

Open-Source Intelligence (OSINT)

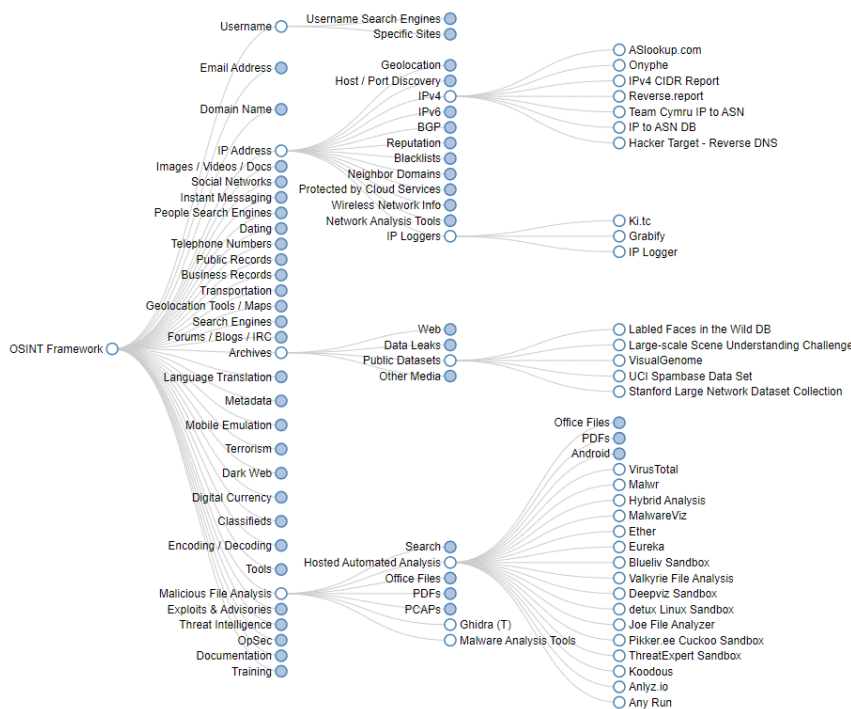
- ❖ OSINT is an abbreviation for "Open Source Intelligence." In order to gather information, facts, and intelligence on a specific topic, organization, person, or event, it is a process that involves gathering and evaluating publicly available information from a range of sources. Governmental organizations, law enforcement, corporate security, and investigators frequently employ OSINT to assist their deliberations and inquiries.

Publicly Available Sources:

OSINT relies on data that can be accessed by anybody without a password or special approval. Websites, social media, news articles, academic journals, official reports, public documents, and more are some examples of these sources.

- **Information Collection:** OSINT practitioners collect a wide range of information, such as data on individuals, organizations, events, technologies, and trends. This information can be textual, visual, or even audio-based.

OSINT Framework



OSINT can be conducted using a variety of tools and resources, including:

- **Search engines:** Search engines are the most common tool used for OSINT, as they can be used to find a wide range of information, including news articles, social media posts, and government documents.
- **Social media:** Social media platforms such as Twitter, Facebook, and LinkedIn can be a valuable source of information about people, organizations, and events.

- **Public records:** Public records databases contain information about people, businesses, and property.
- **Satellite imagery:** Satellite imagery can be used to track the movement of people and vehicles, and to identify changes in the landscape.
- **Commercial databases:** Commercial databases contain information about a wide range of topics, including businesses, people, and products.

Here's a list of the types of information you can potentially collect, as you requested:

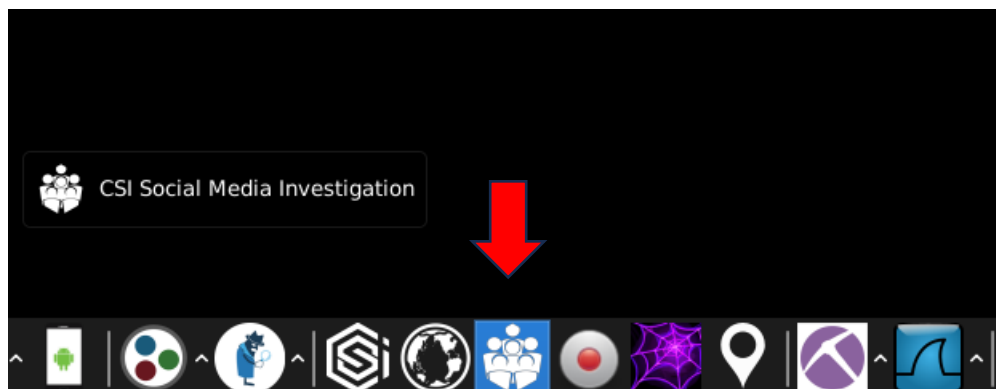
- **Username:** Information related to usernames used on websites, forums, social media platforms, or any online services.
- **Domains:** Details about domains, including domain names, registrant information, IP addresses, and DNS records.
- **Email Addresses:** Information about email addresses, such as the email owner's name, associated domains, and contact details.
- **Profiles:** Data from online profiles, including social media profiles, professional networking profiles, and forum or website user profiles. This might include names, photos, biographical information, and posts.
- **Phone Numbers:** Publicly available phone numbers associated with individuals or organizations.
- **IP Addresses:** Information about IP addresses, including geolocation, hosting providers, and associated websites or services.
- **Physical Addresses:** Information about physical locations, which can include street addresses, city, state, and country.
- **Company Information:** Details about businesses and organizations, such as names, addresses, industry type, and leadership personnel.
- **Online Identities:** Information about online aliases or pseudonyms used by individuals on various platforms.
- **Comments and Posts:** Data from comments, posts, reviews, or discussions on websites, blogs, forums, and social media platforms.
- **Biographical Information:** Personal information about individuals, including date of birth, education, employment history, and hobbies.
- **Photos and Images:** Visual content, such as profile pictures, photographs, or images associated with individuals.

- **Social Media URLs:** Links to social media profiles or pages associated with individuals or organizations.
- **Online Activity:** Records of an individual's online activity, such as likes, shares, and comments on social media, or participation in online communities.
- **Affiliations:** Associations with organizations, groups, or communities that an individual is a part of.
- **Document Metadata:** Information extracted from document metadata, which can reveal details about the author, creation date, and document history.

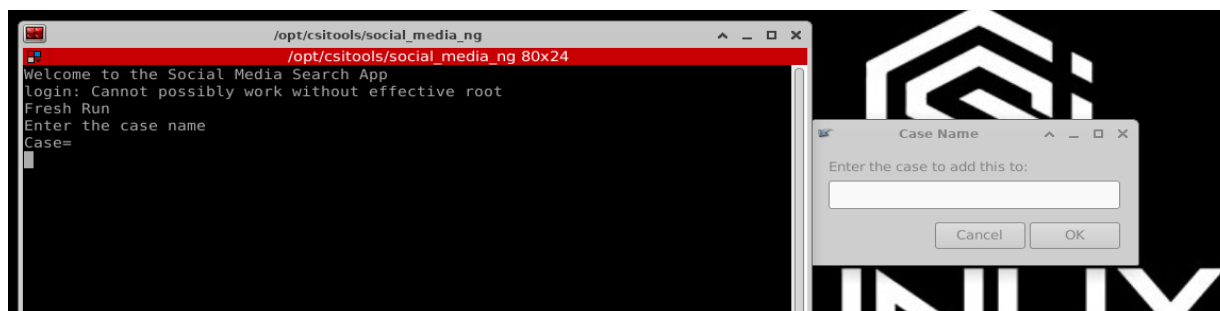
CSI-LINUX

A Linux distribution created primarily for digital forensics and cyber investigations is called CSI Linux. It is built on Ubuntu LTS and comes with several tools and capabilities for gathering, examining, and reporting on digital evidence already installed. CSI Linux is offered as a pre-built workstation, a bootable triage disk image, and a virtual machine appliance.

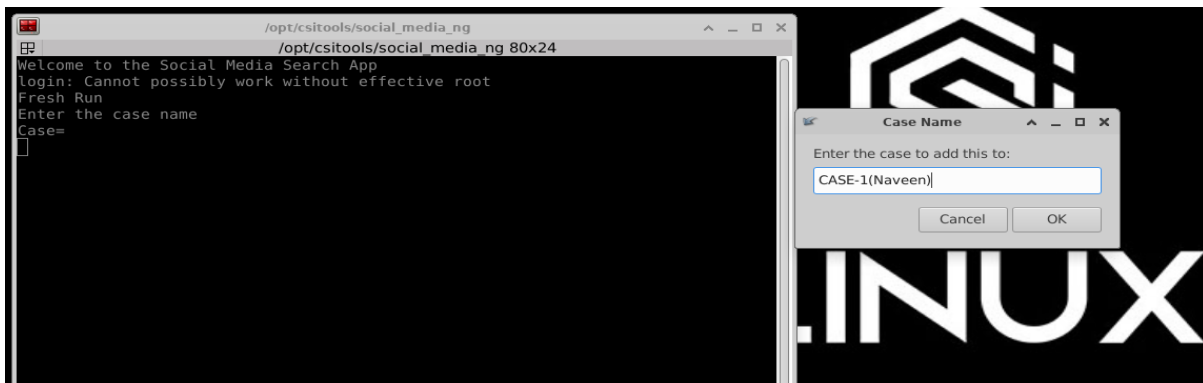
- Let's investigate an particular person
 1. Select the Social Media Investigation that can provide details regarding the person social platforms



- Record the data to an particular Case that entire data for the particular case will be saved in the same file



Provide any name as your wish



2. As we can see that there are many options to search on the data we provide. Here we will be selecting the Username Search.



3. Provide the Username to search in the public records linked to the Username.



- After providing the Username then the search engine will be search all the account which are linked to the particular Username.

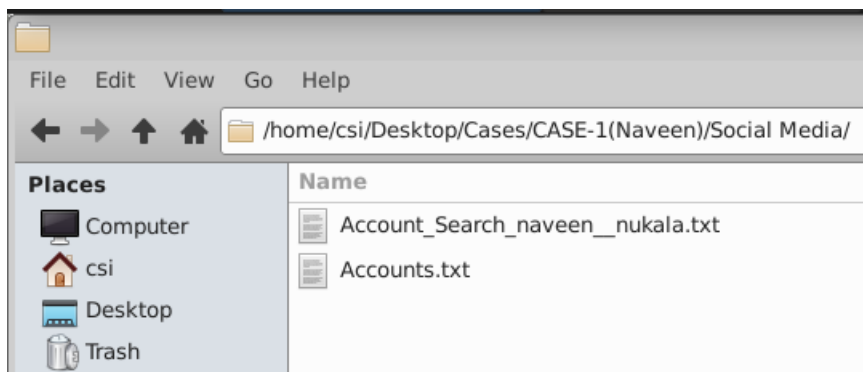
```
..... CSI Linux Social Media Username Search .....

:: Disclaimer: Developers assume no liability and are not ::
:: responsible for any misuse or damage caused by user... ::
:: Verify findings. There may be false positives/negatives. ::

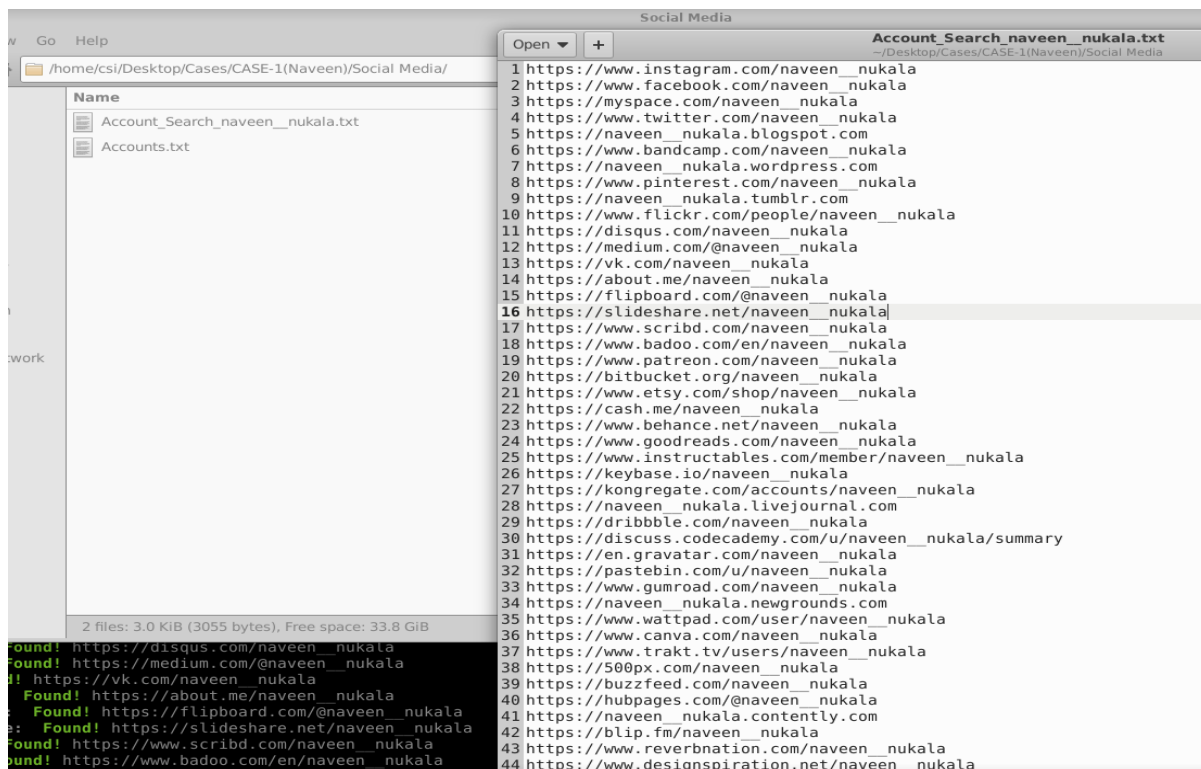
Searching for the Username: naveen__nukala
Saving to the case: CASE-1(Naveen)

[*] Removing previous file: /home/csi/Cases/CASE-1(Naveen)/Social Media/Account_Search_naveen__nukala.txt
[*] Checking username naveen__nukala on:
[+] INSTAGRAM: Found! https://www.instagram.com/naveen__nukala
[+] Facebook: Found! https://www.facebook.com/naveen__nukala
[+] MySpace: Found! https://myspace.com/naveen__nukala
[+] Twitter: Found! https://www.twitter.com/naveen__nukala
[+] Blogspot: Found! https://naveen__nukala.blogspot.com
[+] Bandcamp: Found! https://www.bandcamp.com/naveen__nukala
[+] Redit: Not Found!
[+] Wordpress: Found! https://naveen__nukala.wordpress.com
[+] Pintrest: Found! https://www.pinterest.com/naveen__nukala
[+] Tumblr: Found! https://naveen__nukala.tumblr.com
[+] Flickr: Found! https://www.flickr.com/people/naveen__nukala
[+] Disqus: Found! https://disqus.com/naveen__nukala
[+] Medium: Found! https://medium.com/@naveen__nukala
[+] VK: Found! https://vk.com/naveen__nukala
[+] About.Me: Found! https://about.me/naveen__nukala
[+] Flipboard: Found! https://flipboard.com/@naveen__nukala
[+] SlideShare: Found! https://slideshare.net/naveen__nukala
[+] Scribd: Found! https://www.scribd.com/naveen__nukala
[+] Badoo: Found! https://www.badoo.com/en/naveen__nukala
[+] Patreon: Found! https://www.patreon.com/naveen__nukala
[+] BitBucket: Found! https://bitbucket.org/naveen__nukala
[+] Etsy: Found! https://www.etsy.com/shop/naveen__nukala
[+] Cash.Me: Found! https://cash.me/naveen__nukala
[+] Behance: 
```

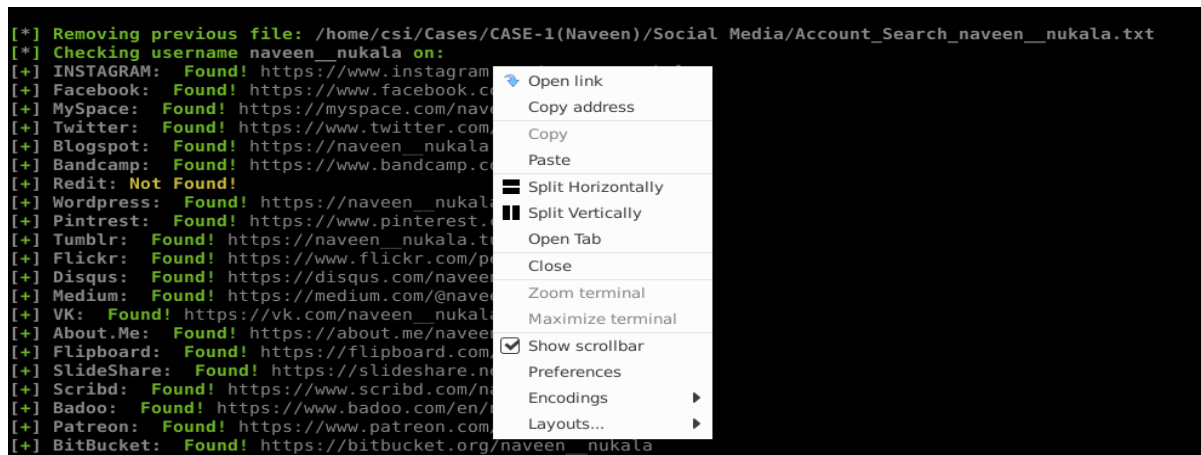
- As we discussed the data related to the particular case will be saved in same file



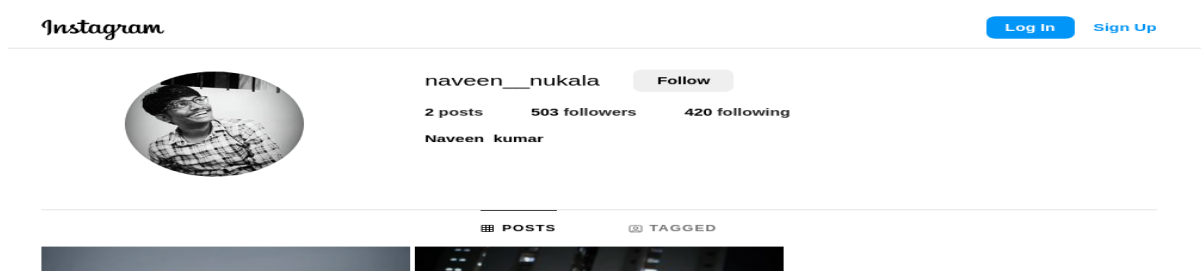
6. The links which are linked to the Username will be saved into the txt file in the Case folder



➤ Select the URL to open the account associated with the username.



➤ Account linked to the Username(Instagram)



- Little Brother is an another tool.

```

      _____
     /         \
    /             \
   /               \
  /                 \
 /                   \
/                     \
(                       )
 \                     /
  \                   /
   \                 /
    \               /
     \             /
      \           /
       \         /
        \       /
         \     /
          \___/

Time:      [ 2023-10-10 | 00:05:15 ]
Author:    [ Lulz3xploit ]
Version:   [ 6.0.2 ]
Pays:      [ India | IN ]
Database:  [ 0 | 4.096 Ko ]

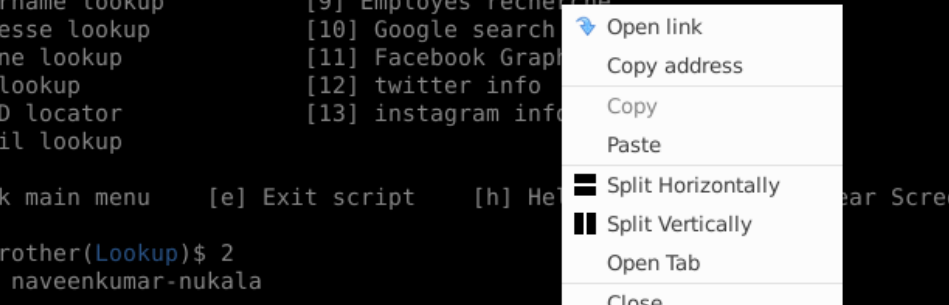
U MAD BRO?


[1] Personne lookup      [8] Mail tracer
[2] Username lookup     [9] Employés recherche
[3] Adresse lookup      [10] Google search
[4] Phone lookup        [11] Facebook GraphSearch
[5] IP lookup           [12] twitter info
[6] SSID locator        [13] instagram info
[7] Email lookup


[b] back main menu      [e] Exit script      [h] Help Message      [c] Clear Screen

LittleBrother(Lookup)$ S
```

- Select the lookup and select the category to get the info



The screenshot shows a terminal window with a list of lookup options on the left and a context menu on the right. The terminal text is as follows:

```
[1] Personne lookup      [8] Mail tracer
[2] Username lookup      [9] Employés recherche
[3] Adresse lookup       [10] Google search
[4] Phone lookup         [11] Facebook Graph
[5] IP lookup            [12] twitter info
[6] SSID locator         [13] instagram info
[7] Email lookup

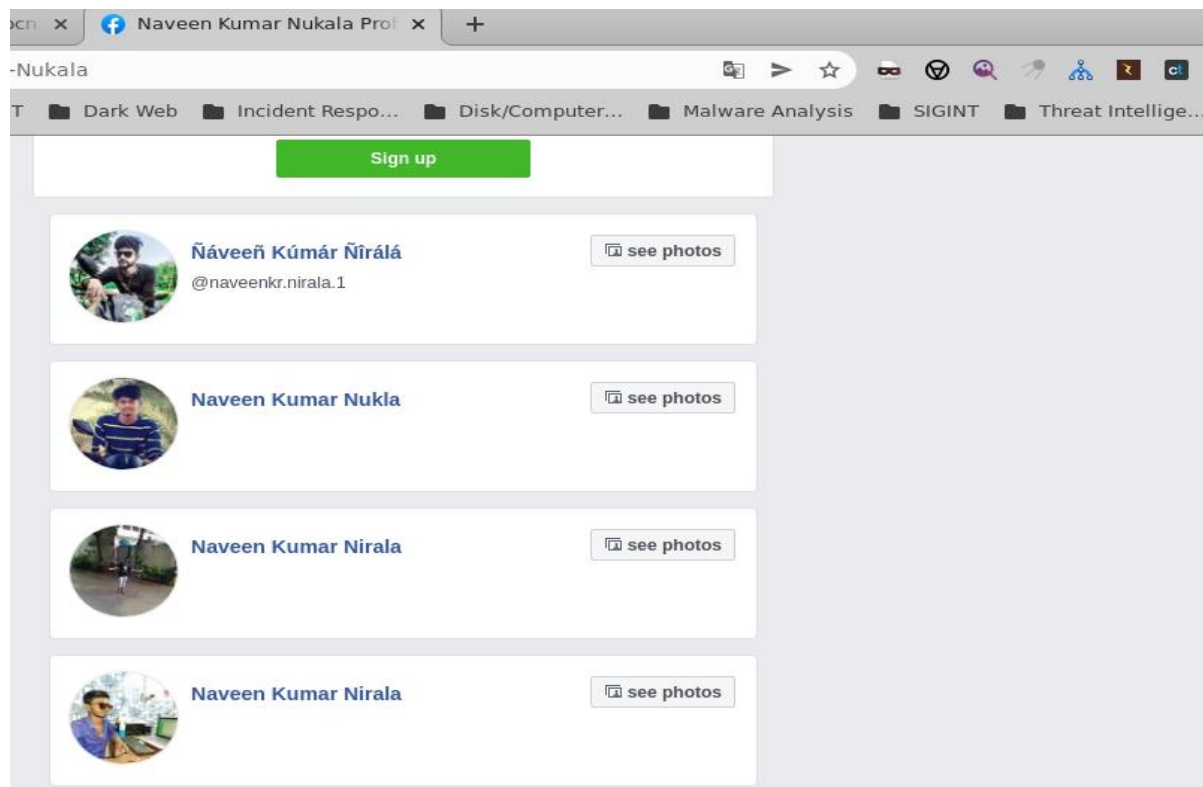
[b] back main menu      [e] Exit script      [h] Help
LittleBrother(Lookup)$ 2
Pseudo: naveenkumar-nukala

[*] Recherche 'naveenkumar-nukala'...
[++] Possible connection: https://www.facebook.com/nukala.n.kumar/
[++] Possible connection: https://m.facebook.com/nukala.n.kumar/?locale=hi_IN
[++] Possible connection: /search?q=\intitle:%22nukala-06471525&num=100&sca_esv=2288&settings_location&continue=https://www.facebook.com/nukala-06471525
[++] Possible connection: https://accounts.google.com/gsi/auth?continue=https://www.facebook.com/nukala-06471525
[+] Possible connection: https://in.linkedin.com/company/nukala-06471525
[+] Possible connection: https://in.linkedin.com/company/nukala-51a13838
[+] Possible connection: https://hi-in.facebook.com/public/naveen-kumar-Nukala
[+] Possible connection: https://www.facebook.com/nukala.n.kumar/
```

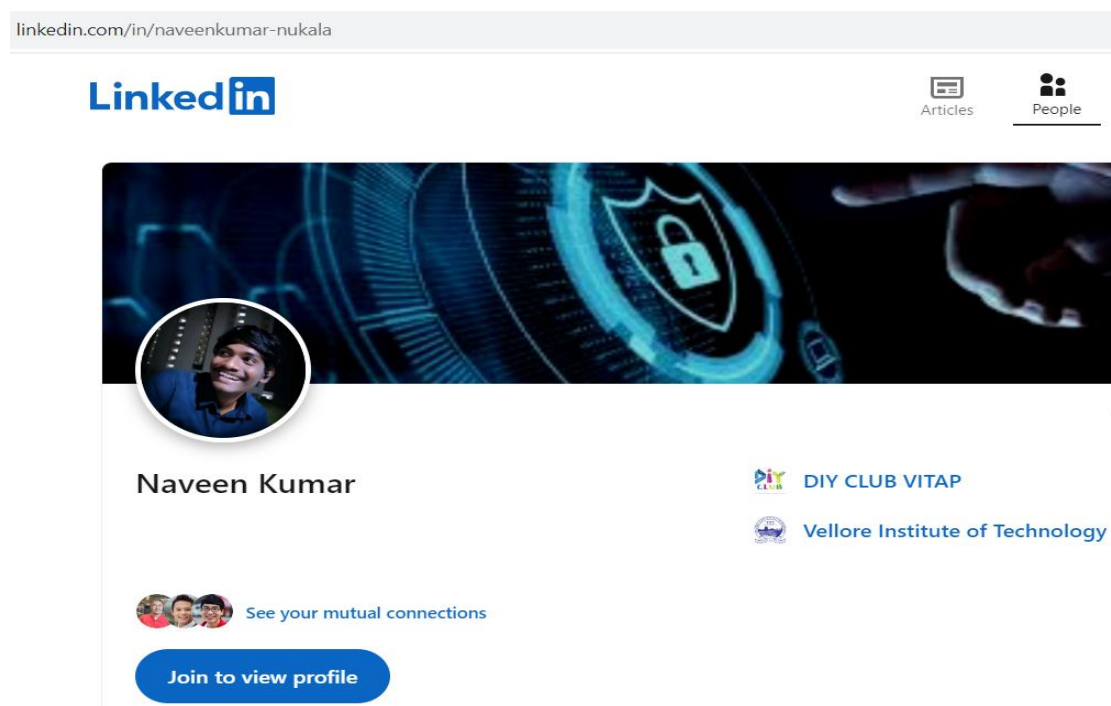
The context menu on the right contains the following options:

- Open link
- Copy address
- Copy
- Paste
- Split Horizontally
- Split Vertically
- Open Tab
- Close
- Zoom terminal
- Maximize terminal
- ☒ Show scrollbar
- Preferences
- Encodings
- Layouts...

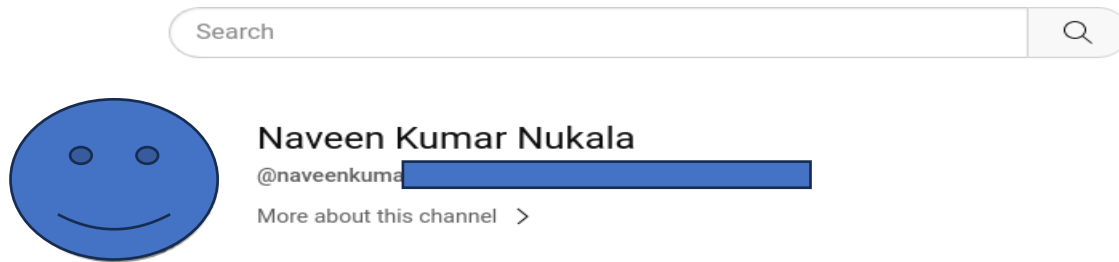
➤ Facebook accounts linked to provided Username



➤ Linked-In account



➤ Youtube Account linked to Username



➤ And some more public records as well

ANIMELASHREE SHA	Female	BC-B	ANDHRA PRADESH	0484234
ANKALLAGARI	Male	BC-A	ANDHRA PRADESH	0484234
BANDARU CHA	Male	OC	ANDHRA PRADESH	0484234
BANGI SUDHAN	Male	SC	ANDHRA PRADESH	0484234
BAJANTRI VEN	Male	BC-A	ANDHRA PRADESH	0484234
BHUPATHI VYS	Male	OC	ANDHRA PRADESH	0484234
BODHANAPU A	Male	BC-B	ANDHRA PRADESH	0484234
CHALLA VENK	Male	OC	ANDHRA PRADESH	0484234
CHIMMANI LAK	Male	BC-B	ANDHRA PRADESH	0484234
GOGULA SIREE	Female	BC-D	ANDHRA PRADESH	0484234
KALAMADI MA	Male	OC	ANDHRA PRADESH	0484234
KAMBALA SIVA	Male	BC-D	ANDHRA PRADESH	0484234
KACHANA LAK	Female	OC	ANDHRA PRADESH	0484234
KANCHANA MI	Male	BC-B	ANDHRA PRADESH	0484234
KATA VENKAT	Male	BC-B	ANDHRA PRADESH	0484234
KODURU DAM	Male	OC	ANDHRA PRADESH	0484234

Email ID	Program name	Unique Enrolment ID / College ID/ University enrolment number	Mobile Number
chennar	B.Tech-CE	168R1	798
shaiktha	B.Tech-CE	168R1	848
shaikjila	B.Tech-CE	168R1	798
j701484	B.Tech-CE	168R1	708
amarjuri	B.Tech-CE	168R1	958
royalpay	B.Tech-CE	168R1	918
tahasye	B.Tech-CE	178RS	968
chakrAN	B.Tech-CE	178RS	888
ali48649	B.Tech-CE	178RS	918
aneesab	B.Tech-CE	178RS	838
madhub	B.Tech-CE	178RS	948
irfanmu	B.Tech-CE	178RS	978
naveen	B.Tech-CE	178RS	898

```
Searching for the Username: 818
[*] Checking username 818 on:
[+] SmartBackgroundChecks: Found! https://www.smartbackgroundchecks.com/phone/818
[+] PeopleFinder: Found! https://www.peoplefinder.com/reverse-phone-search/818
[+] Zabasearch: Found! https://www.zabasearch.com/phone/818
[+] Intelius: Found! https://www.intelius.com/reverse-phone-lookup/818
[+] WhitePages: Found! https://www.whitepages.com/phone/818
Done.
Done
```

```
2023-10-10 00:53:49.469054 Starting search in different platform(s)... Relax!
Press <Ctrl + C> to stop...

2023-10-10 00:53:54.007815 Results obtained:
Sheet Name: Objects recovered (2023-10-10_0h53m).
+-----+-----+-----+
| com.i3visio.URI | com.i3visio.Platform |
+-----+-----+-----+
| http://www.infotelefonica.es/818 | Infotelefonica |
+-----+-----+-----+
```

➤ Here are Some OSNIT CHEATSHEET

Google Hacking

Google dorking, also known as **Google hacking**, can return information that is difficult to locate through simple search queries. Using this technique, information not intended for public access can be discovered.

The **Google Hacking Database (GHDB)** is an authoritative source for querying the ever-widening reach of the Google search engine. Its contents are search terms, which allow to find usernames, passwords, and even files containing sensitive information. The GHDB is located here: <https://www.exploit-db.com/google-hacking-database/>

Google and Bing Search Operators

Operator	Description
"Search Term"	Search for the exact phrase within " "
-	Remove pages that mention a given term from the search results
+	Force Google to return common words that might ordinarily be discarded
OR	Search for a given search term OR another term
site:	Search within a given domain
filetype:	Search for a certain file type
intitle:	Search for sites with the given word(s) in the page title
inurl:	Search for sites with the given word(s) in the URL
intext:	Search for sites with the given word(s) in the text of the page
inanchor:	Search for sites that have the given word(s) in links pointing to them
cache:	Show most recent cache of a webpage
IP:	Bing only: Finds results based on a given IP address
linkfromdomain:	Bing only: Search for links on the given domain

Additional Google Features

Search Tools: The "Tools" button present a new row of options, which allows narrowing down the search results. One of the most interesting options of this feature is "Custom Range", which can be used to search within a given time frame.

Google Images: The most powerful reverse image search service. <https://images.google.com/>

Searching for Archived Information

Google and Bing: both search engines offer a cached view of results

The Wayback Machine: <http://archive.org/web/>

Archive Today: <http://archive.is/>

Yandex

Yandex operates the largest search engine in Russia with about 65% market shares.

Yandex Search Operators

Example	Description
"I * music"	Find all results with any word where the asterisk (*) is located
Cheshire cat hatter Alice	Search for any word in query. This query works for Google as well
croquet +flamingo	This query would mandate that the page has the word flamingo, but not croquet
rhost:org.wikipedia.*	Reverse host search
mime:pdf	Search for specific file type
!Curiouser !and !curiouser	Search for multiple identical words
Twinkle twinkle little -star	Exclude "star" from search results
lang:en	Narrow search by language
date:200712*, date:20071215..20080101, date:>20091231	Narrow search by date or date range

Search Engines: Other Alternatives

carrot2.org: Carrot2 is a clustering search engine that groups search results into sets of topics

www.exalead.com/search: Exalead works well in finding documents that contain the search term

millionshort.com: Million Short allows removing results, which link to the one million most popular websites

globalfilesearch.com: the site claims to have indexed 243 terabytes of files stored on public FTP servers

Shodan - <https://www.shodan.io>

Shodan is a search engine for finding Internet-connected devices and device types. It allows searching for webcams, routers, IoT/SCADA devices, and more.

Shodan Filters

Filter	Description
city:	Search for results in a given city
country:	Search for results in a given country (2-letter code)
port:	Search for a specific port or ports
hostname:	Search for values that match the hostname
net:	Search a given IP or subnet (e.g.: 192.168.1.0/24)
product:	Search for the name of the software identified in the banner
version:	Search for the version of the product
os:	Search for a specific operating system name
title:	Search in the content scraped from the HTML tag
html:	Search in the full HTML contents of the returned page

References:

<https://osintframework.com/>

<https://csilinux.com/>

<https://medium.com/nerd-for-tech/csi-linux-a-new-linux-distribution-for-cyber-and-osint-investigation-3d9498fac6aa>

https://www.compass-security.com/fileadmin/Research/White_Papers/2017-01_osint_cheat_sheet.pdf