# Experiment - 4 Study the use of network reconnaissance tools like WHOIS, dig, traceroute, and analyse the performance of the two protocols. Use crypt APIs


**Name:** Shaikh Shadab **Rollno :** 17DCO74

**Class :** TE.CO **Batch :** B3


## 1. Traceroute

Traceroute prints the route that packets take to a network host. It is used to find network path from machine to server.

The server name above is destination name or IP address.

**Syntax**: traceroute <server name>

**Eg**: traceroute command with google.com and amazon.com

```
codept@codept-22 ~/Desktop $ traceroute google.com
traceroute to google.com (216.58.203.142), 30 hops max, 60 byte packets
 1  172.16.16.1 (172.16.16.1)  0.304 ms  0.301 ms  0.295 ms
 2  103.248.31.49 (103.248.31.49)  1.067 ms  1.072 ms  1.066 ms
 3  12.12.200.41 (12.12.200.41)  2.053 ms * *
 4  72.14.194.60 (72.14.194.60)  4.566 ms  4.579 ms  4.631 ms
 5  108.170.248.177 (108.170.248.177)  4.632 ms  4.626 ms  5.151 ms
 6  209.85.248.27 (209.85.248.27)  5.163 ms 209.85.251.29 (209.85.251.29)  4.462 ms  4.462 ms
 7  bom05s10-in-f14.1e100.net (216.58.203.142)  4.053 ms  3.844 ms  3.833 ms
codept@codept-22 ~/Desktop $
codept@codept-22 ~/Desktop $
codept@codept-22 ~/Desktop $ traceroute amazon.com
traceroute to amazon.com (205.251.242.103), 30 hops max, 60 byte packets
 1  172.16.16.1 (172.16.16.1)  0.275 ms  0.263 ms  0.253 ms
 2  103.248.31.49 (103.248.31.49)  1.112 ms  1.125 ms  1.118 ms
 3  12.12.200.41 (12.12.200.41)  2.467 ms  2.439 ms *
 4  103.39.246.254 (103.39.246.254)  2.395 ms  1.940 ms  2.342 ms
 5  * 103.39.246.253 (103.39.246.253)  2.891 ms *
 6  nsg-static-173.107.75.182-airtel.com (182.75.107.173)  4.330 ms  4.029 ms  4.553 ms
 7  182.79.208.74 (182.79.208.74)  240.786 ms 182.79.211.49 (182.79.211.49)  229.614 ms 182.79.234.175 (182.79.234.175)  225.449 ms
 8  182.79.211.107 (182.79.211.107)  241.844 ms 182.79.178.70 (182.79.178.70)  5.354 ms 182.79.178.78 (182.79.178.78)  4.682 ms
 9  182.79.179.108 (182.79.179.108)  26.643 ms 182.79.181.3 (182.79.181.3)  32.882 ms 182.79.219.153 (182.79.219.153)  26.941 ms
10  182.79.177.48 (182.79.177.48)  22.767 ms 182.79.177.57 (182.79.177.57)  22.303 ms 182.79.188.248 (182.79.188.248)  26.492 ms
11  182.79.152.21 (182.79.152.21)  244.211 ms 123.62.129.194 (123.62.129.194)  240.284 ms 125.62.187.126 (125.62.187.126)  233.015 ms
12  paix01-sfo4.amazon.com (198.32.176.36)  237.252 ms  247.960 ms  252.014 ms
13  54.240.243.28 (54.240.243.28)  266.490 ms 54.240.243.148 (54.240.243.148)  260.822 ms 54.240.243.128 (54.240.243.128)  254.253 ms
14  54.240.243.155 (54.240.243.155)  261.733 ms 54.240.243.17 (54.240.243.17)  262.429 ms 54.240.243.55 (54.240.243.55)  247.017 ms
15  * * *
16  72.21.222.54 (72.21.222.54)  237.970 ms 54.239.41.176 (54.239.41.176)  268.222 ms 54.239.42.15 (54.239.42.15)  276.051 ms
17  54.239.43.66 (54.239.43.66)  259.399 ms * *
18  54.239.43.162 (54.239.43.162)  248.875 ms * *
19  54.239.42.209 (54.239.42.209)  257.183 ms 54.239.110.10 (54.239.110.10)  238.916 ms 54.239.43.62 (54.239.43.62)  252.353 ms
20  54.239.110.29 (54.239.110.29)  252.446 ms 54.239.111.99 (54.239.111.99)  261.335 ms *
21  54.239.109.232 (54.239.109.232)  270.416 ms 54.239.109.62 (54.239.109.62)  274.182 ms *
22  * 52.93.70.5 (52.93.70.5)  266.996 ms 54.239.109.183 (54.239.109.183)  237.639 ms
23  52.93.24.236 (52.93.24.236)  244.655 ms 52.93.24.226 (52.93.24.226)  286.693 ms 54.239.109.130 (54.239.109.130)  261.986 ms
24  * * *
25  * 52.93.27.235 (52.93.27.235)  287.780 ms *
26  * * 52.93.70.5 (52.93.70.5)  278.660 ms
27  * * *
28  * * *
29  * * *
30  * * *
codept@codept-22 ~/Desktop $
```

Fig 1: traceroute command

## 2. WHOIS

whois searches for an object in a WHOIS database. WHOIS is a query and response protocol that is widely used for querying databases that store the registered users of an Internet resource, such as a domain name or an IP address block, but is also used for a wider range of other information.Most modern versions of whois try to guess the right server to ask for the specified object. If no guess can be made, whois will connect to whois.networksolutions.com for NIC handles or whois.arin.net for IPv4 addresses and network names.

**Syntax :** whois [ -h HOST ] [ -p PORT ] [ -aCFHlLMmrRSVx ] [ -g SOURCE:FIRST-LAST ] [ -i ATTR ] [ -S SOURCE ] [ -T TYPE ] object

whois -t TYPE

whois -v TYPE

whois -q keyword

**Example: whois techjunkie.com**

```
jkos — -bash — 80×27
Registrars.
JKOSs-iMac:~ jkos$ whois techjunkie.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: TECHJUNKIE.COM
   Registrar: GODADDY.COM, LLC
   Sponsoring Registrar IANA ID: 146
   Whois Server: whois.godaddy.com
   Referral URL: http://www.godaddy.com
   Name Server: EARL.NS.CLOUDFLARE.COM
   Name Server: JANET.NS.CLOUDFLARE.COM
   Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
   Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibit
ed
   Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Updated Date: 27-nov-2016
   Creation Date: 09-mar-2005
   Expiration Date: 09-mar-2018

>>> Last update of whois database: Wed, 29 Mar 2017 05:39:58 GMT <<<
```

Fig 2: whois command

## 3. DIG

Dig stands for (Domain Information Groper) is a network administration command-line tool for querying Domain Name System (DNS) name servers. It is useful for verifying and troubleshooting DNS problems and also to perform DNS lookups and displays the answers that are returned from the name server that were queried. dig is part of the BIND domain name server software suite. dig command replaces older tool such as nslookup and the host. dig tool is available in major Linux distributions.

**Syntax:** dig [options] <hostname>

**Example:** dig linux-bible.com

```
susel:~ # dig linux-bible.com

; <<>> DiG 9.6-ESV-R7-P4 <<>> linux-bible.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59095
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;linux-bible.com.               IN      A

;; ANSWER SECTION:
linux-bible.com.        5       IN      A       198.57.241.163

;; Query time: 25 msec
;; SERVER: 192.168.198.2#53(192.168.198.2)
;; WHEN: Tue Sep  2 21:05:20 2014
;; MSG SIZE  rcvd: 49
```

Fig 3 : dig command

## 4. NSLOOKUP

The nslookup (which stands for name server lookup) command is a network utility program used to obtain information about internet servers. It finds name server information for domains by querying the Domain Name System.

Most computer operating systems include a built-in command line program with the same name. Some network providers also host web-based services of this same utility (like Network-Tools.com). These programs are all designed to perform name server lookups against specified domains.

**Syntax :** nslookup [option] <hostname>

**Example :** nslookup soet.aiktc.ac.in:8080

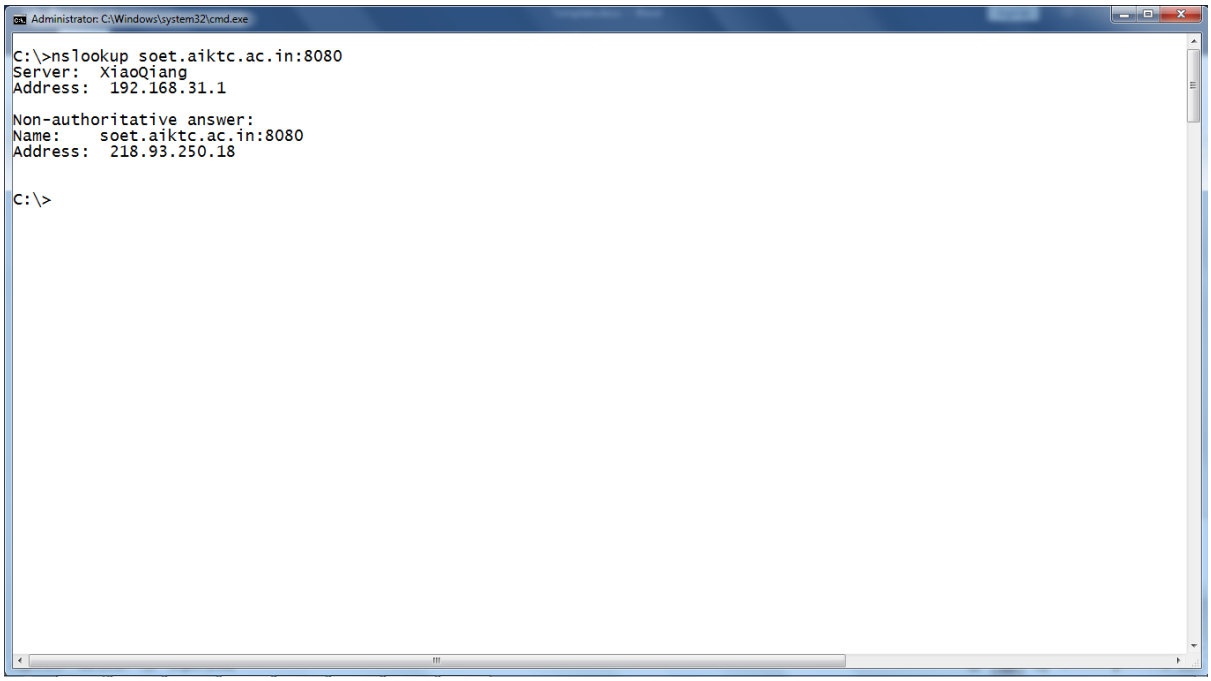


Fig 4 : nslookup command