



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.





Vidyavardhini's College of Engineering and Technology, Vasai

Department of Computer Science & Engineering (Data Science)

[←](#) [→](#) [↺](#) [whois.com/whois/vcet.edu.in](#) [Guest](#)

.COM @ \$9.98 Register a **.COM** domain for only **\$9.98!** While stocks last! [BUY NOW](#)

Domains Hosting Servers Email Security Whois Deals [WHOIS](#)

vcet.edu.in

 Updated 21 hours ago [↺](#) Interested in similar domains?

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
---------------	--

[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](#)

.space [Sale](#)

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.

The screenshot shows the Dig Web Interface (digwebinterface.com) in a web browser. The interface includes a form for entering hostnames or IP addresses, a dropdown for selecting the type of query, a list of options for customizing the output, and a dropdown for selecting nameservers. The "Dig" button is highlighted.

Hostnames or IP addresses:

Type: Unspecified

Nameservers: Resolver: Default

Options:

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

Buttons: Dig, Fix, Reset form

Tips:

After clicking "Dig" the URL contains the information you have entered and can therefore be shared.

This also means you can select your preferred type, options and nameservers (but leave hostnames blank) and click "Dig". Bookmark the following page, and it will contain your settings. It is also possible to put your query in the URL as <https://digwebinterface.com/hostname/type/nameserver>. Hostname is required but type and nameserver are optional.

Should you have a URL or e-mail address click "Fix" to convert it to the clean hostname.

An underlined letter indicates a keyboard shortcut. Use it to (un)select the corresponding option. The shortcut for the "Dig" button is Q or Ctrl + Enter, for "Reset" it is O, and for "Fix" it is X.

Hovering over an option, you will get an explanation of the usage. The same can be done with TTLs and record types in the output. Clicking a record type will take you to the appropriate RFC.

Waiting for page2.googleadsyndication.com... Clicking on a nameserver will add it to the "Specify myself" list. Hovering over an IP address will display the geolocation (data from

The screenshot shows the Dig Web Interface (digwebinterface.com) in a web browser. The interface includes a form for entering hostnames or IP addresses, a dropdown for selecting the type of query, a list of options for customizing the output, and a dropdown for selecting nameservers. The "Dig" button is highlighted.

Hostnames or IP addresses: vcet.edu.in

Type: Unspecified

Nameservers: Resolver: Default

Options:

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

Buttons: Dig, Fix, Reset form

Tips:

After clicking "Dig" the URL contains the information you have entered and can therefore be shared.

This also means you can select your preferred type, options and nameservers (but leave hostnames blank) and click "Dig". Bookmark the following page, and it will contain your settings. It is also possible to put your query in the URL as <https://digwebinterface.com/hostname/type/nameserver>. Hostname is required but type and nameserver are optional.

Should you have a URL or e-mail address click "Fix" to convert it to the clean hostname.

An underlined letter indicates a keyboard shortcut. Use it to (un)select the corresponding option. The shortcut for the "Dig" button is Q or Ctrl + Enter, for "Reset" it is O, and for "Fix" it is X.

Hovering over an option, you will get an explanation of the usage. The same can be done with TTLs and record types in the output. Clicking a record type will take you to the appropriate RFC.

Waiting for securepubads.doubleclick.net... Clicking on a nameserver will add it to the "Specify myself" list. Hovering over an IP address will display the geolocation (data from



Hostnames or IP addresses:
vcet.edu.in

Type:
Unspecified

Nameservers:
☐ Resolver: Default
☒ All
☐ Authoritative
☐ NIC
☐ Specify myself:

Options:
☐ Show command
☒ Colorize output
☐ Stats
☐ Trace
☐ Sort alphabetically
☐ Short
☐ No recursive
☐ Only first nameserver
☐ Compare output
☐ Save to file
☐ Show IP geolocation
☐ DNSSEC

DigFixReset 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.

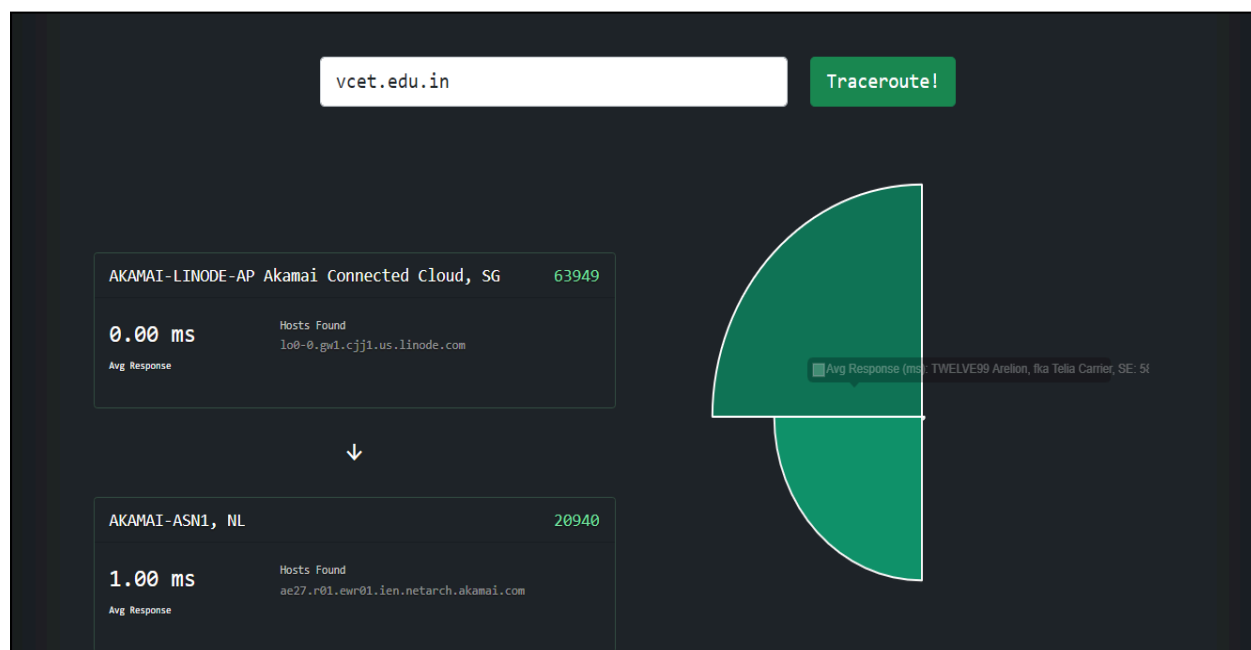
The screenshot shows the Traceroute Online website interface. At the top, there is a navigation bar with links: Home, Check DNS, IP to ASN, mtr, and Intel. The main heading is "Traceroute Online - Trace and Map the Packets Path". Below this, a description states: "Utilize traceroute online to perform an advanced visual traceroute that maps and enriches output from mtr. With ASN and Geolocation data to better understand the network path." There is a text input field with the placeholder "Enter domain or hostname" and a green button labeled "Traceroute!". Below the input field, the text "Traceroute Tool Output" is visible.

This screenshot shows the same Traceroute Online website interface, but with the domain "vcet.edu.in" entered into the input field. The "Traceroute!" button remains green. Below the input field, the text "Sending Packets. Please Wait." is displayed, followed by a progress bar consisting of several green squares.



Vidyavardhini's College of Engineering and Technology, Vasai

Department of Computer Science & Engineering (Data Science)



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	100-0.gw1.cj11.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.iem.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	newfalddigital-ic-380138.ip.twelve99-	TWELVE99 Arelion, fka Telia	62.115.0.0/16		0.0%	88.83ms



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.

The screenshot shows the Nslookup.io website interface. At the top, there is a purple header bar with the text "Module 5 dropped! Learn SPF, DKIM, DMARC, MTA-STS, DANE & BIMI" and a close button. Below the header, the website logo "Nslookup.io" is on the left, and a search bar with the placeholder "Domain name" and a "Find NS records" button is in the center. To the right of the search bar are links for "Learning", "Browser extension", and "DNS lookup API". The main content area has a large heading "NS lookup" and a search bar with the placeholder "Domain name" and a "Find NS records" button. Below the search bar, there is a paragraph: "Find all name servers for a domain name with this online DNS NS checker. For example, try stackoverflow.com or imdb.com to view their NS records."

The screenshot shows the Nslookup.io website interface with the domain "vcet.edu.in" entered in the search bar. The layout is identical to the previous screenshot, but the search bar now contains the text "vcet.edu.in". The "Find NS records" button is still present next to the search bar. The main content area still displays the heading "NS lookup" and the explanatory paragraph about the online DNS NS checker.



Vidyavardhini's College of Engineering and Technology, Vasai

Department of Computer Science & Engineering (Data Science)

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	24h
Email	root@box2289.bluehost.com
Serial	2023082300
Refresh	24h
Retry	2h
Expire	1000h
Negative cache TTL	5m