Experiment 6

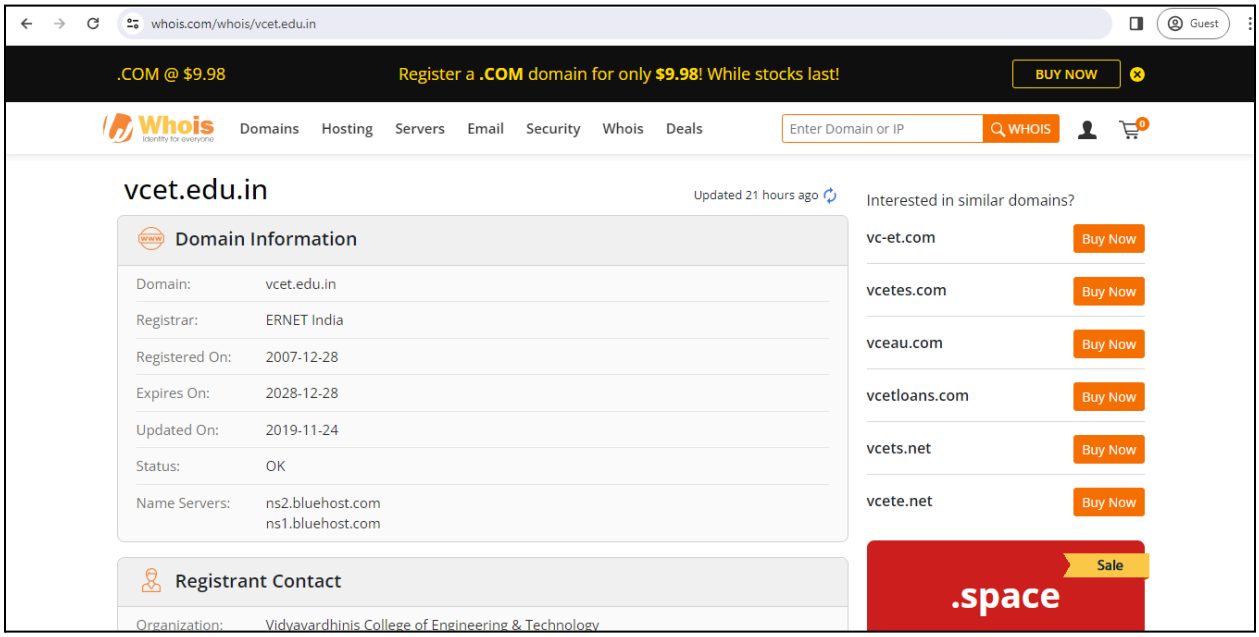
Aim: Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.

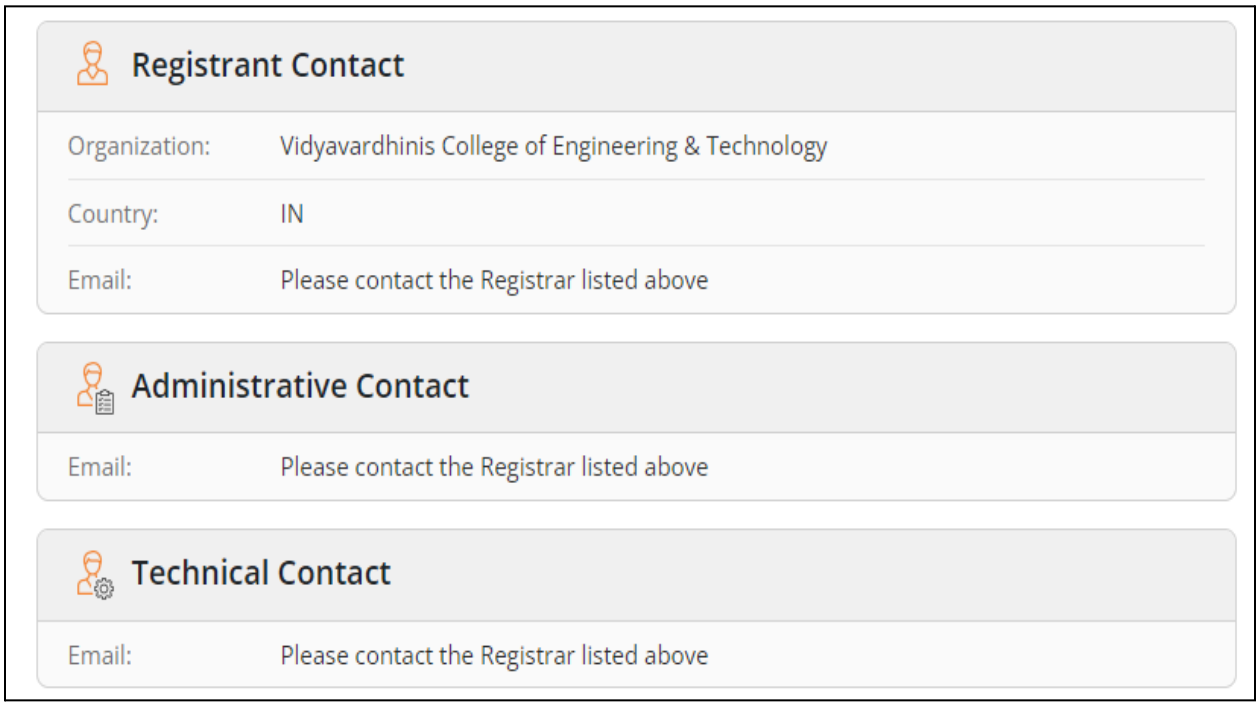
1) Whois:

Whois is a widely used Internet record listing that identifies who owns a domain and how to get in contact with them.

A WHOIS lookup allows you to find a domain name owner's name, contact information, and other important details. ICANN (Internet Corporation for Assigned Names and Numbers) maintains a database the public can search to see who owns any domain.

During domain name registration, you have to provide accurate and current information about yourself. This info is used to ensure the security and reliability of your registered domain names and websites.


whois.com/whois/vcet.edu.in
.COM @ $9.98
Register a .COM domain for only $9.98! While stocks last!
BUY NOW
Whois
Domains
Hosting
Servers
Email
Security
Whois
Deals
Enter Domain or IP
WHOIS
vcet.edu.in
Updated 21 hours ago
Domain Information
Domain: vcet.edu.in
Registrar: ERNET India
Registered On: 2007-12-28
Expires On: 2028-12-28
Updated On: 2019-11-24
Status: OK
Name Servers: ns2.bluehost.com
ns1.bluehost.com
Registrant Contact
Organization: Vidyavardhinis College of Engineering & Technology
Interested in similar domains?
vc-et.com Buy Now
vcetes.com Buy Now
vceau.com Buy Now
vcetloans.com Buy Now
vcets.net Buy Now
vcete.net Buy Now
Sale
.space

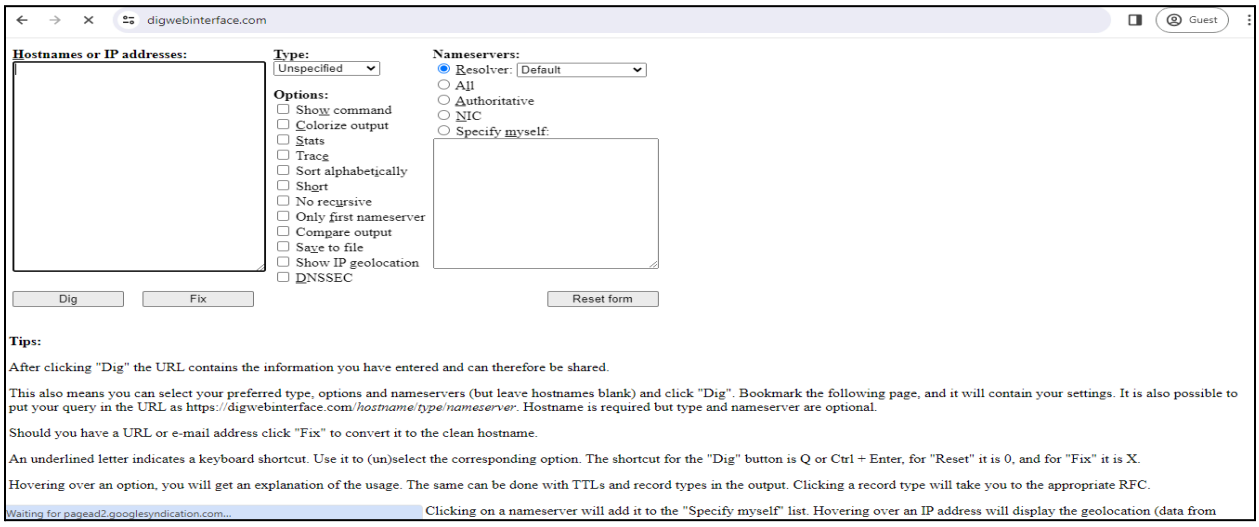

Registrant Contact
Organization: Vidyavardhinis College of Engineering & Technology
Country: IN
Email: Please contact the Registrar listed above
Administrative Contact
Email: Please contact the Registrar listed above
Technical Contact
Email: Please contact the Registrar listed above

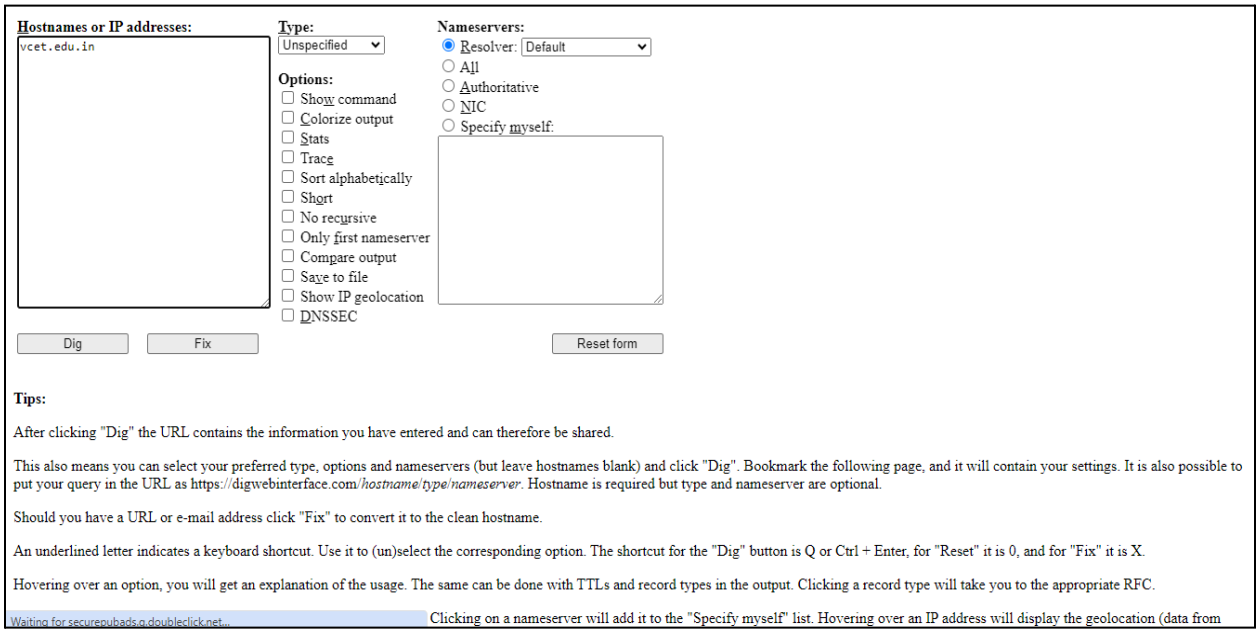
Raw Whois Data

```
Domain Name: vcet.edu.in
Registry Domain ID: D2735175-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2019-11-24T05:59:11Z
Creation Date: 2007-12-28T06:03:37Z
Registry Expiry Date: 2028-12-28T06:03:37Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Vidyavardhinis College of Engineering & Technology
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
```

2) Dig Web Interface:

Dig Web Interface is an online utility that helps you lookup DNS information for a domain name. dig (domain information groper) is a Unix-like network administration command-line tool for querying Domain Name System (DNS) servers.





Hostnames or IP addresses:

vcet.edu.in

Type: Unspecified

Options:

- [ ] Show command
- [x] Colorize output
- [ ] Stats
- [ ] Trace
- [ ] Sort alphabetically
- [ ] Short
- [ ] No recursive
- [ ] Only first nameserver
- [ ] Compare output
- [ ] Save to file
- [ ] Show IP geolocation
- [ ] DNSSEC

Nameservers:

- ( ) Resolver: Default
- (•) All
- ( ) Authoritative
- ( ) NIC
- ( ) Specify myself:

Dig | Fix | Reset form

vcet.edu.in@9.9.9.10 (Default):

```
vcet.edu.in.            12184   IN      A       173.254.89.26
```

vcet.edu.in@94.140.14.14 (AdGuard (CY)):

```
vcet.edu.in.            12258   IN      A       173.254.89.26
```

vcet.edu.in@165.87.13.129 (AT&T (US)):

```
vcet.edu.in.            12947   IN      A       173.254.89.26
```

vcet.edu.in@1.1.1.1 (Cloudflare):

```
vcet.edu.in.            14400   IN      A       173.254.89.26
```

vcet.edu.in@8.26.56.26 (Comodo (US)):

```
vcet.edu.in.            12279   IN      A       173.254.89.26
```

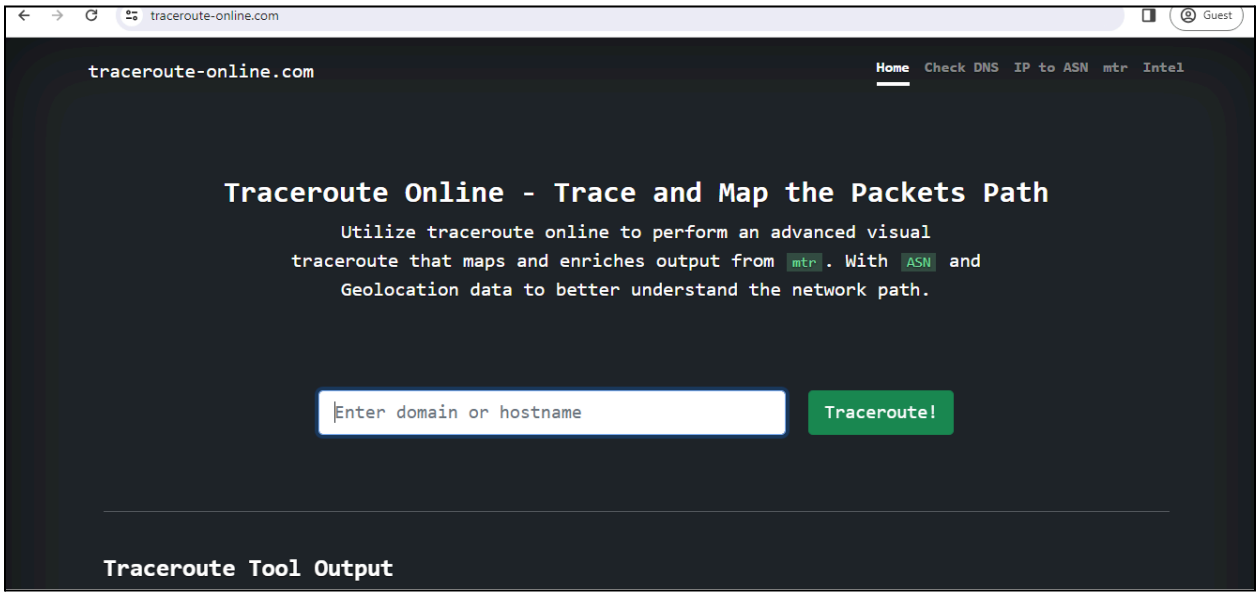
vcet.edu.in@8.8.8.8 (Google):

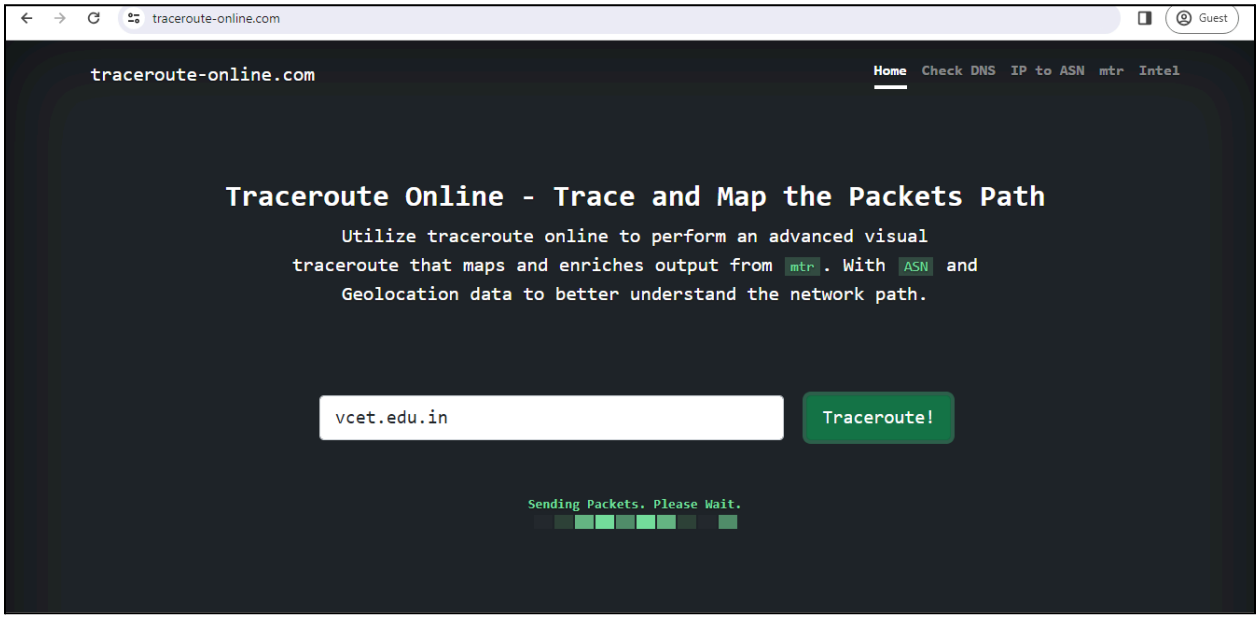
```
vcet.edu.in.            12257   IN      A       173.254.89.26
```

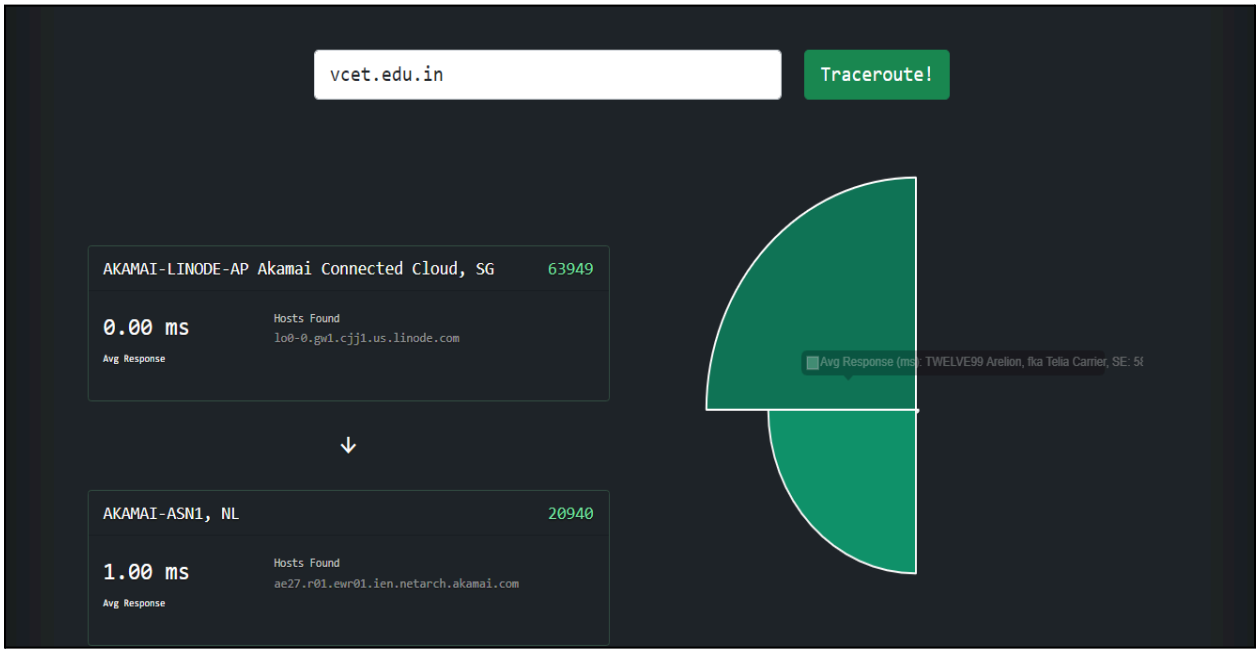
vcet.edu.in@168.95.1.1 (HiNet (TW)):

3) Traceroute:

Traceroute is a network testing term that is used to examine the hops that communication will follow across an IP network. It also is commonly referred to by the name of the tools used to perform the trace; typically traceroute on Linux based systems and tracert on Windows operating systems.



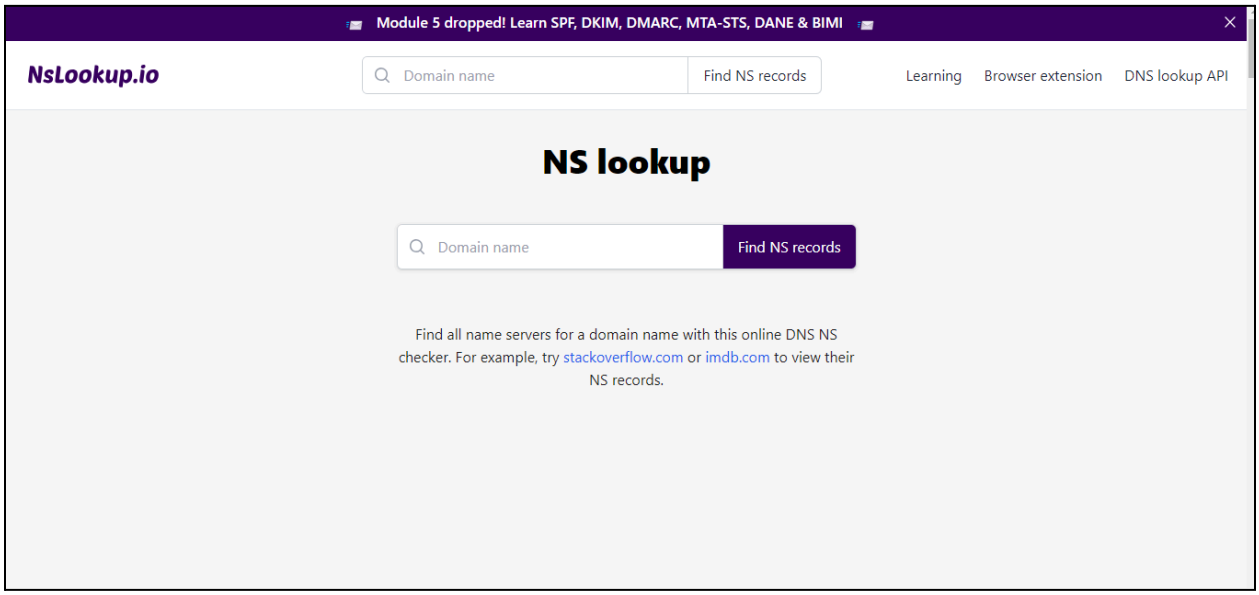


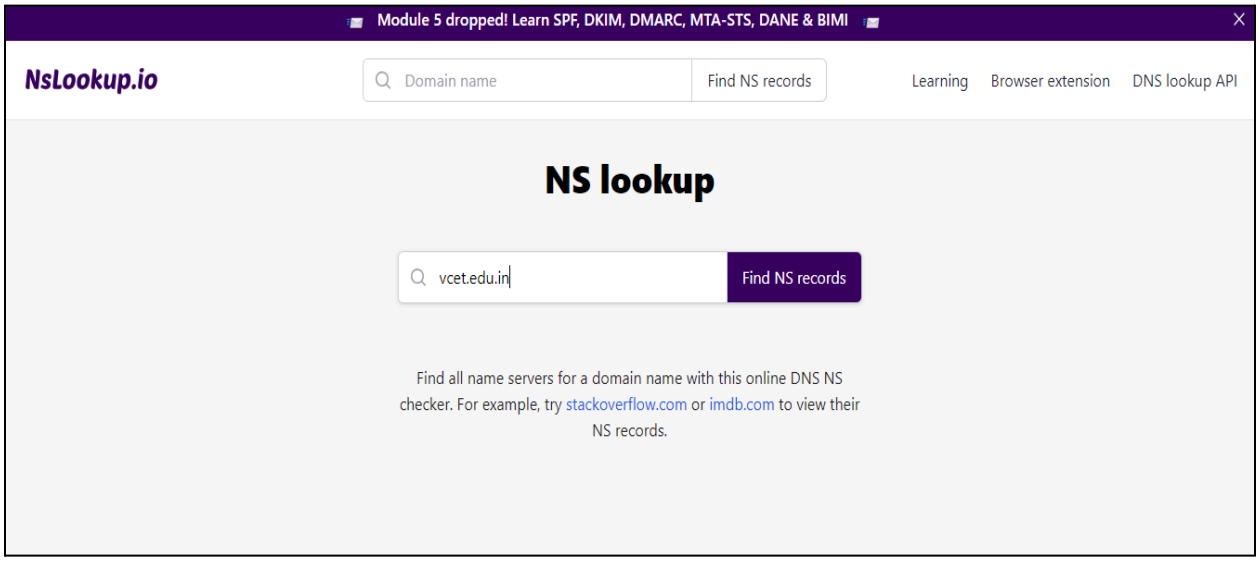


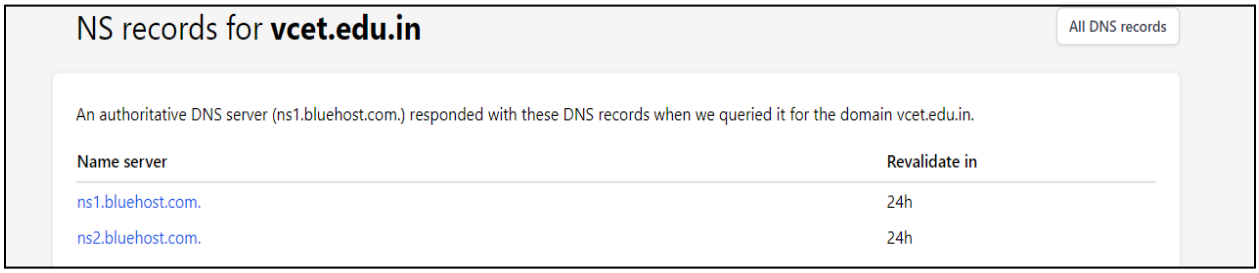
Hop	IP / Host Name	ISP	Netblock	Country	Loss	Response
1	172.17.0.1				0.0%	0.15ms
2	10.206.5.139				0.0%	0.34ms
3	10.206.35.7				0.0%	0.62ms
4	10.206.32.2				0.0%	7.18ms
5	lo0-0.gw1.cjj1.us.linode.com 173.255.239.101	AKAMAI-LINODE-AP Akamai Connected Cloud, SG	173.255.239.0/24		0.0%	0.75ms
6	ae27.r01.ewr01.ien.netarch.akamai.com 23.203.154.22	AKAMAI-ASN1, NL	23.203.154.0/24		0.0%	1.13ms
7	???					
8	nyk-bb2-link.ip.twelve99.net 62.115.135.162	TWELVE99 Arelion, fka Telia Carrier, SE	62.115.0.0/16		0.0%	2.07ms
9	palo-b24-link.ip.twelve99.net 62.115.122.36	TWELVE99 Arelion, fka Telia Carrier, SE	62.115.0.0/16		0.0%	69.13ms
10	salt-b2-link.ip.twelve99.net 62.115.140.53	TWELVE99 Arelion, fka Telia Carrier, SE	62.115.0.0/16		0.0%	83.36ms
11	newfolddigital-ic-380138-ip-twelve99-	TWELVE99 Arelion, fka Telia	80.239.160.0/19		0.0%	80.83ms

4) NS Lookup:

Online nslookup is a web based DNS client that queries DNS records for a given domain name. It allows you to view all the DNS records for a website. It provides the same information as command line tools like dig and nslookup, from the convenience of your web browser.





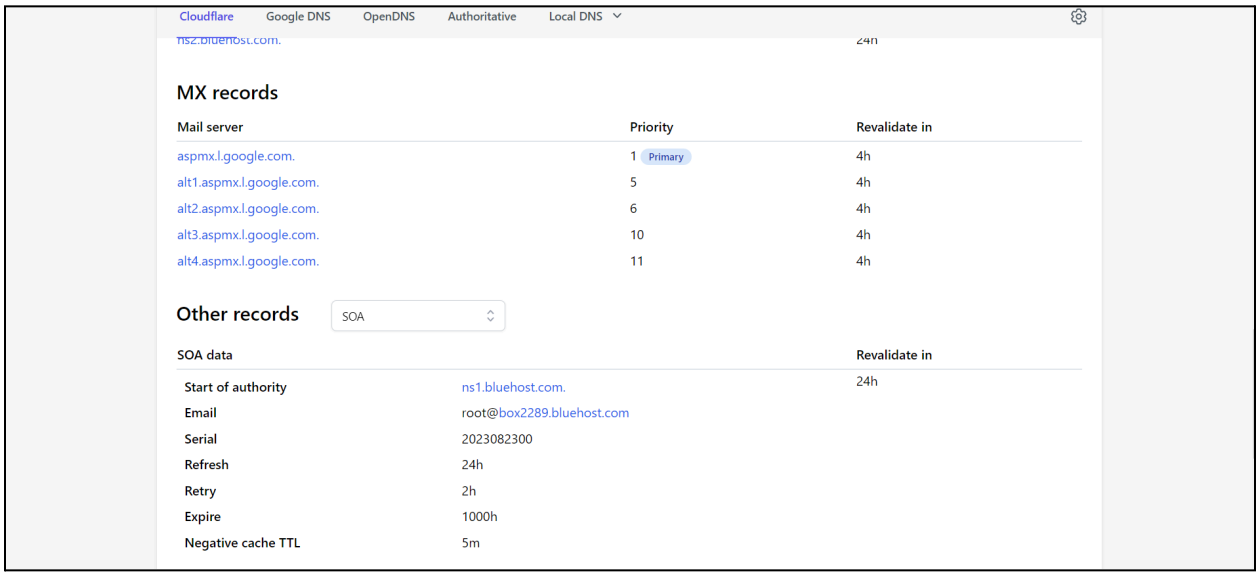


NS records for **vcet.edu.in**

All DNS records

An authoritative DNS server (ns1.bluehost.com.) responded with these DNS records when we queried it for the domain vcet.edu.in.

Name server	Revalidate in
ns1.bluehost.com.	24h
ns2.bluehost.com.	24h



Cloudflare Google DNS OpenDNS Authoritative Local DNS

ns2.bluehost.com. 24h

MX records

Mail server	Priority	Revalidate in
aspmx.l.google.com.	1 Primary	4h
alt1.aspmx.l.google.com.	5	4h
alt2.aspmx.l.google.com.	6	4h
alt3.aspmx.l.google.com.	10	4h
alt4.aspmx.l.google.com.	11	4h

Other records

SOA

SOA data		Revalidate in
Start of authority	ns1.bluehost.com.	24h
Email	root@box2289.bluehost.com	
Serial	2023082300	
Refresh	24h	
Retry	2h	
Expire	1000h	
Negative cache TTL	5m	