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).

```
qarq90@DESKTOP-H2RV5MQ:~$ whois google.com
    Domain Name: GOOGLE.COM
    Registry Domain ID: 2138514_DOMAIN_COM-VRSN
    Registrar WHOIS Server: whois.markmonitor.com
    Registrar URL: http://www.markmonitor.com
    Updated Date: 2019-09-09T15:39:04Z
    Creation Date: 1997-09-15T04:00:00Z
    Registry Expiry Date: 2028-09-14T04:00:00Z
    Registrar: MarkMonitor Inc.
    Registrar IANA ID: 292
    Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
    Registrar Abuse Contact Phone: +1.2086851750
    Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
    Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
    Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
    Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
    Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
    Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
    Name Server: NS1.GOOGLE.COM
    Name Server: NS2.GOOGLE.COM
    Name Server: NS3.GOOGLE.COM
    Name Server: NS4.GOOGLE.COM
    DNSSEC: unsigned######################################################################################
    URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/.......]
>>> Last update of whois database: 2025-07-21T07:09:18Z <<<
```

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 txt

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> nigga.com txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44338
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
nigga.com.              300     IN      SOA     ns1.dyna-ns.net. hostmaster.nigga.com. 2025050701 16384 2048 1209600 300

;; Query time: 392 msec
;; SERVER: 192.168.143.180#53(192.168.143.180) (UDP)
;; WHEN: Mon Jul 21 07:15:11 UTC 2025
;; MSG SIZE  rcvd: 100
```

```
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
```