NullSweep
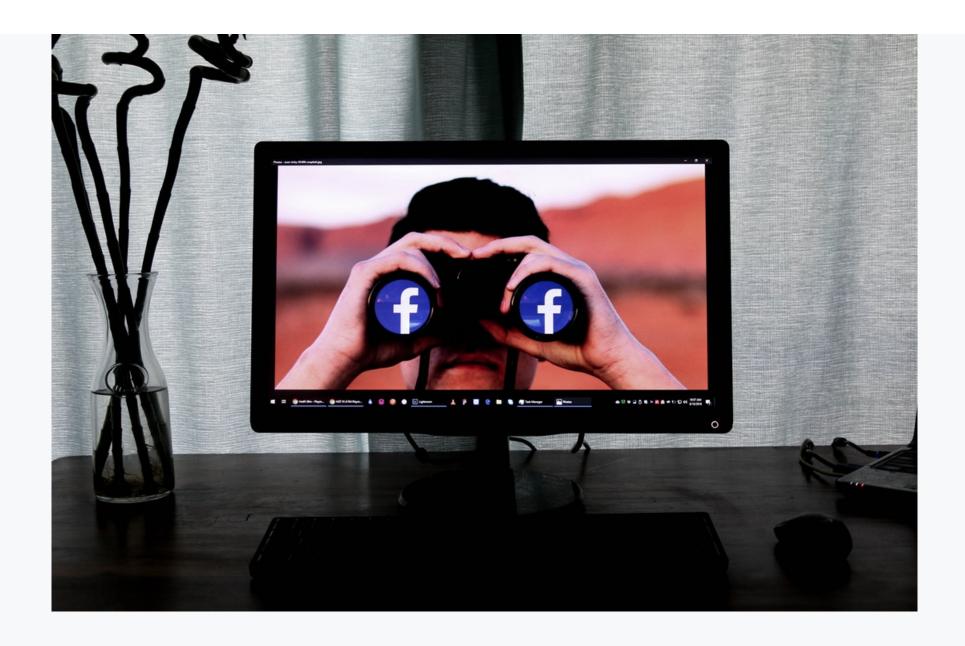
Continuous Security, DevOps, and DevSecOps

Digging Through Someones Past Using OSINT

Posted on 13 March 2019

Recently, a distant cousin reached out to me for help in researching a persons history. My

cousin's father had met and gotten engaged to a woman who my cousin thought was trying to steal from him. After starting this relationship, he started to change his behavior - pushing away his three children, asking for money he had never asked for before (such as returning money spent on education), and generally causing them worry and suspicion about this new person in his life.

I am not an expert in people searching by any means, but I have done some in the past. My cousin asked if I could try to use "hacking" to dig up some information about this woman that might lend some credence to their fears. After I agreed to search (using OSINT, or open source intelligence and not any hacking), he gave me the following sketchy details:

- The woman's name as he knew it. He had never met her.
- The fact that within 3 months she had met his father online via a dating website, moved into his house from somewhere in Utah, and become engaged.
- That she had two previous husbands who had both died soon after marrying her.
- She was masquerading as "rich"
- She was telling the father that the children were unstable and should not be trusted.
- She claimed to be a licensed psychologist (retired).
- She was in her fifties (and the father is in his eighties)

In this post, I'll outline the methods I used to find out this persons personal details from the above, as well as my findings. I have changed all the identifying information in this post,

though the methods remain accurate.

though the methods remain accurate.

Finding Her Social Profiles

The name I was given was Jen X, and I only knew the state she supposedly moved from. When all you have to go on is a real name, the first place to start is with all the (mostly junky) people search sites and social networks.

Searching `"Jen X" UT facebook` in Google and `"Jen X" UT linkedin` led me to a series of possible profiles. I started with LinkedIn because I knew she was supposed to be a psychologist and that might help me narrow it down. Sure enough, one of the profiles was a person of about the right age, living in payson UT, with profession of psychiatrist.

There was a single photo, it looked like a selfie. I used the Firefox Plugin Image Search Options to run multiple reverse image searches hoping to find other profiles that used the same image, but none of them found any results. I saved a screencap of the profile and moved on.

Next up I started looking through the facebook profiles. I immediately saw a profile with the same profile picture, but a different town - Santaquin, UT. Looking this town up on a map, it

was pretty close to Payson, so I copied this location down as well and started looking at her profile.

profile.

Like her linked in, it was locked down and empty of information. A single wall post of an image, with one like, and no other information visible.

At this point, I searched several other social sites without any results. I wanted to get whatever information FB had, so I looked at who had liked her post. It was another woman who had a more open profile. I quickly took this friends profile, and created a replica fake profile that I used to send a fake friend request to Jen. If she accepted, I would be able to view her profile details.

I checked the chrome plugin Prophet to try and locate other social profiles, but it didn't find anything in this case.

Using Person Search

There are about 40 people search sites that I know of, and most of them are pretty terrible. They are full of ads, false positives, and try to sell you access to any (mostly wrong) information they can find.

I stared searching for Jennifer X of around age 55 in UT, but I wasn't getting any matches. At this point, my bias was to assume a fake name for fraud, but I also know that is unlikely if the

fraud involved marriage, since the name would have to be real to have anything be legally binding.

I tried each search again with just Jen instead of Jennifer and Radiaris was the only one to find an interesting hit: Imogen (Jen) X of Payson UT at age 76. The details were different from what I had expected - the woman matched was older than I expected by almost 20 years, but had the right town. Imogen is an unusual but valid full name for the nickname Jen. On a hunch, I used this new name on every person search site again and finally found proper matches.

Collecting the information each site shows for free, I was able to piece together some interesting information:

- First name, last name, two potential middle initials
- An address in both Payson and Santaquin, which boosted my confidence that this was the same person.
- A list of relatives
- 10+ previous town/state combinations lived
- prefixes and suffixes for email and phone numbers

A pretty good list! Now that I have a couple of addresses, I can do some more digging.

Public Records

Public record searches can be challenging because every county has a different way of searching (and some don't even have online access), but a great site to see what's available is BlackBook Online, which provides links to various county search sites.

I was able to look up the address I had gotten and found property records for Jen, listing her home assessed value, full name (first, middle, last, and a fourth name). I then went over to Zillow to check the property and found the sales history (letting me know when the house was purchased and for how much). The property was last sold in 2011.

Going on to the second address and doing the same search, it was owned by an unrelated party, and Zillow showed no recent sales. I would guess this meant that the second address was likely a rental.

The owned home had a total value of less than $100k and was a single story home with only a small bedroom and combined kitchen/living area, meaning her claim of being "rich" was probably false.

Summary of Information so far

At this point I had the following information after just a few searches:

At this point I had the following information after just a few searches:

- Full name - first, middle, last, and another name. My background information indicated at least two marriages, so I make the assumption that the fourth name is either a maiden name or a previous marriage. Same with the middle name.
- Two recent addresses a few miles apart
- Profession
- Facebook and LinkedIn profile pages, neither with much information publicly shared.
- Potential relative names
- Partial email and phone number records
- Rough outline of assets based on home sale information, indicating some assets (home equity) but nothing substantial.
- Correct age (but not birthdate yet)
- Where she received her degree

I was concerned about the discussions about husband death and behavior change, so I wanted to find out more about her past husbands and their information. With the full name information and address data, I can start finding out their names and details

Back to People Search

From the property record, I now had a name Imogen X Y Z. Two new last names to check! Running back through people searches with each of two new names I found some more

interesting information. The following information was pieced together from multiple search site results for each name, as well as people search results for the names of the husbands I found:

- Names of two previous husbands, one of which shared the rented property for years with Jen, and one of which shared the current owned property.
- List of addresses husbands each lived at. The first husband, who shared her currently used last name, had a long list of locations that matched Jens going back decades.
- Extended families for both husbands, including a likely child of Jen
- IP address for rental property (yes, some people search sites will return IP address information!)
- Phone number for rental property
- Email address (from an ISP "jennibell19")

Armed with more details about the husbands, I could try to learn how they died and when they were married. Death and Marriage records are difficult to come by - sometimes they are posted online or in various places, but public records need to be requested formally and are often denied to non-family members. I wasn't willing to do that in this case anyway.

Google Searching the Husbands

If you have read my other posts, you'll know I don't use Google for search, but this is an exception. When doing things that require what's known as "Google hacking", or searching

exception. When doing things that require what's known as "Google hacking", or searching using advanced search tools and commands, I haven't found an alternative that does nearly as well.

I searched google for the husbands, using queries like the below. Putting the name in quotes ensures that Google won't match on other similar names. Sometimes with common names I will find someone who looks similar, but isn't the target. Using "-keyword" will help filter out those results.

- "first last" obituary
- "first last" town name obituary
- "first last" "town name" death/died/sorrow/service/etc.
- "first last" "town name" -keyword -keyword (where keywords are items that came up for other matches who are not the target)
- Try modifying first name in the above for common nick names

I was able to find obituary's for the latest husband. They confirmed that he died about 6

months before Jen met my cousins father, but I couldn't find details about the cause of death.

The first husband had no obituaries that I could find, and appears to be still alive. I switched my searches to look for divorce (sometimes people will post using their names on forums), but couldn't find anything conclusive there either. It seems like perhaps she was lying to my cousins father about having two passed on husbands, but I didn't have confirmation.

Facebook Friend Request Accepted

Around this time, I noticed that I had a new facebook notification with my fake profile - Jen had accepted my friend request and sent me a message!

Now with full access to her information (and a fair amount of access to her friends information), I could gather some additional details. She was not a significant user, so I gleaned less from this profile than I might have hoped. Still, I found a few interesting tidbits:

- List of friends / contacts frequently posted to
- Facebook join date (in 2018 - somewhat close to the time of meeting the father)

- Exact birth date
- Phone number (cellular)
- A few posts revealing a desire to "escape" or be "saved" from her current location along with her adult children

A few things I did not find that I had hoped to:

- Additional images for reverse image search (She only has her profile photo)
- Conversation history related to past relationships

- Conversation related to current relationship (cousins dad was not on her friend list, oddly enough)

Searching the remaining open leads

I was wrapping up my investigation about this time, not wanting to spend too much more effort, but there were still a few things I wanted to search on. I also did the following:

- Check past location history for public psychology credentials and licenses. I couldn't confirm in any online license database that Jen is a licensed Psychologist, though most only go back 5-10 years, meaning her retirement could easily have come before the record history.

- Search dating sites for her profiles. I knew she was first met on a dating website, but I didn't have any luck finding more than the original dating profile.
- Exact details of the terms of split with the first husband, which I couldn't find to my satisfaction without further effort.
- Data Breach information. Dehashed is a great site for finding breach data. This can help confirm an email and show sites that might have more information on a person. I don't believe the ISP email I have is her primary email, but dehashed does show linkedin and a couple of other sites.
- Criminal search in each place she has lived. No criminal records were found.

Wrapping up the investigation

In the end, I didn't find anything definitively incriminating. She seems like a normal person to me, with a smaller online presence than most people. Either she does not use social media extensively (possible due to her age) or a careful amount of curation, which seems likely given her existing profiles.

In summary, here is what I was able to collect given my initial information:

- Full name and property records
- Full address history, going back to at least college
- Details of her two ex-husbands, including one death
- Basic asset information about owned property
- email address
- phone number
- birthday
- previous names
- names of schools she attended
- Several IP addresses

With the details I was able to find, I did not find anything that is an immediate red flag. I did find a few items that are concerning, but not directly a problem:

- FB, dating profile, and linkedIn profiles all seem to be started around the same time in 2018. I find it odd to create everything just a couple of months before meeting a match, though this may be due to her re-entering the dating pool and trying these sites for the first time.
- Couldn't confirm the death of her first husband.
- She had a couple of FB updates that sounded like she was searching for someone to "take her and her kids away" from where she had been living.

In any case, I handed over some of this info to my cousin, though it isn't all that helpful in confirming or denying his fears.

OSINT can be used to find a lot more

I am an amateur at OSINT and people finding. Finding this information and much more only takes a certain amount of effort.

If you are interested in this topic, I can't recommend Michael Bazzell's book Open Source Intelligence Techniques enough. It is the main source I used in my investigation, along with the OSINT tools on his website.

If you want to prevent searches like this, he also has many resources for hiding public

records and making such searches much more difficult.

Charlie Belmer

USA

I live for privacy, security, and online freedom because these are the building blocks of a better society, one I want to help create.

Tagged with: osint, privacy, Technical Guides

Comments

This comment system is self hosted using the Mozilla Coral talk platform, and not connected with any third parties who might collect data. At any time, you can completely delete all comments and data stored, including your email address. I will never send you emails aside from password reset emails you request.

Comments

All Comments 1

Viewing Options ▾

melba 1 month ago

This article is extremely helpful to me in my business when making difficult hiring decisions.

Respect 👁️‍🗨️   Reply ↩

Share 🔗   Report 🚩

←Personal Security & Privacy Tools I Recommend

Launching the Mozilla Plugin Privacy Test Database→