**Experiment 7**

**Date of Performance :**  **Date of Submission:**

**SAP Id: 60004190057** **Name : Junaid Altaf Girkar**

**Div:** **A** **Batch : A4**

**Aim of Experiment**

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

**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.

| **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: +1.2086851750  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: 2022-06-02T15:50:49Z <<<  For more information on Whois status codes, please visit https://icann.org/epp  NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.  TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or modify existing registrations; the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accuracy. By submitting a Whois query, you agree to abide by the following terms of use: You agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of VeriSign. You agree not to use electronic processes that are automated and high-volume to access or query the Whois database except as reasonably necessary to register domain names or modify existing registrations. VeriSign reserves the right to restrict your access to the Whois database in its sole discretion to ensure operational stability. VeriSign may restrict or terminate your access to the Whois database for failure to abide by these terms of use. VeriSign reserves the right to modify these terms at any time.  The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.  Connecting to whois.markmonitor.com...  WHOIS Server: whois.markmonitor.com Registrar URL: http://www.markmonitor.com Updated Date: 2019-09-09T15:39:04+0000 Creation Date: 1997-09-15T07:00:00+0000 Registrar Registration Expiration Date: 2028-09-13T07:00:00+0000 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: ns1.google.com Name Server: ns4.google.com Name Server: ns3.google.com Name Server: ns2.google.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2022-06-02T15:43:07+0000 <<<  For more information on WHOIS status codes, please visit:  https://www.icann.org/resources/pages/epp-status-codes  If you wish to contact this domainΓÇÖs Registrant, Administrative, or Technical contact, and such email address is not visible above, you may do so via our web form, pursuant to ICANNΓÇÖs Temporary Specification. To verify that you are not a robot, please enter your email address to receive a link to a page that facilitates email communication with the relevant contact(s).  Web-based WHOIS:  https://domains.markmonitor.com/whois  If you have a legitimate interest in viewing the non-public WHOIS details, send your request and the reasons for your request to whoisrequest@markmonitor.com and specify the domain name in the subject line. We will review that request and may ask for supporting documentation and explanation.  The data in MarkMonitorΓÇÖs WHOIS database is provided for information purposes, and to assist persons in obtaining information about or related to a domain nameΓÇÖs registration record. While MarkMonitor believes the data to be accurate, the data is provided "as is" with no guarantee or warranties regarding its accuracy.  By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to:  (1) allow, enable, or otherwise support the transmission by email, telephone, or facsimile of mass, unsolicited, commercial advertising, or spam; or  (2) enable high volume, automated, or electronic processes that send queries, data, or email to MarkMonitor (or its systems) or the domain name contacts (or its systems).  MarkMonitor reserves the right to modify these terms at any time.  By submitting this query, you agree to abide by this policy.  MarkMonitor Domain Management(TM) Protecting companies and consumers in a digital world.  Visit MarkMonitor at https://www.markmonitor.com Contact us at +1.8007459229 In Europe, at +44.02032062220 --   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: 2019-09-09T15:39:04+0000 Creation Date: 1997-09-15T07:00:00+0000 Registrar Registration Expiration Date: 2028-09-13T07:00:00+0000 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: ns1.google.com Name Server: ns4.google.com Name Server: ns3.google.com Name Server: ns2.google.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2022-06-02T15:43:07+0000 <<<  For more information on WHOIS status codes, please visit:  https://www.icann.org/resources/pages/epp-status-codes  If you wish to contact this domainΓÇÖs Registrant, Administrative, or Technical contact, and such email address is not visible above, you may do so via our web form, pursuant to ICANNΓÇÖs Temporary Specification. To verify that you are not a robot, please enter your email address to receive a link to a page that facilitates email communication with the relevant contact(s).  Web-based WHOIS:  https://domains.markmonitor.com/whois  If you have a legitimate interest in viewing the non-public WHOIS details, send your request and the reasons for your request to whoisrequest@markmonitor.com and specify the domain name in the subject line. We will review that request and may ask for supporting documentation and explanation.  The data in MarkMonitorΓÇÖs WHOIS database is provided for information purposes, and to assist persons in obtaining information about or related to a domain nameΓÇÖs registration record. While MarkMonitor believes the data to be accurate, the data is provided "as is" with no guarantee or warranties regarding its accuracy.  By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to:  (1) allow, enable, or otherwise support the transmission by email, telephone, or facsimile of mass, unsolicited, commercial advertising, or spam; or  (2) enable high volume, automated, or electronic processes that send queries, data, or email to MarkMonitor (or its systems) or the domain name contacts (or its systems).  MarkMonitor reserves the right to modify these terms at any time.  By submitting this query, you agree to abide by this policy.  MarkMonitor Domain Management(TM) Protecting companies and consumers in a digital world.  Visit MarkMonitor at https://www.markmonitor.com Contact us at +1.8007459229 In Europe, at +44.02032062220 --** |
| --- |

**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

| **C:\Users\DELL>dig google.com  ; <<>> DiG 9.16.29 <<>> google.com ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62757 ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9  ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 4096 ;; QUESTION SECTION: ;google.com. IN A  ;; ANSWER SECTION: google.com. 157 IN A 142.251.42.14  ;; AUTHORITY SECTION: google.com. 35249 IN NS ns4.google.com. google.com. 35249 IN NS ns2.google.com. google.com. 35249 IN NS ns1.google.com. google.com. 35249 IN NS ns3.google.com.  ;; ADDITIONAL SECTION: ns1.google.com. 206783 IN A 216.239.32.10 ns1.google.com. 293783 IN AAAA 2001:4860:4802:32::a ns4.google.com. 31667 IN A 216.239.38.10 ns4.google.com. 31667 IN AAAA 2001:4860:4802:38::a ns3.google.com. 31667 IN A 216.239.36.10 ns3.google.com. 31667 IN AAAA 2001:4860:4802:36::a ns2.google.com. 204464 IN A 216.239.34.10 ns2.google.com. 204464 IN AAAA 2001:4860:4802:34::a  ;; Query time: 6 msec ;; SERVER: 192.168.1.1#53(192.168.1.1) ;; WHEN: Thu Jun 02 21:30:08 India Standard Time 2022 ;; MSG SIZE rcvd: 303** |
| --- |

| **C:\Users\DELL>dig 142.251.42.14  ; <<>> DiG 9.16.29 <<>> 142.251.42.14 ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 38521 ;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1  ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 4096 ;; QUESTION SECTION: ;142.251.42.14. IN A  ;; AUTHORITY SECTION: . 10800 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2022060200 1800 900 604800 86400  ;; Query time: 0 msec ;; SERVER: 192.168.1.1#53(192.168.1.1) ;; WHEN: Thu Jun 02 21:35:01 India Standard Time 2022 ;; MSG SIZE rcvd: 117** |
| --- |

**NSLOOKUP:**

Nslookup (stands for “Name Server Lookup”) is a useful command for getting information from DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS related problems. nslookup followed by the domain name will display the “A Record” (IP Address) of the domain. Use this command to find the address record for a domain. It queries to domain name servers and get the details.

| C:\Users\junai>nslookup amazon.com Server: UnKnown Address: 192.168.0.1  Non-authoritative answer: Name: amazon.com Addresses: 176.32.103.205  54.239.28.85  205.251.242.103 |
| --- |

**SOA record** (start of authority), provides the authoritative information about the domain, the e-mail address of the domain admin, the domain serial number, etc

| C:\Users\junai>nslookup -type=soa amazon.com Server: UnKnown Address: 192.168.0.1  Non-authoritative answer: amazon.com  primary name server = dns-external-master.amazon.com  responsible mail addr = root.amazon.com  serial = 2010158906  refresh = 180 (3 mins)  retry = 60 (1 min)  expire = 3024000 (35 days)  default TTL = 60 (1 min)  amazon.com nameserver = pdns6.ultradns.co.uk amazon.com nameserver = pdns1.ultradns.net amazon.com nameserver = ns1.p31.dynect.net amazon.com nameserver = ns2.p31.dynect.net amazon.com nameserver = ns3.p31.dynect.net amazon.com nameserver = ns4.p31.dynect.net ns1.p31.dynect.net internet address = 108.59.161.31 ns2.p31.dynect.net internet address = 108.59.162.31 ns3.p31.dynect.net internet address = 108.59.163.31 ns4.p31.dynect.net internet address = 108.59.164.31 pdns1.ultradns.net internet address = 204.74.108.1 pdns6.ultradns.co.uk internet address = 204.74.115.1 ns1.p31.dynect.net AAAA IPv6 address = 2600:2000:2210::31 ns2.p31.dynect.net AAAA IPv6 address = 2600:2000:2220::31 ns3.p31.dynect.net AAAA IPv6 address = 2600:2000:2230::31 ns4.p31.dynect.net AAAA IPv6 address = 2600:2000:2240::31 pdns1.ultradns.net AAAA IPv6 address = 2001:502:f3ff::1 pdns6.ultradns.co.uk AAAA IPv6 address = 2610:a1:1017::1 |
| --- |

**NS (Name Server)** record maps a domain name to a list of DNS servers authoritative for that domain. It will output the name serves which are associated with the given domain.

| C:\Users\junai>nslookup -type=ns amazon.com Server: UnKnown Address: 192.168.0.1  Non-authoritative answer: amazon.com nameserver = pdns1.ultradns.net amazon.com nameserver = ns4.p31.dynect.net amazon.com nameserver = pdns6.ultradns.co.uk amazon.com nameserver = ns1.p31.dynect.net amazon.com nameserver = ns2.p31.dynect.net amazon.com nameserver = ns3.p31.dynect.net  ns1.p31.dynect.net internet address = 108.59.161.31 ns2.p31.dynect.net internet address = 108.59.162.31 ns3.p31.dynect.net internet address = 108.59.163.31 ns4.p31.dynect.net internet address = 108.59.164.31 pdns1.ultradns.net internet address = 204.74.108.1 pdns6.ultradns.co.uk internet address = 204.74.115.1 ns1.p31.dynect.net AAAA IPv6 address = 2600:2000:2210::31 ns2.p31.dynect.net AAAA IPv6 address = 2600:2000:2220::31 ns3.p31.dynect.net AAAA IPv6 address = 2600:2000:2230::31 ns4.p31.dynect.net AAAA IPv6 address = 2600:2000:2240::31 pdns1.ultradns.net AAAA IPv6 address = 2001:502:f3ff::1 pdns6.ultradns.co.uk AAAA IPv6 address = 2610:a1:1017::1 |
| --- |

**TRACEROUTE**:

Traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes. The first column corresponds to the hop count. The second column represents the address of that hop and after that, you see three space-separated time in milliseconds. the traceroute command sends three packets to the hop and each of the time refers to the time taken by the packet to reach the hop. In windows, alternative for traceroute command is tracert.

| C:\Users\junai>tracert amazon.com  Tracing route to amazon.com [205.251.242.103] over a maximum of 30 hops:   1 3 ms 3 ms 2 ms 192.168.0.1  2 2 ms 1 ms 3 ms 42-200.59.103.n4uspl.net [103.59.200.42]  3 3 ms 2 ms 3 ms 41-200.59.103.n4uspl.net [103.59.200.41]  4 \* \* 3 ms 254-200.59.103.n4uspl.net [103.59.200.254]  5 6 ms 5 ms 6 ms 123.252.244.1  6 7 ms 4 ms 4 ms 10.0.10.209  7 6 ms 4 ms 5 ms 10.124.253.101  8 \* \* 8 ms 10.118.143.9  9 7 ms 5 ms 5 ms 115.113.165.21.static-mumbai.vsnl.net.in [115.113.165.21]  10 9 ms 7 ms 5 ms 172.23.78.237  11 5 ms 4 ms 5 ms ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]  12 251 ms 201 ms 200 ms if-ae-2-2.tcore2.mlv-mumbai.as6453.net [180.87.38.2]  13 \* \* \* Request timed out.  14 \* 401 ms \* if-ae-66-8.tcore3.nto-newyork.as6453.net [80.231.130.195]  15 207 ms \* 202 ms if-be-2-2.ecore1.n75-newyork.as6453.net [66.110.96.62]  16 211 ms 217 ms 223 ms if-ae-57-2.tcore1.n75-newyork.as6453.net [66.110.96.58]  17 200 ms 200 ms 347 ms 66.110.96.157  18 \* \* \* Request timed out.  19 \* \* \* Request timed out.  20 \* \* \* Request timed out.  21 \* \* \* Request timed out.  22 \* \* \* Request timed out.  23 \* \* \* Request timed out.  24 \* \* \* Request timed out.  25 \* \* \* Request timed out.  26 \* \* \* Request timed out.  27 \* \* \* Request timed out.  28 \* \* \* Request timed out.  29 \* \* \* Request timed out.  30 \* \* \* Request timed out.  Trace complete. |
| --- |

**CONCLUSION**

Thus, we have successfully implemented and studied the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.