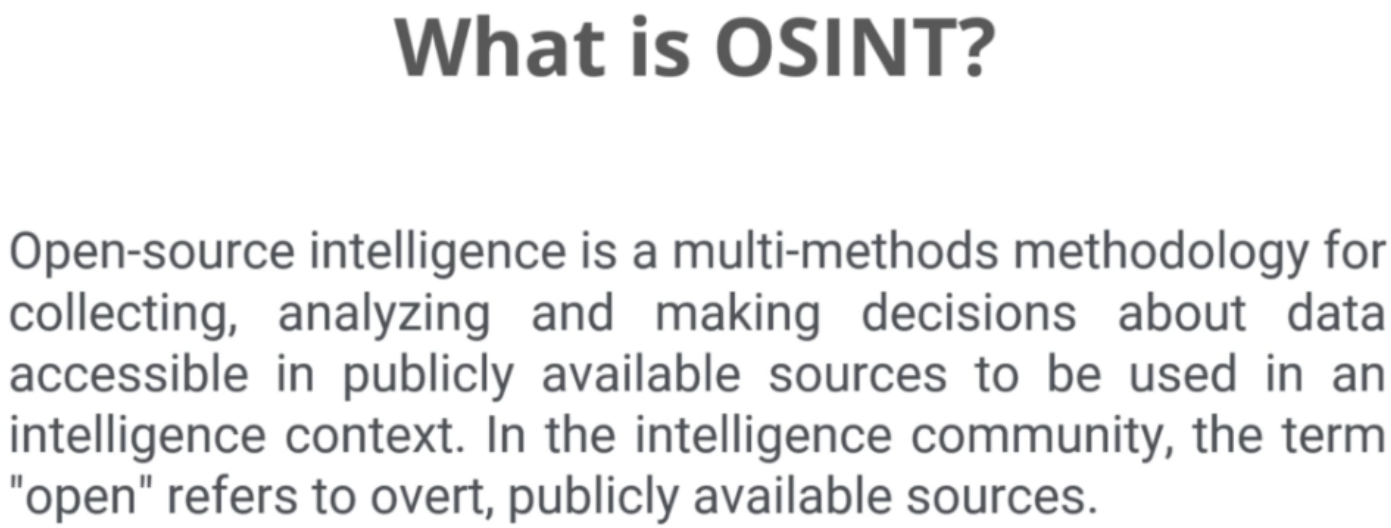
OSINT

OSINT Framework: https://osintframework.com/

What is OSINT

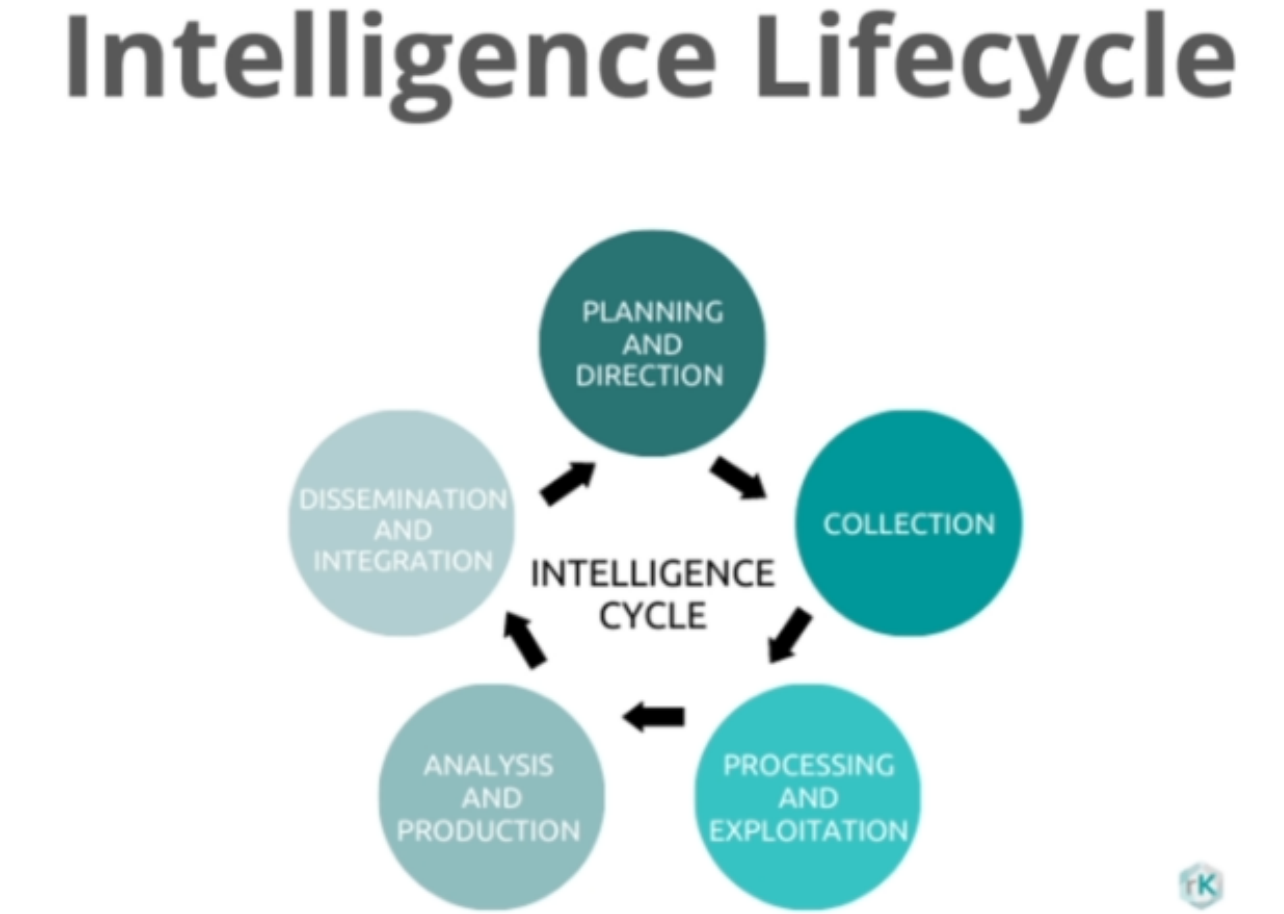


Intelligence Lifecycle

- **Intelligence Lifecycle**

Planning and Direction → Collection → Processing and Exploitation → Analysis and Production -> Dissemination and Integration

Lập kế hoạch và định hướng → Thu thập → Chế biến và Khai thác → Phân tích và Sản xuất ->



Source: https://blog.reknowledge.tech/blog/osint-analyst-replaced-by-automation

Sock Puppets (Fake Account)

- You think of a **sock puppet** as a fake account, alternate identity, etc.
- The point of having a good sock puppet is to not draw attention back to yourself.

So ideally, we're going to create this fake identity or fake person. And this fake person might have a Twitter account, might have a Gmail address or proton mail or something along those lines.

They might have a Facebook and this should never tie back to you, meaning it should never really tie back to your IP address.

It should ever be used on a device that links to your personal information, should never be used on a phone that ties to you.

There's a lot of depth that we can go into to avoid tying our name to a sock puppet. But the purpose is really to be able to have an account that looks legitimate.

So that means creating content on these accounts, you know, making sure that you don't just create a bunch of fake accounts and then start doing research on somebody.

Vì vậy, lý tưởng nhất là chúng ta sẽ tạo ra danh tính giả hoặc người giả này.
Và kẻ giả mạo này có thể có tài khoản Twitter, có thể có địa chỉ Gmail hoặc thư proton hoặc thứ gì đó dọc theo những dòng đó.

Họ có thể có một Facebook và điều này sẽ không bao giờ ràng buộc bạn, có nghĩa là nó không bao giờ thực sự ràng buộc trở lại địa chỉ IP của bạn.

Nó nên được sử dụng trên một thiết bị liên kết đến thông tin cá nhân của bạn, không bao giờ được sử dụng trên điện thoại liên quan đến bạn.

Có rất nhiều chiều sâu mà chúng ta có thể tìm hiểu để tránh gắn tên mình vào một con rối vớ vẩn. Nhưng mục đích thực sự là để có thể có một tài khoản trông hợp pháp.

Vì vậy, điều đó có nghĩa là tạo nội dung trên những tài khoản này, bạn biết đấy, hãy đảm bảo rằng bạn không chỉ tạo một loạt tài khoản giả và sau đó bắt đầu nghiên cứu về ai đó.

Sock Puppets creating

This is my process for setting up an anonymous sockpuppet account.

1. Come up with a persona for the sockpuppet account.

2. Use Fake Name Generator to create a person whom you feel fits your sockpuppet persona.

3. Use This Person Does Not Exist to generate an image. Make sure you inspect the image closely and get one that doesn't have any obvious flaws, as they often do. It is worth picking up some Photoshop, GIMP, Affinity Photo or Designer, or other basic image manipulation skills to fix them and change the background of the image.

4. Get a burner phone, completely wiped and fresh. Can be any brand that will accept a Mint Mobile SIM card.

5. Get a burner credit card from Privacy.com to use for on Amazon and possible the Mint Mobile setup. They might need it to set up the account.

6. Set up a burner Amazon account. We're only going to use it once.

7. Buy two Mint Mobile SIM cards. You can find them various places online and in stores near you, but you can get two of them for $5 on Amazon. They also give you 1 week free trial with

something like 100 text messages, which we're going to use. This gives you two cards for two sockpuppet accounts for only $5.

8. I like to use Amazon to have the card sent to an Amazon pickup box, which can be anonymous.

9. Get a VPN that you can set to the physical area in which you want your sockpuppet to "exist."

10. Set up the Mint Mobile trial account somewhere away from your home; as far as you're willing to go.

11. Use this Mint Mobile trial phone number to set up all of the websites you need.

12. I recommend at least set up a Google account and Protonmail account. Both will come in handy at different times.

13. Once you've set up all the accounts with your trial Mint SIM, set up 2FA on all of the accounts.

14. After setting up 2FA on all of the accounts, change the phone number to one you have more permanent access to, such as MySudo or Google Voice.

15. Make sure everything works!

16. Destroy the SIM card.

17. Wipe the phone.

A lot of these websites are blocking MySudo, Google Voice, and other VoIP numbers.

That's why we go through the Mint phone number first.

They should be less stringent now. As always, feedback is welcome! This was originally posted on my blog where I also talk about the ethics of sockpuppet accounts.

Sock Puppet

https://jakecreps.com/sock-puppets/

• The internet (already a skeptic) defines a sock puppet as "an online identity used for purposes of deception"

• Sock puppets aren't exclusive to deception operations, they can also be used for privacy and

OPSEC for an investigator, journalist, penetration tester, etc

- OPSEC online not only protects the investigator, but it also protects the target in the case that the evidence provided leads nowhere.

→ How to make an intelligence socket puppet?

1. You have to do is **clearly define your intent.**

→ Creating an avatar that's focused around an idea rather than a unique identity.

- Everyone knows Shakira isn't involved in the infosec community. They also know that *that* account isn't Shakira.

- But that account is still a trusted source on Twitter when it comes to OSINT and infosec conversations.

- That account have over 500 followers.

- That account has a function and has built trust.

- That account was easier to create than a blank slate.

⇒ it's recommended to create content, add media (photos, videos), interact with others online in an authentic way

create multiple social profiles, convince others to vouch for you, have a phone number, unique IP, email address, etc.

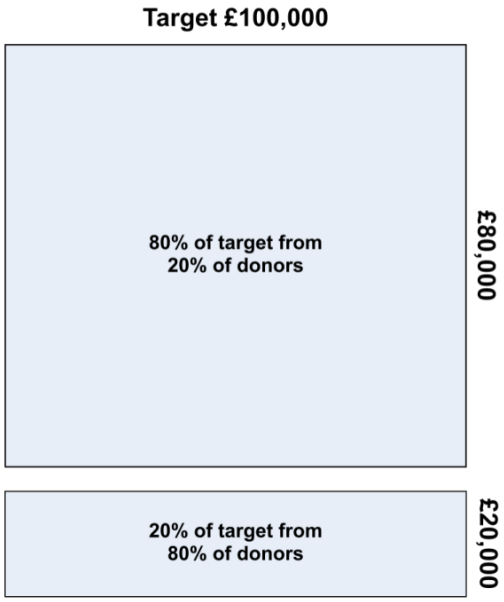
1. Setup

Depending on who you ask, there's an endless list of things you can do to remain anonymous while conducting investigations online.

If you're interested in an almost full proof system, check his book Hiding from the Internet.
If you're asking me how to create a successful sock puppet, I'm more of a subscriber of the

Pareto Principle;
but I also don't have much to lose if caught during an investigation like others may have (back to intent).

Here's the 80/20 on what you need to get started.



1. A dedicated computer that is only used for investigations

2. Encrypted Email – Use Proton Mail

3. A burner phone number (expensive) or a wifi phone number (cheap or free)

4. A social media profile where your target is most active (choose option 1 or 2)

5. A couple different virtual machines

6. A blog or website (you can use a free blog like WordPress, Blogger, or Medium)

7. A VPN (you should probably have one anyway)
Now, this is just a start, but it will help you at least get started. You will have to customize your avatar as you go along to maintain or add credibility.

2. Dedicated Computer

Having a dedicated computer is an absolute must.

You don't want anything you are doing under your avatar to somehow be linked to your personal, real account.

Not only will this reveal that your sock puppet is indeed a sock puppet, it may link your real identity to it (see Surefire Intelligence fail).

This computer doesn't have to be expensive, you could use something as simple as a Raspberry Pi or a cheap laptop.

Using other tools I'll discuss below, your dedicated computer should not be able to be linked to another computer on your network.

---

3. Encrypted Email

This is generally a best practice in the OSINT and infosec community.

• While it may be enticing to use Gmail due to the vast number of free tools they provide and their seamless integration, but don't do it.

Google is tracking you. Even if you provide false information, they will still know it's you eventually.

• Proton Mail is a name brand in the encrypted email industry. There are other options but I'd go with Proton Mail if you haven't

experimented with them before. The user interface is easy to understand and it doesn't require any advanced setup.

4. Phone Number

- If you can, try to get a very cheap phone plan that's dedicated to you avatar.

Cheap plans such as Mint will get you the very basics for close to single digits a month.

If you don't want to spare the cash, consider getting a wifi based phone number from a website that doesn't recycle phone numbers every month.
Google Voice is a good option.

Keep in mind that a lot of these websites request your primary phone number (Google) when signing up.
If you're very concerned about privacy, find one that doesn't.

5. VPN

- It's important to mask your IP when doing **OSINT** research online.

The best way to do this is to use a VPN.

The number one VPN changes frequently so depending on when you read this, it could be different.

I've used ProtonVPN, Windscribe, NordVPN, and Private Internet Access.

Pick one that values your privacy and has a user interface that's easy for you.

Make sure you get a VPN that constantly changes your IP so that you don't establish a pattern during logons or during interaction.

6. Social Media Profiles

Now that you have a dedicated computer, encrypted email, phone number, and VPN, we can get to the fun part.

You can use all of your information (email, phone number) to create your social media profiles of choice.

Since you're starting from scratch, it's important you start interacting in an organic way.

This could **include** following people, posting links, doing status updates, interacting with people in the same niche as your target, etc.

This process will take a long time if you do it right. If you're really skilled, your target will come to you.

I recommend **creating multiple avatars** with multiple emails and phone numbers to decrease your risk and to deploy them in different ways.

More on this later.

7. Virtual Machine

Virtual machines are a great way to create an additional layer of privacy.

You can also use them for specific tools in your OSINT investigation.

I recommend starting with Buscador as it offers a wide variety of OSINT tools.

You can also experiment with Windows VMs to access tools like FOCA and other Windows specific tools.

Experiment with Android emulators to take advantage of mobile apps.

Nox is an excellent emulator to get you started.

8. Blog

If you want to go another layer deep on your avatar, create a free blog on WordPress, Medium, or Blogger and link it to your social media

profile.

Generate content both on social and your blog to increase credibility.

After a period of development, you will have a complex character that's believable and valuable.

9. Chrome Extensions

Part of remaining anonymous on the web is blocking all forms of tracking.

The two extensions I'd recommend of the top of my head are AdBlock and Disconnect Me.

These will stop ads from tracking you as well as all pull requests from social media sites.

Combined with a VPN, you should have what you need to search safely.

10. Bonus

• Once you've developed all of the above, you may want to verify yourself on Keybase and get involved in other opportunities such as Slack

channels or Rocket Chats

• This will grant you an opportunity to open a dialogue with your target or associates in an environment separate from social media.

• Some mistakes Wohl made was using stock images that were easily traceable through image search, not using Whois protection during domain registration, using his socks too soon, and not collecting OSINT/investigating himself before deployment.
Read Aric Toler's write up on this for lessons learned.

Search Engine OSINT

Advanced Search: https://www.google.com/advanced_search

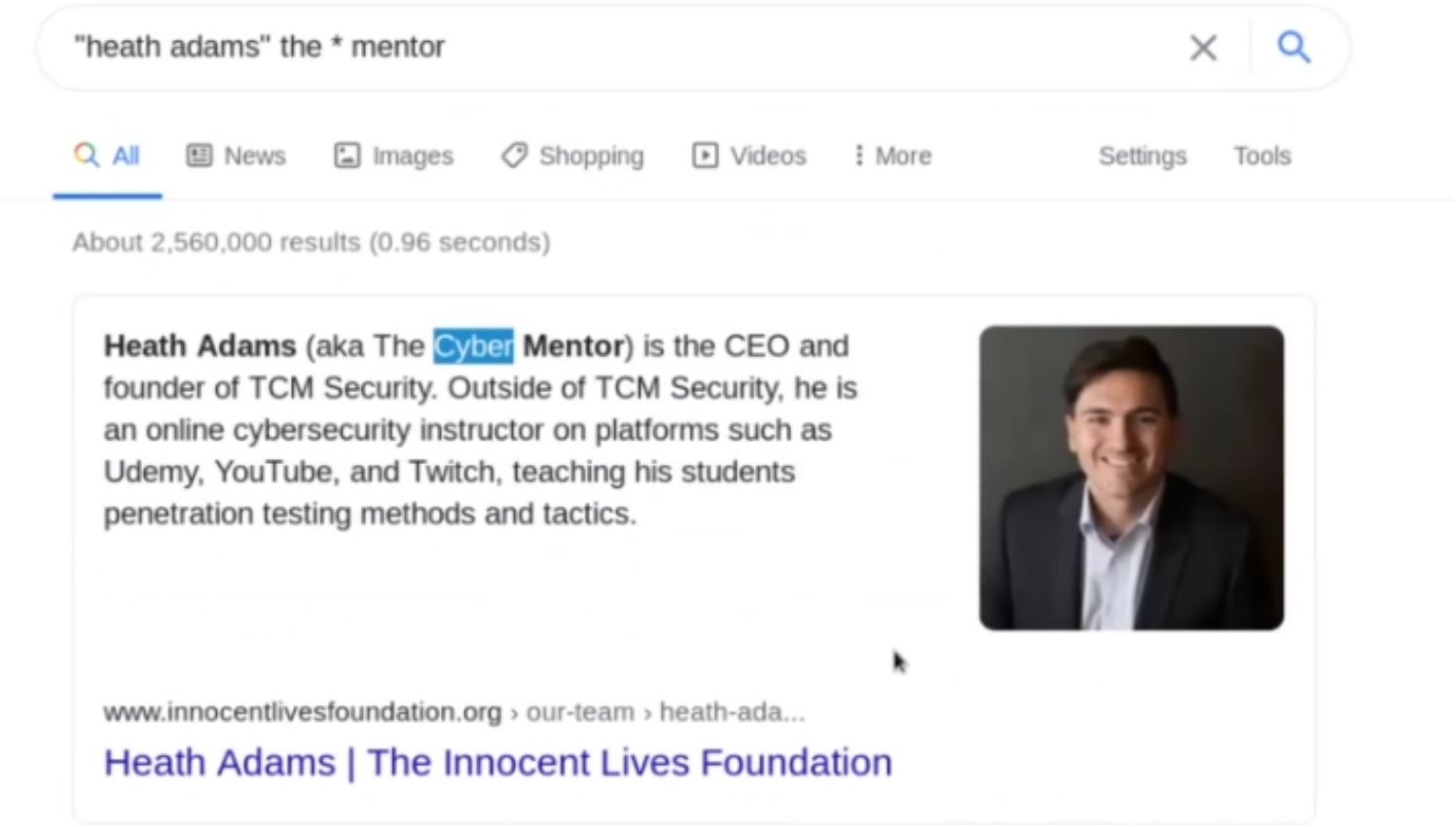
Google Cheat Sheet: https://kinsta.com/blog/google-search-operators/

Google Search Operators List

Here is a complete list of all working Google advanced search operators:

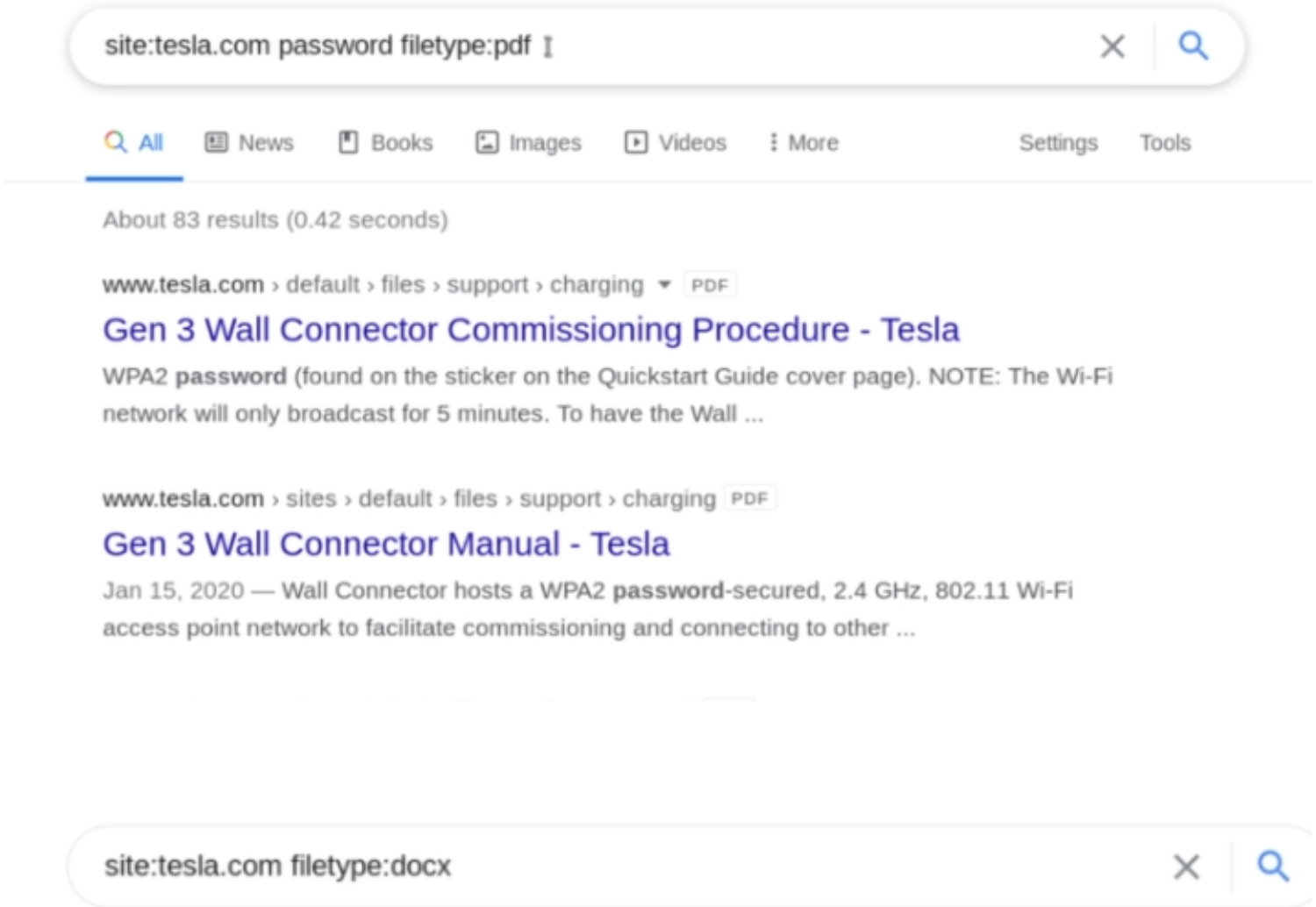
- **"search term"** Use this to do an exact-match search.
- **OR** Search for this OR that. This will return results related to the two terms or both.
- **AND** Search for this AND that. This will only return results related to the two terms
- **–** Exclude a term or search phrase.
- ***** Acts as a wildcard and will match any word or phrase.
- **( )** Groups multiple terms or operators to control how the search is shown.
- **$** Search for prices.
- **define**: Displays the meaning of a word in a card-like result.
- **Cache:** Returns the most recent cached version of a web page (as long as the page is indexed).
- **filetype:** Shows results of a certain filetype (PDF, DOCX, TXT, PPT, etc.)
- **site:** Limit results to a specific website.
- **related:** Find sites related to another site.
- **intitle:** Find pages that contain a specific word in the title.
- **allintitle:** Like "intitle," this finds web pages containing all of the specific words in the page title.
- **inurl:** Finds pages with a certain word in the URL.
- **allinurl:** Similar to "inurl," this finds web pages containing all of the URL's specific words.
- **intext:** Finds pages containing a specific word in the content.
- **allintext:** Finds results containing all of the specific words somewhere on the page.
- **AROUND(X)** This proximity search finds pages containing two words (or phrases) within X words of each other.
- **weather:** Finds the weather for a specific location.
- **stocks:** See stock information
- **map:** View map results for a location search.
- **movie:** Finds information about a specific movie.
- **in** Convert one unit into another (like currencies, weights, temperatures, etc.)
- **source:** Find news results from a certain source within Google News.

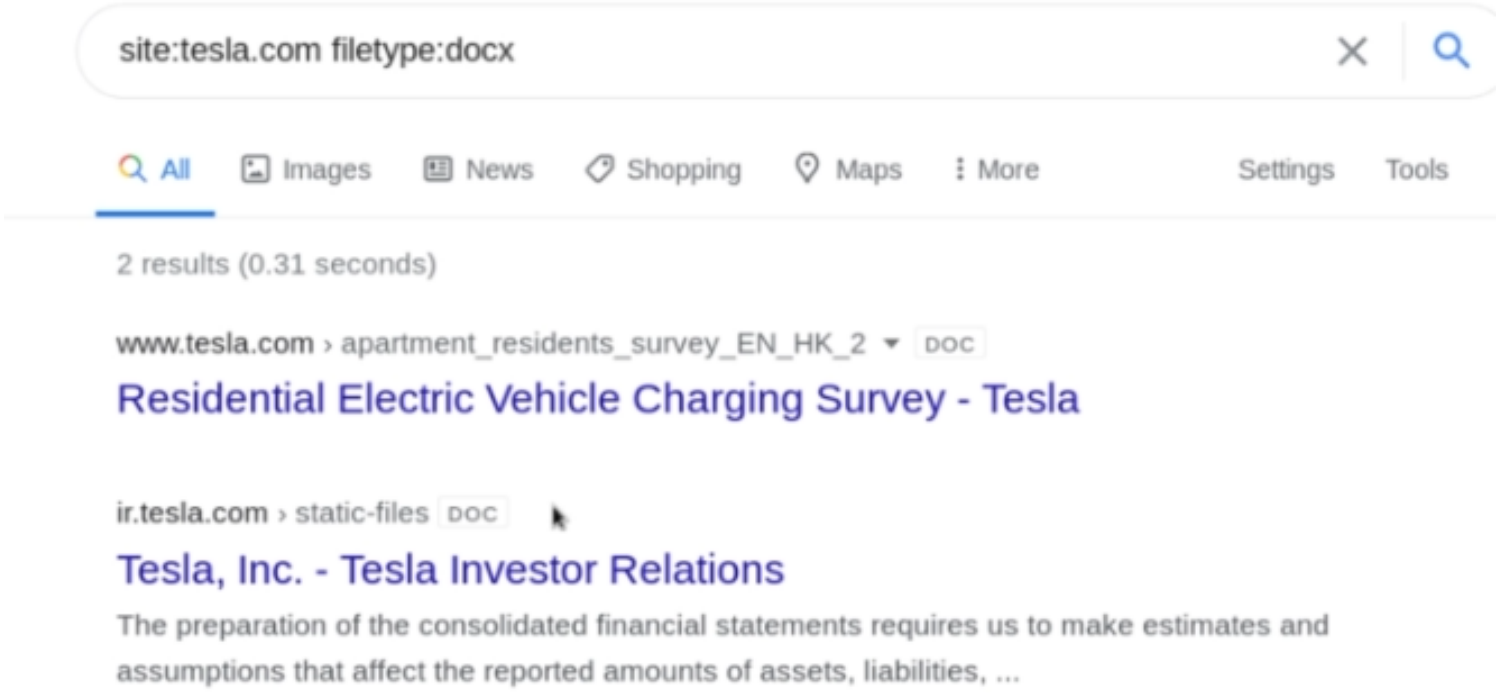
Search for person



So what we might do here is say we're looking at Tesla so we know we want to look at site Tesla.
So a site:Tesla.com
And maybe we want to look for the word password and that's going to bring up some meds is we get the

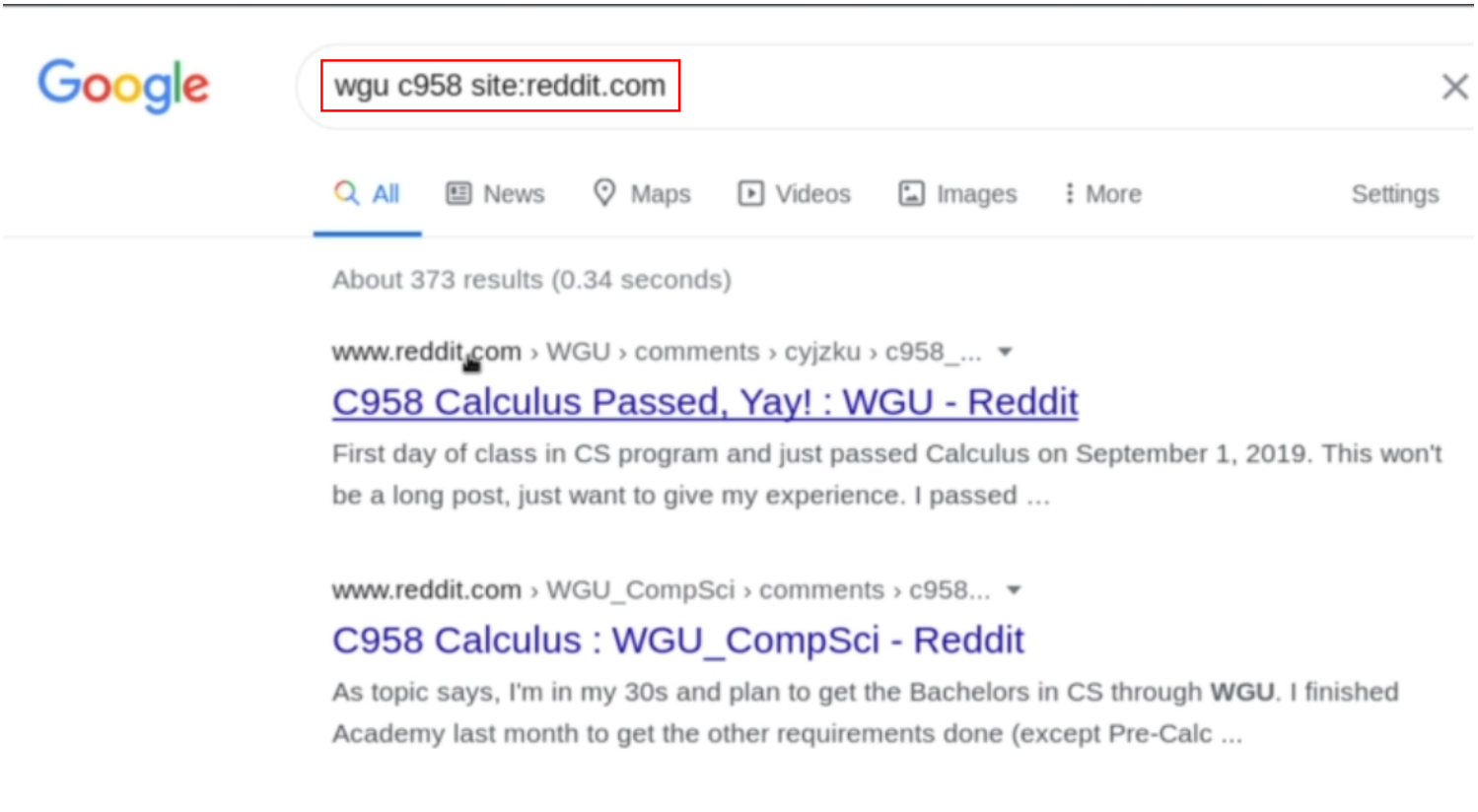
So we're searching is we're saying, hey, I want to look for the word password in the site. Tesla with a file type of PDF hit enter.

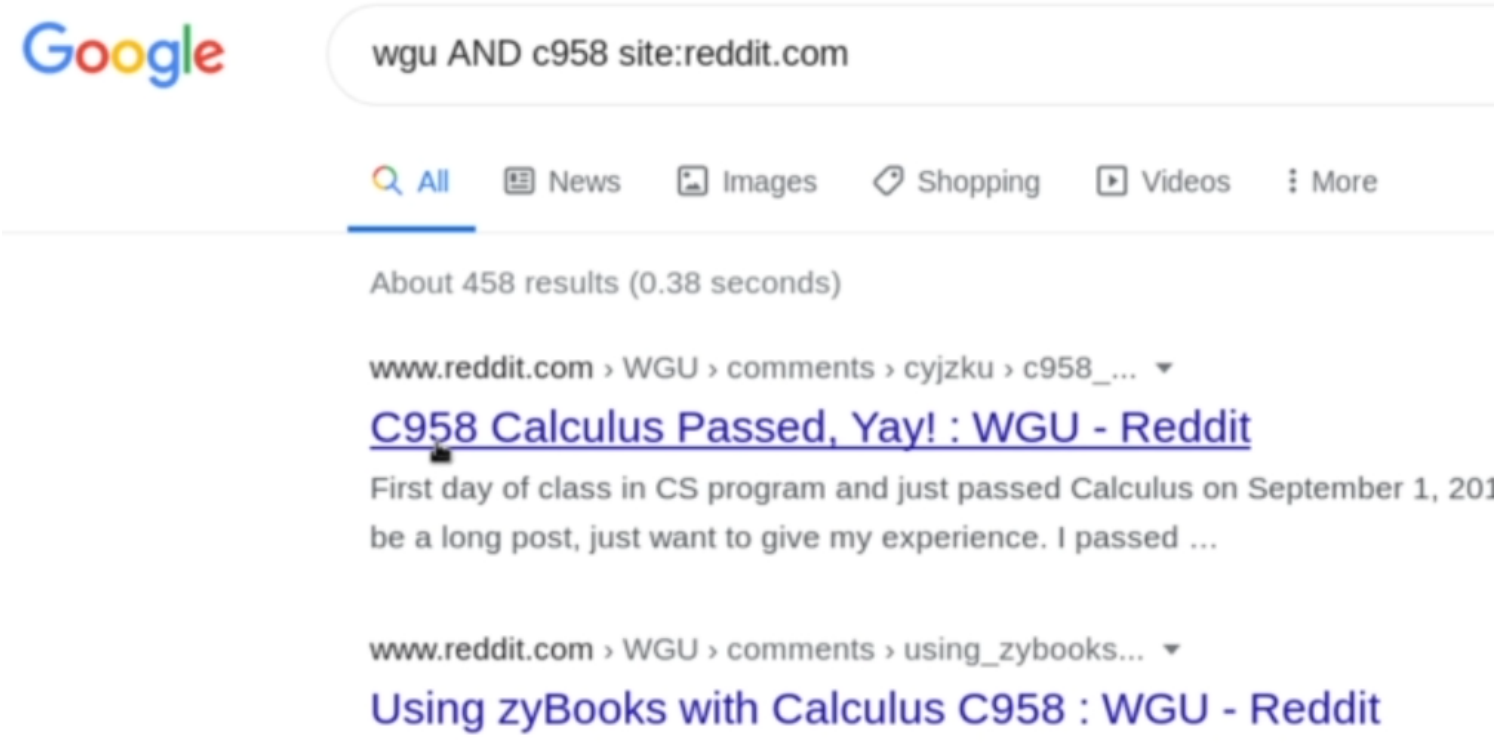


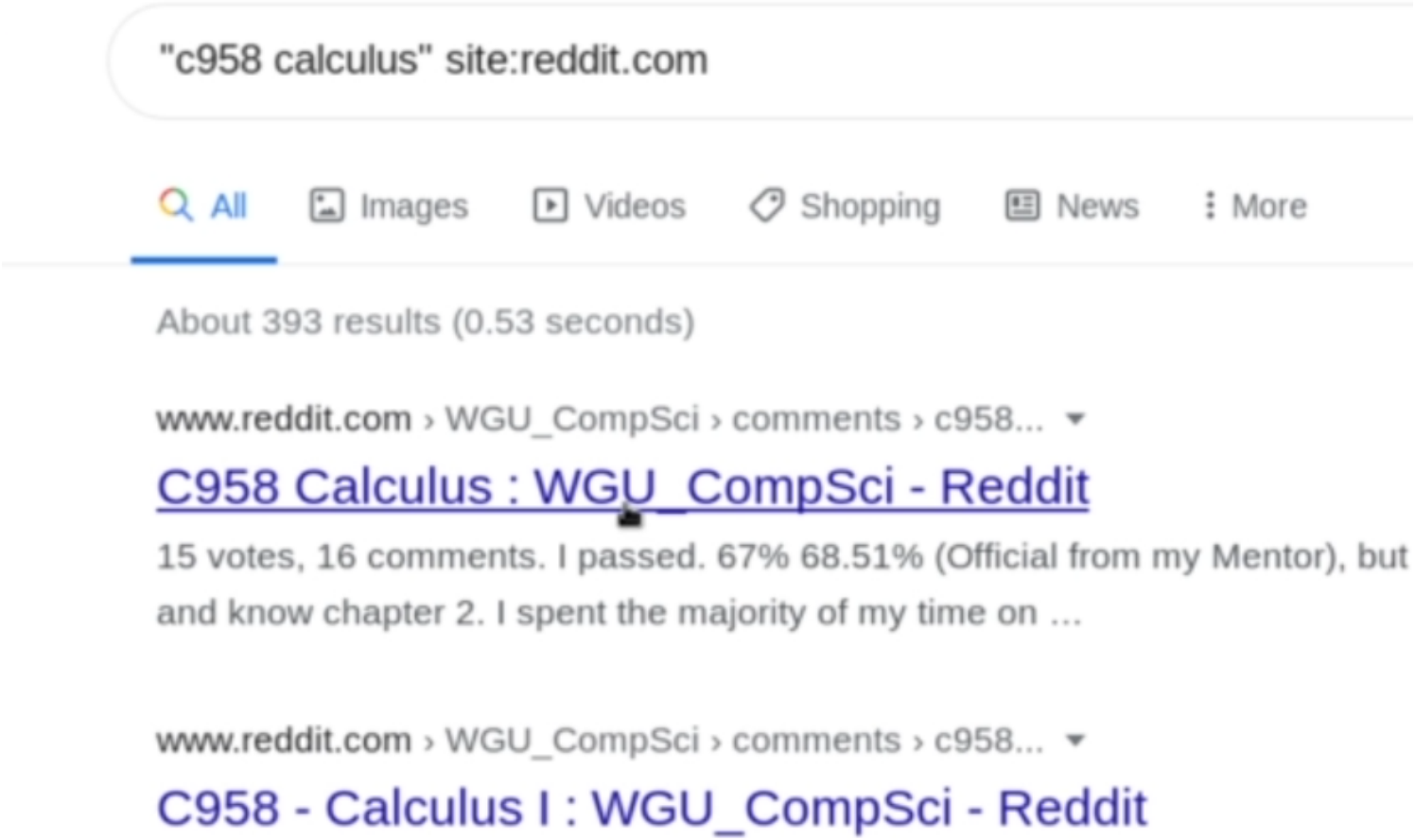


Example

Sources:


Google
wgu c958 site:reddit.com
All
News
Maps
Videos
Images
More
Settings
About 373 results (0.34 seconds)
www.reddit.com › WGU › comments › cyjzku › c958_...
C958 Calculus Passed, Yay! : WGU - Reddit
First day of class in CS program and just passed Calculus on September 1, 2019. This won't be a long post, just want to give my experience. I passed ...
www.reddit.com › WGU_CompSci › comments › c958...
C958 Calculus : WGU_CompSci - Reddit
As topic says, I'm in my 30s and plan to get the Bachelors in CS through WGU. I finished Academy last month to get the other requirements done (except Pre-Calc ...


Google
wgu AND c958 site:reddit.com
All
News
Images
Shopping
Videos
More
About 458 results (0.38 seconds)
www.reddit.com › WGU › comments › cyjzku › c958_...
C958 Calculus Passed, Yay! : WGU - Reddit
First day of class in CS program and just passed Calculus on September 1, 201
be a long post, just want to give my experience. I passed ...
www.reddit.com › WGU › comments › using_zybooks...
Using zyBooks with Calculus C958 : WGU - Reddit


"c958 calculus" site:reddit.com
All
Images
Videos
Shopping
News
More
About 393 results (0.53 seconds)
www.reddit.com › WGU_CompSci › comments › c958...
C958 Calculus : WGU_CompSci - Reddit
15 votes, 16 comments. I passed. 67% 68.51% (Official from my Mentor), but and know chapter 2. I spent the majority of my time on ...
www.reddit.com › WGU_CompSci › comments › c958...
C958 - Calculus I : WGU_CompSci - Reddit

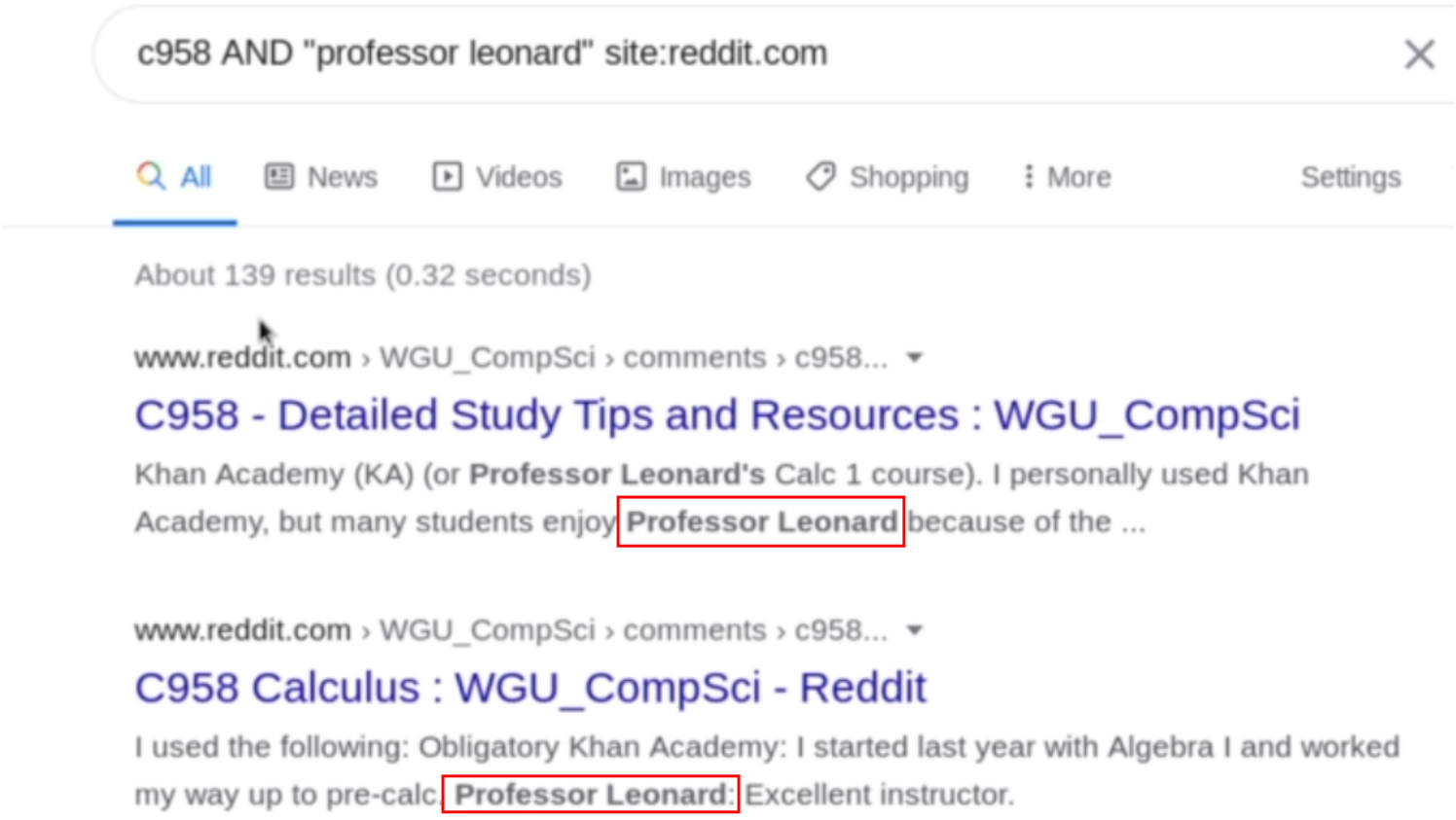

c958 AND "professor leonard" site:reddit.com
All
News
Videos
Images
Shopping
More
Settings
About 139 results (0.32 seconds)
www.reddit.com › WGU_CompSci › comments › c958...
C958 - Detailed Study Tips and Resources : WGU_CompSci
Khan Academy (KA) (or Professor Leonard's Calc 1 course). I personally used Khan Academy, but many students enjoy Professor Leonard because of the ...
www.reddit.com › WGU_CompSci › comments › c958...
C958 Calculus : WGU_CompSci - Reddit
I used the following: Obligatory Khan Academy: I started last year with Algebra I and worked my way up to pre-calc. Professor Leonard: Excellent instructor.

Image OSINT

Google Search Image: https://images.google.com/

https://tineye.com/

https://yandex.com/images/

Reverse Image Searching

Viewing EXIF Data

Search Image Data: http://exif.regex.info/exif.cgi

This is to detect the existed photo.

This tool remains available so long as I can keep it free and the bandwidth doesn't cost me too much. A gift of thanks is always appreciated, but certainly not required. Send a gift via PayPal, or perhaps an Amaz
perhaps send me some good karma by doing something kind for a stranger.

If you have questions about this tool, please see the FAQ.

Basic Image Information

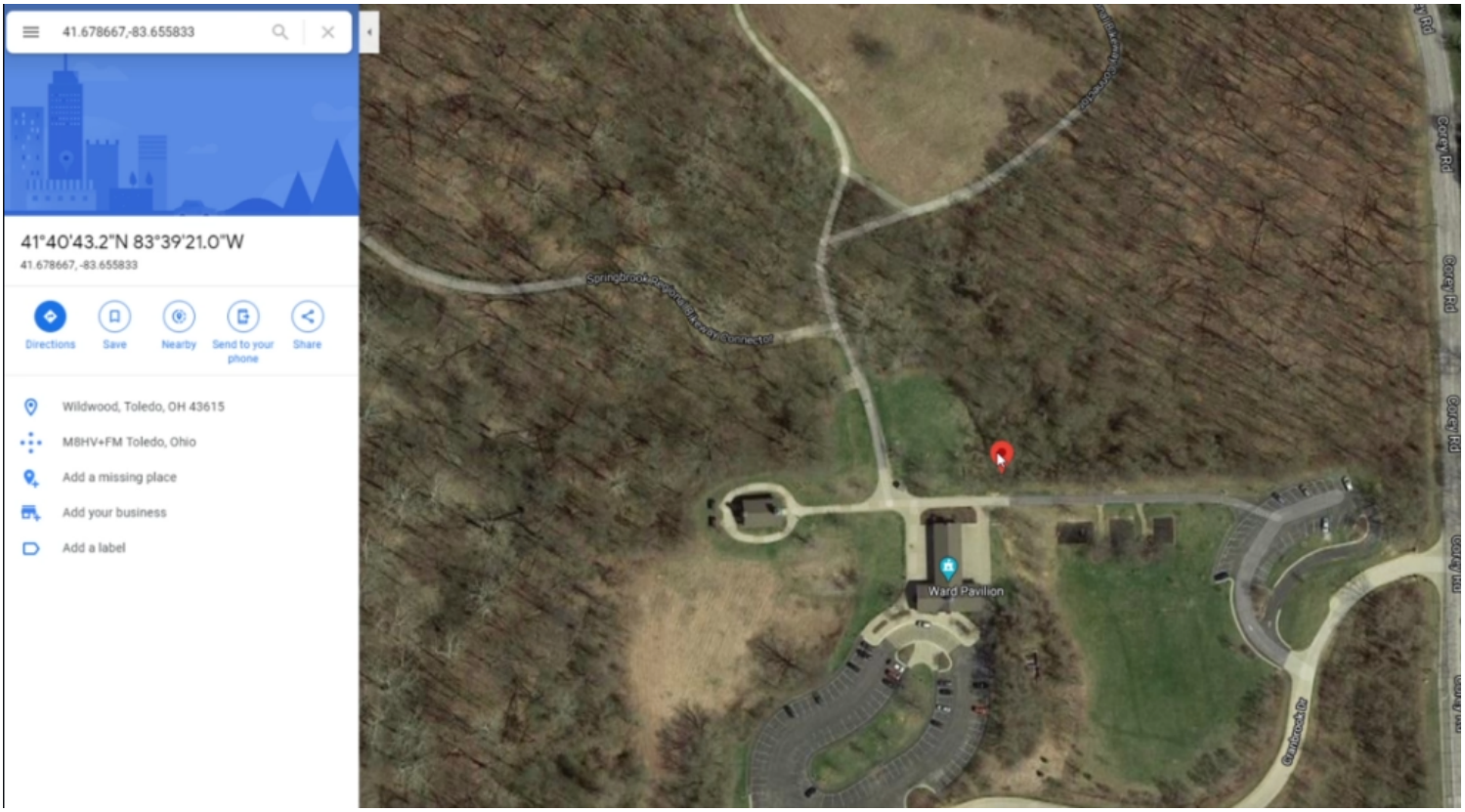
Target file: IMG_0021.JPG

Camera:	Apple iPhone 4S
Lens:	4.3 mm
Exposure:	Auto exposure, Program AE, 1/1,842 sec, f/2.4, ISO 64
Flash:	Off, Did not fire
Date:	**March 11, 2012** 12:01:53PM (timezone not specified) (8 years, 8 months, 5 days, 8 hours, 38 minutes, 58 seconds ago, assuming image timezone of 5 hours behind GMT)
Location:	Latitude/longitude: **41**° 40' 43.2" North, **83**° 39' 21" West (41.678667, -83.655833) Though the photo is not related to Jeffrey's blog, as an aside, you may want to see photos on his blog that might be near this location. Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Altitude: 182 meters (597 feet) Camera Pointing: South-southwest Timezone guess from earthtools.org: 5 hours behind GMT
File:	**3,264** × **2,448** JPEG (**8.0** megapixels) 3,947,861 bytes (3.8 megabytes)
Color Encoding:	**WARNING:** Color space tagged as sRGB, without an embedded color profile. **Windows and Mac browsers and apps treat the colors randomly**. Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.

1:1 Extracted **160** × **120** 9.7-kilobyte "EXIF:ThumbnailImage" JPG
Displayed here at 200% (1/104 the area of the original)

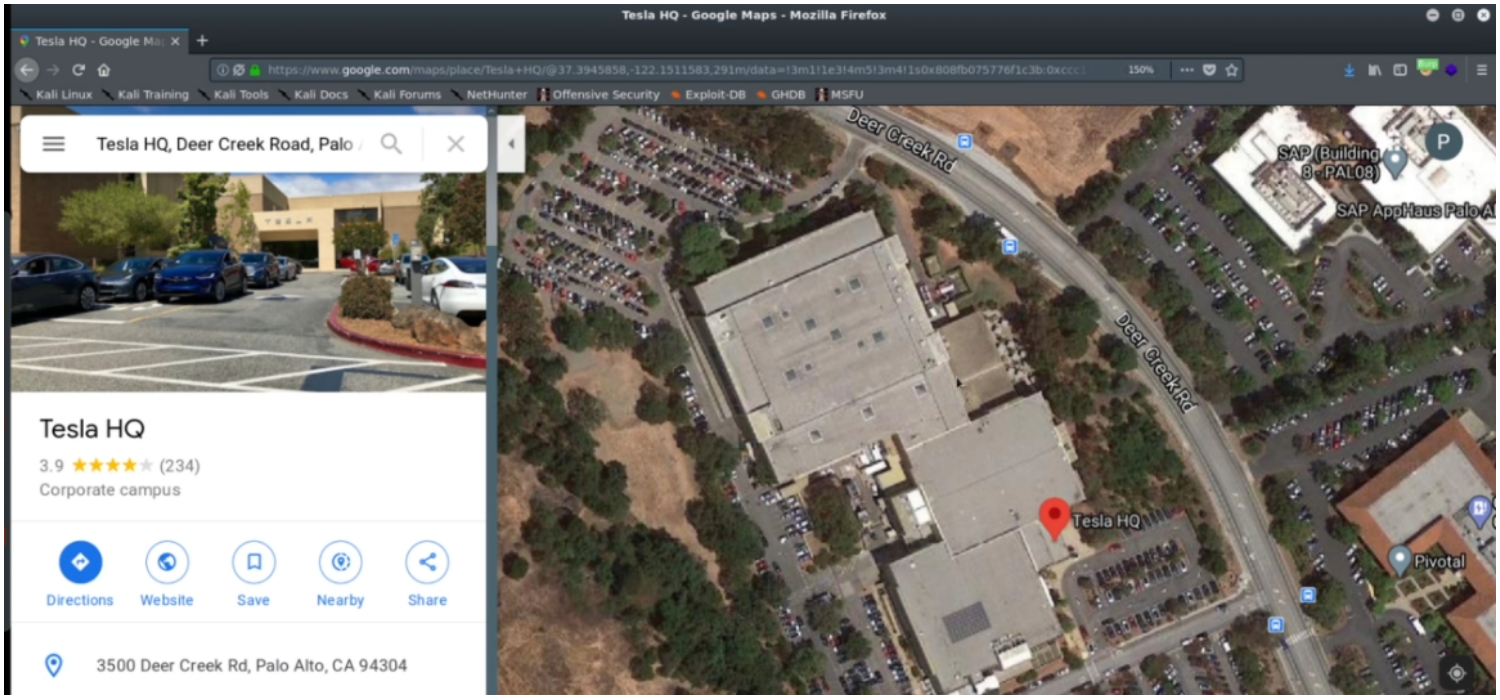
Click image to isolate; click this text to show histogram

1:1 Main JPG image displayed here at 14% width (1/53 the area of the original)



Physical Location OSINT

- **Always try to have the feel on the site**



- **Inspect the area of the target**

Look at all the different tussles around here, so we could try to click through and see if we can find anything.

- Are there any doors that might be of interest?

- Like do we see a door and what's on the door?

- Is there badging?

- You know, can we find or identify any sort of like badge readers, card readers?

- Are employees going to these specific areas to smoke?

- Like, is there a smoke area back here behind the building?

Because that's a really good place to target as well.

If you're trying to do social engineering or you're trying to, you know, just navigate your way in a lot of times employees will just prop doors open. Or, if you go outside and have a cigarette with an employee and you just kind of chat them up, they're more likely to just let you in and hold the door open for you.

So that's not out of the ordinary.

Looks like to have a backpack, no shoes.

It looks like a lot of these people are wearing red.

So it looks like maybe there's some sort of Tesla employee dress code if you're working right here.

Maybe these people are doing some sort of, you know, checking people in and checking people out,