# **Name: Abdurrahman Qureshi**

# **Roll No: 242466**

Practical No: 3

Date Of Performance: 21/07/2025

Aim: To Study of any Two network reconnaissance tools.

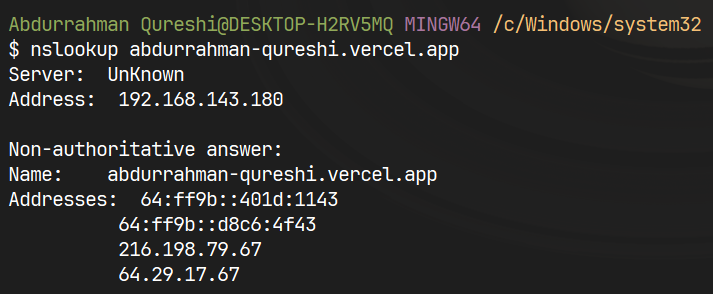
1. nslookup

The nslookup command queries DNS servers to resolve domain names to IP addresses and vice versa.

**Parameters:**

* server: Specify a DNS server.
* type: Set query type (A, MX, NS, etc.).
* debug: Enable detailed debugging.
* timeout: Adjust query timeout.
* port: Change the DNS port.

Example: nslookup -type=MX example.com

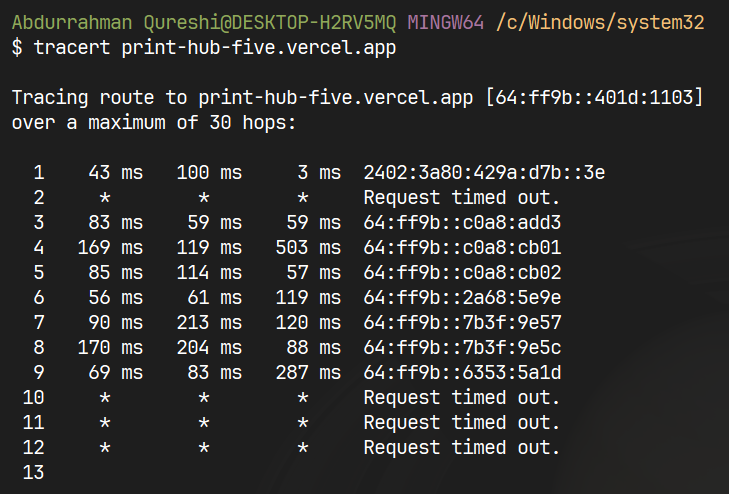


1. tracert

Traces the network path to a host, showing hops and latency.

Parameters:

* -d: Skip DNS resolution (faster).
* -h max\_hops: Set max hops (default: 30).
* -w timeout: Adjust timeout per hop.  
  Example: tracert google.com.

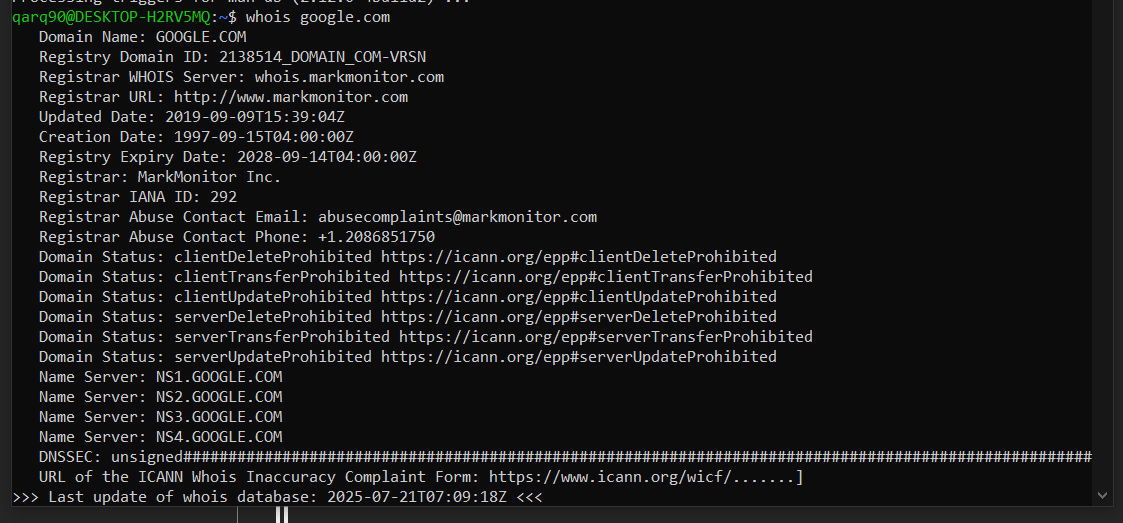


1. whois

The whois command retrieves domain or IP registration details (owner, expiry, registrar).

Parameters:

* -h: Specify WHOIS server.
* -a: Show all fields.
* domain/IP: Query target (e.g., whois example.com).



1. dig (Domain Information Groper)

dig queries DNS records (A, MX, NS) with detailed output.

Parameters:

* @server: Use a specific DNS server.
* +short: Concise output.
* -t TYPE: Query type (A, MX, TXT).  
  Example: dig example.com MX.

