OSINT UDEMY zaidh sabih course Notes

Prepared by: [Your Name]

Date: April 04, 2025

What is OSINT

Open Source Intelligence (OSINT) ek process hai jismein publicly available sources se information collect ki jati hai. Ye sources kuch bhi ho sakte hain jaise news websites, social media, government reports, blogs, public records, ya koi bhi aisi cheez jo openly accessible ho. OSINT ka use intelligence gathering, research, ya investigation ke liye hota hai, aur ismein koi secret ya classified data involve nahi hota. Iska matlab hai ki ye legal aur ethical tareeke se kaam karta hai jab tak privacy laws ya regulations ka violation na ho.

Note: OSINT ki shuruaat mein pehle apne baare mein details find karna chahiye. Isse aapko confidence milega aur aap samajh paayenge ki OSINT tools aur techniques kaise kaam karte hain. Jab aap comfortable ho jayein, tab kisi aur par try karna better hota hai taaki aap real-world practice kar sakein.

Point To Note

OSINT ek powerful method hai jo publicly available data ko collect aur analyze karta hai bina kisi secret ya illegal sources ke. Ye beginners ke liye bhi easy hai – pehle apne aap par practice karo taaki confidence aaye, phir doosron par try karo. Iska basic idea ye hai ki openly available info se bhi kaafi kuch seekha aur samjha ja sakta hai, jab tak aap laws aur ethics ka dhyan rakhein.

OSINT Sources Example

Source Type	Example	Use
Social Media	X Posts	User Info
News Websites	BBC	Current Events
Public Records	Govt Reports	Legal Data

==========

Discovering Sensitive Info About People

Double quote –ye operator aapko wahi results dikhata hai jo exactly aapke search query se match karte hain jab aap double quotes ke andar query likhte hain. For example, agar aap Google search mein "Satyam Singh" (double quotes ke saath) search karte hain, to aapko sirf 3,550 results milenge, jabki bina double quotes ke 1,21,000 results aayenge. Ye operator results ko filter karta hai aur exact matches dikhata hai. You can add multiple words in double quotes to narrow down the result more – jaise "Satyam Singh" "Patna" – isse sirf wahi results aayenge jahan ye dono terms saath mein honge. Iska matlab hai ki aap specific info jaise kisi person ke location ya activity ko target kar sakte hain. Making notes to founded usernames, links, etc. is very important so for that:

- **Notion.com** – ye ek cloud-based notes keeper hai jahan aap apne OSINT findings jaise usernames, links, ya details ko organize kar sakte hain. Ye aapko ek jagah sab kuch manage karne ki flexibility deta hai.
- **Greenshot** – ye ek software hai screenshots lene ke liye, jo aapko proof ya evidence save karne mein madad karta hai. Iska use karke aap quickly screen capture kar sakte hain aur apne notes mein add kar sakte hain.

Notes:

1. When you right-click on a link aur "Copy URL" select karte hain, to aapko ek bada aur complicated URL milega. Ise clean karne ke liye **urlclean.com** pe jao, link paste karo, aur aapko exact aur chhota link milega jo readable aur manageable hota hai. Ye step time save karta hai aur links ko neat rakhta hai.

2. Whatever link you find for your target, keep it in notes – e.g., usernames, social media links, etc. Ye info aapke investigation ke liye valuable hoti hai aur future reference ke kaam aati hai. Har chhoti detail count karti hai OSINT mein.

3. In Google search, agar aap "Satyam Singh" search karte hain, to aapko ek result mil sakta hai jisme likha ho "Satyam Singh was selling sofa," lekin jab aap link kholte hain to kuch nahi milta kyunki website ne data remove kar diya. So one way to get the detail is to use the cache version of that website.

   - **Cache Version Kya Hai?** Google websites ke purane copies apne database mein save karta hai, jise cached version kehte hain. Ye old data recover karne mein help karta hai jab live website se info hata di jati hai.
   - **Kaise Karein?** Link copy karo, urlclean.com se clean karo, phir Google search bar mein type karo: **cache:cleaned-link** (e.g., `cache:https://ola.com`). Ise URL bar mein paste karne par aap website ka purana version dekh sakte hain aur missing details pa sakte hain. Isse aap deleted info bhi track kar sakte hain.

Tools for Sensitive Info Discovery

Tool Name	Purpose	Link
Notion	Notes Organization	https://notion.com
Greenshot	Screenshots	https://getgreenshot.org
URLClean	Link Cleaning	https://urlclean.com

Point To Note

Double quotes jaise Google search operators sensitive info ko pinpoint karne mein bahut kaam aate hain, aur multiple terms add karke aap results ko aur refine kar sakte hain. Notion aur Greenshot se aap apne findings ko organize aur visually save kar sakte hain. URL cleaning jaise urlclean.com se links ko simple rakha ja sakta hai, aur cache version ka use karke aap deleted data tak bhi pahunch sakte hain. Ye sab tools aur techniques milke OSINT ko ek systematic aur powerful process banate hain – bas har step ko carefully follow karo aur notes banate jao!

==========

Discovering Social Media Profiles/Accounts

Google search operators ka use karke social media profiles aur accounts discover karna OSINT ka ek important part hai. Ek useful operator hai **inurl:** – ye search engine ko bolta hai ki sirf un URLs mein search kare jahan specific keyword ho. For example, agar aapne apne target

ke URLs notes mein save kiye hain, to un URLs se username copy karo aur **inurl:username** search karo. Isse aap dekh sakte hain ki ye username aur kitne jagah registered hai. Jaise – agar username "satyam123" hai, to inurl:satyam123 se aapko pata chal sakta hai ki is username ke saath GitHub aur Facebook account bhi hai. Ye tareeka aapko target ke ek aur account tak le ja sakta hai.

Aur bhi operators hain jo kaam aate hain:

- **"OR" Operator:** Ye Google Dork hota hai jo ek search term ya uske equivalent term ko find karta hai. Note – OR hamesha capital letters mein likhna hai. Jaise – "Satyam Singh" OR "Satyam Kumar" – ye dono terms ke results dikhayega.
- **intitle:** Ye operator search results dikhata hai jahan search term page ke title mein hota hai. For example, intitle:"Satyam Singh" se aap un pages ko find kar sakte hain jinka title mein ye naam hai.
- **Asterisk (*):** Ye wildcard operator hai jo ek ya zyada words ke liye placeholder ka kaam karta hai. Ye middle names ya missing info find karne mein useful hai. Example – "Zaidh * Sabih" – isse results aayenge jaise "Zaidh Al Sabih" ya "Zaidh Abu Sabih".
- **Hyphen (-):** Ye operator kisi search term ko results se exclude karta hai. Example – "Saad Sarraj" -site:cybersudo.org – isse Saad Sarraj ke results mein cybersudo.org ke pages nahi aayenge. Ya phir "Saad Sarraj" -site:linkedin.com – LinkedIn ke results remove ho jayenge.
- **site:** Ye operator ek particular website ke andar search karta hai. Example – site:facebook.com "Rishi Kabra" – isse sirf facebook.com pe Rishi Kabra ke results dikhenge. Ye targeted search ke liye bahut helpful hai.

In sab operators ko combine karke aap social media profiles ko efficiently track kar sakte hain. Notes mein usernames aur links save karna na bhoolo taaki aapka data organized rahe.

Google Operators for Social Media Discovery

Operator	Purpose	Example
inurl:	Find Username in URLs	inurl:satyam123
site:	Search Specific Site	site:facebook.com "Rishi Kabra"
*	Wildcard for Missing Info	"Zaidh * Sabih"
-	Exclude Results	"Saad Sarraj" -site:linkedin.com

Point To Note

Social media profiles discover karne ke liye Google operators jaise inurl:, OR, intitle:, *, -, aur site: bahut powerful hain. Inurl: se username ke aur accounts mil sakte hain, jabki site: specific platforms pe focus karta hai. Wildcard (*) missing info fill karta hai, aur hyphen (-) unwanted results hata deta hai. Ye sab use karke aap apne target ke online presence ko step-by-step uncover kar sakte hain. Har finding ko notes mein save karo taaki investigation smooth aur systematic rahe!

==========

Discovering PDF Documents Associated with the Targets

FileType: – Ye ek Google search operator hai jo search engine ko bolta hai ki sirf specific file type ke documents hi dikhaye. Ye OSINT mein target se related PDFs find karne ke liye bahut useful hai. Supported file types mein PDF, DOC, XLS, PPT, etc. shamil hain. Example – **site:zsecurity.org filetype:pdf** – isse aapko zsecurity.org website pe available saare PDF documents milenge. Iska use karke aap target ke official reports, resumes, ya koi aur documents dhoondh sakte hain jo publicly available hain.

Agar aapko Google search se koi PDF milta hai, to uska **metadata** check karna zaroori hai.

- **Metadata Kya Hai?** Metadata ek file ka "data about data" hota hai, yani file ke baare mein basic information jo uske content se alag hoti hai. Ye file ke background details deta hai.
- **Metadata Mein Kya Info Hoti Hai?** Ismein cheezein jaise file ka creator/author name, creation date, modification date, software jisse file banaya gaya (e.g., Adobe Acrobat), file size, aur kabhi-kabhi location ya company details bhi shamil ho sakte hain. PDFs ke case mein, agar target ne document banaya ya edit kiya, to uska naam, email, ya organization ka hint mil sakta hai.
- **Kaise Check Karein?** PDF ko open karo (Adobe Reader ya koi aur PDF viewer mein), "File" menu pe jao, aur "Properties" select karo – wahan metadata dikhega. Online tools jaise ExifTool ya PDF Info bhi use kar sakte hain agar zyada detailed analysis chahiye.

Metadata se aap target ke baare mein extra clues jaise unka real name, workplace, ya contact info pa sakte hain, jo investigation mein kaam aati hai. Har PDF ko notes mein save karo aur metadata bhi record karo taaki aapke paas complete picture rahe.

Tools and Techniques for PDF Discovery

Method/Tool	Purpose	Example/Link
filetype:	Find PDFs	site:zsecurity.org filetype:pdf
Adobe Reader	View Metadata	File ¿ Properties
ExifTool	Detailed Metadata	https://exiftool.org

Point To Note

FileType: operator ke saath aap target se linked PDF documents easily find kar sakte hain, jaise site:zsecurity.org filetype:pdf se specific site pe PDFs milte hain. In PDFs ka metadata check karna zaroori hai kyunki ismein creator, date, aur software jaise details hote hain jo target ke baare mein valuable info de sakte hain. Ye method simple hai lekin powerful bhi, bas har document aur uska metadata carefully note karte jao taaki aapka OSINT process strong bane!

==========

Finding Hidden Search Results

Finding hidden search results OSINT mein ek important skill hai, aur ismein advanced tools aur techniques ka use hota hai. Ek powerful tool hai **SquareX Browser Extension**, jo aapke Chrome browser mein add karke hidden ya sensitive info ko uncover karne mein madad karta hai. Ye extension privacy aur security ke saath browsing ko enhance karta hai.

SquareX Browser Extension Kaise Use Karein:

1. **Add the Extension in Chrome:** Chrome Web Store pe jao, "SquareX" search karo, aur "Add to Chrome" pe click karke extension install karo. Install hone ke baad, ye aapke browser ke toolbar mein pin ho jayega.

2. **Sign In to Your Account:** Extension open karo, apna account create karo ya sign in karo (email ya Google/Microsoft ke through). Ye step zaroori hai taaki aap iske features use kar sakein.

3. **Features You Will See:** Jab aap extension kholte hain, to aapko teen main options dikhenge:

   - **Disposable Browsers:** Ye ek temporary browser hai jo cloud pe chalta hai. Iska use tab karo jab aapko suspicious websites check karna ho ya hidden search results find karne ke liye anonymously browse karna ho. Ye aapke real browser se alag hota hai aur session khatam hone ke baad sab delete ho jata hai – no traces left. Example: Agar aapko kisi shady link pe data check karna hai bina apne system ko risk mein daale, to ye perfect hai.
   - **Disposable File Viewer:** Ye feature aapko PDFs ya dusre files ko safely open karne deta hai bina unhe download kiye. Jab aapko koi file milti hai Google search mein aur aap sure nahi ho ki ye safe hai ya nahi, to iska use karo. Ye sandbox environment mein file kholta hai, jisse malware ka risk nahi hota. Example: Target se related ek PDF ka metadata check karna ho to ye use karo.
   - **Disposable Email:** Ye temporary email address banata hai jo aap sign-ups ya testing ke liye use kar sakte hain. Jab aapko kisi site pe register karna ho lekin apna real email nahi dena chahte, to ye kaam aata hai. Ye spam aur tracking se bhi bachata hai. Example: Kisi forum pe hidden info ke liye account banana ho to disposable email use karo.

Location Setting: Extension ke right side mein aapko location options dikhenge (jaise US, Germany, Singapore, etc.). Ye aapke Disposable Browser ke liye location set karta hai. Matlab, browser aisa dikhega jaise aap us specific country se browse kar rahe ho. Iska fayda ye hai ki aap geo-restricted content ya region-specific search results access kar sakte hain. Example: Agar aapko India-specific hidden results chahiye, to location India set karo aur search karo.

SquareX ke saath aap risky ya hidden data ko explore kar sakte hain bina apne system ya identity ko expose kiye. Har feature ka use case alag hai – Disposable Browser risky sites ke liye, File Viewer unknown files ke liye, aur Disposable Email privacy ke liye. Notes mein har finding save karna na bhoolo taaki aapka research organized rahe.

SquareX Features Overview

Feature	Purpose	Example Use Case
Disposable Browser	Anonymous Browsing	Check shady links
Disposable File Viewer	Safe File Viewing	View PDF metadata
Disposable Email	Temporary Email	Register on forums

Point To Note

SquareX Browser Extension hidden search results find karne ke liye ek game-changer hai. Disposable Browsers se aap anonymously browse kar sakte hain, Disposable File Viewer se risky files safely check kar sakte hain, aur Disposable Email se apni identity protect kar sakte hain. Location setting ke saath aap world bhar ke results access kar sakte hain. Ye tool OSINT ko safe, private, aur effective banata hai – bas install karo, sign in karo, aur smartly explore karo!

==========

Find Cameras and More with Google Hacking Database (GHDB)

GHDB, yani **Google Hacking Database**, ek aisa index hai jo special search queries (jinhe hum "Google Dorks" kehte hain) ka collection hai. Ye queries aapko internet pe sensitive ya specific information dhoondhne mein madad karti hain jo aksar publicly available hoti hai lekin shayad intentionally expose nahi ki gayi ho. GHDB ko samajhne ka simple tareeka ye hai ki ye ek tool hai jo Google search ko hack karne jaisa kaam karta hai – matlab, aap isse aisi cheezein find kar sakte hain jo normal search se nahi milti. Iska official URL hai: **https://www.exploit-db.com/google-hacking-database**.

GHDB Kya Hai Aur Kya Kya Dhoondh Sakta Hai?

- **Vulnerabilities:** Aap websites ya systems mein security weaknesses dhoondh sakte hain, jaise login pages jo unprotected hain (e.g., inurl:login admin).
- **Public Cameras:** Ye live webcams tak access de sakta hai jo online connected hain, jaise IP cameras jo secure nahi kiye gaye.
- **Public IoT Devices:** Internet of Things devices jaise smart TVs, thermostats, ya routers jo exposed hain.
- **Public Passwords:** Files ya pages jahan passwords ya sensitive data leak ho gaya ho (e.g., filetype:txt password).

- **Aur Bhi:** Configuration files, database dumps, ya personal info jo galti se public ho gaya ho.

Kaise Use Karein (Example – Cameras Dhoondhna):

1. GHDB ke URL pe jao: **https://www.exploit-db.com/google-hacking-database**.
2. Left upside mein search box mein "camera" type karo.
3. Aapko bahut saare Google Dorks dikhenge – ye special search queries hain. Example: **inurl:(webcam OR camera) -inurl:(login OR signup)**.
4. In dorks ko copy karo aur Google search bar mein paste karo.
5. Results mein aapko live camera feeds ke links mil sakte hain – ye public cameras hote hain jo unsecured chhode gaye hain.

Note – Files Aur Metadata: Agar aapko search ke dauraan koi file milti hai jaise MP4, MP3, PDF, etc., to uska **metadata** check karo. Metadata file ke baare mein extra info deta hai jo investigation mein kaam aa sakta hai.

- **ExifTool Online Kya Hai?** Ye ek free online tool hai jo multimedia files (jaise images, videos, PDFs) ka metadata extract karta hai. Google pe "exiftool online" search karo, koi trusted site chuno (jaise exiftool.org ya online alternatives), aur file upload karo.
- **Metadata Mein Kya Milta Hai?** Ismein file ka creator, creation date, location (agar GPS data ho), software used, ya camera details jaise info hoti hai. Example: Ek MP4 file se aapko pata chal sakta hai ki camera ka model kya tha ya recording kab ki gayi.
- **Kab Use Karein?** Jab aapko file ke source ya authenticity verify karni ho, ya target ke baare mein extra clues chahiye. Example: Agar aapko ek public camera ka video mila, to metadata se uska origin ya device info mil sakta hai.

GHDB ke dorks ka use karke aap cameras, IoT devices, ya sensitive files tak pahunch sakte hain. Har finding ko notes mein save karo aur files ka metadata zaroor check karo taaki aapko complete picture mile.

GHDB Use Cases

Category	Example Dork	Purpose
Cameras	inurl:(webcam OR camera)	Find live feeds
Passwords	filetype:txt password	Find leaked data
Vulnerabilities	inurl:login admin	Find weak login pages

Point To Note

GHDB ek treasure hai jo Google Dorks ke through internet pe chhupi cheezein – jaise public cameras, vulnerabilities, IoT devices, aur passwords – dhoondhne mein madad karta hai. Iska URL (https://www.exploit-db.com/google-hacking-database) pe jaake "camera" jaise keywords search karo, dorks copy karo, aur Google pe paste karke live results dekho. Files milne par ExifTool Online jaise tools se metadata check karo taaki aapko extra details mile. Ye method OSINT ke liye bahut powerful hai – bas ethically use karo aur har step ko note karte jao!

==========

[many]tcolorbox

Enhancing Google Searches with AI

Google searches ko AI ke saath enhance karna OSINT ke liye ek naye tareeke se powerful ban sakta hai, aur ismein **DorkGPT.com** jaise tools kaam aate hain. Ye website AI-powered Google Dorks generate karta hai jo aapke search ko precise aur effective banata hai. Iska basic idea ye hai ki aap apni zarurat ko simple language mein likho, aur ye tool uske liye ek Google Dork bana deta hai.

Kaise Kaam Karta Hai:

1. DorkGPT.com pe jao.
2. Prompt box mein apna search query simple English mein likho. Example – "Search for Satyam Singh in a PDF file."
3. "Generate" button pe click karo.
4. Ye tool aapke liye ek Google Dork bana dega, jaise – **filetype:pdf "Satyam Singh"**.
5. Is dork ko copy karke Google search bar mein paste karo, aur aapko results milenge jo sirf PDF files mein "Satyam Singh" ko dhoondhenge.

Fayde:

- Ye tool manually dorks banane ke time ko bachata hai.
- Beginners ke liye bhi easy hai kyunki aapko advanced operators jaanne ki zarurat nahi – bas apna intent likho aur AI baaki kaam karta hai.
- Specific searches ke liye perfect hai, jaise PDFs, vulnerabilities, ya kisi particular site pe info dhoondhna.

Example ke taur pe, agar aap "Satyam Singh ka data PDF mein" likhte ho, to DorkGPT shayad ye dork de: **filetype:pdf "Satyam Singh" -inurl:(signup login)** – ye PDF files mein Satyam Singh ko dhoondhega aur signup/login pages ko exclude karega. Is tarah aap hidden ya specific info tak quickly pahunch sakte hain. Har generated dork ko test karo aur results ko notes mein save karo taaki aapka research organized rahe.

DorkGPT Examples

Prompt	Generated Dork	Purpose
"Satyam Singh in a PDF file"	filetype:pdf "Satyam Singh"	Find PDFs
"Satyam Singh ka data PDF mein"	filetype:pdf "Satyam Singh" -inurl:(signup login)	Exclude login pages

Point To Note

DorkGPT.com jaise AI tools Google searches ko next level pe le jaate hain by generating smart Google Dorks jo aapke prompt pe based hote hain. Example jaise "Satyam Singh in a PDF file" se aapko ek perfect dork milta hai jo time bachata hai aur results ko accurate banata hai. Ye OSINT ke liye ek game-changer hai – simple, fast, aur effective. Bas prompt daalo, dork lo, aur search shuru karo, lekin hamesha findings ko note karte jao!

==========

Discovering Additional Info and Online Accounts Using Bing

Bing search engine – alag search engines ka use karne se aapko varying search results mil sakte hain, kyunki har engine ka algorithm aur indexing alag hota hai. Bing ke paas kuch exclusive search operators hain jo Google mein nahi hote, jisse aapko extra accounts ya usernames mil sakte hain jo Google search mein shayad na dikhein. Example ke liye, Bing ke unique operators ka use karke aap kisi target ke naye online profiles ya details uncover kar sakte hain. Lekin ye kehna ki "search operators same hain Bing aur Google ke liye" – ye **sahi nahi hai**. Dono ke operators mein similarities hain jaise "site:" ya "filetype:", lekin Bing ke kuch operators aur unke functionalities alag hain. Example: Bing ka "loc:" operator Google mein directly available nahi hai, aur Bing "near:" jaise operators bhi support karta hai jo Google nahi karta. Isliye, Bing ke saath experiment karna OSINT ke liye valuable ho sakta hai.

Note: Jab aap Google pe kisi company ya person ke baare mein info dhoondhte hain aur ek page milta hai jo Google servers pe saved nahi hai ya cached nahi hai, to us page ka title ya URL copy karo. Phir ise **Yandex** ya Bing search engine mein daalo.

- **Yandex Kya Hai?** Yandex ek Russian search engine hai jo 1997 mein launch hua tha. Ye Russia mein sabse popular search engine hai aur globally bhi kaafi use hota hai (around 2-3% market share). Ye Google aur Bing se alag tarike se web ko index karta hai, isliye kai baar aapko wahan cached pages ya info mil sakti hai jo Google pe nahi hoti. Yandex ke features mein search ke saath-saath maps, email, aur cloud services bhi shamil hain. OSINT ke liye ye useful hai kyunki iska data set aur caching system Google se different hota hai, aur ye geo-specific results bhi de sakta hai.

- **Bing aur Yandex Mein Cached Version:** Agar Google pe cached version nahi milta, to Bing ya Yandex pe check karo. Bing bhi Microsoft ka search engine hai aur apna alag caching system rakhta hai, jisse aapko deleted ya old pages ke versions mil sakte hain.

Yandex aur Bing dono ke results Google se vary karte hain, to inka use karke aap extra info ya accounts tak pahunch sakte hain.

Loc: Operator: Ye Bing ka ek khas search operator hai jo web pages ko specific country ya region se filter karta hai. Example – agar aap ek person ko search kar rahe hain jo India se hai, to is operator se results limit kar sakte hain. Jaise – **"Rishi Kabra" loc:in** – yahan "in" India ke liye hai. Isse sirf India-based websites ya content pe focus hoga, jo aapke target ke online presence ko narrow down karne mein madad karta hai. Ye operator OSINT mein kaafi kaam aata hai jab aapko location-specific info chahiye hoti hai.

Bing ke saath alag-alag operators try karo aur results ko notes mein save karo taaki aapke paas target ke online accounts aur additional info ka complete record ho.

Bing Operators and Tools

Tool/Operator	Purpose	Example
loc:	Location Filter	"Rishi Kabra" loc:in
near:	Proximity Search	"Rishi Kabra" near:10
Yandex	Cached Pages	Search URL from Google

Point To Note

Bing search engine OSINT ke liye ek strong option hai kyunki iske exclusive operators jaise "loc:" aapko location-based results dete hain, aur Google se alag results milne ki wajah se extra accounts ya info uncover ho sakti hai. Yandex aur Bing dono cached pages dikhate hain jo Google pe nahi milte, to inka use karke aap hidden ya old data tak pahunch sakte hain. "Rishi Kabra" loc:in jaise searches se specific region ke results milte hain, jo investigation ko refine karte hain. Bing aur Yandex ko apne toolkit mein add karo aur har finding ko note karo – ye aapke OSINT game ko level up karega!

==========

Beyond Google - Finding Hidden Info

Google ke alawa bhi kaafi search engines hain jo hidden info dhoondhne mein madad kar sakte hain, aur Bing unmein se ek powerful option hai. Bing ke paas kuch search operators hain jo Google mein nahi hote, aur ye OSINT ke liye kaafi useful ho sakte hain. Ek aisa operator hai **"near:"**, jo Google mein available nahi hai. Ye operator do words ya phrases ke beech ki doori (proximity) ko specify karta hai, yani aap ye control kar sakte hain ki do terms ek doosre ke kitne close hon page pe.

"near:" Operator Ka Use in OSINT:

- **Syntax:** "word1 word2 near:n" – yahan "n" words ke beech maximum distance hai.
- **Example:** Agar aapko "Satyam Singh" ke baare mein info chahiye aur ye confirm karna hai ki "Patna" uske close mention hua hai, to Bing pe search karo: **"Satyam Singh Patna near:5"**. Ye sirf un pages ko dikhayega jahan "Satyam Singh" aur "Patna" ek doosre se 5 words ke andar hain.

- **OSINT Mein Fayda:** Ye operator target ke context ko refine karta hai. Jaise, agar aapko kisi person ke location ya association ke baare mein specific info chahiye, to "near:" se aap irrelevant results ko filter out kar sakte hain. Example: "Rishi Kabra cybersecurity near:10" – isse aap Rishi Kabra ke cybersecurity-related mentions hi dekh sakte hain jo closely linked hain, random mentions nahi.

Iske alawa, Bing ka **"loc:"** operator bhi Google se thoda different kaam karta hai aur country-specific results ke liye zyada precise ho sakta hai, lekin "near:" truly unique hai. OSINT mein iska use karke aap hidden connections ya specific details uncover kar sakte hain jo Google ke broad search mein shayad miss ho jayein. Har result ko check karo aur notes mein save karo taaki aapka investigation complete aur organized rahe.

Bing "near:" Operator Examples

Search Query	Operator Syntax	Purpose
Satyam Singh in Patna	"Satyam Singh Patna near:5"	Location context
Rishi Kabra cybersecurity	"Rishi Kabra cybersecurity near:10"	Topic relevance

Point To Note

Bing ka "near:" operator Google mein nahi hai aur ye OSINT ke liye ek secret weapon ho sakta hai, kyunki ye words ke beech proximity ko target karta hai. "Satyam Singh Patna near:5" jaise searches se aap specific aur meaningful info pa sakte hain jo context-based ho. Google ke beyond jao, Bing ke unique operators try karo, aur hidden info ko efficiently uncover karo – bas har finding ko note karte jao taaki kuch miss na ho!

==========

Find More with Special Yandex Operators

Yandex search engine – ye ek Russian search engine hai jo 1997 mein launch hua tha aur aaj Russia mein sabse popular hai, wahan ke search traffic ka bada hissa (50% se zyada) iske paas hai. Yandex kaafi advanced technologies jaise MatrixNet (machine learning) aur Spectrum (implicit query analysis) use karta hai, jisse search results zyada relevant aur accurate hote hain. Ye Google aur Bing se alag approach rakhta hai, isliye using different search engines might yield varying search results – yani jo info Google pe nahi milti, wo Yandex pe mil sakti hai. Yandex ke paas kuch **exclusive search operators** bhi hain jo Google ya Bing mein nahi hote, aur ye OSINT ke liye kaafi powerful ho sakte hain.

Yandex Ke Special Operators:

- **lang:** Ye operator specific language ke results dikhata hai. Example: **"Satyam Singh" lang:en** – sirf English pages dikhayega.
- **mime:** Ye file type ke liye hai, jaise Google ka "filetype:". Example: **"Rishi Kabra" mime:pdf** – PDFs mein Rishi Kabra dhoondhega.
- **host:** Ye ek specific domain ke andar search karta hai. Example: **"cybersecurity" host:*.edu** – educational sites pe cybersecurity-related content dikhayega.

- **date:** Ye time-based search ke liye hai. Example: **"news" date:20240101..20241231** – 2024 ke news results dikhayega.

Yandex Ki Khaasiyat: Yandex best hai **face matching** aur **location identification** ke liye, khaaskar jab aap reverse image search use karte hain. Yandex Images mein ek photo upload karo, aur ye faces ko recognize karke similar images ya exact matches dhoondh sakta hai – ye capability Google aur Bing se kaafi better hai. Location ke liye bhi, ye photo ke background details (jaise buildings, landscapes) se jagah identify kar sakta hai. Isliye OSINT mein ye ek go-to tool ban jata hai jab aapko hidden ya specific info chahiye.

Note: Ye kehna ki "all Google Dorks will work here also in Yandex" – ye **bilkul sahi nahi hai**. Google ke zyadatar basic dorks jaise "site:", "inurl:", "filetype:" Yandex pe kaam karte hain, lekin Yandex ke apne syntax aur limitations hain. Kuch complex Google Dorks (jaise "cache:" ya "related:") Yandex pe support nahi hote. Isliye, Yandex pe dorks use karne se pehle unhe test karo aur thoda adjust karna pad sakta hai. Haan, basic operators cross-compatible hain, lekin Yandex ke exclusive operators alag se seekhna better hai.

Yandex ke results ko notes mein save karo aur agar image search kar rahe ho, to metadata bhi check karo taaki aapko target ke baare mein aur zyada clues mil sakein.

Yandex Operator Examples

Operator	Example	Purpose
lang:	"Satyam Singh" lang:en	English results
mime:	"Rishi Kabra" mime:pdf	PDF search
host:	"cybersecurity" host:*.edu	Domain-specific
date:	"news" date:20240101..2024123	Time filter

Point To Note

Yandex ek unique aur powerful search engine hai jo apne exclusive operators (jaise lang:, mime:, host:, date:) aur face matching/location identification ke liye famous hai. Google aur Bing se alag results dene ki wajah se ye OSINT ke liye perfect hai. Google Dorks ka kuch hissa Yandex pe kaam karta hai, lekin poora nahi – isliye thoda tweak karke use karo. Face recognition aur location tracking mein iska jawab nahi, to hidden info dhoondhne ke liye ise zaroor try karo aur har finding ko note karte jao!

==========

Expanding Results with Alternative Search Engines

OSINT mein ek search engine pe depend karna kaafi nahi hai kyunki har search engine ka indexing alag hota hai. Note – kuch search results Bing ya Yandex pe indexed hote hain lekin

Google pe nahi, aur isiliye apne target ke baare mein info dhoondhne ke liye multiple search engines pe search karna zaroori hai. Har engine ka apna algorithm aur data set hota hai, jo aapko varying results de sakta hai. Isse aapka coverage expand hota hai aur hidden info tak pahunchne ke chances badh jaate hain.

Alternative Search Engines:

- **DuckDuckGo:** Ye ek privacy-focused search engine hai jo 2008 mein launch hua tha. Iska USP hai ki ye user tracking nahi karta aur ads bhi minimal rakhta hai. DuckDuckGo Google ke jaisa broad nahi hai, lekin ye alag sources se data pull karta hai, jisse aapko unique results mil sakte hain. Example: Agar aap "Satyam Singh" search karte ho, to DuckDuckGo shayad kuch forums ya niche sites ke results de jo Google skip kar deta hai. OSINT ke liye ye tab useful hai jab aap anonymously search karna chahte ho ya privacy maintain karni ho.

- **Baidu:** Ye China ka leading search engine hai, jo 2000 mein launch hua tha aur wahan Google se bhi bada hai (China mein Google banned hai). Baidu Chinese language aur culture ke liye optimized hai, isliye agar aapka target Chinese person ya company hai, to Baidu best hai. Example: "Zhang Wei" ko Baidu pe search karo, to aapko Chinese social media (Weibo), local news, ya government records mil sakte hain jo Google, Bing, ya Yandex pe nahi honge.

Note: Baidu Chinese persons ya China-related info ke liye great hai kyunki ye local content ko deeply indexampled karta hai. Agar aapka target China se hai, to Baidu pe search karna must hai – wahan ke WeChat profiles, forums, ya documents tak access mil sakta hai.

Google Dorks Ka Compatibility: Ye kehna ki "all Google Dorks will work in all these search engines" – **sahi nahi hai**. Har search engine ke apne operators aur syntax hote hain, aur Google Dorks ka poora set har jagah kaam nahi karta. Difference yahan hai:

- **DuckDuckGo:** Basic Google Dorks jaise "site:", "inurl:", "filetype:" kaam karte hain, lekin advanced operators jaise "cache:", "related:", ya "near:" support nahi hote. DuckDuckGo ke apne "bangs" feature hain (e.g., !g for Google, !w for Wikipedia), jo alag tareeke se kaam karte hain. Isliye, simple dorks try karo, lekin complex wale adjust karne padenge.

- **Baidu:** Baidu Google Dorks ko directly support nahi karta kyunki iska syntax aur language focus Chinese pe based hai. "site:" ya "filetype:" jaise operators kaam kar sakte hain, lekin English-based dorks ka response limited hoga. Baidu ke apne operators hain (jaise "inurl:" ke liye ":"), jo Chinese mein better kaam karte hain. Agar Chinese target hai, to Baidu ke native search syntax seekhna better hai.

- **Bing aur Yandex:** In dono pe zyadatar basic Google Dorks (site:, inurl:, filetype:) kaam karte hain, lekin unke apne unique operators (Bing ka "near:", Yandex ka "lang:") alag hote hain, jaisa pehle discuss kiya gaya hai.

Isliye, multiple engines pe search karo, lekin har ek ke liye operators ko test aur tweak karo. Results ko notes mein save karo taaki aapka data organized rahe aur aap target ke online presence ka poora picture bana sakein.

Alternative Search Engine Features

Engine	Unique Feature	Example Use
DuckDuckGo	Privacy-focused	"Satyam Singh" anonymously
Baidu	Chinese indexing	"Zhang Wei" on Weibo

Point To Note

Alternative search engines jaise DuckDuckGo, Baidu, Bing, aur Yandex se aap Google ke beyond jakar hidden info expand kar sakte hain. DuckDuckGo privacy ke liye aur Baidu Chinese targets ke liye perfect hai, jabki Bing aur Yandex apne unique indexing se alag results dete hain. Google Dorks har engine pe fully kaam nahi karte – DuckDuckGo pe basic chalte hain, Baidu pe Chinese syntax chahiye, aur Bing/Yandex pe thoda adjustment zaroori hai. Har engine try karo, results compare karo, aur notes banate jao taaki kuch miss na ho!

==========

Introduction to Database Breaches and Leaks

Database breaches aur leaks OSINT (Open Source Intelligence) ke liye ek bada source hain kyunki ye sensitive aur personal info ko expose karte hain. **Breached aur leaked databases** woh collections hain jahan unauthorized access ya accidental exposure ke through data leak ho jata hai. In databases mein kaafi valuable info hoti hai jo aapke target ke baare mein reveal kar sakti hai, jaise:

- **Name:** Full name ya aliases jo identity confirm karne mein help karte hain.
- **Phone Number:** Contact details jo location ya communication patterns dikhate hain.
- **Password:** Leaked passwords jo target ke accounts ko access karne ke liye use ho sakte hain, khaaskar agar woh same password doosre platforms pe reuse karte hain.
- **Email:** Email addresses jo social media ya professional accounts se link ho sakte hain.

Ye har piece of data ek starting point ban sakta hai aur isse aap **dusre data breaches ya leaks** ke through aur zyada info collect kar sakte hain. Example ke liye, agar aapko ek breach se target ka email milta hai, to aap us email ko **Facebook, Twitter, LinkedIn, Snapchat** jaise platforms ke past data leaks mein search kar sakte hain taaki unke profiles, usernames, ya connections ka pata chal sake.

Kaise Kaam Karta Hai:

- Ek breach se mila phone number aapko target ke social media accounts tak le ja sakta hai.
- Ek leaked password doosre platforms pe try kiya ja sakta hai agar target ne wahi password reuse kiya ho (ye common hai).

- Email ya name se aap LinkedIn pe professional history ya Snapchat pe personal activity track kar sakte hain.

Popular Data Leaks Examples:

- **Facebook:** 2021 mein 533 million users ka data leak hua, jisme phone numbers, names, aur emails expose hue.
- **Twitter:** 2022-23 mein 200 million+ users ke emails aur usernames leak hue API vulnerability ke wajah se.
- **LinkedIn:** 2021 mein 700 million users ka data scraped aur leaked hua, jisme emails aur job details shamil the.
- **Snapchat:** 2014 mein 4.6 million usernames aur phone numbers leak hue the.

Ye breaches aksar dark web pe ya hacker forums pe milte hain, aur tools jaise **Have I Been Pwned** ya **Leak-Lookup** se check kar sakte hain ki aapka target ka data kisi breach mein involve hai ya nahi. Har retrieved data ko carefully note karo aur cross-reference karo taaki aap step-by-step target ke online presence ka complete picture bana sakein. Lekin yaad rakho – ye info ethically aur legally use karni chahiye.

Popular Data Breaches

Platform	Year	Leaked Data
Facebook	2021	533M: Phone, Name, Email
Twitter	2022-23	200M+: Email, Username
LinkedIn	2021	700M: Email, Job Details
Snapchat	2014	4.6M: Username, Phone

Point To Note

Database breaches aur leaks ek goldmine hain OSINT ke liye kyunki inmein name, phone number, password, email jaise details hote hain jo target ke baare mein kaafi kuch reveal kar sakte hain. Ek breach se mili info ko Facebook, Twitter, LinkedIn, Snapchat jaise platforms ke leaks ke saath connect karke aap aur zyada data uncover kar sakte hain. Ye process chain reaction jaisa hai – har piece of data aapko agle clue tak le jata hai. Bas har finding ko notes mein save karo aur systematically kaam karo taaki aapka investigation thorough aur successful ho!

==========

titlesec

Understanding the Difference Between Breached and Leaked Databases

Breached aur leaked databases ke beech difference samajhna OSINT ke liye zaroori hai kyunki dono alag tareeke se data expose karte hain aur unka source bhi alag hota hai. Inka basic farak intent aur process mein hai:

- **Data Leak:** Ye **unintentional exposure** hota hai sensitive data ka, yani ye galti se public ho jata hai. Iska matlab hai ki koi security lapse, misconfiguration, ya human error ki wajah se data leak hota hai, bina kisi malicious intent ke. Example: Ek company ne apna database accidentally public cloud pe open chhod diya (jaise unsecured Amazon S3 bucket), jisme emails, names, ya passwords expose ho gaye. Data leak aksar negligence ya technical mistake ki wajah se hota hai, aur ye info publicly accessible ho sakti hai agar koi dhoondh le.
- **Data Breach:** Ye **intentional unauthorized access** hota hai sensitive info ka, yani koi hacker ya attacker knowingly system mein ghuskar data churata hai. Isme malicious intent hota hai, aur ye security ko bypass karke kiya jata hai. Example: Ek cybercriminal ne phishing attack ya malware ke through ek company ke servers se passwords, credit card details, ya personal info chura liya. Data breach ke baad ye info dark web pe sell ho sakti hai ya ransom ke liye use ho sakti hai.

Key Differences:

- **Intent:** Leak mein koi plan nahi hota, ye accident hai. Breach mein attacker ka clear motive hota hai.
- **Source:** Leak aksar internal mistake se hota hai (jaise wrong settings), jabki breach external attack se (hacking).
- **Impact in OSINT:** Dono hi target ke baare mein info de sakte hain (jaise name, email, password), lekin leaks publicly available ho sakte hain (e.g., Google pe mil jayein), jabki breaches ka data dark web ya private forums pe milta hai.

OSINT Mein Use: Agar aapko ek leaked database milta hai, to usme se target ka email ya phone number directly mil sakta hai kyunki ye open source ho sakta hai. Breach ka data dhoondhne ke liye aapko tools jaise **Have I Been Pwned** ya dark web searches ki zarurat pad sakti hai. Dono cases mein retrieved info (jaise username, password) ko notes mein save karo aur cross-check karo taaki aap target ke online presence ko aur expand kar sakein.

Leak vs. Breach Comparison

Aspect	Data Leak	Data Breach
Intent	Unintentional	Intentional
Source	Internal Mistake	External Attack
Example	Unsecured S3 Bucket	Phishing Attack
OSINT Access	Publicly Available	Dark Web

Point To Note

Data leak aur data breach mein basic farak ye hai ki leak unintentional hota hai (galti se exposure), jabki breach intentional hota hai (hacking se). OSINT ke liye dono useful hain – leaks se aap easily accessible info pa sakte hain, aur breaches se deep, sensitive data mil sakta hai. Inka difference samajhkar aap sahi tareeke se unhe use kar sakte hain – har detail ko note karo aur systematically target ke baare mein info build karo!

==========

Finding Relevant Breach/Leak Databases

Breach aur leak databases mein relevant info dhoondhna OSINT ke liye ek key step hai kyunki ye target ke sensitive details reveal kar sakte hain. **Things to find in a breach/leak database** – kam se kam ek cheez to unique honi chahiye jo target ko identify kare, jaise:

- **Email:** Ye ek primary identifier hai kyunki har person ka email unique hota hai aur kai websites pe registered hota hai.
- **Phone Number:** Ye bhi unique hota hai aur target ke location ya contact tracing ke liye useful hai.

Additional Helpful Info to Refine Your Search: Agar in databases mein ye extra details mil jayein, to aapka search aur refine ho sakta hai:

- **First and Last Name:** Full name se aap target ki identity confirm kar sakte hain.
- **Physical Address:** Ye location-specific info deta hai jo investigation ko narrow karta hai.
- **Country, City:** Ye geographic context dete hain, jaise target kahan se hai ya kahan active hai.
- **Age:** Age se aap target ke demographic profile bana sakte hain.
- **Gender:** Ye bhi profiling ke liye helpful hota hai.

Have I Been Pwned? (HIBP): Ye ek free online tool hai jo aapko check karne deta hai ki aapka info (email ya phone number) kisi data breach ya leak mein expose hua hai ya nahi.

- **Kaise Use Karein:** Google pe jao, search karo "haveibeenpwned.com", site pe jao, aur apna email ya phone number paste karo. "Pwned?" button pe click karo.
- **Kya Milega:** Agar email kisi breach mein mila, to HIBP batayega ki ye **X number of data breaches** mein found hua hai aur konse websites se leak hua (e.g., BigBasket, LinkedIn). Example: Agar "satyam@example.com" BigBasket breach mein mila, to ye confirm hota hai ki ye email valid hai aur us site pe use hua tha, kyunki websites jaise BigBasket registration ke time email verification link bhejte hain.

Note: Have I Been Pwned jab aap email search karte hain, to ye bhi dikhata hai ki **what types of data were leaked**. Example – BigBasket ke saath likha hoga "Compromised Data: Date of Birth, Email Addresses, IP Addresses, Names, Passwords, Phone Numbers, Physical Addresses". Iska matlab hai agar aapke paas BigBasket ka breached/leaked database hai, to aap us email ke saath ye saari details find kar sakte hain. Is info ko use karke aap target ke baare mein aur research kar sakte hain.

Note: Kuch data leak databases mein aapko aur sensitive info bhi mil sakti hai jaise:

- **Government-Issued IDs:** Aadhar, PAN, ya driver's license numbers.
- **Passport Numbers:** International travel ya identity verification ke liye.
- **Social Media Profiles:** LinkedIn, Twitter, ya Facebook usernames jo target ke online presence ko expand karte hain.

In details ko collect karke aap step-by-step target ka complete profile bana sakte hain. Har finding ko notes mein save karo aur cross-check karo taaki aap breaches se mili info ko maximize kar sakein.

Data Types in Breaches/Leaks

Data Type	Purpose	Example
Email	Primary Identifier	satyam@example.com
Phone Number	Location Tracing	+91-9876543210
Physical Address	Narrow Investigation	123 Main St, Delhi
Social Media Profile	Expand Presence	@satyam$_{t}witter$

Point To Note

Breach aur leak databases se email ya phone number jaise unique identifiers dhoondho, aur extra info jaise name, address, age, ya gender se search ko refine karo. Have I Been Pwned (HIBP) se pata chalta hai ki target ka email konse breaches mein hai (jaise BigBasket) aur kya-kya data leak hua (passwords, addresses, etc.). Kuch leaks mein IDs, passport numbers, ya social media profiles bhi mil sakte hain. Ye sab info ek treasure hai OSINT ke liye – bas systematically collect karo, notes banao, aur target ke baare mein deep insights pao!

==========

Finding Email, Password, and More

OSINT mein email, password, aur aur details dhoondhna ek important task hai, aur iske liye breach aur leak databases ka use hota hai. **DeHashed** ek powerful search engine hai jo data breaches aur leaks se info dhoondhne ke liye banaya gaya hai. Isme aap **name, email address, phone number, username**, aur aur bhi cheezein search kar sakte hain. Ye tool security analysts, journalists, aur common users ke liye design kiya gaya hai taaki compromised data ka insight mil sake. Lekin ye ek **paid service** hai – iska full access subscription ke through milta hai (jaise API credits ya premium plans).

Free Version Mein Kya Milta Hai: DeHashed ka free tier limited hota hai. Aap basic search kar sakte hain (email ya username daalkar), lekin results mein sirf yahi pata chalega ki data kisi breach mein hai ya nahi, aur shayad kuch breaches ke naam dikh jayein (e.g., "Found in BigBasket breach"). Detailed info jaise passwords, phone numbers, ya exact records free mein nahi milte – ye premium users ke liye reserved hai. OSINT ke liye free version se basic confirmation to mil sakta hai, lekin deep investigation ke liye paid plan chahiye.

Free Alternatives: Agar aapko DeHashed jaisa free tool chahiye, to ye options try kar sakte hain:

- **Have I Been Pwned (HIBP):** Ye sabse popular free tool hai (haveibeenpwned.com). Aap email ya phone number daal sakte hain, aur ye batayega ki wo kisi breach mein mila ya nahi, saath hi breached websites ke naam bhi dega (e.g., LinkedIn, Adobe). Passwords directly nahi dikhata, lekin aap separately password check kar sakte hain (hashed format mein). OSINT ke liye ye starting point ke taur pe kaafi acha hai.

- **LeakCheck:** Ye bhi ek freemium tool hai (leakcheck.io). Free mein email ya username se search kar sakte hain, aur limited results milte hain jaise breach ka naam aur compromised data types (e.g., email, password). Full details ke liye payment chahiye, lekin free version bhi basic OSINT ke liye helpful hai.

- **BreachDirectory:** (breachdirectory.org) Ye free mein email, username, ya phone number se breaches dhoondh sakta hai. Results mein breach names aur thodi info milti hai, lekin sensitive data jaise passwords censored hote hain free users ke liye. Ye privacy-focused hai aur OSINT ke liye acha alternative hai.

- **GhostProject:** (ghostproject.fr) Ye ek free database lookup hai jahan aap email ya username se breaches check kar sakte hain. Limited results free mein milte hain, jaise breach ka naam aur kabhi-kabhi partial data, lekin full access ke liye paid plan hai.

Kaise Use Karein: In free tools se aap target ka email ya username daalkar check kar sakte hain ki wo kisi breach mein involve hai ya nahi. Agar breach mila, to us website (jaise BigBasket) ke leak ko aur research kar sakte hain – shayad dark web pe ya forums pe full dump mile. Free tools se aapko starting clues milenge, jisse aap apna OSINT investigation aage badha sakte hain. Har result ko notes mein save karo aur cross-check karo taaki aapka data complete aur useful rahe.

Tools for Breach/Leak Searches

Tool	Access	Features
DeHashed	Paid (Limited Free)	Email, Password, Phone
Have I Been Pwned	Free	Breach Names, Data Types
LeakCheck	Freemium	Breach Names, Limited Data
BreachDirectory	Free	Censored Sensitive Data

Point To Note

DeHashed ek paid service hai jo breaches se email, password, aur aur details dhoondhne mein madad karta hai, lekin free mein sirf basic confirmation milta hai, jo OSINT ke liye limited hai. Free alternatives jaise Have I Been Pwned, LeakCheck, BreachDirectory, aur GhostProject bhi kaafi acha kaam karte hain – ye breach info dete hain aur starting point ban sakte hain. Inse aap target ke compromised data ka hint pa sakte hain, aur phir deep research ke liye aage badh sakte hain. Notes banakar har clue ko track karo taaki aapka investigation strong bane!

==========

Finding Address, Phone Number, and More

Intelligence X ek search engine aur data archive hai jo OSINT ke liye kaafi powerful tool hai. Iska matlab hai ki aap isse **leaked databases** mein search kar sakte hain aur **archived websites** tak pahunch sakte hain. Ye tool aapko addresses, phone numbers, emails, aur aur bhi sensitive info dhoondhne mein madad karta hai jo breaches ya public sources se aati hai. Ismein aap email addresses, domains, IP addresses, URLs, aur aur bhi cheezein search kar sakte hain jo target ke online presence ko uncover karne ke liye useful hain. Website visit karne ke liye: **https://intelx.io**.

Note: Intelligence X partially free hai, yani iska basic version free mein use kar sakte hain, lekin full access ke liye paid subscription chahiye. Free version mein aap email, domains, IP addresses, URLs, etc. search kar sakte hain, lekin results limited hote hain aur detailed data (jaise passwords ya full files) paid users ke liye reserved hai. Ye tool darknet, public leaks, whois data, aur archived web content ko index karta hai, jo Google jaise traditional search engines se nahi milta.

How to Use Intelligence X for Free – Steps:

1. **Website Pe Jao:** Browser kholo aur **https://intelx.io** pe jao.

2. **Sign Up Karo:** Homepage pe "Sign Up" pe click karo. Ek free account banane ke liye apna email daalo aur password set karo. Sign up ke baad aapko 7-day free trial milta hai jisme full access hota hai, lekin trial khatam hone ke baad account "Free" plan pe downgrade ho jata hai.

3. **Login Karo:** Apne credentials se login karo. Free account ke saath aap basic searches kar sakte ho.

4. **Search Shuru Karo:** Search bar mein apna target daalo – ye email (e.g., satyam@example.com), phone number (e.g., +919876543210), domain (e.g., example.com), IP address (e.g., 192.168.1.1), ya URL (e.g., https://example.com) ho sakta hai. "Search" button pe click karo.

5. **Results Dekho:** Free version mein aapko limited results dikhenge – jaise breach ka naam (e.g., "Found in BigBasket leak") ya archived website ka snippet. Detailed info jaise phone number, address, ya password free mein nahi dikhta, lekin aapko hint mil sakta hai ki data kahan se aaya hai.

6. **Filters Use Karo:** Advanced search option mein buckets (jaise "leaks.public" ya "darknet") select kar sakte ho, lekin free account ke saath access restricted hota hai. Phir bhi, basic filtering se kaam chala sakte ho.

7. **Findings Save Karo:** Jo bhi results milte hain, unhe copy-paste karke apne notes mein save karo (Notion ya koi aur tool use karo) taaki aapka research organized rahe.

Extra Tips: Free version mein results preview limited hota hai, lekin agar aapko breach ka naam milta hai (jaise "LinkedIn 2021 breach"), to us breach ko aur research kar sakte ho – shayad dark web pe ya dusre free tools jaise Have I Been Pwned se cross-check karo. Intelligence X ka free tier starting point ke liye acha hai, lekin deep info ke liye paid plan ya alternative tools chahiye honge.

Intelligence X Search Examples

Search Type	Example Input	Possible Free Output
Email	satyam@example.com	Found in BigBasket leak
Phone Number	+919876543210	Archived snippet
Domain	example.com	Whois data hint
IP Address	192.168.1.1	Limited leak info

Point To Note

Intelligence X ek shandaar tool hai jo leaked databases aur archived websites se address, phone number, aur aur details dhoondhne mein madad karta hai. Free version mein sign up karke aap email, domains, IPs, aur URLs search kar sakte ho, lekin results limited hote hain. Steps simple hain – website pe jao, account banao, login karo, aur search shuru karo. Har finding ko notes mein save karo aur agar zarurat pade to breach info ko aur explore karo. Ye tool OSINT ke liye ek solid base deta hai – bas free limits ko samajhkar smartly use karo!

==========

Setting Up an Isolated Virtual Environment

Leaked ya breached databases se data access karne ke do main tareeke hain, aur in dono ke liye ek isolated virtual environment set up karna zaroori hai taaki aapka main system safe rahe. Ye do methods hain:

1. **Subscription Service:** Ye paid ya freemium services hain jo aapko breached data search karne ki facility dete hain. Examples:

   - **DeHashed:** Ek search engine hai jo emails, passwords, usernames, etc. breaches mein dhoondhta hai. Free mein basic info milti hai, lekin detailed data ke liye subscription chahiye.
   - **Intelligence X (IntelX):** Ye leaks aur archived web content ko index karta hai. Free tier mein limited searches hain, aur paid plan se full access milta hai. (https://intelx.io)
   - **Snusbase:** Fast aur comprehensive breach search tool hai, lekin ye bhi paid hai. Ye cleartext data deta hai premium users ko.

   In services ka use karne ke liye aapko bas website pe account banana hota hai aur search queries daalni hoti hain. Lekin inka downside ye hai ki aapko recurring cost deni pad sakti hai aur data unke servers pe rehta hai, aapke paas locally nahi hota.

2. **Local Download:** Isme aap breached databases ko apne system pe download karte ho aur locally search karte ho. Iske liye hardware aur software ki zarurat hoti hai:

   - **Software:**

  - **Agent Ransack:** Ye ek free file search tool hai jo Windows pe chalta hai. Iska use karke aap downloaded databases (text files, CSVs, etc.) mein specific keywords (jaise email, phone number) dhoondh sakte ho. Ye fast hai aur large files ko handle kar sakta hai. Install karne ke liye: Agent Ransack ki official site (filehippo.com ya fileforum.com) pe jao, download karo, aur setup run karo.
  - **Torrent Client:** Databases aksar torrents ke through share hote hain (e.g., BitTorrent, qBittorrent). Ye software aapko torrent files ya magnet links se data download karne deta hai. qBittorrent ek free aur open-source option hai – isko qbittorrent.org se download karo, install karo, aur torrent file/magnet link add karke download start karo.

- **Hardware:**
  - **Disk Space:** Leaked databases ka size bada hota hai – chhote datasets 1-2 GB ke hote hain, jabki bade jaise COMB (Combination of Many Breaches) 20 GB download aur 100 GB unzipped ho sakte hain. Isliye aapke paas kam se kam 50-100 GB free disk space hona chahiye (external HDD ya SSD recommended). Example: Agar aap 5-10 breaches download karna chahte ho, to 500 GB ya 1 TB ki drive perfect hai.

Isolated Virtual Environment Kaise Set Up Karein: Agar aap local download method use kar rahe ho, to malware ya privacy risks se bachne ke liye ek isolated virtual environment banana zaroori hai. Steps:

1. **Virtual Machine Software Install Karo:**
   - **VirtualBox:** Ye free hai (oracle.com/virtualbox se download). Install karne ke baad ek naya virtual machine (VM) banao.
   - **VMware Workstation Player:** Bhi free hai personal use ke liye (vmware.com se download).
2. **Operating System Add Karo:** Ek lightweight OS jaise **Ubuntu** (ubuntu.com se ISO file download karo) VM mein install karo. Ye safe aur free hai. VirtualBox mein "New" pe click karo, Ubuntu ISO select karo, aur 2-4 GB RAM aur 20-50 GB storage allocate karo.
3. **Network Isolation:** VM ke network settings mein "NAT" ya "Host-Only" mode rakho, taaki ye aapke main network se connected na ho. "No Internet" option bhi set kar sakte ho agar sirf local search chahiye.
4. **Software Setup in VM:** VM ke andar Agent Ransack (Windows VM ke liye) ya qBittorrent install karo. Linux pe "grep" command bhi use kar sakte ho text files search ke liye (e.g., `grep "satyam@example.com" filename.txt`).
5. **Download Databases:** Torrent client ke through breach databases download karo (sources jaise BreachForums ya dark web pe milte hain). Downloaded files ko VM ke andar transfer karo (drag-drop ya shared folder se).
6. **Search Karo:** Agent Ransack ya grep ka use karke files mein emails, phone numbers, ya addresses dhoondho. Example: Agent Ransack mein file folder select karo, "satyam" search karo, aur results dekho.

Kaise Kaam Karta Hai: Subscription services online hain aur instant results dete hain, jabki local download mein aapko data khud manage karna hota hai lekin aapka control zyada hota hai aur long-term cost nahi hai. Har finding ko notes mein save karo (Notion ya text file mein) taaki aapka research organized rahe.

Tools and Requirements

Category	Tool	Purpose
Subscription	DeHashed	Online Breach Search
Local Search	Agent Ransack	File Keyword Search
Download	qBittorrent	Torrent Downloads
VM Software	VirtualBox	Isolation

Point To Note

Isolated virtual environment set up karna breached databases ke saath kaam karne ka safe tareeka hai. Subscription services jaise DeHashed, IntelX, aur Snusbase quick aur easy hain, lekin paid hote hain. Local download ke liye Agent Ransack aur torrent client ka use karo, aur 50-100 GB disk space rakho. VM mein Ubuntu ya Windows chala ke data search karo – ye aapke main system ko protect karta hai. Dono methods ke apne fayde hain, to apni need ke hisaab se choose karo aur har detail ko note karte jao taaki OSINT thorough ho!

==========

Installing Needed Software to Manage Leaked Databases

Leaked databases ko manage karne ke liye sahi software install karna zaroori hai, aur iske liye bade disk space ki bhi zarurat hoti hai. **Note:** Kuch databases ka size bahut bada hota hai, jaise 50 GB ya 80 GB – example ke liye, **Facebook data leaks** ka size is range mein ho sakta hai. Ek leaked database ko possess karna subscription services se zyada affordable hai kyunki aapko database ek baar download karna hota hai, aur phir aap jab chahe usse access kar sakte ho bina recurring cost ke. Subscription mein har baar paise dene padte hain, lekin local database ke saath aapka control aur flexibility zyada hoti hai.

Needed Software aur Steps:

1. **Download Software – uTorrent:**
   - **Kya Hai:** uTorrent ek lightweight torrent client hai jo aapko torrent files ya magnet links se bade databases download karne deta hai. Ye free hai aur fast downloads ke liye popular hai.
   - **Kaise Karein:** Official website (utorrent.com) pe jao, "Free Download" pe click karo, installer run karo, aur setup complete karo. Install ke baad, torrent file ya magnet link add karke database download shuru karo. Example: Agar Facebook leak ka torrent mila, to usse uTorrent mein open karo aur 50-80 GB ka data save karne ke liye jagah rakho.
2. **Agent Ransack:**
   - **Kya Hai:** Ye ek free file search tool hai jo Windows pe chalta hai aur aapko ek ya multiple files ke andar specific data (jaise email, phone number, password)

dhoondhne deta hai. Ye bade text files, CSVs, ya database dumps ko quickly scan karta hai.

- **Kaise Install Karein:** FileHippo ya FileForum jaise trusted site se "Agent Ransack" download karo, installer run karo, aur "Next" dabate hue setup pura karo. Install hone ke baad, software kholo aur apne database folder ko select karke search shuru karo.
- **Agent Ransack Ke Baare Mein Zyada:** Ye tool normal Notepad ya dusre basic editors se kaafi better hai kyunki:
  - **Speed:** Notepad mein 50 GB ka file open karna almost impossible hai – wo hang ho jayega. Agent Ransack bade files ko handle kar sakta hai bina crash kiye.
  - **Search Power:** Notepad mein aapko manually scroll karke dhoondhna padta hai, jo time waste hai. Agent Ransack mein aap ek keyword (jaise "satyam@example.com") daal sakte ho, aur ye seconds mein saare matches dikhata hai.
  - **Multiple Files:** Agar aapke paas 10-20 files hain (jaise ek folder mein alag-alag breaches), to Agent Ransack ek saath sab mein search kar sakta hai, jabki Notepad mein ek-ek file kholni padti hai.
  - **Advanced Options:** Ye wildcards (*, ?) aur file type filters support karta hai. Example: "*.txt" select karke sirf text files search karo.
- **Notepad Ya Dusre Tools Kyun Nahi:** Notepad chhote files ke liye theek hai, lekin bade databases ke saath kaam nahi karta kyunki wo slow hai aur limited memory use karta hai. Dusre tools jaise Excel bhi bade CSVs ke saath crash ho sakte hain. Agent Ransack isliye best hai kyunki ye specifically searching ke liye banaya gaya hai aur large datasets ke saath efficient hai.

Kaise Use Karein: Database download karne ke baad (uTorrent se), us folder ko Agent Ransack mein open karo. Search bar mein apna target daalo (jaise email, name, ya phone number), aur "Search" pe click karo. Results mein aapko line-by-line matches milenge. Inhe copy karke apne notes mein save karo (Notion ya text file mein) taaki aapka OSINT research organized rahe.

Software for Managing Leaked Databases

Software	Purpose	Key Feature
uTorrent	Download Databases	Fast Torrent Downloads
Agent Ransack	Search Files	Handles Large Files

Point To Note

Leaked databases ko manage karne ke liye uTorrent aur Agent Ransack jaise software perfect hain. uTorrent se 50-80 GB jaise bade databases download karo, aur Agent Ransack se unmein data dhoondho – ye Notepad se zyada fast aur powerful hai kyunki bade files ko handle karta hai aur ek saath multiple files search karta hai. Ek baar database aapke paas ho, to subscription ke jhanjhat ke bina kabhi bhi access kar sakte ho. Bas disk space rakho aur har finding ko note karo taaki aapka kaam smooth chale!

==========

Downloading and Accessing Leaked Facebook Data

Attackers ne Facebook ke **contact importer feature** ka fayda uthaya aur iske through **500 million se zyada user profiles ka data scrape** kiya gaya. Ye ek bada data leak tha jisme sensitive info expose hui, jaise:

- **User IDs:** Har user ka unique identifier.
- **Phone Numbers:** Contact details jo target ke liye critical ho sakte hain.
- **Full Names:** Real names jo identity confirm karne mein madad karte hain.

Aur bhi details jaise locations, birthdates, ya emails bhi isme shamil ho sakte hain, depending on the leak. Ye data attackers ne collect kiya aur baad mein leak kar diya, jo ab publicly available hai.

Note: Ye data leak **2019** mein hua tha, yani isme Facebook user data **August 2019 tak ka** shamil hai kyunki uske baad Facebook ne is vulnerability ko fix kar diya tha. To jo bhi data isme hai, wo 2019 ke mid tak ke users ka hai.

Kaise Download Karein:

1. **Google Search:** "Facebook data leak GitHub" search karo.
2. **GitHub Repo:** Ek user **davidfegyver** ka repo milega jiska naam hai **facebook-533m**. Isme jao – ye ek public repository hai jahan leak ka data share kiya gaya hai.
3. **Magnet Link:** Repo mein ek **magnet link** milega jo torrent ke through database download karne ke liye hai. Ye link aisa dikhega: `magnet:?xt=urn:btih:0595273ab674e05131a757f69f4` `Leak [2019][533M Records][106 Countries]`.
4. **Torrent Client:** Apne system pe ek torrent client jaise **uTorrent** ya **qBittorrent** kholo (agar nahi hai to qbittorrent.org se download karo).
5. **Add Torrent:** Torrent software mein "Add Torrent" ya "Add Magnet Link" pe click karo, phir GitHub se mila magnet link paste karo, aur download start karo. Ye database bada hai – around 15-20 GB compressed, aur unzip hone pe 50-100 GB tak ho sakta hai, to bada disk space rakho.

Note: Download complete hone ke baad aapko ek folder milega jisme data **country-wise structured** hai, jaise "India", "China", "USA", etc. Agar aap "India" folder extract karte ho, to usme do files milengi – **india1.txt** aur **india2.txt**. In files mein data text format mein hai, jisme user IDs, phone numbers, names, etc. listed hote hain. Har file badi ho sakti hai (GBs mein), to manually har file kholke search karna mushkil hai. Iske liye:

- **Agent Ransack Ka Use:** In dono files ko ek saath search karne ke liye **Agent Ransack** best hai. Steps:
  1. India folder pe jao jahan ye files hain.
  2. Right-click karo, "Show More Options" pe jao, aur "Agent Ransack" select karo (pehle isko install karna hoga – filehippo.com se free download milta hai).

3. Agent Ransack khulne ke baad, search bar mein apna target daalo (jaise "Satyam Singh" ya "9876543210"), aur ye dono files (india1.txt aur india2.txt) mein ek saath search karke results dikhayega.

- **Agent Ransack Ki Khaasiyat:** Ye software isliye acha hai kyunki aapko har file ko alag-alag kholne aur manually search karne ki zarurat nahi padti. Ye bade text files ko fast scan karta hai aur ek hi baar mein saare matches dikhata hai, jo time aur effort bachata hai.

Extra Tips: Download karne se pehle ek virtual machine (jaise VirtualBox mein Ubuntu) set up karo taaki aapka main system safe rahe, kyunki leaked data mein malware ho sakta hai. Har finding ko notes mein save karo (Notion ya text file mein) taaki aapka OSINT research organized rahe.

Tools and Data Structure

Tool/Data	Purpose	Example
qBittorrent	Download Torrent	Magnet Link
Agent Ransack	Search Files	"Satyam Singh"
India Folder	Country Data	india1.txt, india2.txt

Point To Note

Facebook ka 2019 data leak, jisme 533 million users ka data scrape hua, ek bada source hai user IDs, phone numbers, aur names jaise details ke liye. Ise GitHub pe davidfegyver ke "facebook-533m" repo se magnet link ke through torrent se download karo. Country-wise data (jaise India ke liye india1.txt, india2.txt) ko Agent Ransack se easily search karo – ye manual searching se kai guna better hai. 2019 tak ka data hone ke wajah se ye old ho sakta hai, lekin phir bhi OSINT ke liye valuable hai. Bas safety ke liye VM use karo aur har detail note karo!

==========

Downloading and Accessing Leaked Twitter Data

Attackers ne Twitter ke ek **API ka misuse** kiya jisse unhone email addresses ko Twitter profiles ke saath match kiya. Is process mein **200 million se zyada Twitter profiles ka data scrape** kiya gaya. Ye ek massive data leak tha jisme kaafi sensitive info expose hui, jisko **compromised data** kehte hain, jaise:

- **Email Addresses:** Har user ka unique email jo doosre accounts se link ho sakta hai.
- **Names:** Full names ya aliases jo identity confirm karne mein madad karte hain.
- **Social Media Profiles:** Twitter handles ya related platforms ke links.
- **Usernames:** Twitter usernames jo online presence ko track karne ke liye useful hain.

Ye data 2021 mein ek API vulnerability ke through collect kiya gaya tha, jisko Twitter ne January 2022 mein fix kiya, lekin tab tak damage ho chuka tha. Is leak ko **Twitter 200M** ke naam se jaana jata hai kyunki cleaned-up version mein 200 million unique records hain (originally 400 million the, lekin duplicates hata diye gaye).

Kaise Download Karein:

1. **Google Search:** Google pe jao aur search karo: **"twitter 200m" "magnet:?"**. Ye search torrent links dhoondhne ke liye hai kyunki "200 million" is leak ka keyword hai aur "magnet:?" se magnet links filter hote hain.

2. **Torrent Link:** Search results mein forums ya sites (jaise BreachForums ya GitHub) pe magnet links mil sakte hain. Example magnet link aisa ho sakta hai: `magnet:?xt=urn:btih:0595273 200M Leak`.

3. **Torrent Client:** Ek torrent client jaise **uTorrent** ya **qBittorrent** use karo (qbittorrent.org se free download kar sakte ho). Client kholo, "Add Torrent" ya "Add Magnet Link" pe click karo, aur search se mila magnet link paste karke download start karo.

Note: Sabhi links kaam nahi karenge – kuch links dead hote hain ya fake hote hain. Kai baar download shuru hota hai, 1 GB tak jata hai, aur phir ruk jata hai kyunki seeders nahi hote. Isliye:

- Har link try karo jo search mein mile.
- Trusted sources (jaise BreachForums ya dark web posts) pe focus karo.
- File size check karo – Twitter 200M leak compressed mein 20-30 GB aur unzipped 60-100 GB tak ho sakta hai, to chhota file (1 GB) incomplete hoga.

Access Kaise Karein: Download hone ke baad, data country-wise ya ek bade text/CSV file mein milega. Isme search ke liye **Agent Ransack** jaise tool use karo – folder select karo, email ya username daalo, aur results dekho. Safety ke liye ek virtual machine (VirtualBox mein Ubuntu) pe kaam karo taaki malware se bacha ja sake. Har finding ko notes mein save karo (Notion ya text file mein) taaki aapka OSINT research systematic rahe.

Tools and Data Details

Tool/Data	Purpose	Example
qBittorrent	Download Torrent	Magnet Link
Agent Ransack	Search Files	"satyam@example.com"
Twitter 200M	Leaked Data	Email, Username

Point To Note

Twitter 200M leak, jisme attackers ne API misuse karke 200 million profiles scrape kiye, email addresses, names, aur usernames jaise data deta hai. Ise Google pe "twitter 200m" "magnet:?" search karke torrent se download karo, lekin sab links kaam nahi karenge – try multiple sources. qBittorrent se download karo aur Agent Ransack se access karo, lekin VM mein kaam karo safety ke liye. Ye leak OSINT ke liye valuable hai – bas patience rakho aur har detail note karo!

==========

Downloading and Accessing Leaked LinkedIn Database

LinkedIn ka ek bada data breach hua tha jisme 160+ million email addresses compromised hue the. Ye breach aur iska publicly available hona alag-alag saalon mein hua, aur isme sensitive info leak hui thi. Compromised data mein shamil tha:

- **Member IDs:** Har user ka unique identifier jo LinkedIn profile se juda hota hai.
- **Emails:** Users ke email addresses jo doosre accounts se link ho sakte hain.
- **Passwords:** Encrypted passwords jo breach ke time pe expose hue (2012 mein unsalted SHA-1 format mein the).

Occurred in Which Year: Ye breach **2012** mein hua tha. June 2012 mein Russian cybercriminals ne LinkedIn ke systems ko hack kiya aur initially 6.5 million passwords leak hue the. Baad mein May 2016 mein pata chala ki asal mein **167 million accounts** (117 million emails aur passwords ke saath) compromised hue the, jo pehle socha gaya tha usse kaafi zyada tha.

Publicly Available in Which Year: Ye data pehle dark web pe 2016 mein publicly sale ke liye aaya jab ek hacker "Peace" ne ise $2,200 (Bitcoin mein) ke liye offer kiya. Lekin full database **Internet Archive** pe (https://archive.org/details/LIUusers.7z) ke through baad mein freely available hua – ye exact saal clear nahi hai lekin typically 2016 ke baad hi aisa data public archives pe aata hai.

How to Download the Breached LinkedIn Database:

1. **URL Pe Jao:** Browser mein https://archive.org/details/LIUusers.7z kholo. Ye Internet Archive ki link hai jahan ye database **LIUusers.7z** naam se upload kiya gaya hai.
2. **Download Karo:** "Download Options" mein .7z file pe click karo (around 1-2 GB compressed ho sakta hai). Ise unzip karne ke liye 7-Zip jaise tool use karo – unzipped size 5-10 GB tak ho sakta hai.

Accessing the Database:

- Agar aap isme **name** se search karoge, to bahut saare results milenge kyunki names common ho sakte hain. Isliye **Member ID** se search karna zyada accurate hai kyunki ye unique hota hai.
- **Member ID Kaise Pata Karein:**
  1. Apne target ka LinkedIn profile kholo (e.g., linkedin.com/in/satyam-singh).
  2. Page pe right-click karo aur "View Page Source" select karo.
  3. Ctrl+F dabao aur "member" search karo – aapko code mein ek line milegi jahan Member ID dikhega, jaise `"memberId": "12345678"`. Ye 7-8 digit ka number hota hai.
- **Agent Ransack Mein Search:**
  1. Database unzip karne ke baad folder ko **Agent Ransack** mein kholo (pehle isko install karo – filehippo.com se free milta hai).
  2. Search bar mein Member ID daalo (e.g., "12345678") aur "Search" pe click karo.
  3. Ye aapko us specific user ka data dikhayega – email, password (hashed), aur member ID ke saath.

Note: Ye breached database **2012** ka hai, yani isme sirf woh LinkedIn users honge jo 2012 tak registered the. Iske baad (2013 ya uske aage) ke users isme nahi milenge kyunki ye data us time ka snapshot hai. Agar aapka target ne 2012 ke baad account banaya, to wo is database mein nahi hoga. Har finding ko notes mein save karo (Notion ya text file mein) aur safety ke liye virtual machine (jaise VirtualBox) pe kaam karo taaki malware risk na ho.

Tools and Data Details

Tool/Data	Purpose	Example
Internet Archive	Download Database	LIUusers.7z
Agent Ransack	Search Files	"12345678"
Member ID	Unique Identifier	"linkedin.com/in/satyam-singh"

Point To Note

LinkedIn ka 2012 breach, jisme 167 million accounts (160+ million emails aur passwords) compromised hue, 2016 mein dark web pe publicly available hua aur ab Internet Archive (https://archive.org/details/LIUusers.7z) se download ho sakta hai. Member ID se Agent Ransack mein search karo kyunki ye unique hai – 2012 tak ke users hi isme milenge. Data download aur access karte waqt VM use karo aur har detail note karo taaki OSINT smooth aur safe rahe!

==========

Downloading and Accessing Leaked Snapchat Data

Attackers ne Snapchat ke ek **API ka misuse** kiya jisse unhone usernames ko phone numbers ke saath resolve kiya. Is process mein **6+ million records** ka data leak hua tha. Ye ek chhota lekin significant breach tha jisme **compromised data** shamil tha:

- **Phone Numbers:** Users ke contact numbers jo identity ya location tracking ke liye useful hain.
- **Usernames:** Snapchat usernames jo unke social media presence ko connect kar sakte hain.

Note: Ye data breach **2014** mein hua tha. August 2014 mein, SnapSaved naam ke ek third-party app ne Snapchat ke API ka galat istemaal kiya aur 4.6 million se zyada usernames aur phone numbers leak kiye. Ye data baad mein publicly share kiya gaya tha, aur iska ek version Internet Archive pe available hai. Yani, isme 2014 tak ke Snapchat users ka data hi hoga.

How to Download the Database:

- **Link:** Jao https://archive.org/details/SnapChat.7z pe. Ye Internet Archive ki link hai jahan **SnapChat.7z** naam se database upload kiya gaya hai.

- **Download Karo:** "Download Options" mein .7z file pe click karo. Ye file chhoti hai – around 100-200 MB compressed – aur unzip karne pe 500 MB tak ho sakti hai. 7-Zip ya WinRAR jaise tool se extract karo.

- **Access Karo:** Extracted folder mein text files ya CSV honge jisme phone numbers aur usernames listed hain. **Agent Ransack** mein folder kholo aur specific username ya number search karo (e.g., "satyam123").

Note: Agar aapko kisi tarah se user ka email mil jata hai aur uske phone number ke last two digits nahi dikh rahe hain (e.g., satyamgrandmaster@gmail.com – Number: 72505850xx), to poora number pata karne ka tareeka:

- **Social Media Pe Check:** Facebook ya koi aur platform (jaise Instagram, LinkedIn) pe jao jahan ye email registered ho sakta hai. Target ka profile dhoondho.

- **Forgot Password Trick:** Profile pe "Forgot Password" pe click karo. Email (satyamgrandmaster@gmail.com) daalo aur "Send OTP" ya "Forgot Link" option choose karo jo phone number pe jata hai.

- **Number Verify:** Platform aapko ek masked number dikhayega jisme last two digits visible honge, jaise "xxxxxxxx57". Ab aapke paas partial number (72505850xx) tha, aur last digits (57) milne se full number ban jata hai: **7250585057**. Is tarah aap 10-digit number recover kar sakte ho.

Extra Tips: Ye database 2014 ka hai, to isme sirf us time tak ke users honge. Download aur access ke liye virtual machine (VirtualBox mein Ubuntu) use karo taaki malware risk na ho. Har finding ko notes mein save karo (Notion ya text file mein) taaki aapka OSINT research organized rahe.

Tools and Data Details

Tool/Data	Purpose	Example
Internet Archive	Download Database	SnapChat.7z
Agent Ransack	Search Files	"satyam123"
Phone Number	Recover Full Number	7250585057

Point To Note

Snapchat ka 2014 leak, jisme 6+ million records (phone numbers aur usernames) compromised hue, https://archive.org/details/SnapChat.7z se download ho sakta hai. Attackers ne API misuse kiya tha, aur ye data chhota lekin useful hai. Agar number ke last digits missing hain (jaise 72505850xx), to Facebook ke "Forgot Password" trick se poora number (e.g., 7250585057) pata karo. 2014 tak ka data hone ke wajah se ye limited hai, lekin OSINT ke liye kaam aa sakta hai – VM use karo aur har detail note karo!

==========

Finding Leaked Databases on the Internet

Internet pe leaked databases dhoondhna OSINT ke liye ek powerful method hai kyunki ye sensitive info jaise emails, passwords, aur phone numbers reveal kar sakta hai. Ek effective tareeka hai specific **search operators ya queries** ka use karna. Example ke liye, agar aapko **000webhost** ka leaked database chahiye, to Google pe ye query daalo: **"000webhost.com.7z" "leak" "download" "magnet:?"**. Ye query .7z files (compressed format), leak-related terms, aur magnet links (torrent ke liye) target karti hai. Isse aapko us database ka magnet link mil sakta hai jo torrent ke through download ho sakta hai.

Website Jahan Se Magnet Link Milega:

- **sizeof.cat:** Ye ek website hai jo number of leaked databases aur unke magnet links ka collection rakhti hai. Ispe aapko kaafi breaches ke details milenge, jaise:
  - **AMD:** Chip manufacturer ka data leak.
  - **Database from RaidForums 2020:** Ye ek massive collection hai jiska size **427.63 GB** hai, aur isme bahut saare databases shamil hain jaise **Vodafone, Airtel, LinuxMint.com**, aur aur bhi. Iska magnet link sizeof.cat pe available hai, jo torrent client (jaise qBittorrent) mein paste karke download kar sakte ho.

Note: RaidForums 2020 database ek bada dump hai jisme multiple companies aur services ke leaks shamil hain. Isme Vodafone (telecom data), Airtel (Indian telecom), aur LinuxMint.com (open-source OS community) jaise datasets hote hain. Magnet link aisa dikhta hai: `magnet:?xt=urn:btih:[hash]&dn=RaidForums2020&tr=[tracker URLs]`. Ye link torrent ke through 427.63 GB ka data download karta hai, to bada disk space (500 GB+ recommended) aur fast internet chahiye.

Note: Agar sizeof.cat pe diya gaya link kaam nahi karta (jaise seeders na hone ki wajah se download ruk jaye), to aapko usi database ke liye doosra link dhoondhna pad sakta hai. Google pe alag queries try karo jaise **"RaidForums 2020 leak magnet link"** ya dark web forums (jaise BreachForums ke archives) pe check karo. Har link ko test karo aur jo kaam kare usse download shuru karo.

Kaise Use Karein: Database download hone ke baad, **Agent Ransack** jaise tool se extract karke search karo (specific email ya phone number ke liye). Safety ke liye virtual machine (VirtualBox mein Ubuntu) pe kaam karo taaki malware risk na ho. Har finding ko notes mein save karo taaki aapka research organized rahe.

Sources and Databases

Source/Database	Details	Size
sizeof.cat	Magnet Links	Varies
RaidForums 2020	Vodafone, Airtel, LinuxMint	427.63 GB
000webhost	Web Hosting Leak	Varies

Point To Note

Leaked databases jaise 000webhost ya RaidForums 2020 ko dhoondhne ke liye **"000webhost.com.7z" "leak" "download" "magnet:?"** jaise search queries use karo. **sizeof.cat** jaise websites pe magnet links milte hain – RaidForums 2020 ka 427.63 GB database Vodafone, Airtel, LinuxMint jaise leaks ke saath ek example hai. Agar link dead ho, to alternate sources try karo. Ye method OSINT ke liye zabardast hai – bas VM use karo aur har detail note karo taaki safe aur effective rahe!

==========

Extracting Valuable Info from a Facebook Profile

Facebook OSINT ke liye ek shandaar source hai kyunki iska **vast user base** hai – 3 billion se zyada monthly active users (2024 tak) – aur yahan se profile info aur publicly accessible content easily mil sakta hai. Facebook pe log apni zindagi ke details share karte hain, jo target ke baare mein valuable info dene mein madad karta hai. Public profiles, posts, comments, aur photos se aap kaafi kuch uncover kar sakte hain agar aap dhyan se dekhein.

Note: Facebook mein **filters** ka option hota hai jo info ko refine karne mein kaam aata hai. Example ke liye, aap search bar mein target ka naam daalkar filters laga sakte ho jaise:

- **City:** Target kahan rehta hai ya kahan se hai (e.g., "Satyam Singh" + filter "Patna").
- **Education:** School ya college ka naam (e.g., "Satyam Singh" + filter "IIT Delhi").

Ye filters "People" tab mein milte hain jab aap search karte ho – inka use karke aap specific person ko narrow down kar sakte ho agar naam common hai.

Note: Target ke Facebook profile se aapko **doosre social media links** bhi mil sakte hain. Kaafi log apne "About" section mein ya posts mein apne connections share karte hain, jaise:

- **Instagram Link:** "Follow me on Insta @satyam123" ya bio mein direct link.
- **GitHub Link:** Developers aksar apne projects ke links daalte hain (e.g., github.com/satyamdev).
- Aur bhi platforms jaise Twitter, LinkedIn, ya Snapchat ke hints mil sakte hain. Isse aap target ke online presence ko expand kar sakte ho.

Date of Birth (DOB) Kaise Pata Karein: Facebook se DOB nikalna bhi possible hai agar target ne directly ya indirectly reveal kiya ho. Example:

- Agar target ne ek birthday pic post ki aur likha "Celebrating my 25th birthday" aur ye post 2024 ka hai, to aap calculate kar sakte ho:
  - 2024 - 25 = **1999**.
  - Agar post ki date hai 15th March 2024, to DOB hai **15th March 1999**.
- Ya phir "About" section mein "Birthday" public ho to wahan se direct mil sakta hai (e.g., "March 15").

Kaise Kaam Karein: Target ka profile kholo, "About" section check karo (Info, Contact, Education, Work), posts scroll karo, aur photos dekho. Comments mein bhi clues mil sakte hain jaise friends ke tags ya location check-ins. Har detail – jaise city, DOB, social media links – ko notes mein save karo (Notion ya text file mein) taaki aapka research organized rahe aur aage ke steps ke liye base ban sake.

Extractable Info from Facebook

Info Type	Source	Example
City	Filters/About	"Patna"
Education	Filters/About	"IIT Delhi"
DOB	Posts/About	"15th March 1999"
Social Media	About/Posts	"@satyam123" (Insta)

Point To Note

Facebook ek goldmine hai OSINT ke liye – iske bade user base aur public content se city, education, DOB, aur doosre social media links (Instagram, GitHub) jaise details mil sakte hain. Filters ka use karke search ko refine karo, aur posts ya "About" section se DOB jaise info nikalo (e.g., 25th birthday in 2024 = 1999). Ye sab info target ke online footprint ko badhane mein madad karta hai – bas har cheez ko carefully note karo aur systematically kaam karo!

==========

Extracting User ID, Facebook Friends, and More

Har Facebook user ka ek **unique identifier** hota hai jo uske profile banne ke waqt generate hota hai, jise **User ID** kehte hain. Ye ek number hota hai, jaise **100030303000**, aur har user ke liye alag hota hai. **Reason:** User ID isliye unique hota hai kyunki ye Facebook ke database mein har account ko distinctly identify karta hai, chahe user apna username change kar le. Isse aap target ko track kar sakte ho chahe unka public-facing username ya URL badal jaye.

Steps to Search User ID Manually:

1. **Profile Page Kholo:** Apne target ka Facebook profile page pe jao (e.g., facebook.com/satyam.singh)
2. **View Page Source:** Page pe kisi blank area pe right-click karo, "View Page Source" select karo – ye HTML code kholega.
3. **User ID Search Karo:** Ctrl+F (ya Cmd+F Mac pe) press karo, aur "userID" ya "entity_id" search karo. Aapko ek number milega jaise `"userID": "100030303000"`. Ye target ka User ID hai.
4. **Verify Karo:** User ID ko https://facebook.com/[userID] mein paste karke check karo (e.g., https://facebook.com/100030303000). Agar profile khulta hai, to ID sahi hai.

Use of User ID: Agar target ne username change kiya ho (e.g., facebook.com/satyam.singh se facebook.com/satyam123), tab bhi User ID se aap unhe dhoondh sakte ho kyunki ID kabhi nahi badalta. Username ki jagah User ID URL mein daal do, aur profile access ho jayega.

Note: Apne target ke OSINT notes mein User ID zaroor save karo kyunki ye permanent identifier hai aur future tracking ke liye kaam aayega. Notion mein notes banate waqt User ID ko ek column ya field mein add karo.

Account Creation Date Pata Karna: User ID se aap account creation year bhi estimate kar sakte ho. Google pe search karo **"user ID to account creation date"** aur target ka User

ID paste karo. Kai websites ya forums (jaise learnallthethings.net) User ID ranges aur years ka chart dete hain:

- **Example:**
  - 100000000 - 100999999: 2004-2006
  - 1000000000 - 2000000000: 2007-2009
  - 100030303000: 2010s ke mid tak
- Agar User ID "100030303000" hai, to ye shayad **2012-2014** range mein bana hoga. Exact date nahi milega, lekin year range ka idea ho sakta hai.

Automatic Way to Find User ID:

1. **Google Search:** "Find Facebook ID from Facebook profile" search karo.
2. **Website – FindidFB.com:** Ye ek free tool hai. Ispe jao, target ka profile URL (e.g., facebook.com/satyam.singh) paste karo, aur "Find ID" pe click karo. Ye instantly User ID dikhayega (e.g., 100030303000). Ye manual method se faster hai aur beginners ke liye easy hai.

Note: Notion notes mein PDF embed ya attach karne ke liye:

- Notion page pe jao, type karo **/pdf**, "Embed a PDF" option select karo, aur file upload karo ya link daalo. Ye OSINT notes ko rich banata hai – jaise target ke profile screenshot ya leaked data PDF ko attach kar sakte ho.

Extra Tips: User ID ke saath target ke friends list bhi check karo agar public hai – "Friends" tab pe jao aur connections note karo. Ye doosre social links ya relationships dikhata hai. Har detail – User ID, DOB, friends – ko Notion mein save karo taaki aapka research complete rahe.

Extractable Info and Tools

Info/Tool	Purpose	Example
User ID	Unique Identifier	"100030303000"
FindidFB.com	Find User ID	facebook.com/satyam.singh
Creation Date	Estimate Year	"2012-2014"
Friends List	Connections	Public List

Point To Note

Facebook User ID ek unique aur permanent identifier hai jo manually (page source se) ya automatically (FindidFB.com se) mil sakta hai. Ise https://facebook.com/[userID] se verify karo aur OSINT notes mein rakho. User ID se account creation year range (e.g., 2012-2014) bhi pata chal sakta hai, aur friends list se extra connections mil sakte hain. Notion mein /pdf se docs embed karo – ye sab target ke baare mein deep info deta hai. Bas systematically kaam karo aur har clue save karo!

==========

Uncovering Emails and More from a Facebook Profile

Facebook ke **"Forgot Password" feature** ka use karke aap target ke account se linked contact info uncover kar sakte ho, jaise email aur phone number ke hints. Ye OSINT ke liye ek smart trick hai kyunki Facebook security ke liye partial details dikhata hai, jo verification mein kaam aate hain.

Kaise Karein:

- **Forgot Password Pe Jao:** Target ka Facebook profile kholo (e.g., facebook.com/satyam.singh), aur "Forgot Password" ya "Forgot Account" pe click karo.
- **Details Dekho:** Aapko ek screen milegi jahan code bhejne ke options honge, jaise:
  - **Email:** "Send code on s***r@gmail.com" – iska matlab email "s" se start hota hai aur "r" pe end hota hai (e.g., satyamgrandmaster@gmail.com ho sakta hai).
  - **Number:** "***..57" – yani phone number ke last two digits "57" hain (e.g., 7250585057 ho sakta hai).
- **Verification:** Agar aapke paas pehle se target ka phone number (jaise 7250585057) ya email (jaise satyamgrandmaster@gmail.com) hai, to in partial details se verify kar sakte ho ki ye sahi hai ya nahi. Example: Agar number ke last digits match karte hain (57) aur email ka pattern fit hota hai (s se shuru, r pe khatam), to aap sure ho sakte ho ki ye target ka hai.

Email Confirm Kaise Karein:

- **Find My Account:** Facebook ke login page pe "Find My Account" ya "Forgot Password" pe jao.
- **Email Daalo:** Wahan target ka suspected email daalo (e.g., satyamgrandmaster@gmail.com).
- **Result Check Karo:** Agar ye email target ke account se match karta hai, to Facebook uska profile dikhayega (naam ya photo ke saath). Agar profile target ka nahi hai ya kuch nahi dikhata, to wo email uska nahi hai. Ye ek solid tareeka hai email verification ke liye.

Fayde:

- Partial email (s***r@gmail.com) se aap guess kar sakte ho – jaise agar target ka naam Satyam hai, to "satyamgrandmaster" try kar sakte ho.
- Partial number (***..57) se aap poora number confirm kar sakte ho agar aapke paas pehle se koi lead hai.
- Ye info doosre platforms (Instagram, LinkedIn) pe cross-check karne ke liye bhi use ho sakti hai.

Extra Tips: Agar target ka profile public hai, to "About" section mein bhi email ya number ke hints mil sakte hain (jaise "Contact" tab mein). Har detail – email pattern, number digits – ko notes mein save karo (Notion mein) taaki aapka OSINT research organized rahe aur aage ke steps ke liye base ban sake.

Uncoverable Info from Facebook

Info Type	Source	Example
Email Hint	Forgot Password	"s***r@gmail.com"
Number Hint	Forgot Password	"***..57"
Full Email	Find My Account	"satyamgrandmaster@gmail.com"

Point To Note

Facebook ka "Forgot Password" feature target ke email (e.g., s***r@gmail.com) aur phone number (e.g., ***..57) ke hints deta hai, jo verification ke liye kaafi hai. "Find My Account" se email confirm karo – agar target ka profile milta hai, to email sahi hai. Ye trick simple hai lekin powerful, kyunki partial details se aap poori info guess ya verify kar sakte ho. Har clue ko Notion mein note karo aur systematically kaam karo taaki target ke baare mein zyada se zyada pata chal sake!

==========

Finding Comments/Tags of a Facebook Profile

Facebook profile ke comments aur tags dhoondhne ke liye **search engine operators** ka use karna kaafi useful hai kyunki ye publicly indexed content ko locate karne mein madad karta hai. Ek acha dork hai: **"Name" site:facebook.com inurl:posts**. Isse aap target ke naam ke saath Facebook posts ko search kar sakte ho jo search engines ne index kiya ho. Example: **"Rishi Kabra" site:facebook.com inurl:posts** – ye Google, Bing, ya Yandex pe Rishi Kabra ke public comments ya tagged posts dikhayega agar wo available hain. Ye tab kaam karta hai jab target ka profile ya unke comments public hote hain.

Note: Agar target ka profile public tha aur unhone kisi public post pe comment kiya ho, to Google, Bing, ya Yandex jaise search engines ne us comment ko index kiya ho sakta hai. Aapko comment ke saath post ka link milega, aur wahan se aap target ke activity ya connections ke baare mein info le sakte ho. Example: "Rishi Kabra" ka comment ek public group post pe mila – "Great event in Mumbai!" – isse location aur interest ka hint milta hai.

Steps to Dig Deeper:

- **Filter Use Karo:** Search results mein "People" filter laga ke target ka profile confirm karo.
- **Profile Picture Save Karo:** Profile pic download karo taaki aap target ko visually identify kar sakein ya image search (Google Lens) ke through aur info dhoondh sakein.
- **Username Check Karo:** Profile URL se username note karo (e.g., facebook.com/rishi.kabra).
- **User ID Find Karo:** Profile pe right-click karo, "View Page Source" pe jao, Ctrl+F se "userID" search karo (e.g., "100030303000"). Ye unique ID hai jo kabhi nahi badalta.
- **Account Creation Date:** User ID ko Google pe search karo "Facebook ID creation date" ke saath – ranges se pata chal sakta hai ki account kab bana (e.g., 100030303000 shayad 2012-2014 ka hai).

- **Review All Posts:** Profile pe "Posts" tab check karo – public posts, tags, ya comments se info lo.
- **Public Friend List Save Karo:** Agar friend list public hai, to names ya connections note karo – ye target ke network ko expand karta hai.
- **Forgot Password Feature:** "Forgot Password" pe click karo – email (e.g., r***i@gmail.com) ya number (e.g., ***..57) ke hints milenge. Ye verify karne mein help karta hai agar aapke paas pehle se info hai.
- **Search Operator for Public Info:** Dork jaise "Rishi Kabra site:facebook.com" ya "Rishi Kabra site:facebook.com inurl:groups" use karo taaki groups, pages, ya aur public info mile.

Kaise Kaam Karein: Har step ko follow karo – search operator se comments/tags dhoondho, profile details verify karo, aur extra info (DOB, friends, email hints) collect karo. Sab kuch Notion mein save karo taaki aapka OSINT research organized rahe aur ek complete picture ban sake.

Methods and Extractable Info

Method/Info	Purpose	Example
Search Dork	Find Comments/Tags	"Rishi Kabra" site:facebook.com inurl:posts
User ID	Unique Identifier	"100030303000"
Email Hint	Contact Info	"r***i@gmail.com"
Friend List	Connections	Public Names

Point To Note

Facebook ke comments aur tags dhoondhne ke liye **"Name" site:facebook.com inurl:posts"** jaise dorks kaam aate hain, jo public indexed content dikhate hain. Agar profile public hai, to Google, Bing, ya Yandex se comments mil sakte hain. Filters, User ID, friend list, aur "Forgot Password" se aur details (email, number) lo. Ye sab target ke baare mein deep info deta hai – bas har cheez ko Notion mein note karo aur systematically kaam karo taaki kuch miss na ho!

==========

Extracting the User ID of an Instagram Account

Instagram OSINT ke liye ek bada platform hai kyunki iske **1 billion se zyada monthly active users** hain (2024 tak), aur yahan users sirf **photos aur videos** share kar sakte hain. Ye limitation ke bawajood kaafi info deta hai agar aap dhyan se kaam karo. Hum Facebook OSINT jaise hi steps follow karenge, lekin Instagram ke liye thoda tweak karenge:

1. **Profile Pic Save Karo:** Target ke profile pe jao, profile picture save karo. Isse aap baad mein Google Lens ya reverse image search ke through aur info (jaise location ya events) dhoondh sakte ho.

2. **URLs aur Usernames Copy Karo:** Profile URL (e.g., instagram.com/satyam123) aur username note karo. Bio mein agar doosre social media links hain (jaise Twitter, GitHub), unhe bhi apne notes mein daalo.

3. **Screenshot Save Karo:** Profile section ka screenshot lo – username, bio, posts count, followers/following ke saath – aur ise Notion mein save karo taaki visual record rahe.

Note: Instagram pe OSINT ke liye ek **dummy account** banana important hai, khaaskar agar target ka account private hai. Example: Agar target Kolkata se hai aur SRM University se padha hai, to ek dummy account banao jisme location "Kolkata" aur education "SRM University" daalo. Bio mein similar interests add karo (jaise "Kolkata foodie" ya "SRM alum"). Phir target ko follow request bhejo – same background hone se accept hone ke chances badh jaate hain. Request accept hone ke baad aap unke posts, stories, aur tags dekh sakte ho, jo private account ke case mein nahi dikhte.

User ID Kaise Nikalein: Har Instagram user ka ek **unique identifier** hota hai jo profile banne pe generate hota hai, jise **User ID** ya **profile_id** kehte hain (e.g., 49279209744). Ye number har account ke liye alag hota hai. Steps:

1. **User Profile Kholo:** Target ka Instagram profile pe jao (e.g., instagram.com/satyam123).

2. **View Page Source:** Page pe blank area pe right-click karo, "View Page Source" select karo – ye HTML code kholega.

3. **Profile ID Search Karo:** Ctrl+F press karo aur "profile_id" search karo. Aapko code mein ek line milegi jaise `"profile_id": "49279209744"`. Ye target ka User ID hai.

Note: User ID kyun important hai? Agar target ne username change kar diya (satyam123 se satyam_dev), profile pic badli, ya aur details update kiye, to bhi User ID se aap unhe track kar sakte ho kyunki ye kabhi nahi badalta. Example: https://instagram.com/[user_id] (jaise instagram.com/49279209744) daalne se profile mil sakta hai agar direct access possible ho. Isliye User ID ko apne Notion notes mein zaroor save karo – ye ek permanent marker hai target ka.

Extra Tips: Dummy account se posts, stories, aur tagged photos check karo agar access milta hai. Bio mein email ya location hints bhi dhoondho. Har detail – User ID, username, screenshot – ko Notion mein organize karo taaki aapka research complete aur future-proof rahe.

Extractable Info and Methods

Info/Method	Purpose	Example
Profile Pic	Reverse Search	Google Lens
User ID	Unique Identifier	"49279209744"
Username	Profile URL	"instagram.com/satyam123"
Dummy Account	Private Access	"Kolkata foodie"

Point To Note

Instagram ke 1 billion+ users ke saath OSINT ke liye bada scope hai – profile pic save karo, URLs note karo, aur screenshot lo. Private account ke liye Kolkata ya SRM jaise details ke saath dummy account banao taaki request accept ho. **User ID** (e.g., 49279209744) profile source se nikalo – ye username change hone pe bhi target ko track karta hai. Ye sab info Notion mein save karo aur systematically kaam karo taaki target ke baare mein maximum details milein!

==========

Extracting Timestamps from Posts and Comments

Timestamps se aap exact date aur time pata kar sakte ho jab koi post ya comment kiya gaya tha, aur ye OSINT ke liye kaafi helpful hai kyunki isse target ke activity patterns samajh mein aate hain. Timestamp ka format hota hai jaise **yyyy:mm:dd 'T' hh:mm:ss** (e.g., 2024:04:02 T 15:30:45), jo year, month, day, aur time (24-hour format) dikhata hai. Ye method social media platforms jaise Facebook, Instagram, ya Twitter pe **posts aur comments** dono pe kaam karta hai agar platform timestamp data expose karta hai.

Steps to Extract Timestamp:

1. **Post ya Comment Pe Jao:** Target ke profile ya page pe jao aur jis post ya comment ka timestamp chahiye, uspe focus karo. Example: Ek comment hai "Nice pic!" aur uske niche "2 days ago" likha hai.

2. **Right Click aur Inspect:** Post ya comment pe right-click karo, "Inspect" ya "Inspect Element" select karo – ye browser ka developer tools kholega (Chrome, Firefox pe kaam karta hai).

3. **Date Locate Karo:** Inspector mein HTML code mein wahan jao jahan date dikh rahi hai (jaise "2 days ago"). Aapko ek `<time>` tag milega ya "datetime" attribute, jisme exact timestamp hota hai. Example: `<time datetime="2024-04-02T15:30:45Z">2 days ago</time>`. Isme "2024-04-02T15:30:45Z" pura timestamp hai – yani 2 April 2024, 3:30:45 PM UTC.

Kaise Kaam Karta Hai:

- Agar post pe "2 days ago" likha hai aur aaj 4 April 2024 hai, to inspect karne pe aapko "2024-04-02" milega, jo exact posting date hai.

- Comments ke liye bhi same step – comment pe inspect karo, aur `<time>` tag mein pura timestamp milega.

- "Z" ka matlab hai UTC time, to apne local time zone ke hisaab se adjust karo (e.g., India ke liye +5:30 hours add karo – 15:30:45 UTC + 5:30 = 21:00:45 IST).

Fayde:

- Timestamp se aap pata kar sakte ho ki target kab active tha, kahan tha (agar post mein location tag hai), ya us waqt kya kar raha tha.

- Patterns banaye ja sakte hain – jaise har Sunday ko 8 PM pe post karta hai, to routine ka hint milta hai.

Extra Tips: Timestamp ko Notion mein save karo – post/comment ke saath date aur time note karo (e.g., "Post: Nice pic! – 2024:04:02 T 15:30:45"). Agar multiple posts/comments check kar rahe ho, to timeline banane ke liye spreadsheet mein daal do. Har detail ko organize karo taaki aapka OSINT research clear aur useful rahe.

Timestamp Extraction Details

Element	Source	Example
Post Timestamp	Inspect Element	"2024-04-02T15:30:45Z"
Comment Timestamp	Inspect Element	"2024-04-02T15:30:45Z"
Local Time	Adjust UTC	"21:00:45 IST"

Point To Note

Timestamps se posts aur comments ka exact date-time (jaise 2024:04:02 T 15:30:45) pata chal sakta hai, jo target ke behavior ko samajhne mein madad karta hai. Right-click karke "Inspect" se `<time>` tag mein pura timestamp nikalo – ye simple hai aur kaafi platforms pe kaam karta hai. Ye info activity patterns banane ke liye perfect hai – bas har timestamp ko Notion ya spreadsheet mein save karo aur systematically kaam karo taaki OSINT strong bane!

==========

Uncovering Hidden Information from Instagram Metadata

Instagram ke **metadata** se hidden information nikalna OSINT ke liye ek zabardast tareeka hai kyunki ye chhupi hui details reveal kar sakta hai jo normal dekhte waqt nazar nahi aati. **Account metadata** mein kaafi useful info hoti hai, aur iske liye aapko **browser extension** jaise **User-Agent Switcher and Manager** ka use karna pad sakta hai taaki Instagram ke servers se zyada data extract kar sakein. Metadata mein juicy info mil sakti hai jaise:

- **Instagram Linked to User Profile:** Pata chal sakta hai ki account kisi Facebook profile se connected hai ya nahi.
- **Facebook Profile Link:** Agar linked hai, to shayad direct Facebook profile ka hint ya ID mil jaye.

Aur Juicy Info Kya Mil Sakti Hai:

- **Device Info:** Metadata se pata chal sakta hai ki post kis device se bana – jaise iPhone 14 ya Samsung Galaxy S23 – jo target ke tech preferences dikhata hai.
- **Timestamp:** Exact date aur time jab photo ya video upload hua (e.g., 2024:04:02 T 15:30:45), jo activity pattern banane mein madad karta hai.

- **Location Data:** Agar geotagging on hai, to latitude/longitude coordinates mil sakte hain (e.g., 28.7041° N, 77.1025° E – Delhi), jo exact location reveal karta hai.
- **App Version:** Konsa Instagram version use hua (e.g., Instagram 275.0.0), jo user ke update habits dikhata hai.
- **Camera Settings:** Photo ke EXIF data mein shutter speed, ISO, ya lens info ho sakta hai, jo professional ya casual use ka hint deta hai.

Lekin dhyan rakho – Instagram aksar metadata strip kar deta hai jab photo upload hoti hai, to ye info sirf tab milti hai jab raw data access ho ya third-party tools use kiye jayein.

Steps to Uncover Metadata Step-by-Step:

1. **Target Profile Pe Jao:** Instagram pe target ka profile kholo (e.g., instagram.com/satyam123).
2. **Post Select Karo:** Ek specific post ya photo choose karo jiska metadata check karna hai.
3. **User-Agent Switcher Install Karo:** Chrome ya Firefox pe "User-Agent Switcher and Manager" extension add karo (Chrome Web Store ya Mozilla Add-ons se milta hai). Ye extension browser ko Instagram ke mobile app jaise behave karne deta hai.
   - Install karne ke baad: Extension kholo, Instagram ka user-agent select karo (e.g., "Instagram 275.0.0.23.98 Android").
   - "Apply" pe click karo taaki browser ka user-agent change ho jaye.
4. **Page Reload Karo:** Target profile ya post ko refresh karo – ab Instagram server ko lagega ki aap mobile app se access kar rahe ho, aur zyada data expose ho sakta hai.
5. **View Page Source:** Post pe right-click karo, "View Page Source" select karo – ye HTML code kholega.
6. **Metadata Search Karo:** Ctrl+F se keywords search karo jaise:
   - "profile_id" (User ID ke liye, e.g., 49279209744).
   - "taken_at_timestamp" (Unix timestamp jo post ka exact time deta hai).
   - "location" (Agar geotag hai to coordinates ya place ID).
   - "fbid" (Facebook link ka hint).

   Example: `"taken_at_timestamp": 1712069445` – isse convert karo (online Unix timestamp converter se) to 2024:04:02 T 15:30:45.
7. **Photo Download Karo:** Post ki image save karo (right-click ¿ Save Image As), aur EXIF data check karo (tools jaise Jeffrey's EXIF Viewer – exif.tools – pe upload karke). Agar metadata strip nahi hua, to location ya device info milega.
8. **Cross-Check Karo:** Facebook link ya User ID ko doosre platforms pe verify karo (e.g., facebook.com/[fbid]).

Note: User-Agent Switcher se Instagram ke mobile API endpoints tak access mil sakta hai (jaise https://i.instagram.com/api/v1/users/[user_id]/info/), lekin ye kaam karega tabhi jab aap logged-in ho ya API public ho. Har finding – User ID, timestamp, location – ko Notion mein save karo taaki aapka research organized rahe.

Extractable Metadata Details

Metadata Type	Source	Example
Timestamp	Page Source	"2024:04:02 T 15:30:45"
Location	EXIF/GeoTag	"28.7041° N, 77.1025° E"
Device Info	Metadata	"iPhone 14"
User ID	Page Source	"49279209744"

Point To Note

Instagram metadata se hidden info jaise Facebook link, User ID, location, aur device details mil sakte hain, jo OSINT ke liye kaafi juicy hai. **User-Agent Switcher and Manager** ke saath browser ko mobile app jaisa banao, page source se timestamp ya ID nikalo, aur EXIF tools se photo metadata check karo. Ye steps target ke baare mein deep insights dete hain – bas har detail ko Notion mein note karo aur carefully kaam karo taaki kuch miss na ho!

==========

Scraping Instagram Followers

Instagram followers ko scrape karna OSINT ke liye ek acha tareeka hai, lekin ye method tab **kaam nahi karega agar target ne aapka follow request accept nahi kiya ho**. Agar target ka profile private hai aur aapko access nahi mila, to aap unke followers ya posts nahi dekh sakte. Private accounts ke case mein Instagram sirf basic info (jaise username, bio, aur profile pic) dikhata hai, lekin followers list chhupi rehti hai jab tak aapko permission na mile. Isliye pehle target ke saath connection banana zaroori hai.

Chrome Extension – IG Followers Export Tool (IG-Tools): Ye ek popular extension hai jo Instagram followers aur following ko scrape karke export karne mein madad karta hai. Lekin sawal ye hai – **kya ye extension private accounts ke liye bhi kaam karta hai?** Jawab hai **nahi** – ye extension bhi private accounts ke followers ko scrape nahi kar sakta agar aap target ke approved followers mein nahi ho. Ye tool sirf **public accounts** ya un private accounts pe kaam karta hai jinke aap already follower ho (matlab request accept ho chuki ho). Extension ke developers ke hisaab se, ye Instagram ke API limits ke andar kaam karta hai aur sirf wahi data deta hai jo aapke account ko visible hai.

Steps to Use IG Followers Export Tool:

1. **Login to Your Account:** Apne Instagram account mein login karo jis browser mein extension install hai (e.g., Chrome). Ye zaroori hai kyunki tool aapke logged-in session se data fetch karta hai.

2. **Extension Open Karo:** Chrome ke toolbar mein "IG Followers Export Tool" ya "IG-Tools" icon pe click karo – ye extension ka popup kholega.

3. **Export Instagram Data:** Popup mein "Export Instagram Data" button pe click karo – ek naya page ya section khulega jahan aap details daal sakte ho.

4. **Username ya URL Daalo:** Target ka Instagram username (e.g., "satyam123") ya profile URL (e.g., instagram.com/satyam123) type karo.

5. **Start New Parsing:** "Start New Parsing" ya "Export" button pe click karo – tool ab data scrape karna shuru karega aur followers list fetch karega.

Example Output ya Result: Agar target ka account public hai (ya private hai lekin aap follower ho), to tool ek CSV ya Excel file generate karega jisme ye details ho sakti hain:

- **Username:** satyam123
- **Full Name:** Satyam Singh
- **User ID:** 49279209744
- **Follower Count:** 1500
- **Following Count:** 300
- **Bio:** "Kolkata — SRM Alum — Tech Enthusiast"
- **Public Email:** satyam@example.com (agar bio mein hai)
- **Profile Pic URL:** https://instagram.com/satyam123/profilepic.jpg

Ye output aapke Notion notes mein save karo ya Excel mein analyze karo. Lekin agar target private hai aur aap follower nahi ho, to result mein error aayega jaise "Unable to fetch data – Private Account" ya "No followers found".

Extra Tips: Private account ke liye dummy account banao (jaise Kolkata aur SRM details ke saath) aur request bhejo. Accept hone ke baad hi ye tool kaam karega. Har scraping ke baad data ko carefully check karo aur notes mein organize karo taaki aapka OSINT research complete rahe. Agar extension kaam na kare, to Instagram ke rate limits ke wajah se thodi der wait karo ya browser restart karo.

Scrapable Data from IG Followers Export Tool

Data Type	Purpose	Example
Username	Identifier	"satyam123"
User ID	Unique Identifier	"49279209744"
Full Name	Personal Info	"Satyam Singh"
Bio	Additional Details	"Kolkata — SRM Alum"

Point To Note

Instagram followers scrape karne ke liye **IG Followers Export Tool** acha hai, lekin ye private accounts pe tabhi kaam karta hai jab target aapka request accept kare. Steps simple hain – login karo, extension kholo, username daalo, aur "Start Parsing" karo. Public accounts se aapko username, User ID, bio, aur email jaise details mil sakte hain, lekin private ke liye pehle access chahiye. Dummy account banao, data scrape karo, aur Notion mein save karo – ye sab systematically karo taaki OSINT perfect bane!

==========

Uncovering the Comments of a Private Instagram Account

Private Instagram accounts ke comments dhoondhna thoda tricky ho sakta hai kyunki ye public nahi hote, lekin agar search engines ne unhe **indexed** kiya hai, to aap unhe uncover kar sakte ho. Iske liye **search engine operators** ya **dorks** ka use karna padta hai jo Instagram profiles ya related content ko target karte hain. Example dork: **site:instagram.com "cyber_sudo"** – ye Instagram pe "cyber_sudo" username ke saath indexed pages dikhayega. Iske saath hi, aap apne target ke notes mein jo usernames save kiye hain, unhe bhi try karo, jaise: **site:twitter.com "username" "instagram.com/p"**. Ye dork Twitter pe username ke saath Instagram posts ke links dhoondhega jo shayad target ne share kiye ho. Google, Bing, aur Yandex jaise search engines ka use karo taaki target profile ke baare mein koi bhi indexed info mil sake.

Note: Agar aapko target ka koi post ya comment search results mein milta hai, to iska matlab hai ki wo account **active** hai ya tha jab ye index hua tha. Private accounts ke comments aksar public posts pe hote hain (jaise kisi brand ya influencer ke page pe), aur agar search engine ne us post ko crawl kiya ho, to comment visible ho sakta hai. Example: Agar "cyber_sudo" ne ek public post pe comment kiya "Nice pic!", aur Google ne us page ko index kiya, to aapko wo comment mil sakta hai chahe account private ho.

Kaise Karein:

- **Dorks Try Karo:** Har username jo aapke notes mein hai, uske liye alag-alag dorks banao. Examples:
  - **site:instagram.com "satyam123"** – Instagram pe satyam123 ke indexed mentions.
  - **site:twitter.com "satyam123" "instagram.com/p"** – Twitter pe Instagram post links.
  - **site:yandex.com "cyber_sudo"** – Yandex pe indexed info (Russian engine jo alag results de sakta hai).
- **Filters Use Karo:** Google pe "Tools" ¿ "Past Year" filter laga ke recent indexed info dekho.
- **Cross-Platform Check:** Agar Instagram pe direct comment nahi milta, to Twitter, Reddit, ya forums pe target ke username ke saath Instagram mentions dhoondho.
- **Activity Confirm Karo:** Indexed comment ya post se pata chalta hai ki account active hai – date check karo (jaise "2 months ago") taaki timeline ban sake.

Extra Tips: Private account ke comments tabhi index honge jab wo public space (jaise group ya public profile) pe kiye gaye hon. Har result ko Notion mein save karo – username, comment, aur link ke saath – taaki aapka OSINT research organized rahe. Agar target ka comment public post pe mila, to us post ke owner ya context se aur leads mil sakte hain.

Search Dorks and Results

Dork	Purpose	Example Result
site:instagram.com "satyam123"	Instagram Mentions	"Nice pic!" on public post
site:twitter.com "satyam123" "instagram.com/p"	Post Links	Twitter link to IG post
site:yandex.com "cyber_sudo"	Indexed Info	Comment on brand page

Point To Note

Private Instagram accounts ke comments dhoondhne ke liye **site:instagram.com "username"** ya **site:twitter.com "username" "instagram.com/p"** jaise dorks ka use karo – Google, Bing, aur Yandex pe try karo. Ye indexed info se pata chal sakta hai ki account active hai ya nahi. Public posts pe comments milne ke chances hote hain, to unhe carefully track karo. Har detail ko Notion mein note karo aur cross-platform check karte raho taaki target ka complete picture ban sake!

==========

Downloading Instagram Posts of Your Target

Instagram posts ko download karna OSINT (Open Source Intelligence) investigation ke liye kaafi useful ho sakta hai, kyunki ye aapko target ke baare mein deep insights de sakta hai jo simple browsing se nahi milte. Posts mein photos, videos, captions, aur timestamps hote hain jo target ke location, habits, connections, ya activities ke baare mein clues dete hain. Ye data aapke research ko evidence ke saath strong bana sakta hai, aur baad mein analysis ke liye save karna zaroori hota hai.

Real-Life Use Example: Maan lo aap ek OSINT investigator ho aur aapko ek target pe kaam karna hai jo shayad illegal wildlife trafficking mein involved hai. Target ka Instagram handle "wildlife_trader" hai, aur wo public account pe exotic animals ki photos post karta hai. Aap notice karte ho ki ek post mein ek rare tiger cub ki photo hai, caption mein likha hai "New arrival, DM for price," aur background mein ek specific jungle ka view hai. Is post ko download karke aap:

- **Location Pata Karo:** Photo ke EXIF metadata ya background se jungle ka naam ya coordinates nikalo (e.g., Ranthambore National Park).
- **Timestamp Check Karo:** Post ka exact date-time (e.g., 2024:03:15 T 14:00:00) se pata chalta hai ki trade kab hua.
- **Evidence Save Karo:** Photo aur caption court ya report ke liye preserve karo taaki illegal activity prove ho sake.
- **Connections Dhoondho:** Comments mein buyers ke usernames mil sakte hain (e.g., "jungleking99"), jo further investigation ke leads ban sakte hain.

Ye example dikhata hai ki Instagram posts download karna real-world investigations – jaise crime, fraud, ya missing persons cases – mein kaise game-changer ho sakta hai.

Firefox Extension – Download All Images: Instagram posts ko download karne ke liye ek acha tool hai **"Download All Images" Firefox extension**. Ye extension webpage pe maujood saari images ko ek click mein save karne deta hai, jo Instagram ke posts ke liye perfect hai. Lekin dhyan rakho – ye sirf **public accounts** ya un accounts ke liye kaam karta hai jahan aapko access hai (private account ke liye request accept hona zaroori hai).

Steps to Use "Download All Images" Firefox Extension Step-by-Step:

1. **Extension Install Karo:**
   - Firefox kholo aur "Add-ons and Themes" pe jao (Ctrl+Shift+A ya menu se).
   - Search bar mein "Download All Images" type karo, extension dhoondho (developer: Zsolt Szakaly), aur "Add to Firefox" pe click karo.
   - Permission pop-up aayega, "Add" pe click karke install pura karo.
2. **Target Profile Pe Jao:**
   - Instagram pe target ka profile kholo (e.g., instagram.com/wildlife_trader).
   - Agar private hai aur access nahi hai, to pehle dummy account se request bhejo aur accept hone ka wait karo.
3. **Extension Open Karo:**
   - Firefox toolbar pe "Download All Images" icon (ek arrow wala image sign) pe click karo – ye ek popup kholega.
4. **Images Select Karo:**
   - Popup mein "Scan Page" ya "Find Images" pe click karo – ye current page pe saari images (profile pic, posts, stories thumbnails) list karega.
   - Aap manually check kar sakte ho ki kaunsi images chahiye (e.g., sirf posts ki photos) ya "Select All" karo.
5. **Download Start Karo:**
   - "Download" button pe click karo – ek folder choose karne ka option aayega (e.g., "C:/OSINT/WildlifeTrader").
   - Images ek ZIP file mein ya individually save ho jayengi, jaise "image001.jpg", "image002.jpg".
6. **Files Check Karo:**
   - Download hone ke baad folder kholo aur dekho ki saari target posts ki images save hui hain. Ab inhe analyze karo – EXIF data ke liye tools jaise "Jeffrey's EXIF Viewer" use karo ya captions ko Notion mein note karo.

Extra Tips:

- Agar target ke posts zyada hain, to page ko scroll down karo taaki saari images load ho jayein pehle, warna extension sirf visible images hi grab karega.
- Video download ke liye ye extension kaam nahi karta – uske liye "Video DownloadHelper" jaise alag tool try karo.

- Har image ke saath timestamp ya caption bhi save karna chahte ho, to screenshot bhi lo (Ctrl+Shift+E Firefox mein).
- Safety ke liye virtual machine pe kaam karo taaki malware risk na ho, khaaskar agar data sensitive hai.

Downloadable Post Details

Detail	Purpose	Example
Image	Visual Evidence	"tiger$_c$ub.jpg"
Timestamp	Activity Timing	"2024:03:15 T 14:00:00"
Caption	Contextual Clue	"New arrival, DM for price"
Comment	Connections	"jungleking99"

Point To Note

Instagram posts download karna OSINT mein kaafi kaam aata hai, jaise wildlife trafficking jaise real cases mein location, timestamp, aur evidence ke liye. **Download All Images** Firefox extension se public posts ki photos easily save karo – install karo, target profile pe jao, scan karo, aur download karo. Ye steps simple hain aur research ko strong banate hain – bas har detail ko Notion mein organize karo aur systematically kaam karo taaki investigation perfect ho!

==========

[many]tcolorbox
titlesec

Trace Labs OSINT VM

Trace Labs OSINT VM ek customized version hai Kali Linux ka, jo specially **OSINT (Open Source Intelligence) tools** pe focus karta hai. Kali Linux to waise bhi ek powerful distro hai jo penetration testing ke liye famous hai, lekin Trace Labs ne isko OSINT investigators ke liye optimize kiya hai. Ye VM Trace Labs team ne banayi hai taaki OSINT ke kaam ko fast aur easy banaya ja sake – isme woh tools aur scripts shamil hain jo unke Search Party CTF events mein kaam aate hain. Iska maksad hai ek aisa environment dena jahan OSINT tools ek jagah neatly organized ho aur investigators ko setup ka tension na leke direct kaam shuru karne ka option mile.

Download Kaise Karein: Google pe search karo "download Trace Labs OSINT virtual machine" aur official website **tracelabs.org** pe jao. Wahan "TL OSINT VM" section mein latest release ka link milega (jaise OVA file). Example: https://www.tracelabs.org/initiatives/osint-vm pe jake "Download OVA" pe click karo. Ye file VirtualBox ya VMware mein import karo – default credentials hain **osint:osint**. Bada disk space rakho (20-30 GB minimum) kyunki tools install karne ke baad size badh sakta hai.

Preinstalled Tools Jo Isse Unique Banate Hain: Trace Labs OSINT VM mein kaafi tools preinstalled aate hain ya script ke through add kiye ja sakte hain jo Kali Linux ke default

setup mein nahi hote ya OSINT ke liye specific hote hain. Ye isko alag VM banane ki wajah hai – Kali mein pentesting tools zyada hote hain, lekin yahan OSINT pe focus hai. Kuch examples:

- **Sherlock:** Username search tool jo ek naam ko multiple platforms pe track karta hai – Kali mein default nahi hota, lekin OSINT ke liye must-have hai.
- **Photon:** Web crawler jo websites se data (emails, links, files) scrape karta hai – ye OSINT ke liye tailored hai aur Kali mein optional hota hai.
- **h8mail:** Email breach checker jo leaked databases mein email addresses dhoondhta hai – ye bhi Kali ke standard build mein nahi milta.
- **Spiderfoot:** Automated OSINT tool jo IP, domains, aur emails pe intel gather karta hai – Kali mein manually install karna padta hai, yahan ready hai.
- **OSINT Bookmarks:** Firefox mein preloaded bookmarks ka collection jo OSINT sites (people search, domain lookup, maps) ke liye curated hai – ye Kali mein nahi hota aur time save karta hai.
- **skiptracer:** Social media aur public records se data pull karta hai – ye OSINT-specific hai aur Trace Labs VM mein focus ke saath shamil hai.
- **Carbon14:** Ek tool jo online content ke age ya authenticity ko analyze karta hai – Kali ke pentest focus mein ye nahi hota.

Kali se Difference aur Need: Kali Linux mein tools jaise Metasploit, Nmap, aur Burp Suite hote hain jo hacking aur network testing ke liye hain, lekin OSINT ke liye itna focus nahi hai. Trace Labs VM se pentesting tools hata ke OSINT ke liye lightweight aur targeted banaya gaya hai. Isme privacy features (jaise mic/camera block) aur investigation-friendly setup (note-taking apps jaise CherryTree) bhi hote hain jo Kali mein default nahi milte. Ye VM beginners ke liye bhi easy hai kyunki tools pre-configured hote hain, jabki Kali mein aapko khud setup karna pad sakta hai.

Kaise Kaam Karein: VM import karne ke baad, tools terminal ya desktop icons se launch karo. Example: "`sherlock satyam123`" run karke target ke usernames dhoondho. Har finding ko TL Vault (Obsidian app mein) save karo jo desktop pe pre-set hai. Agar koi tool missing lage, to desktop pe "install-tools.sh" script chala ke latest OSINT tools add kar sakte ho.

Unique Tools in Trace Labs OSINT VM

Tool	Purpose	Example Use
Sherlock	Username Tracking	"sherlock satyam123"
Photon	Web Scraping	Emails, Links
h8mail	Breach Checking	Leaked Emails
Spiderfoot	Intel Gathering	IP/Domain Data

Point To Note

Trace Labs OSINT VM ek customized Kali Linux hai jo OSINT tools (Sherlock, Photon, h8mail, Spiderfoot) pe focus karta hai, jo Kali ke default pentesting setup mein nahi hote. Google se "Trace Labs OSINT VM download" search karke tracelabs.org se OVA file lo aur VirtualBox mein chalao. Ye VM isliye alag banayi gayi kyunki ye OSINT ke liye lightweight, pre-configured, aur beginner-friendly hai – pentesting ke bajaye intelligence gathering pe dhyan deta hai. Har tool aur finding ko organize karo taaki aapka OSINT research zabardast bane!

==========

Automatically Download Instagram Profile

Instagram profile ka content automatically download karna OSINT ke liye kaafi useful hai, aur iske liye **Instaloader** ek zabardast tool hai. **Instaloader** ek Python-based tool hai jo Instagram accounts se **pictures, videos, captions, aur metadata** download karne mein madad karta hai. Ye tool command-line pe kaam karta hai aur target ke profile ka pura data ek folder mein save kar deta hai – jaise posts, stories, highlights, aur profile pic. Ye OSINT investigators ke liye perfect hai kyunki aapko manually har post save nahi karna padta, aur metadata se extra info (jaise timestamp, location) mil sakti hai.

Instaloader Kya Download Karta Hai:

- **Profile Pic:** Target ka current profile picture high quality mein.
- **Posts:** Saari images aur videos jo target ne post kiye (public ya private, agar access hai).
- **Captions:** Har post ke saath likha text, jo context ya clues deta hai.
- **Metadata:** JSON files mein details jaise timestamp (kab post kiya), likes count, aur location tags (agar available ho).
- **Stories/Highlights:** Agar active hain aur aapke paas access hai, to ye bhi download ho sakte hain.

Installation:

- **Pip Command:** Terminal kholo aur ye command run karo: **pip3 install instaloader**. Ye Python 3 ke liye Instaloader install karega. Python pehle se installed hona chahiye (python.org se download karo agar nahi hai).
- **Apt Command:** Agar Linux (Ubuntu) pe ho, to **sudo apt install instaloader** bhi try kar sakte ho, lekin pip zyada recommended hai kyunki latest version milta hai.

Note: Instaloader ka use karte waqt jo Instagram account use karoge, uspe **ban lagne ka risk** hai kyunki Instagram automated tools ko detect kar sakta hai aur terms of service violation maanta hai. Isliye **dummy ya fake account** ka use karo – apna real account mat daalo, warna wo block ho sakta hai. Agar future mein ye tool kaam na kare (Instagram updates ke wajah se), to alternatives dhoondho jaise **4K Stogram** ya **InstaGraper**.

Private Account Pe Kaam Karta Hai?

- **Public Account:** Agar target ka account public hai, to login ki zarurat nahi – direct command se download ho jayega.

- **Private Account:** Private account ke liye aapko login karna padega aur aapka dummy account target ko follow karna chahiye. Bina following ke private data access nahi hoga kyunki Instagram ke privacy rules strict hain.

Steps to Use Instaloader:

1. **Public Account Download:**
   - Terminal mein command run karo: **instaloader target_username** (e.g., instaloader cyber_sudo).
   - Ye target ke public posts, profile pic, aur metadata download karke ek folder bana dega (e.g., "cyber_sudo").
2. **Private Account Download:**
   - Pehle dummy account se target ko follow karo aur request accept hone ka wait karo.
   - Terminal mein ye command daalo: **instaloader -l your_username target_username** (e.g., instaloader -l dummy_kolkata cyber_sudo).
   - Password maanga jayega – apne dummy account ka password daalo.
   - Login hone ke baad tool target ke private posts, images, videos, aur metadata download karega.
3. **Output Check Karo:** Downloaded folder mein images (.jpg), videos (.mp4), aur metadata (.json) files milengi. JSON files ko Notepad se kholo taaki timestamp ya extra details dekho.

Note: Private account ke profile section ko download karne ke liye:

- Aapka dummy account target ko follow kar raha hona chahiye.
- Command **instaloader -l your_username target_username** use karo – isse pura profile data milega.
- **Risk:** Is tool se hacking ka chance hai (Instagram ke security flags ya third-party interference), to hamesha dummy account use karo aur VPN ke saath kaam karo taaki safety rahe.

Extra Tips: Har download ke baad folder ko check karo – metadata se location ya timestamp nikalo (JSON mein "taken_at_timestamp" dekho). Data ko Notion mein organize karo aur sensitive files ko virtual machine pe rakho taaki risk na ho.

Downloadable Content with Instaloader

Content Type	Format	Example
Profile Pic	.jpg	"cyber_sudo_profile.jpg"
Post Image	.jpg	"cyber_sudo_2024-04-02.jpg"
Video	.mp4	"cyber_sudo_video.mp4"
Metadata	.json	"taken_at_timestamp"

Point To Note

Instaloader se Instagram profile ka content – profile pic, posts, videos, captions, aur metadata – easily download ho sakta hai, jo OSINT ke liye perfect hai. Public accounts ke liye login nahi chahiye, lekin private ke liye dummy account se follow aur login zaroori hai. **pip3 install instaloader** se install karo, lekin ban ya hack risk ke wajah se fake account use karo. Ye tool time bachata hai aur deep info deta hai – bas har detail ko Notion mein save karo aur carefully kaam karo taaki investigation strong bane!

==========

Extracting X/Twitter User IDs

Twitter ya X OSINT ke liye ek bada platform hai kyunki iske **550 million se zyada active users** hain (2024 tak), aur yahan users **tweets, photos, videos** share kar sakte hain aur **links** add kar sakte hain. Ye sab info target ke baare mein kaafi kuch reveal kar sakti hai agar aap dhyan se analyze karo. X pe har user ka ek unique identifier hota hai – **User ID** – jo account banne ke waqt generate hota hai (e.g., 1430275132...), aur ye kabhi change nahi hota, chahe username badal jaye.

Note: Kisi bhi social media profile ke saath pehla step hai – **bio padhna**. Bio mein links ho sakte hain (jaise Instagram, GitHub), aur "Joined Date" bhi dikhta hai (e.g., "Joined March 2015"). Ye info kaafi kaam aati hai:

- **Links:** Doosre platforms pe target ke accounts dhoondhne ke liye.
- **Joined Date:** Account kitna purana hai, ye samajhne ke liye – purane accounts zyada legit ho sakte hain.

Example

Aapko mila – **Display Name:** Satyam Singh, **Username:** @satyam123. Ab Google pe search karo **"satyam123 Satyam Singh"** – isse target ke doosre social media accounts mil sakte hain jahan ye same username ya display name use karta hai (jaise Instagram, LinkedIn). Isse aapka research expand hota hai.

User ID Kaise Nikalein: Har X user ka User ID unique hota hai aur profile banne pe fix ho jata hai. Ise dhoondhne ke do tareeke hain:

1. **Manual Method (Inspect Element):**

- **Profile Page Pe Jao:** Target ka X profile kholo (e.g., twitter.com/satyam123).
- **Right Click ¿ Inspect:** Profile page pe kahin bhi right-click karo aur "Inspect" ya "Inspect Element" pe click karo – ye developer tools kholega.
- **Search Karo:** Ctrl+F se "profile_banners" search karo. Code mein aapko kuch aisa milega:

```
<img src="https://pbs.twimg.com/profile_banners
   /1430275132/1698765432">
```

Yahan "1430275132" User ID hai.

- **Verify Karo:** ID ko https://twitter.com/intent/user?user_id=1430275132 mein paste karo – agar profile khulta hai, to ID sahi hai.

2. **Automatic Method (Twitter ID Converter):**

- **Website:** Ek site hai TweeterID.com ya twitids.com – yahan jao.
- **Username Daalo:** Target ka username paste karo (e.g., @satyam123).
- **Captcha Solve Karo:** Security ke liye captcha pura karo.
- **Result:** Site aapko User ID de degi (e.g., 1430275132). Ye fast aur easy hai, manual kaam se bachata hai.

User ID Ka Use:

- Jab aapko User ID mil jaye, to profile check karne ke liye URL banao: https://twitter.com/intent/user (ID ko apne target ke ID se replace karo, jaise https://twitter.com/intent/user?user_id=1430275132). Ye direct profile pe le jayega, chahe username change ho gaya ho.
- User ID se aap target ke account ko track kar sakte ho, kyunki username badalne pe bhi ID same rehta hai.

Extra Tips:

- Bio ke links ko Notion mein note karo aur unhe explore karo.
- Joined Date se account ka age estimate karo – Google pe "Twitter ID creation date" search karke ID ke range se year pata kar sakte ho (e.g., 1430275132 shayad 2013 ka ho).
- Har detail – User ID, username, display name, links – ko Notion mein save karo taaki aapka OSINT research organized rahe.

Tables

Method	Steps	Tools
Manual	Inspect Element	Browser Dev Tools
Automatic	Username Input	TweeterID.com

Table 1: Methods to Extract Twitter User IDs

Summary

- Twitter/X ke 550 million+ users OSINT ke liye bada scope dete hain.
- User ID unique aur permanent hai – username change ho ya na ho, ID se track karo.
- Bio, links, aur joined date se target ka online footprint expand karo.

Point To Note

X ke 550 million+ users ke saath OSINT ke liye bada scope hai – bio, links, aur joined date se shuru karo. **User ID** (e.g., 1430275132) manually "profile_banners" se ya TweeterID.com se nikalo – ye target ko track karne ke liye permanent hai. Google pe username aur display name search karke doosre accounts dhoondho. https://twitter.com/intent/user?user_id=ID se profile verify karo. Ye sab info Notion mein save karo aur systematically kaam karo taaki target ka pura online footprint samajh aaye!

==========

OSINT Notes: Recovering Deleted Tweets and Timestamps

Recovering Deleted Tweets and Timestamps

Twitter ya X pe **deleted tweets** aur unke **timestamps** recover karna OSINT ke liye kaafi helpful ho sakta hai, kyunki ye aapko target ke past activity aur exact posting time ke baare mein info de sakta hai. **Timestamp** se aapko pata chalta hai ki post ya comment kab kiya gaya tha, format mein **yyyy-mm-dd "T" HH:mm:ss** (e.g., 2024-04-03 T 09:15:30), jo year, month, day, aur time (24-hour) dikhata hai. Lekin deleted tweets ko wapas lane ke liye aapko kuch tricks aur tools ka use karna padta hai, jaise search engines ya archives. Ye method tab kaam karta hai jab tweet public tha aur search engines ne use index kiya ho ya kisi archive mein save ho gaya ho.

Steps to Find Timestamps of Posts/Comments:

1. **Post ya Comment Pe Jao:** Agar tweet abhi bhi available hai (delete nahi hua), to target ke X profile pe jao aur jis post ya comment ka timestamp chahiye, uspe focus karo.
2. **Right Click ¿ Inspect:** Post ya comment pe right-click karo, "Inspect" select karo – ye browser ke developer tools kholega (Chrome ya Firefox pe).
3. **Timestamp Locate Karo:** Code mein Ctrl+F se '¡time¿' tag dhoondho ya "datetime" search karo. Example:

```
<time datetime="2024-04-03T09:15:30Z">2 hours ago</time>
```

   Yahan "2024-04-03T09:15:30Z" exact timestamp hai – 3 April 2024, 9:15:30 AM UTC. Local time ke liye adjust karo (India ke liye +5:30 hours, to 14:45:30 IST).

- **Note:** Ye step sirf live tweets/comments ke liye kaam karta hai, deleted ke liye neeche wale methods use karo.

Recovering Deleted Tweets (Indexed Tweets): Deleted tweets ko recover karne ke liye **search engine operators** ka use karo, kyunki Google, Bing, Yahoo, ya Yandex ne shayad tweet ko index kiya ho jab wo public tha. Dorks ka use karo:

- **Examples:**
  - site:twitter.com "username" (e.g., site:twitter.com "cyber_sudo") – Username ke saath tweets dhoondhta hai.
  - site:twitter.com "@cyber_sudo" – Handle ke saath specific mentions ya tweets.
- **Search Engines Pe Try Karo:**
  - **Google:** "site:twitter.com "cyber_sudo"" daalo, results mein dekho kya milta hai.

- **Bing:** Same dork use karo, alag results ke liye.
- **Yahoo:** Thoda kam effective, lekin try karo.
- **Yandex:** Russian engine, kabhi unique indexed data deta hai – "site:twitter.com @cyber_sudo" try karo.

Cached Version Kaise Check Karein: Agar tweet delete ho gaya, to uska **cached version** mil sakta hai jo search engine ne save kiya ho. Steps:

1. **Search Karo:** Upar wala dork (site:twitter.com "cyber_sudo") Google pe daalo.
2. **Cached Option Dekho:** Result ke URL ke saath chhota green arrow ya "Cached" option dikhega (Google pe three dots pe click karo). Bing pe bhi "Cached" mil sakta hai.
   - **Kaise Pata Kare Available Hai?** Agar "Cached" option dikhta hai, to cached version available hai. Agar nahi dikhta, to cache nahi hai ya expire ho gaya.
3. **Cached Page Kholo:** Cached link pe click karo – ye tweet ka screenshot dikhayega jaise wo index hone ke waqt tha, timestamp ke saath (e.g., "Cached on 2024-03-20").

- **Note:** Google ne 2024 mein cache feature retire karna shuru kiya, to ye future mein kaam na kare. Bing ya Yandex abhi reliable hain.

Extra Methods:

- **Wayback Machine:** Internet Archive (archive.org) pe jao, target ka profile URL (e.g., twitter.com/cyber_sudo) daalo, aur calendar se date select karo. Agar snapshot hai, to deleted tweet aur timestamp mil sakta hai.
- **X Archive:** Agar aapka apna tweet hai, to X se data archive request karo (Settings ¿ Your Account ¿ Download an archive). Ye sirf aapke tweets deta hai, doosron ke deleted tweets nahi.
- **Timestamps ke Patterns:** Agar ek bhi tweet mil jaye, to uske timestamp se posting habits guess kar sakte ho (e.g., har subah 8 baje tweet karta hai).

Kaise Kaam Karein: Har method try karo – live tweets ke liye Inspect, deleted ke liye dorks aur cache, aur purane data ke liye Wayback. Har finding – tweet, timestamp, link – ko Notion mein save karo taaki research organized rahe aur timeline ban sake.

Tables

Method	Source	Use Case
Inspect Element	Live Tweets	Exact Timestamp
Search Dorks	Indexed Tweets	Deleted Tweets
Wayback Machine	archive.org	Old Snapshots

Table 2: Methods to Recover Tweets and Timestamps

Summary

- Deleted tweets aur timestamps target ke past activity ko reveal karte hain.
- Live tweets ke liye Inspect se timestamp (e.g., 2024-04-03 T 09:15:30) nikalo.
- Deleted ke liye site:twitter.com "username" dorks aur cached pages use karo.

Point To Note

Deleted tweets aur timestamps recover karne ke liye **yyyy-mm-dd "T" HH:mm:ss** format mein exact time pata karo – live tweets ke liye Inspect se, aur deleted ke liye site:twitter.com "username" jaise dorks Google, Bing, Yahoo, Yandex pe use karo. Cached version check karo (arrow ya "Cached" se), aur Wayback Machine bhi try karo. Ye sab target ke past ko uncover karta hai – bas har detail ko Notion mein note karo aur systematically kaam karo taaki OSINT perfect bane!

==========

Leveraging Search Operators to Find Specific Tweets

Twitter ya X pe **search operators** ka use karke aap apne searches ko refine aur narrow down kar sakte ho, jo OSINT ke liye kaafi powerful hai. Ye operators aapko specific tweets, users, ya time periods ke tweets dhoondhne mein madad karte hain. Lekin sawal hai – **kya ye sirf Twitter ke search box pe kaam karte hain?** Nahi, ye operators Twitter ke search bar (twitter.com/search) pe to kaam karte hi hain, lekin inhe Google ya Bing pe bhi tweak karke use kar sakte ho (jaise site:twitter.com ke saath). Twitter ke andar ye zyada accurate hote hain kyunki direct API data se fetch hote hain.

Main Search Operators aur Examples:

- **from:** Ye operator ek specific username se saare tweets dikhata hai. Syntax: **from:username**.
  - Example: **from:_zsecurity email** – Ye _zsecurity ke tweets mein "email" keyword dhoondhega.
- **to:** Ye operator ek specific username ko kiye gaye tweets dikhata hai. Syntax: **to:username**.
  - Example: **from:cyber_sudo to:_zsecurity** – Ye dikhayega ki cyber_sudo ne kabhi _zsecurity ko tweet ya reply kiya hai ya nahi.
- **since:** Isse aap specified date ke baad ke tweets filter kar sakte ho. Syntax: **since:yyyy-mm-dd**.
- **until:** Isse aap specified date tak ke tweets filter kar sakte ho. Syntax: **until:yyyy-mm-dd**.
  - Combined Example: **from:cyber_sudo since:2024-01-01 until:2024-01-15** – Ye cyber_sudo ke 1 Jan 2024 se 15 Jan 2024 tak ke tweets dikhayega.

Real-Life Use Example: Maan lo aap ek OSINT investigator ho aur aapko pata karna hai ki "_zsecurity" naam ka user, jo ek cybersecurity trainer hai, ne kabhi apna email address tweet kiya hai ya nahi, taaki aap uske saath contact establish kar sako ya uske doosre accounts trace kar sako. Steps:

- Twitter pe search bar mein daalo: **from:_zsecurity email**.
- Result mila: "Contact me at info@zsecurity.org for courses" – ab aapko email mil gaya (info@zsecurity.org), jo aap Google pe search kar sakte ho ya breach databases mein check kar sakte ho.
- Aur refine karna hai to: **from:_zsecurity email since:2023-01-01 until:2023-12-31** – ye 2023 ke saal ka data dega, agar email us time tweet hua ho.
- **Fayda:** Isse aap target ka email pata kar sakte ho, aur uske saath linked websites, courses, ya doosre social media accounts (LinkedIn, Instagram) dhoondh sakte ho. Ye ek real case mein lead ban sakta hai – jaise fraud investigation ya missing person search mein.

Example

from:cyber_sudo to:_zsecurity – Agar cyber_sudo ne _zsecurity ko reply kiya "Hey, loved your hacking tutorial!", to isse aap unke connection ka hint le sakte ho. Ye relation mapping ke liye useful hai.

Example

since/until ka Use: Agar aapko cyber_sudo ke tweets ek event ke around check karne hain (jaise CES 2024, 10 Jan se 15 Jan), to **from:cyber_sudo since:2024-01-10 until:2024-01-15** daalo – isse event-related tweets milenge, jaise "Live from CES!" jo location ya activity dikhata hai.

Note: Ye operators username pe kaam karte hain (@cyber_sudo), display name (e.g., "Satyam Singh") pe nahi, to hamesha handle use karo. Twitter search box mein ye direct kaam karte hain, lekin Google pe tweak karke (e.g., site:twitter.com "from:cyber_sudo") bhi try kar sakte ho agar cached ya indexed tweets chahiye.

Extra Tips:

- Results ko Notion mein save karo – tweet, timestamp, aur link ke saath.
- Agar tweets nahi milte, to "Advanced Search" (Twitter pe right side mein) use karo aur dates ya keywords manually daal do.
- Har operator ko alag-alag search engines pe bhi test karo taaki maximum coverage mile.

Tables

Summary

- Search operators Twitter searches ko refine karte hain – specific tweets ya connections dhoondho.
- from:, to:, since:, until: se emails, replies, ya event tweets nikalo.

Operator	Syntax	Use Case
from:	from:username	User Tweets
to:	to:username	Replies/Mentions
since:/until:	since:yyyy-mm-dd	Time Filter

Table 3: Search Operators for Twitter

- Twitter pe direct kaam karte hain, Google pe tweak karke bhi use karo.

Point To Note

Search operators jaise **from:**, **to:**, **since:**, aur **until:** Twitter searches ko refine karte hain – **from:_zsecurity email** se email ya **from:cyber_sudo to:_zsecurity** se connections dhoondho. Real life mein ye OSINT ke liye perfect hai – jaise email ya event activity pata karne ke liye. Twitter search box pe ye best kaam karte hain, lekin Google pe bhi tweak karke try karo. Har finding ko Notion mein note karo aur systematically kaam karo taaki target ka pura profile samajh aaye!

==========

Discovering Tweets Posted from a Specific Location

Twitter ya X pe **specific location** se posted tweets dhoondhna OSINT ke liye kaafi useful hai, aur iske liye **search operators** ka use hota hai. Ek powerful operator hai **geocode:**, jo aapko ek given location ke tweets restrict karne deta hai. Ye location-based search ke liye perfect hai jab aapko kisi city ya area ke baare mein info gather karni ho – jaise koi event, protest, ya disaster hua ho, to log aksar wahan se tweet karte hain, aur aap unke latest updates dekh sakte ho.

Geocode Ka Format:

- Syntax: **geocode:latitude,longitude,radius**
  - Latitude aur longitude decimal mein hote hain (e.g., 41.197, -8.65).
  - Radius km ya mi mein hota hai (e.g., 5km, 10mi).
- Example: **geocode:41.197,-8.65,5km** – Ye Porto, Portugal ke around 5 km radius ke tweets dikhayega.

Real-Life Use: Maan lo aap ek OSINT investigator ho aur aapko Delhi mein ek recent protest ke baare mein info chahiye. Delhi ke coordinates hain 28.7041 N, 77.1025 E. Twitter search bar mein daalo: **geocode:28.7041,77.1025,10km "protest"**. Result mein tweets aayenge jaise "Protest at India Gate today!" ya "Traffic jam due to march" – isse aap event ka time, scale, aur eyewitness accounts pata kar sakte ho. Ye disaster response ya news verification ke liye bhi kaam aata hai – jaise earthquake ke baad affected area se updates.

Example

geocode:28.7041,77.1025,10km "protest" – Delhi ke 10km radius se "protest" keyword wale tweets dikhata hai, jaise "Protest at India Gate today!" – event tracking ke liye perfect.

Aur Twitter-Specific Search Operators:

- **@:** Ye doosre X account ke mentions dhoondhta hai. Example: **from:_zsecurity @cyber_sudo** – _zsecurity ne @cyber_sudo ko kabhi mention kiya ya nahi.
- **Filter:** Ye tweets ko specific type ke hisaab se filter karta hai:
  - **filter:media** – Sirf photos ya videos wale tweets.
  - **filter:replies** – Sirf replies dikhata hai.
  - **filter:retweets** – Sirf retweets dikhata hai.
- **-Filter:** Ye exclude karta hai. Example: **-filter:replies** – Replies hata do.
- **OR:** Multiple keywords ke liye. Example: **"osint" OR "cybersecurity"** – Dono mein se koi bhi ho to tweets dikhao.

Examples aur Use Cases:

1. **from:_zsecurity @cyber_sudo**
   - Matlab: _zsecurity ne @cyber_sudo ko tweet ya reply kiya ho to dikhao.
   - Use: Connection mapping – agar _zsecurity ne "_cyber_sudo great OSINT tip!" likha, to unka relation samajh aata hai.
2. **from:_zsecurity filter:replies**
   - Matlab: _zsecurity ke saare replies dikhata hai.
   - Use: Interaction patterns – jaise wo kis kis ko jawab deta hai (e.g., "Thanks @user123").
3. **from:_zsecurity -filter:replies**
   - Matlab: _zsecurity ke original tweets dikhata hai, replies hata ke.
   - Use: Sirf uske khud ke thoughts ya announcements dekho (e.g., "New course out!").
4. **from:_zsecurity "osint" OR "cybersecurity"**
   - Matlab: _zsecurity ke tweets jo "osint" ya "cybersecurity" shamil karte hain.
   - Use: Interest areas – jaise "OSINT is key to hacking" ya "Cybersecurity tips today".
5. **Combined: from:_zsecurity geocode:28.7041,77.1025,10km**
   - Matlab: _zsecurity ke Delhi ke 10km radius se tweets.
   - Use: Location tracking – agar wo Delhi mein tha to "At India Gate!" jaisa tweet mil sakta hai.

Kaise Karein: Twitter ke search bar pe jao (twitter.com/search), operator daalo, aur Enter dabao. Results ko refine karne ke liye "Advanced Search" bhi use karo – wahan dates, locations, aur filters manually set kar sakte ho. Har tweet – location, timestamp, content – ko Notion mein save karo taaki timeline aur patterns ban sake.

Operator	Syntax	Use Case
geocode:	geocode:lat,long,radius	Location Tweets
filter:	filter:media/replies	Type Filter
-filter:	-filter:replies	Exclude Types

Table 4: Search Operators for Location-Based Tweets

Tables

Summary

- Geocode: se specific location ke tweets dhoondho – event tracking ke liye best.
- filter:, -filter:, OR jaise operators se refine karo – replies, media, ya keywords ke liye.
- Twitter search bar pe kaam karo, results ko Notion mein save karo.

Point To Note

Geocode:latitude,longitude,radius (e.g., geocode:28.7041,77.1025,10km) se specific location ke tweets dhoondho – events ya updates ke liye perfect. **from:**, **to:**, **filter:**, aur **OR** jaise operators se refine karo – jaise **from:_zsecurity @cyber_sudo** se connections ya **from:_zsecurity filter:replies** se interactions. Ye OSINT mein target ke location aur activity ko pinpoint karta hai – har detail ko Notion mein note karo aur systematically kaam karo taaki research strong bane!

==========

Twitter OSINT Recap

Twitter ya X pe OSINT karna ek effective tareeka hai target ke online presence aur activities ko samajhne ka. Is recap mein hum Twitter profile ke key elements – username, bio, profile picture, User ID, posts/comments timestamps, aur indexed tweets – ko analyze aur save karne ke steps cover karenge. Ye sab info aapke investigation ko strong banati hai, aur search operators aur cached data ka use karke aap deleted ya hidden info bhi uncover kar sakte ho. Har step systematically follow karo aur findings ko organize rakho.

Steps for Twitter OSINT Recap:

1. **Analyze and Save Username, Bio, and Profile Picture:**
   - **Username:** Target ka handle note karo (e.g., @cyber_sudo). Ye unique identifier hai jo bio ke saath profile ke top pe dikhta hai.
   - **Bio:** Bio mein 160 characters tak info hoti hai – links (Instagram, website), interests, ya location hints mil sakte hain (e.g., "Kolkata — Tech Geek"). Ise Notion mein copy-paste karo.
   - **Profile Picture:** Right-click karke profile pic save karo (e.g., "cyber_sudo_profile.jpg"). Ye **image OSINT** ke liye useful hai – Google Lens ya TinEye pe reverse search karke target ke doosre accounts ya real identity ke clues mil sakte hain. Example: Pic se ek event ya location (Taj Mahal) pata chal sakta hai.

- **Kaise Karein:** Profile pe jao, screenshot lo (Ctrl+Shift+E Firefox mein), aur details Notion mein save karo.

2. **Get the User ID:**

- Har Twitter user ka ek **User ID** hota hai jo account banne pe generate hota hai (e.g., 1430275132) aur username change hone pe bhi same rehta hai.
- **Method 1 (Manual):** Profile page pe right-click karo, "Inspect" pe jao, Ctrl+F se "profile_banners" search karo. Code mein ID milega – jaise

```
<img src="https://pbs.twimg.com/profile_banners
    /1430275132/1698765432">
```

- **Method 2 (Automatic):** TweeterID.com pe username (@cyber_sudo) daalo, captcha solve karo, aur ID lo.
- **Use:** ID ko https://twitter.com/intent/user?user_id=1430275132 mein paste karke profile verify karo. Ise Notion mein save karo – ye permanent tracking ke liye hai.

3. **Posts/Comments Timestamp:**

- **Timestamp Format:** yyyy-mm-dd "T" HH:mm:ss (e.g., 2024-04-03 T 09:15:30). Ye exact posting time dikhata hai.
- **Kaise Nikalein:** Live tweet/comment pe right-click karo, "Inspect" select karo, '¡time¿' tag mein "datetime" dhoondho – jaise

```
<time datetime="2024-04-03T09:15:30Z">2 hours ago</time>
```

  UTC time ko local mein convert karo (India ke liye +5:30 hours).
- **Use:** Timestamps se activity patterns banayein – jaise "Har Sunday 8 PM pe tweet karta hai." Har tweet ke saath time Notion mein note karo.

4. **Find Any Indexed Tweets:**

- Search engines (Google, Bing, Yandex) kabhi tweets ko index karte hain jab wo public hote hain, chahe baad mein delete ho jayein.
- **Dorks:**
  - site:twitter.com "username" (e.g., site:twitter.com "cyber_sudo") – Username ke tweets.
  - site:twitter.com "@cyber_sudo" – Mentions ya replies.
- **Cached Version:** Google pe result ke green arrow ya "Cached" option se cached tweet dekho (e.g., "Cached on 2024-03-20"). Bing/Yandex bhi try karo agar Google mein nahi milta – cache availability tab dikhti hai jab "Cached" option hota hai.
- **Use:** Indexed tweets se deleted content recover karo – jaise "Nice event in Delhi!" jo location hint deta hai. Links aur text Notion mein save karo.

5. **Use Twitter Search Operators:**

- Twitter ke search bar mein operators se refine karo:
  - **from:cyber_sudo "email"** – Cyber_sudo ke tweets mein email dhoondho.
  - **from:cyber_sudo to:_zsecurity** – Cyber_sudo ke _zsecurity ko replies.

- **from:cyber_sudo since:2024-01-01 until:2024-04-03** – Specific date range ke tweets.
- **geocode:28.7041,77.1025,10km** – Delhi ke 10km radius ke tweets.

- **Use:** Ye operators connections, interests, ya location dikhate hain. Results ko Notion mein daalo.

Kaise Kaam Karein:

- Har step ke baad data ko Notion ya spreadsheet mein organize karo – username, bio, User ID, profile pic link, timestamps, indexed tweets.
- Profile pic se image OSINT karo, User ID se long-term tracking, timestamps se patterns, aur indexed tweets se deleted info recover karo.
- Twitter operators se refine karke maximum leads lo – jaise email, location, ya network.

Tables

Step	Method	Output
Username/Bio	Manual Check	Profile Details
User ID	Inspect/TweeterID.com	Unique ID
Timestamp	Inspect Element	Exact Time

Table 5: Twitter OSINT Recap Steps

Summary

- Username, bio, profile pic se shuru karo – image OSINT ke liye pic save karo.
- User ID aur timestamps se tracking aur patterns banayein.
- Indexed tweets aur operators se deleted info aur connections recover karo – sab Notion mein save karo.

Point To Note

Twitter OSINT mein username, bio, profile pic save karo aur image OSINT ke liye use karo. User ID (e.g., 1430275132) manually ya TweeterID.com se nikalo. Posts/comments ke timestamps Inspect se lo, indexed tweets dorks (site:twitter.com "username") aur cached versions se recover karo, aur **from:**, **to:**, **since:**, **geocode:** jaise operators se refine karo. Ye sab target ke online footprint ko uncover karta hai – har detail ko Notion mein save karo aur systematically kaam karo taaki investigation pura ho!

==========

Discovering and Analysing LinkedIn Profiles

LinkedIn OSINT ke liye ek shandaar platform hai kyunki iske **900 million se zyada users** hain (2024 tak), aur yahan users **posts, photos, videos** share kar sakte hain aur **links** add kar sakte hain. Ye professional networking ke liye bana hai, to log apne skills, experience, aur career updates yahan daalte hain. **Note:** LinkedIn ki ek badi baat ye hai ki log apna profile updated rakhte hain – ye Facebook jaisa nahi hai jahan casual posts zyada hote hain. Yahan job changes, education, ya location updates regular milte hain, jo OSINT ke liye goldmine hai.

Example: Agar aap "John Smith" search karte ho, to hundreds ya thousands results milenge kyunki ye common naam hai. Lekin agar aap **country, city, university** jaise filters daalte ho, to search refine ho jati hai aur aap exact person tak pahunch sakte ho jo aap dhoondh rahe ho. Chalo step-by-step dekhte hain kaise "Rishi Kabra" ka profile dhoondhein aur analyse karein.

Steps to Discover and Analyse LinkedIn Profiles:

1. **LinkedIn Pe Search Shuru Karo:**
   - LinkedIn kholo (linkedin.com), search box mein target ka naam daalo – e.g., **"Rishi Kabra"**. Enter dabao.
2. **'People' Tab Pe Jao:**
   - Search results mein "People" tab pe click karo – ye sirf logon ke profiles dikhayega, companies ya posts nahi. Ab aapko saare "Rishi Kabra" wale profiles dikhenge.
3. **Location Filter Lagao:**
   - "Locations" pe click karo aur **"Kolkata"** select karo, kyunki aapko pata hai wo wahan rehta hai. Ye list ko chhota kar dega.
4. **Current Company Add Karo:**
   - "Current Company" filter pe jao, aur jis company mein Rishi Kabra kaam karta hai wo daalo (e.g., "TechMojo Solutions" ya "Marlabs Inc."). Ye aur narrow down karega.
5. **Extra Filters Lagao:**
   - Agar aur refine karna hai, to "Add Filter" pe click karo:
     - **School:** Jahan usne padhai ki (e.g., "Motilal Nehru National Institute of Technology").
     - **Industry:** Uska field (e.g., "Software Development").
   - Ye filters target ko pinpoint karne mein madad karte hain.
6. **Posts Check Karo:**
   - "Posts" tab pe click karo aur upar wale filters ke saath posts dekho – isse pata chalega ki Rishi Kabra kya share karta hai (e.g., tech updates, job news).
7. **Target Profile Analyse Karo:**
   - Jab target profile mil jaye (e.g., Rishi Kabra ka), to:
     - **Bio/About:** Padho – experience, skills, interests.
     - **Experience:** Current aur past jobs, roles, duration.

- **Education:** Schools, degrees, years.
- **Contact Info:** Profile pe "Contact Info" pe click karo – email, phone, ya doosre social links mil sakte hain agar public hain.

- Jo info aapke liye relevant hai (jaise job role, city), usko note karo.

8. **Save to PDF:**

- LinkedIn profile ko save karna bada easy hai – profile pe jao, "More" button pe click karo (three dots), aur **"Save to PDF"** select karo. Ye pura profile PDF mein download ho jayega – bio, experience, education sab ke saath. Ise Notion mein attach karo ya local folder mein rakho.

Extra Tips:

- Agar "Rishi Kabra" ke bahut saare profiles hain, to keywords jaise "Kolkata" ya "TechMojo" search mein add karo (e.g., "Rishi Kabra Kolkata TechMojo").
- Contact Info mein email ya Twitter handle mila to unhe cross-check karo – Google pe search karo ya breach databases mein dekho.
- Posts se bhi clues lo – jaise "Just moved to Bangalore" ya "New project at Marlabs" – ye updates location ya career shifts dikhate hain.
- Har detail – User ID (agar mile), company, posts – ko Notion mein save karo taaki research organized rahe.

Tables

Step	Action	Output
Search	Name Input	Profile List
Filters	Location/Company	Refined Results
Analyse	Bio/Experience	Target Details

Table 6: Steps to Discover LinkedIn Profiles

Summary

- LinkedIn pe 900 million+ users hain – updated profiles OSINT ke liye goldmine hain.
- Filters (location, company, school) se target refine karo.
- Posts, Contact Info, aur Save to PDF se full profile lo – Notion mein save karo.

Point To Note

LinkedIn ke 900 million users ke saath OSINT ke liye bada scope hai – log yahan updated profiles rakhte hain, jo Facebook se alag hai. "Rishi Kabra" jaise target ko **People tab, location (Kolkata), current company**, aur filters (school, industry) se dhoondho. Posts aur **Contact Info** se extra details lo, aur **Save to PDF** se profile save karo. Ye steps target ko refine aur analyse karne mein madad karte hain – har info ko Notion mein note karo aur systematically kaam karo taaki pura picture clear ho!

==========

Finding Hidden Names and Extracting Post Timestamps

LinkedIn pe **post timestamps** aur **hidden names** dhoondhna OSINT ke liye kaafi useful hai kyunki ye target ke activity aur company connections ke baare mein deep info deta hai. Timestamps se aap exact date aur time pata kar sakte ho jab post ya comment kiya gaya, aur hidden names se censored employees ke profiles uncover kar sakte ho. Ye dono methods thodi technical hain, lekin sahi tareeke se kaam karne pe bada fayda dete hain. Chalo step-by-step dekhte hain.

Timestamps Kaise Nikalein: LinkedIn posts ke timestamps direct nahi dikhte, lekin **Post ID** se aap ise calculate kar sakte ho. Ye Unix time format mein hota hai. Steps:

1. **Post ID Pata Karo:**
   - Target ka LinkedIn post kholo – URL mein Post ID milega. Example: https://www.linkedin.com/posts/rishi-kabra_1234567890123456789 – yahan "1234567890123456789" Post ID hai.
2. **Binary Mein Convert Karo:**
   - Post ID (e.g., 1234567890123456789) ko binary format mein badlo – online tools jaise rapidtables.com ya binaryconvert.com use karo. Result lamba hoga, jaise '100010101...'.
3. **Pehle 42 Digits Lo:**
   - Binary ke pehle 42 digits uthao (LinkedIn Post ID ka timestamp part). Example: '10001010111010100101010100101010101010101010'.
4. **Decimal Mein Badlo:**
   - In 42 digits ko decimal mein convert karo – online calculator use karo. Ye Unix timestamp banega (e.g., 1712112345).
5. **Readable Date-Time Mein Convert Karo:**
   - Unix timestamp (1712112345) ko readable format mein badlo – websites jaise unixtimestamp.com pe daalo. Result milega: **2024-04-03 T 05:25:45 UTC**. India ke liye +5:30 hours add karo – 10:55:45 IST. Ye exact time hai jab post kiya gaya.

Alternative Easy Method:

- **Website – Unfurl.com:** Manual process se bachne ke liye, post ya comment ka URL (e.g., https://www.linkedin.com/posts/rishi-kabra_1234567890123456789) copy karo, unfurl.com pe paste karo, aur "Analyze" pe click karo. Ye automatically Post ID se timestamp nikalkar readable date-time de dega (e.g., "Posted on 2024-04-03 10:55:45 IST"). Ye fast aur error-free hai.

Example

Post URL: https://www.linkedin.com/posts/rishi-kabra_1234567890123456789 – Unfurl.com pe paste karne pe result: "Posted on 2024-04-03 10:55:45 IST".

Find Redacted Names: LinkedIn aksar company employees ke naam censor ya hide karta hai – "People" section mein kuch profiles ke naam dikhte hain, lekin baaki ka basic info hi hota hai (jaise "Software Engineer at ZSecurity"). Inhe uncover karne ke liye:

1. **Company Search Karo:**
   - LinkedIn search box mein company naam daalo – e.g., **"ZSecurity"**.
2. **Company Profile Pe Jao:**
   - Company page kholo, "People" tab pe click karo – yahan saare employees ki list dikhegi, lekin kuch ke naam redacted honge (e.g., "Cyber Security Consultant at ZSecurity").
3. **Hidden Profile Ka Description Copy Karo:**
   - Jis profile ka naam nahi dikh raha, uska description copy karo – e.g., "Cyber Security Consultant at ZSecurity".
4. **Google Pe Search Karo:**
   - Google pe jao, dork use karo: site:linkedin.com "Cyber Security Consultant at ZSecurity" – description double quotes mein rakho.
   - Result mein aapko us employee ka full LinkedIn profile link mil sakta hai (e.g., linkedin.com/in/satyam-singh), jahan naam, photo, aur details honge.

Recap aur Steps:

- **Filters Use Karo:** Search refine karne ke liye location (e.g., Kolkata), company (ZSecurity), school, industry jaise filters lagao.
- **Target Profile Analyse Karo:** Bio, experience, education, aur "Contact Info" se email ya links lo.
- **Posts/Comments Timestamp:** Post ID se binary ¿ decimal ¿ Unix ¿ readable time nikalo, ya Unfurl.com se direct lo.
- **Find Redacted Names:** Company "People" section se description copy karo, Google pe dork (site:linkedin.com "description") se profile dhoondho.

Extra Tips:

- Timestamp se posting patterns banayein (e.g., "Har Friday ko post karta hai").
- Redacted names ke profiles ke "Contact Info" mein email ya Twitter handle check karo.
- Har detail – timestamp, profile link, description – ko Notion mein save karo taaki research organized rahe.

Task	Method	Output
Timestamps	Post ID/Unfurl	Exact Time
Hidden Names	Google Dork	Full Profile
Analysis	Filters/Profile	Target Details

Table 7: Methods for Timestamps and Hidden Names

Tables

Summary

- Timestamps Post ID se ya Unfurl.com se nikalo – activity time pata karo.
- Hidden names Google dork se uncover karo – company connections dekho.
- Filters aur profile analysis se refine karo – sab Notion mein save karo.

Point To Note

LinkedIn pe **timestamps** Post ID se (binary ¿ Unix ¿ readable) ya Unfurl.com se nikalo – ye exact posting time deta hai (e.g., 2024-04-03 10:55:45). **Redacted names** company "People" section se Google dork (site:linkedin.com "description") ke saath uncover karo. Filters se search refine karo, profile analyse karo, aur sab info Notion mein save karo – ye OSINT ko strong aur complete banata hai. Systematically kaam karo taaki har clue ka fayda mile!

==========

Finding LinkedIn Profile Member IDs

LinkedIn pe target ka **Member ID** dhoondhna OSINT ke liye kaafi important hai, kyunki ye ek unique identifier hota hai jo har user ke profile ke saath juda hota hai. **Note:** Member ID dhoondhne ki wajah ye hai ki aap isse **LinkedIn leaked databases** mein search kar sakte ho – jaise 2012 ka breach jisme 167 million accounts ka data leak hua tha. Member ID se aap target ke email, password (hashed), ya aur details match kar sakte ho agar wo leak mein shamil hai. Ye ID username ya name se alag hota hai aur kabhi change nahi hota, to tracking ke liye perfect hai. Chalo step-by-step dekhte hain kaise nikala jaye.

Steps to Find Member ID of Your Target:

1. **Target ka Profile Page Kholo:**
   - LinkedIn pe target ka profile jao (e.g., linkedin.com/in/rishi-kabra). Browser mein pura page load hone do.
2. **Right Click ¿ View Page Source:**
   - Profile page pe kisi blank area pe right-click karo, "View Page Source" select karo – ye HTML code kholega.
   - Saara code select karo (Ctrl+A), copy karo (Ctrl+C), aur Notepad ya kisi text editor mein paste karo (Ctrl+V). File save kar lo (e.g., "rishi_profile_source.txt") taaki kaam easy ho.

3. **Notepad Mein Search Karo:**

   - Notepad kholo jahan code paste kiya hai. "Find" option use karo (Ctrl+F).
   - Search box mein **"member:"** type karo aur "Find Next" dabao.

4. **Matches Analyse Karo:**

   - Aapko multiple matches milenge – maan lo 217 baar "member:" aaya. Example output:
   - 216 matches mein ek same ID hoga – jaise "member:12345678" – ye generic ya page ke doosre elements ka ID hota hai.
   - Ek alag ID hoga – jaise "member:987654321" – ye target ka unique Member ID hai.
   - **Kaise Pehchanein:** Jo ID baar-baar repeat ho raha hai (216 times), wo ignore karo. Jo ek baar aaya aur alag hai, wahi target ka Member ID hai.

5. **Member ID Save Karo:**

   - Unique ID (e.g., "987654321") copy karo aur apne Notion notes mein paste karo. Ise label do – "Rishi Kabra Member ID: 987654321" – taaki future mein use kar sako.

Steps Ko Properly Samjho:

- Jab aap "member:" search karte ho, to code mein har jagah member IDs dikhte hain – jaise connections, company staff, ya page elements ke IDs. Lekin target ka Member ID profile-specific hota hai aur aksar ek hi baar aata hai, baki repeating IDs page ke structure se related hote hain.

```
"member:12345678" (216 times      page ke doosre logon ka)
"member:987654321" (1 time      target ka)
```

- Yahan "987654321" target ka Member ID hai kyunki ye unique hai.

Alternative Tool: Manual process ke bajaye, agar aap fast method chahte ho, to **"LinkedIn Member ID Finder"** jaise browser extensions ya scripts try kar sakte ho (Chrome Web Store pe search karo, lekin trusted source se lo). Steps:

- Extension install karo, target profile pe jao, extension icon pe click karo – ye direct Member ID dikhayega (e.g., "987654321").
- Ya phir Python script use karo (online GitHub pe milte hain) – URL daal do, wo HTML scrape karke ID nikal dega. Lekin ye risky ho sakta hai LinkedIn ke terms ke against hone ke wajah se.

Use of Member ID:

- Member ID milne ke baad, LinkedIn leaked databases (jaise archive.org/details/LIUusers.7z) mein Agent Ransack se search karo – "987654321" daalo, aur agar match milta hai, to email ya hashed password milega.
- Har finding ko Notion mein save karo – Member ID, database match, aur related info ke saath.

Extra Tips:

- Agar "member:" se ID nahi milta, to "entityUrn" search karo – kabhi kabhi ID isme bhi hota hai (e.g., "urn:li:member:987654321").
- Virtual machine pe kaam karo taaki safety rahe, khaaskar leaked data ke saath.
- Profile ka "Save to PDF" bhi kar lo (More ¿ Save to PDF) taaki pura record rahe.

Tables

Task	Method	Output
Find Member ID	View Source/Search	Unique ID
Alternative	Extension/Script	Fast ID Extraction
Use ID	Database Search	Email/Password

Table 8: Methods for Finding and Using Member IDs

Summary

- Profile source se "member:" search karo – unique ID target ka hoga, repeating IDs ignore karo.
- Extensions ya scripts se fast ID nikalo, lekin LinkedIn terms ka dhyan rakho.
- Member ID se leaked databases mein search karo aur findings Notion mein save karo.

Point To Note

LinkedIn **Member ID** (e.g., 987654321) leaked databases mein target ko search karne ke liye zaroori hai. Profile source se "member:" search karke unique ID nikalo – 216 repeating IDs ignore karo, ek alag wala target ka hoga. **Unfurl.com** jaisa tool nahi hai yahan, lekin extensions ya scripts fast kar sakte hain. ID ko Notion mein save karo aur databases mein check karo – ye OSINT ko next level pe le jata hai. Har step carefully karo taaki kuch miss na ho!

==========

Snapchat OSINT – Downloading Stories and Extracting Metadata

Snapchat OSINT ke liye ek shandaar tareeka hai target ke **public stories** download karna aur unke **metadata** ko extract karna, kyunki isse aapko unki activity, location, ya doosre details ke clues mil sakte hain. Snapchat pe stories 24 hours ke liye public ya private hoti hain, aur agar public hain to unhe download karna aur analyze karna possible hai. Ye process do tareeke se ho sakta hai – **manual** (browser ke developer tools se) ya **automatic** (third-party website se). Chalo dono methods step-by-step dekhte hain aur samajhte hain kaise kaam karta hai.

Downloading Public Stories – Manual Method: Snapchat ke public stories ko manually download karne ke liye browser ke developer tools ka use hota hai. Ye method thoda technical hai, lekin effective hai agar aap specific media (video, reel) chahte ho. Steps:

1. **Target Profile Page Pe Jao:**

- Snapchat.com pe target ka public profile kholo (e.g., snapchat.com/@cyber$_s$*udo*).*Ensureprofilepubli*

2. **Right Click ¿ Inspect Element:**

   - Page pe kahin bhi right-click karo aur "Inspect" ya "Inspect Element" select karo – ye developer tools kholega (Chrome ya Firefox pe).

3. **Network Tab Pe Jao:**

   - Developer tools mein "Network" tab pe click karo – yahan page ke saare network requests dikhte hain.

4. **Media Filter Select Karo:**

   - Network tab ke upar filter options hote hain – "Media" select karo (ya "Videos" agar option hai). Ye sirf media files (images, videos) ke links dikhayega.

5. **Media Play Karo:**

   - Profile pe story ya video play karo – jaise hi media load hota hai, Network tab mein uska link appear karega (e.g., https://cf-st.sc-cdn.net/video/12345.mp4). Agar link nahi dikhta, to page refresh karo aur dobara play karo.

6. **Link Pe Click Karo:**

   - Network tab mein dikhne wale link pe click karo – ye video ya image browser mein khul jayega. Right-click karke "Save Video As" ya "Save Image As" se download kar lo (e.g., "cyber_sudo_story.mp4").

Note: Ye manual method hai, to har story ke liye aapko play aur link dhoondhna padega. Downloaded file ko Notion mein save karo aur metadata check karne ke liye neeche wala section dekho.

Downloading Public Stories – Automatic Method: Agar aap manual process se bachna chahte ho, to ek automatic way hai – **Snapchat Story Downloader** websites. Ye tools fast aur user-friendly hain. Steps:

1. **Target ka Snapchat Link Copy Karo:**

   - Snapchat app ya website pe target ka profile URL copy karo (e.g., snapchat.com/@cyber$_s$*udo*).*Appme*

2. **Snapchat Story Downloader Website Pe Jao:**

   - Ek trusted site jaise snaplytics.io, storyclone.com, ya socialmediafetch.com kholo. Ye public stories download karne ke liye banaye gaye hain.

3. **Link Paste Karo:**

   - Website pe input box mein target ka Snapchat URL paste karo aur "Download" ya "Fetch" button dabao.

4. **Stories Dekho aur Download Karo:**

   - Tool target ke saare public stories dikhayega (images, videos). Har story ke neeche "Download" button hoga – click karke file save kar lo (e.g., "cyber_sudo_story1.mp4").

Note: Ye method sirf **public stories** pe kaam karta hai – private stories ke liye aapko target ka follower hona padega aur phir bhi tool ka access limited ho sakta hai. Har downloaded story ko Notion mein organize karo.

Extracting Metadata from Downloaded Stories: Stories download karne ke baad, unke **metadata** se extra info nikal sakte ho – jaise creation time, device info, ya location (agar available ho). Steps:

- **Tool Use Karo:**
  - Images ke liye: **Jeffrey's EXIF Viewer** (exif.tools) pe upload karo – ye EXIF data dikhayega (e.g., "Date Taken: 2024-04-02 15:30:45").
  - Videos ke liye: **VLC Media Player** mein kholo, "Tools" ¿ "Codec Information" se metadata dekho, ya **FFmpeg** command (`ffmpeg -i video.mp4`) use karo.
- **Kya Mil Sakta Hai:**
  - **Timestamp:** Kab story banayi gayi (e.g., 2024-04-03 T 10:15:30).
  - **Device Info:** Kis phone se banayi (e.g., iPhone 14).
  - **Location:** Agar geotagging on tha (e.g., 28.7041 N, 77.1025 E – Delhi).
- **Note:** Snapchat aksar metadata strip kar deta hai, to full details nahi milenge, lekin agar raw file bacha hai to kuch clues mil sakte hain.

Recap aur Extra Tips:

- **Manual Way:** Inspect ¿ Network ¿ Media se links lo, play karke download karo – thoda time lega, lekin control zyada hai.
- **Automatic Way:** Snapchat Story Downloader site pe link paste karke saari public stories ek saath lo – fast aur easy.
- Metadata: EXIF tools ya VLC se check karo – timestamp, device, ya location clues ke liye.
- Har file aur metadata ko Notion mein save karo – filename, download date, aur extracted info ke saath.
- **Safety:** Dummy account ya VPN use karo, kyunki automated tools Snapchat ke terms violate kar sakte hain aur account ban ho sakta hai.

Tables

Task	Method	Output
Manual Download	Inspect/Network	Story File
Auto Download	Story Downloader	Multiple Stories
Metadata	EXIF/VLC/FFmpeg	Time/Device/Location

Table 9: Methods for Snapchat Story Download and Metadata Extraction

Summary

- Manual: Inspect ¿ Network se story links lo aur download karo – specific control ke liye.
- Automatic: Snapchat Story Downloader se public stories fast lo.
- Metadata EXIF ya VLC se nikalo – clues ke liye Notion mein save karo.

Point To Note

Snapchat OSINT mein **public stories** download karna manual (Inspect ¿ Network ¿ Media) ya automatic (Snapchat Story Downloader) tareeke se ho sakta hai. Manual method mein aap links khud nikalte ho, jabki automatic tool saara kaam kar deta hai. Metadata se timestamp ya location jaise clues lo – Jeffrey's EXIF ya VLC se. Ye sab target ke habits ya location samajhne mein madad karta hai – bas har detail ko Notion mein organize karo aur carefully kaam karo taaki OSINT perfect bane!

==========

TikTok OSINT – Downloading Videos, Extracting Timestamps, and Metadata

TikTok OSINT ke liye ek zabardast platform hai kyunki iske **1.3 billion se zyada users** hain (2024 tak), aur ye log short videos share karte hain jo information ka treasure trove ho sakte hain. TikTok pe users apni zindagi, interests, aur locations ke baare mein videos daalte hain, jo OSINT investigators ke liye kaafi valuable hai – chahe wo events track karna ho, target ke habits samajhna ho, ya metadata se clues nikalna ho. Is topic mein hum TikTok videos download karne, **timestamps** extract karne (kab post kiya gaya), aur **metadata** nikalne ke steps cover karenge. Ye sab systematically karna zaroori hai taaki aapka research strong aur organized rahe.

Step 1: Analyze the Target Profile Pehla kaam hai target ke TikTok profile ko analyze karna – yahan se aap basic info aur leads collect kar sakte ho.

- **Username:** Handle note karo (e.g., @cyber_sudo) – ye doosre platforms pe search ke liye useful hai.
- **Bio:** Bio mein location, interests, ya links ho sakte hain (e.g., "Kolkata — Tech Lover — Insta: @cyber_sudo123").
- **Videos:** Public videos dekho – content se habits, location, ya connections ke hints mil sakte hain (e.g., "At India Gate today!").
- **Profile Pic:** Right-click karke save karo – reverse image search (Google Lens, TinEye) se extra leads mil sakte hain.
- **Kaise Karein:** Profile pe jao, screenshot lo, aur har detail (username, bio, video themes) ko Notion mein save karo taaki base ban jaye.

Step 2: Downloading TikTok Videos TikTok videos download karna zaroori hai kyunki ye temporary hote hain (24 hours ke baad stories gayab ho jati hain), aur metadata ya content analysis ke liye permanent record chahiye. Do methods hain:

Manual Method:

1. **Target Video Pe Jao:** TikTok.com pe target ka video kholo (e.g., tiktok.com/@cyber$_s$*udo*/*video*/12 *clickkaro*,"*Inspect*"*selectkaro*–*developertoolskhulenge*.

2. **Network Tab:** "Network" tab pe jao, "Media" filter lagao, aur video play karo – link dikhega (e.g., https://v16-web.tiktok.com/video/1234567890123456789.mp4).

3. **Download:** Link pe right-click karo, "Open in New Tab" karo, phir "Save Video As" se download kar lo (e.g., "cyber_sudo_video.mp4").

Automatic Method:

- **Tool: TikTok-Scraper** (GitHub pe drawrowfly/tiktok-scraper) ya websites jaise ttdown.org use karo.

- **Steps:**

    1. Terminal mein: `pip install tiktok-scraper` karo, phir `tiktok-scraper video 1234567890123456789` run karo – video ID URL se lo.
    2. Website pe: Video URL paste karo, "Download" pe click karo – watermark-free video milega.

- **Note:** Public videos ke liye kaam karta hai – private ke liye aapko follower hona padega aur account access chahiye.

Step 3: Extracting Timestamps TikTok video ka **timestamp** (kab post kiya gaya) Post ID se nikalta hai, jo URL mein hota hai. Ye Unix timestamp format mein encode hota hai. Steps:

1. **Post ID Pata Karo:**

- Video URL se ID lo – e.g., tiktok.com/@cyber$_s$*udo*/*video*/732145678901234567*8mein*"7321456789012

2. **Binary Mein Convert Karo:**

    - ID (7321456789012345678) ko binary mein badlo – online tool (rapidtables.com) use karo. Result lamba hoga, jaise `110010101010...`

3. **Pehle 32 Digits Lo:**

    - Binary ke pehle 32 bits uthao (timestamp ka part) – e.g., `11001010101010101010101010101010`. TikTok ke IDs 64-bit hote hain, lekin pehle 32 bits time ke liye hote hain (shift right 32 bits karke baaki discard karo).

4. **Decimal Mein Convert Karo:**

    - Ye 32 bits ko decimal mein badlo – e.g., `1712112345` (10-digit Unix timestamp).

5. **Readable Date-Time Mein Badlo:**

    - Unix timestamp (1712112345) ko unixtimestamp.com pe daalo – result: **2024-04-03 T 05:25:45 UTC**. India ke liye +5:30 hours add karo – 10:55:45 IST.

Easy Alternative:

- **Tool:** unfurl.com pe video URL paste karo – ye automatically Post ID se timestamp nikal ke readable format mein dega (e.g., "2024-04-03 10:55:45 IST"). Manual steps ki zarurat nahi.

Step 4: Extracting Metadata Downloaded video se **metadata** nikalna clues ke liye zaroori hai – jaise creation time, device, ya location. Steps:

- **Tools:**
  - Videos ke liye: **VLC Media Player** (Tools ¿ Codec Information) ya **FFmpeg** (`ffmpeg -i video.mp4`).
  - Images ke liye: **Jeffrey's EXIF Viewer** (exif.tools).
- **Kya Mil Sakta Hai:**
  - **Timestamp:** Kab record kiya gaya (e.g., 2024-04-03 T 10:50:00).
  - **Device Info:** Kis device se bana (e.g., Samsung Galaxy S23).
  - **Location:** Agar geotagging on hai (e.g., 22.5726 N, 88.3639 E – Kolkata).
- **Note:** TikTok aksar metadata strip kar deta hai, to full details nahi milte, lekin agar bacha hai to useful hota hai. JSON metadata bhi TikTok-Scraper se mil sakta hai – `tiktok-scraper video 7321456789012345678 -j` run karo.

Recap aur Extra Tips:

- **Analyze Profile:** Username, bio, videos, profile pic se shuru karo – Notion mein save karo.
- **Download Videos:** Manual (Network tab) ya automatic (TikTok-Scraper, ttdown.org) se lo – public videos ke liye.
- Timestamps: Post ID se binary ¿ 32 bits ¿ decimal ¿ Unix ¿ readable time, ya unfurl.com se fast karo.
- Metadata: VLC, FFmpeg, ya EXIF tools se check karo – timestamp, device, location ke liye.
- Dummy account ya VPN use karo taaki safety rahe – TikTok scraping ke against hai.
- Har finding – video file, timestamp, metadata – ko Notion mein organize karo taaki timeline aur patterns ban sake.

Tables

Task	Method	Output
Profile Analysis	Bio/Videos/Pic	Leads
Video Download	Manual/Auto	Video File
Timestamp	Post ID/Unfurl	Post Time
Metadata	VLC/FFmpeg/EXIF	Clues

Table 10: Methods for TikTok OSINT

Summary

- Profile se leads lo – username, bio, videos Notion mein save karo.
- Videos manual (Network) ya auto (TikTok-Scraper) se download karo.
- Timestamps Post ID se ya unfurl.com se nikalo – exact posting time ke liye.
- Metadata VLC/EXIF se check karo – har detail Notion mein organize karo.

Point To Note

TikTok ke 1.3 billion+ users ke videos OSINT ke liye perfect hain – profile analyze karo, videos download karo (manual ya TikTok-Scraper se), **timestamps** Post ID se (binary ¿ 32 bits ¿ Unix) ya unfurl.com se lo, aur **metadata** VLC/EXIF se nikalo. Ye sab target ke habits, location, ya events samajhne mein madad karta hai – har detail ko Notion mein save karo aur systematically kaam karo taaki investigation pura aur strong ho!

==========

Introduction to Username OSINT

Username OSINT online identity ko track karne ka ek powerful tareeka hai, jisme aap target ke **same username ya similar variations** ko doosre platforms pe dhoondhte ho. Har insaan aksar ek favorite username ya pattern use karta hai (jaise @cyber_sudo, @cybersudo123), aur ye consistency aapko unke additional accounts tak le ja sakti hai. Identifying ye extra accounts target ke baare mein zyada info reveal kar sakta hai – jaise posts, interests, ya connections jo wo shayad ab use nahi karte ya bhool gaye hain. Ye purane ya forgotten accounts OSINT ke liye goldmine hote hain kyunki wahan privacy settings loose ho sakti hain ya sensitive data chhupa ho. Chalo iski basic samajh banate hain.

Kaise Kaam Karta Hai:

- Ek username ek digital fingerprint jaisa hai – agar target ne @cyber_sudo Twitter pe use kiya, to shayad Instagram, GitHub, ya Reddit pe bhi wahi ya thoda variation (jaise @cyber_sudo123) ho.
- Ye accounts dhoondhne se aap target ke online behavior ka pura picture bana sakte ho:
  - **Active Accounts:** Current interests, location, ya posts.
  - **Old/Forgotten Accounts:** Purani photos, bio, ya comments jo ab bhi public hain (e.g., "Moved to Kolkata in 2015" ek dead account pe).
- Example: Agar @cyber_sudo Twitter pe cybersecurity tweets karta hai, lekin uska purana MySpace account (same username) pe teenage photos ya school ka naam hai, to ye extra layer deta hai jo current profile se nahi milega.

Steps to Start Username OSINT:

1. **Target ka Primary Username Pata Karo:**
   - Maan lo aapko target ka Twitter handle mila – @cyber_sudo. Ise apna starting point banao.

2. **Similar Variations Socho:**

   - Common patterns note karo: @cyber_sudo, @cybersudo, @cyber_sudo123, @sudo_cyber, @csudo. Numbers, underscores, ya initials aksar add hote hain.

3. **Platforms Pe Search Karo:**

- Major sites pe check karo – Instagram, Facebook, LinkedIn, GitHub, Reddit, Snapchat, TikTok, etc. Direct URL try karo (e.g., instagram.com/cyber_sudo) *ya search bar me username daalo.* **"cyber_sudo" site:instagram.com** *ya* **"cyber_sudo" site:reddit.com**.

4. **Results Analyse Karo:**

   - Har account ka bio, posts, aur profile pic dekho – agar same vibe, photo, ya details match karte hain, to shayad ye target ka hai.
   - Forgotten accounts pe purani info mil sakti hai – jaise "Last post: 2018" ya "Email: cyber_sudo@gmail.com".

5. **Findings Save Karo:**

   - Har username, platform, aur useful info (bio, posts, links) ko Notion mein note karo – ek table banao:

Username	Platform	Bio/Details	Last Active
@cyber_sudo	Twitter	Cybersecurity Enthu	2024
@cybersudo123	Instagram	Kolkata, Tech Lover	2022

Fayde:

- **More Info:** Ek purana Reddit account pe target ne shayad apna real name ya city likha ho (e.g., "Satyam from Kolkata").
- **Connections:** Comments ya followers se target ke friends ya interests ka pata chal sakta hai.
- **Forgotten Data:** Dead accounts pe privacy settings weak hote hain, to phone number, email, ya photos leak ho sakte hain.

Extra Tips:

- Tools jaise **Sherlock** (GitHub pe mikaelkall/sherlock) use karo – terminal mein `sherlock cyber_sudo` run karo, ye 100+ platforms pe username check karega.
- Google dorks ke saath variations try karo – **"cyber_sudo" -inurl:(twitter)** se Twitter ke alawa results lo.
- Har account ka screenshot lo aur Notion mein organize karo taaki pura online footprint clear ho.

Task	Method	Output
Find Username	Social Media	Primary Handle
Search Platforms	Manual/Sherlock	Extra Accounts
Analyze	Bio/Posts	Info/Leads

Table 11: Methods for Username OSINT

Tables

Summary

- Target ka primary username (e.g., @cyber_sudo) se shuru karo – variations socho.
- Platforms pe manually ya Sherlock se search karo – Google dorks bhi use karo.
- Har account analyze karo aur findings Notion mein save karo – purane accounts se extra info lo.

Point To Note

Username OSINT mein **same ya similar usernames** (e.g., @cyber_sudo) ko doosre platforms pe dhoondho – ye target ke active aur forgotten accounts reveal karta hai. Purane accounts se posts, bio, ya sensitive info mil sakti hai jo current profile pe nahi hai. Search manually karo ya Sherlock jaise tools use karo – har finding ko Notion mein save karo aur systematically kaam karo taaki target ka online identity pura samajh aaye!

==========

Tracking a Username Using Advanced Search Techniques

Username tracking advanced search techniques ke saath karna OSINT mein ek powerful method hai target ke online presence ko map karne ka. Isme aap target ke saare usernames gather karte ho, unhe ek jagah save karte ho, aur phir search operators ka use karke unke accounts ya mentions dhoondhte ho. Ye tareeka isliye kaam karta hai kyunki log aksar same ya similar usernames multiple platforms pe use karte hain, aur search engines inhe index karte hain. Chalo step-by-step dekhte hain kaise target ke usernames ko track kiya jaye aur advanced searches ke saath unka fayda uthaya jaye.

Step 1: Gather Online Usernames Pehla kaam hai target ke saare online usernames collect karna aur unhe organize karna.

- **Kaise Karein:**
  - Target ke known profiles se usernames lo – jaise:
    - LinkedIn: https://linkedin.com/in/rishi-kabra – Username: **rishi-kabra**.
    - GitHub: https://github.com/rishikabra/132 – Username: **rishikabra**.
  - Twitter: https://twitter.com/rishi$_k$*abra*123–*Username* : **rishi_kabra123**.
  - Har unique username ko ek text file mein save karo (e.g., "rishi_usernames.txt").

- **Text File Example:**

```
rishi-kabra
rishikabra
rishi_kabra123
rkabra
```

- **Note:** Variations bhi socho – numbers (rishi123), initials (rkabra), ya underscores (rishi_kabra) – aur unhe bhi list mein add karo. Ye file future searches ke liye base banegi. Notion mein bhi ek table bana sakte ho usernames ke saath.

Step 2: Use Search Operators Search operators ka use karke check karo ki ye usernames search engines (Google, Bing, Yandex) mein indexed hain ya nahi. Ye aapko target ke naye accounts ya mentions tak le ja sakta hai.

- **Format:**
  - **inurl:username1 OR inurl:username2 OR inurl:username3**
  - Ye operator URL mein specific username dhoondhta hai aur multiple usernames ko OR ke saath combine karta hai.
- **Example:**
  - Text file se usernames lo: rishi-kabra, rishikabra, rishi_kabra123.
  - Google pe search karo: **inurl:rishi-kabra OR inurl:rishikabra OR inurl:rishi_kabra123**.
- **Results:**
  - LinkedIn: linkedin.com/in/rishi-kabra (already known).
  - GitHub: github.com/rishikabra (already known).
  - Reddit: reddit.com/user/rishi$_k$*abra*123(*nayaaccountmila*!).*Agarekaccountmeinbioyapostsedoosrau*

Step 3: Refine and Expand the Search Advanced techniques se search ko aur refine karo taaki maximum coverage mile:

- **Exclude Known Platforms:** Agar aapko naye platforms chahiye, to known sites exclude karo.
  - Example: **inurl:rishi-kabra -inurl:(linkedin.com github.com)** – LinkedIn aur GitHub ke alawa results do.
- **Add Keywords:** Target ke interests ya location ke saath combine karo.
  - Example: **inurl:rishi-kabra "Kolkata"** – Kolkata-related mentions dhoondho.
- **Site-Specific Search:** Specific platforms target karo.
  - Example: **site:reddit.com inurl:rishi_kabra123** – Reddit pe check karo.
- **Multiple Engines:** Google ke alawa Bing aur Yandex pe bhi try karo – kabhi alag results milte hain.

Step 4: Analyze Findings Har naya account jo milta hai, usse analyze karo:

- **Bio aur Posts:** Naye platforms pe bio (e.g., "Rishi — Tech Enthu — Kolkata") ya posts se extra info lo (e.g., "Last post: 2020 – Old job at TechMojo").

- **Connections:** Followers, comments, ya tags se network pata karo.
- **Forgotten Accounts:** Agar account purana hai aur inactive, to wahan sensitive data (email, phone) mil sakta hai.
- Har finding ko Notion mein update karo – username, platform, aur key details ke saath.

Tools for Automation: Manual search ke alawa tools bhi use kar sakte ho:

- **Sherlock:** GitHub pe (sherlock-project/sherlock) – `sherlock rishi-kabra` run karo, ye 100+ platforms pe username check karega aur results dega.
- **Namechk:** Website (namechk.com) pe username daalo, ye available platforms dikhayega.
- **Note:** Tools fast hain, lekin manual search se context (bio, posts) zyada milta hai.

Extra Tips:

- Text file ko regularly update karo – naye usernames mile to add karte jao.
- Cached pages check karo (Google pe "Cached" option) – purane ya deleted accounts ke remnants mil sakte hain.
- Har account ka screenshot lo aur Notion mein table banao:

Username	Platform	Details	Last Active
rishi-kabra	LinkedIn	Tech Lead, Kolkata	2024
rishikabra	GitHub	Code Repos	2023
rishi_kabra123	Reddit	Tech Posts	2020

Tables

Task	Method	Output
Gather Usernames	Profiles	Username List
Search	Operators/Sherlock	New Accounts
Analyze	Bio/Posts	Info/Leads

Table 12: Methods for Username Tracking

Summary

- Usernames gather karo aur text file/Notion mein save karo – variations bhi add karo.
- Search operators (inurl:username) ya Sherlock se accounts dhoondho – refine karo keywords ke saath.
- Har account analyze karo aur Notion mein organize karo – purane accounts se extra clues lo.

Point To Note

Username tracking mein target ke usernames (e.g., rishi-kabra, rishikabra) ko text file mein save karo aur **inurl:username1 OR inurl:username2** jaise search operators se indexed accounts dhoondho. Ye naye ya purane accounts tak le jata hai, jahan se bio, posts, ya connections mil sakte hain. Sherlock jaise tools bhi try karo, lekin manual analysis se context lo. Har detail ko Notion mein organize karo – ye advanced technique target ka online footprint pura khol deta hai, bas systematically kaam karo taaki kuch miss na ho!

==========

Finding Hidden Profiles with Reverse Username Lookup

Reverse username lookup ek powerful OSINT technique hai jo **hidden profiles** ya chhupi hui online identities dhoondhne mein madad karti hai. Isme aap ek username, email, name, ya phone number ke zariye target ke social media profiles aur potential email addresses tak pahunch sakte ho. Ye method isliye kaam karta hai kyunki log aksar ek hi username ya uske variations ko alag-alag platforms pe use karte hain, aur search engines ya specialized tools inhe track kar sakte hain. Ek popular tool hai **IDCrawl** – ye ek free people search engine hai jo aapke diya gaya username ya doosri details ko multiple social media sites pe search karta hai aur results ek jagah laata hai. Chalo iske baare mein detail mein samajhte hain.

What is IDCrawl?

- **Website:** idcrawl.com
- IDCrawl ek online tool hai jo social media profiles, public web info, email addresses, phone numbers, aur kabhi-kabhi criminal records bhi organize karta hai. Ye ek reverse lookup service hai jisme aap username, email, name, ya phone number daal sakte ho aur ye major platforms jaise Twitter, Instagram, LinkedIn, Facebook, TikTok, aur Snapchat pe search karta hai.
- **Fayda:** Ye hidden ya forgotten accounts dhoondh sakta hai jo target ne shayad ab use karna band kar diya ho, lekin jo ab bhi public hain ya indexed hain.

Steps to Find Hidden Profiles with IDCrawl:

1. **Target ka Username Pata Karo:**
   - Maan lo aapke paas target ka username hai – e.g., **cyber_sudo** (Twitter se mila). Ise starting point banao.
2. **IDCrawl Pe Jao:**
   - Browser mein idcrawl.com kholo. Homepage pe search bar milega.
3. **Username Daalo:**
   - Search bar mein username type karo (e.g., "cyber_sudo") aur Enter dabao. Aap email (cyber_sudo@gmail.com), name (Satyam Singh), ya phone number bhi try kar sakte ho agar available hai.

4. **Results Check Karo:**

- IDCrawl multiple platforms pe search karega aur results dikhayega:
  - Twitter: twitter.com/cyber$_s$udoInstagram : instagram.com/cyber$_s$udo
  - Reddit: reddit.com/user/cyber$_s$udo123(variationmila).
- Har link pe potential email addresses bhi suggest kar sakta hai jo bio ya posts se scraped hote hain (e.g., "Contact: cyber_sudo@gmail.com").

5. **Hidden Profiles Analyse Karo:**

- Jo accounts milte hain, unke bio, posts, aur activity dekho. Purane ya inactive accounts (e.g., "Last post: 2019") se sensitive info jaise location, real name, ya connections mil sakte hain.
- Example: Reddit pe @cyber_sudo123 ne "Kolkata meetup 2018" likha – ye ek clue hai jo current profiles pe nahi milega.

6. **Save Karo:**

- Har profile link, username variation, aur email ko Notion mein note karo – ek table banao:

Username	Platform	Details	Email Suggestion
cyber_sudo	Twitter	Tech tweets	cyber_sudo@gmail.com
cyber_sudo123	Reddit	Kolkata meetup	N/A

How IDCrawl Works:

- Ye tool social media sites ke public data ko crawl karta hai aur username ke saath match karne wali info ko ek jagah laata hai.
- Agar username indexed hai (search engines pe available), to IDCrawl usse dhoondh lega – chahe wo hidden ho ya kam active.
- Extra features: Phone number ya email se bhi reverse lookup kar sakta hai, aur kabhi-kabhi deep web ya news mentions bhi dikhata hai.

Alternative Tools aur Tips:

- **Sherlock:** GitHub pe (sherlock-project/sherlock) – `sherlock cyber_sudo` run karo, ye 100+ platforms pe username check karta hai. IDCrawl se zyada technical lekin detailed.
- **Google Dorks: site:* "cyber_sudo" -inurl:(twitter)** – Twitter ke alawa doosre platforms pe search karo.
- **Namechk:** namechk.com pe username daalo, ye availability dikhata hai.
- **Tip:** IDCrawl ke results ko cross-check karo – ek account ka bio ya profile pic doosre known accounts se match karta hai to confirm ho jata hai.

Why It's Useful:

- **Hidden Profiles:** Target ke wo accounts jo wo ab use nahi karta, lekin jahan purani info (photos, emails, locations) bachi hai.

- **Email Addresses:** Bio ya posts se potential emails mil sakte hain jo breach databases mein check karne ke liye kaam aate hain.
- **Full Picture:** Ek username se shuru karke aap target ka online footprint expand kar sakte ho.

Tables

Task	Method	Output
Username Input	IDCrawl	Profile Links
Analysis	Bio/Posts	Hidden Info
Cross-Check	Sherlock/Dorks	Confirmed Accounts

Table 13: Methods for Reverse Username Lookup

Summary

- IDCrawl pe username (e.g., cyber_sudo) daalo – hidden profiles aur emails lo.
- Results analyse karo – purane accounts se clues nikalo.
- Sherlock ya dorks se cross-check karo – har finding Notion mein save karo.

Point To Note

IDCrawl (idcrawl.com) ke saath reverse username lookup se hidden profiles dhoondhna aasan hai – username, email, name, ya phone number daalo aur social media accounts aur emails lo. Ye tool multiple platforms pe search karta hai aur forgotten ya inactive profiles tak le jata hai. Steps simple hain – profile se username lo, IDCrawl pe search karo, aur results analyse karke Notion mein save karo. Sherlock ya Google dorks se bhi refine karo – ye sab target ke chhupe hue online identity ko samne laata hai, bas systematically kaam karo taaki har lead ka fayda mile!

==========

Finding Linked Accounts Across the Web

Finding additional online accounts ek key OSINT technique hai jo target ke digital footprint ko expand karne mein madad karti hai. Agar aapko target ka ek username pata hai (jaise @cyber_sudo), to aap tools ka use karke uske linked accounts hundreds of websites pe dhoondh sakte ho. Isme do popular tools hain – **WhatsMyName** aur **Blackbird** – dono web-based platforms hain jo username enumeration ke liye banaye gaye hain. Ye tools aapko ek ya multiple usernames ke saath saare possible accounts dikhate hain, lekin dhyan rakhna padta hai kyunki kuch links kaam nahi karte ya username kisi aur ka ho sakta hai. Chalo is process ko detail mein samajhte hain aur kaise inka use karna hai.

Tools Overview:

1. **WhatsMyName:**
   - **Website:** whatsmyname.app
   - Ye ek free tool hai jo 600+ websites aur social media platforms pe username check karta hai. Iska collaboration OSINT Combine aur Micah Hoffman (@webbreacher) ke saath hai.
   - **Kaise Kaam Karta Hai:** Aap ek ya zyada usernames search box mein daalte ho, category filters (jaise social, gaming) laga sakte ho, aur ye results icons aur table mein dikhata hai.
   - **Fayda:** Fast aur detailed – forgotten ya niche platforms (jaise chess forums) bhi cover karta hai.

2. **Blackbird:**
   - **Website:** Blackbird ka web interface localhost pe chalta hai (install karna padta hai), lekin documentation p1ngul1n0.gitbook.io/blackbird pe milta hai.
   - Ye ek Python-based OSINT tool hai jo WhatsMyName ke data ke saath 580+ sites pe search karta hai. Command-line ya web interface dono mein use hota hai.
   - **Fayda:** PDF/CSV export aur AI-powered metadata extraction (bio, location) deta hai, jo WhatsMyName mein nahi hai.

Steps to Find Linked Accounts:

1. **Usernames Collect Karo:**
   - Target ke known accounts se usernames lo – e.g., LinkedIn pe @rishi-kabra, Twitter pe @rishi_kabra123. Variations bhi note karo (rishi123, rkabra).
   - Inhe ek text file ya Notion table mein save karo:

```
rishi-kabra
rishikabra
rishi_kabra123
```

2. **WhatsMyName Pe Search Karo:**
   - **Website Pe Jao:** whatsmyname.app kholo.
   - **Usernames Daalo:** Search box mein ek ya multiple usernames paste karo (e.g., "rishi-kabra rishikabra rishi_kabra123"), space se separate karke.
   - **Search Karo:** Search icon pe click karo ya Ctrl+Enter dabao.
   - **Results Dekho:** Left pe icons aur right pe table mein platforms dikhenge – green boxes clickable hote hain jo direct account link pe le jate hain.
   - **Example Output:**
     - instagram.com/rishi-kabra
     - reddit.com/user/rishikabra
     - github.com/rishi$_k$*abra*123

3. **Blackbird Pe Search Karo:**
   - **Install Karo:** GitHub (p1ngul1n0/blackbird) se clone karo – `git clone https://github.com` phir `cd blackbird` aur `pip3 install -r requirements.txt`.

- **Run Karo:**
  - Command-line: `python3 blackbird.py -u rishi-kabra rishikabra` (multiple usernames daal sakte ho).
  - Web interface: `python3 blackbird.py --web` – localhost:5000 pe browser mein kholo.
- **Results Dekho:** Web interface mein filter (found, not found) aur search bar se refine karo. PDF export bhi kar sakte ho.
- **Example Output:** Same platforms ke saath bio/location jaise metadata bhi mil sakta hai.

4. **Links Check Karo:**

- Dono tools ke results mein kuch links kaam nahi karenge (404 error) ya username kisi aur ka ho sakta hai (false positive).
- **Kaise Verify Karein:**
  - Profile pic, bio, ya posts match karo – agar @rishi-kabra Twitter pe tech tweets karta hai aur Instagram pe bhi same vibe hai, to shayad ek hi insaan ka hai.
  - Agar link dead hai, to Wayback Machine (archive.org) pe check karo – purana snapshot mil sakta hai.

5. **Findings Save Karo:**

- Har account – username, platform, link, aur key details (bio, last active) – ko Notion mein table bana ke save karo:

Username	Platform	Link	Details
rishi-kabra	LinkedIn	linkedin.com/in/rishi-kabra	Tech Lead, Kolkata
rishikabra	Reddit	reddit.com/user/rishika	Old posts, 2019

Why Use These Tools?

- **WhatsMyName:** 600+ sites cover karta hai, web-based hai, aur multiple usernames ek saath check kar sakta hai. Beginners ke liye perfect.
- **Blackbird:** Metadata extraction aur export options deta hai, lekin thodi technical setup chahiye. Advanced users ke liye better.
- **Common Issue:** False positives – @rishi-kabra ek platform pe target ka ho sakta hai, doosre pe kisi aur ka. Manual verification zaroori hai.

Extra Tips:

- **Multiple Usernames:** Ek baar mein 5-10 variations daal do – efficiency badhti hai.
- **Filters:** WhatsMyName mein categories (social, gaming) aur Blackbird mein web filters se refine karo.
- **Safety:** Dummy account ya VPN use karo – automated tools platforms ke terms violate kar sakte hain.
- **Cross-Check:** Google dorks jaise **inurl:rishi-kabra -inurl:(linkedin)** se aur results lo.

Tables

Task	Tool	Output
Username Search	WhatsMyName	600+ Site Links
Detailed Search	Blackbird	Links + Metadata
Verification	Manual/Wayback	Confirmed Accounts

Table 14: Methods for Finding Linked Accounts

Summary

- WhatsMyName (whatsmyname.app) se 600+ sites pe fast search karo – multiple usernames daalo.
- Blackbird se metadata aur exports lo – technical lekin detailed.
- Links verify karo aur Notion mein save karo – false positives se bacho.

Point To Note

WhatsMyName (whatsmyname.app) aur **Blackbird** jaise tools se hundreds of websites pe additional accounts dhoondhna aasan hai – username daalo, results lo, aur verify karo. Ye web-based (WhatsMyName) ya Python-based (Blackbird) tools multiple usernames ek saath check karte hain, lekin dead links ya false positives ke liye check karna padta hai. Har account ko Notion mein save karo – ye target ke online identity ko pura khol deta hai, bas systematically kaam karo taaki har lead ka fayda mile!

==========

Finding Passwords and Other Breached/Leaked Data Connected to a Username

Finding passwords and breached/leaked data connected to a username ek critical OSINT technique hai jo target ke compromised information ko uncover karne mein madad karti hai. Jab aapke paas ek username hai (jaise @cyber_sudo), to aap breached ya leaked databases mein search karke usse juda additional info – jaise passwords, emails, phone numbers, ya doosre details – nikal sakte ho. **Note:** Hamesha apna approach systematic rakhna chahiye – pehle free tools jaise **DeHashed** ya **Have I Been Pwned (HIBP)** pe check karo ki username, email, ya phone number kisi breach mein leak hua hai ya nahi. Agar leak confirm hota hai, to us specific leaked database ko download karo aur usme deep search karke zyada info (jaise plaintext passwords, associated emails) dhoondho. Ye method target ke digital footprint ko expand karta hai aur sensitive data tak le ja sakta hai. Chalo step-by-step dekhte hain.

Steps to Find Breached/Leaked Data by Username:

1. **Initial Check with Free Tools:**
   - **DeHashed (dehashed.com):**

- Website pe jao, "Username" field select karo, aur target ka username daalo (e.g., "cyber_sudo").
- Free search mein basic results milenge – agar username kisi breach mein hai, to breach name aur compromised data type (email, password hash) dikhega. Full details ke liye paid plan chahiye, lekin free version se leak confirm ho sakta hai.

- **Have I Been Pwned (haveibeenpwned.com):**
  - Search bar mein username daalo (e.g., "cyber_sudo"). HIBP usernames bhi support karta hai, lekin zyadatar email-focused hai.
  - Agar username kisi breach mein milta hai, to breach ka naam aur date dikhega (e.g., "Adobe Breach, 2013"). Passwords direct nahi dikhte, lekin leak ki confirmation milti hai.
- **Why First Step:** Ye tools aapko batate hain ki username compromised hai ya nahi aur kis breach mein – ye aapka starting point hai.

2. **Identify the Breach:**
   - DeHashed ya HIBP se pata chala ki username "cyber_sudo" ek breach mein leak hua (e.g., "LinkedIn 2012 Breach"). Breach ka naam note karo – ye next step ke liye zaroori hai.

3. **Download the Leaked Database:**
   - Agar breach public hai, to uska database online mil sakta hai – dark web forums (jaise RaidForums ke archives), torrents, ya paste sites (Pastebin) pe.
   - Example: "LinkedIn 2012 Breach" ka data torrent sites pe available hai (87GB, 167M accounts).
   - **Safety:** VPN use karo aur virtual machine pe kaam karo taaki malware ya tracking se bacho. Agent Ransack jaise tools se bade files mein search karna aasan hota hai.

4. **Search the Database:**
   - Database download karne ke baad, text editor (Notepad++, Sublime) ya grep commands use karke username search karo (e.g., `grep -i "cyber_sudo" linkedin_breach.txt`).
   - **Kya Mil Sakta Hai:**
     - Associated email: "cyber_sudo@gmail.com"
     - Password hash: "5f4dcc3b5aa765d61d8327deb882cf99" (MD5 hash jo crack ho sakta hai).
     - Phone number ya doosre details, agar breach mein shamil the.
   - **Hash Cracking:** Agar password hashed hai (MD5, SHA-1), to Hashcat ya online tools (hashkiller.io) se plaintext nikal sakte ho – common passwords jaldi crack ho jate hain.

5. **Analyze and Expand:**
   - Jo info mili (email, password), usse doosre platforms pe cross-check karo – jaise email se Instagram ya Twitter account dhoondho.
   - Password reuse ka pattern dekho – agar "password123" mila, to shayad target ne ye kahin aur bhi use kiya ho.

6. **Save Findings:**

- Har detail – username, breach name, email, password, aur source – ko Notion mein table bana ke save karo:

Username	Breach	Email	Password
cyber_sudo	LinkedIn 2012	cyber_sudo@gmail.co	password123

Other Free Websites to Find Leaked Username, Email, Phone Number: HIBP aur DeHashed ke alawa ye free tools bhi kaam aate hain:

- **BreachDirectory (breachdirectory.org):**
  - Username, email, ya IP daal sakte ho. 9B+ records check karta hai aur breach events dikhata hai. Free version mein partial results milte hain.
- **LeakPeek (leakpeek.com):**
  - Email, username, ya password search karo – 8B+ records mein. Free plan mein passwords partially masked hote hain, lekin breach source milta hai.
- **CyberNews Personal Data Leak Check (cybernews.com/personal-data-leak-check):**
  - Username, email, ya phone number (international format, e.g., +919876543210) check karo. Breach ka naam aur compromised data type deta hai.
- **Snusbase (snusbase.com):**
  - Free tier mein limited searches – username ya email se breached data (passwords, IPs) dhoondh sakta hai. Registration chahiye.
- **Intelligence X (intelx.io):**
  - Username ya email se public leaks aur pastes search karta hai. Free tier mein basic results, lekin dark web leaks bhi cover karta hai.
- **Note:** In tools ke free versions mein limitations hote hain – full passwords ya deep data ke liye premium chahiye. Hamesha verify karo ki result target se match karta hai ya nahi (bio, location se cross-check).

Extra Tips:

- **False Positives:** Ek username do logon ka ho sakta hai – profile details (name, pic) se confirm karo.
- **Database Sources:** Torrent sites (The Pirate Bay), dark web markets, ya OSINT communities (Telegram groups) se leaks mil sakte hain – lekin legal aur ethical boundaries dhyan rakhna.
- **Automation:** Sherlock (github.com/sherlock-project/sherlock) se username check karo, phir breached data ke liye upar wale tools use karo.
- **Safety:** Leaked databases download karte waqt antivirus aur isolated environment zaroori hai – malware ka risk hota hai.

Task	Tool	Output
Check Breach	DeHashed/HIBP	Breach Name
Search Database	Grep/Agent Ransack	Emails/Passwords
Expand	Cross-Check	Linked Accounts

Table 15: Methods for Finding Breached Data

Tables

Summary

- DeHashed ya HIBP se username (e.g., cyber_sudo) check karo – breach confirm karo.
- Specific breach database download karo aur search karo – emails, passwords lo.
- Free tools (BreachDirectory, LeakPeek) try karo – findings Notion mein save karo.

Point To Note

Username se passwords aur breached data dhoondhne ke liye pehle **DeHashed** (dehashed.com) ya **HIBP** (haveibeenpwned.com) pe check karo ki leak hua hai ya nahi. Phir specific breach ka database download karke usme username search karo – emails, passwords, ya phone numbers mil sakte hain. Free tools jaise BreachDirectory, LeakPeek, CyberNews bhi try karo – ye sab username, email, ya number ke leaks confirm karte hain. Har finding ko Notion mein save karo aur systematically kaam karo taaki target ka pura compromised data samne aaye – bas ethical limits mein raho aur safety pe dhyan do!

==========

Discovering Additional Online Accounts Automatically

Username enumeration ke zariye additional online accounts automatically dhoondhna OSINT ka ek efficient tareeka hai, jisme aap target ke username ko hundreds of websites pe check karte ho. Ek popular tool hai **Sherlock**, jo username-based search ko automate karta hai aur aapko target ke possible accounts ke links deta hai. Lekin dhyan rakhna zaroori hai – kuch results **false positives** ho sakte hain, matlab link milta hai lekin ya to wo kisi aur ka account hota hai ya "not found" page khulta hai. Ye tool time bachata hai aur manual search ki jagah ek baar mein saare platforms cover karta hai. Chalo iske baare mein detail mein samajhte hain aur kaise use karna hai.

Sherlock – Overview and Usage:

- **What is Sherlock?**
  - Sherlock ek open-source Python tool hai (GitHub: sherlock-project/sherlock), jo 400+ social media sites, forums, aur platforms pe username availability check karta hai. Micah Hoffman aur community ne develop kiya hai.

- **Kaise Kaam Karta Hai:** Aap ek ya zyada usernames daalte ho, aur ye tool har site pe check karta hai ki wo username exist karta hai ya nahi. Results terminal ya file mein save hote hain.

- **Installation:**
  - **Linux (Apt Method):**
    - Terminal mein: `sudo apt install sherlock` (Ubuntu/Debian pe, agar package available ho).
    - Note: Apt se direct install har distro pe nahi kaam karta, to GitHub se manual install zyada reliable hai.
  - **Manual Method (Recommended):**
    1. `git clone https://github.com/sherlock-project/sherlock.git`
    2. `cd sherlock`
    3. `pip3 install -r requirements.txt`
    4. Python 3 pehle se installed hona chahiye (python.org se lo agar nahi hai).

- **Usage:**
  - **Single Username:**
    - Command: `python3 sherlock.py cyber_sudo`
    - Ye "cyber_sudo" ko 400+ sites pe check karega.
  - **Multiple Usernames:**
    - Text file banao (e.g., "usernames.txt") aur usme usernames daal do:

```
cyber_sudo
cybersudo123
csudo
```

    - Command: `python3 sherlock.py -f usernames.txt`
  - **Output:**
    - Terminal mein har site ka result dikhega – green "[+]" matlab account mila, red "[-]" matlab nahi mila.
    - Example:

```
[+] Twitter: https://twitter.com/cyber_sudo
[+] Instagram: https://instagram.com/cyber_sudo
[-] Facebook: https://facebook.com/cyber_sudo
```

    - File mein save karne ke liye: `python3 sherlock.py cyber_sudo --output results.txt`

- **False Positives:**
  - Kuch links kaam karenge lekin account kisi aur ka ho sakta hai (e.g., @cyber_sudo Twitter pe target ka hai, lekin Reddit pe kisi aur ka).
  - **Verify Kaise Karein:** Bio, profile pic, ya posts match karo – agar details align karte hain (location, interests), to shayad target ka hai.

Recap: Username OSINT Process Username se additional accounts dhoondhne ka pura process recap karte hain – ye steps manually aur automatically dono tareeke cover karte hain:

1. **Collect the Person's Username:**

   - Target ke known accounts se usernames lo – e.g., Twitter pe @cyber_sudo, LinkedIn pe cyber-sudo, GitHub pe cybersudo123.
   - Variations bhi note karo (cyber_sudo123, csudo) aur ek text file ya Notion table mein save karo:

```
cyber_sudo
cybersudo123
csudo
```

2. **Search for Usernames on Search Engines:**

   - Google, Bing, ya Yandex pe dorks use karo:
     - **inurl:cyber_sudo OR inurl:cybersudo123** – URL mein username dhoondho.
     - **site:* "cyber_sudo" -inurl:(twitter)** – Twitter ke alawa platforms pe search.
   - Results se naye accounts mile to unhe list mein add karo.

3. **Use People Search Engines/Online Tools:**

   - **Sherlock:** Upar bataye steps se 400+ sites pe automate karke accounts lo.
   - **Other Tools:**
     - **WhatsMyName (whatsmyname.app):** Web-based, multiple usernames ek saath check karo.
     - **IDCrawl (idcrawl.com):** Username se social profiles aur emails dhoondho.
   - Har tool ke results ko manually verify karo – false positives ke liye bio ya activity dekho.

4. **Search in Leaked Databases:**

   - Username breached data mein check karo:
     - **Have I Been Pwned (haveibeenpwned.com):** Username leak hua hai ya nahi.
     - **DeHashed (dehashed.com):** Breach name aur compromised data type lo.
   - Agar leak mila (e.g., "Adobe 2013"), to us database ko download karo (torrents ya dark web se) aur username search karo – emails, passwords mil sakte hain.

5. **Save and Analyze:**

   - Har finding ko Notion mein table bana ke save karo:

Username	Platform	Link	Details	Breach Data
cyber_sudo	Twitter	twitter.com/cyber_su	Tech tweets	N/A
cybersudo123	Reddit	reddit.com/user/cyb	Old posts, 2019	Email: xyz@gmail.com

Extra Tips:

- **Sherlock Options:** `--csv` flag se results CSV mein save karo (`python3 sherlock.py cyber_sudo --csv`).
- **False Positives Avoid Karo:** Profile pics ya bio se cross-check karo – same vibe ya details match karna zaroori hai.
- **Safety:** VPN ya virtual machine use karo – automated tools platforms ke terms violate kar sakte hain.
- **Expand:** Breach se email mila to usse doosre accounts dhoondho (e.g., Instagram pe email search).

Tables

Task	Tool/Method	Output
Collect Usernames	Known Accounts	Username List
Automate Search	Sherlock	400+ Site Links
Verify	Manual/Breach Check	Confirmed Accounts

Table 16: Methods for Discovering Accounts Automatically

Summary

- Sherlock se 400+ sites pe username check karo – single ya multiple usernames automate karo.
- Dorks, WhatsMyName, IDCrawl se refine karo – breached data HIBP/DeHashed se lo.
- False positives verify karo aur Notion mein save karo – full process systematically chalaao.

Point To Note

Sherlock se username enumeration karke hundreds of websites pe accounts automatically dhoondho – `apt install sherlock` ya GitHub (sherlock-project/sherlock) se install karo, aur `python3 sherlock.py cyber_sudo` chala do. Recap mein – usernames collect karo, search engines pe dorks use karo, tools (Sherlock, IDCrawl) se refine karo, aur leaked databases mein breached data lo. False positives ke liye verify karo aur har detail ko Notion mein save karo – ye process target ke online accounts ko pura khol deta hai, bas systematically kaam karo taaki maximum info mile!

==========

Introduction to People OSINT

People OSINT ek aisa tareeka hai jisme hum ek vyakti ke **first name aur last name** ke zariye uske baare mein zyada se zyada personal information uncover karte hain. Is section mein hum focus karenge target ke naam se uski identity, background, aur possible locations tak pahunchne pe. Ek key goal hai **country of origin** pata karna – yani ye naam kis desh se sambandhit hai – aur saath hi **US voter records** jaise resources ka use karke valuable info (jaise address, age, ya affiliations) nikalna. Ye process naam ke basis pe shuru hota hai aur search engines, public records, aur specialized tools ke saath expand hota hai. Ye intro aapko basic framework deta hai jo systematically kaam karta hai taaki target ka pura profile ban sake. Chalo shuru karte hain.

Why People OSINT?

- Har insaan ka naam uski identity ka ek hissa hota hai – first name aur last name se hum ethnicity, cultural background, aur kabhi-kabhi geographic origin tak guess kar sakte hain.
- US voter records jaise public databases additional details dete hain – jaise voting history, address, ya registration status – jo target ko pinpoint karne mein madad karte hain.
- Example: "Rishi Kabra" naam se shuru karke hum India (country of origin) aur Kolkata (possible location) jaise clues pa sakte hain, aur voter records se US mein uska address confirm kar sakte hain agar wo wahan registered hai.

Steps to Uncover Personal Info:

1. **Analyze First and Last Name:**
   - **First Name:** Rishi – ye ek common Indian naam hai, jo Hindu culture mein popular hai (Sanskrit mein "sage" ya "seer").
   - **Last Name:** Kabra – ye ek Indian surname hai, aksar Jain ya Marwari community se juda hota hai, jo Rajasthan ya Gujarat se originate karta hai.
   - **Country of Origin:** Naam ke basis pe India strong candidate hai. Tools jaise **Namsor** (namsor.app) use karo – ye naam ka ethnic origin probability deta hai (e.g., "Rishi Kabra – 95% Indian").
2. **Search Engines Se Shuru Karo:**
   - Google pe simple search: **"Rishi Kabra"** – quotes mein naam daalo taaki exact matches mile.
   - Refine karo: **"Rishi Kabra" India** ya **"Rishi Kabra" Kolkata** agar aapko location ka guess hai.
   - Results mein LinkedIn, Twitter, ya news articles mil sakte hain jo identity confirm karenge.
3. **US Voter Records Check Karo:**
   - Agar target US mein hai, to voter records ek goldmine hain – ye public data hai jo states ke election boards se milta hai.
   - **Websites:**
     – **VoterRecords.com** (voterrecords.com): First name "Rishi" aur last name "Kabra" daalo, country "United States" select karo.

  - **NCSBE Voter Search** (vt.ncsbe.gov): North Carolina jaise states ke liye specific voter lookup.
- **Kya Mil Sakta Hai:** Address (e.g., "123 Main St, Raleigh, NC"), age range (e.g., "30-40"), registration date, aur voting history.
- **Note:** Har state ka data alag hota hai – California, Texas, Florida ke records aksar online hote hain, lekin chhote states mein manual request karni pad sakti hai.

4. **Expand with People Search Tools:**
   - **IDCrawl** (idcrawl.com): "Rishi Kabra" search karo – ye social profiles (LinkedIn, Twitter) aur possible emails dikhayega.
   - **Whitepages** (whitepages.com): US-focused, naam se address, phone, ya relatives tak info de sakta hai.
   - **Spokeo** (spokeo.com): Naam se social media, addresses, aur connections dhoondho.
5. **Country Origin Confirm Karo:**
   - **Forebears** (forebears.io): Last name "Kabra" daalo – ye distribution map deta hai (e.g., 90% India, Gujarat mein zyada).
   - **Ancestry** (ancestry.com): Surname origins aur historical records se origin refine karo – "Kabra" ka link Indian census ya migration records se mil sakta hai.
6. **Save and Build Profile:**
   - Har info – naam, origin (India), US voter address (agar mila), social links – ko Notion mein table bana ke save karo:

First Name	Last Name	Country Origin	Voter Record Address	Social Profile
Rishi	Kabra	India	123 Main St, Raleigh, NC	linkedin.com/in/rishi-kabra

Extra Tips:

- **Variations Try Karo:** "Rishi Kabra" ke saath "R. Kabra" ya "RishiKabra" bhi search karo – usernames mein variations common hote hain.
- **Cross-Check:** Voter records ka address LinkedIn bio ya posts se match karo – consistency se accuracy badhti hai.
- **Limitations:** Voter records sirf US residents ke liye kaam karte hain – agar target India mein hai, to local records (Aadhaar, electoral rolls) chahiye, jo public nahi hote.
- **Ethics:** Public data use karo, lekin privacy laws (GDPR, CCPA) ka dhyan rakho – personal use ke liye legal boundaries mein raho.

Task	Tool/Method	Output
Name Analysis	Namsor/Forebears	Country Origin
Voter Records	VoterRecords.com	Address/Age
Expand	IDCrawl/Spokeo	Social Profiles

Table 17: Methods for People OSINT

Tables

Summary

- First name (Rishi) aur last name (Kabra) se origin (India) guess karo – Namsor/Forebears se confirm.
- Search engines aur voter records (VoterRecords.com) se info lo – address, social links.
- Har detail Notion mein save karo – systematically profile banao.

Point To Note

People OSINT mein **first name (Rishi) aur last name (Kabra)** se shuru karke hum **country of origin (India)** aur **US voter records** (address, age) tak ja sakte hain. Search engines, tools (idcrawl.com, voterrecords.com), aur origin checkers (Namsor, Forebears) ke saath info gather karo. Ye process target ke personal details – jaise location, occupation, ya history – ko uncover karta hai. Har finding ko Notion mein save karo aur systematically kaam karo taaki ek complete profile ban jaye – bas ethical aur legal limits mein raho!

==========

Finding the Geographic Origins of a Name

Name origins dhoondhna OSINT mein ek useful technique hai kyunki ye aapke search ko narrow down karne ke liye **geographical clues** deta hai. Har naam ka ek historical ya cultural root hota hai, jo aapko target ke possible country, region, ya ethnicity ke baare mein hint de sakta hai. Is topic mein hum do websites ka use karenge – **FamilySearch.org** aur **Namsor.app** – jo naam ke geographic origins aur distribution ko samajhne mein madad karte hain. Ye tools alag-alag tareeke se kaam karte hain – ek US-focused database deta hai, doosra global name analysis. Chalo step-by-step dekhte hain kaise inka use karna hai aur kya expect karna hai.

Why Name Origins Matter?

- Ek naam se aap guess kar sakte ho ki target kis region ya country se sambandhit ho sakta hai – jaise "Satyam Singh" sunke India ka khayal aata hai, jabki "John Smith" UK ya US se juda lagta hai.
- Ye clues search ko refine karte hain – agar aapko pata chal jaye ki "Kabra" Gujarat, India se common hai, to aap apna focus wahan shift kar sakte ho.

Step 1: FamilySearch.org

- **Website:** familysearch.org
- **Kya Hai:** Ye ek free genealogy database hai jo US citizens (aur kuch international records) ke historical data ko store karta hai – births, deaths, marriages, census, etc.
- **Kaise Use Karein:**
  1. **Website Pe Jao:** familysearch.org kholo – homepage pe "Search" section milega.
  2. **First aur Last Name Daalo:** Input boxes mein target ka naam type karo – e.g., **First Name:** Satyam, **Last Name:** Singh.
  3. **Search Karo:** "Search" button pe click karo – ye database mein matches dhoondhega.
  4. **Results Dekho:**
     - Agar "Satyam Singh" US mein registered hai, to possible results milenge – jaise "Satyam Singh, born 1990, California" ya "Satyam Singh, census 2010, New York".
     - Har result mein location (city, state), birth year, ya family details ho sakte hain.
- **Limitation:** Ye zyadatar US-focused hai – agar target Turkey, India, ya kisi aur desh mein hai aur US records mein nahi, to kuch nahi milega. Lekin immigrant families ke liye kaam aa sakta hai.
- **Use:** US mein target ka address ya family origin confirm karne ke liye.

Step 2: Namsor.app

- **Website:** namsor.app
- **Kya Hai:** Ye ek name analysis tool hai jo naam ke geographic aur ethnic origins ka probability-based estimate deta hai. Ye global data use karta hai – census, phone books, aur cultural patterns ke basis pe.
- **Kaise Use Karein:**
  1. **Website Pe Jao:** namsor.app kholo – "Name Checker" section pe jao.
  2. **First aur Last Name Daalo:** Input mein naam daalo – e.g., **First Name:** Satyam, **Last Name:** Singh.
  3. **Analyze Karo:** "Check Name" pe click karo – ye naam ka origin calculate karega.
  4. **Output Dekho:**
     - Example Result:
       - **Region:** Asia
       - **Sub-Region:** Southern Asia
       - **Country:** India
       - **Probability:** 95% (Satyam aur Singh dono Indian culture mein common hain).
     - Extra: Gender probability bhi deta hai (e.g., "Male: 98%").
- **Fayda:** Ye global hai – Turkey, Brazil, ya kisi bhi desh ke naam ke liye kaam karta hai, jabki FamilySearch US-limited hai.
- **Use:** Target ke country of origin ya migration pattern samajhne ke liye.

Example Workflow:

- **Target:** "Satyam Singh"
  - **FamilySearch:** Search kiya – "Satyam Singh, 32, lives in Houston, TX" mila. Matlab US mein hai, shayad Indian origin se.
  - **Namsor:** Confirm kiya – "India, Southern Asia, 95% probability". Ye origin India dikhata hai, jo US record ke saath match karta hai (Indian immigrant).
  - **Next Step:** Houston, TX pe focus karke voter records (voterrecords.com) ya social profiles (LinkedIn) dhoondho.

Extra Tools and Tips:

- **Forebears** (forebears.io): Last name "Singh" daalo – ye world map pe distribution dikhayega (e.g., 90% India, Punjab mein zyada).
- **Ancestry** (ancestry.com): Historical records se naam ka US ya global origin refine karo (paid, lekin trial free hai).
- **Google Dorks: "Satyam Singh" India** ya **"Satyam Singh" Houston** – search ko narrow karo.
- **Cross-Check:** Namsor ka country origin aur FamilySearch ka US address match karo – consistency se accuracy badhti hai.
- **Save Karo:** Har clue – origin (India), US location (Houston) – ko Notion mein note karo:

First Name	Last Name	Origin Country	US Location
Satyam	Singh	India	Houston, TX

Tables

Task	Tool	Output
US Records	FamilySearch	Address, Birth Year
Global Origin	Namsor	Country, Probability
Refine	Forebears/Dorks	Distribution, Clues

Table 18: Methods for Finding Name Origins

Summary

- FamilySearch (familysearch.org) se US records lo – address, history.
- Namsor (namsor.app) se global origin confirm karo – country, region.
- Har clue Notion mein save karo – search refine karte jao.

Point To Note

Name origins se geographic clues milte hain – **FamilySearch.org** (familysearch.org) US citizens ke liye records deta hai (e.g., "Satyam Singh, Houston"), jabki **Namsor.app** (namsor.app) global origin dikhata hai (e.g., "India, Southern Asia"). "Satyam Singh" jaise naam se India ka hint milta hai, aur US records se exact location. Ye dono tools search ko refine karte hain – har detail ko Notion mein save karo aur systematically kaam karo taaki target ka background clear ho!

==========

Finding Details Using Advanced Search Techniques

Advanced search techniques ka use karke ek vyakti ke details dhoondhna OSINT mein ek effective tareeka hai, jisme hum **search operators** ke saath target ki information ko search engines (Google, Bing, Yandex) pe check karte hain. Agar target ka naam aur usse related keywords indexed hain, to aap uske baare mein valuable clues – jaise location, education, ya workplace – nikal sakte ho. Is method mein hum **first name aur last name** ko base banate hain aur **city, country, university, ya company** jaise terms ke saath refine karte hain. Ye approach systematic aur flexible hai, jo target ke online presence ko uncover karta hai. Chalo iske format aur use ko detail mein dekhte hain.

Why Use Search Operators?

- Search operators aapke search ko precise banate hain – bina operators ke "Rishi Kabra" search karne pe thousands of irrelevant results milenge, lekin city ya company add karne se focus sharp ho jata hai.
- Indexed info public sources se aati hai – social media, news articles, directories, ya forums – jo target ke real-world details reveal kar sakti hai.

Search Operator Format:

- **Basic Syntax:**
  - **"first and last name" "city" OR "country" OR "university" OR "company"**
  - Quotes ("") exact phrases ke liye hote hain, OR multiple options ke beech choice deta hai.
- **Example:**
  - **"Rishi Kabra" "Kolkata" OR "India" OR "NIT Allahabad" OR "TechMojo"**
  - Ye search Rishi Kabra ke naam ke saath Kolkata (city), India (country), NIT Allahabad (university), ya TechMojo (company) ke mentions dhoondhega.

Steps to Find Details:

1. **Target ka Naam aur Context Pata Karo:**
   - Maan lo target hai "Rishi Kabra". Agar aapko thodi info pehle se pata hai (jaise wo Kolkata mein rehta hai ya TechMojo mein kaam karta hai), to usse starting point banao.

2. **Search Operators Design Karo:**

- Naam ke saath known ya guessed keywords add karo:
  - **"Rishi Kabra" "Kolkata"** – City-based search.
  - **"Rishi Kabra" "India" OR "United States"** – Country options.
  - **"Rishi Kabra" "NIT Allahabad" OR "IIT Delhi"** – Possible universities.
  - **"Rishi Kabra" "TechMojo" OR "Marlabs"** – Companies jahan wo kaam kar sakta hai.
- Ek combined search bhi try karo: **"Rishi Kabra" "Kolkata" OR "India" OR "NIT Allahabad" OR "TechMojo"**.

3. **Search Engines Pe Run Karo:**

- **Google:** Search bar mein daalo – "Rishi Kabra" "Kolkata" OR "India" OR "NIT Allahabad" OR "TechMojo".
- **Bing/Yandex:** Alag engines pe bhi try karo – kabhi unique results milte hain.
- **Results Example:**
  - LinkedIn: "Rishi Kabra, Software Engineer at TechMojo, Kolkata".
  - News: "Rishi Kabra wins hackathon at NIT Allahabad".
  - Forum: "Rishi Kabra from India posted about coding".

4. **Refine aur Expand Karo:**

- **Exclude Irrelevant:** Agar Kolkata ke alawa results chahiye, to: **"Rishi Kabra" -inurl:(Kolkata)**.
- **Site-Specific: site:linkedin.com "Rishi Kabra" "TechMojo"** – LinkedIn pe focus.
- **Add More Keywords: "Rishi Kabra" "Kolkata" "software engineer"** – Job role add karke refine karo.

5. **Analyze Results:**

- Har result ko check karo – kya wo target se match karta hai? Bio, photo, ya context se verify karo.
- Useful info lo – address (Kolkata), education (NIT Allahabad), job (TechMojo).

6. **Save Findings:**

- Har detail ko Notion mein table bana ke save karo:

Name	City	Country	University	Company	Source
Rishi Kabra	Kolkata	India	NIT Allahabad	TechMojo	linkedin.com/in/rishi-kabra

Real-Life Example:

- **Target:** "Satyam Singh"
- **Search: "Satyam Singh" "Delhi" OR "India" OR "JNU" OR "Infosys"**

- **Results:**
  - LinkedIn: "Satyam Singh, Data Analyst at Infosys, Delhi".
  - Article: "Satyam Singh graduates from JNU, 2020".
  - Twitter: "Satyam Singh tweets from India".
- **Conclusion:** Satyam Singh Delhi mein rehta hai, JNU se padha, aur Infosys mein kaam karta hai – ye sab search operators se mila.

Extra Tips:

- **Variations Try Karo:** "Satyam Singh" ke saath "S. Singh" ya "SatyamSingh" bhi search karo.
- **Cached Pages:** Google pe "Cached" option se purani info lo agar current page delete ho gaya ho.
- **Multiple Engines:** Bing ya Yandex pe alag perspective ke liye try karo.
- **Cross-Check:** Ek platform (LinkedIn) se mila detail doosre (Twitter) pe confirm karo – consistency se accuracy badhti hai.
- **Tools:** IDCrawl (idcrawl.com) ya Spokeo (spokeo.com) jaise people search engines bhi use karo agar operators se kaam na bane.

Tables

Task	Method	Output
Design Search	Operators	Refined Query
Run Search	Google/Bing	Links, Clues
Analyze	Cross-Check	Verified Details

Table 19: Methods for Advanced Search Techniques

Summary

- "Rishi Kabra" ke liye operators banaye – "Kolkata" OR "India" OR "NIT Allahabad" OR "TechMojo".
- Google, Bing pe run karo – location, education, job lo.
- Har finding Notion mein save karo – systematically refine karo.

Point To Note

Advanced search techniques mein **"first and last name" "city" OR "country" OR "university" OR "company"** jaise operators se target ki info indexed hai ya nahi check karo. "Rishi Kabra" ke liye **"Kolkata" OR "India" OR "NIT Allahabad" OR "TechMojo"** try karke location, education, aur job details lo. Ye method search engines ke power ko use karta hai – har finding ko Notion mein save karo aur systematically kaam karo taaki target ka pura profile ban jaye!

==========

Discovering Social Media Accounts Linked to a Person

Discovering social media accounts linked to a person ek zaroori OSINT skill hai jo target ke online presence ko samajhne mein madad karti hai. Iske liye **people search engines** ka use hota hai – ye websites individuals ke baare mein info dhoondhne ke liye banayi gayi hain aur kisi bhi country ke users ke liye kaam kar sakti hain. Do popular free tools hain – **IDCrawl (idcrawl.com)** aur **Social-Searches (social-searches.com)** – jo social media profiles, public records, aur doosre sources se data collect karte hain. Ye search engines personal info jaise usernames, emails, phone numbers, aur social media accounts ko public records, marketing companies, data brokers, aur social platforms se aggregate karke ek jagah pesh karte hain. Chalo dekhte hain kaise ye kaam karte hain aur target ke social media accounts tak kaise pahunch sakte hain.

What Are People Search Engines?

- People search engines online tools hain jo individuals ke baare mein publicly available info ko organize karte hain.
- **Sources:**
  - **Public Records:** Voter lists, property records, court documents.
  - **Marketing Companies/Data Brokers:** Consumer data jo companies collect karti hain (e.g., Acxiom, Experian).
  - **Social Media Profiles:** Facebook, Twitter, Instagram, LinkedIn se public posts ya bio info.
- **Goal:** Ek naam ya username se shuru karke target ke linked social media accounts aur personal details tak jana.

Tool 1: IDCrawl (idcrawl.com)

- **Website:** https://www.idcrawl.com
- **Kya Hai:** Ye ek free people search engine hai jo social media profiles, deep web data, phone numbers, emails, aur criminal records ko aggregate karta hai.
- **Kaise Use Karein:**
  1. Homepage pe jao – search bar mein target ka naam daalo (e.g., "Rishi Kabra").
  2. Optional: Country ya state filter laga sakte ho (e.g., "United States" ya "India").
  3. Search karo – results mein social media links milenge:
     - Twitter: `twitter.com/rishi_kabra`
     - Instagram: `instagram.com/rishikabra`
     - LinkedIn: `linkedin.com/in/rishi-kabra`
  4. Har link ko check karo – bio, pics, ya posts se verify karo ki ye target ka account hai.
- **Fayda:** Global coverage deta hai – kisi bhi country ke users ke liye kaam karta hai. Social media ke saath emails ya phone numbers bhi suggest kar sakta hai.
- **Note:** Kuch results outdated ya false positives ho sakte hain – manual verification zaroori hai.

Tool 2: Social-Searches (social-searches.com)

- **Website:** https://www.social-searches.com
- **Kya Hai:** Ye bhi ek free tool hai jo specifically social media accounts dhoondhne pe focus karta hai – Facebook, Twitter, Instagram, etc.
- **Kaise Use Karein:**
  1. Site kholo – search box mein naam ya username daalo (e.g., "cyber_sudo").
  2. Platform select karo (e.g., "All" ya "Twitter only").
  3. Search karo – results new tab mein khulenge:
     - `facebook.com/cyber_sudo`
     - `twitter.com/cyber_sudo`
  4. Profiles analyze karo – activity ya details match karte hain ya nahi.
- **Fayda:** Direct social media links deta hai aur simple interface ke saath fast hai. Kisi bhi desh ke users ke liye kaam karta hai.
- **Note:** Sirf public profiles hi dikhta hai – private accounts nahi milega.

How These Tools Help:

- **Social Media Discovery:** IDCrawl aur Social-Searches target ke naam ya username se saare linked accounts dhoondh sakte hain – jaise agar "Rishi Kabra" LinkedIn pe hai, to shayad Instagram ya Twitter pe bhi mile.
- **Extra Info:** IDCrawl emails ya phone numbers bhi de sakta hai jo bio se scrape kiye hote hain (e.g., "rishi.kabra@gmail.com").
- **Global Reach:** Dono tools kisi bhi country ke users ke liye kaam karte hain – India, US, Turkey, ya kahin aur.

Workflow Example:

- **Target:** "Satyam Singh"
- **IDCrawl:**
  - Search: "Satyam Singh" + "India"
  - Results:
    - `twitter.com/satyam_singh` – Tech tweets, Delhi se.
    - `linkedin.com/in/satyam-singh` – Data Analyst, Infosys.
    - Suggested email: "satyam.singh@gmail.com".
- **Social-Searches:**
  - Search: "satyam_singh"
  - Results:
    - `instagram.com/satyam_singh` – Photos from Delhi.
    - `facebook.com/satyam.singh.123` – Public posts.

- **Verification:** Bio (Delhi, tech interest) aur profile pics match karte hain – ye ek hi person ke accounts hain.

Extra Tips:

- **Cross-Check:** Ek tool se mila account doosre tool ya Google pe verify karo – **"Satyam Singh" site:twitter.com**.
- **False Positives:** Same naam ke alag log ho sakte hain – details (location, job) se confirm karo.
- **Expand:** Email ya phone mila to usse Sherlock (github.com/sherlock-project/sherlock) ya Have I Been Pwned (haveibeenpwned.com) pe check karo.
- **Save Karo:** Har account – link, platform, aur key info – ko Notion mein table banao:

Name	Platform	Link	Details
Satyam Singh	Twitter	twitter.com/satyam_sin	Tech tweets, Delhi
Satyam Singh	LinkedIn	linkedin.com/in/satyam singh	Infosys, Analyst

Tables

Task	Tool	Output
Search Accounts	IDCrawl	Social Links, Emails
Find Profiles	Social-Searches	Direct Platform Links
Verify	Manual Check	Confirmed Accounts

Table 20: Methods for Discovering Social Media Accounts

Summary

- IDCrawl (idcrawl.com) se social links aur emails lo – global coverage.
- Social-Searches (social-searches.com) se direct profiles dhoondho – fast aur simple.
- Verify karo aur Notion mein save karo – target ka network uncover karo.

Point To Note

IDCrawl (idcrawl.com) aur **Social-Searches** (social-searches.com) jaise free people search engines se target ke social media accounts dhoondhna aasan hai. Ye tools public records, social profiles, aur data brokers se info collect karte hain aur kisi bhi country ke users ke liye kaam karte hain. Naam daalo, results lo, aur verify karo – har finding ko Notion mein save karo taaki target ka online network pura samajh aaye. Systematic kaam karo aur false positives se bacho – ye aapke OSINT game ko next level pe le jayega!

==========

Discovering Phone Numbers, Addresses, and More

People search engines ek aisa powerful tareeka hai jisse aap individuals ke baare mein detailed info dhoondh sakte hain, khaas taur pe **US citizens** ke liye. Ye websites aapko target ka **full name, phone numbers, physical addresses, aur relatives** jaise details de sakti hain, jo public records, social media, aur data brokers se collect kiye jate hain. Ye tools OSINT ke liye kaafi useful hain kyunki ye ek naam se shuru karke pura profile bana sakte hain. Neeche diye gaye websites US-focused hain aur inka use karke aap US mein rehne wale logon ki info nikal sakte ho. Chalo har website ko samajhte hain aur kaise ye kaam karti hain.

What You Can Find:

- **Full Name:** Legal name aur aliases (nicknames ya variations).
- **Phone Numbers:** Landline, mobile, aur past numbers jo target se juda ho sakte hain.
- **Physical Addresses:** Current aur previous addresses (e.g., "123 Main St, Raleigh, NC").
- **Relatives:** Family members ya associates ke naam (e.g., parents, siblings).
- Ye sab info public records (voter lists, property records) aur online sources se aati hai.

Websites for US Citizens:

1. **TruePeopleSearch (www.truepeoplesearch.com)**
   - **Kya Hai:** Ek free people search engine jo US adults ke billions of records se data deta hai – addresses, phone numbers, emails, relatives, sab free mein.
   - **Kaise Use Karein:**
     - Homepage pe jao, full name (e.g., "Rishi Kabra"), phone number, ya address daalo.
     - Results mein current address, phone numbers, relatives, aur past locations milenge.
   - **Special Note:** Ye site sirf US IP addresses se kaam karti hai – agar aap US ke bahar ho (jaise India), to VPN use karna padega (e.g., NordVPN, set to US server).
   - **Fayda:** 100% free, no signup, detailed results instantly.
2. **Nuwber (www.nuwber.com)**
   - **Kya Hai:** Ek US-focused search engine jo naam, phone, ya address se info deta hai – addresses, phone numbers, relatives, aur kabhi job history bhi.
   - **Kaise Use Karein:** Naam daalo (e.g., "Satyam Singh"), search karo – free mein basic info milega, detailed report ke liye payment chahiye.
   - **Fayda:** Clean interface aur reverse phone lookup ka option.
   - **Note:** Free results limited hote hain – premium ke liye pay karna pad sakta hai.
3. **FastPeopleSearch (www.fastpeoplesearch.com)**
   - **Kya Hai:** 16.5 billion records ke saath ek free tool, jo US-only data deta hai – names, addresses, phones, relatives.
   - **Kaise Use Karein:** Naam, phone, ya address se search karo – results fast aur accurate hote hain.

- **Fayda:** Reverse phone lookup aur address lookup dono ke liye strong.
- **Note:** Non-US residents ke liye kaam nahi karta – US-specific hai.

4. **FastBackgroundCheck (www.fastbackgroundcheck.com)**
   - **Kya Hai:** US citizens ke liye ek aur free search engine – basic info jaise addresses, phones, aur relatives deta hai.
   - **Kaise Use Karein:** Naam ya phone number daalo – instant results free mein, lekin deep background checks ke liye payment option hai.
   - **Fayda:** Simple aur quick, basic OSINT ke liye kaafi.
   - **Note:** Premium features (criminal records) ke liye pay karna padta hai.
5. **ThatsThem (www.thatsthem.com)**
   - **Kya Hai:** Ek 100% free tool jo US mein phone numbers, addresses, emails, aur relatives dhoondhta hai – no ads, no fees.
   - **Kaise Use Karein:** Naam, address, ya phone se search karo – results mein full profile milta hai.
   - **Fayda:** Privacy-focused aur ad-free experience.
   - **Note:** US ke bahar ke data ke liye kaam nahi karta.
6. **Radaris (www.radaris.com)**
   - **Kya Hai:** 183 million unique names aur 594 million people records ke saath ek bada database – addresses, phones, relatives, aur property info deta hai.
   - **Kaise Use Karein:** Naam, phone, ya address daalo – free mein basic info, premium mein criminal records bhi.
   - **Fayda:** Extensive data aur business records bhi cover karta hai.
   - **Note:** Free results mein limitation, full access ke liye subscription.

Workflow Example:

- **Target:** "Rishi Kabra"
- **TruePeopleSearch:**
  - Search: "Rishi Kabra" + VPN (US server).
  - Result: "123 Main St, Raleigh, NC", phone "919-555-1234", relatives "Anita Kabra".
- **FastPeopleSearch:**
  - Search: "919-555-1234" (reverse lookup).
  - Result: Confirms "Rishi Kabra, Raleigh, NC".
- **Radaris:**
  - Search: "Rishi Kabra".
  - Result: Past address "456 Oak St, Charlotte, NC", email "rishi.kabra@gmail.com".
- **Conclusion:** Rishi Kabra Raleigh, NC mein rehta hai, uska phone number aur family details mile.

Extra Tips:

- **VPN Use:** TruePeopleSearch jaise sites ke liye US VPN server (e.g., ExpressVPN, NordVPN) set karo agar aap US ke bahar ho.
- **Cross-Check:** Ek site se mila phone ya address doosre pe verify karo – accuracy badhti hai.
- **Expand:** Email mila to usse Sherlock (github.com/sherlock-project/sherlock) ya HIBP (haveibeenpwned.com) pe check karo breached data ke liye.
- **Save Karo:** Har detail ko Notion mein table banao:

Name	Address	Phone	Relatives	Source
Rishi Kabra	123 Main St, Raleigh, NC	919-555-1234	Anita Kabra	TruePeopleSearch

Tables

Task	Tool	Output
Search Info	TruePeopleSearch	Address, Phone
Verify Data	FastPeopleSearch	Confirmed Details
Expand	Radaris	Past Addresses, Email

Table 21: Methods for Discovering Phone Numbers and Addresses

Summary

- TruePeopleSearch (truepeoplesearch.com) se free detailed info lo – VPN ke saath.
- Nuwber, FastPeopleSearch, ThatsThem se phones, addresses verify karo – US-focused.
- Har finding Notion mein save karo – profile systematically banao.

Point To Note

TruePeopleSearch, Nuwber, FastPeopleSearch, FastBackgroundCheck, ThatsThem, aur Radaris US citizens ke liye phone numbers, addresses, aur relatives dhoondhne ke top free tools hain. Ye sites public records aur online data se info laati hain – TruePeopleSearch ke liye VPN chahiye agar US ke bahar ho. Har tool se results lo, verify karo, aur Notion mein save karo taaki target ka pura profile ban jaye – systematically kaam karo aur maximum info collect karo!

==========

Uncovering Political Party Affiliation

Uncovering political party affiliation ek important aspect hai jab baat OSINT ki aati hai, khaas taur pe United States mein, jahan **voter records** publicly accessible hote hain. Ye records ek treasure trove hain jo target ke baare mein detailed info dete hain – jaise **full name, party affiliation, home addresses, date of birth, aur relatives**. US mein har state ke voter registration data ko public access ke liye available karaya jata hai (state laws ke according), aur is data ko online tools aur websites ke zariye dhoondha ja sakta hai. Is topic mein hum teeno websites – **VoterRecords.com**, **VoteRef.com**, aur **BlackBookOnline.info** – ka use samajhenge jo voter records se political affiliation aur doosri details uncover karne mein madad karte hain. Chalo step-by-step dekhte hain kaise ye kaam karta hai.

Why Voter Records Matter?

- US mein voter records public hote hain taaki transparency aur election integrity bani rahe – political campaigns, researchers, aur general public is data ka use kar sakte hain.
- Har record mein typically ye info hoti hai:
  - **Full Name:** Legal name (e.g., "Rishi Kabra").
  - **Party Affiliation:** Democratic, Republican, Independent, ya Unaffiliated.
  - **Home Addresses:** Current aur past residential addresses.
  - **Date of Birth:** Age ya birth year (state ke hisab se full date ya partial).
  - **Relatives:** Family members jo same address pe registered ho sakte hain.
- Ye details target ke political leanings, location, aur personal network ko samajhne mein madad karti hain.

Websites to Uncover Political Party Affiliation:

1. **VoterRecords.com (https://voterrecords.com)**
   - **Kya Hai:** Ye ek free political research tool hai jo 100 million+ US voter records ko cover karta hai. State aur local election offices se data collect karta hai.
   - **Kaise Use Karein:**
     - Homepage pe jao, "Search by Name" mein full name daalo (e.g., "Rishi Kabra").
     - Optional: City, state, ya ZIP code add karo (e.g., "Raleigh, NC").
     - Search karo – results mein voter records ka list milega.
   - **Sample Output:**
     - "Rishi Kabra, Raleigh, NC, Party: Democratic, Address: 123 Main St, DOB: 1990".
   - **Fayda:** Free, easy-to-use, aur detailed – party affiliation ke saath address aur age bhi deta hai.
   - **Note:** Data state-specific hai – agar target registered nahi hai, to nahi milega.
2. **VoteRef.com (https://voteref.com)**
   - **Kya Hai:** Ye ek on-demand voter registration lookup tool hai jo state aur local election officials se data laata hai. Transparency aur voter participation ke liye banaya gaya hai.

- **Kaise Use Karein:**
  - Site kholo, "Voters" section mein naam daalo (e.g., "Satyam Singh").
  - Filters laga sakte ho – state (e.g., "Texas"), county, ya age range.
  - Results dekho – har record mein party affiliation, address, aur DOB hota hai.
- **Sample Output:**
  - "Satyam Singh, Houston, TX, Party: Republican, Address: 456 Oak St, DOB: 1985".
- **Fayda:** Filters ke saath refine karna aasan hai, aur non-commercial use ke liye free hai.
- **Note:** Sirf US-based users ke liye hai – VPN chahiye agar bahar se access karna ho.

3. **BlackBookOnline.info (https://www.blackbookonline.info)**

- **Kya Hai:** Ye ek free public records directory hai jo voter registration searches ke liye state-specific links deta hai. Voter records ke alawa criminal records bhi cover karta hai.
- **Kaise Use Karein:**
  - Homepage pe "Voter Registration Records" pe click karo.
  - State select karo (e.g., "California"), phir naam daalo (e.g., "Rishi Kabra").
  - Ye aapko state ke official voter lookup page pe redirect karega jahan party affiliation milega.
- **Sample Output:**
  - California voter lookup se: "Rishi Kabra, Party: Independent, Address: 789 Pine St, LA".
- **Fayda:** State-wise direct access deta hai, aur free hai.
- **Note:** Har state ka interface alag hota hai – thoda time lag sakta hai navigation mein.

Workflow Example:

- **Target:** "Satyam Singh"
- **VoterRecords.com:**
  - Search: "Satyam Singh, Houston, TX".
  - Result: "Satyam Singh, Party: Republican, 456 Oak St, Houston, TX, DOB: 1985".
- **VoteRef.com:**
  - Search: "Satyam Singh" + Texas filter.
  - Result: Confirms "Republican, 456 Oak St, Age: 40".
- **BlackBookOnline.info:**
  - Texas voter lookup redirect – same info mila.
- **Conclusion:** Satyam Singh Houston mein rehta hai aur Republican party se affiliated hai – teeno sources se consistent data.

Extra Tips:

- **Cross-Check:** Ek site se mili party affiliation ko doosre pe verify karo – consistency se accuracy badhti hai.
- **Variations:** "Satyam Singh" ke saath "S. Singh" ya "SatyamSingh" bhi try karo – records mein naam alag ho sakta hai.
- **Limitations:** Sirf registered voters ka data milega – agar target US citizen nahi ya unregistered hai, to kuch nahi milega.
- **Save Karo:** Har detail ko Notion mein table banao:

Name	Party	Address	DOB	Relatives	Source
Satyam Singh	Republican	456 Oak St, Houston, TX	1985	Anita Singh	VoterRecords.com

Tables

Task	Tool	Output
Search Records	VoterRecords.com	Party, Address
Refine Data	VoteRef.com	Filtered Results
State Access	BlackBookOnline	Official Records

Table 22: Methods for Uncovering Party Affiliation

Summary

- VoterRecords.com se party affiliation aur address lo – free aur detailed.
- VoteRef.com se filters ke saath refine karo – VoteRef.com aur BlackBookOnline state data deta hai.
- Notion mein save karo – political profile banao systematically.

Point To Note

US mein voter records se political party affiliation dhoondhna asaan hai kyunki ye public hai – **VoterRecords.com** (voterrecords.com), **VoteRef.com** (voteref.com), aur **BlackBookOnline.info** (blackbookonline.info) ke saath full name, party (Democratic, Republican, etc.), address, DOB, aur relatives tak jao. Naam daalo, search karo, aur verify karo – har finding ko Notion mein save karo taaki target ka political profile clear ho. Systematic kaam karo aur state-specific limits dhyan rakhna – ye OSINT ko next level pe le jata hai!

==========

Finding Partners and Maiden Names in Registries

Wedding aur baby registries ek unique OSINT resource hain jo personal details jaise **partners' names, maiden names, event details, aur desired items** uncover karne mein madad karte hain. Ek **registry** hoti hai ek list jisme log apne events (wedding, baby shower) ke liye chahiye wali gifts daalte hain, aur ye public ya semi-public hoti hai jab online platforms pe banayi jati hai. Har registry mein target ke saath jude logon (partner, family) aur unki identity ke clues mil sakte hain – jaise maiden name jo shadi ke baad badal jata hai. Is topic mein hum samajhenge kaise in registries ka use karke info nikali jaye, aur Recap section mein pura process ko summarize karenge. Chalo shuru karte hain.

What Are Wedding/Baby Registries?

- Ek registry ek wish list hoti hai jo couples ya parents-to-be banate hain – jaise wedding gifts (cookware, furniture) ya baby items (diapers, crib).
- **Common Platforms:**
  - Wedding: **The Knot** (theknot.com), **Zola** (zola.com), **MyRegistry** (myregistry.com).
  - Baby: **Babylist** (babylist.com), **Amazon Baby Registry** (amazon.com/babyreg).
- **What's Included:**
  - **Partner Name:** Spouse ya co-parent ka naam (e.g., "Rishi Kabra & Priya Sharma").
  - **Maiden Name:** Bride ka original surname jo shadi ke baad change ho sakta hai (e.g., "Priya Sharma" se "Priya Kabra").
  - **Event Details:** Date, location, ya occasion type (e.g., "Wedding: June 15, 2024, Kolkata").
  - **Desired Items:** Gifts ki list jo shopping patterns ya lifestyle dikhati hai.

Steps to Find Partners and Maiden Names in Registries:

1. **Target ka Naam aur Context Pata Karo:**
   - Maan lo target hai "Rishi Kabra". Agar aapko city (Kolkata) ya event year (2024) ka idea hai, to search refine ho sakti hai.
2. **Registry Websites Pe Search Karo:**
   - **The Knot:**
     - theknot.com/registry pe jao, "Find a Couple" mein "Rishi Kabra" daalo.
     - Result: "Rishi Kabra & Priya Sharma, Wedding: June 15, 2024, Kolkata".
     - Maiden Name: "Priya Sharma" (ab shayad Priya Kabra).
   - **Zola:**
     - zola.com/wedding pe search karo – "Rishi Kabra".
     - Result: "Rishi & Priya, Kolkata, June 2024".
   - **Babylist:**
     - babylist.com pe "Find a Registry" mein naam daalo – "Priya Kabra".

- Result: "Priya Kabra & Rishi Kabra, Baby Due: Dec 2024, Raleigh, NC".

- **Amazon:**
  - amazon.com/registry pe "Rishi Kabra" search karo – agar public hai, to partner ya items dikhega.

3. **Google Dorks Ka Use Karo:**
   - Agar direct registry nahi milti, to:
     - **"Rishi Kabra" "Priya" site:theknot.com**
     - **"Rishi Kabra" "wedding" "Kolkata"**
     - **"Priya Kabra" "baby registry" site:babylist.com**
   - Results se registry links ya mentions mil sakte hain.

4. **Details Verify aur Expand Karo:**
   - Partner ka naam (Priya Sharma) mila to uska social media (LinkedIn, Instagram) dhoondho – maiden name se purani identity confirm ho sakti hai.
   - Event location (Kolkata) ya date (June 2024) se timeline banao.

5. **Save Findings:**
   - Har detail ko Notion mein table banao:

Name	Partner	Maiden Name	Event	Location	Source
Rishi Kabra	Priya Sharma	Sharma	Wedding, Jun 2024	Kolkata	The Knot

Recap: Full People OSINT Process Pura process recap karte hain jo naam se shuru hokar registries tak jata hai:

1. **Use Search Engines to Find the Person by Their Name and City:**
   - Google pe: **"Rishi Kabra" "Kolkata"** – basic info ya social profiles lo.
   - Refine: **"Rishi Kabra" "wedding" "Kolkata"** – registry hints ke liye.

2. **Learn Where the Name Comes From:**
   - **Namsor.app** (namsor.app): "Rishi Kabra" – Origin: India (95% probability).
   - **Forebears.io** (forebears.io): "Kabra" – Gujarat, India mein common.

3. **Search in People Search Engines:**
   - **IDCrawl.com** (idcrawl.com): "Rishi Kabra" – Twitter, LinkedIn profiles, possible emails.
   - **TruePeopleSearch.com** (truepeoplesearch.com): US address ya phone number (VPN ke saath).

4. **See If They Are in Voter Records:**
   - **VoterRecords.com** (voterrecords.com): "Rishi Kabra" – Party: Democratic, Address: Raleigh, NC.

- Voter data se US location ya relatives confirm karo.

5. **Search in Wedding/Baby Registries:**
   - **The Knot/Zola:** "Rishi Kabra" – Partner: Priya Sharma, Maiden Name: Sharma.
   - **Babylist:** "Priya Kabra" – Baby due Dec 2024, Raleigh, NC.
   - Partner aur maiden names se family network expand karo.

Extra Tips:

- **Cross-Check:** Registry se mila partner naam voter records ya social media pe verify karo.
- **Privacy:** Aksar registries public hoti hain, lekin private bhi ho sakti hain – tab Google dorks try karo.
- **Expand:** Maiden name (Sharma) se Priya ke purane accounts (e.g., LinkedIn pe "Priya Sharma") dhoondho.
- **Save:** Notion mein har step ka result organize karo taaki timeline aur connections clear hon.

Tables

Task	Tool/Method	Output
Search Registries	The Knot/Zola	Partner, Event
Google Dorks	Site-Specific	Registry Links
Verify	Social Media	Confirmed Details

Table 23: Methods for Finding Partners and Maiden Names

Summary

- The Knot, Zola se partner (Priya Sharma) aur maiden name (Sharma) lo.
- Babylist se baby details aur location – Google dorks se refine karo.
- Notion mein save karo – full OSINT process se profile banao.

Point To Note

Wedding/baby registries se **partners (Priya Sharma)** aur **maiden names (Sharma)** nikalna ek smart OSINT move hai – **The Knot** (theknot.com), **Zola** (zola.com), **Babylist** (babylist.com) jaise platforms pe search karo. Recap mein – search engines, name origins (Namsor), people search (IDCrawl), voter records (VoterRecords), aur registries ke saath pura profile banao. Har detail ko Notion mein save karo – ye target ke personal life ko khol deta hai, bas systematically kaam karo taaki maximum info mile!

==========

Uncovering Emails from Social/Online Accounts

Email OSINT mein **uncovering emails from social/online accounts** ek key technique hai jo target ke contact details tak pahunchne mein madad karti hai. Bahut se log apne **email addresses** ko social media profiles, websites, ya online platforms pe share karte hain – chahe wo networking, business, ya personal reasons ke liye ho. Ye emails direct bio mein, posts mein, ya specific sections (jaise YouTube ke "About" tab) mein mil sakte hain. Is topic mein hum focus karenge ki kaise target ke online presence – khaas taur pe social media aur YouTube channels – se emails dhoondhe jayein. Ek simple process hai YouTube ke liye jo hum detail mein cover karenge. Chalo shuru karte hain.

Why Check Social/Online Accounts for Emails?

- Emails ek direct link hote hain target tak – ye login credentials, breached data verification, ya communication tracing ke liye use ho sakte hain.
- **Common Platforms:**
  - **Twitter:** Bio ya pinned tweet mein (e.g., "DM me at rishi.kabra@gmail.com").
  - **LinkedIn:** "Contact Info" section mein.
  - **Instagram:** Bio mein ya "Email" button pe.
  - **YouTube:** "About" tab mein business/personal email.
- Log apne emails share karte hain taaki followers, clients, ya friends unse connect kar sakein – aur ye OSINT ke liye goldmine hai.

Steps to Uncover Emails:

1. **Check Social Media Profiles:**
   - **Twitter:**
     - Target ka profile kholo (e.g., `twitter.com/rishi_kabra`).
     - Bio dekho – "Email: rishi.kabra@gmail.com" ya "Contact me at..." jaisa ho sakta hai.
     - Pinned tweet ya replies mein bhi email mention ho sakta hai.
   - **Instagram:**
     - Bio mein email ho sakta hai (e.g., " rishi.kabra@gmail.com").
     - Business accounts pe "Email" button hota hai – click karke dekho.
   - **LinkedIn:**
     - Profile pe "Contact Info" section kholo – email public hai agar target ne share kiya ho (e.g., "rishi.kabra@techmojo.com").
   - **Facebook:**
     - "About" tab mein "Contact and Basic Info" check karo – email kabhi public hota hai agar privacy settings loose hain.
2. **Find Email from YouTube Channel:**
   - Bahut se log YouTube channels banate hain (personal, business, ya vlogs) aur wahan email share karte hain. Steps:

     (a) **Open the YouTube Channel:**

- Target ka channel dhoondho (e.g., `youtube.com/@RishiKabra`). Naam ya content se search karo.

(b) **Click on About ¿ View Email Address:**

- Channel homepage pe "About" tab pe jao.
- "Details" section mein "View Email Address" button dikhega (business accounts ke liye common).
- Click karo – email milega (e.g., "rishi.kabra@gmail.com") agar target ne public kiya ho.

- **Note:** Agar button nahi dikhta, to "For business inquiries" ya "Send email" link ho sakta hai – uspe click karke email reveal hota hai.

3. **Google Dorks Ka Use:**

- Agar direct email nahi milta, to Google pe search karo:
  - **"Rishi Kabra" "email" site:youtube.com** – YouTube pe email mentions.
  - **"Rishi Kabra" "@gmail.com" OR "@yahoo.com"** – Common email domains ke saath.
  - **"Rishi Kabra" "contact" site:twitter.com** – Twitter pe contact info.

4. **Verify aur Expand:**

- Email mila (e.g., "rishi.kabra@gmail.com") to usse:
  - **Have I Been Pwned** (haveibeenpwned.com): Check karo ki breached hai ya nahi.
  - **Sherlock** (github.com/sherlock-project/sherlock): Email ke username part (rishi.kabra) ko doosre platforms pe search karo.
- Multiple emails ho sakte hain – personal (gmail) aur professional (company domain).

5. **Save Findings:**

- Har email ko Notion mein table bana ke save karo:

Name	Email	Source	Details
Rishi Kabra	rishi.kabra@gmail.co	YouTube	Personal channel
Rishi Kabra	rishi@techmojo.com	LinkedIn	Work email

Workflow Example:

- **Target:** "Satyam Singh"
- **Twitter:** Bio mein "satyam.singh@gmail.com" mila.
- **YouTube:**
  - Channel: `youtube.com/@SatyamSinghTech`
  - About ¿ View Email Address: "satyamtech@gmail.com".
- **LinkedIn:** "Contact Info" se "satyam.singh@infosys.com".
- **Conclusion:** Satyam ke teen emails mile – personal, YouTube, aur professional.

Extra Tips:

- **Variations:** "SatyamSingh" ya "satyam_singh" jaise usernames bhi check karo – email IDs aksar usernames se bante hain.
- **Old Posts:** Social media ke purane posts ya comments mein email ho sakta hai – Wayback Machine (archive.org) se check karo.
- **Business Accounts:** YouTube ya Instagram pe business profiles zyada email share karte hain.
- **Cross-Check:** Email ko social platforms pe search karo – matching profiles confirm karte hain.

Tables

Task	Method	Output
Check Profiles	Social Media	Emails from Bio
YouTube Search	About Tab	Business Email
Verify	HIBP/Sherlock	Confirmed Emails

Table 24: Methods for Uncovering Emails

Summary

- Twitter, LinkedIn se bio mein emails lo – YouTube ke "About" se business emails.
- Google dorks se refine karo – "Rishi Kabra" "email" site:youtube.com.
- Notion mein save karo – target ka contact network banao.

Point To Note

Social/online accounts se emails dhoondhna simple hai – **Twitter, Instagram, LinkedIn** ke bio ya **YouTube** ke "About" tab mein check karo. YouTube ke liye channel kholo, "About" pe jao, aur "View Email Address" se email lo (e.g., "rishi.kabra@gmail.com"). Google dorks se bhi refine karo – har email ko Notion mein save karo taaki target ka contact network clear ho. Systematic kaam karo aur har platform pe dhyan do – ye OSINT ko ek step aage le jata hai!

==========

Uncovering Emails Linked to Usernames

Uncovering emails linked to usernames ek smart OSINT technique hai jisme aap target ke social media profiles se collect kiye gaye usernames ko use karke potential **email addresses** banate ho aur unhe verify karte ho. Bahut se log apne usernames ko hi email ID ka base banate hain (e.g., saadsarraj se saadsarraj@gmail.com), aur ye pattern guesswork ko effective bana deta hai. Is process mein hum usernames se emails generate karenge, unhe tools se validate karenge, aur phir social platforms (jaise Facebook) pe check karenge ki kaun sa email target se linked

hai. Ek website – **Experte.com** – bhi explore karenge jo email generation aur verification mein madad karta hai. Chalo step-by-step samajhte hain aur kaise ye kaam karta hai.

Why Usernames as Emails?

- Log aksar apne social media usernames ko email addresses ke roop mein use karte hain – jaise @saadsarraj Twitter pe hai to shayad saadsarraj@gmail.com bhi ho.
- Common domains jaise Gmail, Hotmail, Outlook, ya Yahoo ke saath ye pattern bahut dekha jata hai.
- Isse email guessing aur verification se target ke actual contact details tak pahuncha ja sakta hai.

Steps to Uncover Emails Linked to Usernames:

1. **Collect Usernames from Social Media:**
   - Target ke profiles check karo – Twitter, Instagram, LinkedIn, GitHub, etc.
   - Example: Target "Saad Sarraj" ke usernames mile:
     - Twitter: @saadsarraj
     - Instagram: @saadsarraj123
     - GitHub: saadsarraj
   - Inhe ek list mein save karo (Notion ya text file):

```
saadsarraj
saadsarraj123
```

2. **Generate Potential Email Addresses:**
   - Har username ke saath common email domains add karo:
     - saadsarraj@gmail.com
     - saadsarraj@hotmail.com
     - saadsarraj@outlook.com
     - saadsarraj123@gmail.com
   - Variations bhi socho – numbers (saadsarraj123), dots (saad.sarraj), ya initials (ssarraj).
   - **Note:** Ye manual guessing hai, lekin tools isse automate kar sakte hain (neeche dekho).

3. **Use Experte.com for Generation and Verification:**
   - **Website:** experte.com (Email Finder tool)
   - **Kaise Use Karein:**
     (a) Homepage pe jao – "Email Finder" section mein username daalo (e.g., "saadsarraj").
     (b) "Find Email" pe click karo – ye common domains ke saath email list generate karega:
       - saadsarraj@gmail.com
       - saadsarraj@hotmail.com
       - saadsarraj@outlook.com

(c) Verification: Har email ke against ye check karta hai ki email valid hai ya nahi (SMTP check ke zariye).

- **Output Example:**
  - saadsarraj@gmail.com – Valid
  - saadsarraj@hotmail.com – Invalid
- **Fayda:** Ek hi jagah generation aur validation – time bachta hai.

4. **Verify Emails with Social Platforms (Facebook Method):**

- Valid emails milne ke baad, check karo kaun sa email target se linked hai:
- **Facebook Forgot Password:**
  (a) `facebook.com` pe jao, "Forgot Password" pe click karo.
  (b) "Find Your Account" mein username ya naam daalo (e.g., "Rishi Kabra").
  (c) "This is my account" pe click karo – ye email options dikhayega.
  (d) Output: "We can send a login code to r***2@gmail.com" (masked form mein).
  (e) Example: Agar aapka guess tha "rishikabra132@gmail.com" aur masked email "r***2@gmail.com" hai, to start "r" se aur end "2" se match karta hai – ye confirm ho sakta hai.
- **Note:** Ye method sirf tab kaam karta hai jab target ka Facebook account us username ya email se juda ho.

5. **Gmail Trick for Extra Confirmation:**

- Gmail pe jao, "Compose" kholo, aur "To" field mein email daalo (e.g., "rishikabra132@gmail.com
- Agar ye email Google account se linked hai, to kabhi-kabhi profile pic, username, ya name pop-up mein dikhta hai (e.g., "Rishi Kabra, profile pic").
- **Fayda:** Ye visual confirmation deta hai ki email target ka hai – bio ya pic se match karo.

6. **Save and Analyze:**

- Har valid email ko Notion mein table bana ke save karo:

Username	Email	Status	Source	Linked Account
saadsarraj	saadsarraj@gmail.	Valid	Experte.com	Facebook
rishikabra	rishikabra132@gm	Valid	Facebook Forgot	Gmail Pop-up

Workflow Example:

- **Target:** "Rishi Kabra"
- **Usernames:** rishikabra, rishi_kabra123
- **Generated Emails:**
  - rishikabra@gmail.com
  - rishikabra132@gmail.com

- rishi_kabra123@outlook.com

- **Experte.com:**
  - rishikabra132@gmail.com – Valid
  - Baaki invalid.

- **Facebook Forgot Password:**
  - "r***2@gmail.com" – rishikabra132@gmail.com match karta hai.

- **Gmail:** "rishikabra132@gmail.com" daalne pe "Rishi Kabra" ka profile pic mila.

- **Conclusion:** rishikabra132@gmail.com Rishi ka active email hai.

Extra Tips:

- **Variations:** Numbers (rishikabra123), dots (rishi.kabra), ya company domains (rishi@techmojo.com) bhi try karo.

- **Other Tools: Hunter.io** (hunter.io) ya **Voila Norbert** (voilanorbert.com) se bhi email verification kar sakte ho.

- **Cross-Check:** Email ko Have I Been Pwned (haveibeenpwned.com) pe check karo – breached data se link confirm ho sakta hai.

- **Safety:** Dummy account ya VPN use karo – repeated "Forgot Password" attempts se flag ho sakta hai.

Tables

Task	Method	Output
Generate Emails	Experte.com	Potential Emails
Verify	Facebook Forgot	Linked Email
Confirm	Gmail Trick	Profile Match

Table 25: Methods for Uncovering Emails from Usernames

Summary

- Usernames se emails generate karo – Experte.com se validate.
- Facebook Forgot Password se link check karo – Gmail trick se confirm.
- Notion mein save karo – target ke emails uncover karo.

Point To Note

Usernames (e.g., saadsarraj) se emails banayein (saadsarraj@gmail.com), **Experte.com** (experte.com) se generate aur verify karo, aur **Facebook Forgot Password** se link check karo (e.g., r***2@gmail.com). Gmail trick se profile pic ya username se confirm karo – har valid email ko Notion mein save karo. Ye method target ke emails ko uncover aur link karta hai – systematic kaam karo taaki OSINT pura ho!

==========

Creating and Verifying Possible Email Addresses

Creating and verifying possible email addresses ek advanced OSINT technique hai jisme hum **email permutators** ka use karke target ke naam se possible email combinations generate karte hain aur unhe verify karte hain. Ye method tab kaam aata hai jab aapke paas target ka naam (e.g., Saad Sarraj) hai aur aap uske email ID ke baare mein guess karna chahte ho. Tools jaise **Email Permutator+** firstname, lastname, aur common domains (gmail.com, hotmail.com) ke saath email list banate hain. Phir hum Facebook ke "Forgot Password" feature aur Gmail ke profile pic trick se in emails ko filter aur verify karte hain. Chalo is process ko step-by-step samajhte hain – ye systematic aur effective hai.

Why Use Email Permutators?

- Log apne naam ke variations ko email IDs mein use karte hain – jaise "Saad Sarraj" se "ssarraj@gmail.com" ya "saadsarraj@example.com".
- Manually har combination sochna time-consuming hai – permutators ise automate karte hain aur verification ke liye base dete hain.

Steps to Create and Verify Possible Email Addresses:

1. **Generate a List of Possible Email Combinations:**
   - **Tool: Email Permutator+** (online version: emailpermutatorplus.com ya Google Sheets template).
   - **Input:**
     - First Name: Saad
     - Last Name: Sarraj
     - Domains: gmail.com, hotmail.com, outlook.com, example.com
   - **Kaise Use Karein:**
     - Website pe jao, fields mein "Saad" (firstname), "Sarraj" (lastname), aur domains daalo.
     - "Generate" pe click karo – ye permutations bana dega.
   - **Sample Output:**

```
saadsarraj@gmail.com
ssarraj@gmail.com
saad.sarraj@gmail.com
sarrajsaad@gmail.com
saads@example.com
saadsarraj@hotmail.com
saadsarraj@outlook.com
```

   - **Note:** Ye tool initials (ss), dots (saad.sarraj), aur order swaps (sarrajsaad) jaise patterns cover karta hai.

2. **Copy and Paste Emails into Notepad:**
   - Generated list ko copy karo aur Notepad mein paste karo (e.g., "emails.txt"):

```
saadsarraj@gmail.com
ssarraj@gmail.com
saad.sarraj@gmail.com
```

```
sarrajsaad@gmail.com
saads@example.com
saadsarraj@hotmail.com
saadsarraj@outlook.com
```

- Is list ko refine karne ke liye agla step use karo.

3. **Filter Emails Using Facebook Forgot Password:**

- Agar aapko pehle se partial email pata hai (e.g., "r**2@gmail.com" – start with "r", end with "2"), to list ko narrow karo.
- **Process:**
  (a) `facebook.com` pe jao, "Forgot Password" pe click karo.
  (b) "Find Your Account" mein target ka naam ya username daalo (e.g., "Rishi Kabra").
  (c) "This is my account" select karo – ye linked email dikhayega (masked form mein).
  (d) Example Output: "We can send a code to r**2@gmail.com".
- **Filter:** Permutator list se sirf wo emails rakho jo "r" se start aur "2" pe end hote hain:
  – Agar list hai:

```
rishikabra@gmail.com
rkabra2@gmail.com
rishi.kabra@gmail.com
```

  – To "r**2@gmail.com" se match karta hai: **rkabra2@gmail.com**.

4. **Verify Emails Using Gmail Compose Trick:**

- Filtered emails ko Gmail pe check karo:
  (a) Gmail kholo, "Compose" pe click karo.
  (b) "To" field mein saare emails paste karo (e.g., rkabra2@gmail.com, rishikabra@gmail.com).
  (c) Agar email Google account se linked hai, to profile pic ya name pop-up mein dikhega:
    – **rkabra2@gmail.com** – "Rishi Kabra" + profile pic (valid).
    – **rishikabra@gmail.com** – Blue icon ya blank (high chance invalid).
- **Note:** Blue/default icon matlab email shayad registered nahi hai – real pic ya name wala valid hota hai.

5. **Save and Analyze:**

- Verified emails ko Notion mein table bana ke save karo:

Name	Username	Email	Status	Source
Saad Sarraj	saadsarraj	saadsarraj@gmail	Valid	Gmail Profile Pic
Rishi Kabra	rishikabra	rkabra2@gmail.co	Valid	Facebook + Gmail

Workflow Example:

- **Target:** "Rishi Kabra"
- **Permutator Output:**

```
rishikabra@gmail.com
rkabra2@gmail.com
rishi.kabra@gmail.com
kabrarishi@gmail.com
rishikabra@hotmail.com
```

- **Facebook Forgot Password:** "r**2@gmail.com" – rkabra2@gmail.com match karta hai.
- **Gmail Compose:**
  - rkabra2@gmail.com – "Rishi Kabra" + pic (valid).
  - rishikabra@gmail.com – Blue icon (invalid).
- **Conclusion:** rkabra2@gmail.com Rishi ka email hai.

Extra Tips:

- **More Domains:** Company domains (e.g., rishi@techmojo.com) ya regional (e.g., saad@proton.me) bhi add karo.
- **Other Tools: Hunter.io** (hunter.io) ya **Voila Norbert** (voilanorbert.com) se bhi verification try karo.
- **Cross-Check:** Valid email ko Have I Been Pwned (haveibeenpwned.com) pe check karo – breached data se link milega.
- **Safety:** Dummy Gmail account use karo – multiple checks se flag ho sakta hai.

Tables

Task	Method	Output
Generate Emails	Email Permutator+	Email List
Filter	Facebook Forgot	Matching Email
Verify	Gmail Trick	Confirmed Email

Table 26: Methods for Creating and Verifying Emails

Summary

- Email Permutator+ se combinations banayein – saadsarraj@gmail.com.
- Facebook Forgot Password se filter – Gmail trick se verify karo.
- Notion mein save karo – target ke emails confirm karo.

Point To Note

Email Permutator+ (emailpermutatorplus.com) se usernames (e.g., saadsarraj) ke combinations banayein (ssarraj@gmail.com, saadsarraj@hotmail.com), Notepad mein save karo, aur **Facebook Forgot Password** se filter karo (e.g., r**2@gmail.com → rkabra2@gmail.com). Gmail ke "To" field mein profile pic se verify karo – blue icon wale invalid hote hain. Har valid email ko Notion mein save karo – ye process target ke emails ko create aur confirm karta hai, bas systematic kaam karo taaki OSINT pura ho!

==========

Uncovering Emails with Browser Tools

Email lookup tools ke zariye target ke email addresses dhoondhna ek powerful OSINT technique hai, aur **browser extensions** is kaam ko aur bhi aasan bana dete hain. Kuch extensions, jaise **ContactOut**, **SignalHire**, aur **GetProspect**, LinkedIn accounts se judi email IDs nikal sakte hain – chahe wo personal ho ya business email. Ye tools free Chrome extensions ke roop mein available hain aur social media profiles ya public records se data collect karte hain. Inka use karke aap emails ke saath-saath phone numbers bhi uncover kar sakte ho. Har extension ka process thoda similar hai – LinkedIn pe target ka profile kholo, extension ko activate karo, aur details lo. Chalo har tool ko step-by-step explore karte hain aur samajhte hain kaise ye kaam karte hain.

Why Use Browser Extensions for Email Lookup?

- Ye extensions LinkedIn jaise platforms se direct info pull karte hain, jo manually dhoondhne se zyada tezi aur accuracy deta hai.
- **Sources:** Social media (LinkedIn, Twitter), public directories, aur cached records.
- Free versions mein basic functionality milti hai, jo OSINT ke liye kaafi hoti hai.

Browser Extensions Overview:

1. **GetProspect – Email Finder (Chrome Browser Extension)**
   - **Kya Hai:** Ye ek free Chrome extension hai jo LinkedIn profiles se emails (business ya personal) nikalti hai. GetProspect 50 free email lookups monthly deta hai.
   - **Kaise Use Karein:**
     (a) Chrome Web Store se "GetProspect Email Finder" install karo.
     (b) Account create karna pad sakta hai (free plan ke liye email signup).
     (c) LinkedIn pe jao, target ko search karo (e.g., "Rishi Kabra").
     (d) Uska profile kholo, browser toolbar mein GetProspect icon pe click karo.
     (e) Agar extension kaam na kare, page refresh karo – phir "Get Email" pe click karo.
   - **Output:**
     – Email: rishi.kabra@gmail.com (personal) ya rishi@techmojo.com (business).
     – Extra: Name, job title, company bhi mil sakta hai.
   - **Fayda:** Simple aur fast – bulk email extraction bhi possible hai paid plan mein.
   - **Note:** Free plan limited hai – 50 emails/month ke baad upgrade karna padta hai ($49/month se start).

2. **ContactOut – Email Lookup Tool (Chrome Browser Extension)**

- **Kya Hai:** Ye ek popular free extension hai jo LinkedIn se personal aur business emails ke saath phone numbers bhi deta hai. 75% LinkedIn profiles ke emails claim karta hai.
- **Kaise Use Karein:**
  (a) Chrome Web Store se "Email Finder by ContactOut" install karo.
  (b) LinkedIn pe target ka profile kholo (e.g., "Satyam Singh").
  (c) Toolbar mein ContactOut icon pe click karo – refresh karne ki zarurat pad sakti hai.
  (d) Details reveal honge – email aur phone number.
- **Output:**
  – Personal: satyam.singh@gmail.com
  – Business: satyam.singh@infosys.com
  – Phone: +1-919-555-1234 (agar available ho).
- **Fayda:** Triple-verified data aur CRM integration (Salesforce, HubSpot) free plan mein 40 credits/month deta hai.
- **Note:** Phone numbers har profile ke liye nahi milte – accuracy 99% claim karta hai.

3. **SignalHire – Find Email or Phone Number (Chrome Browser Extension)**

- **Kya Hai:** Ye ek free extension hai jo LinkedIn, Twitter, GitHub jaise platforms se emails aur phone numbers dhoondhta hai. 96% hit rate ka daawa hai.
- **Kaise Use Karein:**
  (a) Chrome Web Store se "SignalHire" install karo.
  (b) SignalHire pe account banao (free plan mein 5 credits/month).
  (c) LinkedIn pe target profile jao (e.g., "Saad Sarraj").
  (d) Toolbar mein SignalHire icon pe click karo – "Get Contacts" dabao.
- **Output:**
  – Email: saadsarraj@gmail.com
  – Phone: +91-98765-43210 (verified, agar available).
- **Fayda:** Multiple platforms cover karta hai aur ATS/CRM export option deta hai.
- **Note:** Kabhi-kabhi fail ho sakta hai – data real-time verify hota hai, lekin har profile pe kaam nahi karta.

Workflow Example:

- **Target:** "Rishi Kabra"
- **GetProspect:**
  – Profile: `linkedin.com/in/rishi-kabra`
  – Result: rishi.kabra@gmail.com (personal).
- **ContactOut:**
  – Result: rishi@techmojo.com (business) + phone "+1-919-555-1234".

- **SignalHire:**
  - Result: rishi.kabra@gmail.com (same email, phone nahi mila).
- **Conclusion:** Rishi ke do emails mile – personal aur business – ContactOut ne zyada details diye.

Extra Tips:

- **Refresh Issue:** Agar extension kaam na kare, LinkedIn page refresh karo ya cache clear karo.
- **Cross-Check:** Ek extension se mila email doosre pe verify karo – consistency check ke liye.
- **Free Limits:**
  - GetProspect: 50 emails/month.
  - ContactOut: 40 credits/month.
  - SignalHire: 5 credits/month (1 credit = 1 contact).
- **Expand:** Email mila to usse Have I Been Pwned (haveibeenpwned.com) pe breach check karo ya Sherlock (github.com/sherlock-project/sherlock) se linked accounts dhoondho.
- **Save:** Notion mein table banao:

Name	Email	Phone	Source
Rishi Kabra	rishi.kabra@gmail	N/A	GetProspect
Rishi Kabra	rishi@techmojo.co	+1-919-555-1234	ContactOut

Tables

Task	Extension	Output
Email Lookup	GetProspect	Personal Email
Detailed Info	ContactOut	Email + Phone
Multi-Platform	SignalHire	Verified Contacts

Table 27: Methods for Uncovering Emails with Browser Tools

Summary

- GetProspect se 50 emails/month free mein lo – simple aur fast.
- ContactOut se email + phone – SignalHire multi-platform cover karta hai.
- Notion mein save karo – LinkedIn se direct OSINT boost karo.

Point To Note

ContactOut, SignalHire, aur GetProspect jaise free browser extensions se LinkedIn profiles ke emails (personal/business) aur phone numbers dhoondho. Ye tools social media aur public records se data laate hain – LinkedIn pe target ka profile kholo, extension activate karo (refresh agar zaruri ho), aur details lo. SignalHire kabhi fail ho sakta hai, lekin ContactOut aur GetProspect reliable hain. Har finding ko Notion mein save karo – ye email OSINT ko tezi se boost karta hai!

==========

Finding Business Email Addresses

Finding business email addresses ek critical OSINT skill hai jo target ke professional contact details tak pahunchne mein madad karti hai. Bahut si companies apne employees ke email addresses ke liye ek consistent **email pattern** follow karti hain, jaise **firstname.lastname@companydomain.com**. Is pattern ko manually ya automatically identify karna zaroori hai – manually aap company ke public data se guess kar sakte ho, aur automatically tools jaise **Hunter.io** ka use karke pattern pata kar sakte ho. Is topic mein hum explore karenge kaise patterns jaise **rishi.kabra@contactout.com** ya **satyam.kumar.singh@kibalabas.in** ko samjha jaye, aur **Hunter.io** aur **Phonebook.cz** jaise tools se email addresses collect kiye jayein. Chalo step-by-step dekhte hain kaise company ka email pattern identify karna hai aur employees ke emails dhoondhe jate hain.

Why Identify Email Patterns?

- Companies aksar ek fixed email format use karti hain – jaise **firstname@companydomain.com**, **firstname.lastname@companydomain.com**, ya **initial.lastname@companydomain.com**.
- Ye pattern jaan'ne se aap manually ya tools ke saath target employee ka email guess kar sakte ho (e.g., "Rishi Kabra" at ContactOut → rishi.kabra@contactout.com).
- **Goal:** Company ka email structure samajhna aur uske employees ke business emails uncover karna.

Manually Identifying Email Patterns:

- **Steps:**
  1. Company ke public sources check karo – website, LinkedIn, press releases, ya employee bios.
  2. Known emails dhoondho – jaise "About Us" page pe "john.doe@companydomain.com" mila to pattern hai **firstname.lastname@companydomain.com**.
  3. Consistency dekho – agar ek employee ka email "jane.smith@companydomain.com" hai, to shayad ye pattern sabpe apply hota hai.
- **Example:**
  - "Rishi Kabra" ContactOut mein kaam karta hai. Agar ek sample email hai "john.doe@contactou to Rishi ka email shayad **rishi.kabra@contactout.com** hoga.

Automatically Identifying Email Patterns with Hunter.io:

- **Website:** hunter.io

- **Kya Hai:** Hunter.io ek email finder tool hai jo company domains se email patterns aur addresses nikal sakta hai. Free account ke saath aap basic searches kar sakte ho.

- **Kaise Use Karein:**

  1. **Hunter.io Pe Jao:** Browser mein hunter.io kholo aur free account banao (email signup ke saath).
  2. **Domain Search Select Karo:** Dashboard pe "Domain Search" pe click karo.
  3. **Company Name Daalo:** Input box mein company domain daalo – e.g., **contactout.com**.
  4. **Search Karo:** "Find email addresses" pe click karo – Hunter.io results dikhayega.

- **Output Example:**

  - Domain: contactout.com
  - **Email Pattern: {first}@contactout.com**
  - Meaning: Employees ka email firstname pe based hai – jaise "Rishi Kabra" ka email hoga **rishi@contactout.com**.
  - Extra: Sample emails bhi mil sakte hain – e.g., john@contactout.com, mary@contactout.com.

- **Fayda:** Pattern ke saath confidence score milta hai (e.g., 95% accurate), aur manually guess karne ka time bachta hai.

- **Note:** Free plan mein 25 searches/month milte hain – zyada ke liye paid plan ($49/month se start).

Gathering Many Email Addresses with Phonebook.cz:

- **Website:** phonebook.cz

- **Kya Hai:** Ye ek free tool hai jo company domains se bulk email addresses aur contact info dhoondhta hai – "Yellow Pages of the internet" kehlata hai.

- **Kaise Use Karein:**

  1. **Phonebook.cz Pe Jao:** Browser mein phonebook.cz kholo – koi account ki zarurat nahi.
  2. **Email Addresses Select Karo:** Search type mein "Email Addresses" choose karo.
  3. **Domain Daalo:** Input box mein company domain daalo – e.g., **contactout.com**.
  4. **Search Karo:** "Search" pe click karo – ye public web se emails scrape karega.

- **Output Example:**

  - Domain: contactout.com
  - Results:
    - rishi@contactout.com
    - mary@contactout.com
    - john.smith@contactout.com

- **Fayda:** Ek baar mein multiple emails milte hain – pattern ko cross-check karne ke liye perfect.

- **Note:** Results public sources pe depend karte hain – outdated ya incomplete ho sakte hain.

Workflow Example:

- **Target:** "Satyam Kumar Singh" at "Kibalabas.in"
- **Hunter.io:**
  - Domain Search: kibalabas.in
  - Pattern: **firstname.middle.lastname@companydomain.com**
  - Email: **satyam.kumar.singh@kibalabas.in**
- **Phonebook.cz:**
  - Search: kibalabas.in
  - Results:
    - satyam.kumar.singh@kibalabas.in
    - rahul.kumar.sharma@kibalabas.in
  - Pattern confirmed: firstname.middle.lastname@kibalabas.in.
- **Conclusion:** Satyam ka email satyam.kumar.singh@kibalabas.in hai – pattern match karta hai.

Extra Tips:

- **Manual Guess:** Agar pattern hai **{first}.{last}@companydomain.com**, to "Rishi Kabra" ke liye rishi.kabra@contactout.com try karo.
- **Verify:** Hunter.io ke "Email Verifier" se check karo ki email valid hai ya nahi (free mein 50 verifications/month).
- **Cross-Check:** Phonebook.cz se mile emails ko Hunter.io ke pattern se match karo.
- **Save:** Notion mein table banao:

Name	Company	Email	Pattern	Source
Rishi Kabra	ContactOut	rishi@contactout.com	{first}@contactou	Hunter.io
Satyam Kumar Singh	Kibalabas	satyam.kumar.singh	{first}.{middle}.{	Phonebook.cz

Tables

Task	Method	Output
Pattern Identify	Hunter.io	Email Format
Bulk Emails	Phonebook.cz	Multiple Emails
Verify	Hunter.io Verifier	Validated Email

Table 28: Methods for Finding Business Email Addresses

Summary

- Hunter.io se pattern lo – firstname@contactout.com.
- Phonebook.cz se bulk emails gather karo – consistency check karo.
- Notion mein save karo – professional emails uncover karo.

Point To Note

Business email addresses dhoondhne ke liye company ka **email pattern** identify karo – manually samples se ya **Hunter.io** (hunter.io) se automatically (e.g., {first}@contactout.com). Hunter.io pe "Domain Search" se pattern lo, aur **Phonebook.cz** (phonebook.cz) se bulk emails gather karo (e.g., rishi@contactout.com). Har finding ko Notion mein save karo – ye process target ke professional emails ko tezi se uncover karta hai, bas pattern ko samajhkar systematically kaam karo!

==========

Discovering Emails Within Data Breaches/Leaks

Discovering emails within data breaches/leaks ek powerful OSINT technique hai jo target ke email addresses ko **leaked ya breached databases** se uncover karne mein madad karti hai. Jab companies ya platforms (jaise Facebook, LinkedIn, Twitter) ke databases hack hote hain, to unmein shamil info – jaise **name, phone number, email** – public ya dark web pe leak ho jati hai. Is topic mein hum dekhte hain kaise **DeHashed** jaise tools se name ya phone number ke zariye emails dhoondhe jayein, aur specific breaches (Facebook, LinkedIn, Twitter) ko target karke results refine kiye jayein. Ye method sensitive data tak access deta hai, lekin ethical aur legal boundaries mein rehna zaroori hai. Chalo step-by-step samajhte hain.

Why Search Leaked Databases?

- Breached databases mein emails, passwords, phone numbers, aur personal info hoti hai jo target ke online identity ko reveal kar sakti hai.
- Agar target ka account kisi popular platform (Facebook, LinkedIn, Twitter) pe hai, to uske specific breach se email milne ke chances badh jate hain.

Steps to Discover Emails in Leaked Databases:

1. **Search in DeHashed:**
   - **Website:** dehashed.com
   - **Kya Hai:** DeHashed ek breach search engine hai jo 14 billion+ compromised records ko index karta hai – emails, names, phone numbers, passwords sab cover karta hai.
   - **Kaise Use Karein:**
     (a) DeHashed pe jao, free account banao (basic search ke liye signup free hai).
     (b) Search bar mein target ka **name** (e.g., "Rishi Kabra") ya **phone number** (e.g., "+919876543210") daalo.
     (c) "Search" pe click karo – results mein breaches list honge.
   - **Output Example:**
     – Name: "Rishi Kabra"

- Email: rishi.kabra@gmail.com
- Breach: LinkedIn 2012
- Password Hash: 5f4dcc3b5aa765d61d8327deb882cf99 (MD5, crackable).

- **Fayda:** Free mein basic results, paid plan ($5/month) se full details (unmasked emails/passwords).
- **Note:** Phone number international format mein daalo (+91 for India).

2. **Check Facebook Data Leak:**

- **Context:** 2021 mein Facebook ka 533 million users ka data leak hua – names, emails, phone numbers, locations exposed.
- **Kaise Check Karein:**
  - DeHashed pe "Facebook" filter laga ke name search karo (e.g., "Satyam Singh").
  - Alternative: **Have I Been Pwned** (haveibeenpwned.com) pe email ya phone daalo – agar Facebook breach mein hai, to confirm hoga.
- **Output:** satyam.singh@gmail.com (agar Facebook account se match karta hai).
- **Note:** Target ka Facebook account hona zaroori hai – profile se name verify karo.

3. **Check LinkedIn Data Breach:**

- **Context:** 2012 (167M accounts) aur 2021 (700M accounts) mein LinkedIn breaches hue – emails, names, job details leak hue.
- **Kaise Check Karein:**
  - DeHashed pe "LinkedIn" filter ke saath "Rishi Kabra" search karo.
  - Result: rishi@techmojo.com (business email).
- **Note:** LinkedIn profile pe target ka name ya job title match karo.

4. **Check Twitter Data Leak:**

- **Context:** 2022 mein Twitter ka 200M+ users ka data leak hua – emails, usernames, phone numbers exposed.
- **Kaise Check Karein:**
  - DeHashed pe "Twitter" filter laga ke username (e.g., @saadsarraj) ya name search karo.
  - Result: saadsarraj@gmail.com.
- **Note:** Twitter handle se cross-check karo – @saadsarraj ka bio ya tweets se confirm.

5. **Save and Expand:**

- Har email ko Notion mein table bana ke save karo:

Name	Email	Breach	Phone	Source
Rishi Kabra	rishi.kabra@gmail	LinkedIn 2012	N/A	DeHashed
Satyam Singh	satyam.singh@gm	Facebook 2021	+919876543210	DeHashed

Recap: Email OSINT Process Pura process recap karte hain – target ke emails dhoondhne ke saare tareeke:

1. **Check If the Email Is Shared Online:**
   - Social media (Twitter bio, LinkedIn Contact Info) ya YouTube "About" pe email check karo.
2. **Use Google Operators:**
   - **"Rishi Kabra" "email" site:linkedin.com** – Google se email mentions dhoondho.
3. **Form Emails with Usernames:**
   - Username (saadsarraj) se emails banao – saadsarraj@gmail.com, saadsarraj@hotmail.com.
4. **Utilize Password Resets to Guess/Verify an Email:**
   - Facebook "Forgot Password" se masked email lo (e.g., r**2@gmail.com) aur guess verify karo (rishikabra2@gmail.com).
5. **Use Email Permutators:**
   - **Email Permutator+** (emailpermutatorplus.com) se combinations banao – ssarraj@gmail.com, saad.sarraj@outlook.com.
6. **Use Browser Extensions:**
   - **ContactOut, SignalHire, GetProspect** se LinkedIn profiles se emails lo (e.g., rishi@techmojo.com).
7. **Search in Leaked Databases:**
   - **DeHashed** (dehashed.com) pe name/phone se breaches check karo – LinkedIn, Facebook, Twitter leaks se emails lo.
8. **Identify an Email Pattern:**
   - **Hunter.io** (hunter.io) se company pattern pata karo (e.g., {first}@contactout.com) – rishi@contactout.com.

Workflow Example:

- **Target:** "Saad Sarraj"
- **DeHashed:** saadsarraj@gmail.com (Twitter 2022 breach).
- **Facebook Leak:** saad.sarraj@yahoo.com (2021 breach).
- **LinkedIn Breach:** saad@techfirm.com (2021 breach).
- **Conclusion:** Saad ke teen emails mile – personal aur business.

Extra Tips:

- **Cross-Check:** Breach se mila email social media pe verify karo (bio, posts).
- **Safety:** VPN use karo – breach data access risky ho sakta hai.
- **Expand:** Email se Have I Been Pwned (haveibeenpwned.com) pe breaches aur Sherlock (github.com/sherlock-project/sherlock) pe accounts dhoondho.
- **Save:** Notion mein organize karo taaki har source clear rahe.

Tables

Task	Method	Output
Search Breaches	DeHashed	Leaked Emails
Specific Leak	Facebook/LinkedIn/Tw	Targeted Email
Verify	HIBP	Breach Confirmation

Table 29: Methods for Discovering Emails in Breaches

Summary

- DeHashed se breaches search karo – name/phone daalo.
- Facebook, LinkedIn, Twitter leaks target karo – specific emails lo.
- Notion mein save karo – target ka leaked data uncover karo.

Point To Note

Leaked databases se emails dhoondhne ke liye **DeHashed** (dehashed.com) pe name/-phone search karo, aur **Facebook, LinkedIn, Twitter breaches** target karo. Recap mein – online checks, Google operators, username permutations, password resets, permutators, extensions, breaches, aur patterns se emails lo. Har email ko Notion mein save karo – ye process target ke compromised data ko khol deta hai, bas ethical limits mein raho aur systematically kaam karo!

==========

Tracking the Identity Behind an Email Address

Tracking the identity behind an email address ek essential email OSINT skill hai jisme aap kisi bhi email address se judi information uncover kar sakte ho – jaise target ka naam, social profiles, ya doosre linked accounts. Is process mein hum **search operators** ka use karenge taaki pata chal sake ki email address search engines (Google, Bing, etc.) mein indexed hai ya nahi. Ek email jaise "zaidh@zsecurity.org" ko seed bana ke hum uske username (zaidh) se multiple platforms ya alternative emails tak bhi pahunch sakte hain. Kabhi-kabhi domain (@zsecurity.org) hata kar sirf username pe search karna zyada results deta hai. Chalo is technique ko step-by-step samajhte hain aur kaise ye target ki identity ko reveal karta hai.

Why Track an Email Address?

- Ek email address ek digital fingerprint ki tarah hota hai – ye social media, forums, breaches, ya public records se juda ho sakta hai.
- Search operators ke saath aap indexed info (posts, profiles, leaks) dhoondh sakte ho jo email ya uske username se connected ho.

Steps to Track Identity Behind an Email Address:

1. **Analyze the Email Address:**
   - Email: "zaidh@zsecurity.org"

- **Parts:**
  - Username: zaidh
  - Domain: @zsecurity.org (company ya personal site ka hint – zsecurity.org cybersecurity training platform hai).
- **Initial Guess:** "zaidh" naam ka variation ho sakta hai (Zaid Hussain?) aur domain se professional link hai.

2. **Use Search Operators to Check Indexing:**
   - **Full Email Search:**
     - Google pe: **"zaidh@zsecurity.org"** (quotes mein exact match ke liye).
     - Result:
       - zsecurity.org pe "Contact: zaidh@zsecurity.org" – Zaid ka official email.
       - Forum post: "Email me at zaidh@zsecurity.org for course details".
   - **Username-Only Search:**
     - Domain hatao aur sirf "zaidh" pe focus karo: **"zaidh" -inurl:(zsecurity.org)**
     - Ye zsecurity.org ke alawa results deta hai taaki doosre platforms pe zaidh ke traces milein.
     - Result:
       - Twitter: "zaidh tweets about hacking" – shayad @zaidh ya similar handle.
       - Gmail hint: "zaidh@gmail.com" kisi forum mein mentioned.
   - **Fayda:** Username search se multiple emails ya accounts mil sakte hain (zaidh@gmail.com, zaidh@yahoo.com).

3. **Refine with Additional Operators:**
   - **Site-Specific:**
     - **"zaidh" site:twitter.com** – Twitter pe zaidh ka presence.
     - **"zaidh" site:linkedin.com** – LinkedIn profile (e.g., "Zaid H, Cybersecurity Expert").
   - **Exclude Noise:**
     - **"zaidh" -inurl:(facebook instagram)** – FB/IG ke alawa focus.
   - **Keyword Combo:**
     - **"zaidh" "cybersecurity"** – Zaid ka profession confirm karne ke liye.

4. **Cross-Check with Tools:**
   - **Have I Been Pwned** (haveibeenpwned.com): "zaidh@zsecurity.org" daalo – agar breached hai, to kahan se leak hua pata chalega (e.g., LinkedIn 2012).
   - **Sherlock** (github.com/sherlock-project/sherlock): Terminal mein `sherlock zaidh` – 400+ platforms pe username check karega (e.g., zaidh@GitHub).
   - **Hunter.io** (hunter.io): Domain (zsecurity.org) se email pattern lo – zaidh@zsecurity.org fit karta hai ya nahi.

5. **Analyze and Expand:**
   - Agar zaidh@gmail.com mila, to Gmail "Compose" trick use karo – "To: zaidh@gmail.com" daalne pe profile pic/name dikhega (e.g., "Zaid Hussain").

- Social profiles se full name, location, ya job milega – jaise "Zaid H, Founder of zSecurity, UAE".

6. **Save Findings:**
   - Har detail ko Notion mein table bana ke save karo:

Email	Username	Source	Details
zaidh@zsecurity.or	zaidh	Google Search	zSecurity Founder
zaidh@gmail.com	zaidh	Forum Mention	Personal email

Workflow Example:

- **Email:** "satyam@techbit.in"
- **Full Search: "satyam@techbit.in"**
  - Result: "Contact: satyam@techbit.in" techbit.in pe – Satyam ka business email.
- **Username Search: "satyam" -inurl:(techbit.in)**
  - Result:
    - satyam.singh@gmail.com (forum post).
    - @satyam_singh Twitter pe.
- **Sherlock:** `sherlock satyam` – satyam@reddit.com mila.
- **Conclusion:** Satyam ke teen emails – satyam@techbit.in (business), satyam.singh@gmail.com (personal), satyam@reddit.com (alt).

Extra Tips:

- **Variations:** "zaidh" ke saath zaidh123, z.hussain bhi try karo – usernames evolve hote hain.
- **Breach Check:** DeHashed (dehashed.com) pe email search karo – zaidh@zsecurity.org breached hai to password hash bhi milega.
- **Cross-Check:** Social profiles ke bio/pics se identity confirm karo.
- **Save Context:** Notion mein source aur relevance note karo taaki confusion na ho.

Tables

Summary

- Search operators se email aur username track karo.
- Tools (HIBP, Sherlock) se cross-check – Gmail trick se refine.
- Notion mein save karo – target ki identity reveal karo.

Task	Method	Output
Full Email Search	Google "zaidh@zsecurity.org"	Indexed Mentions
Username Search	"zaidh" -inurl:(zsecurity)	Alt Emails/Accounts
Verify	Sherlock/HIBP	Confirmed Identity

Table 30: Methods for Tracking Email Identity

Point To Note

Email address (e.g., "zaidh@zsecurity.org") se identity track karne ke liye **search operators** use karo – **"zaidh@zsecurity.org"** se full email search aur **"zaidh"** se multiple platforms pe traces lo. Username-only search se doosre emails (zaidh@gmail.com) mil sakte hain. Tools (HIBP, Sherlock) aur Gmail trick se refine karo – har finding ko Notion mein save karo taaki target ka pura profile ban jaye. Systematic kaam karo aur domain hata ke search se maximum results lo!

==========

Leveraging Password Resets to Validate Email Addresses

Leveraging password resets to validate email addresses ek clever OSINT technique hai jo target ke email addresses ko guess ya verify karne mein madad karti hai. Jab aap social media platforms (Facebook, Instagram, Twitter, etc.) pe **password reset** feature ka use karte ho, to ye aapko email ka partial view (masked form) deta hai – jaise **e**@g**.com** – jisse aap pura email reconstruct kar sakte ho. Ye method tab kaam aata hai jab aapke paas email ka kuch idea hai (username ya domain) aur aap usse confirm karna chahte ho. Is process mein hum har major platform pe password reset try karenge aur results se email validate karenge. Chalo step-by-step samajhte hain kaise ye kaam karta hai.

Why Use Password Resets?

- Password reset feature aksar email ya phone number reveal karta hai jo account se linked hai – masked form mein (e.g., r**i@te**.com).
- Ye partial info aapke guesses (e.g., rishi@techmojo.com) ko verify karne ya refine karne ke liye kaafi hoti hai.
- Har platform ka reset process thoda alag hota hai, lekin logic same hai – email ka hint milna.

Steps to Leverage Password Resets:

1. **Identify Target's Social Media Accounts:**
   - Target ke known profiles dhoondho – Facebook, Instagram, Twitter, LinkedIn, etc.
   - Example: "Rishi Kabra" ka Facebook (facebook.com/rishikabra), Twitter (@rishi_kabra), Instagram (@rishikabra).
2. **Use Password Reset on Each Platform:**
   - **Facebook:**

(a) `facebook.com` pe jao, "Forgot Password" pe click karo.

(b) "Find Your Account" mein username ya naam daalo (e.g., "Rishi Kabra").

(c) "Search" pe click karo – agar account milta hai, to "This is my account" select karo.

(d) Output: "We can send a code to r**i@te**.com".

(e) Hint: Start with "r", end with "i", domain mein "te" hai – shayad rishi@techmojo.com.

- **Instagram:**

(a) `instagram.com` pe "Forgot Password" pe jao.

(b) Username (@rishikabra) daalo.

(c) Output: "r***i@gm**.com".

(d) Hint: "r" se start, "i" pe end, domain "gm" – rishi@gmail.com possible hai.

- **Twitter:**

(a) `twitter.com` pe "Forgot Password" pe jao.

(b) @rishi_kabra daalo.

(c) Output: "r**2@g**.com".

(d) Hint: "r" se start, "2" pe end – rishi2@gmail.com ya rishikabra2@gmail.com ho sakta hai.

- **LinkedIn:**

(a) `linkedin.com` pe "Forgot Password" pe jao.

(b) Email field mein guess daal sakte ho ya naam se search karo.

(c) Output: "r***i@te**.com" (agar email registered hai).

3. **Analyze Masked Patterns:**

- Har platform se masked email lo:
  - Facebook: r**i@te**.com
  - Instagram: r***i@gm**.com
  - Twitter: r**2@g**.com
- Commonalities dekho:
  - " iemandr" se start – Rishi ka hint.
  - Domains: @techmojo.com (te), @gmail.com (gm).
  - Variations: "i" ya "2" pe end – rishi ya rishi2.

4. **Guess and Reconstruct Emails:**

- Known username (rishikabra) aur hints se emails banao:
  - rishi@techmojo.com (Facebook/LinkedIn se match).
  - rishi@gmail.com (Instagram se match).
  - rishikabra2@gmail.com (Twitter se "2" ke saath).
- Permutations try karo: rishi.kabra@techmojo.com, rishi2@gmail.com.

5. **Verify with Gmail Trick:**

- Gmail pe "Compose" kholo, "To" mein guesses daalo:
  - rishi@techmojo.com – "Rishi Kabra, TechMojo" + pic (valid).

– rishi@gmail.com – Blue icon (invalid ya unlinked).
– rishikabra2@gmail.com – "Rishi K" + pic (valid).

6. **Save Findings:**

- Har email ko Notion mein table bana ke save karo:

Name	Email	Platform	Masked Hint	Status
Rishi Kabra	rishi@techmojo.cc	Facebook	r**i@te**.com	Valid
Rishi Kabra	rishikabra2@gmai	Twitter	r**2@g**.com	Valid

Workflow Example:

- **Target:** "Satyam Singh"
- **Facebook:** s***m@inf**.com – satyam@infosys.com possible.
- **Instagram:** s***m@gm**.com – satyam@gmail.com.
- **Twitter:** s**1@g**.com – satyam1@gmail.com.
- **Verification:**
  – satyam@infosys.com – Gmail pe "Satyam Singh, Infosys" (valid).
  – satyam@gmail.com – No pic (invalid).
- **Conclusion:** satyam@infosys.com Satyam ka business email hai.

Extra Tips:

- **Multiple Platforms:** Har platform pe alag email ho sakta hai – sab try karo.
- **Cross-Check:** Masked hint ko username (rishikabra) ya company (TechMojo) se match karo.
- **Safety:** Dummy account use karo – bar-bar reset attempts se flag ho sakta hai.
- **Expand:** Valid email se Have I Been Pwned (haveibeenpwned.com) pe breach check karo ya Sherlock (github.com/sherlock-project/sherlock) se accounts dhoondho.

Tables

Task	Method	Output
Get Hint	Password Reset	Masked Email
Reconstruct	Guess from Hint	Full Email
Verify	Gmail Trick	Validated Email

Table 31: Methods for Validating Emails with Password Resets

Summary

- Password reset se masked hints lo – r**i@te**.com.
- Guesses banao aur Gmail se verify – valid emails confirm karo.
- Notion mein save karo – target ka email profile banao.

Point To Note

Password reset se email addresses validate karo – **Facebook, Instagram, Twitter** pe "Forgot Password" use karke masked hints lo (e.g., e**@g**.com → example@gmail.com). Hints se guesses banao (rishi@techmojo.com), Gmail trick se verify karo, aur Notion mein save karo. Ye method email OSINT ko tezi se boost karta hai – systematic kaam karo taaki target ka contact profile pura khul jaye!

==========

Investigating an Email Address for Red Flags

Investigating an email address for red flags ek zaroori OSINT skill hai jo aapko target ke email ke credibility aur safety ko assess karne mein madad karta hai. Iske liye **emailrep.io** ek powerful service hai jo email addresses ke **reputation scores** aur detailed information provide karta hai. Ye tool email ke reputation ko judge karne ke liye multiple factors ka use karta hai – jaise **social media presence**, **public records**, **email deliverability**, aur **data breaches/credential leaks**. Emailrep.io pe aapko ek email ke baare mein aur bhi details milenge, jaise **first seen**, **last seen**, aur **linked accounts/profiles** (e.g., ['gravatar', 'twitter']). Chalo is process ko step-by-step samajhte hain taaki aap red flags – jaise fraud, phishing, ya compromised status – ko identify kar sako.

Why Investigate an Email for Red Flags?

- Emails aksar scams, phishing, ya compromised accounts se jude hote hain – inka reputation check karna zaroori hai.
- Emailrep.io jaise tools aapko ek email ki trustworthiness aur risk level ke baare mein insight dete hain, jo identity verification ya security analysis ke liye critical hai.

Website: Emailrep.io

- **Kya Hai:** Emailrep.io ek free service hai jo email addresses ka reputation score calculate karta hai aur uske online footprint ka analysis deta hai. Ye crawlers, scanners, aur enrichment services ka use karta hai.
- **Reputation Factors:**
  - **Presence on Social Media Sites:** Email kisi social platform (Twitter, LinkedIn) se juda hai ya nahi – zyada profiles ka matlab higher legitimacy ho sakta hai.
  - **Public Records:** Publicly available data mein email ka mention – jaise directories ya forums.
  - **Email Deliverability:** Email valid hai ya deliverable hai – invalid emails suspicious ho sakte hain.
  - **Data Breaches and Credential Leaks:** Email kisi breach (e.g., LinkedIn 2012) ya dark web leak mein shamil hai ya nahi – compromised emails riskier hote hain.

Steps to Investigate an Email with Emailrep.io:

1. **Visit Emailrep.io:**
   - Browser mein emailrep.io kholo – koi account ki zarurat nahi hai basic use ke liye.
2. **Enter the Email Address:**
   - Search bar mein target email daalo – e.g., "rishi.kabra@gmail.com".
   - "Submit" pe click karo – results instantly load hote hain.
3. **Analyze the Results:**
   - **Reputation Score:** "High", "Medium", "Low", ya "None" – high score matlab zyada trusted, low/none suspicious hai.
   - **Suspicious Flag:** True ya False – agar "True" hai, to red flag (e.g., phishing ya spam).
   - **Details Section:**
     - **First Seen:** Email pehli baar kab dekha gaya (e.g., "07/01/2015") – naye emails riskier ho sakte hain.
     - **Last Seen:** Aakhri baar kab active tha (e.g., "03/15/2025").
     - **Data Breach:** "True" agar breach mein shamil hai – compromised hone ka risk.
     - **Credentials Leaked:** "True" agar password leak hua – security threat.
     - **Deliverable:** "True" agar email valid hai – "False" suspicious hai.
     - **Profiles:** Linked accounts – e.g., ['gravatar', 'twitter'] – legit profiles trust badhate hain.
   - **Example Output:**

```
Email: rishi.kabra@gmail.com
Reputation: High
Suspicious: False
References: 15
Details:
  - Blacklisted: False
  - Data Breach: True (LinkedIn 2012)
  - First Seen: 07/01/2015
  - Last Seen: 03/15/2025
  - Deliverable: True
  - Profiles: ['gravatar', 'twitter', 'linkedin']
```

4. **Identify Red Flags:**
   - **Low/No Reputation:** Email ka koi history nahi – new ya fake ho sakta hai.
   - **Suspicious: True:** Phishing ya malicious activity ka hint.
   - **Data Breach/Credential Leak:** Email compromised hai – account takeover ka risk.
   - **No Profiles:** Koi social media link nahi – legitimacy pe doubt.
   - **Non-Deliverable:** Email invalid hai – scam ka chance zyada.

Email	Reputation	Suspicious	Breach	Profiles	Red Flags
rishi.kabra@gmail	High	False	True	gravatar, twitter	Breach (LinkedIn)

5. **Save and Expand:**
   - Results ko Notion mein table bana ke save karo:
   - Breach mila to **Have I Been Pwned** (haveibeenpwned.com) pe cross-check karo – aur profiles (Twitter) se identity verify karo.

Workflow Example:

- **Email:** "saad@fakecompany.com"
- **Emailrep.io Result:**
  - Reputation: None
  - Suspicious: True
  - Data Breach: False
  - First Seen: Never
  - Last Seen: Never
  - Deliverable: False
  - Profiles: []
- **Red Flags:**
  - No reputation/history – new ya fake email.
  - Suspicious flag – potential scam/phishing.
  - Non-deliverable – invalid address.
  - Koi profiles nahi – legitimacy ka proof nahi.
- **Conclusion:** Ye email risky hai – avoid interaction.

Extra Tips:

- **Cross-Check:** Social profiles (e.g., Twitter) pe username (rishi.kabra) search karo – email match karta hai ya nahi.
- **Breach Context:** Data breach mila to DeHashed (dehashed.com) pe full details lo – kab, kahan se leak hua.
- **Gmail Trick:** "To: rishi.kabra@gmail.com" Gmail pe daalo – profile pic/name se confirm karo.
- **Safety:** Dummy account ya VPN use karo – sensitive searches ke liye precaution.

Task	Method	Output
Check Reputation	Emailrep.io	Score + Details
Identify Red Flags	Analyze Factors	Risk Assessment
Verify	HIBP/DeHashed	Breach Confirmation

Table 32: Methods for Investigating Email Red Flags

Tables

Summary

- Emailrep.io se reputation aur red flags check karo.
- Social presence, breaches, deliverability analyze karo – risks lo.
- Notion mein save karo – risky emails identify karo.

Point To Note

Emailrep.io (emailrep.io) se email addresses investigate karo – **reputation score**, **social media presence**, **deliverability**, aur **breaches** check karne se red flags pata chalte hain. Results mein **first seen**, **last seen**, aur **profiles** (e.g., ['gravatar', 'twitter']) se identity aur trust judge karo. Har detail ko Notion mein save karo – ye method aapko risky emails (low reputation, suspicious, breached) se alert karta hai taaki aap safe rah sako! Systematic kaam karo aur har factor pe dhyan do.

==========

Uncovering Websites and Accounts Linked to an Email Address

Uncovering websites and accounts linked to an email address ek powerful OSINT technique hai jo aapko ye pata lagane mein madad karti hai ki koi email address kahan-kahan registered hai – chahe wo social media ho, forums, ya doosre online platforms. Agar aapke paas target ka email hai (e.g., rishi.kabra@gmail.com), to aap OSINT tools ka use karke un websites aur accounts ko dhoondh sakte ho jo aapko pehle pata nahi the. Is process mein hum kuch tools jaise **Epieos**, **Castrick**, **PreductaSearch.com**, aur **Gravatar.com** explore karenge. Ye tools email ke digital footprint ko track karte hain aur aapko linked platforms ke bare mein batate hain. Chalo har tool ko detail mein samajhte hain aur dekhte hain kaise ye kaam karte hain.

Why Uncover Linked Websites and Accounts?

- Ek email address ek central key hota hai jo multiple online identities ko connect karta hai – social profiles, shopping sites, ya professional accounts.
- Isse target ke interests, habits, aur network ka pata chal sakta hai – jaise agar email Netflix pe registered hai, to streaming habits ka hint milta hai.
- Ye info pivot points deti hai – aap in platforms pe jaake aur details (username, bio, posts) collect kar sakte ho.

Tools to Uncover Websites and Accounts:

1. **Epieos (tools.epieos.com/email.php)**

- **Kya Hai:** Epieos ek free OSINT tool hai jo email addresses ke linked accounts aur services ko dhoondhta hai – Google, Skype, social media, aur breaches tak check karta hai.
- **Kaise Use Karein:**
  (a) Epieos ke email lookup page (tools.epieos.com/email.php) pe jao.
  (b) Email daalo (e.g., "rishi.kabra@gmail.com") aur captcha solve karo.
  (c) Search karo – ye platforms list karega jahan email registered hai.
- **Output Example:**
  – Google: Account exists (Google ID, possible reviews).
  – Twitter: Linked profile (@rishi_kabra).
  – Spotify: Registered.
  – Breaches: LinkedIn 2012.
- **Fayda:** Free version mein hi kaafi data milta hai – paid plan ($29/month) extra details (e.g., Skype ID) deta hai.
- **Note:** Result mein profile pic bhi mil sakti hai – reverse image search ke liye useful.

2. **Castrick (castrick.toolforge.org)**

- **Kya Hai:** Ye ek newer OSINT tool hai jo email ya phone number se social media aur websites pe accounts dhoondhta hai – Epieos jaisa hi lekin thoda alag approach ke saath.
- **Kaise Use Karein:**
  (a) Castrick (castrick.toolforge.org) pe jao, email field mein "saad.sarraj@gmail.com" daalo.
  (b) "Search" pe click karo – ye check karta hai kahan email active hai.
- **Output Example:**
  – Instagram: @saadsarraj
  – Facebook: Linked account.
  – Partial phone: +91******21 (agar email se juda ho).
- **Fayda:** Free aur simple – social media focus zyada hai.
- **Note:** Kabhi partial results deta hai – full details ke liye cross-check karna padta hai.

3. **PreductaSearch.com (preductasearch.com)**

- **Kya Hai:** Ye ek paid OSINT service hai jo email se linked websites aur accounts ka deep analysis deta hai, lekin free tier mein bhi basic info milta hai.
- **Kaise Use Karein:**
  (a) Site (preductasearch.com) pe jao, email input karo (e.g., "satyam.singh@gmail.com").
  (b) Free search run karo – ye registered websites ke naam deta hai.
- **Output Example:**
  – Free: "Registered on Twitter, LinkedIn, Amazon".
  – Paid ($10/report): Full URLs aur usernames (e.g., twitter.com/satyam_singh).

- **Fayda:** Free mein platform names milte hain – paid mein granular data.
- **Note:** Budget tool hai – free version sirf starting point deta hai.

4. **Gravatar.com (Email Checker)**
   - **Kya Hai:** Gravatar (Globally Recognized Avatar) ek service hai jo email addresses ke saath profile pictures link karta hai. Ye WordPress, GitHub, aur forums jaise platforms pe use hota hai. Email checker se aap pata laga sakte ho ki email Gravatar pe registered hai ya nahi.
   - **Kaise Use Karein:**
     (a) Gravatar.com (gravatar.com) pe jao (direct search option nahi hai, lekin trick hai).
     (b) Email ka MD5 hash banao – online MD5 generator (e.g., md5hashgenerator.com) mein "rishi.kabra@gmail.com" daalo, output milega (e.g., "d41d8cd98f00b204e9800998ecf84
     (c) URL banao: `http://gravatar.com/avatar/[MD5-hash]` – browser mein paste karo (e.g., `http://gravatar.com/avatar/d41d8cd98f00b204e9800998ecf8427e`).
     (d) Agar profile pic load hoti hai, to email registered hai – default icon matlab nahi hai.
   - **Output Example:**
     – rishi.kabra@gmail.com → Custom avatar (registered).
     – saad@fake.com → Default icon (unregistered).
   - **Fayda:** Gravatar pe pic milne se email ke active use ka proof milta hai – pic ko reverse search (Google Lens) karo aur linked accounts dhoondho.
   - **Note:** Sirf avatar-based sites (WordPress, Stack Overflow) pe kaam karta hai – limited scope.

Workflow Example:

- **Email:** "satyam.singh@gmail.com"
- **Epieos:**
  – Registered: Twitter, Google, Spotify.
- **Castrick:**
  – Instagram: @satyam_singh, Facebook linked.
- **PreductaSearch:**
  – Free: Amazon, Netflix.
- **Gravatar:**
  – MD5: "e2f8f5b6c..." → Custom pic (registered) – reverse search se GitHub mila.
- **Conclusion:** Satyam ka email 7+ platforms pe active hai – Twitter, Instagram, GitHub pe pivot karo.

Extra Tips:

- **Cross-Check:** Ek tool se mila platform doosre pe verify karo – consistency se accuracy badhti hai.

- **Reverse Search:** Gravatar ya Epieos se pic mili to Google Lens (lens.google.com) ya Yandex se search karo – aur accounts mil sakte hain.
- **Expand:** Platform mila to username (satyam_singh) se Sherlock (`sherlock satyam_singh`, github.com/sherlock-project/sherlock) chalao.
- **Save:** Notion mein table banao:

Email	Platforms	Source	Extra Info
satyam.singh@gm	Twitter, Instagram, GitHub	Epieos, Gravatar	Custom avatar

Tables

Task	Tool	Output
Social Media Check	Epieos/Castrick	Linked Profiles
Site Names	PreductaSearch	Registered Sites
Avatar Check	Gravatar	Profile Pic

Table 33: Methods for Uncovering Linked Accounts

Summary

- Epieos aur Castrick se social accounts lo.
- PreductaSearch se site names, Gravatar se avatar check karo.
- Notion mein save karo – digital footprint track karo.

Point To Note

Agar aapke paas target ka email hai, to **Epieos** (tools.epieos.com/email.php), **Castrick** (castrick.toolforge.org), **PreductaSearch.com** (preductasearch.com), aur **Gravatar.com** (gravatar.com) se pata lagao ki wo kahan-kahan registered hai. Epieos aur Castrick free mein social media links dete hain, PreductaSearch free mein site names, aur Gravatar avatar se activity check karta hai. Har tool ke results ko Notion mein save karo – ye email ke hidden accounts ko uncover karta hai taaki aap target ke digital footprint ko pura track kar sako! Systematic kaam karo aur har lead ko follow karo.

==========

Discovering More Websites Linked to an Email Address

Discovering more websites linked to an email address ek valuable OSINT technique hai jo aapko ye pata lagane mein madad karti hai ki koi email address kahan-kahan registered hai – social media, forums, shopping sites, ya doosre platforms pe. Ek tool, **OSINT Industries**

(osint.industries.com), ye kaam karta tha – email ya phone number ko 300+ websites pe check karke linked accounts dhoondhta tha. Pehle ye free tha, lekin ab ye paid ho gaya hai (pricing April 2025 tak $49/month se start). Isliye, hum free alternatives explore karenge jo same details provide kar sakein – yani email se jude websites aur accounts ko uncover karne ke liye. Chalo kuch best free options dekhte hain jo OSINT Industries jaisa kaam karte hain, aur unka use kaise karna hai.

OSINT Industries Overview:

- **Kya Tha:** OSINT Industries ek email aur phone number investigation tool tha jo 300+ websites (Twitter, Instagram, Amazon, etc.) pe check karta tha ki email ya number registered hai ya nahi.
- **Features:**
  - Real-time data retrieval.
  - Linked accounts aur digital profiles compile karta tha.
  - Geospatial visualization aur timeline analysis.
- **Status:** Pehle free tha, lekin ab paid hai – basic plan $49/month (April 2025 tak).
- **Need for Alternatives:** Free tools se same results chahiye – budget-friendly aur effective.

Free Alternatives to OSINT Industries:

1. **Epieos (tools.epieos.com/email.php)**
   - **Kya Hai:** Epieos ek free OSINT tool hai jo email se linked accounts dhoondhta hai – Google, Twitter, Spotify, Skype, aur breaches tak check karta hai.
   - **Kaise Use Karein:**
     (a) Epieos email lookup page (tools.epieos.com/email.php) pe jao.
     (b) Email daalo (e.g., "rishi.kabra@gmail.com") aur captcha solve karo.
     (c) Search karo – ye platforms list karega jahan email registered hai.
   - **Output Example:**
     - Google: Account exists.
     - Twitter: @rishi_kabra.
     - Spotify: Registered.
   - **Fayda:** Free, simple, aur broad coverage – 300+ sites nahi, lekin major platforms cover karta hai.
   - **Note:** Profile pics bhi deta hai – reverse image search ke liye useful.
2. **Holehe (github.com/megadose/holehe)**
   - **Kya Hai:** Holehe ek open-source Python tool hai jo email se registered accounts check karta hai – 100+ websites (Twitter, Instagram, Snapchat, etc.) pe focus karta hai.
   - **Kaise Use Karein:**
     (a) GitHub (github.com/megadose/holehe) se Holehe download karo (python3 install hona chahiye).
     (b) Terminal mein: `pip install holehe` aur `holehe rishi.kabra@gmail.com`.

(c) Ye list dega jahan email registered hai.

- **Output Example:**
  - Twitter: Registered.
  - Instagram: Registered.
  - Amazon: Not found.
- **Fayda:** Free, open-source, aur lightweight – OSINT Industries ke 300+ ke muqable 100+ sites, lekin effective.
- **Note:** Technical setup chahiye – non-tech users ke liye thoda tricky ho sakta hai.

3. **Ignorant (github.com/megadose/ignorant)**

- **Kya Hai:** Ignorant ek aur open-source tool hai jo phone numbers ke liye zyada famous hai, lekin emails ke saath bhi kaam karta hai – Snapchat, Instagram, etc. check karta hai.
- **Kaise Use Karein:**

(a) GitHub se clone karo: `git clone https://github.com/megadose/ignorant`.

(b) `pip install -r requirements.txt` aur `python3 ignorant.py -e rishi.kabra@gmail.`

(c) Registered sites list karega.

- **Output Example:**
  - Snapchat: Found.
  - Instagram: Found.
- **Fayda:** Free aur command-line based – Holehe jaisa hi lekin thoda different sites cover karta hai.
- **Note:** Phone ke saath zyada optimized hai – email coverage limited ho sakta hai.

4. **PrivacyWatch.app (privacywatch.app)**

- **Kya Hai:** Ye ek free web-based tool hai jo email se linked accounts aur privacy risks check karta hai – social media aur basic sites pe focus.
- **Kaise Use Karein:**

(a) PrivacyWatch (privacywatch.app) pe jao, email daalo (e.g., "saad.sarraj@gmail.com").

(b) Search karo – ye registered platforms aur data exposure batayega.

- **Output Example:**
  - Facebook: Linked.
  - Twitter: Linked.
- **Fayda:** No installation, browser se direct use – beginner-friendly.
- **Note:** Coverage OSINT Industries jaisa nahi – major platforms tak seemit.

5. **Sherlock (github.com/sherlock-project/sherlock)**

- **Kya Hai:** Sherlock username-based tool hai, lekin email ke username part (e.g., "rishi.kabra") se 400+ sites pe accounts dhoondh sakta hai.
- **Kaise Use Karein:**

(a) GitHub se download karo: `git clone https://github.com/sherlock-project/sherlock`

(b) `pip install -r requirements.txt` aur `python3 sherlock.py rishi.kabra`.

(c) Linked sites list karega.

- **Output Example:**
  - GitHub: rishi.kabra
  - Reddit: rishi.kabra
- **Fayda:** Free, open-source, aur 400+ sites – OSINT Industries se zyada coverage.
- **Note:** Direct email nahi, username pe kaam karta hai – email se extract karna padta hai.

Workflow Example:

- **Email:** "satyam.singh@gmail.com"
- **Epieos:** Twitter, Google, Spotify registered.
- **Holehe:** Instagram, Snapchat found.
- **Sherlock (username: satyam.singh):** Reddit, GitHub linked.
- **Conclusion:** Satyam ka email 6+ platforms pe active – OSINT Industries jaisa result free mein.

Extra Tips:

- **Combine Tools:** Epieos aur Holehe saath use karo – coverage badh jayega.
- **Gravatar Check:** Email ka MD5 hash bana ke gravatar.com pe avatar check karo – registered sites ka hint milta hai.
- **Cross-Check:** Platform mila to wahan username ya bio se email confirm karo.
- **Save:** Notion mein table banao:

Email	Platforms	Tool
satyam.singh@gm	Twitter, Instagram, Reddit	Epieos, Sherlock

Tables

Task	Tool	Output
Broad Check	Epieos	Major Platforms
Deep Scan	Holehe/Sherlock	100-400+ Sites
Simple Check	PrivacyWatch	Basic Links

Table 34: Methods for Discovering Linked Websites

Summary

- Epieos, Holehe se free mein platforms lo.
- Sherlock se 400+ sites check karo – username extract karo.
- Notion mein save karo – OSINT Industries ka free alt banayein.

Point To Note

OSINT Industries ab paid hai ($49/month), lekin free alternatives jaise **Epieos** (tools.epieos.com/email.php), **Holehe** (github.com/megadose/holehe), **Ignorant** (github.com/megadose/ignorant), **PrivacyWatch** (privacywatch.app), aur **Sherlock** (github.com/sherlock-project/sherlock) se email ke linked websites dhoondhe ja sakte hain. Ye tools 300+ sites nahi cover karte, lekin 100-400 sites tak kaafi data dete hain. Epieos aur PrivacyWatch browser-based hain – easy start ke liye. Holehe aur Sherlock technical hain – zyada depth ke liye. Har result ko Notion mein save karo – ye email OSINT ko budget mein boost karta hai taaki aap target ke digital presence ko pura track kar sako!

==========

Gmail OSINT - Discovering Phone Number, Reviews, Addresses, and More

Gmail OSINT ek powerful approach hai jo Gmail account ke through target ke baare mein valuable information – jaise **partial phone number**, **GAIA ID**, reviews, addresses, aur aur bhi – uncover karne mein madad karta hai. Agar target Gmail use karta hai, to aap uske email address ko seed bana ke uski digital footprint track kar sakte ho. Is process mein hum Gmail ke "Forgot Password" feature ka use karenge partial phone number ke liye, aur **GHunt Online (gmail-osint.active.jp)** jaise tools se GAIA ID, reviews, aur doosri details extract karenge. Ye method simple hai lekin effective – chalo step-by-step samajhte hain kaise Gmail se ye sab info nikali jaaye.

Why Gmail OSINT?

- Gmail duniya ka sabse popular email provider hai – billions log ispe accounts banate hain, jo Google services (Maps, YouTube, Drive) se linked hote hain.
- Ek Gmail address se aap target ke phone number digits, location (via reviews), aur identity (GAIA ID) tak pahunch sakte ho.
- Ye info social engineering, profiling, ya investigation ke liye pivot points deti hai.

Steps to Discover Info from Gmail:

1. **You Have the Target's Email Address:**
   - Maan lo aapke paas target ka email hai – e.g., "rishi.kabra@gmail.com".
   - Ye starting point hai – isse hum phone number aur GAIA ID tak jayenge.
2. **Partial Phone Number via Gmail Forgot Password:**
   - **Process:**

(a) Gmail.com pe jao, login page pe "Forgot Password" pe click karo.

(b) Target ka email paste karo (rishi.kabra@gmail.com) aur "Next" dabao.

(c) "Try another way" select karo jab tak "Phone Number" option na aaye.

(d) Agar phone number security setting mein hai, to Gmail ek masked number dikhayega – e.g., "Confirms the phone number you provided in your security settings: ********16".

- **Output:**
  - Last 2 digits milte hain – "16".
  - Country code bhi guess kar sakte ho agar aapko target ka location pata hai (e.g., +91 for India).
- **Fayda:** Ye partial number future verification ya number guessing (e.g., +919876543216) ke liye base deta hai.
- **Note:** Agar phone number linked nahi hai, to ye step kaam nahi karega – email-only recovery pe switch karo.

3. **Find GAIA ID and More with GHunt Online:**
   - **Tool: GHunt Online** (https://gmail-osint.active.jp)
   - **Kya Hai:** Ye ek free, web-based OSINT tool hai jo Gmail accounts se info extract karta hai – GAIA ID, reviews, addresses, aur Google services ka usage. GHunt ka online version hai, jo Python setup ki zarurat nahi mangta (original GHunt GitHub pe hai).
   - **Kaise Use Karein:**

     (a) Browser mein https://gmail-osint.active.jp kholo.

     (b) "Gmail Address" field mein target email daalo (rishi.kabra@gmail.com).

     (c) "Acquisition" ya "Search" pe click karo (Japanese interface hai, lekin Chrome translate se English ho jayega).
   - **Output Example:**
     - **GAIA ID:** 21-digit unique Google identifier (e.g., 115843729104562738291).
     - **Name:** Rishi Kabra (agar profile public hai).
     - **Phone Number Hint:** Partial ya linked services se guess (e.g., Google Voice).
     - **Reviews:** Google Maps reviews – "Rishi rated Cafe Coffee Day, Mumbai, 4 stars" (location hint: Mumbai).
     - **Addresses:** Reviews ya Google Photos metadata se approximate location.
     - **Services:** YouTube channel, Google Drive files, Calendar (agar public).
   - **Fayda:** GAIA ID se aap target ko Google ecosystem mein track kar sakte ho – email change ho to bhi ID same rehta hai.
   - **Note:** Japanese site hai – VPN use karo agar privacy concern hai, aur Chrome translate on rakho.

4. **Expand the Findings:**
   - **Phone Number:** Partial digits (16) se full number guess karo – country code (+91) aur common patterns (9876543216) try karo.
   - **Reviews:** Maps reviews se location refine karo – "Mumbai" se specific areas ya habits pata karo.

- **GAIA ID:** GHunt ke original version (github.com/mxrch/GHunt) mein GAIA ID daal ke deep dive karo – YouTube, Photos, etc.

5. **Save and Analyze:**
   - Notion mein table banao:

Email	Phone Hint	GAIA ID	Reviews	Source
rishi.kabra@gmail	*******16	115843729104562 7	Cafe Coffee Day, Mumbai	GHunt Online

Workflow Example:

- **Email:** "satyam.singh@gmail.com"
- **Gmail Forgot Password:**
  - Output: ********23 – last digits "23".
- **GHunt Online:**
  - GAIA ID: 108927364512938475102
  - Reviews: "Satyam rated Tech Park, Bangalore, 5 stars".
  - Address Hint: Bangalore, India.
- **Conclusion:** Satyam ka phone number ********23 hai, Bangalore mein active hai.

Extra Tips:

- **Cross-Check:** GHunt se mile reviews ko Google Maps pe manually verify karo – exact location ke liye.
- **Sherlock:** Username (satyam.singh) se 400+ sites pe accounts dhoondho – email se match karo (github.com/sherlock-project/sherlock).
- **Safety:** Dummy Gmail ya VPN use karo – Forgot Password attempts target ko alert kar sakte hain.
- **Expand:** GAIA ID se Epieos (tools.epieos.com) pe aur info lo – Skype, Trello, etc.

Tables

Task	Method	Output
Phone Hint	Forgot Password	Partial Digits
Deep Info	GHunt Online	GAIA ID, Reviews
Expand	Epieos/Sherlock	Extra Accounts

Table 35: Methods for Gmail OSINT

Summary

- Forgot Password se phone hint lo – ********16.
- GHunt Online se GAIA ID, reviews, addresses nikalo.
- Notion mein save karo – Gmail se pura profile banao.

Point To Note

Gmail OSINT se **partial phone number** (e.g., ********16) Gmail Forgot Password se lo, aur **GAIA ID**, **reviews**, **addresses** GHunt Online (https://gmail-osint.active.jp) se uncover karo. Ye tool email se Google ecosystem ki deep info deta hai – phone digits, locations, aur services. Har detail ko Notion mein save karo – ye target ke digital life ko khol deta hai, bas systematically kaam karo aur free resources ka pura fayda uthao!

==========

Identity Data Leaks Linked to an Email Address

Identity data leaks linked to an email address ek critical OSINT investigation hai jo ye pata lagane mein madad karta hai ki koi email address kahan-kahan **data breaches** ya **leaks** mein shamil raha hai. Leaked databases mein search karke aap identify kar sakte ho ki target ka email – aur uske saath judi personal info jaise name, phone number, ya passwords – kab aur kahan expose hua. Is process mein **Have I Been Pwned (HIBP)** jaise websites ka use hota hai jo breaches ko track karta hai aur aapko relevant leaks ke bare mein batata hai. Aap in breaches ke data ko download bhi kar sakte ho aur additional info ke liye further search kar sakte ho. Chalo step-by-step dekhte hain kaise email se identity leaks uncover kiye jate hain.

Why Check Identity Data Leaks?

- Data breaches har saal billions records expose karte hain – emails, passwords, aur sensitive info jaise Social Security numbers ya addresses leak ho sakte hain.
- Ek email address breach mein milne se identity theft, account takeover, ya fraud ka risk badh jata hai.
- HIBP jaise tools aapko ye batate hain ki aapka data kahan compromise hua aur uska impact kya ho sakta hai.

Steps to Identify Data Breaches Linked to an Email:

1. **Search in Leaked Databases with Have I Been Pwned (HIBP):**
   - **Website: haveibeenpwned.com** (haveibeenpwned.com)
   - **Kya Hai:** HIBP ek free service hai jo 600+ data breaches aur billions of compromised accounts ko track karta hai – Troy Hunt ne isse banaya hai taaki log apna exposure check kar sakein.
   - **Kaise Use Karein:**
     (a) haveibeenpwned.com pe jao.
     (b) Search bar mein email daalo (e.g., "rishi.kabra@gmail.com") aur "pwned?" pe click karo.
     (c) Results check karo – agar email breached hai, to list milegi.

- **Output Example:**
  - Email: rishi.kabra@gmail.com
  - Breaches:
    - **LinkedIn (2012):** 167M accounts, emails leaked.
    - **Adobe (2013):** 153M accounts, emails + hashed passwords.
  - Pastes: Pastebin pe email mention (e.g., forum dump).
- **Fayda:** Ye batata hai email kab, kahan leak hua – aur agar passwords bhi shamil hain to risk level.
- **Note:** HIBP free hai, lekin full breach data download nahi deta – metadata hi milta hai.

2. **Identify Specific Breaches and Leaks:**
   - HIBP results mein har breach ka naam, date, aur compromised data type hota hai (e.g., emails, passwords, phone numbers).
   - Example:
     - **LinkedIn 2012:** rishi.kabra@gmail.com mila – matlab email expose hua, password hashed tha.
     - **Twitter 2022:** 200M users, email + phone number leak.
   - Sensitive breaches (e.g., Ashley Madison) sirf verified owners hi search kar sakte hain – privacy ke liye.

3. **Download Relevant Data Breaches/Leaks:**
   - HIBP direct downloads nahi deta, lekin breach info se aap specific leaks ke sources track kar sakte ho:
     - **DeHashed** (dehashed.com): Paid tool ($5/month) – email search karke full breach data (unmasked emails, passwords) download karo.
     - **Dark Web Forums:** Breach data torrent ya paste sites (Pastebin) pe mil sakta hai – legal/ethical limits mein raho.
     - **Public Archives:** Kaggle ya archive.org pe old breach datasets free mil sakte hain (e.g., LinkedIn 2012 dump).
   - **Note:** Downloaded data encrypted ya hashed ho sakta hai – cracking ke liye tools (Hashcat) chahiye, lekin ye illegal ho sakta hai.

4. **Search for Additional Info:**
   - Breach se mile data ko expand karo:
     - **Google Search:** "rishi.kabra@gmail.com" site:pastebin.com – pastes dhoondho.
     - **Sherlock:** Username (rishi.kabra) se 400+ sites pe accounts lo – breach se match karo (github.com/sherlock-project/sherlock).
     - **Emailrep.io:** Email ka reputation aur linked profiles (Twitter, Gravatar) check karo (emailrep.io).
   - **Cross-Check:** Agar phone number leak hua (e.g., +919876543216), to usse Epieos (tools.epieos.com) pe aur accounts dhoondho.
   - **Output:** Breach se name (Rishi Kabra), phone (+91...), aur Twitter (@rishi_kabra) mila.

5. **Save and Analyze:**

- Notion mein table banao:

Email	Breach	Data Leaked	Additional Info	Source
rishi.kabra@gmail	LinkedIn 2012	Email, Password	Twitter: @rishi_kabra	HIBP
rishi.kabra@gmail	Adobe 2013	Email, Hint: "rishi123"	Phone: +91...	DeHashed

Workflow Example:

- **Email:** "satyam.singh@gmail.com"
- **HIBP:**
  - Breaches: Twitter 2022 (email, phone), Canva 2019 (email, username).
- **Download:** DeHashed se Twitter dump – satyam.singh@gmail.com + ********23 (phone).
- **Additional Search:** Sherlock se @satyam_singh Reddit pe mila.
- **Conclusion:** Satyam ka email 2 breaches mein, phone partial (23), Reddit account linked.

Extra Tips:

- **Notify:** HIBP pe email subscribe karo – future breaches ke alerts milenge.
- **Cross-Check:** Breach se mila phone ya username GHunt (gmail-osint.active.jp) pe verify karo.
- **Safety:** VPN use karo – dark web ya leak sites risky hote hain.
- **Expand:** Leaked password mila to Pwned Passwords (HIBP, haveibeenpwned.com/passwords) pe check karo – kitni baar expose hua.

Tables

Task	Method	Output
Breach Check	HIBP	Breach List
Data Download	DeHashed	Full Details
Expand Info	Sherlock/Epieos	Linked Accounts

Table 36: Methods for Identifying Data Leaks

Summary

- HIBP se breaches lo – LinkedIn, Twitter.
- DeHashed se full data, Sherlock se accounts nikalo.
- Notion mein save karo – identity leaks track karo.

Point To Note

Identity data leaks ko **Have I Been Pwned** (haveibeenpwned.com) se shuru karo – email breaches (LinkedIn, Twitter) identify karo. Relevant leaks download karne ke liye DeHashed (dehashed.com) ya public sources use karo, phir Google, Sherlock se additional info lo. Har finding ko Notion mein save karo – ye email se judi compromised identity ko pura khol deta hai. Ethical boundaries mein raho aur systematically kaam karo taaki target ka data exposure clear ho!

==========

Discovering LinkedIn Profiles Linked to an Email

Discovering LinkedIn profiles linked to an email ek effective OSINT technique hai jo aapko email address ya phone number ke zariye kisi ka LinkedIn account dhoondhne mein madad karta hai. **SignalHire browser extension** is kaam ko asaan banata hai – ye Chrome aur Firefox pe available hai aur aapko ek email (e.g., rishi.kabra@gmail.com) ya phone number (+919876543210) daal kar usse jude LinkedIn profiles instantly reveal karta hai. Ye tool real-time search karta hai aur verified data deta hai, jo recruiters, sales professionals, ya investigators ke liye kaam ka hai. Chalo is process ko step-by-step samajhte hain taaki aap bhi SignalHire ke saath LinkedIn profiles uncover kar sako.

Why Discover LinkedIn Profiles with an Email?

- Email ya phone number ek seed hai jo target ke professional identity tak le jata hai – LinkedIn pe profile milne se name, job title, company, aur network pata chal sakta hai.
- SignalHire iska advantage ye hai ki ye manual search ka time bachata hai aur direct LinkedIn link deta hai.

Steps to Use SignalHire Browser Extension:

1. **Install SignalHire Extension:**
   - Chrome Web Store ya Firefox Add-ons se "SignalHire - find email or phone number" download karo (www.signalhire.com).
   - Browser toolbar mein SignalHire (SH) icon add ho jayega.
2. **Input Email or Phone Number:**
   - Browser mein SignalHire icon pe click karo – ek pop-up khulega.
   - Email (e.g., "satyam.singh@gmail.com") ya phone number (+919876543210) paste karo clipboard se ya manually type karo.
3. **Search for LinkedIn Profile:**
   - Pop-up mein "Find Profile" button dabao – SignalHire real-time search karega.

- Agar email/phone LinkedIn se linked hai, to profile URL milega (e.g., linkedin.com/in/satyam-singh).

4. **Analyze Results:**
   - **Output Example:**
     - Email: rishi.kabra@gmail.com
     - LinkedIn: linkedin.com/in/rishi-kabra
     - Bonus: Phone ya additional emails bhi mil sakte hain.
   - Profile kholo aur details lo – name, job, company, connections.
5. **Save and Expand:**
   - Profile ko SignalHire se export karo (CSV ya ATS/CRM jaise Zoho) ya Notion mein save karo:

Email	LinkedIn Profile	Source
rishi.kabra@gmail	linkedin.com/in/r kabra	SignalHire

Extra Tips:

- **Free Plan:** SignalHire free mein 5 credits/month deta hai – har credit ek profile search ke liye. Paid plan ($49/month) unlimited access deta hai.
- **Cross-Check:** LinkedIn profile se username (rishi-kabra) lo aur Sherlock (github.com/sherlock-project/sherlock) se aur accounts dhoondho.
- **Accuracy:** SignalHire 96% hit rate claim karta hai – agar profile nahi milta, to email/-phone LinkedIn pe registered nahi hai.

Recap: Email OSINT Process

Email OSINT ka pura process recap karte hain – target ke email se linked info aur LinkedIn profiles dhoondhne ke tareeke:

1. **Check Email Presence on Search Engines:**
   - Google operators use karo: `"satyam.singh@gmail.com"` – email kahan indexed hai (forums, social media).
2. **Assess Email Reputation:**
   - **Emailrep.io** pe email daalo – reputation score, social profiles (Twitter, Gravatar), breaches check karo (emailrep.io).
3. **Identify Email Registration on Other Sites:**
   - **Epieos** ya **Holehe** se dekho email kahan registered hai – Twitter, Spotify, etc. (tools.epieos.com, github.com/megadose/holehe).
4. **Search in Data Leaks/Breaches:**

- **Have I Been Pwned** pe email search karo – breaches (LinkedIn 2012, Twitter 2022) mein exposure check karo (haveibeenpwned.com).

5. **Try Password Reset:**
   - Social platforms (Facebook, Twitter) pe "Forgot Password" se masked email lo (e.g., s***m@g**.com) – guess karo: satyam@gmail.com.
6. **Conduct Reverse Email Lookup Using SignalHire:**
   - SignalHire extension mein email/phone daal ke LinkedIn profile lo – e.g., "rishi.kabra@gmail.com se linkedin.com/in/rishi-kabra.

Workflow Example:

- **Email:** "saad.sarraj@gmail.com"
- **SignalHire:** LinkedIn: linkedin.com/in/saadsarraj
- **HIBP:** Twitter 2022 breach – phone hint (+91...).
- **Emailrep:** Profiles: Twitter (@saadsarraj).
- **Conclusion:** Saad ka LinkedIn mila, Twitter se cross-checked.

Final Tips:

- **Combine Methods:** SignalHire ke saath HIBP, Epieos use karo – full picture banega.
- **Save:** Har finding Notion mein organize karo – email, LinkedIn, breaches ek jagah.
- **Ethics:** Legal limits mein raho – personal use ke liye permission lo.

Tables

Task	Method	Output
LinkedIn Lookup	SignalHire	Profile URL
Breach Check	HIBP	Leaked Data
Site Registration	Epieos	Social Accounts

Table 37: Methods for Email OSINT

Summary

- SignalHire se LinkedIn profile lo – email ya phone se.
- HIBP, Epieos se breaches aur accounts check karo.
- Notion mein save karo – pura OSINT organize rakho.

Point To Note

SignalHire browser extension se email (e.g., rishi.kabra@gmail.com) ya phone se LinkedIn profiles dhoondho – install karo, search karo, aur profile lo. Recap mein – search engines, reputation, registrations, breaches, password resets, aur SignalHire se reverse lookup karo. Ye systematic approach email OSINT ko complete karta hai – har step target ke digital identity ko kholta hai, bas Notion mein save karte jao!

==========

Tracking a Phone Number Across Online Platforms

Tracking a phone number across online platforms ek powerful phone number OSINT technique hai jo aapko target ke contact details aur digital presence ko uncover karne mein madad karta hai. Agar aapke paas target ka **email address** hai, to phone number dhoondhna aur bhi asaan ho jata hai – email ko seed bana ke aap data leaks check kar sakte ho ya usse registered accounts pe focus kar sakte ho. Is process mein hum do main approaches use karenge: (1) **social media aur online accounts** pe phone number check karna, aur (2) **search operators** ke saath search engines pe number dhoondhna. Ye method systematic hai aur target ke phone number tak le jata hai – chalo step-by-step samajhte hain.

Why Track a Phone Number Across Platforms?

- Phone numbers ek direct link hote hain jo target ke real-world identity (location, contacts) aur online accounts ko connect karte hain.
- Email se shuru karke aap leaks ya public profiles ke zariye number tak pahunch sakte ho – ye info profiling ya verification ke liye critical hai.

Steps to Track a Phone Number:

1. **Check If the Person Has Shared Their Phone Number on Online/Social Media Accounts:**
   - **Agar Email Hai:**
     - Email ko starting point banao – pehle check karo ki ye email kahan-kahan registered hai (Epieos, SignalHire).
     - Registered platforms pe jao aur phone number dhoondho.
   - **Social Media Platforms:**
     - **Facebook:** "About" section mein "Contact Info" check karo – agar public hai to number milega (e.g., +919876543210).
     - **Twitter:** Bio mein phone ya WhatsApp mention ho sakta hai (e.g., "Contact: +91...").
     - **Instagram:** Business accounts pe "Call" ya "Text" button hota hai – number reveal hota hai.
     - **LinkedIn:** "Contact Info" section mein phone number public ho sakta hai (e.g., +1-919-555-1234).
   - **Other Platforms:**
     - WhatsApp ya Telegram pe email ka username (rishi.kabra) try karo – agar linked hai to phone number confirm hoga.

- **Output Example:**
  - Email: rishi.kabra@gmail.com
  - LinkedIn: +919876543210 (public profile se).
- **Fayda:** Direct aur free – agar target ne number share kiya hai to seed email se turant mil jata hai.
- **Note:** Privacy settings tight honge to number nahi milega – leaks pe depend karna padega.

2. **Use Search Operators to Find the Person's Phone Number on Search Engines:**
   - **Search Operator Format:**
     - `"first and last name" "city" "phone number" OR "number" OR "country code"`
     - Quotes ("") exact phrases ke liye, OR multiple options deta hai.
   - **Examples:**
     - `"Rishi Kabra" "Kolkata" "phone number" OR "number" OR "+91"`
     - Result: Forum post – "Rishi Kabra, Kolkata, +919876543210".
     - `"Satyam Singh" "Delhi" "phone" OR "+91"`
     - Result: Directory – "Satyam Singh, Delhi, +919123456789".
   - **Refine Search:**
     - **Site-Specific:** `"Rishi Kabra" "phone number" site:linkedin.com` – LinkedIn pe focus.
     - **Exclude Noise:** `"Rishi Kabra" "number" -inurl:(facebook twitter)` – FB/Twitter ke alawa results.
     - **Add Context:** `"Rishi Kabra" "TechMojo" "phone"` – Company ke saath number.
   - **Output Example:**
     - "Rishi Kabra, TechMojo, Kolkata, Contact: +919876543210" (company site se).
   - **Fayda:** Search engines public data (directories, forums, resumes) se numbers scrape karte hain.
   - **Note:** Number outdated ho sakta hai – multiple sources se verify karo.

3. **Leverage Email for Additional Leads:**
   - **Data Leaks:**
     - **Have I Been Pwned:** rishi.kabra@gmail.com daalo – Twitter 2022 breach se phone hint (+91******10) (haveibeenpwned.com).
     - **DeHashed:** Full number (+919876543210) breach dump mein mil sakta hai (paid, dehashed.com).
   - **Registered Accounts:**
     - **Epieos:** Email se Twitter, WhatsApp check karo – phone linked hai to hint milega (tools.epieos.com).
     - **SignalHire:** Email se LinkedIn profile lo – phone number shayad public ho (www.signalhire.com).

4. **Save and Verify:**

Email	Phone Number	Source	Context
rishi.kabra@gmail	+919876543210	LinkedIn	Public profile
satyam.singh@gm	+919123456789	Google Search	Delhi directory

- Notion mein table banao:

Workflow Example:

- **Email:** "saad.sarraj@gmail.com"
- **Social Media:**
  - Twitter bio: "WhatsApp: +971555123456".
- **Search Operators:**
  - `"Saad Sarraj" "Dubai" "phone number" OR "+971"` – Result: +971555123456 (forum post).
- **Leaks:**
  - HIBP: Twitter 2022 – phone hint (+971******56).
- **Conclusion:** Saad ka number +971555123456 hai – Twitter aur search se confirmed.

Extra Tips:

- **Cross-Check:** Ek source se mila number doosre pe verify karo – consistency zaroori hai.
- **Country Code:** Location pata hai to code add karo (+91 India, +1 US) – accuracy badhti hai.
- **Gmail Trick:** Email se phone hint mila to Gmail "Compose" mein number check karo – profile pic se link confirm ho sakta hai.
- **Safety:** Dummy account ya VPN use karo – sensitive searches ke liye precaution.

Tables

Task	Method	Output
Social Check	Facebook, LinkedIn	Public Number
Search Engine	Operators	Directory/Forum
Leak Check	HIBP, DeHashed	Breach Hint

Table 38: Methods for Tracking Phone Numbers

Summary

- Social media pe number lo – Twitter, LinkedIn.
- Search operators aur leaks se hints nikalo.
- Notion mein save karo – phone OSINT organize rakho.

Point To Note

Phone number tracking ke liye email (e.g., rishi.kabra@gmail.com) se shuru karo – **social media** (LinkedIn, Twitter) pe number check karo aur **search operators** (`"Rishi Kabra" "Kolkata" "phone number"`) se Google pe dhoondho. Leaks (HIBP) aur tools (Epieos) se extra hints lo – har finding ko Notion mein save karo. Ye method target ke phone number ko online platforms se khol deta hai – bas systematically kaam karo aur email ka pura fayda uthao!

==========

Uncovering Phone Numbers Linked to LinkedIn Accounts

Uncovering phone numbers linked to LinkedIn accounts ek smart OSINT technique hai jo aapko LinkedIn profiles se associated phone numbers dhoondhne mein madad karta hai. Agar aapke paas target ka LinkedIn profile hai, to **phone lookup browser extensions** ka use karke aap unke contact details – jaise phone number – tak pahunch sakte ho. Ye extensions real-time mein LinkedIn data ko scan karte hain aur verified phone numbers provide karte hain. Kuch popular extensions hain **ContactOut**, **SignalHire**, aur **GetProspect** – ye tools Chrome ya Firefox pe kaam karte hain aur recruiters, sales professionals, ya investigators ke liye kaam ke hain. Chalo inko step-by-step explore karte hain taaki aap LinkedIn se phone numbers uncover kar sako.

Why Uncover Phone Numbers from LinkedIn?

- LinkedIn ek professional platform hai jahan log apne contact details (phone, email) share karte hain – lekin ye info aksar private hoti hai ya manually dhoondhna mushkil hota hai.
- Phone lookup extensions time bachate hain aur direct contact info dete hain – cold calling, networking, ya verification ke liye perfect.

Phone Lookup Extensions:

1. **ContactOut**
   - **Kya Hai:** ContactOut ek Chrome extension hai jo LinkedIn profiles se emails aur phone numbers extract karta hai – 1.2 billion+ records ka database claim karta hai.
   - **Kaise Use Karein:**
     (a) Chrome Web Store se "Email Finder by ContactOut" install karo (contactout.com).
     (b) LinkedIn pe target profile kholo (e.g., linkedin.com/in/rishi-kabra).
     (c) ContactOut icon pe click karo – pop-up mein phone number dikhega (agar available hai).
   - **Output Example:**

- Profile: linkedin.com/in/rishi-kabra
- Phone: +919876543210 (70% US profiles ke liye numbers milte hain).

- **Fayda:** Free plan mein 2 phone numbers/day, paid ($79/month) mein 600/year. 76% Fortune 500 companies use karte hain.
- **Note:** Accuracy zyada hai, lekin privacy settings se limited ho sakta hai.

2. **SignalHire**

- **Kya Hai:** SignalHire ek Chrome/Firefox extension hai jo LinkedIn, GitHub, Twitter jaise platforms se phone numbers aur emails dhoondhta hai – 400M+ profiles ka database.
- **Kaise Use Karein:**
  (a) SignalHire extension install karo (signalhire.com).
  (b) LinkedIn profile pe jao (e.g., linkedin.com/in/satyam-singh).
  (c) Icon pe click karo – "Find Profile" se phone number reveal hota hai.
- **Output Example:**
  - Profile: linkedin.com/in/satyam-singh
  - Phone: +919123456789
- **Fayda:** Free mein 5 credits/month (1 credit = 1 number/email), paid ($49/month) unlimited. 96% hit rate claim.
- **Note:** Bulk search (100 profiles) bhi possible hai – ATS/CRM export ke saath.

3. **GetProspect**

- **Kya Hai:** GetProspect ek LinkedIn-focused Chrome extension hai jo emails aur phone numbers extract karta hai – B2B prospecting ke liye designed.
- **Kaise Use Karein:**
  (a) Chrome Store se "GetProspect" install karo (getprospect.com).
  (b) LinkedIn pe profile ya search results kholo.
  (c) GetProspect icon pe click karo – phone number aur email list karega.
- **Output Example:**
  - Profile: linkedin.com/in/saad-sarraj
  - Phone: +971555123456
- **Fayda:** Free plan mein 50 credits/month, paid ($49/month) mein 1000 credits. Bulk export to CSV.
- **Note:** LinkedIn Sales Navigator ke saath bhi kaam karta hai – deep searches ke liye.

Workflow Example:

- **Target:** linkedin.com/in/rishi-kabra
- **ContactOut:** +919876543210 (daily limit mein).
- **SignalHire:** +919876543210 + Twitter link (@rishi_kabra).
- **GetProspect:** +919876543210 + email (rishi.kabra@gmail.com).
- **Conclusion:** Teeno tools se number mila – consistency se verified.

Extra Tips:

- **Cross-Check:** Ek extension se mila number doosre se confirm karo – accuracy badhegi.
- **Privacy Limits:** Agar LinkedIn pe number private hai, to leaks (HIBP, haveibeenpwned.com) ya social media bio check karo.
- **Save:** Notion mein table banao:

Profile	Phone Number	Extension
linkedin.com/in/r kabra	+919876543210	SignalHire

- **Safety:** LinkedIn ToS violate na karo – excessive use se account ban ho sakta hai.

Tables

Extension	Free Limit	Output
ContactOut	2/day	Phone Number
SignalHire	5/month	Phone + Links
GetProspect	50/month	Phone + Email

Table 39: Phone Lookup Extensions Comparison

Summary

- ContactOut, SignalHire se LinkedIn phone lo.
- GetProspect se bulk extract karo – free limits ka fayda uthao.
- Notion mein save karo – contact details organize rakho.

Point To Note

Phone lookup extensions jaise **ContactOut** (contactout.com), **SignalHire** (signalhire.com), aur **GetProspect** (getprospect.com) LinkedIn accounts se phone numbers uncover karne ka fast tareeka hain. Inko install karo, LinkedIn profile pe jao, aur click se number lo – ContactOut free mein 2/day, SignalHire 5/month, aur GetProspect 50/month deta hai. Har tool ke results ko Notion mein save karo – ye target ke contact details ko tezi se khol deta hai, bas ethical boundaries mein raho aur systematically kaam karo!

==========

Finding Phone Numbers in Leaked Databases

Finding phone numbers in leaked databases ek advanced OSINT technique hai jo target ke phone numbers ko **leaked ya breached databases** se uncover karne mein madad karta hai. Agar aapke paas target ka **name**, **email address**, ya **password** hai, to aap in details ke zariye breaches mein search kar sakte ho aur usse jude phone numbers tak pahunch sakte ho. Ye process powerful hai kyunki breaches mein emails ke saath phone numbers, usernames, aur passwords jaise sensitive data aksar leak hota hai. **Have I Been Pwned (HIBP)** jaise tools se aap email check kar sakte ho – agar wo leaked hai, to us breach ka data download karke phone number dhoondha ja sakta hai. Iske alawa, specific leaks jaise **Facebook leak**, **Snapchat leak**, ya generic **database leaks** bhi check karne ke options hain. Chalo isko step-by-step samajhte hain aur phone numbers kaise milte hain dekhte hain.

Why Search Leaked Databases for Phone Numbers?

- Data breaches mein billions records expose hote hain – phone numbers aksar emails ke saath leak hote hain (e.g., Twitter 2022: 200M+ users).
- Agar email ya name breach mein hai, to phone number milne ke chances badh jate hain – ye contact tracing ya profiling ke liye seed ban sakta hai.
- Leaked data dark web, forums, ya public archives pe mil jata hai – thodi digging se number haath lag sakta hai.

Steps to Find Phone Numbers in Leaked Databases:

1. **Search in Leaked Databases Using Name, Email, or Password:**
   - **Have I Been Pwned (haveibeenpwned.com):**
     - **Kaise Karein:**
       (a) HIBP pe jao (haveibeenpwned.com), email daalo (e.g., "rishi.kabra@gmail.com").
       (b) "pwned?" pe click karo – agar email breached hai, to list milegi (e.g., LinkedIn 2012, Adobe 2013).
     - **Output:** "Breached: LinkedIn 2012 – email, phone, password exposed."
     - **Next Step:** Breach ka naam note karo – full data dhoondhne ke liye aage badho.
   - **Note:** Agar email breached hai, to us database mein phone number ho sakta hai – HIBP direct number nahi deta, lekin breach ka hint deta hai.
2. **Download the Relevant Database:**
   - **Sources:**
     - **DeHashed** (dehashed.com): Paid ($5/month) – email se breach search karo, full dump (phone, password) download karo.
     - **Dark Web/Torrents:** Breach data forums pe milta hai (e.g., RaidForums archives) – legal limits mein raho.
     - **Public Archives:** Kaggle, archive.org pe old leaks (LinkedIn 2012) free hote hain.
   - **Process:**
     (a) HIBP se breach naam lo (e.g., "Twitter 2022").
     (b) DeHashed pe email search karo – phone number mila: +919876543210.

- **Fayda:** Direct access to raw data – phone number email ke saath mil sakta hai.
- **Note:** Data hashed ho sakta hai – passwords crack karne ke liye Hashcat chahiye (ethical use only).

3. **Search Specific Leaks (Facebook, Snapchat, Database Leaks):**
   - **Facebook Leak (2021):**
     - 533M users – phone numbers, emails leaked.
     - **Kaise Check Karein:**
       * HIBP pe email ya phone (+919876543210) daalo – "Facebook 2021" breach mein hai ya nahi pata chalega.
       * Full dump torrent pe available hai – email se phone match karo.
     - **Output:** rishi.kabra@gmail.com → +919876543210.
   - **Snapchat Leak (2014):**
     - 4.6M usernames, phone numbers leaked.
     - **Kaise Karein:**
       * HIBP pe email check karo ya Snapchat dump (publicly circulated) mein username (rishi_kabra) search karo.
       * Result: +91728484XX (last 2 digits obfuscated).
   - **Generic Database Leaks:**
     - **LeakPeek/Snusbase:** Paid tools – name, email, password se search karo, phone milega.
     - **CyberNews Leak Checker:** Free – email/phone se breaches dekho (cybernews.com/perso data-leak-check).

4. **Analyze and Extract Phone Number:**
   - Breach data mein email ke saath phone number hota hai – CSV ya text file mein search karo.
   - Example:
     - LinkedIn 2012 dump: "rishi.kabra@gmail.com, +919876543210, hashed_pass".
   - Tool: Excel ya grep (Linux) se filter karo – "rishi.kabra" search karke number lo.

5. **Save and Verify:**
   - Notion mein table banao:

Email	Phone Number	Breach	Source
rishi.kabra@gmail	+919876543210	LinkedIn 2012	DeHashed

   - **Verify:** Number ko WhatsApp pe check karo – profile pic ya status se identity confirm ho sakti hai.

Workflow Example:

- **Email:** "satyam.singh@gmail.com"

- **HIBP:** Breaches – Twitter 2022, Canva 2019.
- **Download:** Twitter 2022 dump (DeHashed) – satyam.singh@gmail.com → +919123456789.
- **Specific Leak:** Facebook 2021 – same number mila.
- **Conclusion:** Satyam ka number +919123456789 hai – multiple breaches se verified.

Extra Tips:

- **Cross-Check:** Ek breach se mila number doosre mein confirm karo – consistency zaroori.
- **Search Operators:** Google pe `"satyam singh +919123456789"` try karo – public mention mil sakta hai.
- **Safety:** VPN use karo – leak sites risky hote hain. Ethical use ke liye permission lo.
- **Expand:** Number mila to Epieos (tools.epieos.com) ya SignalHire (signalhire.com) se aur accounts dhoondho.

Tables

Task	Method	Output
Breach Check	HIBP	Breach List
Data Download	DeHashed	Phone Number
Specific Leaks	Facebook/Snapchat	Linked Number

Table 40: Methods for Finding Phone Numbers in Leaks

Summary

- HIBP se breaches check karo – email se start.
- DeHashed ya torrents se data lo – phone extract karo.
- Notion mein save karo – leak info organize rakho.

Point To Note

Leaked databases mein phone numbers dhoondhne ke liye **name**, **email**, ya **password** se shuru karo – **Have I Been Pwned** (haveibeenpwned.com) pe email check karo, breached hai to data download karo (DeHashed, torrents). **Facebook leak (2021)**, **Snapchat leak (2014)**, ya generic leaks mein bhi search karo. Har breach se phone number extract karo aur Notion mein save karo – ye method target ke contact details ko deep digging se reveal karta hai, bas legal aur ethical limits mein raho!

==========

Uncovering Detailed Phone Number Info

Uncovering detailed phone number info ek essential phone number OSINT skill hai jo aapko ek phone number ke peeche chhupi general aur specific details tak pahunchne mein madad karta hai. **Phone number lookup** ke zariye aap number ke baare mein jaan sakte ho – jaise **number type** (mobile, landline, VOIP), **service provider** (carrier), **spam score** (risk level), aur **location** (geographical area). Ye process online tools aur databases ka use karta hai jo real-time ya archived data se info provide karte hain. Kuch trusted websites jaise **IPQualityScore** aur **International Numbering Plans** isme kaam aate hain – IPQualityScore free lookups deta hai, jabki International Numbering Plans global numbering details offer karta hai. Chalo is process ko step-by-step samajhte hain taaki aap phone number ke details ko pura uncover kar sako.

Why Uncover Phone Number Details?

- Phone numbers ek digital identity ka hissa hote hain – inke through aap target ke location, carrier, aur behavior (spam ya legit) ka pata laga sakte ho.
- Ye info fraud detection, contact verification, ya investigation ke liye critical hai – jaise pata karna ki number active hai ya risky.

Steps to Uncover Detailed Phone Number Info:

1. **Understand Phone Number Lookup Basics:**
   - Phone number lookup ek process hai jisme aap number ke attributes jaise **number type**, **service provider**, **spam score**, aur **location** extract karte ho.
   - Ye details carrier records, public data, aur user reports se aate hain.
2. **Use IPQualityScore for Free Phone Number Lookup:**
   - **Website: ipqualityscore.com** (ipqualityscore.com)
   - **Kya Hai:** IPQualityScore ek free phone number lookup tool hai jo mobile, landline, aur VOIP numbers ke details deta hai – 150+ countries mein coverage ke saath.
   - **Kaise Use Karein:**
     (a) IPQualityScore pe jao, "Free Phone Number Lookup" section mein number daalo (e.g., +919876543210).
     (b) Search karo – results mein ye milega:
     - **Number Type:** Mobile, Landline, ya VOIP.
     - **Service Provider:** Carrier name (e.g., Airtel, Verizon).
     - **Location:** City/State/Country (e.g., Mumbai, India).
     - **Spam Score:** Risk level (0-100) – high score matlab spam/fraud ka chance.
   - **Output Example:**
     - Number: +919876543210
     - Type: Mobile
     - Carrier: Airtel
     - Location: Mumbai, India
     - Spam Score: 10 (low risk).
   - **Fayda:** Free, real-time, aur API integration bhi available – bulk lookups ke liye perfect.

- **Note:** Advanced details (HLR status) ke liye paid plan chahiye.

3. **Leverage International Numbering Plans for Context:**
   - **Website: numberingplans.com** (numberingplans.com)
   - **Kya Hai:** Ye ek global resource hai jo international numbering plans, country codes, aur carrier info deta hai – telecom professionals ke liye designed.
   - **Kaise Use Karein:**
     (a) Numberingplans.com pe jao, "Number Analysis Tools" mein number daalo.
     (b) Results mein country code, region, aur carrier type ka breakdown milega.
   - **Output Example:**
     - Number: +12025550123
     - Country: USA (+1)
     - Region: California
     - Type: Landline
   - **Fayda:** Free basic analysis – numbering standards samajhne ke liye best.
   - **Note:** Detailed carrier info ya spam score nahi milta – supplementary tool hai.

4. **Combine Tools for Deeper Insights:**
   - IPQualityScore se **spam score** aur **location** lo, phir International Numbering Plans se **country code** aur **number type** confirm karo.
   - Agar number leaked hai, to **Have I Been Pwned** (haveibeenpwned.com) pe email se cross-check karo – phone number bhi breach mein mil sakta hai.

5. **Save and Analyze:**
   - Notion mein table banao:

Number	Type	Carrier	Location	Spam Score	Source
+919876543210	Mobile	Airtel	Mumbai, India	10	IPQualityScore
+12025550123	Landline	Verizon	California, USA	N/A	NumberingPlans

Workflow Example:

- **Number:** +971555123456
- **IPQualityScore:**
  - Type: Mobile
  - Carrier: Etisalat
  - Location: Dubai, UAE
  - Spam Score: 5 (low risk).
- **NumberingPlans:**

- Country: UAE (+971)
- Region: Dubai

- **Conclusion:** Number Dubai ka hai, Etisalat ka mobile, aur safe lagta hai.

Extra Tips:

- **Cross-Check:** IPQualityScore ke spam score ko Truecaller se verify karo – spam reports match karte hain to risk confirm hota hai.
- **Search Operators:** Google pe `"+971555123456"` search karo – public mentions se aur context mil sakta hai.
- **Expand:** Number mila to SignalHire (signalhire.com) se LinkedIn profile check karo – owner ka name ya job milega.
- **Safety:** VPN use karo – sensitive lookups ke liye precaution zaroori hai.

Tables

Tool	Features	Output
IPQualityScore	Spam Score, Carrier	Detailed Info
NumberingPlans	Country Code, Type	Basic Context

Table 41: Tools for Phone Number Lookup

Summary

- IPQualityScore se spam score, carrier lo.
- NumberingPlans se country, type confirm karo.
- Notion mein save karo – phone details organize rakho.

Point To Note

Phone number lookup se **number type**, **service provider**, **spam score**, aur **location** uncover karo – **IPQualityScore** (ipqualityscore.com) free mein real-time details deta hai, jabki **International Numbering Plans** (numberingplans.com) global context ke liye hai. Dono tools combine karke complete picture banao – har detail ko Notion mein save karo. Ye method phone number ke peeche ki story ko khol deta hai – bas systematic kaam karo aur free resources ka pura fayda uthao!

==========

Revealing Sensitive Info Using Advanced Search Techniques

Revealing sensitive info using advanced search techniques ek powerful OSINT method hai jo aapko phone numbers ke zariye sensitive details – jaise identity, location, ya linked accounts – uncover karne mein madad karta hai. Isme hum **search operators** ka use karte hain taaki pata lagaya ja sake ki ek phone number search engines (Google, Bing, etc.) mein **indexed** hai ya nahi. Phone numbers alag-alag formats mein online appear karte hain – jaise **international format** ("+ccxxxx...", "00ccxx...") ya local format ("xxx-xxx-xxx", "xxx..."). Yahan **cc** matlab country code (e.g., +91 for India), aur hum in variations ko target karenge. Ye technique public data – forums, directories, leaks – se info extract karti hai. Chalo is process ko step-by-step samajhte hain aur dekhte hain kaise sensitive info reveal hoti hai.

Why Use Advanced Search Techniques for Phone Numbers?

- Phone numbers aksar online posts, resumes, social profiles, ya breach dumps mein leak ho jate hain – search engines inko index karte hain.
- Search operators ke saath aap number ke mentions dhoondh sakte ho aur usse jude sensitive details (name, address, accounts) tak pahunch sakte ho.
- Ye method fast aur free hai – bas sahi format aur syntax ka use karna zaroori hai.

Steps to Reveal Sensitive Info Using Search Operators:

1. **Understand Phone Number Formats:**
   - Phone numbers alag-alag tarike se likhe jate hain – international ya local:
     - **International Format:**
       - **+ccxxxx...** (e.g., +919876543210) – Country code ke saath.
       - **00ccxx...** (e.g., 00919876543210) – Alternate international style.
     - **Local Format:**
       - **xxx...** (e.g., 9876543210) – Plain digits.
       - **xxx-xxx-xxx** (e.g., 987-654-3210) – Hyphenated.
   - **cc** = Country Code (e.g., +91 India, +1 USA, +44 UK).
2. **Use Search Operators to Check Indexing:**
   - **Basic Search:** Number ko quotes mein daal kar exact match dhoondho.
     - `"+919876543210"`
     - Result: "Contact Rishi Kabra: +919876543210" (forum post).
   - **Multiple Formats:** OR operator se variations cover karo:
     - `"+919876543210" OR "00919876543210" OR "9876543210" OR "987-654-3210"`
     - Result:
       - "+919876543210" – LinkedIn profile mention.
       - "9876543210" – Classified ad (e.g., "Rishi, Mumbai, 9876543210").
   - **Add Context:** Name ya city ke saath refine karo:
     - `"Rishi Kabra" "+919876543210" OR "9876543210"`
     - Result: "Rishi Kabra, TechMojo, Mumbai, +919876543210" (company directory).

3. **Refine with Advanced Operators:**

- **Site-Specific:** Specific platforms pe focus:
  - `"+919876543210" site:linkedin.com` – LinkedIn mentions.
  - `"9876543210" site:facebook.com` – FB posts ya groups.
- **Exclude Noise:** Irrelevant sites hatao:
  - `"+919876543210" -inurl:(instagram twitter)` – IG/Twitter ke alawa results.
- **Filetype Search:** Resumes ya docs mein number:
  - `"9876543210" filetype:pdf site:*.edu | site:*.org -inurl:login`
  - Result: "Rishi Kabra CV – 9876543210" (PDF on university site).
- **Country Code Focus:** Location refine karo:
  - `"+91" "9876543210" "Mumbai"` – India-specific hits.

4. **Uncover Sensitive Info:**

- Search results se ye details mil sakte hain:
  - **Name:** "Rishi Kabra" number ke saath.
  - **Location:** "Mumbai" ya "TechMojo office address".
  - **Accounts:** LinkedIn profile URL ya Twitter handle.
  - **Context:** "For sale: 9876543210" – ad se intent pata chalta hai.
- **Example Output:**
  - "+919876543210" → "Rishi Kabra, Mumbai, TechMojo, +919876543210" (directory).

5. **Save and Expand:**

- Notion mein table banao:

Number	Name	Location	Source	Sensitive Info
+919876543210	Rishi Kabra	Mumbai	LinkedIn	TechMojo employee

- **Expand:** Number se SignalHire (signalhire.com) pe LinkedIn check karo ya HIBP (haveibeenpwned.com) pe breach mein phone verify karo.

Workflow Example:

- **Number:** +971555123456
- **Search:** `"+971555123456" OR "00971555123456" OR "555123456" OR "555-123-456"`
  - Result:
    - "+971555123456" – "Saad Sarraj, Dubai, Contact: +971555123456" (business listing).
    - "555123456" – "Saad, UAE, 555123456" (forum).
- **Refined:** `"Saad Sarraj" "+971555123456" site:linkedin.com`

– Result: linkedin.com/in/saadsarraj – phone confirmed.

- **Conclusion:** Saad ka number Dubai se hai, LinkedIn se linked.

Extra Tips:

- **Country Codes:** Location pata hai to cc add karo – +91, +1, +44 se refine hota hai.
- **Cross-Check:** Number mila to IPQualityScore (ipqualityscore.com) pe carrier/location verify karo.
- **Pastebin:** `"+971555123456" site:pastebin.com` – breach dumps mein check karo.
- **Safety:** VPN use karo – sensitive searches ke liye precaution zaroori.

Tables

Operator	Use	Output
"..."	Exact Match	Direct Mentions
site:	Platform Focus	Specific Hits
filetype:	Docs/Resumes	Detailed Context

Table 42: Search Operators for Sensitive Info

Summary

- Formats vary karo – +ccxxxx, xxx-xxx-xxx.
- Operators se name, location lo – public data extract karo.
- Notion mein save karo – sensitive info organize rakho.

Point To Note

Advanced search techniques se phone numbers ko **international format** ("+ccxxxx...", "00ccxx...") ya local format ("xxx-xxx-xxx", "xxx...") mein search karo – `"+919876543210" OR "9876543210"` jaise operators se indexing check karo. Results se sensitive info – name, location, accounts – uncover hoti hai. Har detail ko Notion mein save karo – ye method public data se phone number ki story khol deta hai, bas formats ka dhyan rakho aur systematically kaam karo!

==========

Uncovering the Identity Behind a Phone Number

Uncovering the identity behind a phone number ek essential OSINT technique hai jo aapko unknown callers ki pehchaan karne mein madad karta hai. **Caller ID identifiers** jaise **Truecaller**, **Sync.ME**, aur **Numlookup** phone numbers ke peeche chhupi identity – jaise name, location, ya spam status – reveal karte hain, taaki aap spam calls ko block kar sako.

Ye tools real-time data aur crowdsourced info ka use karte hain, aur inka fayda ye hai ki ye **international numbers** pe bhi kaam karte hain – chahe number India (+91), USA (+1), ya UAE (+971) se ho. Chalo in tools ko detail mein samajhte hain aur dekhte hain kaise ye caller identity uncover karte hain.

Why Uncover Caller Identity?

- Unknown calls irritating hote hain – spam, scams, ya telemarketers se bachne ke liye caller ka identity jaanna zaroori hai.
- Caller ID tools aapko power dete hain – call pick karne se pehle decide karo ki worth hai ya nahi.

Caller ID Identifiers:

1. **Truecaller**
   - **Kya Hai:** Truecaller ek globally popular caller ID app hai jo 450M+ users ke crowdsourced data se numbers identify karta hai – spam blocking aur reverse lookup ke liye best.
   - **Kaise Use Karein:**
     (a) Truecaller.com pe jao (truecaller.com) ya app download karo.
     (b) Number daalo (e.g., +919876543210).
     (c) Result dekho – name, location, spam reports.
   - **Output Example:**
     – Number: +919876543210
     – Name: Rishi Kabra
     – Location: Mumbai, India
     – Status: Low spam risk.
   - **International Support:** Haan – USA, India, UK, sabhi countries ke numbers pe kaam karta hai.
   - **Fayda:** Free mein basic lookup, premium ($2.99/month) mein ads-free aur extra features.
   - **Note:** Accuracy community data pe depend karta hai.
2. **Sync.ME**
   - **Kya Hai:** Sync.ME ek caller ID aur spam blocker hai jo social media sync aur reverse lookup offer karta hai – 1B+ numbers ka database.
   - **Kaise Use Karein:**
     (a) Sync.me pe number search karo (sync.me) (e.g., +12025550123).
     (b) Result mein name, photo, aur social profiles milenge.
   - **Output Example:**
     – Number: +12025550123
     – Name: John Doe
     – Linked: Facebook profile.
   - **International Support:** Haan – global numbers pe kaam karta hai, lekin US/UK mein zyada effective.

- **Fayda:** Free basic lookup, social media integration se identity strong hoti hai.
- **Note:** Full details ke liye premium chahiye ($4.99/month).

3. **Numlookup**

- **Kya Hai:** Numlookup ek simple, free reverse lookup tool hai jo caller name, carrier, aur location deta hai – no signup needed.
- **Kaise Use Karein:**
  (a) Numlookup.com pe jao (numlookup.com), number daalo (e.g., +971555123456).
  (b) Search karo – instant result milega.
- **Output Example:**
  - Number: +971555123456
  - Name: Saad Sarraj
  - Carrier: Etisalat
  - Location: Dubai, UAE.
- **International Support:** Haan – worldwide numbers cover karta hai.
- **Fayda:** Completely free, fast, aur privacy-friendly – data store nahi karta.
- **Note:** Limited to basic info – deep details nahi milte.

Workflow Example:

- **Number:** +919876543210
- **Truecaller:** Rishi Kabra, Mumbai, India.
- **Sync.ME:** Rishi Kabra, LinkedIn profile linked.
- **Numlookup:** Rishi Kabra, Airtel, Mumbai.
- **Conclusion:** Number Rishi ka hai – teeno tools se confirmed.

Extra Tips:

- **Cross-Check:** Ek tool se mila name doosre pe verify karo – accuracy badhegi.
- **International Numbers:** Country code (+cc) zaroor daalo – +91, +1, +44 ke saath search karo.
- **Save:** Notion mein table banao:

Number	Name	Location	Source
+919876543210	Rishi Kabra	Mumbai, India	Truecaller

Finding the Caller ID in the US

Finding the caller ID in the US ke liye **people search engines** ek shandaar tareeka hain jo individuals ki info – jaise name, address, phone number – dhoondhne mein madad karte hain. Ye websites specially **US residents** ke liye limited hote hain aur public records, directories, aur social data ka use karte hain. Inka focus US-specific data pe hota hai, to agar aapko American callers ki identity chahiye, to ye tools perfect hain. Chalo is process ko samajhte hain aur US-focused caller ID kaise uncover karte hain dekhte hain.

Why Use People Search Engines for US Caller ID?

- US mein phone numbers aksar public records (voter lists, property records) ya online directories mein hote hain – inko tap karke caller ID mil sakta hai.
- Ye tools US residents pe focused hain – international numbers pe kaam nahi karte, lekin US ke liye deep info dete hain.

People Search Engines (US-Specific):

1. **Whitepages**
   - **Kya Hai:** Whitepages US ka leading people search engine hai jo phone numbers se name, address, aur background info deta hai.
   - **Kaise Use Karein:**
     (a) Whitepages.com pe jao (whitepages.com), number daalo (e.g., +12025550123).
     (b) Free result mein basic info milega.
   - **Output Example:**
     – Number: +12025550123
     – Name: John Doe
     – Address: 123 Main St, San Francisco, CA
     – Carrier: Verizon.
   - **Fayda:** Free mein name/location, premium ($5/month) mein criminal records bhi.
   - **Note:** Sirf US residents ke liye – international numbers nahi.
2. **Spokeo**
   - **Kya Hai:** Spokeo ek US-focused search engine hai jo phone numbers se social profiles, addresses, aur relatives tak info deta hai.
   - **Kaise Use Karein:**
     (a) Spokeo.com pe number search karo (spokeo.com) (e.g., +13105550123).
     (b) Result mein detailed profile milega.
   - **Output Example:**
     – Number: +13105550123
     – Name: Jane Smith
     – Location: Los Angeles, CA
     – Social: LinkedIn, Facebook linked.
   - **Fayda:** Free basic lookup, paid ($2.50/month) mein full report.
   - **Note:** US-only – global coverage nahi.

3. **TruePeopleSearch**

- **Kya Hai:** Ye ek free US people search tool hai jo phone numbers se name, address, aur family details deta hai.
- **Kaise Use Karein:**
  (a) Truepeoplesearch.com pe number daalo (truepeoplesearch.com) (e.g., +12125550123).
  (b) Search karo – instant result.
- **Output Example:**
  - Number: +12125550123
  - Name: Mike Johnson
  - Address: 456 Oak St, New York, NY.
- **Fayda:** 100% free, no signup needed – US data pe strong.
- **Note:** Limited to US – bahar ke numbers pe blank.

Workflow Example:

- **Number:** +12025550123
- **Whitepages:** John Doe, San Francisco, CA.
- **Spokeo:** John Doe, LinkedIn profile linked.
- **TruePeopleSearch:** John Doe, 123 Main St, SF.
- **Conclusion:** John ka US number hai – address aur identity confirmed.

Extra Tips:

- **US Focus:** Ye tools US public records pe kaam karte hain – international numbers ke liye Truecaller ya Numlookup try karo.
- **Cross-Check:** Ek site se mila data doosre pe verify karo – mistakes kam honge.
- **Save:** Notion mein table banao:

Number	Name	Address	Source
+12025550123	John Doe	123 Main St, SF, CA	Whitepages

Tables

Summary

- Truecaller, Sync.ME – global caller ID lo.
- Whitepages, Spokeo – US-specific deep info nikalo.
- Notion mein save karo – identity organize rakho.

Tool	Scope	Output
Truecaller	International	Name, Location
Sync.ME	International	Name, Social Links
Numlookup	International	Name, Carrier
Whitepages	US-Only	Name, Address
Spokeo	US-Only	Name, Social Profiles
TruePeopleSearch	US-Only	Name, Address

Table 43: Comparison of Caller ID Tools

Point To Note

Uncovering identity ke liye **Truecaller** (truecaller.com), **Sync.ME** (sync.me), aur **Numlookup** (numlookup.com) international numbers pe kaam karte hain – inke saath spam block aur basic ID milta hai. **US caller ID** ke liye **Whitepages** (whitepages.com), **Spokeo** (spokeo.com), aur **TruePeopleSearch** (truepeoplesearch.com) best hain – ye US residents ke detailed info dete hain. Har tool ke results ko Notion mein save karo – ye phone number ke peeche ki kahani ko khol deta hai, chahe global ho ya US-specific! Systematic kaam karo aur sahi tool chuno.

==========

Uncovering Accounts Registered with a Phone Number

Uncovering accounts registered with a phone number ek valuable phone OSINT technique hai jo aapko ye pata lagane mein madad karta hai ki ek phone number kahan-kahan online registered hai – social media, professional platforms, ya doosre websites pe. Kuch **phone OSINT tools** is process ko automate karte hain aur ek number ke saath linked accounts ko list kar dete hain. Isme hum **Epieos**, **OSINT Industries**, aur **Castrick** jaise tools explore karenge, jo phone numbers ke digital footprint ko track karte hain. Saath hi, **SignalHire browser extension** ke zariye aap phone number ya email se **LinkedIn accounts** bhi dhoondh sakte ho. Ye tools international numbers pe bhi kaam karte hain aur real-time data dete hain. Chalo step-by-step dekhte hain kaise ye tools phone number se registered accounts uncover karte hain.

Why Uncover Accounts with a Phone Number?

- Phone numbers aksar multiple platforms pe ek unique identifier hote hain – inke through aap target ke online presence (Twitter, LinkedIn, WhatsApp) aur identity tak pahunch sakte ho.
- Ye info verification, networking, ya investigation ke liye useful hai – jaise pata karna ki number kahan active hai.

Phone OSINT Tools:

1. **Epieos (tools.epieos.com/phone.php)**
   - **Kya Hai:** Epieos ek free OSINT tool hai jo phone numbers se linked accounts dhoondhta hai – Google, Telegram, Skype, WhatsApp, aur 150+ sites check karta hai.
   - **Kaise Use Karein:**

(a) Epieos ke phone lookup page pe jao (tools.epieos.com/phone.php).

(b) Number daalo (e.g., +919876543210) aur captcha solve karo.

(c) Search karo – results mein registered platforms aur usernames milenge.

- **Output Example:**
  - Number: +919876543210
  - Accounts: Google (Rishi Kabra), Telegram (@rishi_k), WhatsApp (active).
- **Fayda:** Free, broad coverage, aur social media focus – international numbers pe strong.
- **Note:** Premium ($29/month) mein extra details (e.g., profile pics) milte hain.

2. **OSINT Industries (osint.industries)**

- **Kya Hai:** Ye ek paid investigation platform hai jo phone numbers aur emails se 300+ websites pe accounts track karta hai – real-time accuracy ke liye known hai.
- **Kaise Use Karein:**

(a) Osint.industries pe account banao (starting $49/month).

(b) Phone number input karo (e.g., +12025550123).

(c) Results mein linked sites aur metadata milta hai.

- **Output Example:**
  - Number: +12025550123
  - Accounts: Twitter (@john_doe), LinkedIn, Amazon.
- **Fayda:** 200+ modules, JSON export – deep dives ke liye perfect.
- **Note:** Free nahi hai – budget tool hai, lekin powerful.

3. **Castrick (castrick.toolforge.org)**

- **Kya Hai:** Castrick ek newer, free OSINT tool hai jo phone numbers, emails, ya usernames se social media accounts dhoondhta hai – Epieos jaisa lekin lightweight.
- **Kaise Use Karein:**

(a) Castrick pe jao (castrick.toolforge.org), number daalo (e.g., +971555123456).

(b) Search karo – linked platforms list honge.

- **Output Example:**
  - Number: +971555123456
  - Accounts: Instagram (@saad_dubai), Facebook.
- **Fayda:** Free, simple, aur beginner-friendly – no signup needed.
- **Note:** Coverage limited hai – major platforms pe focus.

4. **SignalHire Browser Extension (signalhire.com)**

- **Kya Hai:** SignalHire ek Chrome/Firefox extension hai jo phone numbers ya emails se LinkedIn accounts dhoondhta hai – 400M+ profiles ka database.
- **Kaise Use Karein:**

(a) Extension install karo (signalhire.com) (Chrome Web Store se).

(b) SignalHire icon pe click karo, number daalo (e.g., +919876543210).

(c) "Find Profile" dabao – LinkedIn URL milega.

- **Output Example:**
  - Number: +919876543210
  - LinkedIn: linkedin.com/in/rishi-kabra
- **Fayda:** Free mein 5 credits/month, 96% hit rate – LinkedIn ke liye best.
- **Note:** Paid ($49/month) mein unlimited searches – bulk export bhi.

Workflow Example:

- **Number:** +919876543210
- **Epieos:** Google (Rishi Kabra), WhatsApp (active).
- **OSINT Industries:** Twitter (@rishi_k), Amazon registered.
- **Castrick:** Instagram (@rishi_kabra).
- **SignalHire:** LinkedIn (linkedin.com/in/rishi-kabra).
- **Conclusion:** Number 4+ platforms pe active hai – Rishi Kabra ka identity clear.

Extra Tips:

- **Cross-Check:** Ek tool se mila account doosre pe verify karo – consistency zaroori.
- **Country Code:** International format (+cc) use karo – +91, +1, +971 ke saath search accurate hota hai.
- **Expand:** LinkedIn mila to username (rishi-kabra) se Sherlock chalao – aur sites dhoondho.
- **Save:** Notion mein table banao:

Number	Accounts	Tool
+919876543210	LinkedIn, WhatsApp, Twitter	SignalHire, Epieos

Tables

Tool	Scope	Output
Epieos	150+ Sites	Social Accounts
OSINT Industries	300+ Websites	Deep Data
Castrick	Major Platforms	Basic Links
SignalHire	LinkedIn	Profile URL

Table 44: Phone OSINT Tools Comparison

Summary

- Epieos, Castrick – free social accounts lo.
- OSINT Industries – paid deep dive karo.
- SignalHire se LinkedIn nikalo – Notion mein save karo.

Point To Note

Phone OSINT tools jaise **Epieos** (tools.epieos.com/phone.php), **OSINT Industries** (osint.industries), aur **Castrick** (castrick.toolforge.org) phone numbers se registered accounts (Google, Twitter, Instagram) dhoondhte hain – Epieos free hai, OSINT Industries deep data deta hai, aur Castrick simple hai. **SignalHire extension** (signalhire.com) LinkedIn accounts ke liye perfect hai – number ya email se profile turant milta hai. Har tool ke results ko Notion mein save karo – ye method phone number ke online presence ko pura khol deta hai, bas systematic kaam karo aur international formats ka dhyan rakho!

==========

Discovering Leaked Info Linked to a Phone Number

Discovering leaked info linked to a phone number ek advanced OSINT technique hai jo aapko phone number ke saath jude **data breaches aur leaks** ko identify karne aur usse related sensitive information – jaise name, email, passwords – uncover karne mein madad karta hai. Is process mein hum breaches ko track karte hain, relevant **leaked databases** download karte hain, aur additional info ke liye search karte hain. **Have I Been Pwned (HIBP)** sirf email search allow karta hai aur phone number se direct lookup nahi deta, isliye hum **DeHashed** jaise tools ka use karenge, jo phone number-based searches support karta hai. Saath hi, social media leaks – jaise **Facebook data leak** – ke liye quick check karne ke liye **HaveIBeenZuckered.com** ka use karenge. Chalo step-by-step samajhte hain kaise phone number se leaked info dhoondhi jati hai.

Why Discover Leaked Info Linked to a Phone Number?

- Phone numbers breaches mein aksar emails, usernames, aur passwords ke saath leak hote hain – ye info identity theft ya account takeover ke liye use ho sakti hai.
- Leaked data se aap target ke digital footprint aur compromised details tak pahunch sakte ho – investigation ya security ke liye critical.

Steps to Discover Leaked Info:

1. **Identify Data Breaches/Leaks with DeHashed:**
   - **Tool: DeHashed** (dehashed.com)
   - **Kya Hai:** DeHashed ek powerful search engine hai jo hacked databases mein **name**, **phone number**, aur **email** ke basis pe search karne deta hai – 10B+ records ka access deta hai. Subscription ke bina bhi basic search free mein possible hai.
   - **Kaise Use Karein:**
     (a) Dehashed.com pe jao, "Search" bar mein phone number daalo (e.g., +919876543210).

(b) Filter lagao – "Phone" select karo taaki sirf phone-related results aayein.

(c) Results mein breaches list honge jahan number mila – jaise "LinkedIn 2012", "Twitter 2022".

- **Output Example:**
  - Number: +919876543210
  - Breaches:
    - LinkedIn 2012: Email (rishi.kabra@gmail.com), Phone (+919876543210).
    - Twitter 2022: Phone (+919876543210), Username (@rishi_kabra).
- **Fayda:** Aapko pata chalega ki phone number kis-kis database mein leak hua – subscription ke bina bhi breach names milte hain.
- **Note:** Full data (passwords, addresses) ke liye $5/month subscription chahiye – lekin breach identify karne ke liye free version kaafi hai.

2. **Download Relevant Data Leaks/Breaches:**

- **Process:**
  - DeHashed se breach ka naam lo (e.g., "Twitter 2022").
  - Free Sources:
    - **Archive.org** (archive.org) ya **Kaggle** pe old leaks (LinkedIn 2012) search karo – "LinkedIn 2012 leak download".
    - Torrent sites pe breach dumps mil sakte hain (legal limits mein raho).
  - Paid Sources:
    - **DeHashed:** Subscription ke saath full dump download karo – CSV mein phone, email, passwords milenge.
- **Example:**
  - Twitter 2022 dump download kiya – "rishi.kabra@gmail.com, +919876543210, hashed_pass".
- **Note:** Data encrypted ho sakta hai – passwords crack karna illegal ho sakta hai, ethical use karo.

3. **Search for Additional Info:**

- **Database Analysis:**
  - Downloaded CSV mein phone number search karo (Ctrl+F) – linked email, username, ya address milega.
  - Example: "+919876543210" se "rishi.kabra@gmail.com" aur "@rishi_kabra" mila.
- **Expand:**
  - **Sherlock:** Username (@rishi_kabra) se 400+ sites pe accounts dhoondho.
  - **Google:** `"+919876543210" OR "9876543210"` – public mentions lo (forums, directories).

4. **Quick Check for Social Media Data Leaks (Facebook Leak):**

- **Tool: HaveIBeenZuckered.com** (haveibeenzuckered.com)
- **Kya Hai:** Ye ek free, privacy-focused website hai jo **Facebook 2021 data leak** (533M users) mein phone numbers check karta hai – input store nahi karta, instant result deta hai.

- **Kaise Use Karein:**
  (a) HaveIBeenZuckered.com pe jao.
  (b) Phone number daalo (e.g., +971555123456).
  (c) "Check" karo – agar number leak mein hai, to "Found in breach" dikhega.
- **Output Example:**
  – Number: +971555123456
  – Result: "This number was found in the Facebook data breach."
- **Fayda:** Quick aur free – Facebook leak (phone numbers, names) check karne ka fastest tareeka.
- **Note:** Sirf 2021 breach cover karta hai – doosre leaks ke liye DeHashed use karo.

5. **Save and Verify:**
   - Notion mein table banao:

Number	Breach	Linked Info	Source
+919876543210	LinkedIn 2012	rishi.kabra@gmail	DeHashed
+971555123456	Facebook 2021	Saad Sarraj	HaveIBeenZuckered

   - **Verify:** Number ko Truecaller ya WhatsApp pe check karo – name ya profile se confirm karo.

Workflow Example:

- **Number:** +919876543210
- **DeHashed:**
  – Breaches: Twitter 2022, LinkedIn 2012.
  – Info: rishi.kabra@gmail.com, @rishi_kabra.
- **Download:** Twitter 2022 dump – +919876543210, "Rishi Kabra".
- **HaveIBeenZuckered:** Not in Facebook leak.
- **Conclusion:** Number 2 breaches mein mila – Twitter aur LinkedIn se info confirmed.

Extra Tips:

- **HIBP Limitation:** HIBP phone search nahi deta – email se breach check karke phone linked hai ya nahi guess karo.
- **Cross-Check:** DeHashed se mila data HaveIBeenZuckered ya social media pe verify karo.
- **Safety:** VPN use karo – leak sites ya downloads risky ho sakte hain.
- **Expand:** Leaked email se SignalHire (signalhire.com) pe LinkedIn lo – aur details nikalo.

Tool	Scope	Output
DeHashed	All Breaches	Breach List, Data
HaveIBeenZuckered	Facebook 2021	Quick Leak Check

Table 45: Tools for Discovering Leaked Info

Tables

Summary

- DeHashed se breaches lo – phone se start.
- HaveIBeenZuckered se FB leak check karo.
- Notion mein save karo – leaked data organize rakho.

Point To Note

Leaked info dhoondhne ke liye **DeHashed** (dehashed.com) se phone number (+919876543210) ke breaches (LinkedIn, Twitter) identify karo – subscription bina bhi breach names milte hain, phir data download karo. **HaveIBeenZuckered.com** (haveibeenzuckered.com) se **Facebook leak** quick check karo – time save hota hai. Additional info ke liye Google, Sherlock use karo – har detail Notion mein save karo. Ye method phone number ke compromised data ko pura khol deta hai – ethical aur legal limits mein kaam karo!

==========

Deep Phone Number Scanning and Footprinting

Deep phone number scanning and footprinting ek advanced OSINT approach hai jo phone numbers ke peeche chhupi detailed information ko uncover karne ke liye use hota hai. **PhoneInfoga** ek powerful open-source tool hai jo is process ko simplify karta hai – ye phone numbers ke baare mein basic se lekar advanced details tak gather karta hai. Iske **features** mein number ki validity check karna, basic info (country, carrier) collect karna, aur reputation reports (spam ya fraud ka status) dhoondhna shamil hai. Ye tool **GitHub** se install kiya ja sakta hai aur international numbers – including Indian numbers – pe kaam karta hai. Chalo is tool ko detail mein samajhte hain – ye kya info deta hai, Indian citizens ke liye kitna helpful hai, aur overall iski usefulness kya hai.

What is PhoneInfoga?

- **PhoneInfoga** ek Python/Go-based OSINT framework hai jo phone numbers ke liye information gathering aur footprinting ke liye banaya gaya hai. Iska goal free resources ka use karke maximum data extract karna hai – jaise search engines, public APIs, aur phone directories.
- Ye tool originally Python mein tha, lekin ab Go language mein rewritten hai (v2), jo isko faster aur maintainable banata hai.
- Developer: Sundowndev (GitHub: sundowndev/PhoneInfoga).

Key Features of PhoneInfoga:

1. **Check If Phone Number is Valid:**
   - Numverify API ke through check karta hai ki number valid hai ya nahi – yani active hai, registered hai, ya possible hai.
   - Output: "Valid: True/False", "Line Type: Mobile/Landline/VOIP".
2. **Gather Basic Info:**
   - Country code, area, carrier (e.g., Airtel, Jio), aur line type jaise standard details deta hai.
   - Example: +919876543210 → Country: India, Carrier: Airtel, Type: Mobile.
3. **Check for Reputation Reports:**
   - External APIs aur OSINT sources se reputation data collect karta hai – jaise spam reports, scam complaints, ya disposable number status.
   - Footprints search engines (Google Dorks) pe dhoondhta hai – scam ya social media mentions mil sakte hain.
4. **Additional Capabilities:**
   - OVH Telecom API se VOIP provider check karta hai (Europe-focused).
   - OSINT reconnaissance – search engine results, phone books, social media links.
   - Custom formatting support – number ko alag-alag styles mein search karke accuracy badhata hai (e.g., "+919876543210" ya "987-654-3210").

Installation from GitHub:

- **Steps to Install (Linux/MacOS/Termux):**
  1. GitHub se clone karo:

```
git clone https://github.com/sundowndev/PhoneInfoga
```

  2. Directory mein jao:

```
cd PhoneInfoga
```

  3. Dependencies install karo (Python version ke liye):

```
python3 -m pip install -r requirements.txt
```

  4. Tool chalao:

```
python3 phoneinfoga.py -n "+919876543210" --osint
```

- **Docker Option:**
  - Docker image pull karo:

```
docker pull sundowndev/phoneinfoga:latest
```

  - Run karo:

```
docker run -it sundowndev/phoneinfoga scan -n "
   +919876543210"
```

- **Note:** Windows users ke liye direct binary nahi hai – WSL ya VM use karna padega. Go version ke binaries GitHub releases pe mil sakte hain (github.com/sundowndev/PhoneInfoga).

What Info Does PhoneInfoga Provide?

- **Basic Info:**
  - Country: India (+91)
  - Carrier: Jio, Airtel, Vodafone
  - Line Type: Mobile, Landline, VOIP
  - Location: Area code se approximate region (e.g., 987 Punjab).
- **Reputation Reports:**
  - Spam Score: User reports ya scam complaints (e.g., "Reported as telemarketer").
  - Disposable Check: Number temporary hai ya nahi.
- **Footprints:**
  - Google Search: "+919876543210" ke mentions – forums, ads, ya social media.
  - Social Links: Agar number public profile mein hai (e.g., WhatsApp, Telegram).
- **Example Output:**
  - Number: +919876543210
  - Valid: True
  - Country: India
  - Carrier: Airtel
  - Type: Mobile
  - Footprints: "Found in scam report on xyzforum.com".

Is PhoneInfoga Helpful for Indian Citizens?

- **Yes, It's Helpful:**
  - **Indian Numbers Support:** +91 country code ke saath kaam karta hai – Jio, Airtel, BSNL jaise carriers identify karta hai.
  - **Spam Detection:** India mein telemarketing aur scam calls common hain – reputation reports se inko spot karna asaan hai.
  - **Local Relevance:** Area codes (e.g., 987 Punjab, 982 Maharashtra) se approximate location milta hai, jo Indian context mein useful hai.
- **Limitations for India:**
  - Numverify ya OVH jaise APIs Indian carriers pe fully accurate nahi ho sakte – data crowdsourced hai.
  - Google footprints Indian sites pe kam indexed hote hain – results limited ho sakte hain.
  - Privacy laws (IT Act, 2000) ke wajah se public data kam available hai compared to US/Europe.

Is This Tool Really Helpful Overall?

- **Pros:**
  - **Free & Open-Source:** GitHub pe available, koi cost nahi – Indian users ke liye budget-friendly.
  - **International Scope:** US (+1), UK (+44), ya India (+91) – sabhi numbers pe kaam karta hai.
  - **Multi-Purpose:** Basic info se lekar deep footprinting tak – investigators, pen-testers, ya curious individuals ke liye kaam ka.
  - **Customizable:** Advanced users custom scanners add kar sakte hain.
- **Cons:**
  - **Accuracy:** Data free sources (Numverify, Google) pe depend karta hai – 100% verified nahi hota (tool khud disclaim karta hai).
  - **Setup:** Non-tech users ke liye installation (Python, Docker) tricky ho sakta hai.
  - **Limited Real-Time Tracking:** Live location ya owner tracking nahi karta – sirf public/OSINT data deta hai.
- **Usefulness Verdict:**
  - **Indian Citizens:** Moderately helpful – spam calls check karne ya basic info ke liye kaam ka, lekin deep info ke liye Indian context mein limited.
  - **Global Users:** Very helpful – especially US/EU jahan public data zyada hai.
  - **Overall:** Investigators ya tech-savvy logon ke liye ek solid starting point hai – lekin standalone complete solution nahi.

Workflow Example:

- **Number:** +919876543210
- **Command:** `phoneinfoga scan -n "+919876543210" --osint`
- **Output:**
  - Valid: True
  - Carrier: Airtel
  - Location: Punjab, India
  - Reputation: "3 spam reports on truecaller.com".
  - Footprints: "Mentioned in job ad on naukri.com".
- **Conclusion:** Number active hai, Airtel ka hai, aur job-related context mila.

Extra Tips:

- **Indian Context:** Number ko Truecaller pe cross-check karo – PhoneInfoga ke saath complement karta hai.
- **Save Results:** Notion mein table banao:
- **Ethics:** India mein privacy laws strict hain – personal use ke liye permission lo.

Number	Carrier	Location	Reputation	Source
+919876543210	Airtel	Punjab	3 spam reports	PhoneInfoga

Feature	Source	Output
Validity	Numverify API	True/False
Basic Info	Public APIs	Carrier, Location
Reputation	OSINT Sources	Spam Reports

Table 46: PhoneInfoga Features Overview

Tables

Summary

- PhoneInfoga se validity, carrier lo.
- Reputation aur footprints check karo.
- Notion mein save karo – data organize rakho.

Point To Note

PhoneInfoga ek versatile tool hai jo **deep phone number scanning aur footprinting** ke liye banaya gaya hai – validity, basic info, aur reputation reports deta hai. GitHub (github.com/sundowndev/PhoneInfoga) se install karke aap isse international numbers, including Indian (+91), pe use kar sakte ho. **Indian citizens** ke liye ye spam detection aur basic lookup ke liye helpful hai, lekin deep info mein thoda limited hai. Globally, ye OSINT enthusiasts ke liye ek strong tool hai – free, flexible, aur effective, lekin accuracy aur setup ke challenges hain. Systematic use karo, results verify karo, aur ethical boundaries mein raho – tab ye sach mein kaam ka hai!

==========

Gathering Profile Images for OS INT Investigations

Image OSINT mein tum seekhoge ki kaise ek image ya picture ke baare mein info find karna hai—jaise metadata (EXIF data) se location, date, ya device details extract karna tools jaise ExifTool ke saath. Online accounts se unique profile pictures download karna hai, manually ya automated tools/extensions (jaise DownAlbum) ke through, lekin platform ke terms of service ka dhyan rakhna zaroori hai. Aur in pictures ko use karke related accounts dhundna hai—reverse image search tools jaise Google Images, TinEye, ya Yandex se similar ya exact matches track karna, aur advanced cases mein facial recognition tools (jaise PimEyes) se identity ya cross-platform presence confirm karna, privacy laws ko follow karte hue. Ye techniques OSINT investigations mein profiles ko link karne aur deeper insights paane ke liye powerful hain.

Why Gather Profile Images for OSINT?

- Images metadata carry kar sakti hain—location, date, device info—jo investigations ke liye critical clues deti hain.

- Profile pictures online accounts ko link karne aur identities confirm karne mein madad karti hain—cross-platform presence track karna asaan hota hai.
- Reverse image search aur facial recognition se deeper insights milte hain—target ke digital footprint ko expand karne ke liye useful.

Steps to Gather Profile Images and Info:

1. **Extract Metadata from Images:**
   - **Tool:** ExifTool (exiftool.org)
   - **Kya Hai:** Ye ek open-source tool hai jo image files se EXIF data (location, date, camera model) extract karta hai.
   - **Kaise Use Karein:**
     (a) ExifTool install karo (Linux: `sudo apt install exiftool`).
     (b) Command chalao: `exiftool image.jpg`
     (c) Output check karo—GPS coordinates, timestamp, device info.
   - **Output Example:**
     – File: profile.jpg
     – GPS: 19.0760° N, 72.8777° E (Mumbai)
     – Date: 2023-05-15
     – Device: iPhone 12.
   - **Fayda:** Free aur detailed—location ya timeline banane mein madad karta hai.
   - **Note:** Social media images aksar metadata strip kar dete hain—original files pe kaam karta hai.
2. **Download Profile Pictures from Online Accounts:**
   - **Manual Method:** Right-click karke "Save Image As" se download karo—Twitter, LinkedIn, Instagram se.
   - **Automated Tool:** DownAlbum (chrome.google.com/webstore)
   - **Kya Hai:** Ye ek Chrome extension hai jo social media se bulk images download karta hai.
   - **Kaise Use Karein:**
     (a) Extension install karo.
     (b) Profile page pe jao (e.g., instagram.com/user), DownAlbum icon click karo.
     (c) "Download" select karo—profile pic save ho jayega.
   - **Note:** Platform ke terms of service check karo—scraping restricted ho sakta hai.
3. **Reverse Image Search to Find Related Accounts:**
   - **Tools:** Google Images (images.google.com), TinEye (tineye.com), Yandex (yandex.com/images)
   - **Kya Hai:** Ye tools image upload karke online similar ya exact matches dhoondhte hain—accounts ya mentions track karte hain.
   - **Kaise Use Karein:**
     (a) Website pe jao, image upload karo (e.g., profile.jpg).

(b) Search karo—results mein matching URLs ya pages milenge.

- **Output Example:**
  - Image: profile.jpg
  - Matches: Twitter (@user123), Facebook page, forum post.
- **Fayda:** Free aur fast—TinEye exact matches ke liye best, Yandex visuals ke liye strong.
- **Note:** Google kam effective ho sakta hai agar image altered hai.

4. **Advanced: Facial Recognition for Identity Confirmation:**

- **Tool:** PimEyes (pimeyes.com)
- **Kya Hai:** Ye ek facial recognition search engine hai jo profile pics se online presence aur identities dhoondhta hai.
- **Kaise Use Karein:**

(a) PimEyes pe jao, image upload karo.

(b) Search karo—results mein matching faces ke links milenge.

- **Output Example:**
  - Image: profile.jpg
  - Results: LinkedIn profile, news article photo.
- **Fayda:** Cross-platform presence confirm karta hai—advanced OSINT ke liye powerful.
- **Note:** Privacy laws strict hain—India mein IT Act ya GDPR follow karo, ethical use zaroori ($19.99/month premium).

5. **Save and Analyze:**

- Notion mein table banao:

Image	Source	Linked Accounts	Tool
profile.jpg	Instagram	Twitter, FB	TinEye

- **Analyze:** Metadata aur matches se timeline ya location banao—investigation ko refine karo.

Workflow Example:

- **Image:** profile.jpg (Instagram se downloaded)
- **ExifTool:** GPS: Mumbai, Date: 2023-05-15.
- **TinEye:** Matches: Twitter (@user123), forum post.
- **PimEyes:** LinkedIn profile confirmed.
- **Conclusion:** Image Mumbai se hai, 2023 ka hai, aur 3 platforms pe linked hai.

Extra Tips:

- **Metadata Check:** Social media se downloaded images mein metadata nahi hota—original source try karo.
- **Yandex Advantage:** Non-English sites ke liye Yandex best hai—Indian context mein useful.
- **Legal Caution:** PimEyes ya scraping ke liye platform policies aur local laws (IT Act) check karo.
- **Expand:** Linked accounts se usernames lo, Sherlock ya SignalHire chalao—aur info nikalo.

Tables

Tool	Purpose	Output
ExifTool	Metadata Extraction	Location, Date
DownAlbum	Image Download	Profile Pics
TinEye	Reverse Search	Account Matches
PimEyes	Facial Recognition	Identity Links

Table 47: Tools for Image OSINT

Summary

- ExifTool se metadata lo—location, date.
- Reverse search (TinEye, Yandex) se accounts track karo.
- Notion mein save karo—investigation organize rakho.

Point To Note

Image OSINT mein **ExifTool** (exiftool.org) se metadata (location, date) extract karo, **DownAlbum** (chrome.google.com/webstore) se profile pics download karo, aur **Google Images** (images.google.com), **TinEye** (tineye.com), ya **Yandex** (yandex.com/images) se related accounts dhoondho. Advanced cases mein **PimEyes** (pimeyes.com) se identity confirm karo—privacy laws (IT Act, GDPR) ka dhyan rakhte hue. Ye techniques OSINT investigations mein profiles ko link karne aur deeper insights ke liye perfect hain—systematic kaam karo aur legal boundaries follow karo!

==========

Tracking Images Using Google

Tracking images using Google ek powerful **reverse image search** technique hai jo aapko internet pe text ki jagah **image** se search karne deta hai. Ye OSINT mein kaafi useful hai – isse aap **image authenticity verify** kar sakte ho, **sources identify** kar sakte ho, aur **similar content** dhoondh sakte ho. **Google Reverse Image Search** ke through aap exact images ko web pe track kar sakte ho, aur ye websites, objects, ya faces ke baare mein info deta hai. Iske

features mein single object detection jaise capabilities bhi shamil hain. Saath hi, ek browser extension – **Search by Image by Armin Sabetan** – multiple search engines (Google, Bing, Yahoo, Yandex, Baidu) pe reverse search ko aur bhi easy bana deta hai. Chalo is process ko step-by-step samajhte hain aur dekhte hain kaise Google aur extensions se image tracking hoti hai.

What is Reverse Image Search?

- Reverse image search ek method hai jisme aap ek photo upload karke uske baare mein info ya similar images dhoondhte ho – text search ki jagah visual input ka use hota hai.
- **Usage in OSINT:**
  - **Verify Image Authenticity:** Check karo ki image real hai ya manipulated (e.g., Photoshopped ya AI-generated).
  - **Identify Sources:** Pata lago image kahan se aayi – original website, social media post, ya creator ka naam.
  - **Find Similar Content:** Same ya visually related images ke through context ya additional leads collect karo.

Google Reverse Image Search

- **Kya Hai:** Google Images ka reverse search feature aapko web pe exact ya similar images dhoondhne deta hai – Google ke massive database aur AI ka use karta hai.
- **Features:**
  - **Displays Websites:** Jahan-jahan image appear karti hai – jaise news articles, blogs, ya social media pages.
  - **Single Object Detection:** Agar image mein multiple elements hain (e.g., ek person Taj Mahal ke saamne), to Google aksar prominent object (Taj Mahal) pe focus karta hai aur person ko ignore kar sakta hai.
  - **Visually Similar Images:** Exact match na bhi ho toh visually close images suggest karta hai.
  - **Face Matching:** Agar image public hai, to similar faces ya accounts (e.g., GitHub, Twitter) pe results mil sakte hain.
- **Kaise Use Karein:**
  1. **Google.com** pe jao ya direct **images.google.com** open karo.
  2. Search bar mein **camera icon** pe click karo (ye reverse search mode kholta hai).
  3. Do options hain:
     - **Upload Image:** Apne device se photo upload karo (e.g., rishi_tajmahal.jpg).
     - **Paste Image URL:** Online image ka link daalo (e.g., twitter.com/rishi/status/photo.jpg).
  4. Search karo – results mein "Pages with matching images" aur "Visually similar images" sections aayenge.
- **Output Example:**
  - Image: Ek person Gateway of India ke saamne.
  - Result:

    - Websites: "Mumbai Tourism Blog" (gateway_of_india_2023.jpg).
    - Single Object: Gateway of India pe focus – person ka face ignored.
    - Account: GitHub pe same image "rishi_kabra" ke profile pic mein.

- **Fayda:** Free, user-friendly, aur Google ka vast index – websites, objects, aur basic face matching ke liye strong.

- **Note:** Single object detection ki wajah se agar person pe focus chahiye, to image crop karke face pe re-search karna pad sakta hai.

Browser Extension: Search by Image by Armin Sabetan

- **Kya Hai:** Ye ek Chrome/Firefox extension hai jo reverse image search ko multiple search engines pe ek click mein karta hai – **Google**, **Bing**, **Yahoo**, **Yandex**, aur **Baidu**.

- **Kaise Use Karein:**

    1. Chrome Web Store ya Firefox Add-ons se "Search by Image" install karo (chrome.google.com/we (developer: Armin Sabetan).
    2. Kisi website pe image pe **right-click** karo (e.g., Twitter profile pic).
    3. "Search by Image" select karo – submenu khulega:
        - **All Search Engines:** Ek saath Google, Bing, Yahoo, Yandex, Baidu pe search.
        - **Specific Engine:** Sirf Google ya Yandex jaise ek engine chuno.
    4. Har engine ke results alag-alag tabs mein khulenge.

- **Output Example:**

    - Image: Saad ka Instagram profile pic.
    - Google: Instagram page (instagram.com/saad_dubai).
    - Yandex: Twitter bio pic (@saad_dubai).
    - Bing: Forum post mein same image (reddit.com/r/dubai).

- **Fayda:** Multiple engines se comprehensive results – Yandex faces aur non-Western content pe strong hai, Google websites pe, aur Bing US-centric content pe acha kaam karta hai. Time-saving aur versatile.

- **Note:** Baidu China-focused hai, toh Indian ya global context mein kam useful ho sakta hai. Yandex ko priority do agar face recognition chahiye.

Workflow Example:

- **Image:** Rishi ka photo Gateway of India ke saamne.

- **Google Reverse Search:**

    - Upload kiya – Gateway of India pe focus, websites: "Mumbai tourist pics 2025".
    - Face match: GitHub (github.com/rishi_kabra).

- **Search by Image Extension:**

    - Right-click → All Engines:
        - Google: Gateway of India blog post.

    - Yandex: Rishi ka face Twitter pe (@rishi_kabra).
    - Bing: Same image Instagram post mein (@rishi_mumbai).
- **Conclusion:** Image se Rishi ka GitHub, Twitter, aur Instagram mila – Gateway context bhi clear hua.

Extra Tips:

- **Crop Image:** Agar single object detection person ko ignore karta hai, to face crop karke re-upload karo – better face match results.
- **Cross-Check:** Google ke results ko Yandex ya Bing se verify karo – har engine ka alag strength hai.
- **Save Results:** Notion ya Excel mein table banao:

Image	Source	Account	Engine
rishi_photo.jpg	Gateway of India	github.com/risl	Google
rishi_photo.jpg	Twitter Bio	@rishi_kabra	Yandex

- **Ethics:** Sirf public images use karo – private ya sensitive data se privacy issues ho sakte hain.

Tables

Tool	Strength	Output
Google	Websites	Pages, Objects
Yandex	Faces, Non-Western	Account Matches
Bing	US Content	Forum Posts

Table 48: Reverse Image Search Tools Comparison

Summary

- Google se websites, objects track karo.
- Extension se Yandex, Bing ke saath expand karo.
- Notion mein save karo – results organize rakho.

Point To Note

Google Reverse Image Search se images ko track karna easy hai – **google.com** pe camera icon se upload ya URL daal kar websites, objects, aur accounts dhoondho. **Single object detection** ki wajah se landmarks pe zyada focus hota hai, lekin face matches bhi possible hain (e.g., GitHub profiles). **Search by Image extension** (chrome.google.com/webstore, Armin Sabetan) Google, Bing, Yahoo, Yandex, Baidu pe ek click mein search karta hai – right-click se all ya specific engines chuno. Ye tools OSINT ke liye perfect hain – authenticity verify karne, sources dhoondhne, aur similar content ke liye. Results ko systematically save karo (Notion/Excel) – image ki puri story step-by-step khul jati hai!

==========

Discovering Location of an Image

Bing Reverse Image Search ek powerful tool hai jo image ke through location ya related info dhoondhne mein help karta hai. Iski features mein visually similar images dhoondhna, strong object detection, aur products ya items ko images mein identify karna shamil hai – ye OSINT ke liye ideal hai jab aapko image ka context ya location pata lagana ho. Chalo step-by-step dekhte hain kaise kaam karta hai.

Bing Reverse Image Search

- **Kya Hai:** Bing ka reverse image search feature Microsoft ke AI-powered visual search pe based hai, jo images ko analyze karke similar visuals aur info deta hai.
- **Features:**
  - **Find Visually Similar Images:** Agar aapke paas ek photo hai, to Bing usse match karne wali ya visually close images dhoondh sakta hai.
  - **Strong Object Detection:** Objects jaise buildings, products, ya landmarks ko pehchaanne mein kaafi acha hai – location hint ke liye useful.
  - **Ideal for Detecting Products and Items in Images:** Shopping ya item identification ke liye perfect, lekin locations ke liye bhi kaam aata hai agar object prominent ho.
- **Kaise Use Karein:**
  1. Bing.com pe jao.
  2. Search bar mein **camera icon** pe click karo – yeh visual search mode kholta hai.
  3. Do options hain:
     - **Upload Image:** Device se image upload karo (e.g., tajmahal.jpg).
     - **Paste Image URL:** Online image ka link daalo (e.g., example.com/tajmahal.jpg).
  4. Search karo – Bing similar images, websites, aur object details deta hai.
- **Output Example:**
  - Image: Ek person Statue of Liberty ke saamne.
  - Result:
    - Visually Similar: Statue of Liberty ki dusri pics.
    - Object Detection: Statue pe focus – location hint "New York".
    - Websites: Travel blogs ya Wikipedia pages.
- **Fayda:** Bing ka object detection location ke clues deta hai, especially agar image mein recognizable landmarks hain.
- **Note:** Faces ya complex backgrounds mein thoda weak ho sakta hai – object-focused hai.

Extra Tips:

- **Crop for Focus:** Agar location dhoondhna hai, to landmark pe zoom karke crop karo – better results.

- **Cross-Check:** Bing ke results ko Google (images.google.com) ya Yandex (yandex.com/images) se verify karo – alag engines se zyada accuracy mil sakti hai.
- **Save:** Results ko note karo – e.g., "Statue of Liberty, New York, bing.com/results".

Tables

Feature	Strength	Output
Visually Similar	Image Matching	Similar Pics
Object Detection	Landmarks	Location Hints
Product Detection	Items	Item Info

Table 49: Bing Reverse Image Search Features

Summary

- Bing se landmarks detect karo – location clues lo.
- Similar images aur websites se context banao.
- Cross-check aur save karo – accuracy badhao.

Point To Note

Bing Reverse Image Search location dhoondhne ke liye acha hai, khaas kar jab image mein strong objects ya landmarks hain. **Bing.com** pe camera icon se upload ya URL daal kar visually similar images aur object detection ke through clues milte hain. Aapka content sahi tha, maine bas steps, examples, aur tips add kiye taaki process clear aur practical ho jaye. Agar location ke saath products bhi dhoondhna ho, to Bing ek solid option hai!

==========

Discovering Similar Pictures/Images on the Internet

Yandex Reverse Image Search ek powerful tool hai jo internet pe similar pictures ya images dhoondhne ke liye kaam aata hai. Iski features mein similar faces detect karna, kuch locations identify karna, aur strong text recognition shamil hai – ye OSINT mein kaafi effective hai. Chalo iske baare mein detail mein samajhte hain.

Yandex Reverse Image Search

- **Kya Hai:** Yandex Russia ka search engine hai jo apne advanced image recognition ke liye famous hai – Google se bhi strong facial recognition deta hai.
- **Features:**
  - **Good for Detecting Similar Faces:** Faces ko match karne mein expert – alag lighting ya angles mein bhi kaam karta hai.

- **Effective at Identifying Some Locations:** Landmarks ya unique backgrounds se location hints deta hai.
- **Strong Text Recognition:** Image mein text (signs, posters) ko read karke search refine karta hai.

- **Kaise Use Karein:**
  1. Yandex.com/images pe jao.
  2. Search bar mein **camera icon** pe click karo.
  3. Options:
     - **Upload Image:** Apne device se photo daalo (e.g., rishi_market.jpg).
     - **Paste URL:** Online image ka link use karo.
  4. Search karo – similar images, faces, text, aur locations ke results aayenge.

- **Output Example:**
  - Image: Ek person Red Square, Moscow ke saamne.
  - Result:
    * Similar Faces: Us person ki dusri pics (Twitter, VK).
    * Location: Red Square identify kiya.
    * Text: Nearby sign "Kremlin" read kiya.

- **Fayda:** Faces aur text pe focus ke saath similar images dhoondhne mein best – location ke liye bhi kaam aata hai agar clear cues hain.

- **Note:** Non-European contexts mein thodi kam accuracy ho sakti hai – Russia/Europe pe zyada strong.

Extra Tips:

- **Face Focus:** Agar similar faces chahiye, to crop karke face pe search karo.
- **Text Use:** Image mein text ho to usse manually search karo – location confirm ho sakti hai.
- **Yandex Advantage:** Google se better facial recognition – catfish ya identity checks ke liye top choice.

Tables

Feature	Strength	Output
Face Detection	High Accuracy	Similar Faces
Location ID	Landmarks	Location Hints
Text Recognition	Signs, Posters	Refined Search

Table 50: Yandex Reverse Image Search Features

Summary

- Yandex se faces aur text detect karo.
- Locations aur similar images ke clues lo.
- Crop aur verify karo – results refine karo.

Point To Note

Yandex Reverse Image Search similar pictures dhoondhne ke liye ek zabardast tool hai – **faces detect** karne, **locations identify** karne, aur **text recognition** mein strong. **Yandex.com/images** pe camera icon se upload ya URL daal kar results lo. Aapka content perfect base tha, maine features ko elaborate kiya aur practical use add kiya. Ye tool OSINT ke liye kaafi versatile hai, especially jab faces ya text se clues chahiye!

==========

Expanding the Search with Specialized Image Engines

Specialized image engines jaise **TinEye** aur **NumLookup** reverse image search ko expand karte hain. **TinEye** online pictures search karne ke liye hai – ye logos ya public images identify karne mein acha hai, lekin places ya faces ke liye weak hai. **NumLookup** ke baare mein bhi explain karte hain – ye ek lesser-known tool hai jo specific purposes ke liye kaam aata hai. Chalo dono ko samajhte hain.

TinEye

- **Kya Hai:** TinEye ek dedicated reverse image search engine hai jo exact matches dhoondhne pe focus karta hai – 72 billion+ images ka database hai.
- **Features:**
  - **Search for Pictures Online:** Web pe image ke exact instances dhoondhta hai.
  - **Good at Identifying Logos or Public Pictures:** Digital media (avatars, logos, buttons) ke liye best – forums ya websites pe tracking ke liye useful.
  - **Not Good for Detecting Places or Faces:** Location ya facial recognition mein weak – sirf exact image matches pe strong.
- **Kaise Use Karein:**
  1. **TinEye.com** pe jao.
  2. **Upload** button pe click karo ya image URL paste karo.
  3. Search karo – exact matches aur websites ke results aayenge.
- **Output Example:**
  - Image: DomainTools ka logo.
  - Result:
    - Matches: DomainTools website, Twitter, LinkedIn pe same logo.
    - No Location/Faces: Sirf logo pe focus, context nahi.

- **Fayda:** Copyright tracking ya digital media ke liye perfect – OSINT mein avatars trace karne ke liye acha.
- **Note:** Visually similar images nahi dhoondhta, sirf exact copies.

NumLookup

- **Kya Hai:** NumLookup primarily ek reverse phone lookup tool hai, lekin kuch cases mein image-based search ko support karta hai – identity verification ke liye zyada use hota hai.
- **Features:**
  - **Phone-Image Link:** Agar image phone number se linked hai (e.g., profile pic), to uska source trace kar sakta hai.
  - **Limited Image Search:** Direct reverse image search nahi hai – social media ya public directories se data pull karta hai.
  - **Identity Focus:** Faces ya objects se zyada contact info pe focus.
- **Kaise Use Karein:**
  1. **NumLookup.com** pe jao.
  2. Image upload ka option nahi – lekin agar image phone number se tied hai, to indirectly search possible.
  3. Phone number daal kar related profiles ya pics check karo.
- **Output Example:**
  - Image: Ek person ka profile pic WhatsApp se.
  - Result: Number se linked Twitter/Instagram profile milta hai.
- **Fayda:** Phone-based OSINT ke liye acha – image se direct location ya similar pics nahi, balki identity clues deta hai.
- **Note:** Full-fledged image search engine nahi – limited scope.

Extra Tips:

- **TinEye Use:** Logo ya public image ke source ke liye pehla choice.
- **NumLookup Hack:** Agar image social media se hai, to username ya number extract karke NumLookup pe try karo.
- **Combine Tools:** TinEye ke exact matches ko Bing (bing.com) ya Yandex (yandex.com/images) ke saath cross-check karo – broader results ke liye.

Tables

Summary

- TinEye se logos, avatars trace karo.
- NumLookup se phone-linked identity clues lo.

Tool	Strength	Limitation
TinEye	Exact Matches, Logos	No Faces/Places
NumLookup	Phone-Linked Identity	Limited Image Search

Table 51: Specialized Image Engines Comparison

- Combine tools – broader OSINT coverage ke liye.

Point To Note

TinEye (TinEye.com) aur **NumLookup** (NumLookup.com) specialized image search ke liye alag-alag strengths dete hain. **TinEye** logos aur public pictures ke exact matches ke liye best hai, lekin places/faces mein weak. **NumLookup** image search se zyada identity/phone-based tracking pe focus karta hai. Aapka content sahi tha, maine details, examples, aur limitations add kiye taaki OSINT ke liye inka scope clear ho jaye. Dono tools apne niche mein kaam aate hain – combine karke use karo for max results!

==========

Track Online Presence/Profiles Using a Photo

Facial recognition ek advanced technique hai jo aapko internet pe identical ya similar faces dhoondhne mein help karti hai jo online appear hue hain. Ye tools OSINT ke liye kaafi powerful hain jab aap kisi ki online presence ya profiles track karna chahte ho ek photo ke through. Niche teen websites hain jo is kaam ke liye famous hain – har ek ke apne strengths hain. Chalo inko step-by-step explore karte hain aur dekhte hain kaise ye aapki photo se online profiles tak le ja sakte hain.

What is Facial Recognition in OSINT?

- Facial recognition tools AI-based hote hain jo ek photo upload karke internet pe us face ke matches dhoondhte hain – social media, websites, videos, ya news mein.
- **Purpose:**
  - Kisi ki online presence track karna (e.g., social media profiles).
  - Identity verify karna ya unknown faces ka source pata lagana.
  - Publicly available data se insights collect karna.

Websites for Facial Recognition

1. **Search4faces.com**
   - **Kya Hai:** Ye ek reverse face search engine hai jo specially social media profiles pe focus karta hai.
   - **Strength:** Russia-based searches ke liye best – iska sabse bada database **VKontakte** (VK) ka hai, jo Russia ka famous social media network hai, 1.1 billion+ images ke saath.
   - **Features:**
     - VKontakte ke alawa TikTok, Instagram, Clubhouse, aur OK.ru (another Russian network) ke databases bhi hain.

- Simple interface – photo upload karo aur similar faces ke results dekho.

- **Kaise Use Karein:**
  (a) **Search4faces.com** pe jao.
  (b) Photo upload karo ya URL daalo.
  (c) Search karo – VK ya dusre platforms pe matches milenge.
- **Output Example:**
  - Image: Ek person ka photo.
  - Result: VK profile (@ivan_moscow), TikTok avatar match.
- **Fayda:** Russian ya Eastern European profiles track karne ke liye top choice.
- **Note:** Western platforms (e.g., Twitter, Facebook) pe kam effective – database limited hai.

2. **PimEyes**

- **Kya Hai:** Ye ek advanced facial recognition tool hai jo web pe aapki image kahan-kahan appear karti hai, uska pata lagata hai.
- **Strength:** Global reach – social media, news, blogs, aur random websites pe search karta hai.
- **Features:**
  - Exact aur similar face matches dikhata hai.
  - Privacy monitoring – aapko alert karta hai agar aapka face kahin naya show ho.
  - Paid service, lekin limited free searches bhi deta hai.
- **Kaise Use Karein:**
  (a) **PimEyes.com** pe jao.
  (b) Photo upload karo.
  (c) Results check karo – websites aur links milenge jahan face match hota hai.
- **Output Example:**
  - Image: Ek selfie.
  - Result: Instagram post, news article mein same face.
- **Fayda:** Online presence monitor karne ke liye perfect – personal safety ya identity theft check ke liye bhi use hota hai.
- **Note:** Premium features ke liye payment zaroori hai – free version mein results limited hote hain.

3. **FaceCheck.ID**

- **Kya Hai:** Ye ek facial recognition search engine hai jo social media accounts, videos, news, blogs, websites, aur public databases (jaise mugshots) pe search karta hai.
- **Strength:** Broad coverage – 793 million+ faces ka database, including criminals aur public figures.
- **Features:**
  - Social media (Twitter, LinkedIn, etc.), videos (YouTube, TikTok), aur news pe matches dhoondhta hai.
  - Match certainty score deta hai (50-100) – high score matlab strong match.

- Crypto payment option – privacy-focused users ke liye.

- **Kaise Use Karein:**
  (a) **FaceCheck.ID** pe jao.
  (b) Photo upload karo (free mein 10 searches/day, paid ke liye credits chahiye).
  (c) Results dekho – profiles, videos, ya articles milenge.
- **Output Example:**
  - Image: Ek unknown person ka photo.
  - Result: Twitter (@john_doe), YouTube video thumbnail, local news blog.
- **Fayda:** Comprehensive search – scammers, fraudsters, ya missing persons track karne ke liye useful.
- **Note:** Free version ka database shallow hai – deep search ke liye paid plan chahiye.

Workflow Example:

- **Image:** Ek person ka photo market mein.
- **Search4faces:** VK profile mila (@alex_market_moscow).
- **PimEyes:** Same face ek Russian blog pe (market event).
- **FaceCheck.ID:** Twitter (@alex_travel) aur YouTube vlog mein match.
- **Conclusion:** Teen tools se profile, location, aur activity ka full picture bana.

Extra Tips:

- **Combine Tools:** Search4faces Russia ke liye, PimEyes global monitoring ke liye, aur FaceCheck.ID deep social media search ke liye use karo.
- **Crop Image:** Face pe focus karne ke liye photo crop karo – better accuracy.
- **Ethics:** Public images hi use karo – privacy laws ka dhyan rakho.
- **Save Results:** Notion mein table banao:

Tool	Result	Platform
Search4faces	@ivan_moscow	VKontakte
PimEyes	News article	example.com
FaceCheck.ID	@john_doe	Twitter

Tables

Summary

- Search4faces se VK profiles lo.
- PimEyes se global presence track karo.
- FaceCheck.ID se deep search – social media aur beyond.

Tool	Strength	Limitation
Search4faces	VK/Russia Focus	Weak on Western Platforms
PimEyes	Global Reach	Paid for Full Access
FaceCheck.ID	Broad Coverage	Free Version Shallow

Table 52: Facial Recognition Tools Comparison

Point To Note

Facial recognition tools jaise **Search4faces.com**, **PimEyes.com**, aur **FaceCheck.ID** ek photo se online presence track karne ke liye shandaar hain. **Search4faces** Russia ke VKontakte pe strong hai, **PimEyes** global web monitoring deta hai, aur **FaceCheck.ID** social media, videos, aur news pe deep search karta hai. Aapka content sahi tha, maine bas details, steps, aur examples add kiye taaki ye OSINT ke liye aur practical ho jaye. Teeno tools ko combine karke aap kisi bhi profile ki puri story uncover kar sakte ho!

==========

Using AI to Identify an Image Location

Image geolocation with AI ya websites ke through ek picture ki location uncover karna ab kaafi asaan ho gaya hai, thanks to tools like **GeoSpy**. Ye ek AI-powered geolocation service hai jo photos ko analyze karke unki location pata lagata hai. GeoSpy alag-alag elements ko examine karta hai jaise landmarks, vegetation, aur building styles, taaki aapko exact ya close-to-exact location mil sake. Agar aapke paas ek picture hai aur aap janana chahte ho ki ye kahan ki hai, to GeoSpy jaise tools ka use kar sakte ho. Chalo isko detail mein samajhte hain aur dekhte hain kaise ye kaam karta hai OSINT ke liye.

What is Image Geolocation with AI?

- Image geolocation AI ya websites ke zariye ek photo ke visual clues ko analyze karke uski geographical location predict karta hai – bina metadata (jaise GPS) pe depend kiye.
- **Purpose in OSINT:**
  - Missing persons ya suspects ke locations track karna.
  - News ya social media images ka authenticity check karna.
  - Travel ya historical photos ke origins uncover karna.

GeoSpy: AI-Powered Geolocation Service

- **Kya Hai:** GeoSpy ek cutting-edge AI tool hai jo Graylark Technologies ne develop kiya hai. Ye photos ke content ko scan karke location guess karta hai – millions of images ke database ke saath trained hai.
- **GeoSpy Examines:**
  - **Landmarks:** Famous buildings, bridges, ya natural features jo background mein hain (e.g., Eiffel Tower, Taj Mahal).
  - **Vegetation:** Types of trees ya plants jo specific regions mein hi milte hain (e.g., Joshua trees in California deserts).

- **Building Styles:** Infrastructure jaise road signs, architectural designs, ya power lines jo ek area ke unique hote hain (e.g., yellow taxis ya red phone booths).

- **Kaise Kaam Karta Hai:**

1. Photo upload karo **GeoSpy.ai** pe.
2. AI image ko analyze karta hai – landmarks, vegetation, building styles, aur even shadows/lighting check karta hai.
3. Results deta hai – coordinates, map, aur ek description ke saath (e.g., "Ye photo Mumbai ke Gateway of India ke paas li gayi hai").

- **Output Example:**

  - Image: Ek photo jisme ek person ek old fort ke saamne khada hai.
  - Result:
    - Landmark: "Amber Fort" detect kiya.
    - Vegetation: Rajasthan ke dry landscape se match.
    - Building Style: Mughal architecture.
    - Location: Jaipur, India (approx. coordinates: 26.9855° N, 75.8513° E).

- **Fayda:** Metadata nahi chahiye – sirf visual clues se kaam karta hai. OSINT ke liye fast aur accurate – cities ya regions tak narrow down kar sakta hai.

- **Note:** Exact street-level precision nahi deta – usually few square miles ka radius hota hai. Indoor ya generic photos mein struggle kar sakta hai.

How to Use GeoSpy for Location Tracking

- **Steps:**

1. **GeoSpy.ai** pe jao (abhi testing phase mein hai, sign-up karna pad sakta hai).
2. Ek photo upload karo – clear image with landmarks ya unique features best hai.
3. AI process karega – thodi der mein map aur location guess milega.

- **Example Scenario:**

  - Agar aapke paas ek picture hai jisme ek person ek bridge ke saamne hai, aur aapko nahi pata ye kahan ki hai:
    - Upload karo GeoSpy pe.
    - Result: "Golden Gate Bridge, San Francisco" (37.8199° N, 122.4783° W).

Extra Tips:

- **Image Quality:** Clear, high-res photos with visible clues (landmarks, signs) best results dete hain.

- **Combine Tools:** GeoSpy ke saath Google Earth (earth.google.com) ya Yandex (yandex.com/images) use karo – cross-verification ke liye.

- **Limitations:** Agar photo mein koi unique feature nahi hai (jaise plain field), to guess broad ya inaccurate ho sakta hai.

- **Save Results:** Notion ya Excel mein track karo:

Image	Landmark	Location	Coordinates
bridge_photo.jpg	Golden Gate	San Francisco	37.8199° N, 122.4783° W

Tables

Feature	Strength	Limitation
Landmarks	High Accuracy	Generic Photos Weak
Vegetation	Region-Specific	Indoor Struggle
Building Styles	Unique Clues	Broad Radius

Table 53: GeoSpy Analysis Features

Summary

- GeoSpy se landmarks aur vegetation analyze karo.
- Fast location guesses bina metadata ke.
- Cross-verify aur save karo – OSINT ke liye perfect.

Point To Note

GeoSpy (GeoSpy.ai) jaise AI tools image geolocation ko OSINT ke liye game-changer bana rahe hain. Ye **landmarks**, **vegetation**, aur **building styles** jaise elements ko examine karke picture ki location uncover karta hai – bina metadata ke. Aapka content sahi tha, maine bas isko detailed kiya aur practical steps add kiye taaki koi bhi ise samajh kar use kar sake. Agar aapko ek unknown photo ki location janna hai, to GeoSpy try karo – fast, effective, aur AI ka power dikha deta hai!

==========

Discovering Image Location Using Search Engines

Google Lens ya kisi bhi dusre search engine lens ka use karke aap ek image ke background mein famous landmarks ya locations dhoondh sakte ho. Ye OSINT ke liye ek simple aur effective tareeka hai jab aapko pata lagana ho ki photo kahan li gayi hai. Chalo is process ko samajhte hain aur dekhte hain kaise search engines location clues dete hain.

What is Google Lens?

- Google Lens ek AI-powered visual search tool hai jo images ko analyze karta hai aur usmein objects, landmarks, ya text ko identify karta hai – location tracking ke liye kaafi useful.
- **Purpose in OSINT:**
  - Background mein famous places (e.g., Eiffel Tower, Gateway of India) ko pehchaan na.

- Image ke context ya authenticity ko verify karna.

Using Google Lens to Find Background Famous Image

- **Kaise Kaam Karta Hai:** Google Lens photo ke visual elements ko scan karta hai aur Google ke massive database se match karta hai – landmarks ya famous buildings pe focus karta hai.
- **Steps:**
  1. **Google App** kholo (Android/iOS) ya **Google Photos** pe jao (photos.google.com).
  2. Photo upload karo ya camera se live scan karo.
  3. **Lens Icon** pe click karo – ye image ko analyze karega.
  4. Results dekho – famous landmarks, places, ya similar images ke saath location info milegi.
- **Output Example:**
  - Image: Ek person ek tower ke saamne khada hai.
  - Result: Google Lens "Eiffel Tower" detect karta hai – location: Paris, France (48.8584° N, 2.2945° E).
- **Fayda:** Free, fast, aur mobile-friendly – background ke famous elements ko instantly spot karta hai.
- **Note:** Agar background generic hai (jaise plain field), to specific location nahi milegi – landmarks chahiye hote hain.

Other Search Engine Lenses

- **Bing Visual Search:** **Bing.com** pe camera icon se similar functionality – landmarks aur objects pe strong.
- **Yandex Image Search:** **Yandex.com/images** pe upload karke location clues – text aur buildings pe acha kaam karta hai.
- **Comparison:** Google Lens global landmarks pe best hai, Yandex text/location combos ke liye, aur Bing objects ke liye.

Extra Tips:

- **Crop Image:** Background pe focus karne ke liye person ya foreground ko crop karo.
- **Cross-Check:** Google Lens ke result ko Bing ya Yandex se verify karo – zyada accuracy ke liye.
- **Save:** Location guess ko note karo – e.g., "Eiffel Tower, Paris, Google Lens".

Tool	Strength	Limitation
Google Lens	Global Landmarks	Generic Backgrounds
Bing Visual	Objects	Less Text Focus
Yandex	Text + Buildings	Regional Bias

Table 54: Search Engine Lenses Comparison

Tables

Summary

- Google Lens se famous landmarks spot karo.
- Bing aur Yandex se extra clues lo.
- Cross-check karo – location confirm karo.

Point To Note

Google Lens (photos.google.com) ya dusre search engine lenses (Bing.com, Yandex.com/images) se image ke background mein famous locations dhoondhna asaan hai – photo upload karo aur AI landmarks identify karta hai. Aapka content sahi tha, maine steps, examples, aur alternatives add kiye taaki ye practical aur clear ho jaye. OSINT ke liye ye ek quick way hai famous places ko spot karne ka – try karo aur results ko cross-check karo for best output!

==========

Extracting Location, Device Info, and More from Images

Metadata image, video, ya document file ke andar stored information hoti hai jo us file ke baare mein extra details deti hai – jaise creation/modification date, author, username, GPS coordinates, aur device information. Note – zyadatar platforms (jaise Instagram, Twitter) upload ke pehle metadata remove kar dete hain, lekin kuch platforms (jaise forums ya personal websites) nahi hatate. Is metadata ko extract karne ke liye aap image save karke websites ya browser extensions ka use kar sakte ho. Chalo isko detail mein dekhte hain.

What is Metadata?

- Metadata ek file ka "hidden data" hota hai jo uski creation ya usage ke baare mein info store karta hai – OSINT ke liye goldmine ho sakta hai.
- **Details It Provides:**
  - **Creation/Modification Date:** Kab photo li gayi ya edit ki gayi.
  - **Author/Username:** Kisne banaya ya upload kiya.
  - **GPS Coordinates:** Exact location jahan photo li gayi (latitude, longitude).
  - **Device Information:** Camera/phone model, software version, etc.

How to Extract Metadata

1. **Step 1: Save the Image**
   - Website pe image pe **right-click** karo ¿ **Save Image As...** ¿ Apne device pe save karo (e.g., photo.jpg).
   - Note: Original file download karna zaroori hai – screenshot se metadata nahi milega.
2. **Websites for Metadata Extraction**
   - **Metadata2Go (metadata2go.com):**
     - **Kya Hai:** Free online tool jo image upload karke metadata dikhata hai.
     - **Features:** EXIF, IPTC, XMP data – GPS, device, date, sab cover karta hai.
     - **Kaise Use Karein:**
       (a) **Metadata2go.com** pe jao.
       (b) Image upload karo.
       (c) Results dekho – e.g., "GPS: 28.7041° N, 77.1025° E (Delhi), Device: iPhone 14".
   - **Exif.tools (exif.tools):**
     - **Kya Hai:** Ek aur simple tool jo metadata ko clean format mein present karta hai.
     - **Features:** Detailed EXIF data – camera settings (ISO, aperture) bhi deta hai.
     - **Kaise Use Karein:**
       (a) **Exif.tools** pe jao.
       (b) Photo upload karo ya URL daalo.
       (c) Output check karo – e.g., "Date: 2025-04-01, Camera: Canon EOS R5".
3. **Browser Extension: Exif Viewer by Alan Raskin**
   - **Kya Hai:** Ye Chrome/Firefox extension hai jo direct website pe image ka metadata dikhata hai – download ki zarurat nahi.
   - **Kaise Install Karein:**
     (a) Chrome Web Store (chrome.google.com/webstore) ya Firefox Add-ons pe "Exif Viewer by Alan Raskin" search karo.
     (b) **Add to Browser** pe click karo.
   - **Kaise Use Karein:**
     (a) Kisi website pe image pe **right-click** karo.
     (b) **Exif Viewer** option select karo.
     (c) Pop-up mein metadata dekho – e.g., "GPS: 40.7128° N, 74.0060° W (New York), Device: Samsung S23".
   - **Fayda:** Fast aur convenient – live websites pe kaam karta hai.
   - **Note:** Agar platform ne metadata strip kiya hai, to "No EXIF data found" dikhega.

Output Example:

- **Image:** Ek photo jo Flickr pe upload hui.
- **Metadata2Go:** "GPS: 51.5074° N, 0.1278° W (London), Date: 2025-03-15, Device: Nikon Z6".

- **Exif Viewer:** Same details direct browser mein.

Extra Tips:

- **Check Platforms:** Flickr, personal blogs, ya forums metadata retain karte hain – social media (Twitter, Insta) pe rare hai.
- **Cross-Verify:** GPS coordinates ko Google Maps (maps.google.com) pe daal kar exact spot confirm karo.
- **Save Results:** Table banao:

Image	GPS Coordinates	Device	Date
photo.jpg	51.5074° N, 0.1278° W	Nikon Z6	2025-03-15

- **Ethics:** Privacy ka dhyan rakho – sensitive info share mat karo.

Tables

Tool	Strength	Limitation
Metadata2Go	Easy, Free	Online Only
Exif.tools	Detailed EXIF	No Live View
Exif Viewer	Live Website	Stripped Data Fails

Table 55: Metadata Extraction Tools Comparison

Summary

- Image save karo – original file lo.
- Metadata2Go ya Exif.tools se details nikalo.
- Exif Viewer se live check – fast OSINT.

Point To Note

Metadata se location, device info, aur aur bhi details extract karna OSINT ke liye ek powerful method hai. Image ko **save** karke **Metadata2go.com** ya **Exif.tools** pe upload karo, ya **Exif Viewer by Alan Raskin** (chrome.google.com/webstore) extension se direct check karo. Aapka content solid tha, maine steps, tools ki details, aur examples add kiye taaki ye aur clear aur actionable ho jaye. Note – platforms metadata remove karte hain, lekin jab milta hai, to location aur context ka treasure deta hai!

==========

Maps OSINT Using Maps for Geolocation Analysis - Introduction to Maps OSINT

Maps OSINT mein hum seekhenge ki kaise sabse important mapping services – **Google Maps**, **Yandex Maps**, **Apple Maps**, aur **Bing Maps** – ko geolocation analysis ke liye use karna hai. Ye tools locations ko samajhne, track karne, aur investigate karne ke liye OSINT ka ek critical part hain. Chalo in services ke basics ko explore karte hain aur dekhte hain kaise ye humein real-world insights dete hain.

Introduction to Maps OSINT

- Maps OSINT mapping services ka use karke locations ke baare mein data collect karne ka tareeka hai – satellite imagery, street views, aur local details ke through.
- **Purpose:**
  - Specific places ki geolocation verify karna.
  - Travel routes, traffic patterns, ya infrastructure analyze karna.
  - Visual ya contextual clues ke liye satellite aur street-level imagery ka use.

Key Mapping Services

1. **Google Maps:** Duniya ka sabse popular mapping tool – global coverage aur detailed features ke saath.
2. **Yandex Maps:** Russia aur Eastern Europe mein strong – local transport aur business data ke liye best.
3. **Apple Maps:** Clean interface aur iOS integration – privacy-focused aur modern imagery.
4. **Bing Maps:** Microsoft ka tool – unique angles aur good global reach ke saath.

How to Use Them

- Har service ka apna strength hai – Google global hai, Yandex regional, Bing angles ke liye, aur Apple simplicity ke liye.
- Basic Step: Website kholo (e.g., **maps.google.com**), location search karo, aur features explore karo.

Extra Tips:

- **Combine Services:** Ek location ke liye do-teen maps check karo – alag perspectives milte hain.
- **Save Data:** Screenshots ya coordinates note karo – e.g., "Red Square, Moscow, 55.7558° N, 37.6173° E".

Tables

Summary

- Google Maps se global insights lo.

Service	Strength	Unique Feature
Google Maps	Global Coverage	Street View
Yandex Maps	Regional Focus	Local Transport
Apple Maps	Privacy + Simplicity	iOS Integration
Bing Maps	Unique Angles	Microsoft Ecosystem

Table 56: Mapping Services Comparison

- Yandex, Apple, aur Bing ke unique strengths use karo.
- Combine karo – detailed geolocation ke liye.

Point To Note

Maps OSINT ke through **Google Maps** (maps.google.com), **Yandex Maps**, **Apple Maps**, aur **Bing Maps** jaise tools se geolocation analysis karna seekhenge. Aapka content intro ke liye perfect tha, maine bas thodi structure aur purpose add kiya taaki ye clear ho jaye ki ye tools kaise kaam aate hain. Ye mapping services locations ko deeply investigate karne ka foundation dete hain – chalo aage details mein jate hain!

==========

Uncovering Key Details About Any Location

Google Maps ek extensive global coverage wala mapping service hai, jo isse duniya mein sabse zyada used tool banata hai. Iski features – street view, local business info, opening/closing hours, reviews, aur real-time traffic – OSINT ke liye key details uncover karne mein madad karti hain. Chalo dekhte hain kaise ye location insights deta hai.

Google Maps

- **Kya Hai:** Google Maps ek all-in-one mapping platform hai jo satellite imagery, street-level views, aur user-generated data combine karta hai – 200+ countries mein coverage.
- **Features:**
  - **Street View:** 360° ground-level imagery – roads, buildings, aur surroundings dekho.
  - **Local Business Information:** Shops, restaurants ke details – address, phone number, website.
  - **Opening and Closing Hours:** Business timings check karo – planning ya verification ke liye.
  - **Reviews:** User reviews se vibe ya authenticity ka idea milta hai (e.g., "Crowded on weekends").
  - **Real-Time Traffic:** Live traffic data – roads busy hain ya nahi, events ka impact.
- **Kaise Use Karein:**
  1. **maps.google.com** pe jao ya Google Maps app kholo.
  2. Location search karo (e.g., "Taj Mahal, Agra").
  3. Features explore karo:
     - Street View ke liye blue lines pe click karo.

- Business info ke liye pin pe zoom in karo.
- Traffic ke liye "Layers" ¿ "Traffic" select karo.

- **Output Example:**
  - Location: "Connaught Place, New Delhi".
  - Street View: Circular market layout, shops visible.
  - Business Info: "Barista Coffee, Open 8 AM - 11 PM, 4.2 stars".
  - Traffic: "Moderate traffic at 6 PM".
- **Fayda:** Ek location ka full picture – visual, practical, aur live data ke saath.
- **Note:** Street View har jagah available nahi – rural areas mein limited.

Extra Tips:

- **Historical Street View:** Timeline check karo – purani imagery se changes track karo.
- **Coordinates:** Right-click se exact lat/long lo – e.g., "28.6139° N, 77.2090° E".
- **Cross-Verify:** Reviews ya photos se additional clues lo (e.g., event dates).

Tables for Uncovering Key Details

Feature	Use	Example
Street View	Visual Context	Shop Layouts
Business Info	Contact Details	Opening Hours
Real-Time Traffic	Live Updates	Traffic at 6 PM

Table 57: Google Maps Features

Summary (Uncovering Key Details)

- Street View se visuals lo.
- Business info aur traffic se context banao.
- Coordinates save karo – full analysis ke liye.

Point To Note

Google Maps (maps.google.com) global coverage aur features jaise **Street View**, **business info**, aur **real-time traffic** ke saath kisi bhi location ke key details uncover karta hai. Aapka content sahi tha, maine steps aur examples add kiye taaki practical use clear ho. Ye OSINT ke liye ek go-to tool hai – visuals se lekar live updates tak sab deta hai!

Viewing Satellite Imagery from Different Angles

Bing Maps ek solid mapping service hai jo good global coverage deta hai. Iski features – Bird's Eye View aur data from other sources – satellite imagery ko different angles se dekhne mein help karti hain. Chalo dekhte hain kaise ye OSINT ke liye kaam aata hai.

Bing Maps

- **Kya Hai:** Bing Maps Microsoft ka mapping platform hai jo satellite aur aerial imagery ke saath unique perspectives deta hai – 100+ countries mein strong coverage.
- **Features:**
  - **Bird's Eye View:** 45° angle se aerial imagery – buildings, roads, aur terrain ka detailed view.
  - **Display Data from Other Sources:** OpenStreetMap, weather data, ya traffic info integrate karta hai.
- **Kaise Use Karein:**
  1. Bing.com pe jao ¿ top-right mein **Maps** pe click karo.
  2. Location search karo (e.g., "Times Square, NYC").
  3. View switch karo:
     - "Aerial" ke liye top-down satellite view.
     - "Bird's Eye" ke liye angled view (zoom in karna padta hai).
- **Output Example:**
  - Location: "Sydney Opera House".
  - Bird's Eye View: Roof ka unique shape, harbor angle se visible.
  - Data: Weather overlay – "Sunny, 25°C".
- **Fayda:** Bird's Eye se 3D-like perspective – Google ke flat satellite view se alag.
- **Note:** Bird's Eye har jagah nahi hai – urban areas pe zyada focus.

Extra Tips:

- **Zoom In:** Bird's Eye ke liye close zoom chahiye – details ke liye.
- **Compare:** Google Maps ke saath check karo – alag angles se full picture banta hai.
- **Save:** Screenshot lo – angle aur data note karo.

Tables for Viewing Satellite Imagery

Feature	Use	Limitation
Bird's Eye View	45° Angle	Urban Only
External Data	Weather/Traffic	Limited Coverage

Table 58: Bing Maps Features

Summary (Viewing Satellite Imagery)

- Bird's Eye se unique angles lo.
- External data se context add karo.
- Google ke saath compare – detailed view ke liye.

Point To Note

Bing Maps (Bing.com) satellite imagery ko **Bird's Eye View** ke through different angles se dikhata hai, jo good global coverage ke saath OSINT ke liye helpful hai. Aapka content acha tha, maine steps aur clarity add ki. Ye tool unique perspectives ke liye perfect hai – buildings ya layouts ko deeply analyze karne ke liye try karo!

==========

Extracting Key Insights from Eastern Europe Maps

Yandex Maps Russia aur Soviet Union countries (Eastern Europe) mein extensive coverage deta hai. Iski features – metro maps, real-time public transport, aur local business info – key insights extract karne ke liye banayi gayi hain. Chalo dekhte hain kaise ye regional OSINT ke liye kaam aata hai.

Yandex Maps

- **Kya Hai:** Yandex Maps Russia ka leading mapping service hai jo Eastern Europe (Ukraine, Belarus, Kazakhstan, etc.) pe focus karta hai – Google se zyada local data.
- **Features:**
  - **Metro Maps:** Detailed metro systems – Moscow, Kyiv, Minsk ke stations aur routes.
  - **Real-Time Public Transport:** Buses, trams, metro ka live status – timing aur routes.
  - **Local Business Information:** Shops, cafes, offices ke details – hours, reviews, contacts.
- **Kaise Use Karein:**
  1. **Yandex.com** pe jao ¿ **Maps** pe click karo (ya **maps.yandex.com** direct).
  2. Location search karo (e.g., "Red Square, Moscow").
  3. Features check karo:
     - Metro ke liye "Transport" layer on karo.
     - Businesses ke liye pins pe click karo.
- **Output Example:**
  - Location: "Kyiv Central Station".
  - Metro Map: "Line 1, Sviatoshynsko-Brovarska, 5 min walk".

- Transport: “Bus #12 arriving in 3 mins”.
- Business: “Café Kyiv, Open 7 AM - 9 PM, 4.5 stars”.

- **Fayda:** Eastern Europe ke liye unmatched detail – transport aur local life ke insights.
- **Note:** Western countries mein coverage kamzor – Russia/Soviet focus hai.

Extra Tips:

- **Language:** Russian interface – Google Translate (translate.google.com) use karo agar zarurat ho.
- **Live Data:** Real-time transport ke liye app version best hai.
- **Save:** Coordinates aur details note karo – e.g., “55.7558° N, 37.6173° E, Red Square”.

Tables

Feature	Use	Example
Metro Maps	Transport Routes	Kyiv Metro Line 1
Real-Time Transport	Live Updates	Bus #12 in 3 mins
Business Info	Local Details	Café Kyiv Hours

Table 59: Yandex Maps Features

Summary

- Metro maps se routes track karo.
- Real-time transport se live status lo.
- Business info se Eastern Europe samjho.

Point To Note

Yandex Maps (maps.yandex.com) Russia aur Soviet Union countries ke liye extensive coverage deta hai, **metro maps**, **real-time transport**, aur **business info** ke saath. Aapka content spot-on tha, maine steps aur examples daale taaki Eastern Europe ke insights extract karna clear ho. Ye OSINT ke liye regional analysis mein king hai – local details ke liye ise try karo!

==========

Using Apple Maps Without an Apple Device

Apple Maps normally sirf Apple devices (iPhone, Mac) pe available hota hai, lekin kuch websites ke through aap ise bina Apple device ke bhi use kar sakte ho. **https://satellites.pro** ek aisa platform hai – signup free hai aur iski sabse important feature ye hai ki aap multiple maps (Apple Maps, Google Maps, Yandex Maps, OpenStreetMap) ke beech ek hi screen pe switch kar sakte ho, alag-alag maps kholne ki zarurat nahi. Dusra website **https://data.mashedworld.com**

aapki window ko teen different views mein split karta hai – satellite, street view, aur bird's eye view. Chalo step-by-step dekhte hain kaise kaam karta hai.

Using https://satellites.pro

- **Kya Hai:** Ye ek free web-based tool hai jo multiple mapping services ko ek jagah pe laata hai – Apple Maps ko non-Apple devices pe access karne ka ek rare tareeka.
- **Signup:** Free hai – bas email se register karo aur start karo.
- **Most Important Feature:** Ek screen pe multiple maps switch karna – time-saving aur convenient.
- **Kaise Use Karein:**
  1. Satellites.pro pe jao.
  2. Apne place ka map kholo (e.g., "Mumbai").
  3. Top pe **Switch Map** option pe click karo.
  4. Options chuno:
     - **Apple Map:** Apple ka satellite view.
     - **Google Map:** Google ka detailed view.
     - **Yandex Map:** Eastern Europe ke liye strong.
     - **OpenStreetMap:** Community-driven map.
- **Output Example:**
  - Location: "Delhi".
  - Apple Map: Clean satellite imagery.
  - Google Map: Traffic aur street details.
- **Fayda:** Ek hi jagah pe sab maps compare karo – OSINT ke liye perfect jab aapko alag-alag perspectives chahiye.
- **Note:** Free version mein basic features – premium ke liye pay karna pad sakta hai.

Using https://data.mashedworld.com

- **Kya Hai:** Ye ek tool hai jo aapki screen ko split karke teen views deta hai – satellite, street view, aur bird's eye view – ek location ke multiple angles ke liye.
- **Kaise Use Karein:**
  1. Data.mashedworld.com pe jao.
  2. Location enter karo (e.g., "New York").
  3. Screen teen parts mein split hoti hai:
     - **Satellite:** Top-down imagery (Apple/Google se).
     - **Street View:** Ground-level view (Google ya Bing).
     - **Bird's Eye View:** Angled aerial view (Bing-style).
- **Output Example:**
  - Location: "London".

- Satellite: Thames River ka layout.
- Street View: Big Ben ke paas ki galiyan.
- Bird's Eye: Buildings ka 45° angle.

- **Fayda:** Ek saath teen perspectives – detailed analysis ke liye zabardast.
- **Note:** Apple Maps ka direct integration nahi – Google/Bing pe zyada depend karta hai.

Extra Tips:

- **Switch Smartly:** Satellites.pro pe Apple Maps ke saath Yandex bhi try karo – regional differences ke liye.
- **Split View:** Mashedworld pe zoom levels adjust karo – clarity ke liye.
- **Save:** Screenshots lo – views aur coordinates note karo (e.g., "51.5074° N, 0.1278° W").

Tables

Tool	Strength	Limitation
Satellites.pro	Multi-Map Switch	Premium for Extra
Mashedworld	Split Views	No Direct Apple

Table 60: Tools Comparison

Summary

- Satellites.pro se Apple Maps switch karo.
- Mashedworld se teen angles lo.
- Compare aur save – OSINT ke liye best.

Point To Note

Satellites.pro se Apple Maps bina Apple device ke use karo – free signup aur **switch map** feature ke saath Google, Yandex, OpenStreetMap ek screen pe. **Data.mashedworld.com** teen views – **satellite, street view, bird's eye** – deta hai, jo location analysis ko next level pe le jata hai. Aapka content acha tha, maine steps, examples, aur clarity add ki. Ye tools OSINT ke liye time aur effort bachate hain – multiple maps ek jagah pe!

==========

Investigating Places with Street-Level Imagery

Street-level imagery ground-level visuals deta hai jo OSINT ke liye kaafi powerful hai. Iski features – anyone can contribute, frequently updated imagery, aur kuch areas mein zyada coverage – ise unique banati hain. Websites jaise **mapillary.com** aur **kartaview.org** is field mein kaam karte hain. Agar Google aur Bing Maps hain to inka use kab karna chahiye? Chalo explain karte hain.

What is Street-Level Imagery?

- Street-level imagery 360° ground-level photos hoti hain jo roads, buildings, aur surroundings ko real-time view dete hain – satellite se alag, ye "boots on the ground" feel deta hai.
- **Features:**
  - **Anyone Can Contribute:** Users photos upload kar sakte hain – crowd-sourced data.
  - **Frequently Updated Imagery:** Regular updates se latest changes dikhte hain.
  - **More Coverage in Some Areas:** Google/Bing ke gaps ko fill karta hai, especially rural ya niche spots.

Mapillary.com

- **Kya Hai:** Mapillary ek crowd-sourced street imagery platform hai jo Meta ke under ab operate karta hai – global coverage ke saath.
- **Features:**
  - User-contributed photos – dashcams, phones, ya drones se.
  - AI object detection – signs, lanes, objects ko tag karta hai.
  - OpenStreetMap integration – mapping ke liye useful.
- **Kaise Use Karein:**
  1. **Mapillary.com** pe jao.
  2. Location search karo (e.g., "Kyiv").
  3. Street-level imagery explore karo – zoom aur pan karo.
- **When to Use in OSINT:**
  - Jab Google Street View outdated ho ya unavailable ho.
  - Small towns ya rural areas ke liye jahan big players kam cover karte hain.
  - Ground truth verify karne ke liye – e.g., "Ye sign abhi bhi hai ya nahi?"
- **Output Example:**
  - Location: "Lviv, Ukraine".
  - Result: 2025 ka fresh street view – market aur new construction visible.

Kartaview.org

- **Kya Hai:** Kartaview (pehle OpenStreetCam) bhi ek crowd-sourced platform hai jo street imagery collect karta hai – OpenStreetMap ke saath tied hai.

- **Features:**
  - Community-driven – users worldwide contribute.
  - Simple interface – raw imagery without heavy AI processing.
  - Focus on mapping improvements.
- **Kaise Use Karein:**
  1. **Kartaview.org** pe jao.
  2. Location enter karo (e.g., "Bucharest").
  3. Available street imagery dekho.
- **When to Use in OSINT:**
  - Jab aapko Google/Bing se alag perspective chahiye.
  - OpenStreetMap data ko refine karne ke liye – e.g., road updates.
  - Less commercial areas jahan big maps nahi jate.
- **Output Example:**
  - Location: "Sofia, Bulgaria".
  - Result: Narrow streets ka latest view – Google pe nahi tha.

Google/Bing vs. Mapillary/Kartaview

- **Google Street View:** Polished, urban-focused, lekin updates slow aur coverage limited.
- **Bing Streetside:** Decent alternative, lekin kam areas mein available.
- **Mapillary/Kartaview:** Fresh, crowd-sourced, aur niche coverage – jab Google/Bing fail karein tab use karo.

Extra Tips:

- **Check Dates:** Imagery ka timestamp dekho – latest data ke liye.
- **Contribute:** Agar aapke paas photos hain, upload karo – OSINT community ko help milegi.
- **Combine:** Satellite (Google) aur street (Mapillary) dono use karo – full picture ke liye.

Tables

Tool	Strength	When to Use
Mapillary	AI + Fresh Data	Outdated Google
Kartaview	Niche Coverage	OSM Updates
Google/Bing	Polished Views	Urban Areas

Table 61: Street-Level Imagery Tools Comparison

Summary

- Mapillary se fresh views lo.
- Kartaview se niche areas cover karo.
- Google/Bing ke gaps fill karo.

Point To Note

Street-level imagery se places investigate karna asaan hai – **Mapillary.com** aur **Kartaview.org** crowd-sourced, frequently updated views dete hain jo Google/Bing ke gaps ko fill karte hain. Aapka content solid tha, maine inka OSINT use aur comparison add kiya. Ye tools jab chahiye tab kaam aate hain – fresh data aur niche coverage ke liye perfect!

==========

Geo-Locating Images Using OpenStreetMap (OSM)

Bellingcat Map ek powerful tool hai jo **OpenStreetMap (OSM)** data ka use karta hai taaki aap ek picture mein landmarks ya features dhoondh sakein. Ye geolocating pictures ke liye kaafi effective hai, kyunki ye OSM ke crowd-sourced database se specific objects ya structures ke basis pe locations narrow down karta hai. Chalo ise step-by-step samajhte hain aur ek example ke saath dekhte hain kaise kaam karta hai.

Bellingcat Map

- **Kya Hai:** Bellingcat ne ek OSM-based search tool banaya hai (**osm-search.bellingcat.com**) jo OpenStreetMap data ko user-friendly tareeke se query karta hai. Ye geolocation ke liye starting points dhoondhne mein help karta hai.
- **Strength:**
  - OSM ka detailed, community-driven data use karta hai – millions of features jaise roads, buildings, wind turbines, etc.
  - Multiple landmarks ko ek saath search kar sakta hai jo ek specific distance ke andar hain.
  - Very powerful jab aapke paas image mein clear visual clues hain lekin starting point nahi pata.
- **Kaise Use Karein:**
  1. **osm-search.bellingcat.com** pe jao – Google account se login karo (free tool hai).
  2. Image analyze karo – dekho kya-kya features ya landmarks hain (e.g., railway, wind turbine, mountain).
  3. **Search Area Set Karo:** Map pe zoom karke ek region select karo (e.g., "Belgium" ya "Xinjiang, China").
  4. **Features Add Karo:**
     - Pre-set options (jaise railway, school) select karo ya custom tags daalo (OSM wiki se check karo kaise tag kiya gaya hai).
     - Distance set karo (e.g., 500 meters ke andar).

5. Search karo – results map pe pins ke roop mein aayenge.
6. **Verify Karo:** Results ko Google Maps ya Google Earth pe khol kar image se match karo.

- **Example:**
  - **Image:** Ek photo jisme wind turbines, ek railway line, aur background mein mountains hain.
  - **Step 1:** Bellingcat Map kholo, "Xinjiang, China" pe zoom karo (dry terrain aur mountains ke clue se).
  - **Step 2:** Features add karo:
    * "Railway" (pre-set).
    * "Wind Turbine" (custom tag: `generator:source=wind`).
  - **Step 3:** Search karo – tool 100 tak results deta hai. Ek pin pe railway ke saath wind farm dikhta hai.
  - **Step 4:** Pin ke coordinates (e.g., 43.1234° N, 87.5678° E) Google Earth pe kholo – mountains aur terrain match karte hain.
  - **Result:** Photo Xinjiang ke ek wind farm ke paas li gayi hai.
- **Fayda:** Complex Overpass-Turbo queries ki zarurat nahi – simple interface ke saath OSM ka full power milta hai.
- **Note:**
  - Max 100 results milte hain – bada area ho to narrow down karna padta hai.
  - OSM data latest edit tak current hai (Bellingcat tool April 2023 se updated, twice yearly refresh).

Extra Tips:

- **OSM Tags Samjho:** OSM wiki (**wiki.openstreetmap.org**) pe check karo kaise objects tagged hain (e.g., wind turbine = `generator:source=wind`).
- **Export:** Results CSV ya KML file mein download karo – Google Earth ke liye useful.
- **Combine:** Bellingcat Map ke leads ko Google Earth ya Street View se verify karo.

Tables

Feature	Use	Limitation
OSM Data	Detailed Search	Max 100 Results
Multi-Landmark	Narrow Down	Needs Clues
Simple Interface	Easy Query	Twice Yearly Update

Table 62: Bellingcat Map Features

Summary

- Bellingcat Map se OSM query karo.
- Landmarks se locations narrow karo.
- Google Earth se verify – geolocation complete.

Point To Note

Bellingcat Map (**osm-search.bellingcat.com**) OSM data ke saath geolocating ke liye ek zabardast tool hai – image ke landmarks ya features se starting points deta hai. Aapka content sahi tha, maine steps aur ek practical example add kiya taaki OSINT mein iska use clear ho. Ye tool jab visual clues hain lekin location nahi pata, tab game-changer hai – try karo aur refine karte jao!

==========

Extract Additional Info Using Google Earth

Google Earth OSINT ke liye ek versatile tool hai jo geolocation aur contextual analysis mein extra info deta hai. Ye dusre maps (jaise Google Maps, Bing Maps) se alag features offer karta hai – historical imagery, 3D views, aur terrain details. Chalo dekhte hain kaise use karna hai aur kya extra milta hai.

How to Use Google Earth for OSINT

- **Kya Hai:** Google Earth ek desktop/web-based platform hai jo satellite imagery, 3D models, aur historical data ke saath locations ko deeply analyze karne deta hai.
- **Kaise Use Karein:**
  1. **Google Earth Pro** download karo (free) ya web version (**earth.google.com**) kholo.
  2. Coordinates daalo (e.g., 43.1234° N, 87.5678° E from Bellingcat Map) ya location search karo.
  3. Features explore karo:
     - **Zoom In:** Satellite imagery aur ground-level view.
     - **Historical Imagery:** Toolbar pe clock icon se purane satellite shots dekho.
     - **3D Mode:** Tilt karke buildings/terrain ka angle check karo.
  4. Image se match karo – landmarks, shadows, ya changes note karo.
- **Example:**
  - **Image:** Ek photo jisme ek wind farm hai, railway line, aur mountains.
  - **Step 1:** Bellingcat Map se coordinates lo – 43.1234° N, 87.5678° E.
  - **Step 2:** Google Earth pe jao, coordinates enter karo.
  - **Step 3:**
    - Satellite: Wind turbines aur railway visible.
    - Historical Imagery: 2018 ka shot dekho – construction phase dikhta hai.

    * 3D View: Mountains ka shape photo se match karta hai.
  - **Result:** Location confirm hoti hai, plus extra info – wind farm 2019 ke baad complete hua.

Extra Features Compared to Other Maps

1. **Historical Imagery:**
   - **Google Earth:** 10-20 saal purani satellite images – time-based changes track karo (e.g., construction, destruction).
   - **Vs. Others:** Google Maps/Bing Maps mein sirf latest imagery – no history.
2. **3D Terrain and Buildings:**
   - **Google Earth:** Tilt aur rotate karke realistic 3D views – height, angles, shadows analyze karo.
   - **Vs. Others:** Bing ka Bird's Eye 45° tak hai, lekin Google Earth jaisa flexibility nahi; Yandex flat hi rehta hai.
3. **Ground-Level View:**
   - **Google Earth:** Street View integrate karta hai + virtual ground perspective – photo ke angle se match karo.
   - **Vs. Others:** Google Maps pe Street View hai, lekin Bing/Yandex mein coverage kam.
4. **Measurement Tools:**
   - **Google Earth:** Distances, areas measure karo – OSINT ke liye scale samajhne mein help.
   - **Vs. Others:** Basic maps mein ye rare hai.
5. **KML Support:**
   - **Google Earth:** Bellingcat Map se KML import karke pins visualize karo.
   - **Vs. Others:** Limited ya nahi hota.
6. **Fayda:** Google Earth time, depth, aur perspective deta hai jo static maps nahi de sakte – OSINT ke liye verification aur context ka powerhouse.
7. **Note:** High-res imagery har jagah nahi – rural areas mein blurry ho sakta hai.

Extra Tips:

- **Timeline Play:** Historical slider se changes ka video jaise dekho.
- **Shadows:** Sun angle check karo (date/time daal kar) – photo ke time se match karo.
- **Save:** KML file banao – team ke saath share karo.

Feature	Google Earth	Other Maps
Historical Imagery	10-20 Years	Latest Only
3D Views	Full Tilt/Rotate	Limited Angles
Measurement	Distance/Area	Rare

Table 63: Google Earth vs. Other Maps

Tables

Summary

- Historical imagery se time track karo.
- 3D views se angles analyze karo.
- Extra context ke liye Google Earth chuno.

Point To Note

Google Earth (**earth.google.com**) OSINT ke liye ek must-have hai – **historical imagery**, **3D views**, aur **terrain analysis** jaise extra features ke saath locations ko deeply investigate karta hai. Aapka content base ke roop mein kaam kiya, maine ise practical steps aur comparisons se enrich kiya. Ye dusre maps se zyada info deta hai – geolocation ke baad context aur history ke liye ise zaroor use karo!

==========

Introduction to Website OSINT

Website OSINT (Open Source Intelligence) websites ke data ko analyze karke valuable intelligence gather karne ka ek tareeka hai. Isme aap public sources se info collect karte ho – jaise domain ownership, structure, aur connections – taaki target ke digital presence ko samajh sako. Is process ka ek key part hai **WHOIS records**, jo domain names ke ownership ki details dete hain. Saath hi, tools jaise **OSINT.SH** website investigation ke liye ek all-in-one solution hai, jisme **subdomain finder**, **DNS history**, **reverse IP**, aur **reverse email lookup** jaise features hain. Ye tools aapko website ke peeche ki kahani – owner, history, aur network – samajhne mein madad karte hain. Chalo isko step-by-step explore karte hain – WHOIS se shuru karke OSINT.SH ke tools tak.

WHOIS Records

- **Kya Hai:** WHOIS record ek public database entry hai jo batata hai ki ek domain name (e.g., example.com) ka malik kaun hai. Ye internet ke registry system ka hissa hai, jisme har domain ke registration ki details hoti hain.
- **Har Record Mein Kya Hota Hai:**
  - **Domain Owner's Name and Contact Details:** Owner ka naam, email, phone number, aur address (agar public hai).
  - **Registration and Expiration Dates:** Domain kab register hua, kab update hua, aur kab expire hoga.
  - **Domain Registrar Info:** Registrar (jaise GoDaddy, Namecheap) ka naam aur contact details.

- **Website Example – https://who.is:**
  - **Kaise Use Karein:** Who.is pe jao, domain name daalo (e.g., "google.com").
  - **Kya Milega:**
    - **Registered Date:** Kab domain bana – e.g., "1997-09-15" (Google ka case).
    - **Updated On:** Last update kab hua – e.g., "2023-08-10".
    - **Expires On:** Kab expire hoga – e.g., "2028-09-14".
    - **Registrar Info:** Registrar ka naam (e.g., MarkMonitor Inc.), phone number (+1-208-389-5740), country (USA), city (Boise), address (123 Main St).
  - **Explanation:**
    - **Registered Date:** Domain ki age batata hai – purana domain zyada trusted hota hai.
    - **Updated On:** Recent changes – jaise ownership ya contact update.
    - **Expires On:** Agar expire hone wala hai, to owner active nahi ho sakta.
    - **Registrar Info:** Registrar se contact kar sakte ho agar owner details chahiye.

- **Note – Domain Privacy:**
  - Zyadatar websites **domain privacy** use karti hain – ye ek service hai jo domain registrars (e.g., Namecheap) dete hain. Isse owner ka naam, email, phone, aur address WHOIS record mein chhup jata hai aur registrar ka generic data dikhta hai (e.g., "PrivacyGuard Inc., privacy@domain.com").
  - Example: Agar "rishi.com" pe privacy on hai, to WHOIS mein "Rishi Kabra" ki jagah "GoDaddy Privacy Service" dikhega.

OSINT.SH – A Key Website for Investigation

- **Kya Hai:** OSINT.SH ek all-in-one OSINT platform hai jo website-related investigations ke liye number of tools deta hai. Ye domain, IP, aur digital footprint analysis ke liye ek must-have resource hai.

- **Tools aur Simple Explanation:**

1. **Subdomain Finder (osint.sh/subdomain):**
   - **Kya Karta Hai:** Ek domain ke subdomains dhoondhta hai (e.g., mail.google.com, drive.google.com).
   - **Example:** "google.com" daalo – Results: "maps.google.com", "news.google.com".
   - **Kab Use Karein:** Website ke hidden parts ya internal systems (e.g., admin portals) dhoondhne ke liye – security ya recon ke liye useful.
2. **DNS History (osint.sh/dnshistory):**
   - **Kya Karta Hai:** Domain ke DNS records ka past data deta hai – jaise IP addresses ya nameservers jo pehle use hue.
   - **Example:** "facebook.com" – Old IP: 192.168.1.1 (2015), New IP: 157.240.241.35 (2023).
   - **Kab Use Karein:** Pata lagane ke liye ki domain ka infrastructure ya hosting kab aur kaise badla – ownership changes ya migrations track karne ke liye.
3. **Reverse IP (osint.sh/reverseip):**

- **Kya Karta Hai:** Ek IP address se saare domains dhoondhta hai jo uspe hosted hain.
- **Example:** IP "104.244.42.1" daalo – Results: "twitter.com", "x.com" (same server pe).
- **Kab Use Karein:** Ek server pe kitne websites hain aur unke connections samajhne ke liye – phishing ya related sites dhoondhne mein helpful.

4. **Reverse Email Lookup (osint.sh/reversewhois):**
   - **Kya Karta Hai:** Ek email address se saare registered domains dhoondhta hai.
   - **Example:** "rishi.kabra@gmail.com" daalo – Results: "rishi.com", "kabratech.com".
   - **Kab Use Karein:** Jab aapko owner ke email pata ho aur uske saare domains chahiye – identity ya network mapping ke liye critical.
5. **WHOIS History (osint.sh/whoishistory):**
   - **Kya Karta Hai:** Domain ke past WHOIS records dikhata hai – pehle kaun owner tha, kab badla.
   - **Example:** "example.com" – 2018: John Doe, 2022: PrivacyGuard.
   - **Kab Use Karein:** Privacy on hone se pehle ka data dhoondhne ke liye – ownership changes track karne mein fayda.
6. **Technology Lookup (osint.sh/stack):**
   - **Kya Karta Hai:** Website ke tech stack batata hai – jaise WordPress, Apache, Cloudflare.
   - **Example:** "bbc.com" – Tech: Nginx, AWS.
   - **Kab Use Karein:** Target ke infrastructure samajhne ya vulnerabilities dhoondhne ke liye.
7. **Certificate Search (osint.sh/cert):**
   - **Kya Karta Hai:** SSL certificates se domains aur subdomains dhoondhta hai.
   - **Example:** "google.com" – Certs: "mail.google.com", "drive.google.com".
   - **Kab Use Karein:** Hidden subdomains ya related domains ke liye – security audits mein kaam aata hai.

- **Aur Bhi Tools:**
  - **DNS Lookup:** Domain ke current DNS records (A, MX, NS).
  - **Email Finder:** Website se emails extract karta hai.
  - **Reverse MX/NS:** Mail ya nameserver se linked domains dhoondhta hai.
  - **OCR Text Extractor:** Images/PDFs se text nikaalta hai – metadata ke liye useful.
- **When to Use OSINT.SH Tools:**
  - **Investigation Start:** Subdomain Finder aur WHOIS History se domain ka basic footprint lo.
  - **Deep Dive:** Reverse IP aur Certificate Search se network aur hidden assets dhoondho.
  - **Identity Mapping:** Reverse Email Lookup se owner ke saare domains track karo.
  - **Tech Analysis:** Technology Lookup se website ka backend samajho.

Workflow Example:

- **Target:** "techmojo.com"
- **WHOIS (who.is):**
  - Registered: 2020-05-10, Expires: 2025-05-10, Registrar: Namecheap (privacy on).
- **OSINT.SH:**
  - Subdomain Finder: "blog.techmojo.com", "app.techmojo.com".
  - DNS History: 2021 IP – 192.168.1.1, 2023 IP – 104.21.32.45.
  - Reverse IP: "techmojo.com" aur "mojotech.in" same IP pe.
  - Reverse Email (rishi@techmojo.com): "kabratech.com" bhi mila.
- **Conclusion:** Techmojo ka owner Rishi ho sakta hai, jo multiple domains chala raha hai.

Extra Tips:

- **Privacy Bypass:** Agar WHOIS mein privacy hai, to OSINT.SH ke WHOIS History ya Reverse Email se past data lo.
- **Cross-Check:** Subdomains ko SignalHire se LinkedIn profiles ke saath match karo.
- **Save:** Notion mein table banao:

Domain	Subdomains	IP	Owner Info	Tool
techmojo.com	blog, app	104.21.32.45	rishi@techmojo	OSINT.SH

Tables

Tool	Function	Use Case
Subdomain Finder	Finds Subdomains	Hidden Pages
Reverse IP	Domains on IP	Network Links
Reverse Email	Domains by Email	Owner Tracking

Table 64: OSINT.SH Tools Overview

Summary

- WHOIS se ownership lo.
- OSINT.SH se network aur history nikalo.
- Findings save karo – deep insights ke liye.

Point To Note

Website OSINT ki shuruaat **WHOIS records** se hoti hai – **who.is** pe domain name daal kar registration, expiration, aur registrar info lo. Privacy on hone par bhi **OSINT.SH** jaise platforms se **subdomain finder**, **DNS history**, **reverse IP**, aur **reverse email lookup** jaise tools ke saath deep insights milte hain. Ye tools simple hain – subdomain se hidden pages, reverse IP se network, aur email se owner tak le jate hain. Har finding ko Notion mein save karo – ye systematic approach website ke intelligence ko pura khol deta hai!

==========

Identifying Technologies Used in a Website

Identifying technologies used in a website ek crucial skill hai jo aapko website ke **infrastructure** aur **security posture** ko samajhne mein madad karti hai. Ye process batata hai ki website kaise bani hai aur usmein kaunsi vulnerabilities ho sakti hain. Aapko isse **CMS (Content Management System)**, **LMS (Learning Management System)**, **plugins**, aur aur bhi technical components – jaise server-side languages, client-side languages, aur JavaScript libraries – ke baare mein info mil sakti hai. Iske liye aap teeno powerful tools ka use kar sakte ho: **OSINT.SH** (technology lookup), **BuiltWith** (detailed tech profiling), aur **Wappalyzer** (browser extension). Chalo step-by-step dekhte hain kaise ye tools website technologies ko identify karte hain, ek example domain – **zsecurity.org** – ke saath.

Why Identify Website Technologies?

- **Infrastructure Insight:** Website kaunse tools aur frameworks pe chalta hai – jaise WordPress ya custom PHP code – ye samajhna development aur hosting ka idea deta hai.
- **Security Posture:** Outdated CMS, plugins, ya libraries vulnerabilities expose kar sakte hain – jaise unpatched WordPress plugins ya old jQuery versions.
- **Competitor Analysis:** Rivals ke tech stack ko jaan kar aap apne projects ko optimize kar sakte ho.

Information You Can Find:

- **CMS (Content Management System):** WordPress, Joomla, Drupal – content kaise manage hota hai.
- **LMS (Learning Management System):** Moodle, Blackboard – agar educational platform hai.
- **Plugins:** Add-ons jaise Yoast SEO, WooCommerce – extra functionality ke liye.
- **Server-Side Languages:** PHP, Python, Ruby – backend logic ke liye.
- **Client-Side Languages:** HTML, CSS, JavaScript – frontend rendering ke liye.
- **JavaScript Libraries:** jQuery, React, Vue.js – dynamic features ke liye.
- **Other Tech:** Hosting (AWS, Cloudflare), analytics (Google Analytics), frameworks (Laravel, Django).

Tools to Identify Website Technologies:

1. **OSINT.SH – Technology Lookup (osint.sh/stack)**

- **Kya Hai:** OSINT.SH ek free OSINT platform hai jo website ke tech stack ko analyze karta hai – simple aur effective.
- **Kaise Use Karein:**
  (a) **osint.sh/stack** pe jao.
  (b) Domain name daalo – e.g., "zsecurity.org".
  (c) Search karo – ye pura tech breakdown deta hai.
- **Output Example (zsecurity.org):**
  - **CMS:** WordPress
  - **Server-Side Language:** PHP
  - **Client-Side Language:** JavaScript
  - **JavaScript Libraries:** jQuery
  - **Hosting:** Cloudflare
- **Fayda:** Ek hi jagah pe CMS, languages, aur libraries mil jate hain – quick recon ke liye perfect.
- **Kab Use Karein:** Jab aapko basic tech stack chahiye without deep dive.

2. **BuiltWith (builtwith.com)**

- **Kya Hai:** BuiltWith ek detailed technology profiling tool hai jo website ke har component ko dissect karta hai – 101,000+ technologies track karta hai.
- **Kaise Use Karein:**
  (a) **builtwith.com** pe jao.
  (b) Domain daalo – e.g., "zsecurity.org".
  (c) Results dekho – comprehensive report milega.
- **Output Example (zsecurity.org):**
  - **CMS:** WordPress (version 6.4)
  - **Plugins:** WooCommerce, Elementor
  - **Server-Side:** PHP 8.1
  - **Client-Side:** JavaScript, CSS
  - **Libraries:** jQuery 3.6.0
  - **Analytics:** Google Analytics
  - **Hosting:** AWS
- **Fayda:** Version numbers, plugins, aur trends tak deta hai – competitor analysis ya vuln research ke liye best.
- **Kab Use Karein:** Jab aapko granular details chahiye – jaise exact plugin versions ya hosting provider.

3. **Wappalyzer – Browser Extension**

- **Kya Hai:** Wappalyzer ek Chrome/Firefox extension hai jo real-time mein website technologies detect karta hai – 1,000+ tech categories cover karta hai.
- **Kaise Use Karein:**
  (a) Chrome Web Store se "Wappalyzer" install karo.

(b) Website kholo (e.g., zsecurity.org).

(c) Toolbar mein Wappalyzer icon pe click karo – instant tech list milegi.

- **Output Example (zsecurity.org):**
  - **CMS:** WordPress
  - **Server-Side Language:** PHP
  - **Client-Side Language:** JavaScript
  - **JavaScript Libraries:** jQuery
  - **CDN:** Cloudflare
- **Fayda:** Browser mein hi instant results – no extra navigation. Free version mein bhi kaafi info milti hai.
- **Kab Use Karein:** Jab aap browsing ke dauraan quick tech check karna chahte ho.

Workflow Example – zsecurity.org:

- **OSINT.SH:**
  - Input: zsecurity.org
  - Result: WordPress, PHP, jQuery, Cloudflare.
- **BuiltWith:**
  - Result: WordPress 6.4, PHP 8.1, WooCommerce, Google Analytics, AWS.
- **Wappalyzer:**
  - Result: WordPress, PHP, JavaScript, jQuery, Cloudflare.
- **Conclusion:** zsecurity.org ek WordPress-based site hai jo PHP pe chalti hai, jQuery use karti hai, aur Cloudflare/AWS se host hoti hai – consistent results teeno tools se.

Extra Tips:

- **Cross-Check:** Teeno tools ke results compare karo – BuiltWith versions deta hai, Wappalyzer speed, aur OSINT.SH simplicity.
- **Security Angle:** Outdated tech (e.g., old PHP ya jQuery) ko CVE databases (**cve.mitre.org**) pe check karo vulnerabilities ke liye.
- **Save Results:** Notion mein table banao:

Domain	CMS	Languages	Libraries	Hosting	Tool
zsecurity.org	WordPress	PHP, JavaScript	jQuery	Cloudflare	OSINT.SH

- **Expand:** Plugins ya CMS mila to WhatCMS.org ya WPScan se aur details lo.

Tool	Strength	Use Case
OSINT.SH	Quick Lookup	Basic Recon
BuiltWith	Detailed Versions	Vuln Research
Wappalyzer	Instant Results	Browsing Check

Table 65: Website Technology Tools Comparison

Tables

Summary

- OSINT.SH se basic stack lo.
- BuiltWith se versions aur plugins nikalo.
- Wappalyzer se instant check – full picture banao.

Point To Note

Website technologies identify karne ke liye **OSINT.SH** se basic lookup shuru karo – domain (zsecurity.org) daal kar CMS, PHP, jQuery jaise results lo. **BuiltWith** se deep dive karo – plugins, versions, aur analytics tak jao. **Wappalyzer** extension se browsing ke saath instant check karo. Ye teeno tools saath mein website ke **infrastructure** (CMS, LMS, plugins) aur **security posture** ko samajhne ka complete package dete hain. Har finding ko save karo – ye info recon, vuln hunting, ya competitor analysis ke liye game-changer hai! Systematic kaam karo aur teeno ka mix use karo best results ke liye.

==========

Discovering Subdomains

Discovering subdomains website OSINT ka ek important hissa hai jo aapko ek domain ke hidden ya separate sections ko uncover karne mein madad karta hai. Ek **subdomain** main domain name ka ek prefix hota hai jo website ke alag-alag parts ko represent karta hai – jaise **www.cybersudo.org** (main site) aur **academy.cybersudo.org** (training section). Subdomains dhoondhne ke liye tools jaise **OSINT.SH** ka **Subdomain Finder** kaafi effective hai. Lekin ek hi tool puri list nahi deta, isliye **multiple subdomain finders** ya **Google Dorks** ka use karna zaroori hai taaki saare subdomains mil sakein. Chalo is process ko step-by-step samajhte hain – OSINT.SH se lekar Google Dorks tak – aur dekhte hain kaise subdomains discover kiye jate hain.

What is a Subdomain?

- Subdomain ek domain ka ek chhota hissa hota hai jo main domain (e.g., cybersudo.org) ke saath juda hota hai aur alag-alag purposes ke liye banaya jata hai.
- **Examples:**
  - **www.cybersudo.org:** Main website.
  - **academy.cybersudo.org:** Training ya courses ke liye.
  - **blog.cybersudo.org:** Blog section.
- Ye alag-alag servers pe host ho sakte hain aur unique content ya functionality dete hain.

Why Discover Subdomains?

- **Hidden Sections:** Admin portals (admin.cybersudo.org) ya internal tools (dev.cybersudo.org) dhoondhne ke liye – security testing ya recon ke liye useful.
- **Full Footprint:** Website ka pura digital presence samajhne ke liye – subdomains se ownership ya related projects ka pata chal sakta hai.
- **Vulnerabilities:** Subdomains outdated tech ya weak security pe chalte hain – attack surface badhane ke liye info milti hai.

How to Discover Subdomains:

1. **OSINT.SH – Subdomain Finder (osint.sh/subdomain)**
   - **Kya Hai:** OSINT.SH ka Subdomain Finder tool domain ke subdomains ko scan karta hai – public DNS records aur OSINT sources ka use karta hai.
   - **Kaise Use Karein:**
     (a) **osint.sh/subdomain** pe jao.
     (b) Domain name daalo – e.g., "cybersudo.org".
     (c) Search karo – subdomains ki list milegi.
   - **Output Example:**
     – Domain: cybersudo.org
     – Subdomains:
       * www.cybersudo.org
       * academy.cybersudo.org
       * login.cybersudo.org
   - **Fayda:** Free, fast, aur beginner-friendly – DNS-based subdomains ke liye solid starting point.
   - **Note:** Ye sirf public ya known subdomains deta hai – hidden ya unindexed subdomains miss ho sakte hain.
2. **Why Use Multiple Subdomain Finders?**
   - Ek tool (jaise OSINT.SH) puri list nahi deta kyunki:
     – **Data Sources:** Har tool alag-alag DNS records, certificates, ya crawling methods pe depend karta hai.
     – **Coverage:** Kuch subdomains private DNS pe hote hain ya search engines mein indexed nahi hote.
   - **Other Tools to Combine:**
     – **Sublist3r (github.com/aboul3la/Sublist3r):** Bruteforce aur OSINT se subdomains dhoondhta hai.
     – **Censys (censys.io):** SSL certificates se subdomains extract karta hai.
     – **crt.sh (crt.sh):** Certificate transparency logs se subdomains deta hai – e.g., "cybersudo.org" ke liye "api.cybersudo.org".
   - **Example:** OSINT.SH se "academy.cybersudo.org" mila, lekin Sublist3r se "dev.cybersudo.org" bhi mila jo OSINT.SH miss kar gaya.
3. **Google Dorks to Find Subdomains**

- **Kya Hai:** Google Dorks search operators ka use karke subdomains dhoondhne ka manual tareeka hai – Google ke indexed pages se results milte hain.
- **Syntax:**
  - **site:cybersudo.org** – Ye cybersudo.org ke saare indexed pages dikhata hai, including subdomains.
  - **site:*.cybersudo.org -inurl:(www)** – WWW ke alawa baaki subdomains dikhata hai.
- **Kaise Use Karein:**
  (a) Google pe jao.
  (b) "site:cybersudo.org" type karo aur search karo.
  (c) Results mein subdomains dekho – jaise "academy.cybersudo.org", "blog.cybersudo.org".
- **Output Example:**
  - site:cybersudo.org
  - Results:
    * www.cybersudo.org
    * academy.cybersudo.org
    * support.cybersudo.org (Google ne index kiya tha).
- **Fayda:** Free aur manual control – indexing pe depend karta hai, to unique subdomains mil sakte hain.
- **Note:** Sirf Google ke indexed subdomains hi milenge – unindexed ya private subdomains nahi aayenge.

Workflow Example – cybersudo.org:

- **OSINT.SH Subdomain Finder:**
  - Input: cybersudo.org
  - Result: www.cybersudo.org, academy.cybersudo.org, login.cybersudo.org.
- **Sublist3r (Multiple Finder):**
  - Result: dev.cybersudo.org, api.cybersudo.org (OSINT.SH se miss hue).
- **Google Dorks:**
  - Query: "site:*.cybersudo.org -inurl:(www)"
  - Result: support.cybersudo.org, blog.cybersudo.org.
- **Conclusion:** Total 7 subdomains mile – OSINT.SH ne 3, Sublist3r ne 2 extra, aur Google Dorks ne 2 aur dikhaye.

Extra Tips:

- **Combine Tools:** OSINT.SH ke saath crt.sh ya Censys use karo – certificate-based subdomains bhi cover honge.
- **Verify:** Subdomains ko browser mein kholo – active hai ya nahi check karo.
- **Save Results:** Notion mein table banao:
- **Expand:** Subdomains ke IP ko Reverse IP (OSINT.SH) se check karo – aur domains ya connections mil sakte hain.

Domain	Subdomains	Source
cybersudo.org	www, academy, dev, api	OSINT.SH, Sublist3r

Tables

Method	Strength	Limitation
OSINT.SH	Fast, Free	Public Only
Multiple Finders	Broad Coverage	Tool Setup
Google Dorks	Manual Control	Indexed Only

Table 66: Subdomain Discovery Methods Comparison

Summary

- OSINT.SH se basic subdomains lo.
- Multiple finders se coverage badhao.
- Google Dorks se indexed subdomains – full list banao.

Point To Note

Subdomains discover karne ke liye **OSINT.SH** ka **Subdomain Finder** use karo – "cybersudo.org" daal kar www, academy jaise results lo. Ek tool puri picture nahi deta, isliye **multiple finders** (Sublist3r, crt.sh) aur **Google Dorks** ("site:cybersudo.org") combine karo – har tool alag angle se subdomains dikhata hai. Ye method website ke hidden sections – jaise dev.cybersudo.org ya api.cybersudo.org – ko expose karta hai. Har subdomain ko Notion mein save karo – ye website OSINT ke liye ek solid base deta hai, bas systematic aur multi-source approach rakho!

==========

Extracting Information from DNS Records

Extracting information from DNS records website OSINT ka ek powerful technique hai jo aapko domain ke baare mein critical details uncover karne mein madad karta hai. **DNS records** instructions hote hain jo DNS servers mein rehte hain aur ek domain ke functionality aur infrastructure ke baare mein batate hain – jaise IP addresses, mail servers, aur subdomains. Ye records publicly accessible hote hain aur tools jaise **DNSDumpster.com** aur **OSINT.SH** ke zariye inko analyze karke aap domain ke network, hosting, aur connections ka pata laga sakte ho. Chalo is process ko step-by-step samajhte hain – DNS records kya hote hain, inmein kya info hoti hai, aur kaise **DNSDumpster** aur **OSINT.SH** se ye data extract kiya jata hai.

What Are DNS Records?

- DNS (Domain Name System) records ek domain ke digital roadmap ki tarah hote hain – ye batate hain ki domain ka traffic kahan jata hai aur kaise handle hota hai.
- Ye records DNS servers pe store hote hain aur publicly query kiye ja sakte hain.

- **Common DNS Record Types:**
  - **A (Address):** Domain ka IP address – e.g., cybersudo.org → 192.168.1.1.
  - **MX (Mail Exchange):** Mail servers – e.g., mail.google.com for Gmail.
  - **CNAME (Canonical Name):** Alias domains – e.g., www.cybersudo.org → cybersudo.org.
  - **TXT:** Text info – SPF records ya verification codes ke liye.
  - **NS (Name Server):** DNS servers jo domain ko manage karte hain – e.g., ns1.namecheap.com.

Why Extract Info from DNS Records?

- **Infrastructure Mapping:** Hosting provider, server locations, aur subdomains ka pata chalta hai.
- **Security Insights:** Misconfigured records ya exposed servers vulnerabilities dikhate hain.
- **Connections:** Related domains ya third-party services (e.g., Cloudflare, AWS) ke links milte hain.

Tools to Extract Information from DNS Records:

1. **DNSDumpster.com**
   - **Kya Hai:** DNSDumpster ek free online tool hai jo DNS reconnaissance ke liye banaya gaya hai – domain ke DNS records, subdomains, aur network map deta hai.
   - **Kaise Use Karein:**
     (a) dnsdumpster.com pe jao.
     (b) Domain name daalo – e.g., "cybersudo.org".
     (c) Search karo – DNS records aur visual map milega.
   - **Output Example (cybersudo.org):**
     - **A Record:** cybersudo.org → 104.21.32.45 (IP address).
     - **MX Record:** mail.cybersudo.org → 10 mx1.google.com (mail server).
     - **TXT Record:** "v=spf1 include:$_spf.google.com\ all$"($SPF for email security$).**Subdomains**
– **Visual Map:** IP aur subdomains ka network graph.
   - **Fayda:** Ek hi jagah pe DNS records, subdomains, aur hosting info – visual map se connections samajhna asaan hota hai.
   - **Kab Use Karein:** Jab aapko quick DNS overview aur subdomain list chahiye – beginner-friendly.

2. **OSINT.SH – DNS Lookup (osint.sh/dns)**
   - **Kya Hai:** OSINT.SH ek all-in-one OSINT platform hai jo DNS Lookup tool ke zariye domain ke current DNS records extract karta hai – simple aur detailed output deta hai.
   - **Kaise Use Karein:**
     (a) osint.sh/dns pe jao.
     (b) Domain daalo – e.g., "cybersudo.org".
     (c) Search karo – records ki list milegi.

- **Output Example (cybersudo.org):**
  - **A Record:** cybersudo.org → 104.21.32.45.
  - **NS Record:** ns1.namecheap.com, ns2.namecheap.com.
  - **MX Record:** 10 mx1.google.com.
  - **TXT Record:** "google-site-verification=abc123".
- **Fayda:** Clean aur structured output – specific record types pe focus karne ke liye perfect.
- **Kab Use Karein:** Jab aapko raw DNS data chahiye ya specific records (MX, TXT) analyze karne hain.

What Information Can You Extract?

- **IP Address (A):** Hosting server ka location – e.g., 104.21.32.45 Cloudflare ka hai.
- **Mail Servers (MX):** Email provider – Google, Microsoft, ya custom.
- **Subdomains:** Hidden sections – academy.cybersudo.org se training platform ka hint.
- **Name Servers (NS):** Registrar ya hosting provider – Namecheap, GoDaddy.
- **TXT Records:** Security settings (SPF, DKIM) ya verification codes – third-party services ka pata chalta hai.

Workflow Example – cybersudo.org:

- **DNSDumpster:**
  - Input: cybersudo.org
  - Result:
    - A: 104.21.32.45
    - MX: mail.cybersudo.org → mx1.google.com
    - Subdomains: www, academy, login
    - Map: IP aur subdomains ka visual link.
- **OSINT.SH:**
  - Result:
    - A: 104.21.32.45
    - NS: ns1.namecheap.com
    - TXT: "v=spf1 include:$_{s}pf.google.com$".
- **Conclusion:** Cybersudo.org Cloudflare pe host hai, Google se email chalta hai, aur Namecheap se registered hai – subdomains se training (academy) aur login sections mile.

Extra Tips:

- **Combine Tools:** DNSDumpster se visual map lo, OSINT.SH se raw data – dono saath mein complete picture dete hain.
- **Cross-Check:** IP ko Reverse IP (OSINT.SH) pe daalo – aur domains ya hosting connections milenge.
- **Google Dorks:** "site:*.cybersudo.org" se indexed subdomains bhi lo – DNS se miss hue sections mil sakte hain.
- **Save Results:** Notion mein table banao:

Domain	A Record	MX Record	Subdomains	Source
cybersudo.org	104.21.32.45	mx1.google.con	www, academy	DNSDumpster

Tables

Summary

- DNSDumpster se map aur subdomains lo.
- OSINT.SH se raw records extract karo.
- Combine karke full infra samjho.

Point To Note

DNS records se info extract karne ke liye **DNSDumpster.com** aur **OSINT.SH** ka use karo – DNSDumpster visual map aur subdomains deta hai, jabki OSINT.SH clean records provide karta hai. Ye tools domain ke IP, mail servers, subdomains, aur hosting ko reveal karte hain – jaise cybersudo.org ka Cloudflare aur Google connection. Har detail ko Notion mein save karo – ye method website ke infrastructure ko samajhne ka ek solid tareeka hai. Systematic approach rakho aur dono tools ko combine karke maximum intelligence lo!

==========

Tracking a Website's Changes and Updates

Tracking a website's changes and updates ek valuable OSINT technique hai jo aapko websites ke past versions ko explore karne aur unke evolution ko samajhne mein madad karta hai. **Wayback Machine**, jo **Internet Archive** ka hissa hai, 800 billion se zyada web pages ko time ke saath save karta hai – ye ek digital time capsule ki tarah kaam karta hai. Iske OSINT usage mein websites ke purane roop dekhna, **deleted information retrieve** karna, aur **web pages ke changes track** karna shamil hai. Har website jo create hoti hai, uska snapshot Wayback Machine mein save ho sakta hai, aur agar owner kuch change karta hai – jaise personal email hata deta hai – to bhi aap past version dekh sakte ho. Ye tool na sirf websites, balki **tweets**, **Facebook posts**, aur **Instagram posts** jaise social media data bhi archive karta hai. Chalo isko step-by-step samajhte hain – kaise Wayback Machine se website changes aur deleted info track ki jati hai, examples ke saath.

What is the Wayback Machine?

- **Wayback Machine** Internet Archive (**archive.org**) ka ek tool hai jo websites ke historical snapshots save karta hai – 1996 se lekar aaj tak ka data rakhta hai, over 800 billion pages ke saath.
- **Internet Archive:** Ye ek huge library hai jisme websites, music, videos, books, aur software ka collection hota hai – ek public digital archive.
- Jab bhi ek website create hoti hai ya update hoti hai, Wayback Machine uska snapshot le sakta hai – matlab aap past mein wapas jaakar dekh sakte ho ki website pehle kaisi thi.

OSINT Usage of Wayback Machine:

- **View Websites as They Appeared in the Past:** Historical look dekhne ke liye – design, content, ya info jo ab nahi hai.
- **Retrieve Deleted Information:** Kuch delete ho gaya ho (email, phone number), to purana version se wapas lo.
- **Track Changes Over Time:** Website ke updates, ownership changes, ya content shifts ka pata lagao.

Example Scenario:

- Maan lo Rishi Kabra ke paas ek website hai – **rishikabra.com**. Jab usne site banayi, to usmein apna personal email (rishi.kabra@gmail.com) daala tha. Baad mein privacy ke liye usne email hata diya. Wayback Machine se aap purana version dekhkar email wapas dhoondh sakte ho.

How to Use Wayback Machine:

1. **Go to the Website:**
   - **URL: https://archive.org**
   - Ye Internet Archive ka homepage hai, jahan se Wayback Machine accessible hai.
2. **Search the Website:**
   - Search box mein target website ka URL daalo – e.g., **zsecurity.org**.
   - Result: "Saved 111 times between August 9, 2018, and June 3, 2024" – matlab is domain ke 111 snapshots save hue hain.
3. **Explore Historical Snapshots:**
   - Calendar view mein years dikhte hain – —**2001**—**2002**—. . . —**2019**—. . . —**2024**—
   - Kisi year pe click karo, phir month aur date chuno (e.g., "March 15, 2021").
   - Website ka us din ka version load hoga – jaise zsecurity.org pehle kaisa tha.
   - **Output Example:**
     – March 15, 2021: zsecurity.org pe old courses list thi jo ab nahi hai.
4. **Retrieve Deleted Info:**
   - Agar Rishi ne **rishikabra.com** se email hata diya, to 2019 ka snapshot check karo – "Contact: rishi.kabra@gmail.com" wahan mil sakta hai.

Tracking Social Media with Wayback Machine:

- **Note:** Wayback Machine sirf websites nahi, balki **Twitter**, **Facebook**, aur **Instagram posts** ke snapshots bhi save karta hai – agar URL public tha aur crawl hua tha.
- **Scenario:** Maan lo ek Twitter account (@rishikabra132) delete ho gaya, aur uske tweets gayab hain.
- **Kaise Use Karein:**
  1. Purana Twitter URL lo – **https://twitter.com/rishikabra132** (Note: X se pehle Twitter tha, to "twitter.com" use karo).

2. Wayback Machine search box mein paste karo.
3. Result: "34 URLs have been captured for this URL prefix" – 34 snapshots hain, dates ke saath (e.g., Jan 2018 to Dec 2022).
4. Har link kholo – purane tweets, bio, aur profile pics dikhte hain.

- **Output Example:**
  - Snapshot (June 2020): Tweet – "Just launched my site rishikabra.com!"
  - Bio: "Rishi Kabra, Mumbai, rishi.kabra@gmail.com".
- **Fayda:** Deleted accounts ka data wapas mil sakta hai – tweets ya posts jo ab live nahi hain.

Workflow Example:

- **Website:** zsecurity.org
- **Wayback Machine:**
  - Search: zsecurity.org
  - Snapshot (Aug 9, 2018): Old design, email – "support@zsecurity.org".
  - Snapshot (June 3, 2024): Updated design, email gayab.
- **Twitter:** https://twitter.com/zsecurity
  - Result: 50 snapshots, 2019 tweet – "New course launched, contact us at info@zsecurity.org".
- **Conclusion:** zsecurity.org ne email hata diya, lekin Wayback se purana contact mila.

Extra Tips:

- **Google/Bing/Yandex First:** Pehle search engines ke cached pages check karo (e.g., "cache:zsecurity.org" on Google). Agar cached copy nahi milti, tab Wayback Machine jao.
- **Social Media URLs:** Twitter ke liye "twitter.com" use karo, X.com recent hai – purane snapshots ke liye old format better.
- **Cross-Check:** Wayback se mila email ya info SignalHire pe verify karo – active hai ya nahi.
- **Save Results:** Notion mein table banao:

URL	Date	Info Retrieved	Source
zsecurity.org	Aug 9, 2018	support@zsecurity.or	Wayback Machine
twitter.com/zsecu	2019	New course tweet	Wayback Machine

Notes:

- **Wayback Limitations:** Har website ka har update save nahi hota – crawl frequency pe depend karta hai.
- **Social Media:** Deleted posts tabhi milenge jab URL pehle crawl hua ho – random posts miss ho sakte hain.
- **Ethics:** Personal info retrieve karte waqt privacy laws ka dhyan rakho.

Tables

Feature	Strength	Limitation
Historical Snapshots	Past Versions	Crawl Dependent
Deleted Info	Retrieve Old Data	Not Always Saved
Social Media	Archived Posts	Public URLs Only

Table 67: Wayback Machine Features

Summary

- Wayback se past snapshots lo.
- Deleted info retrieve karo.
- Changes track – full history dekho.

Point To Note

Wayback Machine se website changes track karo – **https://archive.org** pe URL (e.g., zsecurity.org) daal kar past snapshots lo, jaise Rishi ka email jo delete ho gaya tha. Ye 800 billion+ pages ke saath websites, tweets, aur posts ke purane versions deta hai – **deleted info** (email, tweets) retrieve karne aur **updates** (design, content) dekhne ke liye best hai. Pehle Google cached pages try karo, phir Wayback jao – har finding ko Notion mein save karo. Ye tool OSINT ke liye ek goldmine hai – systematically use karo aur past data ko unlock karo!

==========

Investigating Website's Files for Hidden Information

Investigating a website's files for hidden information ek powerful OSINT technique hai jo public documents ke metadata se sensitive aur valuable insights nikalne mein madad karta hai. **FOCA (Fingerprinting Organizations with Collected Archives)** ek open-source program hai jo ek domain name ke public documents ko download, extract, aur analyze karta hai – ye process Google Dorks ke manual kaam se kai guna faster aur efficient hai. FOCA ke features mein ek given domain ke saare public documents ko automatically download karna aur unke metadata ko extract karna shamil hai. Google Dorks se aapko har file manually download aur analyze karni padti hai, lekin FOCA ye sab ek baar mein kar deta hai. Isse aapko **usernames**, **emails**, **software versions**, aur **operating systems** jaise details mil sakte hain, jo OSINT ke liye goldmine hote hain. Chalo step-by-step dekhte hain kaise FOCA GitHub se download hota hai, install hota hai, aur kaise website files se hidden info extract ki jati hai – ek example domain **zsecurity.org** ke saath.

Why Investigate Website Files?

- Public documents (PDFs, DOCs) mein metadata hota hai jo website ke internal details leak kar sakta hai – jaise employee names, software stack, ya system info.

- Manual Google Dorks time-consuming hai – FOCA automation ke saath scale aur speed deta hai.
- **Valuable Info:** Usernames se login guesses, emails se phishing, aur outdated software se vuln hunting possible hai.

Features of FOCA:

- **Download Public Documents:** Ek domain ke saare public files (DOC, PDF, etc.) ko ek click mein download karta hai.
- **Extract Metadata:** Files se hidden info – jaise creator, software, OS – nikalta hai.
- **Analyze Metadata:** Extracted data ko organize karke actionable insights deta hai.

Step-by-Step Guide to Using FOCA:

1. **Download FOCA from GitHub:**
   - **URL:** https://github.com/ElevenPaths/FOCA
   - **Requirements:** GitHub pe README mein requirements likhe hote hain –
     - Microsoft Windows (64-bit) – Windows 7, 8, 8.1, ya 10.
     - **Microsoft .NET Framework 4.7.1** – Pehle install karo.
     - **SQL Server Express** – FOCA ke database ke liye zaroori hai (install instructions neeche).
   - **Releases:** GitHub pe "Releases" section hota hai – ye FOCA ke latest aur past versions ka collection hai. Har release mein changelog hota hai (e.g., bug fixes, new features).
   - **Download:** "Releases" pe click karo → Latest version (e.g., v3.4.0.6) ka ZIP file download karo – isme executable aur dependencies hoti hain.
2. **Install FOCA:**
   - ZIP file extract karo – "FOCA.exe" milega.
   - Pehle **SQL Server Express** install karo:
     - Microsoft site se "SQL Server Express 2017" download karo → "Basic" installation chuno → Install.
   - FOCA.exe run karo – agar SQL setup sahi hai, to tool launch hoga.
3. **Set Up a Project in FOCA:**
   - **Open FOCA:** Tool kholo – ek GUI dikhega jisme projects manage hote hain.
   - **Project Name:** Koi bhi naam do – e.g., "ZSecurity_Analysis".
   - **Domain Website:** Target domain daalo – e.g., **zsecurity.org**. Ye domain batata hai ki FOCA kis site ke documents dhoondhega.
   - **Folder:** Ek folder chuno jahan downloaded files save honge – e.g., "C:\FOCA_Docs".
   - **Create:** "Create" pe click karo – project initialize hoga.
4. **Configure Search Settings:**

- **Extensions:** Top mein extensions ka dropdown hai – "All" tick karo ya specific select karo (DOC, DOCX, PDF, etc.).
- **Search Engines:** Google, Bing, DuckDuckGo – sab tick karo taaki maximum files milein.
- **Search All:** "Search All" pe click karo – FOCA in search engines pe dorks chalayega aur public documents ki list banayega (e.g., PDFs, Word files on zsecurity.org).

5. **Download Public Documents:**

- Left panel mein files ki list aayegi – kisi bhi file pe **right-click** karo.
- **Download All:** "Download All" chuno – saare files us folder mein save ho jayenge (e.g., C:\FOCA_Docs).

6. **Extract Metadata:**

- Files download hone ke baad, left panel mein documents dikhte hain.
- Kisi bhi file pe **right-click** karo → **Extract All Metadata** chuno – ye saare files se metadata nikaal lega (e.g., creator, software).

7. **Analyze Metadata:**

- Phir se kisi file pe **right-click** karo → **Analyze All Metadata** chuno.
- **Why Do This?** Extracted metadata ko organize karta hai aur readable format mein present karta hai – raw data se insights banata hai.
- **What Info It Gives:** Left panel mein "Metadata Analysis Completed" ke baad categories dikhti hain – e.g., "ZSecurity-Network-Client-Domain-Document Analysis", "Metadata Summary".

What Info You Get from Metadata Analysis (with Examples):

- **Left Panel Categories:**

1. **ZSecurity-Network-Client-Domain-Document Analysis:**
   - Network-related info – jaise IP addresses ya server names jo documents mein mention hote hain.
   - Example: "Server: 104.21.32.45" – hosting provider (Cloudflare) ka hint.
2. **Metadata Summary:**
   - Organized metadata – Users, Emails, Software, OS, etc.
   - Example:
     * **Users:** "Rishi Kabra" – document creator ka naam.
     * **Emails:** "rishi@zsecurity.org" – contact info.
     * **Software:** "Microsoft Word 2016" – creation tool aur version.
     * **OS:** "Windows 10" – system jahan file bani.

- **How This Info Helps in OSINT:**

- **Usernames:** "Rishi Kabra" se login guesses ya social media profiles dhoondhe ja sakte hain.
- **Emails:** Phishing campaigns ke liye target – e.g., rishi@zsecurity.org ko spear-phishing email bhejo.

- **Software Versions:** "Microsoft Word 2016" outdated hai – agar unpatched hai, to exploits dhoondhe ja sakte hain (CVE database check karo).
- **Operating System:** "Windows 10" ka specific build number mila to vuln research ke liye useful – outdated systems attack surface banate hain.
- **Example Insight:** FOCA ne detect kiya ki ek PDF "Adobe Acrobat 9" se bana, jo 2008 ka hai aur unsupported hai – user outdated software use karta hai, jo hackable ho sakta hai.

Workflow Example – zsecurity.org:

- **Setup:** Project "ZSec", Domain "zsecurity.org", Folder "C:\FOCA_Docs".
- **Search:** DOC, PDF tick kiya → Google, Bing, DuckDuckGo pe "Search All".
- **Download:** 15 files mili – 5 PDFs, 10 DOCs – "Download All" se save hue.
- **Extract & Analyze:** "Extract All Metadata" → "Analyze All Metadata".
- **Result:**
  - Users: "Zed"
  - Email: "support@zsecurity.org"
  - Software: "Word 2019", "Acrobat 11"
  - OS: "Windows 10"
- **Insight:** "Acrobat 11" old hai (2013) – potential vuln (CVE-2013-0640) check kar sakte ho.

Extra Tips:

- **Requirements Check:** SQL Server na ho to FOCA crash karega – pehle setup pura karo.
- **Cross-Check:** Emails ko SignalHire pe verify karo – active hai ya nahi.
- **Save Results:** Notion mein table banao:

Domain	File	User	Email	Software	OS
zsecurity.org	doc1.doc	Zed	support@zsecu	Word 2019	Win 10

- **Expand:** Software versions ko CVE databases pe check karo – security gaps dhoondho.

Tables

Feature	Strength	Use Case
Download Docs	Automation	Bulk Collection
Extract Metadata	Hidden Info	Recon Insights
Analyze Metadata	Organized Data	Actionable Intel

Table 68: FOCA Features Overview

Summary

- FOCA se files download karo.
- Metadata extract aur analyze karo.
- Hidden info lo – OSINT ke liye goldmine.

Point To Note

FOCA se website files ki investigation asaan ho jati hai – GitHub se download karo (**https://github.com/ElevenPaths/FOCA** releases se latest lo), requirements (SQL, .NET) install karo, aur domain (e.g., zsecurity.org) ke public documents ko **download**, **extract**, aur **analyze** karo. Ye tool usernames, emails, software versions, aur OS jaise hidden info deta hai – OSINT ke liye ye intel phishing, vuln hunting, ya target profiling mein kaam aata hai. "Extract All Metadata" se raw data aur "Analyze All Metadata" se organized insights milte hain – jaise outdated Acrobat ka hint. Har finding ko Notion mein save karo – ye systematic approach website ke secrets khol deta hai!

==========

Discovering Subdomains with OSINT TraceLabs VM

Discovering subdomains website OSINT ka ek critical part hai, aur **TraceLabs OSINT VM** ke saath ye kaam aur bhi efficient ho jata hai kyunki ye pre-configured tools ke saath aata hai. Subdomains dhoondhna domain ke hidden sections – jaise admin panels ya internal services – ko expose karne mein madad karta hai. Is process mein hum do powerful tools use karenge: **Subfinder** aur **Httprobe**. **Subfinder** ek fast subdomain enumeration tool hai jo ek given domain ke subdomains dhoondhta hai, jabki **Httprobe** in subdomains ki list ko check karta hai ki kaunse live (active) hain ya nahi. Ye tools TraceLabs VM pe easily install kiye ja sakte hain aur ek pipeline ke through saath mein chalaye ja sakte hain. Chalo step-by-step dekhte hain kaise **subfinder** aur **httprobe** ko install karte hain aur **cybersudo.org** ke subdomains discover karte hain, output ko file mein save karte hue.

Why Discover Subdomains?

- Subdomains ek website ke alag-alag sections ko represent karte hain – e.g., **academy.cybersudo.org** training ke liye ya **login.cybersudo.org** authentication ke liye.
- OSINT mein ye hidden assets, infrastructure details, ya vulnerabilities dhoondhne ke liye zaroori hai.
- **TraceLabs OSINT VM:** Ye Kali Linux-based VM hai jo OSINT investigators ke liye banayi gayi hai – subfinder aur httprobe jaise tools ke liye optimized environment deta hai.

Tools Overview:

1. **Subfinder:**
   - **Kya Hai:** Ek open-source tool jo passively subdomains enumerate karta hai – search engines, DNS records, aur APIs ka use karta hai.
   - **Fayda:** Fast aur silent mode mein kaam karta hai – unnecessary noise nahi karta.

- **Output:** Subdomains ki list – e.g., www.cybersudo.org, api.cybersudo.org.

2. **Httprobe:**

- **Kya Hai:** Ek tool jo subdomains ki list le kar unko probe karta hai – HTTP/HTTPS services check karta hai ki kaunse live hain.
- **Fayda:** Dead subdomains ko filter karke sirf active ones deta hai.
- **Output:** Live subdomains – e.g., http://academy.cybersudo.org.

Installation on TraceLabs OSINT VM:

- **Pre-requisite:** TraceLabs VM pe root access hona chahiye (default creds: osint:osint). VM Kali-based hai, to APT package manager kaam karta hai.
- **Command:**

```
sudo apt update && sudo apt install subfinder httprobe
```

- **Explanation:**
  - `apt update`: Package lists refresh karta hai.
  - `apt install subfinder httprobe`: Subfinder aur Httprobe dono install ho jayenge – Go-based tools hone ke wajah se dependencies minimal hain.
- **Verify:**

```
subfinder -version && httprobe -version
```

- Output: Installed versions dikhega (e.g., Subfinder v2.6.6).

Discovering Subdomains – Step-by-Step:

- **Command to Run:**

```
subfinder -d cybersudo.org -silent -o /desktop/subdomain.txt |
    httprobe
```

- **Breakdown:**
  1. **Subfinder Part:**
     - `-d cybersudo.org`: Target domain specify karta hai.
     - `-silent`: Sirf results dikhata hai, extra logs nahi – clean output ke liye.
     - `-o /desktop/subdomain.txt`: Subdomains ko "subdomain.txt" file mein save karta hai Desktop pe.
     - **Example Output in File:**

```
www.cybersudo.org
academy.cybersudo.org
login.cybersudo.org
```

  2. **Pipe to Httprobe:**
     - `| httprobe`: Subfinder ke output ko real-time Httprobe ko bhejta hai – ye har subdomain pe HTTP/HTTPS check karta hai.

– **Example Terminal Output:**

```
http://www.cybersudo.org
https://academy.cybersudo.org
http://login.cybersudo.org
```

– Sirf live subdomains dikhte hain – dead ones filter ho jate hain.

- **What This Means:**
  - **cybersudo.org**: Ye target domain hai jiske subdomains dhoondhne hain.
  - Pipeline (|): Subfinder se subdomains nikalkar Httprobe ko pass karta hai – ek seamless workflow banata hai.
  - **Output File:** /desktop/subdomain.txt mein raw list save hoti hai, jabki terminal pe live subdomains dikhte hain.

Workflow Example – cybersudo.org:

- **Run Command:**

```
subfinder -d cybersudo.org -silent -o /desktop/subdomain.txt |
   httprobe
```

- **Results:**
  - **subdomain.txt (Raw List):**

```
www.cybersudo.org
academy.cybersudo.org
login.cybersudo.org
dev.cybersudo.org
```

  - **Terminal (Live Subdomains):**

```
http://www.cybersudo.org
https://academy.cybersudo.org
http://login.cybersudo.org
```

- **Conclusion:** "dev.cybersudo.org" live nahi tha, baaki teeno active hain – academy HTTPS pe chal raha hai.

Extra Tips:

- **Expand:** Httprobe ke baad `| tee live.txt` add karo – live subdomains bhi file mein save ho jayenge.

```
subfinder -d cybersudo.org -silent -o /desktop/subdomain.txt |
   httprobe | tee /desktop/live.txt
```

- **Cross-Check:** Live subdomains ko browser mein kholo ya `curl -I` se headers check karo – extra info (server type, status) mil sakta hai.
- **Save Results:** Notion mein table banao:
- **More Tools:** TraceLabs VM pe Sublist3r ya Amass bhi try karo – Subfinder ke saath combine karke zyada subdomains mil sakte hain.

Domain	Subdomains	Live Status	Tool
cybersudo.org	www, academy, login	http://, https://, http://	Subfinder + Httprobe

Tables

Tool	Strength	Use Case
Subfinder	Fast Enumeration	Raw Subdomains
Httprobe	Live Check	Active Filtering

Table 69: Subfinder vs Httprobe

Summary

- Subfinder se raw subdomains lo.
- Httprobe se live check karo.
- Pipeline se efficient workflow – results save karo.

Point To Note

TraceLabs OSINT VM pe **subfinder** aur **httprobe** se subdomain discovery ek streamlined process hai – `apt install subfinder httprobe` se install karo, phir `subfinder -d cybersudo.org -silent -o /desktop/subdomain.txt | httprobe` chalao. Subfinder raw subdomains deta hai (e.g., www, academy), aur Httprobe unko live check karta hai (e.g., http://www.cybersudo.org). Ye combo OSINT ke liye perfect hai – hidden sections dhoondhne aur website footprint banane mein kaam aata hai. Results ko file mein save karo aur Notion mein organize rakho – systematic approach se cybersudo.org jaise domains ke secrets khul jate hain!

==========

Investigating WordPress Websites

Investigating a WordPress website ke liye **WPScan** ek powerful security scanner hai jo WordPress par bani websites ke **attack vectors** (matlab, vulnerabilities ya weak points jahan se attack ho sakta hai) ko identify karta hai. Agar aapko WordPress ke baare mein kuch nahi pata, to chinta mat karo – main ise bilkul basic level se samjhaunga. WordPress ek popular platform hai jisse websites banayi jati hain – jaise blogs, online stores, ya company pages. WPScan is platform ke components – jaise **plugins**, **themes**, aur **usernames** – ko scan karta hai taaki pata chal sake ki kahan security risks hain. Ye tool Linux pe `apt install wpscan` command se install hota hai aur WordPress sites ke baare mein detailed info deta hai. Chalo step-by-step samajhte hain ki WPScan kya karta hai, WordPress kya hota hai, aur isse kya-kya info milti hai.

What is WordPress? (Basic Intro for Beginners)

- WordPress ek free aur open-source **Content Management System (CMS)** hai – matlab, ek software jo aapko website banane aur manage karne deta hai bina coding janne ke.

- Iska use karna asaan hai – jaise Lego blocks se ghar banate ho – aur ismein **plugins** aur **themes** add karke functionality aur look change kar sakte ho.
- **Example:** Ek blog banaya (e.g., cybersudo.org) – WordPress uska base hai, plugins se comments ya contact form add kiya, aur theme se design chuna.

What is WPScan?

- WPScan ek **security scanner** hai jo specially WordPress websites ke liye banaya gaya hai. Ye "black box" scanner hai – yani, ye site ke bahar se (jaise hacker) check karta hai bina admin access ke.
- Ye WordPress ke weak points dhoondhta hai jo attackers exploit kar sakte hain – jaise outdated software ya exposed info.
- Linux pe install karne ke liye:

```
sudo apt install wpscan
```

- Ye command TraceLabs OSINT VM ya Kali Linux jaise systems pe WPScan ko ready karta hai.

What Information Does WPScan Collect? WPScan WordPress sites se specific components aur details collect karta hai. Agar aap WordPress nahi samajhte, to main har term ko simple language mein explain karunga:

1. **Plugins:**
   - **Kya Hai:** Plugins chhote software hote hain jo WordPress mein extra features add karte hain – jaise contact form, security, ya SEO tools.
   - **WPScan Kya Karta Hai:** Ye check karta hai ki kaunse plugins install hain aur unki versions outdated ya vulnerable hain ya nahi.
   - **Example:** "Yoast SEO" plugin agar purana hai, to ismein security holes ho sakte hain jo hackers use kar sakte hain.
   - **Kyoon Zaroori:** Outdated plugins WordPress sites ke hack hone ka sabse bada reason hote hain.
2. **Themes:**
   - **Kya Hai:** Themes WordPress site ka design ya look decide karte hain – jaise site ka color, layout, ya style.
   - **WPScan Kya Karta Hai:** Ye installed themes ki list banata hai aur dekhta hai ki unmein known vulnerabilities hain ya nahi.
   - **Example:** "Twenty Twenty-One" theme agar old version pe hai, to usmein bugs ho sakte hain.
   - **Kyoon Zaroori:** Themes mein bhi code hota hai, aur agar ye outdated hai, to site attack ke liye open ho jati hai.
3. **Usernames:**
   - **Kya Hai:** Ye WordPress site ke users ke login names hote hain – jaise "admin" ya "rishi". Har user ka ek username hota hai jo site manage karta hai.

- **WPScan Kya Karta Hai:** Ye public info (jaise author pages) se usernames guess karta hai – is process ko "user enumeration" kehte hain.
- **Example:** cybersudo.org/author/rishi se "rishi" username mil sakta hai.
- **Kyoon Zaroori:** Agar hackers ko usernames pata chal jayein, to wo password guess karke login try kar sakte hain (brute force attack).

4. **More Info WPScan Collects:**

- **WordPress Version:** Site kaunsa WordPress version use kar rahi hai – agar purana hai, to vulnerabilities ho sakti hain.
- **Config Files:** "wp-config.php" jaise sensitive files exposed hain ya nahi – isme database passwords hote hain.
- **Backup Files:** Agar site ke backups public hain (e.g., db_backup.sql), to hackers pura data le sakte hain.
- **TimThumb Files:** Ek purana script jo themes mein hota tha – ismein vulnerabilities hoti thi.

How WPScan Works (Simple Explanation):

- WPScan site ko bahar se scan karta hai – jaise ek hacker kisi ghar ke darwaze-diwaron ko check karta hai bina andar jaye.
- Ye public info (HTML code, URLs) aur WordPress ke patterns (jaise plugin folders) analyze karta hai.
- Iske paas ek **vulnerability database** hai – jisme WordPress, plugins, aur themes ke known security issues listed hote hain. Ye har finding ko is database se match karta hai.

Basic Command to Investigate a WordPress Site:

- **Command:**

```
wpscan --url https://cybersudo.org
```

- **Explanation:**
  - `--url`: Target website ka address.
  - Ye basic scan karta hai – WordPress version, plugins, themes, aur interesting findings dikhata hai.
- **Example Output:**
  - WordPress Version: 6.4.2
  - Plugins: Yoast SEO v20.1 (vulnerable), Contact Form 7 v5.7
  - Themes: Astra v3.9 (outdated)
  - Usernames: "admin", "rishi"
- **Advanced Command:**

```
wpscan --url https://cybersudo.org -e ap -e at -e u
```

- `-e ap`: All plugins enumerate karta hai.

- `-e at`: All themes enumerate karta hai.
- `-e u`: Usernames dhoondhta hai.

Why This Info is Useful in OSINT?

- **Plugins/Themes:** Outdated versions se pata chalta hai ki site secure nahi hai – aap vulnerabilities (CVE database) check kar sakte ho.
- **Usernames:** Ye identities ya social engineering ke liye use ho sakte hain – jaise "rishi" ka LinkedIn dhoondhna.
- **Config/Backups:** Exposed files se sensitive data (passwords, database) mil sakta hai.
- **Example:** cybersudo.org pe "Contact Form 7 v5.7" mila – is version mein XSS vulnerability hai. Hacker iska faida utha sakta hai.

Workflow Example – cybersudo.org:

- **Install WPScan:**

```
sudo apt install wpscan
```

- **Run Scan:**

```
wpscan --url https://cybersudo.org -e ap -e u
```

- **Results:**
  - Plugins: "WooCommerce v7.1" (outdated), "Elementor v3.8".
  - Usernames: "cybersudo_admin", "rishi".
- **Insight:** WooCommerce ka purana version hackable hai – CVE-2023-1234 check karo.

Extra Tips:

- **API Token:** Vulnerability details ke liye WPScan.com se free API token lo (25 requests/day) – command mein `--api-token YOUR_TOKEN` add karo.
- **Save Output:** Results file mein save karne ke liye `-o output.txt` use karo.
- **Notion Table:**

Domain	Plugins	Themes	Usernames	Findings
cybersudo.org	WooCommerce Elementor	Astra	cybersudo_adm rishi	Outdated plugin

Component	WPScan Action	OSINT Use
Plugins	Detects Versions	Vulnerability Check
Themes	Lists Installed	Security Risks
Usernames	Enumerates Users	Social Engineering

Table 70: WPScan Components Overview

Tables

Summary

- WPScan se plugins aur themes scan karo.
- Usernames aur weak points lo.
- Attack vectors identify – OSINT ke liye perfect.

Point To Note

WPScan WordPress websites ke **attack vectors** dhoondhne ka ek shandaar tool hai – `apt install wpscan` se install karo aur `--url cybersudo.org` jaise commands se **plugins**, **themes**, aur **usernames** jaise info lo. Ye beginners ke liye bhi samajhna asaan hai – WordPress ek CMS hai, plugins usmein features add karte hain, themes design dete hain, aur usernames users ko identify karte hain. WPScan in sab ko scan karke security risks batata hai – jaise outdated plugins ya exposed usernames. Is info se aap site ke weak points samajh sakte ho aur OSINT ke liye next steps plan kar sakte ho. Systematic approach rakho aur har finding ko save karo – ye WordPress investigation ka game-changer hai!

==========

Automating OSINT Investigation

Automating OSINT investigations ke liye **SpiderFoot** ek shandaar tool hai jo internet ke vibhinn sources se information gather karta hai, manual kaam ko kam karke time aur effort bachata hai. Ye ek open-source intelligence (OSINT) automation tool hai jo **domains**, **IP addresses**, **hostnames**, **network subnets**, **email addresses**, **phone numbers**, **names**, **usernames**, **Bitcoin addresses**, aur aur bhi kai data points pe intelligence collect karta hai. SpiderFoot 100+ public data sources (jaise DNS, WHOIS, Shodan, social media) se integrate hota hai aur ek user-friendly web interface ya command-line ke through kaam karta hai. Iske zariye aap ek target ka digital footprint bana sakte ho – chahe wo penetration testing ke liye ho ya threat intelligence ke liye. Chalo ise **install** karne, **use** karne ke steps, aur ek **real-life OSINT example** ke saath samajhte hain – SpiderFoot kaise investigation ko automate karta hai.

What is SpiderFoot?

- SpiderFoot ek Python-based OSINT tool hai jo reconnaissance ko automate karta hai – yani, ye ek seed target (jaise domain ya email) le kar usse related saari info ek jagah lata hai.
- **Collects Information On:**

  - **Domains:** cybersudo.org, zsecurity.org
  - **IPs:** 192.168.1.1
  - **Hostnames:** www.cybersudo.org
  - **Network Subnets:** 192.168.1.0/24
  - **Email Addresses:** rishi@cybersudo.org
  - **Phone Numbers:** +12025550123
  - **Names:** Rishi Kabra
  - **Usernames:** rishikabra132
  - **Bitcoin Addresses:** 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
- Ye tool modules ke through kaam karta hai – har module ek specific data source ya task ke liye hota hai (e.g., DNS lookup, email scraping).

Installing SpiderFoot on Linux: SpiderFoot ko TraceLabs OSINT VM ya Kali Linux pe install karna asaan hai. Ye steps follow karo:

1. **Update System:**

```
sudo apt update && sudo apt upgrade -y
```

2. Ye system ke packages ko latest karta hai taaki compatibility issues na ho.
3. **Install SpiderFoot:**

```
sudo apt install spiderfoot
```

4. Ye pre-built package install karta hai. Agar GitHub se latest version chahiye, to:

```
git clone https://github.com/smicallef/spiderfoot.git
cd spiderfoot
pip3 install -r requirements.txt
```

5. **Verify Installation:**

```
python3 sf.py --version
```

6. Output: SpiderFoot ka version dikhega (e.g., 4.0).

Running SpiderFoot – Step-by-Step: SpiderFoot ko web interface ya command-line se chala sakte ho. Web interface zyada intuitive hai, to uspe focus karte hain:

1. **Start SpiderFoot:**

```
cd spiderfoot
python3 sf.py -l 127.0.0.1:5001
```

2. `-l 127.0.0.1:5001`: Localhost pe port 5001 par server start karta hai.
3. Terminal mein: "SpiderFoot web server listening on 127.0.0.1:5001" dikhega.
4. **Access Web Interface:**

- Browser kholo aur URL daalo: **http://127.0.0.1:5001**
- SpiderFoot ka dashboard khulega.

5. **Create a New Scan:**
   - **New Scan** tab pe jao.
   - **Scan Name:** Koi naam do – e.g., "CyberSudo_Investigation".
   - **Seed Target:** Target daalo – e.g., "cybersudo.org" (domain), "rishi@cybersudo.org" (email), ya "rishikabra132" (username).
   - **Scan Type:**
     - **By Use Case:** "Footprint" (basic recon) ya "Investigate" (deep dive).
     - **By Required Data:** Specific data chuno (e.g., emails, subdomains).
     - **By Module:** Manual module select karo (e.g., sfp_dnsresolve, sfp_email).
   - Default "Footprint" chhod sakte ho pehle try ke liye.
   - **Run Scan:** "Run Scan Now" pe click karo.
6. **View Results:**
   - Scan chalte waqt **Scans** tab pe jao – status "Running" dikhega.
   - Complete hone pe **Browse** tab pe results dekho:
     - Graph view: Data nodes aur connections.
     - List view: Domains, IPs, emails ki list.
7. **Export Results:**
   - **Settings** ¿ **Export** se CSV ya JSON mein save karo.

Real-Life OSINT Example – Investigating a Phishing Domain: Scenario: Maan lo aapko ek suspicious email mila jisme link hai – "secure-login-cybersudo.org". Aapko shak hai ki ye phishing site hai. SpiderFoot se kaise investigate karoge?

1. **Setup Scan:**
   - **Target:** "secure-login-cybersudo.org"
   - **Scan Name:** "Phishing_Check"
   - **Scan Type:** "Investigate" (deep analysis ke liye).
   - Command-line alternative:

```
python3 sf.py -s secure-login-cybersudo.org -m sfp_dnsresolve,
   sfp_email,sfp_webcontent -q
```

   - `-s`: Seed target
   - `-m`: Specific modules
   - `-q`: Quiet mode (sirf results).
2. **Results:**
   - **Domains/Subdomains:**
     - www.secure-login-cybersudo.org

– mail.secure-login-cybersudo.org

- **IPs:** 172.67.123.45 (Cloudflare-hosted).
- **Emails:** admin@secure-login-cybersudo.org (WHOIS se mila).
- **Hostnames:** server1.secure-login-cybersudo.org
- **Web Content:** Fake login page ka HTML snippet.
- **Bitcoin Address:** 3FkenCiXpSLqD8L79 (scam payment link se).
- **Malicious Flag:** AbuseIPDB se IP malicious mark hua.

3. **Analysis:**

   - **Subdomains:** "mail" aur "server1" se infrastructure ka hint – phishing site hosted hai.
   - **Email:** "admin@secure-login-cybersudo.org" se domain owner ka clue – social media pe check karo.
   - **IP:** Cloudflare pe host hai, lekin AbuseIPDB flag se scam confirm hota hai.
   - **Bitcoin:** Address ko blockchain explorer (e.g., Blockchain.com) pe trace karo – transactions se scammer ka pattern milega.

4. **OSINT Outcome:**

   - Ye domain ek phishing scam ka part hai – fake login page se credentials churaya ja raha hai.
   - Admin email aur Bitcoin address se scammer ki identity ya related scams dhoondhne ke liye pivot points mil gaye.
   - Report banakar security team ko do – domain block karne aur users ko warn karne ke liye.

How SpiderFoot Helps in OSINT:

- **Automation:** Manual Google Dorks ya WHOIS lookups ki jagah ek click mein 100+ sources scan.
- **Comprehensive:** Ek hi scan mein domains, IPs, emails, aur Bitcoin tak cover hota hai.
- **Real-Time:** Results live aate hain – wait karne ki zarurat nahi.
- **Example Insight:** Phishing domain ke IP se related subnets mile – 172.67.123.0/24 pe aur scam sites hain.

Extra Tips:

- **API Keys:** Shodan, VirusTotal jaise services ke liye API keys add karo (Settings ¿ API Keys) – results aur rich honge.
- **Save Results:** Notion mein table banao:
- **Expand:** IPs ko Reverse DNS se check karo – aur related domains mil sakte hain.

Target	Domains/Sul	IPs	Emails	Bitcoin Address	Findings
secure-login-cybersudo.org	www, mail	172.67.123.4	admin@secure-login-cybersudo.org	3FkenCiXpSLq	Phishing site

Feature	Strength	OSINT Use
Automation	Time-Saving	Broad Recon
Data Sources	100+ Integrations	Comprehensive Intel
Web Interface	User-Friendly	Easy Analysis

Table 71: SpiderFoot Features Overview

Tables

Summary

- SpiderFoot se 100+ sources scan karo.
- Domains, IPs, emails automate karke lo.
- Digital footprint banao – OSINT ko fast-track karo.

Point To Note

SpiderFoot OSINT investigations ko automate karta hai – `apt install spiderfoot` se install karo, `python3 sf.py -l 127.0.0.1:5001` se chalao, aur web interface pe **domains**, **IPs**, **emails**, ya **usernames** jaise targets scan karo. Real-life mein, jaise phishing domain "secure-login-cybersudo.org" ka case, ye tool subdomains, IPs, aur scam indicators deta hai jo manual kaam se miss ho sakte hain. Har finding ko save karo aur pivot points (email, Bitcoin) se deeper investigation karo – ye OSINT ka game-changer hai! Systematic aur automated approach ke saath, SpiderFoot time bachata hai aur intelligence ko actionable banata hai.

==========

Cleaning and Structuring Notes

Cleaning and structuring notes OSINT investigations ka ek zaroori step hai jo aapke collected data ko organized, readable, aur actionable banata hai. Jab aap apne target ke baare mein details gather karte ho – jaise full name, date of birth, ya social media profiles – to har detail ke saath **source** add karna critical hai taaki aapko yaad rahe ki info kahan se mili aur uski credibility kya hai. Tools jaise **Notion** iske liye perfect hain kyunki ye aapko notes ko sections mein divide karne, resources (jaise profile pics, PDFs) store karne, aur offline backup banane ki flexibility deta hai. Isse agar target apne online accounts delete bhi kar de, tab bhi aapke paas uska digital footprint safe rahta hai. Chalo step-by-step dekhte hain kaise notes clean aur structure kiye jate hain, sources kaise add kiye jate hain, aur Notion mein data kaise manage aur export kiya jata hai – real examples ke saath.

Why Clean and Structure Notes?

- **Clarity:** Raw data (jaise random usernames, emails) ko organized format mein rakhna asaan banata hai – quick reference ke liye.

- **Verification:** Sources ya direct links add karne se info ki authenticity track hoti hai.
- **Preservation:** Profile pics ya documents save karne se target ke deleted accounts ka bhi record rehta hai.
- **Sharing:** Structured notes team ya reporting ke liye professional look dete hain.

How to Clean and Structure Notes:

1. **Add Sources to Every Detail:**
   - Har piece of info ke saath uska source mention karo – ya to platform ka naam (e.g., "Facebook") ya direct URL.
   - **Example Without Source:**
     - Fullname: Rishi Raj Kabra
     - DOB: 1.12.1996
   - **Cleaned with Source:**
     - Fullname: Rishi Raj Kabra (Source: Facebook, Username: rishikabra132)
     - DOB: 1.12.1996 (Source: https://facebook.com/rishikabra132)
   - **Why?** Source batata hai ki ye info kahan se aayi – agar Facebook delete ho jaye, to bhi aapke paas reference hai.
   - **Pro Tip:** Direct URL zyada specific hota hai – clicking se exact page tak jaya ja sakta hai (jab tak active hai).
2. **Use Notion for Structuring:**
   - Notion mein ek page banao apne target ke liye – e.g., "Rishi Raj Kabra Investigation".
   - **Sections Banao:**
     - **Basic Info:** Name, DOB, Phone, Email
     - **Social Media:** Usernames, Links
     - **Resources:** Profile pics, PDFs, Screenshots
   - **Example Structure:**

```
# Rishi Raj Kabra Investigation
## Basic Info
- Fullname: Rishi Raj Kabra (Source: https://facebook.com/
  rishikabra132)
- DOB: 1.12.1996 (Source: https://linkedin.com/in/rishi-kabra)
- Email: rishi.kabra@gmail.com (Source: Wayback Machine,
  rishikabra.com, 2019 snapshot)

## Social Media
- Facebook: rishikabra132 (https://facebook.com/rishikabra132)
- Twitter: @rishikabra (https://twitter.com/rishikabra)

## Resources
- [Profile Pic] (Uploaded: fb_profile.jpg)
- [PDF] (Uploaded: resume_rishi.pdf)
```

3. **Resources Section in Notion:**

   - Notion mein "Resources" naam ka ek section banao.
   - Isme saari **profile pics**, **PDFs**, aur **screenshots** upload karo jo aapne investigation mein gather kiye – jaise Rishi ki Facebook DP ya resume PDF.
   - **Kaise Upload Karein:**
     - Notion page pe "/file" type karo → "Upload a file" → File select karo (e.g., fb_profile.jpg).
   - **Why?** Agar target apne accounts delete kar de (e.g., Facebook profile gayab), to bhi aapke paas uski pics aur docs ka offline record rahta hai – evidence ke liye critical.

Exporting Notes from Notion for Offline Backup: Agar aap apne OSINT notes ka offline copy chahiye – jaise HTML ya PDF format mein – to Notion se export kar sakte ho. Ye steps follow karo:

1. **Open Notion Page:**
   - Apne target ka page kholo – e.g., "Rishi Raj Kabra Investigation".
2. **Click Three Dots:**
   - Page ke top-right corner pe three dots (...) pe click karo – ye menu kholta hai.
3. **Select Export:**
   - Dropdown mein "Export" option chuno.
4. **Choose Export Format:**
   - **HTML:** Webpage format mein save hota hai – links clickable rehte hain.
   - (Other options: Markdown, PDF – HTML zyada versatile hai).
   - Select: "HTML".
5. **Include Content:**
   - **Everything:** Saara content – text, images, files – include hota hai.
   - Chuno: "Everything".
6. **Include Subpages:**
   - Agar aapke page ke andar subpages hain (e.g., "Social Media" ek alag page), to "Include Subpages" tick karo – saara data ek saath export hoga.
   - **What is This?** Ye nested pages ya linked sections ko bhi backup mein shamil karta hai – ek complete package banata hai.
7. **Click Export:**
   - "Export" button dabao – Notion ek ZIP file generate karega (e.g., "Rishi_Raj_Kabra_Investigatio
   - Isme HTML files aur uploaded resources (pics, PDFs) honge – unzip karke browser mein kholo.

Why Export? Offline copy se aap Notion ke bina bhi data access kar sakte ho – ya team ke saath share kar sakte ho.

Real-Life Example:

- **Target:** Rishi Raj Kabra
- **Raw Notes:**
  - Rishi Raj Kabra, 1.12.1996, rishi.kabra@gmail.com, rishikabra132
- **Cleaned Notes:**
  - Fullname: Rishi Raj Kabra (Source: https://facebook.com/rishikabra132)
  - DOB: 1.12.1996 (Source: https://linkedin.com/in/rishi-kabra)
  - Email: rishi.kabra@gmail.com (Source: Wayback Machine, https://web.archive.org/web/2019*/
  - Username: rishikabra132 (Source: Twitter, https://twitter.com/rishikabra)
- **Resources in Notion:**
  - Profile Pic: fb_profile.jpg (Facebook se 2023 mein download kiya).
  - PDF: resume_rishi.pdf (zsecurity.org se mila).
- **Export:** HTML file banayi – "RishiInvestigation.html" – jo offline bhi khulti hai aur pics/PDFs dikhaati hai.

Extra Tips:

- **Consistency:** Har entry ke liye same format rakho – "Field: Value (Source: Link)".
- **Screenshots:** Profile pics ke saath webpage ka screenshot bhi save karo – context ke liye.
- **Backup Regularly:** Har bade update ke baad export karo – data loss se bacho.
- **Notion Table:**

Field	Value	Source
Fullname	Rishi Raj Kabra	https://facebook.com/rishikabra132
DOB	1.12.1996	https://linkedin.com/in/rishi-kabra
Email	rishi.kabra@gmail	Wayback Machine, rishikabra.com

Tables

Task	Action	Benefit
Add Sources	Link/Platform	Verification
Structure in Notion	Sections/Resources	Organization
Export Notes	HTML Backup	Offline Access

Table 72: Cleaning and Structuring Benefits

Summary

- Har detail ke saath source add karo.
- Notion mein structure aur resources save karo.
- Export se offline backup lo – data safe rakho.

Point To Note

Cleaning and structuring notes ke liye har detail (e.g., Fullname: Rishi Raj Kabra) ke saath **source** ya **direct link** add karo – jaise Facebook URL. **Notion** mein "Resources" section banao taaki **profile pics** aur **PDFs** save rahein – target ke accounts delete hone par bhi evidence rahega. Offline backup ke liye Notion se **export** karo – three dots ¿ Export ¿ HTML ¿ Everything + Subpages → ZIP file milega. Ye structured approach OSINT data ko organized rakhta hai aur investigation ko professional banata hai – har finding ko trackable aur reusable rakho!

==========

Creating an OSINT Relationship Map

Creating an OSINT relationship map ek powerful technique hai jo aapke gathered information ko visually represent karti hai – isse aap apne target ke connections, identities, aur digital footprint ko ek **network graph** ke roop mein samajh sakte ho. **OSINT Tracker** (osintracker.com) ek free online tool hai jo aapko ye network banane mein madad karta hai – jaise ek detective board jahan aap entities (people, accounts, numbers) ko pins se jodte ho. Ismein aap entities add kar sakte ho (e.g., person, Facebook profile), unke beech **relationships** define kar sakte ho, aur critical nodes highlight kar sakte ho. Ye tool aapke investigation ko structured aur visual banata hai – chahe aap Rishi Kabra ke LinkedIn se phone numbers tak ka trail bana rahe ho ya companies ke saath uske links dhoondh rahe ho. Chalo step-by-step dekhte hain kaise OSINT Tracker pe ek relationship map banaya jata hai, ek real example ke saath – Rishi Kabra ke LinkedIn, SignalHire, aur phone numbers ka graph.

Why Create an OSINT Relationship Map?

- **Visualization:** Complex data (names, accounts, numbers) ko ek glance mein samajhna asaan hota hai.
- **Connections:** Target ke relationships – personal, professional, ya online – clear hote hain.
- **Pivot Points:** Ek entity se doosre tak ka trail banakar deeper insights milte hain – e.g., LinkedIn se phone number tak.
- **OSINT Tracker:** Ye tool free hai, browser-based hai, aur data ko graph mein convert karta hai – no coding needed.

Steps to Create a Relationship Map on OSINT Tracker:

1. **Launch OSINT Tracker:**
   - Website: **osintracker.com**
   - Homepage pe **"Launch App"** pe click karo – ye tool ka interface kholega.

2. **Create a New Investigation:**

- Left sidebar mein **"Investigation"** ¿ **"Add"** pe click karo.
- **Name:** Koi naam do – e.g., "Rishi Kabra Investigation".
- **Add:** "Add" button pe click karo – ek blank graph canvas khulega.

3. **Add Entity #1 – Person (Rishi Kabra):**

- Canvas pe **"Add Entity"** pe click karo.
- **Value:** "Rishi Kabra" (target ka naam).
- **Search/Type:** Dropdown se "Person" chuno – ye entity type define karta hai.
- **Color/Badge:** Koi color select karo (e.g., blue) aur badge chuno (optional).
- **Image:** Target ki profile pic upload karo – e.g., Rishi ki LinkedIn ya Facebook DP.
- **Result:** Graph pe "Rishi Kabra" ek node ban jayega, image ke saath.

4. **Add Entity #2 – Facebook Profile:**

- Phir se **"Add Entity"** pe click karo.
- **Value:** "Facebook" (ya username, e.g., "rishikabra132").
- **URL:** Target ka Facebook URL daalo – e.g., "https://facebook.com/rishikabra132".
- **Search/Type:** "Facebook" select karo.
- **Color/Badge:** Alag color do (e.g., green).
- **Result:** Graph pe "Facebook" node add ho jayega.

5. **Create a Relationship:**

- **"Relationship"** button pe click karo (graph ke upar).
- **Drag:** "Rishi Kabra" node se "Facebook" node tak drag karo – ek box khulega.
- **Information Label:** Relationship define karo – e.g., "Uses" (Rishi uses this Facebook profile).
- **Save:** Box mein "Save" karo – ek line dono entities ko jod degi, label ke saath.

6. **Add More Entities and Relationships:**

- **LinkedIn:**
  - Value: "LinkedIn"
  - URL: "https://linkedin.com/in/rishi-kabra"
  - Type: "LinkedIn"
  - Color: Yellow
  - Relationship: "Rishi Kabra" se "LinkedIn" tak – Label: "Works At".
- **SignalHire – Personal Phone:**
  - Value: "+91-9876543210"
  - Type: "Phone Number"
  - Color: Red
  - Relationship: "LinkedIn" se "Phone Number" tak – Label: "Found Via SignalHire".

- **SignalHire – Business Phone:**
  - Value: "+91-1234567890"
  - Type: "Phone Number"
  - Color: Purple
  - Relationship: "LinkedIn" se "Business Phone" tak – Label: "Found Via SignalHire".

7. **Highlight Critical Entities:**
   - Kisi entity (e.g., "Rishi Kabra") pe click karo – right sidebar mein toggle dikhega.
   - **Toggle On:** "Critical" toggle on karo – ye entity highlight ho jayega (e.g., bold ya glowing).
   - **Why?** Critical nodes investigation ke key points hote hain – jaise main target ya sensitive data.
8. **Export the Investigation:**
   - Top-right mein **three-line symbol (hamburger menu)** pe click karo.
   - **Export:** "Export" option chuno – ye JSON file banayega (e.g., "Rishi_Kabra_Investigation.json").
   - **Import:** Agar future mein wapas load karna ho, to "Import" se ye file upload kar sakte ho.
   - **Why Export?** Offline backup ya team ke saath sharing ke liye.

Real-Life Example – Rishi Kabra's Relationship Map:

- **Scenario:** Aap Rishi Kabra ke digital footprint ka OSINT kar rahe ho – LinkedIn se phone numbers tak ka trail chahiye.
- **Graph Creation:**
  1. **Entity 1 – Rishi Kabra:** Person node (blue), profile pic add kiya.
  2. **Entity 2 – LinkedIn:** "https://linkedin.com/in/rishi-kabra" (yellow), "Works At" relationship banaya.
  3. **Entity 3 – Personal Phone:** "+91-9876543210" (red), SignalHire extension se mila – "Found Via SignalHire" link banaya LinkedIn se.
  4. **Entity 4 – Business Phone:** "+91-1234567890" (purple), SignalHire se company profile pe mila – "Found Via SignalHire" link banaya LinkedIn se.
  5. **Entity 5 – Facebook:** "https://facebook.com/rishikabra132" (green), "Uses" relationship banaya Rishi se.
- **Critical Node:** "Rishi Kabra" ko critical mark kiya – central figure hai.
- **Resulting Graph:**
  - Rishi Kabra → LinkedIn (Works At) → Personal Phone (Found Via SignalHire).
  - Rishi Kabra → LinkedIn → Business Phone (Found Via SignalHire).
  - Rishi Kabra → Facebook (Uses).
- **Insight:** LinkedIn se pata chala Rishi do companies mein kaam karta hai, SignalHire ne personal aur business phone numbers diye, aur Facebook se social presence confirm hui.

How This Helps in OSINT:

- **Trail Building:** LinkedIn se phone numbers tak ka connection clear hota hai – SignalHire jaise tools pivot points dete hain.
- **Context:** Relationships (e.g., "Uses", "Works At") se data ka meaning samajh aata hai.
- **Visualization:** Graph se ek glance mein Rishi ka network dikhta hai – manual notes se zyada effective.
- **Export:** JSON file se investigation portable aur shareable ban jata hai.

Extra Tips:

- **Color Coding:** Har entity type ke liye alag color rakho – e.g., Persons (blue), Social Media (green), Phones (red).
- **Badges:** Icons se entity type visually differentiate karo – e.g., phone ke liye call icon.
- **Save Progress:** Har bade update ke baad export karo – data loss se bacho.
- **Notion Integration:** Graph ka screenshot Notion mein "Resources" section mein daalo.

Tables

Step	Action	Purpose
Add Entity	Define Person/Phone	Build Nodes
Create Relationship	Link Entities	Show Connections
Export Graph	Save JSON	Backup/Share

Table 73: Relationship Map Creation Steps

Summary

- Entities add karo – Rishi, LinkedIn, phones.
- Relationships define karo – Uses, Found Via.
- Graph export karo – visual OSINT rakho.

Point To Note

OSINT Tracker se relationship map banane ke liye **"Launch App"** se shuru karo, investigation banao (e.g., "Rishi Kabra"), entities add karo (Rishi, LinkedIn, Facebook, phones), aur **relationships** define karo (Uses, Found Via). LinkedIn se SignalHire tak ka trail banao – jaise Rishi ke personal aur business phone numbers ka connection. Critical entities highlight karo aur end mein **export** karo – ye visual graph OSINT ko structured aur insightful banata hai. Har step ko systematically follow karo aur Rishi jaise targets ka network ek clear picture mein dekho!

==========

Structuring Open Source Investigations

Structuring open source investigations ke liye ek **OSINT flowchart** ek step-by-step visualization hai jo investigation process ko systematic aur manageable banata hai. Ye flowchart aapko har piece of information ke saath kya karna hai – uska next step kya hoga – ye batata hai aur ensure karta hai ki koi bhi important step miss na ho. OSINT mein data chaotic ho sakta hai – emails, usernames, phone numbers sab bikhar jate hain – lekin ek flowchart is mess ko organize karta hai, taaki aap efficiently target ke digital footprint tak pahunch sako. Chalo ek detailed **OSINT flowchart** step-by-step banate hain – har stage ko samajhte hue – jo aapko investigation ke har point pe direction dega.

Why Use an OSINT Flowchart?

- **Guidance:** Har piece of info (e.g., username, domain) ke saath aage kya karna hai, ye clear hota hai.
- **Completeness:** Steps miss hone ka risk kam hota hai – structured approach se sab cover hota hai.
- **Efficiency:** Random trial-and-error ki jagah, ek defined path investigation ko fast-track karta hai.

OSINT Flowchart: Step-by-Step Visualization Ye flowchart ek typical OSINT investigation ka blueprint hai – har step ke baad decision points aur actions hain. Ise aap Notion ya paper pe draw kar sakte ho.

1. **Step 1: Define the Seed (Starting Point)**
   - **Action:** Investigation ka initial piece of info chuno – ye "seed" hai jisse shuruaat hoti hai.
   - **Examples:**
     - Username: rishikabra132
     - Email: rishi.kabra@gmail.com
     - Domain: cybersudo.org
     - Phone: +91-9876543210
   - **What to Do:** Seed ko note karo aur decide karo ki iska type kya hai (person, account, contact).
   - **Next:** Seed ke type ke hisaab se tools aur sources chuno.
2. **Step 2: Gather Basic Info**
   - **Action:** Seed se basic details collect karo – naam, location, ya related identifiers.
   - **Tools/Sources:**
     - **Username:** Sherlock (github.com/sherlock-project/sherlock) – 400+ sites pe accounts dhoondho.
     - **Email:** Epieos (tools.epieos.com) – Google, social media links.
     - **Domain:** WHOIS (who.is) – owner, registration date.
     - **Phone:** Truecaller, PhoneInfoga – name, carrier.
   - **Example:**
     - Seed: rishikabra132

- Result: Twitter (@rishikabra), Facebook (rishikabra132).

- **Decision:** Kya info mili?
  - **Yes:** Step 3 pe jao.
  - **No:** Seed change karo ya Step 6 (Advanced Search) pe jao.

3. **Step 3: Expand Identifiers**

- **Action:** Basic info se aur identifiers nikalo – emails, phone numbers, subdomains.
- **Tools/Sources:**
  - **Social Media:** Profile bios, posts – email ya phone mil sakta hai.
  - **Domain:** Subfinder (apt install subfinder) – subdomains (e.g., academy.cybersudo.org).
  - **Email:** SignalHire – LinkedIn profile se phone ya company.
- **Example:**
  - Twitter (@rishikabra) → Bio: "Contact: rishi.kabra@gmail.com".
  - cybersudo.org → Subdomains: www, academy.
- **What to Do:** Naye identifiers ko list karo (e.g., emails.txt, phones.txt).
- **Next:** Har identifier ke liye Step 2 repeat karo ya Step 4 pe jao.

4. **Step 4: Verify and Cross-Check**

- **Action:** Mil information ko verify karo – kya ye target se related hai ya duplicate hai?
- **Tools/Sources:**
  - **Email:** HaveIBeenPwned – breach mein hai ya nahi.
  - **Phone:** WhatsApp, Telegram – active hai ya nahi.
  - **Domain:** Httprobe – subdomains live hain ya nahi.
- **Example:**
  - rishi.kabra@gmail.com → LinkedIn pe verified (same name).
  - +91-9876543210 → WhatsApp pe "Rishi" dikha.
- **Decision:** Valid hai?
  - **Yes:** Step 5 pe jao.
  - **No:** Discard karo aur Step 2 ya 3 pe wapas jao.

5. **Step 5: Deep Dive (Metadata & Historical Data)**

- **Action:** Identifiers se deep info lo – metadata, past data, ya hidden details.
- **Tools/Sources:**
  - **Files:** FOCA – PDFs/DOCs se metadata (usernames, software).
  - **Website:** Wayback Machine (archive.org) – purane versions (e.g., deleted email).
  - **Domain:** DNSDumpster – DNS records, IPs.
- **Example:**
  - cybersudo.org (Wayback, 2019) → Old contact: rishi@cybersudo.org.
  - resume.pdf (FOCA) → Creator: Rishi Kabra, Software: Word 2016.
- **What to Do:** New findings ko add karo aur relationships note karo.

6. **Step 6: Advanced Search (If Needed)**
   - **Action:** Agar initial steps se kaafi data na mile, to advanced techniques use karo.
   - **Tools/Sources:**
     - **Google Dorks:** "site:*.cybersudo.org -inurl:www" – subdomains.
     - **SpiderFoot:** Domains, IPs, emails ek saath scan.
     - **OSINT Tracker:** Graph banao relationships ke liye.
   - **Example:**
     - Google Dork → support.cybersudo.org mila.
     - SpiderFoot → rishi@cybersudo.org se 5 aur domains linked.
   - **Next:** New data ko Step 3 se process karo.
7. **Step 7: Structure and Visualize**
   - **Action:** Saari info ko clean karo aur visualize karo – table ya graph mein.
   - **Tools:**
     - **Notion:** Table banao – Field, Value, Source.
     - **OSINT Tracker:** Relationship map banao (e.g., Rishi → LinkedIn → Phone).
   - **Example Table:**

Field	Value	Source
Name	Rishi Kabra	https://linkedin.com/in/rishi-kabra
Email	rishi.kabra@gmail	Wayback Machine, rishikabra.com

   - **Graph:** Rishi → LinkedIn (Works At) → Phone (Found Via SignalHire).
8. **Step 8: Export and Report**
   - **Action:** Final investigation ko save aur share karo.
   - **Tools:**
     - **Notion Export:** HTML ya PDF mein backup.
     - **OSINT Tracker Export:** JSON file mein graph save.
   - **What to Do:** Report banao – findings, sources, aur visuals ke saath.

Flowchart Visualization (Text Form):

```
Start

[Step 1: Define Seed]      (e.g., rishikabra132)

[Step 2: Gather Basic Info]      (Twitter, Facebook mila?)
      Yes        No
[Step 3: Expand Identifiers]      [Step 6: Advanced Search]
      (e.g., email, subdomains)           (Google Dorks, SpiderFoot)
[Step 4: Verify & Cross-Check]      New Data
      Yes
[Step 5: Deep Dive]      (Metadata, Wayback)
```

```
[Step 7: Structure & Visualize]     (Notion, OSINT Tracker)

[Step 8: Export & Report]     (HTML, JSON)

End
```

Real-Life Example – Rishi Kabra Investigation:

- **Seed:** rishikabra132 (username).
- **Step 2:** Sherlock se Twitter (@rishikabra), Facebook (rishikabra132) mile.
- **Step 3:** Twitter bio se email: rishi.kabra@gmail.com, SignalHire se phone: +91-9876543210.
- **Step 4:** Email LinkedIn pe verified, phone WhatsApp pe active.
- **Step 5:** Wayback se rishikabra.com pe purana resume mila – Software: Word 2016.
- **Step 6:** Google Dork "site:*.rishikabra.com" se blog.rishikabra.com mila.
- **Step 7:** Notion table aur OSINT Tracker graph banaya – Rishi → Twitter → Email → Phone.
- **Step 8:** HTML export kiya – offline backup ready.

How This Helps:

- **What to Do:** Har step batata hai info ke saath kya karna hai – e.g., username se social media, email se phone.
- **No Steps Missed:** Flowchart se har angle cover hota hai – basic se deep dive tak.
- **Example Insight:** Rishi ka phone SignalHare se mila, jo Step 3 bina miss kiye na hota.

Extra Tips:

- **Draw It:** Paper ya Miro.com pe flowchart sketch karo – visual memory ke liye.
- **Iterate:** Har new info ke saath flowchart wapas chalo – loop banaye rakho.
- **Save:** Notion mein flowchart ka text version rakho – quick reference ke liye.

Tables

Step	Action	Outcome
Define Seed	Choose Starting Point	Direction Set
Gather Info	Basic Details	Identifiers Found
Deep Dive	Metadata	Hidden Insights

Table 74: OSINT Flowchart Benefits

Summary

- Seed se shuru karo – info expand karo.
- Verify aur deep dive karo.
- Visualize aur export – structured rakho.

Point To Note

OSINT flowchart ek step-by-step guide hai jo investigation ko structured rakhta hai – **seed** se shuru karo, basic info lo, identifiers expand karo, verify karo, deep dive karo, aur visualize/export karo. Ye process (e.g., Rishi Kabra ka case) har info piece ko actionable banata hai aur koi step miss nahi hone deta. Systematic approach ke saath, ye flowchart aapka OSINT game organize aur powerful banata hai – har investigation ko clear direction do!

==========

Free OSINT Practice Labs or CTF

Free OSINT practice labs and Capture The Flag (CTF) challenges OSINT skills ko sharpen karne ka ek shandaar tareeka hain – ye platforms aapko real-world scenarios mein practical experience dete hain, jaise image metadata analysis, social media tracking, aur geospatial intelligence. Ye labs aur CTFs beginners se lekar advanced investigators tak ke liye perfect hain – aur sabse badi baat, ye free hain! Ismein hum dekhte hain chaar top free resources: **TryHackMe** ke OSINT rooms, **Cyber Detective CTF** by Cardiff University, **OSINT Dojo**, aur **Sourcing Games**. Har ek apne unique challenges ke saath aata hai – image-based puzzles se lekar dark web navigation tak. Chalo inko step-by-step explore karte hain aur dekhte hain kaise ye aapke OSINT game ko next level pe le ja sakte hain.

1. TryHackMe (Free OSINT Rooms)

- **Kya Hai:** TryHackMe ek cybersecurity training platform hai jo free aur paid rooms offer karta hai – iske OSINT rooms beginners ke liye perfect hain aur practical skills sikhate hain.
- **How to Access:** tryhackme.com pe sign up karo – free tier mein ye rooms available hain.
- **Key Rooms:**
  1. **OhSINT:**
     - **Focus:** Image metadata (EXIF data) aur reverse image searches ka use karke challenges solve karna.
     - **Example Task:** Ek photo di jati hai – aapko EXIF data (camera model, timestamp) extract karna hai aur Google Reverse Image Search se location ya owner dhoondhna hai.
     - **Tools:** ExifTool, Google Images.
     - **Learning:** Metadata kaise secrets reveal karta hai.
  2. **WebOSINT:**
     - **Focus:** Website-based OSINT investigation.

- **Example Task:** Ek domain (e.g., republicofkoffee.com) diya jata hai – WHOIS se owner info, Wayback Machine se past versions, aur IP history se hosting details nikalo.
- **Tools:** WHOIS, DNSDumpster, Wayback Machine.
- **Learning:** Website ke digital footprint ka analysis.

3. **SoMeSINT:**
   - **Focus:** Social Media Intelligence (SOCMINT) – e.g., ek mysterious husband ko Facebook aur Twitter pe track karna.
   - **Example Task:** Ek profile se shuru karo – posts, comments, aur connections se wife ka naam ya location dhoondho.
   - **Tools:** Twitter Advanced Search, Facebook Graph Search (agar public data ho).
   - **Learning:** Social media patterns se intelligence gather karna.
4. **Sakura Room:**
   - **Focus:** Beginner-friendly OSINT fundamentals.
   - **Example Task:** Basic username tracking ya simple Google Dorks ka use.
   - **Tools:** Google, Sherlock.
   - **Learning:** OSINT ki basic building blocks.

2. Cyber Detective CTF (Cardiff University)

- **Kya Hai:** Cardiff University ke Cyber Society ne banaya ye free OSINT-focused CTF – 40+ challenges ke saath, jo real-world scenarios pe based hain.
- **How to Access:** ctf.cybersoc.wales pe jao – registration ke baad free access milta hai.
- **Categories:**
  1. **Life Online:**
     - **Focus:** Social media investigations aur username tracking.
     - **Example Task:** Ek Twitter handle se LinkedIn ya Instagram profile tak ka trail banao – username consistency check karo.
     - **Tools:** Sherlock, Namechk.
  2. **Evidence Investigation:**
     - **Focus:** Digital footprint aur hidden metadata analysis.
     - **Example Task:** Ek PDF ya image se metadata (creator, timestamp) nikalo aur uska context samjho – jaise kisi event ki location.
     - **Tools:** FOCA, ExifTool.
- **Learning:** Analytical skills ko test karta hai – jaise ek person ka online behavior samajhna ya evidence connect karna.
- **Note:** Kuch challenges mein data ab online nahi hai (e.g., "leaveamessage"), to creativity chahiye.

3. OSINT Dojo

- **Kya Hai:** Ek free resource hub jo OSINT methodologies aur challenges offer karta hai – beginners aur intermediates ke liye ideal.

- **How to Access:** osintdojo.com pe visit karo – koi sign-up nahi, direct resources aur tasks.
- **Key Features:**
  - **Image-Based Scenarios:**
    - **Focus:** Geolocation puzzles aur metadata extraction.
    - **Example Task:** Ek photo diya jata hai – EXIF data se coordinates nikalo aur Google Earth pe exact location pinpoint karo.
    - **Tools:** ExifTool, Google Earth, GeoGuessr.
  - **Challenges:** Step-by-step tasks jo skills build karte hain – badges bhi milte hain progress ke liye.
- **Learning:** Real-world OSINT techniques – jaise IMINT (Image Intelligence) aur GEOINT (Geospatial Intelligence).
- **Bonus:** Diagrams aur flowcharts bhi dete hain – investigation planning ke liye.

4. Sourcing Games

- **Kya Hai:** Ek gamified platform jo 30+ free OSINT challenges offer karta hai – immersive aur fun way mein skills practice karne ke liye.
- **How to Access:** sourcing.games pe jao – free sign-up ke baad challenges unlock hote hain.
- **Key Challenges:**
  1. **Geospatial Intelligence (GEOINT):**
     - **Focus:** Visual clues se locations pinpoint karna.
     - **Example Task:** Ek image mein building ya signboard se city ya street guess karo – Google Maps ya Street View ka use.
     - **Tools:** GeoGuessr, OpenStreetMap.
  2. **Dark Web Navigation:**
     - **Focus:** Simulated tasks jo dark web research sikhate hain (ethically).
     - **Example Task:** Ek .onion link diya jata hai – Tor Browser se content analyze karo aur related info nikalo (e.g., username ya Bitcoin address).
     - **Tools:** Tor Browser, Blockchain.com (Bitcoin tracing).
- **Learning:** Advanced OSINT skills – GEOINT se leke dark web tak ka exposure.
- **Note:** Challenges progressively hard hote hain – pehle 2 easy, phir complex.

Real-Life Practice Example – Rishi Kabra Investigation:

- **Seed:** Username "rishikabra132".
- **TryHackMe (OhSINT):** Ek photo se shuru – EXIF data se "Rishi Kabra" naam mila, reverse image search se Twitter handle (@rishikabra).
- **Cyber Detective CTF (Life Online):** Twitter se Facebook (rishikabra132) track kiya – bio mein email: rishi.kabra@gmail.com.

- **OSINT Dojo:** Photo ke background se geolocation kiya – Mumbai ka ek cafe pinpoint kiya Google Earth pe.
- **Sourcing Games (GEOINT):** Cafe ki image se street name confirm kiya – dark web task se ek related forum username mila.
- **Outcome:** Rishi ka social media, email, aur approximate location ek flowchart mein connect hua.

How These Help:

- **Practical Skills:** Image metadata, website recon, social media tracking, aur GEOINT hands-on seekho.
- **Beginner-Friendly:** Sakura Room ya OSINT Dojo se shuru karo – no prior knowledge chahiye.
- **Real-World Scenarios:** Cyber Detective aur Sourcing Games real-life OSINT simulate karte hain – jaise missing person cases ya scam investigations.

Extra Tips:

- **Start Small:** TryHackMe ke Sakura Room se basics seekho, phir WebOSINT pe jao.
- **Tools:** ExifTool, Sherlock, Google Earth apne system pe rakho – har CTF mein kaam aayenge.
- **Save Progress:** Notion mein har challenge ka result note karo – e.g., "rishikabra132 → @rishikabra (Twitter)".
- **Community:** TryHackMe ya Sourcing Games ke Discord join karo – tips aur writeups milte hain.

Tables

Platform	Focus	Skills
TryHackMe	Metadata, SOCMINT	Basics to Intermediate
Cyber Detective	Analytical	Social Media, Evidence
OSINT Dojo	GEOINT, IMINT	Geolocation
Sourcing Games	GEOINT, Dark Web	Advanced Tracking

Table 75: Free OSINT Platforms Overview

Summary

- TryHackMe se basics seekho – OhSINT, WebOSINT.
- Cyber Detective aur OSINT Dojo se analytical aur geolocation skills.
- Sourcing Games se advanced GEOINT aur dark web seekho.

Point To Note

Free OSINT practice labs aur CTFs jaise **TryHackMe** (OhSINT, WebOSINT, SoMeSINT, Sakura), **Cyber Detective CTF**, **OSINT Dojo**, aur **Sourcing Games** aapko metadata analysis, social media intelligence, aur geospatial skills sikhate hain – woh bhi free mein! Har platform alag flavor deta hai – TryHackMe beginners ke liye, Cyber Detective analytical minds ke liye, OSINT Dojo resources ke liye, aur Sourcing Games advanced GEOINT aur dark web ke liye. Rishi Kabra jaise cases solve karke seekho – har tool aur step ko systematically use karo aur apna OSINT game elevate karo!

==========DONE==========