



Vidyavardhini's College of Engineering & Technology

Department of Artificial Intelligence and Data Science

EXPERIMENT 06

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

Theory:

WHOIS:

Whois is a protocol and database system used for querying information about internet resources, such as domain names, IP addresses, and autonomous system numbers. It provides details about the registrant, administrative contact, and other pertinent information related to the resource.

Features:

1. Domain Name Lookup: Whois allows users to look up information about a specific domain name to find out details such as the registrar, registration date, expiration date, and contact information of the domain owner.
2. IP Address Query: Besides domain names, Whois also supports querying for information about IP addresses. Users can use Whois to find out information about the organization or individual associated with a particular IP address.

The screenshot shows a Whois website interface. At the top, there's a navigation bar with links: Domains, Hosting, Servers, Email, Security, Whois, Deals. A search bar contains 'Enter Domain or IP' and a 'WHOIS' button. The main content area displays 'vcet.edu.in' with a 'Updated 6 days ago' status. Below this, there's a 'Domain Information' table and a 'Registrant Contact' table. To the right, there's a list of 'Interested in similar domains?' with options like 'vc-et.com', 'vcetes.com', 'vceau.com', 'vcetloans.com', 'vcets.net', and 'vcete.net', each with a 'Buy Now' button. At the bottom right, there's a red banner for '.space' domains with a 'Sale' tag, showing a price of '\$1.88' (down from '\$29.88') and a 'BUY NOW' button.

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
Country:	IN

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

.space Sale
\$29.88 **\$1.88**
BUY NOW

DIG WEB INTERFACE: The DIG Web Interface is a tool used for querying and displaying DNS (Domain Name System) information directly from a web browser. It allows users to perform DNS queries such as looking up IP addresses, finding mail servers, and checking domain records.

Features:

1. User-Friendly Interface: It provides an intuitive web-based interface, making it easy for users to input their queries and interpret the results without needing to use command-line tools or navigate complex DNS settings.
2. Comprehensive DNS Query Support: The DIG Web Interface supports a wide range of DNS query types,



Vidyavardhini's College of Engineering & Technology

Department of Artificial Intelligence and Data Science

The screenshot shows the Dig tool interface. On the left, there's a text box for 'Hostnames or IP addresses:' containing 'vcet.edu.in'. Below it are 'Dig' and 'Fix' buttons. In the center, there's a 'Type:' dropdown set to 'Unspecified' and a list of 'Options' with checkboxes for 'Show command', 'Colorize output', 'Stats', 'Trace', 'Sort alphabetically', 'Short', 'No recursive', 'Only first nameserver', 'Compare output', 'Save to file', 'Show IP geolocation', and 'DNSSEC'. On the right, there's a 'Nameservers:' section with a 'Resolver:' dropdown set to 'Default' and radio buttons for 'All', 'Authoritative', 'NIC', and 'Specify myself'. A 'Reset form' button is at the bottom right. Below the main interface, the command 'vcet.edu.in@9.9.9.10 (Default):' is shown, followed by the output: 'vcet.edu.in. 14400 IN A 173.254.89.26'.

including A (IPv4 address), AAAA (IPv6 address), MX (Mail Exchange), NS (Name Server), TXT (Text), and more. Users can quickly obtain various DNS-related information they need for troubleshooting or analysis purposes.

Traceroute: Traceroute is a network diagnostic tool used to track the pathway (or route) taken by data packets from one computer to another over a network, such as the Internet.

Features:

1. Hop-by-Hop Analysis: Traceroute displays each router or "hop" along the network path, allowing users to identify where potential bottlenecks or issues might be occurring.
2. Round-Trip Time (RTT) Measurement: Traceroute measures the round-trip time it takes for packets to travel from the source to each router and back. This information helps in assessing network latency and identifying slow segments of the network.

```
Command Prompt
C:\Users\Mokshu>tracert vcet.edu.in

Tracing route to vcet.edu.in [173.254.89.26]
over a maximum of 30 hops:

  1  1 ms  1 ms  1 ms  192.168.0.1
  2  3 ms  2 ms  2 ms  103.31.144.7
  3  *      *      *      Request timed out.
  4  2 ms  2 ms  3 ms  103.31.144.21
  5  5 ms  5 ms  5 ms  static-21.173.248.49-tataidc.co.in [49.248.173.21]
  6  6 ms  *      *      10.118.143.1
  7  4 ms  4 ms  5 ms  115.113.165.21.static-mumbai.vsnl.net.in [115.113.165.21]
  8  *      *      *      Request timed out.
  9  30 ms  30 ms  30 ms  ix-ae-4-2.tcore1.cxr-chennai.as6453.net [180.87.36.9]
 10 59 ms  58 ms  58 ms  if-be-34-2.ecore2.esin4-singapore.as6453.net [180.87.36.41]
 11 63 ms  73 ms  62 ms  180.87.108.163
 12 63 ms  *      86 ms  ae-4.r22.sngpsi07.sg.bb.gin.ntt.net [129.250.5.61]
 13 137 ms 139 ms 135 ms  ae-4.r27.osakjp02.jp.bb.gin.ntt.net [129.250.2.67]
 14 *      233 ms *      ae-3.r24.lsanca07.us.bb.gin.ntt.net [129.250.2.176]
 15 233 ms 232 ms 232 ms  ae-0.a03.lsanca07.us.bb.gin.ntt.net [129.250.3.140]
 16 237 ms 237 ms 236 ms  ce-3-0-1.a03.lsanca07.us.ce.gin.ntt.net [168.143.228.173]
 17 237 ms 238 ms 237 ms  162-215-195-128.unifiedlayer.com [162.215.195.128]
 18 260 ms 258 ms 258 ms  162-215-195-141.unifiedlayer.com [162.215.195.141]
 19 257 ms 258 ms 258 ms  69-195-64-103.unifiedlayer.com [69.195.64.103]
 20 257 ms 258 ms 256 ms  po97.prv-leaf6a.net.unifiedlayer.com [162.144.240.11]
 21 257 ms 257 ms 257 ms  box2289.bluehost.com [173.254.89.26]

Trace complete.
C:\Users\Mokshu>
```

Nslookup: `nslookup` stands for "Name Server Lookup". It's a command-line tool used to query DNS (Domain Name System) servers to obtain DNS-related information, such as IP addresses associated with domain names or vice versa.



Vidyavardhini's College of Engineering & Technology

Department of Artificial Intelligence and Data Science

Features:

1. **DNS Querying:** `nslookup` allows users to query DNS servers for various types of DNS records, such as A (Address) records, MX (Mail Exchange) records, PTR (Pointer) records, etc. This enables users to retrieve information about domain names, IP addresses, mail servers, and more.
2. **Interactive Mode:** `nslookup` provides an interactive mode where users can enter commands and perform multiple DNS queries without having to exit and relaunch the tool. This mode allows for greater flexibility and efficiency when troubleshooting DNS-related issues.

The screenshot shows the Nslookup.io website interface. At the top, there is a search bar with the text "vcet.edu.in" and a "Find DNS records" button. To the right of the search bar are links for "Learning", "Browser extension", and "DNS lookup API". Below the search bar, the title "DNS records for vcet.edu.in" is displayed. Underneath the title, there are tabs for "Cloudflare", "Google DNS", "OpenDNS", "Authoritative", and "Local DNS". The "Cloudflare" tab is selected. A message states: "The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers." Below this message, there are three sections: "A records", "AAAA records", and "CNAME record". The "A records" section shows a table with two columns: "IPv4 address" and "Revalidate in". The table contains one row with the IP address "173.254.89.26" and a revalidation time of "4h". The "AAAA records" section states "No AAAA records found." and the "CNAME record" section states "No CNAME record found."

IPv4 address	Revalidate in
> 173.254.89.26	4h

Conclusion:

This experiment delved into network reconnaissance tools such as WHOIS, dig, traceroute, and nslookup, essential for gathering information about networks and domain registrars. WHOIS provides details about domain names and IP addresses, while dig offers a user-friendly web interface for querying DNS information comprehensively. Traceroute aids in analyzing network pathways and measuring round-trip times, crucial for troubleshooting network issues. Lastly, nslookup facilitates DNS querying and interactive mode functionality for efficient troubleshooting. Together, these tools empower users to gather critical network and domain information, enhancing network management and security practices.