EXPERIMENT 06

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

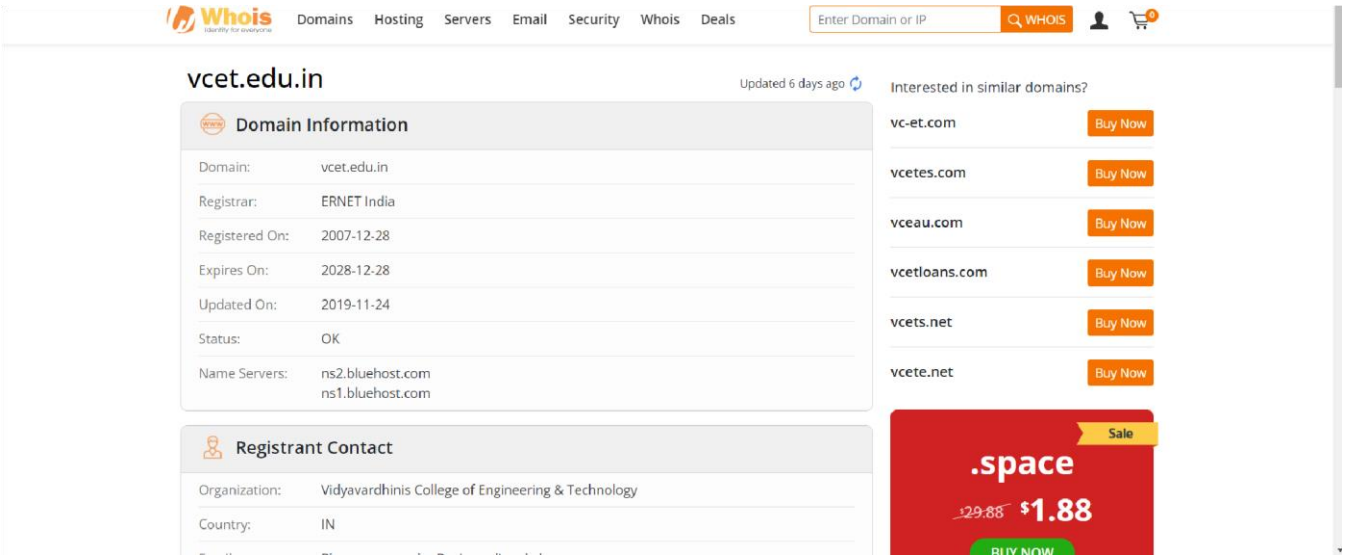
Theory:

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.



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:

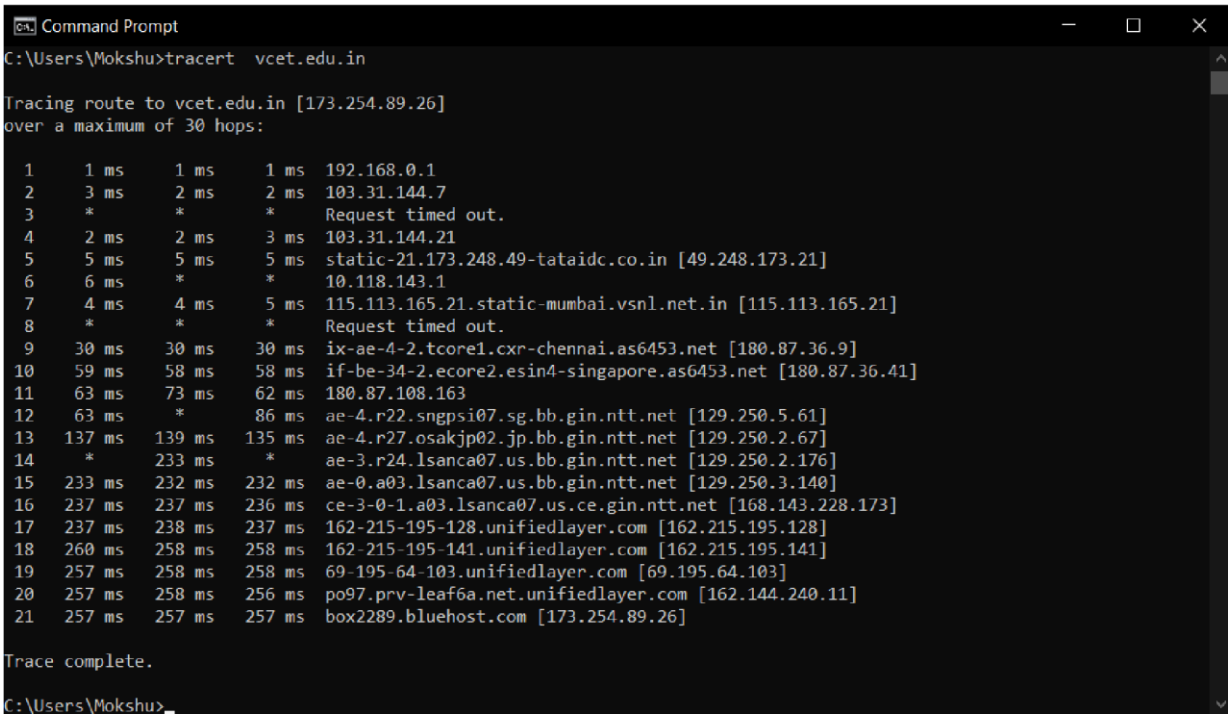
1. User-Friendly Interface: It provides an intuitive web-based interface, making it easy for users to input their queries and interpret the results without needing to use command-line tools or navigate complex DNS settings.
2. Comprehensive DNS Query Support: The DIG Web Interface supports a wide range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

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.

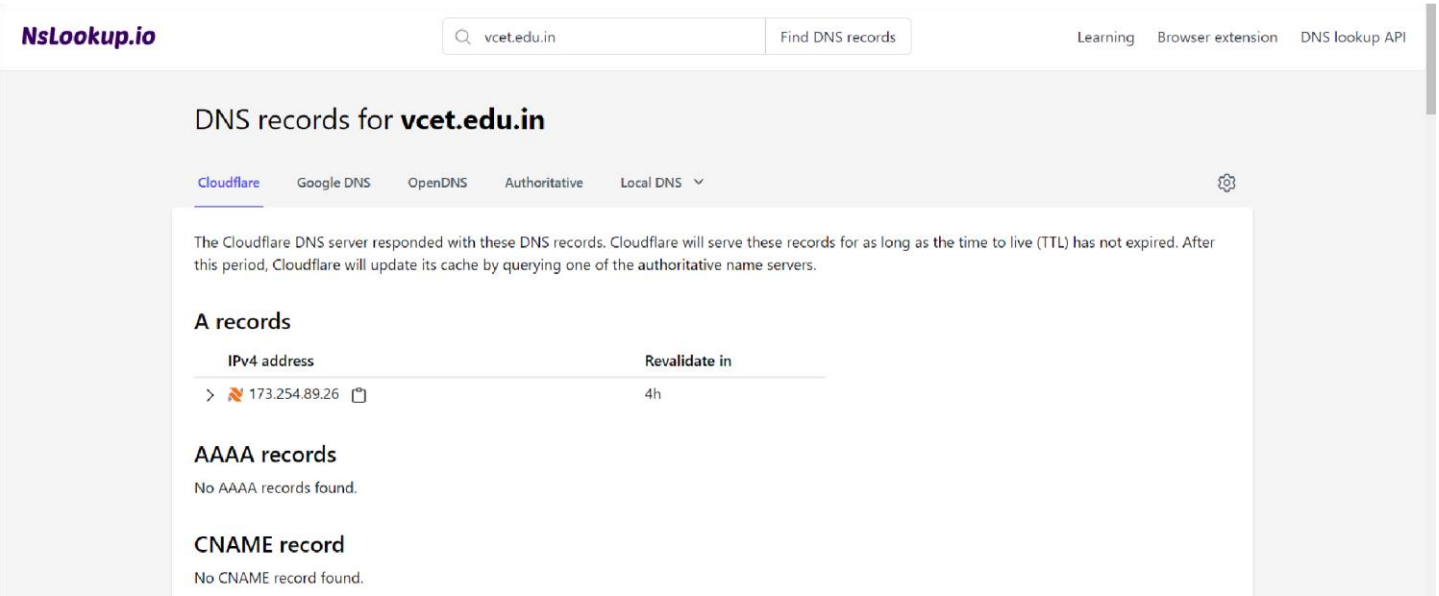


Nslookup: `nslookup` stands for "Name Server Lookup". It's a command-line tool used to query DNS (Domain Name System) servers to obtain DNS-related information, such as IP addresses associated with domain names or vice versa.

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.



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.