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

```
Abdurrahman Qureshi@DESKTOP-H2RV5MQ MINGW64 /c/Windows/system32
$ nslookup abdurrahman-qureshi.vercel.app
Server:  UnKnown
Address:  192.168.143.180

Non-authoritative answer:
Name:    abdurrahman-qureshi.vercel.app
Addresses:  64:ff9b::401d:1143
          64:ff9b::d8c6:4f43
          216.198.79.67
          64.29.17.67
```

2) tracert

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

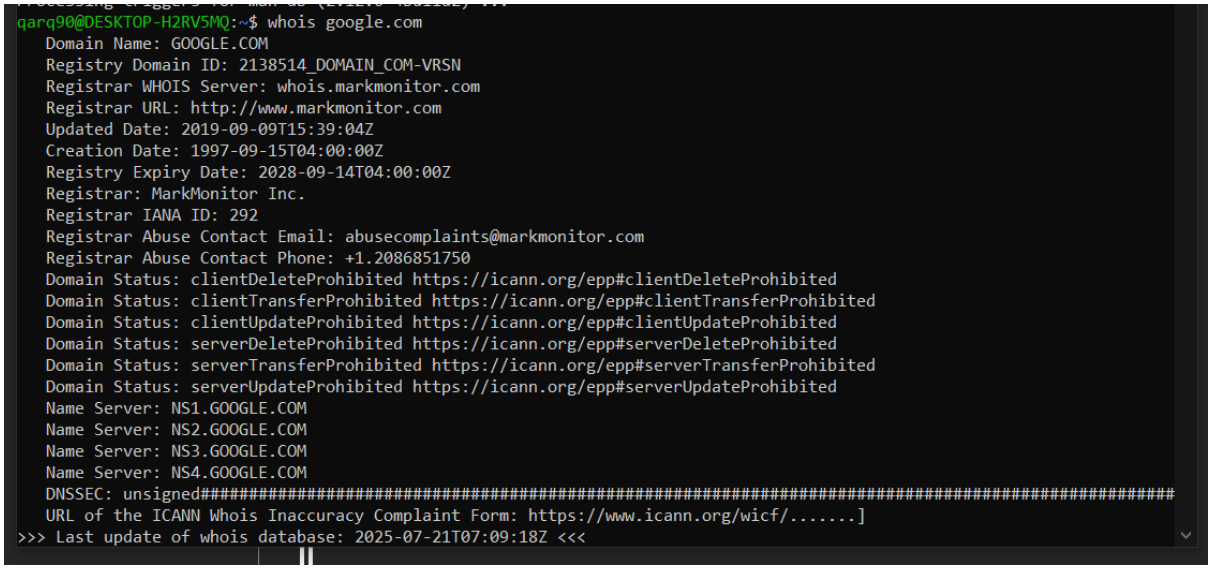
- -d: Skip DNS resolution (faster).
- -h max_hops: Set max hops (default: 30).
- -w timeout: Adjust timeout per hop.
  Example: tracert google.com.

```
Abdurrahman Qureshi@DESKTOP-H2RV5MQ MINGW64 /c/Windows/system32
$ tracert print-hub-five.vercel.app

Tracing route to print-hub-five.vercel.app [64:ff9b::401d:1103]
over a maximum of 30 hops:

  1    43 ms   100 ms     3 ms  2402:3a80:429a:d7b::3e
  2     *        *        *     Request timed out.
  3    83 ms    59 ms    59 ms  64:ff9b::c0a8:add3
  4   169 ms   119 ms   503 ms  64:ff9b::c0a8:cb01
  5    85 ms   114 ms    57 ms  64:ff9b::c0a8:cb02
  6    56 ms    61 ms   119 ms  64:ff9b::2a68:5e9e
  7    90 ms   213 ms   120 ms  64:ff9b::7b3f:9e57
  8   170 ms   204 ms    88 ms  64:ff9b::7b3f:9e5c
  9    69 ms    83 ms   287 ms  64:ff9b::6353:5a1d
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13
```

3) 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).

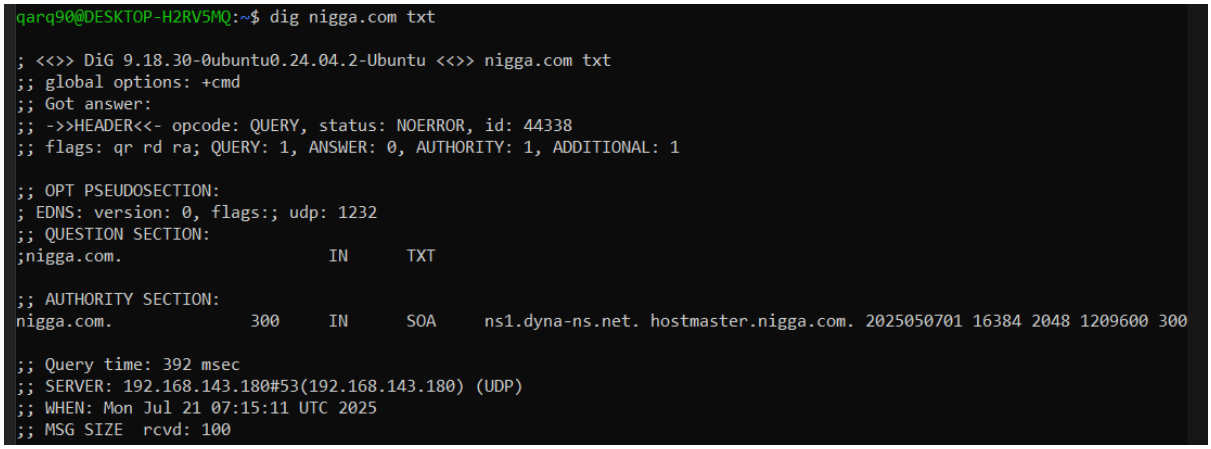


4) dig (Domain Information Groper)

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.



```
qarq90@DESKTOP-H2RV5MQ:~$ dig nigga.com

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> nigga.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12802
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;nigga.com.                     IN      A

;; ANSWER SECTION:
nigga.com.              300     IN      A       188.214.128.77

;; Query time: 555 msec
;; SERVER: 192.168.143.180#53(192.168.143.180) (UDP)
;; WHEN: Mon Jul 21 07:14:12 UTC 2025
;; MSG SIZE  rcvd: 54
```

```
qarq90@DESKTOP-H2RV5MQ:~$ dig nigga.com A

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> nigga.com A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49395
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;nigga.com.                     IN      A

;; ANSWER SECTION:
nigga.com.              283     IN      A       188.214.128.77

;; Query time: 7 msec
;; SERVER: 192.168.143.180#53(192.168.143.180) (UDP)
;; WHEN: Mon Jul 21 07:14:29 UTC 2025
;; MSG SIZE  rcvd: 43
```

```
qarq90@DESKTOP-H2RV5MQ:~$ dig nigga.com AAAA

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> nigga.com AAAA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14157
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;nigga.com.                     IN      AAAA

;; ANSWER SECTION:
nigga.com.              300     IN      AAAA    64:ff9b::bcd6:804d

;; Query time: 585 msec
;; SERVER: 192.168.143.180#53(192.168.143.180) (UDP)
;; WHEN: Mon Jul 21 07:14:34 UTC 2025
;; MSG SIZE  rcvd: 66
```

```
qarq90@DESKTOP-H2RV5MQ:~$ dig nigga.com ns

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> nigga.com ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41044
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;nigga.com.                     IN      NS

;; ANSWER SECTION:
nigga.com.              300     IN      NS      ns2.dyna-ns.net.
nigga.com.              300     IN      NS      ns1.dyna-ns.net.

;; Query time: 702 msec
;; SERVER: 192.168.143.180#53(192.168.143.180) (UDP)
;; WHEN: Mon Jul 21 07:15:23 UTC 2025
;; MSG SIZE  rcvd: 85
```

Performance (7M)	Journal (3M)	Lab Ethics (2M)	Attendance (3M)	Total (15M)	Faculty Signature