OSINT Uncovered

Unlocking the Hidden Gems of Online Information

with Mishaal Khan

www.MishaalKhan.com

Agenda

- Holy $#!T
- Goals
- Tools (beyond Google)
- Verification/Disinformation
- Pivoting

About Me

What I Do	What my friends think I am
Certified Ethical Hacker	[Mr Robot]
Certified Social Engineer Pentester	[The Pretender]
Network (CCIE) / Coder	[Super Analytic]
vCISO / Security Practice Lead	[The Consultant]
Privacy Advisor	[Mr Tin Foil Hat]
OSINT Investigator	[The Good Stalker]
Wrote a book (The Phantom CISO)	[Bestselling Author]

OSINT

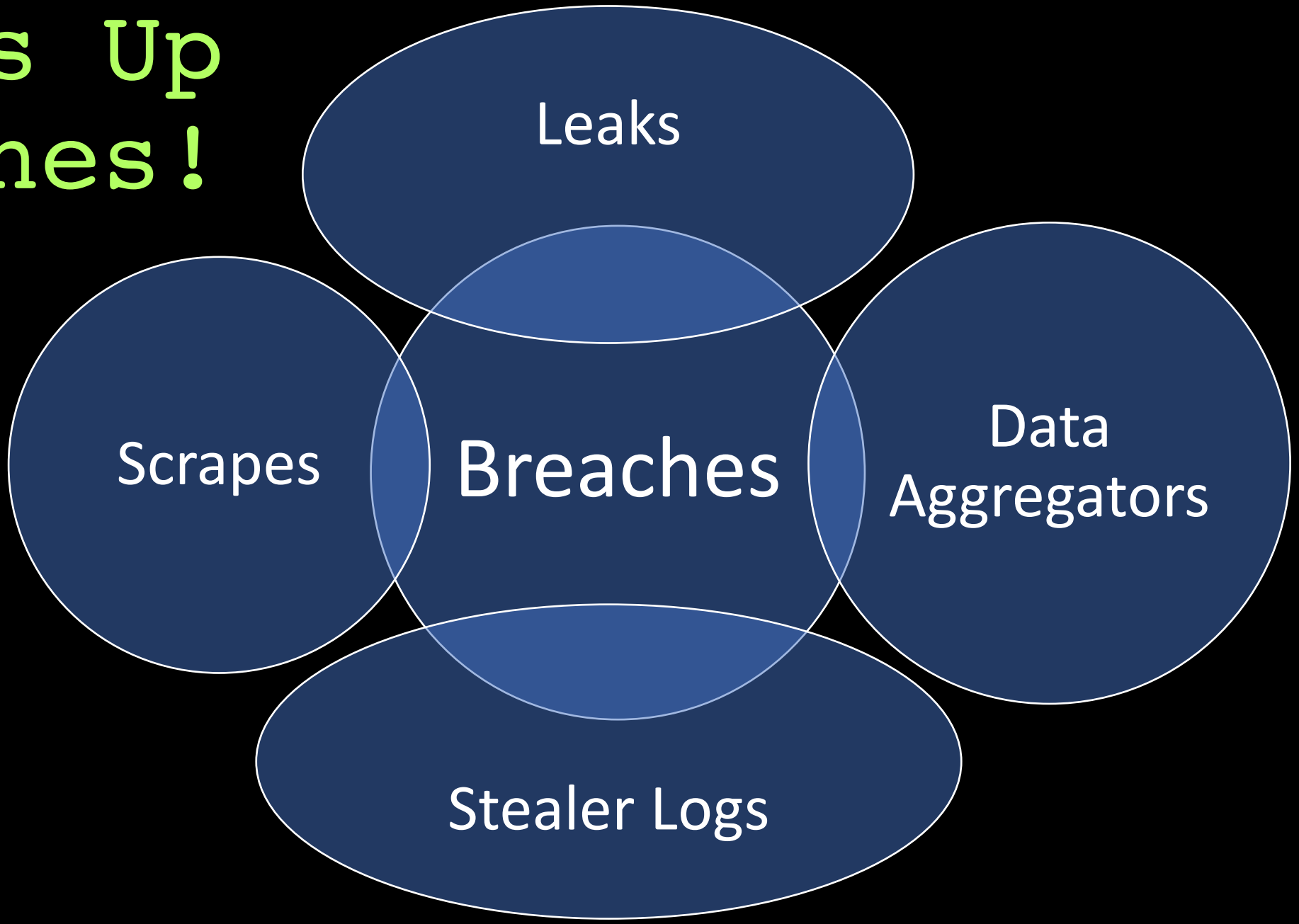
(~~Stalking~~ Open Source Intelligence)

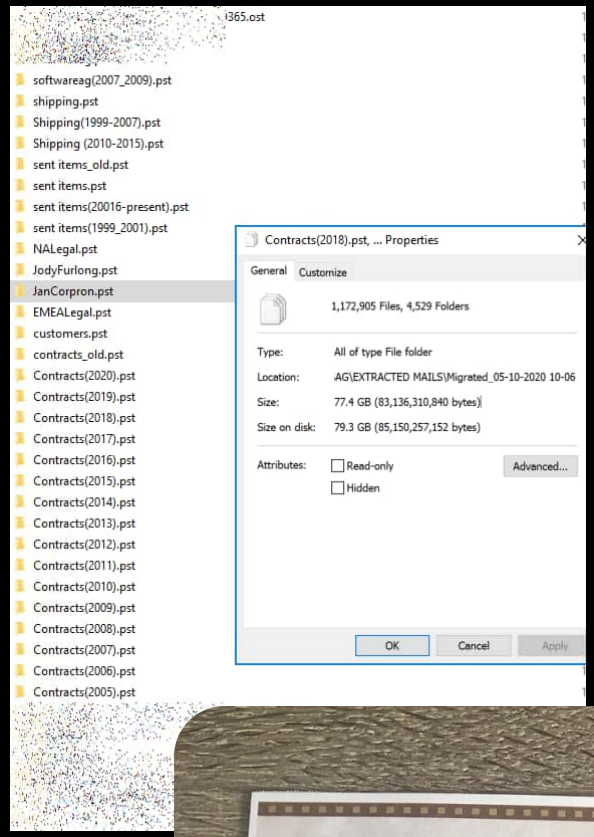
Categories

- Corporate OSINT
- Network OSINT (Recon)
- GeoINT
- SocMINT
- Everything else

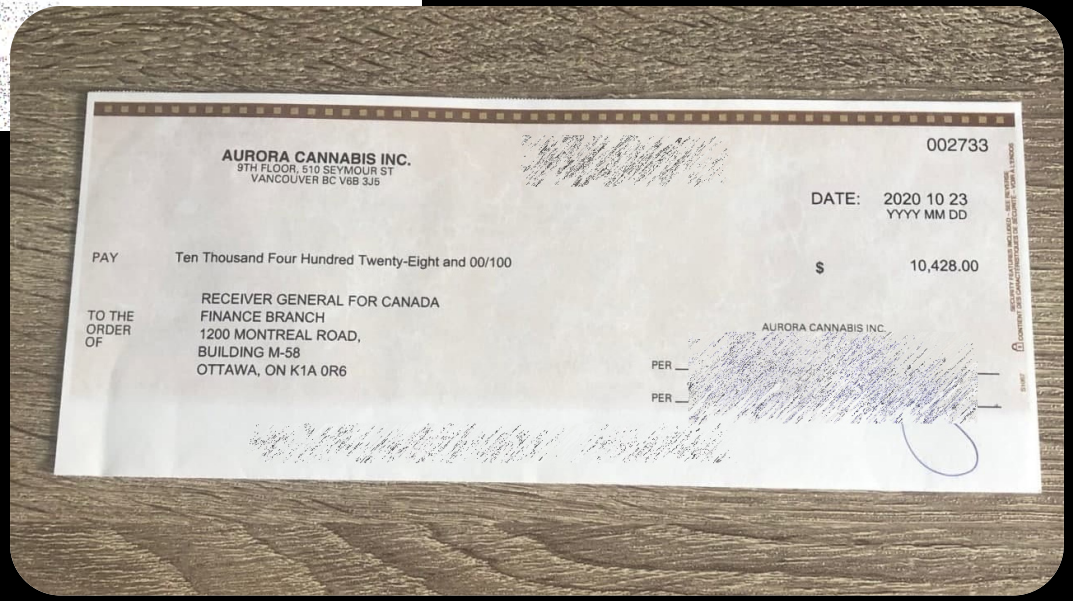

BREACHES
LIGHTYEAR
BREACHES EVERYWHERE
memegenerator.n

What's Up Breaches!





HR Files, Software AG



Aurora Cannabis

Class Member SSN	Class Member with additional SSN	Class Member Name	UC D
561	370	ABERNA	
572	173	ABROTT	
564	713	ADAMSI	
562	389	ALLEN, L	
473	455	ALLEN, R	
422	341	ALVARE	ND A
463	214	ANDERS	
570	764	BALUN,	
550	861	BATTI, A	
559	015	BERING	
566	560	BERKEY	
562	374	BERNRE	
565	926	BETTEN	
469	299	BEVENS	
572	805	BOKAN	
548	352	BORDEI	
572	411	BRENKV	
120	715	BROWN	
559	600	BUBP, D	
553	505	CALEY, L	
192	229	CAMPBI	
560	774	CARPEN	
277	987	CHATMI	
576	400	COMAG	
472	723	COOME	
548	543	CORL, M	
560	433	CORMI	
559	704	DASHER	
493	435	DAVISS	
541	745	DENNIS	
566	067	DIACON	
534	736	DIMMI	
530	395	DORAN,	
558	532	DOUGL	
202	575	DUARTE	
203	389	EBY, NA	
544	306	EHRLIC	
560	321	ERICKSE	
560	843	FOX, JA	
558	488	FRANCE	
560	706	FURR, C	

University Of California, Merced

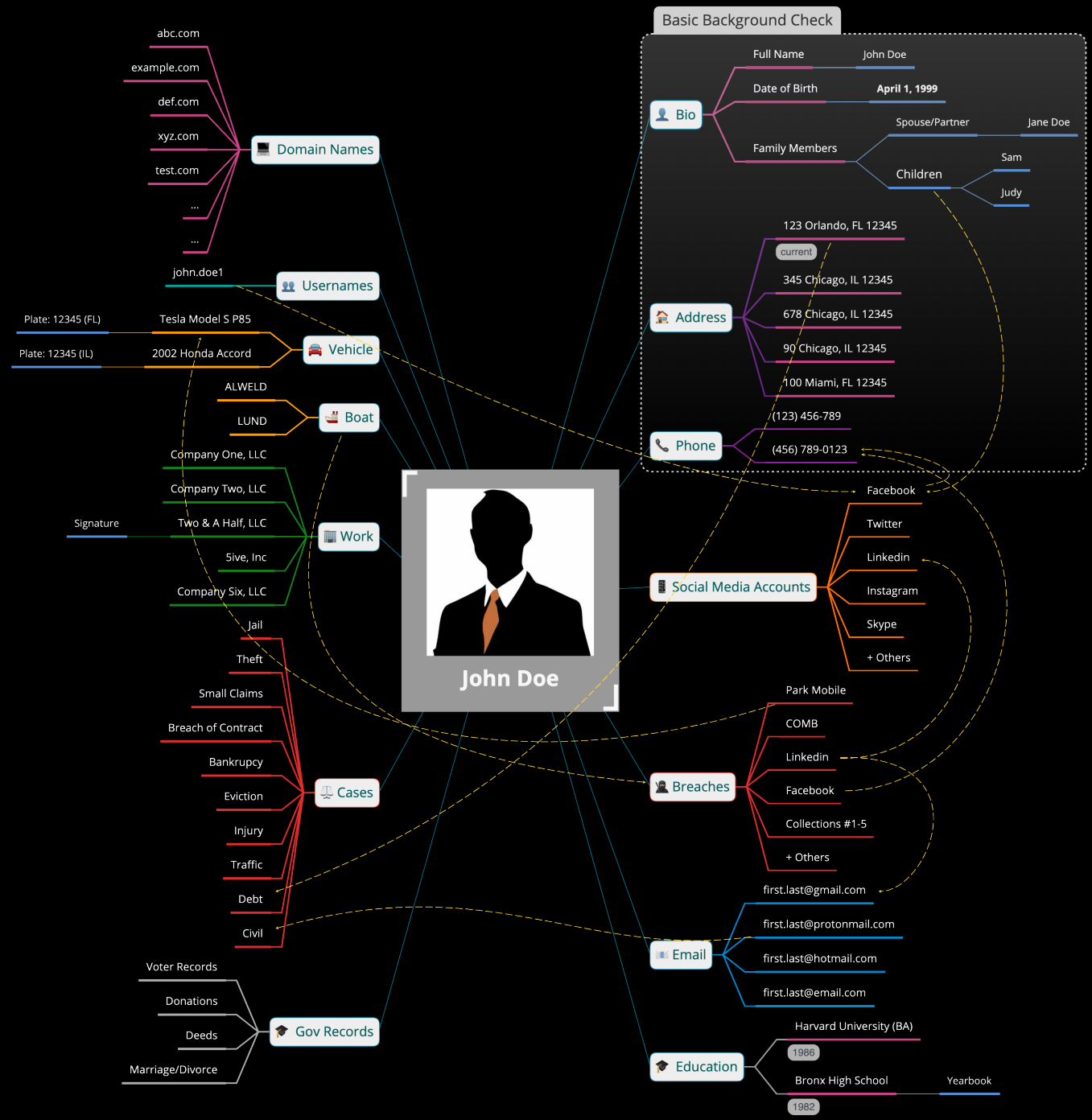
Not so common breached data

- US Boat Owners
- Voter Database
- Divorce Records
- Porn Sites
- Banks
- Experian
- Bitcoin Talk
- Guns.com
- Ashley Madison
- Park Mobile (Plate #)

The Goal

(Due Diligence)

The Bigger Picture



The Tools

OSINT like a hacker

(Beyond Googling)

[Next Level OSINT]

- Kali Linux
- Ask the gov!
  - ✓ Voter registration
- Historical Data
  - ✓ Archive.org
  - ✓ whoxy.com
  - ✓ Street View
- Fooling IVRs
  - ✓ Utility companies
- Extract Data from APIs
- Extracting paid data indirectly
  - ✓ Insurance providers

Kali Linux

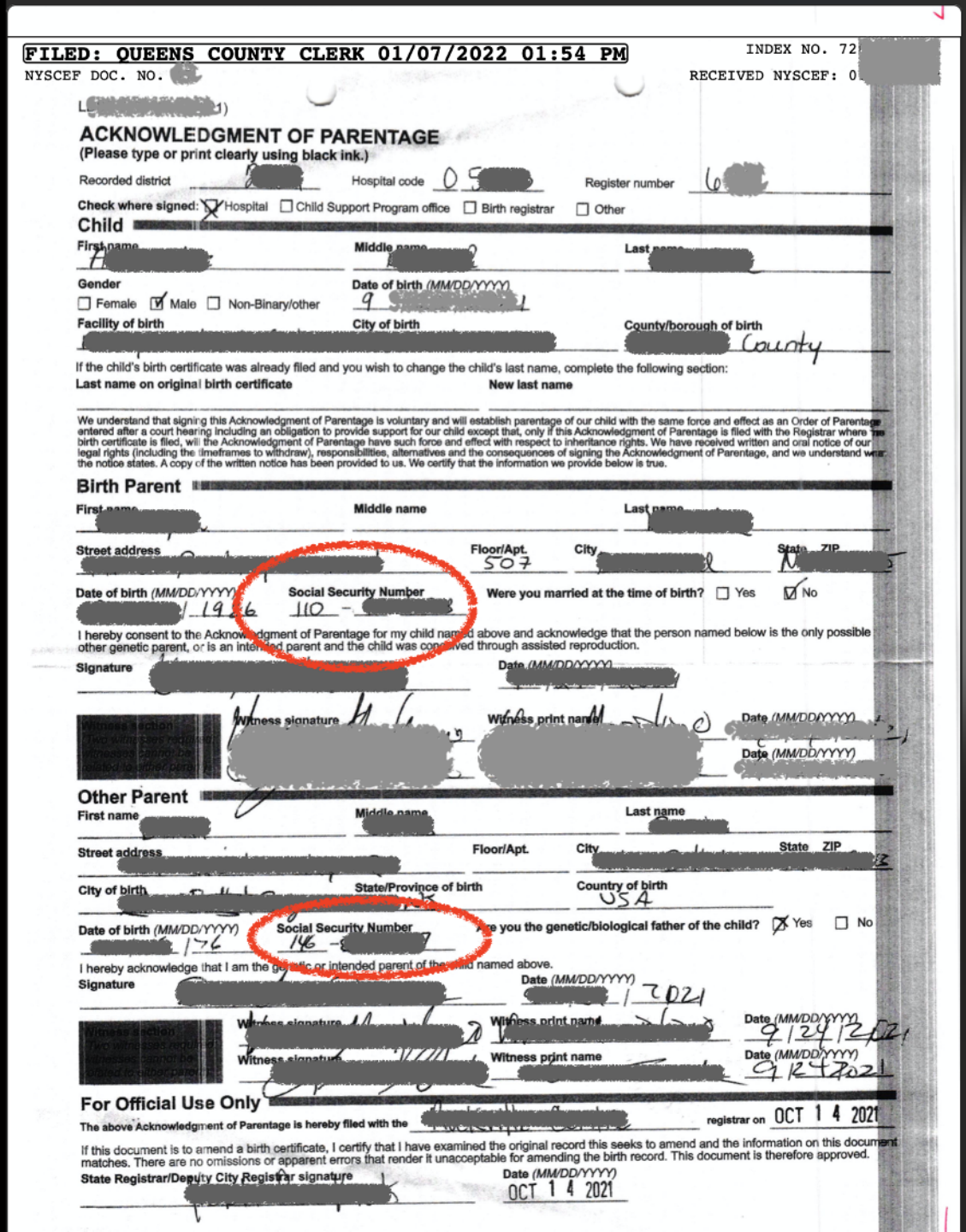
Technical tools for OSINT

(BurpSuite, Holehe, Toutatis, Hashcat)

[Live Demo]

Just ask the gov

(Public Court Records)



FILED: QUEENS COUNTY CLERK 01/07/2022 01:54 PM INDEX NO. 72[redacted]
NYSCEF DOC. NO. [redacted] RECEIVED NYSCEF: 0[redacted]

ACKNOWLEDGMENT OF PARENTAGE
(Please type or print clearly using black ink.)

Recorded district [redacted] Hospital code 05[redacted] Register number 6[redacted]

Check where signed: ☒ Hospital ☐ Child Support Program office ☐ Birth registrar ☐ Other

Child

First name [redacted] Middle name [redacted] Last name [redacted]

Gender ☐ Female ☑ Male ☐ Non-Binary/other Date of birth (MM/DD/YYYY) 9[redacted]

Facility of birth [redacted] City of birth [redacted] County/borough of birth [redacted] County

If the child's birth certificate was already filed and you wish to change the child's last name, complete the following section:

Last name on original birth certificate New last name

We understand that signing this Acknowledgment of Parentage is voluntary and will establish parentage of our child with the same force and effect as an Order of Parentage entered after a court hearing including an obligation to provide support for our child except that, only if this Acknowledgment of Parentage is filed with the Registrar where the birth certificate is filed, will the Acknowledgment of Parentage have such force and effect with respect to inheritance rights. We have received written and oral notice of our legal rights (including the timeframes to withdraw), responsibilities, alternatives and the consequences of signing the Acknowledgment of Parentage, and we understand what the notice states. A copy of the written notice has been provided to us. We certify that the information we provide below is true.

Birth Parent

First name [redacted] Middle name [redacted] Last name [redacted]

Street address [redacted] Floor/Apt. 507 City [redacted] State [redacted] ZIP [redacted]

Date of birth (MM/DD/YYYY) [redacted]/1976 Social Security Number 110-[redacted] Were you married at the time of birth? ☐ Yes ☑ No

I hereby consent to the Acknowledgment of Parentage for my child named above and acknowledge that the person named below is the only possible other genetic parent, or is an intended parent and the child was conceived through assisted reproduction.

Signature [redacted] Date (MM/DD/YYYY) [redacted]

Witness section Witness signature [redacted] Witness print name [redacted] Date (MM/DD/YYYY) [redacted]

Witness signature [redacted] Date (MM/DD/YYYY) [redacted]

Other Parent

First name [redacted] Middle name [redacted] Last name [redacted]

Street address [redacted] Floor/Apt. [redacted] City [redacted] State [redacted] ZIP [redacted]

City of birth [redacted] State/Province of birth [redacted] Country of birth USA

Date of birth (MM/DD/YYYY) [redacted] Social Security Number 146-[redacted] Are you the genetic/biological father of the child? ☒ Yes ☐ No

I hereby acknowledge that I am the genetic or intended parent of the child named above.

Signature [redacted] Date (MM/DD/YYYY) [redacted]/2021

Witness section Witness signature [redacted] Witness print name [redacted] Date (MM/DD/YYYY) 9/24/2021

Witness signature [redacted] Witness print name [redacted] Date (MM/DD/YYYY) 9/24/2021

For Official Use Only

The above Acknowledgment of Parentage is hereby filed with the [redacted] registrar on OCT 14 2021

If this document is to amend a birth certificate, I certify that I have examined the original record this seeks to amend and the information on this document matches. There are no omissions or apparent errors that render it unacceptable for amending the birth record. This document is therefore approved.

State Registrar/Deputy City Registrar signature [redacted] Date (MM/DD/YYYY) OCT 14 2021

Historical Data

The internet never forgets

(whoxy.com, archive.org, Google Street View)

[Live Demo]

Paid/Private Data

Indirectly

(Insurance providers)

[Live Demo]

Xfinity

☎️ IVR Exploitation

(Like stealing data 🍭 from a bot 🤖)

[Demo] 

API

Extracting Data

(GitHub)

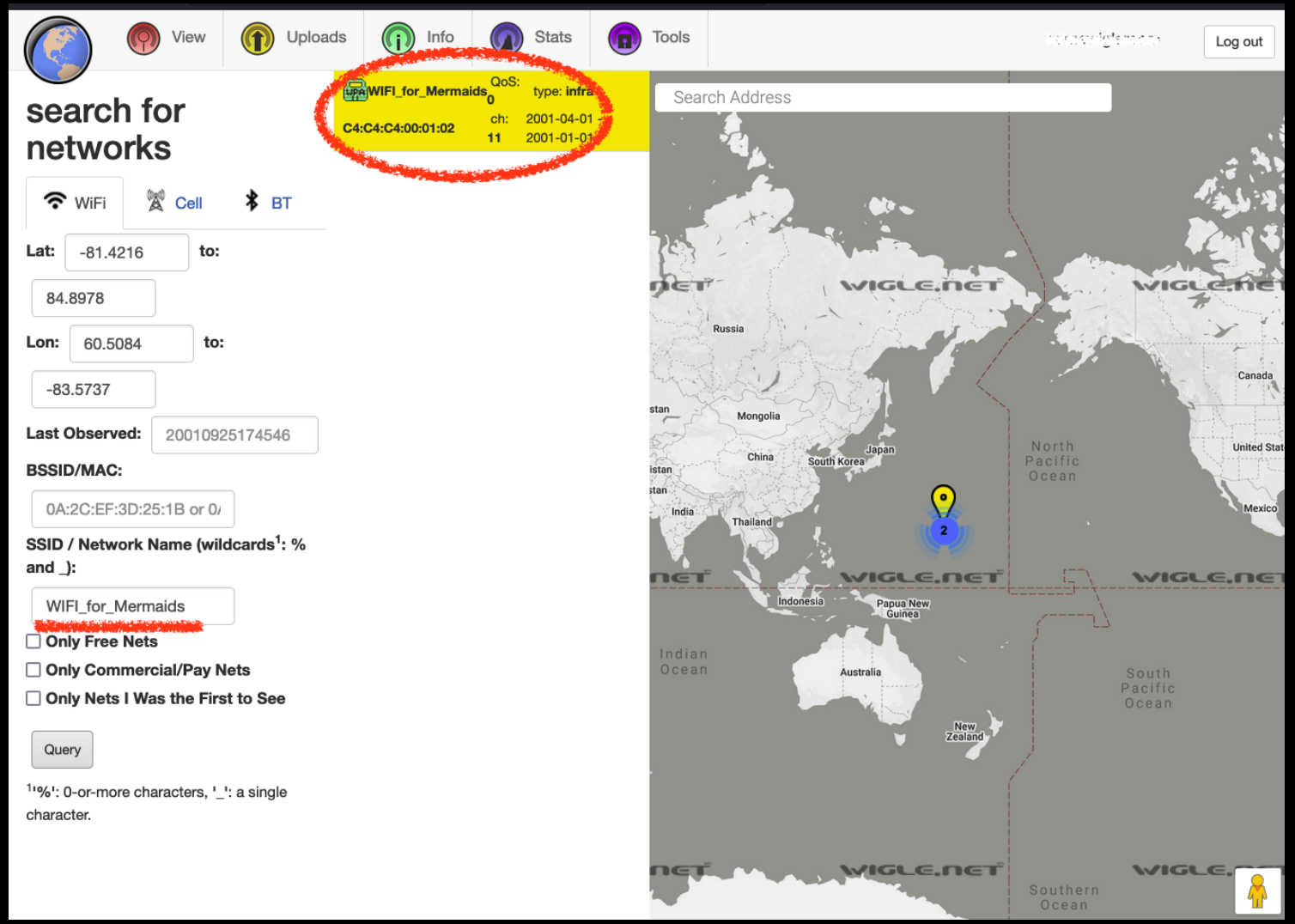
[Live Demo]

Verify

(Don’t believe everything you see on the internet)

Mermaids Exist

(Disinformation)



[Next Level OSINT]

- Kali Linux
- Ask the gov!
  - ✓ Voter registration
- Historical Data
  - ✓ Archive.org
  - ✓ whoxy.com
  - ✓ Street View
- Fooling IVRs
  - ✓ Utility companies
- Extract Data from APIs
- Extracting paid data indirectly
  - ✓ Insurance providers

Pivoting (OSINT)

- Email Existence
  - Legitimacy
  - Age of account
  - Interests
- Password Reuse
- Phone number mapping
- Vehicles
- Historical Records (scrapes, whois)
- IPs (location, ISP)
- Hidden Accounts
- Unmasking

[Thank You]