OSINT

How to freak out friends and family with your strange google-fu addiction

Who Am I?

Anthony Tippy - @Tibbbbz

#Infosec Student | Amateur Security Researcher | Audio/Visual Tech | DIY | sloth enthusiast | Breaker of Things | Shitposter | reason we don't have nice things

Disclaimer

Don’t be a **dick**. As with many infosec tools, they can be used for good *and* bad. Be the ***good guy***. If you’re using this to stalk, abuse, or intimidate. You’re doing it WRONG.

OSINT Challenge #1 - Easy

Find this location

https://twitter.com/Tibbbbz

Source: @Maxwellcrafter

Define- OSINT

“Open-source intelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources” - Wikipedia

OSINT Types

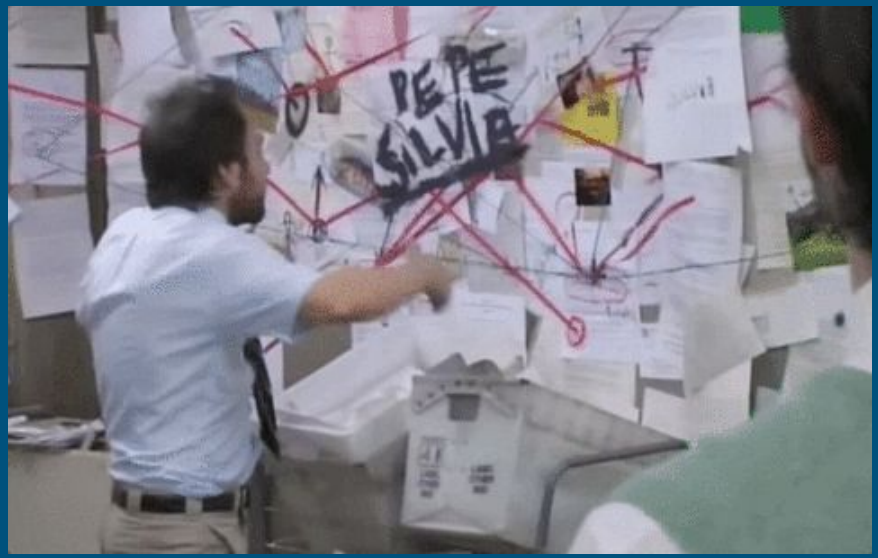
- Web Searches
- Shodan
- Library books/ records
- Maps
- Dating sites
- Phone Numbers
- Videos/Photos
- Malware
- Geolocation

What can you do with it?

1. People search (Who is this? Phone number?
2. Employer / employee search
3. Cyber threat investigation (IP addresses, similar incidents...etc)
4. Location search (Where was this?)
5. Data leaks/exposure (Trello boards, AWS buckets...etc)
6. Social engineering leads

OSINT Process

1. What am I looking for?
2. What is my main research goal?
3. What or who is my target?
4. How am I going to conduct my research?
5. Scope of research?
6. Length of project
7. Consistently look to prove theories



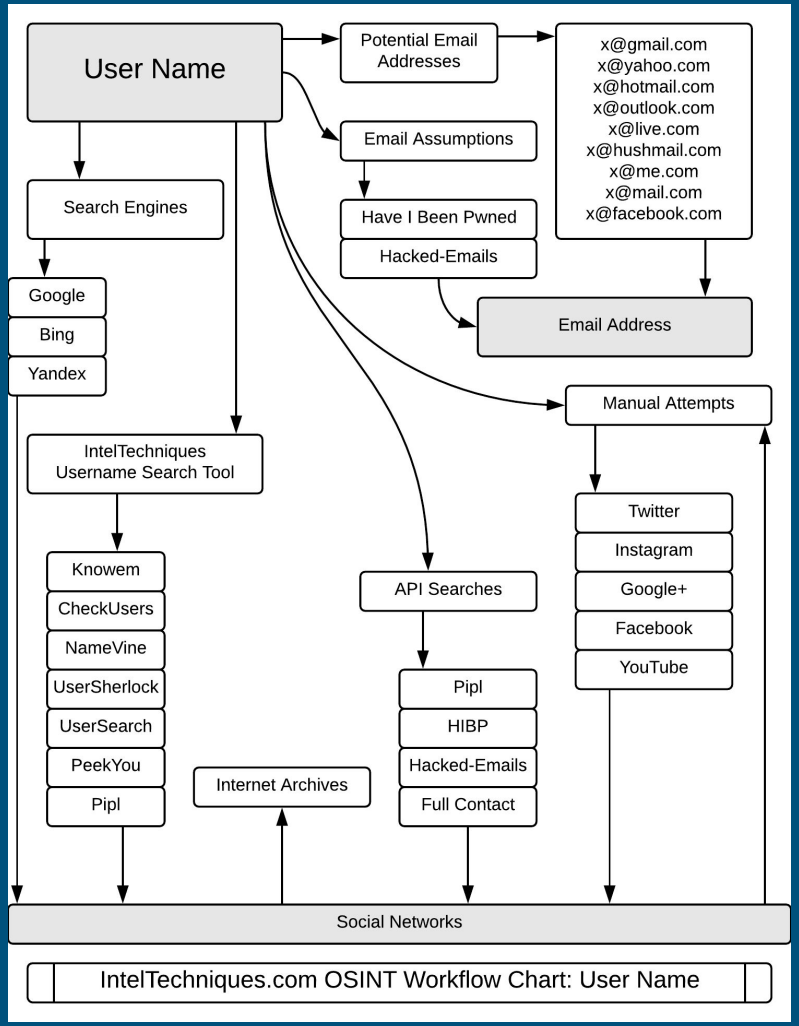
“The Google”

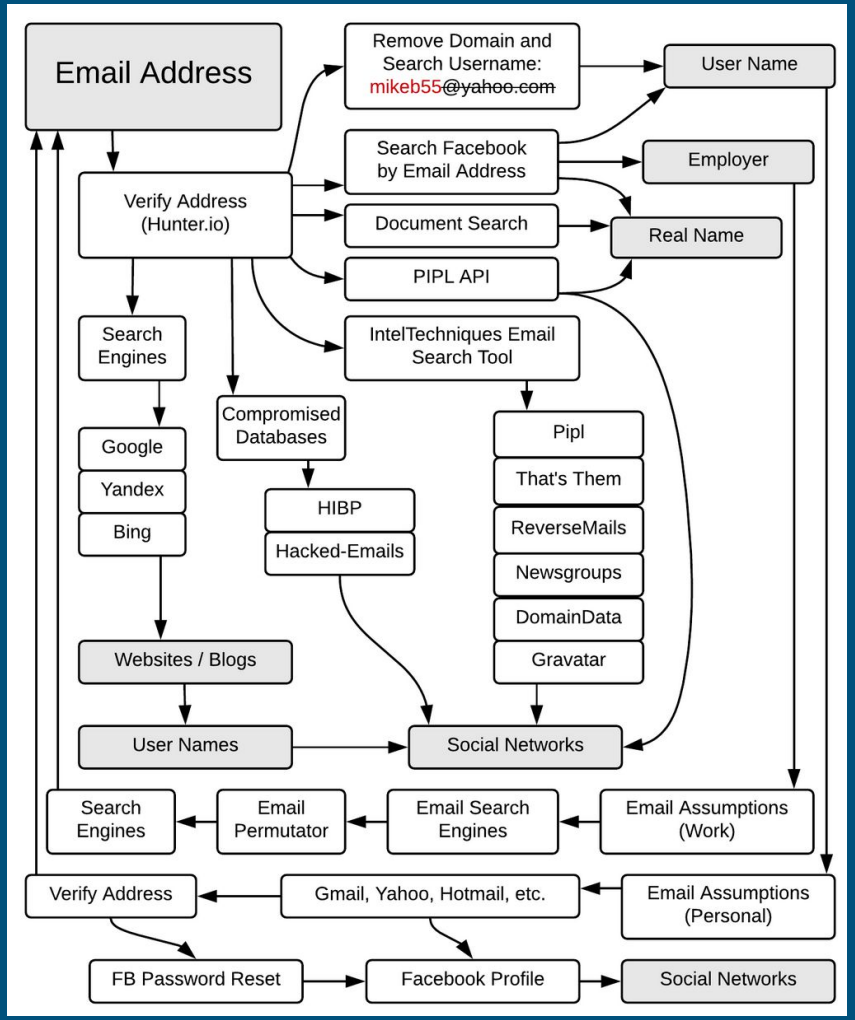
1. Other search engines
   a. Bing
   b. Yandex
   c. DuckDuckGo
   d. Baidu
2. Start with the basics
   a. Name?
   b. Phone Number?
   c. Username?
   d. Email
3. Google Advanced Search
4. Page 2

Pivot Points

- Pivot between data points

1. HackerBoi@gmail.com
2. Hacker Boi → Social Media
3. HackerBoi → Yahoo, apple...etc
4. HackerBoi → Phone #


User Name
Potential Email Addresses
x@gmail.com
x@yahoo.com
x@hotmail.com
x@outlook.com
x@live.com
x@hushmail.com
x@me.com
x@mail.com
x@facebook.com
Email Assumptions
Have I Been Pwned
Hacked-Emails
Search Engines
Google
Bing
Yandex
Email Address
Manual Attempts
IntelTechniques Username Search Tool
Twitter
Instagram
Google+
Facebook
YouTube
Knowem
CheckUsers
NameVine
UserSherlock
UserSearch
PeekYou
Pipl
API Searches
Pipl
HIBP
Hacked-Emails
Full Contact
Internet Archives
Social Networks
IntelTechniques.com OSINT Workflow Chart: User Name


Email Address
Remove Domain and Search Username: mikeb55@yahoo.com
User Name
Search Facebook by Email Address
Employer
Verify Address (Hunter.io)
Document Search
Real Name
PIPL API
Search Engines
IntelTechniques Email Search Tool
Compromised Databases
Pipl
That's Them
ReverseMails
Newsgroups
DomainData
Gravatar
Google
Yandex
Bing
HIBP
Hacked-Emails
Websites / Blogs
User Names
Social Networks
Search Engines
Email Permutator
Email Search Engines
Email Assumptions (Work)
Verify Address
Gmail, Yahoo, Hotmail, etc.
Email Assumptions (Personal)
FB Password Reset
Facebook Profile
Social Networks

Google Dorks

*	inurl	*	filetype or ext	*	*
*	site	*	link	*	**
*	intitle	*	inanchor	*	.
*	allintitle	*	allintext	*	|
*	allinurl	*	intext	*	+
*	cache			*	-

“Anthony Tippy” -facebook filetype:pdf intitle:OSINT

Google Hacking Database

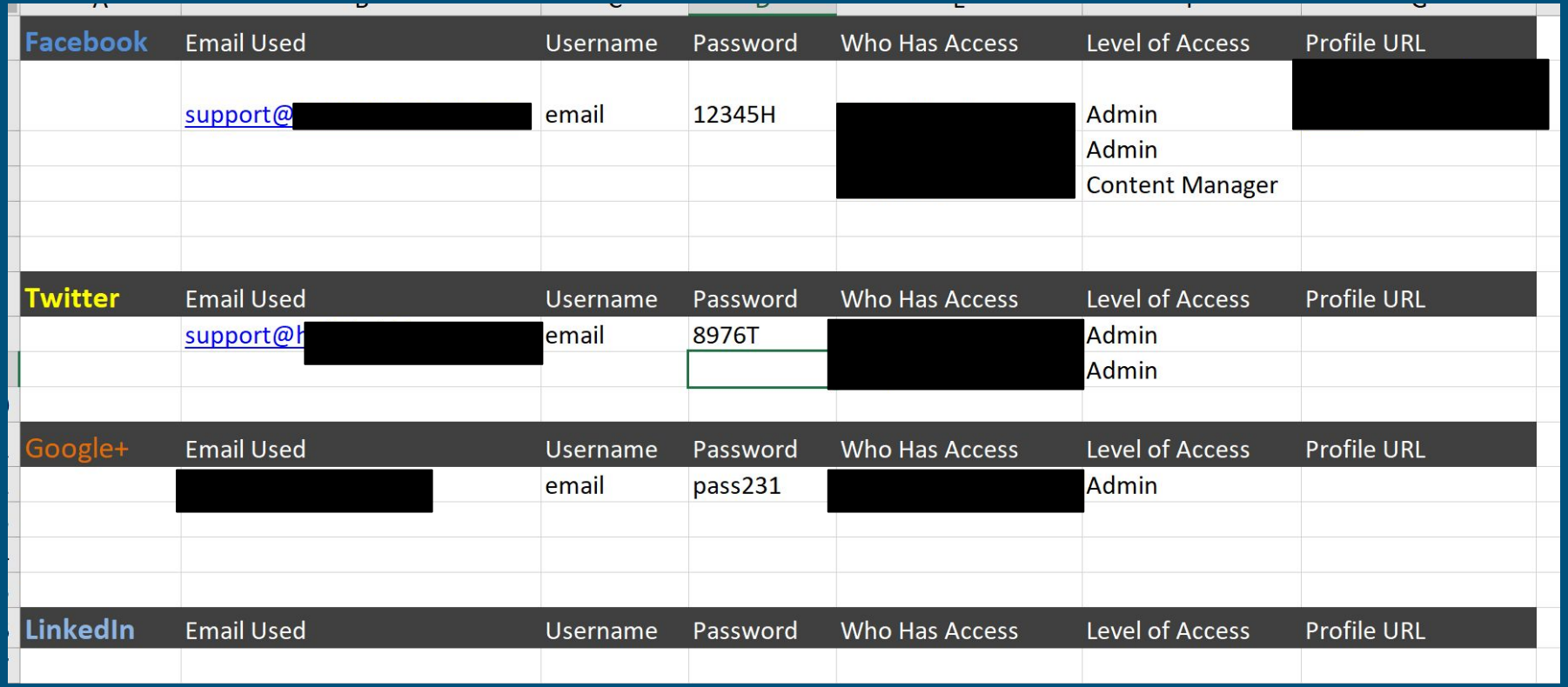
Filters | Reset All

Show 15

Quick Search

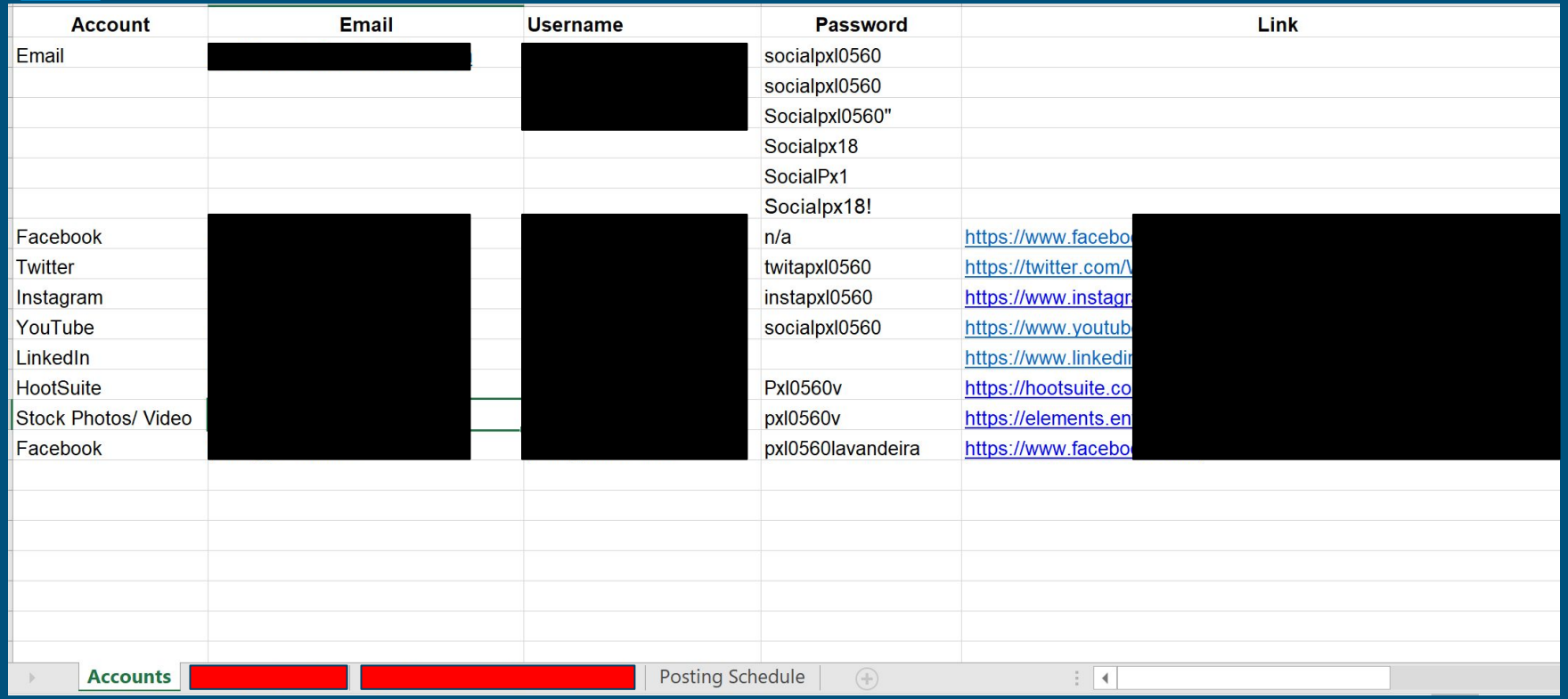
Date Added	Dork	Category	Author
2020-02-03	intitle:"index of" share.passwd OR cloud.passwd OR ftp.passwd -public	Files Containing Passwords	Bruno Schmid
2020-02-03	krb.conf OR krb.realms intitle:"index of" -public -archive -packages -pub	Files Containing Juicy Info	Bruno Schmid
2020-02-03	accdb OR accde intitle:"index of" -pub -google -books	Files Containing Juicy Info	Bruno Schmid
2020-02-03	filetype:env intext:APP_NAME	Files Containing Juicy Info	Puneet Choudhary
2020-01-30	"Firmware Version" intitle:"iLO" ProLiant Login -hpe.com -update	Various Online Devices	Bruno Schmid
2020-01-29	-pub -pool intitle:"index of" db.key OR server.key OR ftp.key OR exchange.key OR host.key OR mail.key	Files Containing Juicy Info	Bruno Schmid
2020-01-29	intitle:"index of" "/Cloudflare-CPanel-7.0.1"	Sensitive Directories	Pankaj Kumar Thakur
2020-01-28	intitle:"index of" "Served by Sun-ONE"	Web Server Detection	Bruno Schmid

“filetype:xls username password email”



Facebook	Email Used	Username	Password	Who Has Access	Level of Access	Profile URL
	support@[redacted]	email	12345H	[redacted]	Admin	[redacted]
					Admin	
					Content Manager	
Twitter	**Email Used**	**Username**	**Password**	**Who Has Access**	**Level of Access**	**Profile URL**
	support@h[redacted]	email	8976T	[redacted]	Admin	
					Admin	
Google+	**Email Used**	**Username**	**Password**	**Who Has Access**	**Level of Access**	**Profile URL**
	[redacted]	email	pass231	[redacted]	Admin	
LinkedIn	**Email Used**	**Username**	**Password**	**Who Has Access**	**Level of Access**	**Profile URL**

filetype:xlsx username password



Account	Email	Username	Password	Link
Email	[redacted]	[redacted]	socialpxl0560	
			socialpxl0560	
			Socialpxl0560"	
			Socialpx18	
			SocialPx1	
			Socialpx18!	
Facebook	[redacted]	[redacted]	n/a	https://www.facebo[redacted]
Twitter			twitapxl0560	https://twitter.com/[redacted]
Instagram			instapxl0560	https://www.instagr[redacted]
YouTube			socialpxl0560	https://www.youtub[redacted]
LinkedIn				https://www.linkedi[redacted]
HootSuite			Pxl0560v	https://hootsuite.co[redacted]
Stock Photos/ Video			pxl0560v	https://elements.en[redacted]
Facebook			pxl0560lavandeira	https://www.facebo[redacted]

Accounts [redacted] [redacted] Posting Schedule

Defense:

1. Password Managers
2. Regular vulnerability scans against your site/org
3. Learn the google fu
4. Request sensitive data removal (Removals Tool)
5. Block sensitive content by using a robots.txt file

Google Maps

1. Street view
2. Google Earth
3. Location Comparison
4. Image Location search

Youtube & Google Maps

Toms toys

ain Street, Great Barrington, MA

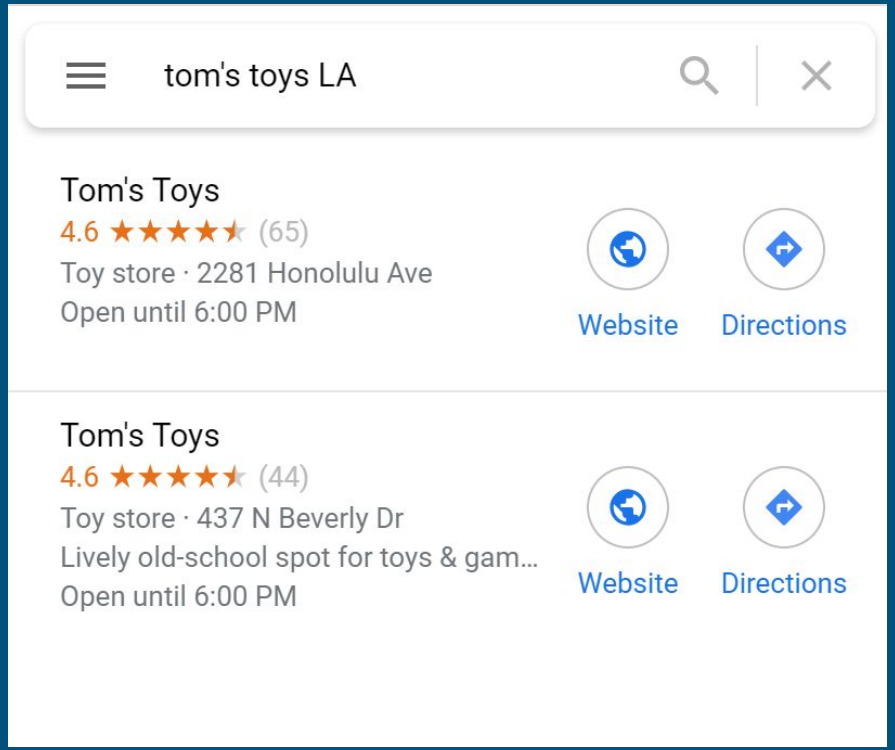
rth Beverly Drive, Beverly Hills, CA

guera Street, San Luis Obispo, CA

Site: Tom’s Toys - very likely

State: California - very likely

Exact Location: ?

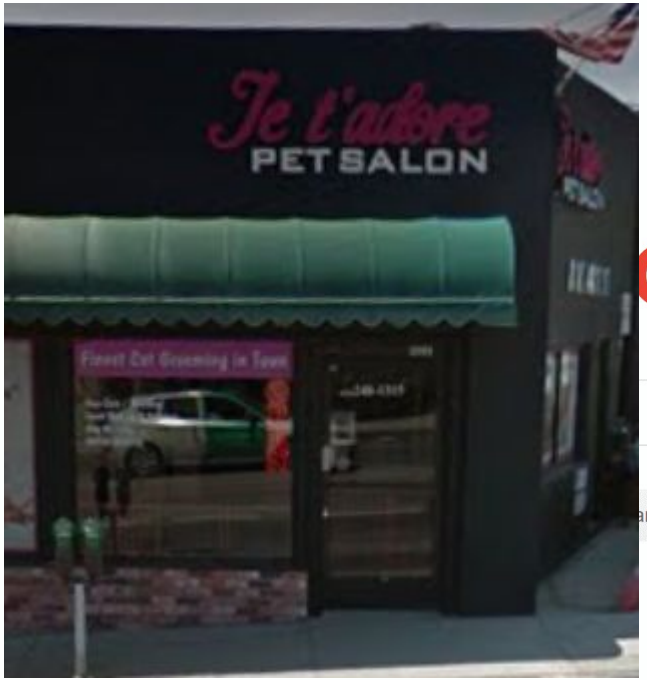



R.GHT
TURN
ONLY

google.com

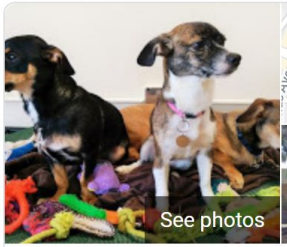
About Store

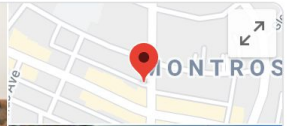
Gmail Images

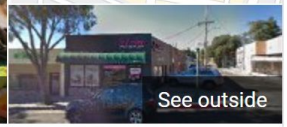


oogle

arch I'm Feeling Lucky







Je t'adore Pet Salon

Website Directions Save

4.4 ★★★★½ 14 Google reviews

Pet groomer in Glendale, California

Address: 3809 Ocean View Blvd, Montrose, CA 91020

Hours: Closed · Opens 8AM

Site: Tom’s Toys - very likely

State: California - very likely

Exact Location: Montrose CA

Tom's Toys

4.6 ★★★★½ (65)

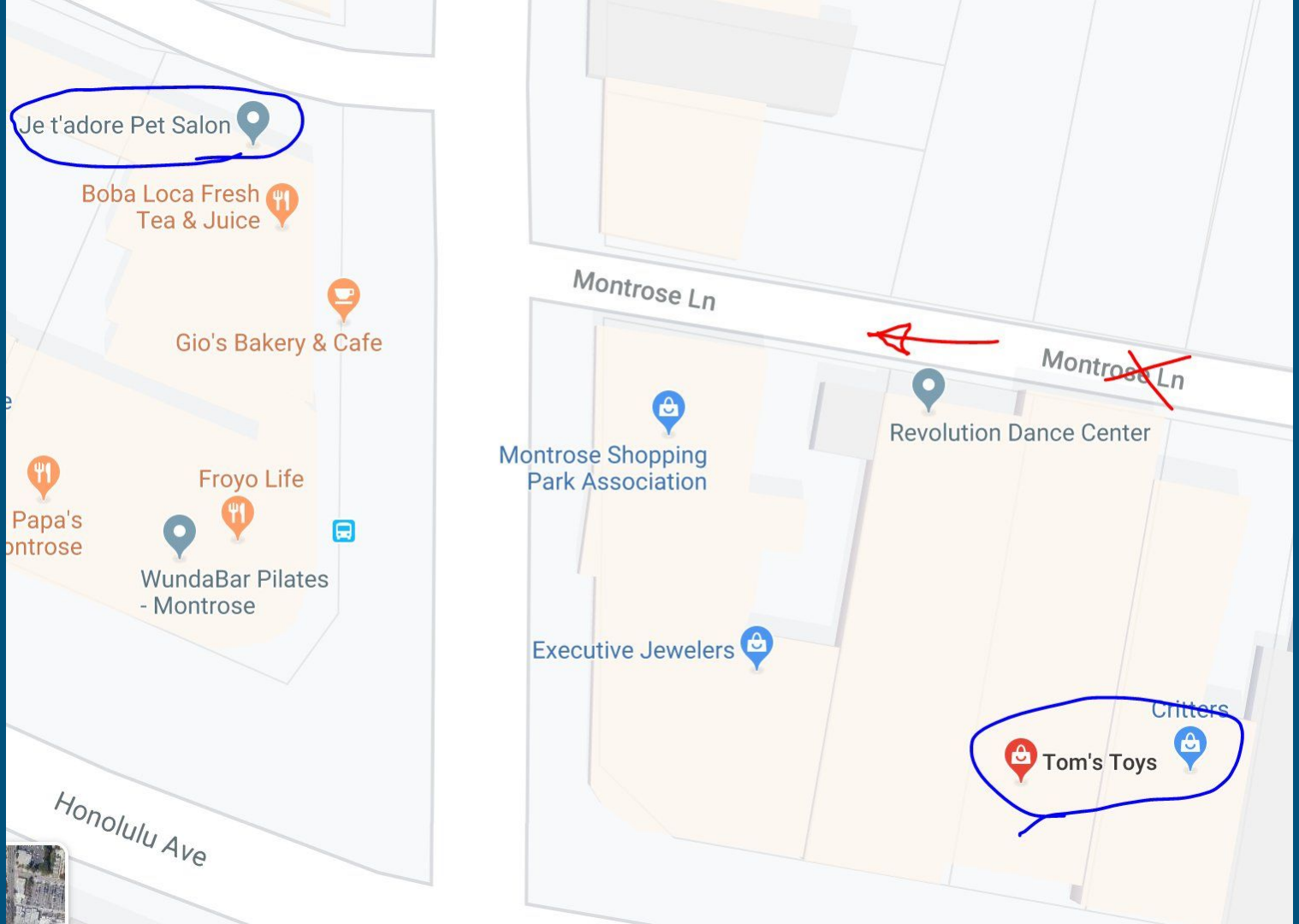
Toy store

Directions Save Nearby Send to your phone Share

2281 Honolulu Ave, Montrose, CA 91020

6Q4F+62 Montrose, La Crescenta-Montrose, CA

tomstoystore.com


Je t'adore Pet Salon
Boba Loca Fresh Tea & Juice
Gio's Bakery & Cafe
Froyo Life
Papa's
ontrose
WundaBar Pilates - Montrose
Honolulu Ave
Montrose Ln
Montrose Ln
Revolution Dance Center
Montrose Shopping Park Association
Executive Jewelers
Critters
Tom's Toys

How’d we do?

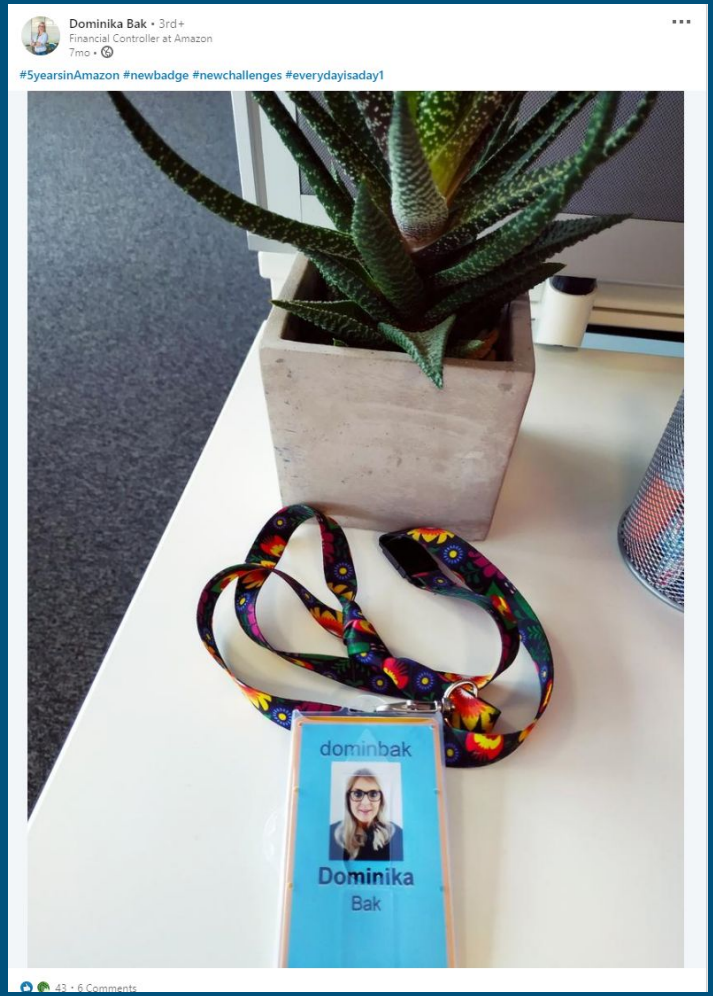
Social Media - My Best Friend

- People LOVE to share
- Overexposing information

#newbadge


ISHWARYA
RAMACHANDRAN
EMPLOYEE
ISHWARYA
Ramachandran
EMPLOYEE
ISHWARYA
Ramachandran
EMPLOYEE


#newpassport
Passport
Kingston
Editar
ESPAÑA
UNIÓN EUROPEA
PASAPORTE
An tAontas Eorpach
European Union
ÉIRE
IRELAND
Pas
Passport
PASSPORT
AUSTRALIA
GRENADA
Home Office


Dominika Bak • 3rd+
Financial Controller at Amazon
7mo •
#5yearsinAmazon #newbadge #newchallenges #everydayisaday1
dominbak
Dominika
Bak
43 • 6 Comments

#newbadge

8,915 posts

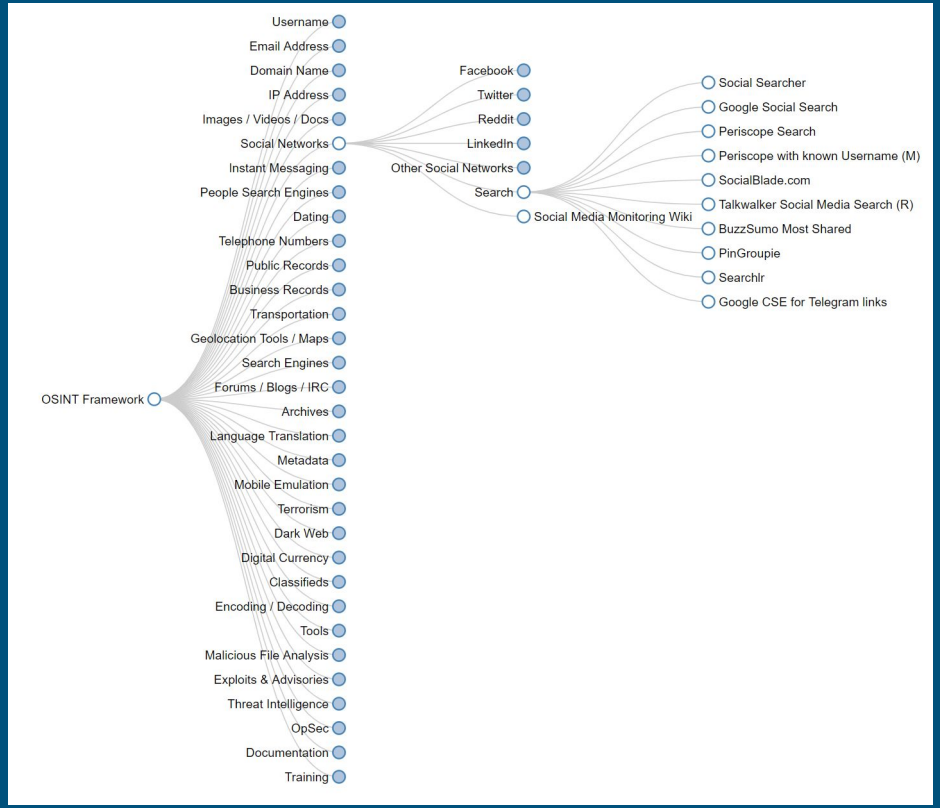
Follow

Related Hashtags #elite_apparel_exclusive #traillöpning #4thtrimesterworkout #runnerswholift #löpningärkul #learntorun #lond
#teampowerwoman_official #terränglöpning #träningspodden

Top posts

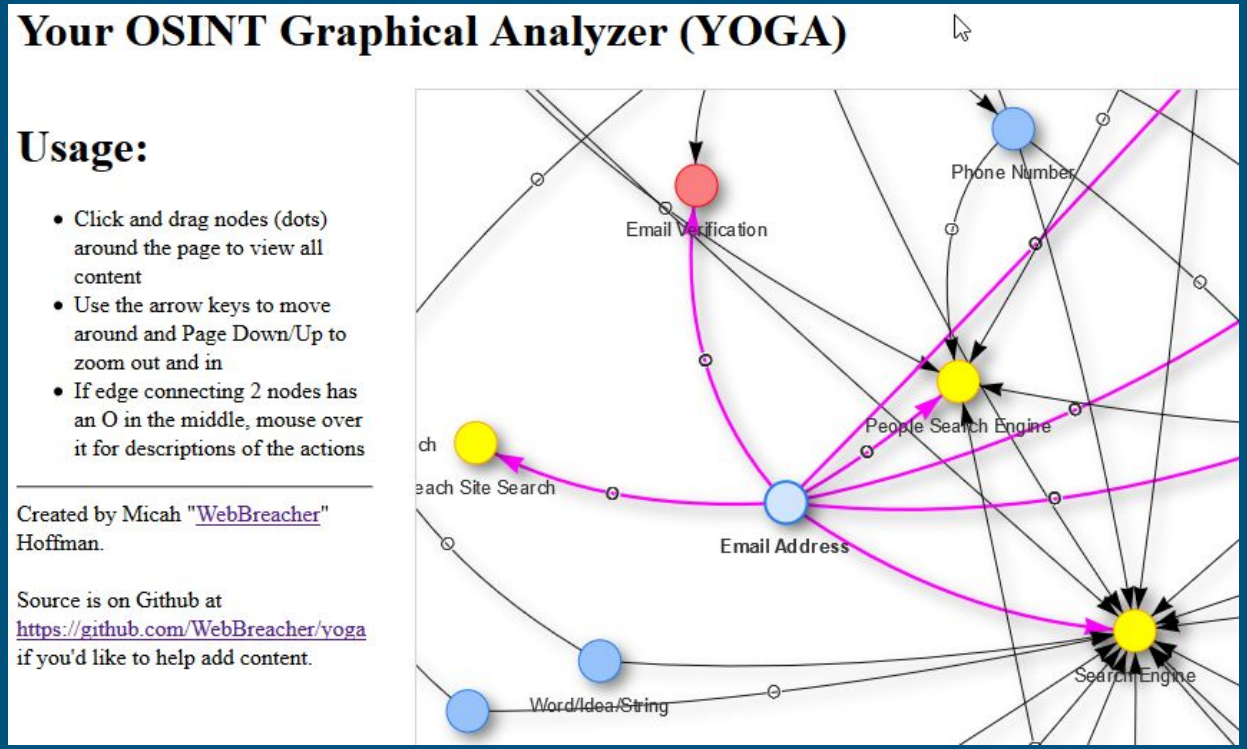
OSINTFramework.com

- OSINT Bookmarks
- Starting pages
- There’s a ton more



Yoga.Osint.Ninja

- Michah “WeBreacher” Hoffman
- “I have this information. What can I transform it into or use it for?”
- Next steps in OSINT investigations



Takeaways

- Learn how to use “the google”
- Google dorking
- Explore the public information that’s online
- Don’t post your passwords online
- Be careful what information you share/expose
- Don’t be afraid of new search methods
- Hack the planet

Thank you!