PROFESYONEL STALKING :)

OSINT (OPEN SOURCE INTELLIGENCE)

"0 TO HERO"

BEN KİMİM?

- Halit İnce
- Ege Üniversitesi Bilgisayar Mühendisliği
- Öğrenci

/halitiince

www.halitince.com

THREE ARROW SECURITY

OSINT

Linux

Programlama

Siber Güvenlik

Wargames / CTFs

/three-arrow-security

İÇERİK

- OSINT Nedir?
- Domain Merkezli Arama
- Kişi Merkezli Arama
    - Sosyal Medya
    - Telefon Numaraları
    - E-mailler
    - Konumlar
- Diğer

OSINT NEDİR ?

- Open Source Intelligence (Açık Kaynak İstihbarat)

  - Medya içerikleri: ses, video, resim ve fotoğraflar
  - Metin içerikleri: dokümanlar, makaleler, blog yazıları
  - Sosyal Medya
  - Veri Tabanları (Arşivler)
  - Domain'ler(Etki Alanları)

AKTİF VE PASİF BİLGİ TOPLAMA

- Etkileşim

Hedef ile etkileşime geçip geçmemek aktifliği ve pasifliği belirler.

OPSEC (OPERATIONAL SECURITY)

- Tor Network ve Browser
- VPN
- Spoofing User Agent
- Fake Persona Creation

fakenamegenerator.com

VPN

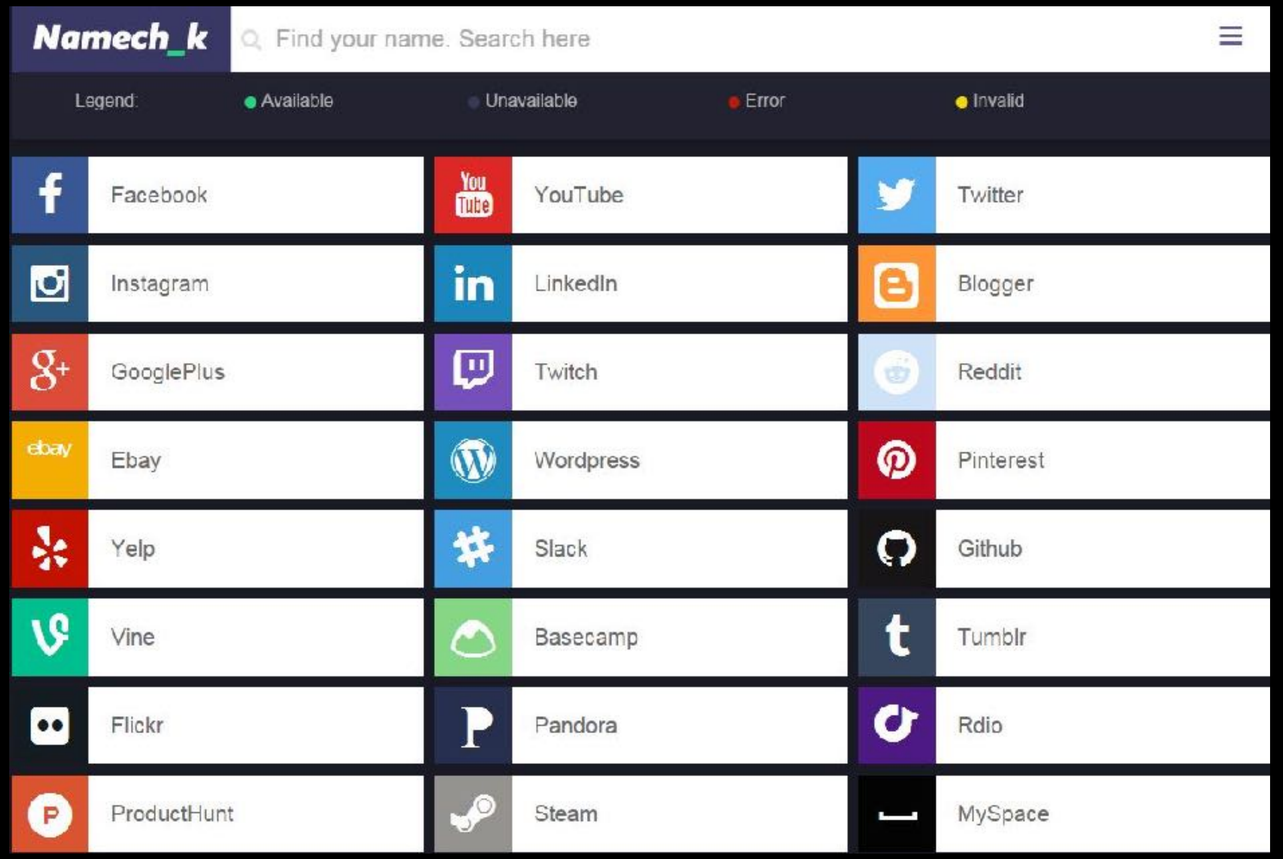
KİŞİ MERKEZLİ ARAMA

SOSYAL MEDYA

USERNAME

- Namechk
- Namechk (T)
- KnowEm
- NameCheckr
- UserSearch.org
- WhatsMyName (T)
- IntelTechniques Username Tools
- Thats Them
- Check Usernames
- Gaddr.me

Namechk



TWITTER

SEARCH

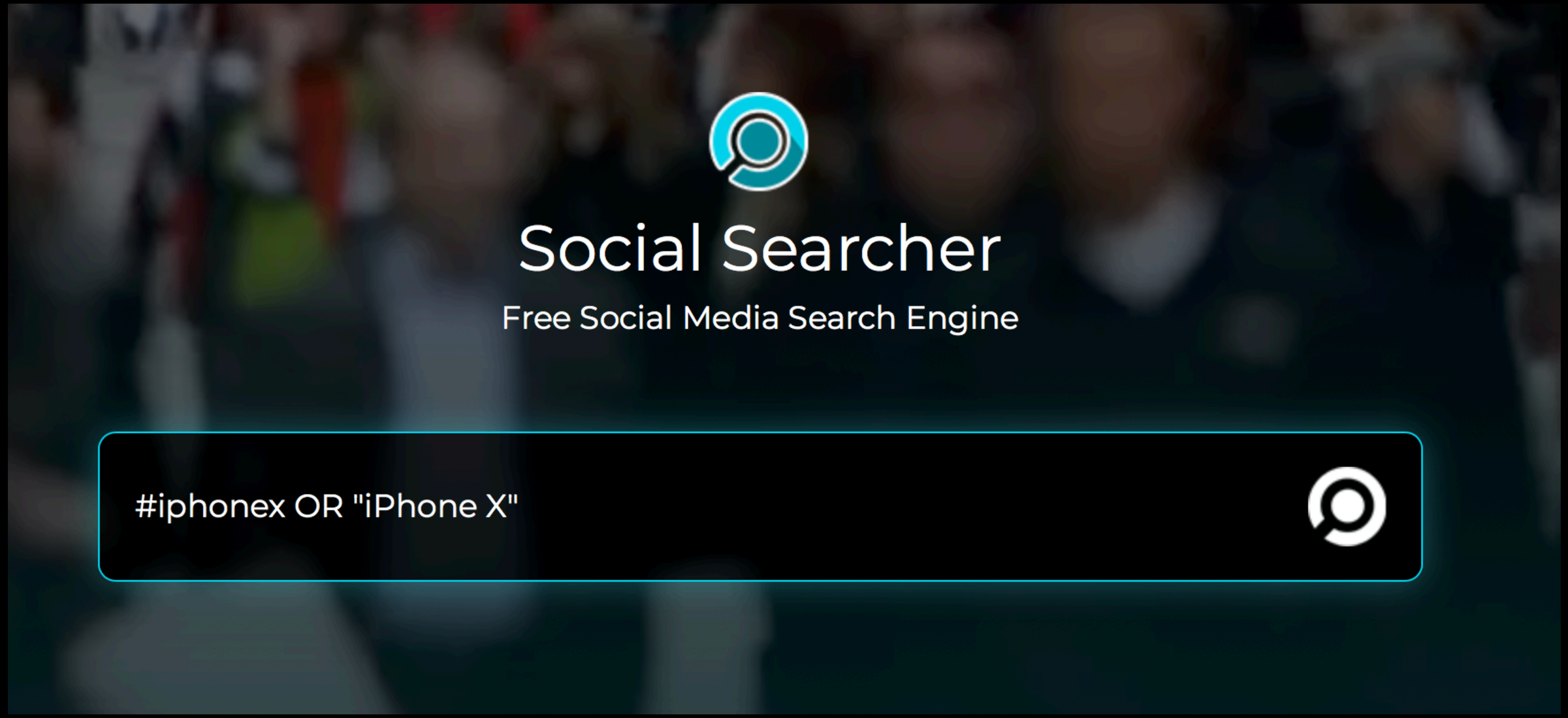
- Twitter Advanced Search
- Twitter Location Search
- Twitter Date Search
- Twitter Name Search
- Twitter User Directory
- Twitter Search for Live Streaming Video
- ConWeets
- Twitterfall
- Twellow
- First Tweet
- TweetReach
- BackTweets
- Moz Profile Search
- IntelTechniques Twitter Tools
- HootSuite
- TweetDeck
- Twopcharts
- Twitter Email Test
- Twoogel Search Engine
- Treeverse (T)

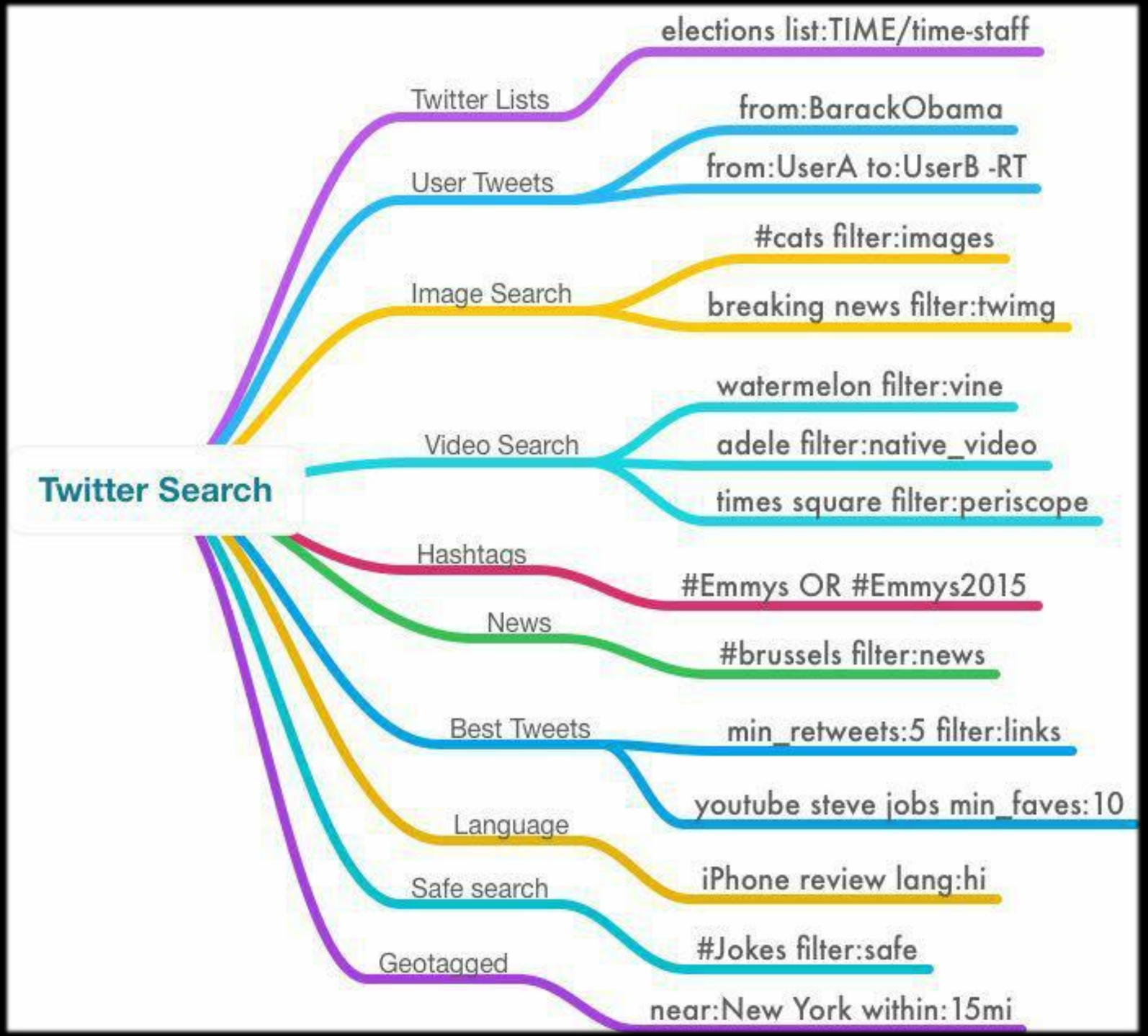
PROFILE

- Tweepsect
- Followerwonk Analyze
- Followerwonk Compare
- Twitonomy
- Fake Follower Check
- Klear
- First Tweet
- TweetTunnel
- Twitalyzer
- Foller.me Analytics
- MentionMapp
- SleepingTime
- Bioischanged (M)
- X0rz Tweets_analyzer
- Social Bearing

LOCATION

- GeoChirp
- GeoSocial Footprint
- TweetPaths
- TeachingPrivacy
- Echosec
- MIT Map
- Harvard Map
- One Million Tweet Map
- Creepy
- Tweepsmap
- GeoTweet
- MapD Tweetmap


Social Searcher
Free Social Media Search Engine
#iphonex OR "iPhone X"


Twitter Search
Twitter Lists
elections list:TIME/time-staff
User Tweets
from:BarackObama
from:UserA to:UserB -RT
Image Search
#cats filter:images
breaking news filter:twimg
Video Search
watermelon filter:vine
adele filter:native_video
times square filter:periscope
Hashtags
#Emmys OR #Emmys2015
News
#brussels filter:news
Best Tweets
min_retweets:5 filter:links
youtube steve jobs min_faves:10
Language
iPhone review lang:hi
Safe search
#Jokes filter:safe
Geotagged
near:New York within:15mi

FACEBOOK

SEARCH

- IntelTechniques Facebook Tools
- Find my Facebook ID
- FB Email Search
- Recover FB Account
- Facebook Photos by ID (M)
- FB People Directory
- NetBootCamp FB Search Tool
- FB Lookup ID
- FB Identify (Requires Logout)
- Search is Back!
- Socialsearching
- Facebook Live Map

ANALYTICS

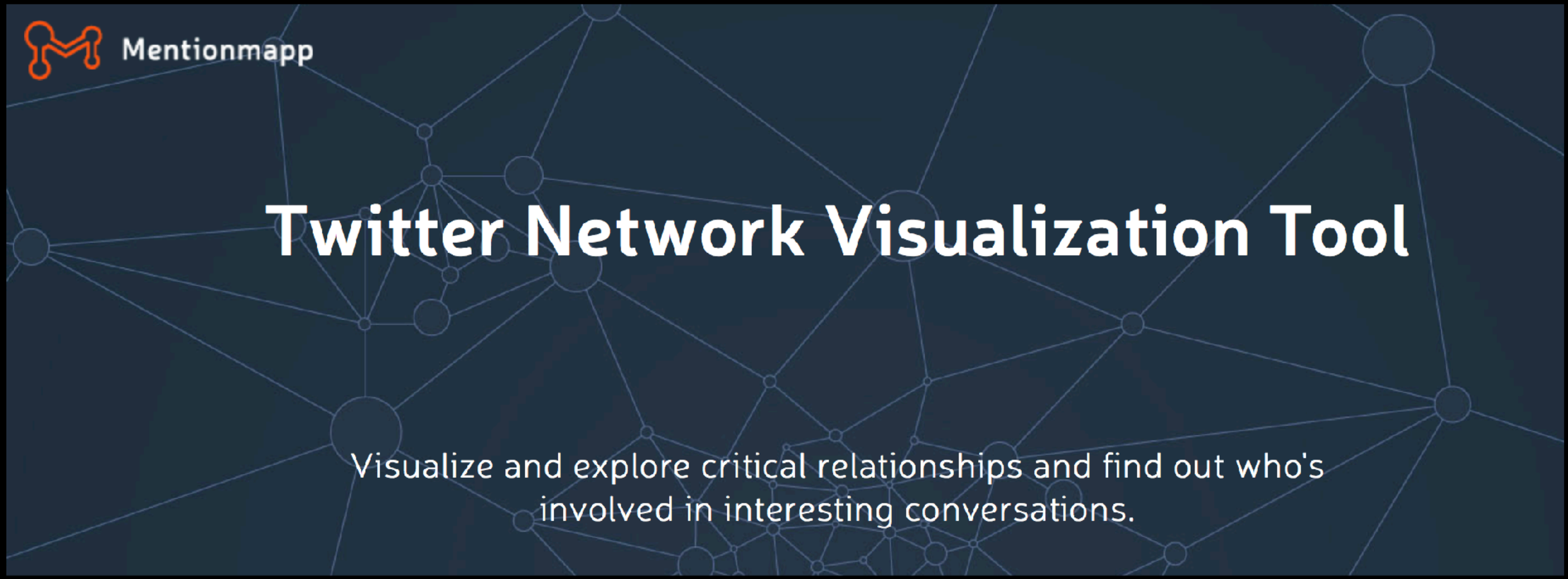
- fb-sleep-stats (T)
- Facebook Scanner

TELEFON NUMARALARI

- IntelTechniques Phone Tools
- Pipl API (M)
- WhoCalld
- 411
- CallerID Test
- ThatsThem - Reverse Phone Lookup
- Twilio Lookup
- Fone Finder
- True Caller
- Reverse Genie
- SpyDialer
- Phone Validator
- Free Carrier Lookup
- Mr. Number (M)

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

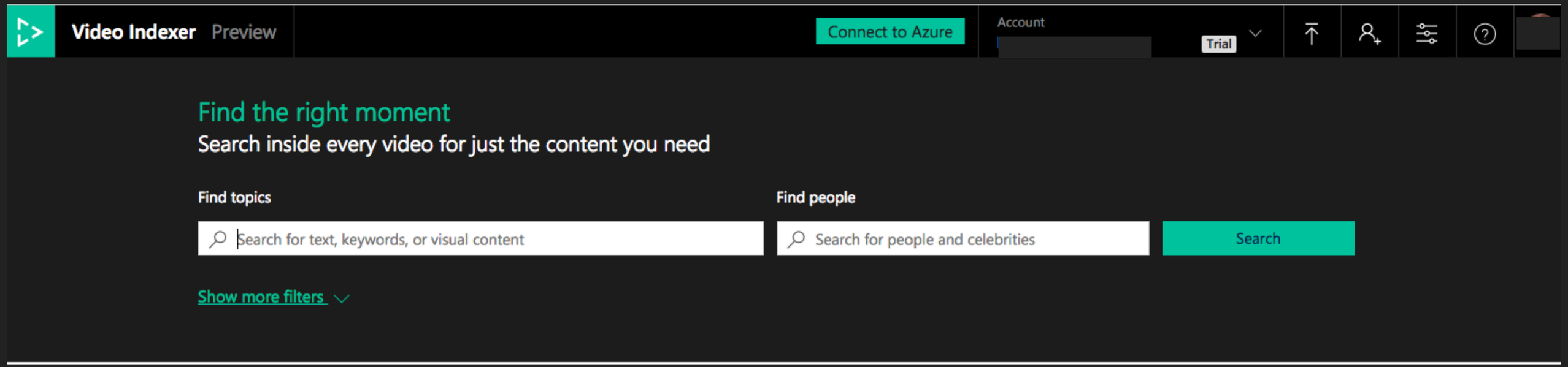

Mentionmapp
Twitter Network Visualization Tool
Visualize and explore critical relationships and find out who's involved in interesting conversations.

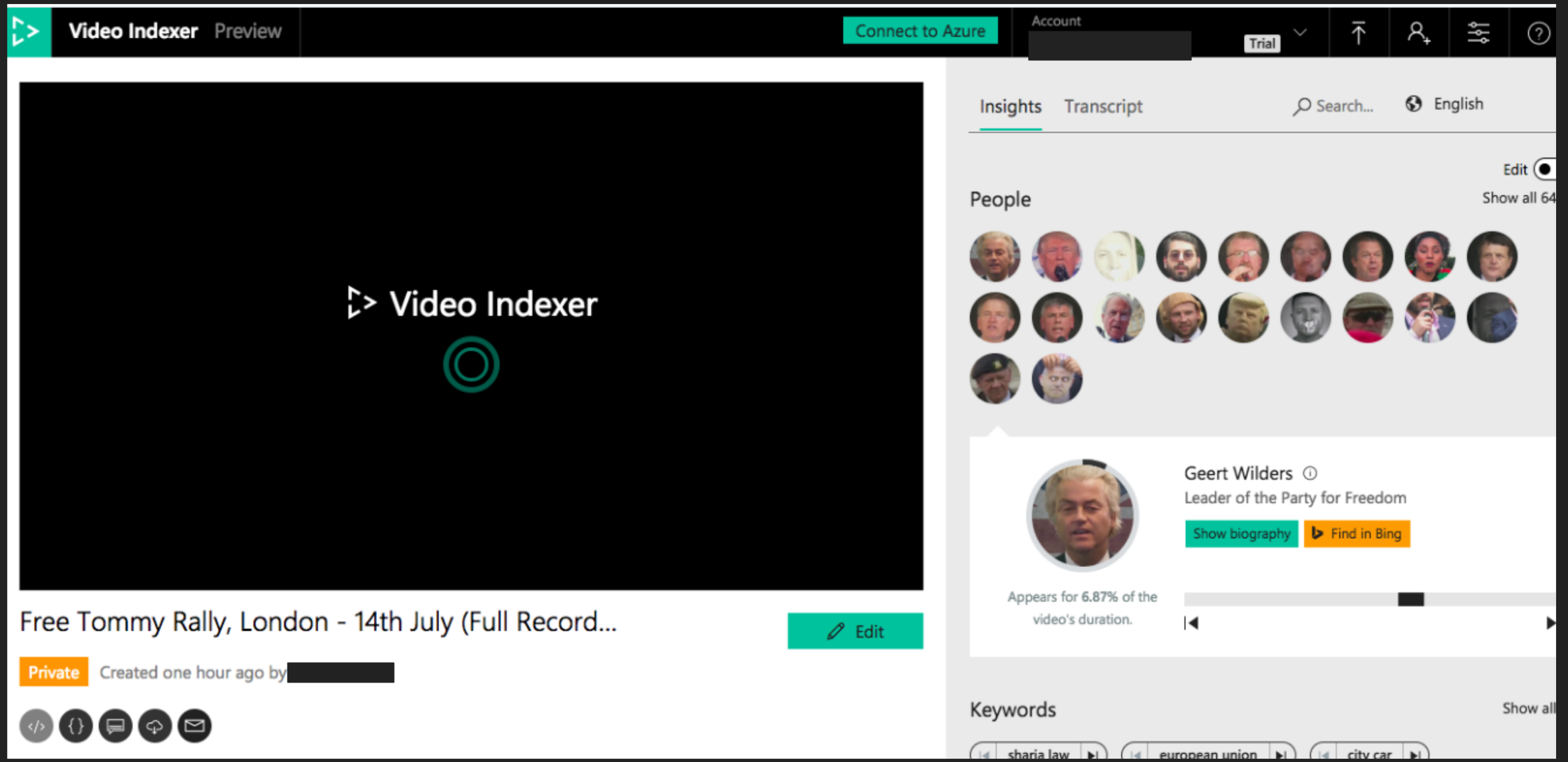

GOOGLE
HACKING-DATABASE


FEAR THE
FCA


SHODAN
Computer Search Engine


ExifTool
TOOL FOR READING, WRITING AND EDITING META INFORMATION IN FILES


Video Indexer Preview
Connect to Azure
Account
Trial
Find the right moment
Search inside every video for just the content you need
Find topics
Search for text, keywords, or visual content
Find people
Search for people and celebrities
Search
Show more filters


Video Indexer Preview
Connect to Azure
Account
Trial
Video Indexer
Free Tommy Rally, London - 14th July (Full Record...
Edit
Private
Created one hour ago by
Insights
Transcript
Search...
English
Edit
People
Show all 64
Geert Wilders
Leader of the Party for Freedom
Show biography
Find in Bing
Appears for 6.87% of the video's duration.
Keywords
Show all
sharia law
european union
city car

Video Indexer Preview

Connect to Azure

Account [redacted] Trial

Free Tommy Rally, London - 14th July (Full Record...

Edit

Private Created one hour ago by [redacted]

More videos with similar people and keywords

Insights Transcript Search... English

Keywords

Show less

- sharia law
- european union
- city car
- united kingdom
- prime minister
- citi card
- western civilization
- vicious snake
- bad guys
- united states
- boring word
- middle east
- election system
- true nature
- jesus christ
- justin smith
- convicted criminals
- joy villa
- mass immigration
- government betrayed
- darkest hour
- failed policies
- fighters gathered
- political class
- mainstream media
- real opposition
- donald trump
- british government
- previous rallies
- robin hood
- sweden democrats
- good guys
- good friend
- political establishment
- tommy robinson
- world cup
- lord pearson
- years ago
- big round
- western europe
- laws made
- back home
- free world
- hate speech
- london today

TWITTER -

First tweet

Social Bearing

One Million Tweet Map

All my tweets

Allegedly

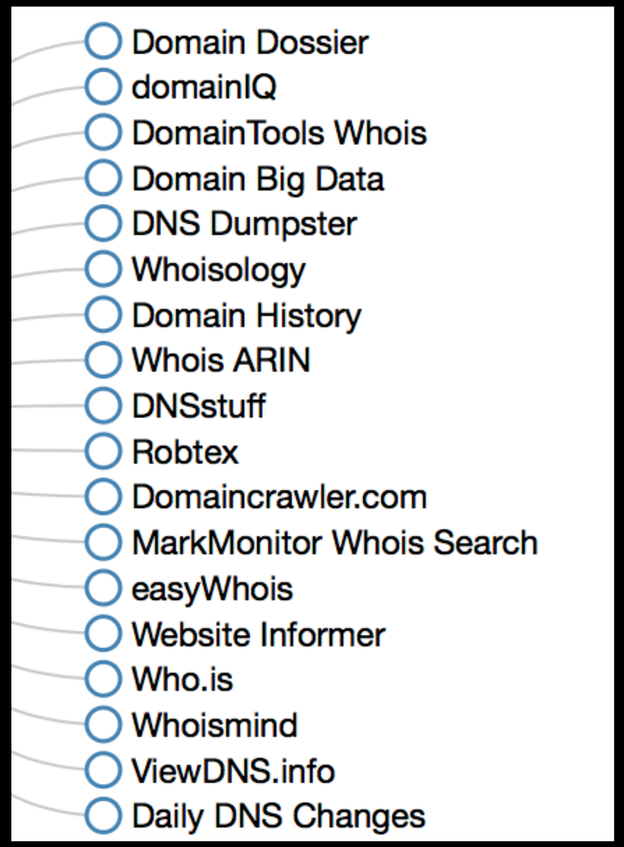
Sleeping time

Fake follower check

Tweetbeaver

DOMAIN MERKEZLİ ARAMA

WHOIS SORGUSU

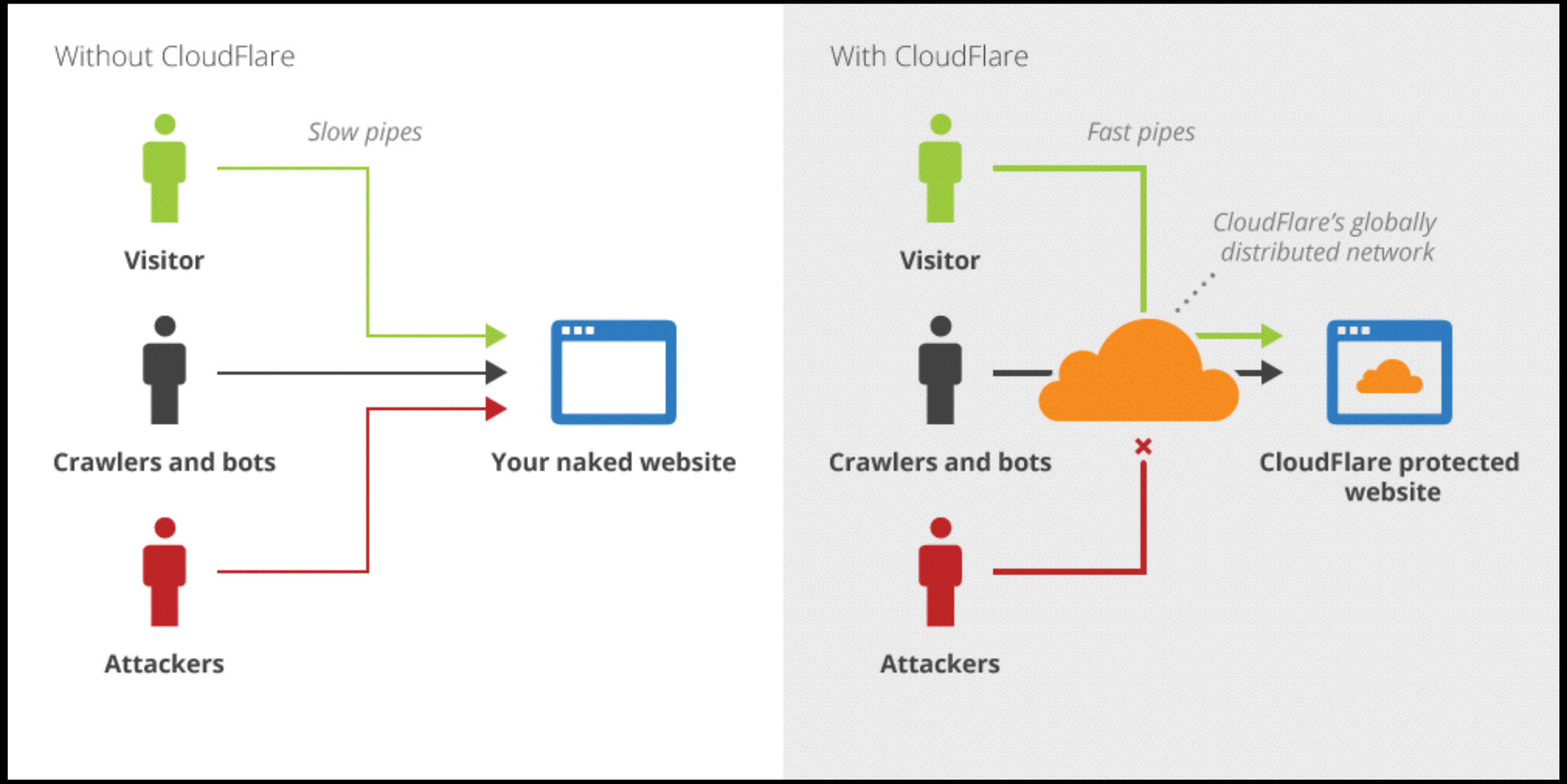


Whois sorgusu için alternatifler

```
halitince➜~» whois www.halitince.com
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object
```

who.is

CLOUDFLARE


Without CloudFlare
Slow pipes
Visitor
Crawlers and bots
Attackers
Your naked website
With CloudFlare
Fast pipes
CloudFlare's globally distributed network
Visitor
Crawlers and bots
Attackers
CloudFlare protected website

BİRKAÇ CLOUDFLARE BYPASS YÖNTEMİ

1- Nmap

nmap --script dns-brute -sn example.com

2- Dnsmap

dnsmap example.com

3- Netcraft ile eski kayıtlar

4- viewdns.info

5- Online cloudflare bypass yapan siteler

Cloud Resolve

6- Websploit cloudflare_resolver modülü

URLSCAN.IO

urlscan.io v0.3 | Home | Search | Map | API | Live | About | Login New! | 1 running | 0 queued

www.halitince.com 2400:cb00:2048:1::681c:92b

Lookup | Go To | Report | Rescan

Submitted URL: http://www.halitince.com
Effective URL: https://www.halitince.com/
Submission: On August 18 via manual (August 18th 2018, 2:46:38 pm)

Summary | HTTP 6 | Links 5 | Behaviour | IoCs | DOM | Content | Related | JSON | API

6	0	0	100%	100%	2	2	2	1	15kB	42kB	1
Requests	Ad-blocked	Malicious	HTTPS	IPv6	Domains	Subdomains	IPs	Countries	Transfer	Size	Cookies

This website contacted **2 IPs** in **1 countries** across **2 domains** to perform **6 HTTP transactions**. Of those, **6** were HTTPS (100 %) and 100% were IPv6.
The main IP is **2400:cb00:2048:1::681c:92b**, located in **United States** and belongs to CLOUDFLARENET - Cloudflare, Inc., US. The main domain is www.halitince.com. It took **0.523 seconds** to load this page.

IP/ASNs | IP Detail | (Sub)Domains | Domain Tree | Links | Certificates

	IP Address	AS Autonomous System
1 → 1	2400:cb00:2048:1::681c:82b	13335 (CLOUDFLARENET - Cloudflare)
3	2400:cb00:2048:1::681c:92b	13335 (CLOUDFLARENET - Cloudflare)
1 → 4	2400:cb00:2048:1::6819:3920	13335 (CLOUDFLARENET - Cloudflare)
6	2	

Screenshot (click to see full image) Expand Image

Detected technologies

CloudFlare (CDN) Website

DNS DUMPSTER

dns recon & research, find & lookup dns records

exampledomain.com

Search

DNSdumpster.com is a FREE domain research tool that can discover hosts related to a domain. Finding visible hosts from the attackers perspective is an important part of the security assessment process.

this is a HackerTarget.com project

PASSIVE DNS KAYITLARI

mnemonic

Search ...

www.ege.edu.tr

Record Type	Query	Answer	First seen	Last seen	# times	TTL
a	www.ege.edu.tr	155.223.64.111	2015-02-12 00:55	2018-07-23 11:09	804	86400
a	www.ege.edu.tr	155.223.64.15	2013-01-28 13:51	2015-02-09 23:45	187	81593
a	www.ege.edu.tr	155.223.64.14	2013-01-28 13:51	2015-02-09 23:45	182	82227
a	www.ege.edu.tr	155.223.64.13	2013-01-28 13:51	2015-02-09 23:45	187	81593

ANALİZ VE TEKNOLOJİ KEŞFİ

- BuiltWith
- SiteSleuth
- Wappalyzer (T)
- SEMrush
- Moonsearch
- StackShare
- Ewhois
- Netcraft
- StatsCrop
- Open Site Explorer
- SpyOnWeb
- SecurityHeaders.io
- Keyword Density
- Alexa Site Statistics
- Cisco Umbrella Popularity List
- Alexa Top 500 Global Sites
- W3bin.com
- Sitedossier
- Visual Site Mapper
- ClearWebStats.com
- PubDB
- WWW Domain Tools
- SimilarWeb
- Website Outlook
- Siteliner
- WebPagetest
- WhatWeb

URL EXPANDERS

- Link Expander
- GetLinkInfo
- CheckShortURL
- Lengthen Me
- URL Expander
- URL Unshortener
- Where Does This Link Go?
- KnowURL

getlinkinfo.com

REPUTATION

- UrlQuery.net
- PassiveTotal
- URL Void
- Threat Crowd
- FortiGuard Reputation Service
- McAfee TrustedSource
- Trend Micro Site Safety Center
- WatchGuard ReputationAuthority
- Sucuri SiteCheck
- ThreatMiner.org
- BlueCoat WebPulse
- Zscaler Zulu URL Risk Analyzer
- Joe Sandbox Url Analyzer
- Deepviz Domain Search
- Cisco SenderBase
- AVG Threat Labs
- Webroot BrightCloud URL/IP Lookup
- vURL Online
- AlienVault Open Threat Exchange
- Malware Domain List
- Web Inspector Online Scan
- Google Safe Browsing API
- hpHosts Online

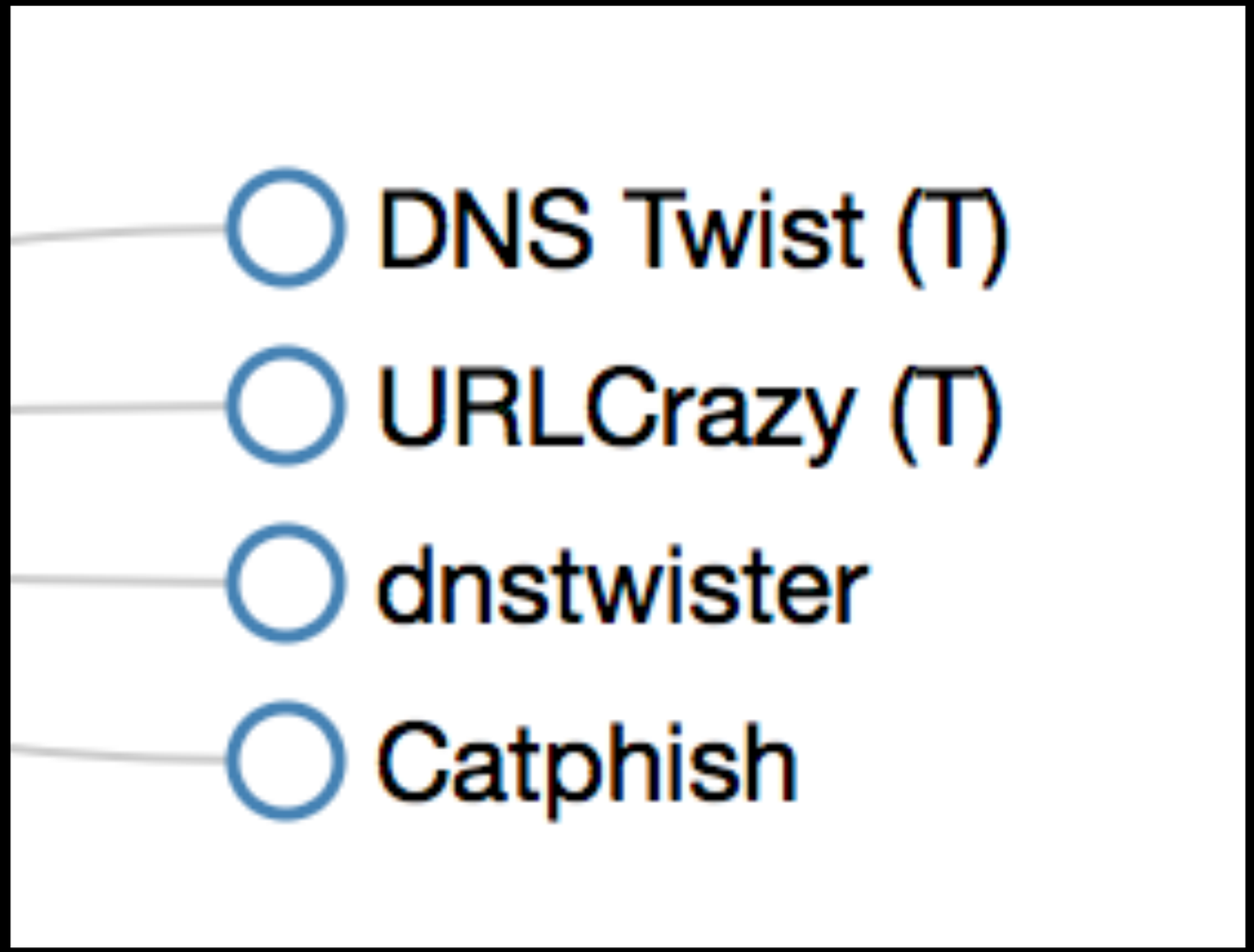
BLACKLIST KAYITLAR

- Ransomware Tracker Abuse.ch
- Threatexpert.com Malicious URLs
- Zeus C2 Tracker
- Malware Domains Blacklist
- Blackweb
- Critical Stack Intel (R)
- DNS Sinkhole
- DNS-BH Malware Domain Blocklist
- Malware Domain List
- Malware Patrol (R)
- MalwareURL (R)
- scumware.org
- ZeuS Tracker
- Shadowserver Foundation

Blackweb

malc0de

TYPOSQUATTING



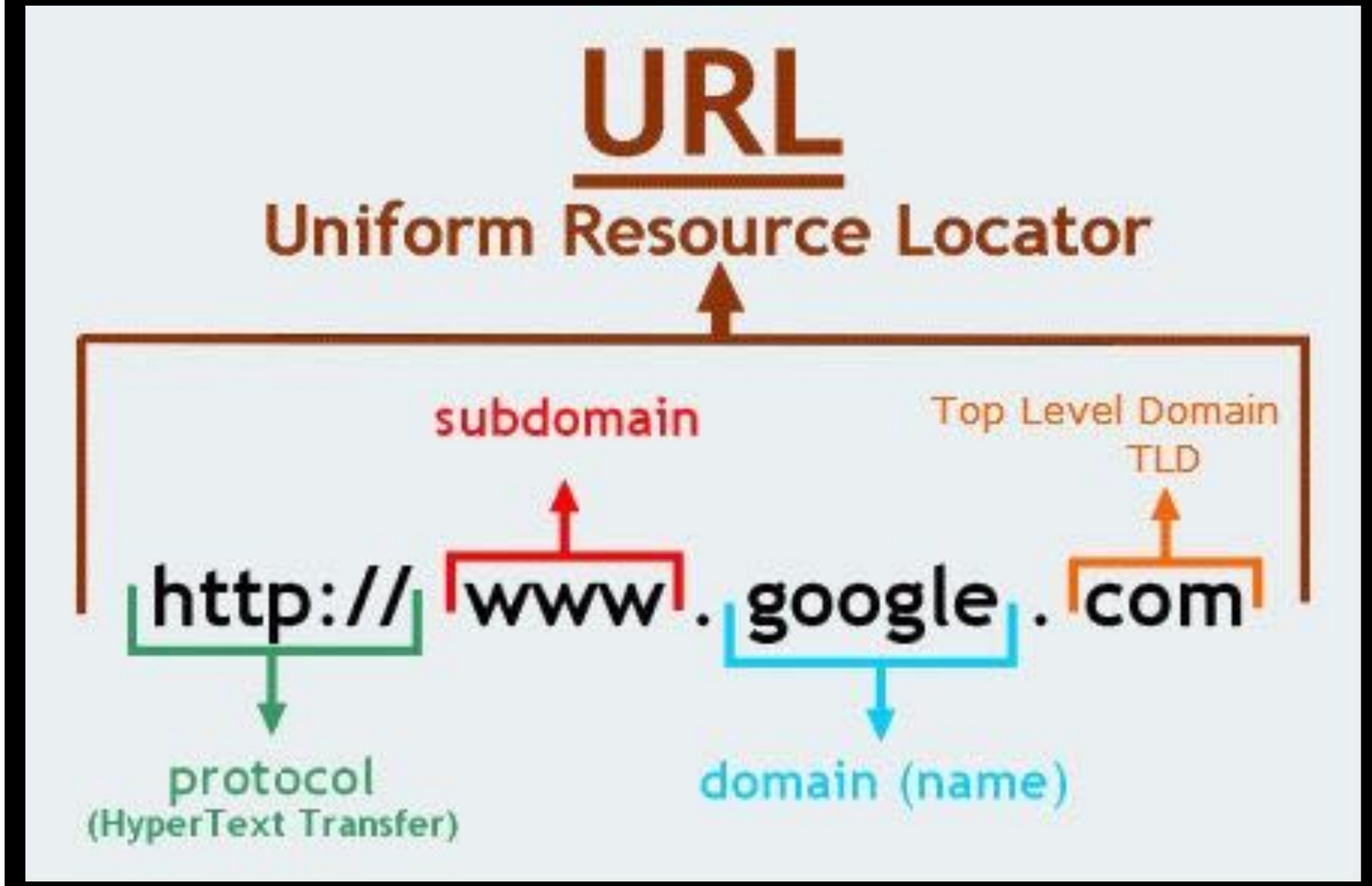
Dnstwister

CHANGE DETECTION

visualping

SUBDOMAIN ENUMERATION

- Aquatone (T)
- Google Subdomains (D)
- Recon-ng (T)
- XRay
- DNS Recon (T)
- Gobuster (T)
- Fierce Domain Scanner (T)
- Bluto (T)
- theHarvester (T)
- Pentest-tools.com Subdomains
- SecLists DNS Subdomains (T)
- dnspop (T)
- gdns (T)
- assetnote (T)
- Network Intelligence
- Sublist3r
- AltDNS (T)
- FindSubDomains



E-MAIL

hunter.io

```
root@kali:~# theharvester

**************************************************************************
*                                                                        *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __       *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__|      *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |         *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|         *
*                                                                        *
* TheHarvester Ver. 2.7                                                  *
* Coded by Christian Martorella                                          *
* Edge-Security Research                                                 *
* cmartorella@edge-security.com                                          *
**************************************************************************


Usage: theharvester options

       -d: Domain to search or company name
       -b: data source: google, googleCSE, exalead, bing, bingapi, pgp, linkedin,
                        google-profiles, jigsaw, twitter, googleplus, all

       -s: Start in result number X (default: 0)
       -v: Verify host name via dns resolution and search for virtual hosts
       -f: Save the results into an HTML and XML file (both)
       -n: Perform a DNS reverse query on all ranges discovered
       -c: Perform a DNS brute force for the domain name
       -t: Perform a DNS TLD expansion discovery
       -e: Use this DNS server
       -l: Limit the number of results to work with(bing goes from 50 to 50 results,
            google 100 to 100, and pgp doesn't use this option)
       -h: use SHODAN database to query discovered hosts

Examples:
        theharvester -d microsoft.com -l 500 -b google -f myresults.html
        theharvester -d microsoft.com -b pgp
        theharvester -d microsoft -l 200 -b linkedin
        theharvester -d apple.com -b googleCSE -l 500 -s 300
```


WayBackMachine

IP MERKEZLİ ARAMA

GEOLOCATION

- MaxMind Demo
- IPv4/IPv6 lists by country code
- IP2Location.com
- IP Fingerprints
- DB-IP
- ipintel.io
- IP Location Finder
- Info Sniper
- utrace
- InfobyIP.com
- ipTRACKERonline

ipintel.io

ipfingerprints

TEŞEKKÜRLER