Open Source Intelligence Report

"Protection of computer systems and data from digital threats."

Group Members

Junaid
Azam Hussain
Muhammad Adnan
Syed Zain Ul Hasan Naqvi

NAVTTC PMYSDP Batch II – Cyber Security - NIIT

Note: This Report is for educational purpose only.

Assessment Number 1
Target: https://www.nadra.gov.pk

Introduction

The Open Source Intelligence (OSINT) Report provides a comprehensive analysis of publicly available information relevant to https://www.nadra.gov.pk. This report serves to practice OSINT techniques for cybersecurity, investigations, and Intelligence gathering

Report Objective

The primary objective of this report is to provide an in-depth analysis of https://www.nadra.gov.pk based on open source information. The report aims to identify key trends, patterns, and potential risks or opportunities within the scope of the organisation.

Scope of Analysis:

The analysis covers a wide range of open sources, including but not limited to press releases, social media platforms, public databases, and online portals.
The scope encompasses digital footprint aspect relevant to https://www.nadra.gov.pk.

Data Collection Methodologies

Dorking & SOCMINT

Website & Domain Reconnaissance

Geolocation & Image Analysis

Advanced Search Engine OSINT

Dorking Techniques - Using Google, Bing and Yandex
Finding Hidden Pages - Data Leaks using Google Dorks
Hands-On Challenge - PDF, XLS Files and site specific data

Hidden Page:
fal.nadra.gov.pk

site:nadra.gov.pk
intitle:“admin”
inurl: “admin”
filetype:"pdf“
OR | AND & Operators

Google Results

https://www.nadra.gov.pk

https://succession.nadra.gov.pk

https://supremecourt.nadra.gov.pk

https://balochistansuccession.nadra.gov.pk

https://poa.nadra.gov.pk

https://ebil.nadra.gov.pk

https://sindhsuccession.nadra.gov.pk

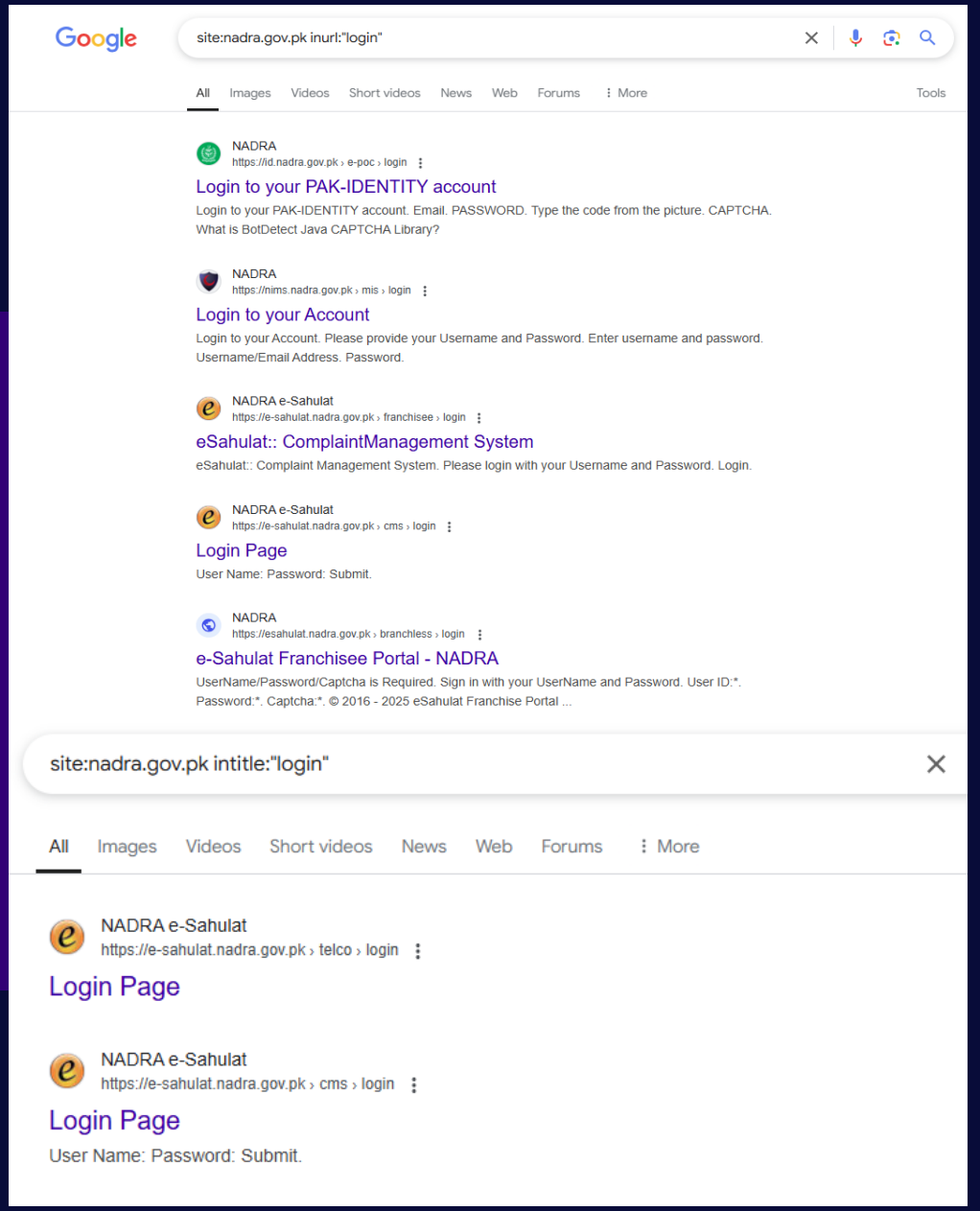
https://ictsuccession.nadra.gov.pk

https://kpsuccession.nadra.gov.pk

https://punjabsuccession.nadra.gov.pk

https://fatatdp.nadra.gov.pk

- https://visa.nadra.gov.pk/Chinese_guide.pdf
- https://visa.nadra.gov.pk/downloads/application_guide.pdf
- https://supremecourt.nadra.gov.pk/downloads_judgements/JR_Detailed_Judgment_in_Appointment_of_Supreme_Court_Judges_Case.pdf
- https://supremecourt.nadra.gov.pk/downloads_judgements/JR_Fecto_Belarus_Tractor_Limited_Case.pdf
- https://id.nadra.gov.pk/docs/PPOsites.pdf
- https://tenders.nadra.gov.pk/Lookup/DownloadTenderApplicantAttachment?Id=CfDJ8LYxafjT5SRMm8M4pl_qvYOkcAeYnaPP5bgVQfbun9dgXOGTxSqPS0NoTYRUQdK7ACKXP_XSKReO5HLvsItI_kOywCzrrn9E1KTge2yIn0zmrNWMwZ82ccocD6jSiEwgTw



Bing Results

https://www.nadra.gov.pk

https://id.nadra.gov.pk

https://visa.nadra.gov.pk

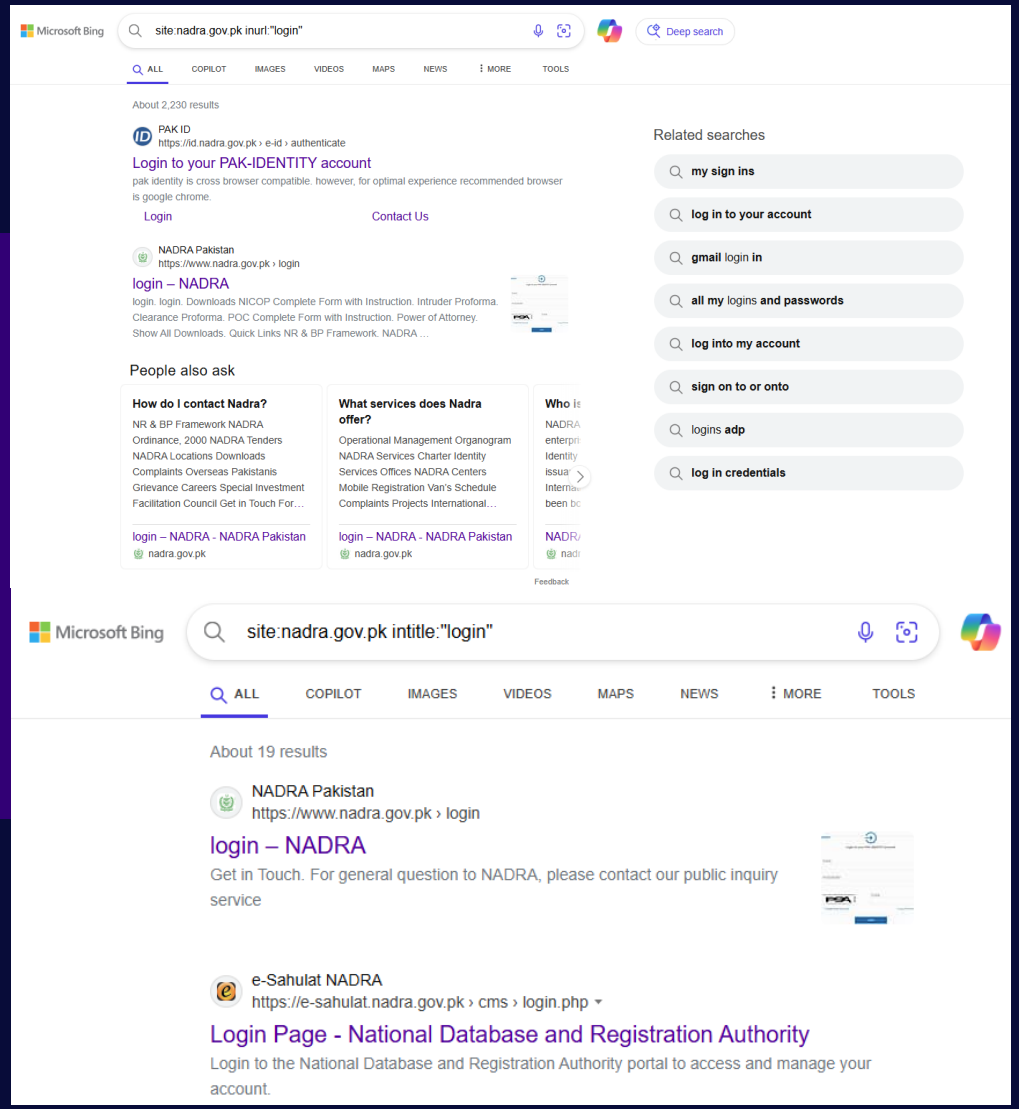
https://complaints.nadra.gov.pk

https://e-sahulat.nadra.gov.pk

https://poa.nadra.gov.pk

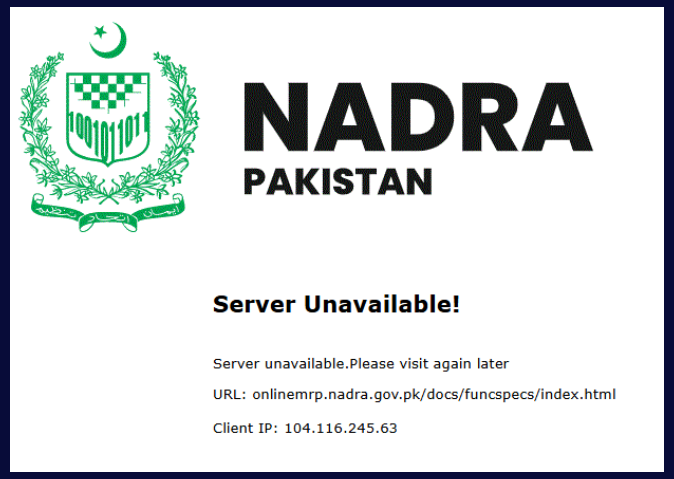
https://careers.nadra.gov.pk

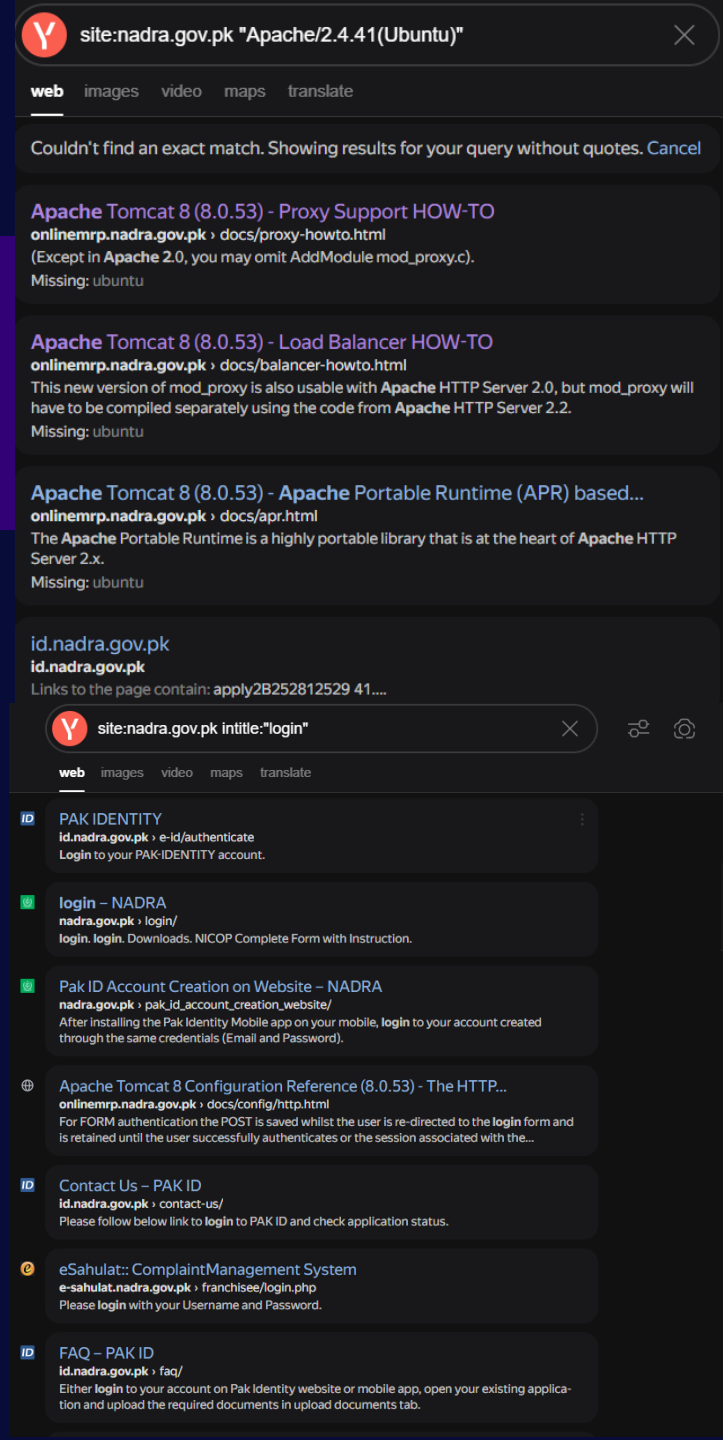
- https://www.nadra.gov.pk/wp-content/uploads/2024/04/nadra-ordianance-2000-07.10.2022.pdf
- https://ebil.nadra.gov.pk/downloads/UndertakingFormForeigners.pdf
- https://www.nadra.gov.pk/author/admin/
- https://fal.nadra.gov.pk

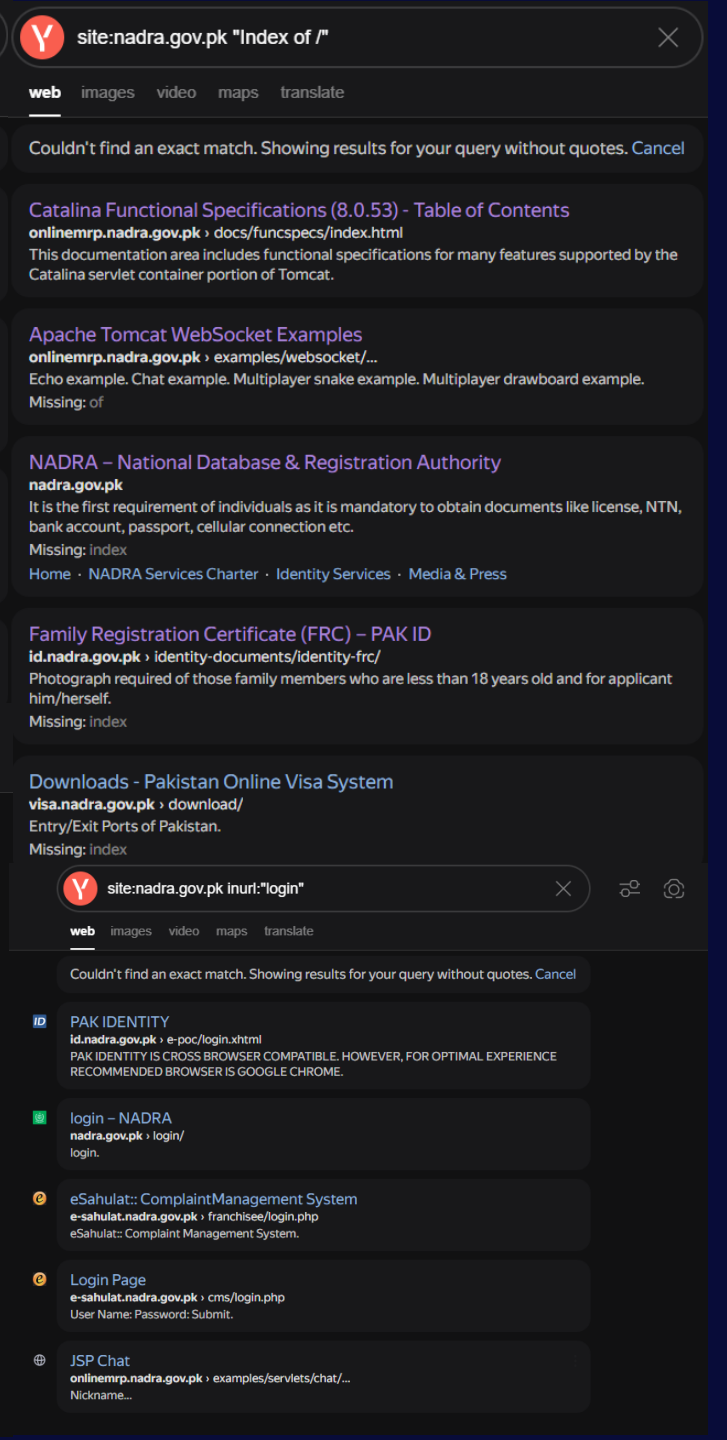


Yandex Results

nims.nadra.gov.pk
pal.nadra.gov.pk
id.nadra.gov.pk
ictsuccession.nadra.gov.pk
visa.nadra.gov.pk
poa.nadra.gov.pk
nishan.nadra.gov.pk
ebil.nadra.gov.pk







Hidden Pages & Files

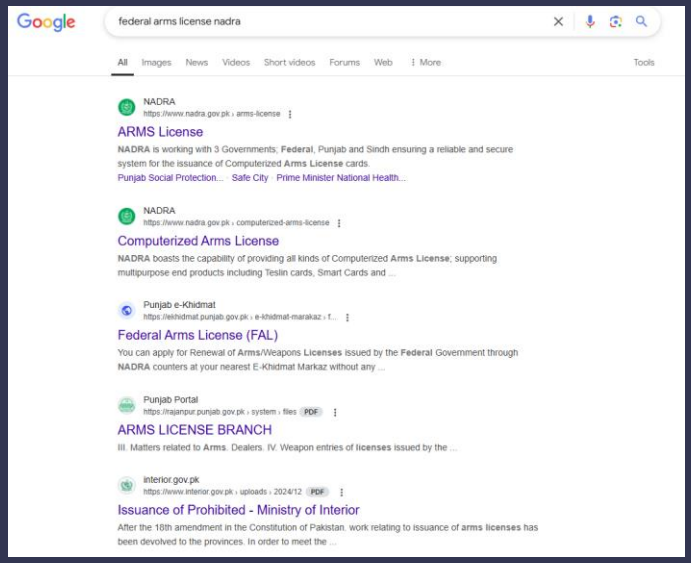
fal.nadra.gov.pk

01

https://blog.drhack.net/nadra-hacked-pitb-data-leak/

02

https://freenote.biz/F7OPEdGpXb



Social Media Intelligence

SOCMINT

Finding footprints on social media along with recent activity and mutual connections between profiles

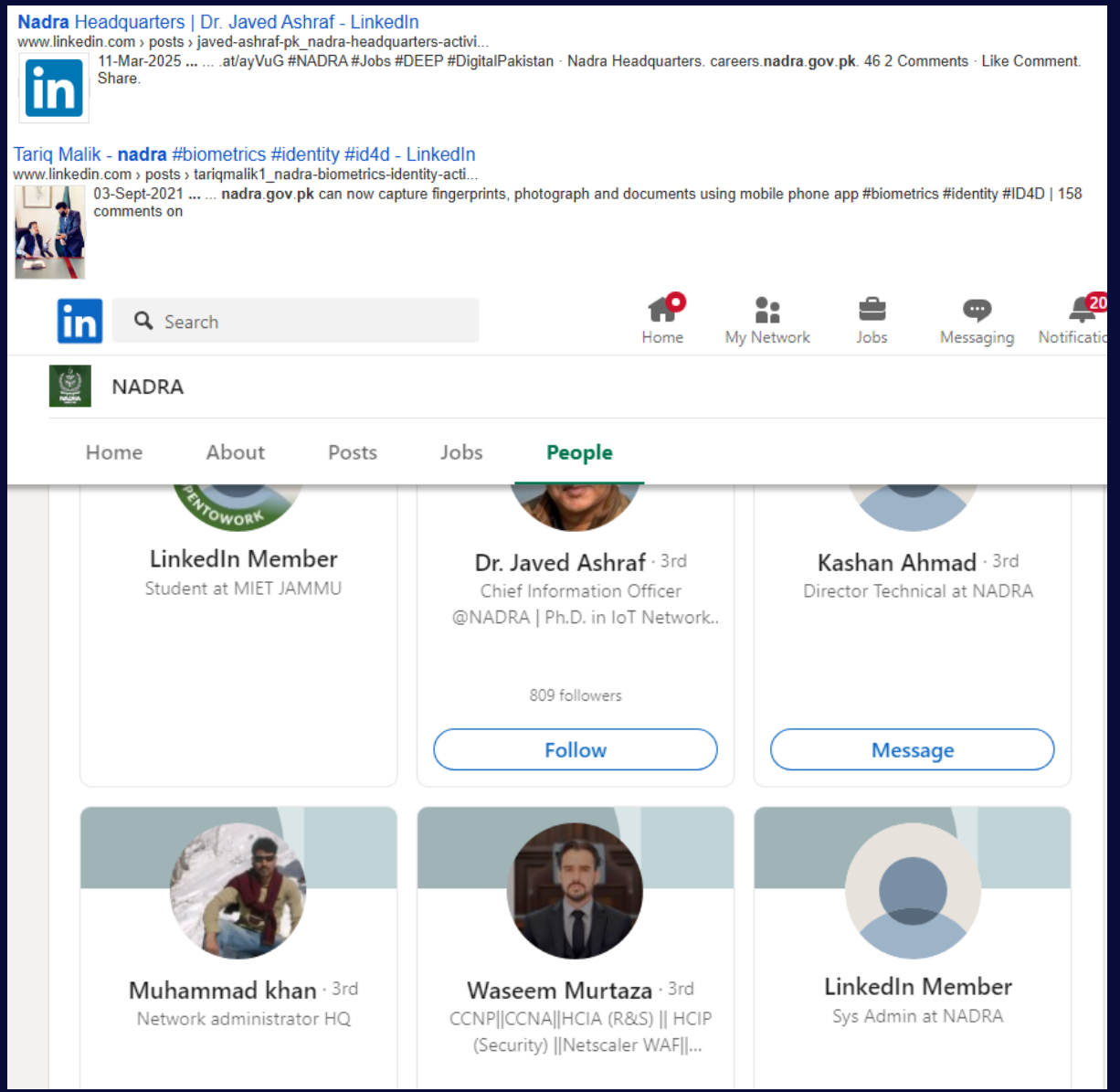
01 social-searcher.com

02 linkedin.com

03 brandmentions.com

NADRA Social Media & Senior Employees

Finding connections between social media profiles



Website & Domain Reconnaissance

Data into Information through WHOIS, Historic DNS Records, Metadata extraction from images and documents

01 whois.com

02 viewdns.info

03 MW Metadata

04 netcraft.com

Background

Site title	The URL you requested has been blocked	**Date first seen**	March 2015
Site rank	81223	**Primary language**	English
Description	Not Present		

IP delegation

IPv4 address (2.19.176.128)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
2.0.0.0-2.255.255.255	Netherlands	2-RIPE	RIPE Network Coordination Centre
2.16.0.0-2.23.255.255	European Union	NL-AKAMAI-20100910	Akamai International B.V.
2.19.176.0-2.19.191.255	European Union	AKAMAI-PA	Akamai Technologies
2.19.176.128	European Union	AKAMAI-PA	Akamai Technologies

IPv6 address (2a02:26f0:9b00:0:0:0:17d8:9aeb)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inet6num object
2a00::/11	European Union	EU-ZZ-2A00	RIPE NCC
2a00::/12	Netherlands	EU-ZZ-2A00	RIPE Network Coordination Centre
2a02:26f0::/29	European Union	NL-AKAMAI-20101022	Akamai International B.V.
2a02:26f0:9b00::/48	European Union	AKAMAI-PA	Akamai Technologies
2a02:26f0:9b00:0:0:0:17d8:9aeb	European Union	AKAMAI-PA	Akamai Technologies

IP

Source: netcraft.com

```
# WHOIS .PK Domains (PKNIC)

    Domain: nadra.gov.pk
    Status: Domain is Registered


    Creation Date: 2001-05-09
    Expiry Date: 2028-05-09
    Name Server: ian.ns.cloudflare.com
    Name Server: rose.ns.cloudflare.com
    Name Server:
    Name Server:
```

DNS

Source: whois.com

Rank	Site	First seen	Netblock	OS	Site Report
80254	www.nadra.gov.pk	March 2015	Cloudflare, Inc.	Linux	
82523	id.nadra.gov.pk	September 2015	Nayatel (Pvt) Ltd	unknown	
88563	careers.nadra.gov.pk	July 2022	Cloudflare, Inc.	Linux	
95117	visa.nadra.gov.pk	May 2019	Cloudflare, Inc.	Linux	
209498	pal.nadra.gov.pk	April 2024	Cloudflare, Inc.	Linux	
225409	nims.nadra.gov.pk	August 2017	Cloudflare, Inc.	Linux	
490462	payment.nadra.gov.pk	January 2024	Cloudflare, Inc.	Linux	
548451	complaints.nadra.gov.pk	July 2022	Cloudflare, Inc.	Linux	
580386	ebil.nadra.gov.pk	June 2020	National Wimax/IMS environment	unknown	
590757	e-sahulat.nadra.gov.pk	November 2015	Cloudflare, Inc.	Linux	
947521	crms.nadra.gov.pk	December 2018	Nayatel (Pvt) Ltd	unknown	
1121080	esahulat.nadra.gov.pk	August 2018	Nayatel (Pvt) Ltd	unknown	
1347525	nadra.gov.pk	June 2013	Cloudflare, Inc.	Linux	
1393958	sindhsuccession.nadra.gov.pk	September 2021	Cloudflare, Inc.	Linux	

Sub Domain

Source: netcraft.com

Domain registrar	Unknown
Nameserver organisation	whois.cloudflare.com
Organisation	Unknown
DNS admin	dns@cloudflare.com
Top Level Domain	Pakistan (.gov.pk)
DNS Security Extensions	Enabled
IPv4 address	2.19.176.128 (VirusTotal)
IPv4 autonomous systems	AS20940
IPv6 address	2a02:26f0:9b00:0:0:0:17d8:9aeb
IPv6 autonomous systems	AS20940
Reverse DNS	a2-19-176-128.deploy.static.akamaitechnologies.com

DNS Records

Source: netcraft.com

nadra.gov.pk DNS records as of Mar 19, 2025

A records

Akamai International B.V.

23.48.104.87 0

23.55.176.172 0

AAAA records

2600:1408:20::172e:ef39 0

2600:1408:20::172e:ef49 0

MX records

Nayatel (Pvt) Ltd

5 mail1.nadra.gov.pk 0

10 mail.nadra.gov.pk 0

NS records

Cloudflare, Inc.

rose.ns.cloudflare.com 0

ian.ns.cloudflare.com 0

SOA records

ttl: 10000

email: dns.cloudflare.com 0

TXT

v=spf1 ip4:115.186.143.25 ip4:58.27.228.25 ip4:115.186.143.26 ip4:115.186.143.28 ip4:115.186.143.207 ip4:115.186.143.219 ip4:115.186.143.124 ip4:115.186.143.125 ip4:58.27.228.124 ip4:58.27.228.125 a:ksmg1out.nadra.gov.pk a:ksmg2out.nadra.gov.pk a:mail.nad ra.gov.pk a:mail1.nadra.gov.pk a:mail2.nadra.gov.pk ~all

google-site-verification=-pRfPQA7pJ0w5bIY4f4Bl3OAIHzpjj03Hf48kJnJfCQ

DNS Records

Source: viewdns.info & securitytrails.com

nadra.gov.pk

DNS information

Whois | RDAP | DNS Records | Uptime | Diagnostics

DNS Records for nadra.gov.pk

Hostname	Type	TTL	Priority	Content
nadra.gov.pk	SOA	1800		ian.ns.cloudflare.com dns@cloudflare.com 2367852930 10000 2400 604800 1800
nadra.gov.pk	NS	21600		rose.ns.cloudflare.com
nadra.gov.pk	NS	21600		ian.ns.cloudflare.com
nadra.gov.pk	A	6		23.48.104.73
nadra.gov.pk	A	6		23.48.104.87
nadra.gov.pk	AAAA	6		2600:1408:20::6870:ebda
nadra.gov.pk	AAAA	6		2600:1408:20::6870:ebab
nadra.gov.pk	MX	300	10	mail.nadra.gov.pk
nadra.gov.pk	MX	300	5	mail1.nadra.gov.pk
www.nadra.gov.pk	A	20		23.48.104.87
www.nadra.gov.pk	A	20		23.48.104.73
www.nadra.gov.pk	AAAA	20		2600:1408:ec00:2e::1735:baf
www.nadra.gov.pk	AAAA	20		2600:1408:ec00:2e::1735:bae
www.nadra.gov.pk	CNAME	300		edge-www.nadra.gov.pk.edgekey.net

nadra.gov.pk

Uptime & Server Information

Historical uptime rate: **100%** based on 8 data points

Whois | RDAP | DNS Records | Uptime | Diagnostics

Current Status

Status	Active
Server Type	Unknown
Page Title	NADRA – National Database & Registration Authority
Meta Description	Not available
Meta Keywords	Not available
Most Recent Data	0 hours, 0 minutes ago

Historical Data

Date	Status	Server
2025-03-19 18:51:47	Active	Unknown
2025-03-13 12:14:57	Active	Unknown
2025-02-24 05:39:28	Active	Unknown
2025-02-17 23:26:01	Active	Unknown
2025-01-23 15:40:13	Active	cloudflare
2025-01-21 09:59:24	Active	Unknown
2025-01-09 05:22:48	Active	Unknown

IP & DNS Records

Source: viewdns.info & securitytrails.com

Reverse IP results for nadra.gov.pk (23.45.46.198, 23.45.46.211)

There are 130 domains hosted on this server.
The complete listing of these is below:

IP history results for 'nadra.gov.pk'.

IP ADDRESS	LOCATION	IP ADDRESS OWNER	LAST SEEN ON THIS IP
23.45.46.211	Chicago - United States	Akamai International B.V.	2025-03-19
23.45.46.198	Chicago - United States	Akamai International B.V.	2025-03-19
23.213.203.64	Chicago - United States	Akamai International B.V.	2025-03-19
23.213.203.50	Chicago - United States	Akamai International B.V.	2025-03-19
2.17.100.216	Frankfurt am Main - Germany	Akamai International B.V.	2025-03-18
2.17.100.187	Frankfurt am Main - Germany	Akamai International B.V.	2025-03-18
23.213.203.50	Chicago - United States	Akamai International B.V.	2025-03-17
23.213.203.24	Chicago - United States	Akamai International B.V.	2025-03-17
23.64.119.60	Dallas - United States	Akamai Technologies, Inc.	2025-03-13
172.67.30.179	Unknown	Cloudflare, Inc	2025-03-02
104.22.15.154	Unknown	Cloudflare, Inc	2025-03-02
104.22.14.154	Unknown	Cloudflare, Inc	2025-03-02
188.114.99.228	Unknown	Cloudflare, Inc	2025-02-24
188.114.98.228	Unknown	Cloudflare, Inc	2025-02-24

nadra.gov.pk

DNS information

Whois | RDAP | DNS Records | Uptime | Diagnostics

DNS Records for nadra.gov.pk

Hostname	Type	TTL	Priority	Content
nadra.gov.pk	SOA	1800		ian.ns.cloudflare.com dns@cloudflare.com 2367852930 10000 2400 604800 1800
nadra.gov.pk	NS	21600		rose.ns.cloudflare.com
nadra.gov.pk	NS	21600		ian.ns.cloudflare.com
nadra.gov.pk	A	6		23.48.104.73
nadra.gov.pk	A	6		23.48.104.87
nadra.gov.pk	AAAA	6		2600:1408:20::6870:ebda
nadra.gov.pk	AAAA	6		2600:1408:20::6870:ebab
nadra.gov.pk	MX	300	10	mail.nadra.gov.pk
nadra.gov.pk	MX	300	5	mail1.nadra.gov.pk
www.nadra.gov.pk	A	20		23.48.104.87
www.nadra.gov.pk	A	20		23.48.104.73
www.nadra.gov.pk	AAAA	20		2600:1408:ec00:2e::1735:baf
www.nadra.gov.pk	AAAA	20		2600:1408:ec00:2e::1735:bae
www.nadra.gov.pk	CNAME	300		edge-www.nadra.gov.pk.edgekey.net

nadra.gov.pk

Uptime & Server Information

Historical uptime rate: **100%** based on 8 data points

Whois | RDAP | DNS Records | Uptime | Diagnostics

Current Status

Status	Active
Server Type	Unknown
Page Title	NADRA – National Database & Registration Authority
Meta Description	Not available
Meta Keywords	Not available
Most Recent Data	0 hours, 0 minutes ago

Historical Data

Date	Status	Server
2025-03-19 18:51:47	Active	Unknown
2025-03-13 12:14:57	Active	Unknown
2025-02-24 05:39:28	Active	Unknown
2025-02-17 23:26:01	Active	Unknown
2025-01-23 15:40:13	Active	cloudflare
2025-01-21 09:59:24	Active	Unknown
2025-01-09 05:22:48	Active	Unknown

DNS Records for 'nadra.gov.pk'

RECORD NAME	TTL	CLASS	TYPE	PRIORITY	DATA
nadra.gov.pk.	1800	IN	SOA		ian.ns.cloudflare.com. dns.cloudflare.com. 2367852930 10000 2400 604800 1800
nadra.gov.pk.	21600	IN	NS		rose.ns.cloudflare.com.
nadra.gov.pk.	21600	IN	NS		ian.ns.cloudflare.com.
nadra.gov.pk.	30	IN	A		23.45.46.198
nadra.gov.pk.	30	IN	A		23.45.46.211
nadra.gov.pk.	30	IN	AAAA		2600:1407:3c00:cd::172d:2ea9
nadra.gov.pk.	30	IN	AAAA		2600:1407:3c00:cd::172d:2ea5
nadra.gov.pk.	300	IN	TXT		"google-site-verification=-pRfPQA7pJ0w5bIY4f4BI3OAIHzpjj03Hf48kJnJfCQ"
nadra.gov.pk.	300	IN	TXT		"v=spf1 ip4:115.186.143.25 ip4:58.27.228.25 ip4:115.186.143.26 ip4:115.186.143.28 ip4:115.186.143.207 ip4:115.186.143.219 ip4:115.186.143.124 ip4:115.186.143.125 ip4:58.27.228.124 ip4:58.27.228.125 a:ksmg1out.nadra.gov.pk a:ksmg2out.nadra.gov.pk a:mail.nad" "ra.gov.pk a:mail1.nadra.gov.pk a:mail2.nadra.gov.pk ~all"
nadra.gov.pk.	300	IN	MX	10	mail.nadra.gov.pk.
nadra.gov.pk.	300	IN	MX	5	mail1.nadra.gov.pk.
_dmarc.nadra.gov.pk.	300	IN	TXT		"v=DMARC1; p=reject; rua=mailto:dmarc@nadra.gov.pk; ruf=mailto:dmarc_forensic@nadra.gov.pk; rf=afrf; sp=none; pct=100; fo=1:d:s; ri=7200; adkim=s; aspf=s"

MAC Lookup Results for 'nadra.gov.pk'

LOOKUP ERROR

INVALID MAC ADDRESS SUPPLIED.
Valid MAC address formats are
xxxxxx... - e.g. 00010203...
xx:xx:xx... - e.g. 00:01:02:03...
xx-xx-xx... - e.g. 00-01-02-03...
xx.xx.xx... - e.g. 00.01.02.03...

Source: viewdns.info

HOP	HOSTNAME / IP	ISP	LOCATION	RESPONSE TIME
1	obfuscated.internal.network.com (0.0.0.0)			0.000ms
2	obfuscated.internal.network.com (0.0.0.0)			1.000ms
3	149.56.61.126	OVH SAS	Montreal, Canada	0.261ms
4	10.98.80.0	QUAD9-AS-1		0.292ms
5	10.196.145.44	QUAD9-AS-1		0.450ms
6	10.74.10.8	QUAD9-AS-1		0.286ms
7	10.95.81.10	QUAD9-AS-1		0.693ms
8	be101.yto-tr1-sbb2-8k.on.ca (192.99.146.49)	OVH SAS	Canada	7.999ms
9	10.200.5.3	QUAD9-AS-1		10.039ms
10	akamai.ip4.torontointernetxchange.net (206.108.34.24)	IHI	Canada	17.732ms
11	???			
12	???			
13	a23-222-17-228.deploy.static.akamaitechnologies.com (23.222.17.228)	Akamai International B.V.	Toronto, Canada	7.037ms

Traceroute

Source: viewdns.info

Advanced Techniques & Live Investigations

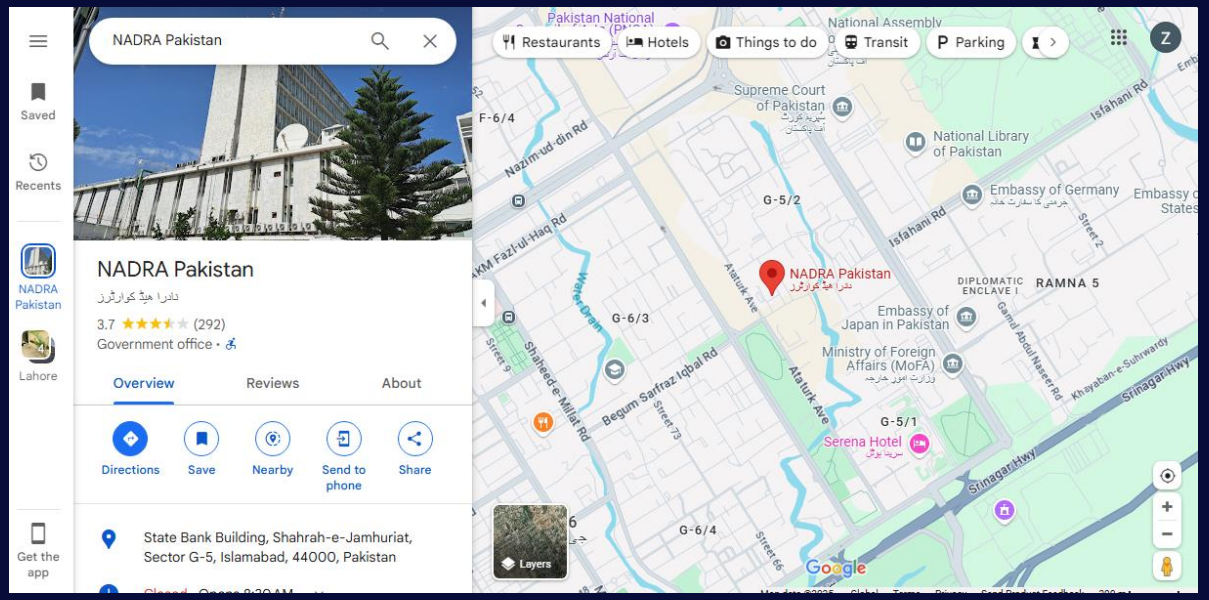
Practicing reverse image search with Geolocation & Image Analysis along with Email & Phone Number OSINT

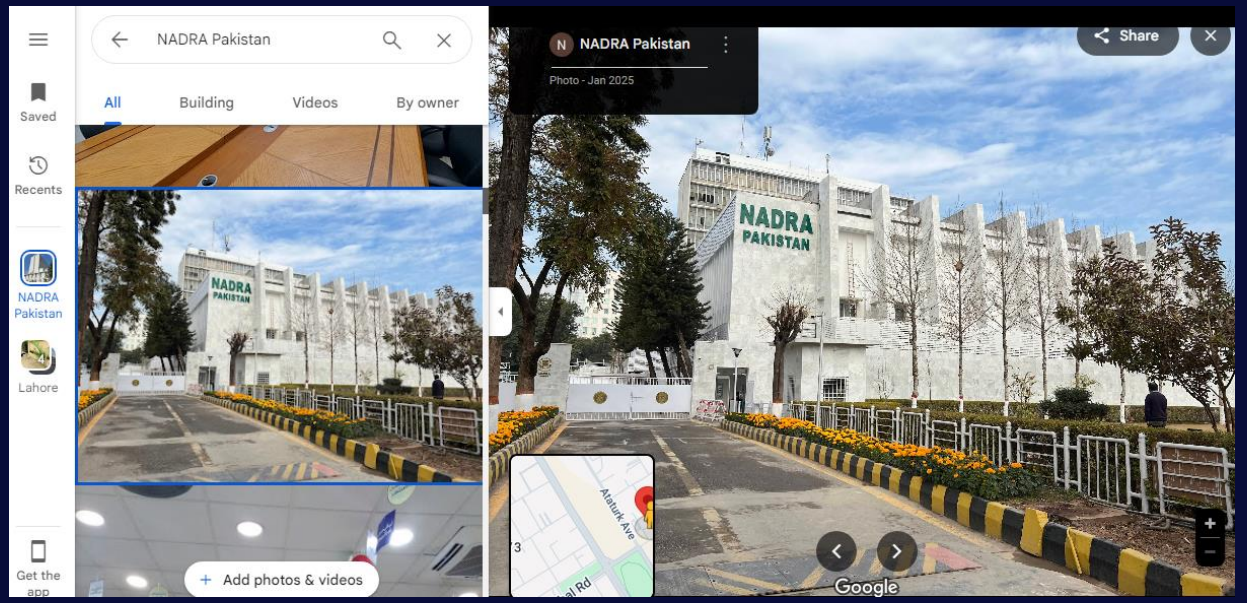
01 Google Lens

02 Yandex Image Search

03 osint.email

04 truecaller / Numspy



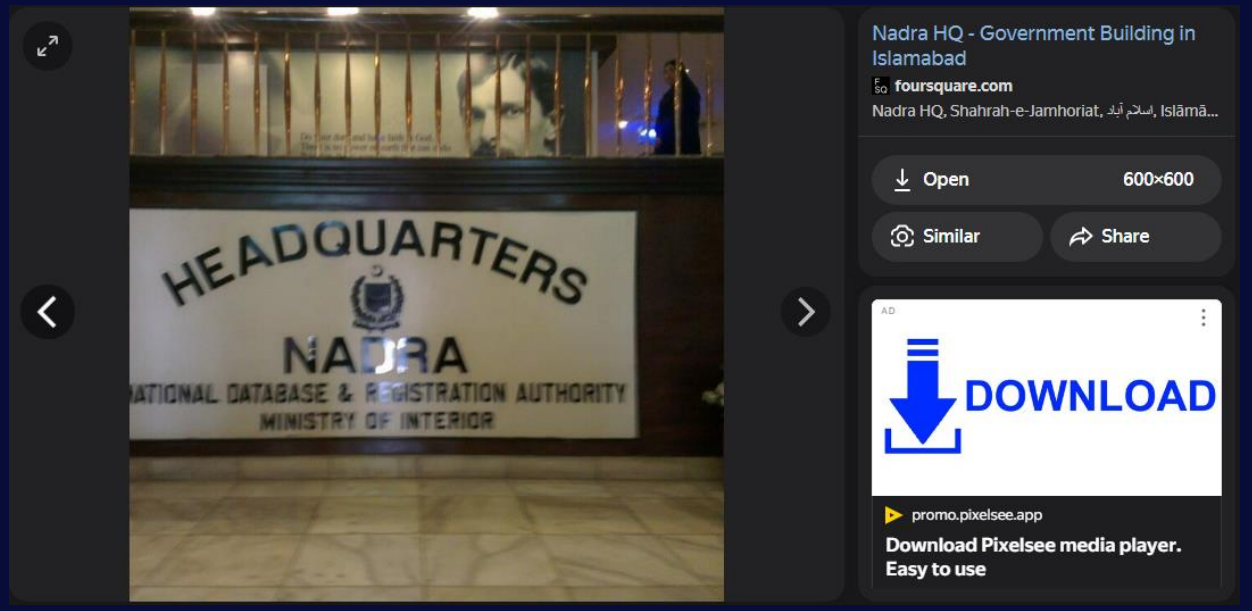


Reverse Image Search

Google Maps, Google Lens,

Google StreetView, Yandex & MW

Metadata

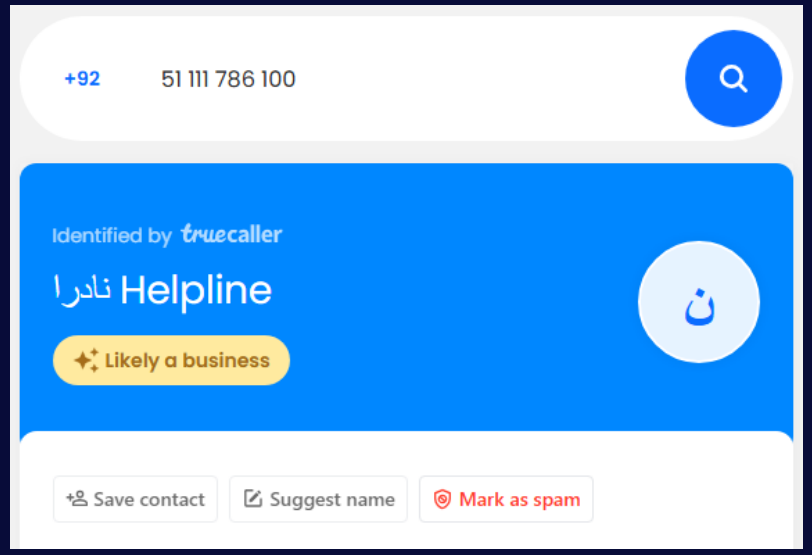


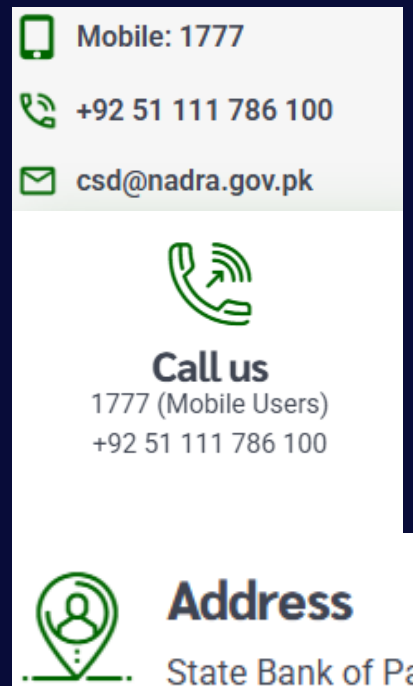
Email & Phone Number OSINT

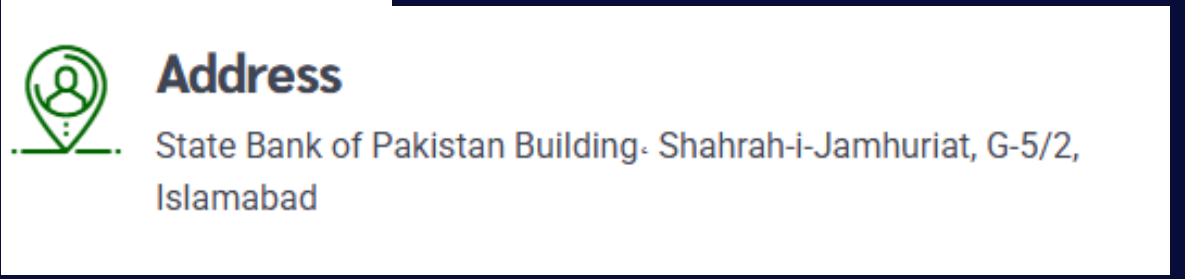
Target Website, Google Maps,

TrueCaller, Numspy,

osint.email







Conclusion

The OSINT Report provides a comprehensive analysis of https://www.nadra.gov.pk based on publicly available information. By leveraging open source intelligence, this report aims to inform decision-makers, enhance situational awareness, and support strategic planning efforts.

Thank You!

We respect your valuable time!
If you have any questions, please reach us

Jazak'Allah Khairan

GROUP MEMBERS

Junaid
Azam Hussain
Muhammad Adnan
Syed Zain Ul Hasan Naqvi