**Tactics for Telegram OSINT**

**ARJUN SURESH**

CYBER SECURITY STUDENT

**TABLE OF CONTENTS**

1. Introduction …………………………………………………………………………………………….. 3
   1. What is Telegram? ……………………………………………………………………….. 4
   2. Entities in Telegram ……………………………………………………………………… 5
   3. Importance of Telegram OSINT …………………………………………………….. 9
2. Requirements
   1. Setting up a Telegram Account ……………………………………………………. 10
3. Methodology
   1. An Overview of the OSINT methods ……………………………………………… 11
   2. Manual methods ………………………………………………………………………….. 12
   3. Automated methods …………………………………………………………………….. 17
   4. Storing and Analysing information
4. Conclusion ………………………………………………………………………………………………... 29

1. References ………………………………………………………………………………………………… 30

**INTRODUCTION TO TELEGRAM**

In the Modern world, most of our life revolves around the internet. We are increasingly dependent on the Internet for most of our day-to-day activities. We use various services available on the internet for carrying out our actions and duties. Most of us share various personal information to some services and also look up others information. Since people have started using the internet and the services available on it more and more, the value of a piece of data has exponentially increased. Like Gold and other metals were precious to our ancestors during their era, information, a.k.a. data, has become the new valuable entity.

Today, large MNCs would pay anything for obtaining data that they require. But, we, as regular users of the internet, can also access these data which is publicly available to us. This publicly available data which is freely accessible to everyone is known as Open Source Intelligence or OSINT for short. Even though OSINT is considered to be a part of Cyber Security and Hacking, we use it daily in our lives. Whenever we are searching for any piece of information on the internet, we are actually performing OSINT.

This research paper aims to outline some methods and tactics available to carry out efficient OSINT operations in a specific platform called Telegram, which is widely popular today.

**WHAT IS TELEGRAM?**

There are various sources of OSINT available to us, such as search engines, social media platforms, blogs etc. to name a few. One of the active sources from where we can gather some information today is from an Instant Messaging platform known as Telegram. Telegram is a cloud based instant messaging platform available on both mobile phones and desktops. One of the main reasons why people choose Telegram over other similar platforms is due to the security that it provides. Telegram also provides means to automate various tasks using the so-called bots. People use telegram for various activities like messaging, joining groups and channels, sharing content and for business activities. But due to the anonymity and secrecy provided by Telegram, it has become a thriving spot for various cyber criminals who carry out various illegal activities via Telegram.

Some of the core features of Telegram which prompted cyber criminals to use it include:

* End-to-End Encryption (E2EE)
* Self-destruct secret chats
* Hiding online available statuses
* Account self-destruct

In the recent years, various illegal criminal operations are being run through Telegram. Using Telegram makes it difficult for the responsible authorities to track down the responsible individuals who are running the operations. Apart from cyber criminals, normal people use Telegram for sending messages and also for downloading/uploading content such as Audio/video files, text files, apps etc.

Telegram supports large-sized files up to 2GB. This makes it convenient to share movies and other huge files via the app. Due to this reason, various piracy activities are also being run on Telegram. Another important aspect of Telegram which makes it a safe haven for cyber criminals is the feature to hide the mobile number associated with an account even from group admins. This provides a very high level of secrecy and anonymity to the offender.

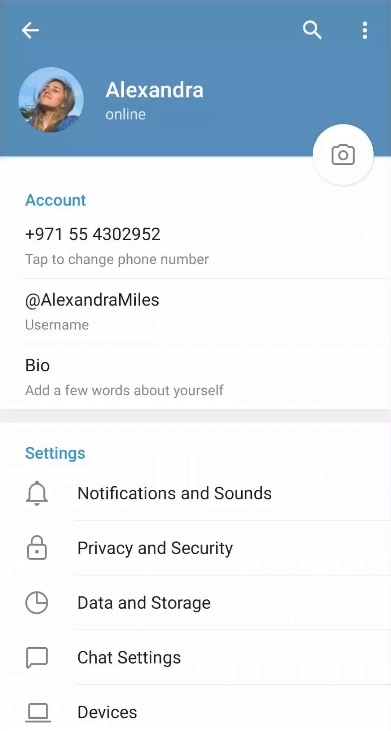
**ENTITIES IN TELEGRAM**

Like any other instant messaging platforms, telegram supports a variety of entities. Of course, the most common among them would the actual users itself. But in addition to normal individual user accounts, Telegram supports other entities which are listed below:

* User
* Group
* Channel
* Bots

Let’s look at each of these various entities in detail and discuss how they differ from each other.

**User:** A user account is normal individual account that anyone can set up to start using Telegram. This is similar to a WhatsApp account. Telegram accounts are based on phone numbers and not any other identifiable entities. You need to have a phone number to register with your Telegram account and once registered, Telegram will send a verification code to the provided mobile number to verify that it actually belongs to you. User accounts can also have a username associated with them, but is not necessary. You would need to provide some kind of name though. You could also add a profile picture and a short description of the account. These extra features are not mandatory. Users can join groups and channels after creating an account.

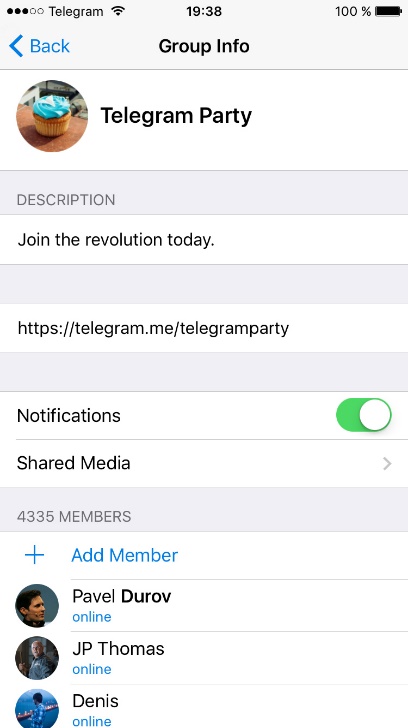


**Group:** Groups basically mean a collection of users. Again, this is similar to the concept of groups on other platforms. Usernames are optional for a group. Having a username makes the group publicly accessible and searchable. In addition to the features mentioned in the Users section, groups can include a title which shortly describes the purpose of the group. Groups could also display the number of members that the group currently has. In Telegram, there are 2 different types of groups:

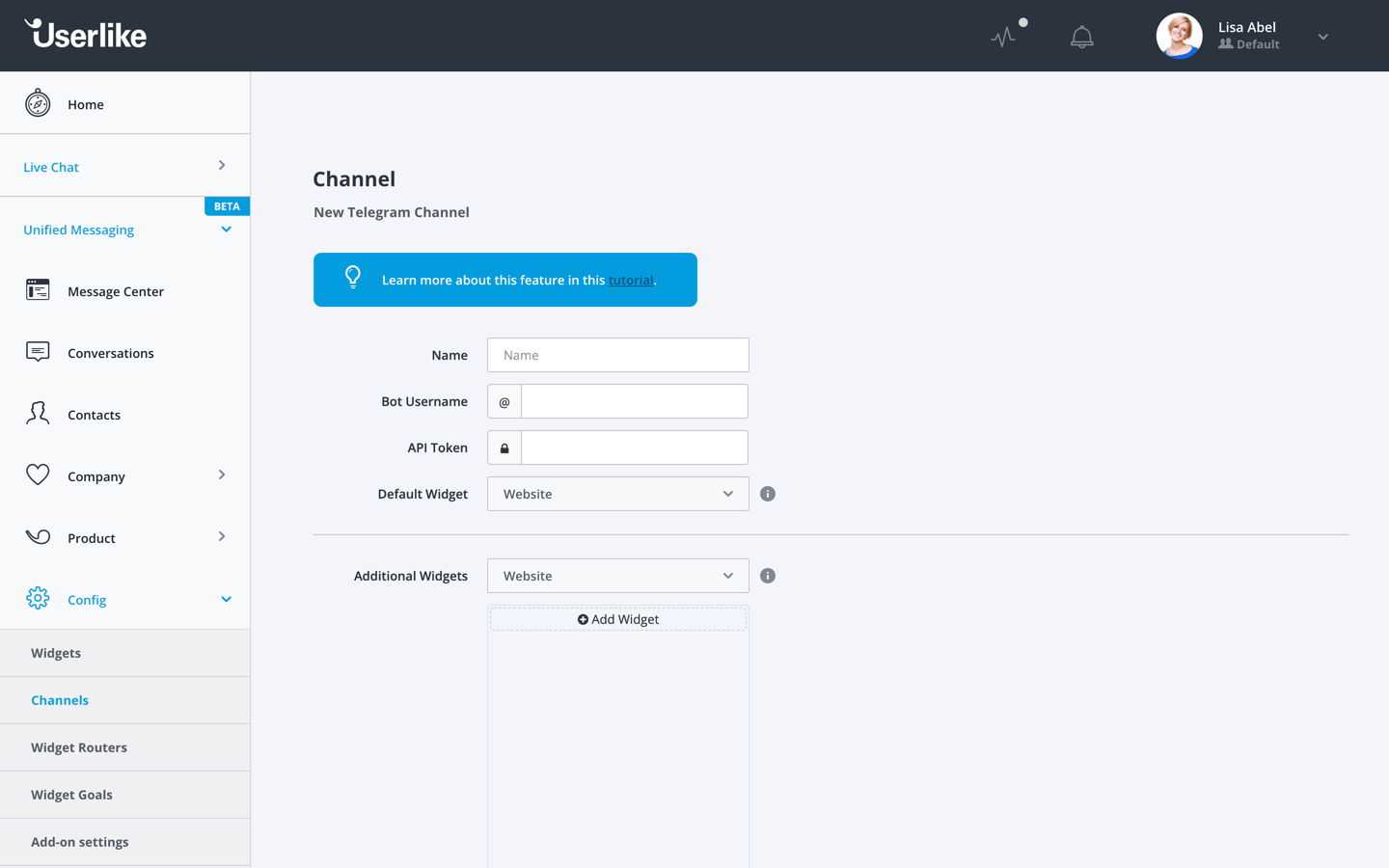
* A Normal(basic) Group and,
* A Super Group

A basic group can have up to 200 members. These can include both normal users and bots. A normal or basic group would always be private and would not be publicly accessible by anyone else. Members are added to the group by the administrators or by sending out invite links to join the groups.

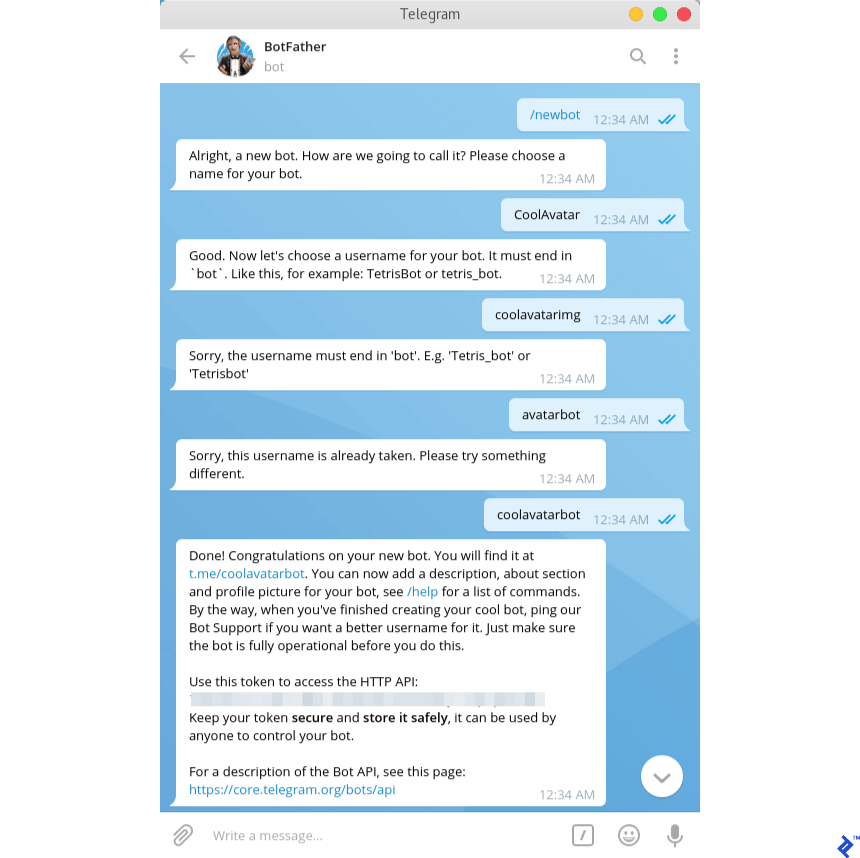
A super group can have up to 200,000 members (previously 100,000). A super group can either be private or public. By default, the group would be private but can be changed to public by the administrators. For making the group public, you would have to provide a username to the group so that external parties can join the group by searching for the username.



**Channel:** Channels are a different concept that we only see in Telegram. Channels also contain administrators and channel members, similar to a group. But it differs in that, in a channel, only the channel administrators can send messages or content and view the people subscribed to the channel. Most of the Telegram users would be familiar with the concept of a channel. Like Super groups, channels can be either private or public. Private channels only allow access to it by means of an invite link.



**Bots:** Bots enable a whole lot of automation to be carried out in Telegram. Bots must have a username. It does not require a phone number and has restricted freedom compared to a normal Telegram account. They carry out specific actions which have been previously configured by the people employing the bots. This is done via some bot APIs. Bots also cannot join groups or channels by themselves. Administrators have to add these bots to their channels or groups.



Using these 4 entities, we can gather a whole lot of information from Telegram. Knowing the basics of these entities and how they operate within Telegram can enable us to understand how to look for specific pieces of information and from where to obtain them.

**IMPORTANCE OF TELEGRAM OSINT**

Telegram can provide a whole lot of information about users, groups or channels. As stated, and explained earlier, Telegram has recently become a hotspot for cyber criminals to carry out their illegal operations. There are lots of information that we can gather about them and their activities, some of which are listed below:

* Propaganda
* Training
* Networking
* Illicit trade
* Cyber crime
* Fraud
* Piracy

The types of information that we can gather is not limited to the above-mentioned ones. It all depends on our ability to understand what to look for and how to look for them.

Examples of information that we can gather from Telegram include:

* Users/Username enumeration
* Chat history and messages
* Information on channels and members
* ‘Information on groups and members
* Finding groups and channels providing a particular service or performing some functions
* And so much more …

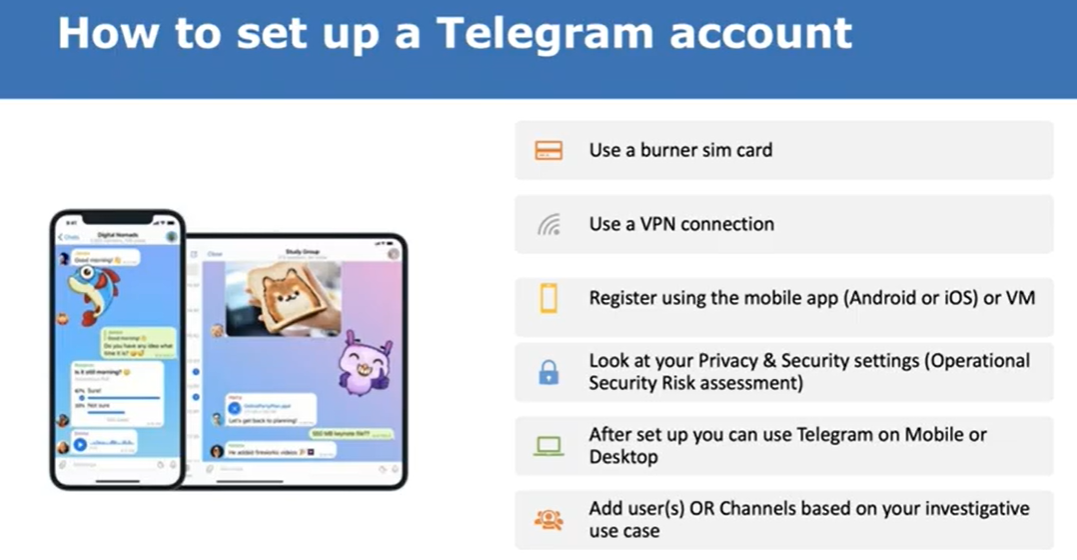
**REQUIREMENTS FOR LEVERAGING TELEGRAM FOR OSINT**

The only thing that we need to gather information from Telegram and perform OSINT using it is a Telegram account. It is really easy to set up a Telegram account. But using a personal account would be dangerous and ineffective in doing these OSINT activities. It is advised to use a burner sim card while registering an account and use a VPN when accessing it. Additionally, you could change the security and privacy settings on the account after creating it.

After creating an account, you can try to get into some groups and channels for gathering the info that you are looking for. It is not advised to directly interact with the people in these groups for collecting information. Rather, a more “passive” method would be effective in this case.

In this Research paper, we would be coming across some tools and websites which help us to gather information from Telegram. So, some level of browsing experience would be recommended. We would also employ some tools created using some programming/scripting languages. Knowing the basics of using and running such tools is also appreciated. A basic understanding of the Linux Operating System would also enable you to efficiently run such tools and maybe create your own ones.

Since Telegram can provide us a wide variety of information, it is also important to acquire the knowledge to understand what exactly are we looking for. Knowing how to make use of the data collected is also an important requirement.



**TELEGRAM OSINT**

Searching for information in Telegram primarily involves simply knowing what to search for and then using Telegram’s own search option. There are some external sites available to gather information on groups and channels and also to gather information about text messages. We can search for users, groups, bots or channels using the Telegram search bar which is available in both the Telegram and mobile apps. If we know the username to search for, we can search for people from outside our contact list. Also, knowing the phone numbers of the people that we are looking for can enable us to search for them, if they have linked their phone numbers to their Telegram accounts.

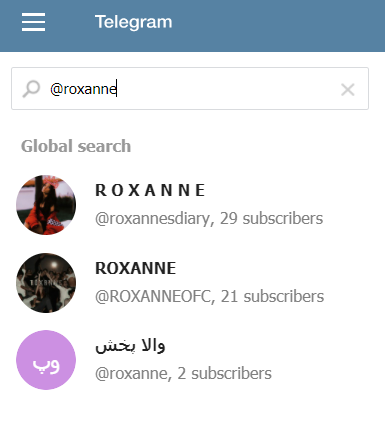
One important thing to note here is that in Telegram, usernames are unique while Names of people are not. There are manual and automatic ways to search for people or groups in Telegram. Manual probing involves directly searching for people with the help of their usernames, names or phone numbers, using the Telegram search bar. We could also gather more information by going through each group or channel one-by-one. In automatic ways, we could employ the help of some third-party websites or tools to gather information from Telegram.

We could also use invite links to gather some information about the groups or channels to whom the link belongs to. After gathering and storing all the data that we collect from Telegram, we could export them using some tools for later analysis.

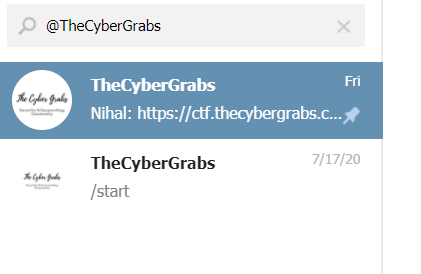
**TELEGRAM OSINT- MANUAL METHODS**

In manual methods, we do not require the use of any tools or other external sources to gather information from Telegram. We could use the Telegram search bar to find specific accounts, groups, or channels.

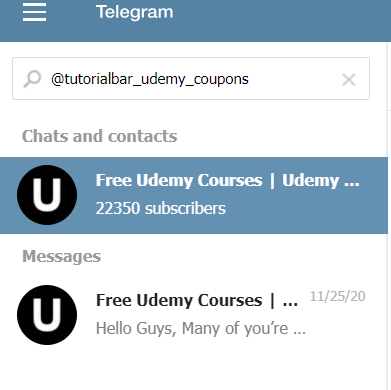
Using the search bar, simply type in the username of the account that we want to search for. Since usernames are unique, we shouldn’t get any duplicate results.



Searching for groups via usernames:



Searching for channels via username:

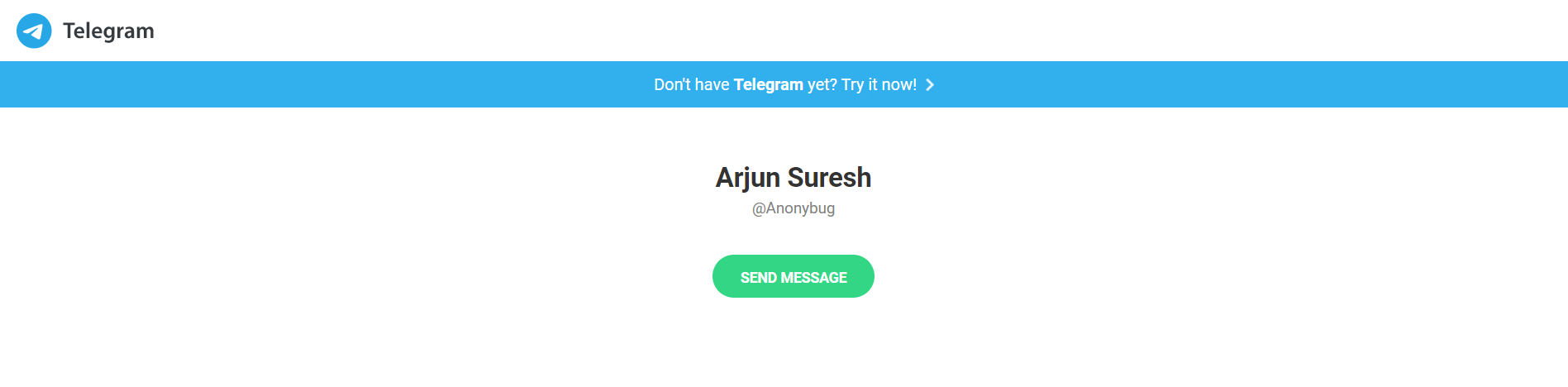


We could also use Google to gather information from Telegram. For example, to search for the existence of a username in Telegram, we could type in the following google query:

[*https://t.me/<username*](https://t.me/%3cusername)*>*

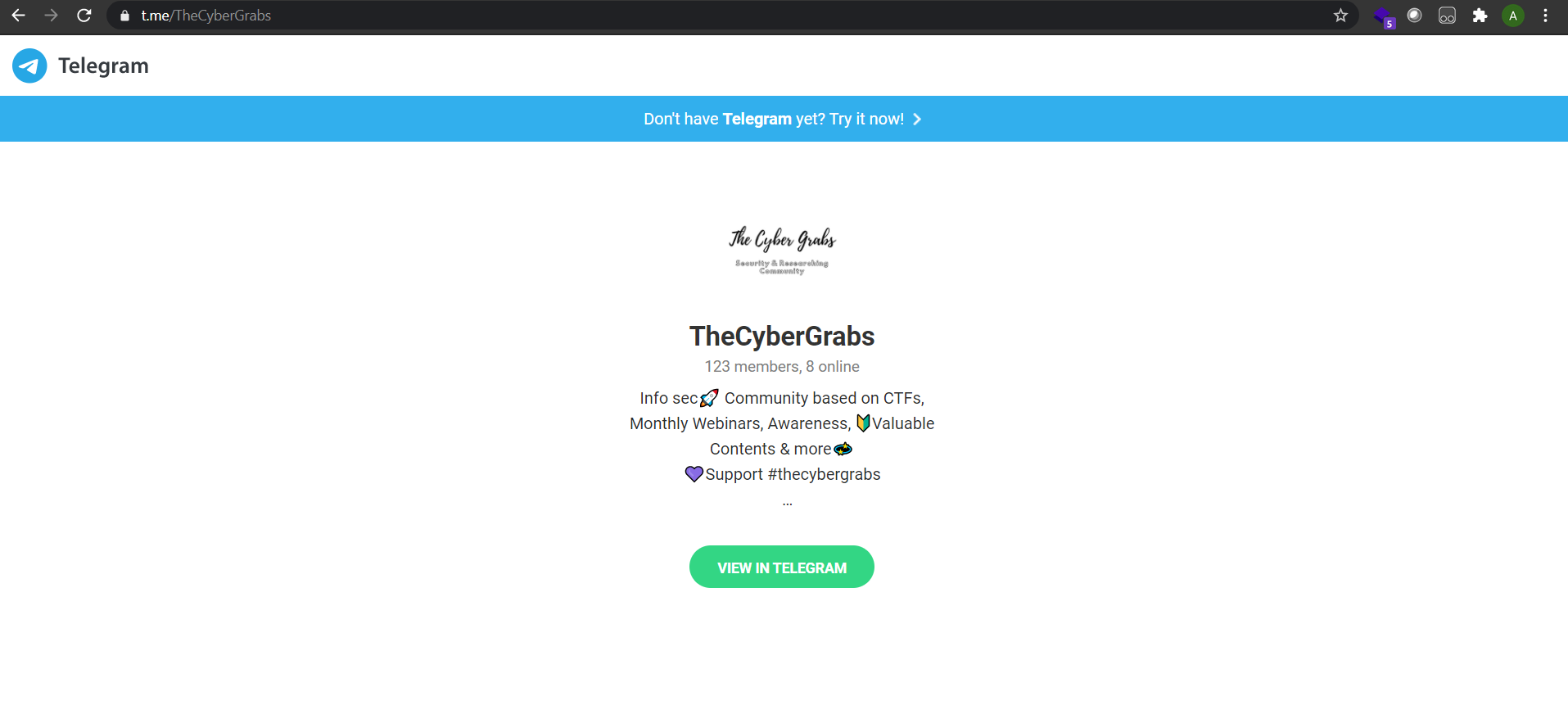


where <username> is the value we are searching for. If such an account exists, we get the following output:



We could also use the following query to search for groups and channels.

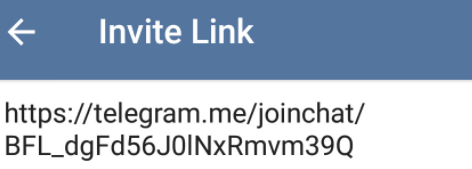
Eg:



We could also use the invite links for groups and channels to gather more information from them. Since we are doing this manually, we are going to search via Google using these links. But before getting into the information gathering part, we need to understand the concept of invite links in Telegram. Invite links in Telegram are of the following format:

[*https://t.me/joinchat/<hash*](https://t.me/joinchat/%3chash) *value>*

An example of an invite link is shown below:



The hash value at the end of the URL is specific and unique to each invite link generated.

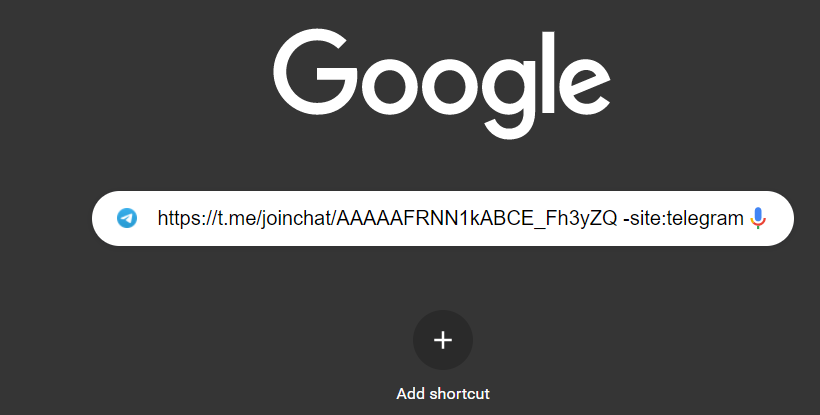
By simple searching google with the above-mentioned URL, we can know from where the link was shared and who shared it.

An example query is shown below:



By using Google dorks, we could further refine our search. By eliminating all URLs from Telegram.org, we could see where the links got shared and by whom.

An example is demonstrated below:



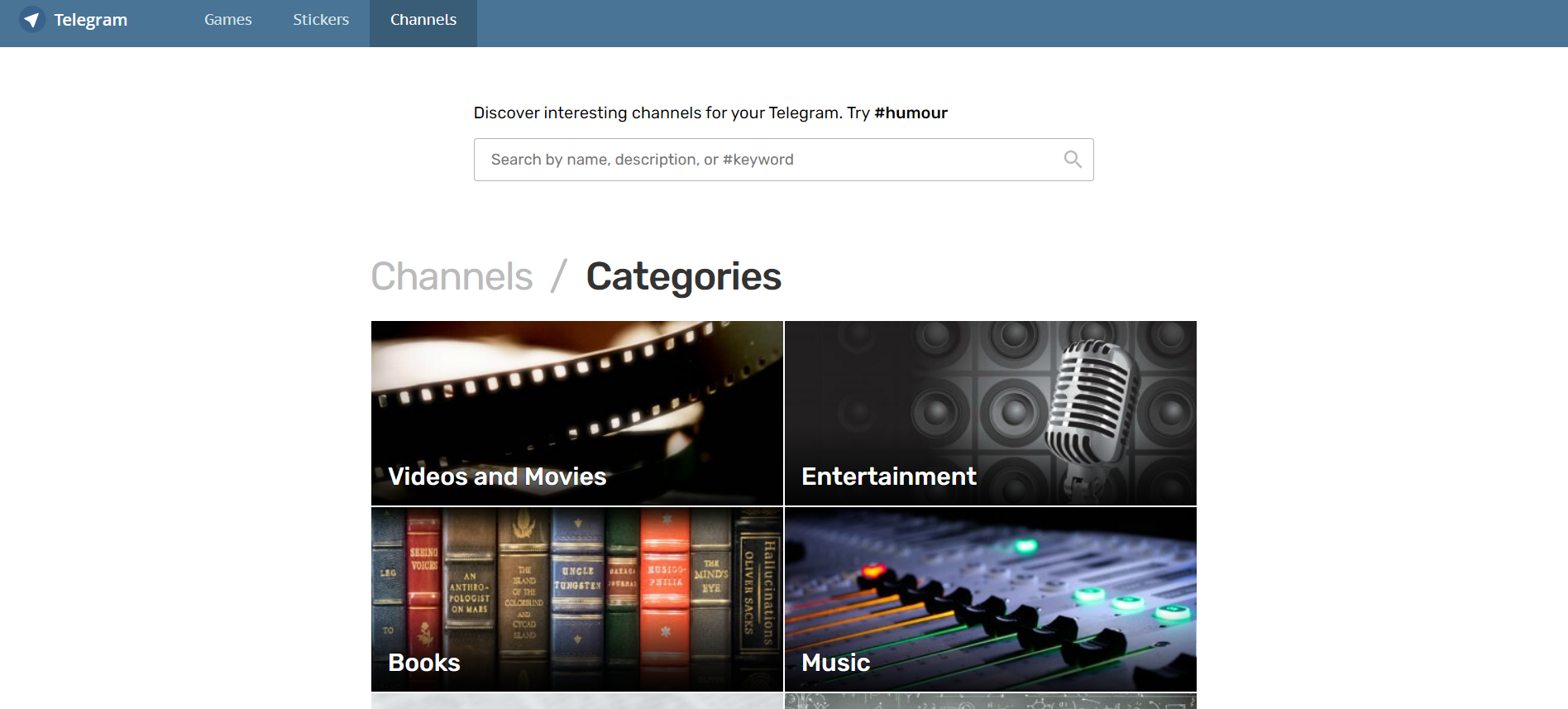
Using the above methods, we could gather plenty of information from free sources. The only caveat is that we should know what to search for and how to make use of the information collected from the above methods.

In the next section, we are going to look at some automated methods for collecting information from Telegram. These include using third-party websites and tools for automating our workflow.

**TELEGRAM OSINT- AUTOMATED METHODS**

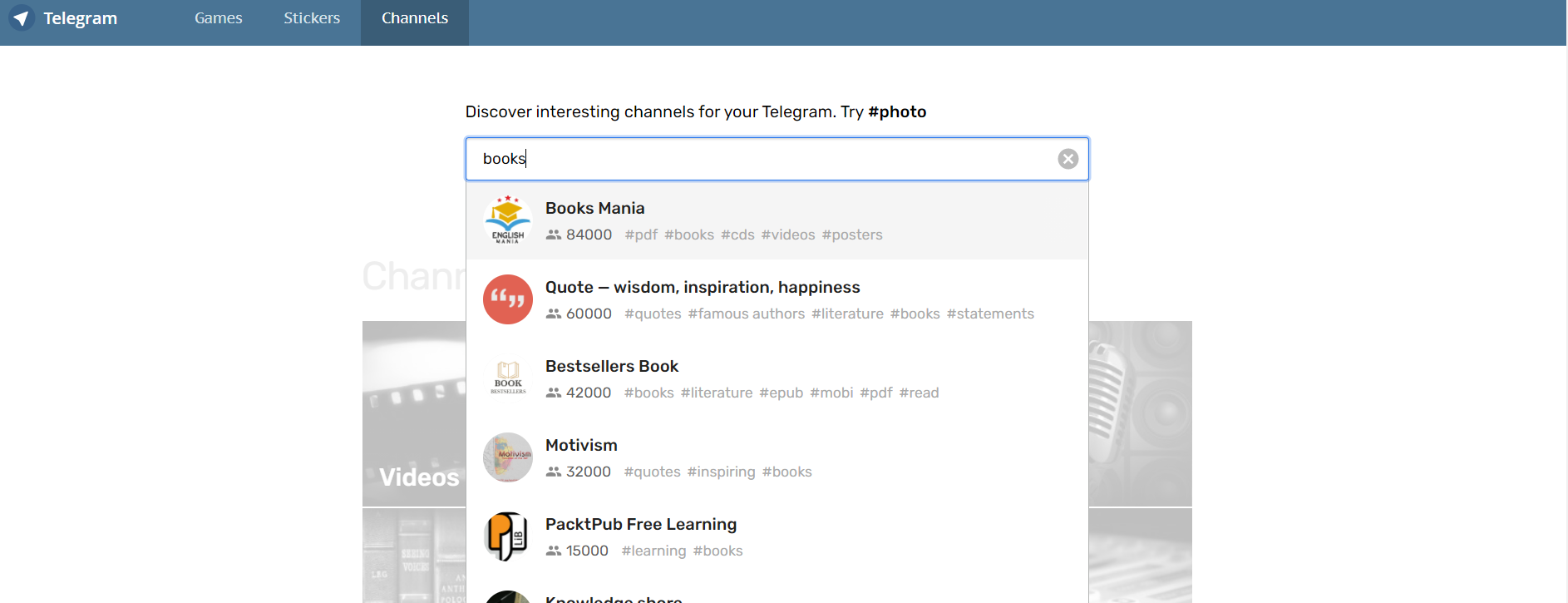
In automated information gathering from Telegram, we employ various third-party tools and services for gathering information from Telegram. We are going to take a look at some popular methods one-by-one.

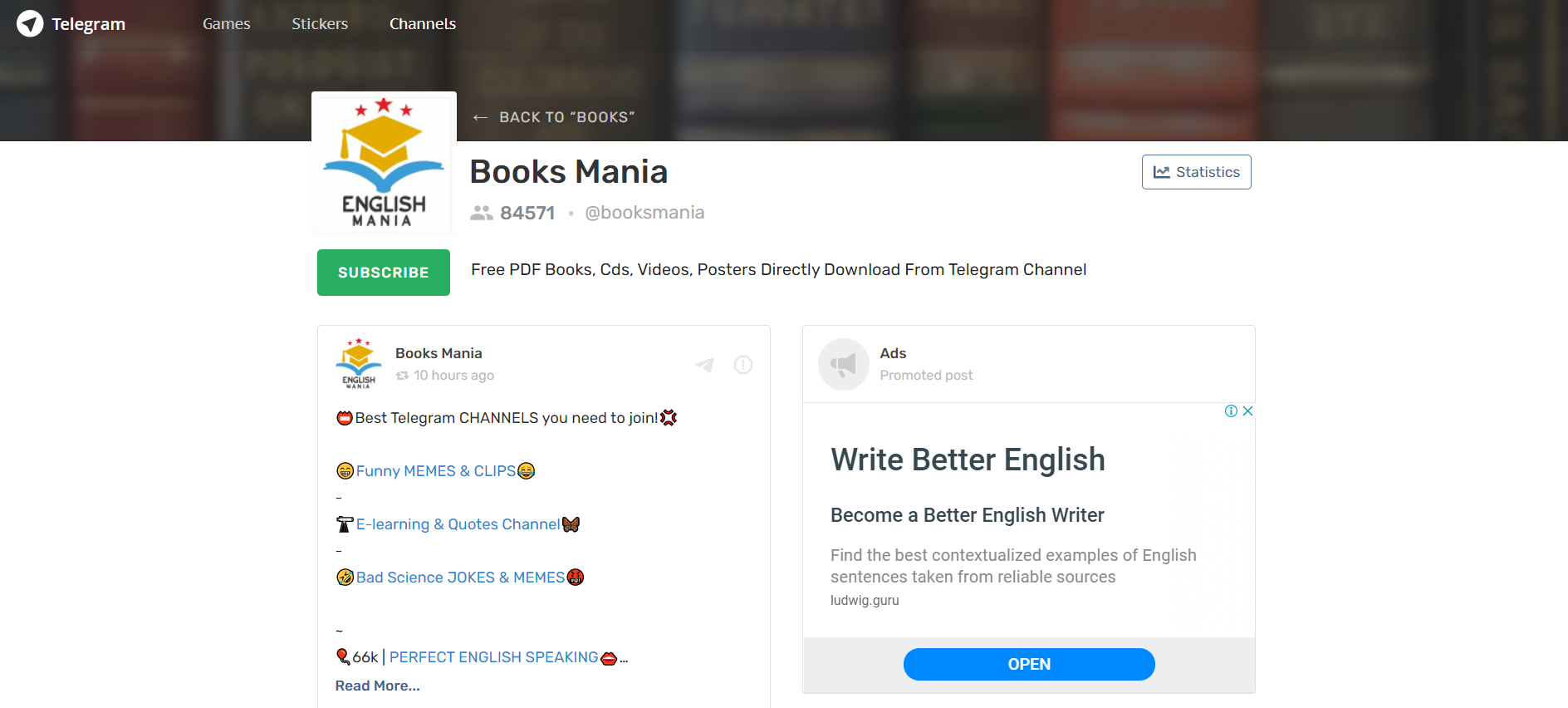
The first website that we are going to explore today is called [*https://tlgrm.eu/channels*](https://tlgrm.eu/channels)*.*



Using the search feature in this site, we can gather information about channels in Telegram. We could search using the channel name, or some part of the channel name, using the description of the channel or by searching for channels that have certain hashtags associated with them.

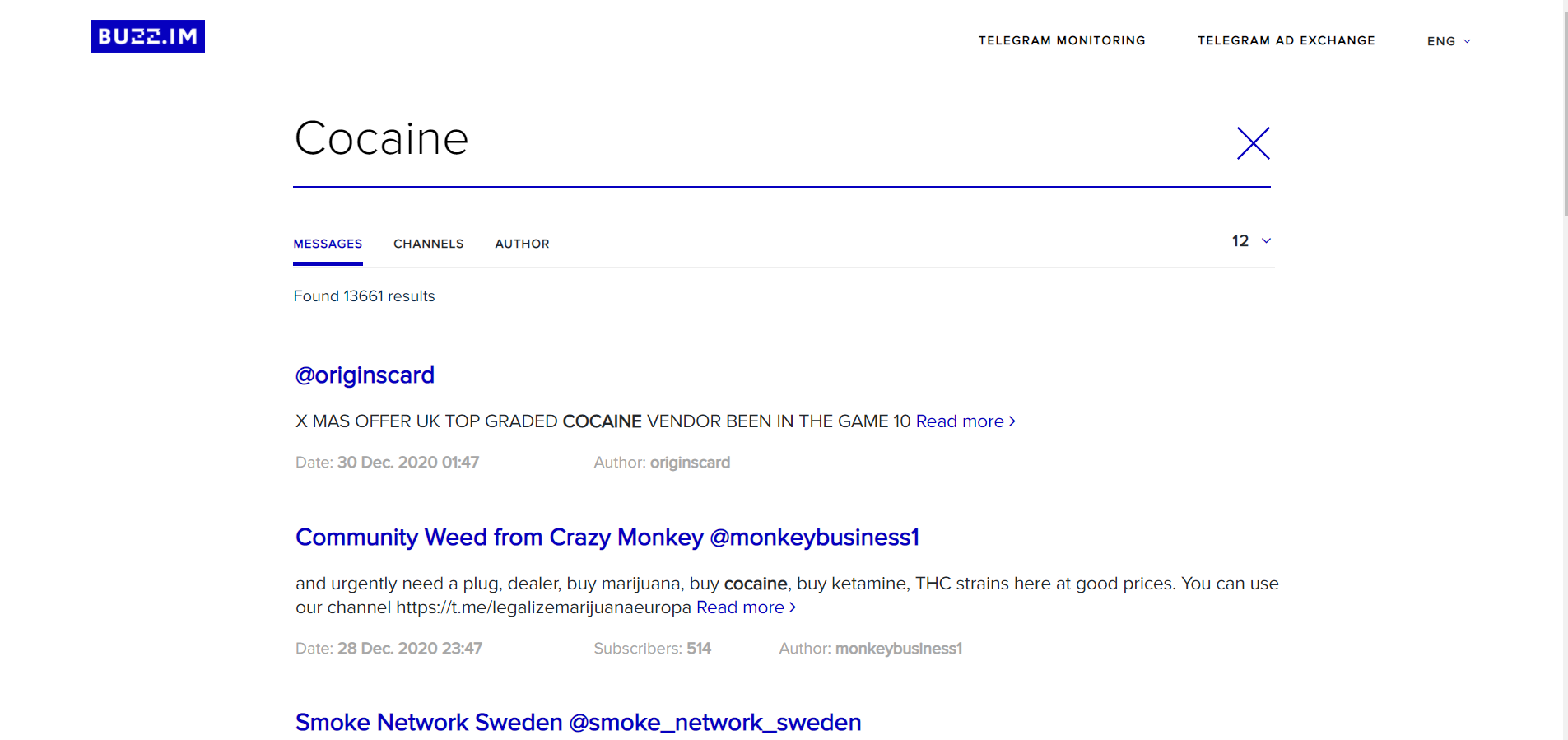
Some examples of using this site is demonstrated below:





The next website which provides useful information to us from Telegram is called [*https://search.buzz.im*](https://search.buzz.im). This site provides a rather peculiar way for gathering Telegram information. We can search through public messages in Telegram using this particular website. All we need to do is provide some keywords that we want to look for.

For example, if we want to search for messages on the topic “Cocaine”, we could simply type in the word “Cocaine” and search.buzz.im displays all the messages which includes this keyword.



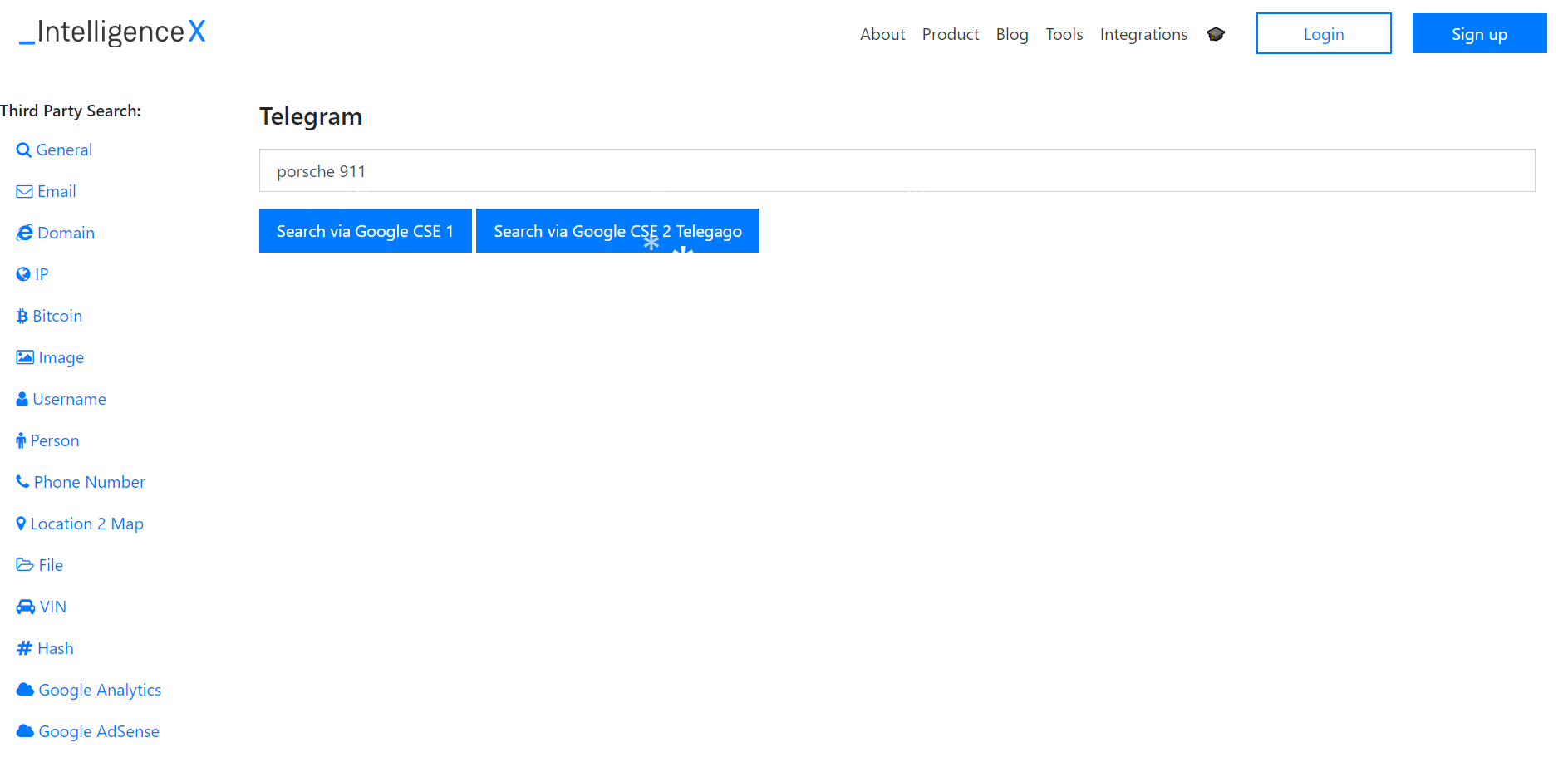
We could also see the usernames, if available, of the people who posted the messages.

One important thing to note is that this site only searches through the messages in public groups and channels, as it is not possible to read the messages in a private group/channel.

The results include a variety of information including:

* The actual message containing the keyword
* The author of the message
* Date the message was sent by the recipient
* In which group/channel the message was posted to
* And finally, if the message is a reply to another message from someone else, it also provides us with that information.

The next website is called [https://*intelx.io*](https://intelx.io)*.* This site is not specific to Telegram OSINT, but can be used for various OSINT activities in other platforms like Facebook, Twitter etc.

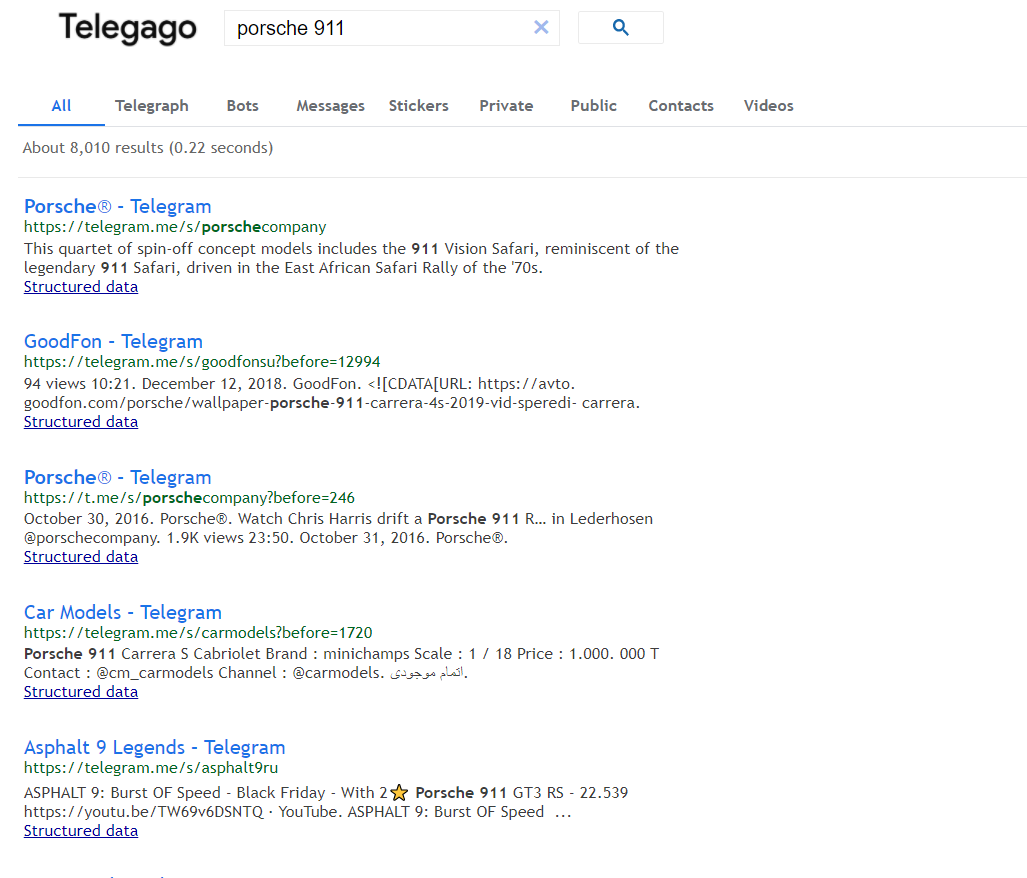


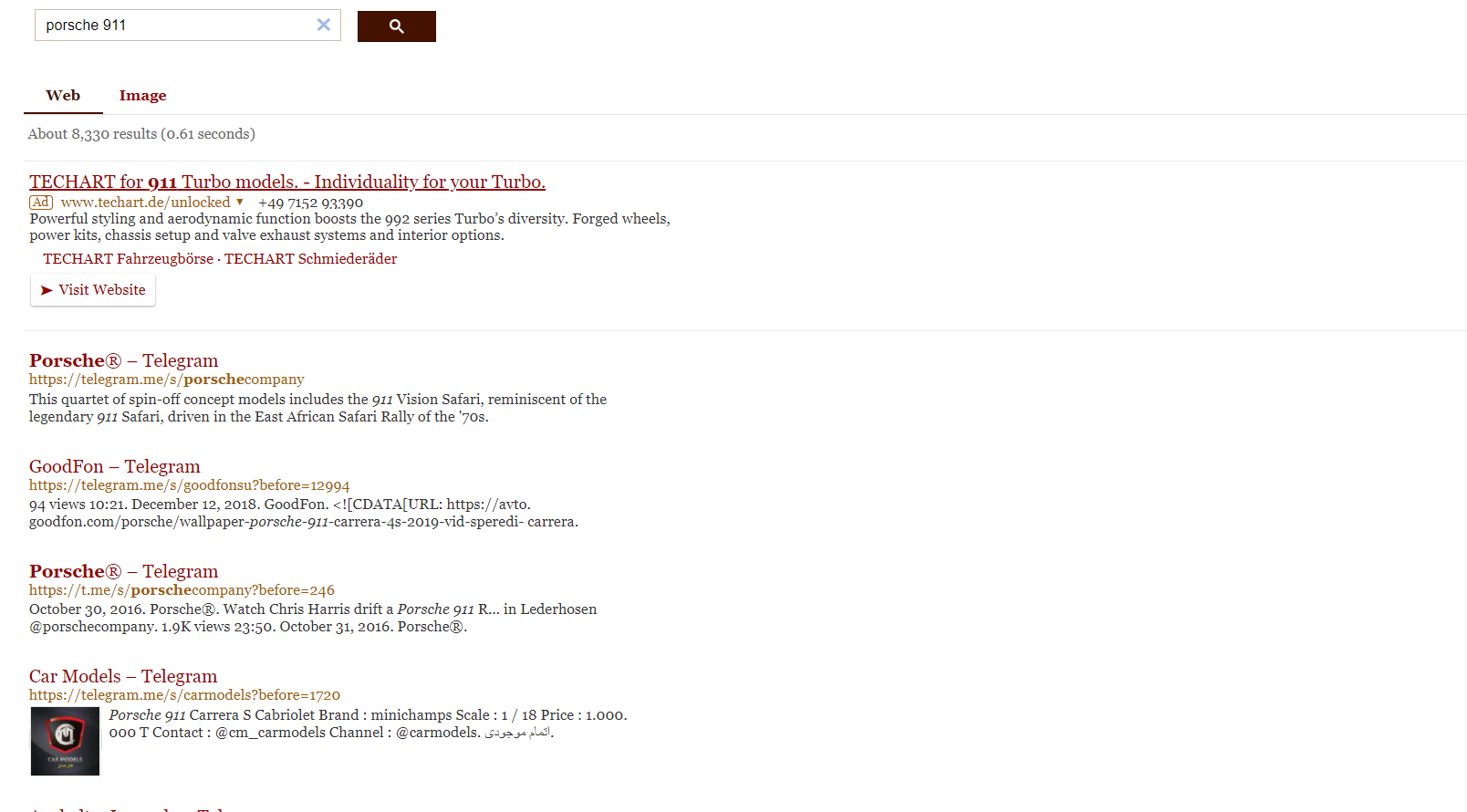
We can just specify a keyword and it searches for usernames, groups/channels containing that keyword. It uses two search engines for this purpose:

* Telegago
* cse google

Telegago is a specialized search engine for Telegram OSINT.

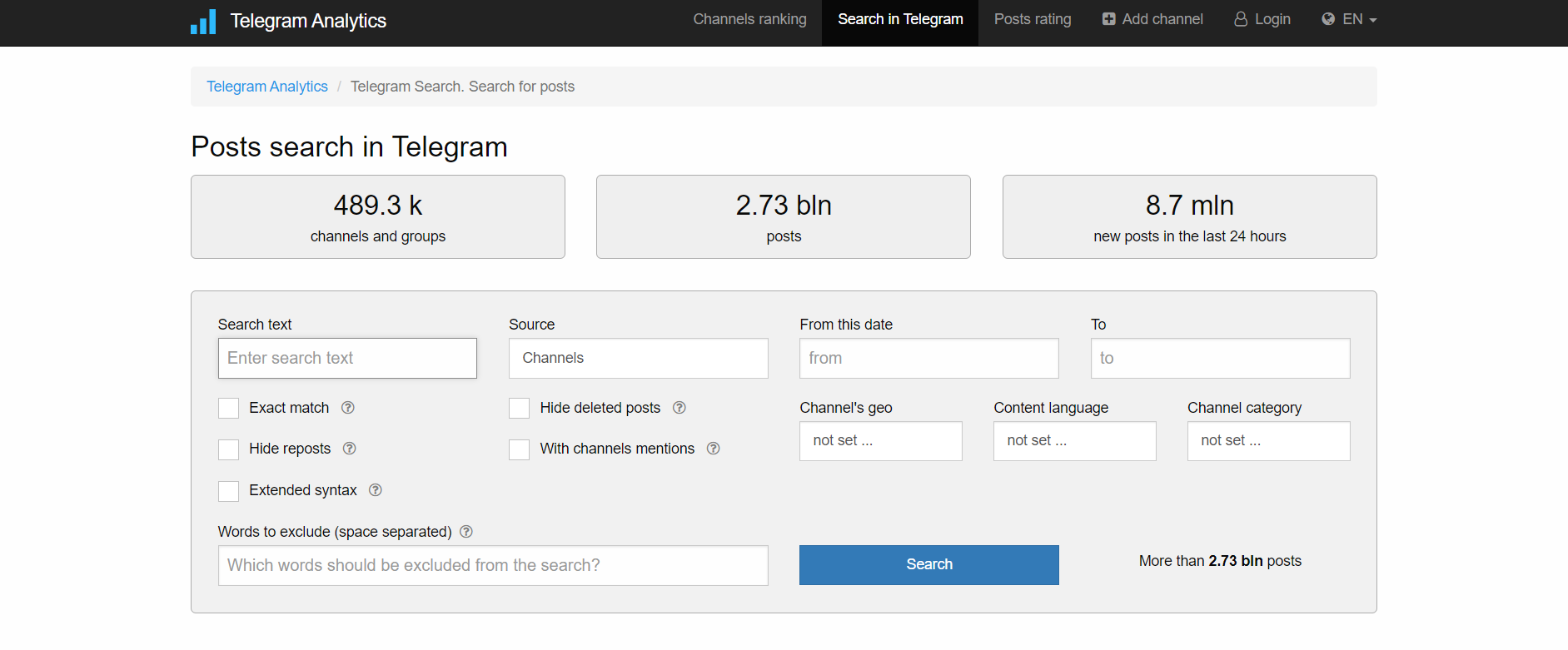
Searching for a keyword using both these search engines is demonstrated below:





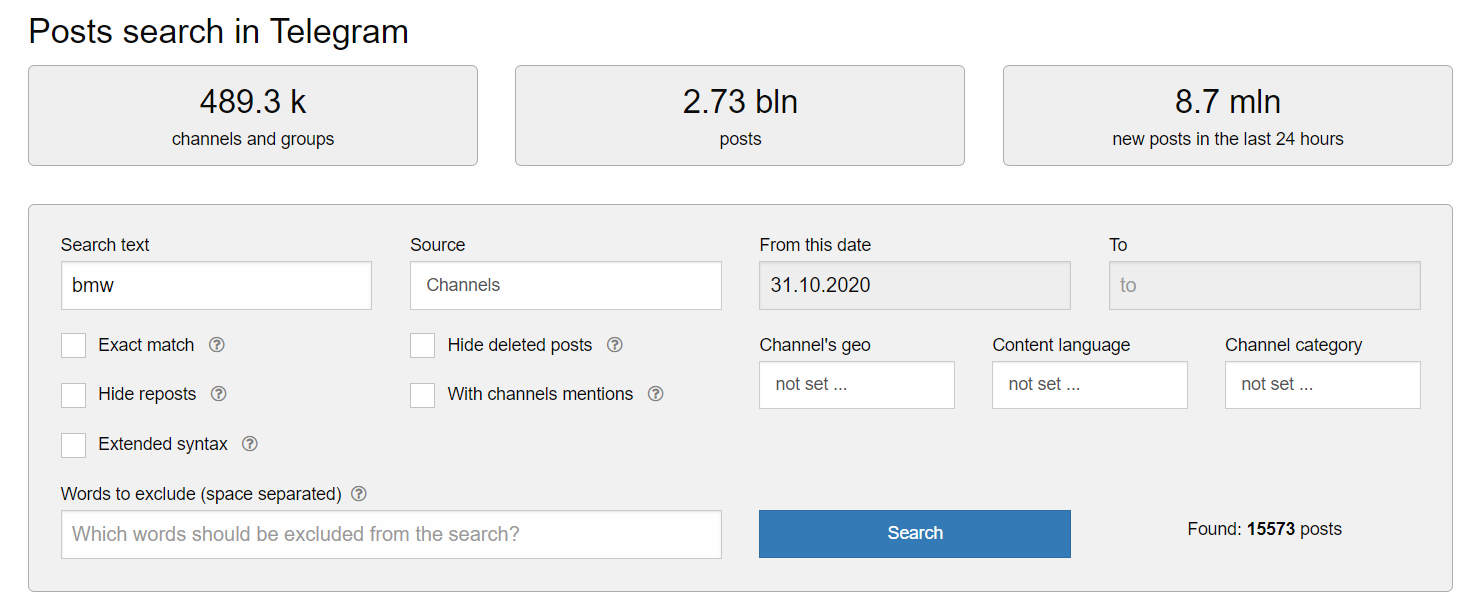
Another website which provides analytical data from Telegram is <https://tgstat.ru/en>.

This site provides information about various posts on Telegram, either posted by an individual or by a channel/group.

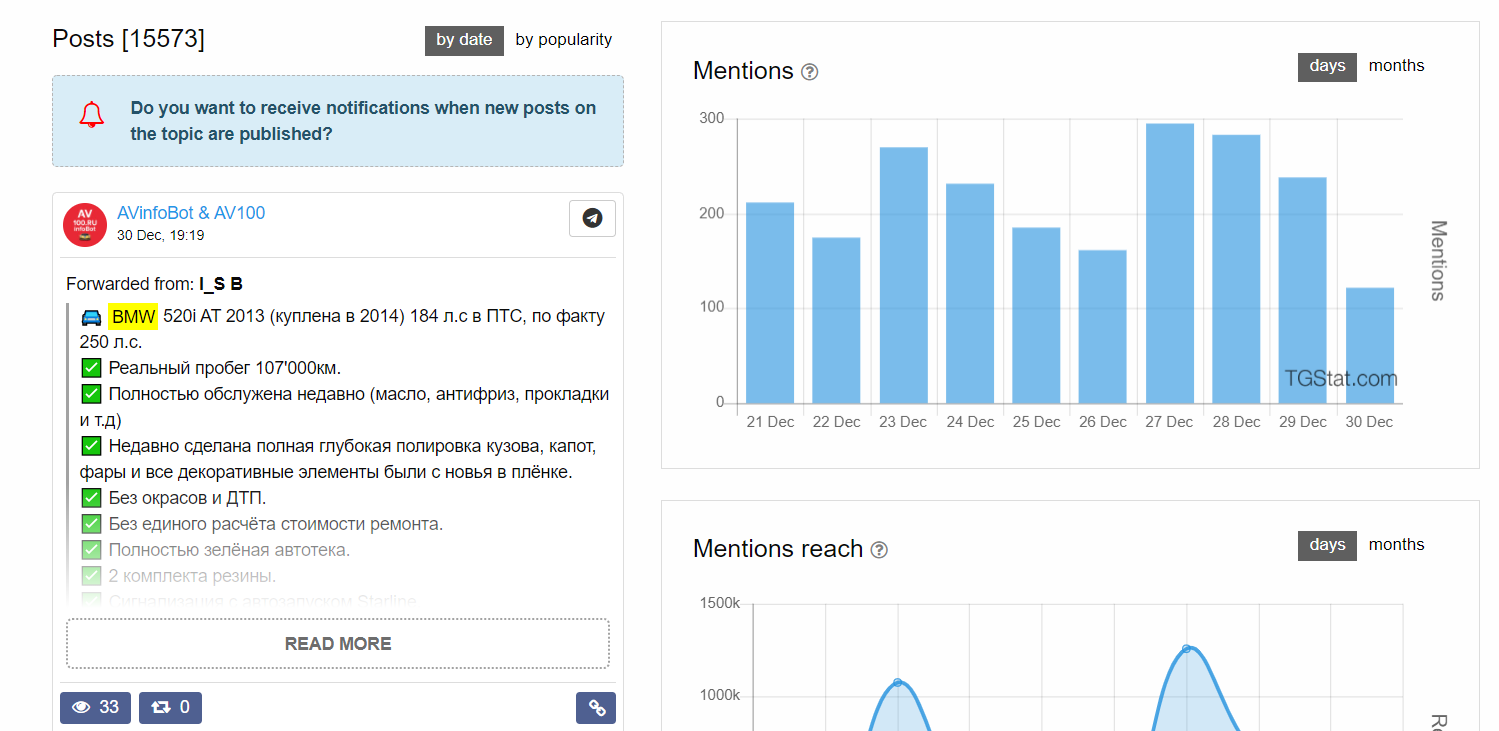


We can refine our search using various filters like the dates between which the post has been sent, the keywords to include, where to search for the keyword (channel/chats) etc. If the site finds a hit for the specified keyword, it returns the post/s containing the keyword and various the keyword along with other associated information about it.

An example of using the service is demonstrated below:



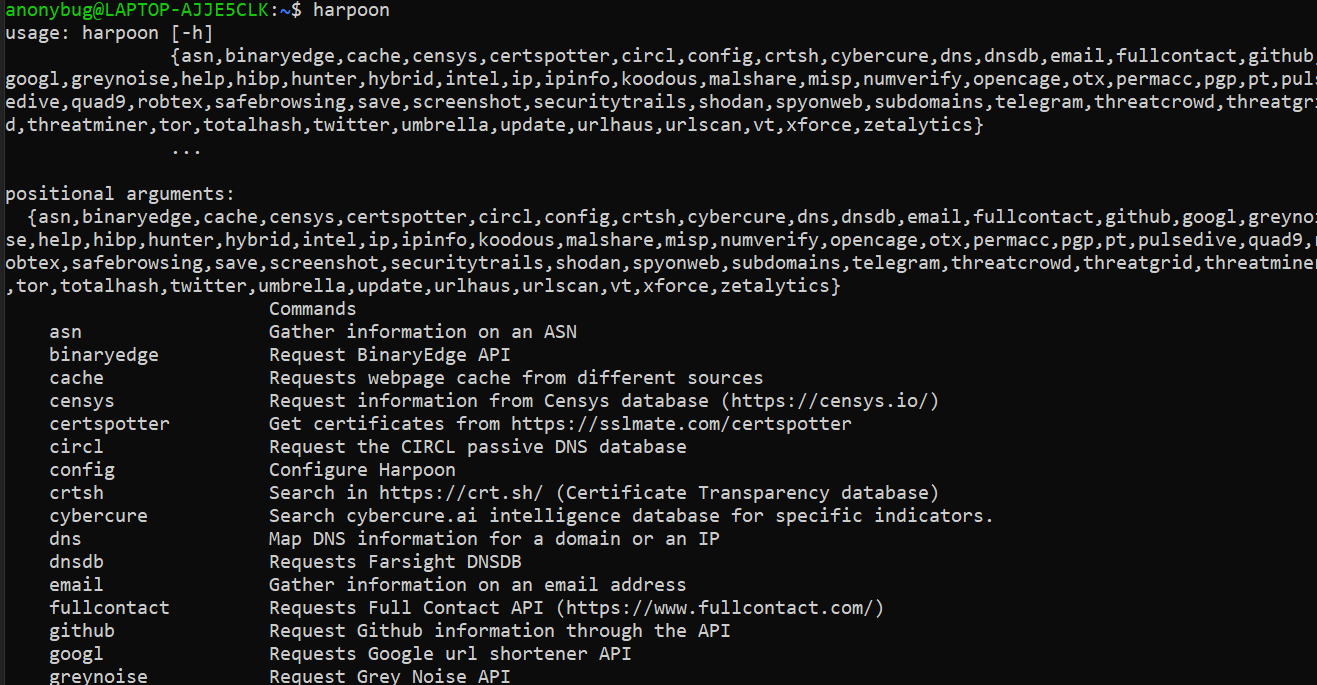
Output of the above query:



In the next section, we are going to explore a couple of tools which helps us in our OSINT activities using Telegram.

**TELEGRAM OSINT AUTOMATION USING TOOLS**

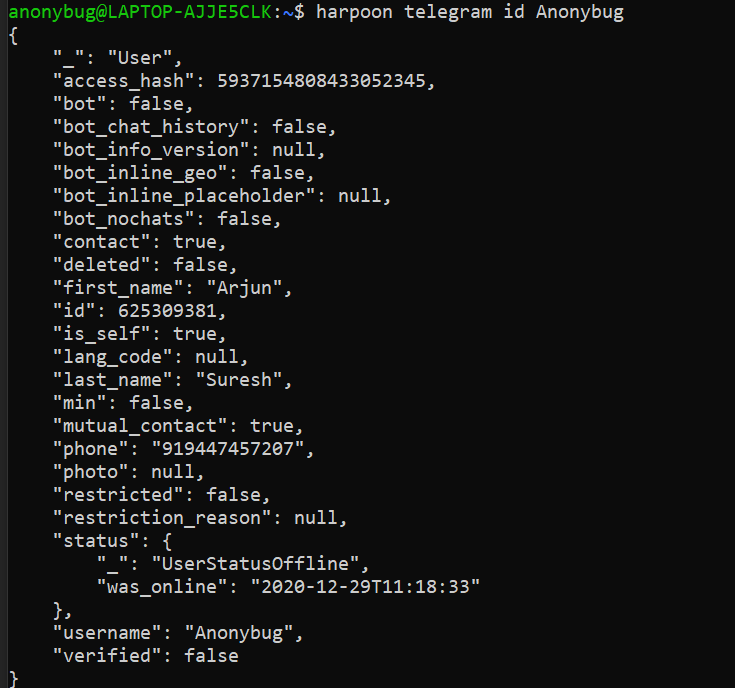
There are a few automated tools available for Telegram OSINT, but we would only be discussing one. The one we are going to discuss is called ***Harpoon.*** This is a very powerful tool which can help us gather plenty of information about other users and groups in Telegram. The tool is written in Python and it is easy to use.

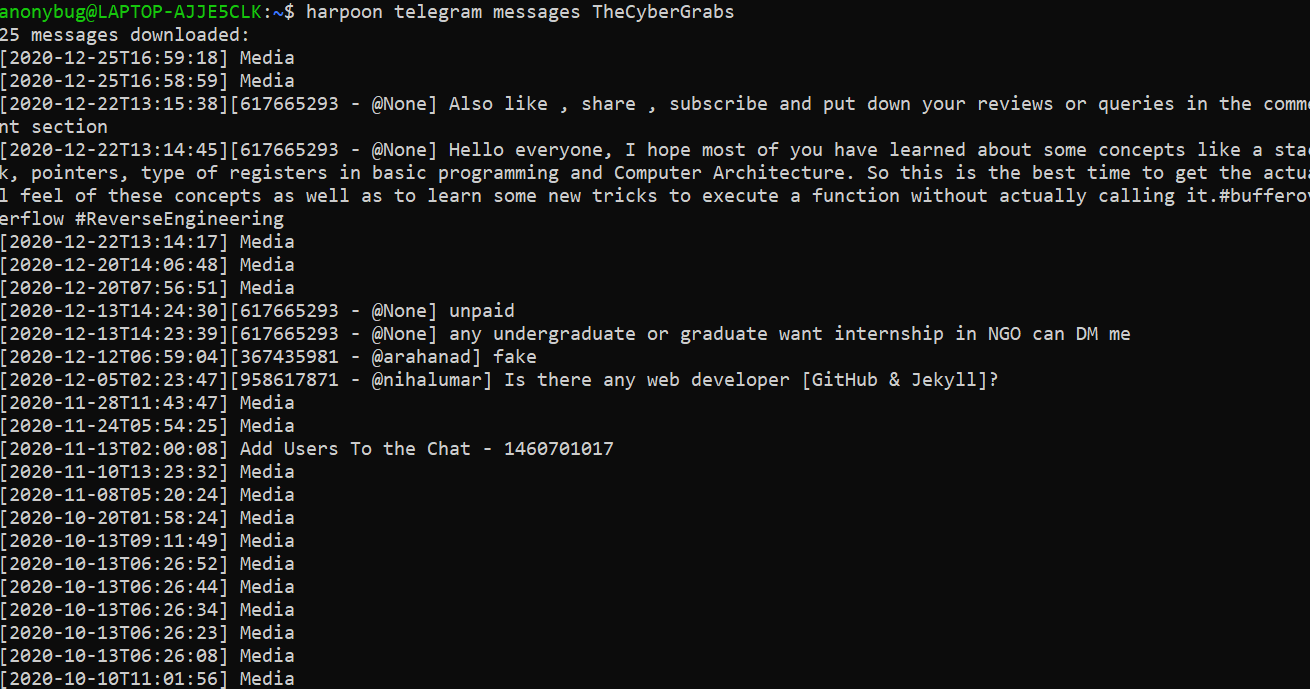


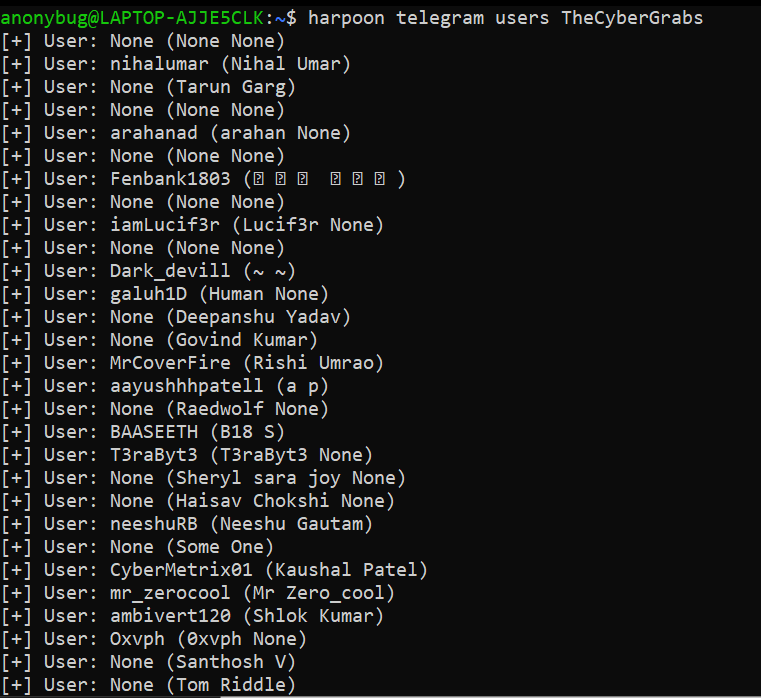
The initial configuration of the tool requires some time. We would need to share our app id, api hash and the phone number associated with our account to use this tool. We are not going in depth about the configurations since it is out of the scope of this paper.

But after initializing everything that the tool requires, we can gather information about an account just by providing a username. We can also gather users in a particular group, provided we have access to that group. We could also search through messages in a channel.

Some examples of using this tool are demonstrated below:







The information that we can gather about an account include account creation date, last accessed date, phone numbers linked to the account, if any, id of the account etc.

Apart from just Telegram OSINT, this tool can also pull information from a large variety of sources including Security Trails, Virus total etc.

The tool is freely available on GitHub and can easily be installed in a Linux/Windows/Mac OS environment, provided that python3 is installed on them.

**STORING AND ANALYZING INFORMATION**

There is an extension for scraping users and messages in a group/channel, which is available for Google Chrome and Mozilla browsers. It is called Greasemonkey in Mozilla Firefox and TamperMonkey in Google Chrome.

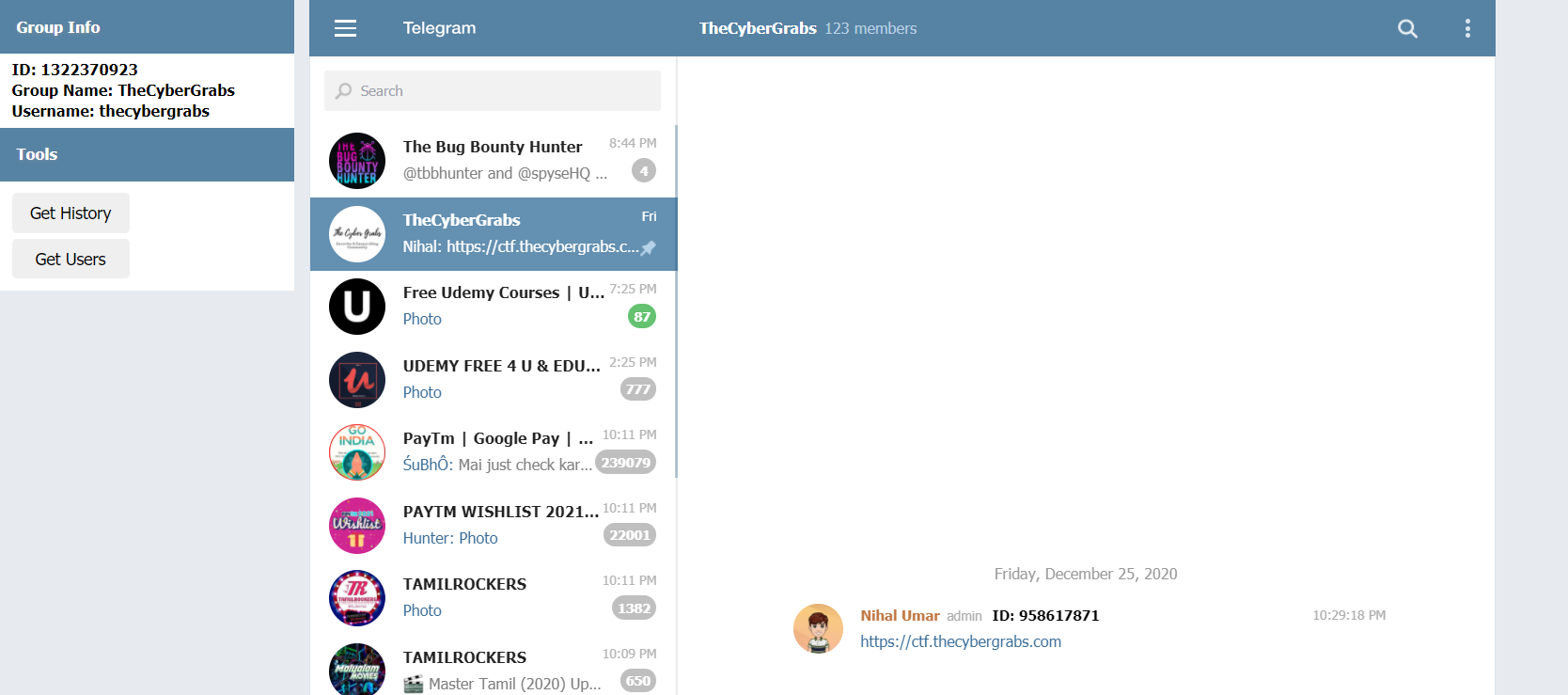
This extension can scrape the users in a group that we are in and export the results into a much more readable format like .csv. The extension requires a couple of scripts for doing this particular task. We can find these scripts at:

[https://gist.github.com/fabledowl/](https://gist.github.com/fabledowl/4d6f84b211a2918fb9ee9556550df5b0)

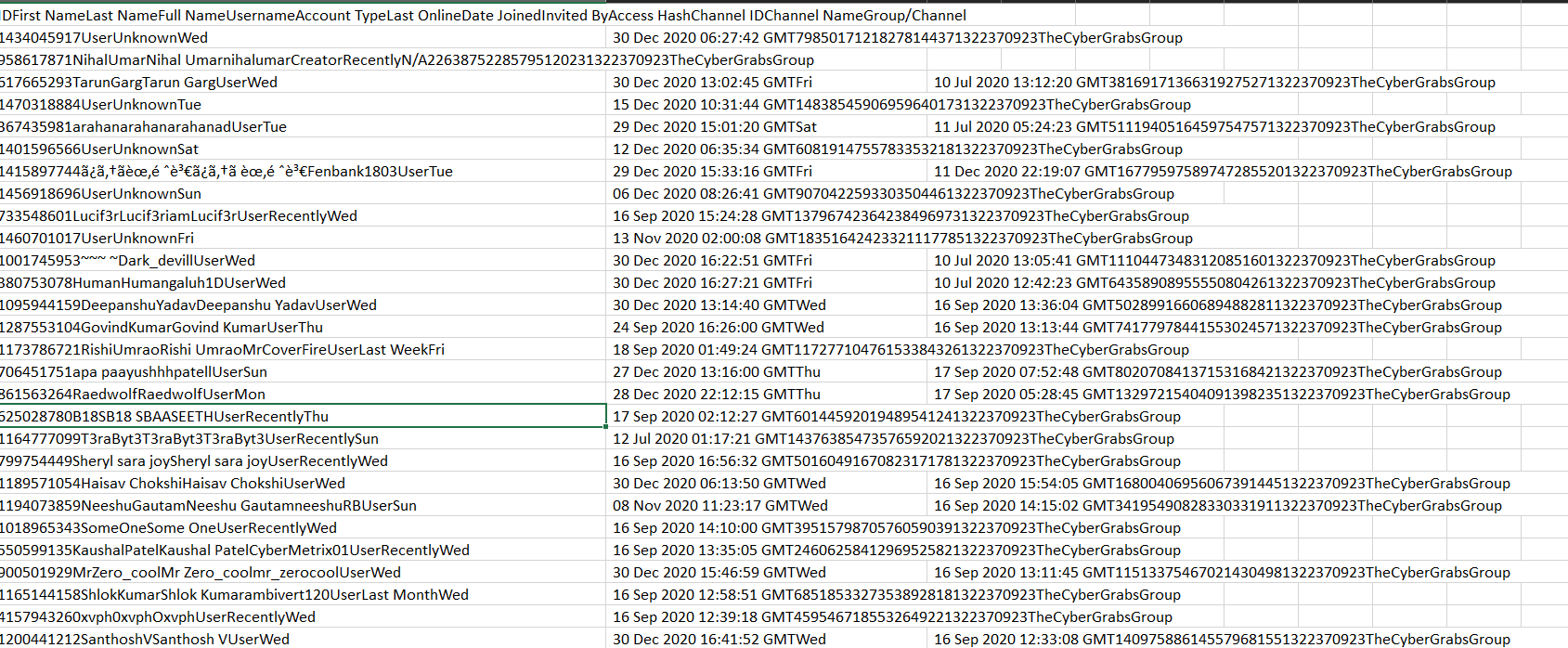
The two scripts that we require are:

* telegramScript.User.js
* getUsers.User.js

We can add these scripts to the TamperMonkey/GreaseMonkey extensions. After doing so, we should just open Telegram web and reload the page. We can see new options to the left-hand side of the screen, showing us some information about the selected group/channel and options to export the messages/users in that particular group/channel as shown below:



The results after exporting the data would look something like this:



We can export the output to a .csv format to make it more readable. This is a really efficient method to gather some publicly available information and analyse them for extracting useful data.

**CONCLUSION**

As discussed throughout this paper, Telegram is a useful and efficient instant messaging cloud-based platform which is widely used today. One of the key features of Telegram is the security that it provides to users. Due to this particular reason, cyber criminals and other malicious people have resorted to carrying out their illegal activities through Telegram. Since they can operate from any part of the world with complete anonymity, it has become a thriving spot for cyber criminals today.

Even though Telegram offers high level of security and anonymity, there are still lots of information that a person can gather from Telegram. It all depends on knowing what to look for and where to look for it. We discussed about the various entities in Telegram including Users, Groups, Channels, and bots. We also discussed about the key features of each of these entities. There are various methods available to gather useful information from Groups/Channels in Telegram. This can be done either manually or automatically. Manual methods include going through the groups/channels and looking for information. It also includes using Public search engines like Google to gather various information like usernames, invite links etc. Automatic methods include using various external tools and websites to gather information from Telegram.

The sites we discussed for information gathering are:

* inelx.io
* buzz.im
* tlgrm.eu
* tgstat.re/en

The tools/extensions we discussed are:

* Harpoon
* GreaseMonkey/TamperMonkey

**REFERENCES**

1. SANS@MIC Talk on Telegram OSINT

<https://www.youtube.com/watch?v=e_aXQYq2l6U>

1. Telegram Basics

<https://medium.com/@weibeld/telegram-basics-7c566d6d35c1>

<https://justaskthales.com/en/telegram-different-messaging-apps/>

1. Telegram OSINT

<https://medium.com/week-in-osint/week-in-osint-2019-18-ab45a6c1b810>

1. Telegram OSINT: Searching public messages in Telegram

<https://www.youtube.com/watch?v=vJOQdWk6WMw>

1. Crimes on Telegram

<https://www.business-standard.com/article/pti-stories/telegram-app-a-safe-haven-for-cyber-criminals-ker-police-to-119112501344_1.html#:~:text=The%20Kerala%20High%20Court%20was,under%20the%20purview%20of%20law>.