Reconnaissance_Footprinting

What is Reconnaissance?

Collect Elementary Intel

Discover OS, Web Servers & Platforms

Perform Queries

Discover Vulnerabilities

Types of Recon

Goals of Recon

What Am I Looking For?

Network Information

- Domain Names
- Internal Domains
- IP Addresses
- Unmonitored/Private Websites
- TCP/UDP Services
- IDS/Access Controls
- VPN Info
- Phone Numbers/VoIP

Operating System Information

- User & Group Names/Info
- Banner Grabbing
- Routing Tables
- SNMP
- System Architecture
- Remote Systems
- System Names
- Passwords

Tools of Recon

Hundreds of Tools

Search engines | Websites | Applications and built-in commands

Where to Start?

- Search engines
- Websites
- Whois
- PING & DNS

Using Search Engines

Looking up info about website/target

Looking up URL paths

Not settling on first page of results

Hack This Site!

https://www.hackthissite.org

HackThisSite IRC Forums Radio Store URL Shortener Like Us Follow Us

HACK THIS SITE.ORG

[Advertise With HackThisSite.org]

For God hates utterly The bray of bragging tongues.

You are browsing HackThisSite over SSL

Login (or Register):

Login

Lost Your Password?

Donate

DONATE

HTS costs up to $300 a month to operate. We need your help!

Challenges

- Basic missions
- Realistic missions
- Application missions
- Programming missions
- Phonephreaking missions
- Javascript missions
- Forensic missions
- Extbasic missions
- Stego missions
- Irc missions

Get Informed

- Blogs
- News
- Articles

Hack This Site is a free, safe and legal training ground for hackers to test and expand their hacking skills. More than just another hacker wargames site, we are a living, breathing community with many active projects in development, with a vast selection of hacking articles and a huge forum where users can discuss hacking, network security, and just about everything. Tune in to the hacker underground and get involved with the project.

First timers should read the HTS Project Guide and create an account to get started. All users are also required to read and adhere to our Legal Disclaimer.
Get involved on our IRC server: irc.hackthissite.org SSL port 7000 #hackthissite or our web forums.

NOW PLAYING ON OFFLINE:
» Unknown - Unknown (kbps, listeners)

LATEST FORUM POSTS:
Please login to see this feature.

LATEST IRC LINES:
Please login to see this feature.

Latest site news:

25/01/15: HTS Reflects on U.S. State of the Union

STAFF BLOGS / SHORT NEWS:
news Security News - Marc...
blog Metasploit Unleashed
news [UPDATE] CDN TLS Cer...
news Happy new year!
blog POSITION FILLED

LATEST ARTICLES:
Java Basics
Java Platform
GNU/Linux: A Short Story
Solving Programming 8 The Al...
jQuery Selectors & Basic...

RSS FEEDS:
News: Change in Focus
Vuln: FFmpeg libavcodec 'sp5...
FortiGuard Labs sees fast ri...
Fortune 1000 companies keep ...
Evaluating network security ...

CONTRIBUTE:
» IRC - Chat
» Forums - Discussion

https://www.google.com/search?ei=9IcAXaXuLcaasAe2IKCoCg&q=hackthissite&oq=hackthissite&gs_l=psy-ab.3..35i39j0i203l9.20055.20055..20583...0.0..0.204.204.2-1.....0....1..gws-wiz.jEoCFOLkq2c

Google hackthissite

الكل فيديو صور الأخبار الكتب المزيد الإعدادات الأدوات

حوالي 325.000 من النتائج (عدد الثواني: 0,36)

Hack This Site!

https://www.hackthissite.org/ ترجم هذه الصفحة

HackThisSite! is a legal and safe network security resource where - 2018/12/27
users test their hacking skills on various challenges and learn about hacking ...

User/login

HackThisSite! is a legal and safe network security resource ...

About the Project

This guide is an introduction to the site, community, philosophy and ...

Register

Notice to Microsoft Mail Users. We are receiving reports of mail ...

Forums

HackThisSite: Topics: Posts: Last post. News News and Updates ...

HTS

First timers should read the HTS Project Guide and create an ...

Lost Your Password?

You will find a link that allows you to reset your password. That link ...

حوالي 308.000 من النتائج (عدد الثواني: 0,38)

Libyana

https://www.libyana.ly/

المدن المغطاة بخدمة **ليبيانا**. 49+. فريقنا. 1500+. مراكزنا. 34+. مشتركينا. 5000000+. آخر الأخبار والأحداث. عقد اتفاق رعاية البطل الليبي العالمي كمال القرقني. 02/01/ ...

كروت التعبئة المكشوطة
الصفحة الرئيسية · الدعم والمساعدة؛ كروت التعبئة المكشوطة. في حال ...

الاستعلام عن الأرقام المميزة
الاستفسار عن الأرقام المميزة. الصفحة الرئيسية · الدعم ...

باقات الجيل الرابع
باقات الجيل الرابع. يمكنك الاشتراك في باقتي 7 جيجابايت و 10 ...

Libyana
ليبيانا · نبذة عن شركة ليبيانا · فريق ليبيانا · اتصل بنا ...

الحصول على رمز PUK
الصفحة الرئيسية · الدعم والمساعدة؛ الحصول على رقم ال PUK. يرجى ...

انترنت
باقات الانترنت : تمتع بباقات الانترنت الجديدة ومميزاتها من ...

مزيد من النتائج من libyana.ly »

ليبيانا

شركة

ليبيانا للهاتف المحمول هي شركة اتصالات عبر الهاتف المحمول تم تأسيسها سنة 2004. ليبيانا هي إحدى اثنين من شركات الاتصالات في ليبيا ومملوكة من طرف الشركة الليبية للبريد والاتصالات وتقنية المعلومات القابضة. ويكيبيديا

المؤسسة الأم: الشركة الليبية للبريد والاتصالات وتقنية المعلومات القابضة

التأسيس: يناير 2004

المقر الرئيسي: طرابلس

عدد الموظفين: 800

يبحث الأشخاص أيضًا عن

عرض +5 أخرى



Using Websites

Targets website

Research website

Things on a website that make you go hmmmmm

www.r

High Speed Search: GO

[redacted] INTERNET

| Home | Coverage | Residential | Business | Signup |

Search by Google

Quick Links

[redacted] Webmail

Webmail Login for Hosted/Private Domains

Email HowTo's

Help for Sending Email
Outlook 2003 setup
Outlook Express setup

Is Your PC Healthy?
What is a PC Virus?
What is Spyware?
What is Adware?

Virus & Spyware Protection Tools
AVG anti-virus
MS Windows® Defender;
Ad-Aware
Spybot Search & Destroy

Global Internet Traffic Report

Remote Assistance

Mikogo

[redacted]

Click here to read the letter mailed to all our current customers!

Techsupport Note:

We have recently upgraded our Email Server! If any of our customers are having trouble Sending email please refer to the Help for Sending Email link.

For new customer sign up please visit our website

[redacted]

or call us toll free.

[redacted]

SOLUTIONS...

New Service Options

- Site Survey Signup
- Prequalify
- Contact F[redacted]

Customer Plans

- Residential
- Business

Your broadband Internet has to be fast, reliable and able to meet your growing demands. We have invested over $200 million to create the next evolution in connectivity – *The Network*. Engineered with one goal in mind, to provide you with the best Broadband Internet choice. We are the largest Digital Fixed Wireless network in the country.

Call today to get connected

CLICK HERE

View all posts

Broadband Wonders: Five Netflix-Only Shows to Check Out

October 1, 2014

Netflix has gained considerable traction as a video streaming application across America. Allowing you to watch a number of shows and movies via a broadband connection for a monthly fee is just too good to

READ MORE

Wireless Internet Wonders: Samsung's New Curved TV – What The Experts Are Saying

September 24, 2014

Television technologies have exploded in the last decade. From flat-screens to high definition TVs to Smart TV, innovation in the industry has not ceased. Ever since January of this year, yet another innovation can be

READ MORE

Receive eNews

Like us on Facebook

Follow us on Twitter

RSS feed

ASK A QUESTION
LIVE CHAT

Why Residential Business Support Contact Us My Account

https://www.[redacted].ly/ar/

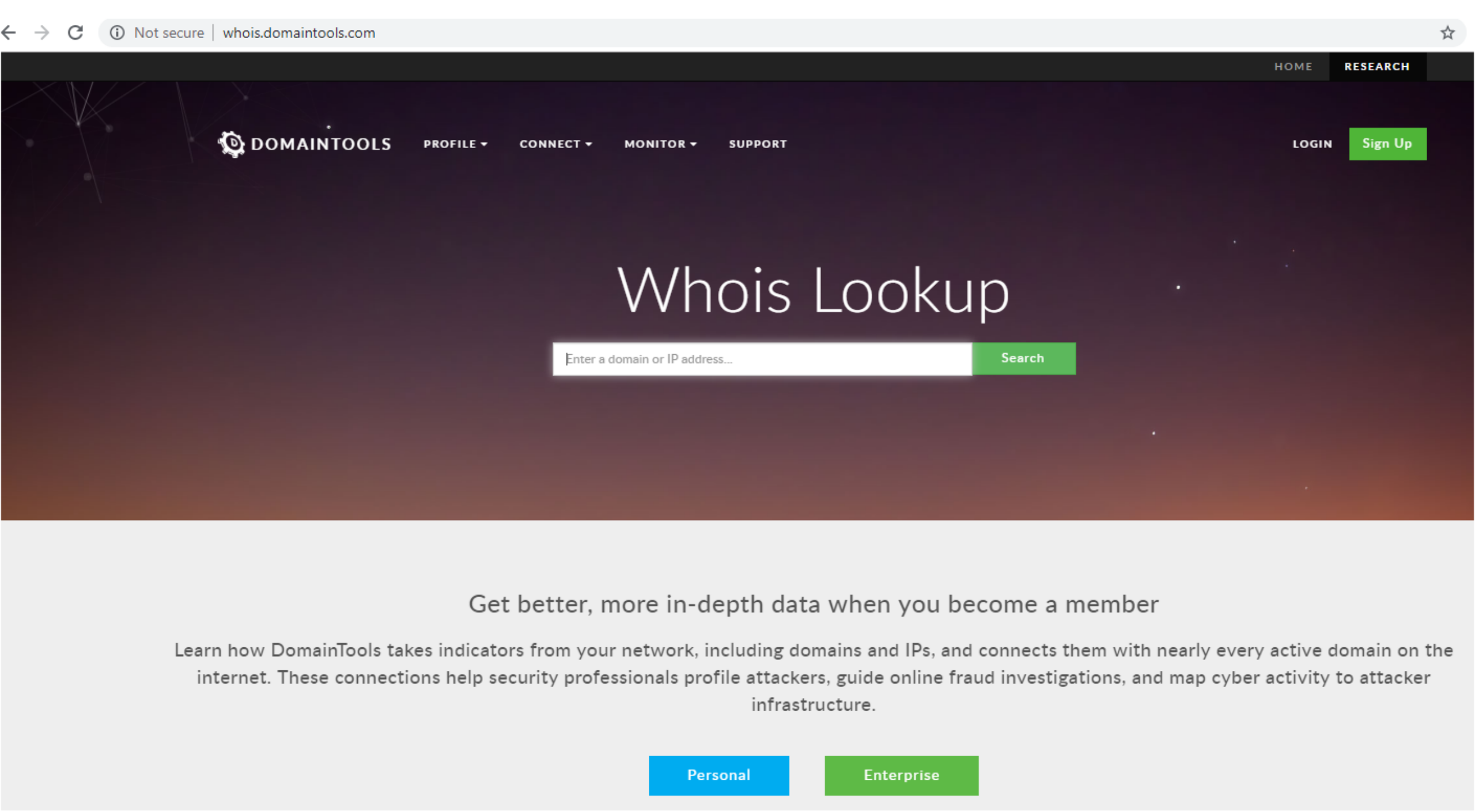
English إتصل بنا النماذج والأدوات وظائف المركز الإعلامي العلاقات مع المساهمين تسجيل دخول الموظفين ابحث في موقعنا

[redacted]

الأفراد الشركات كيف تتعامل معنا من نحن خدمة الزبائن

Using Whois

Domain name info (IP address, owner, expiration)


Not secure | whois.domaintools.com
HOME
RESEARCH
DOMAINTOOLS
PROFILE
CONNECT
MONITOR
SUPPORT
LOGIN
Sign Up
Whois Lookup
Enter a domain or IP address...
Search
Get better, more in-depth data when you become a member
Learn how DomainTools takes indicators from your network, including domains and IPs, and connects them with nearly every active domain on the internet. These connections help security professionals profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure.
Personal
Enterprise

Whois Record for HackThisSite.org

Domain Profile

Registrant Org	Whois Privacy Protection Service, Inc.
Registrant Country	us
Registrar	eNom, Inc. IANA ID: 48 URL: http://www.enom.com Whois Server: whois.enom.com abuse@enom.com (p) 14252982646
Registrar Status	clientTransferProhibited
Dates	5,784 days old Created on 2003-08-10 Expires on 2019-08-10 Updated on 2019-04-16
Name Servers	C.NS.BUDDYNS.COM (has 11,808 domains) F.NS.BUDDYNS.COM (has 11,808 domains) G.NS.BUDDYNS.COM (has 11,808 domains) H.NS.BUDDYNS.COM (has 11,808 domains) J.NS.BUDDYNS.COM (has 11,808 domains)
Tech Contact	—
IP Address	137.74.187.100 - 3 other sites hosted on this server
IP Location	- Hauts-de-france - Roubaix - Ovh Sas
ASN	AS16276 OVH, FR (registered Feb 15, 2001)
Domain Status	Registered And Active Website

Website

Website Title	500 SSL negotiation failed:
Response Code	500
Terms	1,017 (Unique: 523, Linked: 275)
Images	32 (Alt tags missing: 7)
Links	148 (Internal: 112, Outbound: 36)

Whois Record (last updated on 2019-06-11)

```
Domain Name: HACKTHISSITE.ORG
Registry Domain ID: D99641092-LROR
Registrar WHOIS Server: whois.enom.com
Registrar URL: http://www.enom.com
Updated Date: 2019-04-17T04:42:11Z
Creation Date: 2003-08-10T15:01:25Z
Registry Expiry Date: 2019-08-10T15:01:25Z
Registrar Registration Expiration Date:
Registrar: eNom, Inc.
Registrar IANA ID: 48
Registrar Abuse Contact Email: abuse@enom.com
Registrar Abuse Contact Phone: +1.4252982646
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Organization: Whois Privacy Protection Service, Inc.
Registrant State/Province: WA
Registrant Country: US
Name Server: C.NS.BUDDYNS.COM
Name Server: F.NS.BUDDYNS.COM
Name Server: G.NS.BUDDYNS.COM
Name Server: H.NS.BUDDYNS.COM
Name Server: J.NS.BUDDYNS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/)

For more information on Whois status codes, please visit https://icann.org/epp
```

SEARCH

Search SEARCH

NRO Executive Council

NRO EC Meeting Minutes

Regional Internet Registries

The Internet Registry System

RIR History

Internet Number Resources

IPv6

IPv6 Deployment FAQs

IPv4 Exhaustion FAQs

About the NRO

The Number Resource Organization (NRO) was established in 2003 as a coordinating body for the world's five Regional Internet Registries (RIRs).

The RIRs manage the distribution of Internet number resources (IP address space and Autonomous System Numbers) within their respective regions.

Mission

The mission of the NRO is to actively contribute to an open, stable and secure Internet, through:

- Providing and promoting a coordinated Internet number registry system.
- Being an authoritative voice on the multi-stakeholder model and bottom-up policy process in Internet governance.
- Coordinating and supporting joint activities of the RIRs.

Executive Council

The CEOs/Directors of the five RIRs form the NRO Executive Council (NRO EC). The positions of Chair, Vice Chair/Secretary and Treasurer rotate annually.

```
root@kali:~# whois hackthissite.org
Domain Name: HACKTHISSITE.ORG
Registry Domain ID: D99641092-LROR
Registrar WHOIS Server: whois.enom.com
Registrar URL: http://www.enom.com
Updated Date: 2019-04-17T04:42:11Z
Creation Date: 2003-08-10T15:01:25Z
Registry Expiry Date: 2019-08-10T15:01:25Z
Registrar Registration Expiration Date:
Registrar: eNom, Inc.
Registrar IANA ID: 48
Registrar Abuse Contact Email: abuse@enom.com
Registrar Abuse Contact Phone: +1.4252982646
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Organization: Whois Privacy Protection Service, Inc.
Registrant State/Province: WA
Registrant Country: US
Name Server: C.NS.BUDDYNS.COM
Name Server: F.NS.BUDDYNS.COM
Name Server: G.NS.BUDDYNS.COM
Name Server: H.NS.BUDDYNS.COM
Name Server: J.NS.BUDDYNS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/)
>>> Last update of WHOIS database: 2019-06-12T05:46:25Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

Using PING & DNS

PING: your best friend

DNS: using NSLOOKUP

```
Ping statistics for 198.148.81.139:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 86ms, Maximum = 86ms, Average = 86ms

C:\>ping www.hackthissite.org -i 13 -n 1

Pinging www.hackthissite.org [198.148.81.135] with 32 bytes of data:
Reply from 198.148.81.135: bytes=32 time=149ms TTL=55

Ping statistics for 198.148.81.135:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 149ms, Maximum = 149ms, Average = 149ms

C:\>ping www.hackthissite.org

Pinging www.hackthissite.org [198.148.81.135] with 32 bytes of data:
Reply from 198.148.81.135: bytes=32 time=86ms TTL=55
Reply from 198.148.81.135: bytes=32 time=87ms TTL=55
Reply from 198.148.81.135: bytes=32 time=86ms TTL=55
Reply from 198.148.81.135: bytes=32 time=99ms TTL=55

Ping statistics for 198.148.81.135:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 86ms, Maximum = 99ms, Average = 89ms
```

```
C:\>nslookup yahoo.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    yahoo.com
Addresses:  206.190.36.45
          98.139.183.24
          98.138.253.109


C:\>nslookup
Default Server:  google-public-dns-a.google.com
Address:  8.8.8.8

> yahoo.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    yahoo.com
Addresses:  98.139.183.24
          98.138.253.109
          206.190.36.45

> sears.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    sears.com
Addresses:  184.25.56.124
          184.25.56.114
```

```
> www.hackthissite.org
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.hackthissite.org
Addresses:  2610:150:8007:0:198:148:81:136
          2610:150:8007:0:198:148:81:135
          2610:150:8007:0:198:148:81:138
          2610:150:8007:0:198:148:81:137
          2610:150:8007:0:198:148:81:139
          198.148.81.138
          198.148.81.136
          198.148.81.139
          198.148.81.135
          198.148.81.137

> set type=mx
> hackthissite.org
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
hackthissite.org        MX preference = 10, mail exchanger = ASPMX.L.GOOGLE.COM
hackthissite.org        MX preference = 20, mail exchanger = ALT1.ASPMX.L.GOOGLE.COM
hackthissite.org        MX preference = 20, mail exchanger = ALT2.ASPMX.L.GOOGLE.COM
hackthissite.org        MX preference = 30, mail exchanger = ASPMX2.GOOGLEMAIL.COM
hackthissite.org        MX preference = 30, mail exchanger = ASPMX3.GOOGLEMAIL.COM
hackthissite.org        MX preference = 30, mail exchanger = ASPMX4.GOOGLEMAIL.COM
hackthissite.org        MX preference = 30, mail exchanger = ASPMX5.GOOGLEMAIL.COM
> set type=a
> alt1.aspmx.l.google.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    alt1.aspmx.l.google.com
Address:  173.194.74.27
```

```
> set type=cname
> hackthissite.org
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

hackthissite.org
        primary name server = ns1.hackthissite.org
        responsible mail addr = admin.hackthissite.org
        serial  = 2014042002
        refresh = 10800 (3 hours)
        retry   = 3600 (1 hour)
        expire  = 604800 (7 days)
        default TTL = 300 (5 mins)
```

```
> set type=soa
> hackthissite.org
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
hackthissite.org
        primary name server = ns1.hackthissite.org
        responsible mail addr = admin.hackthissite.org
        serial  = 2014042002
        refresh = 10800 (3 hours)
        retry   = 3600 (1 hour)
        expire  = 604800 (7 days)
        default TTL = 300 (5 mins)
```

```
> server 198.148.81.188
Default Server:  dns.hackthissite.org
Address:  198.148.81.188

> set type=any
> ls -d hackthissite.org
[dns.hackthissite.org]
*** Can't list domain hackthissite.org: Query refused
The DNS server refused to transfer the zone hackthissite.org to your computer. If this
is incorrect, check the zone transfer security settings for hackthissite.org on the DNS
server at IP address 198.148.81.188.
```

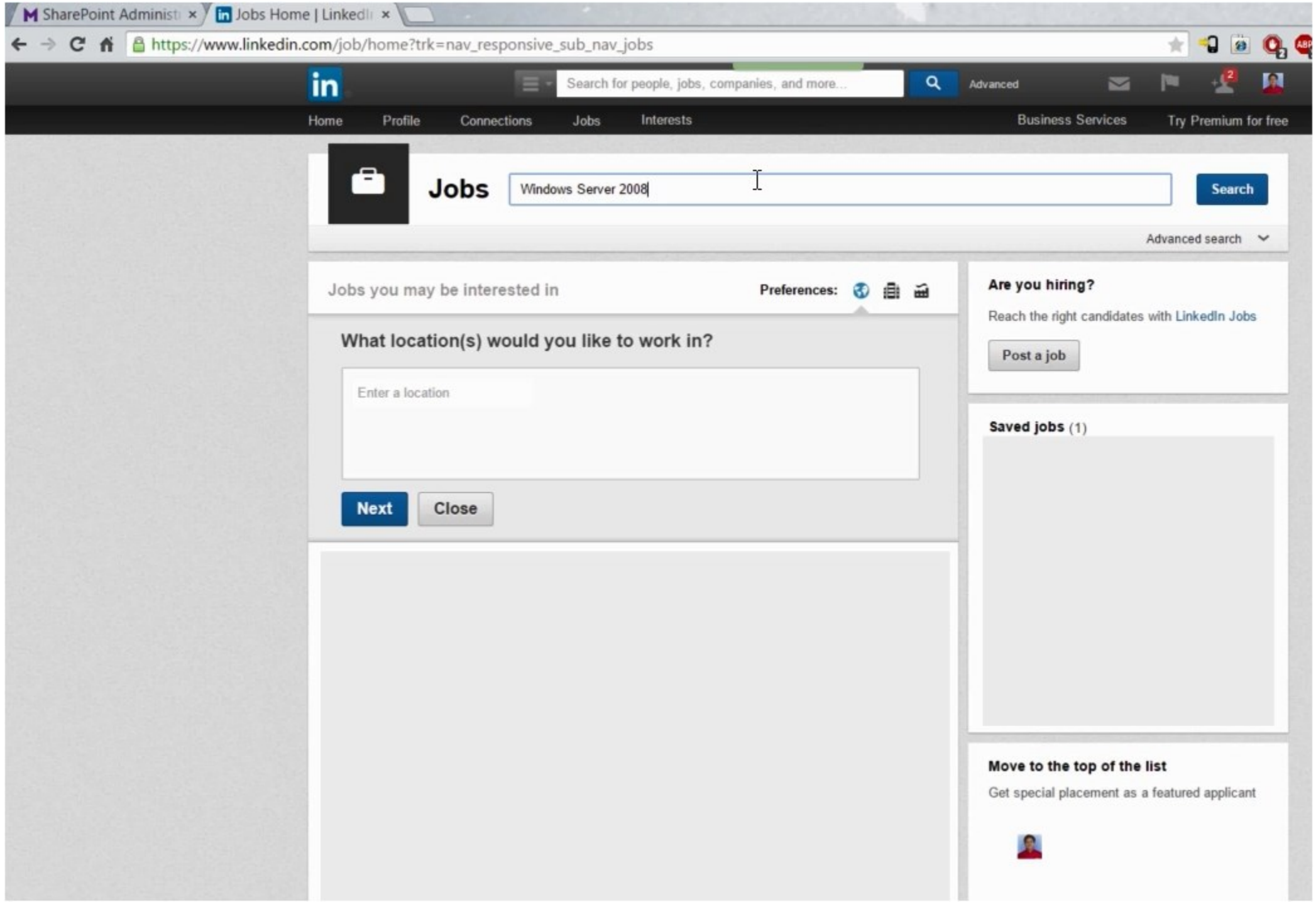
```
> set type=mx
> hackthissite.org
Server:  dns.hackthissite.org
Address:  198.148.81.188

hackthissite.org        MX preference = 10, mail exchanger = ASPMX.L.GOOGLE.COM
hackthissite.org        MX preference = 20, mail exchanger = ALT1.ASPMX.L.GOOGLE.COM
hackthissite.org        MX preference = 20, mail exchanger = ALT2.ASPMX.L.GOOGLE.COM
hackthissite.org        MX preference = 30, mail exchanger = ASPMX2.GOOGLEMAIL.COM
hackthissite.org        MX preference = 30, mail exchanger = ASPMX3.GOOGLEMAIL.COM
hackthissite.org        MX preference = 30, mail exchanger = ASPMX4.GOOGLEMAIL.COM
hackthissite.org        MX preference = 30, mail exchanger = ASPMX5.GOOGLEMAIL.COM
hackthissite.org        nameserver = ns2.hackthissite.org
hackthissite.org        nameserver = b.ns.buddyns.com
hackthissite.org        nameserver = c.ns.buddyns.com
hackthissite.org        nameserver = d.ns.buddyns.com
hackthissite.org        nameserver = e.ns.buddyns.com
hackthissite.org        nameserver = f.ns.buddyns.com
hackthissite.org        nameserver = ns1.hackthissite.org
ns1.hackthissite.org    internet address = 198.148.81.188
ns1.hackthissite.org    AAAA IPv6 address = 2610:150:8007:0:198:148:81:188
ns2.hackthissite.org    internet address = 198.148.81.189
ns2.hackthissite.org    AAAA IPv6 address = 2610:150:8007:0:198:148:81:189
```

Looking at Job Site

Change your view of the information

Look at historical data

Other Job Sites


SharePoint Administ
Jobs Home | LinkedIn
https://www.linkedin.com/job/home?trk=nav_responsive_sub_nav_jobs
Search for people, jobs, companies, and more...
Advanced
Home
Profile
Connections
Jobs
Interests
Business Services
Try Premium for free
Jobs
Windows Server 2008
Search
Advanced search
Jobs you may be interested in
Preferences:
What location(s) would you like to work in?
Enter a location
Next
Close
Are you hiring?
Reach the right candidates with LinkedIn Jobs
Post a job
Saved jobs (1)
Move to the top of the list
Get special placement as a featured applicant

Using NetCraft

Understanding NetCraft

Discover target's external servers

Detect OS and apps

- Top Reporters
- Incentives for reporters
- Phishiest TLDs
- Phishiest Countries
- Phishiest Hosters
- Phishing Map
- Takedown Map
- Most Popular Websites
- Branded Extensions
- Tell a Friend

Phishing & Fraud

- Phishing Site Feed
- Hosting Phishing Alerts
- SSL CA Phishing Alerts
- Registry Phishing Alerts
- Domain Registration Risk
- Bank Fraud Detection
- Phishing Site Countermeasures

Extension Support

- FAQ
- Glossary
- Contact Us
- Report a Bug

Tutorials

- Installing the Extension
- Using the Extension
- Getting the Most
- Reporting a Phish

About Netcraft

Description	HackThisSite! is a legal and safe network security resource where users test their hacking skills on various challenges and learn about hacking and network security. Also provided are articles, comprehensive and active forums, and guides and tutorials. Learn how to hack!
Keywords	challenge, computer, culture, deface, digital, ethics, games, guide, hack, hack forums, hacker, hackers, hacking, hacking challenges, hacking forums, mission, net, programming, radical, revolution, root, rooting, security, site, society, tutorial, tutorials, war, wargame, wargames, web, website

Network

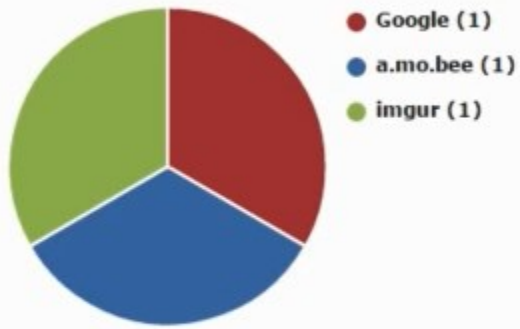
Site	http://www.hackthissite.org	**Netblock Owner**	Sharktech
Domain	hackthissite.org	**Nameserver**	ns1.hackthissite.org
IP address	198.148.81.135	**DNS admin**	admin@hackthissite.org
IPv6 address	2610:150:8007:0:198:148:81:137	**Reverse DNS**	hackthissite.org
Domain registrar	pir.org	**Nameserver organisation**	whois.pir.org
Organisation	Whois Privacy Protection Service, Inc., Kirkland, 98083, US	**Hosting company**	Sharktech Internet Services
Top Level Domain	Organization entities (.org)	**DNS Security Extensions**	*unknown*
Hosting country	US		

Hosting History

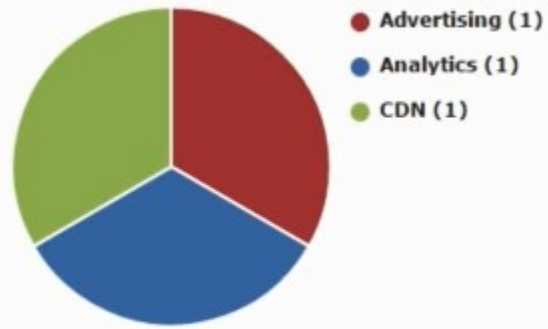
Netblock owner	IP address	OS	Web server	Last seen Refresh
Sharktech 3315 E. Russel Rd A4 112 Las Vegas NV US 89120	198.148.81.138	FreeBSD	HackThisSite Load Balancer	27-Apr-2015
Sharktech 3315 E. Russel Rd A4 112 Las Vegas NV US 89120	198.148.81.137	FreeBSD	HackThisSite Load Balancer	26-Apr-2015
Sharktech 3315 E. Russel Rd A4 112 Las Vegas NV US 89120	198.148.81.135	FreeBSD	HackThisSite Load Balancer	25-Apr-2015
Sharktech 3315 E. Russel Rd A4 112 Las Vegas NV US 89120	198.148.81.139	FreeBSD	HackThisSite Load Balancer	24-Apr-2015
Sharktech 3315 E. Russel Rd A4 112 Las Vegas NV US 89120	198.148.81.136	FreeBSD	HackThisSite Load Balancer	23-Apr-2015
Sharktech 3315 E. Russel Rd A4 112 Las Vegas NV US 89120	198.148.81.138	FreeBSD	HackThisSite Load Balancer	22-Apr-2015
Sharktech 3315 E. Russel Rd A4 112 Las Vegas NV US 89120	198.148.81.139	FreeBSD	HackThisSite Load Balancer	21-Apr-2015
Sharktech 3315 E. Russel Rd A4 112 Las Vegas NV US 89120	198.148.81.138	FreeBSD	HackThisSite Load Balancer	20-Apr-2015
Sharktech 3315 E. Russel Rd A4 112 Las Vegas NV US 89120	198.148.81.139	FreeBSD	HackThisSite Load Balancer	17-Apr-2015
Sharktech 3315 E. Russel Rd A4 112 Las Vegas NV US 89120	198.148.81.135	FreeBSD	HackThisSite Load Balancer	16-Apr-2015

3 known trackers were identified.

Companies



Categories



Company ▲	Primary Category	Tracker	Popular Sites with this Tracker
Google	Analytics	Google Analytics	www.ampparit.com, www.corriere.it, www.chip.de
a.mo.bee	Advertising	Kontera	www.pcadvisor.co.uk, www.thewindowsclub.com, www.macworld.co.uk
imgur	CDN	Imgur	www.rlslog.net, www.smbc-comics.com, www.dasolo.info

Site Technology

Fetched on 12th April 2015

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
PHP	PHP is supported and/or running	www.tomshardware.com , www.ilfattoquotidiano.it , www.chip.de
SSL	A cryptographic protocol providing communication security over the Internet	www.google.fr , www.google.pl , www.google.it

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
JavaScript	Open source programming language commonly implemented as part of a web browser	www.amazon.de , www.google.co.uk , www.dpa-news.de

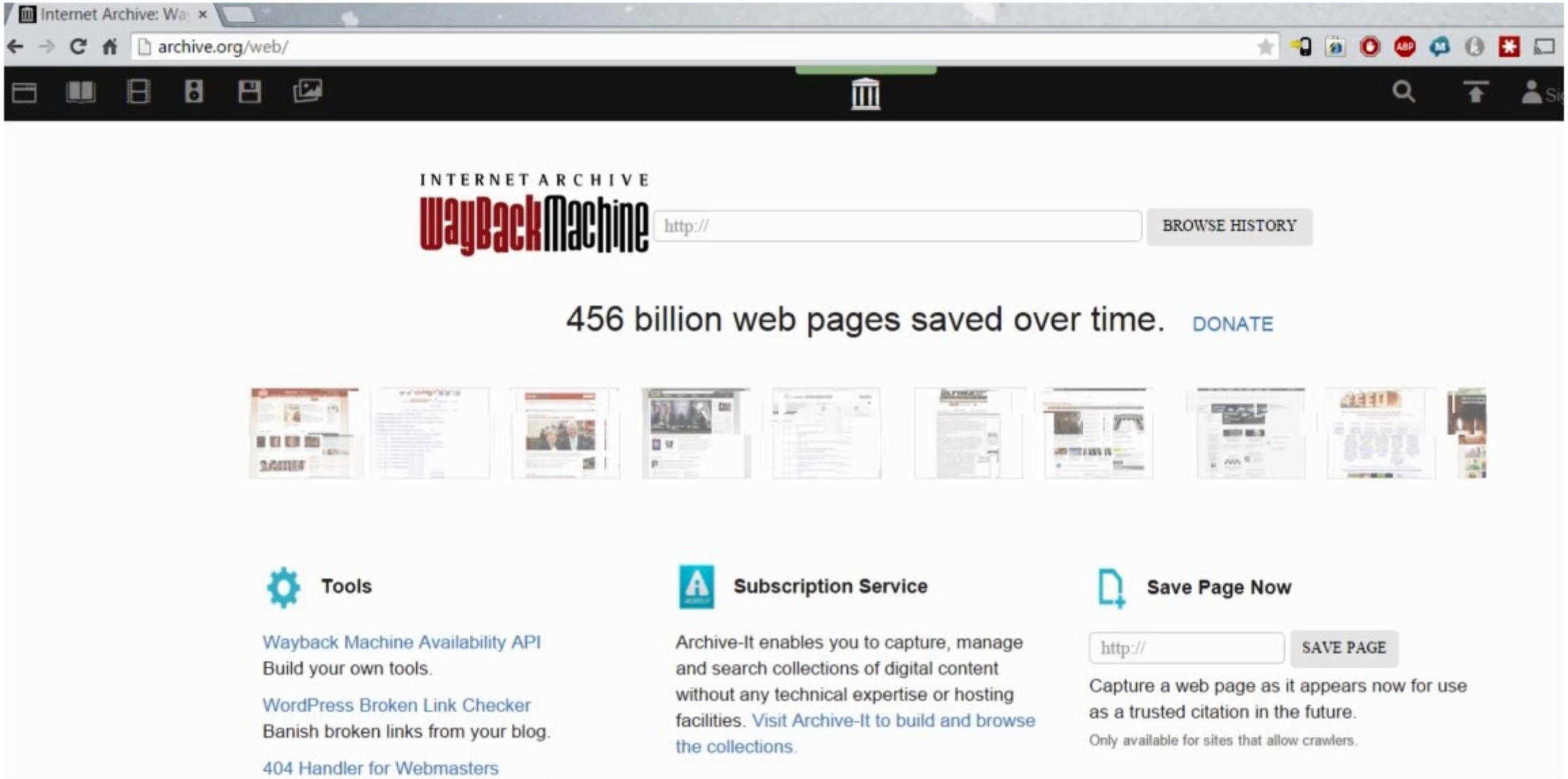
Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow while developing

A Long, Long, Time Ago…

Looking at previous versions

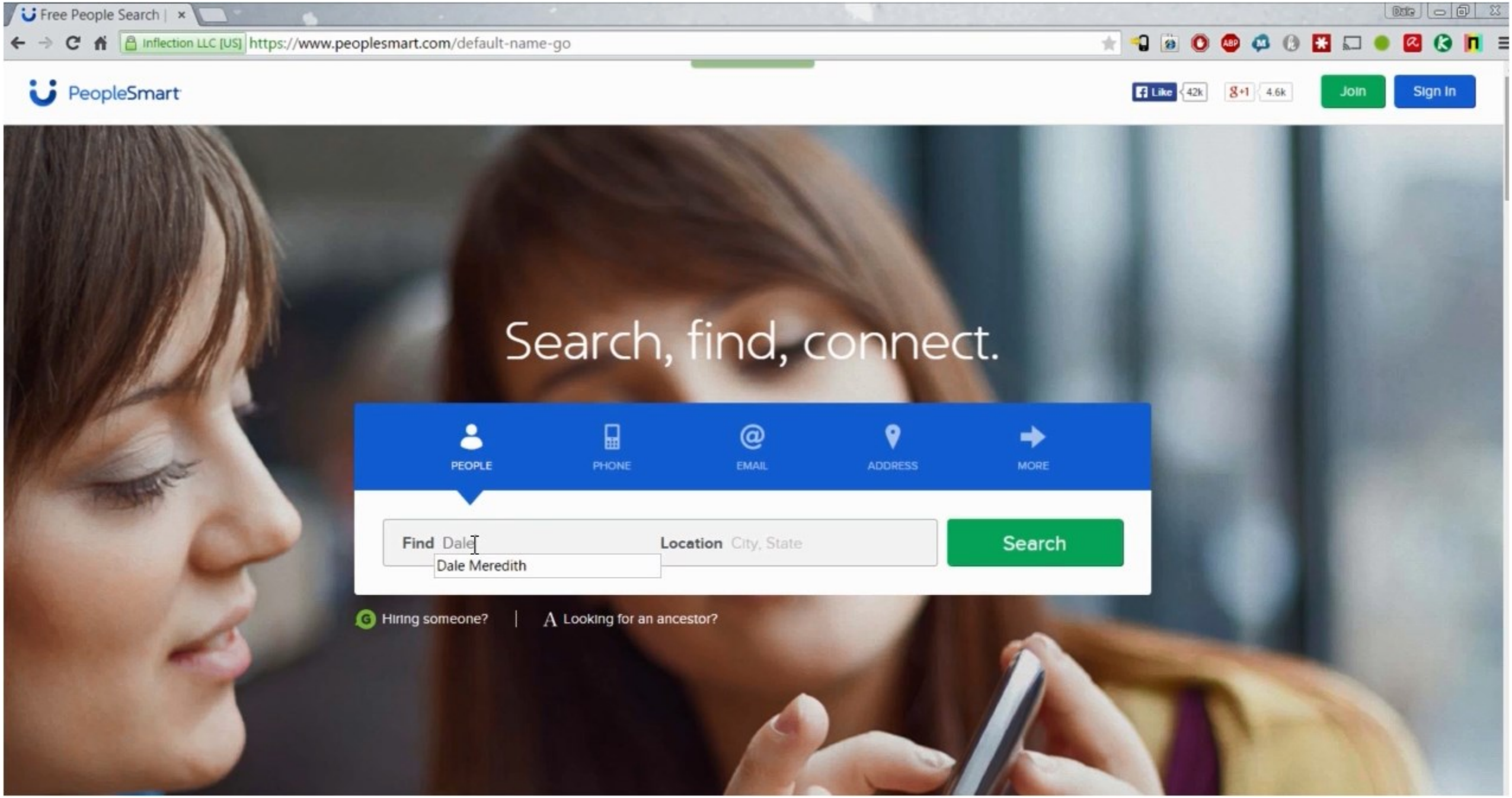
Scanning for data


Internet Archive: Wa
archive.org/web/
INTERNET ARCHIVE
WayBackMachine
http://
BROWSE HISTORY
456 billion web pages saved over time.
DONATE
Tools
Wayback Machine Availability API
Build your own tools.
WordPress Broken Link Checker
Banish broken links from your blog.
404 Handler for Webmasters
Subscription Service
Archive-It enables you to capture, manage and search collections of digital content without any technical expertise or hosting facilities. Visit Archive-It to build and browse the collections.
Save Page Now
http://
SAVE PAGE
Capture a web page as it appears now for use as a trusted citation in the future.
Only available for sites that allow crawlers.

People Search

Here's Looking at You Kid

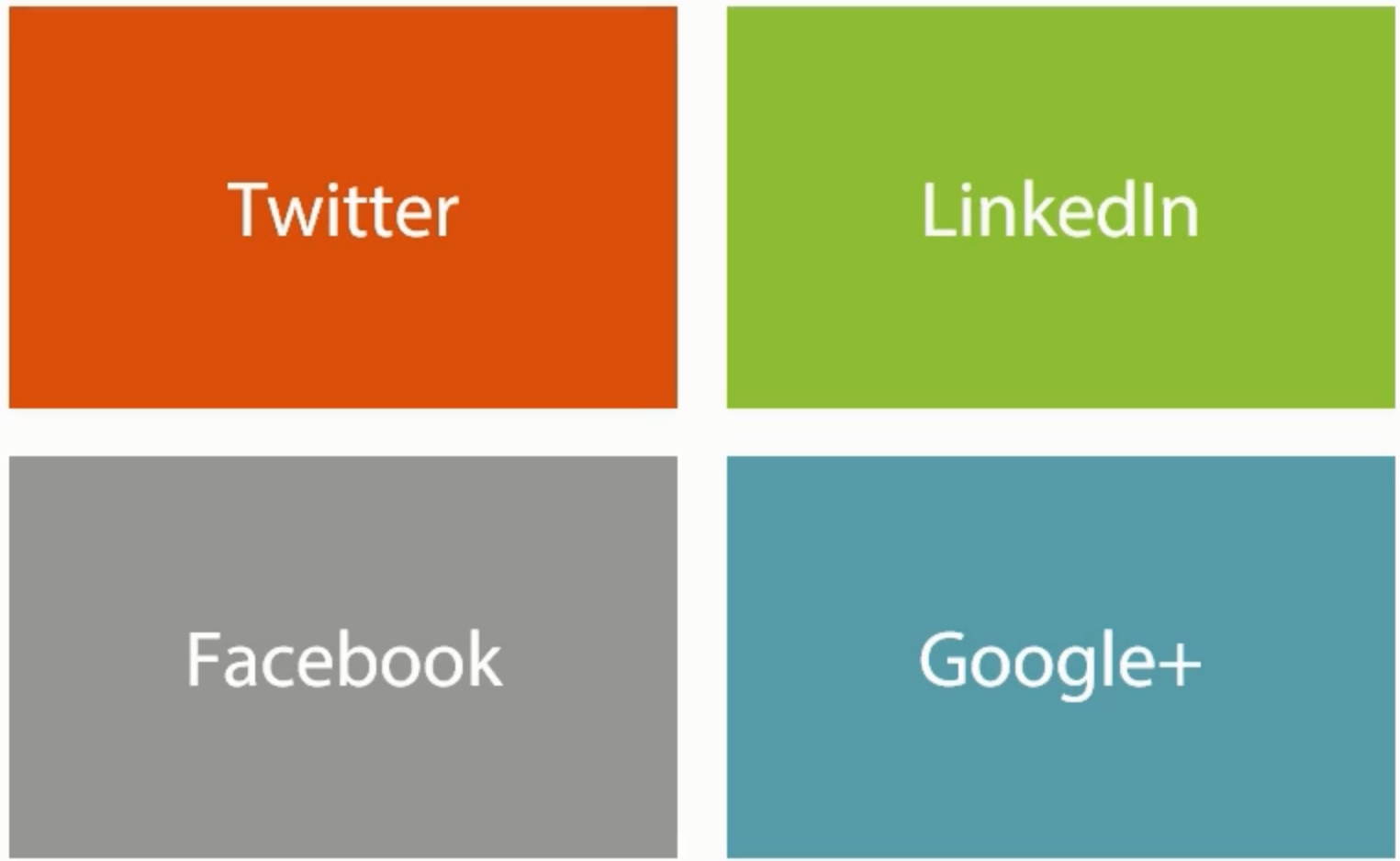
- What are you looking for?
- What personal info can you find


Free People Search
Inflection LLC [US] https://www.peoplesmart.com/default-name-go
PeopleSmart
Like 42k
+1 4.6k
Join
Sign In
Search, find, connect.
PEOPLE
PHONE
EMAIL
ADDRESS
MORE
Find Dale
Location City, State
Search
Dale Meredith
Hiring someone?
Looking for an ancestor?

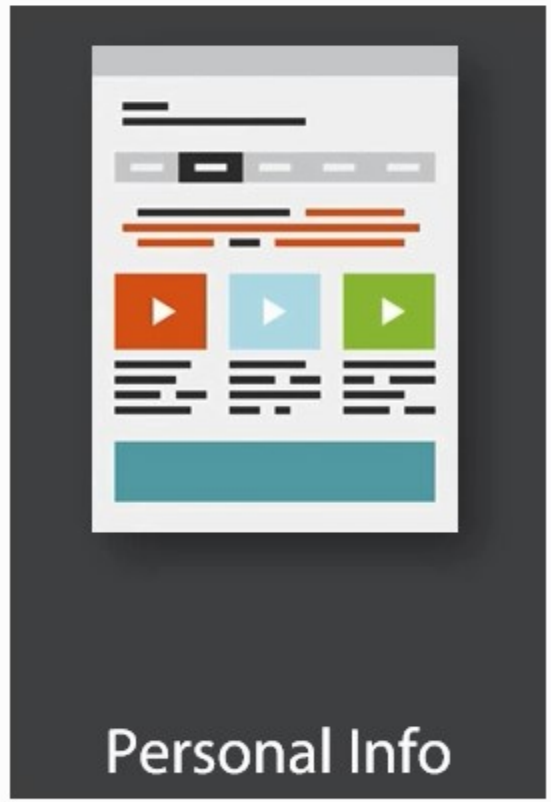
What More Can I Find?

- Social Sources
- Financial Sources
- Competitive Analysis
- Social Engineering
- Email

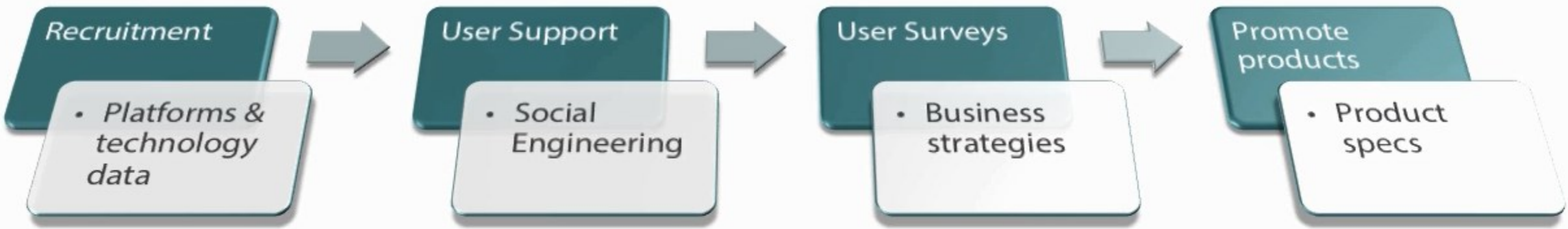
We're Sharing Too Much!



Methods of Data Mining Social Sites



Company: What Can Be Learned

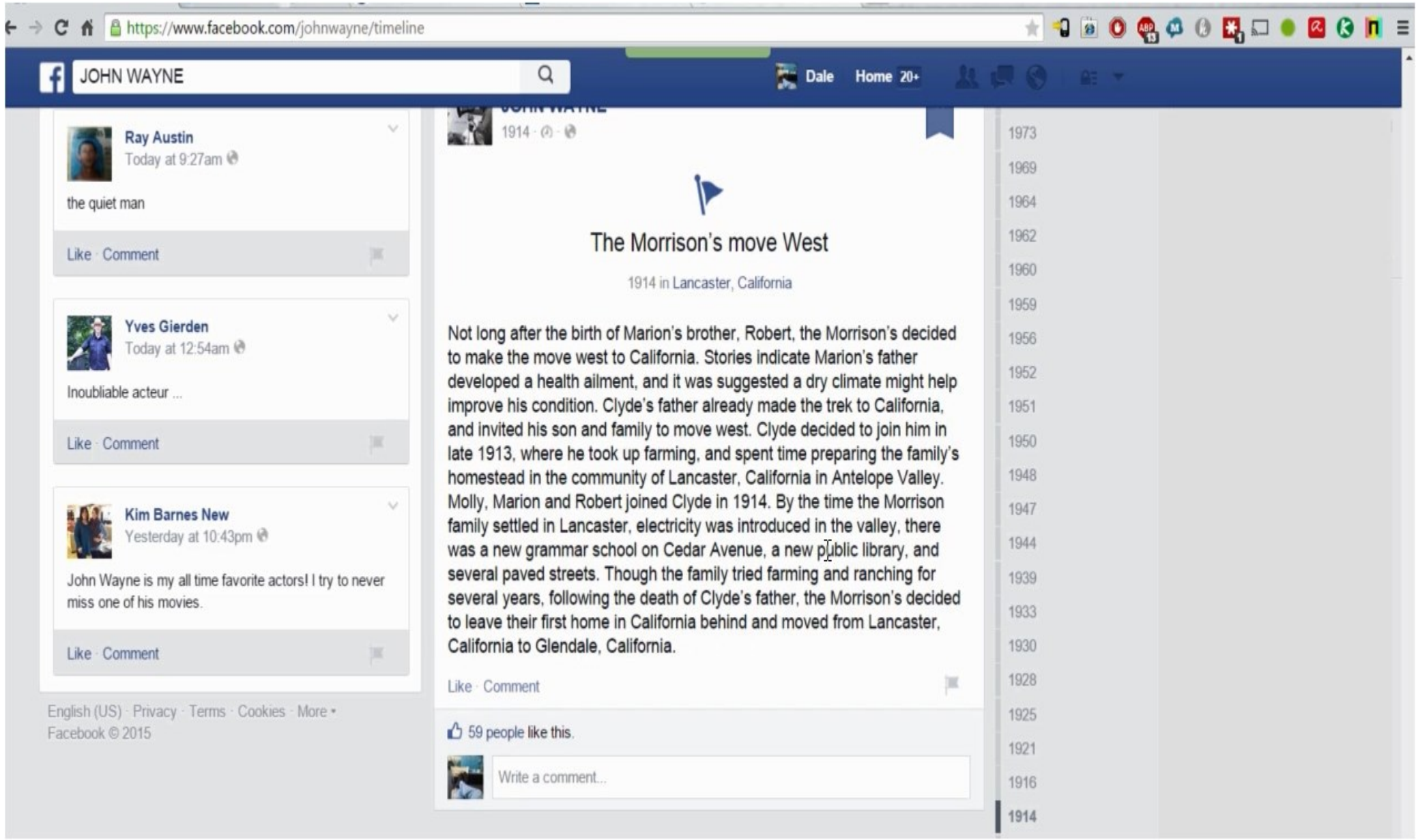


Let’s Look at Facebook

About a person

Photos

Likes


https://www.facebook.com/johnwayne/timeline
JOHN WAYNE
Dale
Home 20+
Ray Austin
Today at 9:27am
the quiet man
Like · Comment
Yves Gierden
Today at 12:54am
Inoubliable acteur ...
Like · Comment
Kim Barnes New
Yesterday at 10:43pm
John Wayne is my all time favorite actors! I try to never miss one of his movies.
Like · Comment
English (US) · Privacy · Terms · Cookies · More
Facebook © 2015
1914
The Morrison's move West
1914 in Lancaster, California
Not long after the birth of Marion's brother, Robert, the Morrison's decided to make the move west to California. Stories indicate Marion's father developed a health ailment, and it was suggested a dry climate might help improve his condition. Clyde's father already made the trek to California, and invited his son and family to move west. Clyde decided to join him in late 1913, where he took up farming, and spent time preparing the family's homestead in the community of Lancaster, California in Antelope Valley. Molly, Marion and Robert joined Clyde in 1914. By the time the Morrison family settled in Lancaster, electricity was introduced in the valley, there was a new grammar school on Cedar Avenue, a new public library, and several paved streets. Though the family tried farming and ranching for several years, following the death of Clyde's father, the Morrison's decided to leave their first home in California behind and moved from Lancaster, California to Glendale, California.
Like · Comment
59 people like this.
Write a comment...
1973
1969
1964
1962
1960
1959
1956
1952
1951
1950
1948
1947
1944
1939
1933
1930
1928
1925
1921
1916
1914

Looking at Linkedin

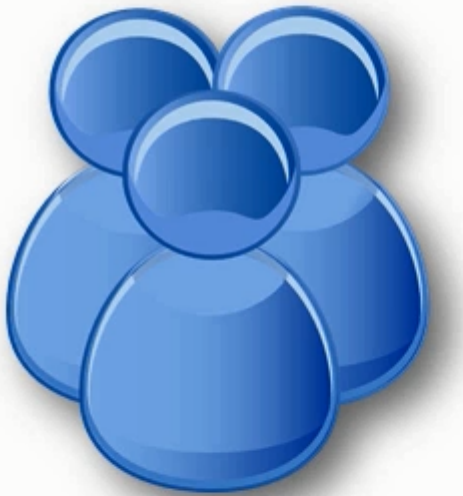
Past employment information

Current employment information

Education information

Contact Information

Human Hacking



- Exposing information
- Gain confidence of target

  Hcommerce:
  https://www.youtube.com/watch?v=yzU82Ul96pU
- Using emotions

https://www.youtube.com/watch?v=lc7scxvKQOo

How It's Done

Dumpster diving

Eavesdropping

Shoulder surfing

Impersonation

You've Got Mail = I've Got You!

- Track
  - When an email is read
  - If it's forwarded
  - Time spent reading
  - Links visited
  - Types of server used
  - OS the recipient is using

It's About the Header

Delivered-To: dale.meredith@gmail.com

Who the email went to

Received: by 10.64.230.234 with SMTP id tb10csp3086933iec;
Thu, 30 Apr 2015 07:14:50 -0700 (PDT)

Date & Time Received

X-Received: by 10.66.154.111 with SMTP id vn15mr8590499pab.108.1430403288686;
Thu, 30 Apr 2015 07:14:48 -0700 (PDT)

Where did it come from

Return-Path: <trc.1843@envfrm.rsys2.com>

Received: from om-thrifty.rsys3.com (om-thrifty.rsys3.com. [12.130.137.168])

Sender's IP Address

by mx.google.com with ESMTP id co1si3721858pad.63.2015.04.30.07.14.48
for <dale.meredith@gmail.com>;
Thu, 30 Apr 2015 07:14:48 -0700 (PDT)

Received-SPF: pass (google.com: domain of trc.1843@envfrm.rsys2.com designates 12.130.137.168 as permitted sender) client-ip=12.130.137.168;

Authentication-Results: mx.google.com;

Sender mail server

spf=pass (google.com: domain of trc.1843@envfrm.rsys2.com designates 12.130.137.168 as permitted sender) smtp.mail=trc.1843@envfrm.rsys2.com;
dkim=pass header.i=@email.thrifty.com;
dmarc=pass (p=NONE dis=NONE) header.from=email.thrifty.com

Original Sender's Email Server's Name

DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=thrifty; d=email.thrifty.com;
h=MIME-Version:Content-Type:Content-Transfer-Encoding:Date:To:From:Reply-To:Subject:Feedback-ID:List-Unsubscribe:Message-ID;
i=thriftycarrental@email.thrifty.com;
bh=qtw22FsUyXmGSoV2Mjp2Sib2LRs=;
b=YnEKd5gKDeTgCnATBObseRFVZUnOQvREUN8Ou/b/0pVn/gHRaSnjoD9jSA2i/VaB57X0kKrb6+P7
ZV4ovfMwstGUsewKmsAQqOPZ3aYEJHVaNzrM4z7N8YeuIS0YsYvkCs5u7n6P02pog5OL0djG6Pcg
ccU7yMqJzYgV3pRAKI4=

DKIM-Signature: v=1; a=rsa-sha1; c=re

Authentication system used (sender)

h=MIME-Version:Content-Type:Content-Transfer-Encoding:Date:To:From:Reply-To:Subject:Feedback-ID:List-Unsubscribe:Message-ID;
bh=qtw22FsUyXmGSoV2Mjp2Sib2LRs=;
b=sGSEoxHmf0cLvIw1p5E7rxvx5Xtig40e9hTCZNQgznJszqbJaukBdQ9Fj59gEp98DXxTtcUnZ4fA
INUa9cOZZsUhQW0KA5NktqZYLPE9oGNd7TiXoGQ1IgpAGngq85cLlnxAebsAySImx7g4v+RMPpcG
vXg6qxxMiLEWQA9JtBk=
DomainKey-Signature: a=rsa-sha1; c=nofws; q=dns; s=thrifty; d=email.thrifty.com;
b=FD1NQARjqKEWUoNKXgV6PijnBhgxL6Kze7kok7Y9knYU2pRbTjrYkc6Bf+E6wpE9B01dA9Bzjr+S

Several Tools to Help

Email Tracking Tools

- PoliteMail
- Email Lookup
- eMailTracker Pro
- DidTheyReadIt
- Read Notify
- WhoReadMe
- GetNotified
- G-Lock Analytics
- MSGTAG
- Trace Email

Reconnaissance via Google Hacking

Get Your Google On!

- Understanding Google
- The Google operators
- Advanced Google operators
- What can you find
- The Google Hacking Database (GHDB)

Advanced Google Operators

Know the Rules

- No space between the operator and the search term
- If a space exists in the search term, use " ". Or use a period .
- You can combine most operators

  - intitle:batman
  - note – searches are NOT case sensitive
  - intitle:"index of"
  - or intitle:index.of
  - intitle:"index of" private

Advanced Operators

- cache:
  Displays Google's cached version
- link:
  Show a list of web pages that have links to your target
- related:
  Similar web pages
- info:
  View information Google has on the target
- site:
  Limits results to just the domain listed
- allintitle:
  Limits results to those websites with ALL the search words in the title
- intitle:
  Limits results to documents that contain the search word in the title
- allinurl:
  Limits results to only those webpages with ALL search words in the URL
- inurl:
  Limits results to documents that contain the search word in the URL

webcache.googleuse ×

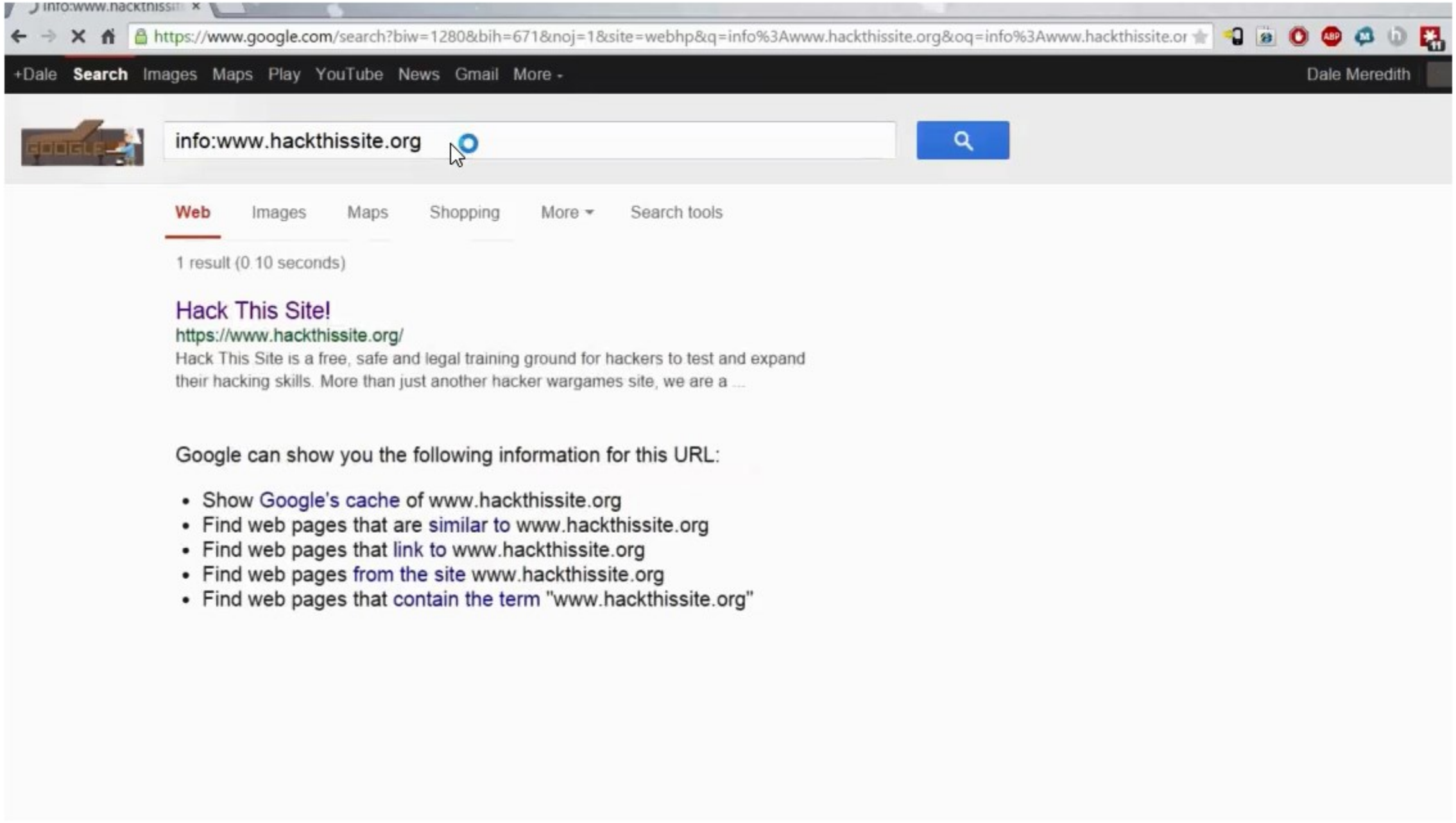
webcache.googleusercontent.com/search?biw=1280&bih=671&noj=1&site=webhp&source=hp&q=cache%3Amsn.com&oq=cache%3Amsn.c

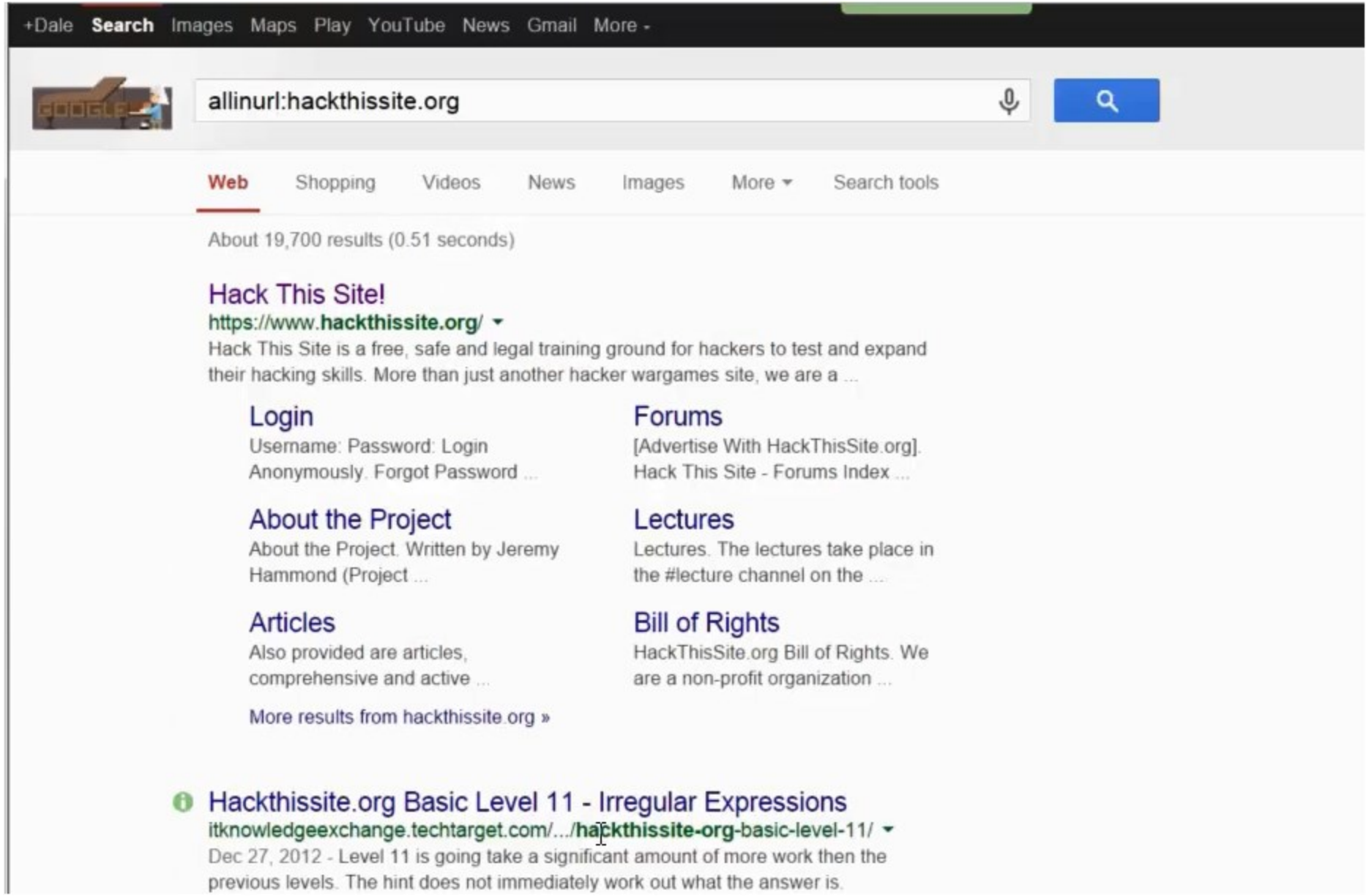
+Dale **Search** Images Maps Play YouTube News Gmail More ▾ Dale Me

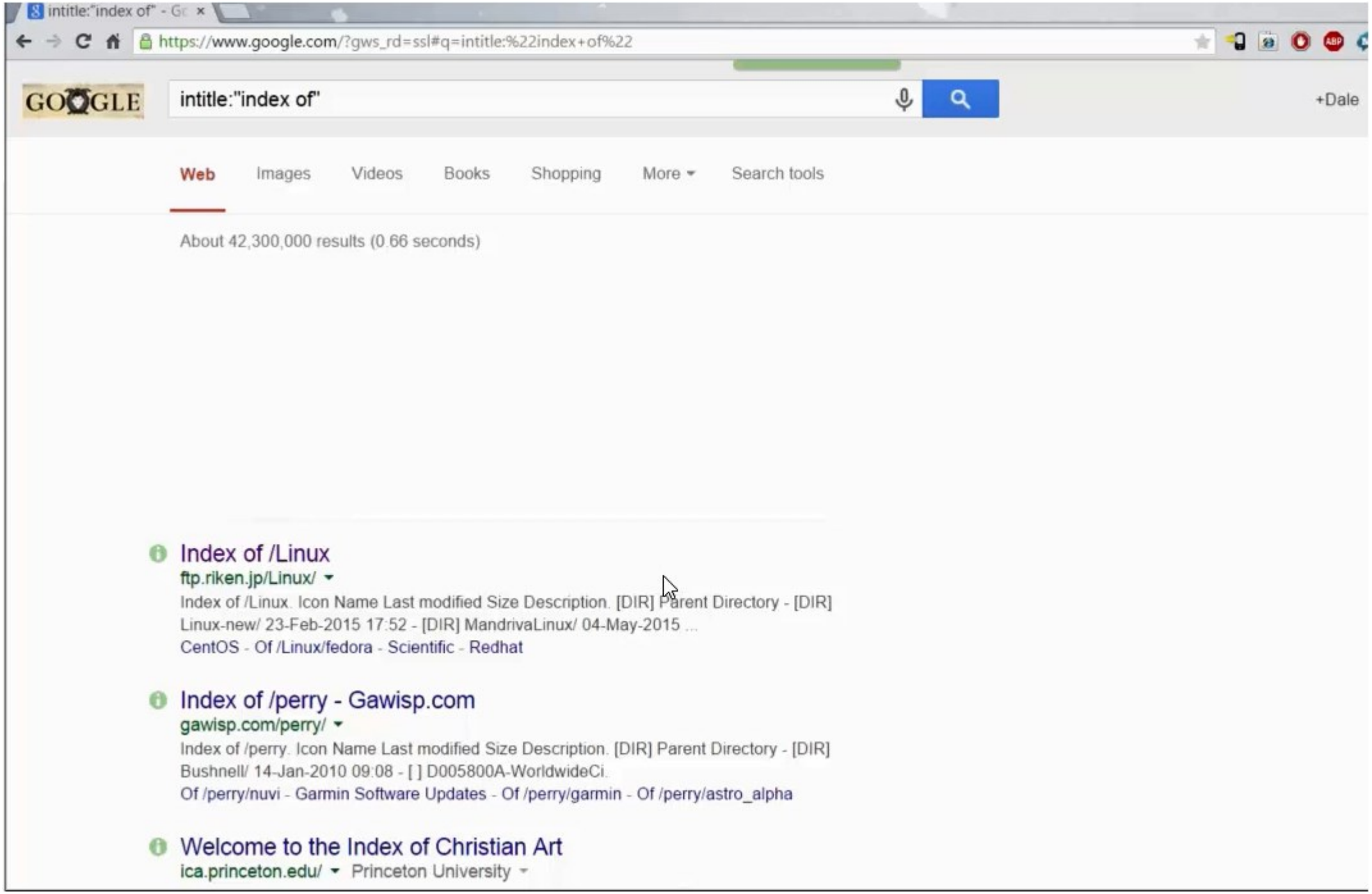
cache:msn.com

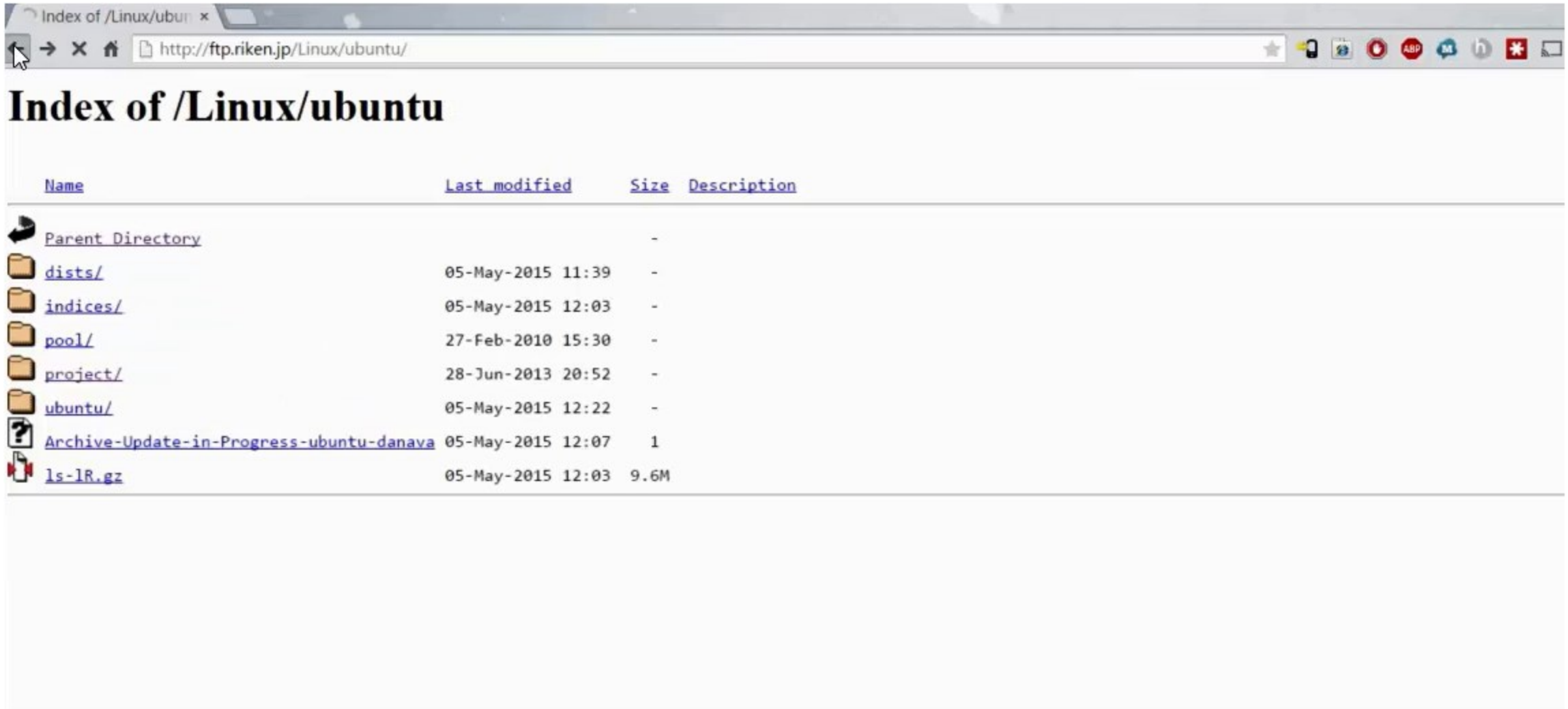
Google Search I'm Feeling Lucky

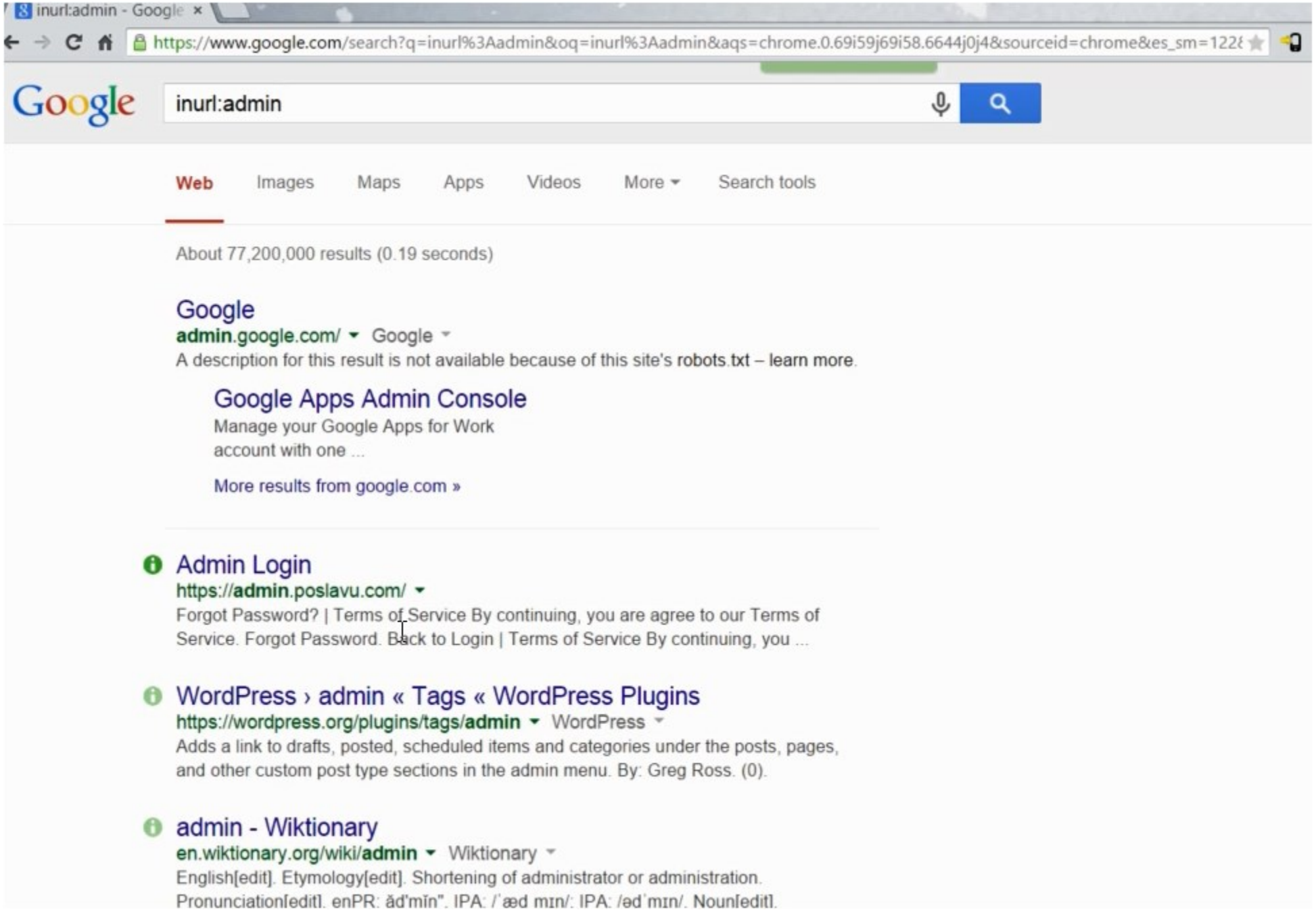
May the Fourth be with you


info:www.hackthissit
https://www.google.com/search?biw=1280&bih=671&noj=1&site=webhp&q=info%3Awww.hackthissite.org&oq=info%3Awww.hackthissite.or
+Dale Search Images Maps Play YouTube News Gmail More
Dale Meredith
info:www.hackthissite.org
Web Images Maps Shopping More Search tools
1 result (0.10 seconds)
Hack This Site!
https://www.hackthissite.org/
Hack This Site is a free, safe and legal training ground for hackers to test and expand their hacking skills. More than just another hacker wargames site, we are a ...
Google can show you the following information for this URL:
Show Google's cache of www.hackthissite.org
Find web pages that are similar to www.hackthissite.org
Find web pages that link to www.hackthissite.org
Find web pages from the site www.hackthissite.org
Find web pages that contain the term "www.hackthissite.org"


+Dale Search Images Maps Play YouTube News Gmail More
allinurl:hackthissite.org
Web Shopping Videos News Images More Search tools
About 19,700 results (0.51 seconds)
Hack This Site!
https://www.hackthissite.org/
Hack This Site is a free, safe and legal training ground for hackers to test and expand their hacking skills. More than just another hacker wargames site, we are a ...
Login
Username: Password: Login Anonymously. Forgot Password ...
Forums
[Advertise With HackThisSite.org]. Hack This Site - Forums Index ...
About the Project
About the Project. Written by Jeremy Hammond (Project ...
Lectures
Lectures. The lectures take place in the #lecture channel on the ...
Articles
Also provided are articles, comprehensive and active ...
Bill of Rights
HackThisSite.org Bill of Rights. We are a non-profit organization ...
More results from hackthissite.org »
Hackthissite.org Basic Level 11 - Irregular Expressions
itknowledgeexchange.techtarget.com/.../hackthissite-org-basic-level-11/
Dec 27, 2012 - Level 11 is going take a significant amount of more work then the previous levels. The hint does not immediately work out what the answer is.


intitle:"index of" - Gc
https://www.google.com/?gws_rd=ssl#q=intitle:%22index+of%22
GOOGLE
intitle:"index of"
+Dale
Web
Images
Videos
Books
Shopping
More
Search tools
About 42,300,000 results (0.66 seconds)
Index of /Linux
ftp.riken.jp/Linux/
Index of /Linux. Icon Name Last modified Size Description. [DIR] Parent Directory - [DIR] Linux-new/ 23-Feb-2015 17:52 - [DIR] MandrivaLinux/ 04-May-2015 ...
CentOS - Of /Linux/fedora - Scientific - Redhat
Index of /perry - Gawisp.com
gawisp.com/perry/
Index of /perry. Icon Name Last modified Size Description. [DIR] Parent Directory - [DIR] Bushnell/ 14-Jan-2010 09:08 - [ ] D005800A-WorldwideCi.
Of /perry/nuvi - Garmin Software Updates - Of /perry/garmin - Of /perry/astro_alpha
Welcome to the Index of Christian Art
ica.princeton.edu/ Princeton University


Index of /Linux/ubun
http://ftp.riken.jp/Linux/ubuntu/
Index of /Linux/ubuntu
Name
Last modified
Size
Description
Parent Directory -
dists/ 05-May-2015 11:39 -
indices/ 05-May-2015 12:03 -
pool/ 27-Feb-2010 15:30 -
project/ 28-Jun-2013 20:52 -
ubuntu/ 05-May-2015 12:22 -
Archive-Update-in-Progress-ubuntu-danava 05-May-2015 12:07 1
ls-lR.gz 05-May-2015 12:03 9.6M


inurl:admin - Google
https://www.google.com/search?q=inurl%3Aadmin&oq=inurl%3Aadmin&aqs=chrome.0.69i59j69i58.6644j0j4&sourceid=chrome&es_sm=122
Google
inurl:admin
Web
Images
Maps
Apps
Videos
More
Search tools
About 77,200,000 results (0.19 seconds)
Google
admin.google.com/ Google
A description for this result is not available because of this site's robots.txt – learn more.
Google Apps Admin Console
Manage your Google Apps for Work account with one ...
More results from google.com »
Admin Login
https://admin.poslavu.com/
Forgot Password? | Terms of Service By continuing, you are agree to our Terms of Service. Forgot Password. Back to Login | Terms of Service By continuing, you ...
WordPress › admin « Tags « WordPress Plugins
https://wordpress.org/plugins/tags/admin WordPress
Adds a link to drafts, posted, scheduled items and categories under the posts, pages, and other custom post type sections in the admin menu. By: Greg Ross. (0).
admin - Wiktionary
en.wiktionary.org/wiki/admin Wiktionary
English[edit]. Etymology[edit]. Shortening of administrator or administration. Pronunciation[edit]. enPR: ăd'mĭn", IPA: /ˈæd mɪn/; IPA: /ədˈmɪn/. Noun[edit].

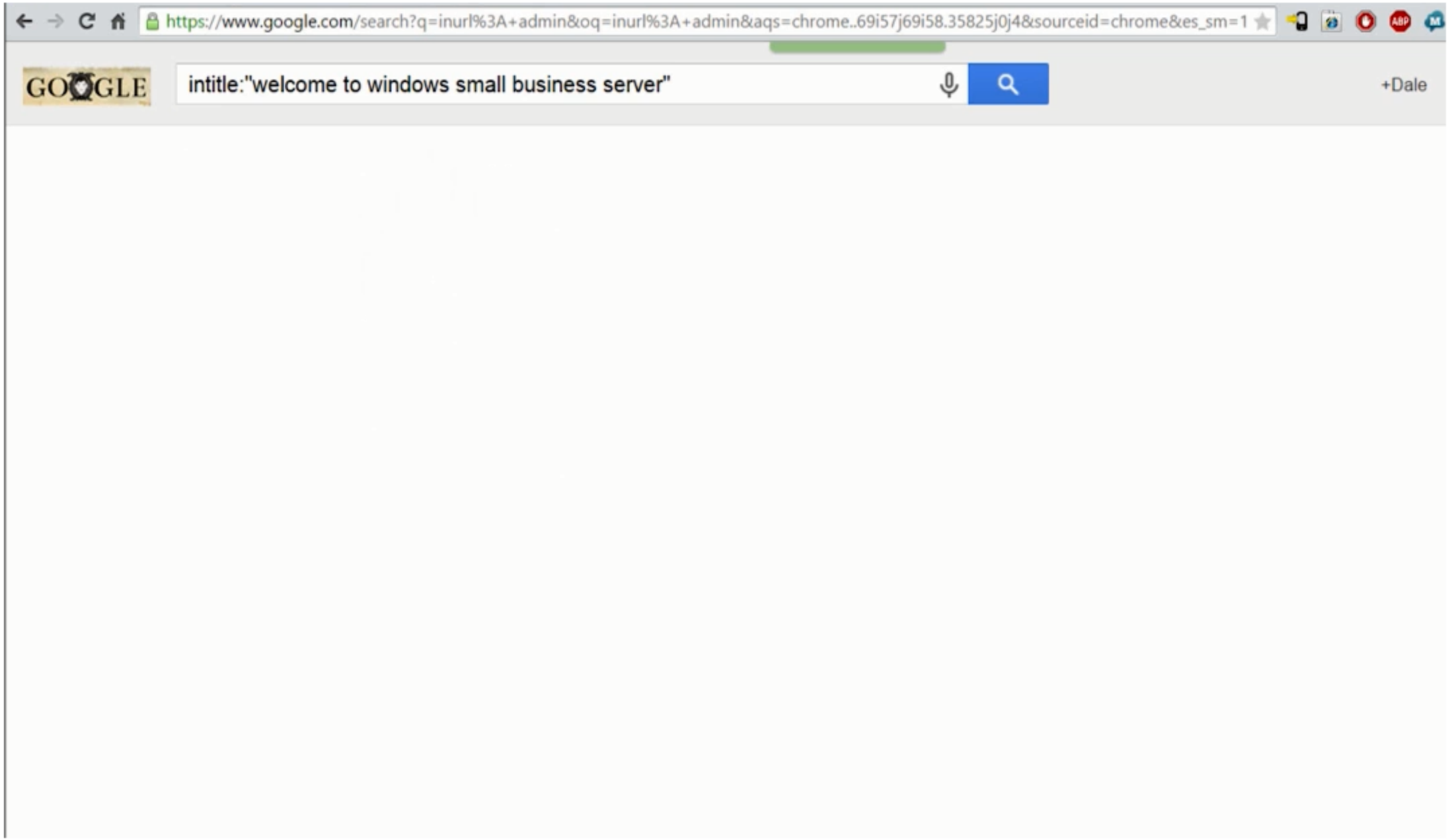
Understanding is Everything

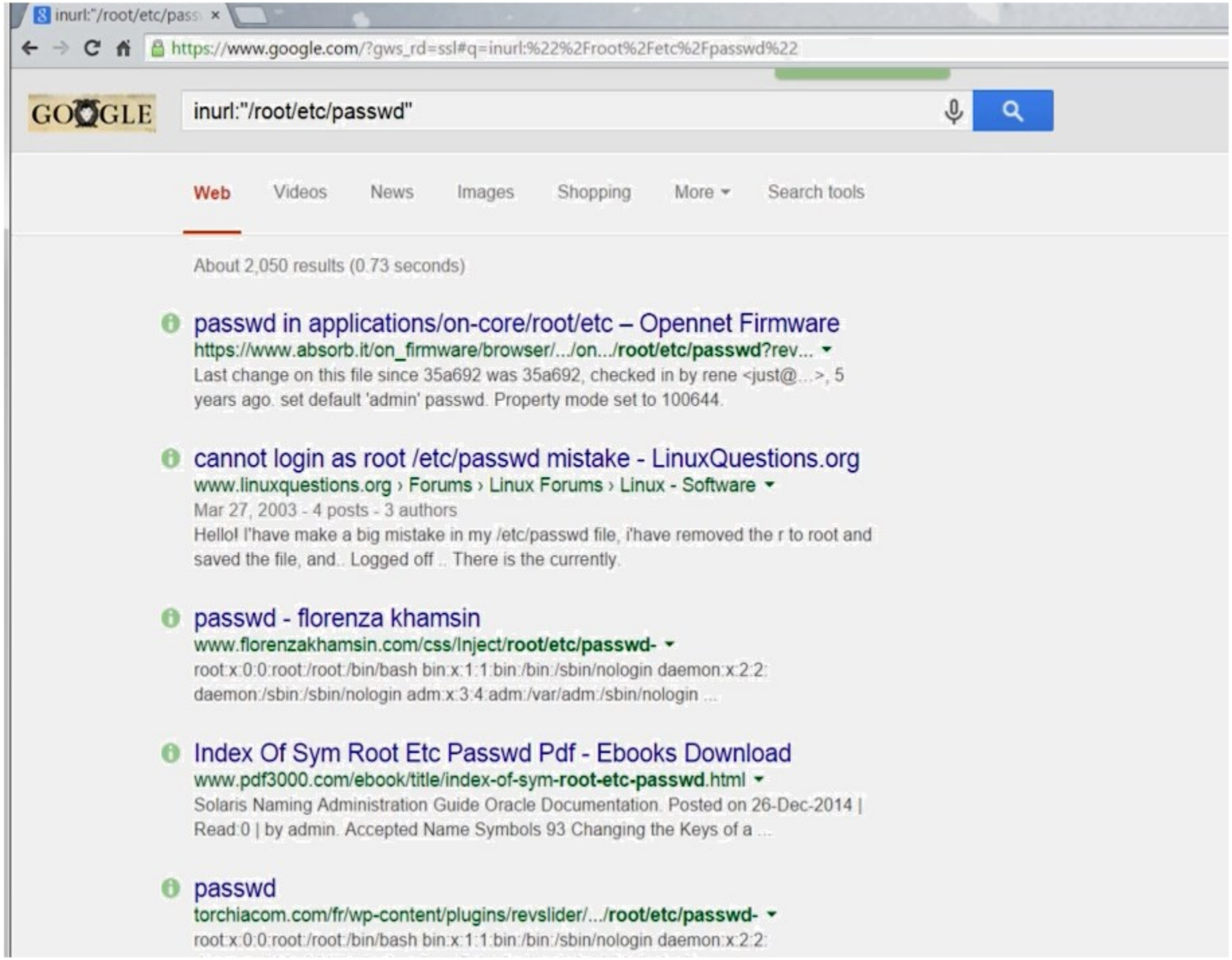
Devices and appliances

- Default settings
- Accessible via browser
- Application defaults
- Internet printing
- Internet cameras
- Server defaults

Think outside the box

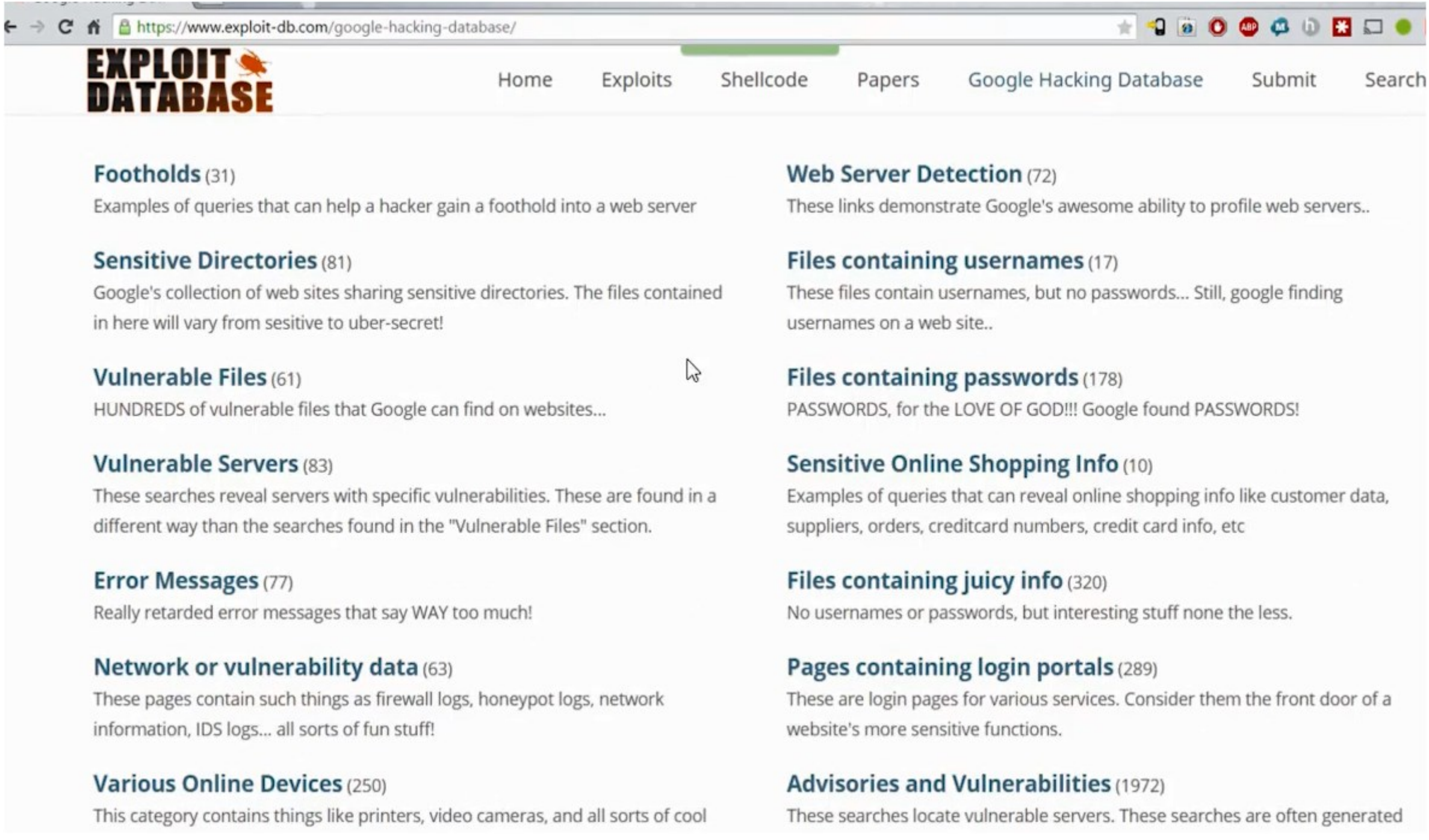
- Directories – intitle:index.of.
  Admin directories?
- Find specific files
  Logs / password files / by file extension
- Web servers
- Directory traversal
- Extension walking


https://www.google.com/search?q=inurl%3A+admin&oq=inurl%3A+admin&aqs=chrome..69i57j69i58.35825j0j4&sourceid=chrome&es_sm=1
GOOGLE
intitle:"welcome to windows small business server"
+Dale


inurl:"/root/etc/pass
https://www.google.com/?gws_rd=ssl#q=inurl:%22%2Froot%2Fetc%2Fpasswd%22
GOOGLE
inurl:"/root/etc/passwd"
Web
Videos
News
Images
Shopping
More
Search tools
About 2,050 results (0.73 seconds)
passwd in applications/on-core/root/etc – Opennet Firmware
https://www.absorb.it/on_firmware/browser/.../on.../root/etc/passwd?rev...
Last change on this file since 35a692 was 35a692, checked in by rene <just@...>, 5 years ago. set default 'admin' passwd. Property mode set to 100644.
cannot login as root /etc/passwd mistake - LinuxQuestions.org
www.linuxquestions.org › Forums › Linux Forums › Linux - Software
Mar 27, 2003 - 4 posts - 3 authors
Hello! I'have make a big mistake in my /etc/passwd file, i'have removed the r to root and saved the file, and.. Logged off .. There is the currently.
passwd - florenza khamsin
www.florenzakhamsin.com/css/Inject/root/etc/passwd-
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin ...
Index Of Sym Root Etc Passwd Pdf - Ebooks Download
www.pdf3000.com/ebook/title/index-of-sym-root-etc-passwd.html
Solaris Naming Administration Guide Oracle Documentation. Posted on 26-Dec-2014 | Read:0 | by admin. Accepted Name Symbols 93 Changing the Keys of a ...
passwd
torchiacom.com/fr/wp-content/plugins/revslider/.../root/etc/passwd-
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:

The Google Hacking Database

(GHDB)


https://www.exploit-db.com/google-hacking-database/
EXPLOIT DATABASE
Home
Exploits
Shellcode
Papers
Google Hacking Database
Submit
Search
Footholds (31)
Examples of queries that can help a hacker gain a foothold into a web server
Sensitive Directories (81)
Google's collection of web sites sharing sensitive directories. The files contained in here will vary from sesitive to uber-secret!
Vulnerable Files (61)
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 (77)
Really retarded error messages that say WAY too much!
Network or vulnerability data (63)
These pages contain such things as firewall logs, honeypot logs, network information, IDS logs... all sorts of fun stuff!
Various Online Devices (250)
This category contains things like printers, video cameras, and all sorts of cool
Web Server Detection (72)
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 (178)
PASSWORDS, for the LOVE OF GOD!!! Google found PASSWORDS!
Sensitive Online Shopping Info (10)
Examples of queries that can reveal online shopping info like customer data, suppliers, orders, creditcard numbers, credit card info, etc
Files containing juicy info (320)
No usernames or passwords, but interesting stuff none the less.
Pages containing login portals (289)
These are login pages for various services. Consider them the front door of a website's more sensitive functions.
Advisories and Vulnerabilities (1972)
These searches locate vulnerable servers. These searches are often generated

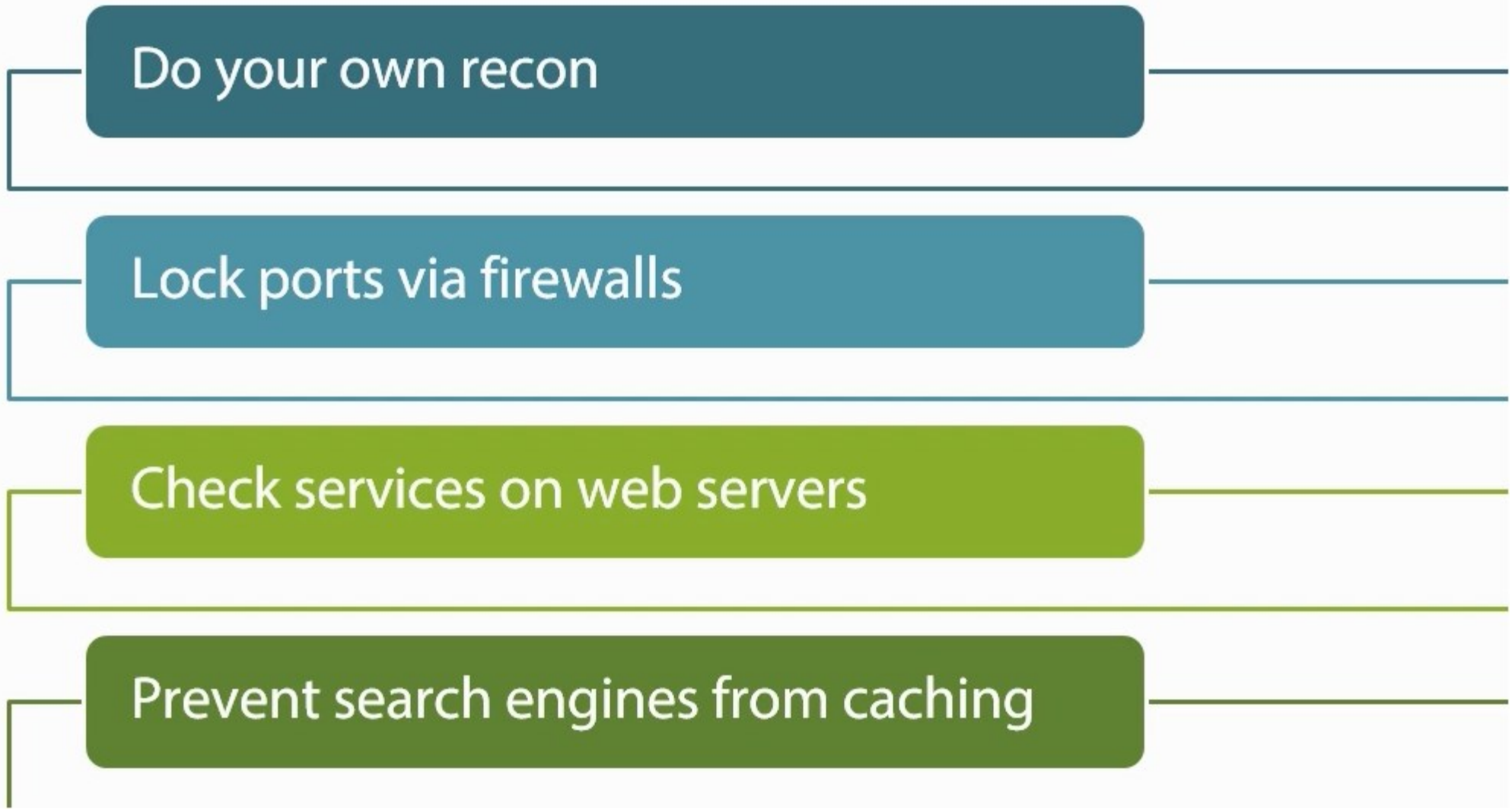
Shields! Red Alert!

- Countermeasures for Recon
- Recon Pen Test Workflow

Best Practices to Defend Against Recon

- Configure your routers
- Use an IDS
- Re-configure web servers
- Enforce security policies

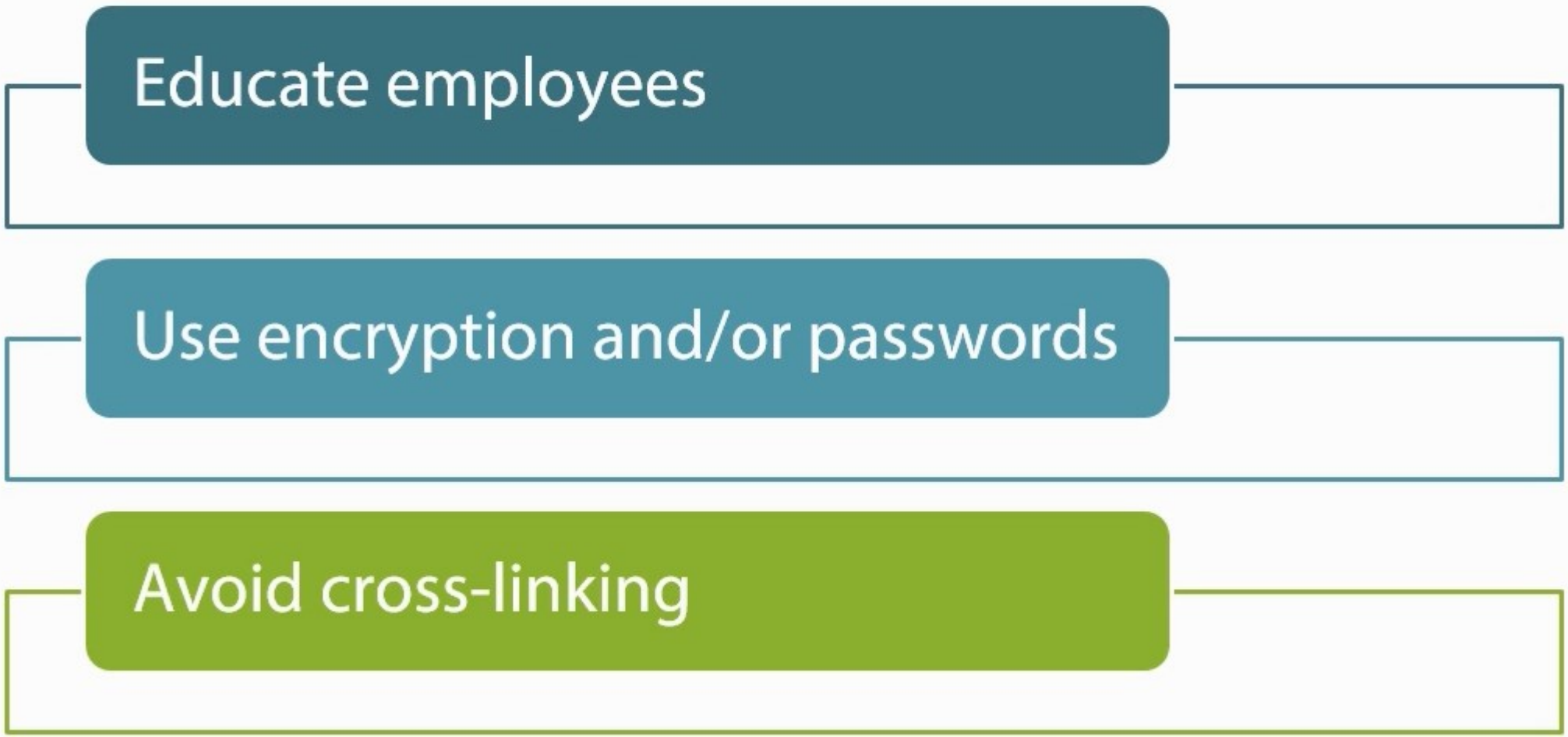
Best Practices to Defend Against Recon



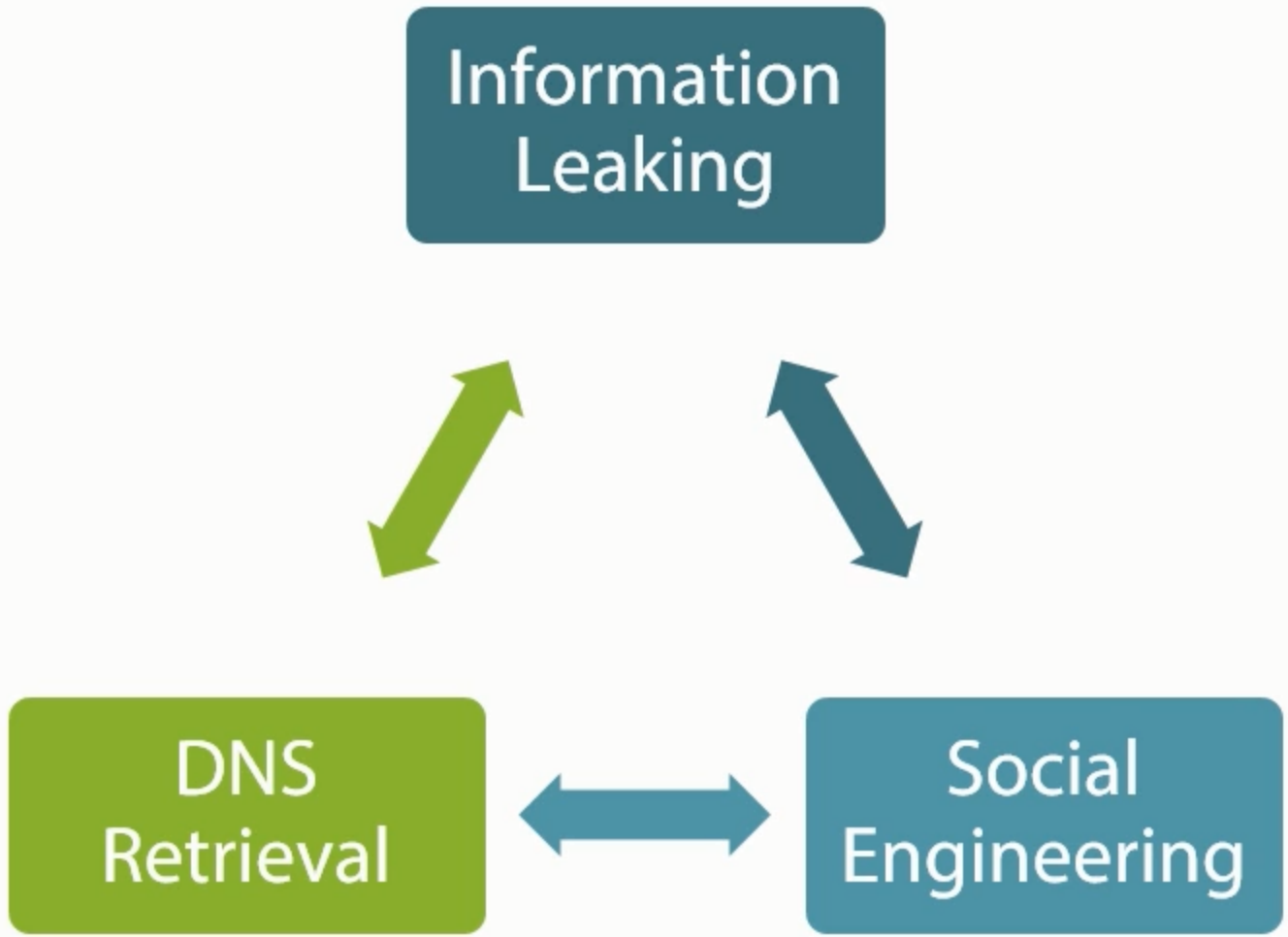
Best Practices to Defend Against Recon

- Disable directory listing
- Configure Internal vs External DNS
- Restrict inputs types (|,;<>)

Best Practices to Defend Against Recon



Recon Pen Testing



The Recon Workflow