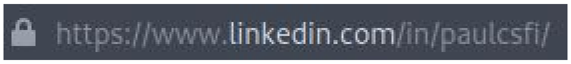
LinkedIn OSINT Techniques: Part I

LinkedIn remains the go-to social media platform for job hunters and recruiters alike. Due to the nature of the platform and the high value of potentially landing a new gig, most users found on the website are providing, intentionally or not, real and attributable information about themselves. Investigators have a wealth of information that is often verifiable with little difficulty. Users walk a fine line between giving out too little information, or giving out too much information which may be detrimental to their, online and physical, safety and privacy.

This guide will contain two sections with this first iteration focusing on some of the "quick hits" that can be found on a user that might not have a fully fleshed out account. The second guide will focus more on exploiting experience, positions, and other information found in a more robust LinkedIn account.

URL

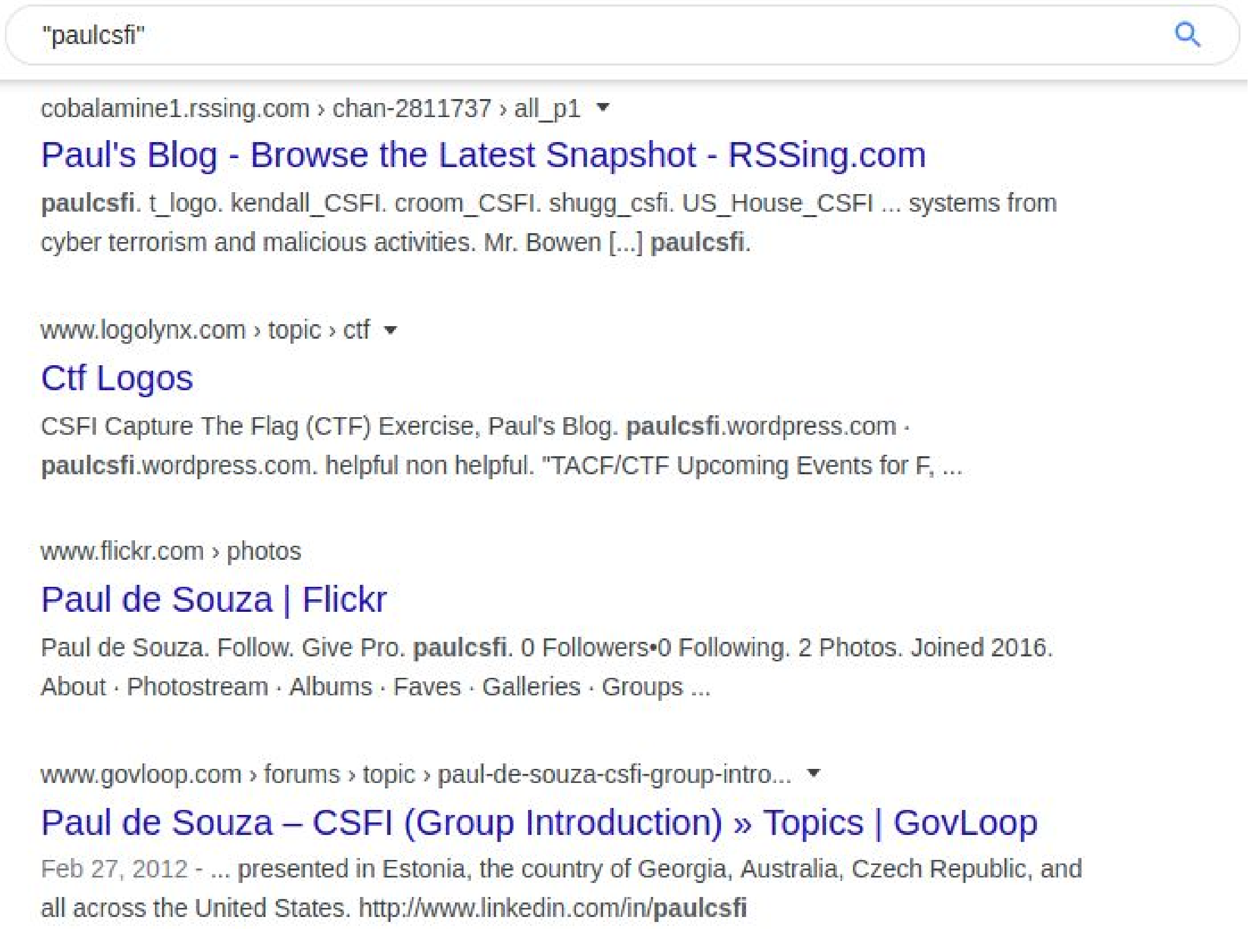


https://www.linkedin.com/in/paulcsfi/

The URL associated with a LinkedIn profile will always be available by default, however it will not always provide exploitable information. By default, a URL will be generated from the first and last name of the account. Unlike other platforms, this URL will automatically update when users change the first or last name on the account. Unfortunately for accounts that only show the initial of the last name, this usually does not uncover the full last name unless they have customized their URL to include it.

Users may create these "custom" URLs (linkedin.com/in/#USERNAME) for their account which is more easily remembered, doesn't change with each name change, and can be treated just like you would treat a username in many cases.

Our above example is a custom URL pulled from a LinkedIn account that can be treated like a username. Running this through Google uncovered a number of additional platforms to look into for information gathering. The results provide us with personal blogs and other information that provides easy jumping off points on our target due to the reuse of this URL as their username on other platforms.



"paulcsfi"

cobalamine1.rssing.com › chan-2811737 › all_p1

Paul's Blog - Browse the Latest Snapshot - RSSing.com

paulcsfi. t_logo. kendall_CSFI. croom_CSFI. shugg_csfi. US_House_CSFI ... systems from cyber terrorism and malicious activities. Mr. Bowen [...] **paulcsfi**.

www.logolynx.com › topic › ctf

Ctf Logos

CSFI Capture The Flag (CTF) Exercise, Paul's Blog. **paulcsfi**.wordpress.com · **paulcsfi**.wordpress.com. helpful non helpful. "TACF/CTF Upcoming Events for F, ...

www.flickr.com › photos

Paul de Souza | Flickr

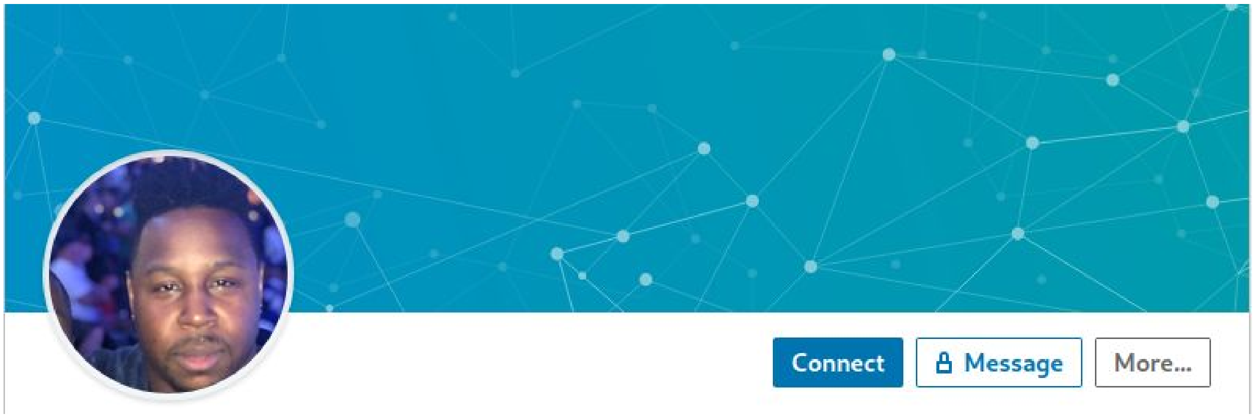
Paul de Souza. Follow. Give Pro. **paulcsfi**. 0 Followers•0 Following. 2 Photos. Joined 2016. About · Photostream · Albums · Faves · Galleries · Groups ...

www.govloop.com › forums › topic › paul-de-souza-csfi-group-intro...

Paul de Souza – CSFI (Group Introduction) » Topics | GovLoop

Feb 27, 2012 - ... presented in Estonia, the country of Georgia, Australia, Czech Republic, and all across the United States. http://www.linkedin.com/in/**paulcsfi**

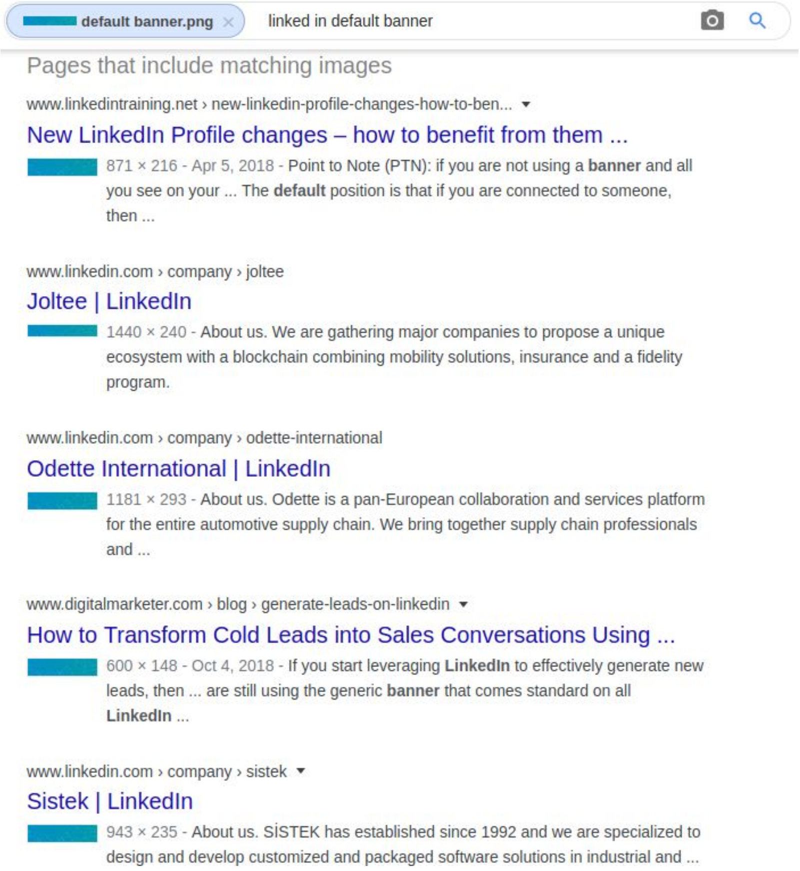
Banner Photo



Like many other social media sites, LinkedIn allows its users to upload a large photo at the top of their page to act as a banner or cover photo. This banner can be exploited like any other photo with reverse image searches to see if the user also uploaded it to another site. I must note that it appears LinkedIn does strip any pertinent metadata from photos and other files uploaded to the site, so no EXIF data will assist you here.

Banner photos can also be analyzed for any relevant information that might appear in the photo, such as the user's workspace, industry-specific equipment, notable locations or office spaces, etc. There is no need for any special tool to view the image, simply right click the banner and click view-image. Be advised that this does not work on the generic cover photo. At this time, I was unable to find any way to obtain the full-size banner photo uploaded by the user.

In our above example, our user has a banner photo, however it is one created by default for users that have not yet uploaded their own. Doing a reverse image search on the image returns a large number of other LinkedIn accounts with the same default image. Although this is a dead-end, it is good for investigators to familiarize themselves with any default images so they do not chase leads that go nowhere.



default banner.png linked in default banner

Pages that include matching images

www.linkedintraining.net › new-linkedin-profile-changes-how-to-ben...

New LinkedIn Profile changes – how to benefit from them ...

871 × 216 - Apr 5, 2018 - Point to Note (PTN): if you are not using a **banner** and all you see on your ... The **default** position is that if you are connected to someone, then ...

www.linkedin.com › company › joltee

Joltee | LinkedIn

1440 × 240 - About us. We are gathering major companies to propose a unique ecosystem with a blockchain combining mobility solutions, insurance and a fidelity program.

www.linkedin.com › company › odette-international

Odette International | LinkedIn

1181 × 293 - About us. Odette is a pan-European collaboration and services platform for the entire automotive supply chain. We bring together supply chain professionals and ...

www.digitalmarketer.com › blog › generate-leads-on-linkedin

How to Transform Cold Leads into Sales Conversations Using ...

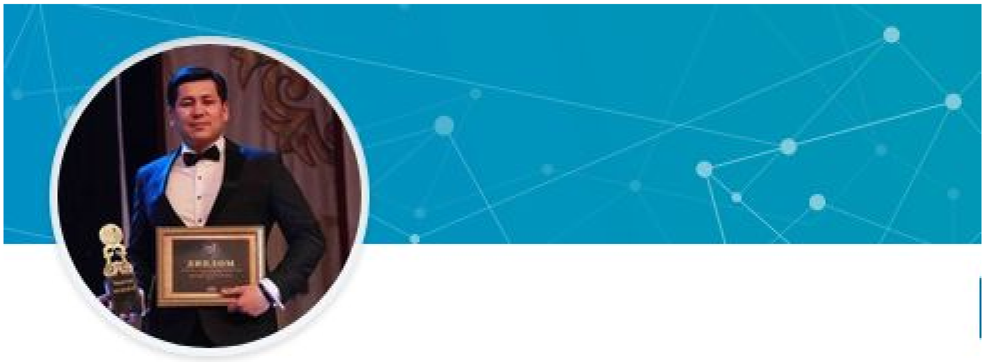
600 × 148 - Oct 4, 2018 - If you start leveraging **LinkedIn** to effectively generate new leads, then ... are still using the generic **banner** that comes standard on all **LinkedIn** ...

www.linkedin.com › company › sistek

Sistek | LinkedIn

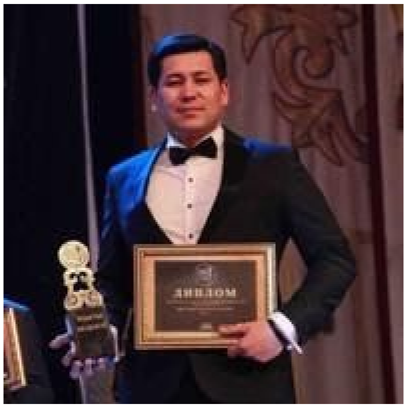
943 × 235 - About us. SİSTEK has established since 1992 and we are specialized to design and develop customized and packaged software solutions in industrial and ...

Profile Photo

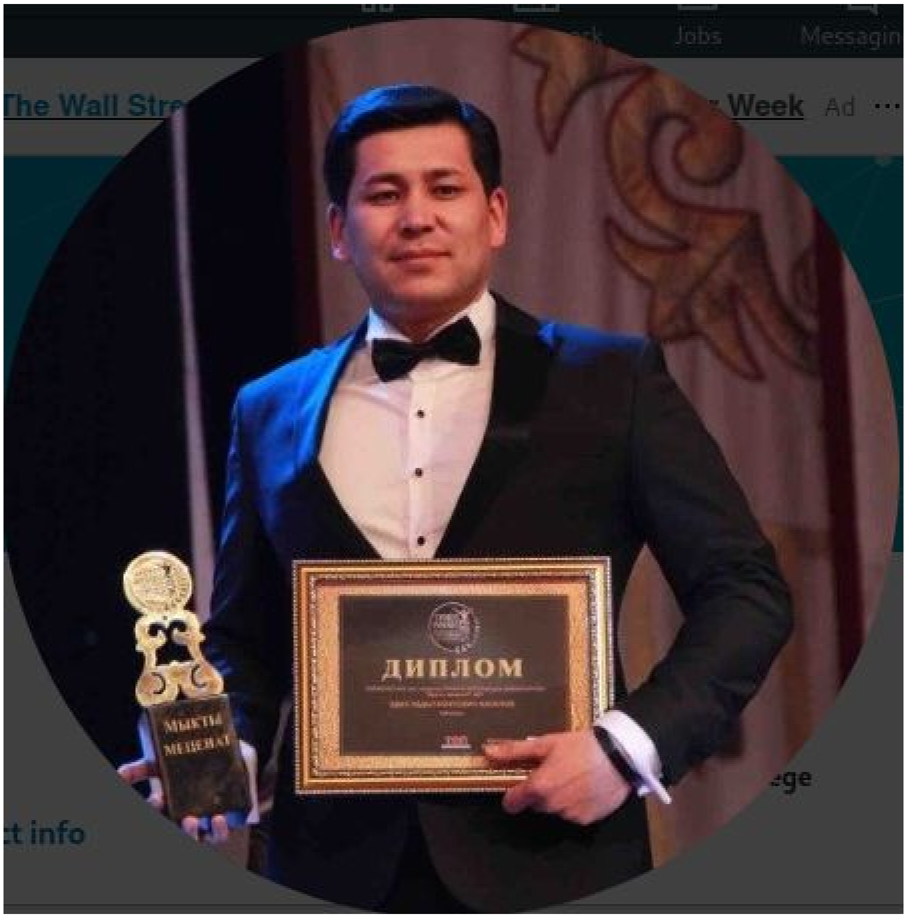


On the left side and below the banner photo will be the user's profile photo. Profile photos help us identify the person behind the account. Although it is usually considered poor OPSEC to upload a personal photo of yourself behind an online handle on most sites, many LinkedIn users freely put their faces out there. Be wary of AI-generated profile photos as well as those that may be stock images or pulled from elsewhere. Usually, a bit of sleuthing coupled with reverse image searches can clear up most cases and may help you find other places online the subject might have used it. Additionally, be sure to look for clues within the background or on other items within the photo that might help drive the investigation.

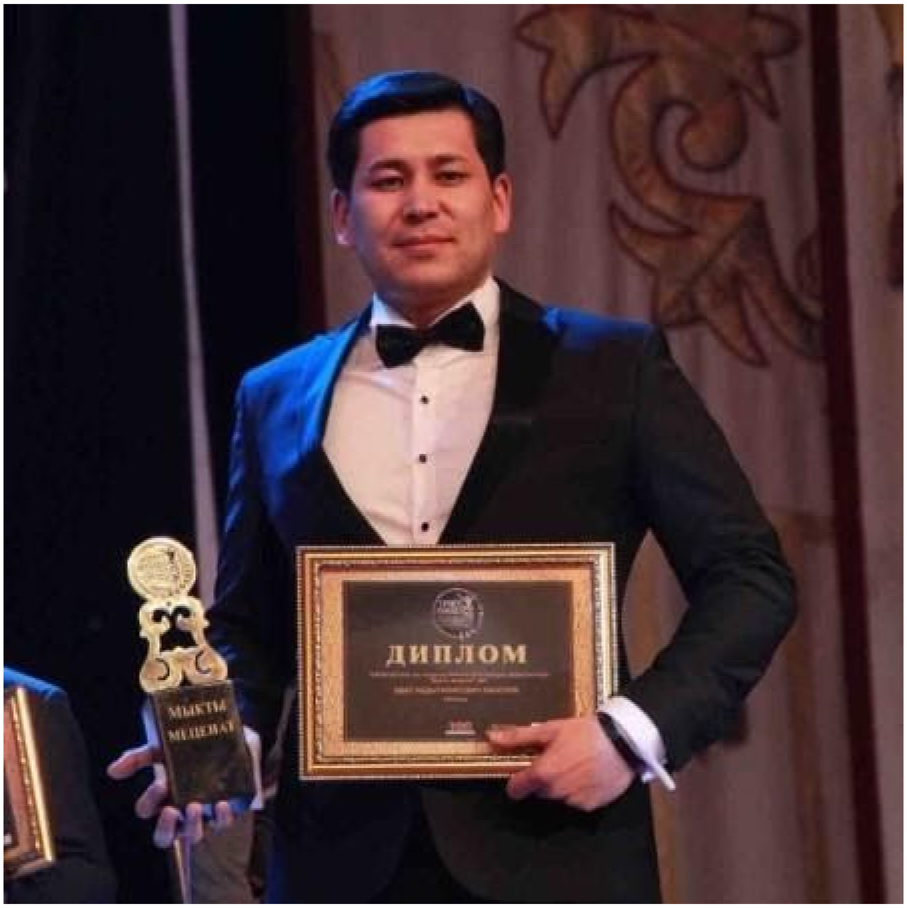
Using our above target as an example, we will see what information we can extract from only his profile photo. With all photos, we always want to obtain the largest, uncropped version of the photo as we can. Right-clicking on the photo and selecting "View Image" will give the below image.



We now have the uncropped version, but what if we needed a larger version, perhaps something where we needed to visually inspect details in the background, or in this example perhaps the text on the awards? We can navigate back to the profile and add "/detail/photo/" to the end of the URL. (ex https://www.linkedin.com/in/davidcameronofficial/detail/photo/) This will open up a larger version of the photo similar to the one below.

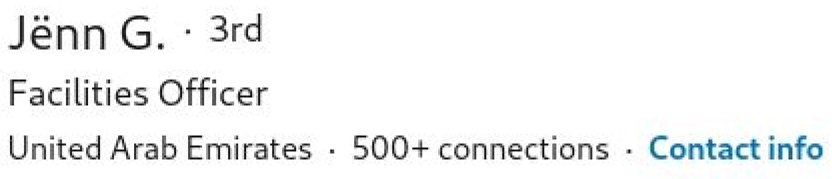


Much larger, but still cropped. Right-click this new photo and click “View Image” to finally get the below.



We can now get a better view of the awards, at least enough to attempt to translate some of the text. The large word on the certificate appears to be ДИПЛОМ (Diploma). I do not know enough about the language to make a reasonable guess regarding the text on the trophy. Knowing that the user has come from a country that using a cryllic script can help us narrow down our starting points.

Name (First, Last, Former)



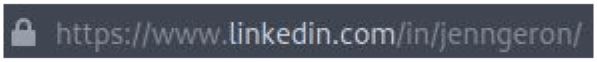
Jënn G. · 3rd

Facilities Officer

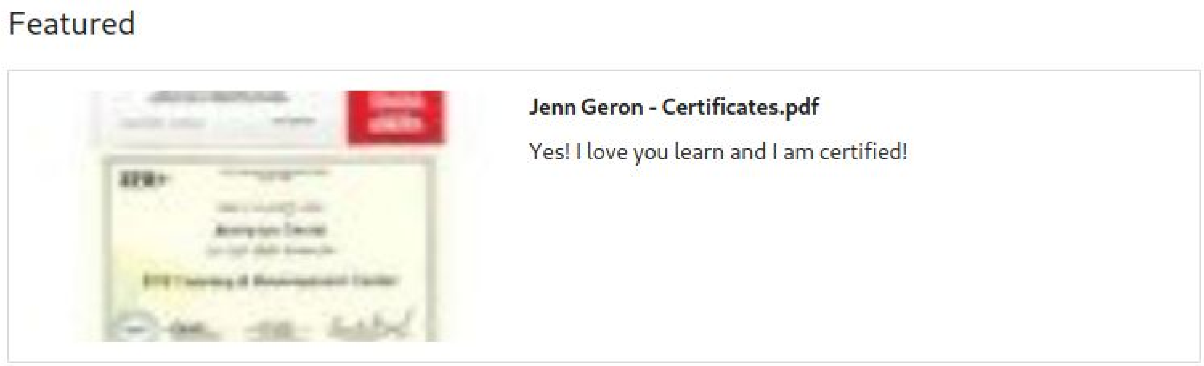
United Arab Emirates · 500+ connections · Contact info

All LinkedIn accounts will contain, at the very least, part of their first and last names that will appear directly below the profile photo. How much of a LinkedIn user's name you may view will depend on their privacy settings and whether or not you have any connection to the user. This can vary from very locked down (LinkedIn User) to partial (Full first name with only initial of last name) to fully open (Full first and last names). There is also the option to add a former name which is sometimes used for nicknames, online aliases, or perhaps maiden names. This does not appear as often, but when it does it will be displayed in parentheses. It is worth noting that the former name does not appear to contribute to anything in the URL structure like the first and last names do.

Our above example shows us a user who has their last name hidden due to their privacy settings. However, there are a few things we can look at to uncover the full last name. Firstly, looking at their custom URL, we can make an assumption regarding their last name.


https://www.linkedin.com/in/jenngeron/

But what if we wanted further confirmation, or perhaps we didn’t have a user with their last name visible in their custom URL? We could also look into the rest of their page and look for clues that might confirm the last name such as files, endorsements, etc.

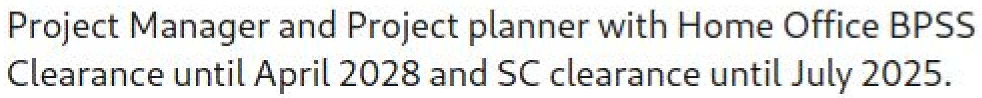

Featured

Jenn Geron - Certificates.pdf

Yes! I love you learn and I am certified!

The screenshot above comes from the same user’s profile. It appears that they left their first and last name as the filename in the pdf they uploaded, confirming our prior assumption. This example shows how inconsistent settings on an account can be useless for privacy if they do not lock down other areas as well.

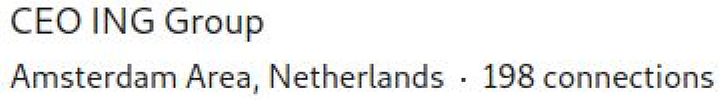
Headline


Project Manager and Project planner with Home Office BPSS Clearance until April 2028 and SC clearance until July 2025.

The headline will appear below the user’s name on a profile and is also a required field. By default, this will be pulled from the initial work or education information provided by the user on signup. This has to be edited separately from the work and education experience, which means that a user can delete their initial work or education experience and if they should forget to update their headline it may still contain this information. In addition to this initial headline, users may also edit this information to contain information that they want others to see first and foremost. This might include relevant professional certifications, security clearances, past or current work or school, etc.

The above user provides their current titles, however it is their security clearance information that is more interesting here. We can see that they have two related clearances that are specific to the British government. Without knowing the user's location information, we could generally assume that the user is in the United Kingdom or perhaps in an overseas territory or a friendly country. This drastically narrows our searching area.

Location



CEO ING Group

Amsterdam Area, Netherlands · 198 connections

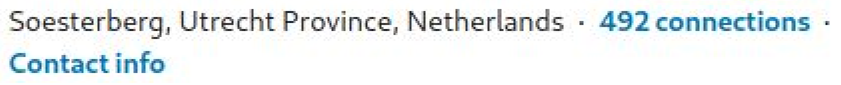
Below a user's headline and before their number of connections will be their location. This is another required field, though be sure not to put too much faith in this as users may choose whatever they wish here without any validation. Additionally, users may change this as they see fit any number of times. This can be as broad as the country or as defined as a city or metropolitan area. Your target's location data can easily help narrow down the field of potential matches to varying degrees, but should be verified utilizing other points on their profile when possible.

Unfortunately, the handy tricks for exploiting via zip codes appear to no longer be supported by LinkedIn. However, with a bit of research we can sometimes narrow down their location even further. Using our above example, we can see the user has set their location as "Amsterdam Area". Going off of the Amsterdam metropolitan area, we can see that this is quite a large area for searching, especially if we only have the information in the photo above to utilize. However, if we cross-reference the location with the user's title and company we can narrow that down to a much smaller area.

First, let's use their title to make a few assumptions. They are a CEO. Is a CEO likely to have their office at a small branch office? Unlikely. Are they going to live hours away by transit in the suburbs due to a lower salary or to save money? Possible, but also unlikely that they would be based too far away from their office. So we are assuming they are going to be near a major office and likely not too far out commuting wise.

Doing some quick research, it appears that ING Group has its headquarters in the South-East area of Amsterdam. A global headquarters would be a likely location for a CEO to have an office in. Knowing this we can start looking for information on our subject among people databases and look specifically for results that are within a reasonable commute from this office. This gives us a more narrow starting point than just “Amsterdam Area” which may contain multiple cities in the local commuting area.

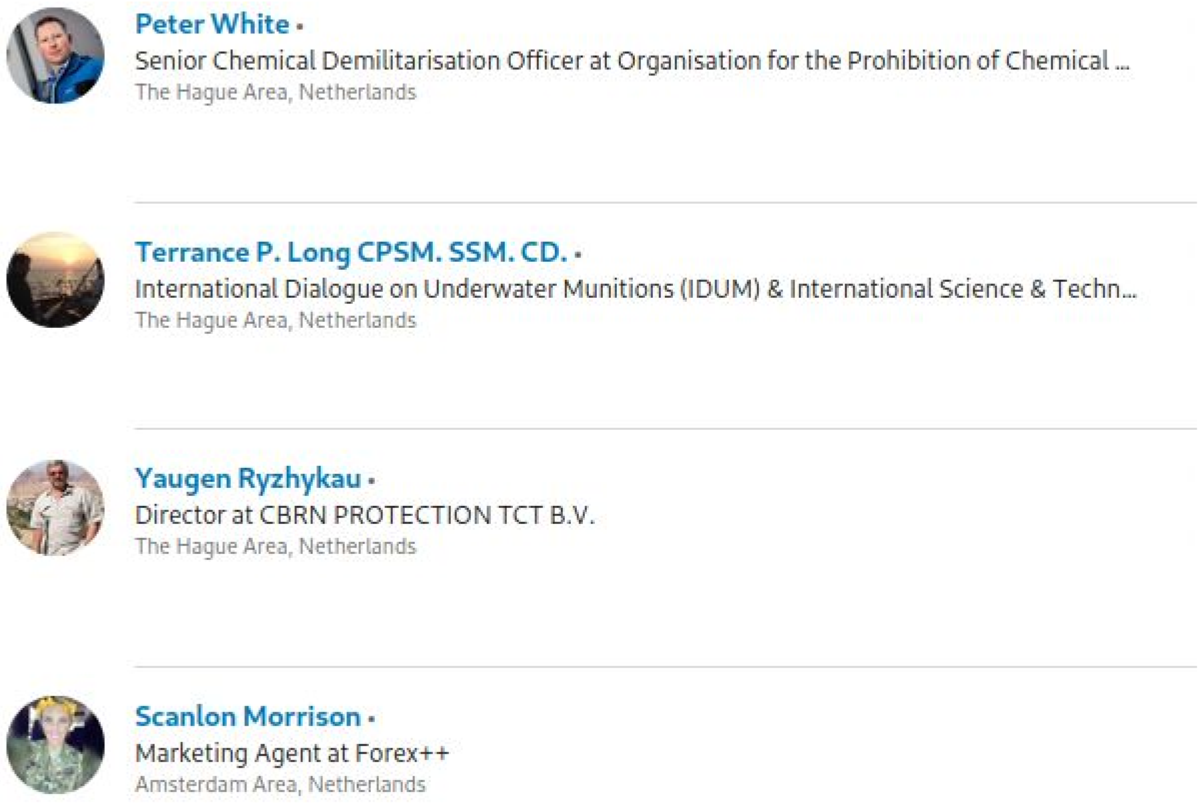
Connections



Soesterberg, Utrecht Province, Netherlands · 492 connections ·
Contact info

The number of connections will appear after the location information on a profile and may or may not be viewable depending on the target’s privacy settings and your connection to the target. By default, a target’s connections will be open to 1st-degree connections, so if possible be sure to connect with your target utilizing a well-crafted sock-puppet. If the information is viewable, investigators may click on the blue hyperlink to open the list of connections, otherwise it will appear as plain black text and not be clickable.

Clicking on the link in our above example, we can get a quick overview of all of the target’s connections. Below is a snapshot that summarizes them quite well in terms of location and field.



Peter White ·
Senior Chemical Demilitarisation Officer at Organisation for the Prohibition of Chemical ...
The Hague Area, Netherlands

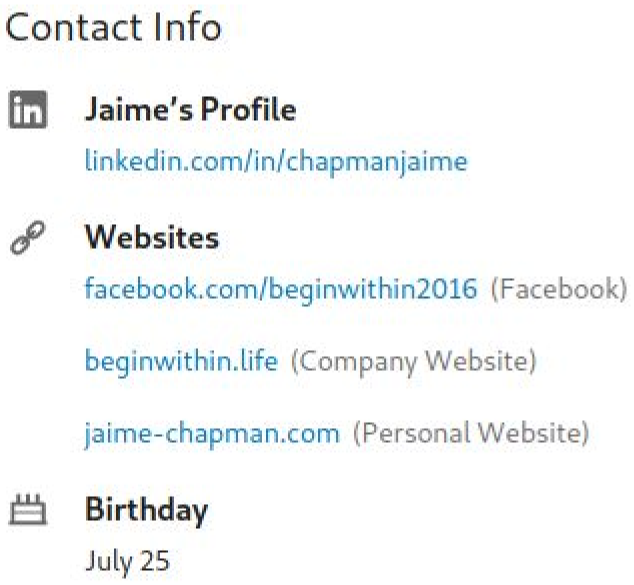
Terrance P. Long CPSM. SSM. CD. ·
International Dialogue on Underwater Munitions (IDUM) & International Science & Techn...
The Hague Area, Netherlands

Yaugen Ryzhykau ·
Director at CBRN PROTECTION TCT B.V.
The Hague Area, Netherlands

Scanlon Morrison ·
Marketing Agent at Forex++
Amsterdam Area, Netherlands

Based on their connections, we can assume that the user is likely based in the Netherlands as they state in their location. Additionally, looking at the positions of their connections, it appears that they likely come from a military background or are otherwise associated with CBRNE and related munitions work.

Contact Info



Contact Info

Jaime's Profile
linkedin.com/in/chapmanjaime

Websites
facebook.com/beginwithin2016 (Facebook)

beginwithin.life (Company Website)

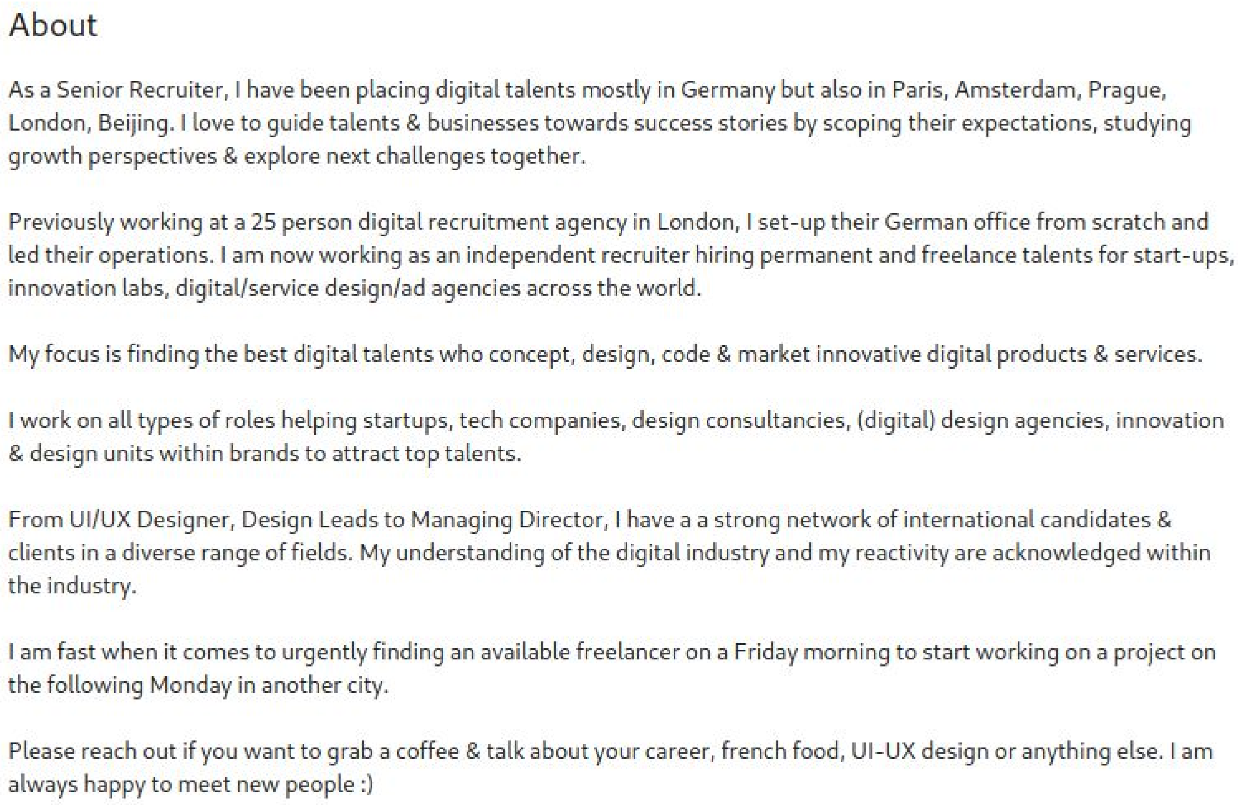
jaime-chapman.com (Personal Website)

Birthday
July 25

Following the location information will be a link to display a user's contact info that will display via a popup. Exploiting contact info can be hit or miss depending on the amount of information provided by the user and if you are a 1st-degree conneciton or not. Despite the name of this section, it may contain far more than just contact info. This section will contain, at the very least, the profile URL. It might also include the user's phone number, address, instant messaging handles, birthday, as well as URLs to their personal and professional websites. It is also worth noting that, by default, the LinkedIn email address is shared with all 1st-degree connections. Not everyone knows to change this so it might be beneficial to add a target if you are able to do so.

The target in our above example provides a number of websites and social media accounts that allow us to spider out and collect further information on them. Should we be searching our target of one of many people searching websites, we could use the birthdate given to narrow down our possible results.

About



About

As a Senior Recruiter, I have been placing digital talents mostly in Germany but also in Paris, Amsterdam, Prague, London, Beijing. I love to guide talents & businesses towards success stories by scoping their expectations, studying growth perspectives & explore next challenges together.

Previously working at a 25 person digital recruitment agency in London, I set-up their German office from scratch and led their operations. I am now working as an independent recruiter hiring permanent and freelance talents for start-ups, innovation labs, digital/service design/ad agencies across the world.

My focus is finding the best digital talents who concept, design, code & market innovative digital products & services.

I work on all types of roles helping startups, tech companies, design consultancies, (digital) design agencies, innovation & design units within brands to attract top talents.

From UI/UX Designer, Design Leads to Managing Director, I have a a strong network of international candidates & clients in a diverse range of fields. My understanding of the digital industry and my reactivity are acknowledged within the industry.

I am fast when it comes to urgently finding an available freelancer on a Friday morning to start working on a project on the following Monday in another city.

Please reach out if you want to grab a coffee & talk about your career, french food, UI-UX design or anything else. I am always happy to meet new people :)

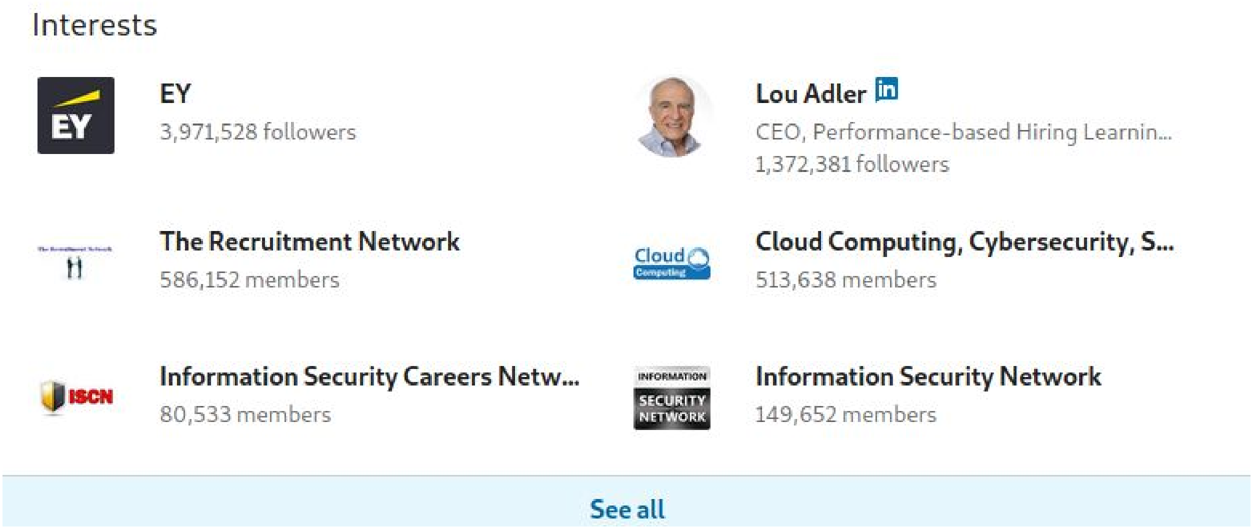
Some Linkedin profiles might contain additional information in their about section that does not occur further down in the experience section of the profile. Like the headline, this is a freetext area of the profile that allows a user to input anything that they feel pertinent to let other users know. For this reason, you might find valuable information such as URLs, alternative email addresses, additional pertinent locations, past and current work information, as well as hobbies, etc.

For users with robust about sections this might appear to look something like an objective or biography statement that might appear on the top of a resume, giving investigations a quick snapshot of a user and their background. Additionally, users may update this section more or less often than their education and experience section. This might result in differing, or even conflicting, information among these sections.

In our above example, we have a good example of a robust about section. This user states they are primarily based in Germany, but they have also placed talent in France, Netherlands, Czechia, UK, and China. They also state they were originally in a London-based agency and then went to the German one to stand it up. Knowing this, we would be able to start off looking for German-based data on the person, while also looking for British-based data for historical (and possibly family) data.

We would also know not to immediately cast out data coming from the other named countries as they have a history of work in those areas (although it appears to be remote).

Interests



Interests

EY
3,971,528 followers

Lou Adler
CEO, Performance-based Hiring Learnin...
1,372,381 followers

The Recruitment Network
586,152 members

Cloud Computing, Cybersecurity, S...
513,638 members

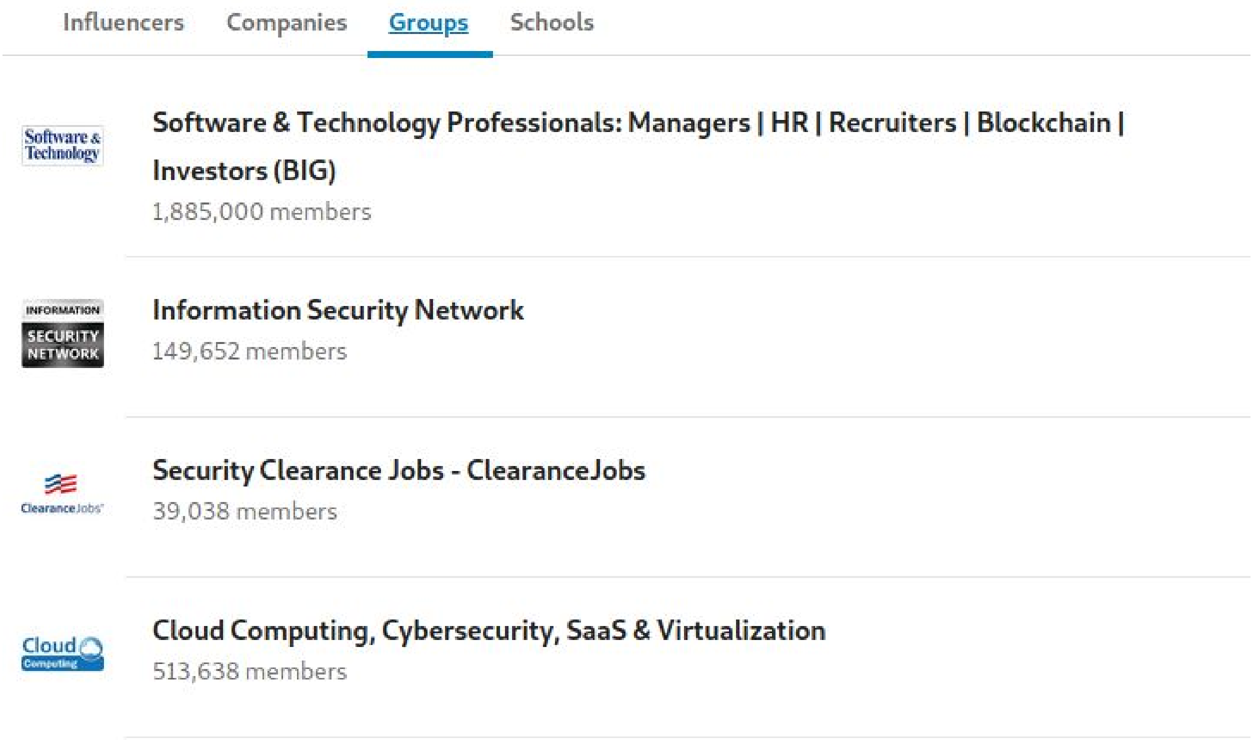
Information Security Careers Netw...
80,533 members

Information Security Network
149,652 members

See all

The interests section of a profile can contain useful information when the user does not fill out their experience or school sections. It may contain a list of influences, companies, or schools a user is following. Additionally, it also contains groups that the user is associated with. All of this can provide information on what field the user is now or previously in, or even what companies and/or schools the user is associated with. By default, only a portion of these interests are shown, with the rest being available by clicking “See all”.

In the above example, we can see a few interests that might suggest the user is involved in Information Security and might be associated with Earnst and Young, or have an interest in working there. Clicking on the “See all” we can gain additional supporting information.



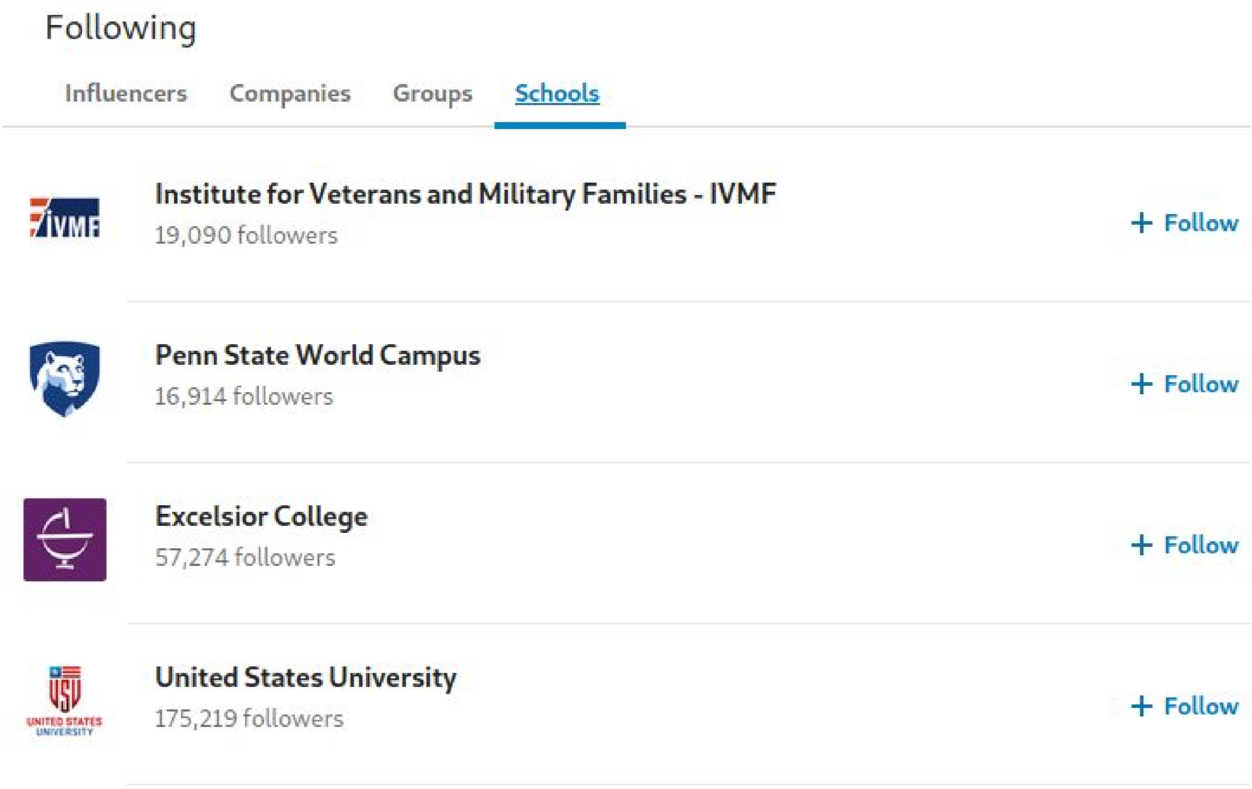
Software & Technology Professionals: Managers | HR | Recruiters | Blockchain | Investors (BIG)
1,885,000 members

Information Security Network
149,652 members

Security Clearance Jobs - ClearanceJobs
39,038 members

Cloud Computing, Cybersecurity, SaaS & Virtualization
513,638 members

Taking a look at the groups they are members of, we see additional InfoSec groups (among those shown above), as well as a group for the website ClearanceJobs. This would help us narrow down their likely location to being in the United States, and might suggest they are or previously were associated with government or military work and have a clearance with active status. Clicking on the tab of schools also adds credibility to this assumption, with one of them being for Veterans and Military families.



Following

Institute for Veterans and Military Families - IVMF
19,090 followers

Penn State World Campus
16,914 followers

Excelsior College
57,274 followers

United States University
175,219 followers

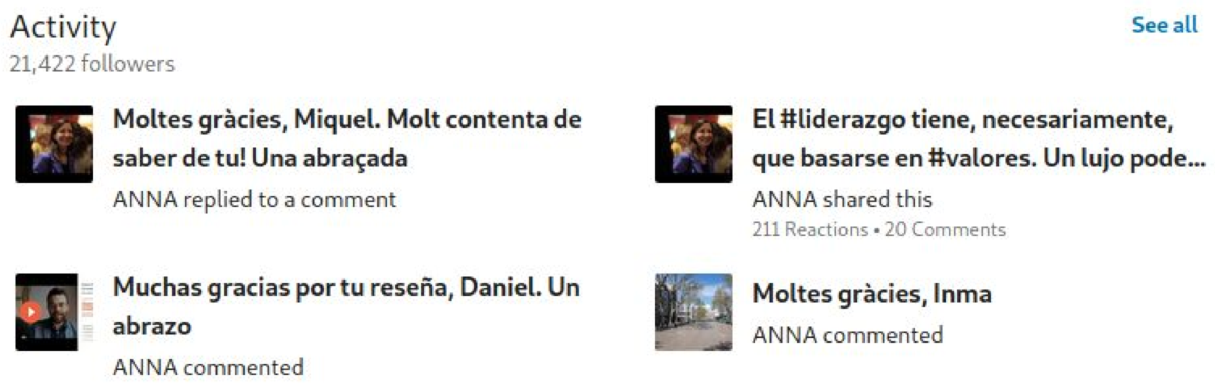
Conclusion Part I

We have just begun scratching the surface of exploiting LinkedIn for OSINT, however you should be able to tackle most accounts with a sense of confidence. In order to give you a running start I have created some simple OSINT bookmarklets and an OSINT attack surface map which can be found over on my Github. Additionally, be sure to keep a look out for the second section of this guide which will go over additional points that you can exploit in regards to a target’s education, work history, and more. Should you have any questions feel free to reach out to me on Twitter.

LinkedIn OSINT Techniques: Part II

Welcome back to this two-part guide on how to extract open source intelligence information from LinkedIn targets. If you haven't read Part I, which covers some of the smaller bits of information that can be exploited, you can do so here. Part II will continue showcasing points of exploitation that are associated with more robust accounts such as a target's experience, volunteer work, education, etc.

Articles and Activity



Activity
21,422 followers

See all

Moltes gràcies, Miquel. Molt contenta de saber de tu! Una abraçada
ANNA replied to a comment

El #liderazgo tiene, necesariamente, que basarse en #valores. Un lujo pode...
ANNA shared this
211 Reactions • 20 Comments

Muchas gracias por tu reseña, Daniel. Un abrazo
ANNA commented

Moltes gràcies, Inma
ANNA commented

This section appears at the top of a LinkedIn profile above the experience sections. It provides a quick snapshot of recent posts that the user commented on, shared, liked, etc. I have seen this section missing on some profiles, however it is possible to still locate it by manipulating the URL from the profile to add "/detail/recent-activity/" to the end (ie https://www.linkedin.com/in/$TARGETPROFILE/detail/recent-activity/). Otherwise, if it shows like in the above example, you can get a full view of the user's activity by clicking on the "See all" button which will open a new view and display a historic view of the following entries:

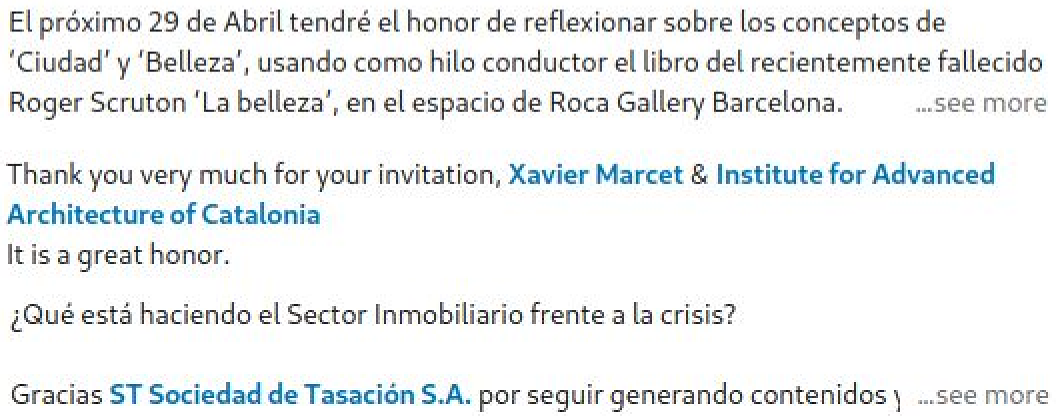
All Activity: This is the default view. It shows all activity of a user such as comments, likes, shares, posts, etc. If this section is modest and not too lengthy, it might be worth collecting the information to see what other accounts the target most frequently interacts with.

Articles: This will display articles written by the user and posted to the site.

Posts: Unlike the all activity view, the posts section will only display posts created by the user and exclude those they simply commented on or liked from other users. Be aware that posts from other users that the target shares will also appear here. This view may be useful in gathering information on the target quickly without going through hundreds or thousands of random posts they happen to like from their timeline.

Documents: This view will display documents uploaded by the user. Be sure to check them for any relevant information that might have been overlooked when the user uploaded it, such as the filename or embedded links or information the user failed to redact.

Clicking on the see more link for the above target, we can quickly scan their posts and see that many of them are in Spanish or English. Additionally, we can see that the user made many posts over time of when and where they will be speaking at specific upcoming events which help us narrow down location information.



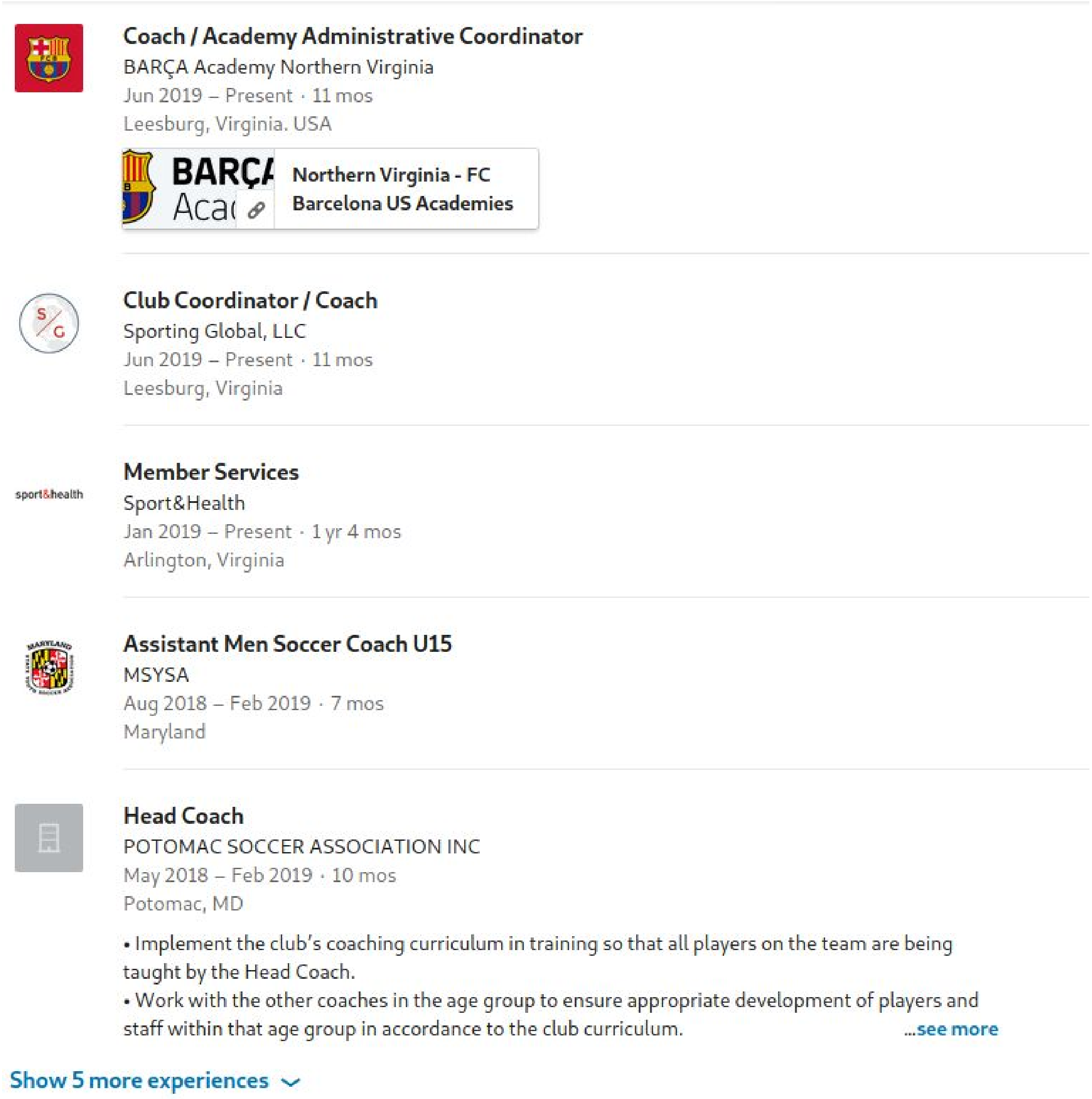
El próximo 29 de Abril tendré el honor de reflexionar sobre los conceptos de 'Ciudad' y 'Belleza', usando como hilo conductor el libro del recientemente fallecido Roger Scruton 'La belleza', en el espacio de Roca Gallery Barcelona. ...see more

Thank you very much for your invitation, **Xavier Marcet** & **Institute for Advanced Architecture of Catalonia**
It is a great honor.

¿Qué está haciendo el Sector Inmobiliario frente a la crisis?

Gracias **ST Sociedad de Tasación S.A.** por seguir generando contenidos y ...see more

Experience



Coach / Academy Administrative Coordinator
BARÇA Academy Northern Virginia
Jun 2019 – Present · 11 mos
Leesburg, Virginia. USA

BARÇA Aca
Northern Virginia - FC Barcelona US Academies

Club Coordinator / Coach
Sporting Global, LLC
Jun 2019 – Present · 11 mos
Leesburg, Virginia

Member Services
Sport&Health
Jan 2019 – Present · 1 yr 4 mos
Arlington, Virginia

Assistant Men Soccer Coach U15
MSYSA
Aug 2018 – Feb 2019 · 7 mos
Maryland

Head Coach
POTOMAC SOCCER ASSOCIATION INC
May 2018 – Feb 2019 · 10 mos
Potomac, MD

• Implement the club's coaching curriculum in training so that all players on the team are being taught by the Head Coach.
• Work with the other coaches in the age group to ensure appropriate development of players and staff within that age group in accordance to the club curriculum. ...see more

The experience section is often the most utilized part of LinkedIn and will appear under the about and/or activity sections. As LinkedIn is mostly used for landing jobs (and you know, phishing) this section will likely be more fleshed out and tends to contain information that is true to the user.

By default, this section will have at least one entry so long as the user did not sign up as a student and did not remove this information after signing up. Each experience entry may include one or all of the following points of information:

Title: This is a free text field that displays the position or job title that the subject held. In the event that the user does not post their company, more unique titles might help narrowing down possible companies. Additionally, you may be able to glean their experience level, and possibly to an extent their age or point in their career, by job titles as well.

Employment Type: This is a drop-down list of employment types such as full and part-time, apprenticeship, self-employed, etc. Not too valuable from an intelligence perspective but might help fill in other gaps later on.

Company: This is a required field where the user can place the name of the company they worked for. Knowing this information allows an investigator to possibly determine the email structure for sending phishing emails or might help with narrowing down a location if the company only operates in a specific area. It can also be searched on LinkedIn to locate additional accounts that were also employed by the company at the same time as the target.

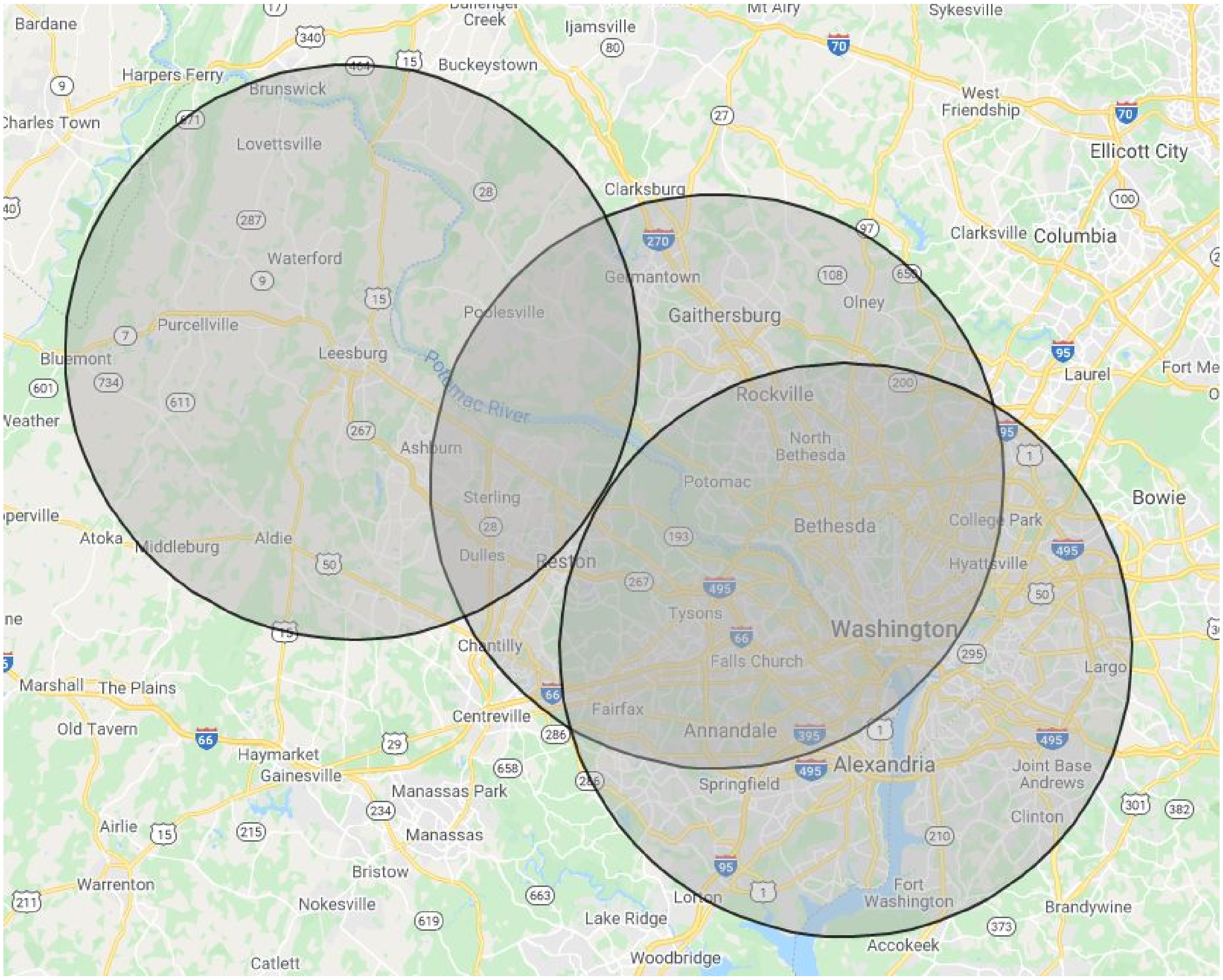
Location: This is a free text box that holds the location, usually at a city level, of where the user physically worked for at this company. Although many roles can be 100% remote, users that work from home might place their home city in this field. I have also seen remote workers use the nearest office's city here as well.

Start and End Dates: This section has included drop-down selectors for years. Using the known dates a target works for an organization allows an investigator to look for press releases and social media posts from the company around that time to see if the user was tagged or commented, thus giving away their other social media accounts.

Description: Another free text form, may include a combination of the information found in the above sections or may include information regarding the target's job duties, workgroups, notable projects, or major accomplishments.

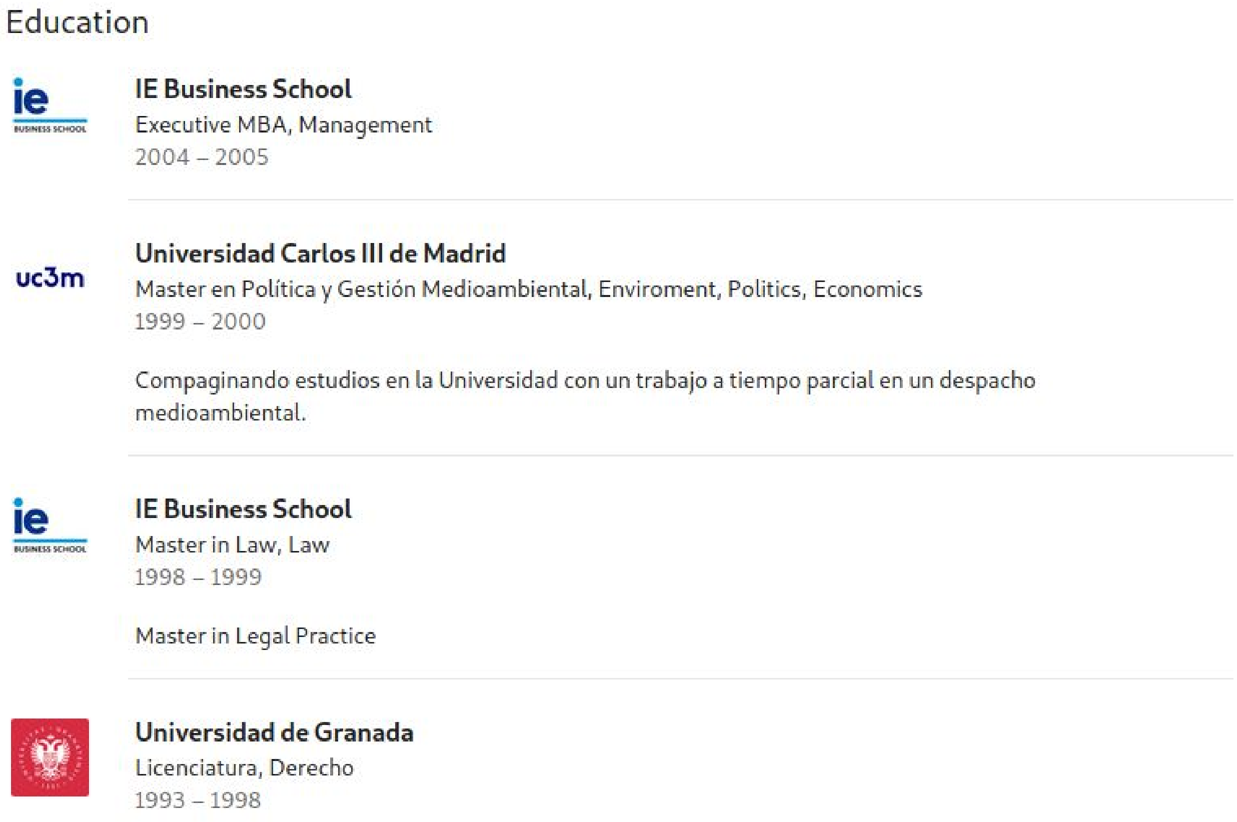
Media: Users may upload files to each entry; some might contain relevant information that helps narrow down the user's workgroup or perhaps include contact information like a work email. To view a list of media requirements, including supported file types, see here.

Going back to our example above, we can see that our target has numerous work entries revolving around coaching and fitness, making it easy to narrow down their field of work. Additionally, we can map out their locations and see if we can narrow down a potential area of where the target might live. I utilized this free tool to mark a 15-mile radius around each of the cities listed in the target’s profile. This is not an exact science with only three entries, but I would likely start my searches where the most overlap is observed from points created on the map.



The link provided on their first entry doesn't provide a whole lot of additional information that would be useful in our instance, however it did help locate additional social media platforms for the organization which could then be exploited for tagged photos of our target.

Education



Education

IE Business School
Executive MBA, Management
2004 – 2005

Universidad Carlos III de Madrid
Master en Política y Gestión Medioambiental, Enviroment, Politics, Economics
1999 – 2000

Compaginando estudios en la Universidad con un trabajo a tiempo parcial en un despacho medioambiental.

IE Business School
Master in Law, Law
1998 – 1999

Master in Legal Practice

Universidad de Granada
Licenciatura, Derecho
1993 – 1998

A user’s education section will usually immediately follow their work experience. It is important to note that by default this section will contain information if the user signed up as a student and did not remove this information after signing up. Be sure to do some research on the school’s syntax for email creation as well if you need to craft a targeted phishing attempt.

This section may not always be complete, but each education entry may include the following points of information:

School Name: Name of the school attended, this might help for narrowing down locations if the user lived on or nearby campus and did not attend school online.

Degree: Free text field for what type of degree was attained. Knowing this information might assist in guessing at what field or positions the user might be in. Level of degree might help in narrowing down an age range, especially when coupled with the start and end dates.

Field of Study: Free text field that often includes the major or minor field of study information. Similar to the degree field, this may assist in narrowing down possible suspects with information regarding what types of positions or work they might be engaged in, assuming they landed a job in their field.

Start and End Years: This section includes drop down selectors for years. If the user is a traditional student, this start and end range might assist in determining when a user went to high school and thereby determine approximately at what point they turned 18. This can then be backtracked to a possible range for a year of birth and current age.

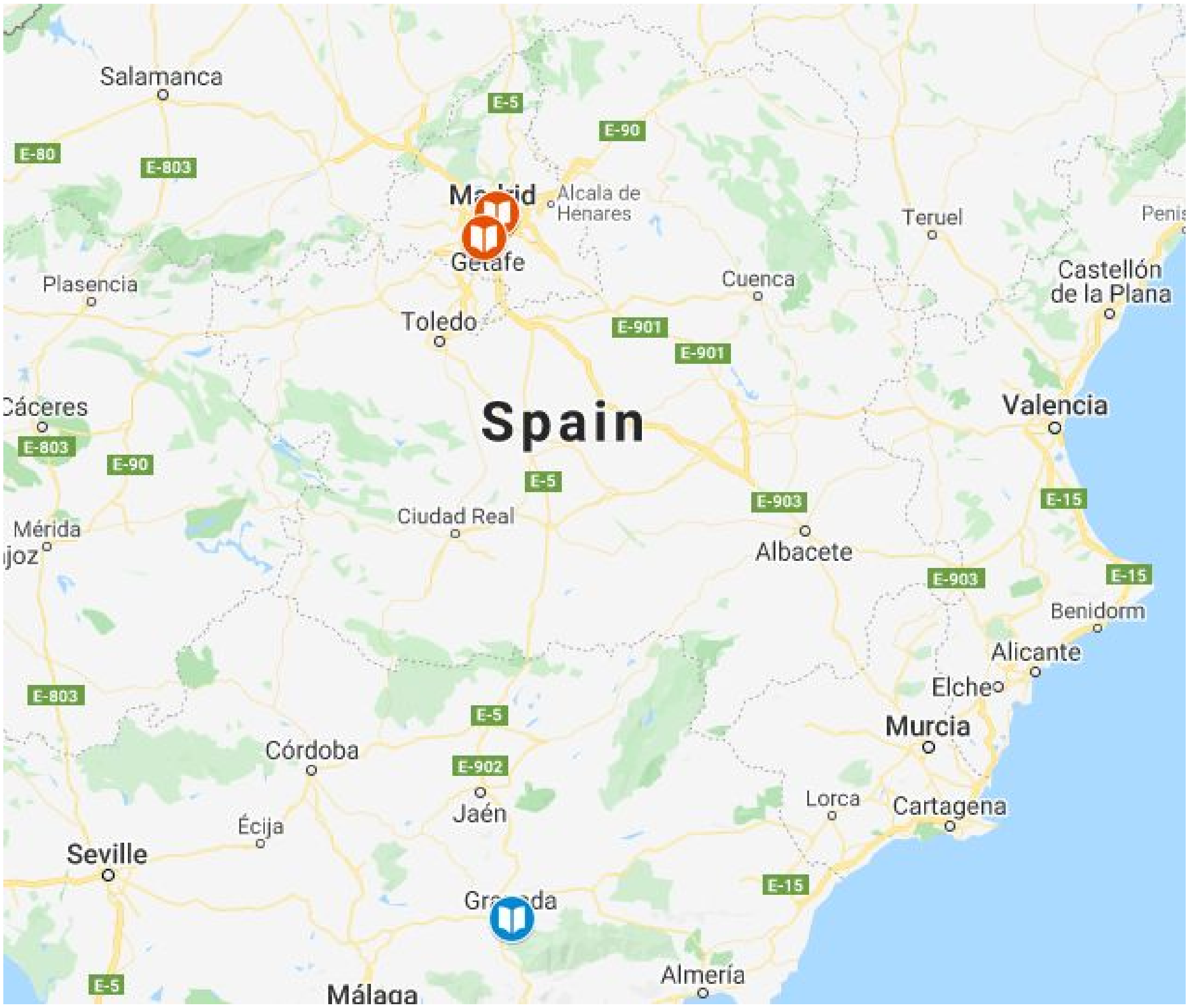
Grade: Free text field that tends to include the GPA. Not the most useful, however if the user has graduated with honors (or was on President’s List or Dean’s List) an investigator might be able to locate press releases or other information posted from the school related to these achievements.

Activities and Societies: Free text form that often has any campus societies or groups the user was a part of during their time in school. I do not see this one filled in often. An investigator may search these groups on social media and may locate additional photos or information, sometimes tagged, on the target.

Description: Another free text form, may include a combination of the information found in the above or may include information regarding their classes or major accomplishments.

Media: This area may contain files that are uploaded and might include transcripts, relevant presentations, or other major reports or projects. Be sure to look out for filenames that might contain additional information. Also be sure to scan documents for relevant school emails, contact information, etc that might appear on the credits or about author sections.

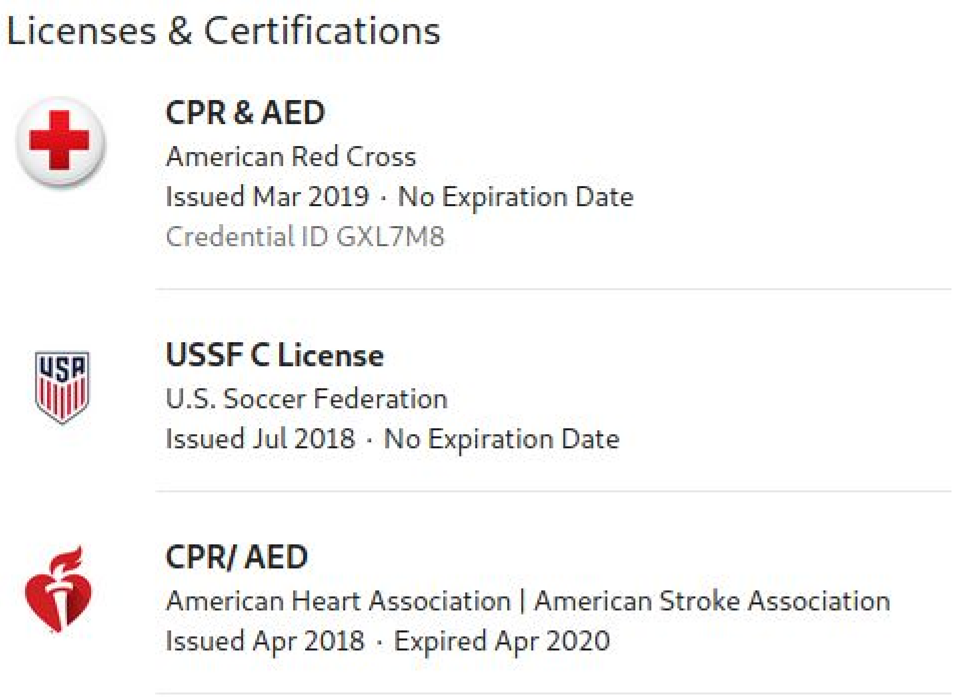
Using our above example, we can see that all of the schools our target is associated with are located in Spain, with the oldest one being in Grenada and the newer ones being in Madrid.



We can make the assumption our target grew up in Spain. Looking at the times of their associated schools, it might be possible to approximate their age as in their mid-forties (assuming they starting their first university at ~18 years of age).

Additionally, it might be worth considering that the target is originally from the southern portion of Spain (based on their initial choice of colleges, though not a certainty) and likely has made their current home, or at least spent a considerable portion of their life, in and around Madrid. Finally, a bit of Google Dorking (madrid contact me "@ie.edu") suggests that the email address format for the target's most recent school is likely first.last@ie.edu. We can use this to see if they still have access to the email and possibly craft a phishing email targeted to them.

Licenses and Certifications



Licenses & Certifications

CPR & AED
American Red Cross
Issued Mar 2019 · No Expiration Date
Credential ID GXL7M8

USSF C License
U.S. Soccer Federation
Issued Jul 2018 · No Expiration Date

CPR/ AED
American Heart Association | American Stroke Association
Issued Apr 2018 · Expired Apr 2020

The licenses and certifications section will often appear near the middle to bottom of a profile and is where a user will note what industry licenses and certifications they currently or previously held. This is not a section that I often see filled out, however should a user provide this information each entry may include some or all of the following items:

Certification Name: This is a required free text field where the user can input the name of their certification. This can be cross-referenced to any known databases or press releases of persons who obtained the certification, particularly those with only a few people holding them.

Issuing Organization: This is another required free text field that holds the name of the company or organization that issued the certification or license. Be sure to take a look at the areas in which the organizations primarily operate to see if some countries or continents may be excluded based on their limited reach or authority.

Issue and Expiration Dates: This is a set of four drop-down selectors that show the months and years the credential was issued on and expires at. This is not a required field.

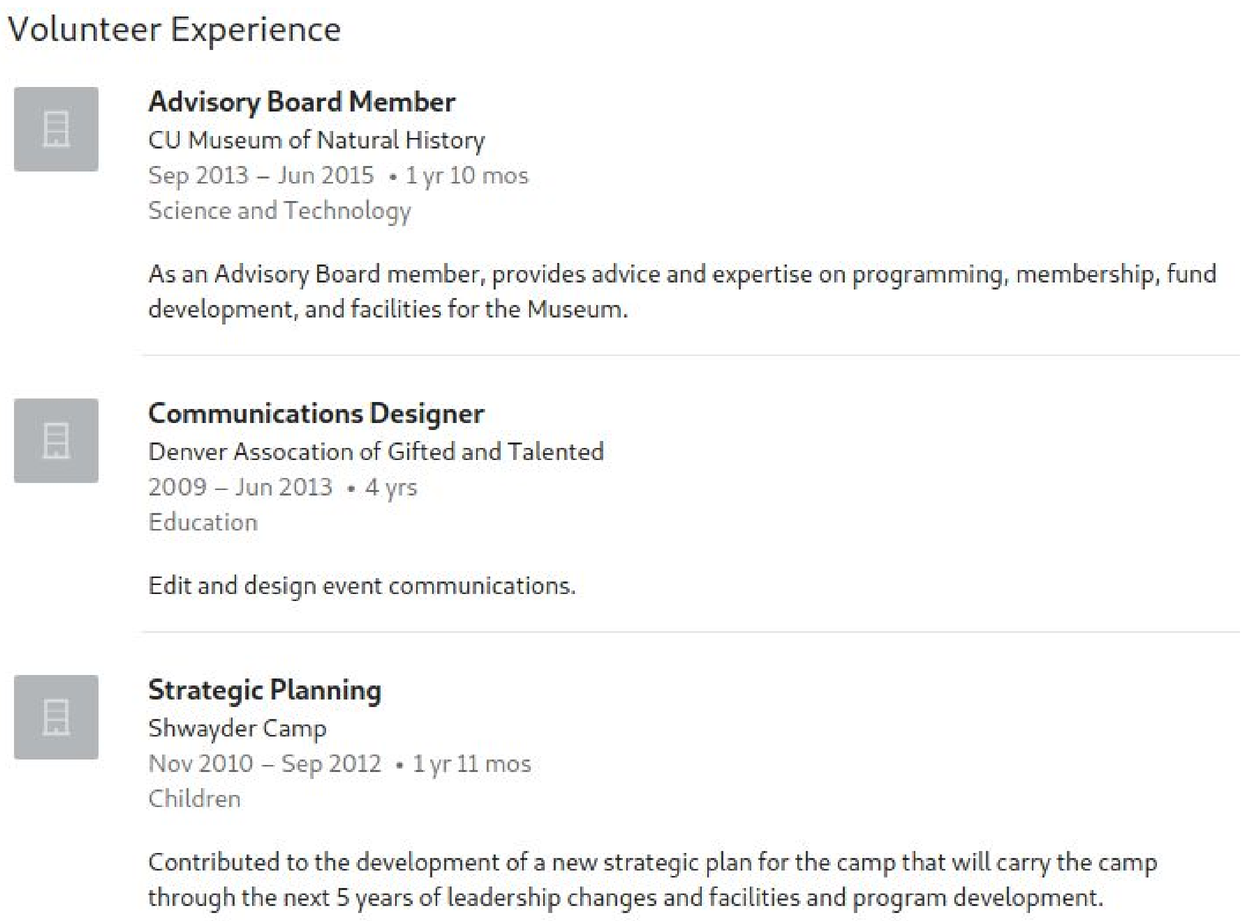
Credential Id: This is a free text field where a user can enter their credential id. Depending on the credential, it may be possible to locate additional information on the target using this id in searches, especially if the list of those holding the credential is made public. This is not a required field.

Credential URL: This is a free text field that allows a user to enter a URL that directs to their credential. This might provide the user's real name, as well as other information that might be left out such as the issue and expiration dates, credential id, etc. This is not a required field.

Our above example is missing many of the non-required information points, but there is still enough to help us with an investigation. Primarily, we can see that all of their credentials come from U.S.-based organizations, suggesting our target is likely living and working in the United States. Additionally, based on the types of credentials they have we can make the assumption they work in sports, specifically futbol, whether paid or on a volunteer basis.

Digging into the USSF C License, we can see that it is specifically for coaches, providing us a possible job title to search for as well. Finally, cross-referencing the time in which the target obtained their USSF C License (July 2018), we can quickly see where the classes were held, suggesting that our target might be located nearby Maryland, USA. We can also do a search on the credential id provided for his first credential, but it appears to only return the target's LinkedIn profile.

Volunteer Experience



Volunteer Experience

Advisory Board Member
CU Museum of Natural History
Sep 2013 – Jun 2015 • 1 yr 10 mos
Science and Technology

As an Advisory Board member, provides advice and expertise on programming, membership, fund development, and facilities for the Museum.

Communications Designer
Denver Assocation of Gifted and Talented
2009 – Jun 2013 • 4 yrs
Education

Edit and design event communications.

Strategic Planning
Shwayder Camp
Nov 2010 – Sep 2012 • 1 yr 11 mos
Children

Contributed to the development of a new strategic plan for the camp that will carry the camp through the next 5 years of leadership changes and facilities and program development.

The section for volunteer experience is great for determining pattern of life information on a user as well as location information. This information in this section may be more valuable than that found within the experience section. This is primarily because volunteer work is often a passion, rather than just a way of making money. Additionally, while users might have longer commutes for well-paying jobs, not many will be willing to take long commutes for unpaid work unless they are extremely dedicated to the mission.

Each entry in this section can contain any or all of the following:

Organization: This is the only required field for any volunteer experience entry. This free text field is used to display the organization or company where the user volunteered. Organizations that are region or city-specific will help narrow down locations.

Role: This is a free text field that is similar to the title field in the employment experience section. Users may enter their volunteer title given here. This might provide insight into how far up in the organization the user was: with lower-level volunteers less likely to have an email address associated with the organization than those at the top.

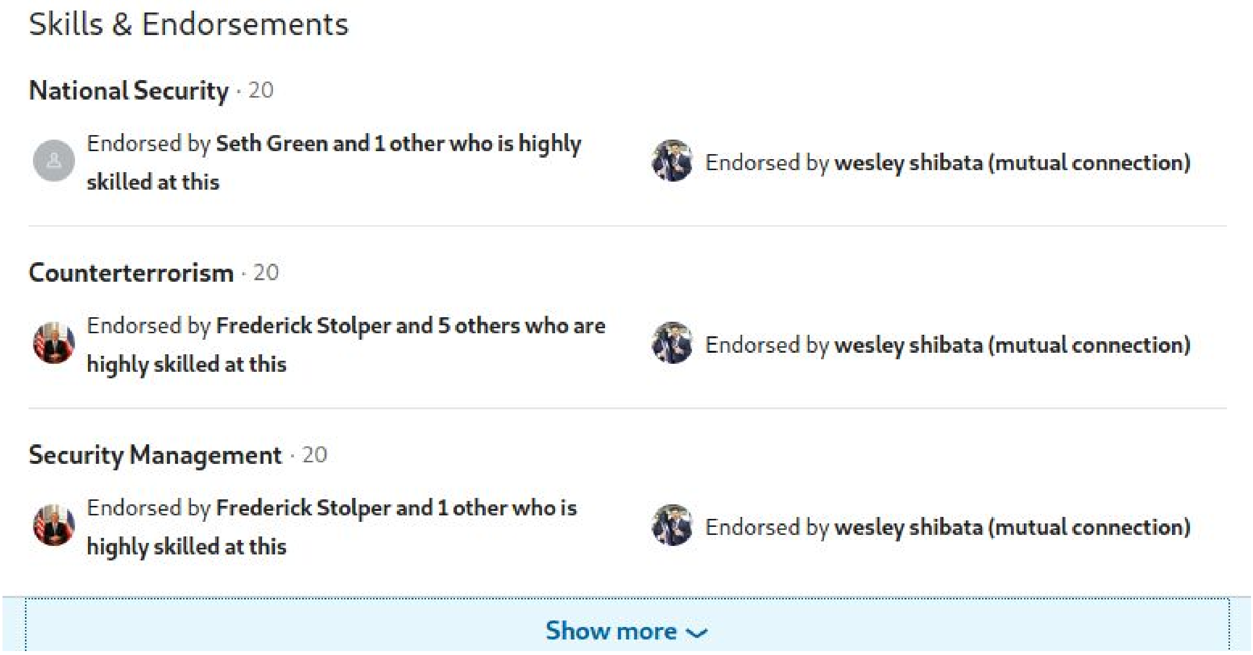
Cause: This is a drop down list of possible causes that the entry is associated with. Not as useful but might assist in determining what causes the target is passionate about if not immediately available based on other known information.

Start and End Dates: These dates are chosen via a drop-down menu and correspond to when a user started and ended their volunteer work. Knowing these dates might assist in narrowing down what times to specify for locating information on our target whether in news stories or social media posts of the organization.

Description: This is a free text field where a user may enter information about what they did while volunteering at this entity.

Our above example displays three (of many) volunteer entries for a target. We can see that the user might be passionate about teaching or helping children based on their last two entries, whereas the totality of the three entries suggest that the user would have lived or worked in the Denver, Colorado area for a significant amount of their lifetime. Additionally, as an advisory board member we can expect our target to have some sort of background or experience in the field of natural history, anthropology, etc, and might be a position in which they are granted an email address to perform their duties.

Skills and Endorsements



Skills & Endorsements

National Security · 20

Endorsed by **Seth Green and 1 other who is highly skilled at this**

Endorsed by **wesley shibata (mutual connection)**

Counterterrorism · 20

Endorsed by **Frederick Stolper and 5 others who are highly skilled at this**

Endorsed by **wesley shibata (mutual connection)**

Security Management · 20

Endorsed by **Frederick Stolper and 1 other who is highly skilled at this**

Endorsed by **wesley shibata (mutual connection)**

The skills and endorsements section offers an insight into the field they might be associated with by showcasing the skills a user wants others to be aware that they are proficient in. These skills are then endorsed by their peers, often those who are also in the same field. This might assist an investigator in narrowing down their field should their experience section otherwise be empty. It may also assist in narrowing down a user's job positions should some of the skills be very unique.

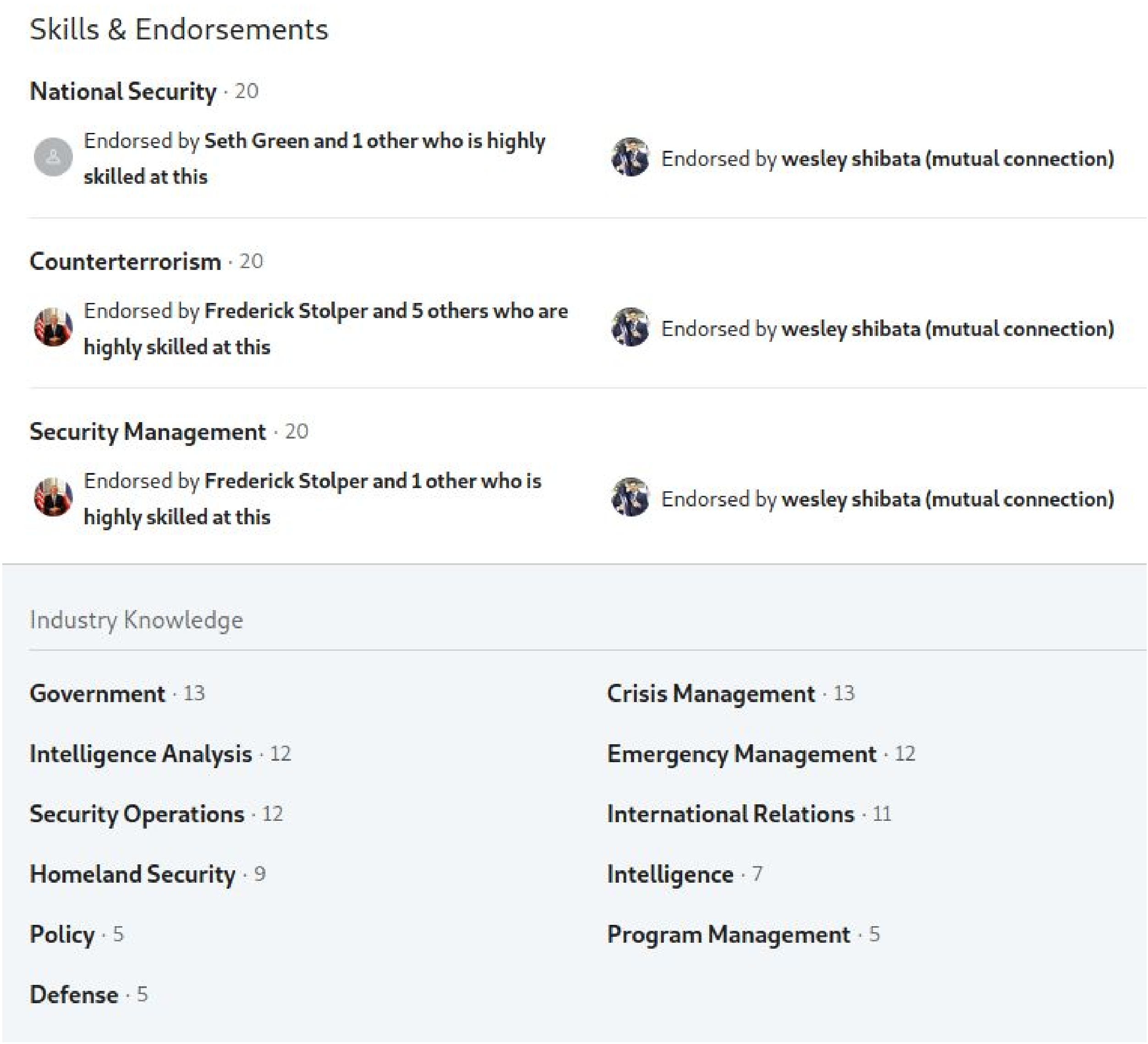
These skills contain any or all of the following points:

Skill: This is a free text field that the user may choose to have others endorse them on. As this is generated by the user it may give an insight into what skills they find most important in their field, as well as which skills are seen as highly valuable by their peers and recruiters. Looking at the totality of skills might help narrow down a field of work.

Number of Endorsements: Connections may endorse one another which is basically vetting other users on their skills. This section is not too useful for OSINT other than knowing that users with a larger number of connections or with a longer work history tend to have a higher number of endorsements.

Endorsed by: Looking at who they are endorsed by may also assist in locating coworkers or colleagues in their fields. This might assist in locating other users that have close or continuing working relationships with the target.

Using our above example, we can glean preliminary information from the shown skills, however we will be able to get a fuller picture by clicking on the "Show more" button at the bottom.



Skills & Endorsements

National Security · 20

Endorsed by **Seth Green and 1 other who is highly skilled at this**

Endorsed by **wesley shibata (mutual connection)**

Counterterrorism · 20

Endorsed by **Frederick Stolper and 5 others who are highly skilled at this**

Endorsed by **wesley shibata (mutual connection)**

Security Management · 20

Endorsed by **Frederick Stolper and 1 other who is highly skilled at this**

Endorsed by **wesley shibata (mutual connection)**

Industry Knowledge

Government · 13

Intelligence Analysis · 12

Security Operations · 12

Homeland Security · 9

Policy · 5

Defense · 5

Crisis Management · 13

Emergency Management · 12

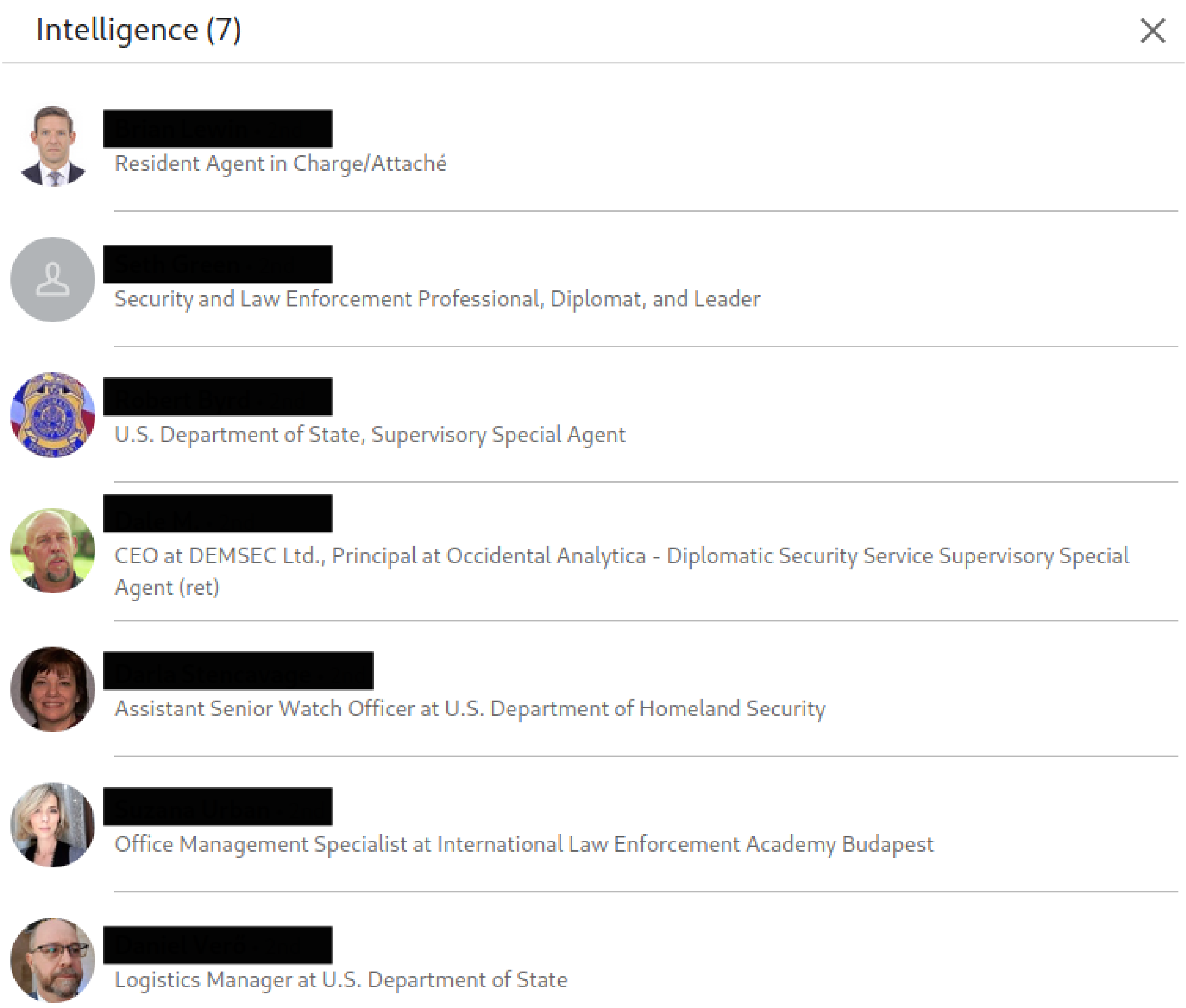
International Relations · 11

Intelligence · 7

Program Management · 5

Looking at the various skills, we can make a few assumptions on their field of work, specifically that they are likely a member of a government organization based on the Government, National Security, Policy, and other skills listed.

We can also possibly narrow down the specific group or organization within the government by the other skills, specifically Intelligence Analysis, Counter-terrorism, Intelligence, Crisis Management, and Emergency Management. We could expect them to work in a position likely in a military or law enforcement organization rather than say the offices for Economics or transportation. By clicking on each individual skill, we can see every user that endorsed our target for that specific skill.



Intelligence (7)

[redacted]
Resident Agent in Charge/Attaché

[redacted]
Security and Law Enforcement Professional, Diplomat, and Leader

[redacted]
U.S. Department of State, Supervisory Special Agent

[redacted]
CEO at DEMSEC Ltd., Principal at Occidental Analytica - Diplomatic Security Service Supervisory Special Agent (ret)

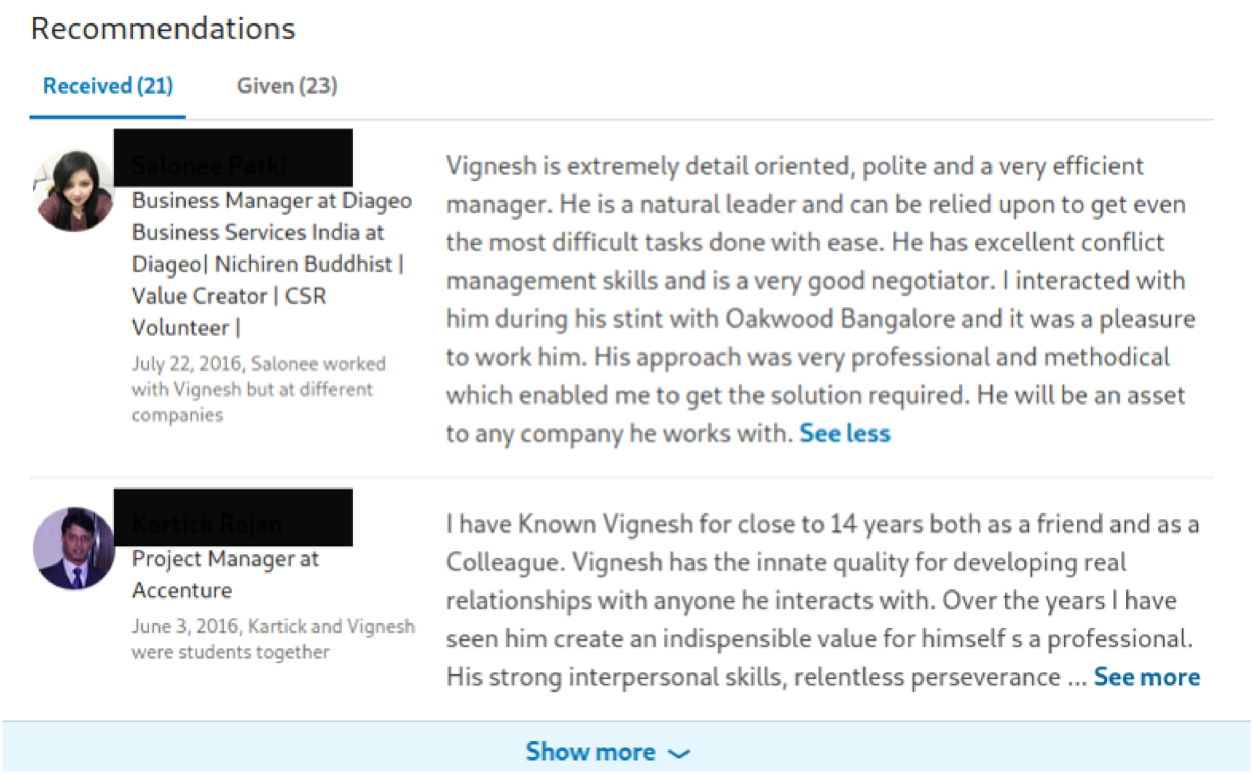
[redacted]
Assistant Senior Watch Officer at U.S. Department of Homeland Security

[redacted]
Office Management Specialist at International Law Enforcement Academy Budapest

[redacted]
Logistics Manager at U.S. Department of State

This helps strengthen our assumption, with his endorsements coming from personnel at many law enforcement agencies. Additionally, we could likely lean towards this target being an employee of the United States federal government based on his connections and endorsements.

Recommendations



Recommendations

Received (21) Given (23)

[redacted]
Business Manager at Diageo Business Services India at Diageo| Nichiren Buddhist | Value Creator | CSR Volunteer |
July 22, 2016, Salonee worked with Vignesh but at different companies

Vignesh is extremely detail oriented, polite and a very efficient manager. He is a natural leader and can be relied upon to get even the most difficult tasks done with ease. He has excellent conflict management skills and is a very good negotiator. I interacted with him during his stint with Oakwood Bangalore and it was a pleasure to work him. His approach was very professional and methodical which enabled me to get the solution required. He will be an asset to any company he works with. See less

[redacted]
Project Manager at Accenture
June 3, 2016, Kartick and Vignesh were students together

I have Known Vignesh for close to 14 years both as a friend and as a Colleague. Vignesh has the innate quality for developing real relationships with anyone he interacts with. Over the years I have seen him create an indispensible value for himself s a professional. His strong interpersonal skills, relentless perseverance ... See more

Recommendations are not the most common point of exploitation, but profiles that have them can be leaking a great deal of information on a subject via their given and received recommendations. This is particularly true for their received recommendations, which may provide information that the target did not originally include on their profile. The more recommendations given and received the more chances that one of them will leak relevant information about your target.

All recommendations on a subject’s profile, whether given or received, should contain the following points of exploitation:

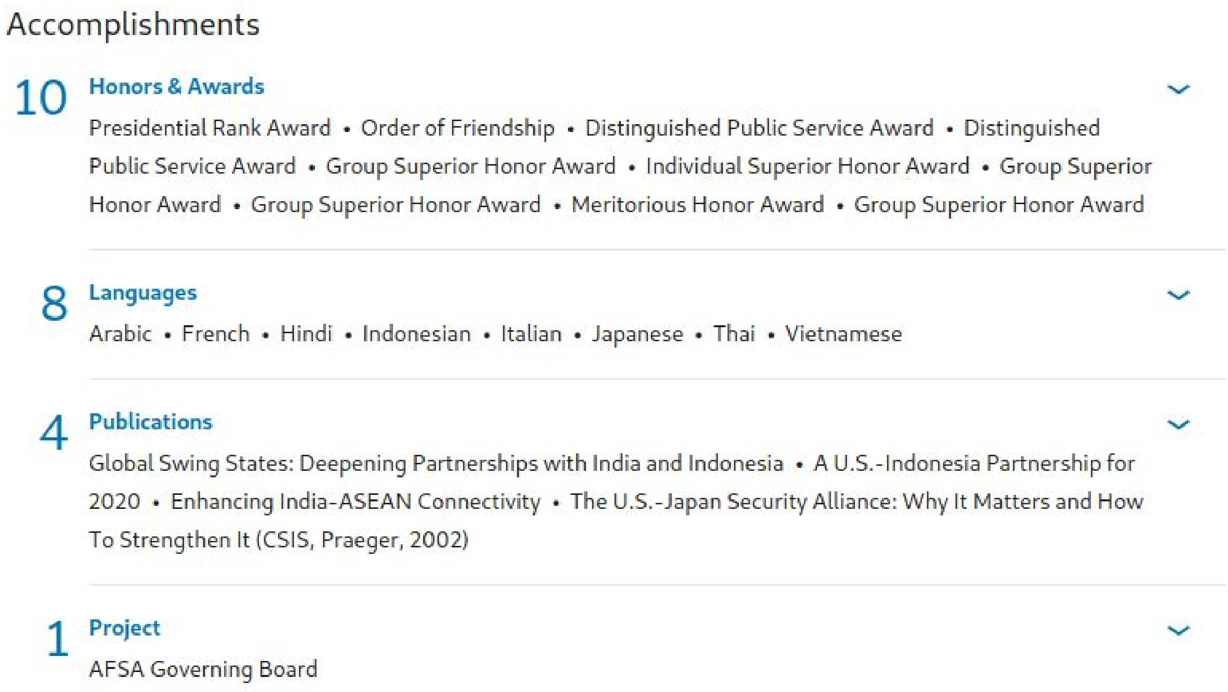
Recommender: This is an automated section that is created based on the profile of the person making the recommendation. It should include the recommender’s profile photo, name, current position, date recommendation was made, and finally the relationship between the recommender and the person they are recommending.

Description: This is a free text field where a user will post the actual recommendation. It might include information such as where, either city or business, the recommender worked with or met the person they are recommending. It might also provide other information that fills in gaps such as job positions, age, schools, names, and associated persons.

Using the above example, we can see two of the many recommendations that the user received. The first one provides us with the target's name and states that they were in a managerial position at Oakwood Bangalore, providing us a possible field of work and a city location to use as a filter when searching for our subject. The second recommendation does not provide a lot of direct information but does provide some indirect details that might be useful with additional digging. This second user states he attended school with our target and was a colleague of theirs as well.

We can also see that this recommendation was provided on June 3, 2016. Should our target have left the work or education sections of their profile empty, we could possibly obtain this information by referencing the LinkedIn profile of the user that recommended our target for any education or work experience that occurred prior to June 3, 2016. Finally, should we wish to view all of their recommendations we could click on "Show more" at the bottom of the section.

Accomplishments



Accomplishments

10 Honors & Awards

Presidential Rank Award • Order of Friendship • Distinguished Public Service Award • Distinguished Public Service Award • Group Superior Honor Award • Individual Superior Honor Award • Group Superior Honor Award • Group Superior Honor Award • Meritorious Honor Award • Group Superior Honor Award

8 Languages

Arabic • French • Hindi • Indonesian • Italian • Japanese • Thai • Vietnamese

4 Publications

Global Swing States: Deepening Partnerships with India and Indonesia • A U.S.-Indonesia Partnership for 2020 • Enhancing India-ASEAN Connectivity • The U.S.-Japan Security Alliance: Why It Matters and How To Strengthen It (CSIS, Praeger, 2002)

1 Project

AFSA Governing Board

The accomplishments section appears to be LinkedIn's version of a "catchall" for anything that doesn't fit nicely into one of the previous categories. The information here can vary widely from totally useless to something that breaks a case. Be sure to click on the drop-down arrow on the right side of each section to see additional information that is hidden by default. The various types of entries that can appear in this section may include:

Publications: Requires a publication title and may also include the publisher or publication information, publication date, a link to the publication, as well as a description. Locating the actual publication is the best way to exploit this information as it may contain the user's title, name (as an author), and other information that might not be shared by the user elsewhere on the profile.

Patents: Requires a patent title and patent number, as well as which country the patent was created in. Other information may include whether the patent is issued or pending, the issue date, and the description. This information might help locate the country in which the target lives and works in as well as what fields of work they may be an expert in. Should they include a link or patent number, it may be possible to locate it in the record of the country issued in to find additional information on the target.

Courses: By default, every course entry requires the course name and may also include a course number and what work or education experience the course was associated with, if any. Pay particular attention to course names and numbers as schools might have unique ones that allow you to narrow down a target's school even if they left it out on their education section.

Project: This section is for listing any projects worked on, and by default only requires a project name. Additional fields are the start and end date of the project, what work or education the project was associated with, as well as a project URL and a description. This section might not provide too much additional information, although it might leak associates that worked on the same project as well as information found about that particular project posted elsewhere online.

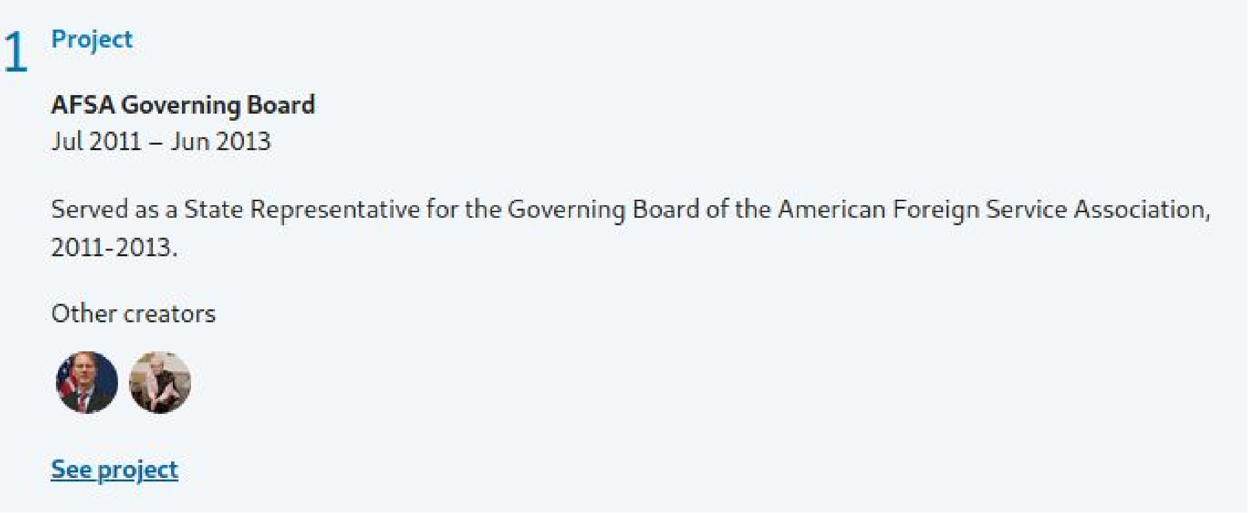
Honors and Awards: Requires only the title by default, although it might also include who issues the award, what work or education the award is associated with, as well as the issue date and a description of the award. Knowing the date and award name or organization might allow an investigator to locate a press release or photos of the award ceremony in which the target attended.

Test Score: This section allows a user to show off their test score, with each entry requiring the test name and score. It might also include what education or work experience the test was associated with as well as the test date and the description. Not too valuable of a section, however if looking at college entry tests such as the SAT or ACT it might be possible to make a ballpark guess on the target's age if they included the date in which they took the particular test.

Languages: This is one of the smallest sections, including only a text field to enter the language and a drop-down menu to display how proficient in the language the user is. Unique languages might assist in determining where a subject grew up or lives, particularly if the user has native proficiency in such a language.

Organization: This section is for listing organizations a user is associated with and by default only requires the organization name for each entry. Other possible fields include the position held, what work or education entry the organization is associated with, as well as the start and end dates and a free text field for a description. I rarely see this section utilized, and often find this information simply listed under the education or work entries instead.

Our above example has numerous points we can exploit, however we are going to focus on two sections, honors and awards and projects. Clicking on the arrow on the right side of projects displays additional information about the project, including two other users associated with the project as well as the time in which our target was involved and a link to the project.



1 Project

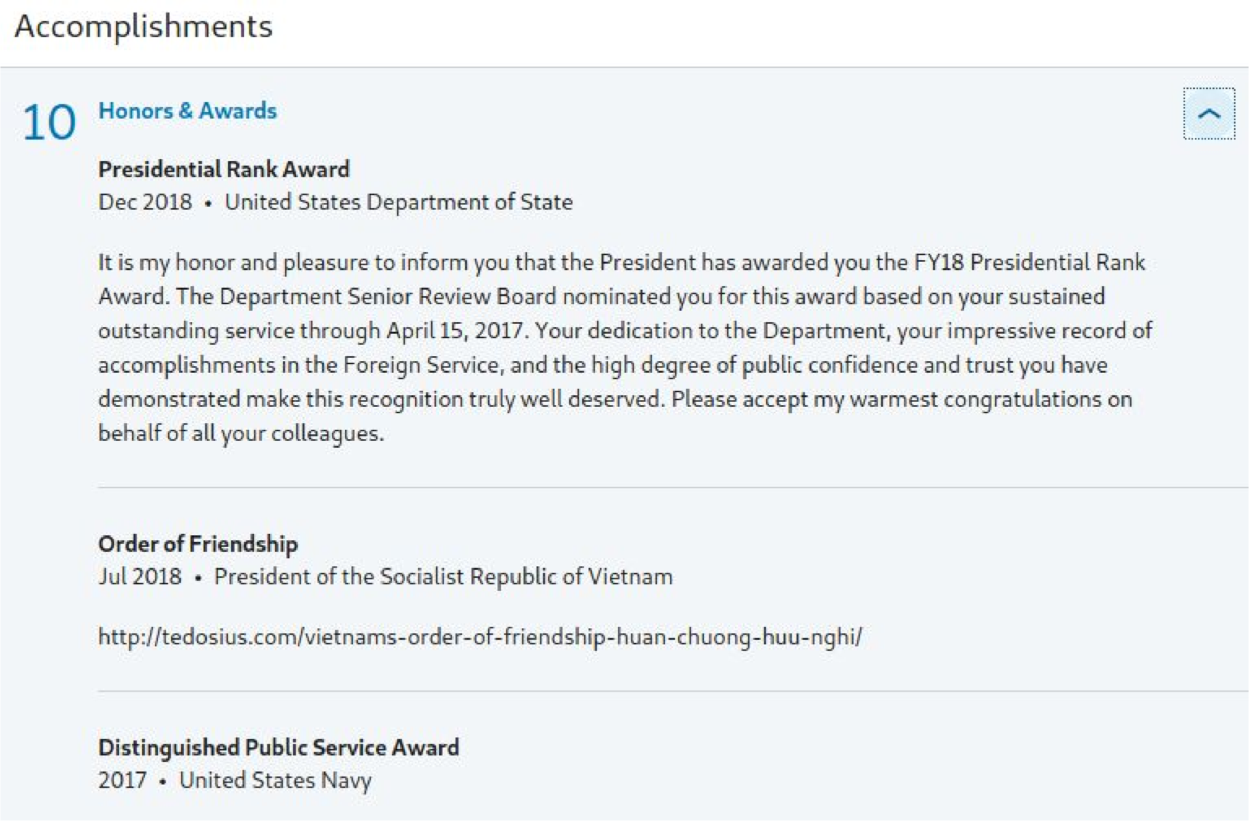
AFSA Governing Board
Jul 2011 – Jun 2013

Served as a State Representative for the Governing Board of the American Foreign Service Association, 2011-2013.

Other creators

See project

Unfortunately, clicking the link goes to a site that no longer works, however seeing the .gov domain associated with the project tells us the use likely worked for the government at this time. Moving on, we can expand the honors and awards section in the same way.


Accomplishments

10 Honors & Awards

Presidential Rank Award
Dec 2018 • United States Department of State

It is my honor and pleasure to inform you that the President has awarded you the FY18 Presidential Rank Award. The Department Senior Review Board nominated you for this award based on your sustained outstanding service through April 15, 2017. Your dedication to the Department, your impressive record of accomplishments in the Foreign Service, and the high degree of public confidence and trust you have demonstrated make this recognition truly well deserved. Please accept my warmest congratulations on behalf of all your colleagues.

Order of Friendship
Jul 2018 • President of the Socialist Republic of Vietnam

http://tedosius.com/vietnams-order-of-friendship-huan-chuong-huu-nghi/

Distinguished Public Service Award
2017 • United States Navy

The results quickly strengthen our assumption about the target working for a government, and we can see that he is associated primarily with the United States, though they also appear to have done work with Vietnam. Looking back at our target’s languages, Vietnamese now stands out as being more important than some of the other ones and should be given more weight when searching on our target.

Conclusion Part II

With so much information available on the platform, LinkedIn remains an OSINT goldmine for investigators. Between the two parts of this guide there should be no part of a LinkedIn profile that you are unable to exploit. Before setting out on your next investigation, be sure to take a look at my LinkedIn OSINT Bookmarklet tools and OSINT Attack Surface guide on my Github to help in simplifying some of the tasks above. As always, should you have any questions feel free to reach out to me on Twitter.