

## PRACTICAL: 3

### AIM:

Footprinting is the process of accumulating data regarding a specific network environment, usually to find ways to intrude into it. It can reveal system vulnerabilities and improve the ease with which they can be exploited. Footprinting is also known as reconnaissance. Study a practical approach to implementing Footprinting: Gathering Target Information using the OSINT Framework.

### THEORY:

OSINT framework focused on gathering information from free tools or resources. The intention is to help people find free OSINT resources. Some of the sites included might require registration or offer more data for \$\$\$, but you should be able to get at least a portion of the available information for no cost.

The five tools we will use in this exercise are:

1. WhatsMyName
2. Web Archive (Wayback Machine)
3. URLScan.io
4. DNSDumpster
5. OpenCorporates

### 1. WhatsMyName: Gathering DNS and Subdomain Information

**Overview:** WhatsMyName is an OSINT tool designed to perform DNS lookups and provide information about domain names. It helps identify various domain records associated with a target, including subdomains, IP addresses, and mail servers.

#### Steps:

- Go to the **WhatsMyName** website.
- Enter the domain name (e.g., "example.com") of the target you wish to investigate.
- The tool will return DNS records, which may include:
  - **A Records:** IP addresses associated with the domain.
  - **MX Records:** Mail servers linked to the domain.
  - **Subdomains:** Any additional domains or subdomains tied to the target.
  - **Nameservers:** Information about the authoritative nameservers for the domain.

This information helps us build a map of the target's domain infrastructure. It can reveal other systems or services the target might be running or any exposed services like mail servers or web applications.

## 2. Web Archive (Wayback Machine): Exploring Historical Web Data

**Overview:** The Wayback Machine, part of the Internet Archive, allows you to access historical versions of websites. It provides snapshots of websites taken at various points in time, enabling you to uncover potentially exposed information that has since been removed or changed.

### Steps:

- Visit the **Wayback Machine** at [archive.org/web](https://archive.org/web).
- Enter the target's URL (e.g., "example.com") and press "Browse History."
- You will be shown a calendar of snapshots taken by the Wayback Machine, which you can explore by clicking on different dates.

Reviewing past versions of the target's website might reveal old content that could have been inadvertently exposed, such as outdated documents, forms, or login pages.

This can help you identify misconfigurations or legacy systems that have since been updated or removed from the live site.

## 3. URLScan.io: Scanning and Analyzing Web Pages

**Overview:** URLScan.io is a security analysis tool that scans websites and provides detailed reports about how a site behaves. It highlights external domains, embedded JavaScript, network activities, and potential security issues that might not be immediately visible from a standard web visit.

### Steps:

- Go to **URLScan.io**.
- Enter the target URL (e.g., "example.com") in the search bar.
- URLScan.io will scan the website and return a report detailing:
  - External domains the site is connected to (e.g., third-party services, trackers).
  - Embedded JavaScript files and other resources.
  - Security headers and potential vulnerabilities.

This tool helps identify connections to external servers or suspicious domains that the target website might be communicating with.

The scan results can reveal potential security risks, such as unprotected scripts or malicious activity linked to the domain.

#### 4. DNSDumpster: Comprehensive DNS and Network Mapping

**Overview:** DNSDumpster is a free tool that maps out DNS records for a given domain. It can provide insights into a target's DNS infrastructure, uncovering subdomains, associated IP addresses, and DNS record details that might help in understanding the target's network architecture.

##### Steps:

- Visit **DNSDumpster.com**.
- Enter the target domain name (e.g., "example.com") in the search bar and click "Search."
- The tool will display:
  - **Subdomains:** A list of subdomains linked to the target domain.
  - **DNS Records:** Information such as A, MX, and CNAME records.
  - **IP Addresses:** The range of IP addresses associated with the target's services.
  - **Geolocation Information:** The physical locations of the associated servers.

Use the subdomain and IP information to uncover additional services or infrastructure related to the target.

Mapping out DNS records helps you identify vulnerable or exposed systems, such as mail servers, that could be potential entry points.

#### 5. OpenCorporates: Investigating Corporate Data

**Overview:** OpenCorporates is a database that aggregates public company registration data from jurisdictions around the world. It provides insights into the legal and business structure of organizations, which can be invaluable for foot printing a target company.

##### Steps:

- Go to **OpenCorporates** at [opencorporates.com](https://opencorporates.com).
- Enter the target company name (e.g., "Example Corp.") or its business registration number.
- OpenCorporates will return:
  - **Corporate Registration Information:** Data about the company's registration, including jurisdiction and date of incorporation.
  - **Corporate Structure:** Information about subsidiaries, parent companies, and related entities.

- **Directors and Key Personnel:** Publicly available data about the company’s executives and board members.

This tool helps us to understand the organizational structure of the target, revealing potential subsidiaries, associated businesses, or directors who may have connections to other vulnerable assets.

The company’s legal records could also provide insights into its history, legal standing, and potential financial issues, all of which can be valuable when assessing security risks.

**CODE:**

N/A

**OUTPUT:**

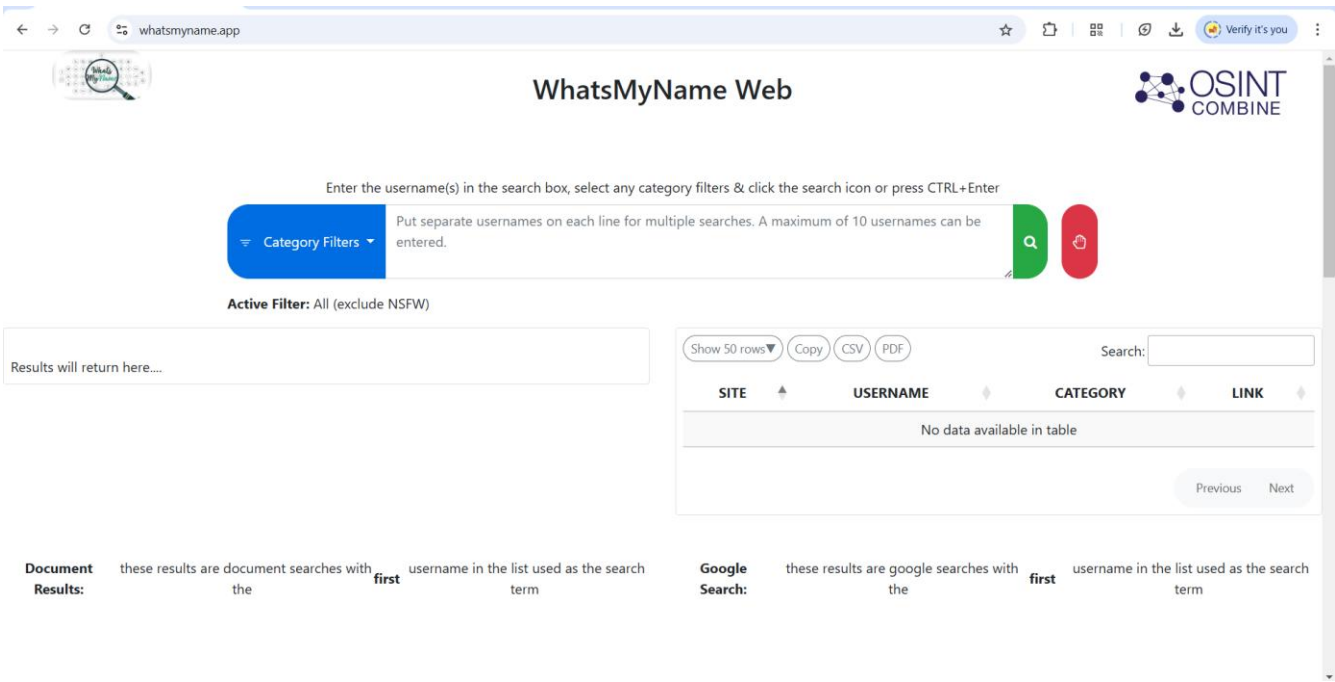


Figure 1: OSINT whatsMyName Web tool

Enter the username(s) in the search box, select any category filters & click the search icon or press CTRL+Enter

Category Filters

Active Filter: All (exclude NSFW)

Found: 4 Processed: 625 / 625

Show Found Show False Positives Show Not Found Show All Open All Links

GitHub Username: trushang28 Category: coding Account Found

giters Username: trushang28 Category: coding Account Found

Internet Archive Username: trushang28 Category: misc Account Found

Steemit Username: trushang28 Category: social Account Found

Filter by Username: trushang28

Show 50 rows Copy CSV PDF Search:

SITE	USERNAME	CATEGORY	LINK
giters	trushang28	coding	<a href="https://giters.com/trushang28">https://giters.com/trushang28</a>
GitHub	trushang28	coding	<a href="https://github.com/trushang28">https://github.com/trushang28</a>
Internet Archive..	trushang28	misc	<a href="https://archive.org/search.php?query=trushang28">https://archive.org/search.php?query=trushang28</a>
Steemit	trushang28	social	<a href="https://steemit.com/@trushang28">https://steemit.com/@trushang28</a>

Figure 2: We provide our username it will check 625 site and found 4 as this username

ONE DAY LEFT: The year is almost over—help us meet our 2024 goal!

Can You Chip In?

Please don't scroll past this—the Wayback Machine is fighting for universal access to quality information. The Internet Archive, which runs this project, relies on online donations averaging \$15.58 to help us keep the record straight. We'd be deeply grateful if you'd join the one in a thousand users that support us financially.

We understand that not everyone can donate right now, but if you can afford to contribute this Tuesday, we promise it will be put to good use. Our resources are crucial for knowledge lovers everywhere—so if you find all these bits and bytes useful, please pitch in.

Choose an amount (USD)

\$5 \$15.58

\$50 Custom: \$

☐ I'll generously add \$0.80 to cover fees.

☐ Make this monthly

Continue Remind Me

INTERNET ARCHIVE WEB TEXTS VIDEO AUDIO SOFTWARE IMAGES SIGN UP | LOG IN UPLOAD Search

ABOUT BLOG PROJECTS HELP DONATE CONTACT JOBS VOLUNTEER PEOPLE

INTERNET ARCHIVE Wayback Machine

DONATE Explore more than 916 billion web pages saved over time

Enter a URL or words related to a site's home page

Tools Subscription Service Collection Search Save Page Now

<https://web.archive.org/web/20131001152630/https://www.spiegel.de/>

Figure 3: Second tools are web archive

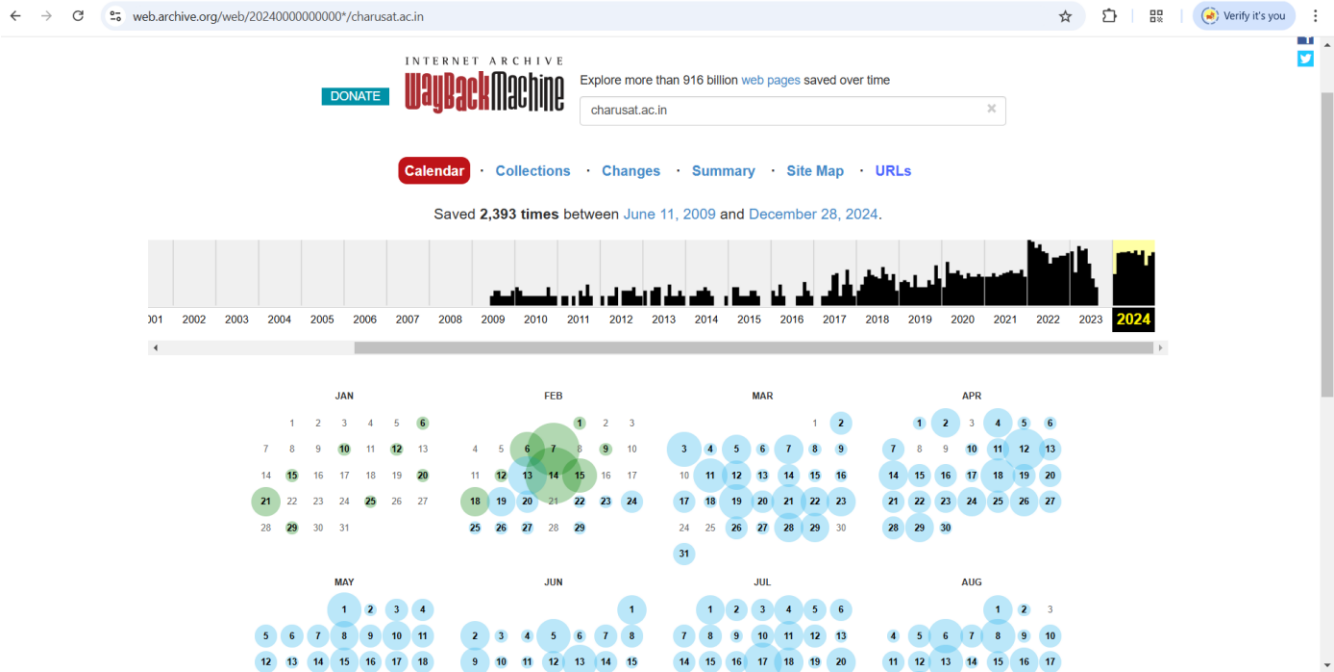


Figure 4: This is change in website month wise

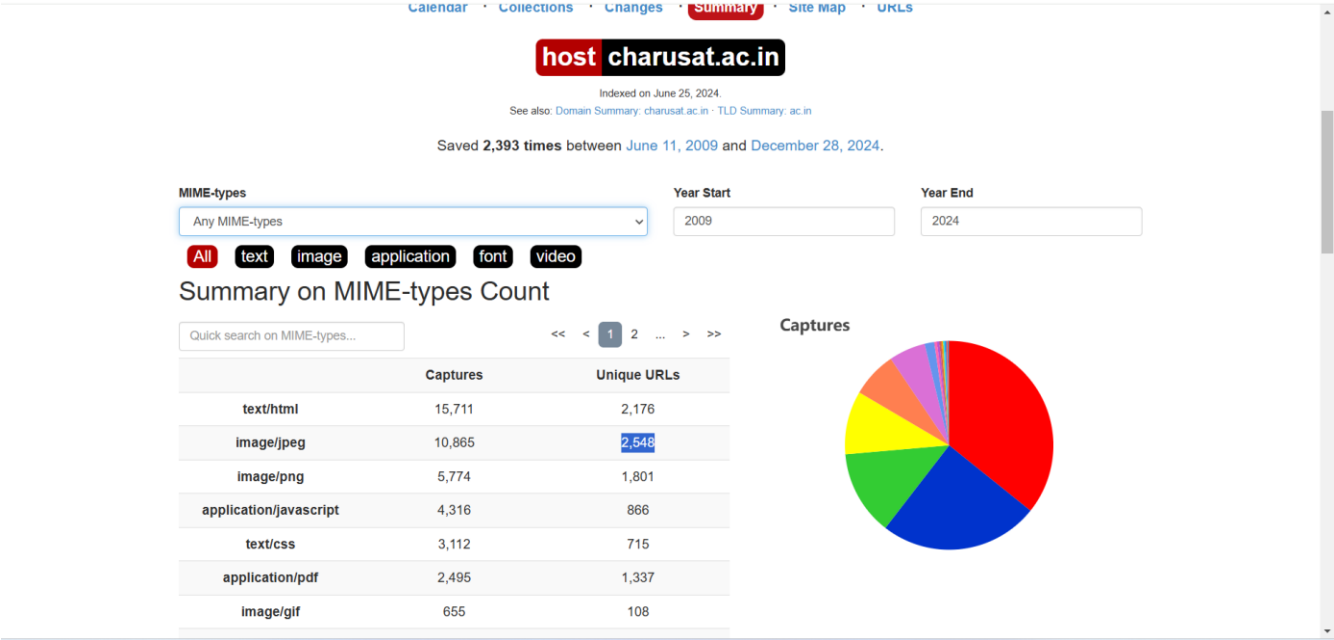


Figure 5: This is summary of charusat.ac.in

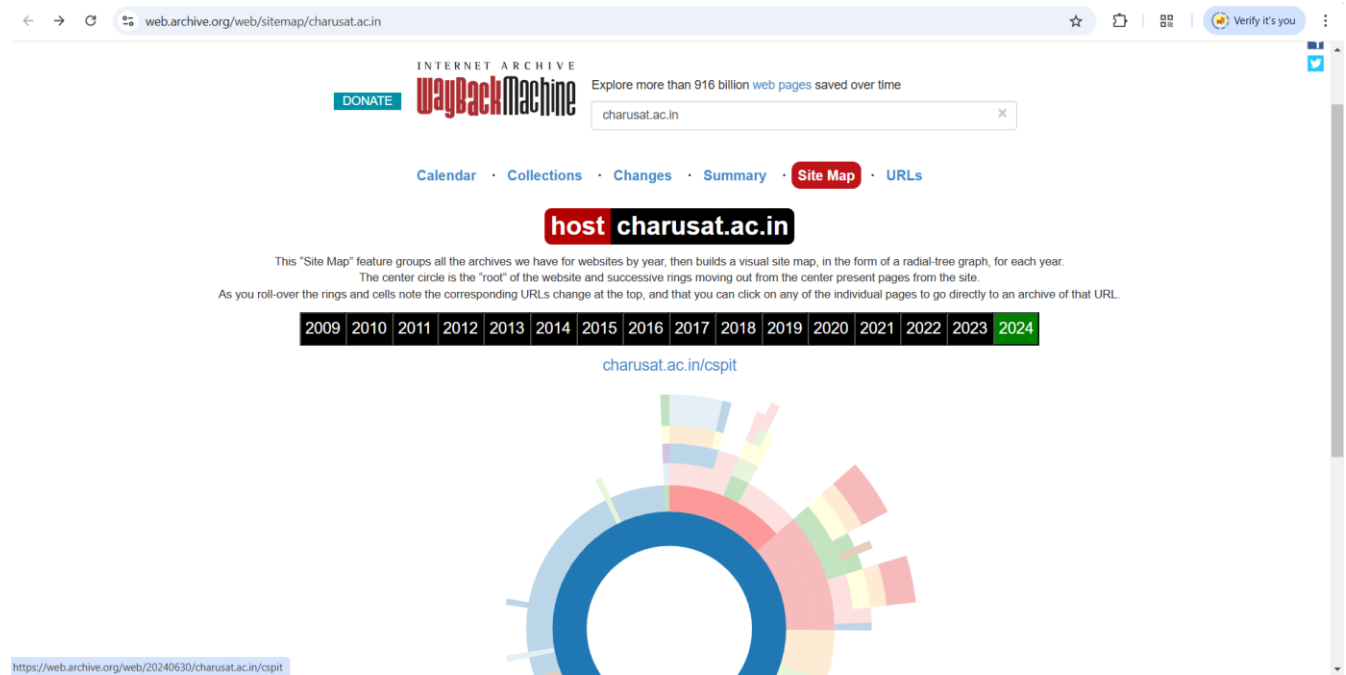


Figure 6: This is site map for charusat.ac.in of year 2024

Filter results by URL or MIME Type (i.e. ".txt")

URL ↑	MIME Type	From	To	Captures	Duplicates	Uniques
http://admissions@charusat.ac.in/?trk=public_post_main-feed-card-text	unk	Apr 11, 2023	Apr 11, 2023	2	0	2
http://charusat.ac.in/	text/html	Mar 9, 2016	Mar 9, 2016	1	0	1
http://charusat.ac.in/CharUSATUI/ http://academyoracle.com/	warc/revisit	Apr 3, 2014	Apr 18, 2015	3	2	1
http://charusat.ac.in/CharUSATUI/ http://cisco.netacad.net	warc/revisit	Apr 3, 2014	Apr 18, 2015	3	2	1
http://charusat.ac.in/CharUSATUI/CaptchaImage.axd?guid=1110ecda-497c-4103-9380-eb39f4bb46db	image/jpeg	Oct 27, 2010	Oct 27, 2010	1	0	1
http://charusat.ac.in/CharUSATUI/CaptchaImage.axd?guid=21a990b4-fdb4-4bfc-ac81-72cb65a9a617	image/jpeg	Nov 21, 2010	Nov 21, 2010	1	0	1
http://charusat.ac.in/CharUSATUI/CaptchaImage.axd?guid=6be65ee3-18ca-4641-9915-ac23636e23c	image/jpeg	Oct 20, 2010	Oct 20, 2010	1	0	1
http://charusat.ac.in/CharUSATUI/CaptchaImage.axd?guid=83646a20-ed29-4ceb-bf0c-6953b8d33819	image/jpeg	Dec 14, 2010	Dec 14, 2010	1	0	1
http://charusat.ac.in/CharUSATUI/CaptchaImage.axd?guid=eea98451-bf2f-46f1-ae59-972e911c1a90	image/jpeg	Sep 25, 2010	Sep 25, 2010	1	0	1
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=7?((*)?)?((*)?)	text/html	Sep 25, 2010	Oct 8, 2010	2	0	2
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=10&name=Institutes and Programmes	text/html	Sep 25, 2010	Aug 2, 2014	8	0	8
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=109	text/html	Aug 1, 2014	Aug 1, 2014	1	0	1
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=11&name=Institutes and Programmes	text/html	Sep 25, 2010	Apr 18, 2015	8	0	8
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=110	text/html	Aug 1, 2014	Aug 1, 2014	1	0	1
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=12	text/html	Sep 25, 2010	Apr 17, 2015	11	0	11
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=13	text/html	Sep 25, 2010	Apr 17, 2015	11	0	11
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=15	text/html	Sep 25, 2010	Apr 17, 2015	12	0	12
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=15&name=Life @ Campus	text/html	Sep 25, 2010	Apr 18, 2015	10	0	10
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=16	text/html	Sep 25, 2010	Apr 16, 2015	12	0	12
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=16&name=Life @ Campus	text/html	Sep 25, 2010	Apr 18, 2015	10	0	10
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=17	text/html	Sep 25, 2010	Apr 16, 2015	12	0	12
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=17&name=Life @ Campus	text/html	Sep 25, 2010	Apr 18, 2015	9	0	9

Figure 7: This are URL where charusat.ac.in is used as prefix

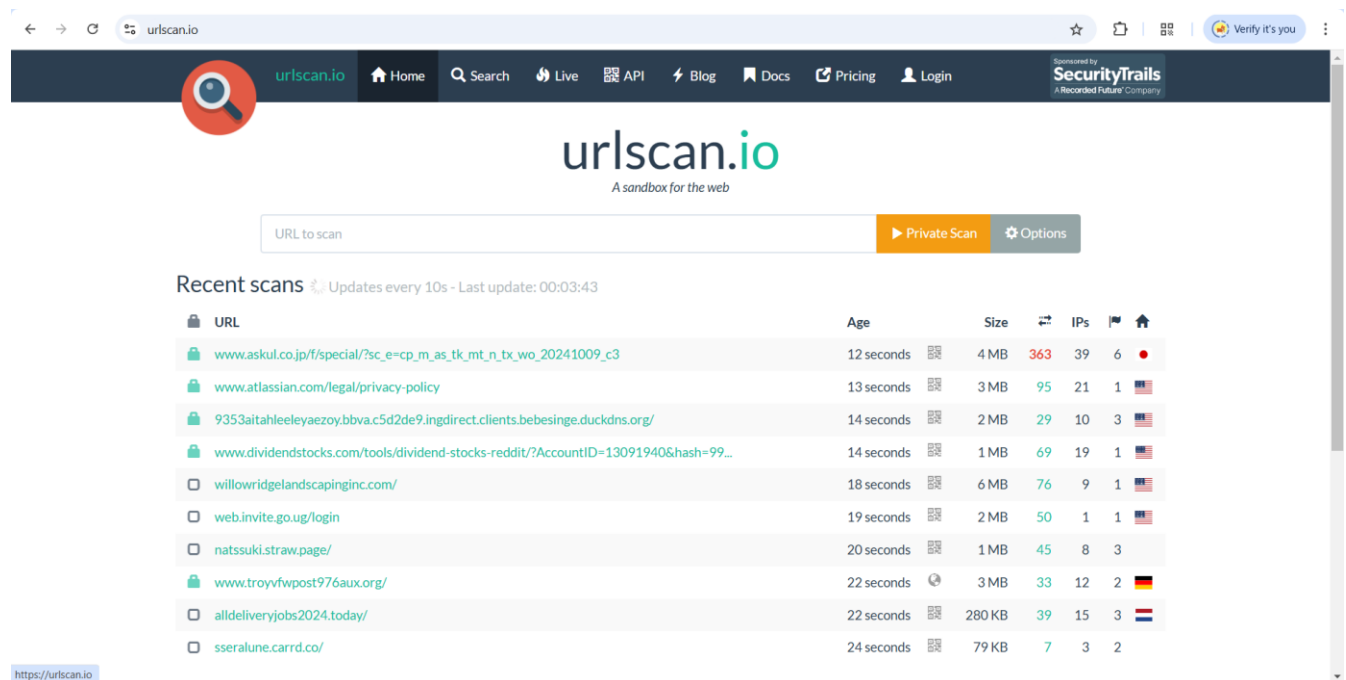


Figure 8: Third tool are urlscan.io

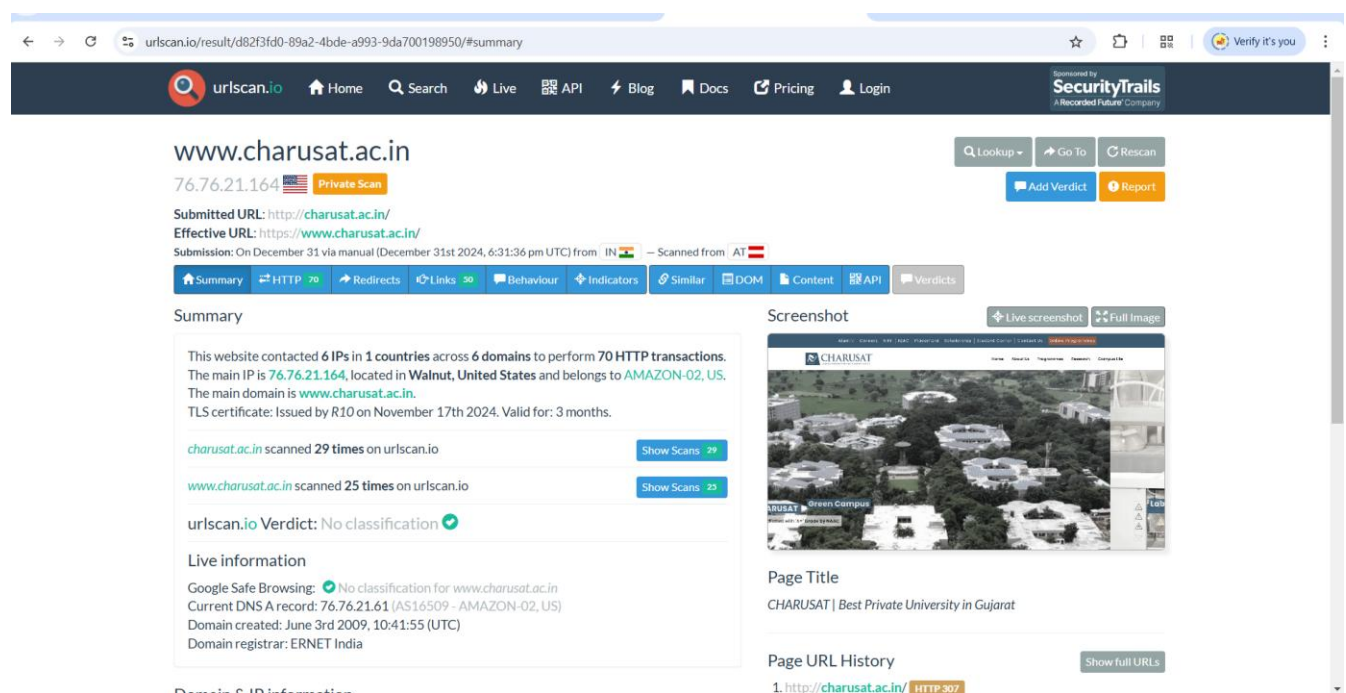


Figure 9: We scan charusat.ac.in privately and we scan charusat.ac.in 25 times



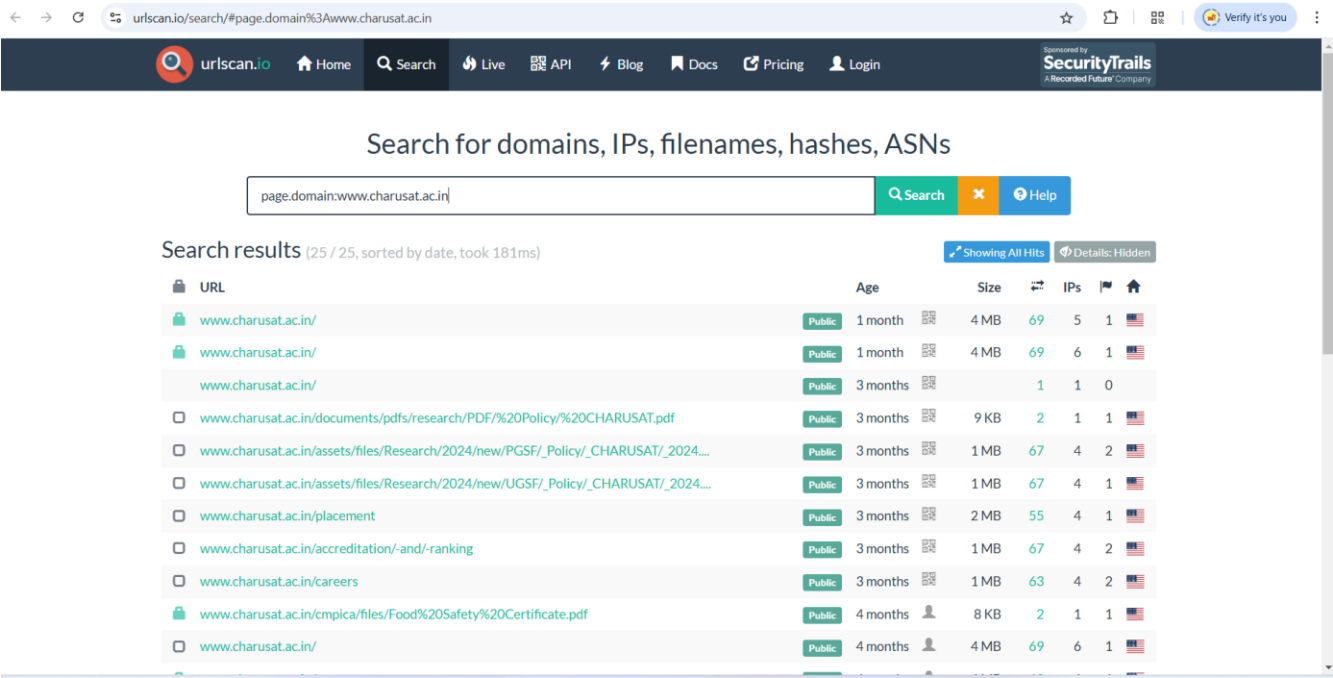


Figure 10: We can see which sub domain URL scan happened

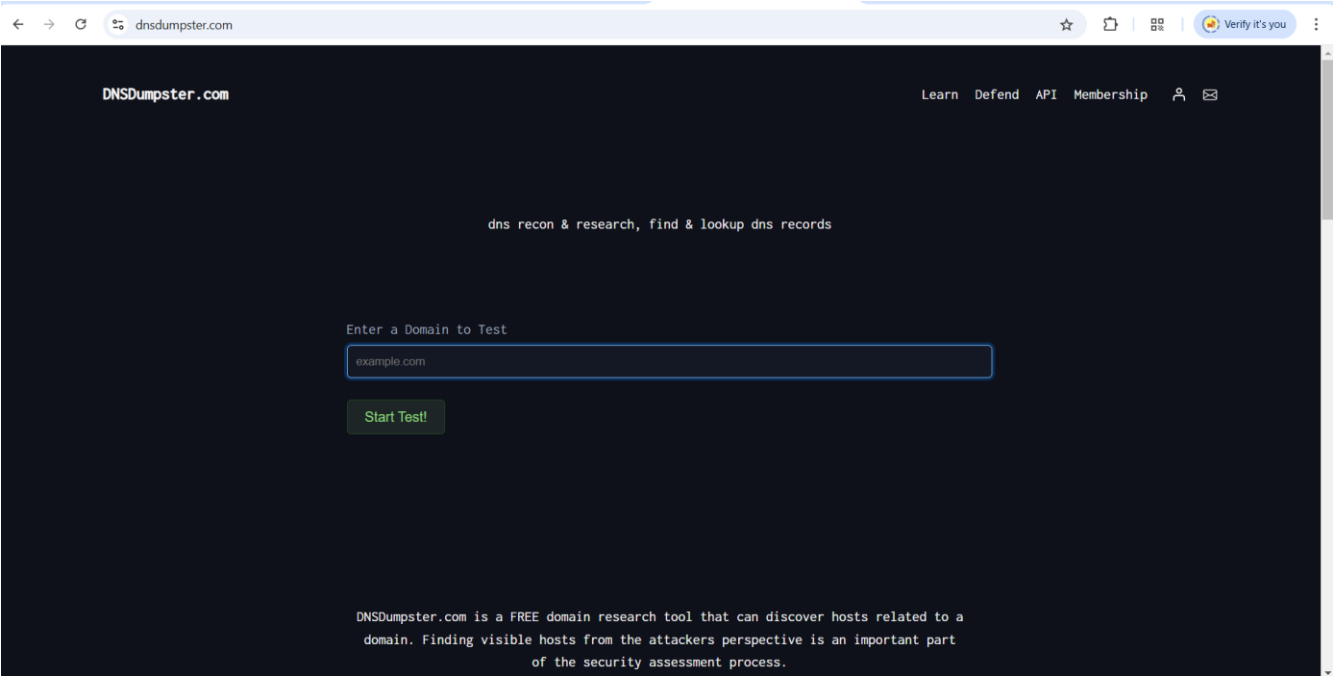


Figure 11: 4th tool is DNSDumpster.com

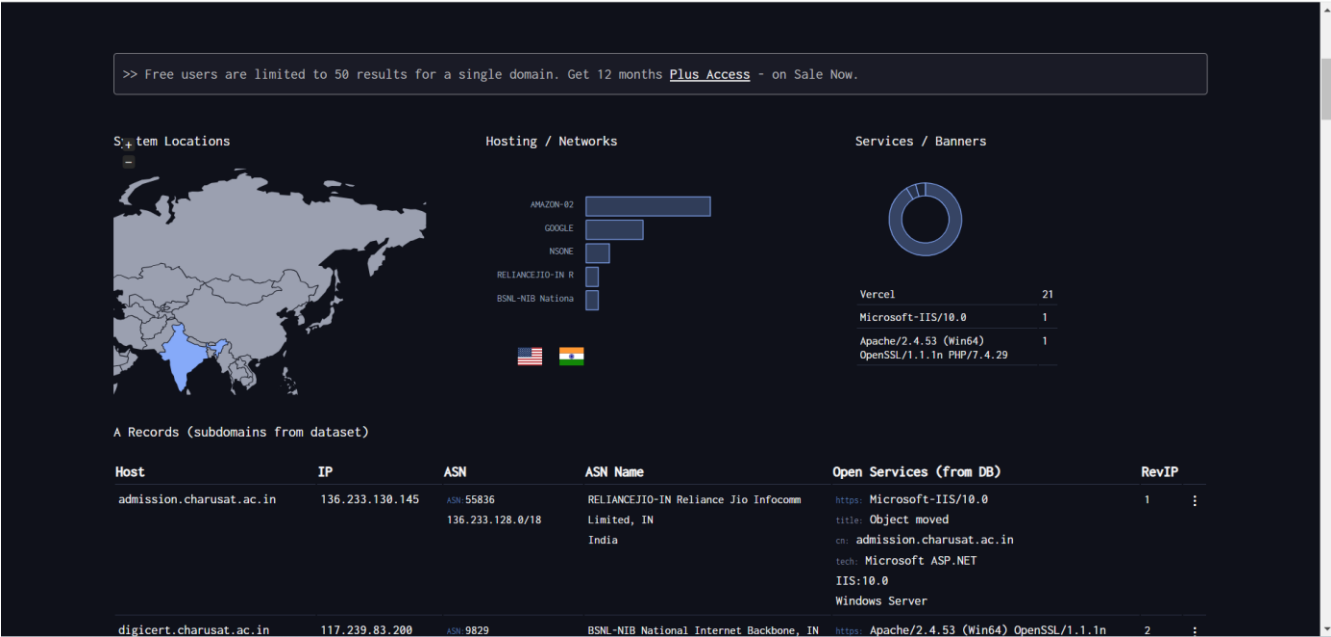


Figure 12: This is a result of dnsdumpster.com

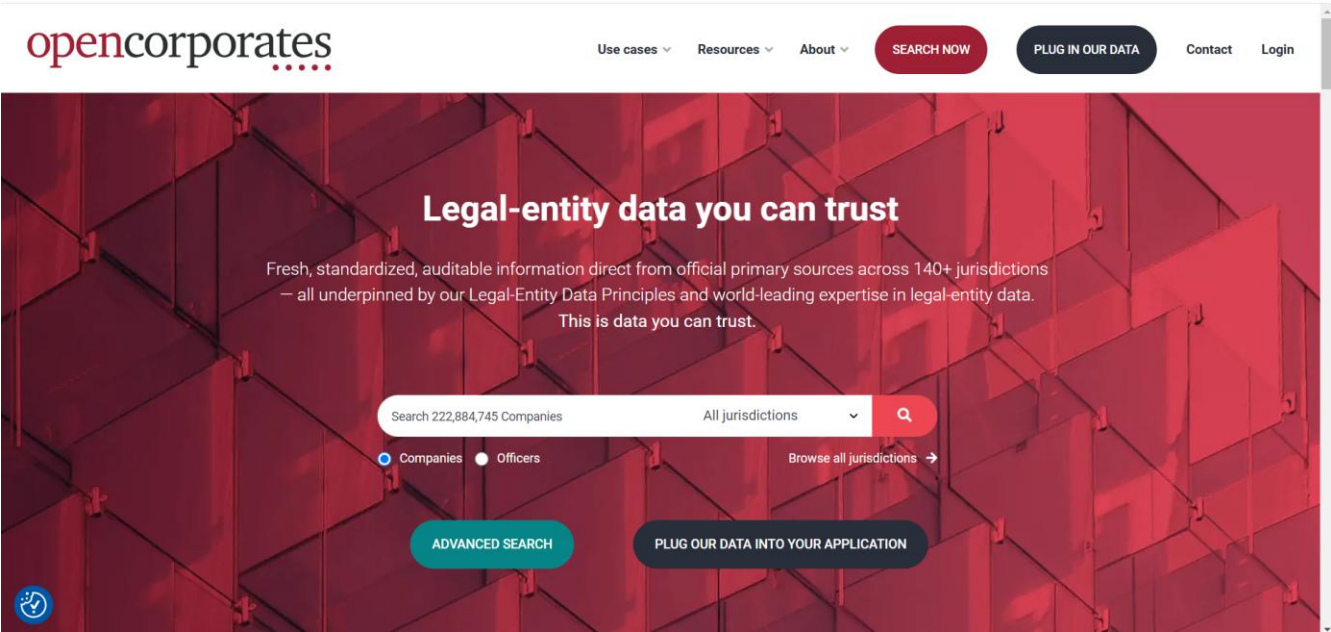


Figure 13: 5th tool are opencorporates

The screenshot shows the OpenCorporates website interface. At the top, the logo 'opencorporates' is displayed with the tagline 'The Open Database Of The Corporate World'. A search bar contains the text 'Company name or number' and a 'SEARCH' button. Below the search bar, there are tabs for 'Companies' and 'Officers'. The main content area shows 'Found 11 companies' with a search input 'elon musk' and a 'GO' button. A list of 11 companies is displayed, including 'ELON MUSK & ASSOCIATES LLC', 'ELON MUSK HEALTHY INTERNATIONAL TRADING LIMITED', 'ELON MUSK LLC', 'ELON REEVE MUSK CORP', 'Elon Musk Investment Charter ICC L.L.C', 'INTELLIGENCE ARTIFICIAL LTD', 'MKT SERVICES DBA ELON MUSK & STUFF LLC', 'NEW ZEALAND ELON MUSK HEALTHY LIVE BROADCAST PLATFORM LIMITED', 'Presse Conference of Twitter founder Elon Musk by Forbes Magazine News Journalist Kabika Moukoumani Kabila', 'Presse Conference of Twitter founder Elon Musk by Washington News Magazine Journalist Kabika Moukoumani Kabila', and 'The Church of Elon Musk'. On the right side, there is a red banner with the text 'This information comes to you from OpenCorporates – the leading authority on legal-entity data'. Below this, there is a 'Certified' badge and a 'Get company data at scale' section with 'XML' and 'JSON' buttons. A 'Filtered by jurisdiction' section lists various countries and their counts.

Found 11 companies

elon musk GO

☐ exclude inactive Advanced Options

**ELON MUSK & ASSOCIATES LLC** (Delaware (US), Sussex, DE)

**ELON MUSK HEALTHY INTERNATIONAL TRADING LIMITED** (New Zealand, 15 Shelby Lane, Flat Bush, Auckland, 2016)

**ELON MUSK LLC** (Florida (US))

**ELON REEVE MUSK CORP** (Louisiana (US))

**Elon Musk Investment Charter ICC L.L.C** (Mississippi (US))

**INTELLIGENCE ARTIFICIAL LTD** (United Kingdom, C/O M Marshall De Siqueira 13 Hanger View Way, London, W3 0EX) Previously/Alternately known as ELON MUSK LIMITED

**MKT SERVICES DBA ELON MUSK & STUFF LLC** (Wisconsin (US))

**NEW ZEALAND ELON MUSK HEALTHY LIVE BROADCAST PLATFORM LIMITED** (New Zealand, 106 Richard Pearse Drive, Mangere, Auckland, 2022)

**Presse Conference of Twitter founder Elon Musk by Forbes Magazine News Journalist Kabika Moukoumani Kabila** (France, 248 New York Central Park Avenue, New York United States, 10008)

**Presse Conference of Twitter founder Elon Musk by Washington News Magazine Journalist Kabika Moukoumani Kabila** (France, 3758 New York Central Park Avenue, New York United States, 10008)

**The Church of Elon Musk** (Colorado (US))

This information comes to you from **OpenCorporates** – the leading authority on legal-entity data

Read more about us and why you should trust this data in our [purpose, history and principles](#)

The OpenCorporates website is free for general-public and public-benefit use

[Use the OpenCorporates API](#)

[License this data in bulk](#)

**Certified** Corporation

Get company data at scale [XML](#) OR [JSON](#)

Filtered by jurisdiction

- 1 Colorado (US)
- 1 Delaware (US)
- 1 Florida (US)
- 2 France
- 1 Louisiana (US)
- 1 Mississippi (US)
- 2 New Zealand
- 1 United Kingdom
- 4 Wisconsin (US)

Figure 14: It will find 11 companies for Elon Musk

The screenshot shows the OpenCorporates website interface with the details for 'ELON MUSK & ASSOCIATES LLC'. The company name is prominently displayed at the top. Below it, various details are listed: Company Number (6434993), Incorporation Date (Please log in to see this data), Company Type (Domestic Limited Liability Company), Jurisdiction (Delaware (US)), Registered Address (Sussex, DE, United States), Agent Name (HARVARD BUSINESS SERVICES, INC), Agent Address (16192 COASTAL HWY - LEWES DE 19958), and Directors / Officers (1 officer available, please log in to see this data). On the right side, there is a 'Data source and freshness' section with fields for 'Last update from source', 'Last change recorded', 'Next update from source', and 'Source'. Below this, there is a red banner with the text 'This information comes to you from OpenCorporates – the leading authority on legal-entity data'. Below this, there is a 'Certified' badge and a 'Get company data at scale' section with 'XML' and 'JSON' buttons. A 'Filtered by jurisdiction' section lists various countries and their counts.

**ELON MUSK & ASSOCIATES LLC**

Company Number 6434993

Incorporation Date Please log in to see this data

Company Type Domestic Limited Liability Company

Jurisdiction Delaware (US)

Registered Address Sussex, DE United States

Agent Name HARVARD BUSINESS SERVICES, INC

Agent Address 16192 COASTAL HWY - LEWES DE 19958

Directors / Officers 1 officer available, please log in to see this data

**Data source and freshness**

Last update from source Please log in to see this data

Last change recorded

Next update from source

Source

[Learn more about our trust and data transparency policy](#)

This information comes to you from **OpenCorporates** – the leading authority on legal-entity data

Read more about us and why you should trust this data in our [purpose, history and principles](#)

The OpenCorporates website is free for general-public and public-benefit use

[Use the OpenCorporates API](#)

[License this data in bulk](#)

**Certified** Corporation

\* While we strive to keep this information correct and up-to-date, it is not the primary source, and the company registry should always be referred to for definitive information

Figure 15: This is a details of Elon Musk company

**LATEST APPLICATIONS:**

- Reconnaissance for Phishing Campaigns
- Cyber Threat Intelligence (CTI) Analysis
- Digital Forensics and Incident Response (DFIR)
- Website Threat Intelligence
- Vulnerability Discovery in Cloud Infrastructure
- Corporate Governance and Insider Threat Analysis
- Mergers and Acquisitions (M&A) Risk Assessment

**LEARNING OUTCOME:**

In this practical we learn about foot printing and reconnaissance using various OSINT frameworks tool

**REFERENCES:**

1. OSINT Framework: <https://osintframework.com/>
2. WhatsMyName: <https://whatsmyname.app/>
3. Urlscan.io: <https://urlscan.io/>
4. Wayback Machine: <https://web.archive.org/>
5. DNSDumpster: <https://dnsdumpster.com/>
6. opencorporates: <https://opencorporates.com/>