**EXPERIMENT 06**

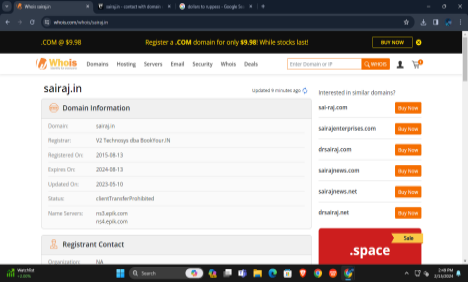
**Aim:-** Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.

**Theory:-**

**WHOIS:**

A Whois domain lookup allows you to trace the ownership and tenure of a domain name. Similar to how all houses are registered with a governing authority, all domain name registries maintain a record of information about every domain name purchased through them, along with who owns it, and the date till which it has been purchased.



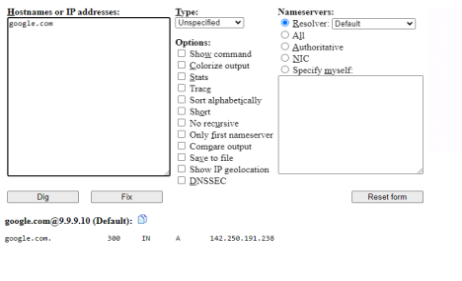
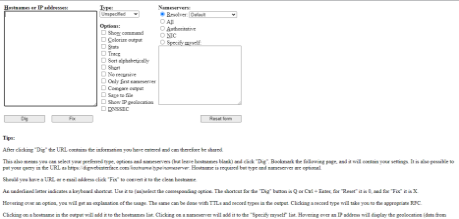


**Dig:**

The dig (domain information groper) command is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the queried name server(s). Most DNS administrators use the dig command to troubleshoot DNS problems because of its flexibility, ease of use, and clarity of output.

Although dig is normally used with command-line arguments, it also has a batch mode for reading lookup requests from a file.

The dig command provides a number of query options that affect the way in which lookups are made and the results displayed.



**Traceroute:**

A traceroute provides a map of how data on the internet travels from its source to its destination. When you connect with a website, the data you get must travel across multiple devices and networks along the way, particularly routers.

**Using command prompt:**

Type 'tracert' followed by a space and the domain name or IP address (for example: tracert example.com)

|  |
| --- |
|  |

**Nslookup:**

Nslookup is the name of a program that lets users enter a host name and find out the corresponding IP address or domain name system (DNS) record. Users can also enter a command in nslookup to do a reverse DNS lookup and find the host name for a specified IP address.

Network administrators use nslookup to troubleshoot server connections or for security reasons.