Jawahar Education Societys Annasaheb Chudaman Patil College of Engineering, Kharghar, Navi Mumbai

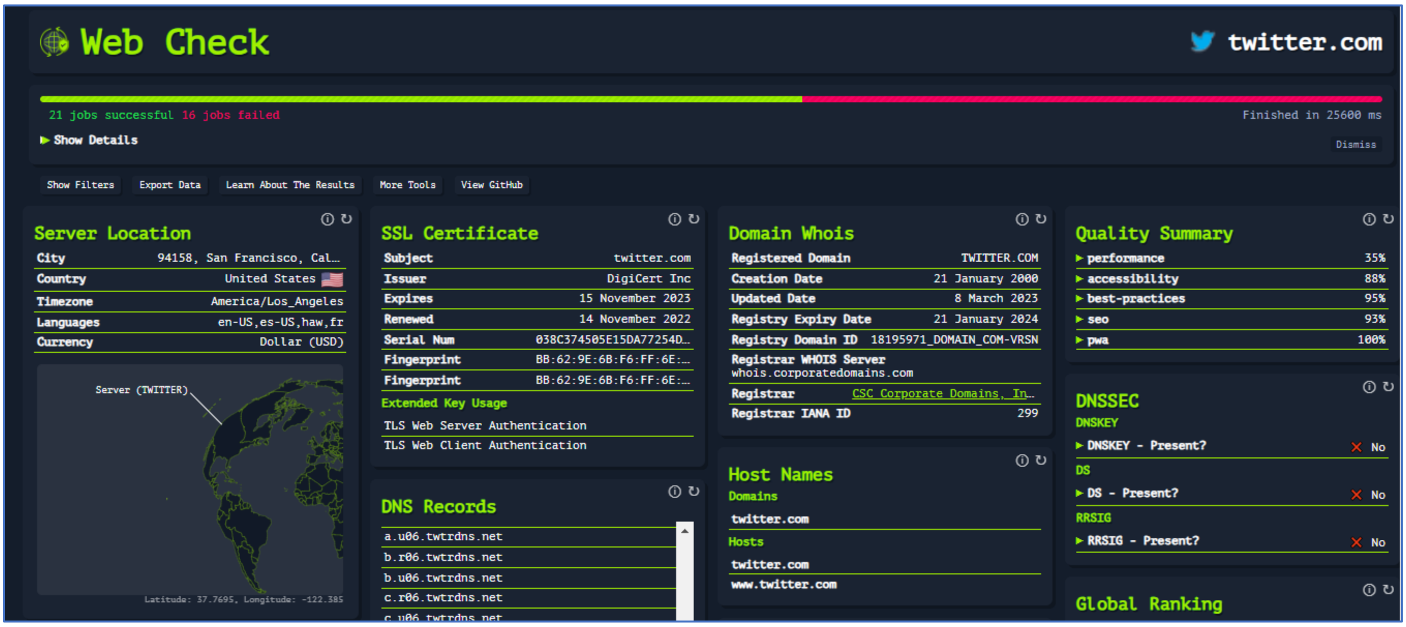
EXPERMINT: 05

● **Aim:** Using OSINT tools gather Tactical information using WHOIS lookup tools or websites like DomainTools (domain, registration details, owner's contact information, registration date, and expiration date.) Archives, Text, Reverse Image Search, Images and EXIF data, Source code, Others TLD, Mentions of target, Check info such as via RSS,SSL certificates, Robots/Sitemap, Port scans, Reverse IP lookup

● Theory:

Analyzing Network Traffic and Data Flow: Network analysis involves studying data traffic patterns to understand connections and behavior:

- **Traffic Analysis**: Monitoring and analyzing network traffic to identify communication patterns and anomalies.
- **Packet Inspection**: Examining individual data packets to gather insights into the type of information being transmitted.
- **Flow Data**: Collecting flow data (e.g., NetFlow) for understanding communication between devices.
- **DNS Lookups** and **WHOIS Queries**: DNS and WHOIS queries reveal information about domains and IP addresses:
- **DNS Analysis**: Investigating domain names and IP addresses to uncover relationships, affiliations, and potential threats.
- **WHOIS Queries**: Querying WHOIS databases to identify domain registrants and contact information.
- **Tracing Network Paths and Hops**: Tracing network paths helps understand data routing and potential bottlenecks:
- **Traceroute**: Tracing the path that data packets take across networks, revealing intermediate devices (hops) and latency.
- **Geolocation of IPs**: Mapping IP addresses to geographical locations aids in understanding network topology.
- **Identifying Online Infrastructure Patterns**: Analyzing online infrastructure patterns involves recognizing common components and their interconnections:
- **Domain Infrastructure**: Identifying domains, subdomains, and their relationships can reveal malicious or suspicious activities.
- **CDN and Cloud Services:** Recognizing the use of content delivery networks and cloud services helps understand a target’s online presence.



21 jobs successful 16 jobs failed

Finished in 25600 ms

Server Location

City	94158, San Francisco, Cal…
Country	United States
Timezone	America/Los_Angeles
Languages	en-US,es-US,haw,fr
Currency	Dollar (USD)

Latitude: 37.7695, Longitude: -122.385

SSL Certificate

Subject	twitter.com
Issuer	DigiCert Inc
Expires	15 November 2023
Renewed	14 November 2022
Serial Num	038C374505E15DA77254D…
Fingerprint	BB:62:9E:6B:F6:FF:6E:…
Fingerprint	BB:62:9E:6B:F6:FF:6E:…

Extended Key Usage

TLS Web Server Authentication

TLS Web Client Authentication

DNS Records

a.u06.twtrdns.net
b.r06.twtrdns.net
b.u06.twtrdns.net
c.r06.twtrdns.net
c.u06.twtrdns.net

Domain Whois

Registered Domain	TWITTER.COM
Creation Date	21 January 2000
Updated Date	8 March 2023
Registry Expiry Date	21 January 2024
Registry Domain ID	18195971_DOMAIN_COM-VRSN
Registrar WHOIS Server whois.corporatedomains.com	
Registrar	CSC Corporate Domains, In…
Registrar IANA ID	299

Host Names

Domains

twitter.com

Hosts

twitter.com
www.twitter.com

Quality Summary

▶ performance	35%
▶ accessibility	88%
▶ best-practices	95%
▶ seo	93%
▶ pwa	100%

DNSSEC

DNSKEY

▶ DNSKEY - Present?	✗ No

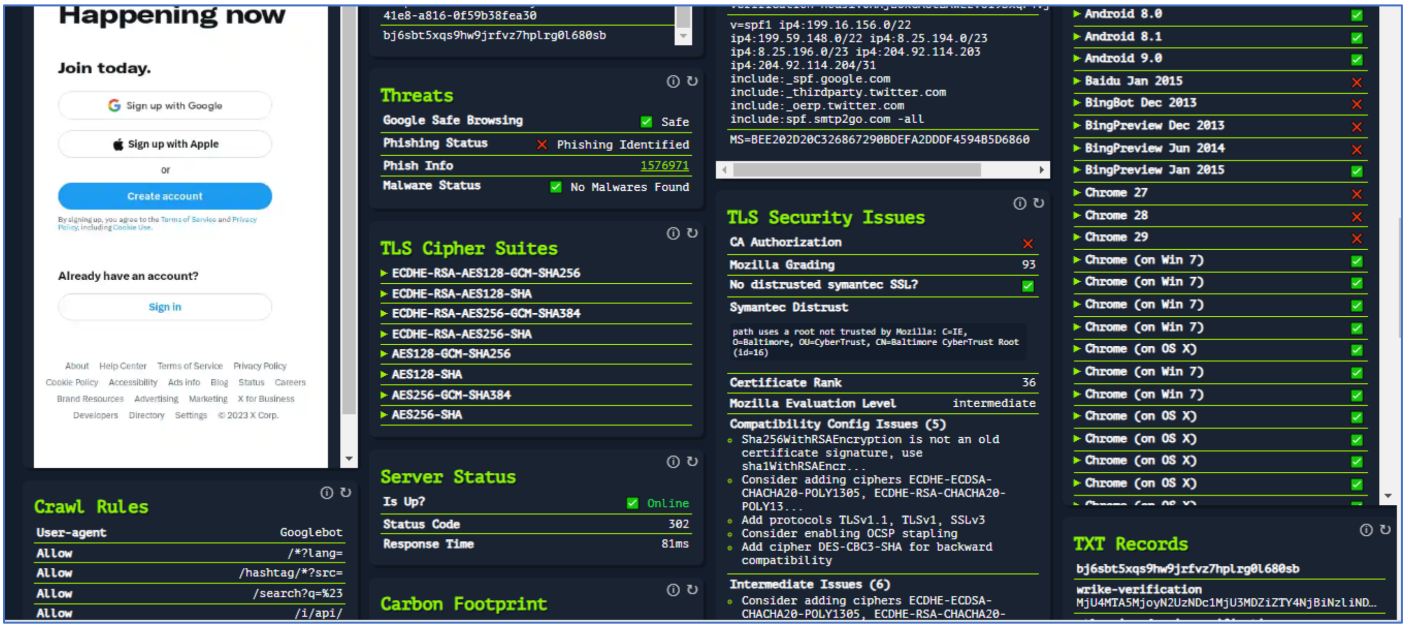
DS

▶ DS - Present?	✗ No

RRSIG

▶ RRSIG - Present?	✗ No

Global Ranking



Happening now

Join today.

Sign up with Google

Sign up with Apple

or

Create account

By signing up, you agree to the Terms of Service and Privacy Policy, including Cookie Use.

Already have an account?

Sign in

About Help Center Terms of Service Privacy Policy Cookie Policy Accessibility Ads info Blog Status Careers Brand Resources Advertising Marketing X for Business Developers Directory Settings © 2023 X Corp.

Crawl Rules

User-agent	Googlebot
Allow	/*?lang=
Allow	/hashtag/*?src=
Allow	/search?q=%23
Allow	/i/api/

```
41e8-a816-0f59b38fea30
bj6sbt5xqs9hw9jrfvz7hplrg0l680sb
```

Threats

Google Safe Browsing	✓ Safe
Phishing Status	✗ Phishing Identified
Phish Info	1576971
Malware Status	✓ No Malwares Found

TLS Cipher Suites

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA
- AES128-GCM-SHA256
- AES128-SHA
- AES256-GCM-SHA384
- AES256-SHA

Server Status

Is Up?	✓ Online
Status Code	302
Response Time	81ms

Carbon Footprint

```
v=spf1 ip4:199.16.156.0/22
ip4:199.59.148.0/22 ip4:8.25.194.0/23
ip4:8.25.196.0/23 ip4:204.92.114.203
ip4:204.92.114.204/31
include:_spf.google.com
include:_thirdparty.twitter.com
include:_oerp.twitter.com
include:spf.smtp2go.com -all
MS=BEE202D20C326867290BDEFA2DDDF4594B5D6860
```

TLS Security Issues

CA Authorization	✗
Mozilla Grading	93
No distrusted symantec SSL?	✓
Symantec Distrust	

```
path uses a root not trusted by Mozilla: C=IE,
O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
(id=16)
```

Certificate Rank	36
Mozilla Evaluation Level	intermediate

Compatibility Config Issues (5)

- Sha256WithRSAEncryption is not an old certificate signature, use sha1WithRSAEncr...
- Consider adding ciphers ECDHE-ECDSA-CHACHA20-POLY1305, ECDHE-RSA-CHACHA20-POLY13...
- Add protocols TLSv1.1, TLSv1, SSLv3
- Consider enabling OCSP stapling
- Add cipher DES-CBC3-SHA for backward compatibility

Intermediate Issues (6)

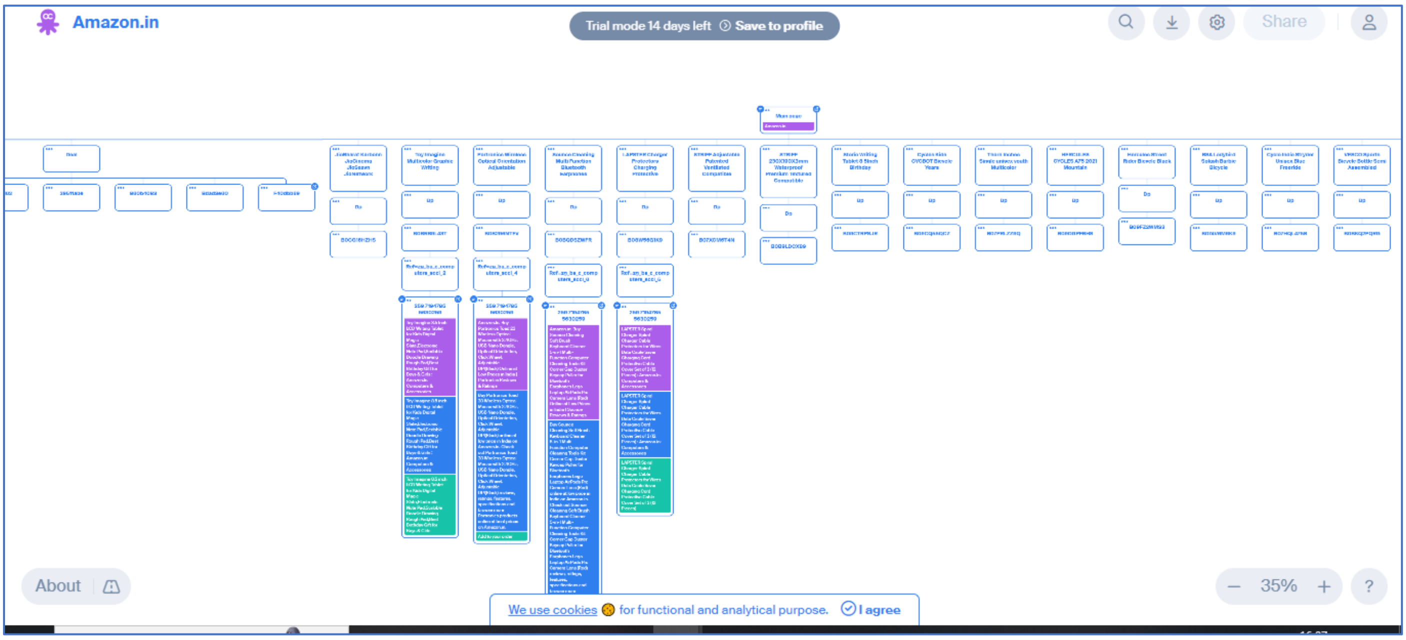
- Consider adding ciphers ECDHE-ECDSA-CHACHA20-POLY1305, ECDHE-RSA-CHACHA20-

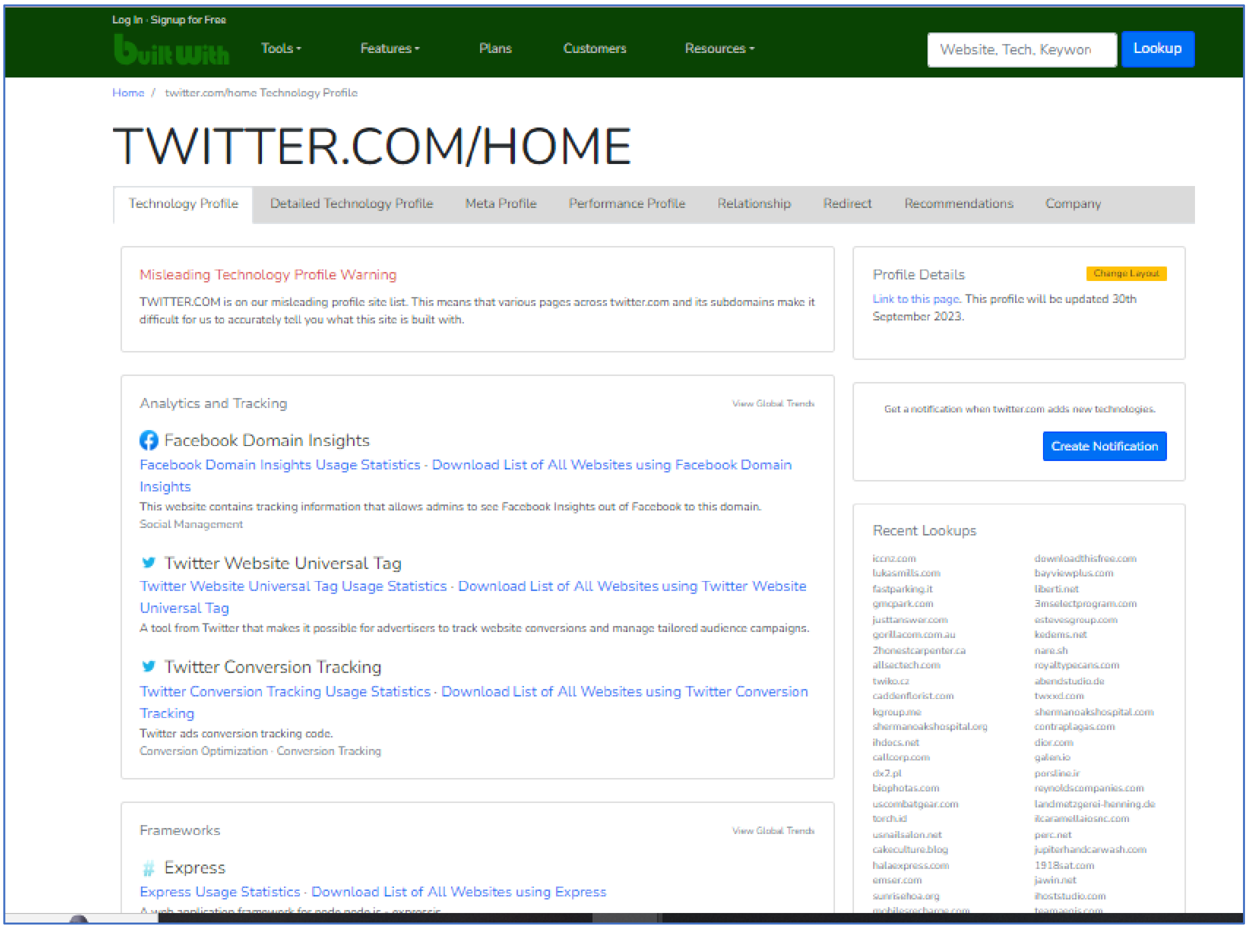
Android 8.0	✓
Android 8.1	✓
Android 9.0	✓
Baidu Jan 2015	✗
BingBot Dec 2013	✗
BingPreview Dec 2013	✗
BingPreview Jun 2014	✗
BingPreview Jan 2015	✓
Chrome 27	✗
Chrome 28	✗
Chrome 29	✗
Chrome (on Win 7)	✓
Chrome (on Win 7)	✓
Chrome (on Win 7)	✓
Chrome (on Win 7)	✓
Chrome (on OS X)	✓
Chrome (on Win 7)	✓
Chrome (on Win 7)	✓
Chrome (on OS X)	✓
Chrome (on OS X)	✓
Chrome (on OS X)	✓
Chrome (on OS X)	✓

TXT Records

```
bj6sbt5xqs9hw9jrfvz7hplrg0l680sb
wrike-verification
MjU4MTA5MjoyN2UzNDc1MjU3MDZiZTY4NjBiNzliND…
```

Sitemap





Home / twitter.com/home Technology Profile

TWITTER.COM/HOME

Technology Profile | Detailed Technology Profile | Meta Profile | Performance Profile | Relationship | Redirect | Recommendations | Company

Misleading Technology Profile Warning

TWITTER.COM is on our misleading profile site list. This means that various pages across twitter.com and its subdomains make it difficult for us to accurately tell you what this site is built with.

Profile Details

Change Layout

Link to this page. This profile will be updated 30th September 2023.

Analytics and Tracking

View Global Trends

Facebook Domain Insights

Facebook Domain Insights Usage Statistics · Download List of All Websites using Facebook Domain Insights

This website contains tracking information that allows admins to see Facebook Insights out of Facebook to this domain.

Social Management

Twitter Website Universal Tag

Twitter Website Universal Tag Usage Statistics · Download List of All Websites using Twitter Website Universal Tag

A tool from Twitter that makes it possible for advertisers to track website conversions and manage tailored audience campaigns.

Twitter Conversion Tracking

Twitter Conversion Tracking Usage Statistics · Download List of All Websites using Twitter Conversion Tracking

Twitter ads conversion tracking code.

Conversion Optimization · Conversion Tracking

Get a notification when twitter.com adds new technologies.

Create Notification

Recent Lookups

iccnz.com
lukasmills.com
fastparking.it
gmcpark.com
justtanswer.com
gorillacom.com.au
2honestcarpenter.ca
allsectech.com
twiko.cz
caddenflorist.com
kgroup.me
shermanoakshospital.org
ihdocs.net
callcorp.com
dx2.pl
biophotas.com
uscombatgear.com
torch.id
usnailsalon.net
cakeculture.blog
halaexpress.com
emser.com
sunrisehoa.org
mobilesrecharge.com

downloadthisfree.com
bayviewplus.com
liberti.net
3mselectprogram.com
estevesgroup.com
kedems.net
nare.sh
royaltypecans.com
abendstudio.de
twxxd.com
shermanoakshospital.com
contraplagas.com
dior.com
galen.io
porsline.ir
reynoldscompanies.com
landmetzgerei-henning.de
ilcaramellaiosnc.com
perc.net
jupiterhandcarwash.com
1918sat.com
jawin.net
ihoststudio.com
teamaenis.com

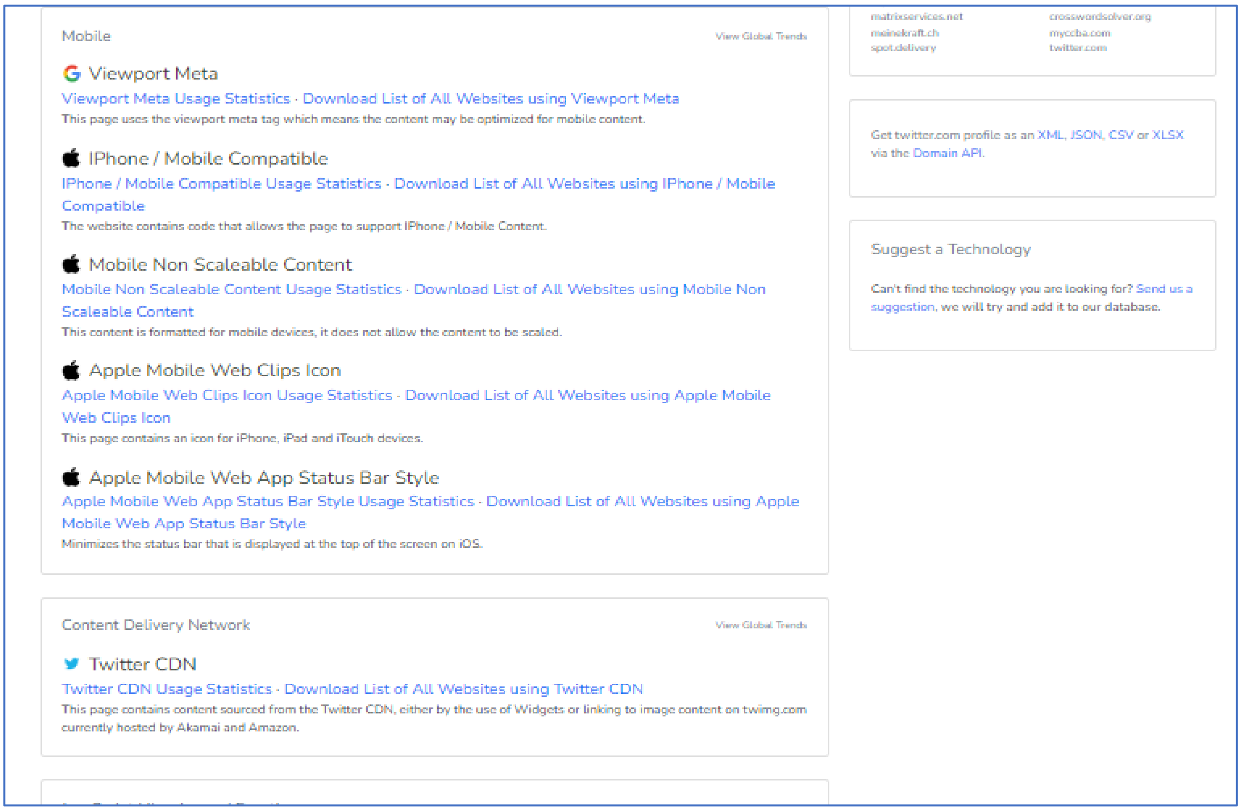
Frameworks

View Global Trends

Express

Express Usage Statistics · Download List of All Websites using Express

A web application framework for node node.js - expressjs



Mobile

View Global Trends

Viewport Meta

Viewport Meta Usage Statistics · Download List of All Websites using Viewport Meta

This page uses the viewport meta tag which means the content may be optimized for mobile content.

IPhone / Mobile Compatible

IPhone / Mobile Compatible Usage Statistics · Download List of All Websites using IPhone / Mobile Compatible

The website contains code that allows the page to support IPhone / Mobile Content.

Mobile Non Scaleable Content

Mobile Non Scaleable Content Usage Statistics · Download List of All Websites using Mobile Non Scaleable Content

This content is formatted for mobile devices, it does not allow the content to be scaled.

Apple Mobile Web Clips Icon

Apple Mobile Web Clips Icon Usage Statistics · Download List of All Websites using Apple Mobile Web Clips Icon

This page contains an icon for iPhone, iPad and iTouch devices.

Apple Mobile Web App Status Bar Style

Apple Mobile Web App Status Bar Style Usage Statistics · Download List of All Websites using Apple Mobile Web App Status Bar Style

Minimizes the status bar that is displayed at the top of the screen on iOS.

Content Delivery Network

View Global Trends

Twitter CDN

Twitter CDN Usage Statistics · Download List of All Websites using Twitter CDN

This page contains content sourced from the Twitter CDN, either by the use of Widgets or linking to image content on twimg.com currently hosted by Akamai and Amazon.

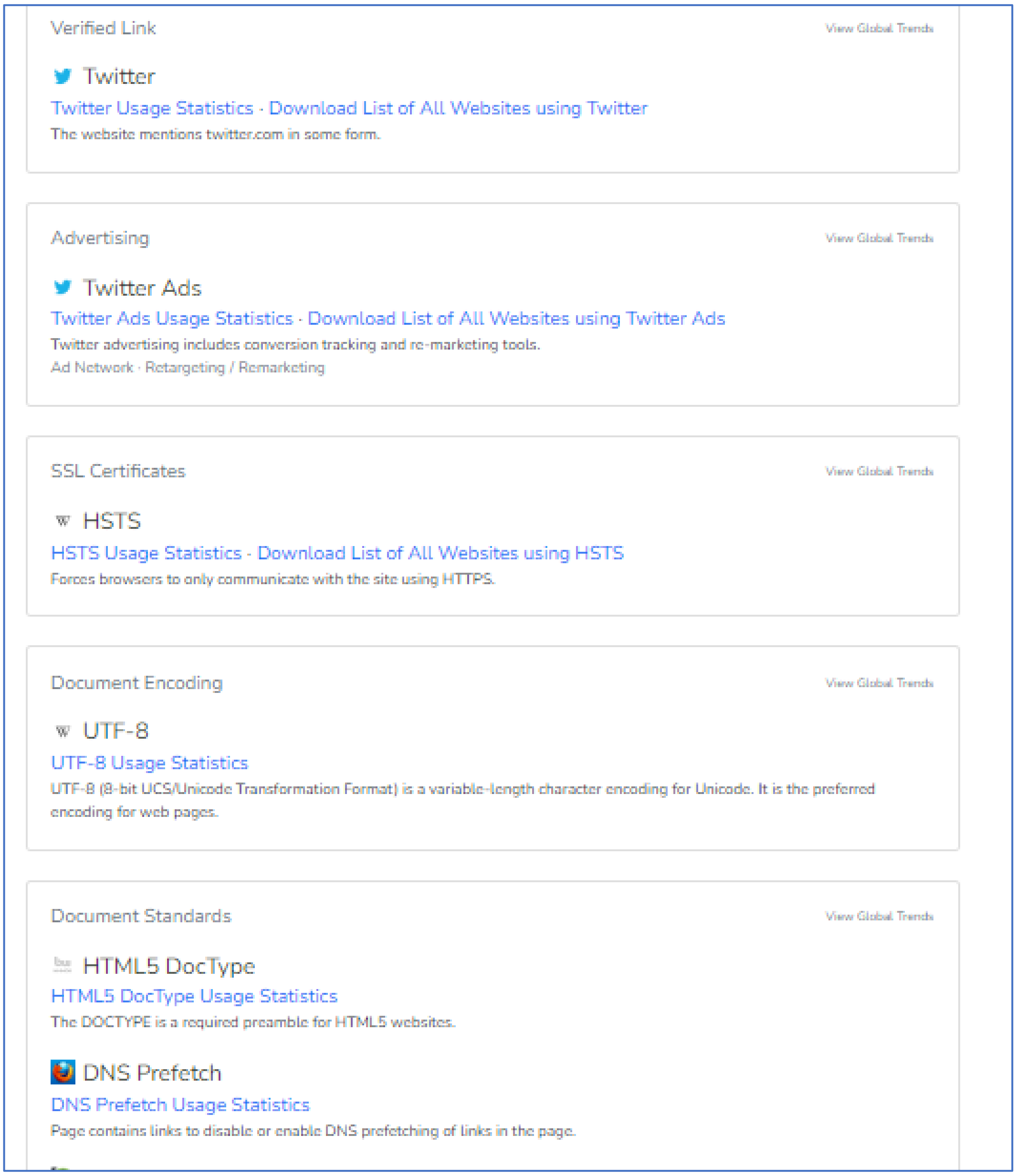
matrixservices.net
meinekraft.ch
spot.delivery

crosswordsolver.org
myccba.com
twitter.com

Get twitter.com profile as an XML, JSON, CSV or XLSX via the Domain API.

Suggest a Technology

Can't find the technology you are looking for? Send us a suggestion, we will try and add it to our database.



Verified Link

View Global Trends

Twitter

Twitter Usage Statistics · Download List of All Websites using Twitter

The website mentions twitter.com in some form.

Advertising

View Global Trends

Twitter Ads

Twitter Ads Usage Statistics · Download List of All Websites using Twitter Ads

Twitter advertising includes conversion tracking and re-marketing tools.

Ad Network · Retargeting / Remarketing

SSL Certificates

View Global Trends

HSTS

HSTS Usage Statistics · Download List of All Websites using HSTS

Forces browsers to only communicate with the site using HTTPS.

Document Encoding

View Global Trends

UTF-8

UTF-8 Usage Statistics

UTF-8 (8-bit UCS/Unicode Transformation Format) is a variable-length character encoding for Unicode. It is the preferred encoding for web pages.

Document Standards

View Global Trends

HTML5 DocType

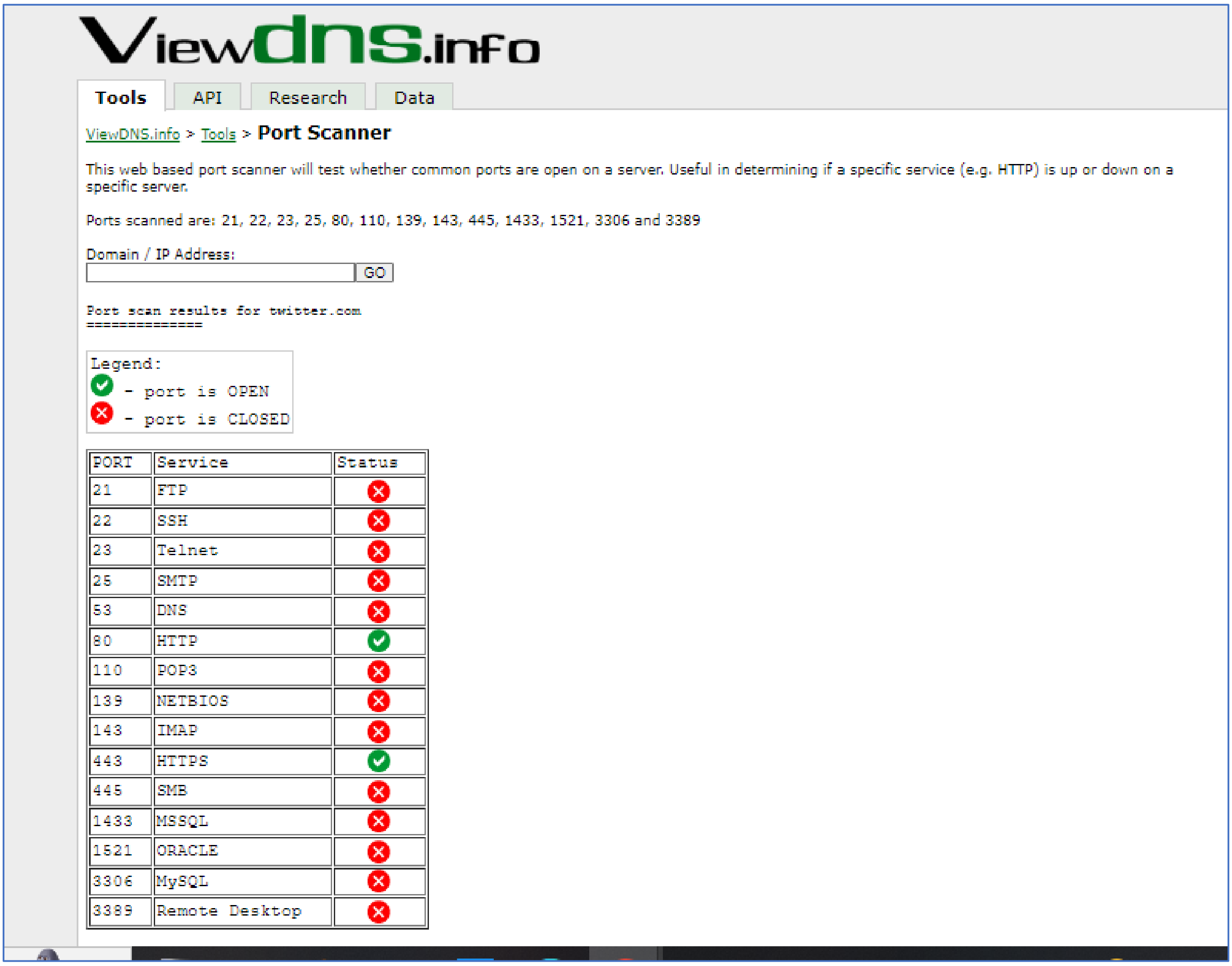
HTML5 DocType Usage Statistics

The DOCTYPE is a required preamble for HTML5 websites.

DNS Prefetch

DNS Prefetch Usage Statistics

Page contains links to disable or enable DNS prefetching of links in the page.



ViewDNS.info > Tools > **Port Scanner**

This web based port scanner will test whether common ports are open on a server. Useful in determining if a specific service (e.g. HTTP) is up or down on a specific server.

Ports scanned are: 21, 22, 23, 25, 80, 110, 139, 143, 445, 1433, 1521, 3306 and 3389

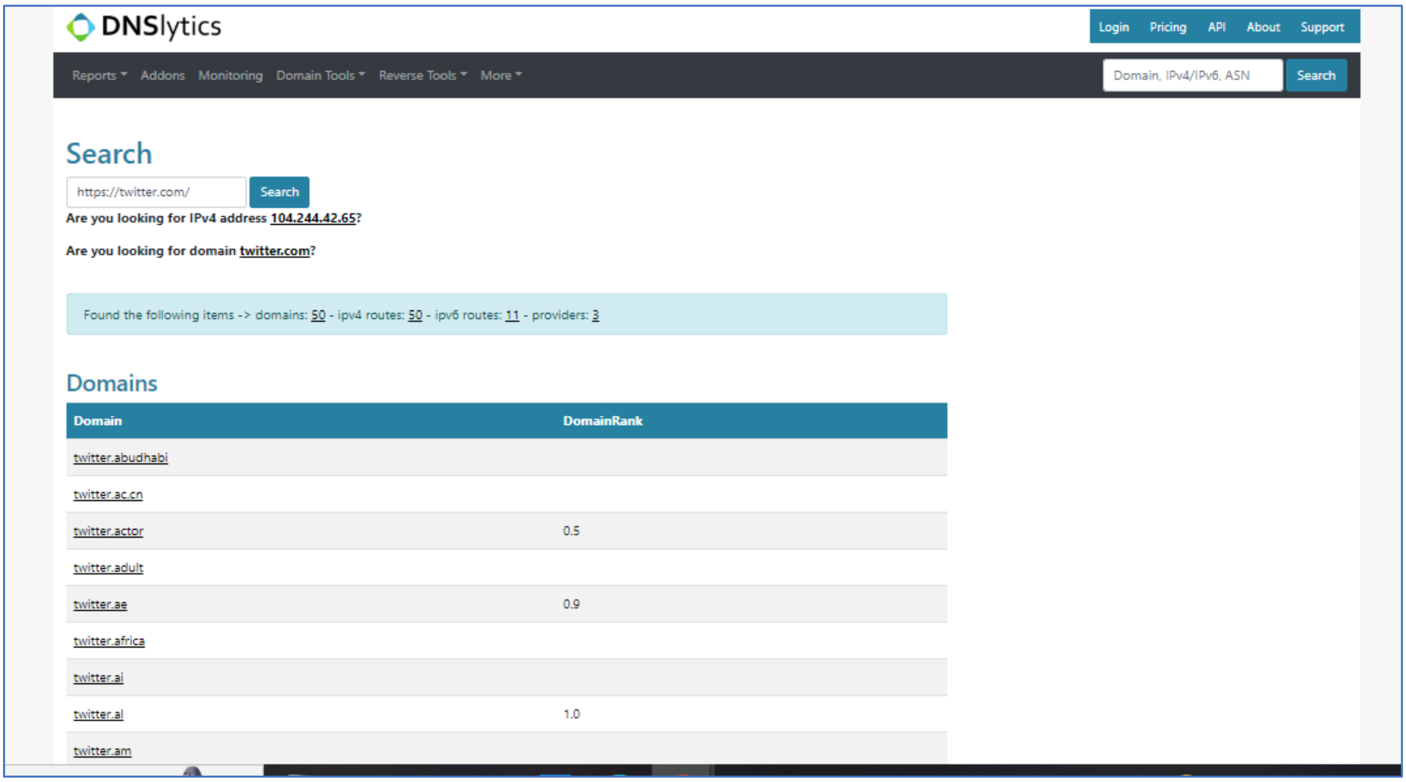
Domain / IP Address:

GO

```
Port scan results for twitter.com
==============
```

Legend:
✓ - port is OPEN
✗ - port is CLOSED

PORT	Service	Status
21	FTP	✗
22	SSH	✗
23	Telnet	✗
25	SMTP	✗
53	DNS	✗
80	HTTP	✓
110	POP3	✗
139	NETBIOS	✗
143	IMAP	✗
443	HTTPS	✓
445	SMB	✗
1433	MSSQL	✗
1521	ORACLE	✗
3306	MySQL	✗
3389	Remote Desktop	✗



Search

https://twitter.com/ Search

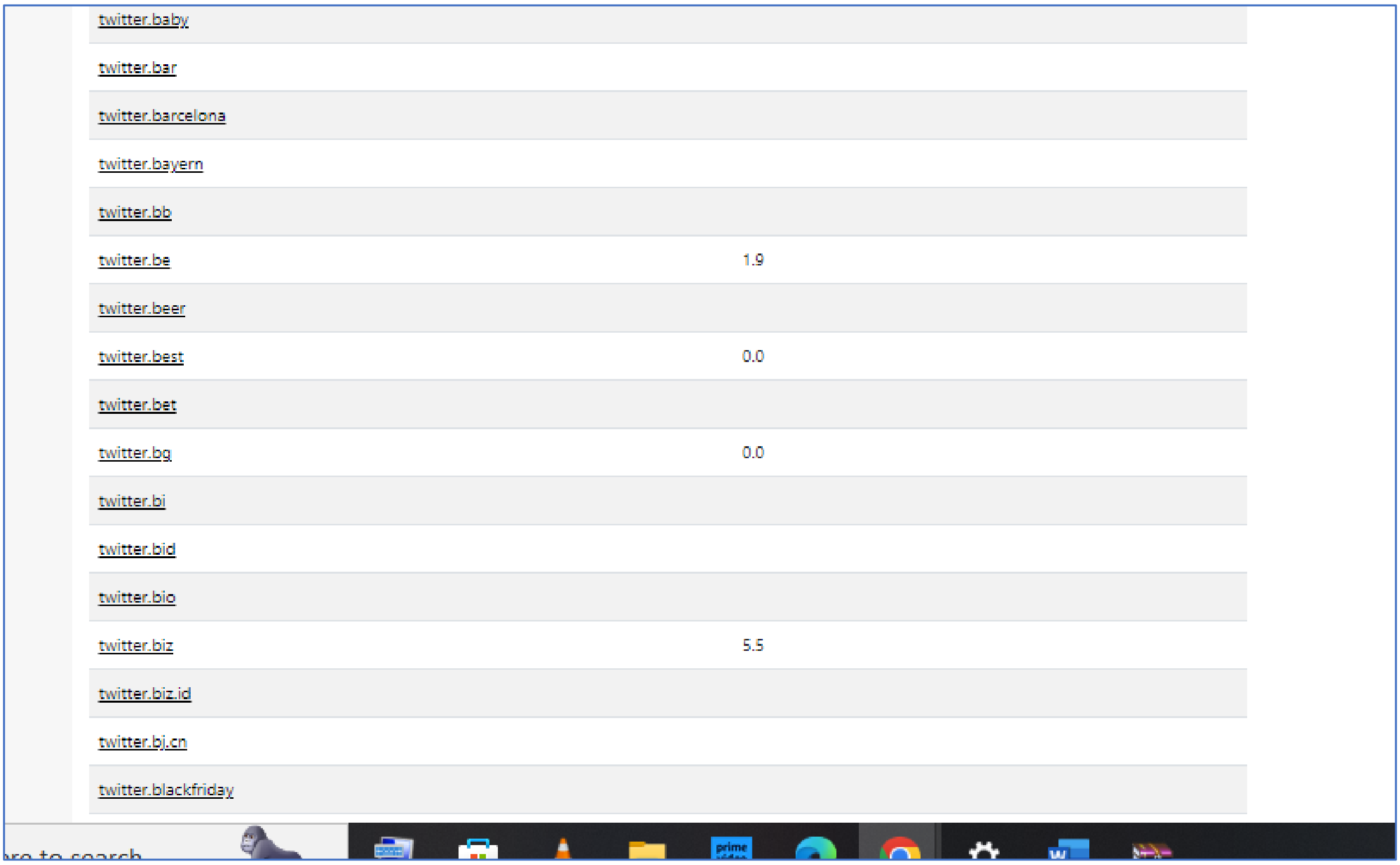
Are you looking for IPv4 address 104.244.42.65?

Are you looking for domain twitter.com?

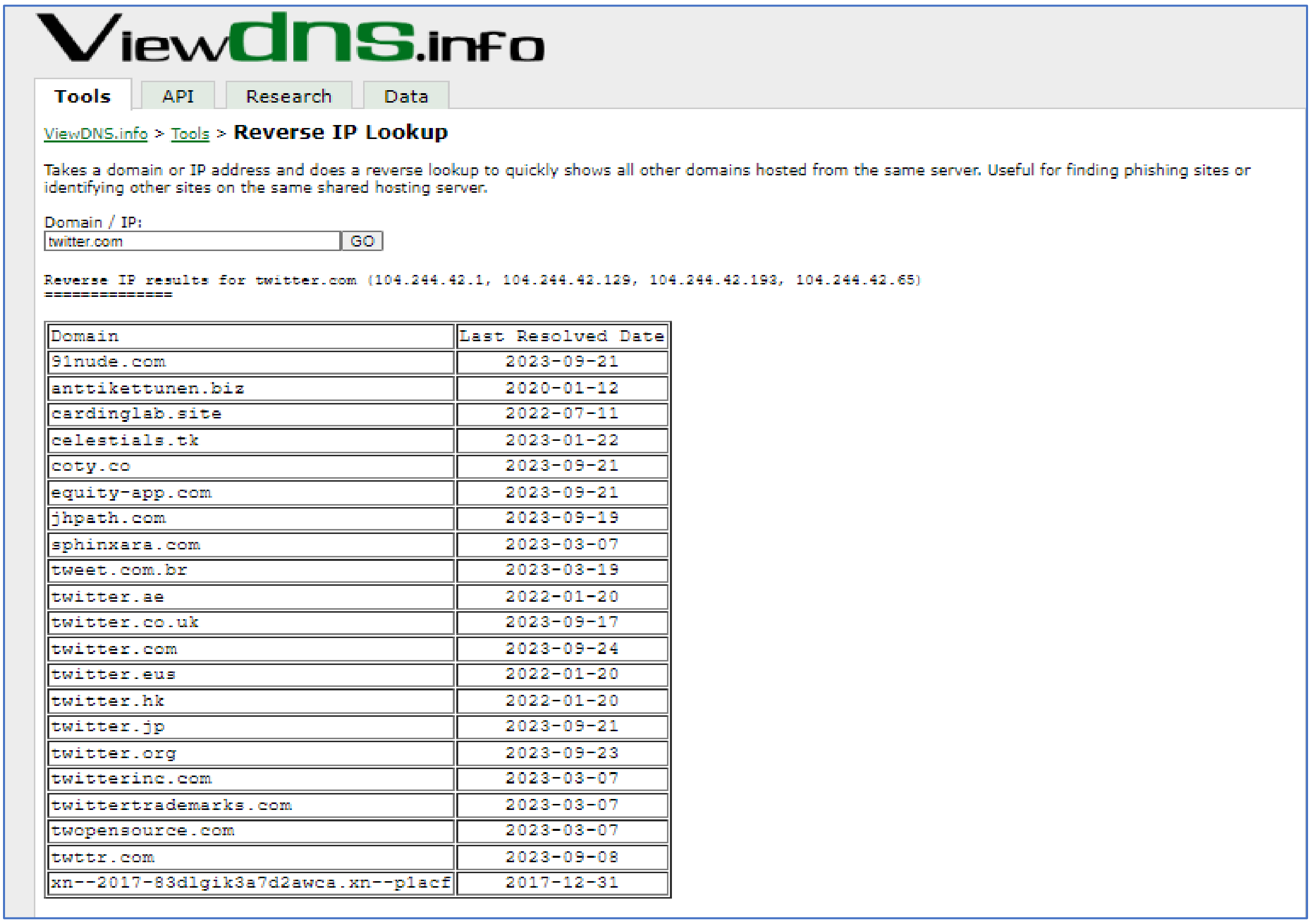
Found the following items -> domains: 50 - ipv4 routes: 50 - ipv6 routes: 11 - providers: 3

Domains

Domain	DomainRank
twitter.abudhabi	
twitter.ac.cn	
twitter.actor	0.5
twitter.adult	
twitter.ae	0.9
twitter.africa	
twitter.ai	
twitter.al	1.0
twitter.am	



twitter.baby	
twitter.bar	
twitter.barcelona	
twitter.bayern	
twitter.bb	
twitter.be	1.9
twitter.beer	
twitter.best	0.0
twitter.bet	
twitter.bg	0.0
twitter.bi	
twitter.bid	
twitter.bio	
twitter.biz	5.5
twitter.biz.id	
twitter.bj.cn	
twitter.blackfriday	



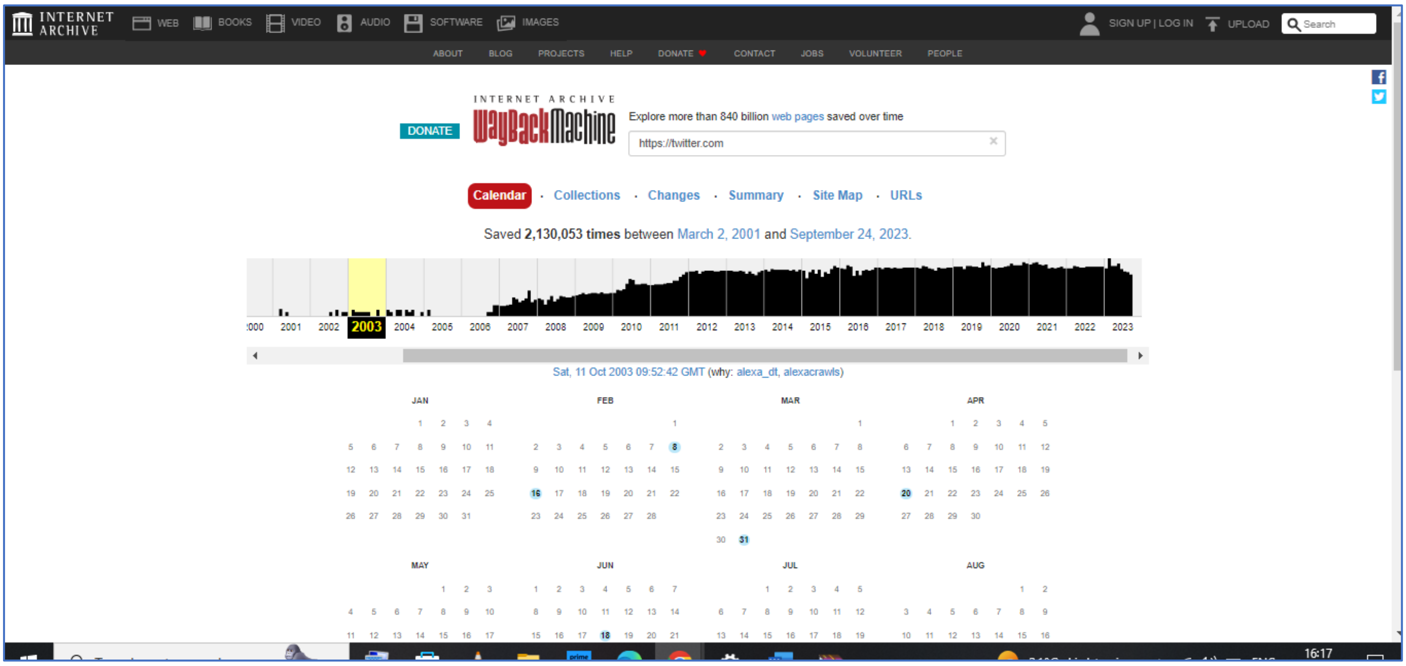
ViewDNS.info > Tools > **Reverse IP Lookup**

Takes a domain or IP address and does a reverse lookup to quickly shows all other domains hosted from the same server. Useful for finding phishing sites or identifying other sites on the same shared hosting server.

Domain / IP:
twitter.com GO

```
Reverse IP results for twitter.com (104.244.42.1, 104.244.42.129, 104.244.42.193, 104.244.42.65)
==============
```

Domain	Last Resolved Date
91nude.com	2023-09-21
anttikettunen.biz	2020-01-12
cardinglab.site	2022-07-11
celestials.tk	2023-01-22
coty.co	2023-09-21
equity-app.com	2023-09-21
jhpath.com	2023-09-19
sphinxara.com	2023-03-07
tweet.com.br	2023-03-19
twitter.ae	2022-01-20
twitter.co.uk	2023-09-17
twitter.com	2023-09-24
twitter.eus	2022-01-20
twitter.hk	2022-01-20
twitter.jp	2023-09-21
twitter.org	2023-09-23
twitterinc.com	2023-03-07
twittertrademarks.com	2023-03-07
twopensource.com	2023-03-07
twttr.com	2023-09-08
xn--2017-83dlgik3a7d2awca.xn--p1acf	2017-12-31



Explore more than 840 billion web pages saved over time

https://twitter.com

Saved 2,130,053 times between March 2, 2001 and September 24, 2023.

Sat, 11 Oct 2003 09:52:42 GMT (why: alexa_dt, alexacrawls)

EXIF DATA WITH IMAGE

Metadata

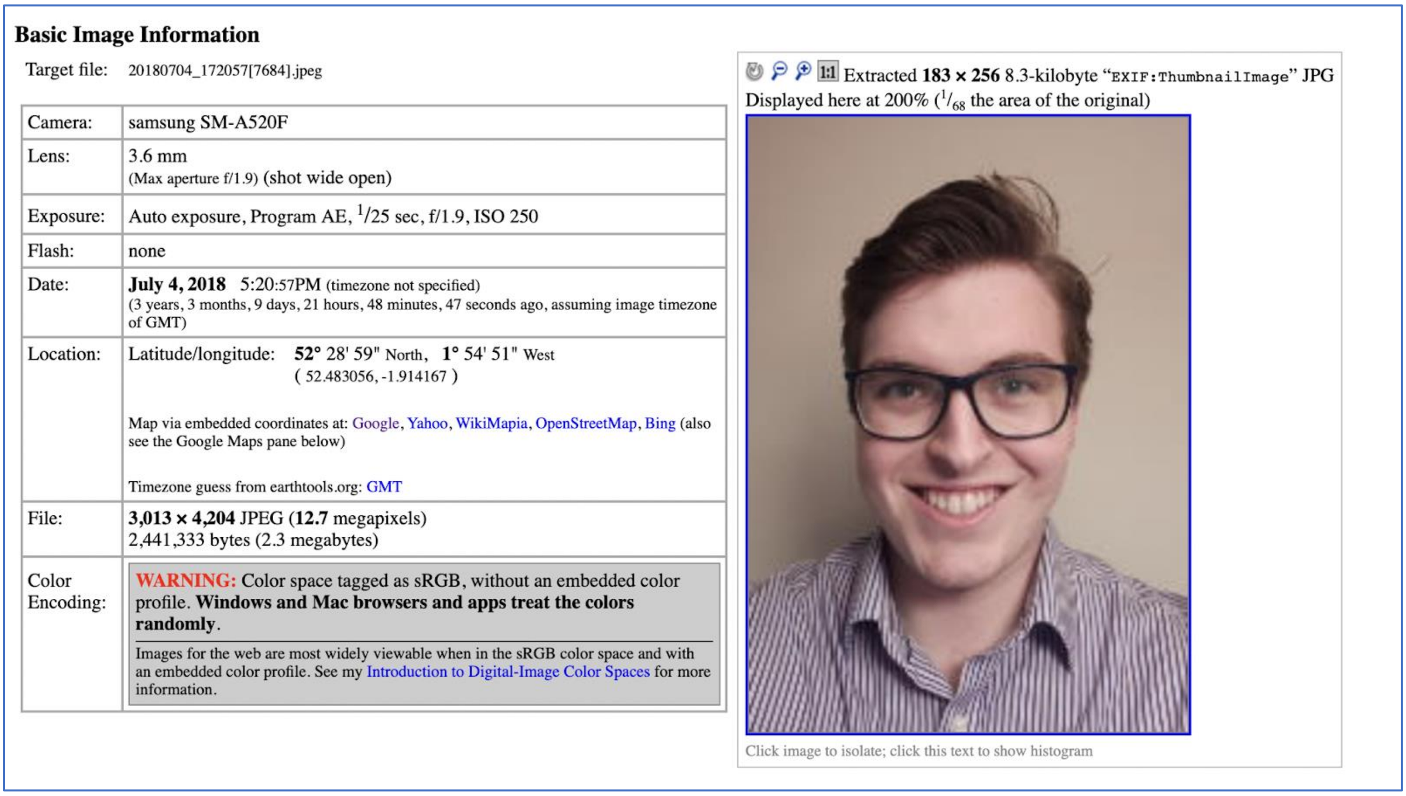
Metadata is data that provides information about data that is not the content of the data itself, i.e. summarising basic information about data to make it easier to find or work with.

Unfortunately, the majority of social media sites remove metadata from images as they are uploaded, however, if an original digital photo can be sourced then it is likely to provide some information on the photograph. Metadata can be viewed freely using a number of tools.

Jeffrey's Image Metadata Viewer — http://exif.regex.info/exif.cgi

Jeffrey's Image Metadata Viewer is a browser-based tool that enables you to upload a photo and view the EXIF data, detailing the time and date the image was taken, the type of camera used, and the location (in the event that location was enabled on the camera).

Jeffrey's Image Metadata Viewer will show all of the Metadata within an image, including Camera, Shutter Speed, Date Captured, and any embedded co-ordinates



Basic Image Information

Target file: 20180704_172057[7684].jpeg

Camera:	samsung SM-A520F
Lens:	3.6 mm (Max aperture f/1.9) (shot wide open)
Exposure:	Auto exposure, Program AE, $^1/25$ sec, f/1.9, ISO 250
Flash:	none
Date:	**July 4, 2018** 5:20:57PM (timezone not specified) (3 years, 3 months, 9 days, 21 hours, 48 minutes, 47 seconds ago, assuming image timezone of GMT)
Location:	Latitude/longitude: **52°** 28' 59" North, **1°** 54' 51" West (52.483056, -1.914167) Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Timezone guess from earthtools.org: GMT
File:	**3,013 × 4,204** JPEG (**12.7** megapixels) 2,441,333 bytes (2.3 megabytes)
Color Encoding:	WARNING: Color space tagged as sRGB, without an embedded color profile. **Windows and Mac browsers and apps treat the colors randomly**. Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.

Extracted **183 × 256** 8.3-kilobyte "EXIF:ThumbnailImage" JPG
Displayed here at 200% ($^1/_{68}$ the area of the original)

Click image to isolate; click this text to show histogram

● Conclusion:

The collection of tactical information using OSINT tools and techniques is a crucial part of cybersecurity, threat intelligence, and information gathering for various purposes. However, it's essential to use these tools and methodologies responsibly and ethically, respecting privacy and adhering to legal and ethical standards while conducting OSINT activities.