

All Things OSINT & OnlyFans

Sharing some OSINT techniques for OnlyFans! This article should probably be considered NSFW.



Open-source intelligence techniques for OnlyFans!

****OBLIGATORY DISCLAIMER:****

OnlyFans™ is a [registered trademark](#) of Fenix International Limited. Myself and any other contributors to this article are NOT in any way affiliated with, sponsored by, or endorsed by Fenix International Limited.

Myself and any other contributors of this article are NOT responsible for the actions of any end users.

In other words, don't be malicious.

OnlyFans? What?

What exactly is OnlyFans and why should you care?

[OnlyFans](#) is a website where users can subscribe to content creators and access their digital content as well as interact with the creators themselves. While not every creator offers nudes and NSFW content, there are artists, musicians, fitness professionals, models and so on. Although its estimated that around ~80% of creator accounts offer porn. So its safe to say they OnlyFans basically is a website where people can purchase a wide range of *mostly* pornographic content offered by women, men, transgender, he/him, she/her, they/them, ect. So, whatever it is that works for you, it's probably offered on OnlyFans (Unless it's kids.. Then you need to leave, right now).

As described by their [Wikipedia page](#) ([WikiLess](#)):

"OnlyFans is an internet content subscription service and based in London. Content creators can earn money from users who subscribe to their content - the "fans". It allows content creators to receive funding directly from their fans on a monthly basis as well as one-time tips and the pay-per-view (PPV) feature. The website has over 2 million content creators and over 130 million users."

Great, so what does some porn site have to do with OSINT? Well, most of the time it doesn't. However, since this website has grown so massive in the last few years due to people being stuck in lock downs, losing their jobs and being increasingly horny thanks to (((COVID-19))).

So because of its increasing popularity, it can be utilized as a great OSINT resource.

There have been cases that I have personally seen that involved people who have been forced to create content as a result of human trafficking, sexual exploitation and even rare cases of child

pornography. Also things like revenge porn, blackmail, catfishing, and straight up theft are more common place than one would like to believe..

So clearly those examples involve some pretty serious illegal activity.

This is why I have decided to write a small article that covers OnlyFans OSINT techniques. I have also not seen that many OSINT related write-ups out there regarding OnlyFans, so I figured I should make one as I feel that it would benefit the intelligence community as a whole.

What I have written here will *hopefully* assist investigators and/or law enforcement agents alike to learn some new techniques that can be utilized during their work.

Alright enough talk, lets get started.

The first thing you need to know is that there are two types of OnlyFans accounts. "**Creator**" accounts and "**User**" accounts.

For general OSINT things, having a creator account is not needed at all. So for this article, we will be focusing on using a user account to gather information on creator accounts as well as other user accounts. So let me guide you through the simple process of creating a sock-puppet account separate from your personal account (I know you have one, don't lie).

Another few things that you should have a look at before creating your sock-puppet account are the OnlyFans [Terms of Service \(Wayback\)](#), ([archive.today](#)), and the OnlyFans [Privacy Policy \(Wayback\)](#), ([archive.today](#)). For law enforcement, check out the OnlyFans [Law Enforcement Guide \(Wayback\)](#), ([archive.today](#)).

Sock Puppet Account Creation

First, make sure you are doing all of this from a disposable and/or dedicated OSINT VM and make sure all of your connections are tunneled through a VPN. You just never know who is watching (Hello NSA glowies!), so it's best to stay on the safe side.

Now you can head over to <https://onlyfans.com/> and click on "**Sign up for OnlyFans**".

For this, I assume you have already created a burner email address. If you haven't, go do that now.

Now just fill in the required information. Click "**Sign Up**" and confirm your email address by checking the inbox of your burner email and login.

Do not add a bio, location or anything else as there is not really any need for any of it. You *can* add a generic profile picture to your account if you really want too, but most other user accounts do not have a profile picture. So it's best that you don't bother uploading one, as its always better to blend into the crowd rather than stick out!

NOTE:

DO NOT use your real name or any usernames that are even remotely related to you!*

Content creators as well as other users are able to see any information you enter on your profile.

Including username, display name, profile picture, header image, bio, location, and so on.

So just don't bother.

That's it, you have created a fresh sock-puppet profile. Pretty simple right?

Secure Purchasing

Although there are many times you will encounter an account that is free to subscribe, but in order to follow a free account, OF still requires you to have a payment method attached to your account. Its highly recommended that you do not use your personal credit cards, VISA debit cards, or bank accounts for OPSEC reasons.

Keep in mind that when you purchase a subscription, the content creator is unable to see any payment information at all. All they can see is your username and any other information displayed on the sock-puppet profile. However, using any payment methods that are attached to your IRL identity is never a good idea.

NOTE:

This method has only been tested in Canada and the United States. I am not sure how pre-paid credit cards work in other countries and locations. If you know, please enlighten me.

The method that I find works well is utilizing the Vanilla pre-paid MasterCard gift cards. You can find these cards at petrol stations, convenience stores and big box stores like Wal-Mart or Target. When buying these cards, be sure to always pay with physical currency (AKA, Cash), this avoids any kind of paper trail and keeps your OPSEC on point.

Extra tip for the extra paranoids:

After purchasing the Vanilla pre-paid card, take the card out of its packaging, throw the packaging in one or more different garbage bins.

First, make sure that ALL of your radios are disabled on your mobile device before taking pictures of the card! Wi-Fi, Bluetooth, Data, Location, NFC, etc, should all be disabled.

*Are they all disabled? Great, now take a picture of the front and back of the card with your phone and **DO NOT** connect to anything until you are home. This will ensure that these images are not being potentially backed up to any cloud services or shared in any way.*

Next, cut the card up in three to four separate pieces and dispose of each piece in separate garbage bins spread around the area. Doing this is mostly overkill, but it will ensure your purchase extremely obfuscated.

Now you need to register the prepaid card in order to use it for online purchases. Connect to a VPN first, then go to the URL listed on the back of the card. Should be the URL or something similar; <https://vanillaprepaid.com>.

Login with the card information, then click **"Assign Postal Code"**. For this you will need a valid postal/ZIP code. **DO NOT** use your own, instead head over to the [Fake Name Generator](#) website, select a city near your location and use the information provided to register the card. Make sure you use a location in the same state/province and country. This is very important, if you do not. Then the pre-paid card will likely not work!

Also, be sure to save this information somewhere safe as you will need it later.

Now enter the card details and link the pre-paid card to your OnlyFans account. Be sure to enter the same information used when you activated the card, to avoid any issues. Once the card is linked, you should be able to subscribe to both free and paid OF accounts.

Locating Accounts

OnlyFans actually does not provide a search function on their site for whatever reason, so you will need to get creative when searching for accounts. If you already know the username, then your work here is done. If not, then you can use Google dorks and/or third-party search sites to search via username, display name, location or keywords.

Here are some examples to search Google for OnlyFans accounts via location or keywords.

```
site:onlyfans.com "New York"  
site:onlyfans.com "Timbuktu"  
site:onlyfans.com "OSINT"  
site:onlyfans.com "keyword"
```

This of course will not only give you accounts from New York, but also any user bios and posts that include the string "New York". This technique is not that effective, but a good first step I guess.

There are a few different sites that index OnlyFans profiles and makes them searchable. My go-to is [OnlyFinder](#), which allows you to search for users, bios and posts via keywords, usernames and geographic locations. Example how to search via location on OnlyFinder:

```
location:"Timbuktu, Mali",50km
```

Here are a few more sites worth mentioning;

- [OnlySearch](#)
Search for OnlyFans accounts via username or keywords.
- [FansMetrics](#)
Lets you search for accounts by username and provides metrics and analytics for a given account.
- [FindrFans](#)
Allows you to search by a username, country, and a few different US states.
- [Hubite](#)
OnlyFans profile search, includes a price filter.

Another simple trick is to search social media link sharing sites like [Linktr.ee](#) and [AllMyLinks](#), as content creator's often use these types of sites to keep all their social media accounts in one place. However, you cannot search these sites directly as they don't include a search function. This is where Google dorking comes in handy once again. Here are a few simple dorks you can use to help locate these types of accounts. Get creative with your Google dorks!

```
site:linktr.ee intext:"onlyfans"  
site:allmylinks.com intext:"onlyfans"  
site:linktr.ee intext:"<Real name or any known usernames>" AND "onlyfans" OR "OF"  
site:allmylinks.com intext:"<Real name or any known usernames>" AND "onlyfans"  
site:linktr.ee intext:"<Location>" AND "onlyfans"
```

Another great place to look is [Reddit](#), as plenty of creator's use Reddit to promote their accounts. You can utilize the Reddit search function as well as dorks. Below are a few examples.

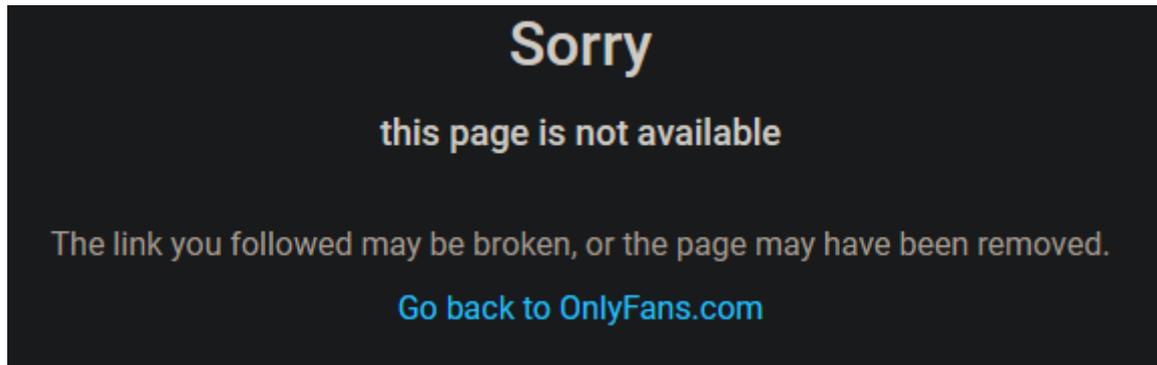
```
site:reddit.com intext:"onlyfans"  
site:reddit.com intext:"<Any known usernames>" AND "onlyfans"  
site:reddit.com intext:"<Location>" AND "onlyfans" OR "OF"  
site:reddit.com inurl:"u/<Any known usernames>" AND "onlyfans"
```

Often times you will encounter a Reddit post of interest that has been previously deleted, and you see the dreaded `u/[deleted]` on the post. This is very annoying at times I know, but Reddit posts (Especially NSFW posts) are very commonly archived on both the [Wayback Machine](#) and [archive.today](#). So be sure to check those as you might get a hit!

Reddit posts are also archived using the [Pushshift API](#), although images are not usually saved. Only the original URLs to the images are provided. All text, usernames and comments are all saved, even if they have been recently deleted, you can still view them. One of the best tools for searching for deleted Reddit posts is this [Reddit Search](#) tool. So be sure to check there as well.

Content creators are also able to restrict access to their accounts by geo-blocking certain locations.

For example, if you are using an IP address located in Canada and are attempting to view an OF profile that has blocked access from Canadian IPs. You will get an error when loading the page as shown in the screenshot below.



Example of an OnlyFans 404 error due to geo-blocking.

To mitigate this simply connect to TOR, or a VPN, or just use a SOCKS5 proxy and connect from a different location such as the United States or somewhere in Europe.

If you are still unable to locate a users profile using these search methods but you have an image of their face. Try running it through the [PimEyes](#) facial recognition search tool, as they are the only service to my knowledge that indexes OnlyFans profile and header images.

UPDATE:

As of October 2021, PimEyes has removed their free tier for searches. All searches now require a subscription. Looks like they followed the Pipl business model.

Once you have their profile picture, you can then reverse image search it and *hopefully* be able to identify their username or other related profiles like Twitter, Instagram or Reddit as these social media sites are commonly used by content creators to promote their OF profiles, so you might just get lucky!

Information Gathering

Now that you have identified an account, you will want to record their username, display name, bio, outgoing links, profile picture, header image, prices, current promotions, number of posts, number of media, number of likes, date last seen and lastly their user ID.

It is always a good idea to both screenshot the page and copy the page as a single .html file for later reference.

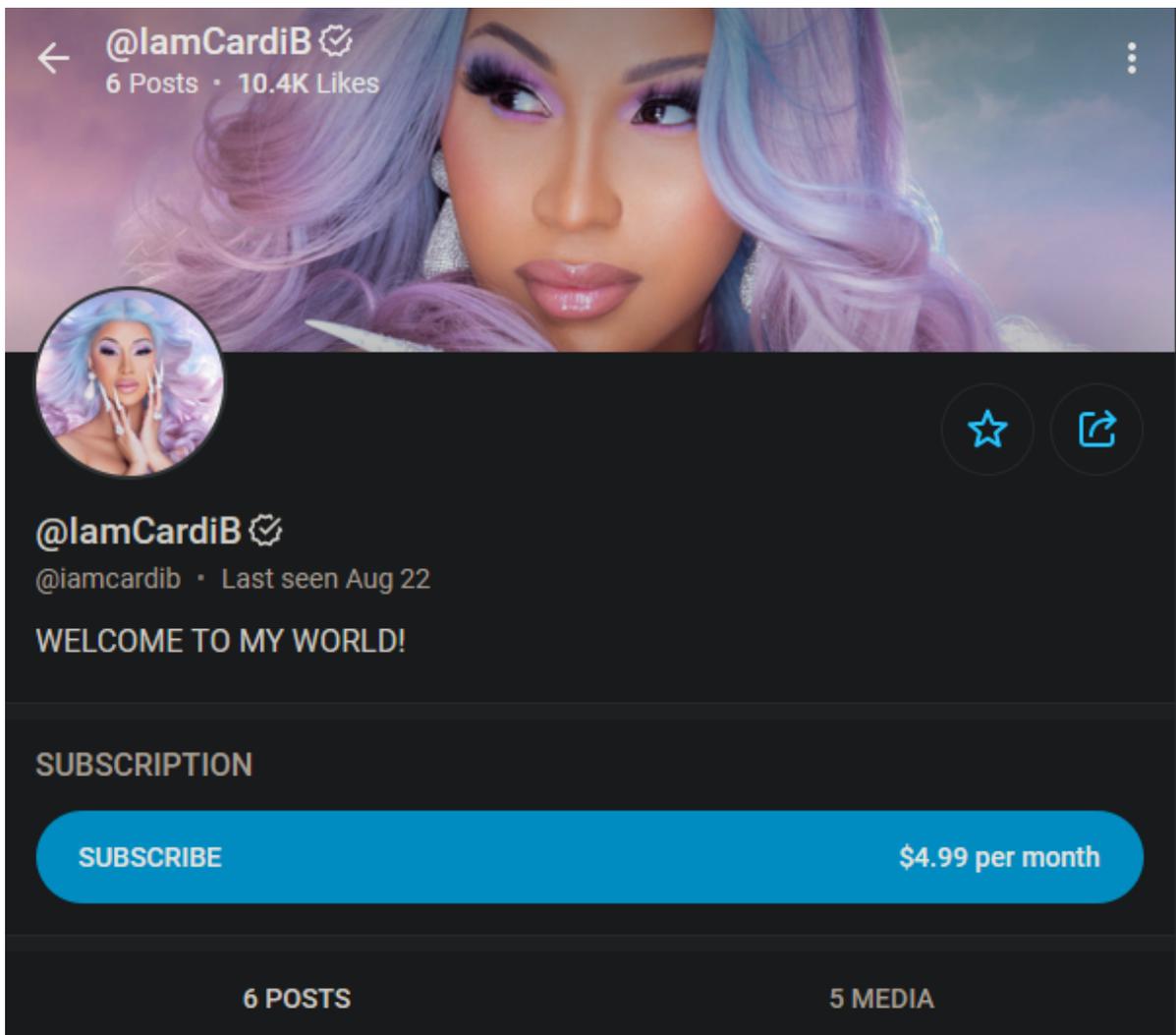
I personally use the [SingleFile](#) browser extension for this. Available for both [Firefox](#) and [Google Chrome](#).

The second thing you should gather is the user ID of the target account. Here is a quick guide on how to get the user ID of an OnlyFans profile, which will be essential in case the user decides to change their username. As the user IDs are permanent and do not change, so be sure to record this in your case file.

There are technically two different ways to pull a user ID. Although, this first method is preferred as it gives more data right off the bat.

For this article I am using Firefox, however the methods are the same if you are using Google Chrome.

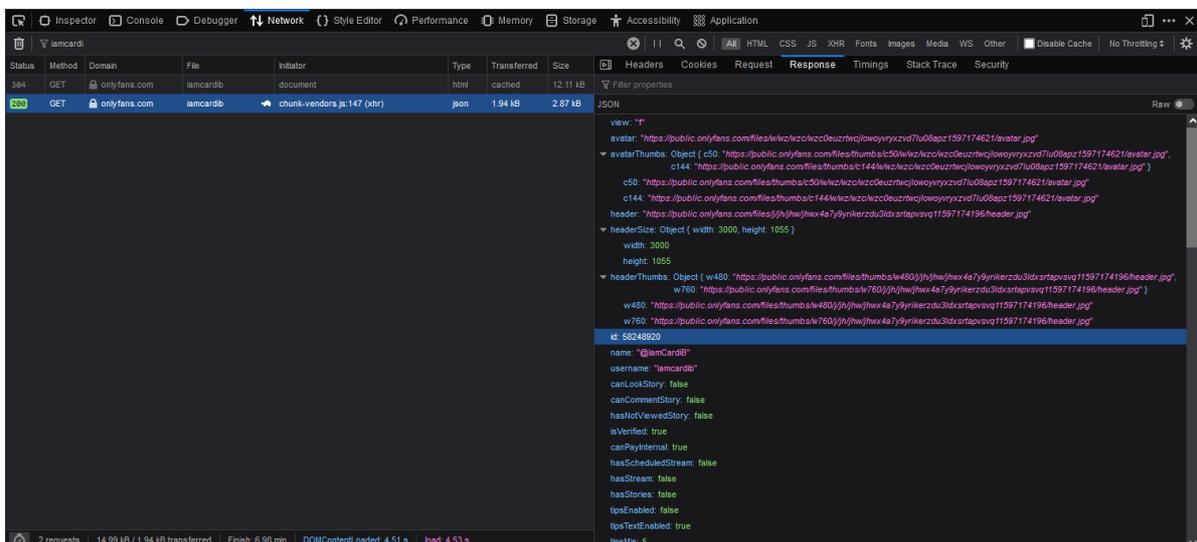
I'll also be using [Cardi B's](#) profile as an example here.



@iamcardib OnlyFans profile - Unsubscribed.

Next, open the **"Inspector"** menu and click on the **"Network"** tab. Hit F5 to refresh the page, now search for the target username in the search bar and you will be presented with user profile information in JSON format. Be sure to save the raw JSON data and open all of the *avatar.jpg* and *header.jpg* image URLs and save them all to your drive for later reference.

- <https://public.onlyfans.com/files/whatever/avatar.jpg>
- <https://public.onlyfans.com/files/whatever/header.jpg>
- <https://public.onlyfans.com/files/thumbs/whatever/avatar.jpg>
- <https://public.onlyfans.com/files/thumbs/whatever/header.jpg>



JSON information and user ID (Highlighted in blue) for @iamcardib.

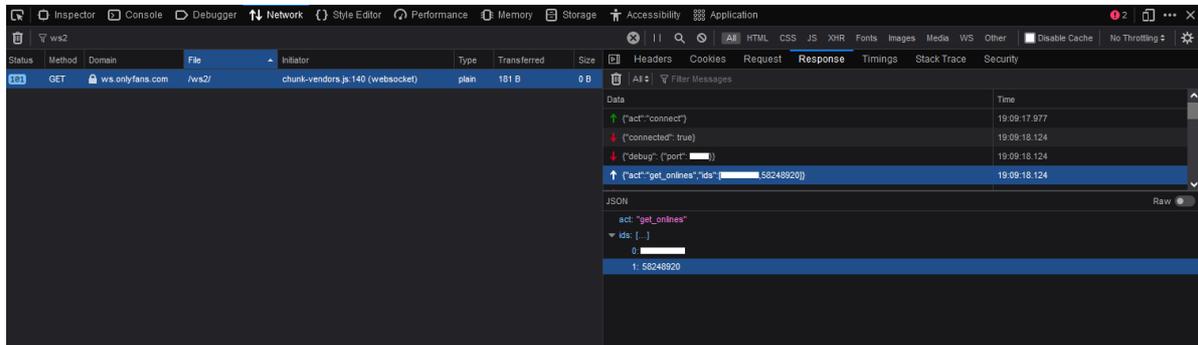
The second method just gives you the targets user ID as well as yours.

Open the **"Inspector"** menu again and open the **"Network"** tab, refresh the page again and search for `ws2`.

Click on the **"Response"** tab and select the `{"act","get_onlines","ids":["***"]}` response as seen below highlighted in blue.

The JSON results are under `ids: [...]` section.

Where as `ids 0:` is your user ID, and `ids 1:` is the user ID of the target profile.



Secondary method for obtaining OnlyFans user ID's.

Downloading Posts, Images and Videos

There are multiple ways of ripping content from OnlyFans, even though they try very hard to make the content "un-rippable" on their desktop website due to people leaking paid and copyrighted content. Which is fair enough I suppose.

Then again, since this is the internet, and the internet has zero regard for any sort of copyright infringement. Let's rip some content!

So the first and probably most common way to rip images and videos from content creator accounts is simply to just go through every single image and video and manually screenshot and/or screen record the content. Certainly not the most effective way of doing things as you will likely not get the full size images in their original quality.

This is no good, especially when dealing with any sort of private or legal cases as you would want the original, unchanged and unaltered data.

So, instead of wasting time with screenshots like a peasant, let's play with some tools.

This method seems to work the best, and this GitHub repository is always receiving new updates to circumvent things that the OnlyFans admins put in-place in an attempt to stop people from scraping data.

Apologies to the OnlyFans executives, web admins, devops teams and to any content creators that may be reading this article, but trying to prevent any online data from being scraped, saved, copied, re-uploaded and shared elsewhere on the internet is unfortunately a very futile exercise when dealing with pirates.

Sorry, but also not sorry.

Just remember kids, the internet always wins.

Open a terminal window and run the following commands to download and install this [handy python tool](#).

This tool was originally designed to be installed and ran on a Windows machine, but it works perfectly fine on Linux boxes. Tested and ran on an Ubuntu 20.10 VM.

```
git clone https://github.com/DIGITALCRIMINAL/OnlyFans.git
cd OnlyFans
pip install --upgrade --user -r requirements.txt
```

Next, configure your credentials. Open and edit this file using `vim`, or any other generic text editor.

```
vim .profiles/OnlyFans/default/auth.json
```

You will have to fill in the following information if you want to authenticate via session cookies:

```
"username": "your_username" `
"cookie": "your_cookie"
"user-agent": "your_user-agent"
```

To get your cookie and user agent, follow the steps explained in-depth on their [GitHub project](#) page. You can also change the settings in the `config.json` file if needed and specify how this script will run and what it will collect, these settings are also explained in the GitHub project's `README.md` file.

So go read it for goodness sake!

If you want to authenticate via browser instead, simply enter your OnlyFans email and password in the `auth.json` file under the following fields.

```
"email": "your@email"
"password": "your_password"
```

Here is an example of a properly configured `auth.json` file.

```
1  {
2    "auth": {
3      "username": "vxunderground",
4      "cookie": "auth_id=146996280; sess=n073v3nmyacc0untlma0;
5      auth_hash=; auth_uniq_146996280=; auth_uid_146996280=;",
6      "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
7      AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.101
8      Safari/537.36",
9      "email": "",
10     "password": "",
11     "hashed": false,
12     "support_2fa": true,
13     "active": true
14   }
15 }
```

Example of a properly configured auth.json file.

Once all of your authentication and whatever optional configurations you wanted are finished, save the changes and run the script like so, then just follow the on-screen prompts.

```
python3 start_ofd.py
```

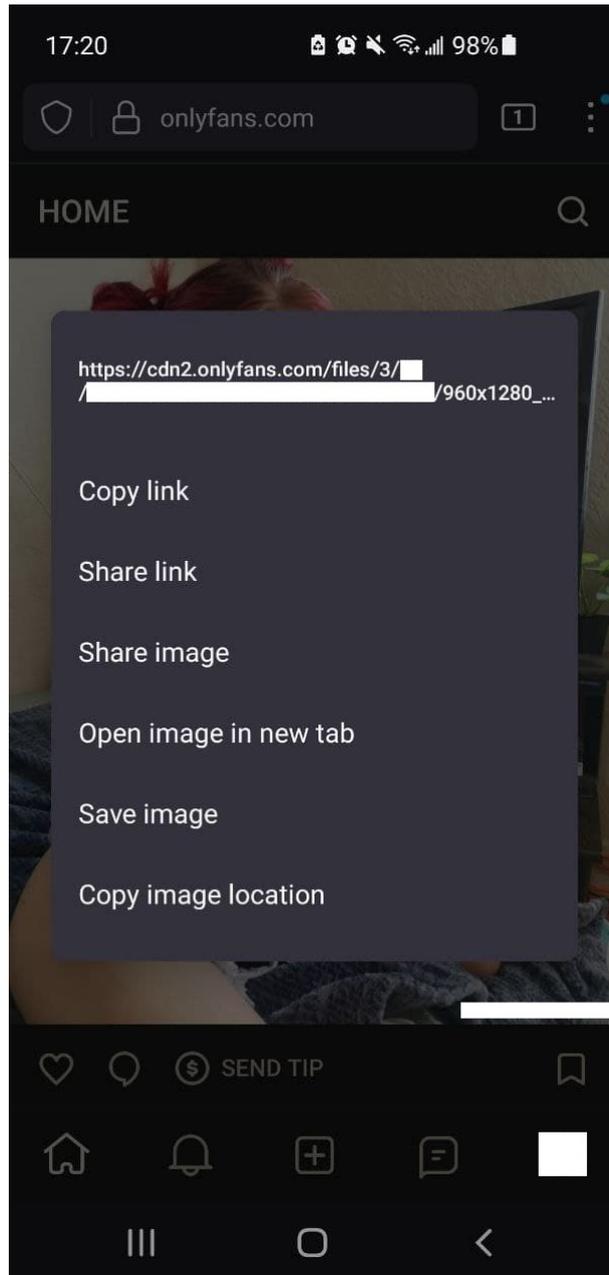
NOTE:

There is always a chance that using this tool and others like it can potentially get your sock-puppet account banned due to it technically being against the [OnlyFans ToS](#) - Under the "Acceptable Use Policy", section 19. Imao.

*This has not happened to me ever, but **the risk is certainly not zero**. So keep that in mind and don't blame me if your OnlyFans account gets banned! You now know the risks.*

Another way you can rip content from OnlyFans is by using an either an actual Android device, or an emulated Android device and the Firefox app.

Login to your account, locate the creator account you wish to rip, then manually open each image and video, then "[long.press](#)" ([Wayback](#)), ([archive.today](#)) on each and every item and click "**Save Image**" and/or "**Save File to Device**".



Example of the "Save Image" option on an Android device using Firefox.

This method is extremely tedious and very time consuming as it requires you to go through every single image and video manually just like you were trying to screenshot or record everything manually. Certainly not ideal, but it does work. Plus the data you download will be the original files, just make sure that you actually open the full images or open each image in a new tab

before clicking on **"Save Image"**.

This will ensure you are getting the full and original resolution of the images.

Images that have been ripped correctly will have a similar filename as the following examples depending on the images original resolution.

Some older image posts (Pre-2019 I believe) will not include the resolution size at the beginning of the filename.

```
3840x2880_05de53e0721044574e51e5b1bd51cd5c.jpg
2316x3088_2532803da569739440bafdaf2fcb7b53.jpg
960x720_d7d3ab44666d0c46a926da600b1243a5.jpg
3402d2ce9b02e50721b09ebe0a077e39.jpg
```

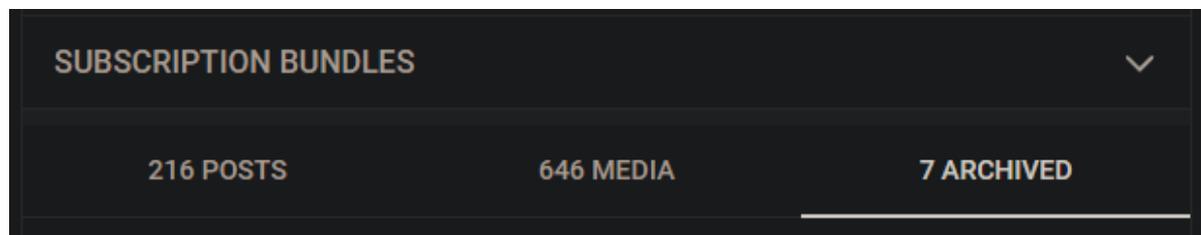
For videos, make sure you click on the small gear icon on the bottom right of any video and select **"Original"**. This will ensure that the videos you download are indeed the original quality.

A correctly downloaded video will have a similar filenames as the following examples.

```
0ifr0hizf5p9fraffs2ka_source.mp4
0gdp0fgxd5n9dpyddq2iy_source.mp4
5p545o597m5m90k357k5n_source.mp4
5f545e597c5c90a357a5d_source.mp4
```

Side note, when collecting images and video posts using this method. Be sure to check if the user has anything under the **"Archived"** section of their account shown in the screenshot below.

As images and videos listed here are not included under the general **"Posts"** or **"Media"** sections. Although, not all creator accounts have this section.



An example of where to find the "Archived" section on a content creator's OF page.

Locating "Leaked" Content

This is quite trivial, as OnlyFans content is very often leaked online and shared for free, because again, the internet does not give a damn about copyright. If you came here hoping I will show you where to find leaked content of the e-girl of your dreams. Then you are out of luck anon, it's time to put your dick back in your pants.

I am not going to actually provide you with links or anything like that here. However, you *could* always just do a little bit of OSINT and figure it out for yourself.

Although, sometimes it is worth checking online to see if a user's content has been leaked.

Story Time:

One such job I worked on involved a professional porn star who had some most of her custom OnlyFans pay-per-view (PPV) videos leaked online.

I was hired to locate every copy of these videos I could find online, document the URLs, domains, WHOIS records for those domains as well as any other data and/or metadata I could find in an attempt to press charges against the alleged "leakers". None of whom were ever sued or formally charged with anything, which is how 99% of these cases turn out.

During the first ~30 minutes of my initial investigation, I was able to locate the leaked content hosted on over 25 different domains just by querying a few search engines. Within about 6 hours, I would hand over my final report to my clients lawyers, who then served a few hundred DMCA take-down notices to those hosting providers and the content was taken down!

Great, another happy client! At least for a few days that is.. Until the videos were then re-uploaded again and again, every day.

My client and her lawyers eventually gave up trying to remove that content from the internet. It is still there to this day.

Content creators and copyright laws, at least from my opinion, cannot and will not ever win that battle.

This is why it is important to always be very clear and up-front about the nature of the internet from the very beginning of any online investigation that involves copyrighted material. You can DMCA things all day long, and most times hosting providers will comply. Assuming the hosting provider is located in a country that actually has, and actually cares about copyright law, such as the United States and *sometimes* Canada.

Although at the end of the day, the material will just be re-uploaded, saved and shared again a few thousand times overnight. This statement proved itself to be fact.

"Once it's on the internet, it's on the internet forever".

Leaked OnlyFans content is regularly posted everywhere online in places like Reddit, Twitter, Telegram channels, image boards, forums, etc. There are also hundreds of different websites out there that are entirely dedicated to hosting leaked OnlyFans content for free.

Be aware though, much like everything else that costs money, offering it for free makes this area wide open for scammers, malware distributors, traffic hoarders, ad-bombers, and honeypots alike.

Do not fall for any of these, and if you do. Then sorry mate, but you are a moron..

You have a brain, so please just try using at least *half* of it!

I have had luck many times by simply running a few simple searches on Google. Here are some basic examples.

```
"<OnlyFans username>" AND "leak"  
"<OnlyFans username>" intext:mega.nz  
"<OnlyFans username>" telegram  
intext:anonfiles.com AND "onlyfans"  
site:reddit.com AND "onlyfans" AND "<OnlyFans username>" AND "leaked"
```

It is worth noting that obviously not all creator content has been leaked online. The most commonly leaked creators are usually in the top 5% on OnlyFans. Still worth checking though.

Also, it's worth noting that if there has been any DMCA take-downs for creator content, always check the [LuminDatabase](#), this sometimes (Albeit, *rarely*) can include the content creators personal information.

Conclusion

Whether you are an actual investigator or just an average pervert looking for a way to download free nudes, I hope this article proves useful to you in some way.

Personally, OnlyFans has been involved in a few cases that I have worked on in the past, and I have not seen really any articles out there that involve OSINT techniques for OnlyFans. This could quite possibly be one of the first ones ever, who knows.

Anyways, I hope you enjoyed the read!

Stick around, as I plan on posting a new article every week. That is, if everything goes according to plan and life doesn't get any crazier..

Until next time friends,
-ohshint.

 28,792 characters in 4,415 words.