Name: Chanchal Teli

Intern ID:125

Proof-of-Concept Report: CRT.sh Certificate Transparency Log Tool

Tool Name

CRT.sh Certificate Search

Description

CRT.sh is a free web-based service that allows users to search Certificate Transparency (CT) logs to discover SSL/TLS certificates issued for any domain.

Why use this tool?

It allows passive discovery of subdomains, relationships between domains, and certificate history to help with reconnaissance, asset tracking, and phishing detection.

Key Characteristics

- Public Certificate Transparency log search engine
- Discovers issued SSL/TLS certificates for any domain
- Wildcard and keyword support (e.g., %.gov.in)
- Helps find subdomains and expired/rogue certificates

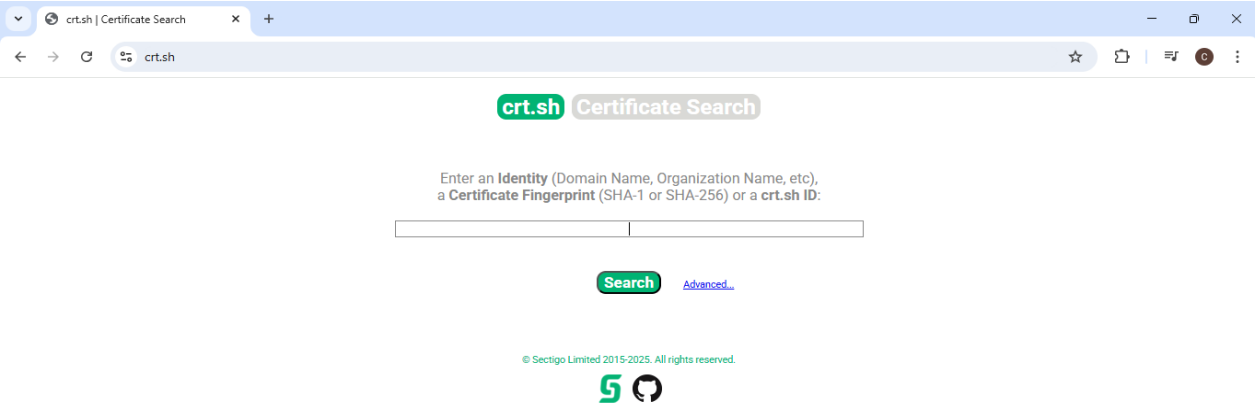
- Useful for passive reconnaissance and OSINT
- No login required for basic use
- Simple UI and API support
- Displays issuer, fingerprint, and expiry details

How CRT.sh Helps Cybersecurity Professionals

- Reveals domain infrastructure using certificates
- Tracks suspicious certificate issuance or misuse
- Passive reconnaissance to avoid alerts/logs
- Enables threat attribution and asset discovery
- Complements tools like FOFA, Shodan, Censys

How to Use CRT.sh

1. Go to https://crt.sh



2. Enter a domain (e.g., example.com)

crt.sh | meity.gov.in

crt.sh/?q=meity.gov.in

crt.sh Identity Search

Group by Issuer

Criteria	Type: Identity Match: ILIKE Search: 'meity.gov.in'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
19661643967	2025-07-14	2025-07-14	2025-10-12	portal.meity.gov.in	portal.meity.gov.in	C=US, O=Let's Encrypt, CN=R11
19661643520	2025-07-14	2025-07-14	2025-10-12	portal.meity.gov.in	portal.meity.gov.in	C=US, O=Let's Encrypt, CN=R11
19529025257	2025-07-08	2025-07-08	2025-10-06	api.meity.gov.in	api.meity.gov.in	C=US, O=Let's Encrypt, CN=R11
19529024948	2025-07-08	2025-07-08	2025-10-06	api.meity.gov.in	api.meity.gov.in	C=US, O=Let's Encrypt, CN=R11
19526117731	2025-07-08	2025-07-08	2025-10-06	sparrow.meity.gov.in	sparrow.meity.gov.in	C=US, O=Let's Encrypt, CN=E5
19526117808	2025-07-08	2025-07-08	2025-10-06	sparrow.meity.gov.in	sparrow.meity.gov.in	C=US, O=Let's Encrypt, CN=E5
19206204876	2025-06-23	2025-06-23	2025-09-21	www.meity.gov.in	www.meity.gov.in	C=US, O=Let's Encrypt, CN=R11
19206204431	2025-06-23	2025-06-23	2025-09-21	www.meity.gov.in	www.meity.gov.in	C=US, O=Let's Encrypt, CN=R11
19136375089	2025-06-20	2025-06-20	2026-07-21	swayaan.meity.gov.in	swayaan.meity.gov.in www.swayaan.meity.gov.in	C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA DV R36
19136374558	2025-06-20	2025-06-20	2026-07-21	swayaan.meity.gov.in	swayaan.meity.gov.in www.swayaan.meity.gov.in	C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA DV R36
19050817001	2025-06-16	2025-06-16	2025-09-14	intern.meity.gov.in	intern.meity.gov.in	C=US, O=Let's Encrypt, CN=E6
19050817191	2025-06-16	2025-06-16	2025-09-14	intern.meity.gov.in	intern.meity.gov.in	C=US, O=Let's Encrypt, CN=E6

3. Use wildcards like %.example.com to discover subdomains

crt.sh | *.gov.in

crt.sh/?q=*.gov.in

crt.sh Identity Search

Group by Issuer

Criteria	Type: Identity Match: ILIKE Search: '*.gov.in'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
19233567504	2025-06-24	2025-06-24	2025-09-22	www.swwcreation.com.bssranchi.in	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R11
19233567300	2025-06-24	2025-06-24	2025-09-22	www.swwcreation.com.bssranchi.in	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R11
18026013288	2025-04-23	2025-04-23	2025-07-22	*.cgstauditranchi.gov.in	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R10
18026020434	2025-04-23	2025-04-23	2025-07-22	*.cgstauditranchi.gov.in	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R10
17307241636	2025-02-21	2025-02-21	2025-05-22	cgstauditranchi.gov.in	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R11
16827674574	2025-02-21	2025-02-21	2025-05-22	cgstauditranchi.gov.in	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R11
16207398110	2024-12-22	2024-12-22	2025-03-22	www.gstauditranchi.gov.in.bssranchi.in	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R10
15856636957	2024-12-22	2024-12-22	2025-03-22	www.gstauditranchi.gov.in.bssranchi.in	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R10
15052183039	2024-10-22	2024-10-22	2025-01-20	www.divinenursingcollege.com	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R11
15046874717	2024-10-22	2024-10-22	2025-01-20	www.divinenursingcollege.com	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R11
14273723619	2024-08-22	2024-08-22	2024-11-20	*.com.bssranchi.in	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R10
14252845033	2024-08-22	2024-08-22	2024-11-20	*.com.bssranchi.in	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R10
13482849027	2024-06-22	2024-06-22	2024-09-20	cgstauditranchi.gov.in	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R11
13482843832	2024-06-22	2024-06-22	2024-09-20	cgstauditranchi.gov.in	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R11
12816872746	2024-04-22	2024-04-22	2024-07-21	cgstauditranchi.gov.in	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R3
12816865473	2024-04-22	2024-04-22	2024-07-21	cgstauditranchi.gov.in	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R3
12151041294	2024-02-21	2024-02-21	2024-05-21	cgstauditranchi.gov.in	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R3
12151041299	2024-02-21	2024-02-21	2024-05-21	cgstauditranchi.gov.in	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R3
11550864800	2023-12-22	2023-12-22	2024-03-21	www.gstauditranchi.gov.in.bssranchi.in	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R3
11518508386	2023-12-22	2023-12-22	2024-03-21	www.gstauditranchi.gov.in.bssranchi.in	*.gov.in.bssranchi.in	C=US, O=Let's Encrypt, CN=R3

4. Review certificate details: issuer, expiry, fingerprints

crt.sh | 18026020434

crt.sh/?id=18026020434

crt.sh Certificate Search

Criteria	ID = '18026020434'

crt.sh ID	18026020434
Summary	Precertificate

Certificate Transparency

Log entries for this certificate:

Timestamp	Entry #	Log Operator	Log URL
2025-04-23 22:38:29 UTC	230414863	Let's Encrypt	https://oak.ct.letsencrypt.org/2025h2
2025-04-23 22:38:30 UTC	1429102258	DigiCert	https://yeti2025.ct.digicert.com/log

Revocation

Report a problem with this certificate to the CA

Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
OCSP	The CA	Check	?	n/a	?
CRL	The CA	Not Revoked (Expired)	n/a	n/a	2025-07-26 01:43:41 UTC
CRLSet/Blocklist	Google	Not Revoked	n/a	n/a	n/a
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a

Certificate Fingerprints

SHA-256 DE0BDD3DAC3DF73B8770FAD426A8C64EE6DD85078721D4C9C052ED7D00481434 SHA-1 295CA60C5FB18A8484798A1343D241B006B46C7F

| ASN.1 | Certificate | Graph | Hierarchy | pv |

Hide metadata

Run linters using pkimetal

Download Certificate: PEM

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            05:52:51:59:a6:15:37:51:78:59:1a:d5:af:a4:51:9f:a7:20
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 295814)
            commonName               = R10
            organizationName         = Let's Encrypt
            countryName              = US
        Validity (Expired)
            Not Before: Apr 23 21:39:59 2025 GMT
            Not After : Jul 22 21:39:58 2025 GMT
        Subject:
            commonName               = *.cgstauditranchi.gov.in
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:ad:4f:68:42:ae:1f:8f:14:a6:7e:32:53:33:34:
                    33:81:6f:01:c1:6a:64:b1:ec:9f:89:a7:dd:fa:79:
                    b6:f8:87:63:ca:05:3c:b2:fa:2f:79:cd:10:66:57:
                    3b:32:38:57:db:d1:30:18:d4:ff:6e:70:f9:99:d2:
                    ea:e6:a9:e7:7b:5f:b9:86:4c:33:1a:0e:c5:96:b6:
                    03:c1:42:c1:b9:65:fb:39:b6:9f:d2:4f:b6:d3:7c:
                    47:cd:49:42:4c:79:c3:23:2c:c0:da:e8:be:6e:6d:
                    4d:f1:24:91:01:43:7b:26:20:e8:d8:55:7d:ad:b4:
                    8c:ed:6d:c4:28:ab:fe:98:c7:8c:a4:99:6d:d3:8a:
                    b8:a5:c2:c7:16:c4:77:cb:fe:c6:17:b8:40:f2:d6:
                    91:37:c9:c3:a4:d1:7b:3f:f2:06:c9:4a:92:bd:21:
                    dc:1b:a6:00:f0:d2:24:28:15:c9:7f:ee:04:77:35:
                    c3:f2:f5:26:1d:72:2d:2f:4c:6b:4f:b7:93:ed:99:
                    93:71:5e:3b:c8:62:de:35:27:7c:3c:70:23:84:f0:
                    26:a0:98:01:60:18:0a:0a:a4:f1:29:7b:21:7c:f9:
                    17:ca:8b:cd:c7:cc:06:0c:cd:5c:c5:f1:d6:00:1d:
                    05:02:95:6f:d8:db:40:02:81:6b:52:70:b4:d1:73:
                    89:7b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:
                CE:A0:89:82:0A:DD:BD:17:81:DE:0C:D6:D8:E1:42:D8:48:C7:B7:01
```

```
            CE:A0:89:82:0A:DD:BD:17:81:DE:0C:D6:D8:E1:42:D8:48:C7:B7:01
        X509v3 Authority Key Identifier:
            keyid:BB:BC:C3:47:A5:E4:BC:A9:C6:C3:A4:72:0C:10:8D:A2:35:E1:C8:E8

        Authority Information Access:
            OCSP - URI:http://r10.o.lencr.org
            CA Issuers - URI:http://r10.i.lencr.org/

        X509v3 Subject Alternative Name:
            DNS:*.cgstauditranchi.gov.in
            DNS:*.com.bssranchi.in
            DNS:*.gov.in.bssranchi.in
            DNS:*.swwcreation.com
            DNS:cgstauditranchi.gov.in
            DNS:swwcreation.com
            DNS:www.cgstauditranchi.gov.in.bssranchi.in
            DNS:www.gstauditranchi.gov.in.bssranchi.in
            DNS:www.swwcreation.com.bssranchi.in
        X509v3 Certificate Policies:
            Policy: 2.23.140.1.2.1

        X509v3 CRL Distribution Points:

            Full Name:
              URI:http://r10.c.lencr.org/33.crl

        CT Precertificate Poison: critical
            NULL
Signature Algorithm: sha256WithRSAEncryption
     2b:38:82:29:c2:0a:38:e6:99:ab:33:54:fd:96:04:71:bc:10:
     0f:e6:ee:47:4a:0b:3b:76:8a:d5:f2:01:54:e0:02:e7:c6:be:
     9d:d9:cf:33:f5:4f:ce:9f:3d:a4:28:2b:58:fe:c0:50:28:75:
     e2:16:ab:15:b3:b2:2f:bf:75:47:97:b3:b0:d9:0b:5c:ca:0b:
     5b:e5:60:c0:46:db:cc:25:38:67:24:4b:6f:63:bf:ad:d9:1f:
     8a:48:78:ab:61:36:18:47:55:12:1a:e3:56:17:38:8a:7f:86:
     e1:88:2e:76:69:7b:6b:4b:9e:58:12:6d:b6:e3:da:01:05:3a:
     12:7c:a8:47:49:e9:e6:24:77:e8:71:a1:81:2c:64:f8:6d:31:
     b1:09:4f:41:47:8e:c6:60:41:01:d1:38:1f:67:c3:0d:77:92:
     ac:11:21:1e:48:1f:80:06:92:f6:d7:c0:bb:92:45:95:08:09:
     7d:30:6d:1e:8d:24:5a:eb:80:ee:3d:35:fb:0a:4f:35:02:f2:
     d3:3c:63:7c:c3:89:56:64:31:50:f2:a9:d2:03:d1:fb:82:1d:
     ff:08:6a:66:b5:82:8c:7c:59:e9:d0:8e:5f:b2:dc:f8:4a:3b:
     82:c9:8a:a7:b5:02:ea:ea:8c:93:99:26:d8:fb:db:9f:fb:d0:
     e2:4f:b9:bd
```


We can also see the hidden metadata

crt.sh | 18026020434

crt.sh/?id=18026020434&opt=nometadata

crt.sh Certificate Search

Criteria	ID = '18026020434'

crt.sh ID	18026020434
Certificate Fingerprints	SHA-256 DE0BDD3DAC3DF73B8770FAD426A8C64EE6DD85078721D4C9C052ED7D00481434 SHA-1 295CA60C5FB18A8484798A1343D241B006B46C7F

| ASN.1 | Certificate | Graph | Hierarchy | pv |

Show metadata

Run linters using pkimetal

Download Certificate: PEM

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            05:52:51:59:a6:15:37:51:78:59:1a:d5:af:a4:51:9f:a7:20
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 295814)
            commonName               = R10
            organizationName         = Let's Encrypt
            countryName              = US
        Validity (Expired)
            Not Before: Apr 23 21:39:59 2025 GMT
            Not After : Jul 22 21:39:58 2025 GMT
        Subject:
            commonName               = *.cgstauditranchi.gov.in
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:ad:4f:68:42:ae:1f:8f:14:a6:7e:32:53:33:34:
                    33:81:6f:01:c1:6a:64:b1:ec:9f:89:a7:dd:fa:79:
                    b6:f8:87:63:ca:05:3c:b2:fa:2f:79:cd:10:66:57:
                    3b:32:38:57:db:d1:30:18:d4:ff:6e:70:f9:99:d2:
                    ea:e6:a9:e7:7b:5f:b9:86:4c:33:1a:0e:c5:96:b6:
                    03:c1:42:c1:b9:65:fb:39:b6:9f:d2:4f:b6:d3:7c:
                    47:cd:49:42:4c:79:c3:23:2c:c0:da:e8:be:6e:6d:
```

5. Export/save info for documentation or follow-up

When Should We Use CRT.sh?

- During subdomain enumeration and asset discovery
- When investigating phishing or impersonation attempts
- For compliance validation and SSL cert auditing
- In passive OSINT gathering for bug bounty or red teaming

Who Should Use CRT.sh?

- Red teamers and OSINT analysts
- Penetration testers
- Security auditors
- Threat hunters

Advantages

- Free and public
- Reveals subdomains and certificate history
- Fast and easy-to-use
- Useful for stealthy recon

Flaws and Limitations

- No real-time alerts
- Does not resolve IPs or geo info
- Basic filtering UI
- No server context behind certs

Proof-of-Concept Report: FOFA (Fingerprint of All)

Tool Name

FOFA (Fingerprint of All)

Description

FOFA is a global cybersecurity search engine used to detect and analyze internet-exposed assets, SSL certificates, ports, technologies, and vulnerabilities.

Why use this tool?

It offers deep visibility into devices, services, and certificates online, helping identify exposures, misconfigurations, and threat infrastructure.

Key Characteristics

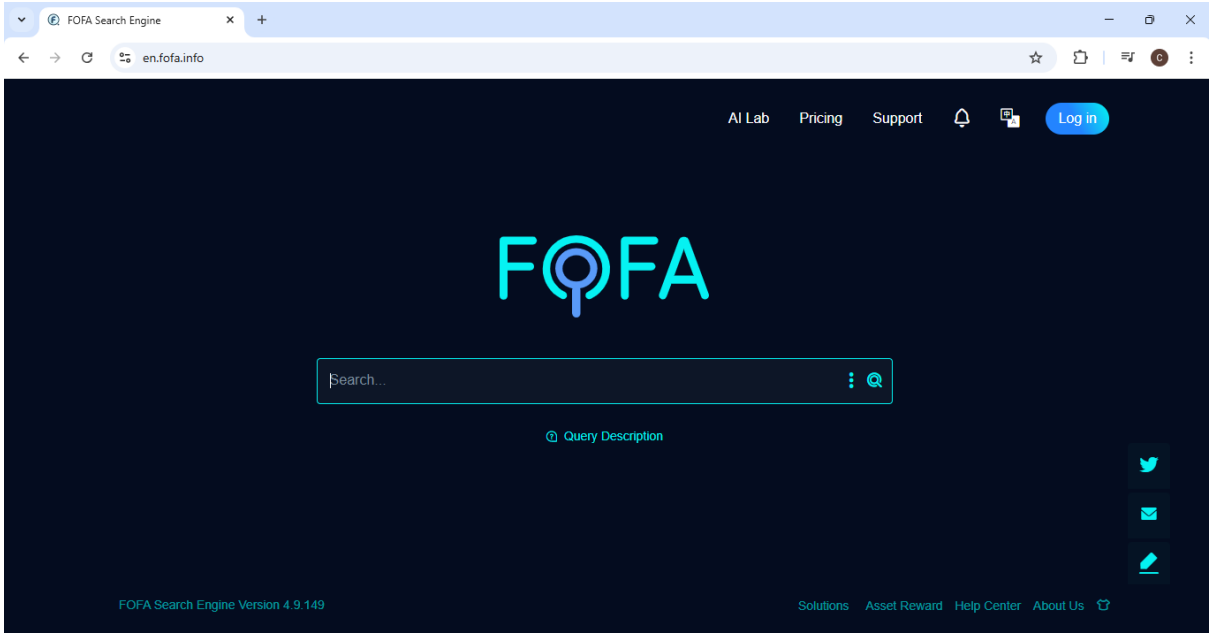
- Advanced search engine for exposed assets
- Filter by IP, domain, port, cert, title, etc.
- Search by banner, protocol, or fingerprint
- Includes screenshots and metadata
- API and UI support
- Covers Chinese + global web space

How FOFA Helps Cybersecurity Professionals

- Map internet-facing assets
- Detect vulnerabilities and leaks
- Track phishing or C2 infrastructure
- Cert and IP reconnaissance

How to Use FOFA

1. Visit https://fofa.info



2. Log in or register (free & paid tiers)
3. Use dorks like:
    - cert="target.com

Search results cert="uidai.gov.in"

en.fofa.info/result?qbase64=Y2VydD0idWlkYWkuZ292LmluIg%3D%3D

FOFA

cert="uidai.gov.in"

AI Lab Pricing Support

Favicon(1): Select all

all

15 results (6 unique IP) ,182 ms ,Keyword Search.

Nearly year results, click to view all results.

API

TOP FID

DFW6...	2
3IsaJ...	2
0OXZ...	1
QrW6...	1

TOP COUNTRIES/REGIONS

IN	15

164.100.211.234:443

443 tls

164.100.211.234

India / Delhi / Delhi

ASN: 4758

Organization: National Informa...

2025-07-24

Products

Data Certificate

d****t

FOFA

cert="uidai.gov.in"

AI Lab Pricing Support

TOP OPEN PORTS

443	15

TOP SERVERS

Apache/2.4.62 (Debian)	2
Apache	1

TOP PROTOCOLS

https	7
tls	2

TOP TITLES

403 Forbidden	2
Language Selection - Unique ...	2
Biochallenge - UIDAI | IIIT, Hy...	1
Not Found	1

https://103.57.226.101

443 https

103.57.226.101

India / Delhi / Delhi

ASN: 134029

Organization: Unique Identific...

2025-07-22

Banner

-1223... 73344...

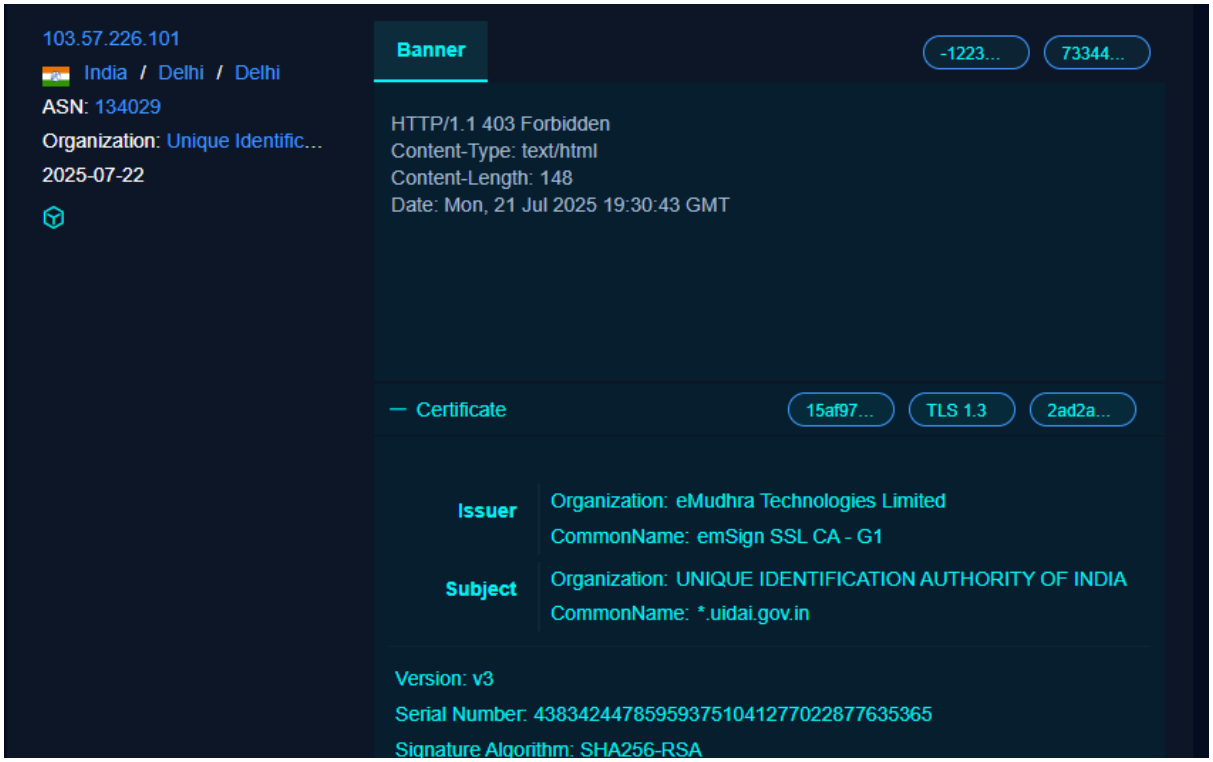
HTTP/1.1 403 Forbidden
Content-Type: text/html
Content-Length: 148
Date: Mon, 21 Jul 2025 19:30:43 GMT

Certificate

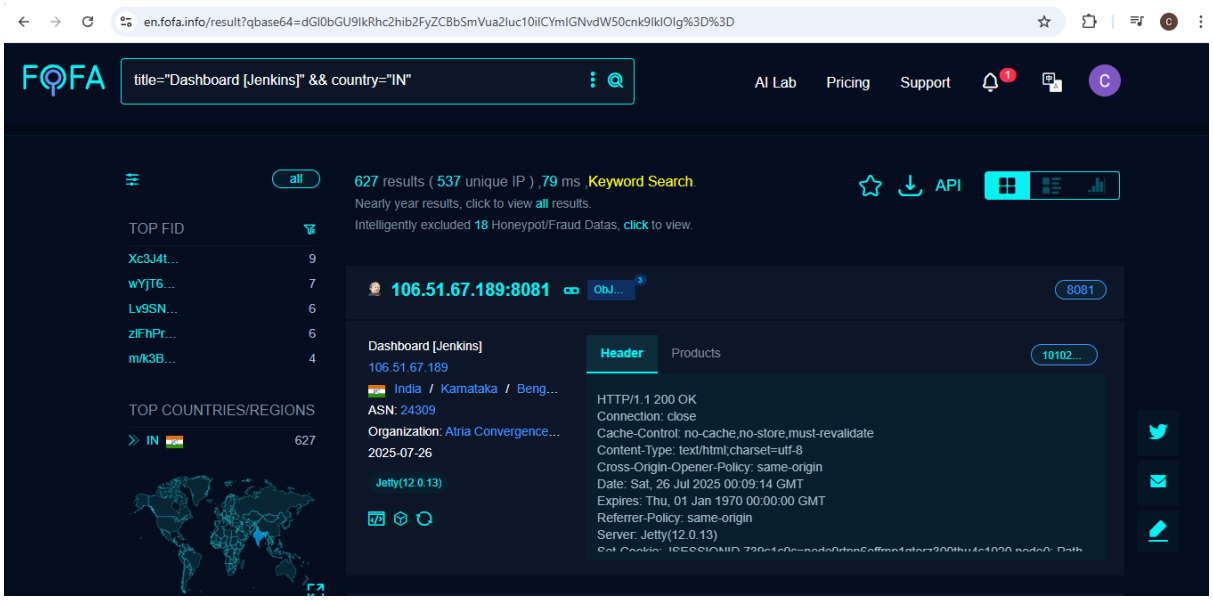
15af97... TLS 1.3 2ad2a...

Issuer
Organization: eMudhra Technologies Limited
CommonName: emSign SSL CA - G1

Subject
Organization: UNIQUE IDENTIFICATION AUTHORITY OF INDIA
CommonName: *.uidai.gov.in



- title="admin login"



4. Review search results, apply filters, and export data

When Should We Use FOFA?

- Red team reconnaissance
- Vulnerability or shadow IT detection

- Threat hunting operations
- Subdomain + cert + IP mapping

Who Should Use FOFA?

- Red teamers and threat hunters
- Bug bounty professionals
- SOC and cyber intelligence teams

Advantages

- Global scan visibility
- Real-time filtering & queries
- Cert and subdomain discovery
- Integrates with other intel tools

Flaws and Limitations

- Full access requires premium
- Default UI is in Chinese
- Can block frequent access/IPs
- Only covers exposed internet assets