**Experiment No 10**

**Aim:** To Study the use of network reconnaissance tools like WHOIS, dig, tracert, nslookup.

**Theory**:

**WHOIS**

WHOIS is a TCP-based query and response protocol that is commonly used to provide information services to Internet users. It returns information about the registered Domain Names, an IP address block, Name Servers and a much wider range of information services.

To use WHOIS in windows we need to install WhoIs from Microsoft site and extract its folder and to switch to its directory in cmd.

**Dig**

Dig (Domain Information Groper) is a powerful command-line tool for querying DNS name servers.

The dig command, allows you to query information about various DNS records, including host addresses, mail exchanges, and name servers. It is the most commonly used tool among system administrators for troubleshooting DNS problems because of its flexibility and ease of use.

To use dig in windows we need to install Bind and set path for it. Bind also provides other commands support such as tracert and nslookup.

**Tracert**

This diagnostic tool determines the path taken to a destination by sending Internet Control Message Protocol (ICMP) echo Request or ICMPv6 messages to the destination with incrementally increasing time to live (TTL) field values. Each router along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it. Effectively, the TTL is a maximum link counter. When the TTL on a packet reaches 0, the router is expected to return an ICMP time Exceeded message to the source computer.

This command determines the path by sending the first echo Request message with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum number of hops is reached. The maximum number of hops is 30 by default and can be specified using the **-h** parameter.

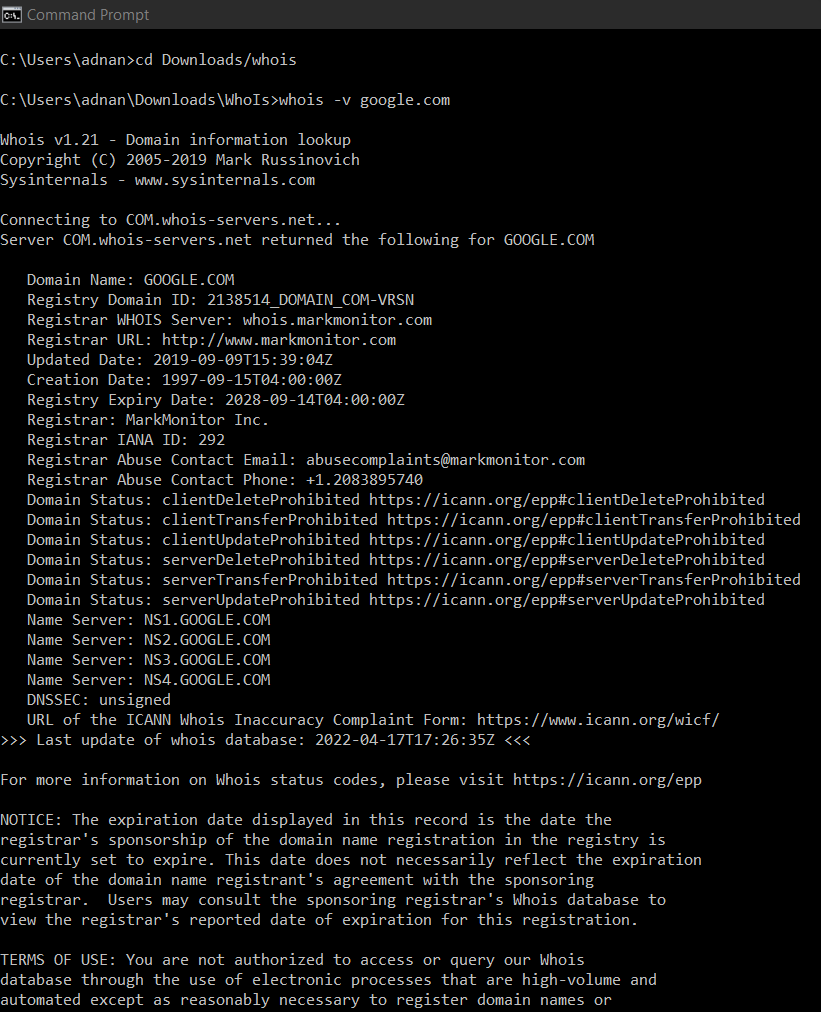
**Nslookup**

The nslookup command queries internet domain name servers in two modes. Interactive mode allows you to query name servers for information about various hosts and domains, or to print a list of the hosts in a domain. In noninteractive mode, the names and requested information are printed for a specified host or domain.

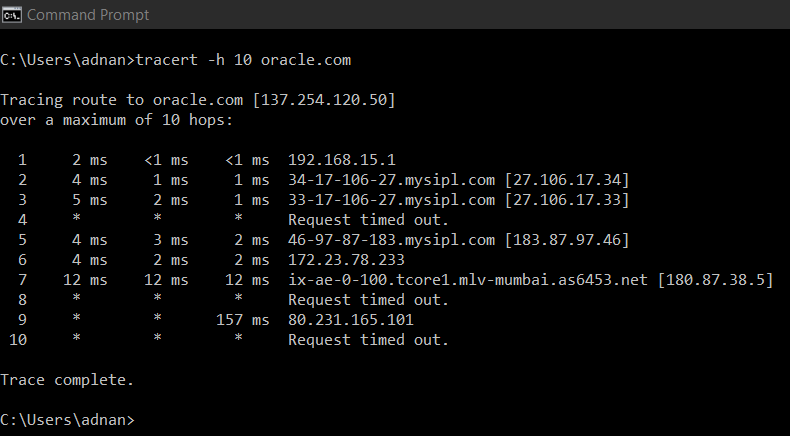
The nslookup command enters interactive mode when no arguments are given, or when the first argument is a - (minus sign) and the second argument is the host name or internet address of a name server. When no arguments are given, the command queries the default name server. The nslookup command enters non-interactive mode when you give the name or internet address of the host to be looked up as the first argument. The optional second argument specifies the host name or address of a name server.

**Output**:

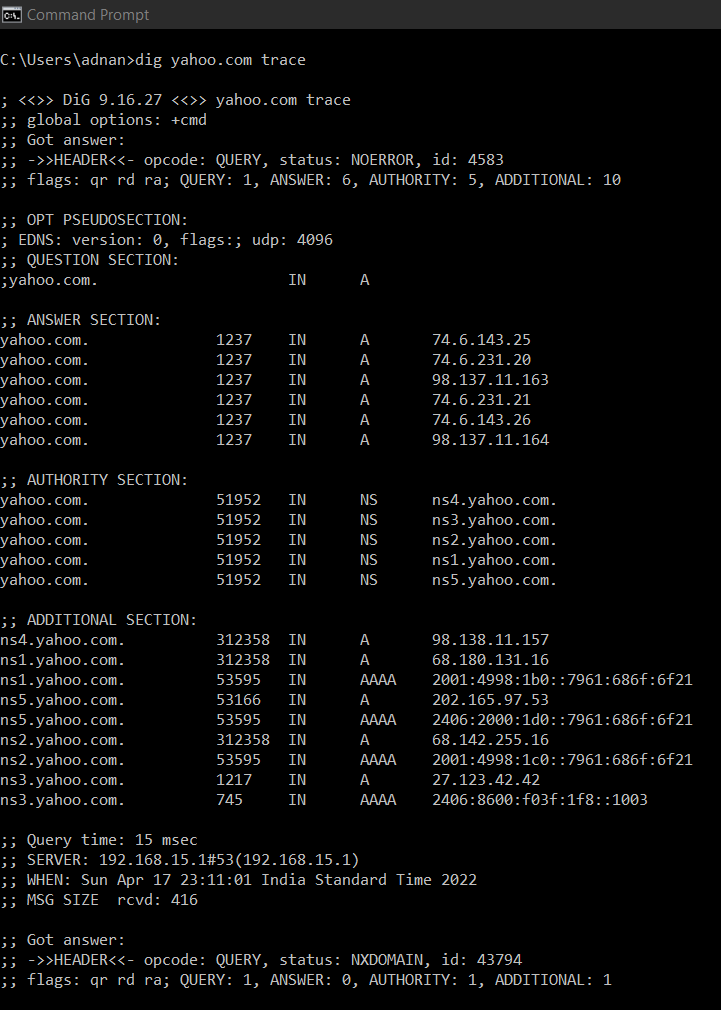
**Whois**



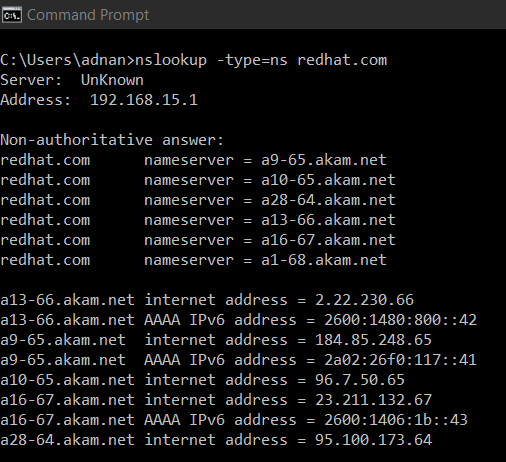
**Tracert**

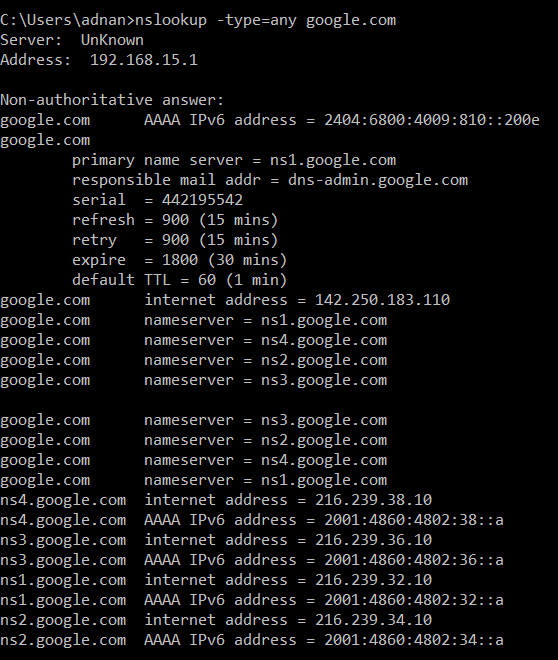
****

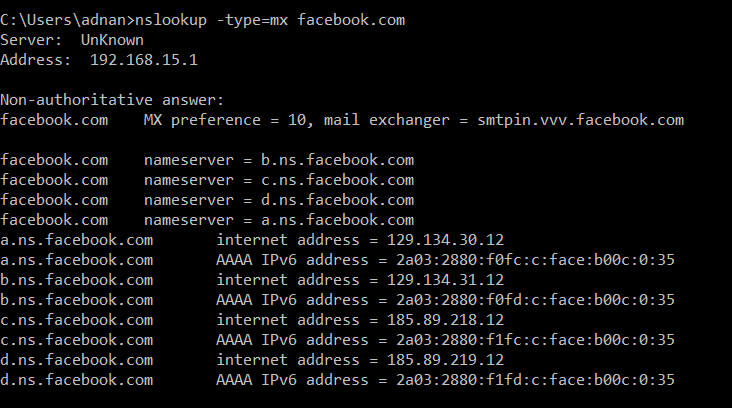
**Dig**

****

**Nslookup**

****

****

****