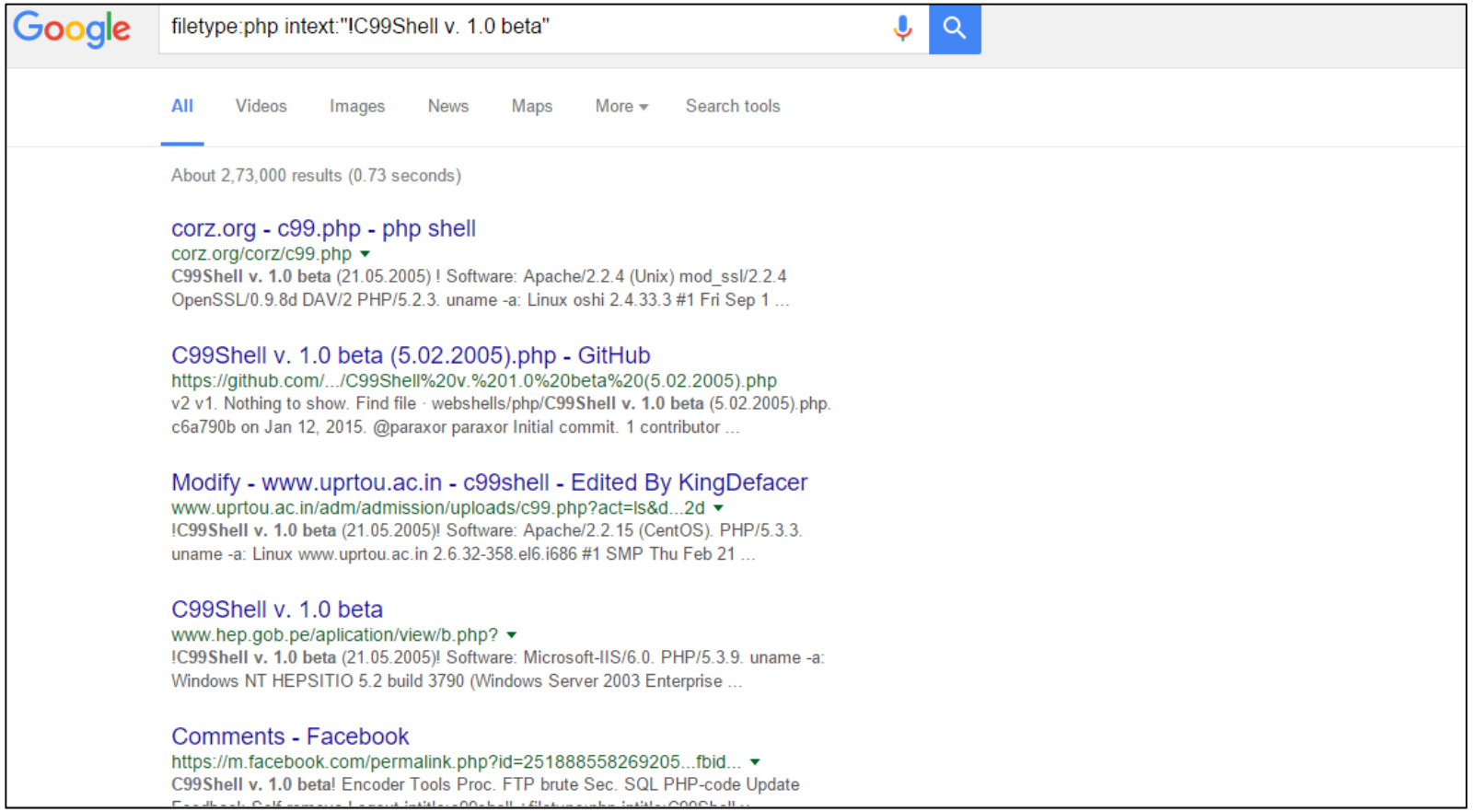
inurl: Operator

For filtering result to matching URL.



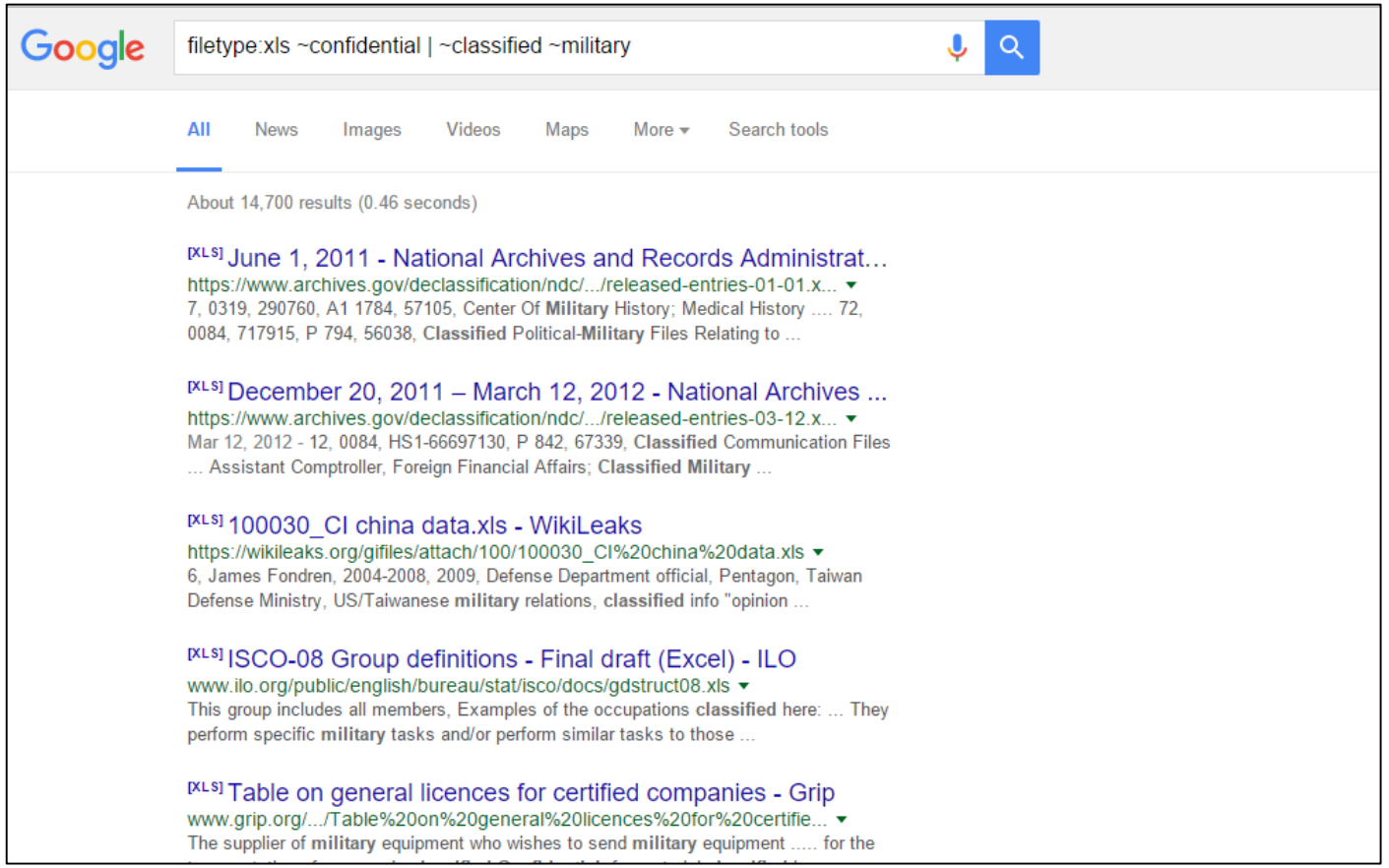
intext: Operator

For filtering result to matching content.



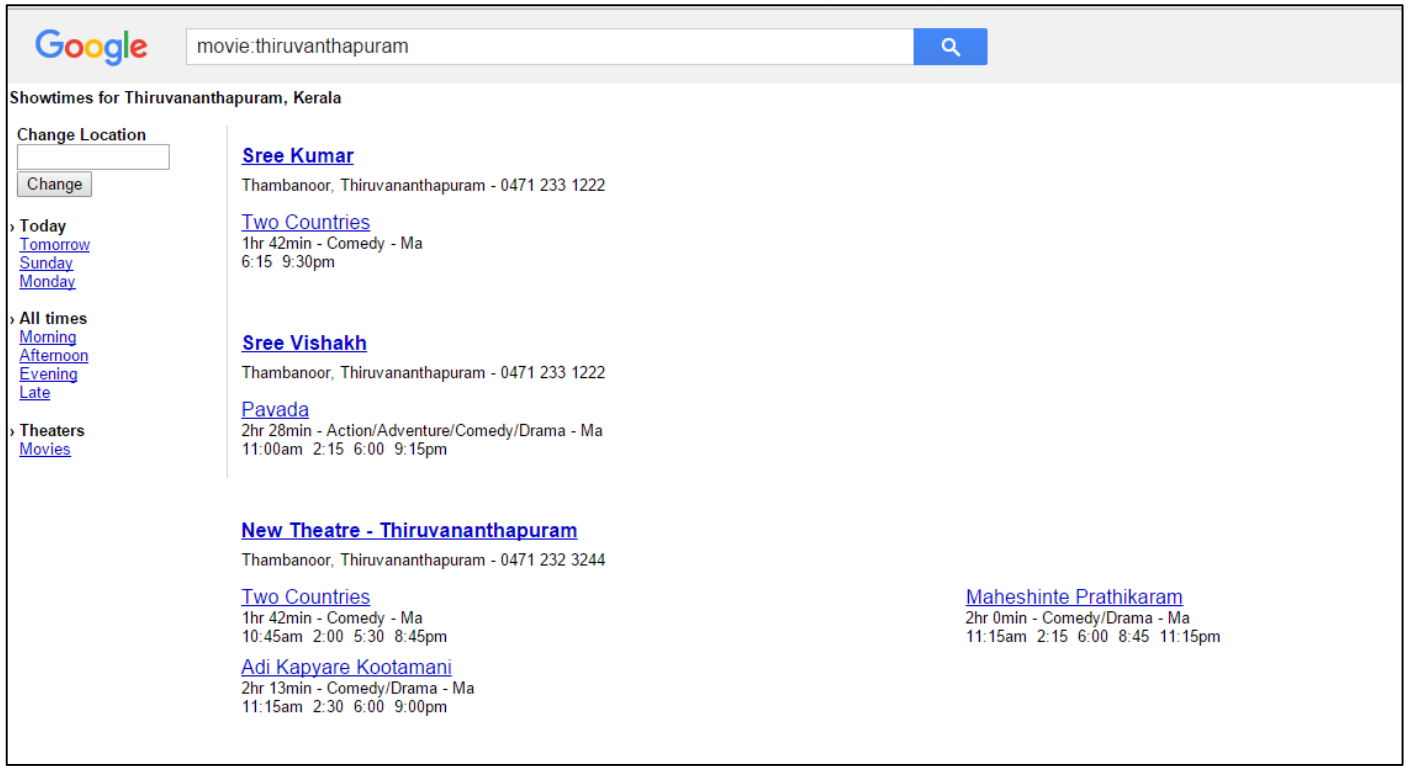
Filetype: Operator

For filtering result to matching filetype.



Movie: Operator

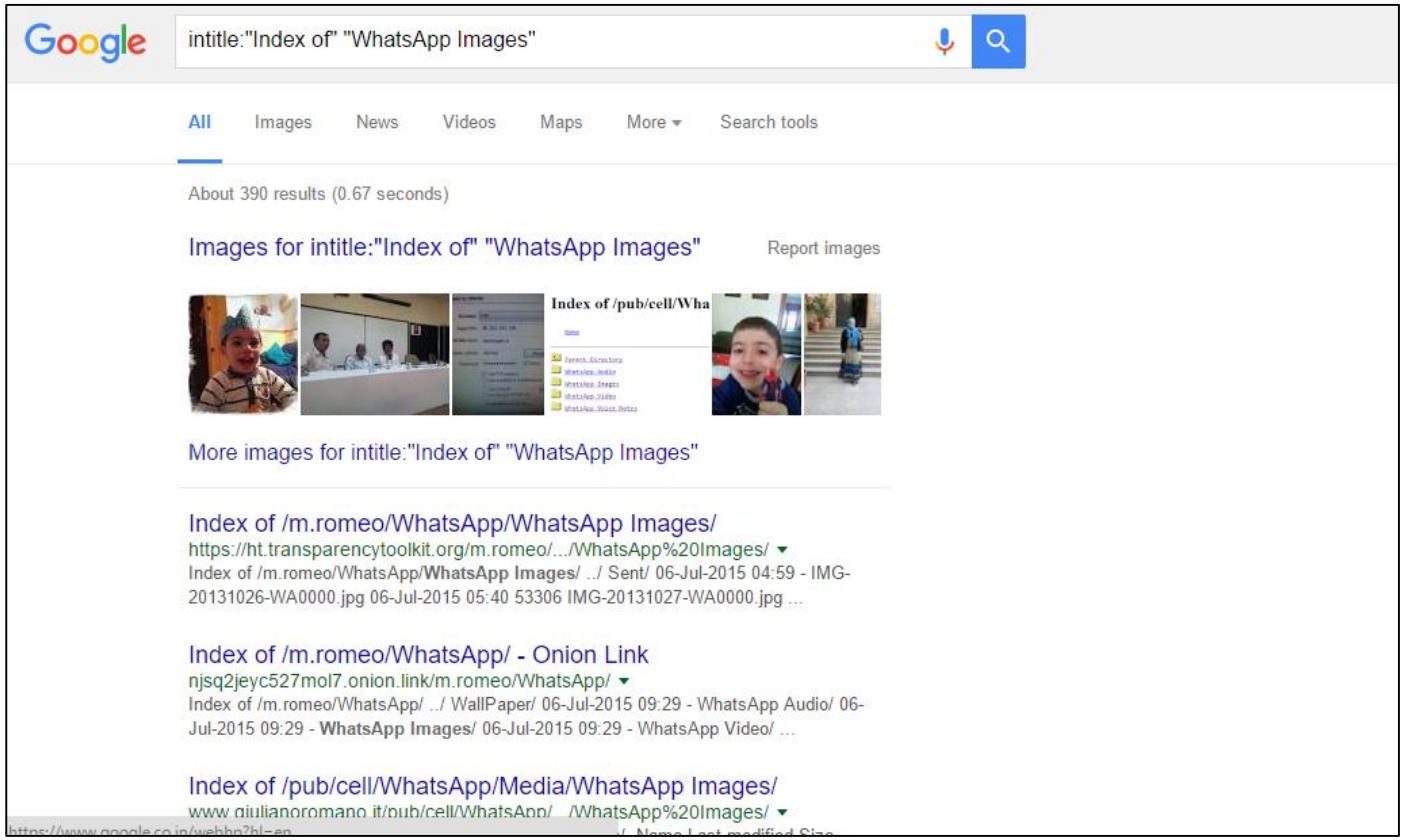
Search for movies in a location



Are you serious??

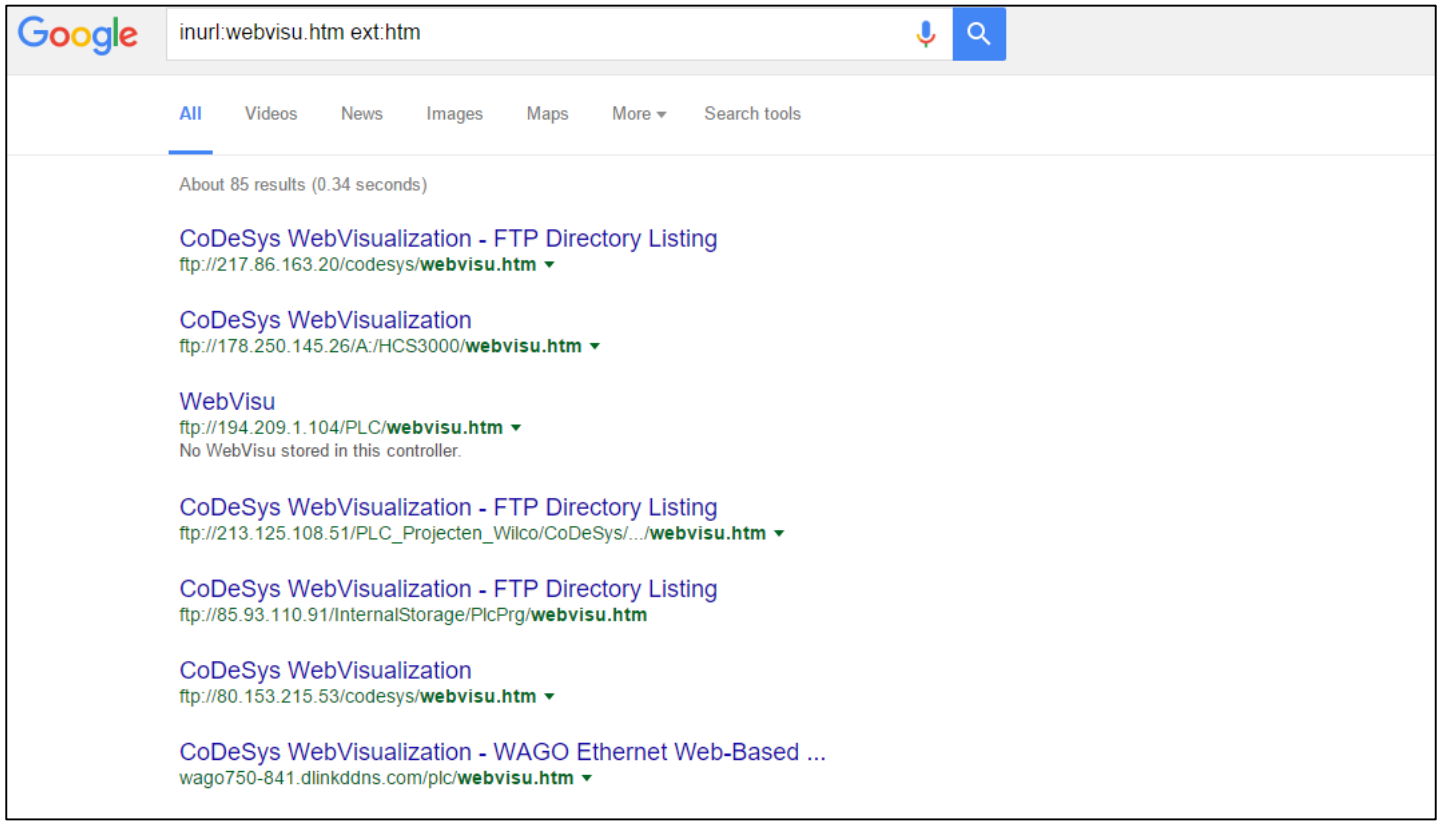
Whatsapp Images

intitle:"Index of" "WhatsApp Images"



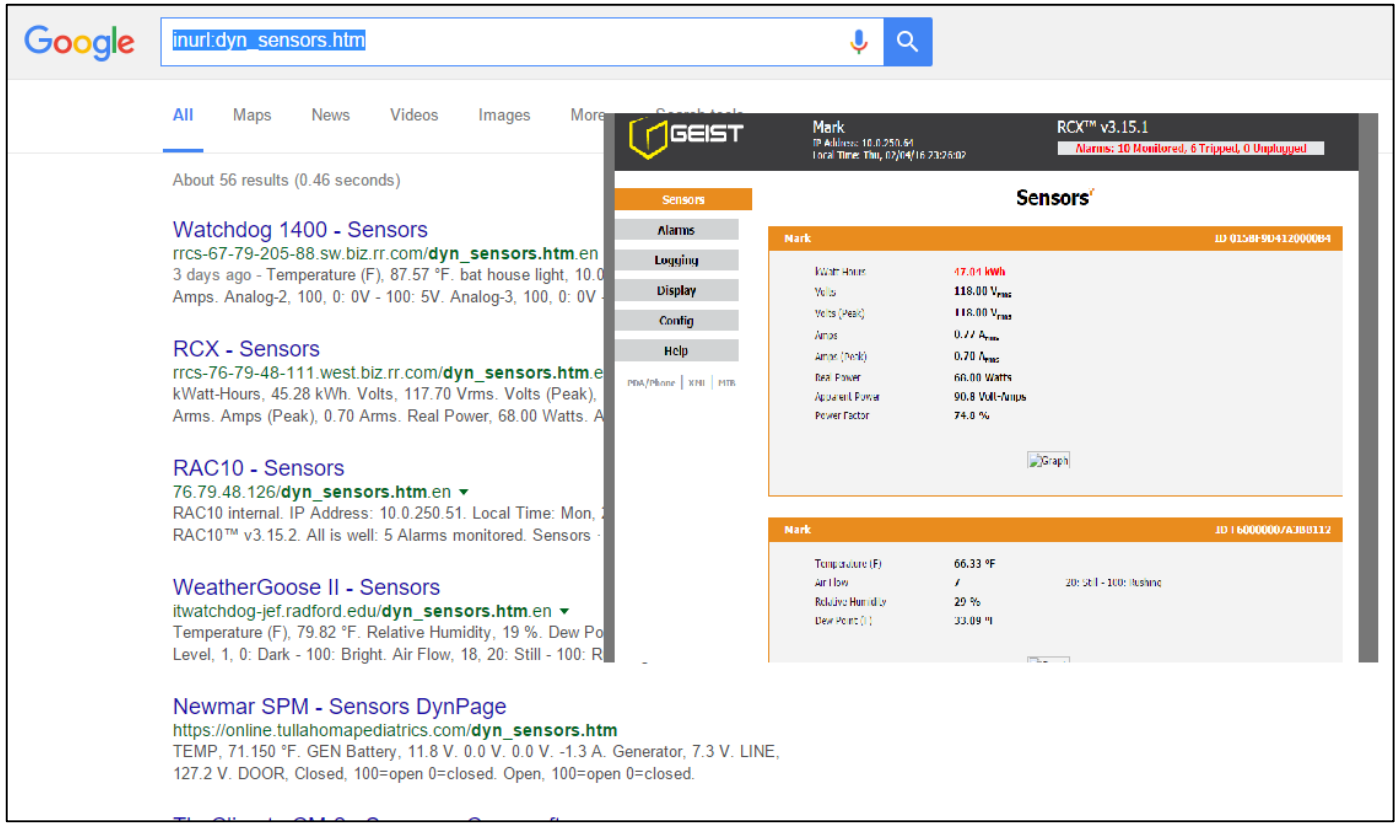
SCADA!!

inurl:webvisu.htm ext:htm



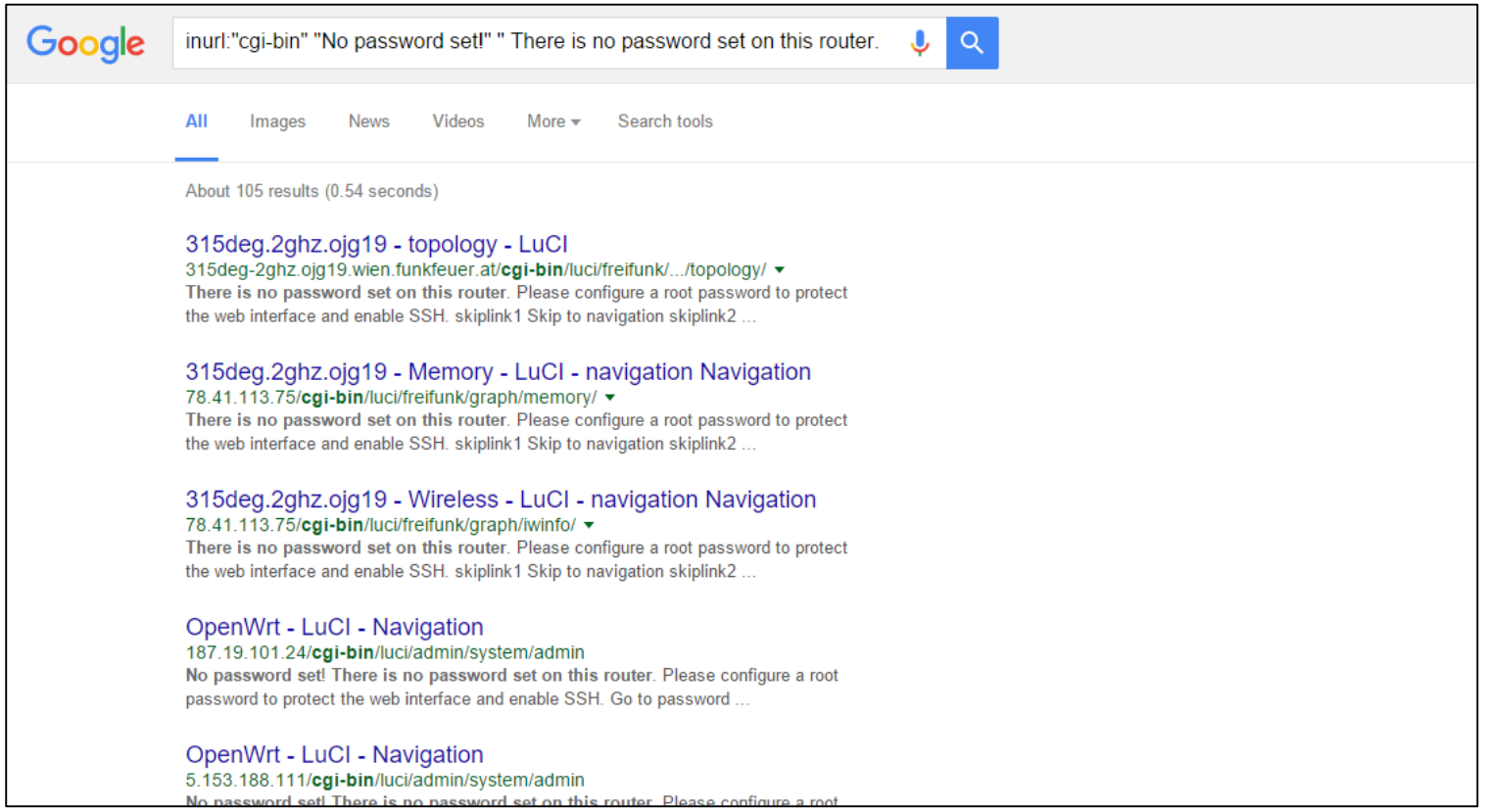
SCADA!!

inurl:dyn_sensors.htm



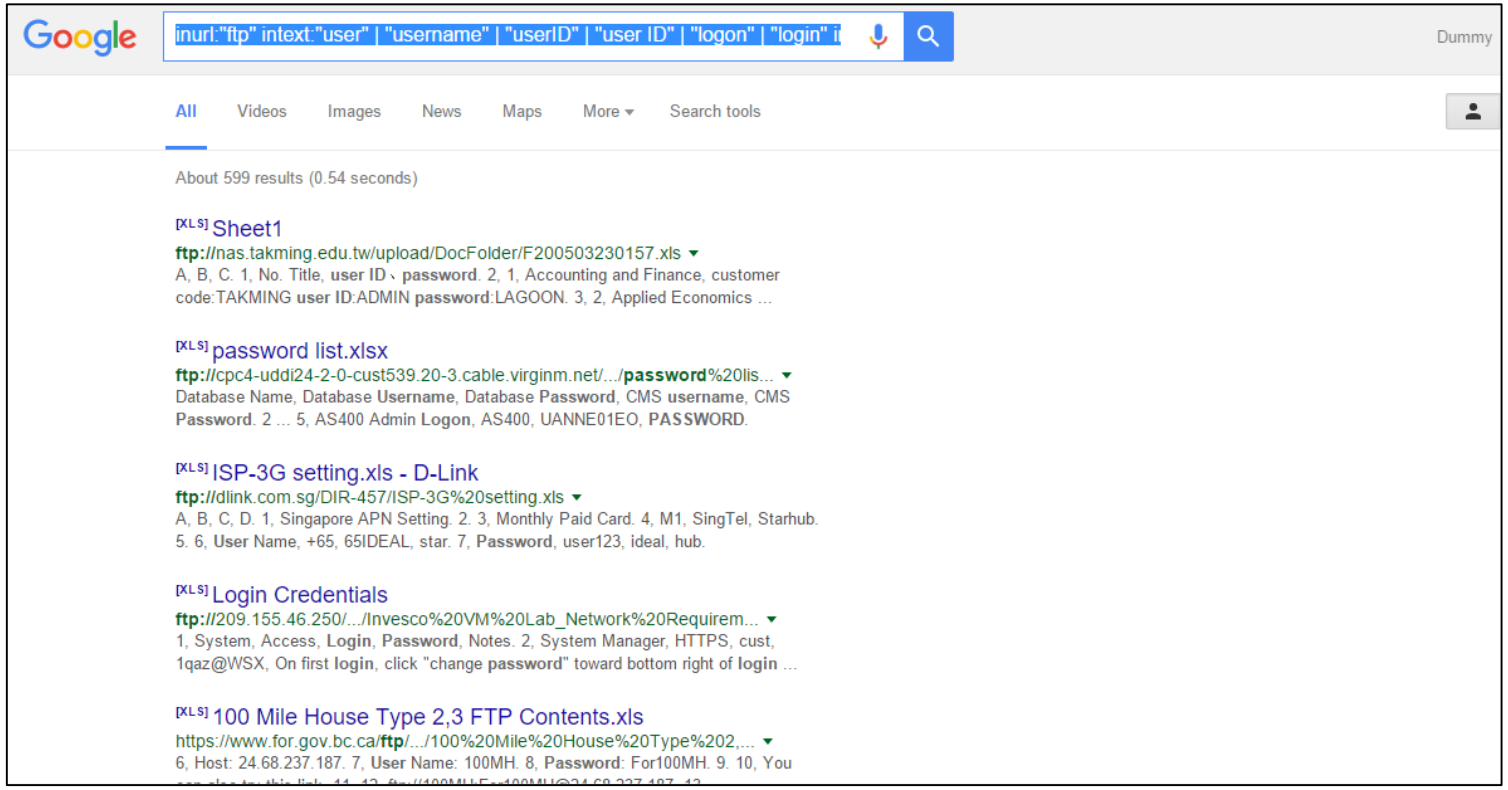
Password Less Router!!

inurl:"cgi-bin" "No password set!" " There is no password set on this router."



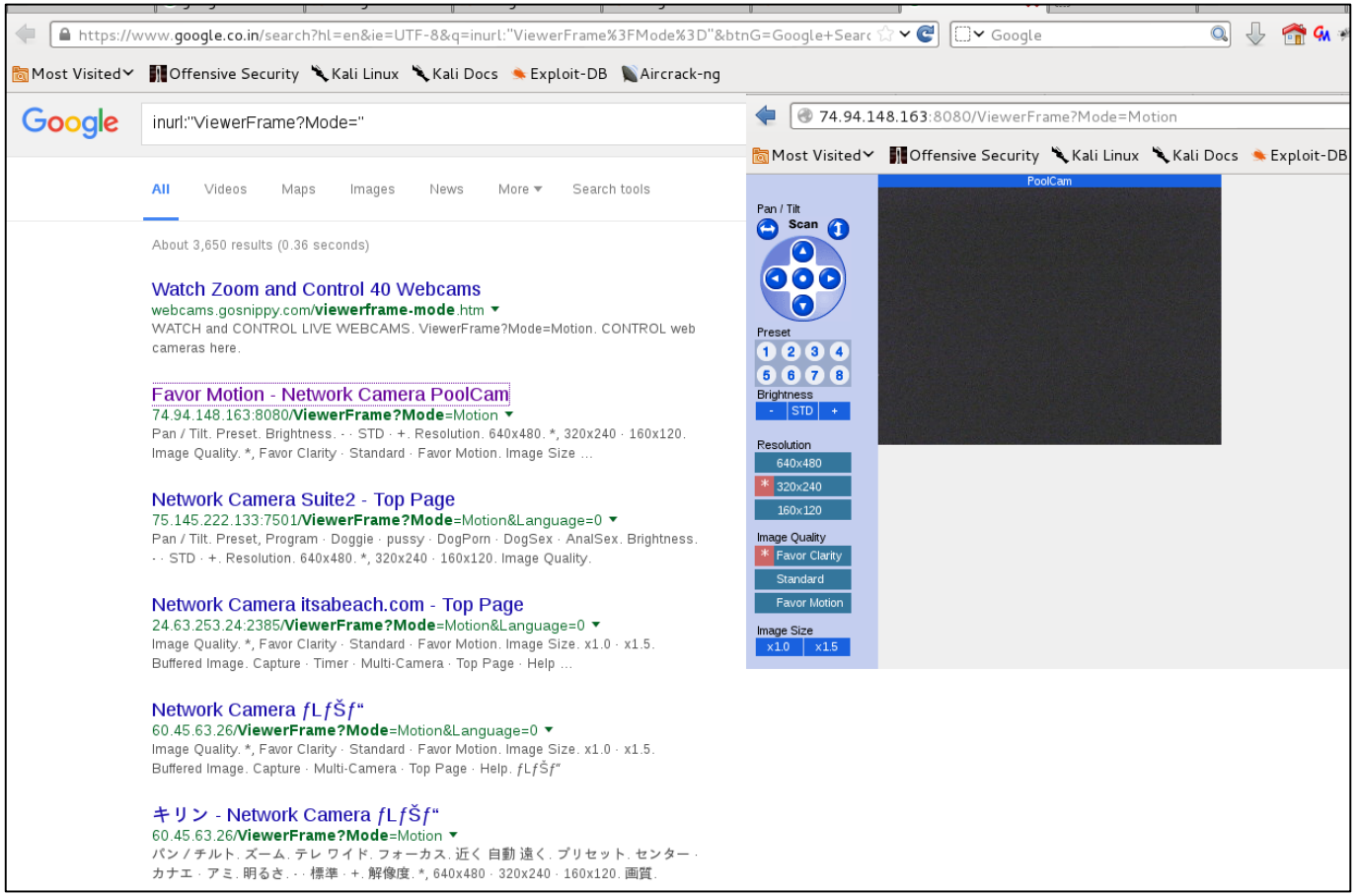
Passwords

inurl:"ftp" intext:"user" | "username" | "userID" | "user ID" | "logon" | "login" intext:"password" | "passcode" filetype:xls | filetype:xlsx



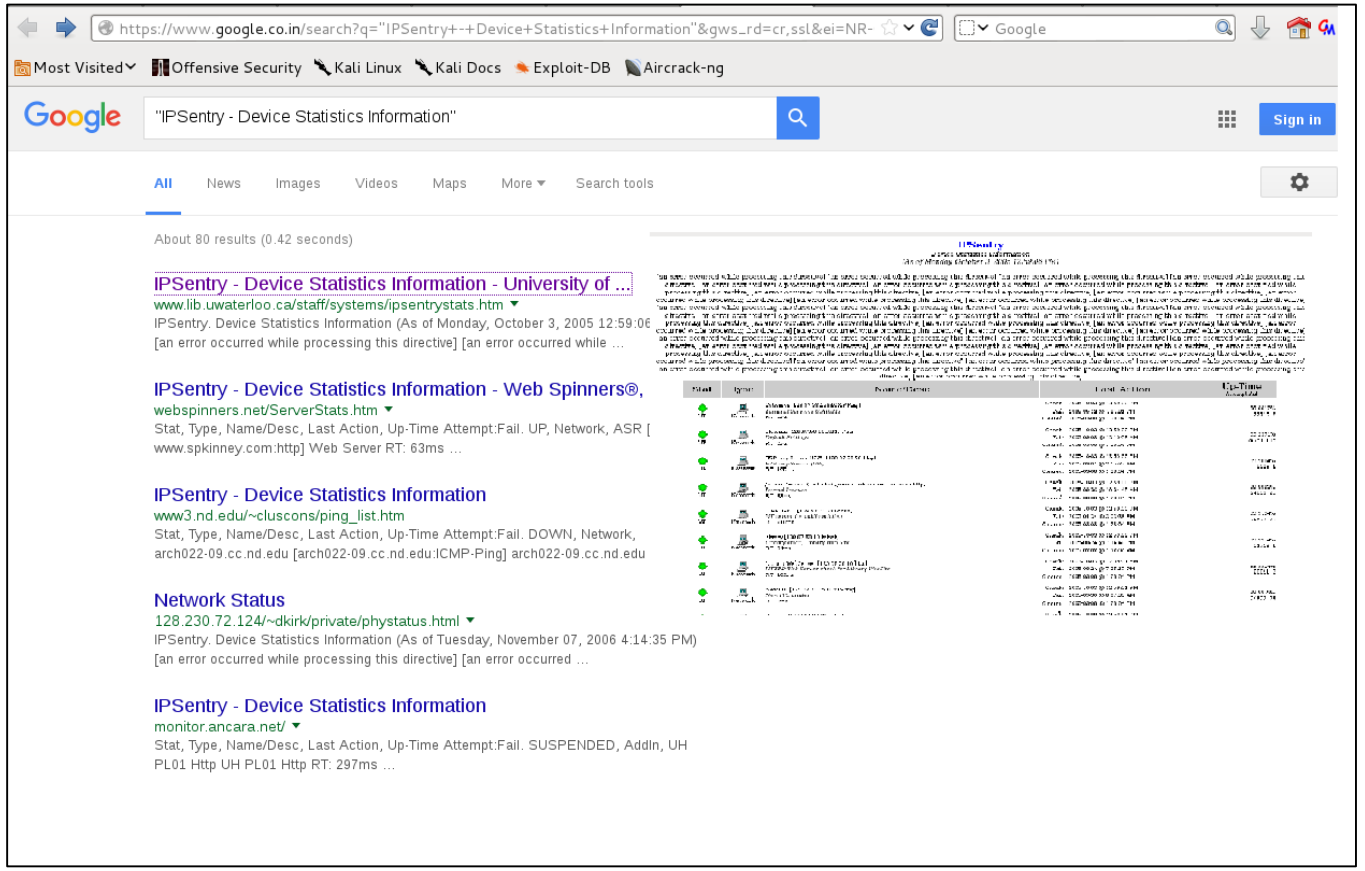
IP Cameras

Inurl:”ViewerFrame?Mode=”



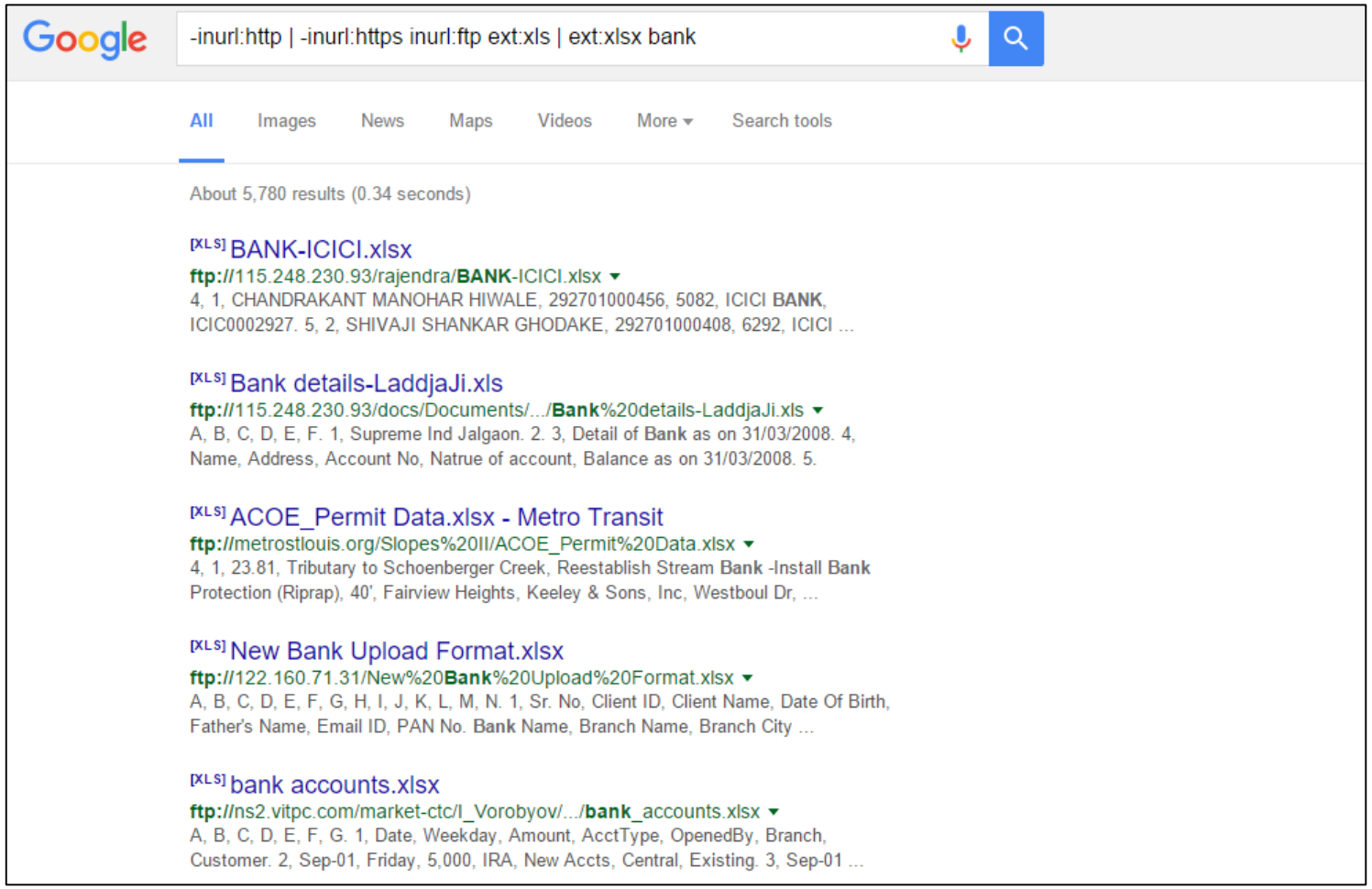
Network monitoring

"IPSentry - Device Statistics Information"



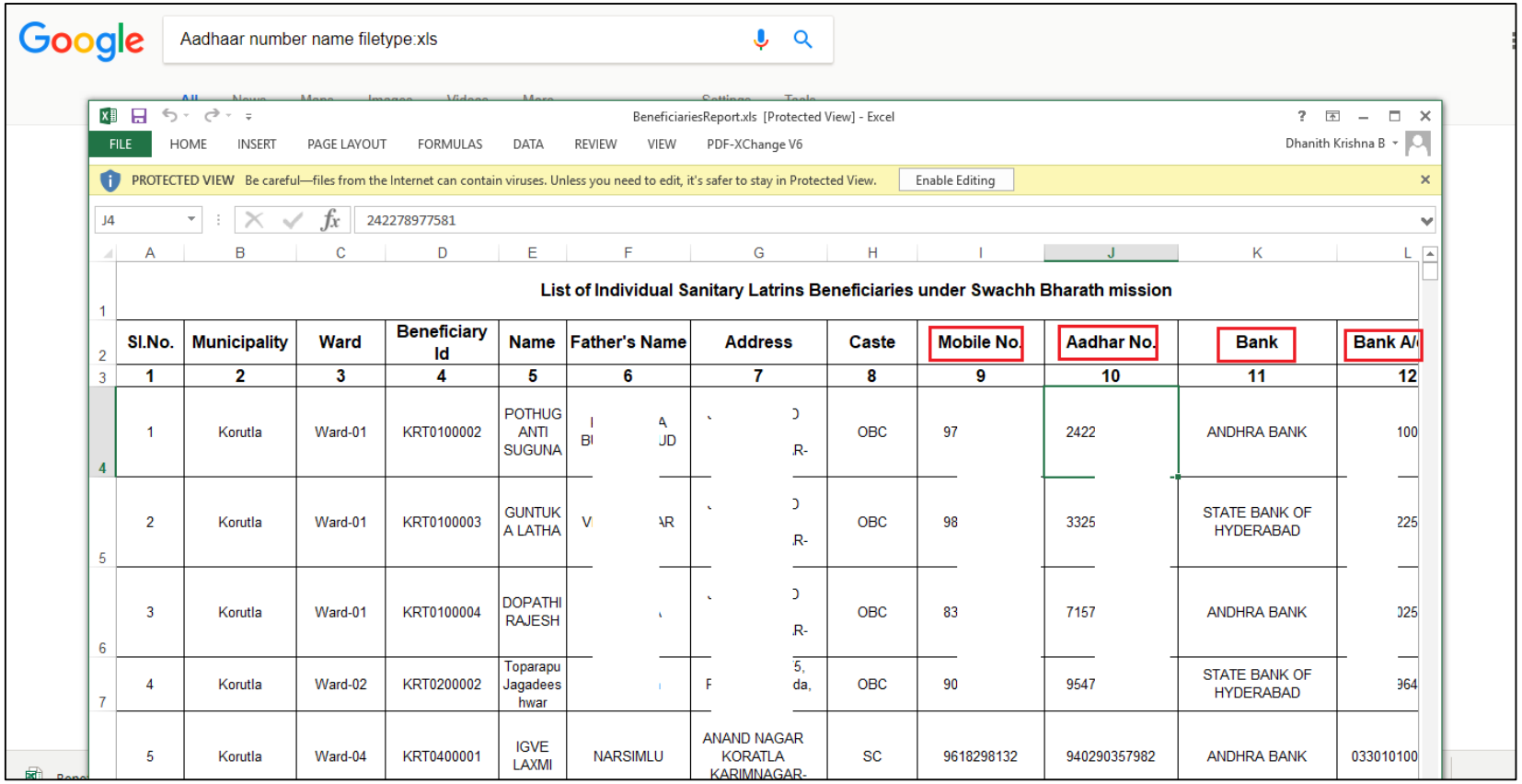
Banking details

-inurl:http | -inurl:https inurl:ftp ext:xls | ext:xlsx bank



Aaadhar :/

Aadhaar number name filetype:xls



List of Individual Sanitary Latrins Beneficiaries under Swachh Bharath mission

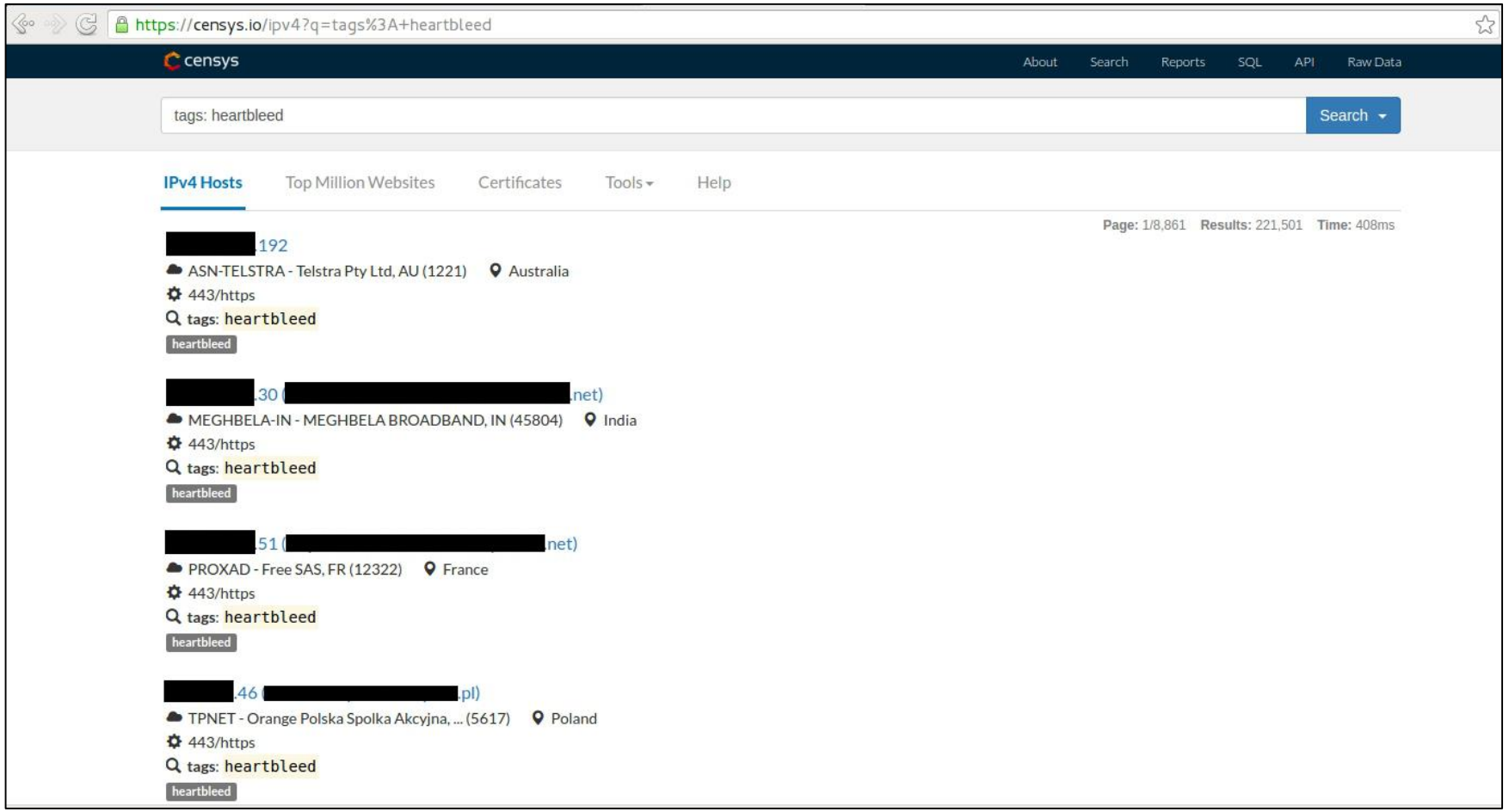
Sl.No.	Municipality	Ward	Beneficiary Id	Name	Father's Name	Address	Caste	Mobile No.	Aadhar No.	Bank	Bank A/
1	2	3	4	5	6	7	8	9	10	11	12
1	Korutla	Ward-01	KRT0100002	POTHUGANTI SUGUNA	I BI A JD	) .R-	OBC	97	2422	ANDHRA BANK	100
2	Korutla	Ward-01	KRT0100003	GUNTUKA LATHA	V AR	) .R-	OBC	98	3325	STATE BANK OF HYDERABAD	225
3	Korutla	Ward-01	KRT0100004	DOPATHI RAJESH		) .R-	OBC	83	7157	ANDHRA BANK	025
4	Korutla	Ward-02	KRT0200002	Toparapu Jagadeeshwar		F 5, da,	OBC	90	9547	STATE BANK OF HYDERABAD	964
5	Korutla	Ward-04	KRT0400001	IGVE LAXMI	NARSIMLU	ANAND NAGAR KORATLA KARIMNAGAR-	SC	9618298132	940290357982	ANDHRA BANK	033010100

Where to find dorks?

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

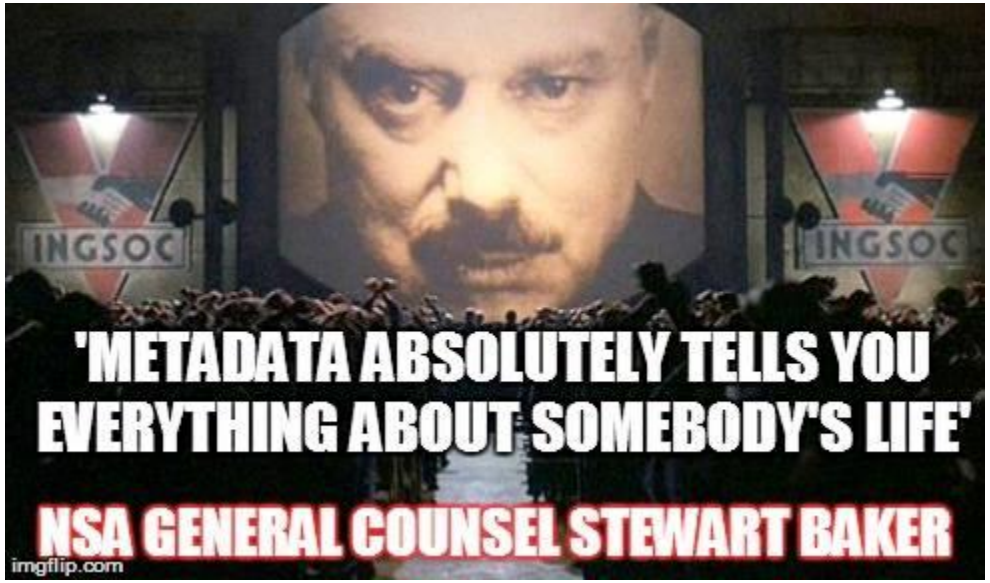
IOT Search Engine

IOT Search Engine

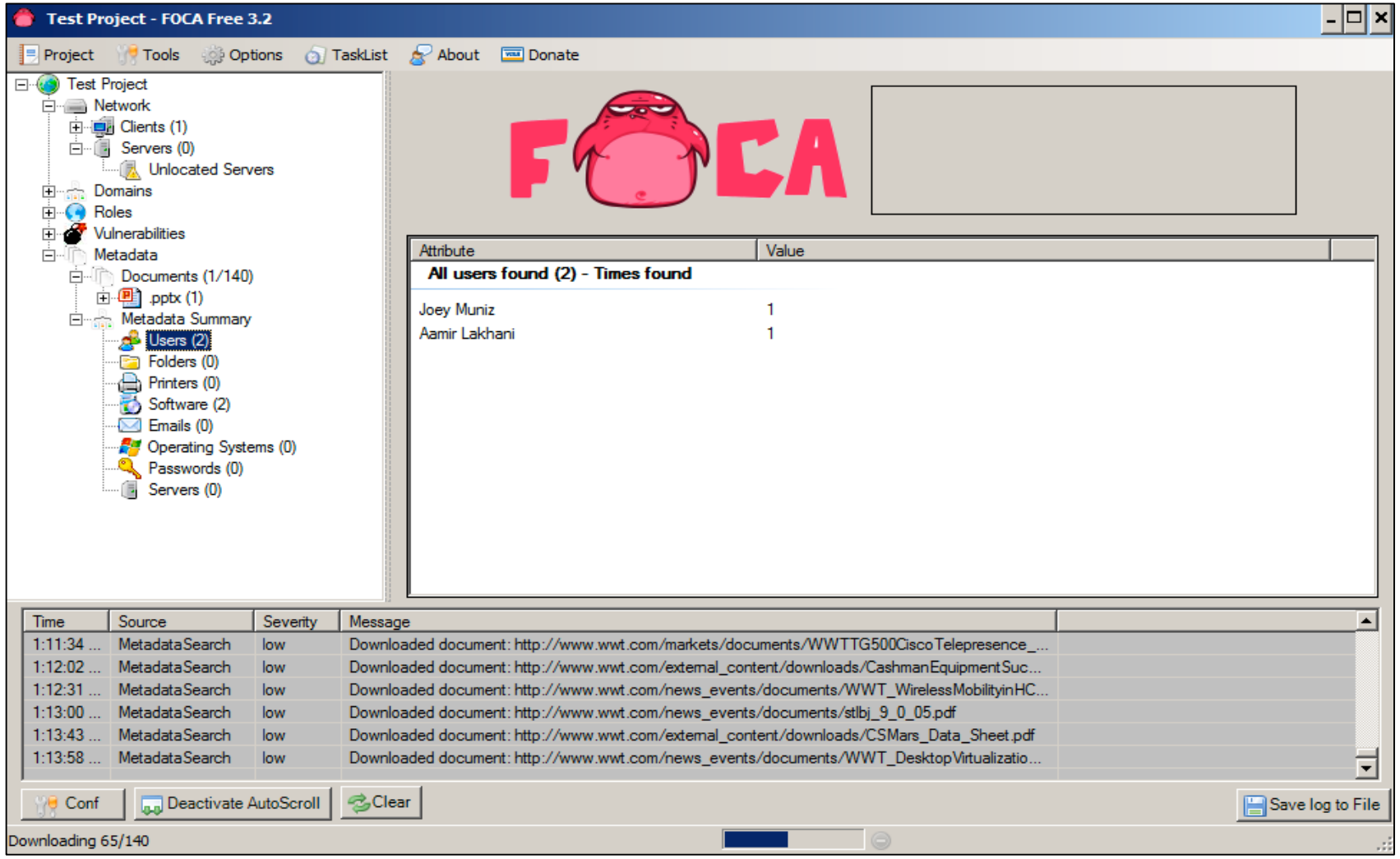


Metadata

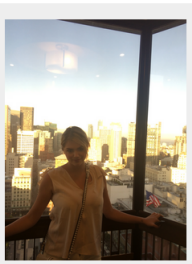
- Metadata is data describing data inside files
- Metadata information reveals lots of juicy info



Metadata


Test Project - FOCA Free 3.2
Project
Tools
Options
TaskList
About
Donate
Test Project
Network
Clients (1)
Servers (0)
Unlocated Servers
Domains
Roles
Vulnerabilities
Metadata
Documents (1/140)
.pptx (1)
Metadata Summary
Users (2)
Folders (0)
Printers (0)
Software (2)
Emails (0)
Operating Systems (0)
Passwords (0)
Servers (0)
FOCA
Attribute
Value
All users found (2) - Times found
Joey Muniz 1
Aamir Lakhani 1
Time Source Severity Message
1:11:34 ... MetadataSearch low Downloaded document: http://www.wwt.com/markets/documents/WWTTG500CiscoTelepresence_...
1:12:02 ... MetadataSearch low Downloaded document: http://www.wwt.com/external_content/downloads/CashmanEquipmentSuc...
1:12:31 ... MetadataSearch low Downloaded document: http://www.wwt.com/news_events/documents/WWT_WirelessMobilityinHC...
1:13:00 ... MetadataSearch low Downloaded document: http://www.wwt.com/news_events/documents/stlbj_9_0_05.pdf
1:13:43 ... MetadataSearch low Downloaded document: http://www.wwt.com/external_content/downloads/CSMars_Data_Sheet.pdf
1:13:58 ... MetadataSearch low Downloaded document: http://www.wwt.com/news_events/documents/WWT_DesktopVirtualizatio...
Conf
Deactivate AutoScroll
Clear
Save log to File
Downloading 65/140

Metadata



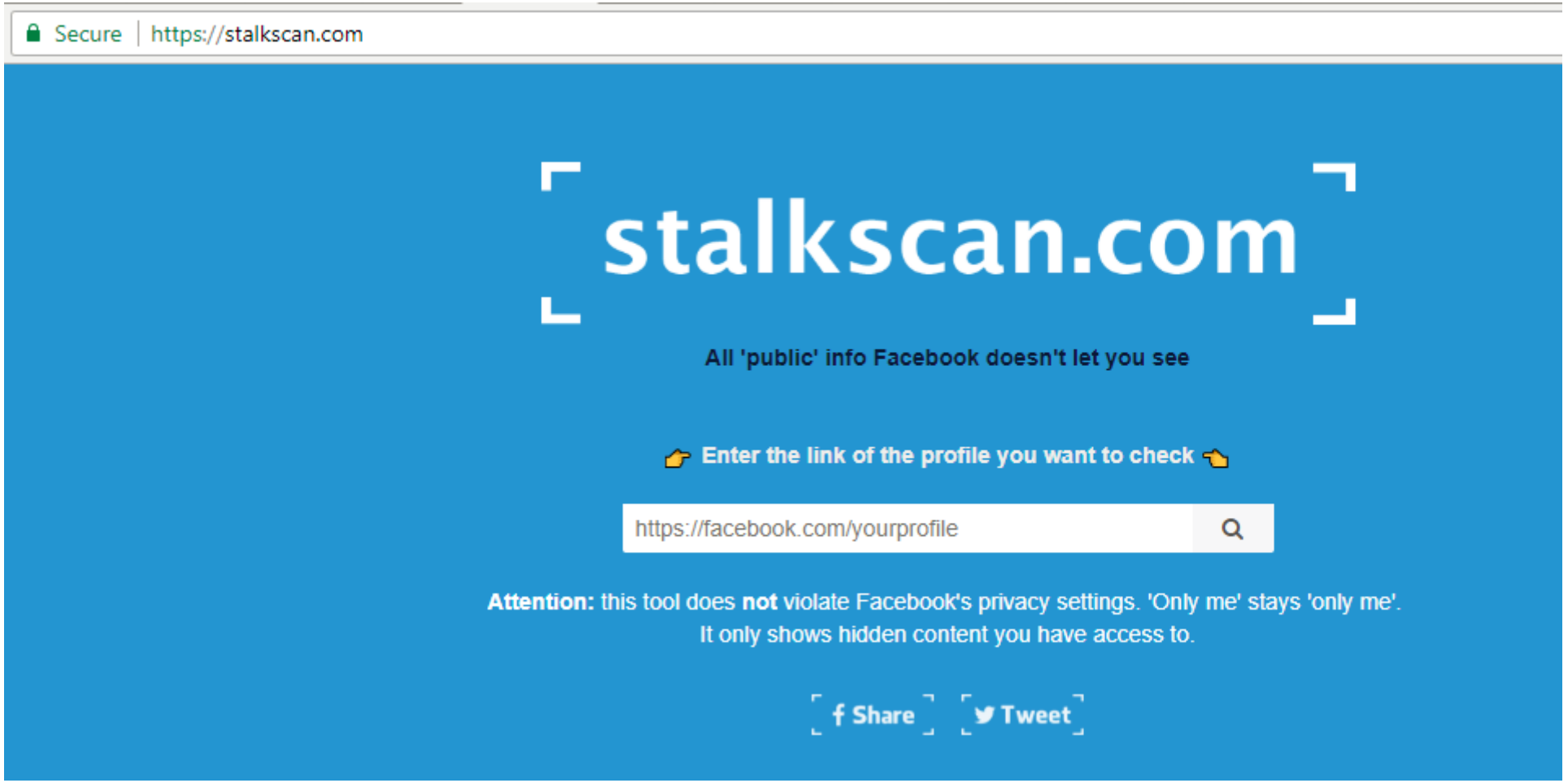
Make	Apple
Model	iPhone 5s
Date	2014:05:26 19:24:31

ApertureValue	2.2750071245369052
BrightnessValue	4.261927945472249
ColorSpace	1
ComponentsConfiguration	YCbCr
DateTime	2014:08:17 18:30:16
DateTimeDigitized	2014:05:26 19:24:31
DateTimeOriginal	2014:05:26 19:24:31
ExifIFDPointer	2316
ExifVersion	0221
ExposureMode	0
ExposureProgram	Normal program
ExposureTime	0.012195121951219513
FNumber	2.2
Flash	Flash fired, compulsory flash mode
FlashpixVersion	0100
FocalLength	4.12
FocalLengthIn35mmFilm	30
GPSAltitude	30.407744874715263
GPSAltitudeRef	0
GPSImgDirection	111.54248366013071
GPSImgDirectionRef	T
GPSInfoIFDPointer	5716
GPSLatitude	37,47,16.48
GPSLatitudeRef	N
GPSLongitude	122,24,35.88
GPSLongitudeRef	W
GPSTimeStamp	2,24,31.24

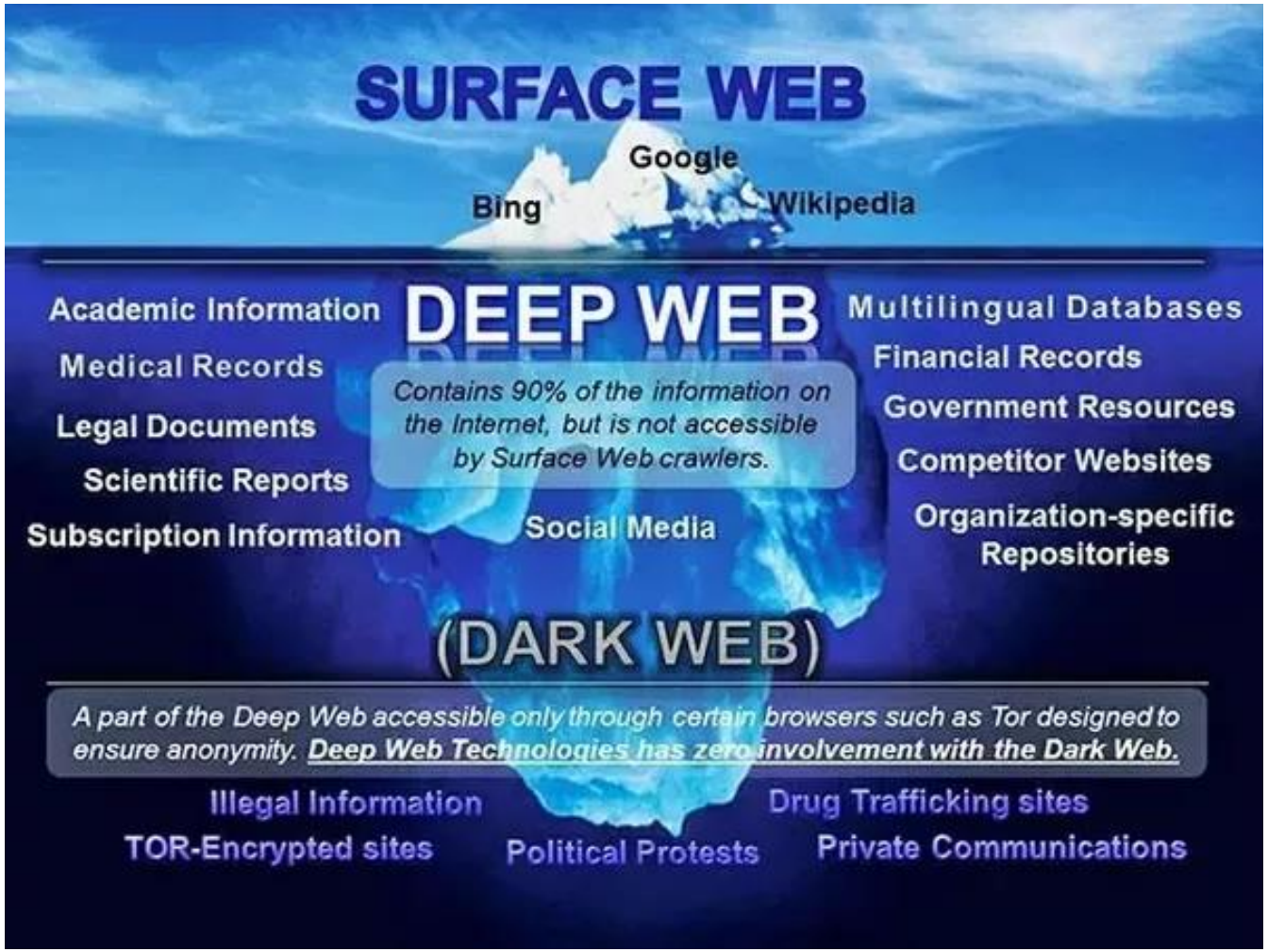
SOCINT

- Social media is an inevitable part of modern life.
- Most social media websites has insecure default privacy settings.
- Real data exposure is not known to end users.
- Facebook Graph Search.

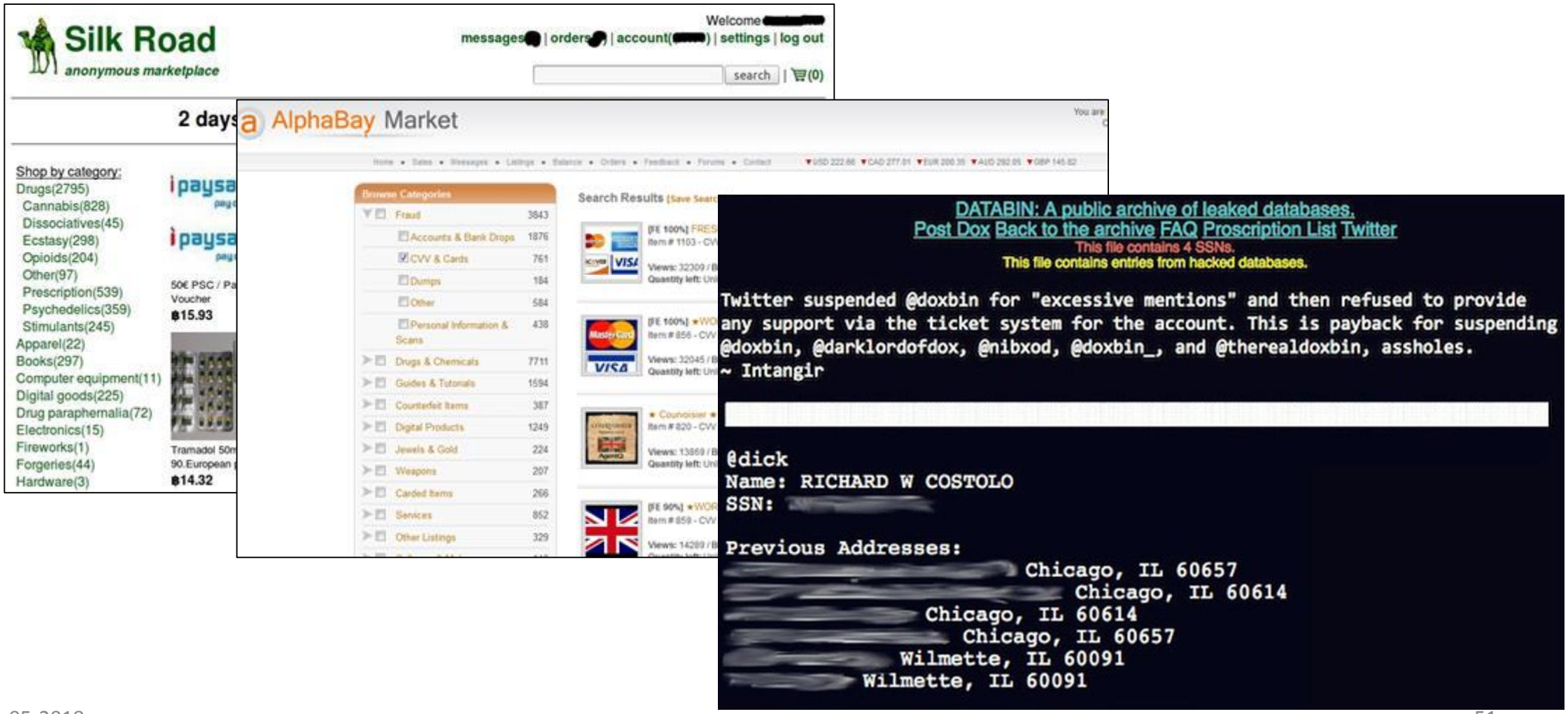
SOCINT


Secure | https://stalkscan.com
stalkscan.com
All 'public' info Facebook doesn't let you see
Enter the link of the profile you want to check
https://facebook.com/yourprofile
Attention: this tool does not violate Facebook's privacy settings. 'Only me' stays 'only me'.
It only shows hidden content you have access to.
Share
Tweet

Dark and Deep Web INTEL



Dark and Deep Web INTEL

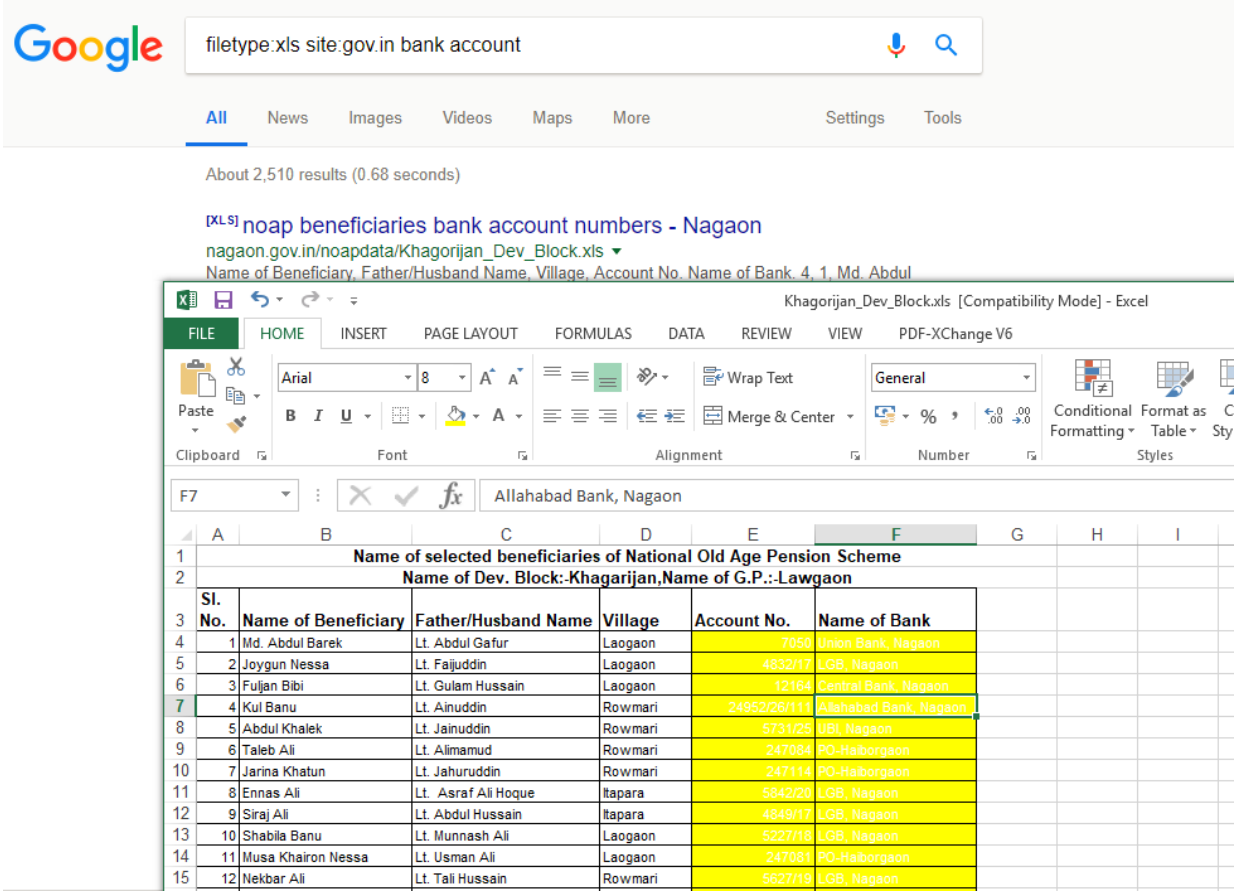


Breach Data

- When online businesses or websites are hacked , hackers sometime makes the breached data public
- Available in paste sites, torrent sites, hacker forums and dark web
- Breach data contains clear text passwords
- People tend to reuse passwords

GOVINT

Government Portals leak a lot of data on us



	A	B	C	D	E	F	G	H	I
1	Name of selected beneficiaries of National Old Age Pension Scheme								
2	Name of Dev. Block:-Khagarijan,Name of G.P.:-Lawgaon								
3	Sl. No.	Name of Beneficiary	Father/Husband Name	Village	Account No.	Name of Bank			
4	1	Md. Abdul Barek	Lt. Abdul Gafur	Laogaon	7050	Union Bank, Nagaon			
5	2	Joygun Nessa	Lt. Faijuddin	Laogaon	4832/17	LGB, Nagaon			
6	3	Fuljan Bibi	Lt. Gulam Hussain	Laogaon	12164	Central Bank, Nagaon			
7	4	Kul Banu	Lt. Ainuddin	Rowmari	24952/26/111	Allahabad Bank, Nagaon			
8	5	Abdul Khalek	Lt. Jainuddin	Rowmari	5731/25	SBI, Nagaon			
9	6	Taleb Ali	Lt. Alimamud	Rowmari	247084	PO-Haiborgaon			
10	7	Jarina Khatun	Lt. Jahuruddin	Rowmari	247114	PO-Haiborgaon			
11	8	Ennas Ali	Lt. Asraf Ali Hoque	Itapara	5842/20	LGB, Nagaon			
12	9	Siraj Ali	Lt. Abdul Hussain	Itapara	4849/17	LGB, Nagaon			
13	10	Shabila Banu	Lt. Munnash Ali	Laogaon	5227/18	LGB, Nagaon			
14	11	Musa Khairon Nessa	Lt. Usman Ali	Laogaon	247081	PO-Haiborgaon			
15	12	Nekbar Ali	Lt. Tali Hussain	Rowmari	5627/19	LGB, Nagaon			

Protecting Yourself

- Keep your sensitive data off the web!
- Audit yourself .
- Request for removal of the content online

Audit Yourself

- Use OSINT tools to perform recon on yourselves
  - http://osintframework.com/
  - https://inteltechniques.com/

- Check your social media privacy settings

Thank You

Happy Hacking