

OSINT ONLINE 

Personal Information Security OSINT Online

Cynthia Hetherington
Hetheringtongroup.com



OSINT ONLINE 

Cynthia is a...


- Librarian
- Analyst
- Security Practitioner
- Investigator
- Author of:
 - Business Background Investigators
 - The Manual to Online Public Records
 - Web of Deceit
 - Data2Know.com: Internet & Online Intelligence Newsletter



OSINT ONLINE 


Cynthia tell them about the trends in...

- Geo location through
 - Maxmind.com
 - Regex.info/exif.cgi
- Facebook updates
 - Photos
 - Cell phones
 - 1 billion targets

OSINT ONLINE 

Online Investigative Scenarios

- **Security:** Watching protestors online.
- **Loss Prevention:** Locate goods in craigslist.com and intellectual property on Myspace.com
- **Competitive Intelligence:** Google.com - confidential <company name> filetype:ppt
- **Opposition Research:** Grab Form 990's on your non-profits
- **Asset Forfeiture:** Getting divorced? Funding Terror? Hunting fraudsters?
- **Due Diligence:** Conduct due diligence quickly and cheaply.
- **Criminal Actions:** Trace cellphone, PO Box & elusive email.

OSINT ONLINE 

The law

- **Legal issues are best covered with your legal counsel.**
- The law varies depending on your purpose:
 - Hiring
 - Investigations
 - Vetting
 - In Germany an employer can look at LinkedIn, but not Facebook for hiring.
- There really are no definitive rules on investigating in Social Networks anywhere on the planet.

OSINT ONLINE 


Open Sources

OSINT ONLINE 


Official Public Records

- Litigation history
- Media history
- Business & personal affiliations
- SEC filings
- Corporate records
- Regulatory history
- Property records
- Academic records
- Financial records
- Vendor & supplier relationships
- Board appointments
- Liens, Judgments & UCCs
- Subsidiaries & franchises
- Physical assets
- Intellectual property
- Political & charitable causes

Depending on the country public records do exist but are not as readily available or legal to obtain.


OSINT ONLINE 

Who's out there?



OSINT ONLINE


Who's Out There?



A screenshot of a Microsoft Internet Explorer browser window showing a Google Images search for "police officer". The search results display a grid of images of police officers in various uniforms and settings. The browser's address bar shows the search URL.

OSINT ONLINE

Essex Police Officers



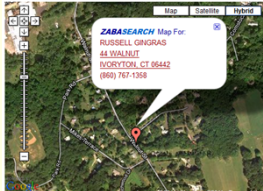
- Officer **Russell Gingras**, Resident Trooper **John Mesham**, Corporal **Marc Piscioti**, Police Officer Trainee **Salvatore Bevilacqua**, and Corporal **Patrick Bowers**
- Source: <http://www.essexct.gov/images/police/induction.html>

OSINT ONLINE

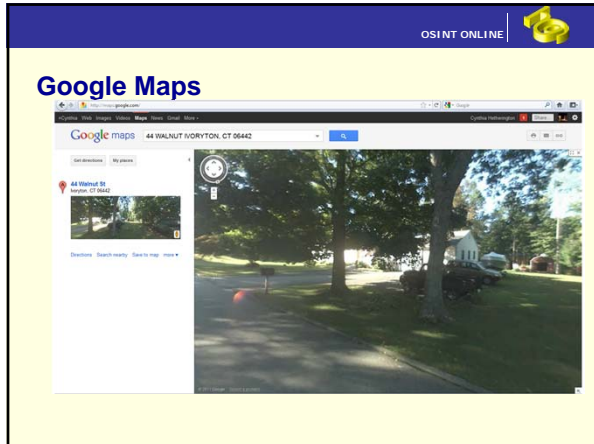
Public: Zabasearch

ZABASEARCH Maps

RUSSELL GINGRAS Get the Dirt Check for Email Address
44 WALNUT HORTON, CT 06442 (860) 767-1368 Confirm Current Phone & Address
Background Check on RUSSELL GINGRAS



A screenshot of the Zabasearch website. It displays a map of Horton, CT, with a callout box for "RUSSELL GINGRAS" at "44 WALNUT HORTON, CT 06442" with phone number "(860) 767-1368". Above the map, there are links for "Get the Dirt", "Check for Email Address", "Confirm Current Phone & Address", and "Background Check on RUSSELL GINGRAS".



Pseudo-Public Records

- Telephones
- Magazine subscriptions
- Voter registration
- Warranty cards
- Vehicles
- Credit cards
- Lawsuits
- Cell phones
- Judgments
- Photographs
- Liens/Loans
- Any open source, such as Web sites or media captures


Can we look that up?

OSINT ONLINE 


What can we look at in open source?




The screenshot shows the OccupyWallStreet website with a navigation bar and a main article. The article title is "While We Watch: A New Documentary on #OWS Media. Streaming Live, April 26th, 8PM". Below the title is a video player with the hashtag #whilewewatch. The website header includes "OccupyWallStreet" and the tagline "The revolution continues worldwide!".

OSINT ONLINE 

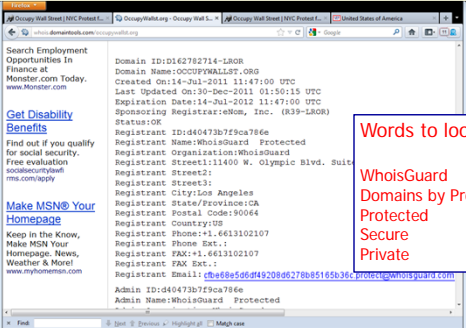
Domaintools.com



The screenshot shows the Domaintools.com website. The main heading is "We know it all. You can too." Below this are navigation tabs: HOME, RESEARCH, MONITOR, BUY DOMAINS, LEARN, and OPEN AN ACCOUNT. A search bar is visible with the text "domaintools.com". The page highlights "DomainTools has the most comprehensive collection of domain name ownership records in the world!" and lists services like "Whois Lookup", "Reverse Whois", and "Domain Availability".

OSINT ONLINE 

Proxy'd Domain



The screenshot shows a WhoisGuard proxy domain lookup for the domain OCCUPYWALLSTREET.ORG. The results include: Domain ID: D162782714-LROR, Domain Name: OCCUPYWALLSTREET.ORG, Created On: 14-Jul-2011 11:47:00 UTC, Last Updated On: 30-Dec-2011 01:50:15 UTC, Expiration Date: 14-Jul-2012 11:47:00 UTC, Sponsoring Registrar: eNom, Inc. (R39-LAOR), Status: OK, Registrant ID: d60473b7f9ca786e, Registrant Name: WhoisGuard - Protected, Registrant Organization: WhoisGuard, Registrant Street: 11400 W. Olympic Blvd, Suite 100, Registrant City: Los Angeles, Registrant State/Province: CA, Registrant Postal Code: 90064, Registrant Country: US, Registrant Phone: +1.6613102107, Registrant Phone Ext.: , Registrant FAX: +1.6613102107, Registrant FAX Ext.: , Registrant Email: cbe68e5d6d49208d6278685165b36c@protectmywhomsguard.com, Admin ID: d60473b7f9ca786e, Admin Name: WhoisGuard - Protected.

Words to look for:
WhoisGuard
Domains by Proxy
Protected
Secure
Private

OSINT ONLINE

Scroll up and look for the tabs

Whois Record | Site Profile | Registration | **Server Stats** | My Whois

Reverse Whois: "WhoisGuard" was found in about 1,496,274 other domains
NS History: 2 changes on 3 unique name servers over 1 year.
IP History: 4 changes on 3 unique IP addresses over 1 year.
Whois History: 123 records have been archived since 2011-07-19
Reverse IP: 3 other sites hosted on this server.

Log In or Create a FREE account to start monitoring

WHOIS FOR WINDOWS FREE LOOKUP TOOL DomainTools

Get it NOW

Select Server Stats Then click the IP Address

Server Type: nginx/0.7.67
IP Address: **173.231.134.109** | Reverse-IP | Ping | DNS Lookup | Traceroute
ASN: AS29791
IP Location: 🇺🇸 - New York - New York - Voxel Dot Net Inc
Response Code: 200
Domain Status: Registered And Active Website

IP Information for 173.231.134.109

IP Location: 🇺🇸 United States New York Voxel Dot Net Inc.
ASN: AS29791
IP Address: 173.231.134.109 | P | D | T
Reverse IP: 4 websites use this address. (examples: donnellyweb.com plibrotest.org natzotest.org occupywallst.org)

NetRange: 173.231.128.0 - 173.231.191.255
CIDR: 173.231.128.0/18
OriginAs: AS29791
Netname: VOXEL-ISP-9
NetHandle: NET-173-231-128-0-1
Parent: NET-173-0-0-0
NetType: Direct Allocation
Comment: Re-assignment data at whois.voxel.net:4321.
Comment: Abuse complaints to abuse@voxel.net.
RegDate: 2010-03-22
Updated: 2012-03-02
Ref: http://whois.arin.net/rest/net/NET-173-231-128-0-1

OrgName: Voxel Dot Net, Inc.
OrgId: VDM-1
Address: 29 Broadway
Address: 30th Floor
City: New York
StateProv: NY
PostalCode: 10006
Country: US
RegDate: 2000-05-04
Updated: 2011-09-11

Leads!

OSINT ONLINE

Check out Donnellyweb.com


Registrant:
donnelly, Sean
1 E 35th Street
Apt 5A
Manhattan, NY 10016
US

Domain Name: DONNELLYWEB.COM

Administrative Contact, Technical Contact:
donnelly, Sean | seanbeachff@hotmail.com
1 E 35th Street
Apt 5A
Manhattan, NY 10016
US
2122138004 fax: 509-471-7617

OSINT ONLINE 

Social Networks

OSINT ONLINE 

Public Information

- Business profile
- Academic history
- Business connections
- Personal affiliations
- Hobbies
- Sports teams
- Opinions
- Work schedule
- Height, weight, gender
- Travel schedule
- Caffeine or no?
- Intellectual property
- Political & charitable causes
- Photos of yourself, your family and friends
- Videos inside facilities
- Where you are and what you are doing every minute of the day!
- Updates on family events
- Drug habits
- Illnesses
- Sexual preferences

OSINT ONLINE 

No one seems concerned

- Children are posting
 - Predators
- Business Professionals are posting
 - Competitors and Bosses are watching
- Everyone's posting
 - Reality TV meet Reality Blogger

Some examples of over exposure!

OSINT ONLINE 

The Weakest Link



- **Vincent_** "Make everyday the best day of your entire life!!!!"
- Male 24 years old
- Clifton, NEW JERSEY
Works for Large German Manufacturing Company
- Former Marine

Are those network schematics?

OSINT ONLINE 

Hello?



- **Employed by:**
- Large German Manufacturing Company
Passaic, NJ, US
Computer Programmer
01/04....CURRENT


CENSORED

OSINT ONLINE 

Meet Peter from Happy Family Company








- Male 22 years old
Los Angeles, CA
- **HFC Feature Animation**
- Burbank, CA, US
- Programmer, Editorial/Post-Production Technical Department
- **Lawrence Livermore National Laboratory**
- Livermore, CA, US
- Computer Programmer Intern, Defense Nuclear Technology
- **Peter's packing!**

OSINT ONLINE 

Some others?

- George Sodini
- Nidal Hasan
- Jared Loughner
- James Holmes
- Anders Behring Breivik




OSINT ONLINE 

Social Network Searches

OSINT ONLINE 

Web 2.0 & Social Network Sites


- Facebook.com
- Myspace.com
- Orkut.com
- Technorati.com
- Icerocket.com
- Ebay.com
- Flickr.com
- Spokeo.com
- Match.com
- Linkedin.com
- Lococitato.com
- Yoname.com
- Youtube.com
- Twitter.com
- Friendwise.com
- Blogs.com
- Cuil.com
- Alt.com
- Bebo.com
- Imeem.com
- Kiwipulse.co.nz
- Hi5.com
- Feedfinder.com
- Hives.com
- Delver.com
- Spoke.com

OSINT ONLINE 

LinkedIn.com

Tips:

1. Read everything.
2. Find out who he recommends.
3. Find out who recommended him.
4. Look for inconsistencies with what you already know.
5. Look for leads to other professionals also searched on.



The screenshot shows a web browser window displaying a LinkedIn profile for Grafton deButts. The profile includes a header with the name and a profile picture, followed by a current position: 'Membership Sales Manager at Loudoun County Chamber of Commerce'. Below this, there is a 'Current' section with a bullet point for the same role. The 'Past' section lists several previous roles, including 'Industry Relations Manager at Loudoun Chamber & Visitors Association', 'PR Intern (St. Joseph) at Washington Redskins', and 'National Marketing Dept. Intern at Fairfax County Economic Development'. The browser's address bar shows the URL 'http://www.linkedin.com/in/graftondebutts'.

OSINT ONLINE 

Facebook.com

- Tips:

1. Do not assume that everyone's Facebook page is secured.
2. Use the lists of friends, which are available in most cases to credit associates lists.
3. Check out the networks they are a member of!
4. Write their name after the URL as follows
[Facebook.com/fullname](https://www.facebook.com/fullname)



The screenshot shows a Facebook profile page for Michaela Sabala. The profile includes a cover photo, a profile picture, and a bio. The bio mentions 'I am a professional model and a fitness enthusiast. I love to travel and explore new places. I am currently based in Washington, DC. I am also a member of the National Model & Fitness Association.' The browser's address bar shows the URL 'https://www.facebook.com/michaelasabala'.

OSINT ONLINE 

Twitter.com

- Search.twitter.com
 - Start with the basic search. Try the person's name, cell phone number, or user handle if you have it. If not, then use the advanced search feature and try searching places "Near this place" option.
 - Don't understand what they are saying? Visit <http://search.twitter.com/operators>

