Understand and Protect Against Open Source Intelligence

Presented by Anastacia Webster

About me. . .

What is Open Source Intelligence?

- What are open sources?
- What is intelligence?
- How do the two meet?
- Why should we care?

OSINT Workflow

1 to ∞

Name
Telephone Number
Address
Past Addresses
Email Address (All of them)
Job Address
Job Telephone Number
Relative
Date of Birth

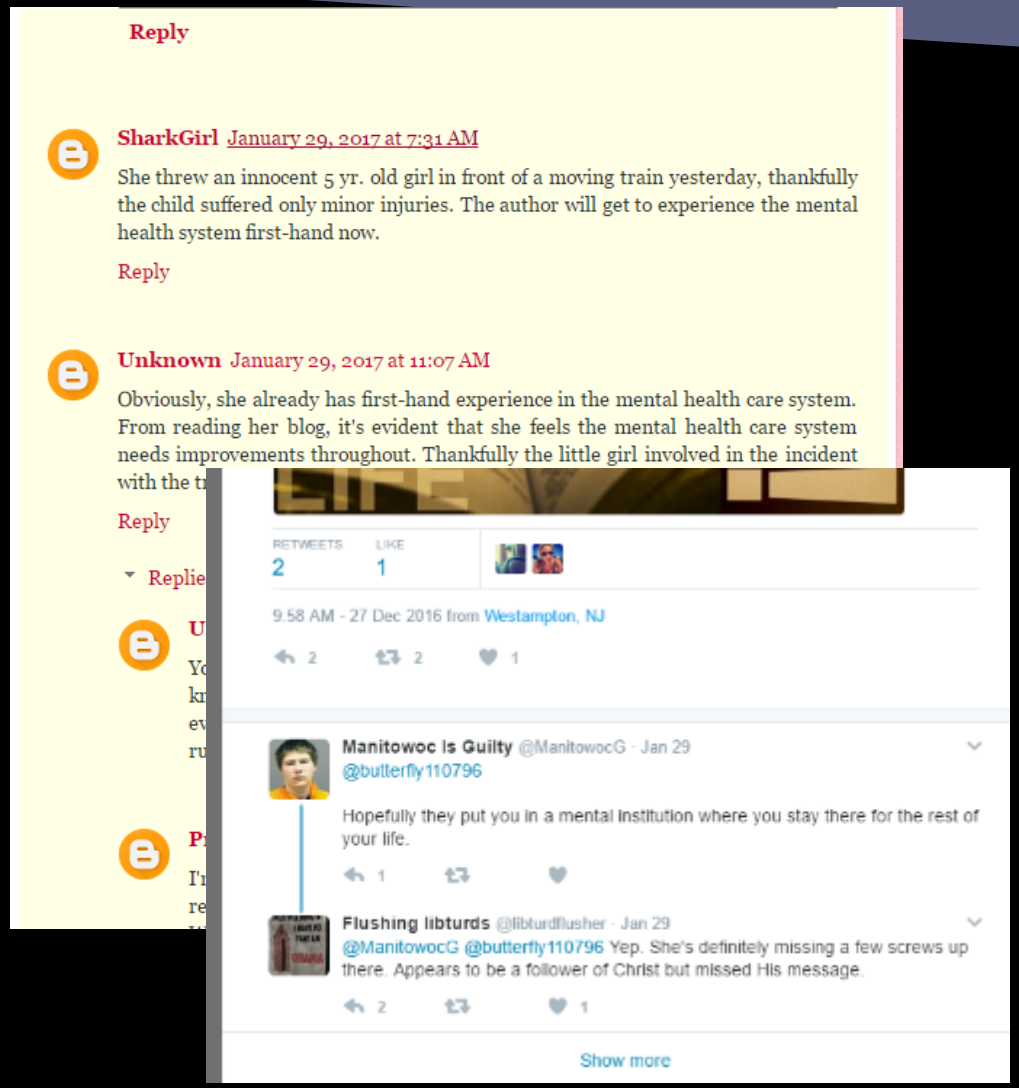
Social Security Number
Civil and Public Court Records
Criminal Records
Photos
Photos of Address
Marriage
Divorce
Voter Registration
Tax Filings
Licenses
Past Employment
Drivers License
Accidents
ETC....

Privacy vs. Information Privacy

- Privacy is NOT absolute. . .
- Information Privacy. . . NON-EXISTANT
- Privacy Arguments
  - Pro:
    - “I have nothing to hide.”
  - Con:
    - Those stories we don’t want our bosses knowing about

Autumn Matacchiera

- Allegedly threw five year old girl in front of a train. . .
- Within hours, comments appeared on her personal blog from users using OSINT techniques to find her online.
- **Note: By this time her FB was already deactivated.



Suitable For Framing

- Store allegedly refused to frame a customers inauguration pics. . .
- Within hours of the story, yelp site was flooded with poor reviews and nasty comments.

Suitable For Framing - 74 Photos & 146 Reviews - Art Galleries - 105 ...
https://www.yelp.com › Arts & Entertainment › Art Galleries
Rating: 1.5 - 146 reviews - Price range: $$$$
146 reviews of **Suitable For Framing** "There were 90 reviews earlier this morning, ... to all who visit the town of Aspen, **Colorado**--AVOID THIS ESTABLISHMENT!

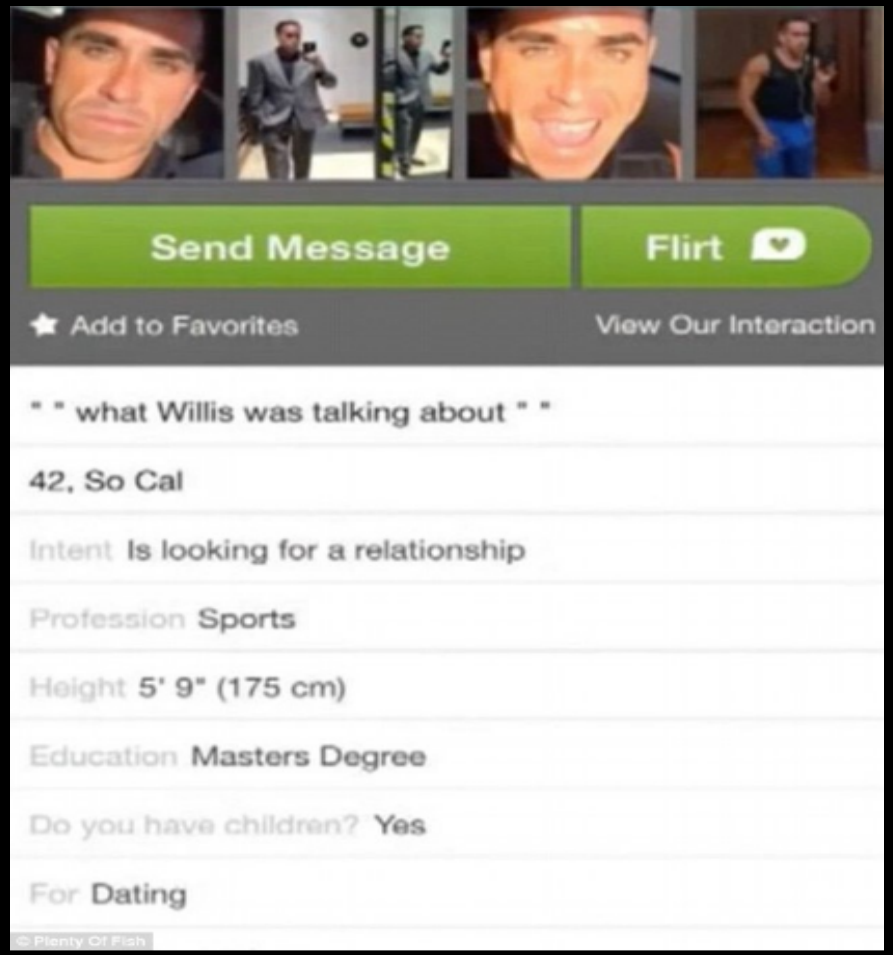
Suitable For Framing - 77 Reviews - Art Galleries - 105 S ... - Yelp
https://www.yelp.com › Arts & Entertainment › Art Galleries
Rating: 1.1 - 77 reviews - Price range: $$$$
77 reviews of **Suitable For Framing** "BEWARE. The owners are hypocrites. Unfair business practice. Take your framing projects to Frame Center, Aspen Art ...

Ethics and OSINT

- Some grey areas…
- Some Ethical Issues
  - Disinformation
  - Accuracy
  - Credibility
  - Reliability
  - Abuse of Power
    - Integrity
  - Exploitation
  - Privacy
  - Aggregation
    - Confidential and Classified Data/Info

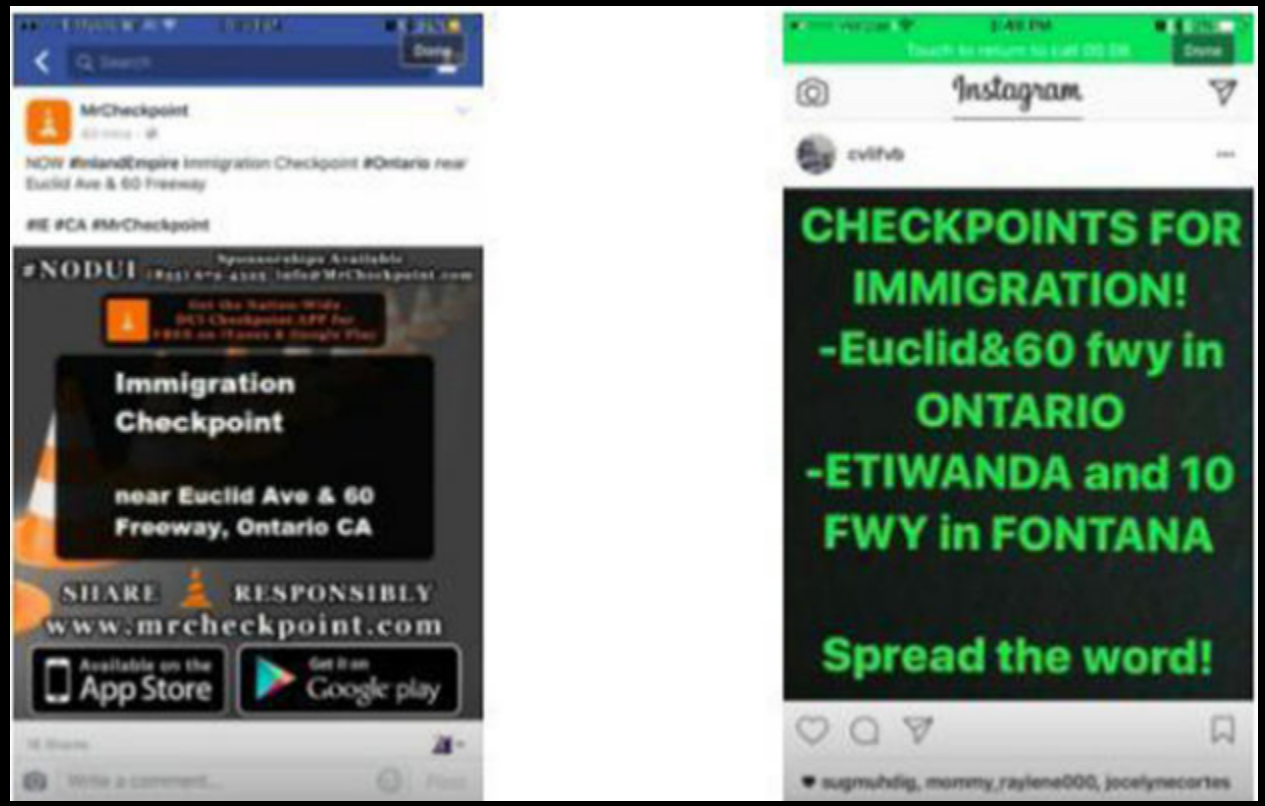
FBI Warns of Online Dating Scams

- Targeting women 40+ who are divorced, widowed, and/or disabled. . . but everyone at risk..
- Scam: Contacted by someone online that appears interested
- Attacker/scammer build rapport, may even send items (i.e. flowers)
- Asks you for money, to cash checks, or to forward packages



News (& Fake News) and Social Media

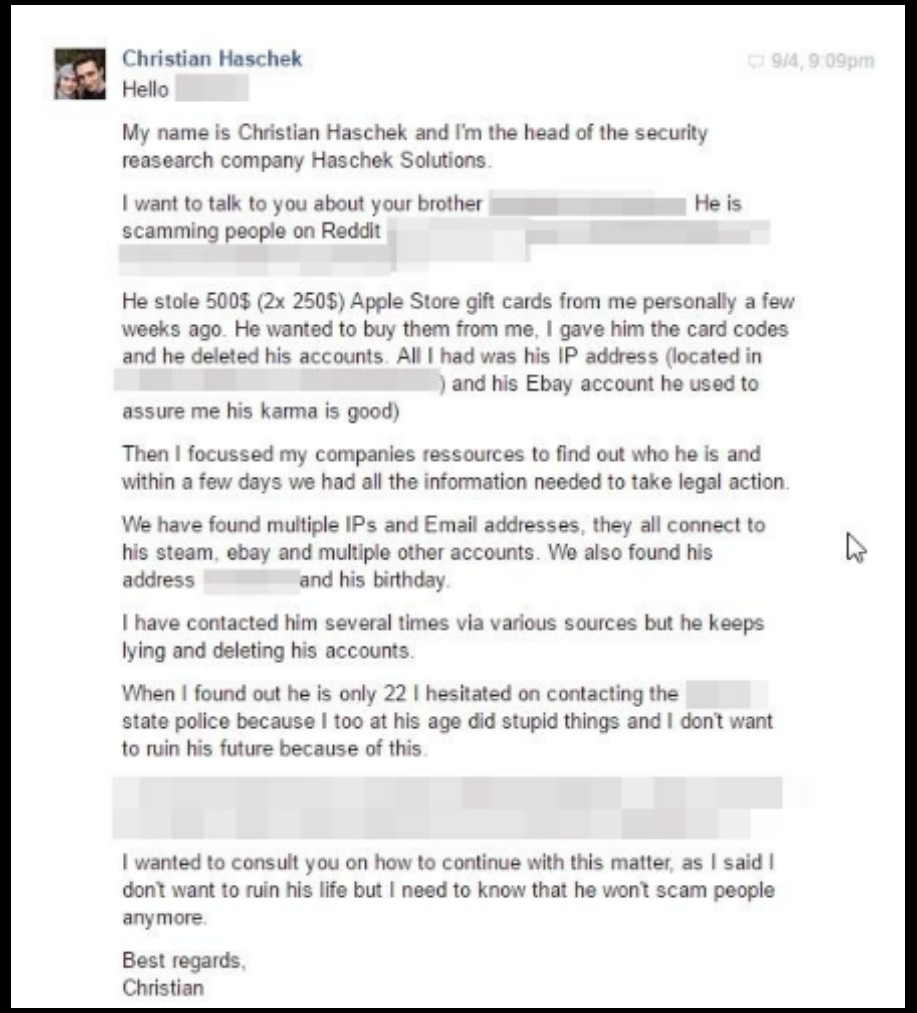
- On February 3, 2016, Law Enforcement, in conjunction with the Los Angeles Times, released a statement against the wave of false deportation checkpoints on popular platforms like Facebook, Instagram and Twitter.



Using OSINT to Find the Scammers

https://blog.haschek.at/2016/how-a-scammer-stole-500-dollars-from-me

- SUCH AN AMAZING STORY...



Christian Haschek 9/4, 9:09pm

Hello [redacted]

My name is Christian Haschek and I'm the head of the security reasearch company Haschek Solutions.

I want to talk to you about your brother [redacted] He is scamming people on Reddit [redacted]

He stole 500$ (2x 250$) Apple Store gift cards from me personally a few weeks ago. He wanted to buy them from me, I gave him the card codes and he deleted his accounts. All I had was his IP address (located in [redacted]) and his Ebay account he used to assure me his karma is good)

Then I focussed my companies ressources to find out who he is and within a few days we had all the information needed to take legal action.

We have found multiple IPs and Email addresses, they all connect to his steam, ebay and multiple other accounts. We also found his address [redacted] and his birthday.

I have contacted him several times via various sources but he keeps lying and deleting his accounts.

When I found out he is only 22 I hesitated on contacting the [redacted] state police because I too at his age did stupid things and I don't want to ruin his future because of this.

[redacted]

I wanted to consult you on how to continue with this matter, as I said I don't want to ruin his life but I need to know that he won't scam people anymore.

Best regards,
Christian

Open Source Intelligence and Research Association (OSIRA) Code of Ethics

1. Responsibility
   - Take responsibility for your actions.
2. Professionalism
   - Always continue to learn and strive for moral high ground.
3. Credibility
   - Be objective and verify the credibility of sources/accuracy of information.
4. Personal Example
   - Be a role model to others by displaying honesty, integrity, and selflessness.
5. Sense of Mission
   - Advance OSIRA and uphold professionalism.
6. Comradeship
   - Help out other OSINT researchers.

. . . Cool story, bro . . . But why should I care?

HACKERS CARE…That's why…

Recon Village

An Open Space with Talks, Live Demos, Workshops,
Discussions, CTFs with a common focus on Reconnaissance.

Get Involved..

Talks & Workshops Announced Talks Workshops

Data + Information= Knowledge = POWER!

- Name
- DOB
- SSN
- Address (Current and past)
- Employers/Coworkers (current and the past, hierarchy, friendliness)
- Phone Number (Cell, home, work)
- Family (Names, #, POB, DOB, SSN)
- Friends (Names, #, DOB, SSN)
- Likes/Dislikes (Movies, music, newspapers, etc.)
- Political/Religious Views
- Relationships (Wife, mistress, girlfriend…)
- System Information (operating systems, IP, software configurations)
- Personnel Information (employees, position, emails, etc.
- Interests/Hobbies
- Photos
- Videos
- Purchases
- Car/Truck/Boats
- Important Life Dates (First Child, Graduation, etc)
- Bank
- Favorite Places
- All aliases online
- Social Medias
- Volunteerism/ Activism
- Personas Online (Avatars)
- Files (.ppt, .xls, .xlsx, .doc, .docx, .csv, .pdf, .txt, .rtf, .odt, .ods, .odg, .odp, .wpd

Hypothetical Situation

(I had permission to show collect the information I collected and show you what I can. . .there is going to be a lot of black)

SPOKEO [redacted] ABOUT LOG

[redacted]

UNLOCK PROFILE

- ✓ Male, Age 50
- ✓ Relatives: [redacted]
- ✓ Locations: [redacted]

Unlock this profile to monitor for updates!

Unlock this profile to monitor it and be notified of any updates.

Profile sections

- A[redacted]
- Updates
- Contact Info (14)
- Location History (4)

Personal Details

Full Name, Age, Relationship Status, and More

Contact Information

Phone, Email, Business Contacts, and Full Ad

Location History

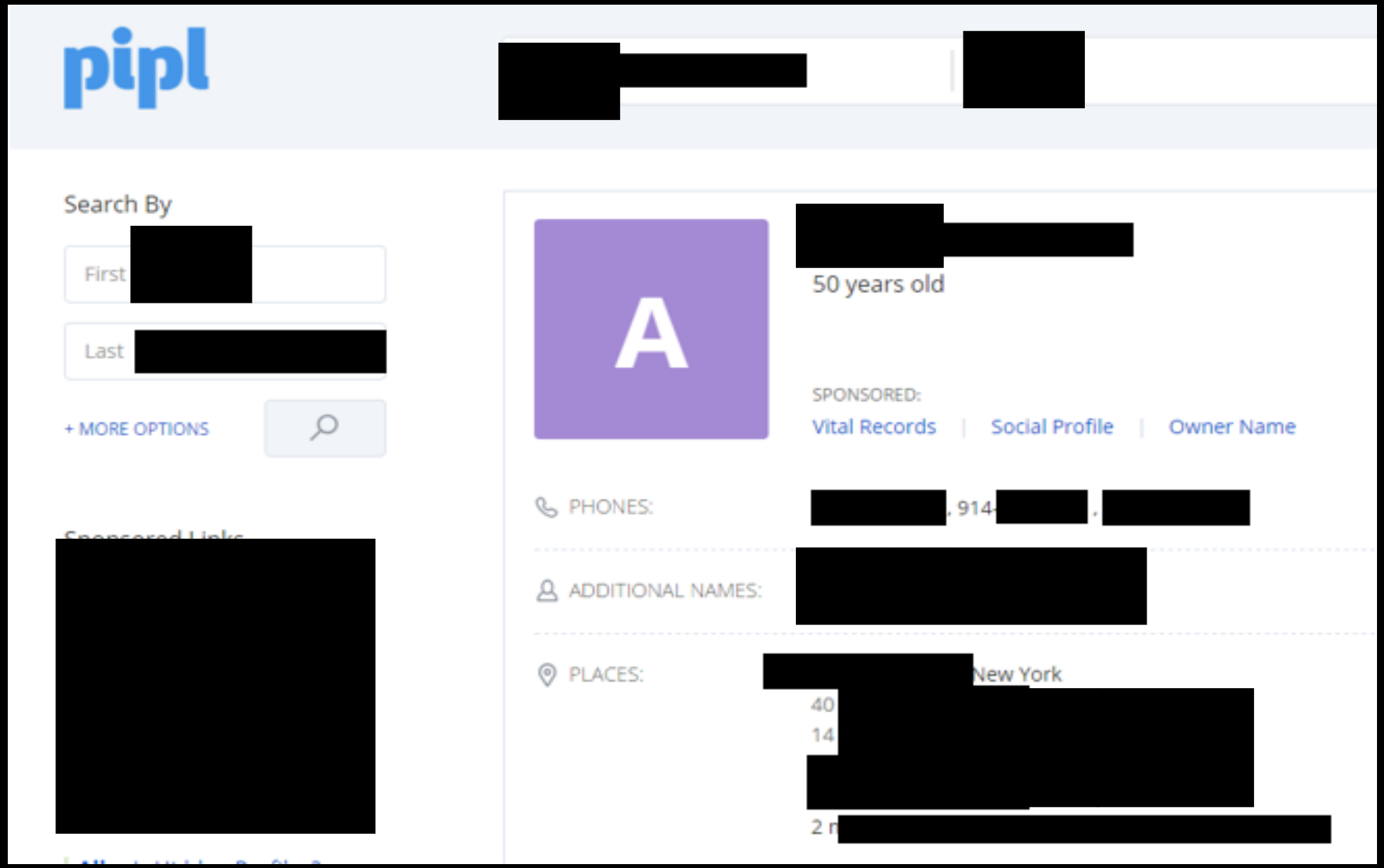
Current & Previous Address and Neighborhood Information

Photos & Online Profiles

Social Profile, Photos, and Videos from Top C Sites

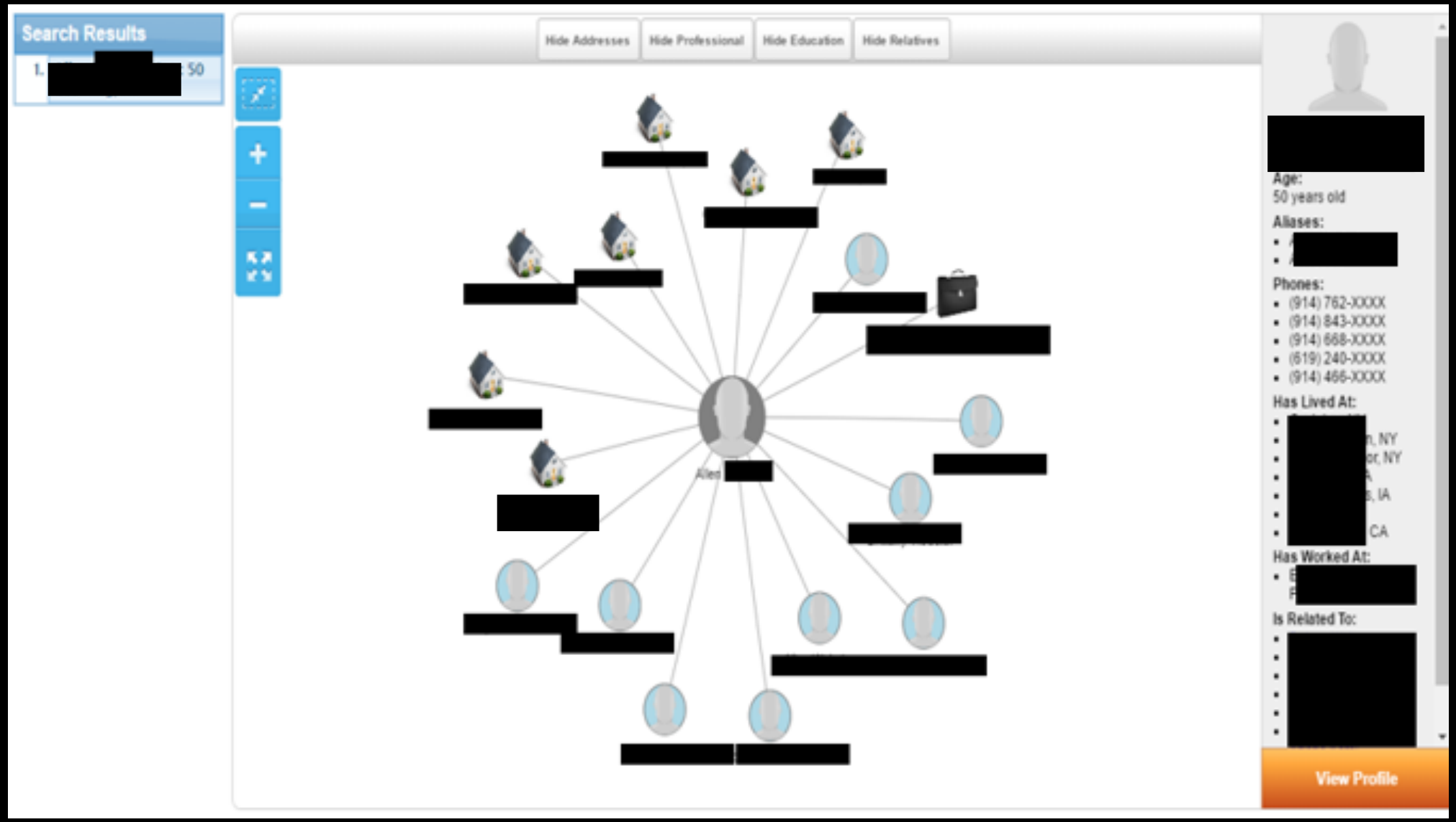
```
.leftPanelClasses()'>
apExpansion.leftPanelContentClasses()'>


arkers='{"home":[{"latitude" [redacted] ,"longitude": [redacted] ,"href":"/reverse-address-search/direct-
/nokia_map>



howUnderMapNav() == false'>
ock " href="https://www.spokeo.com/purchase?
```

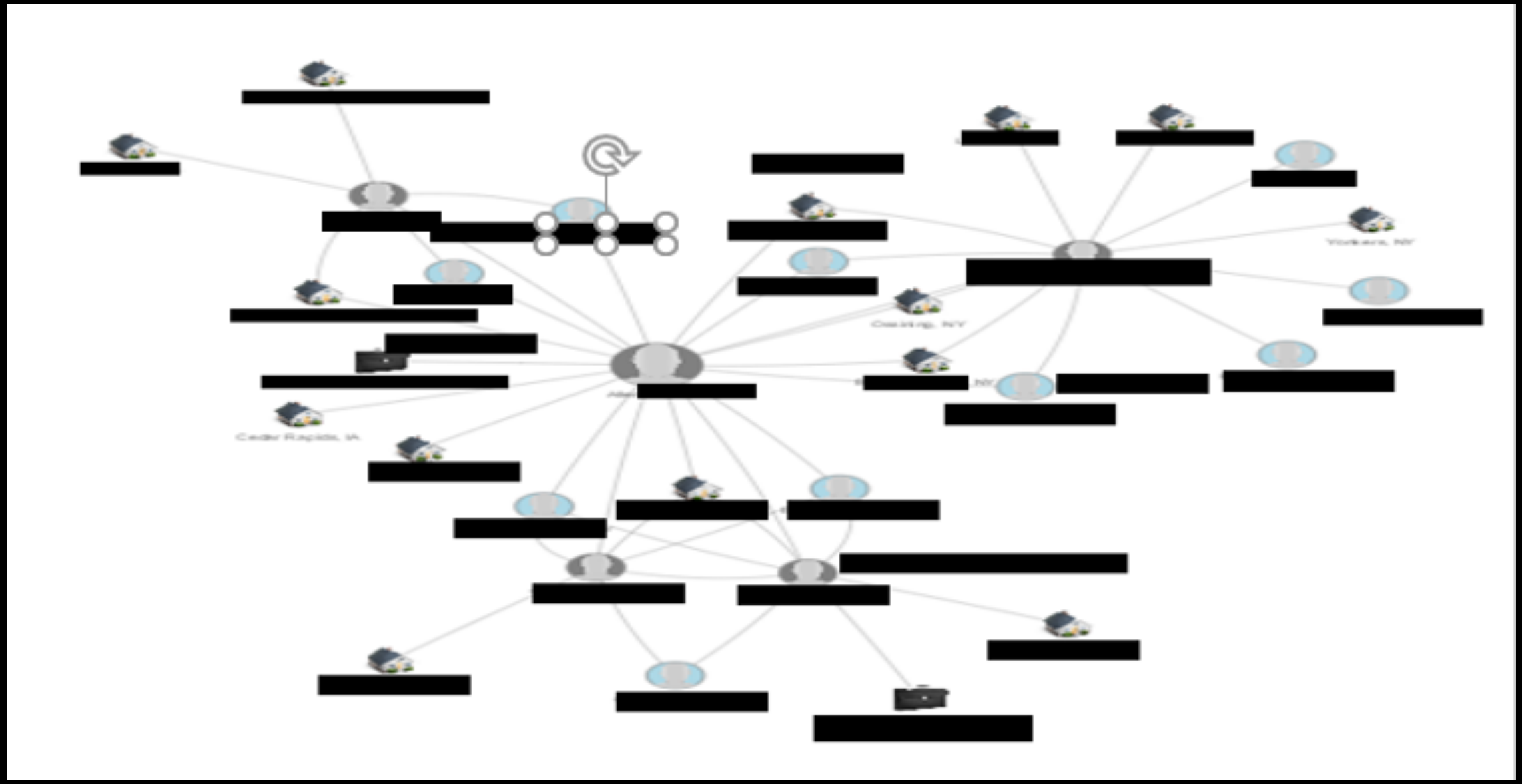

[redacted]
Directions
SAVE
NEARBY
SEND TO YOUR PHONE
SHARE
Add a missing place
Add a label


pipl
[redacted]
Search By
First [redacted]
Last [redacted]
+ MORE OPTIONS
[redacted]
A
[redacted]
50 years old
SPONSORED:
Vital Records | Social Profile | Owner Name
PHONES: [redacted], 914-[redacted], [redacted]
ADDITIONAL NAMES: [redacted]
PLACES: [redacted] New York
40
14
[redacted]
2 r[redacted]

2.	[redacted] AKAs [redacted] More AKAs...	50	[redacted] A , NY r, NY More Addresses...	(914) (401) (619) (914) More Phones...	[redacted] More Relatives...	view details

```
 col-sm-2 col-no-padding-left txt-sml weirdresults padding-top-sm">
        <div>(914)<span style="filter: blur(2px);"> 76[redacted]</span><
        <div>(401)<span style="filter: blur(2px);"> 78[redacted]</span><
        <div>(619)<span style="filter: blur(2px);"> 24[redacted]</span><
        <div>(914)<span style="filter: blur(2px);"> 84[redacted]</span><
<a href="/peoplese
```


Search Results
1. [redacted] 50
Hide Addresses
Hide Professional
Hide Education
Hide Relatives
Allen
[redacted]
Age:
50 years old
Aliases:
Phones:
(914) 762-XXXX
(914) 843-XXXX
(914) 668-XXXX
(619) 240-XXXX
(914) 466-XXXX
Has Lived At:
Has Worked At:
Is Related To:
View Profile



[redacted]

14[redacted]
Mo[redacted]
(914)[redacted]

Infofree Business Profile prepared on 02/09/2017
You have paid for this business profile!

☆☆☆☆☆ 0 Reviews

Claim this Business | Print Profile

Business Profile

Web site	www[redacted].com
Number of Employees	20 to 49
Annual Revenue	$5 to 10 Million
Years in business	10 or More Years
Type of business	[redacted]
SIC	
Square Footage	10,000 to 49,999
No. of PCs	10 to 24
Small Business	Yes

Executives 7

[redacted]	Manager
	President
	President

Business Credit Rating

95 / Excellent

Suggested Credit Capacity:

$6,000

Company Expenses

Accounting Expenses	$25,000 to $99,999
Advertising Expenses	$5,000 to $14,999
Business Expenses	$20,000 to $49,999
Legal Expenses	$25,000 to $99,999
Office Equipment Expenses	$10,000 to $24,999
Rent Expenses	$25,000 to $99,999
Technology Expenses	$25,000 to $99,999
Telecom Expenses	$10,000 to $24,999
Utilities Expenses	$20,000 to $49,999

A	B	C	D	E	F	G	H	I
		HAWTHORNE	NJ	07506	US	973-		
		SPARKS	NV	89431	US	775-		
		SOUTH FALLSBURG	NY	12779	US	845-		
		BROOKLYN	NY	11221	US	718-		
		LONG ISLAND CITY	NY	11101	US	718-		
		MORRISONVILLE	NY	12962	US	518-		
		FLUSHING	NY	11367	US	718-		
		BINGHAMTON	NY	13902	US	607-		
		BROOKLYN	NY	11214	US	718-		
		NIAGARA FALLS	NY	14304	US	716-		
		YONKERS	NY	10701	US	914-		
		COPIAGUE	NY	11726	US	631-		
		BUFFALO	NY	14217-0306	US	716-		
		CANANDAIGUA	NY	14424	US	585-		
		DELMAR	NY	12054	US	518-		
		MOUNT VERNON	NY	10550	US	914-		
		BUFFALO	NY	14210	US	716-		
		ELMONT	NY	11003	US	516-		
		BROOKLYN	NY	11232	US	718-		
		WATERLOO	NY	13165-1240	US	315-		
		MELVILLE	NY	11747	US	631-		
		Mt. Vernon	NY	10553	US	914-		
		NORTH TONAWANDA	NY	14120	US	716-		
		GLENS FALLS	NY	12801	US	518-		
		SYRACUSE	NY	13202	US	315-		
		HASTINGS ON HUDSON	NY	10706	US	914-		
		BRONX	NY	10455	US	718-		
		JOHNSON CITY	NY	13790	US	607-		
		New York	NY	10128	US	212-		
		SYRACUSE	NY	13202	US	315-		

Name	DOB	Photo	Address	Past Residences	Email Addresses	Phone Numbers	Location Geotagging	Likes	Dislikes	Relationships	Friends	Videos	Photos
[redacted]					[redacted]			[redacted]		[redacted]			[redacted]

Like

Like

Like

Like

Data + Information = Knowledge = POWER!

- Name
- Age
- Location
- Relatives
- Phone Numbers
- Position at Work
- Likes
- Possible Addresses
- Place of Work Address
- Files (List of suppliers)
- Network
- Other Employees

- #of Employees
- Business Line
- Photos
- Aliases
- Website
- Company Worth
- Estimated # of PCs
- Years in Business
- Annual Revenue
- Estimated Expenses
- And much, much more!

Digital Dossier Assignment

- Almost all of the students are able to find information about themselves, even those with the most common names.
- Those who cannot find information about themselves, usually try to get away with not doing the assignment. (I know this because then I search them).
- Almost all don't reach the full amount of information available about them online. (I know this because I randomly select assignments for review and realize many miss a lot of information).
- Almost all of the students are terrified of what they find and how easy it is for them to find it. Most of them are unaware that the information exists.

Digital Dossier Assignment

- Some students find shocking things about themselves online. One of my students was unaware his criminal DUI from just a mere 4 months before the assignment was given out was available online.
- Most students reveal that the information they find about themselves online does indeed make them vulnerable. (Many surprised by addresses and phone numbers).
- After the assignment all students recognize the power of OSINT research and how they can use it to find information about themselves and others.

. . . so, Bro . . . what do I do now?

How can I protect myself and others?

- Keep your systems updated….exploit Tuesday, patch Wednesday
- Implement a strong password policy
  - Make sure users have a strong password that changes regularly (password management system)
- Protect your privacy…
  - Limit the amount of personal information you share online
  - Do NOT post anything work related online… (sometimes even your position)
  - Be weary of giving your information to others
- Humans are the weakest link in any security policy…
  - Mandatory Staff Training
  - Bottom Up Approach not Top Down
    - Cybersecurity is everyone's business

Comments/Questions?

Contact us at anastacia.webster@csusb.edu