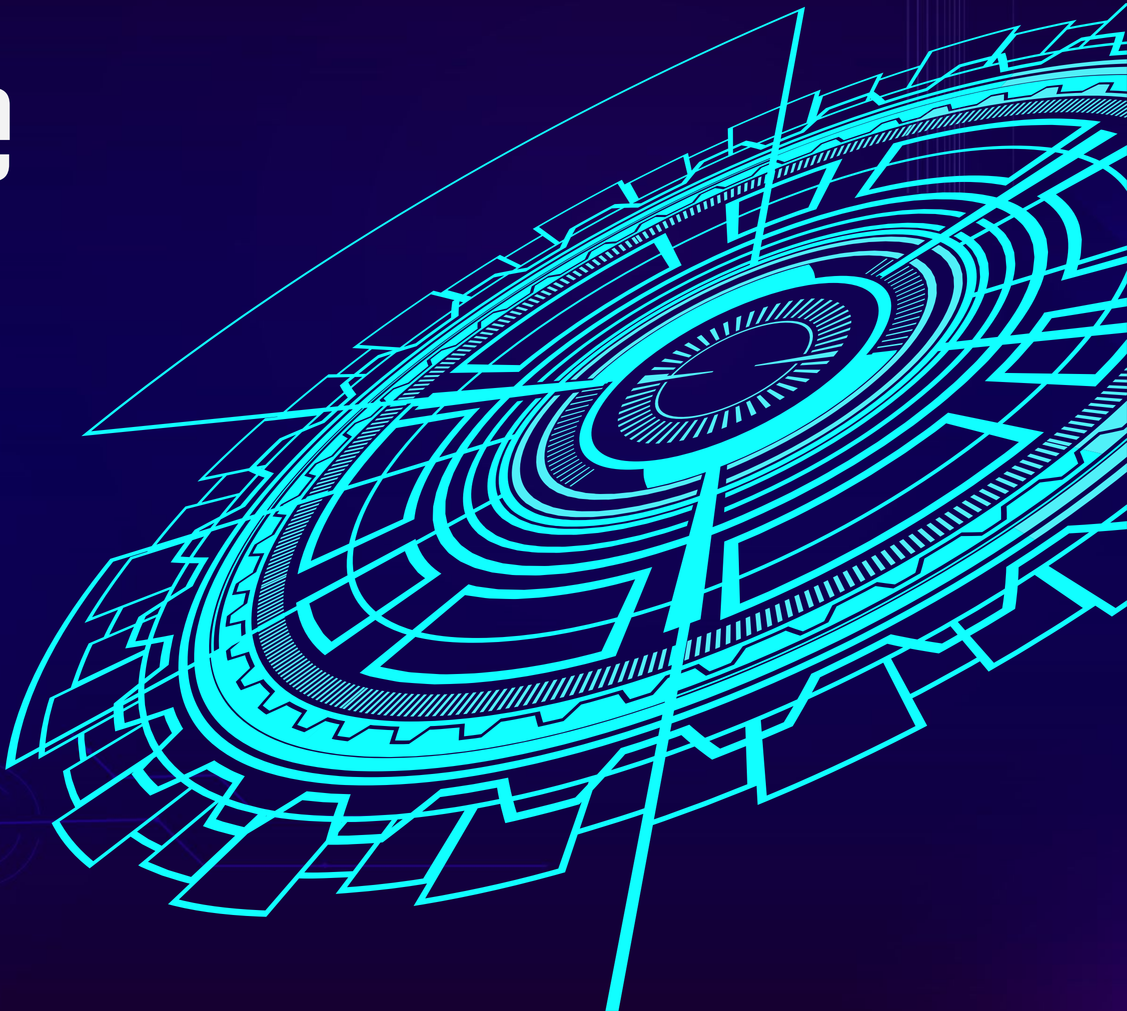
Open Source Intelligence

where common man becomes hacker



$ whoami

ADITHYAN AK

- Offensive Security Certified Professional (OSCP), CEH (Master)
- Head of OWASP Coimbatore
- 6+ years into Infosec
- Expertise in web app security, network security & Open Source Intelligence
- Authored few exploits and owned CVEs
- Speaker at various conferences, workshops (IITM Research Park, NIT, Defcon etc)
- Hall of fame in Microsoft, Apple, Intel, Avira, Oppo, etc
- Passion for making and breaking stuffs

AGENDA

01 Osint

What, where, why OSINT
Demystifying OSINT myths

02 Practicals

scenarios where osint can practically be applied

03 Sources

Sources from where data can be extracted

04 Mitigations & Laws

Preventing yourself from becoming a target

WHAT IS OSINT?

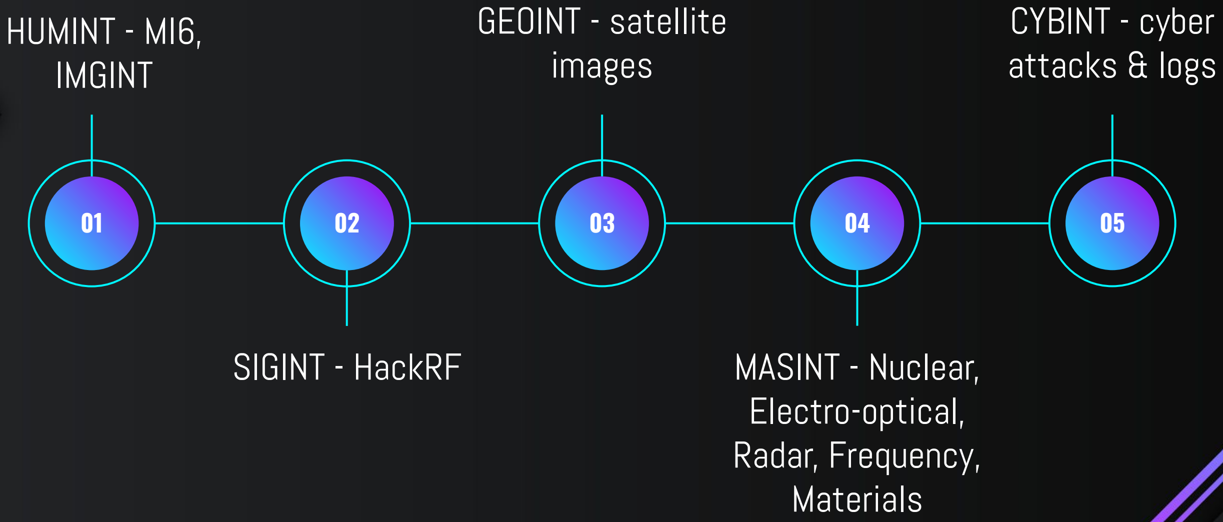
data collected from publicly available sources to be used in an intelligence context.

used in national security, law enforcement, and business intelligence

the easiest subdomain to get started with in cybersecurity

requires more common sense and understanding the connections

INTELLIGENCE GATHERING



01 HUMINT - MI6, IMGINT

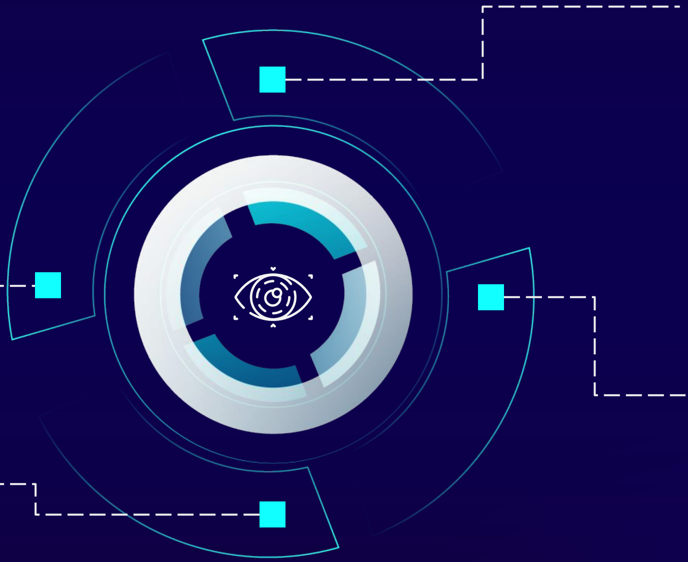
02 SIGINT - HackRF

03 GEOINT - satellite images

04 MASINT - Nuclear, Electro-optical, Radar, Frequency, Materials

05 CYBINT - cyber attacks & logs

WHAT CAN I OSINT



PEOPLE

Name, username, email, phone number, emotions, geoloc and much more information

IP

Geolocation, proxy/vpn/tor, IOT device, download history

DOMAIN

Subdomains, MX records, Ports discovery, WHOIS lookup

OTHERS

MAC address, images, BTC address, vehicle number

WHY OSINT ?

Allows you to gather huge amounts of actionable intelligence without ever sending a packet to your target.

Why OSINT

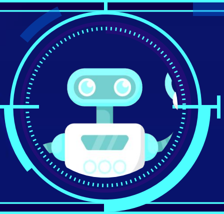
Password cracking/KBA optimization/Social Engineering:

- pet name
- year of birth
- significant other/relatives names
- place of birth
- favorite food
- where they were married
- previous addresses
- previous employers
- list of schools
- year account or mortgage was opened

People OSINT Approach

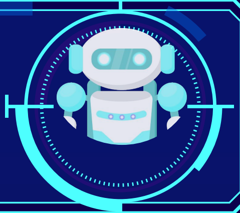
- Start with what you know (email, username, etc.)
- Define requirements (what you want to get)
- Gather the data
- Analyze collected data
- Pivot as-needed using new gathered data
- Validate assumptions
- Generate report

PEOPLE OSINT



Name

High priority input if the person is famous



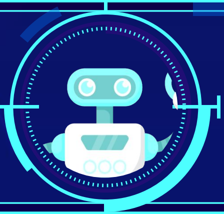
Username

High priority input if the person is an average internet user

Phone number

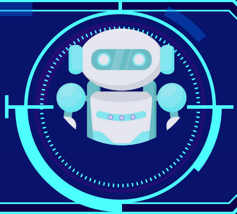
High priority input if the person is a ghost

PEOPLE OSINT



Email

High priority input if you wanna get access to the target

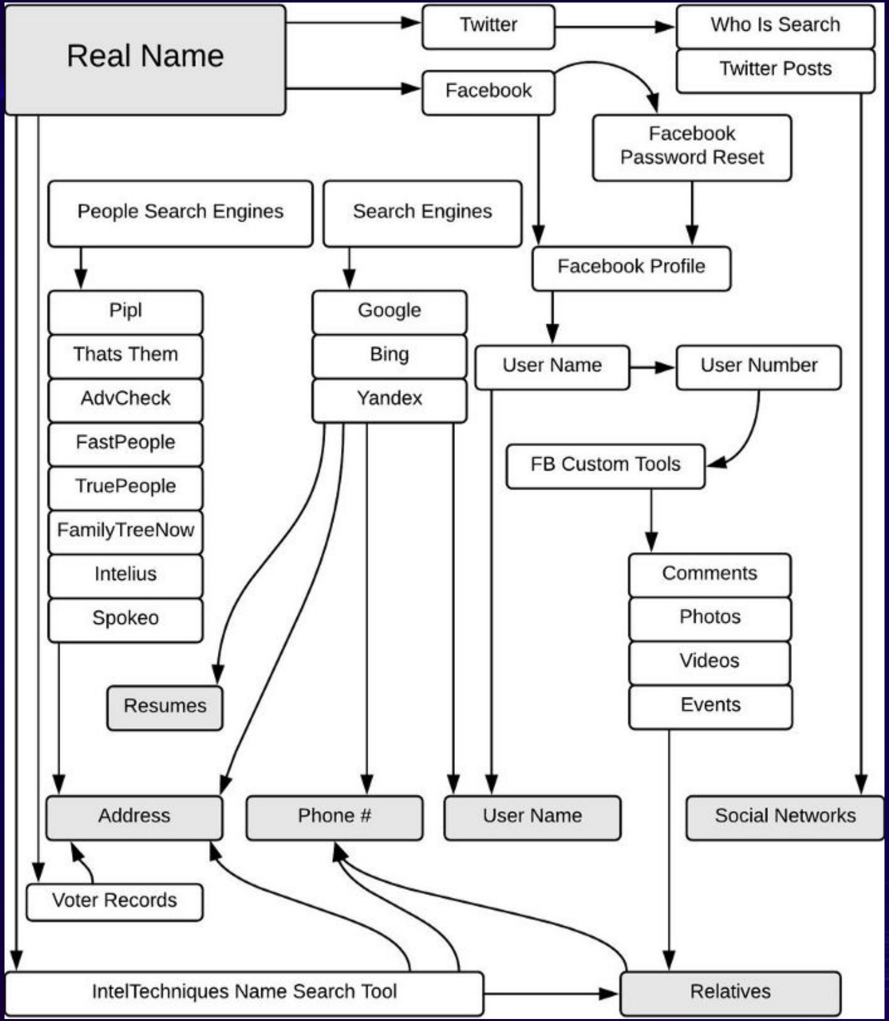


Image

Low priority input unless you have really good image analysis skills

Date Of Birth

Low priority input but unique factor for the search



Real Name

Twitter

Who Is Search

Twitter Posts

Facebook

Facebook Password Reset

People Search Engines

Search Engines

Facebook Profile

Pipl

Thats Them

AdvCheck

FastPeople

TruePeople

FamilyTreeNow

Intelius

Spokeo

Google

Bing

Yandex

User Name

User Number

FB Custom Tools

Comments

Photos

Videos

Events

Resumes

Address

Phone #

User Name

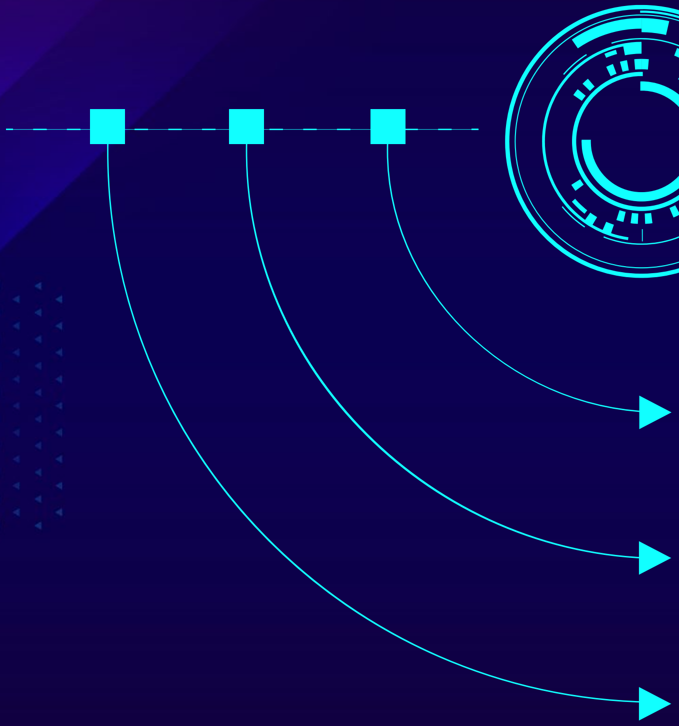
Social Networks

Voter Records

IntelTechniques Name Search Tool

Relatives

NAME



Search Engines	Customised search engines, google dorks
People Search	Inclined towards foreign nationals
Govt Portals	Voter ID, Electoral Rolls

DORKS

Operators :

- inurl - www.example.com/adithyan+ak
- intitle
- intext
- filetype
- site

Format :

- operator : “data”
- Ex : inurl : “adithyanak” | you can combine dorks too
- No space

CUSTOM SEARCH ENGINES

Pre-Configured - https://cse.google.com/cse?cx=005553992128112222999:w1eonxpepby

Create your own - https://programmablesearchengine.google.com/about/

People Search

- Google
- Bing - https://www.bing.com/
- DuckDuckGo - https://duckduckgo.com/
- Yandex - https://yandex.com/
- Voter Information - https://electoralsearch.in/

USER NAME

Search Engines

Leveraging search engines to construct list of possible usernames

Social Networks

Directly searching in social networks for undiscoverable accounts

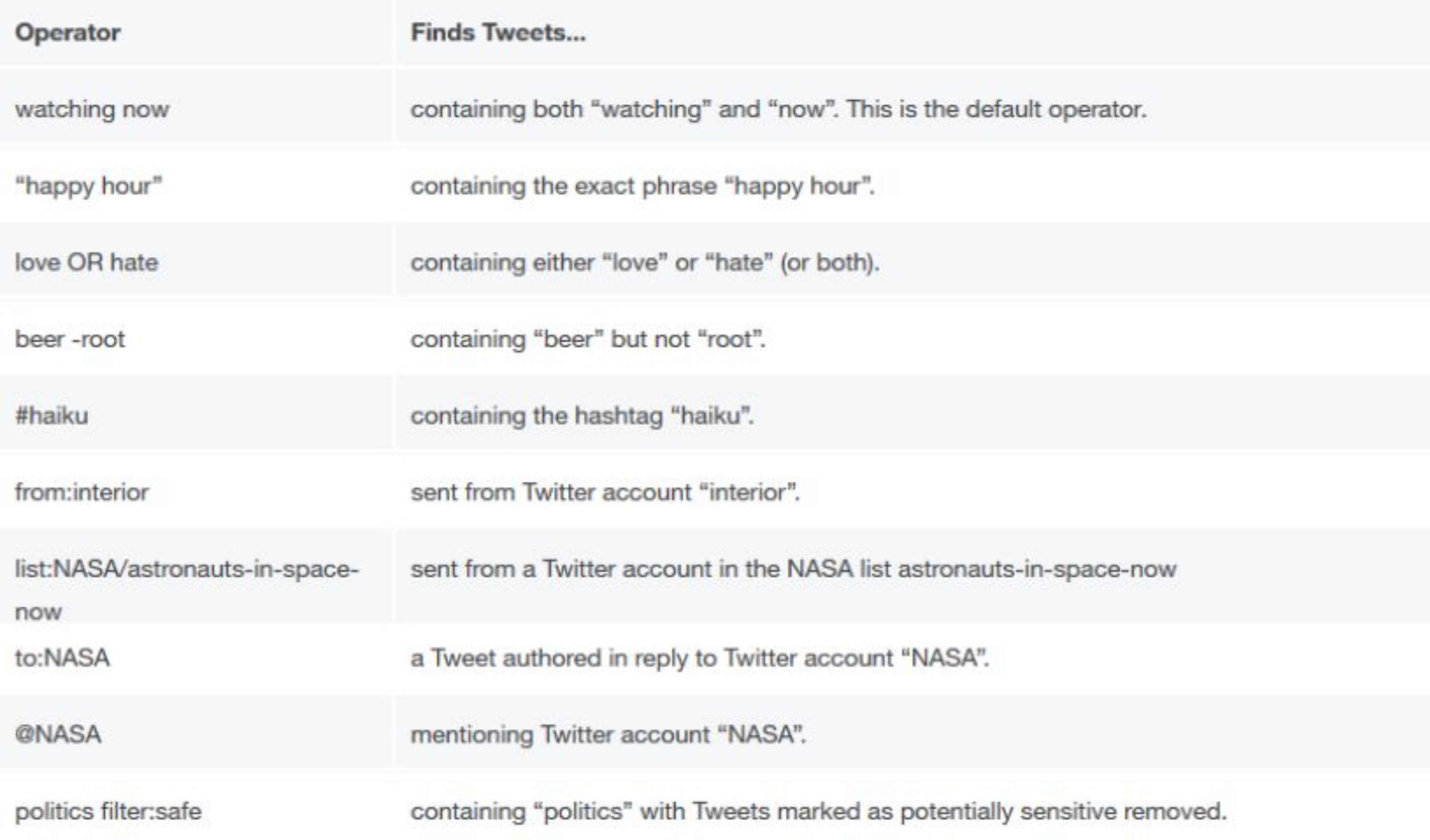
Username Narrow Down

Narrow down approach in search engines

Username

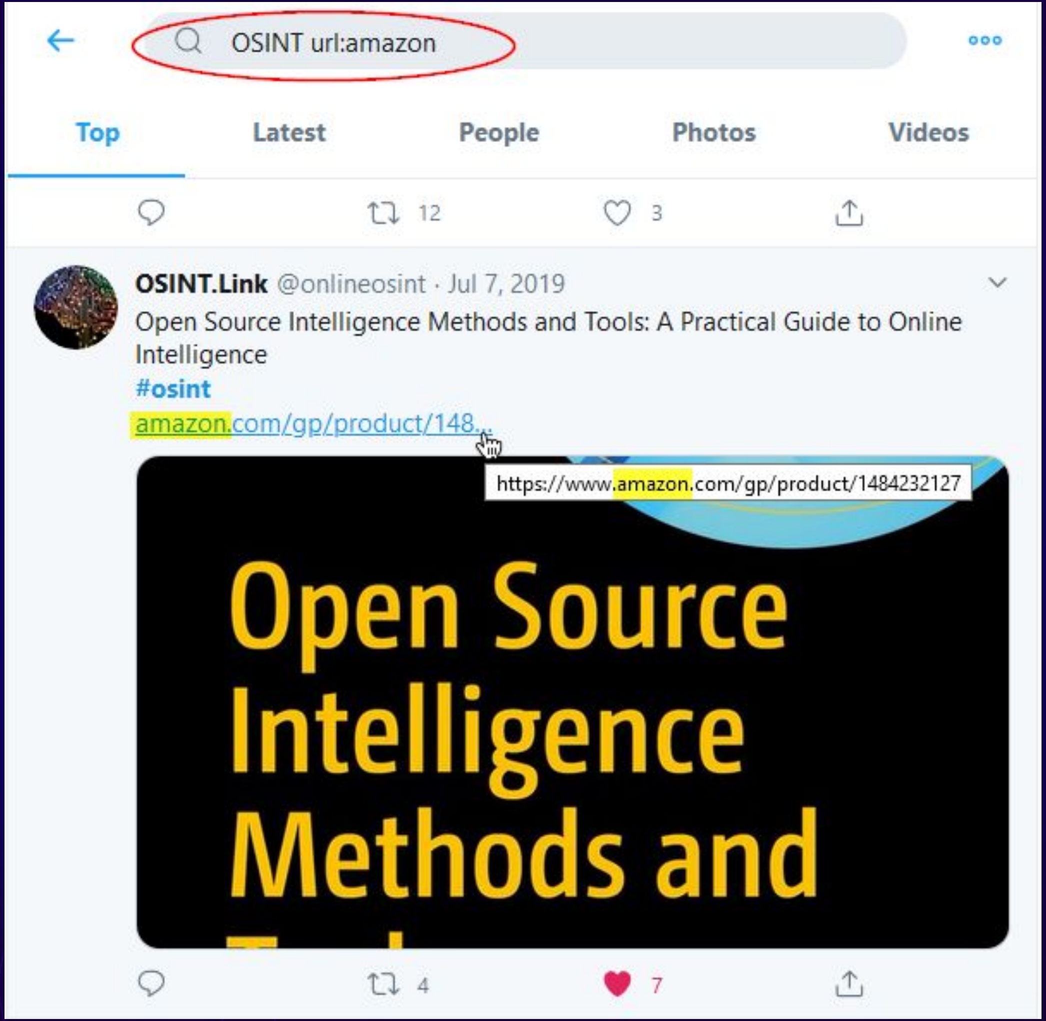
- Check Usernames - https://checkusernames.com/
- Instant Usernames - https://instantusername.com/
- User search - https://usersearch.org/
- Whats my name - https://whatsmyname.app/
- Search POF - https://searchpof.com/
- https://twitter.com/search-advanced
- https://www.trendsmap.com/

Twitter



Operator	Finds Tweets...
watching now	containing both "watching" and "now". This is the default operator.
"happy hour"	containing the exact phrase "happy hour".
love OR hate	containing either "love" or "hate" (or both).
beer -root	containing "beer" but not "root".
#haiku	containing the hashtag "haiku".
from:interior	sent from Twitter account "interior".
list:NASA/astronauts-in-space-now	sent from a Twitter account in the NASA list astronauts-in-space-now
to:NASA	a Tweet authored in reply to Twitter account "NASA".
@NASA	mentioning Twitter account "NASA".
politics filter:safe	containing "politics" with Tweets marked as potentially sensitive removed.

Twitter



OSINT url:amazon

OSINT.Link @onlineosint · Jul 7, 2019

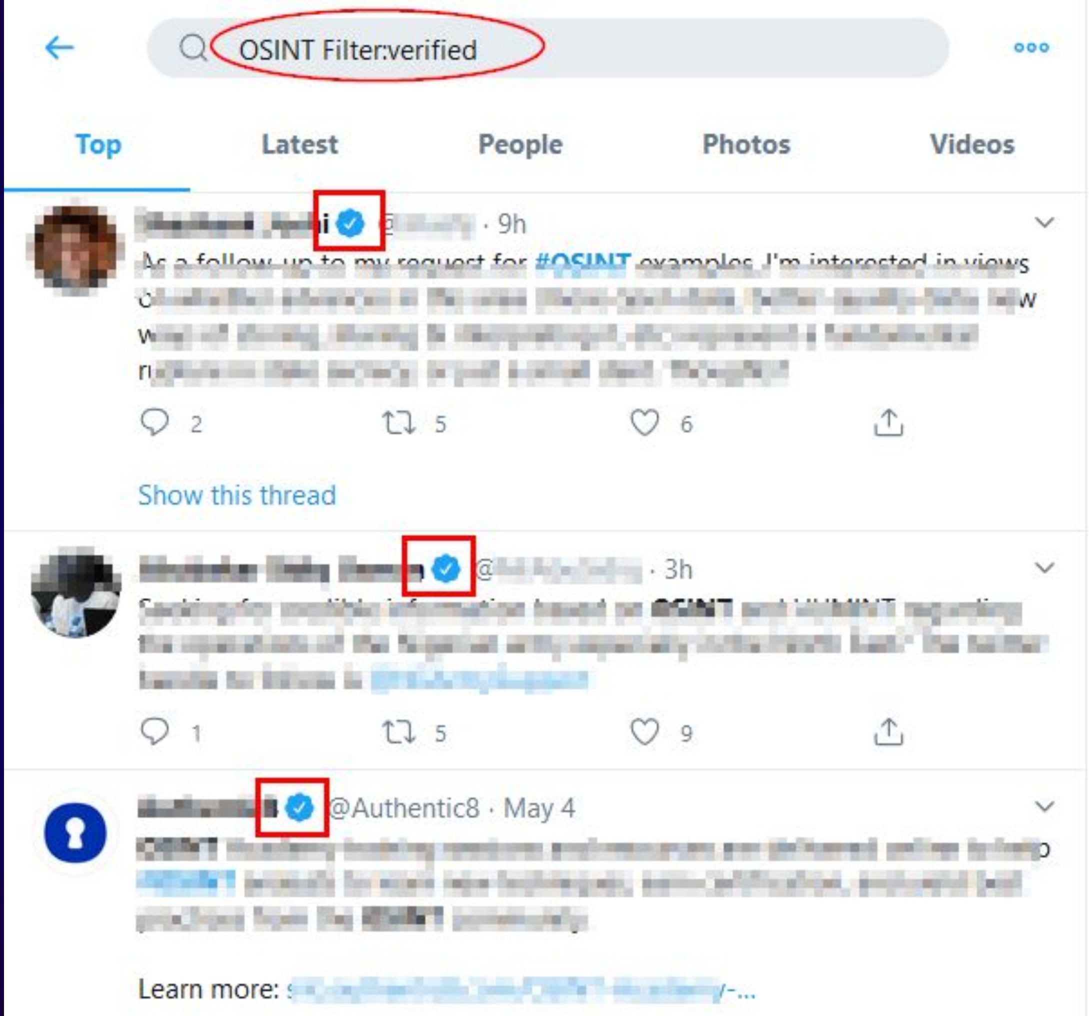
Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence

#osint

amazon.com/gp/product/148...

https://www.amazon.com/gp/product/1484232127

Twitter



OSINT Filter:verified

[redacted] @[redacted] · 9h

[redacted]

Show this thread

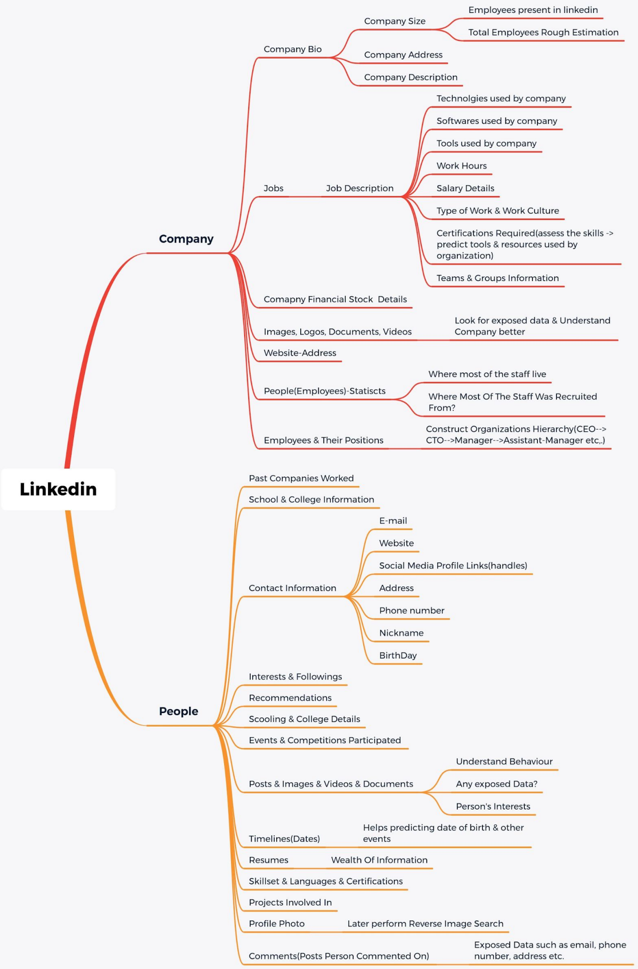
[redacted] @[redacted] · 3h

[redacted]

[redacted] @Authentic8 · May 4

[redacted]

Learn more: [redacted]



- Linkedin
  - Company
    - Company Bio
      - Company Size
        - Employees present in linkedin
        - Total Employees Rough Estimation
      - Company Address
      - Company Description
    - Jobs
      - Job Description
        - Technolgies used by company
        - Softwares used by company
        - Tools used by company
        - Work Hours
        - Salary Details
        - Type of Work & Work Culture
        - Certifications Required(assess the skills -> predict tools & resources used by organization)
        - Teams & Groups Information
    - Comapny Financial Stock Details
    - Images, Logos, Documents, Videos
      - Look for exposed data & Understand Company better
    - Website-Address
    - People(Employees)-Statiscts
      - Where most of the staff live
      - Where Most Of The Staff Was Recruited From?
    - Employees & Their Positions
      - Construct Organizations Hierarchy(CEO-->CTO-->Manager-->Assistant-Manager etc.,)
  - People
    - Past Companies Worked
    - School & College Information
    - Contact Information
      - E-mail
      - Website
      - Social Media Profile Links(handles)
      - Address
      - Phone number
      - Nickname
      - BirthDay
    - Interests & Followings
    - Recommendations
    - Scooling & College Details
    - Events & Competitions Participated
    - Posts & Images & Videos & Documents
      - Understand Behaviour
      - Any exposed Data?
      - Person's Interests
    - Timelines(Dates)
      - Helps predicting date of birth & other events
    - Resumes
      - Wealth Of Information
    - Skillset & Languages & Certifications
    - Projects Involved In
    - Profile Photo
      - Later perform Reverse Image Search
    - Comments(Posts Person Commented On)
      - Exposed Data such as email, phone number, address etc.

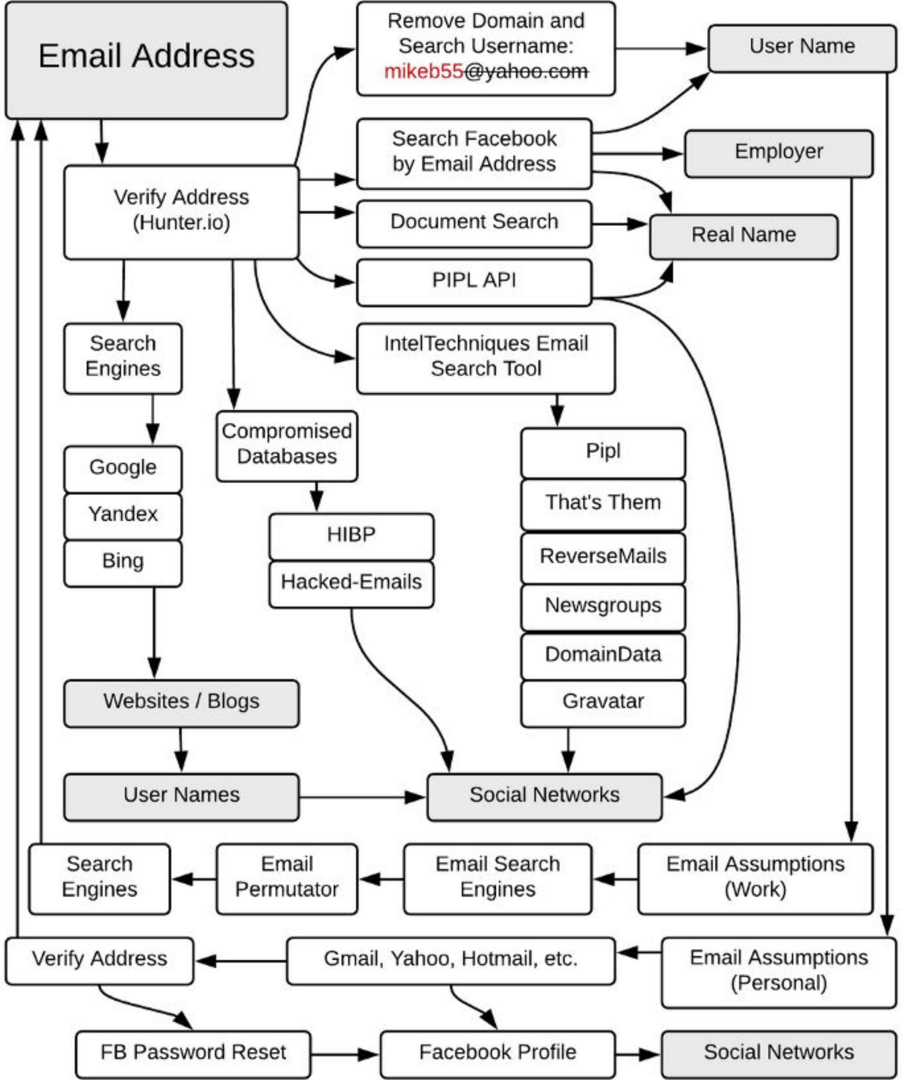
Design by le0li9ht

Phone Number

- Truecaller
- GetContact
- HLR Lookup - https://www.free-hlr.com/
- Numverify - https://numverify.com/
- Google password reset

Email

- Email Permutations - http://metricsparrow.com/toolkit/email-permutator/
- Email Rep - https://emailrep.io/
- Hunter.io - https://hunter.io/
- Ghostproject - https://ghostproject.fr/
- Myrz - http://myrz.org



Email Address

Verify Address (Hunter.io)

Remove Domain and Search Username: mikeb55~~@yahoo.com~~

User Name

Search Facebook by Email Address

Employer

Document Search

Real Name

PIPL API

Search Engines

Google

Yandex

Bing

Compromised Databases

HIBP

Hacked-Emails

IntelTechniques Email Search Tool

Pipl

That's Them

ReverseMails

Newsgroups

DomainData

Gravatar

Websites / Blogs

User Names

Social Networks

Search Engines

Email Permutator

Email Search Engines

Email Assumptions (Work)

Verify Address

Gmail, Yahoo, Hotmail, etc.

Email Assumptions (Personal)

FB Password Reset

Facebook Profile

Social Networks

Image

- Reverse image search - https://www.duplichecker.com
- Metadata - https://www.pic2map.com | EXIF Tool
- Common sense analysis

Domain

- Whois - https://whois.domaintools.com/
- NSlookup - https://mxtoolbox.com/DnsLookup.aspx
- MX Lookup - https://mxtoolbox.com
- Wappalyzer
- Web Archive - https://archive.org/
- Sublister - https://github.com/aboul3la/Sublist3r
- Virustotal - https://www.virustotal.com/gui/home/url
- What CMS - https://whatcms.org

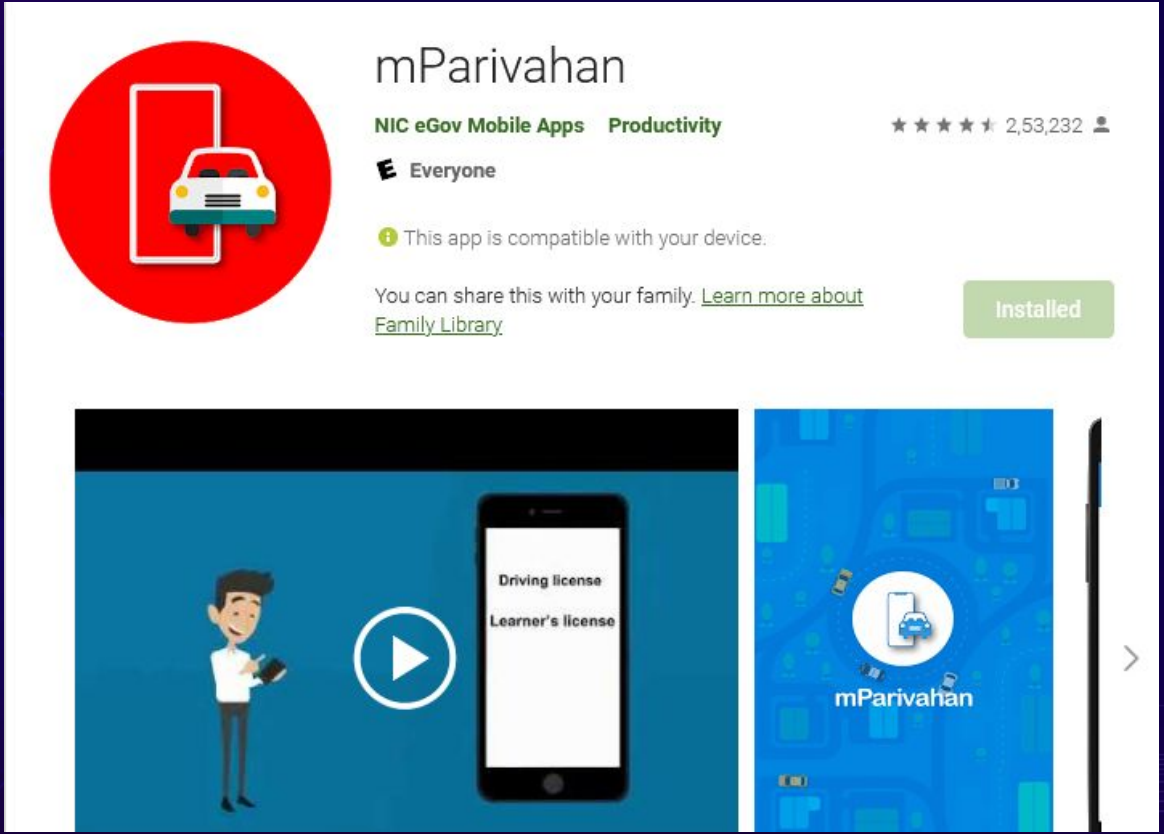
IP

- Shodan
- Censys
- IP API - https://ipapi.co
- Ip2Location
- ip2proxy

Misc

- Emotions - https://tone-analyzer-demo.ng.bluemix.net/
- Vehicle - https://vahan.nic.in/nrservices/faces/user/searchstatus.xhtml
- Google Hacking Database - https://www.exploit-db.com/google-hacking-database
- Camera - http://www.insecam.org/
- People via camera - http://snradar.azurewebsites.net/
- MAC Address

VEHICLE DATA EXTRACTION



mParivahan

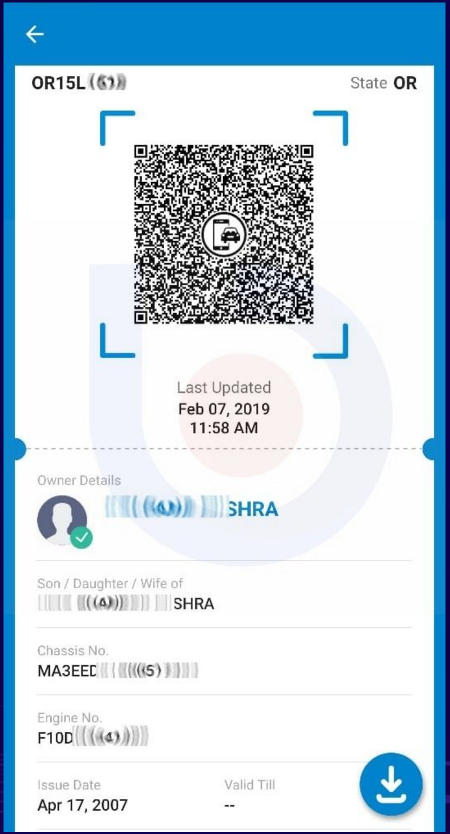
NIC eGov Mobile Apps   Productivity   ★★★★☆ 2,53,232

E Everyone

This app is compatible with your device.

You can share this with your family. Learn more about Family Library

Installed



OR15L [redacted]   State OR

Last Updated
Feb 07, 2019
11:58 AM

Owner Details
[redacted]SHRA

Son / Daughter / Wife of
[redacted]SHRA

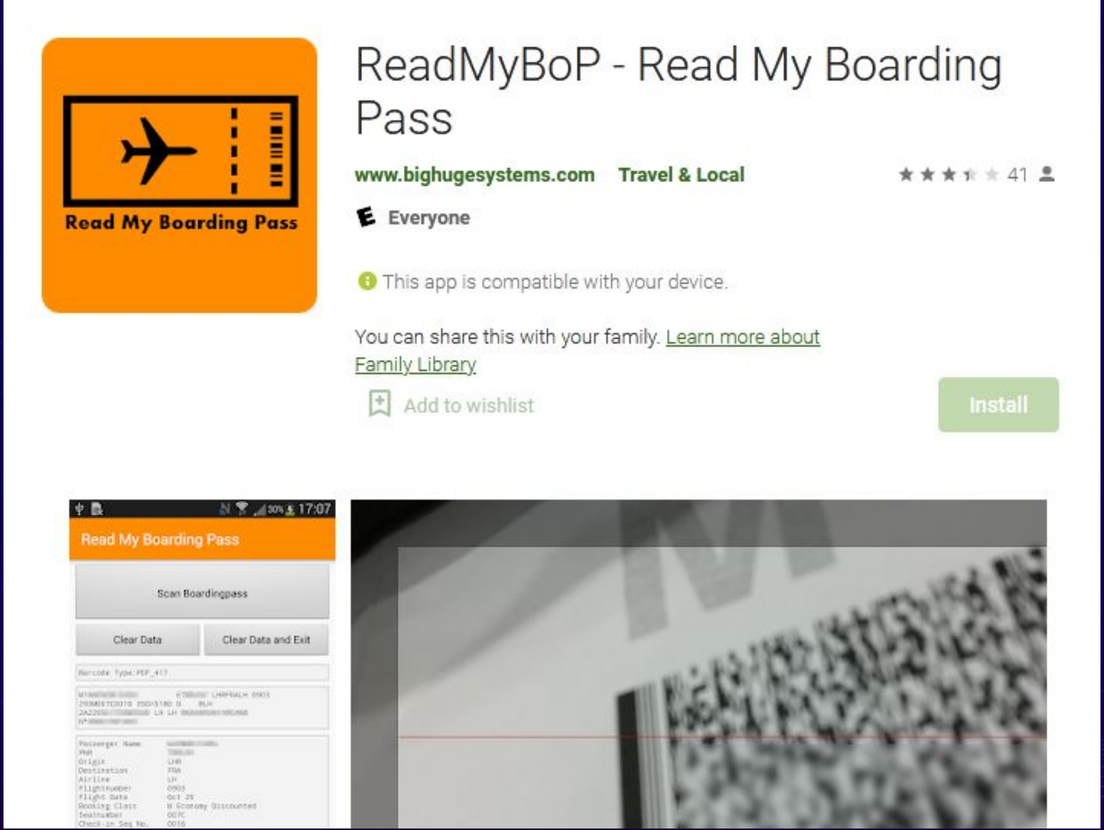
Chassis No.
MA3EED[redacted]

Engine No.
F10D[redacted]

Issue Date
Apr 17, 2007

Valid Till
--

BOARDING PASS



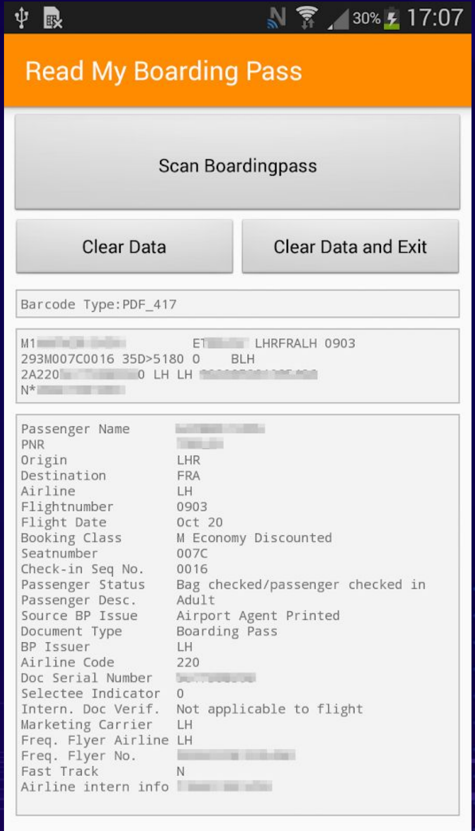
ReadMyBoP - Read My Boarding Pass

www.bighugesystems.com Travel & Local ★★★½☆ 41

Everyone

This app is compatible with your device.

You can share this with your family. Learn more about Family Library



```
Barcode Type:PDF_417
```

```
M1[redacted]          ET[redacted] LHRFRALH 0903
293M007C0016 35D>5180 0    BLH
2A220[redacted]0 LH LH [redacted]
N*[redacted]
```

```
Passenger Name       [redacted]
PNR                  [redacted]
Origin               LHR
Destination          FRA
Airline              LH
Flightnumber         0903
Flight Date          Oct 20
Booking Class        M Economy Discounted
Seatnumber           007C
Check-in Seq No.     0016
Passenger Status     Bag checked/passenger checked in
Passenger Desc.      Adult
Source BP Issue      Airport Agent Printed
Document Type        Boarding Pass
BP Issuer            LH
Airline Code         220
Doc Serial Number    [redacted]
Selectee Indicator   0
Intern. Doc Verif.   Not applicable to flight
Marketing Carrier    LH
Freq. Flyer Airline  LH
Freq. Flyer No.      [redacted]
Fast Track           N
Airline intern info  [redacted]
```

Boarding Pass Can Help Can Get You ?

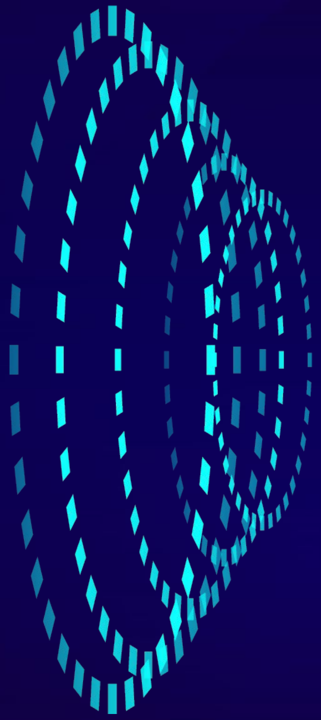
- Gender
- Which passenger number in the ticket
- Passenger Last name
- Passenger First name
- Ticket Type (Online/Physical)
- PNR
- Source
- Destination
- Flight Carrier
- Flight Number

Boarding Pass Can Help Can Get You ?

- Passenger Seat Class
- Seat Number
- Flight Sequence Number
- Passenger Clearance Status
- Passenger Checked IN/Not
- document type
- Where this document was printed at airport or somewhere else
- Flight Date
- Document issuing Flight company
- Document is authorised or not

Famous OSINT Tools

- https://intelx.io/tools
- https://www.aware-online.com/osint-tools/
- Maltego
- Spiderfoot



LEGAL ?

OSINT is 100% legal until you don't cross certain limits.

- Impersonation
- Social Engineering
- Buying breached data from dark web
- Stalking someone with malicious intent

THANKS

Does anyone have any questions?

root@adithyanak.com

adithyan_ak

facebook.com/akoffsec

@akoffsec

akoffsec

akoffsec