# Experiment 05

**AIM:**

Using OSINT tools to gather tactical information via WHOIS lookup, domain registration details, owner's contact information, registration and expiration dates, archived content, reverse image search, EXIF data, source code analysis, TLD checks, mentions of the target, RSS feeds, SSL certificate analysis, robots/sitemap inspection, port scans, and reverse IP lookups.

---

**Theory**

Open-Source Intelligence (OSINT) is the process of collecting, analyzing, and utilizing publicly available information from online and offline open sources for investigative, security, and research purposes. In cybersecurity, OSINT enables the gathering of **tactical intelligence** about a target without breaching any legal boundaries.

One of the core tools in this process is **WHOIS lookup**, which reveals domain registration details such as:

- Registrar name
- Domain creation and expiry dates
- Name servers
- Owner's contact information (if not privacy-protected)

Another key resource is the **Wayback Machine**, which stores archived snapshots of websites, allowing investigators to observe historical changes, recover deleted content, or track ownership patterns.

**Reverse image search** (Google Images, TinEye) helps identify the origin, authenticity, and online presence of images from the target's website, while **EXIF metadata analysis** reveals hidden technical details embedded within images—such as GPS coordinates, camera details, and timestamps—if available.

Examining the **source code** of a website can reveal comments, email addresses, analytics codes, or even indicators of technologies and vulnerabilities in use. Similarly, **robots.txt** and **sitemap.xml** files may disclose hidden URLs, restricted sections, and update timelines.

**SSL certificate inspection** provides insight into encryption protocols, certificate issuers, and validity periods, which reflect the website's security posture. More advanced techniques such as **port scanning** and **reverse IP lookup** reveal active services and other domains hosted on the same server.

By combining these tools and methods, investigators can collect actionable, non-intrusive intelligence useful for **digital forensics, ethical hacking, and threat analysis**.

---

**Procedure**

**Step 1: Select a Target Website**

- Example: openai.com (You may choose any domain for analysis).

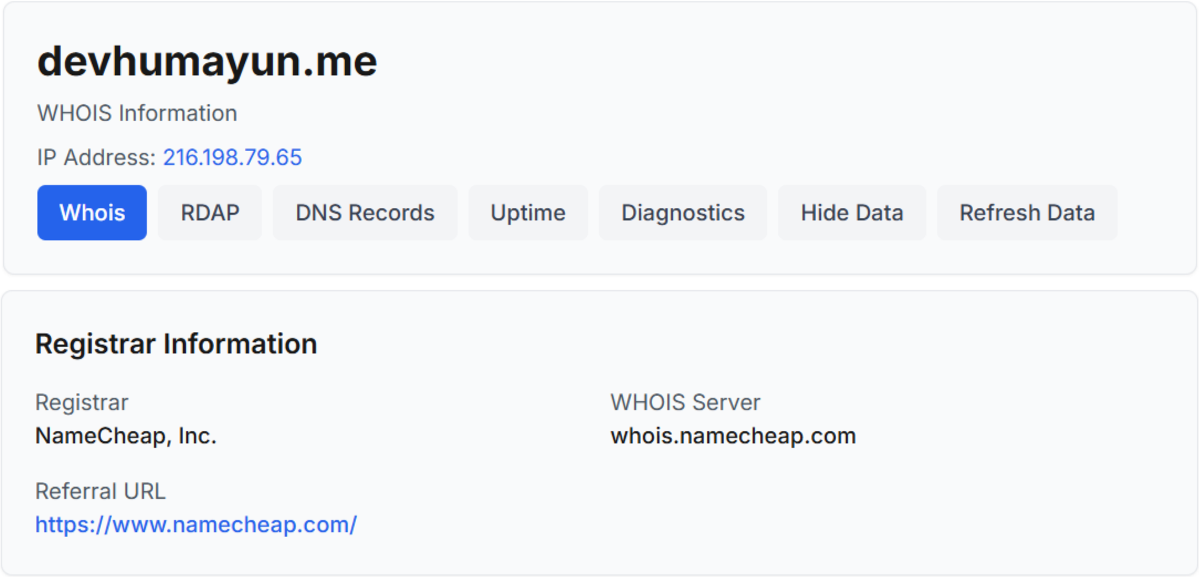
---

**Step 2: Perform WHOIS Lookup**
**Tools:**

- [DomainTools WHOIS]
- [Who.is]

**Steps:**

1. Enter the target domain in the tool.
2. Record:
    - Registrar name
    - Registration & expiry dates
    - Registrant contact (if visible)
    - Name servers



**devhumayun.me**

WHOIS Information

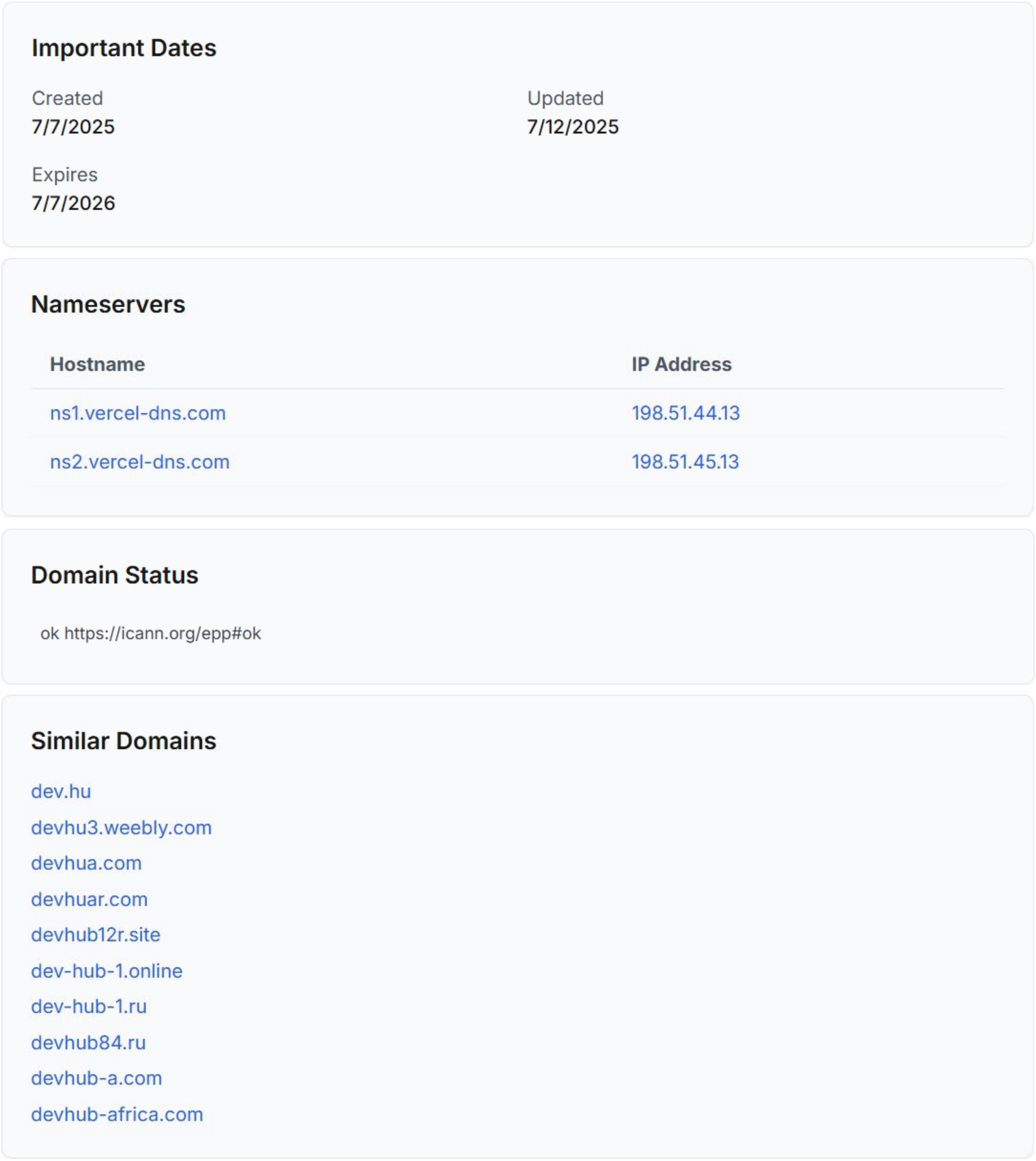
IP Address: 216.198.79.65

**Registrar Information**

Registrar
NameCheap, Inc.

WHOIS Server
whois.namecheap.com

Referral URL
https://www.namecheap.com/



### Important Dates

Created
7/7/2025

Updated
7/12/2025

Expires
7/7/2026

### Nameservers

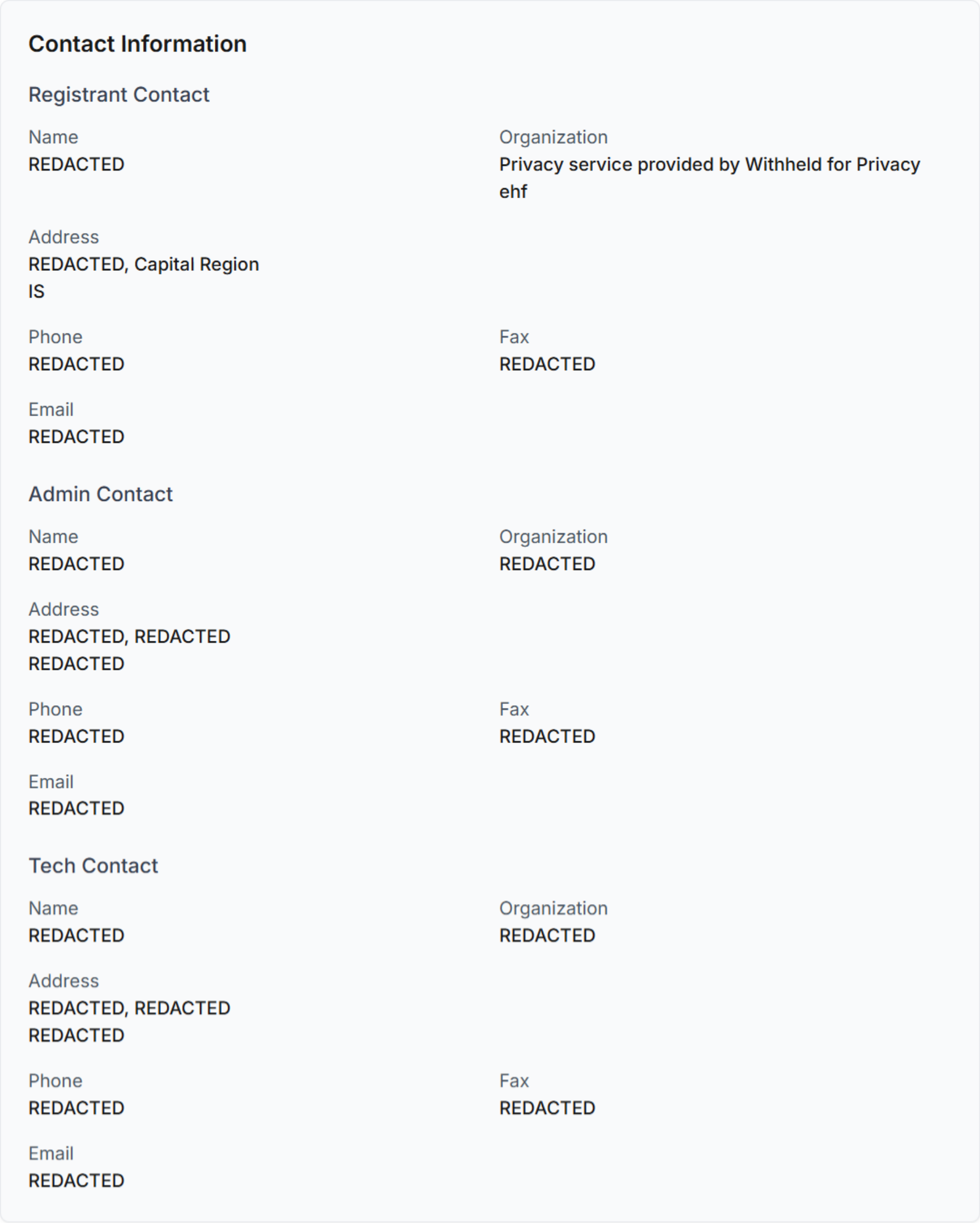
| Hostname | IP Address |
|---|---|
| ns1.vercel-dns.com | 198.51.44.13 |
| ns2.vercel-dns.com | 198.51.45.13 |

### Domain Status

ok https://icann.org/epp#ok

### Similar Domains

dev.hu
devhu3.weebly.com
devhua.com
devhuar.com
devhub12r.site
dev-hub-1.online
dev-hub-1.ru
devhub84.ru
devhub-a.com
devhub-africa.com



Contact Information

Registrant Contact

Name
REDACTED

Organization
Privacy service provided by Withheld for Privacy ehf

Address
REDACTED, Capital Region
IS

Phone
REDACTED

Fax
REDACTED

Email
REDACTED

Admin Contact

Name
REDACTED

Organization
REDACTED

Address
REDACTED, REDACTED
REDACTED

Phone
REDACTED

Fax
REDACTED

Email
REDACTED

Tech Contact

Name
REDACTED

Organization
REDACTED

Address
REDACTED, REDACTED
REDACTED

Phone
REDACTED

Fax
REDACTED

Email
REDACTED

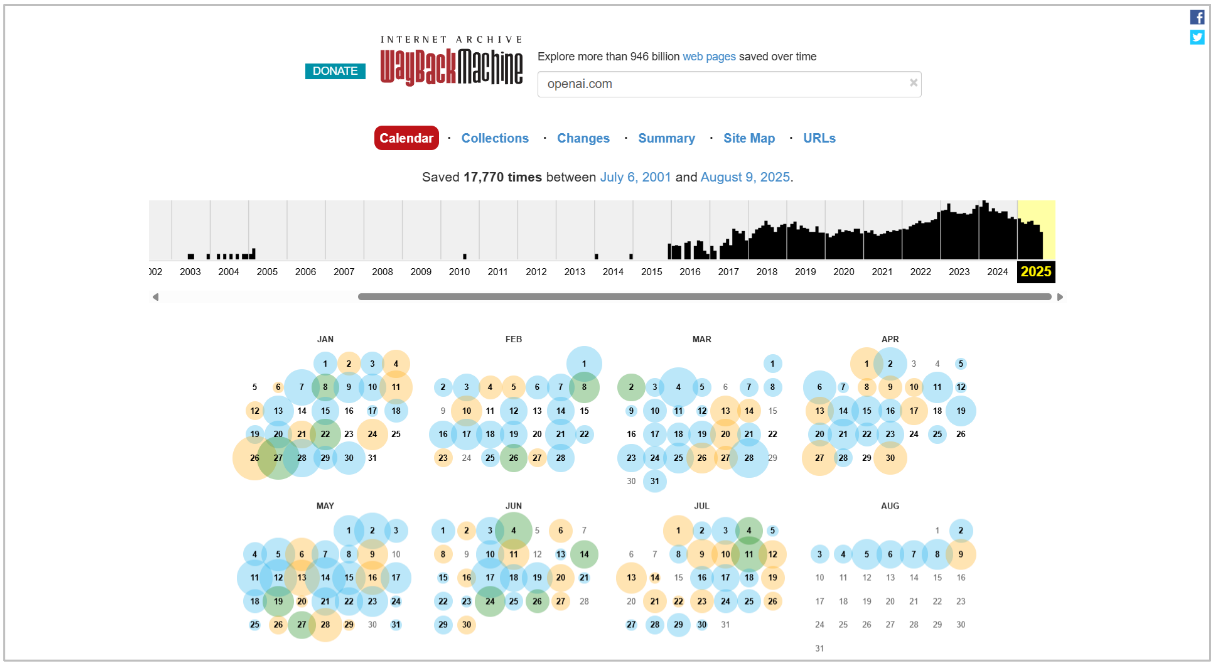
---

**Step 3: Explore Archived Versions with Wayback Machine**
**Tool:** web.archive.org

**Steps:**

1. Enter the domain name.
2. Browse archived snapshots over time.

3. Compare changes in design, content, and functionality.



INTERNET ARCHIVE WaybackMachine

DONATE

Explore more than 946 billion web pages saved over time

openai.com

Calendar · Collections · Changes · Summary · Site Map · URLs

Saved **17,770 times** between July 6, 2001 and August 9, 2025.

---

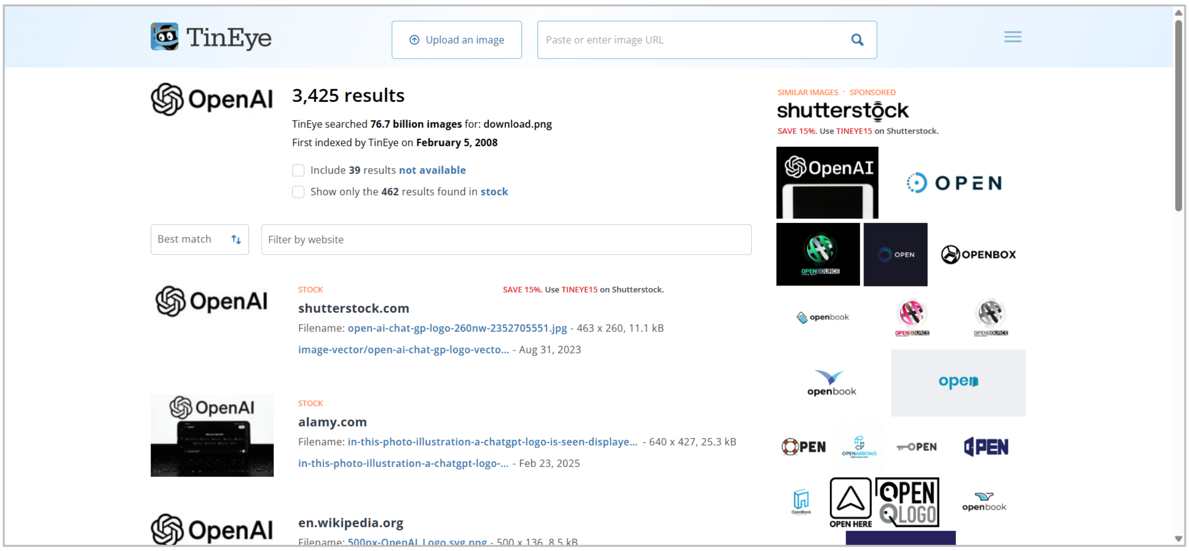
### Step 4: Conduct Reverse Image Search

**Tools:**

- Google Images
- TinEye

**Steps:**

1. Download an image from the target site (e.g., logo).
2. Upload to the search tool.
3. Identify duplicates, source origins, or unauthorized use.



OpenAI 3,425 results

TinEye searched **76.7 billion images** for: **download.png**

First indexed by TinEye on **February 5, 2008**

□ Include **39** results **not available**

□ Show only the **462** results found in **stock**

STOCK SAVE 15%. Use TINEYE15 on Shutterstock.

shutterstock.com

Filename: open-ai-chat-gp-logo-260nw-2352705551.jpg - 463 x 260, 11.1 kB

image-vector/open-ai-chat-gp-logo-vecto... - Aug 31, 2023

STOCK

alamy.com

Filename: in-this-photo-illustration-a-chatgpt-logo-is-seen-displaye... - 640 x 427, 25.3 kB

in-this-photo-illustration-a-chatgpt-logo-... - Feb 23, 2025

en.wikipedia.org

Filename: 500px-OpenAI_Logo.svg.png - 500 x 136, 8.5 kB

SIMILAR IMAGES · SPONSORED

shutterstock

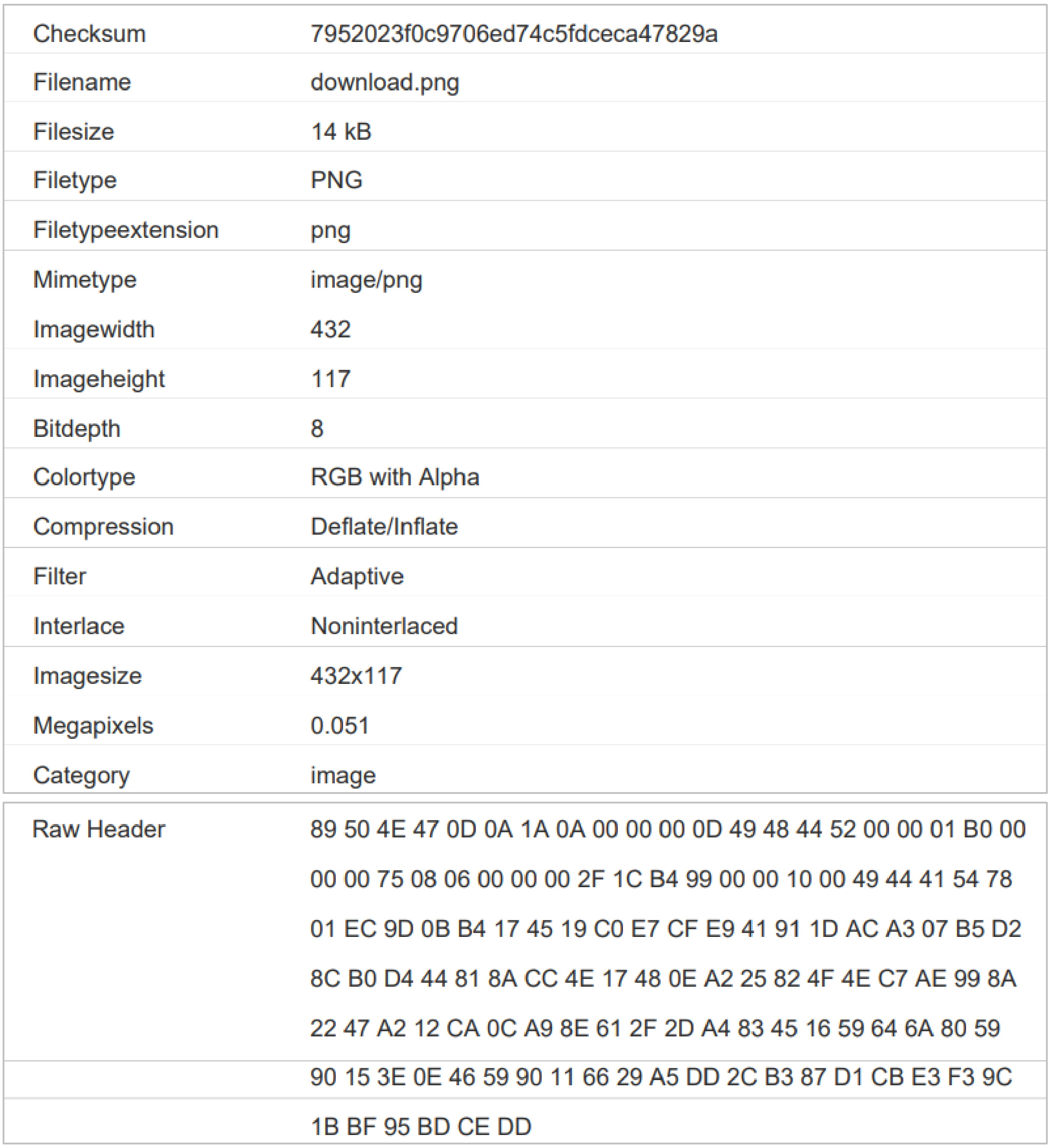
SAVE 15%. Use TINEYE15 on Shutterstock.

**Step 5: Extract EXIF Metadata**
**Tools:**

- Metadata2Go

**Steps:**

1. Download an image from the site.
2. Upload it to the EXIF tool.
3. Check for GPS location, device details, and timestamps.



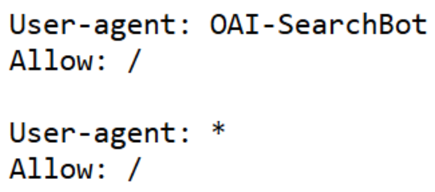
| | |
|---|---|
| Checksum | 7952023f0c9706ed74c5fdceca47829a |
| Filename | download.png |
| Filesize | 14 kB |
| Filetype | PNG |
| Filetypeextension | png |
| Mimetype | image/png |
| Imagewidth | 432 |
| Imageheight | 117 |
| Bitdepth | 8 |
| Colortype | RGB with Alpha |
| Compression | Deflate/Inflate |
| Filter | Adaptive |
| Interlace | Noninterlaced |
| Imagesize | 432x117 |
| Megapixels | 0.051 |
| Category | image |
| Raw Header | 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 00 00 01 B0 00<br>00 00 75 08 06 00 00 00 2F 1C B4 99 00 00 10 00 49 44 41 54 78<br>01 EC 9D 0B B4 17 45 19 C0 E7 CF E9 41 91 1D AC A3 07 B5 D2<br>8C B0 D4 44 81 8A CC 4E 17 48 0E A2 25 82 4F 4E C7 AE 99 8A<br>22 47 A2 12 CA 0C A9 8E 61 2F 2D A4 83 45 16 59 64 6A 80 59 |
| | 90 15 3E 0E 46 59 90 11 66 29 A5 DD 2C B3 87 D1 CB E3 F3 9C |
| | 1B BF 95 BD CE DD |

**Step 6: Analyze Website Source Code**
**Steps:**

1. Right-click on the webpage → “View Page Source.”
2. Look for:
   - HTML comments
   - Embedded scripts and analytics
   - Email addresses
   - Hidden form fields

**Step 7: Review Robots.txt & Sitemap.xml**
**Steps:**

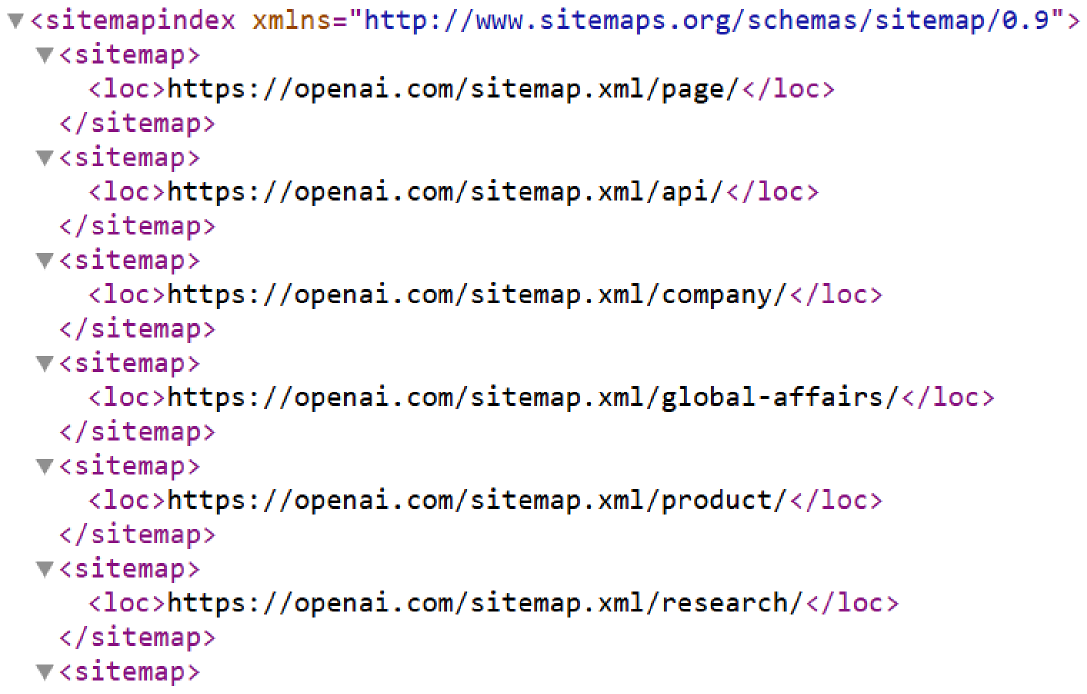
1. Open devhumayun.me/robots.txt to find restricted areas.



```
User-agent: OAI-SearchBot
Allow: /

User-agent: *
Allow: /
```

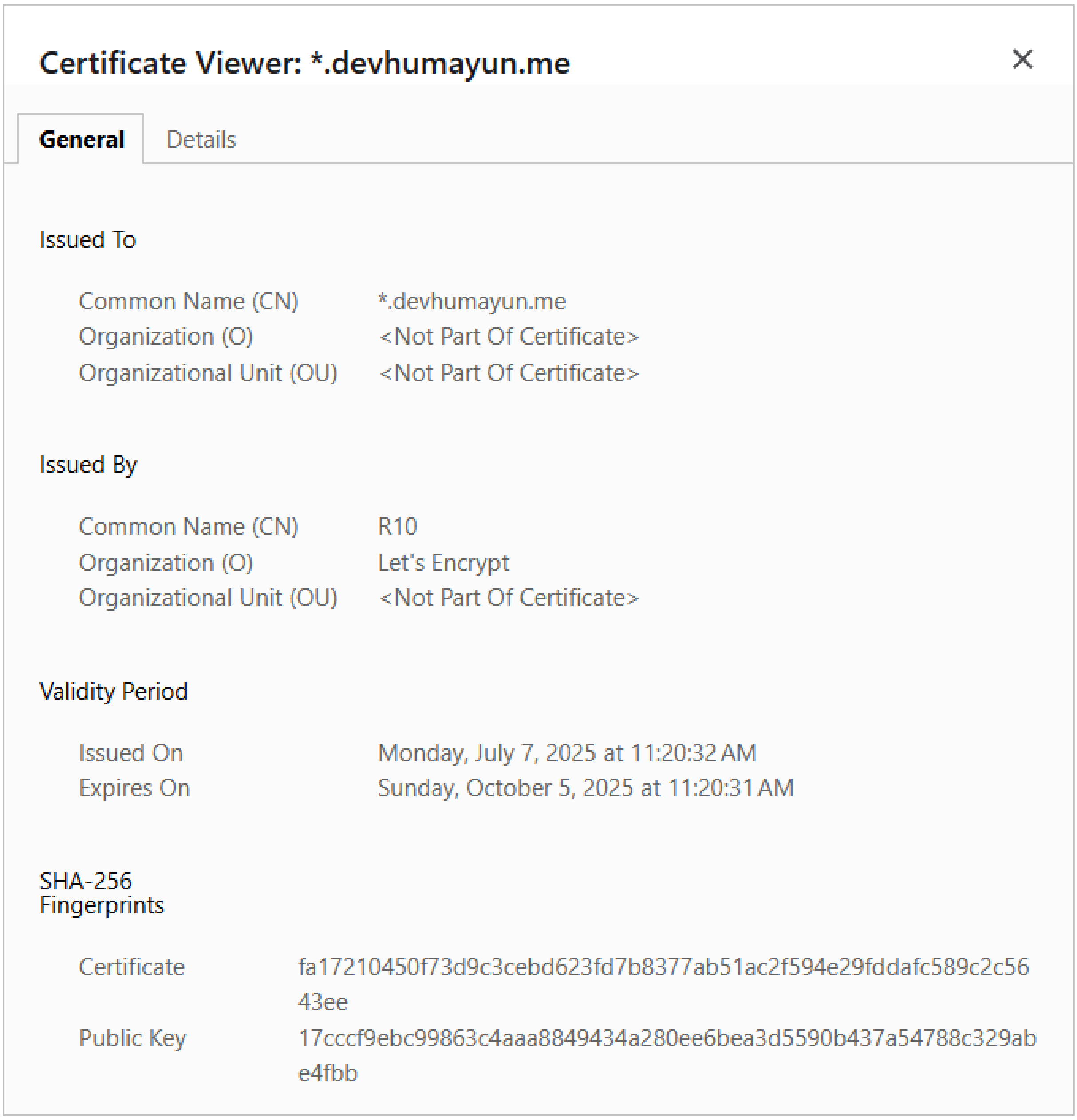
2. Open devhumayun.me /sitemap.xml to view page URLs and last updated dates.



```
▼<sitemapindex xmlns="http://www.sitemaps.org/schemas/sitemap/0.9">
  ▼<sitemap>
     <loc>https://openai.com/sitemap.xml/page/</loc>
   </sitemap>
  ▼<sitemap>
     <loc>https://openai.com/sitemap.xml/api/</loc>
   </sitemap>
  ▼<sitemap>
     <loc>https://openai.com/sitemap.xml/company/</loc>
   </sitemap>
  ▼<sitemap>
     <loc>https://openai.com/sitemap.xml/global-affairs/</loc>
   </sitemap>
  ▼<sitemap>
     <loc>https://openai.com/sitemap.xml/product/</loc>
   </sitemap>
  ▼<sitemap>
     <loc>https://openai.com/sitemap.xml/research/</loc>
   </sitemap>
  ▼<sitemap>
```

**Step 8: Inspect SSL Certificate**
**Steps:**

1. Click the padlock icon in the browser.
2. Check:
   - Certificate issuer
   - Validity dates
   - Encryption details



## Certificate Viewer: *.devhumayun.me

Issued To

| | |
|---|---|
| Common Name (CN) | *.devhumayun.me |
| Organization (O) | <Not Part Of Certificate> |
| Organizational Unit (OU) | <Not Part Of Certificate> |

Issued By

| | |
|---|---|
| Common Name (CN) | R10 |
| Organization (O) | Let's Encrypt |
| Organizational Unit (OU) | <Not Part Of Certificate> |

Validity Period

| | |
|---|---|
| Issued On | Monday, July 7, 2025 at 11:20:32 AM |
| Expires On | Sunday, October 5, 2025 at 11:20:31 AM |

SHA-256 Fingerprints

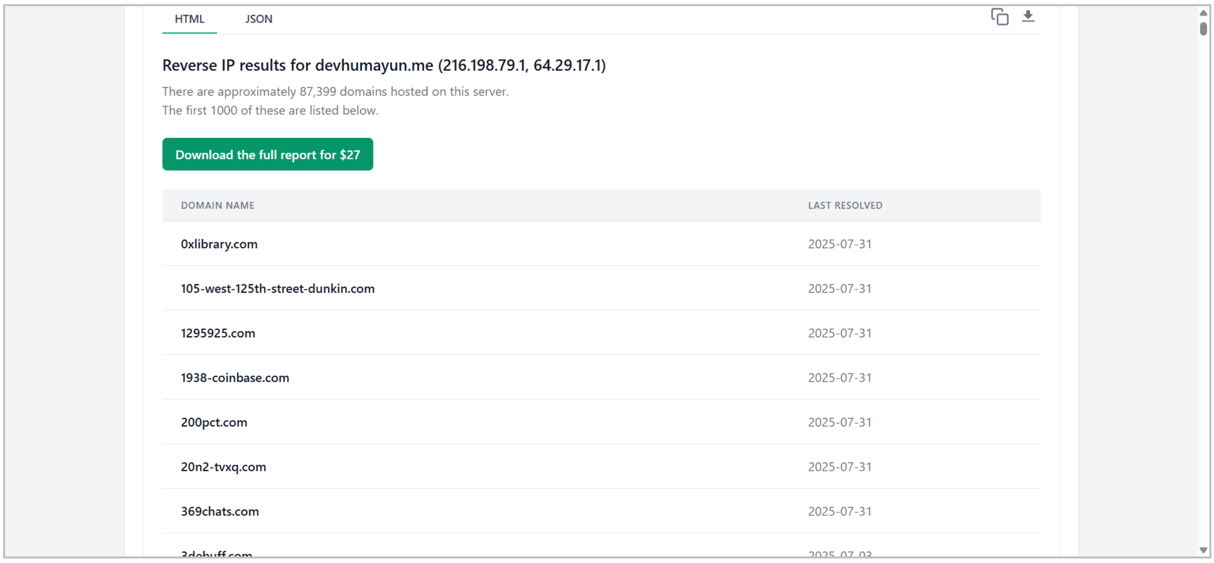
| | |
|---|---|
| Certificate | fa17210450f73d9c3cebd623fd7b8377ab51ac2f594e29fddafc589c2c5643ee |
| Public Key | 17cccf9ebc99863c4aaa8849434a280ee6bea3d5590b437a54788c329abe4fbb |

### Step 9: Perform Reverse IP Lookup

**Tool:** viewdns.info/reverseip

**Steps:**

1. Enter the domain or IP.
2. Identify other domains hosted on the same server.



Reverse IP results for devhumayun.me (216.198.79.1, 64.29.17.1)

There are approximately 87,399 domains hosted on this server.
The first 1000 of these are listed below.

| DOMAIN NAME | LAST RESOLVED |
|---|---|
| 0xlibrary.com | 2025-07-31 |
| 105-west-125th-street-dunkin.com | 2025-07-31 |
| 1295925.com | 2025-07-31 |
| 1938-coinbase.com | 2025-07-31 |
| 200pct.com | 2025-07-31 |
| 20n2-tvxq.com | 2025-07-31 |
| 369chats.com | 2025-07-31 |
| 3dobuff.com | 2025-07-03 |

---

### Conclusion

In this experiment, we gathered tactical intelligence on a target using a range of OSINT tools and techniques, including WHOIS lookups, archive analysis, image tracing, metadata extraction, source code inspection, SSL analysis, and reverse IP lookups. This exercise demonstrated how open-source data can be leveraged for **cybersecurity assessments, threat detection, and forensic investigations** while remaining completely within legal boundaries.