2.1 Aim:

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

2.2 Course Outcome:

- Study and describe the system security, malicious softwares and the Network layer security, Transport layer security and application layer security.

2.3 Lab Objective:

- Use network reconnaissance tools like WHOIS, dig, traceroute, and nslookup to gather information about IP addresses, domains, routing paths, and domain registrars.
- Understand how these tools work and their significance in network diagnostics and security analysis.

2.4 Requirement:

- Command-line access (Terminal/Command Prompt).
- Installed network tools like **WHOIS**, **dig**, **traceroute**, and **nslookup** on Windows.

2.5 Theory: Network reconnaissance tools like **WHOIS**, **dig**, **traceroute**, and **nslookup** are commonly used by IT professionals, ethical hackers, and network administrators to gather information about networks and domain registrars. These tools help understand the structure, ownership, and routing of internet resources. Below is an explanation of each tool and how it is used:

1. WHOIS

Purpose:

- WHOIS is a query and response protocol that retrieves domain registration information from a public database.
- It provides details about domain ownership, registrar, registration date, expiration date, and contact information (if not hidden for privacy).

Use Cases:

- **Network Investigation**: Determine the owner of a suspicious domain.
- **Domain Management**: Verify registration details for a domain you own.
- **Incident Response**: Track down the owner of a domain involved in malicious activity.

Command Example:

whois example.com

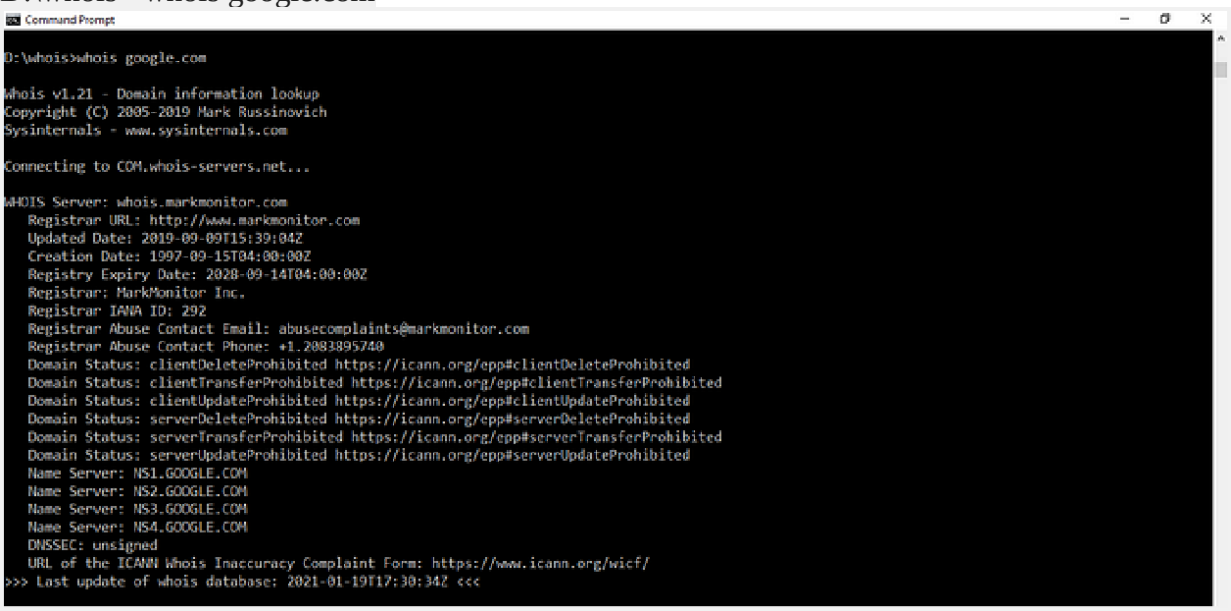
Let's do it. After installation and adding path, It will work on any version of Windows including Windows 10:

1. Download Whois Program from Microsoft's site.
2. Create a folder in your computer(eg. whois) and Extract the content of the downloaded zip file to your created folder.
3. example — D:\whois
4. You will find whois.exe and whois64.exe under your extracted location. In my case it is D:\whois\whois.exe and D:\whois\whois64.exe
5. Open command prompt. (Press Win+R keys and type 'cmd' then hit enter)
6. Navigate to the directory where you extracted the whois.exe. In my case I will type

> cd D:\whois

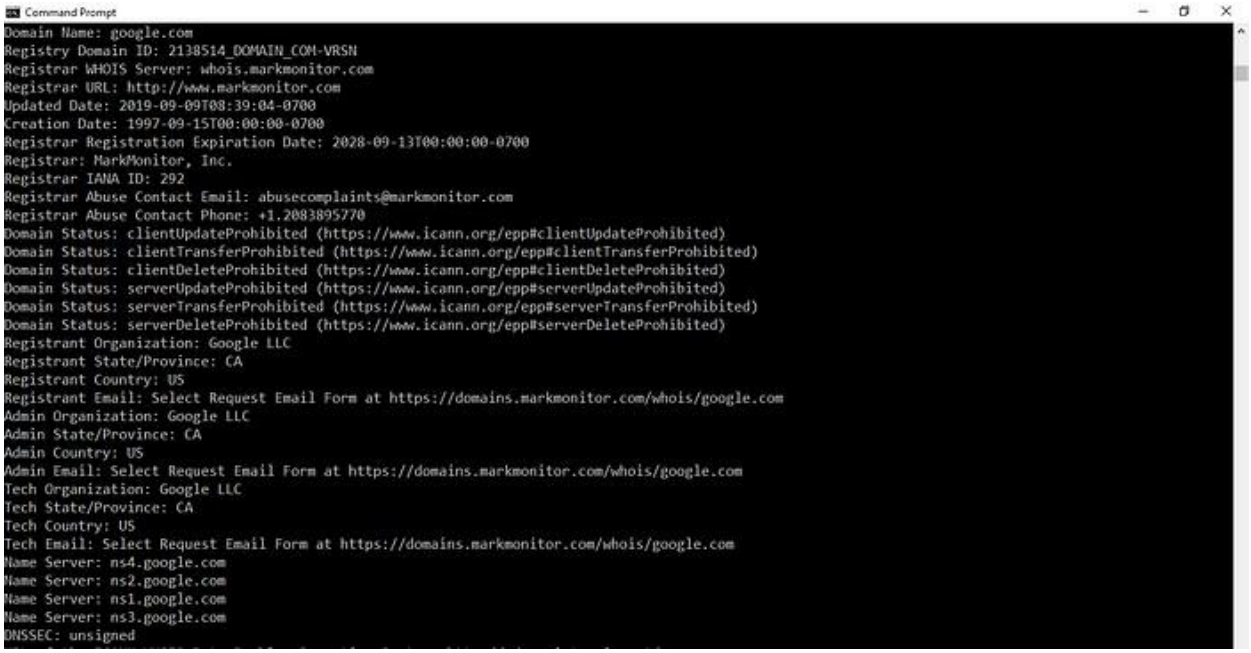
1. Run 'whois' command now and it should work. Example —

D:\whois> whois google.com



```
Command Prompt

D:\whois>whois google.com

Whois v1.21 - Domain information lookup
Copyright (C) 2005-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to COM.whois-servers.net...

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: +1.2083895740
   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: 2021-01-19T17:30:34Z <<<
```

google.com



```
Command Prompt
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: 2019-09-09T08:39:04-0700
Creation Date: 1997-09-15T00:00:00-0700
Registrar Registration Expiration Date: 2028-09-13T00:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Google LLC
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Admin Organization: Google LLC
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Tech Organization: Google LLC
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Name Server: ns4.google.com
Name Server: ns2.google.com
Name Server: ns1.google.com
Name Server: ns3.google.com
DNSSEC: unsigned
```

google.com

Using the method shown above, you will now be able to run ‘whois’ command from the directory where you stored the program.

However, if you want to run the ‘whois’ command from anywhere then you can add the directory (in my case D:\whois) to the system PATH environment variable.

2. dig (Domain Information Groper)

Purpose:

- dig is a command-line tool for querying DNS servers.
- It retrieves DNS records, such as A (address), MX (mail exchange), TXT, NS (name server), and more.

Use Cases:

- **DNS Troubleshooting**: Check if a domain resolves to the correct IP address.
- **Security Analysis**: Investigate DNS misconfigurations or unusual record entries.
- **Reconnaissance**: Gather DNS data for domains of interest.

Command Example:

```
dig example.com
dig example.com A
dig example.com MX
```

3. Traceroute

Purpose:

- Traceroute tracks the path packets take from the source to the destination.
- It identifies the hops (intermediate devices/routers) and measures the latency between each hop.

Use Cases:

- **Network Diagnostics**: Locate bottlenecks or failures in a network path.
- **Routing Analysis**: Understand how data travels through the internet.
- **Performance Testing**: Measure latency and identify inefficient routes.

Command Example:

```
traceroute example.com
tracert example.com
```

4. nslookup

Purpose:

- nslookup is used to query DNS servers for domain-related information.
- It is simpler than dig and is often included in basic network toolsets.

Use Cases:

- **Resolve Domain Names**: Convert domain names to IP addresses and vice versa.
- **Check Nameserver Configurations**: Ensure a domain's DNS records are properly configured.
- **Troubleshooting**: Diagnose issues with DNS resolution.

Command Example:

```
nslookup example.com
nslookup example.com 8.8.8.8
```

Output Includes:

- Non-authoritative answer (resolved IP address)
- Authoritative nameserver information (if queried for NS records)

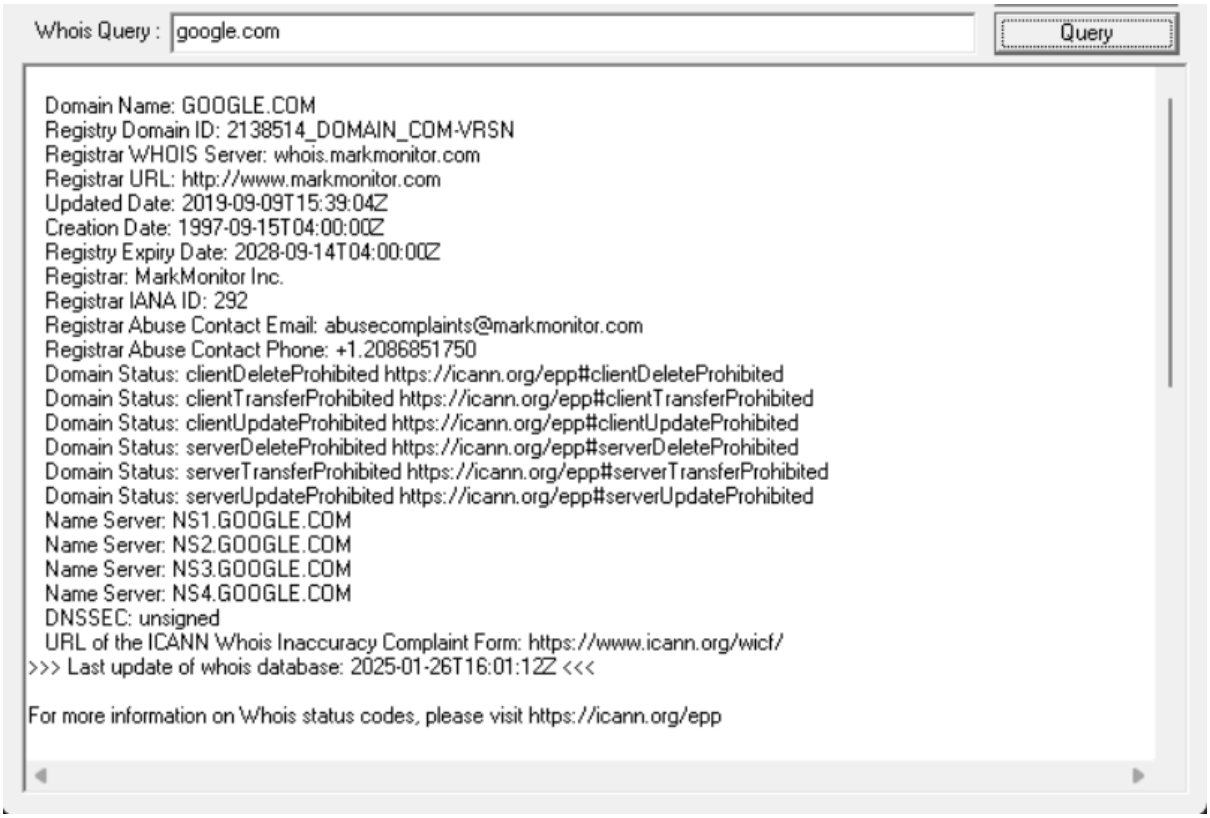
Key Differences Between the Tools

Tool	Primary Function	Key Use Case
WHOIS	Domain registration information	Identify domain owners
dig	DNS record lookup	Retrieve and analyze DNS records
traceroute	Path analysis of packet travel	Diagnose network routing issues
nslookup	Basic DNS resolution	Quick DNS troubleshooting

Practical Applications

1. **Ethical Hacking**: Identify domain ownership, DNS configurations, and infrastructure for penetration testing.
2. **Network Troubleshooting**: Diagnose DNS failures, IP routing issues, and packet delivery delays.
3. **Incident Response**: Investigate malicious domains or IPs involved in cyberattacks.
4. **Network Design and Optimization**: Understand network paths and optimize routing for better performance.

2.7 Result :



```
C:\>tracert google.com

Tracing route to google.com [2404:6800:4002:815::200e]
over a maximum of 30 hops:

  1     3 ms     4 ms     2 ms  2409:40c0:4f:99da::9b
  2    28 ms    17 ms    31 ms  2405:200:5201:0:3924:0:3:69
  3    17 ms    36 ms    23 ms  2405:200:5201:0:3925::ff06
  4    16 ms    36 ms    38 ms  2405:200:802:1513:61::4
  5     *        *        *     Request timed out.
  6    14 ms    37 ms    31 ms  2405:200:801:200::1fba
  7     *        *        *     Request timed out.
  8    22 ms    39 ms    38 ms  2001:4860:1:1::331c
  9    22 ms    37 ms    38 ms  2001:4860:1:1::331c
 10    48 ms    21 ms    52 ms  2001:4860:0:1::87f7
 11     *        *        *     Request timed out.
 12    53 ms    38 ms    38 ms  2001:4860::9:4001:d9e7
 13    65 ms    76 ms    77 ms  2001:4860::9:4001:67bc
 14    58 ms    63 ms    82 ms  2001:4860::9:4001:67bd
 15     *        *        *     Request timed out.
 16    39 ms    60 ms    41 ms  2001:4860:0:1::2b4f
 17    40 ms    68 ms    48 ms  del11s10-in-x0e.1e100.net [2404:6800:4002:815::200e]

Trace complete.

C:\>nslookup google.com
Server:  UnKnown
Address:  192.168.144.216

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4002:82c::200e
          142.250.183.78
```

```
C:\>nslookup google.com 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4009:826::200e
          142.251.42.78
```

2.8 Conclusion

The practical highlighted the importance of network reconnaissance tools like WHOIS, dig, traceroute, and nslookup for gathering domain and network information. These tools are essential for diagnosing issues, improving network security, and supporting ethical hacking efforts.