Manual on Social Media Intelligence (SOCMINT) for Law Enforcement Agencies

(August, 2021)

NATIONAL CYBER CRIME RESEARCH & INNOVATION CENTRE (NCR&IC)
Modernization Division
BUREAU OF POLICE RESEARCH AND DEVELOPMENT
Ministry of Home Affairs, Government of India

Manual on Social Media Intelligence (SOCMINT) for Law Enforcement Agencies

A Guide for Gathering Intelligence from Social Media

National Cyber Crime Research & Innovation Centre
Modernization Division
Bureau of Police Research & Development
New Delhi

Disclaimer

- This document is not a substitute for existing manuals available in the States/UTs. It is only a guide for awareness purpose. In case of any conflict, local manual/ practice may prevail.
- BPR&D does not promote any tool/software of a particular vendor. All the tools and software mentioned in this manual are for illustration purpose only.
- Wherever any Image/graphics/flowchart is taken from other sources, the same has been duly acknowledged.

वरुण सिंधु कुल कौमुदी, भा.पु.से.
महानिदेशक

VSK Kaumudi, IPS
Director General
Tel. : 91-11-26781312 (O)
Fax : 91-11-26781315
Email : dg@bprd.nic.in

पुलिस अनुसंधान एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037

MESSAGE

The setting up of the National Cyber Crime Research & Innovation Centre (NCR&IC) at the BPR&D Hqrs.and its branch, the National Cyber Crime Research, Innovation and Capacity Building, at the CDTI, Hyderabad, has been a major technological milestone in the cyber research and training capabilities of the BPR&D. The NCR&IC, as part of the umbrella scheme of the Indian Cyber Crime Coordination Centre (14C), MHA, has been striving countinuously to strengthen and augment the capacity of Law Enforcement Agencies (LEAs) in their efforts of Cyber Crime prevention and investigation.

I am happy that NCR&IC professionals have come up with the following four booklets to address the urgent need for awareness related to Cyber Crimes, keeping in mind the skill set required by the police officers in the investigation of Cyber Crimes:

- Emerging Cyber Crimes in India - A Concise Compilation
- First Responder Handbook - Computer System Acquisition
- SOP on Investigative Process/Methodologies for Cryptocurrency related Cyber Crimes
- Manual on Social Media Intelligence (SOCMINT) for LEAs

The above manuals/SOPs are result of the sincere efforts of Dr. Karuna Sagar, IPS, IG (Modernization), Sh. B. Shanker Jaiswal, IPS, DIG (Mod), Dr. M. M. Gosal, SSO (T) and NCR&IC professionals/experts, namely, Dr. Pankaj Choudhary, Sh. Gourav Chaurasia, Sh. M. Krishna Chaitanya and Sh. Farhan Sumbul, BPR&D. I record my deep appreciation for their hard work.

I believe, these booklets will guide the police officers in understanding the Cyber Crimes of various categories, including the modus operandi of cyber criminals, Data Acquisition in different scenarios, Methodology for Investigating Cryptocurrency and Social Media Platform, etc.

17/8/21.

(V.S.K. Kaumudi)

Place: New Delhi

नीरज सिन्हा, भा.पु.से.
अपर महानिदेशक

Neeraj Sinha, IPS
Additional Director General

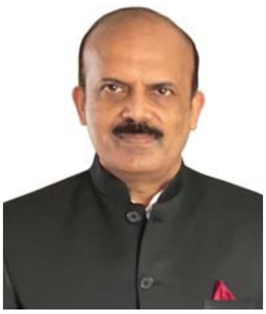
Tel.: + 91 11 26781341 • Fax: 91 11 26782201
Email: adg@bprd.nic.in • Website: www.bprd.nic.in

सत्यमेव जयते

पुलिस अनुसंधान एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037

Message



Technology is often value neutral. It can be used effectively by friends and foes alike. On occasions, the rapid strides by technology, especially in the domain of cyber-space, threatens to outpace the skills of inadequately trained professionals, especially at the cutting edge.

BPR&D, with its motto of 'Promoting Good Standards and Practices', has often bridged the information gap for the LEAs, with its thoughtful seminars and publications. It gives me great pleasure that the National Cyber Research & Innovation Centre (NCR&IC) professionals are putting together 04 significant compilations, including 'Emerging Cyber Crimes in India – A Concise Compilation'; 'First Responder Handbook – Computer System Acquisition'; 'SOP on Investigative Process/Methodologies for Crypto-currency related Cyber Crimes'; and 'Manual on Social Media Intelligence (SOCMINT) for the LEAs'.

The team of the Modernization Division of the BPR&D, led by Dr. Karuna Sagar, IPS, IG, Shri B S Jaiswal, IPS, DIG, Dr. Manjunath M Gosal, SSO (T), Dr. Sarabjit kaur, Dr. Pankaj Choudhary, Sh. Gourav Chaurasia, Sh. M. Krishna Chaitanya and Sh. Farhan Sumbul, are deserving of our appreciation for the publications.

I trust the Investigating Officers, particularly at the cutting edge, would find these compilations useful in their day to day professional lives.

(Neeraj Sinha)

Place: New Delhi.

डॉ. करुणा सागर, भा.पु.से.
महानिरिक्षक/निदेशक (आधुनिकीकरण)

Dr. Karuna Sagar, IPS
Inspector General/Director (Modernisation)

Tel. : 91-11-26782023
91-11-26782030 (F)
Email : igmod@bprd.nic.in

पुलिस अनुसंधन एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037

Executive Summary

As more and more users have the access to the internet and social media on a daily basis, the amount of harmful content and behaviours online is also growing which leads to Cyber Crimes. Many popular Social Media Platforms on the Internet such as Facebook, Twitter, Tumblr, YouTube, Instagram, Flick, Blogs and discussion forums are continuously being misused by cybercriminals and radical/extremist group for gathering sensitive user information, spreading their beliefs and ideologies, promoting radicalization, recruiting members and creating online virtual communities sharing a common agenda.

The "Manual on Social Media Intelligence (SOCMINT) for LEAs" is also one of the intiatives by the NCR&IC and the BPR&D undertaken in consultation with experts and other stakeholders. This manual can aid in the investigation of cyber crimes related to various Social Media Platforms and in determining the mindset and motive of Cyber crime, in finding eyewitnesses, in establishing probable reasons to issue a warrant, tracking the cybercriminals, Evidence location & Evidence collection

The support of Dr. Pankaj Choudhary in bringing out this publication is very commendable as this manual will assist all the Investigating officers across the country towards better preparedness in handling Cyber crimes related to various Social Media platforms

18.8.2021

(Dr. Karuna Sagar)

Place: New delhi

Table of Contents

List of Figures

List of Tables

Acronyms

SOCMINT	:	Social Media Intelligence
OSINT	:	Open-Source Intelligence
LEAs	:	Law Enforcement Agencies
FB	:	Facebook
Insta/IG	:	Instagram
WWW	:	World Wide Web

1. Introduction: Social Media Intelligence (SOCMINT)

Social media sites open up numerous opportunities for investigations on World Wide Web (WWW), because of the vast amount of useful information located in one place. For example, one can get a huge amount of personal information about any person worldwide by just checking his/her Social Media profiles on Facebook, Twitter, Instagram, Youtube etc. Such personal information frequently includes the person of interest's interactions on Facebook, political views, religion, background, country of origin, personal images and videos, spouse details, home and work addresses, frequently visited locations, social activities (e.g., sports, theatre, and restaurant visits), work history, education, important event dates (such as birth date, graduation date, relationship date, or the date when left/started a new job), and social interactions. This can all be found in the Social Media Profiles of an Individual (i.e. Facebook, Twitter, Instagram etc.).

Social Media Intelligence (SOCMINT) is a sub-branch of Open-Source Intelligence (OSINT), it refers to the data/intelligence/information collected from Social Media websites of an Individual or an Organization. The data or information available on Social Media sites can be either available in the Public Domain (i.e., public posts on Facebook, Twitter or LinkedIn) or it may be Private to the user. Private information - such as contents shared with a private friend's circle (i.e. private posts, comments, events, timelines etc.) cannot be retrieved without prior permission from the creator/user.

Data/Information available on Social Media Platforms can be classified into two major categories:

1. The original content posted by the user: (i.e. Facebook post, uploaded image/video, pages, likes, comments, mentions, retweets etc.
2. The metadata associated with original content: multimedia files metadata, the date/time and geo-location info associated with the posted content.

1.1 How Social Media Intelligence is Gathered?

Many popular Social Media Platforms on the Internet such as Facebook, Twitter, Tumblr, YouTube, Instagram, Flickr, Blogs and discussion forums are continuously being misused by cybercriminals and radical/extremist groups for gathering sensitive user information, spreading their beliefs and ideologies, promoting radicalization, recruiting members and creating online virtual communities sharing a common agenda. For example, Twitter (a popular microblogging website) is being used as a real-time platform for information sharing and communication during the planning and mobilization of public conflict-related events.

The first step towards gaining Social Media Intelligence is data/information. This data is collected from Social Networking Sites via a feed known as an Application Protocol Interface (called an API for short). By itself, this data doesn't represent Social Media Intelligence, but the same data can be further used for gathering more intelligence from Social Media. Various metrics derived from parsing the data from APIs and overlapping other data points can be useful in building up the intelligence. Various Open Source Intelligence (OSINT) tools are available in the public domain for gathering such intelligence.

1.2 Objectives

The objective of this manual is to understand various Social Media and Social Networking System like Facebook, Twitter, LinkedIn, Instagram, WhatsApp, Signal etc. Cybercriminals actively use such Social Media sites and news websites to share information, ideas, personal messages, videos, and to spread rumours, fake news etc. Furthermore, cybercriminals carry out numerous unlawful activities such as drugs smuggling, confidential data selling, sex trading etc. via Social Media. They actively use Social Media as their promotion and communication platform for commuting crimes. Also, cybercriminals use such platforms to hide their real identities. The goal of this manual is to explain the major features of popular Social Media Platform covering various evidence aspects for the Investigation of Cyber Crimes.

This manual can aid in the investigation of Cyber Crimes related to various Social Media Platforms, including:

- In determining the mindset and motive of Cyber Crime
- In finding eyewitnesses
- In establishing probable reasons to issue a warrant
- Tracking the cybercriminals
- Evidence location
- Evidence collection

The manual will also introduce the popular terms related to the SOCMINT and determine how several Open-Source Intelligence (OSINT) tools, online services and techniques to gather intelligence from social media sites to support a variety of intelligence needs.

1.3 Social Media vs Social Networking System

Table 1: Social Media vs Social Networking System

Social Media System	Social Networking System
• Anyone can search for anyone • Public platform • The published content may be a reason for interaction and networking • To create buzz, spread rumours • Cyber Criminals utilize it to hide their identity and execute criminal/illegal activities or to honey trap someone	• Used for online personal and professional networking through various apps like WhatsApp, Telegram, Signal, Snapchat, WeChat etc. • Peer to peer networking, only connected users can communicate with each other over the network • Nurture personal and professional relationship • Cyber Criminals utilize it for communication and for spreading rumours

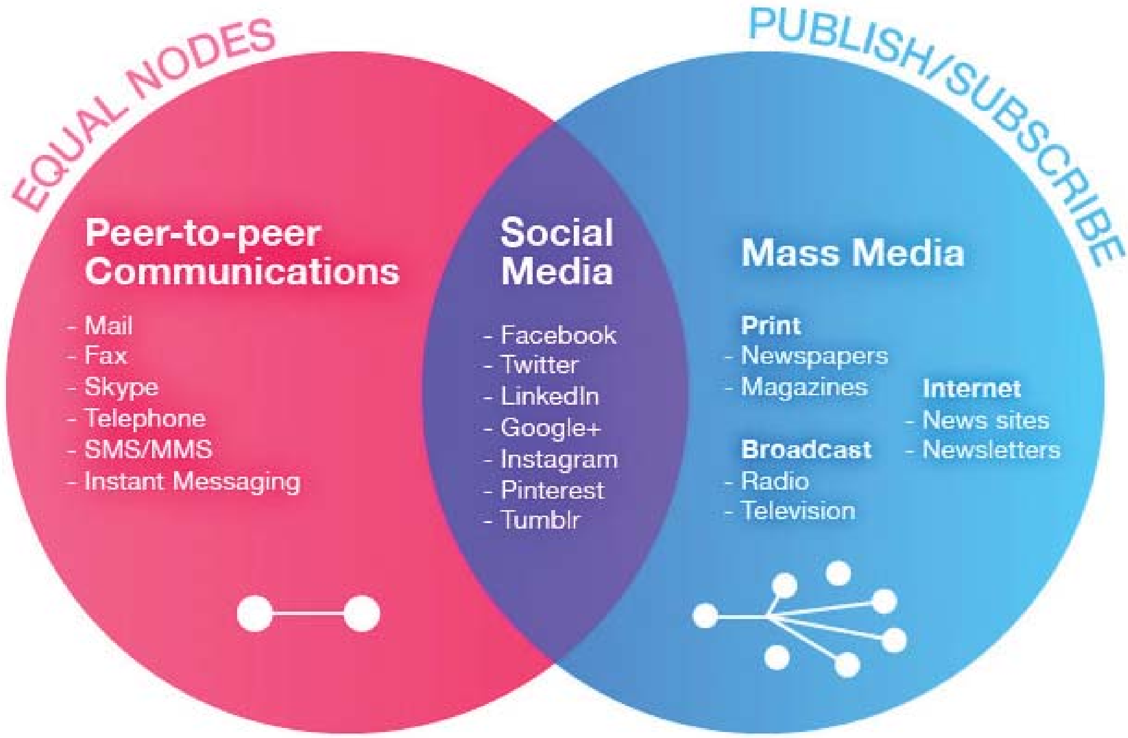


Figure 1: Social Media VS Social Networking

2. Social Media Platforms & Contents

2.1 Classifications of Social Media Platforms

Many people use the terms Social Media and Social Networking interchangeably to refer to Facebook, Twitter, LinkedIn, Instagram, Youtube and related social platforms. Social Media contains many other categories like "Social Networking". The following are the main Social Media types classified according to function:

1. Social networking: This allows people to connect with other people and businesses (brands) online to share information and ideas. Example: Facebook, LinkedIn etc.
2. Photo sharing: Such websites are dedicated to sharing photos between users online. Example: Instagram, Flicker etc.
3. Video sharing: Such websites are dedicated to sharing videos, including live video broadcasts. Example: YouTube, Instagram, Facebook, Twitter etc.
4. Blogs: This is a type of informational website containing a set of posts belonging to one topic or subject organized in descending order according to the publish date. The most popular blogging platforms are WordPress and Blogger, which is powered by Google.
5. Microblog: This allows users to publish a short text paragraph (which can be associated with an image or video) or a link (URL) to be shared with other audience online. Example: Twitter.
6. Forums (message board): This is one of the oldest types of social media. Users exchange ideas and discussions in a form of posted messages and replies. Example: Reddit, Quora.
7. Social gaming: This refers to playing games online with other players in different locations. It has gained more popularity recently. Example: KAMAGAMES, Zynga etc.
8. Social bookmarking: These websites offer a similar function to your web browser's typical bookmark. However, they allow you to do this online and share your Internet bookmarks among your friends in addition to adding annotations and tags to your saved bookmarks. Example: Atavi, Pinterest etc.
9. Product/service review: These websites allow their users to review give feedback about any product or service they have used. Example: Amazon, Flipkart etc.

2.2 Social Media Content Types

People interact with Social Media sites for different purposes. The following are the general interactions used across different social media sites:

1. Post/comment: People access social sites to post or write paragraphs of text that can be seen by other users. Such posts can also include user's geographical info (In Facebook, they call this feature, a "Check-in").

2. Reply: This is a text message (can also be an image, video, or URL) that replies to another user's post, update status or comment.

3. Multimedia content (images and videos): Multimedia is popular; a user can upload a video or image as a part of their post. Many social platforms allow their users to upload multiple images/videos to form an album. Live streams also are available on many social platforms such as Facebook, Twitter and YouTube. This feature allows a user to broadcast live videos and display the recording on their profiles for later viewing.

4. Social interactions: This is the essence of social media sites, where people get connected online by sending/responding to other user's request.

5. Metadata: The results from the sum of user interactions with the social platform. Examples include the date and time when a video/image was uploaded, the date and time when a friend request was accepted, geolocation data if enabled of the uploaded multimedia file or post, and the type of device used to upload the contents (mobile or a standard computer).

SOCMINT is interested in gathering all these content types, however, the ability to do this depends on the privacy control level set by each user when publishing posts/updates online. For example, it is not possible to see other people's updates on Facebook if they restrict a post's visibility to some friend circles or set it to "Only me."

2.3 Popular Social Media Sites, Terminologies & Evidences

2.3.1 Facebook

Facebook is the most popular Social Media platform; it falls under the social networking type and has the largest users base on earth. Facebook was offering an advanced semantic search engine to search within its database by using natural English language phrases and keywords. This semantic search engine called Facebook Graph Search and was first introduced in early 2013. It allows Facebook users to type in their queries in the Facebook search box to return accurate results based on their questions/phrases or combined keywords. For example, you can type: Pages liked by ********* replacing the asterisks with the target's Facebook username, to return a list of pages liked by the specified user.

In 2019, Facebook has removed the Graph search functionality, although, users are still able to utilize Graph Search, however, they need to build their graph search queries manually.

Popular Terminologies on Facebook are shown in Table 2.

Table 2: Popular Terminologies on Facebook

S. No.	Terminology	Description
1.	Timeline	Profile Page
2.	Newsfeed	A continuous stream of updates about friends' activities
3.	Status Update	Short post user shares on Facebook that tells- what is the user doing
4.	Poke	casual gesture- I'm thinking of you
5.	Tagging	Tag links a person, page, or place to something user posts e.g., status update or photo.
6.	Timeline Review	A tool that lets user approve or reject posts that he has been tagged in before these go on his/her Timeline
7.	Trending	List of popular topics on Facebook.
8.	Activity Log	To manage Page's Timeline. It shows the complete list of posts and comments by user/page, including hidden posts.
9.	Check-Ins	User's location to their Facebook friends. If Page includes an address, it will appear in a list of "check into locations" when people are nearby.
10.	Page Admin	After Page creation, the user automatically becomes the Page's admin, which means only the user can change how the Page looks and only he can post as the Page. Further user can assign roles to other people to manage the Page.
11.	Page Roles	There are five different roles for people who manage Facebook Pages like admin, editor, moderator, advertiser, and analyst. The person responsible for these roles logs into his/her own personal account and work on the Page from there.
12.	Daily Active Users	A total number of people who have viewed or interacted with Facebook Page on a date.
13.	Engaged Users	A total number of users who have clicked anywhere on at least one of the user's Facebook Page posts e.g. liked one or more of your posts, commented, or shared it.
14.	**External Referrers**	number of views your Facebook Page received from website URLs other than Facebook.com
15.	**Organic Reach**	A total number of unique individuals who saw a specific post on Facebook Page on their News Feeds, tickers, or directly on their Pages.
16.	**Viral Reach**	A total number of unique individuals who saw a specific post from a user's Page through a story published by one of their Facebook friends.

17.	**Media Consumption**	A total number of times a media content that was published on a user's page, including a video, photo, or audio clip – is clicked and viewed on a specific day.

The following evidence on Facebook can be found during the investigation and intelligence gathering as shown in Table 3.

Table 3: Facebook & Evidence

Facebook	Evidence
• Facebook: owned by Facebook Incorporation • Users create a personal profile; add other users as friends, exchange messages including automatic feed notifications when they update their profile information. • They share news stories, notes, photos, videos, and their achievement and allow their friends (or friends of friends) to comment. • Users join common-interest groups, organize events • Create fans pages for a business, a school/ college, or even a brand or product. • Head Quarter -Menlo Park, California-U.S.	• Instant chats, wall comments and group events leave footprints at various memory locations like RAM, browser cache, page files, unallocated clusters and system restore point of a computer • Investigating Officer can note the following- Created time of a post or message on Facebook, user id, account id, message-id • Facebook Ad displayed on user account can reveal a lot of information about the user to the investigation officer.

2.3.2 Twitter

Twitter has a built-in corner search functionality located in the upper-right side of the screen when using the Twitter web interface after logging into your Twitter account. A simple Twitter search allows you to perform a basic search within the Twitter database.

Advanced search operators can be used similar to Google advanced search operators known as Google Dorks to your search query to force it to dive deep and return accurate results.

Popular Terminologies on Twitter are shown in Table 4.

Table 4: Popular Terminologies on Twitter

S.No	Terminology	Description
1.	@	@ sign is used to address usernames in Tweets: "Hello @Abc!"
2.	Tweet	The message the user posts
3.	Follower	A follower is a Twitter user who has subscribed to another user's account so that he or she can see all of that user's posts and updates on his own page
4.	Re-tweet	Sharing of the original post by another user on his or her own page.
5.	Hashtag	The hashtag is a keyword that is preceded by a pound (#) sign, e.g #article370. Any user who clicks the hashtag will be led to a page that lists all Twitter users who have applied that particular hashtag in their own posts
6.	DM	The direct message is sent privately and can only be seen by the sender and the receiver.
7.	Geotagging	Adding user's location to Tweet to inform the account followers about your location at the time of the tweet.
8.	Trend	A Trend is a topic or hashtag that has been determined most popular on Twitter algorithmically.
9.	Avtar	User's profile picture to identify him/her
10.	Username/ Handle	"Handle" refers to the user's specific URL on Twitter. Twitter username is @modi and the user's Twitter handle is http://www.twitter.com/modi

The following evidence on Twitter can be found during the investigation and intelligence gathering as shown in Table 5.

Table 5: Twitter & Evidence

Twitter	Evidence
• Twitter is a 'microblogging' system to send and receive short messages called tweets. • Tweets are public, but users can also send private direct messages • Tweet's length =up to 280 characters long in most countries except China, Japan and Korea • Can include web links to websites and resources. • Using SMS- Users can send through five gateway (networking hardware that allows data to flow from one discrete network to another) numbers. These are short codes for the United States, Canada, India, New Zealand, and an Isle of Man-based number for international use. • There is also a short code in the United Kingdom that is only accessible to those on Vodafone, O2 and Orange networks. • In India, since Twitter only supports tweets from Bharti Airtel, an alternative platform called smsTweet. • A similar mobile phone platform GladlyCast is being used in Singapore and Malaysia • In 2015, Twitter roll out the ability to attach poll questions to tweets. These polls are open for up to 7 days, and voters are not personally identified • Twitterbot - a computer program that automatically tweets, re-tweet, and follow other accounts. Cybercriminals may use these bots to spread rumours, Fake news etc. • Used for live video streaming	• Time and dates of tweets • Association with followers of the user Association with people whom he follows • Tweets from a mobile device or from Twitter's website • footprints may be available at various memory locations like RAM, browser cache, pagefiles, unallocated clusters and system restore point of a computer

2.3.3 LinkedIn

LinkedIn is a popular 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.

Popular terminologies in LinkedIn are shown in Table 6.

Table 6: LinkedIn Popular Terminology

S.No	Terminology	Description
1.	Update	Status updates and content/news/article that the user posts.
2.	Profile	Resume
3.	Connection	List of persons, the user has added to his LinkedIn network
4.	Recommendation	Recommendations are written by user's connections about user's professional skills and strength
5.	Endorsement	Having other people endorsing a user's skills adds credibility to his profile, it may create a positive impression on potential employers.
6.	Mention	Tag others connection in LinkedIn updates similar to Facebook and Twitter
7.	Degree	The chain link user is connected to a person e.g. 1st-degree connections - People user is directly connected to because either user has accepted their invitation to connect, or they've accepted the user's invitation to connect. Likewise, 3 degree means, people are connected to the user via his 2nd-degree connections.
8.	Groups	Group can be public or private to allow users to connect with each other and discuss a specific topic on one page via the group.
9.	Advanced people search	to search LinkedIn's member database in a variety of ways e.g. past or present job title wise, seniority level wise, postal code wise, company wise, etc.
10.	InMail	Messages that the user can send directly to any LinkedIn member that is not his connection. InMail can be purchased and these are available free with a premium LinkedIn account.
11.	Message	The message is free to first-degree connections and fellow group members.
12.	LinkedIn Pulse	Pulse shares news and content from various channels, influencers, and trending news.

The following evidence on LinkedIn can be found during the investigation and intelligence gathering as shown in Table 7.

Table 7: LinkedIn & Evidences

Linkedin	Evidences
• List of connections can be exported to a notepad file • Showcase pages generate leads and are customized for B2B companies. • who's viewed my profile- on the right side of LinkedIn page. It shows the details of the LinkedIn members who viewed user's profile • LinkedIn relationship note- helps you remember things e.g. something about the person user would like to remember. • Reference Search - For premium members to find job candidates' past colleagues • Review Analytics - shows overall engagement trends & post performance like clicks, likes, comments, shares etc • Alumni Tool –To Identify alumni in your field and of your school/college and connecting with them • Native Videos- These are uploaded directly under the LinkedIn video feed. • LinkedIn video ads - sponsored company videos that appear in the LinkedIn feed • Blogging Interface -publish content directly on LinkedIn just like any other blogging platform and share as blog post • Keyword Search -Enter multiple keywords, and LinkedIn searches for members who have all the keywords in their profile. • Content Suggestion- tells popular topics and trends among user's target audience	Time and dates of posts, messages First degree, second degree, third degree etc. user connections footprints may be available at various memory locations like **RAM, browser cache, pagefiles, unallocated clusters and system restore point of a computer**

2.3.4 Instagram

Instagram is owned by the Facebook. Instagram has been criticized because drugs images were published on it. In 2013, the BBC discovered that users, mostly located in the United States, were posting images of drugs they were selling, attaching specific hashtags, and then completing transactions via instant messaging applications such as WhatsApp.

Popular terminologies in Instagram are shown in Table 8.

Table 8: Instagram Popular Terminology

Terminology	Description
• Instagram Handle	Username
• DM	Direct Message
• Engagement	Total number of likes and comments on a post
• Impressions	Number of times a particular post/content has been seen.
• Mention	Begin with the @ symbol, followed by their handle/ name.
• IG Live or Instagram Live	Videos live streaming similar to Facebook Live or Periscope.
• Hashtag	Hashtags describe and categorize the Instagram posts. The # symbol is used at the beginning of a #hashtag and can be clicked on to find similar posts. Using popular hashtags, can help to increase the visibility of the posts.
• Story	Short, no more than 15 second post visible for 24 hours on the page. Multiple stories can be created in a day.

The following evidence on Instagram can be found during the investigation and intelligence gathering as shown in Table 9.

Table 9: Instagram and Evidences

Instagram	Evidences
• Instagram used for uploading pictures, communication and networking with other people. • **Stories Archive**- Stories created and shared on Instagram are automatically saved in "Stories Archive", so there's no need to save them to phone. • User can turn off Stories Archive at any time in **Settings**. • **Instagram Feed** - To share and connect with the people and things. When user opens Instagram or refreshes his feed, the photos and videos Instagram thinks that are important for that user appear on top of user feed. • In addition to seeing content from people and hashtags user follow, he/she may also see suggested accounts that are relevant to his/her interests. • **Instagram Ad Policy**- Instagram shows ads from businesses that are interesting and relevant to user as per his Instagram and Facebook usage history and on third-party websites and apps. • For example, user might see ads based on the people he/she follows and things he liked on Instagram, his information and interests on Facebook • **Explore Tab**: To search and discover by hashtag or by user.	Post, thread id, recipients, created time, updated time, link, comments, and picture url etc. Footprints may be available at various memory locations like **RAM, browser cache, iPhone Photo album, Android's file folder** Pictures uploaded date is the same as the creation date **-Check** Instagram does not offer a free text search, only existing content terms, existing accounts, hashtags, places, etc. can be searched.

2.3.5 WhatsApp

WhatsApp Messenger, or simply WhatsApp, is an American freeware, cross-platform centralized messaging and voice-over-IP service owned by Facebook, Inc. It allows users to send text messages and voice messages, make voice and video calls, and share images, documents, user locations, and other content.

Popular terminologies in Whatsapp are shown in Table 10.

Table 10: Whatsapp Popular Features & Evidences

Whatsapp	Evidences
• WhatsApp on Web and Desktop • Audio, Video calls • Documents, image, audio, video sharing • End to end encryption • Delivery and read notification • Restoring chat history media to Google Drive • WhatsApp Business lets you create an account using a landline number • Access WhatsApp via web- Open https://web.whatsapp.com in browser and scan the QR code by using the WhatsApp app on user's phone	User profile includes WhatsApp name, status line, and avatar (a picture). The profile of each user is stored on a central system WhatsApp Messenger stores all the messages that have been sent or received into the chat database msgstore.db. msgstore.db contains message and chat list Deleted messages are stored in msgstore.db-wal Database analysis is helpful in reconstructing the chronology of exchanged messages; message sent time, whether it has been received by its recipients. Backup location- msgstore-YYYY-MM DD.1.db.crypt12 to msgstore.db.crypt12 Android: sdcard/WhatsApp/Databases/msgstore.db.cryt WhatsApp database can be inspected for both iOS WhatsApp database can be inspected for both (iOSChatStorage.sqlite) and Android (msgstore.db & wa.db) devices.

Example: Whatsapp messages backup sample

Figure 2: Whatsapp Messages Evidence

2.3.6 Telegram

Telegram is a cloud-based instant messaging and voice over IP service. Telegram apps are available for Android, iOS, Windows, macOS and Linux. Users can send messages and exchange photographs, videos, stickers, audio and files of any type.

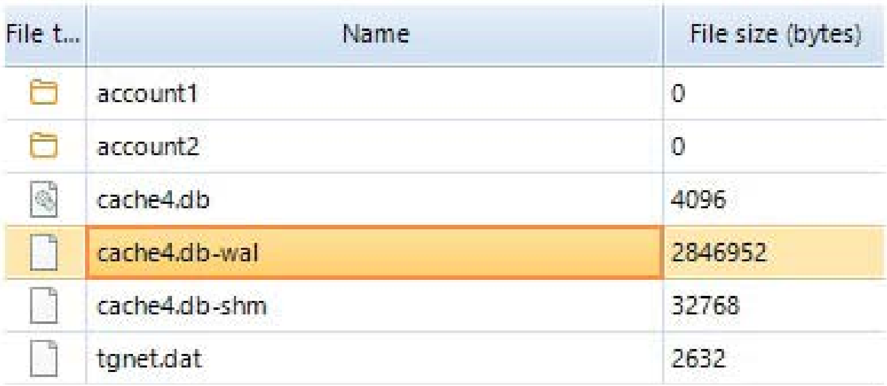
Telegram is registered as both an English LLP and an American LLC. It does not disclose where it rents offices or which legal entities it uses to rent them. The Telegram team is currently based in Dubai.

Popular terminologies and evidence in Telegram are shown in Table 11.

Table 11: Telegram and Evidence

Social Networking System	Evidences
• Telegram messages are heavily encrypted and can self-destruct. • Cloud based to access messages using multiple devices • Voice Calls • Telegram servers are spread worldwide for security and speed. • Free, No ads. No subscription fees. • No limits on the size of media and chats • Sync chats across all connected devices • Self destruct message with timer • Secret chats- Use end-to-end encryption. Only user and the recipient can read those messages — nobody can decipher those messages, including Telegram	• Telegram stores messages in a SQLite database. • cache4.db file can be looked for evidences

Example: Telegram message evidence sample is shown in Figure 3.



File t...	Name	File size (bytes)
	account1	0
	account2	0
	cache4.db	4096
	cache4.db-wal	2846952
	cache4.db-shm	32768
	tgnet.dat	2632

Figure 3: Telegram Messages Evidence

Another telegram evidences sample is shown in Figure 4.

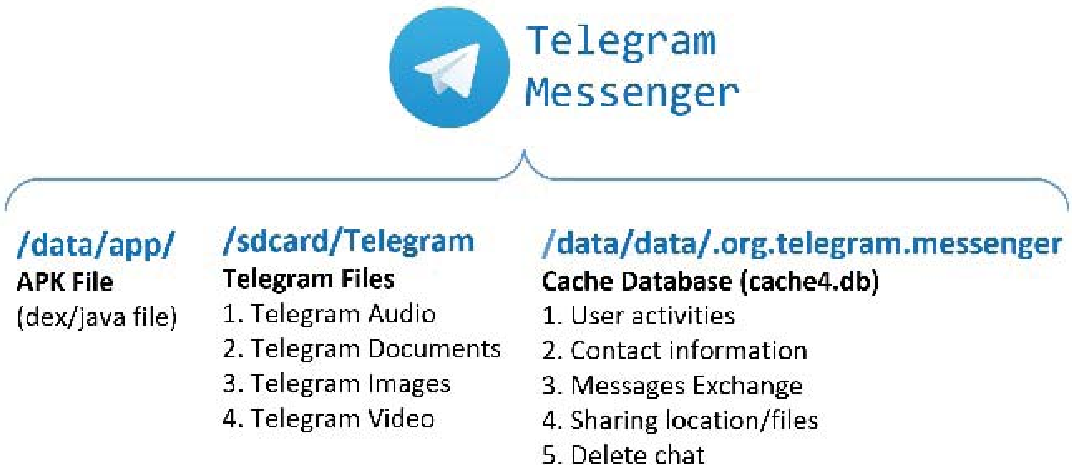


Figure 4: Telegram Messages Evidence

2.3.7 Signal

Signal, a secure app from Open Whisper Systems, is a blend of the encrypted RedPhone VoIP app and TextSecure SMS app, both from Whisper Systems, which was bought and dismantled by Twitter in 2011. Allows secure audio and video calls.

Signal is designed to never collect or store any sensitive information. Signal messages and calls cannot be accessed by us or other third parties because they are always end-to-end encrypted, private, and secure. (https://support.signal.org/hc/en-us/articles/360007318911-How-do-I-know-my-communication-is-private-)

Signal uses standard cellular telephone numbers as identifiers and uses end-to-end encryption to secure all communications to other Signal users.

Popular terminologies and evidence in Signal are shown in Table 12.

Table 12: Signal and Evidence

Signal	Evidences
• Free and open-source software chat, audio, video calling application for Android, iOS, and Desktop that employs end-to-end encryption without being intercepted while in transit • Neither signal now anyone else can else user's contact list • Once registered over signal using any mobile phone, signal app does not need to run on the phone it was registered with. • Signal stores encryption keys only on the user's device, without sending them to the server. Thus, only the sender and the recipient are included in the process of information exchange.	• Only Date & Time of user registration and last date of user's connectivity is stored by signal. • Signal does not keep conversation or encryption keys in local backup on a device. • Signal stores encryption keys only on the user's device • Signal encrypts its database. At the time of user sign in, encryption key is generated and stored in a protected key chain. Without key pictures, documents and voice messages can be extracted. • Elcomsoft may be useful in decrypting signal database.

2.4 Summary

Summary of all the popular Social Media, Networking & Evidences Location is shown in Table 13.

Table 13: Summary of Social Media & Evidence

S.No.	Social Media & Networking System	Device location wherein evidences can be found
1.	Facebook	• Browser cache file • Virtual machine image files • Virtual machine snapshot files • iPhone file system dump • Android phone file system dump • Database folder & files
2.	Twitter	
3.	Linkedin	
4.	Instagram	
5.	Whatsapp	
6.	Telegram	
7.	Signal	

3. Tools and Techniques for Gathering Social Media Intelligence (SOCMINT)

3.1 Intelligence Gathering from Social Media Sites

In the current manual the tools and techniques for Social Media Intelligence Gathering are focused on only 2 major platforms i.e. Facebook and Twitter. However, Intelligence Gathering methods for other platforms like: LinkedIn, Instagram, WhatsApp, Telegram, Signal etc. will be covered in future volumes of the same manual series.

3.1.1 Facebook

Facebook is the most popular social media platform; it falls under the social networking type and has the largest users base on earth. Facebook was offering an advanced semantic search engine to search within its database by using natural English language phrases and keywords. This semantic search engine called Graph Search and was first introduced in early 2013; it allows Facebook users to type in their queries in the Facebook search box to return accurate results based on their questions/ phrases or combined keywords. For example, you can type: Pages liked by ********* replacing the asterisks with the target's Facebook username, to return a list of pages liked by the specified user.

In 2019, Facebook has removed the Graph search functionality, although, users are still able to utilize Graph search, however, they need to build their graph search queries manually. After this Most of the 3rd party tools stopped working (i.e. Stalkscan and tools from Intel Techniques).

After removing its direct support to Graph search, Facebook has improved its search functionality making it more accurate, it also adds many filters (shown in Figure 5) to refine your search as necessary. Now login to the Facebook account is mandatory for using the search options.

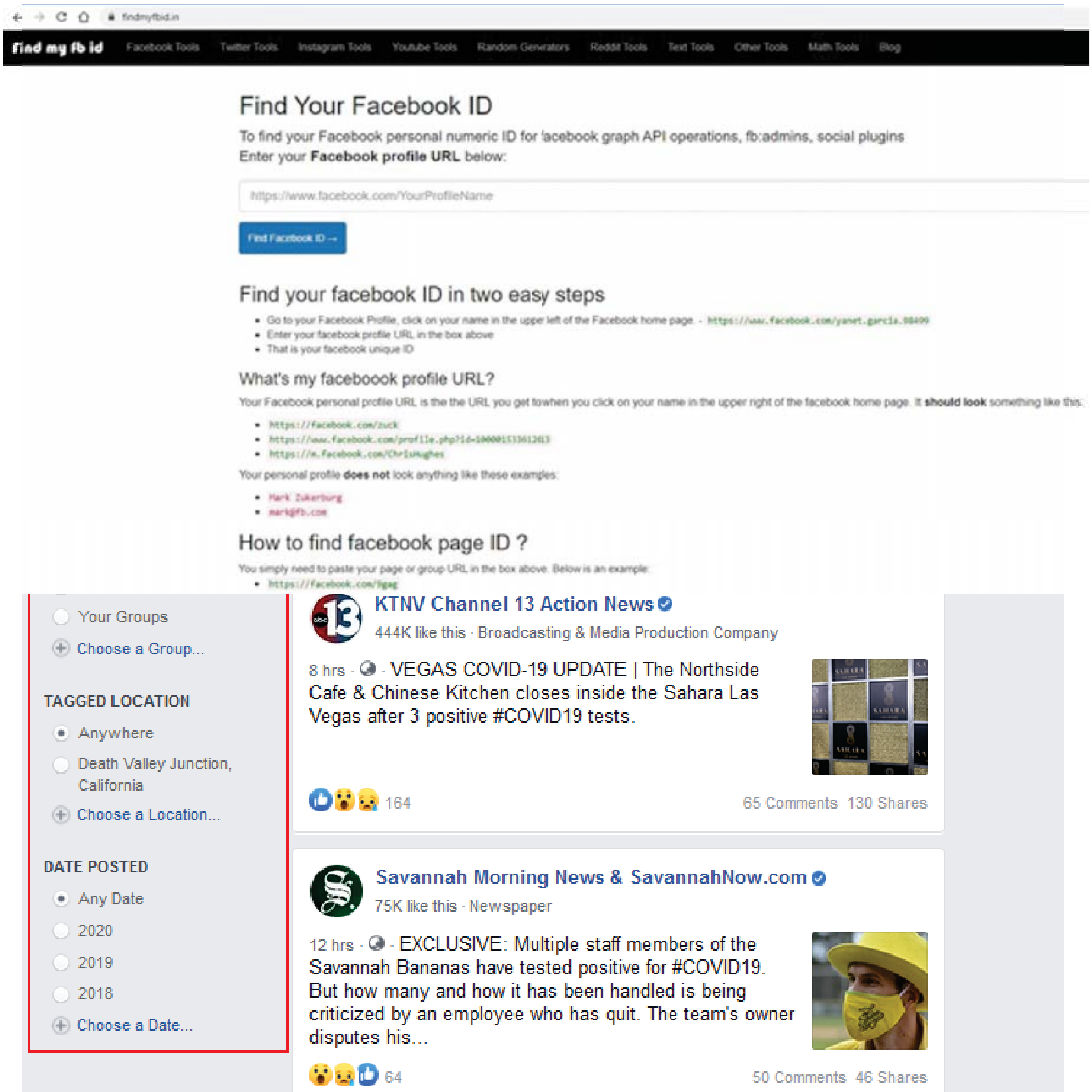


Figure 5: Using Standard Facebook Keyword search, notice the number of filters to refine your returned results

There are several online services for searching Facebook without creating customized search queries, the following list the most popular one:

Finding a Facebook ID from URL:

Facebook unique ID number or User ID is a string of numbers that does not personally identify you but does connect to your Facebook profile. User ID is assigned automatically, whenever anyone create a username. Anyone with the user ID can see your profile, including any public information. Facebook ID finder can help you find your or someone's Facebook numeric user ID easily.

a) Finding a Facebook ID using View Source

i. Open a Facebook Profile using URL

ii. Right Click and Select the View Page Source Option. (Shown in Figure 6)

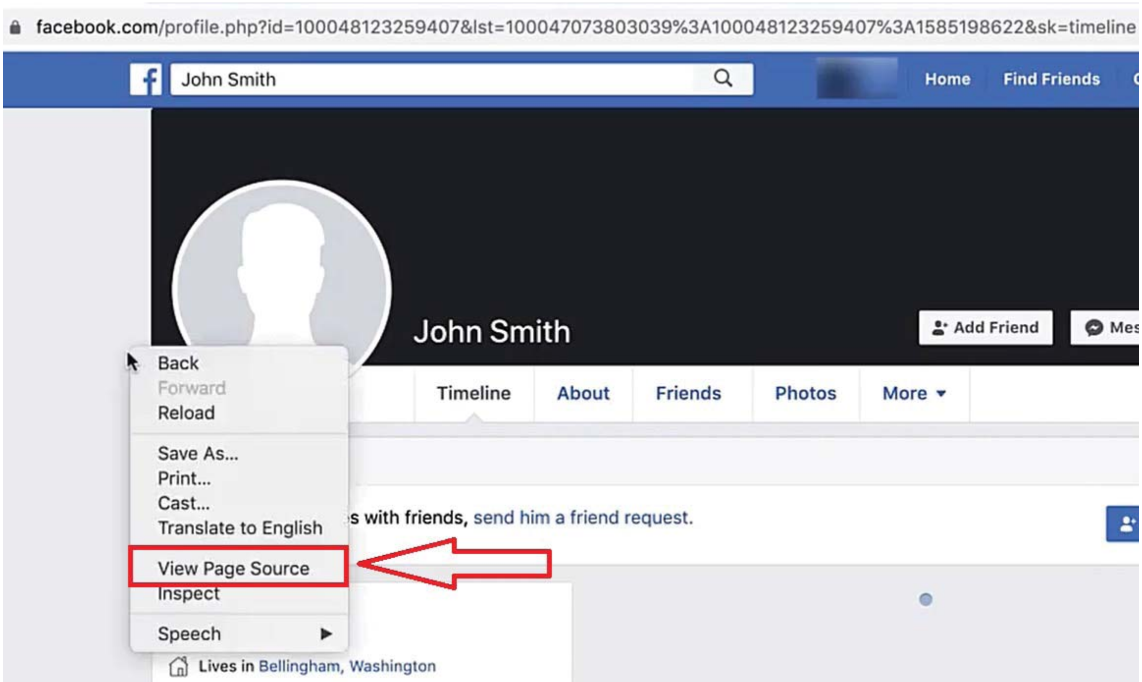


Figure 6: Finding a Facebook ID from URL (1)

iii. Using the Search (Ctrl + F) option in Browser, search for profile_id. The numeric Facebook profile ID can be found as shown in Figure 7.

Figure 7: Finding a Facebook ID from URL (2)

b) FindMyFBID (findmyfbid.in)

i. Example: Copy the profile link:

https://www.facebook.com/AllViralPosts/

Another examples of Facebook profiles should look something like this:

https://www.facebook.com/JohnDoe

https://m.facebook.com/sally.struthers

https://www.facebook.com/profile.php?id=24353623

https://www.facebook.com/AnandKumar1super30/

Figure 8: FindMyFBID (findmyfbid.in)

ii. Success!

Your Facebook personal numeric ID is:

1377348465889595

Figure 9: Finding Facebook ID using FindMyFBID

iii. To find the Facebook Group ID or Page ID, simply copy the Facebook page URL or Group URL.

Examples of Facebook Page URL and Group URL are as follows:

Page URL: https://www.facebook.com/FacebookIndia/

Group URL: https://www.facebook.com/groups/NationalGeographic/

Facebook Advanced Search

Facebook Advanced Search is a robust tool that helps to refine the search using certain filters to efficiently find any individual. Using Facebook Advanced Search option investigators can find any individual if the following information are available:

a. Mutual friends then search his/her friend list.

b. Specific details information about the individual then search the specific group members.

c. School/college/university related information then search by that specific information.

Before starting the Facebook Advanced Search gather the background information with Intel, and type in every detail you have i.e. phone number, address, email, locations, organization, mutual friends etc. Following are the steps for Facebook Advanced Search:

Step 1: Go to Facebook and log in to your account. The homepage of the account logged-in will open as shown in Figure 10.

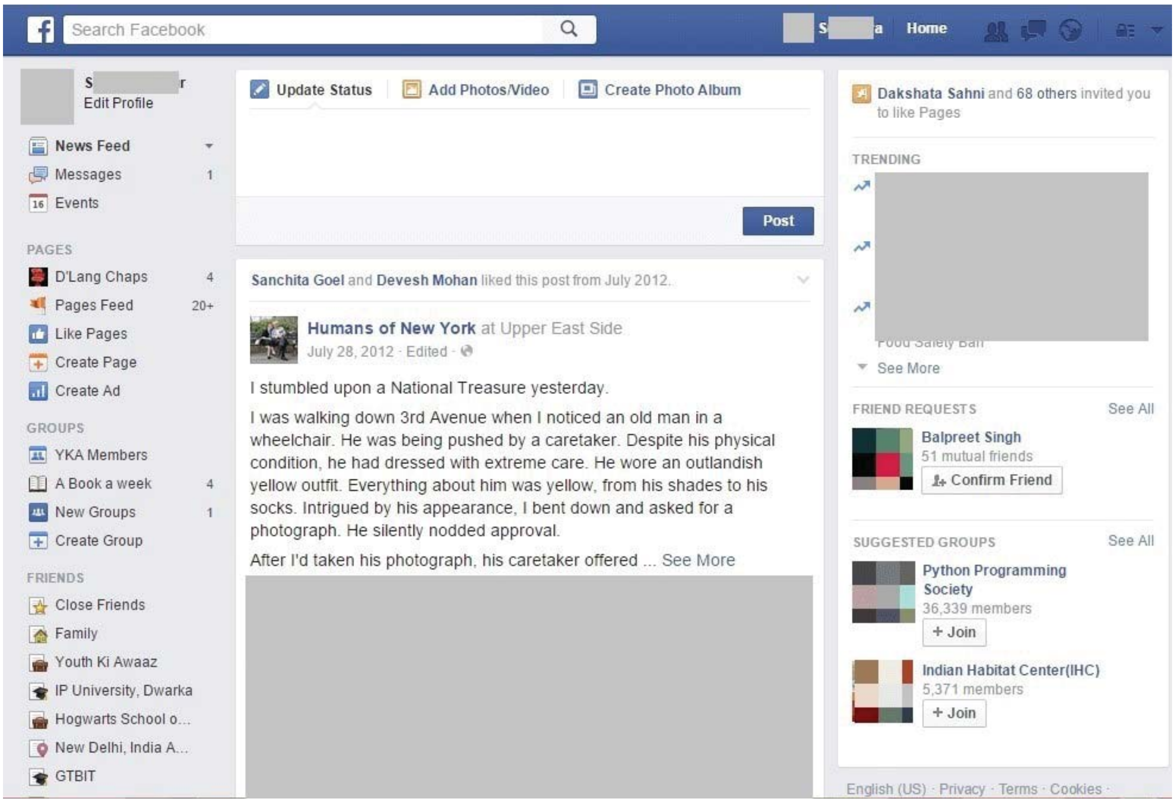


Figure 10: Facebook Advanced Search (1)

Step 2: Type the name of the person/celebrity/page you want to search for in the search bar. You can also add the name of the city the person lives in, or the school they studied in, or any other details you know, right after the name to further enhance your search. Click the magnifying glass to view the complete list of results and to refine your search.

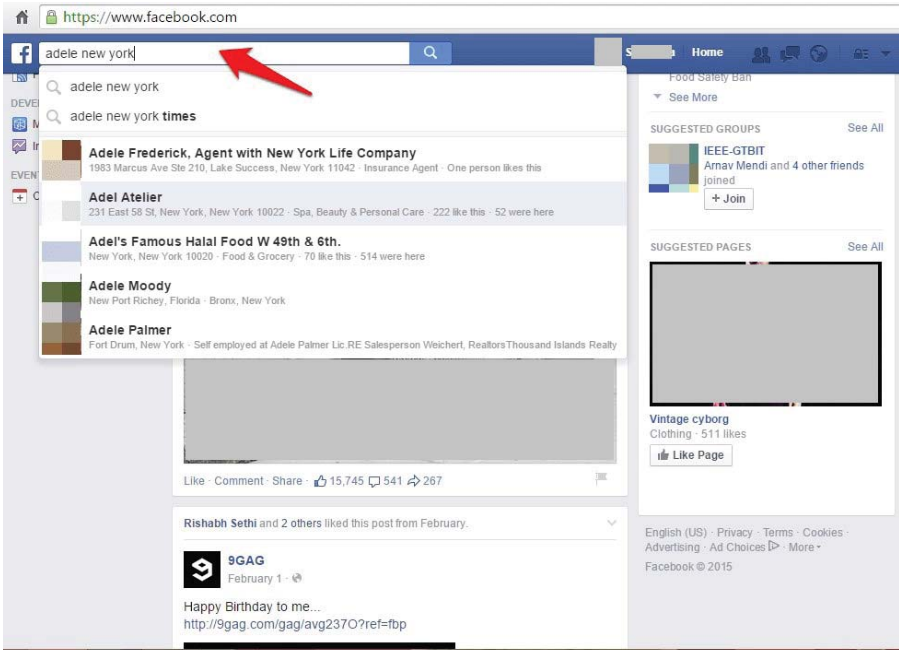


Figure 11: Facebook Advanced Search (2)

Step 3: You can filter the search on people, pages, groups or apps on this screen. You can also search for photos and places.

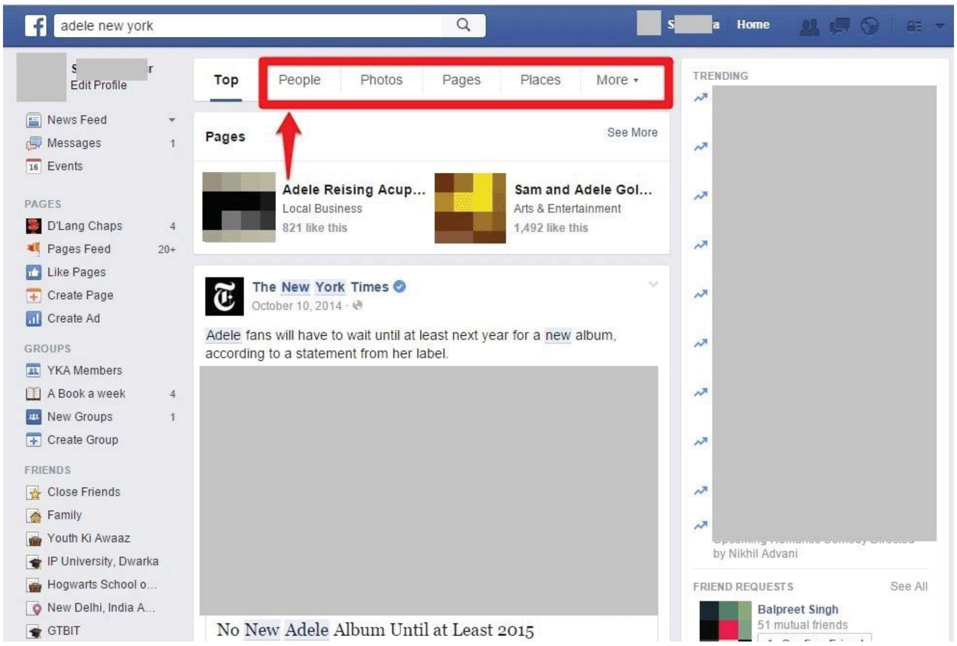


Figure 12: Facebook Advanced Search (3)

Step 4: If the search is specified to people, to get the result for individual named and place he/she lives.

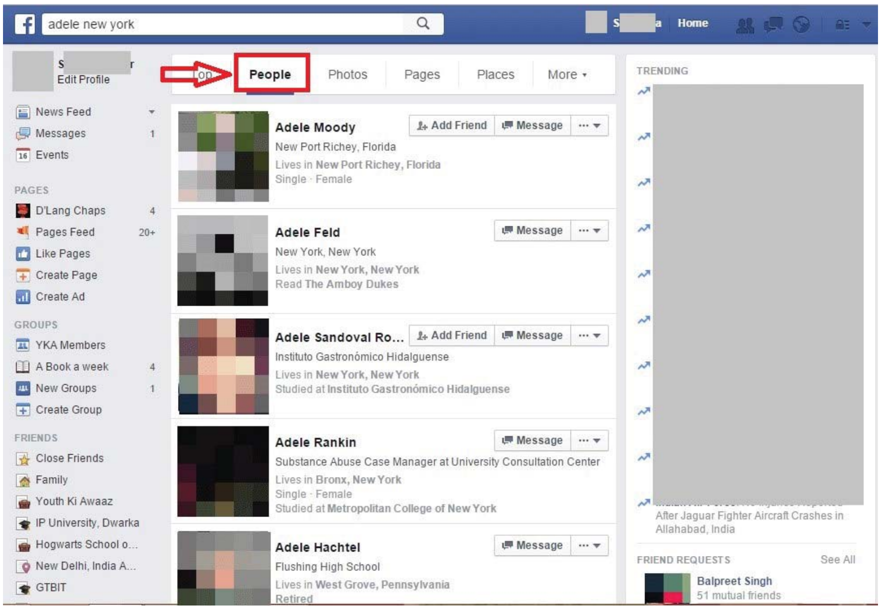


Figure 13: Facebook Advanced Search (4)

Step 5: To further simplify your search to only people you may know, you can use the Find Friends option. This can be found under your friend requests. Scroll down to the Search for Friends option on this screen.

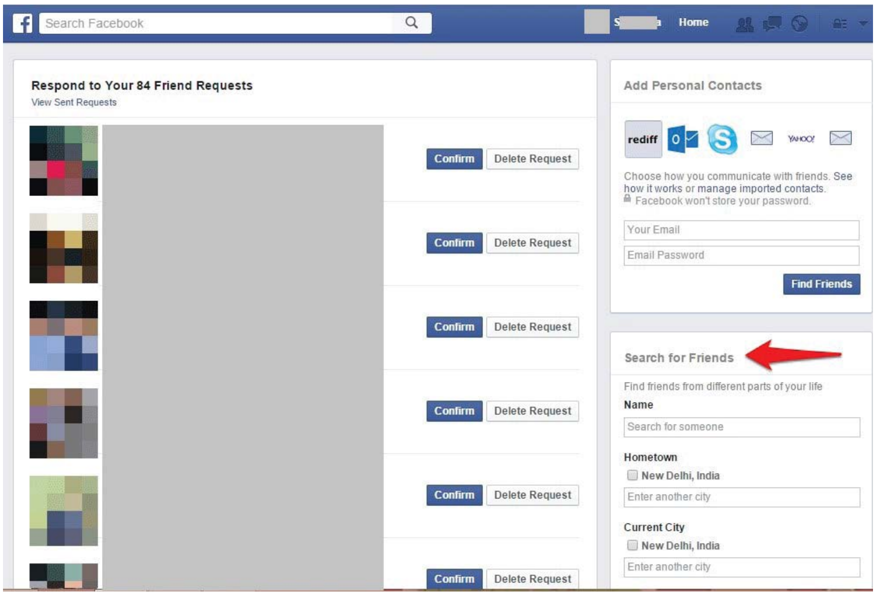


Figure 14: Facebook Advanced Search (5)

Step 6: Now details can be put for the person of interest, such as their city, their school or college, their employers or mutual friend(s), and see the results!

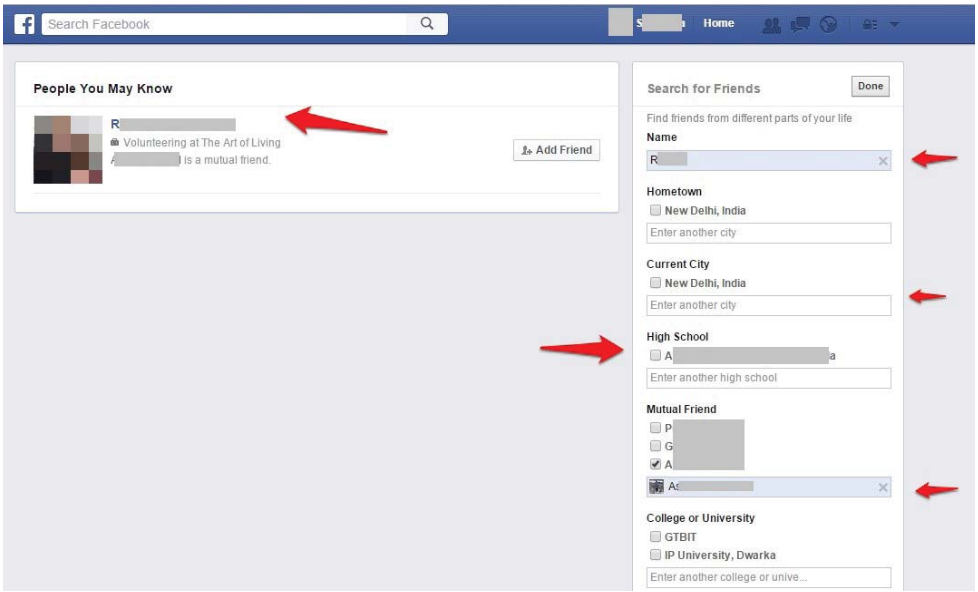


Figure 15: Facebook Advanced Search (6)

Facebook Graph Searcher from Intelligence X (https://intelx.io/tools?tab=facebook): You can search for posts from a specific date or month, post from a specific user posting about something, you can also search for posts posted by unknown users which is beneficial for online investigations (shown in Figure 16).

Figure 16: Searching Facebook using Intelligence X

Sowdust (https://sowdust.github.io/fb-search): This is another online tool to show how the current Facebook search function works, you can search for posts from a specific user/page, restrict to posts published in group or restricting it to specific location. You can filter by Start/End date and Keyword. Other search options include searching for photos, pages, places among others (see Figure 17).

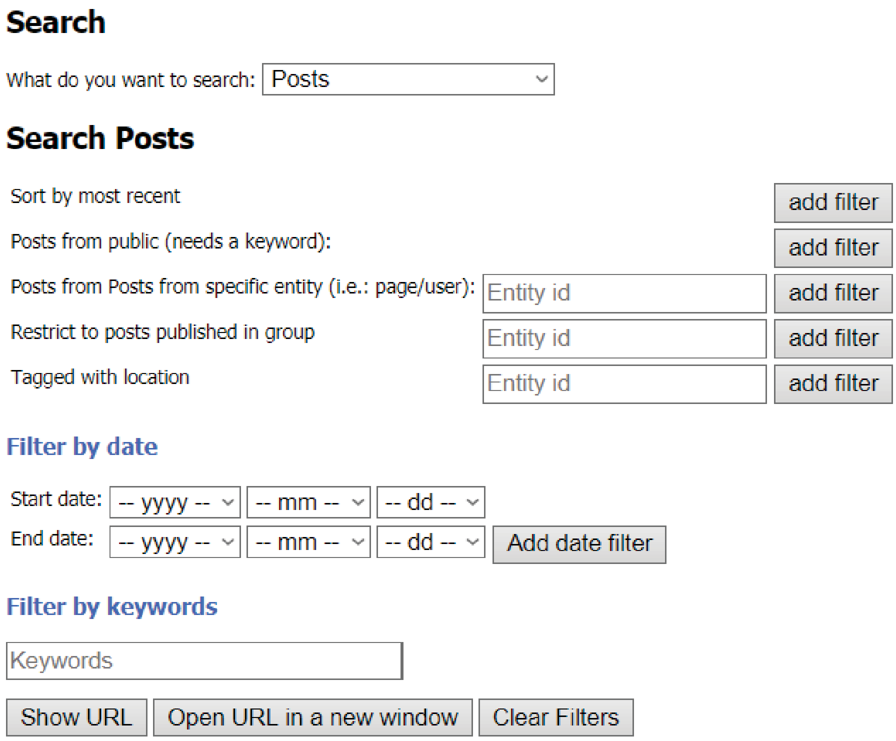


Figure 17: Sowdust interface to search Facebook

SearchBook (https://github.com/sowdust/searchbook): This is a Firefox add-on (a version is also available for Chrome browser) for executing some Graph-like searches against Facebook. The Add-on functionality is based on the research article Facebook graph search workaround published by Social Links (https://mtg-bi.com/blog/tpost/aiaxk4xl4d-facebook-graph-search-workaround). I tested this extension under Firefox, however, it broke many times during usage.

Online Facebook Search Tools/Services

There are many online services that simplify the process of acquiring/analyzing information from Facebook accounts. The following are the most useful ones:

1. Lookup ID (https://lookup-id.com): This site helps you to find Facebook personal IDs. This ID is necessary when using any of the previous online services –mentioned previously- used to compliment Facebook standard keyword search.

2. Facebook Page Barometer (http://barometer.agorapulse.com): This site gives statistics and insight about specific Facebook profiles or pages.

3. Information for Law Enforcement Authorities (https://www.facebook.com/safety/groups/law/guidelines): Offers information and legal guidelines for law enforcement/authorities when seeking information from Facebook and Instagram.

4. A directory of free tools and online services for searching within Facebook can be found at: https://osint.link/osint-part2/#facebook

3.1.2 Twitter

Twitter has a built-in corner search functionality located in the upper-right side of the screen—when using the Twitter web interface—after logging into your Twitter account. A simple Twitter search allows you to perform a basic search within the Twitter database.

However, do not underestimate this little box, as you can add advanced search operators—similar to Google advanced search operators known as Google Dorks—to your search query to force it to dive deep and return accurate results, as you are going to see next.

To begin your search against Twitter database, it is advisable to go to the Twitter Advanced search at https://twitter.com/search-advanced , from this page, you can customize search filters to specific date ranges, people and more.

Twitter Advanced Search Operators

Similar to Google, Twitter allows you to use specialized operators to find related tweets more precisely. Twitter search operators are already available in the Twitter developer site, go to https://developer.twitter.com/en/docs/tweets/rules-and-filtering/overview/standard-operators to view them (see Figure 18).

Operator	Finds Tweets...
watching now	containing both “watching” and “now”. This is the default operator.
“happy hour”	containing the exact phrase “happy hour”.
love OR hate	containing either “love” or “hate” (or both).
beer -root	containing “beer” but not “root”.
#haiku	containing the hashtag “haiku”.
from:interior	sent from Twitter account “interior”.
list:NASA/astronauts-in-space-now	sent from a Twitter account in the NASA list astronauts-in-space-now
to:NASA	a Tweet authored in reply to Twitter account “NASA”.
@NASA	mentioning Twitter account “NASA”.
politics filter:safe	containing “politics” with Tweets marked as potentially sensitive removed.
puppy filter:media	containing “puppy” and an image or video.
puppy -filter:retweets	containing “puppy”, filtering out retweets
puppy filter:native_video	containing “puppy” and an uploaded video, Amplify video, Periscope, or Vine.
puppy filter:periscope	containing “puppy” and a Periscope video URL.
puppy filter:vine	containing “puppy” and a Vine.
puppy filter:images	containing “puppy” and links identified as photos, including third parties such as Instagram.
puppy filter:twimg	containing “puppy” and a pic.twitter.com link representing one or more photos.
hilarious filter:links	containing “hilarious” and linking to URL.
puppy url:amazon	containing “puppy” and a URL with the word “amazon” anywhere within it.
superhero since:2015-12-21	containing “superhero” and sent since date “2015-12-21” (year-month-day).
puppy until:2015-12-21	containing “puppy” and sent before the date “2015-12-21”.
[illegible]	[illegible]
flight :(	containing “flight” and with a negative attitude.
traffic ?	containing “traffic” and asking a question.

Figure 18: Standard Twitter search operators

Twitter search operators can be incorporated with other criteria to create more advanced search queries to find related tweets more precisely, the following are some advanced Twitter search query to start your search with.

1. The negation operator (-) is used to exclude specific keywords or phrases from search results. Example: virus –computer
2. To search for hashtags use the (#)operator followed by the search keyword. For example: #OSINT
3. To search for tweets sent up to a specific date, use the (until) operator. Here's an example: OSINT until:2019-11-30(this will return all tweets containing OSINT and sent until date November 30, 2019).
4. To search for tweets sent since a specific date, use the (since) operator followed by the date. Here's an example: OSINT since:2019-11-30 (this will return all tweets containing OSINT and sent since November 11, 2019).
5. Use the (images) keyword to return tweets that contain an image within it. Here's an example: OSINT Filter:images(this will return all tweets that contain the keyword OSINT and have an image embedded within them).
6. To return tweets with video embedded with them, use the (videos) keyword (similar to the images filter). Here's an example: OSINT Filter:videos
7. To search for video uploaded using the Twitter Periscope service, use the (Periscope) filter. Here's an example: OSINT filter:periscope (this will search for all tweets containing the OSINT keyword with a Periscope video URL).
8. To return tweets with either image or video, use the (media) operator. Here's an example: OSINT Filter:media
9. To return tweets that contain a link (URL) within them, use the (links) keyword. Here's an example: OSINT Filter:links
10. To return tweets that contain a link (URL) and hold a specific word within that URL, use the URL keyword. Here is an example: OSINT url:amazon this will return all tweets that containing OSINT and a URL with the word "amazon" anywhere within it (see Figure 19).

Figure 19: Search for specific keyword within tweets URL

11. To return tweets from verified users only (verified accounts have a blue check mark near their names) (see Figure 20), use the (Verified) operator. Here's an example: OSINT Filter:verified

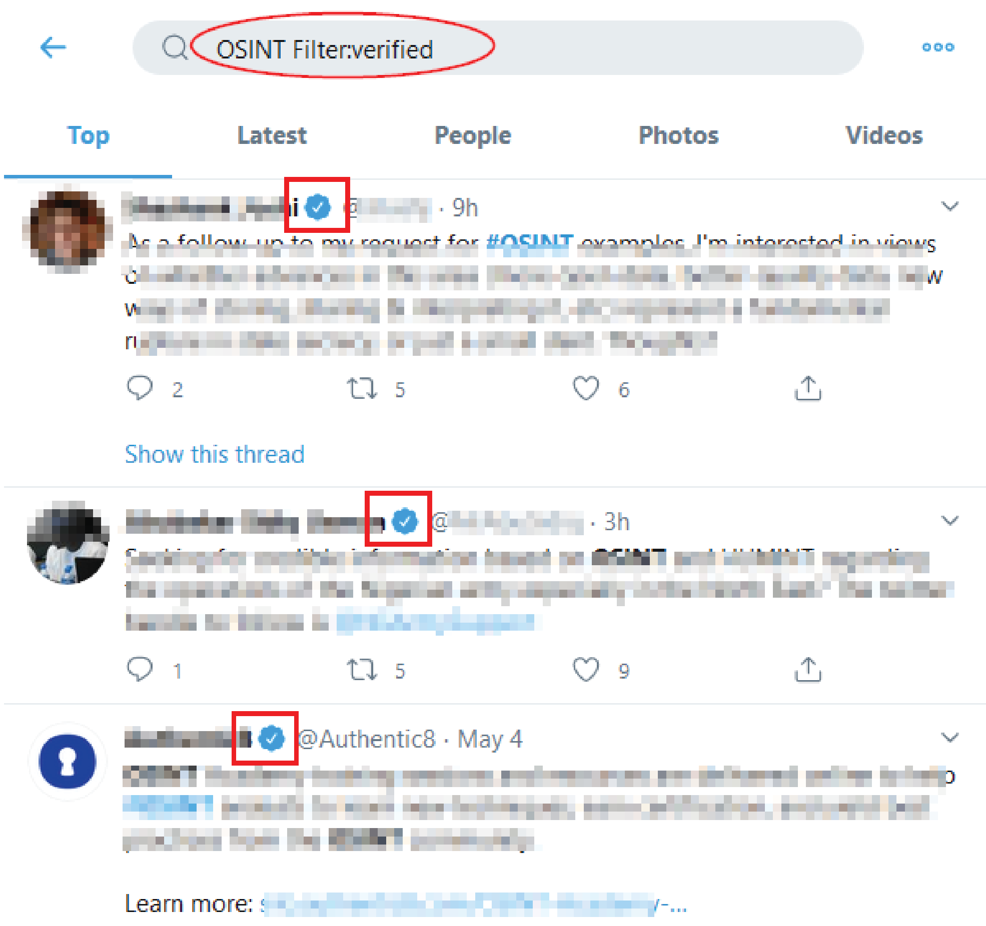


Figure 20: Return results from verified Twitter accounts only

12. Use the (min_retweets) operator followed by a number. Here's an example: OSINT min_retweets:50 (this will return all tweets containing the OSINT search keyword that have been retweeted at least 50 times)

13. Use (min_faves) followed by a number to return all tweets with NUMBER or more likes. Here's an example: OSINT min_faves:11 (this will return all tweets that have at least 11 or more likes and that contain the OSINT search keyword)

14. To limit Twitter returned results to a specific language, use the (lang) operator. Here's an example: OSINT lang:en (this will return all tweets containing OSINT in the English language only). To see a list of Twitter-supported language codes, go to https://developer.twitter.com/en/docs/twitter-for-websites/twitter-for-websites-supported-languages/overview

15. To search for tweets with a negative attitude use the following symbol :(For example: OSINT :(will return all tweets containing the keyword OSINT written in a negative attitude.

We can combine more multiple Twitter search operator to perform a more precise search. For example, type "OSINT" from:darknessgate -Filter:replies lang:en to get only the tweets containing the exact phrase OSINT from the user darknessgate that are not replies to other users and in the English language only.

Twitter Advanced Search Feature can also be used as follows:

Link for Twitter Advanced Searc*h* - https://twitter.com/search-advanced?lang=en

Note: Twitter account is not needed and there are many search options.

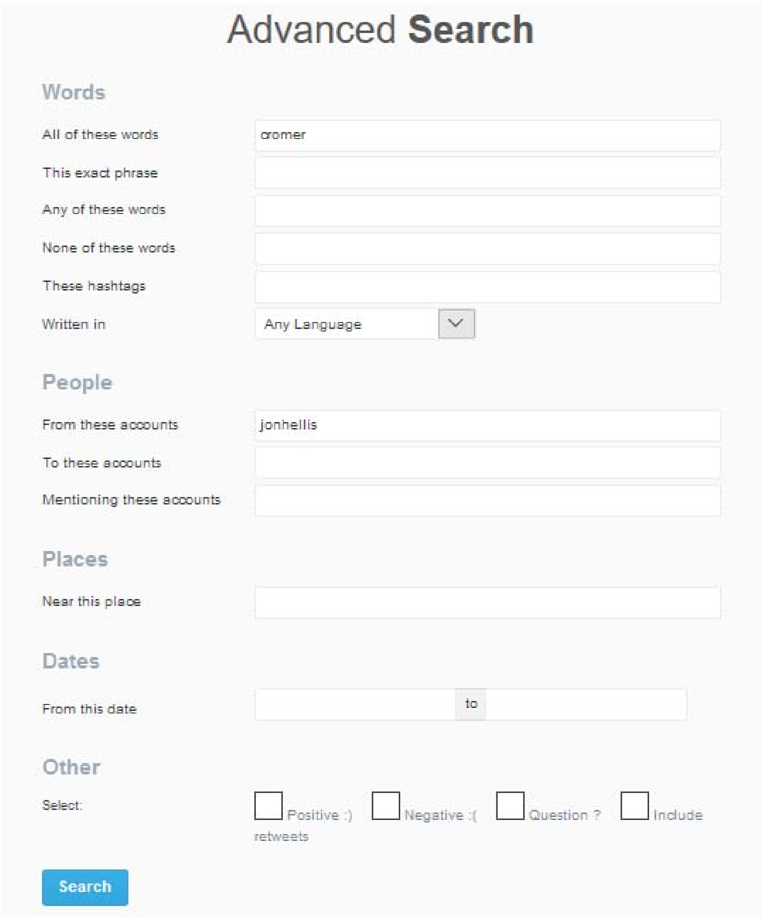


Figure 21: Twitter Advanced Search

Identify the Account ID of the Twitter User

It's important to identify the account ID of the user you are interested in. If they change their user handle, you may struggle to find their account without their account ID. User handles can be changed as often as the user wishes

Use tweeterid.com to convert a Twitter username to an account ID and vice versa (as shown in Figure 22).

Figure 22: Identify the Account ID of the Twitter User (1)

Figure 23: Identify the Account ID of the Twitter User (2)

Hashtag and Keyword Search

The Twitter website allows you to enter search terms, including user handles, #hashtags and keywords, either with an account or without an account:

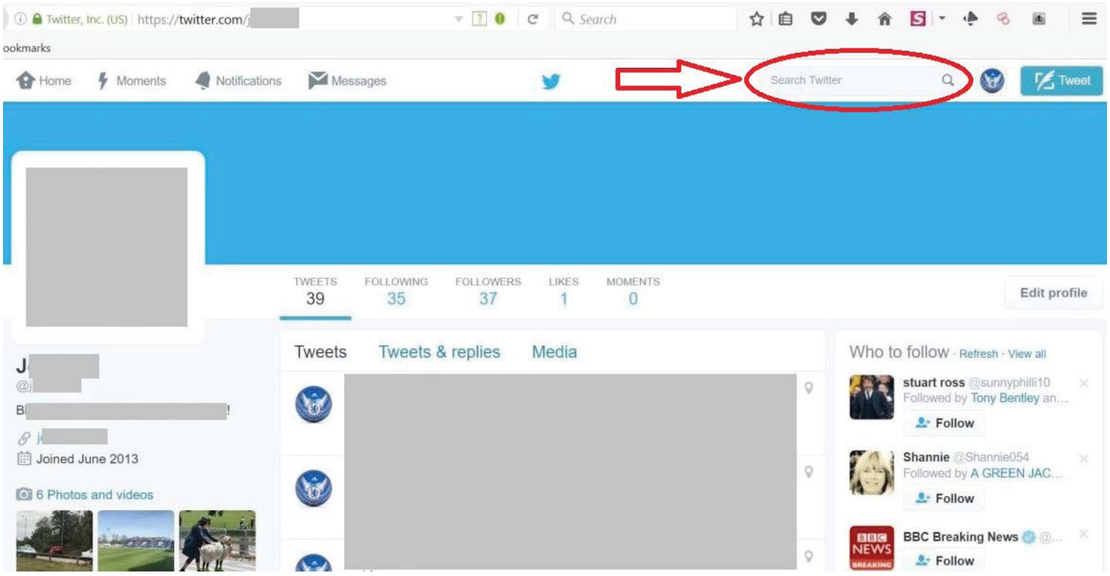


Figure *24*: Twitter Search with Account Login (1)

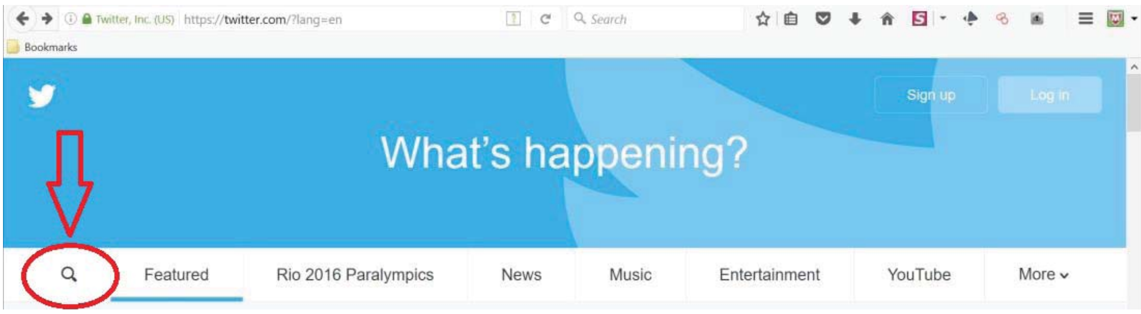


Figure 25: Twitter Search with Account Login (2)

View All Tweets From any user on a Single Page:

a. All My Tweets (allmytweets.net)

Step 1: Visit to allmytweets.net and Sign-in to Twitter.

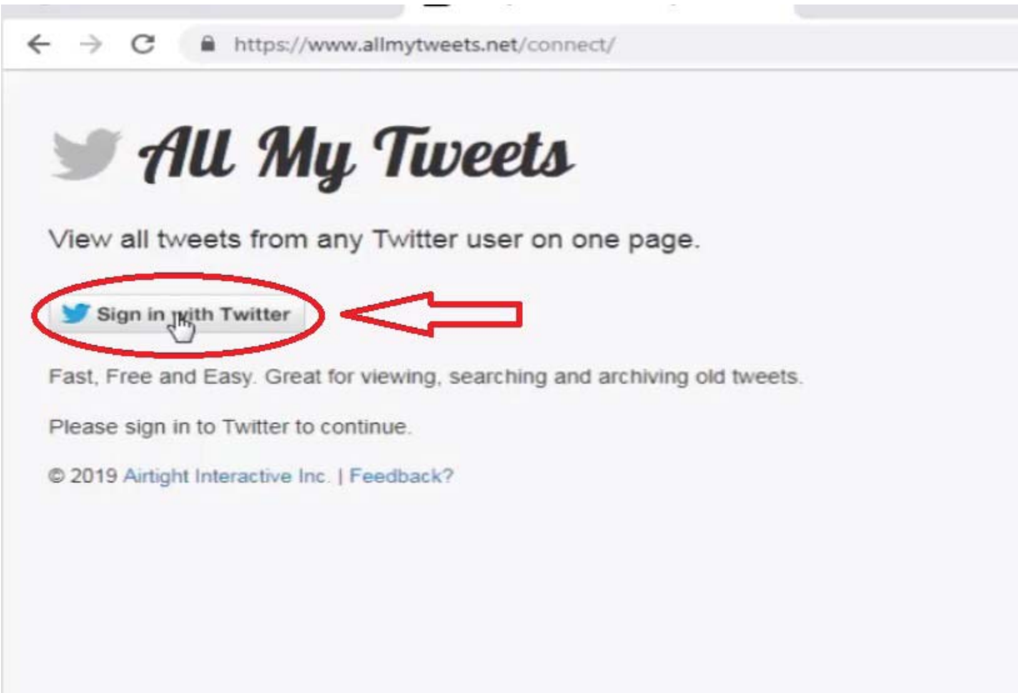


Figure 26: All My Tweets (allmytweets.net)

Step 2: Authorize the All My Tweets to use your account.

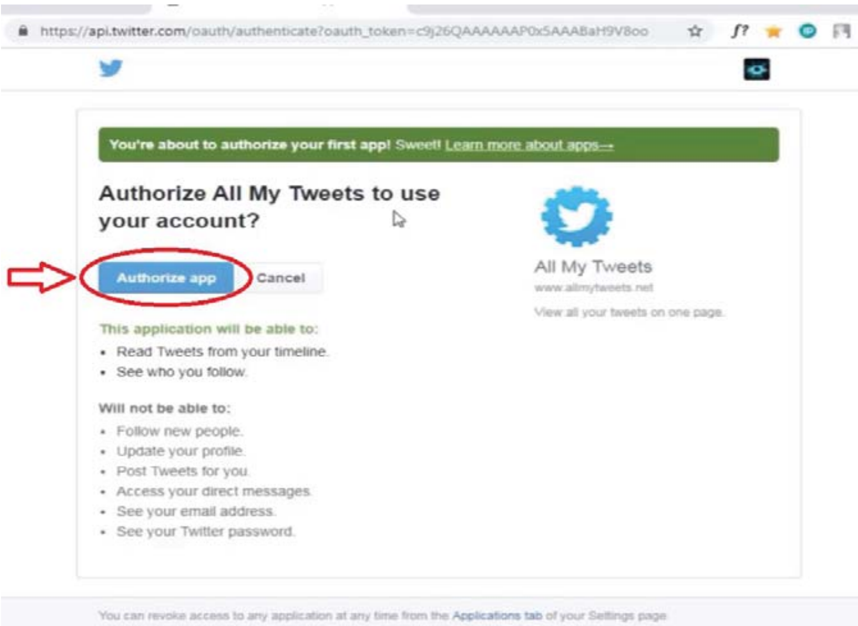


Figure 27: Authorize the All My Tweets

Step 3: Enter the Twitter user-name of any individual and click on GET TWEETS to get all his/her Tweets.

Figure 28: Enter the Twitter username

Step 4: All the Tweets posted by the Twitter User is loaded.

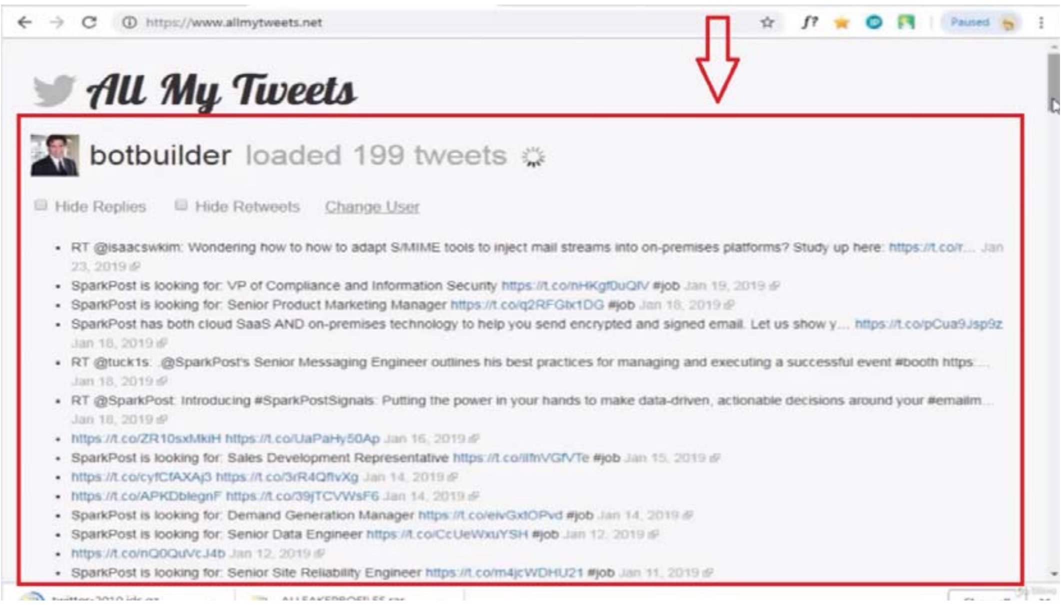


Figure 29: All the Tweets posted by the Twitter User

Discover and Analyze Fake Followers on Twitter

Botometer checks the activity of a Twitter account and gives it a score.

Step 1: Visit to Botometer (https://botometer.osome.iu.edu/) and Login to Twitter Account and Authorize the Botometer. Now enter the Twitter Handle of the Individual for analyzing whether his/her account, friends or followers are real or fake.

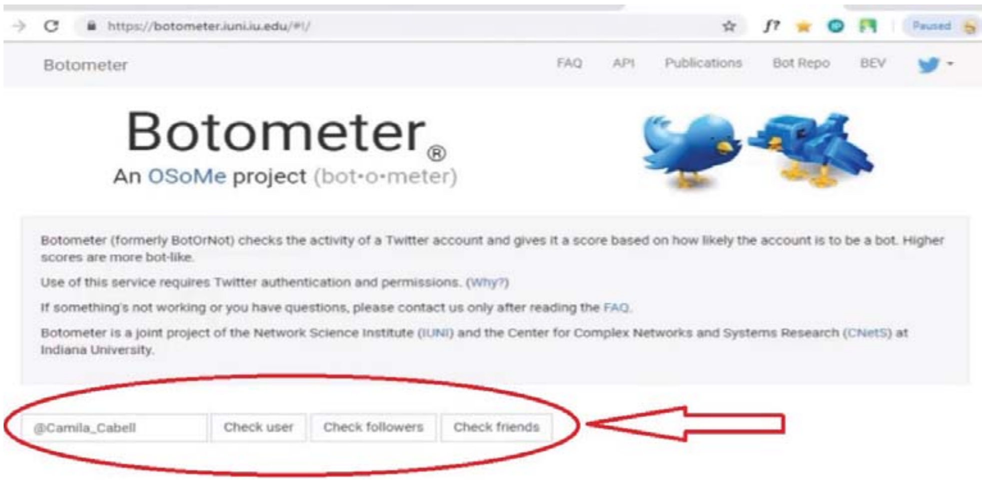


Figure 30: Botometer

Step 2: Now click on Check User, Followers and Friends of the Twitter User to analyze the scores, whether the account and followers are is real or fake. Higher scores mean more bot-like activity.

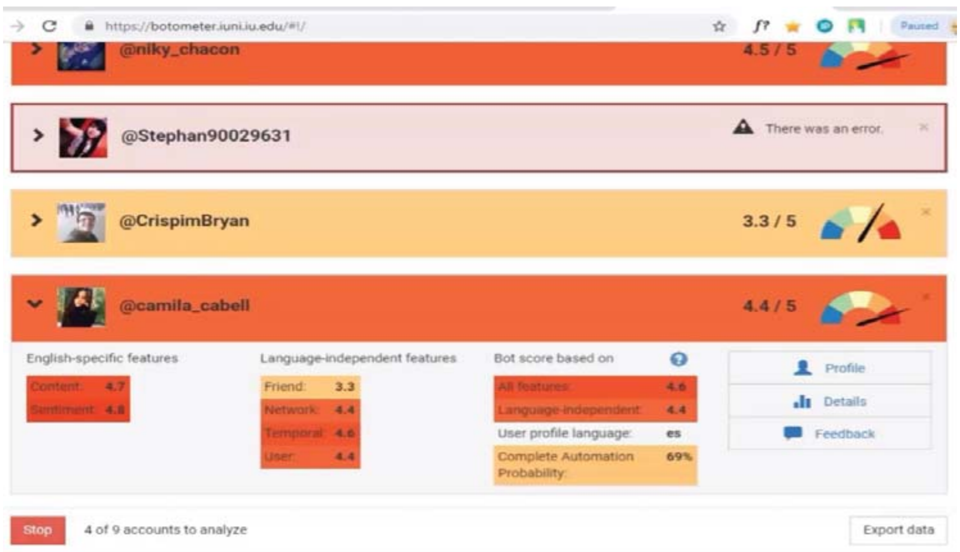


Figure 31: Botometer Results

Online Twitter Analysis Services

The following are online services to help you find information on Twitter:

1. All My Tweets (https://www.allmytweets.net): View all public tweets posted by any Twitter account on one page.
2. Trendsmap (https://www.trendsmap.com): This shows you the most popular trends, hashtags, and keywords on Twitter from anywhere around the world.
3. First Tweet (http://ctrlq.org/first): Find the first tweet of any search keyword or link.
4. Social Bearing (https://socialbearing.com/search/followers): Analyze Twitter followers of any particular account (a maximum of 10,000 followers can be loaded).
5. Spoonbill (https://spoonbill.io): Monitor profile changes from the people you follow on Twitter.

Figure 32: Spoonbill show updated/deleted Twitter profiles of the people you follow

3.2 Tracking Social Media Users across Multiple Platforms

Most internet users have more than one social media account, according to statists [1], average number of social media accounts per internet user was 8.5 in 2018. This information is useful and should be present in our mind when searching social media sites, for instance, many people prefer to use the same username in multiple social media platforms. If we know the username of one social media account of the target, we can search to see where else this username is used on other social media platforms.

You can check specific usernames to see where they are being used (e.g., social media Sites) or to know whether a particular username really exists using any of the following free online services.

1. Check User Name (http://checkusernames.com): Check the use of a specific username on 160 social networks. This is useful to discover target social media accounts to see if they are using the same username on multiple platforms.
2. Namechk (https://namechk.com): Check to see whether a specified username is used for major domain names and social media sites (see Figure 33).

[Note: Please verify the usernames during the Investigation, as sometimes these OSINT Services may show unverified results across various platforms]

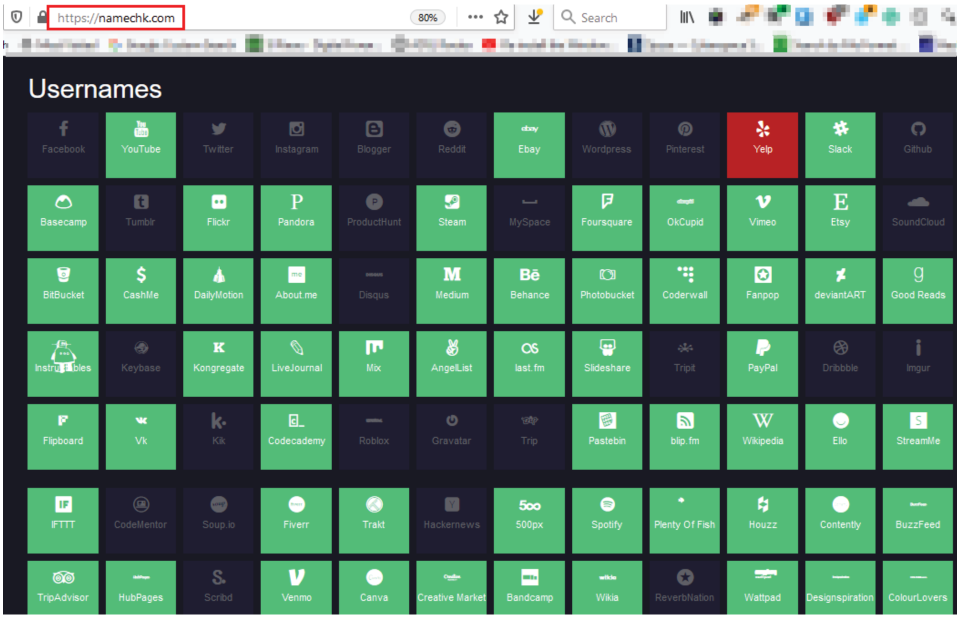


Figure 33: Using namechk to search for similar usernames across different social media platforms

3. Namecheckr (https://www.namecheckr.com): Check a domain and social username availability across multiple networks.

4. User Search (https://www.usersearch.org): Scan 45 popular social media websites.

5. UserRecon (https://github.com/thelinuxchoice/userrecon): A Linux tool to find usernames across over 75 social networks.

6. Sherlock (https://sherlock-project.github.io): Sherlock Project, can be used to find usernames across many social networks. It requires Python 3.6 or higher and works on MacOS, Linux and Windows.

Social Media Psychological Analysis

The psychological status of the person posting the contents on their profile can also give important information, even more than the content itself (in some cases). For instance, the true identity of an anonymous Twitter account can be revealed by performing linguistic analysis of the target account.

In addition, people can be tracked online by examining the way they use language when they chat or when they broadcast their thoughts online (for example, the way a target uses capitalization, omits or includes words, and pronounces some words). The advances in artificial intelligence systems will make analyzing social media accounts more effective and will help examiners uncover the true identity of anonymous social media accounts.

This online service (https://tone-analyzer-demo.mybluemix.net) offers free linguistic analysis to detect human feelings found in text such as tweets, emails, and Facebook messages (see Figure 34).

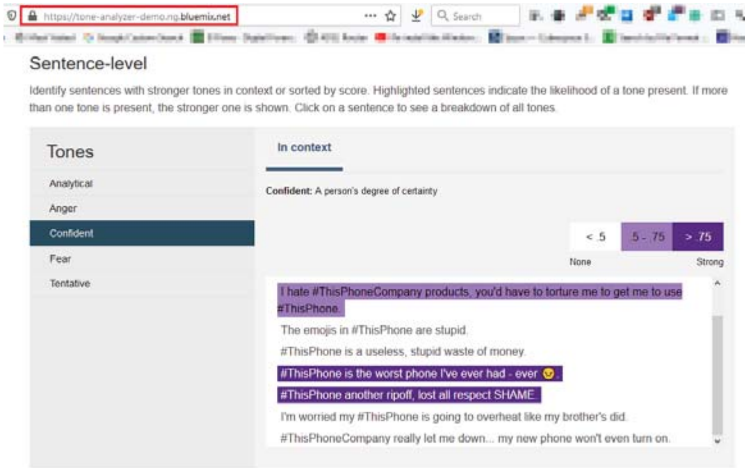


Figure 34: Using tone-analyzer from IBM to detect joy, fear, sadness, anger, analytical, confident and tentative tones found in text

socid_extractor

socid-extractor is a Python script that allows you to extract information about a user from profile webpages / API responses and save it in machine-readable format. Supported websites include:

Google (all documents pages, maps contributions), cookies required

Yandex (disk, albums, znatoki, music, realty, collections), cookies required to prevent captcha blocks

Facebook (user & group pages)

Instagram

Reddit

Medium

Flickr

Tumblr

GitHub

VK (user page)

OK (user page)

Mail.ru (my.mail.ru user

4. Legal Validity of Social Media Surveillance

In today's digital age, it is rare to see an Internet user who does not have at least one account on one or more social media site. People use social media services to post all types of contents online such as photos, videos, text messages, and geolocation data. They also mention their education, employment history, and the addresses where they live. Personal information such as social connections, places visited, habits, likes and dislikes, family members, spouse, and more can all be found easily. Although social networking sites allow their users to tighten their privacy controls to prevent others from seeing posted content, few people care about such issues and post many of their activities especially text posts and check-ins in public status. This makes a large volume of accessible data about citizen's lives readily available to different kinds of online investigations, and this is the essence of "Social Intelligence" (SOCINT).

Is collecting intelligence from social media platforms is considered legal?

> "There is a debate between privacy advocates and OSINT researchers about whether the information available on social media sites is OSINT. Although the majority of social media sites require their users to register before accessing site contents in full, many surveys show that social media users expect to have some form of privacy for their online activities (even when posting content with public access). However, OSINT experts generally consider information shared on social media sites as belonging to the OSINT domain because it is public information shared on public online platforms and thus it can be exploited for intelligence purposes."
>
> *Source: Hassan, Nihad. "Chapter 5." Open-Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence.*

Using the information gathered from social media sites in a legal case is generally allowed under these two conditions:

1. When acquiring permission from a court to gather information about a specific user, a court order is sent to the intended social media site to hand the information to authorities officially.

2. If the information is available publicly (e.g., public posts, images, or videos), then law enforcement can acquire it without a permit, which is the essence of the OSINT gathering concept.

Private OSINT gatherers should have a legal basis when collecting personal information about targets, data protection laws impose restrictions on the way online investigators collect, process, and retain the personal information of citizens. While discussing the legal issues surrounding OSINT, make sure to have a legal intent when collecting personal information from public sources and make sure to destroy this information as soon as you finish your investigation without any delay.

Finally, indiscriminate monitoring of the general population's online communications even when those communications are nominally public runs afoul of due process standards preserved in democratic constitutions and international human rights law.

Figure 35: Legal Validity of Social Media Surveillance

4.1 Social Media Evidence and Accuracy

Surveillance technologies can grant an air of objectivity to assessments that are not necessarily indicative of realities on the ground, due to outdated, inaccurate, or incomplete information. For example, it is not always possible to trace a social media posting back to an individual, given the existence of fake and shared online accounts. Moreover, ephemeral details become permanent records that individuals are not always able to redress in retrospect. Inaccurate or incomplete information poses significant problems for surveillance technologies. These concerns are also relevant where social media surveillance is beginning to inform predictive policing tools. With careful review, machine learning techniques applied to social media could easily reinforce existing patterns of enforcement, which partly reflect an unequal focus on people of colour.

4.2 Legal Questions for Social Media Surveillance

Social media surveillance of law enforcement raises several legal questions. For example, large-scale law enforcement surveillance of social media during protests raises a concern of scale and proportionality.

The use of a person's social media network as evidence of a crime raises its own set of legal concerns. What type of social media activity is likely to constitute sufficient evidence of criminal activity? For prosecutors, what type of social media activity should be allowed as evidence when a person is charged under conspiracy statutes? Are there certain social media attributes like a person's social network that should not be considered as evidence? Impersonation online raises its own set of legal considerations. Importantly, there seems to be an emergent fault line between the creation of an undercover, fake profile compared to the impersonation of an actual person online.

4.3 Critical Questions

Law enforcement use of social media is a powerful new investigative tool. Its growing use opens new questions that will need clear answers to ensure that civil rights are protected as law enforcement moves increasingly online. Specifically:

1. Should certain types of online activity be off-limits to law enforcement intelligence gathering? For example, what limits, if any, should apply to law enforcement surveillance of community organizing activity, including public protest messages on social media?

2. Are new rules needed to govern police impersonation of real people on social media?

3. How can policy and technology be used to ensure that social media surveillance is used equitably, and is not unduly focused on certain communities or groups?

4. Might new forms of training, or other interventions, be necessary to equip police to accurately interpret the meaning of fast-changing and sometimes figurative modes of expression that young people may use online?

5. When and how should social media companies work with law enforcement? Should users –as a group or individually – be notified of such investigations?

6. Are specific protections needed to guarantee that social media is not taken out of context or used to suggest actions or relationships that might be performative?

7. What training might be necessary for judges, prosecutors, and defence attorneys to responsibly use social media data in cases?

5. Conclusions

Social media intelligence (SOCMINT) is a sub-branch of Open-Source Intelligence (OSINT), it refers to the information collected from social media websites. The data available on social media sites can be either open to the public (e.g., Public posts on Facebook or LinkedIn) or private. Private information such as contents shared with a friend's circle - cannot be accessed without proper permission from the creator.

The goal of this manual is to understand various social media and social networking system like Facebook, Twitter, LinkedIn, WhatsApp etc. Cyber criminals actively use web based social media like Facebook, Twitter, Instagram, news websites to share information, ideas, personal messages, videos, and to spread rumors, fake news etc. Moreover, cyber criminals carry out illegal activities such as drugs business, data selling, and sex trading etc. via social media. They use social media as their marketing and communication platform.

Cyber criminals use these platforms to hide their real identities. This manual explains the major features of popular social media platform covering evidences aspect for the purpose of cybercrime investigation. This manual covers various tools and techniques for gathering intelligence over popular social media platforms and track and trace various criminal activities.

References

1. Author Book: Open-Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence, Publisher: Apress; 1 edition, ISBN 978-1-4842-3212-5 By Nihad A. Hassan
2. www.statista.com/statistics/788084/number-of-social-media-accounts
3. www.help.twitter.com/en/using-twitter/supported-mobile-carriers
4. www.en.wikipedia.org/wiki
5. www.support.signal.org
6. www.wjn.sa/digital_forensics
7. www.blog.oxygen-forensic.com/115-2

officialBPRDIndia

BPRDIndia

Bureau of Police Research & Development India

bprdIndia

www.bprd.nic.in

Cyberdost

www.cybercrime.gov.in

Indian Cyber Crime Coordination Centre

NATIONAL CYBER CRIME RESEARCH & INNOVATION CENTRE (NCR&IC)

BUREAU OF POLICE RESEARCH AND DEVELOPMENT

Ministry of Home Affairs, Government of India

NH-8, Mahipalpur, New Delhi-110037